LAB-11

Name: Vanani Prince

Roll no: CE175

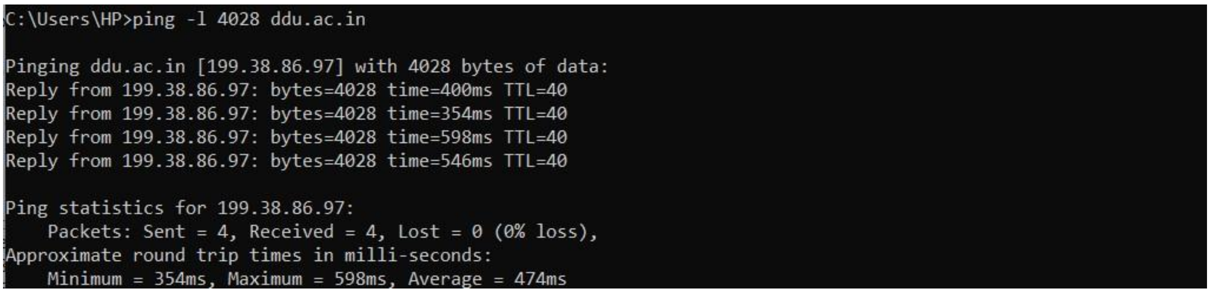
Aim: Understanding functionalities of various layers using Wireshark

1.packet fragmentation in Wireshark

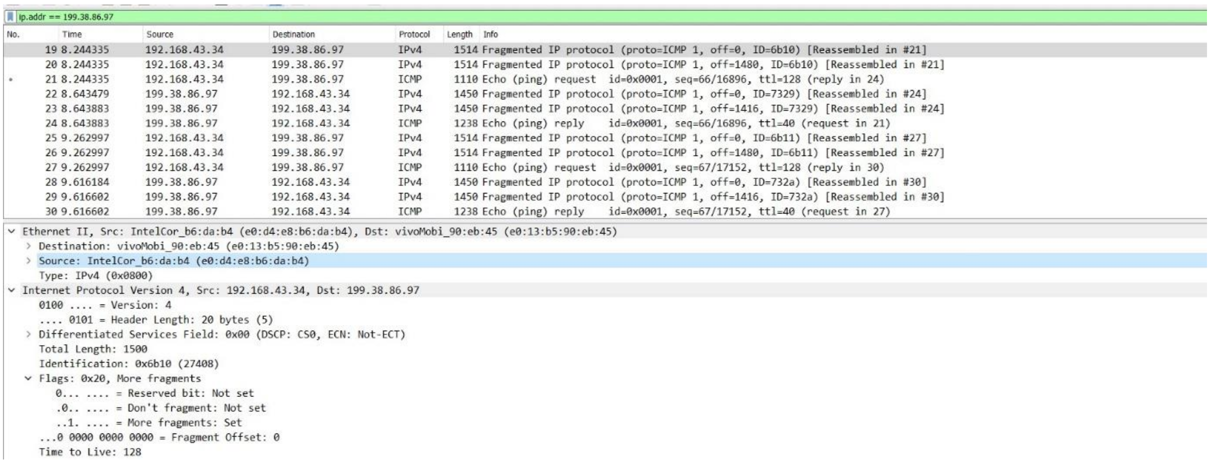
-whenever we send packet using ping command and if it is more than 1500 bytes then fragmentation take place.

-we send size of 4028-bytes packet at destination ddu.ac.in

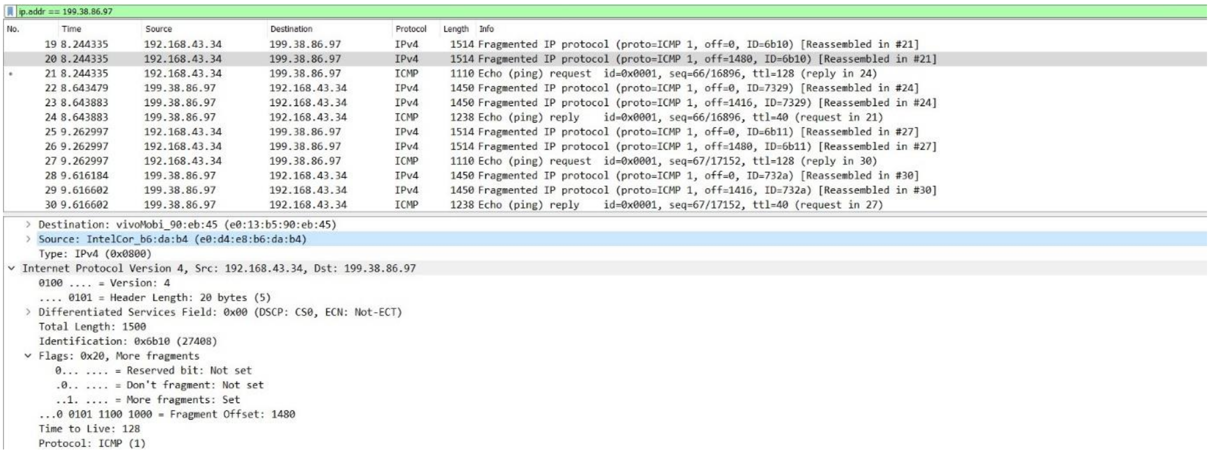
-As you can see fragmentation take place because size is more than 1500 bytes. In this all fragments have same identification field. It indicates all the fragment belong to same packet. In all fragments have more fragment flag set (1) except last fragment because more fragment flag reset (0) indicates it is last fragment in packet. There is also 13 bits fragment offset. it indicates how much data is there before that fragment.



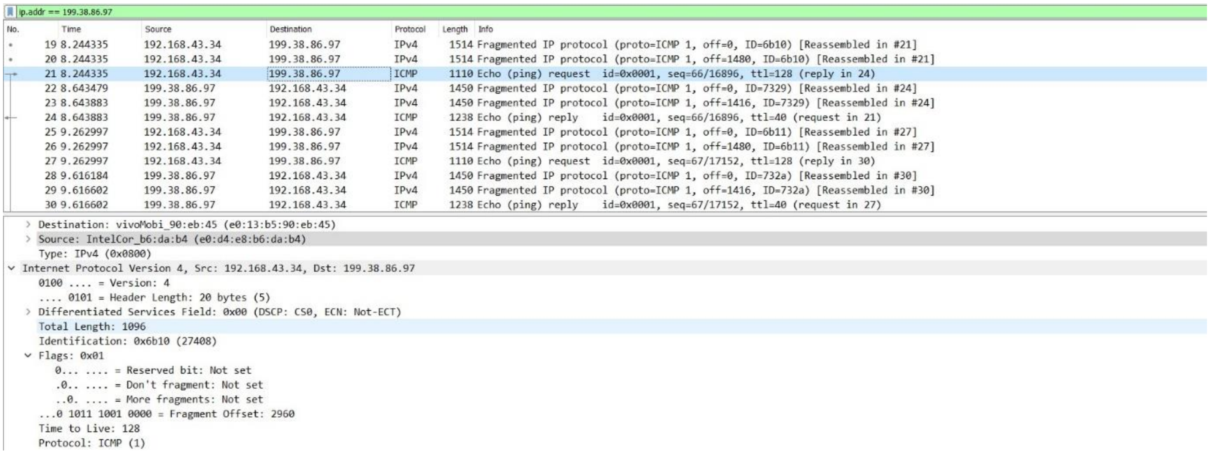
```
C:\Users\HP>ping -l 4028 ddu.ac.in

Pinging ddu.ac.in [199.38.86.97] with 4028 bytes of data:
Reply from 199.38.86.97: bytes=4028 time=400ms TTL=40
Reply from 199.38.86.97: bytes=4028 time=354ms TTL=40
Reply from 199.38.86.97: bytes=4028 time=598ms TTL=40
Reply from 199.38.86.97: bytes=4028 time=546ms TTL=40

Ping statistics for 199.38.86.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 354ms, Maximum = 598ms, Average = 474ms
```



```
ip.addr == 199.38.86.97
No.     Time       Source          Destination     Protocol  Length  Info
    19 8.244335   192.168.43.34   199.38.86.97    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6b10) [Reassembled in #21]
    20 8.244335   192.168.43.34   199.38.86.97    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=6b10) [Reassembled in #21]
    21 8.244335   192.168.43.34   199.38.86.97    ICMP      1110 Echo (ping) request  id=0x0001, seq=66/16896, ttl=128 (reply in 24)
    22 8.643479   199.38.86.97    192.168.43.34   IPv4      1450 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7329) [Reassembled in #24]
    23 8.643883   199.38.86.97    192.168.43.34   IPv4      1450 Fragmented IP protocol (proto=ICMP 1, off=1416, ID=7329) [Reassembled in #24]
    24 8.643883   199.38.86.97    192.168.43.34   ICMP      1238 Echo (ping) reply    id=0x0001, seq=66/16896, ttl=40 (request in 21)
    25 9.262997   192.168.43.34   199.38.86.97    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6b11) [Reassembled in #27]
    26 9.262997   192.168.43.34   199.38.86.97    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=6b11) [Reassembled in #27]
    27 9.262997   192.168.43.34   199.38.86.97    ICMP      1110 Echo (ping) request  id=0x0001, seq=67/17152, ttl=128 (reply in 30)
    28 9.616184   199.38.86.97    192.168.43.34   IPv4      1450 Fragmented IP protocol (proto=ICMP 1, off=0, ID=732a) [Reassembled in #30]
    29 9.616602   199.38.86.97    192.168.43.34   IPv4      1450 Fragmented IP protocol (proto=ICMP 1, off=1416, ID=732a) [Reassembled in #30]
    30 9.616602   199.38.86.97    192.168.43.34   ICMP      1238 Echo (ping) reply    id=0x0001, seq=67/17152, ttl=40 (request in 27)

v Ethernet II, Src: IntelCor_b6:da:b4 (e0:d4:e8:b6:da:b4), Dst: vivoMobi_90:eb:45 (e0:13:b5:90:eb:45)
  > Destination: vivoMobi_90:eb:45 (e0:13:b5:90:eb:45)
  > Source: IntelCor_b6:da:b4 (e0:d4:e8:b6:da:b4)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.43.34, Dst: 199.38.86.97
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x6b10 (27408)
  v Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
```



```
ip.addr == 199.38.86.97
No.     Time       Source          Destination     Protocol  Length  Info
    19 8.244335   192.168.43.34   199.38.86.97    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6b10) [Reassembled in #21]
    20 8.244335   192.168.43.34   199.38.86.97    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=6b10) [Reassembled in #21]
    21 8.244335   192.168.43.34   199.38.86.97    ICMP      1110 Echo (ping) request  id=0x0001, seq=66/16896, ttl=128 (reply in 24)
    22 8.643479   199.38.86.97    192.168.43.34   IPv4      1450 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7329) [Reassembled in #24]
    23 8.643883   199.38.86.97    192.168.43.34   IPv4      1450 Fragmented IP protocol (proto=ICMP 1, off=1416, ID=7329) [Reassembled in #24]
    24 8.643883   199.38.86.97    192.168.43.34   ICMP      1238 Echo (ping) reply    id=0x0001, seq=66/16896, ttl=40 (request in 21)
    25 9.262997   192.168.43.34   199.38.86.97    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6b11) [Reassembled in #27]
    26 9.262997   192.168.43.34   199.38.86.97    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=6b11) [Reassembled in #27]
    27 9.262997   192.168.43.34   199.38.86.97    ICMP      1110 Echo (ping) request  id=0x0001, seq=67/17152, ttl=128 (reply in 30)
    28 9.616184   199.38.86.97    192.168.43.34   IPv4      1450 Fragmented IP protocol (proto=ICMP 1, off=0, ID=732a) [Reassembled in #30]
    29 9.616602   199.38.86.97    192.168.43.34   IPv4      1450 Fragmented IP protocol (proto=ICMP 1, off=1416, ID=732a) [Reassembled in #30]
    30 9.616602   199.38.86.97    192.168.43.34   ICMP      1238 Echo (ping) reply    id=0x0001, seq=67/17152, ttl=40 (request in 27)

  > Destination: vivoMobi_90:eb:45 (e0:13:b5:90:eb:45)
  > Source: IntelCor_b6:da:b4 (e0:d4:e8:b6:da:b4)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.43.34, Dst: 199.38.86.97
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x6b10 (27408)
  v Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0101 1100 1000 = Fragment Offset: 1480
    Time to Live: 128
    Protocol: ICMP (1)
```



```
ip.addr == 199.38.86.97
No.     Time       Source          Destination     Protocol  Length  Info
    19 8.244335   192.168.43.34   199.38.86.97    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6b10) [Reassembled in #21]
    20 8.244335   192.168.43.34   199.38.86.97    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=6b10) [Reassembled in #21]
    21 8.244335   192.168.43.34   199.38.86.97    ICMP      1110 Echo (ping) request  id=0x0001, seq=66/16896, ttl=128 (reply in 24)
    22 8.643479   199.38.86.97    192.168.43.34   IPv4      1450 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7329) [Reassembled in #24]
    23 8.643883   199.38.86.97    192.168.43.34   IPv4      1450 Fragmented IP protocol (proto=ICMP 1, off=1416, ID=7329) [Reassembled in #24]
    24 8.643883   199.38.86.97    192.168.43.34   ICMP      1238 Echo (ping) reply    id=0x0001, seq=66/16896, ttl=40 (request in 21)
    25 9.262997   192.168.43.34   199.38.86.97    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=6b11) [Reassembled in #27]
    26 9.262997   192.168.43.34   199.38.86.97    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=6b11) [Reassembled in #27]
    27 9.262997   192.168.43.34   199.38.86.97    ICMP      1110 Echo (ping) request  id=0x0001, seq=67/17152, ttl=128 (reply in 30)
    28 9.616184   199.38.86.97    192.168.43.34   IPv4      1450 Fragmented IP protocol (proto=ICMP 1, off=0, ID=732a) [Reassembled in #30]
    29 9.616602   199.38.86.97    192.168.43.34   IPv4      1450 Fragmented IP protocol (proto=ICMP 1, off=1416, ID=732a) [Reassembled in #30]
    30 9.616602   199.38.86.97    192.168.43.34   ICMP      1238 Echo (ping) reply    id=0x0001, seq=67/17152, ttl=40 (request in 27)

  > Destination: vivoMobi_90:eb:45 (e0:13:b5:90:eb:45)
  > Source: IntelCor_b6:da:b4 (e0:d4:e8:b6:da:b4)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.43.34, Dst: 199.38.86.97
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1096
    Identification: 0x6b10 (27408)
  v Flags: 0x01
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 1011 1001 0000 = Fragment Offset: 2960
    Time to Live: 128
    Protocol: ICMP (1)
```

2. IPv4 header checksum verification in Wireshark

- we send size of 16-bytes packet at destination ddu.ac.in

- Packet contain IPv4 header and in this header, there is one field checksum. It will use to ensure data integrity.

-we calculate IPv4 header checksum manually and compare with this field whether it is equal or not

-

1 2 2

4 5 0 0

0 0 2 C

E A 6 8

0 0 0 0

8 0 0 1

0 0 0 0

C 0 A 8

0 1 6 5

C 7 2 6

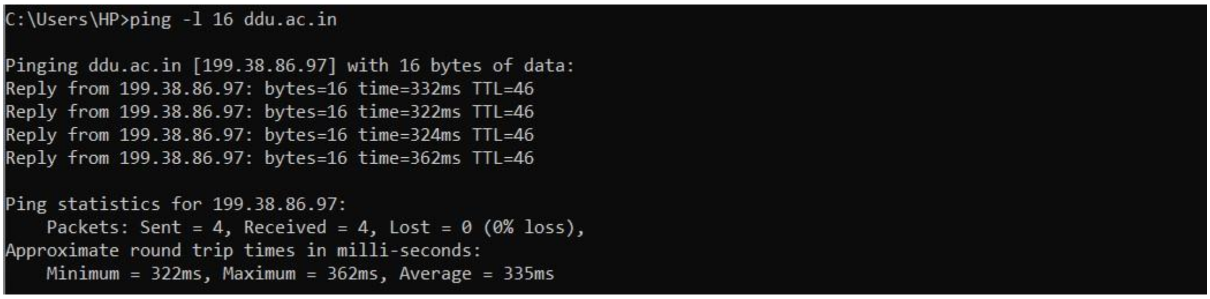
5 6 6 1

----

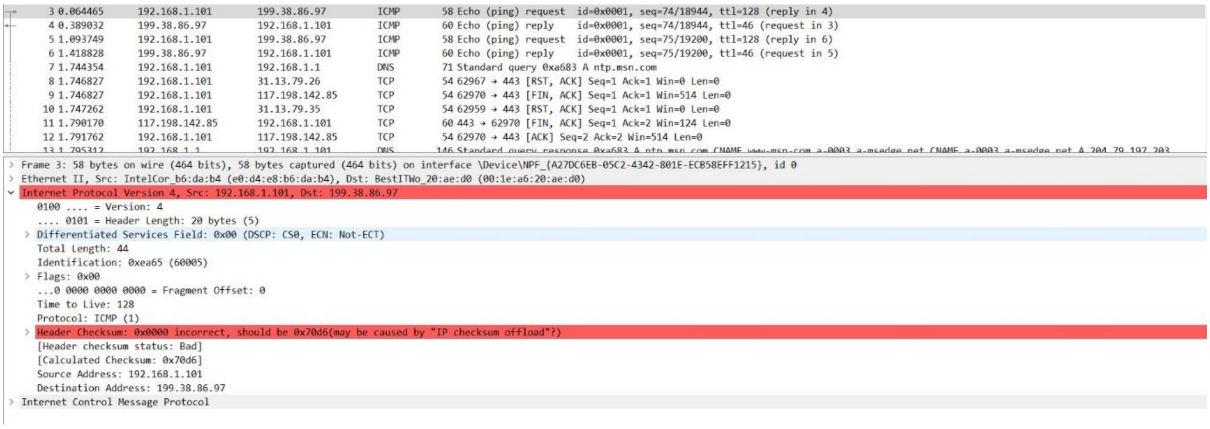
8 F 2 9 (sum)

7 0 D 6 (checksum)

-In this packet checksum field shows 0000 but we get 70D6 that’s why this is incorrect



```
C:\Users\HP>ping -l 16 ddu.ac.in

Pinging ddu.ac.in [199.38.86.97] with 16 bytes of data:
Reply from 199.38.86.97: bytes=16 time=332ms TTL=46
Reply from 199.38.86.97: bytes=16 time=322ms TTL=46
Reply from 199.38.86.97: bytes=16 time=324ms TTL=46
Reply from 199.38.86.97: bytes=16 time=362ms TTL=46

Ping statistics for 199.38.86.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 322ms, Maximum = 362ms, Average = 335ms
```



```
     3 0.064465   192.168.1.101    199.38.86.97     ICMP    58 Echo (ping) request  id=0x0001, seq=74/18944, ttl=128 (reply in 4)
     4 0.389032   199.38.86.97     192.168.1.101    ICMP    60 Echo (ping) reply    id=0x0001, seq=74/18944, ttl=46 (request in 3)
     5 1.093749   192.168.1.101    199.38.86.97     ICMP    58 Echo (ping) request  id=0x0001, seq=75/19200, ttl=128 (reply in 6)
     6 1.418828   199.38.86.97     192.168.1.101    ICMP    60 Echo (ping) reply    id=0x0001, seq=75/19200, ttl=46 (request in 5)
     7 1.744354   192.168.1.101    192.168.1.1      DNS     71 Standard query 0xa683 A ntp.msn.com
     8 1.746827   192.168.1.101    31.13.79.26      TCP     54 62967 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
     9 1.746827   192.168.1.101    117.198.142.85   TCP     54 62970 → 443 [FIN, ACK] Seq=1 Ack=1 Win=514 Len=0
    10 1.747262   192.168.1.101    31.13.79.35      TCP     54 62959 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    11 1.790170   117.198.142.85   192.168.1.101    TCP     60 443 → 62970 [FIN, ACK] Seq=1 Ack=2 Win=124 Len=0
    12 1.791762   192.168.1.101    117.198.142.85   TCP     54 62970 → 443 [ACK] Seq=2 Ack=2 Win=514 Len=0
    13 1.795312   192.168.1.1      192.168.1.101    DNS    146 Standard query response 0xa683 A ntp.msn.com CNAME www-msn-com.a-0003.a-msedge.net CNAME a-0003.a-msedge.net A 204.79.197.203
> Frame 3: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface \Device\NPF_{A27DC6EB-05C2-4342-801E-ECB58EFF1215}, id 0
> Ethernet II, Src: IntelCor_b6:da:b4 (e0:d4:e8:b6:da:b4), Dst: BestITWo_20:ae:d0 (00:1e:a6:20:ae:d0)
v Internet Protocol Version 4, Src: 192.168.1.101, Dst: 199.38.86.97
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 44
    Identification: 0xea65 (60005)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
  > Header Checksum: 0x0000 incorrect, should be 0x70d6(may be caused by "IP checksum offload"?)
    [Header checksum status: Bad]
    [Calculated Checksum: 0x70d6]
    Source Address: 192.168.1.101
    Destination Address: 199.38.86.97
> Internet Control Message Protocol
```

3. Padding in Wireshark

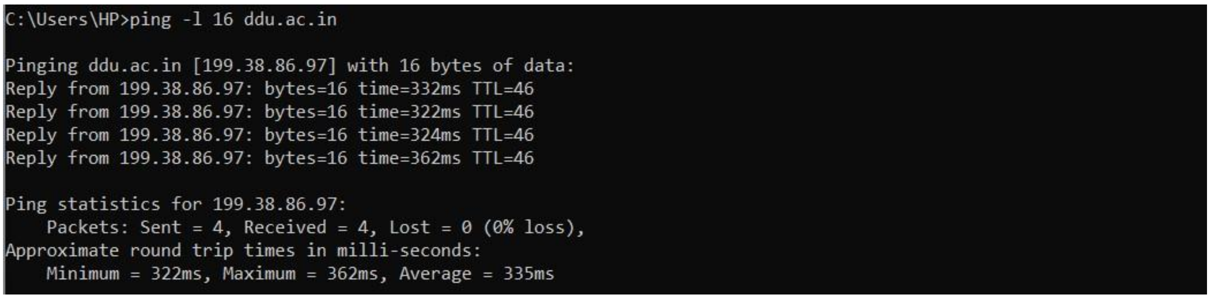
- whenever we send packet using ping command and if it is less than 18 bytes then padding take place.

-we send size of 16-bytes packet at destination ddu.ac.in

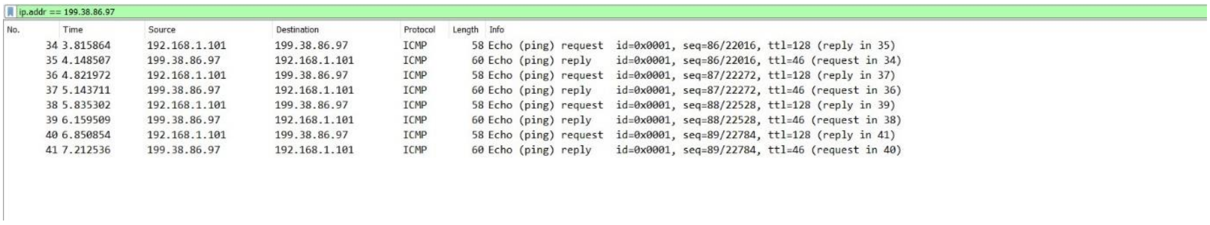
- Please note that Wireshark omits the 4 last bytes of frame names FCS (Frame Check Sequence) which is used to detect corrupted frames. Thus, you see 60 bytes instead of 64 bytes.

-As you can see in request length is 58 bytes means 20 bytes of IPv4 header + 8 bytes ICMP header+18 bytes are necessary in Ethernet +16 bytes of data – 4 bytes are omitted by Wireshark.

-As you can see in reply length is 60 bytes means 2 bytes of padding added and 4 bytes are omitted by Wireshark and we finally get frame length 64 bytes.



```
C:\Users\HP>ping -l 16 ddu.ac.in

Pinging ddu.ac.in [199.38.86.97] with 16 bytes of data:
Reply from 199.38.86.97: bytes=16 time=332ms TTL=46
Reply from 199.38.86.97: bytes=16 time=322ms TTL=46
Reply from 199.38.86.97: bytes=16 time=324ms TTL=46
Reply from 199.38.86.97: bytes=16 time=362ms TTL=46

Ping statistics for 199.38.86.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 322ms, Maximum = 362ms, Average = 335ms
```



ip.addr == 199.38.86.97

No.	Time	Source	Destination	Protocol	Length	Info
34	3.815864	192.168.1.101	199.38.86.97	ICMP	58	Echo (ping) request id=0x0001, seq=86/22016, ttl=128 (reply in 35)
35	4.148507	199.38.86.97	192.168.1.101	ICMP	60	Echo (ping) reply id=0x0001, seq=86/22016, ttl=46 (request in 34)
36	4.821972	192.168.1.101	199.38.86.97	ICMP	58	Echo (ping) request id=0x0001, seq=87/22272, ttl=128 (reply in 37)
37	5.143711	199.38.86.97	192.168.1.101	ICMP	60	Echo (ping) reply id=0x0001, seq=87/22272, ttl=46 (request in 36)
38	5.835302	192.168.1.101	199.38.86.97	ICMP	58	Echo (ping) request id=0x0001, seq=88/22528, ttl=128 (reply in 39)
39	6.159509	199.38.86.97	192.168.1.101	ICMP	60	Echo (ping) reply id=0x0001, seq=88/22528, ttl=46 (request in 38)
40	6.850854	192.168.1.101	199.38.86.97	ICMP	58	Echo (ping) request id=0x0001, seq=89/22784, ttl=128 (reply in 41)
41	7.212536	199.38.86.97	192.168.1.101	ICMP	60	Echo (ping) reply id=0x0001, seq=89/22784, ttl=46 (request in 40)