



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Instituto de Ciências Exatas e de Informática

Trabalho de Redes de Computadores 2 - Wireshark*

Luiz Gustavo Bragança dos Santos¹

*Artigo apresentado ao Instituto de Ciências Exatas e Informática da Pontifícia Universidade Católica de Minas Gerais como pré-requisito para obtenção do título de Bacharel em Ciência da Computação.

¹Aluno, Ciência da Computação, Brasil, luiz.braganca@sga.pucminas.br.

Sumário

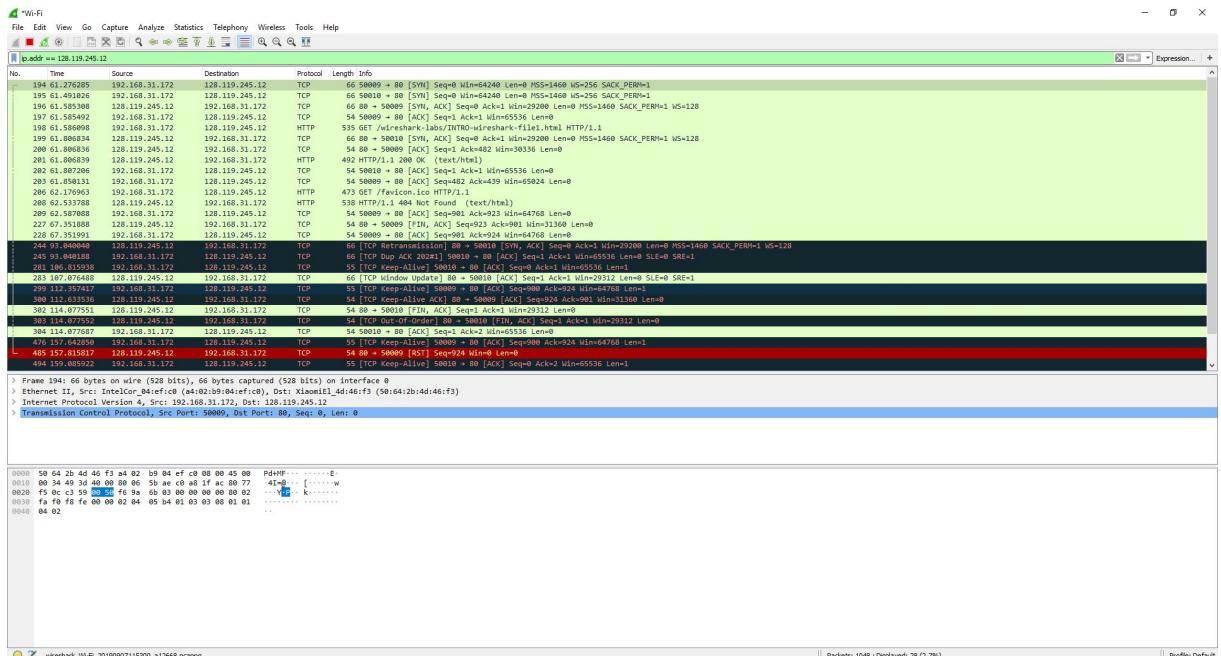
Lista de Figuras	2
1 Introdução	3
2 DNS	4
2.1 nslookup	4
2.2 Rastreando DNS com o Wireshark	6
2.3 Rastreamento Wireshark com nslookup	7
2.4 Rastreamento Wireshark com nslookup e type=NS	8
2.5 Rastreamento Wireshark com nslookup e DNS ns.pucminas.br	9
3 HTTP	10
3.1 A Interação Básica GET/Resposta do HTTP	10
3.2 A Interação HTTP GET Condisional/Resposta	11
3.3 Baixando Documentos Longos	13
3.4 Documentos HTML com Objetos Incluídos	15
3.5 Autenticação HTTP	16

Lista de Figuras

1 INTRODUÇÃO

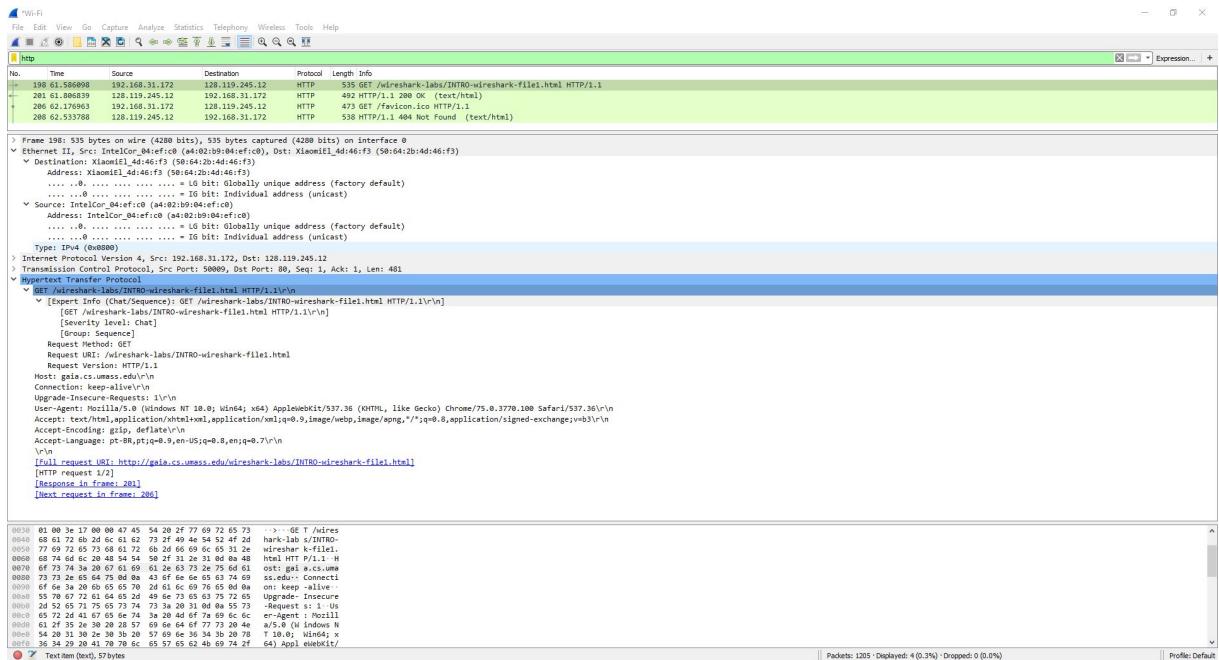
a) Protocolos encontrados:

- Transfer Control Protocol (TCP)
- HyperText Transfer Protocol (HTTP)



b) O tempo de envio da mensagem HTTP GET foi de 12:18:33,451975 e o de OK foi de 12:18:33,770331. Então o tempo passado foi de 0,318356 segundos.

c) O endereço IP do site gaia.cs.umass.edu é: 128.119.245.12, e o endereço IP da interface de rede do meu computador é: 192.168.31.172.



2 DNS

2.1 nslookup

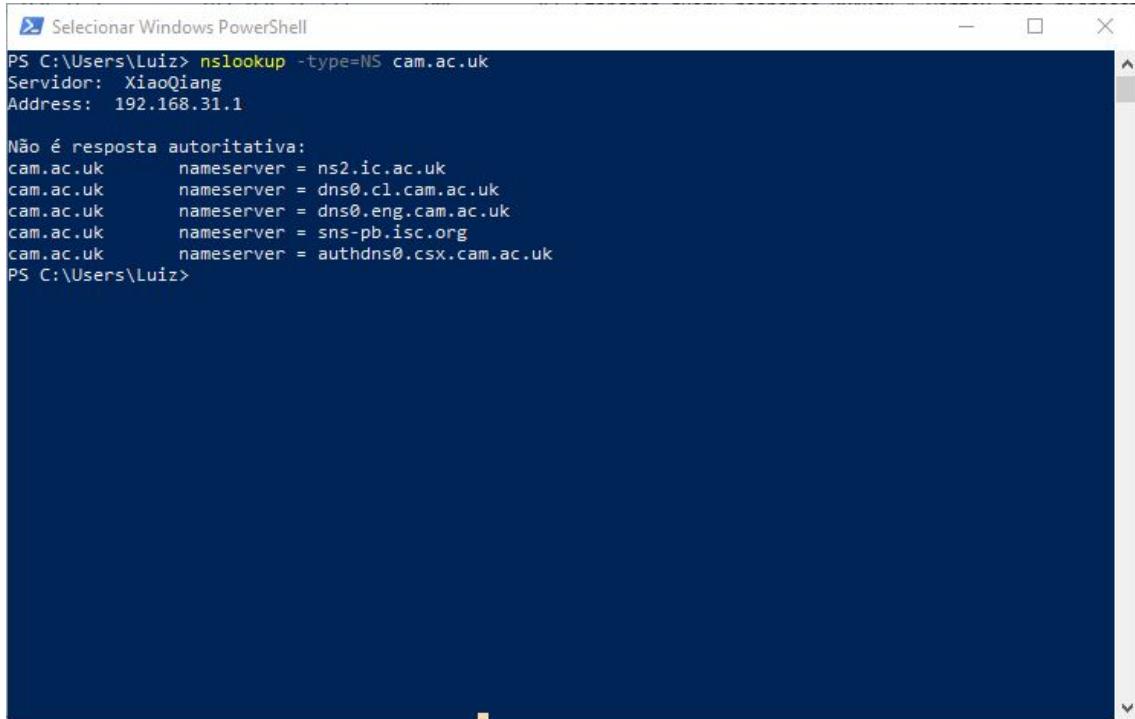
a) "nslookup www.nintendo.co.jp", Endereço IP: 104.78.52.223.

```
Windows PowerShell
PS C:\Users\Luiz> nslookup www.nintendo.co.jp
Servidor: XiaoQiang
Address: 192.168.31.1

Não é resposta autoritativa:
Nome:   e5192.b.akamaiedge.net
Address: 104.78.52.223
Aliases: www.nintendo.co.jp
         www.nintendo.co.jp.edgekey.net

PS C:\Users\Luiz>
```

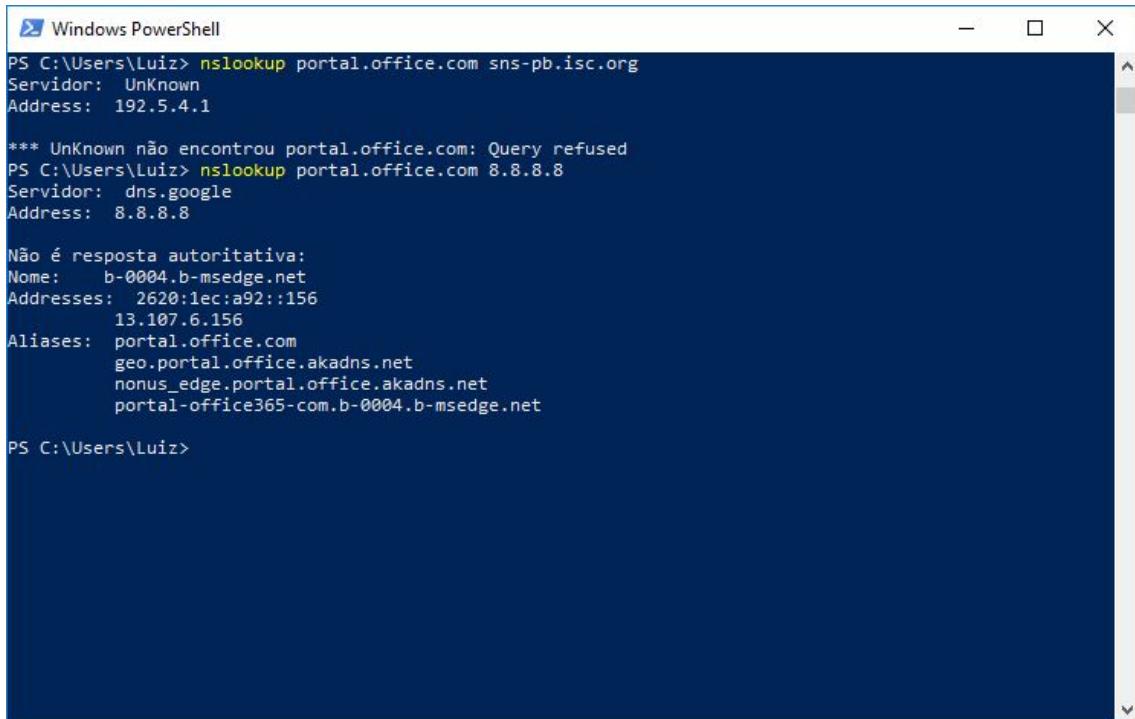
b) "nslookup -type=NS cam.ac.uk"



```
PS C:\Users\Luiz> nslookup -type=NS cam.ac.uk
Servidor: XiaoQiang
Address: 192.168.31.1

Não é resposta autoritativa:
cam.ac.uk      nameserver = ns2.ic.ac.uk
cam.ac.uk      nameserver = dns0.cl.cam.ac.uk
cam.ac.uk      nameserver = dns0.eng.cam.ac.uk
cam.ac.uk      nameserver = sns-pb.isc.org
cam.ac.uk      nameserver = authdns0.csx.cam.ac.uk
PS C:\Users\Luiz>
```

c) "nslookup portal.office.com sns-pb.isc.org", Endereço IP: 13.107.6.156



```
PS C:\Users\Luiz> nslookup portal.office.com sns-pb.isc.org
Servidor: Unknown
Address: 192.5.4.1

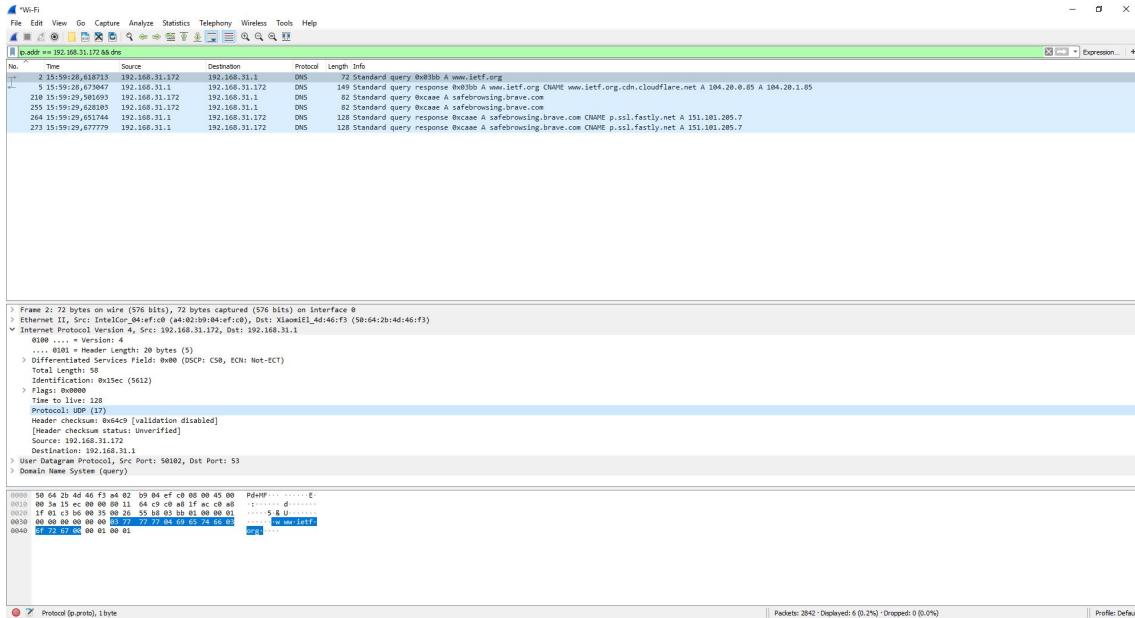
*** Unknown não encontrou portal.office.com: Query refused
PS C:\Users\Luiz> nslookup portal.office.com 8.8.8.8
Servidor: dns.google
Address: 8.8.8.8

Não é resposta autoritativa:
Nome: b-0004.b-msedge.net
Addresses: 2620:1ec:a92::156
          13.107.6.156
Aliases: portal.office.com
          geo.portal.office.akadns.net
          nonus_edge.portal.office.akadns.net
          portal-office365-com.b-0004.b-msedge.net

PS C:\Users\Luiz>
```

2.2 Rastreando DNS com o Wireshark

a) Mensagens de solicitação enviadas com UDP



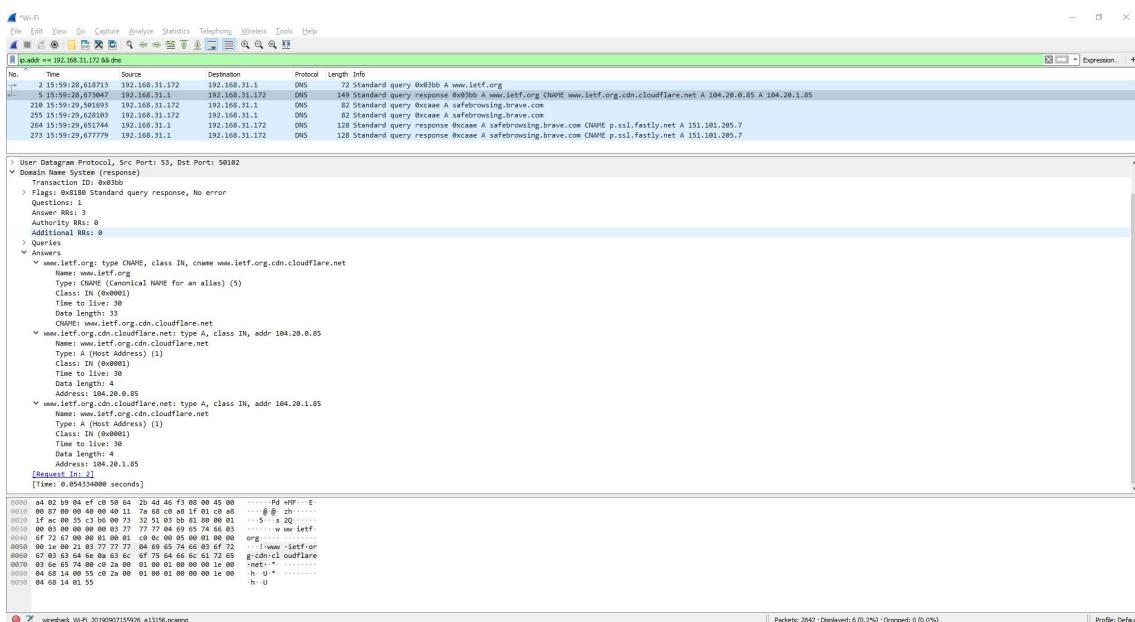
b) Porta origem: 50102 e Porta destino: 53

c) O endereço IP com o qual a mensagem de consulta DNS é enviada, é: 192.168.31.172.

Sim, são os mesmos endereços.

d) O campo Type da mensagem, diz que o DNS é do tipo A, e a mensagem não consta nenhum campo "answer".

e) Há 3 campos "answer"na resposta DNS:



f) Não, o IP de destino não corresponde ao endereço de IP fornecido na mensagem de resposta DNS anterior.

g) Sim, a página web contém imagens, mas nenhuma consulta DNS é realizada para recuperar as imagens do site.

2.3 Rastreamento Wireshark com nslookup

1 Utilizando o comando: "nslookup www.mit.edu"

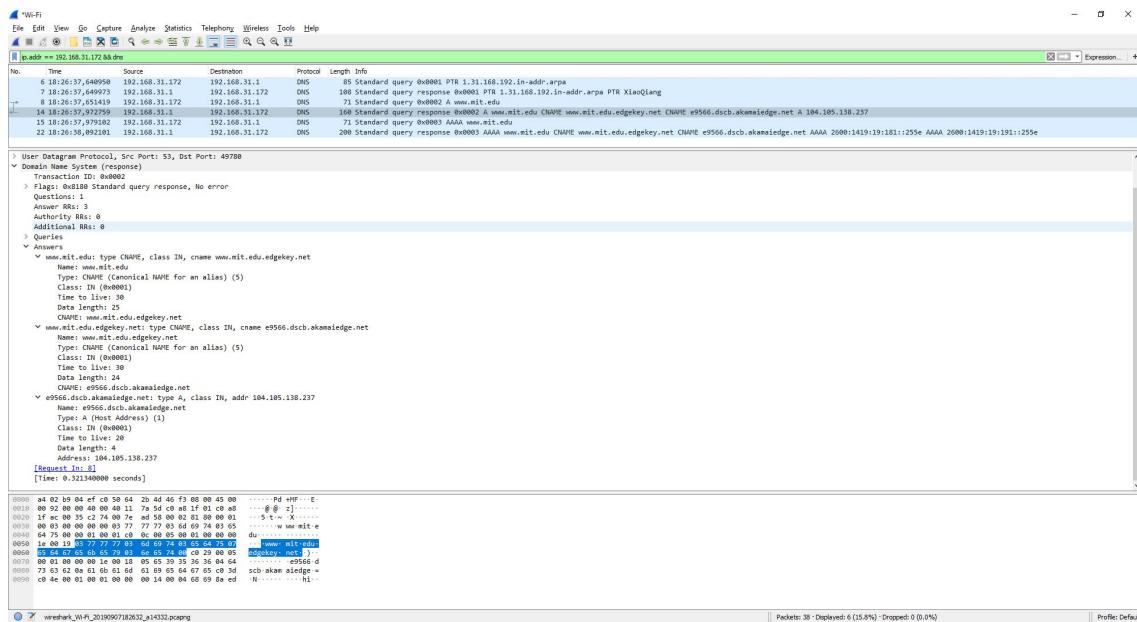
- a) Porta destino: 53, Porta Origem: 49780
- b) A Mensagem de consulta DNS está endereçada ao IP: 192.168.31.1, que é o mesmo IP do servidor DNS local.

c) O campo Type da mensagem, diz que o DNS é do tipo A, e a mensagem de consulta não possui campo "answer".

d) Há 3 campos de "answer", com as seguintes informações:

- Name
- Type
- Class
- Time to live
- Data length

Podemos observar que nas duas primeiras, há o campo CNAME e na última há o campo Address.



2.4 Rastreamento Wireshark com nslookup e type=NS

1 Utilizando o comando: "nslookup -type=NS mit.edu"

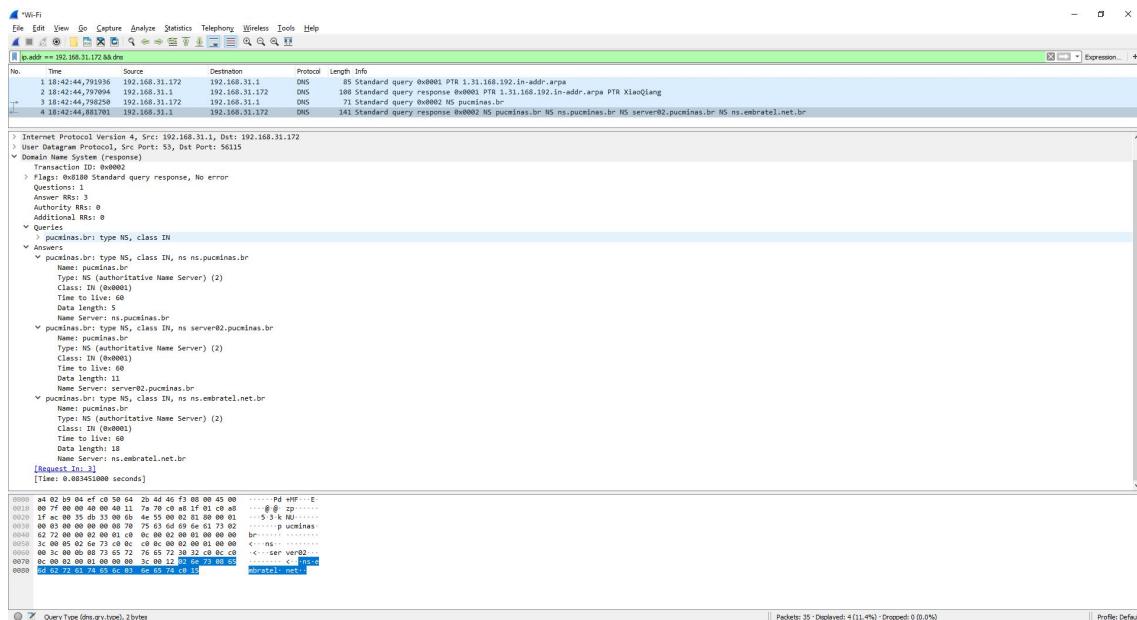
a) A Mensagem de consulta DNS está endereçada ao IP: 192.168.31.1, que é o mesmo IP do servidor DNS local.

b) O campo Type da mensagem, diz que o DNS é do tipo NS, e a não possui nenhum campo de "answer".

c) Os servidores DNS da PUC Minas que foram fornecidos na resposta são:

- ns.pucminas.br
- server02.pucminas.br
- ns.embratel.net.br

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



2.5 Rastreamento Wireshark com nslookup e DNS ns.pucminas.br

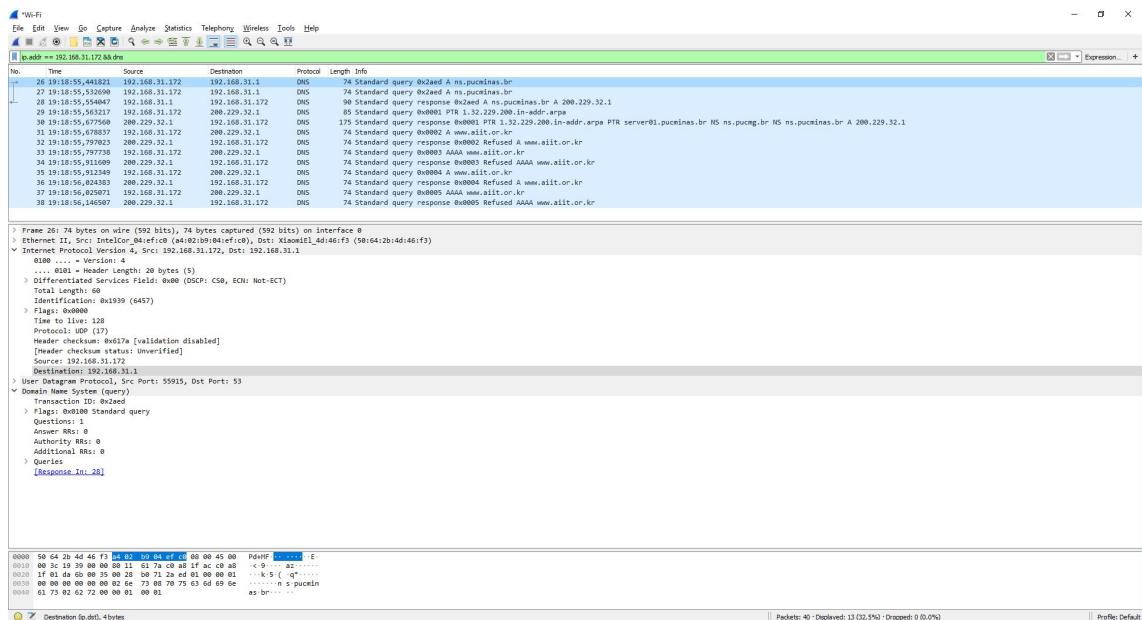
1 Utilizando o comando: "[nslookup www.aiit.or.kr ns.pucminas.br](http://www.aiit.or.kr/ns.pucminas.br)"

a) A Mensagem de consulta DNS está endereçada ao IP: 192.168.31.1, que é o mesmo IP do servidor DNS local.

b) O campo Type da mensagem, diz que o DNS é do tipo A, e a não possui nenhum campo de "answer".

c) Possui apenas 1 campo "answer" com as seguintes informações:

- Name
- Type
- Class
- Time to live
- Data length
- Address



3 HTTP

3.1 A Interação Básica GET/Resposta do HTTP

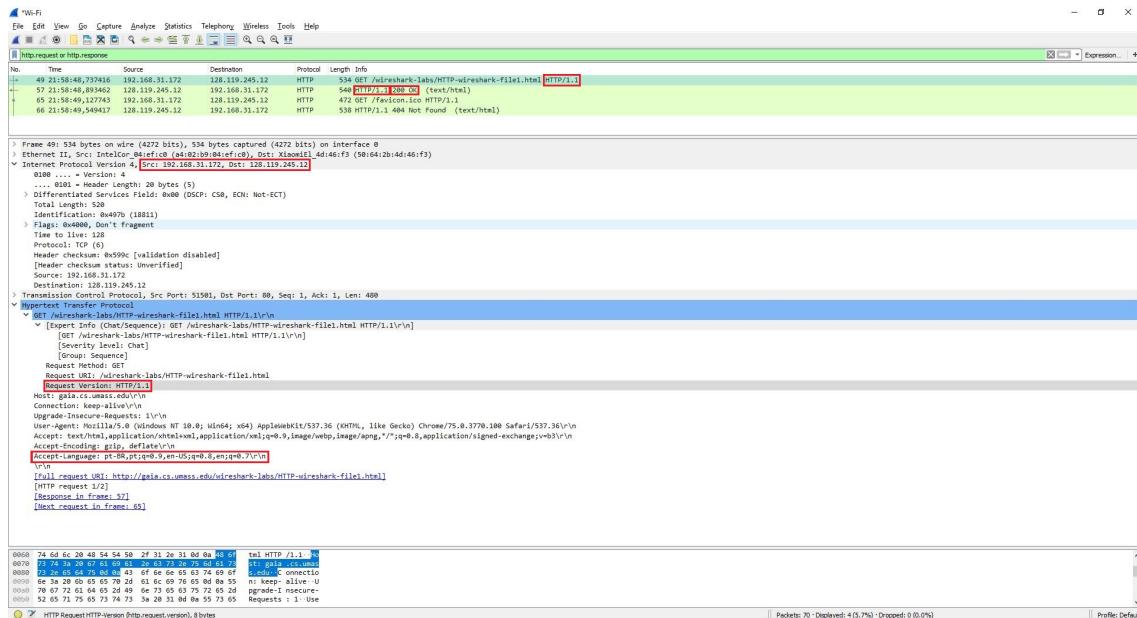
a) O meu navegador e o servidor executam a versão 1.1 do HTTP.

b) As linguagens que o meu navegador pode aceitar do servidor são:

- português (pt-br)
- inglês americano (en-US)
- inglês britânico (en)

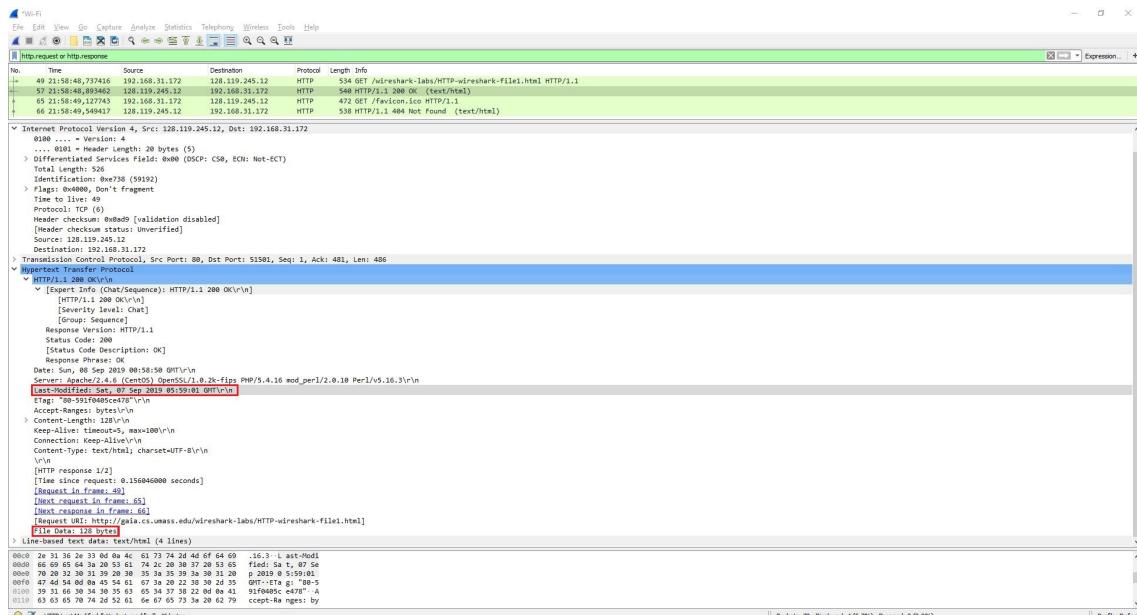
c) O meu IP é: 192.168.31.172 e o do servidor é: 128.119.245.12.

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



e) A última vez que o arquivo foi modificado no servidor foi no dia 07 de Setembro de 2019 às 05:59:01.

f) Foram retornados 128 bytes de conteúdo.

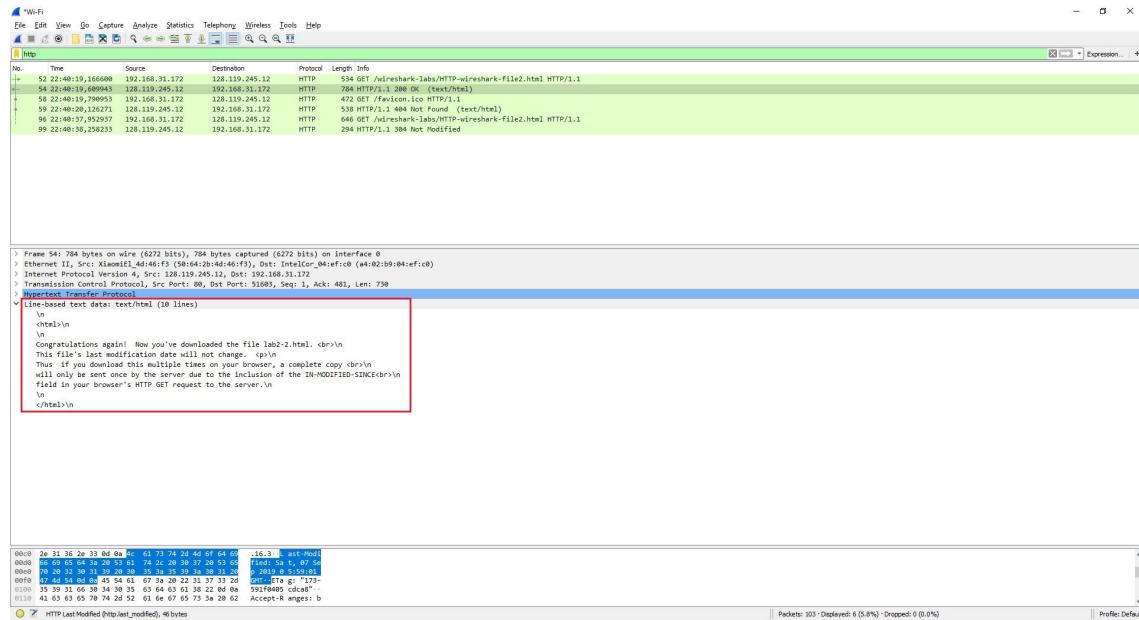


g) Nenhum cabeçalho foi encontrado dentro da janela de conteúdo do pacote.

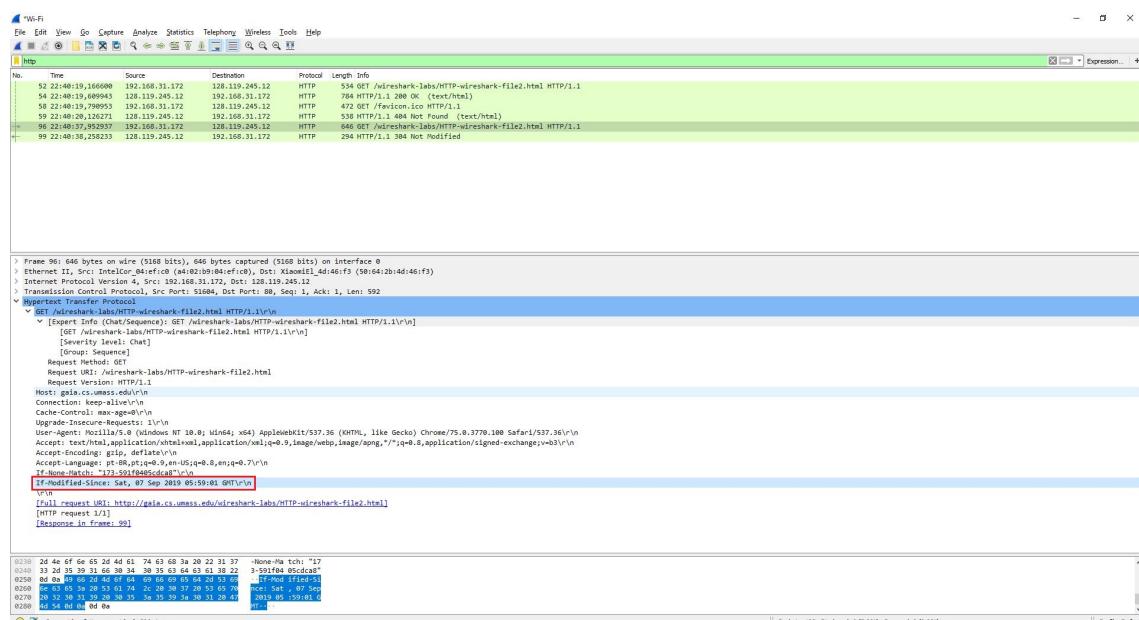
3.2 A Interação HTTP GET Condisional/Resposta

a) Não existe a linha IF-MODIFIED-SINCE na janela de conteúdo do pacote da primeira mensagem GET HTTP.

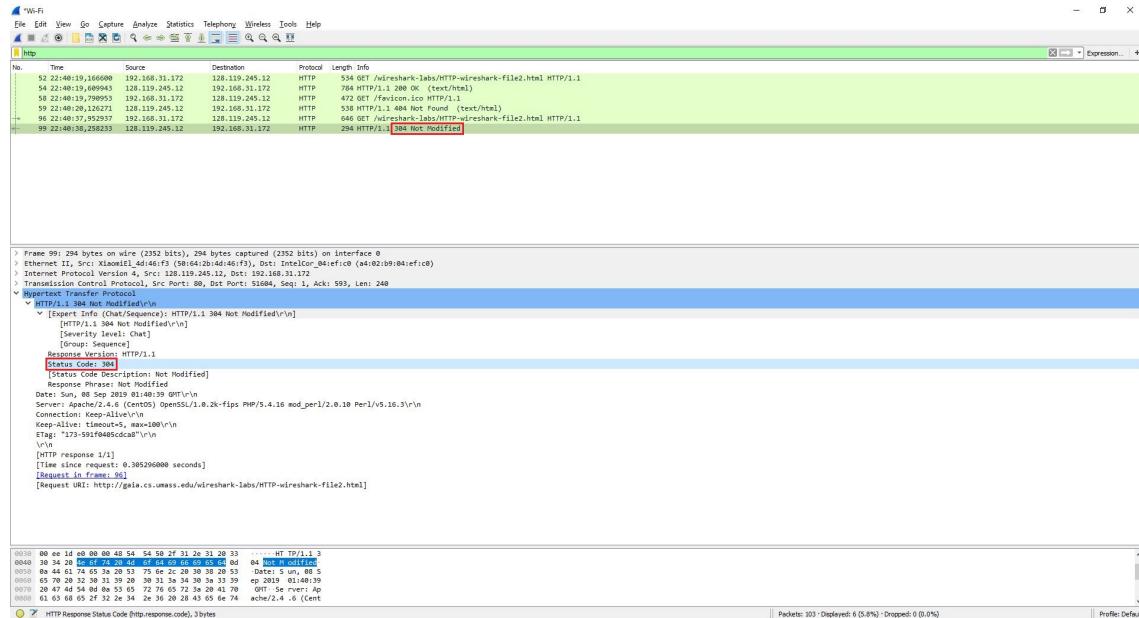
b) Sim, o servidor retornou explicitamente o conteúdo do arquivo.



c) Sim, na segunda mensagem HTTP, possui a linha IF-MODIFIED-SINCE, e o seu conteúdo é a data que estava no Last-Modified da última mensagem HTTP GET.

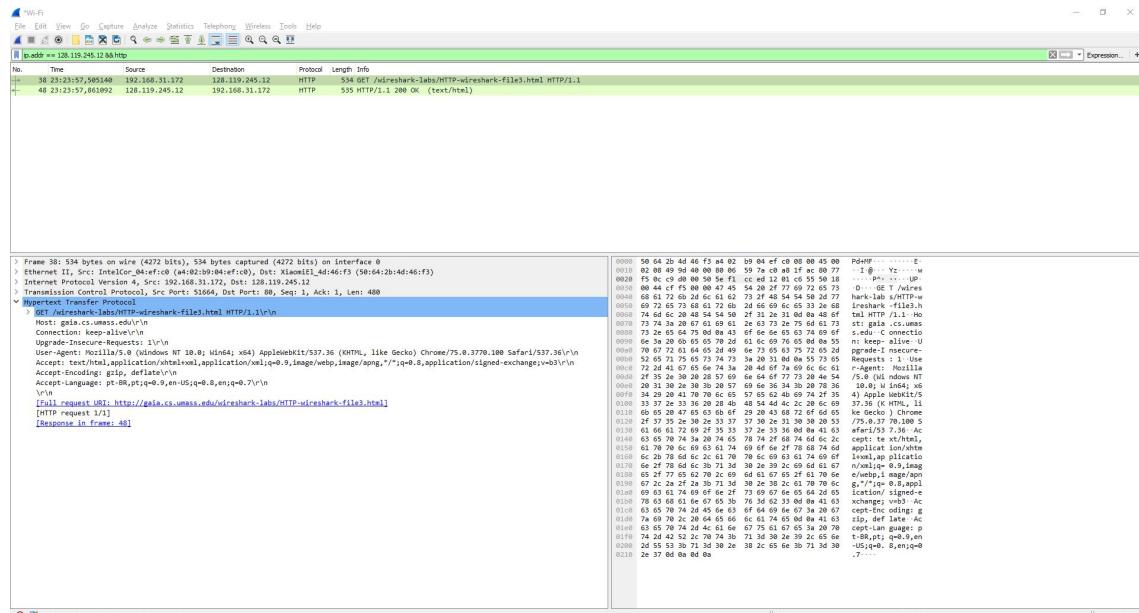


d) O código de status na resposta é o 304, e sua mensagem é de Not Modified, e o servidor não retornou explicitamente o conteúdo do arquivo, pois já constava no cache do navegador sem modificações.

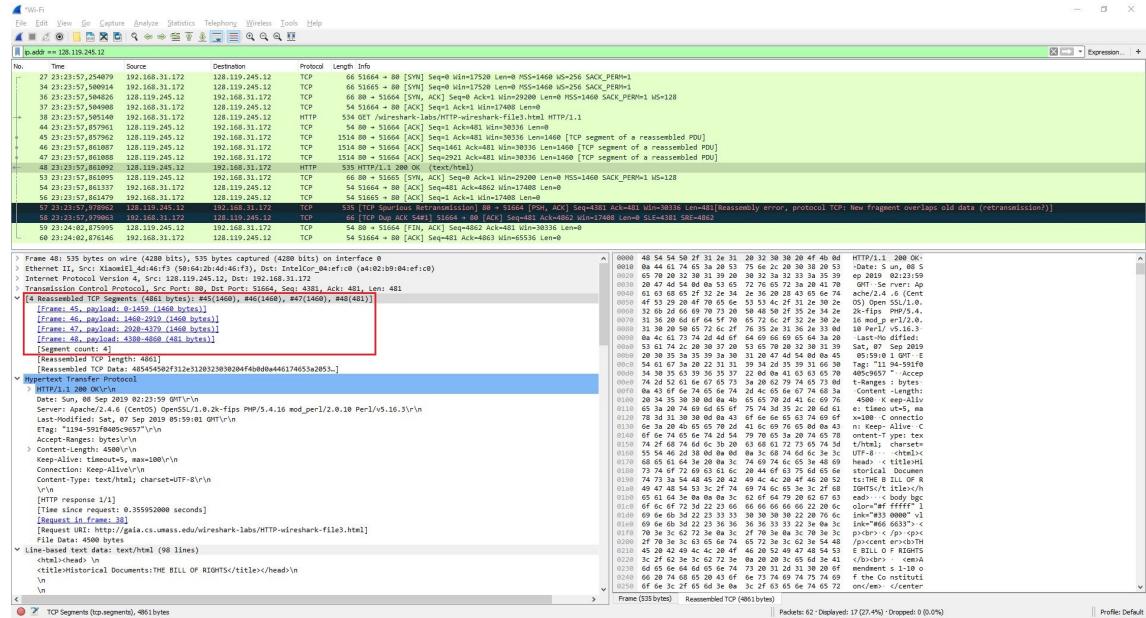


3.3 Baixando Documentos Longos

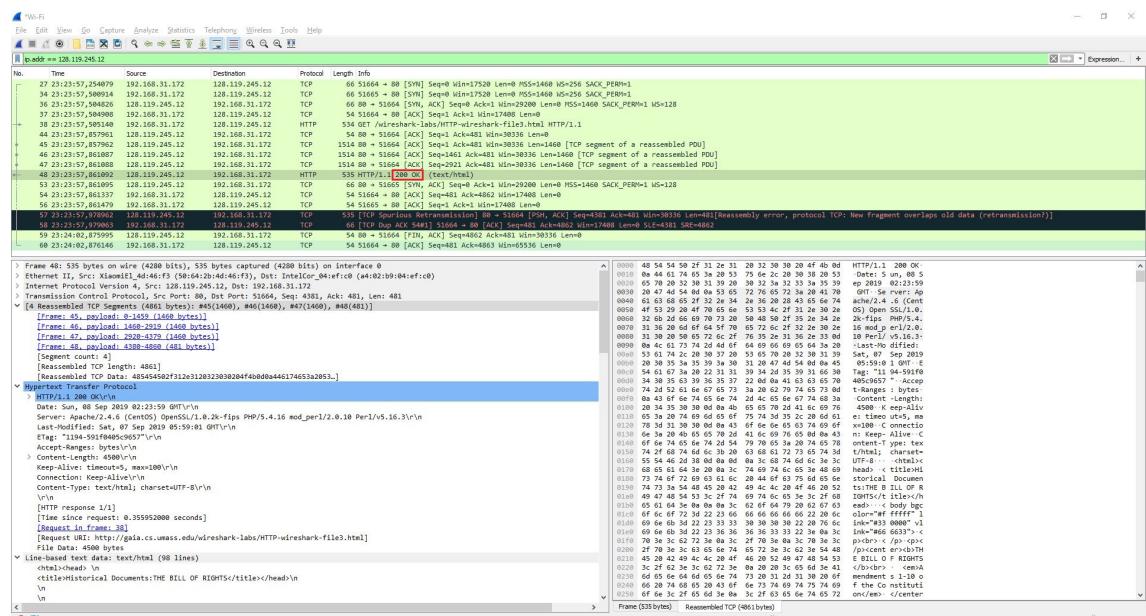
a) Apenas 1 mensagem HTTP GET foi enviada pelo meu navegador.



b) Foram necessários 4 segmentos TCP para carregar a resposta.



c) O Código de status associada com a resposta à mensagem HTTP GET é o 200 e sua mensagem é OK.

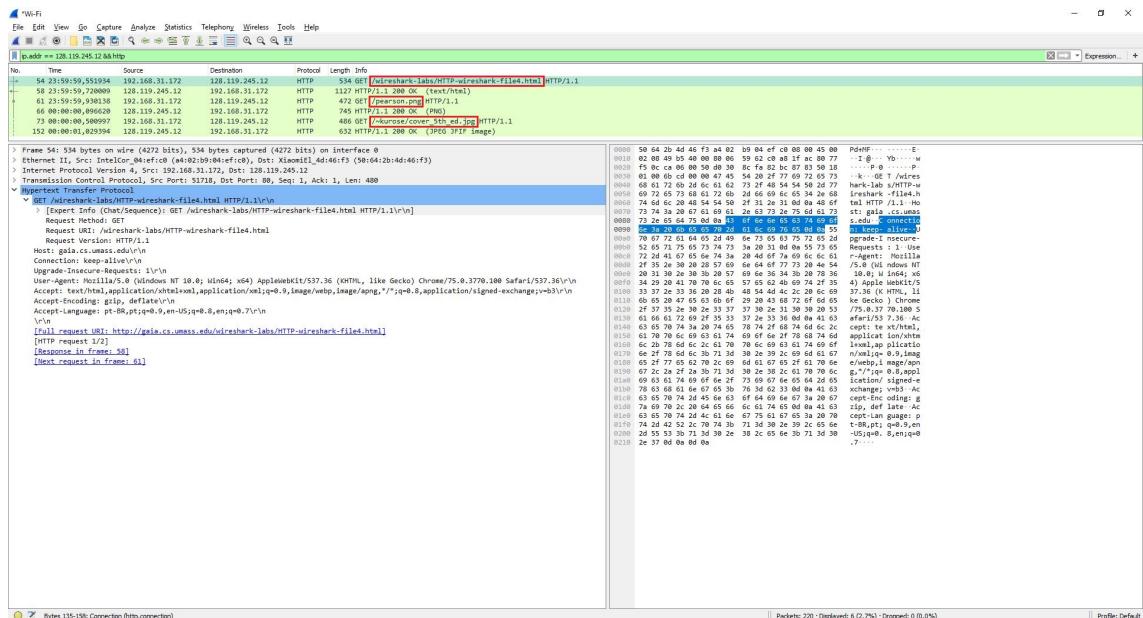


d) Apenas na mensagem de resposta HTTP com o status 200 OK.

3.4 Documentos HTML com Objetos Incluídos

a) Foram enviadas 3 mensagens HTTP GET pelo meu navegador, para os seguintes endereços:

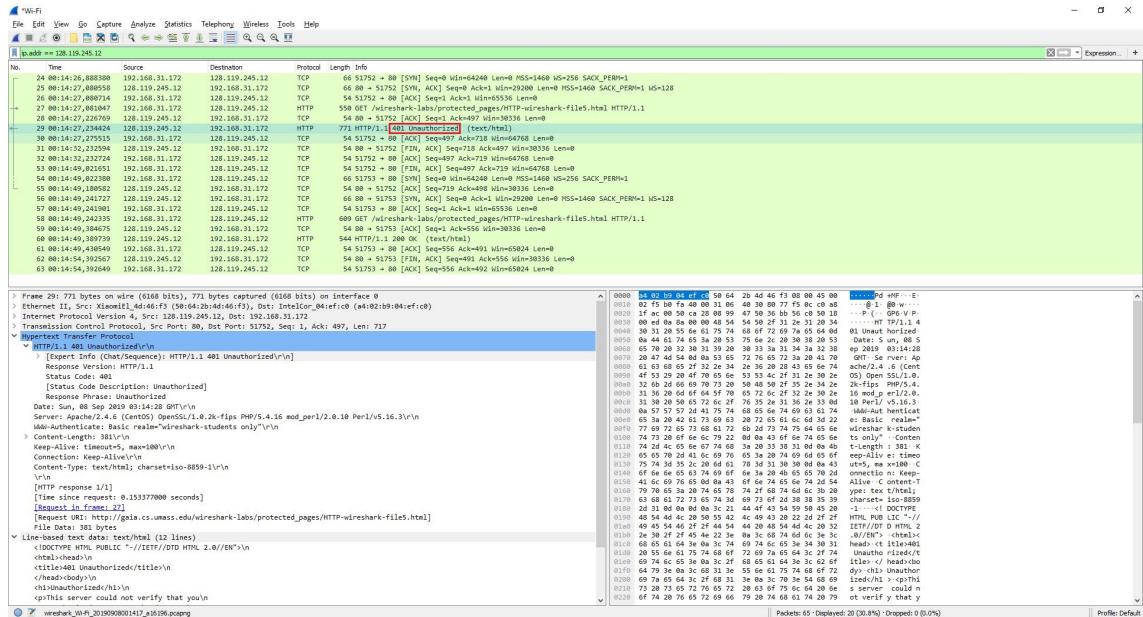
- /wireshark-labs/HTTP-wireshark-file4.html
- /pearson.png
- /kurose/cover_5th_ed.jpg



b) Foram baixadas em sequência, pois o navegador esperou a resposta 200 OK.

3.5 Autenticação HTTP

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



b) O novo campo adicionado na mensagem é o Authorization.

