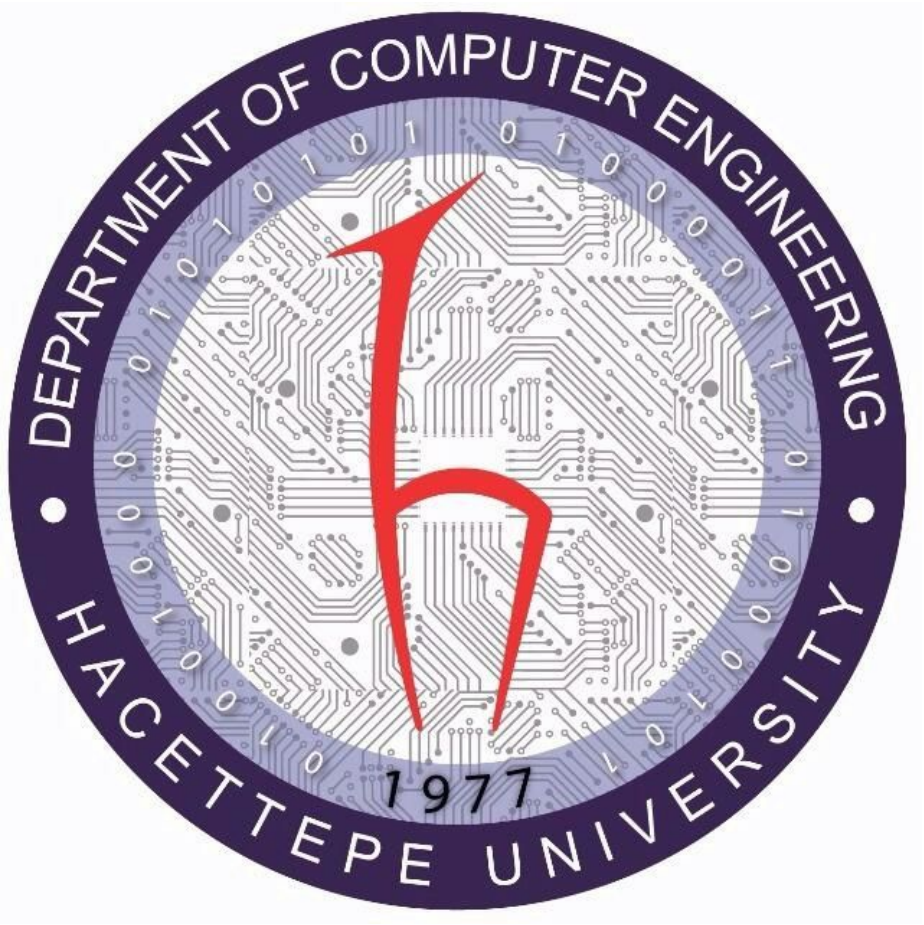


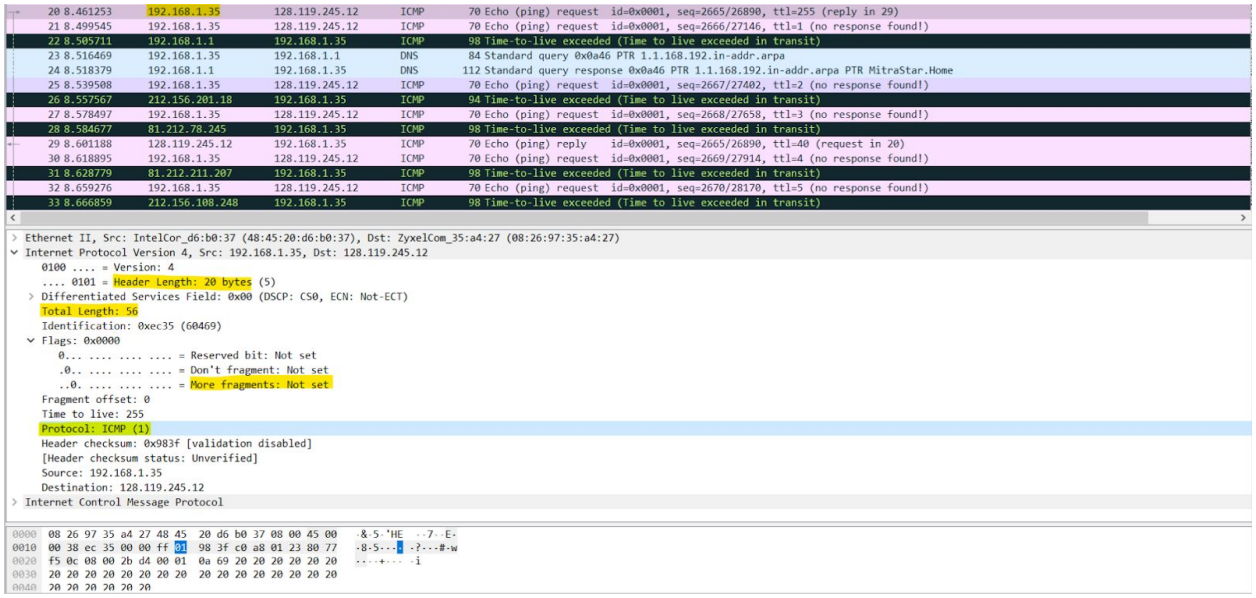
Gökhan Özeloğlu - 21627557
Burak Yılmaz - 21627868

BBM 453 Computer Networks Lab - IP Lab Assignment
Group ID: 1

Note: We were using windows that's why we worked with ICMP protocol rather than UDP as it is mentioned in lab assignment PDF.

1.Select the first UDP segment 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?

ANS: My ip address is 192.168.1.35



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

ANS: As you can see from the above screenshot with the highlighted part the value in the upper layer protocol is ICMP(1)

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.

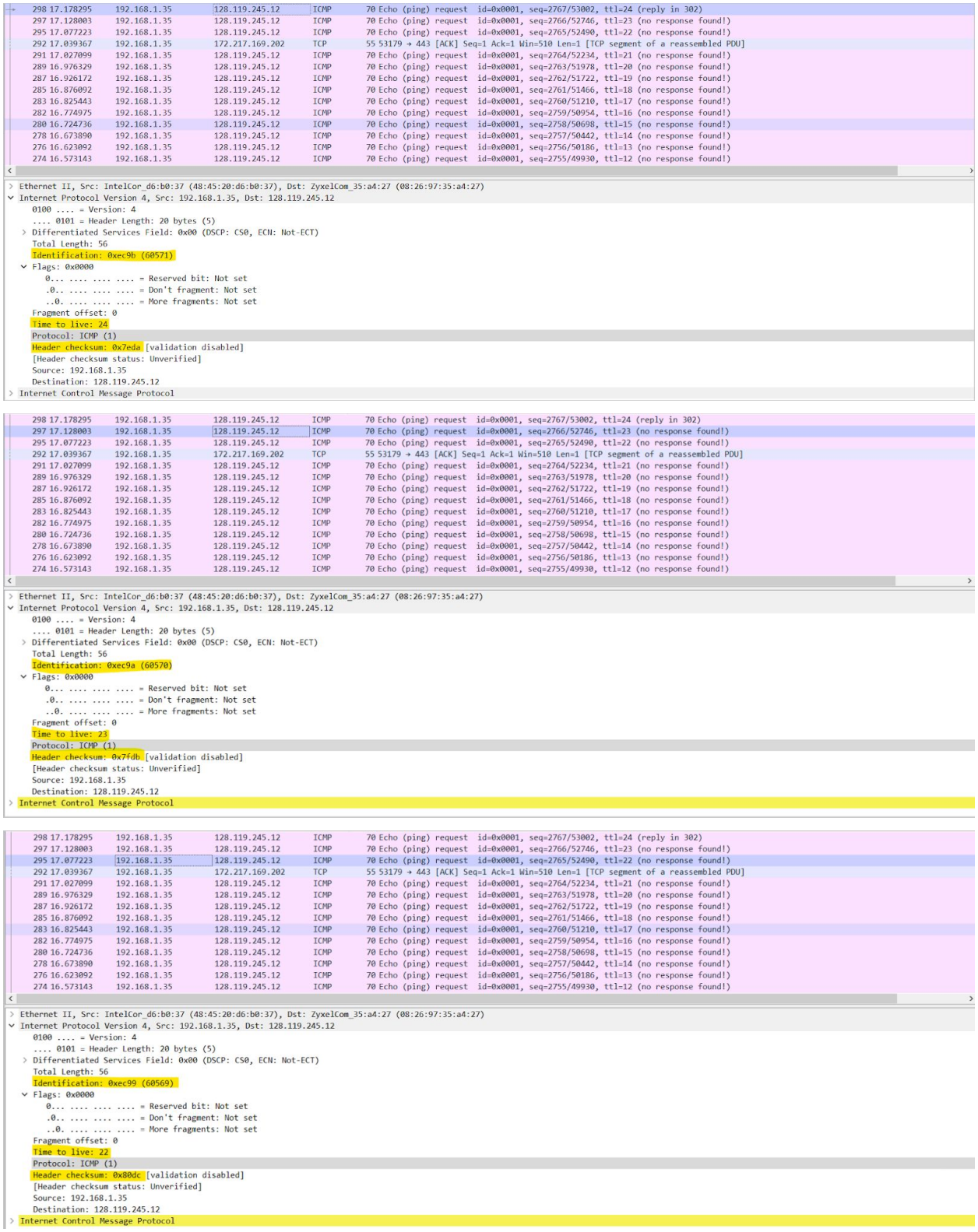
ANS: Header bytes: 20 (as you can seen in screenshot with the highlighted parts)
Payload bytes: 36 (total length 56 minus the 20 header bytes = 36)

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

ANS: According to the screenshot above , under flags section, the more fragments bit = 0, so the data is not fragmented.

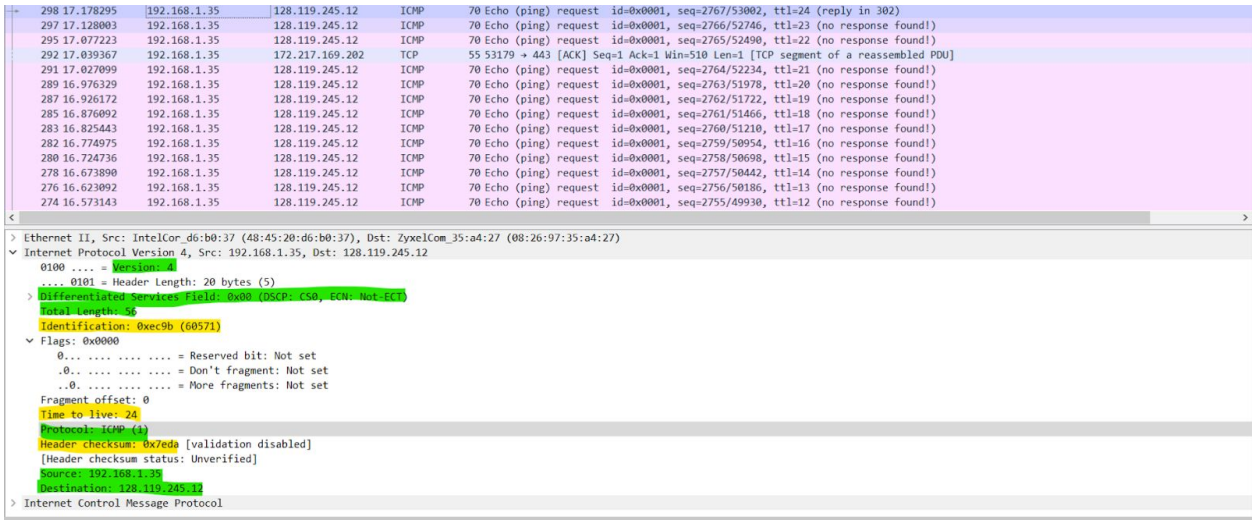
5. Which fields in the IP datagram always change from one datagram to the next within this series of UDP messages sent by your computer?

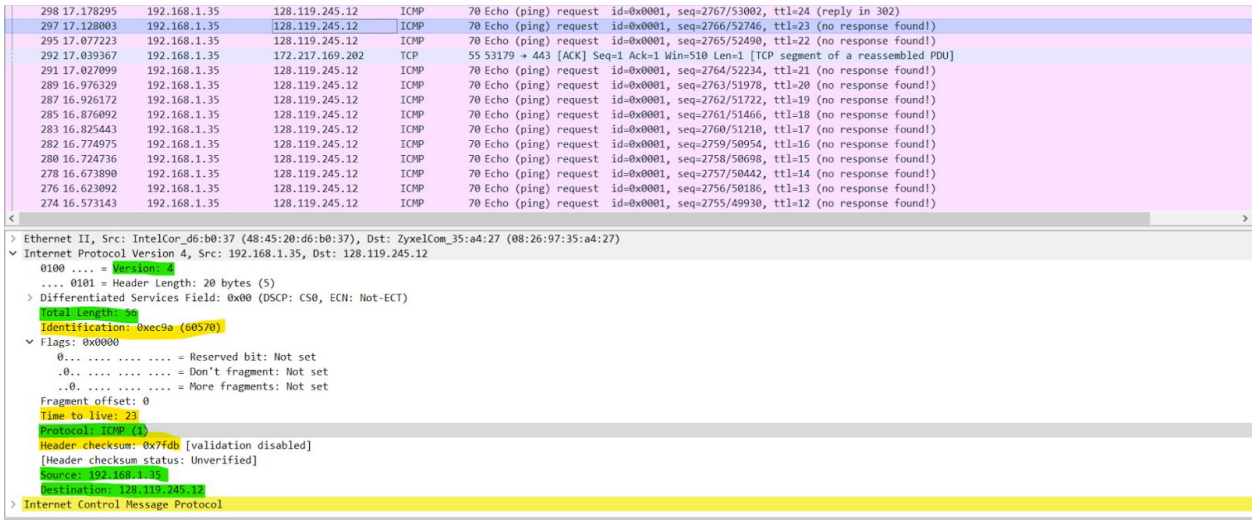
ANS: As you can see the screenshots(example of 3 screenshots) below the identification, Time to live and Header checksum fields are always changing.



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

ANS: Yellow ones are always changing, green ones always stay the same. You can compare two example screenshots.





The fields that stay constant across the IP datagrams are:

- **Version (since we are using IPv4 for all packets)**
- **header length (since these are ICMP packets)**
- **source IP (since we are sending from the same source)**
- **destination IP (since we are sending to the same dest)**
- **Differentiated Services (since all packets are ICMP they use the same Type of Service class)**
- **Upper Layer Protocol (since these are ICMP packets)**

The fields that must stay constant are:

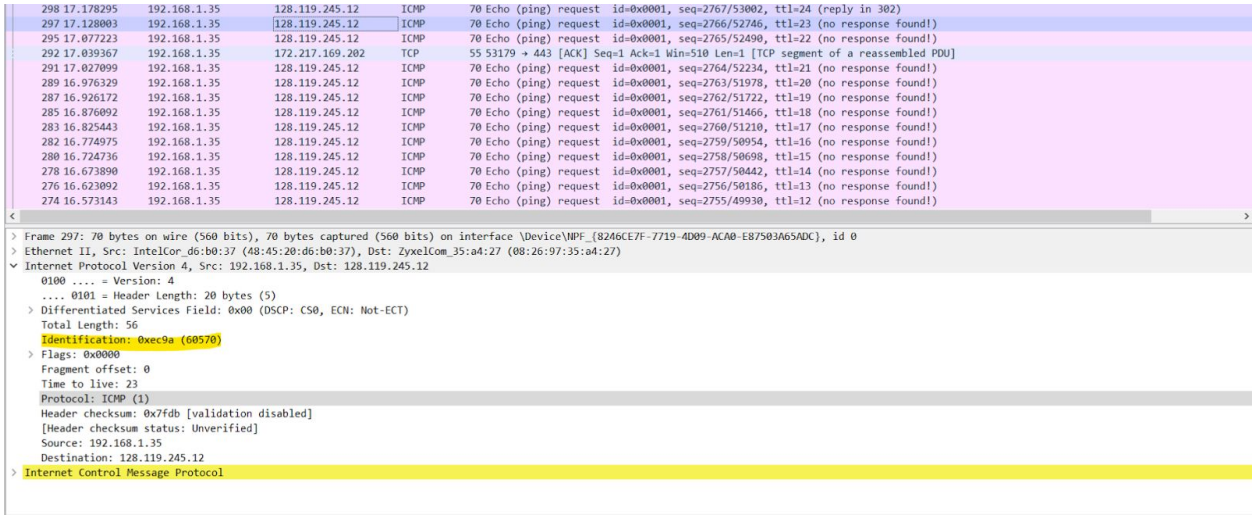
- **Version (since we are using IPv4 for all packets)**
- **header length (since these are ICMP packets)**
- **source IP (since we are sending from the same source)**
- **destination IP (since we are sending to the same dest)**
- **Differentiated Services (since all packets are ICMP they use the same Type of Service class)**
- **Upper Layer Protocol (since these are ICMP packets)**

The fields that must change are:

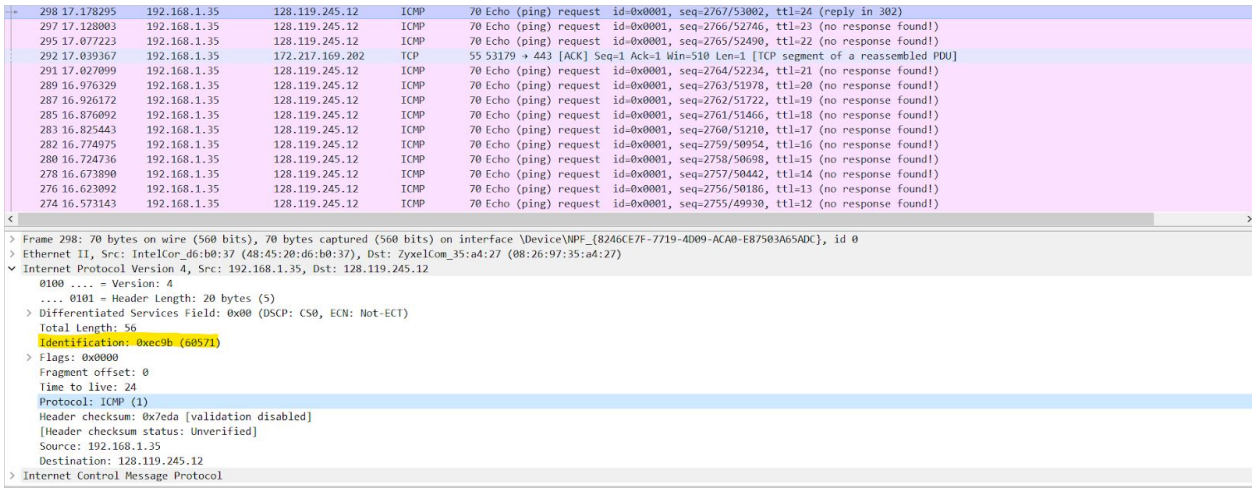
- **Identification(IP packets must have different ids)**
- **Time to live (traceroute increments each subsequent packet)**
- **Header checksum (since header changes, so must checksum)**

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

ANS: The pattern is that the IP header Identification fields increment with each ICMP Echo (ping) request as you can see below screenshots.



Identification number = 60570



Identification number = 60571

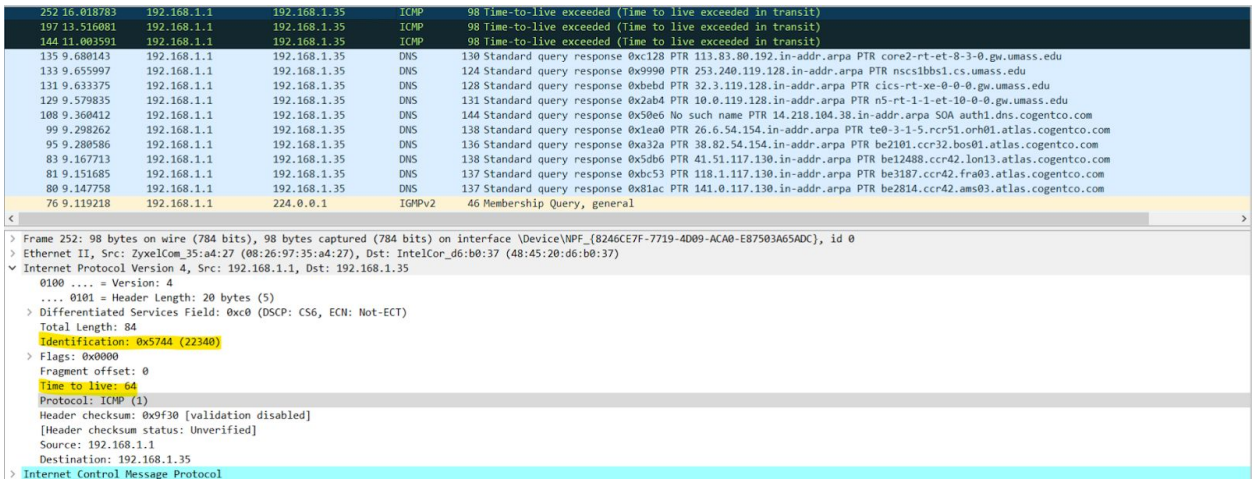
8. What is the value in the Identification field and the TTL field?

Nearest router ip address is 192.168.1.1 as you can see below.

gaia.cs.umass.edu — Interval 2,5 seconds — Focus

Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	5	192.168.1.1	MitraStar.Home	3,2	1,9	2,8	
2	5	212.156.201.18	212.156.201.18.static.turktelekom.com.tr	11,7	7,4	7,4	
3	5	81.212.78.245	81.212.78.245.static.turktelekom.com.tr	7,8	6,3	6,9	
4	5	81.212.211.207	06-balgat-t2-2---06-balgat-t3-3.statik.turktele	9,0	7,3	7,7	
5	5	212.156.108.248	06-ulus-xrs-t2-2---06-balgat-t2-2.statik.turkte	11,1	7,7	10,2	
6	4	81.212.217.121	06-ebgp-ulus-sr12e-k---06-ulus-xrs-t2-2.stati	7,7	7,7	*	75,0
7	5	212.156.101.126	301-fra-col-1---06-ulus-xrs-t2-1.statik.turktele	51,0	49,8	52,5	
8	5	213.198.83.197	213.198.83.197	61,1	55,4	56,3	
9	5	129.250.4.76	ae-4.r20.frnkge13.de.bb.gin.ntt.net	59,9	56,1	59,3	
10	5	129.250.6.14	ae-3.r00.frnkge13.de.bb.gin.ntt.net	68,9	56,8	59,2	
11	5	130.117.14.129	be2914.agr41.fra03.atlas.cogentco.com	64,3	57,0	58,6	

ANS: Identification field = 22340 , TTL = 64

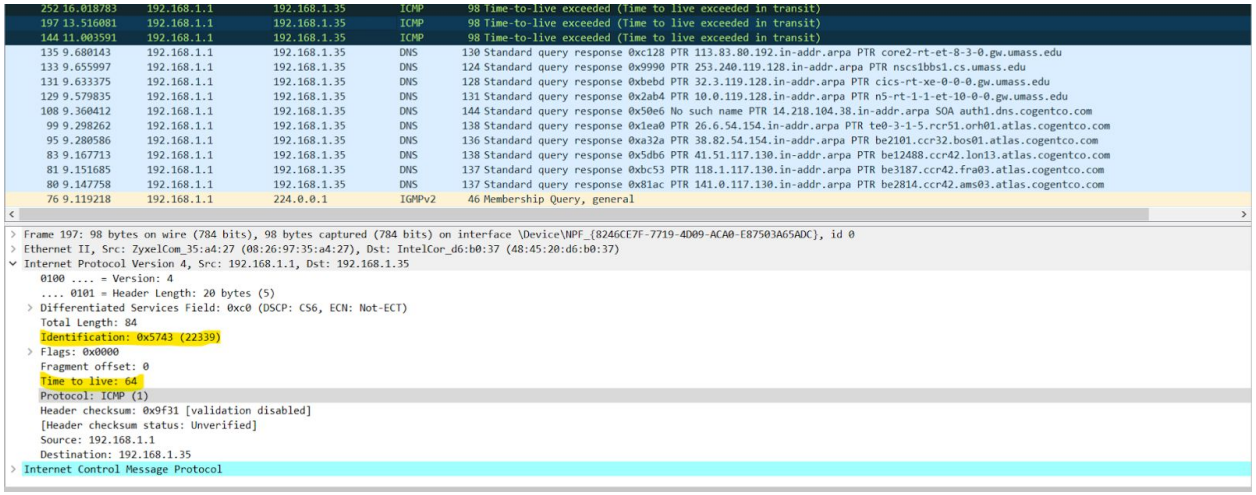


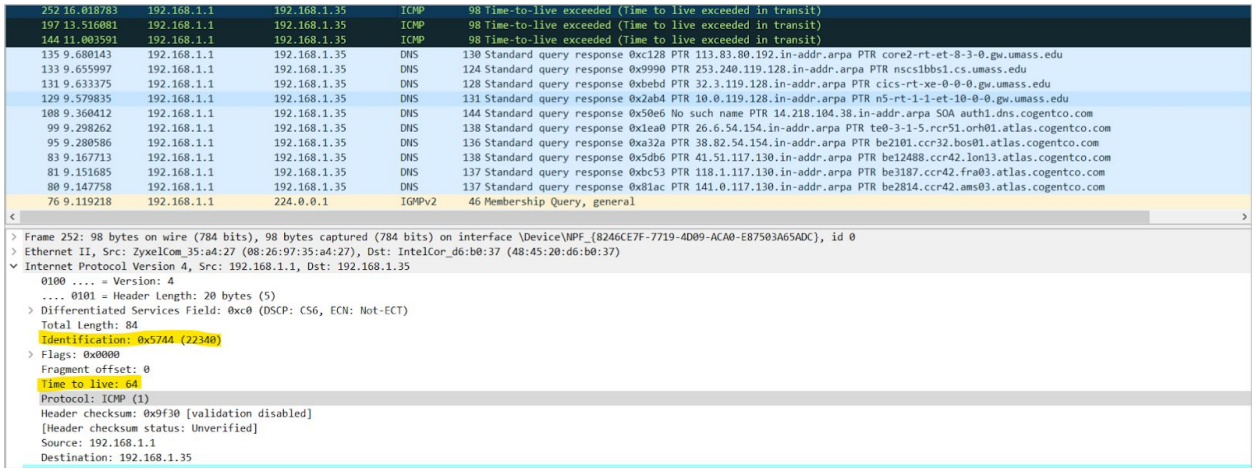
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

ANS: The identification field changes for all the ICMP TTL-exceeded replies because the identification field is a unique value. When two or more IP datagrams have the same identification value, then it means that these IP datagrams are fragments of a single large IP datagram.

The TTL field remains unchanged because the TTL for the first hop router is always the same.

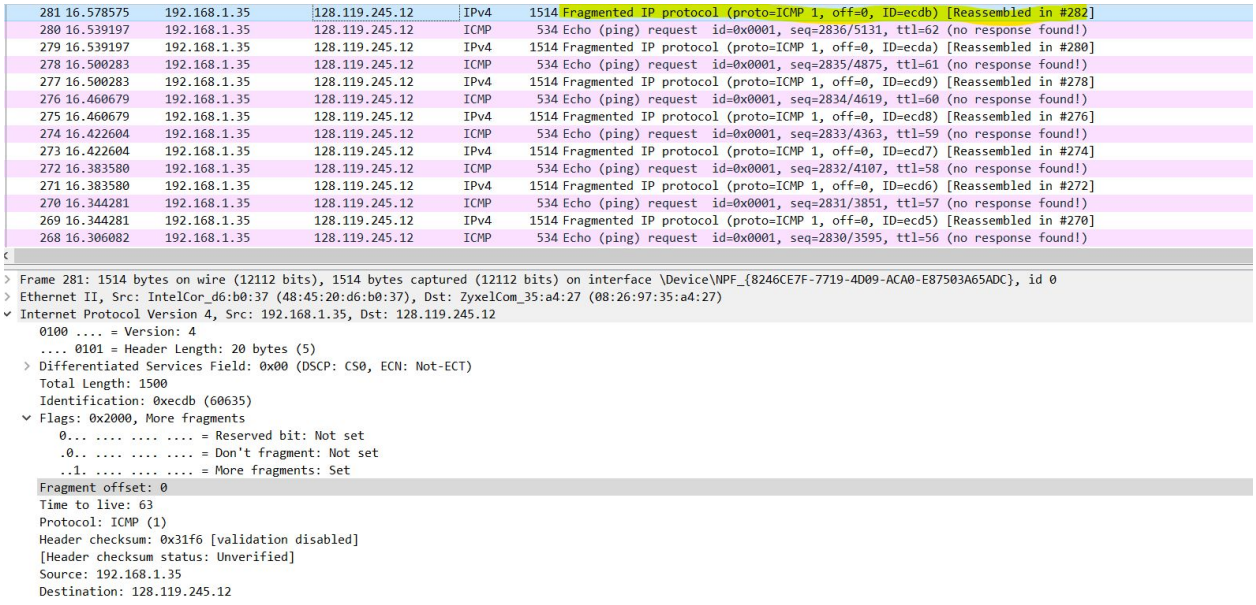
You can see the below with two screenshots.





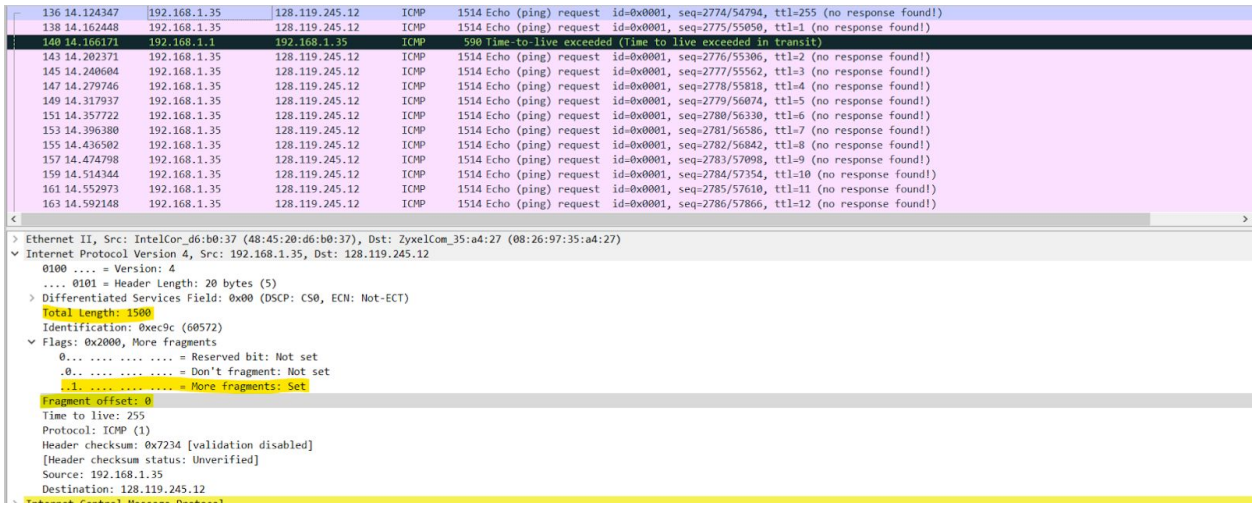
10. Find the first UDP segment message that was sent by your computer after you changed the Packet to be 12000. Has that message been fragmented across more than one IP datagram?

ANS: Yes, this packet has been fragmented across more than one IP datagram



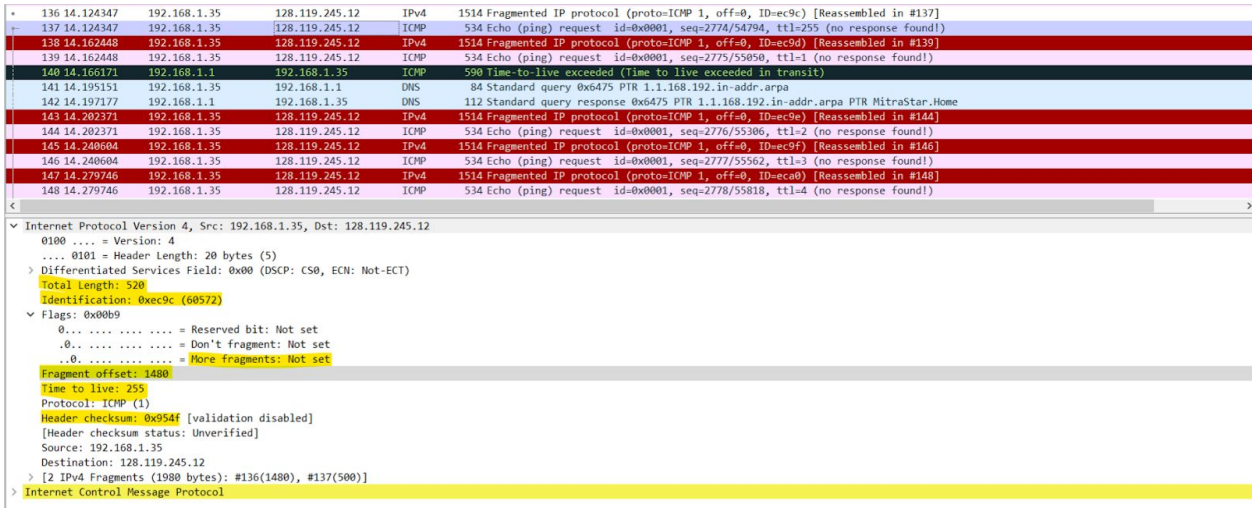
11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram has been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

ANS: According to the screenshot below, The Flags bit for more fragments is set to 1 which means the datagram has been fragmented. The fragment offset is 0, we know this is the first fragment. The length of this first datagram is 1500 including the header



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?

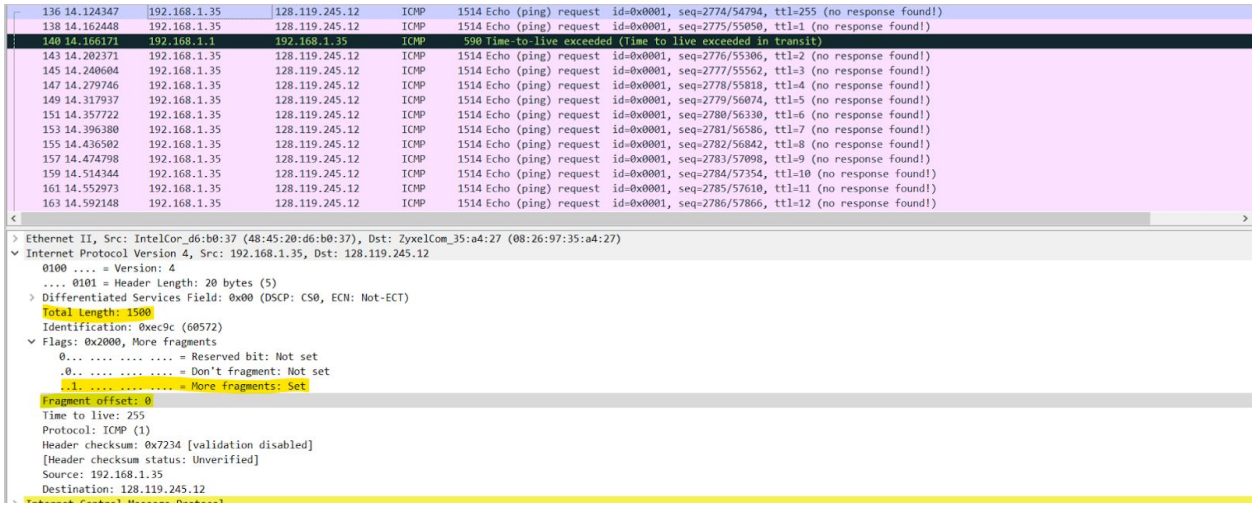
ANS: According to the below screenshot, this is not the first fragment since the fragment offset is 1480 and this should be the last fragment, since the status of more fragments flag is not set.



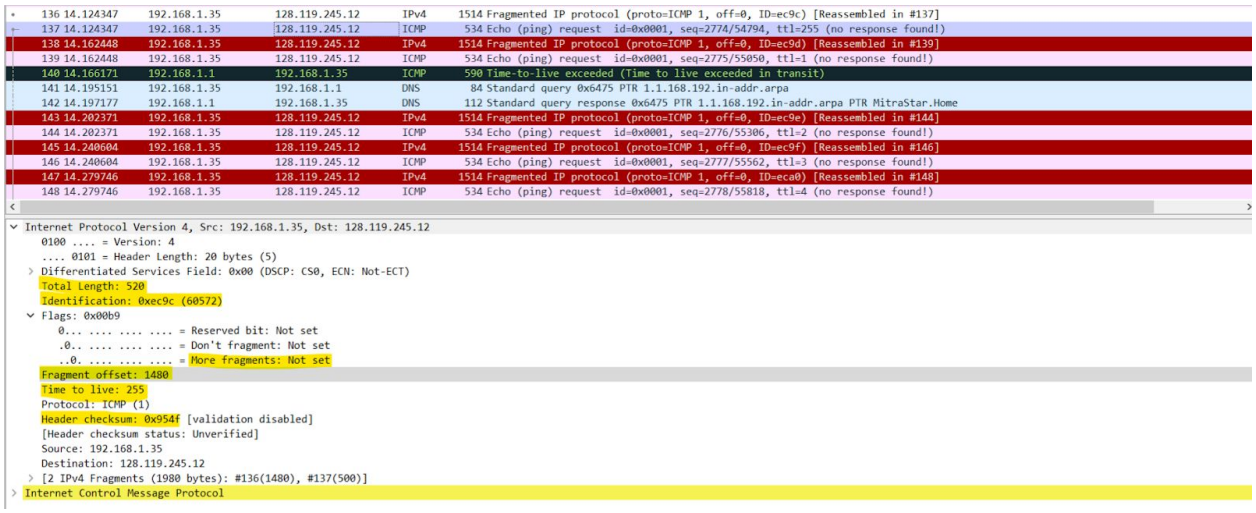
13. What fields change in the IP header between the first and second fragment?

ANS: Total length, the more fragments bit, fragment offset and header checksum.You can compare the results between first and second fragment considering the screenshots below.

First Fragment

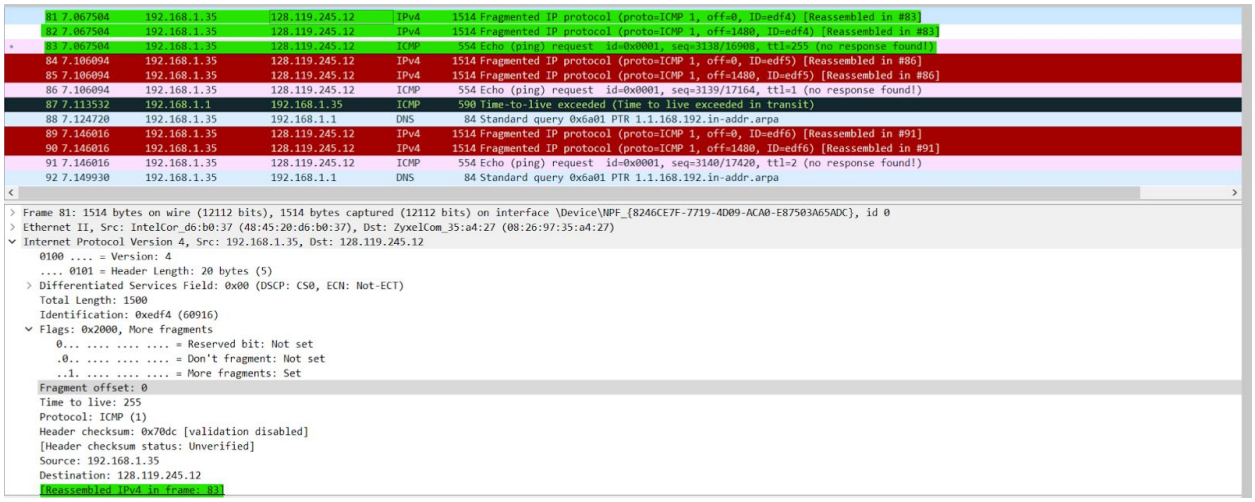


Second Fragment



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

ANS: As you can see from the below screenshot original datagram fragmented to 3 packets.



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

ANS:

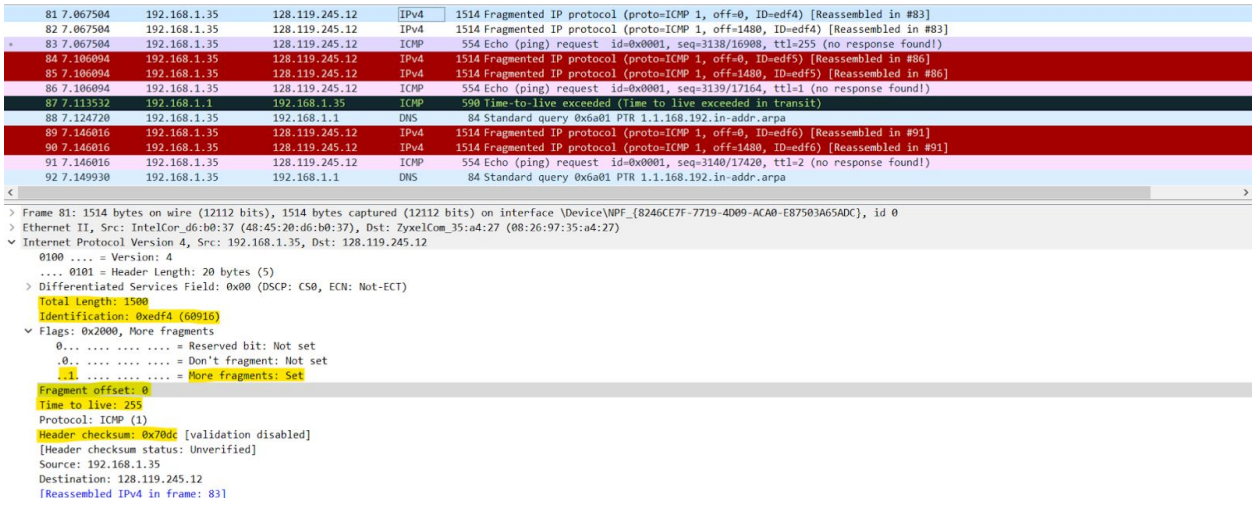
All fragments have different fragment offset and header checksum.

All fragments have the same TTL and identification number.

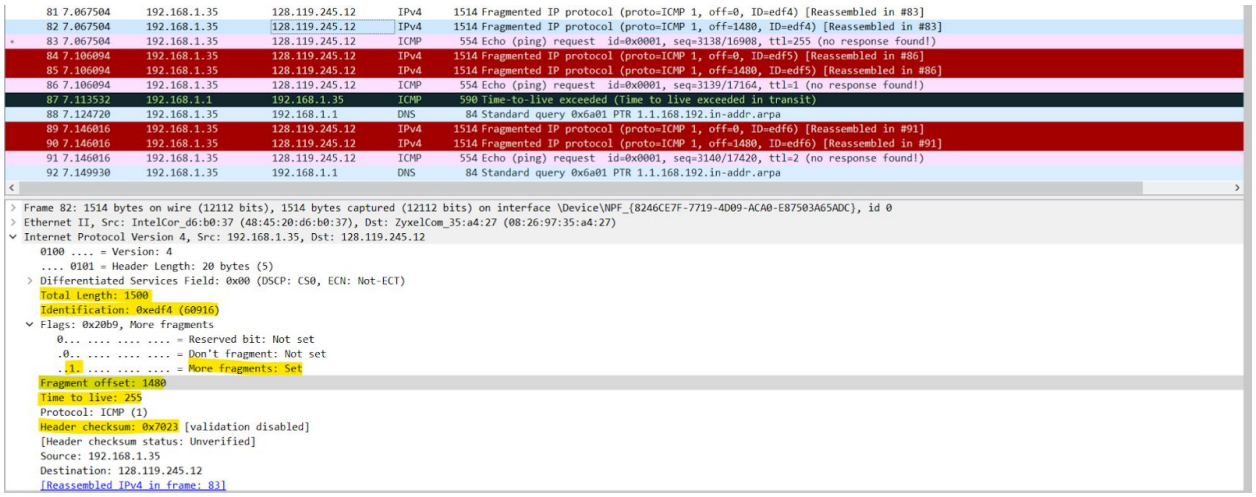
Fragment 1 and fragment 2 have the same total length and same More fragments bit.

So total length, fragment offset, header checksum and More fragments bit changed between these 3 fragments as you can see below screenshots.

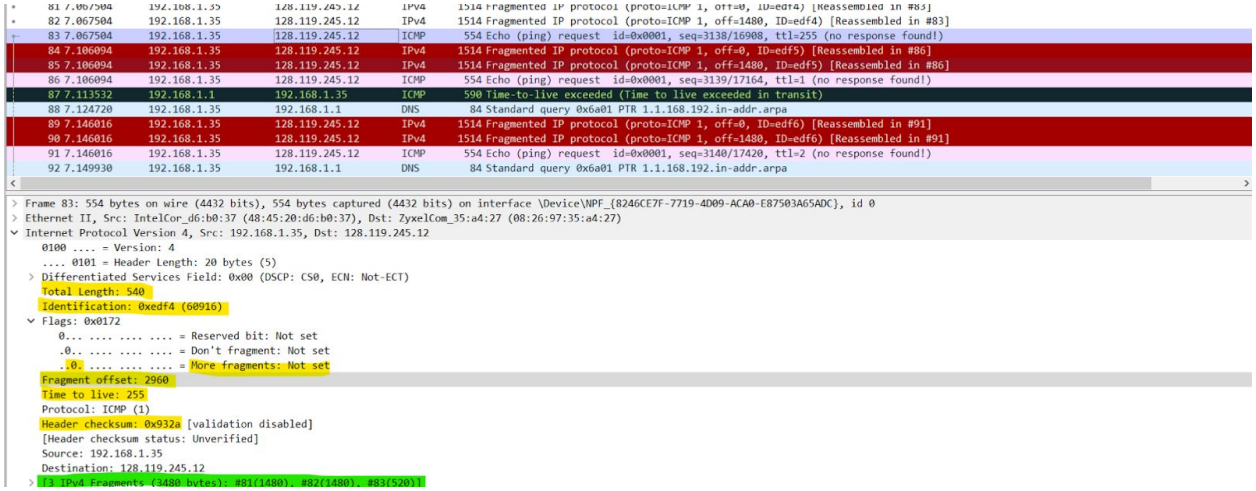
Fragment 1



Fragment 2



Fragment3


81 7.067504 192.168.1.35 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf4) [Reassembled in #83]
82 7.067504 192.168.1.35 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf4) [Reassembled in #83]
83 7.067504 192.168.1.35 128.119.245.12 ICMP 554 Echo (ping) request id=0x0001, seq=3138/16908, ttl=255 (no response found!)
84 7.106094 192.168.1.35 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf5) [Reassembled in #86]
85 7.106094 192.168.1.35 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf5) [Reassembled in #86]
86 7.106094 192.168.1.35 128.119.245.12 ICMP 554 Echo (ping) request id=0x0001, seq=3139/17164, ttl=1 (no response found!)
87 7.113532 192.168.1.1 192.168.1.35 ICMP 590 Time-to-live exceeded (Time to live exceeded in transit)
88 7.124720 192.168.1.35 192.168.1.1 DNS 84 Standard query 0x6a01 PTR 1.1.168.192.in-addr.arpa
89 7.146016 192.168.1.35 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=edf6) [Reassembled in #91]
90 7.146016 192.168.1.35 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=edf6) [Reassembled in #91]
91 7.146016 192.168.1.35 128.119.245.12 ICMP 554 Echo (ping) request id=0x0001, seq=3140/17420, ttl=2 (no response found!)
92 7.149930 192.168.1.35 192.168.1.1 DNS 84 Standard query 0x6a01 PTR 1.1.168.192.in-addr.arpa
Frame 83: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \Device\NPF_{8246CE7F-7719-4D09-ACA0-E87503A65ADC}, id 0
Ethernet II, Src: IntelCor_d6:b0:37 (48:45:20:d6:b0:37), Dst: ZyxelCom_35:a4:27 (08:26:97:35:a4:27)
Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 540
Identification: 0xedf4 (60916)
Flags: 0x0172
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
Fragment offset: 2960
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0x932a [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.35
Destination: 128.119.245.12
[3 IPv4 Fragments (3480 bytes): #81(1480), #82(1480), #83(520)]