**Wireshark Lab 2: ICMP**

**EEL 6935 (Spring 2019)**

**DATA NETWORKS, SYS & SECURITY**

 **PROJECT 2**

Department of Electrical Engineering

Under the Guidance of

**Prof Nasir Ghani**

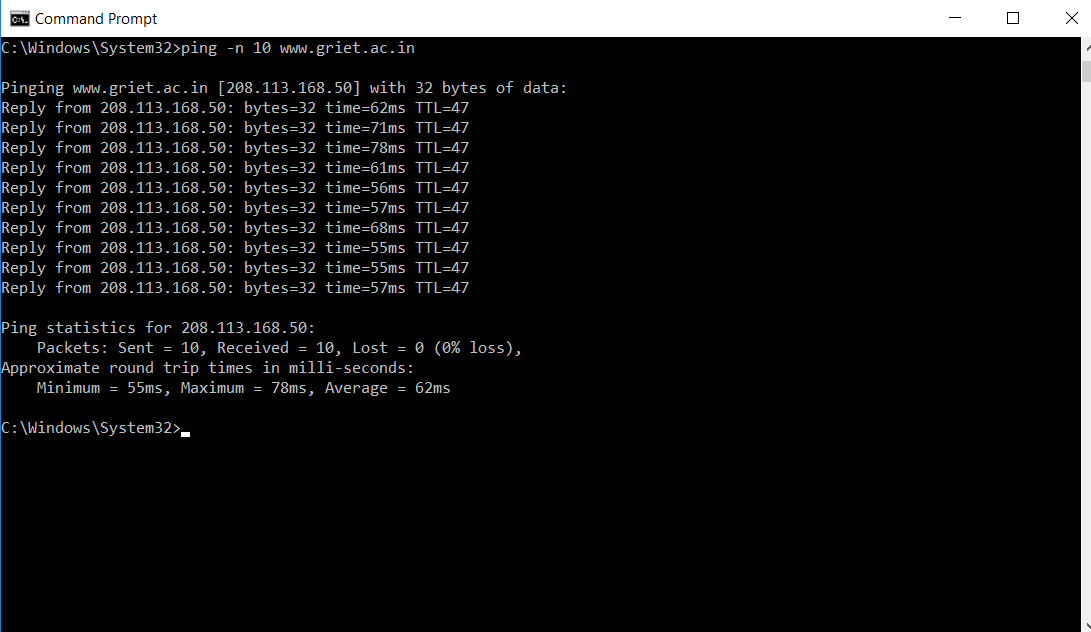
**Submitted by**

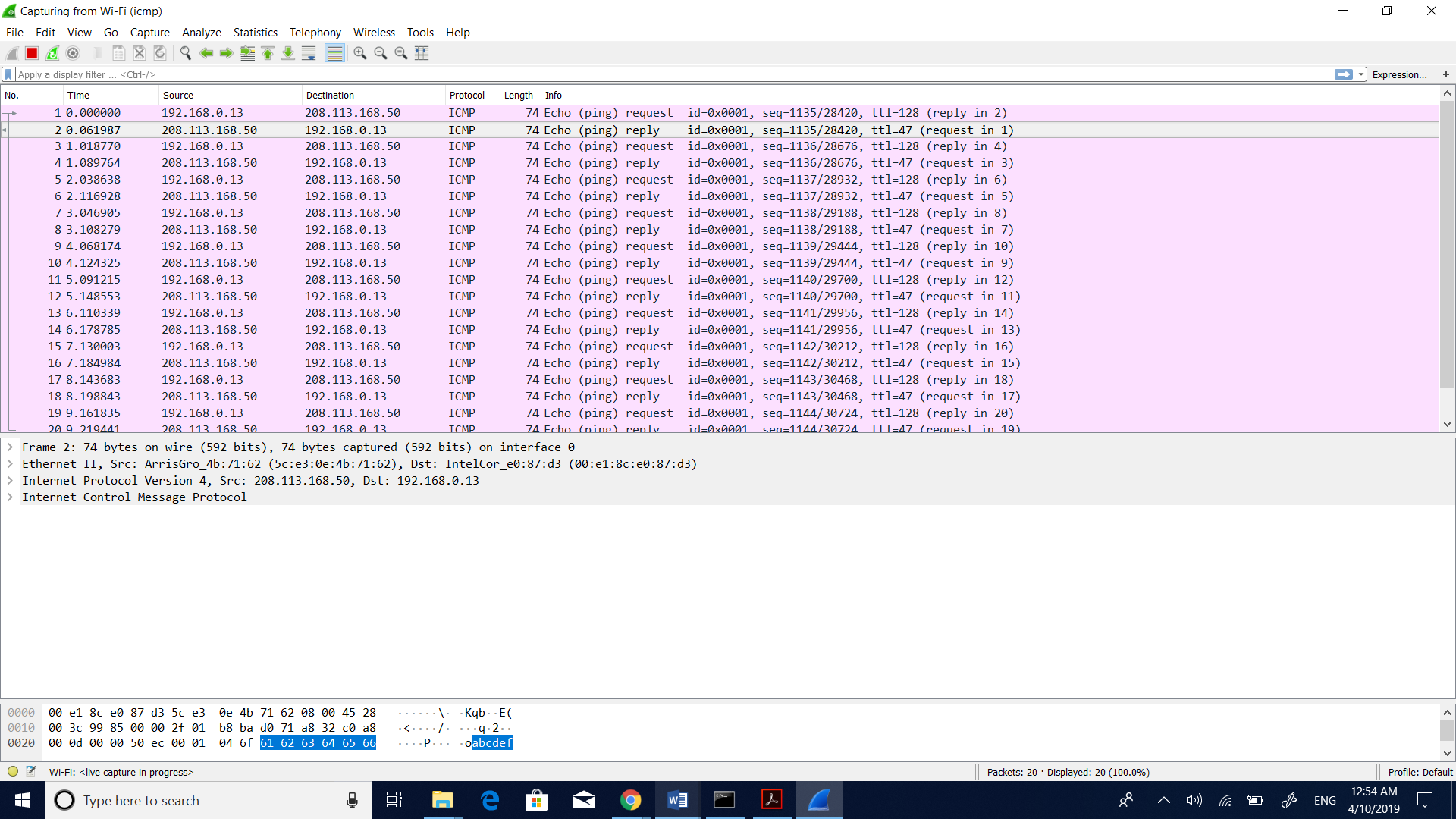
**SAI KRISHNA KANDAGATLA**

**U15974415**

**WIRESHARK LAB 2: ICMP**

**1) ICMP AND PING**

****

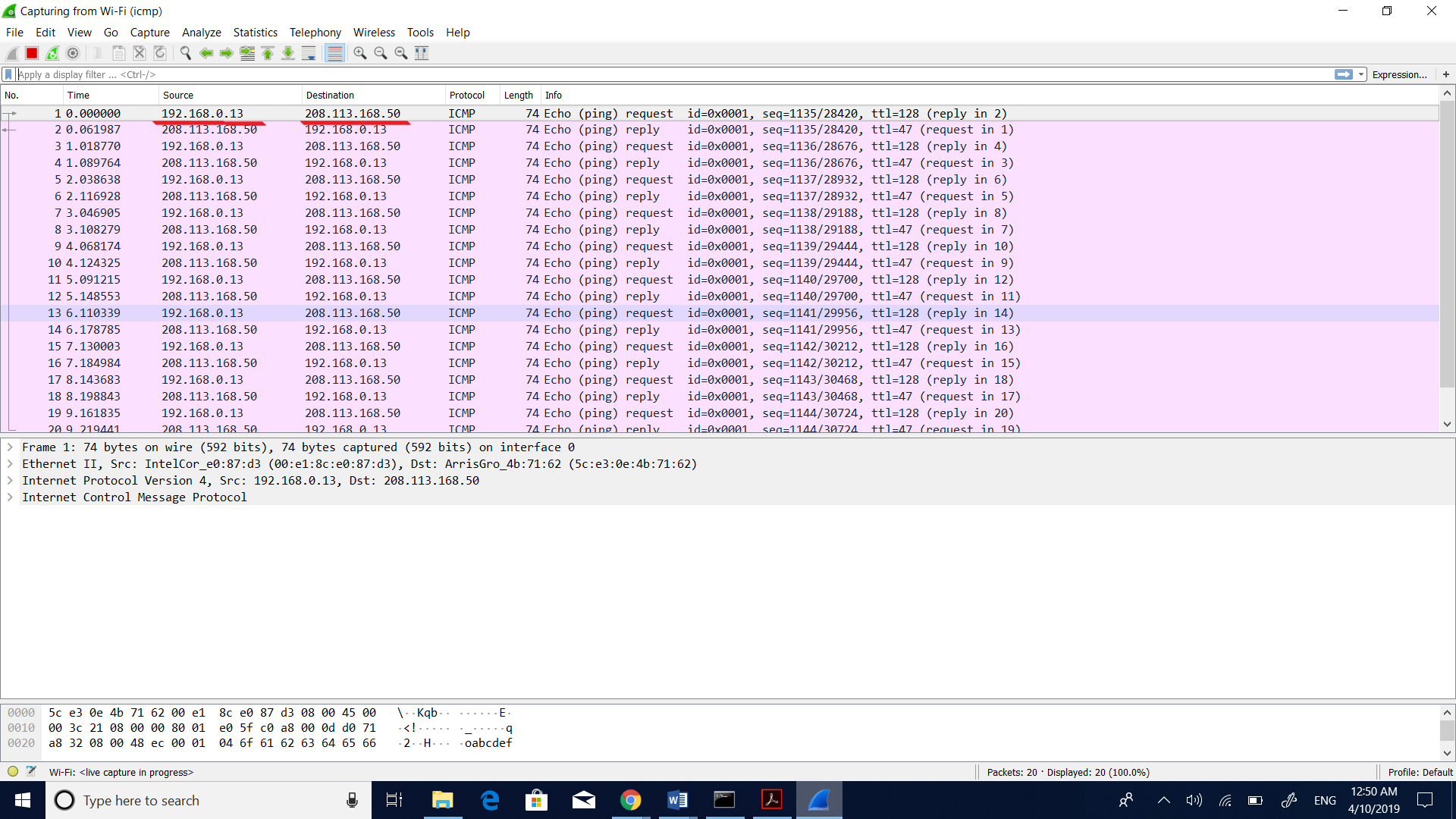


1) What is the IP address of your host? What is the IP address of the destination host?

**Solution:**

IP Address of the source host: **192.168.0.13**

IP Address of the destination host: **208.113.168.50**



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

**Solution:**

ICMP packet does not have packets because it has a network layer protocol not at all like TCP/UDP which has port numbers. The port numbers are utilized for transport layer and ICMP is a protocol which is combined in the IP Datagram. Additionally, it is utilized for communication of data between the hosts and routers. Each ICMP has a type and code parameters which recognizes the message received. We will not need port numbers to direct ICMP messages to application layer as the network software interprets all the ICMP messages.

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?

**Solution:**

ICMP Type:8

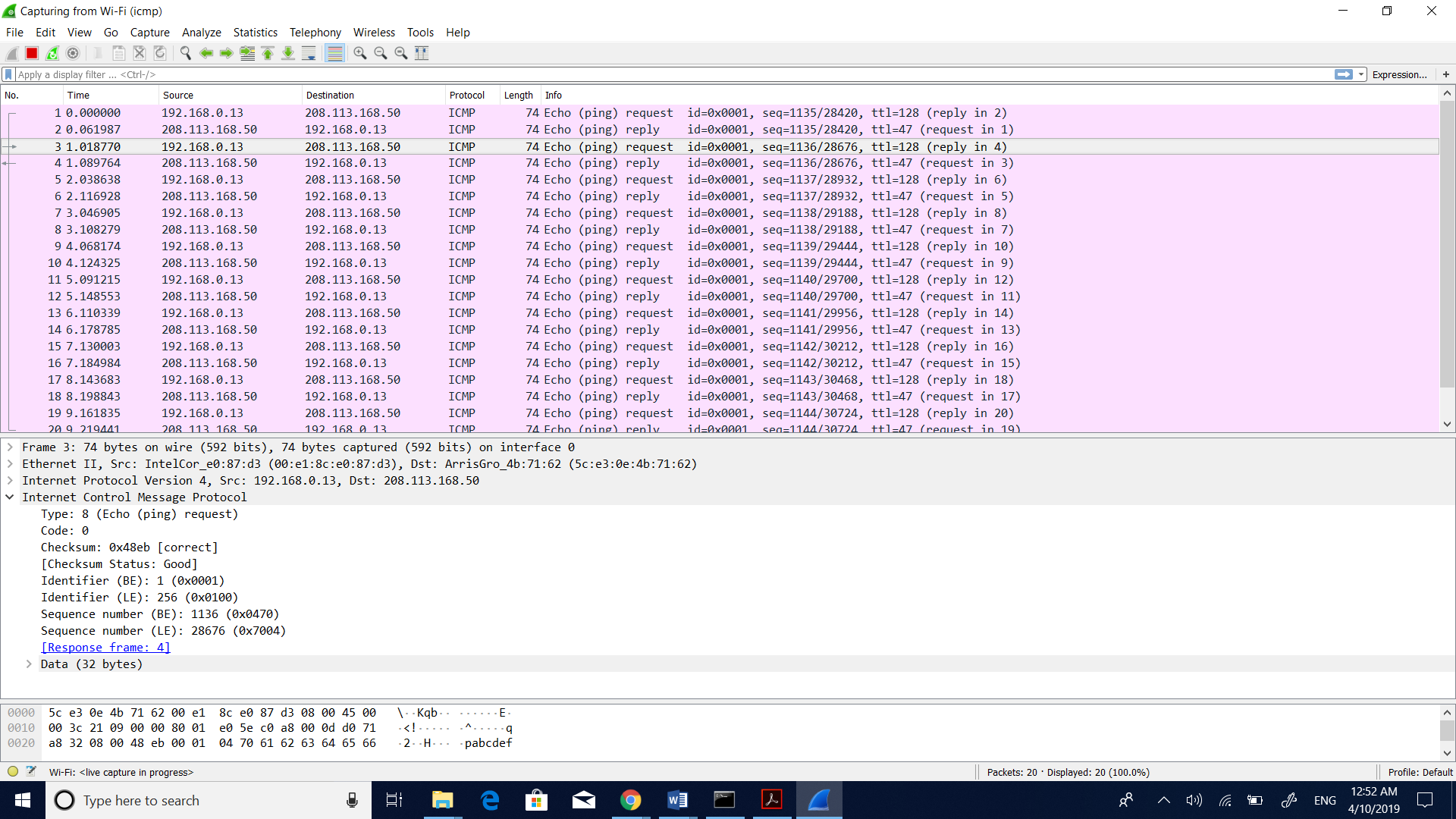
ICMP Code:0

Other fields: checksum, identifier (BE-0x0001)**,** identifier (LE-0x0100), sequence number (BE-0x0470)**,** sequence number (LE-0x7004).

Checksum: 2 bytes(0x48eb)

Sequence number: 2 bytes

Identifier: 2bytes



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?

**Solution:**

ICMP Type:0

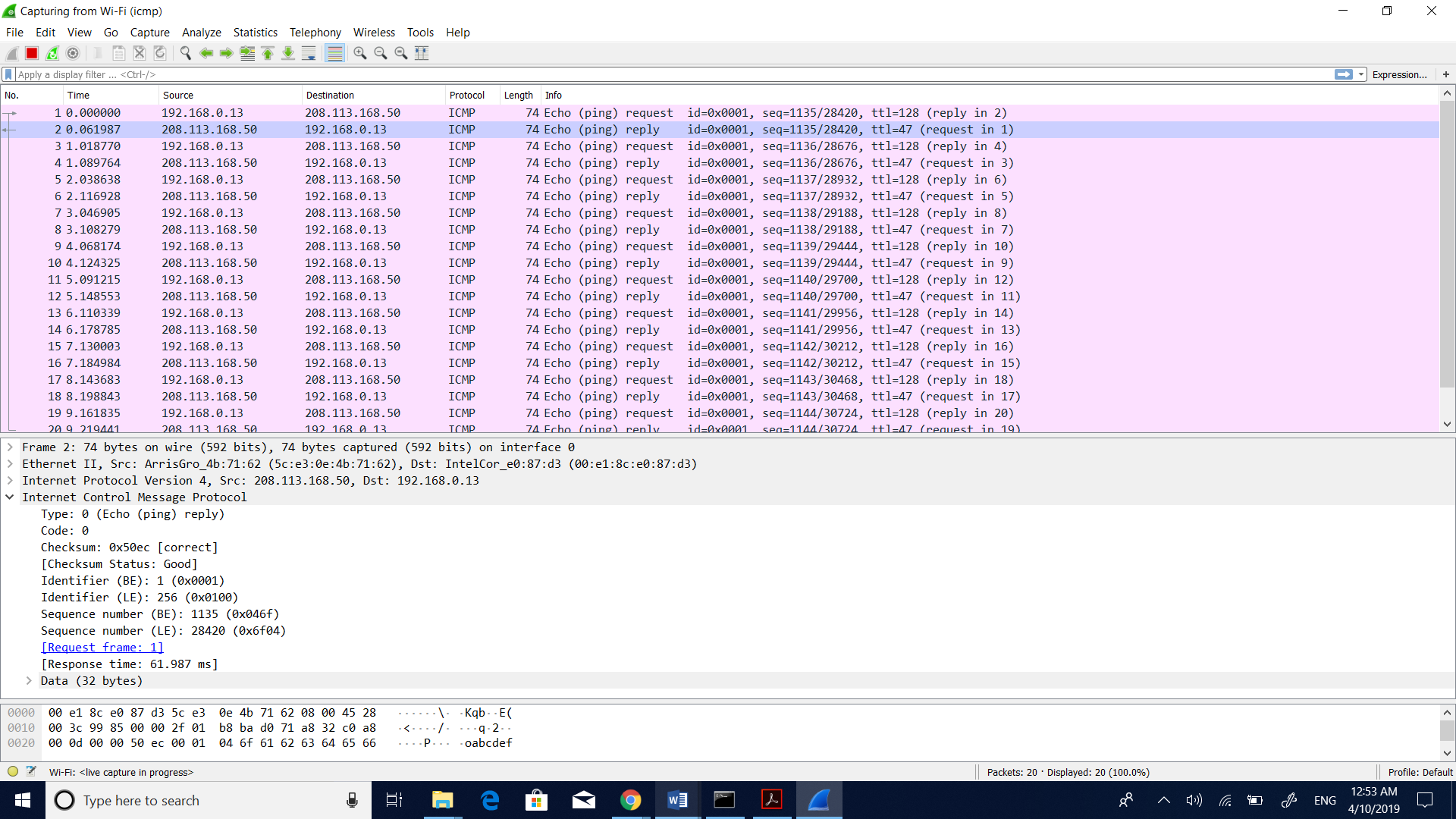
ICMP Code:0

Other fields: checksum, identifier (BE-0x0001)**,** identifier (LE-0x0100), sequence number (BE-0x046f)**,** sequence number (LE-0x6f04).

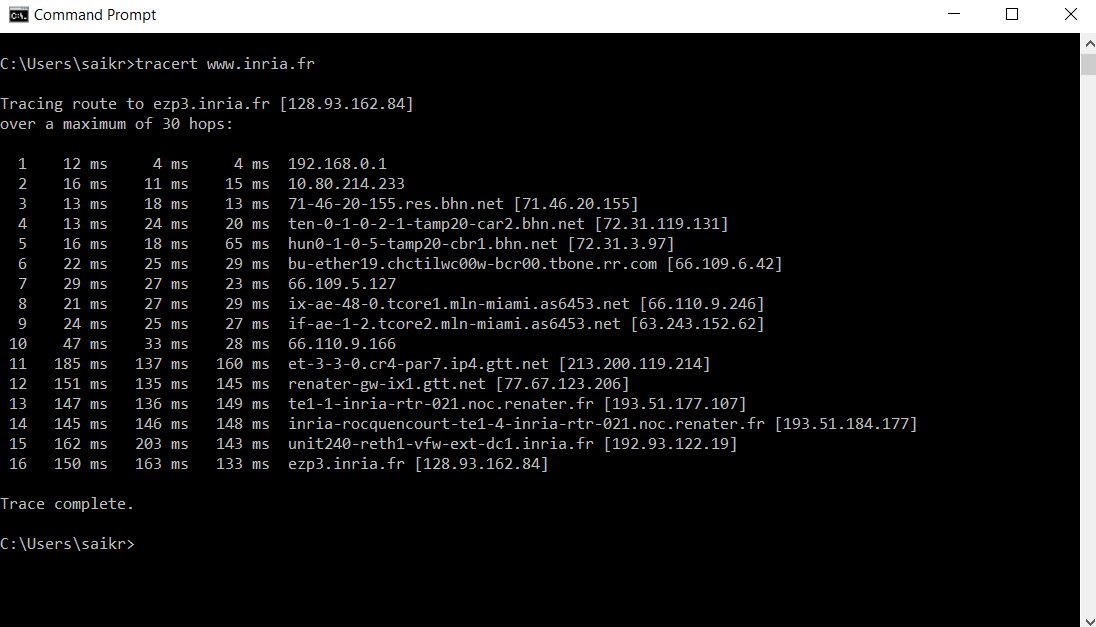
Checksum :2 bytes(0x50ec)

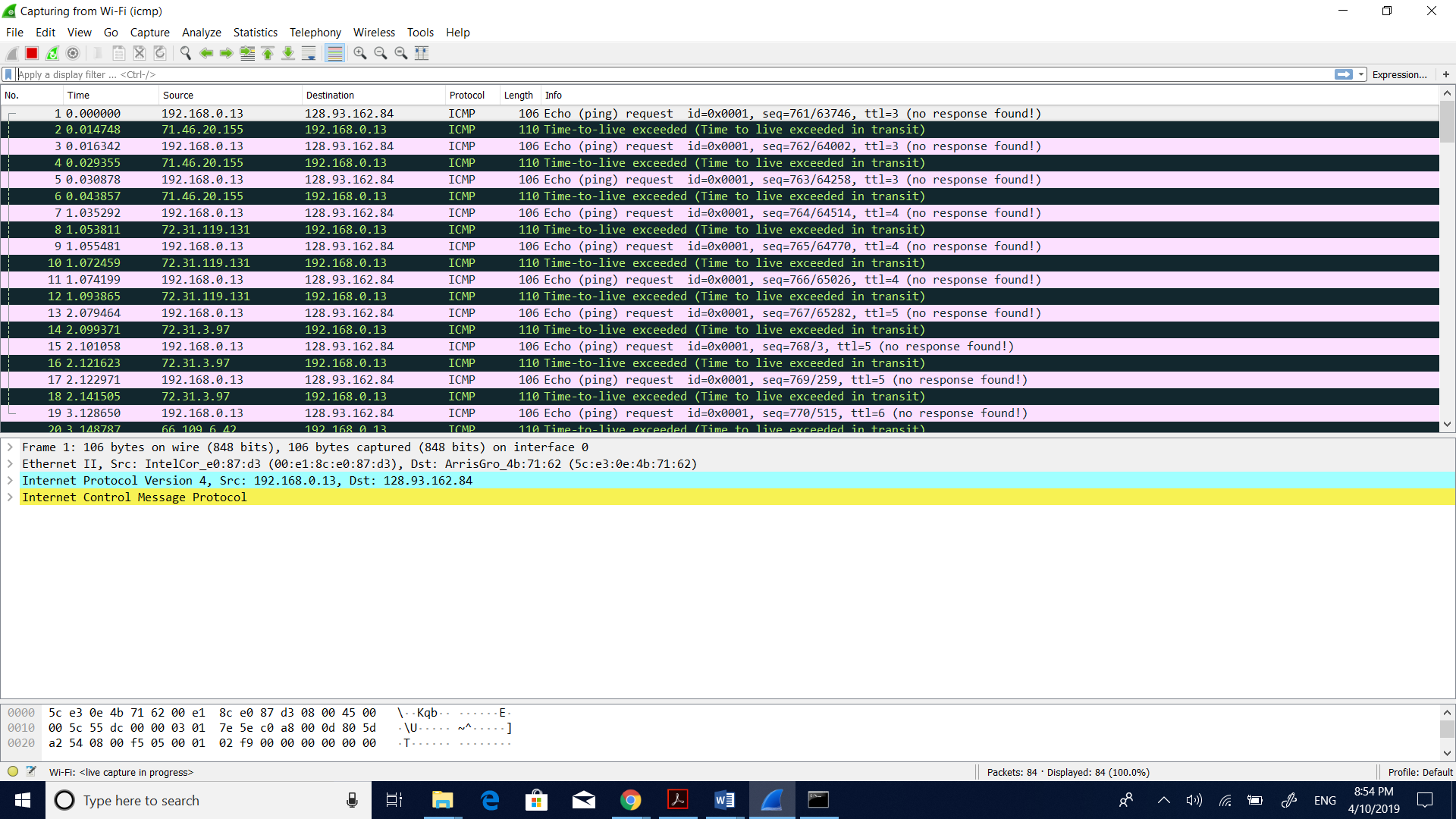
Sequence number:2 bytes

Identifier: 2bytes

****

**2) ICMP AND PINGS**



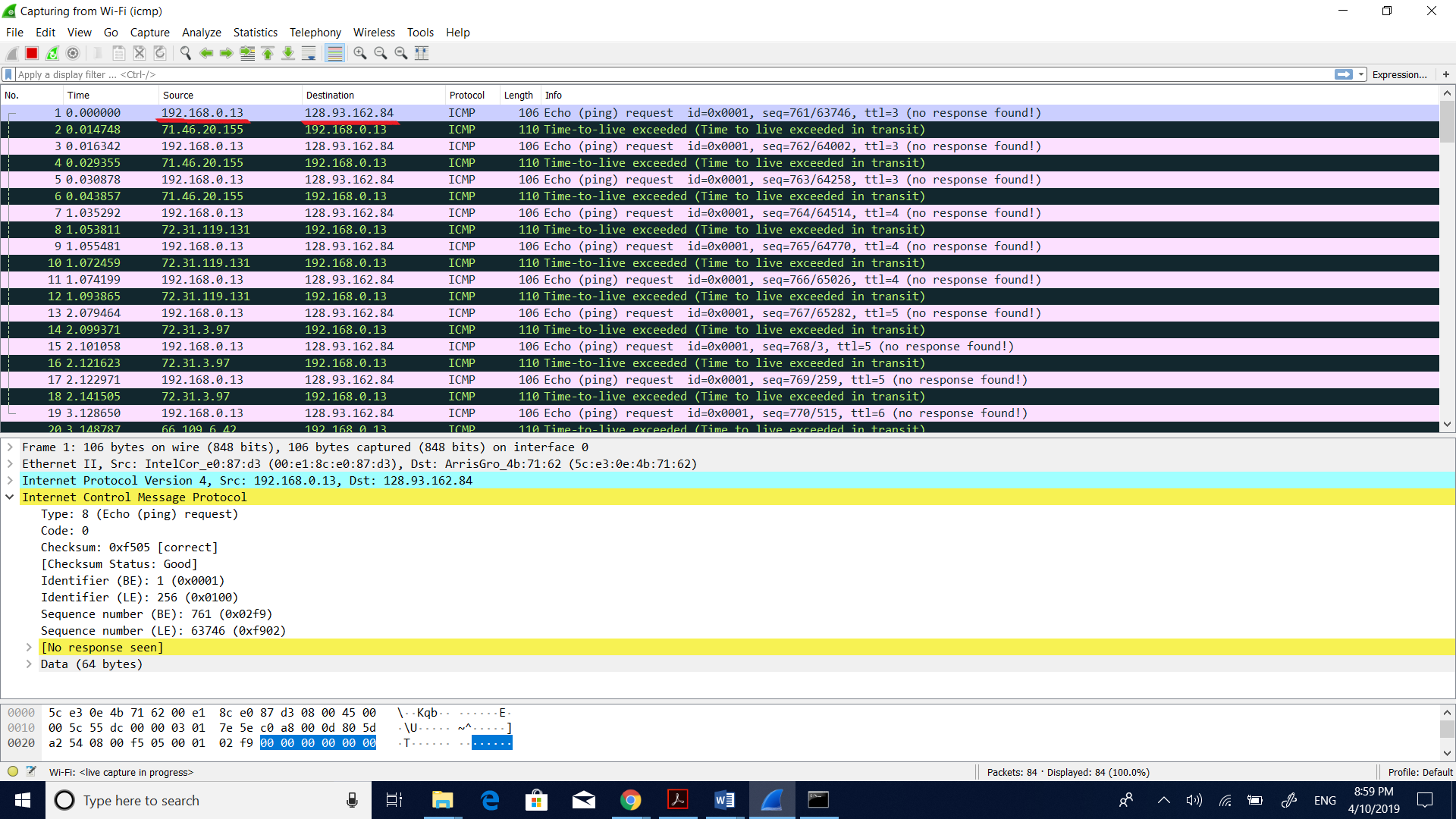


5) What is the IP address of your host? What is the IP address of the destination host?

**Solution:**

Source IP address: **192.168.0.13**

Destination IP address: **128.93.162.84**



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?

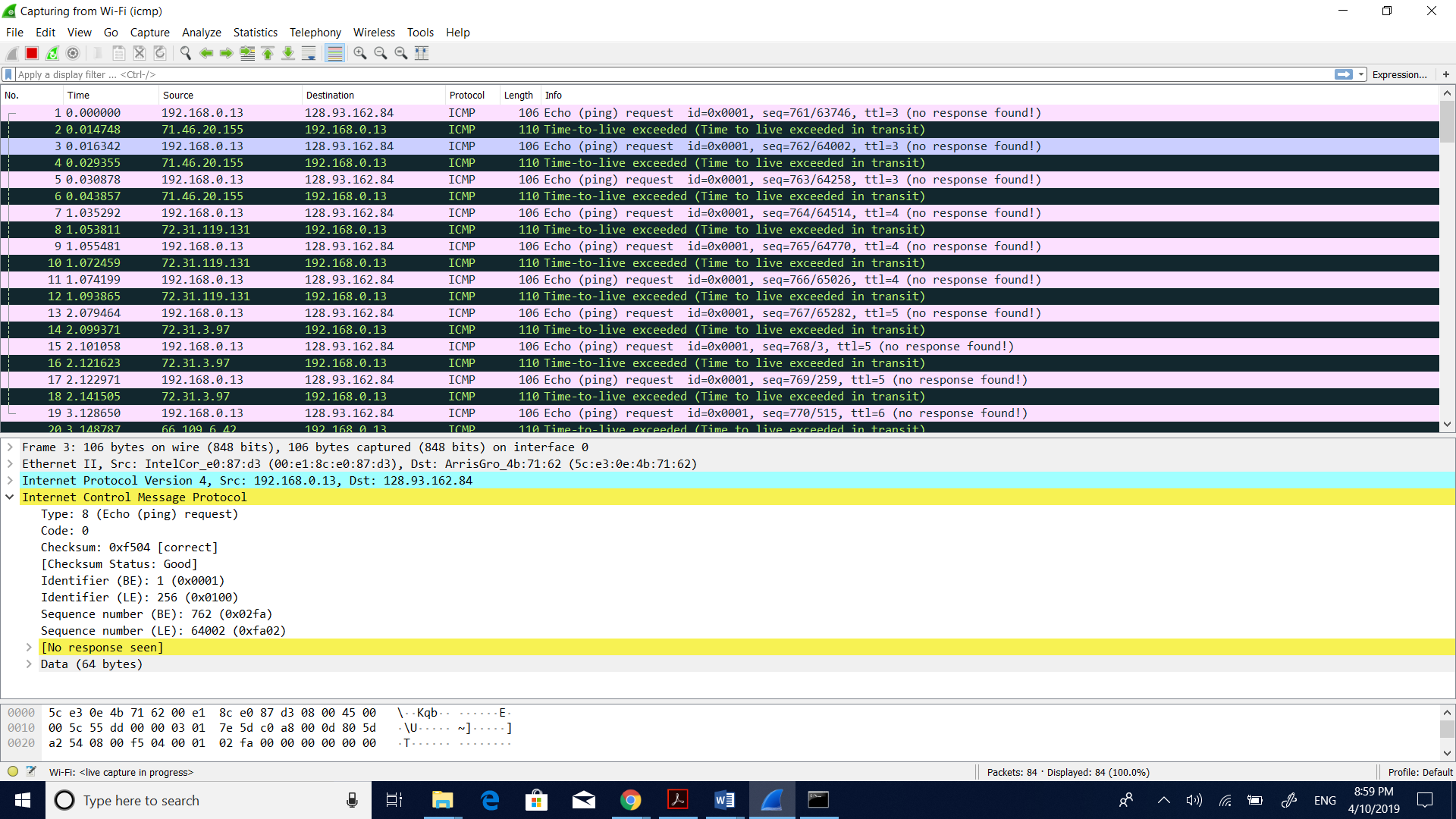
**Solution:**

No, the IP protocol number won’t be 01, if ICMP sent UDP packets then the IP protocol number for the probe packets would be 17 that is 0x11.

7) Examine the ICMP echo packet in the screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

**Solution:**

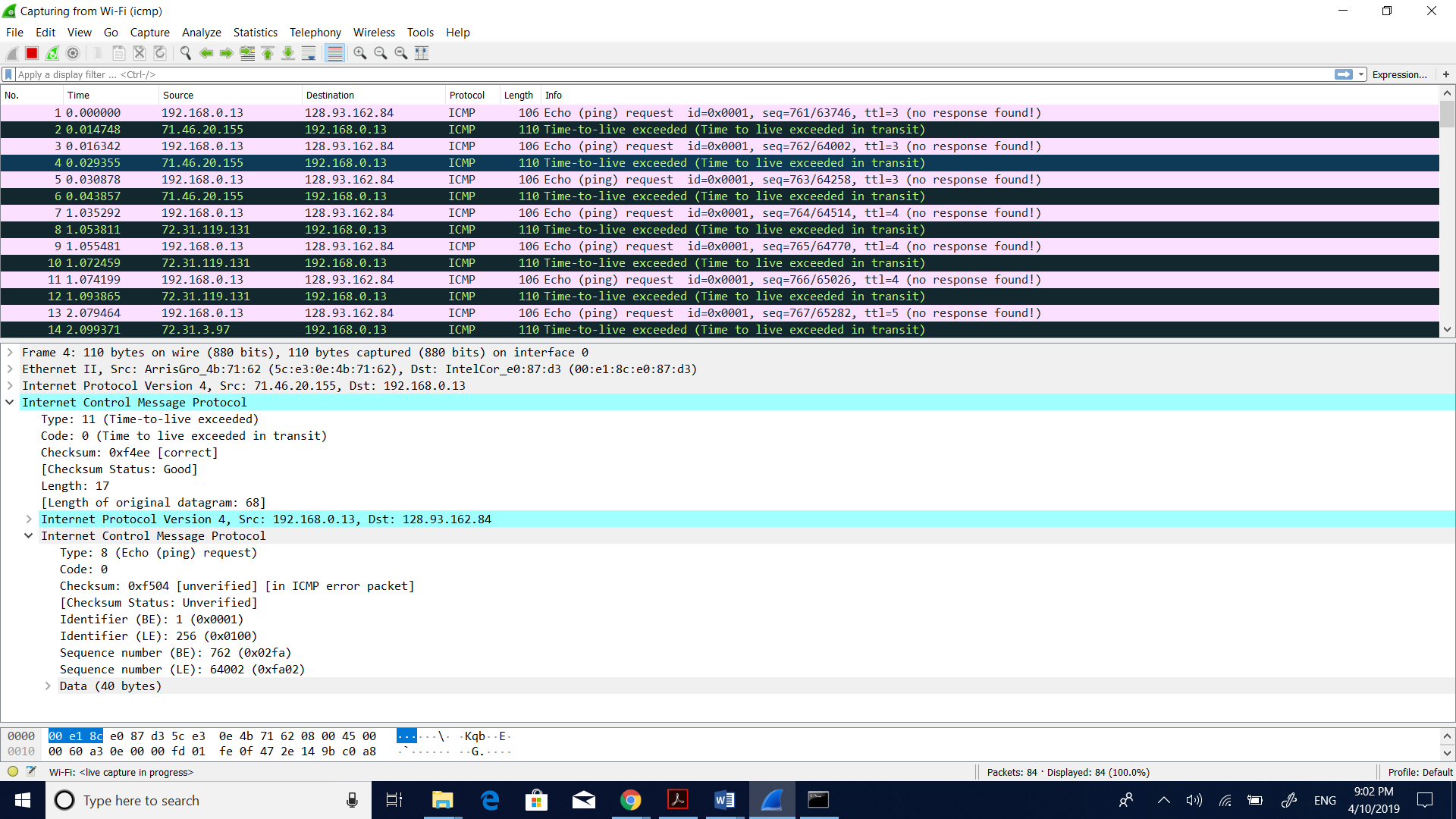
Yes, the fields of ICMP echo packets and the fields of ICMP ping query packets both are same.



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

**Solution:**

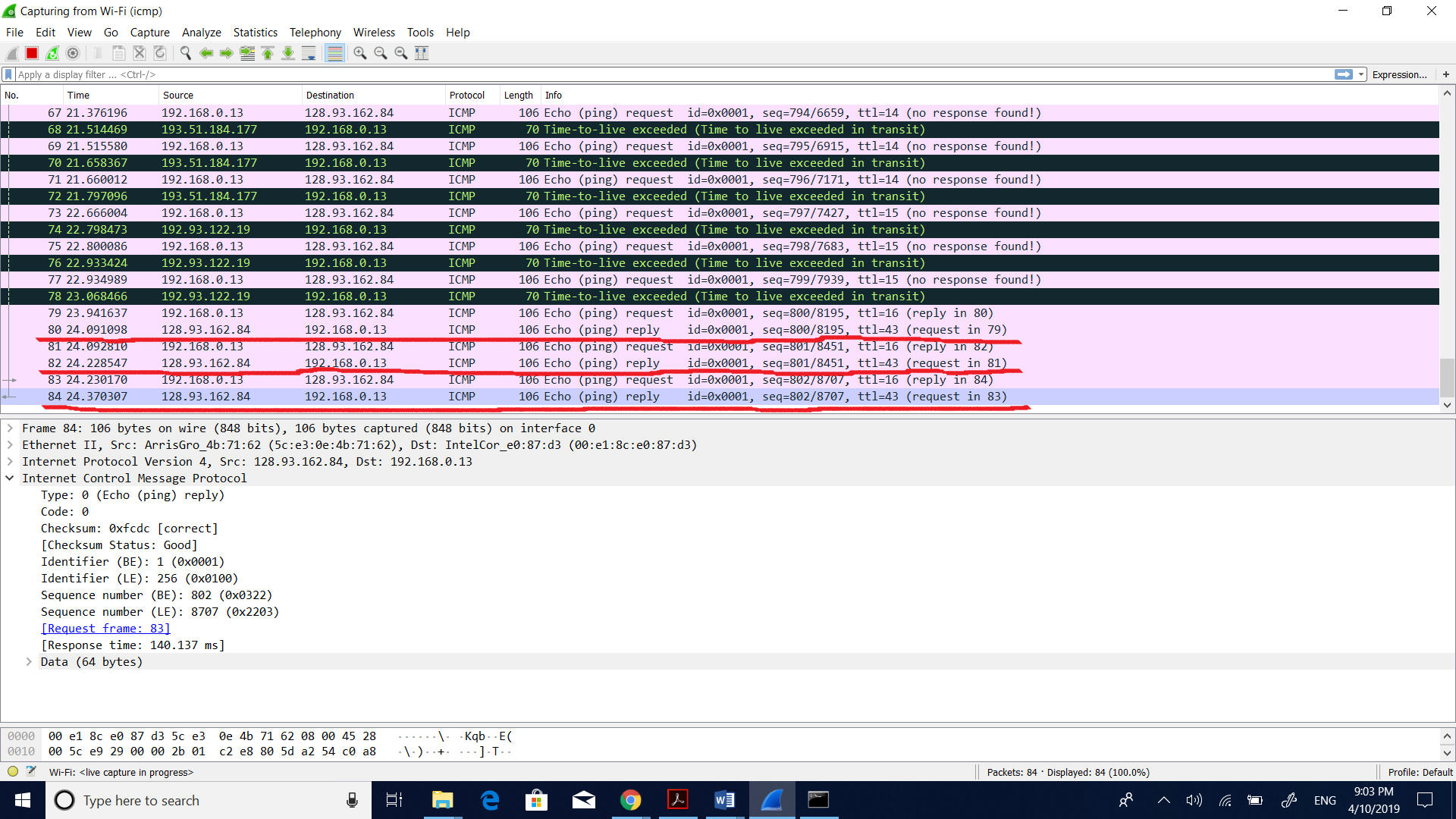
The fields include both the IP header and the first 8 bytes of the original ICMP packet which has information that the error is about the packet like the type, code and checksum. It also includes the extra fields ICMP packet include the Internet Control Message Protocol which provides the required details to be known.



9) Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

**Solution:**

The last three packets are both type0(echo reply) and code0 instead of having type11(TTL expired). These packets are different because from others which means TTL expired and they are dropped. Each one of these packets also include request frames from 79, 81 and 83 respectively. They are different because they reach the destination host before the TTL gets expired.



10) 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?

**Solution:**

Yes, there is a link between step 10 and step 11 that has a longer delay than every other. Because of the router names the location of the two routers end of this link is FRANCE can be guessed.

Here the path is from Tampa – Miami – France i.e., Tampa to Miami and from Miami to France.

