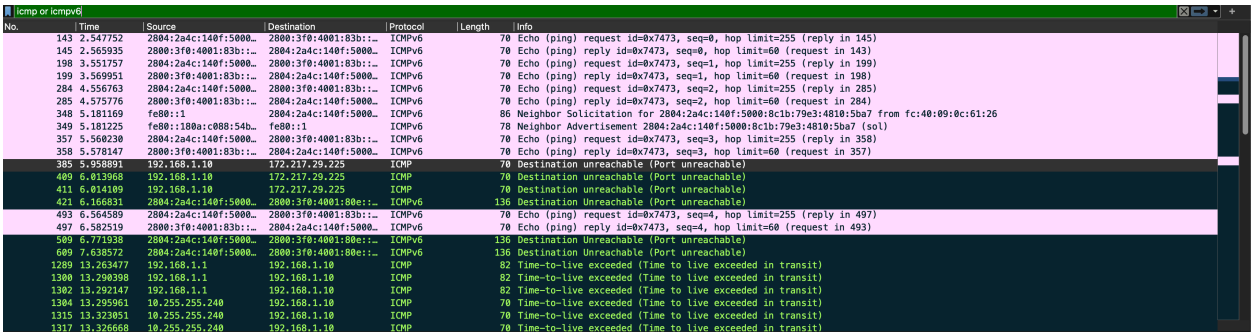
UNISINOS	ATIVIDADE ACADÊMICA: Redes de Computadores: Internetworking, Roteamento e Transmissão TRABALHO: Atividade 4 ALUNOS: Rafael Hansen Klauck

Para realizar essa atividade, rodei o comando *sudo tcpdump -i en0 -w* para poder analisar os pacotes da rede. Após deixar o comando executando por um tempo, abri ele no Wireshark. Como minha rede tem suporte para IPV6, minha máquina acabava priorizando a utilização dele, por isso não conseguia ver nenhum pacote ICMPv4. Então, para que fosse possível visualizar tantos pacotes ICMPv4 e v6, eu abri um segundo terminal para executar o comando *traceroute*.

Foram encontrados pacotes ICMP v4 e v6?



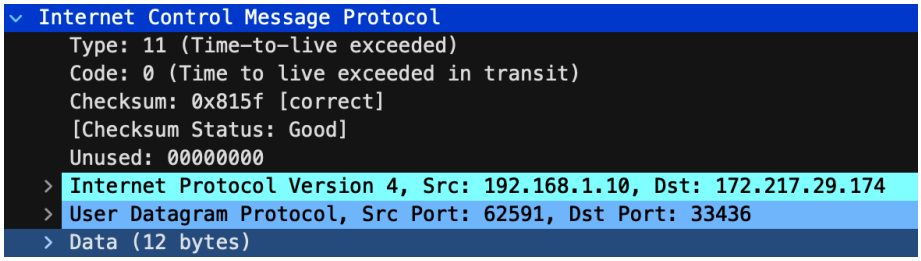
Quais os tipos de ICMP forma capturados?

Para o **ICMPv4** foram encontrados Time-to-Life exceeded(tipo 11) e Destination unreachable(tipo 3).

Para o **ICMPv6** foram encontrados Echo Ping(request), Echo Ping(replay), Neighbor Solicitation, Neighbor Advertisement (136) e Destination Unreachable.

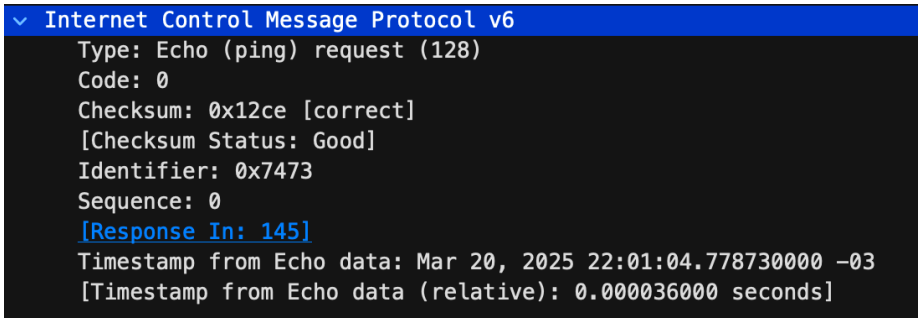
Quais os campos do ICMP encontrados?

ICMPv4: Type, code, checksum, checksum status, unused.

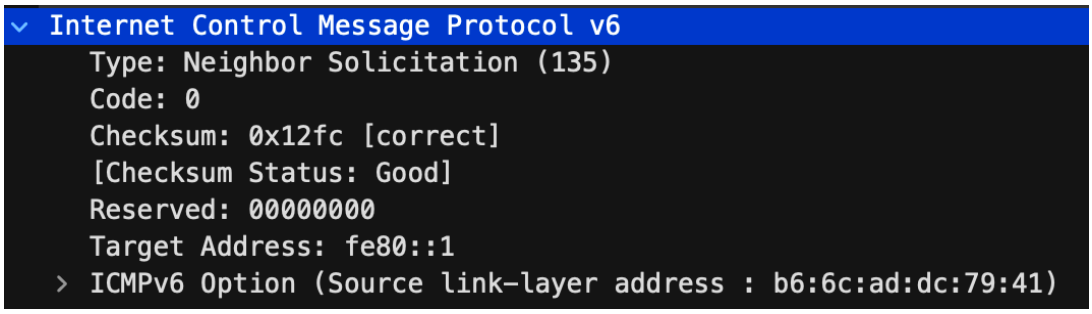


Algo que é importante de comentar é que o type, o code, e o checksum são campos fixos no cabeçalho. Os demais campos, o conteúdo pode alterar, dependendo do tipo de mensagem, como podemos ver na imagem a abaixo, que tem conteúdo diferente da anterior.

ICMPv6: type, code, checksum, checksum status, identifier, sequence, Timestamp from Echo data e Timestamp from Echo data (relative).

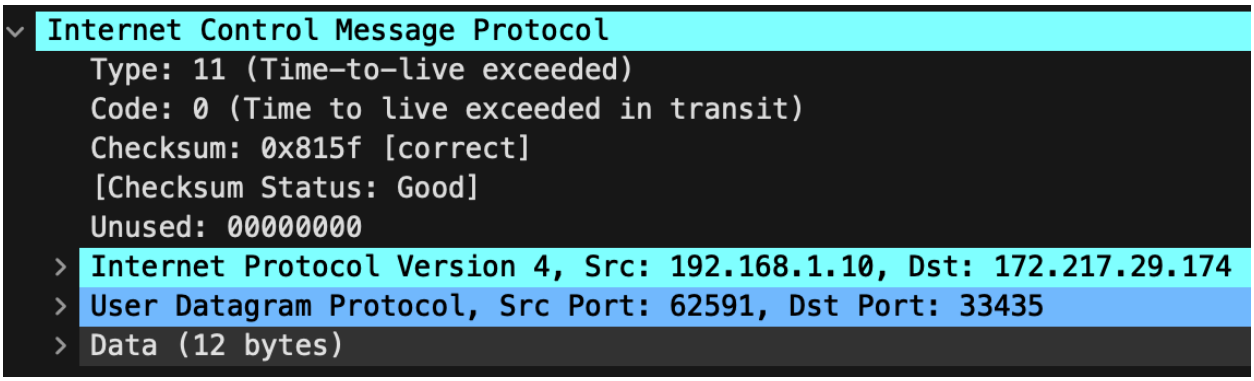


Assim como no ICMPv4, o type, o code, e o checksum são campos fixos no cabeçalho, já os demais podem alterar



Qual o tamanho dos dados ICMP?

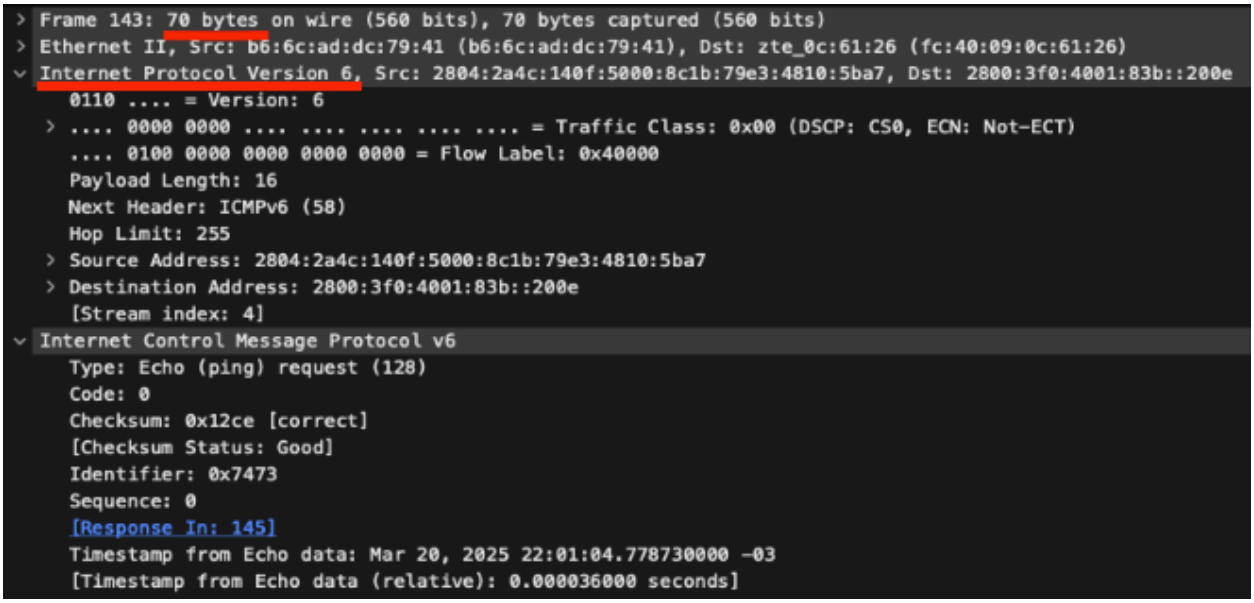
ICMPv4: O tamanho dos dados ICMP varia conforme o tipo da mensagem. No caso da mensagem ICMP Time-to-live exceeded (Type 11) capturada, o Wireshark mostra o campo Data (12 bytes), indicando que a mensagem carrega 12 bytes de dados após o cabeçalho ICMP. Portanto, o tamanho dos dados ICMP nesse pacote é de 12 bytes. Esses dados representam uma cópia do cabeçalho IP e dos primeiros bytes do pacote original que causou o erro, conforme definido pelo padrão do protocolo ICMP.

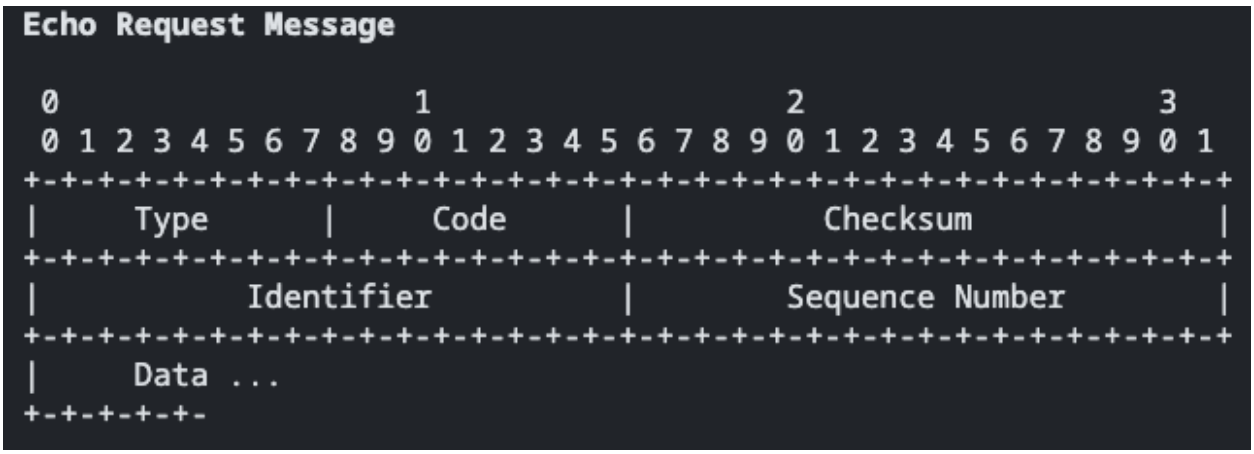


ICMPv6: Embora o Wireshark não exiba o campo Data (X bytes) explicitamente, a presença de campos como Timestamp from Echo data indica que a mensagem ICMPv6 Echo Request carrega dados além do cabeçalho. O cabeçalho ocupa 8 bytes, e o restante corresponde aos dados, que incluem informações como timestamps usados no cálculo do tempo de resposta (RTT). Se analisarmos a imagem a seguir, vemos que esse pacote tem um length de 70 bytes. Sabemos que o cabeçalho IPv6 tem um tamanho fixo

de 40 bytes. Outra informação é que o cabeçalho ICMPv6 de uma mensagem Echo Request tem em seu cabeçalho o Type (8 bits), Code (8 bits), Checksum (16 bits), Identifier (16 bits) e Sequence Number (16 bits), segundo a RFC 4443 (segunda imagem a seguir). Com isso, sabemos que o tamanho do cabeçalho ICMPv6 para essa mensagem é de 64 bits ou 8 bytes. Como o pacote inteiro é de 70 bytes, podemos fazer a seguinte conta:

$$ICMP\ data = 70\ (length\ total) - 40\ (IPv6) - 8\ (ICMPv6) = 22\ bytes$$





Qual a diferença entre o tamanho dos pacotes capturados?

A diferença entre o tamanho dos pacotes ICMP capturados foi de 66 bytes, considerando o maior pacote com 136 bytes e o menor com 70 bytes. Essa variação ocorre devido às diferenças entre os tipos de mensagens ICMP (como Echo Request, Time Exceeded ou Destination Unreachable) e a quantidade de dados ou cabeçalhos encapsulados em cada tipo.