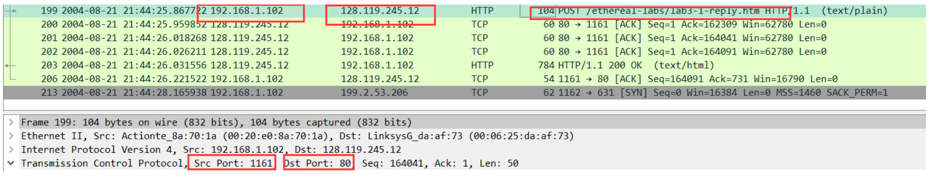
lab4 Wireshark_TCP

- 学号:1813075
- 姓名:刘茵

1. Capturing a bulk TCP transfer from your computer to a remote server.

2. A first look at the captured trace

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it’s probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the “details of the selected packet header window” (refer to Figure 2 in the “Getting Started with Wireshark” Lab if you’re uncertain about the Wireshark windows.



```
199 2004-08-21 21:44:25.867722 192.168.1.102    128.119.245.12   HTTP   104 POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
200 2004-08-21 21:44:25.959852 128.119.245.12   192.168.1.102    TCP     60 80 → 1161 [ACK] Seq=1 Ack=162309 Win=62780 Len=0
201 2004-08-21 21:44:26.018268 128.119.245.12   192.168.1.102    TCP     60 80 → 1161 [ACK] Seq=1 Ack=164041 Win=62780 Len=0
202 2004-08-21 21:44:26.026211 128.119.245.12   192.168.1.102    TCP     60 80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780 Len=0
203 2004-08-21 21:44:26.031556 128.119.245.12   192.168.1.102    HTTP   784 HTTP/1.1 200 OK  (text/html)
206 2004-08-21 21:44:26.221522 192.168.1.102    128.119.245.12   TCP     54 1161 → 80 [ACK] Seq=164091 Ack=731 Win=16790 Len=0
213 2004-08-21 21:44:28.165938 192.168.1.102    199.2.53.206     TCP     62 1162 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

> Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 50
```

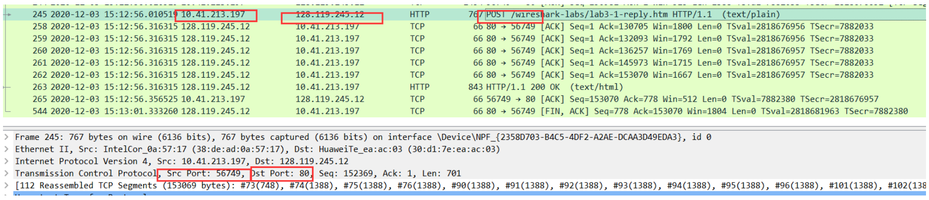
答：IP地址：192.168.1.102

TCP发送端口号：1161

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?
答：IP地址：128.119.245.12

TCP接收端口号：80

3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?



```
245 2020-12-03 15:12:56.010519 10.41.213.197    128.119.245.12   HTTP   767 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
258 2020-12-03 15:12:56.316315 128.119.245.12   10.41.213.197    TCP     66 80 → 56749 [ACK] Seq=1 Ack=130705 Win=1800 Len=0 TSval=2818676956 TSecr=7882033
259 2020-12-03 15:12:56.316315 128.119.245.12   10.41.213.197    TCP     66 80 → 56749 [ACK] Seq=1 Ack=132093 Win=1792 Len=0 TSval=2818676956 TSecr=7882033
260 2020-12-03 15:12:56.316315 128.119.245.12   10.41.213.197    TCP     66 80 → 56749 [ACK] Seq=1 Ack=136257 Win=1769 Len=0 TSval=2818676957 TSecr=7882033
261 2020-12-03 15:12:56.316315 128.119.245.12   10.41.213.197    TCP     66 80 → 56749 [ACK] Seq=1 Ack=145973 Win=1715 Len=0 TSval=2818676957 TSecr=7882033
262 2020-12-03 15:12:56.316315 128.119.245.12   10.41.213.197    TCP     66 80 → 56749 [ACK] Seq=1 Ack=153070 Win=1667 Len=0 TSval=2818676957 TSecr=7882033
263 2020-12-03 15:12:56.316315 128.119.245.12   10.41.213.197    HTTP   843 HTTP/1.1 200 OK  (text/html)
265 2020-12-03 15:12:56.356525 10.41.213.197    128.119.245.12   TCP     66 56749 → 80 [ACK] Seq=153070 Ack=778 Win=512 Len=0 TSval=7882380 TSecr=2818676957
544 2020-12-03 15:13:01.333260 128.119.245.12   10.41.213.197    TCP     66 80 → 56749 [FIN, ACK] Seq=778 Ack=153070 Win=1804 Len=0 TSval=2818681963 TSecr=7882380

> Frame 245: 767 bytes on wire (6136 bits), 767 bytes captured (6136 bits) on interface \Device\NPF_{2358D703-B4C5-4DF2-A2AE-DCAA3D49EDA3}, id 0
> Ethernet II, Src: IntelCor_0a:57:17 (38:de:ad:0a:57:17), Dst: HuaweiTe_ea:ac:03 (30:d1:7e:ea:ac:03)
> Internet Protocol Version 4, Src: 10.41.213.197, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56749, Dst Port: 80, Seq: 152369, Ack: 1, Len: 701
> [112 Reassembled TCP Segments (153069 bytes): #73(748), #74(1388), #75(1388), #76(1388), #90(1388), #91(1388), #92(1388), #93(1388), #94(1388), #95(1388), #96(1388), #101(1388), #102(138
```

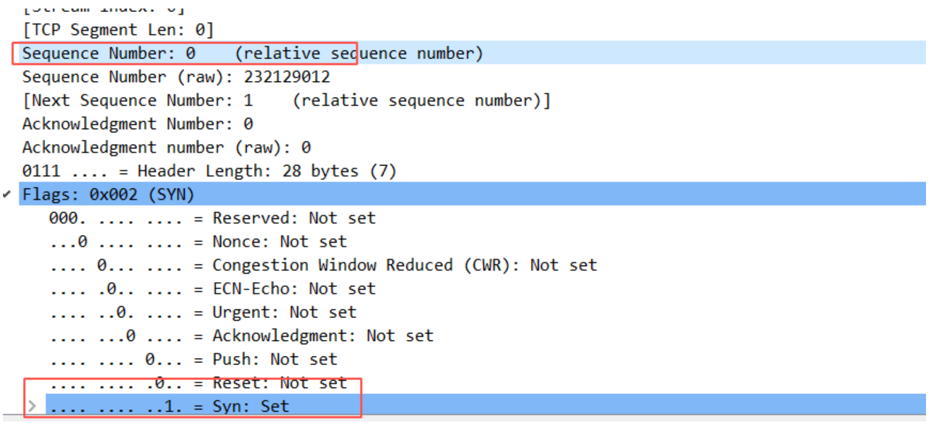
答：IP地址：10.41.213.197

TCP发送端口号：56749

3. TCP Basics

（用官方文档）

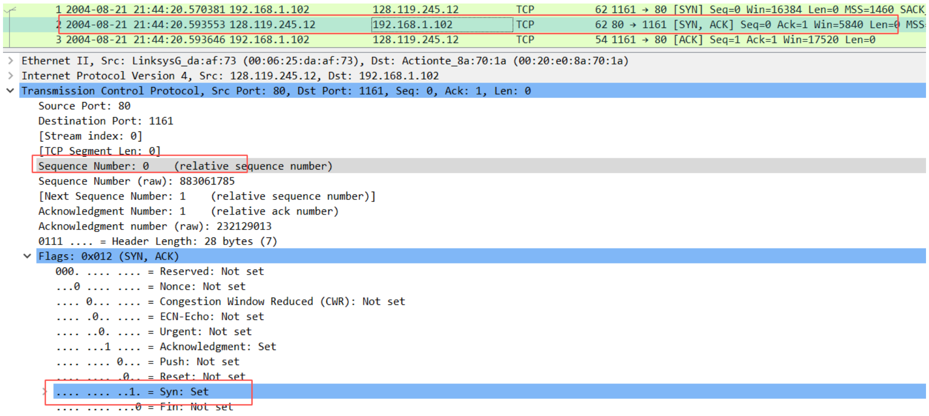
4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?



```
[Stream index: 0]
[TCP Segment Len: 0]
Sequence Number: 0    (relative sequence number)
Sequence Number (raw): 232129012
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0111 .... = Header Length: 28 bytes (7)
Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..1. = Syn: Set
```

答：SYN=1 seq=0（相对序列号） SYN报文负责建立连接，选择客户端初始的序列号.

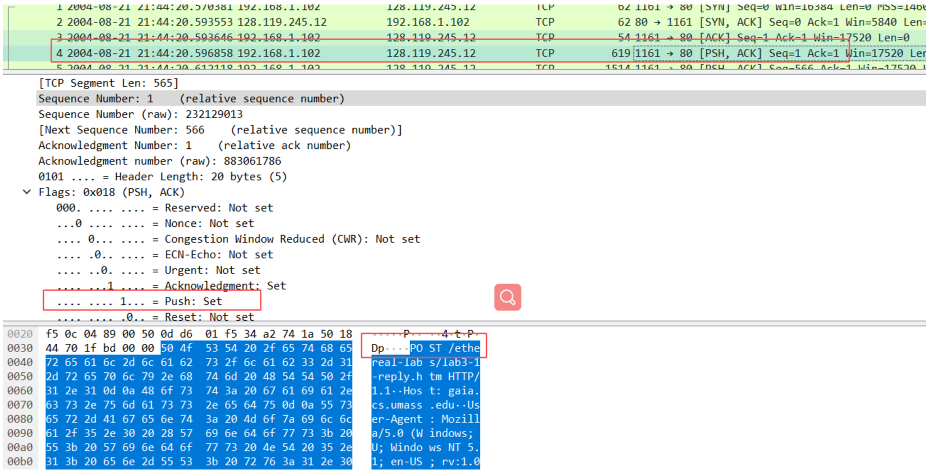
5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?



```
1 2004-08-21 21:44:20.570381 192.168.1.102    128.119.245.12   TCP   62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_
2 2004-08-21 21:44:20.593553 128.119.245.12   192.168.1.102    TCP   62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
3 2004-08-21 21:44:20.593646 192.168.1.102    128.119.245.12   TCP   54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0

> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
v Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 883061785
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 232129013
    0111 .... = Header Length: 28 bytes (7)
  v Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
```

答：seq=0 Acknowledgment=1 Acknowledgment=X（SYN中的seq）+1，确认客户端的连接，选择服务器端初始的序列号。

6. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you’ll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a “POST” within its DATA field.



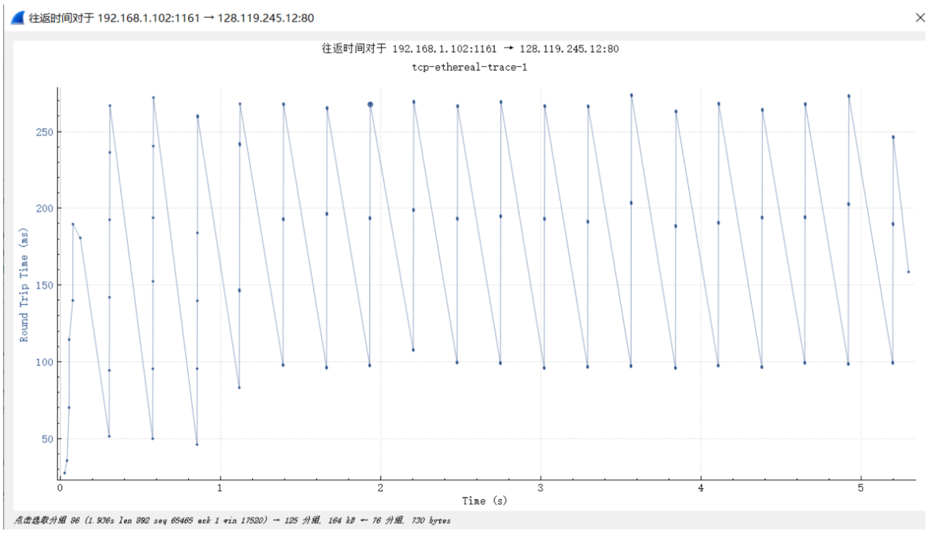
```
1 2004-08-21 21:44:20.570381 192.168.1.102    128.119.245.12   TCP   62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=146
2 2004-08-21 21:44:20.593553 128.119.245.12   192.168.1.102    TCP   62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=
3 2004-08-21 21:44:20.593646 192.168.1.102    128.119.245.12   TCP   54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4 2004-08-21 21:44:20.596858 192.168.1.102    128.119.245.12   TCP  619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len
5 2004-08-21 21:44:20.612118 192.168.1.102    128.119.245.12   TCP 1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 L

    [TCP Segment Len: 565]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 232129013
    [Next Sequence Number: 566    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 883061786
    0101 .... = Header Length: 20 bytes (5)
  v Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set

0020  f5 0c 04 89 00 50 0d d6  01 f5 34 a2 74 1a 50 18   ·····P·· ··4·t·P·
0030  44 70 1f bd 00 00 50 4f  53 54 20 2f 65 74 68 65   Dp····PO ST /ethe
0040  72 65 61 6c 2d 6c 61 62  73 2f 6c 61 62 33 2d 31   real-lab s/lab3-1
0050  2d 72 65 70 6c 79 2e 68  74 6d 20 48 54 54 50 2f   -reply.h tm HTTP/
0060  31 2e 31 0d 0a 48 6f 73  74 3a 20 67 61 69 61 2e   1.1··Hos t: gaia.
0070  63 73 2e 75 6d 61 73 73  2e 65 64 75 0d 0a 55 73   cs.umass .edu··Us
0080  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0090  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 3b 20   a/5.0 (W indows; 
00a0  55 3b 20 57 69 6e 64 6f  77 73 20 4e 54 20 35 2e   U; Windo ws NT 5.
00b0  31 3b 20 65 6e 2d 55 53  3b 20 72 76 3a 31 2e 30   1; en-US ; rv:1.0
```

答：seq= 1 PSH 标志表示有数据传输。

7. 答:前六个TCP报文的具体信息:

EstimatedRTT = (1 - a) × EstimatedRTT + a × SampleRTT

计数	序列号	发送时间	ACK时间	RTT值	ESTIMATEDRTT值
1	1	0.026477	0.053937	0.02746	0.02746
2	566	0.041737	0.077294	0.035557	0.028472125
3	2026	0.054026	0.124085	0.070059	0.033670484375
4	3486	0.054690	0.169118	0.114428	0.043765173828125
5	4046	0.077405	0.217299	0.139894	0.05578127709960937
6	6406	0.078157	0.267802	0.189645	0.07251424246215821



点击选取分组 86 (1.936s len 892 seq 65465 ack 1 win 17520) → 125 分组, 164 kB ← 76 分组, 730 bytes

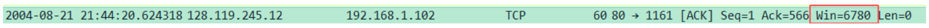
8. What is the length of each of the first six TCP segments?

答： 前6个TCP报文的长度分别为：565，1460，1460，1460，1460，1460

9. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

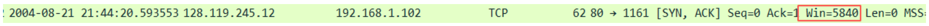
答：

对于服务器而言，收到的最小可用缓冲区空间量为 6780。



```
2004-08-21 21:44:20.624318 128.119.245.12          192.168.1.102          TCP          60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
```

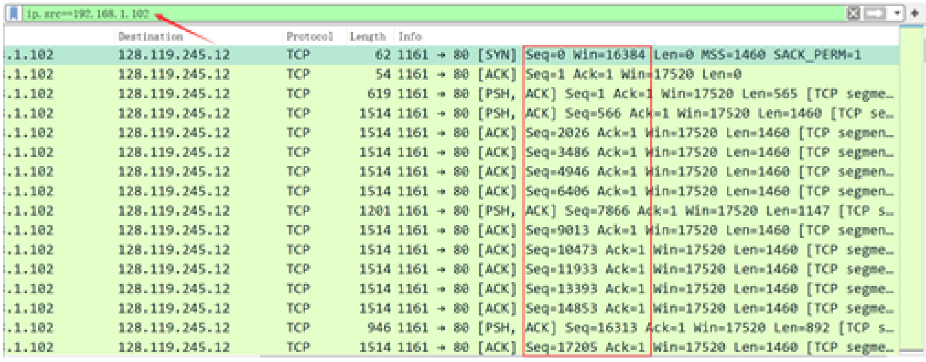
对于主机而言，收到的最小可用缓冲区空间量为 5840。



```
2004-08-21 21:44:20.593553 128.119.245.12          192.168.1.102          TCP          62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
```

缺少接收器缓冲区空间会限制发送方传送 TCP 区段，这是因为 TCP 的**流量控制服务**，能够消除发送方使接收方缓存溢出的可能性，使得发送方的发送速率与接收方应用程序的读取速率相匹配。实现的方式是**滑动窗口协议**。

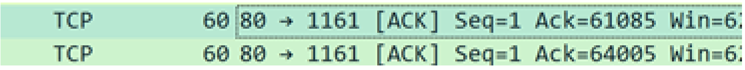
10. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?



```
ip.src==192.168.1.102

         Destination        Protocol  Length  Info
.1.102   128.119.245.12     TCP          62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
.1.102   128.119.245.12     TCP          54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
.1.102   128.119.245.12     TCP         619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segme…
.1.102   128.119.245.12     TCP        1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP se…
.1.102   128.119.245.12     TCP        1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segmen…
.1.102   128.119.245.12     TCP        1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segmen…
.1.102   128.119.245.12     TCP        1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segmen…
.1.102   128.119.245.12     TCP        1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segmen…
.1.102   128.119.245.12     TCP        1201 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP s…
.1.102   128.119.245.12     TCP        1514 1161 → 80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460 [TCP segmen…
.1.102   128.119.245.12     TCP        1514 1161 → 80 [ACK] Seq=10473 Ack=1 Win=17520 Len=1460 [TCP segme…
.1.102   128.119.245.12     TCP        1514 1161 → 80 [ACK] Seq=11933 Ack=1 Win=17520 Len=1460 [TCP segme…
.1.102   128.119.245.12     TCP        1514 1161 → 80 [ACK] Seq=13393 Ack=1 Win=17520 Len=1460 [TCP segme…
.1.102   128.119.245.12     TCP        1514 1161 → 80 [ACK] Seq=14853 Ack=1 Win=17520 Len=1460 [TCP segme…
.1.102   128.119.245.12     TCP         946 1161 → 80 [PSH, ACK] Seq=16313 Ack=1 Win=17520 Len=892 [TCP s…
.1.102   128.119.245.12     TCP        1514 1161 → 80 [ACK] Seq=17205 Ack=1 Win=17520 Len=1460 [TCP segme…
```

答： 没有重传报文。在过滤器中输入ip.src==192.168.1.102，发现序列号一直在增加。

11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment



```
TCP          60 80 → 1161 [ACK] Seq=1 Ack=61085 Win=6
TCP          60 80 → 1161 [ACK] Seq=1 Ack=64005 Win=6
```

答：一般都是1460。

64005-61085=2920=1460*2.接收方收到一个报文即发送一个ACK，没有报多个确认合并，可以确认，根据 ACK 序列号的顺序来推测。

12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

平均吞吐量 = 传输数据的比特数 F ÷ 接收方接收所有数据所用时间 T

答:数据量：164091-1 = 164090 bytes

时间：5.455830-0.026477 = 5.4294

结果：164090/5.4294 = 30.222Kbytes/sec