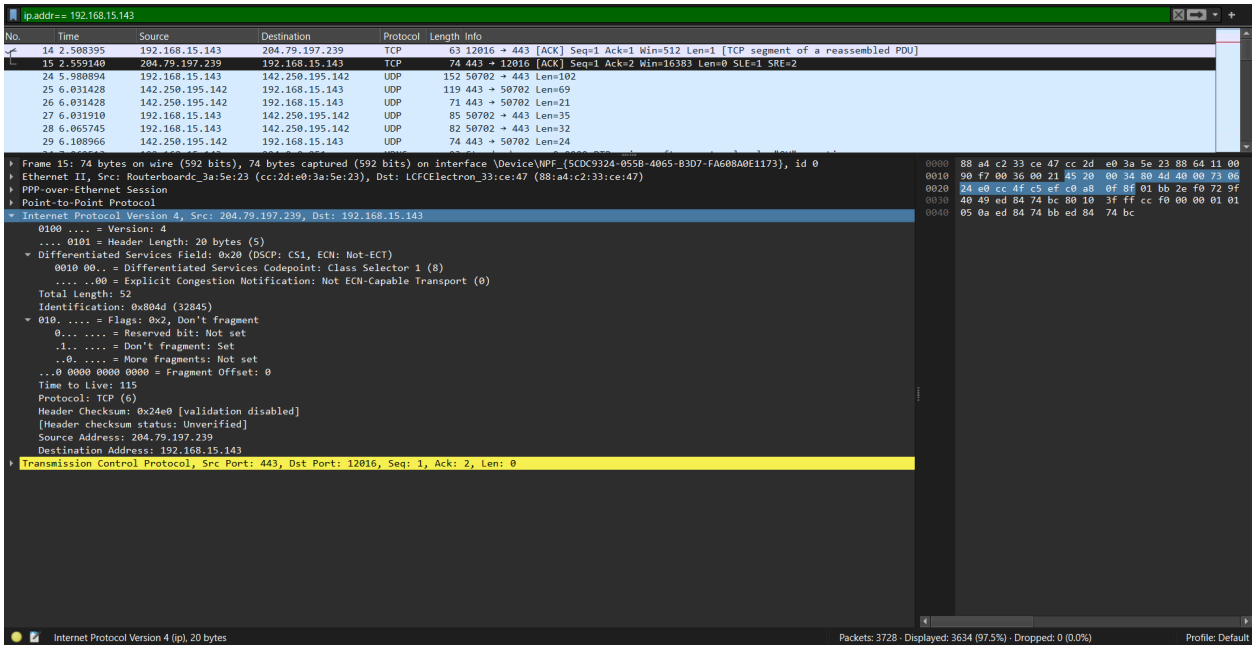
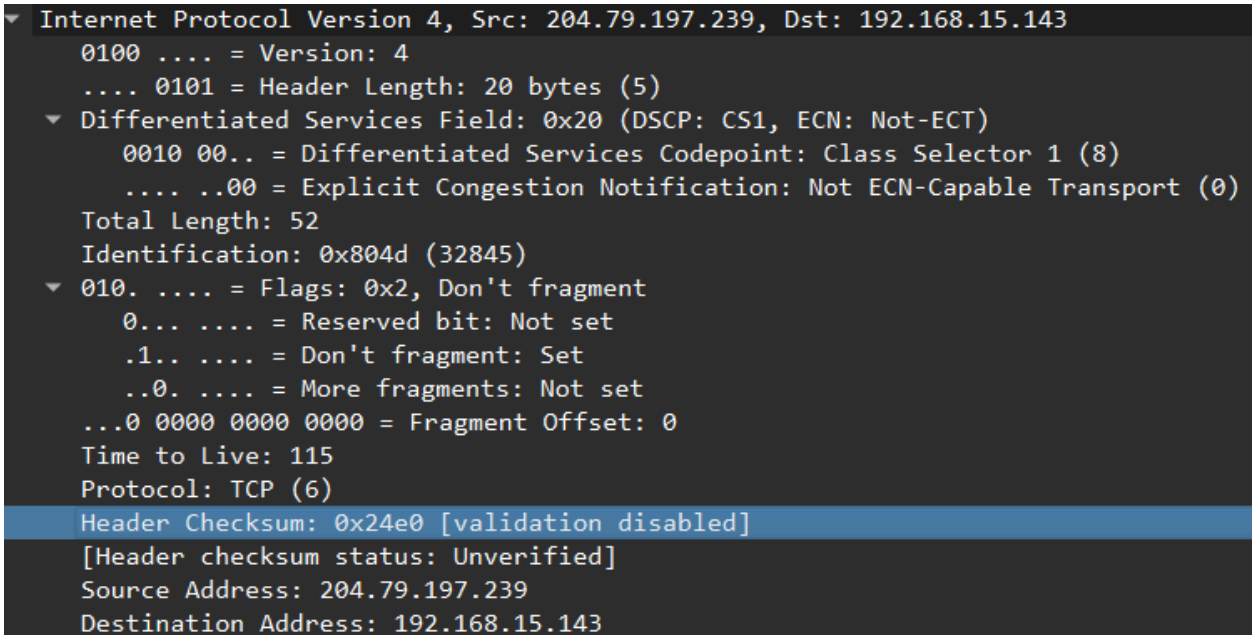
Q. Capture an IPv4 packet in wireshark, list out all of the fields and their values. Calculate the checksum.





(2) Capture a TCP packet in wireshark & calculate the checksum

→ The captured packet is shown above:

→ The fields and their values are: (In hex)

1) Version : 4
2) Header length : 5
3) Differentiated Services Code Point (DSCP): 20
4) Explicit congestion Notification : 00
5) Total length : 34
6) Identification : 804d
7) Flags : 2 (Don't fragment) ~~0100 = 40~~ 2
8) Time to Live : 73
9) Protocol : 06 (TCP)
10) Header checksum: 0000 (for calculation)
11) Source address : cc:4f:c5:ef
12) Destination address : c0:a8:0f:8f

Now, we convent all of the fields value to binary and divide each of them to 16 bits & calculate the sum of the values one by one & adding the carry over back to the LSB of the sum (if there's carry).

Now, the bits are :-

4520 = 0100010100100000
0034 = 0000000000110100
804d = 1000000001001101
4000 = 0100000000000000
7306 = 0111001100000110
0000 = 0000000000000000
cc4f = 1100110001001111
c5ef = 1100010111101111
c0a8 = 1100000010101000
0f8f = 0000111110001111

Here, Sum is 3DB1C, Now adding carry to LSB we get, DB1F, Now, 1's complement is: 2420 which is check sum.