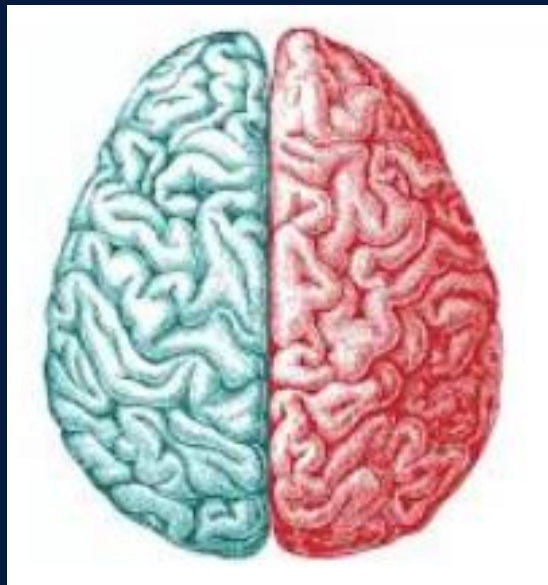




# SharkFest '18 Europe



## TCP Split Brain



Using Wireshark to  
Compare & Contrast  
behavior and TCP state of  
client vs. server

John Pittle

Riverbed Technologies  
Performance Management  
Strategist



# Premise: TCP Split Brain



- When troubleshooting TCP, you often have to consider both the sender's unique perspective and the receiver's unique perspective
- Both endpoints are independent, but at the same time, they do react to packets from the other end
- The joint behavior gets even more interesting when there's "high" latency in the path



# Session Goals



- Compare and contrast TCP end point behavior
- Drill down into the “what is it doing?” and “why is it doing that?”
- Promote Wireshark Profiles Feature
- Share experience and ideas
- Expose you to visualizations that help reinforce the end point behavior we will be discussing



# Session Resources



- Wireshark 2.6.3
- End point capture files for the TCP connection of interest
- Wireshark Profiles
- Riverbed Transaction Analyzer for Visualization



# About me?



- Performance Engineering since 1980
- Protocol Analysis since 1991
- Professional Services with OPNET / Riverbed since 2005
- Love the mystery of a complicated performance issue
- Shaved off beard in 2003...

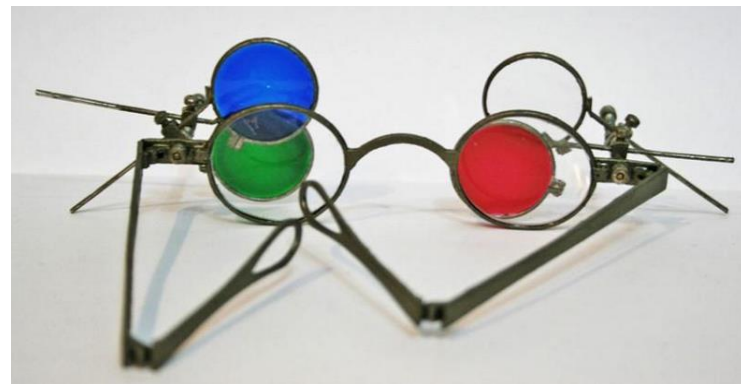




# My Ask of You



- Engage
- Participate
- We have a lot of detailed material
- We will explore conflicting, contradictory, and possibly confusing details
- Ask Questions
- Question Answers





#sf18eu • Imperial Riding School Renaissance Vienna • Oct 29 - Nov 2





# Application Scenario



- HTTPS Web Application
- Private key is not available
- Host based captures on web server and my laptop





# Symptoms to Analyze



- Downloading files take \*forever\*
- 16 seconds to download a 1.4MB file
- One TCP connection has been isolated as the connection of interest – TCP/52942-443



# Very Simple Topology



Web Server  
San Francisco, CA

Home Office  
Orlando, FL



443

10.16.1.251

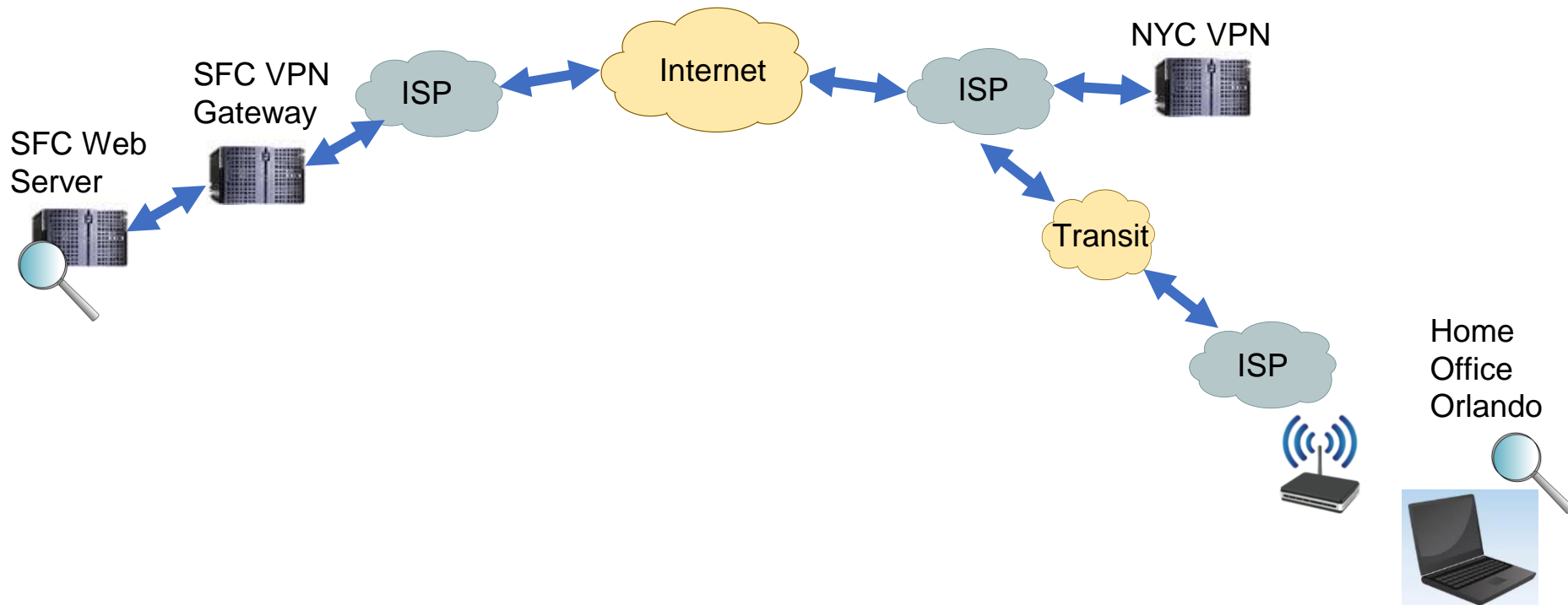
52942



10.36.9.27



# Actual Topology





# Pop Quiz #1



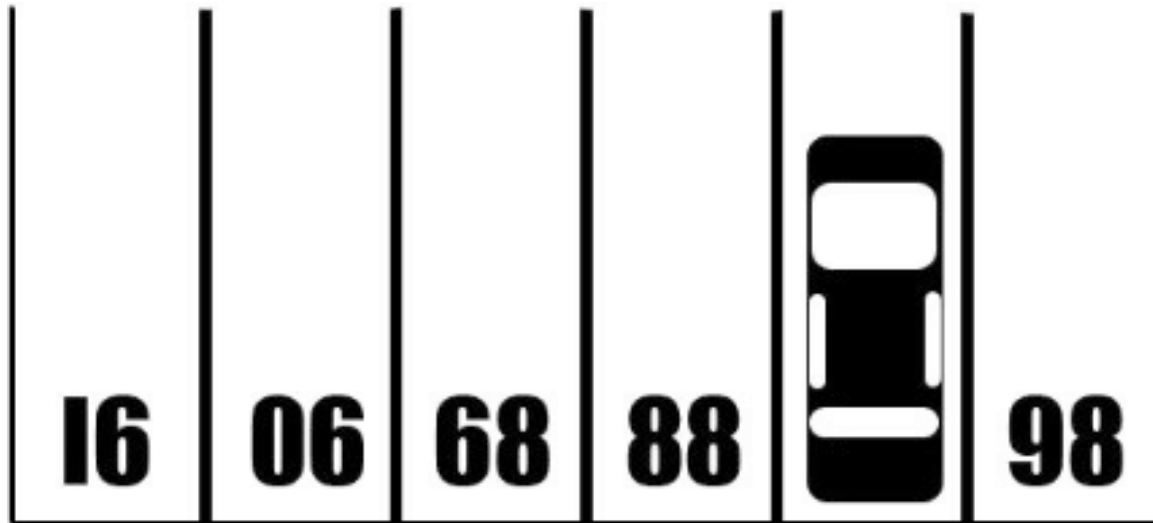
- Ready for our first Quiz?



# Pop Quiz #1



What parking slot # is the car in?  
Can you do the math?

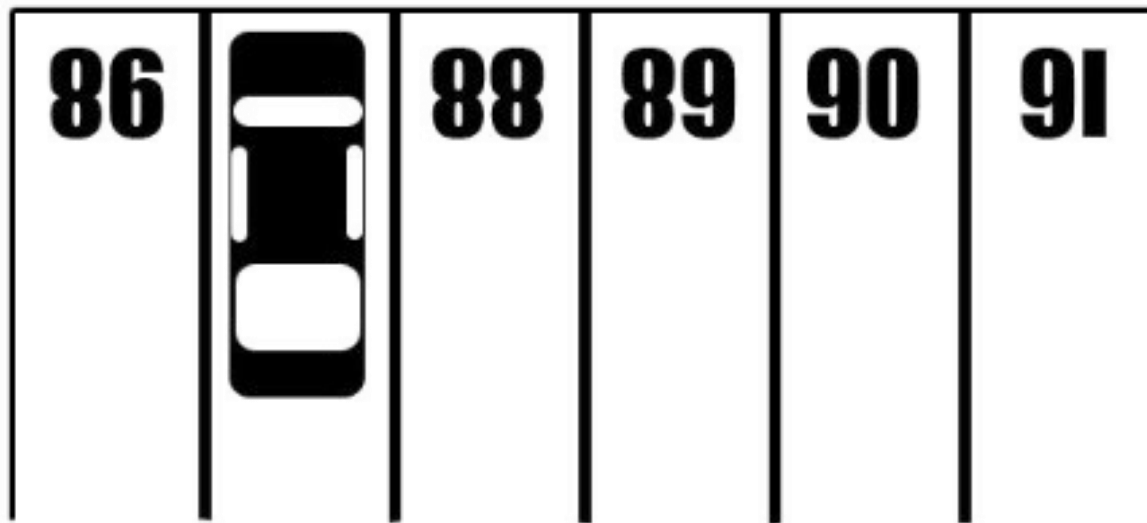




# Perspective



How about now?





# TCP End Point Behavior



- Each end point has a unique perspective
- Independent, yet influenced by the other
- Often during the traffic exchange, TCP stack decisions and actions can be occurring asynchronously on each host
- 3<sup>rd</sup> party actors can also have an affect on behavior

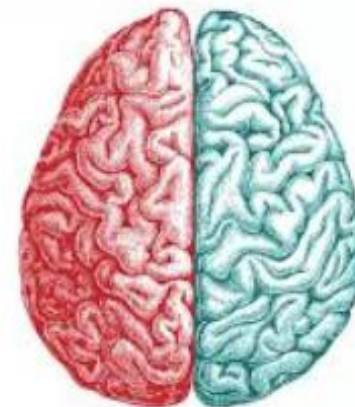




# Comparisons



- 3-way handshake
- Latency
- Expert Info
- Fragment Overlaps / OOS / Packet Loss
- Bytes in Flight
- Congestion





# Split Brain Comparisons



- We'll start with the 3-way handshake signaling





# 3-Way Handshake - Client



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
1	0.000000	0.000000000	10.36.9.27	10.16.1.251	0	0	0	0		52942 → 443 [SYN]
2	0.121491	0.121491000	10.16.1.251	10.36.9.27	0	0	0	1		443 → 52942 [SYN]
3	0.121578	0.000087000	10.36.9.27	10.16.1.251	0	1	1	1		52942 → 443 [ACK]
4	0.124883	0.003305000	10.36.9.27	10.16.1.251	517	1	518	1	517	Client Hello

Acknowledgment number: 0  
1000 .... = Header Length: 32 bytes (8)

- Flags: 0x002 (SYN)
- Window size value: 8192  
[Calculated window size: 8192]
- Checksum: 0xac33 [unverified]  
[Checksum Status: Unverified]
- Urgent pointer: 0
- Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  - TCP Option - Maximum segment size: 1360 bytes
  - TCP Option - No-Operation (NOP)
  - TCP Option - Window scale: 8 (multiply by 256)
  - TCP Option - No-Operation (NOP)
  - TCP Option - No-Operation (NOP)
  - TCP Option - SACK permitted
- [Timestamps]



# 3-Way Handshake - Server



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression.

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
1	0.000000	0.000000000	10.36.9.27	10.16.1.251	0	0	0	0		S+, 52942 → 443 [
2	0.000054	0.000054000	10.16.1.251	10.36.9.27	0	0	0	1		443 → 52942 [SYN,
3	0.129252	0.129198000	10.36.9.27	10.16.1.251	0	1	1	1		52942 → 443 [ACK]

Acknowledgment number: 1 (relative ack number)  
1000 .... = Header Length: 32 bytes (8)

▷ Flags: 0x012 (SYN, ACK)

Window size value: 8192  
[Calculated window size: 8192]  
Checksum: 0x1f70 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0

Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permiss

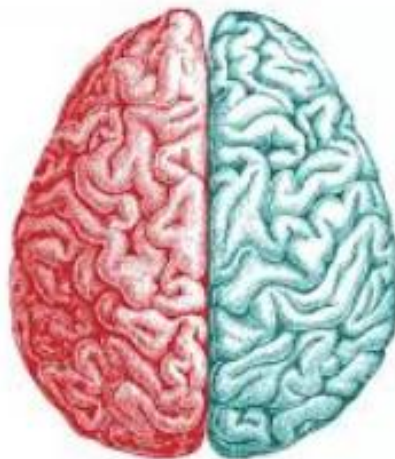
- ▷ TCP Option - Maximum segment size: 1460 bytes
- ▷ TCP Option - No-Operation (NOP)
- ▷ TCP Option - Window scale: 8 (multiply by 256)
- ▷ TCP Option - No-Operation (NOP)
- ▷ TCP Option - No-Operation (NOP)
- ▷ TCP Option - SACK permitted



# Split Brain Comparisons



- Latency Checks

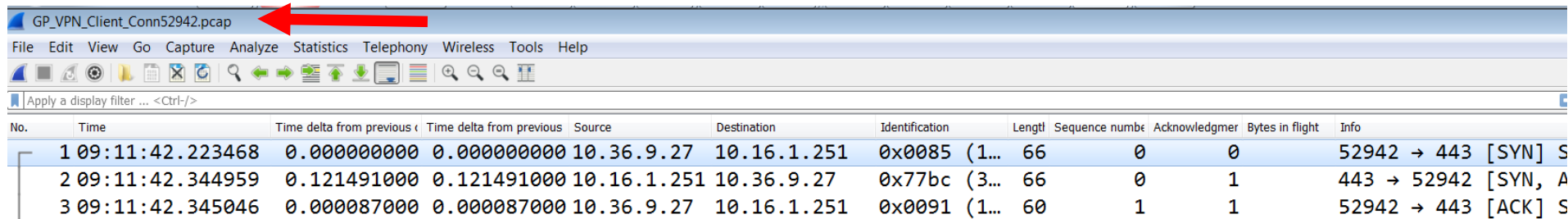




# Latency Check

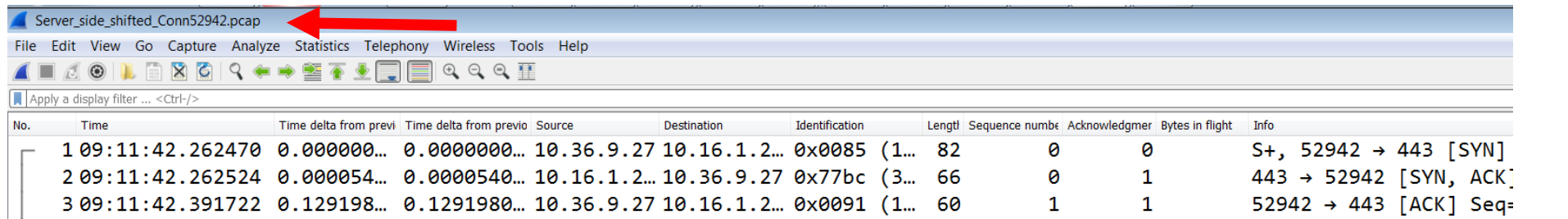


- Client Capture – 121ms



No.	Time	Time delta from previous capture point	Time delta from previous interface capture point	Source	Destination	Identification	Length	Sequence number	Acknowledgment number	Bytes in flight	Info
1	09:11:42.223468	0.000000000	0.000000000	10.36.9.27	10.16.1.251	0x0085 (1...	66	0	0	0	52942 → 443 [SYN] Seq=
2	09:11:42.344959	0.121491000	0.121491000	10.16.1.251	10.36.9.27	0x77bc (3...	66	0	1	1	443 → 52942 [SYN, ACK] Seq=
3	09:11:42.345046	0.000087000	0.000087000	10.36.9.27	10.16.1.251	0x0091 (1...	60	1	1	1	52942 → 443 [ACK] Seq=

- Server Capture – 129ms



No.	Time	Time delta from previous capture point	Time delta from previous interface capture point	Source	Destination	Identification	Length	Sequence number	Acknowledgment number	Bytes in flight	Info
1	09:11:42.262470	0.000000...	0.000000...	10.36.9.27	10.16.1.2...	0x0085 (1...	82	0	0	0	S+, 52942 → 443 [SYN]
2	09:11:42.262524	0.000054...	0.0000540...	10.16.1.2...	10.36.9.27	0x77bc (3...	66	0	1	1	443 → 52942 [SYN, ACK] Seq=
3	09:11:42.391722	0.129198...	0.1291980...	10.36.9.27	10.16.1.2...	0x0091 (1...	60	1	1	1	52942 → 443 [ACK] Seq=



# Wireshark i(nitial)RTT



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack
1	0.000000	0.000000000	10.36.9.27	10.16.1.251	0	0	0	0
2	0.121491	0.121491000	10.16.1.251	10.36.9.27	0	0	0	1
3	0.121578	0.000087000	10.36.9.27	10.16.1.251	0	1	1	1
4	0.124883	0.003305000	10.36.9.27	10.16.1.251	517	1	518	1

[Next sequence number: 1 (relative sequence number)]  
Acknowledgment number: 1 (relative ack number)  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x010 (ACK)  
Window size value: 257  
[Calculated window size: 65792]  
[Window size scaling factor: 256]  
Checksum: 0x6ba1 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
[SEQ/ACK analysis]  
[This is an ACK to the segment in frame: 2]  
[The RTT to ACK the segment was: 0.000087000 seconds]  
[iRTT: 0.121578000 seconds]  
[Timestamps]

GP\_VPN\_Client\_Conn52942.pcap | Packets: 2818 · Displayed: 2818 (100.0%) | Profile: SB-SACK





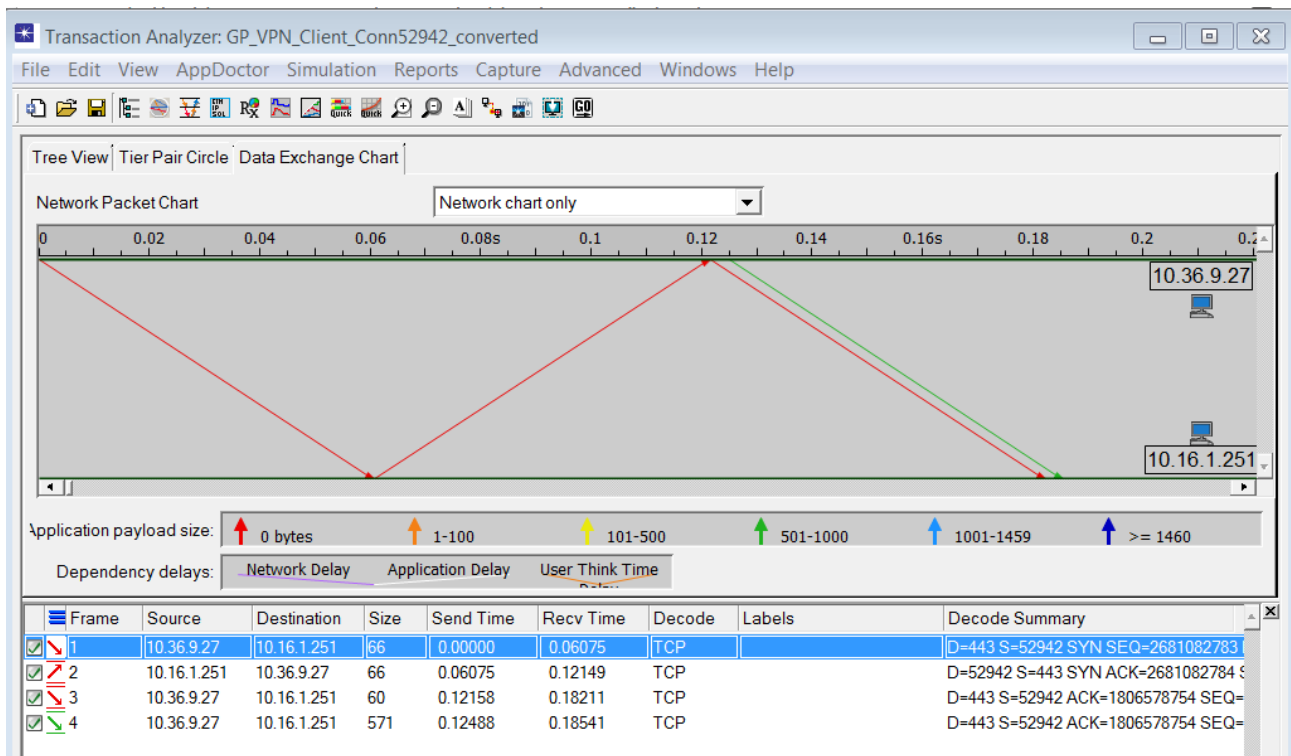
# What if we could visualize the traffic exchanges?



- Traffic bouncing between hosts
- Frequency, density, duration over time
- Expert analytics overlaid with the visualized traffic
- If only there were such a capability...

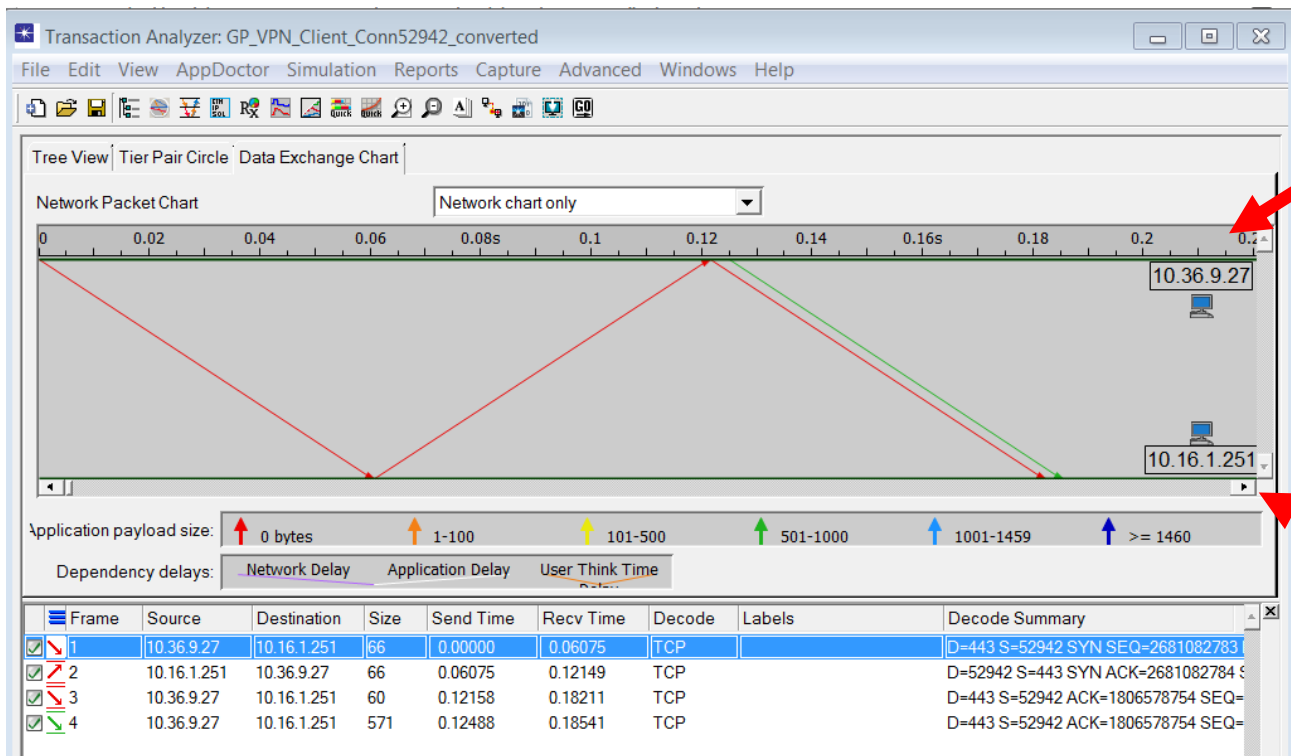


# Visualize Traffic over Time





# Top and Bottom of Swimlane

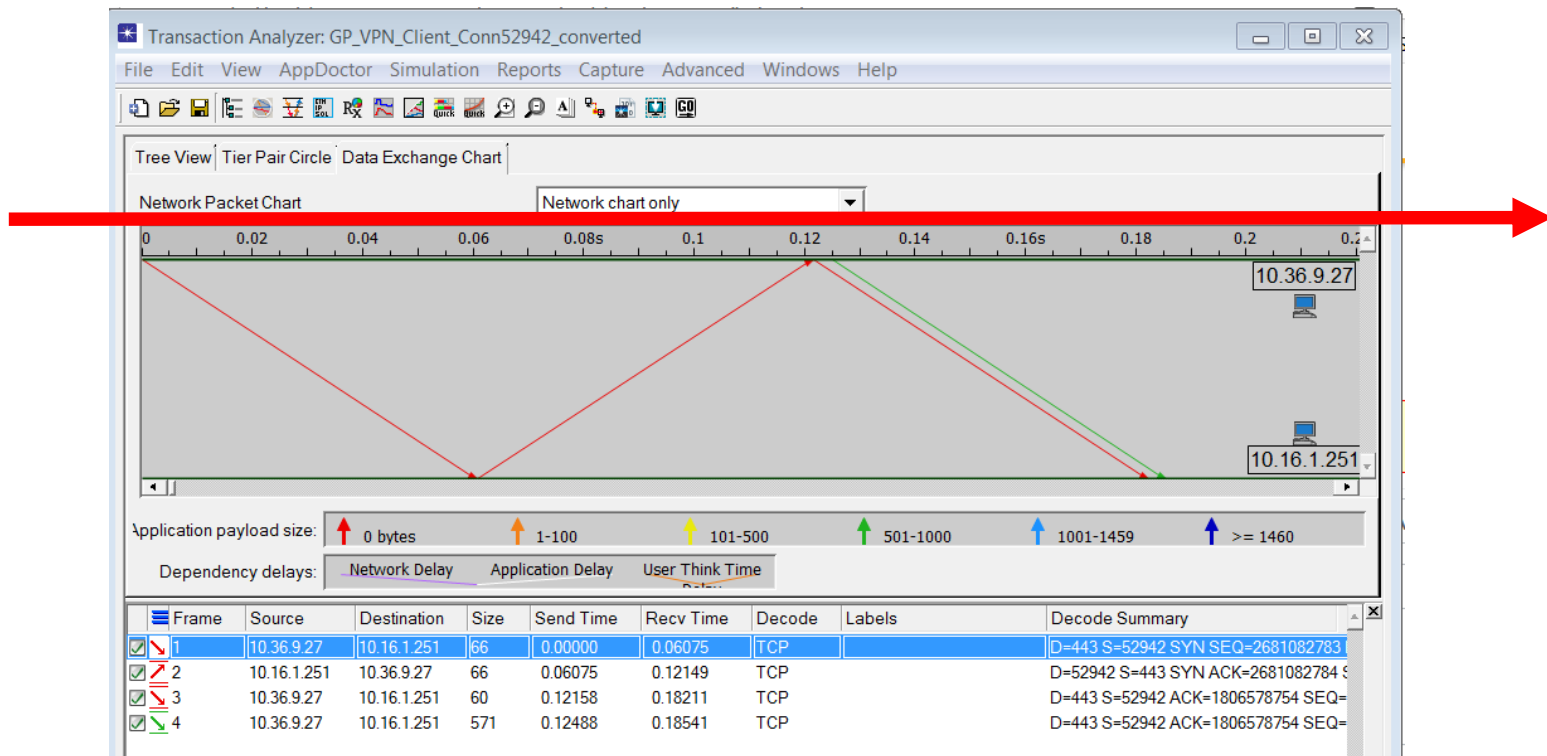


Client

Server

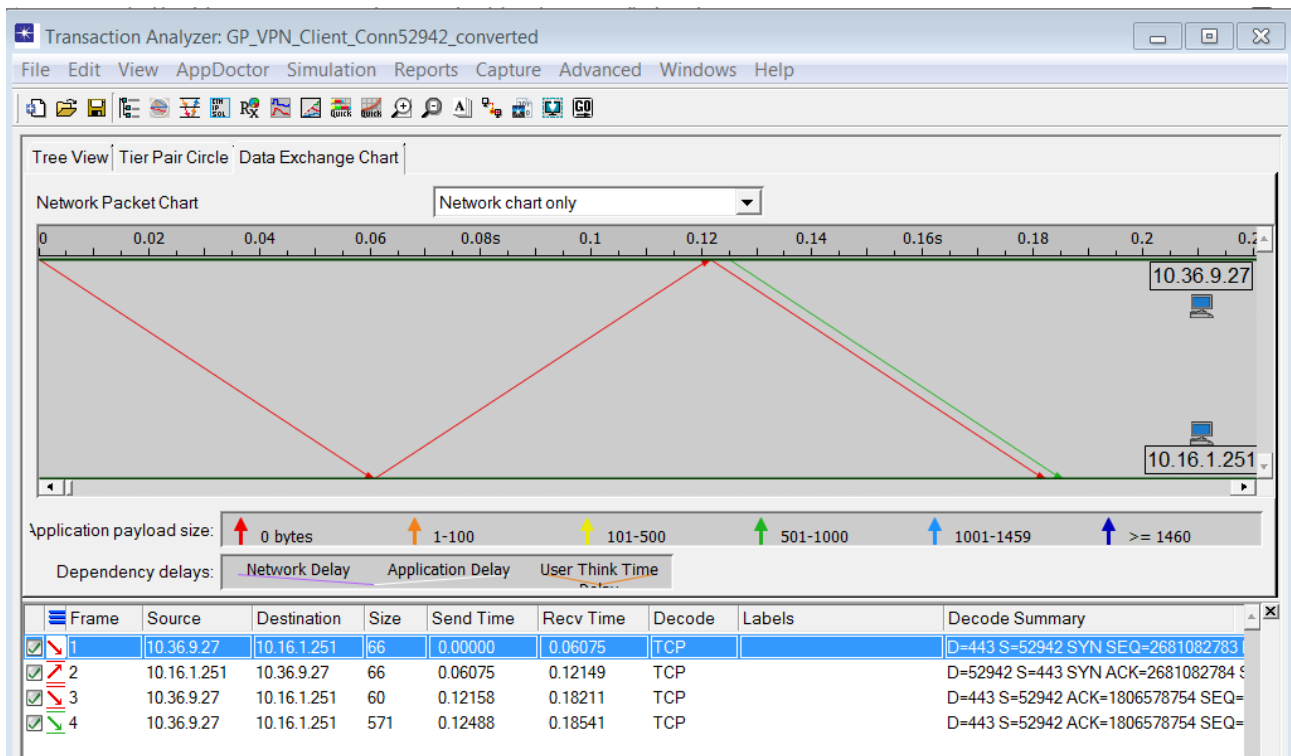


# Time Moves Left to Right



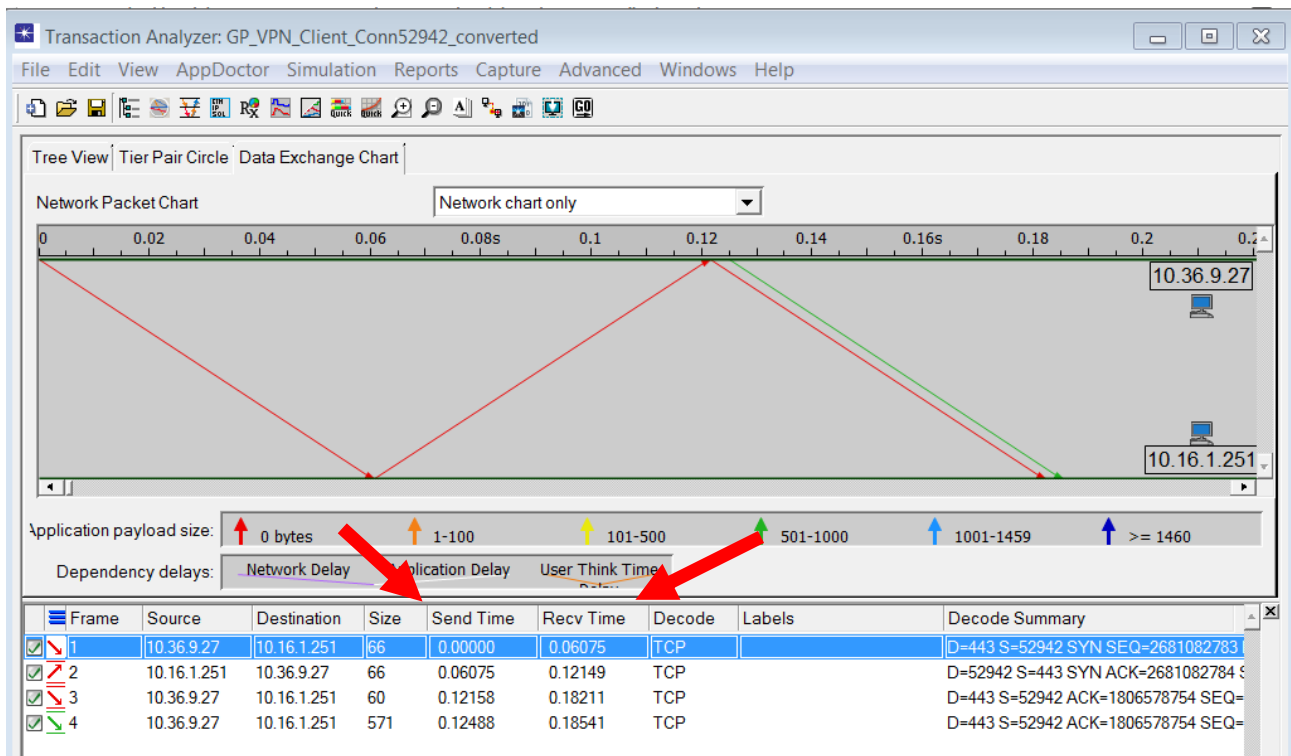


# Optional Summary Decodes





# Send Time / Recv Time





# Estimated vs. Actual Times



- Each capture has the actual times a packet is sent or received from / to that host
- Using what we do know, we can estimate what we don't know





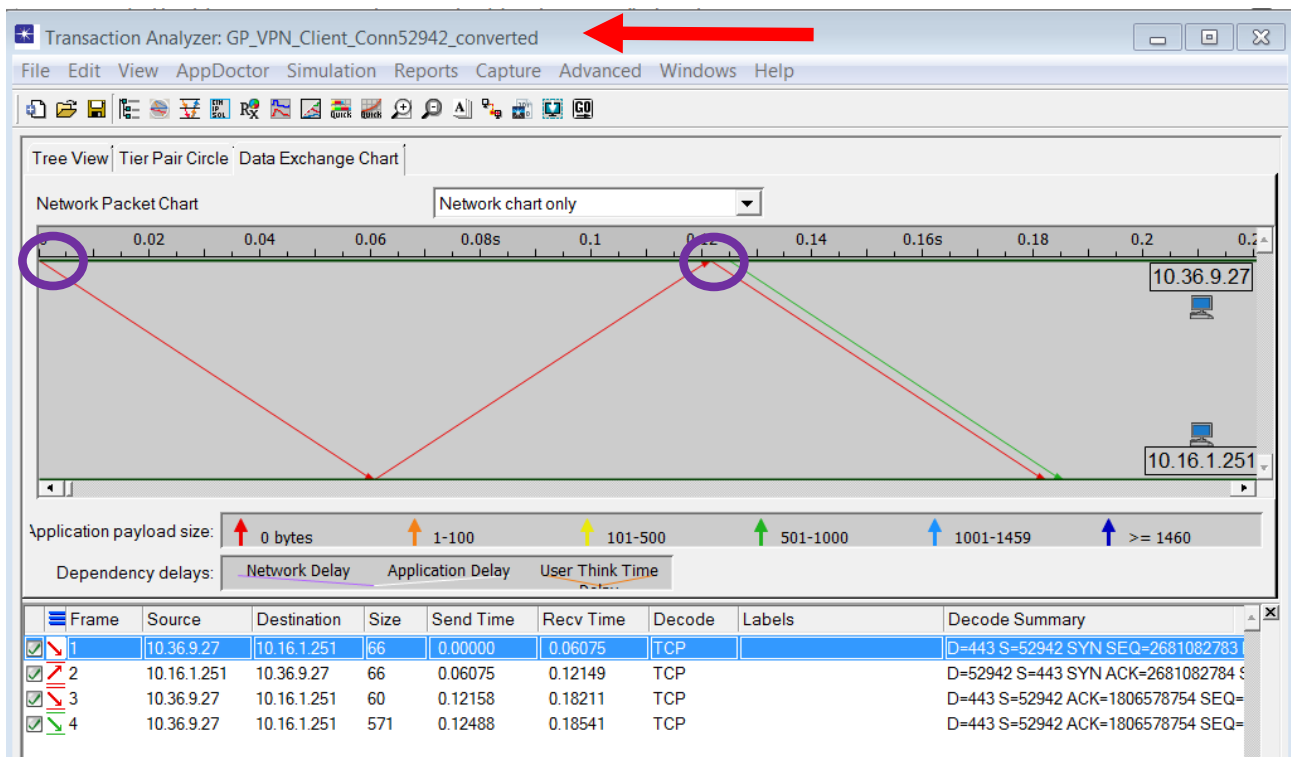
# Estimated vs. Actual Times



- If we know when we received a packet, we can make a reasonable estimate about the time it was transmitted
- If we know when a packet was transmitted, we can make a reasonable estimate about the time it was received

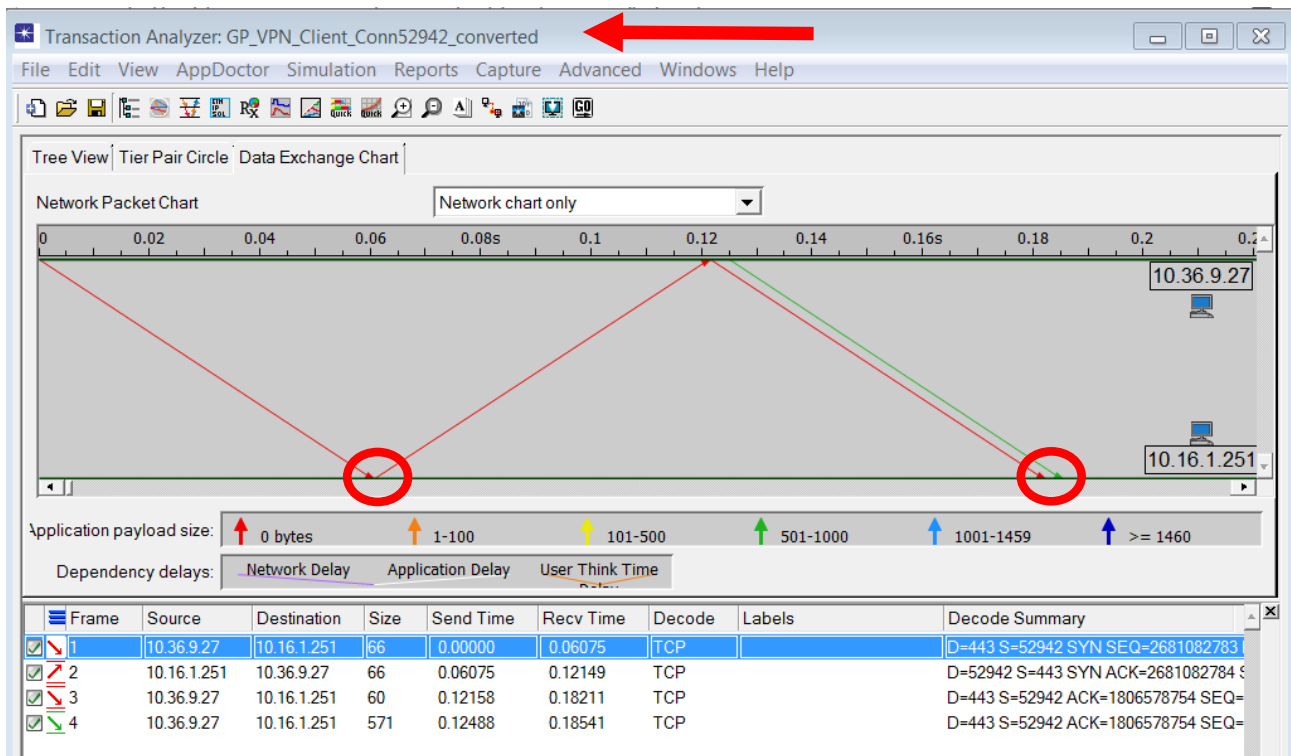


# Here's what we know





# Here's what we can estimate





# Affairs of State



- Now let's look at how we can use the visualization to understand the TCP state of each end point at a given point in time



# RFC 793: TCP State Overview



TCP A		TCP B
1. CLOSED		LISTEN
2. SYN-SENT	--> <SEQ=100><CTL=SYN>	--> SYN-RECEIVED
3. ESTABLISHED	<-- <SEQ=300><ACK=101><CTL=SYN,ACK>	<-- SYN-RECEIVED
4. ESTABLISHED	--> <SEQ=101><ACK=301><CTL=ACK>	--> ESTABLISHED
5. ESTABLISHED	--> <SEQ=101><ACK=301><CTL=ACK><DATA>	--> ESTABLISHED

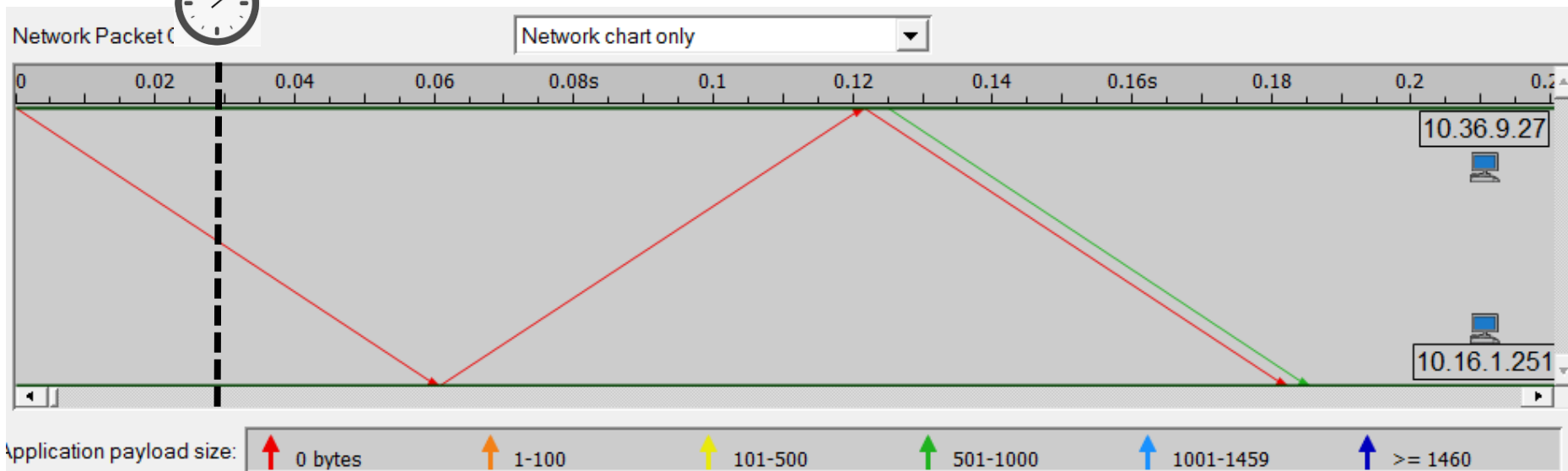
Basic 3-Way Handshake for Connection Synchronization



# Split Brain – State Discussion

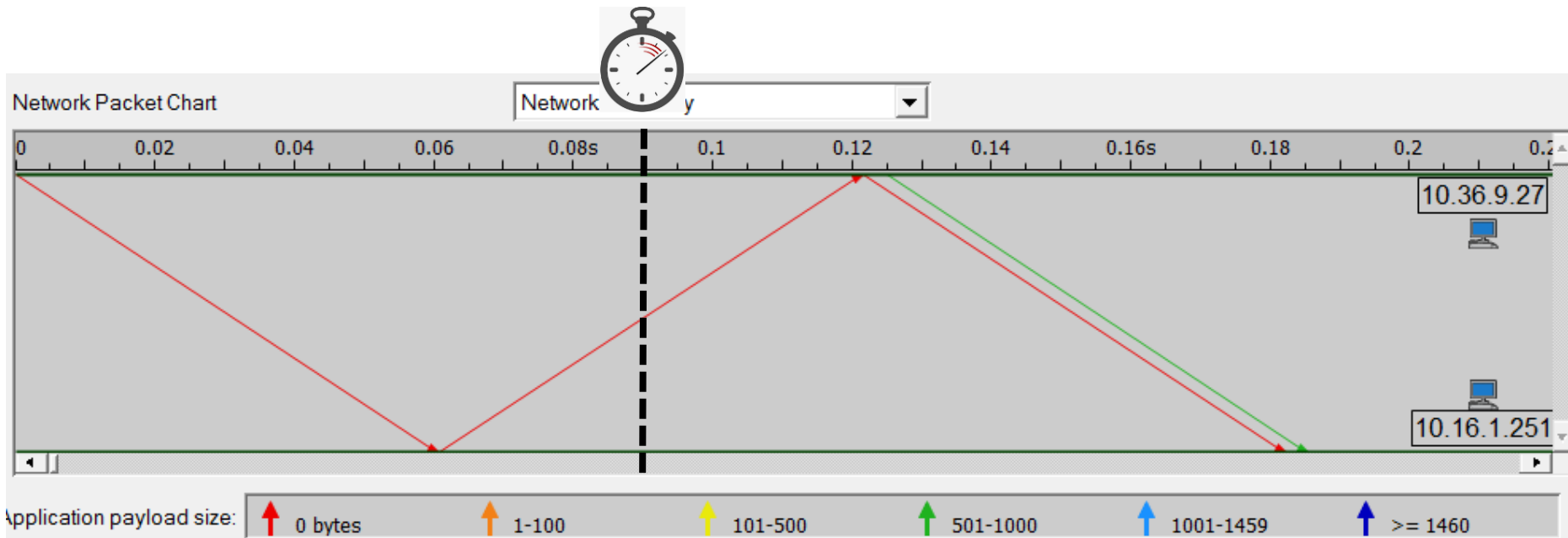


What is the TCP State of each host at this timepoint?





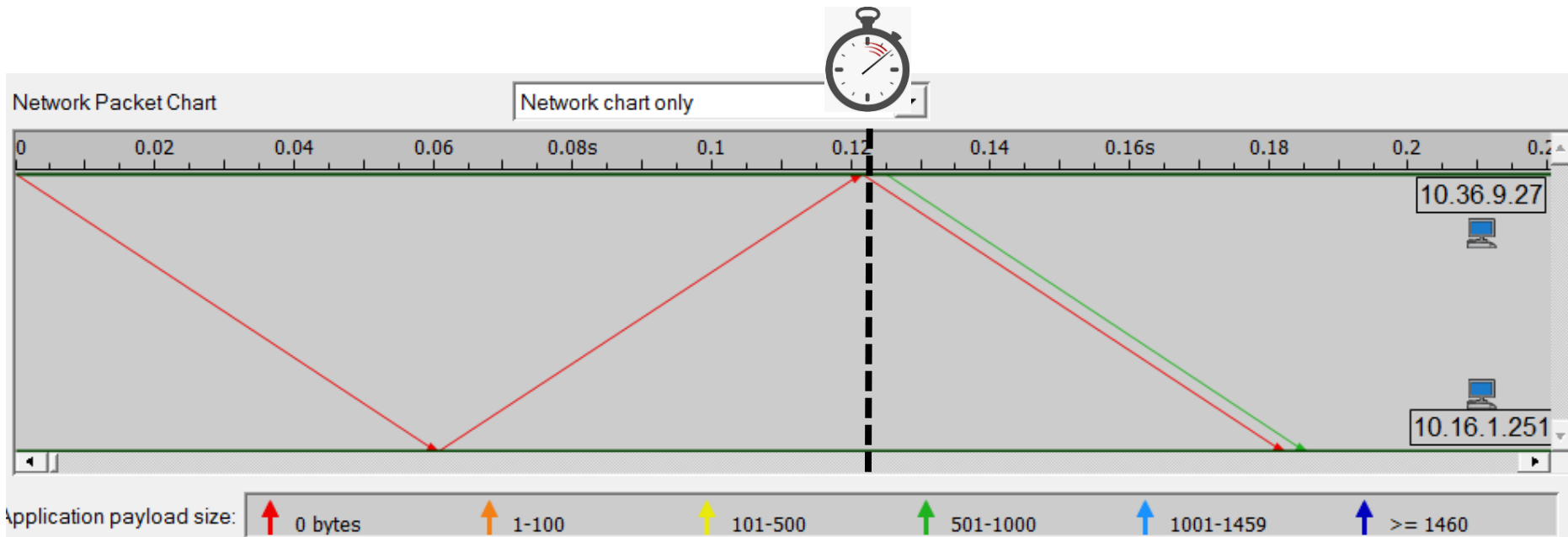
# Split Brain – State Discussion





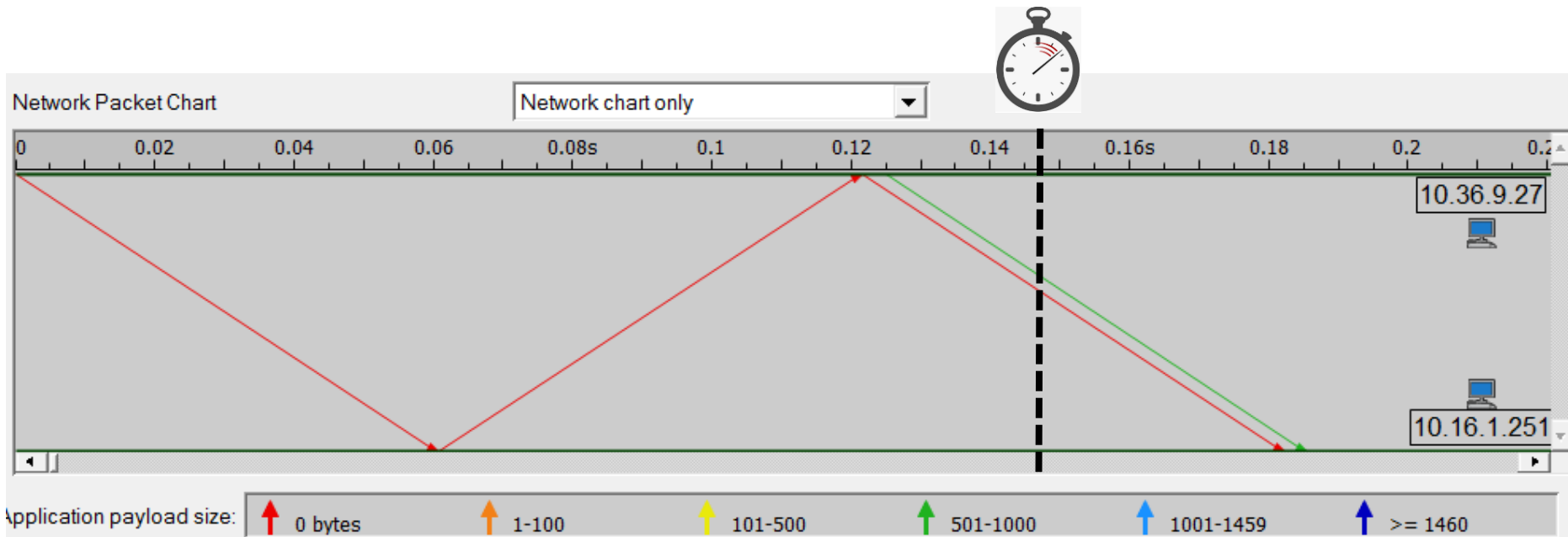


# Split Brain – State Discussion



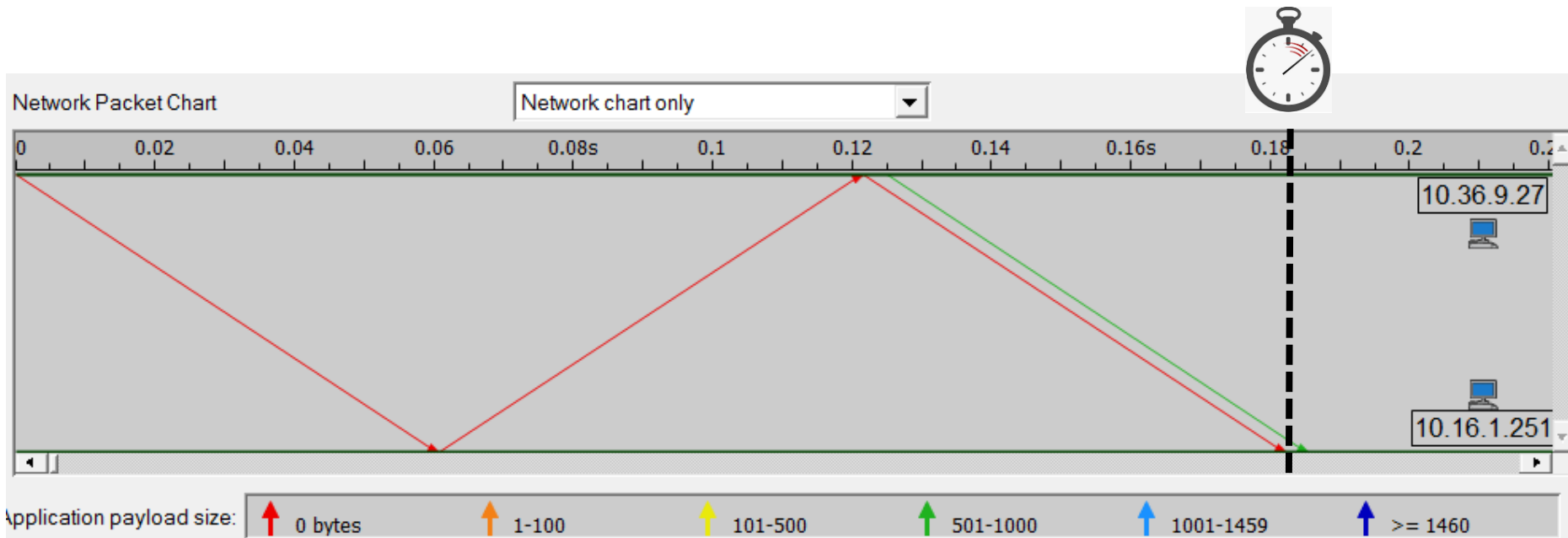


# Split Brain – State Discussion





# Split Brain – State Discussion





# Discussion



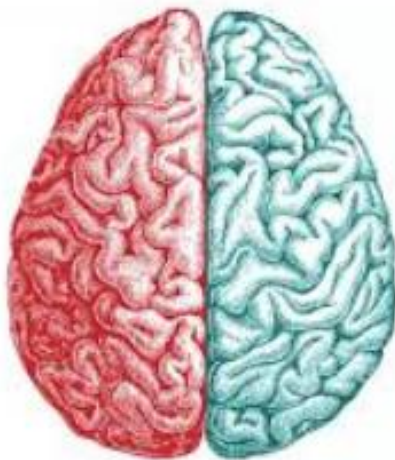
- Do you currently consider the send/receive time of the “other end point” when you do analysis?
- Do you think about each side’s TCP state?
- We’re just getting started on our journey...



# Split Brain Comparisons



- Next we'll compare Wireshark Expert Info for server pcap vs. client pcap





# Client Stats Conn52942



Wireshark · Expert Information · GP\_VPN\_Client\_Conn52942.pcap

Severity	Summary	Group	Protocol	Count
Error	TLSCiphertext length MUST NOT exceed $2^{14} + 2048$	Protocol	SSL	2
Warning	Ignored Unknown Record	Protocol	SSL	128
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	99
Warning	Previous segment(s) not captured (common at capture st...	Sequence	TCP	89
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	4
Note	This frame is a (suspected) retransmission	Sequence	TCP	5
Note	ACK to a TCP keep-alive segment	Sequence	TCP	35
Note	TCP keep-alive segment	Sequence	TCP	35
Note	Duplicate ACK (#1)	Sequence	TCP	183
Note	This session reuses previously negotiated keys (Session re...	Sequence	SSL	1
Chat	Connection finish (FIN)	Sequence	TCP	2
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	1
Chat	Connection establish request (SYN): server port 443	Sequence	TCP	1



# Server Stats Conn52942



Wireshark · Expert Information · Server\_side\_shifted\_Conn52942.pcap

Severity	Summary	Group	Protocol	Count
▶ Error	New fragment overlaps old data (retransmission?)	Malformed	TCP	8
▶ Warning	Ignored Unknown Record	Protocol	SSL	8
▶ Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	6
▶ Warning	Previous segment(s) not captured (common at capture st...	Sequence	TCP	2
▶ Note	This frame is a (suspected) fast retransmission	Sequence	TCP	15
▶ Note	This frame is a (suspected) retransmission	Sequence	TCP	15
▶ Note	ACK to a TCP keep-alive segment	Sequence	TCP	35
▶ Note	TCP keep-alive segment	Sequence	TCP	35
▶ Note	Duplicate ACK (#1)	Sequence	TCP	178
▶ Note	This session reuses previously negotiated keys (Session re...	Sequence	SSL	1
▶ Chat	Connection finish (FIN)	Sequence	TCP	2
▶ Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	1
▶ Chat	Connection establish request (SYN): server port 443	Sequence	TCP	1



# Server Left – Client Right



Server

Client

Wireshark · Expert Information · Server\_side\_shifted\_Conn52942.pcap

Severity	Summary	Group	Protocol	Count	Count
Error	New fragment overlaps old data (retransmission?)	Malformed	TCP	8	2
Warning	Ignored Unknown Record	Protocol	SSL	8	128
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	6	99
Warning	Previous segment(s) not captured (common at capture st...	Sequence	TCP	2	89
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	15	4
Note	This frame is a (suspected) retransmission	Sequence	TCP	15	5
Note	ACK to a TCP keep-alive segment	Sequence	TCP	35	35
Note	TCP keep-alive segment	Sequence	TCP	35	35
Note	Duplicate ACK (#1)	Sequence	TCP	178	183
Note	This session reuses previously negotiated keys (Session re...	Sequence	SSL	1	1
Chat	Connection finish (FIN)	Sequence	TCP	2	2
Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	1	1
Chat	Connection establish request (SYN): server port 443	Sequence	TCP	1	1





# Discussion - Retransmissions



Server      Client

▷ Note	This frame is a (suspected) fast retransmission	Sequence	TCP	15	4
▷ Note	This frame is a (suspected) retransmission	Sequence	TCP	15	5

- Why does server report more retransmissions than client?
- How does Wireshark define a “fast retransmission”?



## TCP Fast Retransmission

Set when all of the following are true:

- This is not a keepalive packet.
- In the forward direction, the segment size is greater than zero or the SYN or FIN is set.
- The next expected sequence number is greater than the current sequence number.
- We have more than two duplicate ACKs in the reverse direction.
- The current sequence number equals the next expected acknowledgement number.
- We saw the last acknowledgement less than 20ms ago.

Supersedes "Out-Of-Order", "Spurious Retransmission", and "Retransmission".



# Discussion – OOS & Drops



Server

Client

▷ Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	6	99
▷ Warning	Previous segment(s) not captured (common at capture st...	Sequence	TCP	2	89

- Why does client report more OOS and “previous segment(s) not captured” than server?
- Why does server report \*any\* OOS?



## TCP Out-Of-Order

Set when all of the following are true:

- This is not a keepalive packet.
- In the forward direction, the segment length is greater than zero or the SYN or FIN is set.
- The next expected sequence number is greater than the current sequence number.
- The next expected sequence number and the next sequence number differ.
- The last segment arrived within the calculated RTT (3ms by default).

Supersedes "Spurious Retransmission" and "Retransmission".



# Discussion – Unknown Records



Server

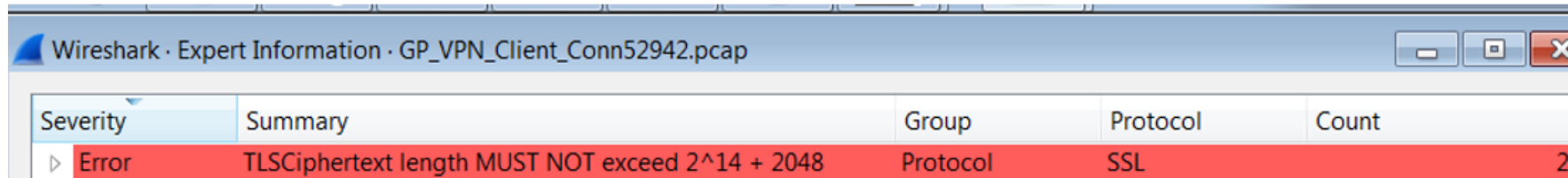
Client

Warning	Ignored Unknown Record	Protocol	SSL	8	128
---------	------------------------	----------	-----	---	-----

- Why does client report more SSL unknown records than server?



# Discussion – Length Error



Wireshark · Expert Information · GP\_VPN\_Client\_Conn52942.pcap

Severity	Summary	Group	Protocol	Count
Error	TLSCiphertext length MUST NOT exceed $2^{14} + 2048$	Protocol	SSL	2

- Why does client report Ciphertext length error and Server does not?



# Wireshark Update



- Wireshark 2.6.3 was used for this course
- The SSL/TLS Expert Info was updated in 2.6.4 and may treat these captures differently



# Discussion Fragment Overlap



Wireshark · Expert Information · Server_side_shifted_Conn52942.pcap				
Severity	Summary	Group	Protocol	Count
▶ Error	New fragment overlaps old data (retransmission?)	Malformed	TCP	8

- Why does Server report Fragment Overlap error and Client does not?
- Should this really be Severity == Error?





# Discussion



- Do these differences make sense?
- Additional thoughts?
- Comments?



# Let's drill into one of these...



Wireshark · Expert Information · Server\_side\_shifted\_Conn52942.pcap

Severity	Summary	Group	Protocol
Error	New fragment overlaps old data (retransmission?)	Malformed	TCP
714	[TCP Fast Retransmission] 443 → 52942 [PSH, ACK] Seq=5...	Malformed	TCP
845	[TCP Fast Retransmission] 443 → 52942 [PSH, ACK] Seq=6...	Malformed	TCP
926	[TCP Fast Retransmission] 443 → 52942 [PSH, ACK] Seq=7...	Malformed	TCP
987	[TCP Fast Retransmission] 443 → 52942 [PSH, ACK] Seq=8...	Malformed	TCP
1231	[TCP Fast Retransmission] 443 → 52942 [PSH, ACK] Seq=1...	Malformed	TCP
1581	[TCP Fast Retransmission] 443 → 52942 [PSH, ACK] Seq=1...	Malformed	TCP

This will be a great opportunity for additional  
Split Brain comparisons



# Split Brain Comparisons



- Drill down into Fragment Overlap Details





# Pop Quiz



- What's one of the best things about Wireshark?
- OK..., besides the Developers?
- Totally flexible columns, views, and profiles!!



# Configuration Profile Help



The screenshot shows the 'Wireshark User's Guide' window. The left sidebar contains a 'Contents' pane with a tree view. The 'Configuration Profiles' section is selected. The main content area displays the text for '10.6. Configuration Profiles'.

## 10.6. Configuration Profiles

Configuration Profiles can be used to configure and use more than one set of preferences and configurations. Select the *Configuration Profiles...* menu item from the *Edit* menu, or simply press Shift-Ctrl-A; and Wireshark will pop up the Configuration Profiles dialog box as shown in [Figure 10.9, "The configuration profiles dialog box"](#). It is also possible to click in the "Profile" part of the statusbar to popup a menu with available Configuration Profiles ([Figure 3.22, "The Statusbar with a configuration profile menu"](#)).

Configuration files stored in the Profiles:

- Preferences (preferences) ([Section 10.5, "Preferences"](#))
- Capture Filters (cfilters) ([Section 6.6, "Defining and saving filters"](#))
- Display Filters (dfilters) ([Section 6.6, "Defining and saving filters"](#))
- Coloring Rules (colorfilters) ([Section 10.3, "Packet colorization"](#))
- Disabled Protocols (disabled\_protos) ([Section 10.4.1, "The "Enabled Protocols" dialog box"](#))
- User Accessible Tables:
  - Custom HTTP headers (custom\_http\_header\_fields)
  - Custom IMF headers (imf\_header\_fields)



# Wireshark Profile Resources



- SB-SACK
  - SB-IP ID
  - SB-Seq Analysis
- 
- (will be posted on the Sharkfest retrospective page with the capture files)



# View with Classic Profile



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
697	350.989481	10.16.1.251	10.36.9.27	TCP	2638	443 → 52942 [ACK] Seq=518959 Ack=64515 Win=130816 Len=2584 [TCP segment of a reassembled P...
698	350.989502	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=507101 Win=65792 Len=0
699	350.989514	10.16.1.251	10.36.9.27	TLSv1	2623	Application Data
700	350.989537	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=509670 Win=65792 Len=0
701	350.989907	10.16.1.251	10.36.9.27	TCP	3930	443 → 52942 [ACK] Seq=524112 Ack=64515 Win=130816 Len=3876 [TCP segment of a reassembled P...
702	351.096868	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=512254 Win=65792 Len=0
703	351.096869	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=514838 Win=65792 Len=0
704	351.096921	10.16.1.251	10.36.9.27	TLSv1	5207	Application Data
705	351.101927	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=516375 Win=65792 Len=0
706	351.101974	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=518959 Win=65792 Len=0
707	351.102241	10.16.1.251	10.36.9.27	TCP	3930	443 → 52942 [ACK] Seq=533141 Ack=64515 Win=130816 Len=3876 [TCP segment of a reassembled P...
708	351.105948	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=521543 Win=65792 Len=0
709	351.105972	10.16.1.251	10.36.9.27	TLSv1	1591	Application Data
710	351.110879	10.36.9.27	10.16.1.251	TCP	66	52942 → 443 [ACK] Seq=64515 Ack=522835 Win=65792 Len=0 SLE=524112 SRE=525404
711	351.110881	10.36.9.27	10.16.1.251	TCP	66	[TCP Dup ACK 710#1] 52942 → 443 [ACK] Seq=64515 Ack=522835 Win=65792 Len=0 SLE=524112 SRE=525404
712	351.110929	10.36.9.27	10.16.1.251	TCP	66	[TCP Dup ACK 710#2] 52942 → 443 [ACK] Seq=64515 Ack=522835 Win=65792 Len=0 SLE=524112 SRE=525404
713	351.214132	10.36.9.27	10.16.1.251	TCP	66	[TCP Dup ACK 710#3] 52942 → 443 [ACK] Seq=64515 Ack=522835 Win=65792 Len=0 SLE=524112 SRE=525404
714	351.214191	10.16.1.251	10.36.9.27	TCP	1346	[TCP Fast Retransmission] 443 → 52942 [PSH, ACK] Seq=522835 Ack=64515 Win=130816 Len=1292 [TCP segment of a reassembled P...
715	351.214233	10.36.9.27	10.16.1.251	TCP	66	[TCP Dup ACK 710#4] 52942 → 443 [ACK] Seq=64515 Ack=522835 Win=65792 Len=0 SLE=524112 SRE=525404
716	351.214235	10.36.9.27	10.16.1.251	TCP	66	[TCP Dup ACK 710#5] 52942 → 443 [ACK] Seq=64515 Ack=522835 Win=65792 Len=0 SLE=524112 SRE=525404



# View with Classic Profile



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
697	350.989481	10.16.1.251	10.36.9.27	TCP	2638	443 → 52942 [ACK] Seq=518959 Ack=64515 Win=130816 Len=2584 [TCP segment of a reassembled P...
698	350.989502	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=507101 Win=65792 Len=0
699	350.989514	10.16.1.251	10.36.9.27	TLSv1	2623	Application Data
700	350.989537	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=507101 Win=65792 Len=0
701	350.989907	10.16.1.251	10.36.9.27	TCP	3930	443 → 52942 [ACK] Seq=518959 Ack=64515 Win=130816 Len=2584 [TCP segment of a reassembled P...
702	351.096868	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=507101 Win=65792 Len=0
703	351.096869	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=507101 Win=65792 Len=0
704	351.096921	10.16.1.251	10.36.9.27	TLSv1	5207	Application Data
705	351.101927	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=507101 Win=65792 Len=0
706	351.101974	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=507101 Win=65792 Len=0
707	351.102241	10.16.1.251	10.36.9.27	TCP	3930	443 → 52942 [ACK] Seq=518959 Ack=64515 Win=130816 Len=2584 [TCP segment of a reassembled P...
708	351.105948	10.36.9.27	10.16.1.251	TCP	60	52942 → 443 [ACK] Seq=64515 Ack=521543 Win=65792 Len=0
709	351.105972	10.16.1.251	10.36.9.27	TLSv1	1591	Application Data
710	351.110879	10.36.9.27	10.16.1.251	TCP	66	52942 → 443 [ACK] Seq=64515 Ack=522835 Win=65792 Len=0 SLE=524112 SRE=525404
711	351.110881	10.36.9.27	10.16.1.251	TCP	66	[TCP Dup ACK 710#1] 52942 → 443 [ACK] Seq=64515 Ack=522835 Win=65792 Len=0 SLE=524112 SRE=525404
712	351.110929	10.36.9.27	10.16.1.251	TCP	66	[TCP Dup ACK 710#2] 52942 → 443 [ACK] Seq=64515 Ack=522835 Win=65792 Len=0 SLE=524112 SRE=525404
713	351.214132	10.36.9.27	10.16.1.251	TCP	66	[TCP Dup ACK 710#3] 52942 → 443 [ACK] Seq=64515 Ack=522835 Win=65792 Len=0 SLE=524112 SRE=525404
714	351.214191	10.16.1.251	10.36.9.27	TCP	1346	[TCP Fast Retransmission] 443 → 52942 [PSH, ACK] Seq=522835 Ack=64515 Win=130816 Len=1292 [TCP segment of a reassembled P...
715	351.214233	10.36.9.27	10.16.1.251	TCP	66	[TCP Dup ACK 710#4] 52942 → 443 [ACK] Seq=64515 Ack=522835 Win=65792 Len=0 SLE=524112 SRE=525404
716	351.214235	10.36.9.27	10.16.1.251	TCP	66	[TCP Dup ACK 710#5] 52942 → 443 [ACK] Seq=64515 Ack=522835 Win=65792 Len=0 SLE=524112 SRE=525404

What columns do we need in our view to better understand Fragment Overlap?





# Profile SB-Seq Analysis



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	Protocol	Length	Sequence number	Next sequence number	Info
699	350.989514	0.000012000	10.16.1.251	10.36.9.27	TLSv1	2623	521543	524112	Application Data
700	350.989537	0.000023000	10.36.9.27	10.16.1.251	TCP	60	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=509670 Win=6579
701	350.989907	0.000370000	10.16.1.251	10.36.9.27	TCP	3930	524112	527988	443 → 52942 [ACK] Seq=524112 Ack=64515 Win=1308
702	351.096868	0.106961000	10.36.9.27	10.16.1.251	TCP	60	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=512254 Win=6579
703	351.096869	0.000001000	10.36.9.27	10.16.1.251	TCP	60	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=514838 Win=6579
704	351.096921	0.000052000	10.16.1.251	10.36.9.27	TLSv1	5207	527988	533141	Application Data
705	351.101927	0.005006000	10.36.9.27	10.16.1.251	TCP	60	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=516375 Win=6579
706	351.101974	0.000047000	10.36.9.27	10.16.1.251	TCP	60	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=518959 Win=6579
707	351.102241	0.000267000	10.16.1.251	10.36.9.27	TCP	3930	533141	537017	443 → 52942 [ACK] Seq=533141 Ack=64515 Win=1308
708	351.105948	0.003707000	10.36.9.27	10.16.1.251	TCP	60	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=521543 Win=6579
709	351.105972	0.000024000	10.16.1.251	10.36.9.27	TLSv1	1591	537017	538554	Application Data
710	351.110879	0.004907000	10.36.9.27	10.16.1.251	TCP	66	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=522835 Win=6579
711	351.110881	0.000002000	10.36.9.27	10.16.1.251	TCP	66	64515	64515	[TCP Dup ACK 710#1] 52942 → 443 [ACK] Seq=64515
712	351.110929	0.000048000	10.36.9.27	10.16.1.251	TCP	66	64515	64515	[TCP Dup ACK 710#2] 52942 → 443 [ACK] Seq=64515
713	351.214132	0.103203000	10.36.9.27	10.16.1.251	TCP	66	64515	64515	[TCP Dup ACK 710#3] 52942 → 443 [ACK] Seq=64515
714	351.214191	0.000059000	10.16.1.251	10.36.9.27	TCP	1346	522835	524127	[TCP Fast Retransmission] 443 → 52942 [PSH, ACK]
715	351.214233	0.000042000	10.36.9.27	10.16.1.251	TCP	66	64515	64515	[TCP Dup ACK 710#4] 52942 → 443 [ACK] Seq=64515

# What are these “jumbo” packets?

Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	Protocol	Length	Sequence number	Next sequence number	Info
699	350.989514	0.000012000	10.16.1.251	10.36.9.27	TLSv1	2623	521543	524112	Application Data
700	350.989537	0.000023000	10.36.9.27	10.16.1.251	TCP	60	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=509670 Win=6579
701	350.989907	0.000370000	10.16.1.251	10.36.9.27	TCP	3930	524112	527988	443 → 52942 [ACK] Seq=524112 Ack=64515 Win=1308
702	351.096868	0.106961000	10.36.9.27	10.16.1.251	TCP	60	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=512254 Win=6579
703	351.096869	0.000001000	10.36.9.27	10.16.1.251	TCP	60	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=514838 Win=6579
704	351.096921	0.000052000	10.16.1.251	10.36.9.27	TLSv1	5207	527988	533141	Application Data
705	351.101927	0.005006000	10.36.9.27	10.16.1.251	TCP	60	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=516375 Win=6579
706	351.101974	0.000047000	10.36.9.27	10.16.1.251	TCP	60	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=518959 Win=6579
707	351.102241	0.000267000	10.16.1.251	10.36.9.27	TCP	3930	533141	537017	443 → 52942 [ACK] Seq=533141 Ack=64515 Win=1308
708	351.105948	0.003707000	10.36.9.27	10.16.1.251	TCP	60	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=521543 Win=6579
709	351.105972	0.000024000	10.16.1.251	10.36.9.27	TLSv1	1591	537017	538554	Application Data
710	351.110879	0.004907000	10.36.9.27	10.16.1.251	TCP	66	64515	64515	52942 → 443 [ACK] Seq=64515 Ack=522835 Win=6579
711	351.110881	0.000002000	10.36.9.27	10.16.1.251	TCP	66	64515	64515	[TCP Dup ACK 710#1] 52942 → 443 [ACK] Seq=64515
712	351.110929	0.000048000	10.36.9.27	10.16.1.251	TCP	66	64515	64515	[TCP Dup ACK 710#2] 52942 → 443 [ACK] Seq=64515
713	351.214132	0.103203000	10.36.9.27	10.16.1.251	TCP	66	64515	64515	[TCP Dup ACK 710#3] 52942 → 443 [ACK] Seq=64515
714	351.214191	0.000059000	10.16.1.251	10.36.9.27	TCP	1346	522835	524127	[TCP Fast Retransmission] 443 → 52942 [PSH, ACK]
715	351.214233	0.000042000	10.36.9.27	10.16.1.251	TCP	66	64515	64515	[TCP Dup ACK 710#4] 52942 → 443 [ACK] Seq=64515



# TCP Large Send Offload



tcp large send offload



7



All

Shopping

News

Images

Videos

More

Settings

Tools

About 205,000 results (0.50 seconds)

## Large Send Offload and Network Performance | Peer Wisdom

[www.peervision.org/2013/04/03/large-send-offload-and-network-performance/](http://www.peervision.org/2013/04/03/large-send-offload-and-network-performance/) ▼

Apr 3, 2013 - So what is **Large Send Offload** (also known as Large Segmentation ... that allows the TCP/IP network stack to build a large TCP message of up to ...

## Disabling Large Send Offload – Windows | Peer Wisdom

[www.peervision.org/2013/04/25/disabling-large-send-offload-windows/](http://www.peervision.org/2013/04/25/disabling-large-send-offload-windows/) ▼

Apr 25, 2013 - In an earlier post, I described the **Large Send Offload** (LSO) feature of modern ... I'll start with disabling LSO in the TCP/IP network stack since ...

## Large send offload - Wikipedia

[https://en.wikipedia.org/wiki/Large\\_send\\_offload](https://en.wikipedia.org/wiki/Large_send_offload) ▼

In computer networking, **large send offload** (LSO) is a technique for increasing egress ... The technique is also called **TCP segmentation offload** (TSO) when applied to **TCP**, or generic segmentation offload (GSO). The inbound counterpart of ...

## Large Send Offload causes performance and slowdown issues

<https://www.bitdefender.com/.../large-send-offload-causes-performance-and-slowdown...> ▼

**Large Send Offload** causes performance and slowdown issues ... initialization or when an interface appears as a Plug and Play event, the TCP/IP driver will ...

## Large send offload



In computer networking, large send offload is a technique for increasing egress throughput of high-bandwidth network connections by reducing CPU overhead. It works by passing a multipacket buffer to the network interface card. The NIC then splits this buffer into separate packets.

[Wikipedia](#)

Feedback



# Discussion





- Where does pcap intercept packets?
- What is the packet's journey after pcap capture?
- How is this different on a VM?
- How about a host based on blade chassis technology (aka Blade Server)?



# TCP Large Receive Offload





[Web](#) [Images](#) [Videos](#) [News](#)

All Regions ▾ Safe Search: Moderate ▾ Any Time ▾


### Large receive offload - Wikipedia

In computer networking, **large receive offload** (LRO) is a technique for increasing inbound throughput of high-bandwidth network connections by reducing CPU overhead.

W [https://en.wikipedia.org/wiki/Large\\_receive\\_offload](https://en.wikipedia.org/wiki/Large_receive_offload)


### Large Receive Offload (LRO) Support for ... - VMware VROOM! Blog

**Large Receive Offload** (LRO) is a technique to reduce the CPU time for processing TCP packets that arrive from the network at a high rate. LRO reassembles incoming packets into larger ones (but fewer packets) to deliver them to the network stack of the system.

 <https://blogs.vmware.com/performance/2015/06/vmxnet3-lro.html>


### Large Receive Offload - VMware Docs Home

**Large Receive Offload** Use **Large Receive Offload** (LRO) to reduce the CPU overhead for processing packets that arrive from the network at a high rate. LRO reassembles incoming network packets into larger buffers and transfers the resulting larger but fewer packets to the network stack of the host or virtual machine.

 <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere...>

### How To Enable Large Receive Offload (LRO) | Mellanox ...

**large-receive-offload**: on Generic **Receive Offload** (GRO) When "hw\_lro" flag cannot be found on a new kernel (LRO type is hardware), packets aggregation can be done using the GRO feature via ethtool.

 <https://community.mellanox.com/docs/DOC-2814>

### Large receive offload

In computer networking, large receive offload is a technique for increasing inbound throughput of high-bandwidth network connections by reducing CPU overhead. It works by aggregating multiple incoming packets from a single stream into a larger buffer before they are passed higher up the networking stack, thus reducing the number of packets that have to be processed. Linux implementations generally use LRO in conjunction with the New API to also reduce the number of interrupts.

W [More at Wikipedia](#)

[Feedback](#)



# Back to Fragment Overlap





# Here is the overlap



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
699	350.989514	0.000012000	10.16.1.251	10.36.9.27	2569	521543	524112	64515	17011	Application Data
700	350.989537	0.000023000	10.36.9.27	10.16.1.251	0	64515	64515	509670		52942 → 443 [ACK] Seq=645
701	350.989907	0.000370000	10.16.1.251	10.36.9.27	3876	524112	527988	64515	18318	443 → 52942 [ACK] Seq=524
702	351.096868	0.106961000	10.36.9.27	10.16.1.251	0	64515	64515	512254		52942 → 443 [ACK] Seq=645
703	351.096869	0.000001000	10.36.9.27	10.16.1.251	0	64515	64515	514838		52942 → 443 [ACK] Seq=645
704	351.096921	0.000052000	10.16.1.251	10.36.9.27	5153	527988	533141	64515	18303	Application Data
705	351.101927	0.005006000	10.36.9.27	10.16.1.251	0	64515	64515	516375		52942 → 443 [ACK] Seq=645
706	351.101974	0.000047000	10.36.9.27	10.16.1.251	0	64515	64515	518959		52942 → 443 [ACK] Seq=645
707	351.102241	0.000267000	10.16.1.251	10.36.9.27	3876	533141	537017	64515	18058	443 → 52942 [ACK] Seq=533
708	351.105948	0.003707000	10.36.9.27	10.16.1.251	0	64515	64515	521543		52942 → 443 [ACK] Seq=645
709	351.105972	0.000024000	10.16.1.251	10.36.9.27	1537	537017	538554	64515	17011	Application Data
710	351.110879	0.004907000	10.36.9.27	10.16.1.251	0	64515	64515	522835		52942 → 443 [ACK] Seq=645
711	351.110881	0.000002000	10.36.9.27	10.16.1.251	0	64515	64515	522835		[TCP Dup ACK 710#1] 52942
712	351.110929	0.000048000	10.36.9.27	10.16.1.251	0	64515	64515	522835		[TCP Dup ACK 710#2] 52942
713	351.214132	0.103203000	10.36.9.27	10.16.1.251	0	64515	64515	522835		[TCP Dup ACK 710#3] 52942
714	351.214191	0.000059000	10.16.1.251	10.36.9.27	1292	522835	524127	64515	15719	[TCP Fast Retransmission]
715	351.214233	0.000042000	10.36.9.27	10.16.1.251	0	64515	64515	522835		[TCP Dup ACK 710#4] 52942



# Server Side Stream Visual



SEQ 521543

524111

2,569 Stream Bytes



SEQ 522835

524126



1,292 Stream Bytes





# Discussion



- At first, it might seem odd that the retransmitted segment does not “line up” with original segment
- We can be reasonably confident this is result of Large Send Offload
- Let’s jump to client capture to confirm...



# Anchor on SEQ==521543



521543



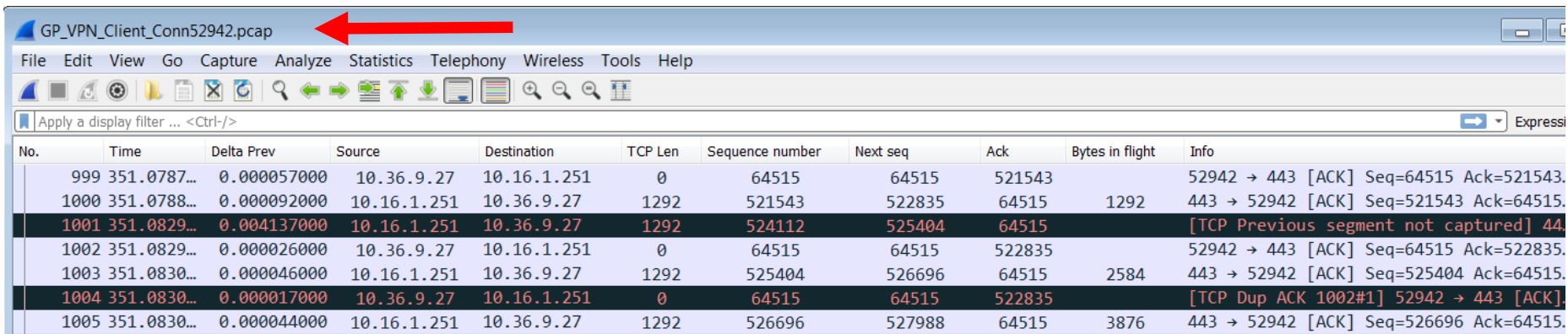
2,569 Stream Bytes

524111





# Several Observations



No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
999	351.0787...	0.000057000	10.36.9.27	10.16.1.251	0	64515	64515	521543		52942 → 443 [ACK] Seq=64515 Ack=521543.
1000	351.0788...	0.000092000	10.16.1.251	10.36.9.27	1292	521543	522835	64515	1292	443 → 52942 [ACK] Seq=521543 Ack=64515.
1001	351.0829...	0.004137000	10.16.1.251	10.36.9.27	1292	524112	525404	64515		[TCP Previous segment not captured] 443 → 52942 [ACK] Seq=524112 Ack=64515.
1002	351.0829...	0.000026000	10.36.9.27	10.16.1.251	0	64515	64515	522835		52942 → 443 [ACK] Seq=64515 Ack=522835.
1003	351.0830...	0.000046000	10.16.1.251	10.36.9.27	1292	525404	526696	64515	2584	443 → 52942 [ACK] Seq=525404 Ack=64515.
1004	351.0830...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835		[TCP Dup ACK 1002#1] 52942 → 443 [ACK] Seq=64515 Ack=522835.
1005	351.0830...	0.000044000	10.16.1.251	10.36.9.27	1292	526696	527988	64515	3876	443 → 52942 [ACK] Seq=526696 Ack=64515.

- Note file name in the title bar



# Segment Size Differences



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Express

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
999	351.0787...	0.000057000	10.36.9.27	10.16.1.251	0	64515	64515	521543		52942 → 443 [ACK] Seq=64515 Ack=521543.
1000	351.0788...	0.000092000	10.16.1.251	10.36.9.27	1292	521543	522835	64515	1292	443 → 52942 [ACK] Seq=521543 Ack=64515.
1001	351.0829...	0.004137000	10.16.1.251	10.36.9.27	1292	524112	525404	64515		[TCP Previous segment not captured] 443 → 52942 [ACK] Seq=524112 Ack=64515.
1002	351.0829...	0.000026000	10.36.9.27	10.16.1.251	0	64515	64515	522835		52942 → 443 [ACK] Seq=64515 Ack=522835.
1003	351.0830...	0.000046000	10.16.1.251	10.36.9.27	1292	525404	526696	64515	2584	443 → 52942 [ACK] Seq=525404 Ack=64515.
1004	351.0830...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835		[TCP Dup ACK 1002#1] 52942 → 443 [ACK] Seq=64515 Ack=522835.
1005	351.0830...	0.000044000	10.16.1.251	10.36.9.27	1292	526696	527988	64515	3876	443 → 52942 [ACK] Seq=526696 Ack=64515.

- Confirmed: Large Send Offload configured on Server
- Looks like the server NIC is handling segmentation



# Dropped or OOS?



GP\_VPN\_Client\_Conn52942.pcap 521543

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

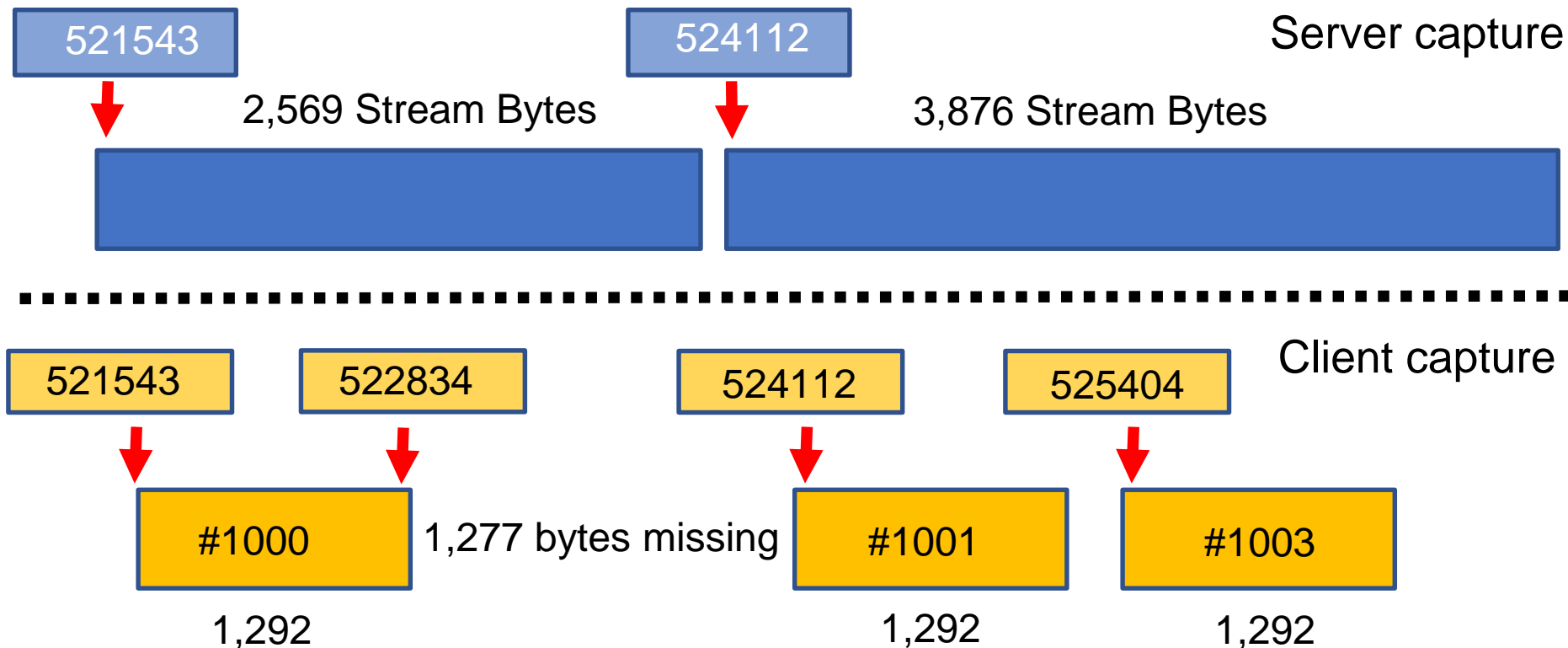
Apply a display filter ... <Ctrl-/> Express

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
999	351.0787...	0.000057000	10.36.9.27	10.16.1.251	0	64515	64515	521543		52942 → 443 [ACK] Seq=64515 Ack=521543.
1000	351.0788...	0.000092000	10.16.1.251	10.36.9.27	1292	521543	522835	64515	1292	443 → 52942 [ACK] Seq=521543 Ack=64515.
1001	351.0829...	0.004137000	10.16.1.251	10.36.9.27	1292	524112	525404	64515		[TCP Previous segment not captured] 443 → 52942 [ACK] Seq=524112 Ack=64515.
1002	351.0829...	0.000026000	10.36.9.27	10.16.1.251	0	64515	64515	522835		52942 → 443 [ACK] Seq=64515 Ack=522835.
1003	351.0830...	0.000046000	10.16.1.251	10.36.9.27	1292	525404	526696	64515	2584	443 → 52942 [ACK] Seq=525404 Ack=64515.
1004	351.0830...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835		[TCP Dup ACK 1002#1] 52942 → 443 [ACK].
1005	351.0830...	0.000044000	10.16.1.251	10.36.9.27	1292	526696	527988	64515	3876	443 → 52942 [ACK] Seq=526696 Ack=64515.

- If we freeze time right here, we can't be sure if it's just OOS or really a dropped packet
- We have to examine what comes next...



# Anchor on SEQ==521543





# Other Clues



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
999	351.0787...	0.000057000	10.36.9.27	10.16.1.251	0	64515	64515	521543		52942 → 443 [ACK] Seq=64515 Ack=521543.
1000	351.0788...	0.000092000	10.16.1.251	10.36.9.27	1292	521543	522835	64515	1292	443 → 52942 [ACK] Seq=521543 Ack=64515.
1001	351.0829...	0.004137000	10.16.1.251	10.36.9.27	1292	524112	525404	64515		[TCP Previous segment not captured] 443 → 52942 [ACK] Seq=524112 Ack=64515.
1002	351.0829...	0.000026000	10.36.9.27	10.16.1.251	0	64515	64515	522835		52942 → 443 [ACK] Seq=64515 Ack=522835.
1003	351.0830...	0.000046000	10.16.1.251	10.36.9.27	1292	525404	526696	64515	2584	443 → 52942 [ACK] Seq=525404 Ack=64515.
1004	351.0830...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835		[TCP Dup ACK 1002#1] 52942 → 443 [ACK] Seq=64515 Ack=522835.
1005	351.0830...	0.000044000	10.16.1.251	10.36.9.27	1292	526696	527988	64515	3876	443 → 52942 [ACK] Seq=526696 Ack=64515.

- Next seq after #1000 should have been 522835
- Wait! Isn't this the segment that was retransmitted by server? (yes)



# Other Clues



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Express

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
999	351.0787...	0.000057000	10.36.9.27	10.16.1.251	0	64515	64515	521543		52942 → 443 [ACK] Seq=64515 Ack=521543.
1000	351.0788...	0.000092000	10.16.1.251	10.36.9.27	1292	521543	522835	64515	1292	443 → 52942 [ACK] Seq=521543 Ack=64515.
1001	351.0829...	0.004137000	10.16.1.251	10.36.9.27	1292	524112	525404	64515		[TCP Previous segment not captured] 44
1002	351.0829...	0.000026000	10.36.9.27	10.16.1.251	0	64515	64515	522835		52942 → 443 [ACK] Seq=64515 Ack=522835.
1003	351.0830...	0.000046000	10.16.1.251	10.36.9.27	1292	525404	526696	64515	2584	443 → 52942 [ACK] Seq=525404 Ack=64515.
1004	351.0830...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835		[TCP Dup ACK 1002#1] 52942 → 443 [ACK].
1005	351.0830...	0.000044000	10.16.1.251	10.36.9.27	1292	526696	527988	64515	3876	443 → 52942 [ACK] Seq=526696 Ack=64515.

- Notice the change in ACK behavior
- Client ACKs every other packet then starts to ACK every packet
- Why is this?





# Profile Power



- Let's flip the view a little so we can quickly see SACK fields in the decode summary



# Profile: SB-SACK



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expressi

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	SACK LE	SACK RE	Info
999	351.0787...	0.000057000	10.36.9.27	10.16.1.251	0	64515	64515	521543			52942 → 443 [ACK] Seq=6
1000	351.0788...	0.000092000	10.16.1.251	10.36.9.27	1292	521543	522835	64515			443 → 52942 [ACK] Seq=!
1001	351.0829...	0.004137000	10.16.1.251	10.36.9.27	1292	524112	525404	64515			[TCP Previous segment r
1002	351.0829...	0.000026000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	525404	52942 → 443 [ACK] Seq=6
1003	351.0830...	0.000046000	10.16.1.251	10.36.9.27	1292	525404	526696	64515			443 → 52942 [ACK] Seq=!
1004	351.0830...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	526696	[TCP Dup ACK 1002#1] 5
1005	351.0830...	0.000044000	10.16.1.251	10.36.9.27	1292	526696	527988	64515			443 → 52942 [ACK] Seq=!
1006	351.0830...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	527988	[TCP Dup ACK 1002#2] 5
1007	351.1858...	0.102797000	10.16.1.251	10.36.9.27	1292	527988	529280	64515			443 → 52942 [ACK] Seq=!
1008	351.1859...	0.000032000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	529280	[TCP Dup ACK 1002#3] 5

- Client “SACKs” the new segments, but continues to report - I’m missing 522835



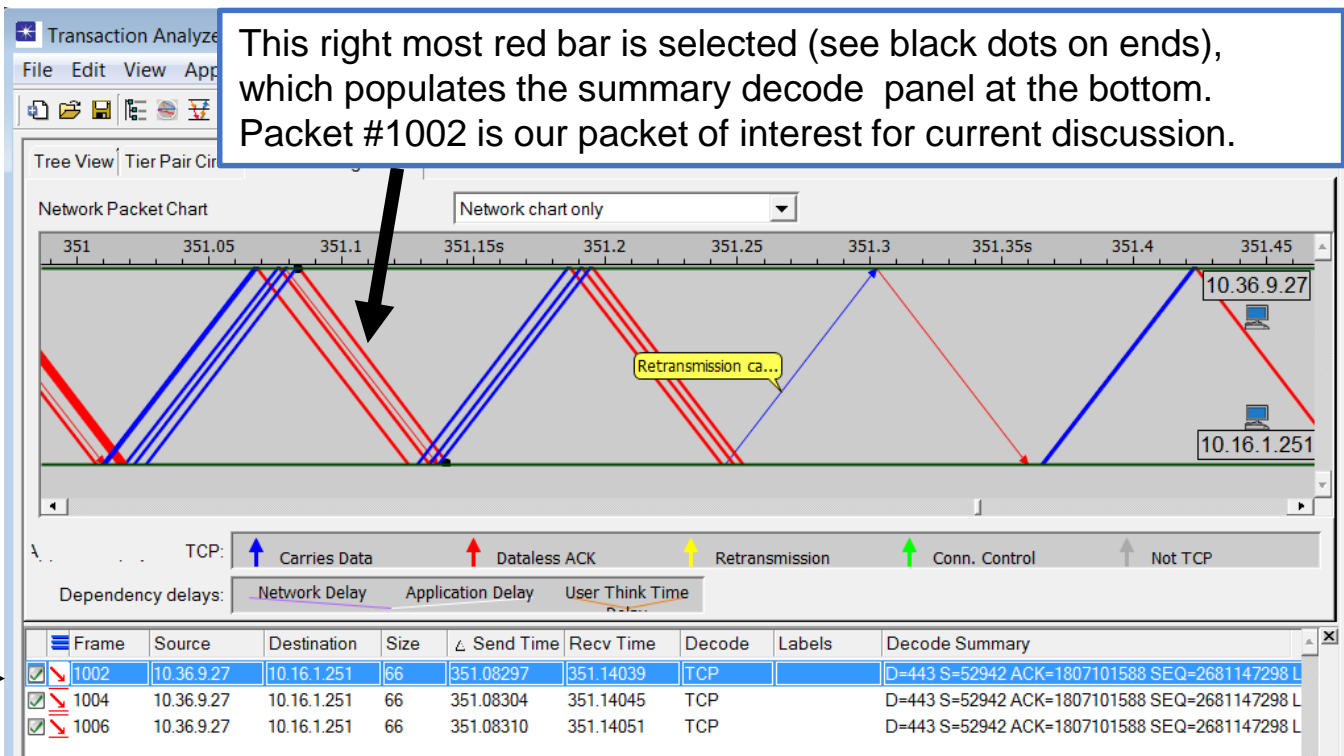
# Discussion



- We can see Client is reporting a missing segment
- Yet, why does server continue to send segments other than the one requested?
- Visualization really helps with this...

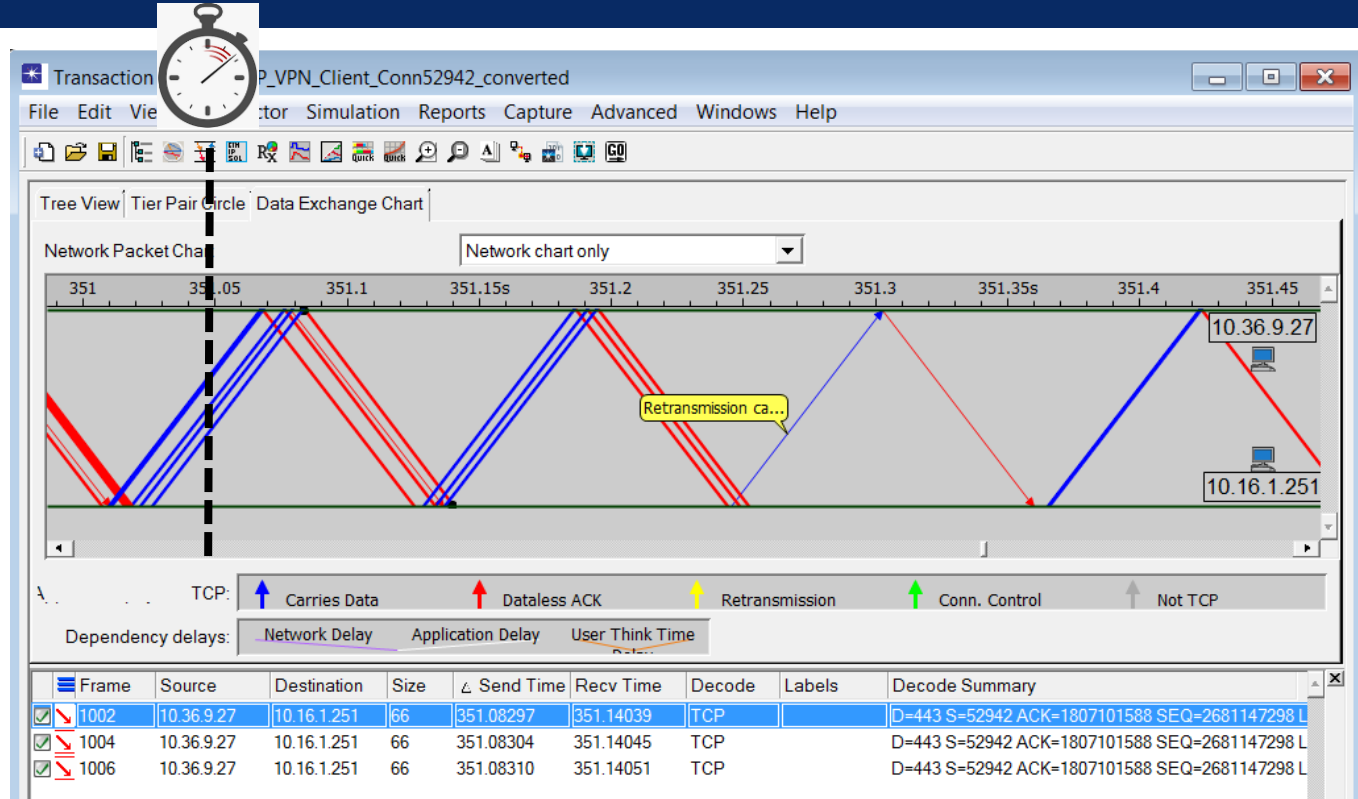


# End Point State Review



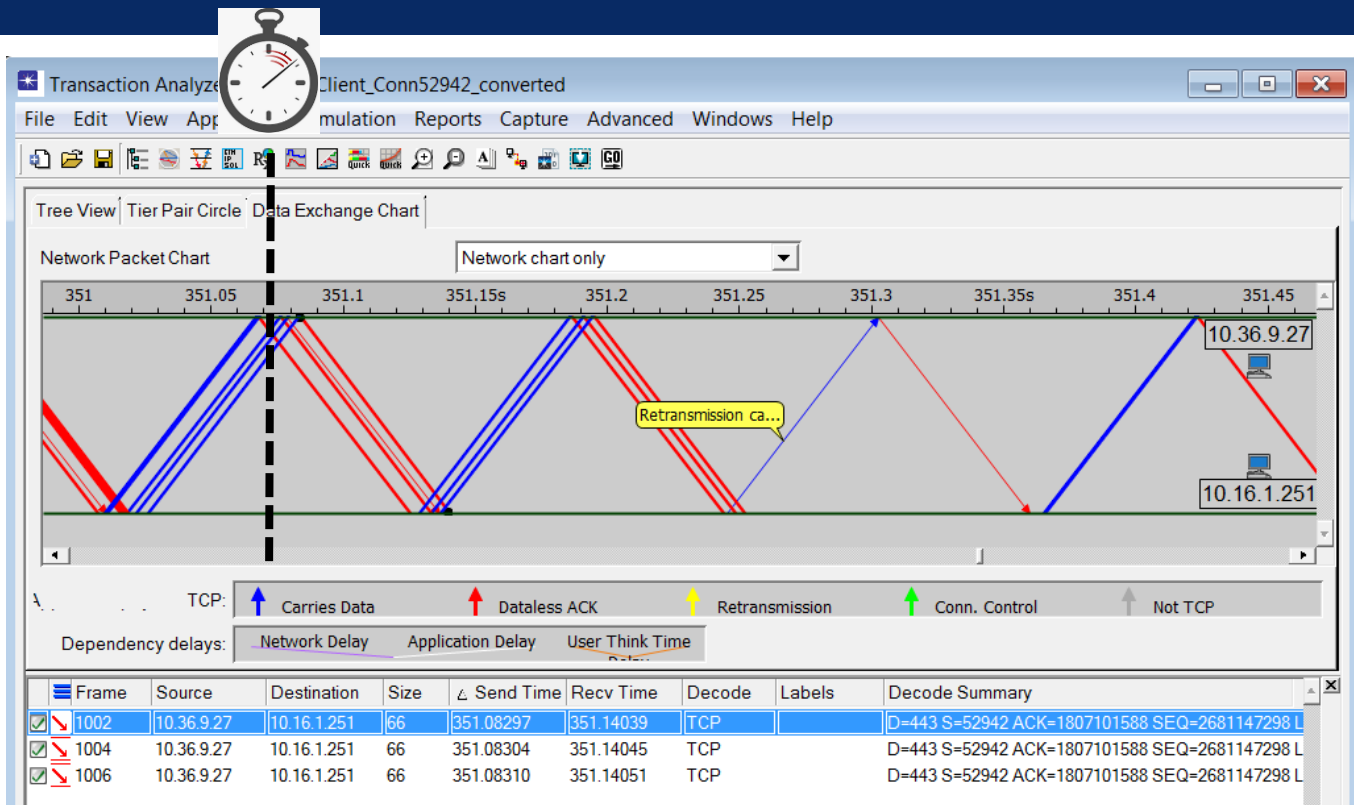


# Discuss state of each end point



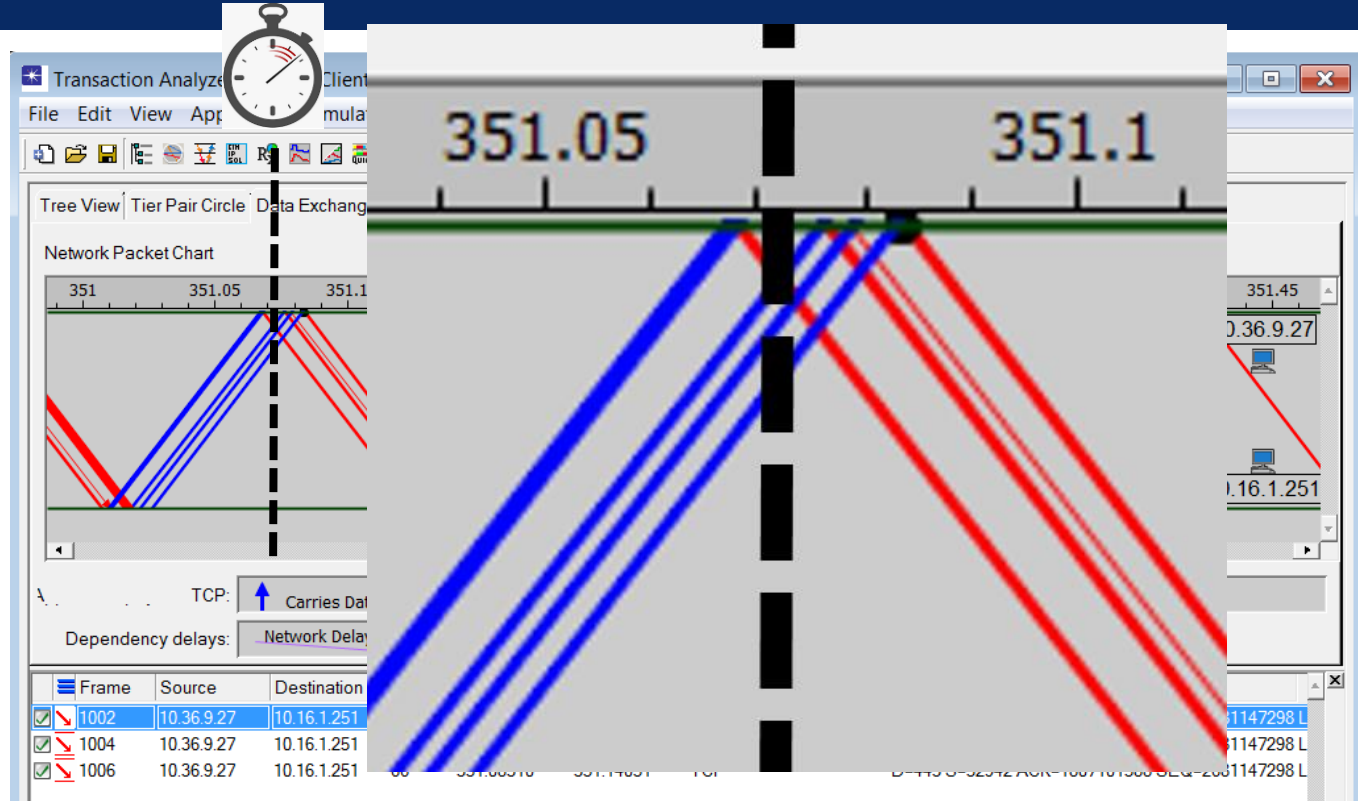


# Discuss state of each end point



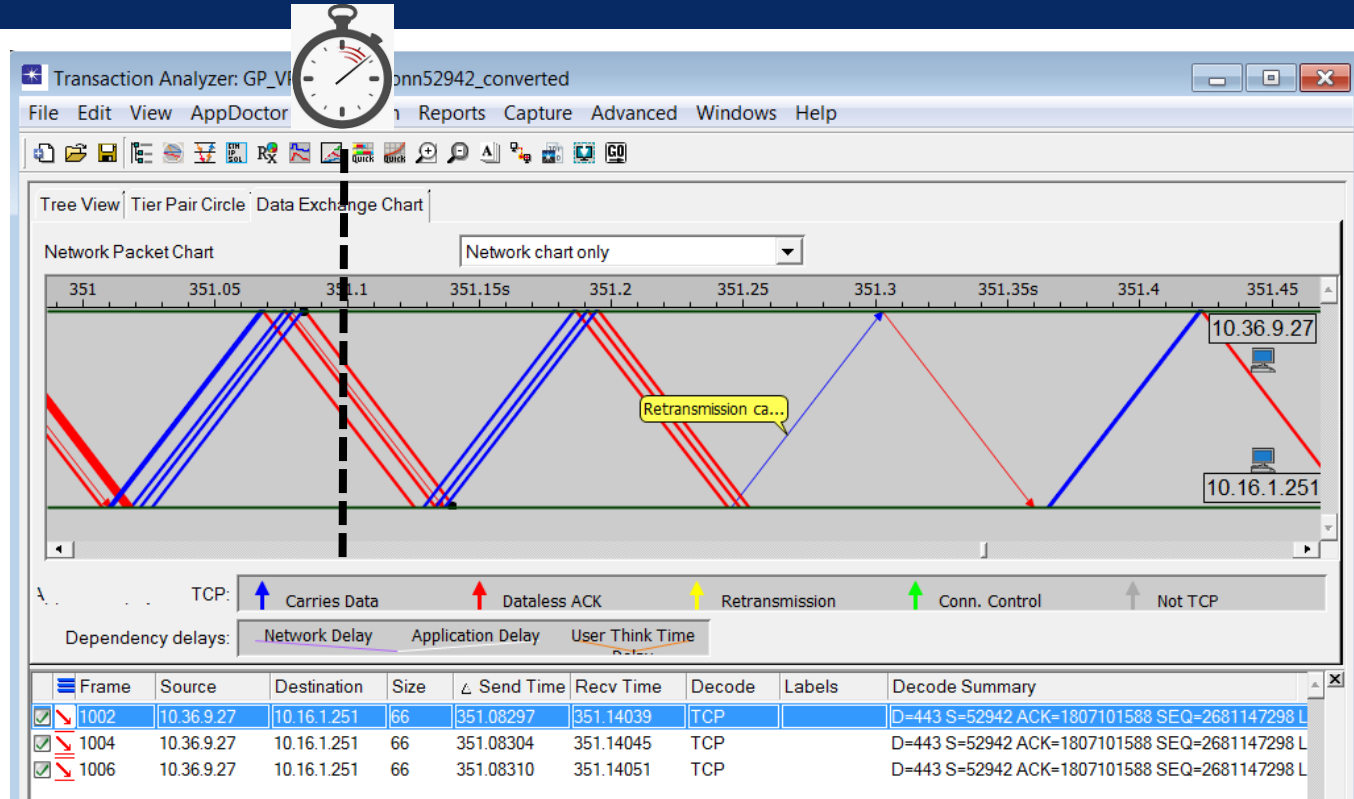


# Zoom-in a little...





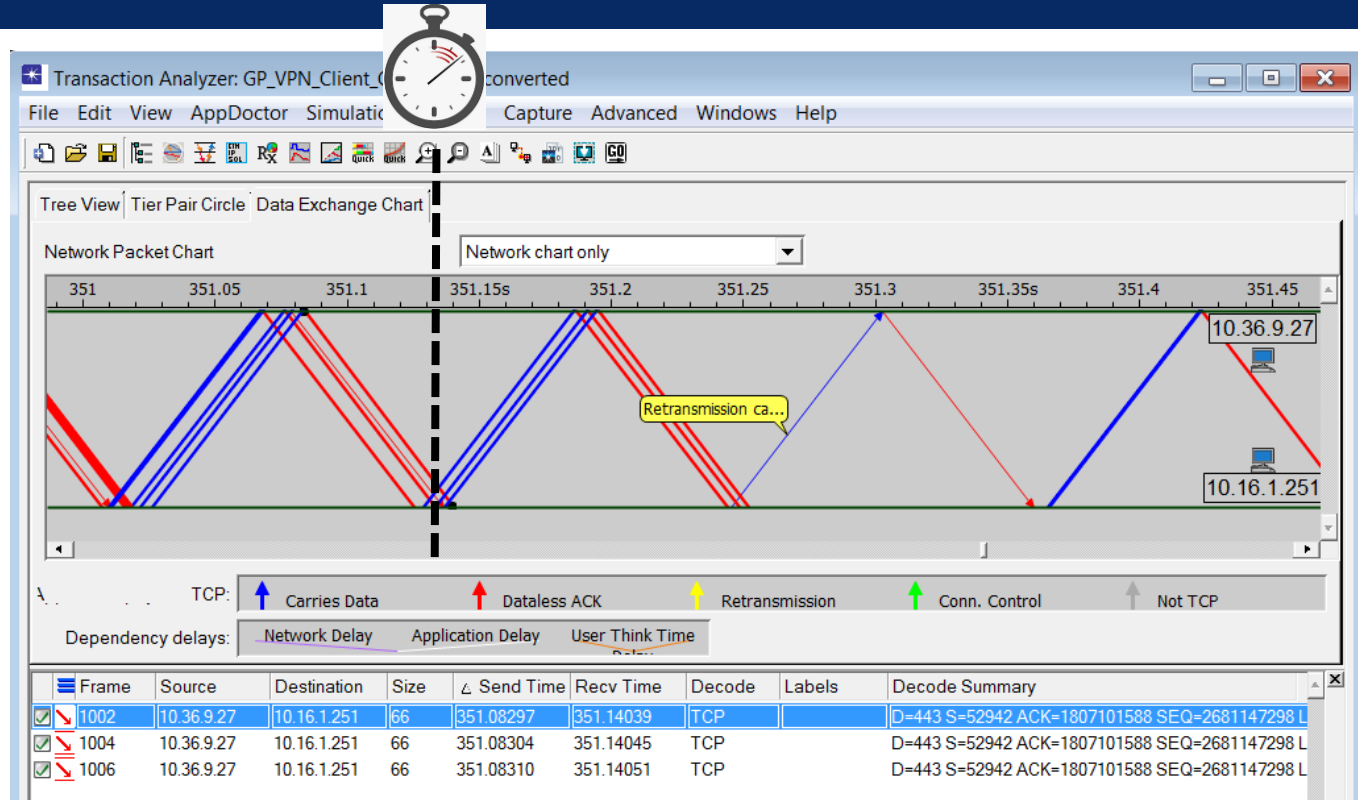
# Discuss state of each end point





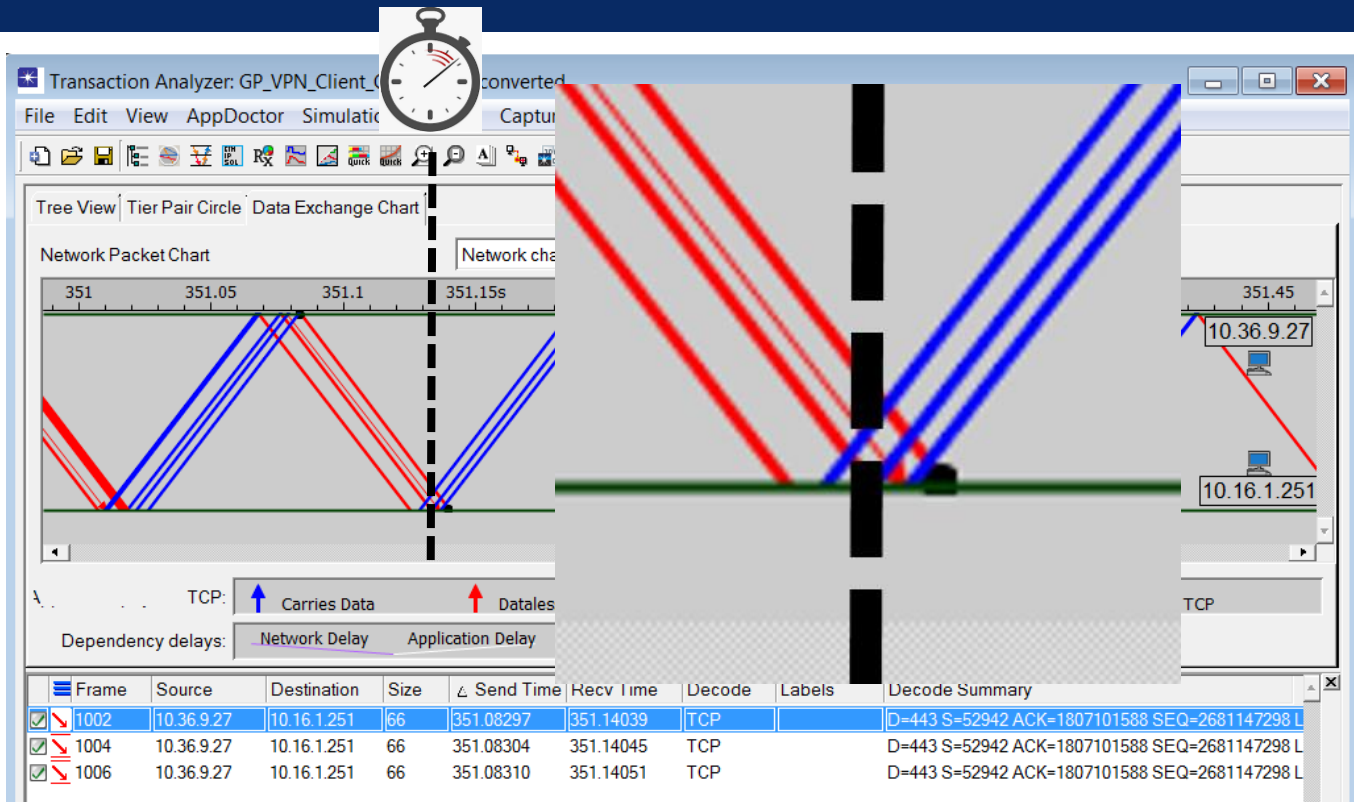


# Discuss state of each end point



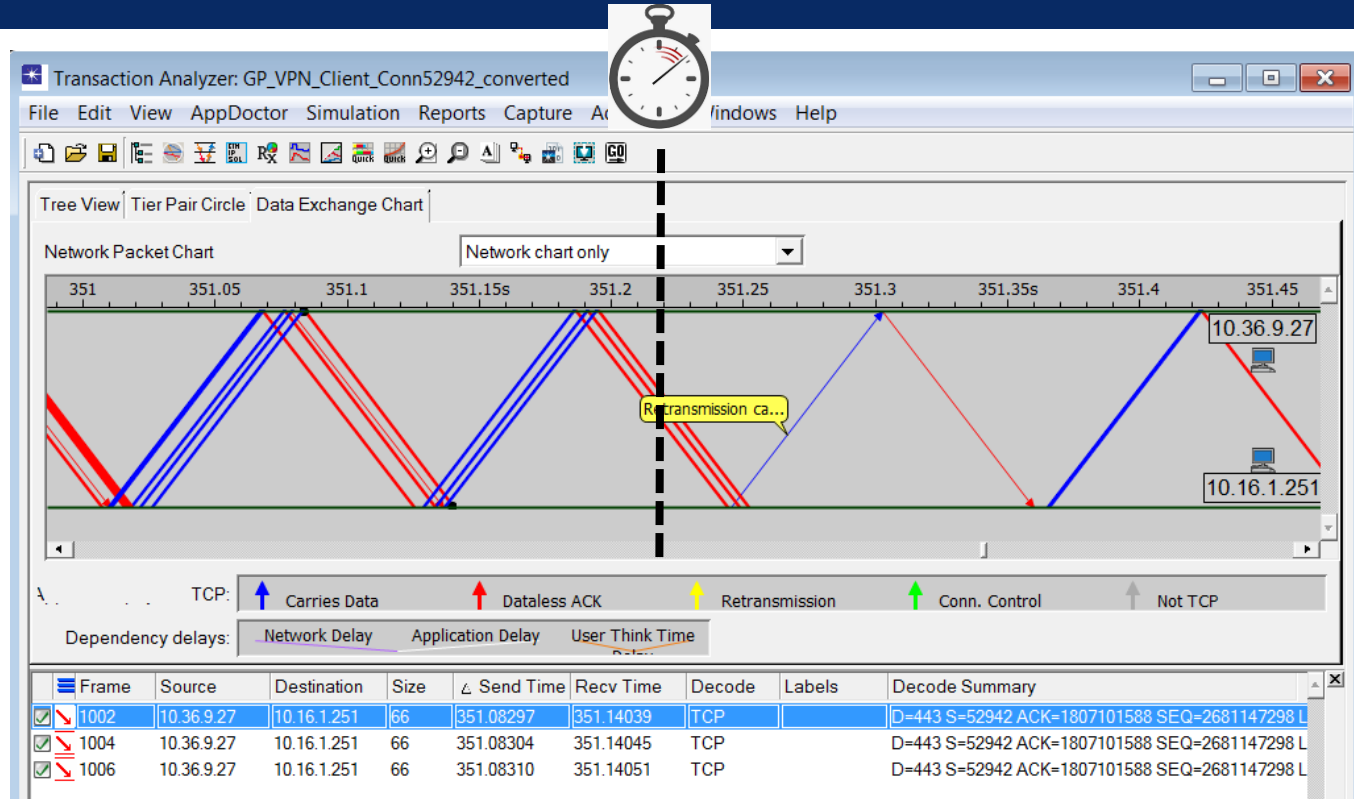


# Zoom-in



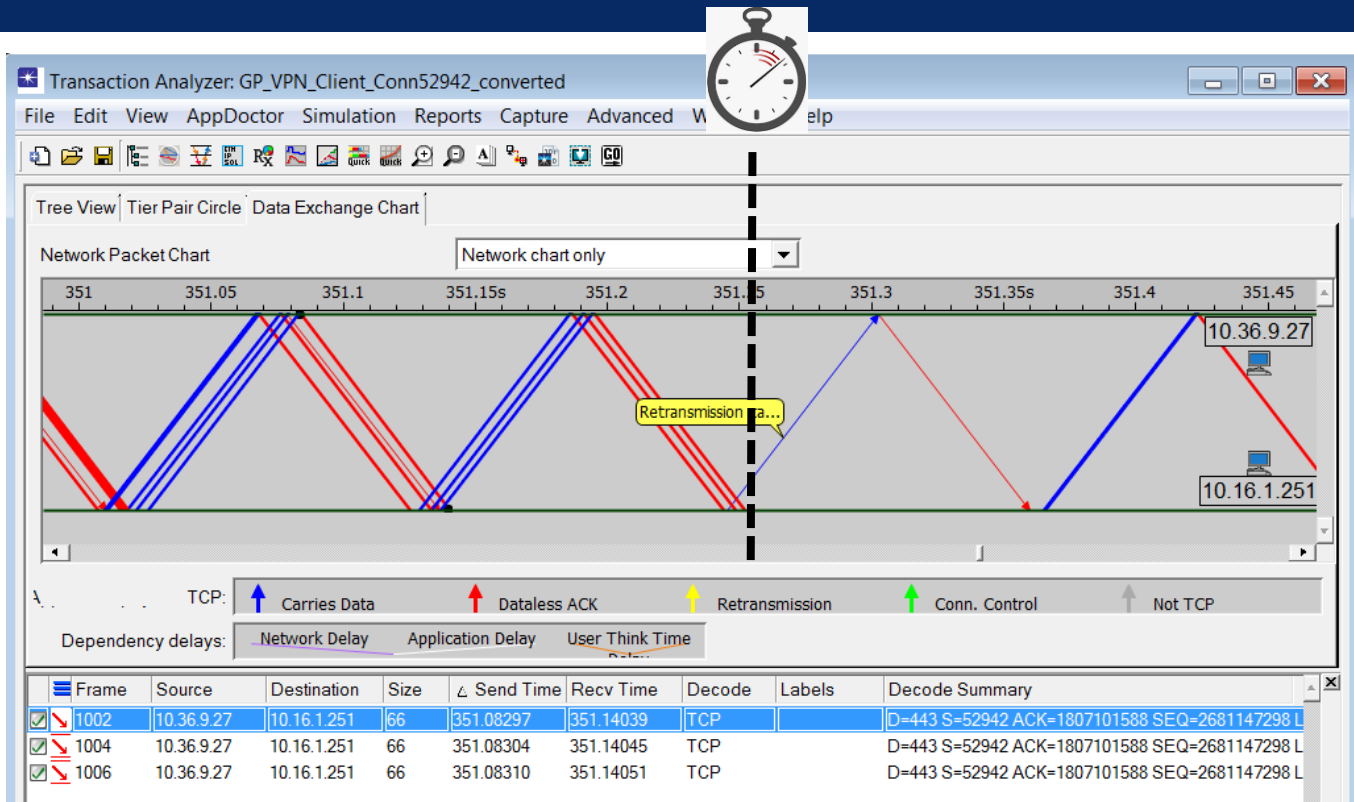


# Discuss state of each end point



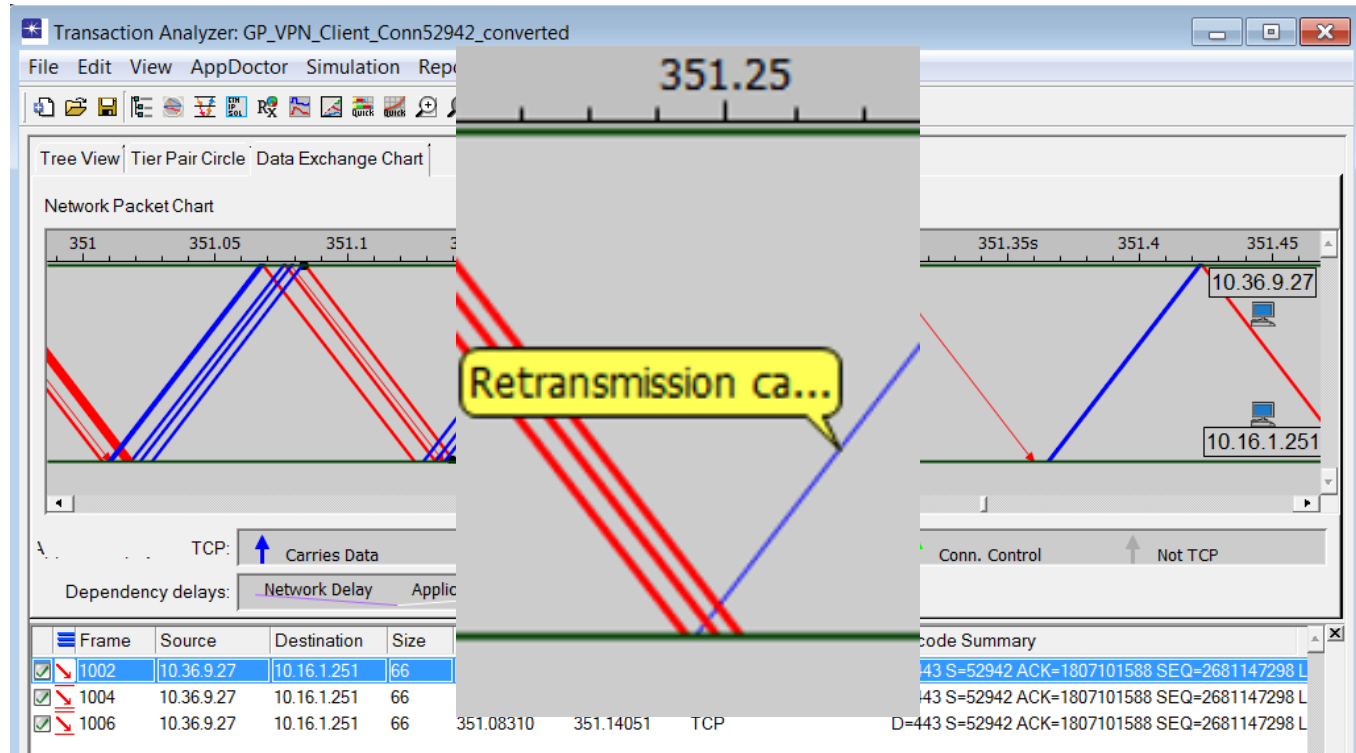


# Discuss state of each end point





# Discuss state of each end point





# Missing segment finally arrives



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	SACK LE	SACK RE	Info
1020	351.1912...	0.000015000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	537017	[TCP Dup ACK 1002#9] 52
1021	351.1939...	0.002666000	10.16.1.251	10.36.9.27	1292	537017	538309	64515			Ignored Unknown Record
1022	351.1939...	0.000029000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	538309	[TCP Dup ACK 1002#10] 5
1023	351.1947...	0.000741000	10.16.1.251	10.36.9.27	245	538309	538554	64515			Ignored Unknown Record
1024	351.1947...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	538554	[TCP Dup ACK 1002#11] 5
1025	351.3023...	0.107661000	10.16.1.251	10.36.9.27	1292	522835	524127	64515			[TCP Out-Of-Order] 443
1026	351.3024...	0.000041000	10.36.9.27	10.16.1.251	0	64515	64515	538554	524112	524127	52942 → 443 [ACK] Seq=6
1027	351.4223...	0.119896000	10.16.1.251	10.36.9.27	1292	538554	539846	64515			443 → 52942 [ACK] Seq=5

- Let's examine a few details...



# 107ms Time Delta



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	SACK LE	SACK RE	Info
1020	351.1912...	0.000015000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	537017	[TCP Dup ACK 1002#9] 52
1021	351.1939...	0.002666000	10.16.1.251	10.36.9.27	1292	537017	538309	64515			Ignored Unknown Record
1022	351.1939...	0.000029000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	538309	[TCP Dup ACK 1002#10] 5
1023	351.1947...	0.000741000	10.16.1.251	10.36.9.27	245	538309	538554	64515			Ignored Unknown Record
1024	351.1947...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	538554	[TCP Dup ACK 1002#11] 5
1025	351.3023...	0.107661000	10.16.1.251	10.36.9.27	1292	522835	524127	64515			[TCP Out-Of-Order] 443
1026	351.3024...	0.000041000	10.36.9.27	10.16.1.251	0	64515	64515	538554	524112	524127	52942 → 443 [ACK] Seq=6
1027	351.4223...	0.119896000	10.16.1.251	10.36.9.27	1292	538554	539846	64515			443 → 52942 [ACK] Seq=5

- Why 107ms from previous packet?





# Wireshark Feature Parade



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination
1009	351.1859...	0.000032000	10.36.9.27	10.16.3...
1010	351.1859...			
1011	351.1859...			
1012	351.1859...			
1013	351.1859...			
1014	351.1859...			
1015	351.1859...			
1016	351.1859...			
1017	351.1859...			
1018	351.1859...			
1019	351.1859...			
1020	351.1859...			
1021	351.1859...			
1022	351.1859...			
1023	351.1859...			

- Mark/Unmark Packet Ctrl+M
- Ignore/Unignore Packet Ctrl+D
- Set/Unset Time Reference Ctrl+T
- Time Shift... Ctrl+Shift+T
- Packet Comment... Ctrl+Alt+C
- Edit Resolved Name
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window







# With time ref set to DupACK #3



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	SACK LE	SACK RE	Info
1006	351.0830...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	527988	[TCP Dup ACK 1002#2]
1007	351.1858...	0.102797000	10.16.1.251	10.36.9.27	1292	527988	529280	64515			443 → 52942 [ACK] Seq
1008	*REF*	0.000032000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	529280	[TCP Dup ACK 1002#3]
1009	0.000077	0.000077000	10.16.1.251	10.36.9.27	1292	529280	530572	64515			443 → 52942 [ACK] Seq
1010	0.000124	0.000047000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	530572	[TCP Dup ACK 1002#4]
1011	0.000175	0.000051000	10.16.1.251	10.36.9.27	1292	530572	531864	64515			443 → 52942 [ACK] Seq
1012	0.000201	0.000026000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	531864	[TCP Dup ACK 1002#5]
1013	0.000515	0.000314000	10.16.1.251	10.36.9.27	1277	531864	533141	64515			443 → 52942 [PSH, ACK]
1014	0.000546	0.000031000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	533141	[TCP Dup ACK 1002#6]
1015	0.004442	0.003896000	10.16.1.251	10.36.9.27	1292	533141	534433	64515			443 → 52942 [ACK] Seq
1016	0.004478	0.000036000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	534433	[TCP Dup ACK 1002#7]
1017	0.005265	0.000787000	10.16.1.251	10.36.9.27	1292	534433	535725	64515			443 → 52942 [ACK] Seq
1018	0.005289	0.000024000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	535725	[TCP Dup ACK 1002#8]
1019	0.005343	0.000054000	10.16.1.251	10.36.9.27	1292	535725	537017	64515			Ignored Unknown Recor
1020	0.005358	0.000015000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	537017	[TCP Dup ACK 1002#9]
1021	0.008024	0.002666000	10.16.1.251	10.36.9.27	1292	537017	538309	64515			Ignored Unknown Recor
1022	0.008053	0.000029000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	538309	[TCP Dup ACK 1002#10]
1023	0.008794	0.000741000	10.16.1.251	10.36.9.27	245	538309	538554	64515			Ignored Unknown Recor
1024	0.008811	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	538554	[TCP Dup ACK 1002#11]
1025	0.116472	0.107661000	10.16.1.251	10.36.9.27	1292	522835	524127	64515			[TCP Out-Of-Order] 44



# Why “Out of Order”?



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	SACK LE	SACK RE	Info
1020	351.1912...	0.000015000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	537017	[TCP Dup ACK 1002#9] 52
1021	351.1939...	0.002666000	10.16.1.251	10.36.9.27	1292	537017	538309	64515			Ignored Unknown Record
1022	351.1939...	0.000029000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	538309	[TCP Dup ACK 1002#10] 5
1023	351.1947...	0.000741000	10.16.1.251	10.36.9.27	245	538309	538554	64515			Ignored Unknown Record
1024	351.1947...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	538554	[TCP Dup ACK 1002#11] 5
1025	351.3023...	0.107661000	10.16.1.251	10.36.9.27	1292	522835	524127	64515			[TCP Out-Of-Order] 443
1026	351.3024...	0.000041000	10.36.9.27	10.16.1.251	0	64515	64515	538554	524112	524127	52942 → 443 [ACK] Seq=6
1027	351.4223...	0.119896000	10.16.1.251	10.36.9.27	1292	538554	539846	64515			443 → 52942 [ACK] Seq=5

- Wouldn't “Retrans” or “Fast Retrans” be more accurate?



# Why ACK with SACK Fields?



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	SACK LE	SACK RE	Info
1020	351.1912...	0.000015000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	537017	[TCP Dup ACK 1002#9] 52
1021	351.1939...	0.002666000	10.16.1.251	10.36.9.27	1292	537017	538309	64515			Ignored Unknown Record
1022	351.1939...	0.000029000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	538309	[TCP Dup ACK 1002#10] 5
1023	351.1947...	0.000741000	10.16.1.251	10.36.9.27	245	538309	538554	64515			Ignored Unknown Record
1024	351.1947...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	538554	[TCP Dup ACK 1002#11] 5
1025	351.3023...	0.107661000	10.16.1.251	10.36.9.27	1292	522835	524127	64515			[TCP Out-Of-Order] 443
1026	351.3024...	0.000041000	10.36.9.27	10.16.1.251	0	64515	64515	538554	524112	524127	52942 → 443 [ACK] Seq=6
1027	351.4223...	0.119896000	10.16.1.251	10.36.9.27	1292	538554	539846	64515			443 → 52942 [ACK] Seq=5

- We're all caught up, nothing is missing...so why send SACK?
- “Oh, btw Sender – I received these 15 bytes of TCP stream unexpectedly. Just letting you know”



# Why 119ms delay here?



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

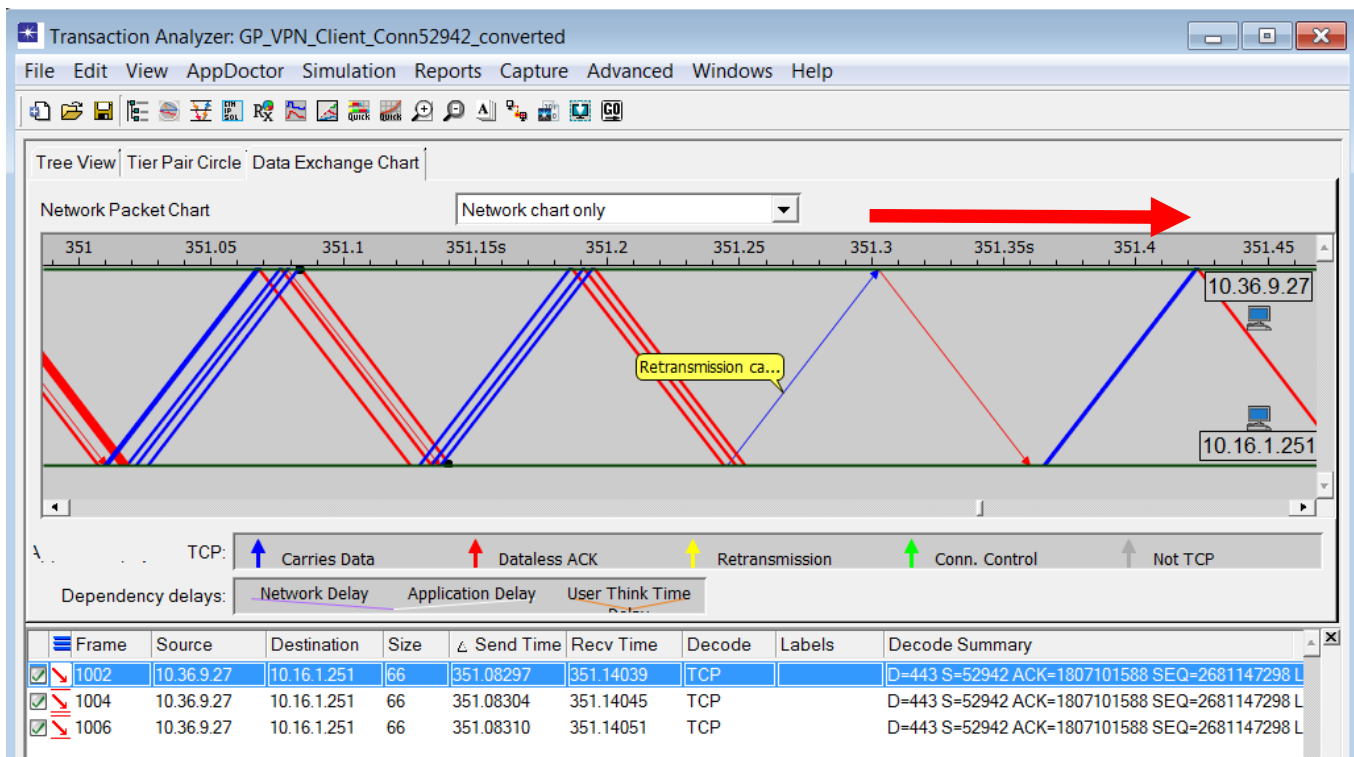
Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	SACK LE	SACK RE	Info
1020	351.1912...	0.000015000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	537017	[TCP Dup ACK 1002#9] 52
1021	351.1939...	0.002666000	10.16.1.251	10.36.9.27	1292	537017	538309	64515			Ignored Unknown Record
1022	351.1939...	0.000029000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	538309	[TCP Dup ACK 1002#10] 5
1023	351.1947...	0.000741000	10.16.1.251	10.36.9.27	245	538309	538554	64515			Ignored Unknown Record
1024	351.1947...	0.000017000	10.36.9.27	10.16.1.251	0	64515	64515	522835	524112	538554	[TCP Dup ACK 1002#11] 5
1025	351.3023...	0.107661000	10.16.1.251	10.36.9.27	1292	522835	524127	64515			[TCP Out-Of-Order] 443
1026	351.3024...	0.000041000	10.36.9.27	10.16.1.251	0	64515	64515	538554	524112	524127	52942 → 443 [ACK] Seq=6
1027	351.4223...	0.119896000	10.16.1.251	10.36.9.27	1292	538554	539846	64515			443 → 52942 [ACK] Seq=5

- What does this tell us about bytes in flight and the congestion window?



# Here's the delay – 1 x RTT





# Discussion



- Did you find that interesting?
- Anything new you've not seen before?
- Do you find visualization helpful?
- Other Comments?



# Summary & Wrap-Up



- Interpreting TCP behavior can be confusing and complicated, especially when there is “high” latency in the path
- Captures from both end points can be beneficial
- You need to split your brain into “server perspective” and “client perspective”



# Summary & Wrap-Up



- Wireshark features are extremely helpful, but can only take you so far
- Visualization can help you understand behavior and quickly interpret root cause
- Advanced analytics are icing on the cake...





# Thank You!



- For your participation
- Hope you found this session informative and insightful
- There's a bonus section to compare Bytes in flight, followed by Latency & Congestion that follow for your viewing enjoyment after the session

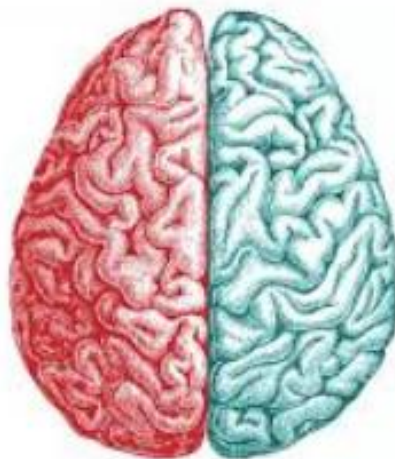
[illegible]



# Split Brain Comparisons



- Bytes in Flight





# Review



- What is the meaning of Bytes in Flight?
- How is this metric related to performance?
- BIF for Server and client captures look very different, let's compare a few packet exchanges



# Server Side



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
32	35.578512	0.000014000	10.16.1.251	10.36.9.27	0	1761	1761	2489		443 → 52942 [ACK]
33	35.580460	0.001948000	10.16.1.251	10.36.9.27	3876	1761	5637	2489	3876	443 → 52942 [ACK]
34	35.696769	0.116309000	10.36.9.27	10.16.1.251	0	2489	2489	4345		52942 → 443 [ACK]
35	35.696866	0.000097000	10.16.1.251	10.36.9.27	5168	5637	10805	2489	6460	Application Data [ACK]
36	35.816829	0.119963000	10.36.9.27	10.16.1.251	0	2489	2489	6929		52942 → 443 [ACK]
37	35.816866	0.000037000	10.16.1.251	10.36.9.27	5168	10805	15973	2489	9044	443 → 52942 [ACK]
38	35.819488	0.002622000	10.36.9.27	10.16.1.251	0	2489	2489	9513		52942 → 443 [ACK]
39	35.819519	0.000031000	10.16.1.251	10.36.9.27	3846	15973	19819	2489	10306	Application Data [ACK]
40	35.930853	0.111334000	10.36.9.27	10.16.1.251	0	2489	2489	12097		52942 → 443 [ACK]
41	35.931371	0.000518000	10.16.1.251	10.36.9.27	6460	19819	26279	2489	14182	443 → 52942 [ACK]
42	35.935034	0.003663000	10.36.9.27	10.16.1.251	0	2489	2489	14681		52942 → 443 [ACK]
43	35.935035	0.000001000	10.36.9.27	10.16.1.251	0	2489	2489	17265		52942 → 443 [ACK]
44	35.935065	0.000030000	10.16.1.251	10.36.9.27	2569	26279	28848	2489	11583	Application Data [ACK]
45	35.935107	0.000042000	10.36.9.27	10.16.1.251	0	2489	2489	15819		52942 → 443 [ACK]
46	35.935477	0.000370000	10.16.1.251	10.36.9.27	9029	28848	37877	2489	18058	Application Data [ACK]
47	36.044837	0.109360000	10.36.9.27	10.16.1.251	0	2489	2489	22403		52942 → 443 [ACK]



# Server Side



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
32	35.573512	0.000014000	10.16.1.251	10.36.9.27	0	1761	1761	2489		443 → 52942 [ACK]
33	35.580464	0.001948000	10.16.1.251	10.36.9.27	3876	1761	5637	2489	3876	443 → 52942 [ACK]
34	35.696769	0.116309000	10.36.9.27	10.16.1.251	0	2489	2489	4345		52942 → 443 [ACK]
35	35.696866	0.000097000	10.16.1.251	10.36.9.27	5168	5637	10805	2489	6460	Application Data [ACK]
36	35.816820	0.119963000	10.36.9.27	10.16.1.251	0	2489	2489	6929		52942 → 443 [ACK]
37	35.816866	0.000037000	10.16.1.251	10.36.9.27	5168	10805	15973	2489	9044	443 → 52942 [ACK]
38	35.819488	0.002622000	10.36.9.27	10.16.1.251	0	2489	2489	9513		52942 → 443 [ACK]
39	35.819519	0.000031000	10.16.1.251	10.36.9.27	3846	15973	19819	2489	10306	Application Data
40	35.930853	0.111334000	10.36.9.27	10.16.1.251	0	2489	2489	12097		52942 → 443 [ACK]
41	35.931371	0.000518000	10.16.1.251	10.36.9.27	6460	19819	26279	2489	14182	443 → 52942 [ACK]
42	35.935034	0.003663000	10.36.9.27	10.16.1.251	0	2489	2489	14681		52942 → 443 [ACK]
43	35.935035	0.000001000	10.36.9.27	10.16.1.251	0	2489	2489	17265		52942 → 443 [ACK]
44	35.935065	0.000030000	10.16.1.251	10.36.9.27	2569	26279	28848	2489	11583	Application Data
45	35.935107	0.000042000	10.36.9.27	10.16.1.251	0	2489	2489	19819		52942 → 443 [ACK]
46	35.935477	0.000370000	10.16.1.251	10.36.9.27	9029	28848	37877	2489	18058	Application Data
47	36.044837	0.109360000	10.36.9.27	10.16.1.251	0	2489	2489	22403		52942 → 443 [ACK]



# Client Side



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Express

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
32	35.696871	0.117113000	10.16.1.251	10.36.9.27	0	1761	1761	2489		443 → 52942 [ACK] Seq=176
33	35.700172	0.003301000	10.16.1.251	10.36.9.27	1292	1761	3053	2489	1292	443 → 52942 [ACK] Seq=176
34	35.700211	0.000039000	10.16.1.251	10.36.9.27	1292	3053	4345	2489	2584	443 → 52942 [ACK] Seq=305
35	35.700238	0.000027000	10.36.9.27	10.16.1.251	0	2489	2489	4345		52942 → 443 [ACK] Seq=248
36	35.700346	0.000108000	10.16.1.251	10.36.9.27	1292	4345	5637	2489	1292	443 → 52942 [ACK] Seq=434
37	35.818796	0.118450000	10.16.1.251	10.36.9.27	1292	5637	6929	2489	2584	443 → 52942 [ACK] Seq=563
38	35.818826	0.000030000	10.36.9.27	10.16.1.251	0	2489	2489	6929		52942 → 443 [ACK] Seq=248
39	35.818934	0.000108000	10.16.1.251	10.36.9.27	1292	6929	8221	2489	1292	443 → 52942 [ACK] Seq=692
40	35.819022	0.000088000	10.16.1.251	10.36.9.27	1292	8221	9513	2489	2584	443 → 52942 [ACK] Seq=822
41	35.819046	0.000024000	10.36.9.27	10.16.1.251	0	2489	2489	9513		52942 → 443 [ACK] Seq=248
42	35.819135	0.000089000	10.16.1.251	10.36.9.27	1292	9513	10805	2489	1292	Application Data [TCP seg
43	35.936054	0.116919000	10.16.1.251	10.36.9.27	1292	10805	12097	2489	2584	443 → 52942 [ACK] Seq=108
44	35.936080	0.000026000	10.36.9.27	10.16.1.251	0	2489	2489	12097		52942 → 443 [ACK] Seq=248



# Inferring Send Buffer Size



- Bytes In-flight can give you some insight into how the Send Buffer size might be limiting the Congestion Window
- How can we find the maximum observed Bytes In-Flight?





# Server Capture



Server\_side\_shifted\_Conn52942.pcap Command Prompt

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Express

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
1473	360.6191...	0.000341000	10.16.1.251	10.36.9.27	9029	1492007	1501036	64515	23471	Application Data
1451	360.3321...	0.000237000	10.16.1.251	10.36.9.27	5413	1454094	1459507	64515	23471	Application Data
1446	360.3274...	0.000002000	10.16.1.251	10.36.9.27	1277	1452817	1454094	64515	23471	Application Data
1416	360.0253...	0.000546000	10.16.1.251	10.36.9.27	9029	1412565	1421594	64515	23471	Application Data
1445	360.3274...	0.000003000	10.16.1.251	10.36.9.27	1292	1451525	1452817	64515	22194	443 → 52942 [ACK] Seq=1451525 Ack=6451
1407	359.8663...	0.000353000	10.16.1.251	10.36.9.27	7752	1398123	1405875	64515	22194	443 → 52942 [ACK] Seq=1398123 Ack=6451
1504	361.2166...	0.000699000	10.16.1.251	10.36.9.27	5413	1547418	1552831	64515	22179	Application Data
1397	359.8611...	0.000341000	10.16.1.251	10.36.9.27	5168	1383681	1388849	64515	21934	443 → 52942 [ACK] Seq=1383681 Ack=6451
1564	362.0364...	0.000019000	10.16.1.251	10.36.9.27	49	1599724	1599773	64515	20902	[TCP Out-Of-Order] 443 → 52942 [PSH, A
1563	362.0364...	0.000029000	10.16.1.251	10.36.9.27	1292	1598432	1599724	64515	20902	[TCP Out-Of-Order] 443 → 52942 [ACK] S
1560	361.9970...	0.000014000	10.16.1.251	10.36.9.27	1292	1597140	1598432	64515	20902	[TCP Out-Of-Order] 443 → 52942 [ACK] S
1558	361.9963...	0.000021000	10.16.1.251	10.36.9.27	196	1596944	1597140	64515	20902	[TCP Out-Of-Order] 443 → 52942 [ACK] S
1556	361.9963...	0.000028000	10.16.1.251	10.36.9.27	1292	1595652	1596944	64515	20902	[TCP Fast Retransmission] , Ignored Un
1554	361.9962...	0.000020000	10.16.1.251	10.36.9.27	1292	1615262	1616554	64515	20902	443 → 52942 [ACK] Seq=1615262 Ack=6451
1444	360.3274...	0.000003000	10.16.1.251	10.36.9.27	1292	1450233	1451525	64515	20902	443 → 52942 [ACK] Seq=1450233 Ack=6451
1388	359.7224...	0.000551000	10.16.1.251	10.36.9.27	7752	1365623	1373375	64515	20902	443 → 52942 [ACK] Seq=1365623 Ack=6451
822	352.6430...	0.000520000	10.16.1.251	10.36.9.27	7752	688400	686161	64515	20902	443 → 52942 [ACK] Seq=688400 Ack=64515



# Wait, something was odd...



- Did you notice anything odd in the last screen?
- Let's look again...



# Server Capture – Out of order?



Server\_side\_shifted\_Conn52942.pcap Command Prompt

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Express

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
1473	360.6191...	0.000341000	10.16.1.251	10.36.9.27	9029	1492007	1501036	64515	23471	Application Data
1451	360.3321...	0.000237000	10.16.1.251	10.36.9.27	5413	1454094	1459507	64515	23471	Application Data
1446	360.3274...	0.000002000	10.16.1.251	10.36.9.27	1277	1452817	1454094	64515	23471	Application Data
1416	360.0253...	0.000546000	10.16.1.251	10.36.9.27	9029	1412565	1421594	64515	23471	Application Data
1445	360.3274...	0.000003000	10.16.1.251	10.36.9.27	1292	1451525	1452817	64515	22194	443 → 52942 [ACK] Seq=1451525 Ack=64515
1407	359.8663...	0.000353000	10.16.1.251	10.36.9.27	7752	1398123	1405875	64515	22194	443 → 52942 [ACK] Seq=1398123 Ack=64515
1504	361.2166...	0.000699000	10.16.1.251	10.36.9.27	5413	1547418	1552831	64515	22179	Application Data
1397	359.8611...	0.000341000	10.16.1.251	10.36.9.27	5168	1383681	1388849	64515	21934	443 → 52942 [ACK] Seq=1383681 Ack=64515
1564	362.0364...	0.000019000	10.16.1.251	10.36.9.27	49	1599724	1599773	64515	20902	[TCP Out-Of-Order] 443 → 52942 [PSH, A
1563	362.0364...	0.000029000	10.16.1.251	10.36.9.27	1292	1598432	1599724	64515	20902	[TCP Out-Of-Order] 443 → 52942 [ACK] S
1560	361.9970...	0.000014000	10.16.1.251	10.36.9.27	1292	1597140	1598432	64515	20902	[TCP Out-Of-Order] 443 → 52942 [ACK] S
1558	361.9963...	0.000021000	10.16.1.251	10.36.9.27	196	1596944	1597140	64515	20902	[TCP Out-Of-Order] 443 → 52942 [ACK] S
1556	361.9963...	0.000028000	10.16.1.251	10.36.9.27	1292	1595652	1596944	64515	20902	[TCP Fast Retransmission] , Ignored Un
1554	361.9962...	0.000020000	10.16.1.251	10.36.9.27	1292	1615262	1616554	64515	20902	443 → 52942 [ACK] Seq=1615262 Ack=64515
1444	360.3274...	0.000003000								→ 52942 [ACK] Seq=1450233 Ack=64515
1388	359.7224...	0.000551000								→ 52942 [ACK] Seq=1365623 Ack=64515
822	352.6430...	0.000520000								→ 52942 [ACK] Seq=689400 Ack=64515

This will be your homework for later



# BIF - Client Side



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta	Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
2404	362.0845...	0.000291000		10.16.1.251	10.36.9.27	1292	1595652	1596944	64515	20902	[TCP Fast Retransmission]
2402	362.0842...	0.000593000		10.16.1.251	10.36.9.27	196	1596944	1597140	64515	19610	[TCP Out-Of-Order] 443
2406	362.0847...	0.000158000		10.16.1.251	10.36.9.27	1292	1597140	1598432	64515	19414	[TCP Out-Of-Order] 443
2408	362.1242...	0.039484000		10.16.1.251	10.36.9.27	1292	1598432	1599724	64515	18122	[TCP Out-Of-Order] 443
2410	362.1247...	0.000188000		10.16.1.251	10.36.9.27	49	1599724	1599773	64515	16830	[TCP Out-Of-Order] 443
2400	362.0835...	0.007057000		10.16.1.251	10.36.9.27	1292	1615262	1616554	64515	16781	443 → 52942 [ACK] Seq=
1841	357.6631...	0.066508000		10.16.1.251	10.36.9.27	1292	1159816	1161108	64515	16567	[TCP Out-Of-Order] 443
2756	365.3851...	0.045392000		10.16.1.251	10.36.9.27	1292	1866618	1867910	64515	15719	[TCP Out-Of-Order] 443
2634	364.3405...	0.028776000		10.16.1.251	10.36.9.27	1292	1773294	1774586	64515	15719	[TCP Out-Of-Order] 443
2322	361.3096...	0.004394000		10.16.1.251	10.36.9.27	1292	1537112	1538404	64515	15719	[TCP Fast Retransmission]
1662	356.3820...	0.003810000		10.16.1.251	10.36.9.27	1292	1018990	1020282	64515	15719	[TCP Fast Retransmission]
1357	353.8360...	0.000191000		10.16.1.251	10.36.9.27	1292	781912	783204	64515	15719	[TCP Fast Retransmission]
1233	352.8511...	0.052475000		10.16.1.251	10.36.9.27	1292	687132	688424	64515	15719	[TCP Out-Of-Order] 443
1025	351.3023...	0.107661000		10.16.1.251	10.36.9.27	1292	522835	524127	64515	15719	[TCP Out-Of-Order] 443
2398	362.0764...	0.041601000		10.16.1.251	10.36.9.27	1292	1613970	1615262	64515	15489	443 → 52942 [ACK] Seq=
1839	357.5965...	0.000175000		10.16.1.251	10.36.9.27	1292	1173998	1175290	64515	15290	[TCP Out-Of-Order] 443
2754	365.2207...	0.000068000		10.16.1.251	10.36.9.27	220	1882107	1882227	64515	14442	Application Data



# In-Flight & OOS / Loss



- Let's look at how Wireshark calculates Bytes in-flight when there is packet loss or OOS



# Client – Receive #1275 OOS



GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
1273	353.2099...	0.000053000	10.36.9.27	10.16.1.251	0	64515	64515	735366		52942 → 443 [ACK] Seq=6451
1274	353.2100...	0.000096000	10.16.1.251	10.36.9.27	1292	735366	736658	64515	1292	443 → 52942 [PSH, ACK] Seq
1275	353.3179...	0.107972000	10.16.1.251	10.36.9.27	1292	737950	739242	64515		[TCP Previous segment not
1276	353.3180...	0.000067000	10.36.9.27	10.16.1.251	0	64515	64515	736658		52942 → 443 [ACK] Seq=6451
1277	353.3189...	0.000875000	10.16.1.251	10.36.9.27	1292	736658	737950	64515	2584	[TCP Out-Of-Order] 443 → 5
1278	353.3190...	0.000081000	10.36.9.27	10.16.1.251	0	64515	64515	739242		52942 → 443 [ACK] Seq=6451

- BIF did not increment for #1275



# Comparison Storyboard



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
871	353.1165...	0.001059000	10.36.9.27	10.16.1.251	0	64515	64515	723493		52942 → 443 [ACK] Seq=6451
872	353.1165...	0.000019000	10.16.1.251	10.36.9.27	3876	732782	736658	64515	13165	Application Data [TCP segm
873	353.2298...	0.113255000	10.36.9.27	10.16.1.251	0	64515	64515	726077		52942 → 443 [ACK] Seq=6451
874	353.2298...	0.000047000	10.16.1.251	10.36.9.27	2584	736658	739242	64515	13165	443 → 52942 [ACK] Seq=7366
875	353.2352...	0.005412000	10.36.9.27	10.16.1.251	0	64515	64515	727614		52942 → 443 [ACK] Seq=6451
876	353.2353...	0.000042000	10.16.1.251	10.36.9.27	1292	739242	740534	64515	12920	443 → 52942 [ACK] Seq=7392
877	353.2356...	0.000301000	10.36.9.27	10.16.1.251	0	64515	64515	730198		52942 → 443 [ACK] Seq=6451

GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
1270	353.2085...	0.000037000	10.36.9.27	10.16.1.251	0	64515	64515	732782		52942 → 443 [ACK] Seq=645
1271	353.2090...	0.000519000	10.16.1.251	10.36.9.27	1292	732782	734074	64515	1292	443 → 52942 [ACK] Seq=732
1272	353.2098...	0.000827000	10.16.1.251	10.36.9.27	1292	734074	735366	64515	2584	Application Data [TCP seg
1273	353.2099...	0.000053000	10.36.9.27	10.16.1.251	0	64515	64515	735366		52942 → 443 [ACK] Seq=645
1274	353.2100...	0.000096000	10.16.1.251	10.36.9.27	1292	735366	736658	64515	1292	443 → 52942 [PSH, ACK] Se
1275	353.3179...	0.107972000	10.16.1.251	10.36.9.27	1292	737950	739242	64515		[TCP Previous segment not
1276	353.3180...	0.000067000	10.36.9.27	10.16.1.251	0	64515	64515	736658		52942 → 443 [ACK] Seq=645
1277	353.3189...	0.000875000	10.16.1.251	10.36.9.27	1292	736658	737950	64515	2584	[TCP Out-Of-Order] 443 →
1278	353.3190...	0.000081000	10.36.9.27	10.16.1.251	0	64515	64515	739242		52942 → 443 [ACK] Seq=645



# Comparison Storyboard



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
871	353.1165...	0.001059000	10.36.9.27	10.16.1.251	0	64515	64515	723493		52942 → 443 [ACK] Seq=6451
872	353.1165...	0.000019000	10.16.1.251	10.36.9.27	3876	732782	736658	64515	13165	Application Data [TCP segm
873	353.2298...	0.113255000	10.36.9.27	10.16.1.251	0	64515	64515	726077		52942 → 443 [ACK] Seq=6451
874	353.2298...	0.000047000	10.16.1.251	10.36.9.27	2584	736658	739242	64515	13165	443 → 52942 [ACK] Seq=7366
875	353.2352...	0.005412000	10.36.9.27	10.16.1.251	0	64515	64515	727614		52942 → 443 [ACK] Seq=6451
876	353.2353...	0.000042000	10.16.1.251	10.36.9.27	1292	739242	740534	64515	12920	443 → 52942 [ACK] Seq=7392
877	353.2356...	0.000301000	10.36.9.27	10.16.1.251	0	64515	64515	730198		52942 → 443 [ACK] Seq=6451

GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
1270	353.2085...	0.000037000	10.36.9.27	10.16.1.251	0	64515	64515	732782		52942 → 443 [ACK] Seq=645
1271	353.2090...	0.000519000	10.16.1.251	10.36.9.27	1292	732782	734074	64515	1292	443 → 52942 [ACK] Seq=732
1272	353.2098...	0.000827000	10.16.1.251	10.36.9.27	1292	734074	735366	64515	2584	Application Data [TCP seg
1273	353.2099...	0.000053000	10.36.9.27	10.16.1.251	0	64515	64515	735366		52942 → 443 [ACK] Seq=645
1274	353.2100...	0.000096000	10.16.1.251	10.36.9.27	1292	735366	736658	64515	1292	443 → 52942 [PSH, ACK] Se
1275	353.3179...	0.107972000	10.16.1.251	10.36.9.27	1292	737950	739242	64515		[TCP Previous segment not
1276	353.3180...	0.000067000	10.36.9.27	10.16.1.251	0	64515	64515	736658		52942 → 443 [ACK] Seq=645
1277	353.3189...	0.000875000	10.16.1.251	10.36.9.27	1292	736658	737950	64515	2584	[TCP Out-Of-Order] 443 →
1278	353.3190...	0.000081000	10.36.9.27	10.16.1.251	0	64515	64515	739242		52942 → 443 [ACK] Seq=645





# Comparison Storyboard



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
871	353.1165...	0.001059000	10.36.9.27	10.16.1.251	0	64515	64515	723493		52942 → 443 [ACK] Seq=6451
872	353.1165...	0.000019000	10.16.1.251	10.36.9.27	3876	732782	736658	64515	13165	Application Data [TCP segm
873	353.2298...	0.113255000	10.36.9.27	10.16.1.251	0	64515	64515	726077		52942 → 443 [ACK] Seq=6451
874	353.2298...	0.000047000	10.16.1.251	10.36.9.27	2584	736658	739242	64515	13165	443 → 52942 [ACK] Seq=7366
875	353.2352...	0.005412000	10.36.9.27	10.16.1.251	0	64515	64515	727614		52942 → 443 [ACK] Seq=6451
876	353.2353...	0.000042000	10.16.1.251	10.36.9.27	1292	739242	740534	64515	12920	443 → 52942 [ACK] Seq=7392
877	353.2356...	0.000301000	10.36.9.27	10.16.1.251	0	64515	64515	730198		52942 → 443 [ACK] Seq=6451

GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
1270	353.2085...	0.000037000	10.36.9.27	10.16.1.251	0	64515	64515	732782		52942 → 443 [ACK] Seq=645
1271	353.2090...	0.000519000	10.16.1.251	10.36.9.27	1292	732782	734074	64515	1292	443 → 52942 [ACK] Seq=732
1272	353.2098...	0.000827000	10.16.1.251	10.36.9.27	1292	734074	735366	64515	2584	Application Data [TCP seg
1273	353.2099...	0.000053000	10.36.9.27	10.16.1.251	0	64515	64515	735366		52942 → 443 [ACK] Seq=645
1274	353.2100...	0.000096000	10.16.1.251	10.36.9.27	1292	735366	736658	64515	1292	443 → 52942 [PSH, ACK] Se
1275	353.3179...	0.107972000	10.16.1.251	10.36.9.27	1292	737950	739242	64515		[TCP Previous segment not
1276	353.3180...	0.000067000	10.36.9.27	10.16.1.251	0	64515	64515	736658		52942 → 443 [ACK] Seq=645
1277	353.3189...	0.000875000	10.16.1.251	10.36.9.27	1292	736658	737950	64515	2584	[TCP Out-Of-Order] 443 →
1278	353.3190...	0.000081000	10.36.9.27	10.16.1.251	0	64515	64515	739242		52942 → 443 [ACK] Seq=645



# Comparison Storyboard



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
871	353.1165...	0.001059000	10.36.9.27	10.16.1.251	0	64515	64515	723493		52942 → 443 [ACK] Seq=6451
872	353.1165...	0.000019000	10.16.1.251	10.36.9.27	3876	732782	736658	64515	13165	Application Data [TCP segm
873	353.2298...	0.113255000	10.36.9.27	10.16.1.251	0	64515	64515	726077		52942 → 443 [ACK] Seq=6451
874	353.2298...	0.000047000	10.16.1.251	10.36.9.27	2584	736658	739242	64515	13165	443 → 52942 [ACK] Seq=7366
875	353.2352...	0.005412000	10.36.9.27	10.16.1.251	0	64515	64515	727614		52942 → 443 [ACK] Seq=6451
876	353.2353...	0.000042000	10.16.1.251	10.36.9.27	1292	739242	740534	64515	12920	443 → 52942 [ACK] Seq=7392
877	353.2356...	0.000301000	10.36.9.27	10.16.1.251	0	64515	64515	730198		52942 → 443 [ACK] Seq=6451

GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
1270	353.2085...	0.000037000	10.36.9.27	10.16.1.251	0	64515	64515	732782		52942 → 443 [ACK] Seq=645
1271	353.2090...	0.000519000	10.16.1.251	10.36.9.27	1292	732782	734074	64515	1292	443 → 52942 [ACK] Seq=732
1272	353.2098...	0.000827000	10.16.1.251	10.36.9.27	1292	734074	735366	64515	2584	Application Data [TCP seg
1273	353.2099...	0.000053000	10.36.9.27	10.16.1.251	0	64515	64515	735366		52942 → 443 [ACK] Seq=645
1274	353.2100...	0.000096000	10.16.1.251	10.36.9.27	1292	735366	736658	64515	1292	443 → 52942 [PSH, ACK] Se
1275	353.3179...	0.107972000	10.16.1.251	10.36.9.27	1292	737950	739242	64515		[TCP Previous segment not
1276	353.3180...	0.000067000	10.36.9.27	10.16.1.251	0	64515	64515	736658		52942 → 443 [ACK] Seq=645
1277	353.3189...	0.000875000	10.16.1.251	10.36.9.27	1292	736658	737950	64515	2584	[TCP Out-Of-Order] 443 →
1278	353.3190...	0.000081000	10.36.9.27	10.16.1.251	0	64515	64515	739242		52942 → 443 [ACK] Seq=645



# Comparison Storyboard



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
871	353.1165...	0.001059000	10.36.9.27	10.16.1.251	0	64515	64515	723493		52942 → 443 [ACK] Seq=64515
872	353.1165...	0.000019000	10.16.1.251	10.36.9.27	3876	732782	736658	64515	13165	Application Data [TCP segment 1 of 1] Seq=732782
873	353.2298...	0.113255000	10.36.9.27	10.16.1.251	0	64515	64515	726077		52942 → 443 [ACK] Seq=64515
874	353.2298...	0.000047000	10.16.1.251	10.36.9.27	2584	736658	739242	64515	13165	443 → 52942 [ACK] Seq=736658
875	353.2352...	0.005412000	10.36.9.27	10.16.1.251	0	64515	64515	727614		52942 → 443 [ACK] Seq=64515
876	353.2353...	0.000042000	10.16.1.251	10.36.9.27	1292	739242	740534	64515	12920	443 → 52942 [ACK] Seq=739242
877	353.2356...	0.000301000	10.36.9.27	10.16.1.251	0	64515	64515	730198		52942 → 443 [ACK] Seq=64515

GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
1270	353.2085...	0.000037000	10.36.9.27	10.16.1.251	0	64515	64515	732782		52942 → 443 [ACK] Seq=64515
1271	353.2090...	0.000519000	10.16.1.251	10.36.9.27	1292	732782	734074	64515	1292	443 → 52942 [ACK] Seq=732782
1272	353.2098...	0.000827000	10.16.1.251	10.36.9.27	1292	734074	735366	64515	2584	Application Data [TCP segment 1 of 1] Seq=734074
1273	353.2099...	0.000053000	10.36.9.27	10.16.1.251	0	64515	64515	735366		52942 → 443 [ACK] Seq=64515
1274	353.2100...	0.000096000	10.16.1.251	10.36.9.27	1292	735366	736658	64515	1292	443 → 52942 [PSH, ACK] Seq=735366
1275	353.3179...	0.107972000	10.16.1.251	10.36.9.27	1292	737950	739242	64515		[TCP Previous segment not received] Seq=737950
1276	353.3180...	0.000067000	10.36.9.27	10.16.1.251	0	64515	64515	736658		52942 → 443 [ACK] Seq=64515
1277	353.3189...	0.000875000	10.16.1.251	10.36.9.27	1292	736658	737950	64515	2584	[TCP Out-Of-Order] 443 → 52942 [ACK] Seq=736658
1278	353.3190...	0.000081000	10.36.9.27	10.16.1.251	0	64515	64515	739242		52942 → 443 [ACK] Seq=64515



# Comparison Storyboard



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
871	353.1165...	0.001059000	10.36.9.27	10.16.1.251	0	64515	64515	723493		52942 → 443 [ACK] Seq=64515
872	353.1165...	0.000019000	10.16.1.251	10.36.9.27	3876	732782	736658	64515	13165	Application Data [TCP segment 1 of 1] Seq=732782
873	353.2298...	0.113255000	10.36.9.27	10.16.1.251	0	64515	64515	726077		52942 → 443 [ACK] Seq=64515
874	353.2298...	0.000047000	10.16.1.251	10.36.9.27	2584	736658	739242	64515	13165	443 → 52942 [ACK] Seq=736658
875	353.2352...	0.005412000	10.36.9.27	10.16.1.251	0	64515	64515	727614		52942 → 443 [ACK] Seq=64515
876	353.2353...	0.000042000	10.16.1.251	10.36.9.27	1292	739242	740534	64515	12920	443 → 52942 [ACK] Seq=739242
877	353.2356...	0.000301000	10.36.9.27	10.16.1.251	0	64515	64515	730198		52942 → 443 [ACK] Seq=64515

GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
1270	353.2085...	0.000037000	10.36.9.27	10.16.1.251	0	64515	64515	732782		52942 → 443 [ACK] Seq=64515
1271	353.2090...	0.000519000	10.16.1.251	10.36.9.27	1292	732782	734074	64515	1292	443 → 52942 [ACK] Seq=732782
1272	353.2098...	0.000827000	10.16.1.251	10.36.9.27	1292	734074	735366	64515	2584	Application Data [TCP segment 1 of 1] Seq=734074
1273	353.2099...	0.000053000	10.36.9.27	10.16.1.251	0	64515	64515	735366		52942 → 443 [ACK] Seq=64515
1274	353.2100...	0.000096000	10.16.1.251	10.36.9.27	1292	735366	736658	64515	1292	443 → 52942 [PSH, ACK] Seq=735366
1275	353.3179...	0.107972000	10.16.1.251	10.36.9.27	1292	737950	739242	64515		[TCP Previous segment not received] Seq=737950
1276	353.3180...	0.000067000	10.36.9.27	10.16.1.251	0	64515	64515	736658		52942 → 443 [ACK] Seq=64515
1277	353.3189...	0.000875000	10.16.1.251	10.36.9.27	1292	736658	737950	64515	2584	[TCP Out-Of-Order] 443 → 52942 [ACK] Seq=736658
1278	353.3190...	0.000081000	10.36.9.27	10.16.1.251	0	64515	64515	739242		52942 → 443 [ACK] Seq=64515



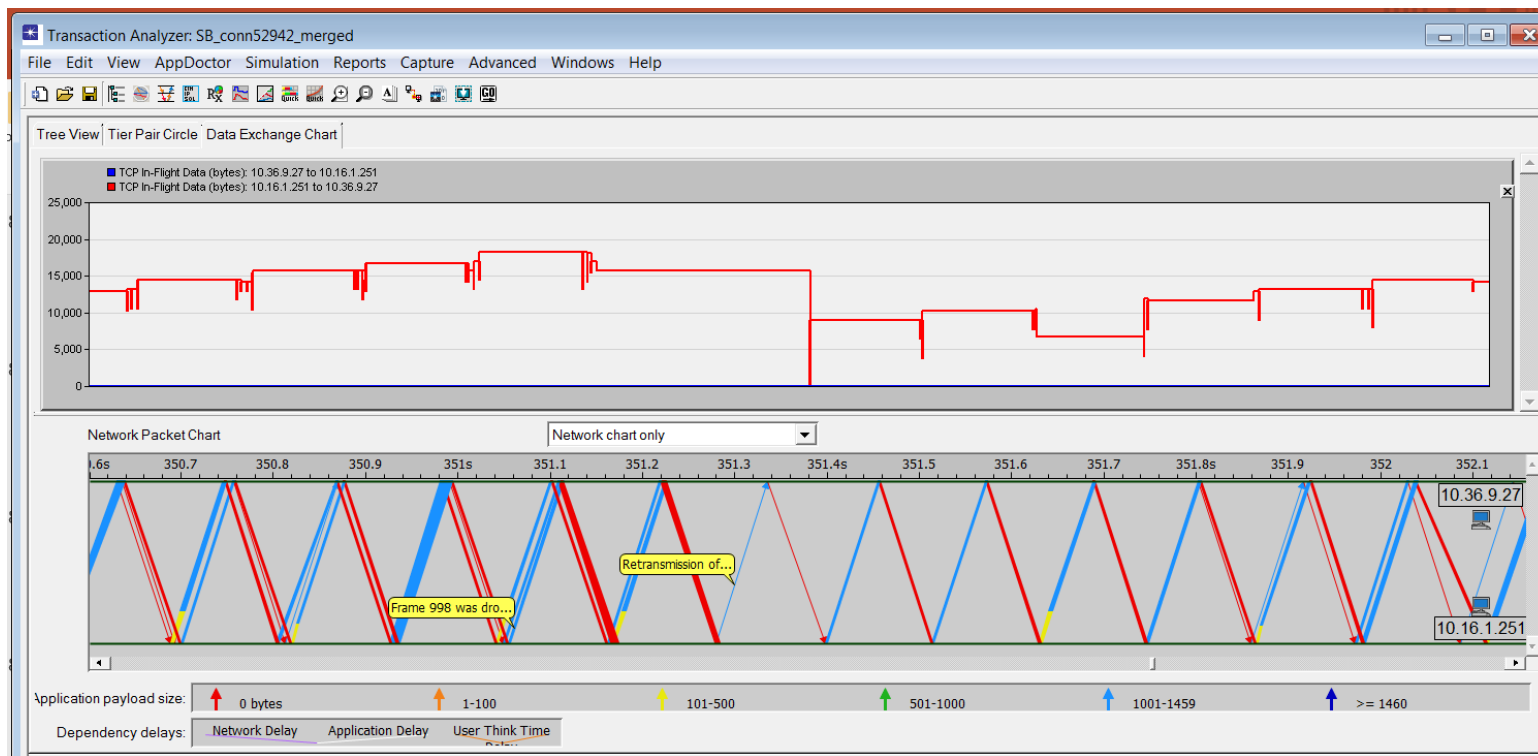
# We need to visualize this...



- Now that we've seen how Wireshark counts bytes in flight...
- ...and some of the challenges of side by side comparisons...
- ...let's look at how we can gain better insight from visualization

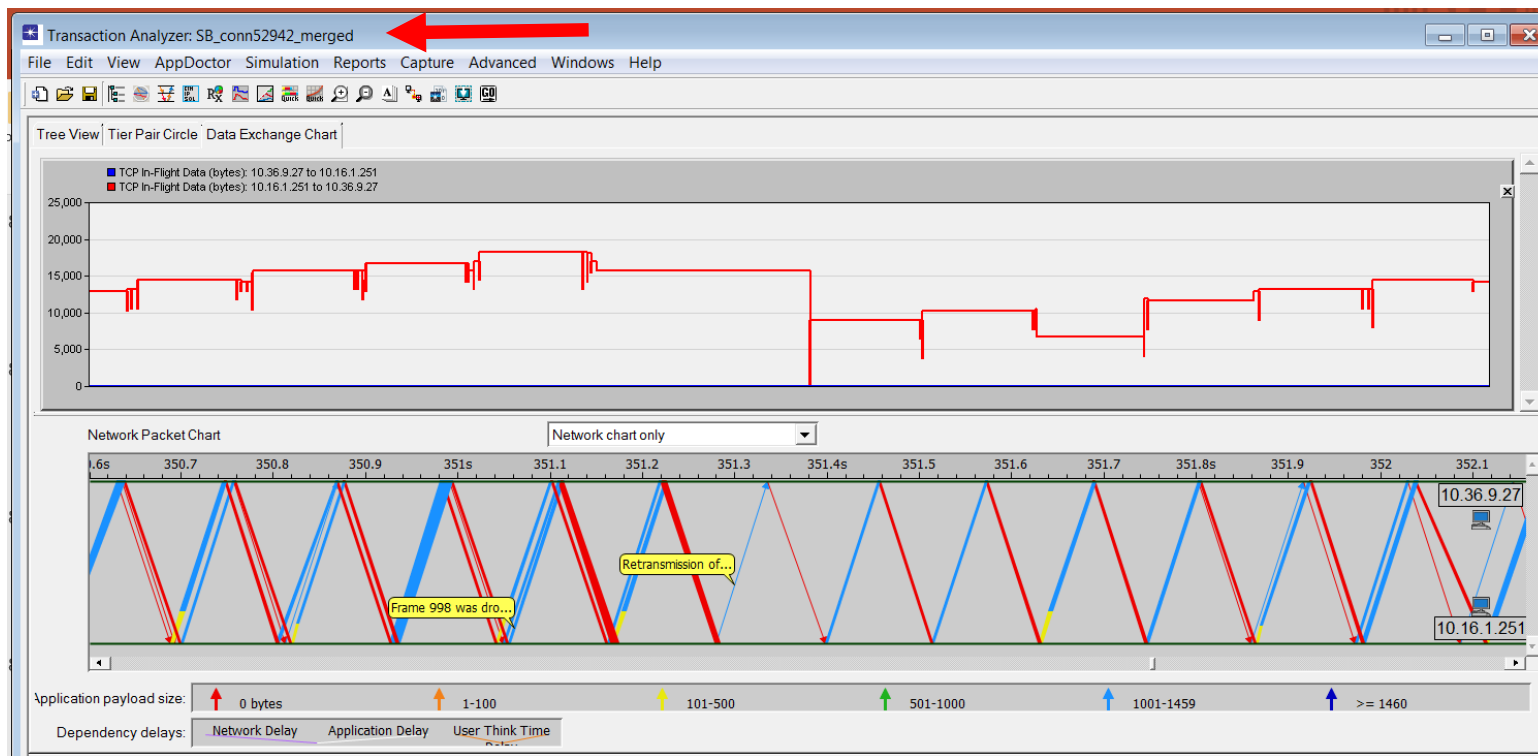


# Packet Exchange with BIF Overlay



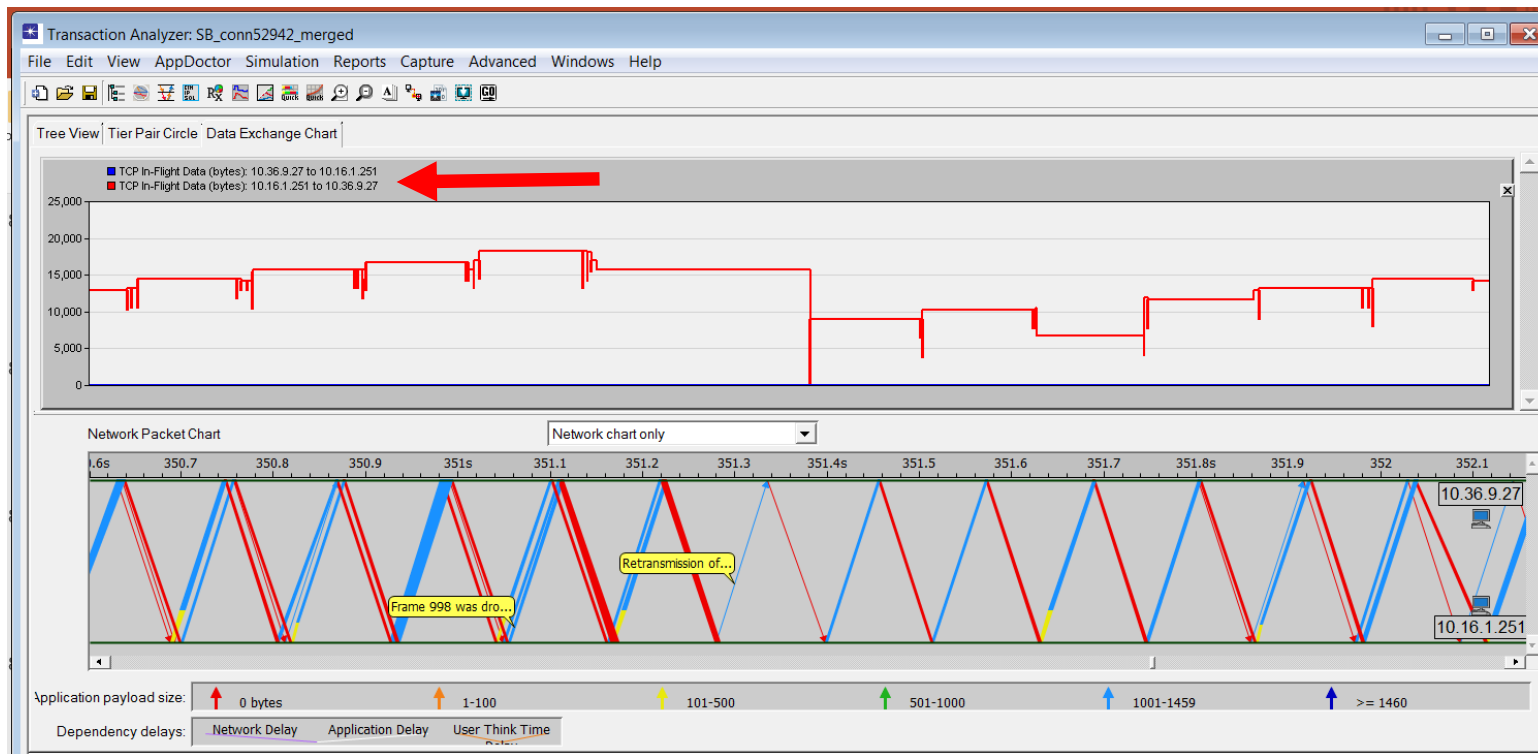


# Quick Orientation





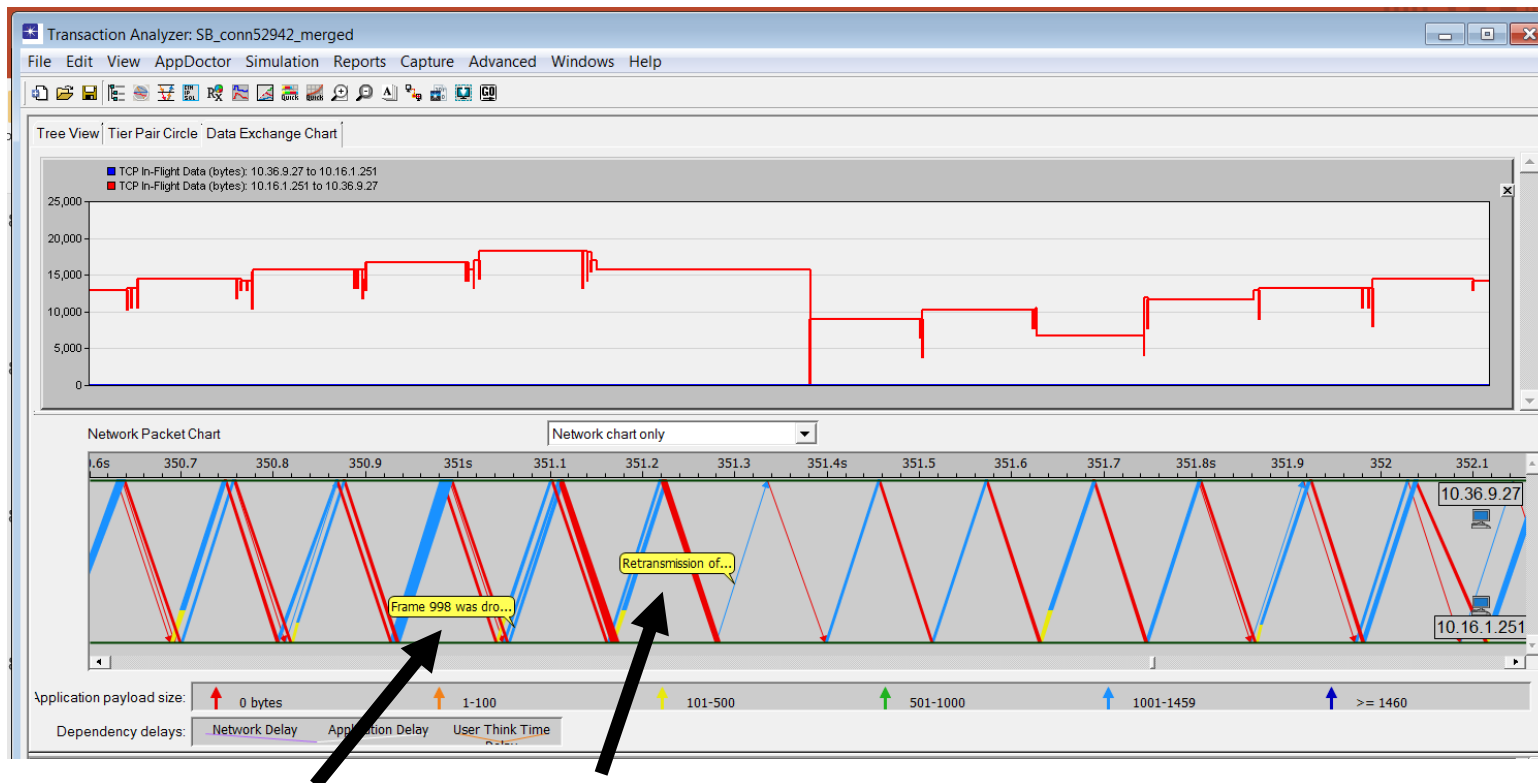
# In-flight Bytes





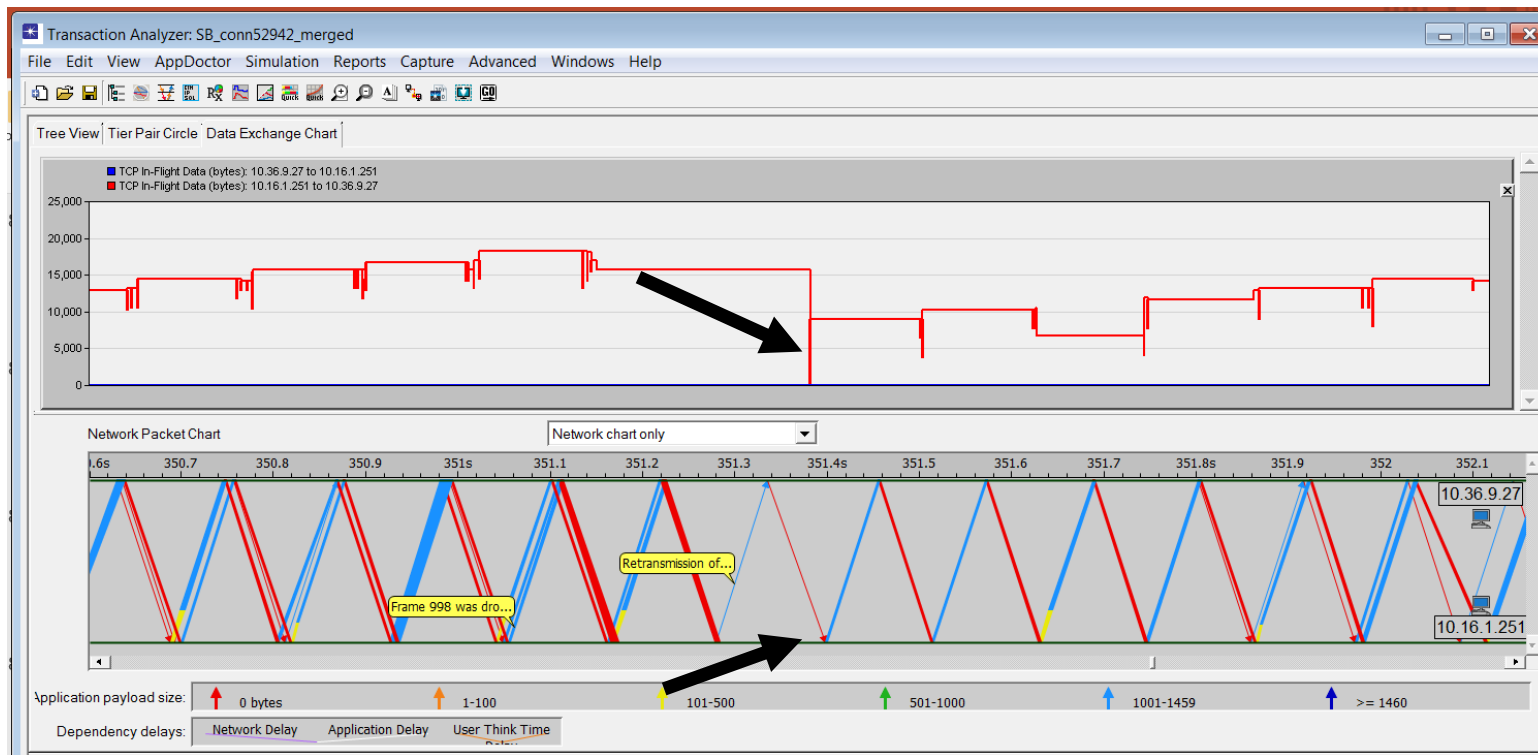


# Symptom Pop-up Labels



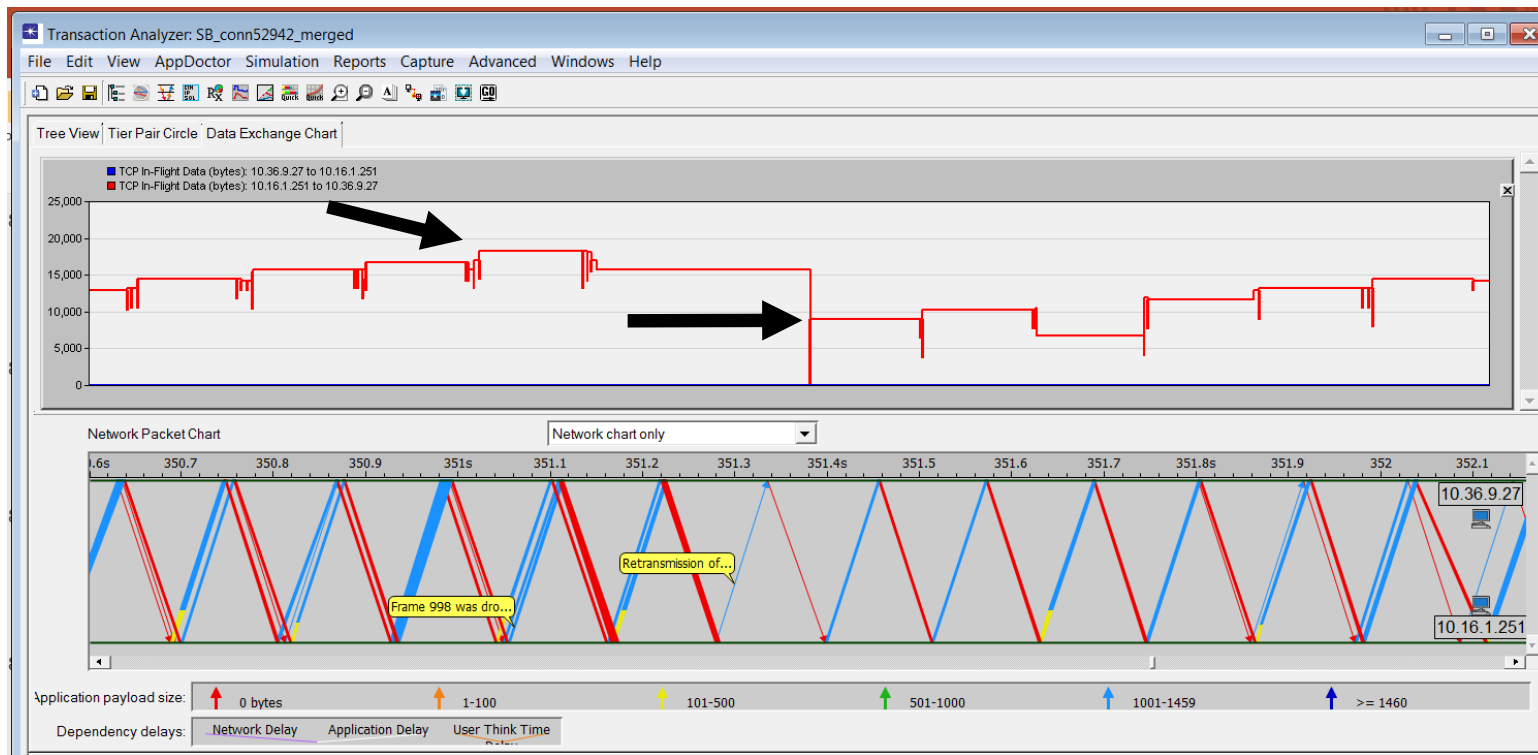


# Why In-flight drops to 0?



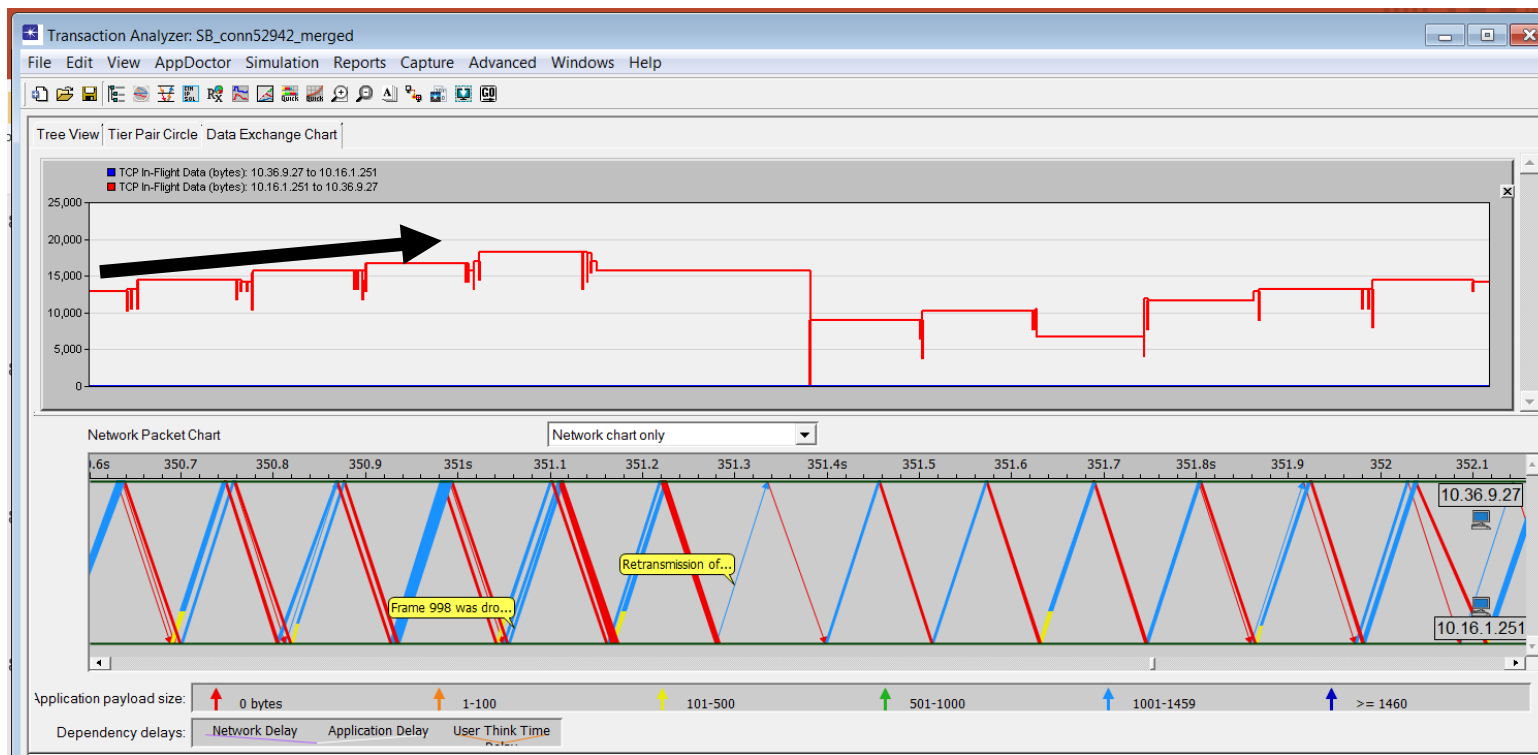


# What does this delta tell us?



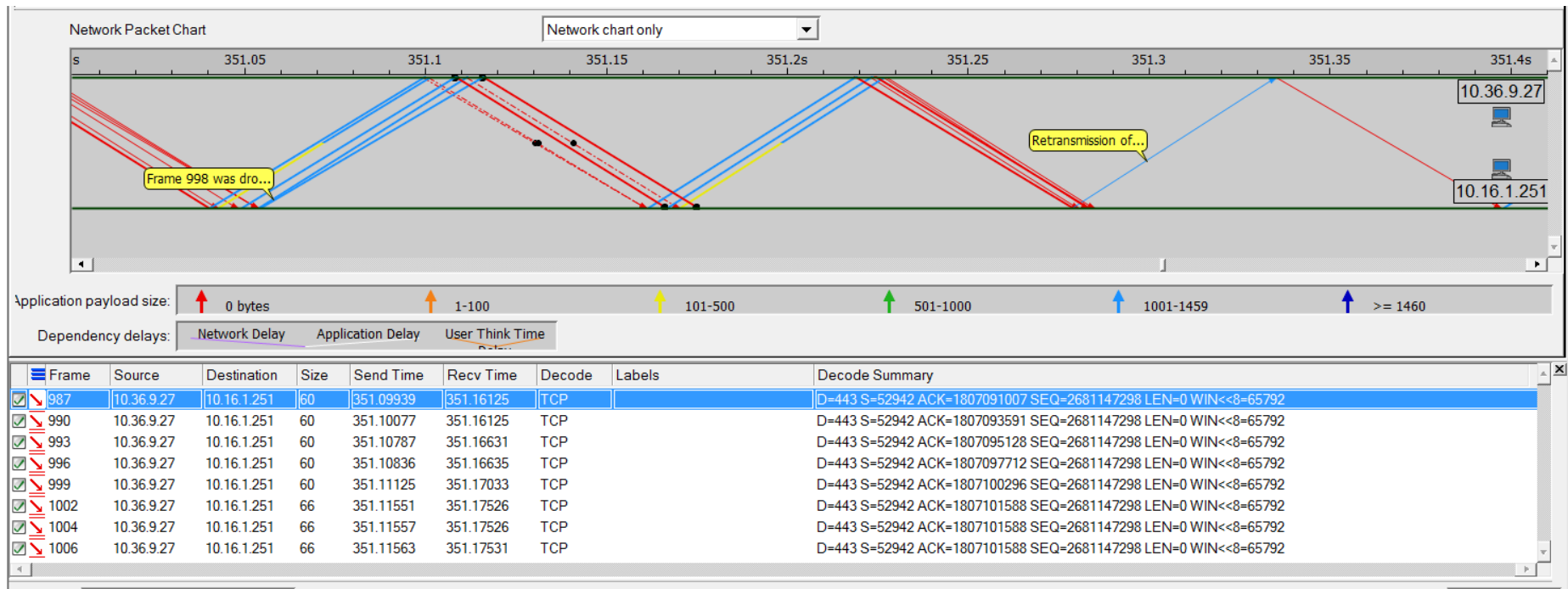


# What does this upward progression tell us?



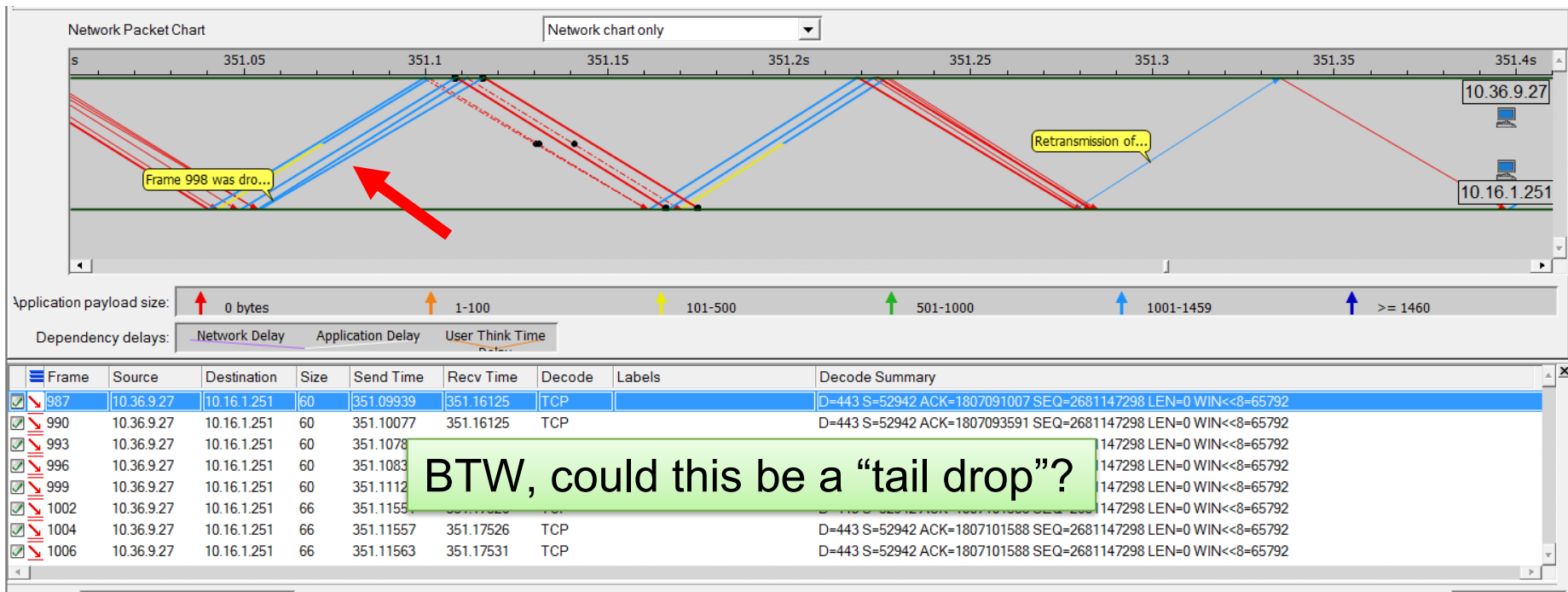


# When does Server hear the news?



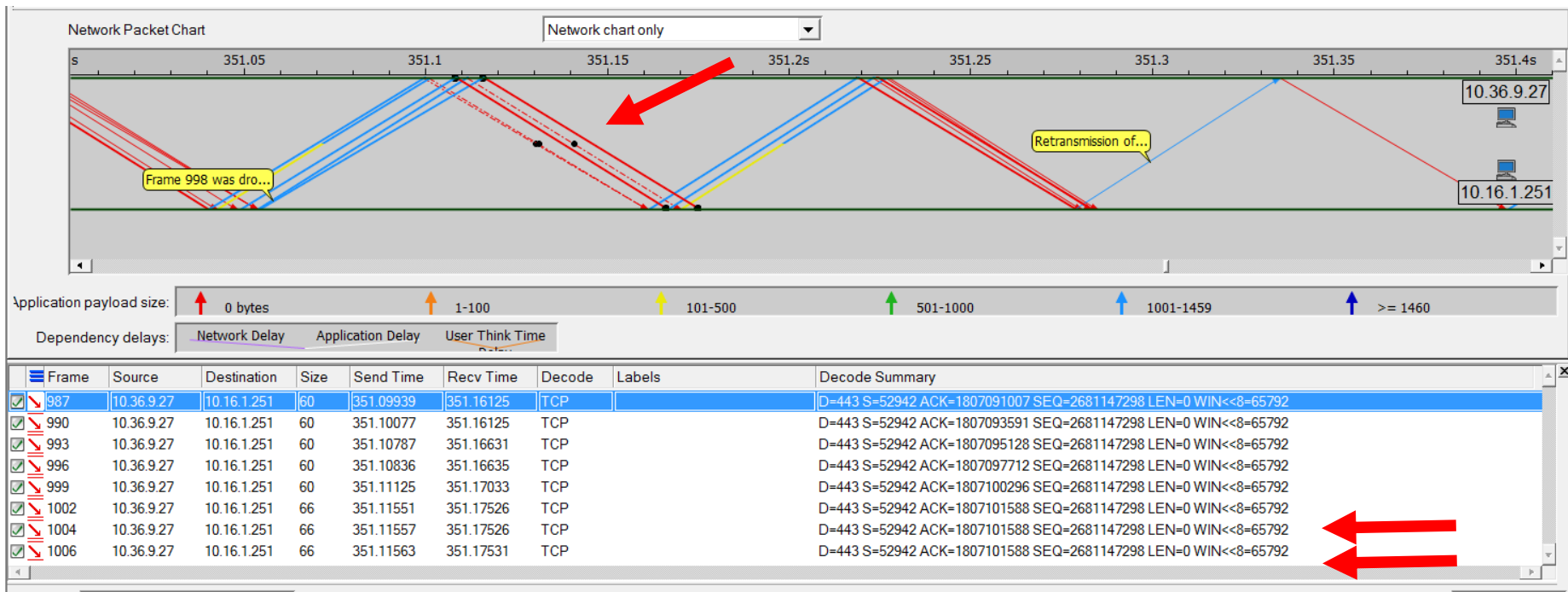


# #998 is dropped



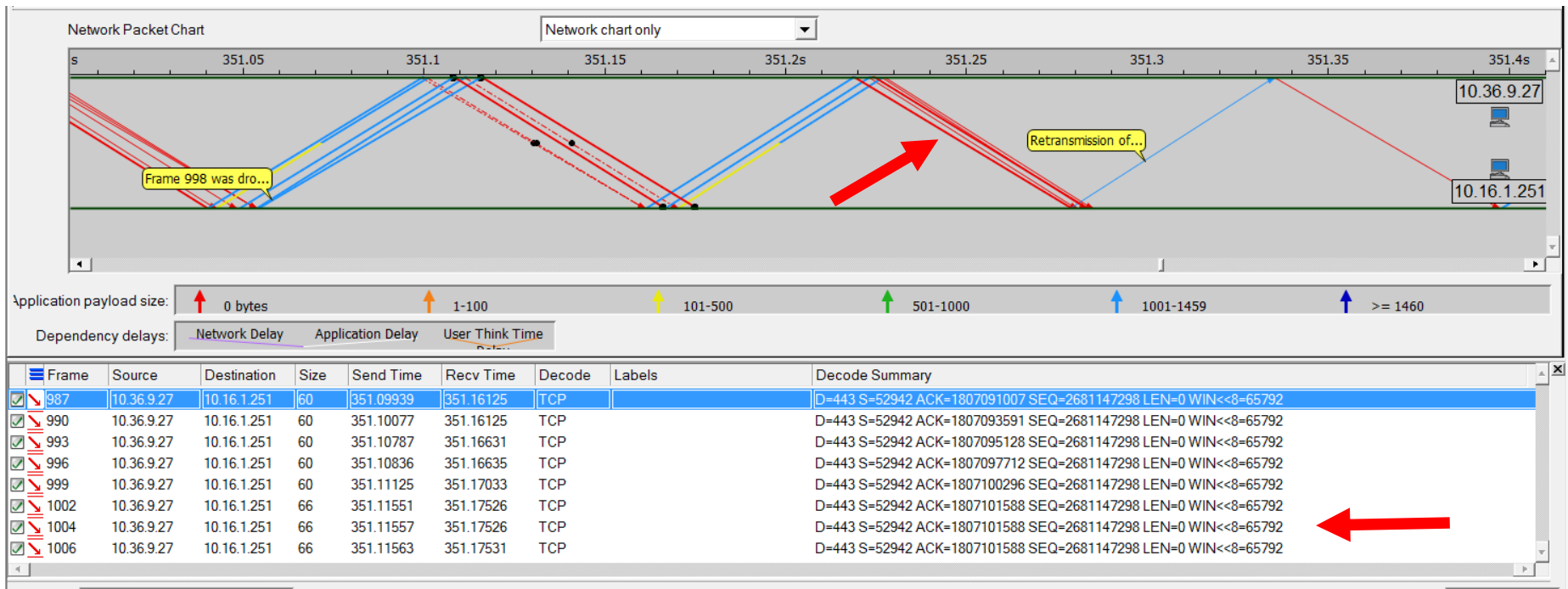


# 2 of the DupACKs





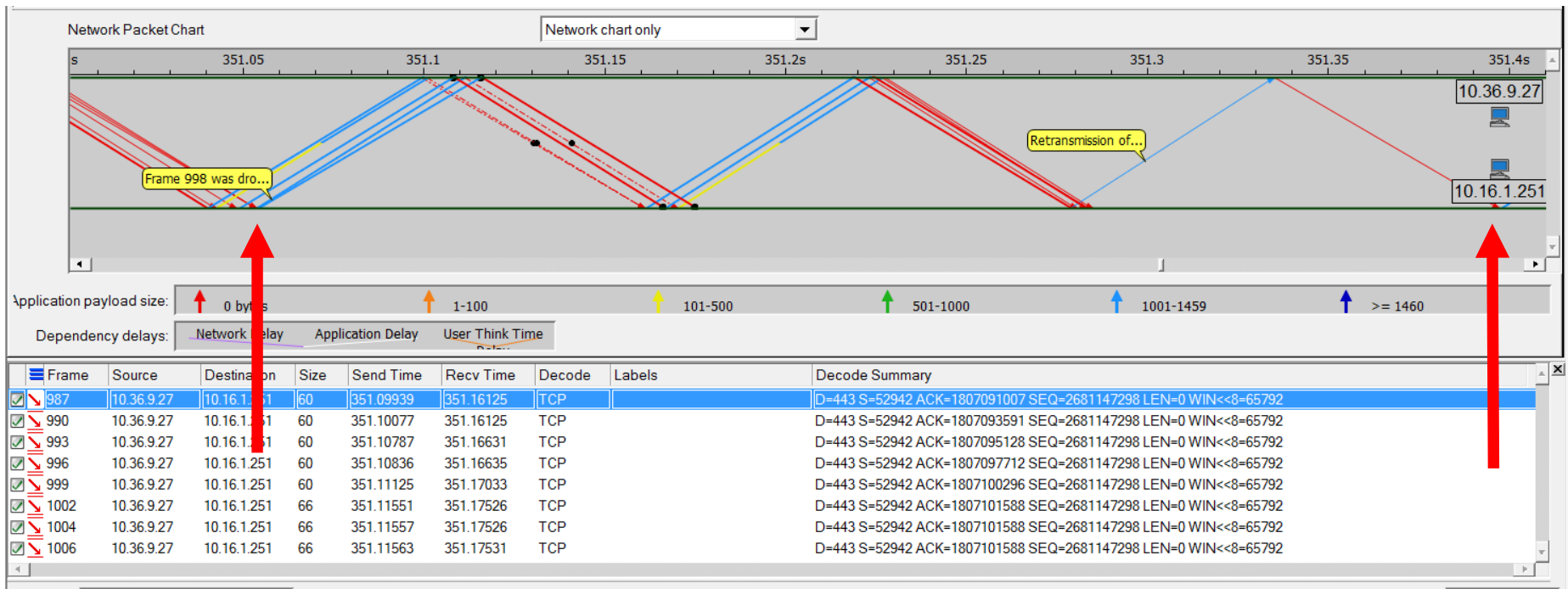
# 3 of 3 DupACKs







# Cost of Drop: # of RTTs?



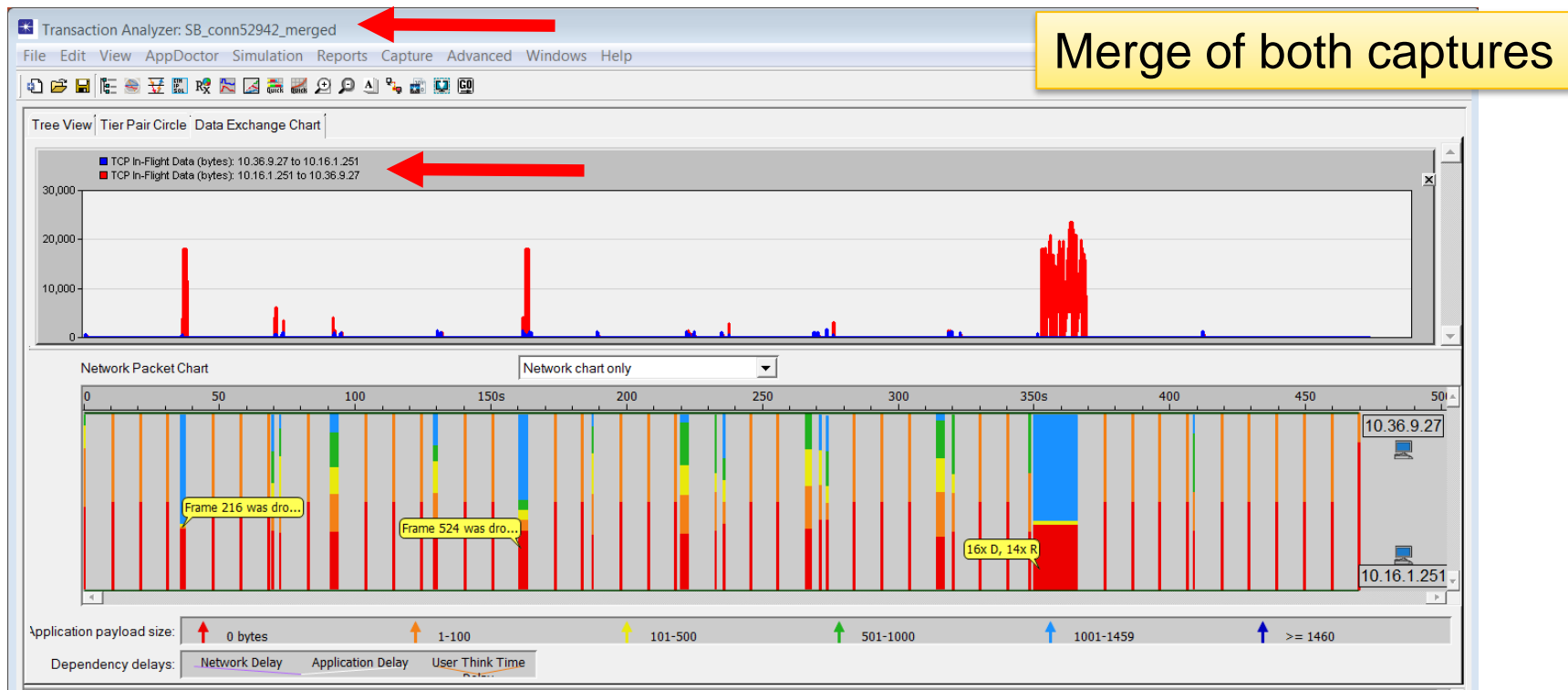


# Discussion



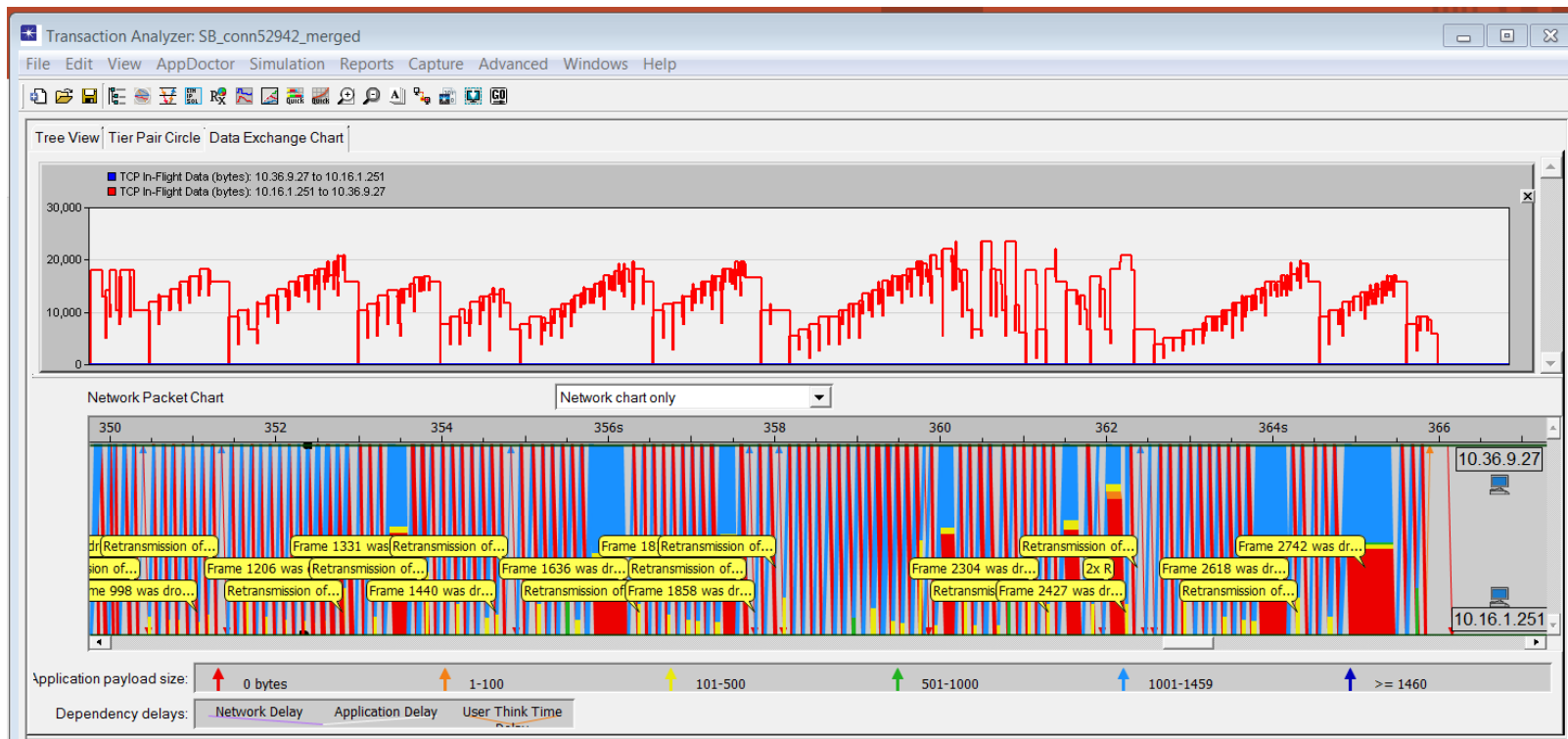


# Let's Visualize the Entire Connection



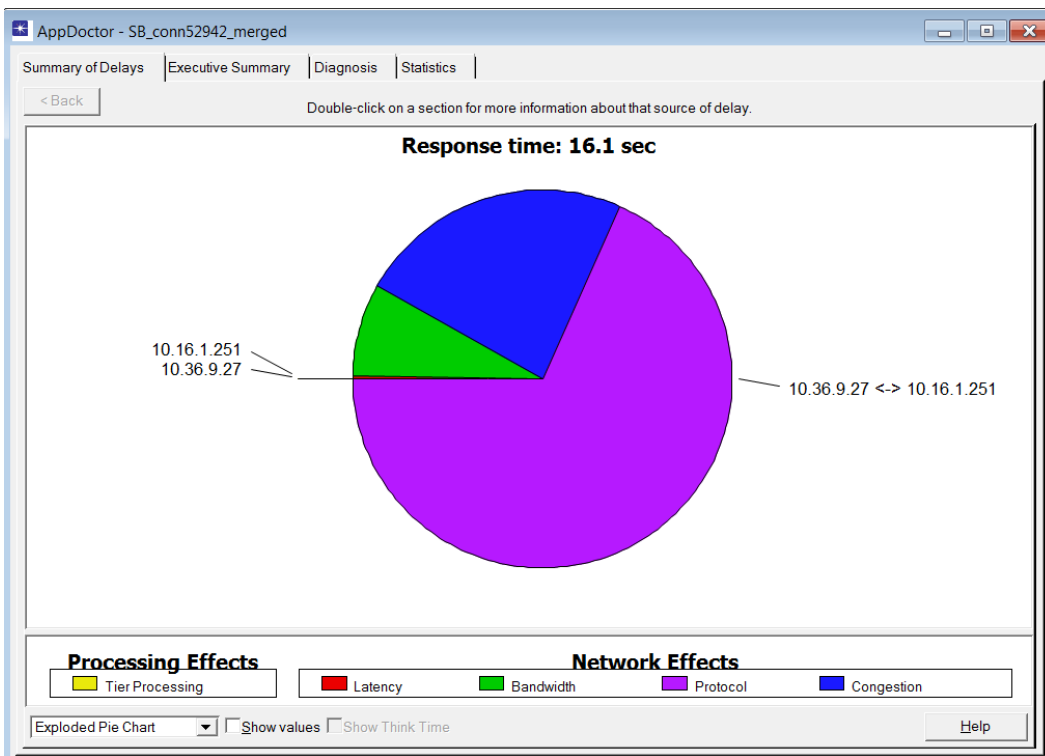


# ...drill into the 1.4MB Xfer





# Delay Analysis during Xfer





# Final Discussion, Questions, Comments

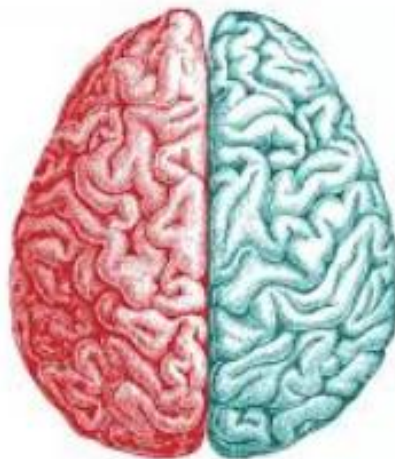




# Split Brain Comparisons



- Latency and Congestion Review





# Remember this?



- Client Capture – 121ms

GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Time delta from previous	Time delta from previous	Source	Destination	Identification	Length	Sequence number	Acknowledgment	Bytes in flight	Info
1	09:11:42.223468	0.000000000	0.000000000	10.36.9.27	10.16.1.251	0x0085 (1...	66	0	0		52942 → 443 [SYN] S
2	09:11:42.344959	0.121491000	0.121491000	10.16.1.251	10.36.9.27	0x77bc (3...	66	0	1		443 → 52942 [SYN, A
3	09:11:42.345046	0.000087000	0.000087000	10.36.9.27	10.16.1.251	0x0091 (1...	60	1	1		52942 → 443 [ACK] S

- Server Capture – 129ms

Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Time delta from previ	Time delta from previo	Source	Destination	Identification	Length	Sequence number	Acknowledgment	Bytes in flight	Info
1	09:11:42.262470	0.000000...	0.0000000...	10.36.9.27	10.16.1.2...	0x0085 (1...	82	0	0		S+, 52942 → 443 [SYN]
2	09:11:42.262524	0.000054...	0.0000540...	10.16.1.2...	10.36.9.27	0x77bc (3...	66	0	1		443 → 52942 [SYN, ACK]
3	09:11:42.391722	0.129198...	0.1291980...	10.36.9.27	10.16.1.2...	0x0091 (1...	60	1	1		52942 → 443 [ACK] Seq=





# Group Discussion



- What's the definition of latency?
- What's the definition of congestion?
- How can you tell latency from congestion?



# One Possible Formula



- Total Delay (TD) minus
- (Bandwidth delay + Latency Delay + Protocol Delay)
- $TD - (BD + LD + PD) == \text{Congestion}$



# Finding congestion



- How can we find examples of high latency (congestion) in the capture?
- High “prev captured” delta \*and\* 0 payload
  - Payload > 0 could be used if we find a “piggy-back” ACK



# Sort by Delta Prev



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
1851	449.348101	10.1965740...	10.36.9.27	10.16.1.251	1	66454	66455	1904975	1	[TCP Keep-Alive] 52942 → 443 [AC
529	303.879311	10.1558280...	10.36.9.27	10.16.1.251	1	54064	54065	372709	1	[TCP Keep-Alive] 52942 → 443 [AC
133	57.548500	10.1389620...	10.36.9.27	10.16.1.251	1	2488	2489	178373	1	[TCP Keep-Alive] 52942 → 443 [AC
588	340.091797	10.1356870...	10.36.9.27	10.16.1.251	1	63784	63785	378502	1	[TCP Keep-Alive] 52942 → 443 [AC
1853	459.479607	10.1314590...	10.36.9.27	10.16.1.251	1	66454	66455	1904975	1	[TCP Keep-Alive] 52942 → 443 [AC
234	113.908796	10.1314200...	10.36.9.27	10.16.1.251	1	16454	16455	202398	1	[TCP Keep-Alive] 52942 → 443 [AC
527	293.723442	10.1299650...	10.36.9.27	10.16.1.251	1	54064	54065	372709	1	[TCP Keep-Alive] 52942 → 443 [AC
1832	396.140034	10.1295880...	10.36.9.27	10.16.1.251	1	64514	64515	1903829	1	[TCP Keep-Alive] 52942 → 443 [AC
1849	439.151487	10.1290200...	10.36.9.27	10.16.1.251	1	66454	66455	1904975	1	[TCP Keep-Alive] 52942 → 443 [AC
1847	429.022425	10.1273540...	10.36.9.27	10.16.1.251	1	66454	66455	1904975	1	[TCP Keep-Alive] 52942 → 443 [AC
236	124.035166	10.1263460...	10.36.9.27	10.16.1.251	1	16454	16455	202398	1	[TCP Keep-Alive] 52942 → 443 [AC
1830	386.010406	10.1261620...	10.36.9.27	10.16.1.251	1	64514	64515	1903829	1	[TCP Keep-Alive] 52942 → 443 [AC
402	183.467112	10.1250520...	10.36.9.27	10.16.1.251	1	32586	32587	356957	1	[TCP Keep-Alive] 52942 → 443 [AC



# Scroll Down to TCP Len == 0



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
243	129.858807	0.912091000	10.16.1.251	10.36.9.27	453	202398	202851	17937	453	Application Data
485	266.005525	0.465380000	10.36.9.27	10.16.1.251	37	45617	45654	366285	37	Application Data
503	267.703699	0.415038000	10.36.9.27	10.16.1.251	37	49753	49790	368097	37	Application Data
15	0.661476	0.342085000	10.36.9.27	10.16.1.251	0	1035	1035	535		52942 → 443 [ACK] Seq=1035
1844	409.110547	0.334864000	10.36.9.27	10.16.1.251	0	66455	66455	1904975		52942 → 443 [ACK] Seq=66455
576	317.047693	0.332477000	10.36.9.27	10.16.1.251	0	61717	61717	377692		52942 → 443 [ACK] Seq=61717
248	130.359245	0.331970000	10.36.9.27	10.16.1.251	0	18971	18971	203944		52942 → 443 [ACK] Seq=18971
472	233.001809	0.329109000	10.36.9.27	10.16.1.251	0	45031	45031	363432		52942 → 443 [ACK] Seq=45031
427	220.077289	0.327739000	10.36.9.27	10.16.1.251	0	37139	37139	358625		52942 → 443 [ACK] Seq=37139
416	187.728667	0.327603000	10.36.9.27	10.16.1.251	0	35849	35849	358124		52942 → 443 [ACK] Seq=35849
163	70.246969	0.325587000	10.36.9.27	10.16.1.251	0	5499	5499	189187		52942 → 443 [ACK] Seq=5499
399	163.546123	0.325216000	10.36.9.27	10.16.1.251	0	32587	32587	356957		52942 → 443 [ACK] Seq=32587
489	266.335429	0.323936000	10.36.9.27	10.16.1.251	0	46651	46651	366738		52942 → 443 [ACK] Seq=46651



# Server Cap Shows 342ms RTT



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
12	0.318137	0.000028000	10.16.1.251	10.36.9.27	0	146	146	614		443 → 52942 [ACK]
13	0.319024	0.000887000	10.36.9.27	10.16.1.251	421	614	1035	146	421	Application Data
14	0.319391	0.000367000	10.16.1.251	10.36.9.27	389	146	535	1035	389	Application Data
15	0.661476	0.342085000	10.36.9.27	10.16.1.251	0	1035	1035	535		52942 → 443 [ACK]

- Could this be right? We just established RTT is 120-ish ms
- What is interesting about this ACK?



# Client shows 209ms delta?



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
12	0.318137	0.000028000	10.16.1.251	10.36.9.27	0	146	146	614		443 → 52942 [ACK]
13	0.319024	0.000887000	10.36.9.27	10.16.1.251	421	614	1035	146	421	Application Data
14	0.319391	0.000367000	10.16.1.251	10.36.9.27	389	146	535	1035	389	Application Data
15	0.661476	0.342085000	10.36.9.27	10.16.1.251	0	1035	1035	535		52942 → 443 [ACK]

GP\_VPN\_Client\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
10	0.321933	0.000216000	10.36.9.27	10.16.1.251	37	577	614	146	96	Application Data
11	0.326855	0.004922000	10.36.9.27	10.16.1.251	421	614	1035	146	517	Application Data
12	0.442252	0.115397000	10.16.1.251	10.36.9.27	0	146	146	518		[TCP Dup ACK 5#1] 4
13	0.442287	0.000035000	10.16.1.251	10.36.9.27	0	146	146	614		443 → 52942 [ACK] 5
14	0.452920	0.010633000	10.16.1.251	10.36.9.27	389	146	535	1035	389	Application Data
15	0.662106	0.209186000	10.36.9.27	10.16.1.251	0	1035	1035	535		52942 → 443 [ACK] 5



# Discussion

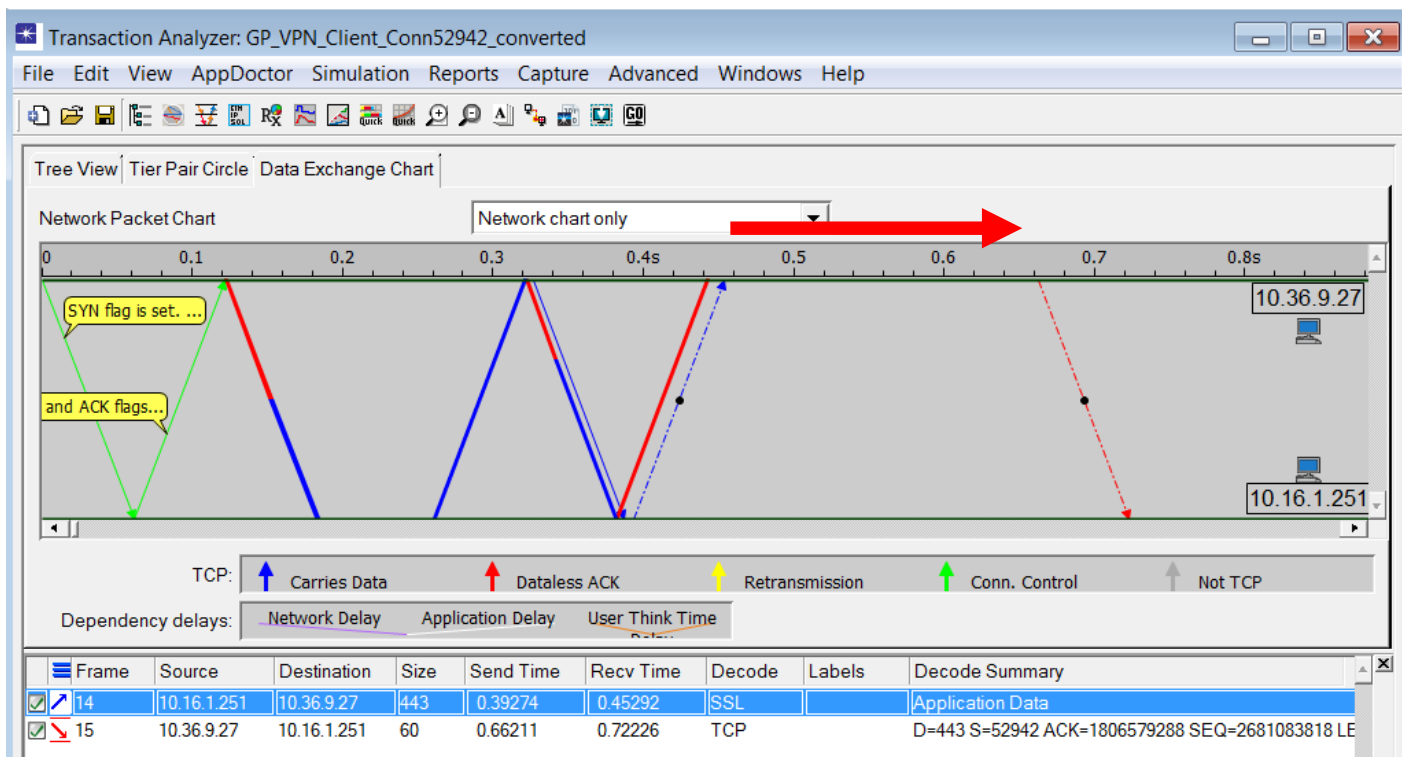


- Server shows 342ms delay
- Latency + Delayed ACK Timer + Latency
- Delayed ACK Timer 209ms
- $RTT\ 342ms - 209ms == 133ms$
- Is this in the ball park?
- What's the smallest latency we've seen so far in these captures?





# Let's Visualize





# Let's look at one more...



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
242	128.9467...	0.213123000	10.16.1.251	10.36.9.27	0	202398	202398	17937		443 → !
1840	408.7539...	0.211754000	10.36.9.27	10.16.1.251	37	65805	65842	1904330	37	Applica
564	316.4461...	0.205041000	10.36.9.27	10.16.1.251	37	58951	58988	376509	37	Applica
478	235.4991...	0.202144000	10.36.9.27	10.16.1.251	0	45617	45617	366285		52942 -
498	266.9674...	0.199534000	10.36.9.27	10.16.1.251	37	48719	48756	367644	37	Applica
8	0.317545	0.179102000	10.36.9.27	10.16.1.251	0	518	518	93		52942 -
395	163.2197...	0.175222000	10.36.9.27	10.16.1.251	37	31985	32022	356728	37	Applica



# Server Side



Server\_side\_shifted\_Conn52942.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
473	235.1794...	2.177615000	10.36.9.27	10.16.1.251	37	45031	45068	363432	37	Application Data
474	235.1800...	0.000639000	10.36.9.27	10.16.1.251	549	45068	45617	363432	586	Application Data
475	235.1800...	0.000031000	10.16.1.251	10.36.9.27	0	363432	363432	45617		443 → 52942 [ACK]
476	235.1817...	0.001658000	10.16.1.251	10.36.9.27	2853	363432	366285	45617	2853	Application Data
477	235.2970...	0.115259000	10.36.9.27	10.16.1.251	0	45617	45617	366016		52942 → 443 [ACK]
478	235.4991...	0.202144000	10.36.9.27	10.16.1.251	0	45617	45617	366285		52942 → 443 [ACK]
479	245.3135...	9.814430000	10.36.9.27	10.16.1.251	1	45616	45617	366285	1	[TCP Keep-Alive]



# Client Side



GP\_VPN\_Client\_Conn52942.pcap

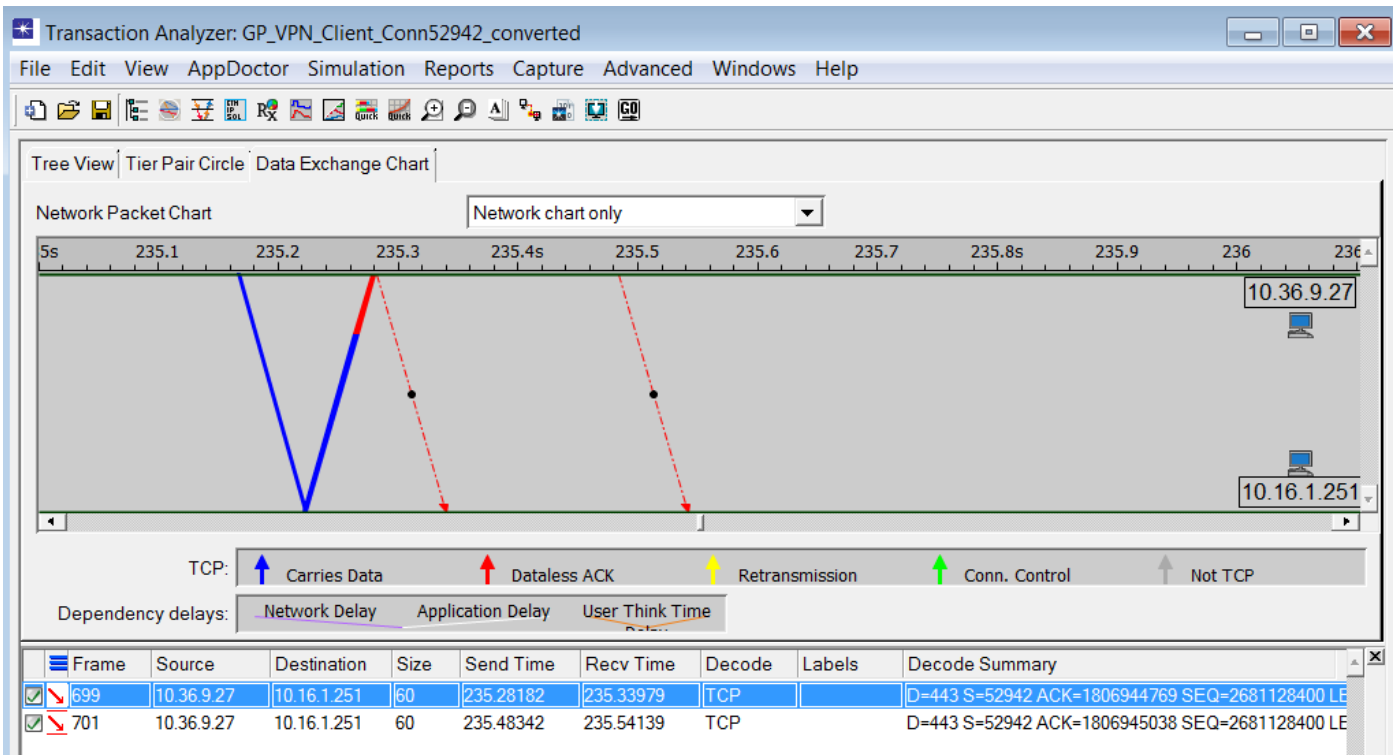
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Delta Prev	Source	Destination	TCP Len	Sequence number	Next seq	Ack	Bytes in flight	Info
694	235.1651...	2.178108000	10.36.9.27	10.16.1.251	37	45031	45068	363432	37	Application Da
695	235.1660...	0.000818000	10.36.9.27	10.16.1.251	549	45068	45617	363432	586	Application Da
696	235.2783...	0.112324000	10.16.1.251	10.36.9.27	0	363432	363432	45617		443 → 52942 [A
697	235.2812...	0.002939000	10.16.1.251	10.36.9.27	1292	363432	364724	45617	1292	443 → 52942 [A
698	235.2818...	0.000525000	10.16.1.251	10.36.9.27	1292	364724	366016	45617	2584	443 → 52942 [A
699	235.2818...	0.000021000	10.36.9.27	10.16.1.251	0	45617	45617	366016		52942 → 443 [A
700	235.2819...	0.000082000	10.16.1.251	10.36.9.27	269	366016	366285	45617	269	Application Da
701	235.4834...	0.201519000	10.36.9.27	10.16.1.251	0	45617	45617	366285		52942 → 443 [A
702	245.2961...	9.812773000	10.36.9.27	10.16.1.251	1	45616	45617	366285	1	[TCP Keep-Aliv

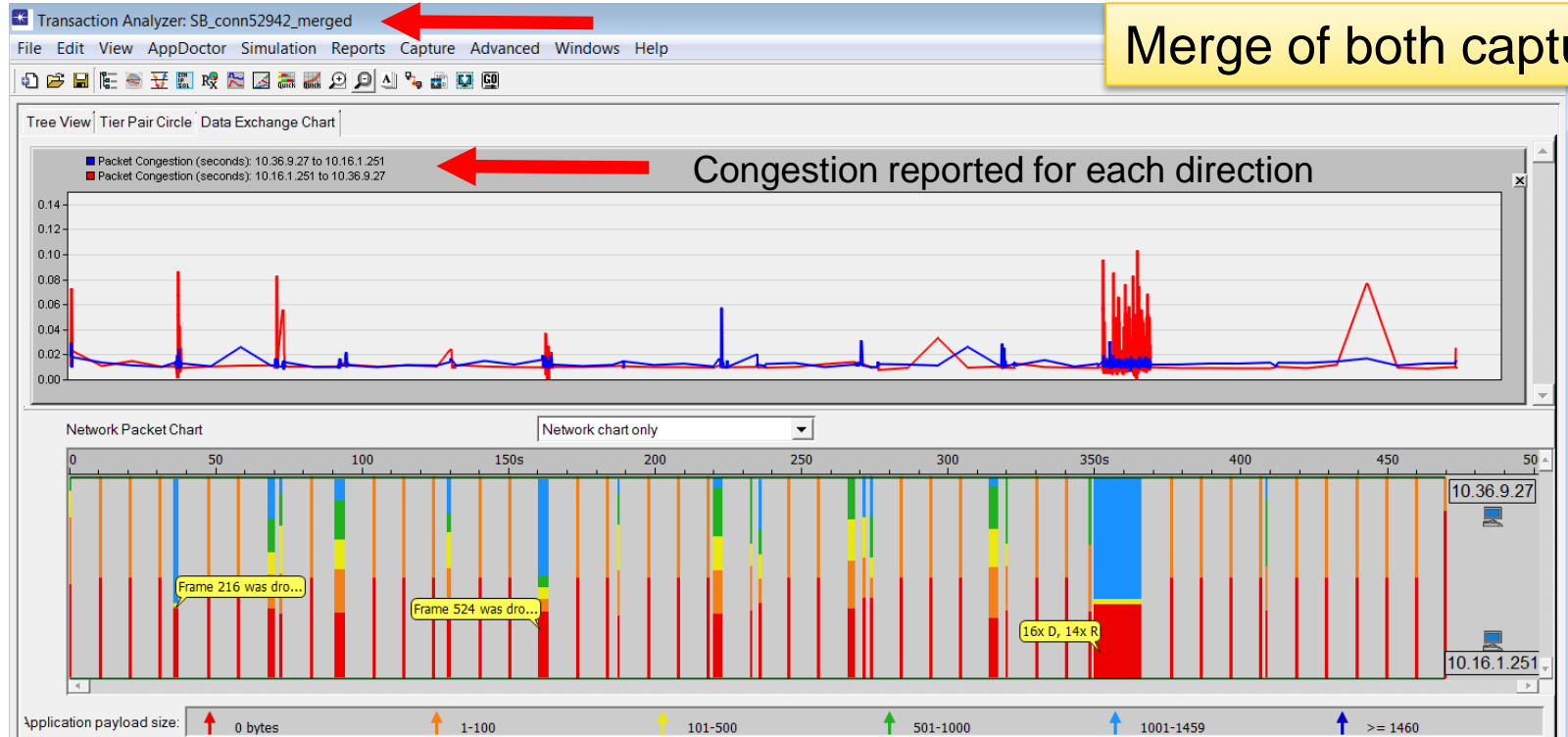


# Visualized



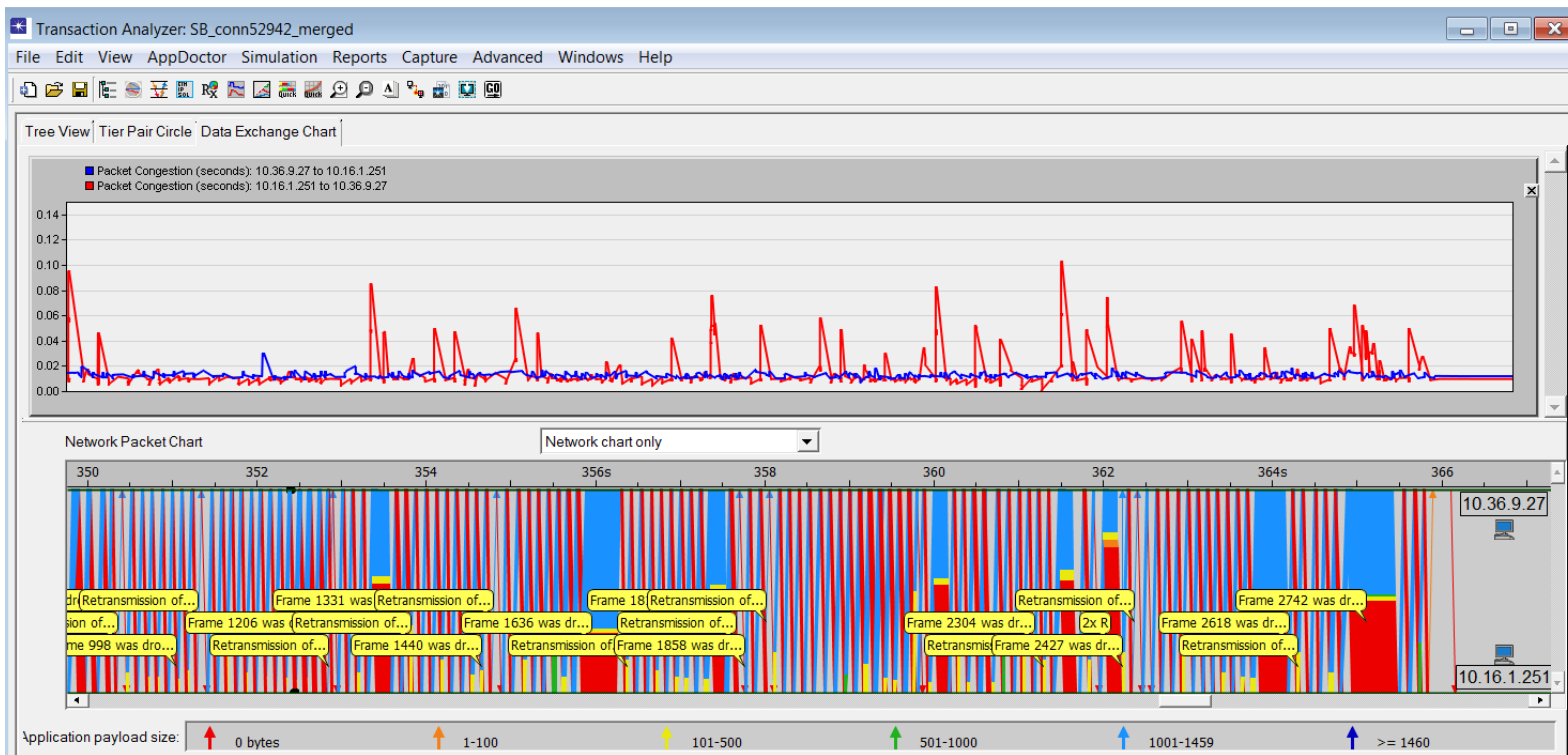


# 10,000 ft/m View





# Zoom-in to File Download





# Discussion



- Any surprises about the amount of congestion?
- Does this view help to explain how congestion impacts performance?





# Post Session – Thank You!



- Thank you for viewing this bonus section after Sharkfest Euro 2018 Conference!

[illegible]