山东大学______计算机________学院

____计算机网络____课程实验报告

学号：	姓名：	班级：

实验题目：
实验四 UDP

实验学时：2h	实验日期： 2023.03.21

实验目的：
学习掌握 UDP 的相关内容，并查看相应的 UDP 封包。

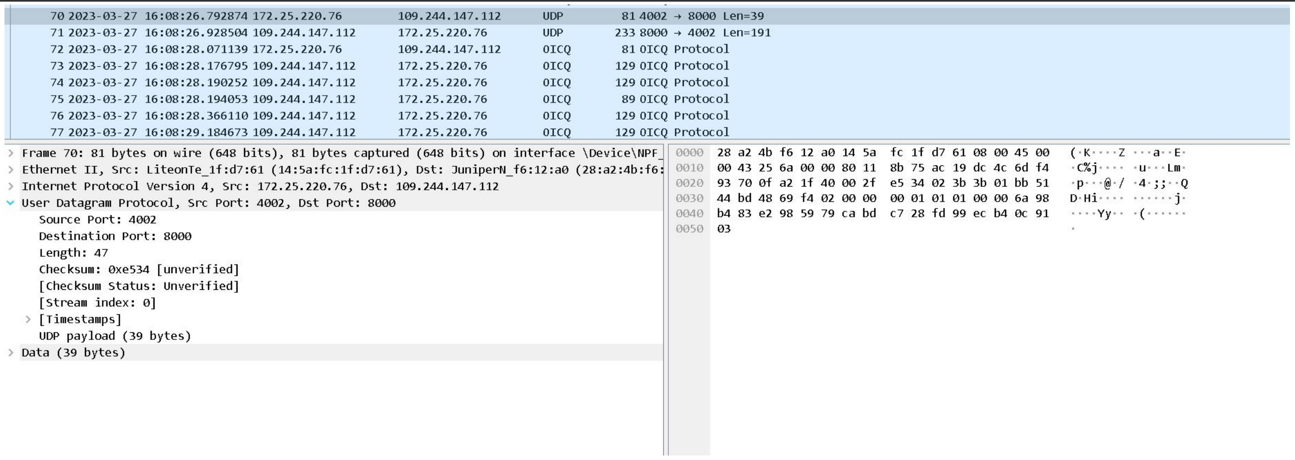
硬件环境：
Windows10 家庭版

软件环境：
Wireshark

实验步骤与内容：
实验内容：

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn’t look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.
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.
3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.
4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)
5. What is the largest possible source port number? (Hint: see the hint in 4.)
6. 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 (see Figure 4.13 in the text, and the discussion of IP header fields).
7. 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. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.

实验步骤：
打开 Wireshark，然后根据实验指导书，使用 WireShark 捕获网络封包，并查看 UDP 封包的相应信息。
1.



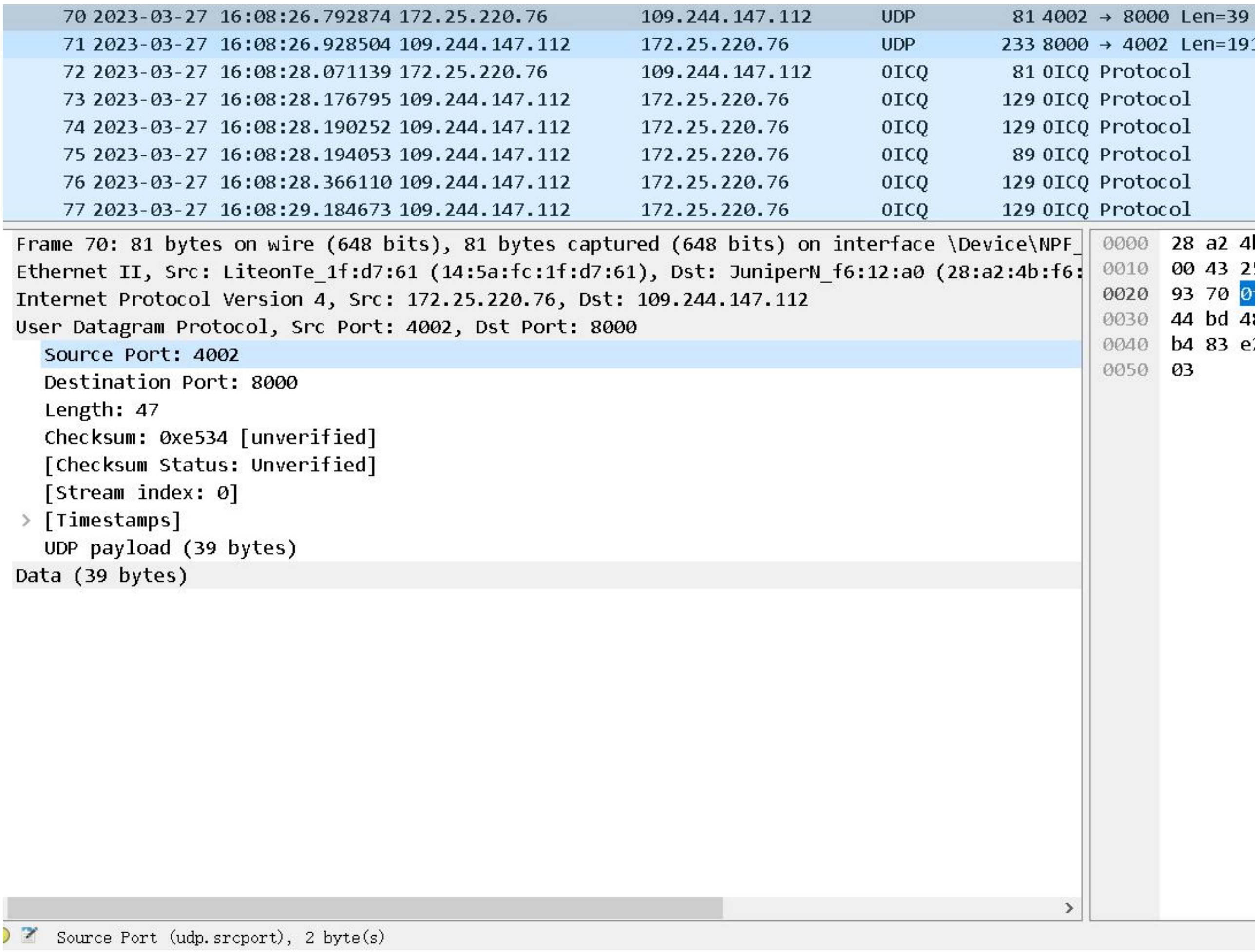
```
70 2023-03-27 16:08:26.792874 172.25.220.76     109.244.147.112   UDP      81 4002 → 8000 Len=39
71 2023-03-27 16:08:26.928504 109.244.147.112   172.25.220.76     UDP     233 8000 → 4002 Len=191
72 2023-03-27 16:08:28.071139 172.25.220.76     109.244.147.112   OICQ     81 OICQ Protocol
73 2023-03-27 16:08:28.176795 109.244.147.112   172.25.220.76     OICQ    129 OICQ Protocol
74 2023-03-27 16:08:28.190252 109.244.147.112   172.25.220.76     OICQ    129 OICQ Protocol
75 2023-03-27 16:08:28.194053 109.244.147.112   172.25.220.76     OICQ     89 OICQ Protocol
76 2023-03-27 16:08:28.366110 109.244.147.112   172.25.220.76     OICQ    129 OICQ Protocol
77 2023-03-27 16:08:29.184673 109.244.147.112   172.25.220.76     OICQ    129 OICQ Protocol
```

```
> Frame 70: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_
> Ethernet II, Src: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61), Dst: JuniperN_f6:12:a0 (28:a2:4b:f6:
> Internet Protocol Version 4, Src: 172.25.220.76, Dst: 109.244.147.112
v User Datagram Protocol, Src Port: 4002, Dst Port: 8000
    Source Port: 4002
    Destination Port: 8000
    Length: 47
    Checksum: 0xe534 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (39 bytes)
> Data (39 bytes)
```

```
0000  28 a2 4b f6 12 a0 14 5a  fc 1f d7 61 08 00 45 00   (·K····Z ···a··E·
0010  00 43 25 6a 00 00 80 11  8b 75 ac 19 dc 4c 6d f4   ·C%j···· ·u···Lm·
0020  93 70 0f a2 1f 40 00 2f  e5 34 02 3b 3b 01 bb 51   ·p···@·/ ·4·;;··Q
0030  44 bd 48 69 f4 02 00 00  00 01 01 01 00 00 6a 98   D·Hi···· ······j·
0040  b4 83 e2 98 59 79 ca bd  c7 28 fd 99 ec b4 0c 91   ····Yy·· ·(······
0050  03                                                 ·
```

有四个字段，分别为源端口号、目的端口号、长度和检验和。

2.



```
70 2023-03-27 16:08:26.792874 172.25.220.76     109.244.147.112   UDP      81 4002 → 8000 Len=39
71 2023-03-27 16:08:26.928504 109.244.147.112   172.25.220.76     UDP     233 8000 → 4002 Len=19
72 2023-03-27 16:08:28.071139 172.25.220.76     109.244.147.112   OICQ     81 OICQ Protocol
73 2023-03-27 16:08:28.176795 109.244.147.112   172.25.220.76     OICQ    129 OICQ Protocol
74 2023-03-27 16:08:28.190252 109.244.147.112   172.25.220.76     OICQ    129 OICQ Protocol
75 2023-03-27 16:08:28.194053 109.244.147.112   172.25.220.76     OICQ     89 OICQ Protocol
76 2023-03-27 16:08:28.366110 109.244.147.112   172.25.220.76     OICQ    129 OICQ Protocol
77 2023-03-27 16:08:29.184673 109.244.147.112   172.25.220.76     OICQ    129 OICQ Protocol
```

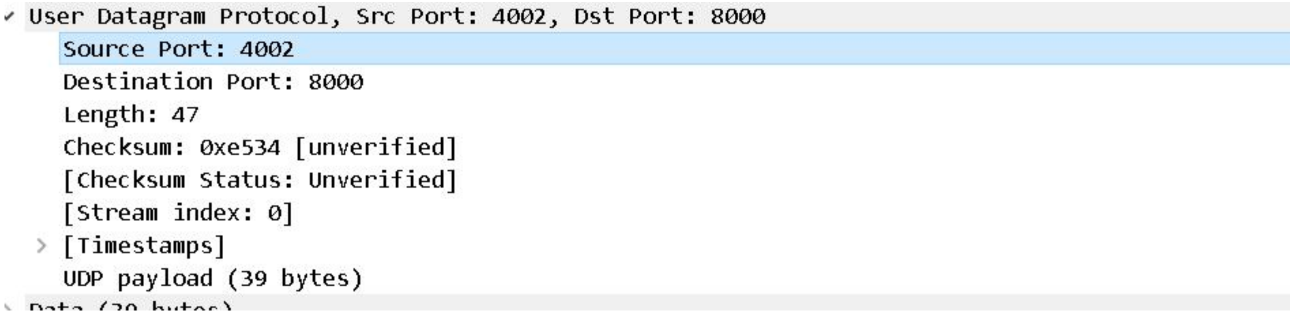
```
Frame 70: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_
Ethernet II, Src: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61), Dst: JuniperN_f6:12:a0 (28:a2:4b:f6:
Internet Protocol Version 4, Src: 172.25.220.76, Dst: 109.244.147.112
User Datagram Protocol, Src Port: 4002, Dst Port: 8000
  Source Port: 4002
  Destination Port: 8000
  Length: 47
  Checksum: 0xe534 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
> [Timestamps]
  UDP payload (39 bytes)
Data (39 bytes)
```

```
0000  28 a2 4
0010  00 43 2
0020  93 70 0
0030  44 bd 4
0040  b4 83 e
0050  03
```

```
Source Port (udp.srcport), 2 byte(s)
```

四个字段长度是一样的，其中每个字段长度都是两个字节。

3. 长度是 UDP 报文的长度，包括首部和数据，下图中 Data 加上首部的 8B 等于 47 字节，是 UDP 报文的总长度。

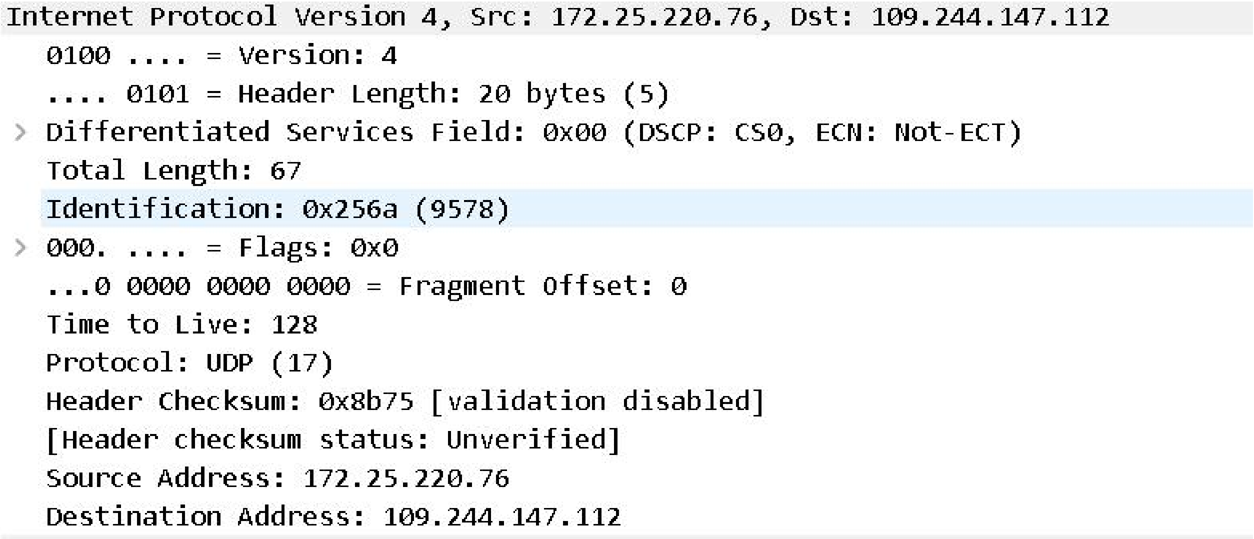


```
✓ User Datagram Protocol, Src Port: 4002, Dst Port: 8000
    Source Port: 4002
    Destination Port: 8000
    Length: 47
    Checksum: 0xe534 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (39 bytes)
> Data (39 bytes)
```

4. 因为长度是两个字节，一共 16 位，所以能表示最大长度就是 2^16-1，又因为首部长度为 8 个字节，所以能够包含最大的字节数是 2^16-9 个字节。

5. 因为源端口号长度也是两个字节的，所以最大端口号为 2^16-1。

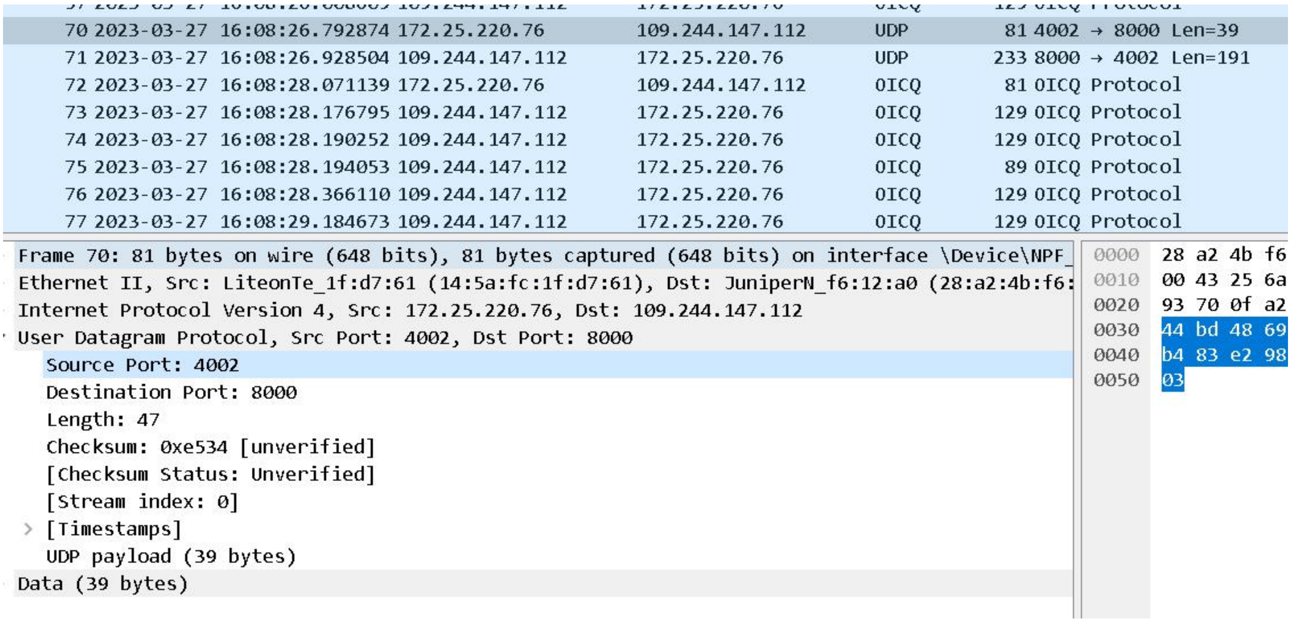
6.



```
Internet Protocol Version 4, Src: 172.25.220.76, Dst: 109.244.147.112
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 67
    Identification: 0x256a (9578)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x8b75 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.25.220.76
    Destination Address: 109.244.147.112
```

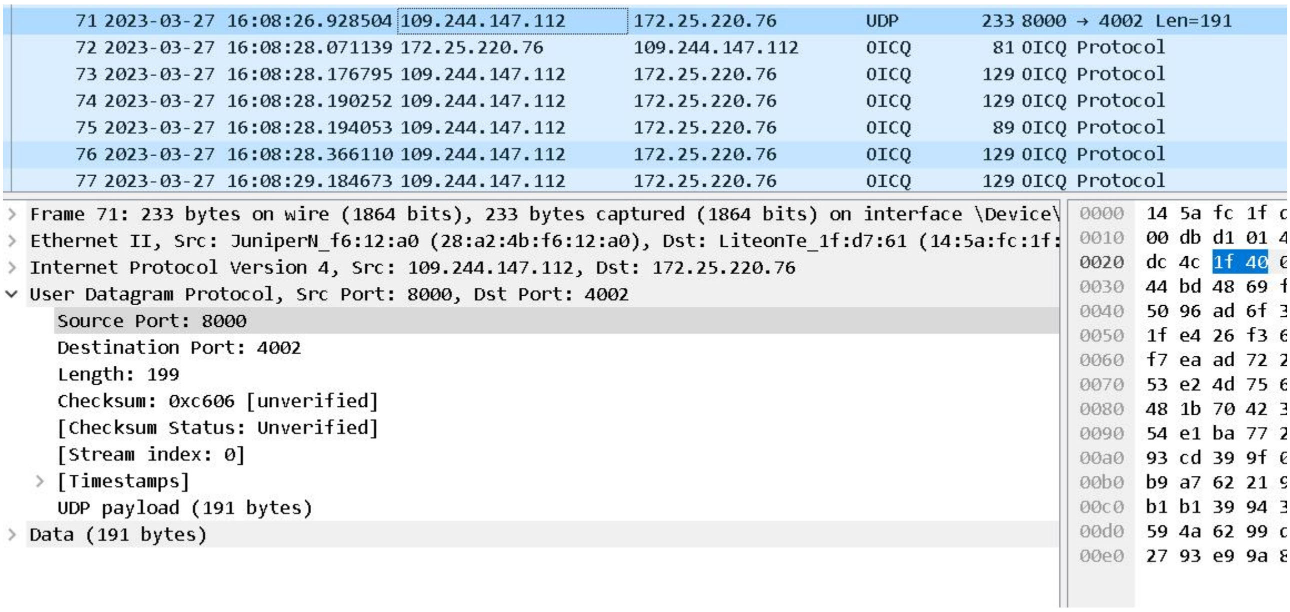
协议编号十进制下是 17，十六进制下是 11。

7.



```
70 2023-03-27 16:08:26.792874 172.25.220.76     109.244.147.112  UDP    81 4002 → 8000 Len=39
71 2023-03-27 16:08:26.928504 109.244.147.112   172.25.220.76    UDP   233 8000 → 4002 Len=191
72 2023-03-27 16:08:28.071139 172.25.220.76     109.244.147.112  OICQ   81 OICQ Protocol
73 2023-03-27 16:08:28.176795 109.244.147.112   172.25.220.76    OICQ  129 OICQ Protocol
74 2023-03-27 16:08:28.190252 109.244.147.112   172.25.220.76    OICQ  129 OICQ Protocol
75 2023-03-27 16:08:28.194053 109.244.147.112   172.25.220.76    OICQ   89 OICQ Protocol
76 2023-03-27 16:08:28.366110 109.244.147.112   172.25.220.76    OICQ  129 OICQ Protocol
77 2023-03-27 16:08:29.184673 109.244.147.112   172.25.220.76    OICQ  129 OICQ Protocol
```

```
Frame 70: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_     0000  28 a2 4b f6
Ethernet II, Src: LiteonTe_1f:d7:61 (14:5a:fc:1f:d7:61), Dst: JuniperN_f6:12:a0 (28:a2:4b:f6:     0010  00 43 25 6a
Internet Protocol Version 4, Src: 172.25.220.76, Dst: 109.244.147.112                              0020  93 70 0f a2
User Datagram Protocol, Src Port: 4002, Dst Port: 8000                                             0030  44 bd 48 69
    Source Port: 4002                                                                              0040  b4 83 e2 98
    Destination Port: 8000                                                                         0050  03
    Length: 47
    Checksum: 0xe534 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (39 bytes)
Data (39 bytes)
```



```
71 2023-03-27 16:08:26.928504 109.244.147.112  172.25.220.76    UDP   233 8000 → 4002 Len=191
72 2023-03-27 16:08:28.071139 172.25.220.76    109.244.147.112  OICQ   81 OICQ Protocol
73 2023-03-27 16:08:28.176795 109.244.147.112  172.25.220.76    OICQ  129 OICQ Protocol
74 2023-03-27 16:08:28.190252 109.244.147.112  172.25.220.76    OICQ  129 OICQ Protocol
75 2023-03-27 16:08:28.194053 109.244.147.112  172.25.220.76    OICQ   89 OICQ Protocol
76 2023-03-27 16:08:28.366110 109.244.147.112  172.25.220.76    OICQ  129 OICQ Protocol
77 2023-03-27 16:08:29.184673 109.244.147.112  172.25.220.76    OICQ  129 OICQ Protocol
```

```
> Frame 71: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface \Device\   0000  14 5a fc 1f c
> Ethernet II, Src: JuniperN_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: LiteonTe_1f:d7:61 (14:5a:fc:1f:   0010  00 db d1 01 4
> Internet Protocol Version 4, Src: 109.244.147.112, Dst: 172.25.220.76                          0020  dc 4c 1f 40 0
v User Datagram Protocol, Src Port: 8000, Dst Port: 4002                                        0030  44 bd 48 69 f
    Source Port: 8000                                                                           0040  50 96 ad 6f 3
    Destination Port: 4002                                                                      0050  1f e4 26 f3 6
    Length: 199                                                                                 0060  f7 ea ad 72 2
    Checksum: 0xc606 [unverified]                                                               0070  53 e2 4d 75 6
    [Checksum Status: Unverified]                                                               0080  48 1b 70 42 3
    [Stream index: 0]                                                                           0090  54 e1 ba 77 2
  > [Timestamps]                                                                                00a0  93 cd 39 9f 0
    UDP payload (191 bytes)                                                                     00b0  b9 a7 62 21 9
> Data (191 bytes)                                                                              00c0  b1 b1 39 94 3
                                                                                                00d0  59 4a 62 99 c
                                                                                                00e0  27 93 e9 9a 8
```

由上图不难发现，第一个数据包的源端口号变成了第二个数据包目的端口号，第一个数据包的目的端口号变成了第二个数据包的源端口号。

结论分析与体会：

通过查看相关的 UDP 封包，对 UDP 报文结构有了进一步认知，同时对 UDP 协议也有了更好地认识。