

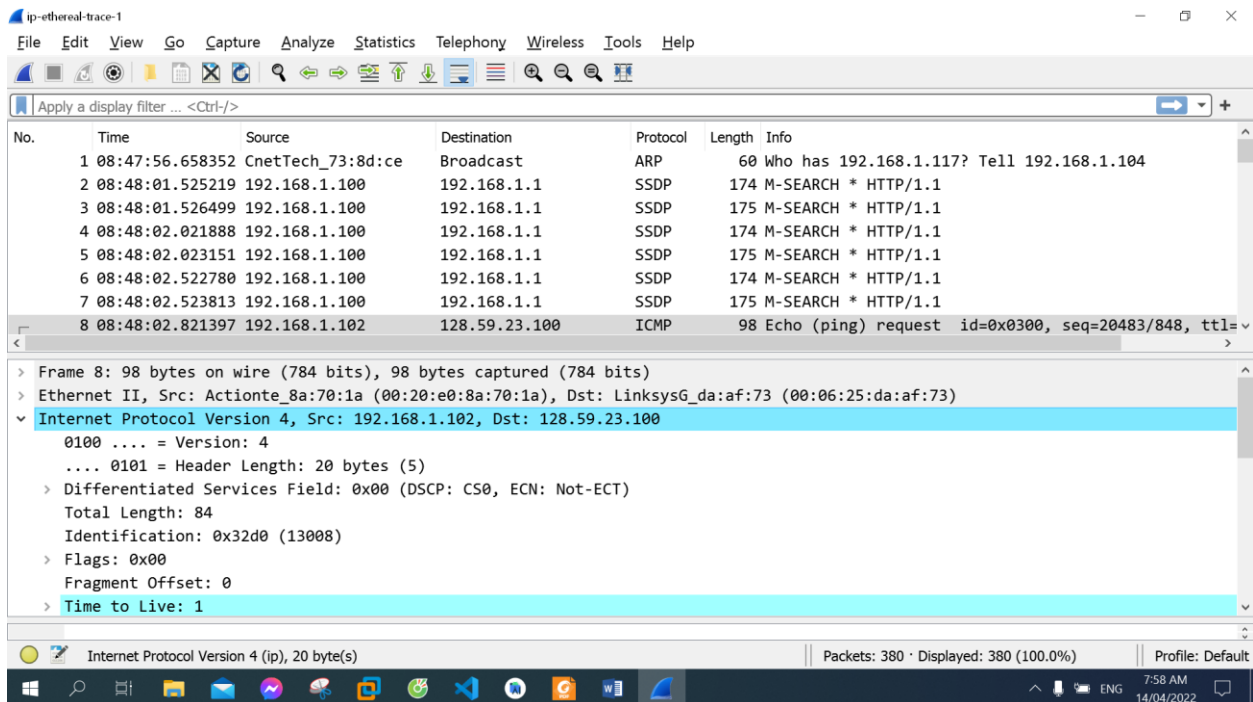
LAB 4A

Wireshark Lab: IP v8.0

Name: Hồ Đức Trí

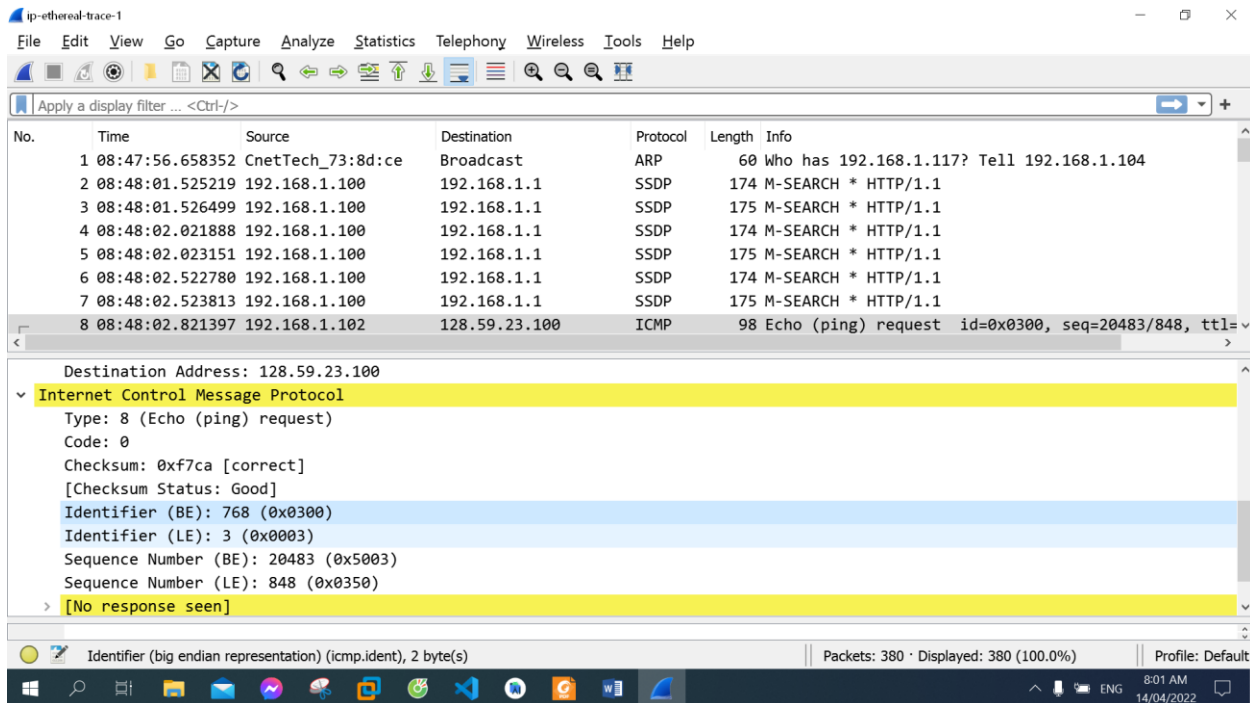
Student No: 1912288

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: 192.168.1.102

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



The value in the upper layer protocol field: 0x03

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.

- ▼ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 84

20 bytes in the IP header

64 bytes in the payload

Total length = 84 = header + payload = 20 + 64

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

- Flags: 0x00
- Fragment Offset: 0
- Time to Live: 1
- Protocol: ICMP (1)

This IP datagram has not been fragmented. Because the Fragment Offset 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?

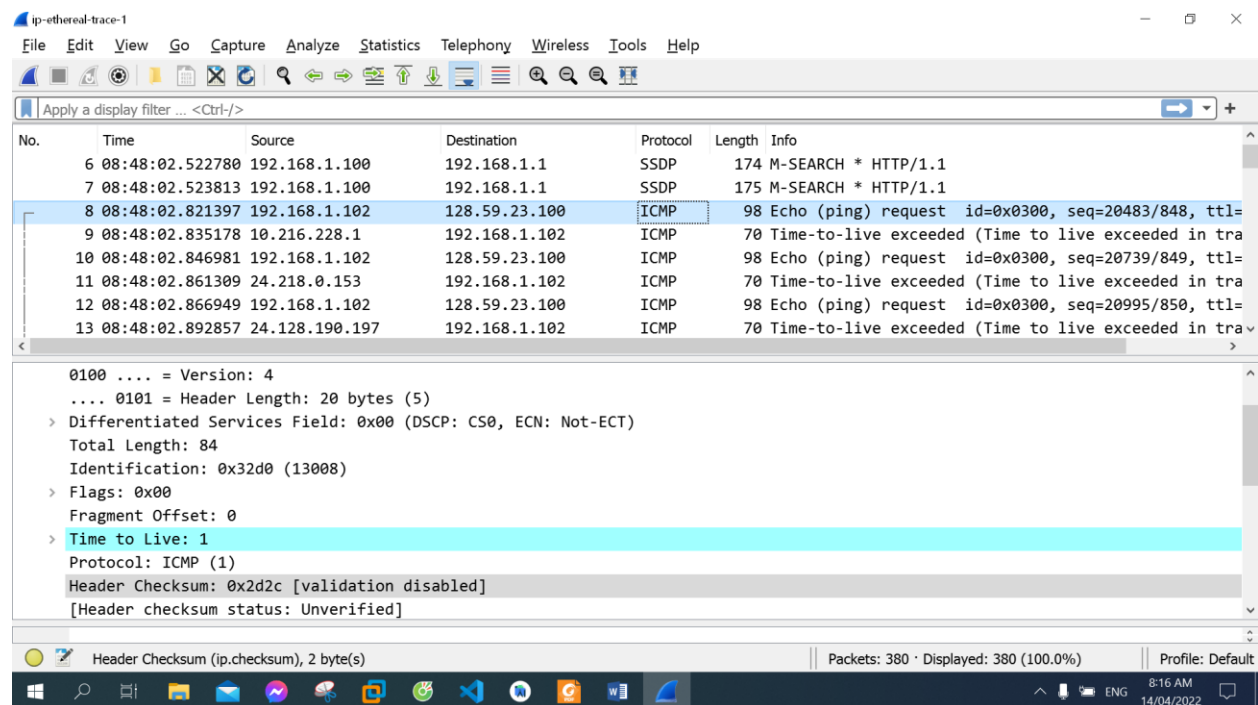
Identification, Header Checksum, Time to live always change from one datagram to the next within this series of ICMP messages

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

Fields stay constant and must stay constant: Version (we are using IPv4 for all packets), Header Length (these are ICMP packets), Source Address (we are sending from the same source), Destination Address (we are sending to the same destination) Differentiated Services Field all packets are ICMP they use the same Type of Service class), Protocol these are ICMP packets)

Fields must change: Identification(IP packets must have different ids), Time to live (traceroute increments each subsequent packet), Header checksum (header changes, so must checksum)

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



The screenshot shows a Wireshark packet capture of ICMP Echo (ping) messages. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
6	08:48:02.522780	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	08:48:02.523813	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
8	08:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=
9	08:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
10	08:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=
11	08:48:02.861309	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
12	08:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=
13	08:48:02.892857	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra

The packet details pane for the selected packet (No. 8) shows the following fields:

- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 84
- Identification: 0x32d0 (13008)
- Flags: 0x00
- Fragment Offset: 0
- Time to Live: 1
- Protocol: ICMP (1)
- Header Checksum: 0x2d2c [validation disabled]
- [Header checksum status: Unverified]

The status bar at the bottom indicates: Header Checksum (ip.checksum), 2 byte(s) | Packets: 380 · Displayed: 380 (100.0%) | Profile: Default

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
6	08:48:02.522780	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	08:48:02.523813	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
8	08:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=
9	08:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
10	08:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=
11	08:48:02.861309	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
12	08:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=
13	08:48:02.892857	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 84
 Identification: 0x32d1 (13009)
 > Flags: 0x00
 Fragment Offset: 0
 > Time to Live: 2
 Protocol: ICMP (1)
 Header Checksum: 0x2c2b [validation disabled]
 [Header checksum status: Unverified]

Header Checksum (ip.checksum), 2 byte(s) | Packets: 380 · Displayed: 380 (100.0%) | Profile: Default

8:16 AM 14/04/2022

The pattern in the identification field is that the field increases by one in each strand of echo requests (0x32d0 -> 0x32d1)

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

ip-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
6	08:48:02.522780	192.168.1.100	192.168.1.1	SSDP	174	M-SEARCH * HTTP/1.1
7	08:48:02.523813	192.168.1.100	192.168.1.1	SSDP	175	M-SEARCH * HTTP/1.1
8	08:48:02.821397	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20483/848, ttl=
9	08:48:02.835178	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
10	08:48:02.846981	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20739/849, ttl=
11	08:48:02.861309	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra
12	08:48:02.866949	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, seq=20995/850, ttl=
13	08:48:02.892857	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to live exceeded in tra

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
 Total Length: 56
 Identification: 0x9d7c (40316)
 > Flags: 0x00
 Fragment Offset: 0
 Time to Live: 255
 Protocol: ICMP (1)
 Header Checksum: 0x6ca0 [validation disabled]
 [Header checksum status: Unverified]

Header Checksum (ip.checksum), 2 byte(s) | Packets: 380 · Displayed: 380 (100.0%) | Profile: Default

8:21 AM 14/04/2022

Identification: 0x9d7c (40316)

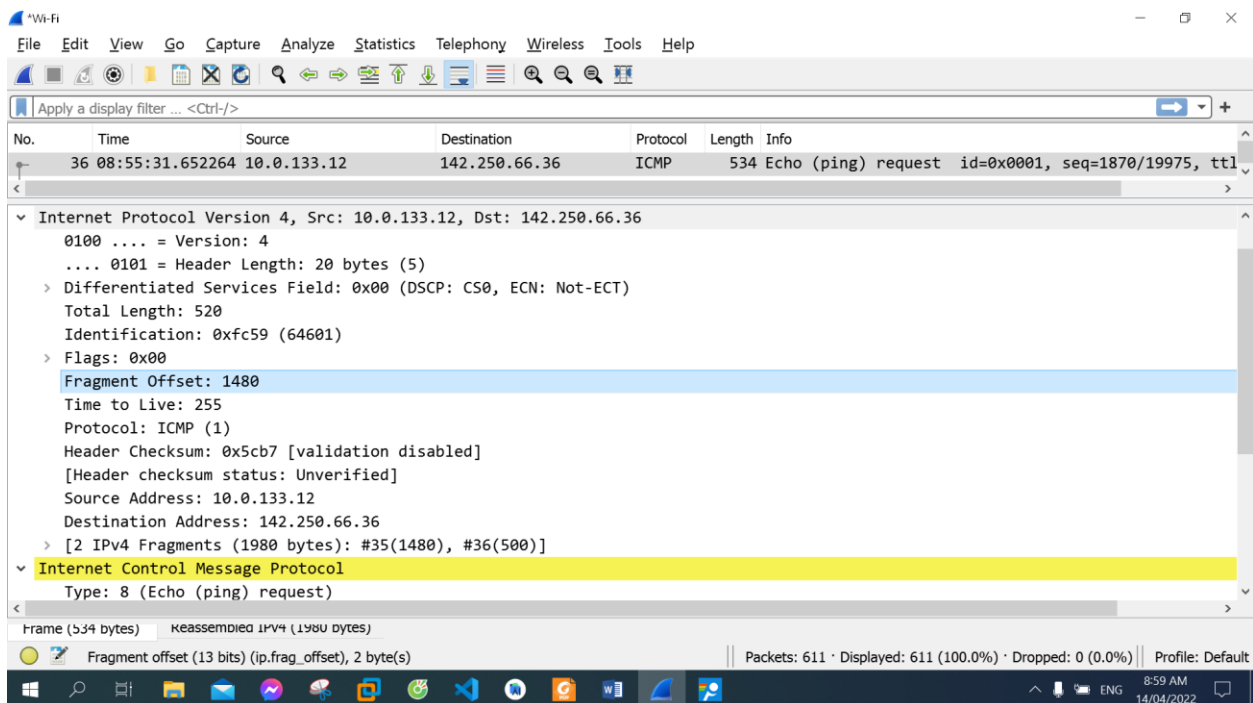
TTL: 255

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?

No, they are not. Identification changes because IP packets must have different ids, Time to live changes because traceroute increments each subsequent packet

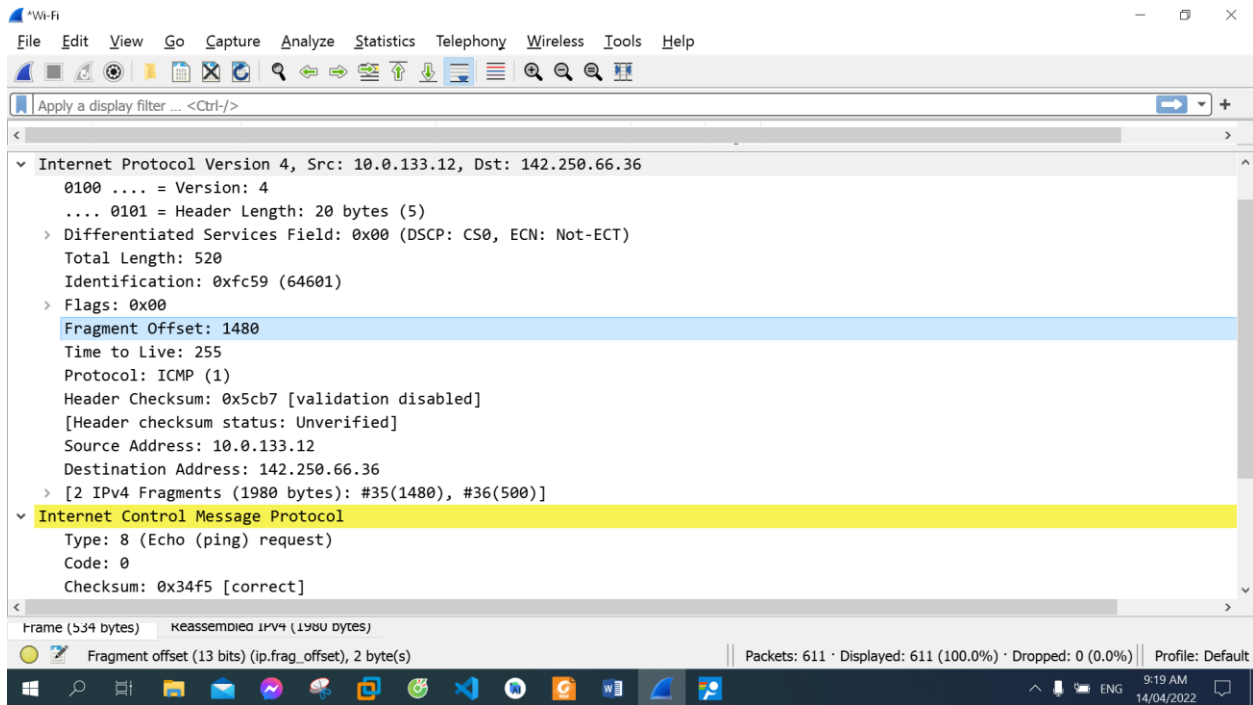
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

Use: *gaia.cs.umass.edu* for Question 10,11,12,13,14,15



Yes, it has. (Fragment Offset > 0)

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?

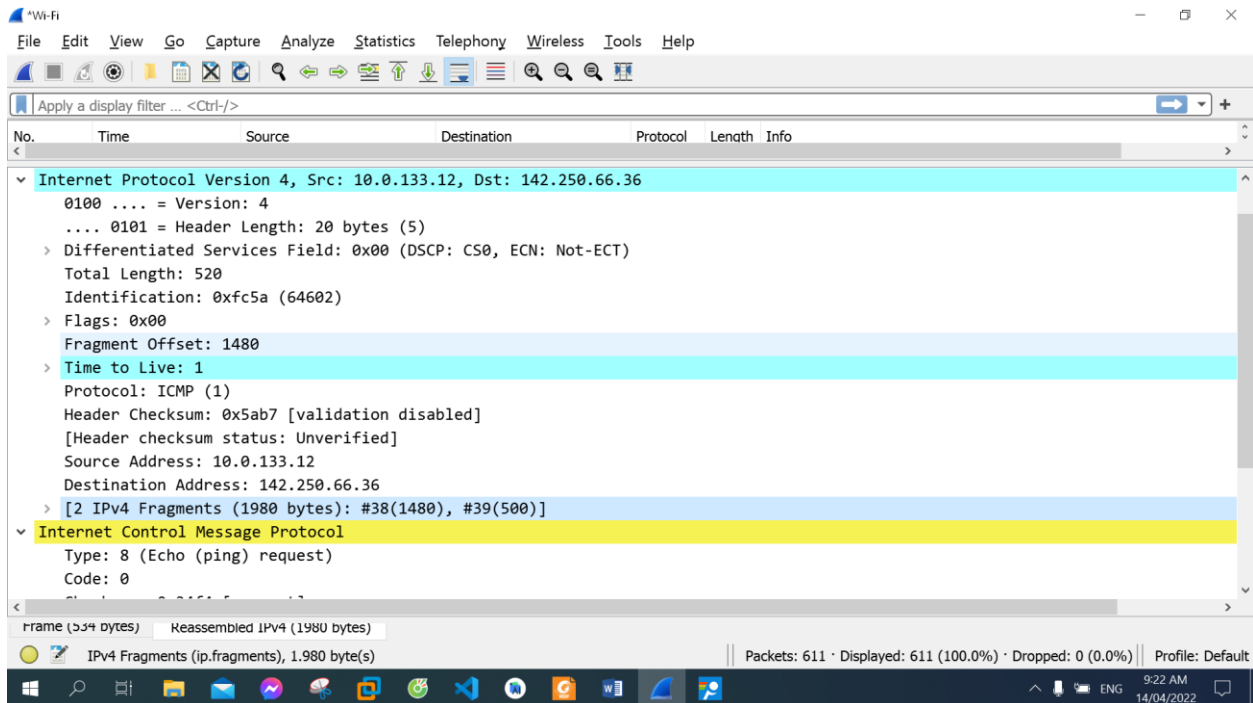


Fragment Offset: 1480 indicates that the datagram been fragmented

Information in the IP header indicates whether this is the first fragment: Fragments number is the smallest (#35)

This IP datagram: 520

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 there more fragments? How can you tell?



It's Fragments number (#38) is greater than the first datagram fragment.

Identification: 0xfc5a (64602)

Flags: 0x00

0... .. = Reserved bit: Not set

.0.. .. = Don't fragment: Not set

..0. = More fragments: Not set

There is no more fragments. Because Flags More fragments is not set.

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

Time to live, Identification, 2 IPv4 Fragments

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

3 fragments were created from the original datagram

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

DESTINATION ADDRESS: 142.250.66.36

> [3 IPv4 Fragments (3480 bytes): #1(1480), #2(1480), #3(520)]

Time to live, Identification, 3 IPv4 Fragments