**Juan Felipe Florez Giraldo** 039614388

**Part I: Traceroute with Wireshark (25 points)**

A screenshot of a computer

AI-generated content may be incorrect.

**Output Script** lab 👾 python3 pcapTraceroute.py trace.pcap hop.txt

hop 1: 100.69.32.2, 4.78, 3.67, 5.14

hop 2: 192.168.2.232, 4.19, 6.19, 5.11

hop 3: 192.168.18.218, 4.37, 4.00, 4.16

hop 4: 172.28.249.139, 4.05, 3.71, 3.75

hop 5: 172.28.249.146, 3.55, 3.96, 3.88

hop 6: \*, \* \* \*

hop 7: 172.28.162.68, 4.97, 4.69, 4.00

hop 8: 192.168.18.4, 4.90, 4.00, 9.54

hop 9: 192.168.18.19, 5.31, 3.52, 4.25

hop 10: 128.10.19.120, 3.36, 3.53, 3.34

**Answer Questions (10 points)**

Based on your traceroute experiment in 3.1 (trace.txt and trace.pcap), please answer the following questions:

• (1 point) What is the maximum TTL value observed in the pcap file, and how does it relate to the hop count?

If you can’t, please explain why not.

The maximum TTL value observed is 10, which is related to the hop count because it indicates the number of routers traversed plus 1; in this case, 10 hops to the destination.

• (1 point) Please go to its pcap file, locate the records as the response from the second-hop router (hint: usethe IP address of the routers on the way to locate the traces). Print only these records (or print the screenshot using wireshark).

A screenshot of a computer

AI-generated content may be incorrect.

• (1 point) What is the average of the round trip delays to the first-hop router towards this destination? If you can’t, please explain why not.

Using hop 1: 100.69.32.2, 4.78, 3.67, 5.14, it will be 4.53 ms

• (2 points) Explain how the router receives a packet with TTL=1, and how this is reflected in the captured

packets.

The router decrements the TTL to 0, discards the packet, and sends an ICMP Time Exceeded message (type 11). Outcome: A request with TTL=1 (e.g., the initial packet) is followed by a response from 100.69.32.2 (e.g., the Time Exceeded message).

Based on the given test.pcap file (which was captured during one traceroute experiment), please answer the following questions:

• (1 point) Please locate the packets with ICMP Echo Reply in the pcap file. Print only these records (or print the screenshot using wireshark). Check their source IP. What can you conclude from them?

A screenshot of a computer

AI-generated content may be incorrect.

Conclution: IP Source: 128.10.19.120, the destination responded, indicating the end of the traceroute.

• (2 points) Check the source and destination IP addresses of all traceroute request packets in the pcap file.

Are they always the same? Why is traceroute designed this way?

Source: 10.186.68.194, Destination: 128.10.19.120 (always the same). Design: Using a fixed destination ensures a single path; changing it would result in different routes.

• (1 point) What is the average of the round trip delays to the first-hop router towards this destination? If you can’t, please explain why not.

Average = (4 + 4 + 3) / 3 = 3.67 ms.

• (1 point) What is the average of the round trip delays to the final destination? If you can’t, please explain

why not.

Average = (5 + 4 + 3) / 3 = 4.00 ms.

**Part II: Analyze non-traceroute pcap files (15 points)**

Please analyze the given sender.pcap and receiver.pcap, and answer the following questions.

• (1 point) What is the sender’s IP? What is the receiver’s?

IPs en sender.pcap: Sender 128.10.106.26, Receiver 128.10.126.34

IPs en receiver.pcap: Sender 128.10.106.26, Receiver 128.10.126.34

• (1 point) How many unique bytes does the sender send in total? For example, for a packet (100, 200), the total bytes will be 200 - 100 = 100 bytes.

1.837.549 bytes

• (1 point) How many bytes are missing? (Check those packets with status = 0.)

91.606 bytes

• (2 points) What is the average time consumed to send data packets (excluding lost, duplicate and retrans-mitted packets)? What is the minimal and maximal time?

Average: 0.865 ms

Minimal: 0.749 ms

Maximal: 1.060 ms