

**Engenharia de Computação**

**Laboratório de Redes de Computadores I**

**Aula Prática 7 – Protocolo HTTP**

**Objetivo:** Utilizando o programa *sniffer Wireshark*, verificar as características e funcionalidades do protocolo HTTP.

**Descrição:**

Nesta aula, investigaremos o comportamento e as características do protocolo HTTP.

O protocolo HTTP é o protocolo responsável pela troca de mensagens entre um cliente, *browser*, e um servidor web. Toda vez que digitamos uma URL no nosso *browser*, estamos realizando uma requisição HTTP a algum servidor web. Este retorna uma resposta. O objetivo desta aula é verificar os tipos de requisições e respostas HTTP, bem como o conteúdo das mensagens deste protocolo e o seu funcionamento.

1. Abra uma janela de terminal.
2. Digite **ipconfig /all** (Windows) ou **ifconfig** (Linux). Qual é o número IP da máquina que você está utilizando?

172.16.2.113

1. Digite **nslookup gaia.cs.umass.edu**. Qual é o número IP deste servidor web?

200.131.36.253

1. Abra o *browser* e minimize a janela.
2. Inicie o **Wireshark**.
3. Clique no campo **Filter** e digite **http and ip.addr==IP da sua máquina**. Clique no botão **apply**. Clique no menu **Capture** e selecione **Options**. Selecione a interface de rede disponível (Ethernet). Clique em **Start** e espere até que apareça na tela que pacotes estão sendo capturados.
4. Volte para o *browser* e acesse o endereço:

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

1. Pare a captura de pacotes do Ethereal. Na tela superior do Ethereal, devem aparecer informações sobre 2 pacotes HTTP: um pacote de requisição, **GET**, do seu browser para o servidor proxy e outro pacote de resposta.
2. Clique na linha da mensagem **GET**. Preste atenção no endereço IP de origem, *Source*, e Destino, *Destination*, para verificar se as mensagens analisadas são as geradas ou recebidas pelo ou para o seu computador. Na tela intermediária, aparecem os detalhes de cada pacote, inclusive sobre os pacotes TCP, IP e Ethernet, correspondentes aos pacotes HTTP selecionados. Clique na ⊳ que está no lado esquerdo da expressão **Hypertext Transfer Protocol** e na ⊳ que estiver dentro e responda:
   1. Qual é a versão do HTTP que está sendo utilizada: HTTP/1.0 ou HTTP/1.1?

HTTP/1.1

* 1. Qual idioma, *Accept-Language*, o browser utiliza?

pt-BR

* 1. Qual é o endereço IP do seu computador? E o do destinatário? Este IP é o do servidor gaia.cs.umass.edu (veja sua resposta do item 4)? Sua requisição passou por um servidor *proxy*? Se sim, qual é o IP do *proxy*?

172.16.2.113

128.119.245.12

1. Na tela superior, clique na linha correspondente à mensagem de resposta do servidor, a que aparece OK à direita. Na tela intermediária, clique na ⊳ que está no lado esquerdo da expressão **Hypertext Transfer Protocol** e na ⊳ que estiver dentro e responda.
2. Qual é o código de estado, *Response Code*, retornado pelo servidor para o browser?

200

1. Quando foi a última atualização, *Last-Modified*, do arquivo HTML?

Fri, 12 Apr 2019 05:59:01 GMT

1. Quantos bytes de conteúdo, *Content-Length*, foram retornados para o browser?

128 bytes

1. Veja que a data da última atualização é próxima à data atual. Isso acontece porque o servidor *gaia* está configurado para indicar a data corrente e não uma data real de atualização do arquivo.
2. Inicie uma nova captura de pacotes no **Wireshark** e acesse, pelo *browser*, o endereço abaixo. Depois que a página carregar a primeira vez, clique em **Atualizar** ou na tecla **F5**, para carregar a página uma segunda vez. Isto significa que você executará a requisição da mesma página 2 vezes, uma após a outra.

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

1. Depois de carregar a página 2 vezes (usando F5 ou o botão atualizar do navegador), pare a captura de pacotes. Procure pelas mensagens das 2 requisições e as 2 respectivas respostas e responda:
2. Analise o conteúdo da primeira requisição HTTP GET do seu browser para o servidor. Há alguma informação do tipo “IF-MODIFIED-SINCE”?

não

1. Analise o conteúdo da primeira resposta do servidor. Veja na tela intermediária a informação *Line-based text data*... e clique na ⊳ para expandir esta informação. O servidor retornou o conteúdo do arquivo?

SIm

1. Agora analise a segunda requisição HTTP GET. Há alguma informação do tipo “IF-MODIFIED-SINCE”? Se sim, qual informação está depois de “IF-MODIFIED-SINCE:”?

If-Modified-Since: Wed, 24 Apr 2019 05:59:01 GMT\r\n

1. Qual é o código de estado http, *Response Code*, retornado pelo servidor na segunda resposta? O servidor retornou o conteúdo do arquivo? Explique.

Not modified. Não. Pois a página que já foi recebida pelo computador e não foi alterada, não sendo necessário reenviar.

1. Inicie uma nova captura de pacotes e acesse o endereço:

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

1. Pare a captura de pacotes. Na tela superior, clique na linha referente à resposta da requisição HTTP e verifique na tela intermediária que a resposta HTTP foi segmentada em alguns pacotes TCP, **Reassembled TCP segments**.... Isso ocorre porque o arquivo enviado pelo servidor é um pouco grande, 4500 bytes, e não cabe em um pacote TCP apenas. Então a resposta é dividida em alguns pacotes TCP.
2. Responda:
   * 1. Quantas requisições HTTP GET foram enviadas pelo seu *browser*?

1

* + 1. Em quantos pacotes TCP a resposta foi segmentada (**Reassembled TCP Segments**. Repare no número de pacotes que aparecem com o símbolo # na frente)?

3

1. Inicie uma nova captura de pacotes e acesse o endereço:

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file5.html>

1. Espere a página carregar completamente, devem aparecer 2 imagens, e pare a captura de pacotes. Esta página contém requisições para outros 2 objetos, as 2 imagens que aparecem na página, que estão em outros servidores web, fora do servidor *gaia*. Quando uma página requisita outros objetos, o protocolo HTTP pode fazer requisições em série ou em paralelo. No primeiro caso, cada requisição só é feita após a requisição anterior ter recebido uma resposta, como aparece na tela abaixo. No segundo caso, as requisições são enviadas pelo browser simultaneamente.
2. Responda:
3. Quantas requisições HTTP GET foram enviadas pelo seu *browser*? Para quais endereços, *proxy* ou outros servidores, estas requisições foram enviadas?

3. ip = 128.119.245.12

1. Você pode dizer se o seu *browser* fez o *download* das 2 imagens em série ou em paralelo? Explique.

Paralelo. Pois as portas de destino e origem do computador são diferentes em cada GET.

1. No *browser*, acesse o endereço (o IP será informado pela professora):

http://IP\_PROFESSORA/teste\_login.html

1. Inicie uma nova captura de pacotes no **Wireshark**. Digite na página um usuário fictício **fulano** e a senha **123456**. Clique no botão **Enviar** e espere a página de resposta.
2. Pare a captura de pacotes. Você enviou os dados de usuário e senha pelo pacote HTTP POST. Clique nesta linha. Na tela intermediária, clique na ⊳ para expandir as informações. Responda:
   1. Você consegue encontrar as informações de login e senha digitados no item anterior?

Sim.

* 1. A autenticação do HTTP é segura? Por quê?

Não, pois qualquer um na rede pode ter acesso aos dados de login do usuário, a partir da inspeção de pacotes.

1. Salve suas respostas num arquivo nomeado com seu nome e envie-o pelo SIGAA.