



Redes de computadores

Prof. Dr. Bruno da Silva Rodrigues

Bruno.rodrigues@mackenzie.br

Análise de protocolo HTTP usando Wireshark.

Procedimentos:

Vamos começar nossa exploração do protocolo HTTP baixando um arquivo HTML simples que não contém objetos incorporados.

Para realizar a atividade, faça o download do arquivo **HTTP.pcap** no moodle e abra o arquivo no Wireshark.

- O arquivo disponível no moodle foi gerado a partir dos procedimentos descritos abaixo (não precisa realizar os procedimentos novamente):

1. Inicie o seu navegador.

2. Inicie o software Wireshark (mas ainda não inicie a captura de pacotes). Digite o "http" na janela de exibição de filtro de especificação, de modo que apenas pacotes do protocolo HTTP capturados durante o procedimento sejam apresentadas na janela de listagem de pacotes. (Nós estamos apenas interessados no protocolo HTTP, e conseqüentemente não há necessidade de avaliar todos os pacotes capturados pelo wireshark).

3. Comece a captura com o Wireshark.

4. Digite a seguinte URL no seu navegador:

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

Obs. O site acessado através da URL é muito simples e contém somente uma linha de arquivo HTML.

5. Pare a captura de pacotes no Wireshark.

Objetivos da atividade:

- Estudar o protocolo HTTP através do estudo dos cabeçalhos de requisição e resposta definidos na RFC2616.

Bibliografias

KUROSE, J. F. e ROSS, K. W. Redes de Computadores e a Internet – Uma Nova Abordagem – Pearson

M. A. Filippetti - Samuel Henrique Bucke Brito - Visual books

Wireshark ORG

Disponível em:
<https://www.wireshark.org/>

Internet Engineering Task Force.

Disponível em:
<https://tools.ietf.org/html/rfc792>

Observação 1: Caso queira verificar as diferenças entre o arquivo disponibilizado e um arquivo gerado na sua casa, realize o procedimento passo a passo acima no seu computador e compare a diferença entre as informações presentes nos dois arquivos.

Agora que você já entendeu como o arquivo **HTTP.pcap disponível no moodle foi gerado, vamos abrir o arquivo no Wireshark para análise.**

Para iniciar a atividade, localize os pacotes de solicitação e resposta do protocolo HTTP trocados entre cliente e servidor para acessar a página localizada na URL: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

Observação 2: Todas as respostas devem estar em negrito na cor vermelha

Atividade:

Questão 1(1,0). Localize os pacotes HTTP e analise os detalhes dos pacotes. Com base na arquitetura TCP/IP, cite o nome das camadas, assim como os protocolos usados em cada camada durante o envio da solicitação ou da resposta do HTTP.

O método de solicitação HTTP foi o GET

Questão 2(1,0). Analise a versão do protocolo HTTP usado na requisição e responda:

a) Qual a versão do protocolo HTTP está sendo usada (HTTP 1.0, HTTP 1.1 ou HTTP 2)?

O protocolo utilizado é o HTTP 1.1

b) Qual a vantagem de usar a versão HTTP 1.1 em detrimento da versão HTTP 1.0?

A versão HTTP 1.1 tem vantagens sobre a versão HTTP 1.0, como conexões persistentes, suporte a pipelining e melhorias no controle de cache, que melhoram o desempenho e reduzem a latência da rede.

Questão 3(1,0). Avaliando as linhas de cabeçalho, quais idiomas o seu navegador pode aceitar?

Português (pt-BR) e Inglês (en)

Questão 4(1,0). Qual é o endereço de IP do cliente? Qual o endereço IP do servidor gaia.cs.umass.edu?

Endereço IP cliente: 192.168.123.190

Endereço IP servidor: 128.119.245.12

Questão 5(1,0). Quantas solicitações HTTP foram realizadas para o servidor Gaia (verificar endereços IPs das solicitações)? Apresente um print da tela com os pacotes que você usou como base para sua resposta.

177	2.264989	192.168.123.190	128.119.245.12	HTTP	561	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
197	2.768744	128.119.245.12	192.168.123.190	HTTP	182	HTTP/1.1 200 OK (text/html)
199	2.802667	192.168.123.190	128.119.245.12	HTTP	507	GET /favicon.ico HTTP/1.1
212	3.062286	128.119.245.12	192.168.123.190	HTTP	557	HTTP/1.1 404 Not Found (text/html)

Foram feitas 2 solicitações do IP local para o IP do servidor.

Questão 6(1,0). Qual ou quais (no caso de mais de um) os códigos de status retornados pelo servidor para o cliente? Apresente um print da tela com os pacotes que você usou como base para sua resposta e interprete o(s) código(s) de status explicando o significado dos valores.

```
182 HTTP/1.1 200 OK (text/html)
557 HTTP/1.1 404 Not Found (text/html)
```

O código de resposta web 200 indica que a requisição foi bem-sucedida e que o servidor retornou os dados solicitados pelo cliente.

Já o código de resposta web 404 indica que o servidor não encontrou o recurso solicitado pelo cliente. Isso pode ocorrer quando a URL está incorreta ou quando o recurso foi movido ou removido do servidor.

Questão 7 (1,0). Localize quais portas estão sendo usadas pelo cliente e pelo servidor Gaia?

Porta do cliente: 49975

Porta do Servidor: 80

a) Como foram atribuídas as numerações de portas acima?

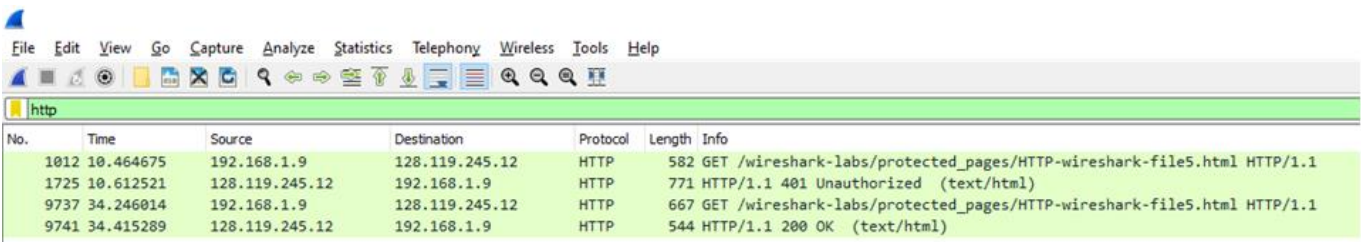
```
Source Port: 49975
Destination Port: 80
```

Questão 8 (1,0). Nas linhas de cabeçalho da requisição HTTP podemos ver a opção "Accept-Encoding". Busque em diferentes fontes de informação o significado desta opção do cabeçalho e qual a vantagem do "Encoding" nas requisições HTTP?

```
Accept-Encoding: gzip, deflate\r\n
```

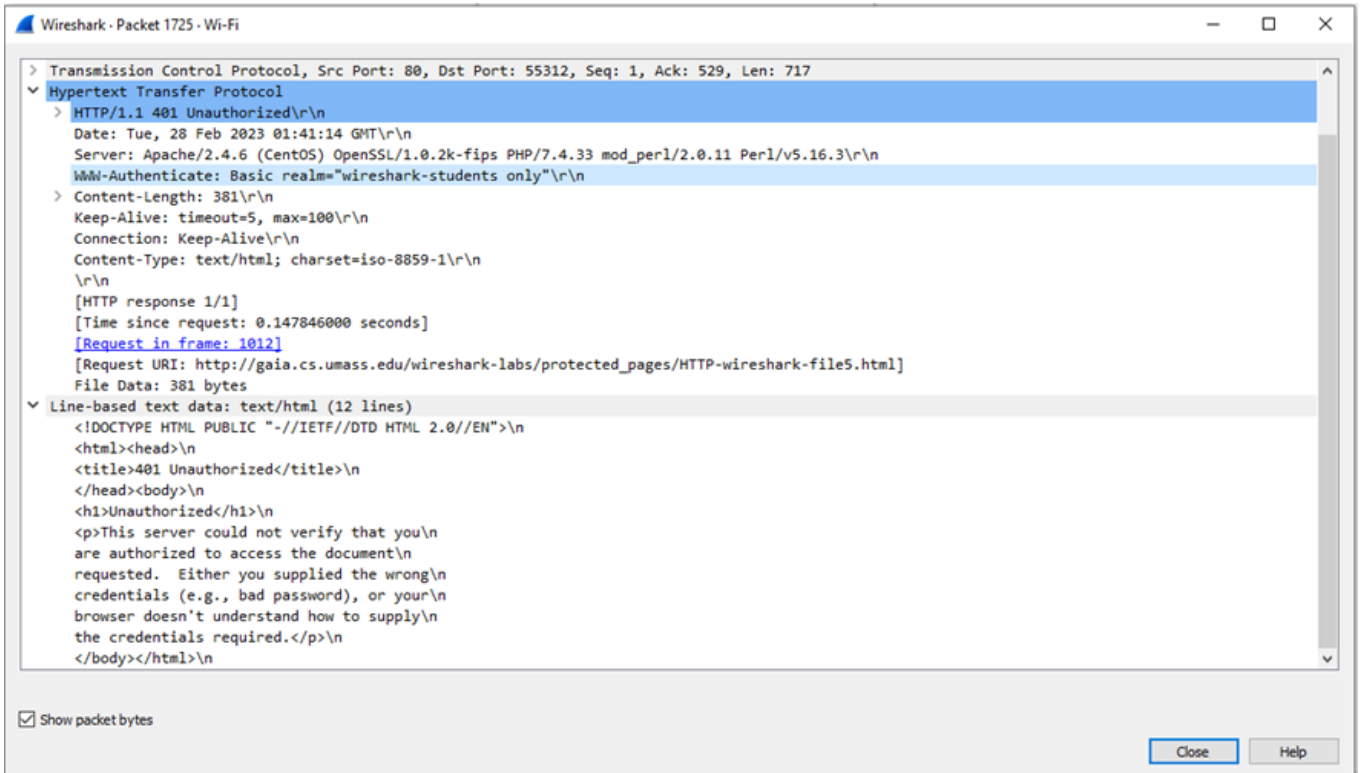
A opção "Encoding" no cabeçalho HTTP é usada para especificar a codificação usada para a transferência de dados entre o cliente e o servidor. A vantagem do "Encoding" nas requisições HTTP é que ele permite reduzir o tamanho da resposta, economizando largura de banda e melhorando o desempenho da rede.

Questão 9 (1,0). Avalie a requisição HTTP presente na figura 1 e a resposta do servidor web a essa requisição presente na captura disponível da figura 2.



No.	Time	Source	Destination	Protocol	Length	Info
1012	10.464675	192.168.1.9	128.119.245.12	HTTP	582	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1725	10.612521	128.119.245.12	192.168.1.9	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
9737	34.246014	192.168.1.9	128.119.245.12	HTTP	667	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
9741	34.415289	128.119.245.12	192.168.1.9	HTTP	544	HTTP/1.1 200 OK (text/html)

Figura 1. Captura de tela do Wireshark de uma requisição HTTP



Wireshark - Packet 1725 - Wi-Fi	
Transmission Control Protocol, Src Port: 80, Dst Port: 55312, Seq: 1, Ack: 529, Len: 717	
Hypertext Transfer Protocol	
HTTP/1.1 401 Unauthorized\r\n	
Date: Tue, 28 Feb 2023 01:41:14 GMT\r\n	
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n	
WWW-Authenticate: Basic realm="wireshark-students only"\r\n	
Content-Length: 381\r\n	
Keep-Alive: timeout=5, max=100\r\n	
Connection: Keep-Alive\r\n	
Content-Type: text/html; charset=iso-8859-1\r\n	
\r\n	
[HTTP response 1/1]	
[Time since request: 0.147846000 seconds]	
[Request in frame: 1012]	
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]	
File Data: 381 bytes	
Line-based text data: text/html (12 lines)	
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n	
<html><head>\n	
<title>401 Unauthorized</title>\n	
</head><body>\n	
<h1>Unauthorized</h1>\n	
<p>This server could not verify that you\n	
are authorized to access the document\n	
requested. Either you supplied the wrong\n	
credentials (e.g., bad password), or your\n	
browser doesn't understand how to supply\n	
the credentials required.</p>\n	
</body></html>\n	

Figura 2. Cabeçalho de Resposta do servidor a uma solicitação HTTP.

Com base nas informações presentes nas figuras 1 e 2, descreva o que ocorreu na solicitação.

Na figura 1 podemos ver que uma solicitação HTTP foi respondida com sucesso, com código 200. Já outra não foi autorizada pelo servidor, devolvendo 401 não autorizado.

Já na figura 2 podemos ver mais detalhes da requisição não autorizada. Mostrando que faltam credenciais ou algo do tipo para autorizar o acesso.

Questão 10 (1,0). Considerando que a solicitação HTTP foi realizada em uma rede que usa o recurso de webcache responda:

a) *Quais parâmetros encontrados nos pacotes seriam diferentes? Justifique sua resposta com base nos tópicos estudados na aula de teoria.*

Quando um servidor intermediário (webcache) é usado para armazenar em cache uma página da web, o cabeçalho da solicitação HTTP pode ser modificado com o parâmetro "Cache-Control".

b) *Quais as vantagens do uso de Webcache?*

Webcache é uma tecnologia que armazena cópias de páginas da web em um servidor intermediário entre o cliente e o servidor de origem, melhorando a velocidade e eficiência da rede. Quando uma solicitação HTTP é feita ao servidor intermediário, o cabeçalho da solicitação pode ser modificado para indicar ao cache como lidar com a solicitação.