Wireshark
Analisador de Redes

Wireshark

- Conhecido anteriormente como Ethereal
- É um programa open-source
- É gratuito e disponível para várias plataformas:
  - Windows
  - Mac
  - Linux
- Pode ser baixado diretamente do site dos desenvolvedores: http://www.wireshark.org

Wireshark

- É um programa de análise de pacotes de rede
- O wireshark permite observar os pacotes que passam por uma máquina em detalhes
- Cada pacote é exibido em detalhes apresentando os dados divididos nas camadas segundo o modelo TCP/IP
- O wireshark é também conhecido como sniffer

Wireshark

- A tela principal do wireshark é dividida em 3 painéis:
  - Pacotes
    - Exibe todos os pacotes capturados
  - Descrição do pacote
    - Exibe as partes do pacote selecionado no painel superior
  - Dados em hexadecimal
    - Exibe o pacote o selecionado completo em formato hexadecimal

Painel dos pacotes

- 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.

Capturar pacotes

- O wireshark pode trabalhar em dois modos:
  - Modo normal
  - Modo promíscuo
- Modo Normal
  - Apenas os pacotes direcionados àquela placa de rede serão capturados
- Modo promíscuo
  - Todos os pacotes que passem pela placa de rede serão capturadores pelo wireshark

Modo promíscuo

- Captura os pacotes que não são direcionados à máquina
- Não faz milagres!
- Apenas os pacotes que passem pela máquina serão capturados

Atividade

- Utilize o wireshark para identificar um pacote saindo da sua máquina:
  - Descreva o conteúdo deste pacote
- Utilize o wireshark para identificar um pacote entrando na sua máquina:
  - Descreva o conteúdo deste pacote