**Ingeniería de Protocolos**

**Grados en Ingenierías Informáticas**

**E.T.S.I. Informática**

**Curso 2021/2022**

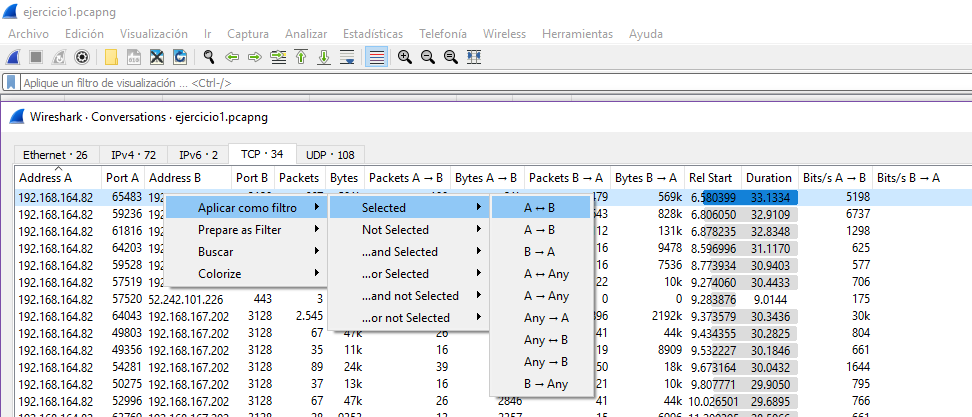
**Práctica I. Análisis de rendimiento con Wireshark.**

**s de rendimiento**

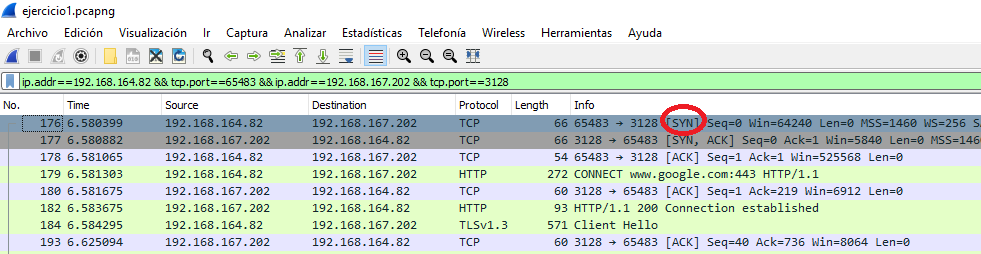
**Ejercicios para clase**

**0.** Usando el fichero “CapturaInicial”, seguir los pasos de la guía y documentarlo con capturas (los valores no tienen porqué coincidir con los indicados en esta guía).

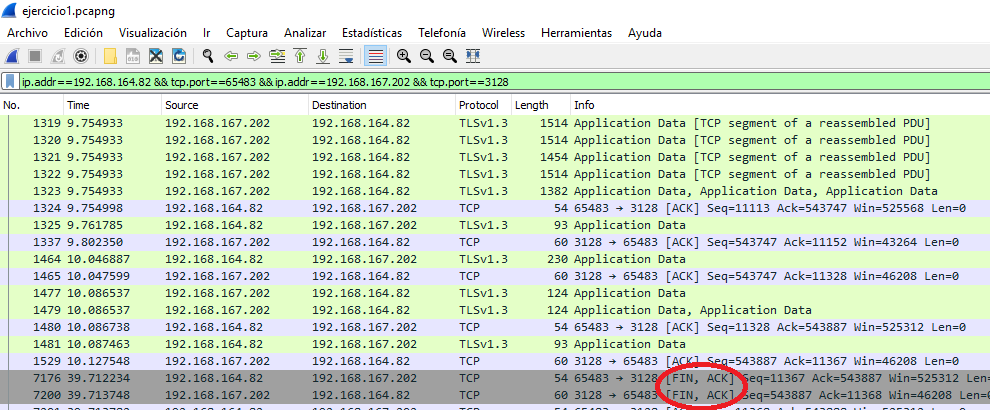
**Realizamos “Statistics Conversation List TCP (IPv4 & IPv 6)” y seguimos con “Apply as Filter Selected A<->B” y cerramos la ventana de las conversaciones.**



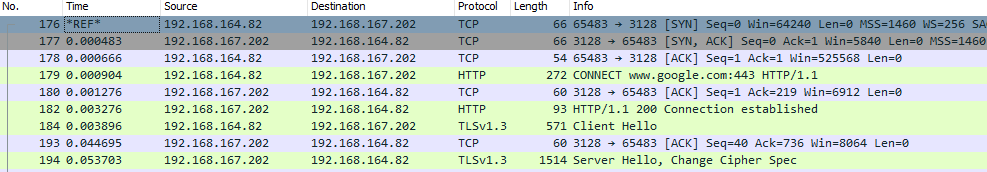
**Podemos ver que el primer paquete de la conexión, el paquete “SYN”, que inicia el “three-way handshake” en el protocolo TCP:**

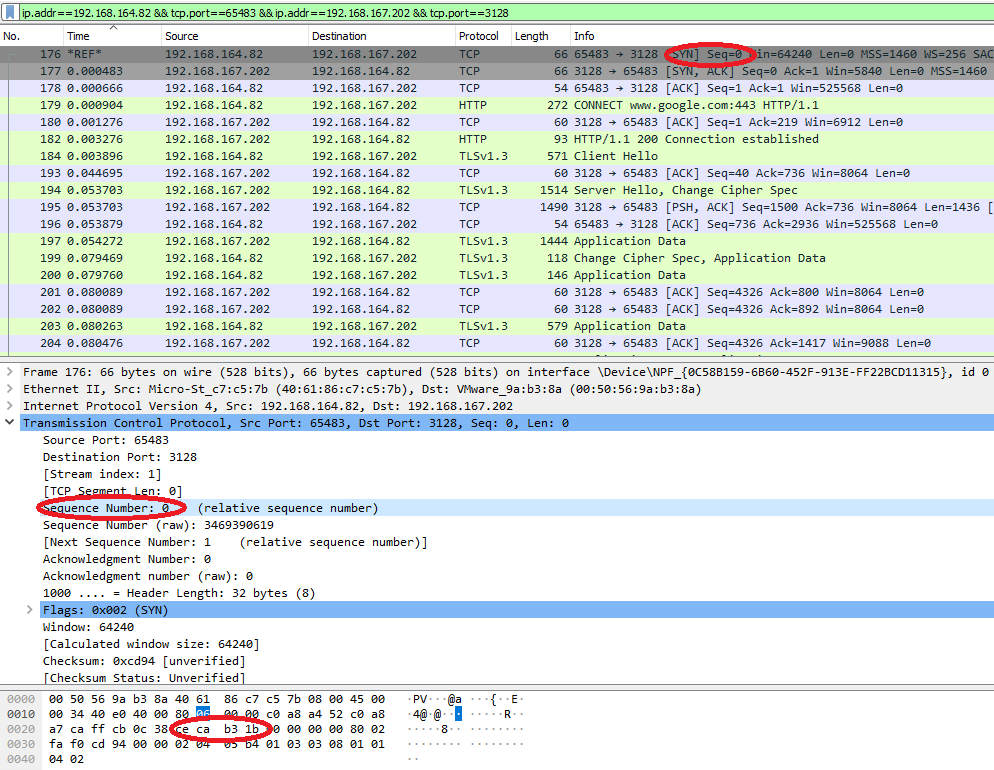


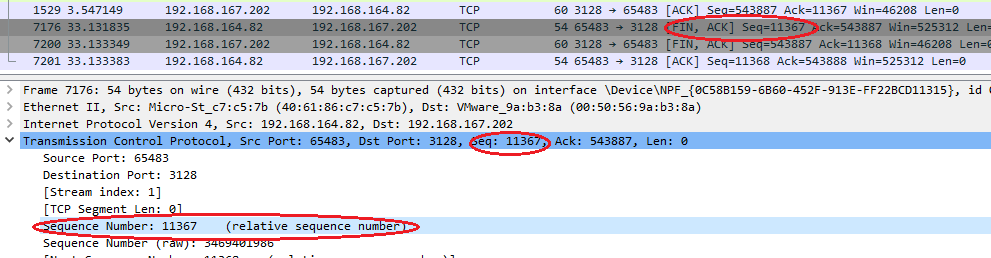
**De la misma manera, al final de la conexión debe verse la secuencia típica para cerrar una conexión TCP (“FIN; ACK; FIN; ACK”):**



Seleccionamos el primer paquete y le damos al botón derecho sobre el paquete y elegimos la opción “Set Time Reference”. Esto hará que el tiempo asociado a este paquete se cambie al valor “\*REF\*” y que el resto de tiempos sea calculado en función a este tiempo de referencia:



Por lo tanto, la marca de tiempo del paquete de final de la conexión (de tipo “FIN”) va a coincidir con la duración total de la conexión:



Por lo tanto, el rendimiento global de la conexión es:

(11367 Bytes \* 8 bits/Byte) / 3.54 s = 0.00274Mbps

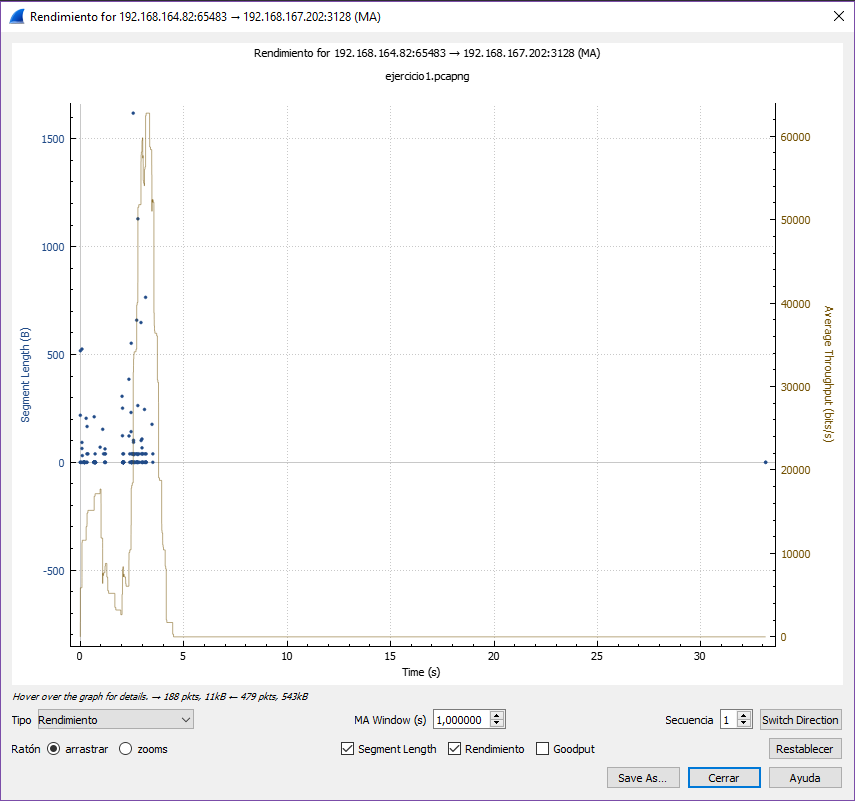
Antes de continuar, desharemos el tiempo de referencia, ya que esto puede interferir con la generación de gráficos más adelante. Simplemente seleccionamos el paquete de referencia, le damos al botón derecho sobre el paquete y elegimos la opción “Set Time Reference” otra vez para dejarlo todo como estaba. Como mencionamos antes, Wireshark produce varios tipos de gráficos para analizar una conexión TCP:

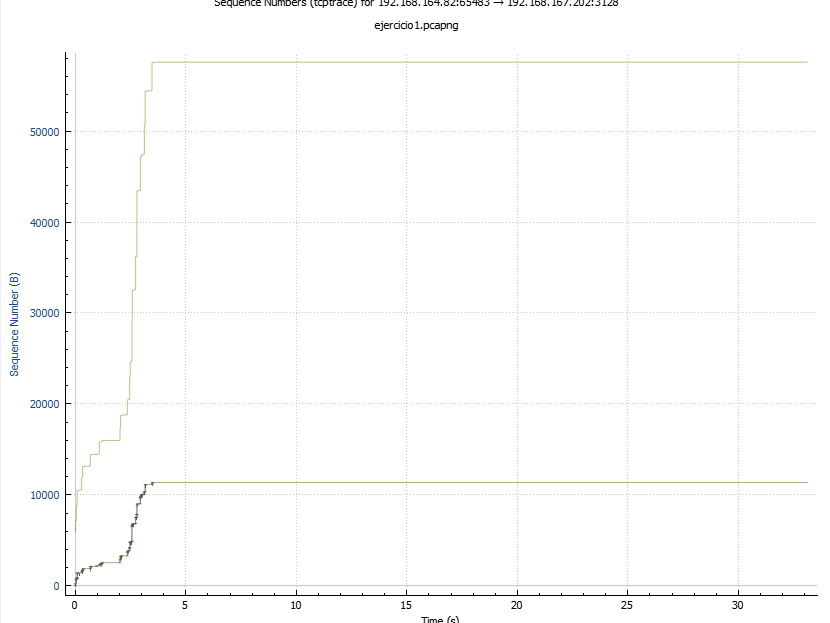
• **Gráfico del tiempo de retorno (“Round-Trip Time”):** Aquí podemos ver el tiempo de retorno para cada paquete. Este tipo de gráfico suele tomar la forma de una nube de puntos.

• **Gráfico de rendimiento (“Throughput”):** Esta gráfica muestra el rendimiento medio (en bits/segundo) a lo largo del tiempo.

• **Gráfico del flujo TCP:** Aquí Wireshark nos ofrece dos tipos de gráficas (“Time/Sequence (Stevens)” y “Time/Sequence (Tcptrace)”) en los que se representa la evolución del número de secuencia a lo largo del tiempo. El segundo tipo es el que ofrece más información.

• **Gráfico del tamaño de ventana (“Window Scaling”):** Muestra cómo varía el tamaño de la ventana a lo largo de la conexión.

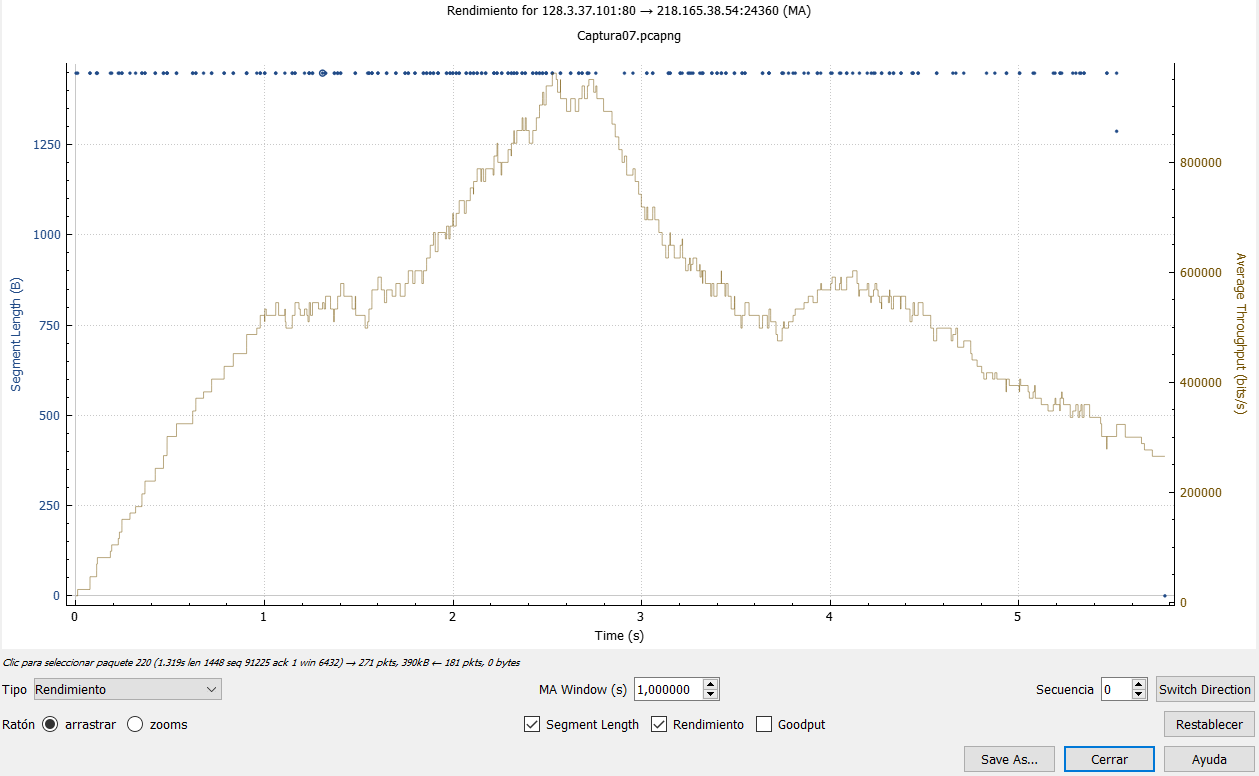




Rendimiento = Pendiente entre Punto 1 y Punto 2 = (Y\_2 – Y\_1)/(X\_2 – X\_1) = = ( 517743– 138402)/(3.12-1.165) = 194036 bytes/segundo = 1552290 bits/segundo = 1,55 Mbps

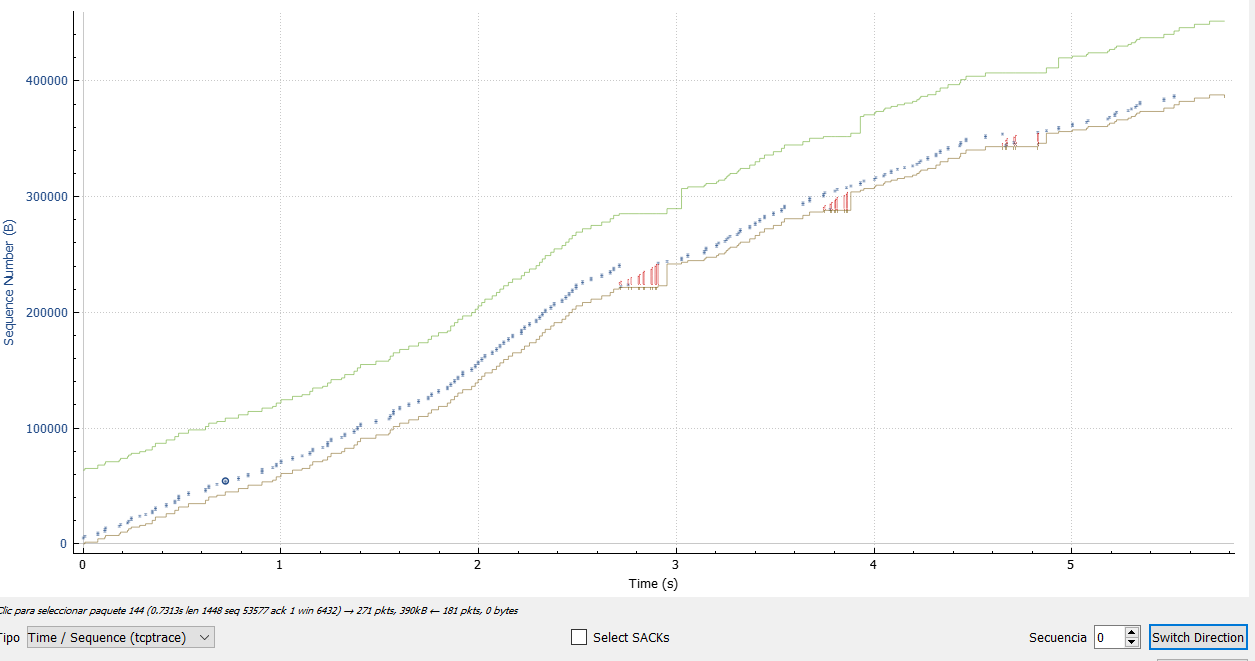
**1.** Usando el fichero “Captura07”, analiza el rendimiento de la conexión que hay entre el nodo 128.3.164.249 (puerto 48805) y el nodo 128.3.38.201 (puerto SMTP). En concreto, se pide:

• Estimar el rendimiento “a ojo” con la gráfica “Thoughput”



**Rendimiento=(157833-70953)/(2-1)= 0,69 Mbps**

• Estimar el rendimiento gráficamente usando la gráfica “Time/Sequence”



**Rendimiento=(157833-70953)/(2-1)=0,69 Mbps**

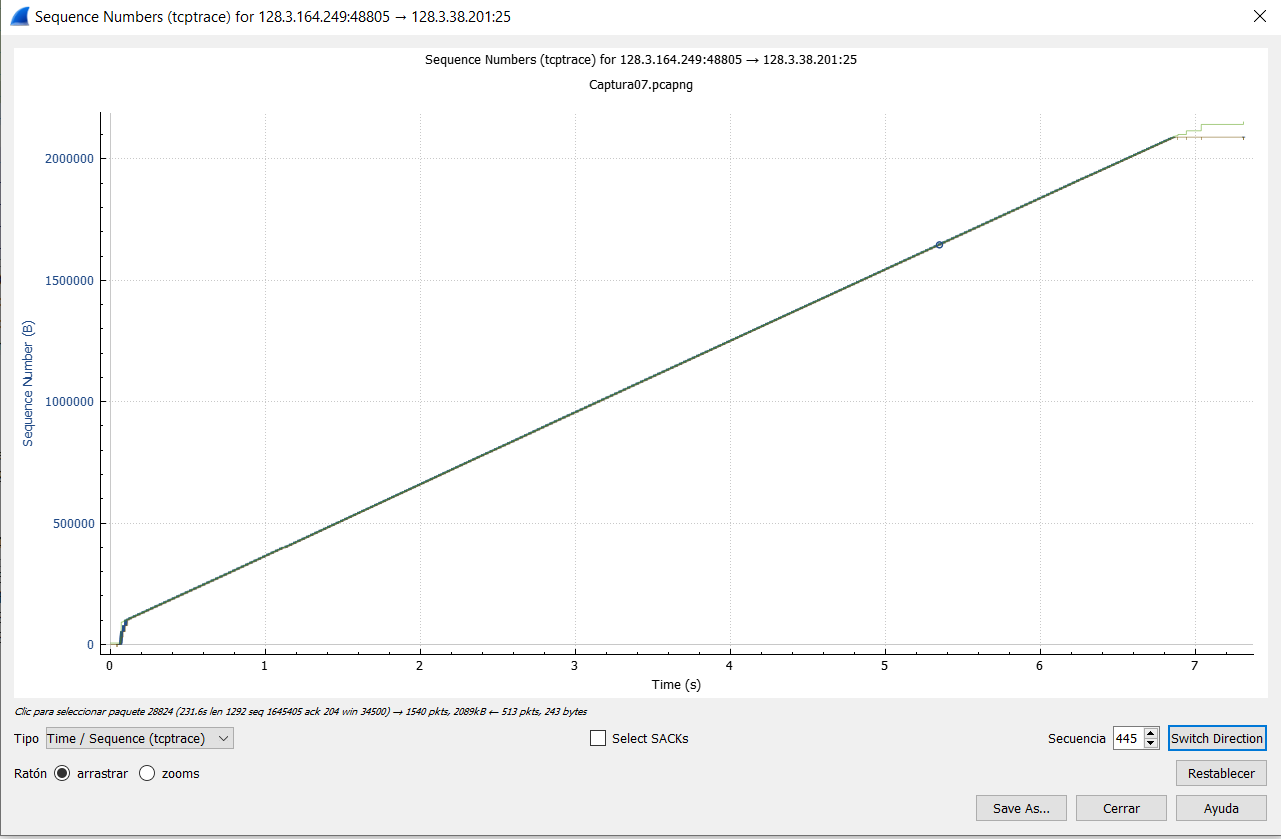
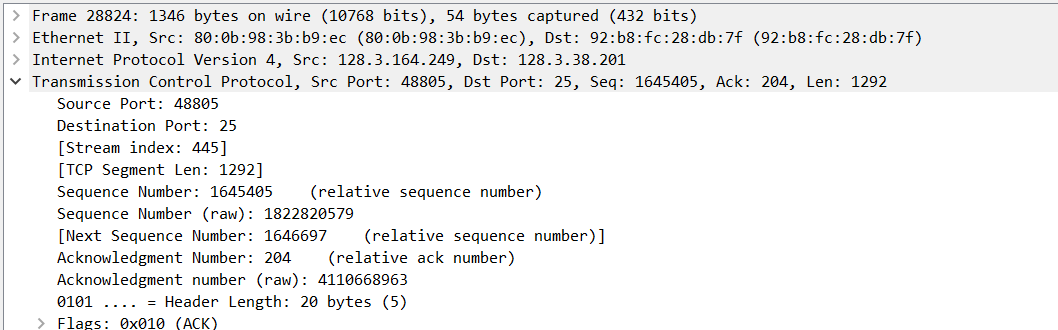
• Calcular el rendimiento de forma exacta

**Rendimiento=(157833-70953)/(2-1)=0,69 Mbps**

Dar todos los resultados en bits por segundo (bps, Kbps, Mbps, etc.), y no en bytes por segundo (Bps, KBps, MBps, etc.)

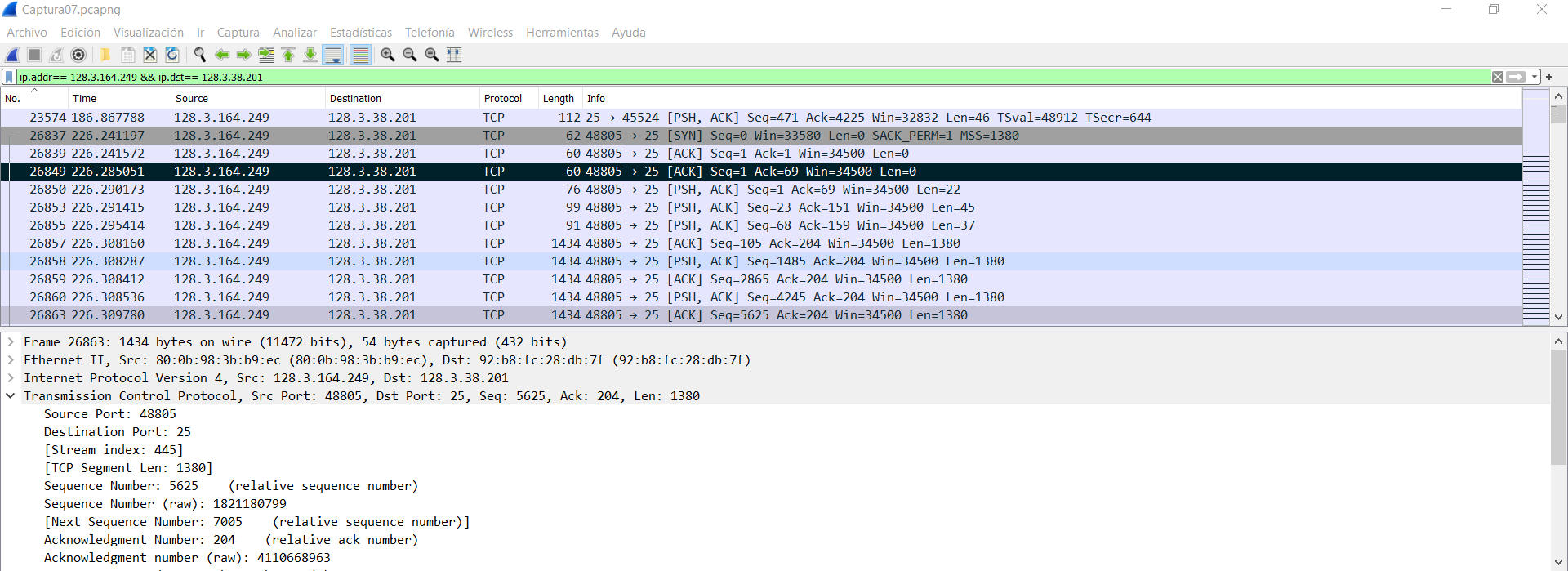
**2.** Selecciona un paquete de datos del flujo TCP y encuentra su correspondiente representación en la gráfica de tipo “**Time/Sequence (tcptrace)**” (tendrás que hacer mucho zoom). ¿Qué número de secuencia tiene este paquete? ¿Qué longitud? Confirma que esta información se corresponde con la gráfica.

El número de secuencia y la longitud se comparten tanto en el paquete como en la gráfica.(Paquete seleccionado: 28824)

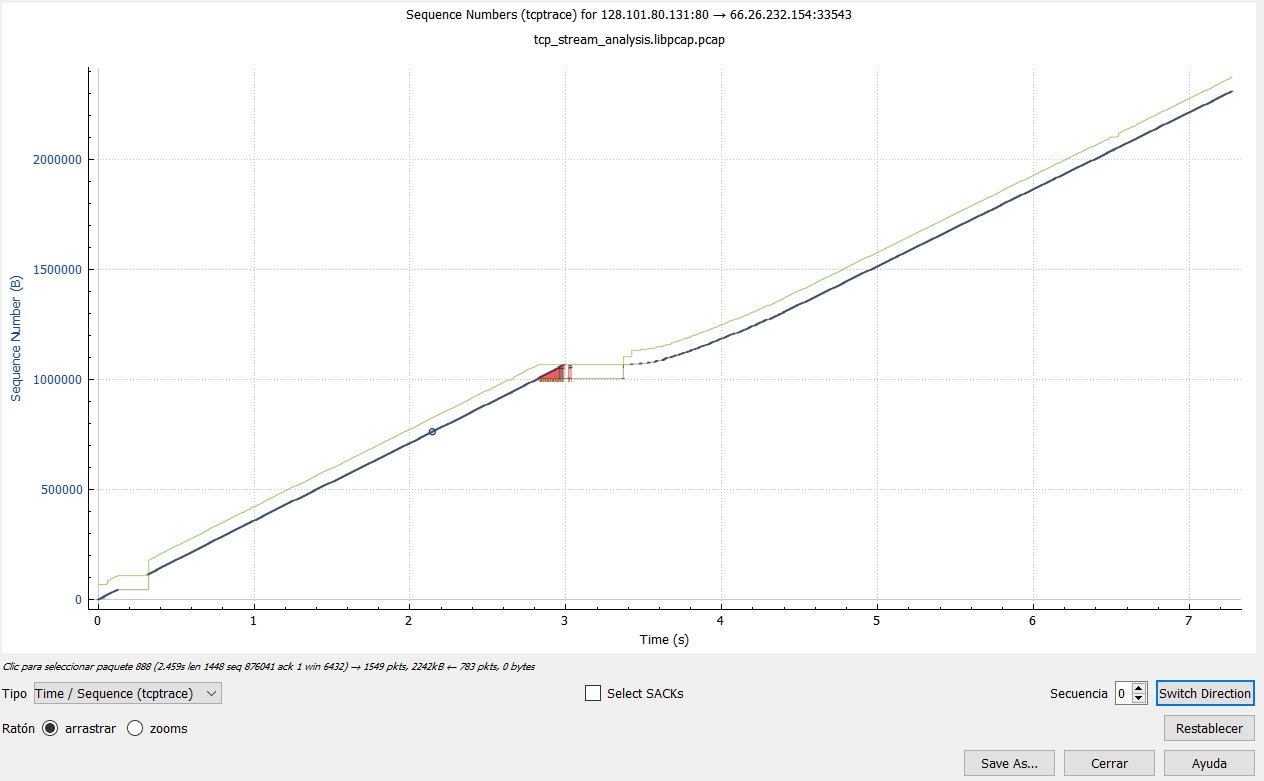


**3.** La velocidad de conexión crecía muy rápido al principio, pero poco después del instante t=0.1 segundos, se mantiene constante. Analiza porqué sucede esto y explícalo.

**Ese intervalo pertenece a los paquetes que tienen desde el 26849 hasta el 26931, en el 26837 se conectan las direcciones ip, 128.3.164.249 y 128.3.38.201. Esa pendiente tan creciente al nivel exponencial, se debe a que hasta entonces se estaban enviados paquetes que no superan los 122 de longitud, sin embargo a partir de esos milésimas de segundos empezaron a enviar paquetes al máximo de longitud en el menor tiempo posible y luego es constante porque se mantiene después de eso.**



**4.** Usaremos ahora el fichero de captura “tcp stream analysis.libpcap.pcap”. Analiza la conexión en la que se envían más datos, en el sentido principal. Podrás ver que en general es una conexión muy estable, pero que sucede algo en la mitad. Analiza qué sucede, y calcula el rendimiento global de la conexión y el rendimiento máximo que consigue de forma mantenida.



**Vemos el mensaje "No se capturó el segmento anterior de TCP" en uno de los paquetes , esto pasa cuando Wireshark observa un paquete que tiene un número de SEC de TCP mayor de lo que esperábamos en este flujo de TCP. En su caso, el paquete se perdió en algún lugar porque observamos Dup ACK y Retransmisión posteriores (el receptor y el remitente reaccionan a la pérdida de paquetes).**

**Para el rendimiento global voy a hacer la media de las dos pendientes mostradas y para la forma mantenida voy a obviar la pérdida de conexión o de paquetes.**

**Rendimiento(Global)= (((712417-363449)+(1514609-118809))/2)\*8=0.109 Mbps**

**Rendimiento(Forma mantenida)=((1514609-363449)/(5-1) )\*8= 2.302 Mbps**

**5.** Ahora compararemos tres conexiones TCP. Hemos descargado el mismo fichero, pero de tres repositorios diferentes, uno en un servidor nacional de Rediris (“rediris.pcapng”), otro de un servidor de la Junta (“andalucía.pcapng”) y otro de Vietnam (“vietnam.pcapng”). Estudia las diferencias e intenta explicarlas. Para el caso de la conexión con Vietnam, vemos que se reciben paquetes en desorden en mitad de la conexión ¿Cómo se representa en la gráfica “**Time/Sequence (tcptrace)**” la llegada de paquetes en desorden?

**El fichero descargado en Rediris no tiene ningún problema de conexión por lo que termina a una velocidad más rápida que las demás. Además la capa de transporte no contiene ningún protocolo de seguridad como puede ser el caso de el fichero descargado de la Junta Andalucía que contiene un protocolo de TLS v1, aunque dentro de su conexión se pueden ver bastantes pérdidas o descuadres de paquetes. La conexión de Vietnam es la que presenta más problemas debido a que es necesario más tiempo de conexión para la descarga del archivo debido a que se ha presentado varios paquetes en desorden debido a que no se encuentran y tienen que ser enviados. Esto se representa mediante puntos rojos dentro de la gráfica.**

