

Laboratório ICMP Wireshark  
Alunos: Eduardo Henrique

```
caiohps@caio-hps:~  
zsh: corrupt history file /home/caiohps/.zsh_history  
→ ~ ping -c 10 www.google.com  
zsh: corrupt history file /home/caiohps/.zsh_history  
→ ~ ping -c 10 www.google.com  
PING www.google.com (142.251.132.228) 56(84) bytes of data.  
64 bytes from gru14s46-in-f4.1e100.net (142.251.132.228): icmp_seq  
=1 ttl=117 time=46.5 ms  
64 bytes from gru14s46-in-f4.1e100.net (142.251.132.228): icmp_seq  
=2 ttl=117 time=35.5 ms  
64 bytes from gru14s46-in-f4.1e100.net (142.251.132.228): icmp_seq  
=3 ttl=117 time=32.2 ms  
64 bytes from gru14s46-in-f4.1e100.net (142.251.132.228): icmp_seq  
=4 ttl=117 time=33.6 ms  
64 bytes from gru14s46-in-f4.1e100.net (142.251.132.228): icmp_seq  
=5 ttl=117 time=36.8 ms  
64 bytes from gru14s46-in-f4.1e100.net (142.251.132.228): icmp_seq  
=6 ttl=117 time=38.6 ms  
64 bytes from gru14s46-in-f4.1e100.net (142.251.132.228): icmp_seq  
=7 ttl=117 time=32.3 ms  
64 bytes from gru14s46-in-f4.1e100.net (142.251.132.228): icmp_seq  
=8 ttl=117 time=36.4 ms  
64 bytes from gru14s46-in-f4.1e100.net (142.251.132.228): icmp_seq  
=9 ttl=117 time=37.7 ms  
64 bytes from gru14s46-in-f4.1e100.net (142.251.132.228): icmp_seq  
=10 ttl=117 time=36.8 ms  
  
--- www.google.com ping statistics ---  
10 packets transmitted, 10 received, 0% packet loss, time 901ms  
rtt min/avg/max/mdev = 32.231/36.636/46.490/3.886 ms  
→ ~ █
```

Terminal do Linux comando para capturar os ICMP.

1) Qual é o endereço IP do seu host? Qual é o endereço IP do destino?

● IPdoHost(Origem):192.168.3.4

● IPdoDestino:142.251.132.228

The image shows a Wireshark packet capture of ICMP Echo (ping) traffic. The packet list on the left shows a series of requests and replies. A red '4' is written over the packet list, likely indicating the fourth packet in the sequence. The packet details pane on the right shows the structure of the selected packet (Frame 2609), including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol.

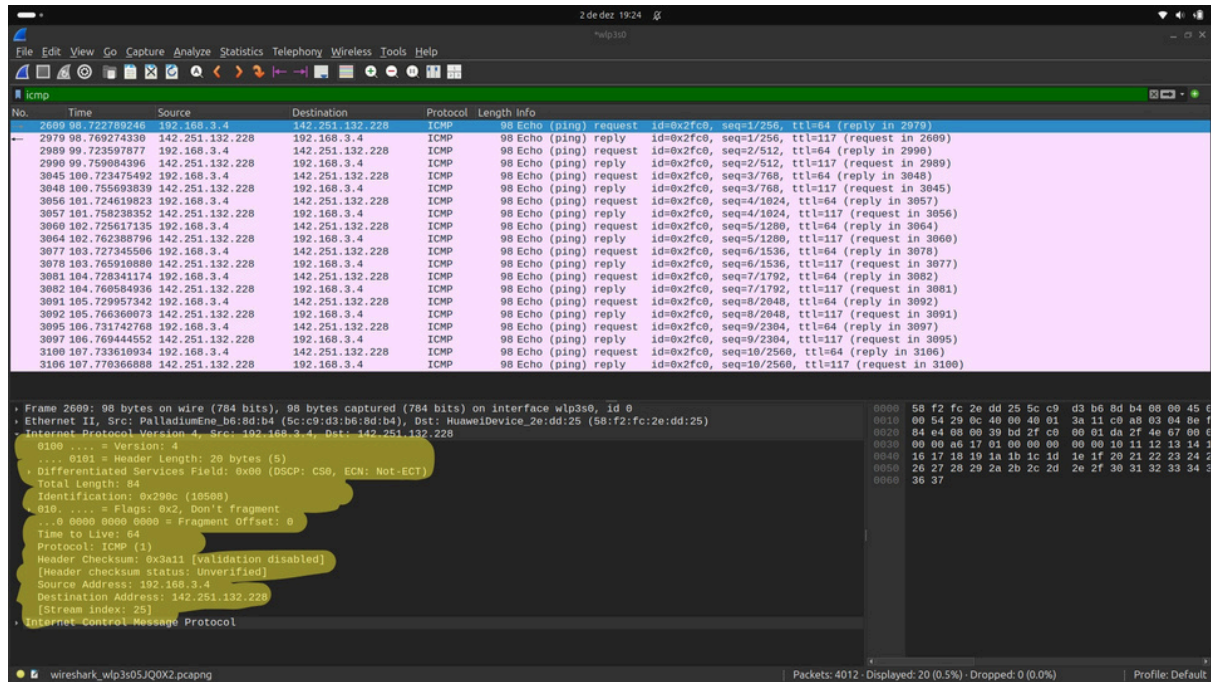
No.	Time	Source	Destination	Protocol	Length	Info
2609	98.72270244	192.168.3.4	142.251.132.228	ICMP	98	Echo (ping) request id=0x2fc0, seq=1/256, ttl=64 (reply in 2979)
2979	98.769274339	142.251.132.228	192.168.3.4	ICMP	98	Echo (ping) reply id=0x2fc0, seq=1/256, ttl=117 (request in 2609)
2989	99.723597877	192.168.3.4	142.251.132.228	ICMP	98	Echo (ping) request id=0x2fc0, seq=2/512, ttl=64 (reply in 2990)
2990	99.759084396	142.251.132.228	192.168.3.4	ICMP	98	Echo (ping) reply id=0x2fc0, seq=2/512, ttl=117 (request in 2989)
3045	100.723475492	192.168.3.4	142.251.132.228	ICMP	98	Echo (ping) request id=0x2fc0, seq=3/768, ttl=64 (reply in 3048)
3048	100.755693839	142.251.132.228	192.168.3.4	ICMP	98	Echo (ping) reply id=0x2fc0, seq=3/768, ttl=117 (request in 3045)
3056	101.724619823	192.168.3.4	142.251.132.228	ICMP	98	Echo (ping) request id=0x2fc0, seq=4/1024, ttl=64 (reply in 3057)
3057	101.758238352	142.251.132.228	192.168.3.4	ICMP	98	Echo (ping) reply id=0x2fc0, seq=4/1024, ttl=117 (request in 3056)
3060	102.725617135	192.168.3.4	142.251.132.228	ICMP	98	Echo (ping) request id=0x2fc0, seq=5/1280, ttl=64 (reply in 3064)
3064	102.762380796	142.251.132.228	192.168.3.4	ICMP	98	Echo (ping) reply id=0x2fc0, seq=5/1280, ttl=117 (request in 3060)
3077	103.727345596	192.168.3.4	142.251.132.228	ICMP	98	Echo (ping) request id=0x2fc0, seq=6/1536, ttl=64 (reply in 3078)
3078	103.765910880	142.251.132.228	192.168.3.4	ICMP	98	Echo (ping) reply id=0x2fc0, seq=6/1536, ttl=117 (request in 3077)
3081	104.728341174	192.168.3.4	142.251.132.228	ICMP	98	Echo (ping) request id=0x2fc0, seq=7/1792, ttl=64 (reply in 3082)
3082	104.766584936	142.251.132.228	192.168.3.4	ICMP	98	Echo (ping) reply id=0x2fc0, seq=7/1792, ttl=117 (request in 3081)
3091	105.729957342	192.168.3.4	142.251.132.228	ICMP	98	Echo (ping) request id=0x2fc0, seq=8/2048, ttl=64 (reply in 3092)
3092	105.766360073	142.251.132.228	192.168.3.4	ICMP	98	Echo (ping) reply id=0x2fc0, seq=8/2048, ttl=117 (request in 3091)
3095	106.731742768	192.168.3.4	142.251.132.228	ICMP	98	Echo (ping) request id=0x2fc0, seq=9/2304, ttl=64 (reply in 3097)
3097	106.769444552	142.251.132.228	192.168.3.4	ICMP	98	Echo (ping) reply id=0x2fc0, seq=9/2304, ttl=117 (request in 3095)
3100	107.733610924	192.168.3.4	142.251.132.228	ICMP	98	Echo (ping) request id=0x2fc0, seq=10/2560, ttl=64 (reply in 3100)
3100	107.770366888	142.251.132.228	192.168.3.4	ICMP	98	Echo (ping) reply id=0x2fc0, seq=10/2560, ttl=117 (request in 3100)

Frame 2609: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp3s0, id 0  
Ethernet II, Src: PalladiumEne\_b6:8d:b4 (5c:c9:d3:b6:8d:b4), Dst: HuaweiDevice\_2e:dd:25 (58:f2:fc:2e:dd:25)  
Internet Protocol Version 4, Src: 192.168.3.4, Dst: 142.251.132.228  
Internet Control Message Protocol

Packets: 4012 · Displayed: 20 (0.5%) · Dropped: 0 (0.0%) · Profile: Default

2) Por que um pacote ICMP não tem porta de origem e destino números?

Pacotes ICMP não têm portas de origem e destino porque o protocolo ICMP opera na camada de rede (camada 3 do modelo OSI), e não na camada de transporte (camada 4). Seu propósito é exclusivamente transmitir mensagens de controle e diagnóstico relacionadas ao funcionamento da rede, como requisições de eco (ping) ou mensagens de erro, que não estão associadas a conexões específicas entre aplicações.



Note que há campos como **Type**, **Code**, **Checksum**, **Identifier** e **Sequence Number**, mas nenhum campo relacionado a portas (como haveria em TCP ou UDP).

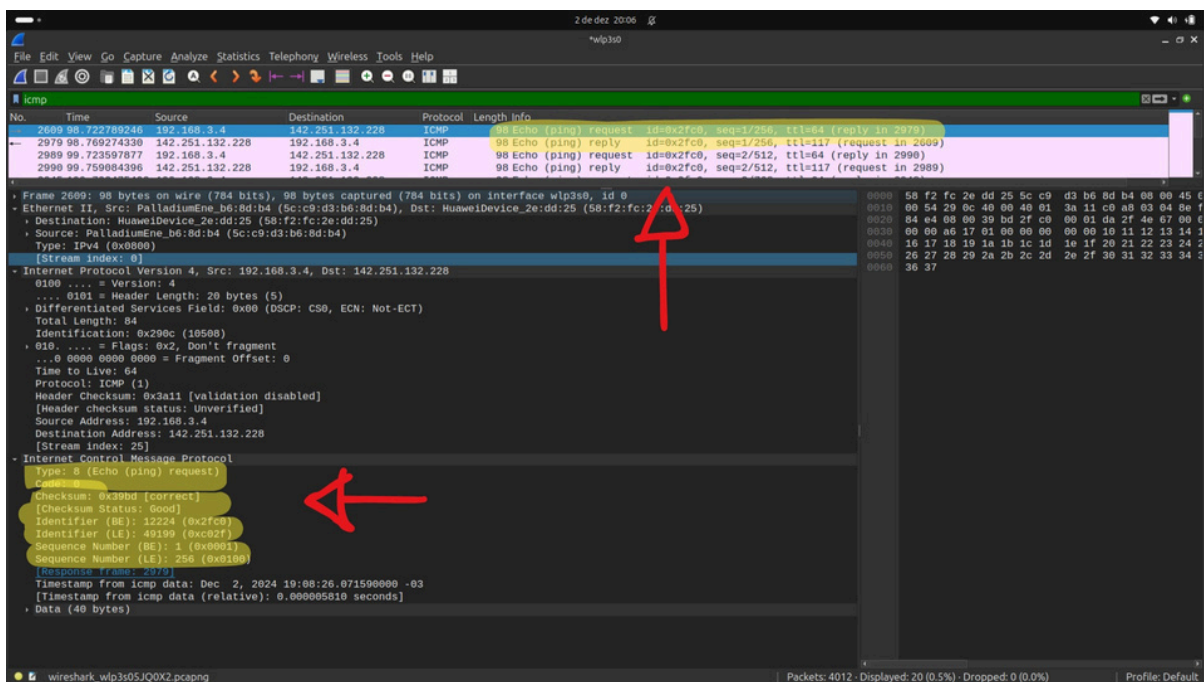
3) Examine um dos pacotes de solicitação de ping enviados pelo seu host. Quais são os tipos e números de código do ICMP? Quais outros campos esse pacote ICMP tem? Quantos bytes são os campos de checksum, número de sequência e identificador?

● **Tipo e Código ICMP:**

- Tipo:8(EchoRequest).
- Código:0.

● **Campos no pacote ICMP:**

- Checksum: 2bytes.
- Identifier: 2bytes.
- Sequence Number: 2bytes.
- Data: 40bytes.



4) Examine o pacote de resposta ping correspondente. Quais são os números de código e tipo ICMP? Quais outros campos esse pacote ICMP tem? Quantos bytes são os campos de checksum, número de sequência e identificador?

### Tipo e Código ICMP:

- Tipo:0(EchoReply).
- Código:0.

### Campos no Pacote ICMP:

- Checksum: 2 bytes.
- Identifier: 2 bytes.
- SequenceNumber: 2 bytes.
- Data: 40 bytes.

The image shows a Wireshark packet capture of ICMP Echo (ping) traffic. The packet list at the top shows four packets: two requests and two replies. The packet details pane shows the structure of the IP and ICMP layers for the selected packet (No. 2979). The packet bytes pane shows the raw data.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
2609	98.722789248	192.168.3.4	142.251.132.228	ICMP	98	Echo (ping) request id=0x2fc0, seq=1/256, ttl=64 (reply in 2979)
2979	98.769274330	142.251.132.228	192.168.3.4	ICMP	98	Echo (ping) reply id=0x2fc0, seq=1/256, ttl=117 (request in 2609)
2989	99.723597877	192.168.3.4	142.251.132.228	ICMP	98	Echo (ping) request id=0x2fc0, seq=2/512, ttl=64 (reply in 2990)
2990	99.759084396	142.251.132.228	192.168.3.4	ICMP	98	Echo (ping) reply id=0x2fc0, seq=2/512, ttl=117 (request in 2989)

**Packet Details (No. 2979):**

- Frame 2979: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp350, id 0
- Ethernet II, Src: HuaweiDevice\_2e:dd:25 (58:f2:fc:2e:dd:25), Dst: PalladiumEne\_b6:8d:b4 (5c:c9:d3:b6:8d:b4)
- Source: HuaweiDevice\_2e:dd:25 (58:f2:fc:2e:dd:25)
- Type: IPv4 (0x0008)
- [Stream index: 0]
- Internet Protocol Version 4, Src: 142.251.132.228, Dst: 192.168.3.4
- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 84
- Identification: 0x0000 (0)
- 0000 .... = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 117
- Protocol: ICMP (1)
- Header Checksum: 0x6e1d [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 142.251.132.228
- Destination Address: 192.168.3.4
- [Stream index: 25]
- Internet Control Message Protocol
- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0x41bd [correct]
- [Checksum Status: Good]
- Identifier (BE): 12224 (0x2fc0)
- Identifier (LE): 49199 (0xc026)
- Sequence Number (BE): 1 (0x0001)
- Sequence Number (LE): 256 (0x0100)
- [Request frame: 2609]
- [Response time: 46.486 ms]
- Timestamp from icmp data: Dec 2, 2024 19:08:26.071590000 -03
- [Timestamp from icmp data (relative): 0.046490894 seconds]
- Data (40 bytes)

**Packet Bytes:**

0000 5c c9 d3 b6 8d b4 58 f2 fc 2e dd 25 08 00 45 00  
0010 00 54 00 00 00 00 75 01 6e 1d 8e fb 84 e4 c0 00  
0020 03 04 00 00 41 bd 2f c0 00 01 da 2f 4e 67 00 00  
0030 00 00 00 17 01 00 00 00 00 00 11 12 13 14 15  
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  
0060 36 37



```
caiohps@caio-hps:~  
→ ~ traceroute -I www.google.com  
You do not have enough privileges to use this traceroute method.  
socket: Operação não permitida  
→ ~ traceroute www.google.com  
  
traceroute to www.google.com (142.251.132.4), 30 hops max, 60 byte  
packets  
1 _gateway (192.168.3.1) 3.772 ms 3.820 ms 3.931 ms  
2 100.127.0.2 (100.127.0.2) 7.364 ms 7.540 ms 7.841 ms  
3 177.126.90.229.novatelecom.com.br (177.126.90.229) 8.985 ms  
8.604 ms 8.587 ms  
4 10.17.17.5 (10.17.17.5) 7.771 ms 7.753 ms 7.967 ms  
5 177.126.88.106.novatelecom.com.br (177.126.88.106) 8.517 ms  
8.492 ms 8.838 ms  
6 201-24-38-89.gnace303.ipd.brasiltelecom.net.br (201.24.38.89)  
8.137 ms 4.478 ms 4.469 ms  
7 100.120.66.142 (100.120.66.142) 5.451 ms * 100.120.66.136 (10  
0.120.66.136) 5.260 ms  
8 100.120.25.109 (100.120.25.109) 19.078 ms 100.120.25.27 (100.  
120.25.27) 21.093 ms 20.984 ms  
9 100.120.31.155 (100.120.31.155) 37.303 ms 100.120.22.210 (100  
.120.22.210) 41.654 ms 100.120.22.212 (100.120.22.212) 39.542 ms  
10 100.120.25.62 (100.120.25.62) 39.164 ms 100.120.31.130 (100.1  
20.31.130) 39.150 ms 100.120.25.80 (100.120.25.80) 42.514 ms  
11 72.14.198.152 (72.14.198.152) 34.551 ms 201.10.242.247 (201.1  
0.242.247) 38.080 ms 72.14.198.152 (72.14.198.152) 37.525 ms  
12 * 108.170.232.1 (108.170.232.1) 30.273 ms *  
13 172.253.73.191 (172.253.73.191) 33.154 ms 108.170.236.216 (10  
8.170.236.216) 35.641 ms 172.253.73.191 (172.253.73.191) 32.191  
ms  
14 192.178.84.180 (192.178.84.180) 40.819 ms gru14s35-in-f4.1e10  
0.net (142.251.132.4) 30.520 ms 172.253.73.191 (172.253.73.191)  
29.889 ms  
→ ~
```

Executando o Traceroute no terminal no linux.

5) Qual é o endereço IP do seu host? Qual é o endereço IP do alvo anfitrião de destino?

Após verificar as informações:

- **Endereço IP do Destino:** 35.201.127.207
- **Identidade do Anfitrião:** O domínio retornad pelo **nslookup** ou pelo comando equivalente.

Se o domínio não for identificado, pode mencionar apenas o IP no relatório, por exemplo:

"O anfitrião de destino é identificado pelo endereço IP **35.201.127.207**. Não há domínio associado ao IP disponível na consulta."

The image shows a Wireshark packet capture of ICMP Echo (ping) requests and replies. The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
1008	75.658555668	192.168.3.4	35.201.127.207	ICMP	598	Destination unreachable (Port unreachable)
2151	181.496848071	192.168.3.4	192.251.132.4	ICMP	98	Echo (ping) request id=0x3d92, seq=1/256, ttl=64 (reply in 2153)
2153	181.532266922	142.251.132.4	192.168.3.4	ICMP	98	Echo (ping) reply id=0x3d92, seq=1/256, ttl=117 (request in 2151)
2510	182.498103066	192.168.3.4	142.251.132.4	ICMP	98	Echo (ping) request id=0x3d92, seq=2/512, ttl=64 (reply in 2513)
2513	183.499997867	192.168.3.4	142.251.132.4	ICMP	98	Echo (ping) request id=0x3d92, seq=3/768, ttl=64 (reply in 2538)
2538	183.537340862	142.251.132.4	192.168.3.4	ICMP	98	Echo (ping) reply id=0x3d92, seq=3/768, ttl=117 (request in 2531)
2541	184.500362751	192.168.3.4	142.251.132.4	ICMP	98	Echo (ping) request id=0x3d92, seq=4/1024, ttl=64 (reply in 2542)
2542	184.538523817	142.251.132.4	192.168.3.4	ICMP	98	Echo (ping) reply id=0x3d92, seq=4/1024, ttl=117 (request in 2541)
2543	185.501368512	192.168.3.4	142.251.132.4	ICMP	98	Echo (ping) request id=0x3d92, seq=5/1280, ttl=64 (reply in 2544)
2544	185.539328084	142.251.132.4	192.168.3.4	ICMP	98	Echo (ping) reply id=0x3d92, seq=5/1280, ttl=117 (request in 2543)
2548	186.502118092	192.168.3.4	142.251.132.4	ICMP	98	Echo (ping) request id=0x3d92, seq=6/1536, ttl=64 (reply in 2554)
2554	186.539531872	142.251.132.4	192.168.3.4	ICMP	98	Echo (ping) reply id=0x3d92, seq=6/1536, ttl=117 (request in 2548)
2569	187.503368000	192.168.3.4	142.251.132.4	ICMP	98	Echo (ping) request id=0x3d92, seq=7/1792, ttl=64 (reply in 2575)
2575	187.540186347	142.251.132.4	192.168.3.4	ICMP	98	Echo (ping) reply id=0x3d92, seq=7/1792, ttl=117 (request in 2569)
2583	188.505383899	192.168.3.4	142.251.132.4	ICMP	98	Echo (ping) request id=0x3d92, seq=8/2048, ttl=64 (reply in 2585)
2585	188.545404362	142.251.132.4	192.168.3.4	ICMP	98	Echo (ping) reply id=0x3d92, seq=8/2048, ttl=117 (request in 2583)
2595	189.506139180	192.168.3.4	142.251.132.4	ICMP	98	Echo (ping) request id=0x3d92, seq=9/2304, ttl=64 (reply in 2596)
2596	189.543407127	142.251.132.4	192.168.3.4	ICMP	98	Echo (ping) reply id=0x3d92, seq=9/2304, ttl=117 (request in 2595)
2600	110.507395021	192.168.3.4	142.251.132.4	ICMP	98	Echo (ping) request id=0x3d92, seq=10/2560, ttl=64 (reply in 2601)
2601	110.545320883	142.251.132.4	192.168.3.4	ICMP	98	Echo (ping) reply id=0x3d92, seq=10/2560, ttl=117 (request in 2600)
7286	245.010811606	192.168.3.1	192.168.3.4	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
7287	245.010904520	192.168.3.1	192.168.3.4	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
7288	245.011037186	192.168.3.1	192.168.3.4	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)

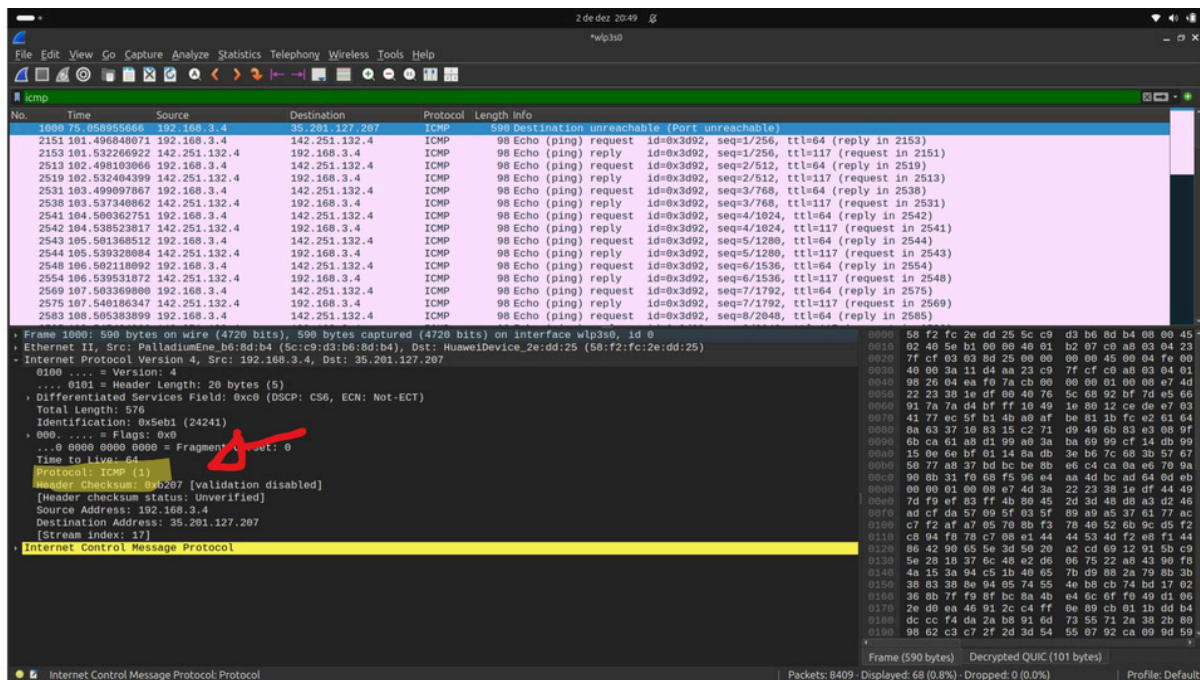
The packet details pane shows the following information for the selected packet (No. 1008):

- Frame 1008: 598 bytes on wire (4728 bits) captured (4728 bits) on interface wlan0, id 0
- Ethernet II, Src: PalladiumEne\_b6:8d:b4 (Src: c9:d3:b6:8d:b4), Dst: HuaweiDevice\_2e:dd:25 (58:f2:fc:2e:dd:25)
- Internet Protocol Version 4, Src: 192.168.3.4, Dst: 35.201.127.207
- Internet Control Message Protocol
  - Type: 3 (Destination unreachable)
  - Code: 3 (Port unreachable)
  - Checksum: 0x8d25 [correct]
  - [Checksum Status: Good]
  - Unused: 00000000
  - Internet Protocol Version 4, Src: 35.201.127.207, Dst: 192.168.3.4
  - User Datagram Protocol, Src Port: 443, Dst Port: 38950
  - QUIC IETF
  - QUIC IETF

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol payload.

6) Se o ICMP enviasse pacotes UDP (como no Unix/Linux), o protocolo IP número ainda será 01 para os pacotes de sonda? Se não, qual seria?

Se o ICMP fosse implementado usando pacotes UDP, o número do protocolo IP seria **17**, pois este é o identificador do protocolo UDP na camada de rede. O ICMP, como visto na captura do Wireshark, usa o número 1.



7) . Examine o pacote de eco ICMP na sua captura de tela. Ele é diferente dos pacotes de consulta ping ICMP na primeira metade deste laboratório? Se sim, como assim?

**Diferença entre os pacotes:**

- **OEchoRequest** possui **Type 8, Code 0**, enquanto o **Echo Reply** possui **Type 0, Code 0**.



- O campo **TTL (Time to Live)** também pode ser diferente:
  - Echo Request: TTL configurado pelo sistema local (geralmente 64 ou 128).
  - Echo Reply: TTL configurado pelo host remoto, normalmente menor devido à redução em cada salto na rede.

### Semelhanças:

- Campos **Checksum, Identifier e Sequence Number** são idênticos entre o Echo Request e o Echo Reply.
- O campo **Data** também permanece o mesmo em ambos os pacotes.

Wireshark capture showing ICMP Echo (ping) request and reply. The packet details for the request (No. 2151) are highlighted with a red arrow.

No.	Time	Source	Destination	Protocol	Length	Info
1000	75.05995566	192.168.3.4	35.201.127.207	ICMP	590	Destination unreachable (Port unreachable)
2151	101.49844071	192.168.3.4	142.251.132.4	ICMP	98	Echo (ping) request id=0x3d92, seq=1/256, ttl=64 (reply in 2153)
2153	101.53226692	142.251.132.4	192.168.3.4	ICMP	98	Echo (ping) reply id=0x3d92, seq=1/256, ttl=117 (request in 2151)

Packet Details for No. 2151 (Echo (ping) request):

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x5C93 [correct]
- Identifier (BE): 15762 (0x3d92)
- Identifier (LE): 37437 (0x923d)
- Sequence Number (BE): 1 (0x0001)
- Sequence Number (LE): 256 (0x0100)
- [Response frame: 2153]
- Timestamp from icmp data: Dec 2, 2024 20:21:36.482899000 -03
- [Timestamp from icmp data (relative): 0.00004887 seconds]
- Data (40 bytes)

Wireshark capture showing ICMP Echo (ping) request and reply. The packet details for the reply (No. 2153) are highlighted with a red arrow.

No.	Time	Source	Destination	Protocol	Length	Info
1000	75.05995566	192.168.3.4	35.201.127.207	ICMP	590	Destination unreachable (Port unreachable)
2151	101.49844071	192.168.3.4	142.251.132.4	ICMP	98	Echo (ping) request id=0x3d92, seq=1/256, ttl=64 (reply in 2153)
2153	101.53226692	142.251.132.4	192.168.3.4	ICMP	98	Echo (ping) reply id=0x3d92, seq=1/256, ttl=117 (request in 2151)

Packet Details for No. 2153 (Echo (ping) reply):

- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0x6493 [correct]
- Identifier (BE): 15762 (0x3d92)
- Identifier (LE): 37437 (0x923d)
- Sequence Number (BE): 1 (0x0001)
- Sequence Number (LE): 256 (0x0100)
- [Request frame: 2151]
- [Response time: 35.419 ms]
- Timestamp from icmp data: Dec 2, 2024 20:21:36.482899000 -03
- [Timestamp from icmp data (relative): 0.035423738 seconds]
- Data (40 bytes)

8) Examine o pacote de erro ICMP na sua captura de tela. Ele tem mais campos do que o Pacote de eco ICMP. O que está incluso nesses campos?

### Diferença nos Campos:

- OpacotedeerroICMPcontémcamposadicionais:
  - **DatagramaOriginal**: Inclui o cabeçalho IP do pacote que gerou o erro nos primeiros 8 bytes de sua carga útil.
  - **Tipo e Código de Erro ICMP**: Específicos para o tipo de erro (por exemplo, Tipo 3 para "Destination Unreachable", Tipo 11 para "Time-to-Live Exceeded").

### Informações Adicionais:

- No pacote número **1000**:
  - Tipo: 3 (Destination Unreachable).
  - Código: 3 (Port Unreachable).
  - O erro foi gerado pelo host com endereço **35.201.127.207**.
  - O pacote original tinha como destino o endereço **142.251.132.4**.

The screenshot shows a Wireshark capture of an ICMP Destination Unreachable packet (No. 1000). The packet list pane shows the packet details: No. 1000, Time 75.05995666, Source 192.168.3.4, Destination 35.201.127.207, Protocol ICMP, Length 590. The packet details pane shows the ICMP header with Type 3 (Destination Unreachable) and Code 3 (Port Unreachable). The original IP header is also visible, showing Source Address 192.168.3.4 and Destination Address 35.201.127.207. The packet bytes pane shows the raw data of the packet.

9) Examine os últimos três pacotes ICMP recebidos pelo host de origem. Como esses pacotes são diferentes dos pacotes de erro ICMP? Por que eles são diferentes?

1. **Últimos três pacotes ICMP:**

- ☐ São pacotes de erro do tipo **Time-to-Live Exceeded (Type 11)**.
- ☐ Cada pacote contém informações adicionais:
  - Cabeçalho do datagrama original.
  - Os primeiros 8 bytes de dados do pacote original.

2. **Diferenças em relação aos pacotes Echo ICMP:**

- ☐ Os pacotes Echo ICMP (Request/Reply) não contêm informações sobre o datagrama original.
- ☐ Os pacotes de erro ICMP são usados para informar problemas na rede, como a expiração do TTL, enquanto os pacotes Echo ICMP servem para verificar conectividade.

3. **Motivo da diferença:**

- ☐ Os pacotes de erro ICMP incluem informações extras para diagnóstico, permitindo que o host origem saiba qual pacote causou o erro e o motivo exato.