Laboratório 11.5.6: Estudo de Caso Final – Análise de Datagrama com Wireshark

Objetivos

Com a conclusão deste exercício, os alunos serão capazes de demonstrar:

- Como um segmento TCP é construído e explicar os seus campos.
- Como um pacote IP é construído e explicar os seus campos.
- Como um quadro Ethernet II é construído e explicar os seus campos.
- Conteúdo de uma SOLICITAÇÃO ARP e RESPOSTA ARP.

Contexto

Este laboratório exige dois arquivos de pacote capturados e o Wireshark, um analisador de protocolo de rede. Faça o download dos arquivos a seguir do servidor Eagle e instale o Wireshark em seu computador se já não estiver instalado:

- eagle1_web_client.pcap (discutido)
- eagle1_web_server.pcap (somente referência)
- wireshark.exe

Cenário

Este exercício detalha a seqüência de datagramas que são criados e enviados por uma rede entre um cliente web, um PC Client e um servidor, eagle1.example.com. Entender o processo envolvido em colocar de maneira seqüencial os pacotes na rede permitirá que o aluno resolva de maneira lógica falhas de rede quando houver perda de conectividade. Para ser breve e ter clareza, sinais indesejados de pacotes de rede foram omitidos das capturas. Antes de executar um analisador de protocolo em uma rede que pertence a outra pessoa ou organização, certifique-se de obter uma permissão por escrito.

A Figura 1 mostra a topologia deste laboratório.

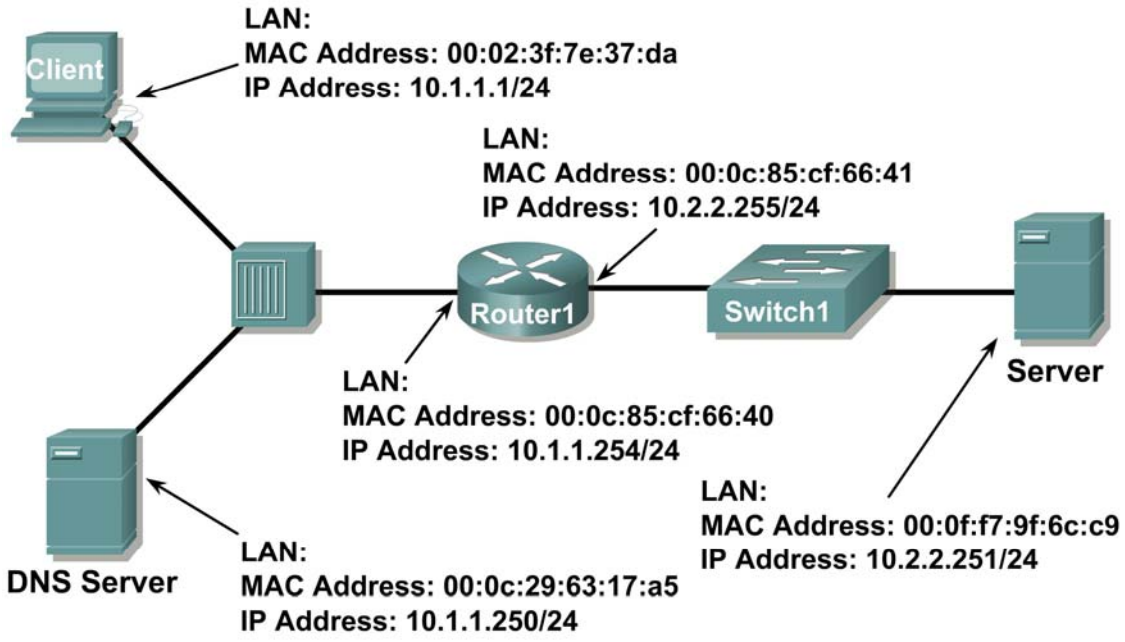

Figura 1. Topologia de Rede

Usando ferramentas Microsoft ® de linha de comando, as informações de configuração ip e os conteúdos da cache ARP são exibidos. Consulte a Figura 2.

```
C: > ipconfig / all
Windows IP Configuration
Adaptador Ethernet Conexão de Área Local:
     Específico de Conexão Sufixo DNS. :
     Descrição . . . . . . . . . . . . : Intel(R) PRO/1000 MT
                                         Conexão de Rede
     Endereço Físico. . . . . . . . . : 00:02:3f:7e:37:da
     Dhcp Habilitado. . . . . . . . . . . : Não
     Endereço IP. . . . . . . . . . . . : 10.1.1.1
     Máscara de Sub-Rede . . . . . . . . . . . : 255.255.255.0
     Gateway Padrão  . . . . . . . . . : 10.1.1.254
     Servidores DNS . . . . . . . . . . . : 10.1.1.250
C: > arp –a
Nenhuma Entrada ARP Encontrada
C: >
```

Figura 2. Estado de rede inicial do PC Client

Um cliente web é iniciado e a URL eagle1.example.com é inserida, conforme mostra a Figura 3. Isso inicia o processo de comunicação com o servidor web e onde se iniciam os pacotes capturados.

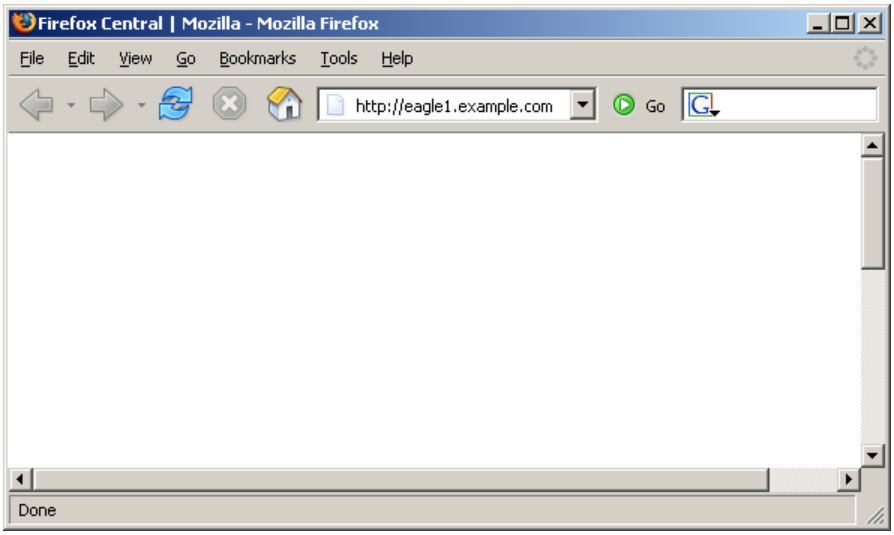

Figura 3. PC Client com navegador

Tarefa 1: Preparando o Laboratório

Passo 1: Iniciar o Wireshark em seu computador.

Consulte a Figura 4 para alterações do resultado padrão. Desmarque Main toolbar, Filter toolbar, e Packet Bytes. Verifique se Packet List e Packet Details estão marcados. Para garantir que não há tradução automática nos endereços MAC, desmarque Name Resolution for MAC layer e Transport Layer.

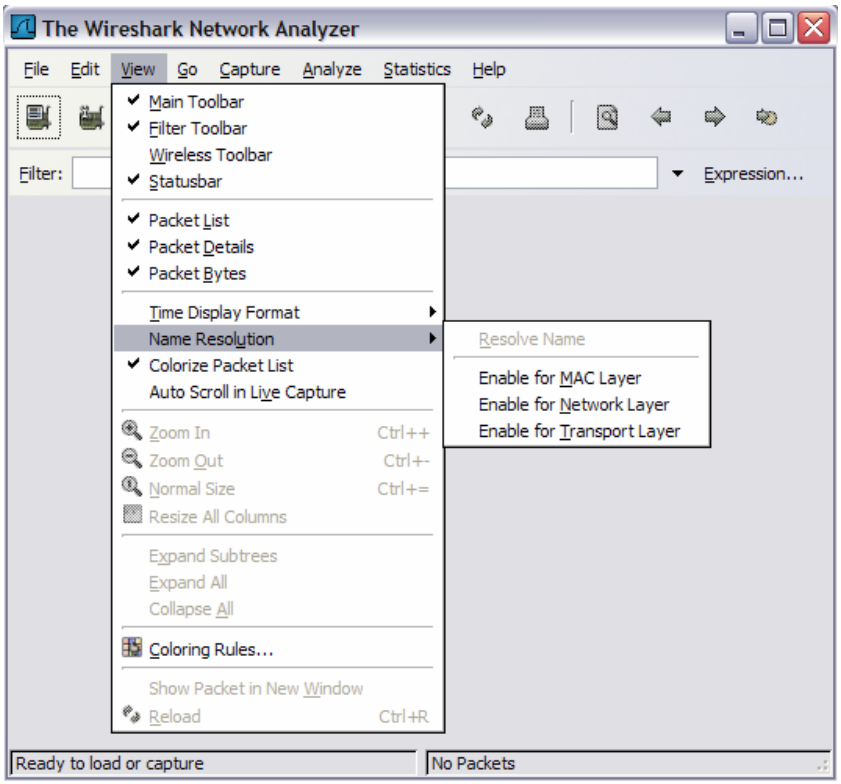

Figura 4. Alterações de visualização padrão do Wireshark

Passo 2: Carregar a captura do cliente `web, eagle1_web_client.pcap`.

Uma tela similar à Figura 5 será exibida. Vários menus e sub-menus que são abertos ao serem clicados estão disponíveis. Existem ainda duas janelas de dados separadas. A janela superior do Wireshark lista todos os pacotes capturados. A janela inferior contém detalhes de pacote. Na janela inferior, cada linha que contém uma caixa de seleção, ☒ indica que informações adicionais estão disponíveis.

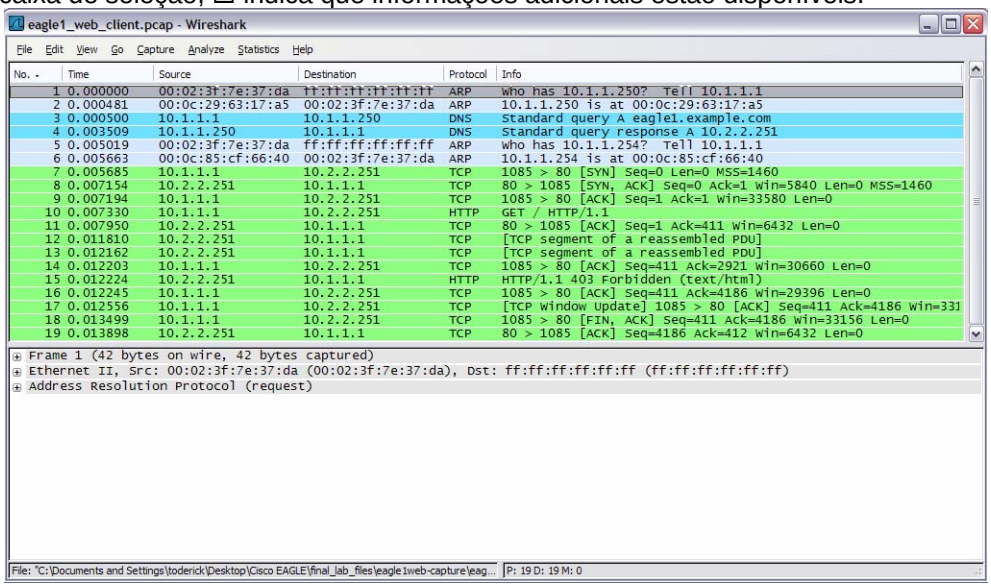

Figura 5. Wireshark com o arquivo eagle1_web_client.pcap carregado

Tarefa 2: Revisando o Processo de Fluxo de Dados pela Rede

Passo 1: Revisar a operação da camada de Transporte.

Quando o PC Client constrói o datagrama para uma conexão com o eagle1.example.com, o datagrama viaja pelas várias Camadas de rede. Em cada Camada, informações importantes de cabeçalho são adicionadas. Pelo fato de que essa comunicação é de um cliente web, o protocolo de Camada de Transporte será o TCP. Considere o segmento TCP, exibido na Figura 6. O PC Client gera um endereço de porta TCP interno, nesta conversa 1085, e sabe o endereço conhecido de porta de servidor web, 80. Da mesma forma, um número de seqüência foi gerado internamente. Os dados são incluídos, fornecidos pela Camada de Aplicação. Algumas informações não serão conhecidas do PC Client, então, elas devem ser descobertas usando-se outros protocolos de rede.

Não há número de confirmação. Antes desse segmento poder se mover para a Camada de Rede, o handshake triplo do TCP deve ser realizado.

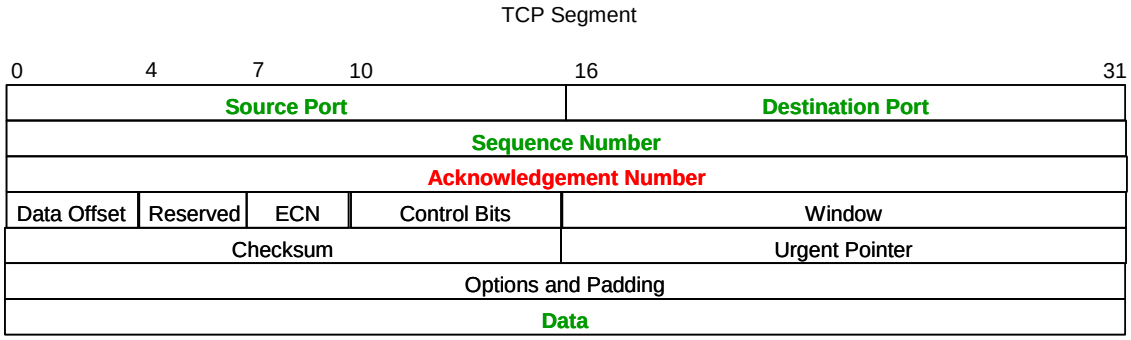

Figura 6. Campos do Segmento TCP

Passo 2: Revisar a operação da camada de Rede.

Na Camada de Rede, o PACOTE IPv4 (IP) possui vários campos prontos com informação. Isso é exibido na Figura 7. Por exemplo, a Versão do pacote (IPv4) é conhecida, bem como o endereço IP de origem.

O destino para esse pacote é eagle1.example.com. O endereço IP correspondente deve ser descoberto pelo DNS (Domain Name Services). Enquanto o datagrama da camada superior é recebido, os campos relacionados aos protocolos da camada superior estão vazios.

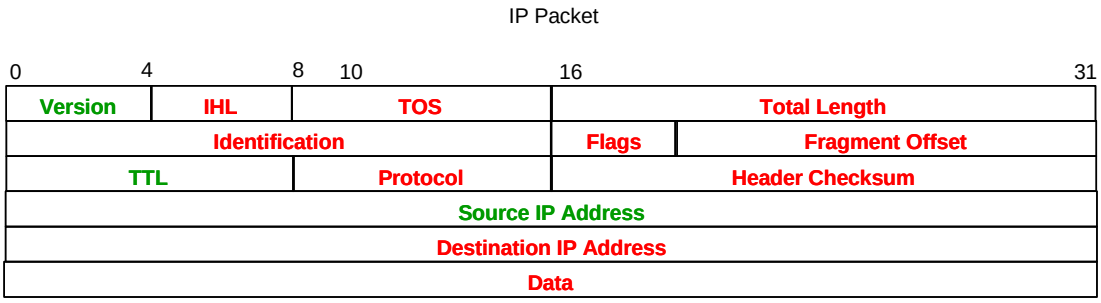

Figura 7. Campos do Pacote ip

Passo 3: Revisar a operação da camada de Enlace de Dados.

Antes do datagrama ser colocado no meio físico, ele deve ser encapsulado dentro de um quadro. Isso é exibido na Figura 8. O PC Client conhece o endereço MAC de origem, mas deve descobrir o endereço MAC de destino.

O endereço MAC de destino deve ser descoberto.

Ethernet II Frame Format

Preamble	Destination Address	Source Address	Frame Type	Data	CRC
8 Octets	**6 Octets**	**6 Octets**	2 Octets	46-1500 Octets	**4 Octets**

Figura 8. Campos do quadro Ethernet II

Tarefa 3: Analisando Pacotes Capturados

Passo 1: Revisar a seqüência de fluxo de dados.

Uma revisão de informações perdidas será de grande ajuda na hora de seguir a seqüência do pacote capturado:

a. O segmento TCP não pode ser construído porque o campo de confirmação está vazio. Um handshake triplo TCP com o eagle1.example.com deve ser primeiramente concluído.

b. O handshake triplo TCP não pode ocorrer porque o PC Client não conhece os endereços ip para o eagle1.example.com. Isso é resolvido com uma solicitação DNS do PC Client ao servidor DNS.

c. O servidor DNS não pode ser consultado porque o endereço MAC para o servidor DNS não é conhecido. O protocolo ARP é usado na LAN para descobrir o endereço MAC para o servidor DNS.

d. O endereço MAC do eagle1.example.com é desconhecido. O protocolo ARP envia uma solicitação em broadcast na LAN para aprender o endereço MAC do eagle1.example.com.

Passo 2: Examinar a solicitação ARP.

Consulte o Wireshark, janela Packet List, No 1. O quadro capturado é uma Solicitação ARP (Address Resolution Protocol ou Protocolo de Resolução de Endereço). O conteúdo do quadro Ethernet II pode ser visualizado clicando na caixa de seleção na segunda linha da janela Packet Details. O conteúdo da Solicitação ARP pode ser visualizado clicando na linha da Solicitação ARP na janela Packet Details.

1. Qual é o endereço MAC de origem para a Solicitação ARP? _____
2. Qual é o endereço MAC de destino para a Solicitação ARP? _____
3. Qual é o endereço IP desconhecido na Solicitação ARP? _____
4. Qual é o Tipo de Quadro Ethernet II? _____

Passo 3: Examinar a resposta ARP.

Consulte o Wireshark, janela Packet List, No 2. O servidor DNS enviou uma Resposta ARP.

1. Qual é o endereço MAC de origem para a Resposta ARP? _____
2. Qual é o endereço MAC de destino para a Solicitação ARP? _____

3. Qual é o Tipo de Quadro Ethernet II? _____

4. Qual é o endereço IP de destino na Resposta ARP? _____

5. Com base na observação do protocolo ARP, o que pode ser concluído sobre um endereço de destino de Solicitação ARP e um endereço de destino de Resposta ARP?
   _____
   _____
   _____

6. Por que o servidor DNS não teve de enviar uma Solicitação ARP para o endereço MAC do PC Client? _____
   _____

Passo 4: Examinar a consulta DNS.

Consulte o Wireshark, janela Packet List, No 3. O PC Client enviou uma consulta DNS ao servidor DNS. Usando a janela Packet Details, responda as perguntas a seguir:

1. Qual é o Tipo de Quadro Ethernet II? _____

2. Qual é o protocolo da Camada de Transporte, e qual é o número da porta de destino?
   _____

Passo 5: Examinar a resposta à consulta DNS.

Consulte o Wireshark, janela Packet List, No 4. O servidor DNS enviou uma resposta à consulta DNS ao PC Client. Usando a janela Packet Details, responda as perguntas a seguir:

1. Qual é o Tipo de Quadro Ethernet II? _____

2. Qual é o protocolo da Camada de Transporte, e qual é o número da porta de destino?
   _____

3. Qual é o endereço IP para o eagle1.example.com? _____

4. Um colega é um administrador de firewall, e perguntou se você pensou em algum motivo do por que todos os pacotes UDP não devem ser bloqueados na entrada da rede interna. Qual é sua resposta? _____
   _____
   _____
   _____

Passo 6: Examinar a solicitação ARP.

Consulte o Wireshark, janela Packet List, No.5 e No 6. O PC Client enviou uma Solicitação ARP ao endereço IP 10.1.1.254.

1. Este endereço IP é diferente do endereço IP do eagle1.example.com? Explique?
   _____
   _____

Passo 7: Examinar o handshake triplo de TCP.

Consulte o Wireshark, janela Packet List, No.7, No.8 e No 9. Essas capturas contêm o handshake triplo TCP entre o PC Client e o eagle1.example.com. Inicialmente, somente a flag TCP SYN é ajustada no datagrama enviado do PC Client, número de seqüência 0. O eagle1.example.com responde com as flags TCP ACK e SYN ajustadas, juntamente com um valor de confirmação 1 e seqüência 0. Na janela Packet List, existe um valor não explicado, **MSS=1460**. MSS significa tamanho Máximo de Segmento. Quando um segmento TCP é transportado sobre IPv4, o MSS é calculado para ser o tamanho máximo de um datagrama ipv4 menos 40 bytes. Esse valor é enviado durante a inicialização da conexão. É também quando as janelas deslizantes TCP são negociadas.

1. Se o valor de seqüência TCP inicial do PC Client é 0, por que o eagle1.example responde com um valor de confirmação 1?
   _____
   _____

2. Em eagle1.example.com, No.8, O que significa o valor da Flag ip 0x04?
   _____

3. Quando o PC Client concluir o handshake triplo TCP, a Packet List No 9 do Wireshark, quais são os estados da flag TCP devolvidos ao eagle1.example.com?
   _____

Tarefa 4: Concluindo a Análise Final

Passo 1: Corresponda o resultado do Wireshark ao processo.

Foi usado um total de nove datagramas enviados entre o PC Client, o servidor DNS, o Gateway e o eagle1.example.com antes do PC Client ter informações suficientes para enviar a solicitação original de cliente web para o eagle1.example.com. Isso é exibido na Packet List No.10 do Wireshark, onde o PC Client enviou uma solicitação GET de protocolo web.

1. Preencha o número correto da Packet List do Wireshark que satisfaça cada uma das entradas perdidas a seguir:

   a. O segmento TCP não pode ser construído porque o campo de confirmação está vazio. Um handshake triplo TCP com o eagle1.example.com deve ser primeiramente concluído. _____

   b. O handshake triplo TCP não pode ocorrer porque o PC Client não conhece os endereços ip para o eagle1.example.com. Isso é resolvido com uma solicitação DNS do PC Client ao servidor DNS. _____

   c. O servidor DNS não pode ser consultado porque o endereço MAC para o servidor DNS não é conhecido. O protocolo ARP é usado na LAN para descobrir o endereço MAC para o servidor DNS. _____

d. O endereço MAC para o gateway alcançar o eagle1.example.com é desconhecido. O protocolo ARP é usado na LAN para descobrir o endereço MAC de destino para o gateway. _____

2. A Packet List No.11 do Wireshark é uma confirmação do eagle1.example.com à solicitação GET do PC Client, a Packet List No 10 do Wireshark.

3. As Packet Lists No.12, 13 e 15 do Wireshark são segmentos TCP do eagle1.example.com. As Packet Lists No.14 e 16 do Wireshark são datagramas ACK do PC Client.

4. Para verificar o ACK, destaque a Packet List No 14 do Wireshark.Em seguida, vá até a parte inferior da janela Packet Details e expanda o quadro [análise SEQ/ACK]. O datagrama ACK para a Packet List No 14 do Wireshark é uma resposta a qual datagrama do eagle1.example.com?
_____

5. O datagrama da Packet List No 17 do Wireshark é enviado do PC Client ao eagle1.example.com. Revise as informações dentro do quadro [análise SEQ/ACK]. Qual é o propósito deste datagrama?
_____

6. Quando o PC Client tiver finalizado, as flags TCP ACK e FIN são enviadas, exibidas na Packet List No 18 do Wireshark.O eagle1.example.com responde com um TCP ACK, e a sessão TCP é fechada.

Passo 2: Usar o Fluxo TCP do Wireshark.

Analisar o conteúdo de pacotes pode ser uma experiência intimidante, consumindo tempo e sujeita a erros. O Wireshark inclui uma opção que constrói o Fluxo TCP em uma janela separada. Para utilizar esse recurso, primeiro selecione um datagrama TCP da Packet List do Wireshark. A seguir, selecione as opções Analyze | Follow TCP Stream do menu Wireshark. Uma janela similar à Figura 9 será exibida.

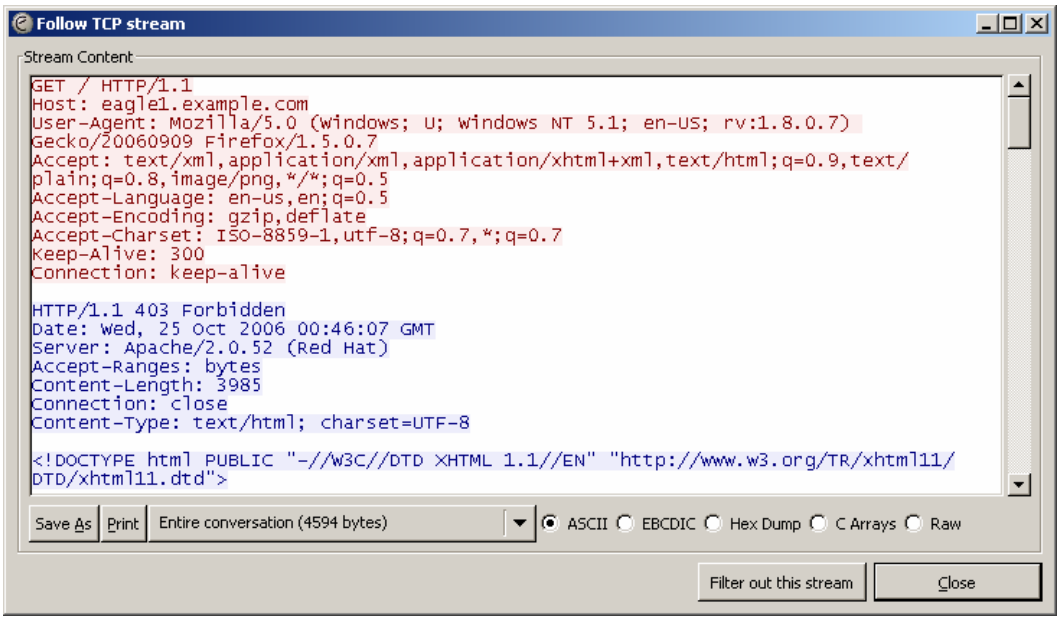

Figura 9. Resultado do fluxo TCP

Tarefa 5: Conclusão

Usar um analisador de protocolo de rede pode servir como uma ferramenta de aprendizado eficaz para compreender elementos cruciais de comunicação de rede. Uma vez estando o administrador de rede

familiarizado com os protocolos de comunicação, o mesmo analisador de protocolo pode se tornar uma ferramenta de resolução eficaz quando houver uma falha de rede. Por exemplo, poderia haver diversas causas se um navegador não conseguir se conectar a um servidor web. Um analisador de protocolo mostrará solicitações ARP sem êxito, consultas DNS sem êxito e pacotes não confirmados.

Tarefa 6: Resumo

Neste exercício, o aluno aprendeu como ocorre a comunicação entre um cliente web e um servidor web. Protocolos ocultos, tais como DNS e ARP são usados para preencher partes que faltam em pacotes ip e quadros Ethernet, respectivamente. Antes do início da sessão TCP, o handshake triplo TCP deve construir um caminho confiável e fornecer a ambas as extremidades da comunicação informações iniciais do cabeçalho TCP. Finalmente, a sessão TCP é finalizada de maneira ordenada com o cliente emitindo uma flag TCP FIN.

