Universidade Federal de Uberlândia – UFU
Bacharelado em Sistemas de Informação – Campus Monte Carmelo
GSI524 – Redes de computadores – 2021/1
RENAN JUSTINO REZENDE SILVA - 11921BSI223

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.

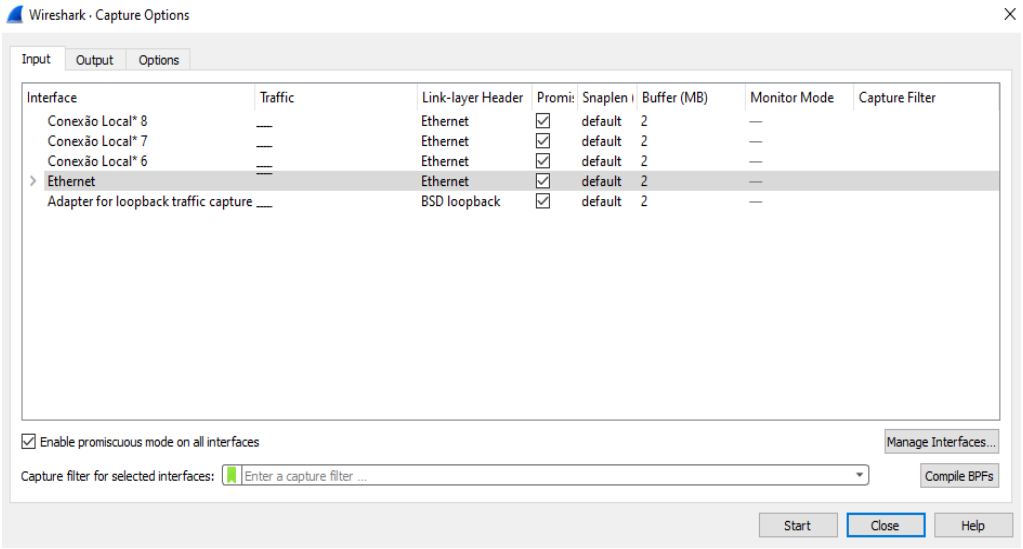

Figura 1: Passo 3 do tutorial.

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

5. Print dos pacotes capturados.

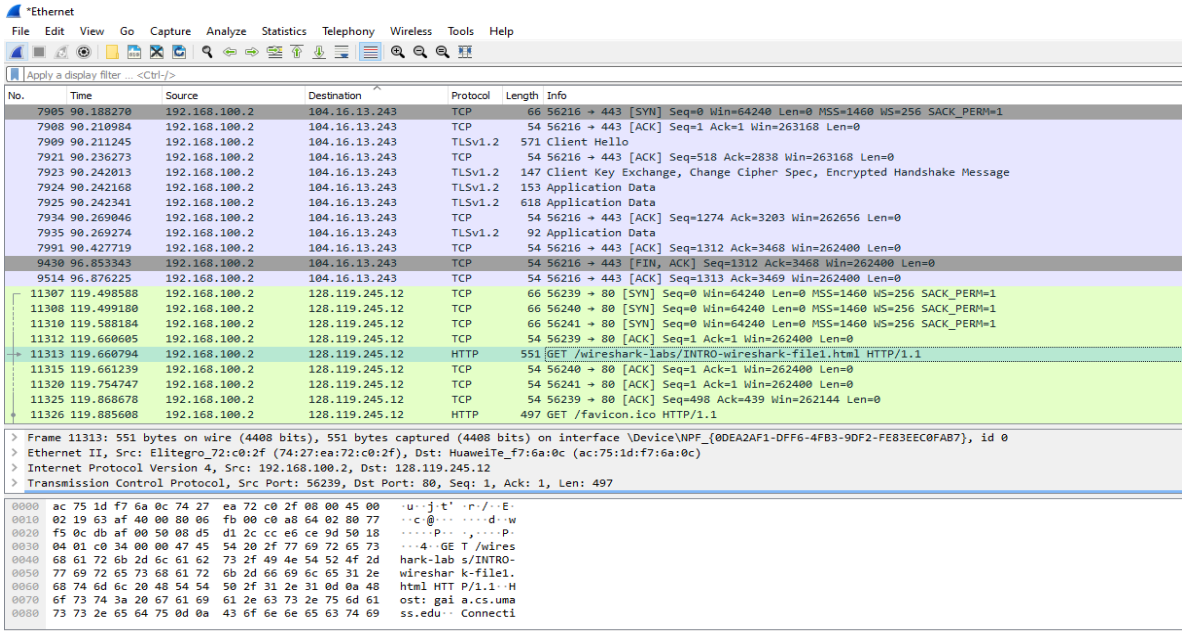

Figura 2: Pacotes capturados, passo 5 tutorial + site gaia aberto

6. 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.

7. 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.

8. Digitado http para filtrar como pedido no tutorial, apareceu os pacotes do site gaia acessado.

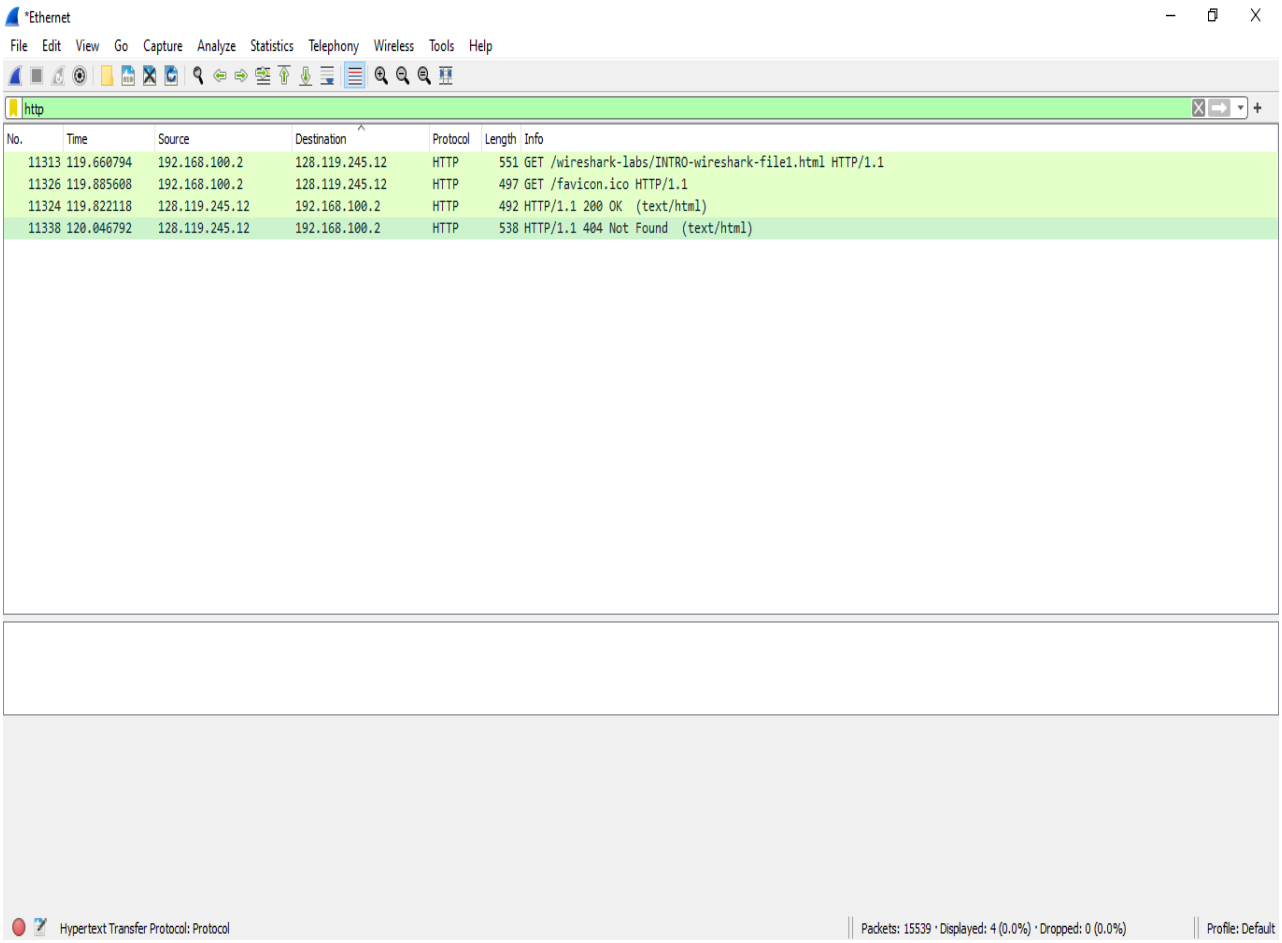

Figura 3: Digitado http para filtrar

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.

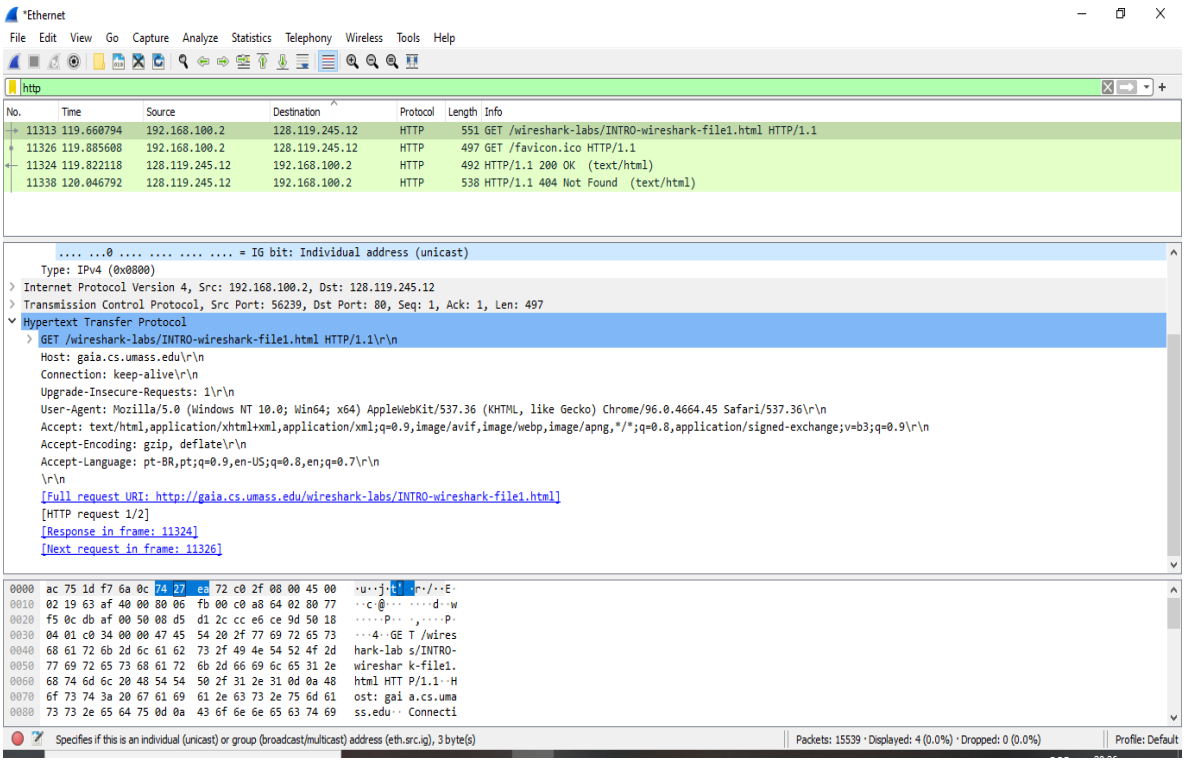

Figura 4: Informações da mensagem GET HTTP filtrada

• 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.

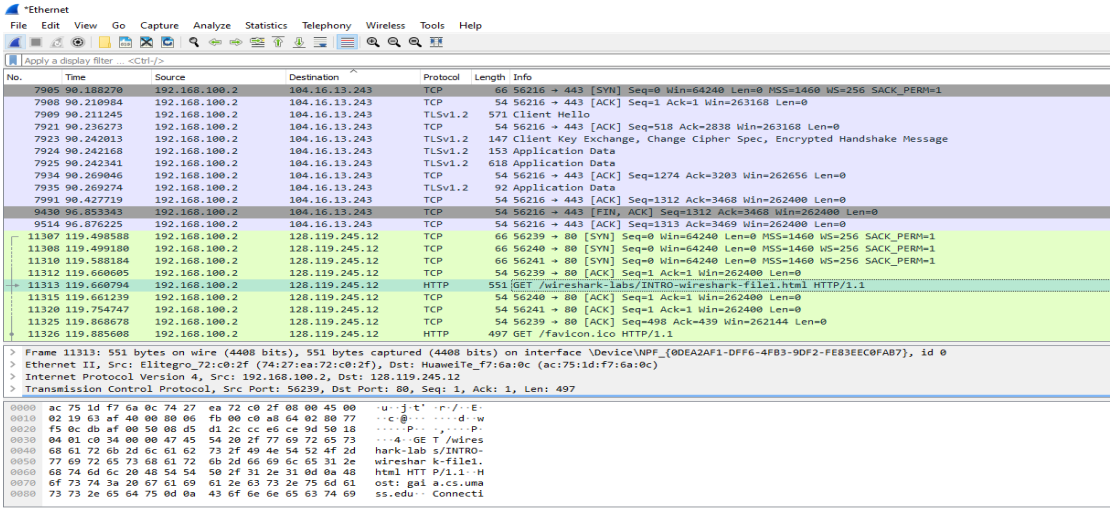

Figura 4: Lista protocolos

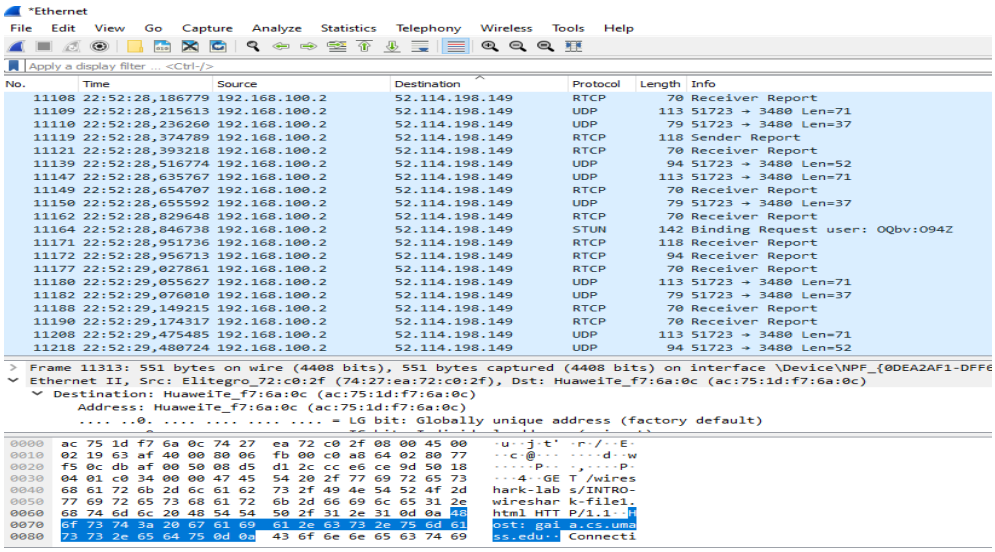

Figura 5: Continuação lista protocolos

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.

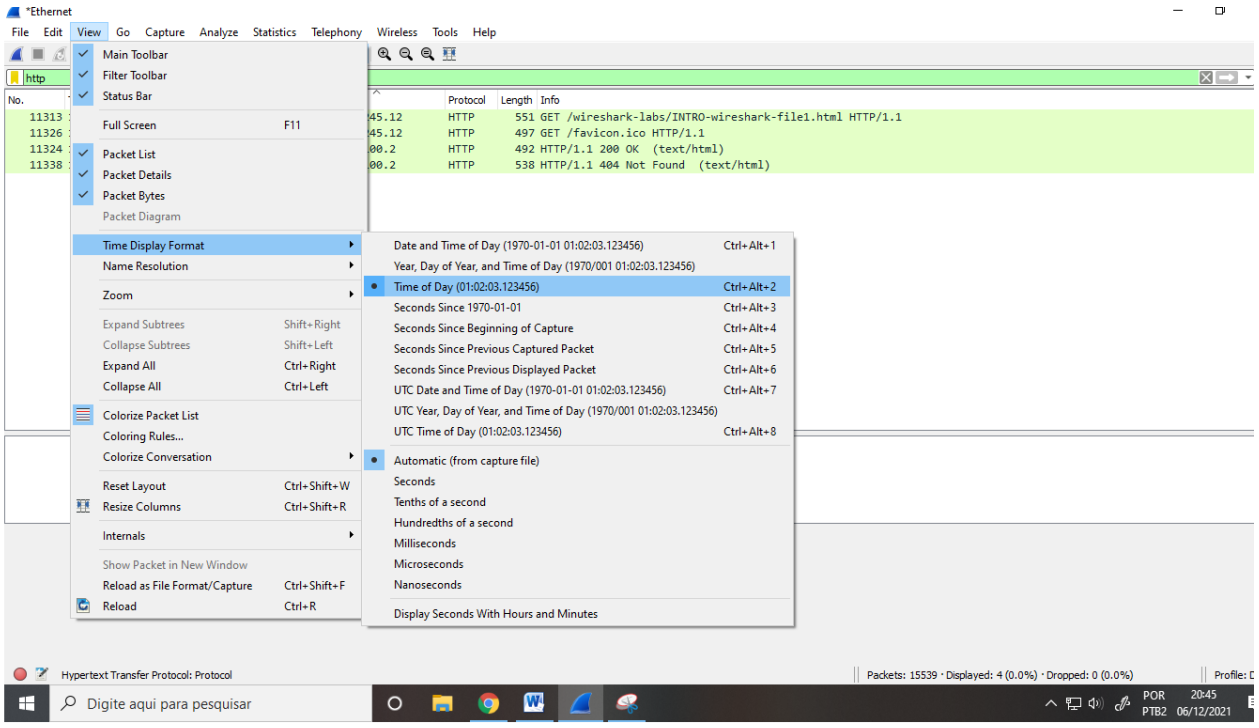

Figura 6: Visualização hora do dia

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.