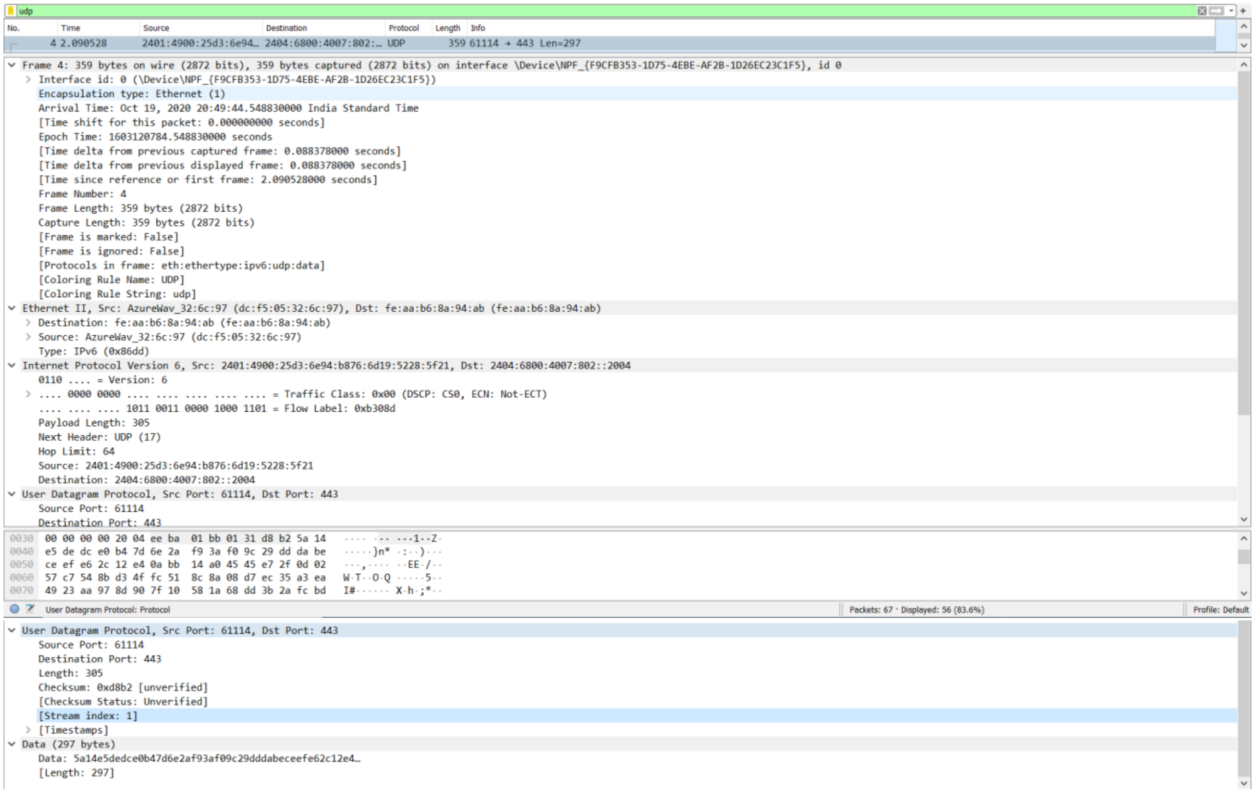
CSE 1004 - (Networks and Communications) LAB

Name: Karthick Raghul V ***Slot:L61+62***

Reg No: 19BCE1660

LAB – 11

1) Capture network traffic using Wireshark. Select one UDP or TCP packet from the captured network traffic.



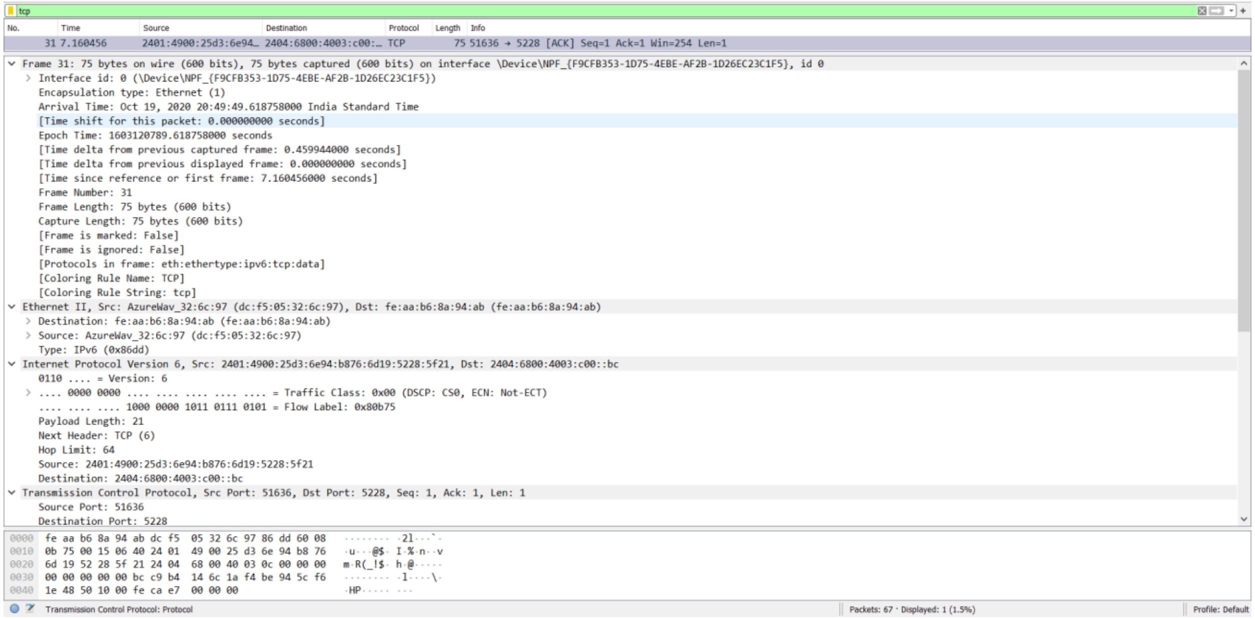
```
udp
No.   Time       Source                Destination           Protocol  Length  Info
    4 2.090528   2401:4900:25d3:6e94…  2404:6800:4007:802:…  UDP          359  61114 → 443 Len=297
```

```
v Frame 4: 359 bytes on wire (2872 bits), 359 bytes captured (2872 bits) on interface \Device\NPF_{F9CFB353-1D75-4EBE-AF2B-1D26EC23C1F5}, id 0
  > Interface id: 0 (\Device\NPF_{F9CFB353-1D75-4EBE-AF2B-1D26EC23C1F5})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 19, 2020 20:49:44.548830000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1603120784.548830000 seconds
    [Time delta from previous captured frame: 0.088378000 seconds]
    [Time delta from previous displayed frame: 0.088378000 seconds]
    [Time since reference or first frame: 2.090528000 seconds]
    Frame Number: 4
    Frame Length: 359 bytes (2872 bits)
    Capture Length: 359 bytes (2872 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:udp:data]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
v Ethernet II, Src: AzureWav_32:6c:97 (dc:f5:05:32:6c:97), Dst: fe:aa:b6:8a:94:ab (fe:aa:b6:8a:94:ab)
  > Destination: fe:aa:b6:8a:94:ab (fe:aa:b6:8a:94:ab)
  > Source: AzureWav_32:6c:97 (dc:f5:05:32:6c:97)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2401:4900:25d3:6e94:b876:6d19:5228:5f21, Dst: 2404:6800:4007:802::2004
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1011 0011 0000 1000 1101 = Flow Label: 0xb308d
    Payload Length: 305
    Next Header: UDP (17)
    Hop Limit: 64
    Source: 2401:4900:25d3:6e94:b876:6d19:5228:5f21
    Destination: 2404:6800:4007:802::2004
v User Datagram Protocol, Src Port: 61114, Dst Port: 443
    Source Port: 61114
    Destination Port: 443
```

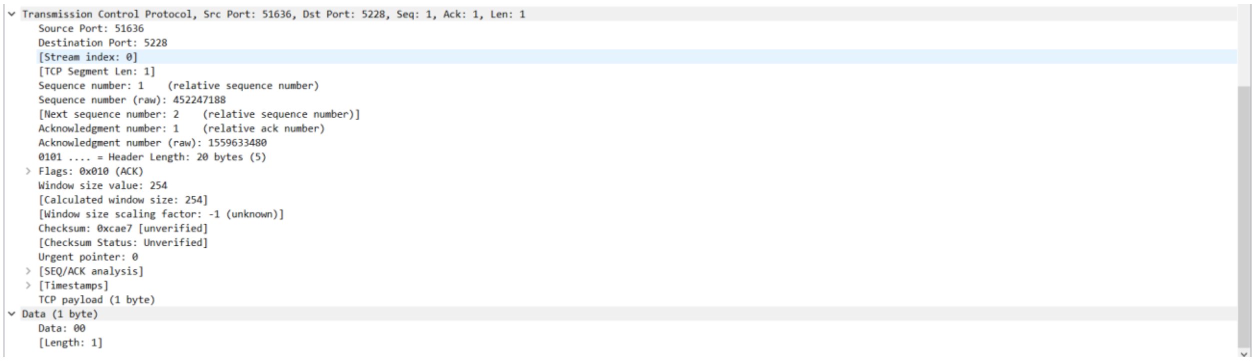
```
0030  00 00 00 00 20 04 ee ba  01 bb 01 31 d8 b2 5a 14   ···· ··· ···1··Z·
0040  e5 de dc e0 b4 7d 6e 2a  f9 3a f0 9c 29 dd da be   ·····}n* ·:··)···
0050  ce ef e6 2c 12 e4 0a bb  14 a0 45 45 e7 2f 0d 02   ···,···· ··EE·/··
0060  57 c7 54 8b d3 4f fc 51  8c 8a 08 d7 ec 35 a3 ea   W·T··O·Q ·····5··
0070  49 23 aa 97 8d 90 7f 10  58 1a 68 dd 3b 2a fc bd   I#······ X·h·;*··
```

```
User Datagram Protocol: Protocol        Packets: 67 · Displayed: 56 (83.6%)        Profile: Default
```

```
v User Datagram Protocol, Src Port: 61114, Dst Port: 443
    Source Port: 61114
    Destination Port: 443
    Length: 305
    Checksum: 0xd8b2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
v Data (297 bytes)
    Data: 5a14e5dedce0b47d6e2af93af09c29dddabeceefe62c12e4…
    [Length: 297]
```

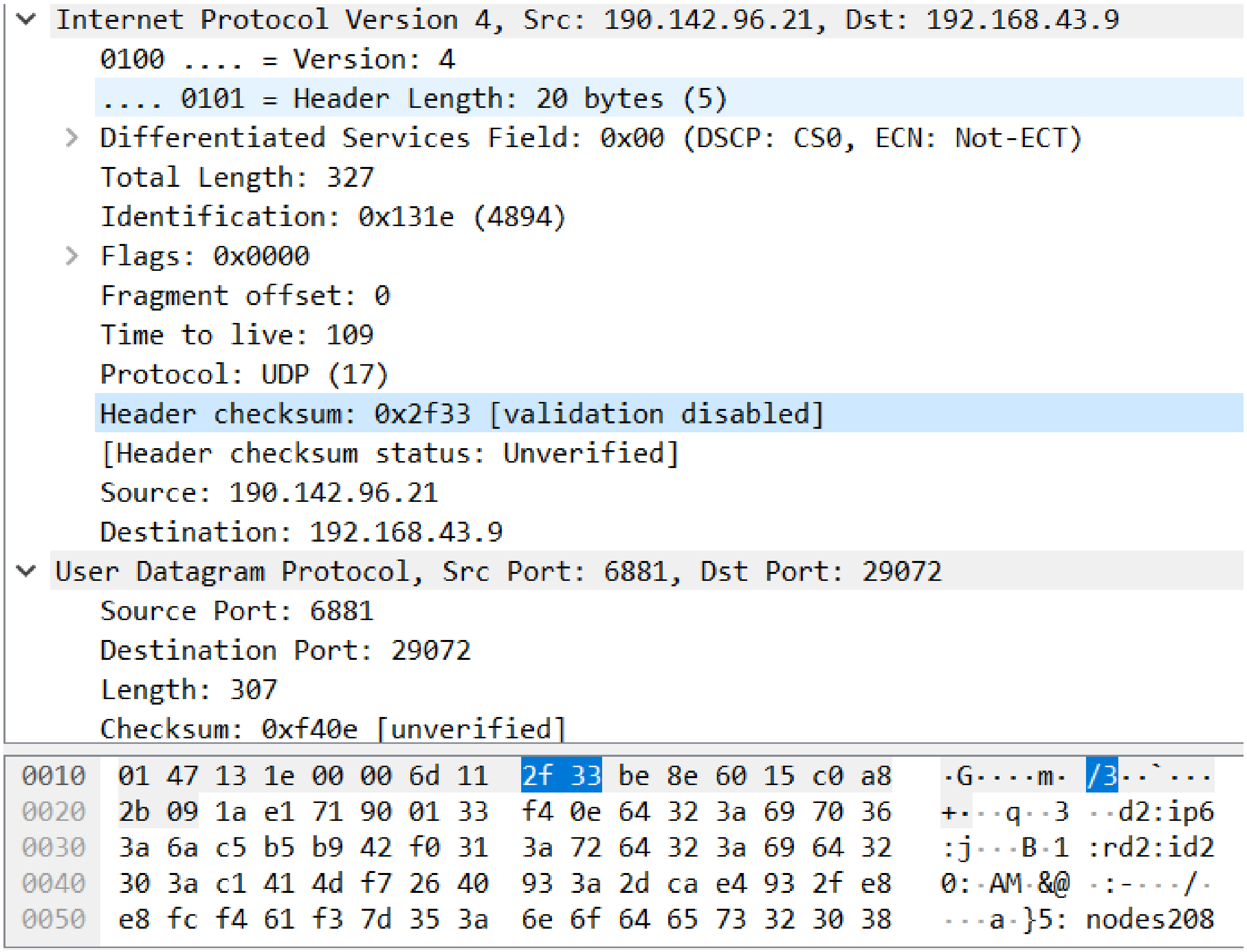


```
tcp
No.   Time       Source                 Destination           Protocol  Length  Info
   31 7.160456   2401:4900:25d3:6e94…   2404:6800:4003:c00:…  TCP           75  51636 → 5228 [ACK] Seq=1 Ack=1 Win=254 Len=1

v Frame 31: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{F9CFB353-1D75-4EBE-AF2B-1D26EC23C1F5}, id 0
  > Interface id: 0 (\Device\NPF_{F9CFB353-1D75-4EBE-AF2B-1D26EC23C1F5})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 19, 2020 20:49:49.618758000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1603120789.618758000 seconds
    [Time delta from previous captured frame: 0.459944000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 7.160456000 seconds]
    Frame Number: 31
    Frame Length: 75 bytes (600 bits)
    Capture Length: 75 bytes (600 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:tcp:data]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
v Ethernet II, Src: AzureWav_32:6c:97 (dc:f5:05:32:6c:97), Dst: fe:aa:b6:8a:94:ab (fe:aa:b6:8a:94:ab)
  > Destination: fe:aa:b6:8a:94:ab (fe:aa:b6:8a:94:ab)
  > Source: AzureWav_32:6c:97 (dc:f5:05:32:6c:97)
    Type: IPv6 (0x86dd)
v Internet Protocol Version 6, Src: 2401:4900:25d3:6e94:b876:6d19:5228:5f21, Dst: 2404:6800:4003:c00::bc
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1000 0000 1011 0111 0101 = Flow Label: 0x80b75
    Payload Length: 21
    Next Header: TCP (6)
    Hop Limit: 64
    Source: 2401:4900:25d3:6e94:b876:6d19:5228:5f21
    Destination: 2404:6800:4003:c00::bc
v Transmission Control Protocol, Src Port: 51636, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
    Source Port: 51636
    Destination Port: 5228

0000  fe aa b6 8a 94 ab dc f5  05 32 6c 97 86 dd 60 08   ········ ·2l···`·
0010  0b 75 00 15 06 40 24 01  49 00 25 d3 6e 94 b8 76   ·u···@$· I·%·n··v
0020  6d 19 52 28 5f 21 24 04  68 00 40 03 0c 00 00 00   m·R(_!$· h·@·····
0030  00 00 00 00 00 bc c9 b4  14 6c 1a f4 be 94 5c f6   ········ ·l····\·
0040  1e 48 50 10 00 fe ca e7  00 00 00                 ·HP····· ···

Transmission Control Protocol: Protocol                Packets: 67 · Displayed: 1 (1.5%)     Profile: Default
```



```
v Transmission Control Protocol, Src Port: 51636, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
    Source Port: 51636
    Destination Port: 5228
    [Stream index: 0]
    [TCP Segment Len: 1]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 452247188
    [Next sequence number: 2    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 1559633480
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 254
    [Calculated window size: 254]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xcae7 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (1 byte)
v Data (1 byte)
    Data: 00
    [Length: 1]
```

2) Compute Checksum for IPV4 header with data in IPv4 and verify the checksum available in the header.



```
∨ Internet Protocol Version 4, Src: 190.142.96.21, Dst: 192.168.43.9
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 327
    Identification: 0x131e (4894)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 109
    Protocol: UDP (17)
    Header checksum: 0x2f33 [validation disabled]
    [Header checksum status: Unverified]
    Source: 190.142.96.21
    Destination: 192.168.43.9
∨ User Datagram Protocol, Src Port: 6881, Dst Port: 29072
    Source Port: 6881
    Destination Port: 29072
    Length: 307
    Checksum: 0xf40e [unverified]
```

```
0010  01 47 13 1e 00 00 6d 11  2f 33 be 8e 60 15 c0 a8   ·G····m· /3··`···
0020  2b 09 1a e1 71 90 01 33  f4 0e 64 32 3a 69 70 36   +···q··3 ··d2:ip6
0030  3a 6a c5 b5 b9 42 f0 31  3a 72 64 32 3a 69 64 32   :j···B·1 :rd2:id2
0040  30 3a c1 41 4d f7 26 40  93 3a 2d ca e4 93 2f e8   0:·AM·&@ ·:-···/·
0050  e8 fc f4 61 f3 7d 35 3a  6e 6f 64 65 73 32 30 38   ···a·}5: nodes208
```

IPv4 ⇒ Checksum

2f 33

⇒ 2 15 3 3

→ 00000010 00001111 00000011 00000011

① ② ③ ④

Sender

① 00000010

② 00001111

00010001

③ 00000011

00010100

④ 00000011

00010111

Sum ↗

Checksum ⇒ 11101000

Receiver

Sum ⇒ 00010111

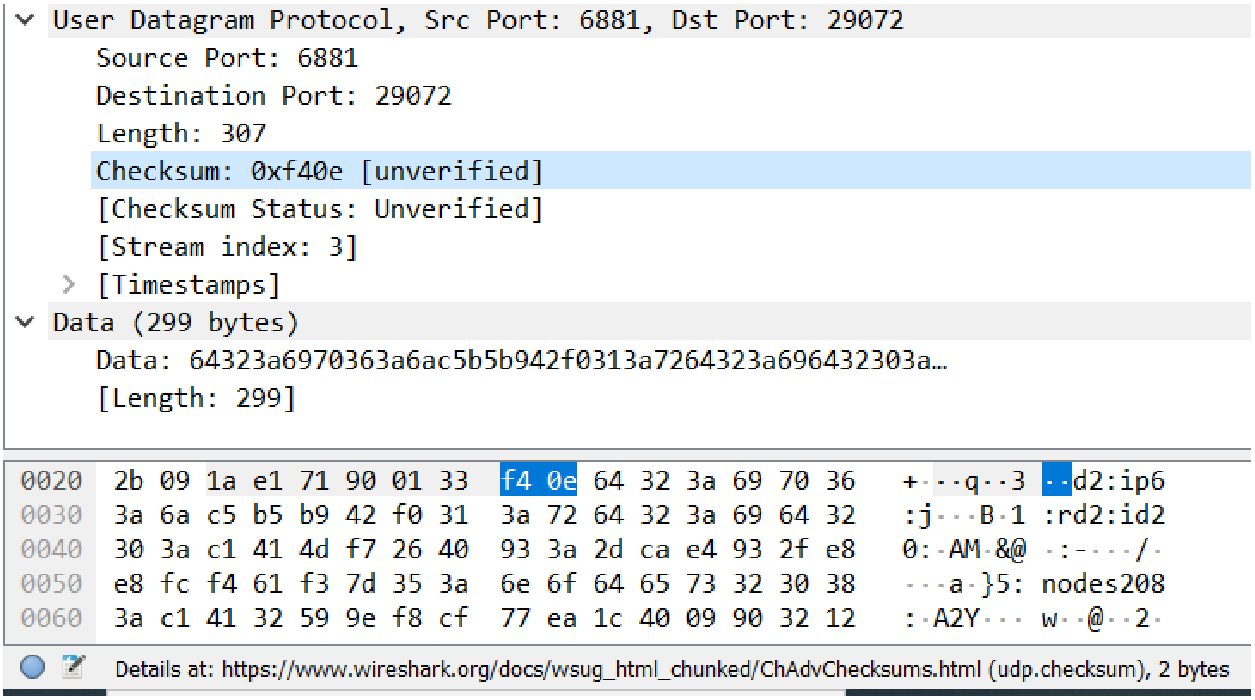
11101000

11111111

Complement : 00000000

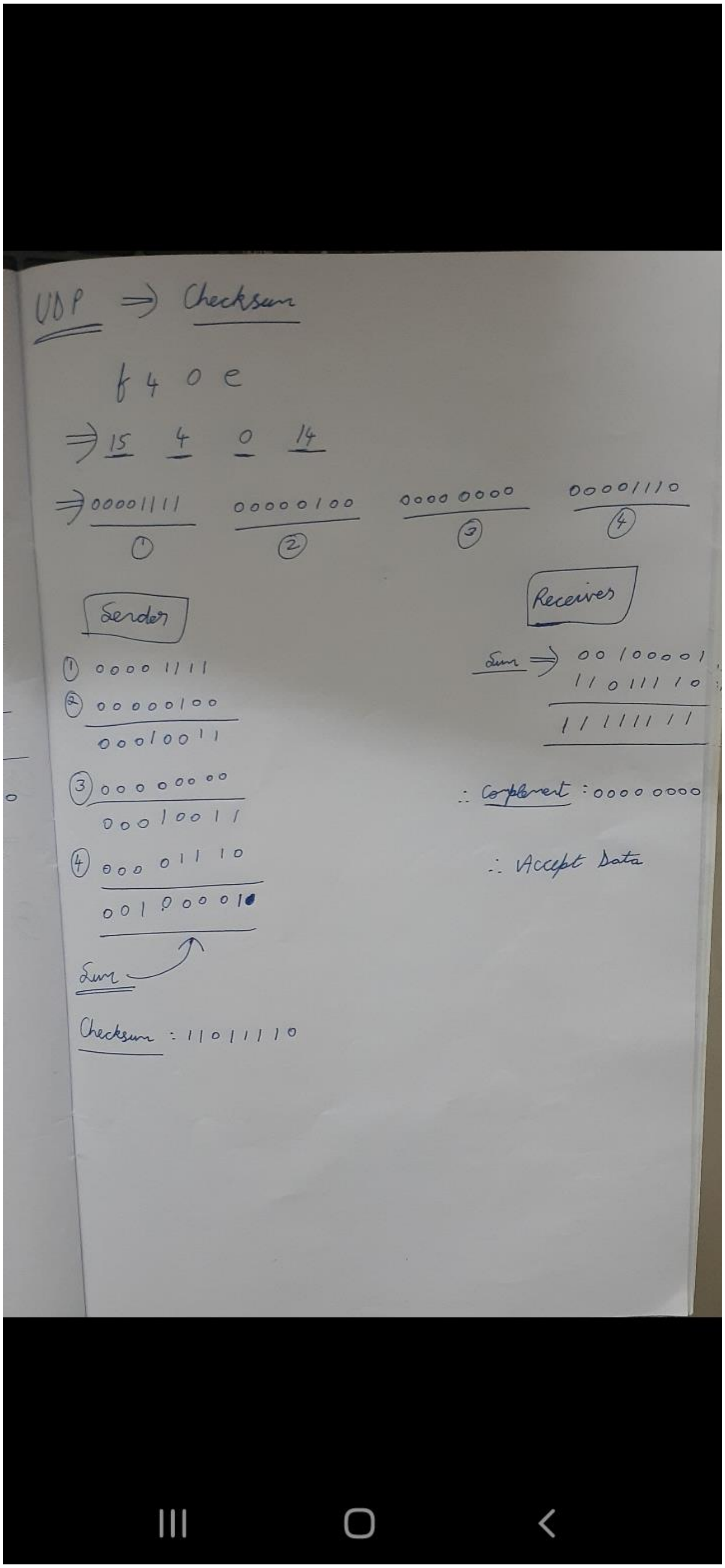
∴ Accept Data

3) Compute Checksum for TCP/UDP header for the captured packet and verify the checksum available in the header.



```
v User Datagram Protocol, Src Port: 6881, Dst Port: 29072
     Source Port: 6881
     Destination Port: 29072
     Length: 307
     Checksum: 0xf40e [unverified]
     [Checksum Status: Unverified]
     [Stream index: 3]
   > [Timestamps]
v Data (299 bytes)
     Data: 64323a6970363a6ac5b5b942f0313a7264323a696432303a…
     [Length: 299]

0020  2b 09 1a e1 71 90 01 33  f4 0e 64 32 3a 69 70 36   +···q··3 ··d2:ip6
0030  3a 6a c5 b5 b9 42 f0 31  3a 72 64 32 3a 69 64 32   :j···B·1 :rd2:id2
0040  30 3a c1 41 4d f7 26 40  93 3a 2d ca e4 93 2f e8   0:·AM·&@ ·:-···/·
0050  e8 fc f4 61 f3 7d 35 3a  6e 6f 64 65 73 32 30 38   ···a·}5: nodes208
0060  3a c1 41 32 59 9e f8 cf  77 ea 1c 40 09 90 32 12   :·A2Y··· w··@··2·
```

Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (udp.checksum), 2 bytes



UDP ⇒ Checksum

f 4 0 e

⇒ 15 4 0 14

⇒ 00001111 (1) 00000100 (2) 0000 0000 (3) 00001110 (4)

Sender

```
(1) 0000 1111
(2) 00000100
    --------
    00010011

(3) 00000000
    --------
    00010011
(4) 00001110
    --------
    00100001
    --------
```

Sum

Checksum : 11011110

Receives

```
Sum ⇒  00100001
       11011110
       --------
       11111111
       --------
```

∴ Complement : 0000 0000

∴ Accept Data