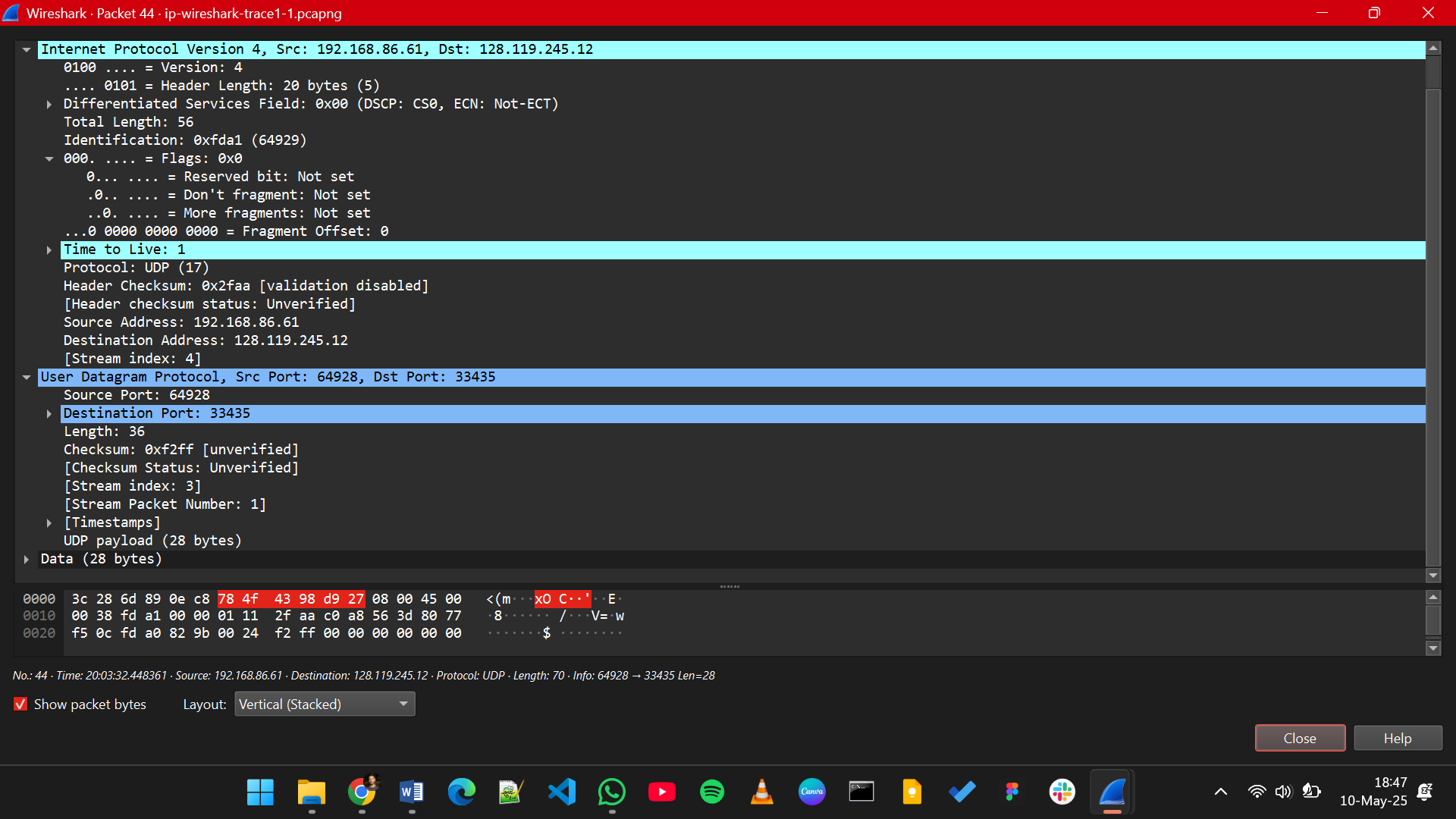
Wireshark IP Lab

# Muhammad Rehan – BSDSF22A001

## Part 1: Basic IPv4



1. Select the first UDP segment sent by your computer via the traceroute command to gaia.cs.umass.edu. What is the IP address of your computer?

**Src: 192.168.86.61**

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

**TTL: 1**

1. What is the value in the upper layer protocol field in this IPv4 datagram’s header?

**Protocol: UDP**

1. How many bytes are in the IP header?

**Header: 20 Bytes**

1. 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 = 36 Bytes**

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

**Not Fragmented.**

**Fragment Offset is 0 and More Fragment Flags is set to False**

1. 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?

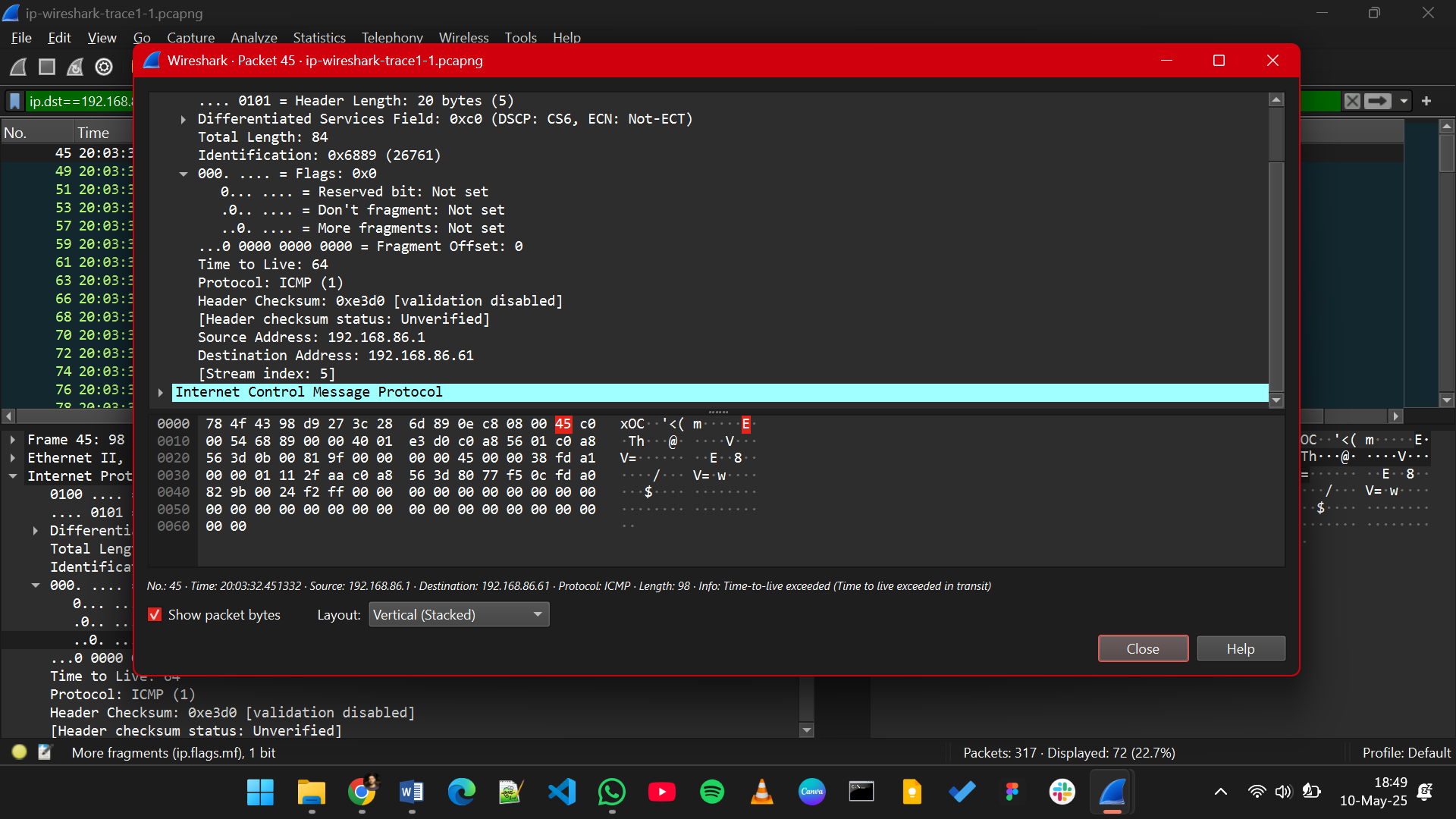
* **Identification**
* **Header Checksum**
* **TTL**

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

* **Source IP:** All datagrams originate from the same device.
* **Destination IP:** All are directed to the same endpoint.
* **Protocol:** traceroute sends UDP packets by default.
* **IP version:** The protocol in use does not change.
* **Header Length:** No options used in standard traceroute packets.

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

**Incrementing pattern**



1. What is the upper layer protocol specified in the IP datagrams returned from the routers?

**ICMP (1)**

1. 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?

**No, the Identification fields in ICMP packets do not follow a sequential pattern like your computer’s UDP packets because they are generated independently by different routers.**

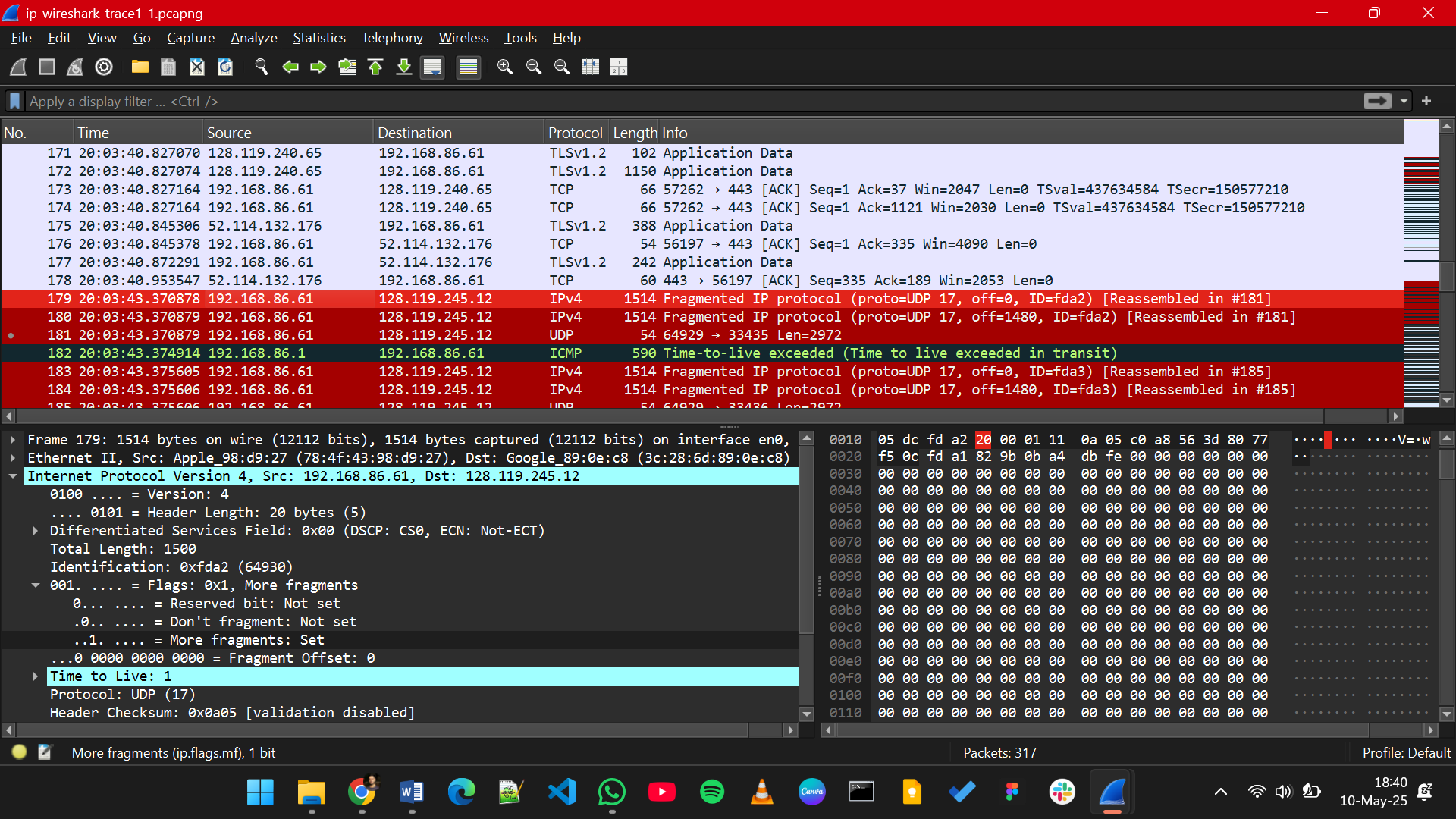
1. Are the values of the TTL fields similar, across all of ICMP packets from all of the routers?

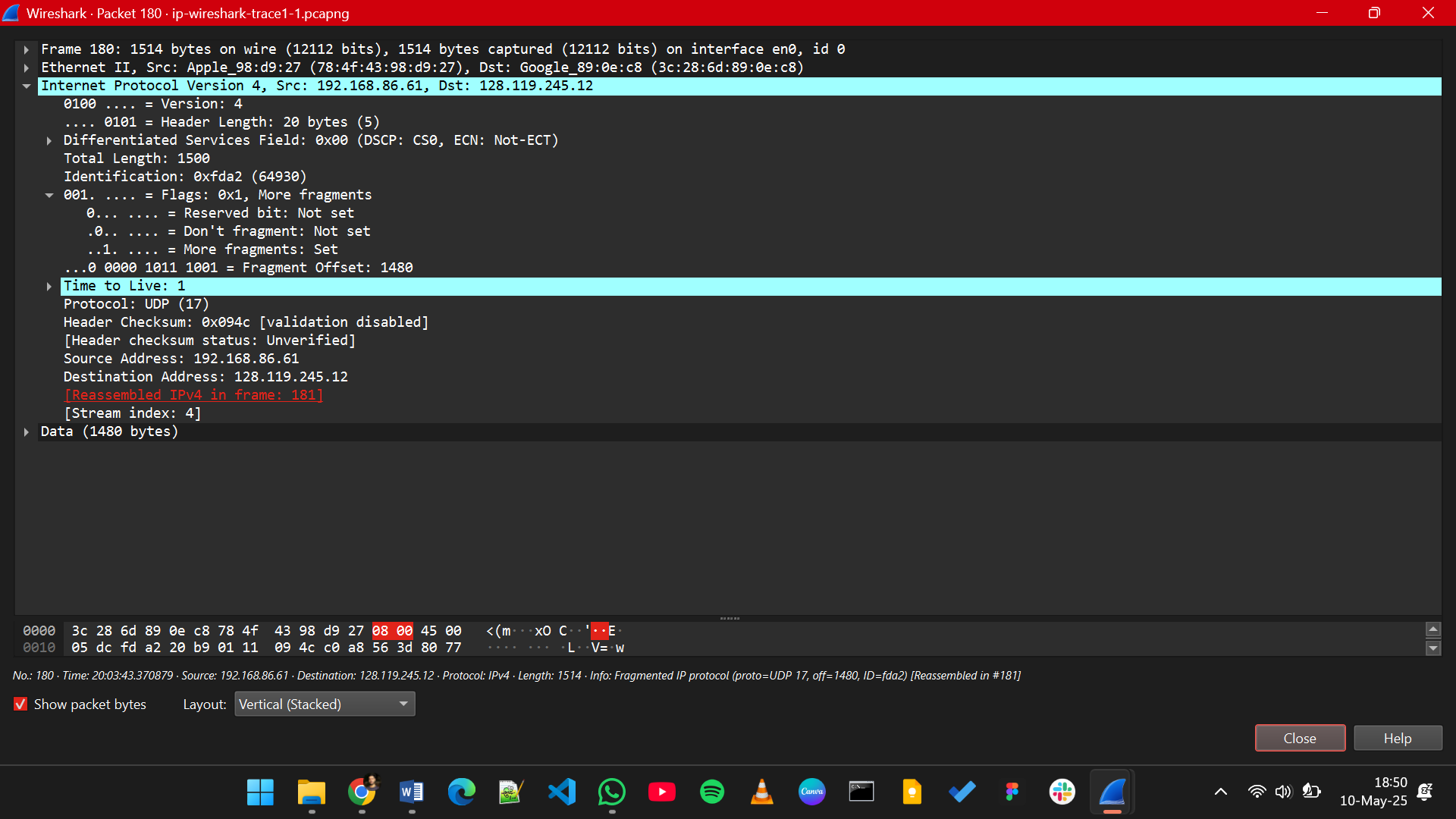
**No, the TTL values in the ICMP packets from different routers are not similar—they vary depending on how far each router is from the destination.**

## Part 2: Fragmentation

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

**Yes, the 3000-byte UDP segment has been fragmented across multiple IP datagrams, as indicated by multiple packets (e.g., 179, 180, 181) with matching Identification fields and different Fragment Offsets.**





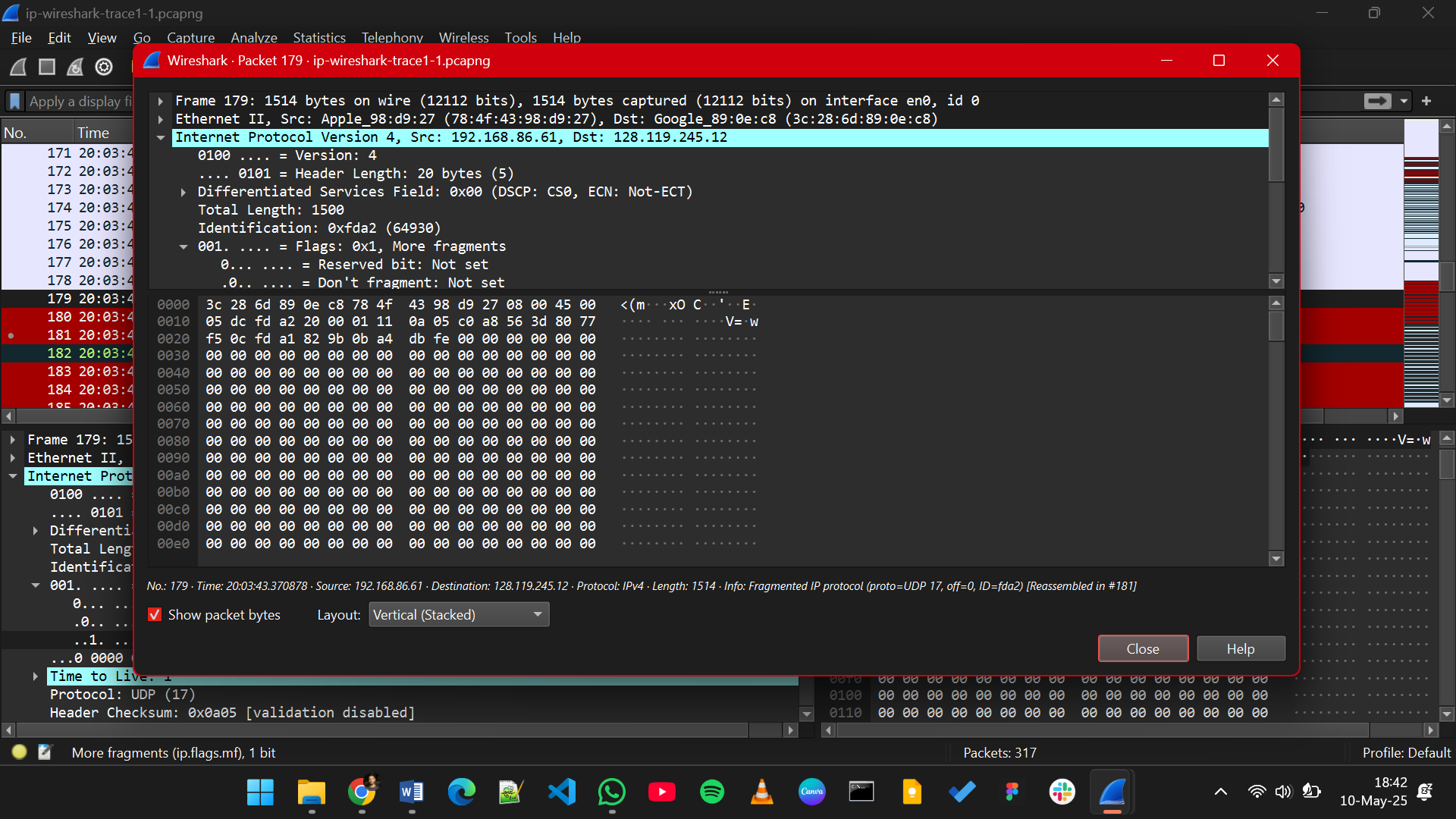
1. What information in the IP header indicates that this datagram has been fragmented?

**Flags: “More Fragments” and “Fragment Offset”**

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

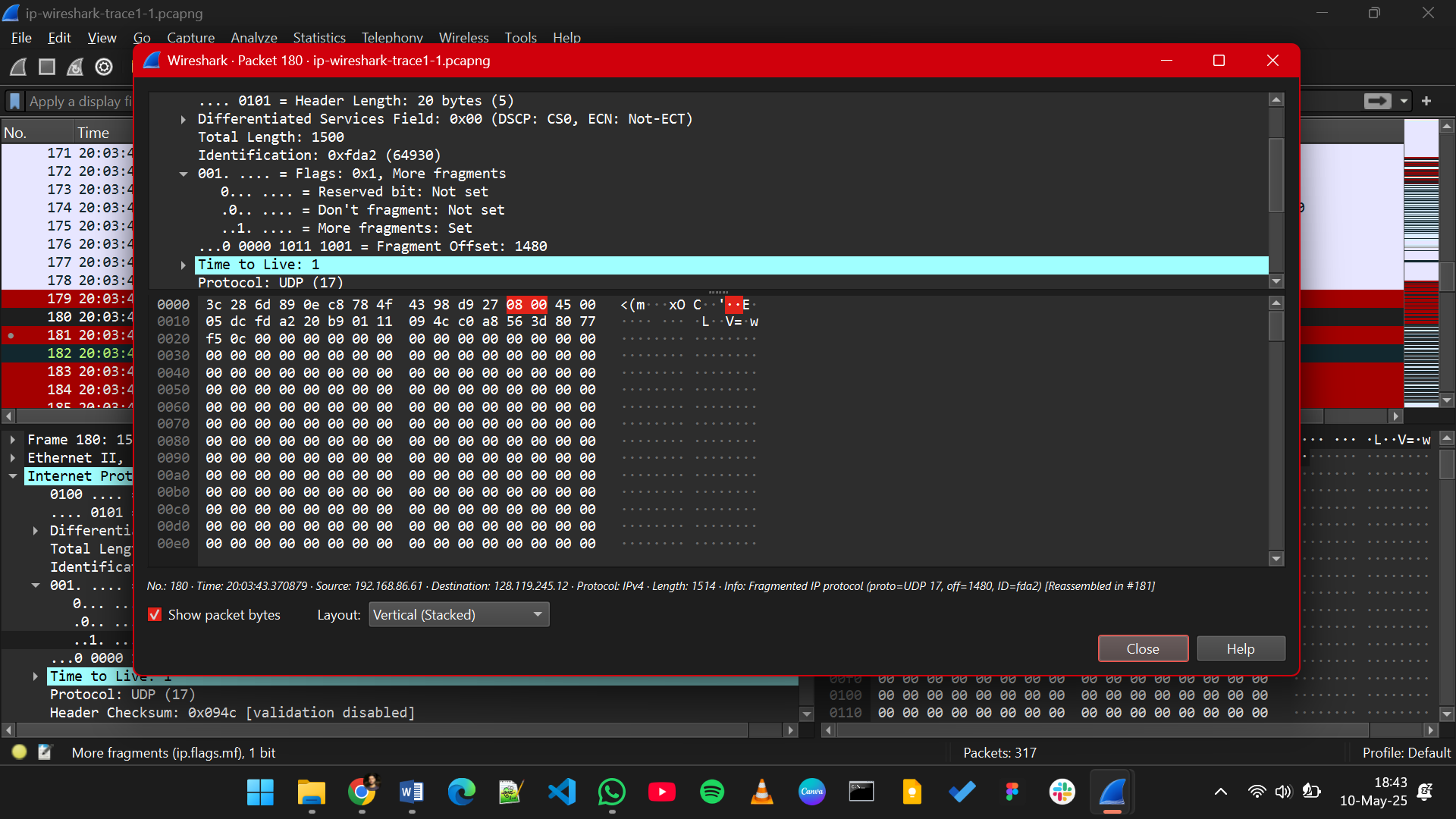
**Fragment offset is 0, More Fragments = 1**

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

**Total Length: 1500**

1. What information in the IP header indicates that this is not the first datagram fragment?

**Fragment Offset > 0**



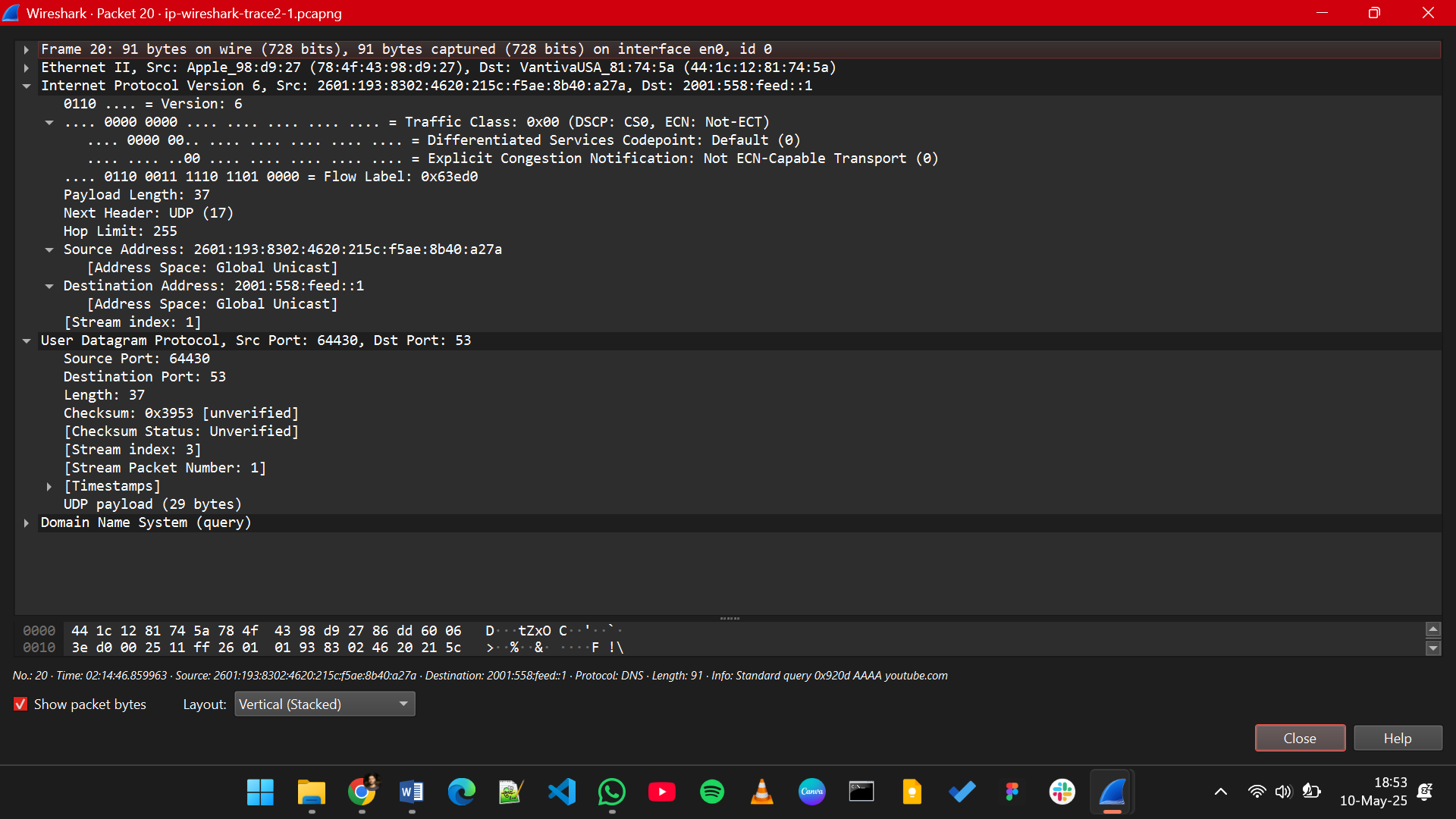
1. What fields change in the IP header between the first and second fragment?

* **Fragment Offset**
* **More Fragments**
* **Total Length**
* **Header Checksum**

1. What information in the IP header indicates that this is the last fragment of that segment?

**The "More fragments" flag in the IP header is set to 0, indicating that this is the last fragment of the original segment.**

## Part 3: IPv6



1. What is the IPv6 address of the computer making the DNS AAAA request?

**2601:193:8302:4620:215c:f5ae:8b40:a27a**

1. What is the IPv6 destination address for this datagram?

**2001:558:feed::1**

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

**0x063ed0**

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

**37**

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

**UDP(17)**

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

**There is 1 IPv6 address returned in the response to this AAAA request.**

1. What is the first of the IPv6 addresses returned by the DNS for youtube.com?

**2607:f8b0:4006:815::200e**

