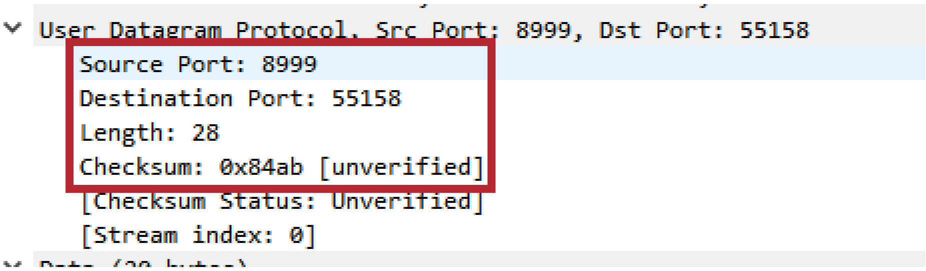
BAYANI, Femo Steven Felicisimo

2015-07104

1. Select one UDP packet from your trace. From this packet, determine how many fields are there in the UDP header. Name these fields.

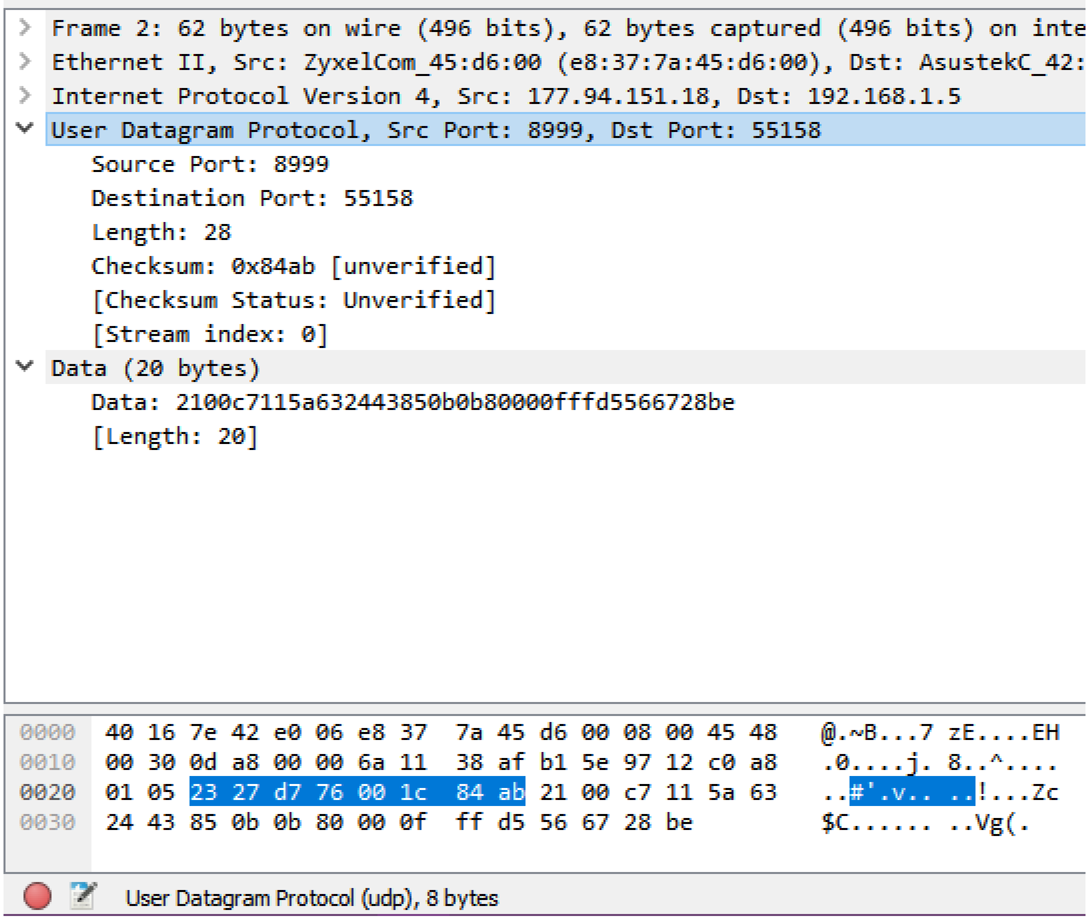
There are **four** fields: **Source Port**, **Destination Port**, **Length**, and **Checksum**.



```
∨ User Datagram Protocol, Src Port: 8999, Dst Port: 55158
     Source Port: 8999
     Destination Port: 55158
     Length: 28
     Checksum: 0x84ab [unverified]
     [Checksum Status: Unverified]
     [Stream index: 0]
∨ Data (20 bytes)
```

2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

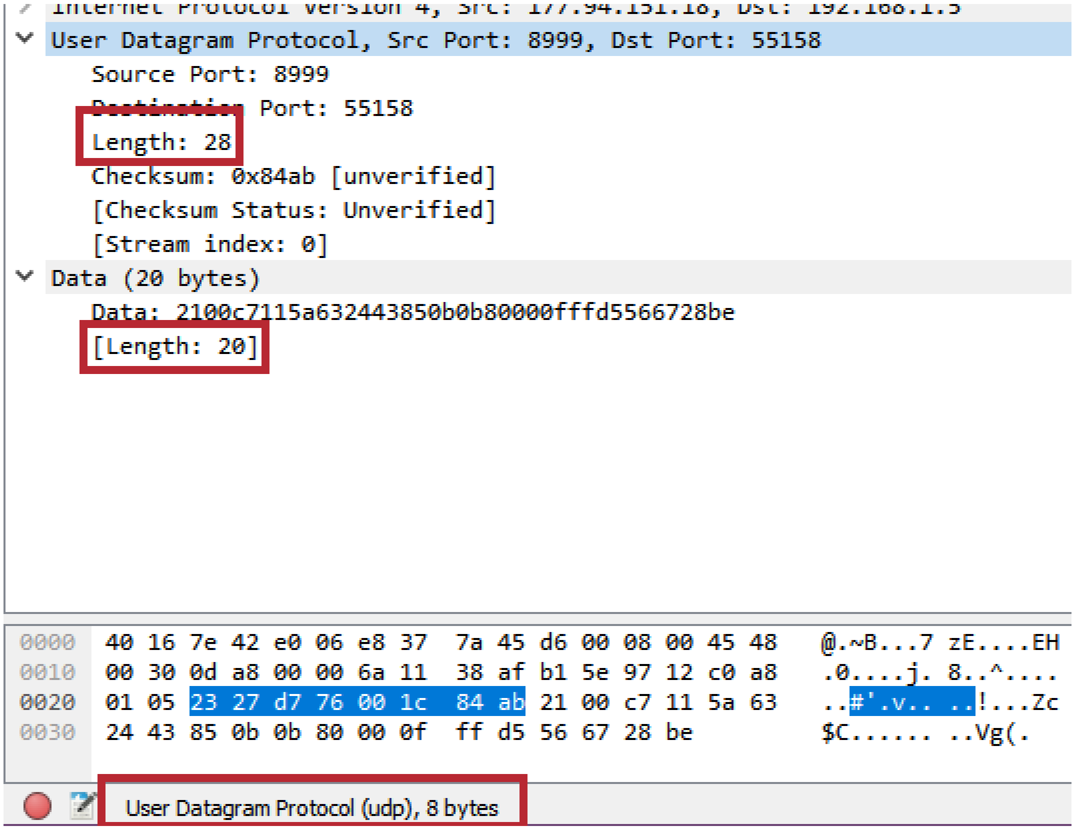
Each of the UDP header fields is 2 bytes long, for a total of 8 bytes.



```
> Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on inte
> Ethernet II, Src: ZyxelCom_45:d6:00 (e8:37:7a:45:d6:00), Dst: AsustekC_42:
> Internet Protocol Version 4, Src: 177.94.151.18, Dst: 192.168.1.5
∨ User Datagram Protocol, Src Port: 8999, Dst Port: 55158
     Source Port: 8999
     Destination Port: 55158
     Length: 28
     Checksum: 0x84ab [unverified]
     [Checksum Status: Unverified]
     [Stream index: 0]
∨ Data (20 bytes)
     Data: 2100c7115a632443850b0b80000fffd5566728be
     [Length: 20]

0000  40 16 7e 42 e0 06 e8 37  7a 45 d6 00 08 00 45 48   @.~B...7 zE....EH
0010  00 30 0d a8 00 00 6a 11  38 af b1 5e 97 12 c0 a8   .0....j. 8..^....
0020  01 05 23 27 d7 76 00 1c  84 ab 21 00 c7 11 5a 63   ..#'.v.. ..!...Zc
0030  24 43 85 0b 0b 80 00 0f  ff d5 56 67 28 be         $C...... ..Vg(.

User Datagram Protocol (udp), 8 bytes
```

3. The value of the Length field is the length of what? Verify your claim with your captured UDP packet.

The value of the length field is the length of the header plus the length of the data. The header is 8 bytes long as indicated above and below, and the data is 20 bytes as indicated below, for a total of 28 bytes.

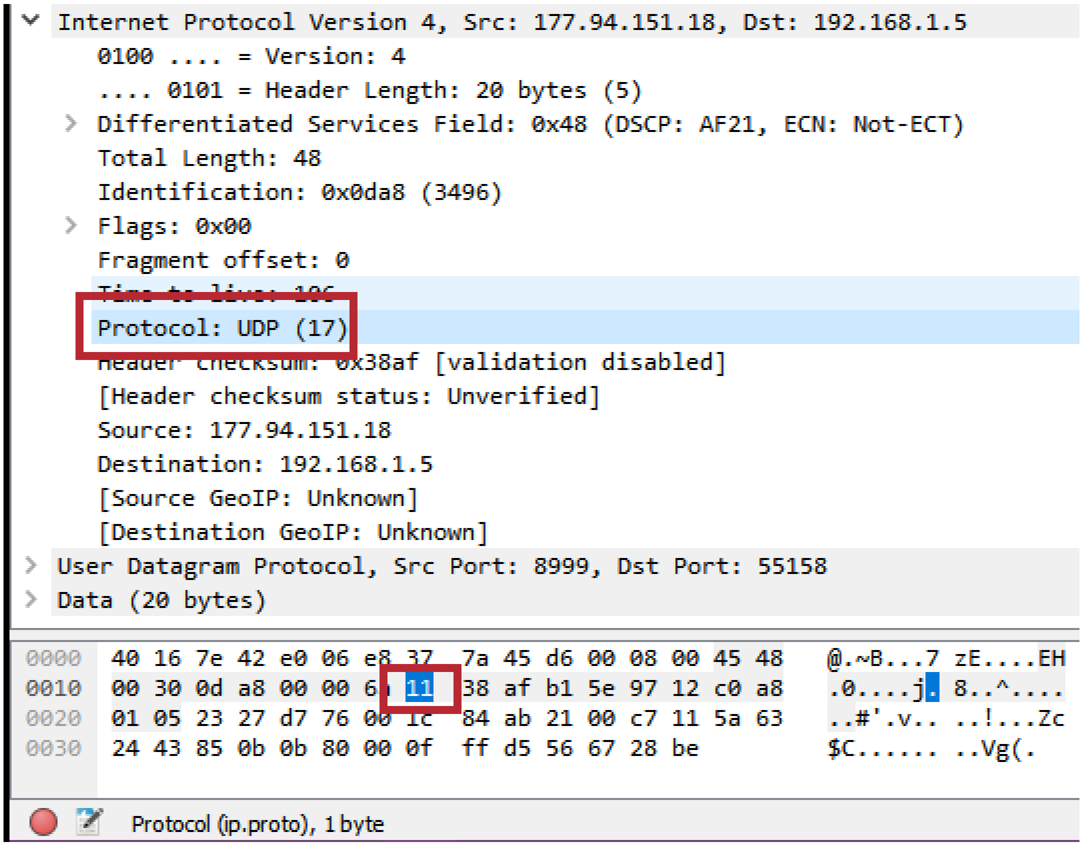


```
  Internet Protocol Version 4, Src: 177.94.151.18, Dst: 192.168.1.5
v User Datagram Protocol, Src Port: 8999, Dst Port: 55158
     Source Port: 8999
     Destination Port: 55158
     Length: 28
     Checksum: 0x84ab [unverified]
     [Checksum Status: Unverified]
     [Stream index: 0]
v Data (20 bytes)
     Data: 2100c7115a632443850b0b80000fffd5566728be
     [Length: 20]

0000  40 16 7e 42 e0 06 e8 37  7a 45 d6 00 08 00 45 48   @.~B...7 zE....EH
0010  00 30 0d a8 00 00 6a 11  38 af b1 5e 97 12 c0 a8   .0....j. 8..^....
0020  01 05 23 27 d7 76 00 1c  84 ab 21 00 c7 11 5a 63   ..#'.v.. ..!...Zc
0030  24 43 85 0b 0b 80 00 0f  ff d5 56 67 28 be         $C...... ..Vg(.
```

User Datagram Protocol (udp), 8 bytes

4. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment.

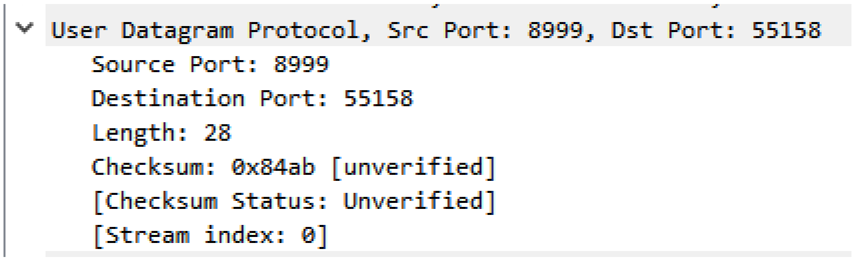
The protocol number is **0x11 in hexadecimal** and **17 in decimal**.



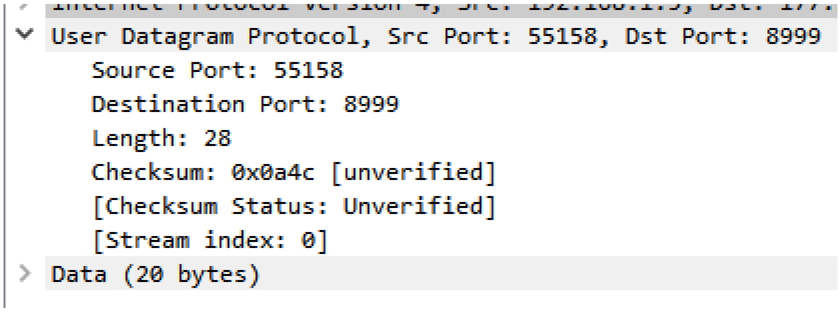
```
Internet Protocol Version 4, Src: 177.94.151.18, Dst: 192.168.1.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x48 (DSCP: AF21, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x0da8 (3496)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 106
    Protocol: UDP (17)
    Header checksum: 0x38af [validation disabled]
    [Header checksum status: Unverified]
    Source: 177.94.151.18
    Destination: 192.168.1.5
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
> User Datagram Protocol, Src Port: 8999, Dst Port: 55158
> Data (20 bytes)

0000  40 16 7e 42 e0 06 e8 37  7a 45 d6 00 08 00 45 48   @.~B...7 zE....EH
0010  00 30 0d a8 00 00 6a 11  38 af b1 5e 97 12 c0 a8   .0....j. 8..^....
0020  01 05 23 27 d7 76 00 1c  84 ab 21 00 c7 11 5a 63   ..#'.v.. ..!...Zc
0030  24 43 85 0b 0b 80 00 0f  ff d5 56 67 28 be         $C...... ..Vg(.

Protocol (ip.proto), 1 byte
```

5. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. Describe the relationship between the port numbers in the two packets.

The source port of the UDP packet sent by the host is the same as the destination port of the reply UDP packet, and so is the destination of the UDP packet sent by the host and the source port of the reply UDP packet. It means that the two UDP packets are related in a way that the other is, as previously mentioned, a reply to the first one sent by the host.



```
User Datagram Protocol, Src Port: 8999, Dst Port: 55158
    Source Port: 8999
    Destination Port: 55158
    Length: 28
    Checksum: 0x84ab [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
```



```
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 177.
User Datagram Protocol, Src Port: 55158, Dst Port: 8999
    Source Port: 55158
    Destination Port: 8999
    Length: 28
    Checksum: 0x0a4c [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
Data (20 bytes)
```