



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

Redes de Computadores  
*Trabalho Prático II - Wireshark\**

Gabriel Luciano Gomes<sup>1</sup>

---

\*Trabalho prático II - Análise de pacotes DNS e HTTP utilizando Wireshark

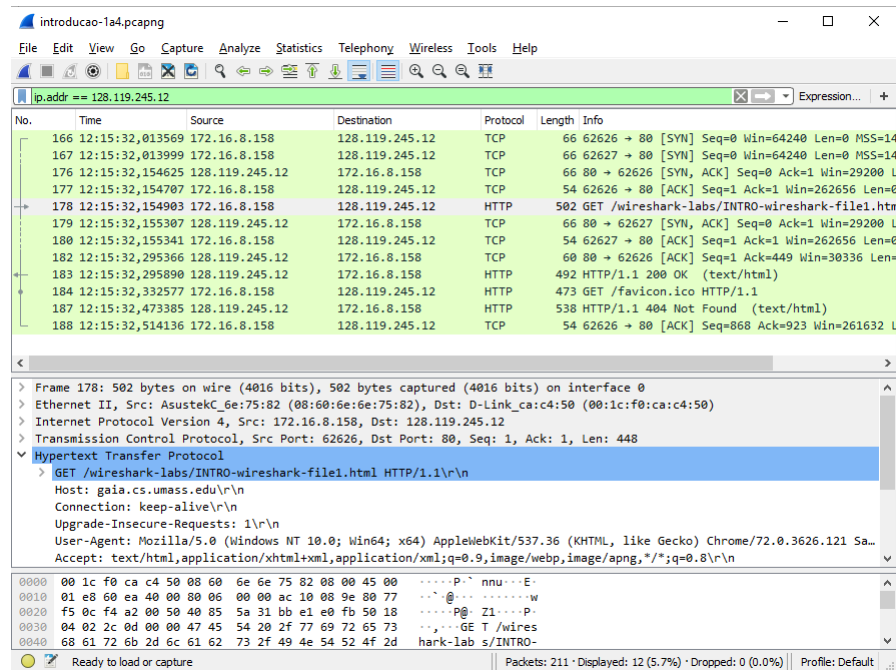
<sup>1</sup>Aluno, Ciência da Computação, Brasil, glgomes@sga.pucminas.br.

**Sumário**

<b>1</b>	<b>Respostas Introdução - Utilizando Roteiro v1.2</b>	<b>3</b>
<b>2</b>	<b>Respostas DNS - Utilizando Roteiro v1.1</b>	<b>4</b>
<b>3</b>	<b>Respostas HTTP - Utilizando Roteiro v1.2</b>	<b>8</b>

**1 RESPOSTAS INTRODUÇÃO - UTILIZANDO ROTEIRO V1.2**

1. Protocolos TPC e HTTP
2. 140 milisegundos
3. IP Gaia: 128.119.245.12, IP Rede: 172.16.8.158

**Figura 1 – Captura de pacotes com MAC Address**

**2 RESPOSTAS DNS - UTILIZANDO ROTEIRO V1.1****1. nslookup**

- (a) Site: nintendo.co.jp, servidor IP: 96.6.213.39
- (b) Universidade de Cambridge, servidores autoritários:
- sns-pb.isc.org
  - dns0.eng.cam.ac.uk
  - authdns0.csx.cam.ac.uk
  - ns2.ic.ac.uk
  - dns0.cl.cam.ac.uk
  - sns-pb.isc.org
- (c) Os DNS da Universidade de Cambridge não realizam pesquisas externas, entretanto ao pesquisar com o DNS do google o IP é 69.147.82.61

```

root@DESKTOP-LUSMCS:~# nslookup www.yahoo.com sns-pb.isc.org
Server:      sns-pb.isc.org
Address:     192.5.4.1953
* server can't find www.yahoo.com: REFUSED

root@DESKTOP-LUSMCS:~# nslookup mail.yahoo.com dns0.cl.cam.ac.uk
Server:      dns0.cl.cam.ac.uk
Address:     128.232.0.19#53
* server can't find mail.yahoo.com: REFUSED

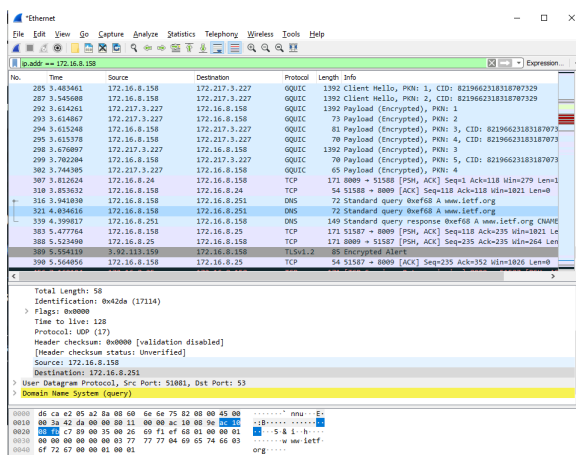
root@DESKTOP-LUSMCS:~# nslookup mail.yahoo.com 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
mail.yahoo.com canonical name = fd-geoycpi-uno.gycpi.b.yahoodns.net.
Name:      fd-geoycpi-uno.gycpi.b.yahoodns.net
Address:   69.147.82.61
Name:      fd-geoycpi-uno.gycpi.b.yahoodns.net
Address:   2081:4998:1c:800::1001
Name:      fd-geoycpi-uno.gycpi.b.yahoodns.net
Address:   2081:4998:1c:800::1000
root@DESKTOP-LUSMCS:~#

```

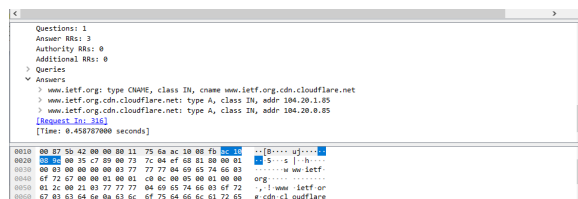
**Figura 2 – Resposta Pesquisa IP utilizando DNS Cambridge****2. Rastreamento DNS com Wireshark**

- (a) Mensagens de solicitação enviadas com UDP

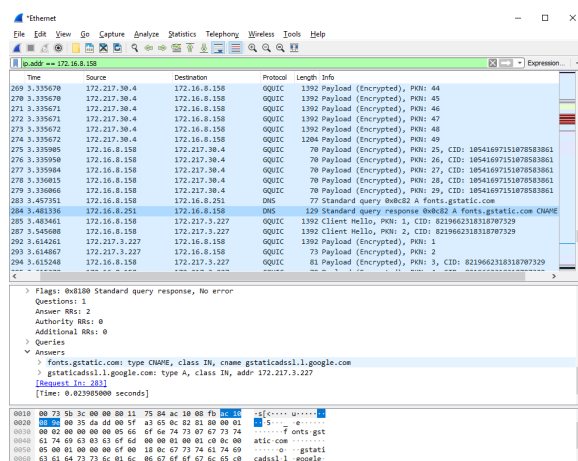
**Figura 3 – Mensagens de Solicitação**

- (b) Porta origem: 51081, porta destino: 53

- (c) IP: 172.16.8.251. Sim, são os mesmos endereços
- (d) Type A. Não possui mensagem "answer".
- (e) Existem 3 campos Answer na resposta DNS

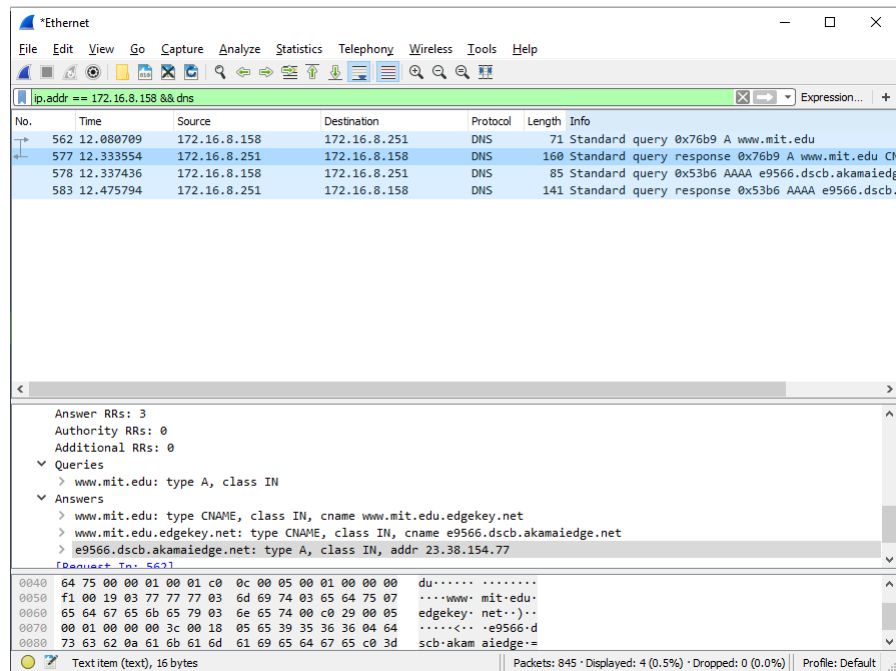
**Figura 4 – Campos Answer**

- (f) Não, o IP é diferente.
- (g) Não, as informações são enviadas diretamente.

**Figura 5 – Envio de informações**

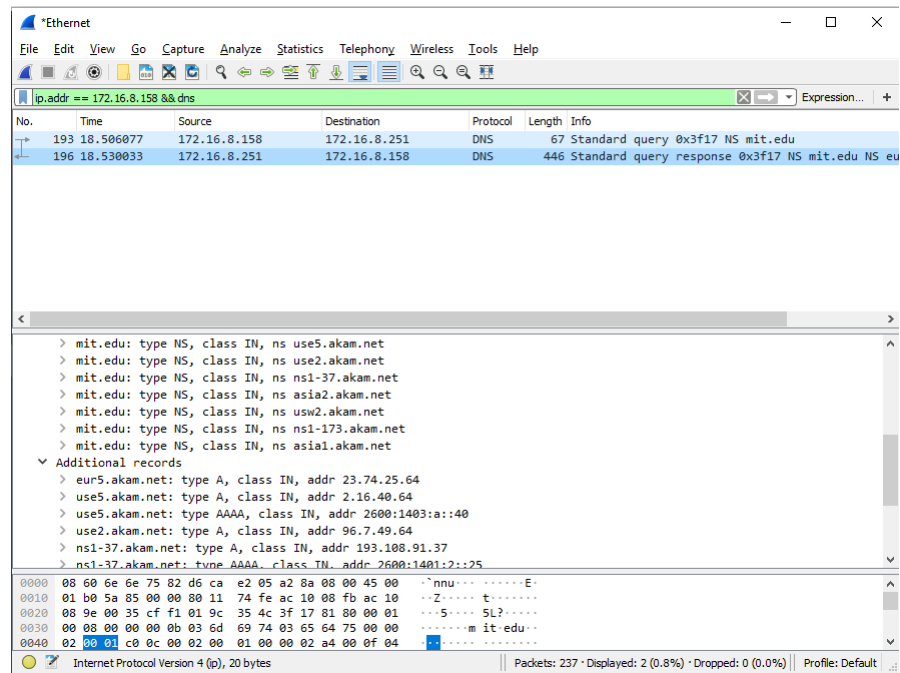
### 3. Rastreamento Wireshark com nslookup

- (a) Porta Destino: 53, Porta Origem: 49263
- (b) 172.16.8.251. Sim, é um dos meus DNS locais.
- (c) Type A, sem mensagens no campo "answer".
- (d) Existem 3 mensagens no campo "answer". Nela se encontram os servidores DNS do site consultado.

**Figura 6 – Captura de tela dos testes**

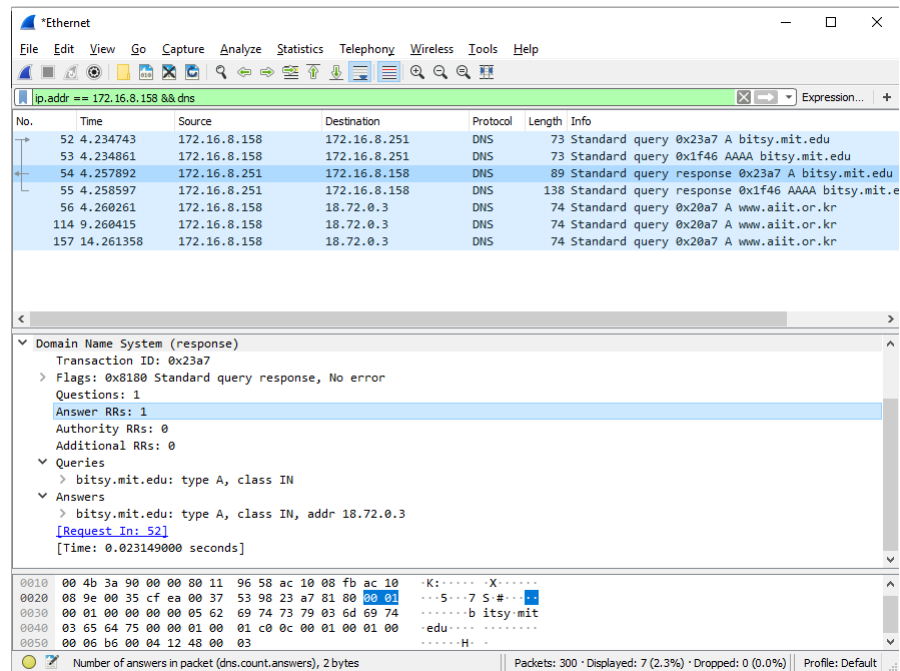
#### 4. Rastreamento Wireshark com nslookup e type=NS

- IP endereçado: 172.16.8.251. Sim, é um dos servidores DNS locais.
- Type: NS, mas não possui mensagens de "answer"
- Servidores DNS listados:
  - eur5.akam.net
  - use5.akam.net
  - use2.akam.net
  - ns1-37.akam.net
  - asia2.akam.net
  - usw2.akam.net
  - ns1-173.aam.net
  - asia1.akam.net
- Sim, os IPs são listados em um campo de informações adicionais.

**Figura 7 – Captura de tela dos testes**

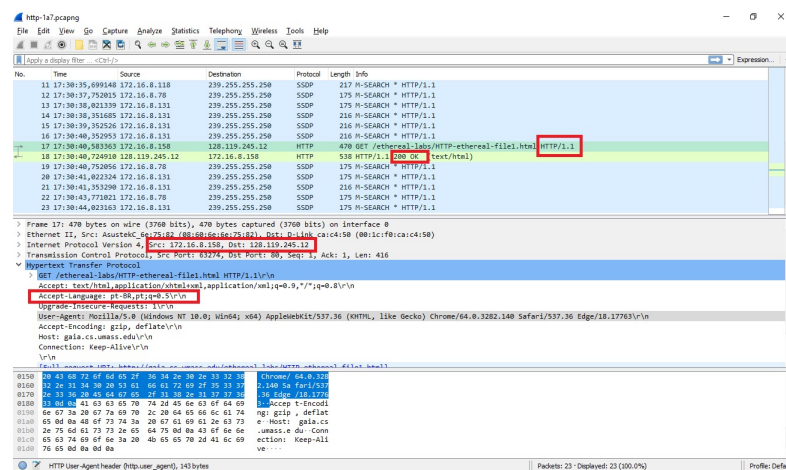
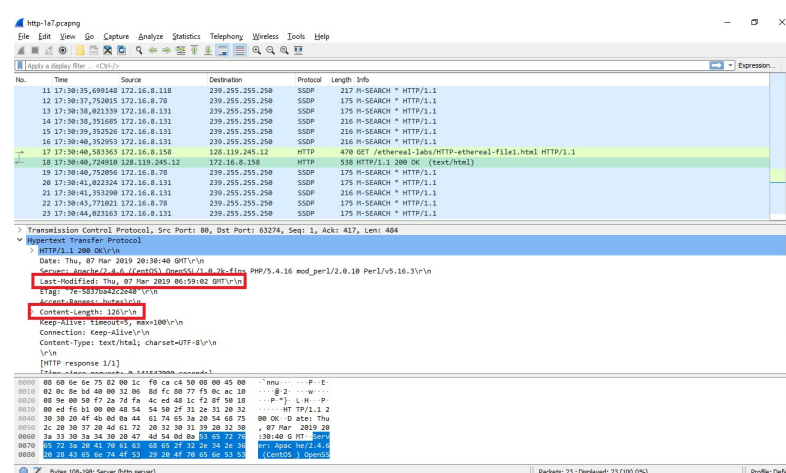
### 5. Rastreamento Wireshark com nslookup e DNS bitsy

- (a) IP: 172.16.8.251, continua sendo de um host local.
- (b) Type A. Sem mensagens "answers" inclusas na consulta.
- (c) Existe um campo em answer, onde informa o IP do endereço solicitado.

**Figura 8 – Captura de tela dos testes**

**3 REPOSTAS HTTP - UTILIZANDO ROTEIRO V1.2****1. Interação Básica GET/Resposta do HTTP**

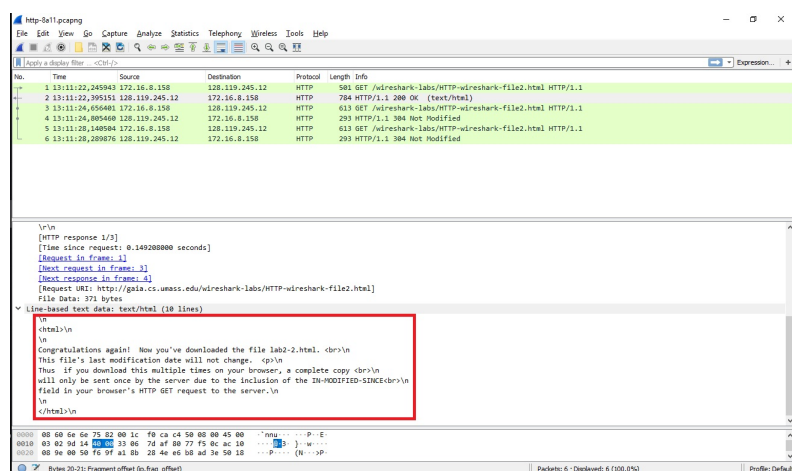
- (a) O navegador executa o HTTP 1.1, o mesmo que o servidor.
- (b) Aceita apenas o pt-br.
- (c) IP de minha máquina: 172.16.8.158. IP do servidor: 128.119.245.12
- (d) Status code 200 - "OK"
- (e) Dia 7 de março de 2019, às 6:59 horas
- (f) 126 Bytes
- (g)

**Figura 9 – Informações dos pacotes de requisição****Figura 10 – Informações dos pacotes de resposta**

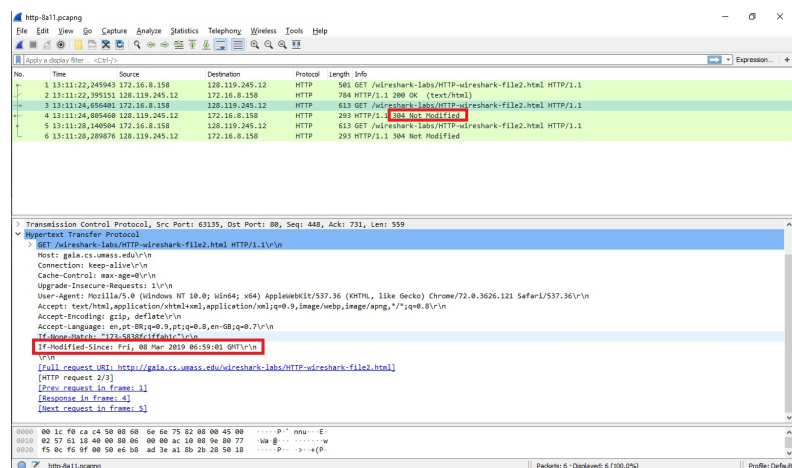


## 2. A Interação HTTP GET Condicional/Resposta

- (a) Não.
- (b) Sim, todo o arquivo HTML está descrito no pacote.
- (c) Sim, contendo a informação de quando houve a ultima modificação da página (Fri, 08 Mar 2019, 06:59:01 GMT)
- (d) Mensagem: Not Modified. O servidor não retorna explicitamente o conteúdo, pois não houveram modificações e, com isso, não sendo necessário o reenvio do conteúdo da página.



**Figura 11 – Informações da primeira requisição**



**Figura 12 – Informações da segunda requisição**

## 3. Baixando Documentos Longos

- (a) Apenas uma mensagem HTTP GET foi enviado pelo navegador
- (b) Para carregar a resposta, foram necessários 4 segmentos.
- (c) Código 200, com a frase OK.
- (d) Não.

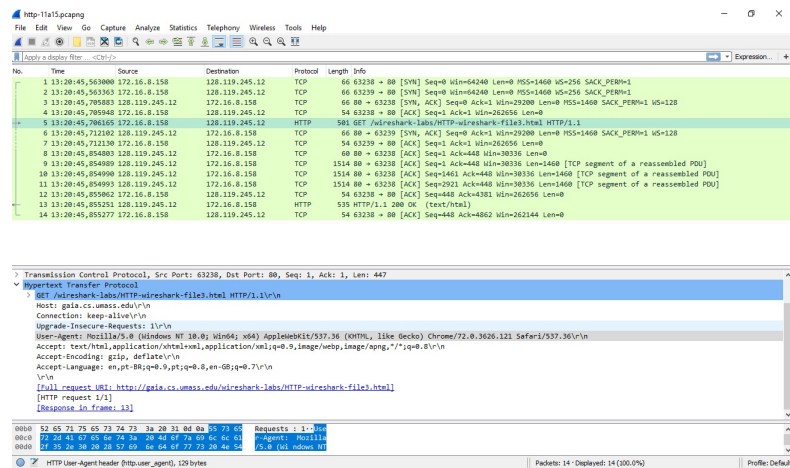


Figura 13 – Informações do pacote de requisição

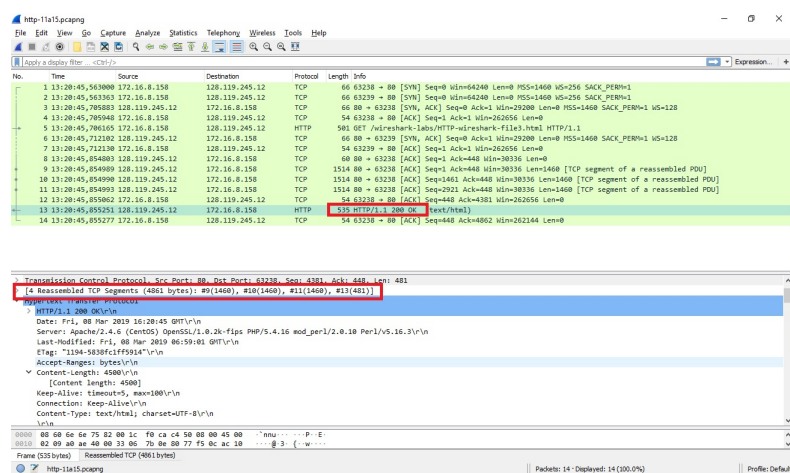


Figura 14 – Informações do pacote de resposta

#### 4. Documentos HTML com Objetos Incluídos

(a) 3 mensagens GET foram enviadas. Para os endereços:

- <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>
- <http://gaia.cs.umass.edu/pearson.png>
- [http://manic.cs.umass.edu/kurose/cover\\_5th\\_ed.jpg](http://manic.cs.umass.edu/kurose/cover_5th_ed.jpg)

(b) Foram baixadas em paralelo, pois não o navegador não esperou a resposta OK de uma imagem para fazer a requisição de outra.

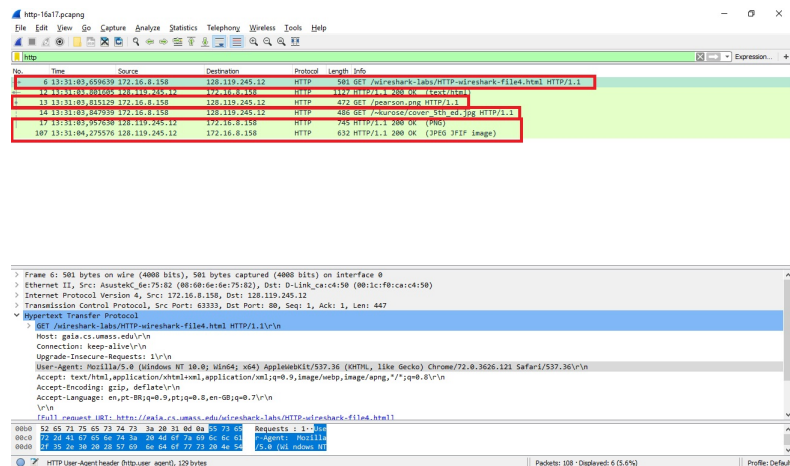


Figura 15 – Informações dos pacotes HTTP

## 5. Autenticação HTTP

- (a) Código 401, com a mensagem: "Unauthorized"
- (b) O campo "Authorization" foi incluído à mensagem.

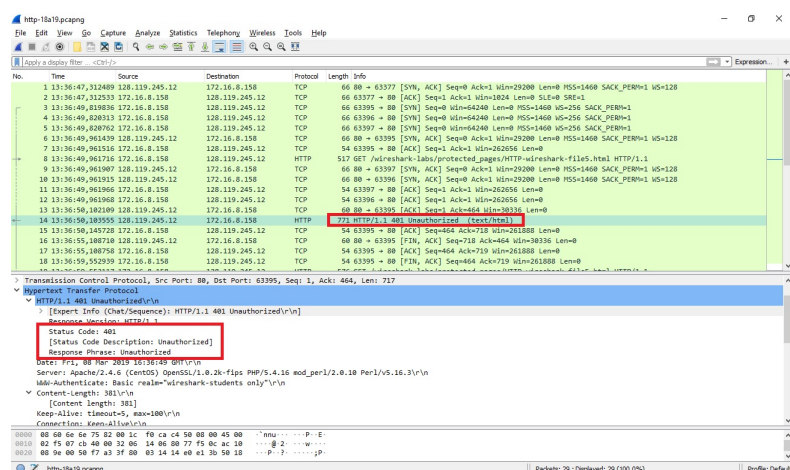


Figura 16 – Informações do pacote primeira requisição

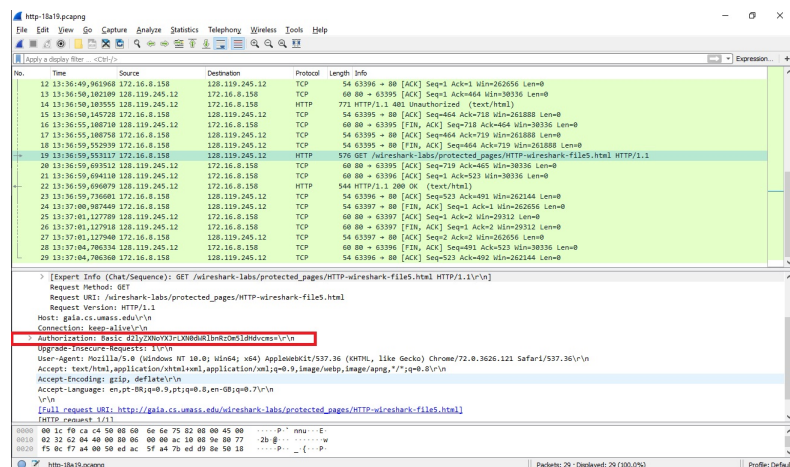


Figura 17 – Informações do pacote segunda requisição