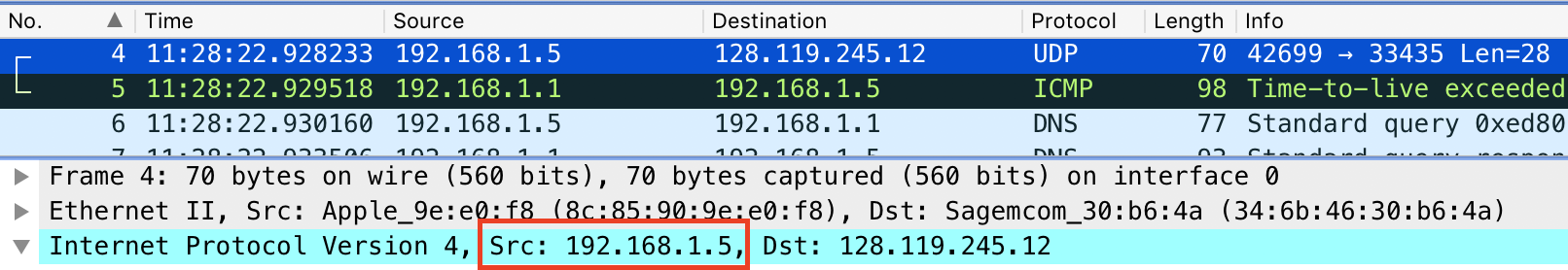
­CSCE 560

2nd Lt David Crow

Wireshark Lab 4

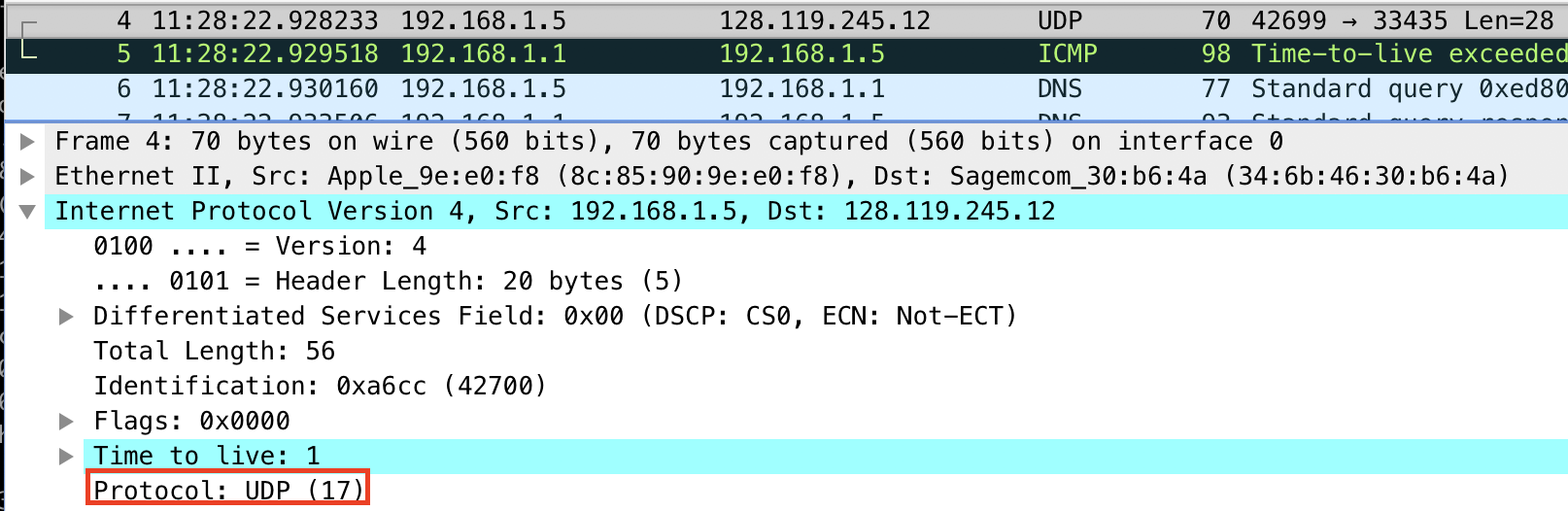
1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

My IP address is 192.168.1.5.



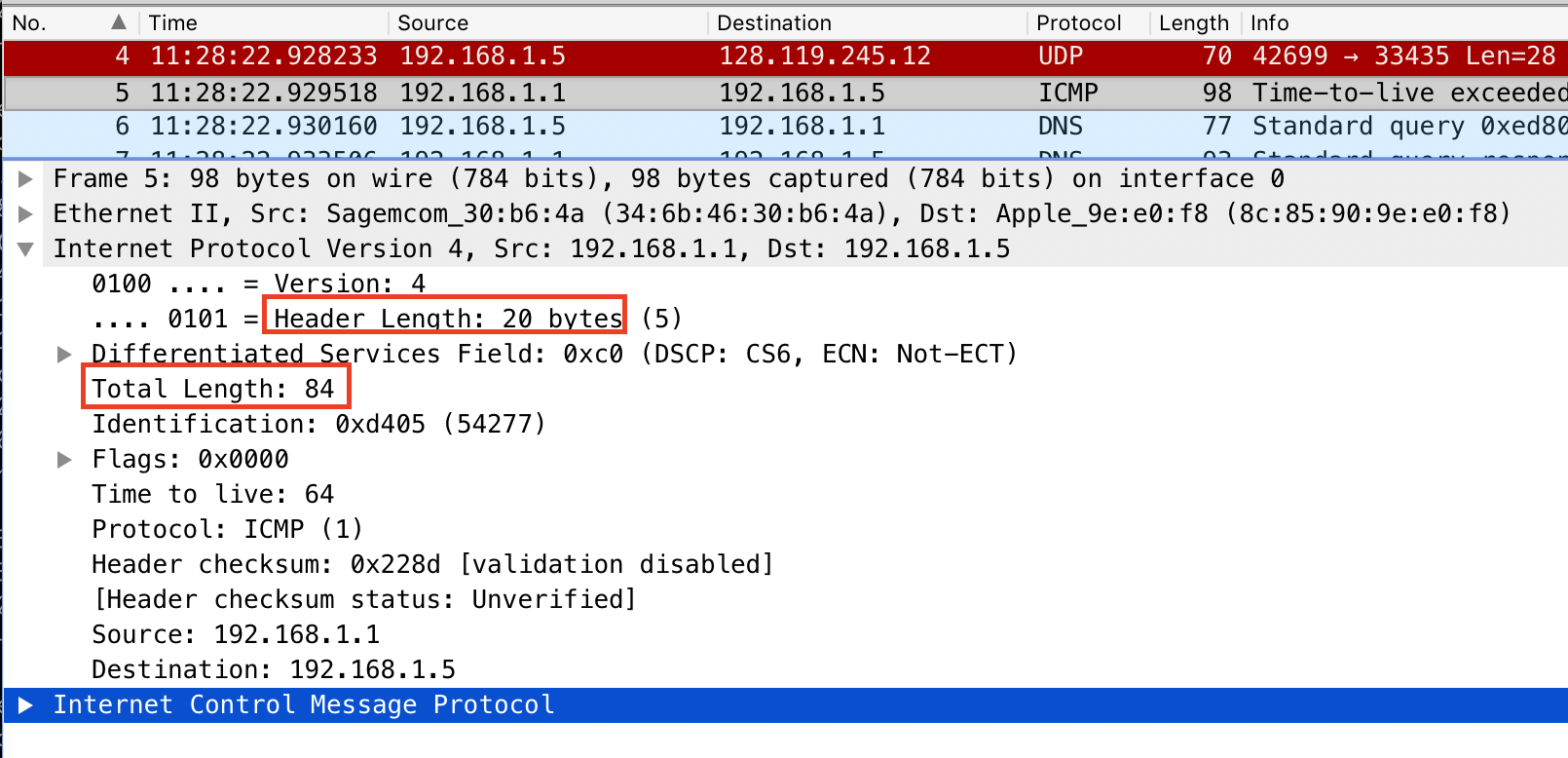
1. Within the IP packet header, what is the value in the upper layer protocol field?

The value in the upper-layer protocol field is 17, which signifies UDP.



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.

The IP header contains 20 bytes. The payload of the IP datagram contains 64 bytes. We know this because the total length of the IP datagram is 84 bytes, and 20 of those bytes are for the header; the other 64 are thus payload.



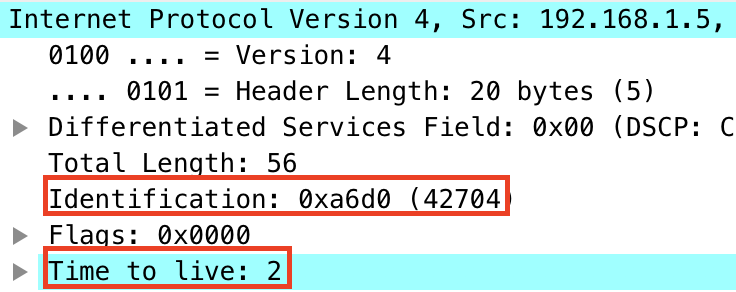
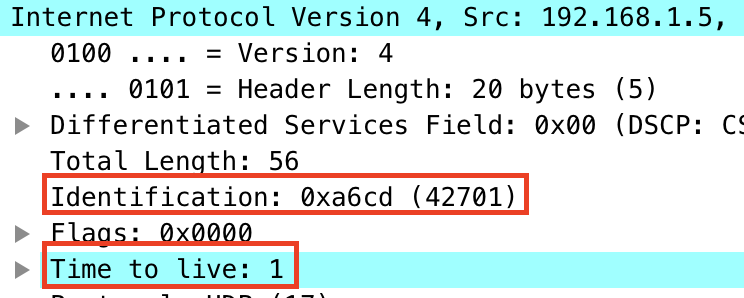
1. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

There are no IPv4 fragments in the below screenshot, so the IP datagram is thus not fragmented.



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

The identification field is strictly increasing. The time to live field is monotonically increasing. I’ve shown two non-consecutive packets that illustrate this.



1. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?

The source and destination IP addresses, the IP version number (and thus the header length), the flags, and the upper-layer protocol fields must all remain constant to ensure the packets are sent to the same place, from the same place, and via the same protocols.

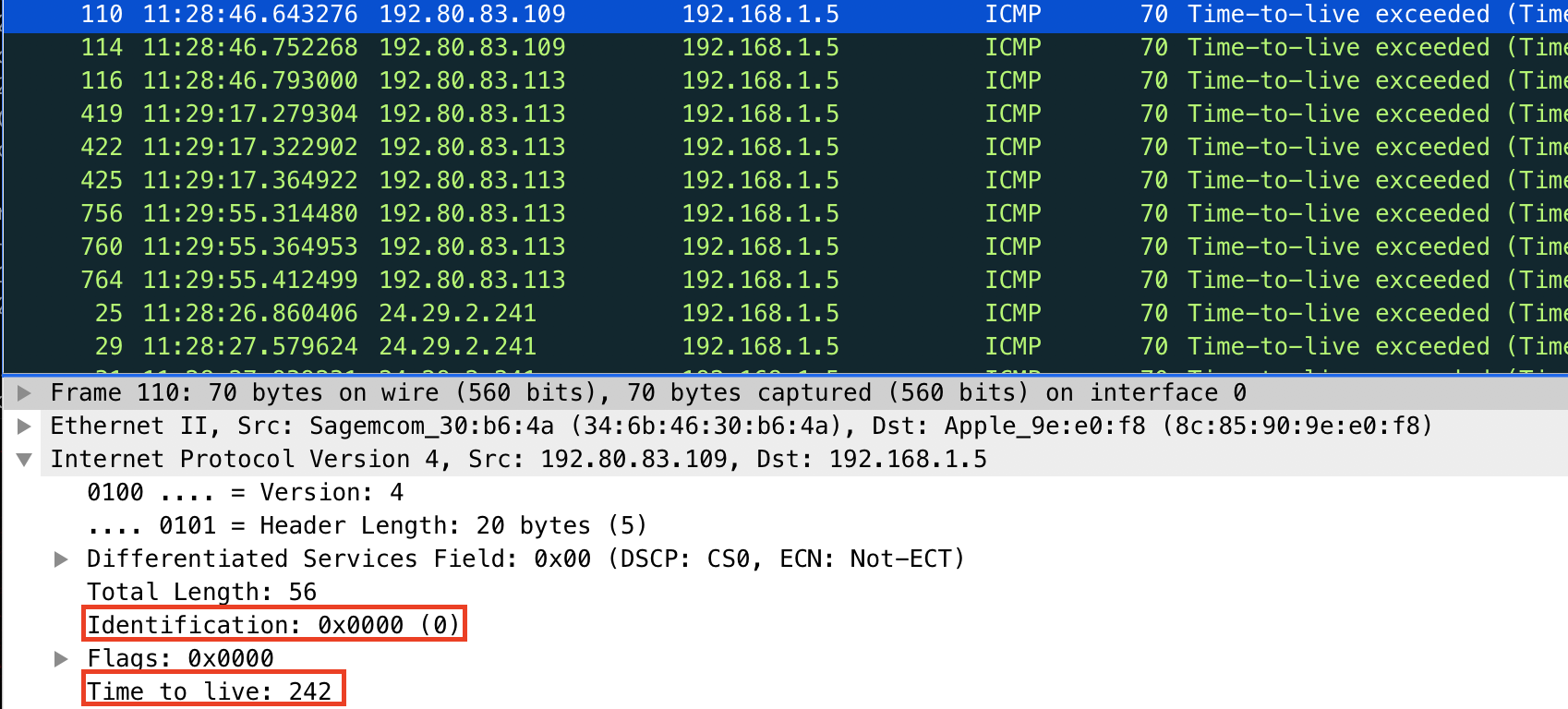
The identification field must change because it uniquely identifies each datagram. The TTL field must change because this is how traceroute works.

1. Describe the pattern you see in the values in the Identification field of the IP datagram.

As mentioned above, the values in the identification field increase from packet to packet.

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

The identification field has a value of 0 for all such packets. The TTL field has a value of 242 or 241 for all such packets.



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

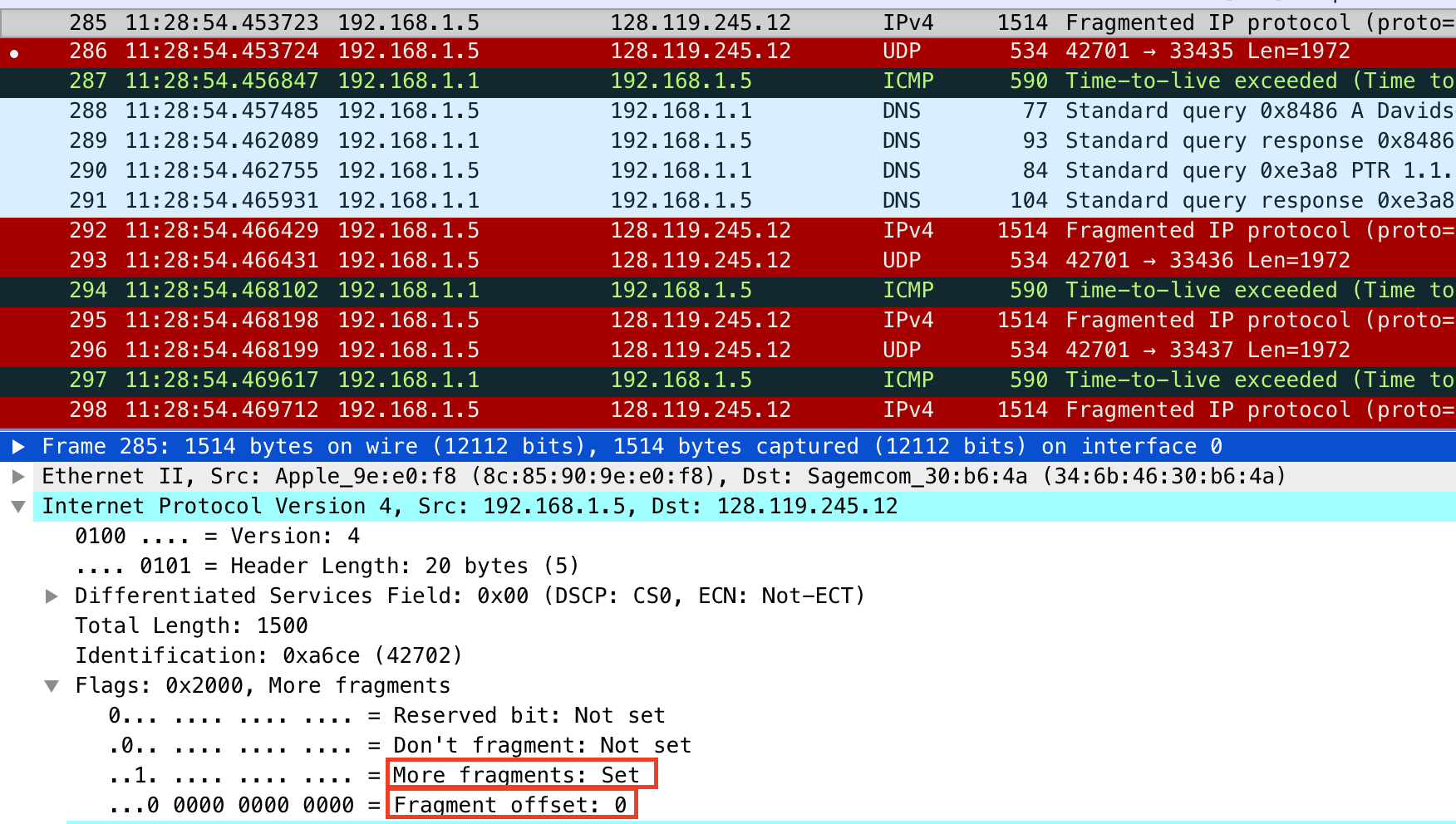
The identification changes because it uniquely identifies packets; a nonidentical identification field indicates that such a packet is a fragment of a larger datagram. The TTL field does not change because traceroute always uses the same TTL for the first-hop router.

1. Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 2000. Has that message been fragmented across more than one IP datagram?

Yes, the message was fragmented. We can see in the Problem 11 screenshot that there are “more fragments” to view.

1. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

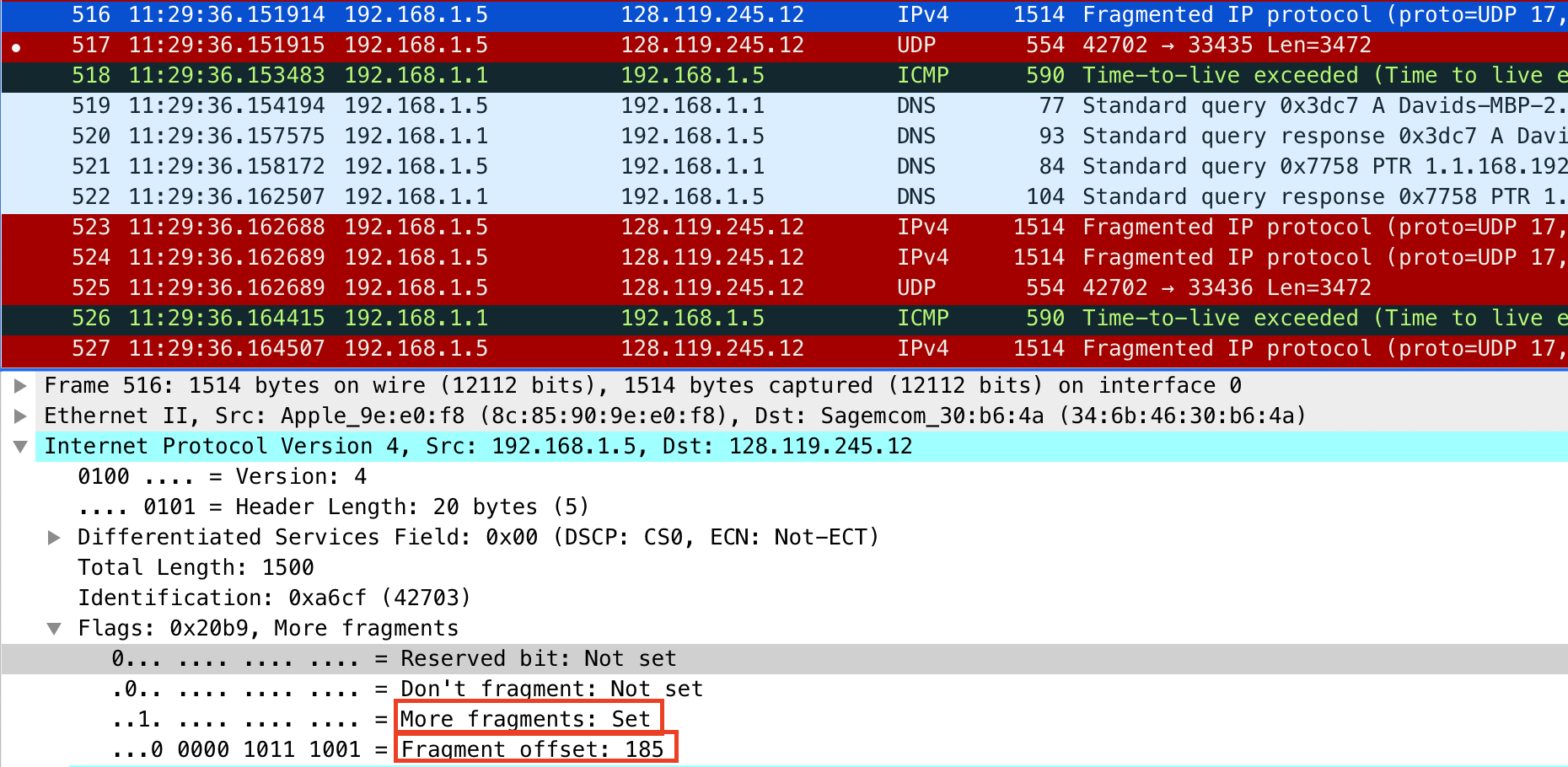
We can see that the “more fragments” flag is set. We can also see that the fragment offset is 0, which means this is the first fragment.



1. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?

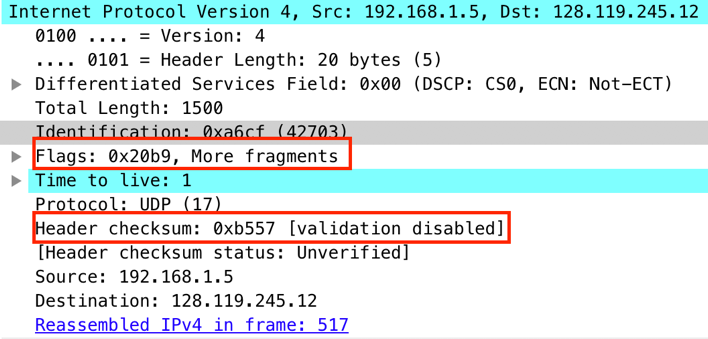
We know that the below fragment (from a different transmission than in the screenshot above) has a fragment offset of 185; this indicates that this is not the first fragment.

Additionally, the “more fragments” bit is set, so we know this is also not the last fragment.



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

We can see from these two fragments that the flags change (because the fragment offset changes) and that the header checksum changes (because the header itself changes).



1. How many fragments were created from the original datagram?

Three fragments were created after switching to 3500 bytes for the traceroute.



1. What fields change in the IP header among the fragments?

The header offset changes in each fragment. The header checksum also changes in each fragment. The more fragments bit is set in the first two fragments, but it is not set in the third. The total length (1500 bytes) is the same for the first two packets, but it changes to 540 bytes for the third packet.