Trabalho Prático III

Analise de Trafego de Rede Com Wireshark

Felipe Longarai Trisotto

Departamento de Informática e Estatística
Centro Tecnológico - CTC
Universidade Federal de Santa Catarina

INE 5414 - Redes de Computadores I
Professor: Carlos Becker Westphall
Nov 20, 2016

1 Introdução

Este relatório expõe a realização do terceiro trabalho prático, solicitado pela matéria de Redes de Computadores I - INE 5414. O objetivo deste trabalho é analisar o tráfego de uma rede para o estabelecimento da conexão, tráfego de dados e finalização da conexão, fazendo uso da ferramenta Wireshark, que registra pacotes que trafegam na rede e suas respectivas informações. Nosso principal interesse nesse trabalho é mostrar os protocolos TCP e HTTP.

2 Descrição do funcionamento

2.1 Estabelecimento da conexão

E possıvel verificar o estabelecimento da conexão através de pacotes e flags. O cliente, inicialmente, envia uma flag SYN juntamente com pacote TCP com a pretensão de estabelecer uma conexão. Se tudo ocorrer da maneira correta, o servidor responde com um SYN + ACK. Se o cliente receber corretamente, ele enviar a um ACK para o servidor, estabelecendo a conexão.

2.2 Transferência de dados

O modelo TCP/IP e um conjunto de protocolos que seguem o modelo OSI visto em sala de aula. Obviamente, existem diversos protocolos (HTTP, SMTP, FTP, SNMP, DNS), porém com a ajuda do próprio WireShark faremos um filtro com aqueles que temos intenção de analisar.

2.3 Finalização da conexão

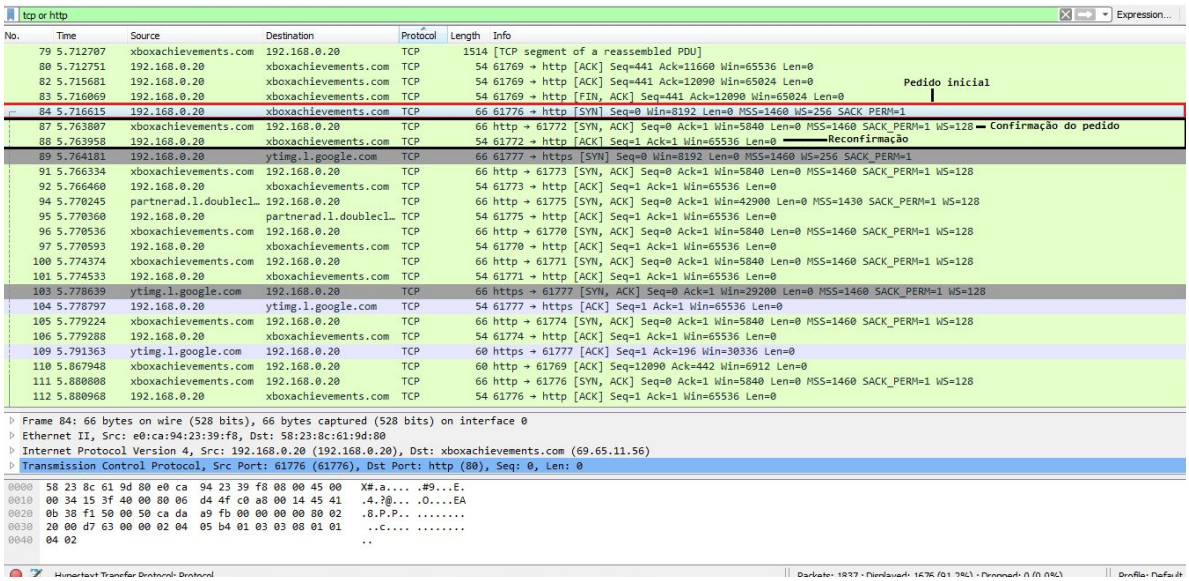
Quando um dos extremos tiver a iniciativa de finalizar a conexão, será enviado desse um pacote TCP com a flag FIN. Contando que não ocorra erros, o outro irá confirmar o pedido com o ACK e seguidamente irá enviar um FIN; sendo realmente interrompida a ligação quando o primeiro enviar um ACK.

3 Desenvolvimento

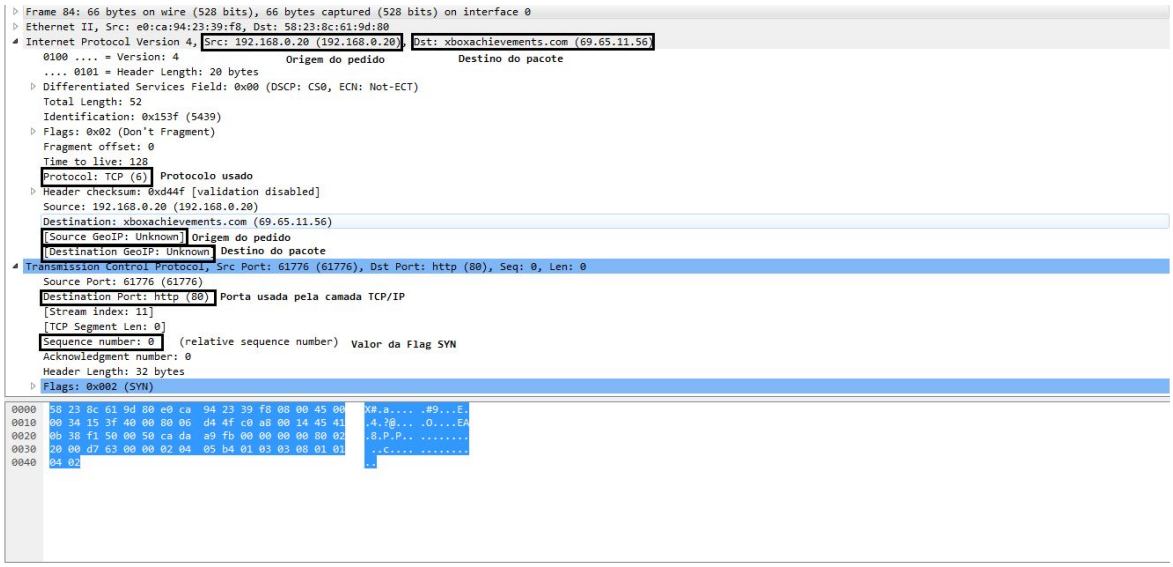
A URL escolhida para realizar a analise da conexao foi: http://www.xboxachievements.com/ , utilizando o filtro “TCP or HTTP” visto que eles sao os de nosso interesse.

3.1 Estabelecimento da conexão

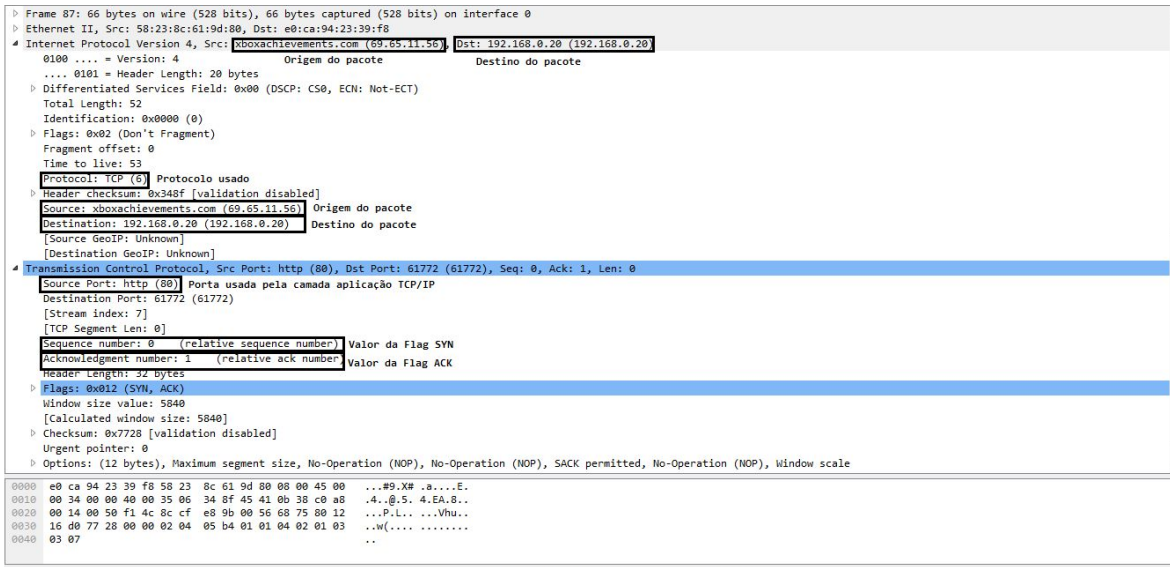
A primeira ação a ser executada e para gerar a conexão com o servidor. Para isso é realizado em três passos:



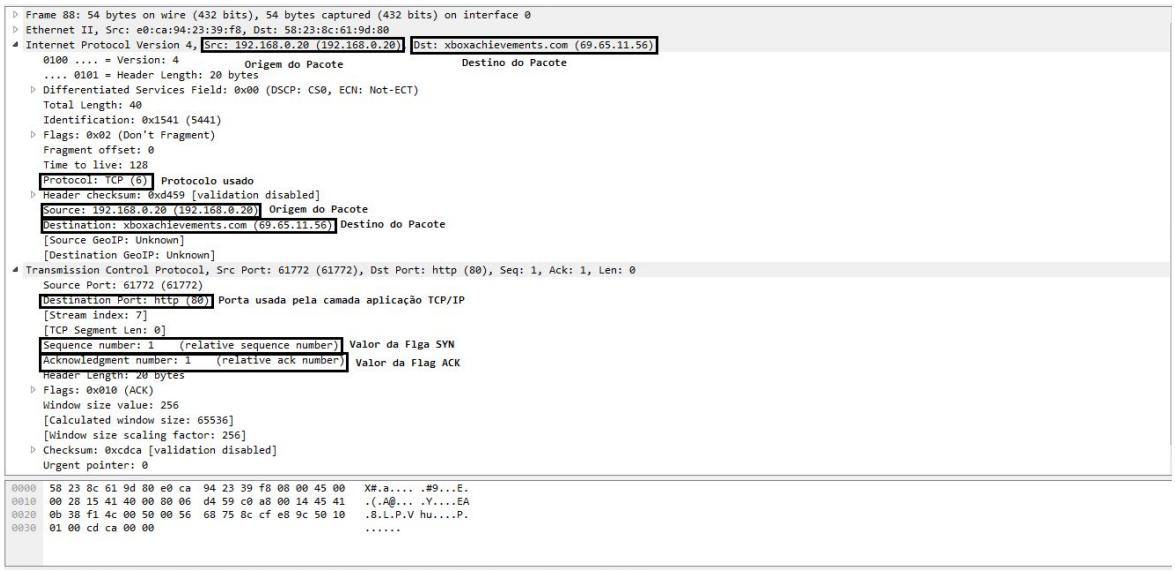
Primeiro Passo: é feito o pedido inicial com a flag SYN, com um valor aleatório.



Segundo Passo: Caso disponıvel, o servidor confirma o pedido enviando SYN+ACK, cujo valor de ACK é o valor recebido acrescentando uma unidade.

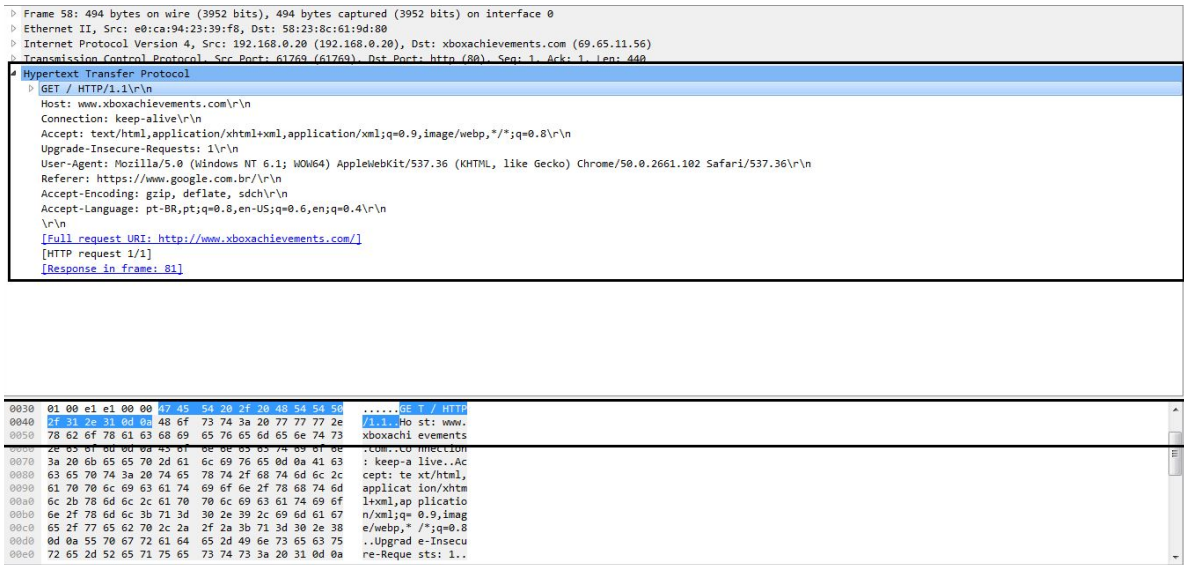


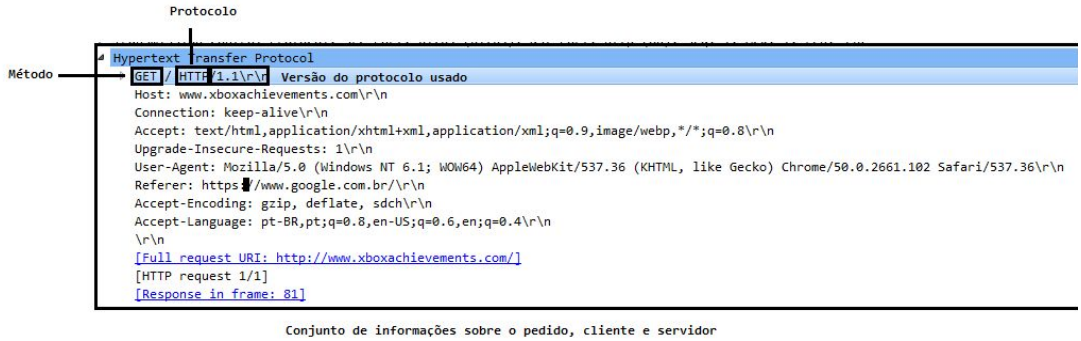
Terceiro Passo: Para estabelecer a conexão o cliente retorna um ACK, com SYN com mesmo número de ACK recebido pelo servidor.



3.2 Transferência de dados

Assim que estabilizada a comunicação entre o navegador, o Firefox, e o servidor da Xbox Achievements. Como ocorre no primeiro pacote HTTP. Dando dois cliques sobre ele e possıvel verificar esse detalhes. Quando selecionado alguma linha de comando do pacote (dentro do quadro superior), na divisão inferior da página é destacado da informação do conjunto, em hexadecimal.

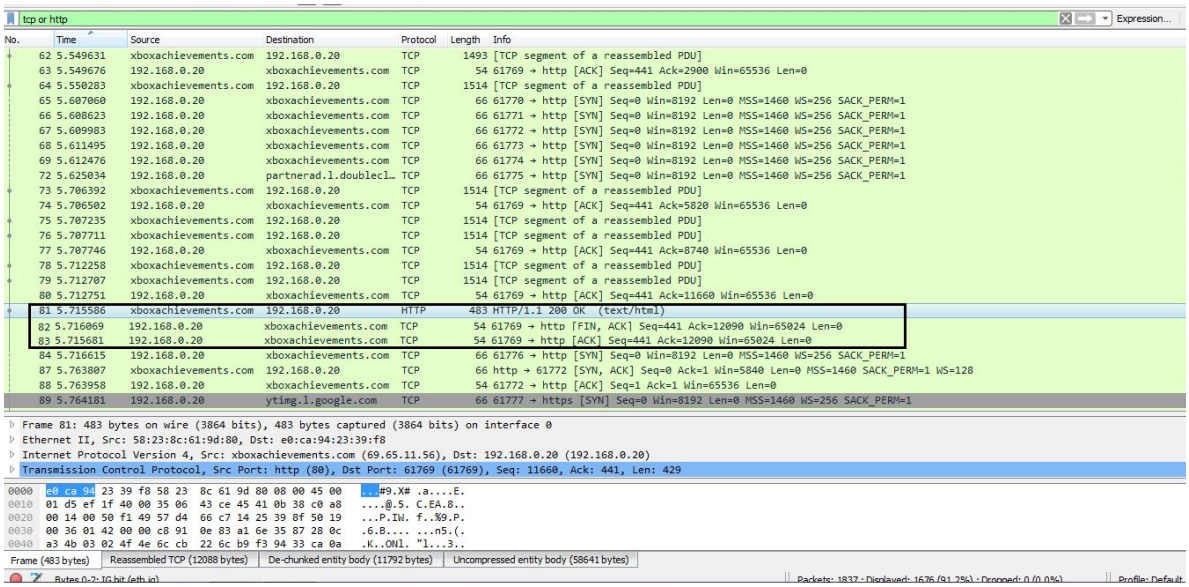




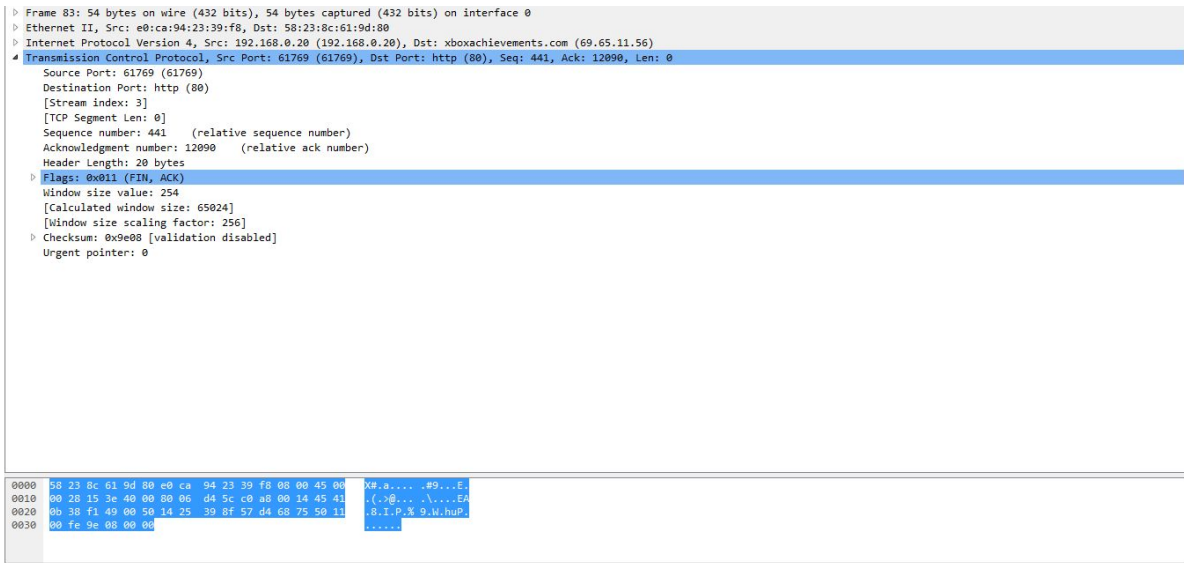
É possível verificar a atuação do protocolo TCP, ordenando os pacotes. No Wireshark ao abrir a página com os detalhes do pacote HTTP selecionado, no cabeçalho de origem TCP há a informação do SYN, NEXT SYN e ACK. Quando solicitado o NEXT SYN, o servidor.

3.3 Finalização da conexão

Quatro passos são necessários, que são executados em três pacotes:



No último pacote com dados, em que o servidor envia, é ativada a flag, FIN. Como mostrado na figura a seguir, que apresenta os detalhes do primeiro pacote da imagem anterior:



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