Pontifícia Universidade Católica de Minas Gerais
Instituto de Ciências Exatas e Informática
Departamento de Ciência da Computação
Curso de Ciência da Computação

Laboratório de Redes e Sistemas Operacionais

Sniffer

Objetivos: Conhecer e verificar o funcionamento de um software de captura de pacotes.

"Conte-me e esquecerei.
Mostre-me e eu lembrarei.
Envolva-me e eu entenderei."
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 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.

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 ao *software* usuail 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.

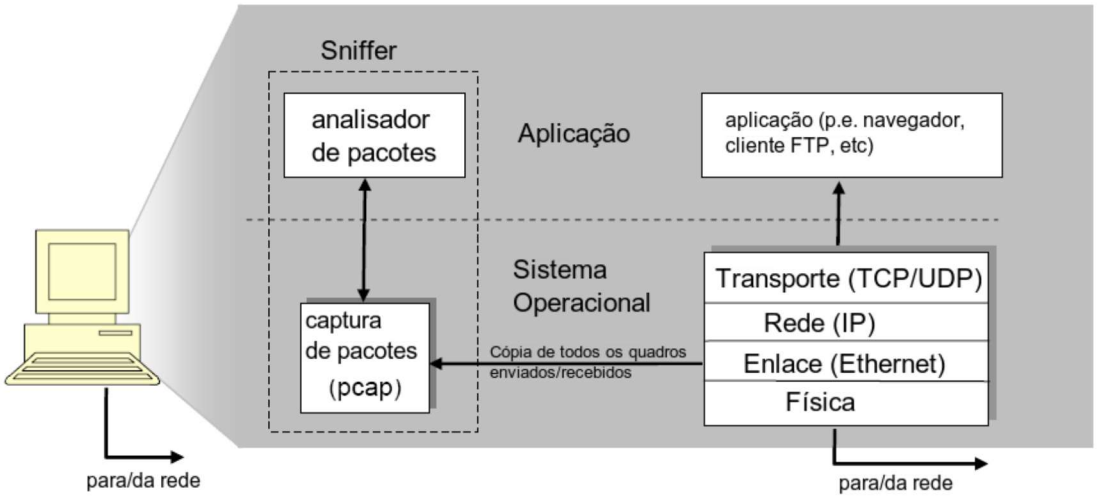

Figura 1 – Estrutura de um Sniffer.

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 o analisador de pacotes ideal, pois é estável, tem uma grande base de usuários e é bem documentado incluindo um guia de usuário, páginas de manual, e uma seção de FAQ detalhada, (http://www.wireshark.org/docs/), 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 o 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 é instalada pelo próprio arquivo de instalação do wireshark. Vá para http://www.wireshark.org, baixe e instale Wireshark para o seu sistema operacional (se for Linux, procure no repositório da distribuição que você usa). O instalador pedirá para instalar o wincap, a biblioteca de captura de pacotes. Instale-a também.

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.

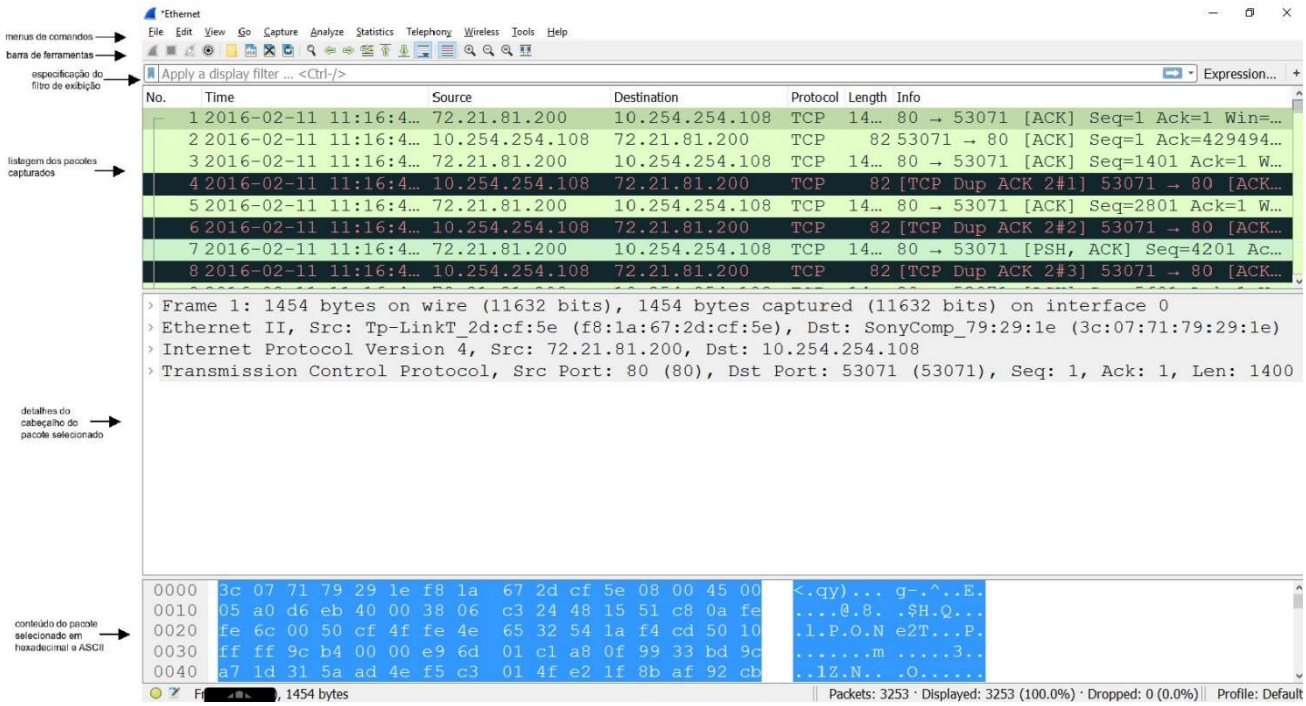

Figura 2 – Interface com o usuário do Wireshark

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 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, 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 do Wireshark

A melhor maneira de aprender um novo software é utilizando-o. Então 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 ou Options dependendo de sua versão do Wireshark. Isso faz com que a janela de interfaces de rede disponíveis seja apresentada (figura 3);

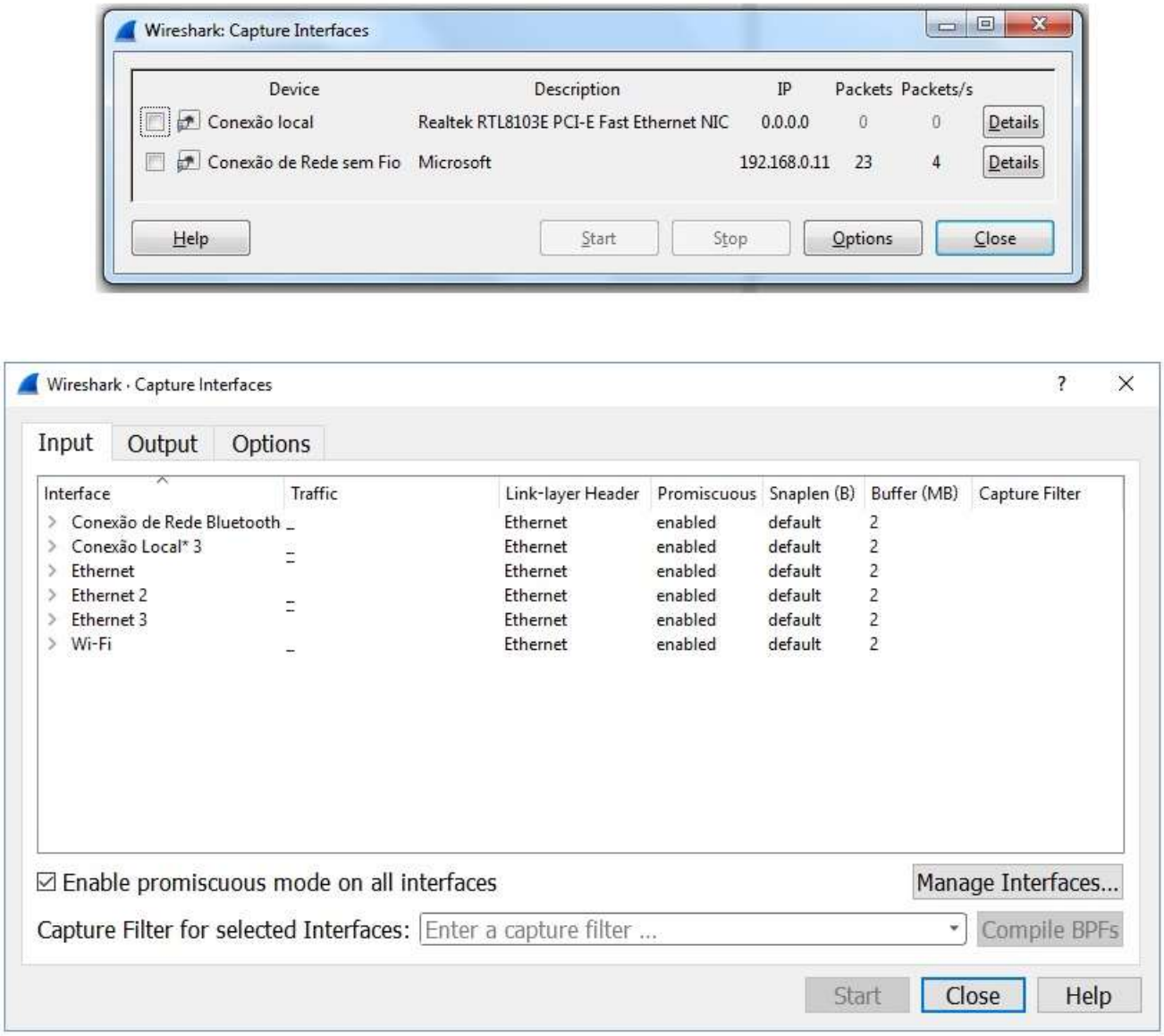

Figura 3 – Interfaces disponíveis para captura

4. Marque a interface desejada e clique em start para iniciar a captura de pacotes. Escolha conexão local se estiver usando uma rede cabeada ou conexão de rede sem fio se estiver usando uma rede wifi.

5. Se nada estiver acontecendo na rede (muito raro, pois as aplicações atualmente sempre enviam alguma informação pela rede) a janela apresenta o conteúdo vazio (figura 4);

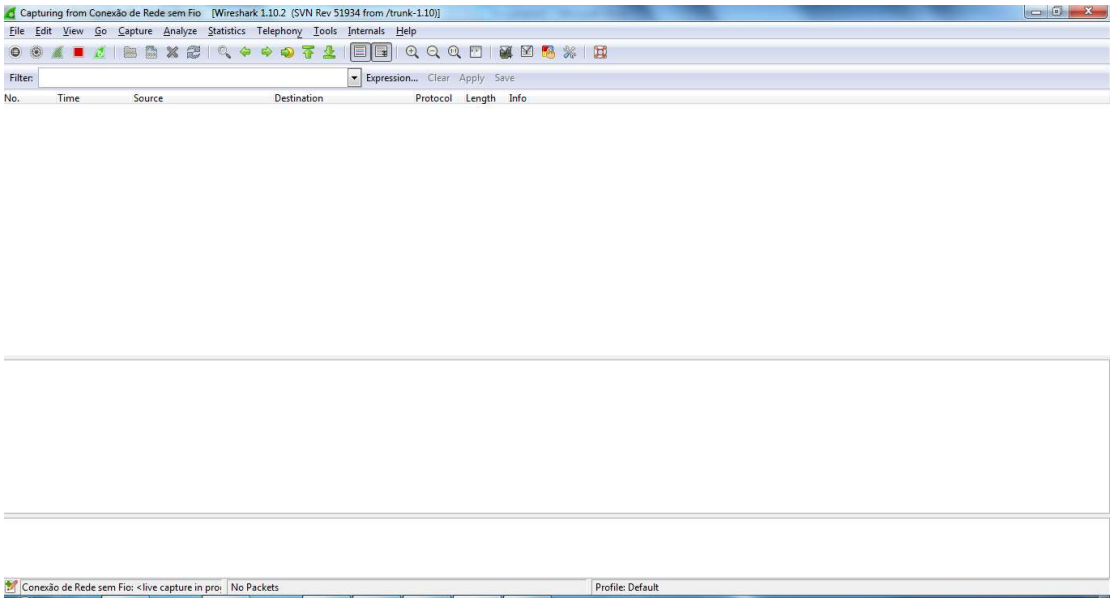

Figura 4 – Janela exibida após escolher uma das interfaces

6. no navegador, acesse www.icei.pucminas.br/alunos;

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

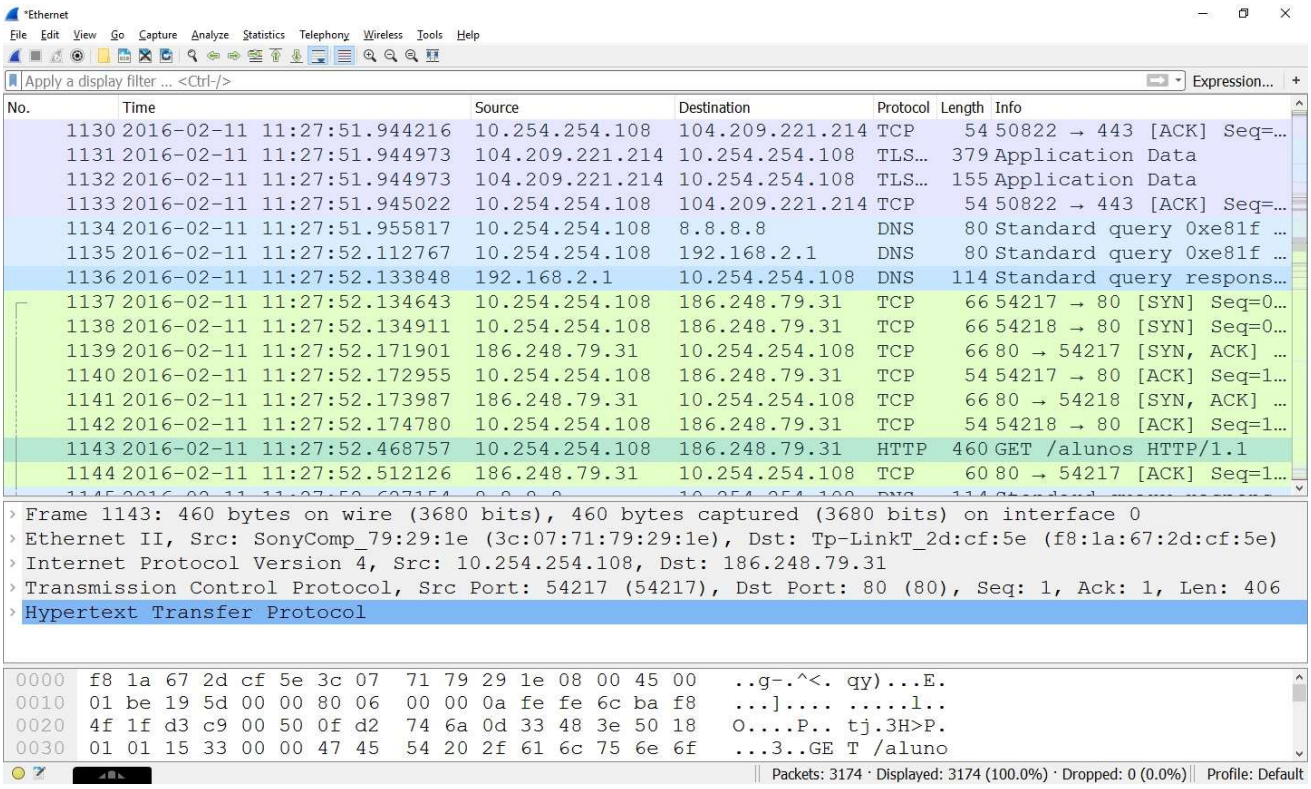

Figura 5 – captura dos pacotes da conexão aberta pelo navegador web

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) na especificação do filtro de exibição e depois selecionar Apply (ou Aplicar). O resultado é exibido na figura 6;

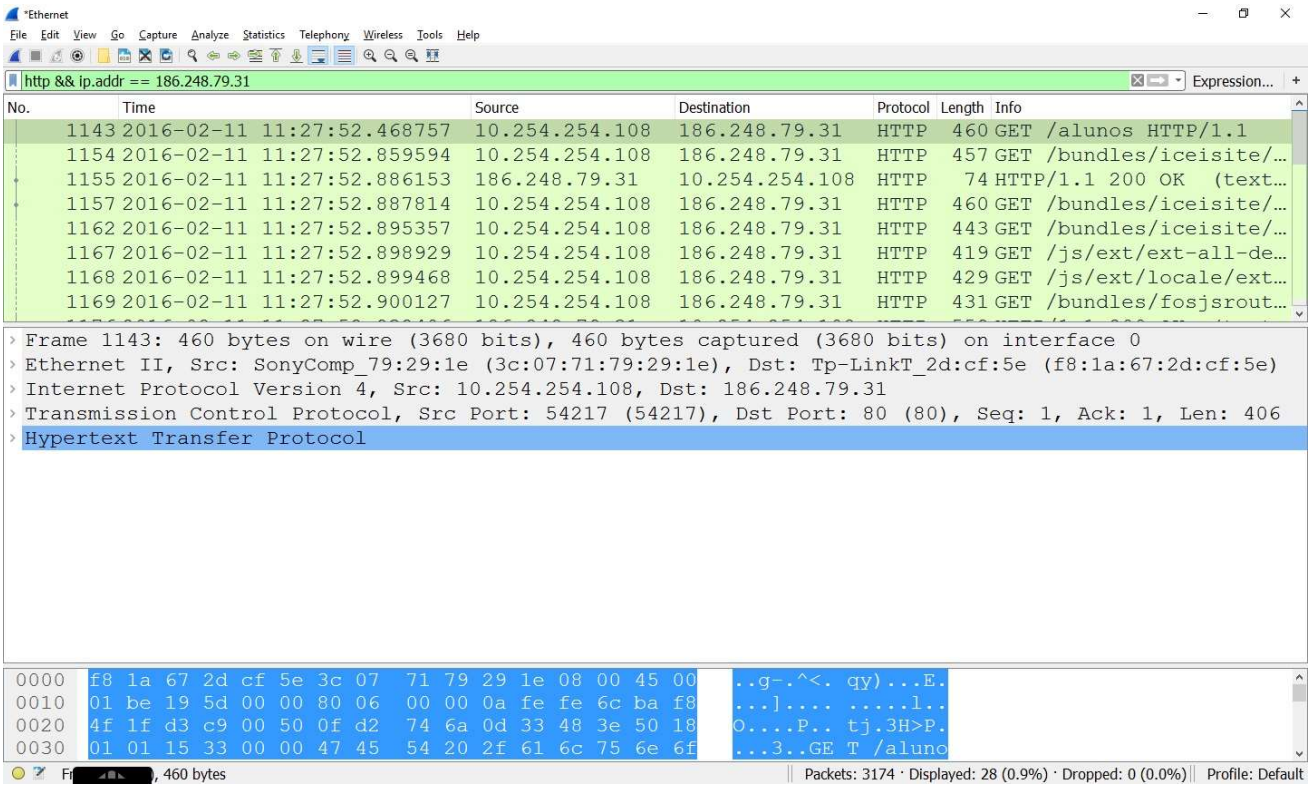

Figura 6 – janela após aplicação do filtro http

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.icei.pucminas.br. 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);

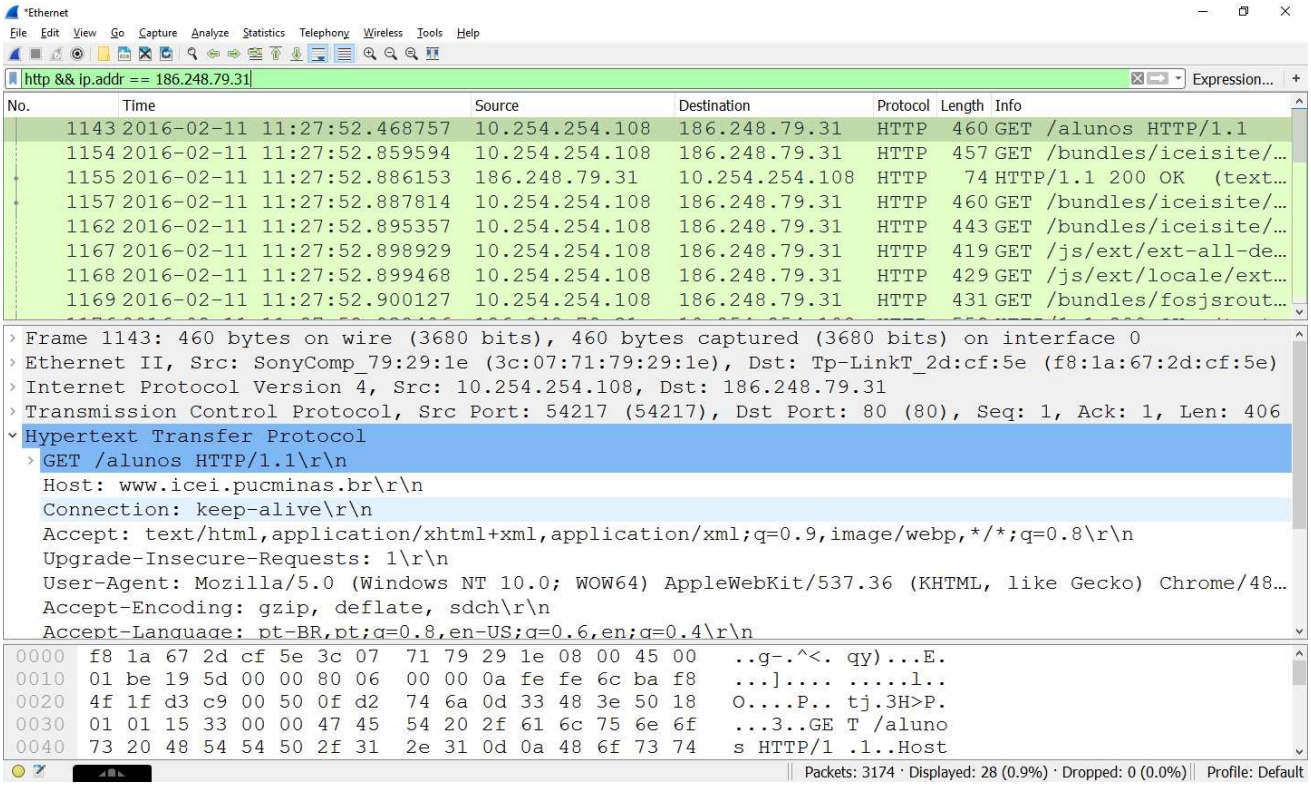

Figura 7 – Mensagem http expandida

Atividades.

Limpe o cache do seu navegador com ctrl+shift+del.

Limpe o cache dns da sua máquina. Vá ao prompt de comando e digite ipconfig /flushdns

Responda às seguintes questões, utilizando o wireshark.

Salve as respostas em um documento e grave os logs das capturas para entrega ao professor. Esta atividade será avaliada em 5 pontos.

1. Inicie a captura de pacotes com o wireshark. Acesse o prompt de comando e dê o comando **ping www.sbc.org.br**. **Pare a captura**. Faça o que se pede:

   a. Qual o endereço MAC do seu computador? Dê um print no pacote que comprove essa informação.
   b. Dê um print nos detalhes dos pacotes ICMP de solicitação e de resposta (use o filtro icmp).
   c. Qual o nome e endereço (cidade, rua, etc) do fabricante[1] do seu adaptador de rede?

[1] Acesse http://standards.ieee.org/develop/regauth/oui/oui.txt, para a lista de fabricantes de adaptadores de rede Ethernet.

d. Quais os endereços IPs de origem e de destino do ping. Dê um print no pacote que comprove essa informação.
e. Destaque os pacotes da consulta e da resposta DNS à www.sbc.org.br. (use o filtro dns). Dê um print nos pacotes que comprovem essa informação.
f. Dê um print nos detalhes do pacote da resposta DNS do item e.

2. Inicie a captura de pacotes com o wireshark. Acesse www.icei.pucminas.br/alunos. Espere alguns segundos e recarregue a mesma página no navegador. Pare a captura. Faça o que se pede:

a. Dê um print destacando os pacotes da consulta DNS e da resposta DNS à www.icei.pucminas.br/alunos (use o filtro dns).
b. Dê um print nos detalhes do pacote da resposta DNS do item a. Qual o endereço IP do site acessado?
c. Mostre os pacotes correspondentes ao handshake de três vias da conexão e o handshake de três vias da desconexão do TCP (use o filtro tcp). Dê um print destacando a conexão e um print destacando a desconexão
d. 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. (use o filtro http). Dê um print nos pacotes que comprovem seus cálculos.
e. Localize o pacote que transporta a mensagem http get ok relacionada ao recarregamento da página (use o filtro http). Dê um print no pacote que comprove essa informação. Os pacotes da página são transportados novamente do servidor para o cliente? Justifique.

3. Inicie a captura de pacotes com o wireshark. Acesse pelo navegador o site ftp.pucmg.br. Entre no diretório computação e faça o download do arquivo Normalização_artigos.pdf. Pare a captura. Faça o que se pede:

a. Dê um print e destaque os pacotes da consulta e da resposta DNS à ftp.pucmg.br. (use o filtro dns)
b. Dê um print nos detalhes do pacote da resposta DNS do item a. Qual o endereço IP do site acessado?

c. Mostre os pacotes correspondentes ao primeiro handshake de três vias da conexão e o ultimo handshake de três vias da desconexão do TCP (use o filtro tcp). Dê um print destacando a conexão e um print destacando a desconexão.
d. Quantos pacotes e qual o tamanho de cada pacote em bytes foram transferidos pelo protocolo ftp? (use o filtro ftp-data e conte todos os pacotes ou verifique o menu statistics/summary e bytes displayed). Dê um print dessa verificação.
e. Qual a porta usada pelo servidor FTP quando se usa o filtro ftp? Qual a porta usada pelo servidor FTP quando se usa o filtro ftp-data? Dê um print nos pacotes que mostrem essa informação.
f. Qual o sistema operacional do servidor FTP? Com qual usuário você está acessando o servidor de FTP? Dê um print nos pacotes que mostrem essa informação.