src.html

Wireshark Lab: DNS

Nome:

Vinícius Gonzaga Rocha

Matrícula:

11511BCC019

Descrição:

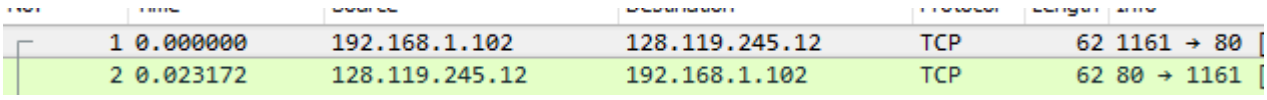
Atividade realizada para o aprofundamento do conhecimento do protocolo TCP.

---

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.

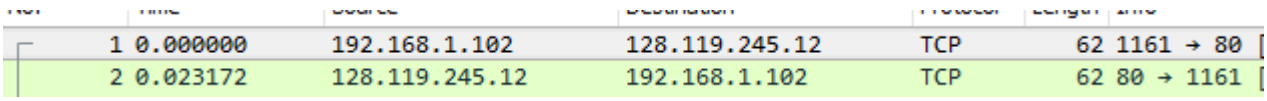
192.168.1.102 porta 1161



1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 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?

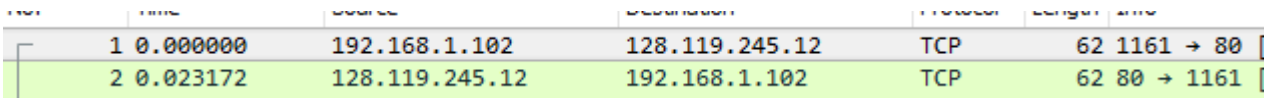
128.119.245.12 porta 80



1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161

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?

192.168.1.102 porta 1161



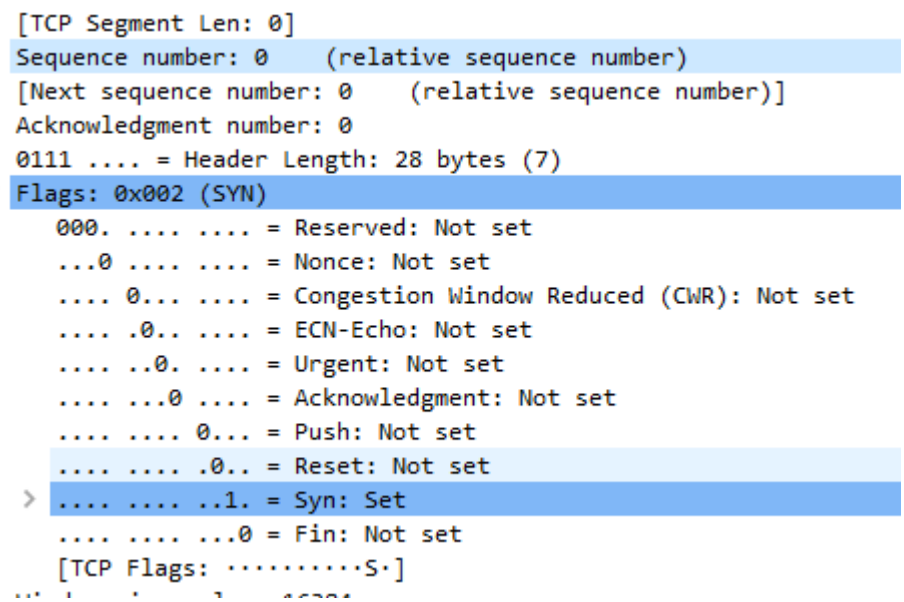
1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161

---

3. TCP Basics

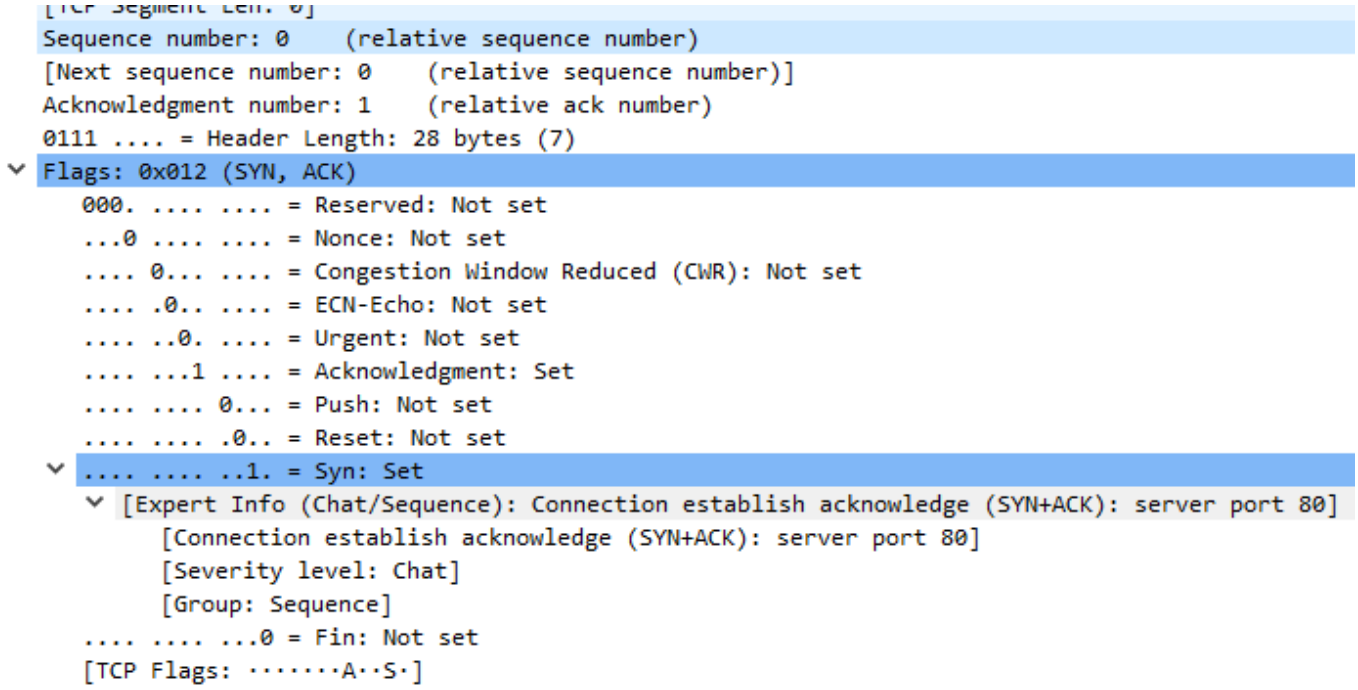
4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

É o número 0; A flag setada em SYN.



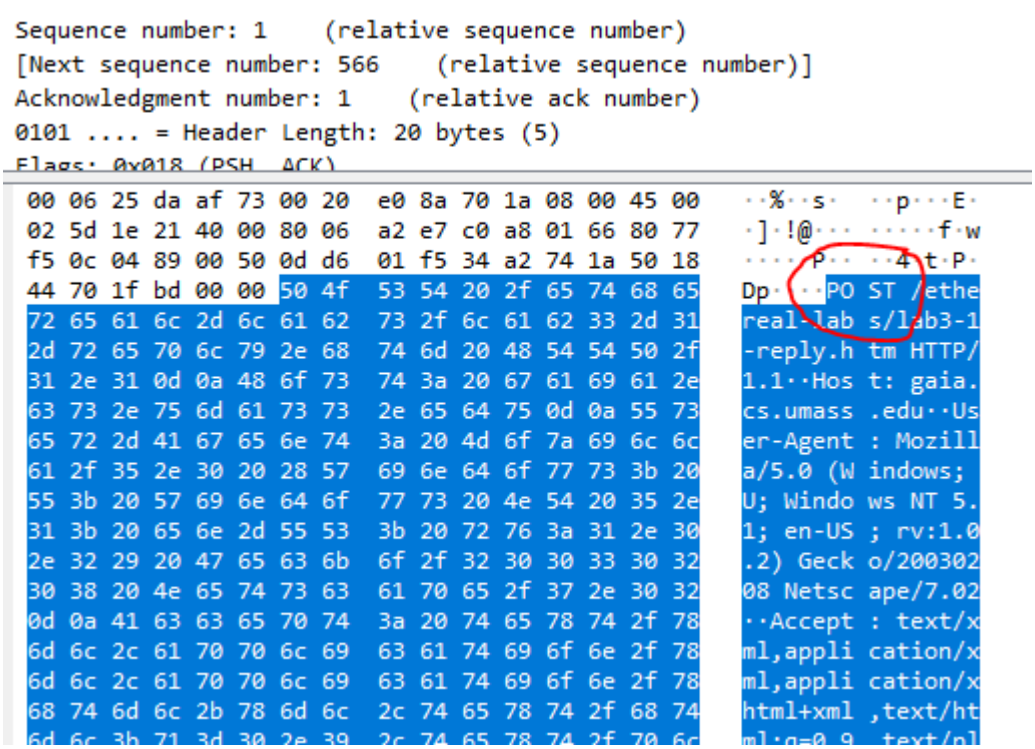
5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK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

É o número 0; O valor do ack é 1; Através do número de sequência; As flags de SYNACK.



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.

É o número 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.

#	Seq. Number	Time	Time ACK	RTT	EstimatedRTT
1	1	0.026477	0.053937	0.027460	0.027460
2	566	0.041737	0.077294	0.035557	0.001151
3	2026	0.050260	0.124085	0.073825	0.001173
4	3486	0.054690	0.169118	0.114428	0.001214
5	4946	0.077405	0.217299	0.139894	0.001251
6	6406	0.078157	0.267802	0.189645	0.001285

```
 4 0.026477    192.168.1.102    128.119.245.12   TCP     619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
 5 0.041737    192.168.1.102    128.119.245.12   TCP    1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1
 6 0.053937    128.119.245.12   192.168.1.102    TCP      60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
 7 0.054026    192.168.1.102    128.119.245.12   TCP    1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
 8 0.054690    192.168.1.102    128.119.245.12   TCP    1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
 9 0.077294    128.119.245.12   192.168.1.102    TCP      60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10 0.077405    192.168.1.102    128.119.245.12   TCP    1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460
11 0.078157    192.168.1.102    128.119.245.12   TCP    1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460
12 0.124085    128.119.245.12   192.168.1.102    TCP      60 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13 0.124185    192.168.1.102    128.119.245.12   TCP    1201 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=
14 0.169118    128.119.245.12   192.168.1.102    TCP      60 80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
15 0.217299    128.119.245.12   192.168.1.102    TCP      60 80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
16 0.267802    128.119.245.12   192.168.1.102    TCP      60 80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
17 0.304807    128.119.245.12   192.168.1.102    TCP      60 80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
18 0.305040    192.168.1.102    128.119.245.12   TCP    1514 1161 → 80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460
```

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

#	Length
1	565
2	1460
3	1460
4	1460
5	1460
6	1460

```
 4 0.026477    192.168.1.102    128.119.245.12   TCP     619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of a reassem
 5 0.041737    192.168.1.102    128.119.245.12   TCP    1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460 [TCP segment of a reas
 6 0.053937    128.119.245.12   192.168.1.102    TCP      60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
 7 0.054026    192.168.1.102    128.119.245.12   TCP    1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460 [TCP segment of a reassemb
 8 0.054690    192.168.1.102    128.119.245.12   TCP    1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP segment of a reassemb
 9 0.077294    128.119.245.12   192.168.1.102    TCP      60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
10 0.077405    192.168.1.102    128.119.245.12   TCP    1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460 [TCP segment of a reassemb
11 0.078157    192.168.1.102    128.119.245.12   TCP    1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP segment of a reassemb
12 0.124085    128.119.245.12   192.168.1.102    TCP      60 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
13 0.124185    192.168.1.102    128.119.245.12   TCP    1201 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147 [TCP segment of a rea
```

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?

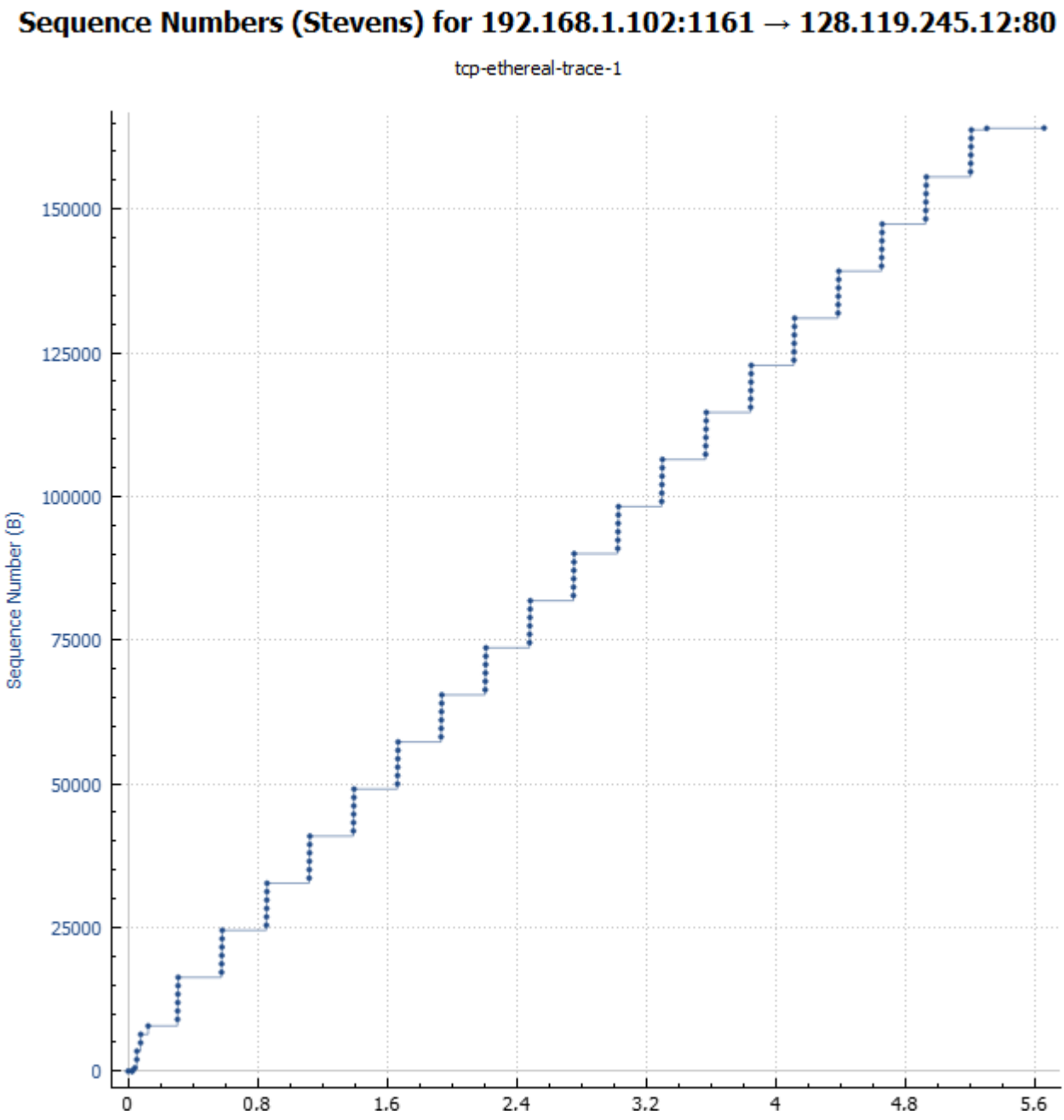
O tamanho do buffer informado é 17520 bytes

```
[Next sequence number: 566    (rel
Acknowledgment number: 1    (relat
0101 .... = Header Length: 20 byte
> Flags: 0x018 (PSH, ACK)
Window size value: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (n
```

```
0030  44 70 1f bd 00 00 50 4f  53 54 20
0040  72 65 61 6c 2d 6c 61 62  73 2f 6c
0050  2d 72 65 70 6c 79 2e 68  74 6d 20
```

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

Não, conforme imagem.

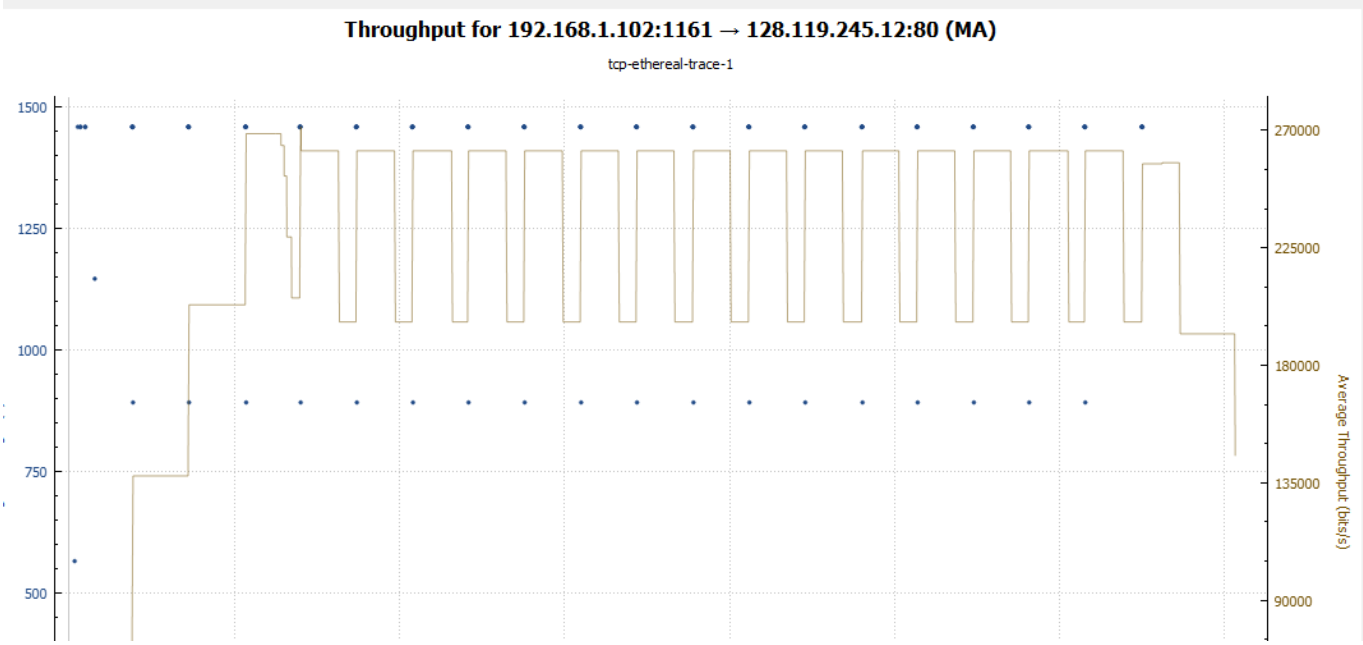


11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 247 in the text).

Os geralmente referem-se a 1460 bytes, que é o temanho médio de pacote sendo enviado.

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

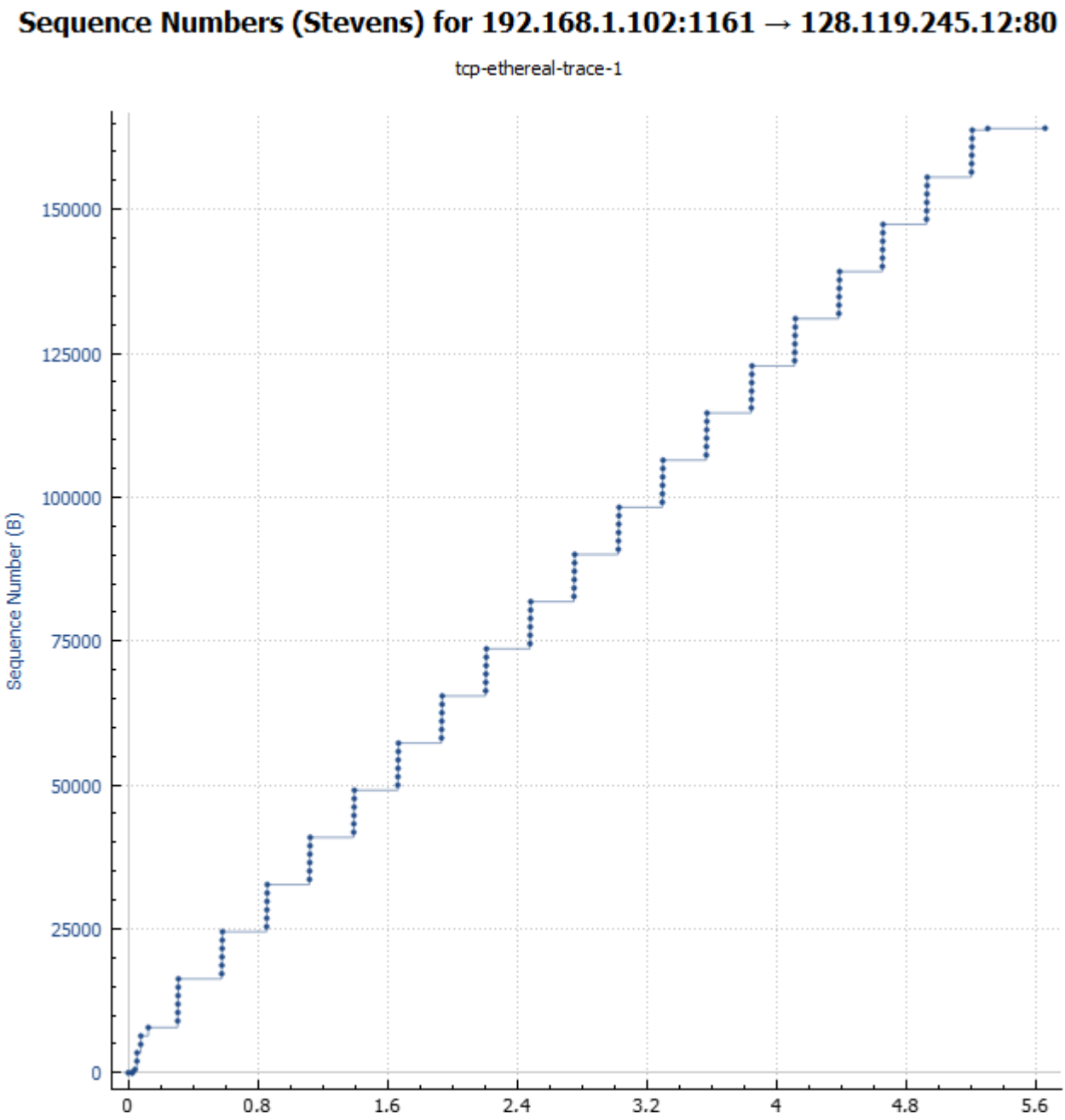
Podemos observar uma média de 225000 bytes por segundo, conforme imagem.



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.

Slowstart começa no pacote 1 e vai até o 11. Congestion avoidance começa a partir do 13.


Sequence Numbers (Stevens) for 192.168.1.102:1161 → 128.119.245.12:80
tcp-ethereal-trace-1
Sequence Number (B)
150000
125000
100000
75000
50000
25000
0
0
0.8
1.6
2.4
3.2
4
4.8
5.6