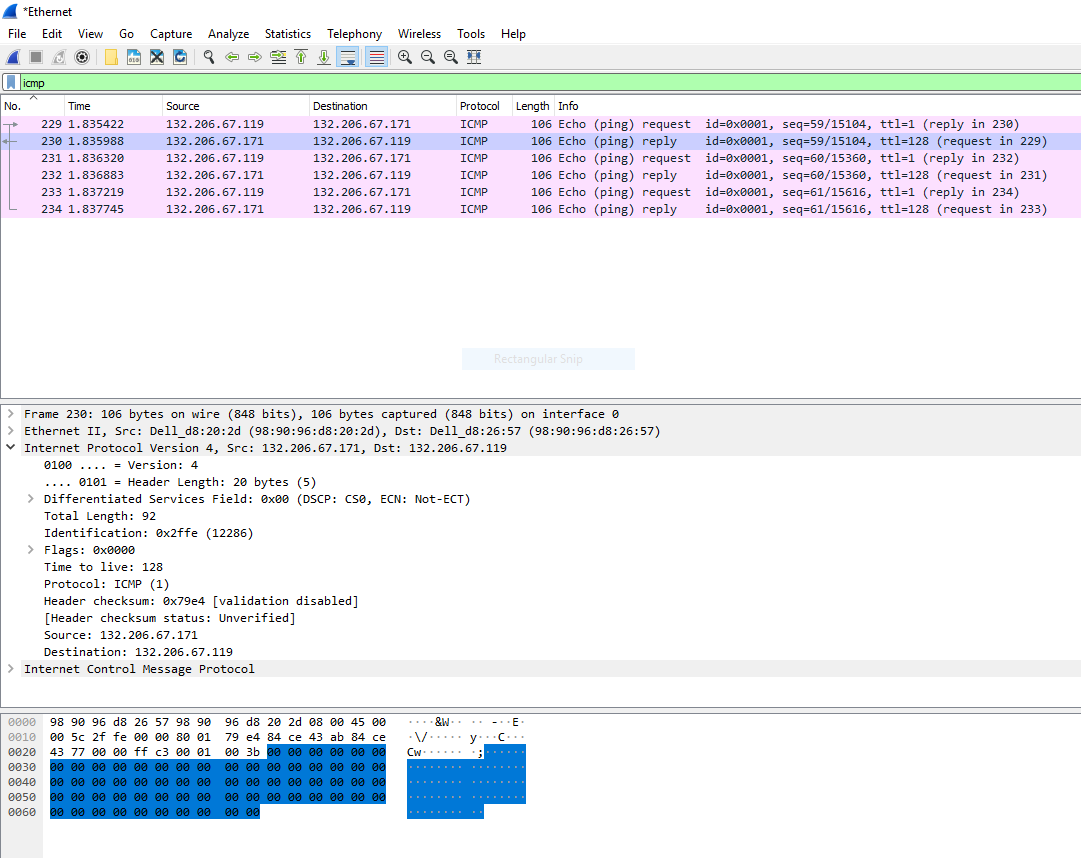
### Part 1: Internet Protocol (IP)



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**](http://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.

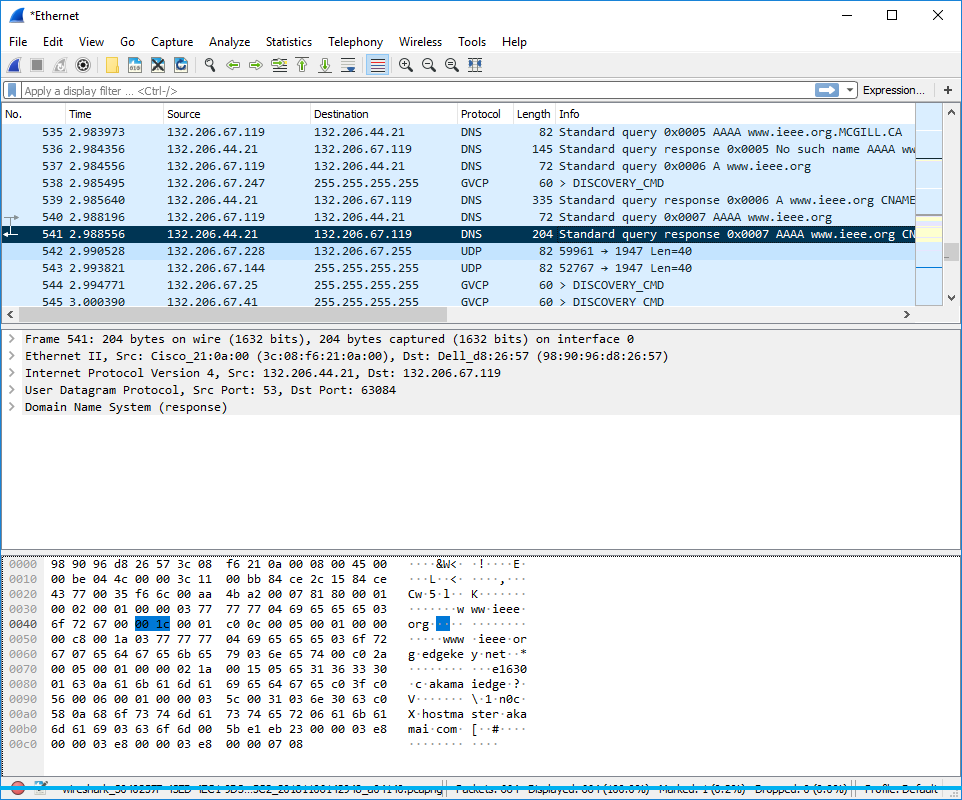
**13. Which bit in the “Flags” field indicates that the message is a query or a response?**

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**](http://www.ieee.org)**?**

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

**15. Provide a screenshot.**



### 

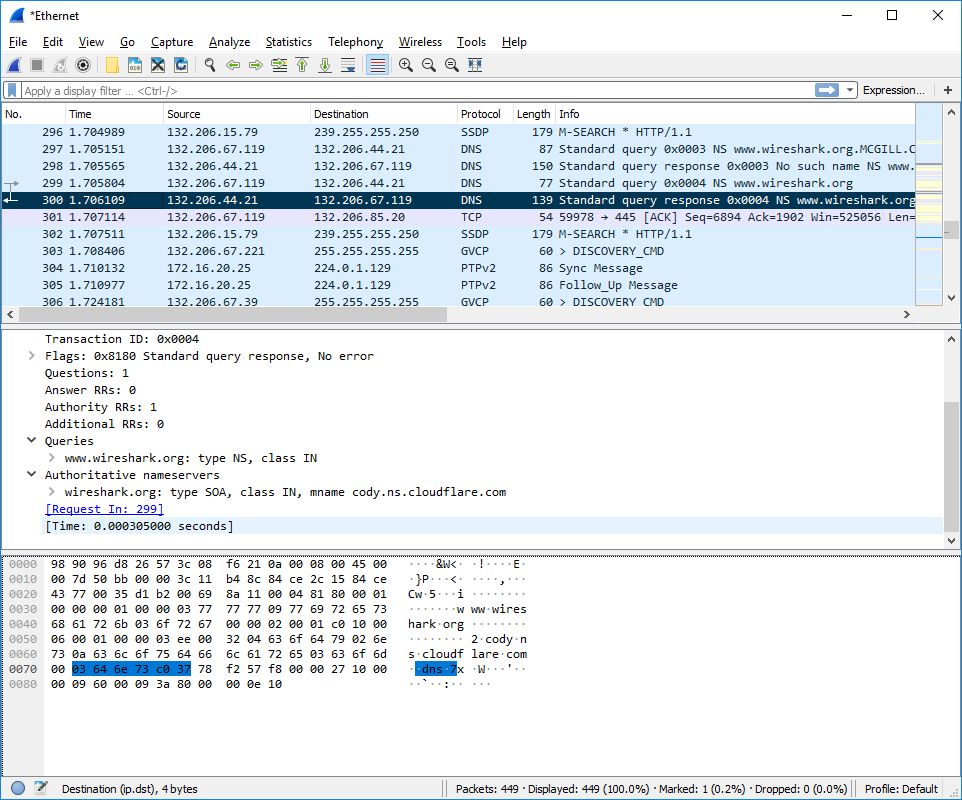
**16. What is the destination IP address of the DNS query? What does this address correspond to?**

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** [**www.wireshark.org**](http://www.wireshark.org)**. 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.**



### 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.

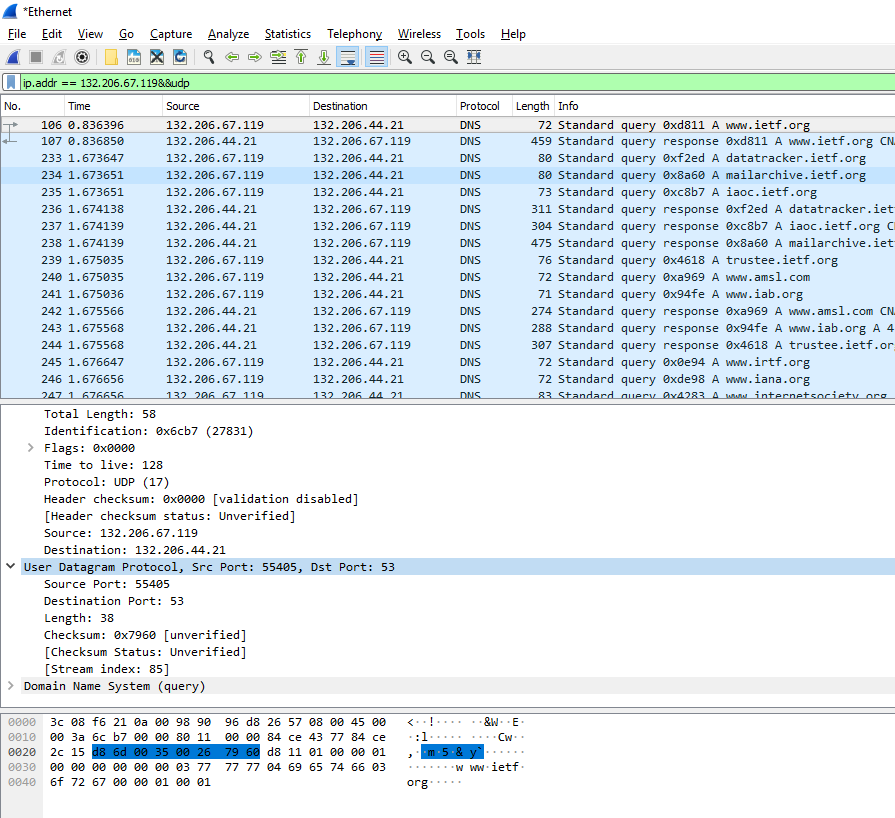
**21. Select the first DNS packet in your trace. From this packet, determine the header fields of UDP.**

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.



**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

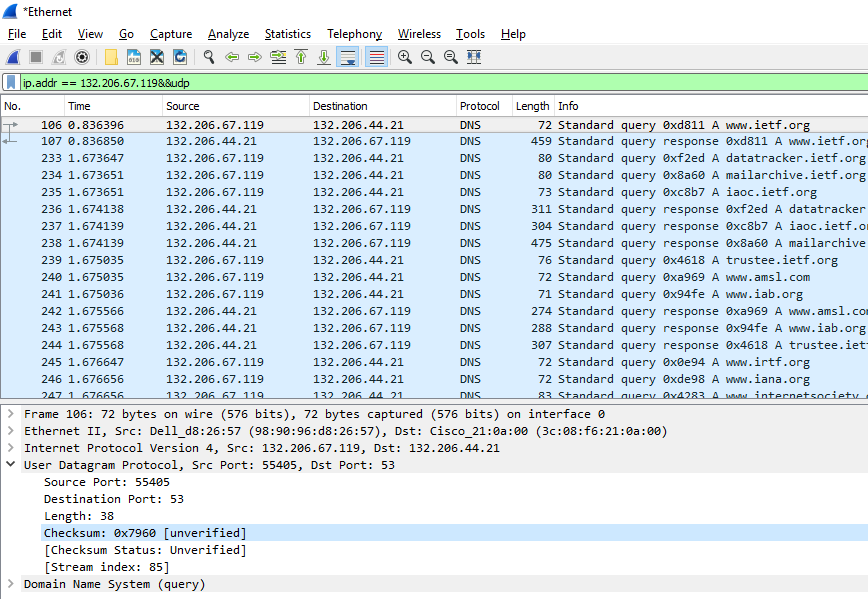
216 – 1 - 8, where we take out the space for the header (8 bytes), then we are left with 65527 bytes.

**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.



**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.

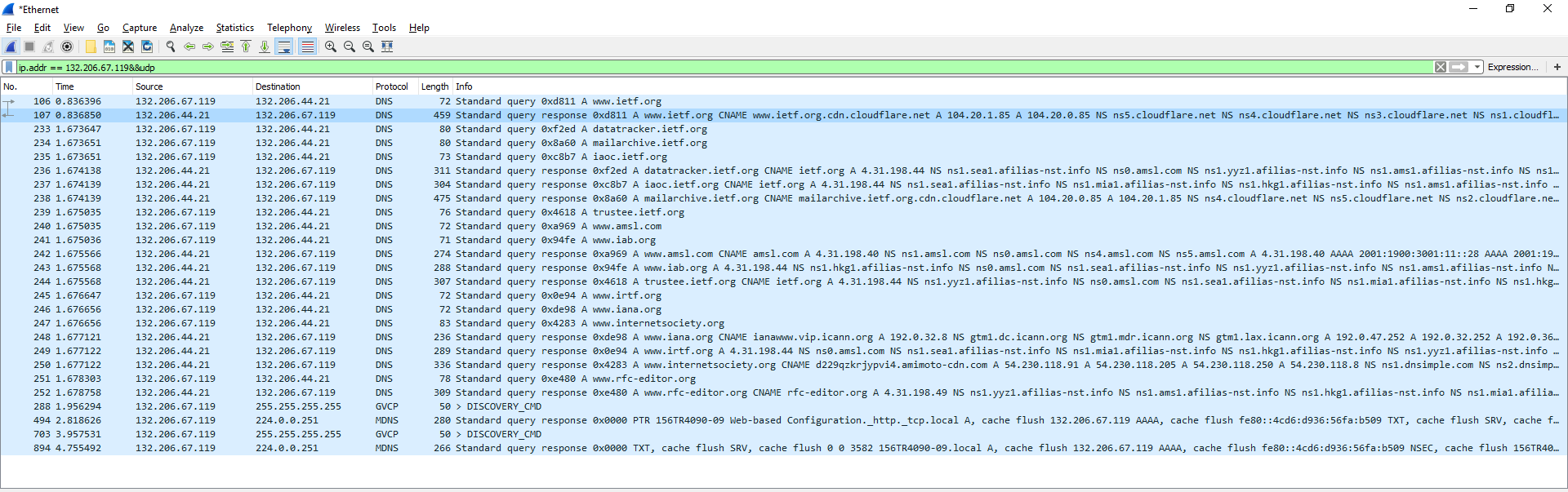
**29. Determine the IP address of your local DNS server (use ipconfig). Is it the same as destination IP address of the DNS query?**

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.**



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.