

## Atividade 2

### Introdução ao Wireshark

• O objetivo desta atividade é apresentar o Wireshark, software que será utilizado em várias outras atividades durante essa disciplina. Leia o texto e execute os passos que estão no arquivo (WiresharkIntro.pdf).

R = Passo a passo realizado do Wireshark abaixo.

1. Aberto o Google Chrome na página globo.com
2. Wireshark inicializado.
3. Configurado de acordo com a imagem.

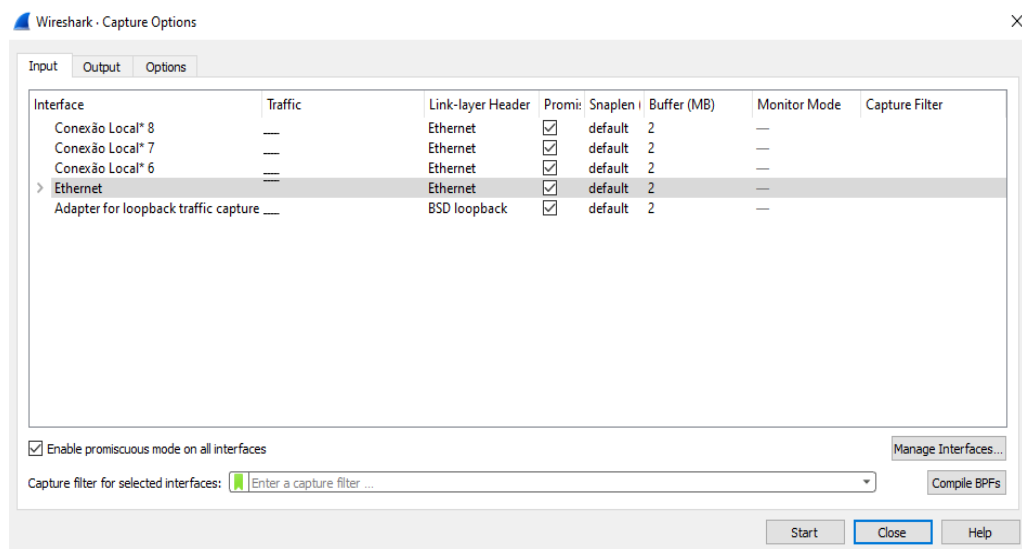


Figura 1: Passo 3 do tutorial.

4. Clicado em start para começar o Wireshark e realizar captura de pacotes enviados e recebidos do computador.
5. Print dos pacotes capturados.

No.	Time	Source	Destination	Protocol	Length	Info
7985	90.188270	192.168.100.2	104.16.13.243	TCP	66	56216 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
7988	90.210984	192.168.100.2	104.16.13.243	TCP	54	56216 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
7989	90.211245	192.168.100.2	104.16.13.243	TLSv1.2	571	Client Hello
7921	90.236273	192.168.100.2	104.16.13.243	TCP	54	56216 → 443 [ACK] Seq=518 Ack=2838 Win=263168 Len=0
7923	90.242013	192.168.100.2	104.16.13.243	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
7924	90.242158	192.168.100.2	104.16.13.243	TLSv1.2	153	Application Data
7925	90.242341	192.168.100.2	104.16.13.243	TLSv1.2	618	Application Data
7934	90.269046	192.168.100.2	104.16.13.243	TCP	54	56216 → 443 [ACK] Seq=1274 Ack=3203 Win=262656 Len=0
7935	90.269274	192.168.100.2	104.16.13.243	TLSv1.2	92	Application Data
7991	90.427719	192.168.100.2	104.16.13.243	TCP	54	56216 → 443 [ACK] Seq=1312 Ack=3468 Win=262400 Len=0
9430	96.853343	192.168.100.2	104.16.13.243	TCP	54	56216 → 443 [FIN, ACK] Seq=1312 Ack=3468 Win=262400 Len=0
9514	96.876225	192.168.100.2	104.16.13.243	TCP	54	56216 → 443 [ACK] Seq=1313 Ack=3469 Win=262400 Len=0
11307	119.498588	192.168.100.2	128.119.245.12	TCP	66	56239 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11308	119.499180	192.168.100.2	128.119.245.12	TCP	66	56240 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11310	119.588184	192.168.100.2	128.119.245.12	TCP	66	56241 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11312	119.660605	192.168.100.2	128.119.245.12	TCP	54	56239 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
11313	119.660794	192.168.100.2	128.119.245.12	HTTP	551	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
11315	119.661239	192.168.100.2	128.119.245.12	TCP	54	56240 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
11320	119.754747	192.168.100.2	128.119.245.12	TCP	54	56241 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
11325	119.868678	192.168.100.2	128.119.245.12	TCP	54	56239 → 80 [ACK] Seq=498 Ack=439 Win=262144 Len=0
11326	119.885608	192.168.100.2	128.119.245.12	HTTP	497	GET /favicon.ico HTTP/1.1

> Frame 11313: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface \Device\NPF\_{0DEA2AF1-0FF6-4FB3-9DF2-FE83EEC0FAB7}, id 0  
 > Ethernet II, Src: Eliteg72:c0:2f (74:27:ea:72:c0:2f), Dst: HuaweiTe\_f7:6a:0c (ac:75:1d:f7:6a:0c)  
 > Internet Protocol Version 4, Src: 192.168.100.2, Dst: 128.119.245.12  
 > Transmission Control Protocol, Src Port: 56239, Dst Port: 80, Seq: 1, Ack: 1, Len: 497

```

0000  ac 75 1d f7 6a 0c 74 27 ea 72 c0 2f 08 00 45 00  -u-j t' r:/E
0010  02 19 63 af 40 00 80 06 fb 00 c0 a8 64 02 80 77  -c @- - - -d-w
0020  f5 0c db af 00 50 08 d5 d1 2c cc e6 ce 9d 50 18  - - - -P- - - -P-
0030  04 01 c0 34 00 00 47 45 54 20 2f 77 69 72 65 73  - - - -GE T /wires
0040  68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d  -hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e  -wireshar k-file1.
0060  68 74 6d 6c 20 4b 54 54 50 2f 31 2e 31 0d 0a 46  -html HTT P/1.1 :H
0070  6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61  -ost: gai a.cs.uma
0080  73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69  -ss.edu- - Connecti
  
```

Figura 2: Pacotes capturados, passo 5 tutorial + site gaia aberto

- Entrado no site <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> e o Wireshark realizou o captura como mostra o print anterior.
- Feito o stop no Wireshark e visto os pacotes e os tipos de protocolos capturados durante essa troca de mensagens entre a conexão do computador e as outras entidades da internet. O pacote do gaia HTTP apareceu na lista.
- Digitado `http` para filtrar como pedido no tutorial, apareceu os pacotes do site gaia acessado.

No.	Time	Source	Destination	Protocol	Length	Info
11313	119.660794	192.168.100.2	128.119.245.12	HTTP	551	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
11326	119.885608	192.168.100.2	128.119.245.12	HTTP	497	GET /favicon.ico HTTP/1.1
11324	119.822118	128.119.245.12	192.168.100.2	HTTP	492	HTTP/1.1 200 OK (text/html)
11338	120.046792	128.119.245.12	192.168.100.2	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Hypertext Transfer Protocol: Protocol

Packets: 15539 • Displayed: 4 (0.0%) • Dropped: 0 (0.0%)

Profile: Default

Figura 3: Digitado `http` para filtrar

9. Encontrado a mensagem GET HTTP que foi enviado para o meu computador através do server do site acessado do gaia. Visto as informações, o tipo ipv4, porta, host e a mensagem criptografada.

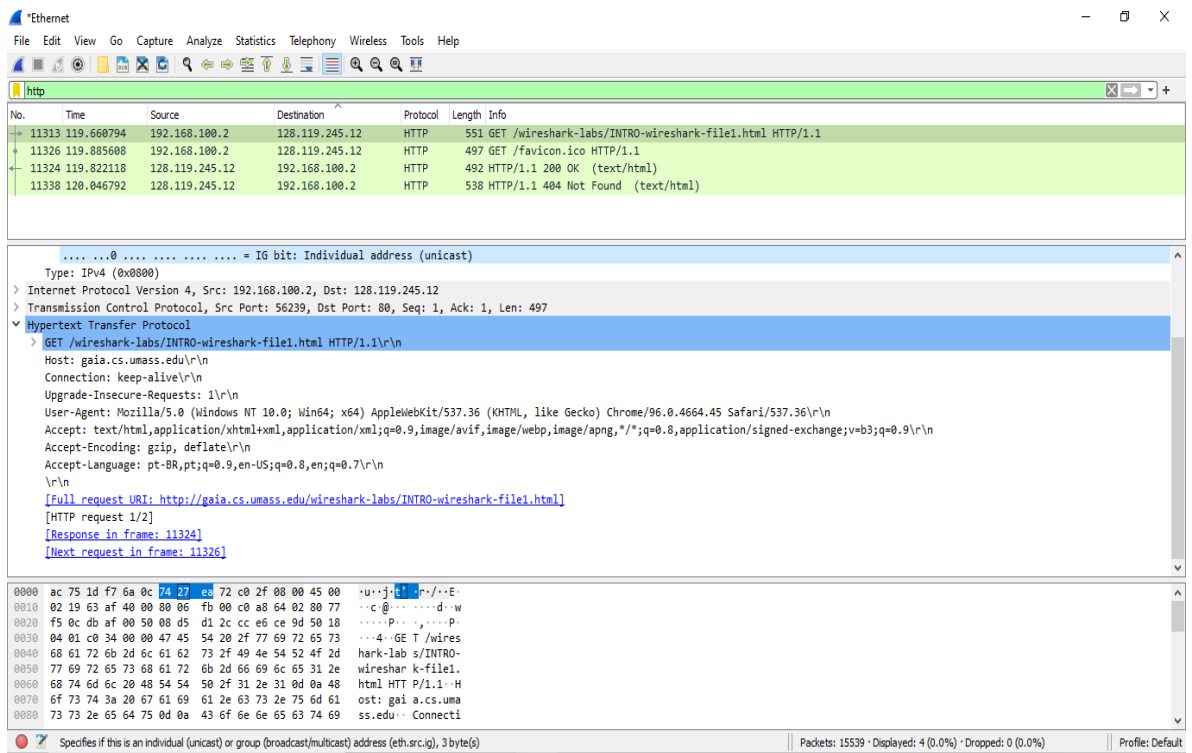


Figura 4: Informações da mensagem GET HTTP filtrada

• As próximas perguntas demonstrarão que você conseguiu colocar o Wireshark em funcionamento e explorou alguns de seus recursos. Baseado em seus experimentos realizados seguindo os passos do arquivo (WiresharkIntro.pdf), responda:

1. Liste 3 protocolos diferentes que aparecem na coluna de protocolos na janela de listagem de pacotes não filtrados na etapa 7.

R = Alguns dos protocolos que apareceram foram: TCP, HTTP, TLSv1.2, UDP, RTCP, STUN.

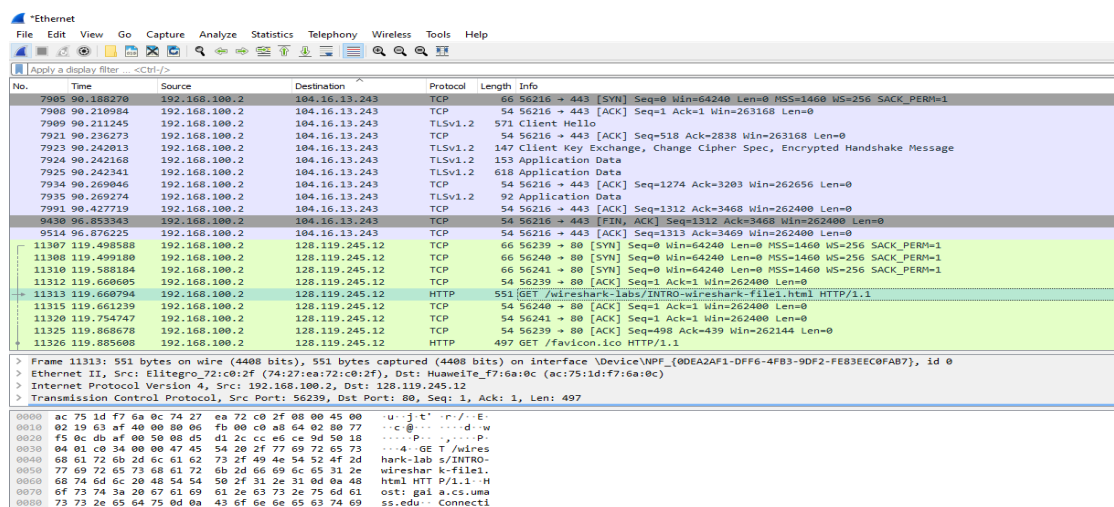


Figura 4: Lista protocolos

No.	Time	Source	Destination	Protocol	Length	Info
11108	22:52:28,186779	192.168.100.2	52.114.198.149	RTP	70	Receiver Report
11109	22:52:28,215613	192.168.100.2	52.114.198.149	UDP	113	51723 → 3480 Len=71
11110	22:52:28,236260	192.168.100.2	52.114.198.149	UDP	79	51723 → 3480 Len=37
11119	22:52:28,374789	192.168.100.2	52.114.198.149	RTP	118	Sender Report
11121	22:52:28,393218	192.168.100.2	52.114.198.149	RTP	70	Receiver Report
11139	22:52:28,516774	192.168.100.2	52.114.198.149	UDP	94	51723 → 3480 Len=52
11147	22:52:28,635767	192.168.100.2	52.114.198.149	UDP	113	51723 → 3480 Len=71
11149	22:52:28,654707	192.168.100.2	52.114.198.149	RTP	70	Receiver Report
11150	22:52:28,655592	192.168.100.2	52.114.198.149	UDP	79	51723 → 3480 Len=37
11162	22:52:28,829648	192.168.100.2	52.114.198.149	RTP	70	Receiver Report
11164	22:52:28,846738	192.168.100.2	52.114.198.149	STUN	142	Binding Request user: QQbv:094Z
11171	22:52:28,951736	192.168.100.2	52.114.198.149	RTP	118	Receiver Report
11172	22:52:28,956713	192.168.100.2	52.114.198.149	RTP	94	Receiver Report
11177	22:52:29,027861	192.168.100.2	52.114.198.149	RTP	70	Receiver Report
11180	22:52:29,055627	192.168.100.2	52.114.198.149	UDP	113	51723 → 3480 Len=71
11182	22:52:29,076010	192.168.100.2	52.114.198.149	UDP	79	51723 → 3480 Len=37
11188	22:52:29,149215	192.168.100.2	52.114.198.149	RTP	70	Receiver Report
11190	22:52:29,174317	192.168.100.2	52.114.198.149	RTP	70	Receiver Report
11208	22:52:29,475485	192.168.100.2	52.114.198.149	UDP	113	51723 → 3480 Len=71
11218	22:52:29,480724	192.168.100.2	52.114.198.149	UDP	94	51723 → 3480 Len=52

Figura 5: Continuação lista protocolos

2. Quanto tempo levou desde o envio da mensagem HTTP GET até o recebimento da resposta HTTP OK? (Por padrão, o valor da coluna Time na janela de listagem de pacotes é a quantidade de tempo (em segundos) desde que o rastreamento do Wireshark começou. Para exibir o campo Time no formato de hora do dia, selecione o menu Wireshark View e selecione Formato Display Format e, em seguida, selecione Hora do dia.)

R = Colocado o display em hora do dia.

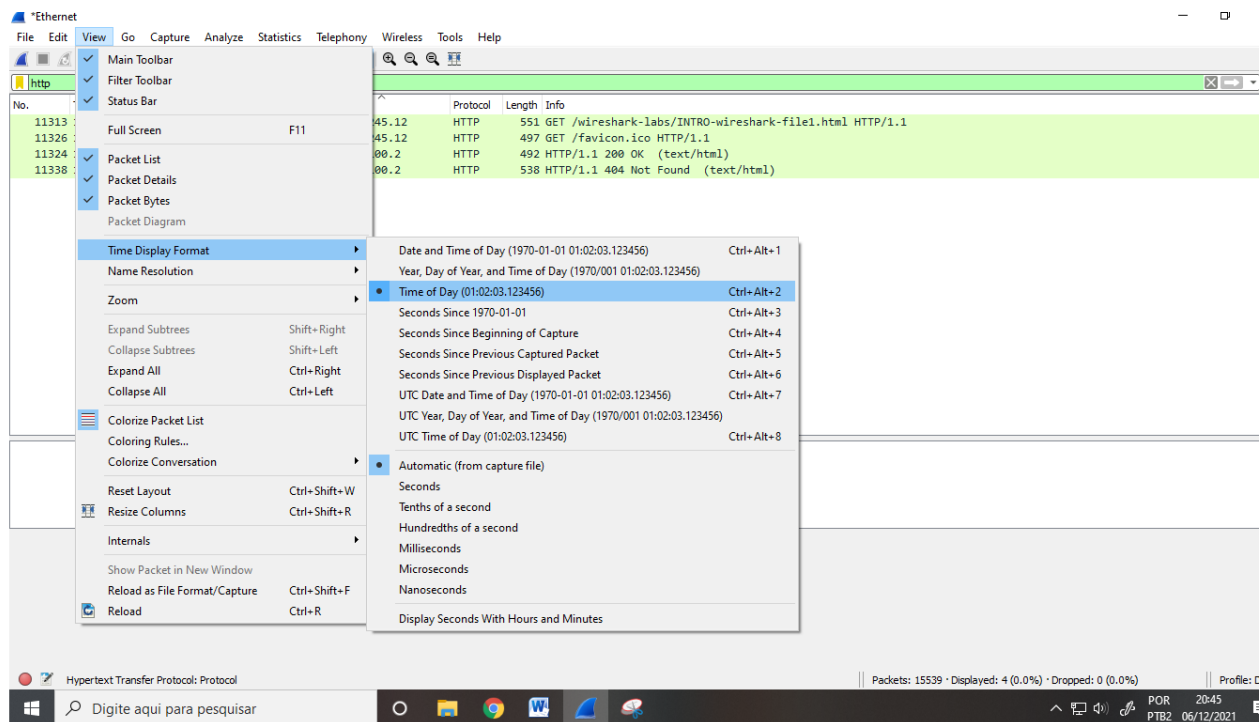


Figura 6: Visualização hora do dia

Tempo demorado entre o HTTP GET e a resposta HTTP OK.

Time	Source	Destination	Protocol	Length	Info
19:52:31,076490	192.168.100.2	128.119.245.12	HTTP	551	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
19:52:31,301304	192.168.100.2	128.119.245.12	HTTP	497	GET /favicon.ico HTTP/1.1
19:52:31,237814	128.119.245.12	192.168.100.2	HTTP	492	HTTP/1.1 200 OK (text/html)
19:52:31,462488	128.119.245.12	192.168.100.2	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Figura 7: Tempo demorado entre GET E OK.

De 19:52:31s,076490 (GET) até 19:52:31s,237814 (OK) = cerca de 0,161324s

**3. Qual é o endereço de Internet do gaia.cs.umass.edu?(também conhecido como www-net.cs.umass.edu)**

Source	Destination
192.168.100.2	128.119.245.12

Figura 8: Endereço gaia a direita e o do meu pc a esquerda

R = O endereço de gaia.cs.umass.edu é 128.119.245.12

**4. Qual é o endereço de Internet do seu computador?**

R = O endereço do meu computador é 192.168.100.2

**5. Imprima as duas mensagens HTTP (GET e OK) mencionadas na pergunta 2 acima. Para fazer isso, selecione Imprimir no menu de comando File do Wireshark e selecione os botões "Selected Packet Only" e "Print as displayed" e clique em OK. Coloque essas imagens no relatório.**

Realizado o print nos pacotes selecionados (GET e OK). Segue as imagens abaixo:

```
C:\Users\Renato\AppData\Local\Temp\wireshark_Ethernet8X0QD1.pcapng 15539 total packets, 4 shown

No.    Time                Source                Destination            Protocol Length Info
 11313 19:52:31.076490     192.168.100.2         128.119.245.12         HTTP      551    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 11313: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface \Device\NPF_{0DEA2AF1-DFF6-4FB3-9DF2-
FE83EEC0FAB7}, id 0
Ethernet II, Src: Elitegro_72:c0:2f (74:27:ea:72:c0:2f), Dst: HuaweiTe_f7:6a:0c (ac:75:1d:f7:6a:0c)
  Destination: HuaweiTe_f7:6a:0c (ac:75:1d:f7:6a:0c)
    Address: HuaweiTe_f7:6a:0c (ac:75:1d:f7:6a:0c)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: Elitegro_72:c0:2f (74:27:ea:72:c0:2f)
    Address: Elitegro_72:c0:2f (74:27:ea:72:c0:2f)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.100.2, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56239, Dst Port: 80, Seq: 1, Ack: 1, Len: 497
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
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 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=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
  [HTTP request 1/2]
  [Response in frame: 11324]
  [Next request in frame: 11326]
No.    Time                Source                Destination            Protocol Length Info
 11324 19:52:31.237814     128.119.245.12        192.168.100.2         HTTP      492    HTTP/1.1 200 OK (text/html)
Frame 11324: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{0DEA2AF1-DFF6-4FB3-9DF2-
FE83EEC0FAB7}, id 0
Ethernet II, Src: HuaweiTe_f7:6a:0c (ac:75:1d:f7:6a:0c), Dst: Elitegro_72:c0:2f (74:27:ea:72:c0:2f)
  Destination: Elitegro_72:c0:2f (74:27:ea:72:c0:2f)
    Address: Elitegro_72:c0:2f (74:27:ea:72:c0:2f)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: HuaweiTe_f7:6a:0c (ac:75:1d:f7:6a:0c)
    Address: HuaweiTe_f7:6a:0c (ac:75:1d:f7:6a:0c)
      ....0. .... = LG bit: Globally unique address (factory default)
```

Figura 9: Print Get e OK pacotes selecionados

```

.....0..... = IG bit: individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.100.2
Transmission Control Protocol, Src Port: 80, Dst Port: 56239, Seq: 1, Ack: 498, Len: 438
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Mon, 06 Dec 2021 22:52:31 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 06 Dec 2021 06:59:02 GMT\r\n
    ETag: "51-5d274cab1a3f8"\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: 0.161324000 seconds]
  [Request in frame: 11313]
  [Next request in frame: 11326]
  [Next response in frame: 11338]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
  File Data: 81 bytes
Line-based text data: text/html (3 lines)

```

Figura 10: Print Get e OK continuação do de cima.