Ministério da Educação
Universidade Tecnológica Federal do Paraná - Câmpus Pato Branco
Curso de Engenharia de Computação
Disciplina: Redes de Computadores
Prof. Fábio Favarim, Dr.

INSTRUÇÕES:

- Esta atividade é presencial. Atividade individual.
- Deve ser executado tudo o que está nesse roteiro e redigir um documento respondendo cada item da Tarefa 1, 2 e 3 listadas a seguir. No início desse documento deve estar identificado o nome completo do aluno.
- Ao final da atividade, o documento deve ser postado no Moodle.
- O nome do arquivo deve ser nomeado como "Atividade1-Laboratório3-NomeAluno.pdf"

Laboratório com o Wireshark: Iniciação

A compreensão de protocolos de rede pode ser muito mais profunda se os virmos em ação e interagirmos com eles – observando a sequencia de mensagens trocadas entre duas entidades do protocolo, pesquisando detalhes de sua operação, fazendo com que eles executem determinadas ações e observando essas ações e suas consequências. Isso pode ser feito em cenários simulados ou em um ambiente real, como a Internet.

Na disciplina de redes de computadores, vamos ambas abordagens. Para isso você executará aplicações de rede em vários cenários utilizando um computador, no laboratório ou em casa. Assim, você observará e aprenderá o funcionamento dos protocolos na prática.

A ferramenta básica para observar as mensagens trocadas entre entidades de protocolos em execução é denominada **analisador de pacotes (packet sniffer)**. Um analisador de pacotes é um software que pode interceptar e registrar tráfego de dados passando em uma rede de dados. A medida que o fluxo de dados trafega em uma rede, o analisador faz a **captura** de cada unidade de dados de protocolo (PDU) e pode decodificar e analisar seu conteúdo de acordo com o RFC apropriado ou com outras especificações. Isso permite que analisador exiba o encapsulamento e campos individuais de uma PDU e interprete seu significado.

O Wireshark é um dos softwares analisadores de protocolos existentes, iremos utilizá-lo em nossa disciplina. Faça o download do aplicativo em www.wireshark.org.

Etapa 1: Conhecendo o Wireshark

Quando se executa o programa, a interface inicial do programa é apresentada como mostra a Figura 1.

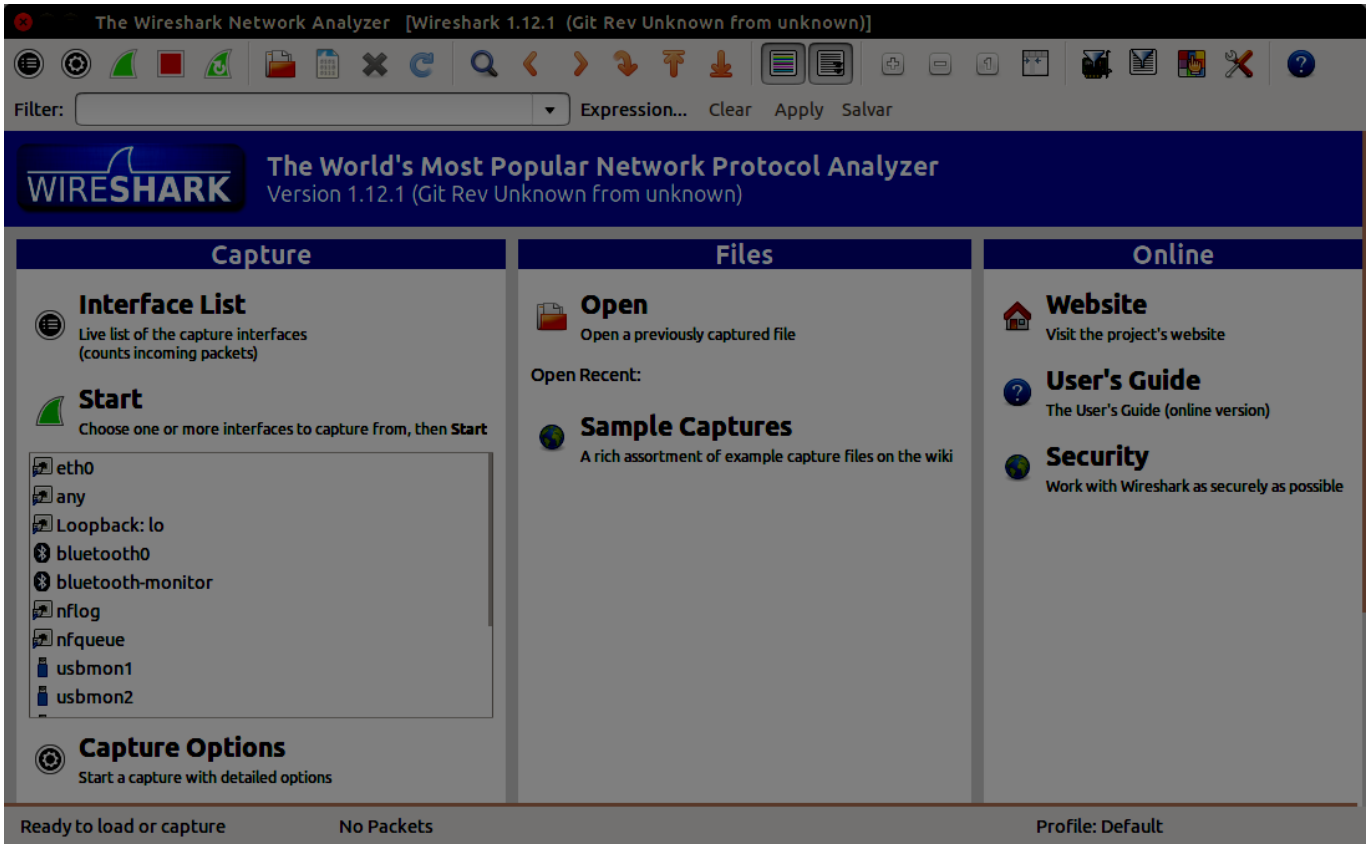

Figura 1 – Interface Gráfica do Wireshark

Etapa 2: Fazendo o primeiro teste com o Wireshark

A melhor forma de aprender sobre um novo programa é experimentá-lo! Para isso siga os passos indicados a seguir.

a) Inicie o seu browser web favorito, que irá apresentar a página que você tiver selecionado.

b) Inicie o Wireshark com **privilégios de administrador**. Você irá inicialmente ver uma janela ainda sem nenhum dado, visto que o Wireshark ainda não começou a capturar pacotes.

c) Agora na tela principal (Figura 1) **selecione a interface de rede** a qual deseja captura pacotes. Depois de selecionar a interface de rede, **clique Start** (primeiro icone – formato de barbatana dorsal de um tubarão). Assim terá início a captura – todos os pacotes que forem transmitidos/recebidos para/pelo seu computador agora estarão sendo capturados pelo Wireshark e são apresentados **"ao vivo"** na janela com a listagem de pacotes capturados!

d) Enquanto o Wireshark estiver executando, use a URL:

http://www.pb.utfpr.edu.br/favarim/redes/paginasupersimples.htmlsupersimples.html e faça com que a página seja apresentada no seu browser. Para apresentar esta página, o seu browser irá contatar o servidor HTTP em **www.pb.utfpr.edu.br** e trocar mensagens http com o servidor de modo a baixar esta página. Os quadros Ethernet que contêm estas mensagens HTTP serão capturadas pelo Wireshark.

e) Depois que o seu browser tiver apresentado a página **paginasupersimples.html**, **pare** a captura de pacotes do Wireshark, através do botão **Stop**, que é o **segundo ícone** da esquerda para a direita na barra de ferramentas principal. Mas, ainda não pare a captura.

f) Agora você terá pacotes reais que conterá todas as mensagens dos protocolos trocadas entre o seu computador e outras entidades de rede! A troca de mensagens HTTP com o servidor web **www.pb.utfpr.edu.br** deve aparecer em algum lugar na **lista de pacotes capturados**. Nessa **lista de pacotes capturados** são exibido um resumo de cada pacote capturado. Cada linha dessa seção corresponde a uma PDU ou pacote dos dados capturados. Se você selecionar uma linha nesta seção, mais detalhes serão exibidos nas seções de **"Detalhes do Pacote (PDU)"** e **"Conteúdo do Pacote (PDU)"**.

- A **seção de Detalhes do Pacote (ou PDU)** exibe o pacote selecionado na seção de pacotes capturados em mais detalhes.
- A **seção Conteúdo do Pacote (ou PDU)** exibe os dados reais (em forma hexadecimal representando o binário real) de pacote selecionado na **lista de pacotes capturados** e destaca o campo selecionado na **seção de Detalhes do Pacote (ou PDU)**.

g) Observe que na **lista de pacotes capturados** serão apresentados também muitos outros tipos de pacotes (veja por exemplo, os diferentes tipos de protocolos mostrados na coluna Protocol. Mesmo que a sua única atividade tenha sido baixar uma página web, devem haver evidentemente muitos outros protocolos executando no seu computador que não são vistos pelo usuário. Assim como, devem aparecer quadro de outros computadores. Nós aprenderemos

muito mais sobre estes protocolos à medida que avançarmos na disciplina! Por enquanto, você só precisa estar ciente de que há muito mais acontecendo do que aquilo que está à vista!

- **Atenção**: As informações capturadas para as PDUs de dados podem ser salvas em um arquivo. Este arquivo pode ser aberto no Wireshark para futura análise sem necessidade de re-capturar o mesmo tráfego de dados novamente. As informações exibidas quando um arquivo de captura é aberto são as mesmas da captura original.

Etapa 3: Aplicando Filtros de visualização – Display Filter

O objetivo desta etapa é utilizar a funcionalidade de filtros de pacotes provida pelo Wireshark. Vamos ver como se faz isso:

a) Na parte superior esquerda da janela do Wireshark, há a seção de especificação de **"filtro de apresentação",** nessa seção há um botão "Filter" com um espaço em branco ao lado.

b) Digite o filtro no espaço em branco. Os filtros devem ser digitados em letras minúsculas.

c) Para ativar o filtro pressione ENTER. Para desativar o filtro (antes de digitar outro), pressione no botão "Clear".

d) Testando os filtros

- Digite **http** na área de especificação do filtro. Aperte ENTER. Isto causará a apresentação apenas de mensagens do protocolo **http** serem exibidas na janela de listagem de pacotes.
- Selecione a mensagem http na janela de listagem de pacotes a que se refere a página buscada, isto é, **paginasupersimples.html**. Deve ser a mensagem do tipo GET do HTTP que foi enviada pelo seu computador para o servidor HTTP (www.pb.utfpr.edu.br) (na Etapa 2). Quando você seleciona a mensagem GET, serão apresentadas na janela a seção de **cabeçalho dos pacotes**, as informações dos cabeçalhos do quadro Ethernet (camada de Enlace), do datagrama IP (camada de Rede), do segmento TCP (camada de Transporte) e da mensagem HTTP[1] (camada de Aplicação).
- Adicionalmente, pode-se inserir mais filtros, por exemplo, filtrando os pacotes por endereço IP:
  - ip.addr == a.b.c.d; sendo que a.b.c.d é o endereço IP a ser filtrado (ex: ip.addr == 172.29.190.10)
  - ip.dst == a.b.c.d; sendo que a.b.c.d é endereço IP de destino a ser filtrado (ex: ip.dst == 172.29.190.10)
  - ip.src == a.b.c.d; sendo que a.b.c.d é endereço IP de origem a ser filtrado (ex: ip.src == 172.29.190.10)
- Além disso pode-se usar mais de uma expressão ao mesmo tempo, por exemplo, fazer a filtragem de pacotes por endereço IP e também por protocolo, por exemplo, ip.addr == 172.29.190.10 and http
- **Atenção: alguns filtros podem não mostrar nenhum pacote, em função da atividade da rede naquele momento.**

Tarefa 1: Captura de Pacote HTTP

- Analise os dois pacotes (requisição e resposta) relacionados a aquisição da página web (Etapa 2) e responda:
  1. Qual protocolo da camada de aplicação é usado para acessar a página html?
  2. Qual protocolo da camada de transporte está sendo usado?
  3. Qual protocolo está sendo usado na camada de rede?
  4. Qual protocolo está sendo usado na camada de enlace?
  5. Qual a porta de origem e de destino da mensagem de requisição (request)?
  6. Qual a porta de origem e de destino da mensagem de resposta (reply)?
  7. Qual o endereço IP (endereço lógico) de origem e de destino da mensagem de requisição (request)?
  8. Qual o endereço IP (endereço lógico) de origem e de destino da mensagem de resposta (reply)?
  9. Qual o endereço MAC (endereço físico) de origem e de destino da mensagem de requisição?
  10. Qual o endereço MAC (endereço físico) de origem e de destino da mensagem de resposta?

Tarefa 2: Captura de Pacote Ping

[1] Lembre que a mensagem GET do http que é enviada para o servidor www.pb.utfpr.edu.br está contida dentro de um segmento TCP, que está contido (encapsulado) dentro de um datagrama IP, que está encapsulado em um quadro Ethernet. Se este processo de encapsulamento ainda não estiver claro, reveja os slides.

- **Inicie** a captura de pacotes
- Use a ferramenta ping, e faça "ping" para o servidor onde está localizado a página web obtida na Etapa 2, isto é, **www.pb.utfpr.edu.br**.
  - ↘ Faça isso através da linha de comando (prompt de comando no windows ou terminal no linux) usando o comando **ping endereço-IP** ou **ping nome-da-máquina**
- Após receber **a primeira** resposta com sucesso do ping na janela de linha de comando, **pare** a captura de pacotes.
- Analise os pacotes listados e localize aqueles (requisição e resposta) equivalentes ao **pacote ping** e responda as questões abaixo:
  1. Qual protocolo está sendo usado na camada de rede?
  2. Qual a porta de origem e de destino da mensagem de requisição (request)?
  3. Qual o endereço IP (endereço lógico) de origem e destino da mensagem de requisição (request) do ping?
  4. Qual o endereço IP (endereço lógico) de origem e destino da mensagem de resposta (reply) do ping?
  5. Qual protocolo está sendo usado na camada de enlace?
  6. Qual o endereço MAC (endereço físico) de origem e destino da mensagem de requisição?
  7. Qual o endereço MAC (endereço físico) de origem e destino da mensagem de resposta?

Tarefa 3: Captura de Pacotes DHCP

- Desative a interface de rede sem fio do computador ou desconecte o cabo do mesmo
- **Inicie** a captura de pacotes
- Ative a interface de rede sem fio do computador ou conecte o cabo do mesmo
- Será dado o processo de negociação DHCP.
- Após receber o endereço IP, **pare** a captura de pacotes. (sugestão filtrar os pacote pelo protocolo bootp)
- Analise os pacotes listados e localize aqueles equivalentes ao processo DHCP e responda:
  1. Foi encontrada a mensagem DHCP Discover? Se sim, responda:

a) Qual o endereço IP (endereço lógico) de origem e destino da mensagem?
b) Qual a porta de origem e de destino da mensagem?
c) Qual o endereço MAC (endereço físico) de origem e destino da mensagem de requisição?

  2. Foi encontrada a mensagem DHCP Offer? Se sim, responda:

a) Qual o endereço IP (endereço lógico) de origem e destino da mensagem?
b) Qual a porta de origem e de destino da mensagem?
c) Qual o endereço MAC (endereço físico) de origem e destino da mensagem de requisição?

  3. Quanto a mensagem DHCP Request, responda:

a) Qual o endereço IP (endereço lógico) de origem e destino da mensagem?
b) Qual a porta de origem e de destino da mensagem?
c) Qual o endereço MAC (endereço físico) de origem e destino da mensagem de requisição?

  4. Quanto a mensagem DHCP ACK, responda:

a) Qual o endereço IP (endereço lógico) de origem e destino da mensagem?
b) Qual a porta de origem e de destino da mensagem?
c) Qual o endereço MAC (endereço físico) de origem e destino da mensagem de requisição?
d) Informe os dados dos campos de opções (option)

1. DHCP Server Identification
2. Subnet Mask
3. Router
4. Domain Name
5. Domain Name Server

Extra) Compare o endereço IP encontrado em DHCP Server Identification com o IP de Origem da mensagem?

- São iguais?
- Na casa de vocês, normalmente ambos endereços são iguais, pois o serviço DHCP normalmente está no mesmo equipamento (roteador)
- Na UTFPR (Pato Branco) o servidor DHCP está em uma máquina específica somente para esse fim que atende a todas as redes, assim o roteador fazer o que se chama de **relay** para o servidor DHCP. Isto é, quando o roteador (gateway) recebe uma mensagem DHCP Discover ou DHCP Request, este encaminha (relay) para o servidor DHCP.

RESPOSTAS:

Tarefa 1)

1- HTTP
2- TCP
3- IPv4
4- Enthernet II e Frame 422
5- Source: 56088 Dst: 80
6- Source:80 Dst: 56088
7- Src: 172.30.13.91 Dst: 200.134.18.46
8- Src: 200.134.18.46 Dst: 172.30.13.91
9- Src: c0:38:96:a1:bb:b5 Dst: 40:01:c6:f4:70:01
10 - Src40:01:c6:f4:70:01 : Dst: c0:38:96:a1:bb:b5

Tarefa 2)

1- Ethernet II
2- Não Tem Porta
3- Scr: 172.30.1.118 Dst: 200.74.18.46
4- Scr: 200.74.18.46 Dst: 172.30.1.118
5- Frame 1307
6- Src: c0:38:96:a1:bb:b5 Dst: 40:01:c6:f4:70:01
7- Src: 40:01:c6:f4:70:01 Dst: c0:38:96:a1:bb:b5

Tarefa 3)

01) Fica em Cash
02) Fica em Cash
03)
a) Src: 0.0.0.0 Dst: 255.255.255.255
b) Src 68 Dst: 67
c) Src: c0:38:96:a1:bb:b5 Dst: ff:ff:ff:ff:ff:ff:ff

04)
a) Src: 172.30.0.1 Dst: 172.30.1.118
b) Src: 67 Dst: 68
c) Src: 40:01:c6:f4:70:01 Dst: c0:38:96:a1:bb:b5

d)
1- DHCP SI: 192.168.224.1
2 - SB MASK: 255.255.240.0
3- ROUTER: 172.30.0.1
4 – DOMAIN NAME: pb.utfpr.edu.br
5 – DOMAIN SERVER NAME: 172.29.150.100 / 200.134.18.36/ 200.134.80.11

Extra)

a) Não.