Aula Prática de Redes Industriais
Wireshark

O entendimento de protocolos de redes pode ser bastante aprofundado através da "observação de protocolos funcionando" e "da manipulação de protocolos" - observando a sequência de mensagens trocadas entre duas entidades, entrando nos detalhes da operação do protocolo, e fazendo com que os protocolos realizem certas ações e então observando estas ações e as consequências. Isso pode ser feito em cenários simulados ou em um ambiente de rede "real" tal como a Internet. Nestes laboratórios Wireshark, você executará várias aplicações de redes em cenários diferentes utilizando um computador em casa ou em um laboratório. Você observará os protocolos de redes em seu computador "em ação", interagindo e trocando mensagens com as entidades executadas em algum lugar da Internet. Assim, você e o seu computador serão uma parte integrante destes laboratórios "ao vivo". Você observará e aprenderá fazendo.

A ferramenta básica para observar as mensagens trocadas entre as entidades em execução é chamada de sniffer. Como o nome sugere, um sniffer captura mensagens sendo enviadas/recebidas pelo seu computador; ele também tipicamente armazena e/ou apresenta os conteúdos dos vários campos dos protocolos nestas mensagens capturadas. Um sniffer isoladamente é um elemento passivo. Ele observa as mensagens sendo enviadas e recebidas pelas aplicações e protocolos executando no seu computador, mas jamais envia pacotes. Similarmente, os pacotes recebidos nunca são explicitamente endereçados ao sniffer. Ao invés disso, um sniffer recebe uma cópia de pacotes que são enviados/recebidos para/de aplicações e protocolos executando no seu computador. A figura 1 mostra a estrutura de um sniffer. À direita da figura 1 estão os protocolos (neste caso, protocolos da Internet) e aplicações (tais como navegador web ou cliente FTP) que normalmente executam no seu computador. O sniffer, exibido dentro do retângulo tracejado na figura 1 é uma adição aos softwares usuais no seu computador, e consiste de duas partes: a biblioteca de captura de pacotes e o analisador de pacotes.

A biblioteca de captura de pacotes recebe uma cópia de cada quadro da camada de enlace que é enviado do ou recebido pelo seu computador. Lembre-se que mensagens trocadas por protocolos das camadas mais altas tais como HTTP, FTP, TCP, UDP, DNS ou IP, são todos eventualmente encapsulados em quadros que são transmitidos para o meio físico como um cabo Ethernet. Na figura 1, assume-se que o meio físico é uma Ethernet, e desta forma, os protocolos das camadas superiores são eventualmente encapsulados em um quadro Ethernet. Capturar todos os quadros fornece todas as mensagens enviadas/recebidas de/ por todos os protocolos e aplicações executando em seu computador.

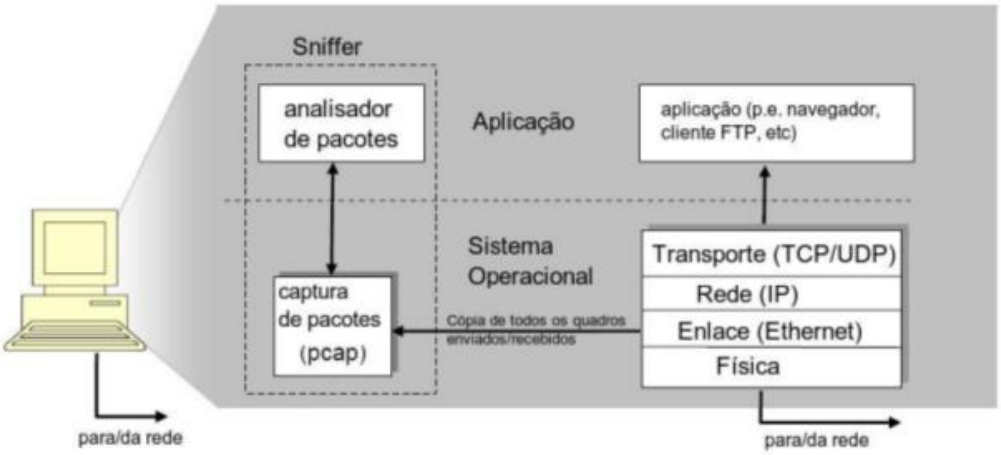

Figura 1: Estrutura de um sniffer.

O analisador de pacotes exibe os conteúdos de todos os campos dentro de uma mensagem de protocolo. Para que isso seja feito, o analisador de pacotes deve "entender" a estrutura de todas as mensagens trocadas pelos protocolos. Por exemplo, suponha que estamos interessados em mostrar os vários campos nas mensagens trocadas pelo protocolo HTTP na figura 1. O analisador de pacotes entende o formato dos quadros Ethernet, e desta forma pode identificar o datagrama IP dentro de um quadro. Ele também entende o formato do datagrama IP, para que ele possa extrair o segmento TCP dentro do datagrama IP. Ele entende a estrutura do segmento TCP, para que possa extrair a mensagem HTTP contida no segmento. Finalmente, ele entende o protocolo HTTP e então, por exemplo, sabe que os primeiros bytes de uma mensagem HTTP contêm a cadeia "GET", "POST" ou "HEAD". Nós utilizaremos o sniffer Wireshark (http://www.wireshark.org) para estes laboratórios, o que nos permite exibir os conteúdos das mensagens sendo enviadas/recebidas de/por protocolos em diferentes camadas da pilha de protocolos. Tecnicamente falando, Wireshark é um analisador de pacotes que pode ser executado em computadores com Windows, Linux/UNIX e MAC. É um analisador de pacotes ideal para nossos laboratórios, pois é estável, tem uma grande base de usuários e é bem documentado incluindo um guia de usuário (http://www.wireshark.org/docs/wsug_html/), páginas de manual (http://www.wireshark.org/docs/man-pages/), e uma seção de FAQ detalhada (http://www.wireshark.org/faq.html), funcionalidade rica que inclui a capacidade de analisar mais que 500 protocolos, e uma interface com o usuário bem projetada. Ele funciona em computadores ligados a uma Ethernet para conectar-se à Internet, bem como protocolos ponto a ponto, tal como PPP. Wireshark é a evolução do analisador de pacotes denominado Ethereal.

Executando o Wireshark

Para executar a aplicação entre como usuário Lab_102_4, cuja senha é redes102. Entre no terminal (CONTROL+ALT+T) e digite:
#sudo wireshark

Informe a senha redes102. A interface com o usuário exibida na Figura 2 aparecerá. Inicialmente, nenhum dado será apresentado nas janelas.

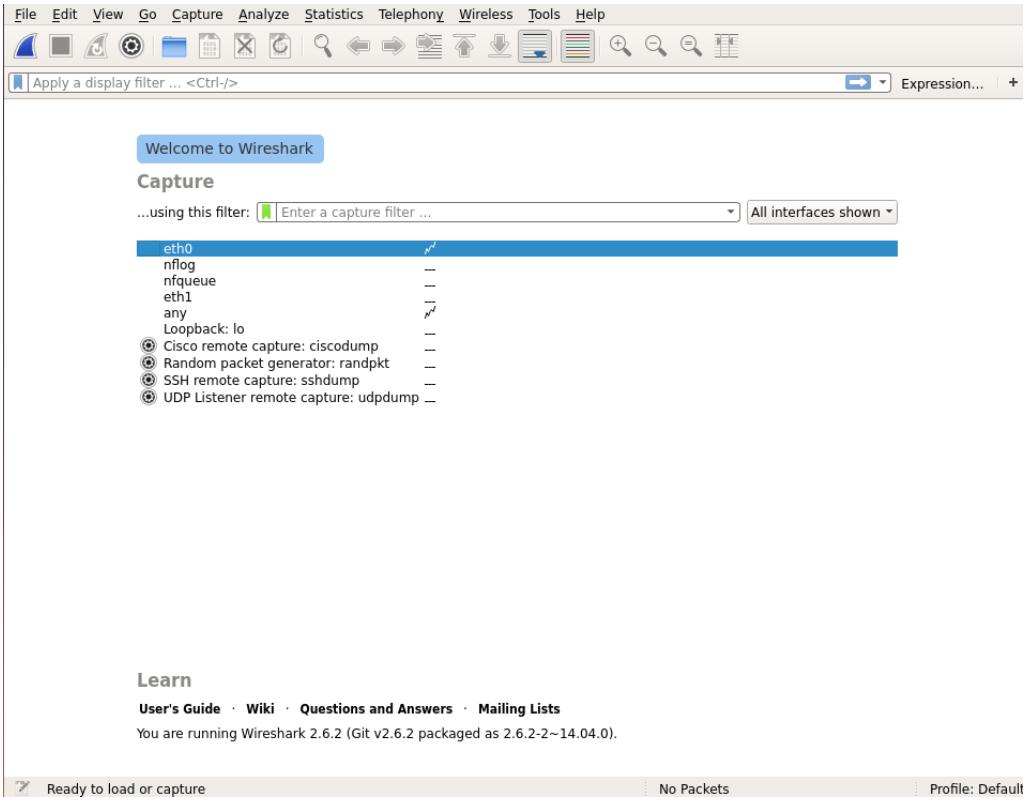

Figura 2: Tela inicial do Wireshark.

Clique em Capture/Start. Entre em um navegador e acesse o site www.ronepage.com.br. Volte para a tela do Wireshark em clique em Capture/Stop.

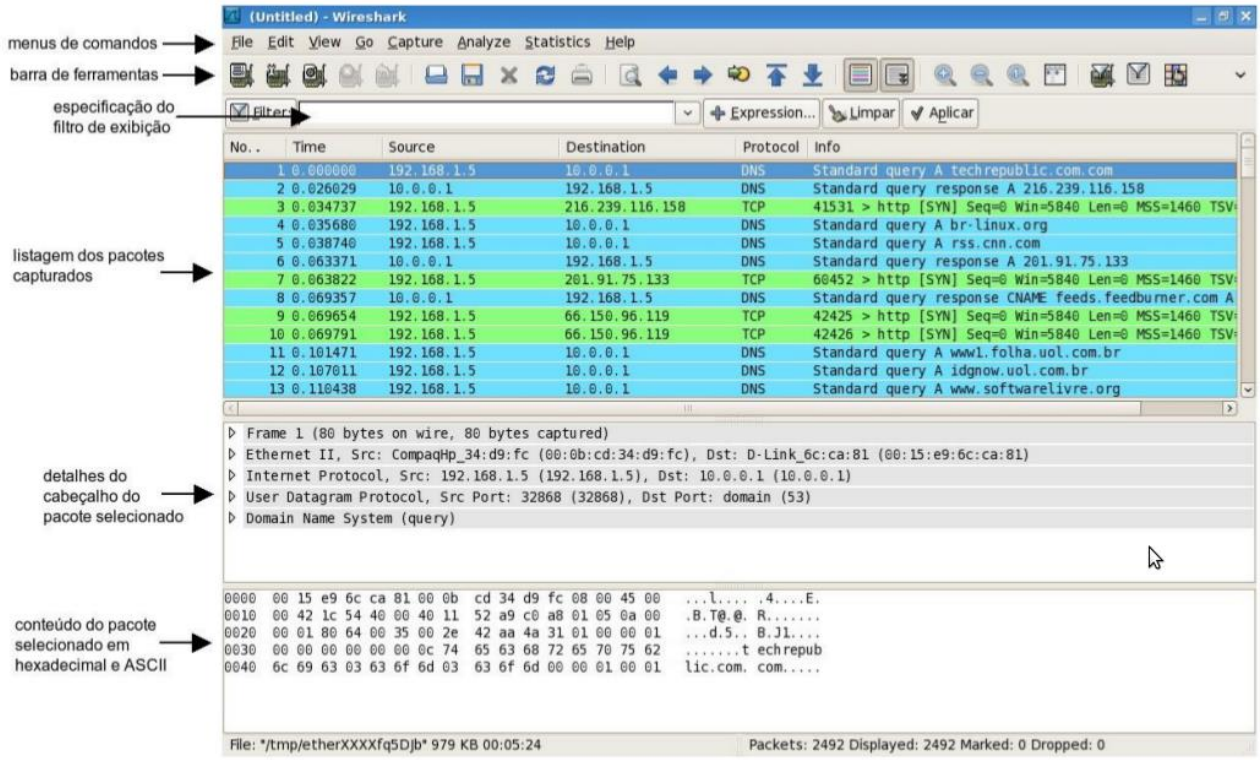

Figura 2. *Interface* com o usuário do Wireshark.

Figura 3: Componentes da tela do Wireshark

A interface do Wireshark tem seis componentes principais:

● os menus de comandos são localizados no topo da janela. Por enquanto, interessam apenas os menus File e Capture. O menu File permite salvar dados de capturas de pacotes ou abrir um arquivo contendo dados de capturas de pacotes previamente realizadas, e sair da aplicação. O menu 3Capture permite iniciar uma captura de pacotes;

● a barra de ferramentas contém os comandos de menu que são mais frequentemente utilizados. Há atalhos para abrir ou salvar dados de captura de pacotes e para iniciar ou parar uma captura de pacotes;

● abaixo da barra de ferramentas, está o campo de filtragem de pacotes exibidos. Nele podem ser digitados nome de protocolo ou outra informação apresentada na janela de listagem de pacotes. Apenas os pacotes que correspondem ao filtro são exibidos;

● a janela de listagem de pacotes apresenta um resumo de uma linha para cada pacote capturado, incluindo o número do pacote (atribuído pelo Wireshark; este não é o número do pacote contido no cabeçalho de qualquer protocolo), o tempo que o pacote foi capturado, os endereços fonte e destino do pacote, o tipo de protocolo, e informação específica do protocolo contida no pacote. A lista de pacotes pode ser ordenada conforme qualquer uma destas categorias clicando no nome de uma coluna correspondente. O campo tipo do protocolo lista o protocolo de mais alto nível que enviou ou recebeu este pacote, i.e., o protocolo que é a fonte ou o último sorvedouro para este pacote;

● a janela de detalhes de cabeçalho de pacotes fornece detalhes sobre o pacote selecionado na janela de listagem de pacotes. Para selecionar um pacote, basta clicar sobre ele com o botão esquerdo do mouse na janela de listagem de pacotes. Os detalhes apresentados incluem informações sobre o quadro Ethernet e o datagrama IP que contém o pacote. A quantidade de detalhes exibida pode ser expandida ou contraída. Se o pacote foi carregado sobre TCP ou UDP, detalhes correspondentes também são apresentados, os quais também podem ser contraídos ou expandidos. Finalmente, detalhes sobre o protocolo de mais alto nível que enviou ou recebeu este pacote também são apresentados;

● a janela de conteúdo de pacotes mostra o conteúdo inteiro do quadro capturado, nos formatos ASCII e hexadecimal.

Para testar as capacidades de filtragem, vamos inserir a cadeia “http” (sem as aspas e em minúsculo) no especificação do filtro de exibição e depois selecionar Apply (ou Aplicar). O resultado é exibido na Figura 4;

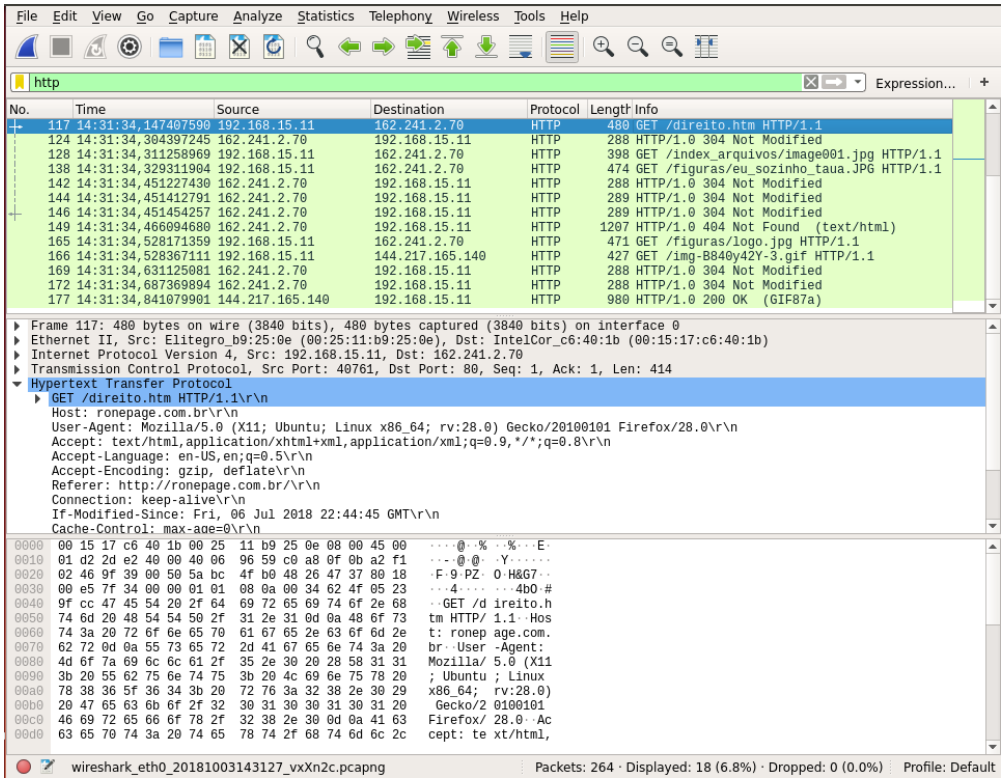

Figura 4: Exibição com o filtro “http”.

Selecione a primeira mensagem HTTP GET exibida na janela de listagem de pacotes. Quando você seleciona uma mensagem, as informações dos cabeçalhos do quadro Ethernet, do datagrama IP, do segmento TCP e da mensagem HTTP aparecem na janela de cabeçalhos de pacotes. É possível ver os detalhes, expandido ou comprimindo os itens com um clique na seta ao lado deles (ver Figura 4).

Tarefas a serem realizadas

1) Liste os diferentes protocolos que aparecem na coluna Protocol na janela de listagem de pacotes após finaliza a escuta.

2) quanto tempo passou de quando a mensagem HTTP GET foi enviada até que a resposta OK foi recebida? (por default, o valor da coluna Time na janela de listagem de pacotes é a quantidade de tempo, em segundos, desde que a captura iniciou). Para exibir o campo Time no formato hora do dia, selecione o menu View, depois Time Display Format, então selecione Time of day.

3) Qual é o endereço IP do site www.ronepage.com.br? Qual é o endereço IP da interface de rede do seu computador?

4) Liste as mensagens TCP e verifique o tipo que é descrito pelo campo FLAG. Quais os tipos que apareceram? Pesquise para descrever o que cada um significa.

5) Qual a interface de rede utilizada pelo computador? Pesquise para saber o que ela representa.