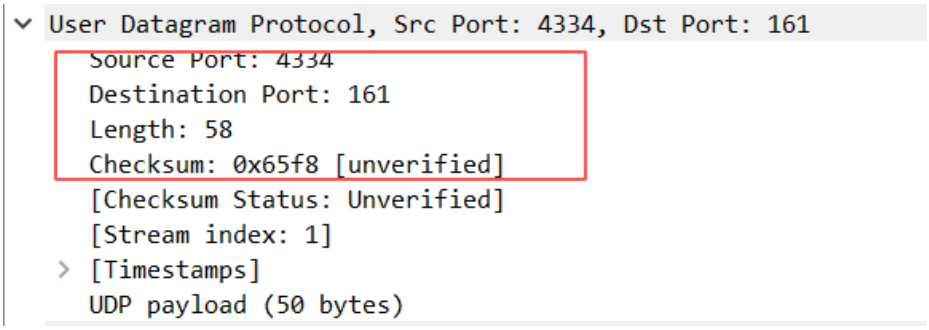
# Lab5 Wireshark_UDP

- 学号:1813075
- 姓名:刘茵

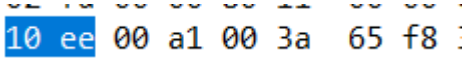
1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.




答：四部分。

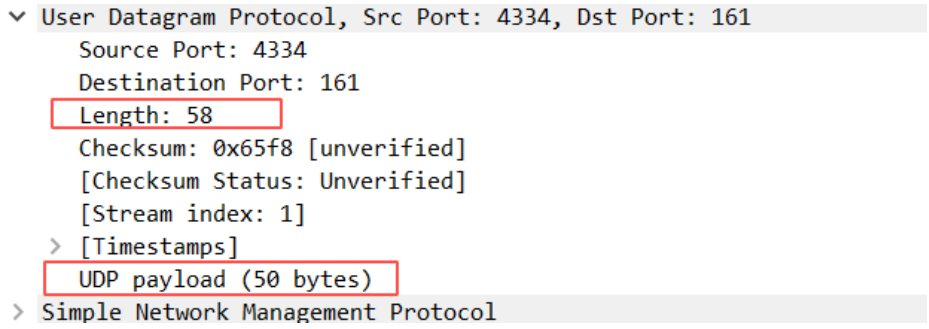
**Source Port**：源端口号
**Destination Port**：目的端口号
**Length**：长度
**Checksum**：校验和

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.




答: 8个字节

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.




答：Length 包含 UDP 报文头和 UDP 数据长度。

UDP 头长度是 8 字节，UDP 数据是 50 字节，Length为 58 字节。

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)
答：有效负载就是可变长度的数据部分。由于 Length 字段占 2byte = 65536 bit，并且其中 8 byte 是 UDP 首部信息。因此有效载荷 = 2^16-1-8=65527bytes

5. What is the largest possible source port number? (Hint: see the hint in 4.)
答：65535

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).

| 十进制 | 十六进制 | 关键字 | 协议 | 引用 |
|---|---|---|---|---|
| 0 | 0x00 | HOPOPT | IPv6逐跳选项 | RFC 2460 |
| 1 | 0x01 | ICMP | 互联网控制消息协议（ICMP） | RFC 792 |
| 2 | 0x02 | IGMP | 因特网组管理协议（IGMP） | RFC 1112 |
| 3 | 0x03 | GGP | 网关对网关协议 | RFC 823 |
| 4 | 0x04 | IPv4 | IPv4 (封装) | RFC 791 |
| 5 | 0x05 | ST | 因特网流协议 | RFC 1190, RFC 1819 |
| 6 | 0x06 | TCP | 传输控制协议（TCP） | RFC 793 |
| 7 | 0x07 | CBT | 有核树组播路由协议 | RFC 2189 |
| 8 | 0x08 | EGP | 外部网关协议 | RFC 888 |
| 9 | 0x09 | IGP | 内部网关协议（任意私有内部网关（用于思科的IGRP）） | |
| 10 | 0x0A | BBN-RCC-MON | BBN RCC 监视 | |
| 11 | 0x0B | NVP-II | 网络语音协议 | RFC 741 |
| 12 | 0x0C | PUP | Xerox PUP | |
| 13 | 0x0D | ARGUS | ARGUS | |
| 14 | 0x0E | EMCON | EMCON | |
| 15 | 0x0F | XNET | Cross Net Debugger | IEN 158 |
| 16 | 0x10 | CHAOS | Chaos | |
| 17 | 0x11 | UDP | 用户数据报协议（UDP） | RFC 768 |

```
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 78
    Identification: 0x02fd (765)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
```

答： ANS:UDP 协议号是 17（10 进制），16 进制 0x11

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.

```
     1 2003-09-23 13:39:52.896793 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
     2 2003-09-23 13:39:52.913753 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    11 2003-09-23 13:39:55.913764 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    12 2003-09-23 13:39:55.930920 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    13 2003-09-23 13:39:58.930512 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    14 2003-09-23 13:39:58.947601 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    15 2003-09-23 13:40:01.947256 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    16 2003-09-23 13:40:01.964285 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    17 2003-09-23 13:40:04.964007 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    18 2003-09-23 13:40:04.981940 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    19 2003-09-23 13:40:05.217358 192.168.1.100 192.168.1.255 NBNS 92 Name query NB NOHO<20>
    20 2003-09-23 13:40:05.217393 192.168.1.102 192.168.1.100 NBNS 104 Name query response NB 192.168.1.102
> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: HewlettP_61:eb:ed (00:30:c1:61:eb:ed)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 192.168.1.104
v User Datagram Protocol, Src Port: 4334, Dst Port: 161
    Source Port: 4334
    Destination Port: 161
    Length: 58
    Checksum: 0x65f8 [unverified]
    [Checksum Status: Unverified]
```

```
     1 2003-09-23 13:39:52.896793 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
     2 2003-09-23 13:39:52.913753 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    11 2003-09-23 13:39:55.913764 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    12 2003-09-23 13:39:55.930920 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    13 2003-09-23 13:39:58.930512 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    14 2003-09-23 13:39:58.947601 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    15 2003-09-23 13:40:01.947256 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    16 2003-09-23 13:40:01.964285 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    17 2003-09-23 13:40:04.964007 192.168.1.102 192.168.1.104 SNMP 92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    18 2003-09-23 13:40:04.981940 192.168.1.104 192.168.1.102 SNMP 93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    19 2003-09-23 13:40:05.217358 192.168.1.100 192.168.1.255 NBNS 92 Name query NB NOHO<20>
    20 2003-09-23 13:40:05.217393 192.168.1.102 192.168.1.100 NBNS 104 Name query response NB 192.168.1.102
> Frame 2: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
> Ethernet II, Src: HewlettP_61:eb:ed (00:30:c1:61:eb:ed), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.102
v User Datagram Protocol, Src Port: 161, Dst Port: 4334
    Source Port: 161
    Destination Port: 4334
    Length: 59
    Checksum: 0x53f2 [unverified]
    [Checksum Status: Unverified]
```

答：发送者发送端口号在接收返回UDP 时候会变成接收端口号。

接收者发送返回UDP 时候接受端口号会变成发送端口号。