Atividade sobre IP

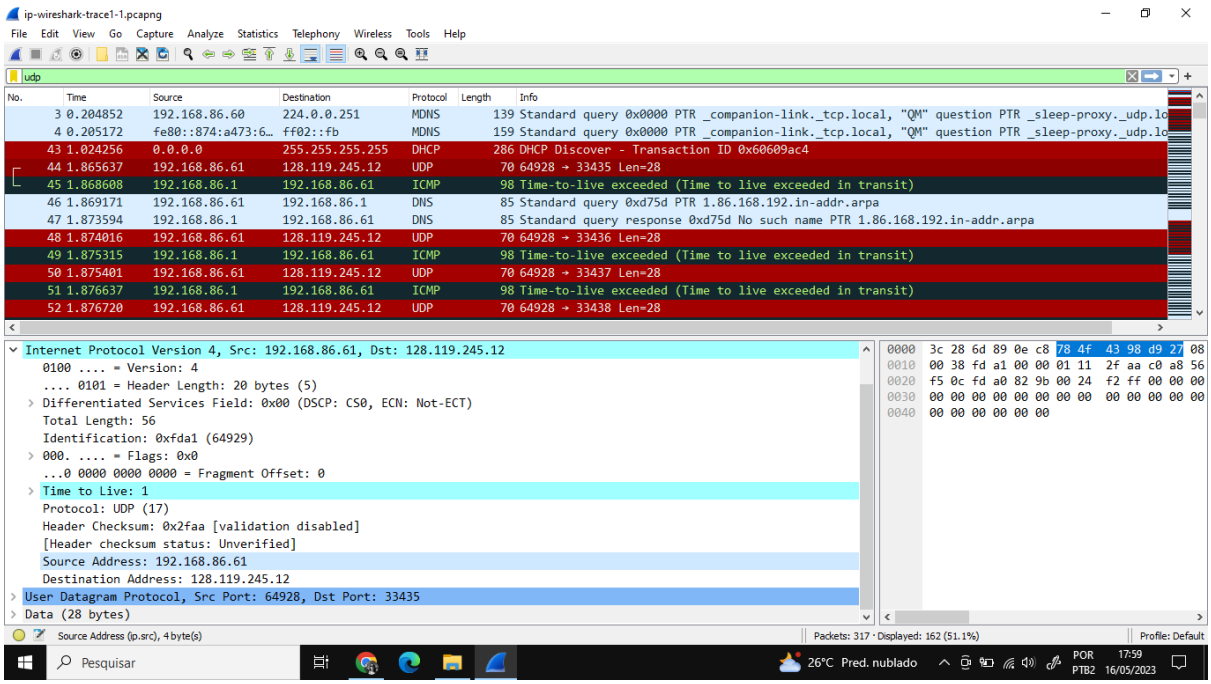
Redes de Computadores

Sabrina Araújo Cardoso - 118210114

Wireshark Lab: IP

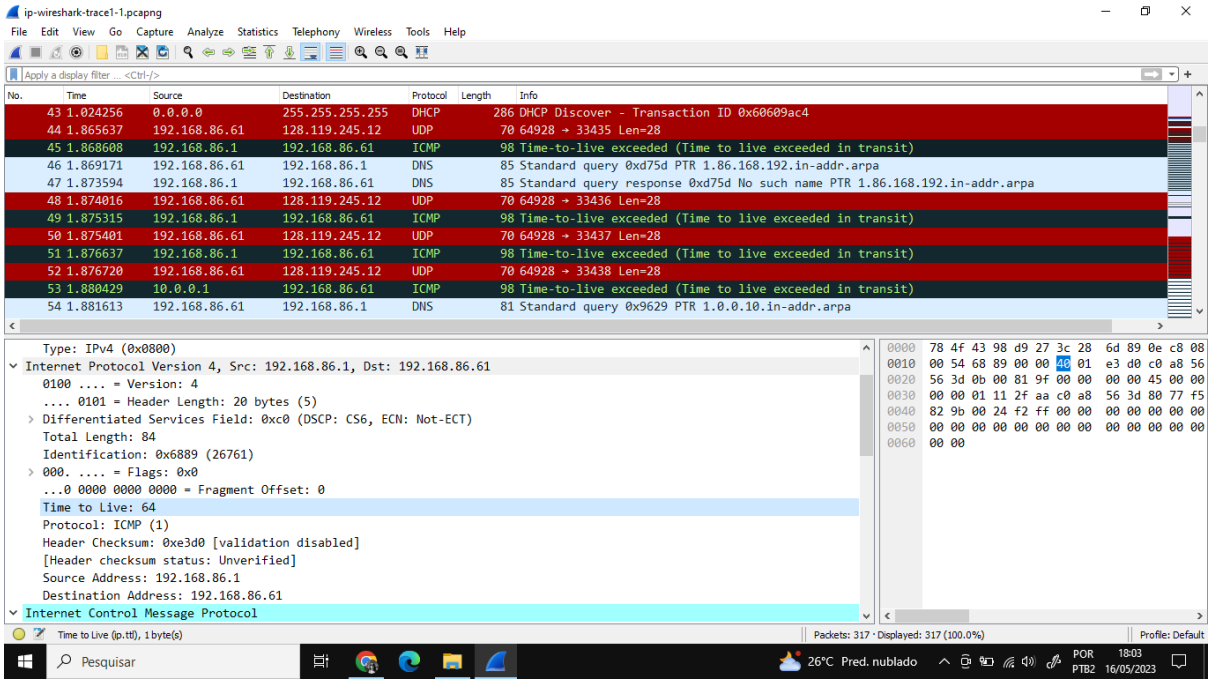
A atividade foi feita utilizando o pacote capturado pelo autor.

- **Questão 1:** Selecione o primeiro segmento UDP enviado pelo seu computador através do comando traceroute para gaia.cs.umass.edu. (Dica: este é o 44º pacote no arquivo de rastreamento ip-wireshark-trace1-1.pcapng no rodapé 2). Expanda a parte do Protocolo da Internet (Internet Protocol) no detalhes do pacote. Qual é o endereço IP do seu computador?



> IP: **192.168.86.61**
>
> Porta: **64928**

- **Questão 2:** Qual é o valor no campo "time-to-live" (TTL) no cabeçalho deste datagrama IPv4?



> TTL : **64**

- **Questão 3:** Qual é o valor no campo "protocolo de camada superior" no cabeçalho deste datagrama IPv4?

> Protocol: **ICMP (1)**

Questão 4: Quantos bytes há no cabeçalho IP?

> Header Length: **20 bytes**

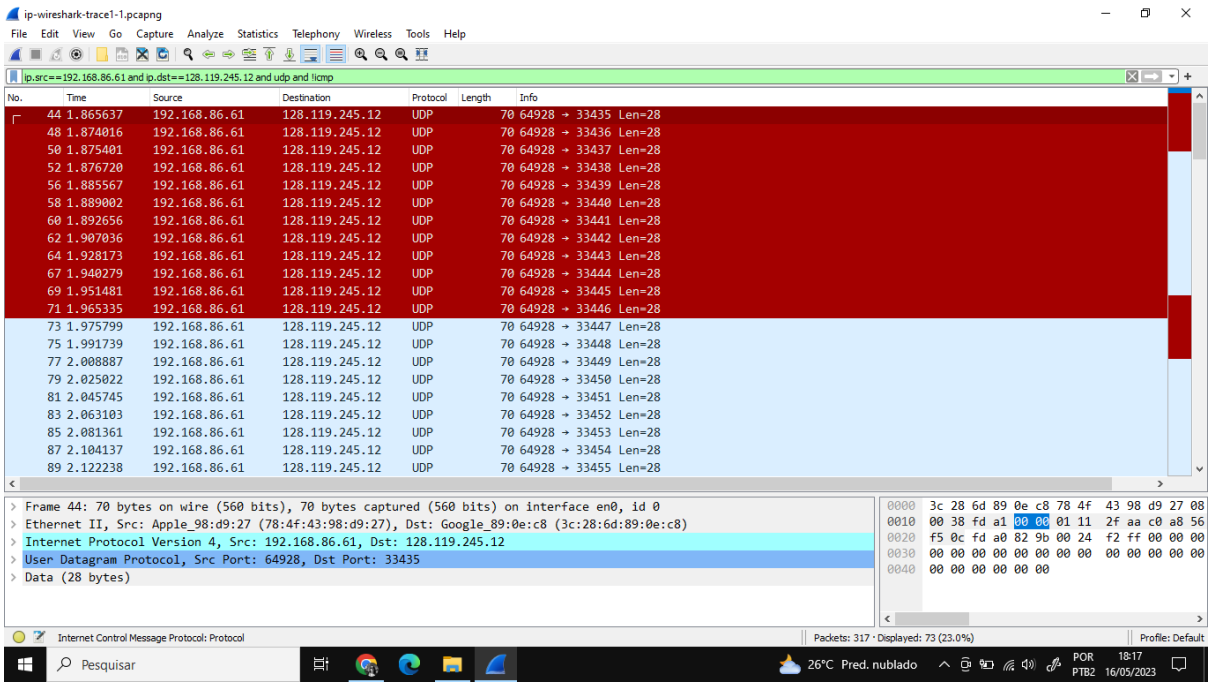
- **Questão 5:** Quantos bytes há na carga útil do datagrama IP? Explique como você determinou o número de bytes da carga útil.

> NºBytes datagram = Total Length - Header Length = 84 - 20 = **64 bytes**

- **Questão 6:** Este datagrama IP foi fragmentado? Explique como você determinou se o datagrama foi fragmentado ou não.

> Fragmet Offset: **0**
> O datagrama não foi fragmentado.

- **Questão 7:** Quais campos no datagrama IP sempre mudam de um datagrama para o próximo nesta série de segmentos UDP enviados pelo seu computador com destino a 128.119.245.12, via traceroute? Por quê?



> **Identificação, Tempo de vida (TTL) e Soma de verificação do cabeçalho (Header checksum) sempre mudam.**

- **Questão 8:** Quais campos nesta sequência de datagramas IP (contendo segmentos UDP) permanecem constantes? Por quê?

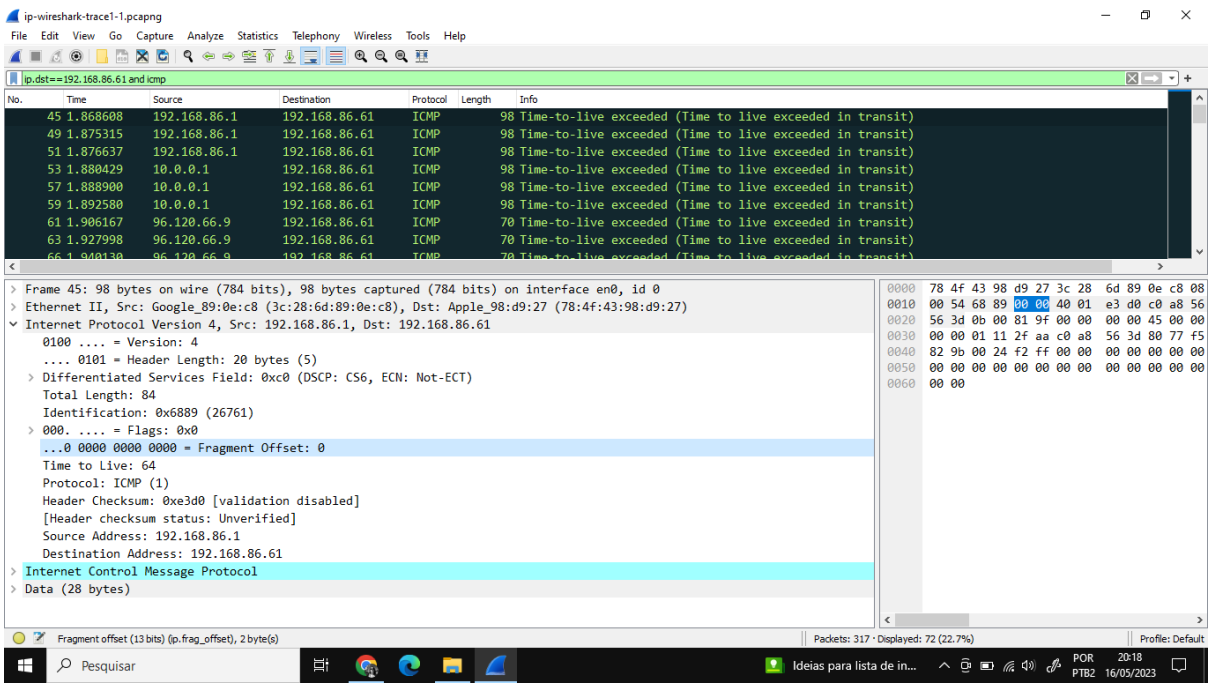
> Os campos que permanecem constantes nos datagramas IP são:

> **• Versão (pois estamos usando IPv4 para todos os pacotes)**
> **• Header Length (pois são pacotes ICMP)**
> **• IP de origem (pois estamos enviando da mesma origem)**
> **• IP de destino (pois estamos enviando para o mesmo destino)**
> **• Serviços Diferenciados (pois todos os pacotes são ICMP e usam a mesma classe de Tipo de Serviço)**
> **• Protocolo de Camada Superior (pois são pacotes ICMP)**

- **Questão 9:** Descreva o padrão que você observa nos valores do campo de Identificação dos datagramas IP sendo enviados pelo seu computador.

> **O padrão é que os campos de Identificação do cabeçalho IP aumentam a cada ICMP Echo (ping) request.**

- **Questão 10:** Qual é o protocolo da camada superior especificado nos datagramas IP retornados pelos roteadores? [Observação: as respostas para Linux/MacOS diferem do Windows aqui].



> Protocol: **ICMP**

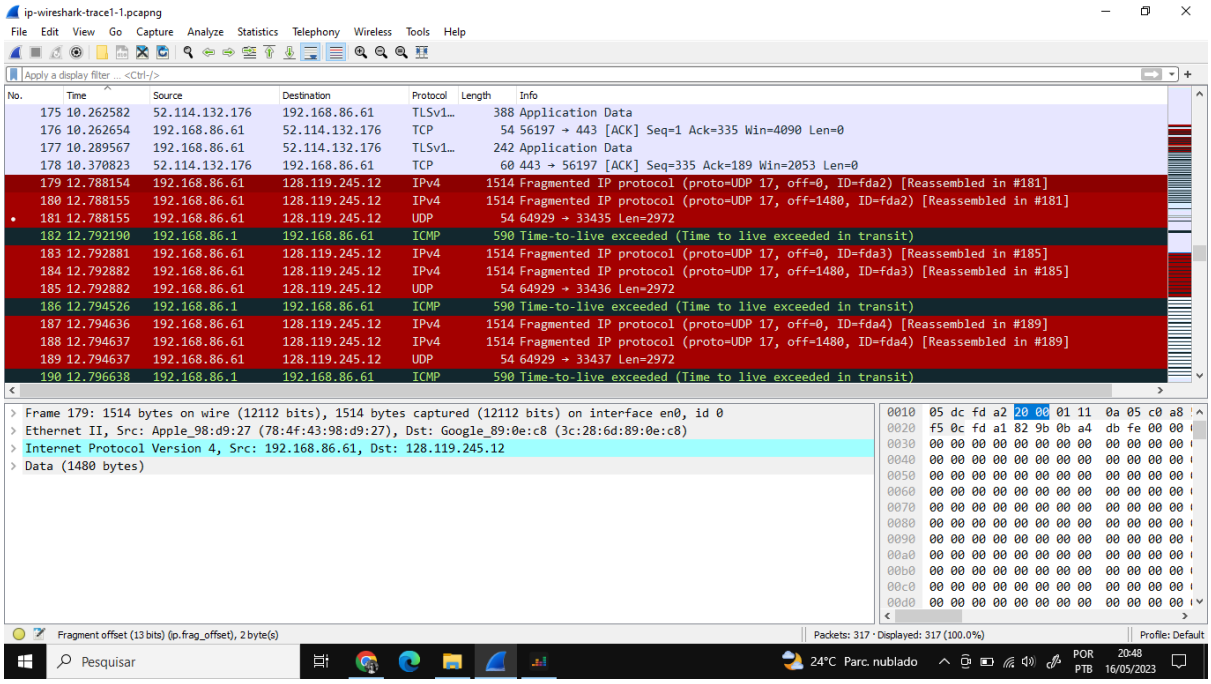
- **Questão 11:** Os valores nos campos de Identificação (através da sequência de todos os pacotes ICMP de todos os roteadores) são semelhantes ao comportamento da resposta à pergunta 9 acima?

> **Sim**

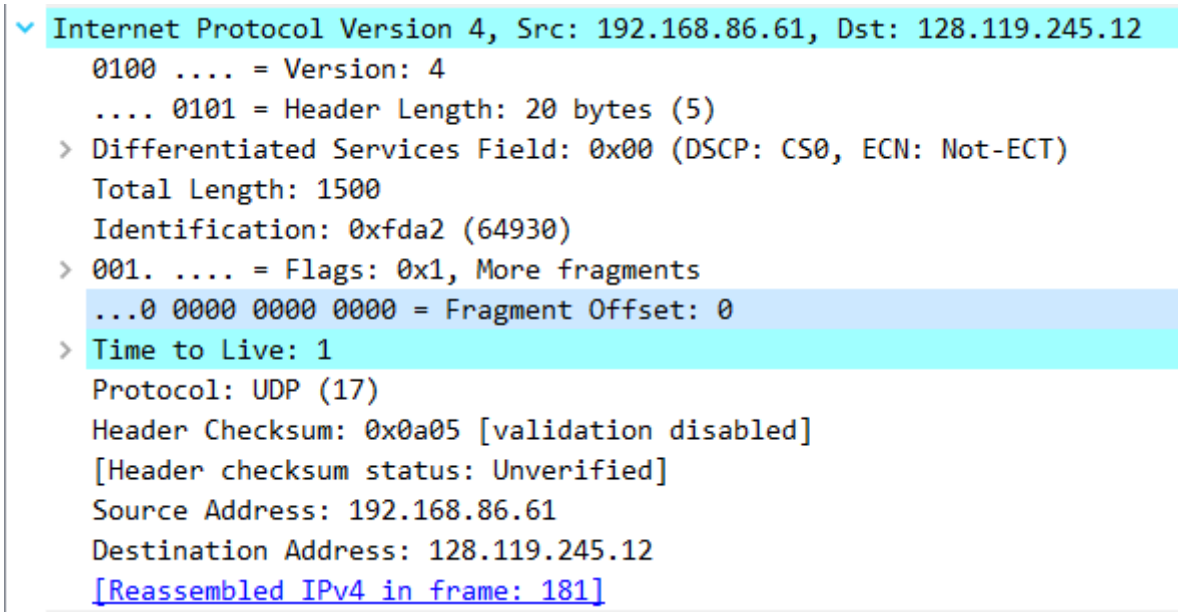
- **Questão 12:** Os valores dos campos TTL são semelhantes em todos os pacotes ICMP de todos os roteadores?

> **Sim. Os valores só mudam quando muda os roteadores e a rota.**

- **Questão 13:** Encontre o primeiro datagrama IP contendo a primeira parte do segmento enviado para 128.119.245.12 pelo seu computador via comando traceroute para gaia.cs.umass.edu, após você especificar que o comprimento do pacote traceroute deve ser 3000. (Dica: Este é o pacote 179 no arquivo de rastreamento ip-wireshark-trace1-1.pcapng na nota de rodapé 2. Os pacotes 179, 180 e 181 são três datagramas IP criados pela fragmentação do primeiro segmento UDP de 3000 bytes enviado para 128.119.145.12). Esse segmento foi fragmentado em mais de um datagrama IP? (Dica: a resposta é sim!)



- **Questão 14:** Quais informações no cabeçalho IP indicam que este datagrama foi fragmentado?



More fragments

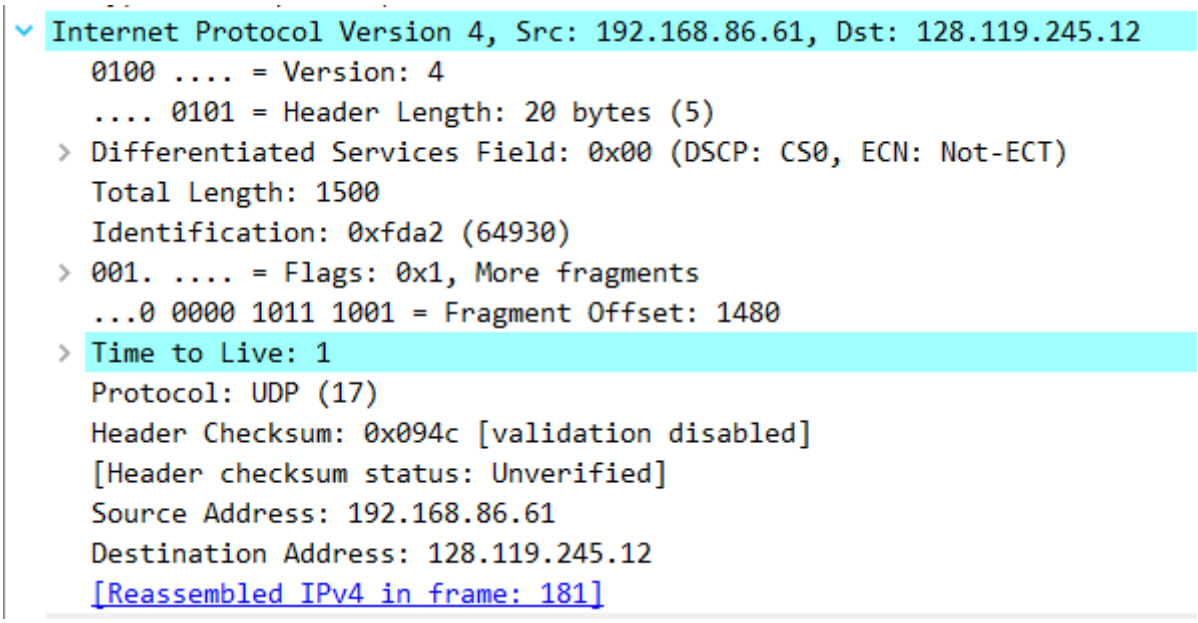
- **Questão 15:** Qual informação no cabeçalho IP deste pacote indica se este é o primeiro fragmento ou um fragmento posterior?

> **Fragment Offset: 0 - indica o primeiro fragmento.**
> **Fragment Offset: 1480 - indica o segundo fragmento.**

- **Questão 16:** Quantos bytes existem neste datagrama IP (header mais payload)?

> **1500+20 = 1520 bytes**

- **Questão 17:** Agora, analise o datagrama contendo o segundo fragmento do segmento UDP fragmentado. Que informação no cabeçalho IP indica que este não é o primeiro fragmento do datagrama?



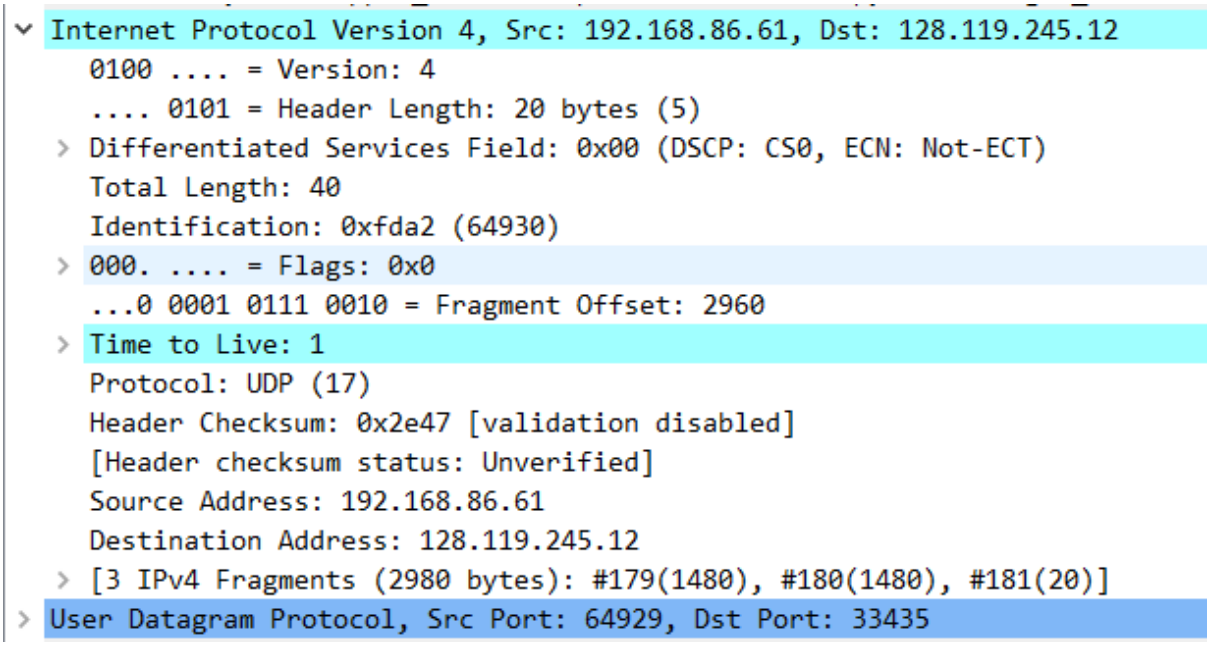
Fragment Offset: 1480 - indica o segundo fragmento.

- **Questão 18:** Agora, analise o datagrama contendo o segundo fragmento do segmento UDP fragmentado. Que informação no cabeçalho IP indica que este não é o primeiro fragmento do datagrama?

> **Os campos do cabeçalho IP que mudaram entre os fragmentos são: comprimento total, flags, fragment offset e**

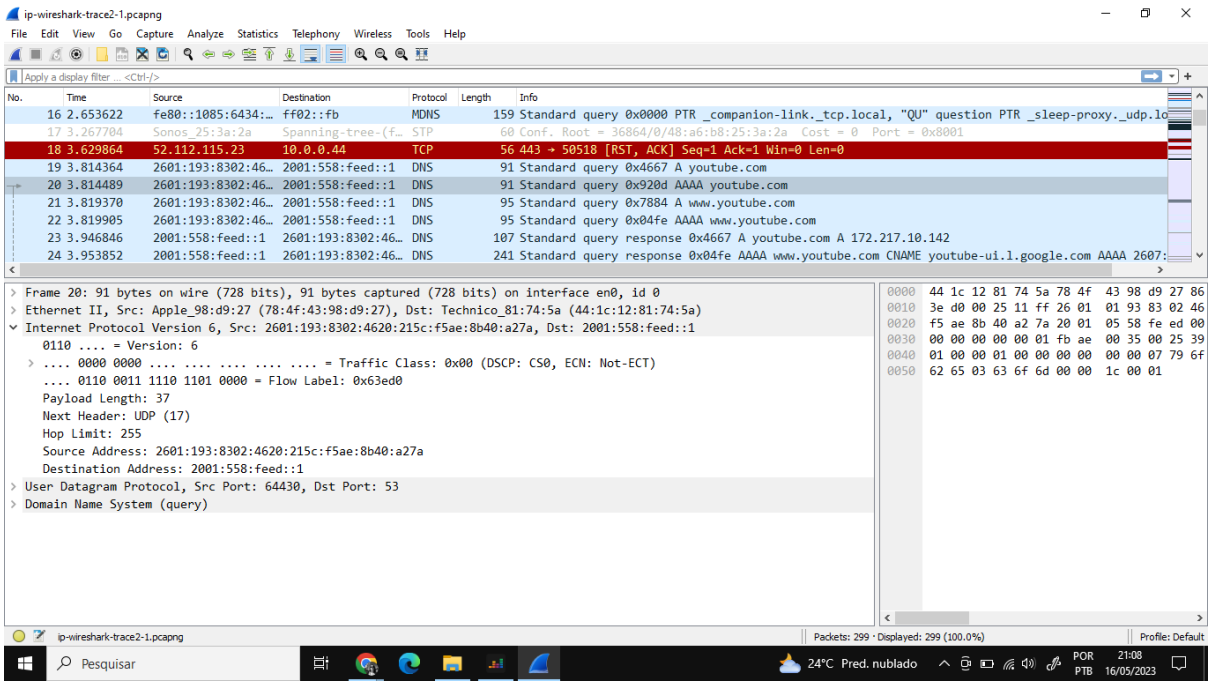
checksum.

- **Questão 19:** Agora encontre o datagrama IP que contém o terceiro fragmento do segmento UDP original. Que informação no cabeçalho IP indica que este é o último fragmento desse segmento?



Fragment Offset: 1480 - Indica o terceiro fragmento

- **Questão 20:** Qual é o endereço IPv6 do computador que está fazendo a solicitação DNS AAAA? Este é o endereço de origem do 20º pacote no trace. Forneça o endereço de origem IPv6 para esse datagrama exatamente na mesma forma que é exibida na janela do Wireshark.



> Source Address: **2601:193:8302:4620:215c:f5ae:8b40:a27a**

- **Questão 21:** Qual é o endereço de destino IPv6 para este datagrama? Forneça este endereço IPv6 exatamente na mesma forma que é exibida na janela do Wireshark.

> Destination Address: **2001:558:feed::1**

- **Questão 22:** Qual é o valor do rótulo de fluxo (flow label) para este datagrama?

> Flow Label: **0x063ed0**

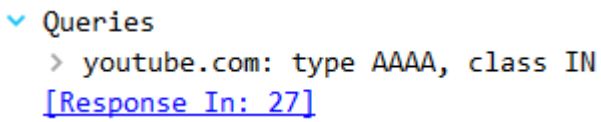
- **Questão 23:** Quantos dados de carga útil (payload) são transportados neste datagrama?

> Payload Length: **37**

- **Questão 24:** Qual é o protocolo da camada superior para o qual a carga útil deste datagrama será entregue no destino?

> Next Header: **UDP (17)**

- **Questão 25:** Quantos endereços IPv6 são retornados na resposta a este pedido AAAA?



> **27**

- **Questão 26:** Qual é o primeiro dos endereços IPv6 retornados pelo DNS para youtube.com (no arquivo de rastreamento ip-wireshark-trace2-1.pcapng, este é também o endereço que é numericamente o menor)? Forneça este endereço IPv6 na mesma forma abreviada exata conforme exibido na janela do Wireshark.

> Source Address: **2601:193:8302:4620:215c:f5ae:8b40:a27a**