UNIVERSIDADE FEDERAL DE OURO PRETO

DEPARTAMENTO DE COMPUTAÇÃO E SISTEMAS

REDES DE COMPUTADORES II – CSI 510

AULA PRÁTICA: Hypertext Transfer Protocol: HTTP (WIRESHARK)

Nesta aula prática usando o Wireshark, exploraremos os vários aspectos do protocolo HTTP: a interação básica GET/response, formatos de mensagens HTTP, recuperação de arquivos HTML grandes e arquivos HTML com objetos embutidos.

A INTERAÇÃO BÁSICA HTTP GET/RESPONSE

Começaremos realizando o download de um arquivo simples HTML que além de pequeno não contém objetos embutidos. Faça o seguinte:

1. Inicie o seu navegador (browser).

2. Inicie o programa Wireshark como descrito na prática anterior (mas não inicie a captura de pacotes ainda). Digite http na janela de filtro para mostrar somente pacotes HTTP capturados.

3. Inicie a captura de pacotes com o Wireshark.

4. Digite o endereço no seu navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html. Seu navegador deve mostrar um arquivo HTML simples de uma única linha.

5. Finalize a captura de pacotes pelo Wireshark.

Sua interface deve estar similar com a interface do Wireshark ilustrada na Figura 1.

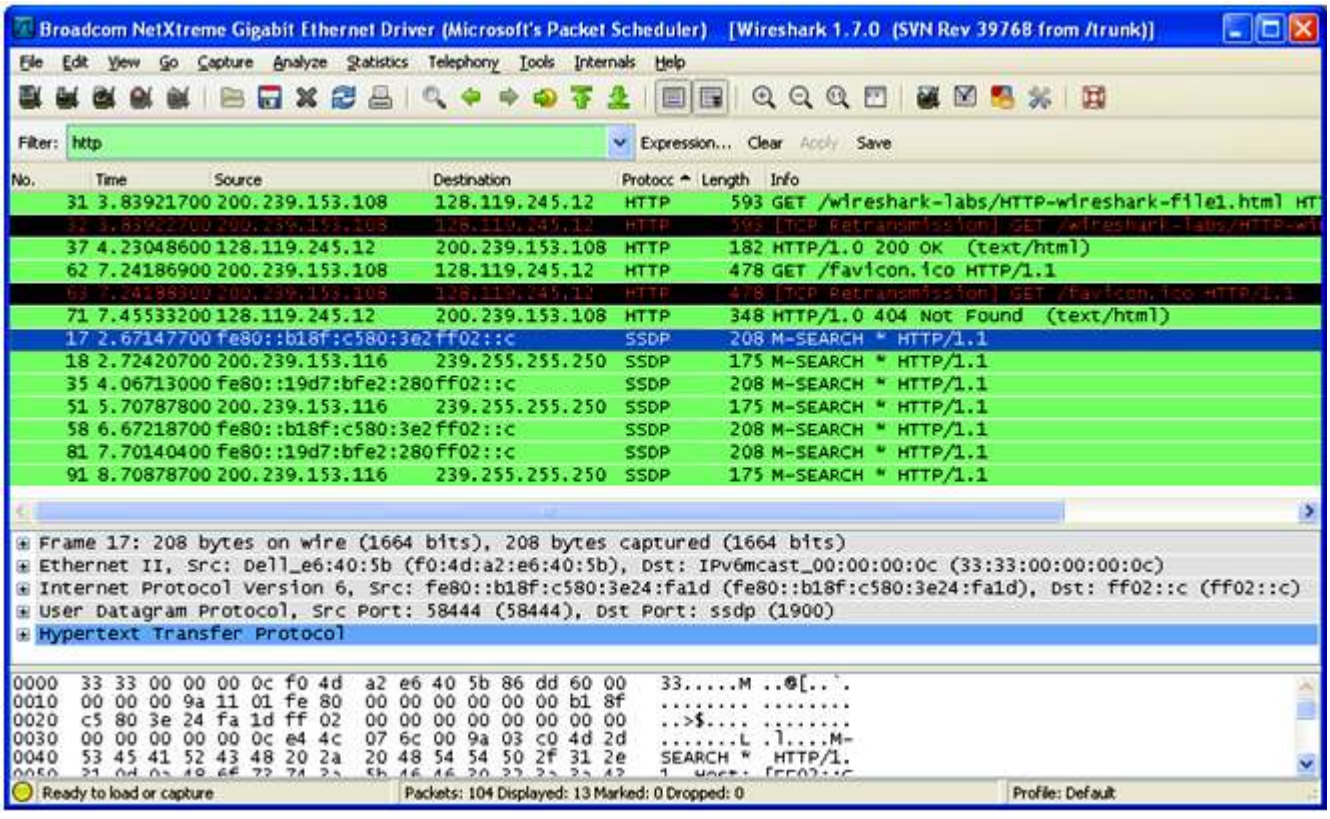

Figura 1 - Wireshark após realização dos passos anteriores descritos

O exemplo na Figura 1 mostra algumas mensagens HTTP na lista de pacotes. É possível visualizar a mensagem GET (#31) (enviada do seu navegador para o servidor gaia.cs.umass.edu web) e a mensagem response do servidor para o seu navegador (#37). O conteúdo dos pacotes mostram os detalhes de cada mensagem selecionada.

Analisando esses dados das mensagens analisadas, responda às seguintes questões (a serem entregues):

1. Seu navegador está executando qual versão do HTTP 1.0 ou 1.1? Qual versão do HTTP está sendo executada no servidor?

2. Qual é o código de retorno da mensagem dado pelo servidor para o seu navegador?

3. Quando o arquivo HTML que você recuperou foi modificado pelo servidor?

4. Quantos bytes de conteúdo estão sendo retornados para o seu navegador?

A INTERAÇÃO CONDICIONAL HTTP GET/RESPONSE

A maioria dos navegadores usam caching de objetos e assim desempenham um GET condicional quando recuperam um objeto HTTP. Antes de executar os passos abaixo, esteja seguro de que o cache do seu navegador está vazio.

(Nota: Geralmente as configurações de cache do navegador estão na aba de "Opções" ou "Ferramentas". Após encontrar a opção, limpe o cache do navegador). Então continue:

• Inicie o navegador.

• Inicie a captura do tráfego HTTP com o Wireshark.

• Digite a seguinte URL no navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html. Seu navegador mostrará um arquivo HMTL de cinco linhas.

• Digite rapidamente a mesma URL no seu navegador novamente (ou simplesmente selecione o botão F5 "atualizar" do navegador).

• Finalize a captura de pacotes pelo Wireshark e digite http na janela de filtros do Wireshark para mostrar somente mensagens HTTP capturadas.

Responda às seguintes questões:

5. Inspecione os conteúdos da primeira mensagem HTTP GET enviada do seu navegador para o servidor. Você vê uma linha IF-MODIFIED-SINCE na mensagem HTTP GET?

6. Inspecione os conteúdos da resposta do servidor. O servidor retornou explicitamente os conteúdos do arquivo?

7. Agora inspecione o conteúdo da segunda mensagem HTTP GET enviada pelo seu navegador para o servidor. Você vê uma linha IF-MODIFIED-SINCE na mensagem HTTP GET? Se a resposta for sim, que informação esta linha contém?

8. Qual é o código de estado HTTP e a frase retornada pelo servidor em resposta à segunda mensagem HTTP GET? O servidor retornou explicitamente os conteúdos do arquivo? Explique.

RECUPERANDO DOCUMENTOS HTTP LONGOS

Nos exemplos anteriores, os arquivos HTML são simples e pequenos. Para ver o que ocorre quando realizamos o download de um arquivo longo HTML faça o seguinte:

• Inicie o navegador e esteja seguro de que o cache está limpo (como descrito anteriormente).

• Inicie a captura do tráfego HTTP com o Wireshark.

• Digite a seguinte URL no seu navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html. Seu navegador deve mostrar um documento que mostre “The US Bill of Rights” como título.

• Finalize a captura de pacotes pelo Wireshark e digite http na janela de filtros para que apenas as mensagens HTTP sejam mostradas.

Na lista de pacotes capturados, você pode ver a mensagem HTTP GET seguida de várias mensagens HTTP response (ou não). Isso pode ocorrer devido a resposta ser maior do que o campo da mensagem HTTP que recebe a página para retornar ao navegador (e mais longo que um pacote TCP). Então, a mensagem HTTP response é quebrada em vários pedaços pelo TCP, com cada pedaço da mensagem sendo enviado por um segmento TCP separado. Cada segmento TCP é registrado pelo Wireshark como uma mensagem separada e de fato um único HTTP response foi fragmentado através de múltiplos pacotes TCP.

Responda às seguintes questões:

9. Quantas mensagens HTTP GET foram enviadas pelo seu navegador?

10. Quantos segmentos TCP contendo dados foram necessários para carregar uma única mensagem HTTP response?

11. Qual é o código de estado e a frase associada com a resposta para a mensagem HTTP GET?

DOCUMENTOS HTML COM OBJETOS EMBUTIDOS

Agora, vamos ver o que ocorre quando o navegador realiza o download de um arquivo HTML com objetos embutidos, ou seja, um arquivo que contenha imagens, por exemplo. Faça o seguinte:

• Inicie o navegador e esteja seguro de que o cache está limpo (como descrito anteriormente).

• Inicie a captura do tráfego HTTP com o Wireshark.

• Digite a seguinte URL no seu navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html. Seu navegador deve mostrar um documento HTML com duas imagens (que são referenciadas no documento HTML, mas que não estão inseridas nele como o habitual).

Nota: lembre que as imagens tem seu próprio URL que é referenciada no código HTML dentro do documento recuperado.

• Finalize a captura de pacotes pelo Wireshark e digite http na janela de filtros para que apenas as mensagens HTTP sejam mostradas.

Responda às seguintes questões:

12. Quantas mensagens HTTP GET foram enviadas pelo seu navegador? Para qual endereço da Internet as mensagens HTTP GET foram enviadas?

13. Você pode dizer se o seu navegador realizou o download das duas imagens de forma serial ou paralela? Explique. Quais as vantagens de cada método?

ARQUIVOS HTTP/HTTPS COM QUIC

Feche o browser, reinicie a captura de pacotes no Wireshark, abra o Chrome e faça uma pesquisa sobre o “Bloqueio X cloudflare” no Google. Agora abra o site da UFOP. Após isto, finalize a captura de pacotes.

14. Qual o percentual de pacotes utilizando o protocolo QUIC? Seu host estava utilizando IPv4 ou IPv6? Qual percentual dos pacotes HTTP/HTTPS?

15. Abra os pacotes no início da conexão QUIC. O campo SCID e DCID do QUIC podem ser comparados à quais parâmetros do protocolo TCP? Qual versão do TLS ele utiliza?