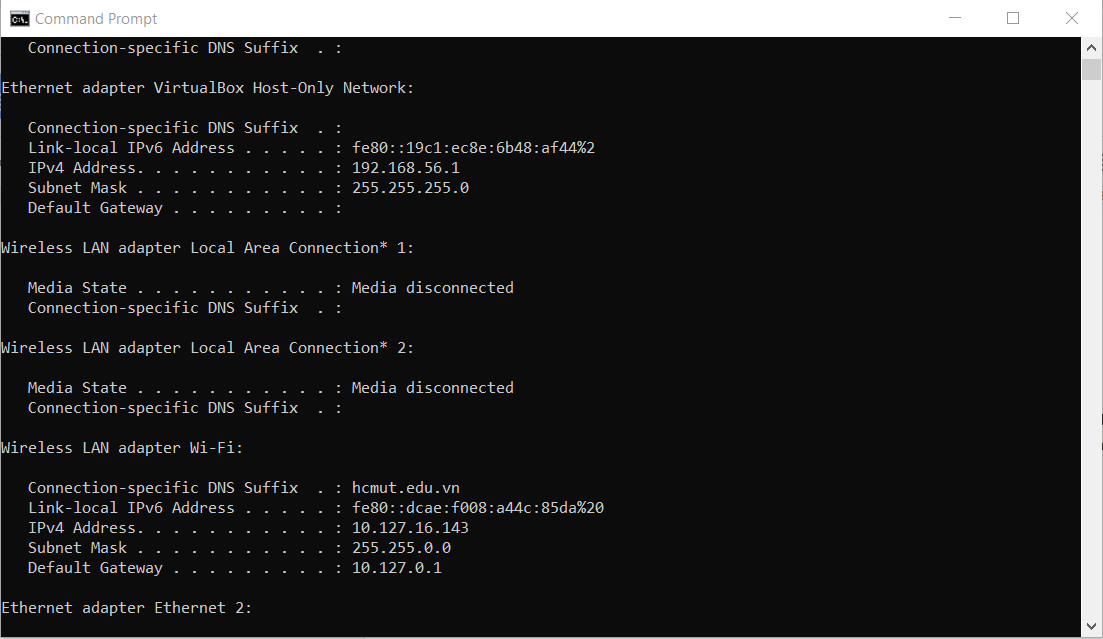
**Computer Network**

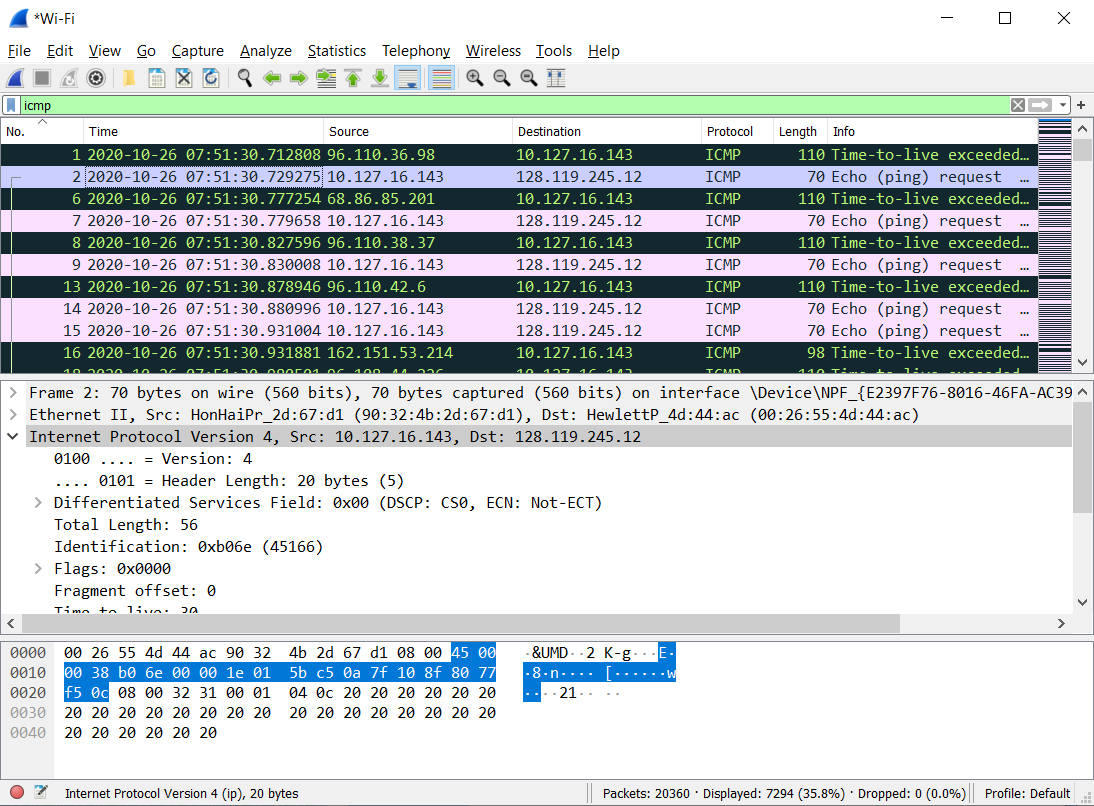
**Wireshark Lab 3a: UDP v8.0**

***Lecturer: Mr. Nguyễn Mạnh Thìn***

***Student: Trần Quốc Anh - 1852247***



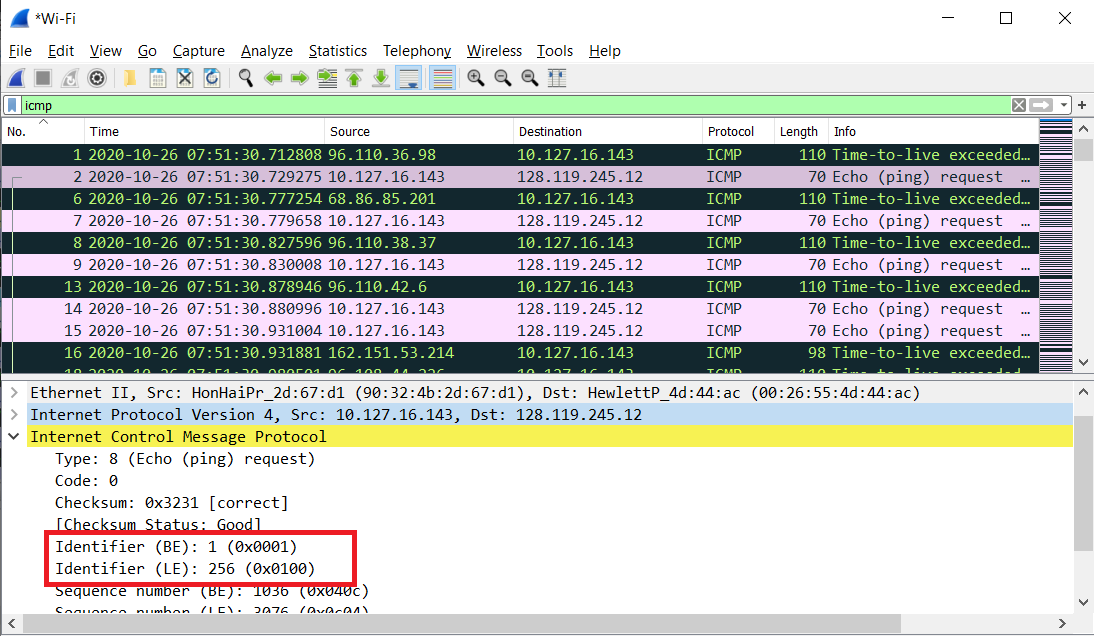
1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?



* The IP address of my computer is: 10.127.16.143

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

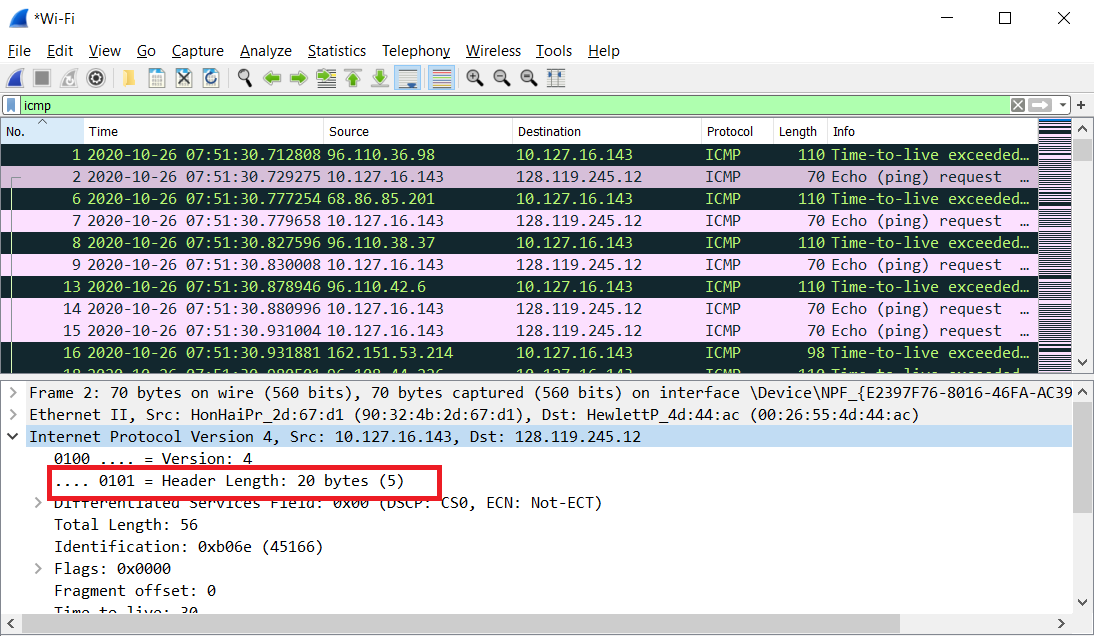
* The value in the upper layer protocol field is: ICMP (0x0100)



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.

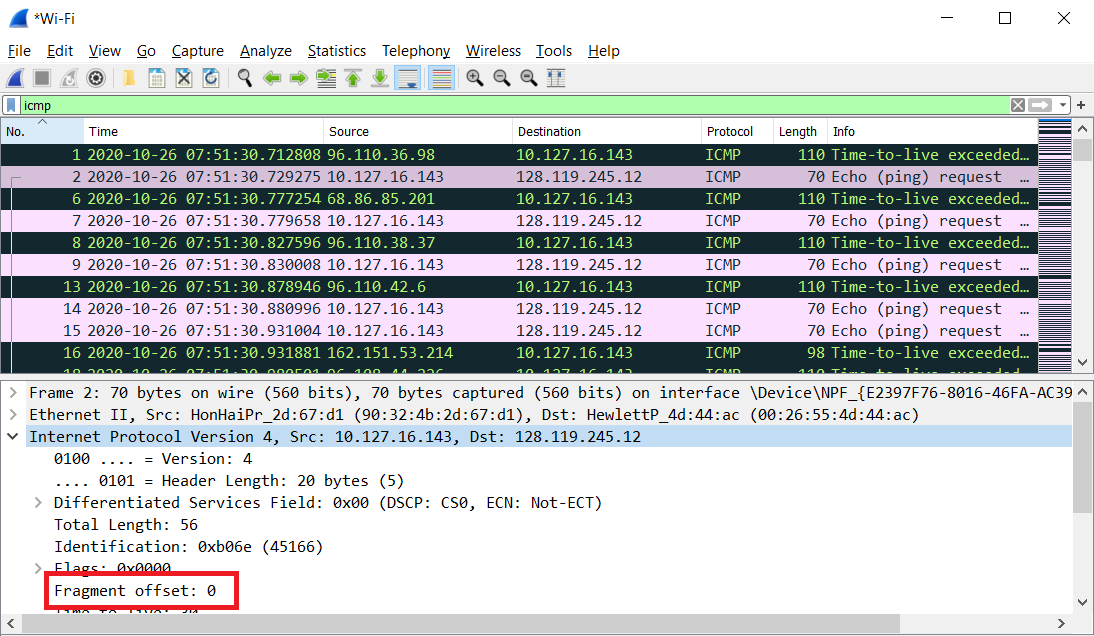
* There are 20 bytes in the IP header.There are 36 bytes in the payload of the IP datagram. Because we were sending a packet of 56 bytes.



1. Has this IP datagram been fragmented? Explain how you determined whether or

not the datagram has been fragmented.

* This IP datagram has not been fragmented because the Fragment offset is 0.



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 header checksum, Identification and Time to live changes from each datagram to the next.

1. Which fields stay constant? Which of the fields must stay constant? Which fields

must change? Why?

Fields that stay constant:

* Version (IPv4)
* Header length (always using IPv4)
* Source IP (sending from same place)
* Destination IP (contacting same site)
* Upper layer protocol (always using ICMP)

Fields that must stay constant:

* Version (IPv4)
* Header length (always using IPv4)
* Source IP (sending from same place)
* Destination IP (contacting same site)
* Upper layer protocol (always using ICMP)

The fields that must change are:

* The header checksum (header changes)
* Identification (to verify packets)
* Time to live (traceroute works)

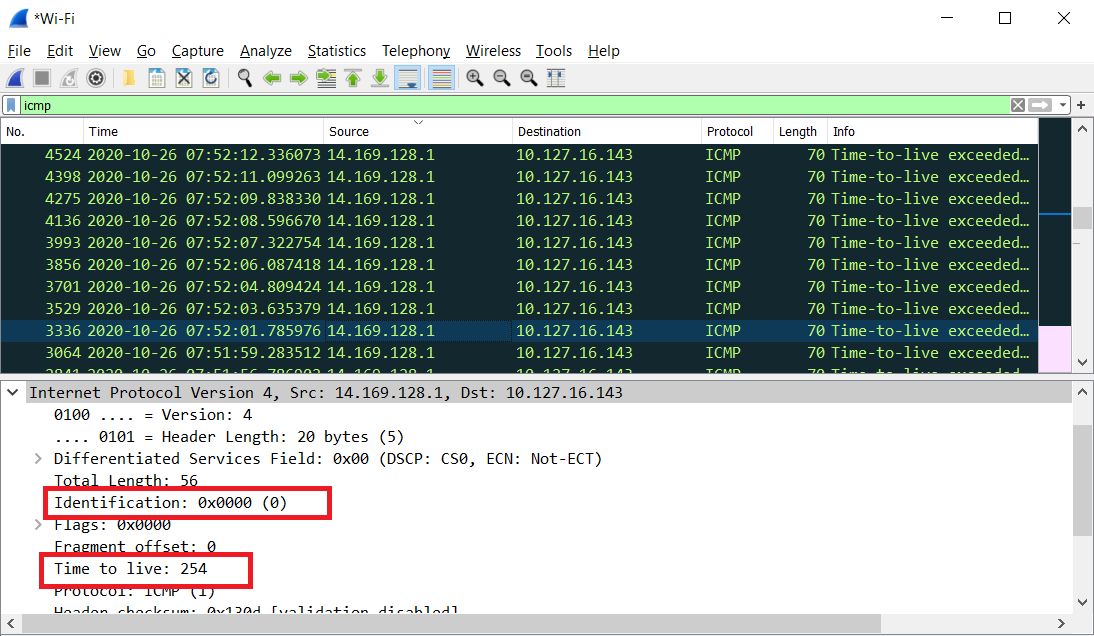
1. Describe the pattern you see in the values in the Identification field of the IP

datagram

* The pattern in the values in the Identification field of the IP datagram increase by 1 in each echo request.

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

* The value in the Identification field: 0x0000 (0)
* The value in the Time to live field: 254



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?

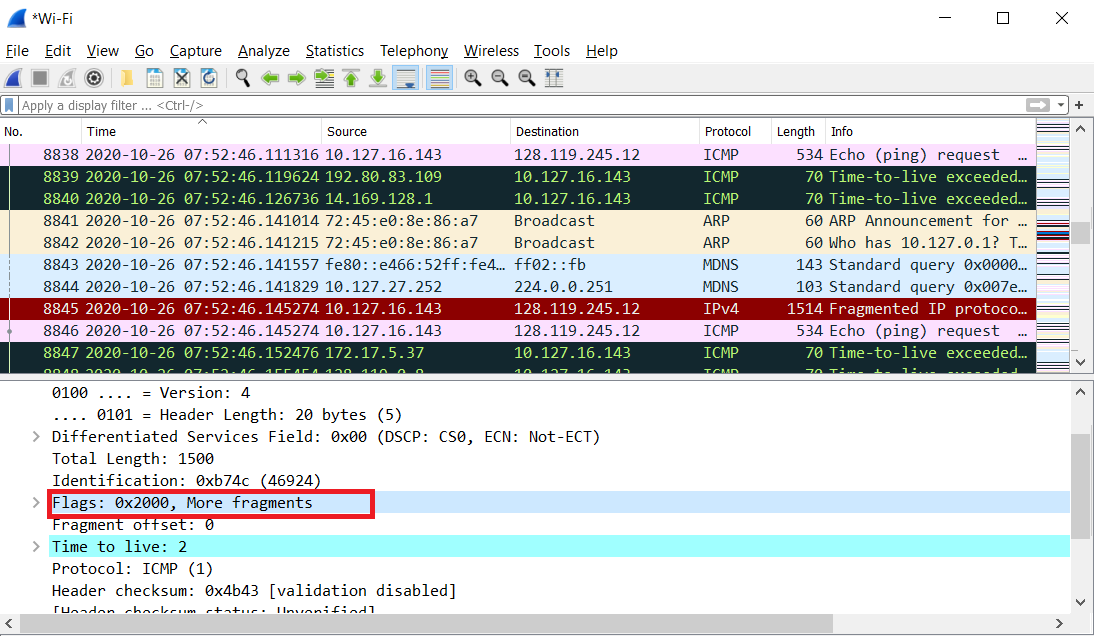
* The values remain unchanged for all of the ICMP TTL-exceeded replies sent to my computer by the nearest router. Because the time to live on the first hop router is always the same, and the Identification has the same value because the replies are fragments of a bigger packet.

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?

* The message has been fragmented across more than one IP datagram.



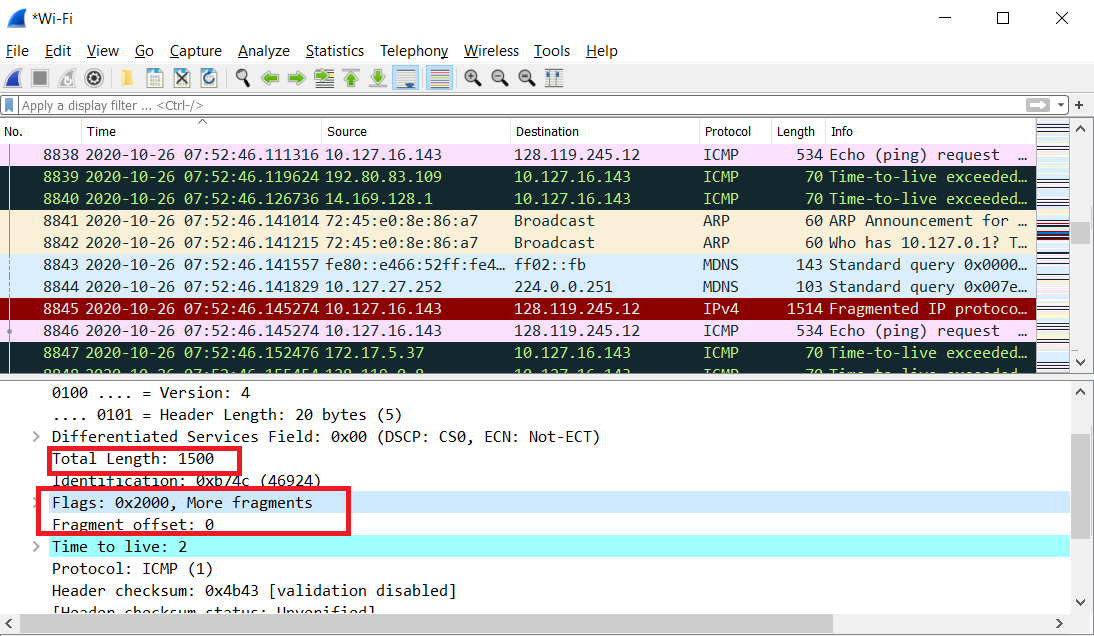
1. Print out the first fragment of the fragmented IP datagram. What information in

the IP header indicates that the datagram has 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?

* The fragment offset is set to 0 indicating that this is the first fragment rather than a later fragment where that value is set to (1480). The datagram has a total length of 1500.

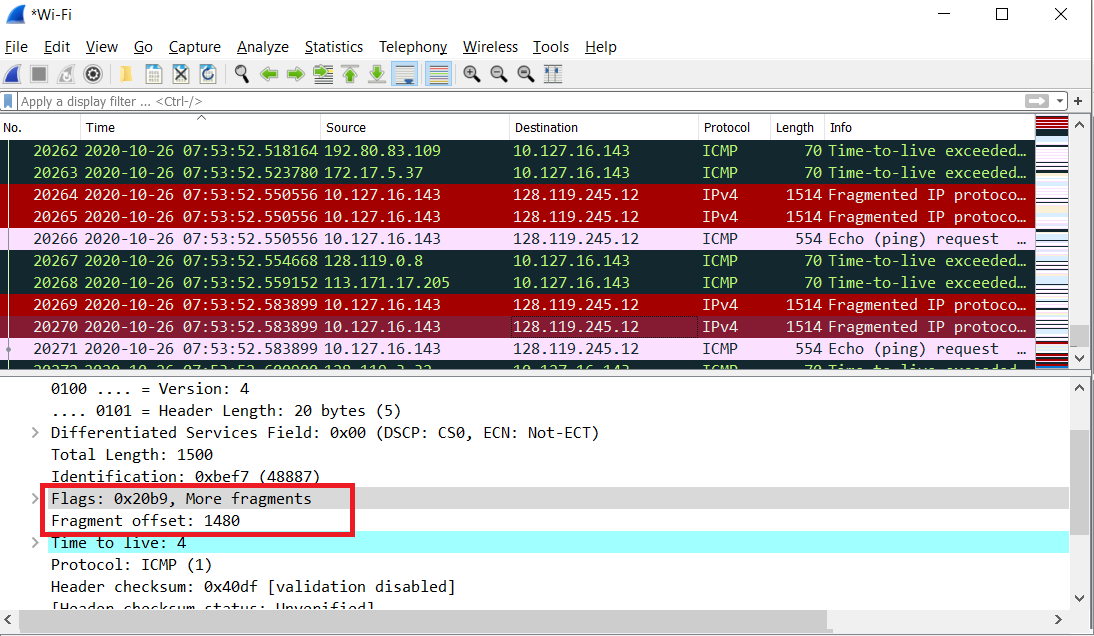


1. Print out the second fragment of the fragmented IP datagram. What information in

the IP header indicates that this is not the first datagram fragment? Are the more

fragments? How can you tell?

* The second fragment is obvious because it now has a fragment offset of 1480. There are no more fragments because it no longer has a flag set for more fragments.



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

The fields that change are

* Length
* Flags Set
* Fragment offset
* header checksum

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

* After switching to 3500 bytes, 3 fragments are created.

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

* The fields that change are the fragment offset (0, 1480, 2960) and checksum. The first 2 packets also have lengths of 1500 and more fragments flags set, while the last fragment is shorter (540) and does not have a flag set.