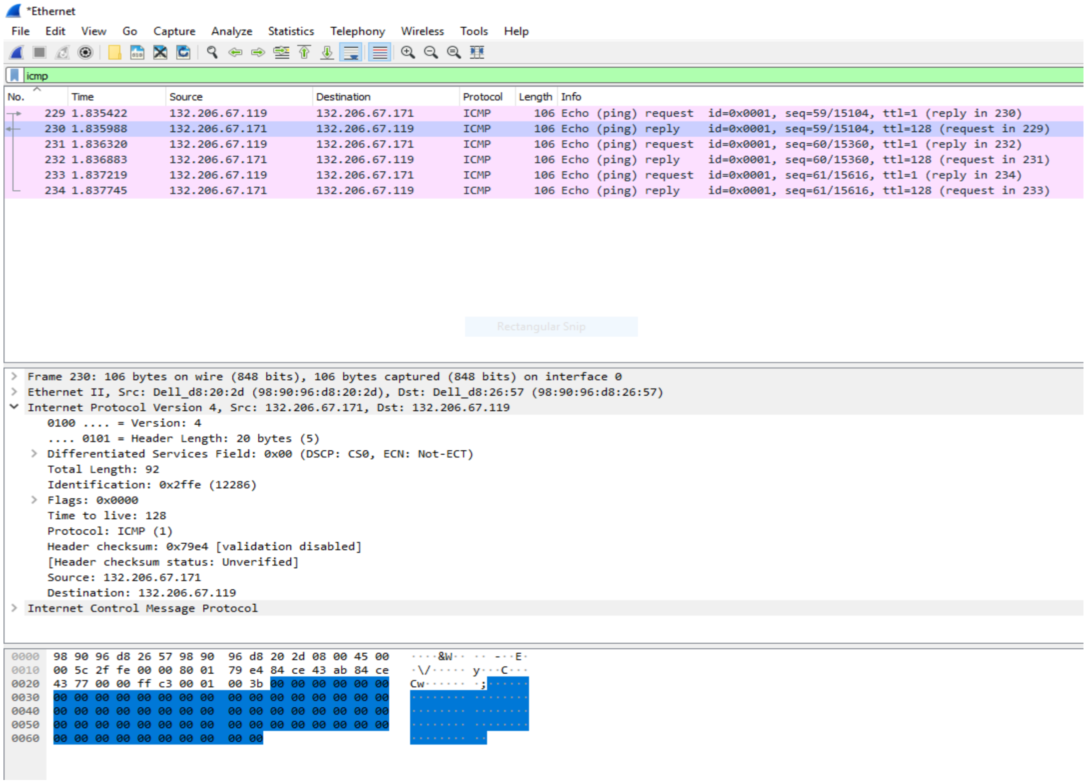
Part 1: Internet Protocol (IP)



```
No.     Time       Source           Destination      Protocol Length Info
    229 1.835422   132.206.67.119   132.206.67.171   ICMP     106 Echo (ping) request  id=0x0001, seq=59/15104, ttl=1 (reply in 230)
    230 1.835988   132.206.67.171   132.206.67.119   ICMP     106 Echo (ping) reply    id=0x0001, seq=59/15104, ttl=128 (request in 229)
    231 1.836320   132.206.67.119   132.206.67.171   ICMP     106 Echo (ping) request  id=0x0001, seq=60/15360, ttl=1 (reply in 232)
    232 1.836883   132.206.67.171   132.206.67.119   ICMP     106 Echo (ping) reply    id=0x0001, seq=60/15360, ttl=128 (request in 231)
    233 1.837219   132.206.67.119   132.206.67.171   ICMP     106 Echo (ping) request  id=0x0001, seq=61/15616, ttl=1 (reply in 234)
    234 1.837745   132.206.67.171   132.206.67.119   ICMP     106 Echo (ping) reply    id=0x0001, seq=61/15616, ttl=128 (request in 233)
```

```
> Frame 230: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: Dell_d8:20:2d (98:90:96:d8:20:2d), Dst: Dell_d8:26:57 (98:90:96:d8:26:57)
v Internet Protocol Version 4, Src: 132.206.67.171, Dst: 132.206.67.119
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x2ffe (12286)
  > Flags: 0x0000
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x79e4 [validation disabled]
    [Header checksum status: Unverified]
    Source: 132.206.67.171
    Destination: 132.206.67.119
> Internet Control Message Protocol
```

```
0000  98 90 96 d8 26 57 98 90  96 d8 20 2d 08 00 45 00   ····&W·· ·· -··E·
0010  00 5c 2f fe 00 00 80 01  79 e4 84 ce 43 ab 84 ce   ·\/····· y···C···
0020  43 77 00 00 ff c3 00 01  00 3b 00 00 00 00 00 00   Cw······ ·;······
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00                     ········ ··
```

Source: 132.206.67.119

Destination: 132.206.67.171

IP of DNS server: 132.206.44.21

1. How many ICMP packets are in the list plane?

There are 6 ICMP packets in the list.

2. How many probe packets are sent from the source to the destination for each TTL?

There are 3 probe packets sent from the source to the destination for each TTL.

3. The last few echo-request ICMP packets are followed by the echo-reply ICMP packets. Compare one of them with the corresponding reply. Determine which fields are similar and which fields are different? Explain the reason.

By comparing one packet echo with its query and its destination, we can observe that only few elements are different. The first element is the TTL values. These values are different because each subsequent packet has its TTL value incremented by 1. The source and destination MAC ID’s are also different since they do not come from the same device. The ip address of the source is 132.206.67.119 and the ip address of the destination is 132.206.67.171. These are different due to the fact that the source must have information on the destination to know exactly where it is, this is a way to make sure they are a pair. The checksum is also another field that is different between the two. For the similarities, the other fields are kept the same, such as the identifier and the data.

4. What are the TTL values for these last few packets? Determine the number of routers between the source and destination based on these TTL values.

The last few packets have a request TTL value of 1 and a reply TTL value of 128. Between the source and the destination, only 1 hop was required to reach destination since we were looking at another computer in the class. This makes sense as they should all be connected to the same router. Therefore, 1 router is between the source and its destination.

5.Examine the IP packet header of the last echo-request ICMP packet, what is the value in the "Protocol" field? What does this field indicate?

The protocol used is ICMP (01). This field indicated that you can reach destination when the TTL value is set to 0.

6. How many bytes are in this IP header? How many bytes are in the payload of this IP packet? Explain how you determined the number of payload bytes.

The ICMP header contains 20 bytes. Then the total length is 92 bytes. Therefore, we can calculate the payload by doing the total minus the header to have the size of the actually data. By doing so, we get 92-20, which is equal to 72 bytes for the payload.

7. Has this IP packet been fragmented? Explain how you determined whether or not the packet has been fragmented.

The IP packet is not fragmented, because the "more fragment" flag is not set, the bit is 0. This permits to determine if it was fragmented. If it were to be, the bit value would be set to 1.

Part 2: Domain Name System (DNS)

8.Use nslookup to determine the IP address of www.cbc.ca. What is the IP address of this web server?

The IP address of the web server is 184.28.201.38.

9. Use nslookup to determine the authoritative DNS servers for McGill University.

The authoritative DNS server name is pirns1.mcgill.ca and its IP address is 132.206.44.21.

10. What are the destination port number for the DNS query message and the Source port number of the DNS response message?

The destination port is 63084 and the source port is 53.

11. What is the destination IP address of the DNS query? Is this the IP address of your default local DNS server?

The IP address of the source is 132.206.44.21. The IP address of the destination is 132.206.67.119. The IP address of the destination does match with the address of the default local DNS server. Therefore, yes, this is the IP address of our default local DNS server.

12. Examine the DNS query. What is the "Type" of the DNS query? What does this "Type" mean? What are the other values for this field?

The type of the query is a standard query of type AAAA. This type returns a IPv6 address, that is commonly used to map hostnames to an IP address of the host. The other values of this field are the name of the host, the type of address and the class.

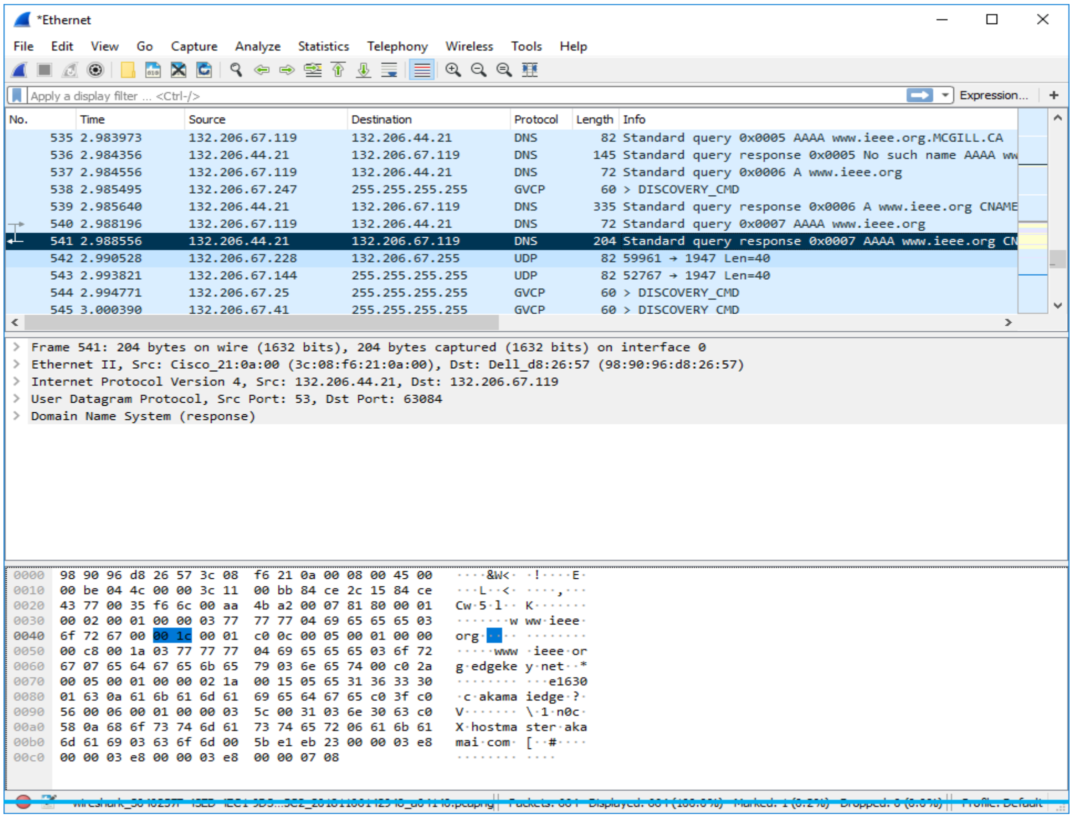
13. Which bit in the "Flags" field indicates that the message is a query or a response?

The bits in the Flags fields are first bit of the sequence. If the value is 0, this means that it is a request, and on the opposite, if the first bit is set to 1, then this is a response.

14. Which field of the response message contains the IP address of www.ieee.org?

The destination field of the response messages contains the IP address.

15. Provide a screenshot.



```
No.   Time       Source           Destination      Protocol Length Info
  535 2.983973   132.206.67.119   132.206.44.21    DNS        82 Standard query 0x0005 AAAA www.ieee.org.MCGILL.CA
  536 2.984356   132.206.44.21    132.206.67.119   DNS       145 Standard query response 0x0005 No such name AAAA ww
  537 2.984556   132.206.67.119   132.206.44.21    DNS        72 Standard query 0x0006 A www.ieee.org
  538 2.985495   132.206.67.247   255.255.255.255  GVCP       60 > DISCOVERY_CMD
  539 2.985640   132.206.44.21    132.206.67.119   DNS       335 Standard query response 0x0006 A www.ieee.org CNAME
  540 2.988196   132.206.67.119   132.206.44.21    DNS        72 Standard query 0x0007 AAAA www.ieee.org
  541 2.988556   132.206.44.21    132.206.67.119   DNS       204 Standard query response 0x0007 AAAA www.ieee.org CN
  542 2.990528   132.206.67.228   132.206.67.255   UDP        82 59961 → 1947 Len=40
  543 2.993821   132.206.67.144   255.255.255.255  UDP        82 52767 → 1947 Len=40
  544 2.994771   132.206.67.25    255.255.255.255  GVCP       60 > DISCOVERY_CMD
  545 3.000390   132.206.67.41    255.255.255.255  GVCP       60 > DISCOVERY_CMD
```

```
> Frame 541: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on interface 0
> Ethernet II, Src: Cisco_21:0a:00 (3c:08:f6:21:0a:00), Dst: Dell_d8:26:57 (98:90:96:d8:26:57)
> Internet Protocol Version 4, Src: 132.206.44.21, Dst: 132.206.67.119
> User Datagram Protocol, Src Port: 53, Dst Port: 63084
> Domain Name System (response)
```

```
0000  98 90 96 d8 26 57 3c 08  f6 21 0a 00 08 00 45 00   ····&W<· ·!····E·
0010  00 be 04 4c 00 00 3c 11  00 bb 84 ce 2c 15 84 ce   ···L··<· ····,···
0020  43 77 00 35 f6 6c 00 aa  4b a2 00 07 81 80 00 01   Cw·5·l·· K·······
0030  00 02 00 01 00 00 03 77  77 77 04 69 65 65 65 03   ·······w ww·ieee·
0040  6f 72 67 00 00 1c 00 01  c0 0c 00 05 00 01 00 00   org····· ········
0050  00 c8 00 1a 03 77 77 77  04 69 65 65 65 03 6f 72   ·····www ·ieee·or
0060  67 07 65 64 67 65 6b 65  79 03 6e 65 74 00 c0 2a   g·edgeke y·net··*
0070  00 05 00 01 00 00 02 1a  00 15 05 65 31 36 33 30   ········ ···e1630
0080  01 63 0a 61 6b 61 6d 61  69 65 64 67 65 c0 3f c0   ·c·akama iedge·?·
0090  56 00 06 00 01 00 00 03  5c 00 31 03 6e 30 63 c0   V······· \·1·n0c·
00a0  58 0a 68 6f 73 74 6d 61  73 74 65 72 06 61 6b 61   X·hostma ster·aka
00b0  6d 61 69 03 63 6f 6d 00  5b e1 eb 23 00 00 03 e8   mai·com· [··#····
00c0  00 00 03 e8 00 00 03 e8  00 00 07 08               ········ ····
```

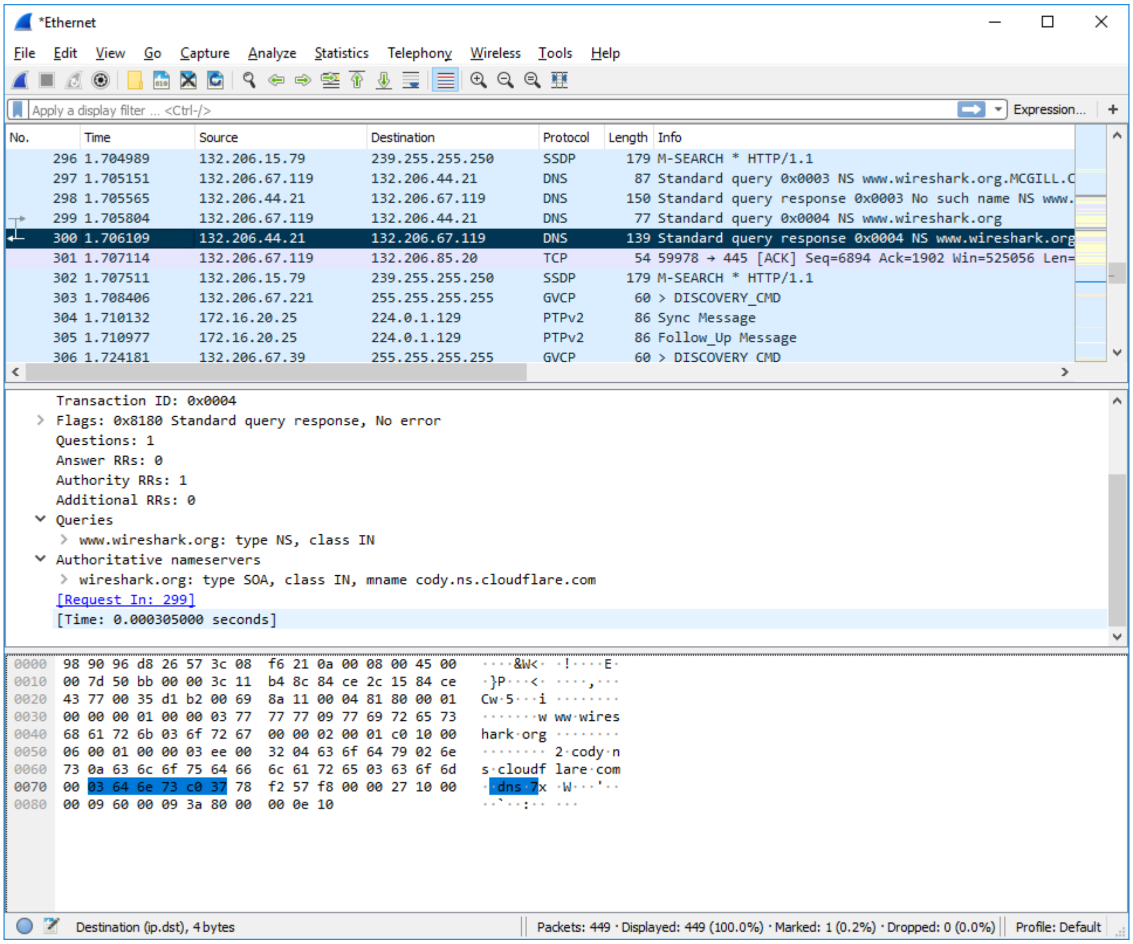
16. What is the destination IP address of the DNS query? What does this address correspond to?

The destination IP address of the DNS query is 132.206.67.119, and it corresponds to our local DNS server.

17. Determine the "Type" of DNS query. What is the authoritative name server of <u>www.wireshark.org</u>. What is the role of an authoritative name server?

The type of the DNS query is NS. The authoritative name server is the same as primary name server and is cody.ns.cloudflare.com. The role of an authoritative name server is to provide actual answer to the DNS queries. Therefore, it provides original and definitive answers to DNS queries. It does not provides just cached answers that were obtained from another name server. Therefore, it only returns answers to queries about DNS that are installed in its configuration system.

18. Provide a screenshot.



```
No.  Time      Source          Destination      Protocol Length Info
 296 1.704989  132.206.15.79   239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
 297 1.705151  132.206.67.119  132.206.44.21    DNS       87 Standard query 0x0003 NS www.wireshark.org.MCGILL.C
 298 1.705565  132.206.44.21   132.206.67.119   DNS      150 Standard query response 0x0003 No such name NS www.
 299 1.705804  132.206.67.119  132.206.44.21    DNS       77 Standard query 0x0004 NS www.wireshark.org
 300 1.706109  132.206.44.21   132.206.67.119   DNS      139 Standard query response 0x0004 NS www.wireshark.org
 301 1.707114  132.206.67.119  132.206.85.20    TCP       54 59978 → 445 [ACK] Seq=6894 Ack=1902 Win=525056 Len=
 302 1.707511  132.206.15.79   239.255.255.250  SSDP     179 M-SEARCH * HTTP/1.1
 303 1.708406  132.206.67.221  255.255.255.255  GVCP      60 > DISCOVERY_CMD
 304 1.710132  172.16.20.25    224.0.1.129      PTPv2     86 Sync Message
 305 1.710977  172.16.20.25    224.0.1.129      PTPv2     86 Follow_Up Message
 306 1.724181  132.206.67.39   255.255.255.255  GVCP      60 > DISCOVERY_CMD
```

```
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  ∨ Queries
      > www.wireshark.org: type NS, class IN
  ∨ Authoritative nameservers
      > wireshark.org: type SOA, class IN, mname cody.ns.cloudflare.com
    [Request In: 299]
    [Time: 0.000305000 seconds]
```

```
0000  98 90 96 d8 26 57 3c 08  f6 21 0a 00 08 00 45 00   ····&W<· ·!····E·
0010  00 7d 50 bb 00 00 3c 11  b4 8c 84 ce 2c 15 84 ce   ·}P···<· ····,···
0020  43 77 00 35 d1 b2 00 69  8a 11 00 04 81 80 00 01   Cw·5···i ········
0030  00 00 00 01 00 00 03 77  77 77 09 77 69 72 65 73   ·······w ww·wires
0040  68 61 72 6b 03 6f 72 67  00 00 02 00 01 c0 10 00   hark·org ········
0050  06 00 01 00 00 03 ee 00  32 04 63 6f 64 79 02 6e   ········ 2·cody·n
0060  73 0a 63 6c 6f 75 64 66  6c 61 72 65 03 63 6f 6d   s·cloudf lare·com
0070  00 03 64 6e 73 c0 37 78  f2 57 f8 00 00 27 10 00   ··dns·7x ·W···'··
0080  00 09 60 00 09 3a 80 00  00 0e 10                  ··`··:·· ···
```

Destination (ip.dst), 4 bytes | Packets: 449 · Displayed: 449 (100.0%) · Marked: 1 (0.2%) · Dropped: 0 (0.0%) | Profile: Default

Part 3: User Datagram Protocol (UDP)

19. What transport layer protocol is used to transfer the DNS query and the response message?

The transport layer protocol used here is the user datagram protocol also known as UDP.

20. To setup the connection, how many UDP datagrams are exchanged between your computer and the server? Explain your answer.

UDP is a connectionless protocol. UDP is connectionless, but there are 26 UDP packets.

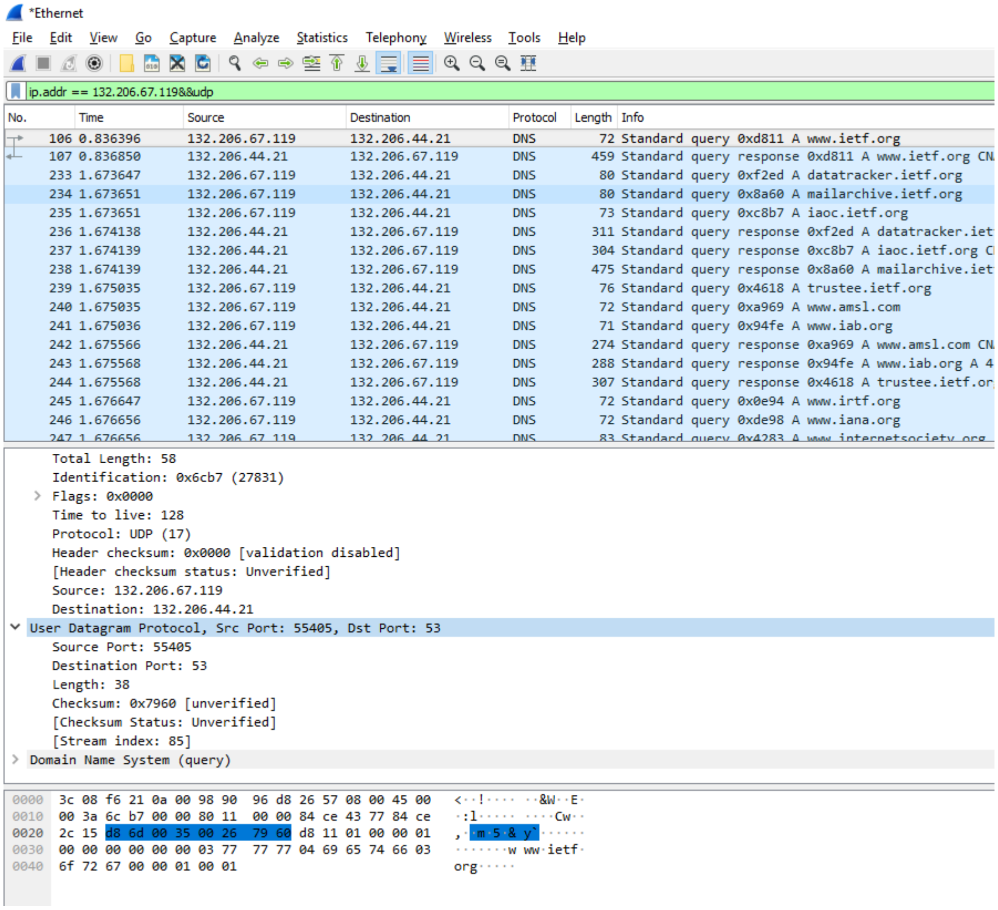
21. Select the first DNS packet in your trace. From this packet, determine the header fields of UDP.

The header fields of UDP consists of 4 fields: the source port, the destination port, the length and the checksum.

22. By consulting the displayed information in Wireshark's packet content field for the first DNS message, determine the length (in bytes) of each of the UDP header fields.

Each field is allocated 2 bytes, and thus, the total length of the header is 8 bytes.

A figure was provide to highlight the 4 fields.



ip.addr == 132.206.67.119&&udp

```
No.   Time      Source          Destination     Protocol Length Info
  106 0.836396  132.206.67.119  132.206.44.21   DNS        72 Standard query 0xd811 A www.ietf.org
  107 0.836850  132.206.44.21   132.206.67.119  DNS       459 Standard query response 0xd811 A www.ietf.org CN
  233 1.673647  132.206.67.119  132.206.44.21   DNS        80 Standard query 0xf2ed A datatracker.ietf.org
  234 1.673651  132.206.67.119  132.206.44.21   DNS        80 Standard query 0x8a60 A mailarchive.ietf.org
  235 1.673651  132.206.67.119  132.206.44.21   DNS        73 Standard query 0xc8b7 A iaoc.ietf.org
  236 1.674138  132.206.44.21   132.206.67.119  DNS       311 Standard query response 0xf2ed A datatracker.iet
  237 1.674139  132.206.44.21   132.206.67.119  DNS       304 Standard query response 0xc8b7 A iaoc.ietf.org C
  238 1.674139  132.206.44.21   132.206.67.119  DNS       475 Standard query response 0x8a60 A mailarchive.iet
  239 1.675035  132.206.67.119  132.206.44.21   DNS        76 Standard query 0x4618 A trustee.ietf.org
  240 1.675035  132.206.67.119  132.206.44.21   DNS        72 Standard query 0xa969 A www.amsl.com
  241 1.675036  132.206.67.119  132.206.44.21   DNS        71 Standard query 0x94fe A www.iab.org
  242 1.675566  132.206.44.21   132.206.67.119  DNS       274 Standard query response 0xa969 A www.amsl.com CN
  243 1.675568  132.206.44.21   132.206.67.119  DNS       288 Standard query response 0x94fe A www.iab.org A 4
  244 1.675568  132.206.44.21   132.206.67.119  DNS       307 Standard query response 0x4618 A trustee.ietf.or
  245 1.676647  132.206.67.119  132.206.44.21   DNS        72 Standard query 0x0e94 A www.irtf.org
  246 1.676656  132.206.67.119  132.206.44.21   DNS        72 Standard query 0xde98 A www.iana.org
  247 1.676656  132.206.67.119  132.206.44.21   DNS        83 Standard query 0x4283 A www.internetsociety.org
```

```
    Total Length: 58
    Identification: 0x6cb7 (27831)
  > Flags: 0x0000
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 132.206.67.119
    Destination: 132.206.44.21
v User Datagram Protocol, Src Port: 55405, Dst Port: 53
    Source Port: 55405
    Destination Port: 53
    Length: 38
    Checksum: 0x7960 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 85]
> Domain Name System (query)
```

```
0000  3c 08 f6 21 0a 00 98 90  96 d8 26 57 08 00 45 00   <··!···· ··&W··E·
0010  00 3a 6c b7 00 00 80 11  00 00 84 ce 43 77 84 ce   ·:l····· ····Cw··
0020  2c 15 d8 6d 00 35 00 26  79 60 d8 11 01 00 00 01   ,··m·5·& y`······
0030  00 00 00 00 00 00 03 77  77 77 04 69 65 74 66 03   ·······w ww·ietf·
0040  6f 72 67 00 00 01 00 01                            org·····
```

23. The value in the Length field indicates the length of what? Verify your claim with your captured UDP packet.

The value in the length field indicated the total length in bits of the header plus its payload. From question 22, we can tell that the header length is 8 bytes. The payload is therefore 30 bytes of data. This can also be confirmed by counting the number of packets in wireshark.

Total length = payload + header (udp) = 8+30 = 38

24. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your previous answer)

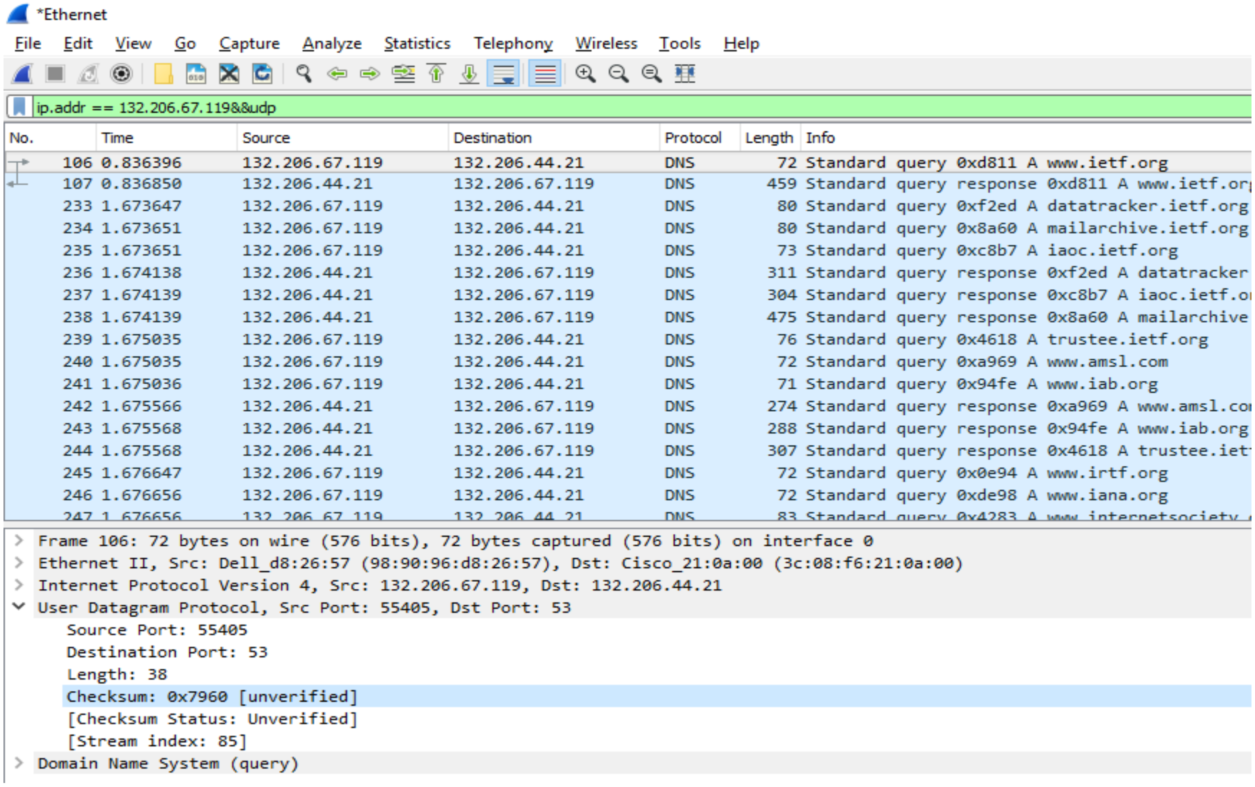
The maximum number of bytes that can be included in a UDP payload can be expressed as 2^{16} – 1 - 8, where we take out the space for the header (8 bytes), then we are left with 65527 bytes.

25. What is the largest possible source port number?

The largest possible source port number is (2^16 – 1) = 65535.

26. Determine whether a checksum is provided for the first DNS message or not. What is the usage of this field?

Yes, checksum is provided. Checksum is used for error detection in UDP.



ip.addr == 132.206.67.119&&udp

```
No.      Time       Source           Destination      Protocol  Length Info
     106 0.836396   132.206.67.119   132.206.44.21    DNS           72 Standard query 0xd811 A www.ietf.org
     107 0.836850   132.206.44.21    132.206.67.119   DNS          459 Standard query response 0xd811 A www.ietf.or
     233 1.673647   132.206.67.119   132.206.44.21    DNS           80 Standard query 0xf2ed A datatracker.ietf.org
     234 1.673651   132.206.67.119   132.206.44.21    DNS           80 Standard query 0x8a60 A mailarchive.ietf.org
     235 1.673651   132.206.67.119   132.206.44.21    DNS           73 Standard query 0xc8b7 A iaoc.ietf.org
     236 1.674138   132.206.44.21    132.206.67.119   DNS          311 Standard query response 0xf2ed A datatracker
     237 1.674139   132.206.44.21    132.206.67.119   DNS          304 Standard query response 0xc8b7 A iaoc.ietf.o
     238 1.674139   132.206.44.21    132.206.67.119   DNS          475 Standard query response 0x8a60 A mailarchive
     239 1.675035   132.206.67.119   132.206.44.21    DNS           76 Standard query 0x4618 A trustee.ietf.org
     240 1.675035   132.206.67.119   132.206.44.21    DNS           72 Standard query 0xa969 A www.amsl.com
     241 1.675036   132.206.67.119   132.206.44.21    DNS           71 Standard query 0x94fe A www.iab.org
     242 1.675566   132.206.44.21    132.206.67.119   DNS          274 Standard query response 0xa969 A www.amsl.co
     243 1.675568   132.206.44.21    132.206.67.119   DNS          288 Standard query response 0x94fe A www.iab.org
     244 1.675568   132.206.44.21    132.206.67.119   DNS          307 Standard query response 0x4618 A trustee.iet
     245 1.676647   132.206.67.119   132.206.44.21    DNS           72 Standard query 0x0e94 A www.irtf.org
     246 1.676656   132.206.67.119   132.206.44.21    DNS           72 Standard query 0xde98 A www.iana.org
     247 1.676656   132.206.67.119   132.206.44.21    DNS           83 Standard query 0x4283 A www.internetsociety
```

```
> Frame 106: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
> Ethernet II, Src: Dell_d8:26:57 (98:90:96:d8:26:57), Dst: Cisco_21:0a:00 (3c:08:f6:21:0a:00)
> Internet Protocol Version 4, Src: 132.206.67.119, Dst: 132.206.44.21
v User Datagram Protocol, Src Port: 55405, Dst Port: 53
    Source Port: 55405
    Destination Port: 53
    Length: 38
    Checksum: 0x7960 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 85]
> Domain Name System (query)
```

27. Determine the destination port number for the DNS query message and the source port number of the DNS response. What is the relationship between the two? Which port number is a well-known port number?

The destination port number is 53 and the source port number is 53 too. The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet. A commonly well-known port number is the port 53.

28. List two other well-known port numbers used by UDP.

Two other well-known ports are port 38 and port 39.

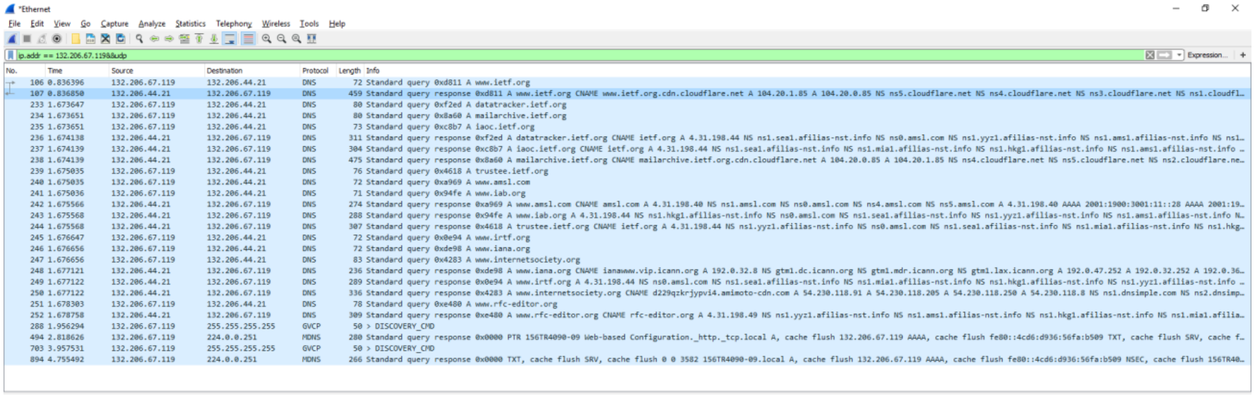
29. Determine the IP address of your local DNS server (use ipconfig). Is it the same as destination IP address of the DNS query?

Local DNS server IP = 132.206.44.21. It is the same as the destination IP address of the DNS query.

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

Three answers are provided, each answer contains the IP address, the name of the host, the type of address, the class, the TTL and the data length. The Figure below shows the answer, and what the answer contains.

31. By checking the trace, determine whether UDP is a reliable protocol or not.



```
ip.addr == 132.206.67.119&&udp
```

```
No.      Time       Source            Destination       Protocol  Length Info
  106 0.836396   132.206.67.119    132.206.44.21      DNS         72 Standard query 0xd811 A www.ietf.org
  107 0.836850   132.206.44.21     132.206.67.119     DNS        459 Standard query response 0xd811 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.20.1.85 A 104.20.0.85 NS ns5.cloudflare.net NS ns4.cloudflare.net NS ns3.cloudflare.net NS ns1.cloudfl…
  233 1.673647   132.206.67.119    132.206.44.21      DNS         80 Standard query 0xf2ed A datatracker.ietf.org
  234 1.673651   132.206.67.119    132.206.44.21      DNS         80 Standard query 0x8a60 A mailarchive.ietf.org
  235 1.673651   132.206.67.119    132.206.44.21      DNS         73 Standard query 0xc8b7 A iaoc.ietf.org
  236 1.674138   132.206.44.21     132.206.67.119     DNS        311 Standard query response 0xf2ed A datatracker.ietf.org CNAME ietf.org A 4.31.198.44 NS ns1.sea1.afilias-nst.info NS ns0.amsl.com NS ns1.yyz1.afilias-nst.info NS ns1.ams1.afilias-nst.info NS ns1…
  237 1.674139   132.206.44.21     132.206.67.119     DNS        304 Standard query response 0xc8b7 A iaoc.ietf.org CNAME ietf.org A 4.31.198.44 NS ns1.sea1.afilias-nst.info NS ns1.mia1.afilias-nst.info NS ns1.hkg1.afilias-nst.info NS ns1.ams1.afilias-nst.info …
  238 1.674139   132.206.44.21     132.206.67.119     DNS        475 Standard query response 0x8a60 A mailarchive.ietf.org CNAME mailarchive.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85 NS ns4.cloudflare.net NS ns5.cloudflare.net NS ns2.cloudflare.ne…
  239 1.675035   132.206.67.119    132.206.44.21      DNS         76 Standard query 0x4618 A trustee.ietf.org
  240 1.675035   132.206.67.119    132.206.44.21      DNS         72 Standard query 0xa969 A www.amsl.com
  241 1.675036   132.206.67.119    132.206.44.21      DNS         71 Standard query 0x94fe A www.iab.org
  242 1.675566   132.206.44.21     132.206.67.119     DNS        274 Standard query response 0xa969 A www.amsl.com CNAME amsl.com A 4.31.198.40 NS ns1.amsl.com NS ns0.amsl.com NS ns4.amsl.com NS ns5.amsl.com A 4.31.198.40 AAAA 2001:1900:3001:11::28 AAAA 2001:19…
  243 1.675568   132.206.44.21     132.206.67.119     DNS        288 Standard query response 0x94fe A www.iab.org A 4.31.198.44 NS ns1.hkg1.afilias-nst.info NS ns0.amsl.com NS ns1.sea1.afilias-nst.info NS ns1.yyz1.afilias-nst.info NS ns1.ams1.afilias-nst.info N…
  244 1.675568   132.206.44.21     132.206.67.119     DNS        307 Standard query response 0x4618 A trustee.ietf.org CNAME ietf.org A 4.31.198.44 NS ns1.yyz1.afilias-nst.info NS ns0.amsl.com NS ns1.sea1.afilias-nst.info NS ns1.mia1.afilias-nst.info NS ns1.hkg…
  245 1.676647   132.206.67.119    132.206.44.21      DNS         72 Standard query 0x0e94 A www.irtf.org
  246 1.676656   132.206.67.119    132.206.44.21      DNS         72 Standard query 0xde98 A www.iana.org
  247 1.676656   132.206.67.119    132.206.44.21      DNS         83 Standard query 0x4283 A www.internetsociety.org
  248 1.677121   132.206.44.21     132.206.67.119     DNS        236 Standard query response 0xde98 A www.iana.org CNAME ianawww.vip.icann.org A 192.0.32.8 NS gtm1.dc.icann.org NS gtm1.mdr.icann.org NS gtm1.lax.icann.org A 192.0.47.252 A 192.0.32.252 A 192.0.36…
  249 1.677122   132.206.44.21     132.206.67.119     DNS        289 Standard query response 0x0e94 A www.irtf.org A 4.31.198.44 NS ns0.amsl.com NS ns1.sea1.afilias-nst.info NS ns1.mia1.afilias-nst.info NS ns1.hkg1.afilias-nst.info NS ns1.yyz1.afilias-nst.info …
  250 1.677122   132.206.44.21     132.206.67.119     DNS        336 Standard query response 0x4283 A www.internetsociety.org CNAME d229qzkrjypvi4.amimoto-cdn.com A 54.230.118.91 A 54.230.118.205 A 54.230.118.250 A 54.230.118.8 NS ns1.dnsimple.com NS ns2.dnsimp…
  251 1.678303   132.206.67.119    132.206.44.21      DNS         78 Standard query 0xe480 A www.rfc-editor.org
  252 1.678758   132.206.44.21     132.206.67.119     DNS        309 Standard query response 0xe480 A www.rfc-editor.org CNAME rfc-editor.org A 4.31.198.49 NS ns1.yyz1.afilias-nst.info NS ns1.ams1.afilias-nst.info NS ns1.hkg1.afilias-nst.info NS ns1.mia1.afilia…
  288 1.956294   132.206.67.119    255.255.255.255    GVCP        50 > DISCOVERY_CMD
  494 2.818626   132.206.67.119    224.0.0.251        MDNS       280 Standard query response 0x0000 PTR 156TR4090-09 Web-based Configuration._http._tcp.local A, cache flush 132.206.67.119 AAAA, cache flush fe80::4cd6:d936:56fa:b509 TXT, cache flush SRV, cache f…
  703 3.957531   132.206.67.119    255.255.255.255    GVCP        50 > DISCOVERY_CMD
  894 4.755492   132.206.67.119    224.0.0.251        MDNS       266 Standard query response 0x0000 TXT, cache flush SRV, cache flush 0 0 3582 156TR4090-09.local A, cache flush 132.206.67.119 AAAA, cache flush fe80::4cd6:d936:56fa:b509 NSEC, cache flush 156TR40…
```

By checking, we can see that UDP is not reliable.

32. Explain your answer.

This is not reliable, because to be reliable, the user needs to be notified when UDP packets are lost or fail to arrive to their destination.

33. Why does DNS use UDP services?

UDP is much faster. TCP is slow as it requires 3 way handshake. The load on DNS servers is also an important factor. DNS servers (since they use UDP) don't have keep connections. DNS requests are generally very small and fit well within UDP segments. UDP is not reliable, but reliability can added on application layer. An application can use UDP and can be reliable by using timeout and resend at application layer.