

## Etapa 2

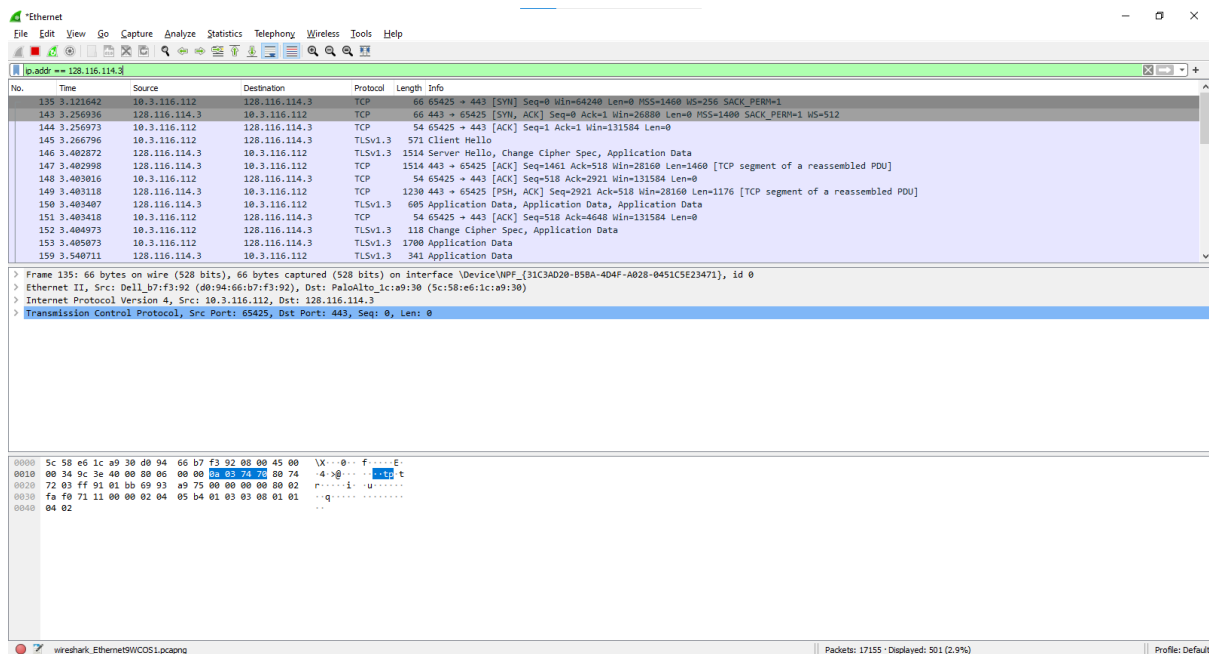
1. Com Wireshark ativo (Abra-o novamente) faça um ping para um site conhecido (você pode usar o nome: www.google.br por exemplo):

```
C:\Users\nicolas_alvarenga>ping web.roblox.com

Disparando us-central-bd1.roblox.com [128.116.114.3] com 32 bytes de dados:
Esgotado o tempo limite do pedido.
Resposta de 128.116.114.3: bytes=32 tempo=135ms TTL=53
Esgotado o tempo limite do pedido.
Resposta de 128.116.114.3: bytes=32 tempo=134ms TTL=53

Estatísticas do Ping para 128.116.114.3:
    Pacotes: Enviados = 4, Recebidos = 2, Perdidos = 2 (50% de
    perda),
    Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 134ms, Máximo = 135ms, Média = 134ms
```

2. Teste outros filtros, por exemplo, mostre somente pacotes originados e/ou destinados a um determinado host (ip.addr == 192.168..., ip.src, ip.dst).  
ip.addr:



ip.src:

No.	Time	Source	Destination	Protocol	Length	Info
133	3.121642	10.3.116.112	128.116.114.3	TCP	66	65425 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
144	3.256973	10.3.116.112	128.116.114.3	TCP	54	65425 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
145	3.266796	10.3.116.112	128.116.114.3	TLSv1.3	571	Client Hello
148	3.403016	10.3.116.112	128.116.114.3	TCP	54	65425 → 443 [ACK] Seq=518 Ack=2921 Win=131584 Len=0
151	3.403418	10.3.116.112	128.116.114.3	TCP	54	65425 → 443 [ACK] Seq=518 Ack=4648 Win=131584 Len=0
152	3.404973	10.3.116.112	128.116.114.3	TLSv1.3	118	Change Cipher Spec, Application Data
153	3.405073	10.3.116.112	128.116.114.3	TLSv1.3	1700	Application Data
162	3.540755	10.3.116.112	128.116.114.3	TCP	54	65425 → 443 [ACK] Seq=2228 Ack=5222 Win=130816 Len=0
167	3.606118	10.3.116.112	128.116.114.3	TCP	54	65425 → 443 [ACK] Seq=2228 Ack=5723 Win=130816 Len=0
157	9.166973	10.3.116.112	128.116.114.3	TLSv1.2	89	Application Data
158	9.166116	10.3.116.112	128.116.114.3	TLSv1.2	89	Application Data
157	9.566807	10.3.116.112	128.116.114.3	TLSv1.3	1657	Application Data
159	9.765435	10.3.116.112	128.116.114.3	TCP	54	65425 → 443 [ACK] Seq=3831 Ack=6225 Win=131584 Len=0

> Frame 135: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on Interface \Device\NPF\_{31C3AD20-B5BA-4D4F-A028-0451C5E23471}, id 0  
 > Ethernet II, Src: Dell\_b7:f3:92 (d0:94:66:b7:f3:92), Dst: PaloAlto\_ic:a9:30 (5c:58:e6:1c:a9:30)  
 > Internet Protocol Version 4, Src: 10.3.116.112, Dst: 128.116.114.3  
 > Transmission Control Protocol, Src Port: 65425, Dst Port: 443, Seq: 0, Len: 0

```

0000  5c 58 e6 1c a9 30 d0 94 66 b7 f3 92 08 00 45 00  \X...f.....E
0010  00 34 9c 3e 40 00 00 00 00 00 0a 03 74 70 80 74  -4>@3...tpt
0020  72 03 ff 91 01 bb 69 93 a9 75 00 00 00 00 00 02  r...i...u...
0030  fa f0 71 11 00 00 02 04 05 b4 01 03 08 01 01    ..q.....x...
0040  04 02
  
```

ip.dst:

No.	Time	Source	Destination	Protocol	Length	Info
142	3.403959	128.116.114.3	10.3.116.112	TCP	60	443 → 65425 [SYN, ACK] Seq=0 Ack=1 Win=28160 Len=0 MSS=1460 SACK_PERM=1 WS=512
146	3.402872	128.116.114.3	10.3.116.112	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
147	3.402998	128.116.114.3	10.3.116.112	TCP	1514	443 → 65425 [ACK] Seq=1461 Ack=518 Win=28160 Len=1460 [TCP segment of a reassembled PDU]
149	3.403118	128.116.114.3	10.3.116.112	TCP	1230	443 → 65425 [PSH, ACK] Seq=2921 Ack=518 Win=28160 Len=1176 [TCP segment of a reassembled PDU]
150	3.403407	128.116.114.3	10.3.116.112	TLSv1.3	605	Application Data, Application Data
159	3.540711	128.116.114.3	10.3.116.112	TLSv1.3	341	Application Data
160	3.540711	128.116.114.3	10.3.116.112	TLSv1.3	341	Application Data
161	3.540711	128.116.114.3	10.3.116.112	TCP	60	443 → 65425 [ACK] Seq=5222 Ack=2228 Win=33792 Len=0
163	3.550946	128.116.114.3	10.3.116.112	TLSv1.3	555	Application Data
156	9.165674	128.116.114.3	10.3.116.112	TLSv1.2	89	Application Data
167	9.308087	128.116.114.3	10.3.116.112	TCP	60	443 → 65379 [ACK] Seq=36 Ack=71 Win=77 Len=0
158	9.702201	128.116.114.3	10.3.116.112	TCP	60	443 → 65425 [ACK] Seq=5723 Ack=3831 Win=39424 Len=0
159	9.722019	128.116.114.3	10.3.116.112	TLSv1.3	556	Application Data

> Frame 143: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{31C3AD20-B5BA-4D4F-A028-0451C5E23471}, id 0  
 > Ethernet II, Src: PaloAlto\_ic:a9:30 (5c:58:e6:1c:a9:30), Dst: Dell\_b7:f3:92 (d0:94:66:b7:f3:92)  
 > Internet Protocol Version 4, Src: 128.116.114.3, Dst: 10.3.116.112  
 > Transmission Control Protocol, Src Port: 443, Dst Port: 65425, Seq: 0, Ack: 1, Len: 0

```

0000  d0 94 66 b7 f3 92 5c 58 e6 1c a9 30 08 00 45 00  \X...f.....E
0010  00 34 00 00 40 00 33 06 d6 d9 80 74 72 03 0a 03  -4>@3...tpt...
0020  74 70 01 0b ff 91 58 9c 5c 68 69 93 a9 76 80 12  tp...X\hi...v...
0030  69 00 c0 f4 00 00 02 04 05 78 01 01 04 02 01 03  i.....x.....
0040  03 09
  
```

3. Qual é o endereço IP do sítio navegado? Qual é o endereço IP da interface de rede do seu computador? Qual o endereço MAC de sua máquina?  
 R: O endereço IP do site navegado é 128.116.114.3  
 O endereço IP da interface de rede do meu computador é 10.3.116.112  
 O endereço MAC da minha máquina é **d0:94:66:b7:f3:92**

4. Selecione no mínimo 3 mensagens de protocolos diferentes e explique os campos da forma mais detalhada que conseguir.

PACOTE 23392:

Hora da chegada do pacote:

Arrival Time: Sep 19, 2022 11:55:49.213408000 Hora oficial do Brasil

PACOTE 10254

Nome e MAC (Respectivamente) do dispositivo de fonte:

**Dell\_b7:f3:92 (d0:94:66:b7:f3:92)**

PACOTE 23398

Tamanho da captura:

Frame Length: 182 bytes (1456 bits)

### ETAPA 3-

1. Encontre um endereço IP de um outro dispositivo da sua rede e faça um experimento para descobrir o endereço MAC do computador dele.

IP do outro dispositivo na minha rede:

10.3.117.88

Endereço MAC:

5c:58:e6:1c:a9:30