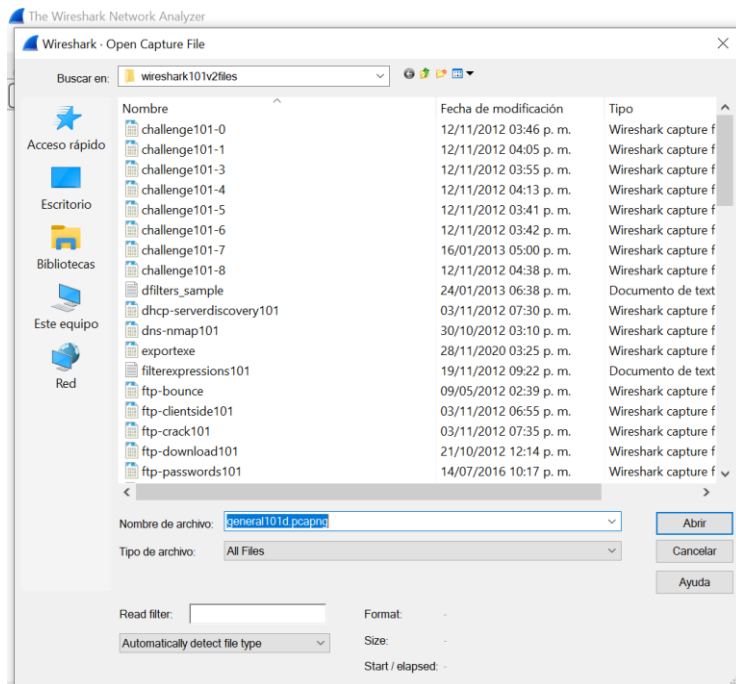
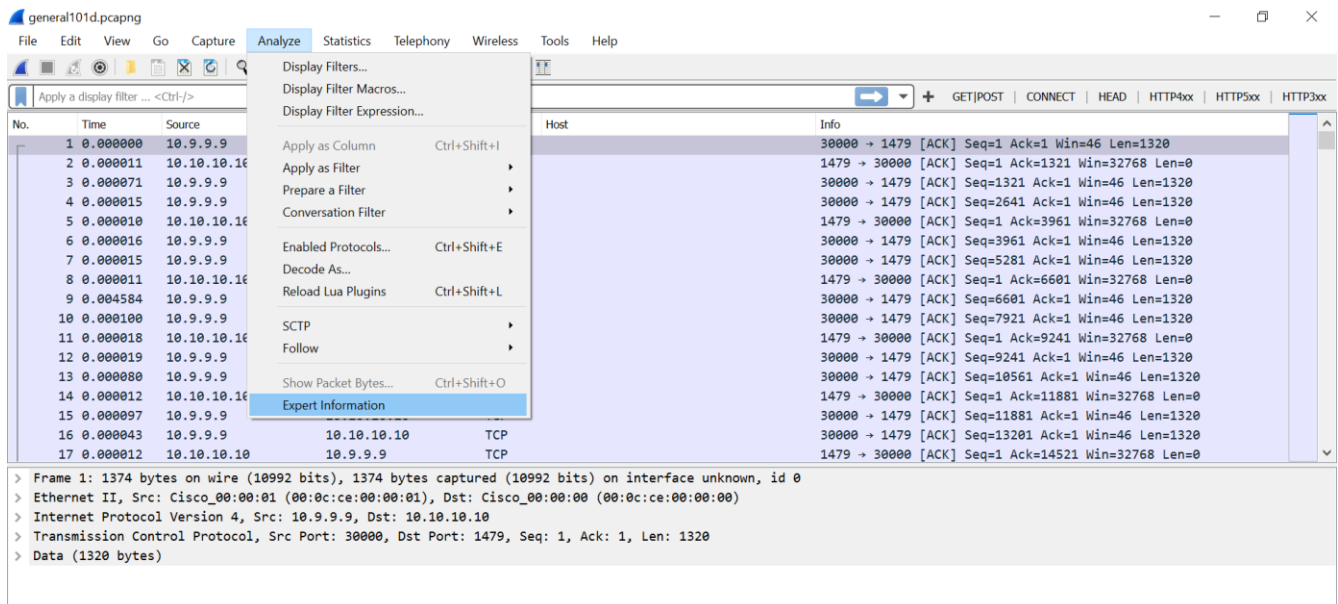


Lab 36

Abriremos el siguiente archivo



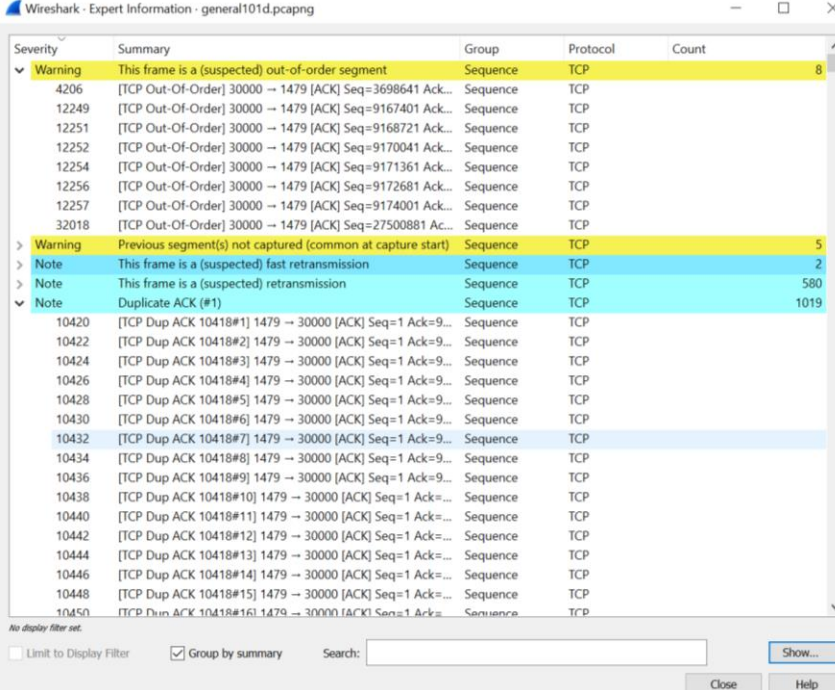
Abrimos en Analyze



Expandir y examinar el warning y Note para identificar los problemas de Wireshark en el archivo de seguimiento, de puede notar lo siguiente:

- Wireshark no indica un numero alto de instancias de segmentos anteriores no capturados
- Wireshark indica que hay muchos ack duplicados
- Wireshark indica que hay buen numero de retransmisiones en el archivo de seguimiento

Todo esto nos indica que hay una perdida significativa de paquetes que ocurre cuando una gran parte de los datos no llega al receptor.



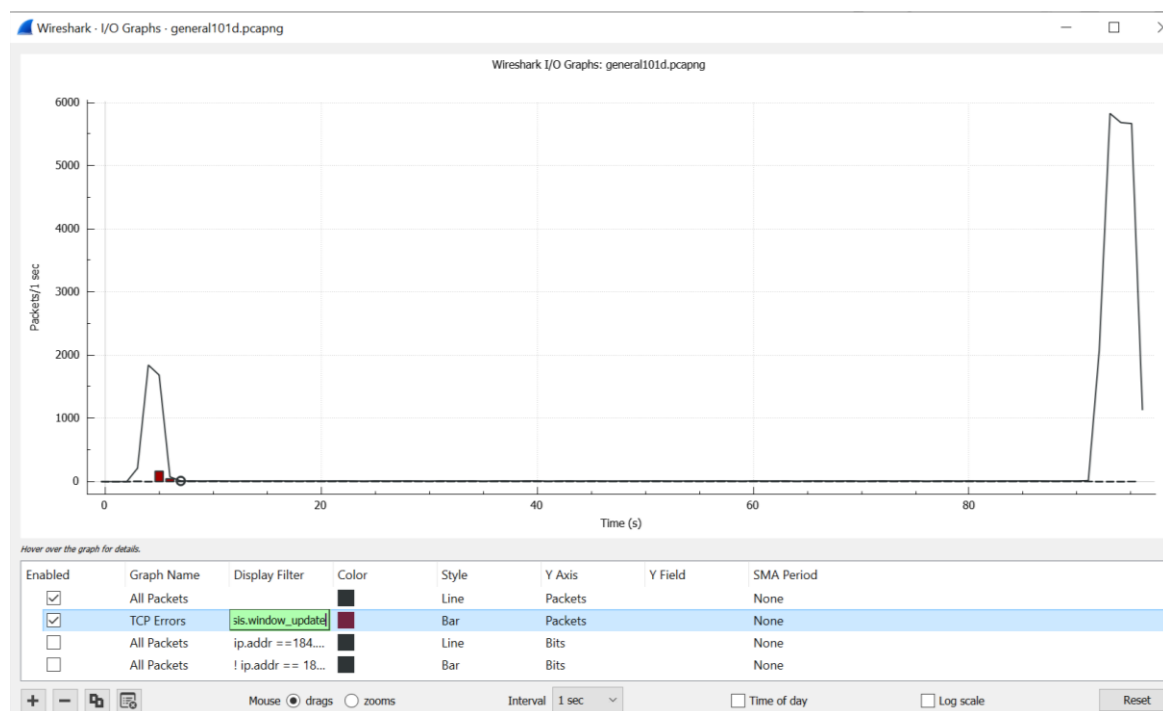
Wireshark - Expert Information - general101d.pcapng

Severity	Summary	Group	Protocol	Count
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	8
	4206 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=3698641 Ack=...	Sequence	TCP	
	12249 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9167401 Ack=...	Sequence	TCP	
	12251 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9168721 Ack=...	Sequence	TCP	
	12252 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9170041 Ack=...	Sequence	TCP	
	12254 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9171361 Ack=...	Sequence	TCP	
	12256 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9172681 Ack=...	Sequence	TCP	
	12257 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=9174001 Ack=...	Sequence	TCP	
	32018 [TCP Out-Of-Order] 30000 → 1479 [ACK] Seq=27500881 Ac...	Sequence	TCP	
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	5
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	2
Note	This frame is a (suspected) retransmission	Sequence	TCP	580
Note	Duplicate ACK (#1)	Sequence	TCP	1019
	10420 [TCP Dup ACK 10418#1] 1479 → 30000 [ACK] Seq=1 Ack=9...	Sequence	TCP	
	10422 [TCP Dup ACK 10418#2] 1479 → 30000 [ACK] Seq=1 Ack=9...	Sequence	TCP	
	10424 [TCP Dup ACK 10418#3] 1479 → 30000 [ACK] Seq=1 Ack=9...	Sequence	TCP	
	10426 [TCP Dup ACK 10418#4] 1479 → 30000 [ACK] Seq=1 Ack=9...	Sequence	TCP	
	10428 [TCP Dup ACK 10418#5] 1479 → 30000 [ACK] Seq=1 Ack=9...	Sequence	TCP	
	10430 [TCP Dup ACK 10418#6] 1479 → 30000 [ACK] Seq=1 Ack=9...	Sequence	TCP	
	10432 [TCP Dup ACK 10418#7] 1479 → 30000 [ACK] Seq=1 Ack=9...	Sequence	TCP	
	10434 [TCP Dup ACK 10418#8] 1479 → 30000 [ACK] Seq=1 Ack=9...	Sequence	TCP	
	10436 [TCP Dup ACK 10418#9] 1479 → 30000 [ACK] Seq=1 Ack=9...	Sequence	TCP	
	10438 [TCP Dup ACK 10418#10] 1479 → 30000 [ACK] Seq=1 Ack=...	Sequence	TCP	
	10440 [TCP Dup ACK 10418#11] 1479 → 30000 [ACK] Seq=1 Ack=...	Sequence	TCP	
	10442 [TCP Dup ACK 10418#12] 1479 → 30000 [ACK] Seq=1 Ack=...	Sequence	TCP	
	10444 [TCP Dup ACK 10418#13] 1479 → 30000 [ACK] Seq=1 Ack=...	Sequence	TCP	
	10446 [TCP Dup ACK 10418#14] 1479 → 30000 [ACK] Seq=1 Ack=...	Sequence	TCP	
	10448 [TCP Dup ACK 10418#15] 1479 → 30000 [ACK] Seq=1 Ack=...	Sequence	TCP	
	10450 [TCP Dup ACK 10418#16] 1479 → 30000 [ACK] Seq=1 Ack=...	Sequence	TCP	

No display filter set.

☐ Limit to Display Filter ☒ Group by summary Search: Show... Close Help

Agregaremos lo siguiente en tcp.analysis.flags && !tcp.analysis.window_update en TCP ERRORS de I/O Graphs



Marcaremos la casilla de Log scale y se pueden ver que los errores TCP aumentaron antes de la caída de rendimiento. Si hace clic en cualquier punto del gráfico, el programa saltará a ese punto en el archivo original lo que le permitirá examinar mas a fondo

