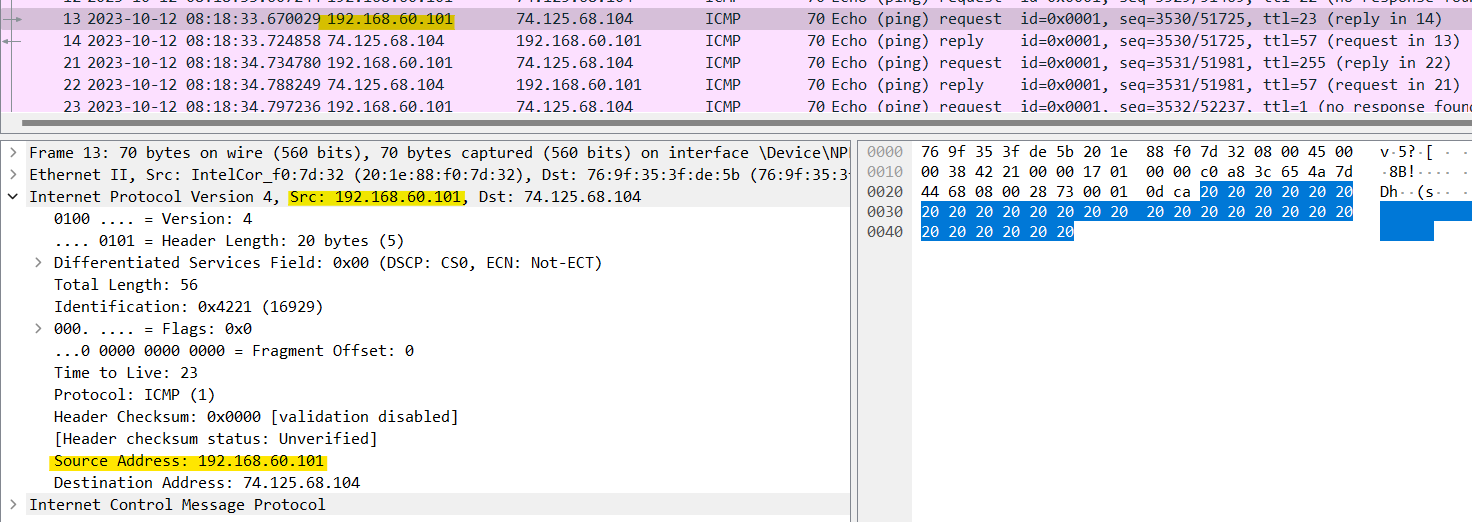
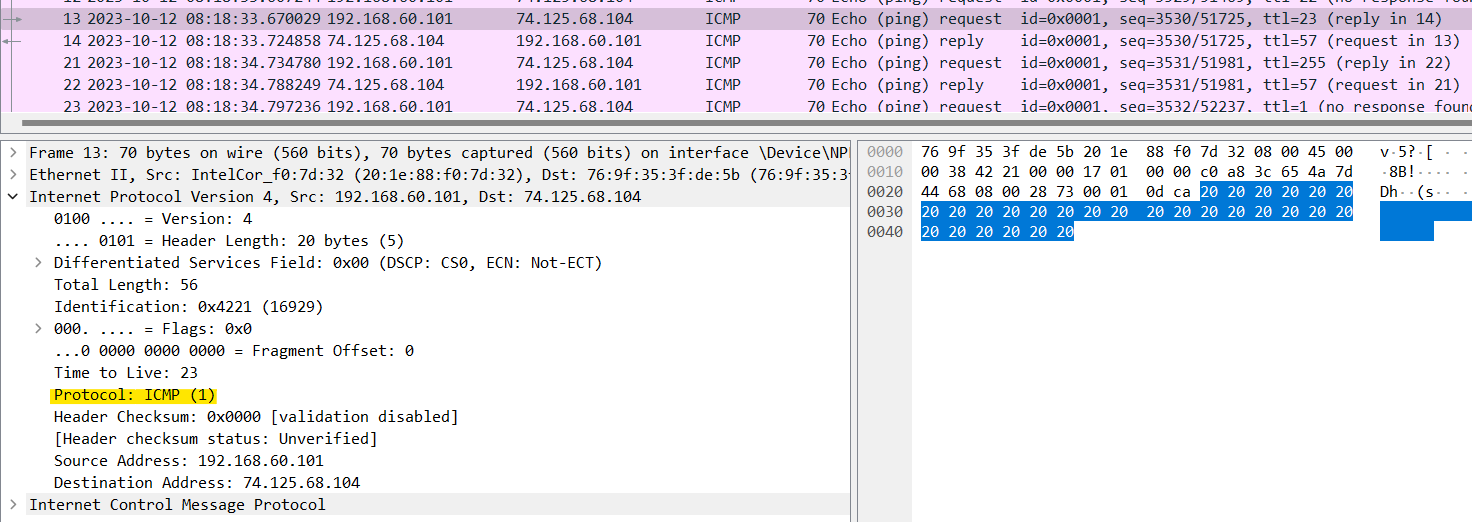
# LAB 4A Wireshark Lab: IP

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?*



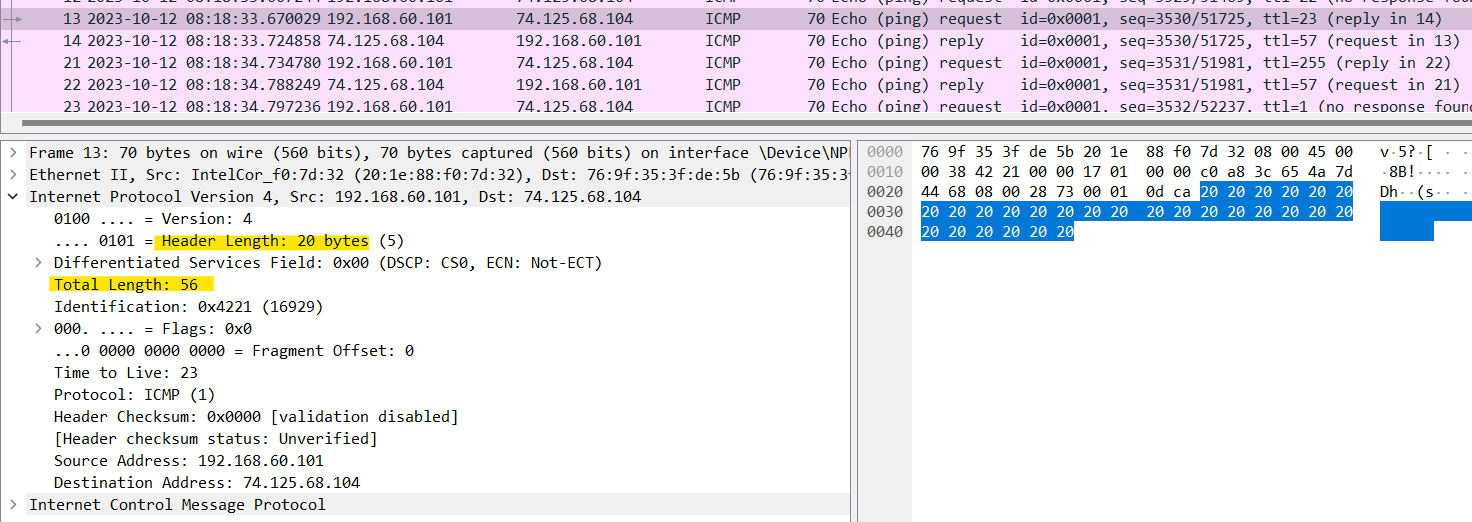
IP address of my computer is: 192.168.60.101

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 ICMP (1)

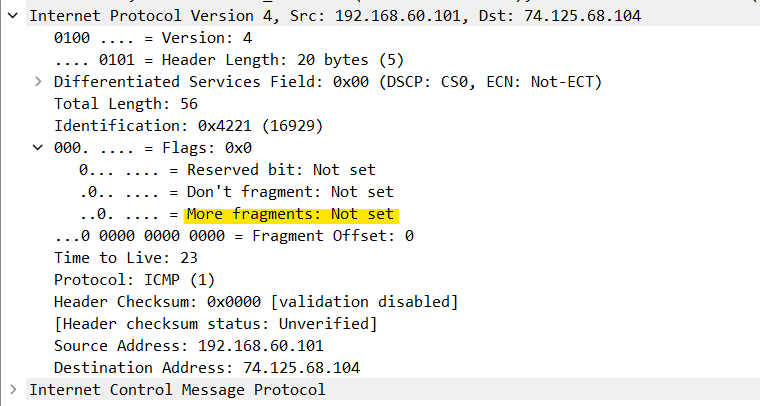
1. *How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.*



The header length is 20 bytes and the total length is 56 bytes. Therefore, the

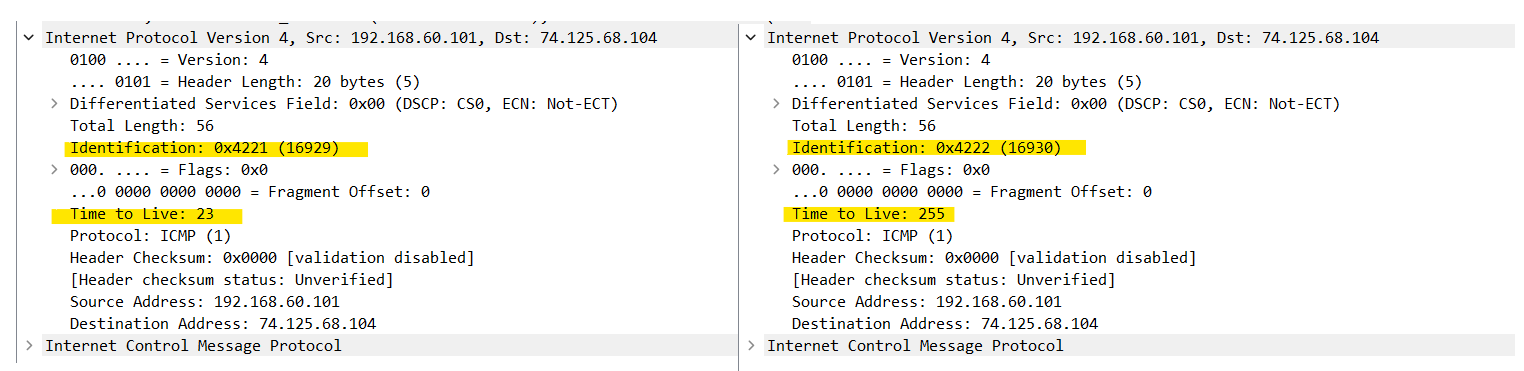
payload of the IP datagram should be 36 bytes (56 bytes – 20 bytes).

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



The more fragments is Not set, so the data is 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, TTL (time to live) field.

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

The following fields remain constant:

• version (IPv4 always used)

• header length (doesn’t change since we are always using IPv4)

• source IP (my computer’s IP address doesn’t change)

• destination IP (usc.edu’s IP address doesn’t change)

• differentiated services (same protocol every time)

• upper layer protocol (same protocol every time)

• header checksum (verification disabled in my tests)

The following fields change:

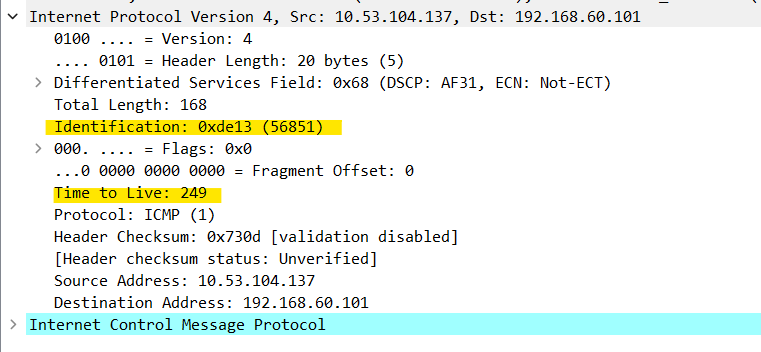
• Identification field (each IP datagram has a different ID)

• Time to live (this is how trace route works, as discussed in the assignment)

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

They are incrementing with each request.

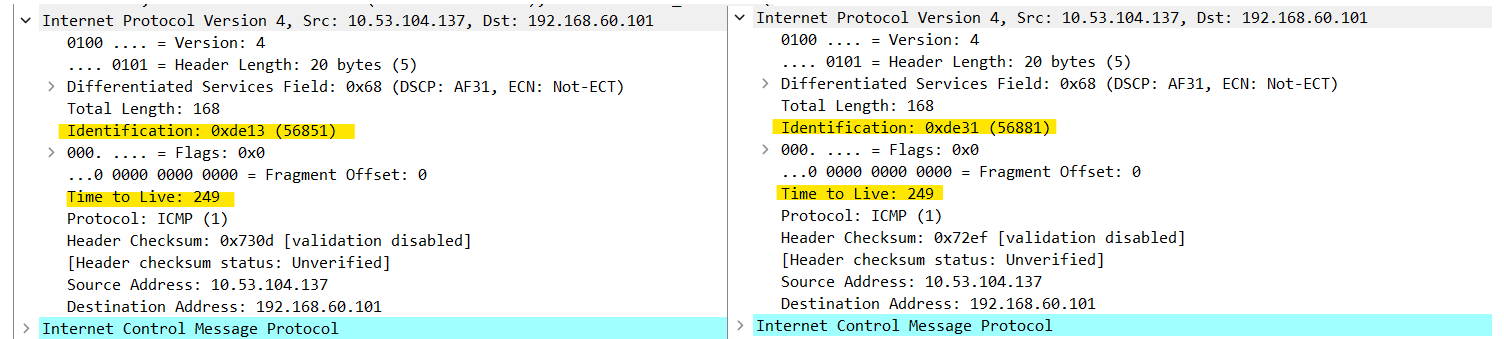
1. *What is the value in the Identification field and the TTL field?*



The value in the Identification field is 0xde13 (56851)

The value in the TTL field is 249

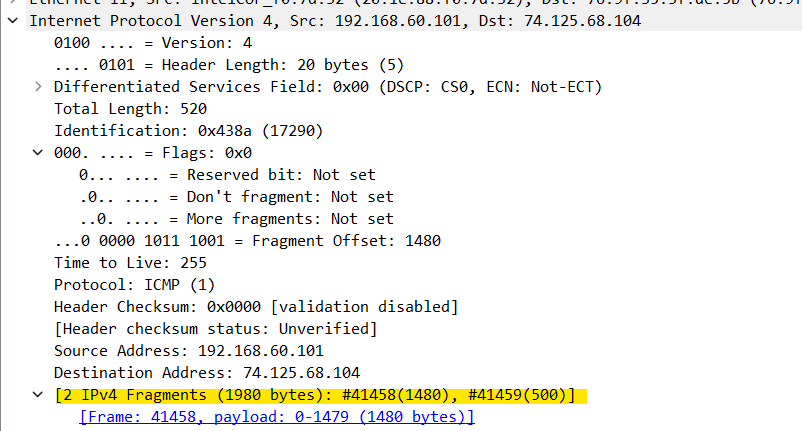
1. *Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?*



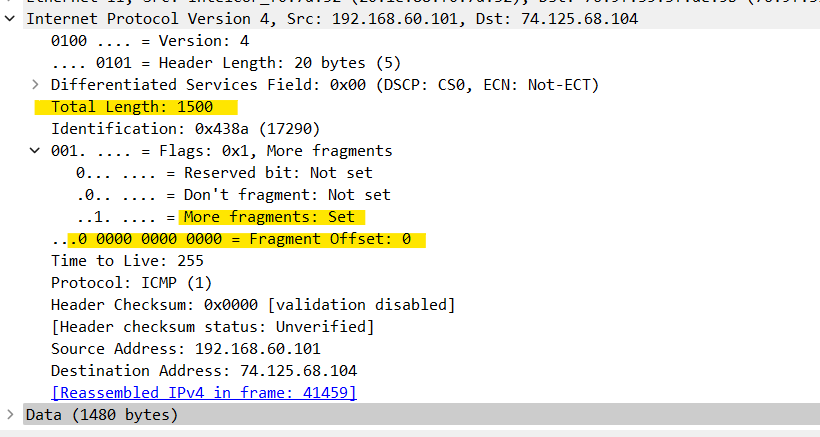
* The Identification field value is changed because the identification field is a unique value. If two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram.
* The TTL field was unchanged since the TTL for the nearest router is always the same

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, it has 2 fragments.



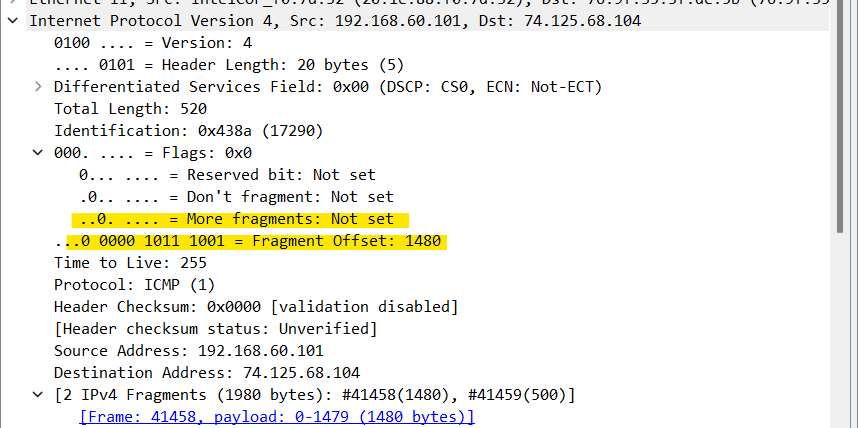
1. *Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?*



In the IP header of the first fragment the more fragment flag was set. It indicates that the datagram been fragmented and has another fragment.

Since the fragment offset is 0, we know that this is the first fragment. This first datagram has a total length of 1500, including the header.

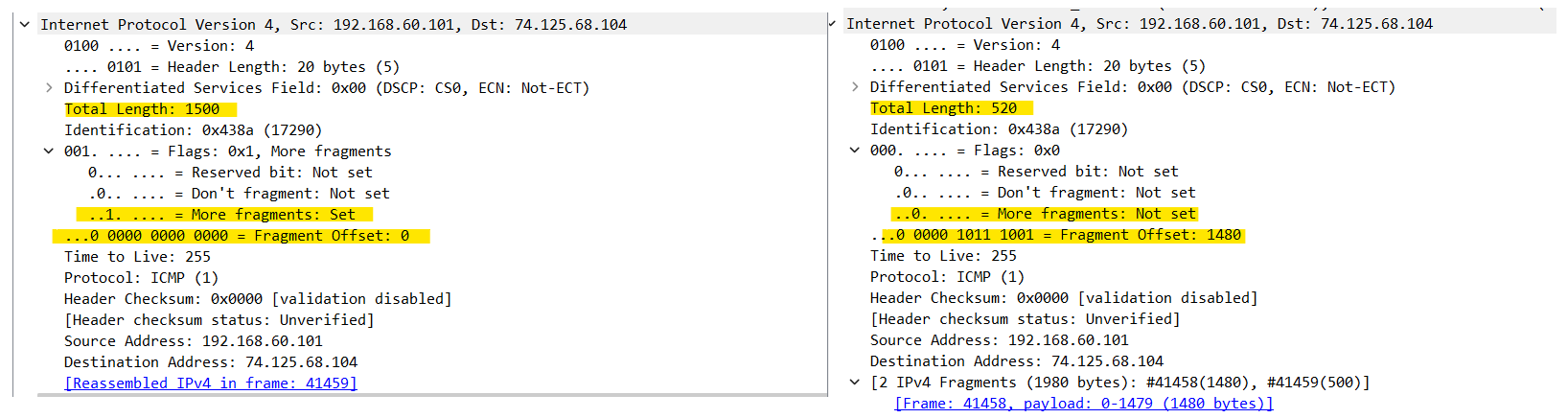
1. *Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?*



We can tell that this is not the first fragment, since the fragment offset is 1480.

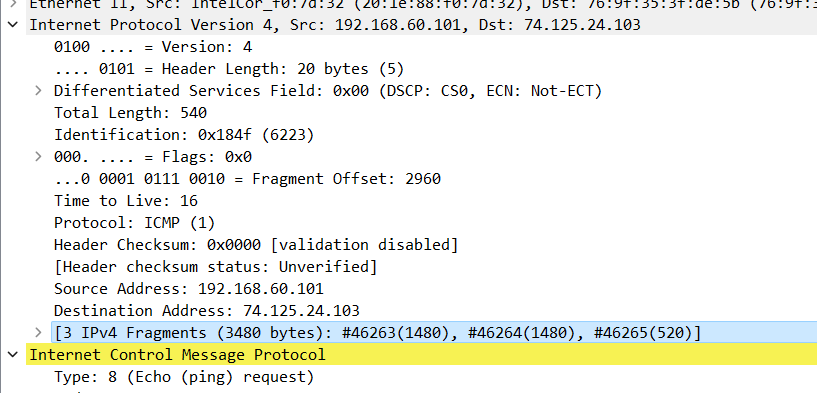
It is the last fragment, since the more fragments flag is not set.

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



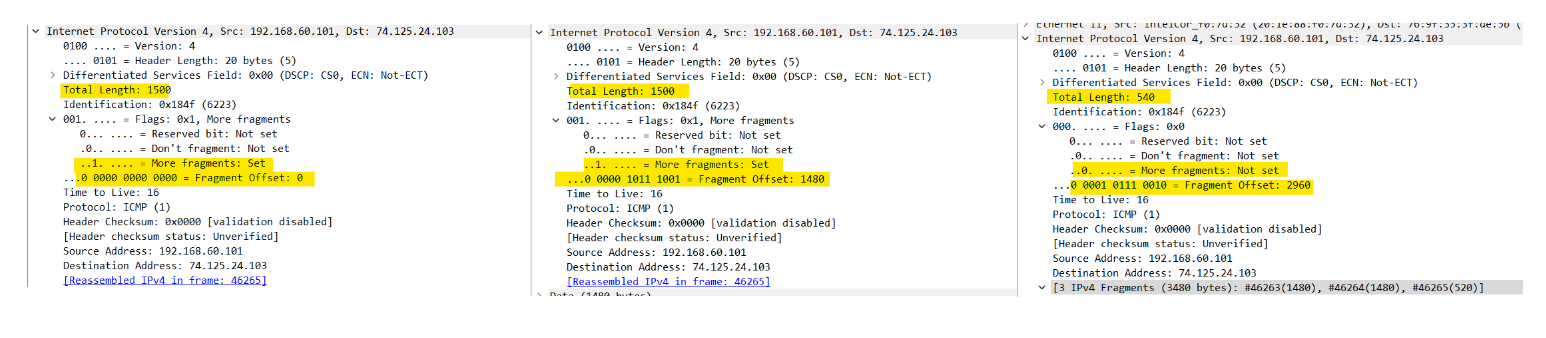
The IP header fields that changed between the fragments are: total length, flags, fragment offset

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



After switching to 3500, there are 3 packets created from the original datagram.

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



The IP header fields that changed between all of the packets are: fragment off- set. Between the first two packets and the last packet, we see a change in total length, and also in the flags. The first two packets have a total length of 1500, with the more fragments bit set to 1, and the last packet has a total length of 540, with the more fragments bit set to 0