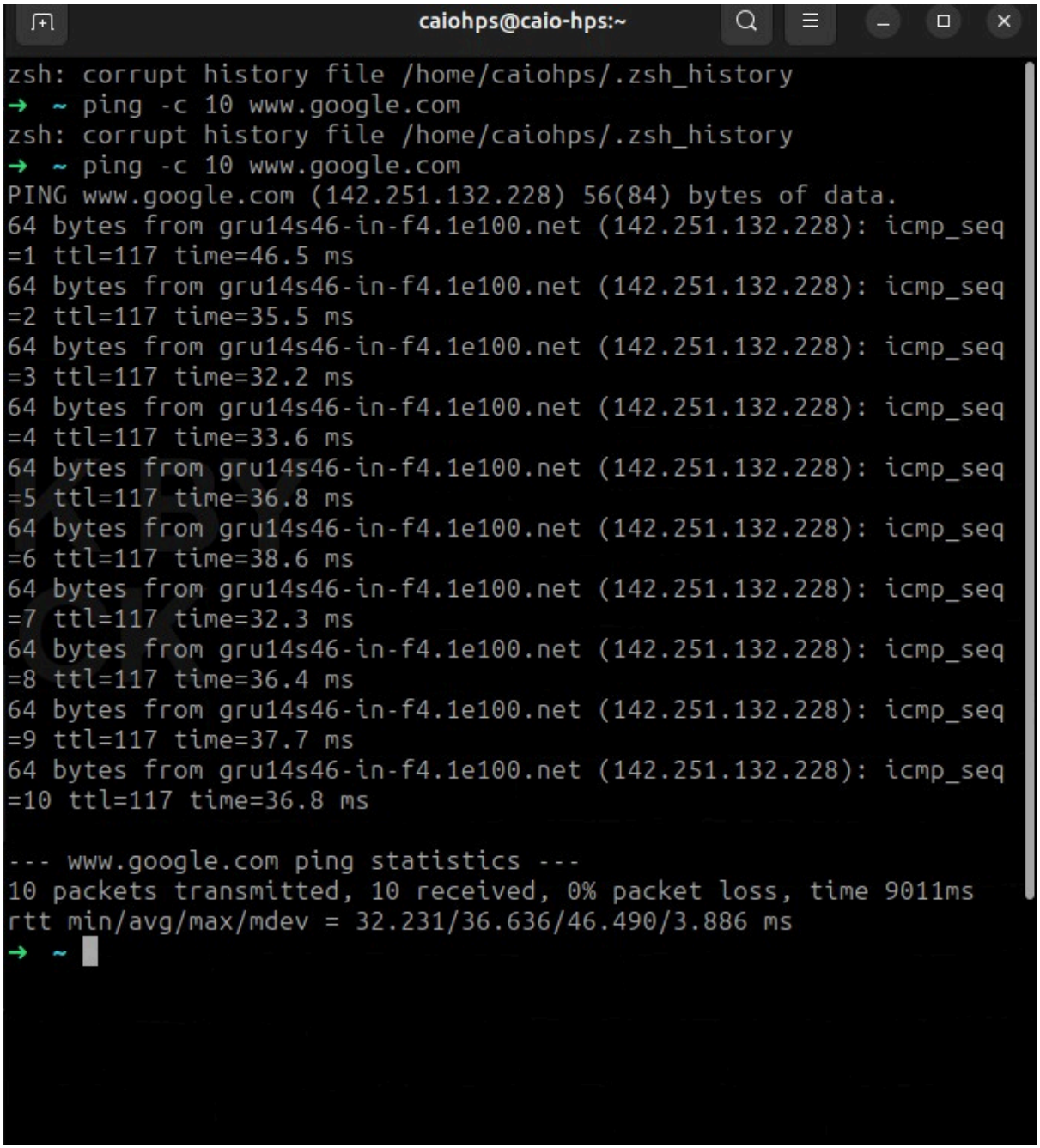
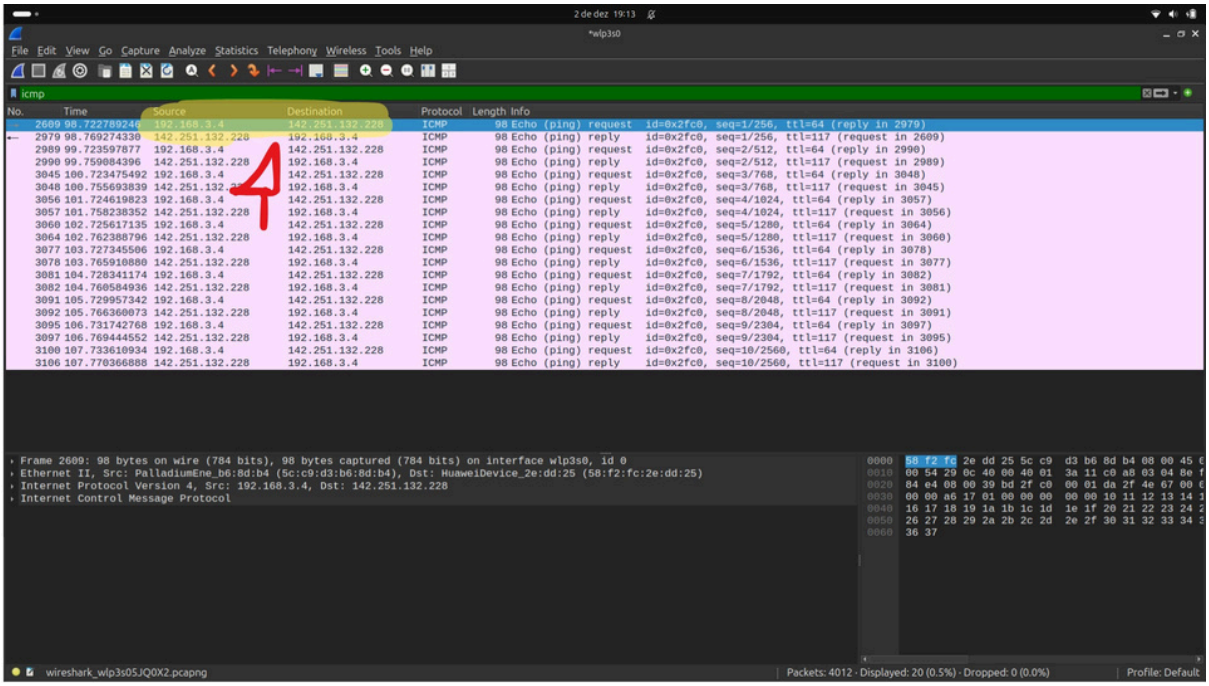
Laboratório ICMP Wireshark
Alunos: Eduardo Henrique



Terminal do Linux comando para capturar os ICMP.

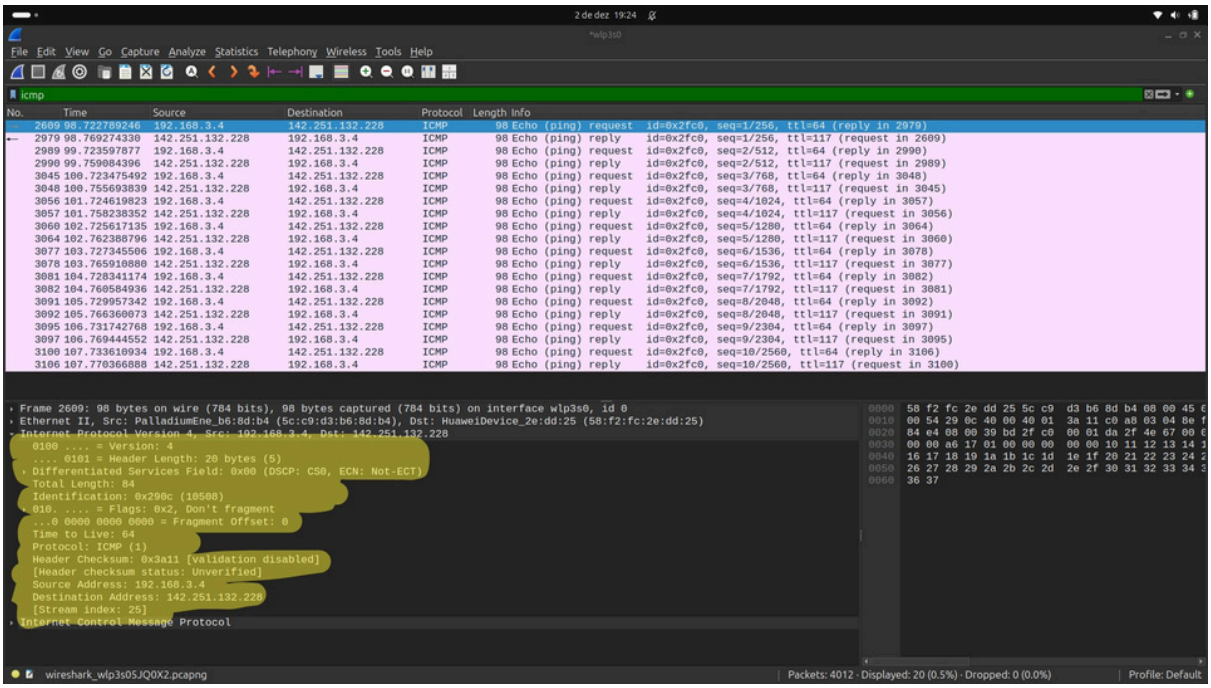
. 1) Qual é o endereço IP do seu host? Qual é o endereço IP do destino?

- **IPdoHost(Origem):**192.168.3.4
- **IPdoDestino:**142.251.132.228



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

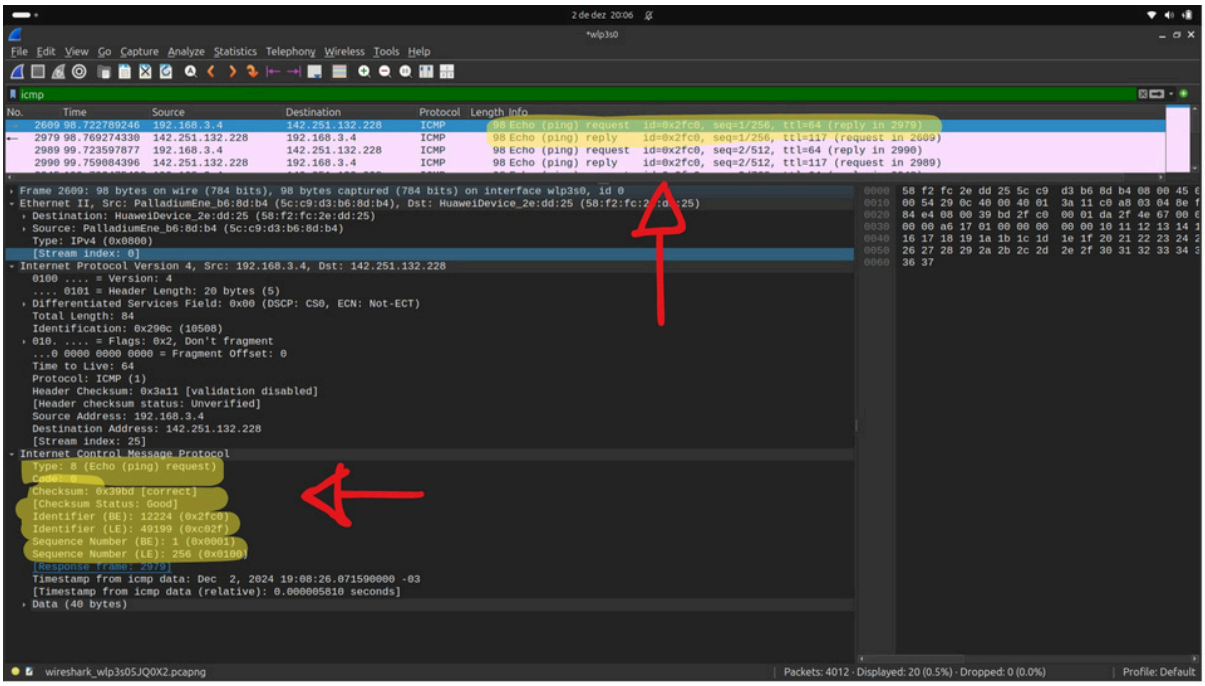
Pacotes ICMP não têm portas de origem e destino porque o protocolo ICMP opera na camada de rede (camada 3 do modelo OSI), e não na camada de transporte (camada 4). Seu propósito é exclusivamente transmitir mensagens de controle e diagnóstico relacionadas ao funcionamento da rede, como requisições de 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.



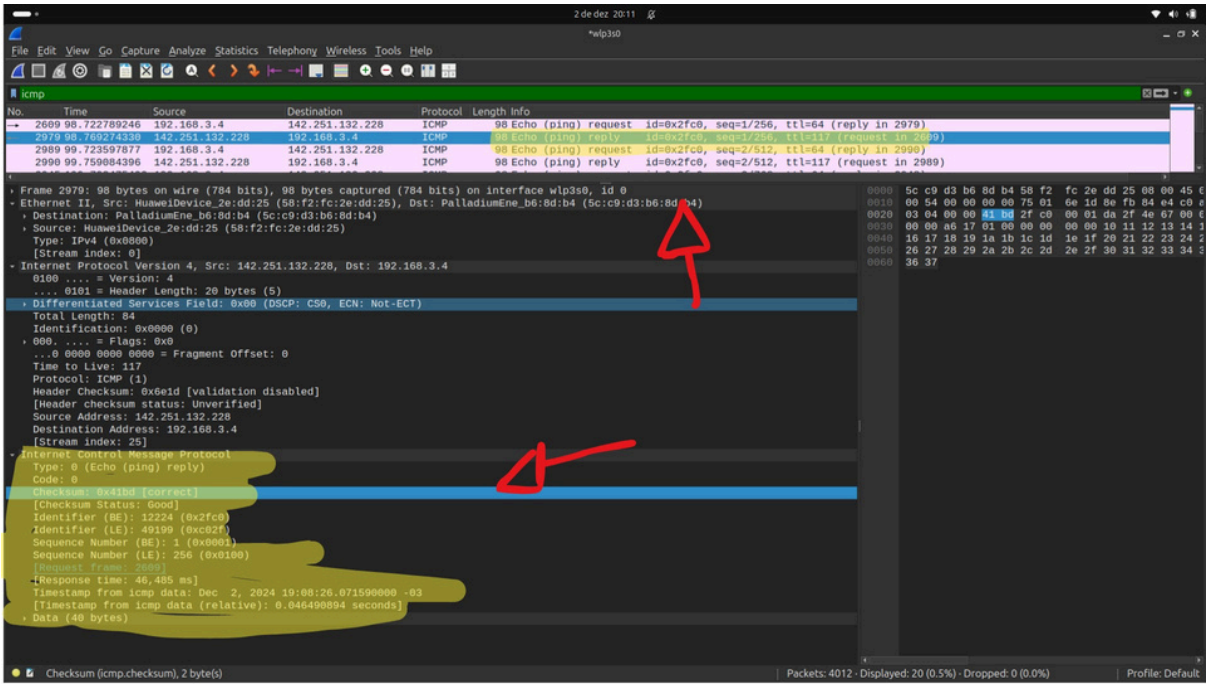
4) Examine o pacote de resposta ping correspondente. Quais são os números de código e tipo ICMP? Quais outros campos esse pacote ICMP tem? Quantos bytes são os campos de checksum, número de sequência e identificador?

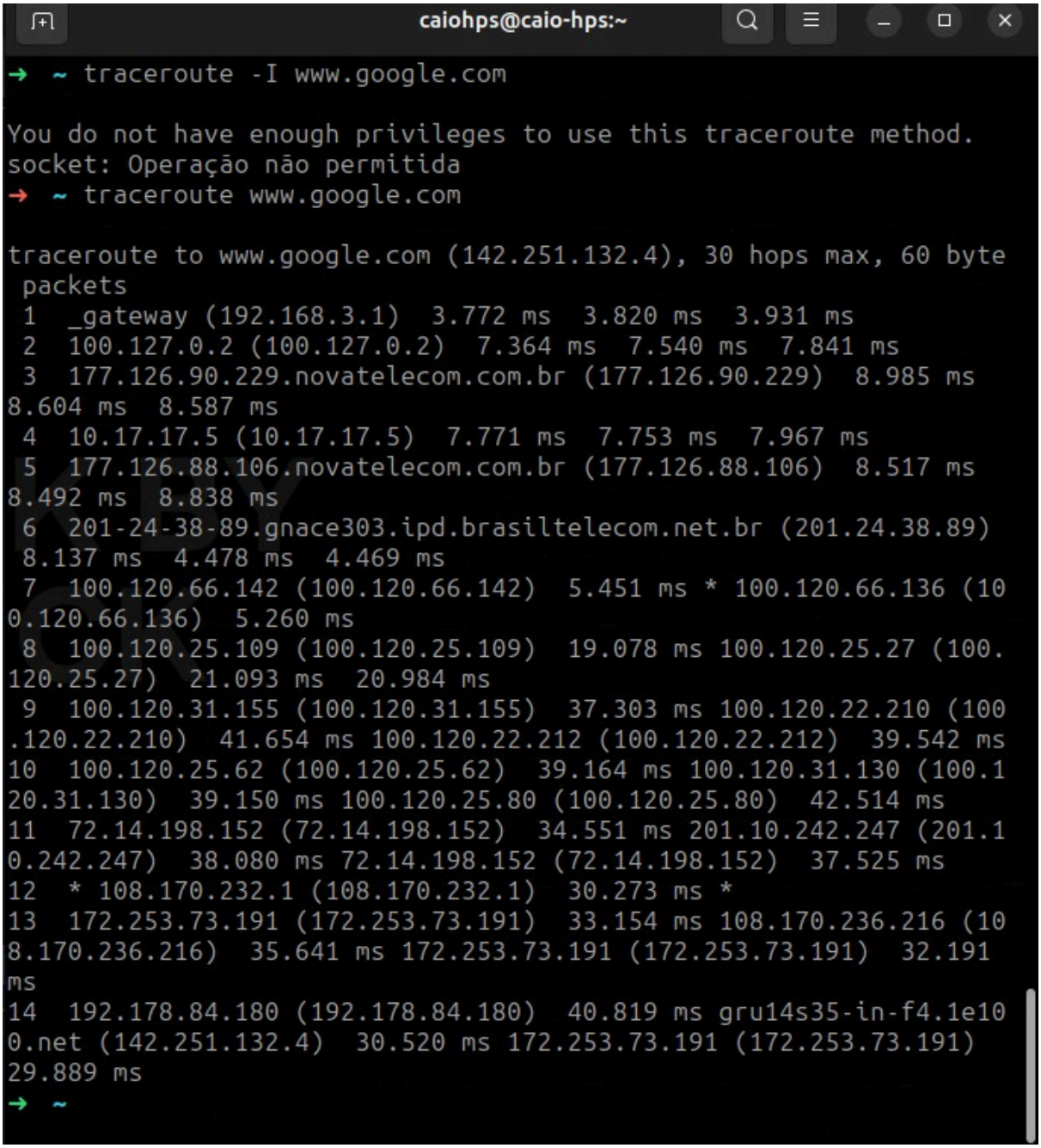
Tipo e Código ICMP:

- Tipo:0(EchoReply).
- Código:0.

Campos no Pacote ICMP:

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





Executando o Traceroute no terminal no linux.

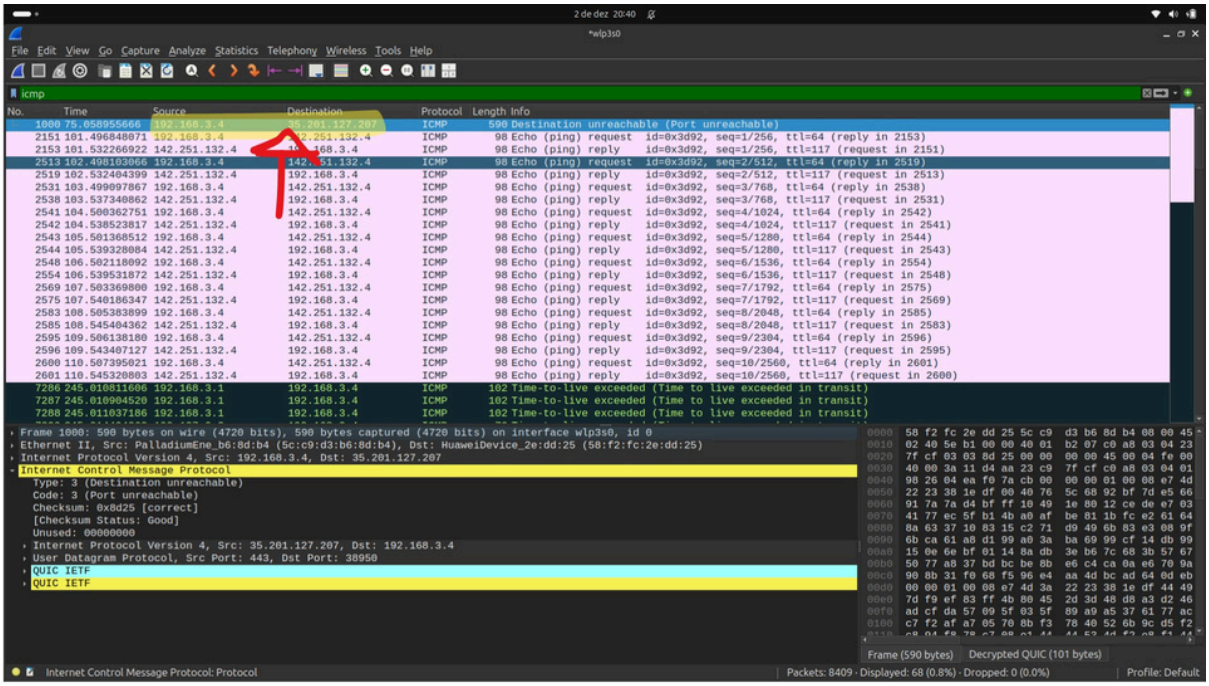
5) Qual é o endereço IP do seu host? Qual é o endereço IP do alvo anfitrião de destino?

Após verificar as informações:

- **EndereçoIPdoDestino:**35.201.127.207
- **IdentidadedoAnfitrião:**Odomínioretornadopelonslookupoupelocomando equivalente.

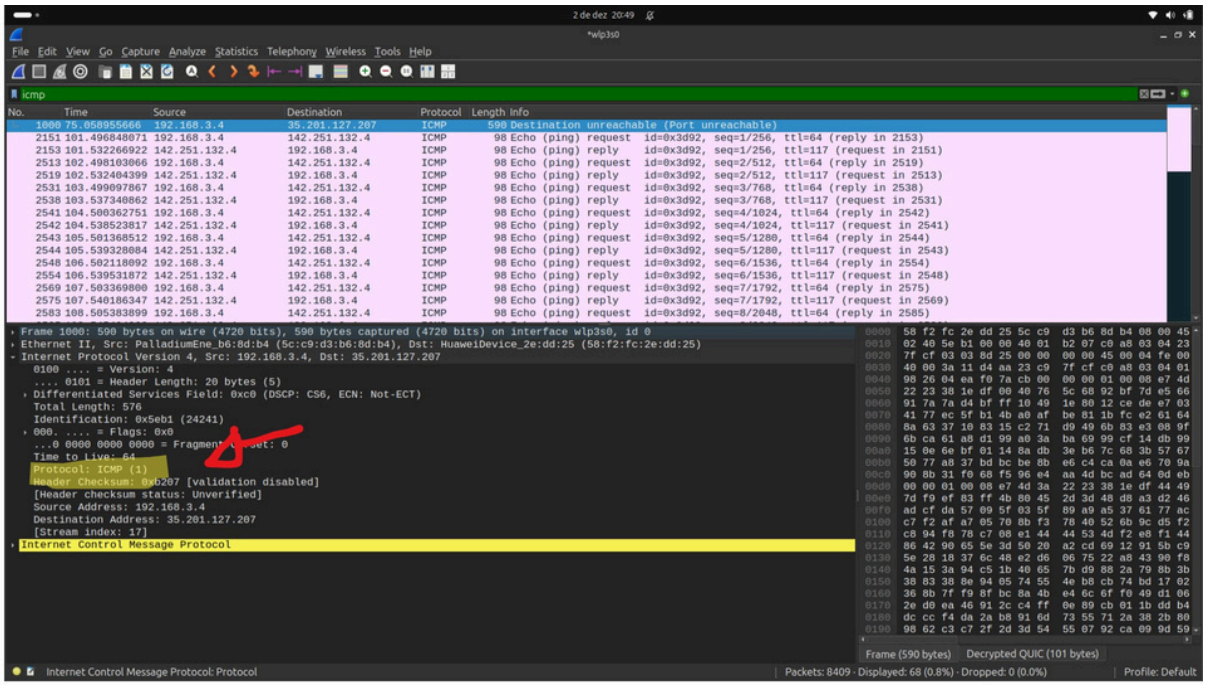
Se o domínio não for identificado, pode mencionar apenas o IP no relatório, por exemplo:

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



6) Se o ICMP enviasse pacotes UDP (como no Unix/Linux), o protocolo IPnúmero 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?

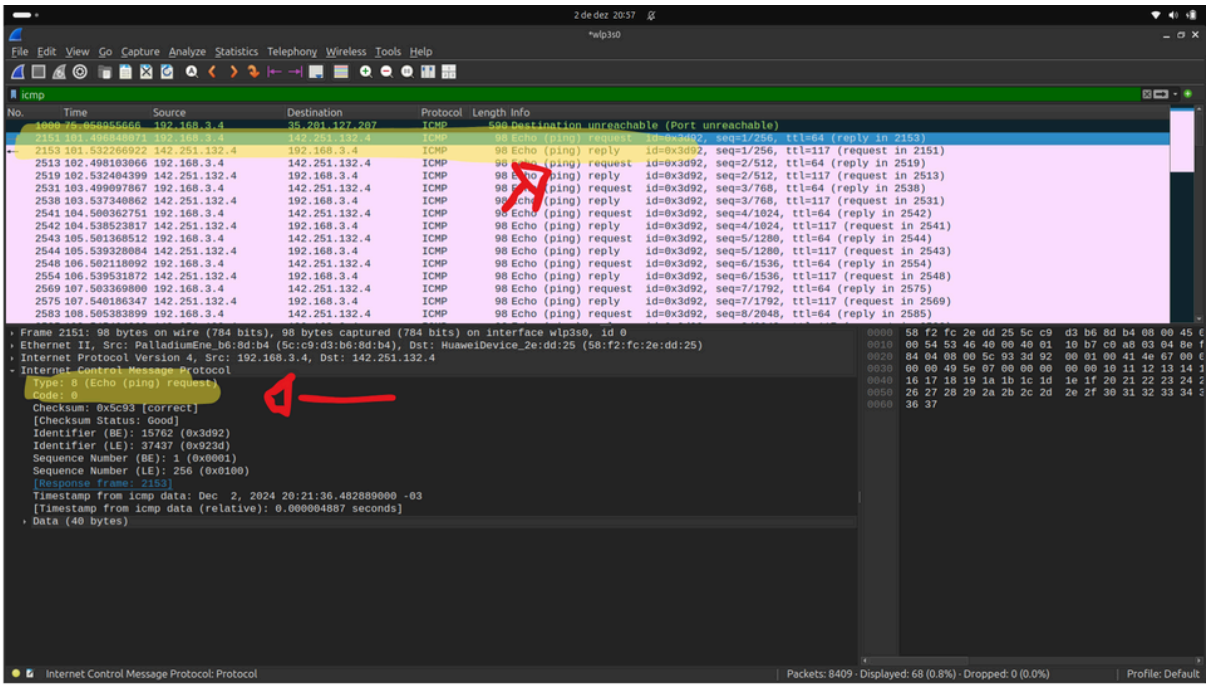
Diferença entre os pacotes:

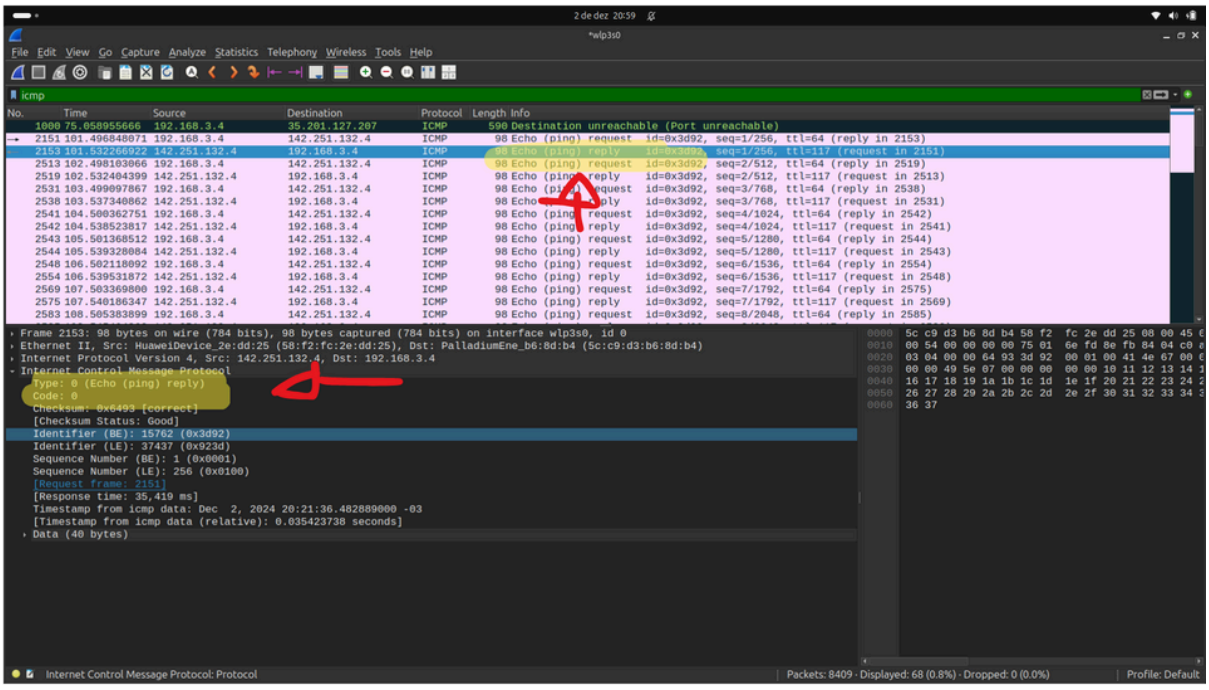
- O**EchoRequest** possui **Type 8, Code 0**, enquanto o **Echo Reply** possui **Type 0, Code 0**.

- Ocampo **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.





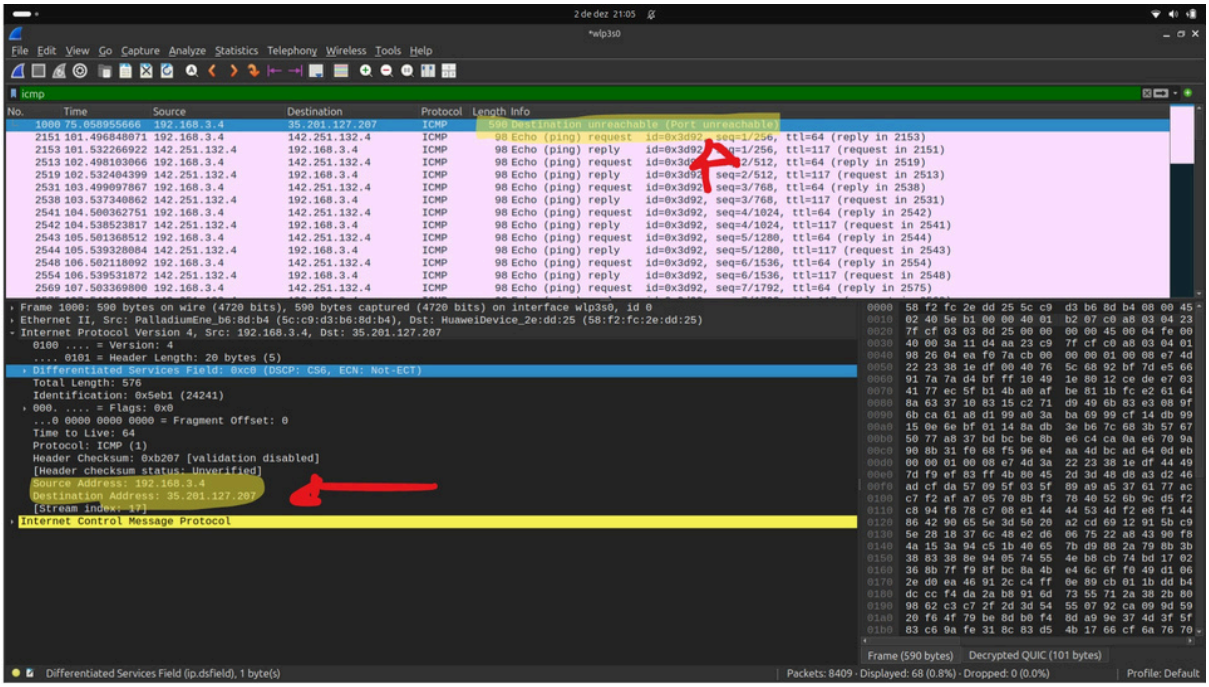
8) Examine o pacote de erro ICMP na sua captura de tela. Ele tem mais campos do que o Pacote de eco ICMP. O que está incluso nesses campos?

Diferença nos Campos:

- O pacote de erro ICMP contém campos adicionais:
  - **Datagrama Original**: Inclui o cabeçalho IP do pacote que gerou o erro e os 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**.



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:**
   - ◯ SãopacotesdeerrodotipoTime-to-LiveExceeded(Type11).
   - ◯ Cadapacotecontéminformaçõesadicionais:
     - ■ CabeçalhododatagramaIPoriginal.
     - ■ Osprimeiros8bytesdedadosdopacoteoriginal.
2. **Diferenças em relação aos pacotes Echo ICMP:**
   - ◯ OspacotesEchoICMP(Request/Reply)nãocontêminformaçõessobreo datagrama original.
   - ◯ OspacotesdeerroICMPsãousadosparainformarproblemasnarede, como a expiração do TTL, enquanto os pacotes Echo ICMP servem para verificar conectividade.
3. **Motivo da diferença:**
   - ◯ OspacotesdeerroICMPinclueminformaçõesextrasparadiagnóstico, permitindo que o host origem saiba qual pacote causou o erro e o motivo exato.