HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY

FACULTY OF COMPUTER SCIENCE AND ENGINEERING

COURSE: COMPUTER NETWORK

LAB 1: INTRODUCTION OF WIRESHARK PACKET SNIFFER TOOL

Supervisor : Nguyễn Lê Duy Lai.

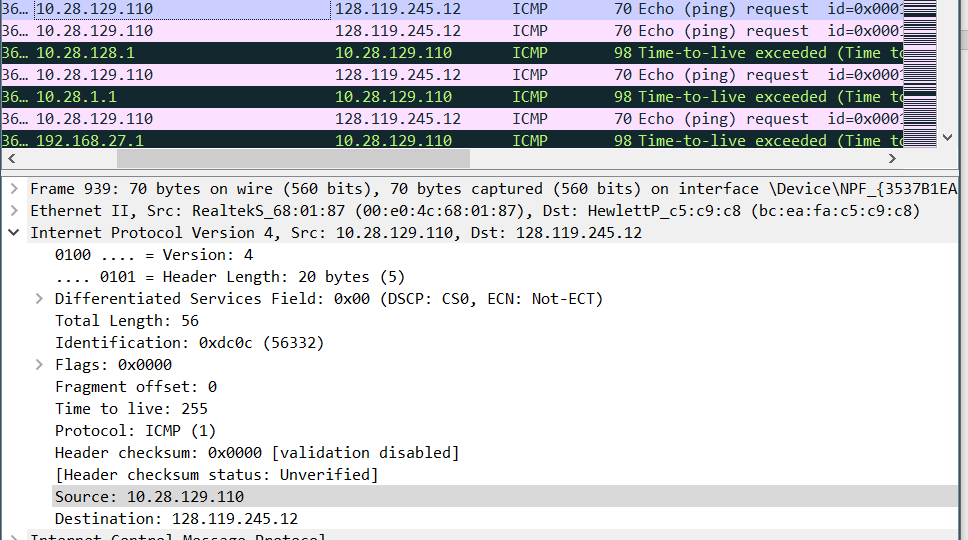
Author : Nguyễn Quang Long.

ID : 1812917.

Monday, October 05th , 2020

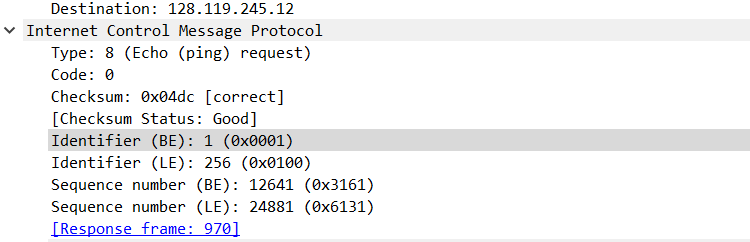
1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

* Answer: my IP is 10.28.129.110



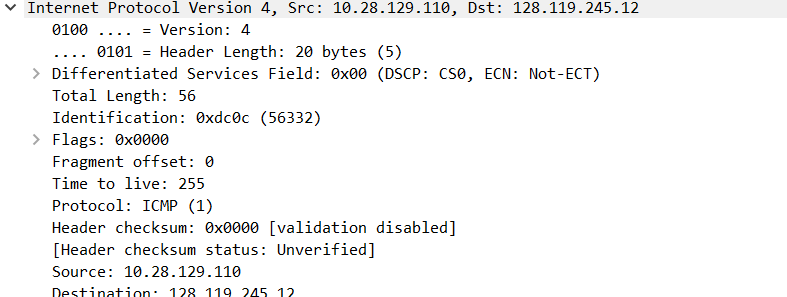
1. Within the IP packet header, what is the value in the upper layer protocol field?

* Answer : it’s 1.

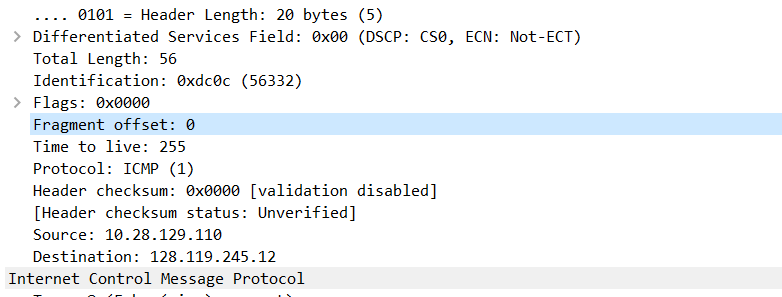


1. How many bytes are in the IP header? How many bytes are in the payload of theIP datagram? Explain how you determined the number of payload bytes.

* Answer: it’s 20 bytes. ‘Cause the total length is 56 and the header is 20 so the payload would be 36.



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

* Answer: it hasn’t been fragmented ‘cause 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?

* **Answer**: they are *identification* and *header checksum , time to live*.

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

* **Answer**: *version,protocol,sourcce,destination,total length* are constant and must be constant. *Identification* must changes cause it is used to determine which of the datagrams are actually fragments of the same larger datagram

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

* Each IP datagram’s identifier is plus one of its previous

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

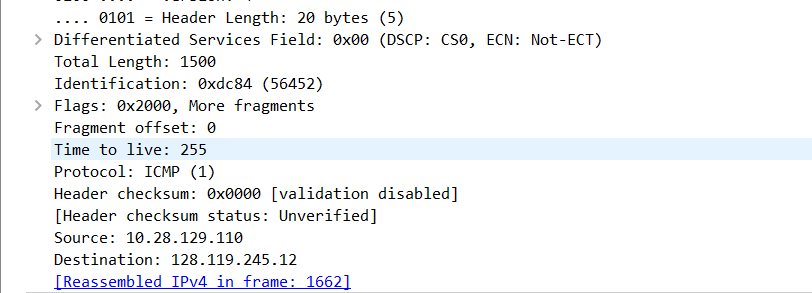
* As you can see in figure 1, the value in the Identification field is 56332 and it TTL is 255

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 changed.

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?

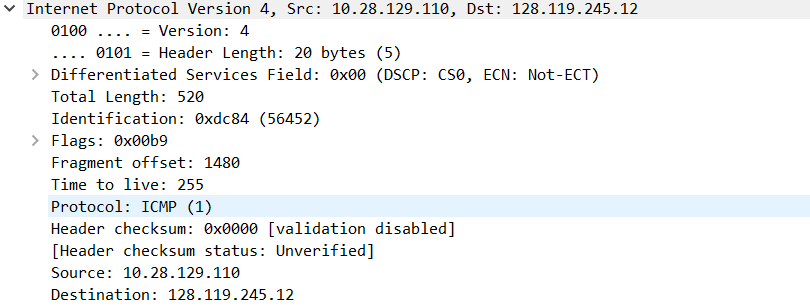
* Answer: yes, it has been fragmented. (notice the fargment flag field in figure 2.)



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?

* Answer: the fragment flag indicates that the datagram been fragmented. The fregment offset indicates whether this is the first fragment versus a latter 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 the more fragments? How can you tell?

* Answer: the fragment offset is not 0 so it ‘s not the first fragment. There is no more fragment left because the flag didn’t say that it would be more.

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

* Answer: they are *total length,flags,fragment offset,checksum.*

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

* Answer: 3 fragments was created from the original datagram.

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

* Answer: they are flag, fragment offset,checksum.