UNIVERSADE FEDERAL DE SANTA CATARINA
REDES DE COMPUTADORES 1
PROFESSOR: CARLOS BECKER WESTPHALL
Aluno: João Victor Macedo Giombelli
Matrícula: 15200600

1. Introdução

O objetivo deste trabalho é analisar o tráfego de uma rede, identificando o estabelecimento da conexão, a transferência de dados e a finalização da conexão. Foi usada a aplicação Wireshark que analisa o trafego de rede.

2. Descrição do Funcionamento

2.1 Estabelecimento de conexão

A verificação do estabelecimento de conexão é feito através de pacotes e flags. O usuário primeiramente envia uma flag **SYN** junto com o pacote TCP com o requerimento de estabelecer uma conexão. Se tudo sair como planejado o servidor responde com um **SYN + ACK**. Caso o cliente receba esse **SYN + ACK** ele envia para o servidor um **ACK** e assim estabelece a conexão.

2.2 Transferência de Dados

TCP/IP é um conjunto de protocolos que segue o modelo OSI, dentre os diversos protocolos contidos nele neste relatório usaremos apenas o HTTP e FTP.

2.3 Finalização da Conexão

Quando um dos agentes tomar a iniciativa de encerrar a conexão, o mesmo enviará um pacote TCP com a flag **FIN**. Se não houver erros, o outro lado deve confirmar o pedido com um **ACK** e em seguida enviará um **FIN** e após o requerente enviar um **ACK** a conexão é finalmente encerrada.

3. Desenvolvimento

Para realizar o trabalho, a URL www.netshoes.com.br foi monitorada, cujo IP é 23.77.40.240.

Foi utilizado o filtro “(tcp or http) and ip.addr ==23.77.40.240” para facilitar a visualização dos pacotes necessários para o trabalho.

3.1 Estabelecimento da Conexão

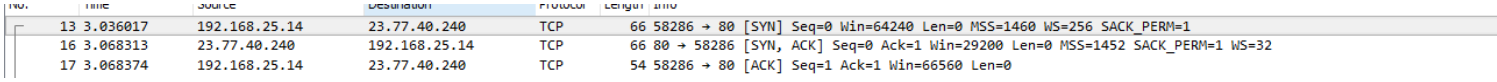

Figura 1: Pacotes para realizar a conexão

O primeiro passo é um pedido inicial do IP 192.168.25.14 para realizar a conexão, usando a flag SYN com um valor aleatório. O protocolo utilizado é o TCP e a porta utilizada pela Camada de Aplicação é a 58286.

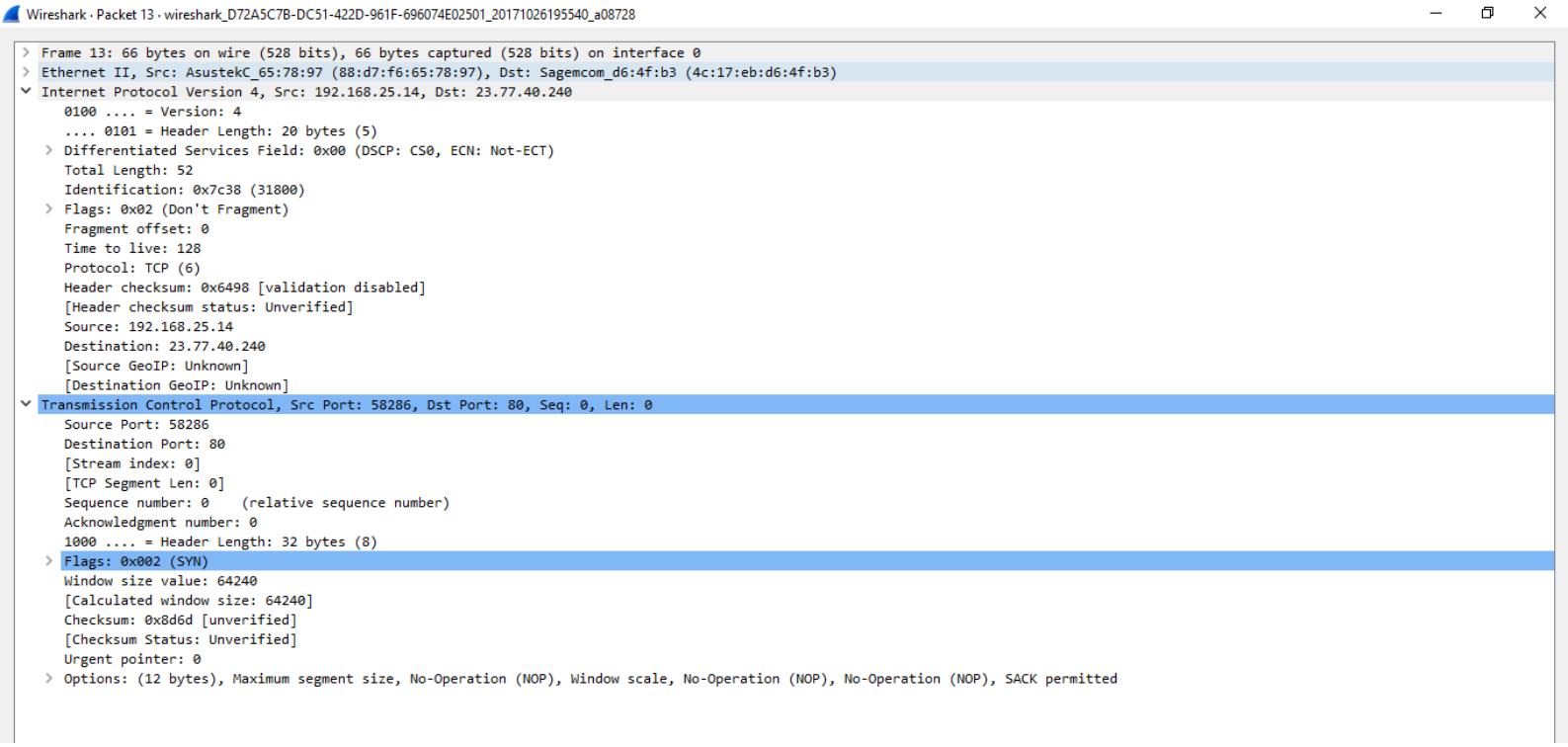

Figura 2: Pacote do primeiro passo

O segundo passo seria o pedido de confirmação do servidor, nesse caso 104.88.122.217, enviando SYN+ ACK para o cliente (192.68.25.14), cujo valor de ACK é o valor recebido (que seria 0) acrescentando uma unidade. Valor de ACK =1. Valor de SYN = 0.

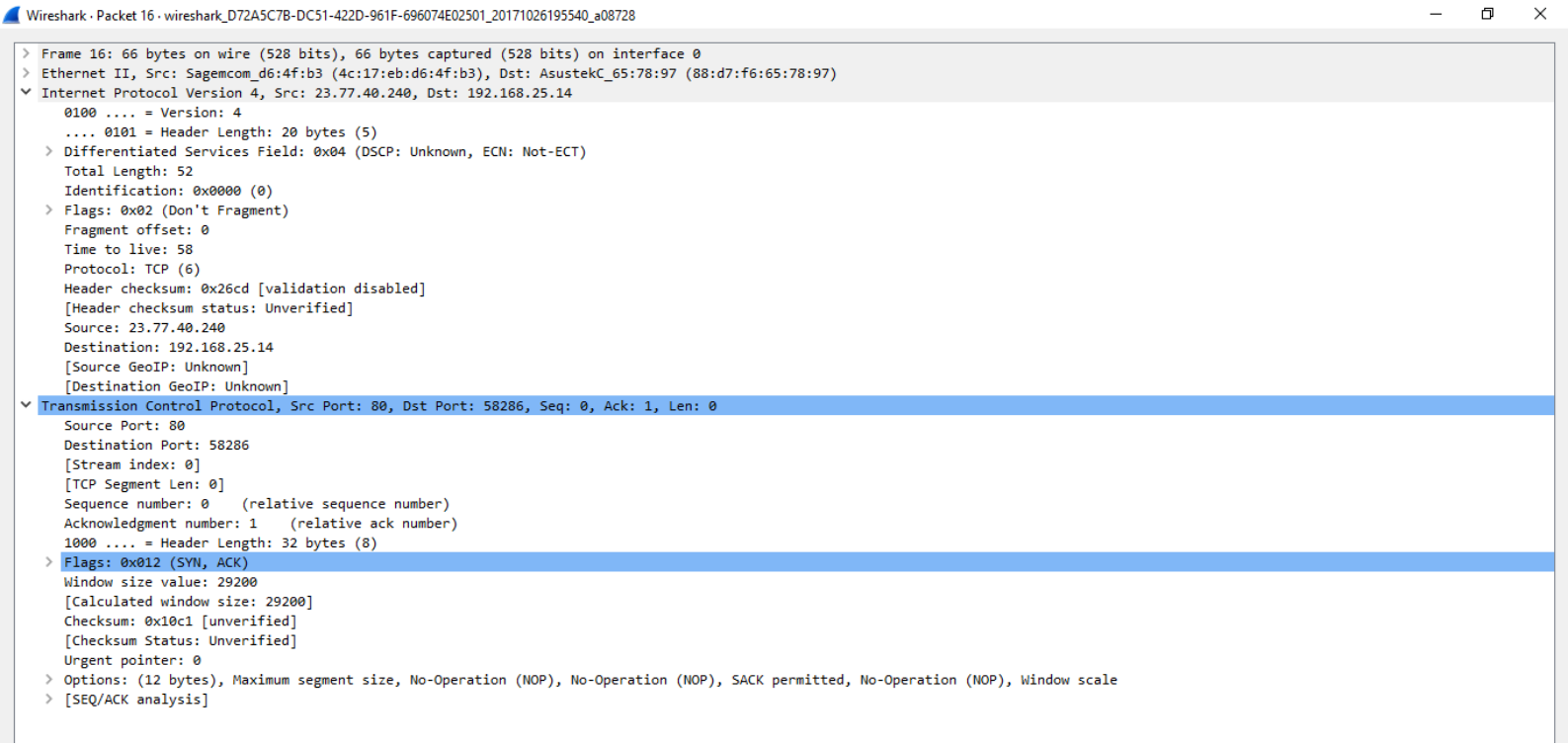

Figura 3: Pacote do Segundo Passo.

O terceiro passo é estabelecer finalmente a conexão entre servidor e cliente. O cliente retorna um ACK, com SYN de mesmo número recebido pelo servidor.

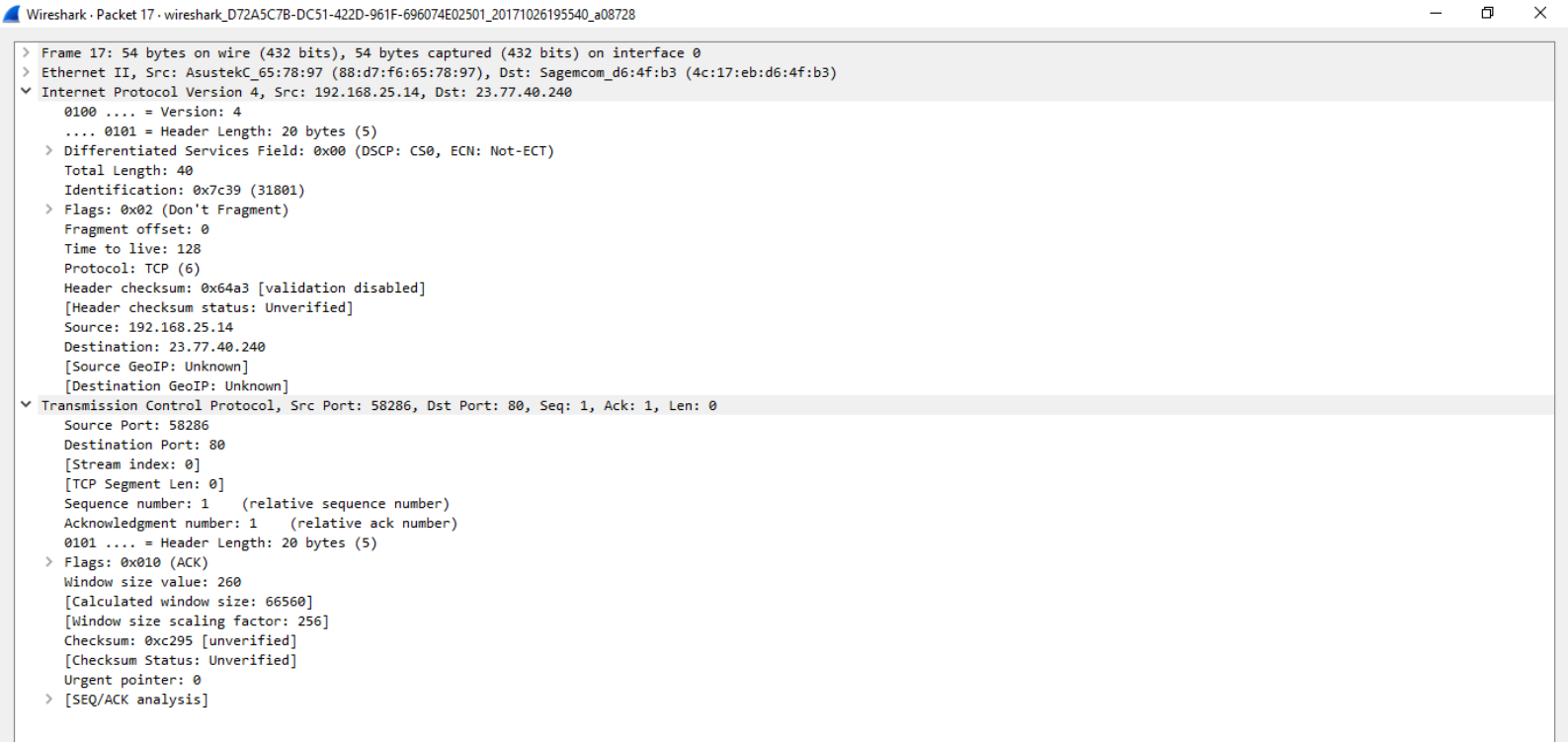

Figura 4: Pacote do Terceiro Passo.

3.2 Transferência de dados

Quando a comunicação se torna estável entre o navegador e o servidor, o primeiro pacote HTTP é enviado e é possível ver a informação enviada.

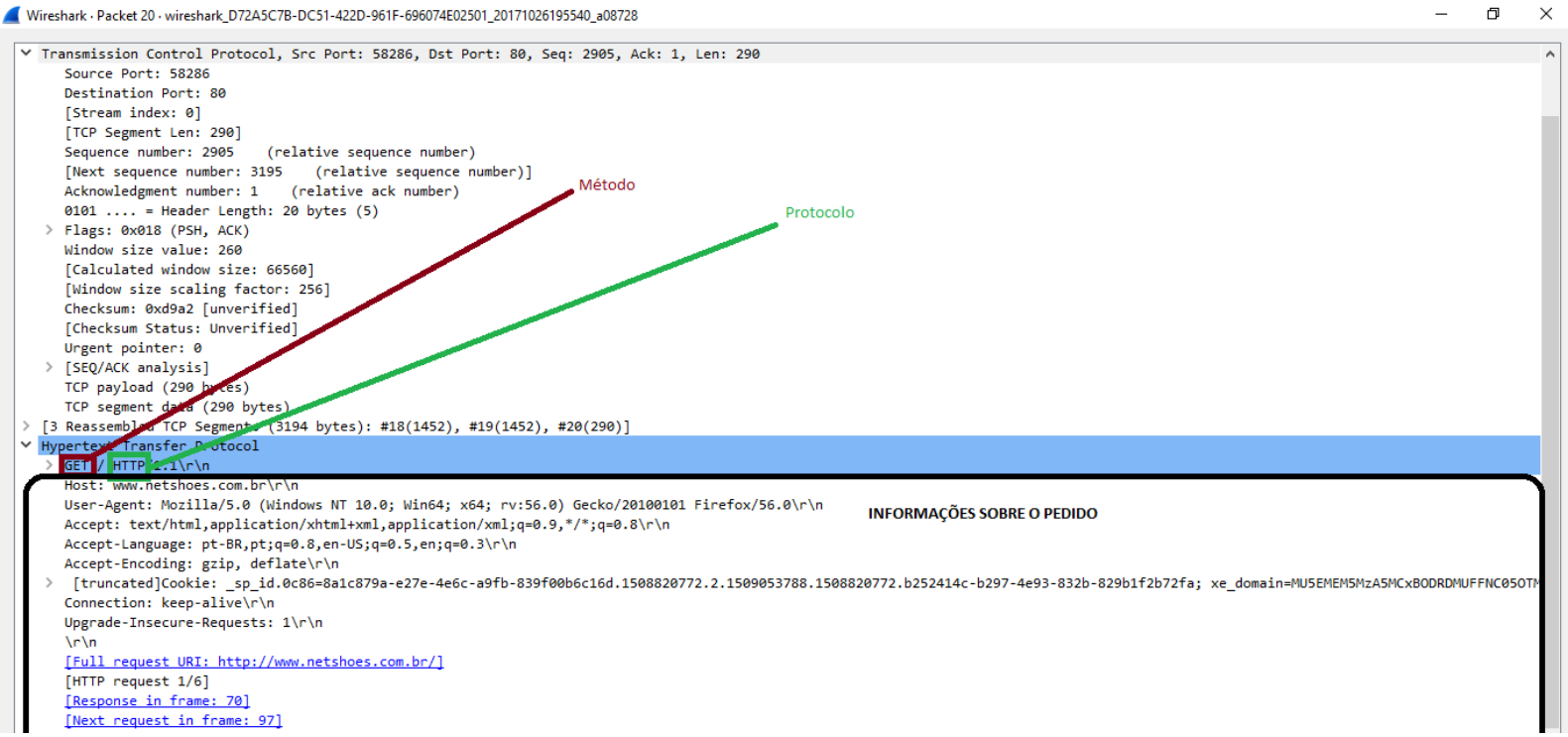

Figura 5: Informações do pacote enviado.

3.3 Finalizando a conexão

Para a conexão ser finalizada são enviados 3 pacotes.

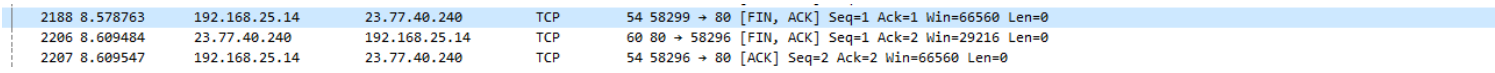

Figura 6: Pacotes que finalizam a conexão.

No último pacote com dados, em que o servidor envia, é ativada a flag [FIN].

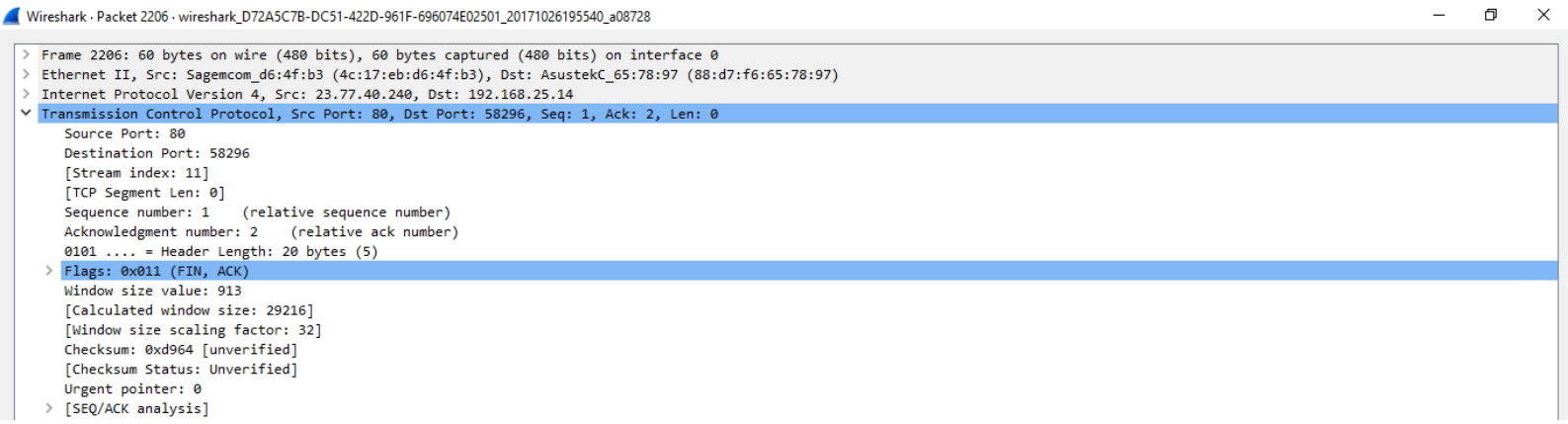

Figura 7: Primeiro passo para a finalização da conexão.

Em seguida, o usuário confirma ao servidor o pedido de término e verifica se o servidor finalizará também.

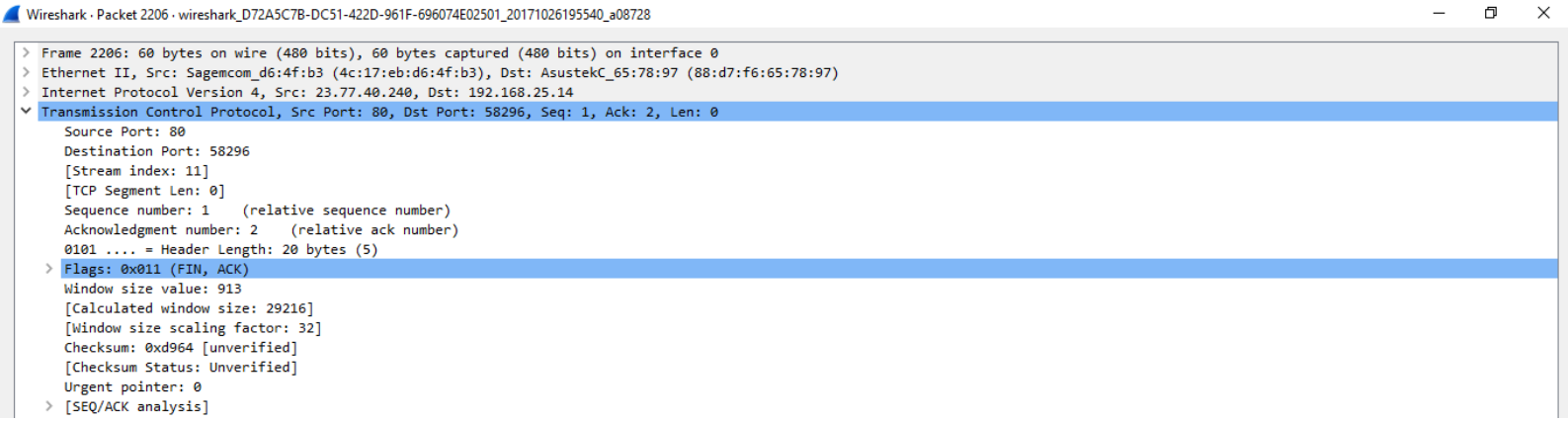

Figura 8: Segundo e terceiro passos para a finalização da conexão.

Por fim, o servidor confirma o pedido e a conexão é desfeita.

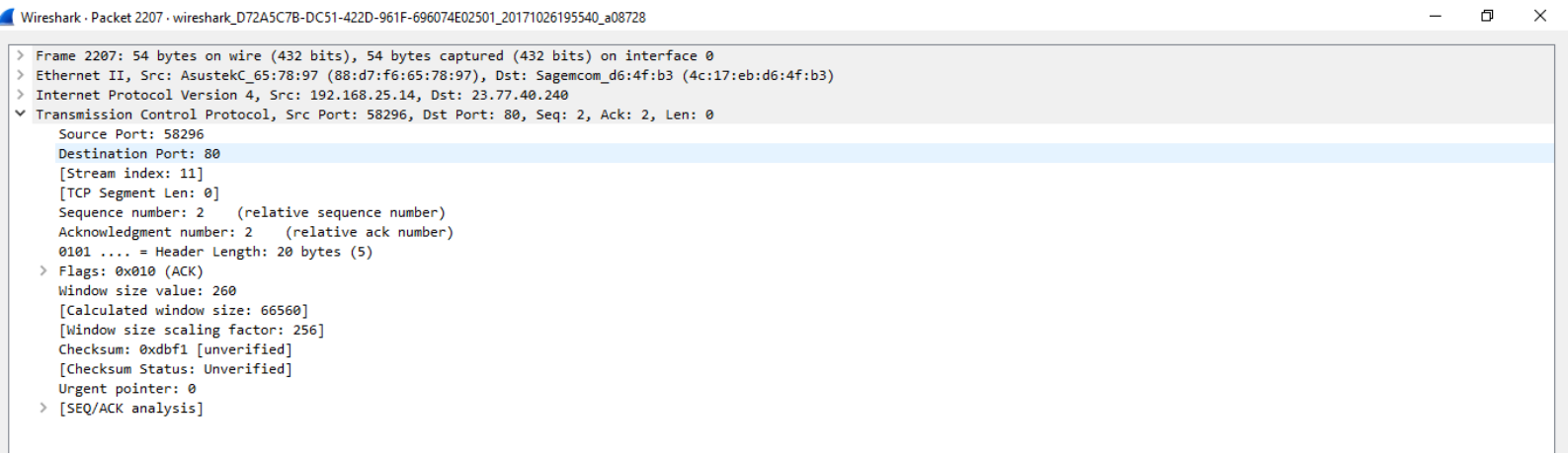

Figura 9: Quarto passo para a finalização da conexão.

4. Referências Bibliográficas

[1] https://pt.wikipedia.org/wiki/TCP/IP

[2] https://pt.wikipedia.org/wiki/Hypertext_Transfer_Protocol

[3] https://pplware.sapo.pt/microsoft/windows/aprenda-a-usar-o-sniffer-wireshark-parte-i/

[4] https://www.wireshark.org/

[5] https://nandovieira.com.br/entendendo-um-pouco-mais-sobre-o-protocolo-http

[6] https://www.citisystems.com.br/protocolo-tcp-ip/