Universidade Federal de Campina Grande

Unidade Acadêmica de Engenharia Elétrica

Disciplina: Redes de Computadores

Professor: Edmar Candeia Gurjão

1º Exercício Prático: Usando o *Wireshark*[1]

1. Introdução

Uma das formas de estudar protocolos de redes de computadores é através de simulações ou vê-los em funcionamento. Neste "laboratório" vamos utilizar um software chamado de *Wireshark* [1], para ver os protocolos em funcionamento pela observação dos pacotes trocados entre as máquinas 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 aspirador de pacotes[2] (*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, mesmo que não sejam destinados a ela. Em seguida, pode-se observar o conteúdo dos pacotes capturados.

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

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.

---

[1] Os experimentos aqui apresentados foram obtidos em http://www.prenhall.com/kurose_br/ e consistem de uma tradução feita por Edmar Candeia Gurjão.

[2] Tradução feita por Edmar Candeia Gurjão

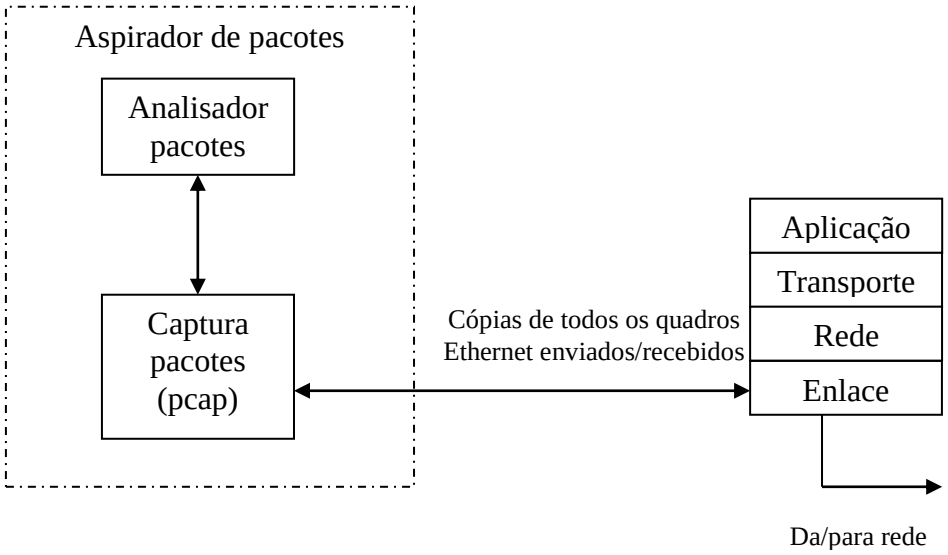

Figura 1 – Estrutura de um analisador de pacotes.

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

2. Obtendo o *Wireshark*

Para executar o *Wireshark* você precisa acessar um computador em que esse software esteja instalado junto com a biblioteca de captura de pacotes *libpcap*. Normalmente o instalador do *Wireshark* já vem com o *libpacap* embutido. Esse software está disponível em http://www.wireshark.org/ onde pode ser obtido gratuitamente. O processo de instalação é simples e segue os mesmos procedimentos dos instaladores de outros softwares para Windows ou Linux.

3. Executando o *Wireshark*

Ao executar o *Wireshark* no Windows[3], a interface gráfica mostrada na Figura 2 é apresentada. Inicialmente nenhum dado é mostrado.

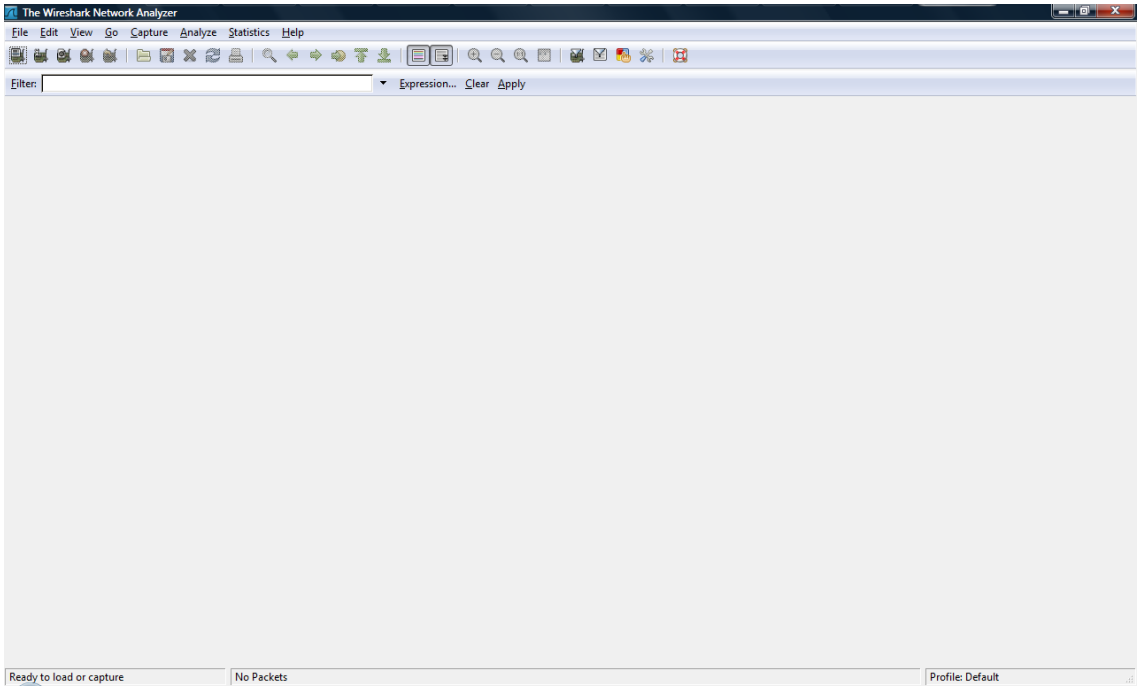

Figura 2 – Tela inicial do *Wireshark.*

4. 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 para rede

[3] Os exemplos serão baseados no sistema operacional Windows, mas o mesmo pode ser feito no Linux.

cabeada e outra para 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.

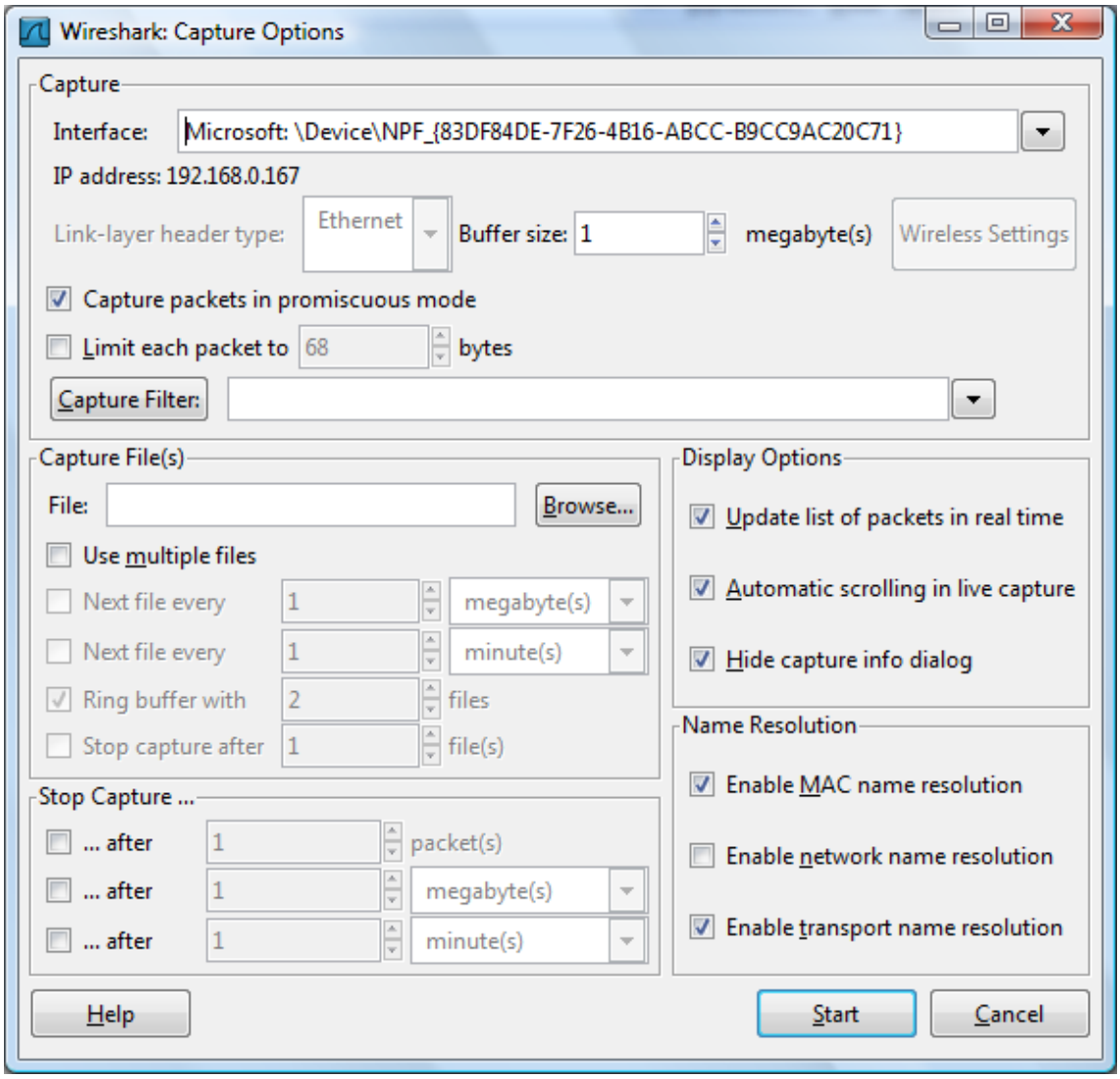

Figura 3 – Tela para configuração de captura de pacotes.

4. Uma vez iniciada a captura uma tela de resumo das quantidades dos pacotes capturados é apresentada. Ao clicar em *Stop* (botão na barra de ferramentas) a captura é interrompida.

5. Interrompida a captura de pacotes, uma lista dos pacotes capturados é apresentada na tela do *Wireshark*, Como está representado na Figura 4.

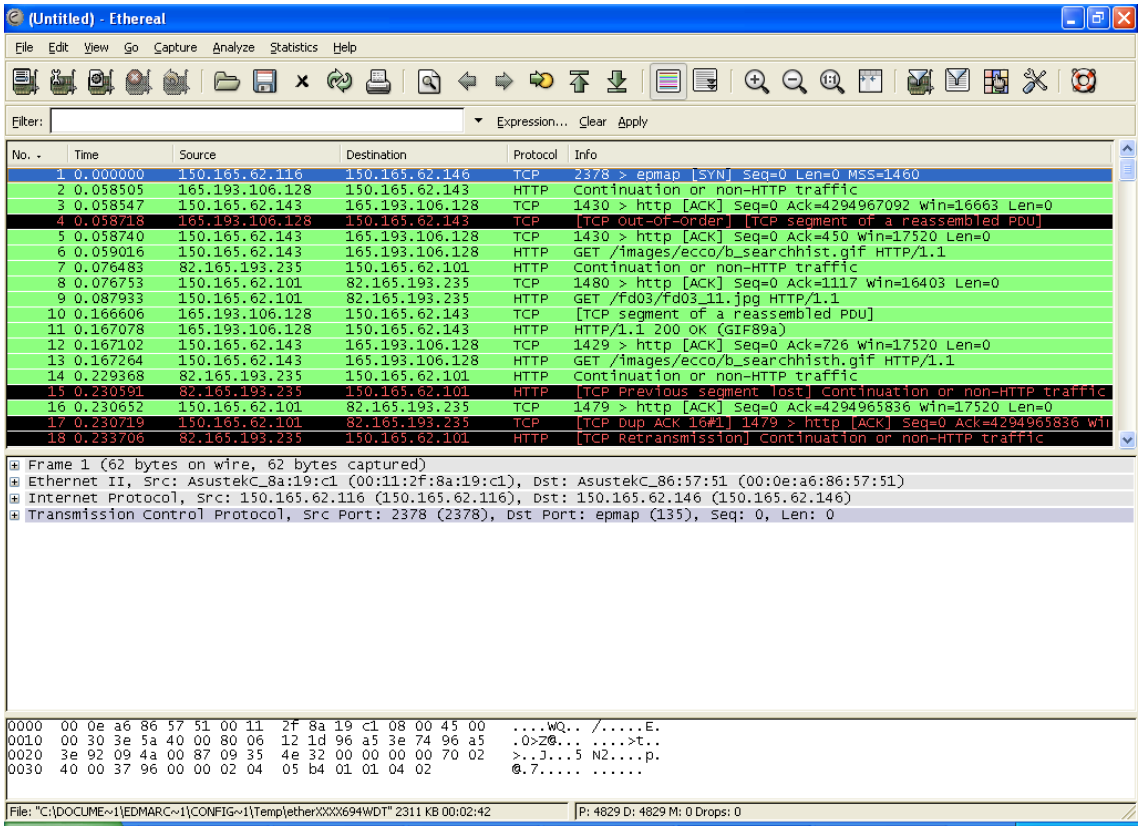

Figura 4 – Tela do *Wireshark* com todos os pacotes capturados.

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 a lista de pacotes são mostrados os dados relativo 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*.

Referências

[1] http://www.wireshark.org/