Answer the following questions, for all 3 generated packet traces:

Select the first UDP message you see sent from your computer to google.com and expand the Internet Protocol (layer 3) section:

1. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

   Total length - header length = payload length

   56: 20 bytes of header, 36 bytes of payload.

   2k: 20 bytes header, 1480 bytes payload

   3.5k: 20 bytes header, 1480 bytes payload

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

   56 is not, and 2k and 3.5k are. Check the “more fragments” flags. Fragmented when it’s 1, otherwise not.

Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source (sort in descending order), afterwards, navigate to the series of UDP messages sent by your computer to google.com:

1. Which fields in the IP datagram always change from one datagram to the next within this series of messages sent by your computer?

   Always change:

   Identification, checksum, and TTL.

2. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

   Constant:

   Version, header length, flags, service field, protocol, source and destination IP

   Must stay constant:

   Version - Stays constant within a series as it indicates whether it's an IPv4 or IPv6 packet

   Header length - Stays constant within a series as it defines the length of the IP header

Source and dest IP - My device and google.com should remain constant

Protocol and service - All use UDP and its relevant service

Must change:

Identification - IP packets must have different id

TTL - ttl changes at each router and traceroute increments each subsequent packet

Checksum - checksum changes whenever the header changes

Next, find the series of ICMP messages sent back to your computer with the “TTL-exceeded” after the first hop (it might help here to look at your terminal window to figure out which was the first hop):

1. What is the value in the Identification field and the TTL field?

   56: Id 57023 and ttl 255

   2k: id 62512 and ttl 255

   3.5k: id 65269 and ttl 255

2. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router?

   Id changes but ttl remains unchanged

Finally, looking at the first UDP message sent for your computer for packet size == 3500:

1. Has that message been fragmented across more than one IP datagram?

   Yes

2. What information in the IP header indicates that the datagram has been fragmented?

   The “More fragments” flag is set to 1.

3. What information in the IP header indicates whether this is the first fragment versus a latter fragment?

   The fragment offset of 0 is the first fragment and the other numbers are the latter ones.

4. How long is this IP datagram?

   Total length of 1500 bytes including a 20-byte header.