

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

Time	Length	Source	Destination	Protocol	Length	Info
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

Time	Length	Source	Destination	Protocol	Length	Info
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

Time	Length	Source	Destination	Protocol	Length	Info
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.

```
[TCP Segment Len: 0]
Sequence number: 0    (relative sequence number)
[Next sequence number: 0    (relative sequence number)]
Acknowledgment number: 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
  .... .... ...0 = Fin: Not set
[TCP Flags: .....S.]
```

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.

```
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0111 .... = Header Length: 28 bytes (7)
▼ 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
        ▼ [Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 80]
            [Connection establish acknowledge (SYN+ACK): server port 80]
            [Severity level: Chat]
            [Group: Sequence]
            .... .... ...0 = Fin: Not set
            [TCP Flags: .....A..S.]
```

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.

```
Sequence number: 1    (relative sequence number)
[Next sequence number: 566    (relative sequence number)]
Acknowledgment number: 1    (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH ACK)
```

00 06 25 da af 73 00 20 e0 8a 70 1a 08 00 45 00	..%.s. .p...E.
02 5d 1e 21 40 00 80 06 a2 e7 c0 a8 01 66 80 77	.].!@... ..f.w
f5 0c 04 89 00 50 0d d6 01 f5 34 a2 74 1a 50 18P.. .4.t.P.
44 70 1f bd 00 00 50 4f 53 54 20 2f 65 74 68 65	Dp..PO ST /ethe
72 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 33 2d 31	real-lab s/lab3-1
2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 54 50 2f	-reply.h tm HTTP/
31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 69 61 2e	1.1..Hos t: gaia.
63 73 2e 75 6d 61 73 73 2e 65 64 75 0d 0a 55 73	cs.umass .edu..Us
65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c	er-Agent : Mozill
61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20	a/5.0 (W indows;
55 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e	U; Windo ws NT 5.
31 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 30	1; en-US ; rv:1.0
2e 32 29 20 47 65 63 6b 6f 2f 32 30 30 33 30 32	.2) Geck o/200302
30 38 20 4e 65 74 73 63 61 70 65 2f 37 2e 30 32	08 Netsc ape/7.02
0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 78	..Accept : text/x
6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78	ml,appli cation/x
6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78	ml,appli cation/x
68 74 6d 6c 2b 78 6d 6c 2c 74 65 78 74 2f 68 74	html+xml ,text/ht
6d 6c 3b 71 3d 30 2e 39 2c 74 65 78 74 2f 70 6c	ml;q=0.9 text/pl

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 reassemb
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

```

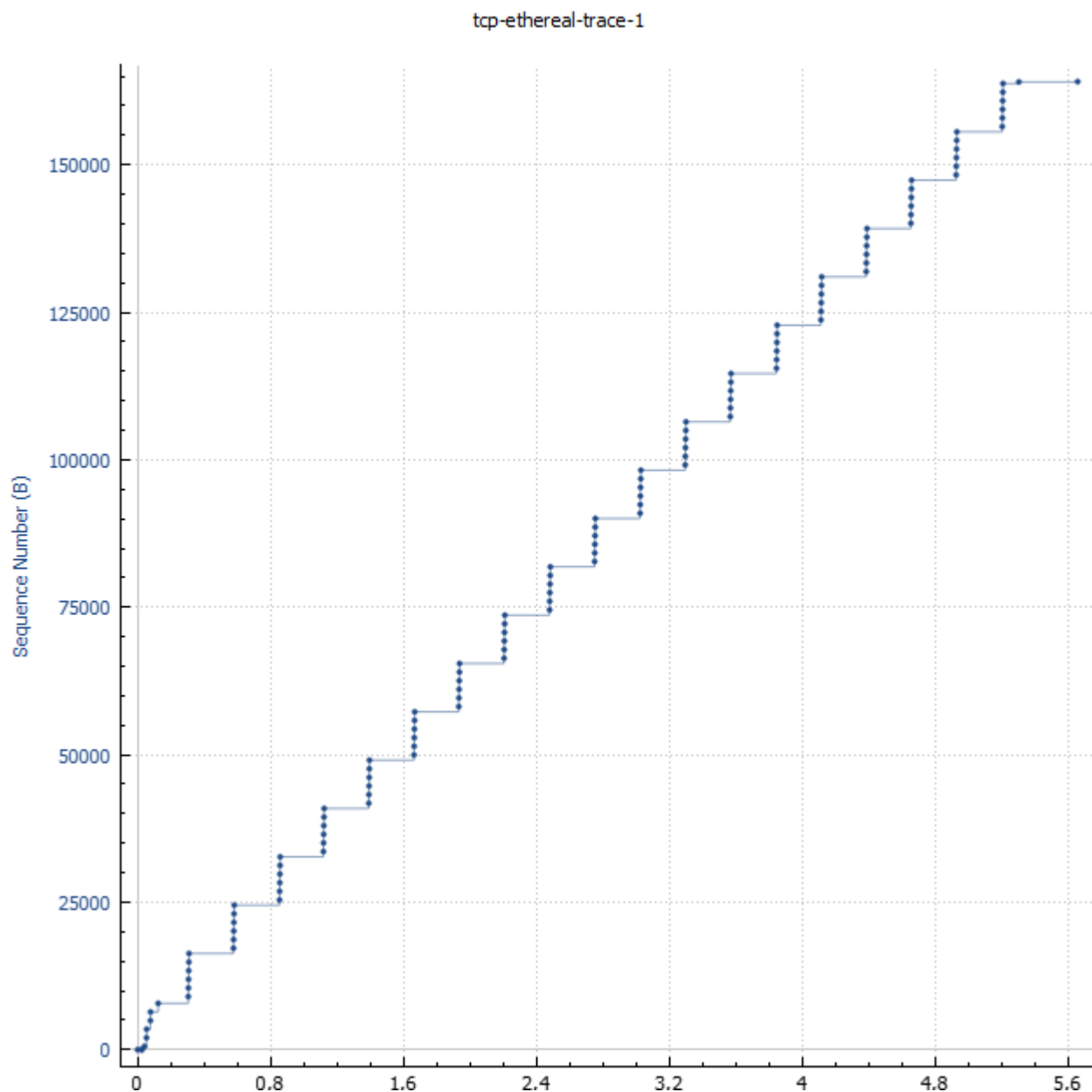
[Next sequence number: 566      (rel
Acknowledgment number: 1      (relat
0101 .... = Header Length: 20 byte
> Flags: 0x018 (PSH, ACK)
Window size value: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (n
0030 44 70 1f bd 00 00 50 4f 53 54 20
0040 72 65 61 6c 2d 6c 61 62 73 2f 6c
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.

Sequence Numbers (Stevens) for 192.168.1.102:1161 → 128.119.245.12:80

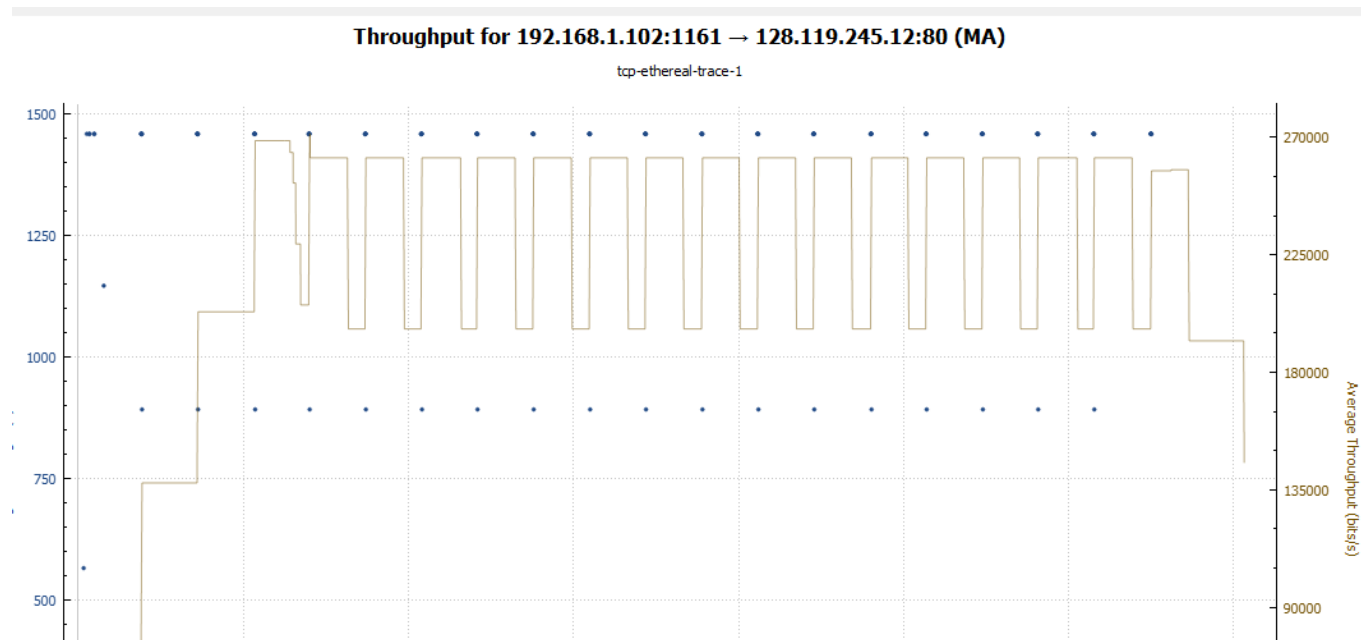


11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 247 in the text).

Os geralmente referem-se a 1460 bytes, que é o tamanho 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

