

# **AULA 05 — A FERRAMENTA WERESHARK**

Por Sediane Carmem Lunardi Hernandes

1

# AGENDA

---



Introdução



Instalação no Linux



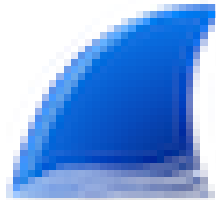
Como utilizar



Analizando o  
tráfego http na rede

# 1. INTRODUÇÃO

- Wireshark é um analisador de pacotes na rede
  - É uma ferramenta que examina o tráfego da rede
    - Captura pacotes da rede e mostra os dados dos pacotes em detalhes
  - É gratuito e de código aberto



**WIRESHARK**

<https://www.wireshark.org/>

# 1. INTRODUÇÃO (CONT.)

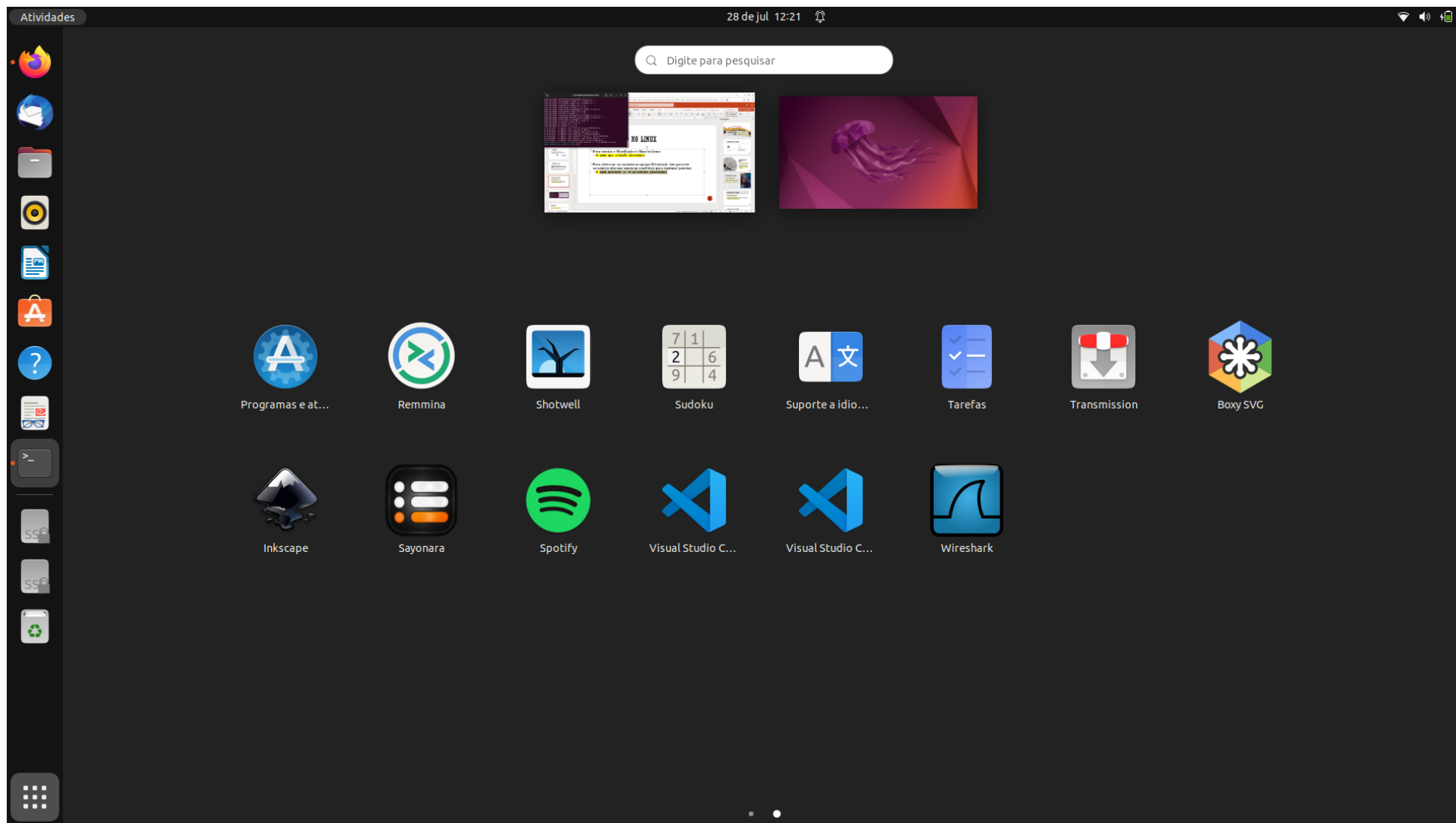
- Wireshark é um software do tipo sniffer
  - Os administradores de rede o usam para solucionar problemas de rede
  - Os engenheiros de segurança de rede o usam para examinar problemas de segurança
  - Os engenheiros de controle de qualidade o usam para verificar os aplicativos de rede
  - Os desenvolvedores o usam para depurar implementações de protocolo
  - As pessoas o usam para aprender sobre os protocolo de rede

## 2. INSTALAÇÃO NO LINUX


- Para instalar o WireShark no Ubuntu Linux:
  - `$ sudo apt install wireshark`
- Para adicionar os usuários ao grupo Wireshark. Isso permite ao usuário não root executar o software para capturar pacotes:
  - `$ sudo usermod -a -G wireshark {username}`

```
usuario@usuario-Inspiron-5590: ~  
usuario@usuario-Inspiron-5590:~$ sudo apt install wireshark  
[sudo] senha para usuario:  
Lendo listas de pacotes... Pronto  
Construindo árvore de dependências... Pronto  
Lendo informação de estado... Pronto  
Os pacotes adicionais seguintes serão instalados:  
  libbcg729-0 libc-ares2 liblua5.2-0 libminizip1 libqt5multimedia5  
  libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5  
  libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data  
  libwireshark15 libwiretap12 libwsutil13 wireshark-common wireshark-qt  
Pacotes sugeridos:  
  snmp-mibs-downloader geoipupdate geoip-database geoip-database-extra  
  libjs-leaflet libjs-leaflet.markercluster wireshark-doc  
Os NOVOS pacotes a seguir serão instalados:  
  libbcg729-0 libc-ares2 liblua5.2-0 libminizip1 libqt5multimedia5  
  libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5  
  libsmi2ldbl libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data  
  libwireshark15 libwiretap12 libwsutil13 wireshark wireshark-common  
  wireshark-qt  
0 pacotes atualizados, 19 pacotes novos instalados, 0 a serem removidos e 157 nã  
o atualizados.  
É preciso baixar 27,7 MB de arquivos.  
Depois desta operação, 132 MB adicionais de espaço em disco serão usados.  
Você quer continuar? [S/n] S
```

```
usuario@usuario-Inspiron-5590: ~  
Configuração de pacotes  
Configurando wireshark-common  
Dumpcap can be installed in a way that allows members of the "wireshark"  
system group to capture packets. This is recommended over the  
alternative of running Wireshark/Tshark directly as root, because less  
of the code will run with elevated privileges.  
For more detailed information please see  
/usr/share/doc/wireshark-common/README.Debian.gz once the package is  
installed.  
Enabling this feature may be a security risk, so it is disabled by  
default. If in doubt, it is suggested to leave it disabled.  
Should non-superusers be able to capture packets?  
<Sim> <Não>
```





A cartoon illustration of a young girl with long, wavy red hair and large blue eyes. She is wearing a pink long-sleeved shirt under a blue jumper dress. She is holding a large green book open and looking at it with a smile. Above her head is a white thought bubble with a black outline, containing text. The background of the thought bubble is filled with green dots.

Qual comando Linux  
utilizamos para  
consultar grupos e  
usuários de cada  
grupo?

Para a ferramenta funcionar  
certifique-se que o seu usuário faz  
parte do grupo wireshark



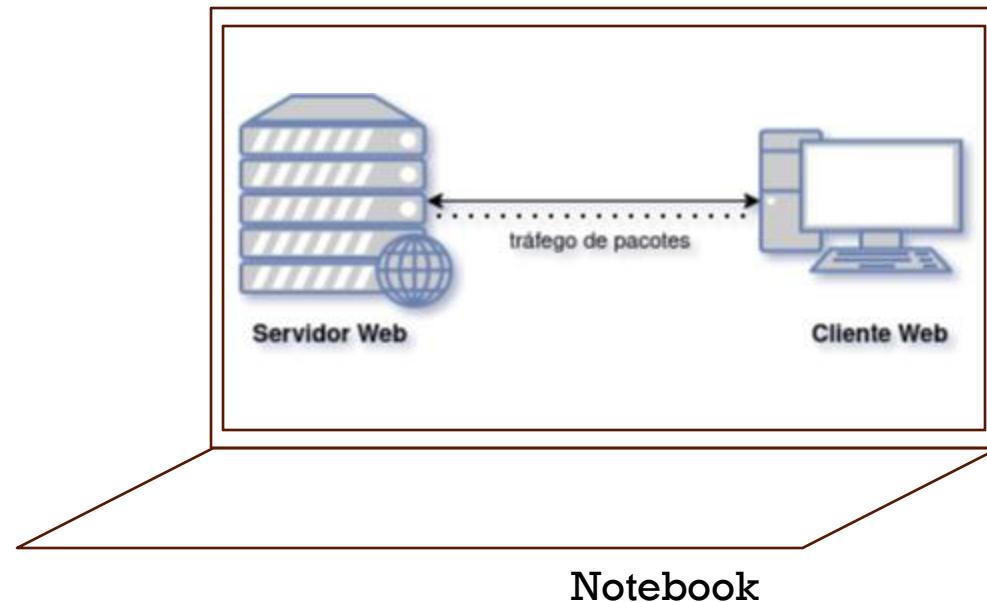
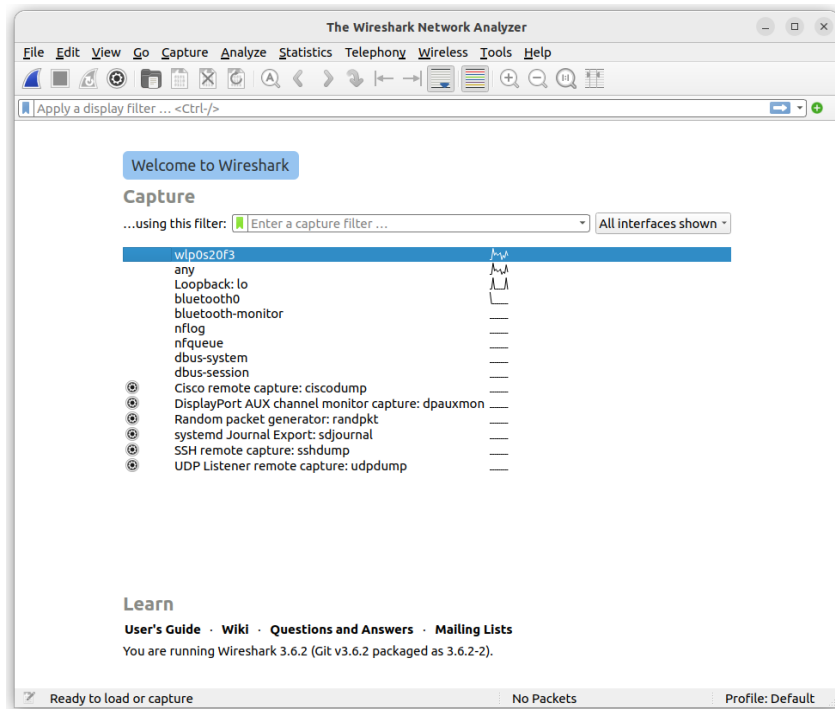
## 2. INSTALAÇÃO NO LINUX (CONT.)

- Para verificar os grupos do sistema:
  - `$ cat /etc/group`
  - Se o seu usuário não faz parte do grupo wireshark adicione (se você executou o segundo comando dos slides não precisará executar esse comando):
    - `$ sudo adduser <usuário> wireshark`
- Para que o Wireshark funcione, precisa modificar a permissão da ferramenta de captura dumpcap que o Wireshark utiliza para capturar pacotes da rede
  - `sudo chmod 771 /usr/bin/dumpcap`

**Agora você já pode utilizar a ferramenta**

# 3. COMO UTILIZAR O WIRESHARK (CONT.)

## ▪ Passo 1: abrir a ferramenta



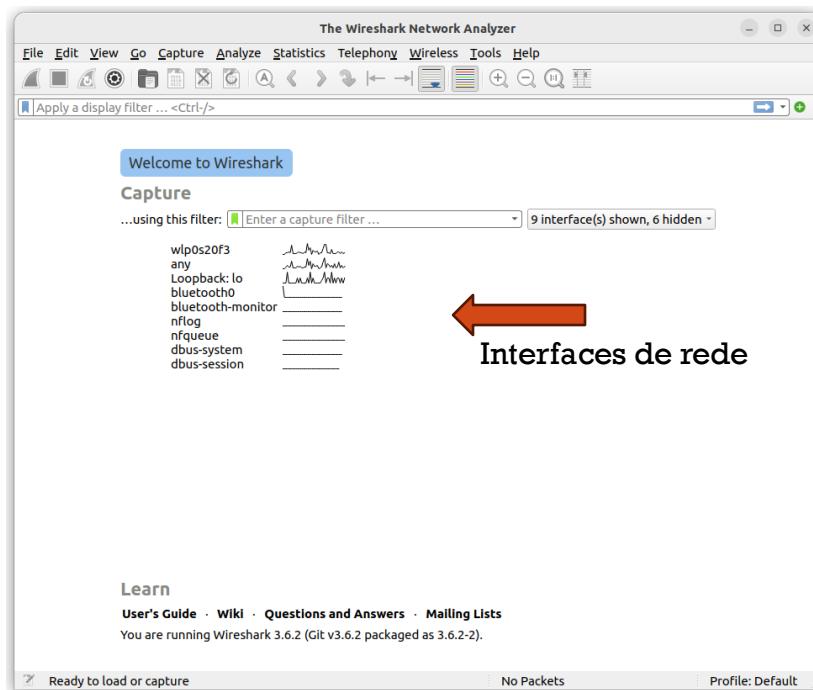
# 3. COMO UTILIZAR O WIRESHARK?



- O que eu faço primeiro?
  - Qual a topologia da rede?
  - Que tipo de pacotes eu preciso/pretendo analisar?
    - Como configurar a ferramenta para capturar os tipos de pacote que eu desejo analisar?
    - O que significa cada linha da minha análise no arquivos de saída?

# 3. COMO UTILIZAR O WIRESHARK (CONT.)

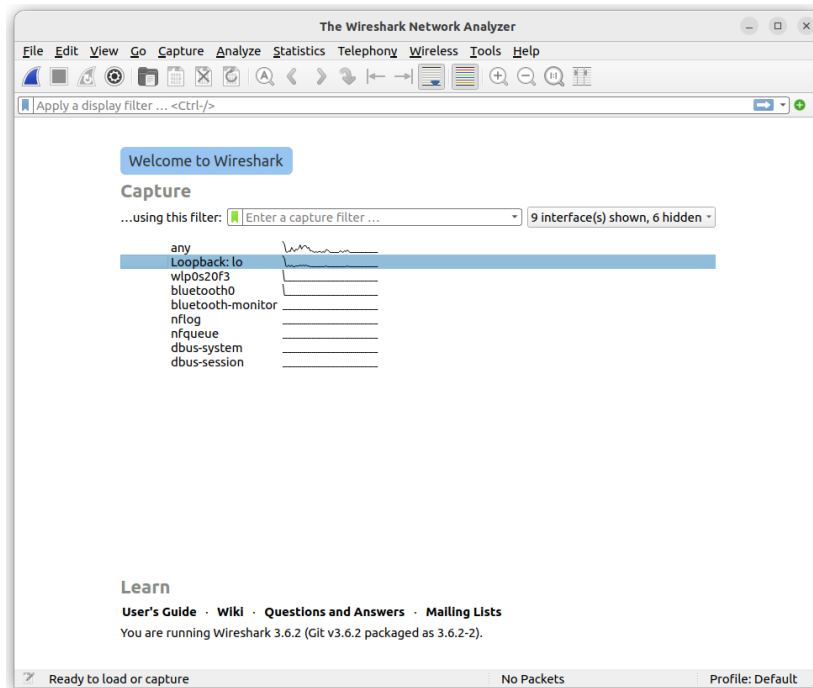
## Tela inicial da ferramenta:



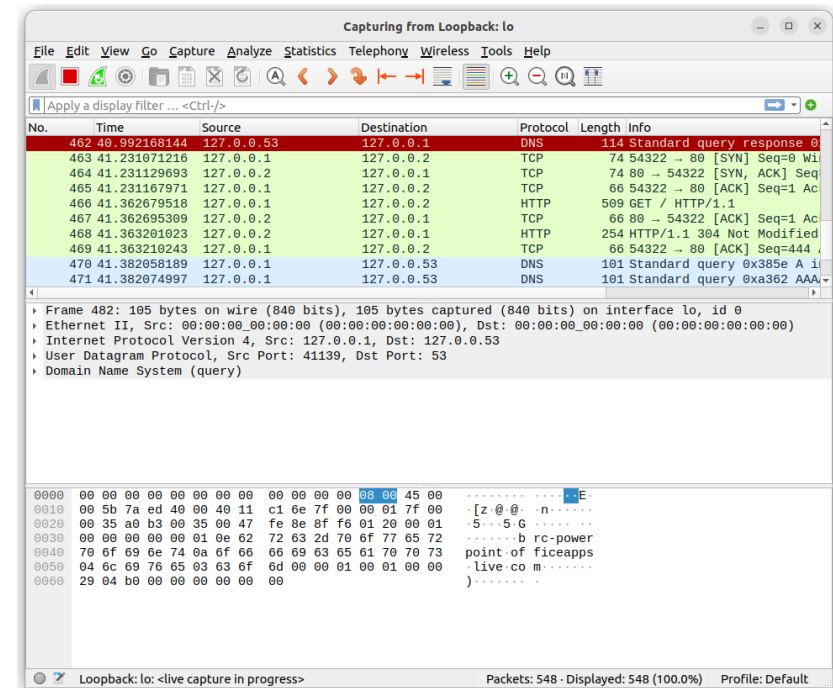
- As interfaces de rede são mostradas
  - Interfaces de rede são pontos de ligação entre dois equipamentos de rede (IP + porta)
- Interface eu iremos utilizar para análise de pacotes:
  - Loopback (127.0.0.1,::1)
  - Interface local (permite conexão com o próprio computador )

# 3. COMO UTILIZAR O WIRESHARK (CONT.)

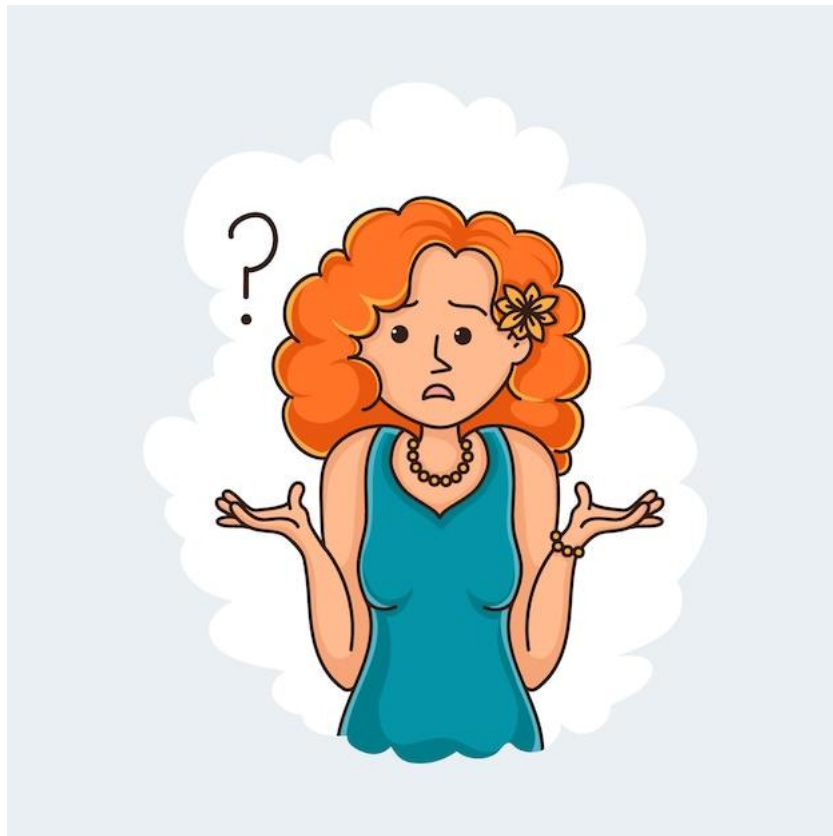
**Passo 2:** Selecionar a interface Loopback



**Passo 3:** Duplo clique na interface Loopback



# 3. COMO UTILIZAR O WIRESHARK (CONT.)



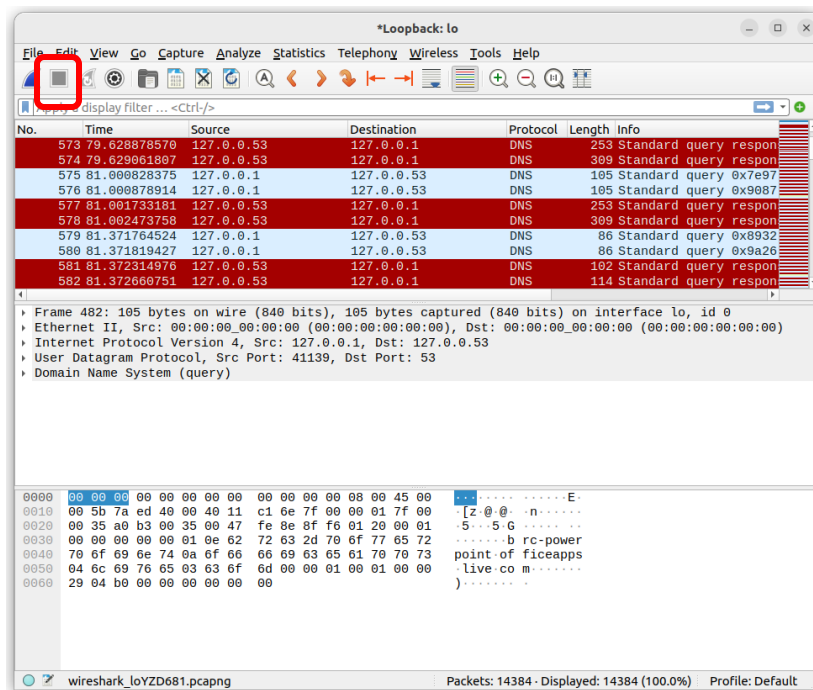
- E agora?
  - São muitas as informações mostradas



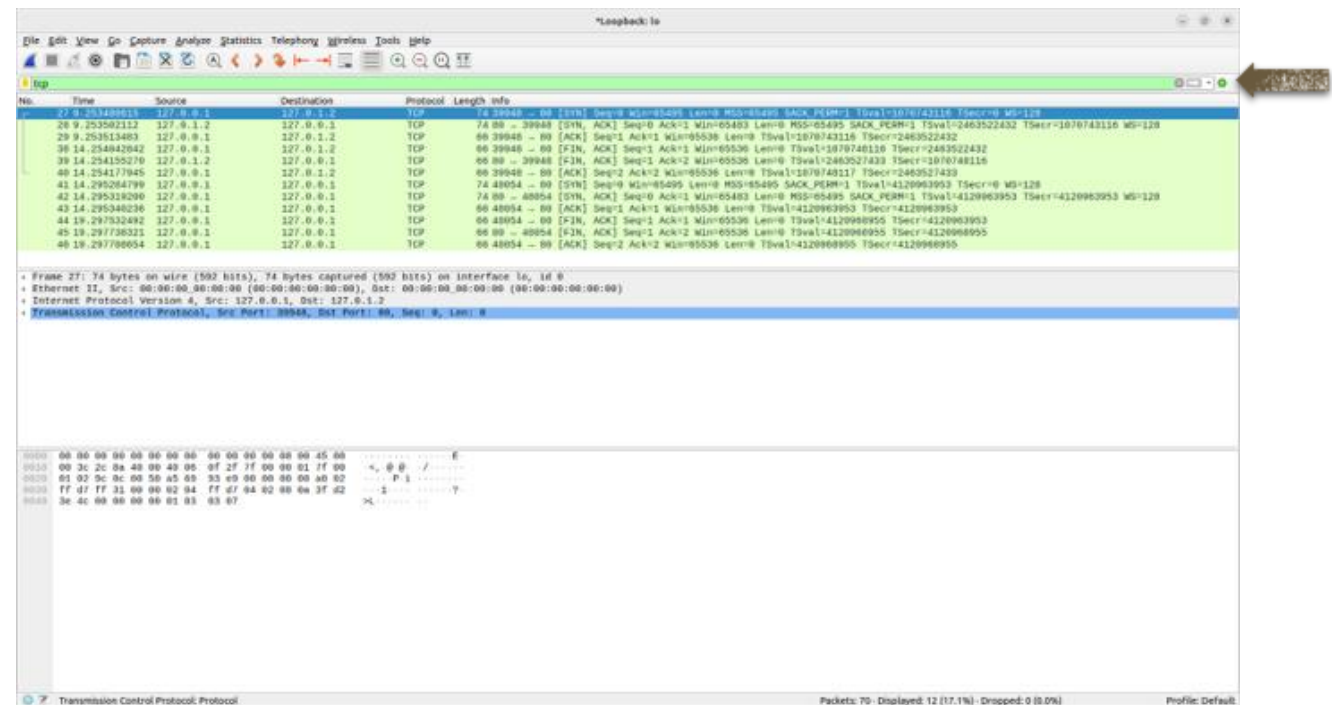
- Aplicar filtros para a captura de pacotes específicos

# 3. COMO UTILIZAR O WIRESHARK (CONT.)

**Passo 4:** Parar a captura de dados



**Passo 5:** Definindo filtros

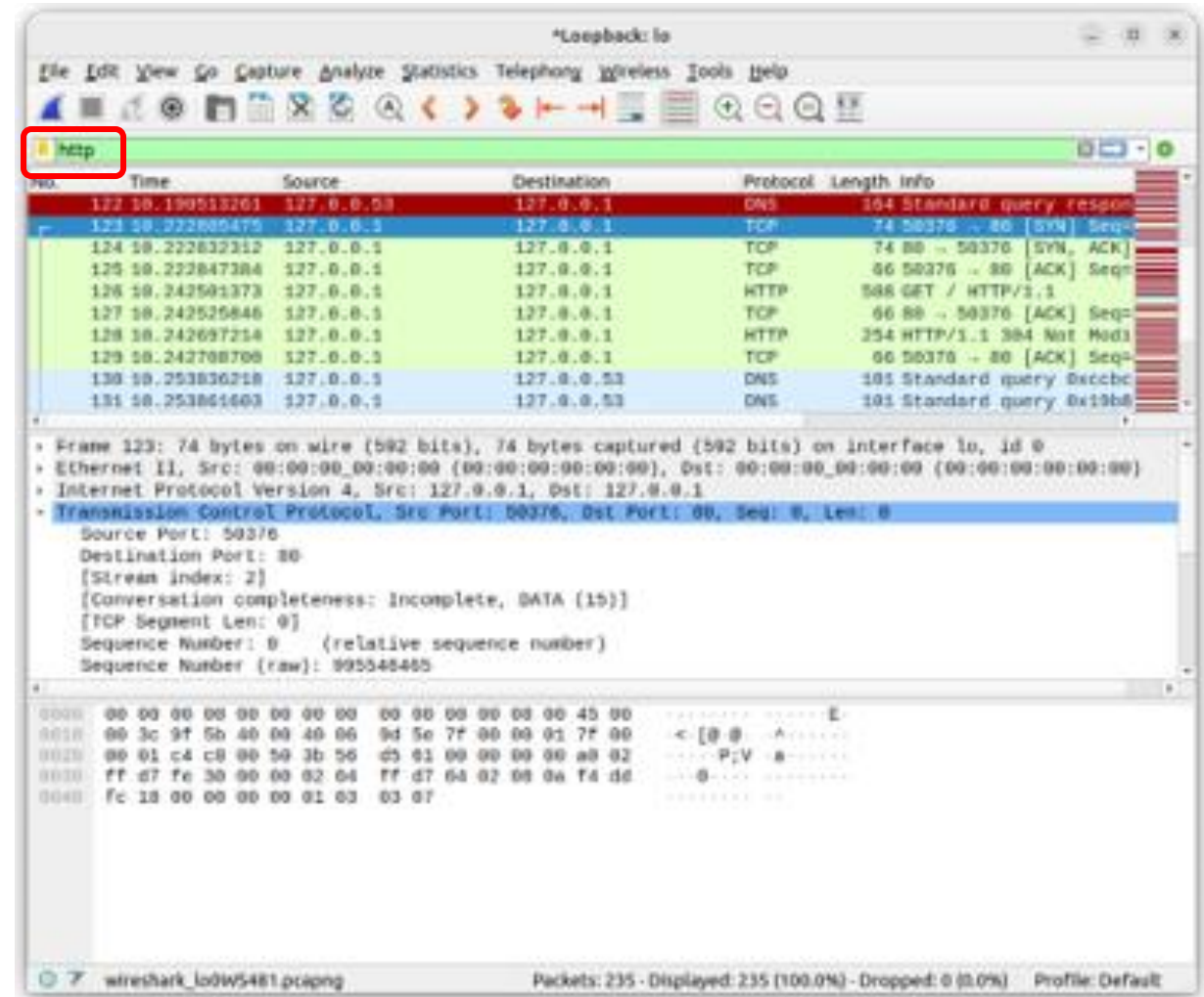


Ou...

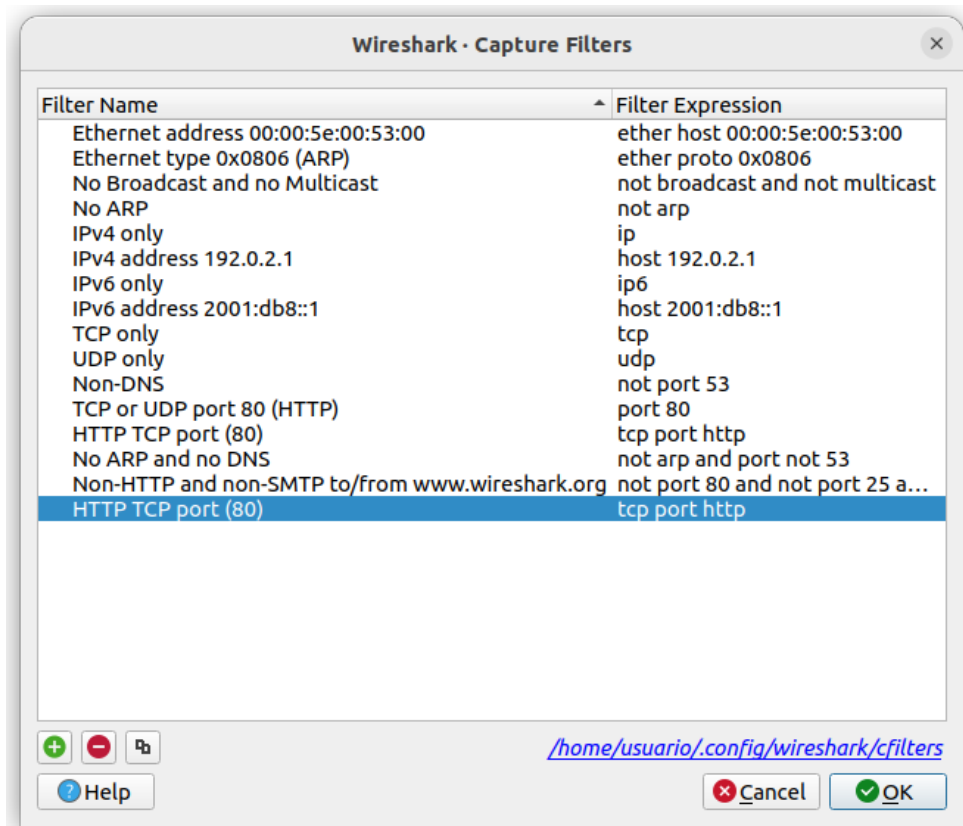


# 3. COMO UTILIZAR O WIRESHARK (CONT.)

## Passo 5: Definindo filtros (cont.)



# 3. COMO UTILIZAR O WIRESHARK (CONT.)



Ou...

- Ir até o Menu Capture
  - escolher HTTP TCP port (80)
  - Clicar em ok
- Deixar executar
- Parar a análise

# ESTABELECIMENTO E ENCERRAMENTO DE CONEXÃO TCP

tcp						
No.	Time	Source	Destination	Protocol	Length	Info
27	9.253488615	127.0.0.1	127.0.1.2	TCP	74	39948 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=6
28	9.253502112	127.0.1.2	127.0.0.1	TCP	74	80 → 39948 [SYN, ACK] Seq=0 Ack=1 Win=65483
29	9.253513483	127.0.0.1	127.0.1.2	TCP	66	39948 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
38	14.254042842	127.0.0.1	127.0.1.2	TCP	66	39948 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65536
39	14.254155270	127.0.1.2	127.0.0.1	TCP	66	80 → 39948 [FIN, ACK] Seq=1 Ack=2 Win=65536
40	14.254177945	127.0.0.1	127.0.1.2	TCP	66	39948 → 80 [ACK] Seq=2 Ack=2 Win=65536 Len=0

## 3. COMO UTILIZAR O WIRESHARK (CONT.)

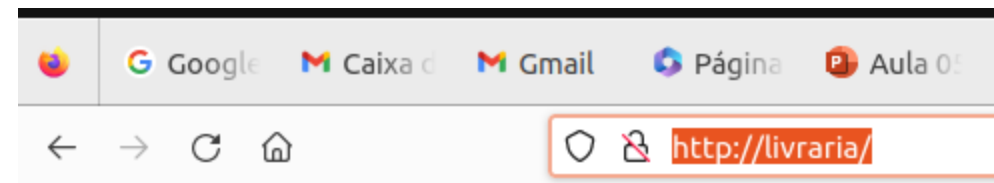
## Passo 5a: Verifique se o servidor NGinx está executando

```

usuario@usuario-Inspiron-5590: ~
usuario@usuario-Inspiron-5590:~$ sudo systemctl start nginx
usuario@usuario-Inspiron-5590:~$ systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: v
   Active: active (running) since Mon 2023-07-31 11:20:20 -03; 9min ago
     Docs: man:nginx(8)
  Process: 16100 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_procv
  Process: 16101 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (v
 Main PID: 16102 (nginx)
    Tasks: 9 (limit: 38160)
  Memory: 7.8M
     CPU: 52ms
  CGroup: /system.slice/nginx.service
          └─16102 "nginx: master process /usr/sbin/nginx -g daemon on; maste
            └─16103 "nginx: worker process"
              └─16104 "nginx: worker process"
                └─16105 "nginx: worker process"
                  └─16106 "nginx: worker process"
                    └─16107 "nginx: worker process"
                      └─16108 "nginx: worker process"
                        └─16109 "nginx: worker process"
                          └─16110 "nginx: worker process"

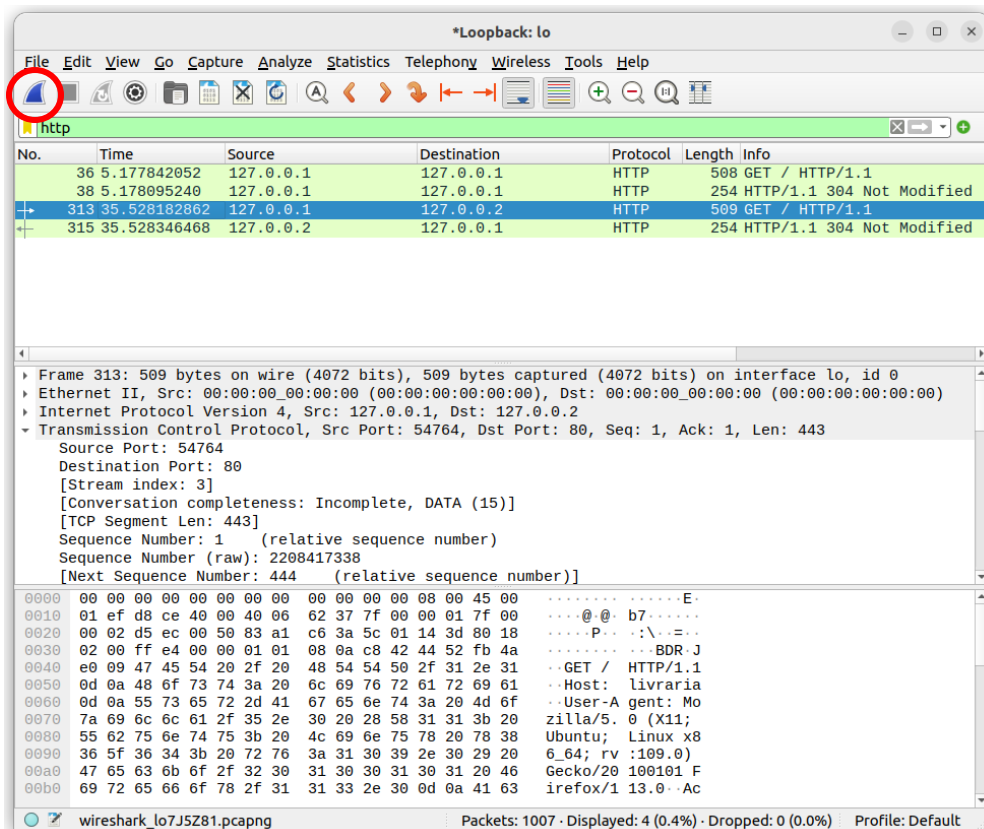
```

### **Passo 5b:** Abrir a página da livraria no navegador



**Página da minha livraria!**

# 3. COMO UTILIZAR O WIRESHARK (CONT.)



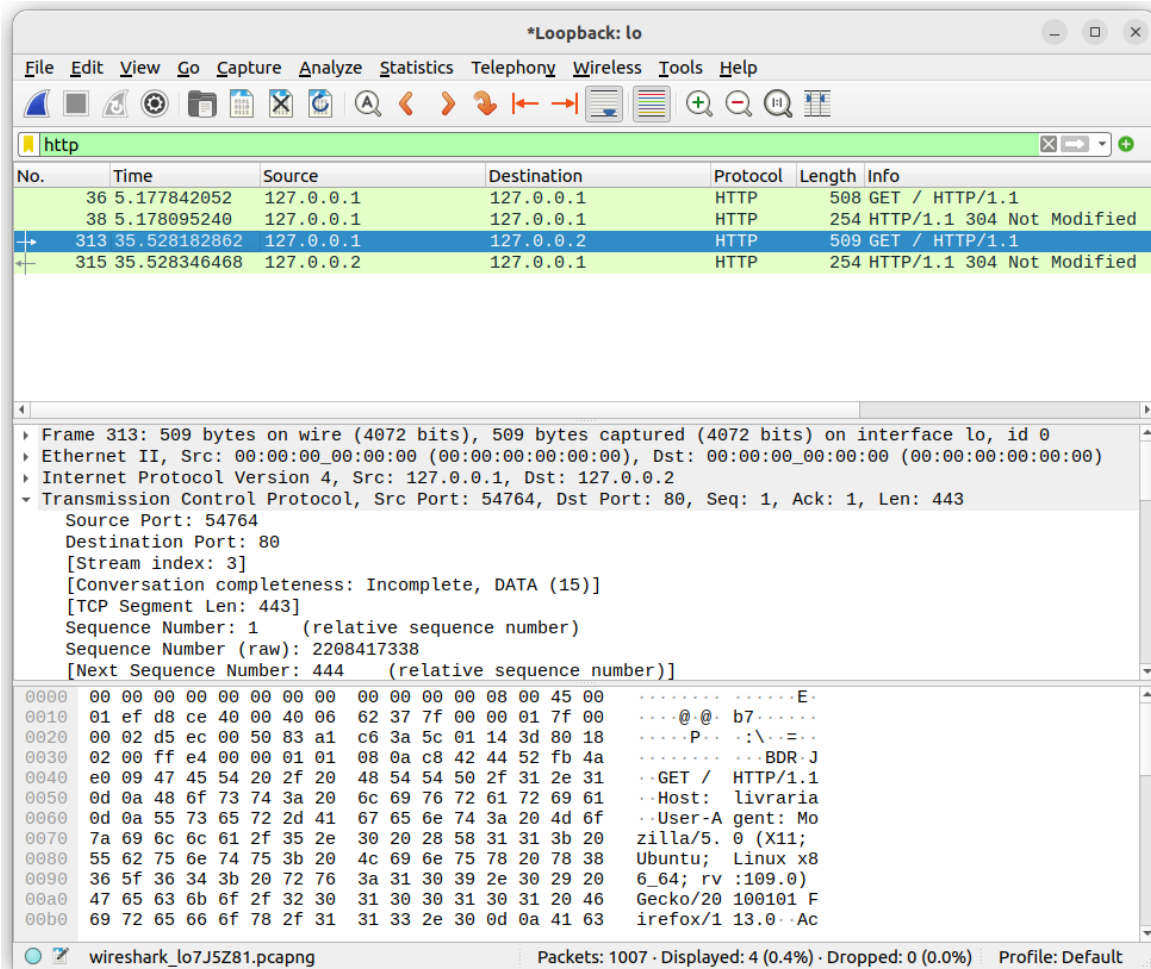
- Iniciar a captura dos pacotes
  - Selecionar o Menu Capture
    - Start

Ou

- Clicar no logo da ferramenta no barra de ferramentas principal



# 4. ANALISANDO O TRÁFEGO HTTP



The image shows a Wireshark capture window titled '\*Loopback: lo'. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area shows a list of captured packets. The first four packets are highlighted in green, and the fifth packet (No. 313) is highlighted in blue. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
36	5.177842052	127.0.0.1	127.0.0.1	HTTP	508	GET / HTTP/1.1
38	5.178095240	127.0.0.1	127.0.0.1	HTTP	254	HTTP/1.1 304 Not Modified
313	35.528182862	127.0.0.1	127.0.0.2	HTTP	509	GET / HTTP/1.1
315	35.528346468	127.0.0.2	127.0.0.1	HTTP	254	HTTP/1.1 304 Not Modified

Below the packet list, the details pane shows the selected packet (No. 313) expanded. It displays the following information:

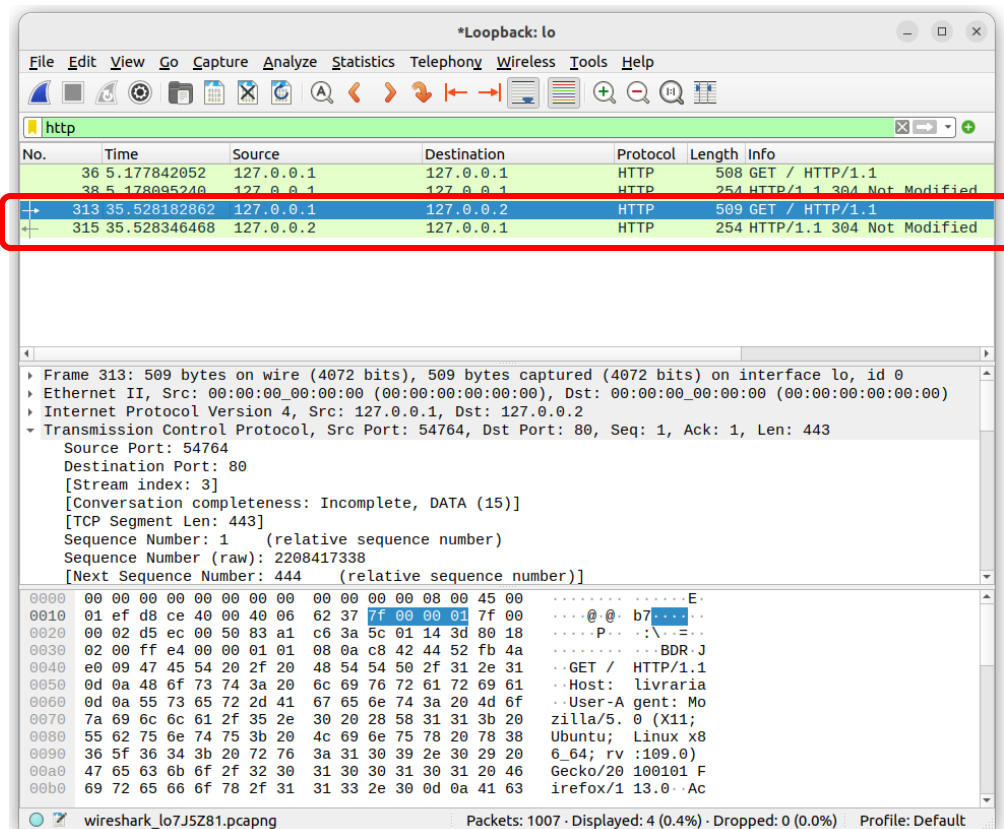
- Frame 313: 509 bytes on wire (4072 bits), 509 bytes captured (4072 bits) on interface lo, id 0
- Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.2
- Transmission Control Protocol, Src Port: 54764, Dst Port: 80, Seq: 1, Ack: 1, Len: 443
  - Source Port: 54764
  - Destination Port: 80
  - [Stream index: 3]
  - [Conversation completeness: Incomplete, DATA (15)]
  - [TCP Segment Len: 443]
  - Sequence Number: 1 (relative sequence number)
  - Sequence Number (raw): 2208417338
  - [Next Sequence Number: 444 (relative sequence number)]

The packet bytes pane at the bottom shows the raw data of the selected packet, displayed in hexadecimal and ASCII. The ASCII column shows the beginning of an HTTP GET request: 'GET / HTTP/1.1'.

- Antes da análise ...
  - Entender os campos apresentados
    - *No* = número do pacote
    - *Time* = tempo em segundos entre o display e o display anterior
    - *Source* = Endereço IP de envio do pacote (quem enviou)
    - *Destination* = Endereço IP de destino do pacote (quem recebeu)
    - *Protocol* = Protocolo utilizado
    - *Lenght* = Tamaho em bytes
    - *info* = informações do pacote



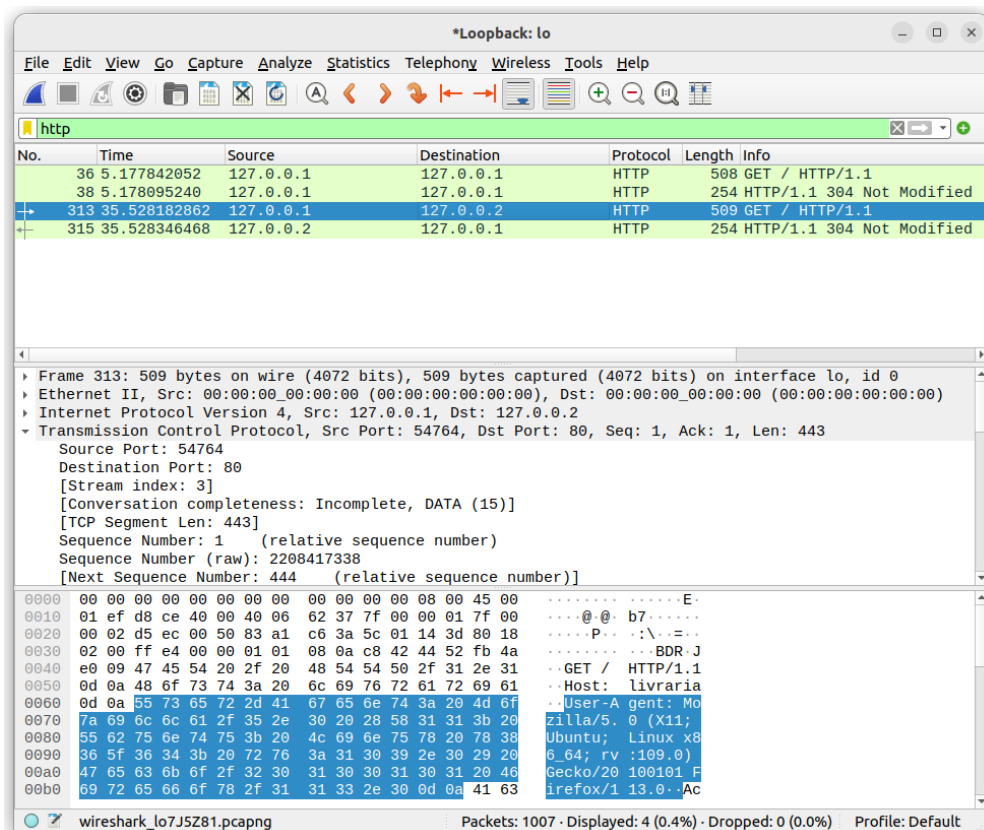
# 4. ANALISANDO O TRÁFEGO HTTP (CONT.)



- Vamos analisar o tráfego
  - 127.0.0.2:80 (IP associado ao domínio local da livraria)
- Duplo clique na linha selecionada



# 4. ANALISANDO O TRÁFEGO HTTP (CONT.)

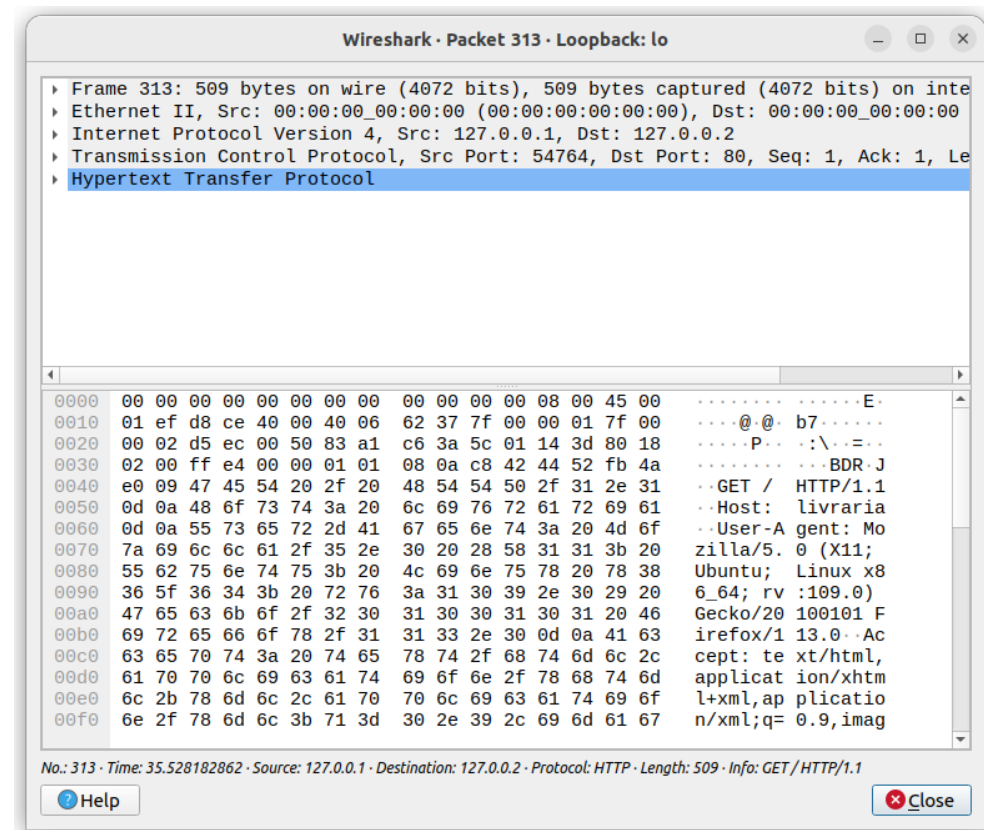


The screenshot shows the Wireshark interface with a packet capture on interface 'lo'. The packet list shows four packets, with packet 313 selected. The packet details pane shows the structure of the selected packet, and the packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
36	5.177842052	127.0.0.1	127.0.0.1	HTTP	508	GET / HTTP/1.1
38	5.178095240	127.0.0.1	127.0.0.1	HTTP	254	HTTP/1.1 304 Not Modified
313	35.528182862	127.0.0.1	127.0.0.2	HTTP	509	GET / HTTP/1.1
315	35.528346468	127.0.0.2	127.0.0.1	HTTP	254	HTTP/1.1 304 Not Modified

Frame 313: 509 bytes on wire (4072 bits), 509 bytes captured (4072 bits) on interface lo, id 0  
Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.2  
Transmission Control Protocol, Src Port: 54764, Dst Port: 80, Seq: 1, Ack: 1, Len: 443  
Source Port: 54764  
Destination Port: 80  
[Stream index: 3]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 443]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 2208417338  
[Next Sequence Number: 444 (relative sequence number)]

0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E.  
0010 01 ef d8 ce 40 00 40 06 62 37 7f 00 00 01 7f 00 ....@. b7.....  
0020 00 02 d5 ec 00 50 83 a1 c6 3a 5c 01 14 3d 80 18 .....P...: \...=  
0030 02 00 ff e4 00 00 01 01 08 0a c8 42 44 52 fb 4a .....BDR-J  
0040 e0 09 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..GET / HTTP/1.1  
0050 0d 0a 48 6f 73 74 3a 20 6c 69 76 72 61 72 69 61 ..Host: livraria  
0060 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ..User-A gent: Mo  
0070 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 zilla/5.0 (X11;  
0080 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 20 78 38 Ubuntu; Linux x8  
0090 36 5f 36 34 3b 20 72 76 3a 31 30 39 2e 30 29 20 6\_64; rv :109.0)  
00a0 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 Gecko/20100101 F  
00b0 69 72 65 66 6f 78 2f 31 31 33 2e 30 0d 0a 41 63 irefox/1.13.0. Ac



The screenshot shows the Wireshark interface with a packet capture on interface 'lo'. The packet list shows four packets, with packet 313 selected. The packet details pane shows the structure of the selected packet, and the packet bytes pane shows the raw data in hexadecimal and ASCII.

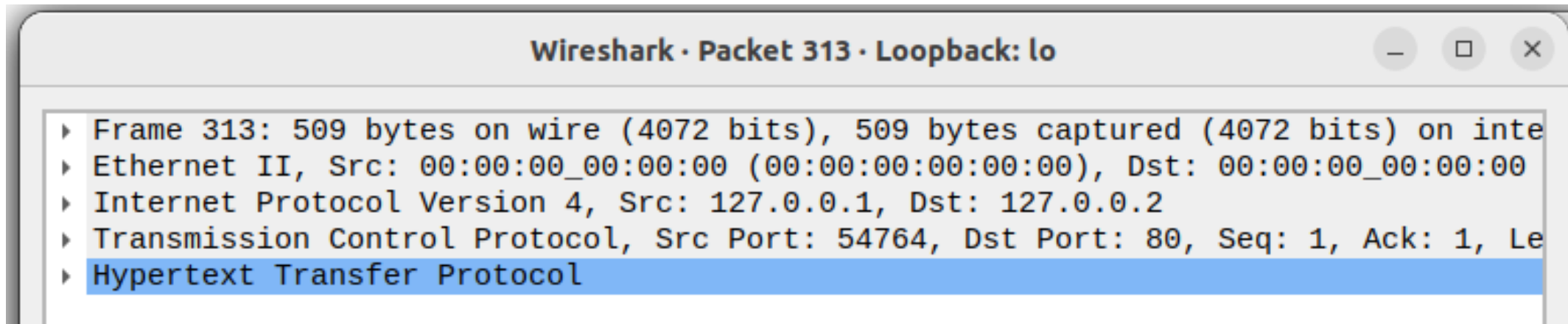
Wireshark - Packet 313 - Loopback: lo

Frame 313: 509 bytes on wire (4072 bits), 509 bytes captured (4072 bits) on interface lo, id 0  
Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.2  
Transmission Control Protocol, Src Port: 54764, Dst Port: 80, Seq: 1, Ack: 1, Len: 443  
Hypertext Transfer Protocol

0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E.  
0010 01 ef d8 ce 40 00 40 06 62 37 7f 00 00 01 7f 00 ....@. b7.....  
0020 00 02 d5 ec 00 50 83 a1 c6 3a 5c 01 14 3d 80 18 .....P...: \...=  
0030 02 00 ff e4 00 00 01 01 08 0a c8 42 44 52 fb 4a .....BDR-J  
0040 e0 09 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..GET / HTTP/1.1  
0050 0d 0a 48 6f 73 74 3a 20 6c 69 76 72 61 72 69 61 ..Host: livraria  
0060 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ..User-A gent: Mo  
0070 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 zilla/5.0 (X11;  
0080 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 20 78 38 Ubuntu; Linux x8  
0090 36 5f 36 34 3b 20 72 76 3a 31 30 39 2e 30 29 20 6\_64; rv :109.0)  
00a0 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 Gecko/20100101 F  
00b0 69 72 65 66 6f 78 2f 31 31 33 2e 30 0d 0a 41 63 irefox/1.13.0. Ac

No.: 313 · Time: 35.528182862 · Source: 127.0.0.1 · Destination: 127.0.0.2 · Protocol: HTTP · Length: 509 · Info: GET / HTTP/1.1

# PILHA DE PROTOCOLOS – TCP/IP



Camadas

0- Física

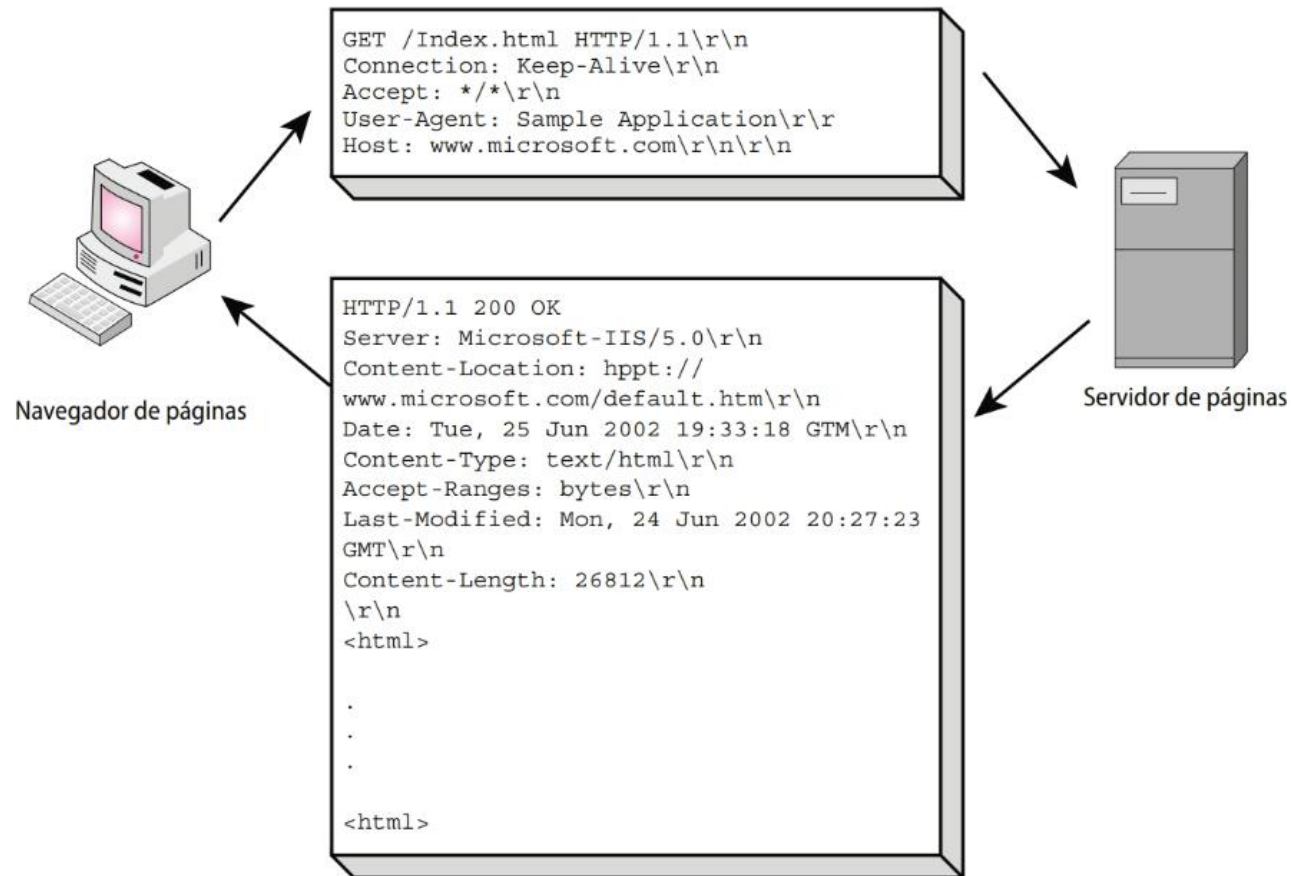
1- Enlace

2- Rede

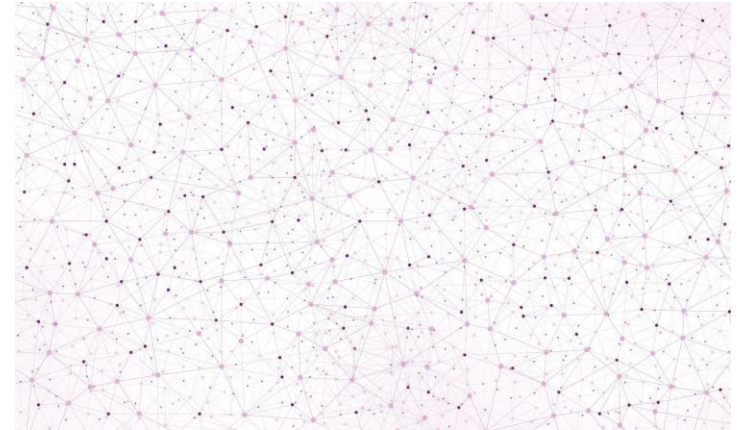
3- Transporte

**4- Aplicação**

# LEMBRANDO DA COMUNICAÇÃO CLIENTE-SERVIDOR...



# LADO CLIENTE





# ANALISANDO O PROTOCOLO IP

Wireshark · Packet 313 · Loopback: lo

- ▶ Frame 313: 509 bytes on wire (4072 bits), 509 bytes captured (4072 bits) on interface lo, id 0
- ▶ Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)

## Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.2

0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 495  
Identification: 0xd8ce (55502)  
▶ Flags: 0x40, Don't fragment  
...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 64  
Protocol: TCP (6)  
Header Checksum: 0x6237 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 127.0.0.1  
Destination Address: 127.0.0.2

- ▶ Transmission Control Protocol, Src Port: 54764, Dst Port: 80, Seq: 1, Ack: 1, Len: 443

## Hypertext Transfer Protocol

0000	00 00 00 00 00 00 00 00	00 00 00 00 08 00 45 00	.....E.
0010	01 ef d8 ce 40 00 40 06	62 37 7f 00 00 01 7f 00	....@.@. b7.....
0020	00 02 d5 ec 00 50 83 a1	c6 3a 5c 01 14 3d 80 18	....P.. :\.=..
0030	02 00 ff e4 00 00 01 01	08 0a c8 42 44 52 fb 4a	.....BDR.J
0040	e0 09 47 45 54 20 2f 20	48 54 54 50 2f 31 2e 31	..GET / HTTP/1.1
0050	0d 0a 48 6f 73 74 3a 20	6c 69 76 72 61 72 69 61	..Host: livraria
0060	0d 0a 55 73 65 72 2d 41	67 65 6e 74 3a 20 4d 6f	..User-Agent: Mo
0070	7a 69 6c 6c 61 2f 35 2e	30 20 28 58 31 31 3b 20	zilla/5.0 (X11;
0080	55 62 75 6e 74 75 3b 20	4c 69 6e 75 78 20 78 38	Ubuntu; Linux x8
0090	36 5f 36 34 3b 20 72 76	3a 31 30 39 2e 30 29 20	6_64; rv :109.0)

...

▶ Frame 313: 509 bytes on wire (4072 bits), 509 bytes captured (4072 bits) on interface lo, id 0  
 ▶ Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
 ▼ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.2  
     0100 .... = Version: 4  
     .... 0101 = Header Length: 20 bytes (5)  
     ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
         Total Length: 495  
         Identification: 0xd8ce (55502)  
     ▶ Flags: 0x40, Don't fragment  
         ...0 0000 0000 0000 = Fragment Offset: 0  
         Time to Live: 64  
         Protocol: TCP (6)  
         Header Checksum: 0x6237 [validation disabled]  
         [Header checksum status: Unverified]  
         Source Address: 127.0.0.1  
         Destination Address: 127.0.0.2  
 ▶ Transmission Control Protocol, Src Port: 54764, Dst Port: 80, Seq: 1, Ack: 1, Len: 443

▶ Hypertext Transfer Protocol

0040	e0 09 47 45 54 20 2f 20	48 54 54 50 2f 31 2e 31	..GET / HTTP/1.1
0050	0d 0a 48 6f 73 74 3a 20	6c 69 76 72 61 72 69 61	..Host: livraria
0060	0d 0a 55 73 65 72 2d 41	67 65 6e 74 3a 20 4d 6f	..User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/2010101 Firefox/13.0
0070	7a 69 6c 6c 61 2f 35 2e	30 20 28 58 31 31 3b 20	cept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
0080	55 62 75 6e 74 75 3b 20	4c 69 6e 75 78 20 78 38	..Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
0090	36 5f 36 34 3b 20 72 76	3a 31 30 39 2e 30 29 20	..Accept-Encoding: gzip, deflate
00a0	47 65 63 6b 6f 2f 32 30	31 30 30 31 30 31 20 46	..Connection: keep-alive
00b0	69 72 65 66 6f 78 2f 31	31 33 2e 30 0d 0a 41 63	..Upgrade: Insecure-Request: 1
00c0	63 65 70 74 3a 20 74 65	78 74 2f 68 74 6d 6c 2c	..If-Modified-Since: Sat, 29 Jul 2023 02:07:31 GMT
00d0	61 70 70 6c 69 63 61 74	69 6f 6e 2f 78 68 74 6d	..Match: w/"64c47463-77"
00e0	6c 2b 78 6d 6c 2c 61 70	70 6c 69 63 61 74 69 6f	
00f0	6e 2f 78 6d 6c 3b 71 3d	30 2e 39 2c 69 6d 61 67	
0100	65 2f 61 76 69 66 2c 69	6d 61 67 65 2f 77 65 62	
0110	70 2c 2a 2f 2a 3b 71 3d	30 2e 38 0d 0a 41 63 63	
0120	65 70 74 2d 4c 61 6e 67	75 61 67 65 3a 20 70 74	
0130	2d 42 52 2c 70 74 3b 71	3d 30 2e 38 2c 65 6e 2d	
0140	55 53 3b 71 3d 30 2e 35	2c 65 6e 3b 71 3d 30 2e	
0150	33 0d 0a 41 63 63 65 70	74 2d 45 6e 63 6f 64 69	
0160	6e 67 3a 20 67 7a 69 70	2c 20 64 65 66 6c 61 74	
0170	65 0d 0a 43 6f 6e 6e 65	63 74 69 6f 6e 3a 20 6b	
0180	65 65 70 2d 61 6c 69 76	65 0d 0a 55 70 67 72 61	
0190	64 65 2d 49 6e 73 65 63	75 72 65 2d 52 65 71 75	
01a0	65 73 74 73 3a 20 31 0d	0a 49 66 2d 4d 6f 64 69	
01b0	66 69 65 64 2d 53 69 6e	63 65 3a 20 53 61 74 2c	
01c0	20 32 39 20 4a 75 6c 20	32 30 32 33 20 30 32 3a	
01d0	30 37 3a 33 31 20 47 4d	54 0d 0a 49 66 2d 4e 6f	
01e0	6e 65 2d 4d 61 74 63 68	3a 20 57 2f 22 36 34 63	
01f0	34 37 34 36 33 2d 37 37	22 0d 0a 0d 0a	

# ANALISANDO O PROTOCOLO TCP

Wireshark · Packet 313 · Loopback: lo

Transmission Control Protocol, Src Port: 54764, Dst Port: 80, Seq: 1, Ack: 1, Len: 443

- Source Port: 54764
- Destination Port: 80
- [Stream index: 3]
- [Conversation completeness: Incomplete, DATA (15)]
- [TCP Segment Len: 443]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 2208417338
- [Next Sequence Number: 444 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 1543574589
- 1000 ... = Header Length: 32 bytes (8)
- Flags: 0x018 (PSH, ACK)
- Window: 512
- [Calculated window size: 65536]
- [Window size scaling factor: 128]
- Checksum: 0xffe4 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (443 bytes)

Hypertext Transfer Protocol

0040	e0 09 47 45 54 20 2f 20	48 54 54 50 2f 31 2e 31	..GET / HTTP/1.1
0050	0d 0a 48 6f 73 74 3a 20	6c 69 76 72 61 72 69 61	..Host: livraria
0060	0d 0a 55 73 65 72 2d 41	67 65 6e 74 3a 20 4d 6f	..User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/2010101 Firefox/13.0
0070	7a 69 6c 6c 61 2f 35 2e	30 20 28 58 31 31 3b 20	..Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
0080	55 62 75 6e 74 75 3b 20	4c 69 6e 75 78 20 78 38	..Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
0090	36 5f 36 34 3b 20 72 76	3a 31 30 39 2e 30 29 20	..Accept-Encoding: gzip, deflate
00a0	47 65 63 6b 6f 2f 32 30	31 30 30 31 30 31 20 46	..Connection: keep-alive
00b0	69 72 65 66 6f 78 2f 31	31 33 2e 30 0d 0a 41 63	..Upgrade: Insecure-Request
00c0	63 65 70 74 3a 20 74 65	78 74 2f 68 74 6d 6c 2c	..If-Modified-Since: Sat, 29 Jul 2023 02:07:31 GMT
00d0	61 70 70 6c 69 63 61 74	69 6f 6e 2f 78 68 74 6d	..If-None-Match: W/"64c47463-77"
00e0	6c 2b 78 6d 6c 2c 61 70	70 6c 69 63 61 74 69 6f	..
00f0	6e 2f 78 6d 6c 3b 71 3d	30 2e 39 2c 69 6d 61 67	..
0100	65 2f 61 76 69 66 2c 69	6d 61 67 65 2f 77 65 62	..
0110	70 2c 2a 2f 2a 3b 71 3d	30 2e 38 0d 0a 41 63 63	..
0120	65 70 74 2d 4c 61 6e 67	75 61 67 65 3a 20 70 74	..
0130	2d 42 52 2c 70 74 3b 71	3d 30 2e 38 2c 65 6e 2d	..
0140	55 53 3b 71 3d 30 2e 35	2c 65 6e 3b 71 3d 30 2e	..
0150	33 0d 0a 41 63 63 65 70	74 2d 45 6e 63 6f 64 69	..
0160	6e 67 3a 20 67 7a 69 70	2c 20 64 65 66 6c 61 74	..
0170	65 0d 0a 43 6f 6e 6e 65	63 74 69 6f 6e 3a 20 6b	..
0180	65 65 70 2d 61 6c 69 76	65 0d 0a 55 70 67 72 61	..
0190	64 65 2d 49 6e 73 65 63	75 72 65 2d 52 65 71 75	..
01a0	65 73 74 73 3a 20 31 0d	0a 49 66 2d 4d 6f 64 69	..
01b0	66 69 65 64 2d 53 69 6e	63 65 3a 20 53 61 74 2c	..
01c0	20 32 39 20 4a 75 6c 20	32 30 32 33 20 30 32 3a	..
01d0	30 37 3a 33 31 20 47 4d	54 0d 0a 49 66 2d 4e 6f	..
01e0	6e 65 2d 4d 61 74 63 68	3a 20 57 2f 22 36 34 63	..
01f0	34 37 34 36 33 2d 37 37	22 0d 0a 0d 0a	..

Help Close



# ANALISANDO O PROTOCOLO HTTP

Wireshark - Packet 313 - Loopback: lo

...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 64  
Protocol: TCP (6)  
Header Checksum: 0x6237 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 127.0.0.1  
Destination Address: 127.0.0.2

Transmission Control Protocol, Src Port: 54764, Dst Port: 80, Seq: 1, Ack: 1, Len: 443

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n  
Host: livraria\r\n  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/113.0\r\n  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8\r\n  
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3\r\n  
Accept-Encoding: gzip, deflate\r\n  
Connection: keep-alive\r\n  
Upgrade-Insecure-Requests: 1\r\n  
If-Modified-Since: Sat, 29 Jul 2023 02:07:31 GMT\r\n  
If-None-Match: W/"64c47463-77"\r\n  
\r\n  
[Full request URI: http://livraria/]  
[HTTP request 1/1]  
[Response in frame: 315]

Offset	Hex	ASCII
0040	e0 09 47 45 54 20 2f 20	..GET / HTTP/1.1
0050	0d 0a 48 6f 73 74 3a 20	..Host: livraria
0060	0d 0a 55 73 65 72 2d 41	..User-Agent: Mo
0070	7a 69 6c 6c 61 2f 35 2e	zilla/5.0 (X11;
0080	55 62 75 6e 74 75 3b 20	Ubuntu; Linux x8
0090	36 5f 36 34 3b 20 72 76	6_64; rv:109.0)
00a0	47 65 63 6b 6f 2f 32 30	Gecko/20100101 F
00b0	69 72 65 66 6f 78 2f 31	firefox/113.0. Ac
00c0	63 65 70 74 3a 20 74 65	cept: text/html,
00d0	61 70 70 6c 69 63 61 74	applicat ion/xhtm
00e0	6c 2b 78 6d 6c 2c 61 70	l+xml,ap plicatio
00f0	6e 2f 78 6d 6c 3b 71 3d	n/xml;q= 0.9,imag
0100	65 2f 61 76 69 66 2c 69	e/avif,i mage/web
0110	70 2c 2a 2f 2a 3b 71 3d	p,*/*;q= 0.8..Acc
0120	65 70 74 2d 4c 61 6e 67	ept-Lang uage: pt
0130	2d 42 52 2c 70 74 3b 71	-BR,pt;q =0.8,en-
0140	55 53 3b 71 3d 30 2e 35	US;q=0.5 ,en;q=0.
0150	33 0d 0a 41 63 63 65 70	3..Accep t-Encodi
0160	6e 67 3a 20 67 7a 69 70	ng: gzip , deflat
0170	65 0d 0a 43 6f 6e 6e 65	e..Conne ction: k
0180	65 65 70 2d 61 6c 69 76	eeep-aliv e..Upgra
0190	64 65 2d 49 6e 73 65 63	de-Insec ure-Requ
01a0	65 73 74 73 3a 20 31 0d	ests: 1..If-Modi
01b0	66 69 65 64 2d 53 69 6e	fied-Sin ce: Sat,
01c0	20 32 39 20 4a 75 6c 20	29 Jul 2023 02:
01d0	30 37 3a 33 31 20 47 4d	07:31 GM T..If-No
01e0	6e 65 2d 4d 61 74 63 68	ne-Match : W/"64c
01f0	34 37 34 36 33 2d 37 37	47463-77 "....

Help Close



# LADO SERVIDOR

# ANALISANDO O PROTOCOLO IP

Wireshark · Packet 315 · Loopback: lo

▶ Frame 315: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface lo, id 0  
▶ Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
▼ Internet Protocol Version 4, Src: 127.0.0.2, Dst: 127.0.0.1  
    0100 .... = Version: 4  
    .... 0101 = Header Length: 20 bytes (5)  
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
        Total Length: 240  
        Identification: 0x3a36 (14902)  
    ▶ Flags: 0x40, Don't fragment  
        ...0 0000 0000 0000 = Fragment Offset: 0  
        Time to Live: 64  
        Protocol: TCP (6)  
        Header Checksum: 0x01cf [validation disabled]  
        [Header checksum status: Unverified]  
        Source Address: 127.0.0.2  
        Destination Address: 127.0.0.1  
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 54764, Seq: 1, Ack: 444, Len: 188  
▶ Hypertext Transfer Protocol

0000	00 00 00 00 00 00 00 00	00 00 00 08 00 45 00	.....E.
0010	00 f0 3a 36 40 00 40 06	01 cf 7f 00 00 02 7f 00	...60@.
0020	00 01 00 50 d5 ec 5c 01	14 3d 83 a1 c7 f5 80 18	...P.\.
0030	02 00 fe e5 00 00 01 01	08 0a fb 4a e0 09 c8 42	.....J...B
0040	44 52 48 54 54 50 2f 31	2e 31 20 33 30 34 20 4e	DRHTTP/1.1 304 N
0050	6f 74 20 4d 6f 64 69 66	69 65 64 0d 0a 53 65 72	ot Modified Ser
0060	76 65 72 3a 20 6e 67 69	6e 78 2f 31 2e 31 38 2e	ver: ngx/1.18.
0070	30 20 28 55 62 75 6e 74	75 29 0d 0a 44 61 74 65	0 (Ubuntu) Date
0080	3a 20 4d 6f 6e 2c 20 33	31 20 4a 75 6c 20 32 30	: Mon, 31 Jul 20
0090	32 33 20 31 34 3a 32 32	3a 30 30 20 47 4d 54 0d	23 14:22 :00 GMT
00a0	0a 4c 61 73 74 2d 4d 6f	64 69 66 69 65 64 3a 20	Last-Modified:
00b0	53 61 74 2c 20 32 39 20	4a 75 6c 20 32 30 32 33	Sat, 29 Jul 2023
00c0	20 30 32 3a 30 37 3a 33	31 20 47 4d 54 0d 0a 43	02:07:31 GMT C
00d0	6f 6e 6e 65 63 74 69 6f	6e 3a 20 6b 65 65 70 2d	onnection: keep-
00e0	61 6c 69 76 65 0d 0a 45	54 61 67 3a 20 22 36 34	alive E Tag: "64
00f0	63 34 37 34 36 33 2d 37	37 22 0d 0a 0d 0a	c47463-7 7"....

Help Close

# ANALISANDO O PROTOCOLO TCP

Wireshark · Packet 315 · Loopback: lo

▶ Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
▶ Internet Protocol Version 4, Src: 127.0.0.2, Dst: 127.0.0.1  
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 54764, Seq: 1, Ack: 444, Len: 188  
    Source Port: 80  
    Destination Port: 54764  
    [Stream index: 3]  
    [Conversation completeness: Incomplete, DATA (15)]  
    [TCP Segment Len: 188]  
    Sequence Number: 1 (relative sequence number)  
    Sequence Number (raw): 1543574589  
    [Next Sequence Number: 189 (relative sequence number)]  
    Acknowledgment Number: 444 (relative ack number)  
    Acknowledgment number (raw): 2208417781  
    1000 .... = Header Length: 32 bytes (8)  
    ▶ Flags: 0x018 (PSH, ACK)  
    Window: 512  
    [Calculated window size: 65536]  
    [Window size scaling factor: 128]  
    Checksum: 0xfe5 [unverified]  
    [Checksum Status: Unverified]  
    Urgent Pointer: 0  
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps  
    ▶ [Timestamps]  
    ▶ [SEQ/ACK analysis]  
    TCP payload (188 bytes)  
▶ Hypertext Transfer Protocol

0000	00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00	...E.
0010	00 f0 3a 36 40 00 40 06 01 cf 7f 00 00 02 7f 00	...6@. .
0020	00 01 00 50 d5 ec 5c 01 14 3d 83 a1 c7 f5 80 18	...P.. =
0030	02 00 fe e5 00 00 01 01 08 0a fb 4a e0 09 c8 42	...J..B
0040	44 52 48 54 54 50 2f 31 2e 31 20 33 30 34 20 4e	DRHTTP/1.1 304 N
0050	6f 74 20 4d 6f 64 69 66 69 65 64 0d 0a 53 65 72	ot Modif ied Ser
0060	76 65 72 3a 20 6e 67 69 6e 78 2f 31 2e 31 38 2e	ver: ngi nx/1.18.
0070	30 20 28 55 62 75 6e 74 75 29 0d 0a 44 61 74 65	0 (Ubunt u) Date
0080	3a 20 4d 6f 6e 2c 20 33 31 20 4a 75 6c 20 32 30	: Mon, 3 1 Jul 20
0090	32 33 20 31 34 3a 32 32 3a 30 30 20 47 4d 54 0d	23 14:22 :00 GMT
00a0	0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20	Last-Mo dified:
00b0	53 61 74 2c 20 32 39 20 4a 75 6c 20 32 30 32 33	Sat, 29 Jul 2023
00c0	20 30 32 3a 30 37 3a 33 31 20 47 4d 54 0d 0a 43	02:07:3 1 GMT C
00d0	6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d	onnectio n: keep-
00e0	61 6c 69 76 65 0d 0a 45 54 61 67 3a 20 22 36 34	alive E Tag: "64
00f0	63 34 37 34 36 33 2d 37 37 22 0d 0a 0d 0a	c47463-7 7"...

Help Close

# ANALISANDO O PROTOCOLO HTTP

Wireshark · Packet 315 · Loopback: lo

▶ Frame 315: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface lo, id 0  
▶ Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)  
▶ Internet Protocol Version 4, Src: 127.0.0.2, Dst: 127.0.0.1  
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 54764, Seq: 1, Ack: 444, Len: 188  
▶ Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n  
Server: nginx/1.18.0 (Ubuntu)\r\n  
Date: Mon, 31 Jul 2023 14:22:00 GMT\r\n  
Last-Modified: Sat, 29 Jul 2023 02:07:31 GMT\r\n  
Connection: keep-alive\r\n  
ETag: "64c47463-77"\r\n  
\r\n  
[HTTP response 1/1]  
[Time since request: 0.000163606 seconds]  
[\[Request in frame: 313\]](#)  
[Request URI: http://livraria/]

0000	00 00 00 00 00 00 00 00 00 00 00 08 00 45 00	.....E:
0010	00 f0 3a 36 40 00 40 06 01 cf 7f 00 00 02 7f 00	...6@-@.....
0020	00 01 00 50 d5 ec 5c 01 14 3d 83 a1 c7 f5 80 18	...P...\r\n=.....
0030	02 00 fe e5 00 00 01 01 08 0a fb 4a e0 09 c8 42	.....J...B
0040	44 52 48 54 54 50 2f 31 2e 31 20 33 30 34 20 4e	DRHTTP/1 .1 304 N
0050	6f 74 20 4d 6f 64 69 66 69 65 64 0d 0a 53 65 72	ot Modif ied..Ser
0060	76 65 72 3a 20 6e 67 69 6e 78 2f 31 2e 31 38 2e	ver: ngi nx/1.18.
0070	30 20 28 55 62 75 6e 74 75 29 0d 0a 44 61 74 65	0 (Ubunt u)..Date
0080	3a 20 4d 6f 6e 2c 20 33 31 20 4a 75 6c 20 32 30	: Mon, 3 1 Jul 20
0090	32 33 20 31 34 3a 32 32 3a 30 30 20 47 4d 54 0d	23 14:22 :00 GMT.
00a0	0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20	..Last-Mo dified:
00b0	53 61 74 2c 20 32 39 20 4a 75 6c 20 32 30 32 33	Sat, 29 Jul 2023
00c0	20 30 32 3a 30 37 3a 33 31 20 47 4d 54 0d 0a 43	02:07:3 1 GMT..C
00d0	6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d	onnectio n: keep-
00e0	61 6c 69 76 65 0d 0a 45 54 61 67 3a 20 22 36 34	alive..E Tag: "64
00f0	63 34 37 34 36 33 2d 37 37 22 0d 0a 0d 0a	c47463-7 7"....

Help Close

# MÃOS A OBRA

- Agora é a sua vez...
  - No Wireshark analise o que acontece quando você solicita uma página do seu servidor Nginx
    - A página pode ser dos domínios locais construídos na aula de instalação do Nginx: **loja** ou **restaurante**
    - Monte um relatório e envie no Moodle para a professora

# REFERÊNCIAS

- <https://www.techtudo.com.br/noticias/2012/09/como-usar-o-wireshark.ghhtml>
- <https://gitlab.com/wireshark/wireshark/-/blob/master/packaging/debian/README.Debian>
- Guia Foca Linux – Interface de rede. Acesso em 31 de julho de 2023. Disponível por www em: <https://www.guiafoca.org/guiaonline/avancado/ch04s04.html>
- SCHMITT, Marcelo A R.; PERES, André; LOUREIRO, César A H. **Redes de computadores**: nível de aplicação e instalação de serviços. (Tekne). Porto Alegre: Grupo A, 2013. E-book. ISBN 9788582600948. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788582600948/>. Acesso em: 01 ago. 2023.
- **Wireshark** = <https://www.youtube.com/watch?v=7NzEMeLi7A0>