ASSIGNMENT 7 INTERNET PROTOCOL

Name: HRISHIKESH RAVINDRA KARANDE

PART1

1. Select the first UDP segment sent by your computer via the `traceroute` command to gaia.cs.umass.edu. Expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

A] IP Address of computer is: 10.240.118.1 that we can see from packet.

2. What is the value in the time-to-live (TTL) field in this IPv4 datagram's header?

   A] TTL field in this IPv4 datagram's header = 1

3. What is the value in the upper layer protocol field in this IPv4 datagram's header? [Note: the answers for Linux/MacOS differ from Windows here].

   A] Protocol field in th IPv4 Datagram header : UDP(17)

4. How many bytes are in the IP header?'

   A] Header Length: 20 bytes

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

   A] Total Length = Header+Payload

   56 bytes = 20+payload

   Payload = 36 bytes

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

   A] To check whether the data is fragmented we can use the fragments field in the Header. If the fragment offset is greater than 0 and More fragments bit is set then it means that there are more fragments available. Also a fragmented packet has same identification number across the fragments. If a packet is not allowed to be fragmented then it's 'Do not fragment' bit is set 1.

   In this case the packet is not fragmented.

7. Which fields in the IP datagram *always* change from one datagram to the next within this series of UDP segments sent by your computer destined to 128.119.245.12, via traceroute? Why?

The Identification, Header Checksum and stream Index change from each datagram to other.

- Identification(IP packets must have different ids)
- Time to live (traceroute increments each subsequent packet)
- Header checksum (since header changes, so must checksum)

Q8 Which fields in this sequence of IP datagrams (containing UDP segments) stay constant? Why?

A] The following fields remain constant.

- Version (since we are using IPv4 for all packets)
- Header length (since these are ICMP packets)
- Source IP (since we are sending from the same source)
- Destination IP (since we are sending to the same dest)
- Differentiated Services (since all packets are ICMP they use the same Type of Service class)
- Upper Layer Protocol (since these are ICMP packets)

Q9

There is no such pattern observerd in the values of Identification field of IP Datagrams, being sent. The identification number are randomly sent.

Q10

The value of Upper Layer Protocol is UDP(17) in the icmp field, but in the IP Datagram the

Upper Layer Protocol specified is ICMP(1)

Q11

Yes they are similar in pattern as in Q9 with no specific pattern observed.

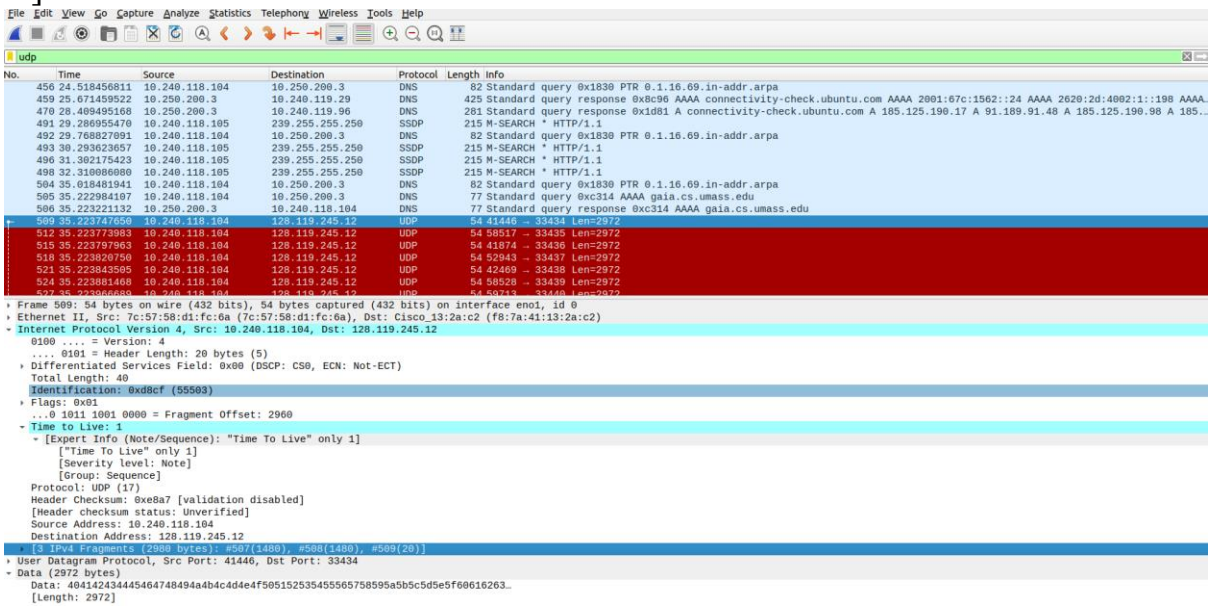
Q12

The values across the TTL field are not similar across all the packets from all the routers, in the icmp field. In the IP field the TTL decrements starting from 255 and some cases it changes to 64 or 57.

Part2:

1. Find the first IP datagram containing the first part of the segment sent to 128.119.245.12 sent by your computer via the traceroute command to gaia.cs.umass.edu, after you specified that the traceroute packet length should be 3000. (Hint: This is packet 179 in the ip-wireshark-trace1-1.pcapng trace file in footnote 2. Packets 179, 180, and 181 are three IP datagrams created by fragmenting the first single 3000-byte UDP segment sent to 128.119.145.12). Has that segment been fragmented across more than one IP datagram? (Hint: the answer is yes1!)

A]



Yes the segment is fragmented across more than one IP. The first IP Datagram containing the first part of segment sent by my computer is in packet 507.

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

A] The fragment offset is not zero and there are three fragments(#507, #508 and #509) with three fragment number visible in the IP Datagram visible in the header. Also the the more fragment bit (MF) = 1 indicating the packet is fragmented and the gradment offset = 0 , indicating that this is first fragments and there are more fragments.

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

   A]The Flags field has fragment offset set to 0 indicating the it is first fragment.

4. How many bytes are there in this IP datagram (header plus payload)?
   A] Total Length = 1500 bytes out of which Header is 20bytes.

5. What fields change in the IP header between the first and second fragment?
   A] The fragment offset which is 0 in first packet is no longer 0 but is set to some value. Also the checksum changes it's value.

6. Now find the IP datagram containing the third fragment of the original UDP segment. What information in the IP header indicates that this is the last fragment of that segment?
   A] The More fragment bit = 0 in the header of this packet thus indicating that there are no more fragments, for that segment. Also there is information available in here regarding the frame numbers and corresponding payload into which the original packet was broken down.

Part 3:

1. What is the IPv6 address of the computer making the DNS AAAA request? This is the source address of the 20th packet in the trace. Give the IPv6 source address for this datagram in the exact same form as displayed in the Wireshark window1 .
   A] The IPv6 address of computer making DNS AAAA request
   src IPv6=2601:193:8302:4620:215c:f5ae:8b40:a27a .

2. What is the IPv6 destination address for this datagram? Give this IPv6 address in the exact same form as displayed in the Wireshark window.
   A] The IPv6 address of destination = 2001:558:feed::1

3. What is the value of the flow label for this datagram?
   Flow Label = 0x063ed0

4. How much payload data is carried in this datagram?
   A] Payload length = 37

5. What is the upper layer protocol to which this datagram's payload will be delivered at the destination?
   A] UDP(17)

6. How many IPv6 addresses are returned in the response to this AAAA request?
   A] There is a sngle IPv6 adress returned as the answer in DNS headers present in response packet 27.

7. What is the first of the IPv6 addresses returned by the DNS for youtube.com (in the ip-wireshark-trace2-1.pcapng trace file, this is also the address that is numerically the smallest)? Give this IPv6 address in the exact same shorthand form as displayed in the Wireshark window.
   A] 2607:f8b0:4006:815::200e