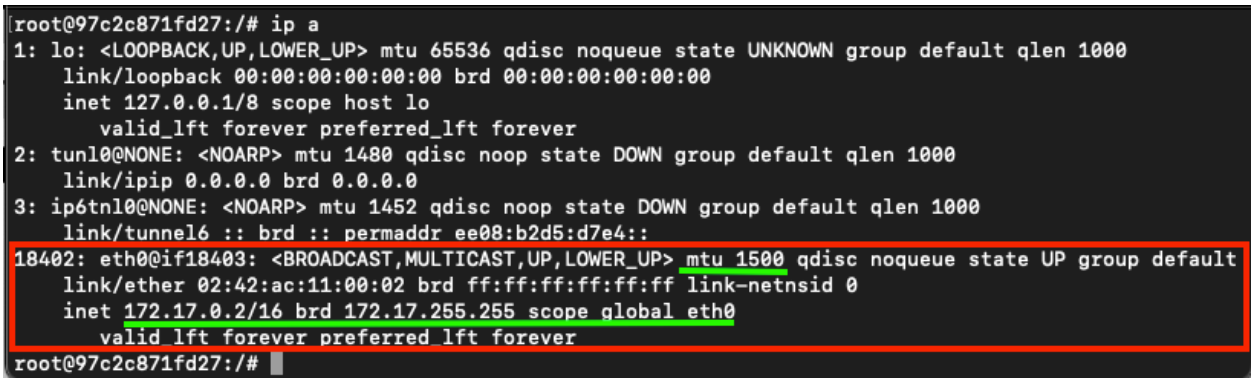
UNISINOS	ATIVIDADE ACADÊMICA: Redes de Computadores: Internetworking, Roteamento e Transmissão TRABALHO: Atividade 2 ALUNOS: Rafael Hansen Klauck

Para fazer essa atividade, utilizei o Docker para criar um container Linux. Isso ajudou a ter um ambiente mais isolado e controlado, facilitando a captura e análise dos pacotes de rede. Além disso, rodar a análise dentro do container reduziu interferências de outros processos do sistema, deixando as informações dos pacotes mais fáceis de visualizar.

1 - Descubra qual IP está configurado na sua máquina?

2 - Qual tamanho do MTU está sendo utilizado?



Para descobrir o IP e o tamanho do MTU foi utilizado o comando *ip* a. Como é possível visualizar na imagem, o IP da máquina é *172.17.0.2* e tamanho do MTU é *1500 bytes.*

3 - Inicie uma coleta de pacotes, como o Wireshark ou tcpdump

Para iniciar uma coleta de pacotes, foi utilizado o tcpdump. Primeiro foi necessário fazer a instalação *apt install -y tcpdump*. Após isso foi utilizado o comando *tcpdump -i eth0 -w captura.pcap* para iniciar a captura. No comando o *-I eth0* significa captura pacotes na interface eth0 e o *-w captura.pcap* é o arquivo em que vai ser salva essa

captura. Após utilizar o comando, foi necessário abrir outro terminal e rodar a mesma instância.

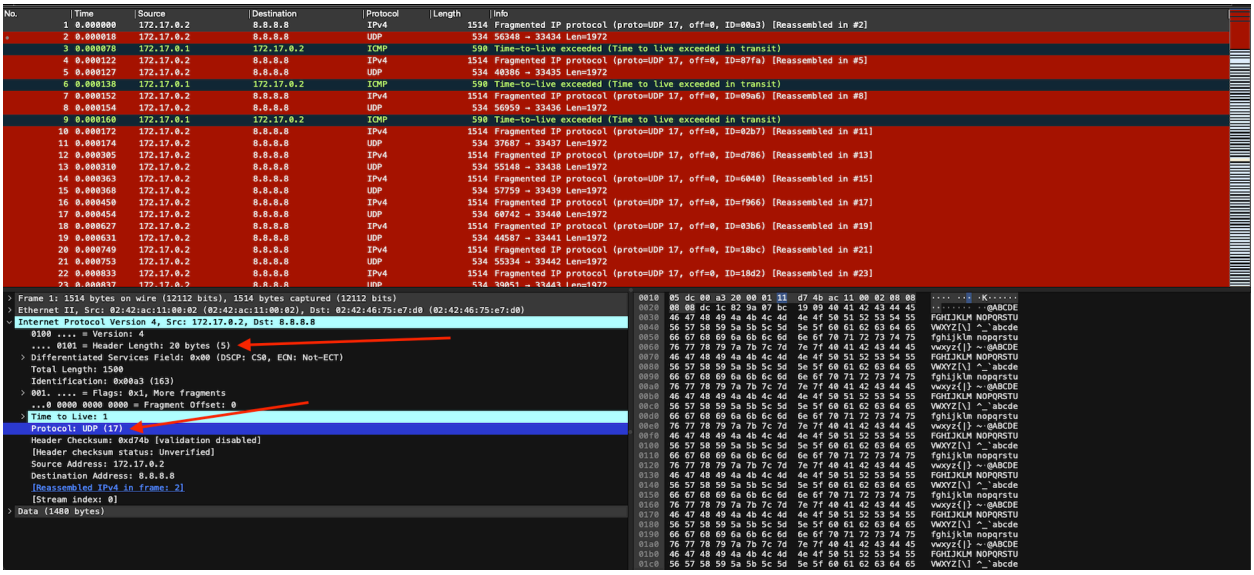
4 - Envie usando o programa traceroute um datagrama de 2000 bytes

Para enviar um datagrama de 2000 bytes foi utilizado o comando *traceroute 8.8.8.8 2000*. Esse comando foi executado em um terminal separado do terminal que estava rodar o comando para capturar pacotes. Após executar o comando *traceroute*, foi necessário finalizar a captura no outro terminal.

Após esses passos, foi necessário transferir o arquivo capturar.pcap do container para meu computador e abrir o arquivo com o Wireshark para visualizar seu conteúdo e responder as demais perguntas.

5 - Dentro do cabeçalho do pacote IP, qual é o valor no campo de protocolo da camada superior?

6 - Quantos bytes há no cabeçalho IP?



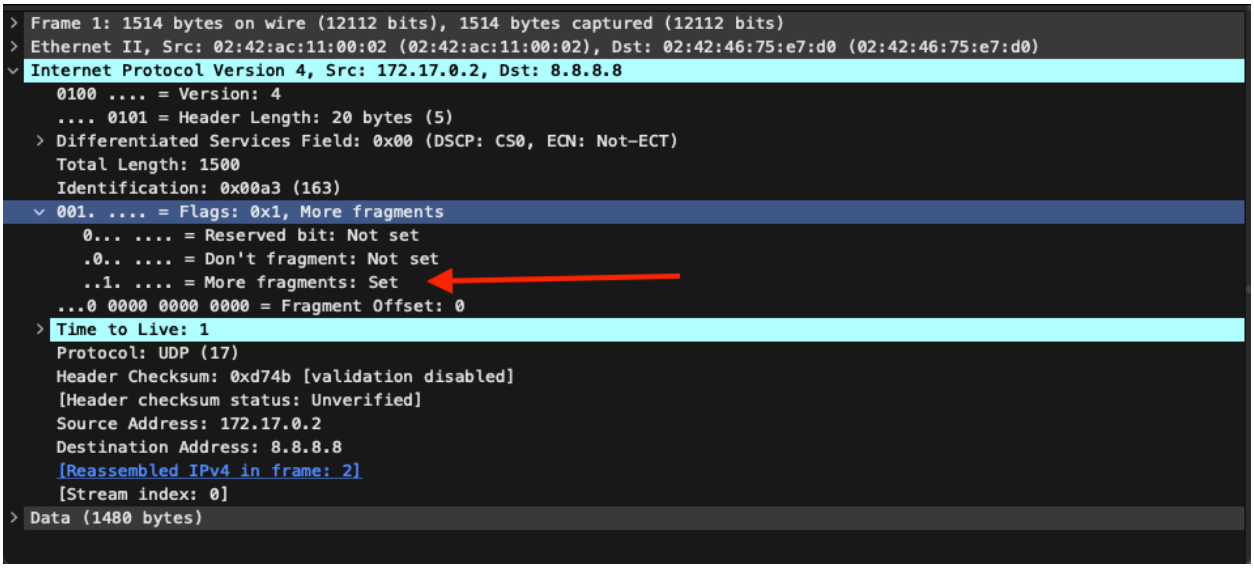
Como podemos ver na imagem, o valor no campo de protoloca da camada superior é 17, que é UDP e o tamanho do cabeçalho IP é 20 bytes.

7 - Quantos bytes estão no payload do datagrama IP? Explique como você determinou o número de bytes de carga útil.

O datagrama IP original tinha 1972 bytes antes da fragmentação. Como o cabeçalho IP ocupa 20 bytes, o payload total do datagrama é 1952 bytes (1972 - 20). Como esse valor excede o MTU da Ethernet (1500 bytes), ele foi fragmentado em dois pacotes menores: o primeiro fragmento contém 1480 bytes de payload e o segundo 472 bytes (1480 + 472 = 1952).

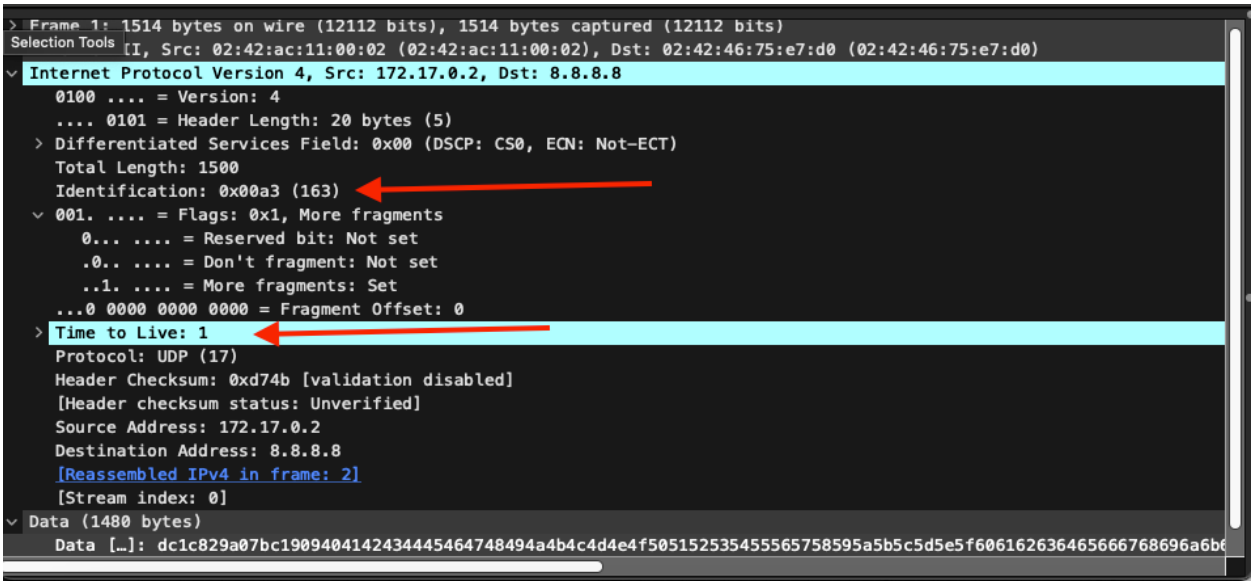
8 - Este datagrama IP foi fragmentado? Explique como você determinou se o datagrama foi ou não fragmentado. Quais os valores dos fragmentos?

Sim, o datagrama foi fragmentado. Para determinar isso, foi analisado as flags do cabeçalho IP, mais precisamente a flag MF(More Fragments). A imagem a seguir, mostra que essa flag está setada com 1, informando que há mais fragmentos após esse.



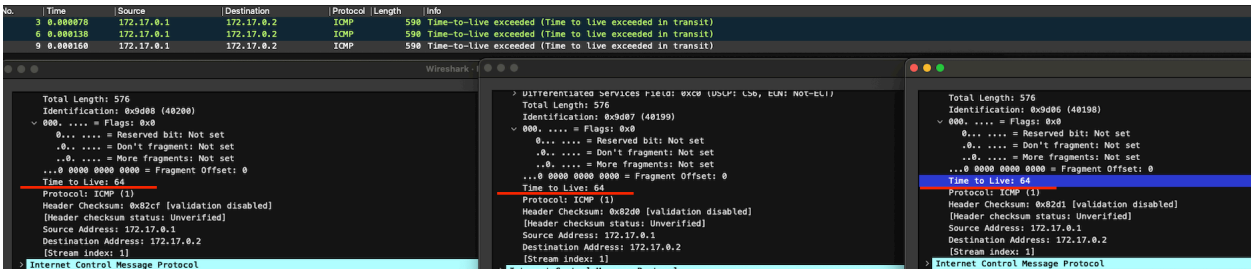
Assim como ja mencionado na resposta da pergunta 7, o tamanho do primeiro fragmento é 1500 bytes (1480 bytes de payload + 20 bytes de cabeçalho) e do segundo fragmento 512 bytes (492 bytes de payload + 20 bytes de cabeçalho).

9 - Qual é o valor do campo Identification e do campo TTL?



Como podemos ver na imagem, o TTL é 1 e o Identiciation é 0x00a3 (163 em decimal)

10 - Esses valores permanecem inalterados para todas as respostas ICMP TTL excedidas enviadas ao seu computador pelo roteador mais próximo (primeiro salto)? Por que?



As respostas ICMP TTL Exceeded enviadas pelo roteador mais próximo ao meu computador não mantêm o mesmo valor no campo Identification. O campo Identification é um identificador único para cada datagrama IP e muda na resposta ICMP, porque essa resposta é um novo pacote gerado pelo roteador. Já o campo TTL também pode mudar, porque o roteador define um novo valor inicial para a resposta ICMP. Além disso, esse TTL diminui a cada roteador pelo qual a resposta passa antes de chegar ao meu

computador. Portanto, o valor de Identification na resposta ICMP não permanece inalterado, pois a resposta é um novo datagrama IP gerado pelo roteador. Já o TTL geralmente muda, pois cada roteador define um TTL inicial diferente para a resposta ICMP. No meu caso, o TTL se manteve igual, mas isso pode variar dependendo da rede e dos roteadores intermediários.