HACETTEPE UNIVERSITY

DEPARTMENT OF
COMPUTER ENGINEERING

BBM453: Computer Networks Laboratory
Lab 5-6: IP ICMP

Author
Kayla AKYÜZ
21726914
Batuhan ÖZTÜRK
21827742

Advisors
T.A. Tuğba ERDOĞAN
tugba.gurgen@hacettepe.edu.tr
Assoc. Prof. Sevil ŞEN
ssen@cs.hacettepe.edu.tr

Group 14
Source IP : 192.168.0.27

Nov 18,2021

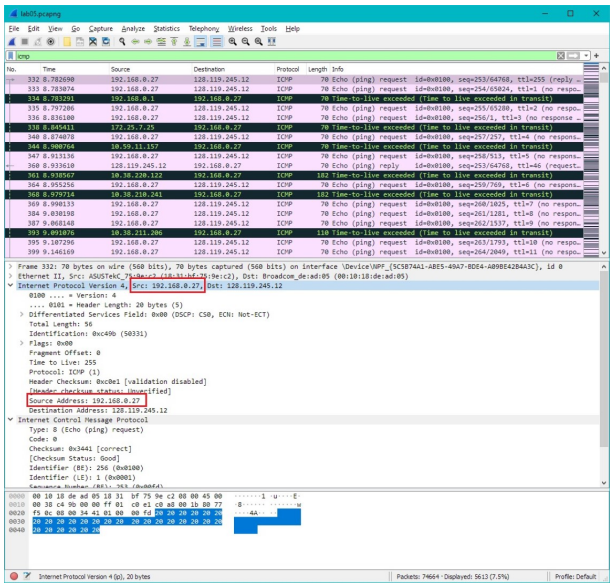
SOLUTIONS

IP

A look at the captured trace

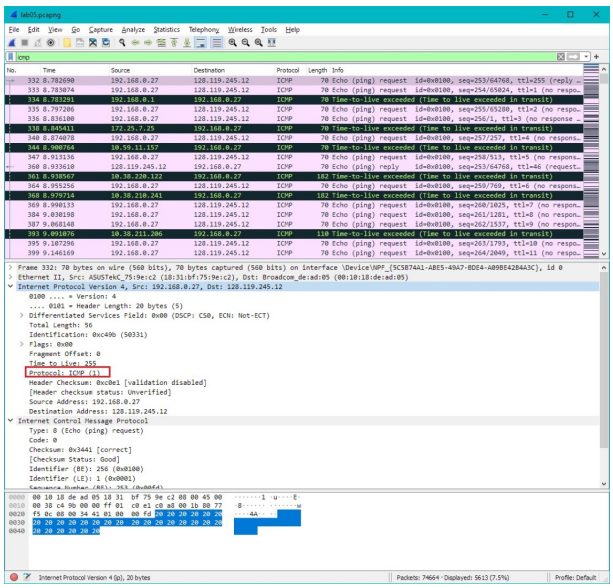
1. What is the IP address of your computer?

The IP address of our computer is: 192.168.0.27



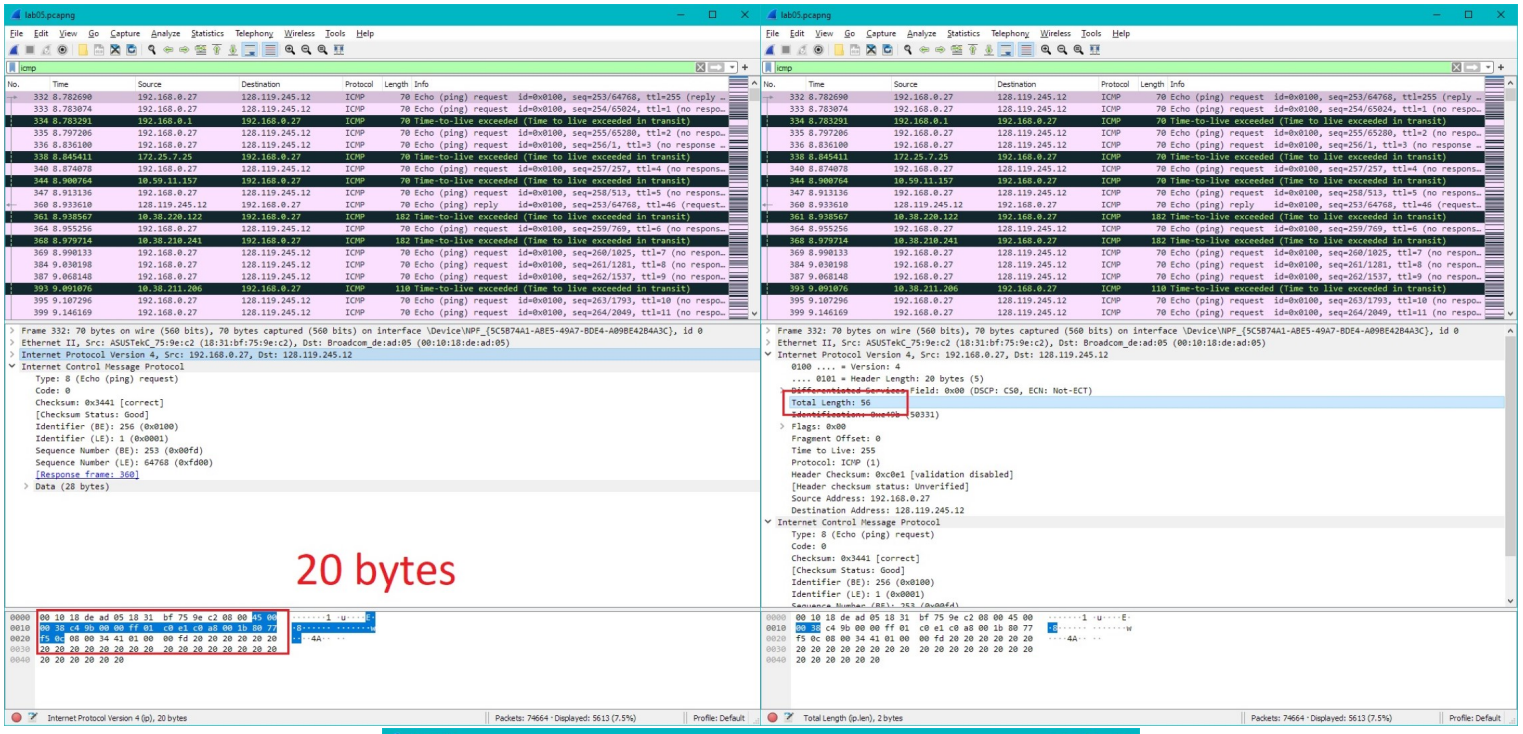
2. Within the IP packet header, what is the value in the upper layer protocol field?

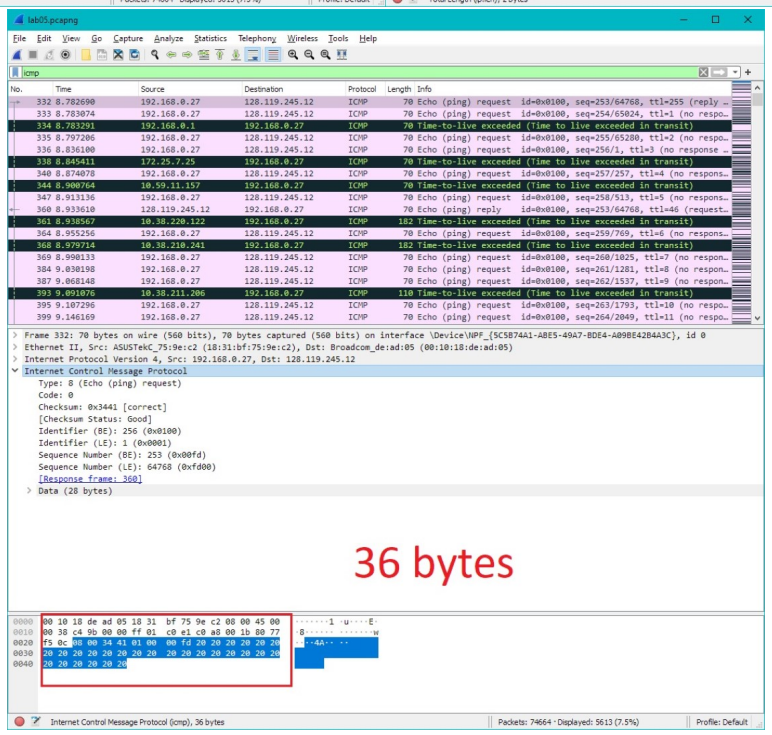
The value in the upper layer protocol field is: ICMP (0x01)



3. 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.

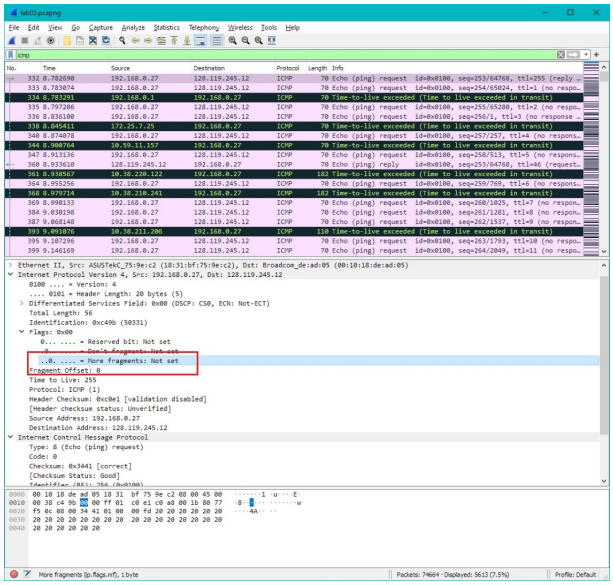
IP header is 20 bytes. We know the total length is 56 by checking length header. This makes payload 36 bytes also we can brute count payload to be 36 bytes.





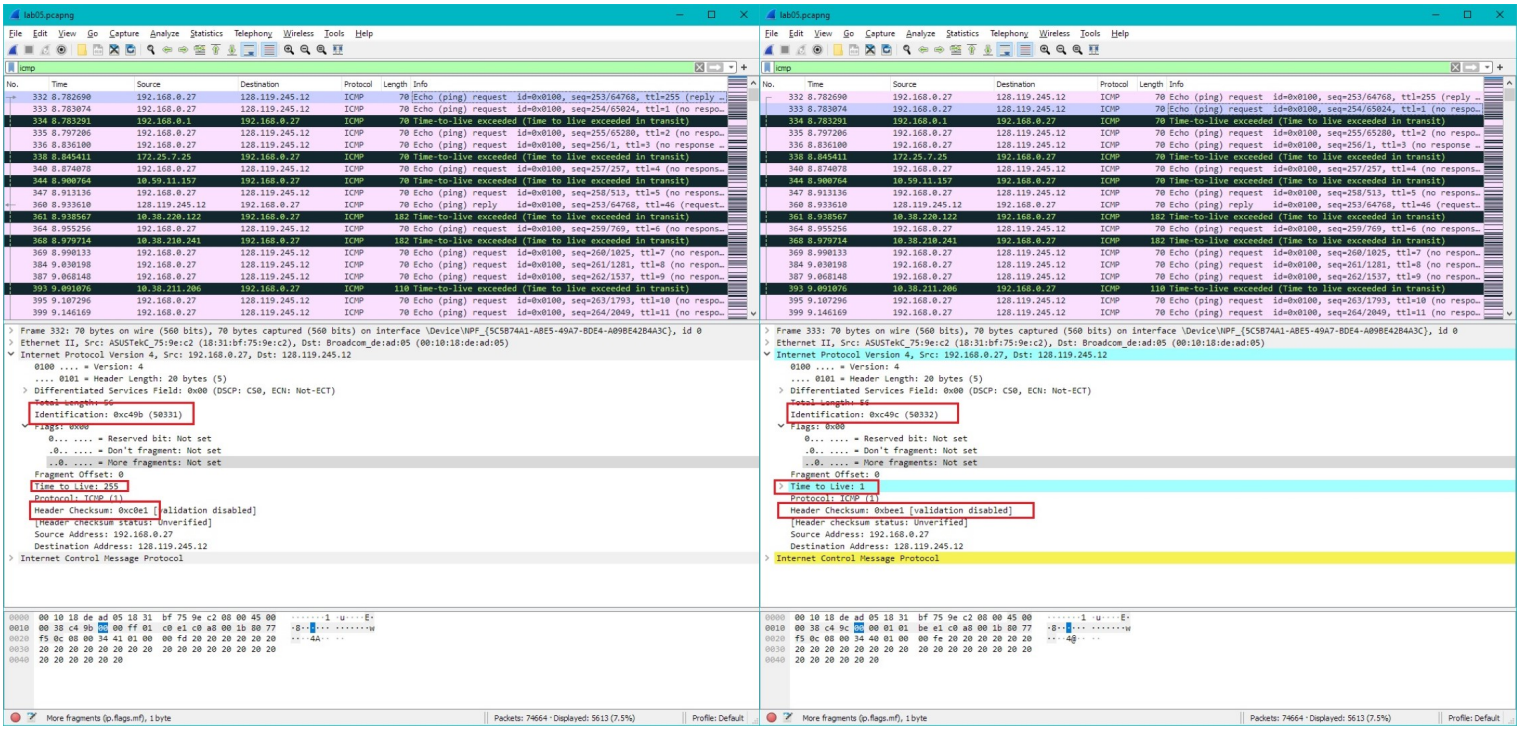
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

It seems datagram is not fragmented. We can check the flag more fragments is 0.



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

As we can see from below comparison the identification and time to live fields seems to be incrementing and also header checksum seems to be changing from one datagram to the next.



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

The fields that stay constant are:

- Version - We are using IPv4 for all packets so it will not change
- Header Length - Did not change since we are using same type of packets
- Total Length - Did not change since we are using same type of packets
- Source IP - Did not change since we are sending from the same source IP
- Destination IP - Did not change since we are sending to the same destination IP
- Differentiated Services - Did not change since we are using same protocol
- Upper Layer Protocol - Did not change since we are using same protocol
- Fragment Flags - Did not change since we had no fragmentation

The fields that must stay constant are:

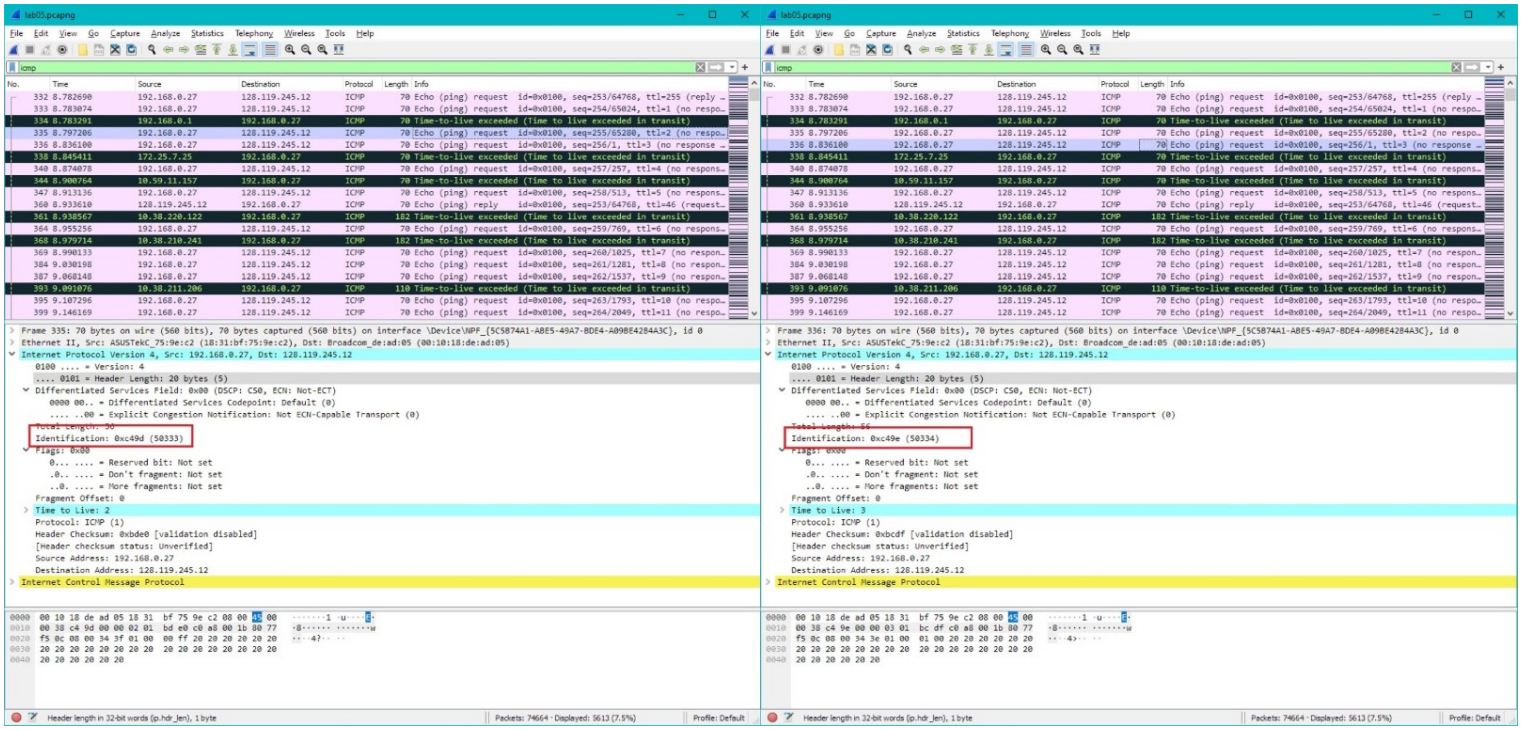
- Version - We are using IPv4 for all packets so it will not change
- Header Length - Should not change since we are using same type of packets
- Source IP - Should not change since we are sending from the same source IP, connection must be constant
- Destination IP - Should not change since we are sending to the same destination IP, connection must be constant
- Differentiated Services - Should not change since we are using same protocol
- Upper Layer Protocol - Should not change since we are using same protocol

The fields that must change are:

- Identification - Each IP datagram must have different ID
- Time to Live - Each packet has different length of route
- Header Checksum - Checksum changes according to header

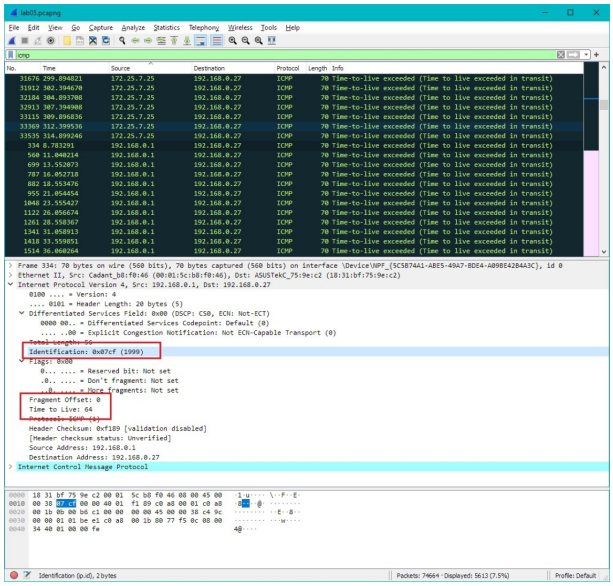
7. Describe the pattern you see in the values in the Identification field of the IP datagram

The Identification field of the IP datagram seems to be incrementing by one at each ICMP Echo (ping) request as we mentioned in question 5.



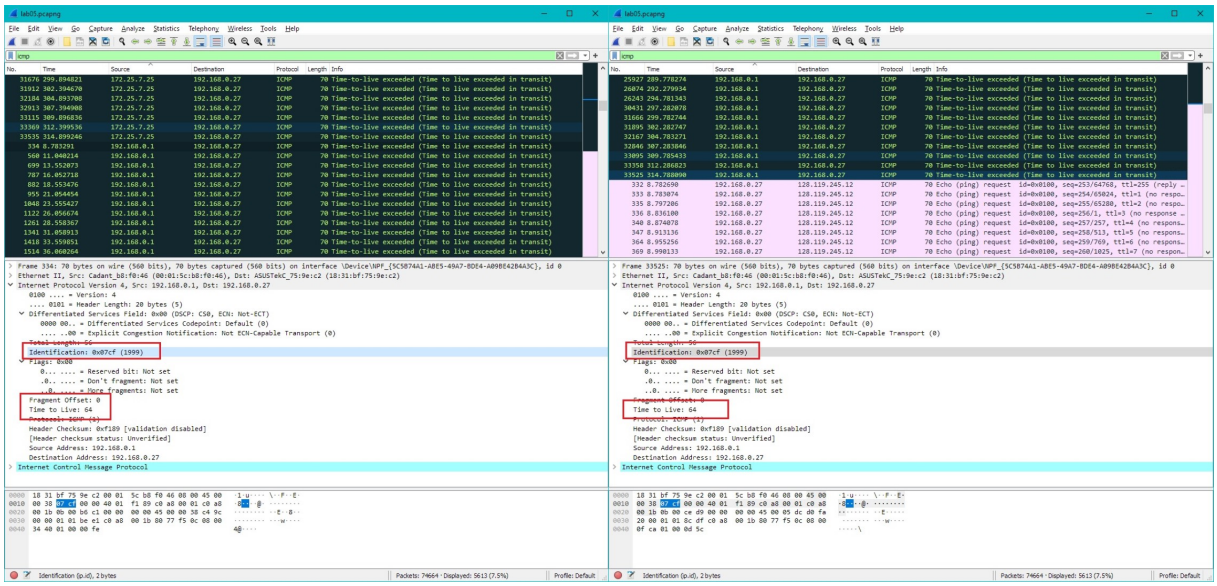
8. What is the value in the Identification field and the TTL field?

Our nearest first hop router is "192.168.0.1". Inspecting the fields we see "Identification: 0x07cf (1999)" and "Time to Live: 64".



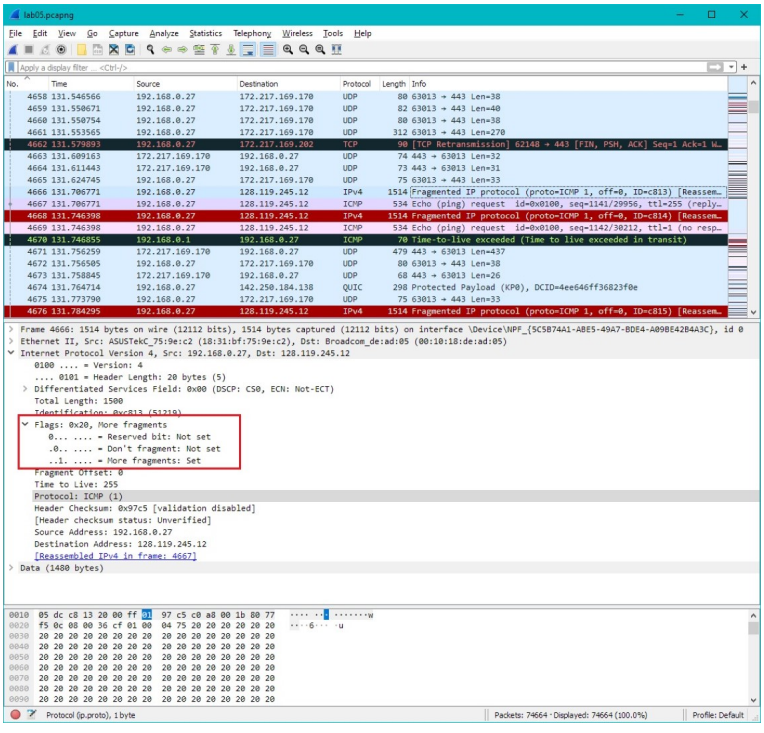
9.Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

The TTL field remain unchanged because replies are sent by the same, nearest router. The Identification field should change since it is unique value for datagram unless the datagrams are fragments of the same datagram. In our test results the Identification field was same for all of the replies from "192.168.0.1". However in the traces shared from document it changed.



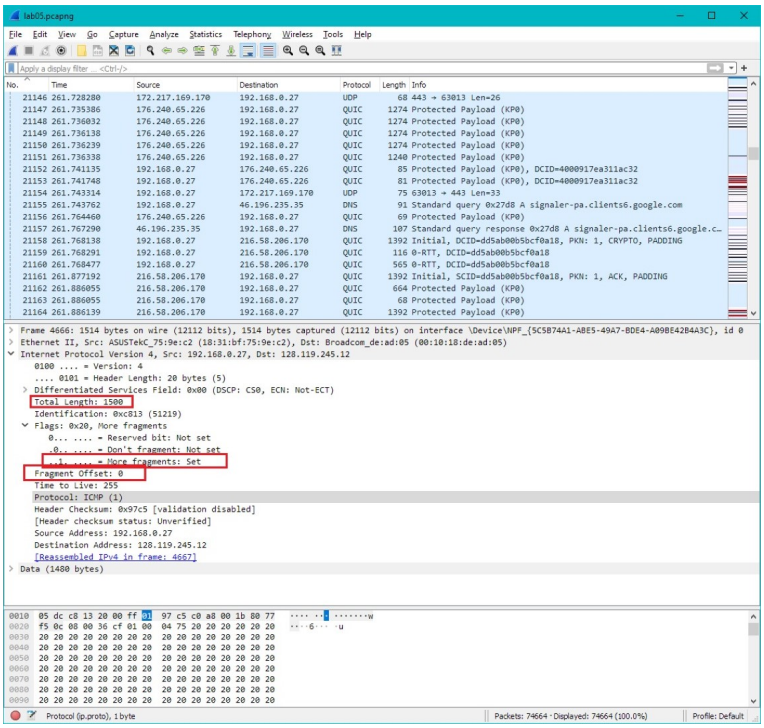
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

Yes it is as we can see in the screenshot below. The flags are set.



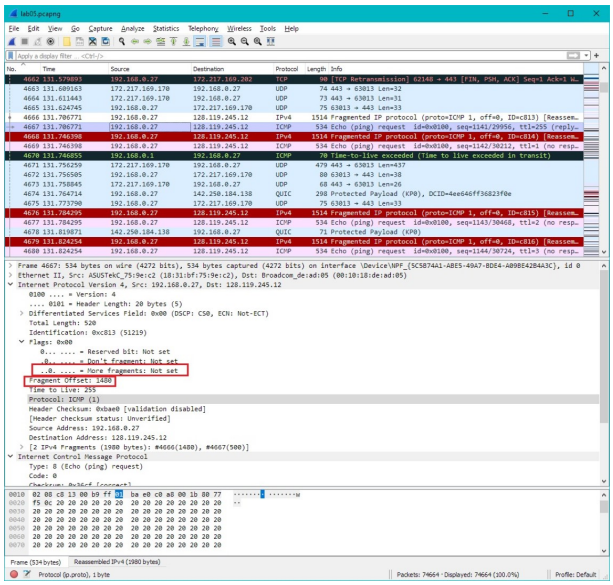
11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

The more fragments flag is set. Offset is 0 so we know it is the first fragment. It's length is 1500. See screenshot below for fields we check these.



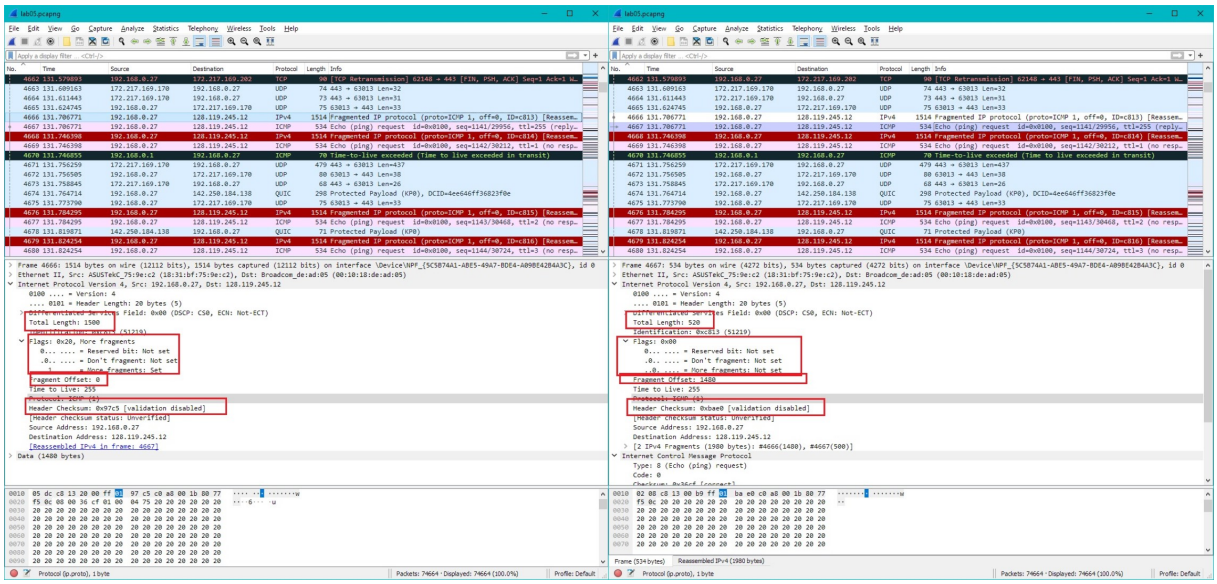
12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

The fragment offset is set meaning this is not the first datagram fragment. We check more fragments flag and it is not set meaning there won't be fragments any more.



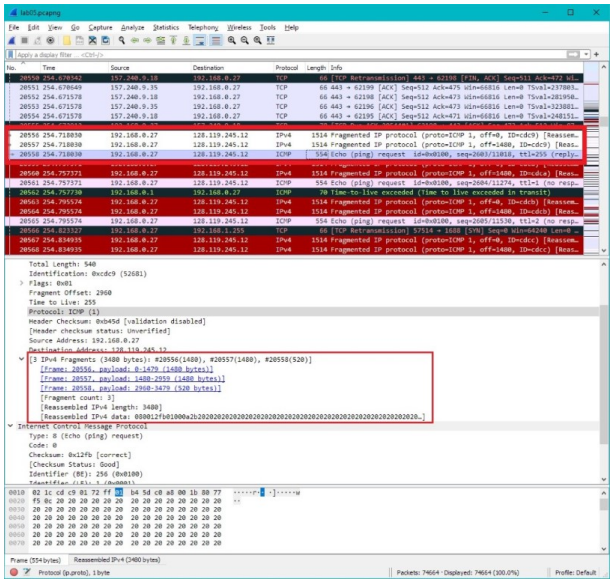
13. What fields change in the IP header between the first and second fragment?

As we can see from comparison below the flag, total length, fragment offset and header checksum changes. Flag changes since there is more fragments for the first one and since second one is the last one. Total length also changes since first one uses max length while second one does not. Fragment offset must always change when we are going upper in fragments. And header checksum changes since these header data is changing.



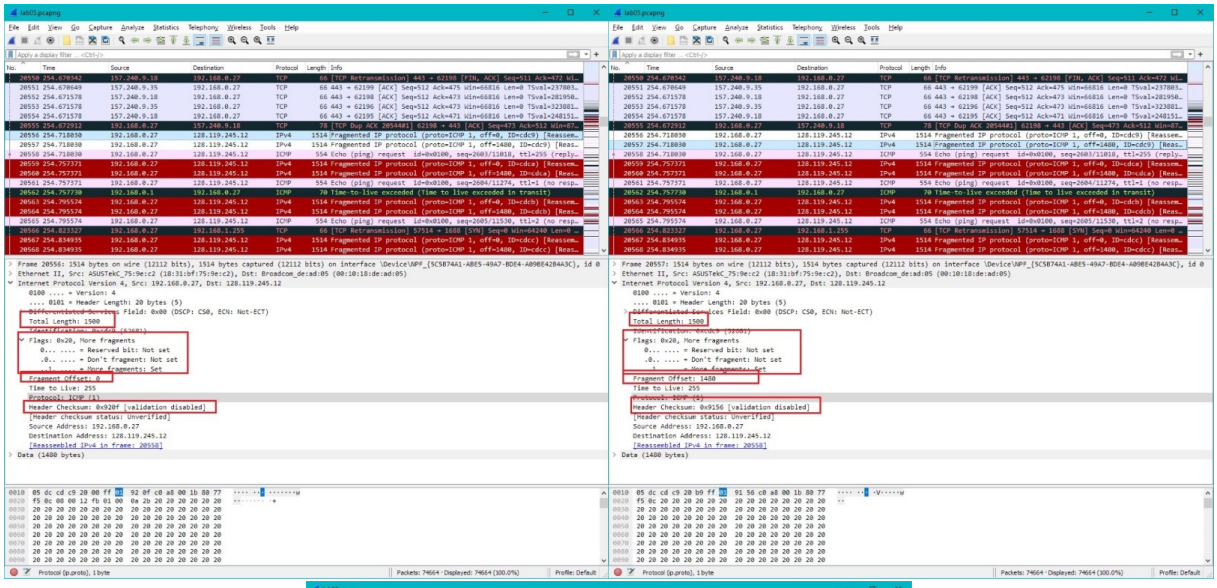
14. How many fragments were created from the original datagram?

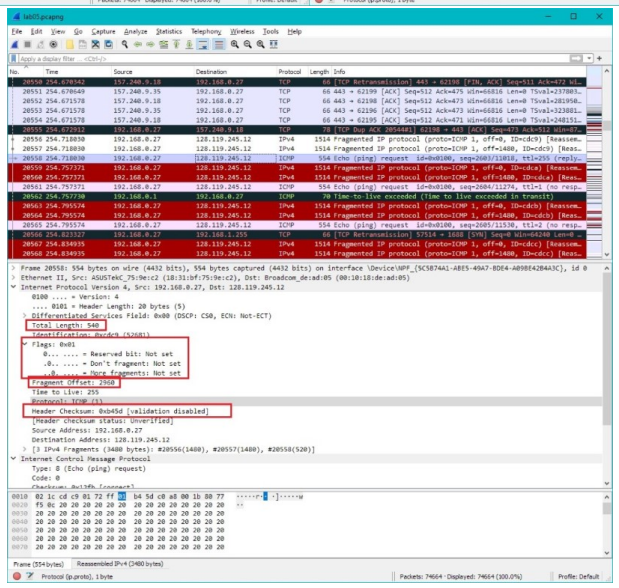
3 fragments were created. This is because maximum size is 1500 and in order to do 3500 we need 3 fragments.



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

From first fragment to second fragment only the fragment offset and the header checksum changes. The total length field does not change since the max length used in both and since they both have more fragments the flag seems to be same. Offset always increases, logically, between fragments of same datagram. And header checksum changes since header changes. From second to last fragment we also see the total length and flags change. Since there are no more fragments after the last fragment it is logical that the flag will change and since last fragment does not use max length the length changes.



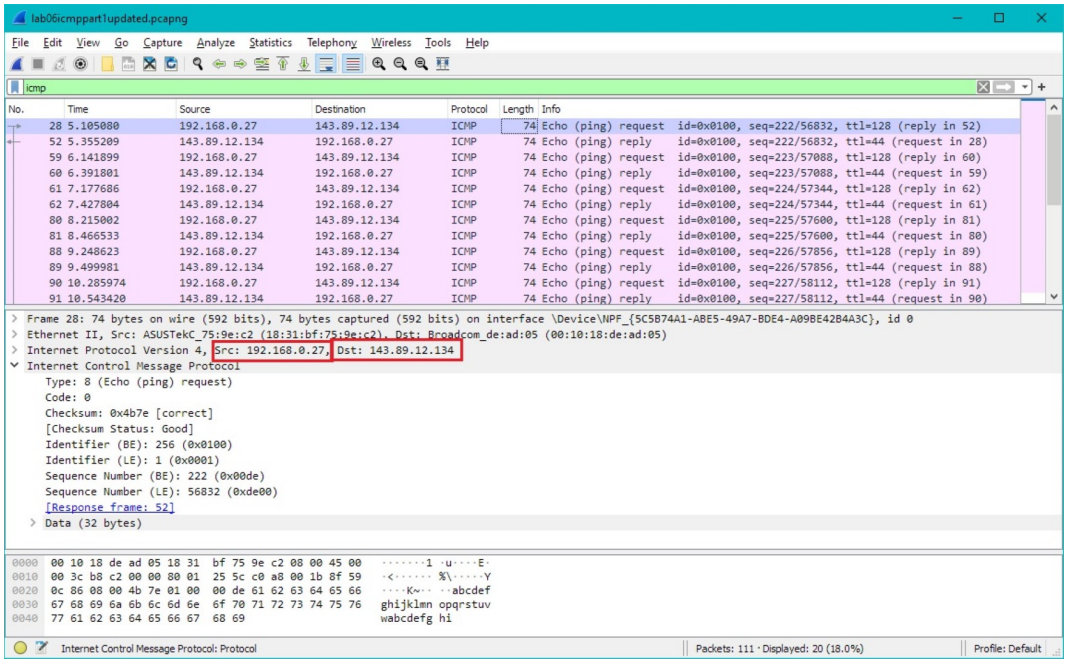


ICMP

ICMP and Ping

1. What is the IP address of your host? What is the IP address of the destination host?

The IP address of our host is: 192.168.0.27 , IP address of the destination host is: 128.119.245.12

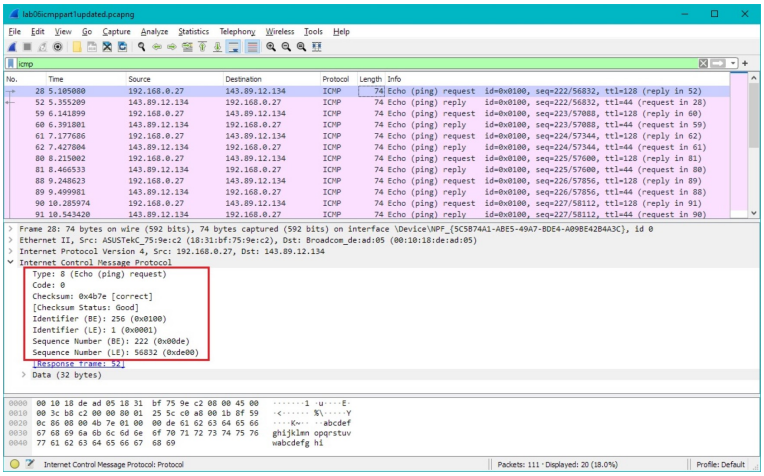


2. Why is it that an ICMP packet does not have source and destination port numbers?

The ICMP packet is transferred in network layer thus do not have port number. Reason for this is the information we need is just that if the IP is connectable or not and this ICMP communication is implemented in network layer, it was not designed for application communication.

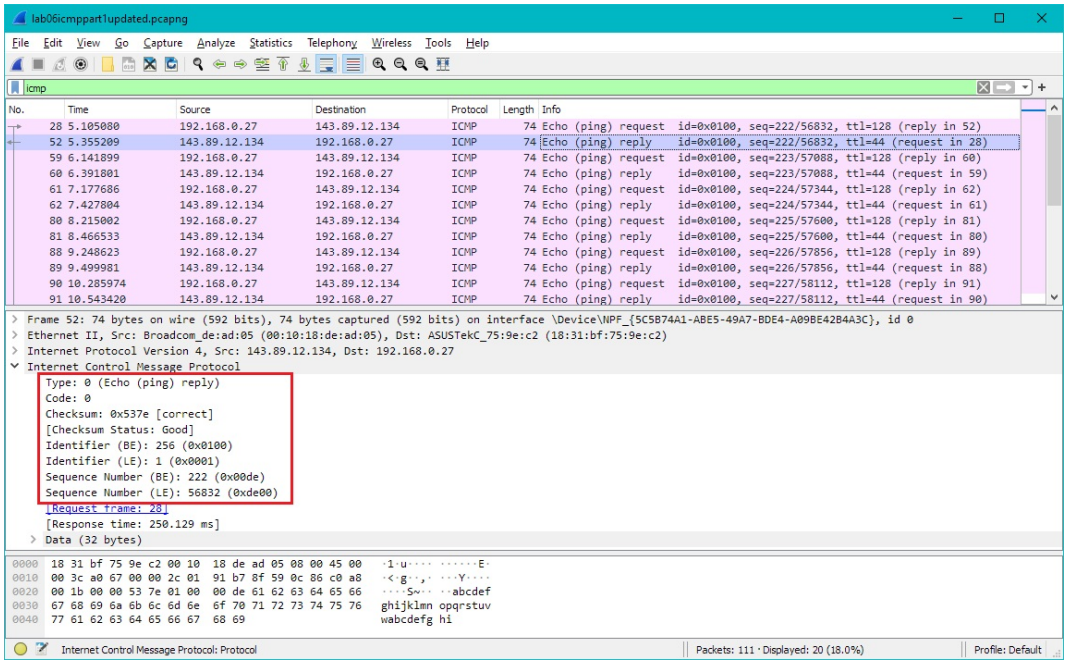
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

ICMP type is 8, code number is 0. The other fields seems to be "Checksum, Identifier (BE), Identifier (LE), Sequence number (BE), and Sequence number (LE)". BE and LE are big endian little endian of the same data. Each of the checksum, sequence number and identifier fields are 2 bytes long.



4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

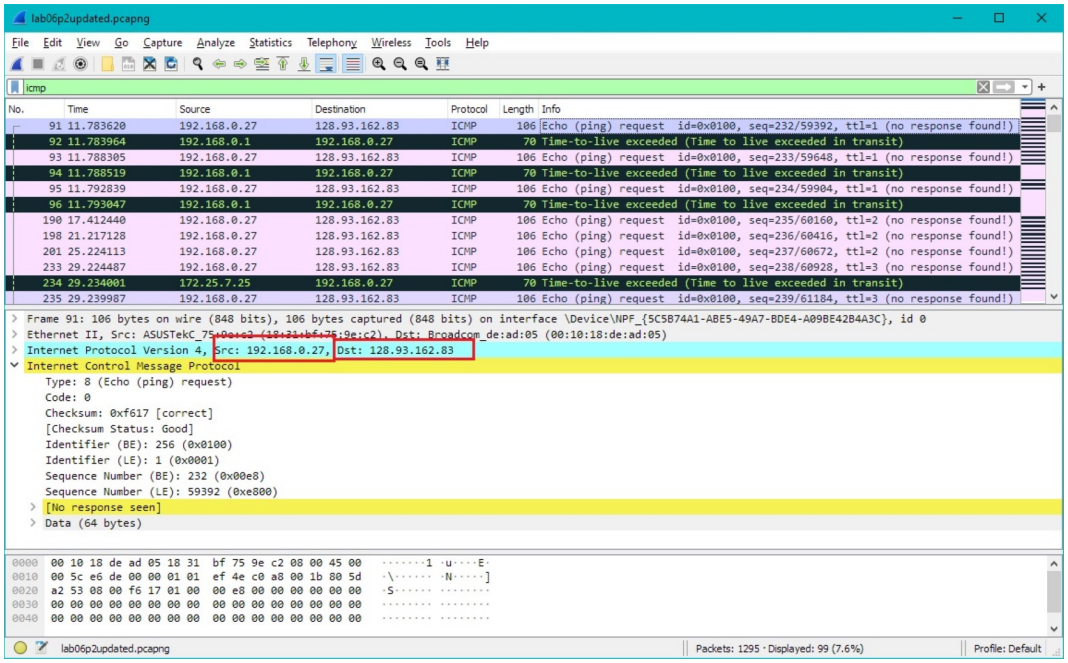
ICMP type is 0, code number is 0. The other fields seems to be "Checksum, Identifier (BE), Identifier (LE), Sequence number (BE), and Sequence number (LE)". BE and LE are big endian little endian of the same data. Each of the checksum, sequence number and identifier fields are 2 bytes long.



ICMP and Traceroute

5. What is the IP address of your host? What is the IP address of the target destination host?

The IP address of our host is: 192.168.0.27 , IP address of the destination host is: 128.93.162.83

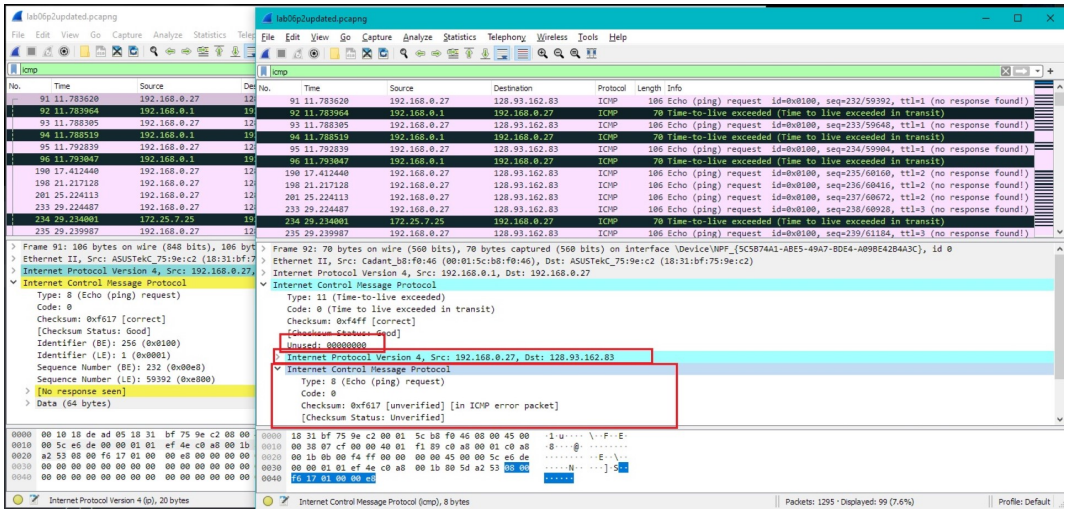


6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

No it would not be still 01, it would be 17 aka 0x11 instead, which identifies UDP layout.

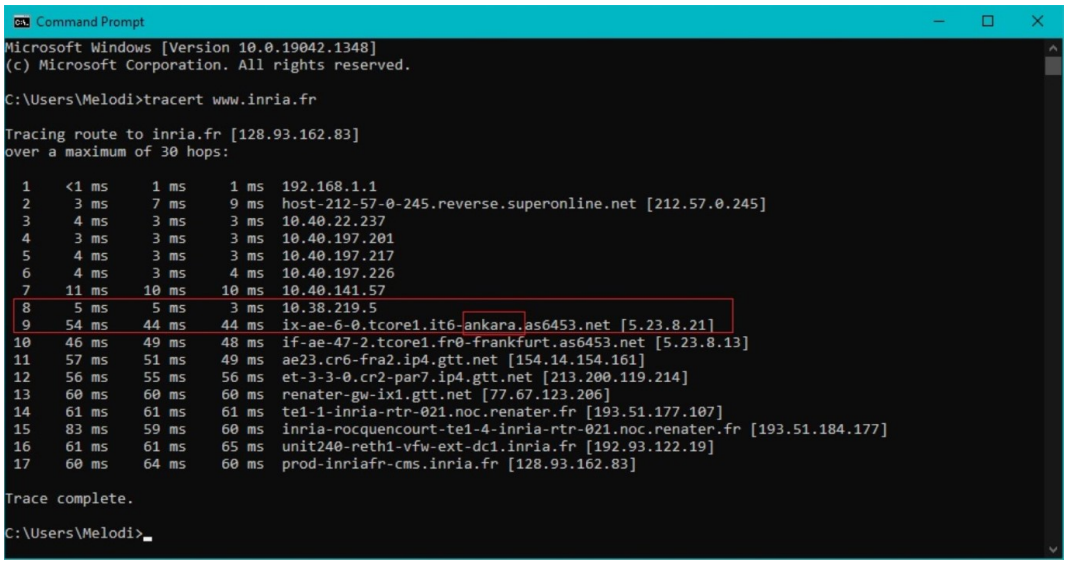
7. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

Comparing side by side we realize there are 3 differences. First one is "Unused: " header which is absent in echo packet and rest two are are data considering the original ICMP packet which is it's IP header and first 8 bytes.



8. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

Yes, with in our calculation the jump happens between link 8-9. Yes we can guess, it indicates Ankara. We guess jump happens while linking local to general. In the lab document Figure 4 the jump happens between link 9-10. The link 9 is in New York since it has "nyc" in the name and 10 seems to be from France and is transoceanic link.



REFERENCES

LaTex Tutorials
Assignment Paper 1
Assignment Paper 2
Wireshark FAQ
Wireshark User's Guide
ICMP vs UDP