UFU 45 ANOS

Prática 5 - Wireshark LAB – TCP

Redes de Comunicações I

Leonardo Vecchi Meirelles

12011ECP002

Outubro 2023

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.**

   O endereço de IP é 192.168.15.157, e a porta de origem é 54423.

```
> Internet Protocol Version 4, Src: 192.168.15.157, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54423, Dst Port: 80, Seq: 634, Ack: 1, Len: 13068
```

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?**

   O endereço de IP do gaia.cs.umass.edu é 128.119.245.12, e a porta é 80.

```
> Internet Protocol Version 4, Src: 192.168.15.157, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54423, Dst Port: 80, Seq: 634, Ack: 1, Len: 13068
```

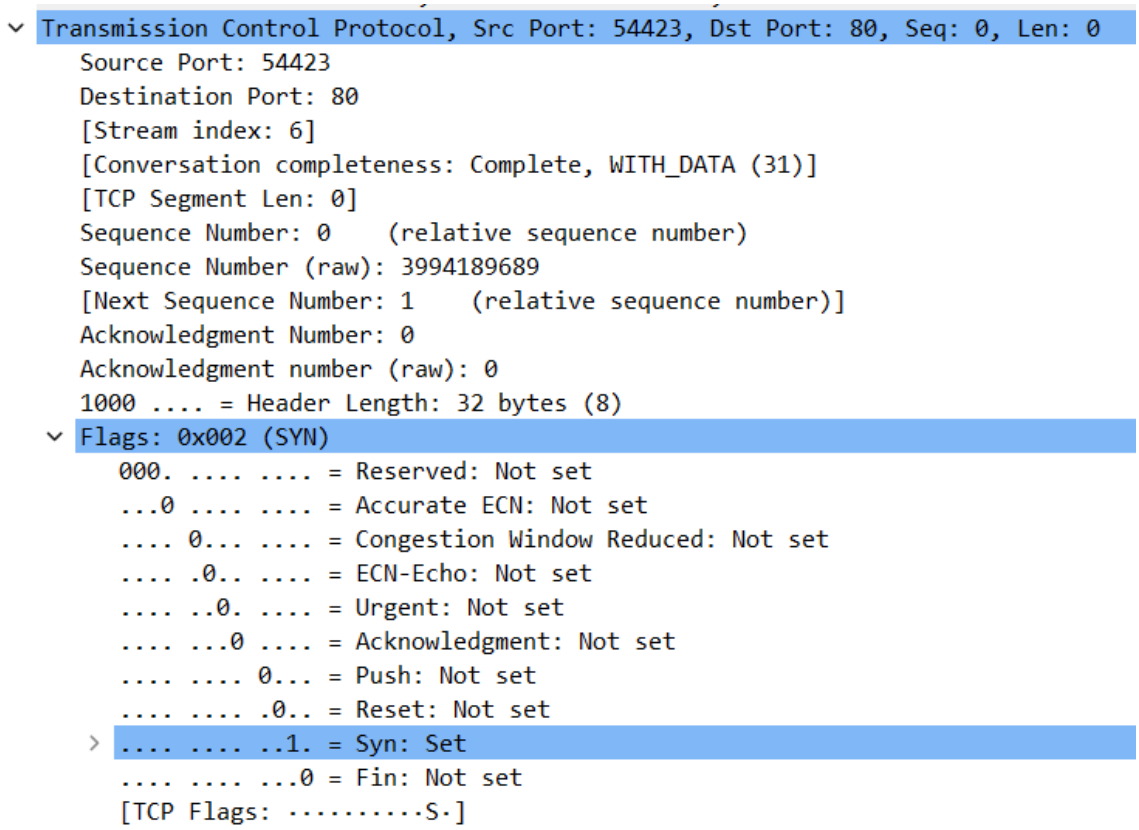
3. **What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?**

   O endereço de IP é 192.168.15.157, e a porta de origem é 54423.

```
> Internet Protocol Version 4, Src: 192.168.15.157, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54423, Dst Port: 80, Seq: 634, Ack: 1, Len: 13068
```

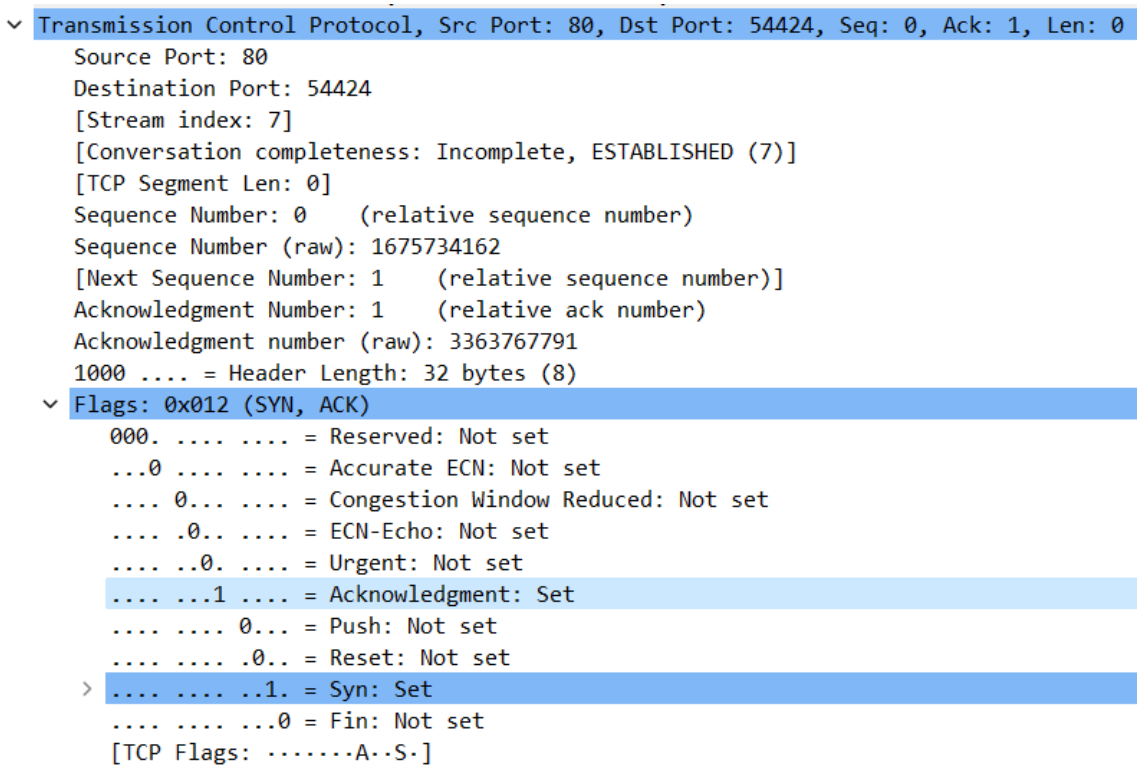
4. **What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?**

   O número de sequência do TCP SYN é 0. O segmento que identifica o segmento como um SYN está nas flags, e mostra que o SYN definido em 1.



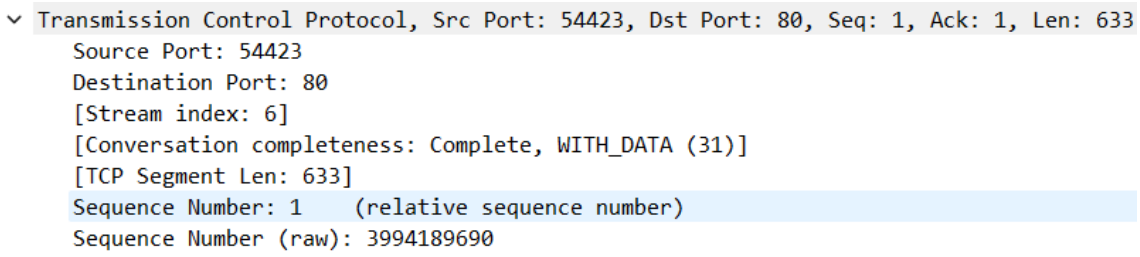
5. **What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the cliente computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as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

O número de sequência do TCP SYNACK é 0. O segmento que identifica o segmento como um SYNACK está nas flags e mostra que o SYN e o ACK estão definidos em 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.**

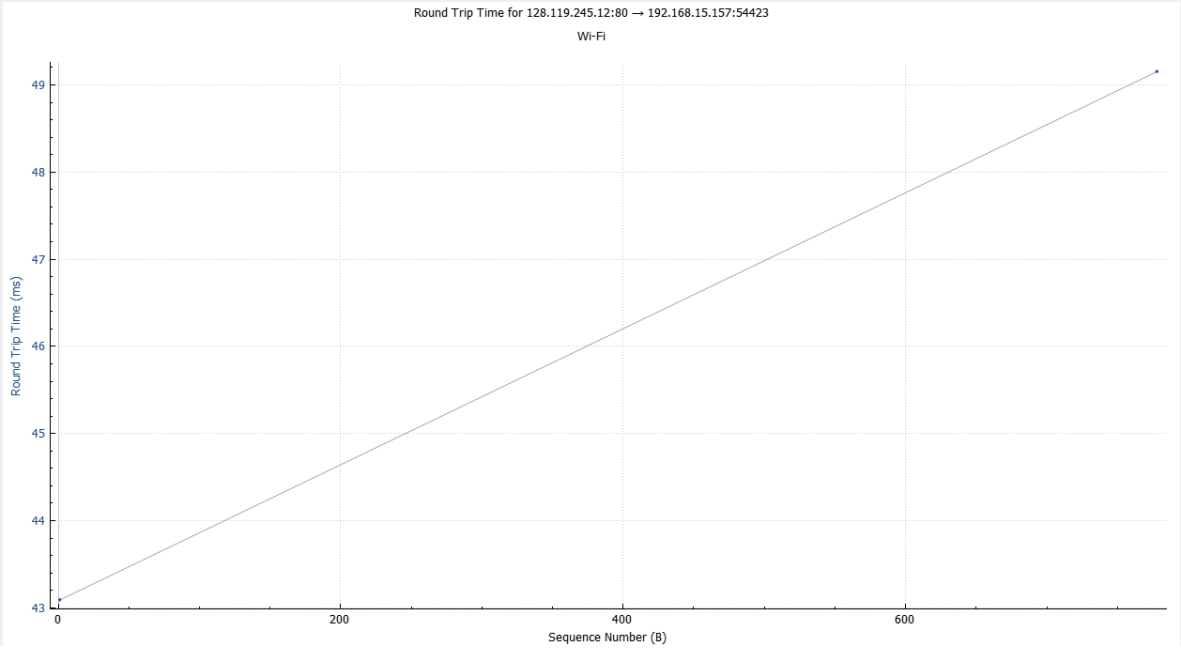
O número de sequência do seguimento TCP que contém o HTTP POST é 1.



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. Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph->Round Trip Time Graph.

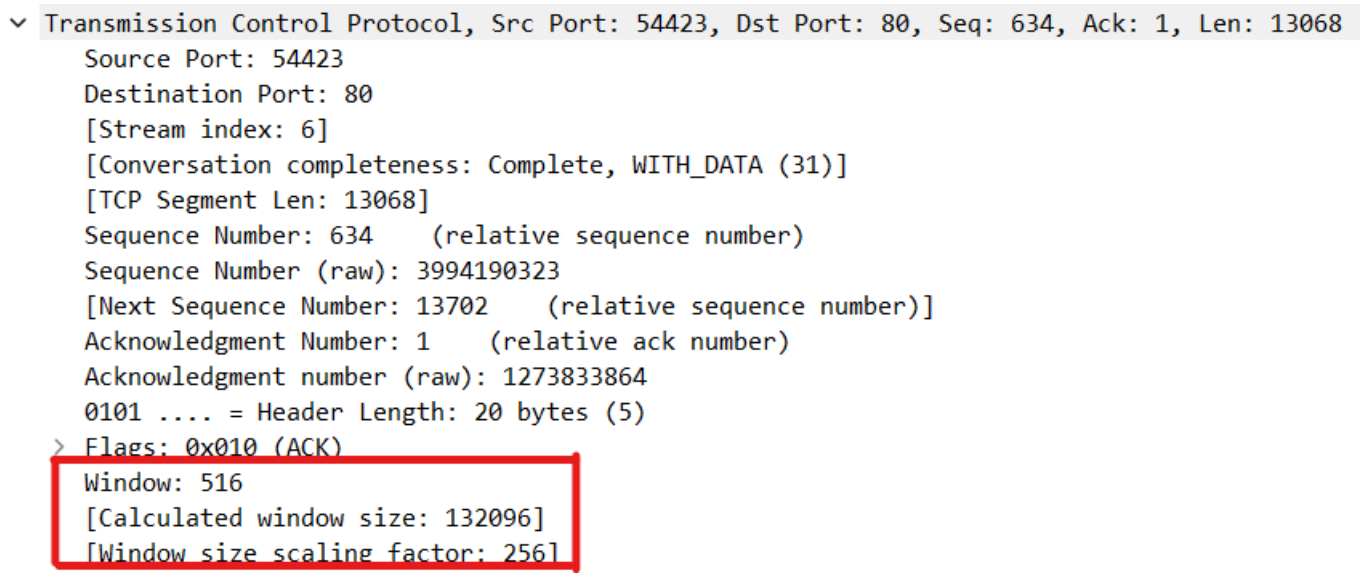
64	13:41:06,608873	192.168.15.157	128.119.245.12	TCP	687	54423 → 80 [PSH, ACK] Seq=1 Ack=1 Win=132096 Len=633
65	13:41:06,609055	192.168.15.157	128.119.245.12	TCP	131…	54423 → 80 [ACK] Seq=634 Ack=1 Win=132096 Len=13068
84	13:41:06,778921	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=634 Win=30592 Len=0
85	13:41:06,778921	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=2086 Win=33408 Len=0
86	13:41:06,778921	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=3538 Win=36352 Len=0
87	13:41:06,778921	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=6442 Win=42240 Len=0
88	13:41:06,778967	192.168.15.157	128.119.245.12	TCP	131…	54423 → 80 [PSH, ACK] Seq=13702 Ack=1 Win=132096 Len=13068
89	13:41:06,782899	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=10798 Win=50944 Len=0
90	13:41:06,782929	192.168.15.157	128.119.245.12	TCP	8766	54423 → 80 [PSH, ACK] Seq=26770 Ack=1 Win=132096 Len=8712
91	13:41:06,786568	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=13702 Win=56704 Len=0
92	13:41:06,786595	192.168.15.157	128.119.245.12	TCP	5862	54423 → 80 [ACK] Seq=35482 Ack=1 Win=132096 Len=5808
98	13:41:06,942833	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=16606 Win=62464 Len=0
99	13:41:06,942873	192.168.15.157	128.119.245.12	TCP	5862	54423 → 80 [ACK] Seq=41290 Ack=1 Win=132096 Len=5808
101	13:41:06,946910	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=19510 Win=68352 Len=0
102	13:41:06,946910	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=20962 Win=71296 Len=0
103	13:41:06,946962	192.168.15.157	128.119.245.12	TCP	8766	54423 → 80 [PSH, ACK] Seq=47098 Ack=1 Win=132096 Len=8712
104	13:41:06,950586	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=23866 Win=77056 Len=0



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

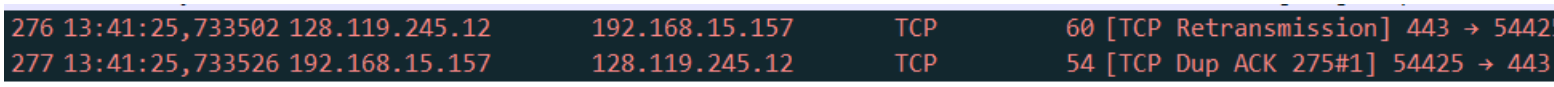
64	13:41:06,608873	192.168.15.157	128.119.245.12	TCP	687	54423 → 80 [PSH, ACK] Seq=1 Ack=1 Win=132096 Len=
65	13:41:06,609055	192.168.15.157	128.119.245.12	TCP	13122	54423 → 80 [ACK] Seq=634 Ack=1 Win=132096 Len=130
84	13:41:06,778921	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=634 Win=30592 Len=0
85	13:41:06,778921	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=2086 Win=33408 Len=0
86	13:41:06,778921	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=3538 Win=36352 Len=0
87	13:41:06,778921	128.119.245.12	192.168.15.157	TCP	60	80 → 54423 [ACK] Seq=1 Ack=6442 Win=42240 Len=0

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?**



A falta de espaço no buffer do receptor não limitou o remetente.

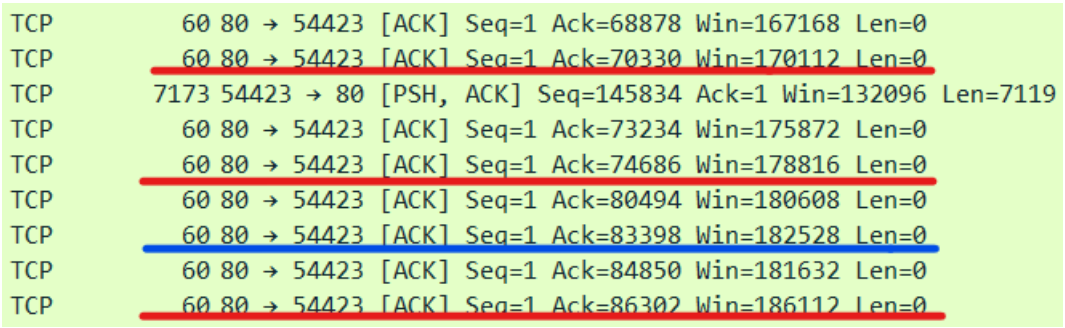
10. **Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?**



Ao final do trace file ocorreu uma retransmissão como apresentado na figura acima.

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).**

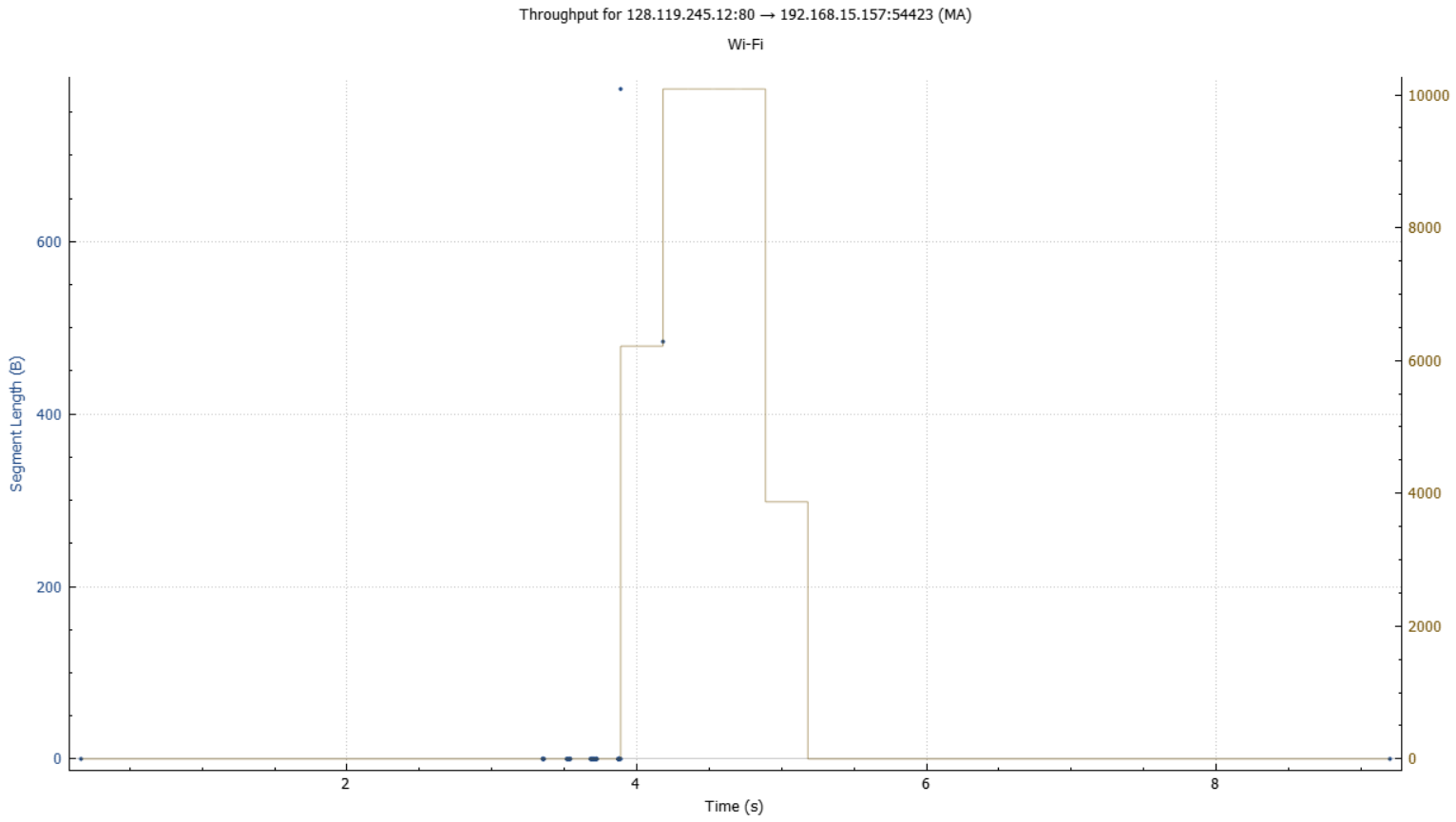
No protocolo TCP, os ACKs são cumulativos, ou seja, a quantidade de dados a ser reconhecida pode variar.



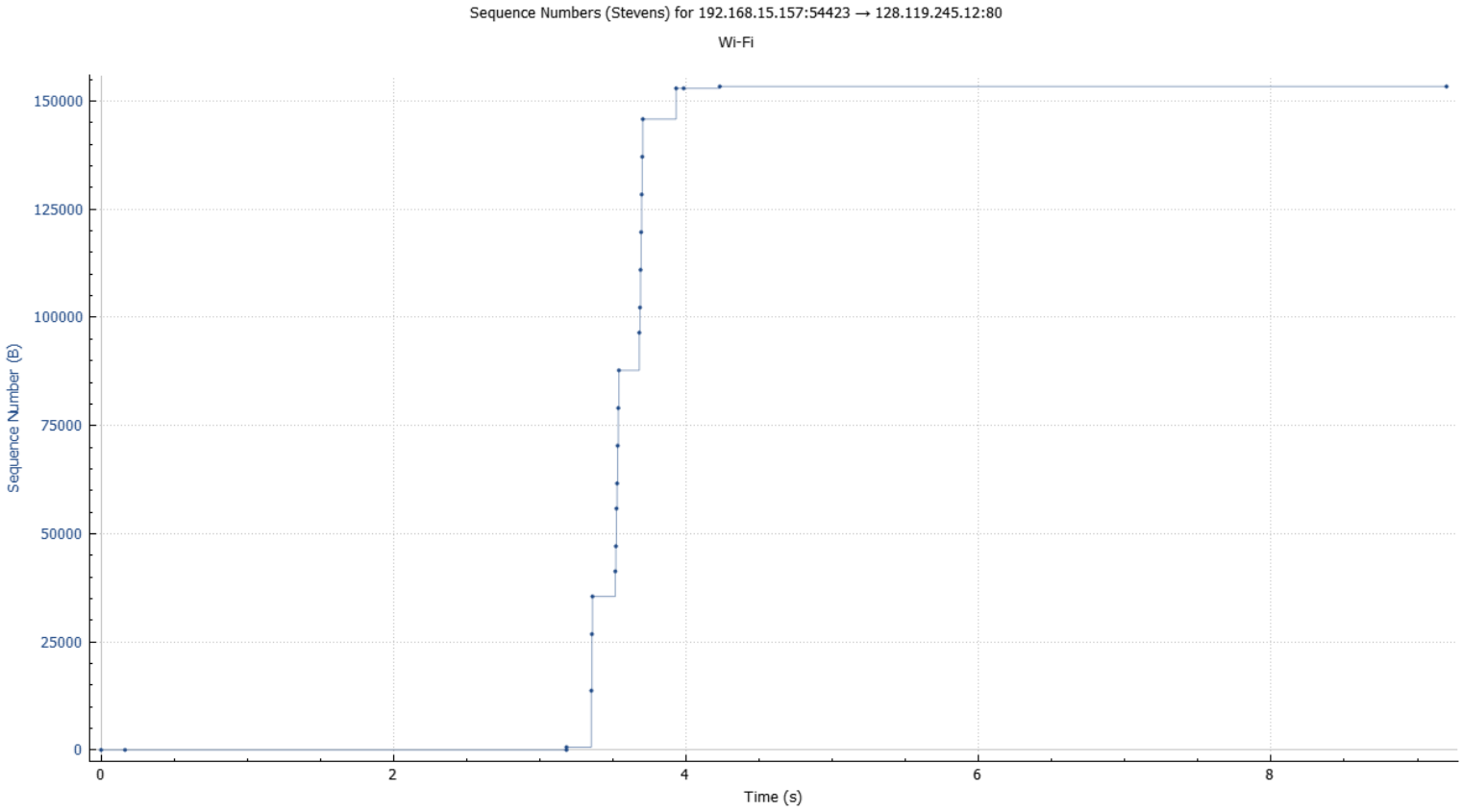
Na imagem apresentada do trace realizado, pode-se verificar que os ACKs em vermelho estão em sequência (1452 bytes de diferença). Mas entre os ACKs representados em azul, pulou-se um “ciclo” (2904 bytes de diferença).

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

A taxa de transferência de uma conexão TCP pode ser calculada dividindo o número total de bytes transferidos pelo tempo necessário para transferi-los. Para calcular a taxa de transferência, você primeiro registraria o horário de início e o horário de término da conexão TCP e, em seguida, subtrairia o horário de início do horário de término para encontrar o tempo total gasto. Em seguida, você determinaria o número total de bytes transferidos durante esse período, que pode ser obtido em ferramentas de monitoramento de rede ou em estatísticas em nível de aplicativo. Finalmente, dividir o total de bytes pelo tempo gasto resulta na taxa de transferência em bytes por unidade de tempo, normalmente medida em bytes por segundo (Bps) ou quilobytes por segundo (KBps).



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.**



A fase de partida lenta do TCP pode ser observada no intervalo aproximado de [3.25, 4.25] segundos.

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**

Todas as medições anteriores foram fazendo uso do trace obtido ao transferir o arquivo do meu computador ao endereço gaia.cs.umass.edu.