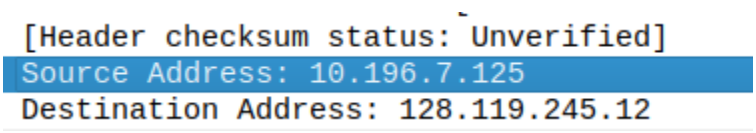
CS315: Assignment-7

Name: Shahil Patel
Roll No.: 200010039

Part 1: Basic IPv4

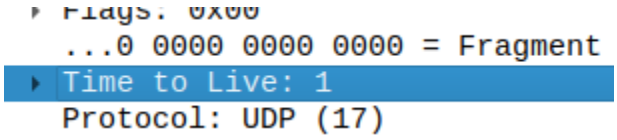
1. Select the first UDP segment sent by your computer via the traceroute command to gaia.cs.umass.edu. Expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

Ans: The IP address of my computer is: **10.196.7.125**



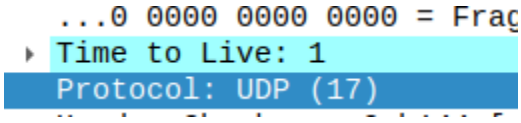
2. What is the value in the time-to-live (TTL) field in this IPv4 datagram's header?

Ans: The time-to-live (TTL) value is: **1**



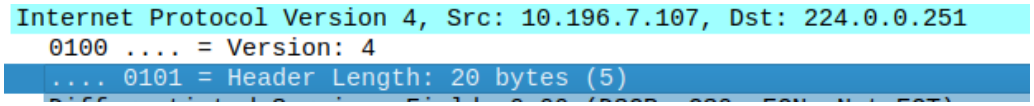
3. What is the value in the upper layer protocol field in this IPv4 datagram's header? [Note: the answers for Linux/MacOS differ from Windows here].

Ans: The value in the upper layer protocol field in this IPv4 datagram's header is: **UDP (17)**



4. How many bytes are in the IP header?

Ans: There are **20** bytes in the IP header.



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

Ans: The total length of IP datagram is 57 bytes and the header length is 20 bytes. Therefore to calculate the length of payload of the IP datagram we subtract header length from total length:

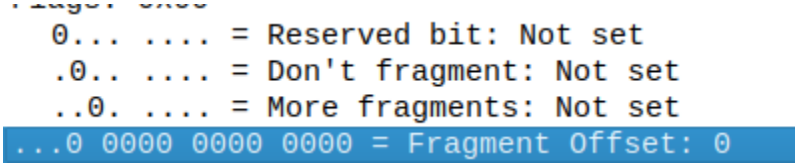
Hence, the length of payload = (Total Length - Header Length)

= 57-20

= 37

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

Ans: The IP datagram is ***not*** fragmented as the *Fragment Offset* is **0**.



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?

Ans: Fields in the IP datagram that always change from one datagram to the next are:

- **Identification** (Reason: IP packets must have different IDs)
- **Time to Live** (Reason: Traceroute increments each subsequent packet)
- **Header Checksum** (Reason: As the header changes, so the checksum should also change)

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

Ans : *The fields that stay constant across the IP datagrams are:*

- **Version** (since we are using IPv4 for all packets)
- **Header** Lenght (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)

The fields that must stay constant are:

- **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 destination)
- **Differentiated Services** (since all packets are ICMP they use the same Type of Service class)
- **Upper Layer Protocol** (since these are ICMP packets)

The fields that must change are:

- **Identification** (IP packets must have different IDs)
- **Time to Live** (Traceroute increments each subsequent packet)
- **Header checksum** (As the header changes, so the checksum should also change)

9. Describe the pattern you see in the values in the Identification field of the IP datagrams being sent by your computer.

Ans: With each **ICMP Echo** (ping) request, IP header Identification field increments.

10. What is the upper layer protocol specified in the IP datagrams returned from the routers? [Note: the answers for Linux/MacOS differ from Windows here].

Ans: The value in the upper layer protocol field in this IPv4 datagram's header is: **ICMP (1)**.

11. Are the values in the Identification fields (across the sequence of all of ICMP packets from all of the routers) similar in behavior to your answer to question 9 above?

Ans: **Yes**, The Identification fields change the values across the sequence of all of ICMP packets from all of the routers.

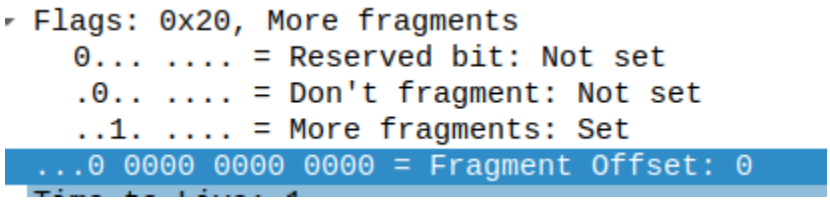
12. Are the values of the TTL fields similar, across all of ICMP packets from all of the routers?

Ans: **No**, the values of TTL fields also change across all of the ICMP packets from all of the routers.

Part 2: Fragmentation

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 yes!)

Ans: **Yes**, The segment has been fragmented across more than one IP datagram



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

Ans: The **More Fragements** offset within the flags header in IP header indicates that the datagram has been fragmented or not.

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

Ans: Since the fragment offset is **0**, we know that this is the first fragment.

4. How many bytes are there in this IP datagram (header plus payload)?

Ans: There are **1500 bytes** *(Header Length + Payload)* in this IP datagram.

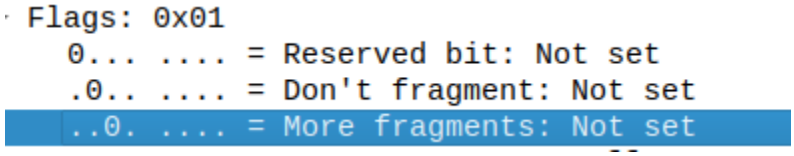
5. What fields change in the IP header between the first and second fragment?

Ans: The fields that change in the IP header between the first and second fragment are:

- **Fragment Offset**
- **Header Checksum**

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?

Ans: The *More fragments* section is **not set**, which indicates that the 3rd fragment of the original UDP segment is the last fragment of that segment.



Part 3: IPv6

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 window.

Ans: The IPv6 address of the computer making the DNS AAAA request is: ***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.

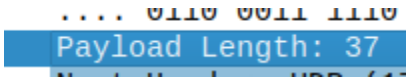
Ans: The IPv6 destination address for this datagram is: ***2001:558:feed::1***

3. What is the value of the flow label for this datagram?

Ans: The value of the flow label for this datagram is: **0x063ed0**

4. How much payload data is carried in this datagram?

Ans: The payload has **37 bytes** of data carried in it.



5. What is the upper layer protocol to which this datagram's payload will be delivered at the destination?

Ans: The upper layer protocol to which the datagram's payload will be delivered is: **UDP (17)**

6. How many IPv6 addresses are returned in the response to this AAAA request?

Ans: **4** IPv6 addresses are returned in the response to this AAAA request.

```
youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:806::200e
youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:81a::200e
youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:81b::200e
youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:807::200e
```

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.

Ans: The first of the IPv6 addresses returned by the DNS for youtube.com is:
2607:f8b0:4006:806::200e