

# **Relatório TCP e DNS**

César Henrique Bernabé

Luana Vettler Reis

Marini Favero

# TCP

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?

No.	Time	Source	Destination	Protocol
198	1.922267	192.168.1.105	128.119.245.12	HTTP
217	2.092108	128.119.245.12	192.168.1.105	HTTP

▶ Frame 198: 935 bytes on wire (7480 bits), 935 bytes captured (7480 bits) on interface  
 ▶ Ethernet II, Src: Apple\_26:b5:2c (b8:e8:56:26:b5:2c), Dst: Tp-LinkT\_d1:8c:5e:40:00:00  
 ▶ Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12  
 ▼ Transmission Control Protocol, Src Port: 50946 (50946), Dst Port: 80 (80)  
     Source Port: 50946  
     Destination Port: 80  
     [Stream index: 0]

IP: 192.168.1.105

Porta Origem: 50946

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?

No.	Time	Source	Destination	Protocol	Length
1	0.000000	192.168.1.105	128.119.245.12	TCP	
2	0.174997	128.119.245.12	192.168.1.105	TCP	
3	0.175095	192.168.1.105	128.119.245.12	TCP	
4	0.175496	192.168.1.105	128.119.245.12	TCP	
5	0.175497	192.168.1.105	128.119.245.12	TCP	
6	0.175497	192.168.1.105	128.119.245.12	TCP	
7	0.265710	64.233.186.189	192.168.1.105	TLSv...	

▶ Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface  
 ▶ Ethernet II, Src: Tp-LinkT\_d1:be:22 (00:27:19:d1:be:22), Dst: Apple\_26:b5:2c  
 ▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105  
 ▼ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 50946 (50946)  
     Source Port: 80  
     Destination Port: 50946  
     [Stream index: 0]  
     [TCP Segment Len: 0]

```

0000  b8 e8 56 26 b5 2c 00 27 19 d1 be 22 08 00 45 00  ..V&.,.' ..."..E.
0010  00 3c 00 00 40 00 31 06 12 27 80 77 f5 0c c0 a8  .<..@.1. .'w....
0020  01 69 00 50 c7 02 d0 02 90 cb 44 33 46 35 a0 12  .i.P.... ..D3F5..
0030  38 90 39 20 00 00 02 04 05 b4 04 02 08 0a 3b 65  8.9 .... .....;e
0040  da 3d 35 8b a0 f2 01 03 03 07                    .=5..... ..
  
```

O computador remoto, cujo IP é 128.119.245.12 está enviando pacotes através da porta 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?**

No.	Time	Source	Destination	Protocol	Length
1	0.000000	192.168.1.105	128.119.245.12	TCP	
2	0.174997	128.119.245.12	192.168.1.105	TCP	
3	0.175095	192.168.1.105	128.119.245.12	TCP	
4	0.175496	192.168.1.105	128.119.245.12	TCP	
5	0.175497	192.168.1.105	128.119.245.12	TCP	
6	0.175497	192.168.1.105	128.119.245.12	TCP	
7	0.265710	64.233.186.189	192.168.1.105	TLSv...	

▶ Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface  
 ▶ Ethernet II, Src: Apple\_26:b5:2c (b8:e8:56:26:b5:2c), Dst: Tp-LinkT\_d1:be:  
 ▶ Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12  
 ▼ Transmission Control Protocol, Src Port: 50946 (50946), Dst Port: 80 (80),  
 Source Port: 50946  
 Destination Port: 80  
 [Stream index: 0]  
 [TCP Segment Len: 66]

```

0000 00 27 19 d1 be 22 b8 e8 56 26 b5 2c 08 00 45 00  .'...'.. V&...E.
0010 00 34 09 9d 40 00 40 06 f9 91 c0 a8 01 69 80 77  .4..@.@. ....i.w
0020 f5 0c c7 02 00 50 44 33 46 35 d0 02 90 cc 80 10  ....PD3 F5.....
0030 10 15 8f b8 00 00 01 01 08 0a 35 8b a1 a1 3b 65  ..... ..5...;e
0040 da 3d                                     .,=
  
```

IP: 192.168.1.105

Porta: 50946

**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?**

No.	Time	Source	Destination	Protocol	Length	Info
1	0....	192.168.1.105	128.119.245.12	TCP	78	50946 → 80 [SYN] Seq
2	0....	128.119.245.12	192.168.1.105	TCP	74	80 → 50946 [SYN, ACK]
3	0....	192.168.1.105	128.119.245.12	TCP	66	50946 → 80 [ACK] Seq
4	0....	192.168.1.105	128.119.245.12	TCP	1514	[TCP segment of a r

.... ..0 .... = Acknowledgment: Not set  
 .... .. 0... = Push: Not set  
 .... .. .0.. = Reset: Not set  
 ▶ .... .. ..1. = Syn: Set

```

0000 00 27 19 d1 be 22 b8 e8 56 26 b5 2c 08 00 45 00  .'...'.. V&...E.
0010 00 40 84 2f 40 00 40 06 7e f3 c0 a8 01 69 80 77  .@./@.@. ~....i.w
0020 f5 0c c7 02 00 50 44 33 46 34 00 00 00 00 b0 02  ....PD3 F4.....
0030 ff ff d7 2f 00 00 02 04 05 b4 01 03 03 05 01 01  .../..... ..
0040 08 0a 35 8b a0 f2 00 00 00 00 04 02 00 00  ..5.....
  
```

Como pode ser visto na figura acima, o Segment Number do pacote SYN usado pra iniciar a conexão com o computador cliente e gaia.cs.umass.edu é 0. Ele pode ser identificado como pacote SYN pois este é o único que possui Acknowledgement Number igual a zero, além disso possui a flag SYN ativada.

**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?**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.105	128.119.245.12	TCP	78	50946 → 80 [SYN] Seq=
2	0.000000	128.119.245.12	192.168.1.105	TCP	74	80 → 50946 [SYN, ACK]
3	0.000000	192.168.1.105	128.119.245.12	TCP	66	50946 → 80 [ACK] Seq=
4	0.000000	192.168.1.105	128.119.245.12	TCP	1514	[TCP segment of a rea

....	...1	....	= Acknowledgment: Set
....	....	0...	= Push: Not set
....	....	.0..	= Reset: Not set
....	....	..1.	= Syn: Set

0000	b8 e8 56 26 b5 2c 00 27 19 d1 be 22 08 00 45 00	..V&.,.' ..."..E.
0010	00 3c 00 00 40 00 31 06 12 27 80 77 f5 0c c0 a8	.<..@.1. .'w....
0020	01 69 00 50 c7 02 d0 02 90 cb 44 33 46 35 a0 12	.i.P.... ..D3F5..
0030	38 90 39 20 00 00 02 04 05 b4 04 02 08 0a 3b 65	8.9 .... ..;e
0040	da 3d 35 8b a0 f2 01 03 03 07	.=5..... ..

O Sequence Number do SYNACK também é zero (como o do pacote SYN), e do Acknowledgment number é igual a 1. Para determinar esses valores, o computador remoto (gaia.cs.umass.edu) replica o Sequence Number do pacote SYN previamente recebido, e seta os bits Syn e Acknowledgment como 1 (no pacote SYN o bit Acknowledgment é zero, e é assim que o SYNACK difere do SYN).

6. What is the sequence number of the TCP segment containing the HTTP POST command?

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000000	192.168.1.105	128.119.245.12	TCP	66	50946 → 80 [ACK] Seq=1448
4	0.000000	192.168.1.105	128.119.245.12	TCP	1514	[TCP segment of a retransmission] Seq=1
5	0.000000	192.168.1.105	128.119.245.12	TCP	1514	[TCP segment of a retransmission] Seq=1

[TCP Segment Len: 1448]  
Sequence number: 1 (relative sequence number)  
[Next sequence number: 1449 (relative sequence number)]  
Acknowledgment number: 1 (relative ack number)  
Header Length: 32 bytes

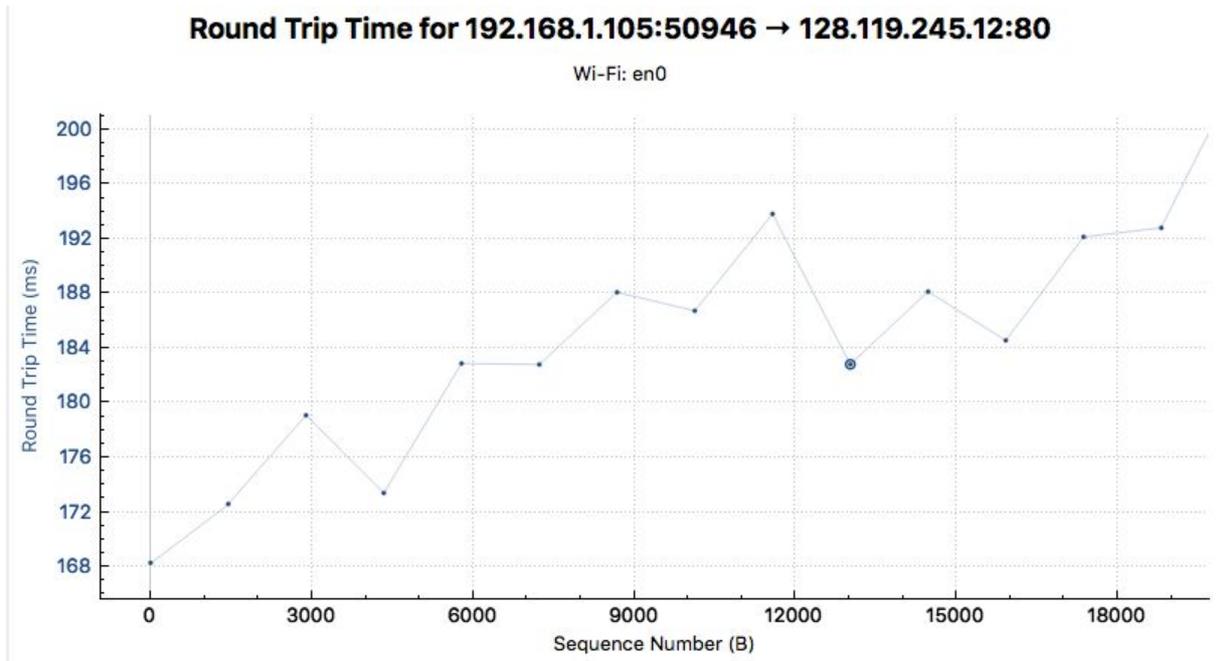
0000	00 27 19 d1 be 22 b8 e8 56 26 b5 2c 08 00 45 00	.\"
0010	05 dc 84 9e 40 00 40 06 78 e8 c0 a8 01 69 80 77	....@.@. x....i.w
0020	f5 0c c7 02 00 50 44 33 46 35 d0 02 90 cc 80 10	....PD3 F5.....
0030	10 15 fd ff 00 00 01 01 08 0a 35 8b a1 a1 3b 65	..... ..5...;e
0040	da 3d 50 4f 53 54 20 2f 77 69 72 65 73 68 61 72	.=POST / wireshar
0050	6b 2d 6c 61 62 73 2f 6c 61 62 33 2d 31 2d 72 65	k-labs/l ab3-1-re

Na imagem, pode-se ver que o campo de dados do pacote possui o comando POST. Por ser o primeiro pacote enviado após o handshake, possui Sequence Number também igual a 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 after the receipt of each ACK?

Pacote TCP	Sequence Number	Tempo Enviado	ACK Recebido (time)
1	1	0.175496	0.343723
2	1449	0.175497	0.348038
3	2897	0.175497	0.348038
4	4345	0.343837	0.354533
5	5793	0.343837	0.517179
6	7241	0.348142	0.526666

O tempo estimado de RTT para os seis (e também dos primeiros 14) é mostrado no gráfico a seguir, onde vemos que o tempo mínimo foi 168 ms e o tempo máximo (para os primeiros 6) foi de 183ms:



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

O tamanho de cada pacote é 1448 bytes de dados, mais 32 bytes de cabeçalho, totalizando 1480 bytes. Isso pode ser verificado através das informações obtidas de cada pacote, como mostrado na imagem a seguir:

```
 3 0.175095      192.168.1.105  128.119.245.12  TCP           66 50946 →
 4 0.175496      192.168.1.105  128.119.245.12  TCP           1514 [TCP se
 5 0.175497      192.168.1.105  128.119.245.12  TCP           1514 [TCP se

  Acknowledgment number: 1      (relative ack number)
  Header Length: 32 bytes
  ▶ Flags: 0x010 (ACK)
  Window size value: 4117
  [Calculated window size: 131744]
  [Window size scaling factor: 32]
  ▶ Checksum: 0xfdf [validation disabled]
  Urgent pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamp:
  ▶ [SEQ/ACK analysis]
  TCP segment data (1448 bytes)
0000  00 27 19 d1 be 22 b8 e8 56 26 b5 2c 08 00 45 00  .'...'.. V&.,..E.
```

**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?**

O espaço mínimo de buffer que pode ser enviado é dado pelo tamanho mínimo da janela, nesse caso 4117 bits. O tamanho da janela não limitou o sender em nenhum momento da transmissão, inclusive o tamanho da janela é diminuído no meio do processo, como pode-se ver na figura a seguir, onde a janela recebe novo tamanho (274) com escala em 128, totalizando 35072, e ainda assim nenhum pacote teve de ser quebrado em pacotes menores para ser reenviado:

tcp							
No.	▲	Time	Source	Destination	Protocol	Length	Info
143		1.327638	192.168.1.105	128.119.245.12	TCP	1514	[TCP segment of
144		1.327639	192.168.1.105	128.119.245.12	TCP	1514	[TCP segment of
145		1.328953	128.119.245.12	192.168.1.105	TCP	66	[TCP Window Upda
146		1.459471	128.119.245.12	192.168.1.105	TCP	66	80 → 50946 [ACK]
147		1.459573	192.168.1.105	128.119.245.12	TCP	1514	[TCP segment of
Window size value: 274							
[Calculated window size: 35072]							
[Window size scaling factor: 128]							
0000		b8 e8 56 26 b5 2c 00 27	19 d1 be 22 08 00 45 00	..V&.,, ' ...".E.			
0010		00 34 4a 64 40 00 31 06	c7 ca 80 77 f5 0c c0 a8	.4Jd@.1. ...w....			
0020		01 69 00 50 c7 02 d0 02	90 cc 44 34 dd 75 80 10	.i.P.... ..D4.u..			
0030		01 12 ff 40 00 00 01 01	08 0a 3b 65 de bf 35 8b	...@.... ..;e.5.			
0040		a5 58		.X			

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

```

tcp
No.  Time      Source           Destination      Protocol Length Info
107  1.136639  128.119.245.12  192.168.1.105   TCP        78    [TCP Dup ACK 104#1] 80 → 5094
108  1.136717  192.168.1.105   128.119.245.12  TCP        1514  [TCP segment of a reassembled
109  1.143496  128.119.245.12  192.168.1.105   TCP        78    [TCP Dup ACK 104#2] 80 → 5094
110  1.143578  192.168.1.105   128.119.245.12  TCP        1514  [TCP Fast Retransmission] [TC
111  1.149179  128.119.245.12  192.168.1.105   TCP        78    [TCP Dup ACK 104#3] 80 → 5094

Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 1448]
Sequence number: 63713 (relative sequence number)
0000  00 27 19 d1 be 22 b8 e8 56 26 b5 2c 08 00 45 00  .'. . . . V& . . . E.
0010  05 dc e7 a5 40 00 40 06 15 e1 c0 a8 01 69 80 77  . . . . @ . @ . . . . i . w
0020  f5 0c c7 02 00 50 44 34 3f 15 d0 02 90 cc 80 10  . . . . PD4 ? . . . . .
0030  10 15 49 6f 00 00 01 01 08 0a 35 8b a5 58 3b 65  ..Io . . . . . 5 . . X ; e
0040  de 06 60 50 6c 65 61 73 65 2c 20 74 68 65 6e 2c  ..`Pleas e, then,
0050  27 20 73 61 69 64 20 41 6c 69 63 65 2c 20 60 68  ' said A lice, `h
0060  6f 77 20 61 6d 20 40 20 74 6f 20 67 65 74 20 69  ow am I to get i

```

Ocorreu retransmissão apenas do pacote de número 110. Esse caso pode ser identificado pois o Sequence Number deste pacote é inferior ao Sequence Number do anterior.

**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.**

Analisando os seguintes pacotes ACK:

Pacote	Acknowledge Number	Diferença
82	47785	-
87	50681	2896
92	53577	2896
95	56473	2896
98	59369	2896

Percebemos que o receptor tipicamente reconhece 2896 bytes de dados, que é equivalente a duas vezes o segmentos de dados de um pacote TCP, ou seja, o receptor está acking dois pacotes por ack.

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

No.	Time	Source	Destination	Protocol	Length	Info
2.036396		128.119.245.12	192.168.1.105	TCP	66	80 → 509
2.084223		128.119.245.12	192.168.1.105	TCP	66	80 → 509
2.091879		128.119.245.12	192.168.1.105	TCP	66	80 → 509
2.092100		128.119.245.12	192.168.1.105	HTTP	945	HTTP/1.1

```

Source Port: 80
Destination Port: 50946
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 152910 (relative ack number)
Header Length: 32 bytes
Flags: 0-010 (ACK)
0000  b8 e8 56 26 b5 2c 00 27 19 d1 be 22 08 00 45 00  ..V&.,.' ..."..E.
0010  00 34 4a 7f 40 00 31 06 c7 af 80 77 f5 0c c0 a8  .4J.@.1. ...w....
0020  01 69 00 50 c7 02 d0 02 90 cc 44 35 9b 82 80 10  .i.P.... ..D5....
0030  02 be 39 a7 00 00 01 01 08 0a 3b 65 e1 b9 35 8b  ..9..... ;;e..5.
0040  a8 3e  .>
  
```

Na imagem acima, vemos que o ultimo pacote ACK referente ao pacote TCP, que o Acknowledgement Number desse foi 152910, ou seja, 152910 bytes de dados foram transmitidos. Dividindo esse número por 1448 bytes (tamanho do segmento de dados do pacote TCP), obtemos o número de pacotes que foram enviados:

$152910/1448 = 105$  pacotes (com segmento de dados completo) + 870 (quantidade de dados no segmento de dados do primeiro pacote enviado, HTTP Post) = 106 pacotes.

Além disso, foram gastos  $106 \times 32$  bytes (tamanho do header de cada pacote) = 3392 bytes.

Finalmente, foram gastos mais  $66 \times 2$  (pacotes ACK) = 132 bytes e 78 bytes do pacote SYN.

Resumindo:

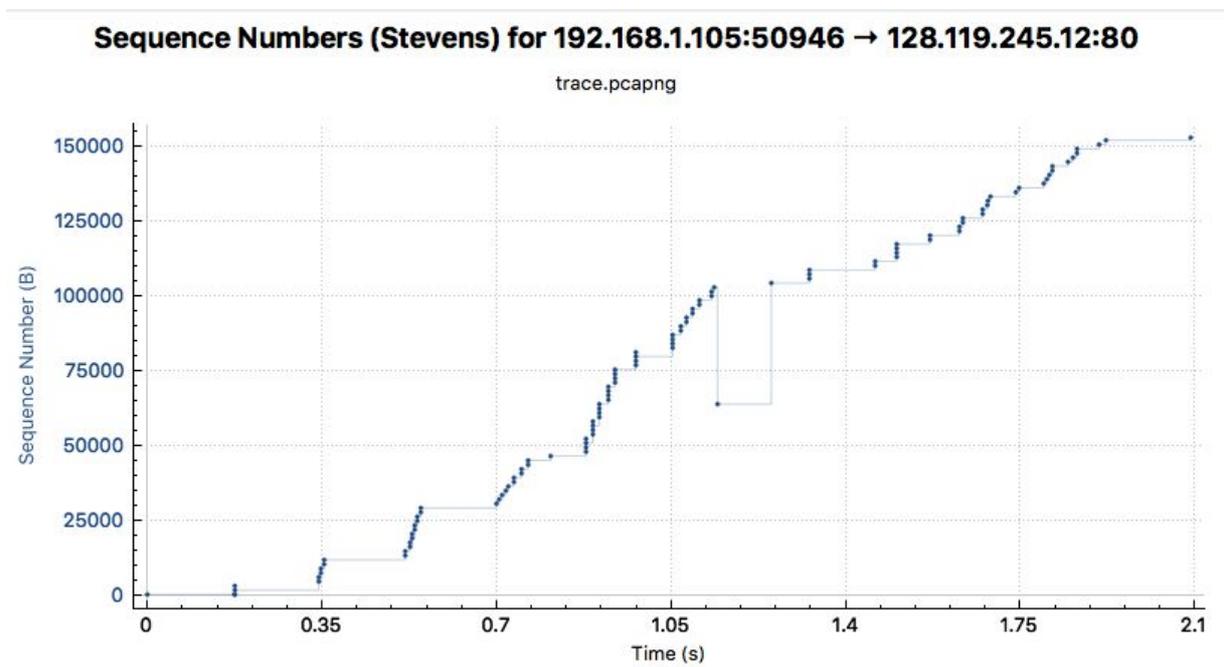
Dados Enviados Dentro do Segmento de Dados do Pacote TCP	152910 bytes
Dados de todos os Headers Enviados	3392 bytes
Pacotes ACK	132 bytes
Pacote SYN	78 bytes
TOTAL	156512

Finalmente, a vazão pode ser calculada:

$$V = 156512 \text{ bytes} / 2.092180 \text{ (tempo em que o ultimo pacote foi recebido)}$$

$$V = 74.8 \text{ bytes/segundo}$$

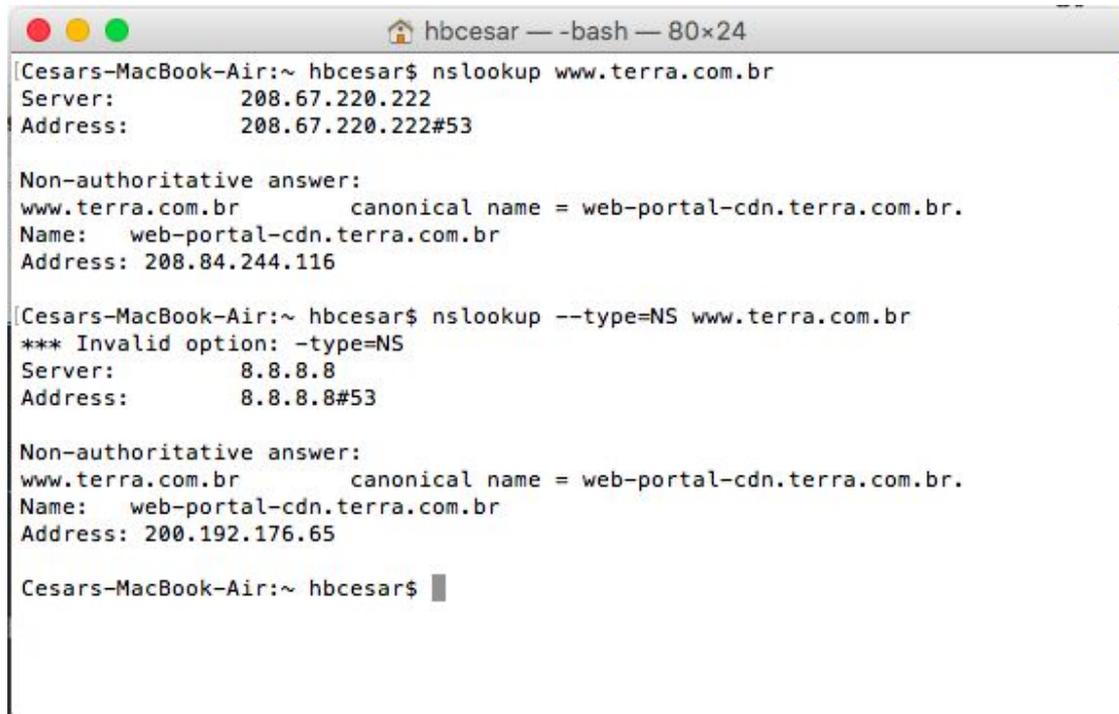
**13. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which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



O controle de fluxo do TCP é realizado pelo método Sliding Window, que é definido por cada um dos lados no estabelecimento da conexão, então o menor tamanho entre os dois é adotado. A medida que os dados vão sendo enviados, o tamanho da janela vai se fechando. Em contrapartida, a medida que os ACKs vão sendo recebidos, o tamanho da janela volta a “se abrir”. Isso permite que mais que um pacote possa ser enviado na espera pelo ACK e implementa um método simples de controle de fluxo. Pelo gráfico, pode-se ver que os pacotes começam a ser enviados com menor intervalo de tempo após 0.7 segundos (o tempo entre um ACK e outro reduz). Em geral, o controle de fluxo também tenta fazer com que o número de pacotes enviados por unidade de tempo aumente gradativamente, e é exatamente isso que

pode-se ver, pois pode-se ver que a linha torna-se mais vertical a medida que avança. Isso evita que a rede congestionue devido a um numero muito grande de pacotes enviado por unidade de tempo.

# DNS



```
Cesars-MacBook-Air:~ hbcesar$ nslookup www.terra.com.br
Server:      208.67.220.222
Address:     208.67.220.222#53

Non-authoritative answer:
www.terra.com.br      canonical name = web-portal-cdn.terra.com.br.
Name:   web-portal-cdn.terra.com.br
Address: 208.84.244.116

Cesars-MacBook-Air:~ hbcesar$ nslookup --type=NS www.terra.com.br
*** Invalid option: -type=NS
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
www.terra.com.br      canonical name = web-portal-cdn.terra.com.br.
Name:   web-portal-cdn.terra.com.br
Address: 200.192.176.65

Cesars-MacBook-Air:~ hbcesar$
```

**1. Execute nslookup para obter o endereço IP de um servidor Web no Brasil.**

O endereço IP do servidor da página web [www.terra.com.br](http://www.terra.com.br) é 200.137.66.240, como exibido acima.

**2. Execute nslookup para determinar o servidor de autoridade DNS para um endereço IP qualquer.**

Não foi encontrado servidor de autoridade DNS para o endereço terra.com.br, como ainda pode-se ver na figura acima.

**4. Localize as mensagens de requisição e resposta DNS. Elas são enviadas sobre o UDP ou TCP?**

No.	Time	Source	Destination	Protocol	Length	Inf
1	0.000000	192.168.1.103	8.8.8.8	DNS	72	St
2	0.310208	8.8.8.8	192.168.1.103	DNS	156	St
3	0.312210	192.168.1.103	104.20.1.85	TCP	78	50
4	0.503312	104.20.1.85	192.168.1.103	TCP	66	80
5	0.503406	192.168.1.103	104.20.1.85	TCP	54	50
6	0.503735	192.168.1.103	104.20.1.85	HTTP	371	GE
7	0.696710	104.20.1.85	192.168.1.103	TCP	54	80

▶ Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interf  
 ▶ Ethernet II, Src: Apple\_26:b5:2c (b8:e8:56:26:b5:2c), Dst: Tp-LinkT\_d1:be:22  
 ▶ Internet Protocol Version 4, Src: 192.168.1.103, Dst: 8.8.8.8  
 ▶ User Datagram Protocol, Src Port: 59301 (59301), Dst Port: 53 (53)  
 ▶ Domain Name System (query)

0000	00 27 19 d1 be 22 b8 e8	56 26 b5 2c 08 00 45 00	..'...."... V&.,...E.
0010	00 3a e9 ac 00 00 ff 11	ff e6 c0 a8 01 67 08 08	..:..... ..g..
0020	08 08 e7 a5 00 35 00 26	7f 0b a4 57 01 00 00 01	.....5.& ...W....
0030	00 00 00 00 00 00 03 77	77 77 04 69 65 74 66 03	.....w ww.ietf.
0040	6f 72 67 00 00 01 00 01		org.....

Como pode-se ver na figura acima, as mensagens de requisição e resposta do DNS são enviadas sobre UDP.

**5. Qual a porta destino para a mensagem de requisição DNS? Qual é a porta fonte da mensagem DNS?**

Ainda analisando a figura da questão anterior, podemos verificar que a porta destino da requisição é a porta 53, e a porta fonte da mensagem DNS é a porta 59301.

**6. Para qual endereço IP a mensagem de requisição DNS é enviada? Use ipconfig para determinar o endereço IP de seu servidor local DNS. Esses dois endereços IP são os mesmos?**

A mensagem de requisição é enviada para 8.8.8.8, que é o servidor de DNS usado pelo meu computador.

**7. Examine a mensagem de requisição DNS. Qual o tipo de requisição DNS?**

No.	Time	Source	Destination	Protocol	Length
1	0.000000	192.168.1.103	8.8.8.8	DNS	72
2	0.310208	8.8.8.8	192.168.1.103	DNS	156
3	0.312210	192.168.1.103	104.20.1.85	TCP	78
4	0.503312	104.20.1.85	192.168.1.103	TCP	66
5	0.503406	192.168.1.103	104.20.1.85	TCP	54
6	0.503735	192.168.1.103	104.20.1.85	HTTP	371
7	0.696710	104.20.1.85	192.168.1.103	TCP	54

Answer RRs: 0  
 Authority RRs: 0  
 Additional RRs: 0  
 ▼ Queries  
 ► www.ietf.org: type A, class IN

0000	00 27 19 d1 be 22 b8 e8 56 26 b5 2c 08 00 45 00	. '... " .. V& ,... E.
0010	00 3a e9 ac 00 00 ff 11 ff e6 c0 a8 01 67 08 08	.: ..... ..g..
0020	08 08 e7 a5 00 35 00 26 7f 0b a4 57 01 00 00 01	.... 5.& ...W....
0030	00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03	.....w ww.ietf.
0040	6f 72 67 00 00 01 00 01	org.....

Pela figura acima, vemos que foi realizada requisição do tipo A, ou Standard Query. Esse tipo de requisição solicita o endereço IP de um domínio.

**8. Examine a mensagem DNS response. Quantas “respostas” são providas? O que cada resposta contém?**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.103	8.8.8.8	DNS	72	Standard query 0
2	0.310208	8.8.8.8	192.168.1.103	DNS	156	Standard query r
3	0.312210	192.168.1.103	104.20.1.85	TCP	78	50126 → 80 [SYN]
4	0.503312	104.20.1.85	192.168.1.103	TCP	66	80 → 50126 [SYN,
5	0.503406	192.168.1.103	104.20.1.85	TCP	54	50126 → 80 [ACK]

Additional RRs: 0

- Queries
  - www.ietf.org: type A, class IN
- Answers
  - www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare-dnssec.net
  - www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.1.85
  - www.ietf.org.cdn.cloudflare-dnssec.net: type A, class IN, addr 104.20.0.85

```

0000 b8 e8 56 26 b5 2c 00 27 19 d1 be 22 08 00 45 28 ..V&.,.'...".E(
0010 00 8e ee 17 00 00 2f 11 cb 00 08 08 08 08 c0 a8 ...../. .....
0020 01 67 00 35 e7 a5 00 7a 87 f6 a4 57 81 80 00 01 .g.5...z ...W....
0030 00 03 00 00 00 00 03 77 77 77 04 69 65 74 66 03 .....w ww.ietf.

```

São providas um total de 3 respostas. A primeira possui resposta do tipo CNAME, que é um mapeamento de um alias, ou seja, de [www.ietf.org](http://www.ietf.org) para [www.ietf.org.cdn.cloudflare-dnssec.net](http://www.ietf.org.cdn.cloudflare-dnssec.net). As segunda e terceira resposta são do tipo A, onde são fornecidos dois endereços de IP para o endereço requisitado (104.20.1.85 e 104.20.0.85).

**9. Considere o pacote subsequente TCP SYN enviado pelo seu host. O endereço IP destino do pacote SYN corresponde ao endereços IP fornecido pela mensagem response DNS?**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.103	8.8.8.8	DNS	72	Standard
2	0.310208	8.8.8.8	192.168.1.103	DNS	156	Standard
3	0.312210	192.168.1.103	104.20.1.85	TCP	78	50126 → 80
4	0.503312	104.20.1.85	192.168.1.103	TCP	66	80 → 50126
5	0.503406	192.168.1.103	104.20.1.85	TCP	54	50126 → 80

Time to live: 64  
 Protocol: TCP (6)  
 ▶ Header checksum: 0x7a6c [validation disabled]  
 Source: 192.168.1.103  
 Destination: 104.20.1.85  
 [Source GeoIP: Unknown]

Sim, o IP de destino usado no pacote TCP é o fornecido pela primeira resposta do tipo A do pacote de DNS Response.

## Usando NSLOOKUP:

11. Qual a porta destino para a mensagem de requisição DNS? Qual é porta fonte da mensagem DNS response?

Porta de Destino para Mensagem de Requisição: 53

Porta Fonte de mensagem DNS Response: 53.

12. Para qual endereço IP a mensagem de requisição DNS é enviada? Este é o endereço IP de seu servidor padrão local DNS?

A mensagem de requisição é enviada para 208.67.220.222 que é o servidor de DNS secundário usado pelo meu computador.

13. Examine a mensagem de requisição DNS. Qual é o tipo mensagem de requisição DNS? A mensagem de requisição contém quais “respostas” ?

A mensagem de requisição é do tipo A, e possui 0 resposta, apenas uma query.

14. Examine a mensagem DNS response. Quantas “respostas” são providas ? O que cada uma dessas mensagens contém ?

No.	Time	Source	Destination	Protocol	Length	Info
3	1.949067	192.168.1.103	8.8.8.8	DNS	71	Standard quer
4	2.950587	192.168.1.103	208.67.220.222	DNS	71	Standard quer
5	3.121541	208.67.220.222	192.168.1.103	DNS	160	Standard quer
6	7.337631	192.168.1.103	52.88.107.124	TCP	54	50907 → 443

▼ Queries	
▶ www.mit.edu: type A, class IN	
▼ Answers	
▶ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net	
▶ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net	
▶ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.203.80.8	

0000	b8 e8 56 26 b5 2c 00 27 19 d1 be 22 08 00 45 00	..V&.,.' ..."..E.
0010	00 92 00 00 40 00 37 11 d4 29 d0 43 dc de c0 a8	....@.7. ).C....
0020	01 67 00 35 d1 4f 00 7e bd 41 d0 6a 81 80 00 01	.g.5.0.~ .A.j....
0030	00 03 00 00 00 00 03 77 77 77 03 6d 69 74 03 65	.....w ww.mit.e
0040	64 75 00 00 01 00 01 c0 0c 00 05 00 01 00 00 05	du..... .....

São providas três respostas, duas do tipo CNAME que redirecionam o alias [www.mit.edu](http://www.mit.edu) para [www.mit.edu.edgekey.net](http://www.mit.edu.edgekey.net) e [e9566.dscb.akamaiedge.net](http://e9566.dscb.akamaiedge.net). A terceira resposta retorna o endereço IP do domínio fornecido pela segunda resposta do tipo CNAME: 23.203.80.8.

## Usando nslookup --type=NS mit.edu

**16. Para qual endereço IP a mensagem de requisição DNS é enviada? Este é o endereço IP de seu servidor padrão local DNS?**

A mensagem de requisição é enviada para 208.67.220.222 que é o servidor de DNS secundário usado pelo meu computador.

**17. Examine a mensagem de requisição DNS. Qual é o tipo mensagem de requisição DNS? A mensagem de requisição contém quais “respostas” ?**

No.	Time	Source	Destination	Protocol	Length	
1	0.000000	192.168.1.103	8.8.8.8	DNS	67	
2	0.999982	192.168.1.103	208.67.220.222	DNS	67	
3	1.146855	208.67.220.222	192.168.1.103	DNS	83	
4	1.647046	192.168.1.103	224.0.0.251	IGMP...	46	

```

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ► mit.edu: type A, class IN
0000  00 27 19 d1 be 22 b8 e8 56 26 b5 2c 08 00 45 00  .'....".. V&,...E.
0010  00 35 bf 87 00 00 40 11 4b ff c0 a8 01 67 d0 43  .5....@. K....g.C
0020  dc de d9 62 00 35 00 21 47 f5 97 30 01 00 00 01  ..b.5.! G..0....
0030  00 00 00 00 00 00 03 6d 69 74 03 65 64 75 00 00  .....m it.edu..
0040  01 00 01  ...
  
```

A mensagem de requisição é do tipo A, e possui 0 resposta, apenas uma query.

18. Examine a mensagem DNS response. Quantas “respostas” são providas ? O que cada uma dessas mensagens contém ?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.103	8.8.8.8	DNS	67	Sta
2	0.999982	192.168.1.103	208.67.220.222	DNS	67	Sta
3	1.146855	208.67.220.222	192.168.1.103	DNS	83	Sta
4	1.647046	192.168.1.103	224.0.0.251	IGMP...	46	Mem

```

Authority RRs: 0
Additional RRs: 0
▼ Queries
  ► mit.edu: type A, class IN
▼ Answers
  ► mit.edu: type A, class IN, addr 23.14.176.128
  
```

0000	b8 e8 56 26 b5 2c 00 27 19 d1 be 22 08 00 45 00	..V&.,. ' ..."..E.
0010	00 45 00 00 40 00 37 11 d4 76 d0 43 dc de c0 a8	.E..@.7. .v.C....
0020	01 67 00 35 d9 62 00 31 11 cc 97 30 81 80 00 01	.g.5.b.1 ...0....
0030	00 01 00 00 00 00 03 6d 69 74 03 65 64 75 00 00	.....m it.edu..
0040	01 00 01 c0 0c 00 01 00 01 00 00 00 14 00 04 17	.....
0050	0e b0 80	...

É provida apenas uma resposta, do tipo A, contendo o endereço de IP do servidor de autoridade para mit.edu.

## Usando nslookup www.aiit.or.kr bitsy.mit.edu

Aparentemente, o domínio bitsy.mit.edu encontra-se fora do ar, assim como o domínio www.aiit.or.kr. No lugar desse, usamos o domínio [www.ig.com.br](http://www.ig.com.br) e 8.8.8.8 (Servidor DNS do Google).

20. Para qual endereço IP a mensagem de requisição DNS é enviada? Este é o endereço IP de seu servidor padrão local DNS?

A mensagem de requisição é enviada para 8.8.8.8, que coincidentemente é o servidor DNS primário do meu computador. Porém, nesse caso a mensagem sempre vai ser enviada para o servidor especificado no comando.

21. Examine a mensagem de requisição DNS. Qual é o tipo mensagem de requisição DNS? A mensagem de requisição contém quais “respostas” ?

```

→ 2 5.004238 192.168.1.103 8.8.8.8 DNS 73
← 3 5.484478 8.8.8.8 192.168.1.103 DNS 187

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
▶ www.ig.com.br: type A, class IN

0000 00 27 19 d1 be 22 b8 e8 56 26 b5 2c 08 00 45 00 .'....". V&.,...E.
0010 00 3b 2e 6b 00 00 40 11 7a 28 c0 a8 01 67 08 08 .;.k..@. z(...g..
0020 08 08 ea 6d 00 35 00 27 a1 97 87 06 01 00 00 01 ...m.5.' .....
0030 00 00 00 00 00 00 03 77 77 77 02 69 67 03 63 6f .....w ww.ig.co
0040 6d 02 62 72 00 00 01 00 01 .....m.br.... .

```

A mensagem de requisição é do tipo A, e possui 0 resposta, apenas uma query.

22. Examine a mensagem DNS response. Quantas “respostas” são providas ? O que cada uma dessas mensagens contém ?

```

← 3 5.484478 8.8.8.8 192.168.1.103 DNS 187 Sta

Answer RRs: 7
Authority RRs: 0
Additional RRs: 0
▼ Queries
▶ www.ig.com.br: type A, class IN
▼ Answers
▶ www.ig.com.br: type CNAME, class IN, cname elb.ig.com.br
▶ elb.ig.com.br: type A, class IN, addr 54.174.7.148
▶ elb.ig.com.br: type A, class IN, addr 54.164.175.169
▶ elb.ig.com.br: type A, class IN, addr 54.172.65.84
▶ elb.ig.com.br: type A, class IN, addr 54.175.12.61
▶ elb.ig.com.br: type A, class IN, addr 54.164.152.127
▶ elb.ig.com.br: type A, class IN, addr 54.174.232.136

0000 b8 e8 56 26 b5 2c 00 27 19 d1 be 22 08 00 45 28 ..V&.,.' ..."..E(
0010 00 ad 23 3a 00 00 31 11 93 bf 08 08 08 08 c0 a8 ..#:..1. ....
0020 01 67 00 35 ea 6d 00 99 8f eb 87 06 81 80 00 01 .g.5.m.. ....
0030 00 07 00 00 00 00 03 77 77 77 02 69 67 03 63 6f .....w ww.ig.co
0040 6d 02 62 72 00 00 01 00 01 c0 0c 00 05 00 01 00 m.br.... ....

```

São providas 7 respostas, onde a primeira possui o endereço cujo alias [www.ig.com.br](http://www.ig.com.br) redireciona para elb.ig.com.br. As outras seis são endereços de IP disponíveis para elb.ig.com.br.