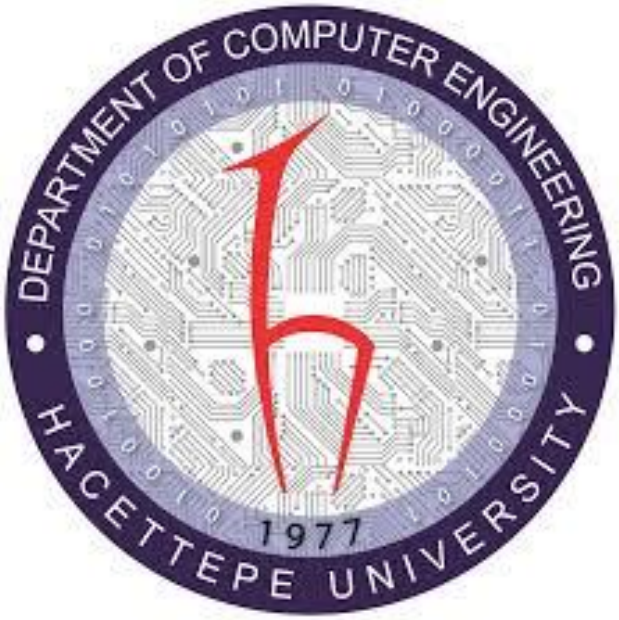
HACETTEPE UNIVERSITY

COMPUTER ENGINEERING DEPARTMENT

COMPUTER NETWORKS LABORATORY



EXPERIMENT IP

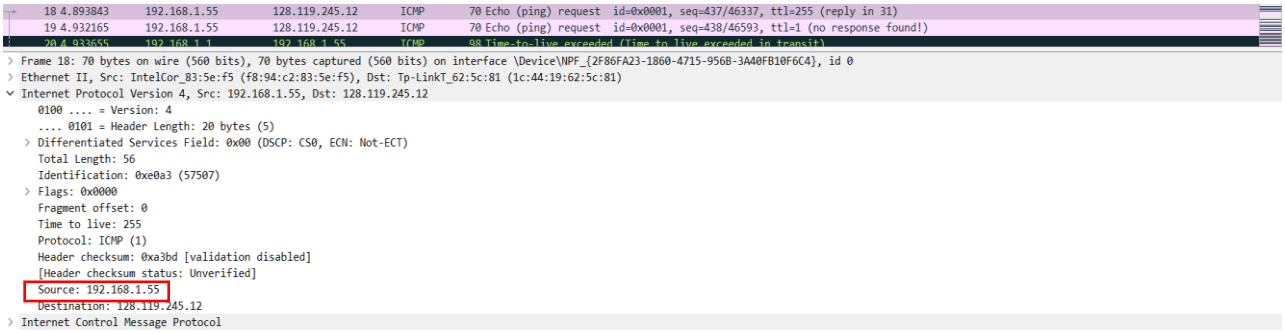
Deniz Ece AKTAŞ 21626901

Ece OMURTAY 21627543

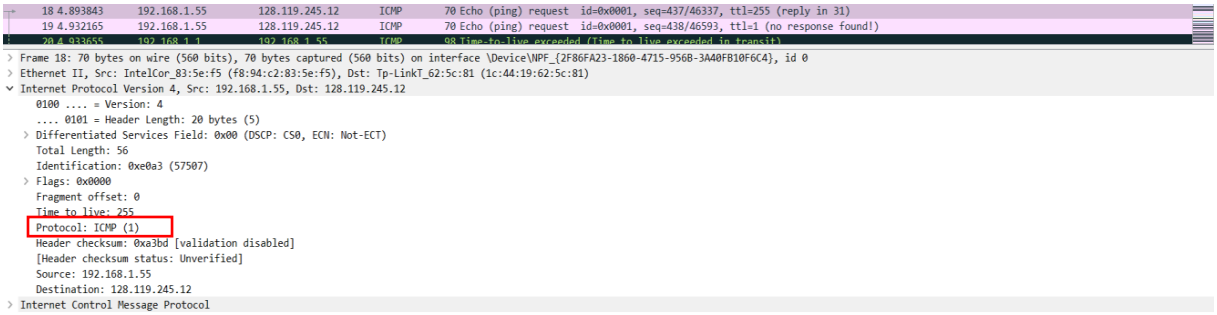
GROUP NUMBER : 12

IP address of our computer: 192.168.1.55

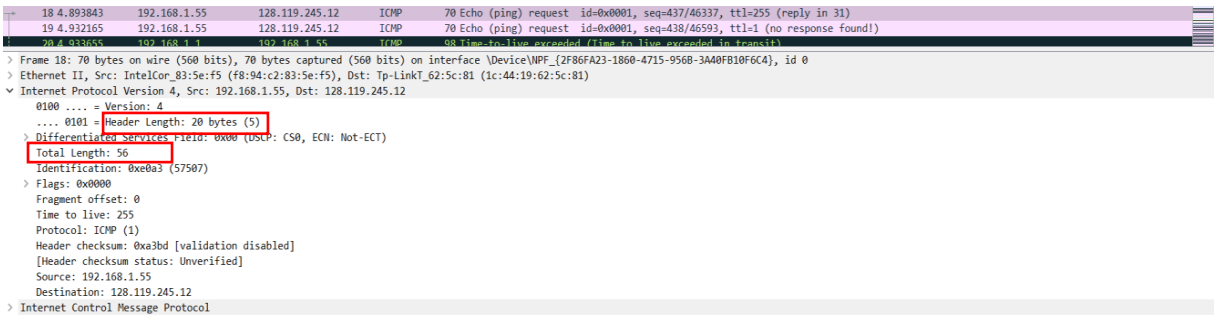
1.The IP address of our computer is:192.168.1.55



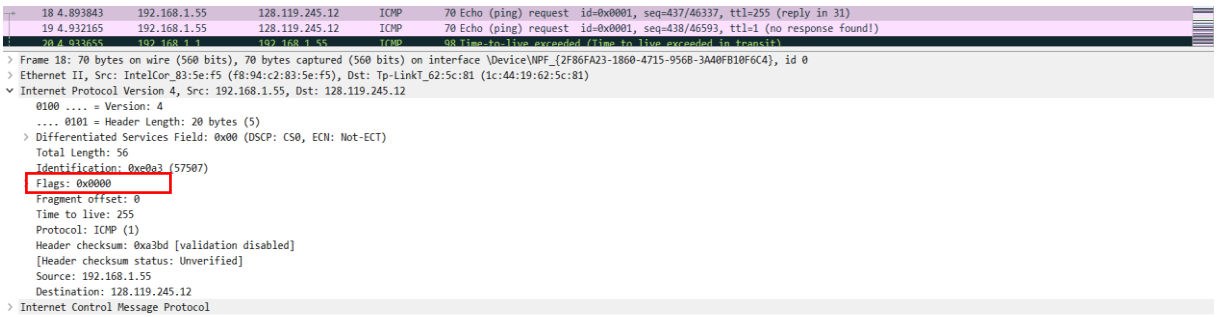
2.Within the IP package header, the value in upper layer protocol field is ICMP(1).



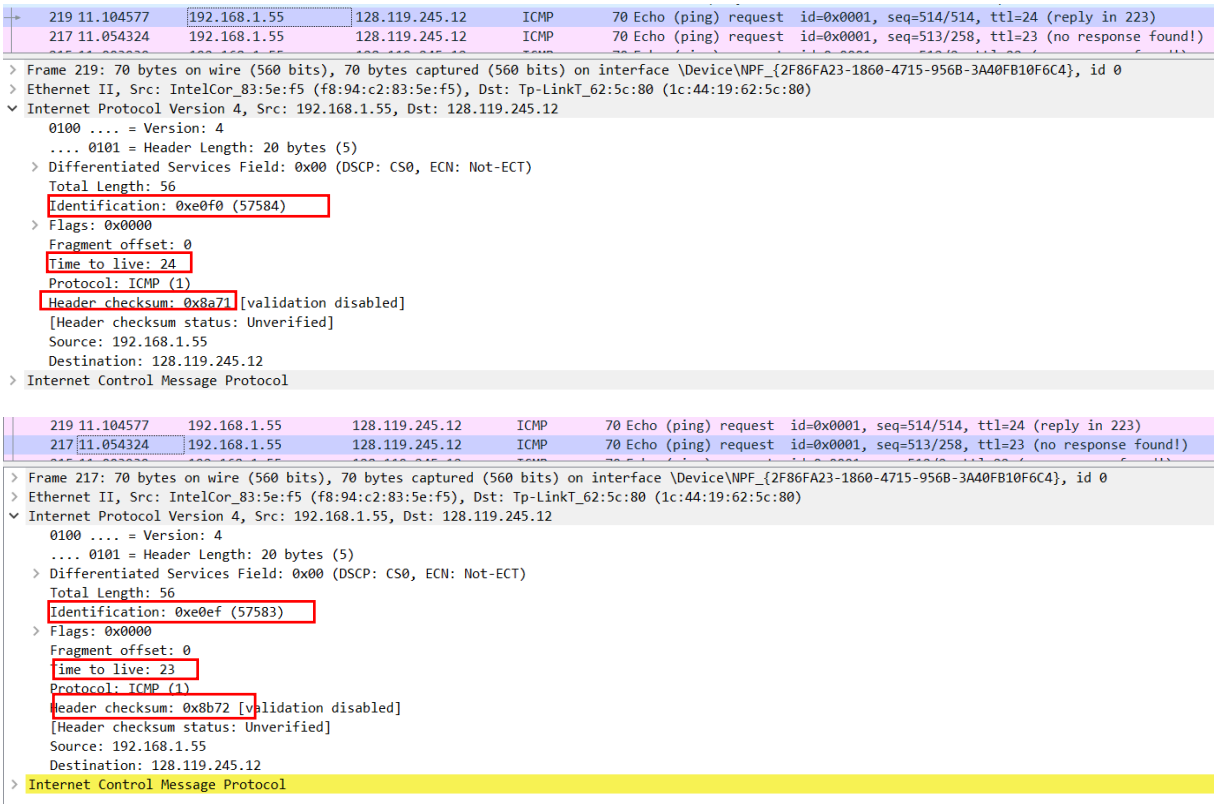
3.There are 20 bytes in the IP header, 56 bytes in total length so 56-20=36 bytes is the payload bytes.



4. The fragments bit is equal to 0, so the data is not fragmented.



5. The Identification field, time to live field and header checksum fields change.

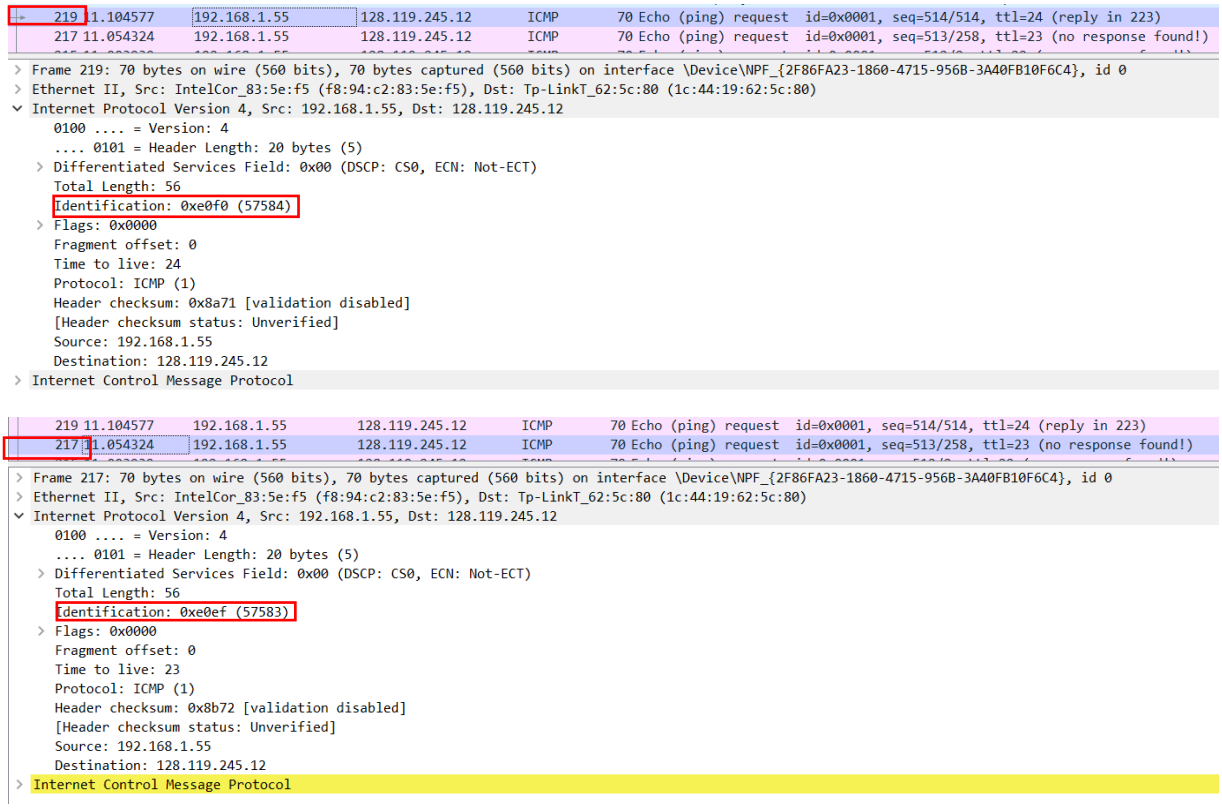


6.The constant fields are; version because IPv4 usage is continuous, header length because ICMP packets stay the same length, source IP because source doesn't change, destination IP because destination doesn't change, Upper Layer protocol because ICMP stays the same, differentiated services because ICMP use same type of service class.

The fields that must stay constant are; version because IPv4 usage is continuous, header length because ICMP packets stay the same length, source IP because source doesn't change, destination IP because destination doesn't change, Upper Layer protocol because ICMP stays the same, differentiated services because ICMP use same type of service class.

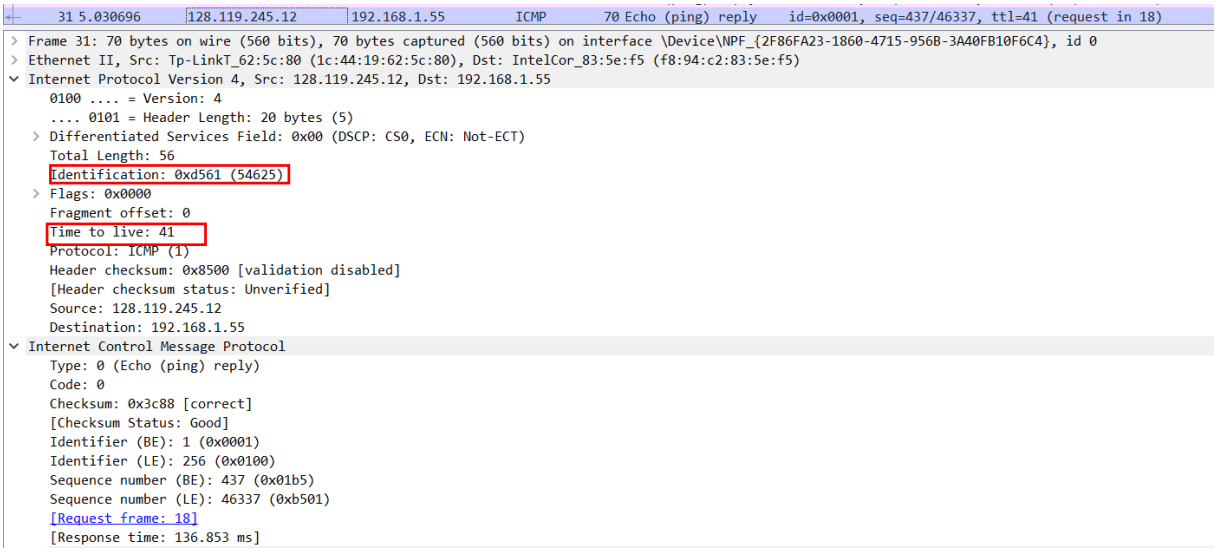
The fields that must change are; Identification because IP packets have different identifications, time to live field because traceroute gets one less each packet, header checksum because headers change.

7.The pattern is Identification increments with each ping.



8.Identification:54625

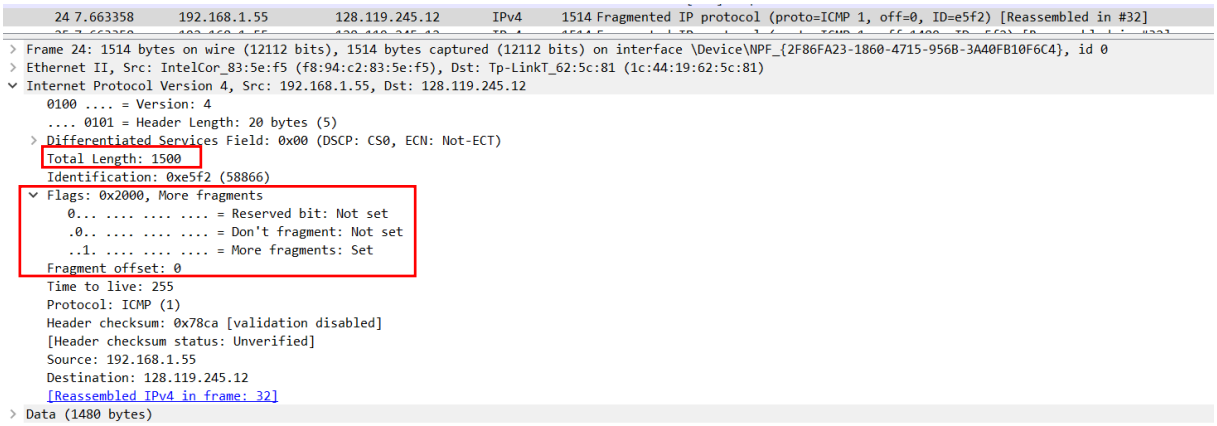
TTL:41



9. The identification changes for every value if 2 IP datagrams have the same identification value then it means that IP datagrams are fragment parts of a large IP datagram.

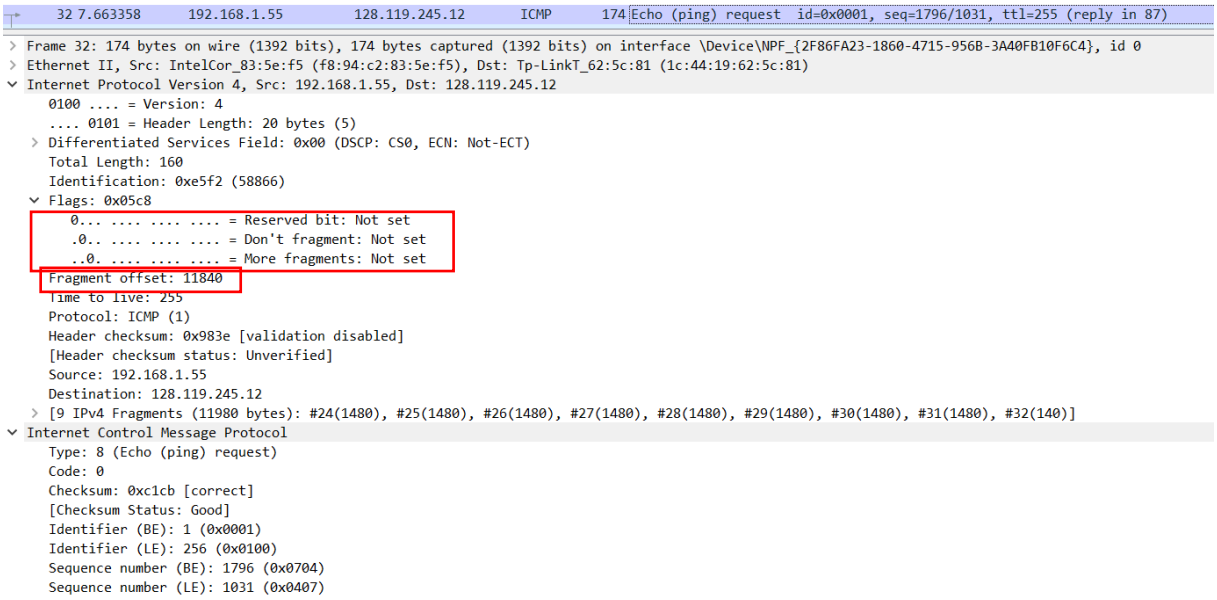
The time to live stays same because TTL for first hop router is the same.

10. Yes, the packet have been fragmented across more than one IP datagram.



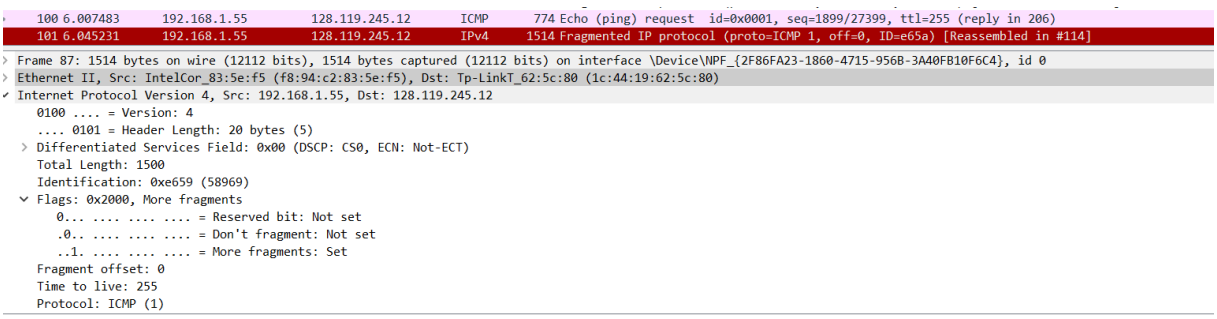
11. The Flags field is 0x2000 and more fragments part is set and this shows that the datagram has been fragmented. Because the fragment offset is 0, this is the first fragment and the total length is 1500 bytes as shown above.

12. This is not the first fragment because the fragment offset is 11840. This is the last fragment because the more fragments field is not set.



13. Fields that have changed are; total length, flags, fragment offset, header checksum as shown above.

14. From the start of the first fragment to the reply point there are 5 packets created from the original datagram.



```
205 6.202832    128.119.245.12    192.168.1.55    IPv4    1466 Fragmented IP protocol (proto=ICMP 1, off=17808, ID=c895) [Reassembled in #206]
206 6.202832    128.119.245.12    192.168.1.55    ICMP     774 Echo (ping) reply    id=0x0001, seq=1899/27399, ttl=41 (request in 100)
```

15. The fields that have changed are; fragment offset, and header checksum values. Also at the last fragments last packet total length is set to 760 bytes, we know that this is the last package because the more fragment field is not set and is 0.

```
87 6.007483    192.168.1.55    128.119.245.12    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e659) [Reassembled in #100]
88 6.007483    192.168.1.55    128.119.245.12    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=e659) [Reassembled in #100]
> Frame 87: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40FB10F6C4}, id 0
> Ethernet II, Src: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5), Dst: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80)
v Internet Protocol Version 4, Src: 192.168.1.55, 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: 1500
    Identification: 0xe659 (58969)
  v Flags: 0x2000, More fragments
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..1. .... .... .... = More fragments: Set
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x7863 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.55
    Destination: 128.119.245.12
    [Reassembled IPv4 in frame: 100]
> Data (1480 bytes)
```

```
206 6.202832    128.119.245.12    192.168.1.55    ICMP     774 Echo (ping) reply    id=0x0001, seq=1899/27399, ttl=41 (request in 100)
> Frame 206: 774 bytes on wire (6192 bits), 774 bytes captured (6192 bits) on interface \Device\NPF_{2F86FA23-1860-4715-956B-3A40FB10F6C4}, id 0
> Ethernet II, Src: Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80), Dst: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5)
v Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.55
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 760
    Identification: 0xc895 (51349)
  v Flags: 0x0965
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set
    Fragment offset: 19240
    Time to live: 41
    Protocol: ICMP (1)
    Header checksum: 0x85a7 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 192.168.1.55
```