Wireshark Lab: Iniciando

Versão 1.1

"Conte-me e esqueço.
Mostre-me e eu lembro.
Envolva-me e eu entendo."
provérbio Chinês

O entendimento de protocolos de redes pode ser bastante aprofundado através da "observação de protocolos funcionando" e "da manipulação de protocolos" - observando a seqüência 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 conseqüências. Isso pode ser feito em cenários simulados ou em um ambiente de rede "real" tal como a Internet. Os *applets* em Java que acompanham este texto representam a primeira abordagem. Nestes laboratórios Wireshark, faremos a última abordagem. 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 da discussão da seção 1.7.2 no texto (figura 1.18) 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.

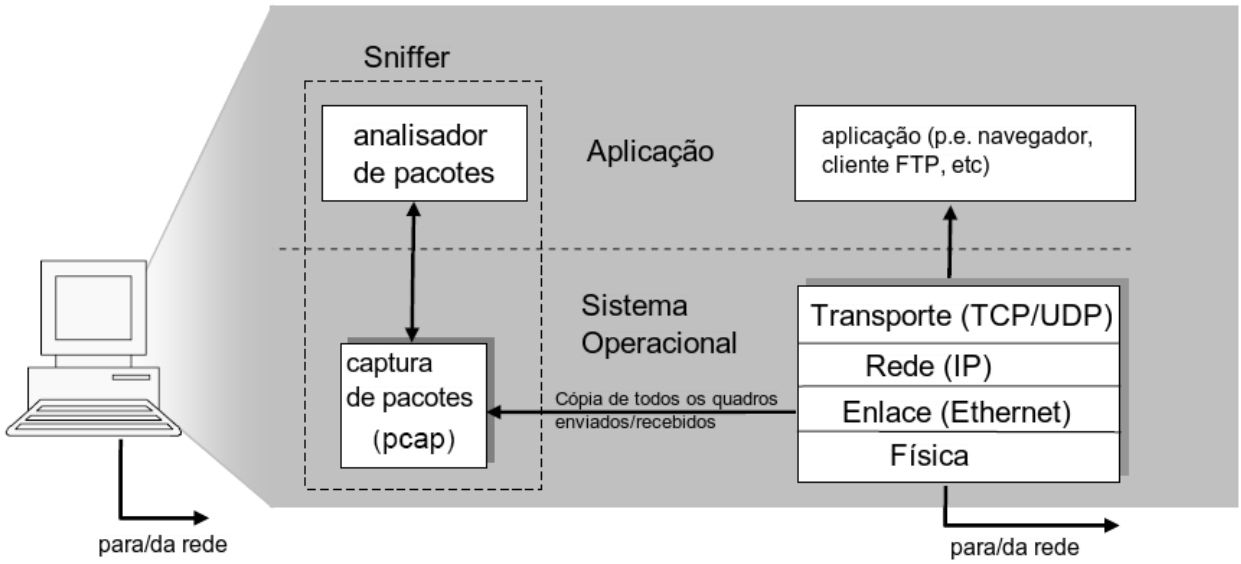

Figura 1. Estrutura de um sniffer.

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 contém a cadeia “GET”, “POST” ou “HEAD” como exibido na figura 2.8 no texto.

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.

Como Obter Wireshark

Para executar o wireshark, você precisará ter acesso a um computador que suporte ambos, o Wireshark e a biblioteca de captura de pacotes libpcap. A biblioteca libpcap precisa ser instalada antes do Wireshark para que este funcione. Veja http://www.wireshark.org/download.html para uma lista de sistemas operacionais suportados e sites para *downloads*.

Baixe e instale Wireshark e, caso seja necessário, libpcap:

- se necessário, baixe e instale libpcap. As distribuições Linux trazem libpcap como uma dependência do Wireshark. No Windows, libpcap chama-se WinPCap e pode ser encontrada em http://www.winpcap.org/. Entretanto, esta biblioteca já está incluída no instalador do Wireshark;

- vá para http://www.wireshark.org/download.html, baixe e instale Wireshark para o seu sistema operacional (se for Linux, procure no repositório da distribuição que você usa);

- baixe o manual do usuário do wireshark.

A seção de FAQ do Wireshark contém várias dicas e informações bem interessantes, particularmente se você teve problema instalando ou executando Wireshark.

Executando o Wireshark

Quando você executar o programa Wireshark, a *interface* com o usuário exibida na figura 2 aparecerá. Inicialmente, nenhum dado será apresentado nas janelas.

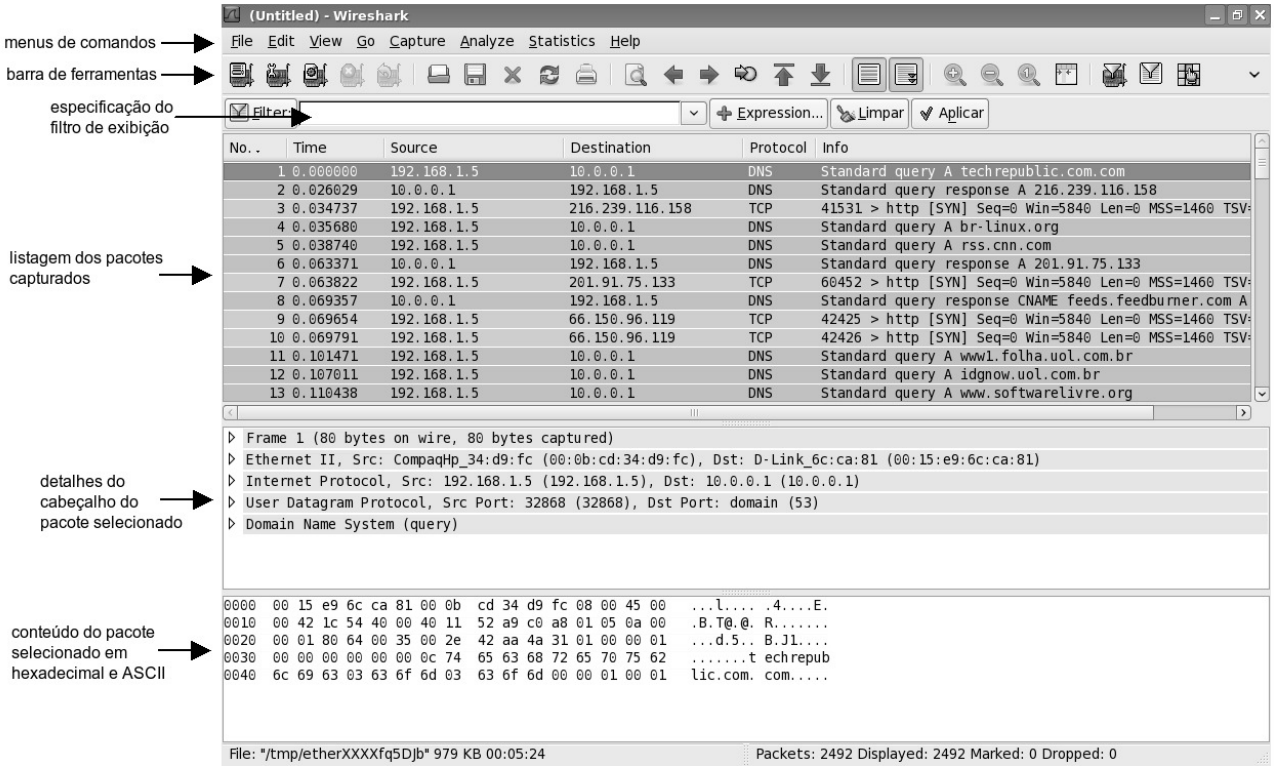

Figura 2. *Interface* com o usuário do Wireshark.

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 Capture permite iniciar uma captura de pacotes;
- a barra de ferramentas contém os comandos de menu que são mais freqüentemente 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.

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.

Execução de Teste do Wireshark

A melhor maneira de aprender um novo software é o utilizando. Faça o seguinte:

1. inicie o seu navegador web favorito;

2. inicie o Wireshark. Inicialmente as janelas estarão vazias, pois não há captura de pacotes em progresso;

3. para iniciar uma captura de pacotes, selecione o menu Capture e depois Interfaces. Isso faz com que a janela de interfaces de rede disponíveis seja apresentada (figura 3);

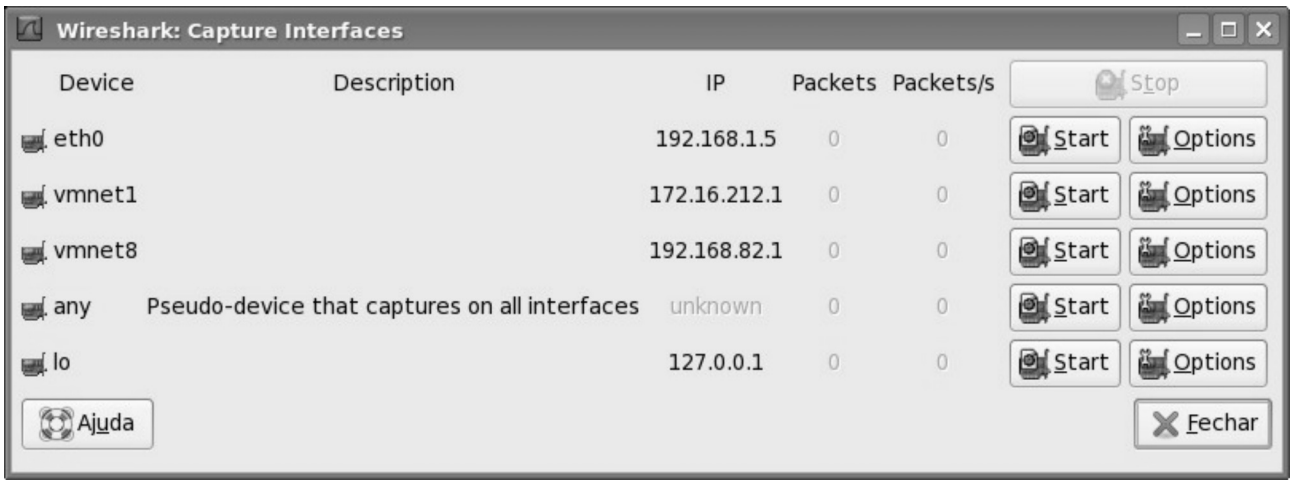

Figura 3. Interfaces de rede existentes no computador.

4. basta clicar no botão Start da interface desejada para iniciar a captura de pacotes. Na figura 3, como o Wireshark está sendo executado no Linux, o botão Start da interface eth0 deve ser selecionado;

5. como nada está acontecendo na rede, a janela apresenta o conteúdo vazio (figura 4);

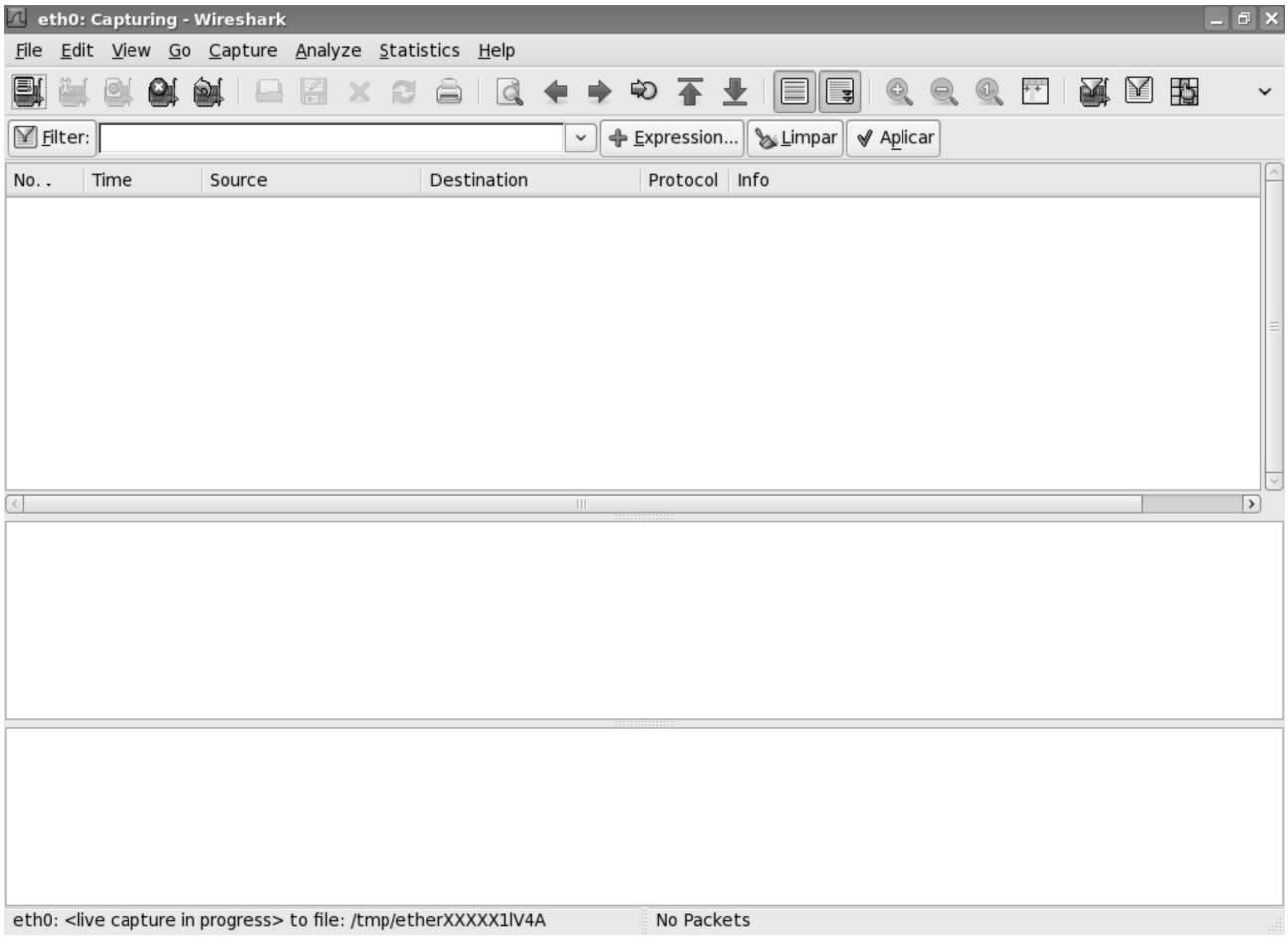

Figura 4. Janela exibida após escolher a interface eth0.

6. no navegador, acesse o site do livro (http://www.aw.com/kurose_br);

7. ao voltar para a janela do Wireshark, houve a captura de todos os pacotes envolvidos na conexão (figura 5);

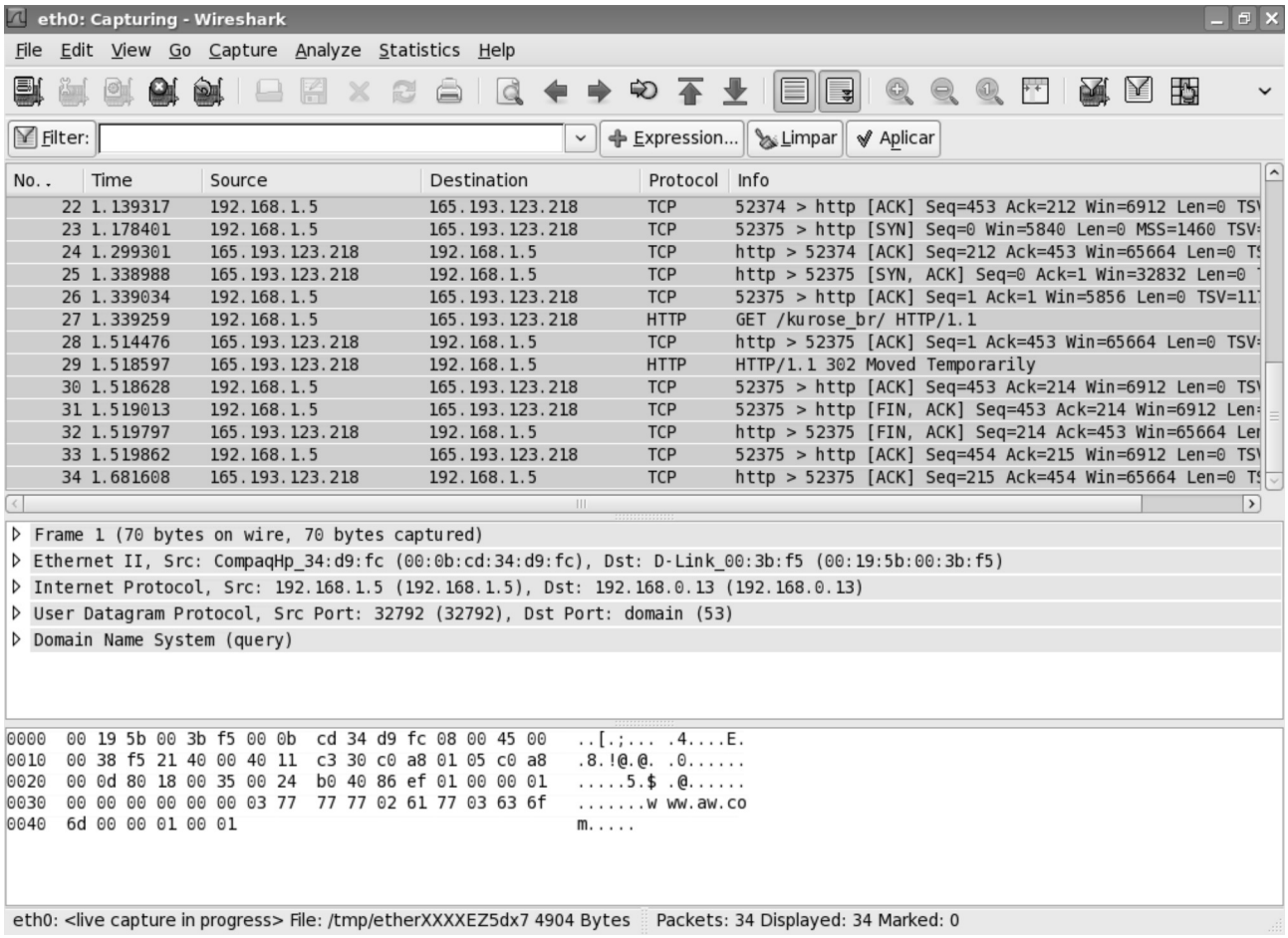

Figura 5. Captura dos pacotes da conexão aberta pelo navegador web.

8. antes de continuar, vamos parar a captura de pacotes e trabalhar com o que temos. Basta clicar em Capture e depois em Stop;

9. 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 6;

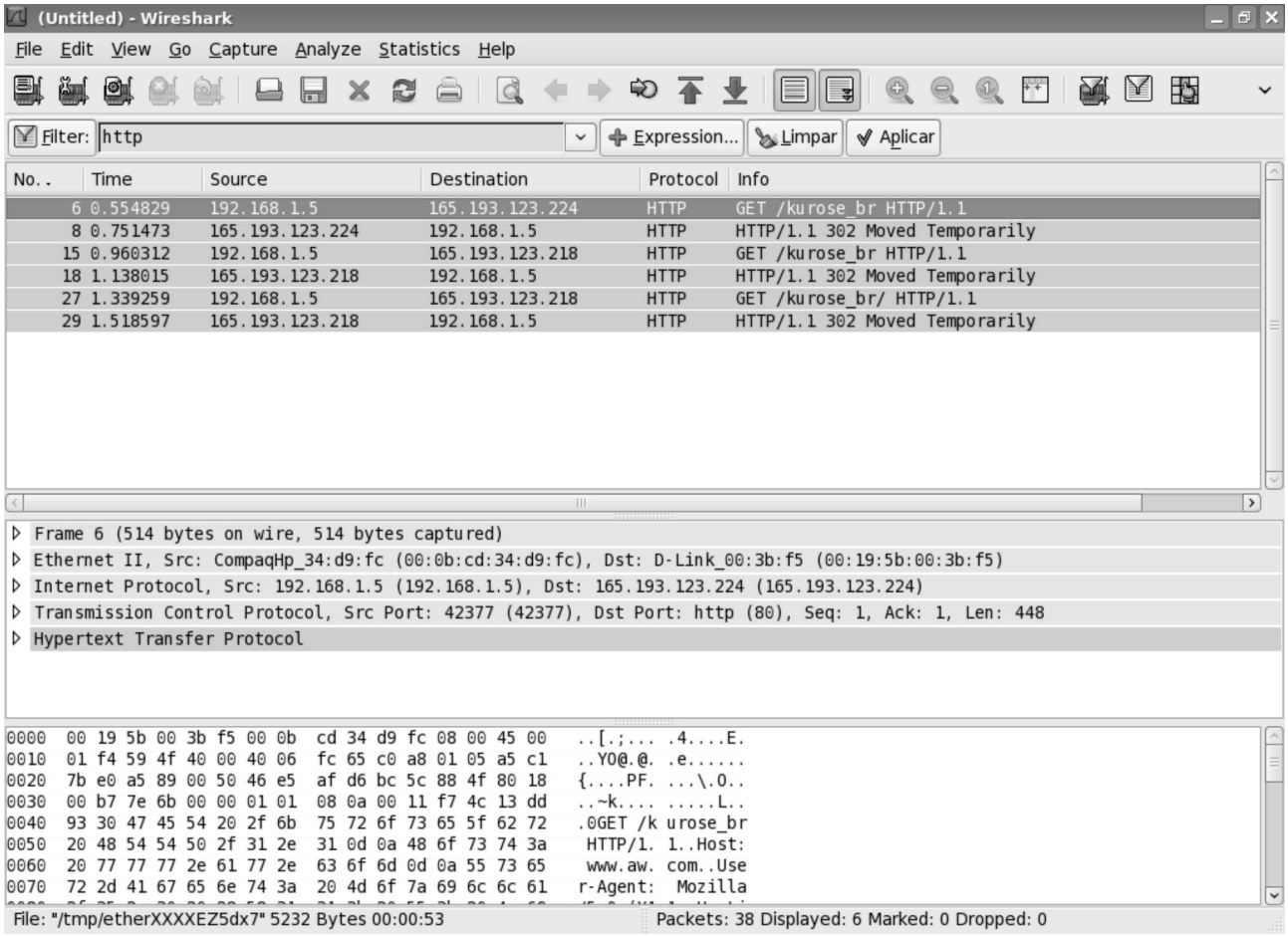

Figura 6. Janela após a aplicação do filtro "http".

10. selecione a primeira mensagem HTTP exibida na janela de listagem de pacotes. Ela deve ser a mensagem HTTP GET que foi enviada do seu computador ao servidor HTTP em www.aw.com. Quando você seleciona a mensagem HTTP GET, 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 (figura 7);

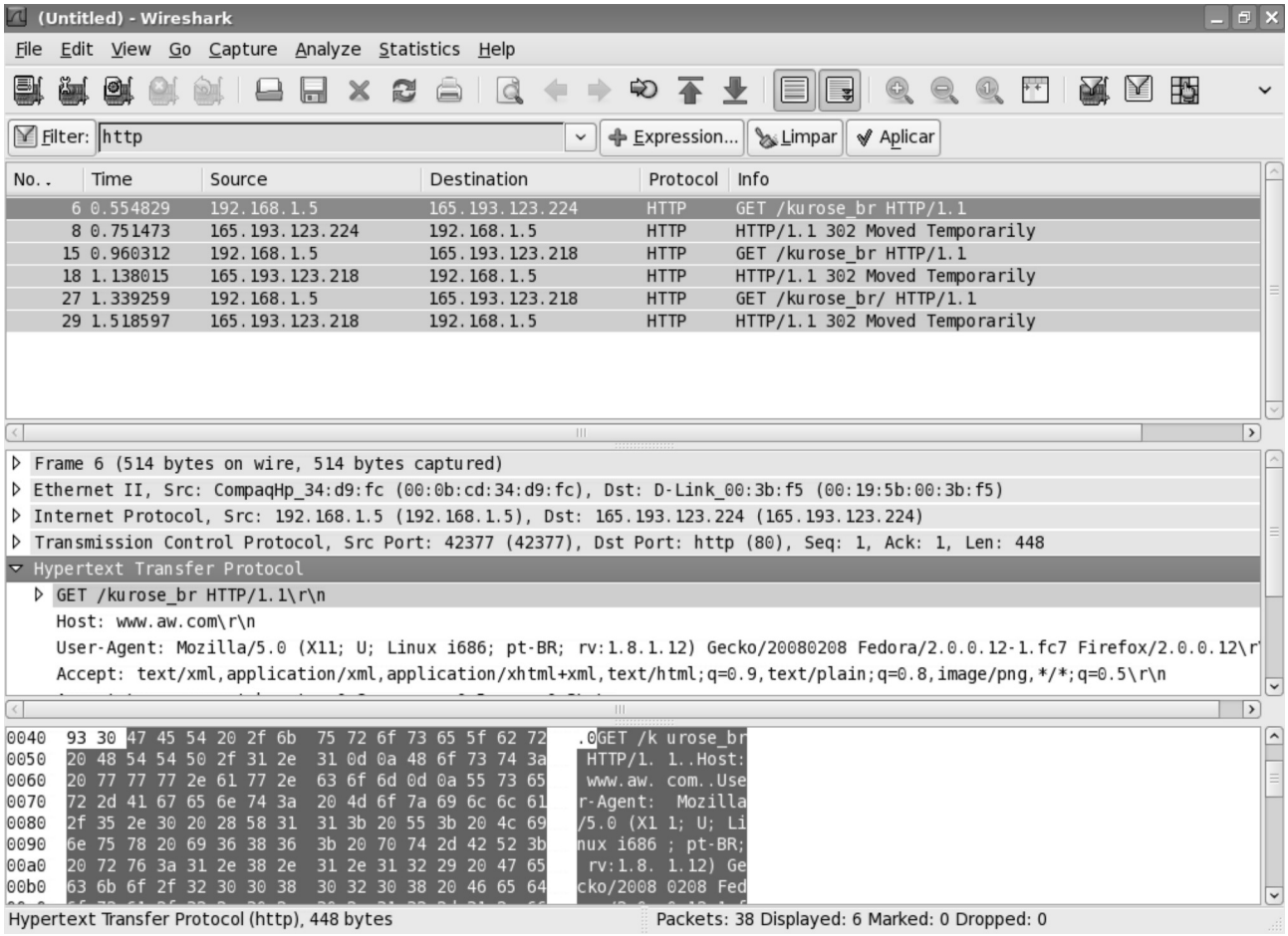

Figura 7. Mensagem HTTP GET expandida.

11. saia do Wireshark. Não precisa salvar os dados da captura de pacotes.

Parabéns! Você completou o primeiro laboratório Wireshark.

O Que Deve Ser Entregue

O objetivo deste primeiro laboratório foi principalmente introduzir o Wireshark. As seguintes questões demonstrarão que você está capacitado a executar o Wireshark e explorou algumas das capacidades dele. Responda às seguintes questões, baseando-se na experimentação realizada com o Wireshark:

1. liste os diferentes protocolos que aparecem na coluna Protocol na janela de listagem de pacotes após o passo 7;

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.aw.com? Qual é o endereço IP da interface de rede do seu computador?

4. imprima as mensagens HTTP GET e a resposta a ela (HTTP/1.1 200 OK). Para fazer isso, selecione Print no menu File, e depois “Selected Packet Only” e “Print as Displayed”. Ok (ou Imprimir) para confirmar.