

## Exercício WIRESHARK - Usando o Wireshark para analisar pacotes

### Preparativos iniciais

#### Instalando o Wireshark


- Apenas faça isto se o seu computador não tem o Wireshark instalado.
- Copie o Wireshark de <http://www.wireshark.org/download.html>
- Depois instale o Wireshark.

#### Anote o seu endereço IP

- Em alguns exercícios abaixo, você deverá informar o número IP da interface Ethernet do seu computador, o qual nos referiremos adiante como "seu IP".
- No windows, existem várias maneiras de saber qual o seu IP. Uma delas é abrir uma janela de comandos MS-DOS (Iniciar→Programas→Prompt do MS-DOS) e digitar o comando **IPCONFIG**. O seu IP está indicado como: "Endereço IP". Exemplo: 10.206.83.132.
- Faça isso agora e anote o seu IP para indicar quando solicitado.

### Exercício a – Capturando pacotes e salvando em um arquivo



1. Ative o Wireshark, clicando no ícone  que está no "Desktop" do windows.
2. Ative a captura de pacotes (Menu Capture→Start).
3. Na opção "interface", escolha a interface Ethernet que conecta o seu computador à rede.
4. Desabilite as opções "Enable MAC name resolution", "Enable network name resolution" e "Enable transport name resolution".
5. Pressione OK. Observe que agora existe uma "janela de captura" ativada.
6. Acesse a rede por alguns segundos (exemplo: acesse o site **www.ifpb.edu.br**). Não precisa demorar (basta acessar uma única página).
7. Pare a captura de pacotes clicando no botão **Stop** da janela de captura.
8. Salve os pacotes capturados (Menu File→Save As...) no arquivo **captura1.eth** (mantenha o diretório padrão=c:\redes\Wireshark)

### Exercício b – Fazendo filtros de visualização – Display Filter

Estabeleça alguns filtros de visualização (display filter). Atenção: alguns filtros podem não mostrar nenhum pacote, em função da atividade da rede naquele momento. Vamos ver como se faz isso:

1. Na parte inferior esquerda da janela do Wireshark, você pode ver um botão "Filter" com um espaço em branco ao lado dele.
2. Digite o filtro no espaço em branco (exemplo: **ip.addr==10.206.83.132 and http**)
3. Para ativar o filtro pressione ENTER.
4. Para desativar o filtro (antes de digitar outro), pressione no botão "Reset".
5. Os filtros devem ser digitados em letras minúsculas.

Atenção: Alguns filtros podem não mostrar qualquer pacote, porque nem todos os protocolos trafegam na rede a todo momento e portanto podem não ter sido capturados.

Construa filtros para as situações abaixo e anote as expressões usadas (dica: consulte as transparências do curso para ver como construir as expressões de filtragem):

1. Apenas pacotes do protocolo IPX
2. Apenas pacotes do protocolo DNS
3. Apenas pacotes do protocolo ARP
4. Apenas pacotes do protocolo HTTP
5. Apenas pacotes do protocolo SNMP
6. Apenas pacotes do protocolo UDP
7. Apenas pacotes do protocolo TCP
8. Apenas os pacotes HTTP enviados ou recebidos pelo seu host (forneça o seu IP)
9. Apenas pacotes do host **www.ifpb.edu.br** (Lembre-se: você deve informar o **endereço IP** desse host e não o nome. Descubra o número IP do desse host com o comando "ping **www.ifpb.edu.br**")
10. Todos os pacotes enviados ou recebidos pelo seu host (forneça o seu IP)

11. Todos os pacotes originados (enviados) pelo seu host.
12. Todos os pacotes UDP originados (enviados) pelo seu host.
13. Todos os pacotes TCP originados (enviados) pelo seu host.
14. Todos os pacotes UDP ou TCP recebidos ou enviados pelo seu host.
15. Descubra o IP de outro host do laboratório e mostre todos os pacotes trocados (enviados ou recebidos) por este host.
16. Mostre todos os pacotes trocados entre o host do exercício anterior e o servidor [www.ifpb.edu.br](http://www.ifpb.edu.br).

### Exercício c – Usando cores diferentes para diferenciar os pacotes

1. Desabilite o filtro de visualização (se houver), clicando no botão "Reset" (parte inferior da janela do Wireshark).
  2. Crie filtros de cores para os pacotes IPX, HTTP, DNS, ICMP e ARP mostrando-os com cores diferentes.
  3. Crie um filtro de cor para o fluxo de pacotes HTTP do seu host (use o mesmo filtro do exercício c.9). Escolha uma cor diferente das que já foram usadas.
  4. Após criar os filtros de cor, salve-os, para que permaneçam em outras sessões do Wireshark.
- Observação: Alguns protocolos de alto nível usam outros protocolos de baixo nível (exemplo: HTTP usa TCP, SNMP usa UDP, ...). Então se um pacote "casar" em mais de um filtro de cor, o filtro aplicado será o que tiver maior prioridade. Use os botões "Up" e "Down" para alterar a prioridade (os de cima têm mais prioridade).

### Exercício d – Capturando dados de uma sessão FTP

Vamos capturar uma sessão FTP (o FTP é uma aplicação que usa o protocolo de comunicação TCP para transferência de arquivos).

1. Desabilite o filtro de visualização (se houver), clicando no botão "Reset" (parte inferior da janela do Wireshark).
2. Ative a captura de pacotes (Menu Capture→Start). Escolha a interface Ethernet.
3. Desabilite as opções "Enable MAC name resolution", "Enable network name resolution" e "Enable transport name resolution".
4. Pressione OK. Observe que agora existe uma janela de captura ativada.
5. Abra uma janela de comandos MS-DOS (Iniciar→Programas→Prompt do MS-DOS).
6. Conecte-se via FTP com algum site. Exemplo: **ftp ftp.rnp.br**  
Atenção: Se o servidor FTP indicado no exemplo acima estiver fora do ar (não responde), tente um dos seguintes: **ftp3.usa.openbsd.org**, **ftp-linux.cc.gatech.edu**. Espera-se que um deles funcione.
7. Quando for solicitado o login, digite o login **anonymous** e a senha **eu@ifpb.edu.br**
8. Observe que a senha não aparece na tela.
9. Agora voce pode digitar comandos do FTP. Por exemplo, para ver os arquivos na máquina remota, digite do comando **ls**
10. Para sair digite **quit**
11. Pare a captura de pacotes (na janela de captura).
12. No Wireshark, filtre a visualização de pacotes usando o seguinte critério: apenas pacotes FTP do host ENDERECO-IP, onde ENDERECO-IP é o número IP do seu host. Ou seja, supondo que seu IP é 10.206.83.132, voce deve digitar o seguinte filtro: **ftp and ip.addr==10.206.83.132**
13. Salve os pacotes no arquivo **ftp.eth**

### Exercício e – Visualizando a senha da sessão FTP do exercício anterior

Quando digitamos a senha (eu@ifpb.edu.br) para a sessão FTP do exercício anterior, ela foi enviada em um pacote TCP para o servidor FTP. Como estávamos capturando pacotes durante a sessão, ela vai poder ser observada (aliás, todos os dados trocados entre o cliente e o servidor durante a sessão FTP).

1. Abra o arquivo de pacotes salvo no exercício anterior.
2. Caso já haja algum filtro ativado, clique antes no botão "Reset".
3. Faça um filtro para mostrar apenas os pacotes FTP do seu host (exemplo: **ftp and ip.addr==10.206.83.132**). Digite em letras minúsculas e não esqueça de pressionar ENTER.
4. Clique duas vezes no primeiro pacote mostrado, para que ele fique marcado.
5. No menu, escolha a opção *Analyze→Follow TCP Stream*.

6. Aparece uma janela mostrando todos os dados (em modo ASCII) que foram trafegados entre seu computador (cliente) e o servidor durante a sessão FTP. Dados mostrados em **azul** foram enviados pelo seu host e em **vermelho** foram recebidos. Não se preocupe em entender o formato dos dados, pois eles são entendidos pela aplicação FTP.
7. Procure dentro do texto mostrado as linhas contendo as palavras "**USER anonymous**" e "**PASS eu@ifpb.edu.br**". Você encontrou ?
  - Suponha que você estivesse acessando o site FTP da sua empresa e tivesse feito sido autenticado (feito o login) com seu nome e senha **reais**. Você acredita que seria difícil alguém capturar sua senha usando um "sniffer" do tipo Wireshark na sua rede local ? :-)

#### Exercício f – Capturando pacotes com filtro de captura

1. Ative a captura de pacotes (Menu Capture→Start).
2. Na opção "interface", escolha a interface Ethernet.
3. No campo "filter", digite: **host SEU\_IP**, onde SEU\_IP é o número IP do seu computador. Exemplo: **host 10.206.83.132**
4. Desabilite as opções "Enable MAC name resolution", "Enable network name resolution" e "Enable transport name resolution".
5. Pressione OK. Observe que agora existe uma "janela de captura" ativada.
6. Acesse a rede por alguns segundos (exemplo: acesse o site **www.ifpb.edu.br**). Não precisa demorar (basta acessar uma única página).
7. Pare a captura de pacotes clicando no botão **Stop** da janela de captura.
8. Salve os pacotes capturados no arquivo **captura2.eth** (mantenha o diretório padrão=c:\redes\Wireshark)

O que acabamos de fazer foi a captura seletiva de pacotes, ou seja capturamos apenas os pacotes que nos interessam, evitando a captura completa. Isso é diferente de fazer uma captura completa e filtrar a visualização de pacotes.

Uma captura completa toma grande espaço no disco e tempo para processar os pacotes. Em uma rede local grande (com muito tráfego), 5 minutos de captura pode representar vários gigabytes de espaço no disco.

#### Exercício g – Capturando pacotes HTTP

1. Ative a captura de pacotes (Menu Capture→Start).
2. Na opção "interface", escolha a interface Ethernet.
3. No campo "filter", digite: **host SEU\_IP**, onde SEU\_IP é o número IP do seu computador. Exemplo: **host 10.206.83.132**
4. Desabilite as opções "Enable MAC name resolution", "Enable network name resolution" e "Enable transport name resolution".
5. Pressione OK. Observe que agora existe uma "janela de captura" ativada.
6. Acesse o seguinte URL:  
**http://www.coinfo.ifpb.edu.br/professor/denio/seg/senha.txt**
7. Pare a captura de pacotes clicando no botão **Stop** da janela de captura.
8. Faça um filtro de visualização para mostrar apenas os pacotes TCP.
9. Clique duas vezes no primeiro pacote **TCP** mostrado, para que ele fique marcado.
10. No menu, escolha a opção Analyze→Follow TCP Stream.
11. Aparece uma janela mostrando todos os dados (em modo ASCII) que foram trafegados entre seu computador (cliente) e o servidor durante a sessão HTTP.
12. Compare os dados dessa janela com os dados mostrados no browser. Suponha que você estivesse consultando uma página contendo dados confidenciais e que algum intruso estivesse rodando o Wireshark. Ele iria ver o arquivo, certo ?

#### Exercício h – Capturando pacotes HTTPS (HTTP com criptografia)

Este exercício requer que haja um servidor HTTP capaz de suportar o serviço HTTPS

1. Faça a mesma coisa do exercício anterior, trocando a URL acessada para: **https://www.coinfo.ifpb.edu.br/professor/denio/seg/senha.txt** (observe que agora é "http**s**")