INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

**Professor: Macêdo Firmino**
**Disciplina: Redes de Computadoores**
**Prática 01: Análise da troca de pacotes na rede**

---

Olá turma bonita, hoje iremos ter a nossa primeira aula prática da Disciplina. Inicialmente iremos conhecer um *software* de análise de tráfego, chamado de Wireshark, que pode ser obtido gratuitamente em: `http://www.wireshark.org`. Depois iremos analisar e entender como acontece o empacotamento dos protocolos da plha TCP/IP.

### Wireshark

O Wireshark é um programa (conhecido como *sniffer*) que verifica os pacotes transmitidos pelo dispositivo de comunicação (placa de rede, placa de fax modem, etc.) do computador. O programa analisa o tráfego de entrada e saída e organiza-os por protocolo. Ele é suportado nas plataformas Unix, Linux, Solaris, FreeBSB, NetBSD, OpenBSD, Mac OS X e Windows.

Exemplos de utilização do Wireshark:

- Administradores de rede utilizam para solucionar problemas de rede;
- Engenheiros de segurança de rede usá-lo para examinar problemas de segurança;
- Desenvolvedores utiliza para depurar implementações do protocolo;
- Pessoas que precisam aprender o protocolo de rede;

A imagem a seguir, que exemplifica alguns pacotes sendo capturados ou carregados, servirá de base para uma breve descrição dos elementos contidos na janela principal do Wireshark.

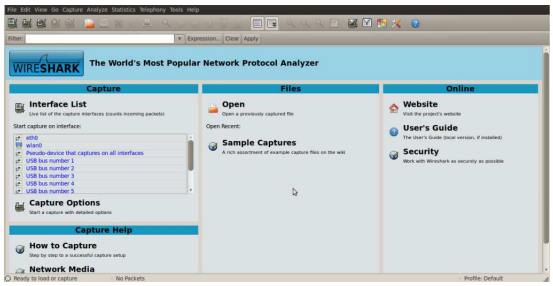


Figura 1: Janela Principal do Wireshark

- O *menu* é usado para iniciar ações;
- A Barra de Ferramentas Principal fornece um rápido acesso aos itens que são frequentemente usados;
- A Ferramenta Filter fornece um campo para manipular diretamente o que será exibido pelo filtro;
- O Painel de Lista dos Pacotes exibe um resumo de cada pacote capturado. Clicando sobre um deles é possível controlar o que será mostrado nos painéis subsequentes;
- O Painel de Detalhes dos Pacotes exibe maiores detalhes dos pacotes selecionados no Painel de Lista dos Pacotes;
- O Painel de Bytes dos Pacotes exibe os dados dos pacotes selecionados no Painel de Lista dos Pacotes e destaca o campo selecionado no Painel de Detalhes dos Pacotes;
- A Barra de Status mostra algumas informações detalhadas acerca do estado atual do programa e dos dados capturados.

Para começar a capturar os pacotes, selecione a interface de rede. Para isso selecione no *menu*: "Capture/Interfaces". Irá aparecer uma janela que permitirá a seleção da interface. Além, das opções que podem ser configuradas para a interface. Selecione a interface Ethernet e clique em "*start*".

A janela principal será preenchida com uma lista dos pacotes capturados. A janela é dividida normalmente em três seções: uma seção mostra a lista de pacotes capturados, uma outra seção mostra uma árvore de protocolo de um pacote selecionado e a última mostra os *bytes* do pacote.

Para selecionar os pacotes baseados no protocolo, basta digitar o nome do protocolo no qual você está interessado no campo *Filter* (Filtro) e pressione o botão "Apply" (aplicar) para iniciar o filtro. A Figura abaixo mostra um exemplo de filtragem sobre o protocolo TCP.

Ao selecionar um pacote específico capturado, podemos obter mais informações sobre os dados captados. Na parte inferior da tela do Wireshark, você pode ver os detalhes do pacote selecionado. Por exemplo, podemos facilmente encontrar a porta de destino TCP selecionando a entrada TCP e procurando a porta de destino. Quando selecionar este campo, a entrada nos bytes brutos do pacote é destaque também.

**Atividade**

**1.** Inicie o Wireshark;

**2.** Começe a captura de tráfego na rede;

**3.** Utilize a Internet normalmente (acesse sites, faça *downloads*, entre em chat, envie e-mails, etc.);

**4.** Pare a captura do Wireshark;

**5.** Liste 10 diferentes protocolos que aparecem na coluna de protocolos na lista de pacotes e informe quais camadas eles fazem parte.

**6.** Procure um datagrama IP (use o filtro ip) e escreve quais são os campos que compõem o cabeçalho.

**7.** Qual é o endereço IP do servidor www.ifrn.edu.br? Qual é o seu endereço IP?

**8.** Procure um segmento TCP (use o filtro tcp) e escreve quais são os campos que compõem o cabeçalho.

**9.** Procure um segmento UDP (use o filtro dns) e escreve quais são os campos que compõem o cabeçalho.

**10.** Acesse o site `www.ifrn.edu.br` e faça um filtro por http. Quanto tempo durou de quando a mensagem HTTP GET foi enviada até a resposta HTTP OK ser recebida? (Por default, o valor da coluna Time está descrita em segundos, desde que o trace Wireshark iniciou. Você pode mudar da forma que desejar no menu "View", selecionando "Time Display Format").