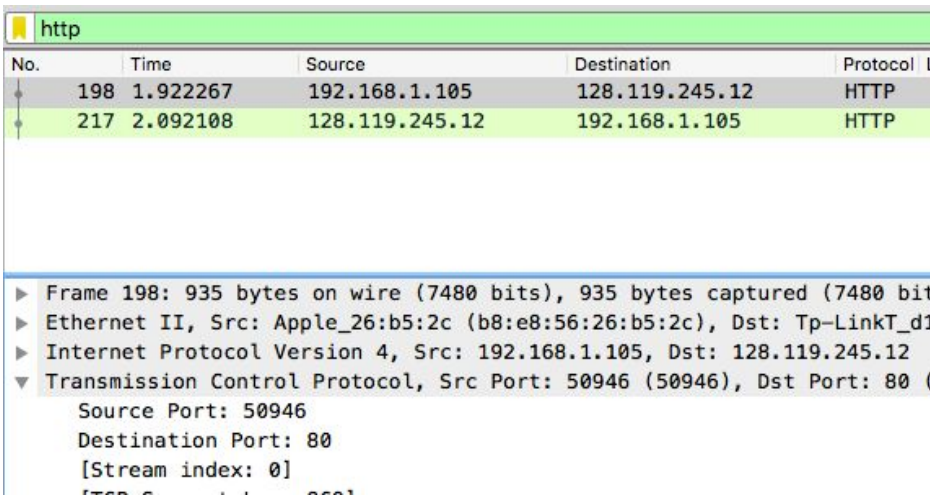
Reltaório TCP e DNS

César Henrique Bernabé
Luana Vettler Reis
Marini Favero

TCP

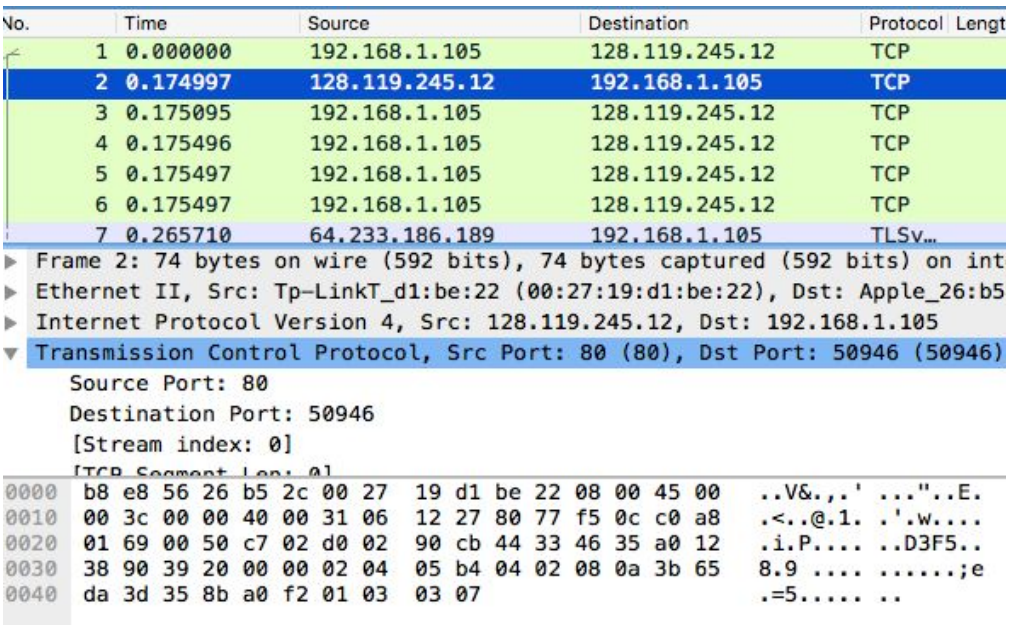
1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?



IP: 192.168.1.105

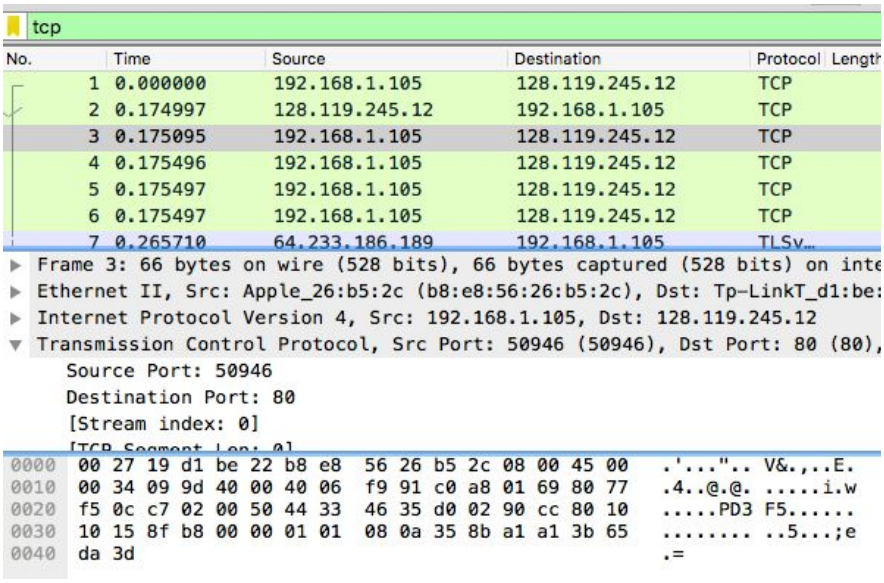
Porta Origem: 50946

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?



O computador remoto, cujo IP é 128.119.245.12 está enviando pacotes através da porta 80.

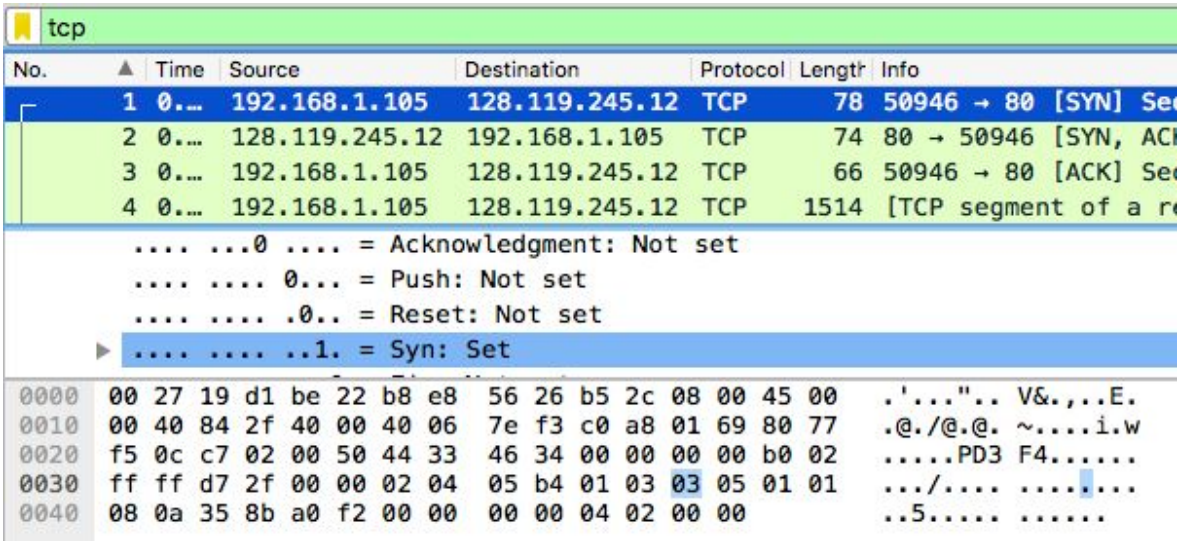
3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?



IP: 192.168.1.105

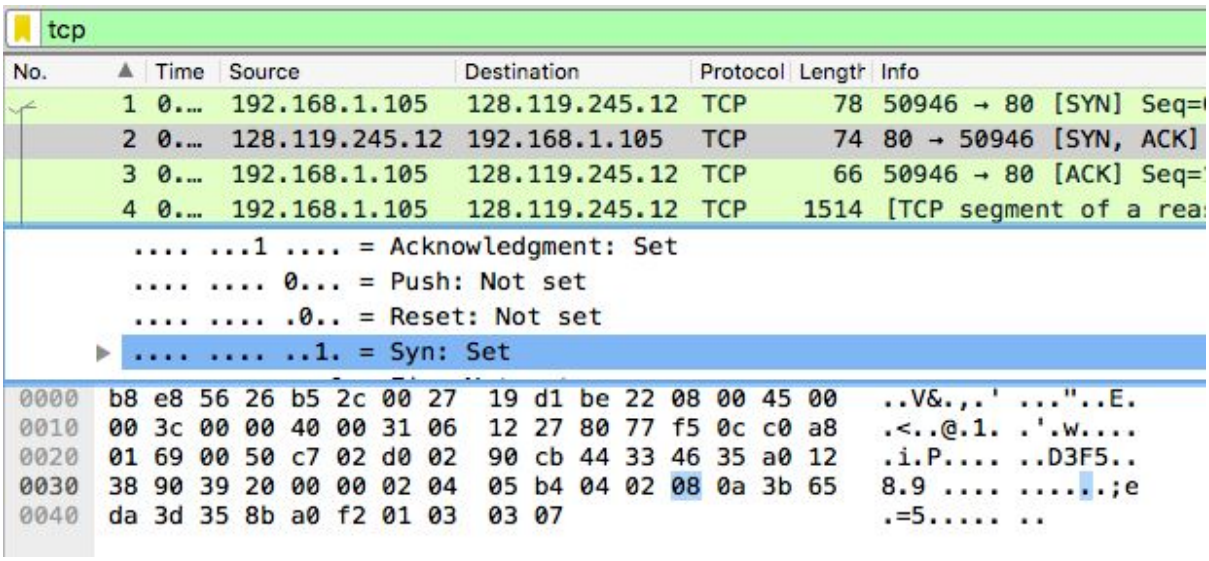
Porta: 50946

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?



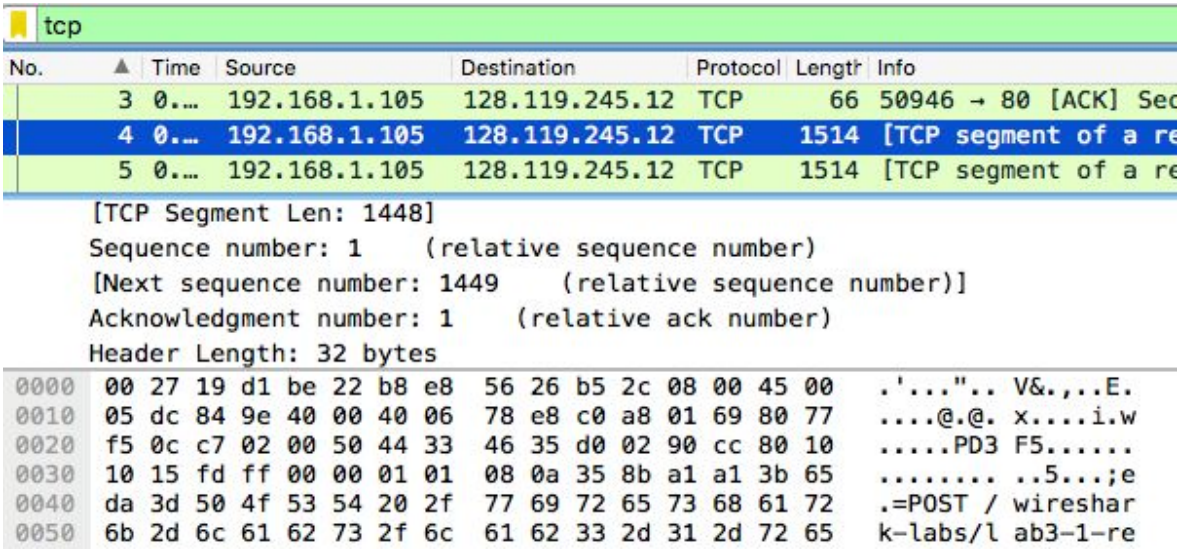
Como pode ser visto na figura acima, o Segment Number do pacote SYN usado pra iniciar a conexão com o computador cliente e gaia.cs.umass.edu é 0. Ele pode ser identificado como pacote SYN pois este é o único que possui Acknowledgement Number igual a zero, além disso possui a flag SYN ativada.

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?



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 Acknowledgement 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?

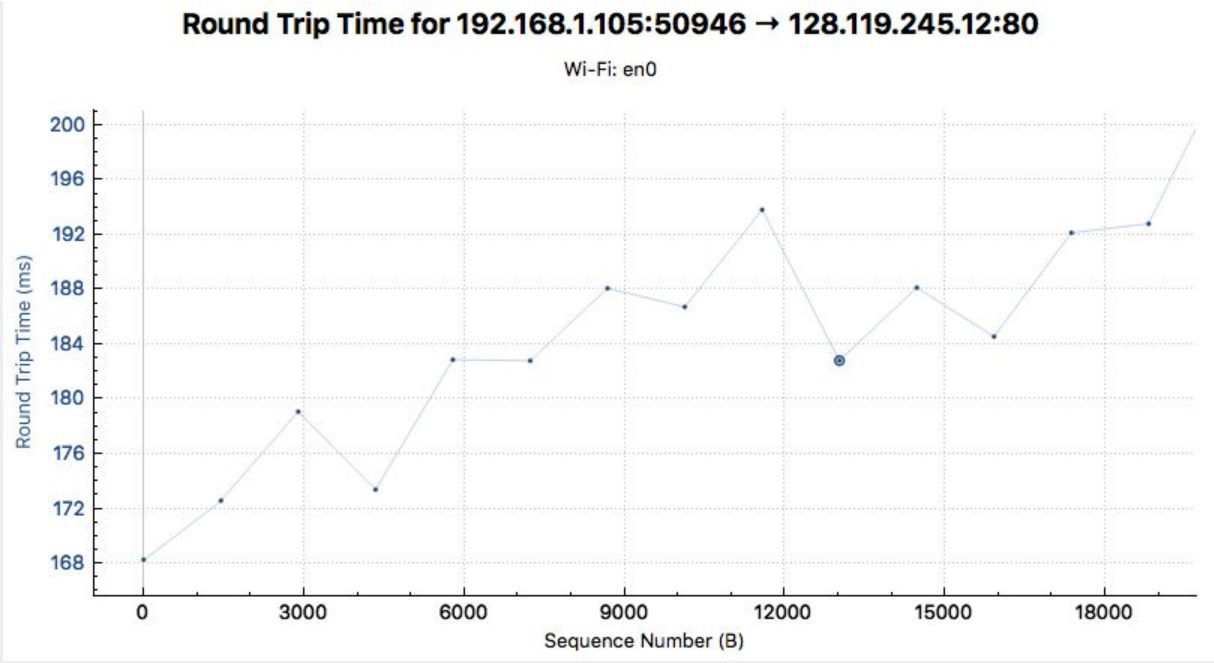


Na imagem, pode-se ver que o campo de dados do pacote possui o comando POST. Por ser o primeiro pacote enviado após o handshake, possui Sequence Number também igual a 1.

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?

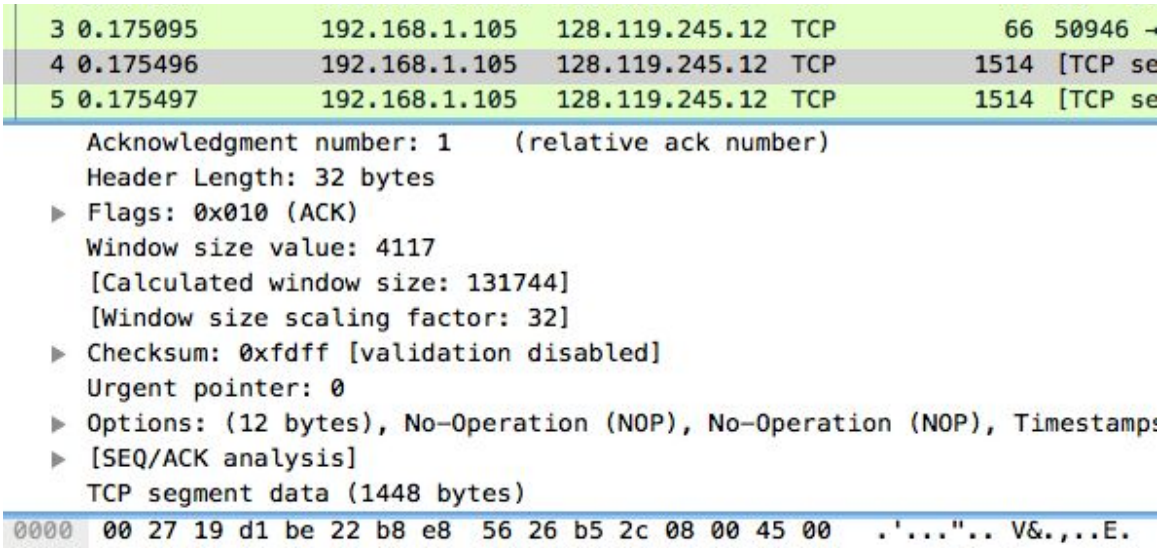
Pacote TCP	Sequence Number	Tempo Enviado	ACK Recebido (time)
1	1	0.175496	0.343723
2	1449	0.175497	0.348038
3	2897	0.175497	0.348038
4	4345	0.343837	0.354533
5	5793	0.343837	0.517179
6	7241	0.348142	0.526666

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:



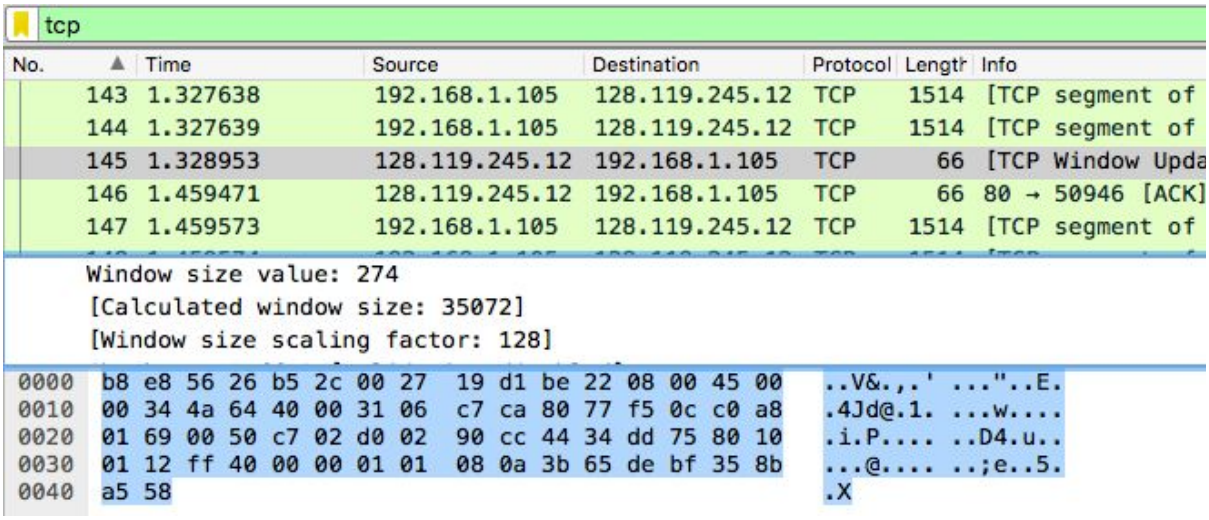
8. What is the length of each of the first six TCP segments?

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:

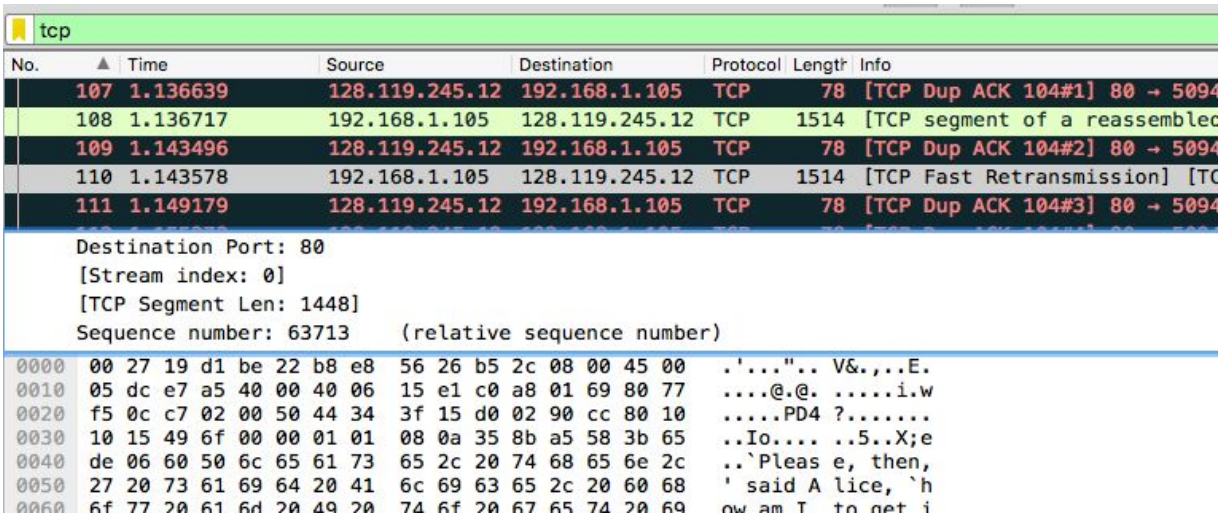


9.What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

O espaço mímino 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 diminuido 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:



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



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.

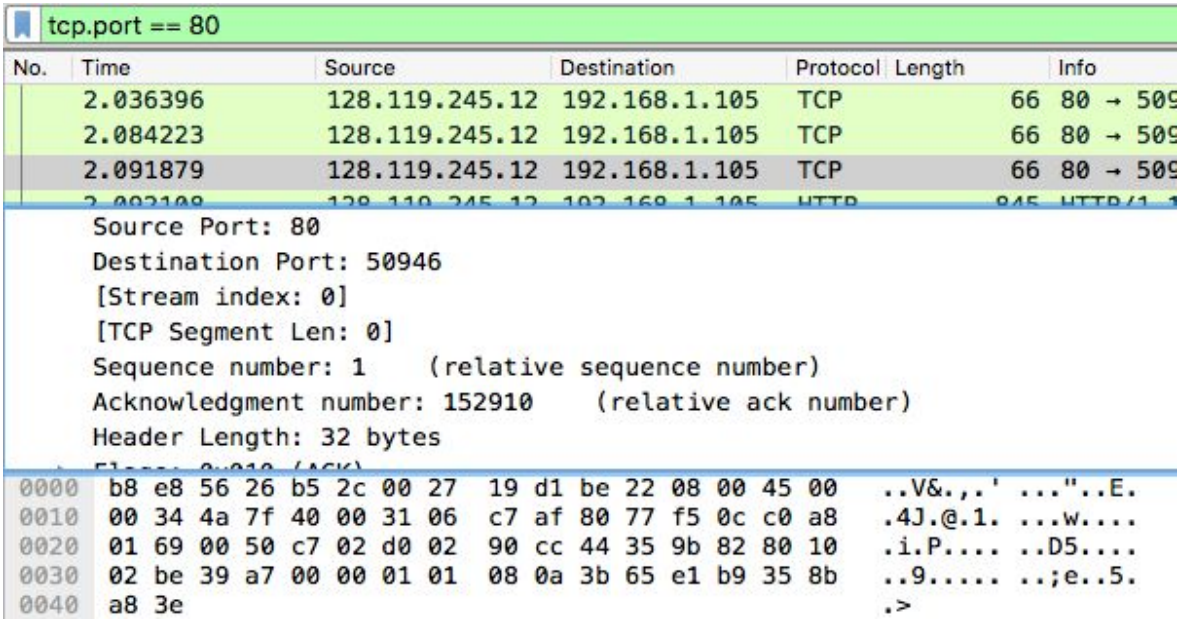
11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment.

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.



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 x 32 bytes (tamanho do header de cada pacote) = 3392 bytes.

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

Resumindo:

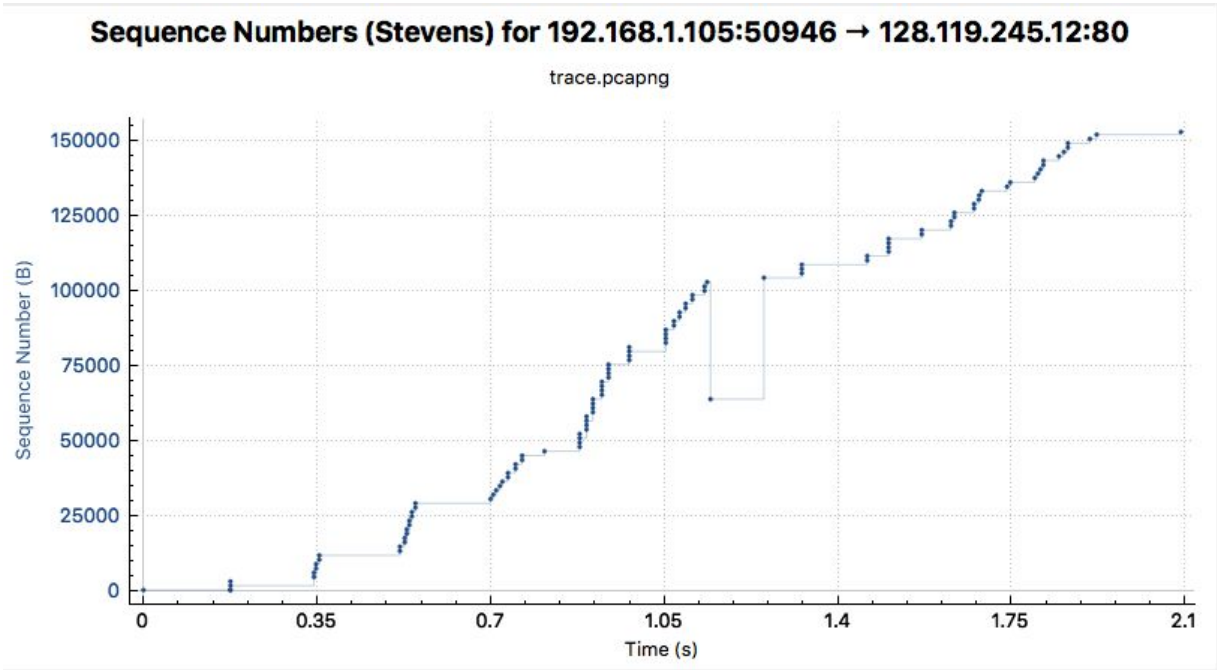
Dados Enviados Dentro do Segmento de Dados do Pacote TCP	152910 bytes
Dados de todos os Headers Enviados	3392 bytes
Pacotes ACK	132 bytes
Pacote SYN	78 bytes
TOTAL	156512

Finalmente, a vazão pode ser calculada:

V = 156512 bytes / 2.092180 (tempo em que o ultimo pacote foi recebido)

V = 74.8 bytes/segundo

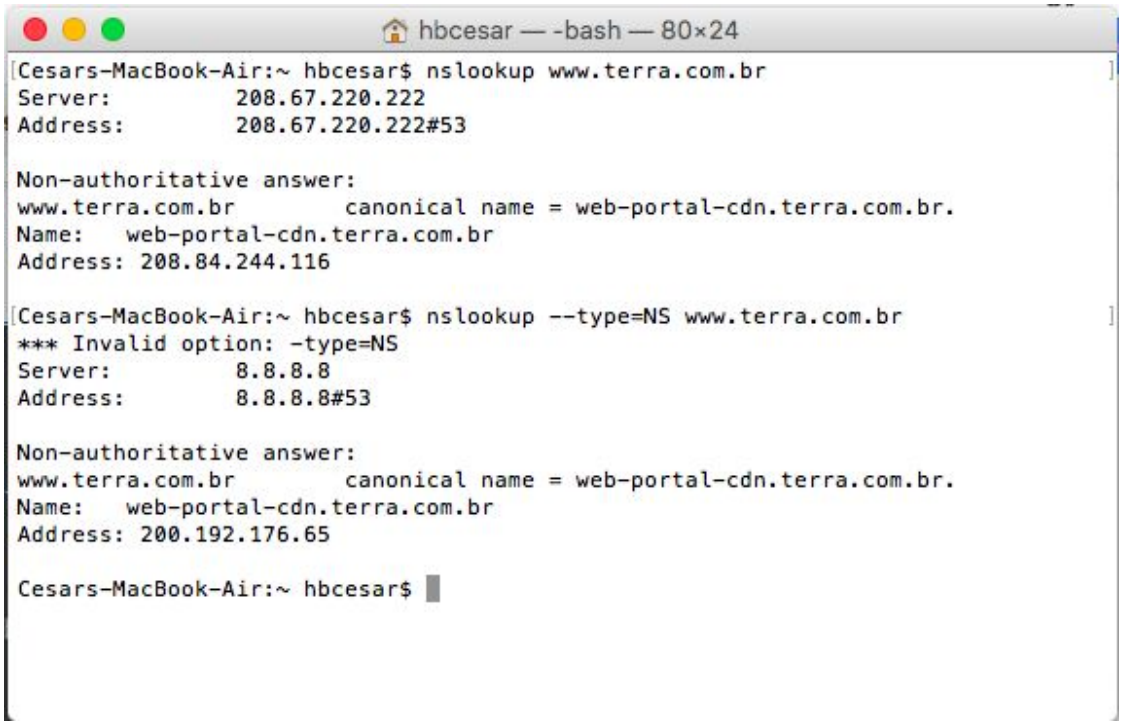
13. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which 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 metodo 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 congestione devido a um numero muito grande de pacotes enviado por unidade de tempo.

DNS



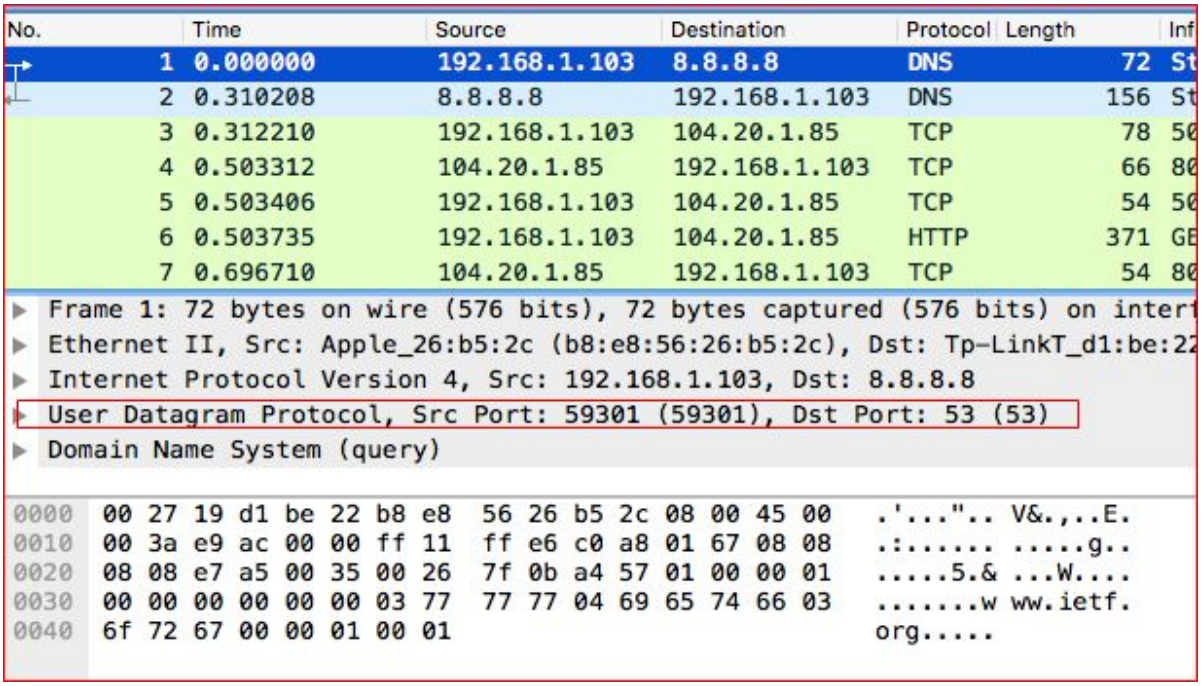
1. Execute nslookup para obter o endereço IP de um servidor Web no Brasil.

O endereço IP do servidor da pagina web www.terra.com.br é 200.137.66.240, como exibido a cima.

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?



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

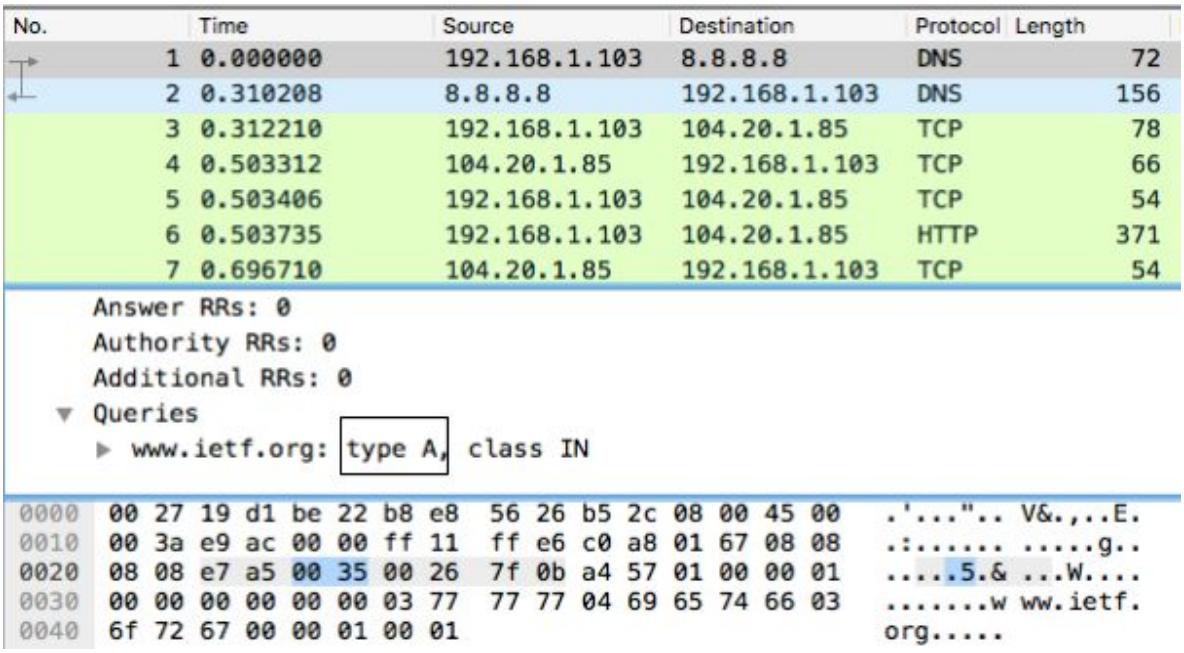
5.Qual a porta destino para a mensagem de requisição DNS? Qual é a porta fonte da mensagem DNS?

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 éa 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?

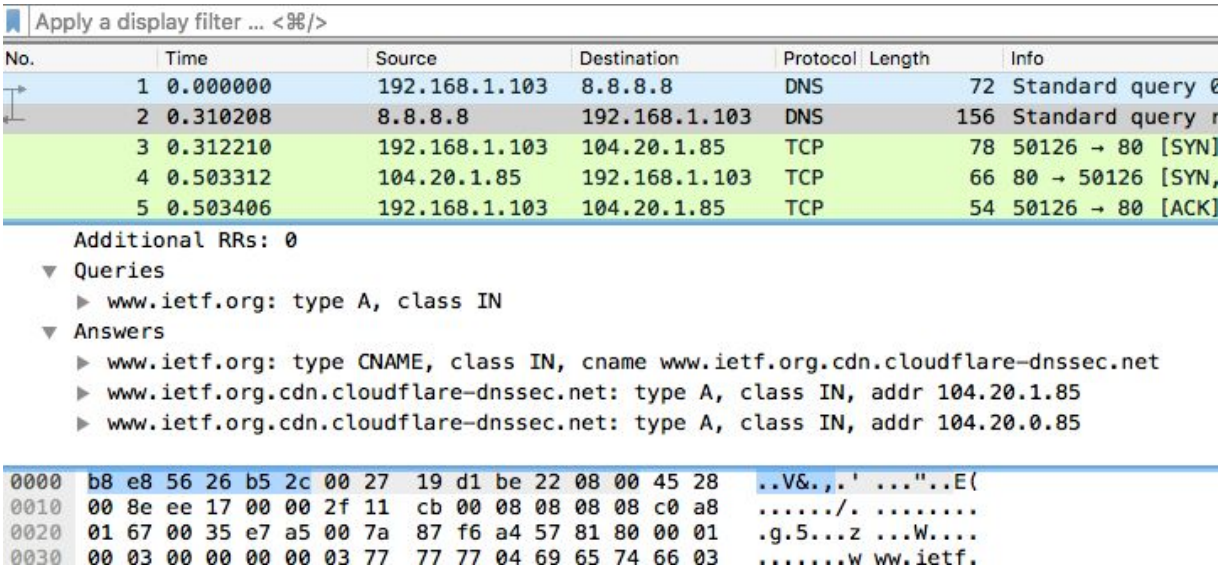
A mensagem de requisição é enviada para 8.8.8.8, que é o servidor de DNS usado pelo meu computador.

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



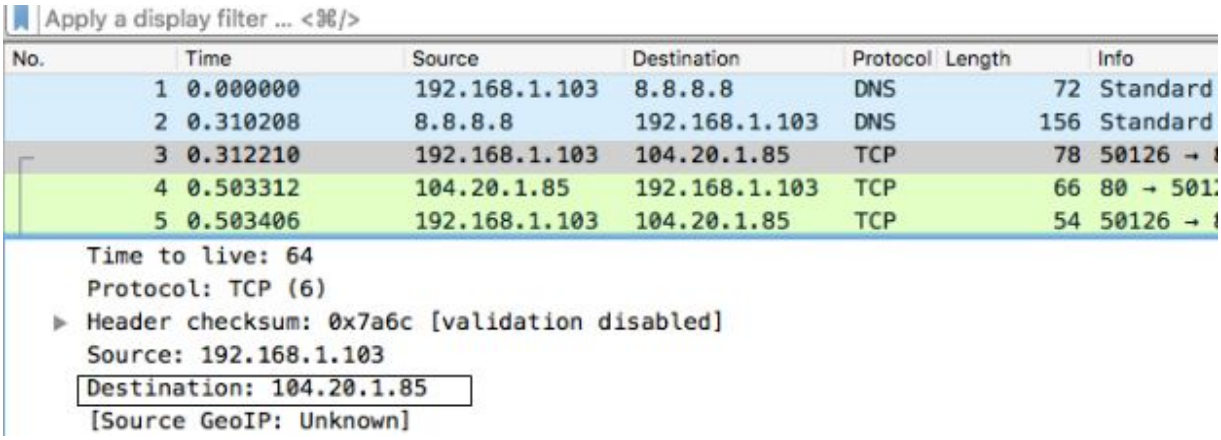
Pela figura acima, vemos que foi realizada requisição do tipo A, ou Standard Query. Esse tipo de requisição solicita o endereço IP de um domínio.

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



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 para 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?



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.

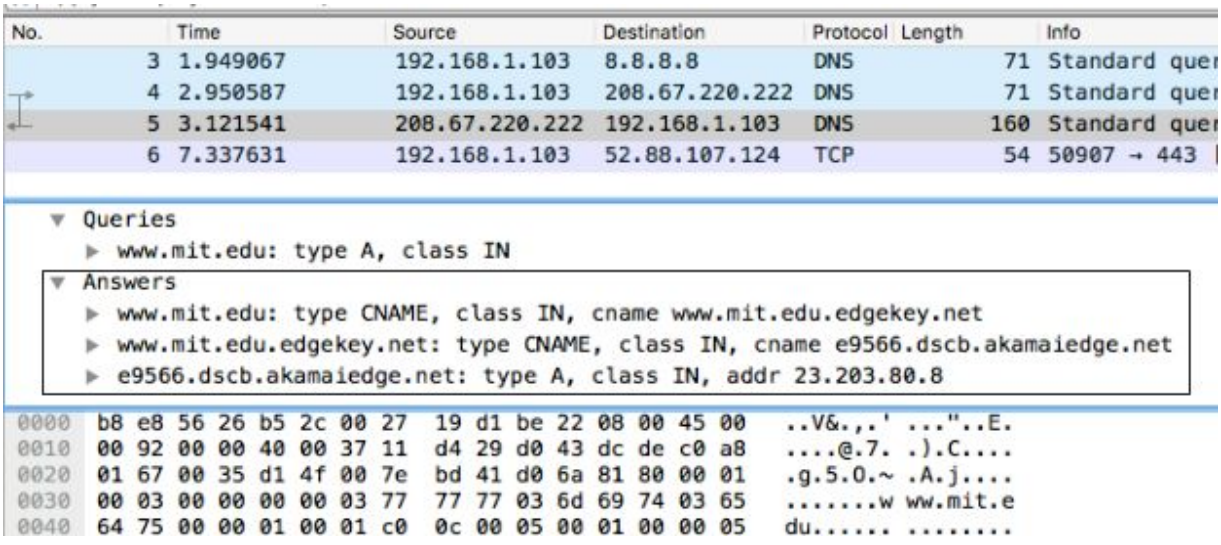
12. Para qual endereço IP a mensagem de requisição DNS é enviada? Este é o endereço IP de seu servidor padrão local DNS?

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 ?



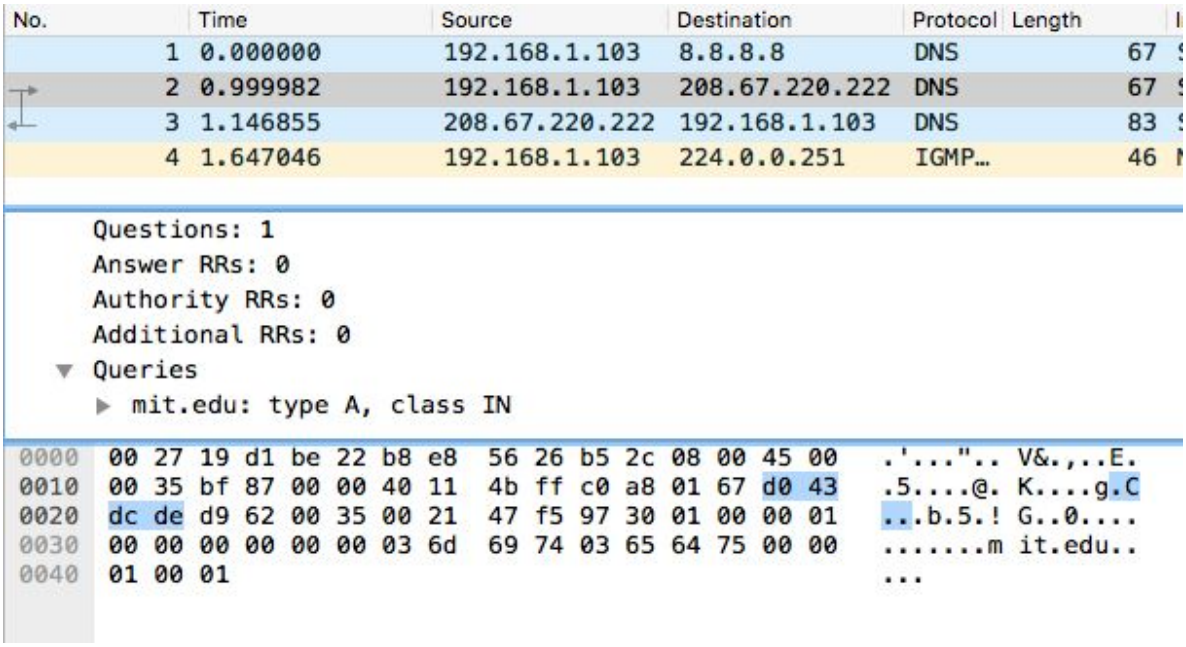
São providas três respostas, duas do tipo CNAME que redirecionam o alias www.mit.edu para www.mit.edu.edgekey.net e e9566.dscb.akamaiedge.net. A terceira resposta retorna o endereço IP do domínio fornecido pela segunda resposta do tipo CNAME: 23.203.80.8.

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?

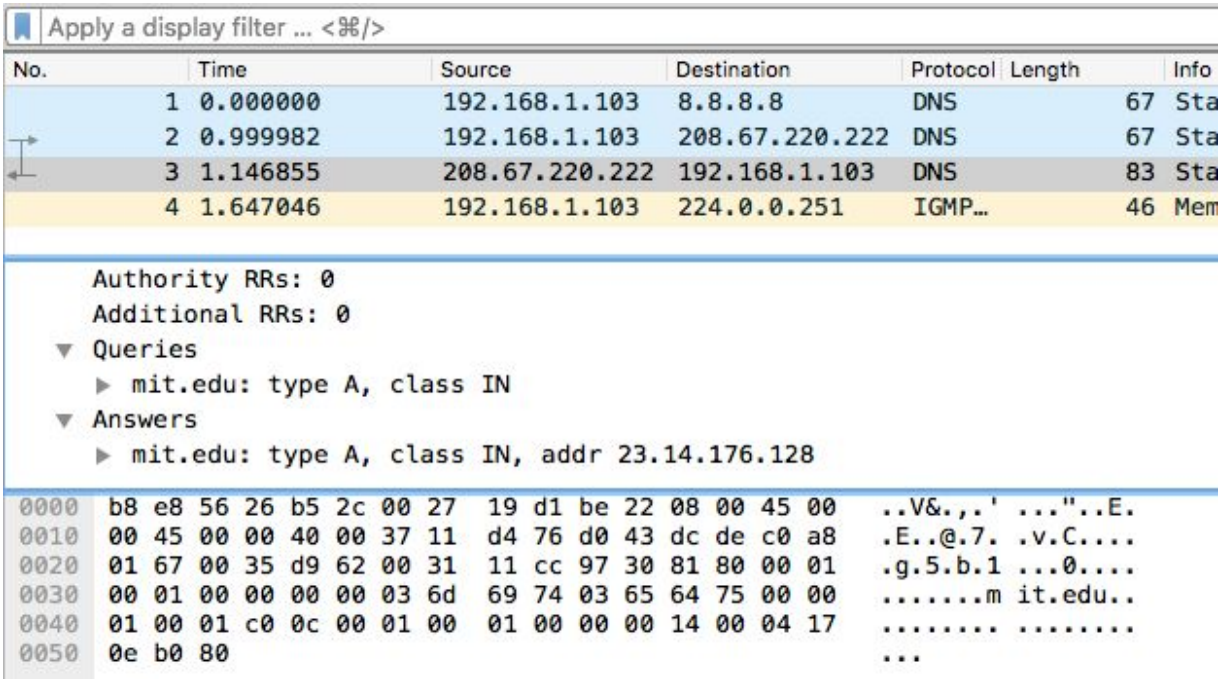
A mensagem de requisição é enviada para 208.67.220.222 que é o servidor de DNS secundário usado pelo meu computador.

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



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 ?



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

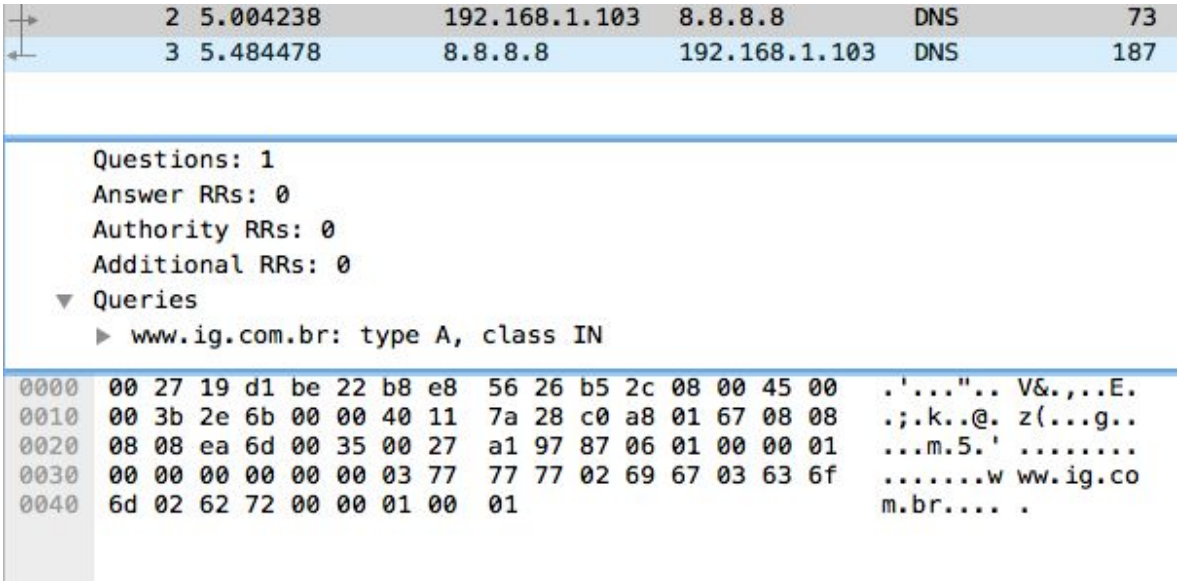
Usando nslookup www.aiit.or.kr bitsy.mit.edu

Aparentemente, o domínio bitsy.mit.edu encontra-se fora do ar, assim como o domínio www.aiit.or.kr. No lugar desse, usamos o dominio 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?

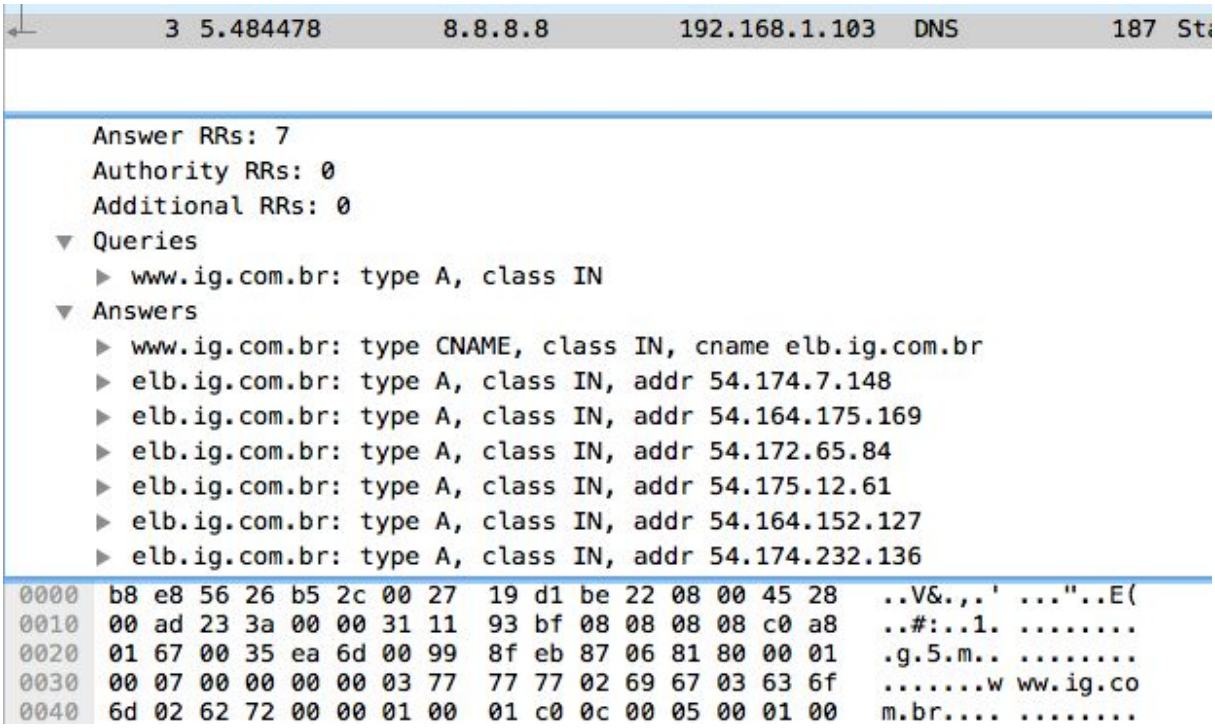
A mensagem de requisição é enviada para 8.8.8.8, que coincidentemente é o servidor DNS primário do meu computador. Porém, nesse caso a mensagem sempre vai ser enviada para o servidor especificado no comando.

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



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 ?



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