­­CSC 265 Lab Assignment 3

Due on 11/03/2017 11:59pm

In this lab, we’ll investigate the IP protocol, focusing on the IP datagram. We’ll do so by analyzing a trace of IP datagrams sent and received by an execution of the traceroute program (the traceroute program itself is explored in more detail in the Wireshark ICMP lab). We’ll investigate the various fields in the IP datagram, and study IP fragmentation in detail.

1. Capturing packets from an execution of traceroute

In order to generate a trace of IP datagrams for this lab, we’ll use the traceroute program to send datagrams of different sizes towards some destination, *X*. Recall that traceroute operates by first sending one or more datagrams with the time-to-live (TTL) field in the IP header set to 1; it then sends a series of one or more datagrams towards the same destination with a TTL value of 2; it then sends a series of datagrams towards the same destination with a TTL value of 3; and so on. Recall that a router must decrement the TTL in each received datagram by 1 (actually, RFC 791 says that the router must decrement the TTL by *at least* one). If the TTL reaches 0, the router returns an ICMP message (type 11 – TTL-exceeded) to the sending host. As a result of this behavior, a datagram with a TTL of 1 (sent by the host executing traceroute) will cause the router one hop away from the sender to send an ICMP TTL-exceeded message back to the sender; the datagram sent with a TTL of 2 will cause the router two hops away to send an ICMP message back to the sender; the datagram sent with a TTL of 3 will cause the router three hops away to send an ICMP message back to the sender; and so on. In this manner, the host executing traceroute can learn the identities of the routers between itself and destination *X* by looking at the source IP addresses in the datagrams containing the ICMP TTL-exceeded messages.

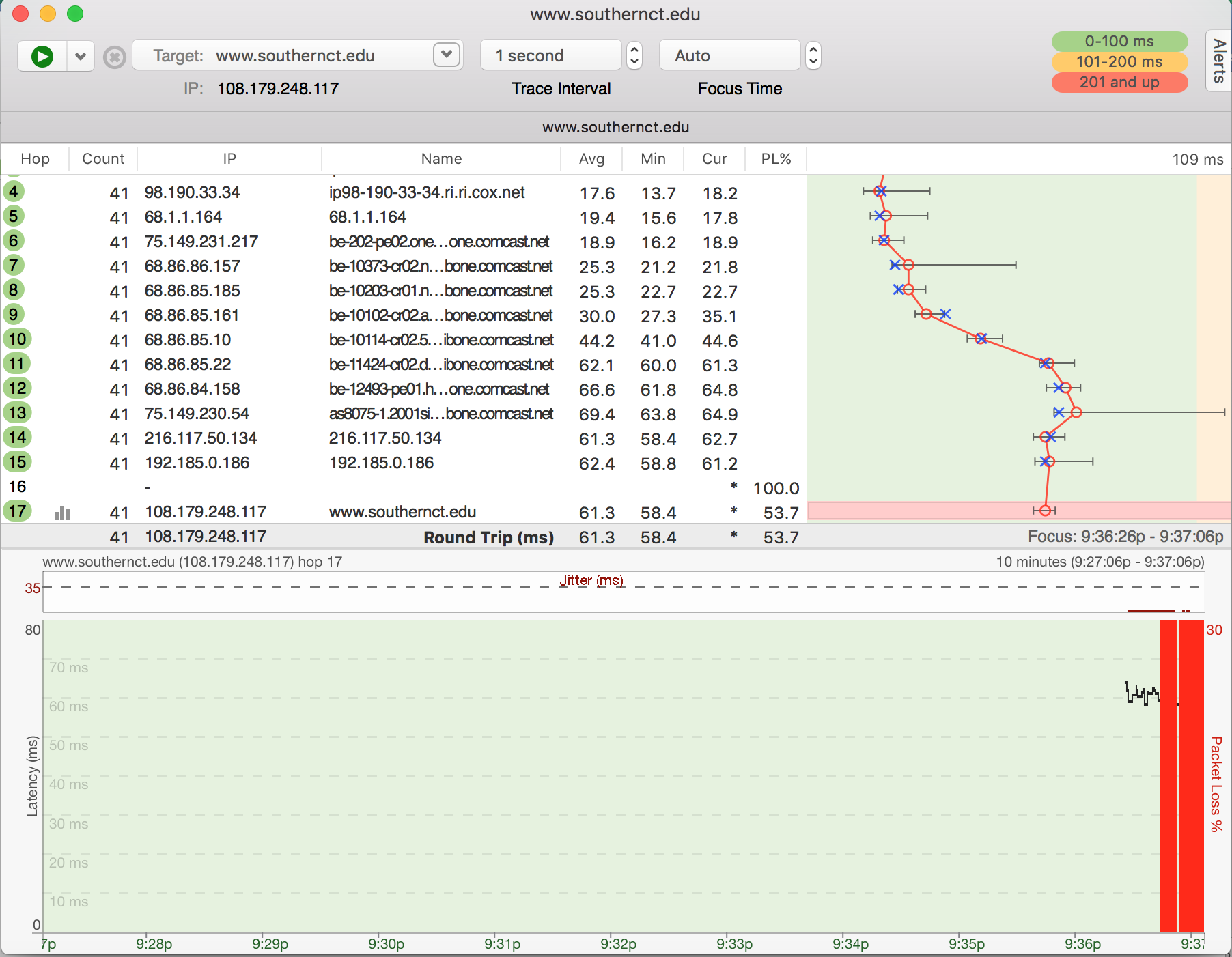
We’ll want to run traceroute and have it send datagrams of various lengths.

* **Windows.** The tracert program (used for our ICMP Wireshark lab) provided with Windows does not allow one to change the size of the ICMP echo request (ping) message sent by the tracert program. A nicer Windows traceroute program is *pingplotter*, available both in free version and shareware versions at <http://www.pingplotter.com>. Download and install *pingplotter*, and test it out by performing a few traceroutes to your favorite sites. Select Pro edition, you have 14 days of free trial. The size of the ICMP echo request message can be explicitly set in *pingplotter* by selecting the menu item *Edit-> Options->Engine* and then filling in the *Packet Size* field. The default packet size is 56 bytes. Once *pingplotter* has sent a series of packets with the increasing TTL values, it restarts the sending process again with a TTL of 1, after waiting *Trace Interval* amount of time. The value of *Trace Interval* and the number of intervals can be explicitly set in *pingplotter*.
* **Linux/Unix/MacOS.** With the Unix/MacOS traceroute command, the size of the UDP datagram sent towards the destination can be explicitly set by indicating the number of bytes in the datagram; this value is entered in the traceroute command line immediately after the name or address of the destination. For example, to send traceroute datagrams of 2000 bytes towards southernct.edu, the command would be:

%traceroute southernct.edu 2000

Do the following:

* Start up Wireshark and begin packet capture *(Capture->Start)* and then press *OK* on the Wireshark Packet Capture Options screen (we’ll not need to select any options here).
* If you are using a Windows platform, start up *pingplotter* and enter the name of a target destination in the “Address to Trace Window.” Select the menu item *Edit-> Options->Engine* and enter a value of 56 in the *Packet Size* field and then press OK. Then press the Trace button. You should see a *pingplotter* window that looks something like this:



Next, send a set of datagrams with a longer length, by selecting *Edit-> Options->Engine* and enter a value of 2000 in the *Packet Size* field and then press OK. Then press the Resume button.

Finally, send a set of datagrams with a longer length, by selecting *Edit-> Options->Engine* and enter a value of 3500 in the *Packet Size* field and then press OK. Then press the Resume button.

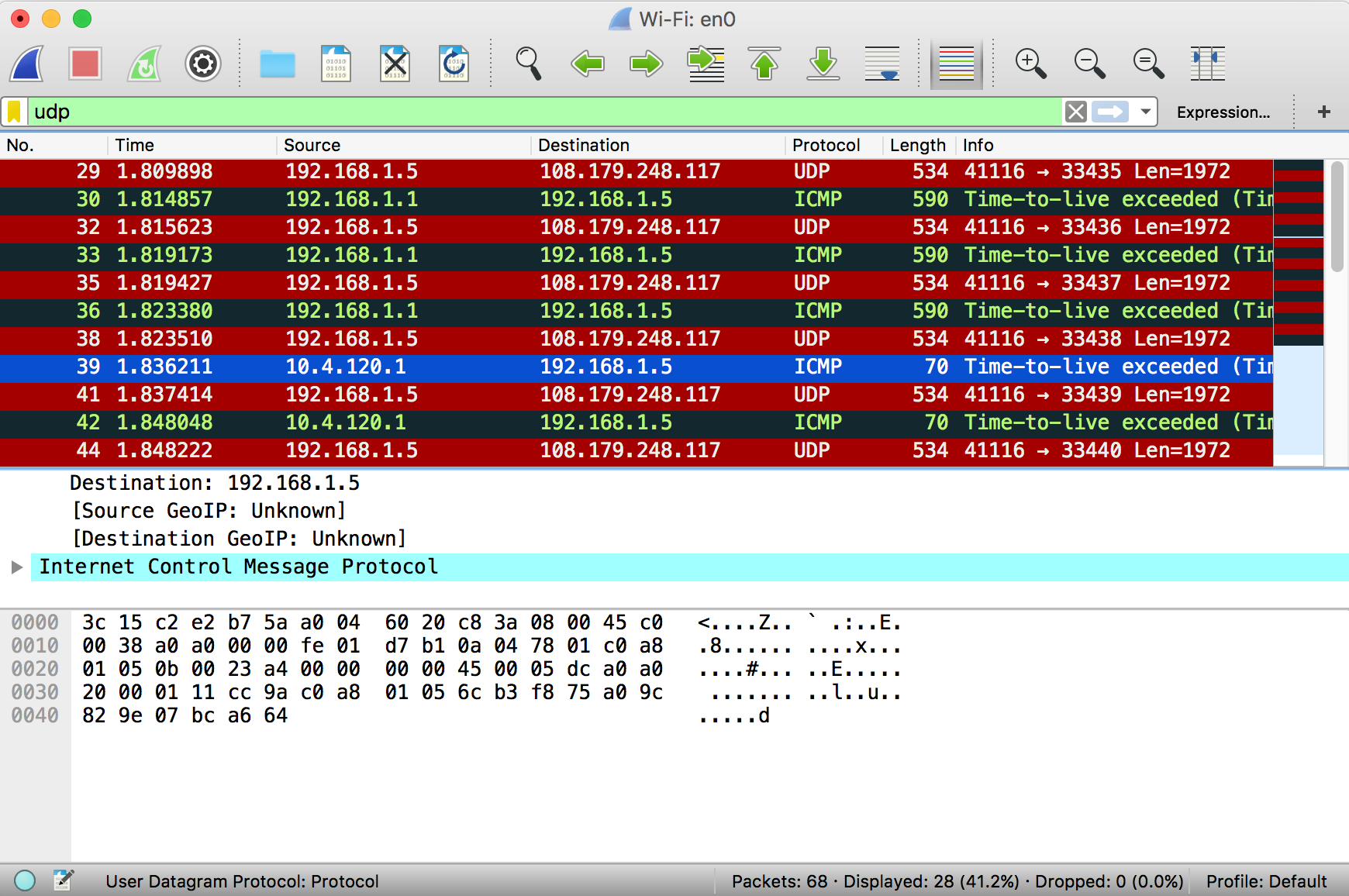
Stop Wireshark tracing.

* If you are using a Unix or Mac platform, enter three traceroute commands, one with a length of 56 bytes, one with a length of 2000 bytes, and one with a length of 3500 bytes.

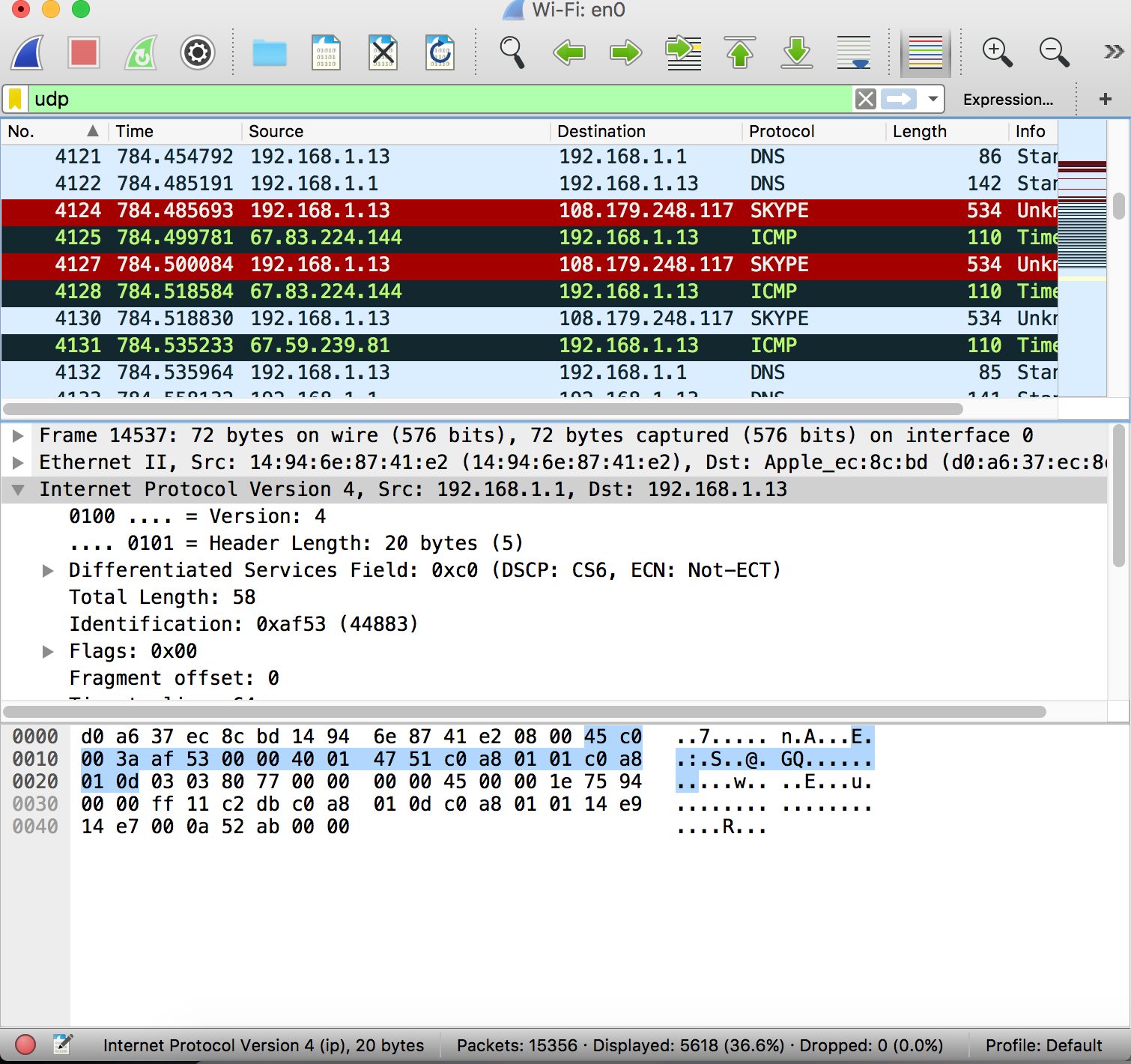
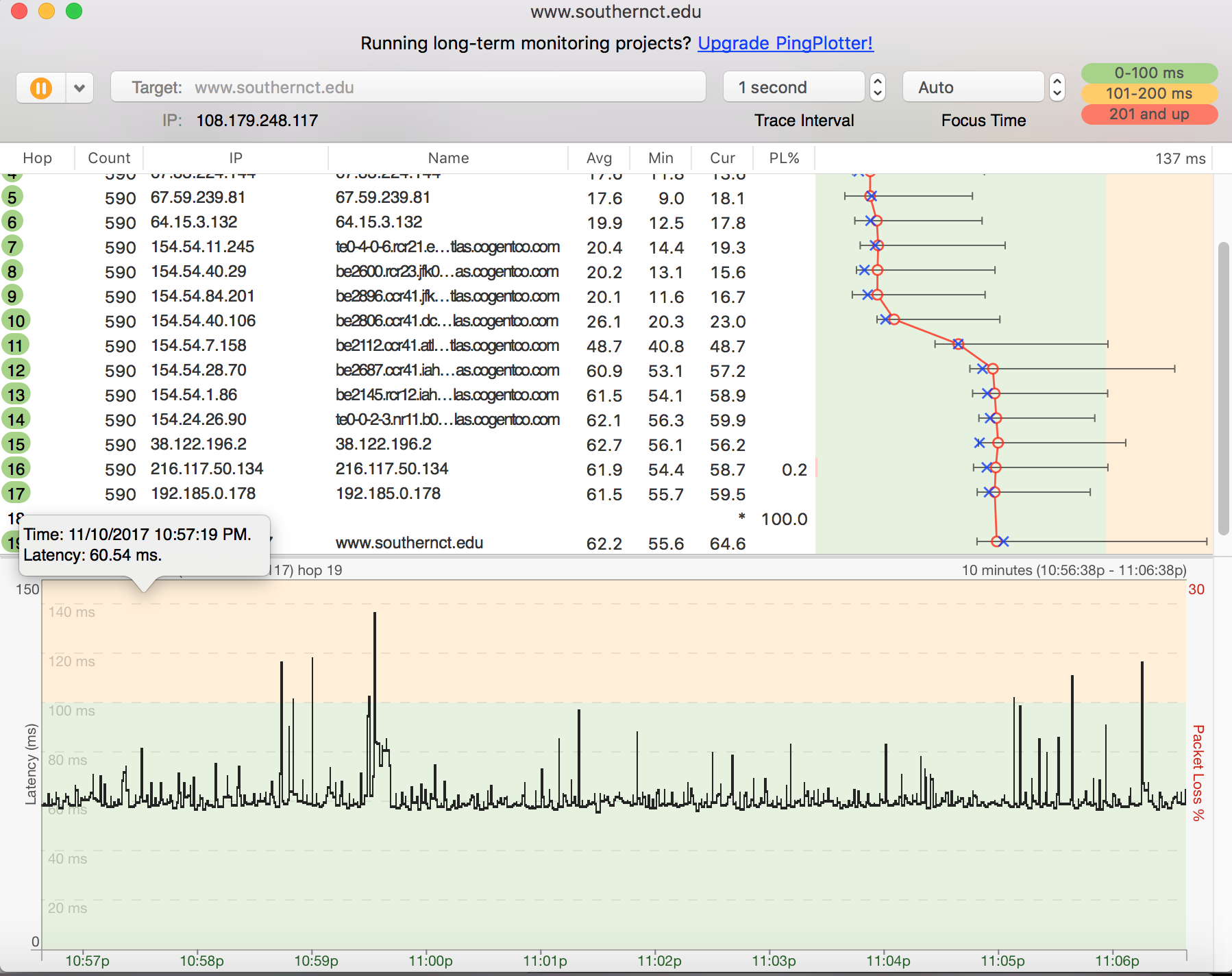
Stop Wireshark tracing.

2. A look at the captured trace

In your trace, you should be able to see the series of ICMP Echo Request (in the case of Windows machine) or the UDP segment (in the case of Unix) sent by your computer and the ICMP TTL-exceeded messages returned to your computer by the intermediate routers. In the questions below, we’ll assume you are using a Windows machine; the corresponding questions for the case of a Unix machine should be clear. Whenever possible, when answering a question below you should attach the screenshots of the packet(s) within the trace that you used to answer the question asked.



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 192.168.1.13

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

* The IP packet header, was the value in the upper layer protocol field which is Skype.

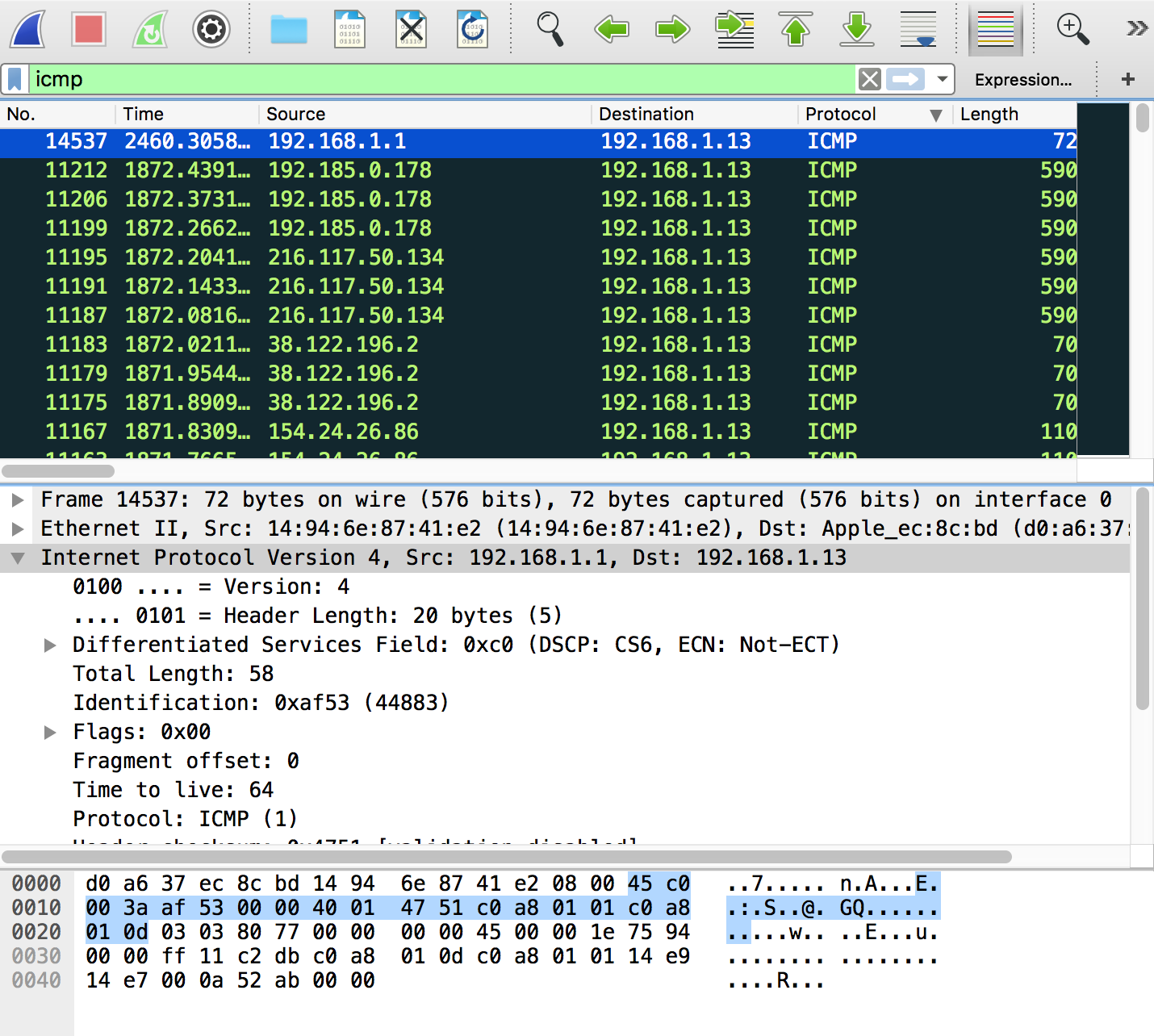
1. How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.

* The bytes are in the IP header length is 20 bytes, the total length is 58 bytes. So, the payload of the IP datagram would be about 38 bytes (58-20).

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

* In the IP datagram fragment the bit =0, which means the data is not a fragment.

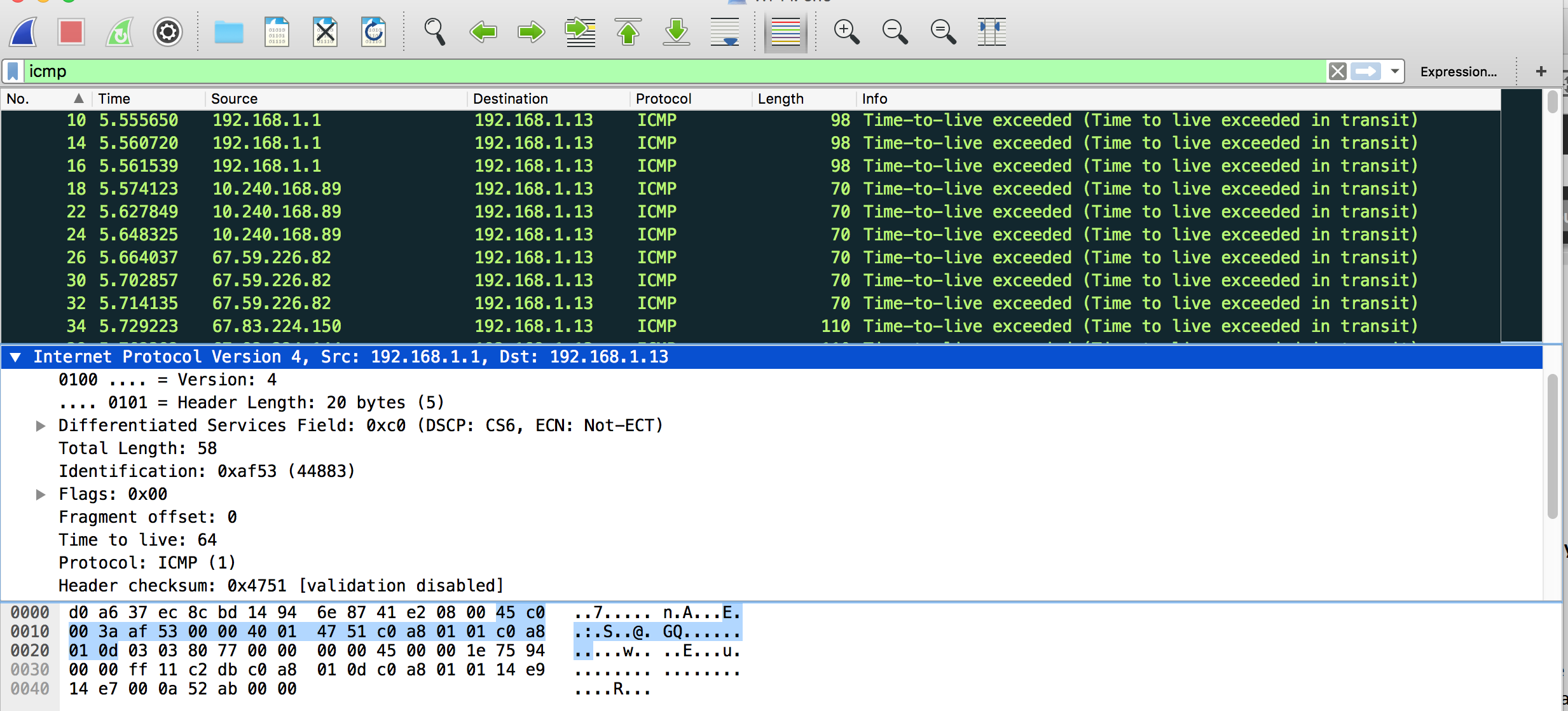
Next, sort the traced packets according to IP source address by clicking on the *Source* column header; a small downward pointing arrow should appear next to the word *Source*. If the arrow points up, click on the *Source* column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the “details of selected packet header” window. In the “listing of captured packets” window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.

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 IP datagram that always changing from one datagram to the next within this series of ICMP messages sent by my computer are the identification field and time to live.
2. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?
   * The fields that stay constant are:
     + Version
     + length
     + Source IP
     + Destination IP
     + Service
     + Upper layer

The reason why is because the version is always used and the length is the same as version and the source IP never change and neither does the destination IP, the services and the protocol are always the same.

* The fields that change is:
  + Identification
  + Time to live

1. Describe the pattern you see in the values in the Identification field of the IP datagram
   * The pattern that is seen in the value in the identification fields are incremented with incrementing each datagram.

Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

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

The identification field is 44883 and the TTL field is 64.

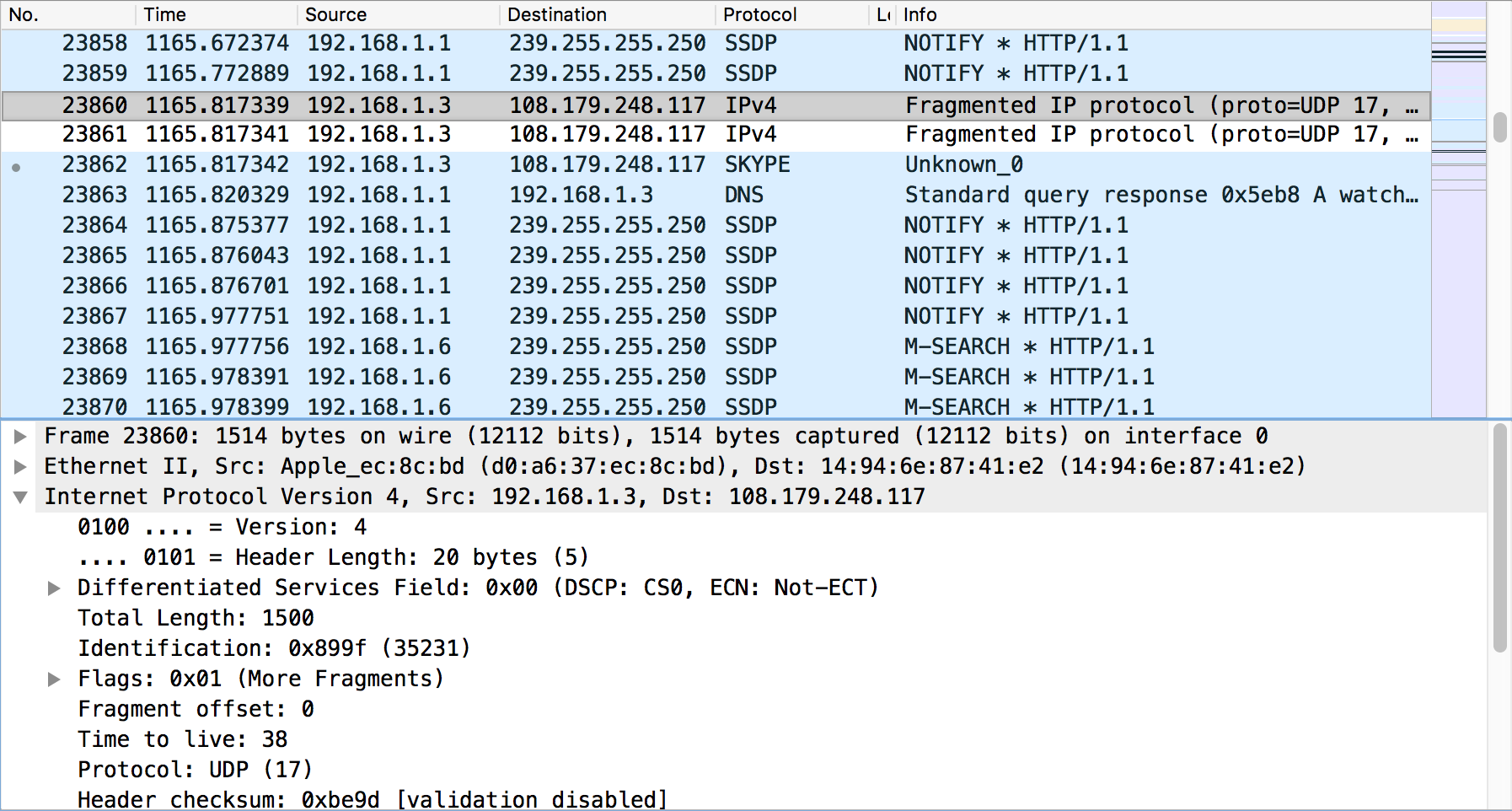
1. Do these values remain unchanged for all the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

The values that remain unchanged for all the ICMP, ttl-exceed replies sent to my computer are the identification field. Ip datagram two or more have the same identification. A Single large datagram of a fragment is IP. The ttl field was unchanged because the TTL are for the nearest router which is always the same.

Fragmentation

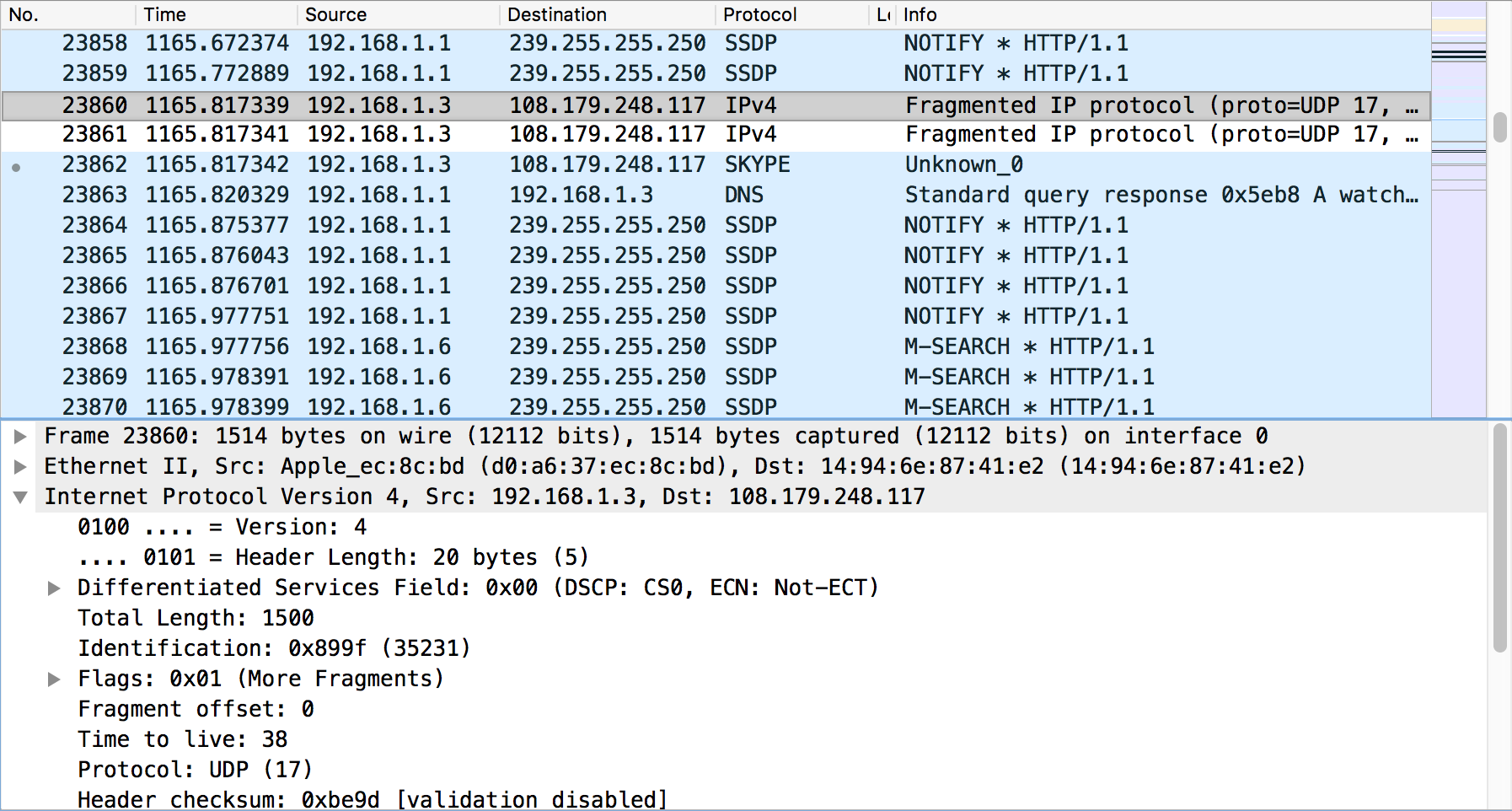
Sort the packet listing according to time again by clicking on the *Time* column.

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.
2. 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?



* + That the flags bit for more fragment that are set, the reason why because the datagram has been fragmented. The fragment offset is 0 in the first fragment and which the length of the first datagram is 1500 in the header.

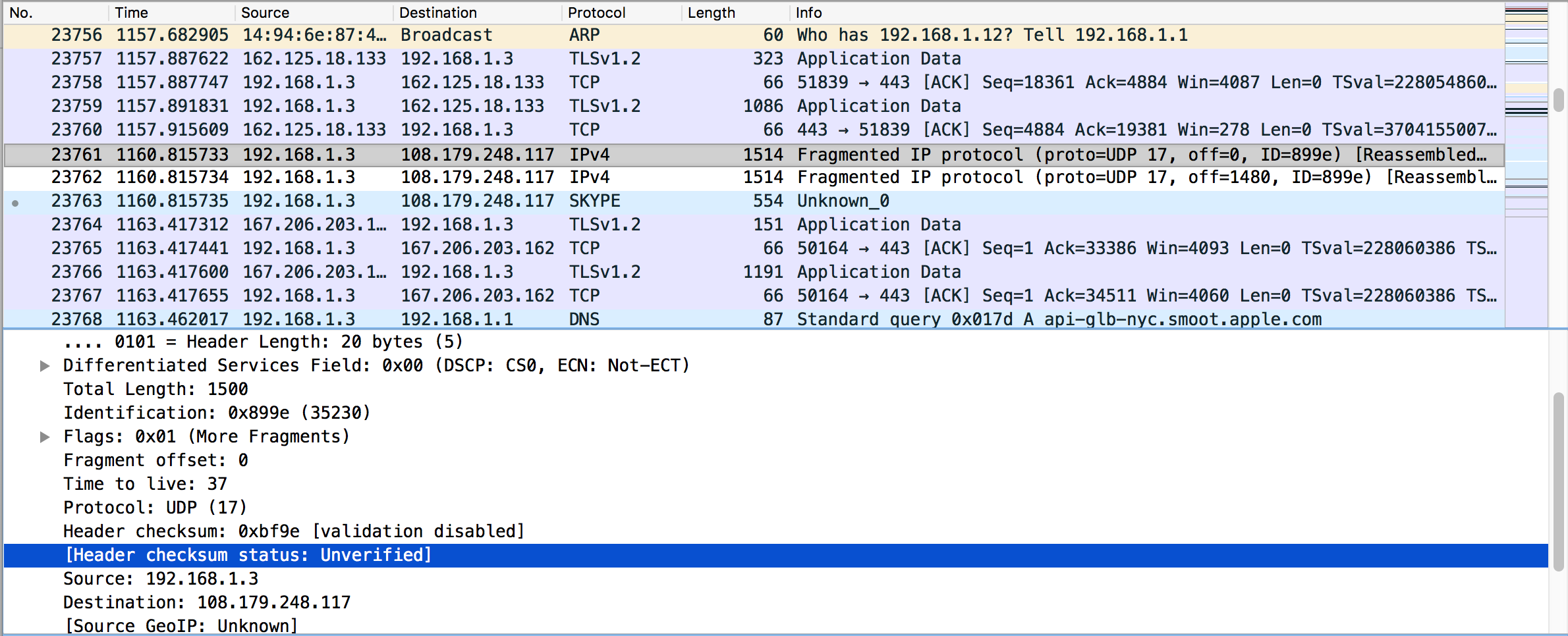
1. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?



* + This is the second fragment since the fragment offset is 1480. In which this should be the last fragment since there is not set of more fragments flags.

1. What fields change in the IP header between the first and second fragment?
   * Total length, flags, Fragment offset and checksum

Now find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 3500.



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

* The number of fragments that created from the original datagram are three fragments.

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

* Fragments from1-2 are offset changes and 2-3 are total length is 1500, bit and offset.