

PRÁTICA 3

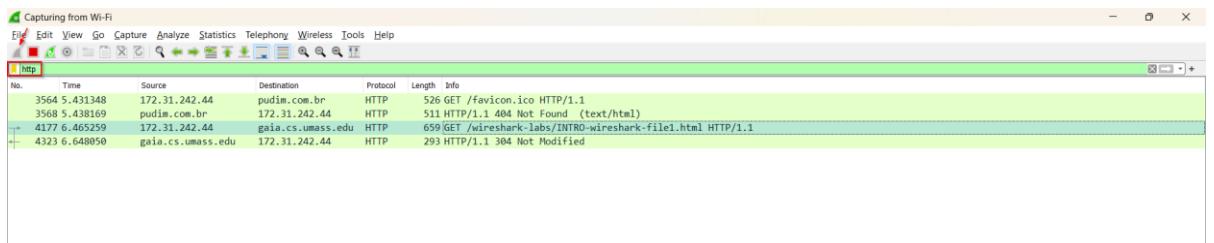
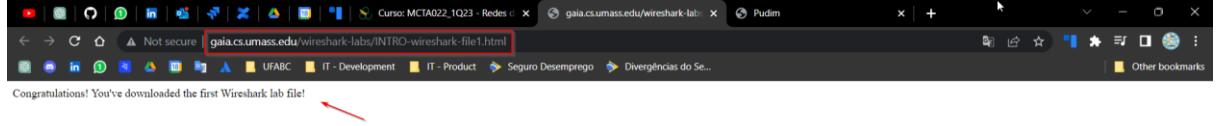
Nome: Igor Carvalho de Oliveira

RA: 11201920763

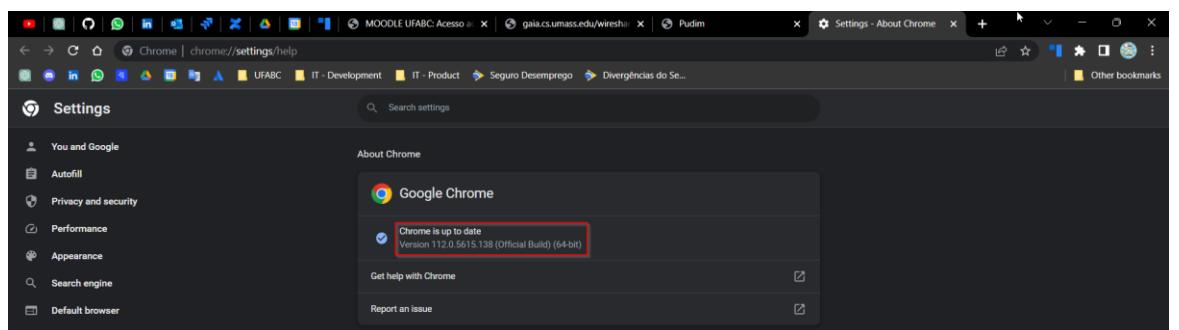
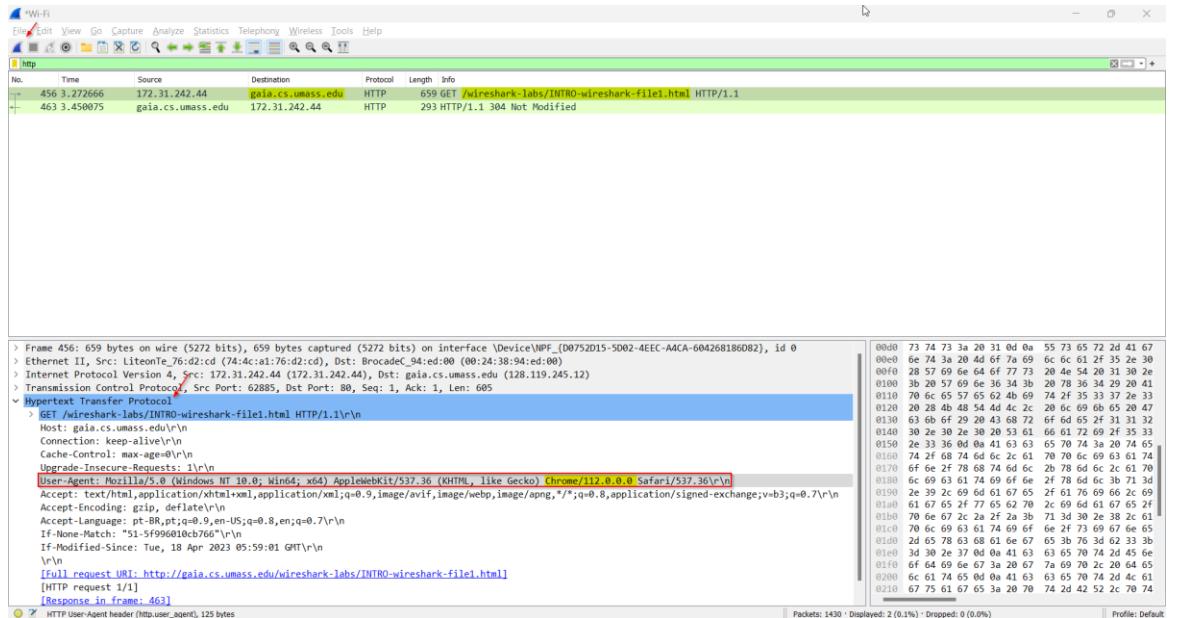
1. Interações básica HTTP.

O Wireshark permite entender os dados que estão sendo enviados em cada interface de rede. Na camada de rede de transporte (Hypertext Transfer Protocol) se encontram todas as informações da página. Para acessar essas informações, basta abrir a camada de rede e verificar os dados.

- Acesse a página mencionada e aplique o filtro HTTP para visualizar os pacotes do protocolo HTTP.



- Consulte a versão do HTTP do navegador/servidor web acessado.



○ Consulte as linguagens aceitas pelo Browser.

Capturing from Wi-Fi

No.	Time	Source	Destination	Protocol	Length	Info
817 8.198989	172.31.242.44	gaia.cs.umass.edu	HTTP	659	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	
837 8.376210	gaia.cs.umass.edu	172.31.242.44	HTTP	293	HTTP/1.1 304 Not Modified	

```
> Frame 817: 659 bytes on wire (5272 bits), 659 bytes captured (5272 bits) on interface \Device\NPF_{D0752015-5D02-4EBC-A4CA-604268186D82}, id 0
> Ethernet II, Src: LiteonTe_76:d2:cd (74:4c:a1:76:d2:cd), Dst: BrocadeC_94:ed:00 (00:24:38:94:ed:00)
> Internet Protocol Version 4, Src: 172.31.242.44 (172.31.242.44), Dst: gaia.cs.umass.edu (128.119.245.12)
> Transmission Control Protocol, Src Port: 63222, Dst Port: 80, Seq: 1, Ack: 1, Len: 605
  Hypertext Transfer Protocol
    > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      Cache-Control: max-age=0\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: pt-BR,pt;q=0.9,en;q=0.8,en;q=0.7\r\n
      If-None-Match: "51-5f996010cb76"\r\n
      If-Modified-Since: Tue, 18 Apr 2023 05:59:01 GMT\r\n
      \r\n
      [Full request URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
      [HTTP request 1/1]
```

HTTP User-Agent header (http.user_agent), 125 bytes

Packets: 1256 · Displayed: 2 (0.2%) · Profile: Default

○ Consulte os idiomas disponíveis pelo Browser.

Capturing from Wi-Fi

No.	Time	Source	Destination	Protocol	Length	Info
817 8.198989	172.31.242.44	gaia.cs.umass.edu	HTTP	659	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	
837 8.376210	gaia.cs.umass.edu	172.31.242.44	HTTP	293	HTTP/1.1 304 Not Modified	

```
> Frame 817: 659 bytes on wire (5272 bits), 659 bytes captured (5272 bits) on interface \Device\NPF_{D0752015-5D02-4EBC-A4CA-604268186D82}, id 0
> Ethernet II, Src: LiteonTe_76:d2:cd (74:4c:a1:76:d2:cd), Dst: BrocadeC_94:ed:00 (00:24:38:94:ed:00)
> Internet Protocol Version 4, Src: 172.31.242.44 (172.31.242.44), Dst: gaia.cs.umass.edu (128.119.245.12)
> Transmission Control Protocol, Src Port: 63222, Dst Port: 80, Seq: 1, Ack: 1, Len: 605
  Hypertext Transfer Protocol
    > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      Cache-Control: max-age=0\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: pt-BR,pt;q=0.9,en;q=0.8,en;q=0.7\r\n
      If-None-Match: "51-5f996010cb76"\r\n
      If-Modified-Since: Tue, 18 Apr 2023 05:59:01 GMT\r\n
      \r\n
      [Full request URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
      [HTTP request 1/1]
```

[Response in frame: 837]

HTTP User-Agent header (http.user_agent), 125 bytes

Packets: 1997 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%) · Profile: Default

○ Consulte as informações de IP do seu PC e do Servidor.

Capturing from Wi-Fi

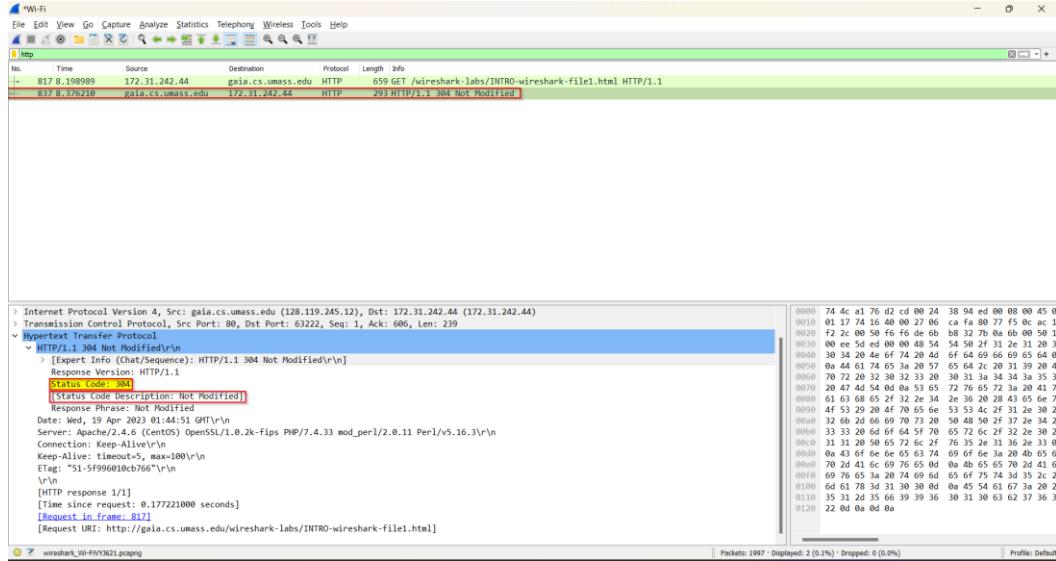
No.	Time	Source	Destination	Protocol	Length	Info
817 8.198989	172.31.242.44	gaia.cs.umass.edu	HTTP	659	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	
837 8.376210	gaia.cs.umass.edu	172.31.242.44	HTTP	293	HTTP/1.1 304 Not Modified	

```
> Frame 817: 659 bytes on wire (5272 bits), 659 bytes captured (5272 bits) on interface \Device\NPF_{D0752015-5D02-4EBC-A4CA-604268186D82}, id 0
> Ethernet II, Src: LiteonTe_76:d2:cd (74:4c:a1:76:d2:cd), Dst: BrocadeC_94:ed:00 (00:24:38:94:ed:00)
> Internet Protocol Version 4, Src: 172.31.242.44 (172.31.242.44), Dst: gaia.cs.umass.edu (128.119.245.12)
> Transmission Control Protocol, Src Port: 63222, Dst Port: 80, Seq: 1, Ack: 1, Len: 605
  Hypertext Transfer Protocol
    > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
      [GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/INTRO-wireshark-file1.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      Cache-Control: max-age=0\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
      Accept-Encoding: gzip, deflate\r\n
      \r\n
      [Full request URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
      [HTTP request 1/1]
```

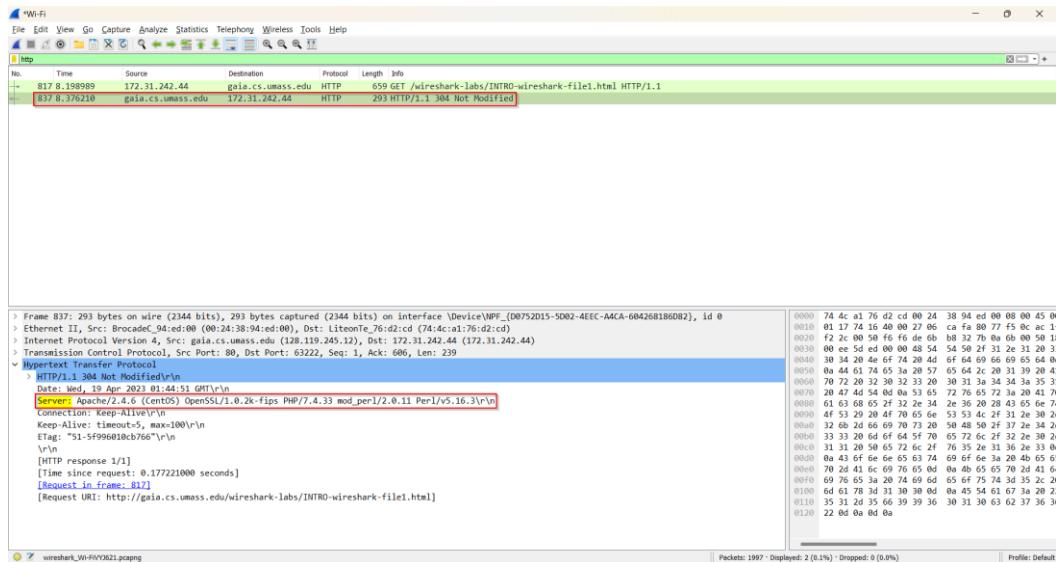
HTTP Connection (http.connection), 24 bytes

Packets: 1997 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%) · Profile: Default

- Consulte o código de status retornado do Servidor para o Navegador.

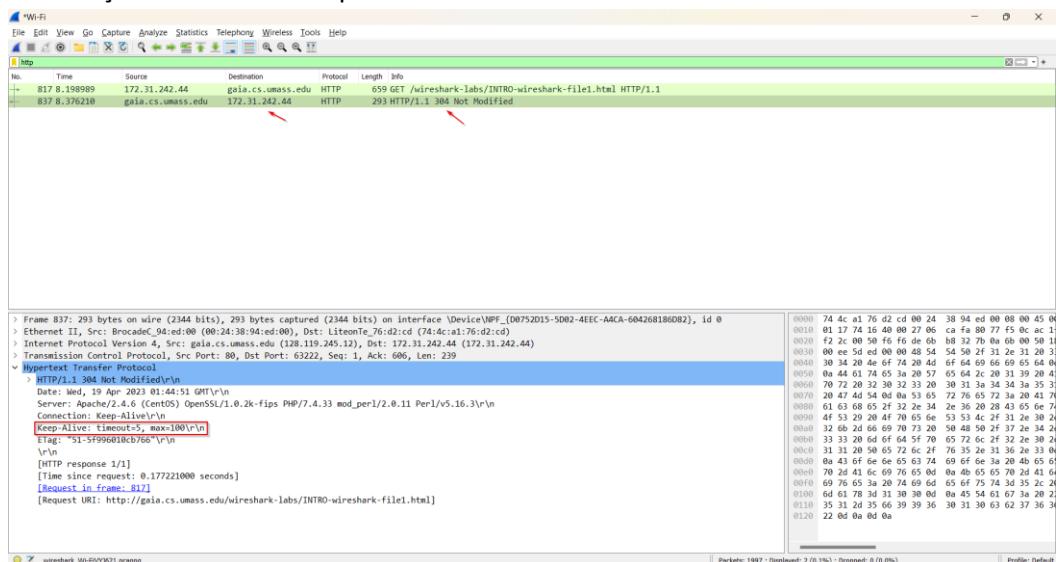


- Consulte as informações do Servidor.



- Consulte o tipo de HTTP. Se é persistente ou não-persistente.

Obs: Note que temos um informações de Keep-Alive. Desta forma, podemos traduzir essa informação como um HTTP persistente.



- Consulte a última modificação do arquivo HTML.

```

No. Time Source Destination Protocol Length Info
1 10774.765518 192.168.15.10 gaia.cs.umass.edu HTTP 659 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2 11094.913728 gaia.cs.umass.edu 192.168.15.10 HTTP 492 HTTP/1.1 200 OK (text/html)
3 11295.807737 gaia.cs.umass.edu 192.168.15.10 HTTP 494 GET /favicon.ico HTTP/1.1
4 11595.5157087 gaia.cs.umass.edu 192.168.15.10 HTTP 538 HTTP/1.1 404 Not Found (text/html)

Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Date: Wed, 19 Apr 2023 14:26:24 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
Last-Modified: Wed, 19 Apr 2023 05:59:01 GMT\r\n
ETag: "51-5f9aa1ee1f57a"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.148202000 seconds]
[Request in frame: 1077]
[Next request in frame: 1129]
[Next response in frame: 1159]
[Request URI: http://gaia.cs.umass.edu/favicon.ico]
File Data: 81 bytes
> Line-based text data: text/html (3 lines)
    
```

- Consulte o número dos bytes de conteúdo retornado ao Navegador.

```

No. Time Source Destination Protocol Length Info
1 10774.765518 192.168.15.10 gaia.cs.umass.edu HTTP 659 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2 11094.913728 gaia.cs.umass.edu 192.168.15.10 HTTP 492 HTTP/1.1 200 OK (text/html)
3 11295.807737 gaia.cs.umass.edu 192.168.15.10 HTTP 494 GET /favicon.ico HTTP/1.1
4 11595.5157087 gaia.cs.umass.edu 192.168.15.10 HTTP 538 HTTP/1.1 404 Not Found (text/html)

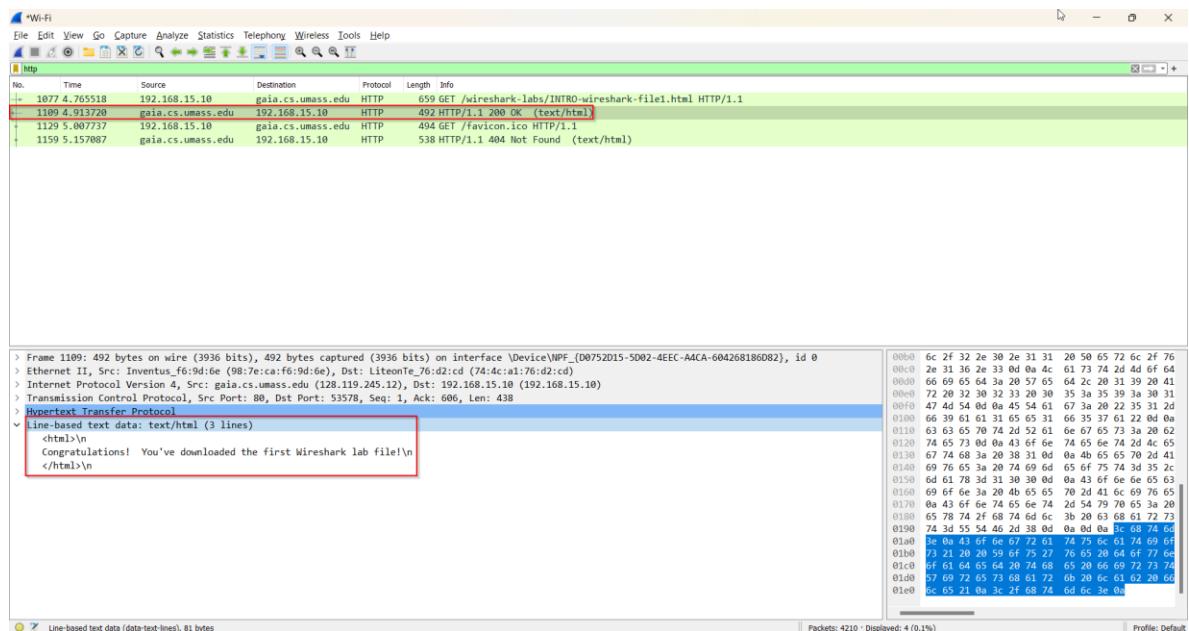
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Date: Wed, 19 Apr 2023 14:26:24 GMT\r\n
Server: Apache/2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3)\r\n
Last-Modified: Wed, 19 Apr 2023 05:59:01 GMT\r\n
ETag: "51-5f9aa1ee1f57a"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.148202000 seconds]
[Request in frame: 1077]
[Next request in frame: 1129]
[Next response in frame: 1159]
[Request URI: http://gaia.cs.umass.edu/favicon.ico]
File Data: 81 bytes
> Line-based text data: text/html (3 lines)
    
```

- Analise os dados (*raw data*) do pacote e descreva o que é possível observar.

R: É possível observar todo o conteúdo presente na página web capturada ao analisar os dados retornados pelo servidor. Conseguimos, inclusive, visualizar o código fonte da página.

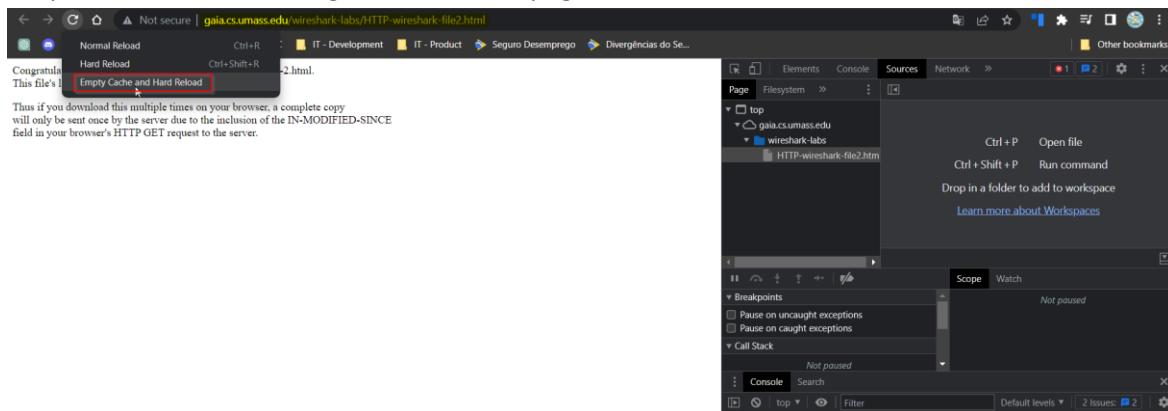
```

Line wrap
1 <html>
2 Congratulations! You've downloaded the first Wireshark lab file!
3 </html>
    
```



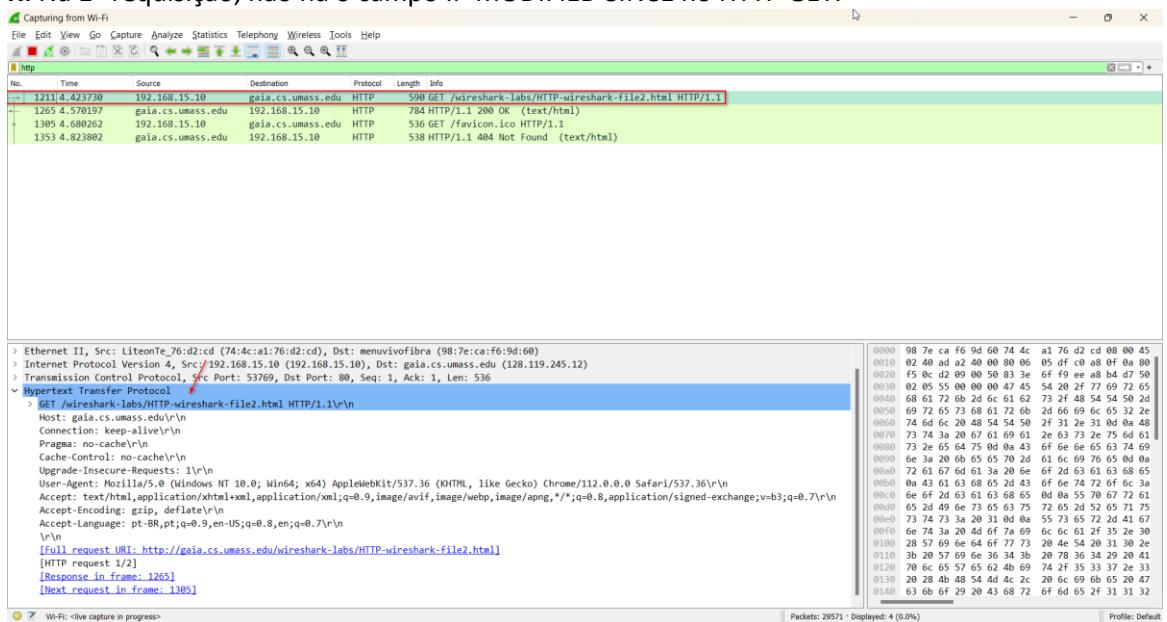
2. GET Condisional.

- a. Limpe o cache do seu navegador e acesse a página.



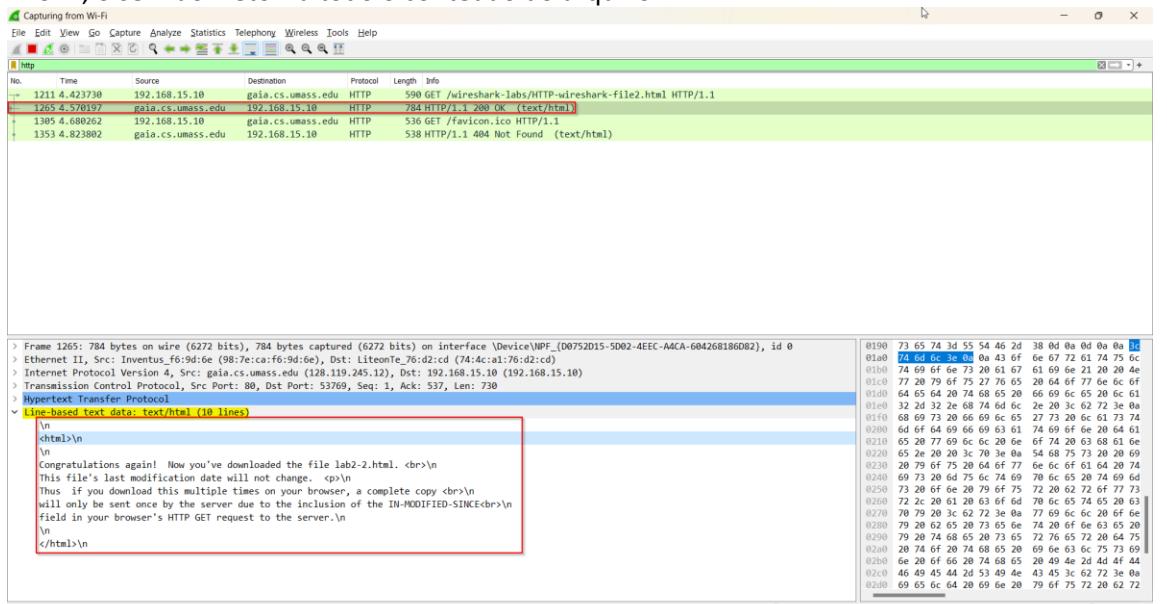
- b. Verifique o conteúdo da 1ª requisição GET. É possível ver IF-MODIFIED-SINCE no HTTP GET?

R: Na 1ª requisição, não há o campo IF-MODIFIED SINCE no HTTP GET.



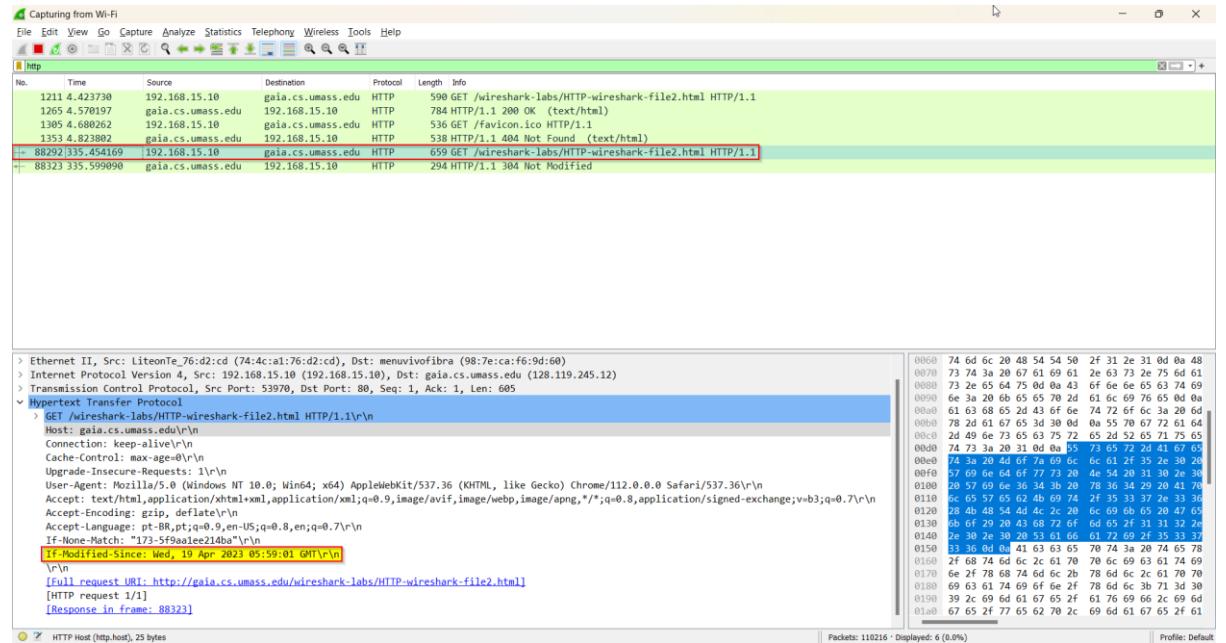
- c. Verifique a resposta do servidor. O servidor retorna o conteúdo do arquivo?

R: Sim, o servidor retorna todo o conteúdo do arquivo.



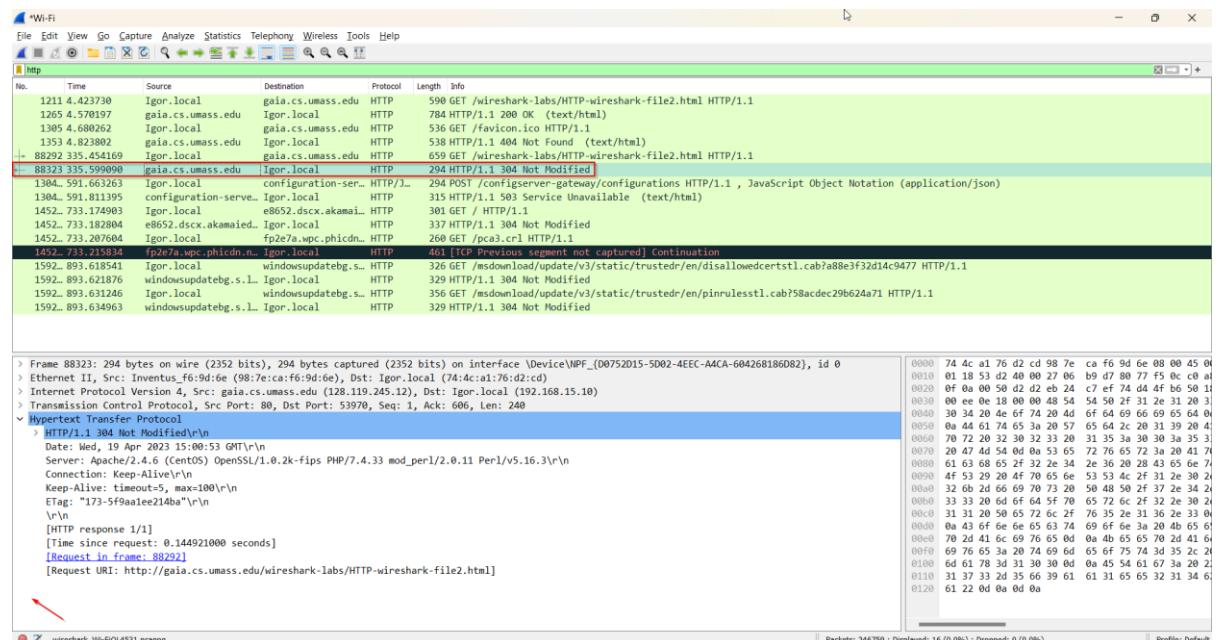
- d. Faça uma 2ª requisição GET e verifique se é possível ver IF-MODIFIED-SINCE no HTTP GET? Explique.

R: É possível ver o campo IF-MODIFIED-SINCE na 2ª requisição porque trata-se do envio de informações repetidas. Esse campo, informa a data da última modificação, para que não seja necessário disponibilizar um payload repetido sempre que houver um envio. Se o arquivo já existe no servidor, ele fica salvo em cache. Se houver um reenvio com modificações, o servidor retorna esse novo payload alterado e grava a data a altaração no campo IF-MODIFIED-SINCE.



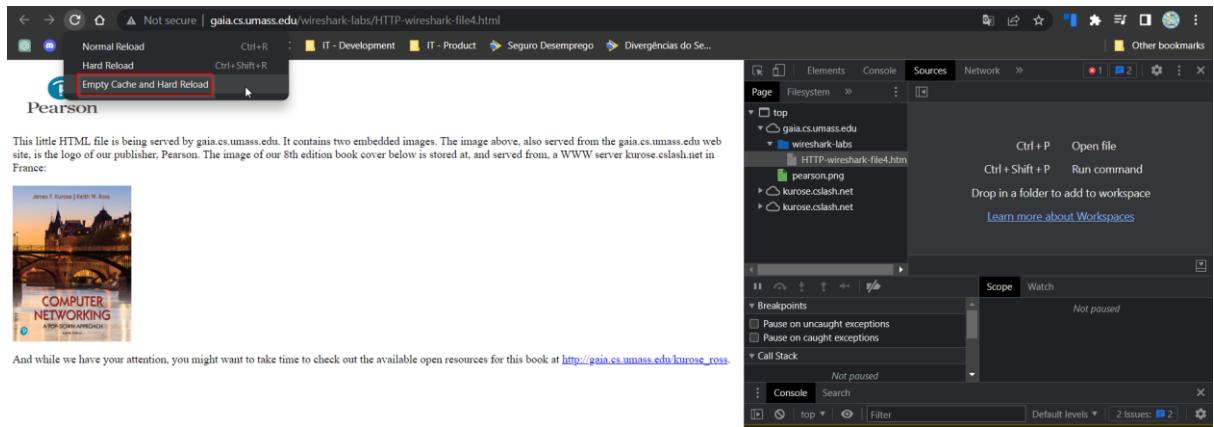
- e. Verifique a resposta do servidor. O servidor retorna o conteúdo do arquivo? Explique.

R: O servidor não retorna o conteúdo na 2ª requisição porque o computador já possui esse arquivo salvo em cache devido o envio da 1ª requisição. Uma vez que o arquivo não sofreu modificações, o servidor evita disponibilizar informações redundantes. Nesse contexto, o campo IF-MODIFIED SINCE informa a última vez que o arquivo foi modificado para que seja possível visualizar o conteúdo nessa data de envio.



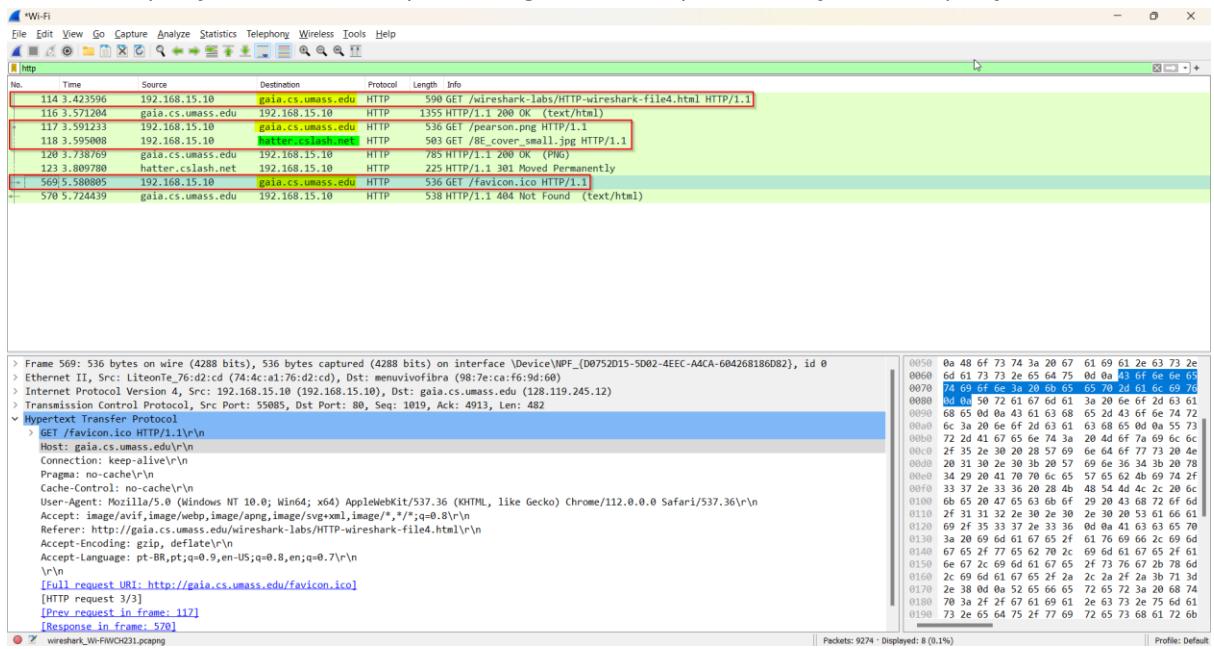
3. HTML com objetos.

- a. Acesse a página mencionada.



This screenshot shows a web browser window with the URL gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html. The page displays the Pearson logo and a small thumbnail of the book 'Computer Networking: A Top-Down Approach'. Below the thumbnail, there is a link to the book's page on the gaia.cs.umass.edu website. The browser's developer tools are open, showing the 'Sources' tab with a tree view of the page's resources, including the main HTML file and several CSS and JavaScript files. The 'Console' tab is also visible at the bottom.

- b. Quantas requisições foram feitas pelo navegador? Para qual endereço IP as requisições foram feitas?



This screenshot of Wireshark shows the network traffic for the URL <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>. The packet list pane shows four distinct HTTP requests:

- Request 114: GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 from 192.168.15.10 to gaia.cs.umass.edu (192.168.15.10) [HTTP 200 OK]
- Request 115: GET /pearson.png HTTP/1.1 from 192.168.15.10 to gaia.cs.umass.edu (192.168.15.10) [HTTP 200 OK]
- Request 116: GET /BE_cover_small1.jpg HTTP/1.1 from 192.168.15.10 to hatter.cslash.net (192.168.15.10) [HTTP 200 OK]
- Request 117: GET /favicon.ico HTTP/1.1 from 192.168.15.10 to gaia.cs.umass.edu (192.168.15.10) [HTTP 200 OK]

The packet details and bytes panes show the raw HTTP requests and their responses. The selected packet is the fourth one (Request 117). The packet bytes pane shows the raw binary data of the favicon request.

R: Foram feitas 4 requisições. 3 delas para mesmo destino (**gaia.cs. umas.edu**) e 1 requisição para o destino (**hatter.cslash.net**). Das 4 requisições realizadas, apenas 1 requisição foi feita para o HTML acessado enquanto as outras 3 são hyperlinks para o carregamento das imagens e ícones da página.

Foram feitas requisições para os seguintes endereços IP's:

128.119.245.12 (*gaia.cs. umas.edu*)
178.79.137.164 (*hatter.cslash.net*)

c. Identifique se o navegador fez o download dos objetos de maneira serial ou paralela. Explique.

R: O navegador fez o download dos objetos de forma sequencial para envios feitos ao mesmo IP, pois foi utilizado o mesmo socket para guardar as informações baixadas do servidor. Para essa conclusão, foi consultado cada uma das requisições feitas ao servidor e observamos as portas de origem em que o arquivo foi baixado. No meu caso, as portas de origem foram iguais para as requisições feitas ao mesmo endereço de IP.

No.	Time	Source	Destination	Protocol	Length	Info
153.6.116981	192.168.15.10	gaia.cs.umass.edu	HTTP	590	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1	
160.6.265505	gaia.cs.umass.edu	192.168.15.10	HTTP	1355	HTTP/1.1 200 OK (text/html)	
161.6.280130	192.168.15.10	gaia.cs.umass.edu	HTTP	536	GET /pearson.png HTTP/1.1	
171.6.426111	gaia.cs.umass.edu	192.168.15.10	HTTP	785	HTTP/1.1 200 OK (PNG)	
207.6.800660	192.168.15.10	hatter.cslash.net	HTTP	503	GET /BE_cover_small.jpg HTTP/1.1	
216.7.014089	hatter.cslash.net	192.168.15.10	HTTP	225	HTTP/1.1 301 Moved Permanently	
696.9.020268	192.168.15.10	gaia.cs.umass.edu	HTTP	536	GET /favicon.ico HTTP/1.1	
714.9.169087	gaia.cs.umass.edu	192.168.15.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)	

> Frame 153: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{D0752015-5002-4ECC-A4CA-604268186082}, id 0
> Ethernet II, Src: LitenTe_76:d2:cd (74:4c:a1:76:d2:cd), Dst: menuvivofibra (98:7e:ca:f6:9d:60)
> Internet Protocol Version 4, Src: 192.168.15.10 (192.168.15.10), Dst: gaia.cs.umass.edu (128.119.245.12)
> Transmission Control Protocol, Src Port: 56641, Dst Port: 80, Seq: 1, Ack: 1, Len: 536
Source Port: 56641
Destination Port: 80
[Stream index: 5]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 536]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1912406608
Acknowledgment Number: 1 (relative ack number)
Acknowledgment Number (raw): 1912406608
Offset: 0x0100
Flags: 0x0108 (PSH, ACK)
Window: 512
[Calculated window size: 132352]
[Window size scaling factor: 256]
Checksum: 0x678a [unverified]

0020 f5 0c fd 41 00 50 0e 9f f6 07 71 fd 02 50 50
0030 02 05 67 8a 00 00 47 45 54 20 2f 77 69 72 65
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 50 2d
0050 69 72 65 73 2d 6b 72 6b 2d 66 69 6c 65 34 2e
0060 70 6c 65 73 4d 6b 72 6b 2d 66 69 6c 65 34 2e
0070 73 74 3a 67 61 69 61 2e 75 63 73 6d 61
0080 73 2d 65 64 75 0d 0a 43 6f 6e 65 63 74 69
0090 6e 3a 2b 6b 65 65 70 2d 61 6e 69 76 65 0d 0a
0100 72 61 67 6d 68 65 70 2d 61 6e 69 76 65 0d 0a
0110 6e 3b 63 61 63 68 65 0d 0a 55 70 67 72 61
0120 65 2d 49 6e 73 65 63 75 72 65 2d 52 05 71 75
0130 73 72 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67
0140 6e 74 3a 2b 6b 65 66 61 2f 35 2e 30
0150 70 6c 65 64 6d 6f 6b 65 70 6c 65 66 61 2f 35 2e
0160 6e 2b 70 57 69 6e 36 34 3b 2b 78 36 34 29 41
0170 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33
0180 29 28 4b 48 54 4d 4c 2c 20 6e 69 65 20 47
0190 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 31 32
0200 30 38 2e 30 20 53 61 61 72 69 2f 35 33
0210 2e 33 36 0d 0a 41 63 63 65 67 74 3a 20 74 65

Packets: 905 - Displayed: 0 (0.0%) - Dropped: 0 (0.0%)
Profile: Default

> Frame 161: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{D0752015-5002-4ECC-A4CA-604268186082}, id 0
> Ethernet II, Src: LitenTe_76:d2:cd (74:4c:a1:76:d2:cd), Dst: menuvivofibra (98:7e:ca:f6:9d:60)
> Internet Protocol Version 4, Src: 192.168.15.10 (192.168.15.10), Dst: gaia.cs.umass.edu (128.119.245.12)
> Transmission Control Protocol, Src Port: 56641, Dst Port: 80, Seq: 537, Ack: 1302, Len: 482
Source Port: 56641
Destination Port: 80
[Stream index: 5]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 482]
Sequence Number: 537 (relative sequence number)
Sequence Number (raw): 245364767
[Next Sequence Number: 1019 (relative sequence number)]
Acknowledgment Number: 1302 (relative ack number)
Acknowledgment Number (raw): 1912407909
Offset: 0x0100
Flags: 0x0108 (PSH, ACK)
Window: 512
[Calculated window size: 131072]
[Window size scaling factor: 256]
Checksum: 0x9e9a [unverified]

0020 f5 0c fd 41 00 50 0e 9f f8 1f 71 fd 07 05 51 72
0030 02 00 9e 9a 00 00 47 45 54 20 2f 77 69 72 65
0040 6f 61 72 6b 2d 6c 61 62 73 2f 48 54 50 2d
0050 69 72 65 73 2d 6b 72 6b 2d 66 69 6c 65 34 2e
0060 69 72 65 73 4d 6b 72 6b 2d 66 69 6c 65 34 2e
0070 73 74 3a 67 61 69 61 2e 75 63 73 6d 61
0080 73 2d 65 64 75 0d 0a 43 6f 6e 65 63 74 69
0090 6e 3a 2b 6b 65 65 70 2d 61 6e 69 76 65 0d 0a
0100 72 61 67 6d 68 65 70 2d 61 6e 69 76 65 0d 0a
0110 6e 3b 63 61 63 68 65 0d 0a 55 70 67 72 61
0120 65 2d 49 6e 73 65 63 75 72 65 2d 52 05 71 75
0130 73 72 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67
0140 6e 74 3a 2b 6b 65 66 61 2f 35 2e 30
0150 70 6c 65 64 6d 6f 6b 65 70 6c 65 66 61 2f 35 2e
0160 6e 2b 70 57 69 6e 36 34 3b 2b 78 36 34 29 41
0170 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33
0180 29 28 4b 48 54 4d 4c 2c 20 6e 69 65 20 47
0190 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 31 32
0200 30 38 2e 30 20 53 61 61 72 69 2f 35 33
0210 2e 33 36 0d 0a 41 63 63 65 67 74 3a 20 74 65

Packets: 905 - Displayed: 0 (0.0%) - Dropped: 0 (0.0%)
Profile: Default

> Frame 161: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{D0752015-5002-4ECC-A4CA-604268186082}, id 0
> Ethernet II, Src: LitenTe_76:d2:cd (74:4c:a1:76:d2:cd), Dst: menuvivofibra (98:7e:ca:f6:9d:60)
> Internet Protocol Version 4, Src: 192.168.15.10 (192.168.15.10), Dst: gaia.cs.umass.edu (128.119.245.12)
> Transmission Control Protocol, Src Port: 56641, Dst Port: 80, Seq: 1019, Ack: 4913, Len: 482
Source Port: 56641
Destination Port: 80
[Stream index: 5]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 482]
Sequence Number: 1019 (relative sequence number)
Sequence Number (raw): 245365249
[Next Sequence Number: 1040 (relative sequence number)]
Acknowledgment Number: 4913 (relative ack number)
Acknowledgment Number (raw): 1912411520
Offset: 0x0100
Flags: 0x0108 (PSH, ACK)
Window: 512
[Calculated window size: 131072]
[Window size scaling factor: 256]
Checksum: 0xa09c [unverified]

0020 f5 0c fd 41 00 50 0e 9f f8 1f 71 fd 07 05 51 72
0030 02 05 a6 9c 00 00 47 45 54 20 2f 66 61 76 69
0040 6f 6e 2e 69 63 6f 20 48 54 50 2f 31 2e 31
0050 0a 48 fd 73 74 3a 20 67 61 69 61 2e 63 73 2e
0060 6d 61 73 73 2e 65 64 75 0d 0a 43 6f 6e 65
0070 74 69 66 6e 3a 20 68 65 65 70 2d 61 6c 69 76
0080 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0090 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0100 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0110 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0120 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0130 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0140 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0150 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0160 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69

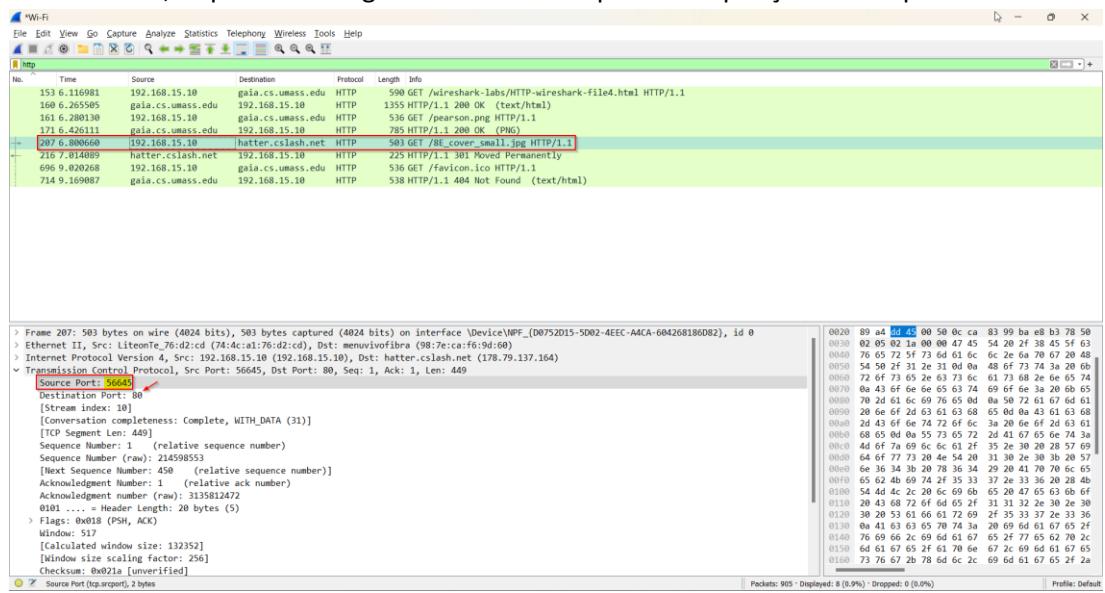
Packets: 905 - Displayed: 8 (0.9%) - Dropped: 0 (0.0%)
Profile: Default

> Frame 161: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{D0752015-5002-4ECC-A4CA-604268186082}, id 0
> Ethernet II, Src: LitenTe_76:d2:cd (74:4c:a1:76:d2:cd), Dst: menuvivofibra (98:7e:ca:f6:9d:60)
> Internet Protocol Version 4, Src: 192.168.15.10 (192.168.15.10), Dst: gaia.cs.umass.edu (128.119.245.12)
> Transmission Control Protocol, Src Port: 56641, Dst Port: 80, Seq: 1019, Ack: 4913, Len: 482
Source Port: 56641
Destination Port: 80
[Stream index: 5]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 482]
Sequence Number: 1019 (relative sequence number)
Sequence Number (raw): 245365249
[Next Sequence Number: 1040 (relative sequence number)]
Acknowledgment Number: 4913 (relative ack number)
Acknowledgment Number (raw): 1912411520
Offset: 0x0100
Flags: 0x0108 (PSH, ACK)
Window: 512
[Calculated window size: 131072]
[Window size scaling factor: 256]
Checksum: 0xa09c [unverified]

0020 f5 0c fd 41 00 50 0e 9f fa 01 71 fd 15 88 50
0030 02 05 a6 9c 00 00 47 45 54 20 2f 66 61 76 69
0040 6f 6e 2e 69 63 6f 20 48 54 50 2f 31 2e 31
0050 0a 48 fd 73 74 3a 20 67 61 69 61 2e 63 73 2e
0060 6d 61 73 73 2e 65 64 75 0d 0a 43 6f 6e 65
0070 74 69 66 6e 3a 20 68 65 65 70 2d 61 6c 69 76
0080 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0090 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0100 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0110 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0120 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0130 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0140 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0150 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69
0160 69 72 65 64 75 0d 0a 43 6f 6e 65 70 2d 61 6c 69

Packets: 905 - Displayed: 8 (0.9%) - Dropped: 0 (0.0%)
Profile: Default

O navegador também fez o download dos objetos de forma paralela para os envios feitos para IP's diferentes, o pois foi utilizado um socket diferente para guardar as informações baixadas do servidor. No meu caso, as portas de origem são diferentes para as requisições feitas para IP's diferentes.



4. Autenticação HTTP.

- a. Acesse a página com o usuário e senha mencionados.

- b. Qual a resposta do servidor ao HTTP GET inicial do navegador?

R: A primeira resposta do servidor retorna o código 401 indicando que a página é protegida por senha. O usuário precisa digitar as credenciais para acessar o conteúdo da página.

- c. Na 2^a mensagem GET do navegador, qual novo campo é incluído na mensagem GET?

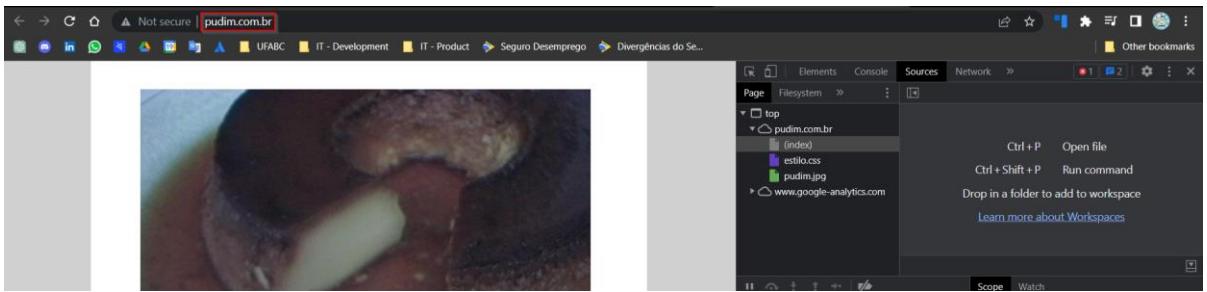
R: É incluso o campo **Autorization** ao digitar os valores de credenciais para validação.

- d. É possível visualizar o nome de usuário e senha no pacote captura pelo Wireshark? Discuta sobre a segurança desta autenticação HTTP.

R: Sim, é possível visualizar o nome de usuário e senha. Basta acessar o campo **Autorization**. De forma geral, essas informações estão desprotegidas para autenticação do tipo HTTP. Para contornar esse problema de segurança de informação, muitos servidores utilizam o HTTPS. O HTTPS é apenas um HTTP rodando junto com um socket de criptografia, para que assim os dados sejam protegidos.

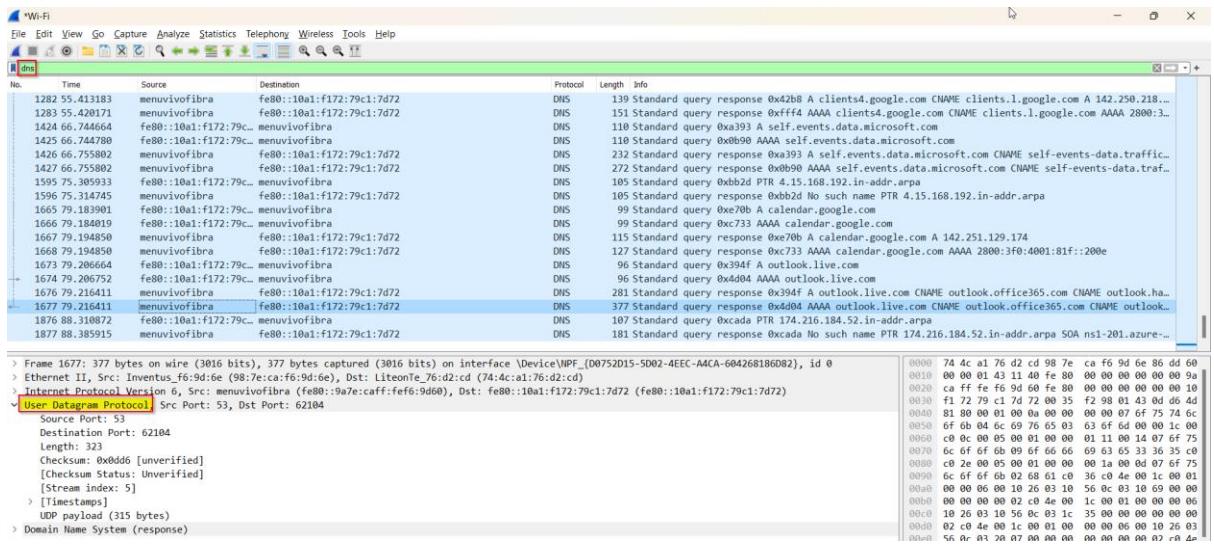
5. Resolução de nomes (Protocolo DNS).

- a. Acesse o site do Pudim e filtre as mensagens DNS.



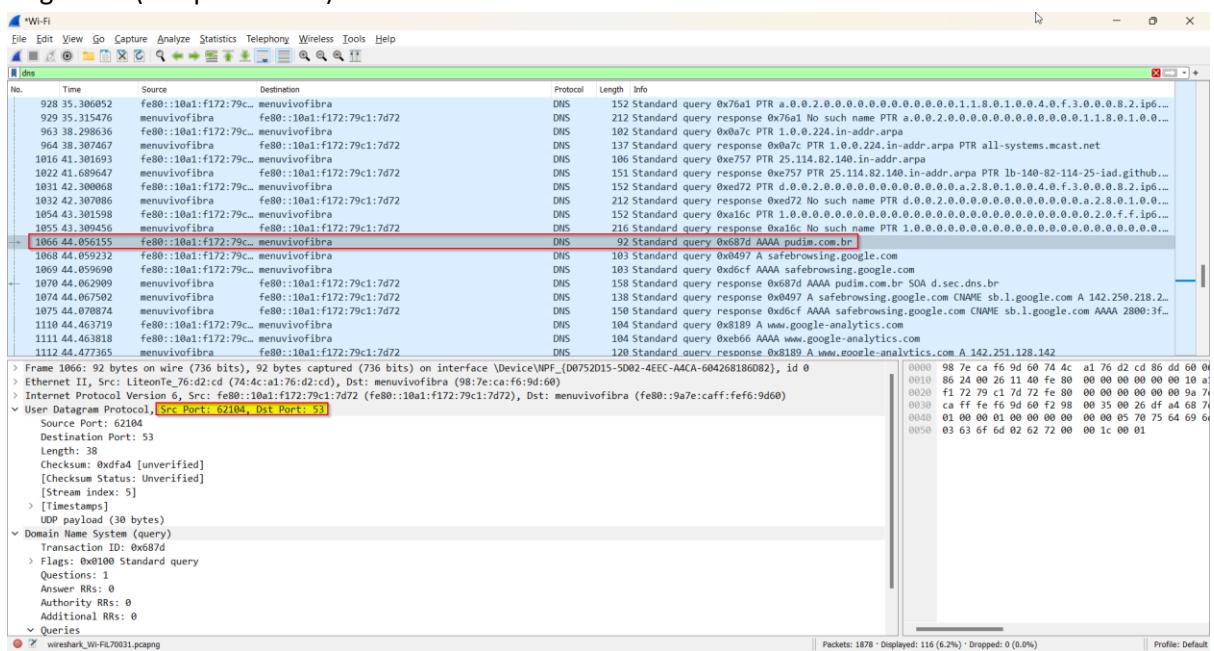
- b. O protocolo DNS usa TCP ou UDP?

R: O DNS é transportado pelo protocolo UDP.



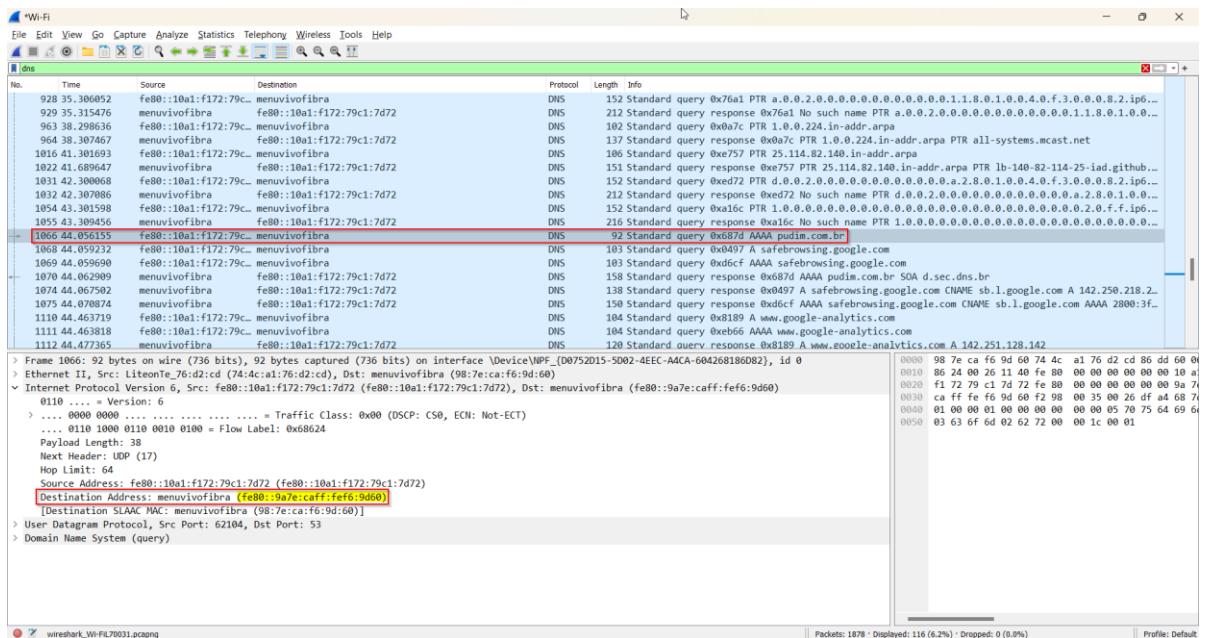
- c. Identifique a porta de destino da msg query DNS e a porta de origem da msg resposta do DNS.

R: DNS utiliza a porta de destino 53 (campo **Dst Port**) e a resposta também é feita com a porta de origem 53 (campo **Src Port**).



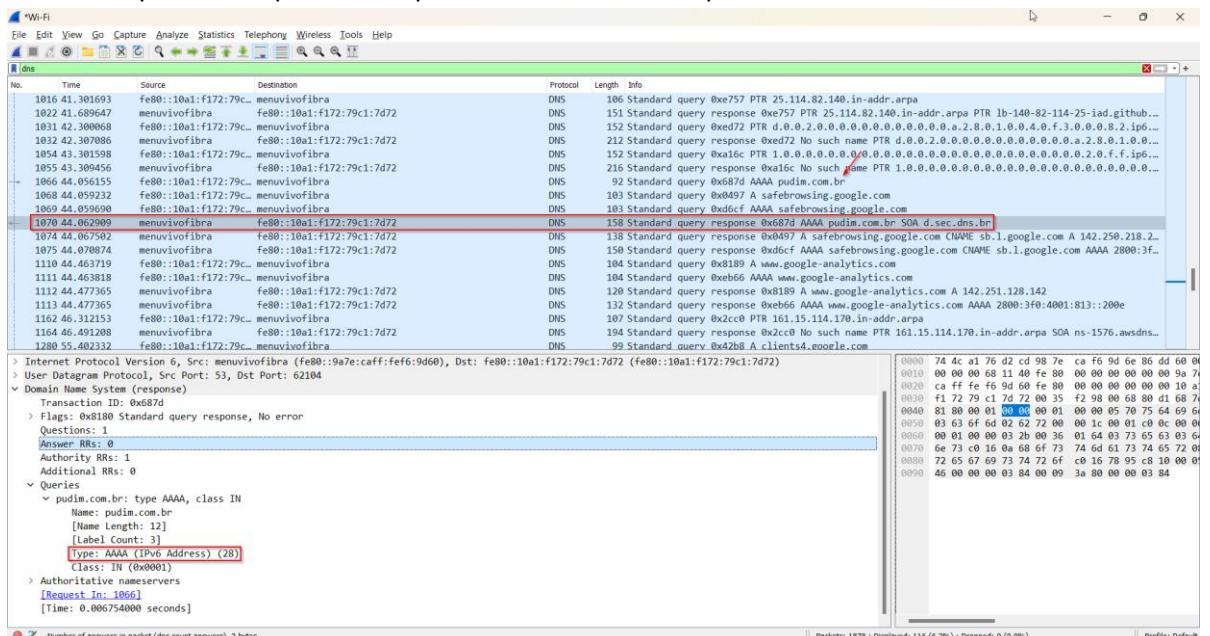
- d. Identifique o endereço IP para qual a mensagem de query do DNS foi enviada.

R:



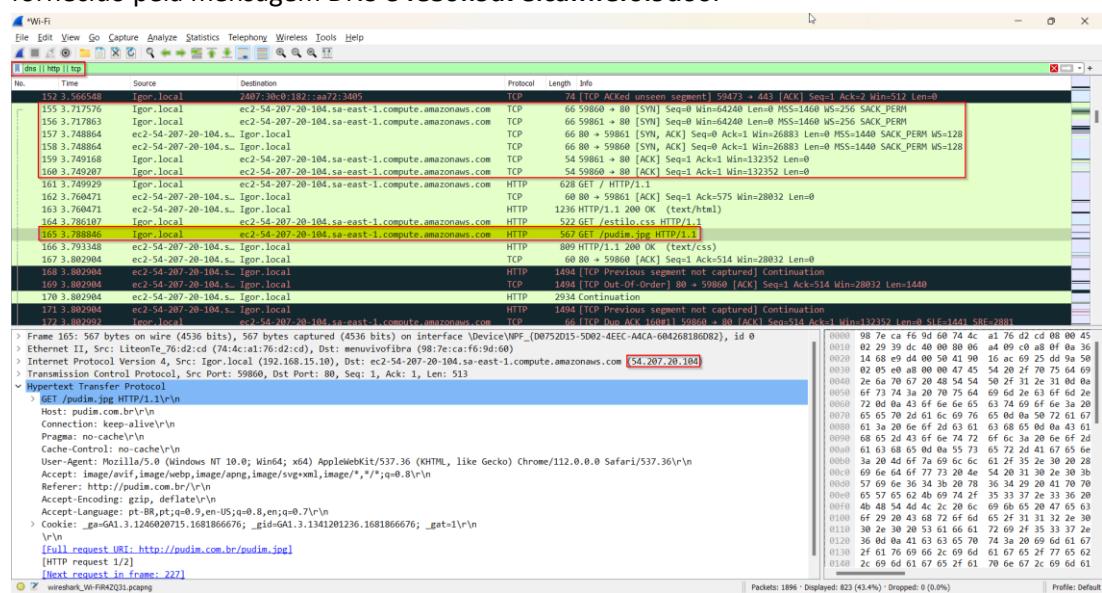
- e. Examine a resposta DNS. Quantas “respostas” foram dadas? Qual o conteúdo destas respostas?

R: Recebi apenas 1 resposta. A resposta recebida está em ipv6.



- f. Aplique os filtros necessários e considere o pacote TCP SYN subsequente enviado pelo navegador. O IP de destino do pacote TCP SYN corresponde ao endereço IP fornecido pela msg de resposta DNS?

R: Não corresponde, pois o IP destino do pacote TCP SYN é **54.207.20.104** enquanto o endereço IP fornecido pela mensagem DNS é **fe80::9a7e:caff:fe:6:9d60**.



- g. Esta página contém imagens. Antes de requisitar cada imagem, seu host faz novas queries DNS?
R: O host não faz novas queries DNS para páginas que contém imagens, pois essas informações já se encontram armazenadas no cache da página.

6. Usando nslookup.

- a. Execute o comando nslookup ***www.mit.edu***

R: O nslookup faz consulta DNS a nível de comando.

```
Prompt de Comando
Microsoft Windows [versão 10.0.22621.1555]
(c) Microsoft Corporation. Todos os direitos reservados.

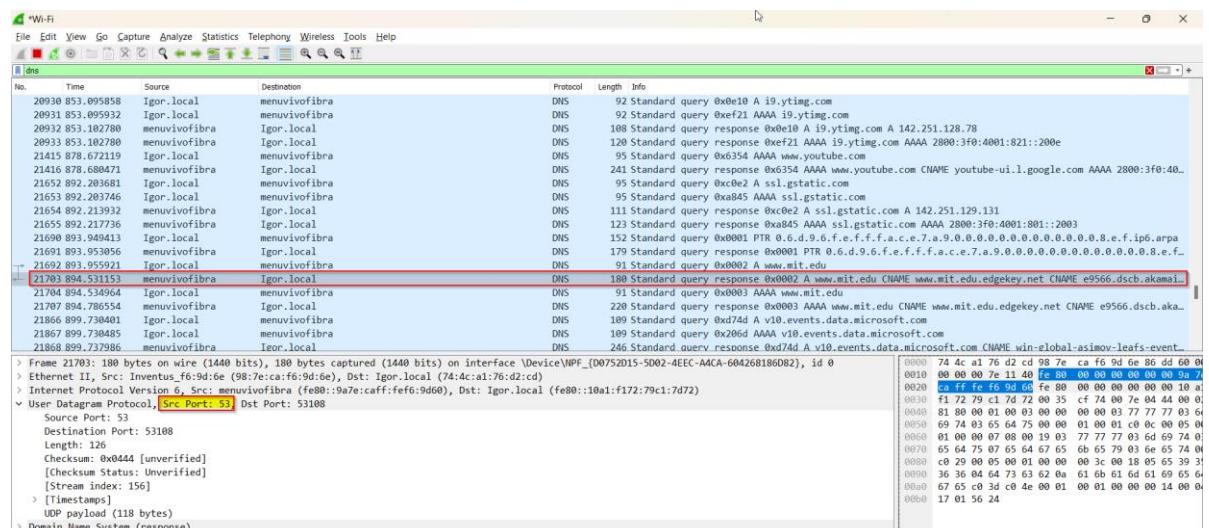
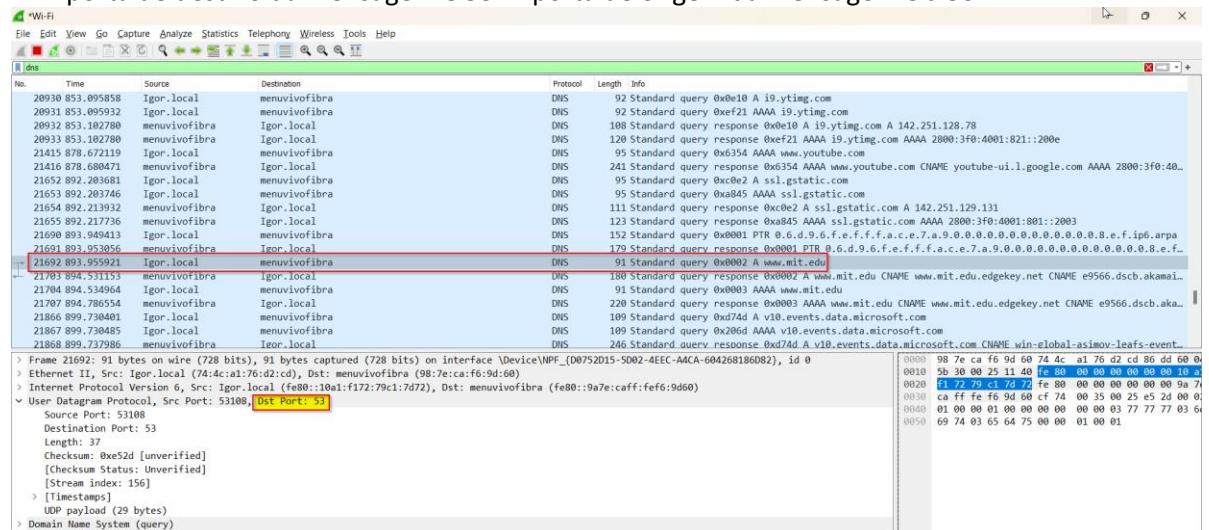
C:\Users\igor>..
'..' não é reconhecido como um comando interno
ou externo, um programa operável ou um arquivo em lotes.

C:\Users\igor>nslookup www.mit.edu
Servidor: menuvivofibra
Address: fe80::9a7e:caff:fef6:9d68

Não é resposta autoritativa:
Nome: e9566_dsch.akamaiedge.net
Addresses: 2608:1419:d400:295::255e
           2608:1419:d400:297::255e
           23.1.86.36
Aliases: www.mit.edu
         www.mit.edu.edgekey.net
```

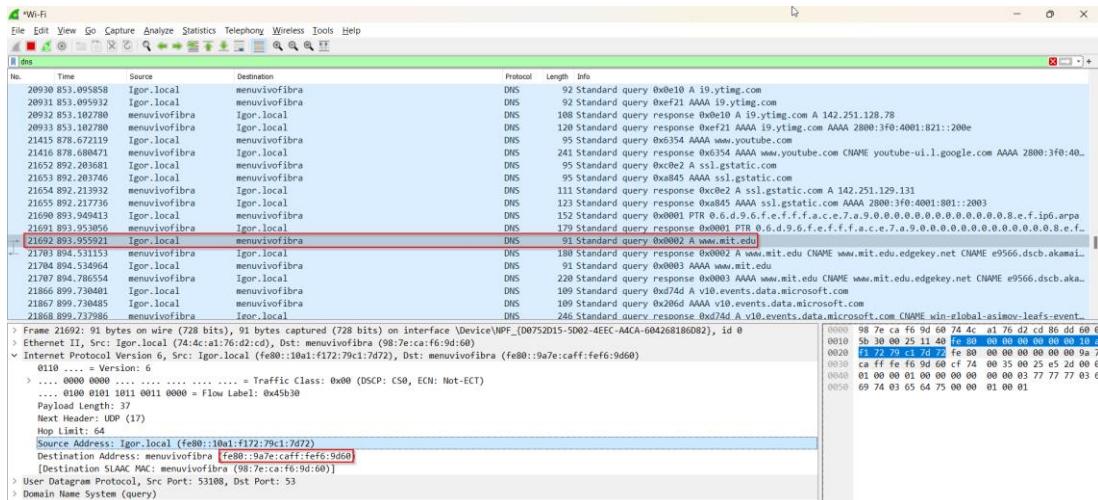
- b. Identifique a porta de destino da mgs de query DNS e a porta de origem da mgs de resposta do DNS.

R: A porta de destino da mensagem é 53. A porta de origem da mensagem é a 53.



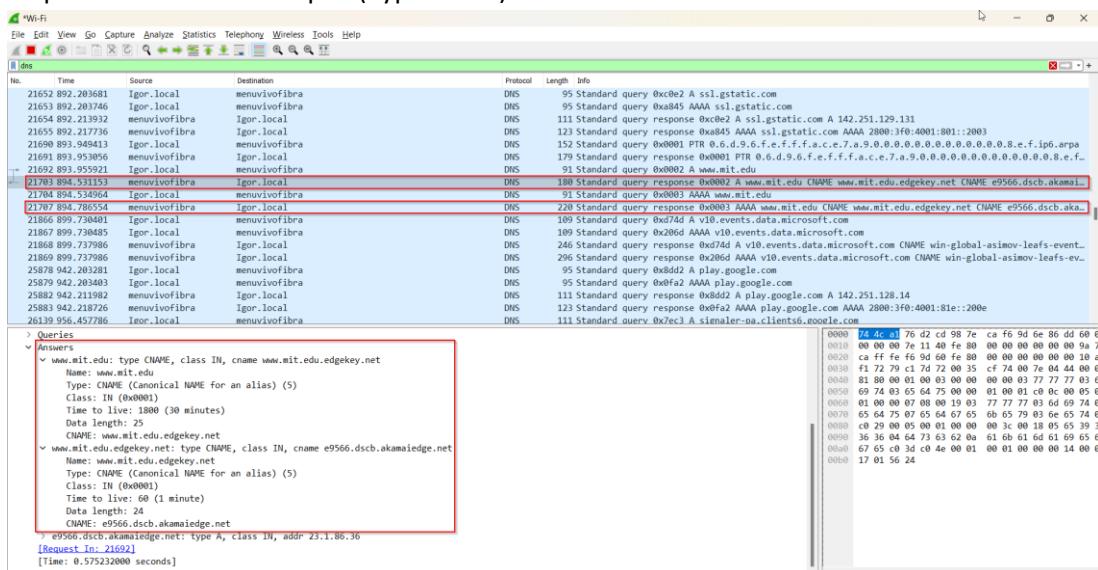
- c. Identifique o endereço IP para qual a msg de query DNS foi enviada.

R: O endereço IP do site www.mit.edu é **23.38.159.112**. O servidor continua sendo o mesmo fe80::9a7e:caff:fef6:9d60.



- d. Examine a resposta DNS. Quantas “respostas” foram dadas? Qual o conteúdo destas respostas?

R: Foram dadas 2 respostas. Uma resposta para a requisição com formato ipv4 (Type A) e outra resposta com o formato ipv6 (Type AAAA).



- e. Execute o comando **nslookup www.aiit.or.kr google-public-dns-a.google.com**

R:

```
C:\Users\igor>..  
'.' não é reconhecido como um comando interno  
ou externo, um programa operável ou um arquivo em lotes.  
  
C:\Users\igor>nslookup www.mit.edu  
Servidor: menuvivofibra  
Address: fe80::9a7e:caff:fef6:9d60  
  
Name: e9566.dsdb.akamaiedge.net  
Addresses: 2600:1419:4d00:295::255e  
2600:1419:4d00:297::255e  
23.1.86.36  
Aliases: www.mit.edu  
www.mit.edu.edgekey.net  
  
C:\Users\igor>nslookup www.aiit.or.kr google-public-dns-a.google.com  
*** Não é possível encontrar o endereço do servidor para 'google-public-dns-a.google.com'.  
Servidor: menuvivofibra  
Address: fe80::9a7e:caff:fef6:9d60  
  
DNS request timed out.  
timeout was 2 seconds.  
DNS request timed out.  
timeout was 2 seconds.  
DNS request timed out.  
timeout was 2 seconds.  
*** O tempo limite da solicitação para menuvivofibra expirou  
  
C:\Users\igor>nslookup www.aiit.or.kr google-public-dns-a.google.com  
Servidor: dns.google  
Address: 2001:4860::8888  
  
Name: www.aiit.or.kr  
Address: 58.229.6.225
```

- f. Identifique o endereço IP para qual a mensagem de query do DNS foi enviada. Este endereço IP é o mesmo do seu servidor DNS local? Caso contrário, esse endereço IP corresponde a que servidor?

R: A mensagem foi enviada para o endereço de IP do site www.aiit.or.kr (**58.229.6.225**) usando o servidor dns.google (**2001:4860:4860::8888**). Esse servidor não é o mesmo do DNS local da região de Santo André, pois o endereço (**58.229.6.225**) corresponde a um servidor localizado na Coreia do Sul.

- g. Examine a resposta DNS. Quantas “respostas” foram dadas? Qual o conteúdo destas respostas?

R: Foi dado apenas 1 resposta para o formato ipv4 (Type A). Não tivemos retorno de dados para o formato ipv6 (Type AAAA).