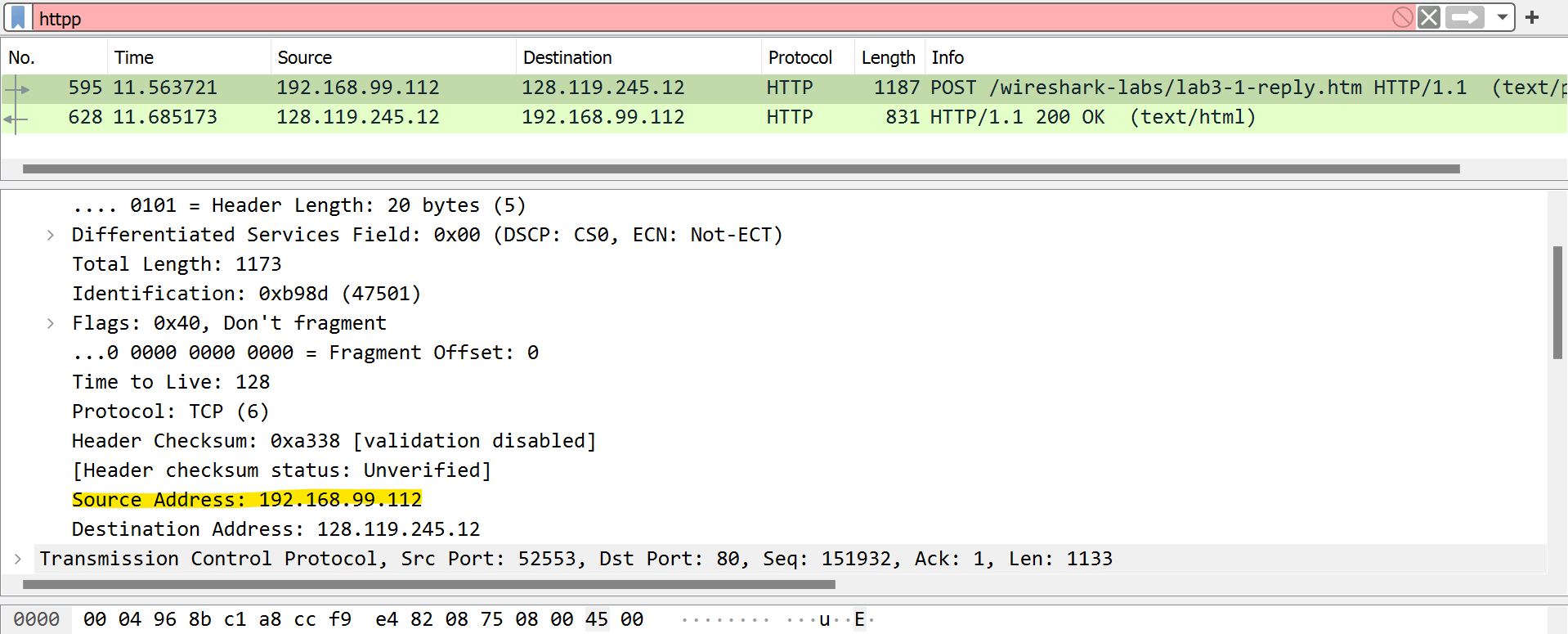
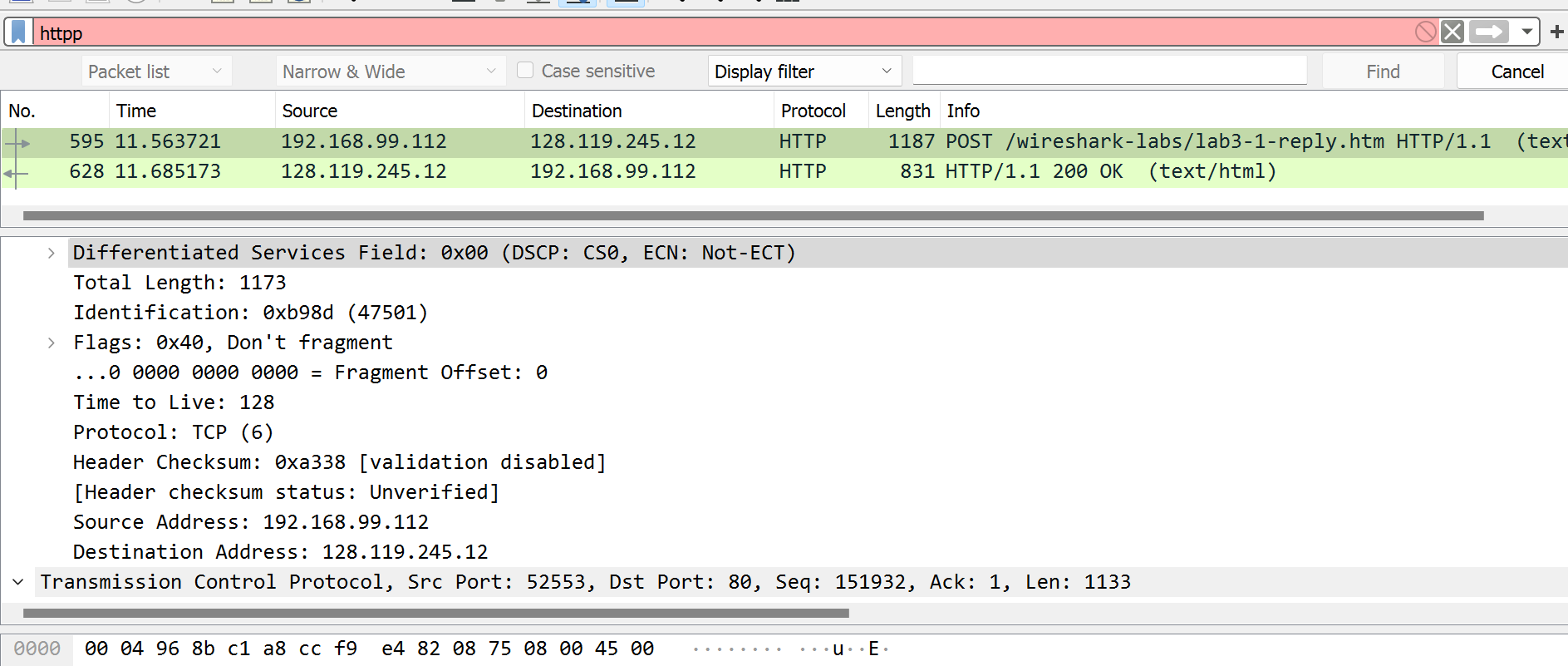
**1 - Qual é o endereço IP e o número da porta TCP usados pelo computador cliente (origem) que está transferindo o arquivo alice.txt para gaia.cs.umass.edu? Para responder a essa pergunta, provavelmente é mais fácil selecionar uma mensagem HTTP e explorar os detalhes do pacote TCP usado para transportar essa mensagem HTTP, usando os “detalhes da janela de cabeçalho do pacote selecionado” (consulte a Figura 2 em “Introdução à Wireshark” Lab se você não tiver certeza sobre as janelas do Wireshark).**

Endereço IP do cliente:



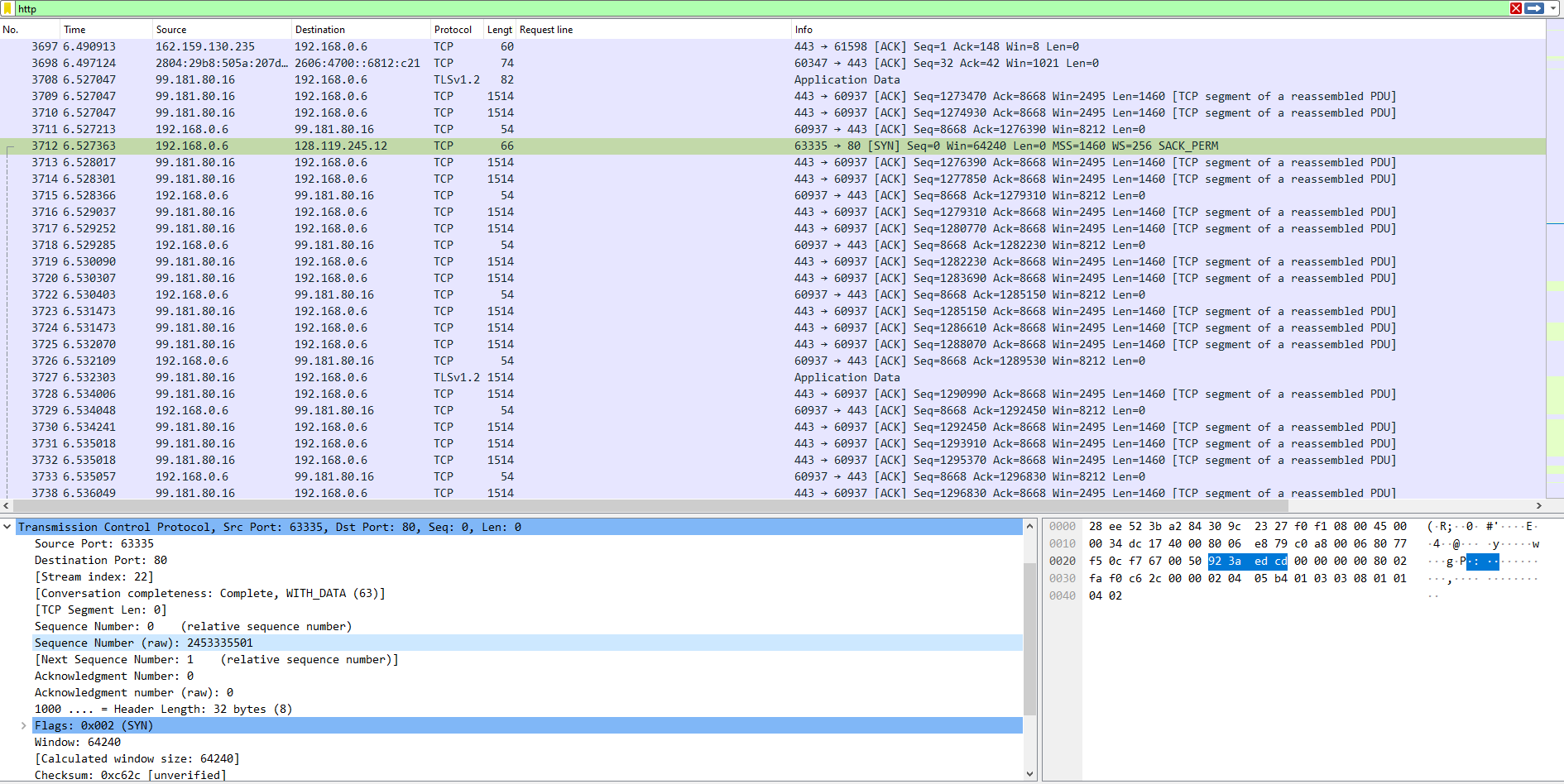
Porta: 80

**2 - Qual é o endereço IP de gaia.cs.umass.edu? Em qual número de porta ele está enviando e recebendo segmentos TCP para esta conexão?**



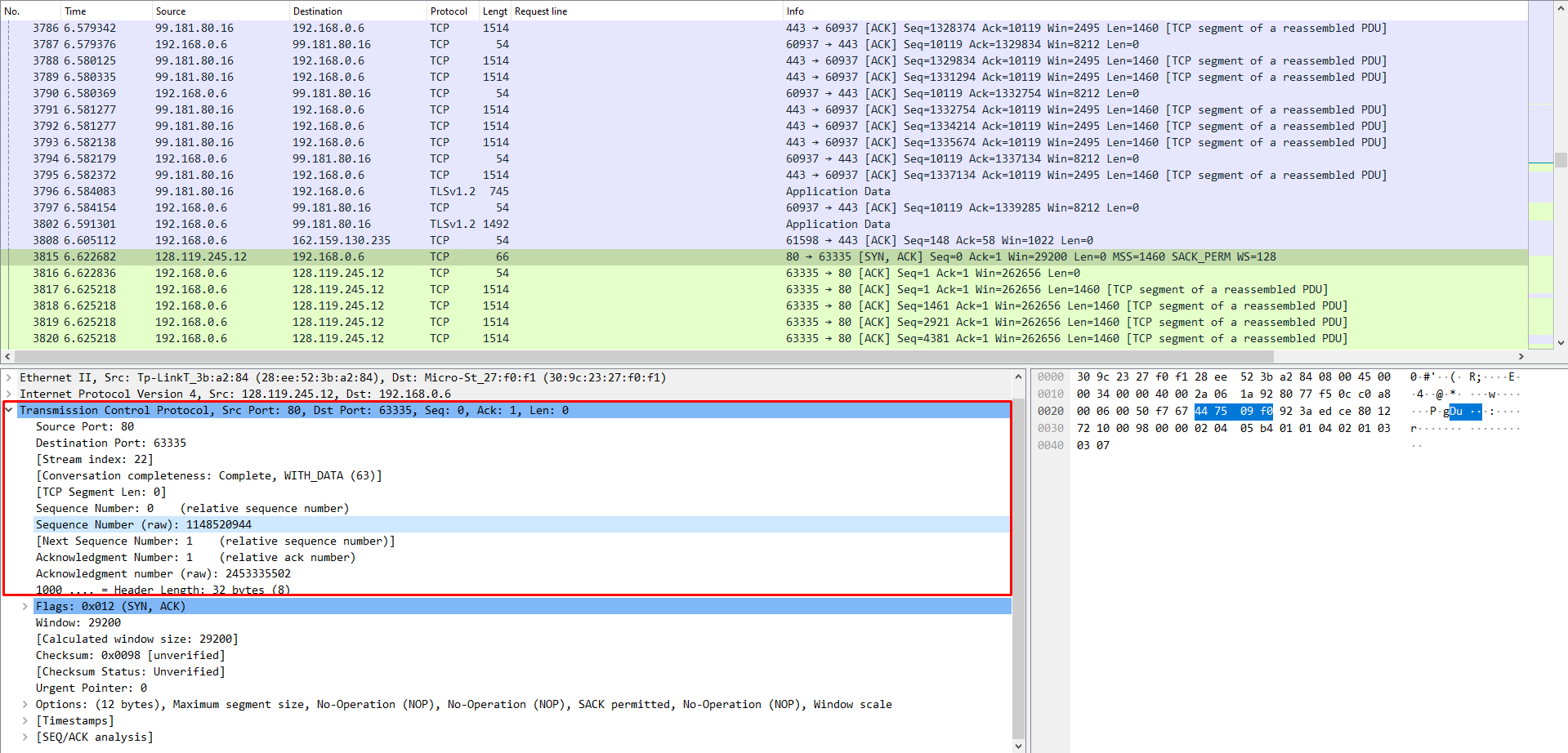
Porta: 80, IP do gaia: 128.119.245.12

**3 - Qual é o número de sequência do segmento TCP SYN que é usado para iniciar a conexão TCP entre o computador cliente e o gaia.cs.umass.edu? (Nota: este é o número de sequência “bruto” carregado no próprio segmento TCP; NÃO é o pacote # na coluna “Não.” na janela Wireshark. Lembre-se de que não existe um “número de pacote” no TCP ou UDP; como você sabe, existem números de seqüência no TCP e é isso que estamos procurando aqui. Observe também que este não é o número de seqüência relativo em relação ao número de seqüência inicial desta sessão TCP.). O que há neste segmento TCP que identifica o segmento como um segmento SYN?**



Sequência: 0, identificamos que é um segmento SYN através do cabeçalho.

**4 - Qual é o número de sequência do segmento SYNACK enviado por gaia.cs.umass.edu ao computador cliente em resposta ao SYN? O que há no segmento que identifica o segmento como um segmento SYNACK? Qual é o valor do campo Acknowledgement no segmento SYNACK? Como gaia.cs.umass.edu determinou esse valor?**

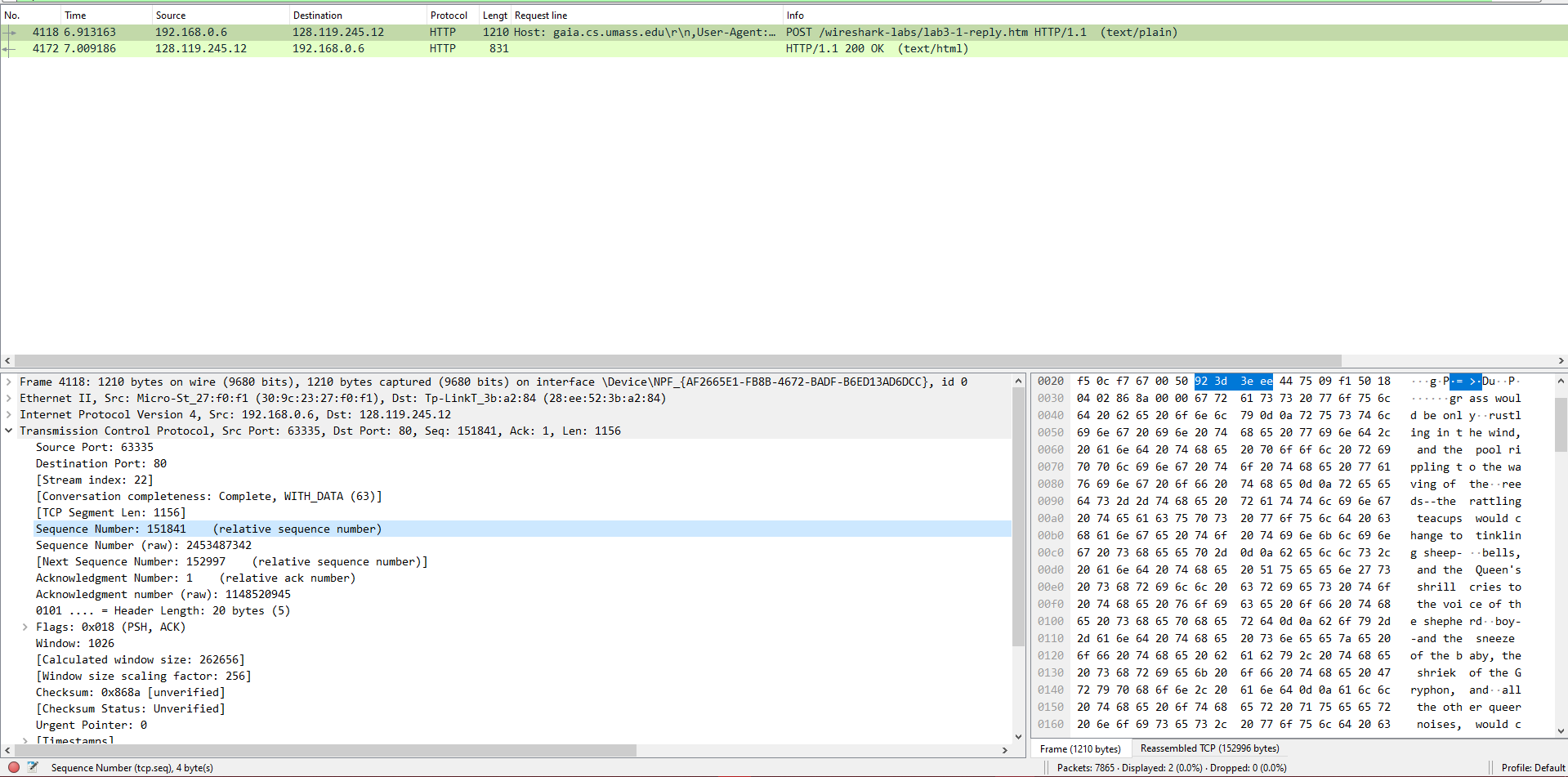


Número de sequência do segmento SYNACK é 0, raw(1148520944);

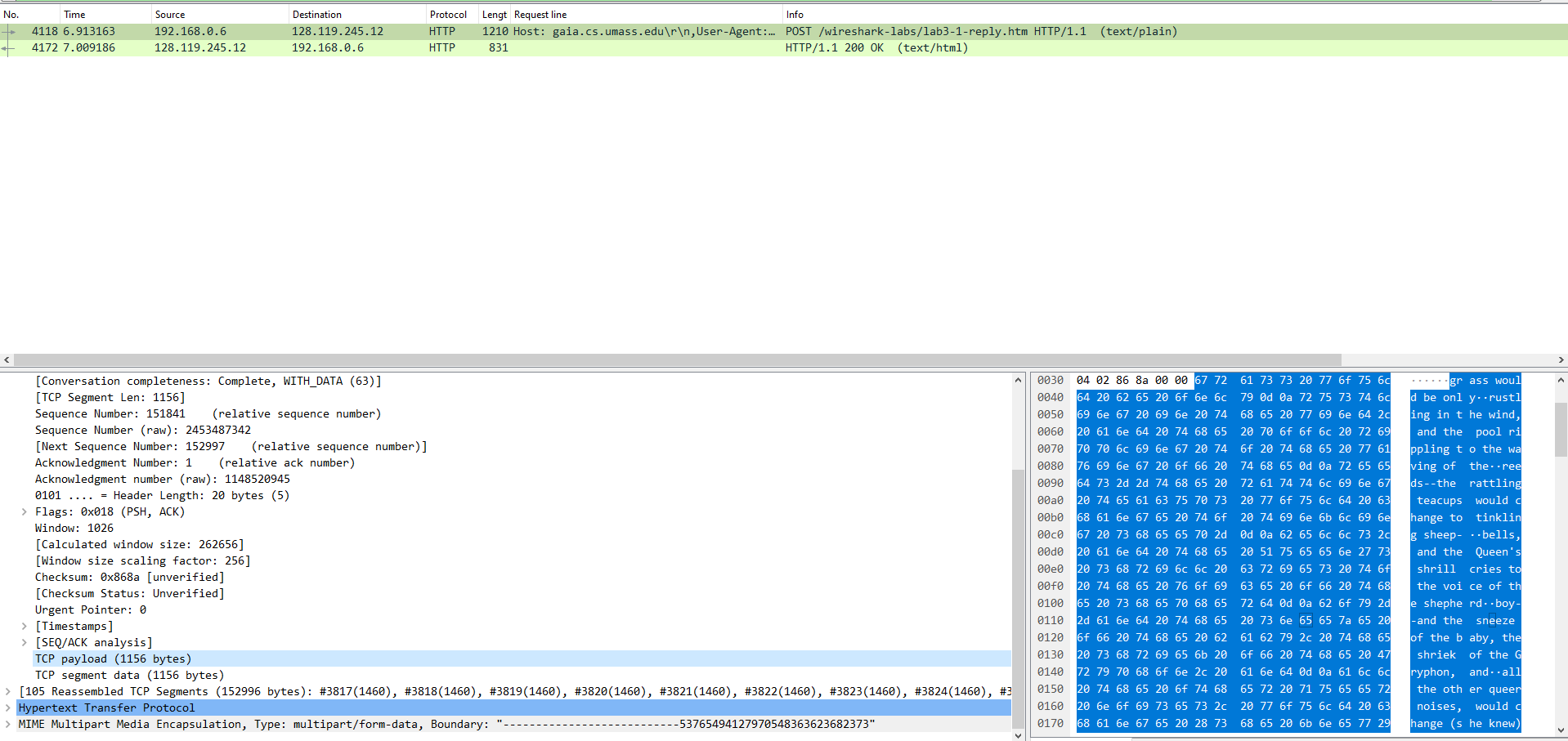
Identificamos o segmento através do cabeçalho com a presença do SYNACK;

Acknowledgement é igual a 1, raw(2453335502);

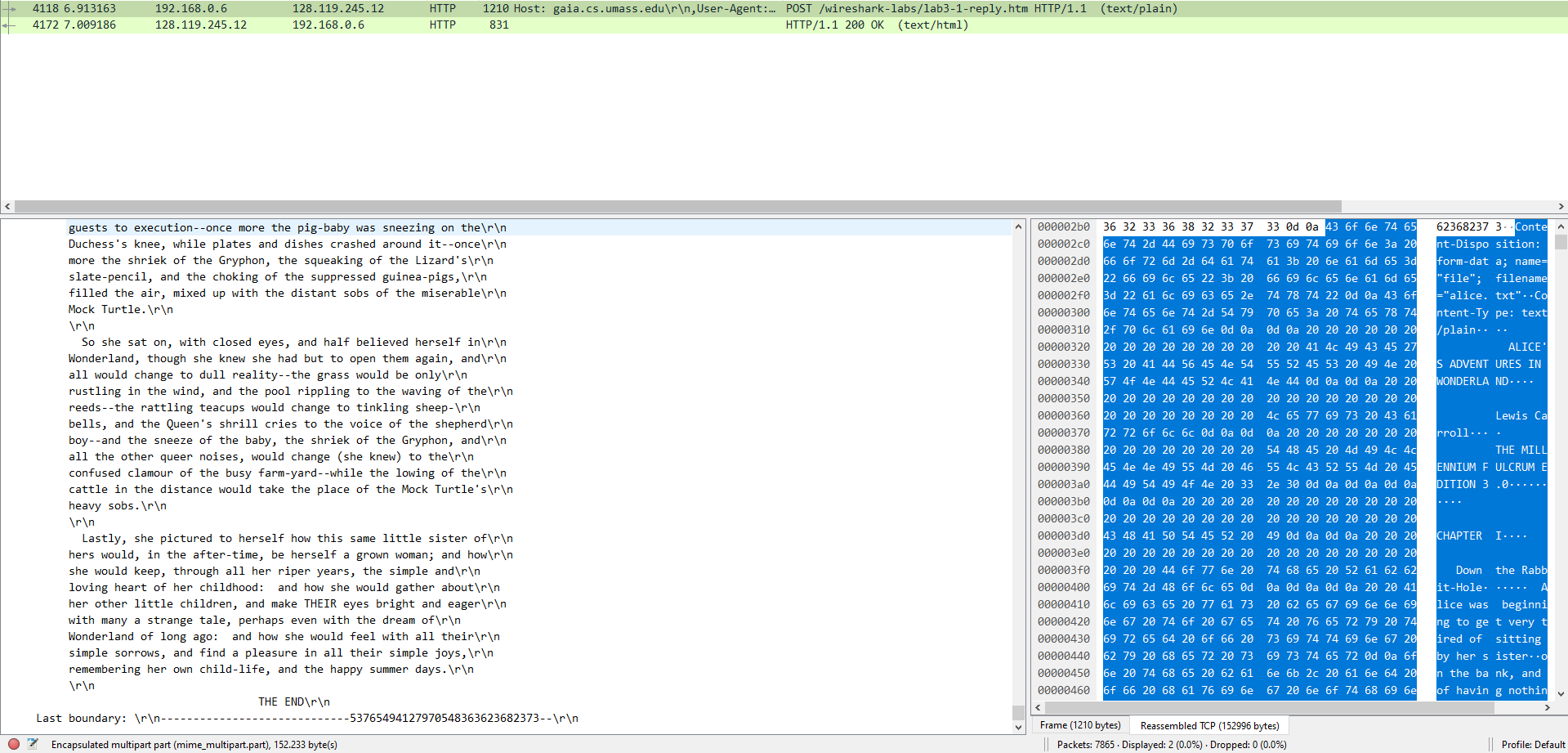
**5 - Qual é o número de sequência do segmento TCP que contém o cabeçalho do comando HTTP POST? Observe que, para encontrar o cabeçalho da mensagem POST, você precisará cavar o campo de conteúdo do pacote na parte inferior da janela do Wireshark, procurando um segmento com o texto ASCII “POST” dentro do campo DATA 2 3. Quantos bytes de dados estão contidos no campo de carga útil (dados) deste segmento TCP? Todos os dados no arquivo transferido alice.txt se encaixam nesse único segmento?**



Número de sequência: 151841,



Total de bytes: 1156.

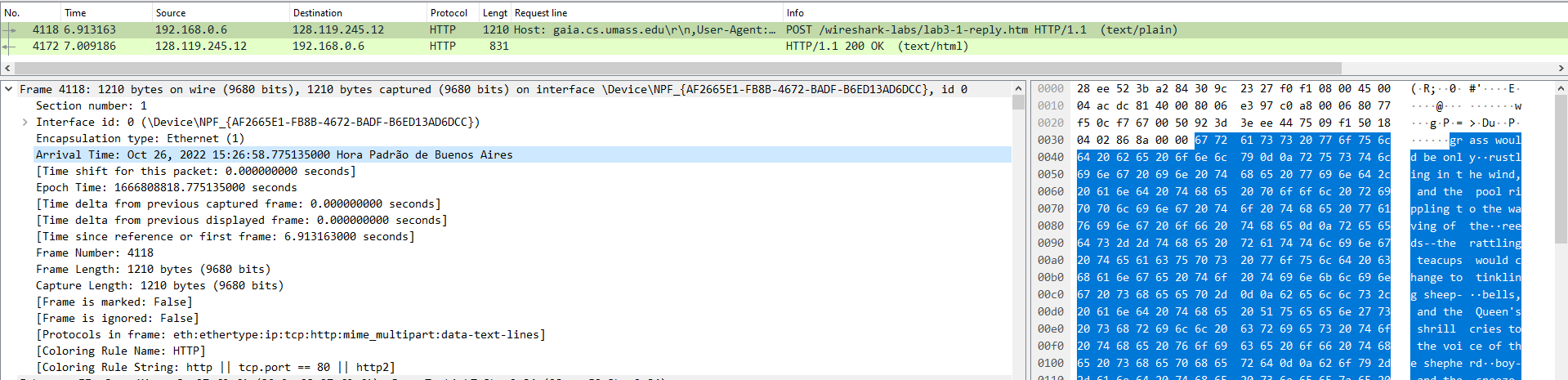


Sim, todos os dados do arquivo se encaixam em um único segmento.

**6 - Considere o segmento TCP contendo o HTTP “POST” como o primeiro segmento na parte de transferência de dados da conexão TCP.**

**Em que momento foi enviado o primeiro segmento (aquele que contém o HTTP POST) na parte de transferência de dados da conexão TCP?**

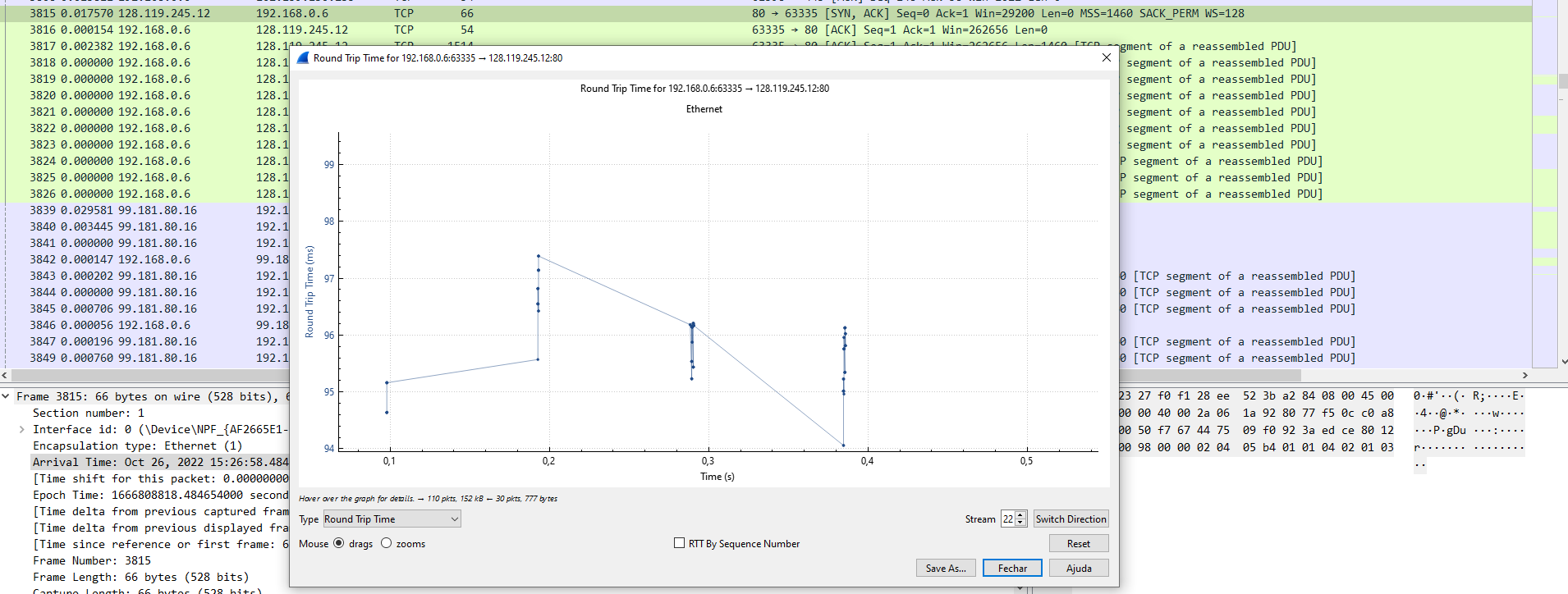
**A que horas foi recebido o ACK para este primeiro segmento contendo dados?**



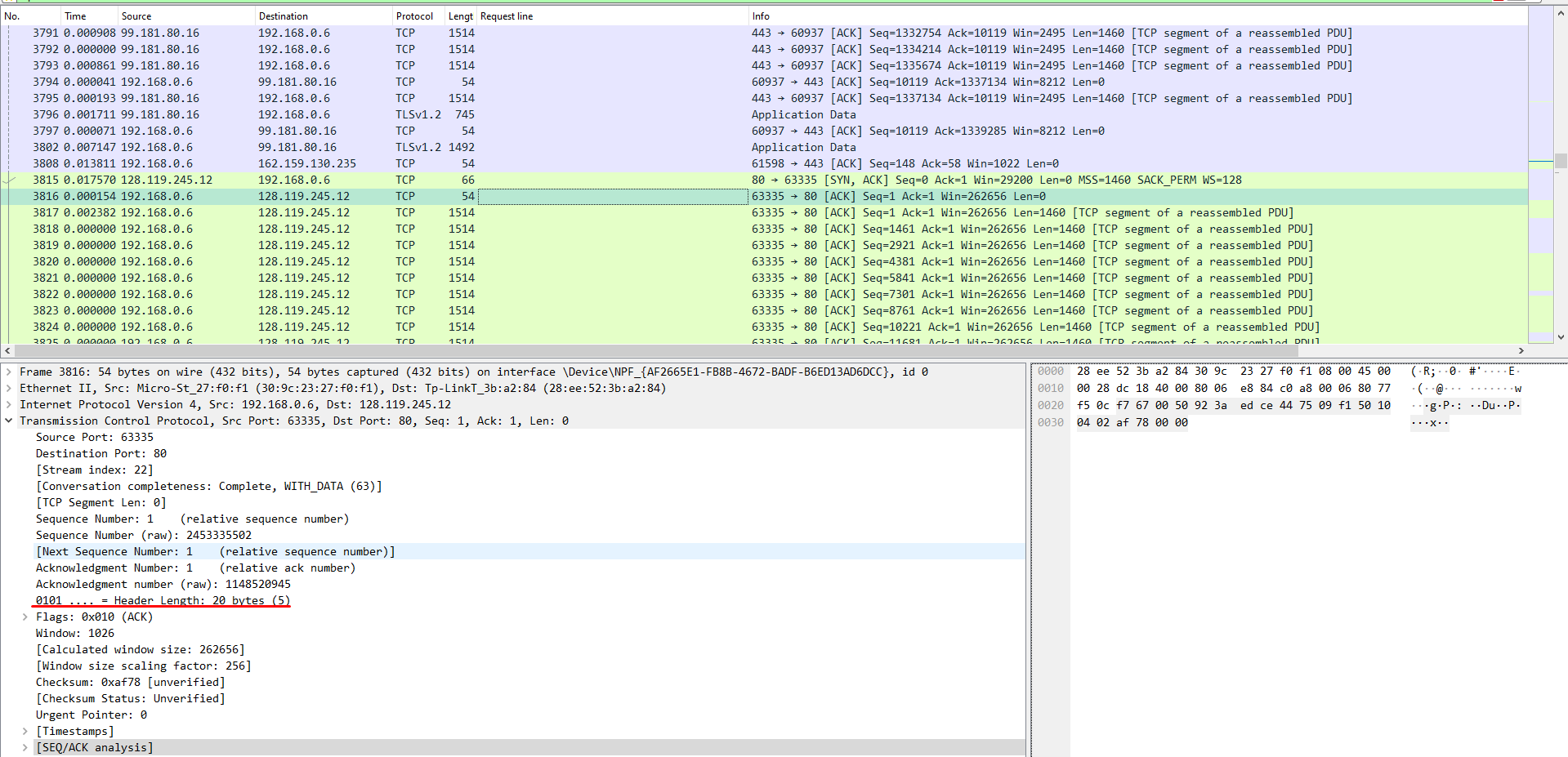
26 de outubro de 2022, 15:26

Qual é o RTT para este primeiro segmento contendo dados?

Qual é o valor RTT do segundo segmento TCP que transporta dados e seu ACK? Nota: O Wireshark tem um bom recurso que permite plotar o RTT para cada um dos segmentos TCP enviados. Selecione um segmento TCP na janela "lista de pacotes capturados" que está sendo enviado do cliente para o servidor gaia.cs.umass.edu. Em seguida, selecione: Estatísticas->Gráfico de fluxo TCP->Gráfico de tempo de viagem de ida e volta.



**7 - Qual é o comprimento (cabeçalho mais carga útil) de cada um dos quatro primeiros segmentos TCP de transporte de dados?**

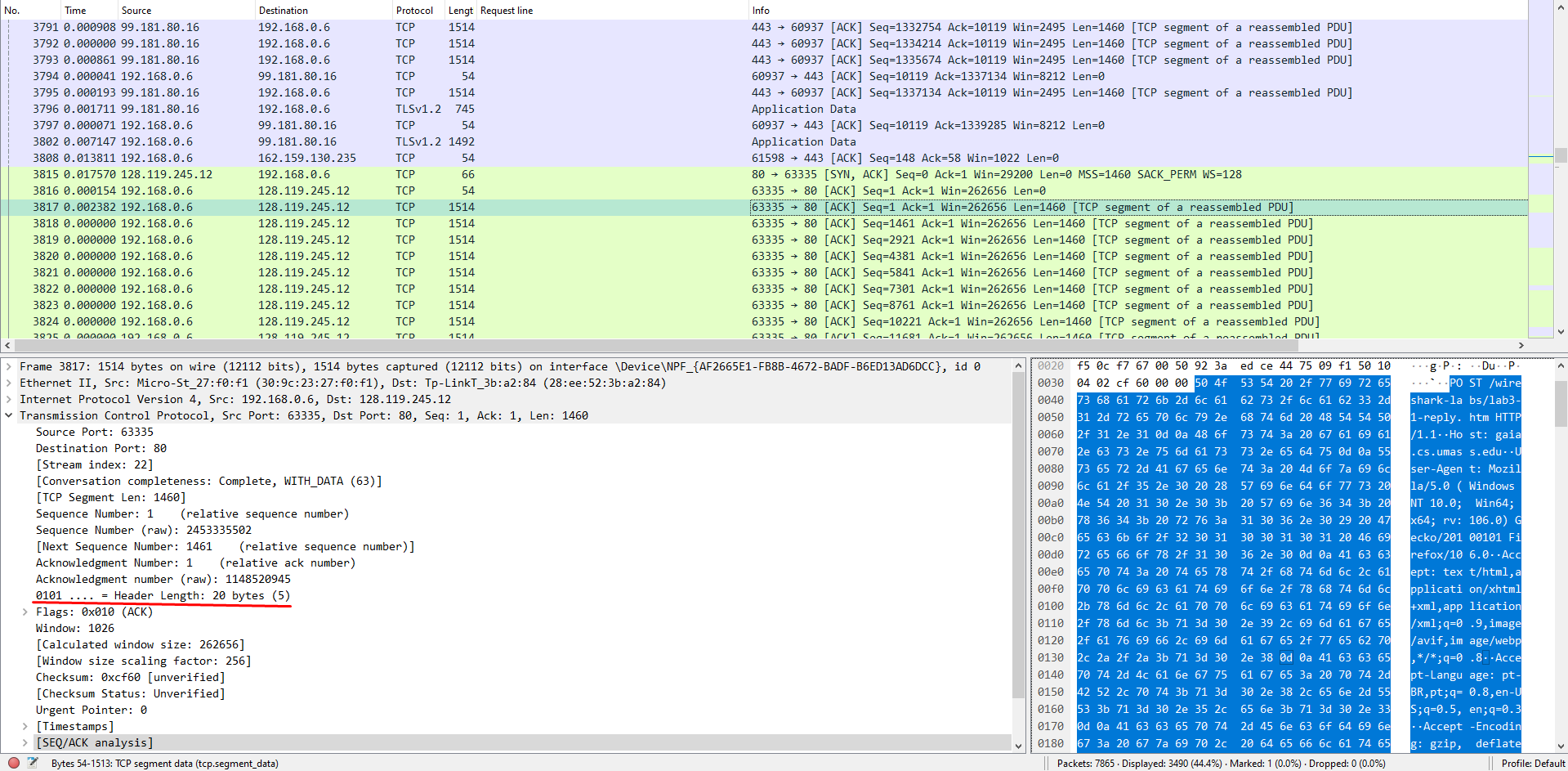
****

TCP segment data: 0

Lenght: 60

Header Lenght: 20

Carga útil = 20

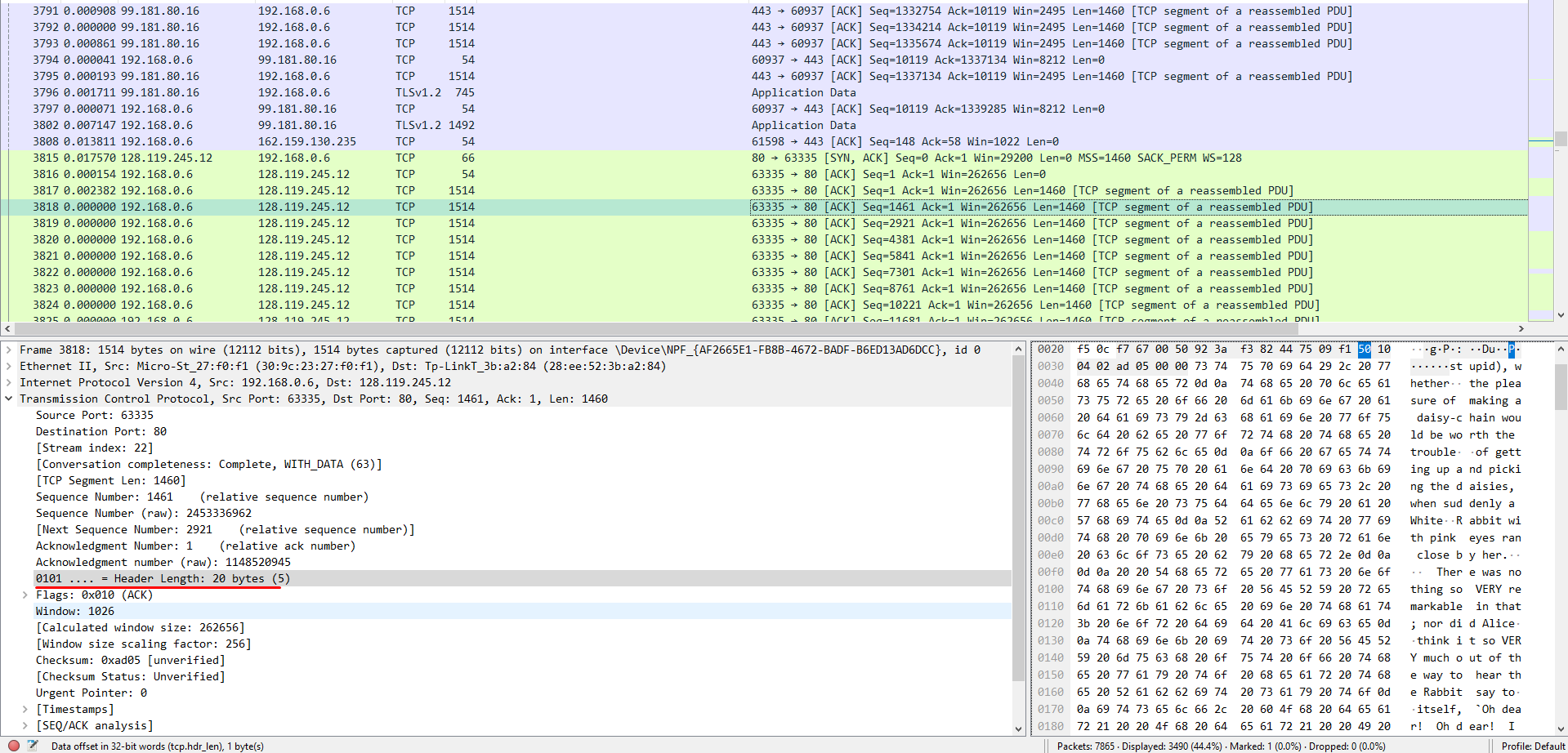


TCP segment data: 1460

Lenght: 1514

Header Lenght: 20

Carga útil = 1480

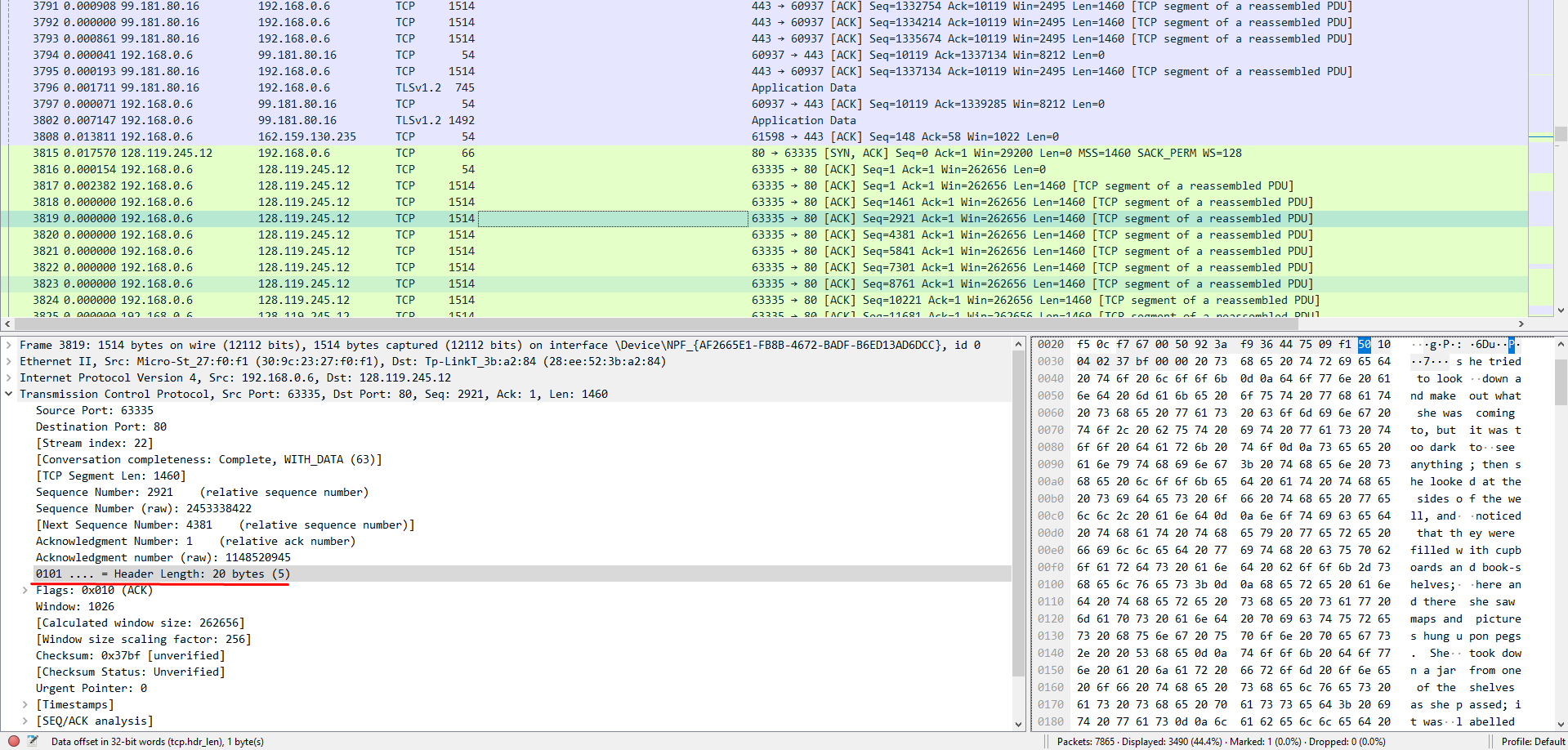


TCP segment data: 1460

Lenght: 1514

Header Lenght: 20

Carga útil = 1480



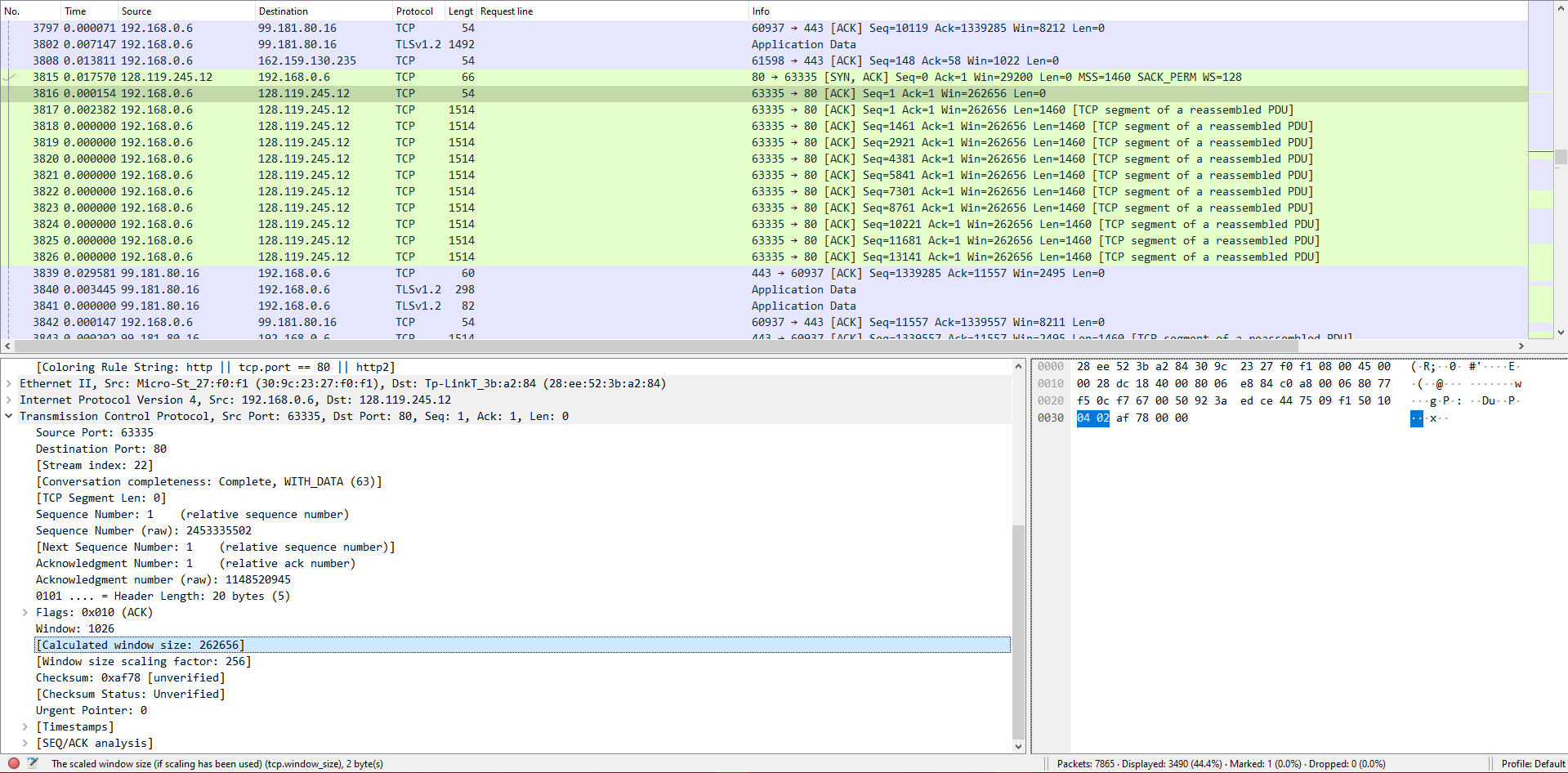
TCP segment data: 1460

Lenght: 1514

Header Lenght: 20

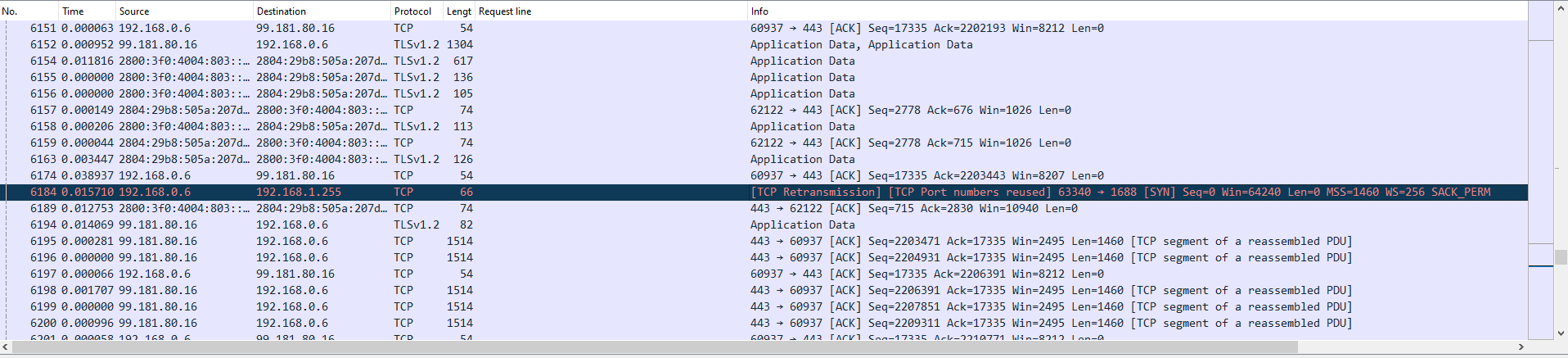
Carga útil = 1480

**8 - Qual é a quantidade mínima de espaço de buffer disponível anunciado ao cliente por gaia.cs.umass.edu entre esses quatro primeiros segmentos TCP de transporte de dados? A falta de espaço no buffer do receptor estrangula o remetente para esses quatro primeiros segmentos de transporte de dados?**

****

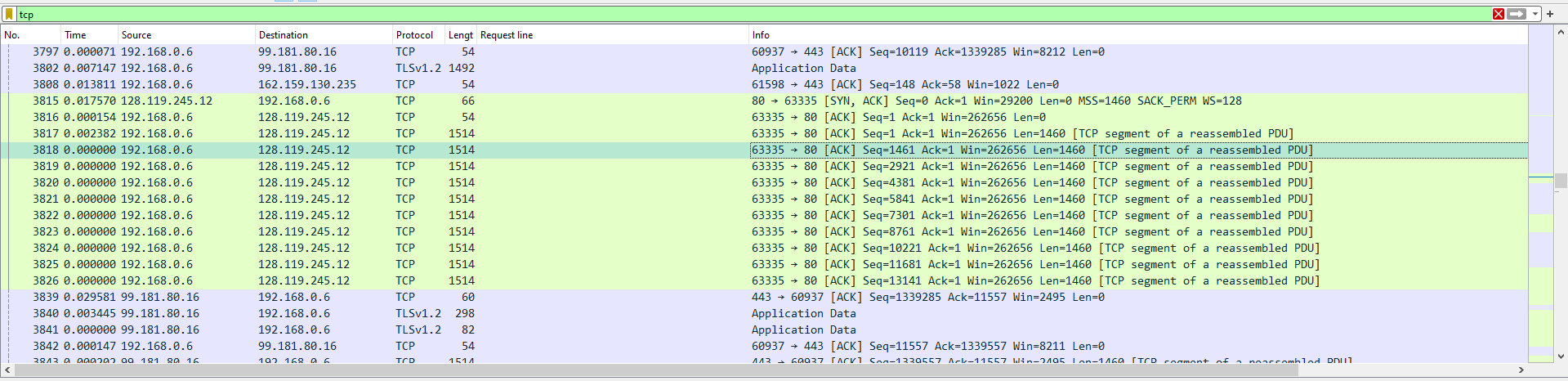
O primeiro ACK do servidor indica a quantidade mínima do buffer, então temos o valor de 262656.

**9 - Existem segmentos retransmitidos no arquivo de rastreamento? O que você verificou (no rastreamento) para responder a essa pergunta?**



Não, pois não foram encontrados pacotes de retransmissão (como o demonstrado acima) na comunicação com o gaia.

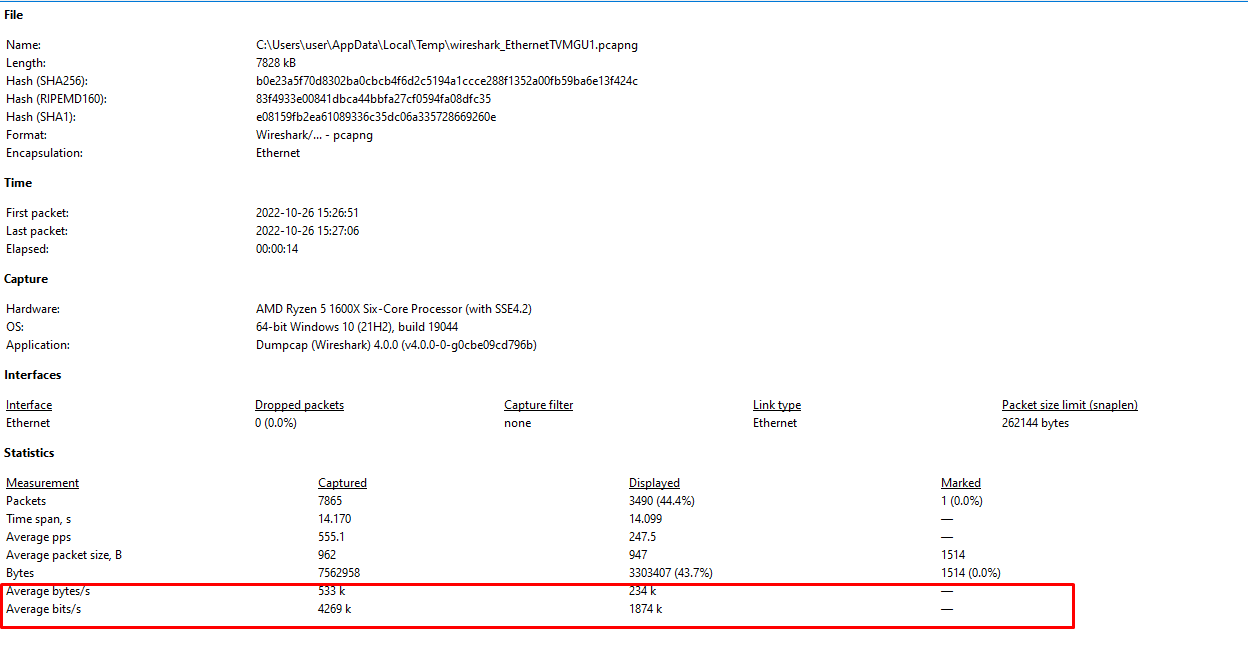
**10 - Quantos dados o receptor normalmente reconhece em um ACK entre os dez primeiros segmentos de transporte de dados enviados do cliente para gaia.cs.umass.edu? Você pode identificar casos em que o receptor é ACK em todos os outros segmentos recebidos entre esses dez primeiros segmentos de transporte de dados?**



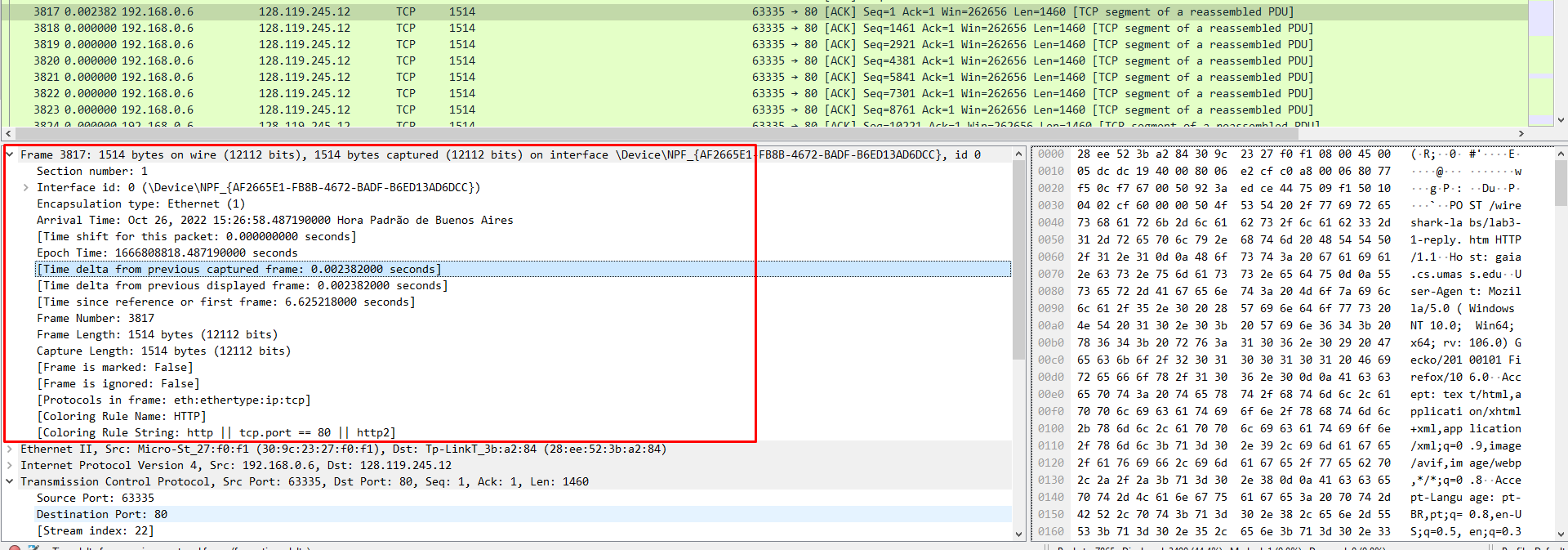
O servidor recebe 1460 bytes de um pacote para outro, pois quando subtraímos o número de sequência de um pacote X com o seu pacote TCP posterior, temos uma diferença de 1460 entre os números de sequência.

**11 - Qual é a taxa de transferência (bytes transferidos por unidade de tempo) para a conexão TCP? Explique como você calculou esse valor.**

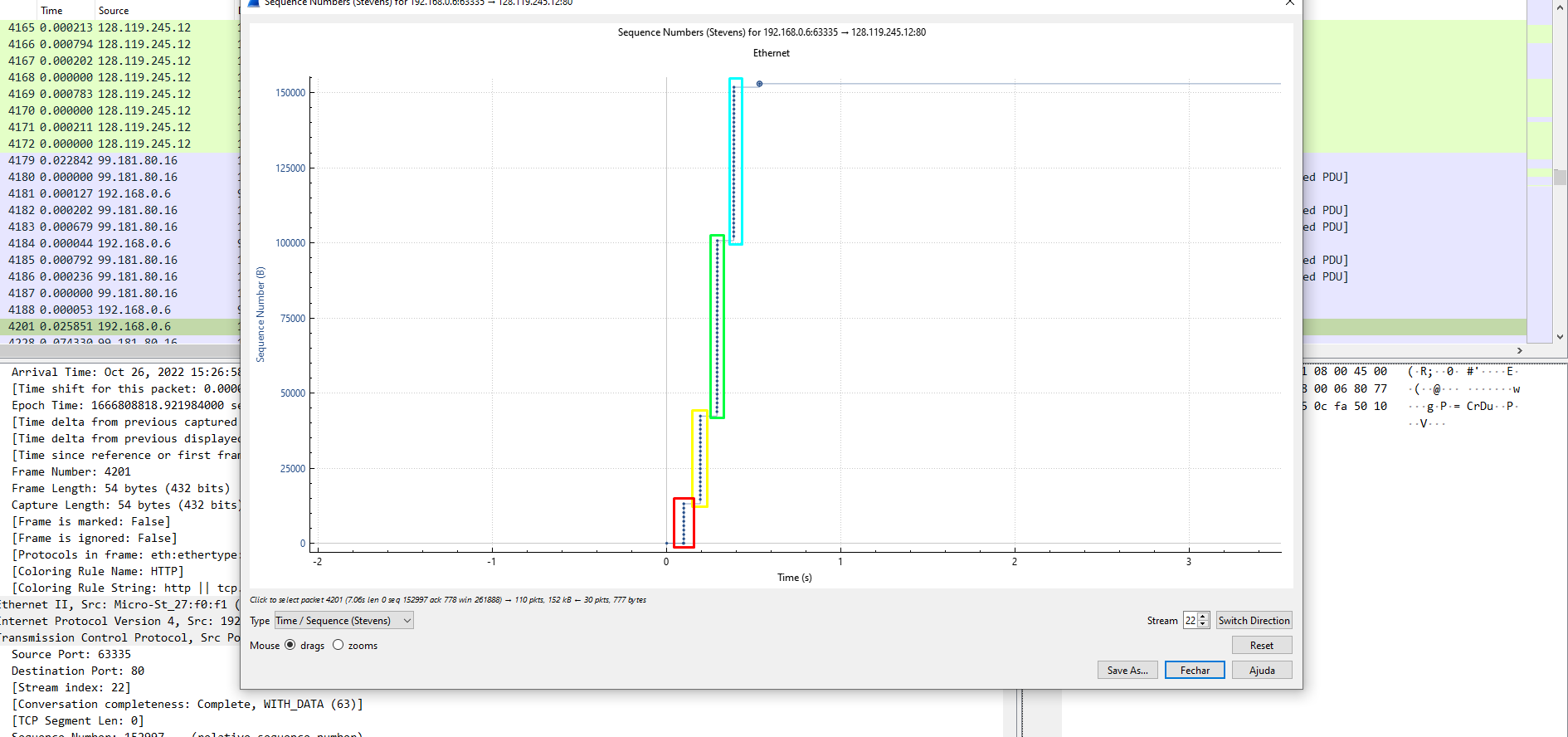
Selecionei o pacote -> Statistics File Properties -> Statistics: Average bits/s



Acho que essa segunda ta mais certa, vi nesse site: <https://ask.wireshark.org/question/12867/how-to-find-the-transfer-rate-in-wireshark-trace-ethernet-interface/>



**12 - Use a ferramenta de plotagem Time-Sequence-Graph(Stevens) para visualizar o gráfico de número de sequência versus tempo dos segmentos que estão sendo enviados do cliente para o servidor gaia.cs.umass.edu. Considere as "frotas" de pacotes enviados em torno de t = 0,025, t = 0,053, t = 0,082 e t = 0,1. Comente se parece que o TCP está em sua fase de início lento, fase de prevenção de congestionamento ou alguma outra fase. A Figura 6 mostra uma visão ligeiramente diferente desses dados.**



* Em vermelho há a primeira frota, a qual está com poucos pacotes a fim de prevenir perdas.
* Em amarelo há a segunda frota, com tamanho dobrado em relação à primeira, já que nela todos os pacotes foram recebidos, nesta segunda frota subtende se que é possível enviar mais pacotes.
* Em verde há a terceira frota, com quantidade de pacotes dobrada em relação à segunda, também pelo mesmo motivo.
* Por fim, em azul, há a quarta e última frota, com o restante dos pacotes.

**13. Essas “frotas” de segmentos parecem ter alguma periodicidade. O que você pode dizer sobre o período?**

Sim, as frotas posteriores à primeira tem uma quantidade de pacotes dobrada em relação à anterior, que tinha poucos pacotes para controlar o congestionamento de pacotes, mas quando são recebidos em sua completude, na frota posterior a quantidade de pacotes é dobrada, e assim posteriormente

**14 - Responda a cada uma das duas perguntas acima para o rastreamento que você coletou quando transferiu um arquivo do seu computador para gaia.cs.umass.edu.**