

ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH TRƯỜNG ĐẠI
HỌC BÁCH KHOA KHOA
KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH



BÁO CÁO MẠNG MÁY TÍNH THỰC HÀNH (CO3094)

LAB 3B

GV hướng dẫn: Lê Bảo Khánh

SV thực hiện: Phùng Xương Cận 2210348

Thành phố Hồ Chí Minh, Tháng 10 năm 2024

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).

436	18.967652	192.168.2.9	128.119.245.12	HTTP	1367	POST /wireshark-labs/lab3-1-rej
<div>> Frame 436: 1367 bytes on wire (10936 bits), 1367 bytes captured (10936 bits) on interface \Device\NPF_{08EAA87...}</div> <div>> Ethernet II, Src: AzureWaveTec_5c:9f:75 (2c:3b:70:5c:9f:75), Dst: zte_9f:2c:43 (d0:59:19:9f:2c:43)</div> <div>> Internet Protocol Version 4, Src: 192.168.2.9, Dst: 128.119.245.12</div> <div>> Transmission Control Protocol, Src Port: 63183, Dst Port: 80, Seq: 151663, Ack: 1, Len: 1313</div> <div>Source Port: 63183</div> <div>Destination Port: 80</div>						

According to above figure, the client computer (source)'s IP address is 192.168.2.9.

Source Port: 63183

Destination Port: 80

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?

452	19.249508	128.119.245.12	192.168.2.9	HTTP	831	HTTP/1.1 200 OK (text/html)
453	19.301238	192.168.2.9	128.119.245.12	TCP	54	63183 → 80 [ACK] Seq=152976 Ack=
<div>Frame 452: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface \Device\NPF_{08EAA87...}</div> <div>Ethernet II, Src: zte_9f:2c:43 (d0:59:19:9f:2c:43), Dst: AzureWaveTec_5c:9f:75 (2c:3b:70:5c:9f:75)</div> <div>Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.9</div> <div>Transmission Control Protocol, Src Port: 80, Dst Port: 63183, Seq: 1, Ack: 152976, Len: 777</div> <div>Source Port: 80</div> <div>Destination Port: 63183</div>						

According to above figure, the IP address of gaia.cs.umass.edu is 128.119.245.12 and the TCP port number is 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?

my client computer's IP address is 192.168.2.9 and the TCP port is 63183.

3. TCP Basics

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?

9	0.703705	192.168.2.9	192.168.2.9	TCP	66 443 → 63143 [ACK] Seq=1 ACK=2 W
12	9.015734	192.168.2.9	40.79.173.40	TCP	66 63180 → 443 [SYN] Seq=0 Win=655
13	9.019853	192.168.2.9	51.116.246.106	TCP	66 63181 → 443 [SYN] Seq=0 Win=655
14	9.025007	192.168.2.9	192.168.2.9	TCP	66 443 → 63180 [SYN] Seq=1 Win=655


```

> Frame 12: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{08EAAA87-8CB1
> Ethernet II, Src: AzureWaveTec_5c:9f:75 (2c:3b:70:5c:9f:75), Dst: zte_9f:2c:43 (d0:59:19:9f:2c:43)
> Internet Protocol Version 4, Src: 192.168.2.9, Dst: 40.79.173.40
v Transmission Control Protocol, Src Port: 63180, Dst Port: 443, Seq: 0, Len: 0
  Source Port: 63180
  Destination Port: 443
  [Stream index: 3]
  [Stream Packet Number: 1]
  > [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 3495881353
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)

```

The sequence number of the segment used to initiate the TCP connection is 0. We can see that the message contains a SYN flag indicating that it is a SYN segment.

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?

```

Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3495881353
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
v Flags: 0x002 (SYN)
  000. .... = Reserved: Not set
  ...0 .... = Accurate ECN: Not set
  .... 0... = Congestion Window Reduced: 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

```

According to the above figure, the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0.

The value of the acknowledgement field in the SYNACK segment is 1. The value of the ACKnowledgement field in the SYNACK segment is determined by the server gaia.cs.umass.edu. The server adds 1 to the initial sequence number of SYN segment from the client computer. For this case, the initial sequence number of SYN segment from the client computer is 0, thus the value of the ACKnowledgement field in the SYNACK segment is 1.

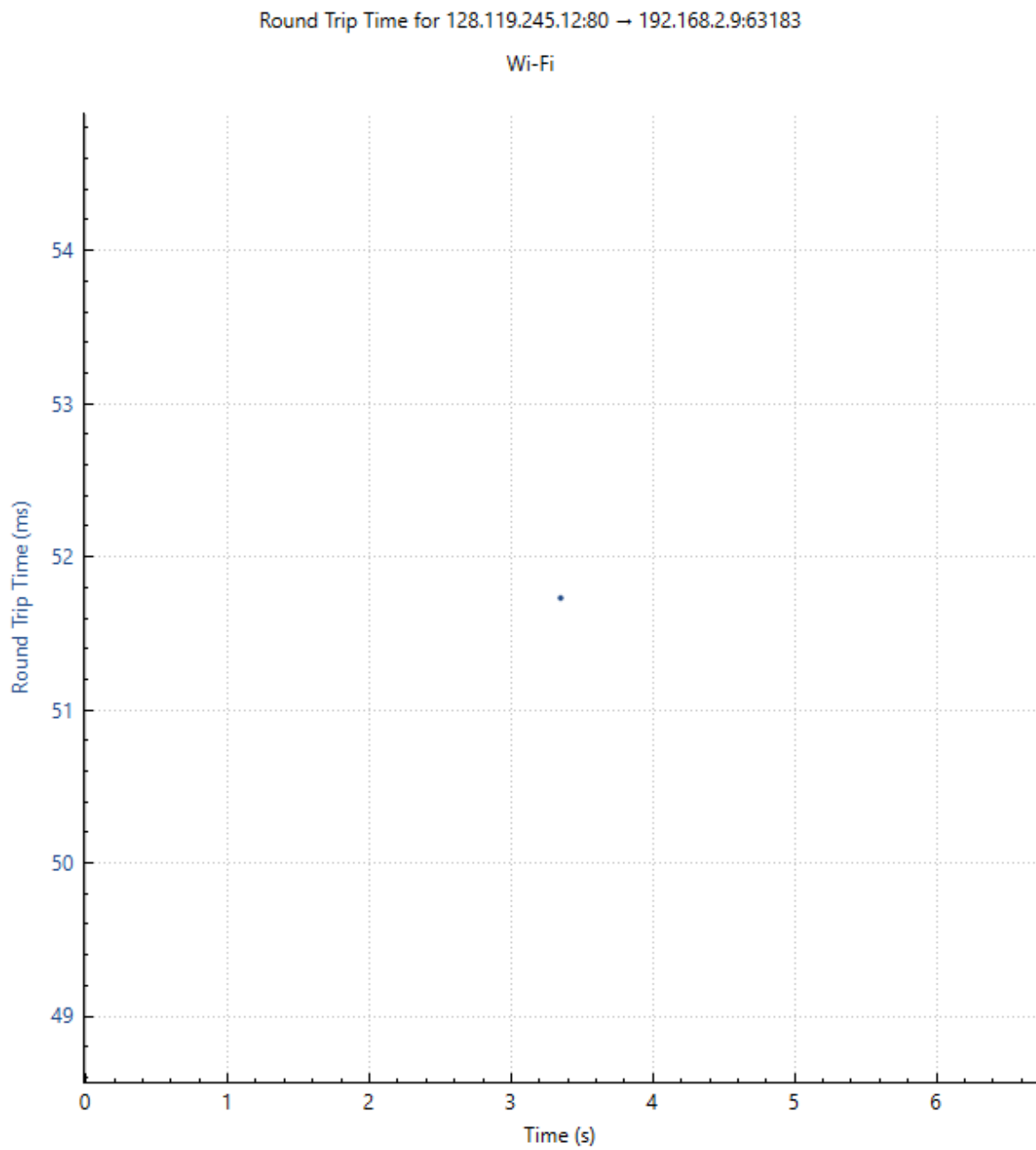
A segment will be identified as a SYNACK segment if both SYN flag and Acknowledgement in the segment are set to 1.

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

```
Sequence Number: 147307 (relative sequence number)
Sequence Number (raw): 2849854882
[Next Sequence Number: 148759 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 233706849
0101 .... = Header Length: 20 bytes (5)
v Flags: 0x018 (PSH, ACK)
```

The sequence number of the TCP segment containing the HTTP Post Command is 147307

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 239 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 239 for all subsequent segments.



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

284	18.138287	192.168.2.9	128.119.245.12	TCP	708	63183 → 80 [PSH, ACK] Seq=1 Ack=1 Win=132096 Len=654
285	18.138493	192.168.2.9	128.119.245.12	TCP	1506	63183 → 80 [ACK] Seq=655 Ack=1 Win=132096 Len=1500
286	18.138493	192.168.2.9	128.119.245.12	TCP	1506	63183 → 80 [ACK] Seq=2107 Ack=1 Win=132096 Len=1500
287	18.138493	192.168.2.9	128.119.245.12	TCP	1506	63183 → 80 [ACK] Seq=3559 Ack=1 Win=132096 Len=1500
288	18.138493	192.168.2.9	128.119.245.12	TCP	1506	63183 → 80 [ACK] Seq=5011 Ack=1 Win=132096 Len=1500
289	18.138493	192.168.2.9	128.119.245.12	TCP	1506	63183 → 80 [ACK] Seq=6463 Ack=1 Win=132096 Len=1500
290	18.138493	192.168.2.9	128.119.245.12	TCP	1506	63183 → 80 [ACK] Seq=7915 Ack=1 Win=132096 Len=1500
291	18.138493	192.168.2.9	128.119.245.12	TCP	1506	63183 → 80 [ACK] Seq=9367 Ack=1 Win=132096 Len=1500
292	18.138493	192.168.2.9	128.119.245.12	TCP	1506	63183 → 80 [ACK] Seq=10819 Ack=1 Win=132096 Len=1500
293	18.138493	192.168.2.9	128.119.245.12	TCP	1506	63183 → 80 [ACK] Seq=12271 Ack=1 Win=132096 Len=1500
296	18.141211	192.168.2.9	13.126.70.76	TCP	1506	63153 → 443 [ACK] Seq=1 Ack=2 Win=514 Len=1452
297	18.141211	192.168.2.9	13.126.70.76	TLSv1.2	119	Application Data
315	18.135860	13.126.70.76	192.168.2.9	TCP	54	TCP, previous segment not captured, 443 → 63153


```

> Frame 284: 708 bytes on wire (5664 bits), 708 bytes captured (5664 bits) on interface \Device\NPF{...}
> Ethernet II, Src: AzureWaveTec_5c:9f:75 (2c:3b:70:5c:9f:75), Dst: zte_9f:2c:43 (d0:59:19:9f:2c:43)
> Internet Protocol Version 4, Src: 192.168.2.9, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 63183, Dst Port: 80, Seq: 1, Ack: 1, Len: 654
  Data (654 bytes)
    Data [...]: 504f5354202f77697265736861726b2d6c6162732f6c6162332d312d7265706c792e68746d2048545354
    [Length: 654]
  
```

The length of the first TCP segment is 654 bytes, the length of the second TCP segment is 1452 bytes. The length of each of the following five TCP segments is 1506 bytes.

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?

```

> .... ..1. = Syn: Set
> .... ..0 = Fin: Not set
  [TCP Flags: .....A..S.]
  Window: 29200
  [Calculated window size: 29200]
  
```

The minimum amount of available buffer space advertised at the received for the entire trace is indicated first ACK from the server, its value is 29200 bytes (shown in above figure).

The sender is never throttled because we never reach full capacity of the window.

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, no segments were ever retransmitted. This is shown by the fact that an old Acknowledgement number was never resent 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 247 in the text).

From the screenshot , we see that the ACK numbers increase in the sequence 32599, 15175, 18079, Note that the ACK numbers increase by 2904 each time, indicating that

4	192.168.2.9	128.119.245.12	TCP	1506 63183 → 80 [PSH, ACK] Seq=32599 Ack=1 Win=132096 Len=1452
4	192.168.2.9	128.119.245.12	TCP	1506 63183 → 80 [ACK] Seq=34051 Ack=1 Win=132096 Len=1452
4	192.168.2.9	128.119.245.12	TCP	1506 63183 → 80 [ACK] Seq=35503 Ack=1 Win=132096 Len=1452
4	192.168.2.9	128.119.245.12	TCP	1506 63183 → 80 [ACK] Seq=36955 Ack=1 Win=132096 Len=1452
4	192.168.2.9	128.119.245.12	TCP	1506 63183 → 80 [ACK] Seq=38407 Ack=1 Win=132096 Len=1452
4	192.168.2.9	142.250.197.206	TCP	55 63151 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1
5	142.250.197.206	192.168.2.9	TCP	66 443 → 63151 [ACK] Seq=1 Ack=2 Win=1046 Len=0 SLE=1 SRE=2
5	128.119.245.12	192.168.2.9	TCP	54 80 → 63183 [ACK] Seq=1 Ack=15175 Win=59648 Len=0
8	192.168.2.9	128.119.245.12	TCP	1506 63183 → 80 [ACK] Seq=39859 Ack=1 Win=132096 Len=1452
8	192.168.2.9	128.119.245.12	TCP	1506 63183 → 80 [ACK] Seq=41311 Ack=1 Win=132096 Len=1452
1	128.119.245.12	192.168.2.9	TCP	54 80 → 63183 [ACK] Seq=1 Ack=18079 Win=65408 Len=0
1	128.119.245.12	192.168.2.9	TCP	54 80 → 63183 [ACK] Seq=1 Ack=22435 Win=74112 Len=0

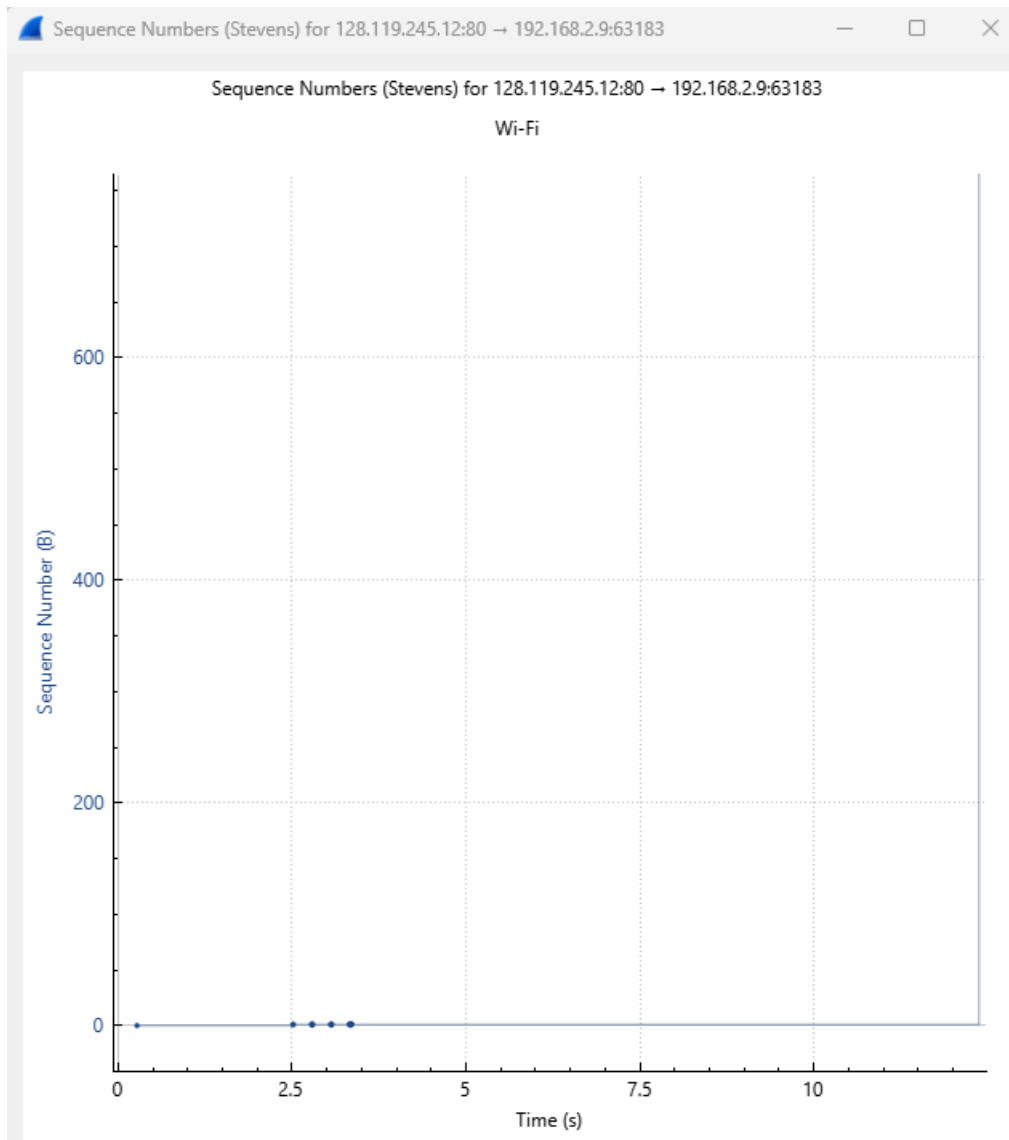
the receiver is acknowledging 2904 bytes.

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

The alice.txt on the hard drive is 152,138 bytes, and the download time is 1.578736000 (First TCP segment) - 0.271257000 (last ACK) = 1.307479 second. Therefore, the throughput for the TCP connection is computed as 152,138/1.307479=116359.803867 bytes/second.

4. TCP congestion control in action

13. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.



14. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu

The questions had been answered