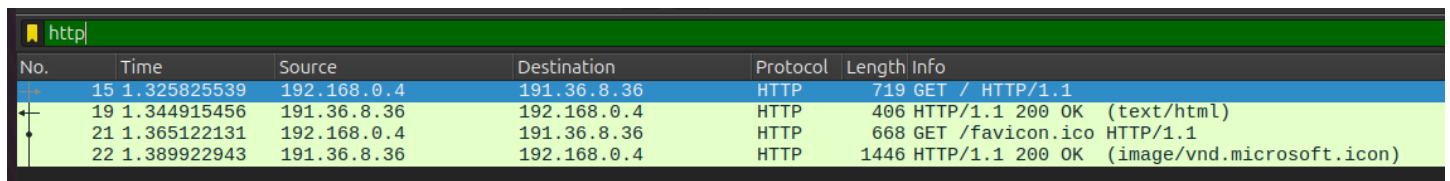


Desvendando o HTTP com Wireshark

A Interação Básica GET/Resposta do HTTP

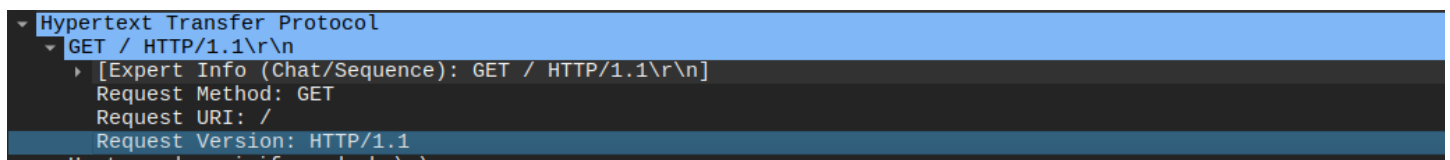
Responda às seguintes perguntas e imprima as mensagens GET e a resposta e indique em que parte da mensagem você encontrou a informação que responde às questões.



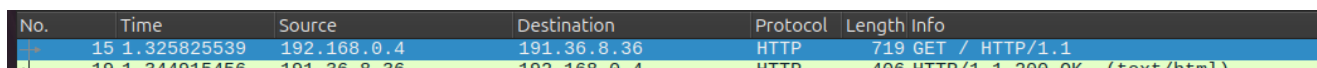
No.	Time	Source	Destination	Protocol	Length	Info
15	1.325825539	192.168.0.4	191.36.8.36	HTTP	719	GET / HTTP/1.1
19	1.344915456	191.36.8.36	192.168.0.4	HTTP	406	HTTP/1.1 200 OK (text/html)
21	1.365122131	192.168.0.4	191.36.8.36	HTTP	668	GET /favicon.ico HTTP/1.1
22	1.389922943	191.36.8.36	192.168.0.4	HTTP	1446	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

1. O seu navegador executa HTTP 1.0 ou 1.1?

O navegador executa **HTTP 1.1**. Informação é obtida na linha “Request Version” ao abrir a janela de detalhamento da mensagem GET ou na própria listagem no pacote, nesse caso é o número 15.



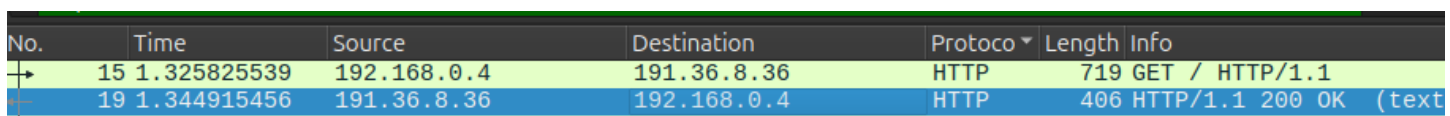
Hypertext Transfer Protocol	
GET / HTTP/1.1\r\n	
[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]	
Request Method: GET	
Request URI: /	
Request Version: HTTP/1.1	



No.	Time	Source	Destination	Protocol	Length	Info
15	1.325825539	192.168.0.4	191.36.8.36	HTTP	719	GET / HTTP/1.1
19	1.344915456	191.36.8.36	192.168.0.4	HTTP	406	HTTP/1.1 200 OK (text/html)
21	1.365122131	192.168.0.4	191.36.8.36	HTTP	668	GET /favicon.ico HTTP/1.1
22	1.389922943	191.36.8.36	192.168.0.4	HTTP	1446	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

2. Qual a versão de HTTP do servidor?

A versão é **HTTP/1.1**. Informação obtida na própria listagem do pacote.



No.	Time	Source	Destination	Protocol	Length	Info
15	1.325825539	192.168.0.4	191.36.8.36	HTTP	719	GET / HTTP/1.1
19	1.344915456	191.36.8.36	192.168.0.4	HTTP	406	HTTP/1.1 200 OK (text/html)
21	1.365122131	192.168.0.4	191.36.8.36	HTTP	668	GET /favicon.ico HTTP/1.1
22	1.389922943	191.36.8.36	192.168.0.4	HTTP	1446	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

3. Quais idiomas (se algum) o seu navegador indica ao servidor que pode aceitar?

Idiomas são o “**en-us**” e “**en**”, duas versões de inglês.

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,pt;q=0.8\r\n
Cookie: _gac_UA-29966545-1=1.1726617027.CjwKCAjw0aS3BhA3EiwAKaD2ZaVsJN75dNPqMg0hAkSBbcal1tN
\r\n
```

4. Qual o endereço IP do seu computador?

O endereço IP do seu computador é **192.168.0.4**. Informação da própria listagem de pacotes.

Source
192.168.0.4
191.36.8.36

5. E do servidor redes.sj.ifsc.edu.br?

O endereço IP do servidor **redes.sj.ifsc.edu.br** é **191.36.8.36**. Informação da própria listagem de pacotes.

Destination
191.36.8.36
192.168.0.4

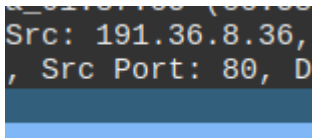
6. Qual o número da porta utilizada no seu computador?

O número da porta utilizada pelo meu computador é **50620**. Informação obtida na visto no campo Src Port (Source Port) na janela de detalhamento de pacote da mensagem GET.

```
c: 192.168.0.4, D
Src Port: 50620,
```

7. E do servidor redes.sj.ifsc.edu.br?

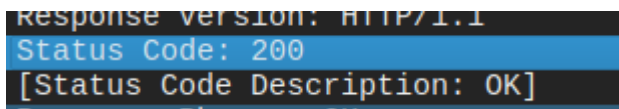
O número da porta utilizada pelo servidor é **80**. Informação obtida no campo Src Port na janela de detalhamento de pacote de resposta.



```
Src: 191.36.8.36,  
, Src Port: 80, D
```

8. Qual o código de status retornado do servidor para o seu navegador?

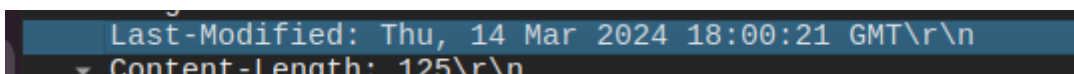
O código de status retornado pelo servidor é **200**. Informação obtida no campo Status Code que está na janela de detalhamento de pacote de resposta.



```
Response version: HTTP/1.1  
Status Code: 200  
[Status Code Description: OK]
```

9. Quando o arquivo em HTML que você baixou foi modificado no servidor pela última vez?

14 de Maio de 2024. A informação estava na janela de detalhamento do pacote.



```
Last-Modified: Thu, 14 Mar 2024 18:00:21 GMT\r\n  
Content-Length: 125\r\n
```

10. Quantos bytes de conteúdo são baixados pelo seu navegador?

Existem dois pacotes de resposta HTTP com código “200 OK”: O primeiro pacote de resposta (número 19) tem 406 bytes e o segundo pacote de resposta (número 22) tem 1446 bytes.

A soma deles é o total de bytes de conteúdo baixado, o que dá o valor de **1852 bytes**.

No.	Time	Source	Destination	Protocol	Length Info
15	1.325825539	192.168.0.4	191.36.8.36	HTTP	719 GET / HTTP/1.1
19	1.344915456	191.36.8.36	192.168.0.4	HTTP	406 HTTP/1.1 200 OK (text/html)
21	1.365122131	192.168.0.4	191.36.8.36	HTTP	668 GET /favicon.ico HTTP/1.1
22	1.389922943	191.36.8.36	192.168.0.4	HTTP	1446 HTTP/1.1 200 OK (image/vnd.microsoft.icon)

11. Encontre a mensagem “Redes de Computadores IFSC - SJ - Telecomunicacoes! - Pagina de teste”. Onde (em qual campo) encontra-se?

A mensagem está listada na captura de tela abaixo. A informação foi obtida novamente no detalhamento de pacotes.

```
Line-based text data: text/html (3 lines)
<html><body><h1>Redes de Computadores IFSC - SJ - Telecomunicacoes!</h1>\n
<h2>Pagina de teste principal.</h2>\n
</body></html>\n
```

12. Qual a diferença entre os endereços IP e porta de origem e destino entre a mensagem GET e a de resposta do HTTP?

Os IPs e portas são invertidos, pois um deles é o cliente enviando solicitações e outro é o servidor respondendo.

Na mensagem GET:

- IP de origem: **192.168.0.4**
- IP de destino: **191.36.8.36**
- Porta de origem: **50620**
- Porta de destino: **80**

Na resposta HTTP:

- IP de origem: **191.36.8.36**
- IP de destino: **192.168.0.4**
- Porta de origem: **80**
- Porta de destino: **50620**

Interação Básica GET/Resposta do HTTP usando TELNET e Requisição Manual

1. Identifique a página html que foi enviada como resposta. Respeita o protocolo HTTP (observe o cabeçalho)?

Sim, pois obtemos o status “*HTTP/1.0 200 OK*” após a requisição.

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ telnet -4 redes.sj.ifsc.edu.br 80
Trying 191.36.8.36...
Connected to redes.sj.ifsc.edu.br.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.0 200 OK
Content-Type: text/html
ETag: "2422842869"
Last-Modified: Thu, 14 Mar 2024 18:00:21 GMT
Content-Length: 125
Connection: close
Date: Sat, 28 Sep 2024 18:21:59 GMT
Server: lighttpd/1.4.59

<html><body><h1>Redes de Computadores IFSC - SJ - Telecomunicacoes!</h1>
<h2>Pagina de teste principal.</h2>
</body></html>
Connection closed by foreign host.
lulu@lulu-ZenBook-UX435EA-UX435EA:~$
```

2. No Wireshark compare o resultado das execuções desses comandos com o que se viu nas capturas Wireshark com acesso pelo navegador, em resumo, compare a troca de mensagens via navegador e terminal (cabeçalhos). Qual a diferença em cada caso?

No terminal, a requisição é compacta, com menos cabeçalhos, enquanto no navegador há muitos cabeçalhos adicionais.

3. Quanto tempo levou para fechar a conexão (após o duplo Enter)?

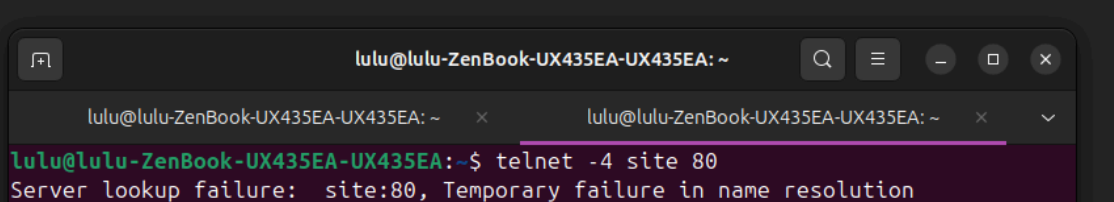
Foi aproximadamente **0.0145 segundos**. A informação foi obtida o tempo entre o último pacote enviado pelo servidor e a mensagem de fechamento de conexão.

Time	Source	Destination	Protocol	Length	Info
2 28.613853756	2620:2d:4000:1::23	2804:14d:bad5:8f15:...	HTTP	174	GET / HTTP/1.1
4 28.628339656	2620:2d:4000:1::23	2804:14d:bad5:8f15:...	HTTP	275	HTTP/1.1 204 No Content

4. Refaça um pedido em que o recurso é inexistente no servidor (ex: página html com nome/URL inexistente). Observe a resposta. Qual é o código da mensagem recebida?

O código foi 204, o que significa que a requisição ocorreu corretamente, porém o servidor não tem conteúdo para retornar.

No.	Time	Source	Destination	Protocol	Length	Info
147	22.401728826	2804:14d:bad5:8f15:...	2620:2d:4000:1::23	HTTP	174	GET / HTTP/1.1
149	22.673197256	2620:2d:4000:1::23	2804:14d:bad5:8f15:...	HTTP	275	HTTP/1.1 204 No Content
158	23.016551592	192.168.0.4	185.125.190.17	HTTP	154	GET / HTTP/1.1
159	23.321174822	185.125.190.17	192.168.0.4	HTTP	255	HTTP/1.1 204 No Content



```
lulu@lulu-ZenBook-UX435EA-UX435EA: ~  
lulu@lulu-ZenBook-UX435EA-UX435EA: ~  
lulu@lulu-ZenBook-UX435EA-UX435EA: ~  
lulu@lulu-ZenBook-UX435EA-UX435EA: ~$ telnet -4 site 80  
Server lookup failure: site:80, Temporary failure in name resolution
```

5. Refaça o pedido, mas agora utilizando o HTTP/1.1, e tente inferir a diferença da versão 1.0. Note que o GET nesta versão deve ser realizado com o campo Host. Quanto tempo levou para fechar a conexão (após o duplo Enter)?

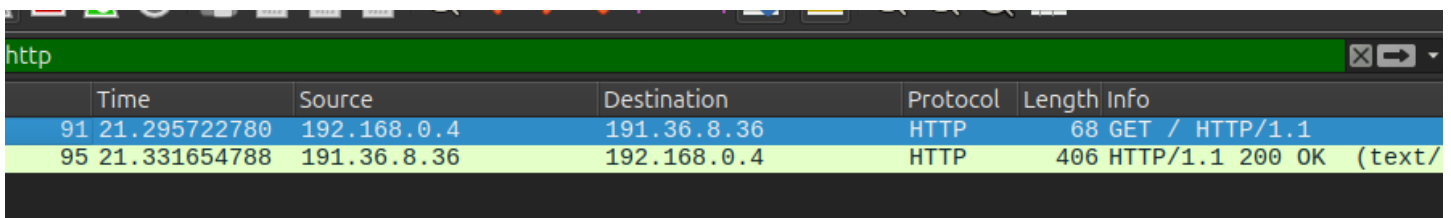
```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ telnet -4 redes.sj.ifsc.edu.br 80
Trying 191.36.8.36...
Connected to redes.sj.ifsc.edu.br.
Escape character is '^]'.
GET / HTTP/1.1
HOST: redes.sj.ifsc.edu.br

HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "2422842869"
Last-Modified: Thu, 14 Mar 2024 18:00:21 GMT
Content-Length: 125
Date: Sat, 28 Sep 2024 18:33:24 GMT
Server: lighttpd/1.4.59

<html><body><h1>Redes de Computadores IFSC - SJ - Telecomunicacoes!</h1>
<h2>Pagina de teste principal.</h2>
</body></html>
Connection closed by foreign host.
```

6. Quanto tempo levou para fechar a conexão (após o duplo Enter)?

Foi aproximadamente **0.0360 segundos**.



The image shows a Wireshark packet capture window with the filter 'http'. The packet list shows two packets: a GET request (packet 91) and a 200 OK response (packet 95). The details pane for packet 95 is expanded, showing the response structure.

	Time	Source	Destination	Protocol	Length	Info
91	21.295722780	192.168.0.4	191.36.8.36	HTTP	68	GET / HTTP/1.1
95	21.331654788	191.36.8.36	192.168.0.4	HTTP	406	HTTP/1.1 200 OK (text/

7. Refaça a conexão com o servidor. Refaça o pedido, mas agora utilizando o HTTP/1.1. Seja rápido. Antes do fechamento da conexão, faça um novo pedido na conexão já aberta:

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ telnet -4 redes.sj.ifsc.edu.br 80
Trying 191.36.8.36...
Connected to redes.sj.ifsc.edu.br.
Escape character is '^]'.
GET / HTTP/1.1
HOST: redes.sj.ifsc.edu.br

HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "2422842869"
Last-Modified: Thu, 14 Mar 2024 18:00:21 GMT
Content-Length: 125
Date: Sat, 28 Sep 2024 18:35:28 GMT
Server: lighttpd/1.4.59

<html><body><h1>Redes de Computadores IFSC - SJ - Telecomunicacoes!</h1>
<h2>Pagina de teste principal.</h2>
</body></html>
GET /Redes_arq1.html HTTP/1.1
Host: redes.sj.ifsc.edu.br

HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "4279571012"
Last-Modified: Thu, 23 Feb 2023 12:22:56 GMT
Content-Length: 126
Date: Sat, 28 Sep 2024 18:35:37 GMT
Server: lighttpd/1.4.59

<html><body><h1>Redes de Computadores IFSC - SJ - Telecomunicacoes!</h1>
<h2>Arquivo 1 pagina de teste.</h2>
</body></html>
Connection closed by foreign host.
```

8. O que explica a diferença de tempo para fechamento de conexão entre as versões HTTP 1.0 e 1.1?

A diferença está no suporte a conexões persistentes. No HTTP 1.0, cada solicitação cria uma nova conexão TCP, que é fechada logo após a resposta do servidor. Já no HTTP 1.1, as conexões são persistentes permitindo múltiplas solicitações em uma mesma conexão.

9. Descreva qual seria o procedimento para o download de dois objetos, via telnet, nos protocolos HTTP 1.0 e 1.1?

Para o protocolo HTTP 1.0, primeiro estabelecer a conexão, enviar a requisição para o primeiro objeto, receber o objeto e encerrar a conexão. Depois, restabelecer a conexão e repetir os passos para outro objeto.

Para o protocolo HTTP 1.1, primeiro estabelecer a conexão, enviar a requisição para o primeiro objeto e receber este objeto. A conexão é mantida, então basta receber o outro objeto, receber o segundo objeto e encerrar a conexão.

Referências:

Author(s): Brad **Title:** "HTTP 1.0 vs 1.1" **Website:** Stack Overflow **URL:** <https://stackoverflow.com/questions/246859/http-1-0-vs-1-1> **Accessed Date:** 28 Sep. 2024