INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RN
DISCIPLINA: REDES DE COMPUTADORES
PROFESSORES: SORAYA CHRISTIANE/ TADEU FERREIRA
TÉCNICO NÍVEL MÉDIO EM INFORMÁTICA

Lab1 – Conhecendo o Wireshark

Introdução

O wireshark é uma ferramenta de análise de pacotes de rede, ele é capaz de capturar pacotes em uma rede e exibi-los de forma detalhada através de vários filtros já disponíveis na ferramenta e usando filtros criados pelo usuário.
O wireshark é disponibilizado na licença GNU, ou seja é um software open-source, disponível em várias plataformas (Windows, Mac, Linux, BSD). Ele pode ser obtido do site oficial dos desenvolvedores (http://www.wireshark.org) ou instalado usando o synaptic no Ubuntu.

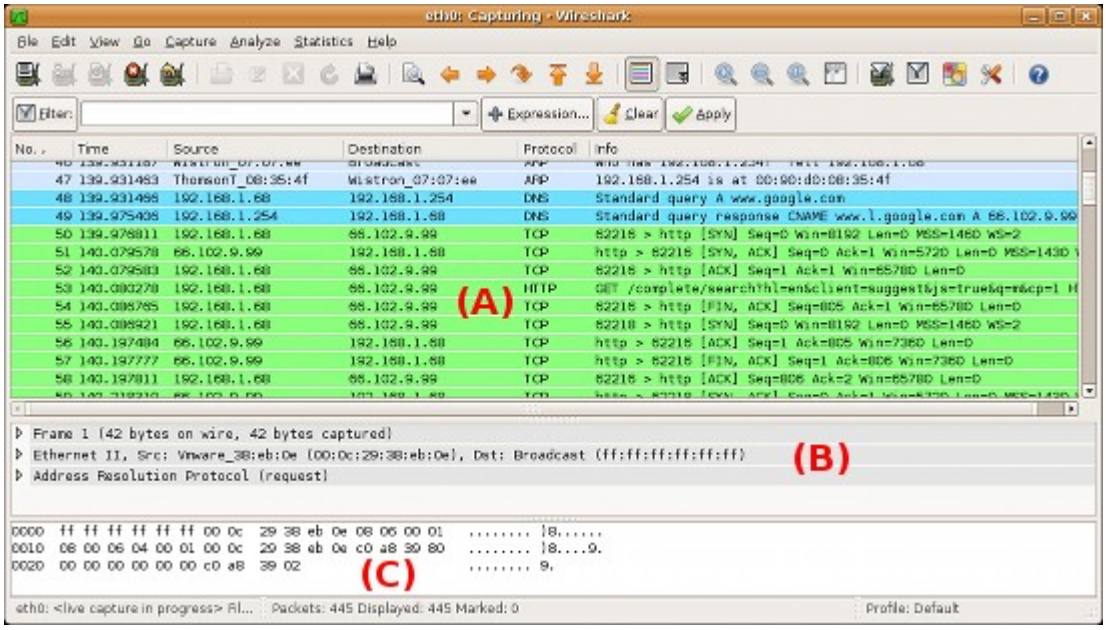

Figura 1: Interface do Wireshark 1.4

Instalação

No windows é ncessário fazer o download do wireshark no site: http://www.wireshark.org na seção download selecionar Windows Installer.
No linux a maioria das grandes distribuição já disponibiliza o wireshark como um pacote, no ubuntu na linha de comando use: **`sudo apt-get install wireshark`** para instalar.

A interface

A interface do wireshark é dividida em 3 painéis o painel superior (A) exibe uma lista de todos os pacotes capturados até o momento. Cada linha representa um pacote capturado na rede. Ao selecionar um pacote no painel superior o painel central (B) exibe o conteúdo do pacote separado por camadas/protocolos. No terceiro painel (C) é possível ver o conteúdo do pacote no formato hexadecimal e o conteúdo em formato de texto.

No painel superior há 6 colunas com informações sobre o pacote em questão:

- **No.:** Um número sequencial dos pacotes capturados pelo wireshark

- **Time:** Momento em que o pacote foi capturado.
- **Source:** Ip ou endereço MAC de origem do pacote
- **Destination:** Ip ou endereço MAC de destino do pacote
- **Protocol:** O protocolo que está sendo usado neste pacote (exibirá o protocolo de mais alto nível. Ex.: se um pacote usa o protocolo TCP e HTTP será exibido HTTP pois este está mais acima no modelo de camadas)
- **Info:** Um resumo das informações que podem ser relevantes para aquele tipo de pacote.

Capturando Pacotes no Wireshark

A primeira coisa a fazer no uso do wireshark é selecionar a interface que se deseja monitorar, para isso clique no ícone da placa de rede com uma lista, (o primeiro da barra de ferramentas) será exibida a tela com a lista de placas de rede da máquina.

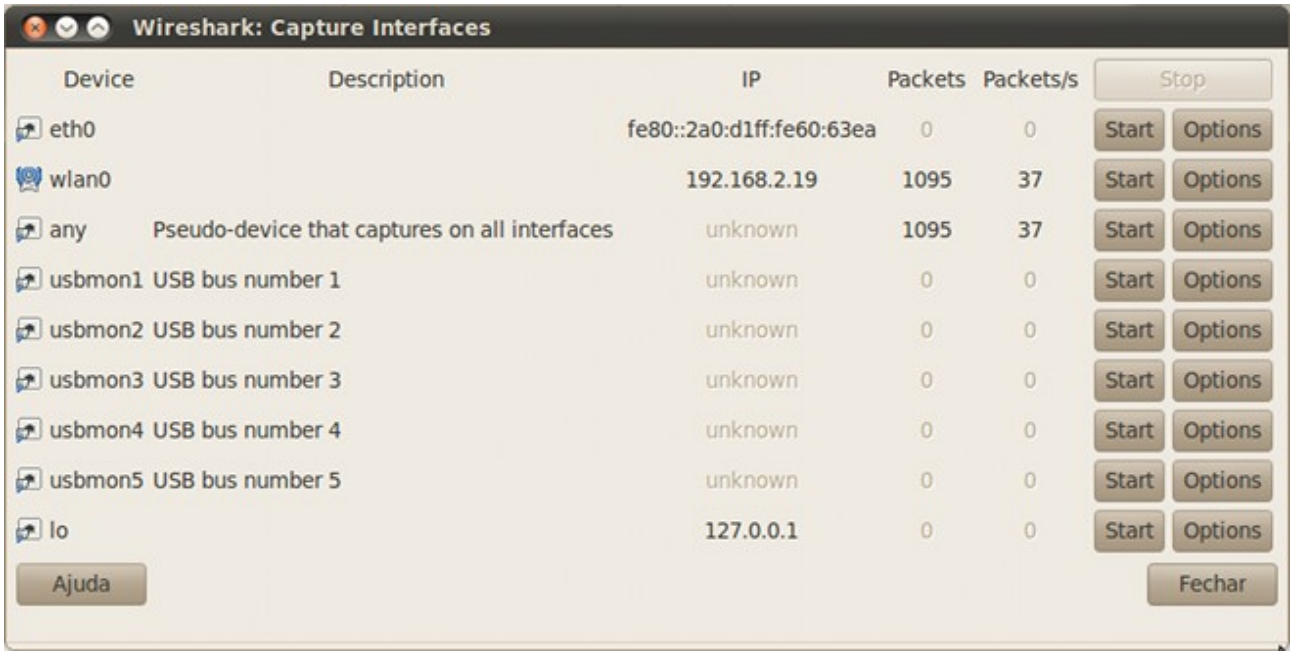

Figura 2: Lista das placas de rede disponíveis

Selecione a placa que deseja usar na captura de pacotes clicando em **Start**. Isto iniciará a captura de todo tipo de pacote que passe pela placa de rede.

Para terminar a captura de pacotes clique no ícone com o X branco e vermelho.

É possível salvar os pacotes capturados para análise posterior usando **`File => Save`**. Será gerado um arquivo *.cap* que pode ser mais tarde aberto para análise usando o wireshark ou outras ferramentas.

Para mais informações acesse: http://www.wireshark.org/docs/