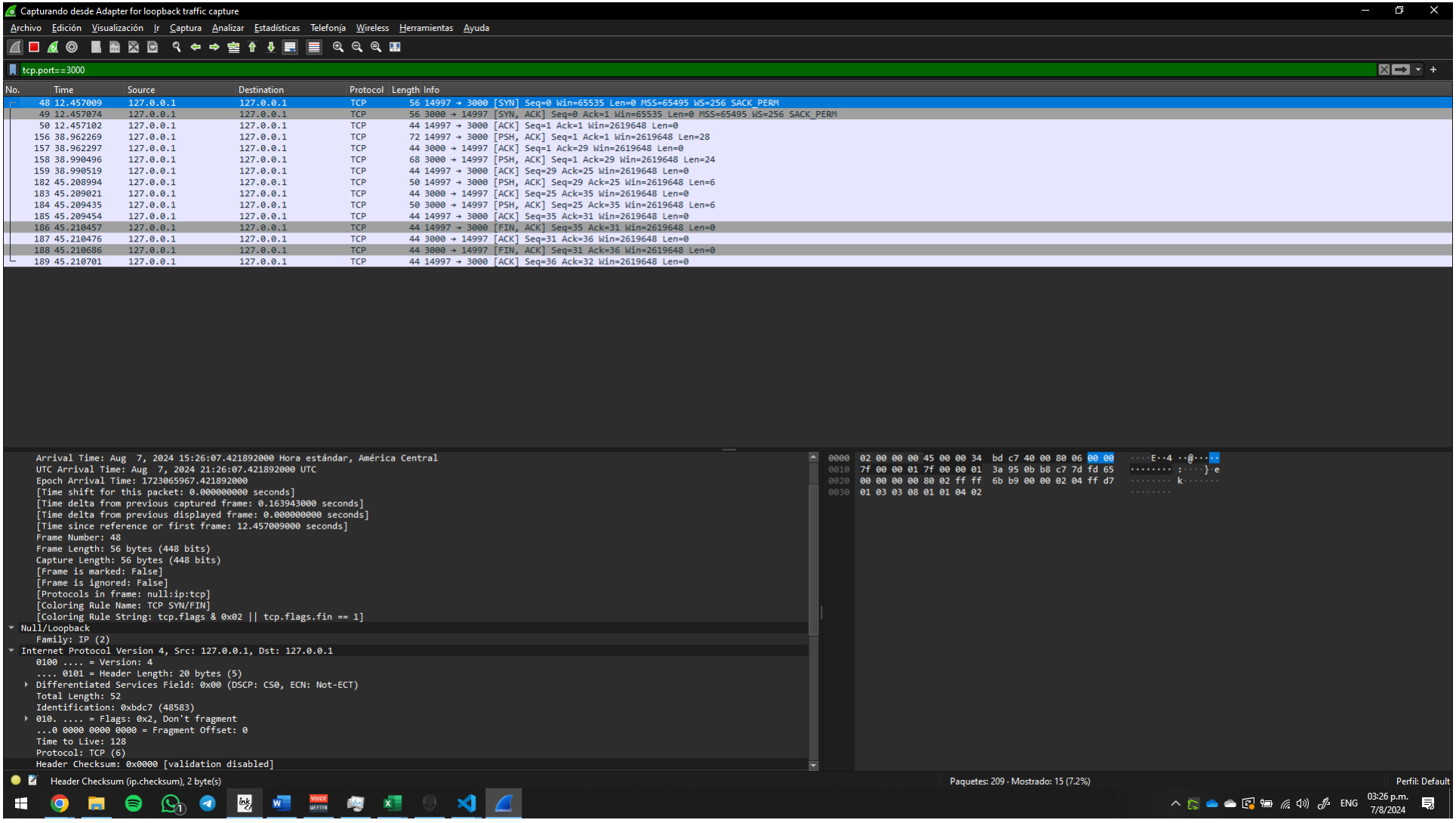
Laboratorio 05 – 21000492

SECCIÓN TCP:

1. Captura de paquetes



2. Análisis de encabezados

No.	Source	Destination	Length	Flags	Seq	Ack	Win	Len	MSS	WS	SACK_PERM
48	14997	3000	56	SYN	0		65535	0	65495	256	SACK_PERM
49	3000	14997	56	SYN, ACK	0	1	65535	0	65495	256	SACK_PERM
50	14997	3000	44	ACK	1	1	2619648	0			
156	14997	3000	72	PSH, ACK	1	1	2619648	28			
157	3000	14997	44	ACK	1	29	2619648	0			
158	3000	14997	68	PSH, ACK	1	29	2619648	24			
159	14997	3000	44	ACK	29	25	2619648	0			
182	14997	3000	50	PSH, ACK	29	25	2619648	6			
183	3000	14997	44	ACK	25	35	2619648	0			
184	3000	14997	50	PSH, ACK	25	35	2619648	6			
185	14997	3000	44	ACK	35	31	2619648	0			
186	14997	3000	44	FIN, ACK	35	31	2619648	0			
187	3000	14997	44	ACK	31	36	2619648	0			
188	3000	14997	44	FIN, ACK	31	36	2619648	0			
189	14997	3000	44	ACK	36	32	2619648	0			

14997 -> Client
3000 -> Server

3. Preguntas de análisis

¿Cuál es el número de secuencia (Sequence Number) inicial y final de la conexión?¿Hace sentido que sean esa cantidad, por qué?

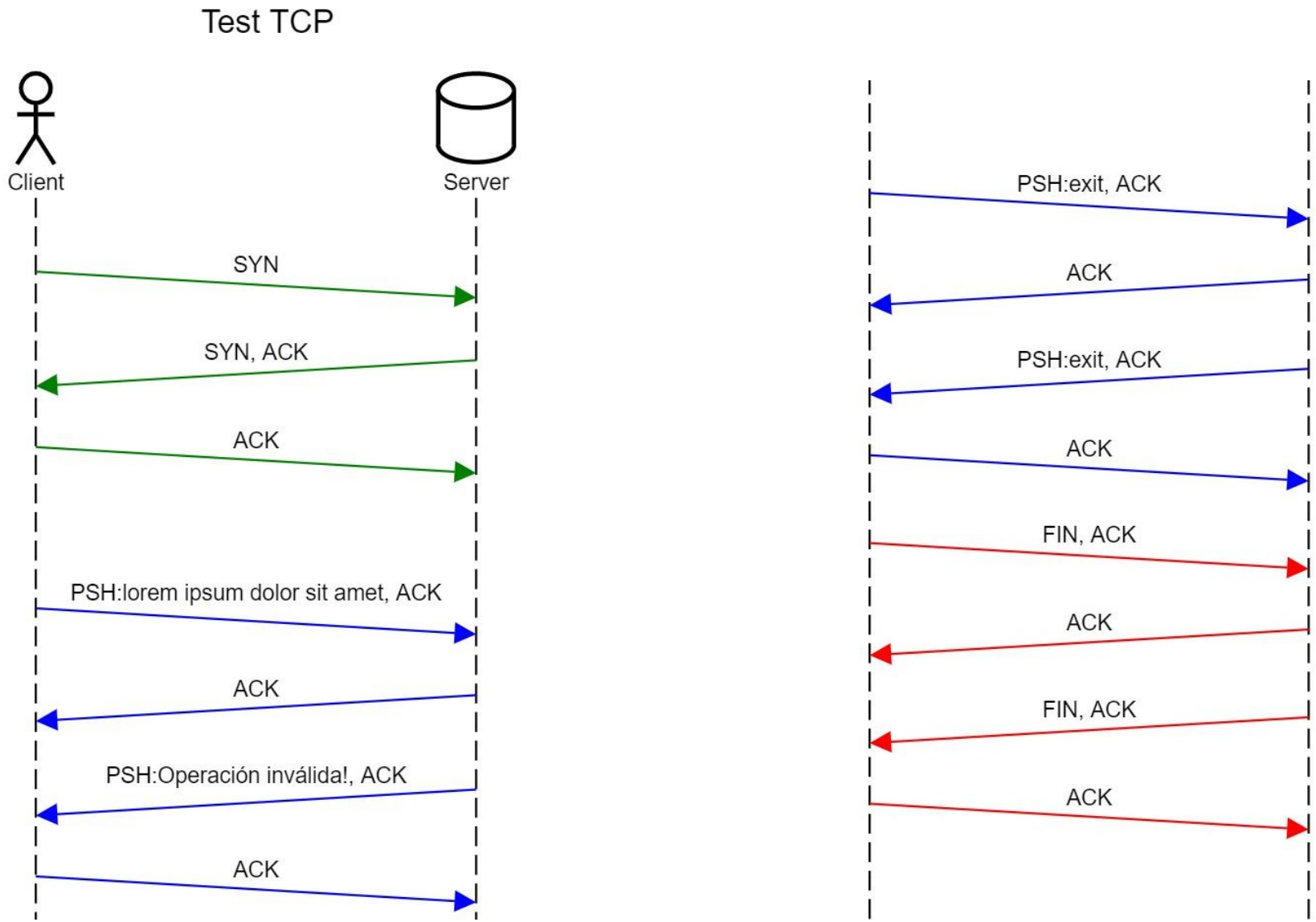
Seq inicial es 0. Seq final es 36 (31 para Server).

Sí tiene sentido, según lo que investigué, el Seq es el número de información que se ha mandado acumulado. Esta comienza en 0, vemos que con el primer mensaje aumenta a 1, cuando el cliente envía 28 el siguiente seq de cliente es 29 y el ack de server también. Y cuando el server manda lenght 24, el ack del cliente es 25 y el siguiente seq del server es 25. Y así continúa hasta cerrar la conexión.

¿Se enviaron 4 mensajes, por lo cual solo deben de existir 4 paquetes con DATA? ¿Es eso correcto o existen más paquetes?

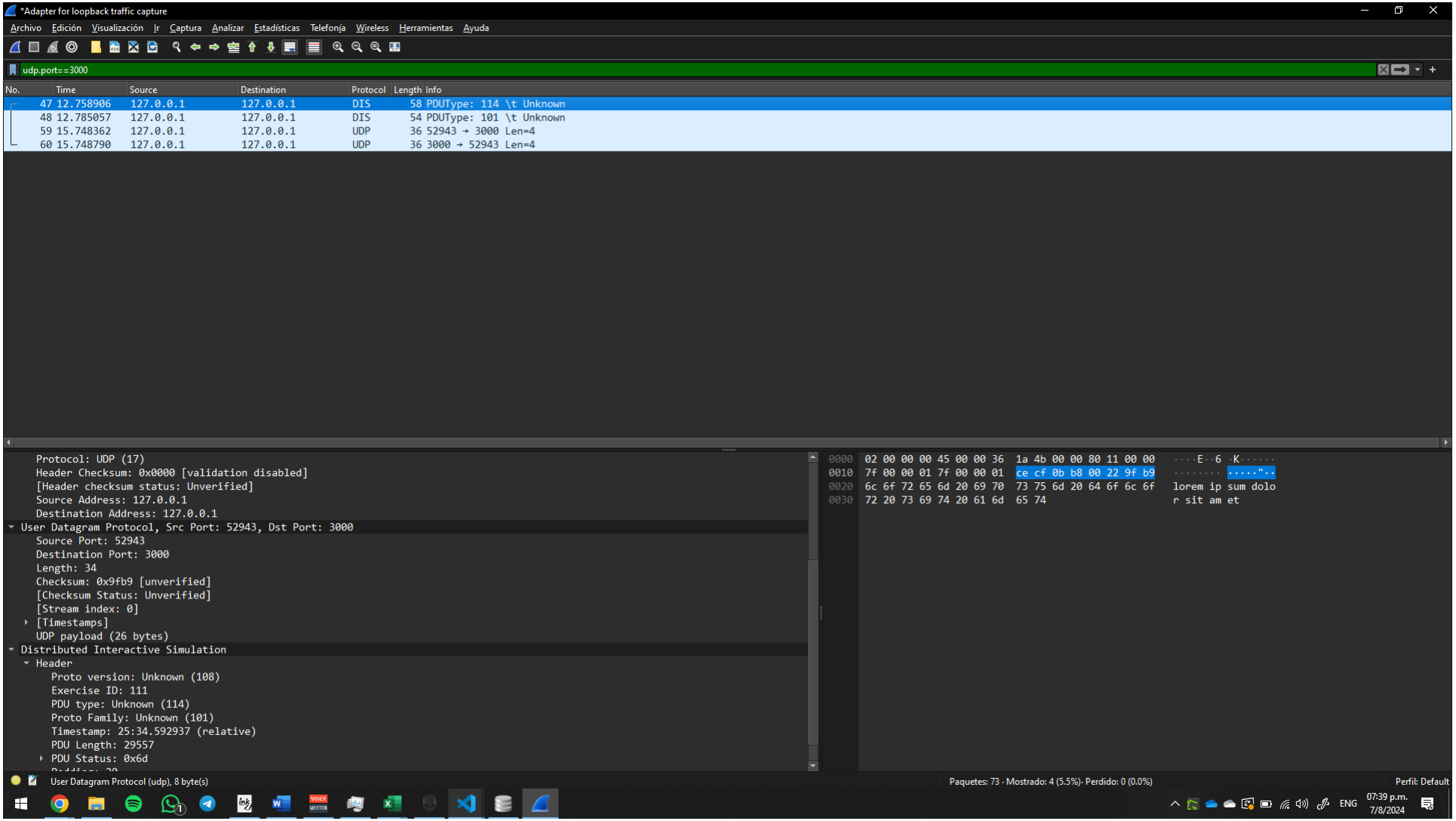
Sí. Los únicos 4 paquetes con DATA deberían ser los mensajes de: Lorem Ipsum...; Operación inválida! ; exit ; exit ;

4. Diagrama Secuencial



Sección UDP:

1. Captura de paquetes



2. Análisis de encabezados

No.	Source	Destination	Length	Len	Checksum	Data
47	52943	3000	58	34	0x9fb9	lorem ipsum dolor sit amet
48	3000	52943	54	30	0x816b	Operación no válida!
59	52943	3000	36	4	0x585f	exit
60	3000	52943	36	4	0x585f	Exit

14997 -> Client
3000 -> Server

3. Preguntas de análisis

¿Se generó algún ICMP durante la transmisión? ¿Podría generarse alguno?

Se colocó el filtro “udp.port==3000 || icmp” para verificar si había algún ICMP, pero tampoco apareció ningún paquete nuevo.

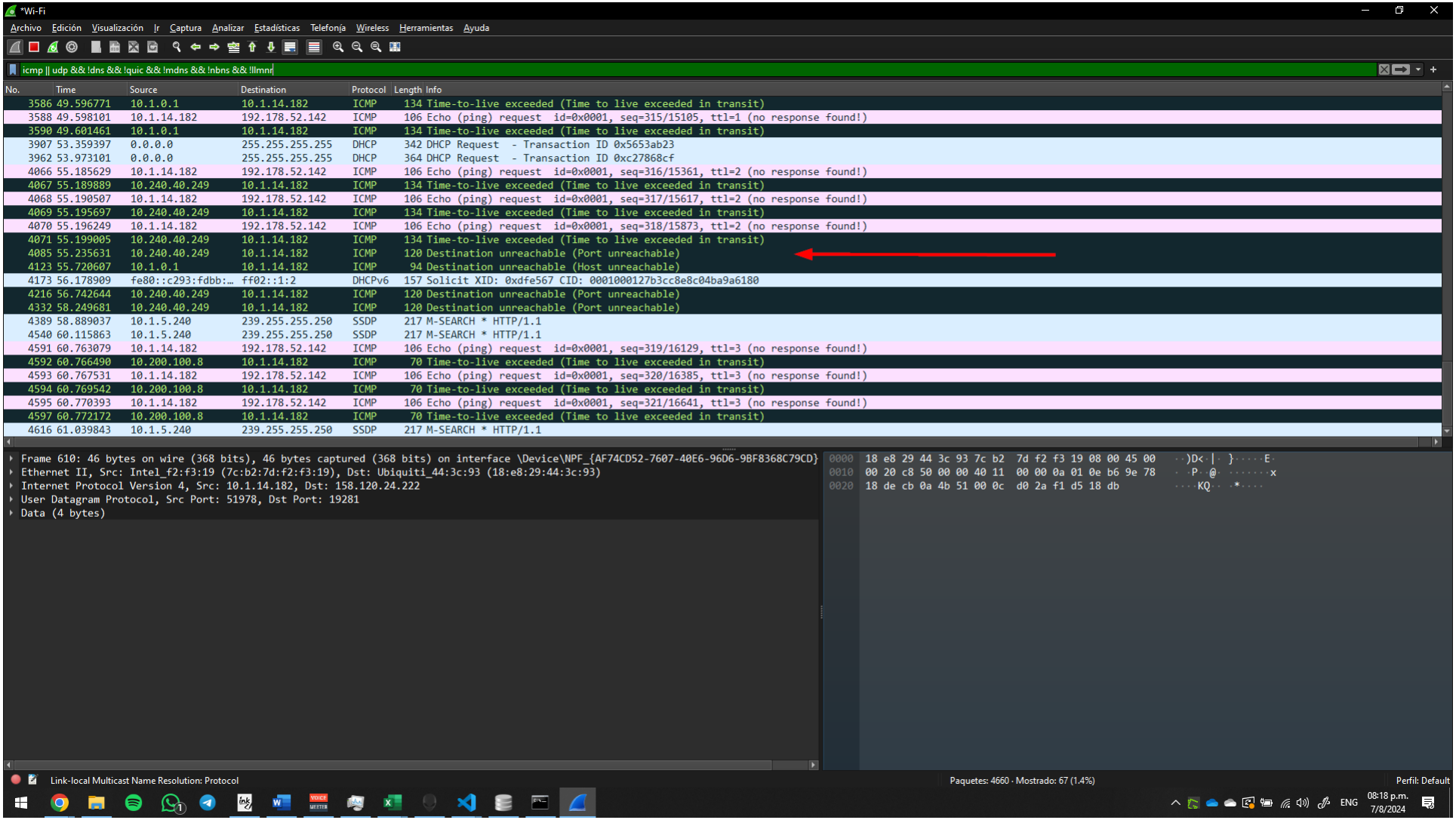
Según la captura, ¿los paquetes tenían el mismo length? Si no, ¿cuál piensa que sea el motivo?

No tenían el mismo length ya que el mensaje (data) no tiene el mismo length. Pero vemos que mensajes con el mismo tamaño (exit) ambos tienen el mismo length ya que tienen el mismo contenido.

Sección ICMP

1. Captura de paquetes

Tracert google.com ----- Port Unreachable, Host unreachable, Time-to-live exceeded



ping google.com ----- Echo Reply y Request