

Pontifícia Universidade Católica de Minas Gerais



Redes de Computadores II

Trabalho Wireshark

Aluno	Geovane Fonseca de Sousa Santos
Professor	Marco Antonio da Silva Barbosa

Belo Horizonte, 10 de Março de 2019

Conteúdo

1	Introdução	1
2	DNS	2
2.1	NSLOOKUP	2
2.2	Rastreando DNS com Wireshark	3
2.3	Capturar os pacotes ao utilizar o comando "nslookup www.mit.edu	4
2.4	Capturar os pacotes ao utilizar o comando "nslookup -type=NS pucminas.br	5
2.5	Capturar os pacotes ao utilizar o comando "nslookup www.aiit.or.kr ns.pucminas.br	5
3	HTTP	7
3.1	A Interação Básica GET/Resposta do HTTP	7
3.2	A Interação HTTP GET Condicional/Resposta	10
3.3	Baixando Documentos Longos	12
3.4	Documentos HTML com Objetos Incluídos	14
3.5	Autenticação HTTP	15

1 Introdução

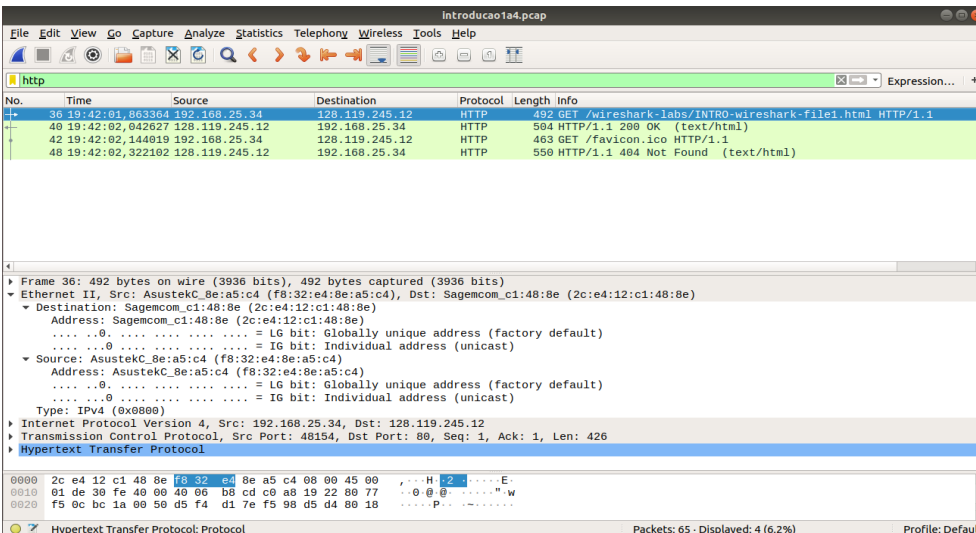
1. Protocolos encontrados:

- HyperText Transfer Protocol (HTTP)
- Transfer Control Protocol (TCP)
- Internet Protocol Version 4 (IPV4)
- Ethernet II

2. O tempo de envio da mensagem HTTP GET foi 19:42:01,863364 e o tempo que a resposta OK foi recebida foi 19:42:02,042627. Dessa forma, o tempo que passou foi de 0,179263 segundos.

3. O IP do site usado no exercício é 128.119.245.12 e o IP da interface do meu computador é 192.168.25.34.

4.

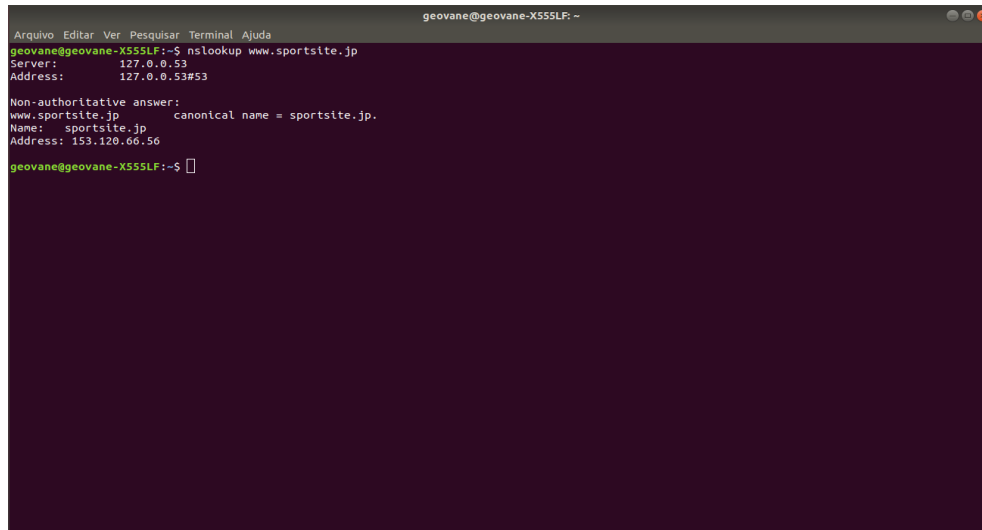


The screenshot shows the Wireshark interface with a packet capture of an HTTP GET request and its response. The packet list shows four packets: a GET request for /wireshark-labs/INTRO-wireshark-file1.html, a 200 OK response, a GET request for /favicon.ico, and a 404 Not Found response. The packet details for the first packet show Ethernet II, IPv4, and Hypertext Transfer Protocol layers. The packet bytes show the raw data.

2 DNS

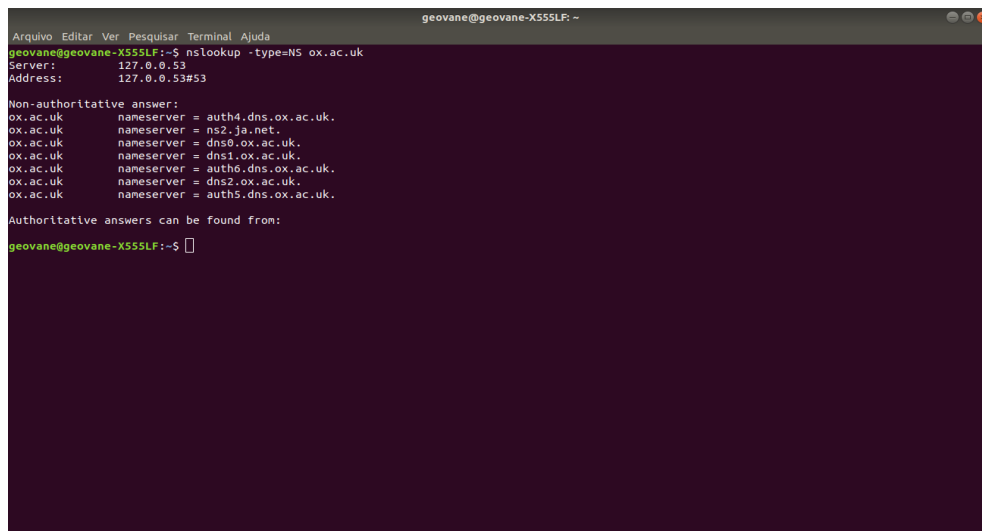
2.1 NSLOOKUP

1. Ao utilizar o site japonês `www.sportsite.jp`, obteve-se o seguinte resultado:



```
geovane@geovane-X555LF: ~  
Arquivo Editar Ver Pesquisar Terminal Ajuda  
geovane@geovane-X555LF:~$ nslookup www.sportsite.jp  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
www.sportsite.jp canonical name = sportsite.jp.  
Name:   sportsite.jp  
Address: 153.120.66.56  
geovane@geovane-X555LF:~$
```

2. Não foi possível analisar os servidores DNS autoritários, pois o comando NSLOOKUP não os retornou.



```
geovane@geovane-X555LF: ~  
Arquivo Editar Ver Pesquisar Terminal Ajuda  
geovane@geovane-X555LF:~$ nslookup -type=NS ox.ac.uk  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
ox.ac.uk      nameserver = auth4.dns.ox.ac.uk.  
ox.ac.uk      nameserver = ns2.ja.net.  
ox.ac.uk      nameserver = dns0.ox.ac.uk.  
ox.ac.uk      nameserver = dns1.ox.ac.uk.  
ox.ac.uk      nameserver = auth6.dns.ox.ac.uk.  
ox.ac.uk      nameserver = dns2.ox.ac.uk.  
ox.ac.uk      nameserver = auth5.dns.ox.ac.uk.  
  
Authoritative answers can be found from:  
geovane@geovane-X555LF:~$
```

3. Utilizando o servidor DNS da Google 8.8.8.8, foi possível determinar o IP do Portal do Office 365:

```
geovane@geovane-X555LF: ~  
Arquivo Editar Ver Pesquisar Terminal Ajuda  
geovane@geovane-X555LF:~$ nslookup portal.office.com 8.8.8.8  
Server:      8.8.8.8  
Address:     8.8.8.8#53  
  
Non-authoritative answer:  
portal.office.com canonical name = geo.portal.office.akadns.net.  
geo.portal.office.akadns.net canonical name = nonus_edge.portal.office.akadns.net.  
nonus_edge.portal.office.akadns.net canonical name = portal-office365-com.b-0004.b-msedge.net.  
portal-office365-com.b-0004.b-msedge.net canonical name = b-0004.b-msedge.net.  
Name:   b-0004.b-msedge.net  
Address: 13.107.6.156  
Name:   b-0004.b-msedge.net  
Address: 2620:1ec:a92::156  
geovane@geovane-X555LF:~$
```

2.2 Rastreando DNS com Wireshark

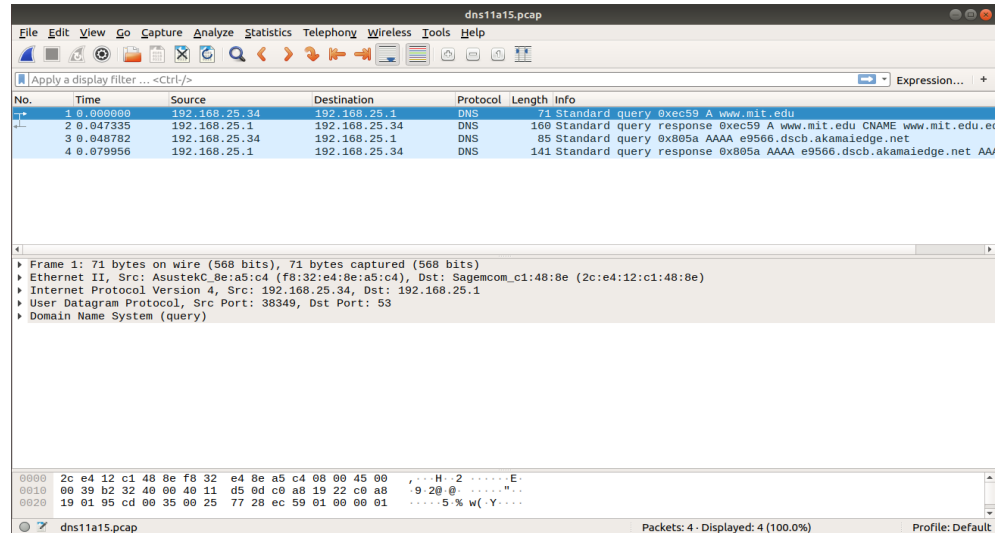
4. As mensagens de solicitação e resposta DNS foram enviadas com UDP.
5. A porta de destino para a mensagem de consulta DNS foi 53 a mesma que a porta fonte para a mensagem de resposta.
6. O endereço de IP com o qual a mensagem de consulta DNS é enviada é 192.168.25.34, que é o mesmo ao consultar o IP do servidor DNS local.
7. O campo Type da mensagem, diz que o DNS é do tipo A. A mensagem de consulta não contém nenhum campo answer.
8. Há três campos answer. Nessas mensagens há:
 - Nome
 - Tipo
 - Classe
 - Tempo de vida
 - Comprimento do dado
 - Endereço
9. Sim, o endereço de IP de destino corresponde ao endereço de IP fornecido na mensagem de resposta DNS anterior.
10. Não. Nenhuma consulta DNS é realizada para recuperar as imagens do site.

2.3 Capturar os pacotes ao utilizar o comando "nslookup www.mit.edu"

11. A porta de destino para a mensagem de consulta do DNS é 53 a mesma que a porta fonte para a mensagem de resposta.
12. O endereço de IP com o qual a mensagem de consulta DNS é enviada é 192.168.25.1, que é o mesmo IP do servidor DNS local.
13. O campo Type da mensagem, diz que o DNS é do tipo A. A mensagem de consulta não contém nenhum campo answer.
14. Há três campos com answer. Nessas mensagens há em todas:
 - Nome
 - Tipo
 - Classe
 - Tempo de vida
 - Comprimento do dado

Em em duas há o campo CNAME enquanto na última há o campo Endereço.

15.



The screenshot shows the Wireshark interface with a display filter of 'dns'. The packet list contains four packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.25.34	192.168.25.1	DNS	71	Standard query 0xec59 A www.mit.edu
2	0.047335	192.168.25.1	192.168.25.34	DNS	168	Standard query response 0xec59 A www.mit.edu CNAME www.mit.edu.e
3	0.048782	192.168.25.34	192.168.25.1	DNS	85	Standard query 0x805a AAAA e9566.dscb.akamaiedge.net
4	0.079956	192.168.25.1	192.168.25.34	DNS	141	Standard query response 0x805a AAAA e9566.dscb.akamaiedge.net AA

The details pane for packet 2 shows the following structure:

- Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
- Ethernet II, Src: AsustekC_8e:a5:c4 (f8:32:e4:8e:a5:c4), Dst: Sagemcom_c1:48:8e (2c:e4:12:c1:48:8e)
- Internet Protocol Version 4, Src: 192.168.25.34, Dst: 192.168.25.1
- User Datagram Protocol, Src Port: 38349, Dst Port: 53
- Domain Name System (query)

The packet bytes section shows the raw data in hexadecimal and ASCII:

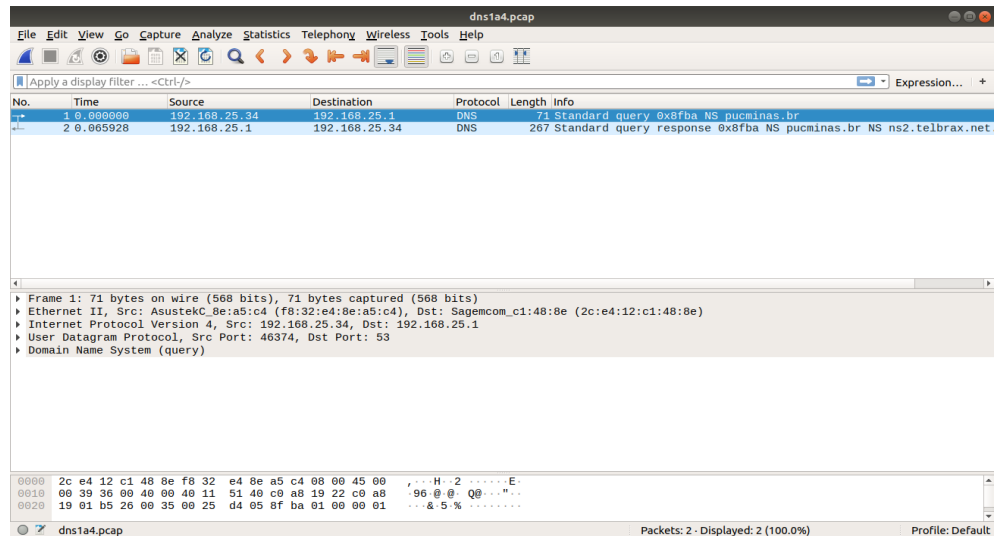
```
0000 2c e4 12 c1 48 8e f8 32 e4 8e a5 c4 08 00 45 00  ,...H...2.....E..
0010 00 39 b2 32 40 00 40 11 d5 0d c0 a8 19 22 c0 a8  '9.2@.: .....".
0020 19 01 95 cd 00 35 00 25 77 28 ec 59 01 00 00 01  ....5.%w(·Y....
```

2.4 Capturar os pacotes ao utilizar o comando "nslookup -type=NS pucminas.br"

16. O endereço de IP com o qual a mensagem de consulta DNS é enviada é 192.168.25.1, que é o mesmo IP do servidor DNS local.
17. O campo Type da mensagem, diz que o DNS é do tipo NS. A mensagem de consulta não contém nenhum campo answer.
18. Os servidores do MIT fornecidos na resposta foram:
 - ns2.telbrax.net.br
 - ns.embratel.net.br
 - ns.pucminas.br
 - ns01.telmex.net.br
 - dns02.redeinfovias.net.br

A mensagem de resposta não forneceu os endereços IP's dos servidores DNS da PUC.

19.



The screenshot shows the Wireshark interface with a capture of two DNS packets. The packet list shows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.25.34	192.168.25.1	DNS	71	Standard query 0x8fba NS pucminas.br
2	0.005928	192.168.25.1	192.168.25.34	DNS	267	Standard query response 0x8fba NS pucminas.br NS ns2.telbrax.net

The packet details for the first packet (Frame 1) are shown below:

- Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
- Ethernet II, Src: AsustekC_8e:a5:c4 (f8:32:e4:8e:a5:c4), Dst: Sagemcom_c1:48:8e (2c:e4:12:c1:48:8e)
- Internet Protocol Version 4, Src: 192.168.25.34, Dst: 192.168.25.1
- User Datagram Protocol, Src Port: 46374, Dst Port: 53
- Domain Name System (query)

The packet bytes are displayed at the bottom, showing the raw data in hexadecimal and ASCII.

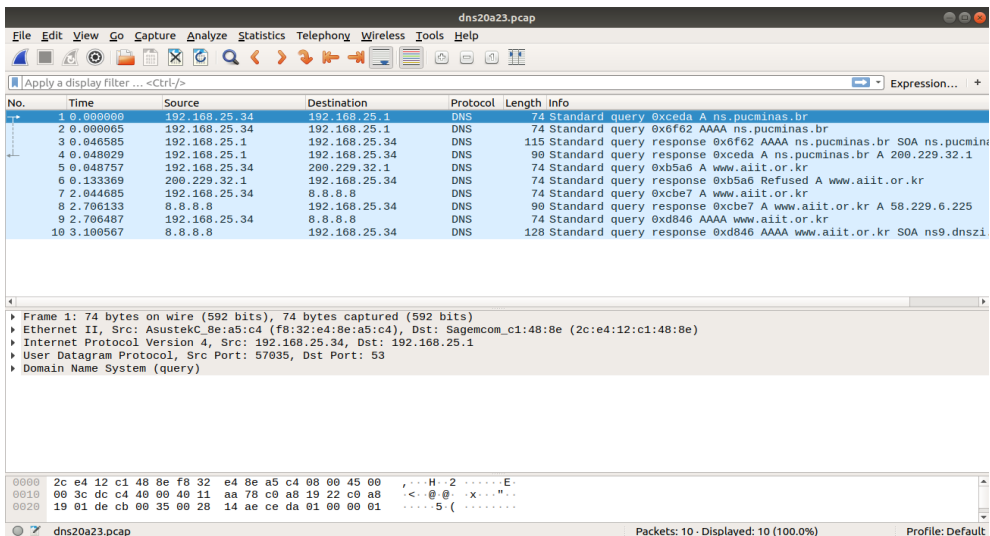
2.5 Capturar os pacotes ao utilizar o comando "nslookup www.aiit.or.kr ns.pucminas.br"

Obs: Não funcionou usando o servidos ns.pucminas.br. Sendo assim o endereço de servidor usado foi o 8.8.8.8 da Google.

20. O endereço de IP com o qual a mensagem de consulta DNS é enviada é 8.8.8.8, que não é o mesmo IP do servidor DNS local. O host é o servidor fornecido para o NSLOOKUP.
21. O campo Type da mensagem, diz que o DNS é do tipo A. A mensagem de consulta não contém nenhum campo answer.
22. Há um campo com answer. Nele há:

- Nome
- Tipo
- Classe
- Tempo de vida
- Comprimento do dado
- Endereço

23.



The screenshot shows the Wireshark interface with a packet capture of a DNS query and response. The packet list shows a query from 192.168.25.34 to 192.168.25.1 and a response from 192.168.25.1 to 192.168.25.34. The packet details show the query for 'exceda A ns.pucminas.br' and the response with the answer 'exceda A ns.pucminas.br'.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.25.34	192.168.25.1	DNS	74	Standard query 0xcda A ns.pucminas.br
2	0.000005	192.168.25.34	192.168.25.1	DNS	74	Standard query 0x6f2 AAAA ns.pucminas.br
3	0.046585	192.168.25.1	192.168.25.34	DNS	115	Standard query response 0x6f2 AAAA ns.pucminas.br SOA ns.pucminas.br
4	0.048029	192.168.25.1	192.168.25.34	DNS	90	Standard query response 0xcda A ns.pucminas.br A 200.229.32.1
5	0.048757	192.168.25.34	200.229.32.1	DNS	74	Standard query 0xb5a6 A www.aiit.or.kr
6	0.133369	200.229.32.1	192.168.25.34	DNS	74	Standard query response 0xb5a6 Refused A www.aiit.or.kr
7	2.044605	192.168.25.34	8.8.8.8	DNS	74	Standard query 0xcbe7 A www.aiit.or.kr
8	2.706133	8.8.8.8	192.168.25.34	DNS	90	Standard query response 0xcbe7 A www.aiit.or.kr A 50.229.6.225
9	2.706487	192.168.25.34	8.8.8.8	DNS	74	Standard query 0xd846 AAAA www.aiit.or.kr
10	3.100567	8.8.8.8	192.168.25.34	DNS	128	Standard query response 0xd846 AAAA www.aiit.or.kr SOA ns9.dnszi

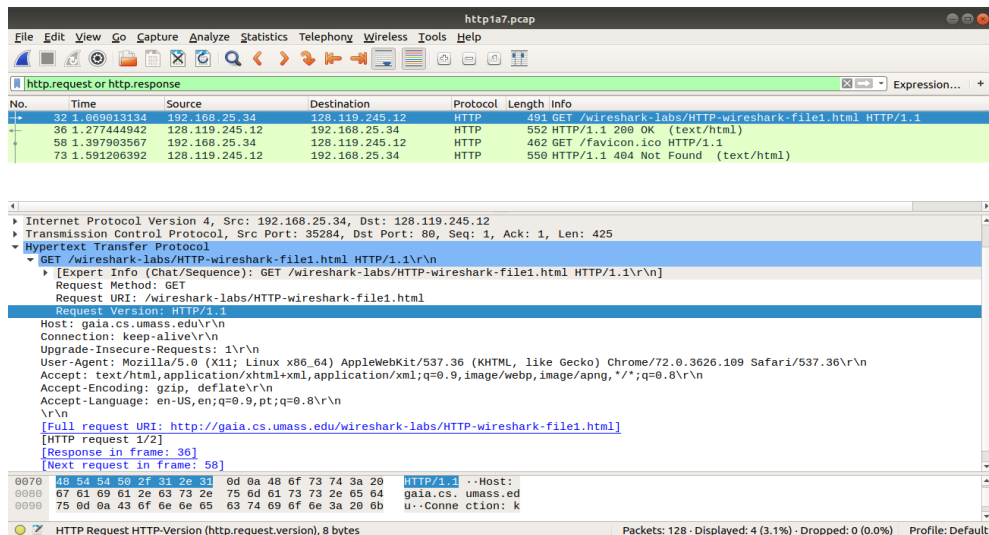
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: AsustekC8e:a5:c4 (f8:32:e4:8e:a5:c4), Dst: Sagemcom_c1:48:8e (2c:e4:12:c1:48:8e)
 Internet Protocol Version 4, Src: 192.168.25.34, Dst: 192.168.25.1
 User Datagram Protocol, Src Port: 57635, Dst Port: 53
 Domain Name System (query)

0000 2c e4 12 c1 48 8e f8 32 e4 8e a5 c4 08 00 45 00H..2.....E..
 0010 08 3c dc c4 48 00 40 11 aa 78 c0 a8 19 22 c0 a8 ..<..@..x.....
 0020 19 01 de cb 00 35 00 28 14 ae ce da 01 00 00 015(.....

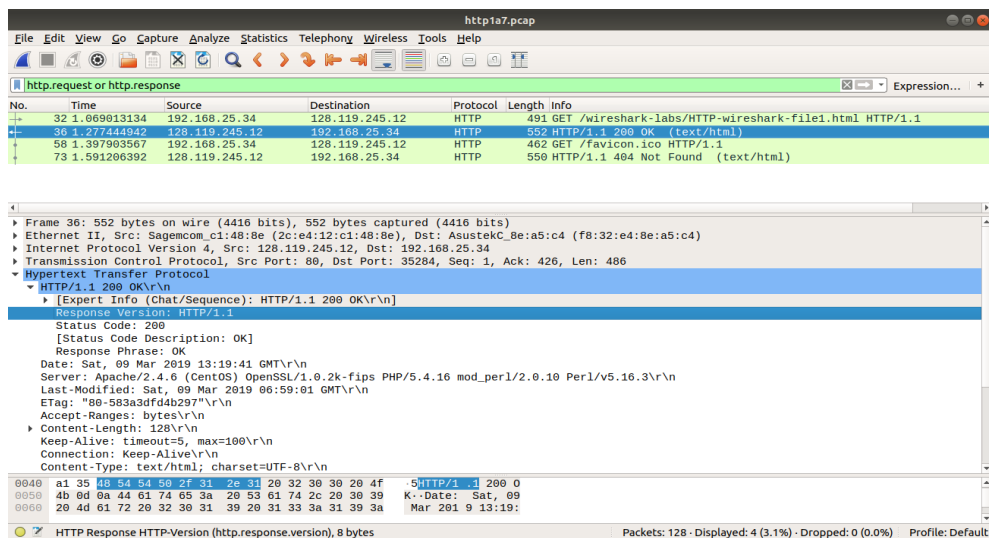
3 HTTP

3.1 A Interação Básica GET/Resposta do HTTP

1.

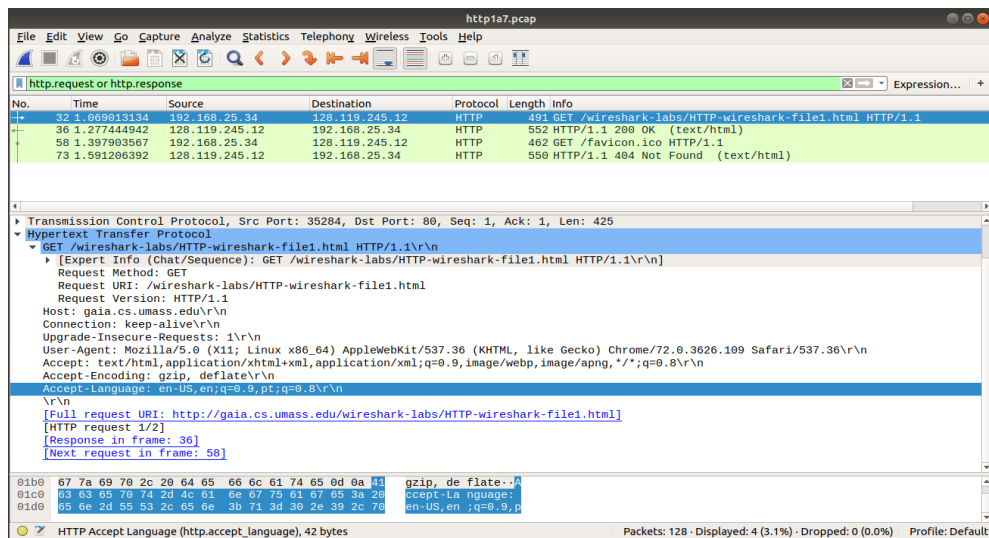


O meu navegador executa a versão 1.1 do HTTP

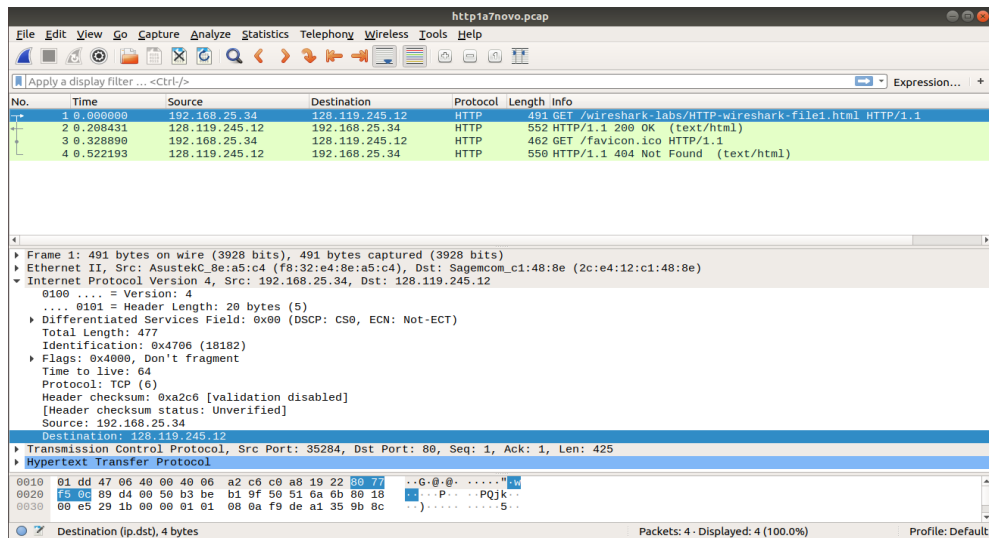


O servidor também executa a versão 1.1 do HTTP

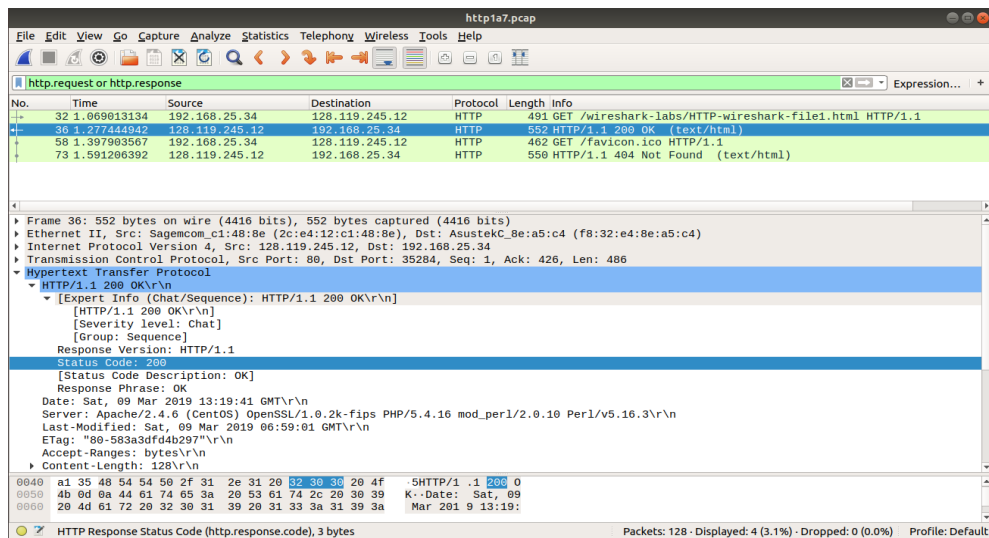
2. As linguagens que o meu navegador pode aceitar do servidor são inglês americano (en-US), inglês britânico (en) e português (pt).



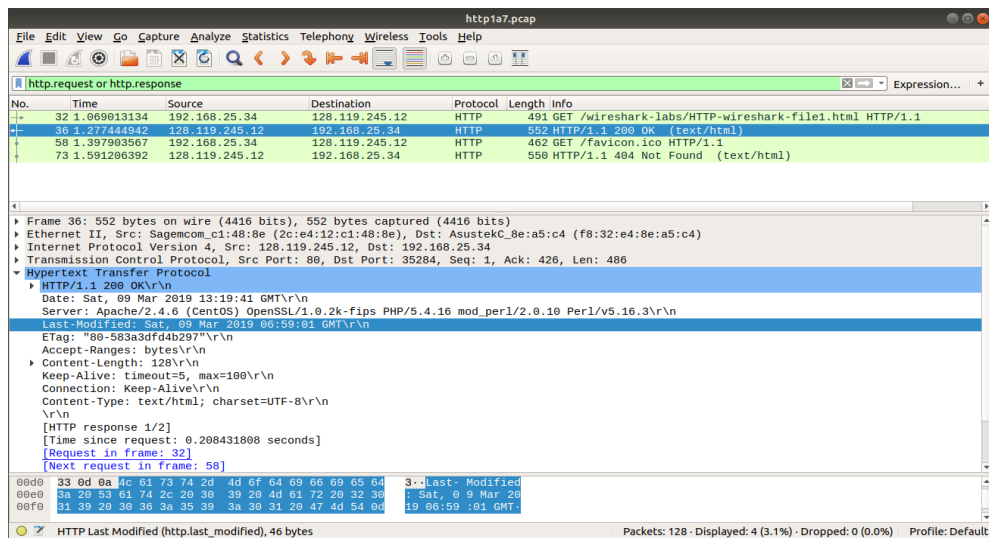
3. O meu IP é 192.168.25.34. O IP do servidor é 128.119.245.12.



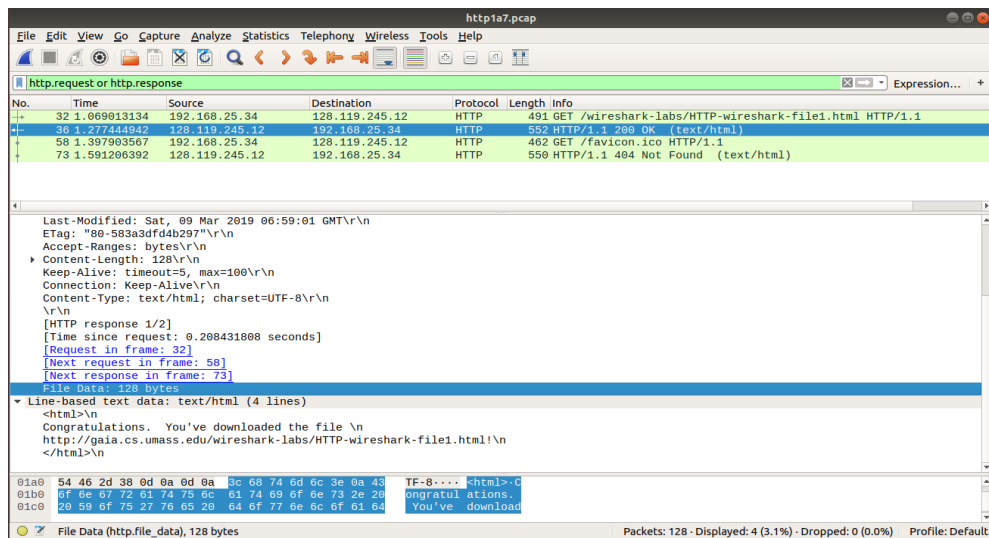
4. O código do status retornado do servidor é o 200 (OK).



5. A última vez que o arquivo foi modificado no servidor foi em 09 de março de 2019 às 06:59:01.



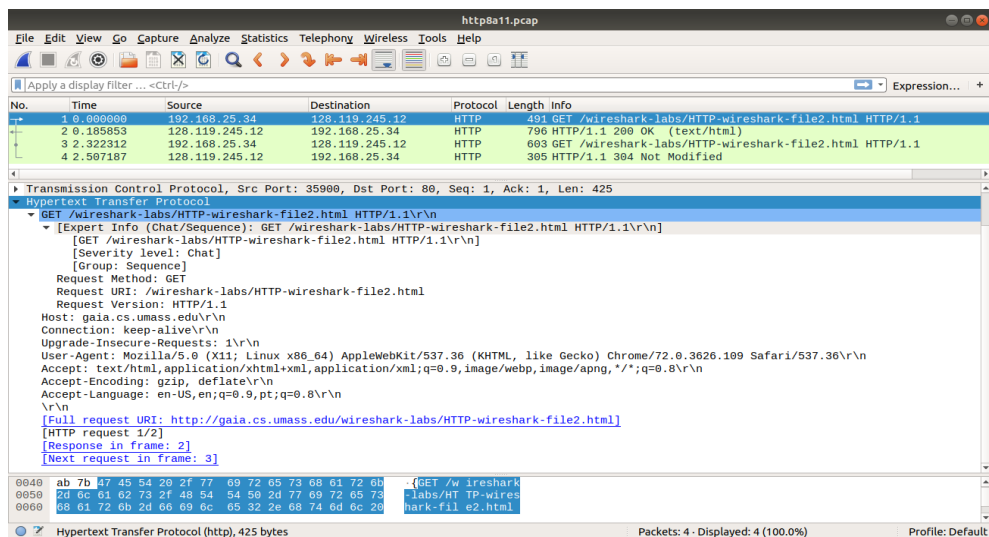
6. São retornados 128 bytes de conteúdo.



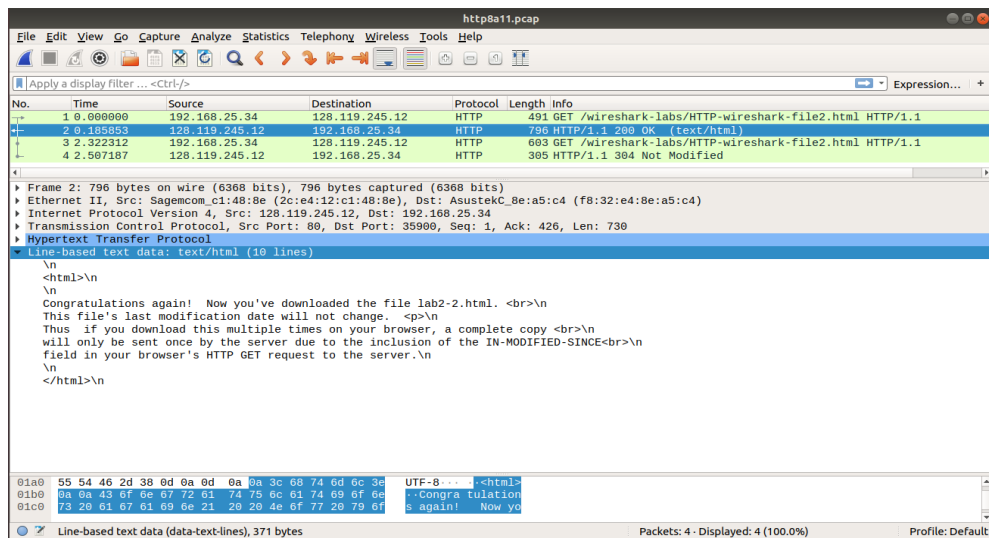
7. Nenhum cabeçalho foi encontrado dentro dos dados que não sejam exibidos na janela de listagem de pacotes.

3.2 A Interação HTTP GET Condicional/Resposta

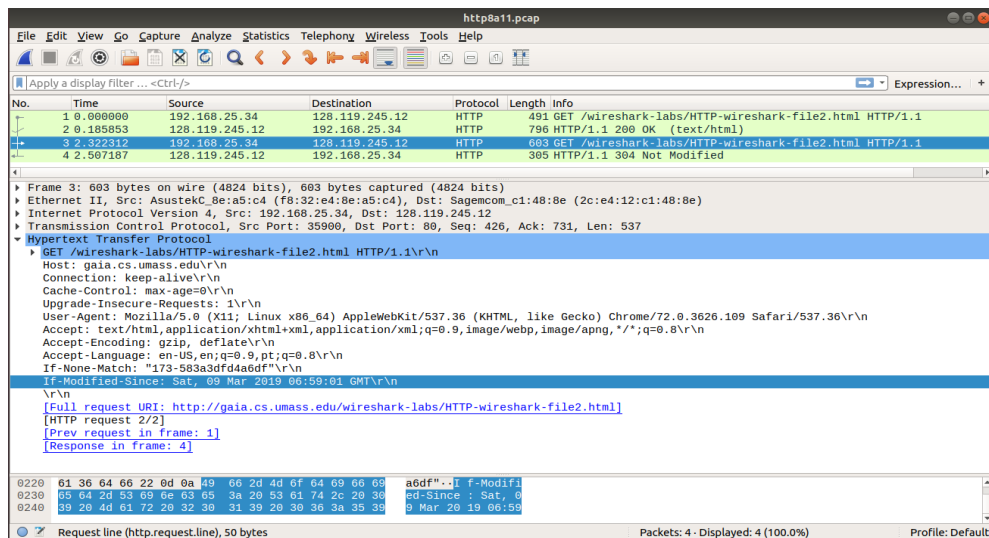
8. Não existe a linha IF-MODIFIED-SINCE no conteúdo do arquivo na primeira mensagem GET HTTP.



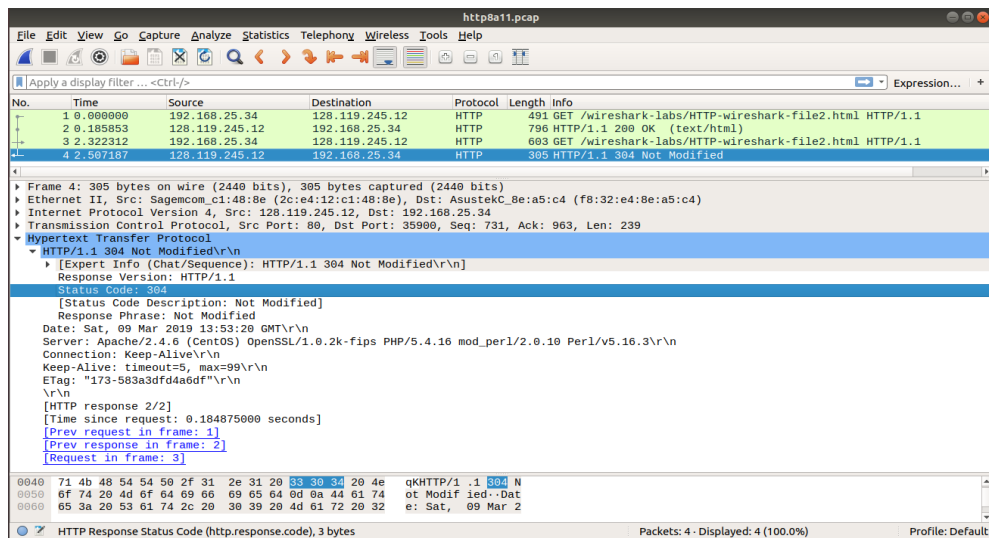
9. Sim, o servidor retornou explicitamente o conteúdo do arquivo. É possível afirmar isso ao abrir o conteúdo da mensagem HTTP e verificar o texto de dados.



10. Sim, na segunda mensagem HTTP há a linha IF-MODIFIED-SINCE. O seu conteúdo é a data que estava no Last-Modified da última mensagem HTTP GET.

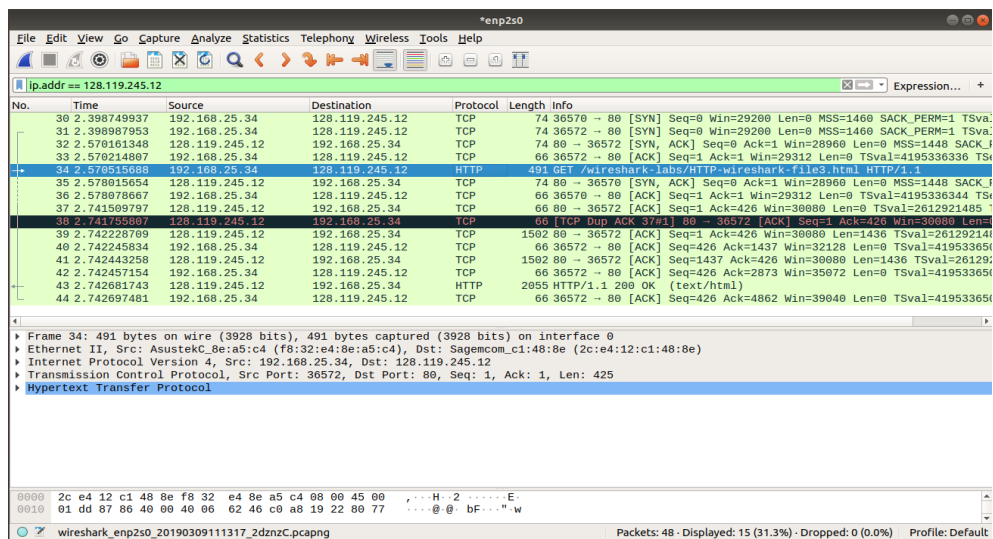


11. O código de status na segunda mensagem é 304 e sua mensagem é Not Modified. O servidor não retornou explicitamente o conteúdo do arquivo, pois este conteúdo já estava na cache do navegador e ele não fora modificado.



3.3 Baixando Documentos Longos

12. Somente uma mensagem GET HTTP foi enviada pelo servidor.



13. Foram necessários 3 segmentos TCP para carregar a resposta.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.171412	128.119.245.12	192.168.25.34	TCP	74	80 → 36572 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1448
4	0.171465	192.168.25.34	128.119.245.12	TCP	66	36572 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=41953363
5	0.171766	192.168.25.34	128.119.245.12	HTTP	491	GET /wireshark-labs/HTTP-wireshark-fil1e3.html HTTP/1.1
6	0.179266	128.119.245.12	192.168.25.34	TCP	74	80 → 36570 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1448
7	0.179329	192.168.25.34	128.119.245.12	TCP	66	36570 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=41953363
8	0.342760	128.119.245.12	192.168.25.34	TCP	66	80 → 36572 [ACK] Seq=1 Ack=426 Win=30080 Len=0 TSval=261292
9	0.343066	128.119.245.12	192.168.25.34	TCP	66	[TCP Dup ACK 8#1] 80 → 36572 [ACK] Seq=1 Ack=426 Win=30080
10	0.343479	128.119.245.12	192.168.25.34	TCP	1502	80 → 36572 [ACK] Seq=1 Ack=426 Win=30080 Len=1436 TSval=261
11	0.343496	192.168.25.34	128.119.245.12	TCP	66	36572 → 80 [ACK] Seq=426 Ack=1437 Win=32128 Len=0 TSval=419
12	0.343693	128.119.245.12	192.168.25.34	TCP	1502	80 → 36572 [ACK] Seq=1437 Ack=426 Win=30080 Len=1436 TSval=
13	0.343707	192.168.25.34	128.119.245.12	TCP	66	36572 → 80 [ACK] Seq=426 Ack=2873 Win=35672 Len=0 TSval=419
14	0.343932	128.119.245.12	192.168.25.34	HTTP	2055	HTTP/1.1 200 OK (text/html)
15	0.343948	192.168.25.34	128.119.245.12	TCP	66	36572 → 80 [ACK] Seq=426 Ack=4862 Win=39640 Len=0 TSval=419

Frame 14: 2055 bytes on wire (16440 bits), 2055 bytes captured (16440 bits)

Ethernet II, Src: Sagemcom_c1:48:8e (2c:e4:12:c1:48:8e), Dst: AsustekC_8e:a5:c4 (f8:32:e4:8e:a5:c4)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.25.34

Transmission Control Protocol, Src Port: 80, Dst Port: 36572, Seq: 2873, Ack: 426, Len: 1989

[3 Reassembled TCP Segments (4861 bytes): #10(1436), #12(1436), #14(1989)]

[Frame: 10, payload: 0-1435 (1436 bytes)]

[Frame: 12, payload: 1436-2871 (1436 bytes)]

[Frame: 14, payload: 2872-4860 (1989 bytes)]

[Segment count: 3]

[Reassembled TCP Length: 4861]

[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a46174653a2053...]

Hypertext Transfer Protocol

Line-based text data: text/html (98 lines)

0000 48 54 54 56 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK

0010 0a 44 61 74 65 3a 20 53 61 74 2c 20 30 39 20 4d Date: Sat, 09 M

Frame (2055 bytes) Reassembled TCP (4861 bytes)

TCP Segments (tcp.segments), 4861 bytes

Packets: 15 - Displayed: 15 (100.0%) - Marked: 3 (20.0%) Profile: Default

14. O código de status da mensagem GET HTTP é 200 e sua mensagem associada é OK.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.060000	192.168.25.34	128.119.245.12	TCP	74	36570 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
2	0.060238	192.168.25.34	128.119.245.12	TCP	74	36572 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
3	0.171412	128.119.245.12	192.168.25.34	TCP	74	80 → 36572 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1448
4	0.171465	192.168.25.34	128.119.245.12	TCP	66	36572 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=41953363
5	0.171766	192.168.25.34	128.119.245.12	HTTP	491	GET /wireshark-labs/HTTP-wireshark-fil1e3.html HTTP/1.1
6	0.179266	128.119.245.12	192.168.25.34	TCP	74	80 → 36570 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1448
7	0.179329	192.168.25.34	128.119.245.12	TCP	66	36570 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=41953363
8	0.342760	128.119.245.12	192.168.25.34	TCP	66	80 → 36572 [ACK] Seq=1 Ack=426 Win=30080 Len=0 TSval=261292
9	0.343066	128.119.245.12	192.168.25.34	TCP	66	[TCP Dup ACK 8#1] 80 → 36572 [ACK] Seq=1 Ack=426 Win=30080
10	0.343479	128.119.245.12	192.168.25.34	TCP	1502	80 → 36572 [ACK] Seq=1 Ack=426 Win=30080 Len=1436 TSval=261
11	0.343496	192.168.25.34	128.119.245.12	TCP	66	36572 → 80 [ACK] Seq=426 Ack=1437 Win=32128 Len=0 TSval=419
12	0.343693	128.119.245.12	192.168.25.34	TCP	1502	80 → 36572 [ACK] Seq=1437 Ack=426 Win=30080 Len=1436 TSval=
13	0.343707	192.168.25.34	128.119.245.12	TCP	66	36572 → 80 [ACK] Seq=426 Ack=2873 Win=35672 Len=0 TSval=419
14	0.343932	128.119.245.12	192.168.25.34	HTTP	2055	HTTP/1.1 200 OK (text/html)
15	0.343948	192.168.25.34	128.119.245.12	TCP	66	36572 → 80 [ACK] Seq=426 Ack=4862 Win=39640 Len=0 TSval=419

Transmission Control Protocol, Src Port: 80, Dst Port: 36572, Seq: 2873, Ack: 426, Len: 1989

[3 Reassembled TCP Segments (4861 bytes): #10(1436), #12(1436), #14(1989)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Sat, 09 Mar 2019 14:13:20 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n

Last-Modified: Sat, 09 Mar 2019 06:59:01 GMT\r\n

0000 48 54 54 56 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK

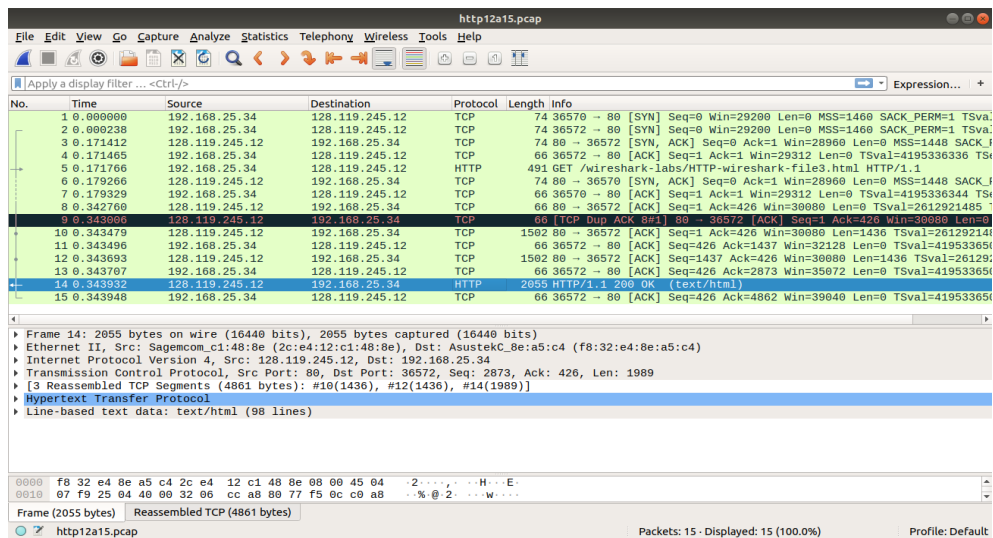
0010 0a 44 61 74 65 3a 20 53 61 74 2c 20 30 39 20 4d Date: Sat, 09 M

Frame (2055 bytes) Reassembled TCP (4861 bytes)

HTTP Response Status Code (http.response.code), 3 bytes

Packets: 15 - Displayed: 15 (100.0%) Profile: Default

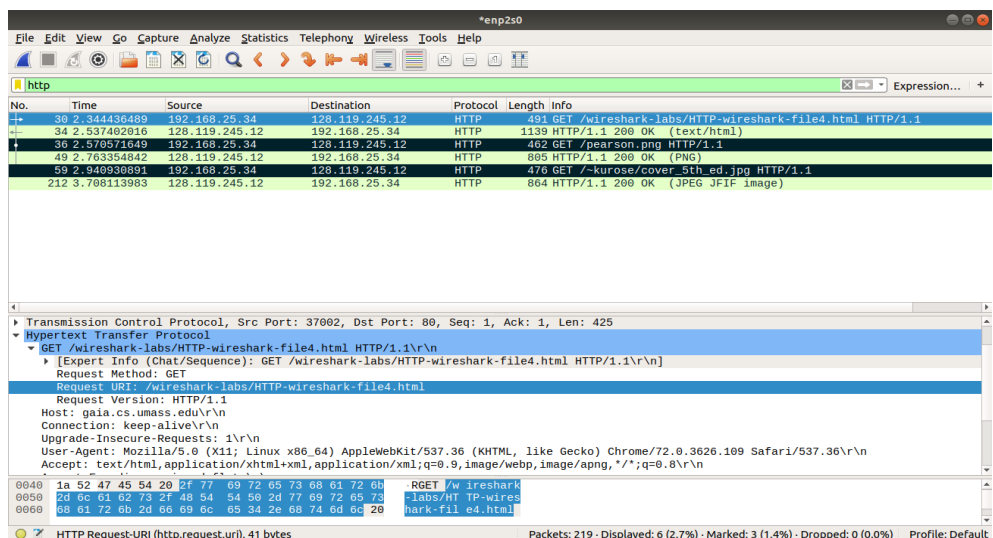
15. Apenas na mensagem de resposta HTTP com o status code 200 (OK).



3.4 Documentos HTML com Objetos Incluídos

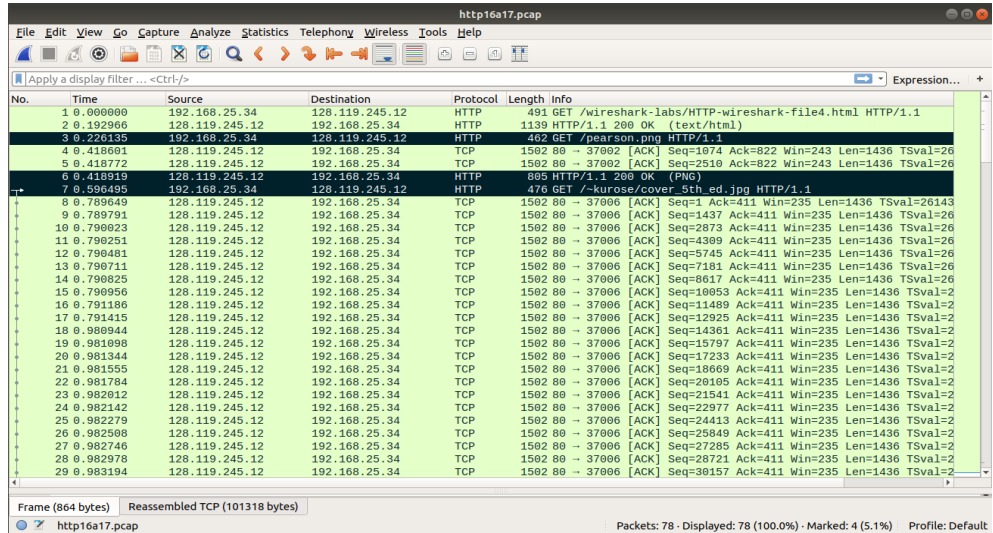
16. Três mensagens GET HTTP foram enviadas pelo meu navegador. Os endereços das mensagens enviadas foram:

- `/wireshark-labs/HTTP-wireshark-file4.html`
- `/pearson.png`
- `/kurose/cover_5th.ed.jpg`



17. As imagens foram baixadas em sequência. Pode-se afirmar isso, pois a mensagem GET HTTP da segunda imagem foi enviada somente depois

da mensagem de resposta da primeira imagem.

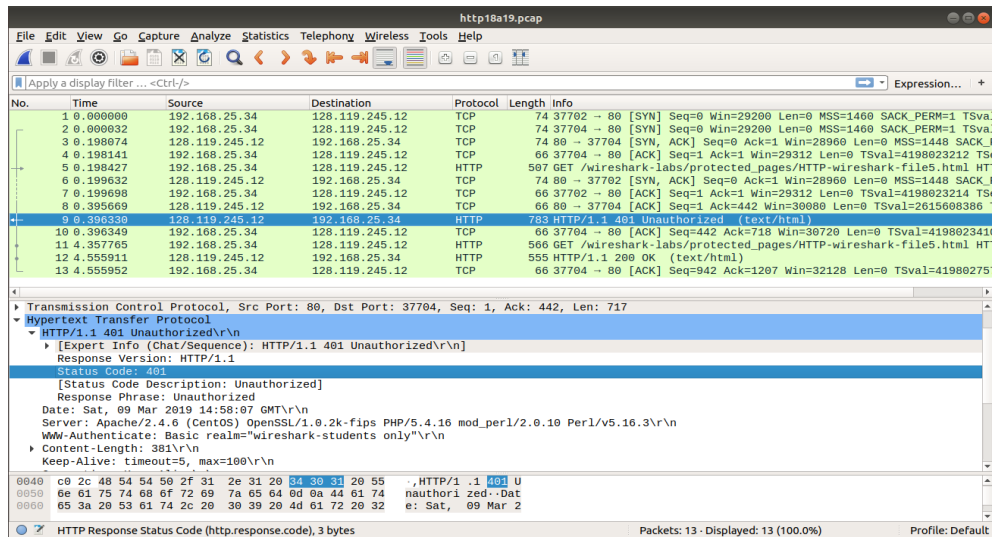


The image shows a Wireshark packet capture of http16a17.pcap. The packet list on the left shows a sequence of packets. Packet 7 is an HTTP GET request for /kurose/cover_5th_ed.jpg. Packet 8 is the corresponding HTTP response, which is a 200 OK status with a Content-Type of image/png. The packet details pane on the right shows the structure of the HTTP response, including the status bar (200 OK) and the response body (PNG image data).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.25.34	128.119.245.12	HTTP	491	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
2	0.192966	128.119.245.12	192.168.25.34	HTTP	1139	HTTP/1.1 200 OK (text/html)
3	0.226135	192.168.25.34	128.119.245.12	HTTP	462	GET /pearson.png HTTP/1.1
4	0.418001	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37002 [ACK] Seq=1074 Ack=822 Win=243 Len=1436 TSval=26
5	0.418772	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37002 [ACK] Seq=2519 Ack=822 Win=243 Len=1436 TSval=26
6	0.418919	128.119.245.12	192.168.25.34	HTTP	805	HTTP/1.1 200 OK (PNG)
7	0.596495	192.168.25.34	128.119.245.12	HTTP	476	GET /kurose/cover_5th_ed.jpg HTTP/1.1
8	0.789649	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=1 Ack=411 Win=235 Len=1436 TSval=26143
9	0.789791	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=1437 Ack=411 Win=235 Len=1436 TSval=26
10	0.790023	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=2873 Ack=411 Win=235 Len=1436 TSval=26
11	0.790251	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=4309 Ack=411 Win=235 Len=1436 TSval=26
12	0.790481	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=5745 Ack=411 Win=235 Len=1436 TSval=26
13	0.790711	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=7181 Ack=411 Win=235 Len=1436 TSval=26
14	0.790825	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=8617 Ack=411 Win=235 Len=1436 TSval=26
15	0.790956	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=10053 Ack=411 Win=235 Len=1436 TSval=26
16	0.791186	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=11489 Ack=411 Win=235 Len=1436 TSval=26
17	0.791415	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=12925 Ack=411 Win=235 Len=1436 TSval=26
18	0.980944	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=14361 Ack=411 Win=235 Len=1436 TSval=26
19	0.981098	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=15797 Ack=411 Win=235 Len=1436 TSval=26
20	0.981344	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=17233 Ack=411 Win=235 Len=1436 TSval=26
21	0.981555	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=18669 Ack=411 Win=235 Len=1436 TSval=26
22	0.981784	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=20105 Ack=411 Win=235 Len=1436 TSval=26
23	0.982012	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=21541 Ack=411 Win=235 Len=1436 TSval=26
24	0.982142	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=22977 Ack=411 Win=235 Len=1436 TSval=26
25	0.982279	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=24413 Ack=411 Win=235 Len=1436 TSval=26
26	0.982508	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=25849 Ack=411 Win=235 Len=1436 TSval=26
27	0.982746	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=27285 Ack=411 Win=235 Len=1436 TSval=26
28	0.982978	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=28721 Ack=411 Win=235 Len=1436 TSval=26
29	0.983194	128.119.245.12	192.168.25.34	TCP	1502	80 -> 37006 [ACK] Seq=30157 Ack=411 Win=235 Len=1436 TSval=26

3.5 Autenticação HTTP

18. O código de status da mensagem GET HTTP é 401 e sua mensagem associada é Unauthorized.



The image shows a Wireshark packet capture of http18a19.pcap. The packet list on the left shows a sequence of packets. Packet 9 is an HTTP GET request for /protected_pages/HTTP-wireshark-file5.html. Packet 10 is the corresponding HTTP response, which is a 401 Unauthorized status. The packet details pane on the right shows the structure of the HTTP response, including the status bar (401 Unauthorized) and the response body (text/html). The status code description is 'Unauthorized' and the response phrase is 'Unauthorized'.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.25.34	128.119.245.12	TCP	74	37702 -> 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSva
2	0.000032	192.168.25.34	128.119.245.12	TCP	74	37704 -> 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSva
3	0.198074	128.119.245.12	192.168.25.34	TCP	74	80 -> 37704 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1448 SACK_I
4	0.198141	192.168.25.34	128.119.245.12	TCP	66	37704 -> 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4198023212 TS
5	0.198427	192.168.25.34	128.119.245.12	HTTP	507	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HT
6	0.198632	128.119.245.12	192.168.25.34	TCP	74	80 -> 37702 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1448 SACK_I
7	0.198698	192.168.25.34	128.119.245.12	TCP	66	37702 -> 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4198023214 TS
8	0.395669	128.119.245.12	192.168.25.34	TCP	66	80 -> 37704 [ACK] Seq=1 Ack=442 Win=30680 Len=0 TSval=2615608386
9	0.396330	128.119.245.12	192.168.25.34	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
10	0.396349	192.168.25.34	128.119.245.12	TCP	66	37704 -> 80 [ACK] Seq=442 Ack=718 Win=30720 Len=0 TSval=419802341
11	4.357765	192.168.25.34	128.119.245.12	HTTP	506	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HT
12	4.555911	128.119.245.12	192.168.25.34	HTTP	555	HTTP/1.1 200 OK (text/html)
13	4.555952	128.119.245.12	128.119.245.12	TCP	66	37704 -> 80 [ACK] Seq=942 Ack=1207 Win=32128 Len=0 TSval=41980275

19. É incluído o campo Authorization.

http18a19.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.25.34	128.119.245.12	TCP	74	37702 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
2	0.000032	192.168.25.34	128.119.245.12	TCP	74	37704 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=...
3	0.190074	128.119.245.12	192.168.25.34	TCP	74	80 → 37704 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1448 SACK_I...
4	0.198141	192.168.25.34	128.119.245.12	TCP	66	37704 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4198023212 TS...
5	0.198427	192.168.25.34	128.119.245.12	HTTP	507	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HT...
6	0.199632	128.119.245.12	192.168.25.34	TCP	74	80 → 37702 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1448 SACK_I...
7	0.199698	192.168.25.34	128.119.245.12	TCP	66	37702 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4198023214 TS...
8	0.395069	128.119.245.12	192.168.25.34	TCP	66	80 → 37704 [ACK] Seq=1 Ack=442 Win=30080 Len=0 TSval=2615608386 TS...
9	0.396330	128.119.245.12	192.168.25.34	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
10	0.396349	192.168.25.34	128.119.245.12	TCP	66	37704 → 80 [ACK] Seq=442 Ack=718 Win=30720 Len=0 TSval=4198023410 TS...
11	4.357765	192.168.25.34	128.119.245.12	HTTP	566	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HT...
12	4.555911	128.119.245.12	192.168.25.34	HTTP	555	HTTP/1.1 200 OK (text/html)
13	4.555952	192.168.25.34	128.119.245.12	TCP	66	37704 → 80 [ACK] Seq=942 Ack=1207 Win=32128 Len=0 TSval=41980275...

Transmission Control Protocol, Src Port: 37704, Dst Port: 80, Seq: 442, Ack: 718, Len: 500

Hypertext Transfer Protocol

GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm9z\r\n

Credentials: wireshark-students:network

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9,pt;q=0.8\r\n

\r\n

00b0 65 65 70 2d 61 6c 69 76 65 0d 0a 41 75 74 68 6f eep-aliv e...Autho

00c0 72 69 7a 61 74 69 6f 6e 53f20 42 61 75 69 63 26 f2zation: Basic

00d0 64 32 6c 79 5a 58 4e 6f 59 58 4a 72 4c 58 4e 38 d2lyZXNo YXJrLXN0

HTTP Authorization header (http.authorization), 59 bytes

Packets: 13 - Displayed: 13 (100.0%)

Profile: Default