Troubleshooting Retransmits

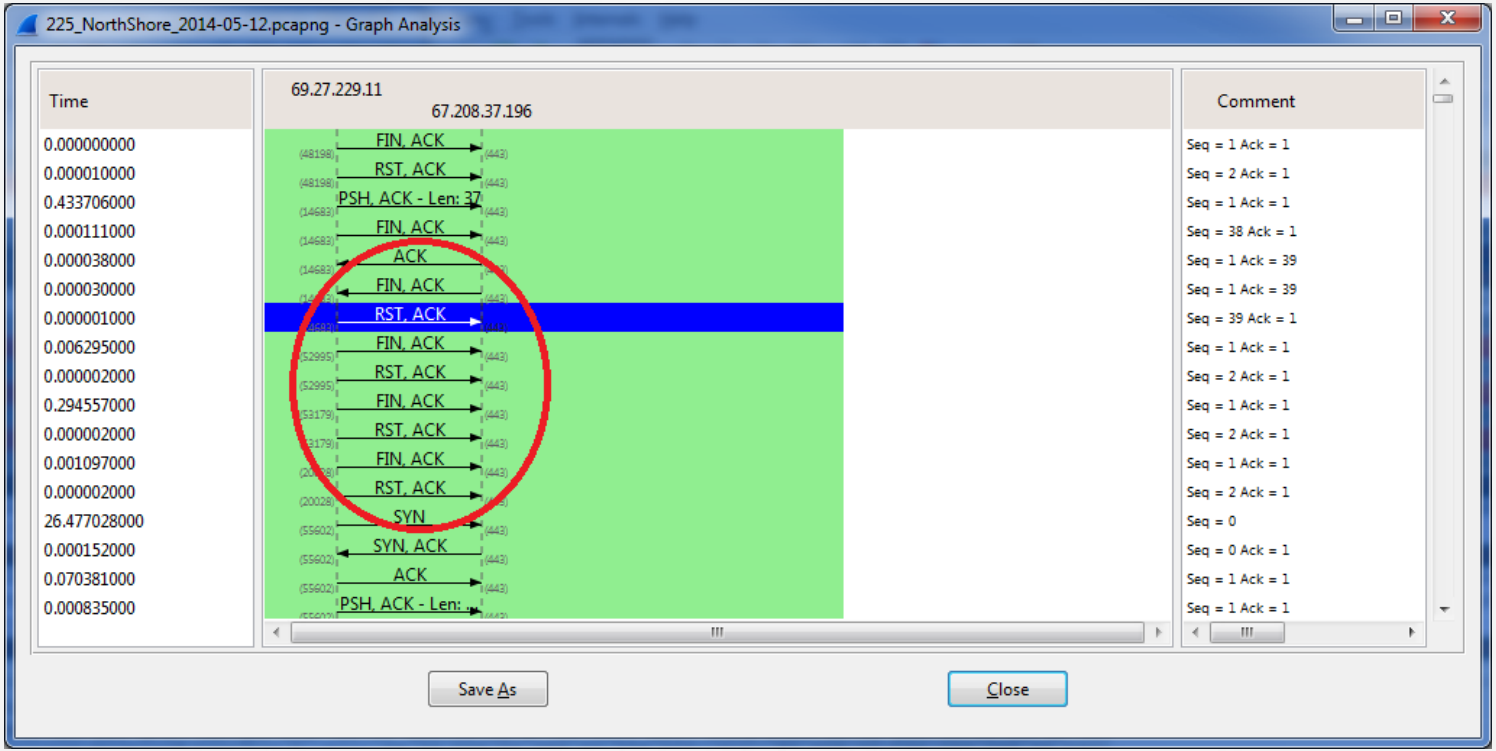
Troubleshooting Retransmits

- What is a retransmit?
- Looking for patterns
  - Duplicate ACKs
  - Expert output
  - Flow Graph output
- Possible port scan?
  - When using a tool like nmap, you can see these patterns

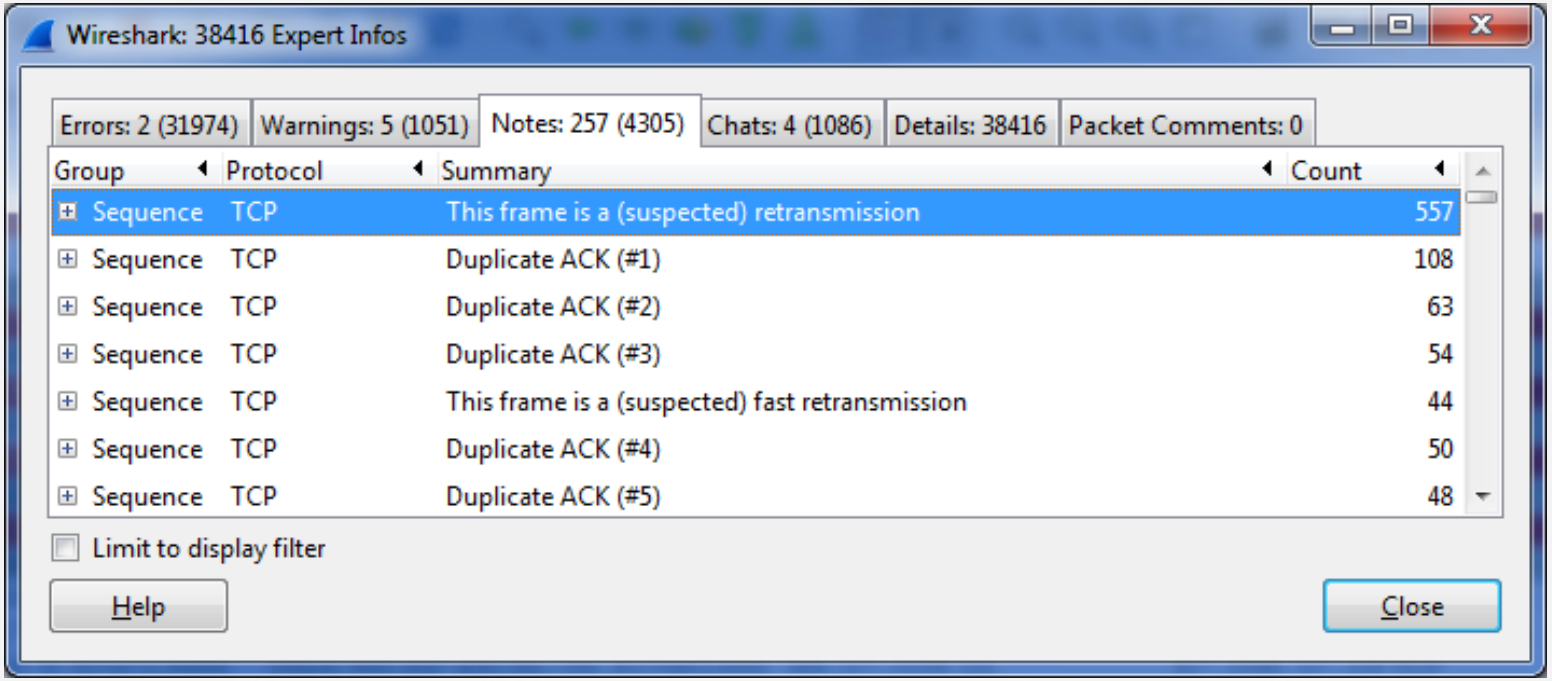
Troubleshooting Retransmits

Info	Length
48198→443 [FIN, ACK] Seq=1 Ack=1 Win=461 Len=0 TSval=1397824194 TSecr=	
48198→443 [RST, ACK] Seq=2 Ack=1 Win=461 Len=0 TSval=1397824194 TSecr=	
Encrypted Alert	
14683→443 [FIN, ACK] Seq=38 Ack=1 Win=513 Len=0 TSval=1397824306 TSecr	
14683→443 [RST, ACK] Seq=39 Ack=1 Win=513 Len=0 TSval=1397824306 TSecr	
52995→443 [FIN, ACK] Seq=1 Ack=1 Win=140 Len=0 TSval=1397824308 TSecr=	
52995→443 [RST, ACK] Seq=2 Ack=1 Win=140 Len=0 TSval=1397824308 TSecr=	
53179→443 [FIN, ACK] Seq=1 Ack=1 Win=204 Len=0 TSval=1397824378 TSecr=	
53179→443 [RST, ACK] Seq=2 Ack=1 Win=204 Len=0 TSval=1397824378 TSecr=	
20028→443 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1397824378 TSecr=	
20028→443 [RST, ACK] Seq=2 Ack=1 Win=501 Len=0 TSval=1397824378 TSecr=	
55602→443 [SYN] Seq=0 Win=5840 Len=0 MSS=1380 SACK_PERM=1 TSval=139783	

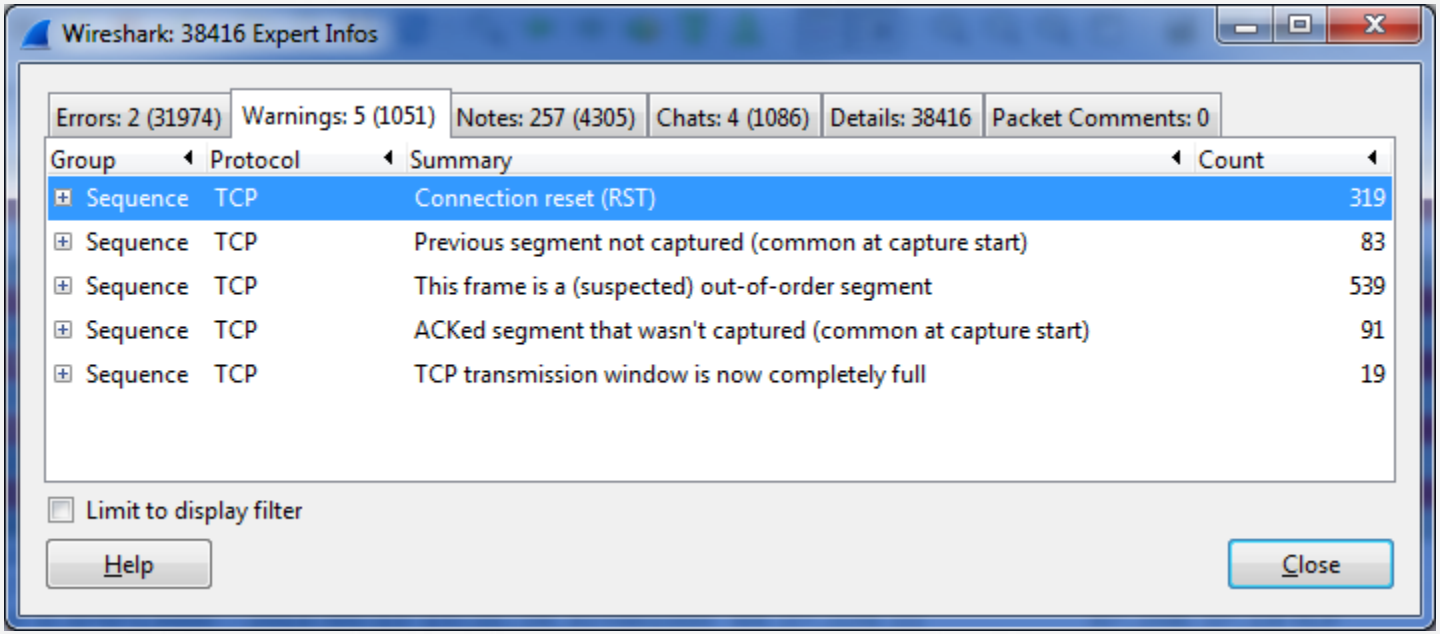
Troubleshooting Retransmits



Troubleshooting Retransmits



Troubleshooting Retransmits



Questions?