计算机网络UDP实验报告

PB19071535徐昊天

一.实验目的

- 学习并了解UDP协议。
- 通过wireshark捕获UDP数据包，通过数据包分析进一步掌握UDP的报文格式。

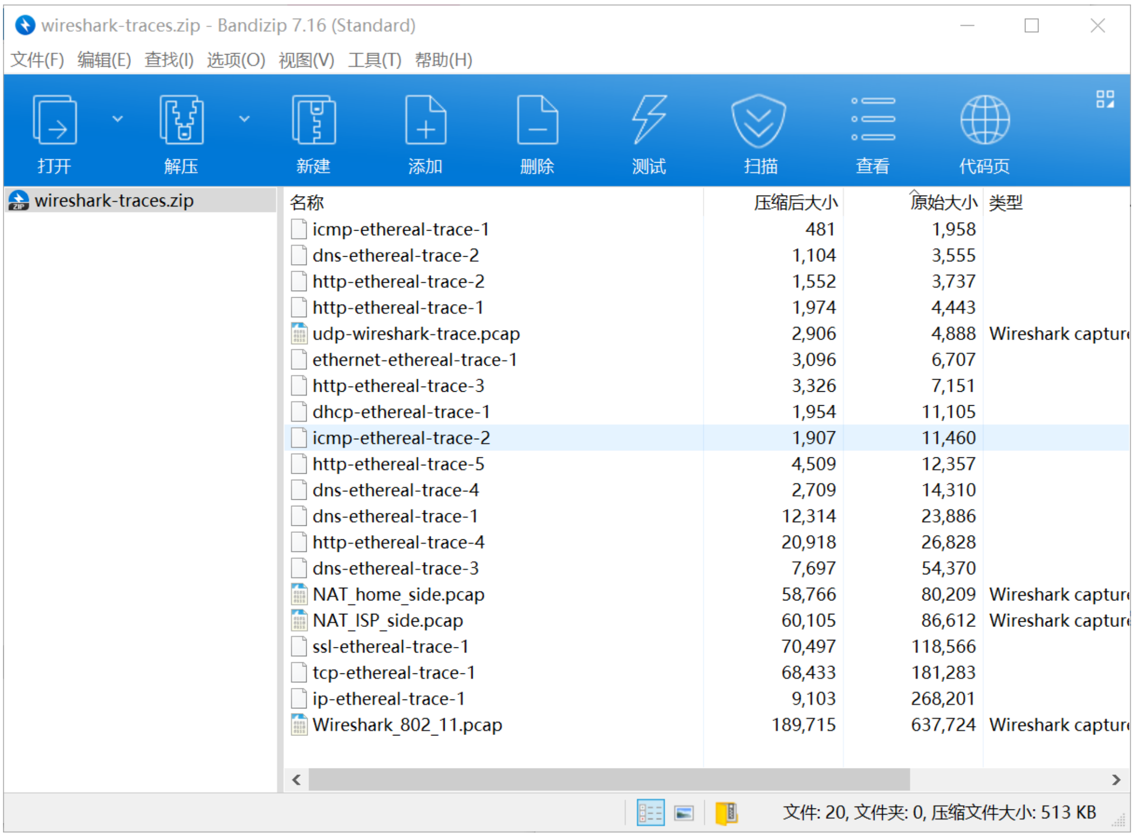
二.实验环境与工具

- windows操作系统
- wireshark数据嗅探器

三.实验步骤

1. 点击http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip下载压缩包。

   压缩包内部文件如下图所示：

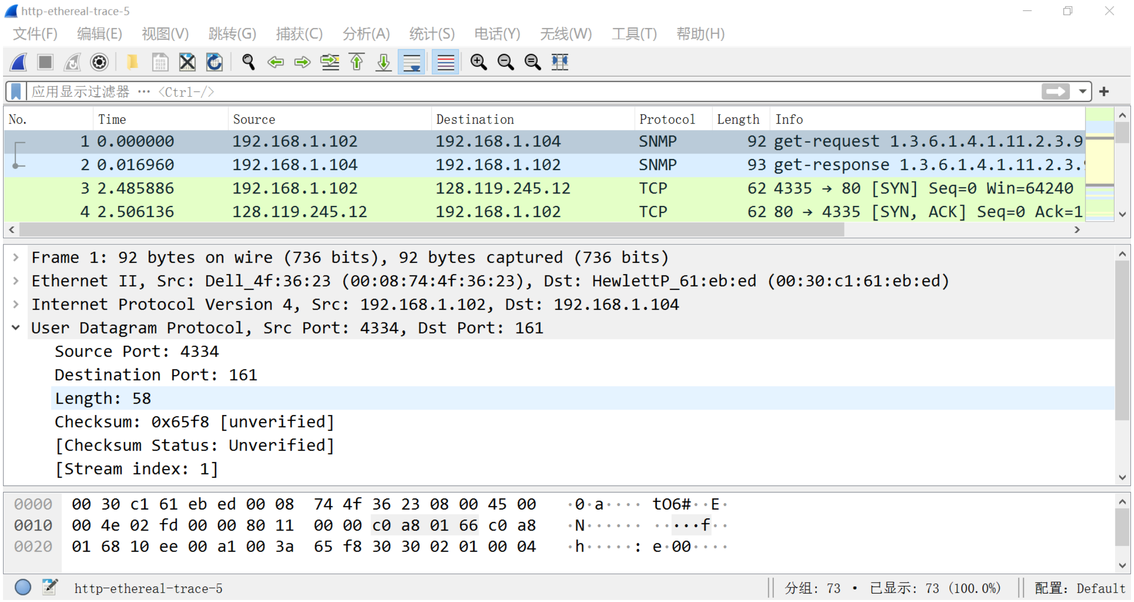

wireshark-traces.zip - Bandizip 7.16 (Standard)
文件(F) 编辑(E) 查找(I) 选项(O) 视图(V) 工具(T) 帮助(H)
打开
解压
新建
添加
删除
测试
扫描
查看
代码页
wireshark-traces.zip
文件: 20, 文件夹: 0, 压缩文件大小: 513 KB

名称	压缩后大小	原始大小	类型
icmp-ethereal-trace-1	481	1,958	
dns-ethereal-trace-2	1,104	3,555	
http-ethereal-trace-2	1,552	3,737	
http-ethereal-trace-1	1,974	4,443	
udp-wireshark-trace.pcap	2,906	4,888	Wireshark captur
ethernet-ethereal-trace-1	3,096	6,707	
http-ethereal-trace-3	3,326	7,151	
dhcp-ethereal-trace-1	1,954	11,105	
icmp-ethereal-trace-2	1,907	11,460	
http-ethereal-trace-5	4,509	12,357	
dns-ethereal-trace-4	2,709	14,310	
dns-ethereal-trace-1	12,314	23,886	
http-ethereal-trace-4	20,918	26,828	
dns-ethereal-trace-3	7,697	54,370	
NAT_home_side.pcap	58,766	80,209	Wireshark captur
NAT_ISP_side.pcap	60,105	86,612	Wireshark captur
ssl-ethereal-trace-1	70,497	118,566	
tcp-ethereal-trace-1	68,433	181,283	
ip-ethereal-trace-1	9,103	268,201	
Wireshark_802_11.pcap	189,715	637,724	Wireshark captur

2. 解压压缩包

3. 打开wireshark,点击`OPEN`选项，选择解压文件夹内的`http-ethereal-trace-5`文件并打开。

   打开后wireshark界面如下图所示：

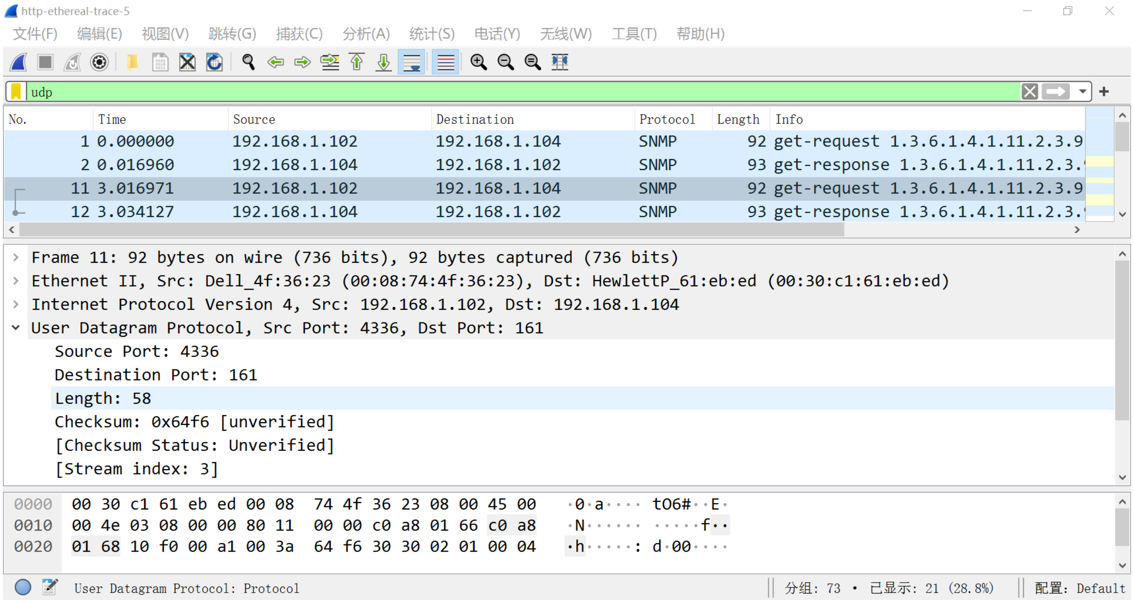

http-ethereal-trace-5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.  Time        Source           Destination      Protocol  Length  Info
   1 0.000000    192.168.1.102    192.168.1.104    SNMP      92 get-request 1.3.6.1.4.1.11.2.3.9
   2 0.016960    192.168.1.104    192.168.1.102    SNMP      93 get-response 1.3.6.1.4.1.11.2.3.
   3 2.485886    192.168.1.102    128.119.245.12   TCP       62 4335 → 80 [SYN] Seq=0 Win=64240
   4 2.506136    128.119.245.12   192.168.1.102    TCP       62 80 → 4335 [SYN, ACK] Seq=0 Ack=1
```

```
> 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]
    [Stream index: 1]
```

```
0000  00 30 c1 61 eb ed 00 08  74 4f 36 23 08 00 45 00   ·0·a····  tO6#··E·
0010  00 4e 02 fd 00 00 80 11  00 00 c0 a8 01 66 c0 a8   ·N······  ·····f··
0020  01 68 10 ee 00 a1 00 3a  65 f8 30 30 02 01 00 04   ·h·····:  e·00····
```

在过滤器中输入 udp 进行筛选，得到界面如下图所示：


http-ethereal-trace-5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
udp

```
No.  Time        Source           Destination      Protocol  Length  Info
   1 0.000000    192.168.1.102    192.168.1.104    SNMP      92 get-request 1.3.6.1.4.1.11.2.3.9
   2 0.016960    192.168.1.104    192.168.1.102    SNMP      93 get-response 1.3.6.1.4.1.11.2.3.
  11 3.016971    192.168.1.102    192.168.1.104    SNMP      92 get-request 1.3.6.1.4.1.11.2.3.9
  12 3.034127    192.168.1.104    192.168.1.102    SNMP      93 get-response 1.3.6.1.4.1.11.2.3.
```

```
> Frame 11: 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: 4336, Dst Port: 161
    Source Port: 4336
    Destination Port: 161
    Length: 58
    Checksum: 0x64f6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
```

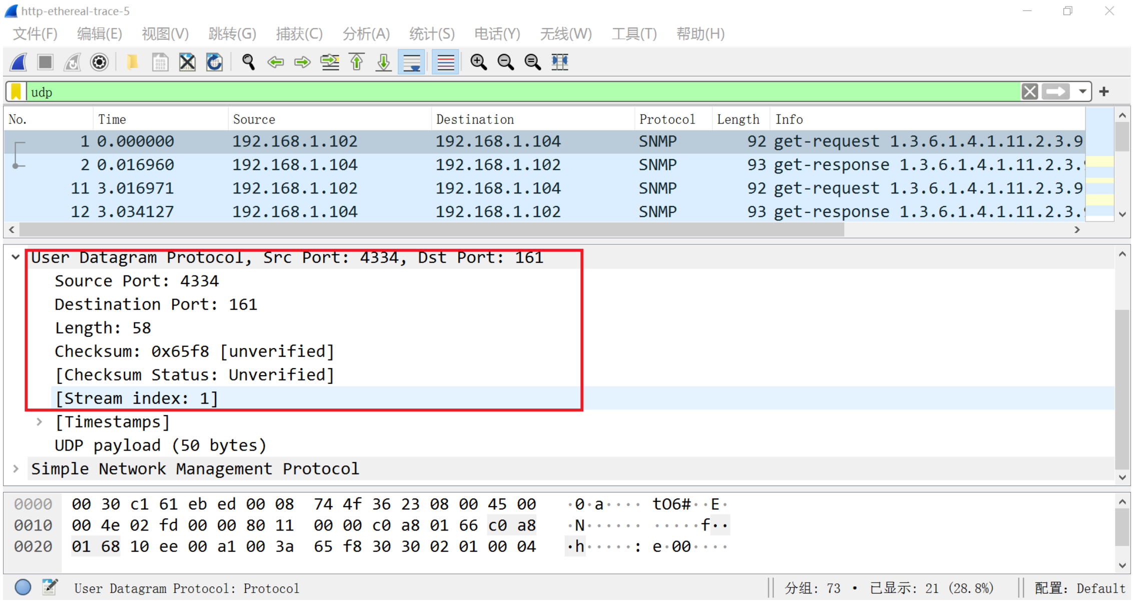
```
0000  00 30 c1 61 eb ed 00 08  74 4f 36 23 08 00 45 00   ·0·a····  tO6#··E·
0010  00 4e 03 08 00 00 80 11  00 00 c0 a8 01 66 c0 a8   ·N······  ·····f··
0020  01 68 10 f0 00 a1 00 3a  64 f6 30 30 02 01 00 04   ·h·····:  d·00····
```

User Datagram Protocol: Protocol
分组: 73 · 已显示: 21 (28.8%)
配置: Default

四.实验结果

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：选择1号数据包，其信息如下图所示：


http-ethereal-trace-5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
udp

```
No.    Time        Source          Destination     Protocol  Length  Info
     1 0.000000    192.168.1.102   192.168.1.104   SNMP          92 get-request 1.3.6.1.4.1.11.2.3.9
     2 0.016960    192.168.1.104   192.168.1.102   SNMP          93 get-response 1.3.6.1.4.1.11.2.3.
    11 3.016971    192.168.1.102   192.168.1.104   SNMP          92 get-request 1.3.6.1.4.1.11.2.3.9
    12 3.034127    192.168.1.104   192.168.1.102   SNMP          93 get-response 1.3.6.1.4.1.11.2.3.
```

```
v User Datagram Protocol, Src Port: 4334, Dst Port: 161
    Source Port: 4334
    Destination Port: 161
    Length: 58
    Checksum: 0x65f8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (50 bytes)
> Simple Network Management Protocol
```

```
0000  00 30 c1 61 eb ed 00 08  74 4f 36 23 08 00 45 00   ·0·a····  tO6#··E·
0010  00 4e 02 fd 00 00 80 11  00 00 c0 a8 01 66 c0 a8   ·N······  ·····f··
0020  01 68 10 ee 00 a1 00 3a  65 f8 30 30 02 01 00 04   ·h·····:  e·00····
```

```
User Datagram Protocol: Protocol        分组: 73 · 已显示: 21 (28.8%)    配置: Default
```

通过读取图中红色框信息可知，UDP标头有4个字段，各字段分别为：

Source Port:源端口号

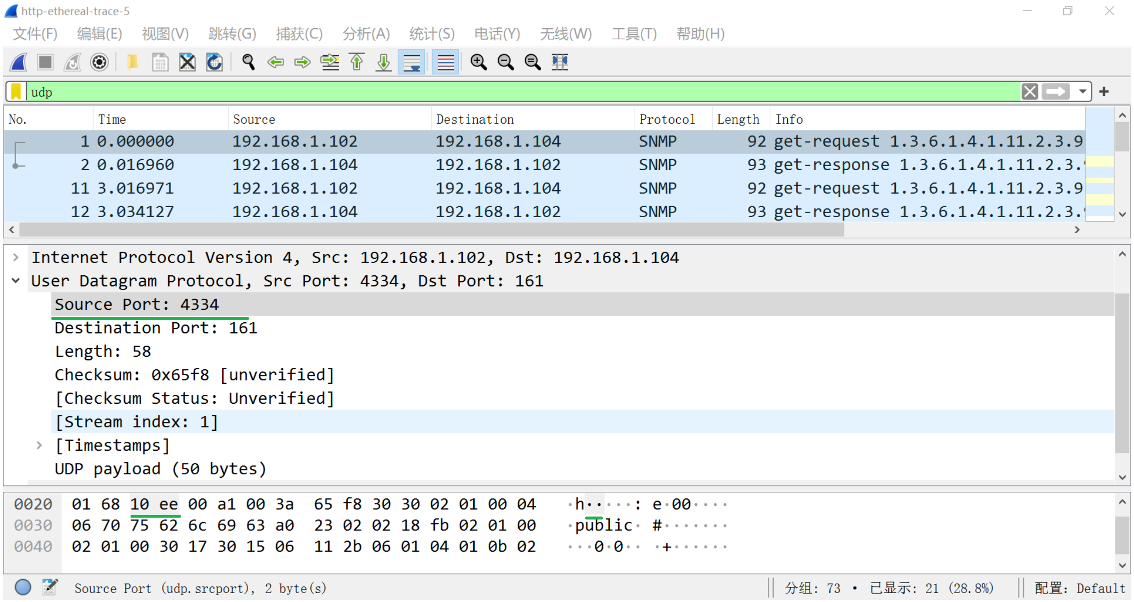
Destination Port:目标端口号

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：读取UDP数据包各个字段信息如下图所示：

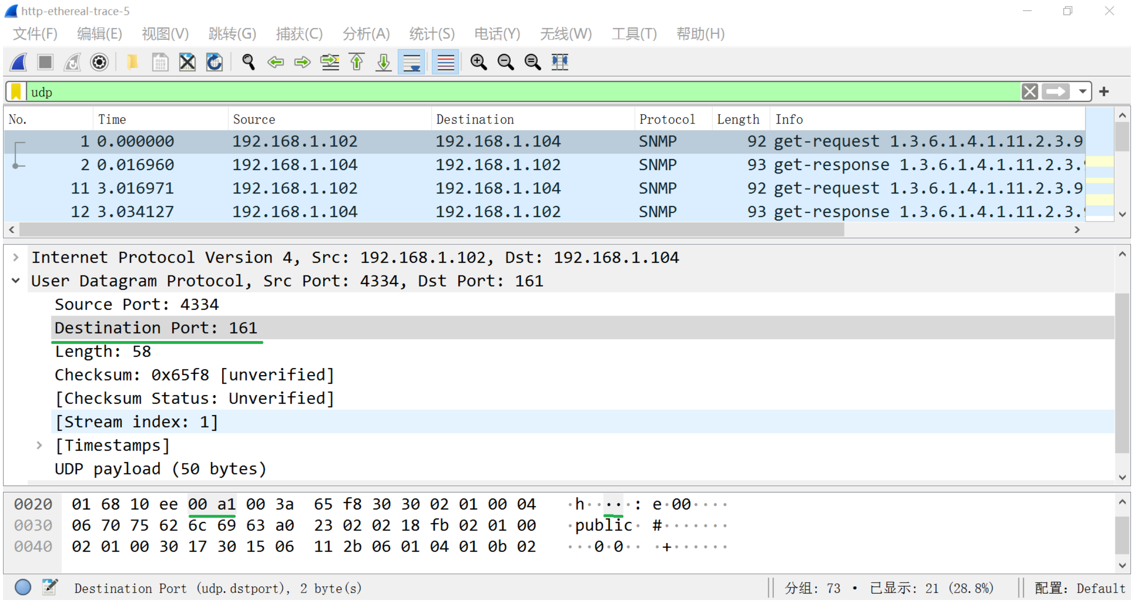

http-ethereal-trace-5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
udp

```
No.    Time        Source          Destination     Protocol  Length  Info
     1 0.000000    192.168.1.102   192.168.1.104   SNMP          92 get-request 1.3.6.1.4.1.11.2.3.9
     2 0.016960    192.168.1.104   192.168.1.102   SNMP          93 get-response 1.3.6.1.4.1.11.2.3.
    11 3.016971    192.168.1.102   192.168.1.104   SNMP          92 get-request 1.3.6.1.4.1.11.2.3.9
    12 3.034127    192.168.1.104   192.168.1.102   SNMP          93 get-response 1.3.6.1.4.1.11.2.3.
```

```
> 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]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (50 bytes)
```

```
0020  01 68 10 ee 00 a1 00 3a  65 f8 30 30 02 01 00 04   ·h·····:  e·00····
0030  06 70 75 62 6c 69 63 a0  23 02 02 18 fb 02 01 00   ·public·  #·······
0040  02 01 00 30 17 30 15 06  11 2b 06 01 04 01 0b 02   ···0·0··  ·+······
```

```
Source Port (udp.srcport), 2 byte(s)    分组: 73 · 已显示: 21 (28.8%)    配置: Default
```


http-ethereal-trace-5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

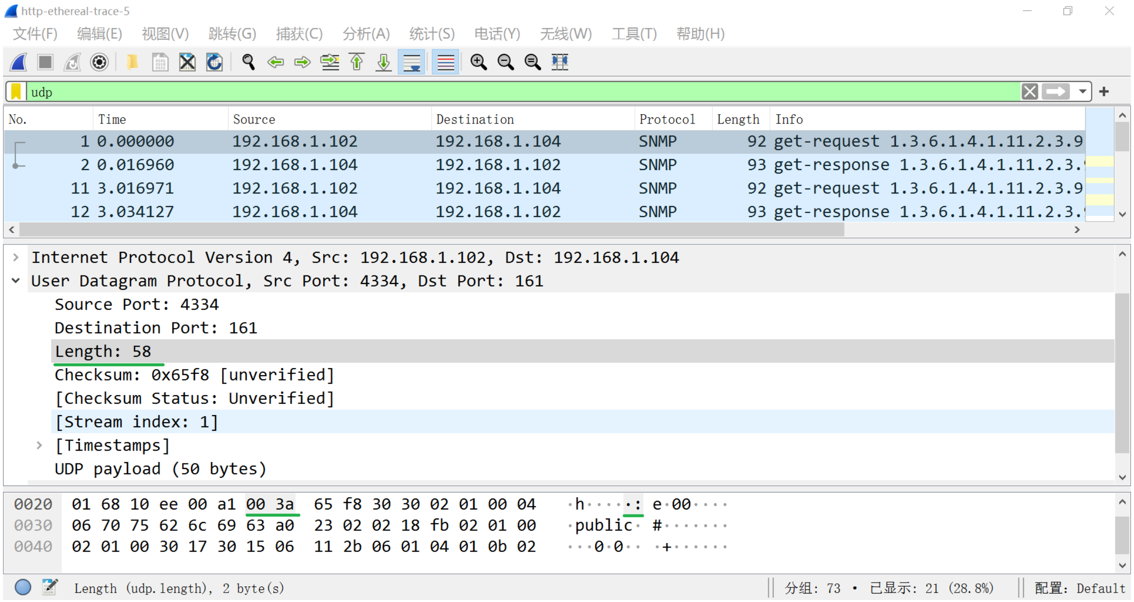
udp

```
No.   Time       Source          Destination     Protocol  Length  Info
   1 0.000000   192.168.1.102   192.168.1.104   SNMP        92  get-request 1.3.6.1.4.1.11.2.3.9
   2 0.016960   192.168.1.104   192.168.1.102   SNMP        93  get-response 1.3.6.1.4.1.11.2.3.
  11 3.016971   192.168.1.102   192.168.1.104   SNMP        92  get-request 1.3.6.1.4.1.11.2.3.9
  12 3.034127   192.168.1.104   192.168.1.102   SNMP        93  get-response 1.3.6.1.4.1.11.2.3.
```

```
> 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]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (50 bytes)
```

```
0020  01 68 10 ee 00 a1 00 3a  65 f8 30 30 02 01 00 04   ·h·····: e·00····
0030  06 70 75 62 6c 69 63 a0  23 02 02 18 fb 02 01 00   ·public· #·······
0040  02 01 00 30 17 30 15 06  11 2b 06 01 04 01 0b 02   ···0·0·· ·+······
```

Destination Port (udp.dstport), 2 byte(s) || 分组: 73 · 已显示: 21 (28.8%) || 配置: Default


http-ethereal-trace-5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

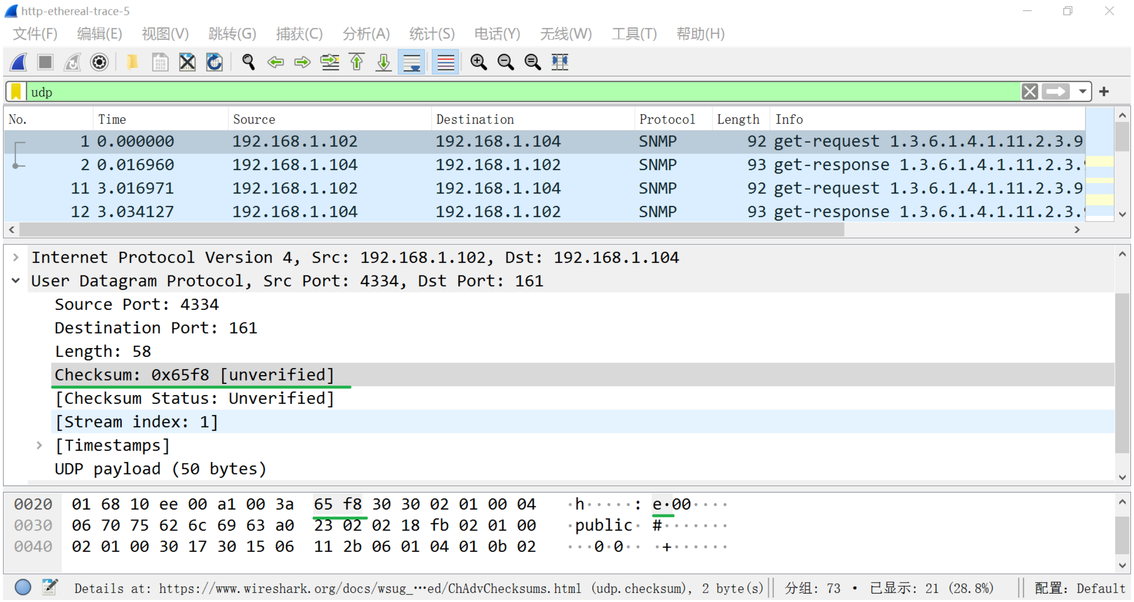
udp

```
No.   Time       Source          Destination     Protocol  Length  Info
   1 0.000000   192.168.1.102   192.168.1.104   SNMP        92  get-request 1.3.6.1.4.1.11.2.3.9
   2 0.016960   192.168.1.104   192.168.1.102   SNMP        93  get-response 1.3.6.1.4.1.11.2.3.
  11 3.016971   192.168.1.102   192.168.1.104   SNMP        92  get-request 1.3.6.1.4.1.11.2.3.9
  12 3.034127   192.168.1.104   192.168.1.102   SNMP        93  get-response 1.3.6.1.4.1.11.2.3.
```

```
> 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]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (50 bytes)
```

```
0020  01 68 10 ee 00 a1 00 3a  65 f8 30 30 02 01 00 04   ·h·····: e·00····
0030  06 70 75 62 6c 69 63 a0  23 02 02 18 fb 02 01 00   ·public· #·······
0040  02 01 00 30 17 30 15 06  11 2b 06 01 04 01 0b 02   ···0·0·· ·+······
```

Length (udp.length), 2 byte(s) || 分组: 73 · 已显示: 21 (28.8%) || 配置: Default


http-ethereal-trace-5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

udp

```
No.   Time       Source          Destination     Protocol  Length  Info
   1 0.000000   192.168.1.102   192.168.1.104   SNMP        92  get-request 1.3.6.1.4.1.11.2.3.9
   2 0.016960   192.168.1.104   192.168.1.102   SNMP        93  get-response 1.3.6.1.4.1.11.2.3.
  11 3.016971   192.168.1.102   192.168.1.104   SNMP        92  get-request 1.3.6.1.4.1.11.2.3.9
  12 3.034127   192.168.1.104   192.168.1.102   SNMP        93  get-response 1.3.6.1.4.1.11.2.3.
```

```
> 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]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (50 bytes)
```

```
0020  01 68 10 ee 00 a1 00 3a  65 f8 30 30 02 01 00 04   ·h·····: e·00····
0030  06 70 75 62 6c 69 63 a0  23 02 02 18 fb 02 01 00   ·public· #·······
0040  02 01 00 30 17 30 15 06  11 2b 06 01 04 01 0b 02   ···0·0·· ·+······
```

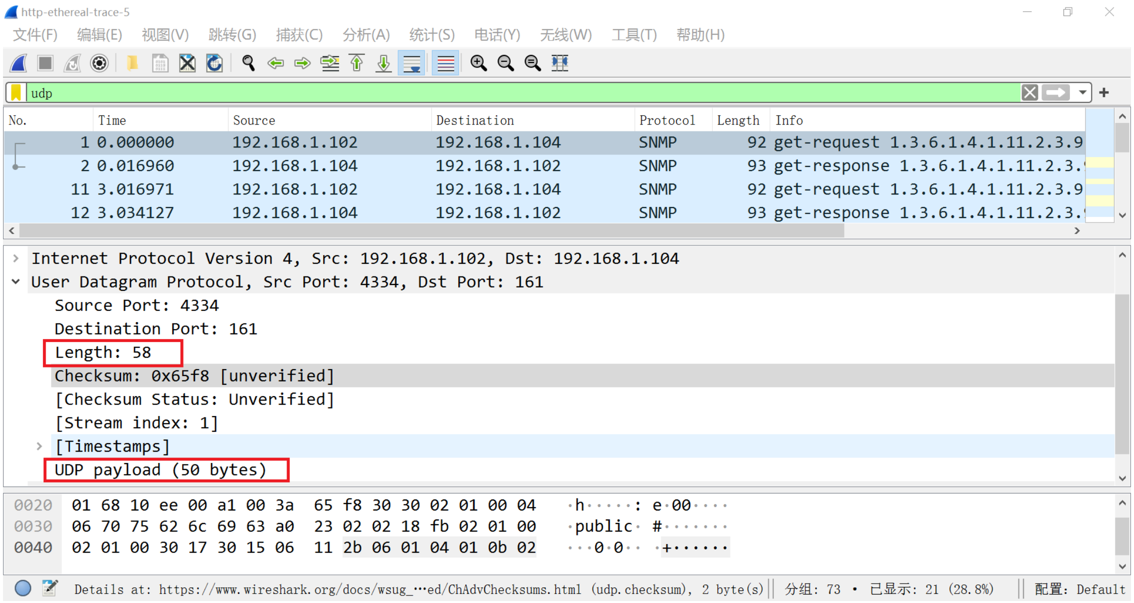
Details at: https://www.wireshark.org/docs/wsug_…ed/ChAdvChecksums.html (udp.checksum), 2 byte(s) || 分组: 73 · 已显示: 21 (28.8%) || 配置: Default

根据各字段绿色横线所示阴影部分，可知四个字段长度各为2bytes，故UDP标头总长度为4×2=8bytes。

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字段表示UDP报文段的字节数，是标头字段字节数与数据字段字节数的总和。

UDP数据包信息如下图所示：


http-ethereal-trace-5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
udp

```
No.     Time        Source          Destination     Protocol  Length  Info
      1 0.000000    192.168.1.102   192.168.1.104   SNMP        92 get-request 1.3.6.1.4.1.11.2.3.9
      2 0.016960    192.168.1.104   192.168.1.102   SNMP        93 get-response 1.3.6.1.4.1.11.2.3.
     11 3.016971    192.168.1.102   192.168.1.104   SNMP        92 get-request 1.3.6.1.4.1.11.2.3.9
     12 3.034127    192.168.1.104   192.168.1.102   SNMP        93 get-response 1.3.6.1.4.1.11.2.3.

> 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]
    [Stream index: 1]
  > [Timestamps]
    UDP payload (50 bytes)

0020  01 68 10 ee 00 a1 00 3a  65 f8 30 30 02 01 00 04   ·h·····: e·00····
0030  06 70 75 62 6c 69 63 a0  23 02 02 18 fb 02 01 00   ·public· #·······
0040  02 01 00 30 17 30 15 06  11 2b 06 01 04 01 0b 02   ···0·0·· ·+······

Details at: https://www.wireshark.org/docs/wsug_…ed/ChAdvChecksums.html (udp.checksum), 2 byte(s) | 分组: 73 • 已显示: 21 (28.8%) | 配置: Default
```

根据红色框中信息，UDP报文段字节数为58bytes，数据字段字节数为50bytes，可得标头字段字节数为8bytes，与第二题结果相同，故原结论得证。

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)

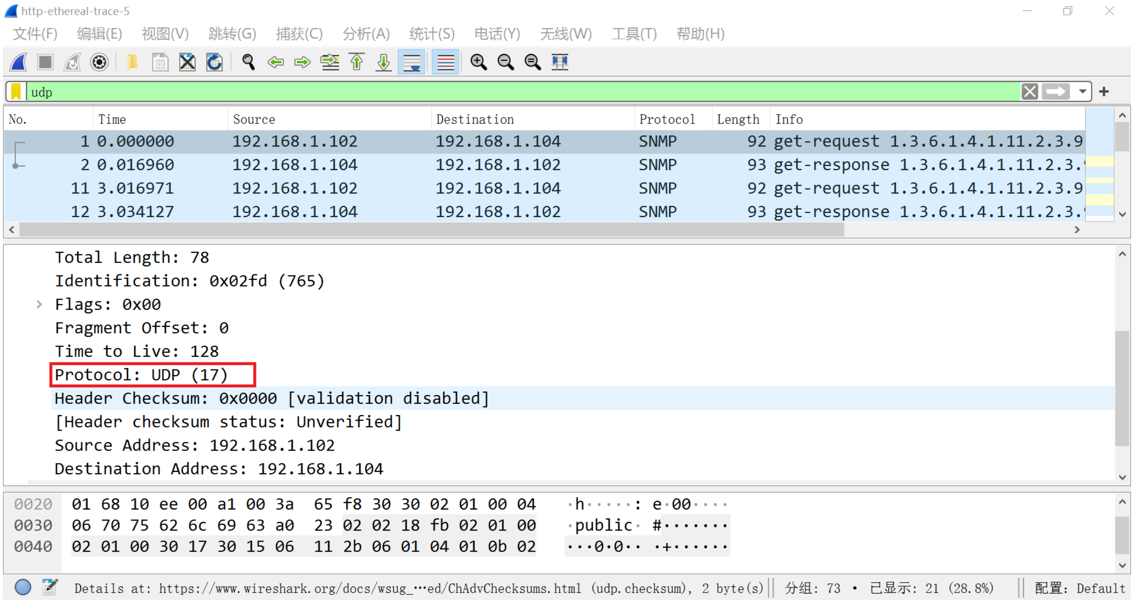
答：由于长度共有16位，故UDP最大长度为2^16=65536bytes,减去标头字段占用的8bytes，有效负载最大字节数为（65536-1-8）=65527bytes。

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

答：根据第四题，UDP最大长度为65536bytes，由于端口号从0开始计算，故最大端口号为（65536-1）=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).

答：UDP数据包信息如下图所示：


http-ethereal-trace-5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
udp

```
No.     Time        Source          Destination     Protocol  Length  Info
      1 0.000000    192.168.1.102   192.168.1.104   SNMP          92  get-request 1.3.6.1.4.1.11.2.3.9
      2 0.016960    192.168.1.104   192.168.1.102   SNMP          93  get-response 1.3.6.1.4.1.11.2.3.
     11 3.016971    192.168.1.102   192.168.1.104   SNMP          92  get-request 1.3.6.1.4.1.11.2.3.9
     12 3.034127    192.168.1.104   192.168.1.102   SNMP          93  get-response 1.3.6.1.4.1.11.2.3.
```

```
    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]
    Source Address: 192.168.1.102
    Destination Address: 192.168.1.104
```

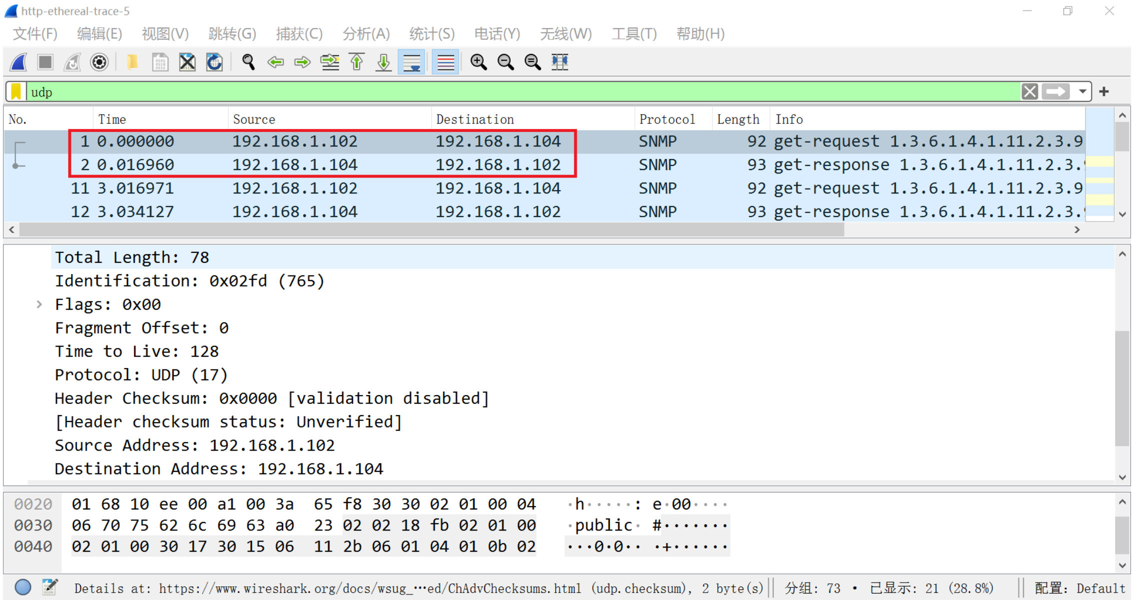
```
0020  01 68 10 ee 00 a1 00 3a  65 f8 30 30 02 01 00 04   ·h·····: e·00····
0030  06 70 75 62 6c 69 63 a0  23 02 02 18 fb 02 01 00   ·public· #·······
0040  02 01 00 30 17 30 15 06  11 2b 06 01 04 01 0b 02   ···0·0·· ·+······
```

Details at: https://www.wireshark.org/docs/wsug_…ed/ChAdvChecksums.html (udp.checksum), 2 byte(s) | 分组: 73 · 已显示: 21 (28.8%) | 配置: Default

根据图中红色框中信息可知：UDP协议号十进制表示为17，十六进制表示为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.

答：观察1号与2号数据包并进行分析，两者信息如下图所示：


http-ethereal-trace-5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
udp

```
No.     Time        Source          Destination     Protocol  Length  Info
      1 0.000000    192.168.1.102   192.168.1.104   SNMP          92  get-request 1.3.6.1.4.1.11.2.3.9
      2 0.016960    192.168.1.104   192.168.1.102   SNMP          93  get-response 1.3.6.1.4.1.11.2.3.
     11 3.016971    192.168.1.102   192.168.1.104   SNMP          92  get-request 1.3.6.1.4.1.11.2.3.9
     12 3.034127    192.168.1.104   192.168.1.102   SNMP          93  get-response 1.3.6.1.4.1.11.2.3.
```

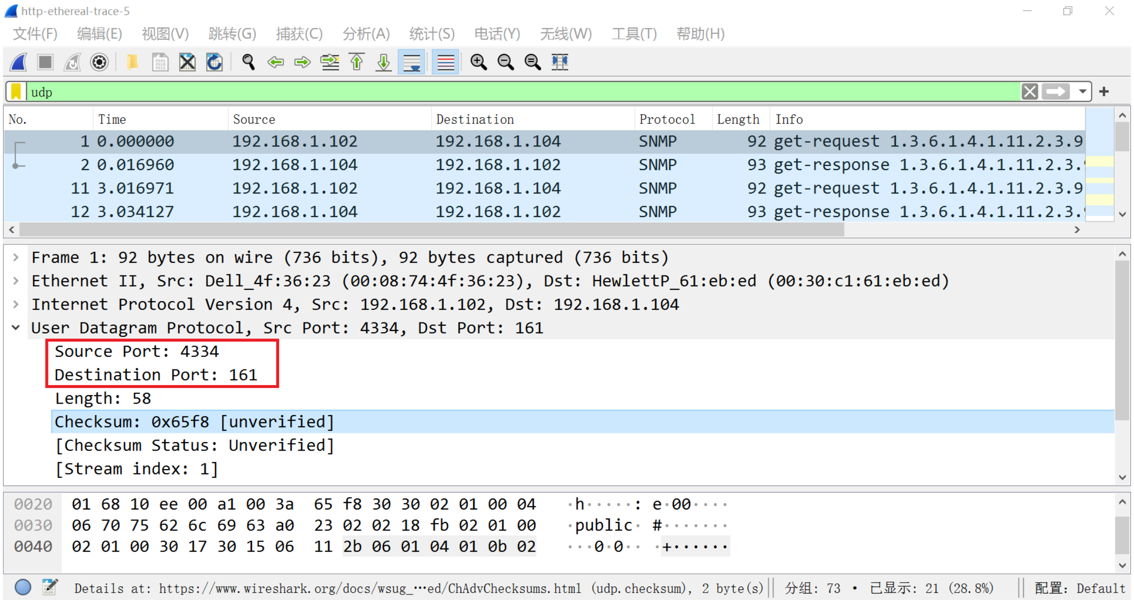
```
    Total Length: 78
    Identification: 0x02fd (765)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 192.168.1.104
```

```
0020  01 68 10 ee 00 a1 00 3a  65 f8 30 30 02 01 00 04   ·h·····: e·00····
0030  06 70 75 62 6c 69 63 a0  23 02 02 18 fb 02 01 00   ·public· #·······
0040  02 01 00 30 17 30 15 06  11 2b 06 01 04 01 0b 02   ···0·0·· ·+······
```

Details at: https://www.wireshark.org/docs/wsug_…ed/ChAdvChecksums.html (udp.checksum), 2 byte(s) | 分组: 73 · 已显示: 21 (28.8%) | 配置: Default

由上图红色框中信息可知，1号数据包的源IP地址为2号数据包的目的IP地址、1号数据包的目的IP地址为2号数据包的源IP地址，故1号数据包为发送UDP数据包、2号数据包为接收UDP数据包。

1号、2号数据包的具体信息如下图所示：

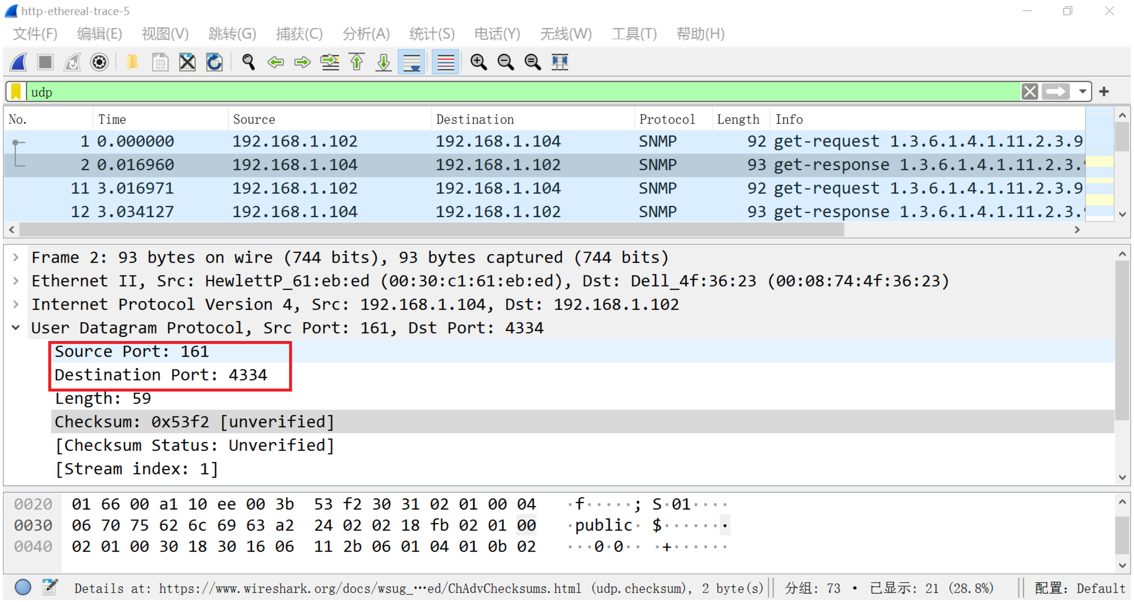

http-ethereal-trace-5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
udp

```
No.   Time        Source          Destination     Protocol  Length  Info
  1 0.000000    192.168.1.102   192.168.1.104   SNMP        92 get-request 1.3.6.1.4.1.11.2.3.9
  2 0.016960    192.168.1.104   192.168.1.102   SNMP        93 get-response 1.3.6.1.4.1.11.2.3.
 11 3.016971    192.168.1.102   192.168.1.104   SNMP        92 get-request 1.3.6.1.4.1.11.2.3.9
 12 3.034127    192.168.1.104   192.168.1.102   SNMP        93 get-response 1.3.6.1.4.1.11.2.3.
```

```
> 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]
    [Stream index: 1]
```

```
0020  01 68 10 ee 00 a1 00 3a  65 f8 30 30 02 01 00 04   ·h·····: e·00····
0030  06 70 75 62 6c 69 63 a0  23 02 02 18 fb 02 01 00   ·public· #·······
0040  02 01 00 30 17 30 15 06  11 2b 06 01 04 01 0b 02   ···0·0·· ·+······
```

Details at: https://www.wireshark.org/docs/wsug_…ed/ChAdvChecksums.html (udp.checksum), 2 byte(s) | 分组: 73 · 已显示: 21 (28.8%) | 配置: Default


http-ethereal-trace-5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
udp

```
No.   Time        Source          Destination     Protocol  Length  Info
  1 0.000000    192.168.1.102   192.168.1.104   SNMP        92 get-request 1.3.6.1.4.1.11.2.3.9
  2 0.016960    192.168.1.104   192.168.1.102   SNMP        93 get-response 1.3.6.1.4.1.11.2.3.
 11 3.016971    192.168.1.102   192.168.1.104   SNMP        92 get-request 1.3.6.1.4.1.11.2.3.9
 12 3.034127    192.168.1.104   192.168.1.102   SNMP        93 get-response 1.3.6.1.4.1.11.2.3.
```

```
> 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]
    [Stream index: 1]
```

```
0020  01 66 00 a1 10 ee 00 3b  53 f2 30 31 02 01 00 04   ·f·····; S·01····
0030  06 70 75 62 6c 69 63 a2  24 02 02 18 fb 02 01 00   ·public· $·······
0040  02 01 00 30 18 30 16 06  11 2b 06 01 04 01 0b 02   ···0·0·· ·+······
```

Details at: https://www.wireshark.org/docs/wsug_…ed/ChAdvChecksums.html (udp.checksum), 2 byte(s) | 分组: 73 · 已显示: 21 (28.8%) | 配置: Default

根据上图红色框中信息可知，1号数据包的源端口号为2号数据包的目的端口号、1号数据包的目的端口号为2号数据包的源端口号。

五.实验收获与感想

1. 本次实验深入了解了UDP传输协议，并掌握了UDP的报文格式。
2. 通过wireshark捕获UDP数据包，提高了对数据包信息的读取能力，学习了读取数据包更多类型的信息。