Aluno: Kauã Melchioretto

**Redes de Computadores**

**Laboratório de Wireshark TCP**

1. Qual é o endereço IP e o número da porta TCP usado 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 do cabeçalho do pacote selecionado” (consulte a Figura 2 em “Introdução ao Wireshark” Lab se você não tiver certeza sobre as janelas do Wireshark).

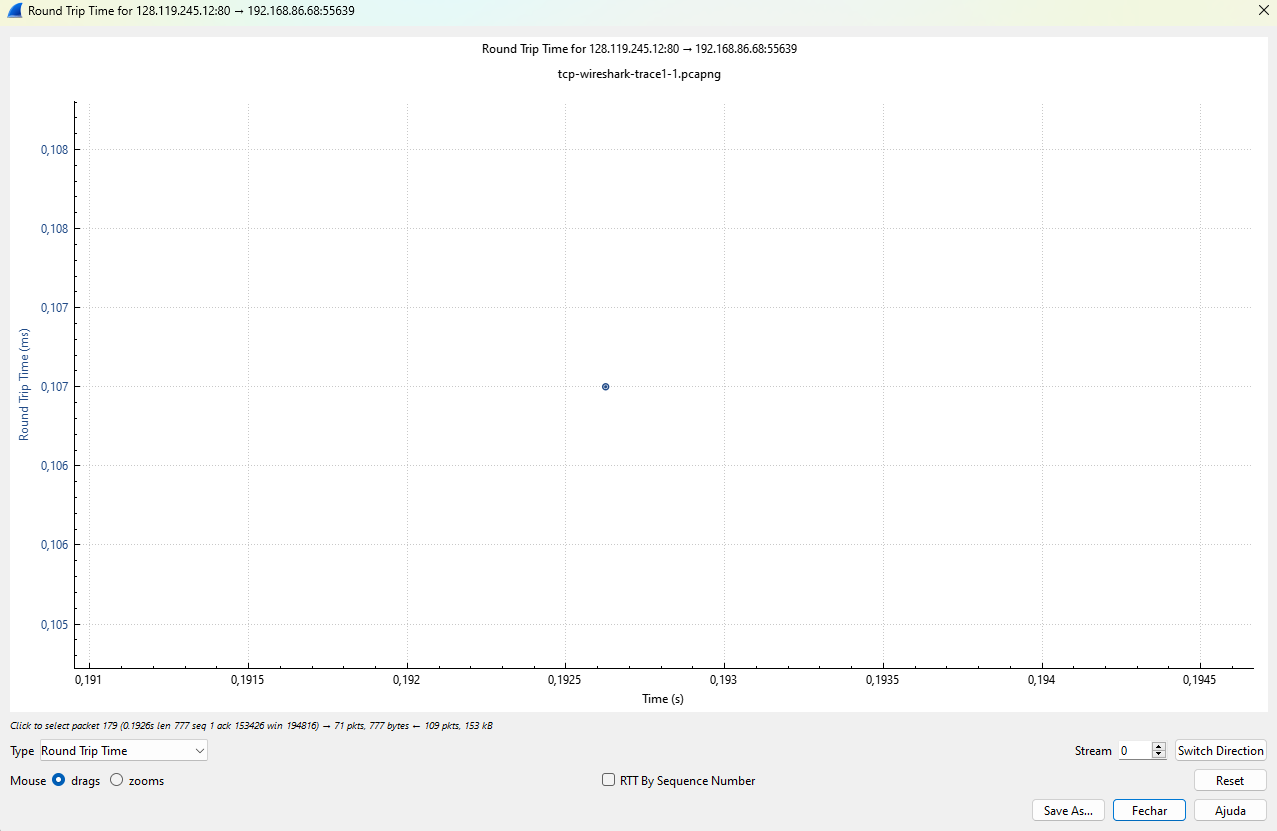
R: As porta do client é “Source Port: 55639” o IP de origem (cliente) é o “Source Address: 192.168.86.68”

1. 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?  
   R: O endereço de IP de gaia.cs.umass.edu é “Destination Address: 128.119.245.12” é a porta de destino é “Destination Port: 80”
2. Qual é o número de sequência do segmento TCP SYN usado para iniciar a conexão TCP entre o computador cliente e gaia.cs.umass.edu? (Observação: este é o número de sequência “bruto” transportado no próprio segmento TCP; **NÃO é o número do pacote na coluna “No.” na janela do Wireshark**. Lembre-se de que não existe um “número do pacote” no TCP ou UDP; como você sabe, existem números de sequência no TCP e é isso que estamos procurando aqui. Observe também que este não é o número de sequência relativo em relação ao número de sequência inicial desta sessão TCP.). O que há neste segmento TCP que identifica o segmento como um segmento SYN? O receptor TCP nesta sessão será capaz de usar Reconhecimentos Seletivos (permitindo que o TCP funcione um pouco mais como um receptor de “repetição seletiva”, consulte a seção 3.4.5 no texto)?  
   R: O número de sequência do segmento TCP SYN é o “Sequence Number (raw): 4236649187”.  
    O que identifica o segmento como SYN é as flags presente na seção “Transmition control protocol” que possuí o valor “Flags: 0x002 (SYN)”  
    Ele pode ser capaz de fazer a repetição seletiva, não é garantido mas é capaz visto que é perceptível os valores “[Next Sequence Number: 1 (relative sequence number)]” no SYN enviado pelo cliente pois, além de que como o SYN não transfere dados, apenas solicitação de conexão.
3. 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?  
   R: O número de sequência enviado do SYNACK pelo servidor é “Sequence Number (raw): 1068969752”.   
    O segmento que indica ser um SYNACK é as flags presente na sub seção TCP “Flags: 0x012 (SYN, ACK)”.   
    O valor no Acknowledgement é “Acknowledgment number (raw): 4236649188”. Esse número é determinado a partir do Sequence Number (raw) enviado pelo cliente que foi citado na questão anterior, o valor é “Sequence Number (raw): 4236649187”, sendo assim o Acknowledgement é somado +1 nesse valor.
4. 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 no campo de conteúdo do pacote na parte inferior da janela do Wireshark, procurando por um segmento com o texto ASCII “POST” dentro de seu campo DATA*[[1]](#footnote-2),[[2]](#footnote-3)*. Quantos bytes de dados estão contidos no campo de carga útil (dados) desse segmento TCP? Todos os dados no arquivo transferido alice.txt couberam neste único segmento?  
   R: O número de sequência do segmento é o “Sequence Number (raw): 4236801228” com o a sequência relativa “Sequence Number: 152041 (relative sequence number)”.

O tamanho em bytes de dados contidos é de “Content-Length: 152359\r\n”.

Não couberam todos os dados do arquivo em um único segmento, por isso que temos vários pacotes TCP os quais transportam os dados do arquivo enviado para o servidor que destaca o tamanho do arquivo na propriedade “File Data: 152359 bytes”.

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

* A que horas foi enviado o primeiro segmento (aquele que contém o HTTP POST) na parte de transferência de dados da conexão TCP?  
  R: Foi enviado na data “Arrival Time: Feb 2, 2021 23:43:26.840557000 Hora oficial do Brasil”
* A que horas foi recebido o ACK para este primeiro segmento contendo dados?  
  R: Foi recebido o ACK para este primeiro segmento contendo os dados na data “Arrival Time: Feb 2, 2021 23:43:26.842501000 Hora oficial do Brasil”
* Qual é o RTT para este primeiro segmento contendo dados?  
  R: O RTT para o primeiro segmento contendo dados é de “[The RTT to ACK the segment was: 0.024938000 seconds]”
* Qual é o valor RTT do segundo segmento TCP portador de dados e seu ACK?  
  R: O valor do RTT do segundo é de “[The RTT to ACK the segment was: 0.024941000 seconds]”
* Qual é o valor EstimatedRTT (ver Seção 3.5.3, no texto) depois que o ACK para o segundo segmento portador de dados é recebido? Suponha que, ao fazer este cálculo após o recebimento do ACK para o segundo segmento, o valor inicial de *EstimatedRTT* seja igual ao RTT medido para o primeiro segmento e, em seguida, seja calculado usando a equação *EstimatedRTT* na página 242 e um valor de α = 0,125.  
  R: O valor do EstimatedRTT é cerca de “0,107”  
    
  Foi utilizado a dica abaixo para obter o resultado

*Nota: O Wireshark possui um bom recurso que permite plotar o RTT para cada um dos segmentos TCP enviados. Selecione um segmento TCP na janela “listagem de pacotes capturados” que está sendo enviado do cliente para o servidor gaia.cs.umass.edu. Em seguida, selecione: Estatísticas->TCP Stream Graph->Round Trip Time Graph.*

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

R: O comprimento é fixo de 1448 bytes visto que é o tamanho limite de cada pacote de TCP enviado com o transporte dos dados. Segue propriedade dos pacotes “TCP segment data (1448 bytes)”

1. Qual é a quantidade mínima de espaço de buffer disponível anunciado ao cliente por gaia.cs.umass.edu entre esses quatro primeiros segmentos TCP portadores de dados? A falta de espaço no buffer do receptor alguma vez estrangulou o transmissor para esses primeiros quatro segmentos de transporte de dados?  
   R: O espaço da janela do servidor ficou em um valor variado como por exemplo “[Calculated window size: 31872]”, “[Calculated window size: 34816]” e “[Calculated window size: 37760]” e aumentando. No client a definição dessa propriedade é fixa em “[Calculated window size: 131712]” e até o final dos pacotes TCP o Window size do servidor foi aumentando, porém, não extrapolou o limite de 131712

1. *Dica: este segmento TCP é enviado pelo cliente logo (mas nem sempre imediatamente) após o segmento SYNACK ser recebido do servidor.* [↑](#footnote-ref-2)
2. Observe que se você filtrar para mostrar apenas mensagens “http”, verá que o segmento TCP que o Wireshark associa à mensagem HTTP POST é o último segmento TCP na conexão (que contém o texto no final de alice.txt: “THE END”) e não o primeiro segmento de transporte de dados na conexão. Alunos (e professores!) geralmente acham isso inesperado e/ou confuso. [↑](#footnote-ref-3)