MONITORAMENTO DE REDES

Fabíola Maria Kretzer – 16100725

INE5414 - Redes de Computadores I

Universidade Federal de Santa Catarina – UFSC

Florianópolis, 21 de outubro de 2017

Sumário

1. Introdução

2. Descrição do Funcionamento e Desenvolvimento

2.1 Estabelecimento da conexão

2.2 Transferência de dados

2.3 Finalização da conexão

3. Conclusão

4. Referências bibliográficas

1. Introdução

Este relatório corresponde ao Terceiro Trabalho Prático de disciplina de Redes de Computadotes I. Neste trabalho será utilizado o wireshark para identificar a ocorrência de conexões e transferências de dados, envolvendo as camadas de aplicação, transporte e rede. No decorrer do relatório serão apresentadas telas capturadas pelo wireshark, a identificação de pacotes relacionados com criação da conexão, a transferênica de dados e a liberação de conexões. Sendo de principal interesse os protocolos TCP e HTTP.

2. Descrição do Funcionamento e Desenvolvimento

Para a realização deste trabalho, foi escolhido para analisar a URL https://www.youtube.com/watch?v=Ey_O48VB_fU, vídeo da banda Roupa Nova tocando a música “Dona”. Depois de executado o vídeo, foi interrompido o Wireshark. Resultando nos pacotes que vão ser utilizados como base para fazer este relatório, sendo de maior interesse os pacotes com protocolo TCP e HTTP, para isto utilizou-se o filtro.

O TCP é orientado a conexão – Para ter o controle dos pacotes enviados e conseguir efetuar a fragmentação, o TCP precisa que os usuários finais tenham o controle do que está sendo enviado. O protocolo TCP especifica três fases durante uma conexão: estabelecimento da ligação, transferência e término de ligação.[5]

2.1 Estabelecimento da conexão

Para estabelecimento da conexão o TCP necessita que: “O cliente inicia a ligação enviando um

pacote TCP com a flag SYN ativa e espera-se que o servidor aceite a ligação enviando um pacote SYN+ACK. Se, durante um determinado espaço de tempo, esse pacote não for recebido ocorre um timeout e o pacote SYN é reenviado. O estabelecimento da ligação é concluído por parte do cliente, confirmando a aceitação do servidor respondendo-lhe com um pacote ACK" - Wikipedia.

A primeira ação a ser executada é para gerar a conexão com o servidor. Isso é realizado em três passos (Figura 1):

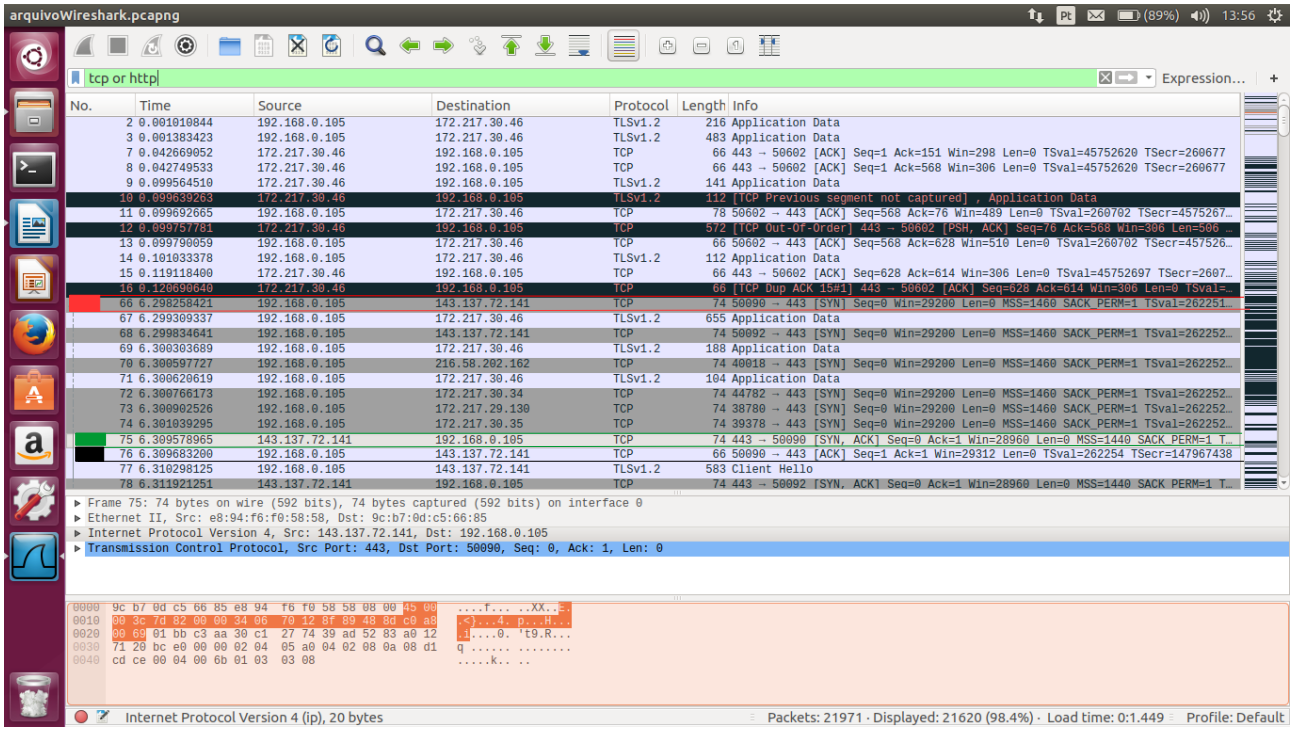

Figura 1: Três passos para estabilizar a conexão e o filtro.

Legenda:

- *Pedido Inicial*
- *Confirmação do Pedido*
- *Reconfirmação, estabilizando a conexão*

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

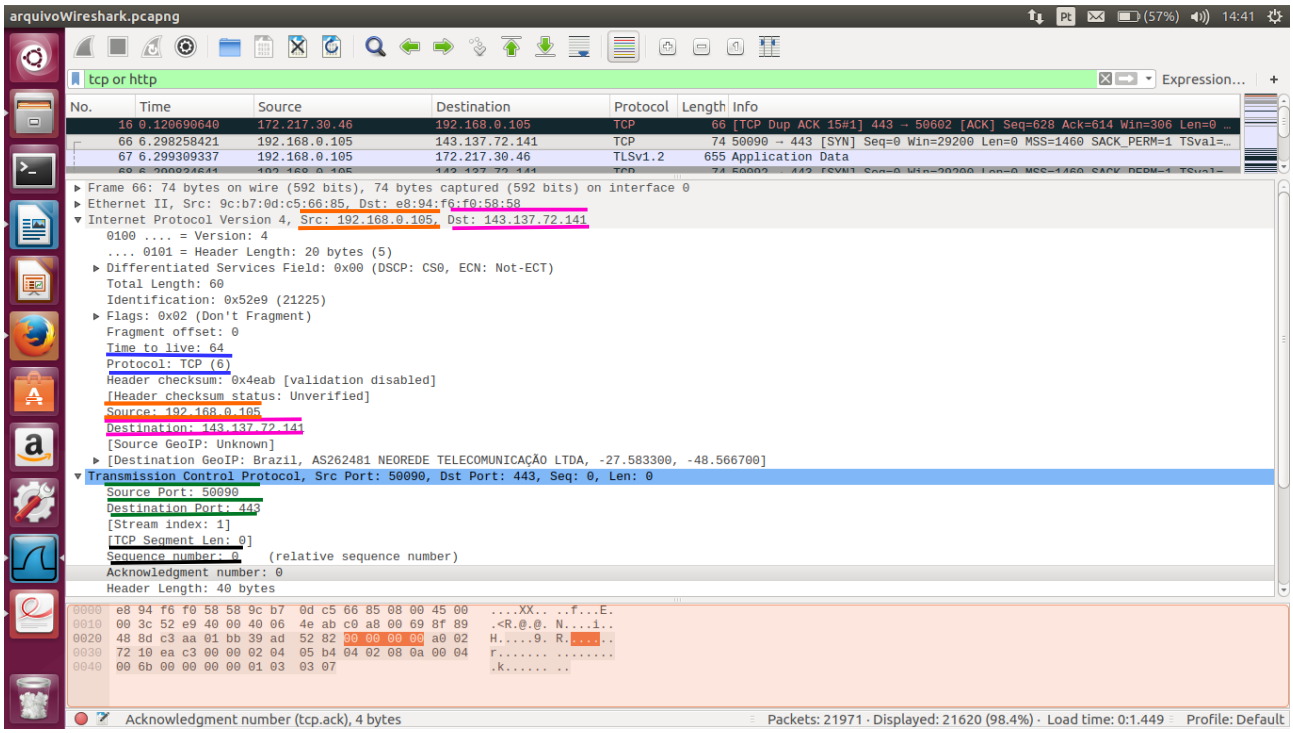

Figura 2: Primeiro Passo

Legenda:

Origem do Pedido, Cliente

Destino do Pacote, Servidor

Protocolo Usado

Portas Usadas pela Camada de Aplicação TCP/IP

Valor da Flag [SYN]

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

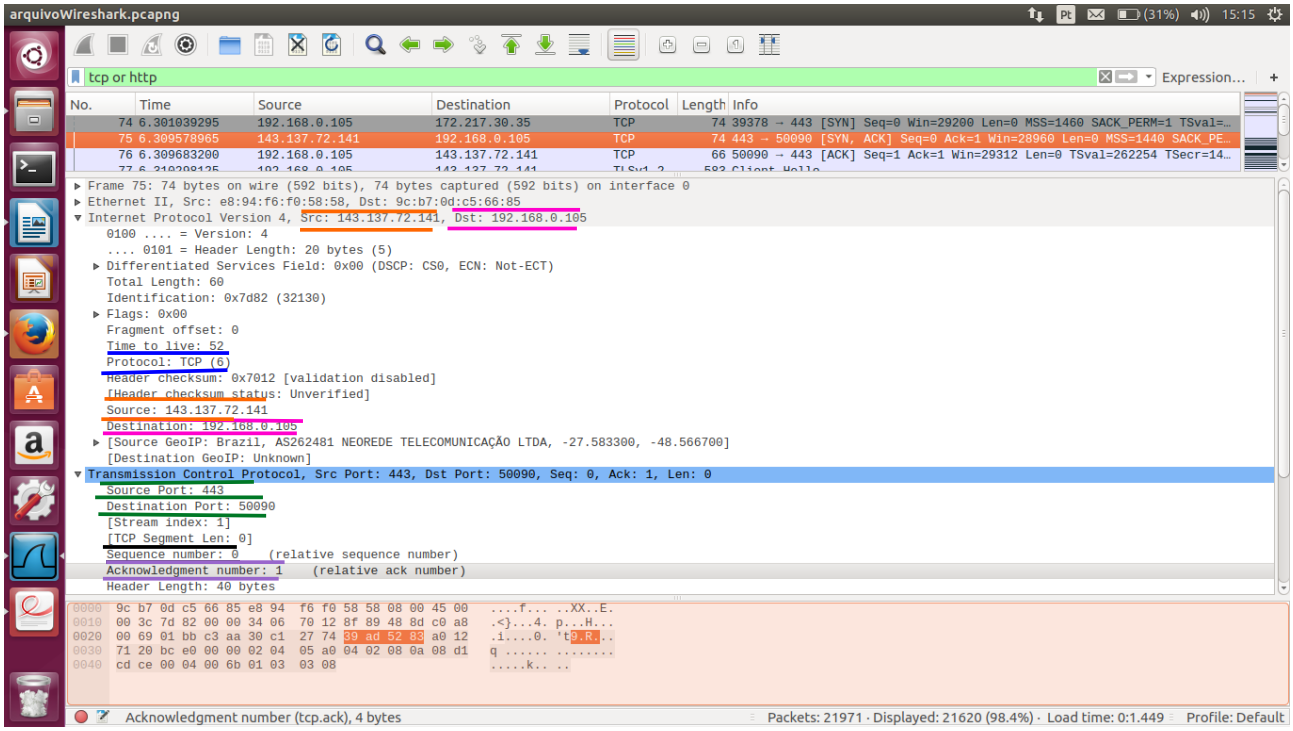

Figura 3: Segundo Passo

Legenda:

Origem do Pedido, Cliente

Destino do Pacote, Servidor

Protocolo Usado

Portas Usadas pela Camada de Aplicação TCP/IP

Valor da Flag [SYN]

Valor da Flag [ACK]

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

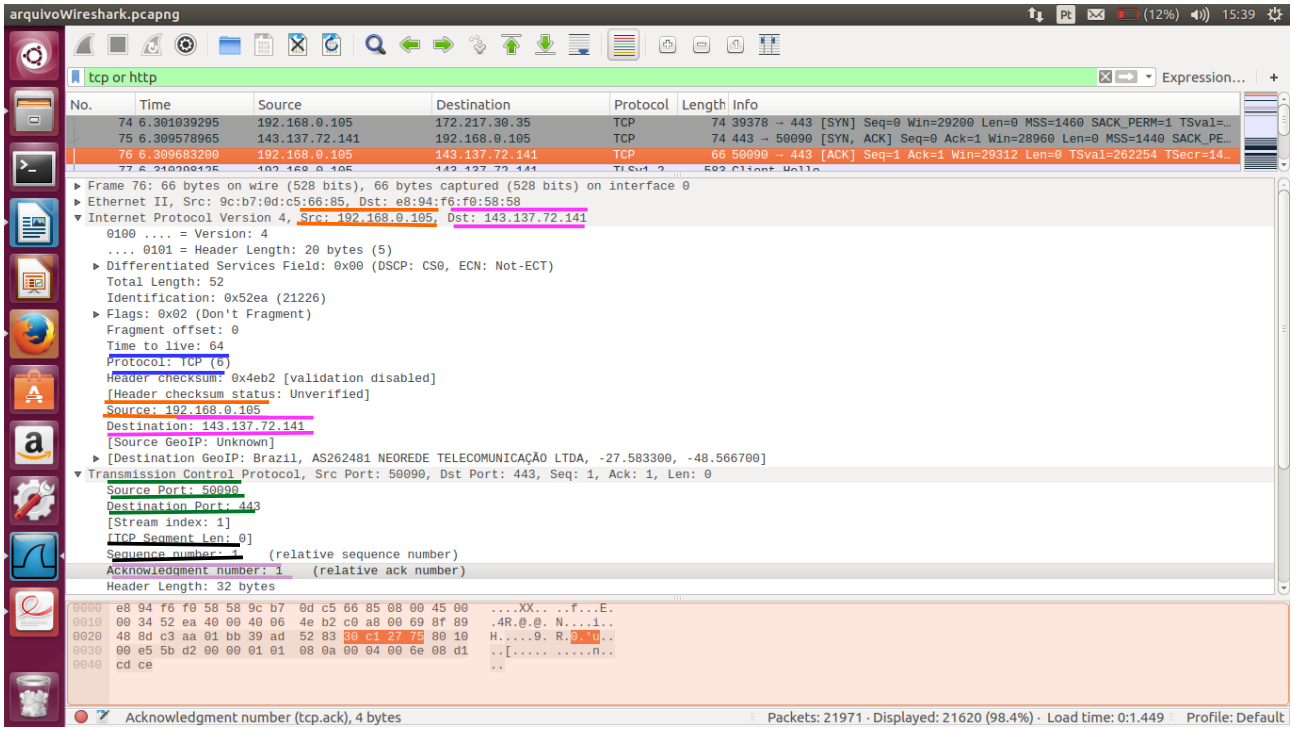

Figura 4: Terceiro Passo

Legenda:

Origem do Pedido, Cliente

Destino do Pacote, Servidor

Protocolo Usado

Portas Usadas pela Camada de Aplicação TCP/IP

Valor da Flag [SYN]

Valor da Flag [ACK]

2.2 Transferência de dados

O TCP/IP é o principal protocolo de envio e recebimento de dados. TCP significa Transmission Control Protocol (Protocolo de Controle de Transmissão) e o IP, Internet Protocol (Protocolo de Internet). Na realidade, o TCP/IP é um conjunto de protocolos. Esse grupo é dividido em quatro camadas: aplicação, transporte, rede e interface. Cada uma delas é responsável pela execução de tarefas distintas. Essa divisão em camadas é uma forma de garantir a integridade dos dados que trafegam pela rede.

A camada é utilizada pelos programas para enviar e receber informações de outros programas através da rede. Nela, você encontra protocolos como SMTP (para email), FTP (transferência de arquivos) e o famoso HTTP (para navegar na internet).

A camada de transporte é responsável por receber os dados enviados pelo grupo acima, verificar a integridade deles e dividi-los em pacotes. Depois essas informações são enviadas a camada de rede.

Na rede, os dados empacotados são recebidos e anexados ao endereço virtual (IP) do computador remetente e do destinatário. Agora é a vez dos pacotes serem, enfim, enviados pela internet. Para isso, são passados para a camada interface.

A tarefa da interface é receber e enviar pacotes pela rede. Os protocolos utilizados nessa camada dependem do tipo de rede que está sendo utilizado. [6]

Um sistema de comunicação em rede possui diversos protocolos que trabalham em conjunto para o fornecimento de serviços. Para que o protocolo HTTP consiga transferir seus dados pela Web, é necessário que os protocolos TCP e IP tornem possível a conexão entre clientes e servidores através de sockets TCP/IP. [7]

Assim que estabilizada a comunicação entre o navegador, o Firefox, e o servidor do youtube. Como ocorre no pacote 21894, que é HTTP. Dando dois cliques sobre ele é possível verificar esse detalhes. (Figura 5 e 6)

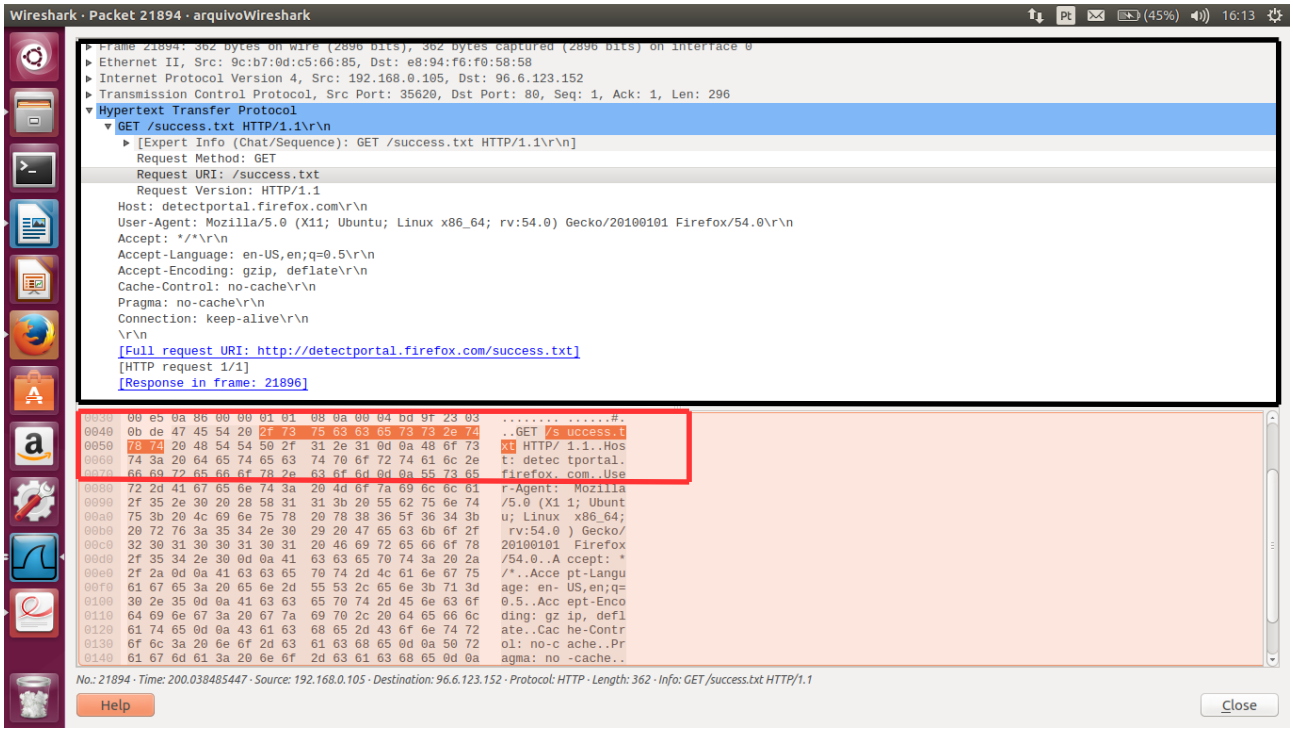

Figura 5: Página com informações do pacote. Obs.: Quando selecionado alguma linha de comando do pacote (dentro do quadro superior), na divisão inferior da página é destacado da informação do conjunto, em hexadecimal.

Figura 6: Conjunto de Informações sobre o Pedido, o Cliente e o Servidor

Legenda:

- *Método*
- *URL*
- *Protocolo Utilizado*
- *Versão do Protocolo*

O código de requisição identifica o estado em que foi correspondido o pedido. Quando concluída com sucesso é 200; ou se não existe, 404; ou se não houver conteúdo, 204; além de muitos outros. [1] O campo de rubricas é onde há informações suplementares sobre a resposta e ou sobre o servidor. Já o corpo de resposta que contem o conteúdo pedido.
A resposta onde o código de requisição é 200, está citada a seguir no pacote 21896:

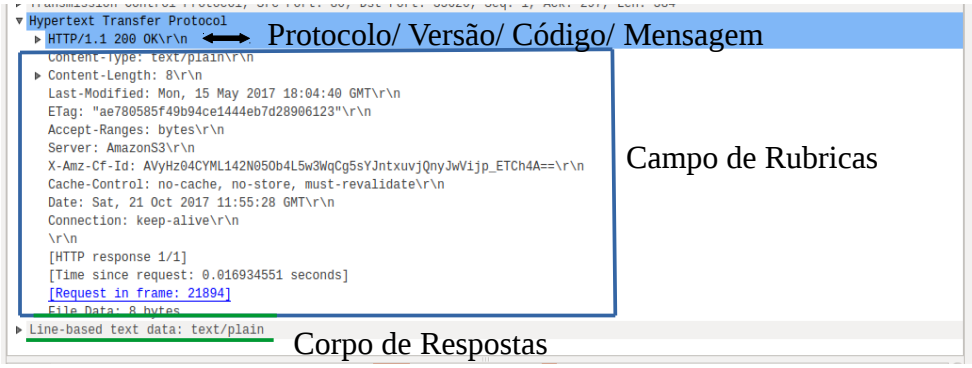

Figura 7: Exemplo de Resposta, pacote 21896

2.3 Finalização da conexão

Embora o estabelecimento da conexão exija três pacotes a serem transmitidos através de nossa mídia em rede, o término de uma conexão confiável exigirá a transmissão de quatro pacotes. Como uma conexão TCP é full duplex (ou seja, os dados podem fluir em cada direção independentemente do outro), cada direção deve ser encerrada independentemente.[4] Como acontece neste exemplo:

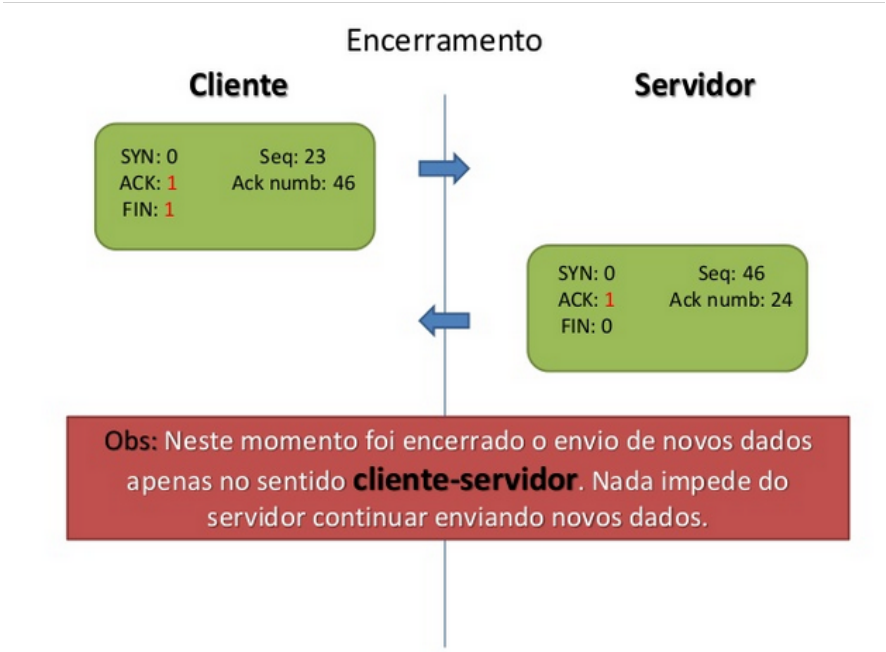

Figura 8: Primeira parte do exemplo. Imagem[5]

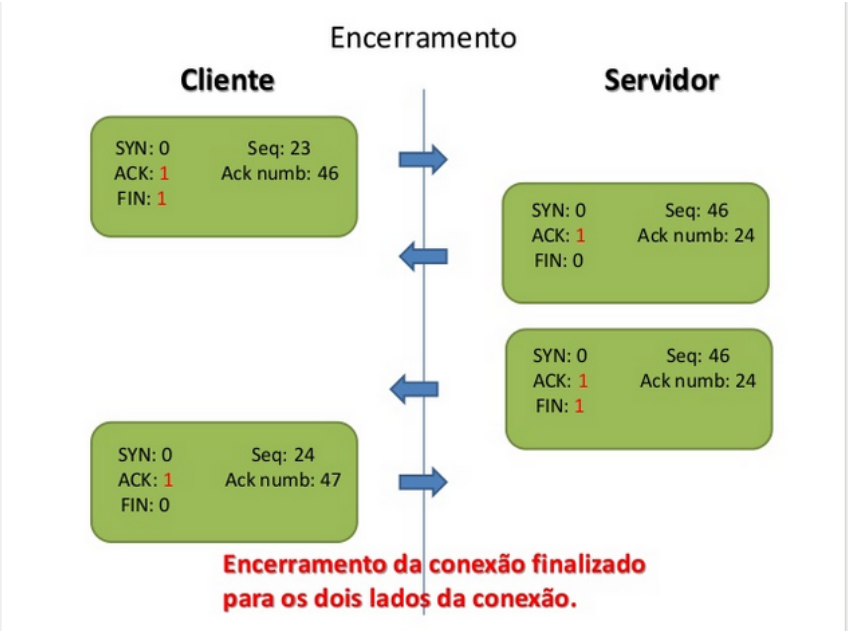

Figura 9: Segunda parte do exemplo. Imagem[5]

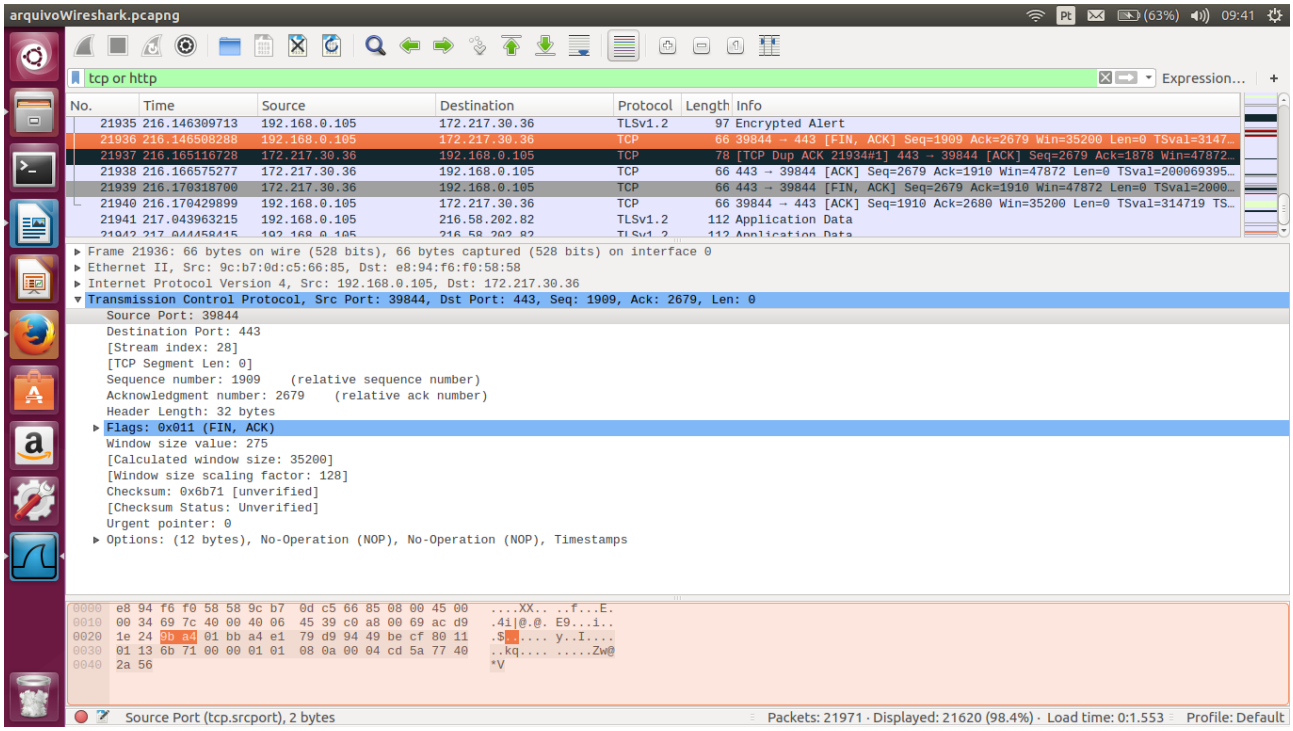

Figura 10: O cliente envia um FIN que é acompanhado por um ACK. Isto possui duas funções básicas. Primeiro, quando o parâmetro FIN está configurado, informará o servidor que não tem mais dados para enviar. Em segundo lugar, o ACK é essencial para identificar a conexão específica que estabeleceram.[4]

Exemplo da finalização da conexão em quatro pacotes coletados pelo wireshark:

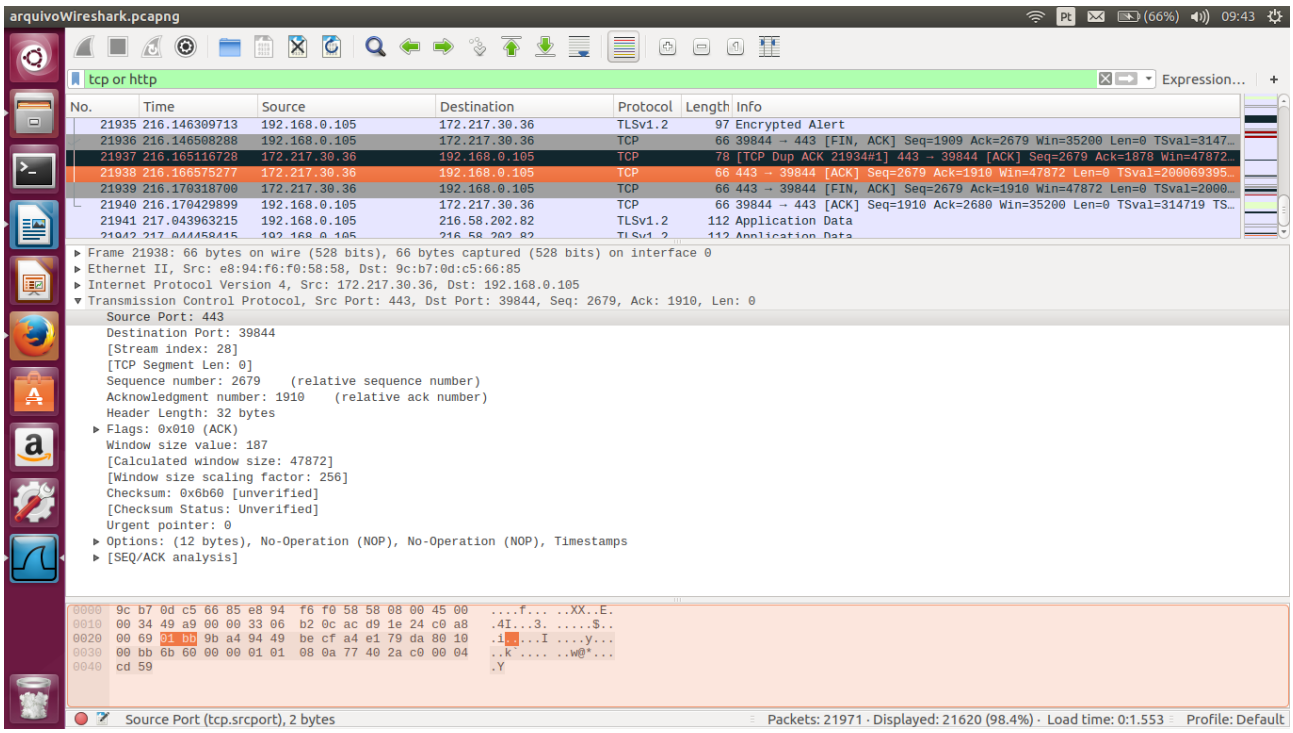

Figura 11: Não há nada especial, exceto para o servidor reconhecendo o FIN que foi transmitido pelo cliente.[4]

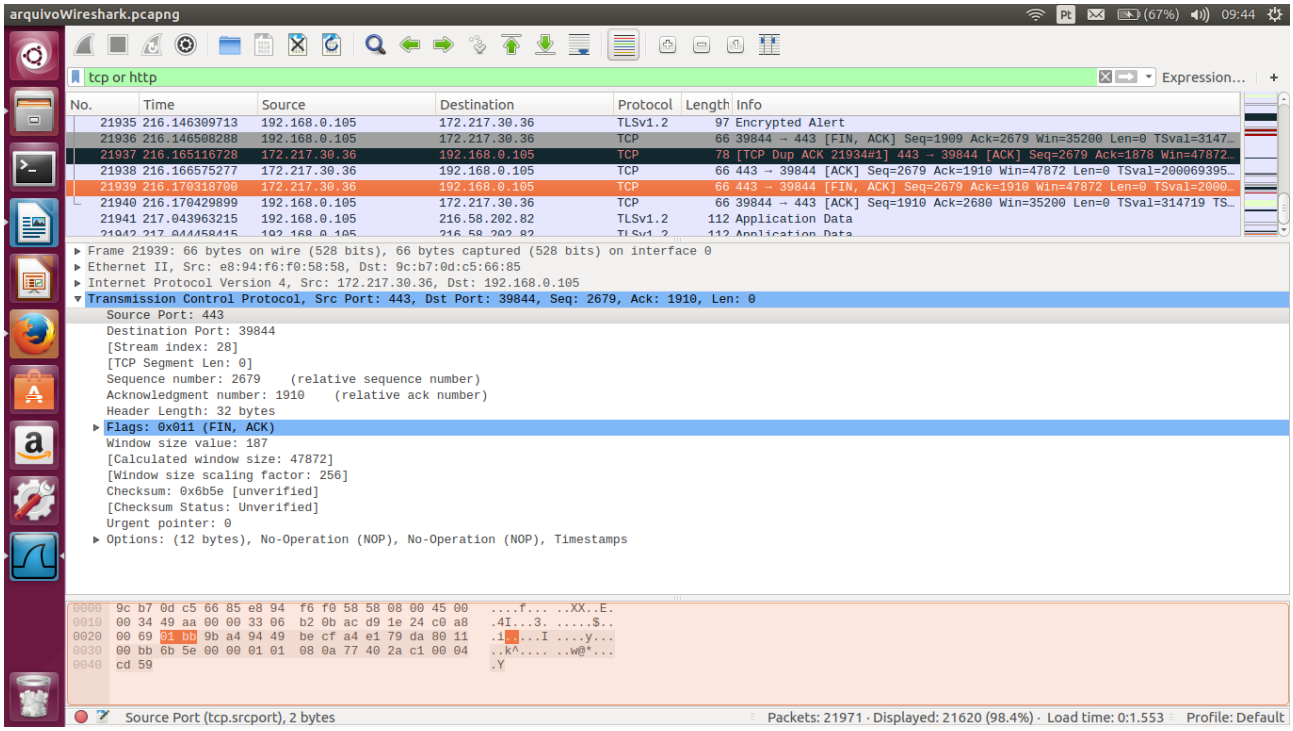

Figura 12: Depois de receber o FIN do computador cliente, o servidor enviará ACK. Embora a TCP tenha estabelecido conexões entre os dois computadores, as conexões ainda são independentes uma da outra. Portanto, o servidor também deve transmitir um FIN para o cliente. [4]

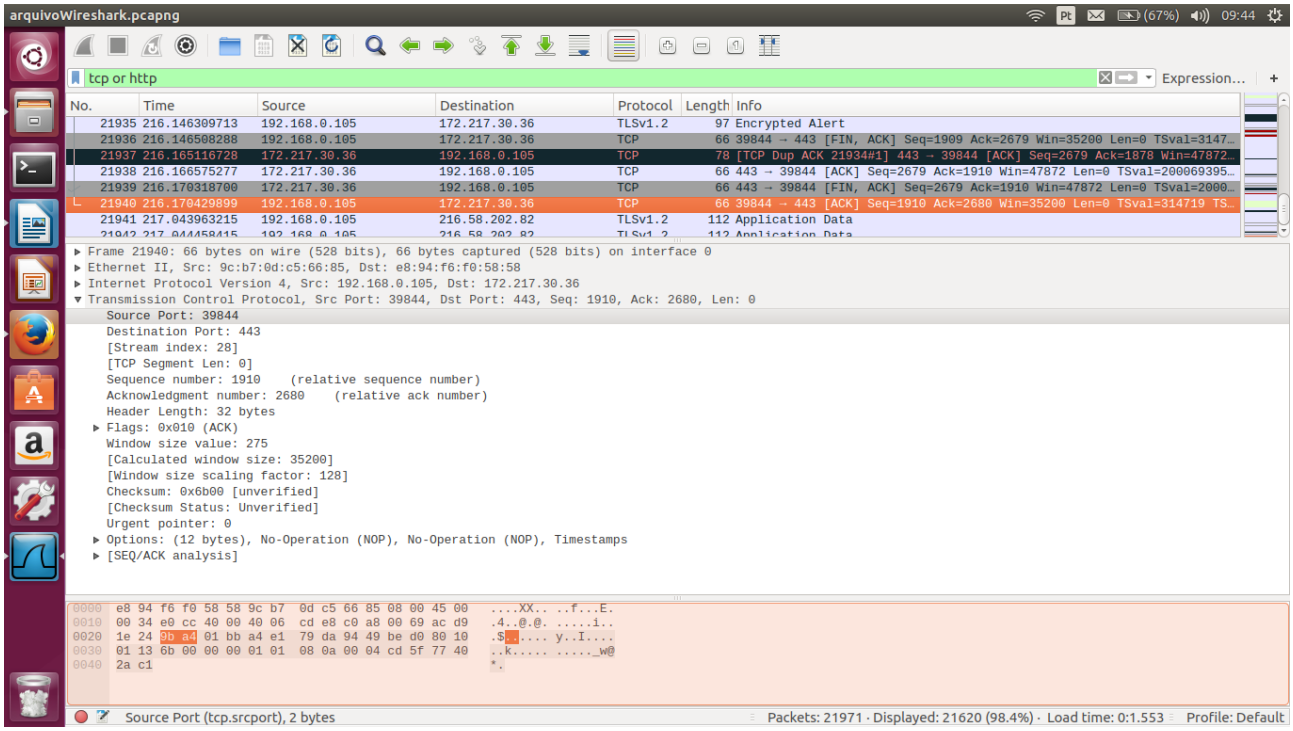

Figura 13: O cliente responde no mesmo formato que o servidor, ACABANDO o FIN do servidor e incrementa o número de seqüência em 1.[4]

3. Conclusão

O uso da ferramenta Wireshark, bem como do protocolo HTTP, junto com o TCP, permitiu a experiência prática e uma maior conhecimento da gerência de redes e desses protocolos utilizados. Além de conhecer o funcinamento dos protocolos citados, também aprenDi sobre a necessidade de utilizar mais de um protocolo para melhor estruturação do modelo OSI. Assim este trabalho trouxe um esclarecimento prático da importância de uma rede para o mundo atual onde cada vez mais dispositivos estão conectados a ela, além de aprender a manusear uma ferramenta que fazem o controle da rede.

4. Referências bibliográficas

[1] Disponível em : <https://en.wikipedia.org/wiki/List_of_HTTP_status_codes>. Acesso em: Outubro de 2017

[2] Disponível em : <https://pt.wikibooks.org/wiki/Redes_de_computadores/Protocolo_TCP>. Acesso em: Outubro de 2017

[3] Disponível em : <http://www2.ufba.br/~romildo/downloads/ifba/transporte.pdf>. Acesso em: Outubro de 2017

[4] Disponível em : <https://support.microsoft.com/en-us/help/172983/explanation-of-the-three-way-handshake-via-tcp-ip>. Acesso em: Outubro de 2017

[5] Disponível em : <https://pt.slideshare.net/LuisOctavioMoraes/estabelecimento-e-encerramento-de-conexo-tcp-17141076>. Acesso em: Outubro de 2017

[6] Disponível em : <https://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-.htm>. Acesso em: Outubro de 2017

[7] Disponível em : <https://www.oficinadanet.com.br/artigo/459/o_protocolo_http>. Acesso em: Outubro de 2017