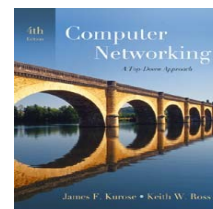


Laboratório de TCP com Wireshark

(Fonte: J. Kurose – Tradução do Prof. Edmar C. Gurjão/UFCG)



1. Introdução

Neste exercício vamos analisar o comportamento do TCP em detalhes. Faremos isso analisando os segmentos TCP enviados e recebidos quando se deseja transferir um arquivo de 150KB do seu computador para um servidor remoto. Serão analisados os números de seqüência e de reconhecimentos que garantem a confiança no TCP, também será observado o controle de congestionamento – início lento e *congestion avoidance* – em ação dentre outros mecanismos do TCP.

2. Capturando uma transferência TCP do seu computador para um servidor remoto

Antes de iniciar é necessário usar o Wireshark para obter um pacote de registro da transferência TCP do seu computador para o servidor. Você fará isso acessando uma página na qual você entra com o nome do arquivo armazenado no seu computador e a transferência do arquivo será feita pelo método HTTP POST (veja a seção 2.2.3 no livro do Kurose). Esse método é usado ao invés do método GET, pois a transferência será do seu computador para um servidor.

Faça o seguinte:

- Inicie o seu navegador e abra a página <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> e salve o arquivo apresentado no seu computador.
- Agora abra a página <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>.
- Você verá a página mostrada na Figura 1. Selecione o arquivo a ser enviado com o botão *Selecionar Arquivo* e espere até receber uma pequena mensagem de *upload complete*. Ainda não pressione o botão *Upload alice.txt file*.
- Agora abra o Wireshark e inicie a captura de pacotes (*Capture->Start*).
- Retorne ao navegador e pressione “*Upload alice.txt file*” para enviar o arquivo ao servidor gaia.cs.umass.edu. Espere até que o arquivo seja enviado totalmente. Quando isso acontecer uma mensagem de *Congratulations* será exibida na janela do seu browser.
- Pare a captura de pacotes no Wireshark. Uma janela do Wireshark semelhante à da Figura 2 será exibida.

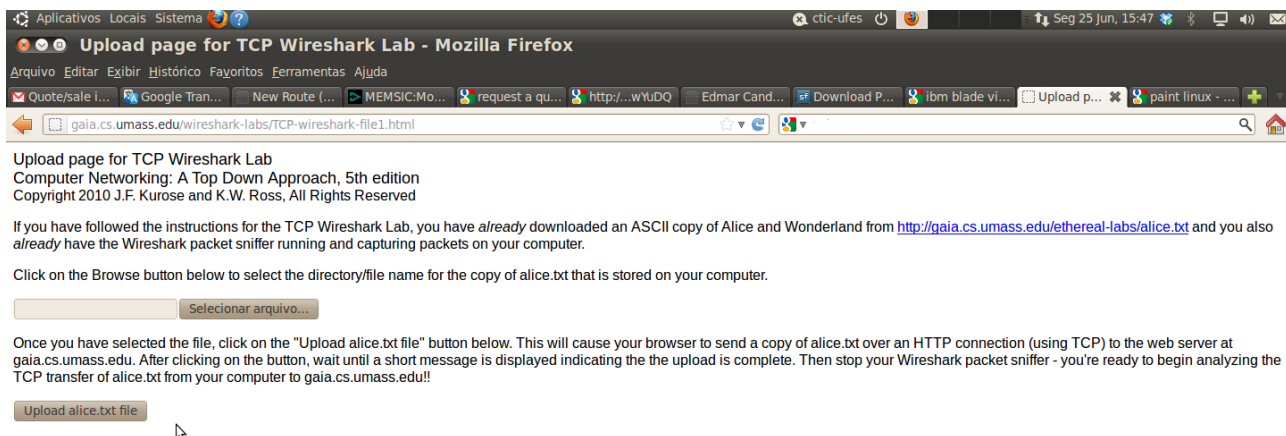


Figura 1 – Página para envio do arquivo para o servidor

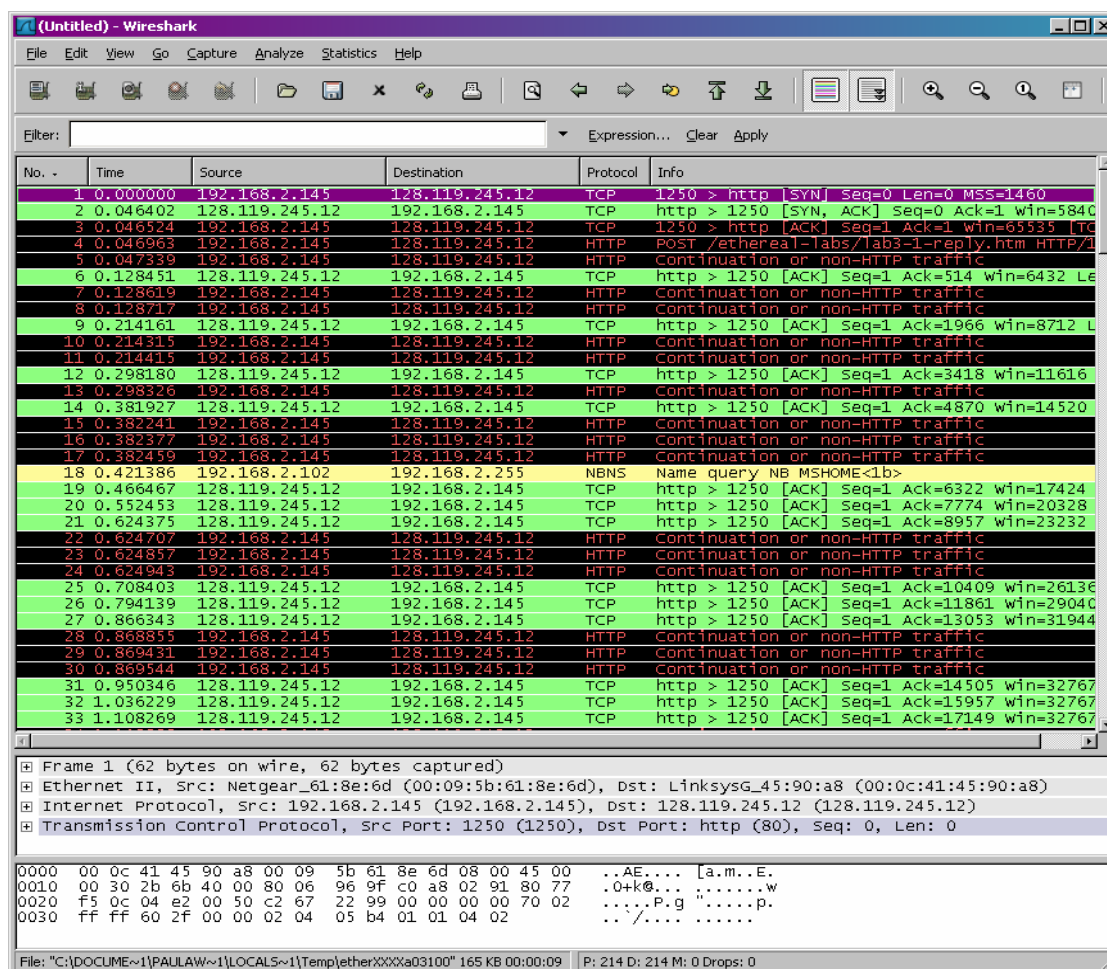


Figura 2 – Página indicando que o envio do arquivo foi realizado com sucesso.

3. Primeira análise dos pacotes capturados

Antes de analisar o comportamento da conexão TCP em detalhes, vamos fazer uma primeira análise dos pacotes capturados.

- No campo *Filter* digite **http**. Você verá uma mensagem HTTP POST indicando que o arquivo *alice.txt* será enviado para o servidor.
- No campo *Filter* digite **tcp**. O que você verá após aplicar o filtro é uma série de mensagens TCP e HTTP entre o seu computador e o servidor *gaia.cs.umass.edu*. Você pode observar os três pacotes iniciais de *handshake* contendo mensagens SYN e uma série de mensagens TCP enviadas do seu computador para *gaia.cs.umass.edu*. Você pode ver também os segmentos TCP ACK sendo retornados do servidor *gaia.cs.umass.edu* para o seu computador (Figura 3).

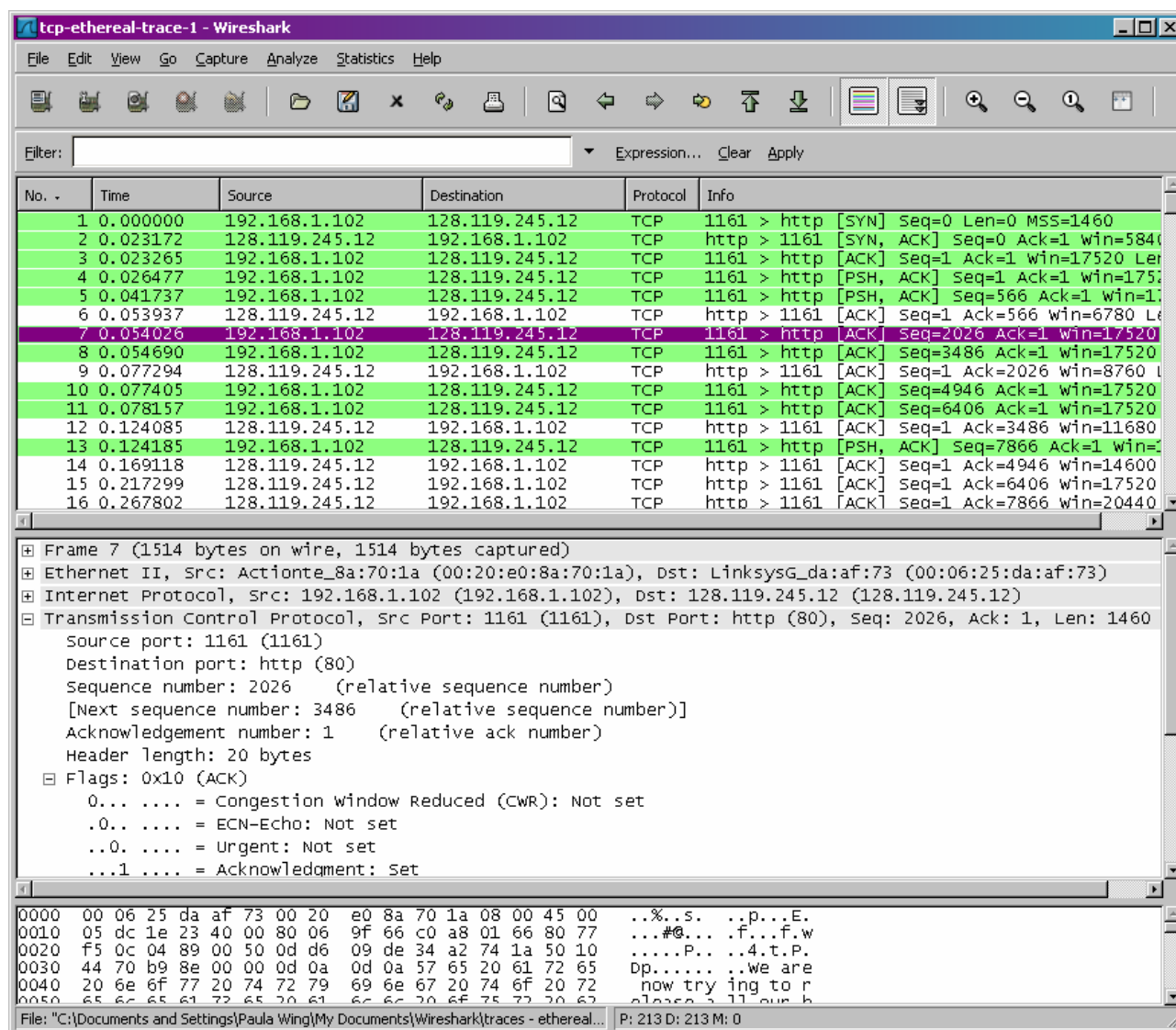


Figura 3 – Mensagens TCP entre o computador e o servidor *gaia.cs.umass.edu*

Responda as seguintes questões abaixo. Sempre que possível, anote e imprima o(s) pacote(s) que você usou para responder a questão. Para imprimir um pacote, use *File->Print -> Selected packet only -> Packet summary line*, e selecione o mínimo de detalhe que você precisa para a resposta da questão.

1. Qual é o endereço IP e o número da porta usado pelo computador cliente para transferir o arquivo para *gaia.cs.umass.edu*? Provavelmente, o meio mais fácil para responder essa questão seja pela seleção da mensagem HTTP e então explorando os detalhes do pacote TCP usado para transportar essa mensagem.
2. Qual é o endereço IP de *gaia.cs.umass.edu*? Em algum lugar da mensagem POST está indicado que o arquivo “*alice.txt*” será enviado para o servidor. Onde está essa informação?

4. Básico sobre TCP

Responda as seguintes questões para os segmentos TCP. Para isso aplique o filtro *tcp*.

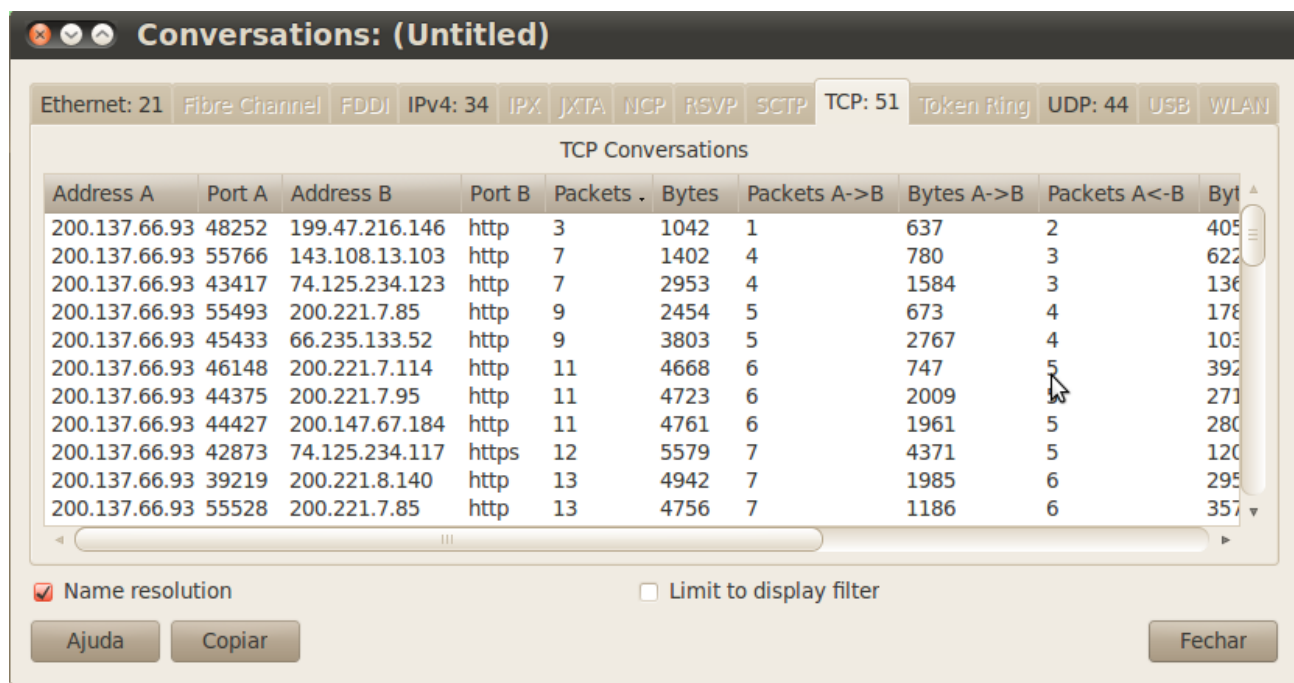
3. Qual é o número de sequência para o segmento TCP SYN usado para iniciar a conexão TCP entre o cliente e *gaia.cs.umass.edu*? Qual parâmetro do segmento permite identificar que ele é o do tipo SYN?
4. Qual o número de sequência do segmento SYNACK enviado por *gaia.cs.umass.edu* para o cliente em resposta ao SYN? Qual o valor do campo ACKnowledgement no segmento SYNACK? Como *gaia.cs.umass.edu* determinou esse valor? Qual é o campo do segmento que o identifica como um SYNACK?
5. Qual o número de sequência do segmento TCP contendo o comando HTTP POST ?
6. Considere o segmento TCP contendo a mensagem HTTP POST como o primeiro segmento na conexão TCP. Quais são os números de sequência para os primeiros segmentos na conexão TCP (incluindo o segmento que contém o HTTP POST)? Em que instante esse segmento foi enviado? Quando foi recebido o segmento ACK? Analisando a diferença entre o instante em que os segmentos TCP foram enviados e quando seus reconhecimentos foram recebidos, qual o valor do RTT (*Round-Trip Time*) para cada um desses segmentos? Qual o valor de *EstimatedRTT*? Assuma que o valor de *EstimatedRTT* é igual ao RTT medido para o primeiro segmento. Usando a fórmula $EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT$ (Cap. 3 do livro do Kurose) calcule os RTT estimados para os próximos segmentos.

O Wireshark pode plotar os RTTs dos segmentos enviados. Para isso, selecione o segmento TCP referente a mensagem HTTP POST na janela de protocolos e então selecione *Statistics->TCP Stream Graph->Round Trip Time Graph* e reponda:

7. Qual a quantidade mínima de espaço disponível no buffer do receptor durante a conexão?
8. Existe algum segmento retransmitido?
9. Qual é a vazão (bytes transferidos por unidade de tempo) para a conexão TCP? Explique como você calculou esse valor .

Agora vá em *Statistics -> Conversations*. Na janela que será aberta escolha a aba TCP. Você deverá ver uma janela como a que está mostrada na Figura 4. Essa janela mostra a quantidade de pacotes e de bytes trocados entre Address A e Address B. Observe os valores para os pacotes TCP e responda:

10. Quantos pacotes foram enviados da sua máquina para o servidor http? E do servidor para sua máquina. Os valores são diferentes? Explique o motivo dessa diferença e se esses valores podem ser iguais.



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B
200.137.66.93	48252	199.47.216.146	http	3	1042	1	637	2	405
200.137.66.93	55766	143.108.13.103	http	7	1402	4	780	3	622
200.137.66.93	43417	74.125.234.123	http	7	2953	4	1584	3	136
200.137.66.93	55493	200.221.7.85	http	9	2454	5	673	4	178
200.137.66.93	45433	66.235.133.52	http	9	3803	5	2767	4	103
200.137.66.93	46148	200.221.7.114	http	11	4668	6	747	5	392
200.137.66.93	44375	200.221.7.95	http	11	4723	6	2009	5	271
200.137.66.93	44427	200.147.67.184	http	11	4761	6	1961	5	280
200.137.66.93	42873	74.125.234.117	https	12	5579	7	4371	5	120
200.137.66.93	39219	200.221.8.140	http	13	4942	7	1985	6	295
200.137.66.93	55528	200.221.7.85	http	13	4756	7	1186	6	357

Figura 4 – Tela que mostra as quantidades de pacotes trocados entre dois pontos.