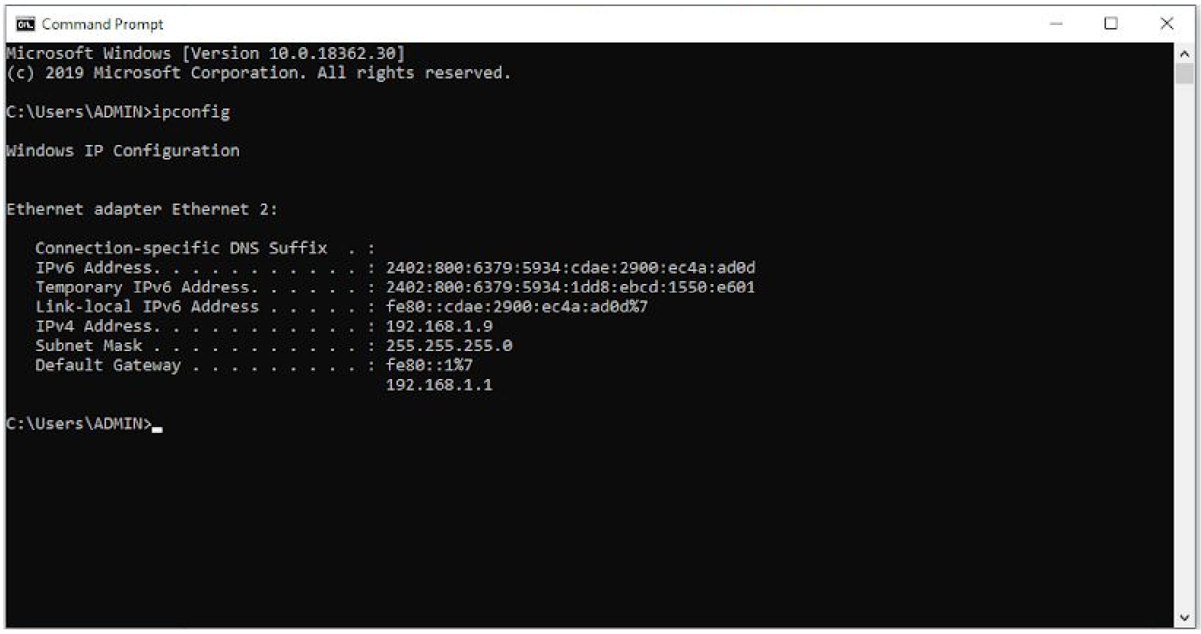
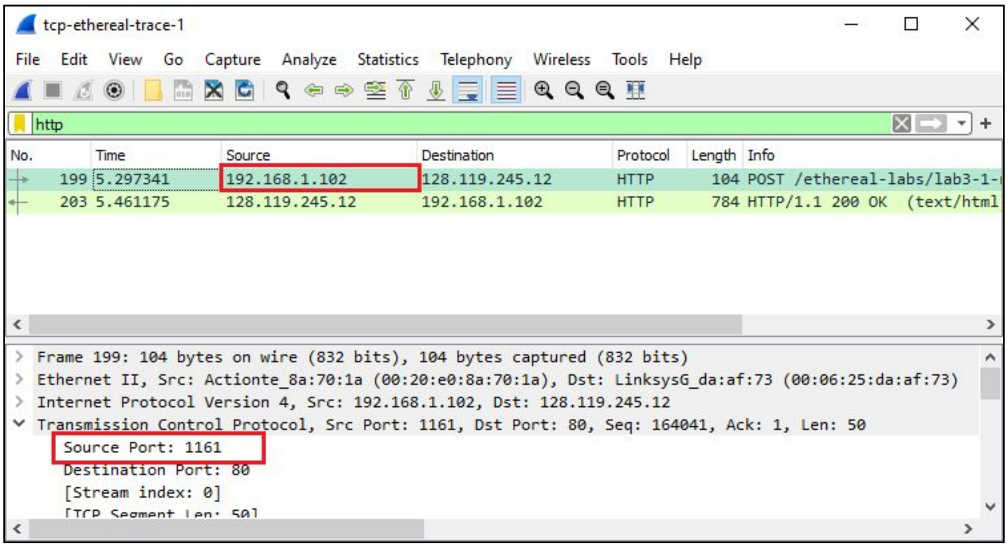
Computer Network
Wireshark Lab 3b: TCP v8.0

Lecturer: Mr. Nguyễn Mạnh Thìn
Student: Trần Quốc Anh - 1852247



```
Microsoft Windows [Version 10.0.18362.30]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\ADMIN>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2402:800:6379:5934:cdae:2900:ec4a:ad0d
   Temporary IPv6 Address. . . . . . : 2402:800:6379:5934:1dd8:ebcd:1550:e601
   Link-local IPv6 Address . . . . . : fe80::cdae:2900:ec4a:ad0d%7
   IPv4 Address. . . . . . . . . . . : 192.168.1.9
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%7
                                       192.168.1.1

C:\Users\ADMIN>_
```

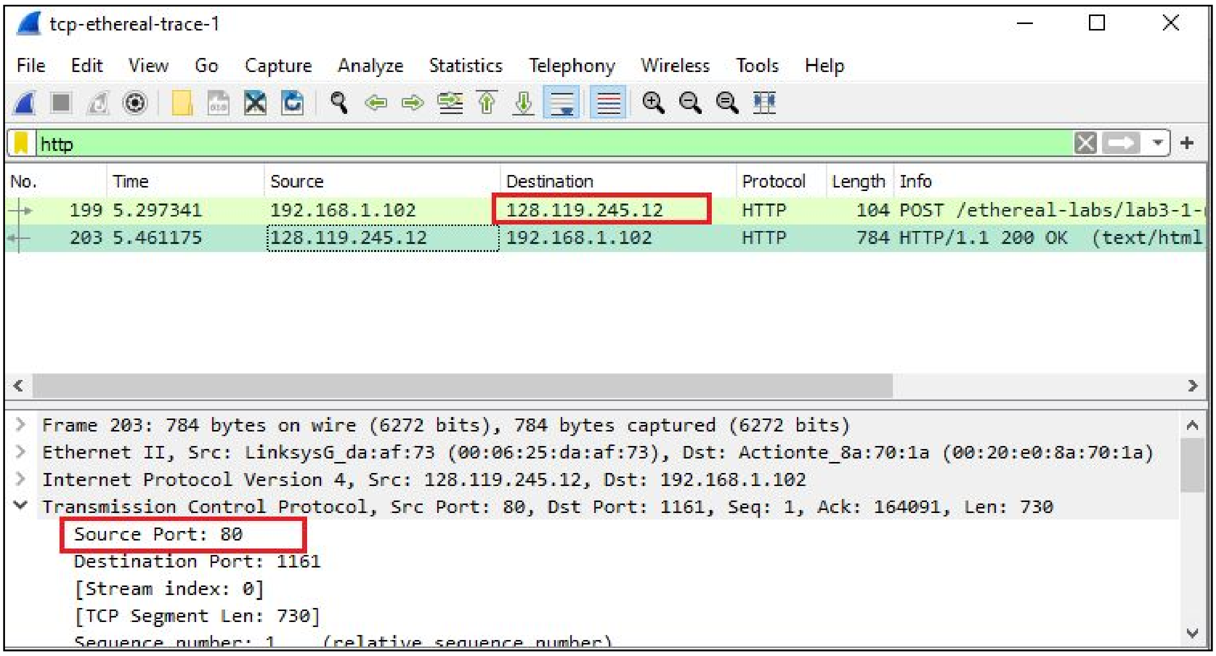
1. **What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details 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.**
   - Source IP Address: 192.168.1.102
   - TCP port number: 1161


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source          Destination     Protocol  Length  Info
 199  5.297341    192.168.1.102   128.119.245.12  HTTP      104 POST /ethereal-labs/lab3-1-
 203  5.461175    128.119.245.12  192.168.1.102   HTTP      784 HTTP/1.1 200 OK  (text/html
```

```
> 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
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 50]
```

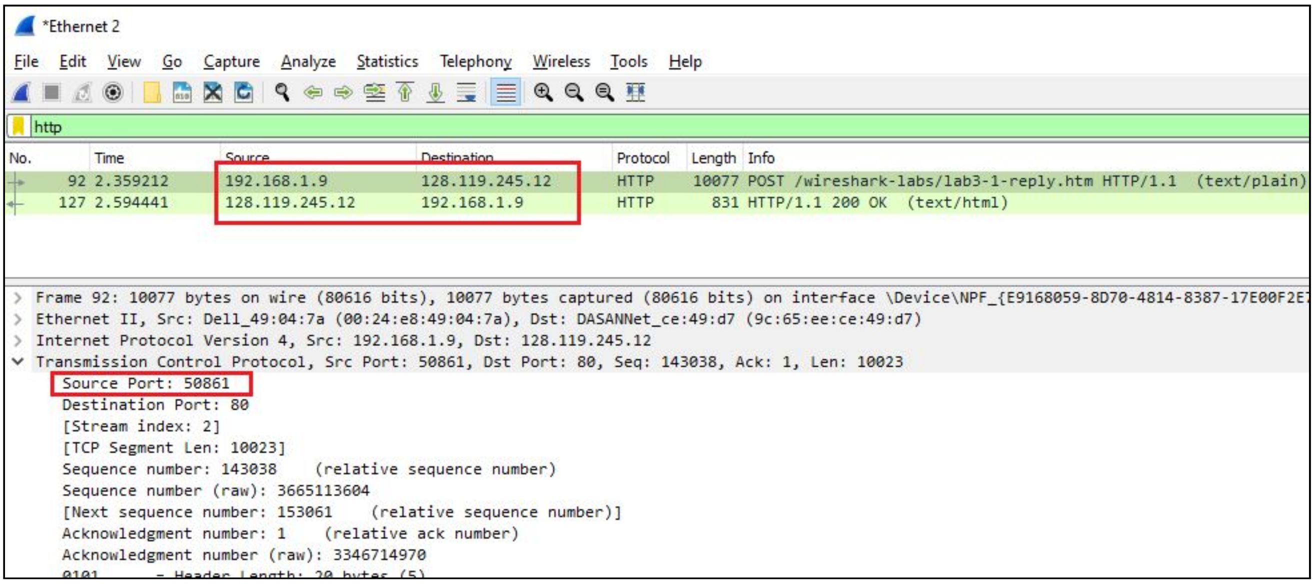
2. **What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?**
    - Destination IP address: 128.119.245.12
    - TCP port number: 80


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source          Destination     Protocol  Length  Info
 199  5.297341    192.168.1.102   128.119.245.12  HTTP      104 POST /ethereal-labs/lab3-1-
 203  5.461175    128.119.245.12  192.168.1.102   HTTP      784 HTTP/1.1 200 OK  (text/html
```

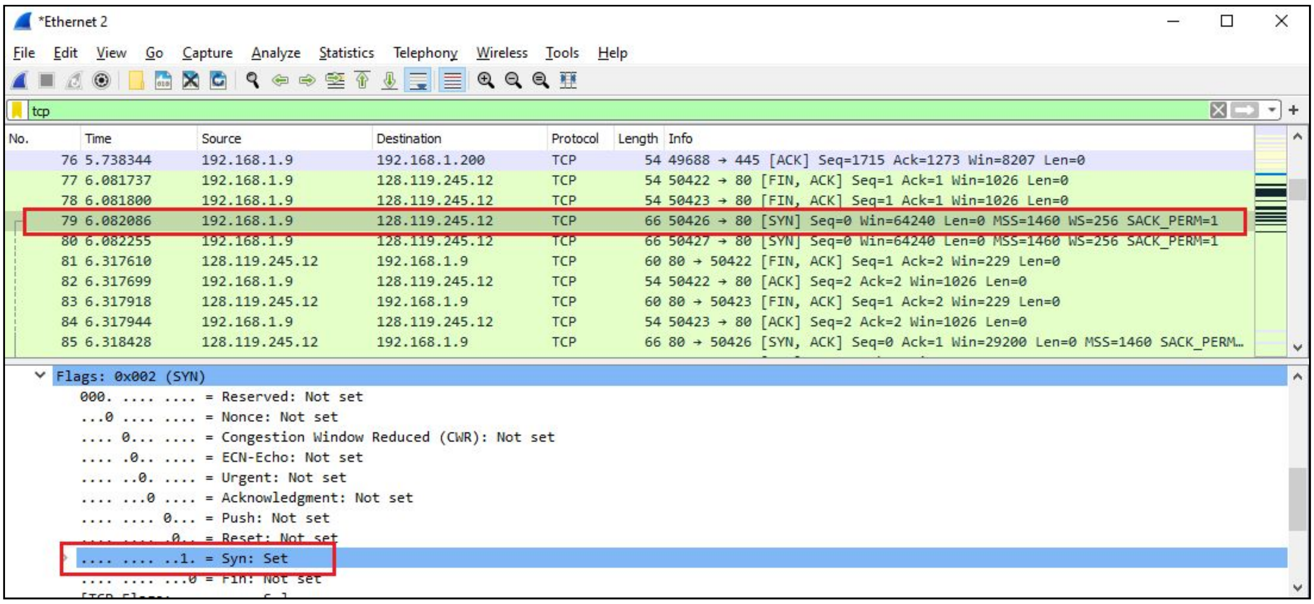
```
> Frame 203: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
v Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 1, Ack: 164091, Len: 730
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [TCP Segment Len: 730]
    Sequence number: 1    (relative sequence number)
```

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?**
    - My IP address: 192.168.1.1
    - My TCP port number: 50861



```
*Ethernet 2
http
No.     Time         Source          Destination     Protocol  Length Info
   92 2.359212       192.168.1.9     128.119.245.12  HTTP      10077 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
  127 2.594441       128.119.245.12  192.168.1.9     HTTP        831 HTTP/1.1 200 OK  (text/html)

> Frame 92: 10077 bytes on wire (80616 bits), 10077 bytes captured (80616 bits) on interface \Device\NPF_{E9168059-8D70-4814-8387-17E00F2E
> Ethernet II, Src: Dell_49:04:7a (00:24:e8:49:04:7a), Dst: DASANNet_ce:49:d7 (9c:65:ee:ce:49:d7)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 50861, Dst Port: 80, Seq: 143038, Ack: 1, Len: 10023
    Source Port: 50861
    Destination Port: 80
    [Stream index: 2]
    [TCP Segment Len: 10023]
    Sequence number: 143038    (relative sequence number)
    Sequence number (raw): 3665113604
    [Next sequence number: 153061    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 3346714970
    0101 .... = Header Length: 20 bytes (5)
```

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?**
    - The sequence number of TCP SYN segment used to initiate the TCP connection is: 0
    - The SYN flag is set to 1 and it indicates that this segment is a SYN segment.

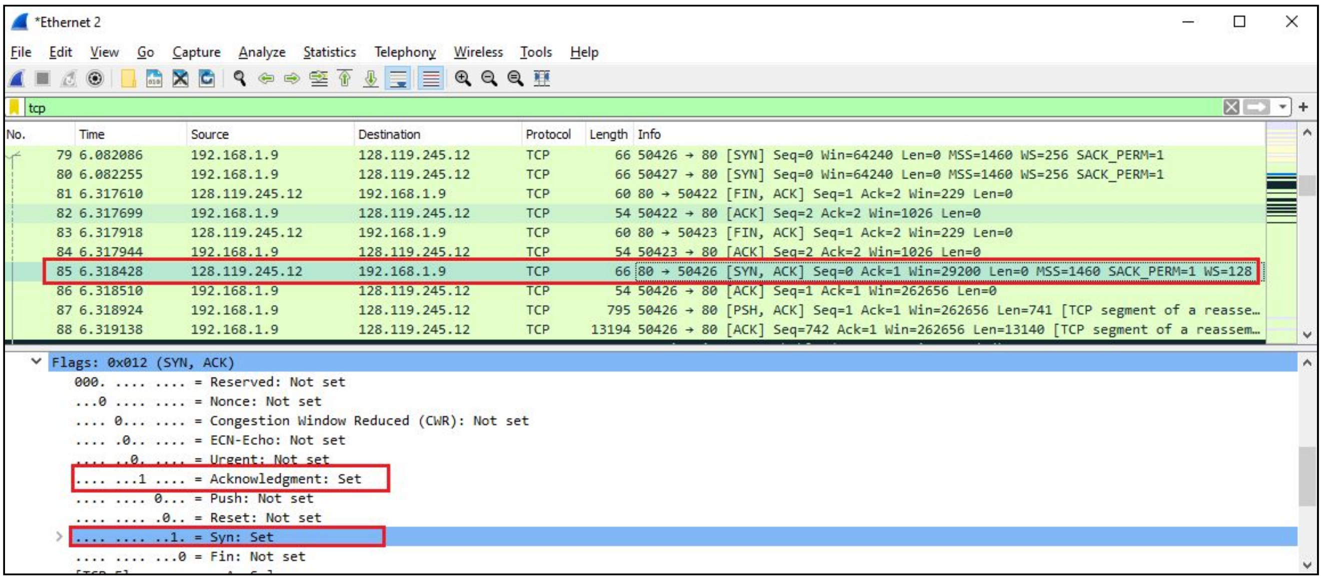


```
*Ethernet 2
tcp
No.     Time        Source          Destination     Protocol  Length Info
   76 5.738344      192.168.1.9     192.168.1.200   TCP       54 49688 → 445 [ACK] Seq=1715 Ack=1273 Win=8207 Len=0
   77 6.081737      192.168.1.9     128.119.245.12  TCP       54 50422 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1026 Len=0
   78 6.081800      192.168.1.9     128.119.245.12  TCP       54 50423 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1026 Len=0
   79 6.082086      192.168.1.9     128.119.245.12  TCP       66 50426 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   80 6.082255      192.168.1.9     128.119.245.12  TCP       66 50427 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   81 6.317610      128.119.245.12  192.168.1.9     TCP       60 80 → 50422 [FIN, ACK] Seq=1 Ack=2 Win=229 Len=0
   82 6.317699      192.168.1.9     128.119.245.12  TCP       54 50422 → 80 [ACK] Seq=2 Ack=2 Win=1026 Len=0
   83 6.317918      128.119.245.12  192.168.1.9     TCP       60 80 → 50423 [FIN, ACK] Seq=1 Ack=2 Win=229 Len=0
   84 6.317944      192.168.1.9     128.119.245.12  TCP       54 50423 → 80 [ACK] Seq=2 Ack=2 Win=1026 Len=0
   85 6.318428      128.119.245.12  192.168.1.9     TCP       66 80 → 50426 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM…

  v 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
      .... .... ...0 = Fin: Not set
```

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?**
    - The sequence number of the SYNACK segment is: 0
    - Value of the Acknowledgement field in the SYNACK segment is: 1. The value of the ACKnowledgement field in the SYNACK segment is determined by

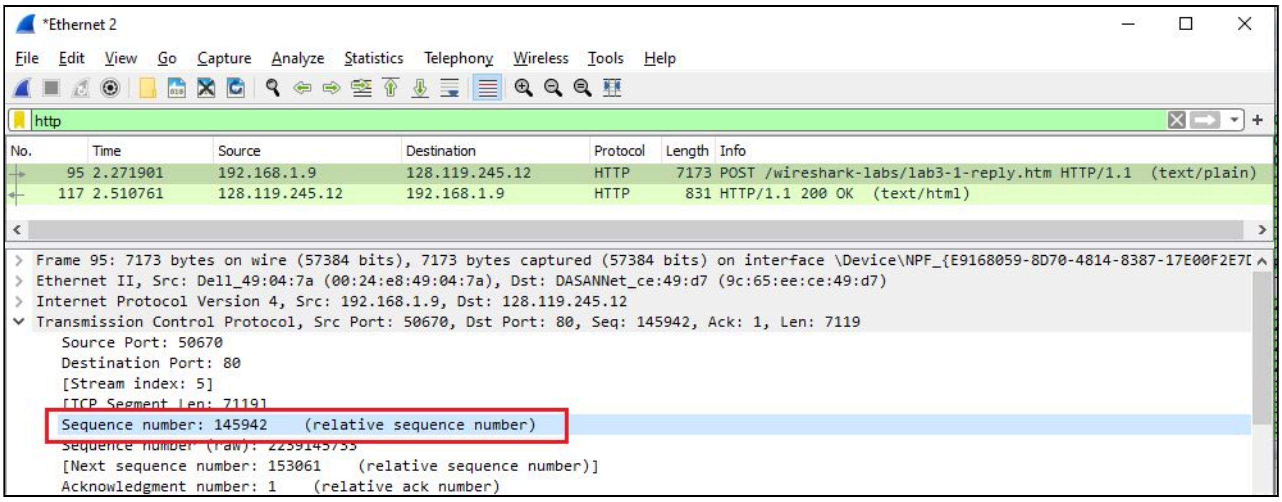
gaia.cs.umass.edu by adding 1 to the initial sequence number of SYN segment from the client computer.

- The SYN flag and Acknowledgement flag in the segment are set to 1 and they indicate that this segment is a SYNACK segment.


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.  Time       Source          Destination     Protocol  Length Info
  79 6.082086   192.168.1.9     128.119.245.12  TCP          66 50426 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  80 6.082255   192.168.1.9     128.119.245.12  TCP          66 50427 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  81 6.317610   128.119.245.12  192.168.1.9     TCP          60 80 → 50422 [FIN, ACK] Seq=1 Ack=2 Win=229 Len=0
  82 6.317699   192.168.1.9     128.119.245.12  TCP          54 50422 → 80 [ACK] Seq=2 Ack=2 Win=1026 Len=0
  83 6.317918   128.119.245.12  192.168.1.9     TCP          60 80 → 50423 [FIN, ACK] Seq=1 Ack=2 Win=229 Len=0
  84 6.317944   192.168.1.9     128.119.245.12  TCP          54 50423 → 80 [ACK] Seq=2 Ack=2 Win=1026 Len=0
  85 6.318428   128.119.245.12  192.168.1.9     TCP          66 80 → 50426 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  86 6.318510   192.168.1.9     128.119.245.12  TCP          54 50426 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
  87 6.318924   192.168.1.9     128.119.245.12  TCP         795 50426 → 80 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=741 [TCP segment of a reasse…
  88 6.319138   192.168.1.9     128.119.245.12  TCP       13194 50426 → 80 [ACK] Seq=742 Ack=1 Win=262656 Len=13140 [TCP segment of a reassem…

  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
```

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.**
    - The sequence number of the TCP segment containing the HTTP POST command: 145942


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time       Source          Destination     Protocol  Length Info
   95 2.271901   192.168.1.9     128.119.245.12  HTTP        7173 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
  117 2.510761   128.119.245.12  192.168.1.9     HTTP         831 HTTP/1.1 200 OK  (text/html)

> Frame 95: 7173 bytes on wire (57384 bits), 7173 bytes captured (57384 bits) on interface \Device\NPF_{E9168059-8D70-4814-8387-17E00F2E7D
> Ethernet II, Src: Dell_49:04:7a (00:24:e8:49:04:7a), Dst: DASANNet_ce:49:d7 (9c:65:ee:ce:49:d7)
> Internet Protocol Version 4, Src: 192.168.1.9, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 50670, Dst Port: 80, Seq: 145942, Ack: 1, Len: 7119
    Source Port: 50670
    Destination Port: 80
    [Stream index: 5]
    [TCP Segment Len: 7119]
    Sequence number: 145942    (relative sequence number)
    Sequence number (raw): 2239145733
    [Next sequence number: 153061    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
```

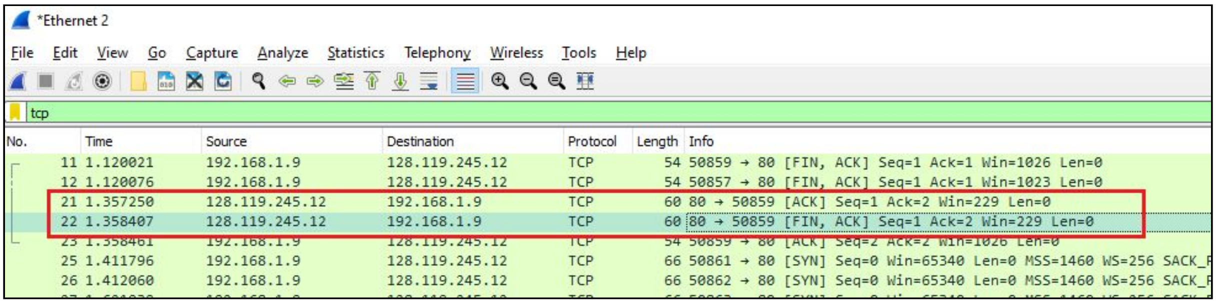
7. **Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments? What is the EstimatedRTT value (see Section 3.5.3, page 242 in**

text) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 242 for all subsequent segments.

- The sequence numbers of the first six segments in the TCP connection: 30,31,

8. **What is the length of each of the first six TCP segments?**
   - Length of first TCP segments: 741
   - Length of second TCP segments: 13068
   - Length of third TCP segments: 1452
   - Length of fourth TCP segments: 2904
   - Length of fifth TCP segments: 11616
   - Length of sixth TCP segments: 8712

9. **What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?**
   - The minimum amount of available buffer space advertised at the receiver for the entire trace: 229
   - The sender is never throttled because we never reach full capacity of the window.



tcp

No.	Time	Source	Destination	Protocol	Length	Info
11	1.120021	192.168.1.9	128.119.245.12	TCP	54	50859 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1026 Len=0
12	1.120076	192.168.1.9	128.119.245.12	TCP	54	50857 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
21	1.357250	128.119.245.12	192.168.1.9	TCP	60	80 → 50859 [ACK] Seq=1 Ack=2 Win=229 Len=0
22	1.358407	128.119.245.12	192.168.1.9	TCP	60	80 → 50859 [FIN, ACK] Seq=1 Ack=2 Win=229 Len=0
23	1.358461	192.168.1.9	128.119.245.12	TCP	54	50859 → 80 [ACK] Seq=2 Ack=2 Win=1026 Len=0
25	1.411796	192.168.1.9	128.119.245.12	TCP	66	50861 → 80 [SYN] Seq=0 Win=65340 Len=0 MSS=1460 WS=256 SACK_P
26	1.412060	192.168.1.9	128.119.245.12	TCP	66	50862 → 80 [SYN] Seq=0 Win=65340 Len=0 MSS=1460 WS=256 SACK_P

10. **Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?**
    - No segments were ever retransmitted. This is shown by the fact that an old Acknowledgement number was never present in order to re-request former packets.

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 (see Table 3.2 on page 250 in the text).**
    - The receiver is typically acking 432 bits. There are cases where the receiver acks every other segment. This is shown when more than one ack occurs in a row.

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