Universidade Estadual da Paraíba
Departamento de Matemática, Estatística e Computação
Disciplina: Redes de Computadores
Professor: Edmar José do Nascimento

1º Exercício Prático: Usando o Wireshark (Ethereal)

Introdução

Uma das formas de estudar protocolos de redes de computadores é através de simulações ou vê-los funcionando na prática. Nesta atividade, vamos utilizar um software chamado de *Wireshark* (as versões anteriores eram chamadas de *Ethereal*) [1] para ver os protocolos na prática através da observação dos pacotes trocados entre os hospedeiros quando esses protocolos estão em funcionamento.

Para que possamos observar as mensagens trocadas na execução dos protocolos devemos capturar os pacotes que transportam essas mensagens, e para isso usamos um artifício chamado de farejador de pacotes (*packet sniffer*). Esse tipo de artifício normalmente é implementado em um software que roda em uma máquina e captura todos os pacotes enviados e recebidos por essa máquina, mesmo que não seja destinado a ela. Em seguida, pode-se observar o conteúdo dos pacotes capturados.

É importante observar que um farejador de pacotes tipicamente é passivo, ou seja, normalmente ele não insere qualquer pacote na rede. Além disso, os pacotes capturados não são endereçados ao farejador de pacotes, são uma cópia dos pacotes que são enviados ou recebidos na máquina em que esse software está sendo executado.

A Figura 1 apresenta a estrutura de um aspirador de pacotes, que consiste basicamente de uma biblioteca de captura de pacotes que é responsável por copiar todos os quadros da camada de enlace e de um analisador de pacotes que mostra o conteúdo de todos os campos da mensagem.

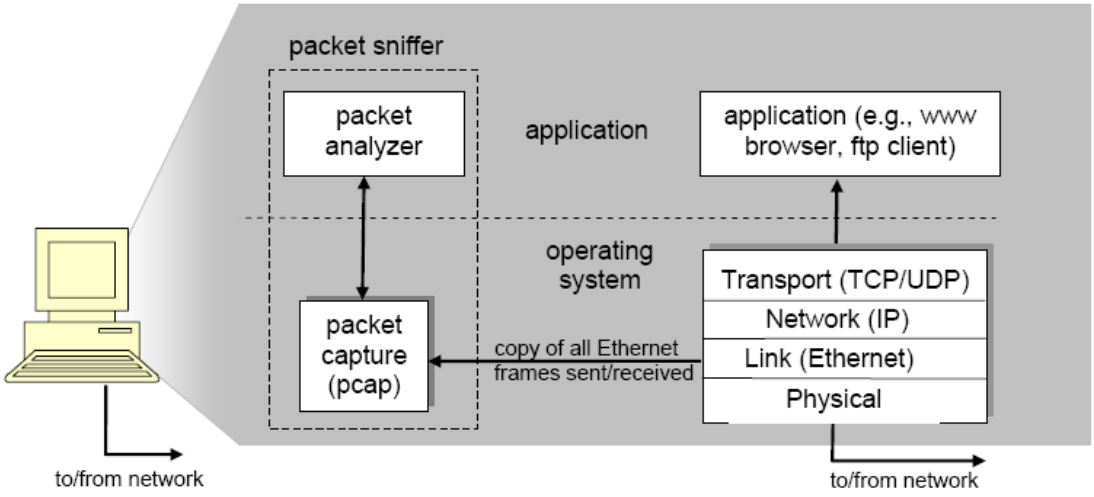

Figura 1 - Estrutura de um Farejador de Pacotes

Nós usaremos o aspirador de pacotes *Wireshark* [1]. Estritamente falando o Wireshark é um analisador de pacotes que usa uma biblioteca de captura de pacotes no seu computador.

Executando o Wireshark

Ao executar o *Wireshark* no Windows, a interface gráfica mostrada na Figura 2 é apresentada. Inicialmente nenhum dado é mostrado.

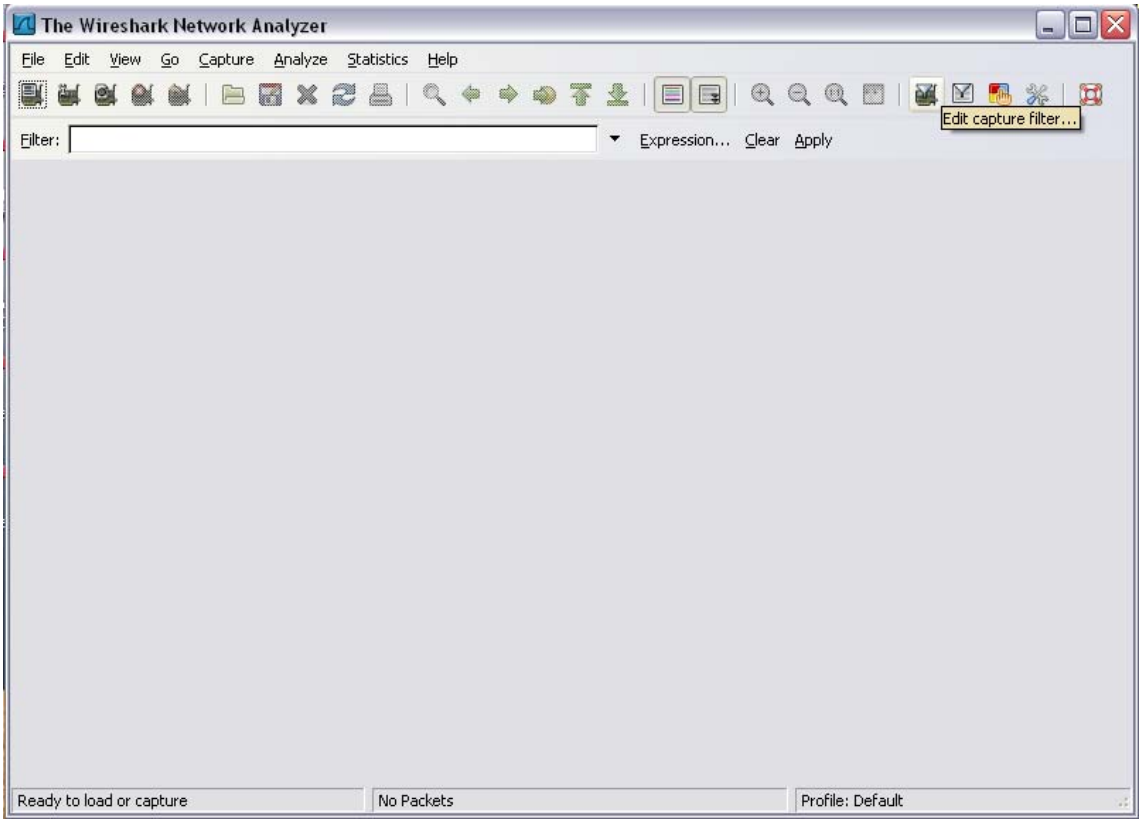

Figura 2 - Tela inicial do Wireshark

Testando o Wireshark

Siga os seguintes passos para testar o funcionamento desse software:

1. Inicie seu navegador web preferido e selecione uma página de sua preferência.
2. Inicie o *Wireshark*. Você verá uma tela como a que está mostrada na Figura 2, pois o software ainda não começou a capturar os pacotes.
3. Para começar a capturar os pacotes, selecione *Options* no menu *Capture*. Será mostrada uma tela como a que está representada na Figura 3, na qual pode-se escolher dentre outras opções qual a interface a ser monitorada. Isso é feito, pois a máquina que você está pode ter mais de uma interface (placa de rede), por exemplo, uma via rede cabeada e outra rede sem fio. Selecione uma das interfaces em seguida clique em *Start*. Isto fará que com que os pacotes que passam por essa interface sejam capturados.

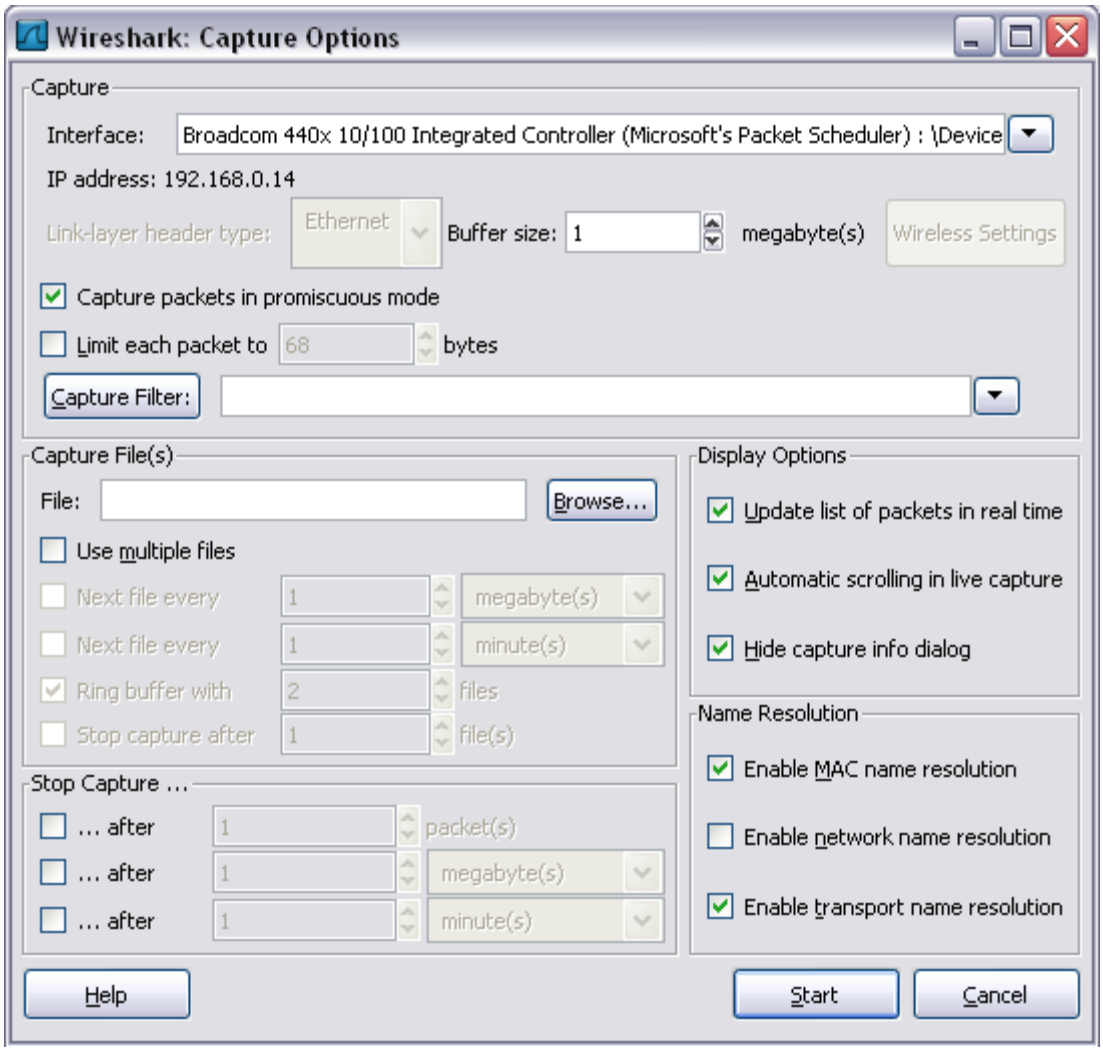

Figura 3 - Tela de configuração de captura de pacotes

4. Ao clicar em *Stop*, a captura é interrompida. Para obter estatísticas sobre os pacotes capturados, clique em *Statistics -> Protocol Hierarchy*.
5. Interrompida a captura de pacotes, uma lista dos pacotes capturados é apresentada na tela do Wireshark, assim como está representado na Figura 4.

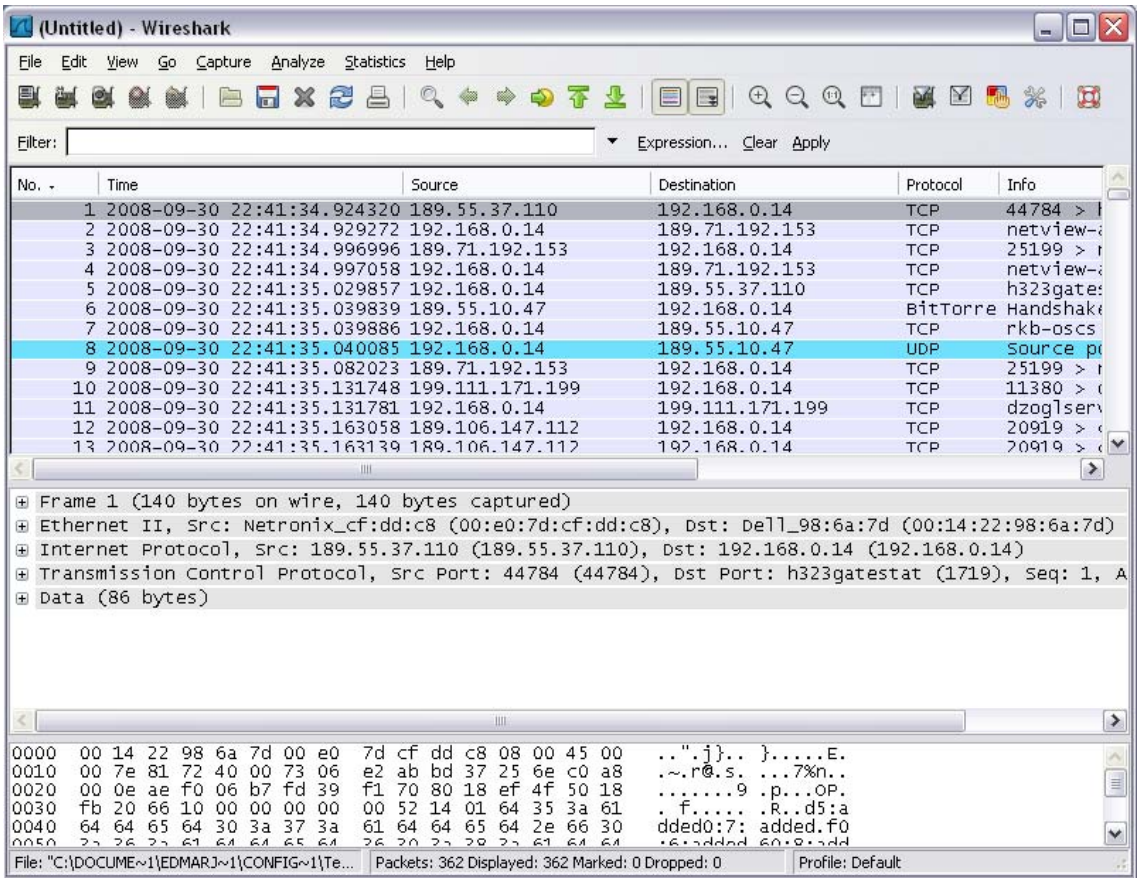

Figura 4 - Pacotes capturados

6. Vamos filtrar os pacotes capturados. Para isso, no campo *Filter* digite *http* e selecione *Apply*. Agora temos somente os pacotes trocados em mensagens *http*;
7. Selecione a primeira mensagem na lista de mensagens, na janela logo abaixo da lista de pacotes são mostrados os dados relativos ao cabeçalho do pacote selecionado. Cada um dos dados apresentados tem detalhes que podem ser observados clicando em + ao lado do seu nome.
8. Na última janela do Wireshark tem-se o conteúdo do pacote em hexadecimal.
9. Para terminar, saia do Wireshark.