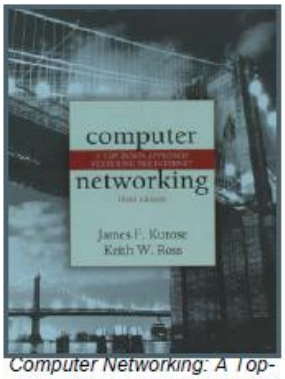
Ethereal Lab: TCP



Computer Networking: A Top-down Approach Featuring the Internet, 3rd edition.

Version: 1.0

Neste laboratório, vamos investigar o comportamento do TCP em detalhes. Faremos isso através da análise de um trace de segmentos TCP enviados e recebidos na transferência de um arquivo de 150KB (contendo o texto de Alice no país das maravilhas, de Lewis Carrol) do seu computador para um servidor remoto. Vamos estudar no TCP a utilização da seqüência e números de confirmação para proporcionar a transferência de dados confiável; vamos ver o algoritmo de controle de congestionamento TCP em ação – partida lenta e como evitar o congestionamento; e veremos o mecanismo de controle fluxo do receptor TCP. Também vamos considerar brevemente a configuração da conexão TCP e investigar o desempenho (throughput e RTT – Round-trip time) da conexão entre seu computador e o servidor.

Antes de iniciar este laboratório, você provavelmente vai querer rever as seções 3.5 e 3.7 na text.[1]

1. Capturando uma transferência TCP em massa de seu computador para um computador servidor remoto

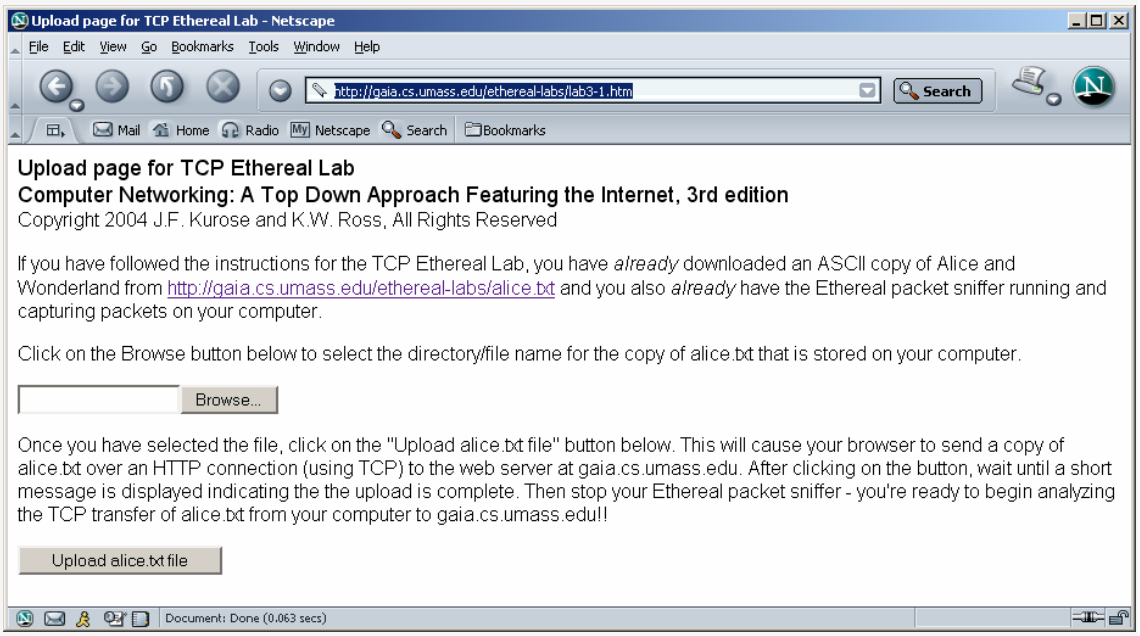
Antes de começar nossa exploração do TCP, vamos precisar usar o Ethereal para obter um arquivo para transferência do seu computador para um servidor remoto. Você vai fazê-lo acessando uma página da Web que permitirá que você digite o nome de um arquivo armazenado em seu computador (que contém o texto ASCII de Alice no País das Maravilhas), e depois transferir o arquivo para um servidor Web utilizando o método POST HTTP (ver secção 2.2.3 no texto). Utilizaremos o método POST em vez do método GET para transferir um grande quantidade de dados do seu computador para outro computador. É claro, vamos estar executando o Ethereal durante esse tempo para obter o rastreamento dos segmentos TCP enviados e recebidos.

[1] Todas as referências ao texto neste laboratório são apresentadas no livro Redes de Computadores e a Internet: Uma Nova Abordagem - 3 ª edição

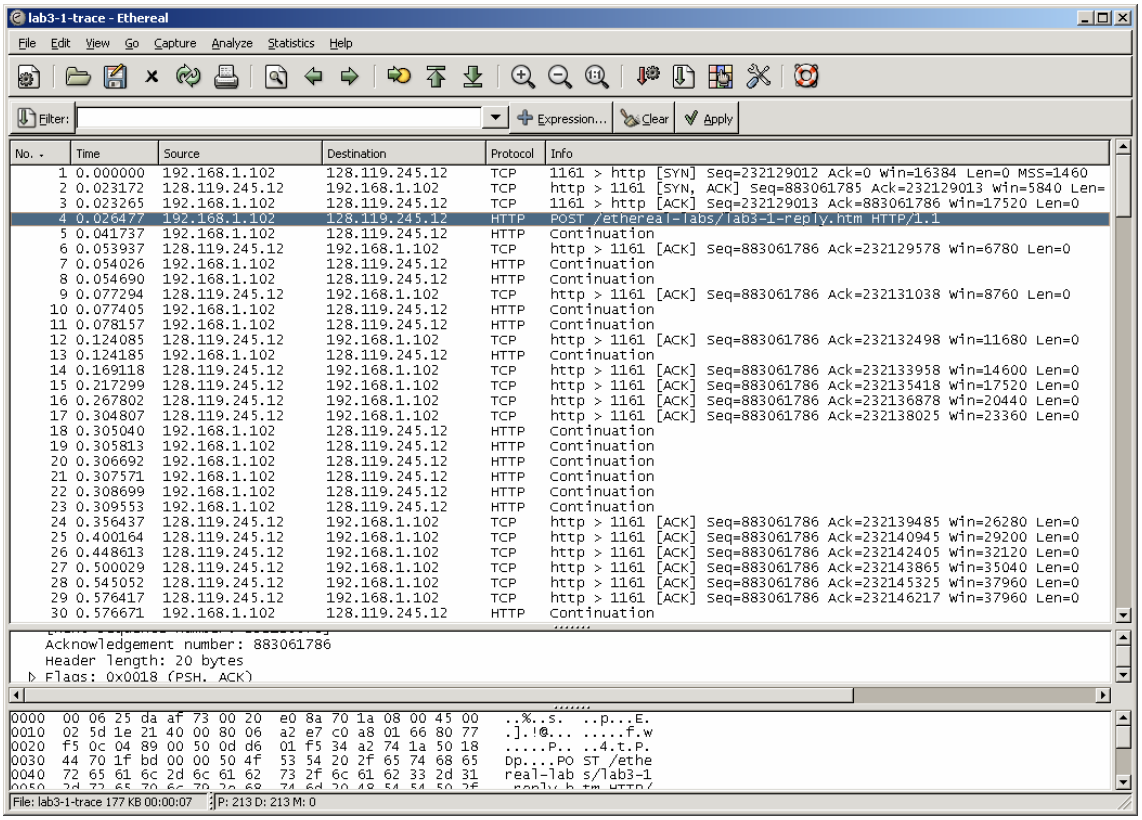
.

Faça o seguinte:

- Inicie o seu browser web. Ir a http://gaia.cs.umass.edu/ethereal-labs/alice.txt e recuperar uma cópia ASCII de Alice no País das Maravilhas. Armazenar esse arquivo em algum lugar no seu computador.
- Em seguida vá para http://gaia.cs.umass.edu/ethereal-labs/TCP-ethereal-file1.html.
- Você deverá ver uma tela que se parece com:



- Use o botão **Browse (Procurar)** para introduzir o nome do arquivo (nome completo do caminho) contendo Alice no País das Maravilhas (ou fazê-lo manualmente) em seu computador. Ainda não pressione o botão "**Upload alice.txt file**" .
- Agora inicie Ethereal e comece a captura de pacotes (Capture-> Interface -> Start) e pressione OK na tela de Opções de Captura de Pacotes Ethereal (não vai ser necessário selecionar qualquer opção).
- Regressando ao seu navegador, pressione o botão "**Upload alice.txt arquivo**" para fazer o upload do arquivo para o servidor gaia.cs.umass.edu. Uma vez que o arquivo foi carregado, uma curta mensagem de parabéns será exibida na janela do browser.
- Pare a captura de pacotes do Ethereal. Sua tela Ethereal deve ser semelhante a mostrada abaixo.



Se você não conseguir executar o Ethereal numa rede conectada, você pode baixar um trace que foi capturado pelo autor quando seguia os passos acima em seus experimentos. Você pode muito bem baixar esse trace, mesmo que você tenha capturado seu próprio rastreamento, e usá-lo como opção ao seu próprio rastreamento, quando você for explorar as perguntas abaixo.

2. Uma primeira visão do o trace capturado

Antes de analisar o comportamento da conexão TCP em detalhes, vamos dar uma olhada, em alto nível, no trace.

- Primeiro, filtrar os pacotes exibidos na janela Ethereal, digitando "tcp" (em letras minúsculas, sem aspas, e não se esqueçer de pressionar APPLY) na janela de especificação do filtro na parte superior da tela do Ethereal.

O que você deve ver é uma série de mensagens TCP e HTTP entre seu computador e gaia.cs.umass.edu. Você deverá ver o three-way handshake inicial contendo mensagens com o bit SYN setado.

[2] Baixe o arquivo zip de http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip e extraia o arquivo tcpethereal-trace-1. Os traces desse arquivo zip foram coletados através da execução Ethereal em um dos computadores do autor, enquanto realizava os passos indicados no laboratório Ethereal. Depois de ter baixado o trace, você pode carregá-lo no Ethereal e exibir o rastreamento usando a opção Arquivo/Abrir no menu suspenso, e em seguida, selecionando o arquivo de rastreamento tcp-ethereal-trace-1.

Você deverá ver uma mensagem HTTP POST e uma série de mensagens de "Continuação HTTP" (TCP segment of a reassembled PDU) enviadas do seu computador para o servidor gaia.cs.umass.edu. Lembre-se da nossa discussão no laboratório anterior Ethereal HTTP, que existe uma Mensagem de continuação HTTP – essa é a forma do Ethereal indicar que há vários segmentos TCP sendo usados para levar uma única mensagem HTTP. Você também deve ver segmentos TCP ACK sendo retornados de gaia.cs.umass.edu para o seu computador.

Responder às seguintes perguntas, abrindo o arquivo de pacotes capturados do Ethereal tcp-ethereal-trace-1 em http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip (que você pode baixar e abrir no Ethereal, conforme nota [2]). Sempre que possível, ao responder uma pergunta, imprimir os pacote(s) dentro do trace que você usou para responder. Para imprimir um pacote, use File-> Imprimir, marque "*selected packet only* ", "*Packet summary line*", e selecione uma quantidade mínima de detalhes do pacote que você precisará para responder a questão.

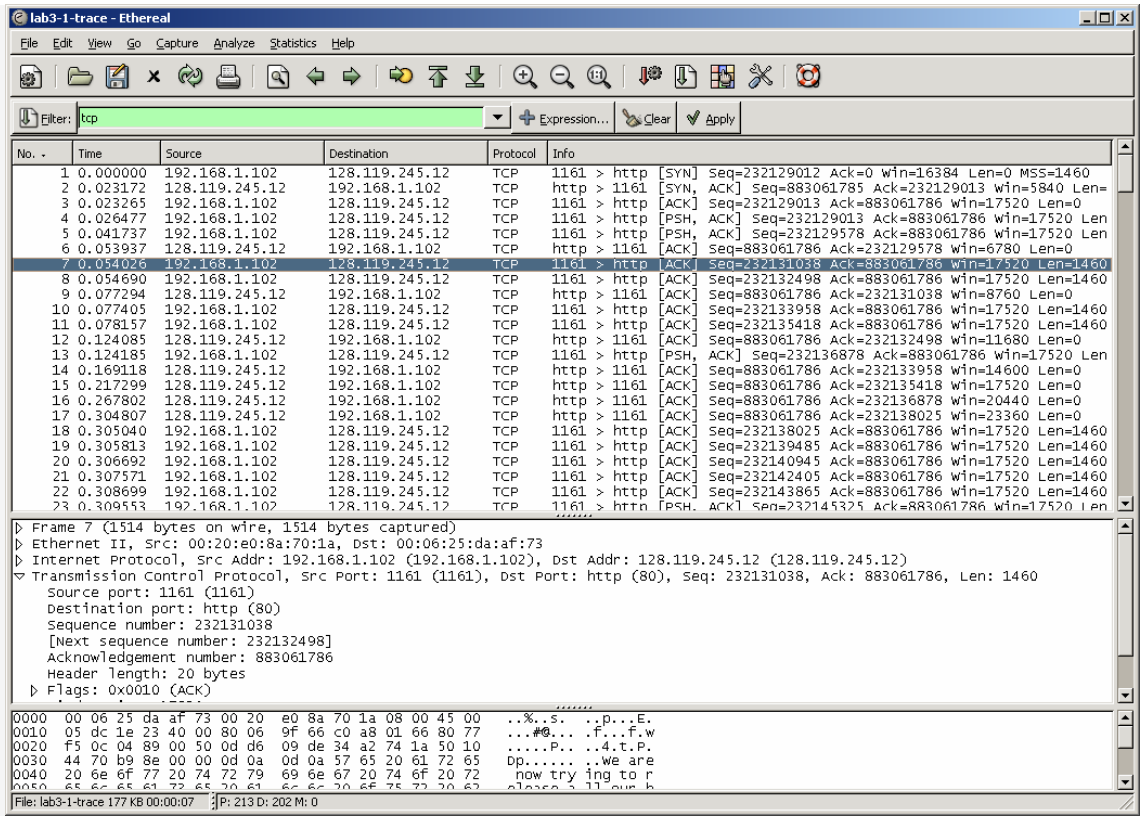
1. Qual é o endereço IP e número da porta TCP usados pelo computador do cliente (fonte) que está transferindo o arquivo para gaia.cs.umass.edu? Para responder a esta pergunta, provavelmente é mais fácil selecionar uma mensagem HTTP e explorar os detalhes do pacote TCP usado para transmitir a mensagem HTTP, usando os detalhes do pacote selecionado na janela de cabeçalho "(veja a Figura 2 na" Introdução ao Ethereal Lab "se você está incerto sobre as janelas Ethereal.
2. Qual é o endereço IP de gaia.cs.umass.edu? E o número da porta de envio e de recebimento de segmentos TCP para esta conexão?

Se você foi capaz de criar seu próprio rastreamento (trace), responda a seguinte pergunta:

3. Qual é o endereço IP e número da porta TCP usada pelo seu computador cliente (fonte) para transferir o arquivo para gaia.cs.umass.edu?

Já que este laboratório é sobre o TCP, em vez de HTTP, vamos mudar na "*janela de pacotes capturados*" do Ethereal para que sejam mostradas informações sobre os segmentos TCP que contém as Mensagens HTTP, em vez de HTTP. Para isso, selecione *Analize-> Enablead Protocols*. Em seguida, desmarque a caixa de HTTP e selecione OK. Você deverá ver uma janela do Ethereal parecida com:

.



Isso é o que estamos procurando - uma série de segmentos TCP enviados entre o seu computador e gaia.cs.umass.edu. Vamos usar o traço de pacotes que você capturou (e / ou o traço de pacotes *tcp-ethereal-trace-1* em http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip ; ver nota [2]) para estudar o comportamento do TCP neste laboratório.

3. O Básico do TCP

Responder às seguintes perguntas para os segmentos TCP:

4. Qual é o número de seqüência do segmento TCP SYN que é usado para iniciar a conexão TCP entre o computador do cliente e gaia.cs.umass.edu?

O que é no segmento que identifica o segmento como um segmento SYN?

5. Qual é o número de seqüência do segmento SYNACK enviado por gaia.cs.umass.edu para o computador cliente em resposta ao SYN?

Qual é o valor do campo ACK no segmento SYNACK?
Como gaia.cs.umass.edu determinou esse valor

O que é no segmento que identifica o segmento como um Segmento SYNACK?

6. Qual é o número de seqüência do segmento TCP que contém o comando HTTP POST? Note que, a fim de encontrar o comando POST, você precisará abrir o campo de conteúdo do pacote na parte inferior da janela do Ethereal, procurando um segmento com um "POST" dentro de seu campo de dados.

7. Considere o segmento TCP que contém o POST HTTP como o primeiro segmento da conexão TCP. Quais são os números de seqüência dos seis primeiros segmentos da conexão TCP (incluindo o segmento que contém o POST HTTP)? Em que tempo foi cada segmento enviado?

Quando ocorreu o ACK para cada segmento recebido?

Dada a diferença entre quando cada segmento TCP foi enviado, e quando sua confirmação foi recebida, qual é o valor RTT para cada um dos seis segmentos?

Qual é o valor do RTT estimado (ver página 237 no texto) após a recebimento de cada ACK? Suponha que o valor do RTT estimado é igual ao RTT medido para o primeiro segmento e em seguida calcule o RTT estimado usando a equação na página 237 para todos os segmentos subseqüentes.

Nota: Ethereal tem um recurso interessante que permite traçar o RTT para cada um dos segmentos TCP enviados. Selecione um segmento TCP na listagem da " *janela de captura dos pacotes* "que está sendo enviado a partir do cliente para o servidor gaia.cs.umass.edu. Em seguida, selecione: ***Statistics-> TCP Stream Graph-> Round Trip Time Graph***.

8. Qual é o comprimento de cada um dos seis primeiros segmentos TCP? [3]

9. Qual é a quantidade mínima de espaço de buffer disponível anunciado pelos receptores no rastreamento inteiro?

Será que o espaço de buffer no receptor regula a tansmissão do remetente?

10. Há algum segmentos retransmitidos no arquivo de rastreamento?

O que o você verificou no traçe para responder a esta pergunta?

11. Qual a quantidade de dados que o receptor normalmente reconhece em um ACK?

Você pode identificar casos em que o receptor está reconhecendo todos os demais segmentos recebidos (ver Tabela 3.2 na página 245 no texto).

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

.

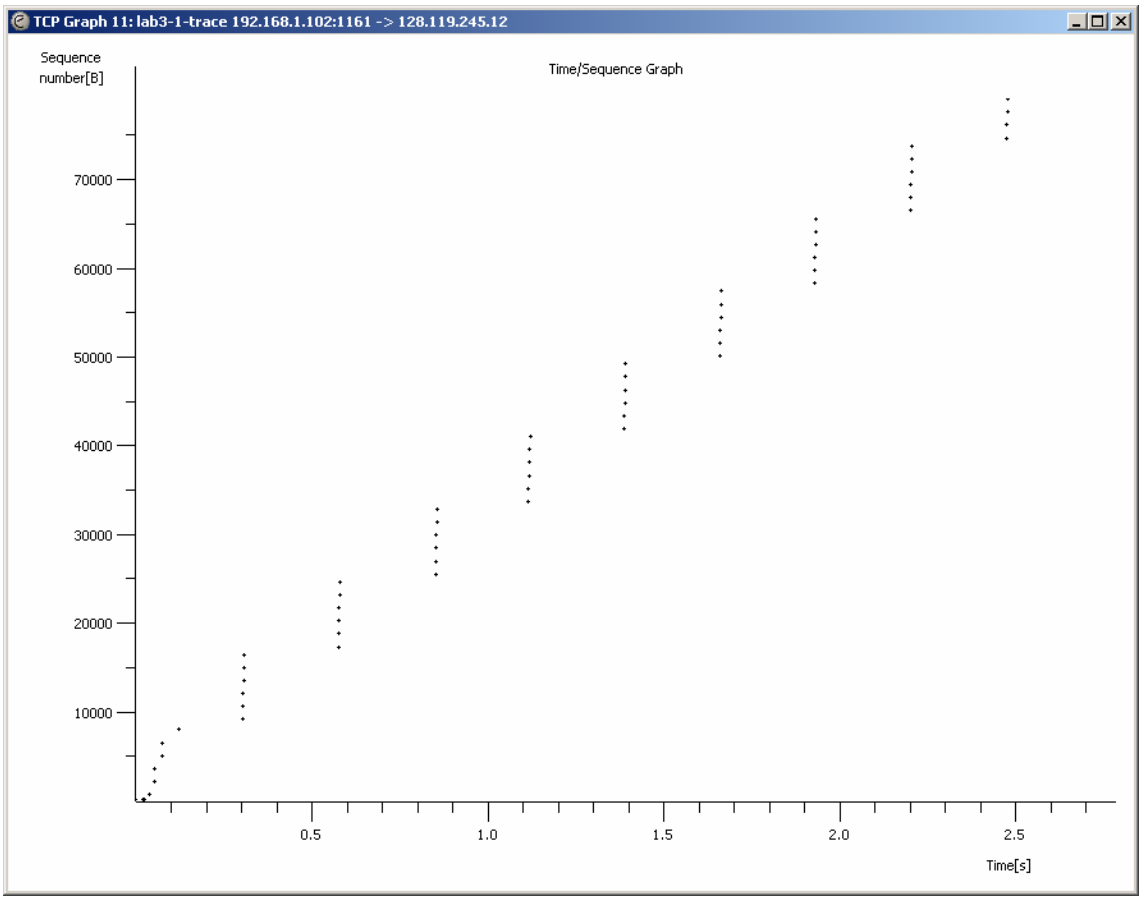
4. Controle de congestionamento TCP em ação

Vamos agora examinar a quantidade de dados enviados por unidade de tempo do cliente para o servidor.

Ao invés do tedioso trabalho de calcular isso a partir dos dados brutos na janela Ethereal, vamos utilizar a facilidade gráfica do Ethereal para TCP - ***Time-Sequence-Graph (Stevens)*** – para plotar os dados.

- Selecione um segmento TCP na janela "*lista de pacotes capturados*," do Ethereal. Em seguida, selecione o menu: ***Statistics-> TCP Stream Graph-> Time-Sequence-Graph (Stevens)***. Você deverá ver uma tela que se parece com o seguinte gráfico, que foi criado a partir dos pacotes capturados no rastreamento de pacotes *tcp-ethereal-trace-1* em http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip (ver nota 2):

[3] Os segmentos TCP no arquivo de rastreamento tcp-ethereal-trace-1 estão todos com menos de 1460 bytes. Isso ocorre porque o computador em que o trace foi recolhida tem uma placa Ethernet que limita o comprimento máximo do pacote IP em 1500 bytes (40 bytes dos dados do cabeçalho do TCP / IP e 1460 bytes de payload do segmento TCP). Este valor de 1500 bytes é o comprimento máximo permitido pelo padrão Ethernet. Se o seu trace indicar segmento TCP maior que 1500 bytes, e seu computador estiver usando uma conexão Ethernet, então Ethereal estará relatando o comprimento do segmento TCP, mas provavelmente também mostra apenas um segmento TCP grande, em vez de várias segmentos menores. Seu computador, na verdade, provavelmente, estará enviando vários segmentos menores, como indicado pela ACKs que recebe. Esta inconsistência em comprimentos de segmentos é devido à interação entre a driver Ethernet e o software Ethereal. Recomendamos que se você tiver essa inconsistência, executar este laboratório usando o arquivo de rastreamento fornecido.



Aqui, cada ponto representa um segmento TCP enviado, plotando o número de seqüência do segmento em relação ao tempo em que foi enviado. Note-se que um conjunto de pontos empilhados acima de si representa uma série de pacotes que foram enviados de volta ao remetente.

Responder às seguintes perguntas para os segmentos TCP do trace de pacotes tcp-etherealtrace-1 em http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip.

13. Use a ferramenta ***Time-Sequence Graph (Stevens)*** para ver, em lote, a seqüência de números de segmentos versus tempo enviados do cliente para o servidor gaia.cs.umass.edu. Você pode identificar onde a fase de partida lenta do TCP começa e termina, e onde evitar o congestionamento? Note que num trace do"mundo real", nem tudo é tão limpo e arrumado como na Figura 3.51 (também note que os rótulos do eixo y para a plotagem ***Time-Sequence-Graph (Stevens)*** e a ferramenta de Figura 3.51 são diferentes).

14. Comente sobre as formas em que os dados medidos diferem do comportamento idealizado da TCP que foi estudado no texto.

15. Responda cada uma das duas perguntas acima para o rastreamento capturado quando você transferiu um arquivo de seu computador para gaia.cs.umass.edu.