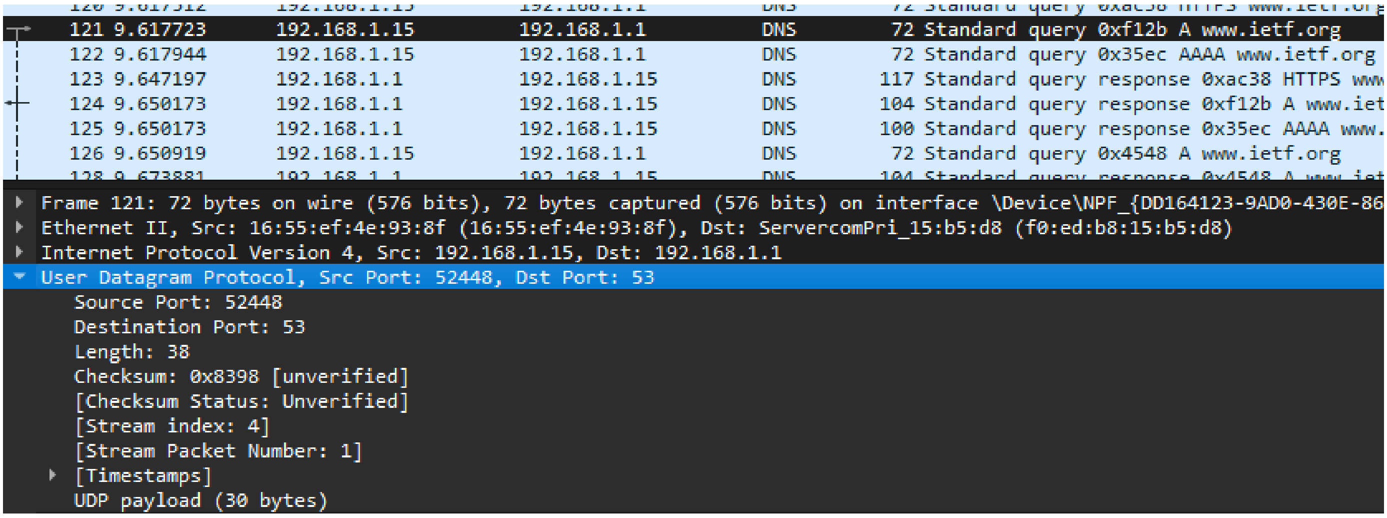
Assignment 5 DNS wireshark

Q1. Locate the DNS query and response messages. Are they sent over UDP or TCP?

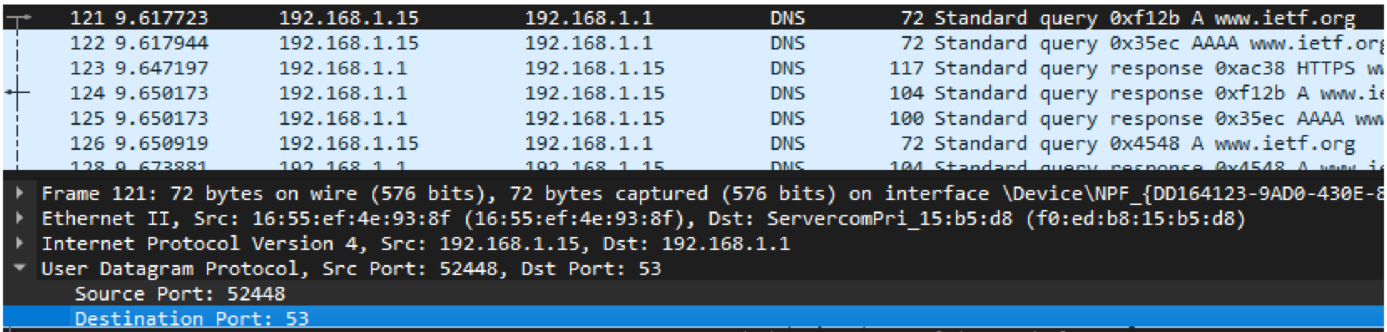
Ans- DNS query and response messages are sent over UDP.



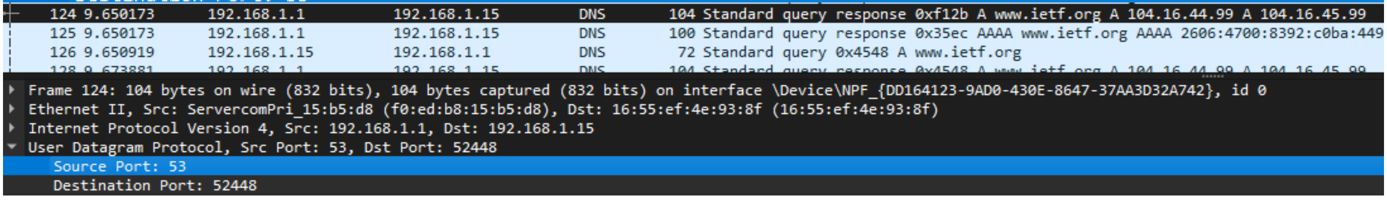
```
120 9.617312   192.168.1.15   192.168.1.1    DNS    72 Standard query 0xac38 HTTPS www.ietf.org
121 9.617723   192.168.1.15   192.168.1.1    DNS    72 Standard query 0xf12b A www.ietf.org
122 9.617944   192.168.1.15   192.168.1.1    DNS    72 Standard query 0x35ec AAAA www.ietf.org
123 9.647197   192.168.1.1    192.168.1.15   DNS   117 Standard query response 0xac38 HTTPS www
124 9.650173   192.168.1.1    192.168.1.15   DNS   104 Standard query response 0xf12b A www.iet
125 9.650173   192.168.1.1    192.168.1.15   DNS   100 Standard query response 0x35ec AAAA www.
126 9.650919   192.168.1.15   192.168.1.1    DNS    72 Standard query 0x4548 A www.ietf.org
128 9.673881   192.168.1.1    192.168.1.15   DNS   104 Standard query response 0x4548 A www.iet
Frame 121: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{DD164123-9AD0-430E-86
Ethernet II, Src: 16:55:ef:4e:93:8f (16:55:ef:4e:93:8f), Dst: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 52448, Dst Port: 53
    Source Port: 52448
    Destination Port: 53
    Length: 38
    Checksum: 0x8398 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
    [Stream Packet Number: 1]
    [Timestamps]
    UDP payload (30 bytes)
```

Q2. What is the destination port for the DNS query message? What is the source port of the DNS response message?

Ans- Destination port for the DNS query message is 53. The source port of the DNS response message is also 53.



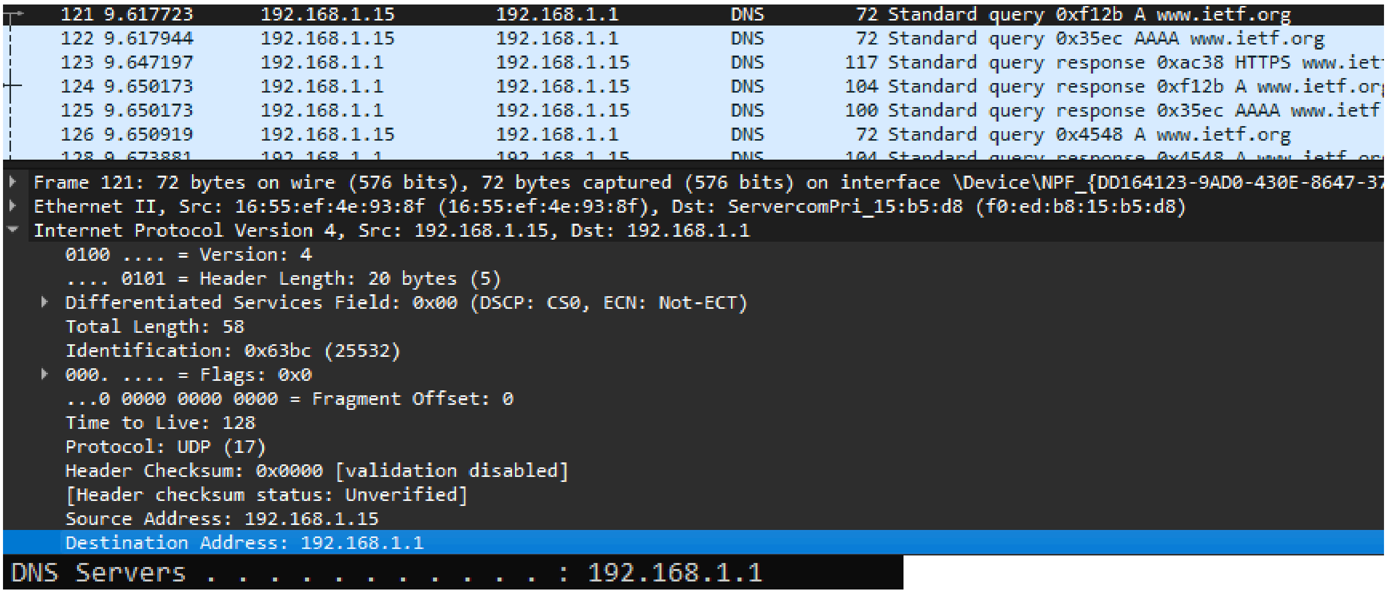
```
121 9.617723   192.168.1.15   192.168.1.1    DNS    72 Standard query 0xf12b A www.ietf.org
122 9.617944   192.168.1.15   192.168.1.1    DNS    72 Standard query 0x35ec AAAA www.ietf.org
123 9.647197   192.168.1.1    192.168.1.15   DNS   117 Standard query response 0xac38 HTTPS ww
124 9.650173   192.168.1.1    192.168.1.15   DNS   104 Standard query response 0xf12b A www.ie
125 9.650173   192.168.1.1    192.168.1.15   DNS   100 Standard query response 0x35ec AAAA ww
126 9.650919   192.168.1.15   192.168.1.1    DNS    72 Standard query 0x4548 A www.ietf.org
128 9.673881   192.168.1.1    192.168.1.15   DNS   104 Standard query response 0x4548 A www.ie
Frame 121: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{DD164123-9AD0-430E-8
Ethernet II, Src: 16:55:ef:4e:93:8f (16:55:ef:4e:93:8f), Dst: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 52448, Dst Port: 53
    Source Port: 52448
    Destination Port: 53
```



```
124 9.650173   192.168.1.1    192.168.1.15   DNS   104 Standard query response 0xf12b A www.ietf.org A 104.16.44.99 A 104.16.45.99
125 9.650173   192.168.1.1    192.168.1.15   DNS   100 Standard query response 0x35ec AAAA www.ietf.org AAAA 2606:4700:8392:c0ba:449
126 9.650919   192.168.1.15   192.168.1.1    DNS    72 Standard query 0x4548 A www.ietf.org
128 9.673881   192.168.1.1    192.168.1.15   DNS   104 Standard query response 0x4548 A www.ietf.org A 104.16.44.99 A 104.16.45.99
Frame 124: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{DD164123-9AD0-430E-8647-37AA3D32A742}, id 0
Ethernet II, Src: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8), Dst: 16:55:ef:4e:93:8f (16:55:ef:4e:93:8f)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.15
User Datagram Protocol, Src Port: 53, Dst Port: 52448
    Source Port: 53
    Destination Port: 52448
```

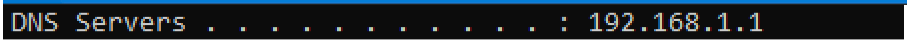
Q3. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Ans- DNS query message is sent to IP address 192.168.1.1 and Yes these two IP address are exactly same.



```
121 9.617723   192.168.1.15   192.168.1.1    DNS    72 Standard query 0xf12b A www.ietf.org
122 9.617944   192.168.1.15   192.168.1.1    DNS    72 Standard query 0x35ec AAAA www.ietf.org
123 9.647197   192.168.1.1    192.168.1.15   DNS   117 Standard query response 0xac38 HTTPS www.iet
124 9.650173   192.168.1.1    192.168.1.15   DNS   104 Standard query response 0xf12b A www.ietf.or
125 9.650173   192.168.1.1    192.168.1.15   DNS   100 Standard query response 0x35ec AAAA www.ietf
126 9.650919   192.168.1.15   192.168.1.1    DNS    72 Standard query 0x4548 A www.ietf.org
128 9.673881   192.168.1.1    192.168.1.15   DNS   104 Standard query response 0x4548 A www.ietf.or
```

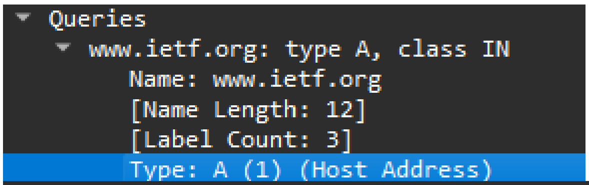
```
Frame 121: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{DD164123-9AD0-430E-8647-37
Ethernet II, Src: 16:55:ef:4e:93:8f (16:55:ef:4e:93:8f), Dst: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0x63bc (25532)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.15
    Destination Address: 192.168.1.1
```



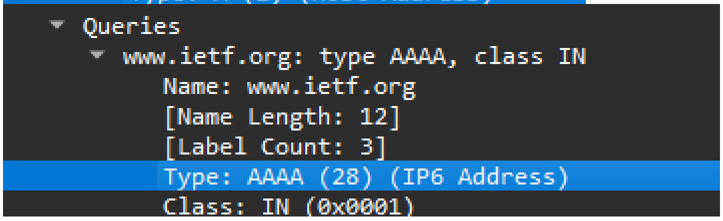
```
DNS Servers . . . . . . . . . . . : 192.168.1.1
```

Q4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans- It is a standard Type A query that means it is querying the DNS server to obtain IPv4 address of the target. No this query message does not contain any answers. Also just below this packet we have AAAA (Quad A) type query request (used for IPv6 address) for the same domain name and again this query message does not contain any answers.



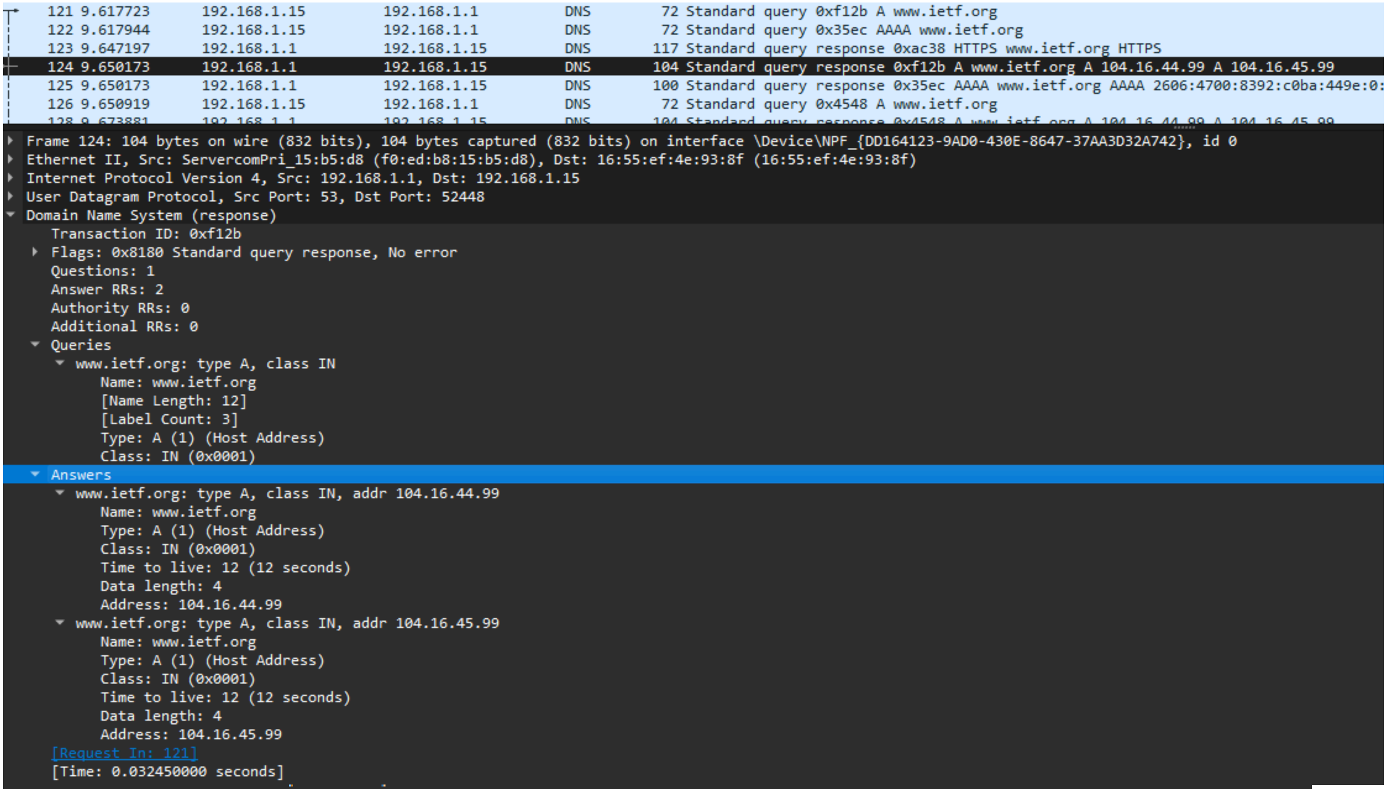
```
Queries
    www.ietf.org: type A, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (1) (Host Address)
```



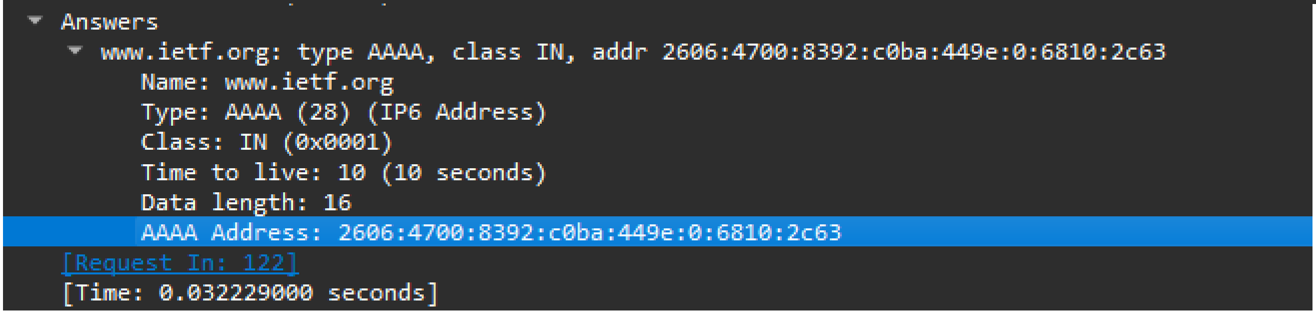
```
Queries
    www.ietf.org: type AAAA, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
```

Q5. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

Ans- There are two answers in the DNS response message. Each answer contains a unique IPv4 address for the domain name www.ietf.org, so in total we have got two IPv4 address from the query in return. Also in case of IPv6 packet the query response contains only one answer that contains a single IPv6 address.



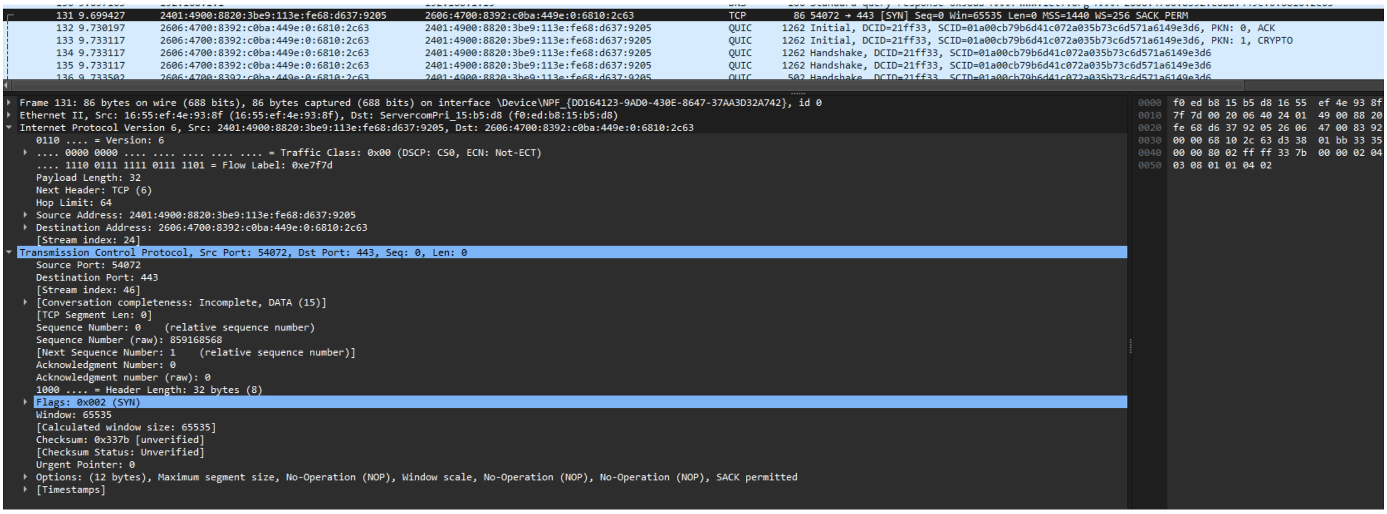
```
121 9.617723   192.168.1.15   192.168.1.1    DNS    72 Standard query 0xf12b A www.ietf.org
122 9.617944   192.168.1.15   192.168.1.1    DNS    72 Standard query 0x35ec AAAA www.ietf.org
123 9.647197   192.168.1.1    192.168.1.15   DNS   117 Standard query response 0xac38 HTTPS www.ietf.org HTTPS
124 9.650173   192.168.1.1    192.168.1.15   DNS   104 Standard query response 0xf12b A www.ietf.org A 104.16.44.99 A 104.16.45.99
125 9.650173   192.168.1.1    192.168.1.15   DNS   100 Standard query response 0x35ec AAAA www.ietf.org AAAA 2606:4700:8392:c0ba:449e:0:
126 9.650919   192.168.1.15   192.168.1.1    DNS    72 Standard query 0x4548 A www.ietf.org
128 9.673881   192.168.1.1    192.168.1.15   DNS   104 Standard query response 0x4548 A www.ietf.org A 104.16.44.99 A 104.16.45.99

Frame 124: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{DD164123-9AD0-430E-8647-37AA3D32A742}, id 0
Ethernet II, Src: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8), Dst: 16:55:ef:4e:93:8f (16:55:ef:4e:93:8f)
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.15
User Datagram Protocol, Src Port: 53, Dst Port: 52448
Domain Name System (response)
    Transaction ID: 0xf12b
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.ietf.org: type A, class IN
            Name: www.ietf.org
            [Name Length: 12]
            [Label Count: 3]
            Type: A (1) (Host Address)
            Class: IN (0x0001)
    Answers
        www.ietf.org: type A, class IN, addr 104.16.44.99
            Name: www.ietf.org
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Time to live: 12 (12 seconds)
            Data length: 4
            Address: 104.16.44.99
        www.ietf.org: type A, class IN, addr 104.16.45.99
            Name: www.ietf.org
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Time to live: 12 (12 seconds)
            Data length: 4
            Address: 104.16.45.99
    [Request In: 121]
    [Time: 0.032450000 seconds]
```



```
Answers
    www.ietf.org: type AAAA, class IN, addr 2606:4700:8392:c0ba:449e:0:6810:2c63
        Name: www.ietf.org
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
        Time to live: 10 (10 seconds)
        Data length: 16
        AAAA Address: 2606:4700:8392:c0ba:449e:0:6810:2c63
[Request In: 122]
[Time: 0.032229000 seconds]
```

Q6. 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?

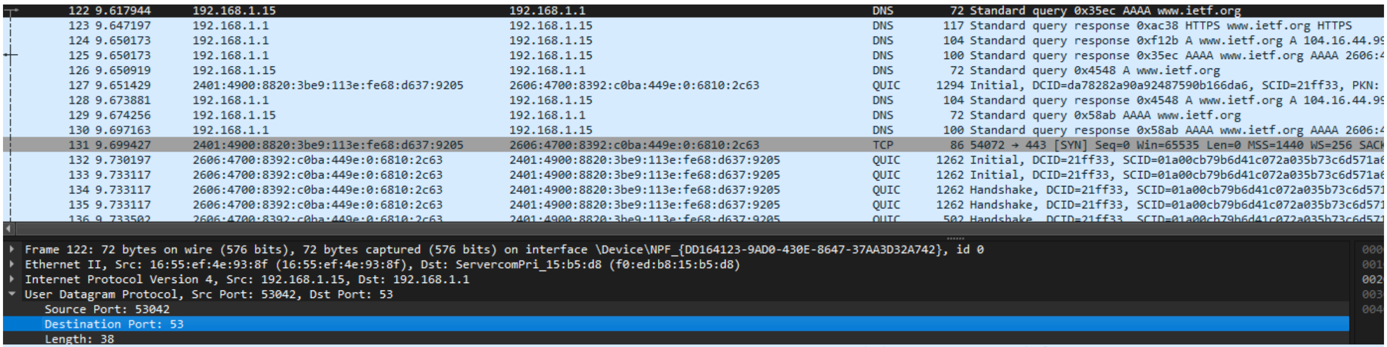
Ans- Yes the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message. But the commnunication is taking place over IPv6 instead of IPv4.



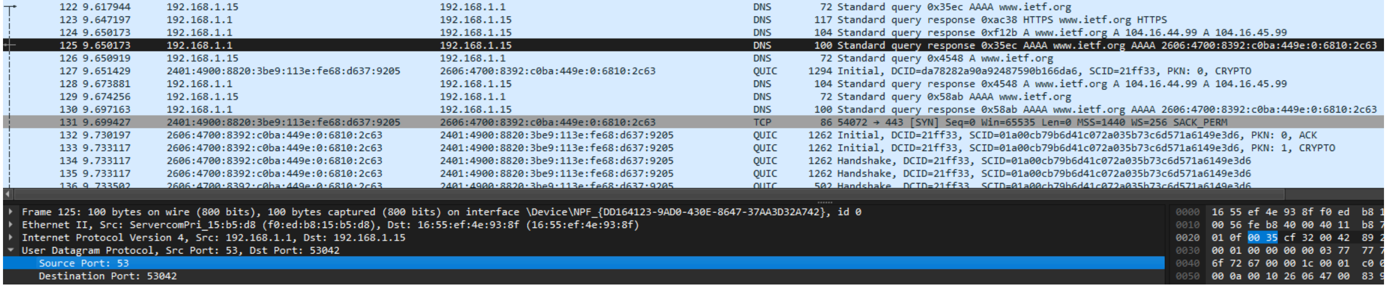
```
131 9.699427   2401:4900:8820:3be9:113e:fe68:d637:9205   2606:4700:8392:c0ba:449e:0:6810:2c63      TCP     86 54072 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
132 9.730197   2606:4700:8392:c0ba:449e:0:6810:2c63      2401:4900:8820:3be9:113e:fe68:d637:9205   QUIC  1262 Initial, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571a6149e3d6, PKN: 0, ACK
133 9.733117   2606:4700:8392:c0ba:449e:0:6810:2c63      2401:4900:8820:3be9:113e:fe68:d637:9205   QUIC  1262 Initial, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571a6149e3d6, PKN: 1, CRYPTO
134 9.733117   2606:4700:8392:c0ba:449e:0:6810:2c63      2401:4900:8820:3be9:113e:fe68:d637:9205   QUIC  1262 Handshake, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571a6149e3d6
135 9.733117   2606:4700:8392:c0ba:449e:0:6810:2c63      2401:4900:8820:3be9:113e:fe68:d637:9205   QUIC  1262 Handshake, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571a6149e3d6
136 9.733502   2606:4700:8392:c0ba:449e:0:6810:2c63      2401:4900:8820:3be9:113e:fe68:d637:9205   QUIC   502 Handshake, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571a6149e3d6

Frame 131: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{DD164123-9AD0-430E-8647-37AA3D32A742}, id 0
Ethernet II, Src: 16:55:ef:4e:93:8f (16:55:ef:4e:93:8f), Dst: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
Internet Protocol Version 6, Src: 2401:4900:8820:3be9:113e:fe68:d637:9205, Dst: 2606:4700:8392:c0ba:449e:0:6810:2c63
    0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 1110 0111 1111 0111 1101 = Flow Label: 0xe7f7d
    Payload Length: 32
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: 2401:4900:8820:3be9:113e:fe68:d637:9205
    Destination Address: 2606:4700:8392:c0ba:449e:0:6810:2c63
    [Stream index: 24]
Transmission Control Protocol, Src Port: 54072, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 54072
    Destination Port: 443
    [Stream index: 46]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 859168568
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x002 (SYN)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0x337b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    [Timestamps]

0000  f0 ed b8 15 b5 d8 16 55  ef 4e 93 8f
0010  7f 7d 00 20 06 40 24 01  49 00 88 20
0020  fe 68 d6 37 92 05 26 06  47 00 83 92
0030  00 00 68 10 2c 63 d3 38  01 bb 33 35
0040  00 00 80 02 ff ff 33 7b  00 00 02 04
0050  03 08 01 01 04 02
```

Q7. What is the destination port for the DNS query message? What is the source port of the DNS response message?

Ans- Destination port for the DNS query message is 53. The source port of the DNS response message is also 53.



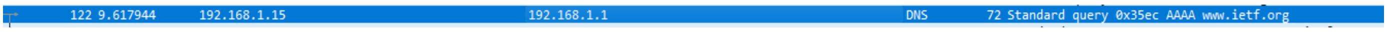
```
122 9.617944   192.168.1.15                            192.168.1.1                             DNS     72 Standard query 0x35ec AAAA www.ietf.org
123 9.647197   192.168.1.1                             192.168.1.15                            DNS    117 Standard query response 0xac38 HTTPS www.ietf.org HTTPS
124 9.650173   192.168.1.1                             192.168.1.15                            DNS    104 Standard query response 0xf12b A www.ietf.org A 104.16.44.9
125 9.650173   192.168.1.1                             192.168.1.15                            DNS    100 Standard query response 0x35ec AAAA www.ietf.org AAAA 2606:4
126 9.650919   192.168.1.15                            192.168.1.1                             DNS     72 Standard query 0x4548 A www.ietf.org
127 9.651429   2401:4900:8820:3be9:113e:fe68:d637:9205 2606:4700:8392:c0ba:449e:0:6810:2c63    QUIC  1294 Initial, DCID=da78282a90a92487590b166da6, SCID=21ff33, PKN:
128 9.673881   192.168.1.1                             192.168.1.15                            DNS    104 Standard query response 0x4548 A www.ietf.org A 104.16.44.9
129 9.674256   192.168.1.15                            192.168.1.1                             DNS     72 Standard query 0x58ab AAAA www.ietf.org
130 9.697163   192.168.1.1                             192.168.1.15                            DNS    100 Standard query response 0x58ab AAAA www.ietf.org AAAA 2606:4
131 9.699427   2401:4900:8820:3be9:113e:fe68:d637:9205 2606:4700:8392:c0ba:449e:0:6810:2c63    TCP     86 54072 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK
132 9.730197   2606:4700:8392:c0ba:449e:0:6810:2c63    2401:4900:8820:3be9:113e:fe68:d637:9205 QUIC  1262 Initial, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571a
133 9.733117   2606:4700:8392:c0ba:449e:0:6810:2c63    2401:4900:8820:3be9:113e:fe68:d637:9205 QUIC  1262 Initial, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571a
134 9.733117   2606:4700:8392:c0ba:449e:0:6810:2c63    2401:4900:8820:3be9:113e:fe68:d637:9205 QUIC  1262 Handshake, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571
135 9.733117   2606:4700:8392:c0ba:449e:0:6810:2c63    2401:4900:8820:3be9:113e:fe68:d637:9205 QUIC  1262 Handshake, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571
136 9.733502   2606:4700:8392:c0ba:449e:0:6810:2c63    2401:4900:8820:3be9:113e:fe68:d637:9205 QUIC   502 Handshake, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571

▸ Frame 122: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{DD164123-9AD0-430E-8647-37AA3D32A742}, id 0
▸ Ethernet II, Src: 16:55:ef:4e:93:8f (16:55:ef:4e:93:8f), Dst: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
▸ Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.1
▾ User Datagram Protocol, Src Port: 53042, Dst Port: 53
    Source Port: 53042
    Destination Port: 53
    Length: 38
```



```
122 9.617944   192.168.1.15                            192.168.1.1                             DNS     72 Standard query 0x35ec AAAA www.ietf.org
123 9.647197   192.168.1.1                             192.168.1.15                            DNS    117 Standard query response 0xac38 HTTPS www.ietf.org HTTPS
124 9.650173   192.168.1.1                             192.168.1.15                            DNS    104 Standard query response 0xf12b A www.ietf.org A 104.16.44.99 A 104.16.45.99
125 9.650173   192.168.1.1                             192.168.1.15                            DNS    100 Standard query response 0x35ec AAAA www.ietf.org AAAA 2606:4700:8392:c0ba:449e:0:6810:2c63
126 9.650919   192.168.1.15                            192.168.1.1                             DNS     72 Standard query 0x4548 A www.ietf.org
127 9.651429   2401:4900:8820:3be9:113e:fe68:d637:9205 2606:4700:8392:c0ba:449e:0:6810:2c63    QUIC  1294 Initial, DCID=da78282a90a92487590b166da6, SCID=21ff33, PKN: 0, CRYPTO
128 9.673881   192.168.1.1                             192.168.1.15                            DNS    104 Standard query response 0x4548 A www.ietf.org A 104.16.44.99 A 104.16.45.99
129 9.674256   192.168.1.15                            192.168.1.1                             DNS     72 Standard query 0x58ab AAAA www.ietf.org
130 9.697163   192.168.1.1                             192.168.1.15                            DNS    100 Standard query response 0x58ab AAAA www.ietf.org AAAA 2606:4700:8392:c0ba:449e:0:6810:2c63
131 9.699427   2401:4900:8820:3be9:113e:fe68:d637:9205 2606:4700:8392:c0ba:449e:0:6810:2c63    TCP     86 54072 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
132 9.730197   2606:4700:8392:c0ba:449e:0:6810:2c63    2401:4900:8820:3be9:113e:fe68:d637:9205 QUIC  1262 Initial, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571a6149e3d6, PKN: 0, ACK
133 9.733117   2606:4700:8392:c0ba:449e:0:6810:2c63    2401:4900:8820:3be9:113e:fe68:d637:9205 QUIC  1262 Initial, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571a6149e3d6, PKN: 1, CRYPTO
134 9.733117   2606:4700:8392:c0ba:449e:0:6810:2c63    2401:4900:8820:3be9:113e:fe68:d637:9205 QUIC  1262 Handshake, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571a6149e3d6
135 9.733117   2606:4700:8392:c0ba:449e:0:6810:2c63    2401:4900:8820:3be9:113e:fe68:d637:9205 QUIC  1262 Handshake, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571a6149e3d6
136 9.733502   2606:4700:8392:c0ba:449e:0:6810:2c63    2401:4900:8820:3be9:113e:fe68:d637:9205 QUIC   502 Handshake, DCID=21ff33, SCID=01a00cb79b6d41c072a035b73c6d571a6149e3d6

▸ Frame 125: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface \Device\NPF_{DD164123-9AD0-430E-8647-37AA3D32A742}, id 0
▸ Ethernet II, Src: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8), Dst: 16:55:ef:4e:93:8f (16:55:ef:4e:93:8f)
▸ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.15
▾ User Datagram Protocol, Src Port: 53, Dst Port: 53042
    Source Port: 53
    Destination Port: 53042

0000  16 55 ef 4e 93 8f f0 ed  b8 1
0010  00 56 fe b8 40 00 40 11  b8 7
0020  01 0f 00 35 cf 32 00 42  89 2
0030  00 01 00 00 00 00 03 77  77 7
0040  6f 72 67 00 00 1c 00 01  c0 0
0050  00 0a 00 10 26 06 47 00  83 9
```

Q8. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans- `192.168.1.1` is the IP address to which DNS query message is sent. Yes this the IP address of your default local DNS server.



```
122 9.617944   192.168.1.15   192.168.1.1   DNS   72 Standard query 0x35ec AAAA www.ietf.org
```

Q9. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans- Repeated Question, answered above already.

Q10. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

Ans- Repeated Question, answered above already.