Universidade Federal de Campina Grande

Unidade Acadêmica de Engenharia Elétrica

Disciplina: Redes de Computadores

Professor: Edmar Candeia Gurjão

2º Exercício Prático: HTTP

1. Introdução

Vamos agora utilizar o *Wireshark* para analisar o funcionamento do protocolo HTTP. Serão observados a interação pedido/resposta, os formatos das mensagens, recuperação de grandes arquivos, obtenção de arquivos HTML com objetos embutidos e HTML com autenticação.

2. A interação HTTP pedido/resposta básica

Iniciemos explorando o acesso a um arquivo HTML que contém somente texto e, portanto, é composto de só um objeto. Para isso siga os seguintes passos:

1. Inicie o navegador.
2. Inicie o *Wireshark* sem iniciar a captura de pacotes. Entre com *http* no filtro de pacotes, isso fará com que somente mensagens http sejam mostradas.
3. Espere alguns instantes (um minuto, por exemplo, isso será explicado depois), e então inicie a captura de pacotes.
4. No seu navegador digite o seguinte endereço: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html , seu navegador vai mostrar uma página web muito simples.
5. Pare a captura de pacotes.
6. Aplique o filtro para mensagens http (basta ir à aba *Filter* e clicar em *Apply*).

Nesse momento você deverá observar uma página bem parecida com a que está sendo mostrada na Figura 1.

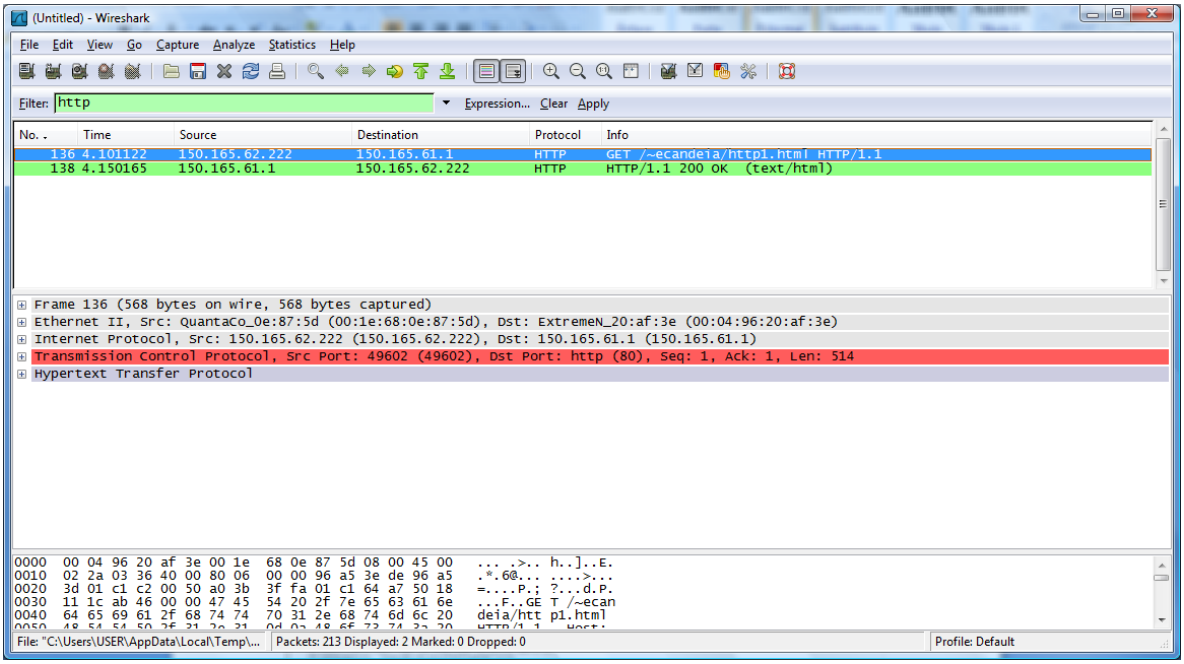

Figura 1 – Tela do Wireshark após o filtro de pacotes http do primeiro exercício.

O exemplo da Figura 1 mostra na tela de listagem de pacotes que duas mensagens HTTP foram capturadas: uma mensagem GET do navegador que está na máquina 150.165.62.222 para o servidor www.dee.ufcg.edu.br que está na máquina 150.165.61.1 e a reposta do servidor para o navegador.

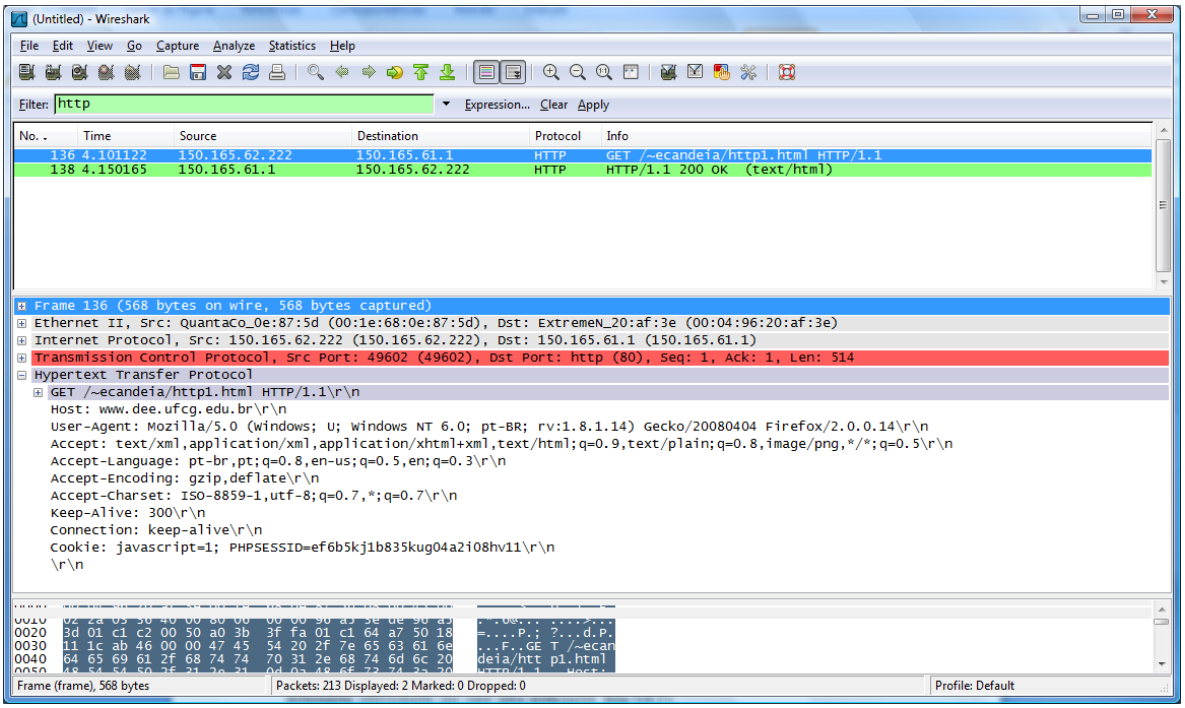

Figura 2 – Expandindo o conteúdo da mensagem http do primeiro pacote http recebido.

Indo na janela de conteúdo dos pacotes e expandindo as mensagens http, para isso basta selecionar uma mensagem e clicar no símbolo + ao lado de Hypertext Transer Protocol, e obtém-se a tela mostrada na Figura 2. Essa janela mostra os detalhes da mensagem selecionada (no caso uma mensagem http GET).

Observando a mensagem http get, responda as seguintes questões:

1. Seu navegador usar a versão 1.0 ou 1.1 do http? Qual a versão do http que está rodando no servidor?
2. Quais linguagens o navegador indica que aceita?
3. Qual o endereço IP do seu computador? E do servidor?

Observando a mensagem de resposta do servidor responda:

4. Qual o código de status que o servidor retornou para o seu navegador, o que isso significa?

5. Quando foi a última vez que o arquivo html que você baixou do navegador foi alterado?
6. Quantos bytes de conteúdo são retornados para o seu navegador?

3. A interação HTTP Condicional pedido/resposta

Muitos navegadores fazem *cache* de objetos e utilizam GET condicional quando estão solicitando objetos. Antes fazer os passos a seguir verifique que o cache do seu navegador está vazio. (Para fazer isso no Mozilla vá em Ferramentas → Opções → Privacidade → cache → Limpar Cache agora.) Agora faça o seguinte:

a) inicie o navegador,
b) Inicie o *Wireshark*
c) Entre o seguinte endereço no seu navegador http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

Seu navegador irá mostrar uma página web simples.
d) Rapidamente entre com o mesmo endereço (ou simplesmente faça o *refresh* (F5))

Para a captura de pacotes no *Wireshark* e digite http na janela de filtro e peça para aplicar.

Responda as seguintes questões:

7. Inspecione o conteúdo do primeiro pedido HTTP GET do seu navegador para o servidor. Você vê uma linha "IF-MODIFIED-SINCE" nesse HTTP GET?
8. Inspecione o conteúdo da resposta do servidor. Ele retornou explicitamente o conteúdo do arquivo?
9. Agora inspecione o conteúdo da segunda mensagem HTTP GET do seu navegador para o servidor. Você vê uma linha "IF-MODIFIED-SINCE:" nesse HTTP GET? Se vê, qual informação segue o cabeçalho "IF-MODIFIED-SINCE:"?

10. Qual o código HTTP de status e a frase retornada pelo servidor em resposta ao Segundo HTTP GET? O servidor retornou explicitamente o conteúdo do arquivo?

4. Obtendo Grandes Documentos

Nos exemplos anteriores trabalhamos com pequenos arquivos html, agora vamos observar a transferência de grandes arquivos html. Para isso faça o seguinte:

a) Inicie o navegador, limpe o *cache* como foi feito no exercício anterior.
b) Inicie a captura de pacotes no *Wireshark*
c) Entre no seu navegador com o seguinte endereços http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

Seu navegador irá mostrar uma página contendo uma texto muito longo.

d) Pare a captura de pacotes no *Wireshark*, e entre com o filtro http para que somente as mensagens http sejam mostradas.

Na janela de listagem de pacotes você pode ver sua mensagem HTTP GET seguida por uma resposta de múltiplos pacotes. Relembre que a mensagem de resposta HTTP consiste de uma linha de status, seguido pelas linhas de cabeçalho, seguido por uma linha em branco, seguido pelo corpo. No caso do nosso HTTP GET, o corpo na resposta é o arquivo HTML solicitado. Esse arquivo é muito grande para caber em um único pacote TCP, logo ele é enviado pelo servidor em vários pedaços, cada um deles segue em um pacote em separado.

Responda as seguintes questões:
11. Quantas mensagens HTTP GET forma enviadas pelo seu navegador?
12. Quantos segmentos TCP contendo dados foram necessários para transportar uma unida resposta http?
13. Qual o código de status a frase associados com a reposta ao pedido HTTP GET?

5. Documentos HTML com Objetos

Agora vamos observar a transferência de arquivos HTML com objetos, i.e. arquivos que contém imagens. Para tanto faça o seguinte:

a) Inicie o navegador e limpe o cache
b) Inicie a captura de pacotes no *Wireshark*
c) Entre com o seguinte endereço http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

Seu navegador deverá mostrar uma página HTML com algumas imagens. As imagens apresentadas são referenciadas no arquivo HTML, como foi visto seu navegador irá fazer o *download* dessas imagens.

d) Para a captura de pacotes e entre com http no filtro.

Responda as seguintes questões:

14. Quantas mensagens HTTP GET seu navegador enviou? Para quais endereços essas mensagens foram enviadas?
15. Você pode dizer se o seu navegador está fazendo o download das imagens em paralelo ou não? Explique.

6. Autenticação HTTP

Finalmente vamos visitar um site que é protegido por senha e verificar a seqüência de mensagens http trocadas com o site. Para tanto faça o seguinte:

a. Limpe o cache do seu navegador, feche-o e então reinicie.
b. Inicie a captura de pacotes no *Wireshark*
c. Vá ao site que você costuma acessar para ver seus e-mails

d. Entre com seu login e sua senha
e. Para a captura de pacotes com o *Wireshark*

Agora vamos examinar a saída. Inicialmente filtre para que somente as mensagens http sejam mostradas, responda as seguintes questões:

16. Qual a reposta do servidor (código de status e frase) em resposta à mensagem http GET inicial?
17. Quando o seu navegador envia a mensagem http GET pela segunda vez, quais novos campos são incluídos nessa mensagem?