

Atividade sobre ICMP

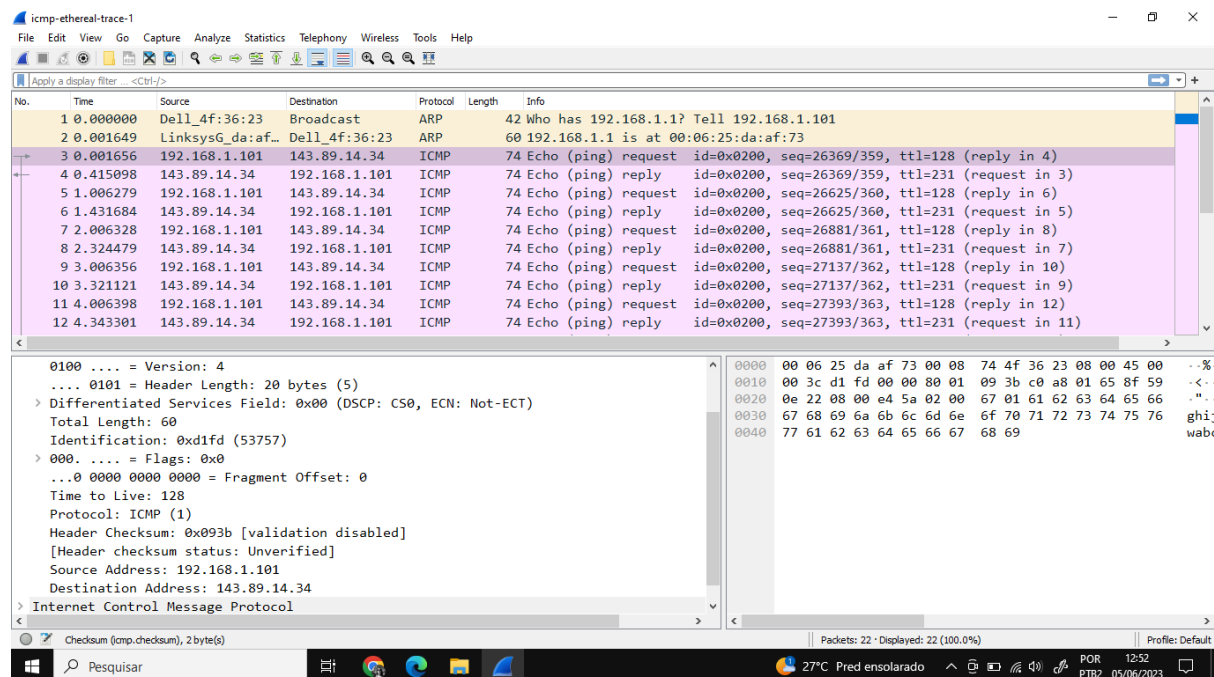
Redes de Computadores

Sabrina Araújo Cardoso - 118210114

Wireshark Lab: ICMP

A atividade foi feita utilizando o pacote capturado pelo autor.

- **Questão 1:** Qual é o endereço IP do seu computador? Qual é o endereço IP do computador de destino?



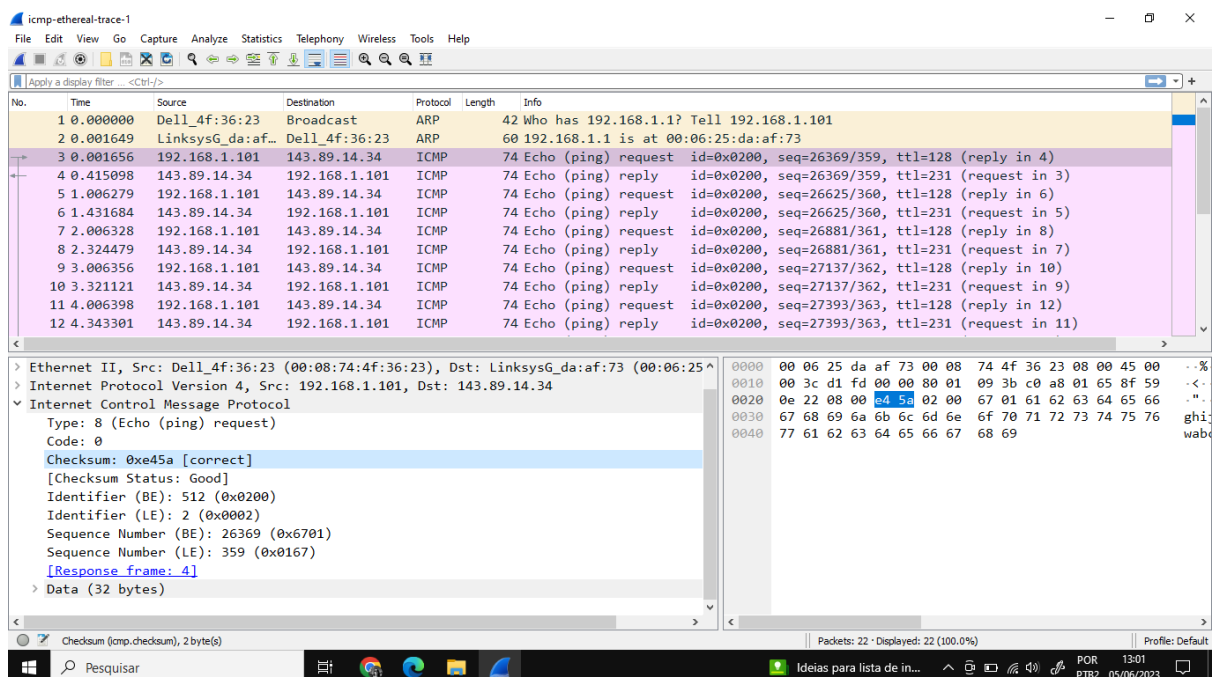
Source Address: **192.168.1.101**

Destination Address: **143.89.14.34**

- **Questão 2:** Por que um pacote ICMP não possui números de porta de origem e destino?

O pacote ICMP não apresenta números de porta de origem e destino devido ao seu propósito de transmitir informações da camada de rede entre hosts e roteadores, sem envolver processos específicos da camada de aplicação. Cada pacote ICMP é caracterizado por seu "Type" e "Code", os quais identificam a mensagem específica transmitida. Dado que o software de rede é responsável por interpretar todas as mensagens ICMP, não há necessidade de utilizar números de porta para direcionar essas mensagens a processos específicos da camada de aplicação.

- **Questão 3:** Examine um dos pacotes de solicitação de ping enviados pelo seu host. Quais são os números de tipo e código ICMP? Quais outros campos esse pacote ICMP possui? Quantos bytes têm os campos de checksum, número de sequência e identificador?



The screenshot shows a Wireshark capture of network traffic. The packet list pane displays several ICMP Echo (ping) requests and replies. The selected packet is an ICMP Echo (ping) request from 192.168.1.101 to 143.89.14.34. The packet details pane shows the following fields:

- Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:af:73)
- Internet Protocol Version 4, Src: 192.168.1.101, Dst: 143.89.14.34
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0xe45a [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 512 (0x0200)
 - Identifier (LE): 2 (0x0002)
 - Sequence Number (BE): 26369 (0x6701)
 - Sequence Number (LE): 359 (0x0167)
 - [Response frame: 4]
 - Data (32 bytes)

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and ICMP Echo (ping) request data.

Type: 8
Code: 0

O pacote ICMP também possui **Checksum, Identifier, Sequence Number e Data.**

Checksum: **2 bytes**

Identifier: **2 bytes**

Sequence Number: **2 bytes**

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

The screenshot shows a Wireshark packet capture of an ICMP Echo (ping) request and reply. The selected packet is an ICMP Echo (ping) reply with Type 0 and Code 0. The packet details show Checksum: 0xec5a, Identifier (BE): 512 (0x0200), Identifier (LE): 2 (0x0002), Sequence Number (BE): 26369 (0x6701), Sequence Number (LE): 359 (0x0167), and Response time: 413,442 ms. The packet data is 32 bytes.

Type: **0**

Code: **0**

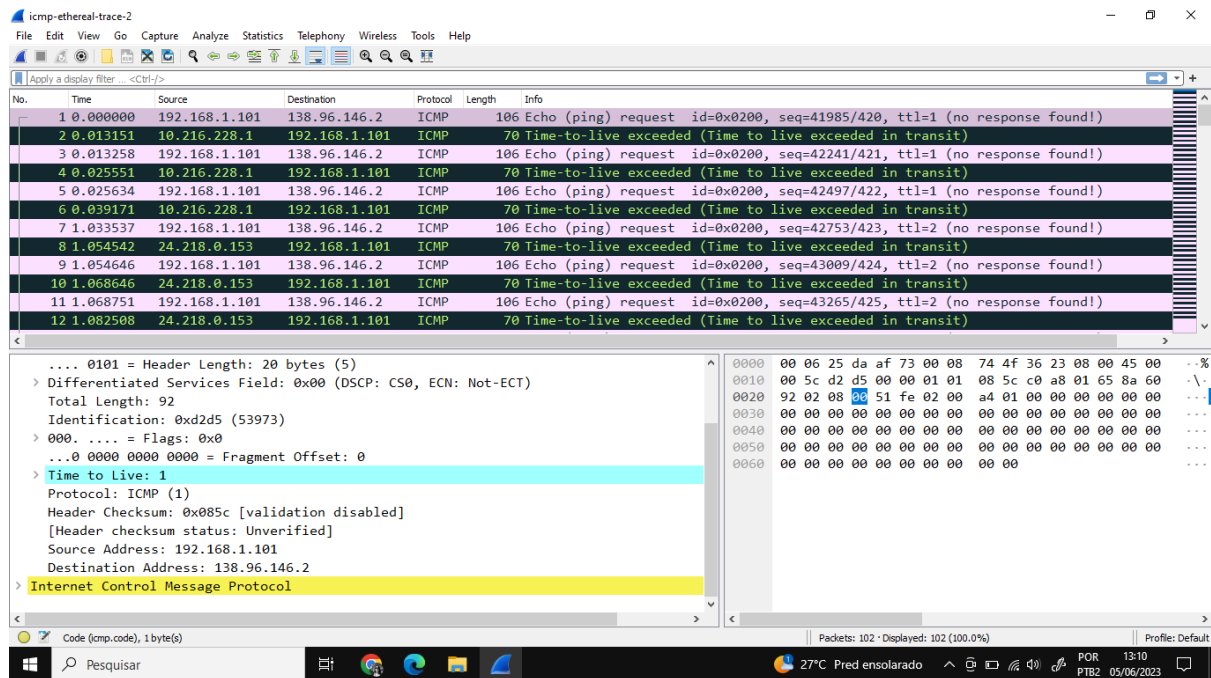
O pacote ICMP também possui **Checksum, Identifier, Sequence Number e Data.**

Checksum: **2 bytes**

Identificador: **2 bytes**

Sequence Number: **2 bytes**

- **Questão 5:** Qual é o endereço IP do seu computador? Qual é o endereço IP do host de destino?



Source Address: **192.168.1.101**

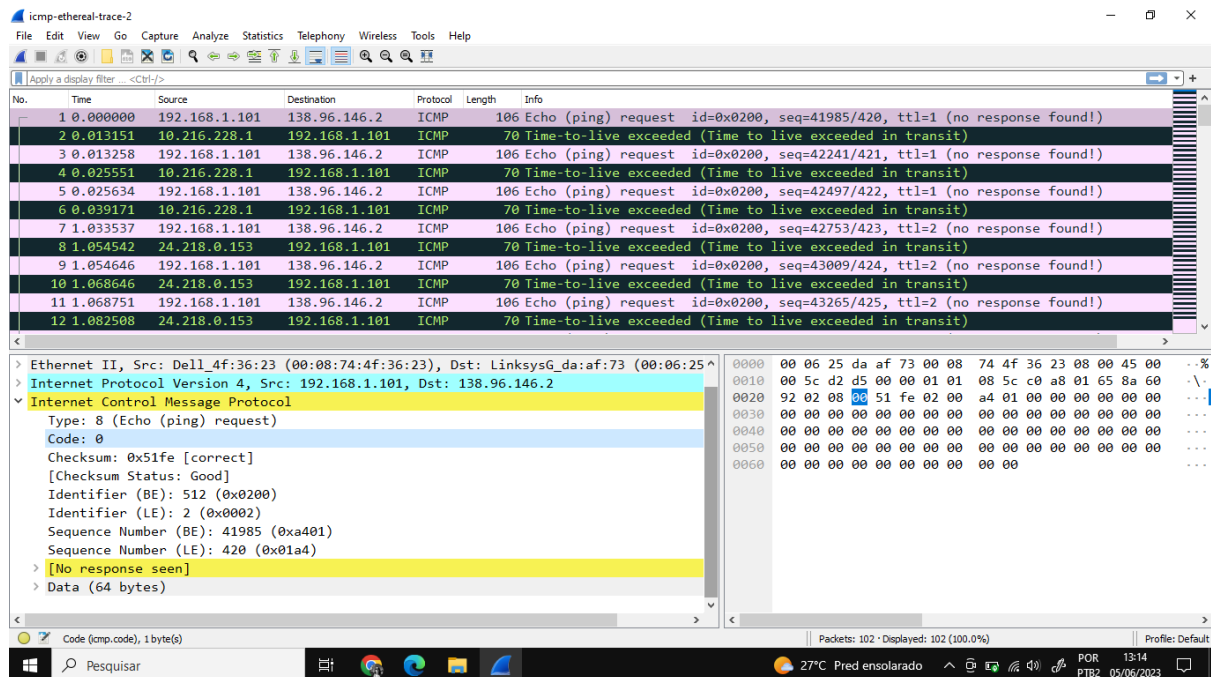
Destination Address: **138.96.146.2**

- **Questão 6:** Se o ICMP enviasse pacotes UDP em vez disso (como no Unix/Linux), o número do protocolo IP ainda seria 01 para os pacotes de sondagem? Se não, qual seria?

Não. Se o ICMP enviasse pacotes UDP em vez disso, o número do protocolo IP deveria ser **0x11.**

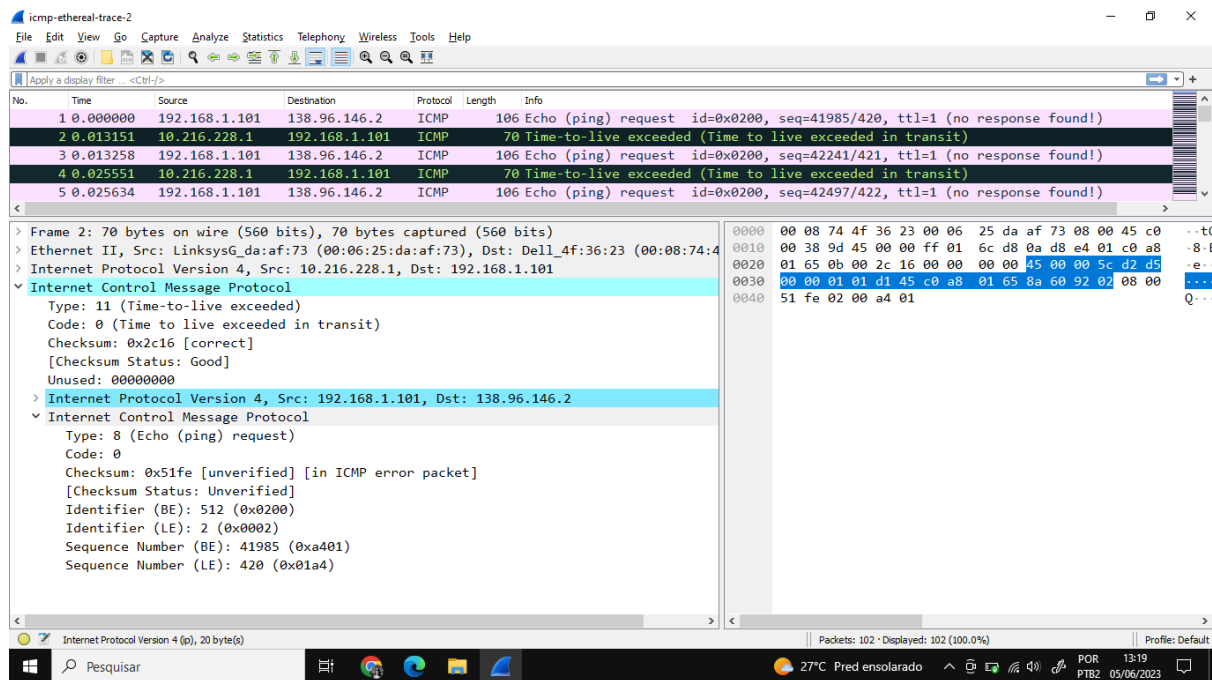
- **Questão 7:** Examine o pacote ICMP echo na captura de tela. Ele é diferente dos pacotes de consulta ICMP ping na primeira metade deste laboratório? Se

sim, de que forma?



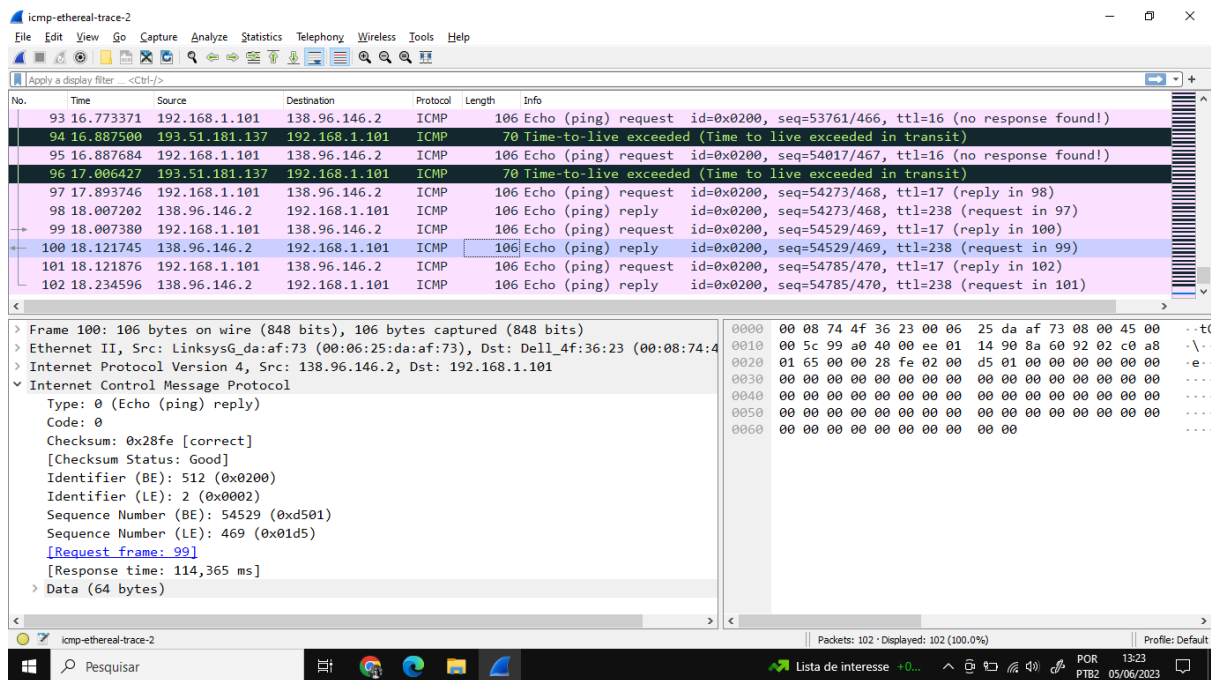
Não. Ele possui os mesmos campos dos pacotes de consulta ICMP ping na primeira metade deste laboratório.

- **Questão 8:** Examine o pacote de erro ICMP na captura de tela. Ele possui mais campos do que o pacote de echo ICMP. O que está incluído nesses campos?



Sim! O pacote de erro ICMP é diferente do pacote echo ICMP. Ele contém tanto o cabeçalho IP quanto os primeiros 8 bytes do pacote ICMP original para o qual o erro é direcionado.

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



Os três últimos pacotes ICMP possuem Type: 0 em vez de Type: 11 (TTL expired).

Eles são diferentes porque os datagramas chegaram até o host de destino antes que o TTL expirasse.

- **Questão 10:** Dentro das medições do tracer, existe algum link cujo atraso seja significativamente maior que os outros? Com base na captura de tela na Figura 4, existe um link cujo atraso é significativamente maior que os outros? Com base nos nomes dos roteadores, você pode supor a localização dos dois roteadores no final desse link?

```
Command Prompt
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>tracert www.inria.fr

Tracing route to www.inria.fr [138.96.146.2]
over a maximum of 30 hops:

  1    13 ms    12 ms    13 ms    10.216.228.1
  2    21 ms    14 ms    13 ms    24.218.0.153
  3    12 ms    11 ms    13 ms    bar01-p4-0.wsfde1.ma.attbb.net [24.128.190.197]
  4    16 ms    16 ms    15 ms    bar02-p6-0.ndhne1.ma.attbb.net [24.128.0.101]
  5    15 ms    15 ms    15 ms    12.125.47.49
  6    17 ms    17 ms    17 ms    12.123.40.218
  7    22 ms    23 ms    22 ms    tbr2-cl1.n54ny.ip.att.net [12.122.10.22]
  8    23 ms    23 ms    23 ms    ggr2-p3120.n54ny.ip.att.net [12.123.3.109]
  9    26 ms    21 ms    25 ms    att-gw.nyc.opentransit.net [192.205.32.138]
 10    98 ms    98 ms    96 ms    P4-0.PASCRI.Pastourelle.opentransit.net [193.251.241.133]
 11    97 ms    98 ms    98 ms    P9-0.AUUCR1.Aubervilliers.opentransit.net [193.251.243.29]
 12    98 ms    98 ms    108 ms    P6-0.BAGCR1.Bagnolet.opentransit.net [193.251.241.93]
 13   104 ms   106 ms    103 ms    193.51.185.30
 14   114 ms   114 ms    117 ms    grenoble-pos1-0.cssi.renater.fr [193.51.179.238]
 15   114 ms   115 ms    114 ms    nice-pos2-0.cssi.renater.fr [193.51.180.34]
 16   129 ms   114 ms    118 ms    inria-nice.cssi.renater.fr [193.51.181.137]
 17   113 ms   114 ms    112 ms    www.inria.fr [138.96.146.2]

Trace complete.
C:\WINDOWS\SYSTEM32>
```

Há uma conexão entre as etapas 11 e 12 que apresenta um considerável atraso. Trata-se de uma ligação transatlântica entre Nova York e Aubervilliers, na França. Na figura do laboratório, o trajeto vai de Nova York a Pastourelle, também na França.