SharkFest'23 US
San Diego, CA • June 10-15

S10 - Wireshark plus Advanced Analytics...

…better together

The Webex 98% Hang Condition – Part II

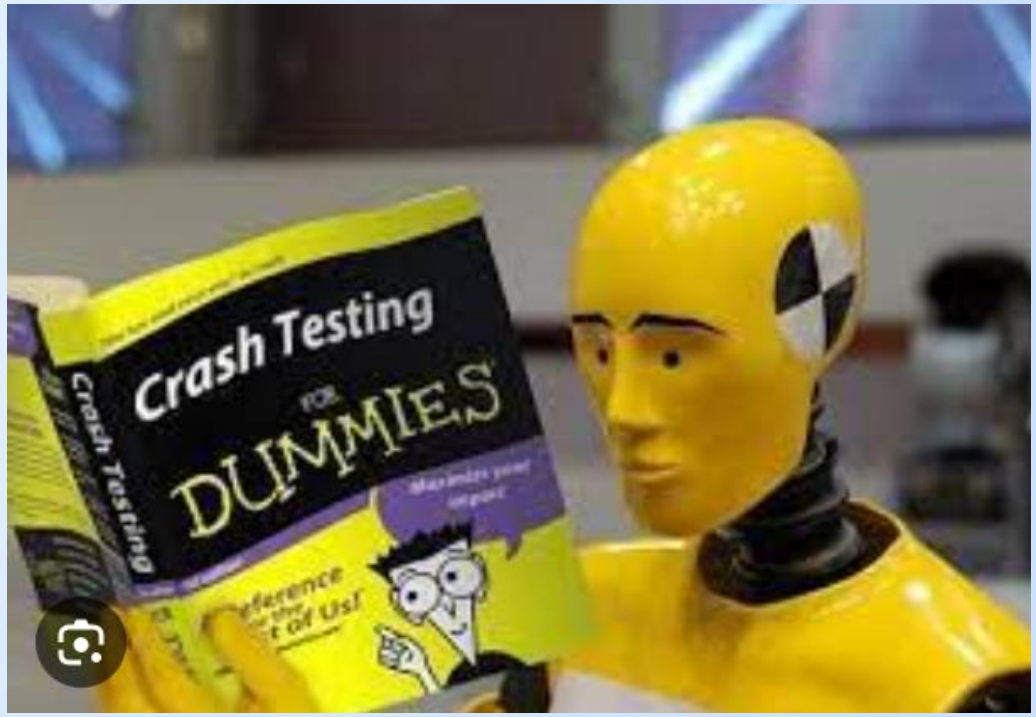
John Pittle
Customer Experience CTO
Riverbed Technologies
john.pittle@riverbed.com
@end2endviz
www.linkedin.com/in/john-pittle

Welcome Back

Thank you for returning for Part II, appreciate your partipation

Me

You



Agenda - Two Sessions

Part I

- Symptom Description
- App Architecture Assumptions
- Analysis Workflow
- Essential Wireshark Display Filters
- Lab #1
- Visualizing App Behavior
- Trimming our PCAP

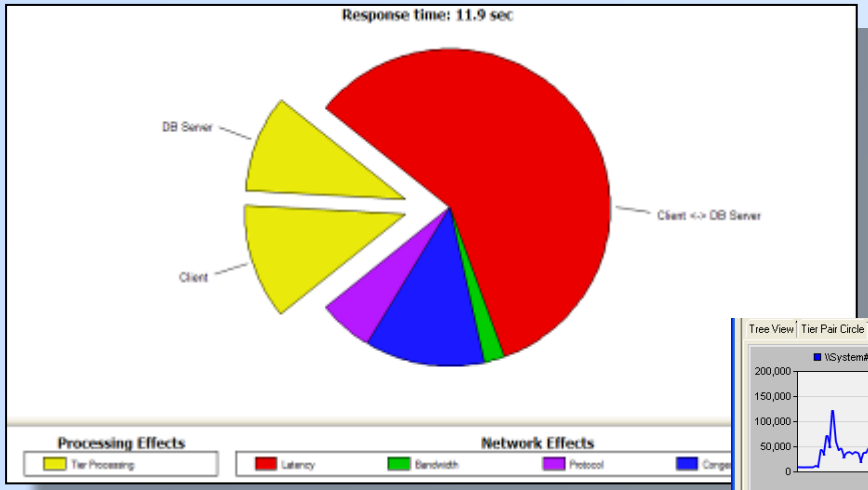
Part II

- Load filtered PCAP into Advanced Analytics
- Visualize the App Behavior
- More Visualizations
- How to do this in Wireshark?
- Lab #2
- Wrap-Up

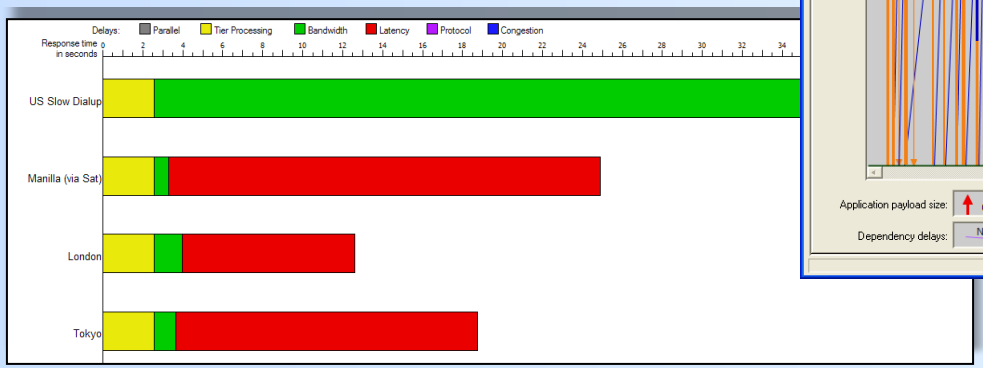
Why Advanced Analytics

Better Together

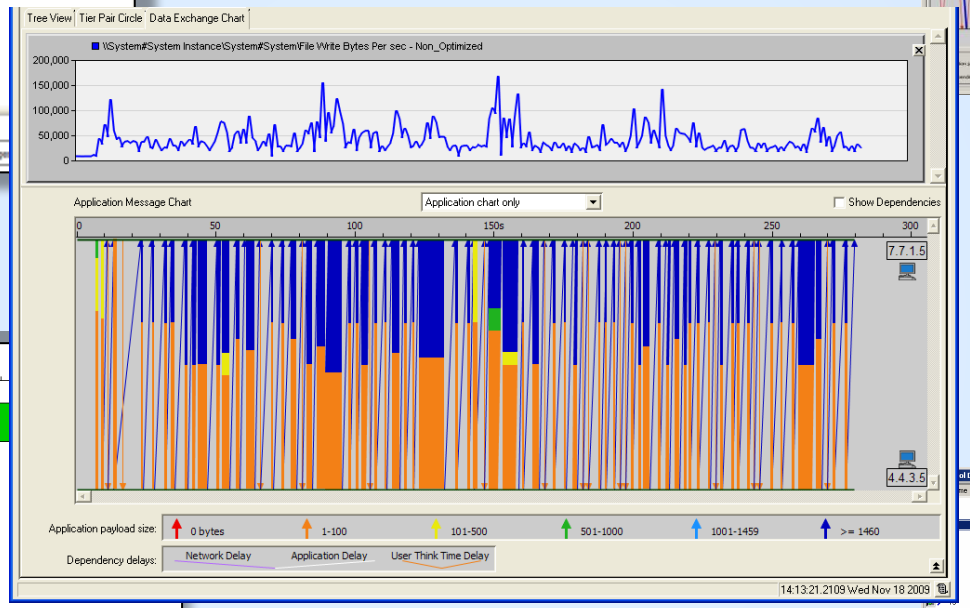
- Supplements & Complements Wireshark Capabilities
- Investigate based on visual clues
- Faster real-time filtering, packets are pre-grouped, easy to navigate
- Delay Analytics for Server, Protocol, Congestion, Latency, and BW
- Protocol decodes from Wireshark
- Screenshots and reports help explain symptom analysis

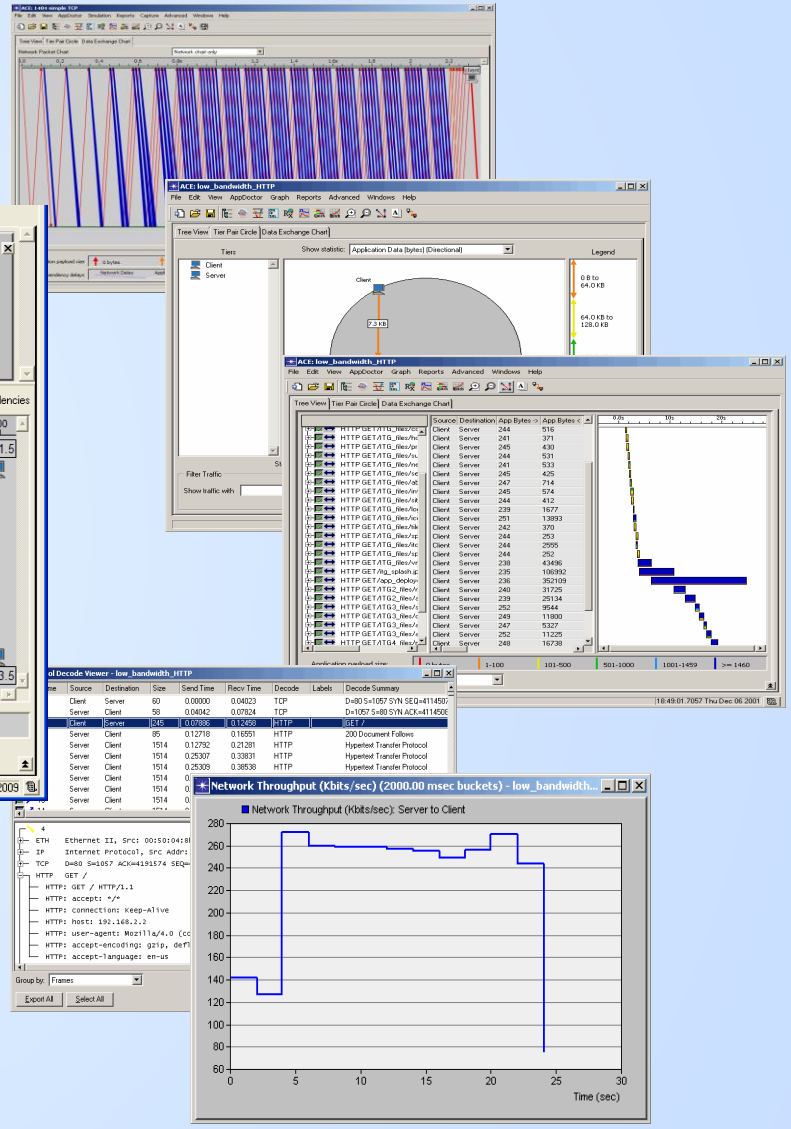


Summarize components of response-time delay



Predict response times





PCAP Before Filtering

Transaction Analyzer: webex_98pct_resolved16_56_52edt

File Edit View AppDoctor Simulation Reports Capture Advanced Windows Help

Tree View | Tier Pair Circle | Data Exchange Chart

Tiers

0.0.0.0
13.107.6.151
18.204.114.38
23.48.180.21
23.56.192.142
23.56.194.147
23.60.1.28
23.100.120.65
23.199.51.101
24.143.206.48
34.196.23.41
34.201.182.42
34.233.26.108
40.97.28.114
40.97.30.162
40.97.31.50
40.97.124.194
40.97.126.18
40.97.126.210
40.97.126.34
40.97.127.114
40.97.154.66
40.97.154.82
40.97.168.114

Show statistic: Application Data (bytes) (directional)

Legend

0 B
0 B to 512.0 KB
512.0 KB to 2.0 MB
2.0 MB to 4.0 MB
> 4.0 MB

Statistic description: Total number of application messages bytes transmitted (per direction.)

Filter Traffic

Show traffic with

Find Top Statistics... Run Layout

backing up file 'C:\Users\jpittle\op_admin\ta-17-7.prefs' ... done

Filter, Filter, and Filter Again

Be aware: Filtering can be a double-edged sword

- … take care not to filter too much… you might miss something important…

Wireshark Display Filter

From our work in Part I

wireshark display filter.txt

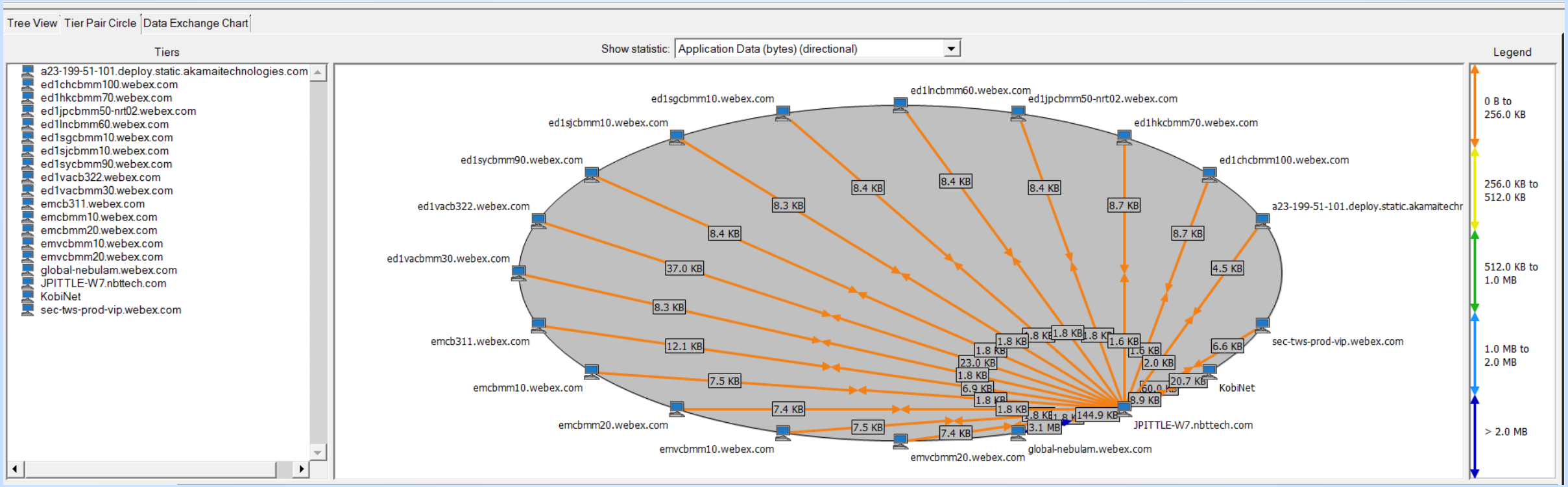
File Edit View

```
(ip.addr==173.243.0.154 || ip.addr==23.199.51.101 || ip.addr == 66.163.35.36 ||
ip.addr==64.68.120.90 || ip.addr==64.68.120.70 || ip.addr== 173.243.0.97 ||
ip.addr== 173.243.0.96 || ip.addr== 64.68.101.20 || ip.addr== 64.68.104.140 ||
ip.addr== 64.68.110.77 || ip.addr== 209.107.222.159 || ip.addr== 114.29.202.139 ||
ip.addr== 64.68.121.153 || ip.addr== 114.29.213.212 || ip.addr== 62.109.231.3 ||
ip.addr== 114.29.204.49 || ip.addr== 114.29.200.11 || ip.addr== 173.243.4.76 ||
ip.addr== 23.199.51.101) || dns
```

After Filter Applied

Extraneous traffic eliminated…

- Can seldom be 100% certain we haven't deleted something we need…



On to visualizing the traffic and behavior

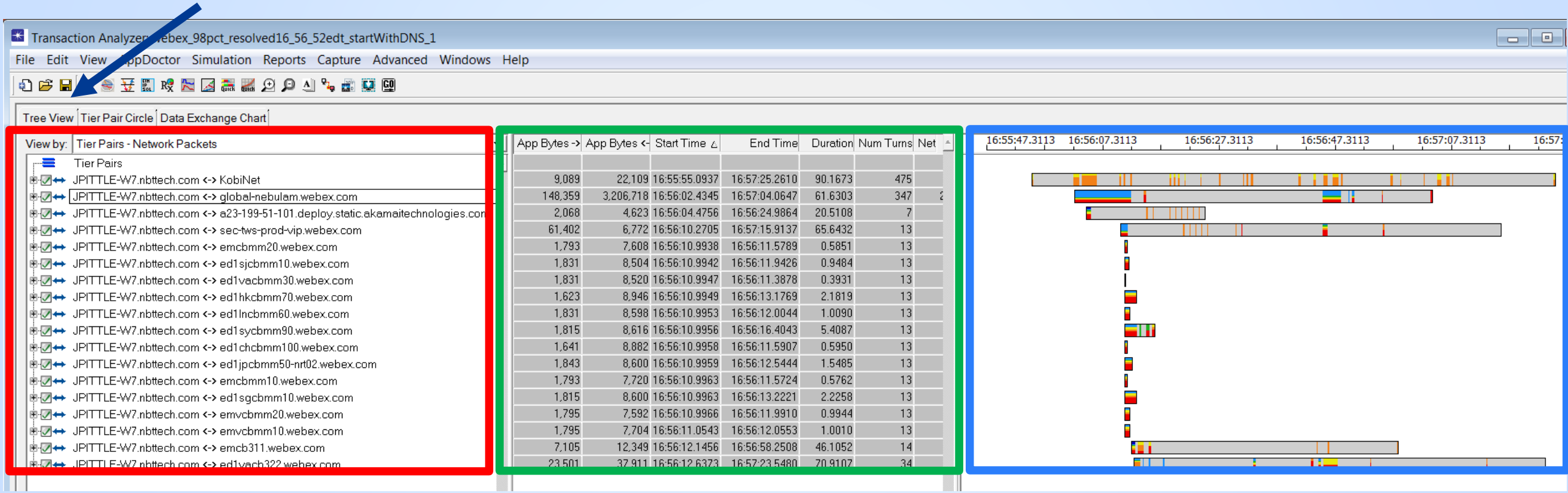
This is where Transaction Analyzer saves you time…

- Now that we've eliminated the extraneous traffic we can leverage TA visualization features to see what application and protocol behaviors may be related to our 98% hang condition

- Goal is to identify cause of "98% hang" condition as quickly as possible

1st Visualization: Treeview

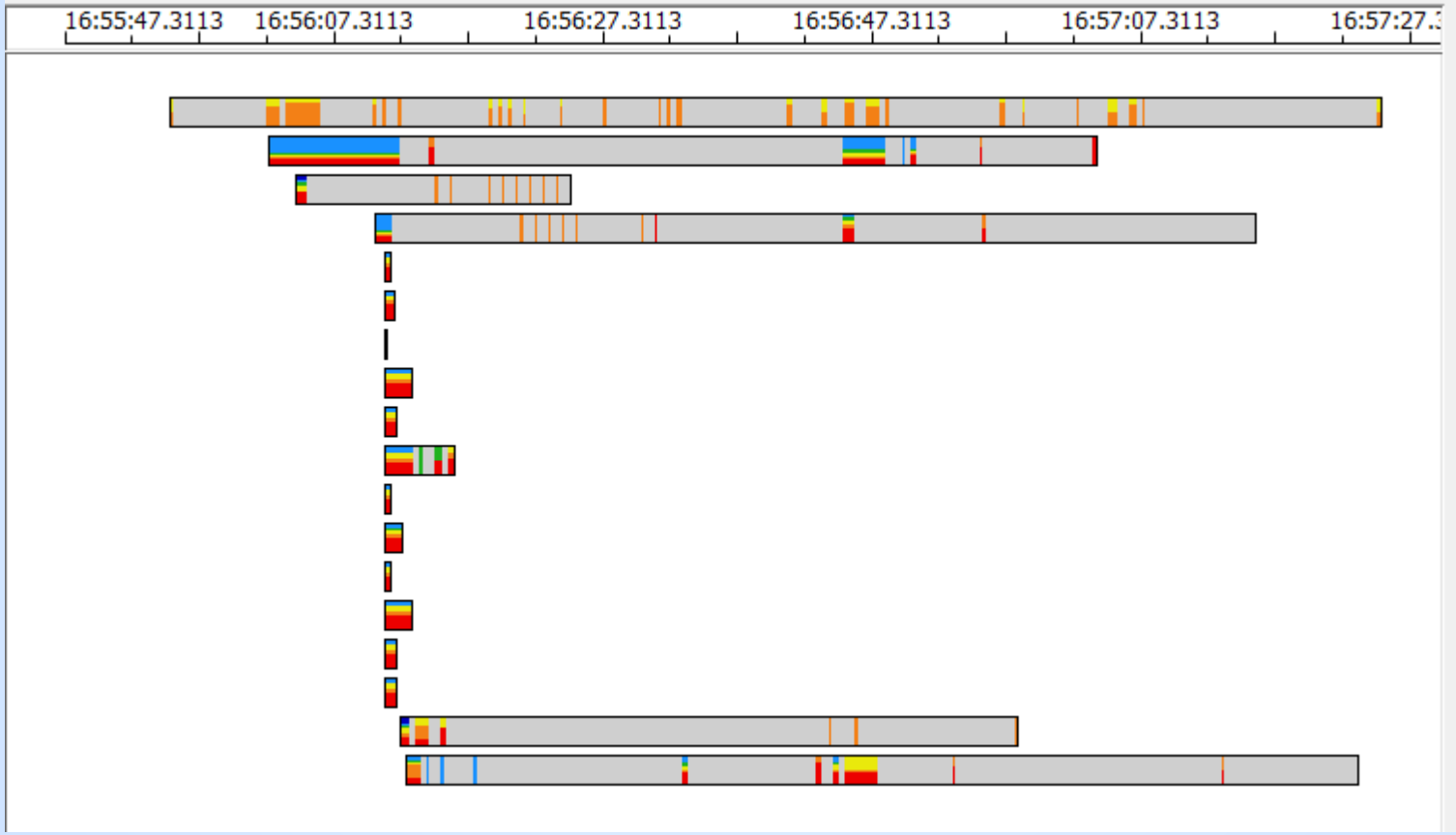
Right panel histograms provide visual clues worthy of research



App Bytes ->	App Bytes <-	Start Time	End Time	Duration	Num Turns	Net
9,089	22,109	16:55:55.0937	16:57:25.2610	90.1673	475	
148,359	3,206,718	16:56:02.4345	16:57:04.0647	61.6303	347	
2,068	4,623	16:56:04.4756	16:56:24.9864	20.5108	7	
61,402	6,772	16:56:10.2705	16:57:15.9137	65.6432	13	
1,793	7,608	16:56:10.9938	16:56:11.5789	0.5851	13	
1,831	8,504	16:56:10.9942	16:56:11.9426	0.9484	13	
1,831	8,520	16:56:10.9947	16:56:11.3878	0.3931	13	
1,623	8,946	16:56:10.9949	16:56:13.1769	2.1819	13	
1,831	8,598	16:56:10.9953	16:56:12.0044	1.0090	13	
1,815	8,616	16:56:10.9956	16:56:16.4043	5.4087	13	
1,641	8,882	16:56:10.9958	16:56:11.5907	0.5950	13	
1,843	8,600	16:56:10.9959	16:56:12.5444	1.5485	13	
1,793	7,720	16:56:10.9963	16:56:11.5724	0.5762	13	
1,815	8,600	16:56:10.9963	16:56:13.2221	2.2258	13	
1,795	7,592	16:56:10.9966	16:56:11.9910	0.9944	13	
1,795	7,704	16:56:11.0543	16:56:12.0553	1.0010	13	
7,105	12,349	16:56:12.1456	16:56:58.2508	46.1052	14	
23,501	37,911	16:56:12.6373	16:57:23.5480	70.9107	34	

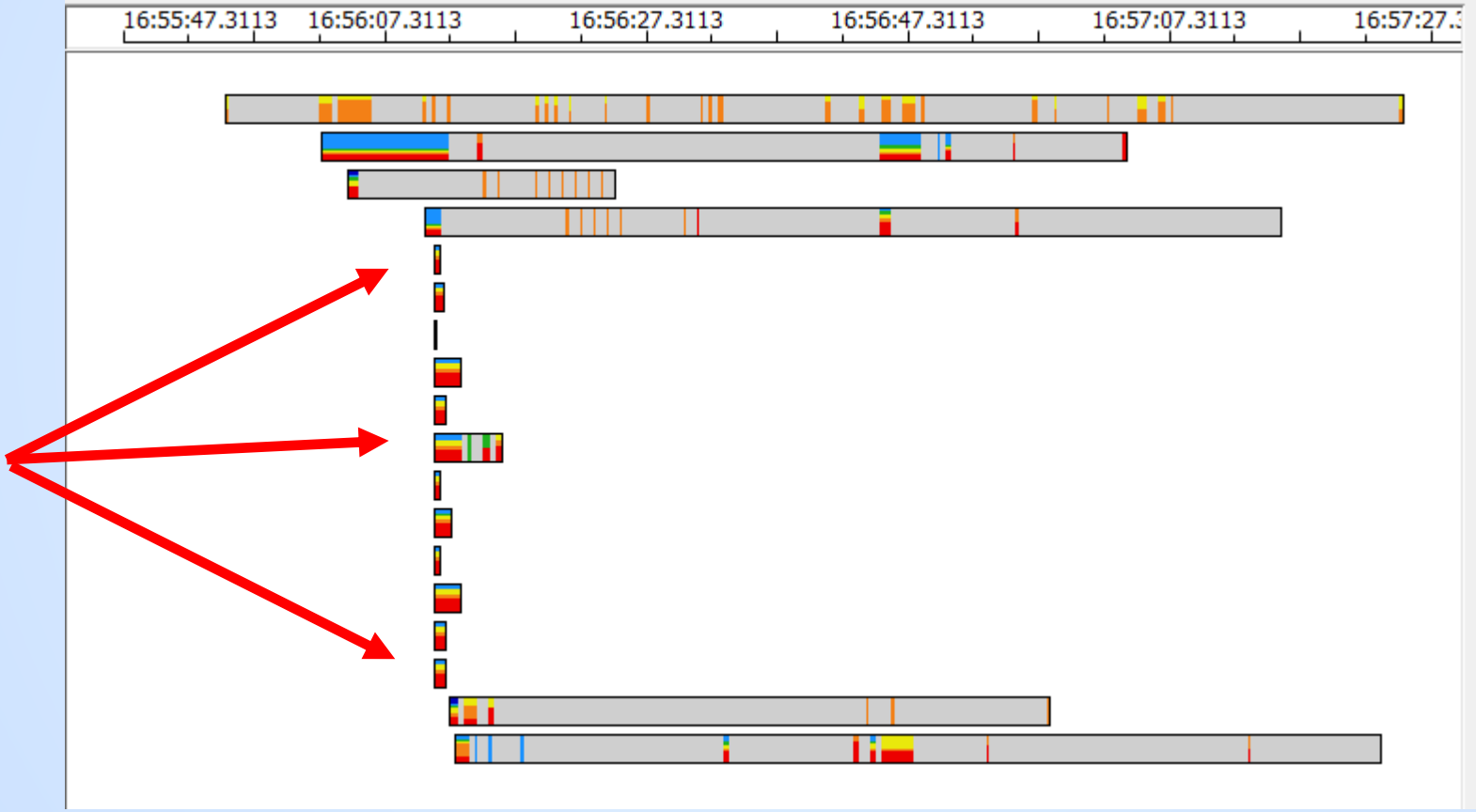
Zoom-in to Right Panel

Histograms show aggregated view of traffic over time



Not likely involved in the timeout / hang (Guess)

These connections are short lived, we can (probably) rule them out



Expand into individual connections

Transaction Analyzer: webex filtered

File Edit View AppDoctor Simulation Reports Capture Advanced Windows Help

Tree View | Tier Pair Circle | Data Exchange Chart

View by: Tier Pairs - Network Packets

Tier Pairs	App Bytes ->	App Bytes <-	Start Time	End Time	Duration	Num Turns	N
192.168.2.105 <-> 192.168.2.1	9,089	21,179	0.0000	90.1673	90.1673	475	
192.168.2.105 <-> dfw02-nebulam.webex.com	148,359	3,206,718	7.3408	68.9711	61.6303	347	
Connections							
TLS: 62037<->443 Client Hello	5,832	12,463	7.3408	8.3651	1.0243	9	
TLS: 62038<->443 Client Hello	11,491	74,055	7.3411	9.0676	1.7265	17	
TLS: 62039<->443 Client Hello	6,213	113,441	7.3413	8.3597	1.0184	11	
TLS: 62043<->443 Client Hello	10,339	144,729	8.3919	9.4884	1.0965	13	
TLS: 62044<->443 Client Hello	5,581	10,807	8.3922	8.8936	0.5013	9	
TLS: 62045<->443 Client Hello	2,227	5,467	8.3954	8.9528	0.5575	5	
TCP: 62048<->443 D=443 S=62048 SYN SEQ=1377699264 LEN	0	0	8.9795	9.0350	0.0555	1	
TLS: 62049<->443 Client Hello	2,255	16,107	8.9827	9.3241	0.3414	6	
TLS: 62050<->443 Client Hello	2,436	16,107	8.9873	11.9855	2.9983	6	
TLS: 62051<->443 Client Hello	2,451	7,747	9.0596	11.9865	2.9269	6	

0.0s 20s 40s 60s 80s

Application payload size: 0 bytes | 1-100 | 101-500 | 501-1000 | 1001-1459 | >= 1460

Frame	Source	Destination	Size	Send Time	Recv Time	Decode	Labels	Decode Summary

Group by: Frames 0 packets Summary decode level First

backing up file 'C:\Users\jpittle\op_admin\ta-17-7.prefs' ... done 13:57:31.7216 Tue Jun 05 2018

Finding #1 - Sample Connection Failures - Nebulem

Client does not respond to SYN+ACK

Clue: no payload / minimal duration

Tree View | Tier Pair Circle | Data Exchange Chart

View by: Tier Pairs - Network Packets

	App Bytes ->	App Bytes <-	Start Time	End Time	Duration	Num Turns	Net Bytes ->	Net Bytes <-
SSL: 62049<->443 Client Hello	2,255	16,107	15:56:04.0764	...:04.4178	0.3414	6	2,951	17,169
SSL: 62050<->443 Client Hello	2,436	16,107	15:56:04.0809	...:07.0792	2.9983	6	3,132	17,169
SSL: 62051<->443 Client Hello	2,451	7,747	15:56:04.1533	...:07.0802	2.9269	6	3,147	8,545
SSL: 62052<->443 Client Hello	2,441	7,420	15:56:04.1536	...:07.0853	2.9317	6	3,137	8,018
SSL: 62054<->443 Client Hello	6,635	13,672	15:56:04.1632	...:10.5767	6.4135	12	7,955	15,022
SSL: 62058<->443 Client Hello	4,942	2,147,806	15:56:04.4174	...:14.5789	10.1014	11	54,934	2,236,534
SSL: 62068<->443 Client Hello	517	147	15:56:06.9334	...:07.0853	0.1519	3	817	381
SSL: 62069<->443 Client Hello	517	147	15:56:06.9366	...:07.0852	0.1487	3	817	441
SSL: 62070<->443 Client Hello	517	147	15:56:06.9407	...:07.0914	0.1507	3	817	441
TCP: 62071<->443 D=443 S=62071 SYN SEQ=62163391 LEN=0 WIN=8192	0	[illegible]	15:56:07.0212	...:07.0802	0.0590	1	66	66
TCP: 62072<->443 D=443 S=62072 SYN SEQ=773784470 LEN=0 WIN=8192	0	0	15:56:07.0231	...:07.0842	0.0611	1	66	66
TCP: 62073<->443 D=443 S=62073 SYN SEQ=307280251 LEN=0 WIN=8192	0	0	15:56:07.0251	...:07.0852	0.0601	1	66	66
TCP: 62074<->443 D=443 S=62074 SYN SEQ=3652127599 LEN=0 WIN=8192	0	0	15:56:07.0267	...:07.0932	0.0665	1	66	66
TCP: 62075<->443 D=443 S=62075 SYN SEQ=4035789346 LEN=0 WIN=8192	0	0	15:56:07.0269	...:07.0912	0.0643	1	66	66
TCP: 62076<->443 D=443 S=62076 SYN SEQ=2183021306 LEN=0 WIN=8192	0	0	15:56:07.0270	...:07.0972	0.0702	1	66	66
TCP: 62077<->443 D=443 S=62077 SYN SEQ=552302023 LEN=0 WIN=8192	0	0	15:56:07.0272	...:07.0973	0.0701	1	66	66
TCP: 62078<->443 D=443 S=62078 SYN SEQ=3923517537 LEN=0 WIN=8192	0	0	15:56:07.0274	...:07.0972	0.0699	1	66	66
TCP: 62079<->443 D=443 S=62079 SYN SEQ=4106680431 LEN=0 WIN=8192	0	0	15:56:07.0284	...:07.0973	0.0689	1	66	66
TCP: 62080<->443 D=443 S=62080 SYN SEQ=3123588224 LEN=0 WIN=8192	0	0	15:56:07.0286	...:07.0972	0.0687	1	66	66
TCP: 62081<->443 D=443 S=62081 SYN SEQ=3076896610 LEN=0 WIN=8192	0	0	15:56:07.0287	...:07.0972	0.0685	1	66	66
TCP: 62082<->443 D=443 S=62082 SYN SEQ=3121197648 LEN=0 WIN=8192	0	0	15:56:07.0289	...:07.0952	0.0663	1	66	66
SSL: 62083<->443 Client Hello	10,400	104,243	15:56:08.7335	...:09.9739	1.2404	11	13,814	109,703
SSL: 62084<->443 Client Hello	4,365	11,425	15:56:08.8632	...:09.8930	1.0298	8	5,169	12,385

15:55:55.093715:56:15.0937

Application payload size: 0 bytes | 1-100 | 101-500 | 501-1000 | 1001-1459

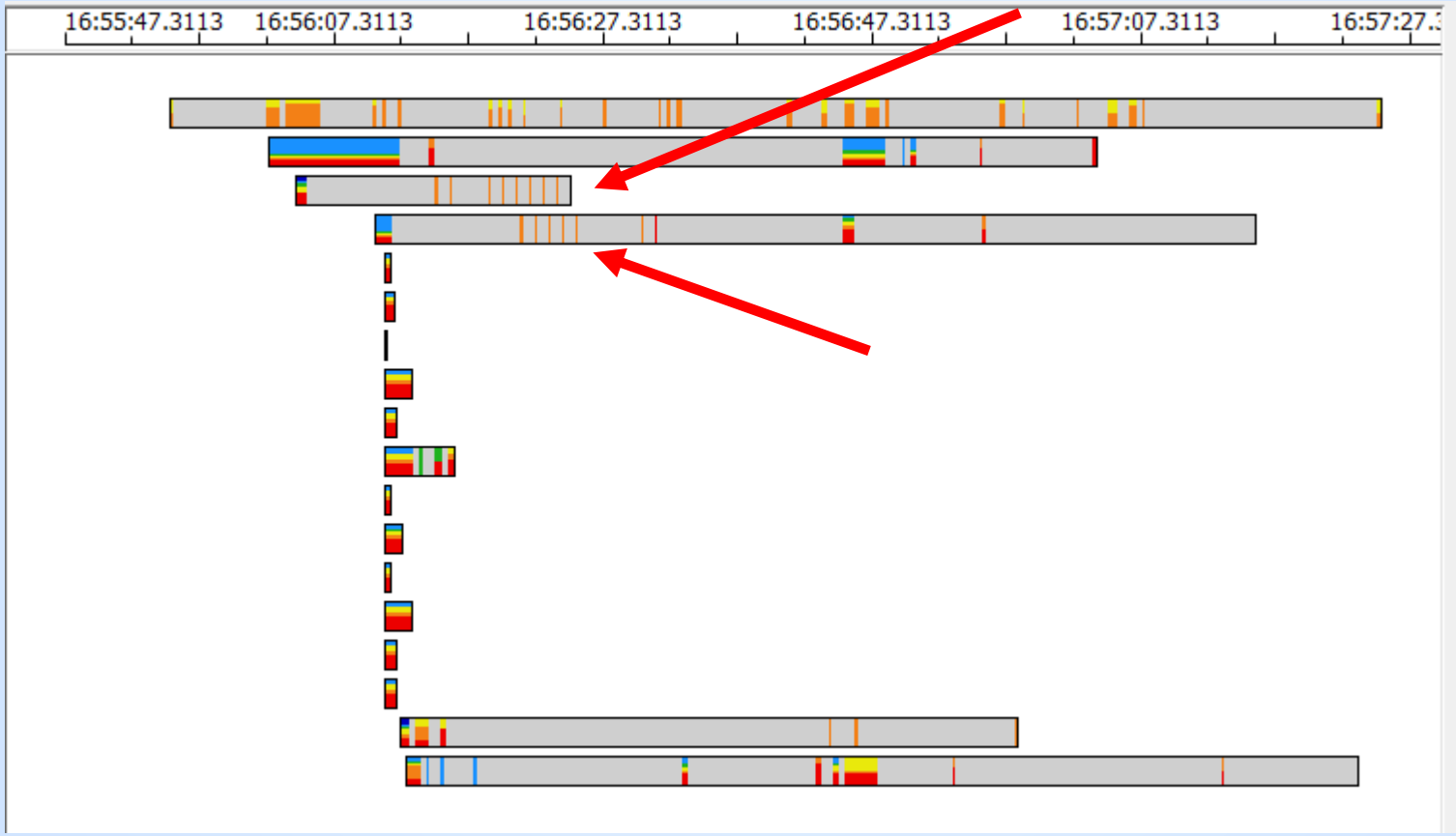
Frame	Source	Destination	Size	Send Time	Recv Time	Decode	Labels	Decode Summary
2764	JPITTLE-W7.nbttech.com	global-nebulam.webex.com	66	15:56:07.0212	15:56:07.0507	TCP		D=443 S=62071 SYN SEQ=62163391 LEN=0 WIN=8192
2847	global-nebulam.webex.com	JPITTLE-W7.nbttech.com	66	15:56:07.0507	15:56:07.0802	TCP		D=62071 S=443 SYN ACK=62163392 SEQ=516034430 LEN=0 WIN=8190

Document Findings

	A	B	C	D	E	F	G
1							
2	**Symptoms found in "98% hang" capture**						
3							
4	**Finding #**	**Symptom**	**Server**	**IP**	**Conn Port#**	**Start Time**	**Stop Time**
5	1	Client does not complete 3-way handshake	nebulam	173.243.0.154	various		
6							
7							
8							
9							
10							
11							

These patterns look interesting

Shows packet exchanges over time – will deep dive into this next



Finding #2 - Akamai does not ACK the client keepalives on connection 62057

Client sends RST after 10 keepalive requests

Protocol Decode Viewer - webex_98pct_resolved16_56_52edt_startWithDNS_1

Frame	Source	Destination	Size	Send Time	Recv Time	Decode	Labels	Decode Summary
1094	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	180	15:56:04.5513	15:56:04.5654	SSL		Client Key Exchange, Change Cipher Spec, Hello Request, Hello Re
1131	a23-199-51-101.deploy.static.akamaitechnologies.com	JPITTLE-W7.nbttech.com	312	15:56:04.5679	15:56:04.5819	SSL		New Session Ticket, Change Cipher Spec, Encrypted Handshake M
1163	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:04.7853	15:56:04.7993	TCP		D=443 S=62057 ACK=3772168691 SEQ=1174355168 LEN=0 WIN<<2=
1175	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	1479	15:56:04.8460	15:56:04.8601	SSL		Application Data
1249	a23-199-51-101.deploy.static.akamaitechnologies.com	JPITTLE-W7.nbttech.com	60	15:56:04.9213	15:56:04.9353	TCP		D=62057 S=443 ACK=1174356593 SEQ=3772168691 LEN=0 WIN<<7=
1274	a23-199-51-101.deploy.static.akamaitechnologies.com	JPITTLE-W7.nbttech.com	514	15:56:04.9584	15:56:04.9724	SSL		Application Data
1331	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:05.1773	15:56:05.1913	TCP		D=443 S=62057 ACK=3772169151 SEQ=1174356593 LEN=0 WIN<<2=
5861	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:14.9728	15:56:14.9868	SSL		Continuation Data
5884	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:15.9760	15:56:15.9900	SSL		Continuation Data
5900	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:16.9738	15:56:16.9878	SSL		Continuation Data
5924	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:17.9749	15:56:17.9889	SSL		Continuation Data
5966	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:18.9790	15:56:18.9931	SSL		Continuation Data
6010	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:19.9735	15:56:19.9875	SSL		Continuation Data
6041	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:20.9736	15:56:20.9876	SSL		Continuation Data
6196	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:21.9744	15:56:21.9885	SSL		Continuation Data
6216	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:22.9728	15:56:22.9868	SSL		Continuation Data
6233	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:23.9733	15:56:23.9873	SSL		Continuation Data
6243	JPITTLE-W7.nbttech.com	a23-199-51-101.deploy.static.akamaitechnologies.com	60	15:56:24.9724	15:56:24.9864	TCP		D=443 S=62057 RST ACK=3772169151 SEQ=1174356593 LEN=0 WIN

```
5861
ETH   Ethernet II, Src: f0:d5:bf:25:2d:3f (f0:d5:bf:25:2d:3f), Dst: 192.168.2.1 (48:f8:b3:91:b1:fe)
IP    Internet Protocol Version 4, Src: 192.168.2.105 (192.168.2.105), Dst: e5169.d.akamaiedge.net (23.199.51.101) ID=18369
TCP   D=443 S=62057 ACK=3772169151 SEQ=1174356592 LEN=1 WIN<<2=65700
SSL   Continuation Data
HEX   Captured bytes
```

Visualization pattern provided the clue that we needed to look closer

Document Findings

	A	B	C	D	E	F	G
1							
2	**Symptoms found in "98% hang" capture**						
3							
4	**Finding #**	**Symptom**	**Server**	**IP**	**Conn Port#**	**Start Time**	**Stop Time**
5	1	Client does not complete 3-way handshake	nebulam	173.243.0.154	various		
6	2	Server does not ACK keepalive	akamai	23.199.51.101	62057	16:56:14	
7							
8							
9							
10							
11							

Finding #3 - Prod VIP same behavior

Client sends RST after 10 keepalives

Protocol Decode Viewer - webex_98pct_resolved16_56_52edt_startWithDNS_1

Frame	Source	Destination	Size	Send Time	Recv Time	Decode	Labels	Decode Summary
4599	sec-tws-prod-vip.webex.com	JPITTLE-W7.nbttech.com	60	15:56:11.0362	15:56:11.0846	TCP		D=62092 S=443 ACK=2103631714 SEQ=176782290 LEN=0 WIN<<4=33216
4570	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	1384	15:56:11.0750	15:56:11.1234	SSL		Continuation Data
4571	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	993	15:56:11.0751	15:56:11.1235	SSL		Continuation Data
4677	sec-tws-prod-vip.webex.com	JPITTLE-W7.nbttech.com	60	15:56:11.1202	15:56:11.1685	TCP		D=62092 S=443 ACK=2103633983 SEQ=176782290 LEN=0 WIN<<4=30960
4678	sec-tws-prod-vip.webex.com	JPITTLE-W7.nbttech.com	449	15:56:11.1216	15:56:11.1700	SSL		Application Data
5000	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	60	15:56:11.3640	15:56:11.4124	TCP		D=443 S=62092 ACK=176782685 SEQ=2103633983 LEN=0 WIN<<2=65588
6046	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	60	15:56:21.1706	15:56:21.2188	SSL		Continuation Data
6199	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	60	15:56:22.1706	15:56:22.2187	SSL		Continuation Data
6217	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	60	15:56:23.1707	15:56:23.2188	SSL		Continuation Data
6237	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	60	15:56:24.1706	15:56:24.2187	SSL		Continuation Data
6244	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	60	15:56:25.1705	15:56:25.2186	SSL		Continuation Data
6254	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	60	15:56:26.1705	15:56:26.2186	SSL		Continuation Data
6288	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	60	15:56:27.1701	15:56:27.2182	SSL		Continuation Data
6319	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	60	15:56:28.1631	15:56:28.2111	SSL		Continuation Data
6353	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	60	15:56:29.1630	15:56:29.2110	SSL		Continuation Data
6359	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	60	15:56:30.1630	15:56:30.2109	SSL		Continuation Data
6367	JPITTLE-W7.nbttech.com	sec-tws-prod-vip.webex.com	60	15:56:31.1629	15:56:31.2108	TCP		D=443 S=62092 RST ACK=176782685 SEQ=2103633983 LEN=0 WIN<<2=0

```
6046
ETH   Ethernet II, Src: f0:d5:bf:25:2d:3f (f0:d5:bf:25:2d:3f), Dst: 192.168.2.1 (48:f8:b3:91:b1:fe)
IP    Internet Protocol Version 4, Src: 192.168.2.105 (192.168.2.105), Dst: sec-tws-prod-vip.webex.com (66.163.35.36) ID=18509
TCP   D=443 S=62092 ACK=176782685 SEQ=2103633982 LEN=1 WIN<<2=65588
SSL   Continuation Data
HEX   Captured bytes
```

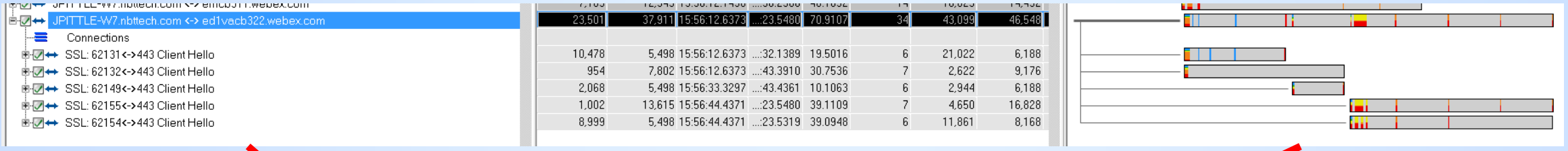
Document Findings

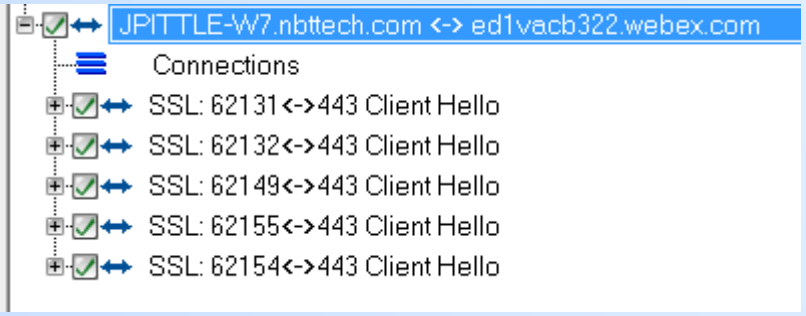
	A	B	C	D	E	F	G
1							
2	**Symptoms found in "98% hang" capture**						
3							
4	**Finding #**	**Symptom**	**Server**	**IP**	**Conn Port#**	**Start Time**	**Stop Time**
5	1	Client does not complete 3-way handshake	nebulam	173.243.0.154	various		
6	2	Server does not ACK keepalive	akamai	23.199.51.101	62057	16:56:14	
7	3	Server does not ACK keepalive	prod-vip	66.163.35.36	62092	16:56:21	
8							
9							
10							
11							

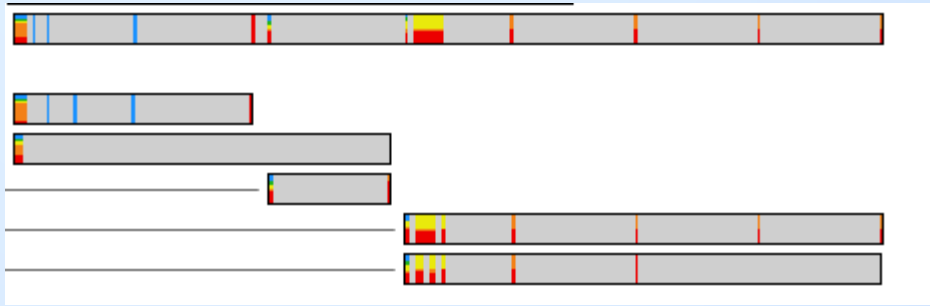
Discussion: Packets show us App and Protocol Behavior

TreeView - Examine another pattern example

Drill Down into Connections for a different Tier Pair

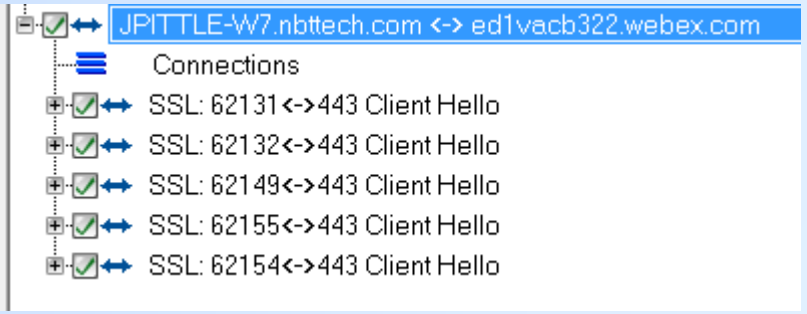


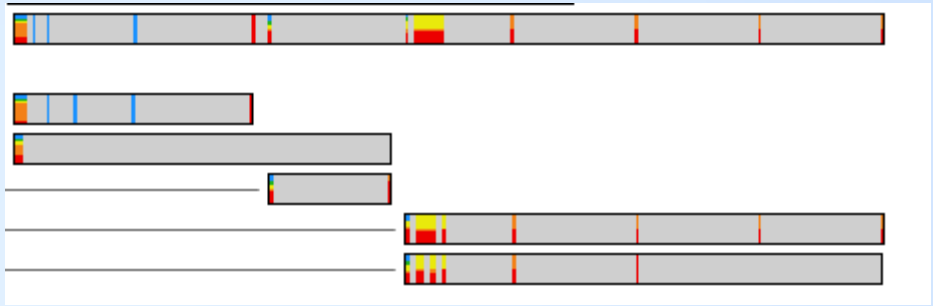




Interpretation & Value of the Visualizations

What can we learn before we start to look at decodes?



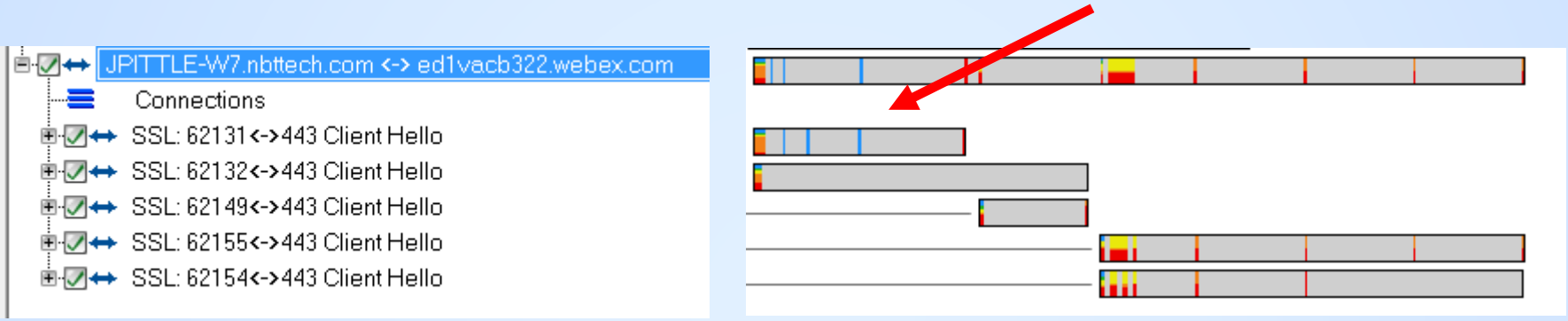


- Conn #1 and #2 opened concurrently
- Conn #3 opened shortly after #1 was reset
- Conn #2 and #3 both closed about the same time
- Conn #4 and #5 opened concurrently after #2 and #3 were closed

- What does this tell us about client thread management?

Interpretation & Value of the Visualizations

What can we learn before we start to look at decodes?



- Sequence and timing progression of blue lines suggest RTO retransmissions

Finding #4: Conn#1 - Unstable connection, five retrans followed by RST (Port 62131)

Protocol Decode Viewer - webex_98pct_resolved16_56_52edt_startWithDNS_1

Frame	Source	Destination	Size	Send Time	Recv Time	Decode	Labels	Decode Summary
5786	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1801	15:56:13.1982	SSL		Application Data
5787	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1802	15:56:13.1982	SSL		Application Data
5788	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1802	15:56:13.1983	SSL		Application Data
5789	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1803	15:56:13.1984	SSL		Application Data
5790	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1804	15:56:13.1984	SSL		Application Data
5791	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1804	15:56:13.1985	SSL		Application Data
5792	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1805	15:56:13.1986	SSL		Application Data
5793	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1806	15:56:13.1986	SSL		Application Data
5794	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1806	15:56:13.1987	SSL		Application Data
5795	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1807	15:56:13.1988	SSL		Application Data
5796	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1808	15:56:13.1988	SSL		Application Data
5797	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1809	15:56:13.1989	SSL		Application Data
5798	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1810	15:56:13.1990	SSL		Application Data
5799	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1810	15:56:13.1991	SSL		Application Data
5800	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1811	15:56:13.1992	SSL		Application Data
5801	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1812	15:56:13.1992	SSL		Application Data
5802	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1812	15:56:13.1993	SSL		Application Data
5803	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1813	15:56:13.1994	SSL		Application Data
5804	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:13.1814	15:56:13.1994	SSL		Application Data
5805	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	427	15:56:13.1815	15:56:13.1995	SSL		Application Data
5810	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	60	15:56:13.1938	15:56:13.2119	TCP		D=62131 S=443 ACK=775463851 SEQ=2605151963 LEN=0 WIN<<4=38016
5835	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	1384	15:56:13.5170	15:56:13.5351	SSL	Retransmission of fram...	Application Data (Retransmission of frame 5757)
5842	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	1384	15:56:14.1169	15:56:14.1351	SSL	Retransmission of fram...	Application Data (Retransmission of frame 5757)
5865	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	1384	15:56:15.3168	15:56:15.3352	SSL	Retransmission of fram...	Application Data (Retransmission of frame 5757)
5909	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	1384	15:56:17.7141	15:56:17.7328	SSL	Retransmission of fram...	Application Data (Retransmission of frame 5757)
6214	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	1384	15:56:22.5188	15:56:22.5383	SSL	Retransmission of fram...	Application Data (Retransmission of frame 5757)
6603	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:32.1179	15:56:32.1389	TCP		D=443 S=62131 RST ACK=2605151963 SEQ=775465181 LEN=0 WIN<<2=0

Document Findings

	A	B	C	D	E	F
1						
2	**Symptoms found in "98% hang" capture**					
3						
4	**Finding #**	**Symptom**	**Server**	**IP**	**Conn Port#**	**Start Time**
5	1	Client does not complete 3-way handshake	nebulam	173.243.0.154	various	13:56:04
6	2	Server does not ACK keepalive	akamai	23.199.51.101	62057	16:56:14
7	3	Server does not ACK keepalive	prod-vip	66.163.35.36	62092	16:56:21
8	4	burst of payload sizes of 85 bytes, followed by retrans of full mss	ed1vab322	64.68.110.77	62131	16:56:13

Conn #2 - “Companion Connection” flows in the opposite direction, no retrans (port 62132)

Client closes with RST about the same time as the earlier connection

Protocol Decode Viewer - webex_98pct_resolved16_56_52edt_startWithDNS_1

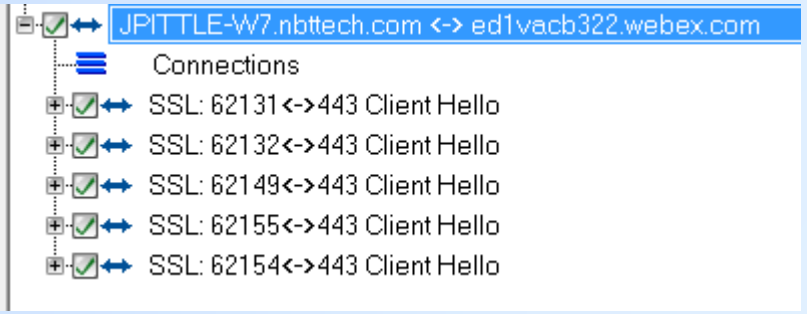
Frame	Source	Destination	Size	Send Time	Recv Time	Decode	Labels	Decode Summary
5753	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.1602	15:56:13.1769	SSL		Application Data
5751	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.1750	15:56:13.1931	TCP		D=443 S=62132 ACK=5772218 SEQ=506799472 LEN=0 WIN<<2=66500
5754	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.1769	15:56:13.1931	TCP		D=443 S=62132 ACK=5772303 SEQ=506799472 LEN=0 WIN<<2=66412
5808	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.1931	15:56:13.2094	SSL		Application Data
5811	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.1983	15:56:13.2150	SSL		Application Data
5813	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.2002	15:56:13.2169	SSL		Application Data
5815	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.2002	15:56:13.2170	SSL		Application Data
5817	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.2003	15:56:13.2170	SSL		Application Data
5819	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.2003	15:56:13.2170	SSL		Application Data
5821	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.2003	15:56:13.2171	SSL		Application Data
5823	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.2004	15:56:13.2171	SSL		Application Data
5825	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.2004	15:56:13.2171	SSL		Application Data
5827	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.2004	15:56:13.2172	SSL		Application Data
5829	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.2005	15:56:13.2172	SSL		Application Data
5831	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:13.2005	15:56:13.2172	SSL		Application Data
5809	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.2094	15:56:13.2275	TCP		D=443 S=62132 ACK=5772388 SEQ=506799472 LEN=0 WIN<<2=66328
5812	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.2151	15:56:13.2331	TCP		D=443 S=62132 ACK=5772473 SEQ=506799472 LEN=0 WIN<<2=66244
5814	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.2169	15:56:13.2350	TCP		D=443 S=62132 ACK=5772558 SEQ=506799472 LEN=0 WIN<<2=66160
5816	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.2170	15:56:13.2350	TCP		D=443 S=62132 ACK=5772643 SEQ=506799472 LEN=0 WIN<<2=66072
5818	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.2170	15:56:13.2351	TCP		D=443 S=62132 ACK=5772728 SEQ=506799472 LEN=0 WIN<<2=65988
5820	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.2170	15:56:13.2351	TCP		D=443 S=62132 ACK=5772813 SEQ=506799472 LEN=0 WIN<<2=65904
5822	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.2171	15:56:13.2351	TCP		D=443 S=62132 ACK=5772898 SEQ=506799472 LEN=0 WIN<<2=65820
5824	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.2171	15:56:13.2352	TCP		D=443 S=62132 ACK=5772983 SEQ=506799472 LEN=0 WIN<<2=65732
5826	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.2171	15:56:13.2352	TCP		D=443 S=62132 ACK=5773068 SEQ=506799472 LEN=0 WIN<<2=65648
5828	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.2172	15:56:13.2352	TCP		D=443 S=62132 ACK=5773153 SEQ=506799472 LEN=0 WIN<<2=65564
5830	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.2172	15:56:13.2352	TCP		D=443 S=62132 ACK=5773238 SEQ=506799472 LEN=0 WIN<<2=65480
5832	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:13.2172	15:56:13.2353	TCP		D=443 S=62132 ACK=5773323 SEQ=506799472 LEN=0 WIN<<2=65392
11978	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:43.3745	15:56:43.3910	TCP		D=443 S=62132 RST ACK=5773323 SEQ=506799472 LEN=0 WIN<<2=0

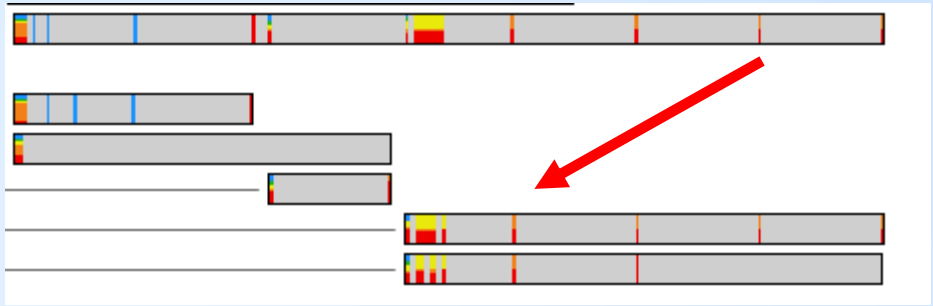
Document Findings

	A	B	C	D	E	F
1						
2	**Symptoms found in "98% hang" capture**					
3						
4	**Finding #**	**Symptom**	**Server**	**IP**	**Conn Port#**	**Start Time**
5	1	Client does not complete 3-way handshake	nebulam	173.243.0.154	various	13:56:04
6	2	Server does not ACK keepalive	akamai	23.199.51.101	62057	16:56:14
7	3	Server does not ACK keepalive	prod-vip	66.163.35.36	62092	16:56:21
8	4	burst of payload sizes of 85 bytes, followed by retrans of full mss	ed1vab322	64.68.110.77	62131	16:56:13
9	5	Unidirectional payload - client to server	ed1vab322	64.68.110.77	62131	16:56:13
10	6	Unidirectional payload - server to client	ed1vab322	64.68.110.77	62132	16:56:13
11	7	Server stops ACK payload packets, client eventually RST connection	ed1vab322		62131	16:56:13
12	8	Client sends RST about the same time as 62131	ed1vab322		62132	16:56:43

Interpretation of the Visualizations

What can we learn before we start to look at decodes?



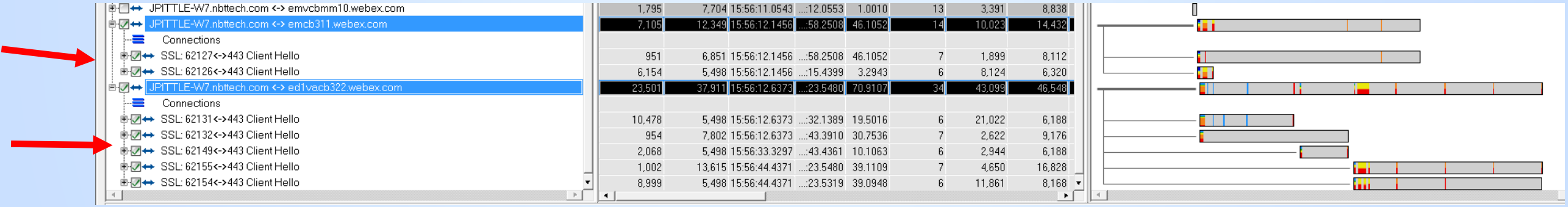


- Concurrent traffic on both connections
- We can't see what is being transferred, but *whatever* is being transferred, is transferred on both connections 4 and 5 near simultaneously

Discuss: App & Protocol Behavior

Zoom in to these six connections

- We'll use a different visualization now to drill deeper into these six connections
- Data Exchange Chart

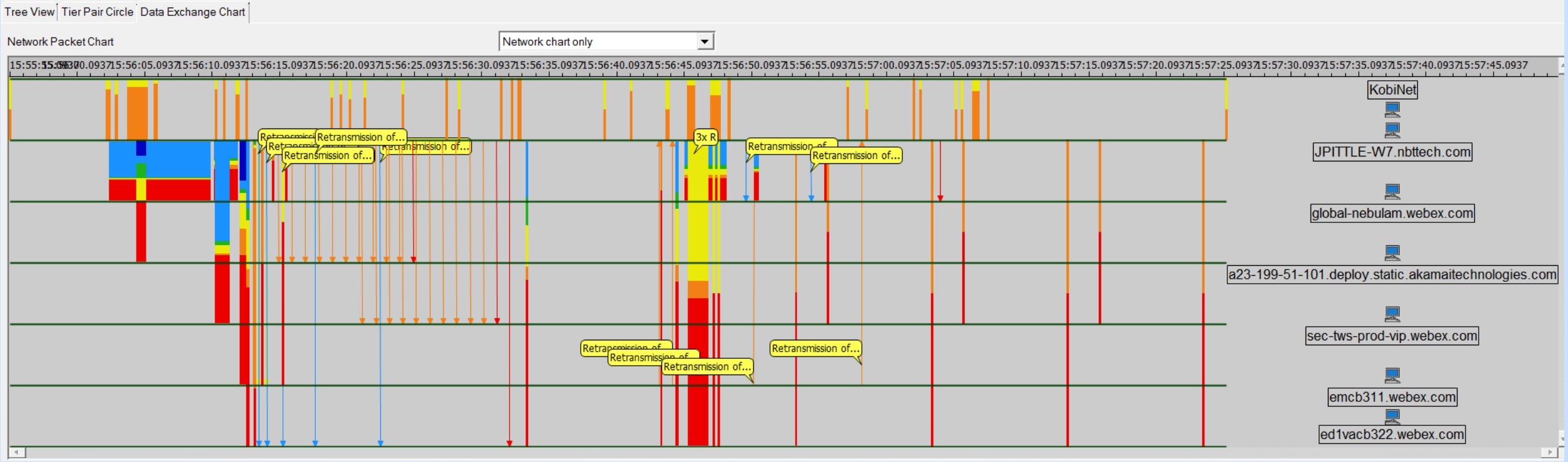


Data Exchange Chart

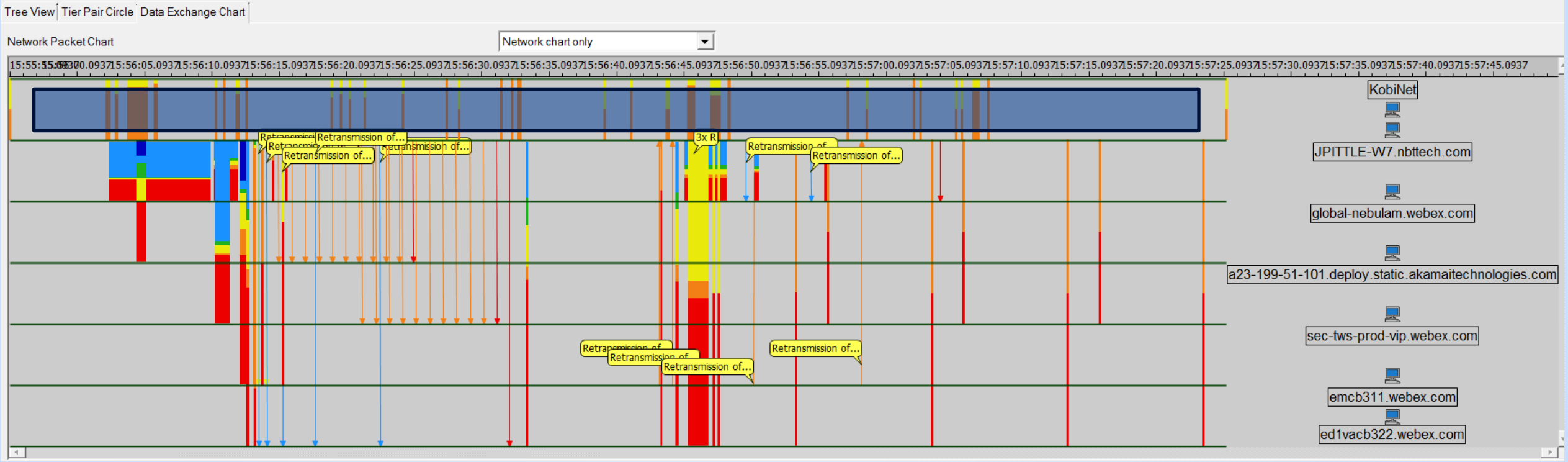
Data Exchange Chart Orientation

Each swim lane provides insights into “When” and “who” patterns

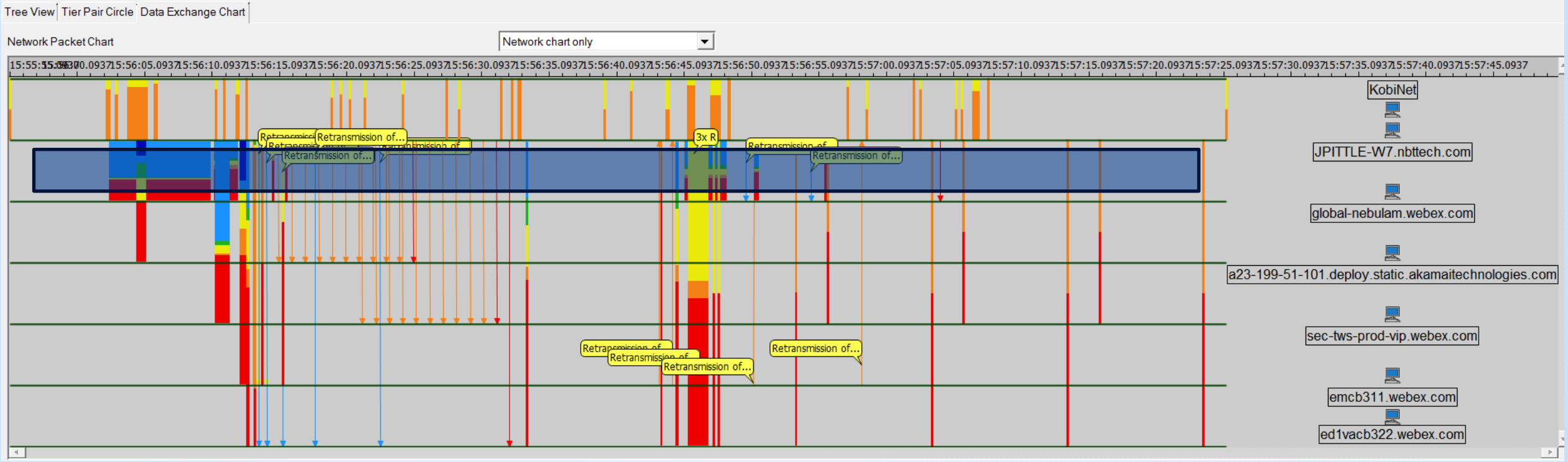
- Time Period: 16:56:02 – 16:57:25



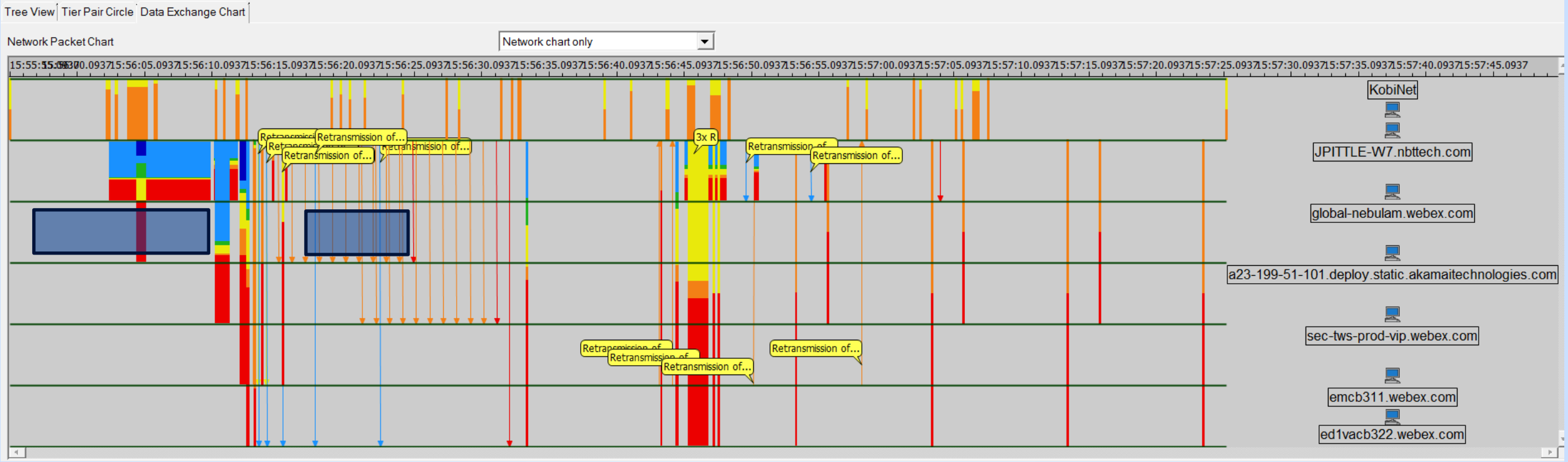
Traffic between client and DNS Server



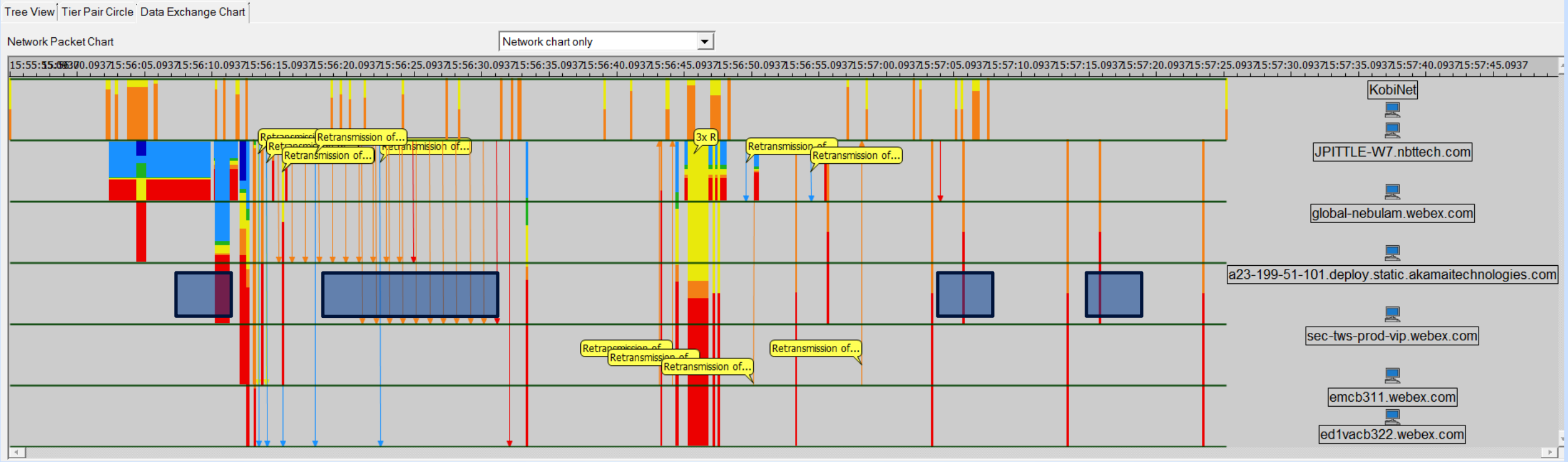
Traffic between client and Global Nebulem



Traffic between client and Akami



Traffic between client and sec-tws-prod-vip

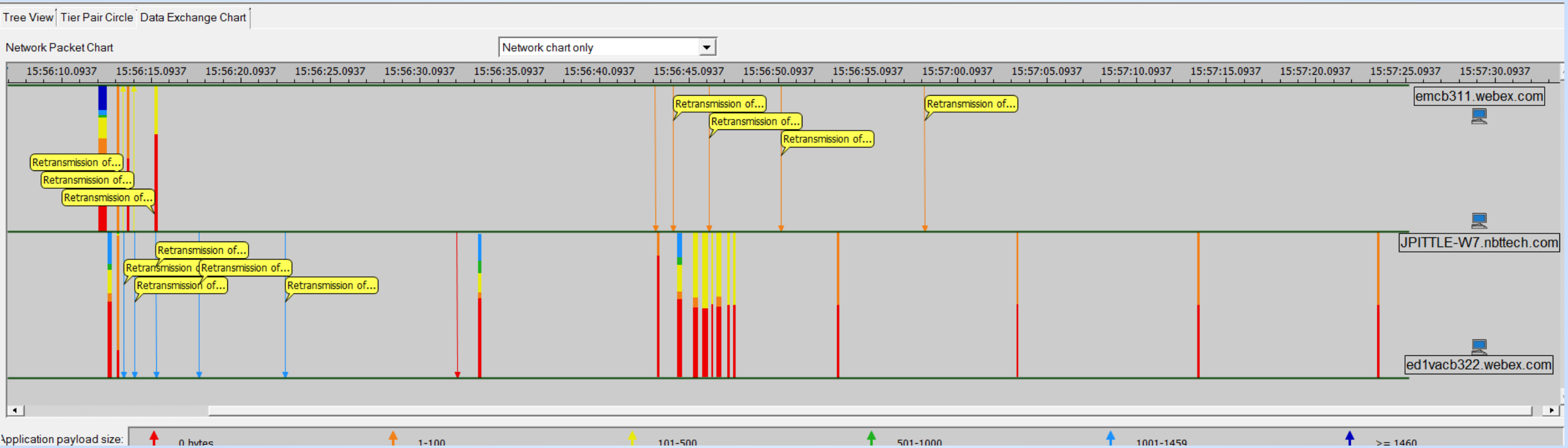


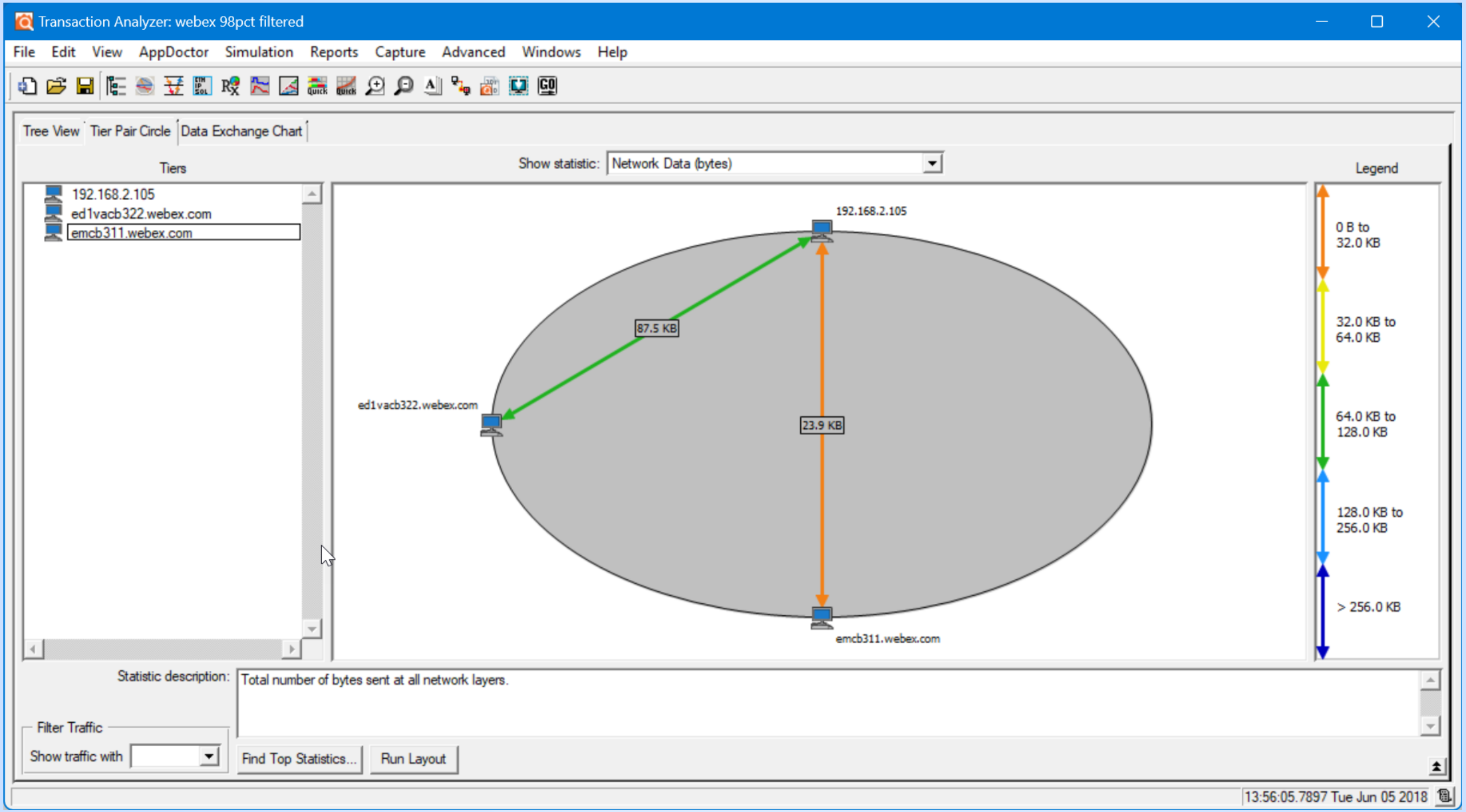
Focus now on two servers

Default “Payload & Retransmission” Visualization

Clearly shows timing of retransmission patterns

- Temp filter and zoom in the time period and isolate client + 2 hosts
- All connections aggregated
- Histogram colors reflect packet sizes within each burst (default)

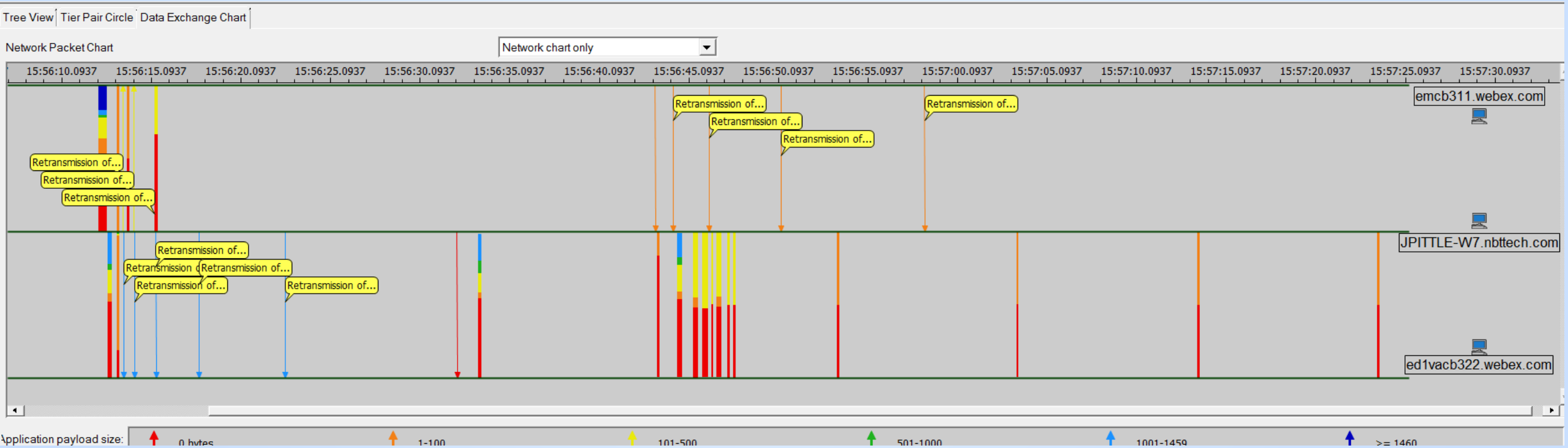



Transaction Analyzer: webex 98pct filtered
File Edit View AppDoctor Simulation Reports Capture Advanced Windows Help
Tree View
Tier Pair Circle
Data Exchange Chart
Tiers
192.168.2.105
ed1vacb322.webex.com
emcb311.webex.com
Show statistic:
Network Data (bytes)
Legend
192.168.2.105
87.5 KB
ed1vacb322.webex.com
23.9 KB
emcb311.webex.com
0 B to 32.0 KB
32.0 KB to 64.0 KB
64.0 KB to 128.0 KB
128.0 KB to 256.0 KB
> 256.0 KB
Statistic description:
Total number of bytes sent at all network layers.
Filter Traffic
Show traffic with
Find Top Statistics...
Run Layout
13:56:05.7897 Tue Jun 05 2018

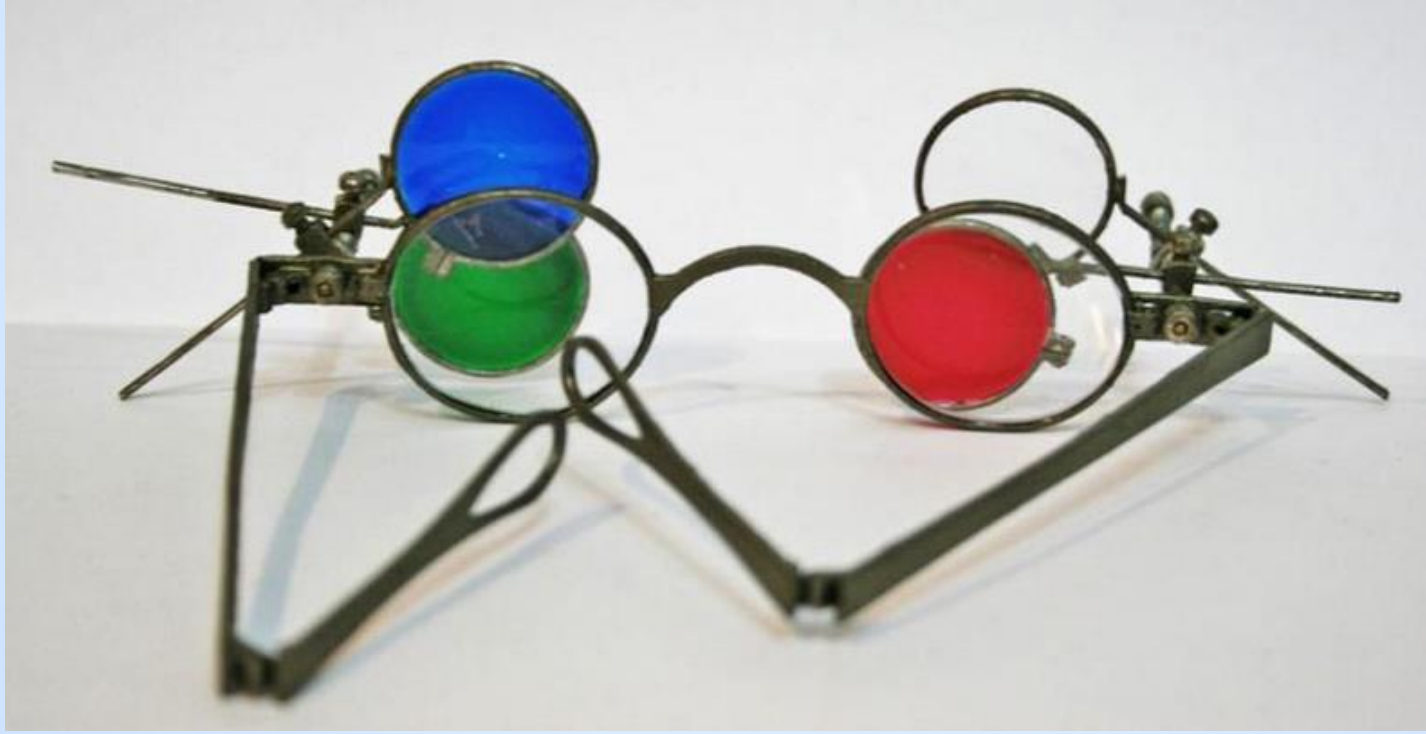
Default “Payload & Retransmission” Visualization

Clearly shows timing of retransmission patterns

- Temp filter and zoom in the time period and isolate client + 2 hosts
- All connections aggregated
- Histogram colors reflect packet sizes within each burst (default)



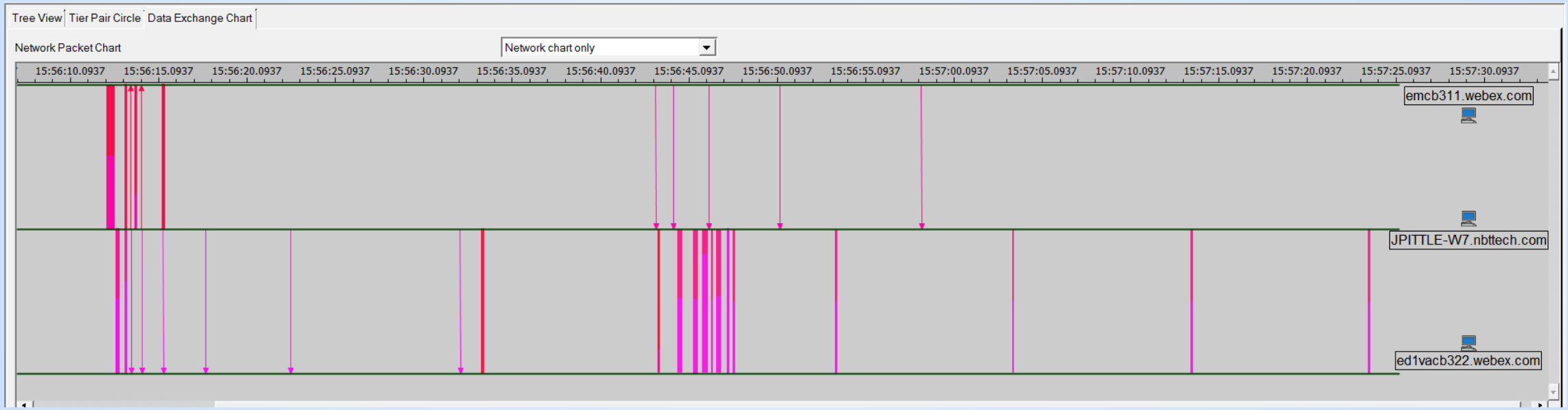
Switching Lens, Same Connections



Switch to “colorize connections” visualization

Same traffic with different coloring scheme…

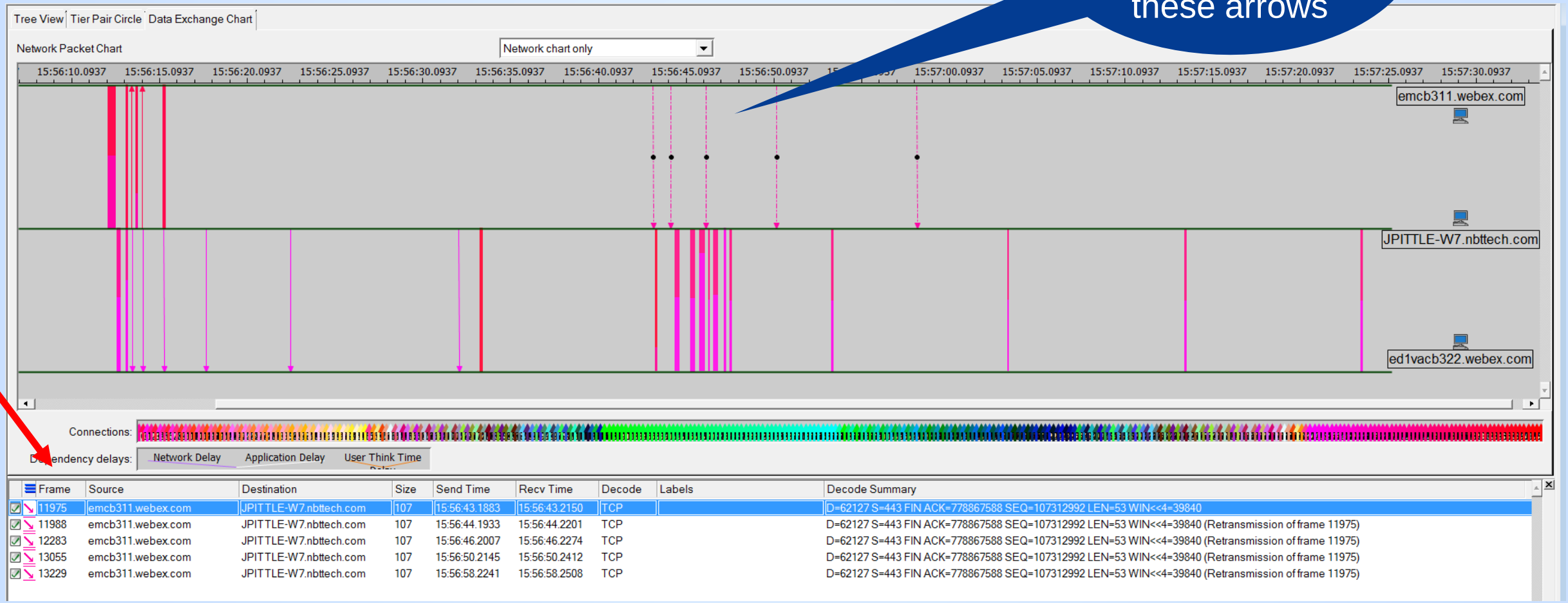
- Now you can see different connections firing at the same time vs. all connections sharing the same histogram
- Select a block or arrow to see summary decodes



Slide Sequence for Discussion

Click through each slide for commentary

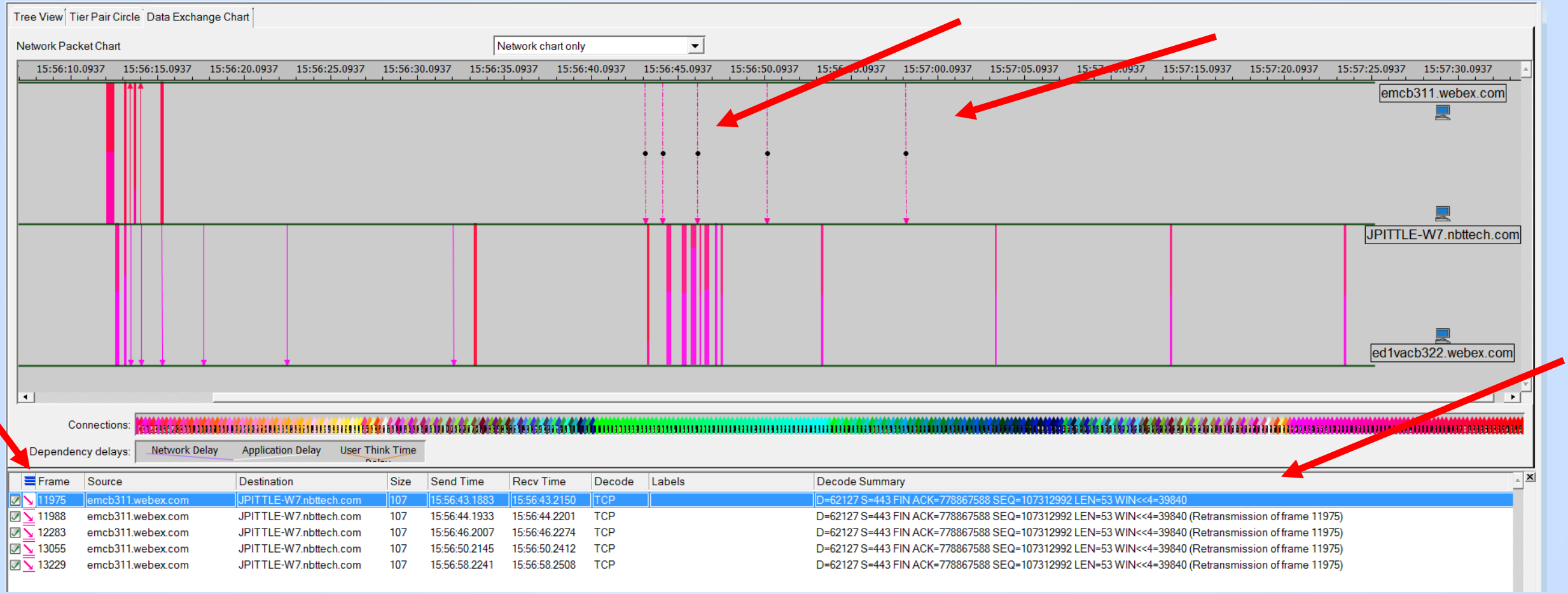
Left Mouse click and drag across to select these arrows



Frame	Source	Destination	Size	Send Time	Recv Time	Decode	Labels	Decode Summary
11975	emcb311.webex.com	JPITTLE-W7.nbttech.com	107	15:56:43.1883	15:56:43.2150	TCP		D=62127 S=443 FIN ACK=778867588 SEQ=107312992 LEN=53 WIN<<4=39840
11988	emcb311.webex.com	JPITTLE-W7.nbttech.com	107	15:56:44.1933	15:56:44.2201	TCP		D=62127 S=443 FIN ACK=778867588 SEQ=107312992 LEN=53 WIN<<4=39840 (Retransmission of frame 11975)
12283	emcb311.webex.com	JPITTLE-W7.nbttech.com	107	15:56:46.2007	15:56:46.2274	TCP		D=62127 S=443 FIN ACK=778867588 SEQ=107312992 LEN=53 WIN<<4=39840 (Retransmission of frame 11975)
13055	emcb311.webex.com	JPITTLE-W7.nbttech.com	107	15:56:50.2145	15:56:50.2412	TCP		D=62127 S=443 FIN ACK=778867588 SEQ=107312992 LEN=53 WIN<<4=39840 (Retransmission of frame 11975)
13229	emcb311.webex.com	JPITTLE-W7.nbttech.com	107	15:56:58.2241	15:56:58.2508	TCP		D=62127 S=443 FIN ACK=778867588 SEQ=107312992 LEN=53 WIN<<4=39840 (Retransmission of frame 11975)

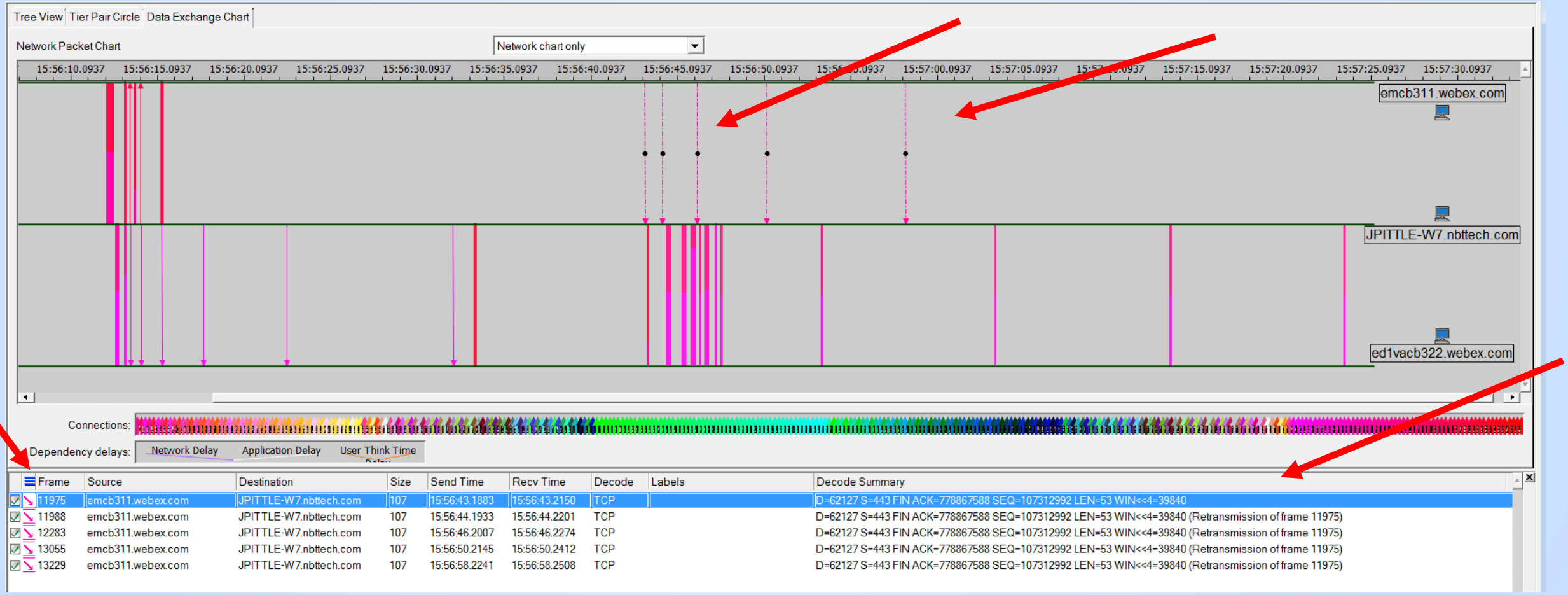
Show summary decodes

Click an arrow / block or “drag” across multiple groups



Server wants to close connection (FIN)

Notice client (webex process) does not respond to FIN, server has to retransmit



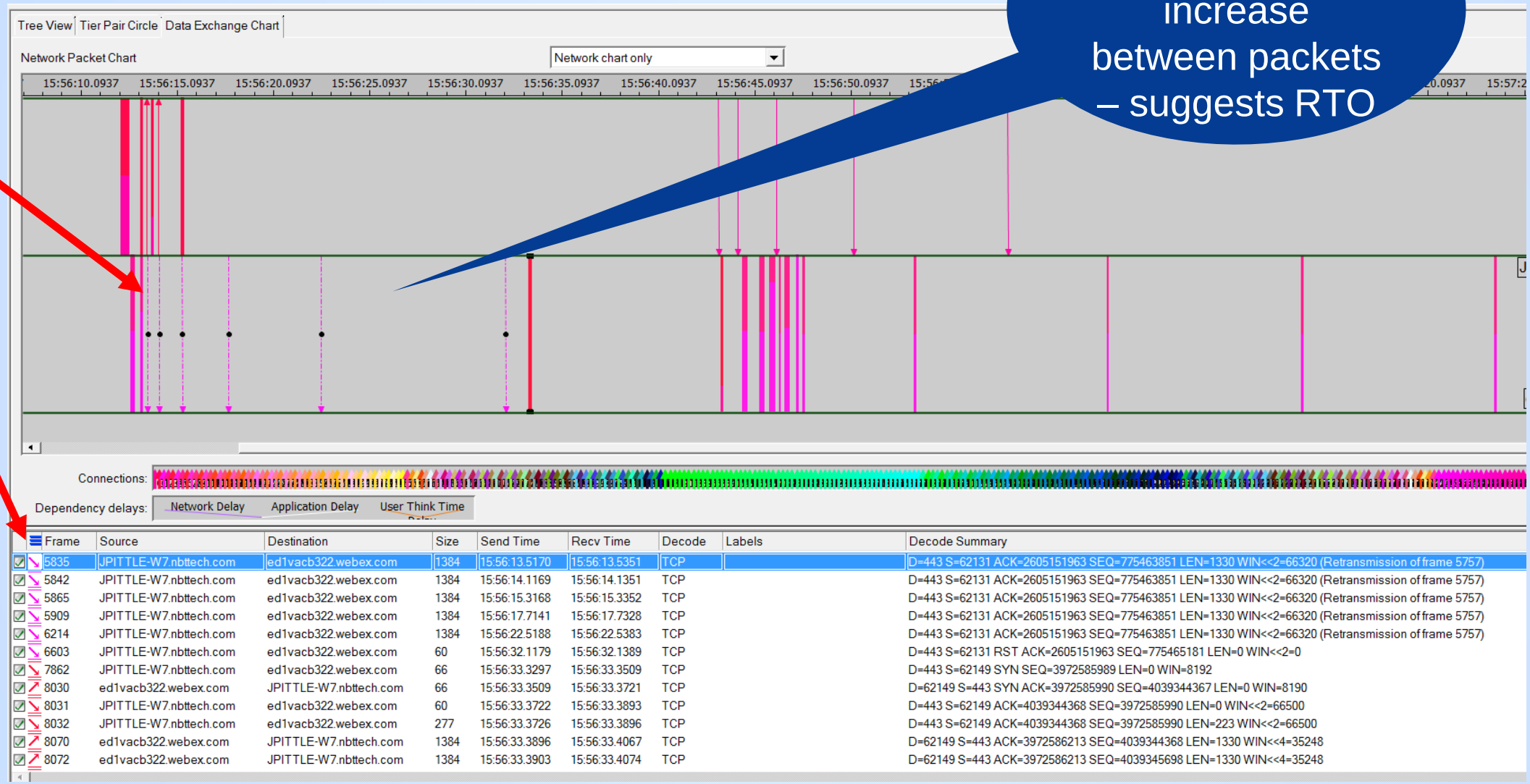
Frame	Source	Destination	Size	Send Time	Recv Time	Decode	Labels	Decode Summary
11975	emcb311.webex.com	JPITTLE-W7.nbttech.com	107	15:56:43.1883	15:56:43.2150	TCP		D=62127 S=443 FIN ACK=778867588 SEQ=107312992 LEN=53 WIN<<4=39840
11988	emcb311.webex.com	JPITTLE-W7.nbttech.com	107	15:56:44.1933	15:56:44.2201	TCP		D=62127 S=443 FIN ACK=778867588 SEQ=107312992 LEN=53 WIN<<4=39840 (Retransmission of frame 11975)
12283	emcb311.webex.com	JPITTLE-W7.nbttech.com	107	15:56:46.2007	15:56:46.2274	TCP		D=62127 S=443 FIN ACK=778867588 SEQ=107312992 LEN=53 WIN<<4=39840 (Retransmission of frame 11975)
13055	emcb311.webex.com	JPITTLE-W7.nbttech.com	107	15:56:50.2145	15:56:50.2412	TCP		D=62127 S=443 FIN ACK=778867588 SEQ=107312992 LEN=53 WIN<<4=39840 (Retransmission of frame 11975)
13229	emcb311.webex.com	JPITTLE-W7.nbttech.com	107	15:56:58.2241	15:56:58.2508	TCP		D=62127 S=443 FIN ACK=778867588 SEQ=107312992 LEN=53 WIN<<4=39840 (Retransmission of frame 11975)

Document Findings

	A	B	C	D	E	F
1						
2	**Symptoms found in "98% hang" capture**					
3						
4	**Finding #**	**Symptom**	**Server**	**IP**	**Conn Port#**	**Start Time**
5	1	Client does not complete 3-way handshake	nebulam	173.243.0.154	various	13:56:04
6	2	Server does not ACK keepalive	akamai	23.199.51.101	62057	16:56:14
7	3	Server does not ACK keepalive	prod-vip	66.163.35.36	62092	16:56:21
8	4	burst of payload sizes of 85 bytes, followed by retrans of full mss	ed1vab322	64.68.110.77	62131	16:56:13
9	5	Unidirectional payload - client to server	ed1vab322	64.68.110.77	62131	16:56:13
10	6	Unidirectional payload - server to client	ed1vab322	64.68.110.77	62132	16:56:13
11	7	Server stops ACK payload packets, client eventually RST connection	ed1vab322		62131	16:56:13
12	8	Client sends RST about the same time as 62131	ed1vab322		62132	16:56:43
13	9	Servers sends FIN, but client does not respond. Server retransmits then finally gives up	emcb311		62127	16:56:43

Examine more highlighted traff

Notice the exponential increase between packets – suggests RTO



Frame	Source	Destination	Size	Send Time	Recv Time	Decode	Labels	Decode Summary
5835	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	1384	15:56:13.5170	15:56:13.5351	TCP		D=443 S=62131 ACK=2605151963 SEQ=775463851 LEN=1330 WIN<<2=66320 (Retransmission of frame 5757)
5842	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	1384	15:56:14.1169	15:56:14.1351	TCP		D=443 S=62131 ACK=2605151963 SEQ=775463851 LEN=1330 WIN<<2=66320 (Retransmission of frame 5757)
5865	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	1384	15:56:15.3168	15:56:15.3352	TCP		D=443 S=62131 ACK=2605151963 SEQ=775463851 LEN=1330 WIN<<2=66320 (Retransmission of frame 5757)
5909	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	1384	15:56:17.7141	15:56:17.7328	TCP		D=443 S=62131 ACK=2605151963 SEQ=775463851 LEN=1330 WIN<<2=66320 (Retransmission of frame 5757)
6214	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	1384	15:56:22.5188	15:56:22.5383	TCP		D=443 S=62131 ACK=2605151963 SEQ=775463851 LEN=1330 WIN<<2=66320 (Retransmission of frame 5757)
6603	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:32.1179	15:56:32.1389	TCP		D=443 S=62131 RST ACK=2605151963 SEQ=775465181 LEN=0 WIN<<2=0
7862	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	66	15:56:33.3297	15:56:33.3509	TCP		D=443 S=62149 SYN SEQ=3972585989 LEN=0 WIN=8192
8030	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	66	15:56:33.3509	15:56:33.3721	TCP		D=62149 S=443 SYN ACK=3972585990 SEQ=4039344367 LEN=0 WIN=8190
8031	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:33.3722	15:56:33.3893	TCP		D=443 S=62149 ACK=4039344368 SEQ=3972585990 LEN=0 WIN<<2=66500
8032	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	277	15:56:33.3726	15:56:33.3896	TCP		D=443 S=62149 ACK=4039344368 SEQ=3972585990 LEN=223 WIN<<2=66500
8070	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	1384	15:56:33.3896	15:56:33.4067	TCP		D=62149 S=443 ACK=3972586213 SEQ=4039344368 LEN=1330 WIN<<4=35248
8072	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	1384	15:56:33.3903	15:56:33.4074	TCP		D=62149 S=443 ACK=3972586213 SEQ=4039345698 LEN=1330 WIN<<4=35248

Discussion

- From the traffic we can see the Webex client process is managing many connections to many servers
- Some of the traffic is asynchronous, which suggests a proprietary protocol contract between client and the servers
- Client would need to be responsible for some aspects error recovery
- Above we can see client is not responding to FIN from server, this is usually the TCP stack's responsibility
  - suspect client thread is interacting with the client OS TCP stack using advanced features / low level interfaces (guessing)

Burst of new DNS queries at 16:56:45

Could this mean client is starting over?

Protocol Decode Viewer - webex_98pct_resolved16_56_52edt_startWithDNS_1

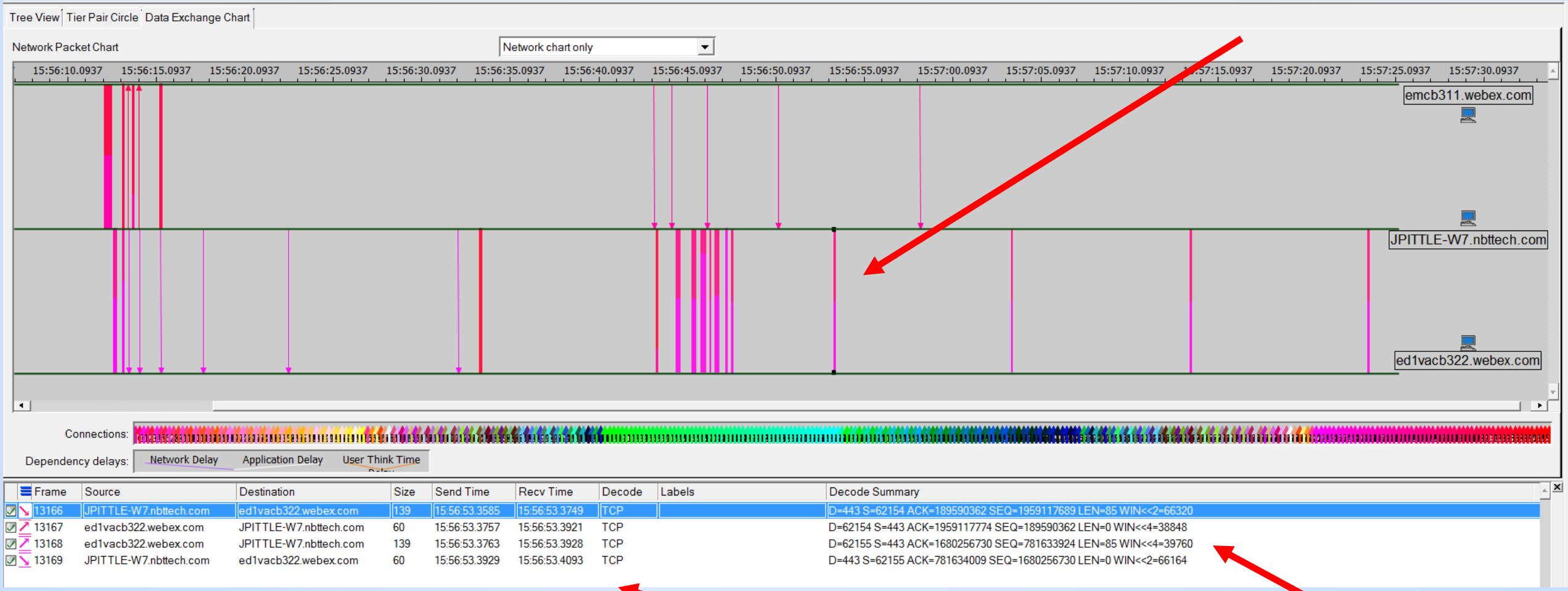
Frame	Source	Destination	Size	Send Time	Recv Time	Decode	Labels	Decode Summary
12048	JPITTLE-W7.nbttech.com	KobiNet	78	15:56:45.3122	15:56:45.3122	DNS		Standard query 0xc40d A riverbed.webex.com
12058	JPITTLE-W7.nbttech.com	KobiNet	86	15:56:45.3392	15:56:45.3392	DNS		Standard query 0x43ed A sec-tws-prod-vip.webex.com
12059	JPITTLE-W7.nbttech.com	KobiNet	86	15:56:45.3392	15:56:45.3392	DNS		Standard query 0xd9d5 A sec-tws-prod-vip.webex.com
12060	KobiNet	JPITTLE-W7.nbttech.com	102	15:56:45.3422	15:56:45.3422	DNS		Standard query response 0xd9d5 A 66.163.35.36
12061	KobiNet	JPITTLE-W7.nbttech.com	102	15:56:45.3432	15:56:45.3432	DNS		Standard query response 0x43ed A 66.163.35.36
12062	JPITTLE-W7.nbttech.com	KobiNet	86	15:56:45.3453	15:56:45.3453	DNS		Standard query 0x684e A sec-tws-prod-vip.webex.com
12064	KobiNet	JPITTLE-W7.nbttech.com	102	15:56:45.3492	15:56:45.3492	DNS		Standard query response 0x684e A 66.163.35.36
12065	JPITTLE-W7.nbttech.com	KobiNet	86	15:56:45.3498	15:56:45.3498	DNS		Standard query 0xd0b7 A sec-tws-prod-vip.webex.com
12066	KobiNet	JPITTLE-W7.nbttech.com	102	15:56:45.3518	15:56:45.3518	DNS		Standard query response 0xd0b7 A 66.163.35.36
12067	JPITTLE-W7.nbttech.com	KobiNet	86	15:56:45.3523	15:56:45.3523	DNS		Standard query 0xf4ab AAAA sec-tws-prod-vip.webex.com
12068	JPITTLE-W7.nbttech.com	KobiNet	78	15:56:45.3557	15:56:45.3557	DNS		Standard query 0xf0ce A riverbed.webex.com
12069	KobiNet	JPITTLE-W7.nbttech.com	86	15:56:45.3592	15:56:45.3592	DNS		Standard query response 0xf4ab
12093	KobiNet	JPITTLE-W7.nbttech.com	145	15:56:45.4097	15:56:45.4097	DNS		Standard query response 0xc40d CNAME nebulam.webex.com CNAME global-nebulam.webex.com A 173.243.0.154
12095	JPITTLE-W7.nbttech.com	KobiNet	78	15:56:45.4103	15:56:45.4103	DNS		Standard query 0xe9dd A riverbed.webex.com
12100	KobiNet	JPITTLE-W7.nbttech.com	145	15:56:45.4321	15:56:45.4321	DNS		Standard query response 0xe9dd CNAME nebulam.webex.com CNAME global-nebulam.webex.com A 173.243.0.154
12101	JPITTLE-W7.nbttech.com	KobiNet	84	15:56:45.4326	15:56:45.4326	DNS		Standard query 0x1ec8 A global-nebulam.webex.com
12103	KobiNet	JPITTLE-W7.nbttech.com	100	15:56:45.4382	15:56:45.4382	DNS		Standard query response 0x1ec8 A 173.243.0.154
12125	KobiNet	JPITTLE-W7.nbttech.com	145	15:56:45.5222	15:56:45.5222	DNS		Standard query response 0xf0ce CNAME nebulam.webex.com CNAME global-nebulam.webex.com A 173.243.0.154
12126	JPITTLE-W7.nbttech.com	KobiNet	84	15:56:45.5231	15:56:45.5231	DNS		Standard query 0x0eab AAAA global-nebulam.webex.com
12168	KobiNet	JPITTLE-W7.nbttech.com	84	15:56:45.6321	15:56:45.6321	DNS		Standard query response 0x0eab
12202	JPITTLE-W7.nbttech.com	KobiNet	81	15:56:45.8319	15:56:45.8319	DNS		Standard query 0xae08 A js-agent.newrelic.com
12203	JPITTLE-W7.nbttech.com	KobiNet	81	15:56:45.8319	15:56:45.8319	DNS		Standard query 0x7b40 A js-agent.newrelic.com
12204	KobiNet	JPITTLE-W7.nbttech.com	138	15:56:45.8461	15:56:45.8461	DNS		Standard query response 0xae08 CNAME f4.shared.global.fastly.net A 151.101.6.110
12205	KobiNet	JPITTLE-W7.nbttech.com	138	15:56:45.8462	15:56:45.8462	DNS		Standard query response 0x7b40 CNAME f4.shared.global.fastly.net A 151.101.6.110
12206	JPITTLE-W7.nbttech.com	KobiNet	87	15:56:45.8517	15:56:45.8517	DNS		Standard query 0xdd93 A f4.shared.global.fastly.net
12210	JPITTLE-W7.nbttech.com	KobiNet	81	15:56:45.8539	15:56:45.8539	DNS		Standard query 0x34fa A js-agent.newrelic.com
12211	KobiNet	JPITTLE-W7.nbttech.com	103	15:56:45.8561	15:56:45.8561	DNS		Standard query response 0xdd93 A 151.101.6.110
12212	JPITTLE-W7.nbttech.com	KobiNet	87	15:56:45.8566	15:56:45.8566	DNS		Standard query 0xad69 AAAA f4.shared.global.fastly.net
12213	KobiNet	JPITTLE-W7.nbttech.com	138	15:56:45.8590	15:56:45.8590	DNS		Standard query response 0x34fa CNAME f4.shared.global.fastly.net A 151.101.6.110
12218	KobiNet	JPITTLE-W7.nbttech.com	148	15:56:45.8724	15:56:45.8724	DNS		Standard query response 0xad69
12229	JPITTLE-W7.nbttech.com	KobiNet	75	15:56:45.9050	15:56:45.9050	DNS		Standard query 0x329c A bam.nr-data.net
12230	JPITTLE-W7.nbttech.com	KobiNet	75	15:56:45.9050	15:56:45.9050	DNS		Standard query 0x76dc A bam.nr-data.net
12236	KobiNet	JPITTLE-W7.nbttech.com	139	15:56:45.9093	15:56:45.9093	DNS		Standard query response 0x329c A 162.247.242.18 A 162.247.242.21 A 162.247.242.19 A 162.247.242.20
12237	KobiNet	JPITTLE-W7.nbttech.com	139	15:56:45.9093	15:56:45.9093	DNS		Standard query response 0x76dc A 162.247.242.20 A 162.247.242.18 A 162.247.242.21 A 162.247.242.19

Document Findings

	A	B	C	D	E	F
1						
2	**Symptoms found in "98% hang" capture**					
3						
4	**Finding #**	**Symptom**	**Server**	**IP**	**Conn Port#**	**Start Time**
5	1	Client does not complete 3-way handshake	nebulam	173.243.0.154	various	13:56:04
6	2	Server does not ACK keepalive	akamai	23.199.51.101	62057	16:56:14
7	3	Server does not ACK keepalive	prod-vip	66.163.35.36	62092	16:56:21
8	4	burst of payload sizes of 85 bytes, followed by retrans of full mss	ed1vab322	64.68.110.77	62131	16:56:13
9	5	Unidirectional payload - client to server	ed1vab322	64.68.110.77	62131	16:56:13
10	6	Unidirectional payload - server to client	ed1vab322	64.68.110.77	62132	16:56:13
11	7	Server stops ACK payload packets, client eventually RST connection	ed1vab322		62131	16:56:13
12	8	Client sends RST about the same time as 62131	ed1vab322		62132	16:56:43
13	9	Servers sends FIN, but client does not respond. Server retransmits then finally gives up	emcb311		62127	16:56:43
14	10	Client seems to start over again with basic DNS	192.168.2.1			16:56:45

Sample (Apparent) Healthy Keepalive Mechanism

Notice two “one-way” connections are involved



Frame	Source	Destination	Size	Send Time	Recv Time	Decode	Labels	Decode Summary
13166	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:53.3585	15:56:53.3749	TCP		D=443 S=62154 ACK=189590362 SEQ=1959117689 LEN=85 WIN<<2=66320
13167	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	60	15:56:53.3757	15:56:53.3921	TCP		D=62154 S=443 ACK=1959117774 SEQ=189590362 LEN=0 WIN<<4=38848
13168	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:53.3763	15:56:53.3928	TCP		D=62155 S=443 ACK=1680256730 SEQ=781633924 LEN=85 WIN<<4=39760
13169	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	60	15:56:53.3929	15:56:53.4093	TCP		D=443 S=62155 ACK=781634009 SEQ=1680256730 LEN=0 WIN<<2=66164

Possibly Normal Behavior

After 2nd round of DNS queries and new connections

- Some sort of payload based keepalive pattern every 10 seconds
- Hypothesis – this is what normal looks like

Frame	Source	Destination	Size	Send Time	Recv Time	Decode	Labels	Decode Summary
13166	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:56:53.3585	15:56:53.3749	TCP		D=443 S=62154 ACK=189590362 SEQ=1959117689 LEN=85 WIN<<2=66320
13168	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:56:53.3763	15:56:53.3928	TCP		D=62155 S=443 ACK=1680256730 SEQ=781633924 LEN=85 WIN<<4=39760
13326	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:57:03.4051	15:57:03.4215	TCP		D=443 S=62154 ACK=189590362 SEQ=1959117774 LEN=85 WIN<<2=66320
13328	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:57:03.4322	15:57:03.4487	TCP		D=62155 S=443 ACK=1680256730 SEQ=781634009 LEN=85 WIN<<4=39760
13734	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:57:13.4505	15:57:13.4669	TCP		D=443 S=62154 ACK=189590362 SEQ=1959117859 LEN=85 WIN<<2=66320
13736	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:57:13.4693	15:57:13.4858	TCP		D=62155 S=443 ACK=1680256730 SEQ=781634094 LEN=85 WIN<<4=39760
15295	JPITTLE-W7.nbttech.com	ed1vacb322.webex.com	139	15:57:23.4973	15:57:23.5137	TCP		D=443 S=62154 ACK=189590362 SEQ=1959117944 LEN=85 WIN<<2=66320
15296	ed1vacb322.webex.com	JPITTLE-W7.nbttech.com	139	15:57:23.5149	15:57:23.5315	TCP		D=62155 S=443 ACK=1680256730 SEQ=781634179 LEN=85 WIN<<4=39760

Document Findings

	A	B	C	D	E	F
1						
2	**Symptoms found in "98% hang" capture**					
3						
4	**Finding #**	**Symptom**	**Server**	**IP**	**Conn Port#**	**Start Time**
5	1	Client does not complete 3-way handshake	nebulam	173.243.0.154	various	13:56:04
6	2	Server does not ACK keepalive	akamai	23.199.51.101	62057	16:56:14
7	3	Server does not ACK keepalive	prod-vip	66.163.35.36	62092	16:56:21
8	4	burst of payload sizes of 85 bytes, followed by retrans of full mss	ed1vab322	64.68.110.77	62131	16:56:13
9	5	Unidirectional payload - client to server	ed1vab322	64.68.110.77	62131	16:56:13
10	6	Unidirectional payload - server to client	ed1vab322	64.68.110.77	62132	16:56:13
11	7	Server stops ACK payload packets, client eventually RST connection	ed1vab322		62131	16:56:13
12	8	Client sends RST about the same time as 62131	ed1vab322		62132	16:56:43
13	9	Servers sends FIN, but client does not respond. Server retransmits then finally gives up	emcb311		62127	16:56:43
14	10	Client seems to start over again with basic DNS	192.168.2.1			16:56:45
15	11	Evidence of healthy keep alive traffic	ed1vab322		62154, 62155	15:56:53

Quick Overview - Analysis Findings

Variety of connection synchronization issues

- For many connections, WebEx client will open the connection, but not respond to SYN-ACK from server
- For two servers in particular the server side does not ACK keepalive packets (having payload LEN=1)
  - Either the host is overloaded or keepalive packets are getting dropped
  - Servers with this behavior: Akamai and prod-VIP
- For some connections, the client sends FIN, but server then sends more payload, client then sends RST
  - This suggests the client and server are not in synch

How would you do this analysis in Wireshark?

Lab #2

- Open the pcap
- Open the display filter text file you downloaded from packet-foo
- Apply the display filter and create a new pcap with only the packets that match the display filter
- Close the big pcap and open the one you just created
- Open Expert Info

Expert Info Provided Some Basic Info

Wireshark · Expert Information · webex filtered.pcap

Severity	Summary	Group	Protocol	Count
Error	New fragment overlaps old data (retransmission?)	Malformed	TCP	13
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	1
Warning	D-SACK Sequence	Sequence	TCP	2
Warning	Connection reset (RST)	Sequence	TCP	60
Note	ACK to a TCP keep-alive segment	Sequence	TCP	2
Note	TCP keep-alive segment	Sequence	TCP	23
Note	This frame is a (suspected) retransmission	Sequence	TCP	21
Note	Duplicate ACK (#1)	Sequence	TCP	1
Note	This frame undergoes the connection closing	Sequence	TCP	42
Note	This session reuses previously negotiated keys (Session res...	Sequence	TLS	43
Note	This frame initiates the connection closing	Sequence	TCP	67
Chat	Connection finish (FIN)	Sequence	TCP	109
Chat	TCP window update	Sequence	TCP	10
Chat	Connection establish acknowledge (SYN+ACK): server port...	Sequence	TCP	91
Chat	Connection establish request (SYN): server port 443	Sequence	TCP	91

No display filter set.

Limit to Display Filter Group by summary Search: Show...

Close Help

Packet Lists have value, but getting context is hard

webex filtered.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Delta Time	Source	Destination	Protocol	Length	Info
1	16:55:55.093712	0.000000000	192.168.2.105	192.168.2.1	DNS	83	Standard query 0xd054 A pollserver.lastpass.com
2	16:55:55.114689	0.020977000	192.168.2.1	192.168.2.105	DNS	171	Standard query response 0xd054 A pollserver.lastpass.com CNAME lastpass.com.edgek…
3	16:56:02.228188	7.113499000	192.168.2.105	192.168.2.1	DNS	78	Standard query 0xa512 A riverbed.webex.com
4	16:56:02.433818	0.205630000	192.168.2.1	192.168.2.105	DNS	145	Standard query response 0xa512 A riverbed.webex.com CNAME nebulam.webex.com CNAME…
5	16:56:02.434520	0.000702000	192.168.2.105	173.243.0.154	TCP	66	62037 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
6	16:56:02.434772	0.000252000	192.168.2.105	173.243.0.154	TCP	66	62038 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
7	16:56:02.435025	0.000253000	192.168.2.105	173.243.0.154	TCP	66	62039 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
8	16:56:02.435714	0.000689000	192.168.2.105	192.168.2.1	DNS	84	Standard query 0xee05 A global-nebulam.webex.com
9	16:56:02.441098	0.005384000	192.168.2.1	192.168.2.105	DNS	100	Standard query response 0xee05 A global-nebulam.webex.com A 173.243.0.154
10	16:56:02.441653	0.000555000	192.168.2.105	192.168.2.1	DNS	84	Standard query 0xa856 AAAA global-nebulam.webex.com
11	16:56:02.490796	0.049143000	173.243.0.154	192.168.2.105	TCP	66	443 → 62037 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1330 WS=16 SACK_PERM=1
12	16:56:02.490895	0.000099000	192.168.2.105	173.243.0.154	TCP	60	62037 → 443 [ACK] Seq=1 Ack=1 Win=66500 Len=0
13	16:56:02.491487	0.000592000	173.243.0.154	192.168.2.105	TCP	66	443 → 62038 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1330 WS=16 SACK_PERM=1
14	16:56:02.491552	0.000065000	192.168.2.105	173.243.0.154	TCP	60	62038 → 443 [ACK] Seq=1 Ack=1 Win=66500 Len=0
15	16:56:02.493633	0.002081000	192.168.2.105	173.243.0.154	TLSv1.2	571	Client Hello
16	16:56:02.496467	0.002834000	192.168.2.105	173.243.0.154	TLSv1.2	571	Client Hello
17	16:56:02.497880	0.001413000	173.243.0.154	192.168.2.105	TCP	66	443 → 62039 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1330 WS=16 SACK_PERM=1
18	16:56:02.497956	0.000076000	192.168.2.105	173.243.0.154	TCP	60	62039 → 443 [ACK] Seq=1 Ack=1 Win=66500 Len=0
19	16:56:02.500821	0.002865000	192.168.2.105	173.243.0.154	TLSv1.2	571	Client Hello
20	16:56:02.547367	0.046546000	173.243.0.154	192.168.2.105	TCP	1384	443 → 62037 [PSH, ACK] Seq=1 Ack=518 Win=34656 Len=1330 [TCP segment of a reassem…
21	16:56:02.549489	0.002122000	173.243.0.154	192.168.2.105	TCP	1384	443 → 62037 [PSH, ACK] Seq=1331 Ack=518 Win=34656 Len=1330 [TCP segment of a reas…
22	16:56:02.549576	0.000087000	192.168.2.105	173.243.0.154	TCP	60	62037 → 443 [ACK] Seq=518 Ack=2661 Win=66500 Len=0

```
> Frame 6181: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits)
> Ethernet II, Src: Cisco-Li_91:b1:fe (48:f8:b3:91:b1:fe), Dst: IntelCor_25:2d:3f (f0:d5:bf:25:2d:3f)
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.105
> User Datagram Protocol, Src Port: 53, Dst Port: 61491
> Domain Name System (response)
```

webex filtered.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Delta Time	Source	Destination	Protocol	Length	Info
5068	16:56:13.217242	0.000011000	192.168.2.105	64.68.110.77	TCP	60	62132 → 443 [ACK] Seq=955 Ack=7718 Win=65480 Len=0
5069	16:56:13.217257	0.000015000	64.68.110.77	192.168.2.105	TLSv1.2	139	Application Data
5070	16:56:13.217268	0.000011000	192.168.2.105	64.68.110.77	TCP	60	62132 → 443 [ACK] Seq=955 Ack=7803 Win=65392 Len=0
5071	16:56:13.477308	0.260040000	192.168.2.105	64.68.101.20	TCP	208	[TCP Retransmission] 62126 → 443 [PSH, ACK] Seq=5895 Ack=5499 Win=64580 …
5072	16:56:13.517045	0.039737000	192.168.2.105	64.68.110.77	TCP	1384	[TCP Retransmission] 62131 → 443 [PSH, ACK] Seq=6026 Ack=5499 Win=66320 …
5073	16:56:13.676985	0.159940000	192.168.2.105	114.29.202.1…	TCP	614	[TCP Retransmission] 62130 → 443 [PSH, ACK] Seq=223 Ack=171 Win=66328 Le…
5074	16:56:13.736104	0.059119000	192.168.2.105	64.68.101.20	TLSv1.2	107	Application Data
5075	16:56:13.736346	0.000242000	192.168.2.105	64.68.101.20	TLSv1.2	107	Application Data
5076	16:56:13.736587	0.000241000	192.168.2.105	64.68.101.20	TCP	60	62126 → 443 [FIN, ACK] Seq=6155 Ack=5499 Win=64580 Len=0
5077	16:56:13.736613	0.000026000	192.168.2.105	64.68.101.20	TCP	60	62127 → 443 [RST, ACK] Seq=952 Ack=6852 Win=0 Len=0
5078	16:56:14.076936	0.340323000	192.168.2.105	64.68.101.20	TCP	314	[TCP Retransmission] 62126 → 443 [FIN, PSH, ACK] Seq=5895 Ack=5499 Win=6…
5079	16:56:14.116949	0.040013000	192.168.2.105	64.68.110.77	TCP	1384	[TCP Retransmission] 62131 → 443 [PSH, ACK] Seq=6026 Ack=5499 Win=66320 …
5080	16:56:14.498285	0.381336000	192.168.2.105	173.243.0.154	TLSv1.2	85	Encrypted Alert
5081	16:56:14.498361	0.000076000	192.168.2.105	173.243.0.154	TCP	60	62058 → 443 [FIN, ACK] Seq=4943 Ack=2147776 Win=262008 Len=0
5082	16:56:14.552994	0.054633000	173.243.0.154	192.168.2.105	TCP	60	443 → 62058 [ACK] Seq=2147776 Ack=4943 Win=40928 Len=0
5083	16:56:14.553035	0.000041000	173.243.0.154	192.168.2.105	TLSv1.2	85	Encrypted Alert
5084	16:56:14.553095	0.000060000	192.168.2.105	173.243.0.154	TCP	60	62058 → 443 [RST, ACK] Seq=4944 Ack=2147807 Win=0 Len=0
5085	16:56:14.557857	0.004762000	173.243.0.154	192.168.2.105	TCP	60	443 → 62058 [ACK] Seq=2147808 Ack=4944 Win=40928 Len=0
5086	16:56:14.972851	0.414994000	192.168.2.105	23.199.51.101	TCP	60	[TCP Keep-Alive] 62057 → 443 [ACK] Seq=2068 Ack=4624 Win=65700 Len=1
5087	16:56:15.076841	0.103990000	192.168.2.105	114.29.202.1…	TCP	614	[TCP Retransmission] 62130 → 443 [PSH, ACK] Seq=223 Ack=171 Win=66328 Le…
5088	16:56:15.277931	0.201090000	192.168.2.105	64.68.101.20	TCP	314	[TCP Retransmission] 62126 → 443 [FIN, PSH, ACK] Seq=5895 Ack=5499 Win=6…
5089	16:56:15.316863	0.038932000	192.168.2.105	64.68.110.77	TCP	1384	[TCP Retransmission] 62131 → 443 [PSH, ACK] Seq=6026 Ack=5499 Win=66320 …
5090	16:56:15.439332	0.122469000	64.68.101.20	192.168.2.105	TCP	66	443 → 62126 [ACK] Seq=5499 Ack=6156 Win=38144 Len=0 SLE=5895 SRE=6049

```
    [Bytes sent since last PSH flag: 154]
  [TCP Analysis Flags]
    [Expert Info (Note/Sequence): This frame is a (suspected) retransmission]
        [This frame is a (suspected) retransmission]
        [Severity level: Note]
```

```
0000  48 f8 b3 91 b1 fe f0 d5  bf 25 2d 3f 08 00 45 00   H······ ·%-?··E·
```

This frame is a (suspected) retransmission (tcp.analysis.retransmission) | Packets: 6246 · Displayed: 6246 (100.0%) | Profile: Default

Filtering and Colorization is Helpful to a Point

webex filtered.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools

ip.addr eq 192.168.2.105 and ip.addr eq 64.68.101.20

webex filtered.pcap

No.	Time	Delta Time	Source	Destination	Protocol	Length	Info
4888	16:56:12.541165	0.006086000	192.168.2.105	64.68.101.20	TLSv1.2	139	Application Data
4893	16:56:12.593702	0.052537000	64.68.101.20	192.168.2.105	TCP	60	443 → 62126 [ACK] Seq=5499 Ack=5895 Win=38384 Len=0
4894	16:56:12.594311	0.000609000	64.68.101.20	192.168.2.105	TLSv1.2	139	Application Data
4895	16:56:12.594387	0.000076000	192.168.2.105	64.68.101.20	TCP	60	62127 → 443 [ACK] Seq=952 Ack=6852 Win=64724 Len=0
4995	16:56:13.177288	0.582901000	192.168.2.105	64.68.101.20	TLSv1.2	139	Application Data
4996	16:56:13.177423	0.000135000	192.168.2.105	64.68.101.20	TLSv1.2	123	Application Data
5071	16:56:13.477308	0.299885000	192.168.2.105	64.68.101.20	TCP	208	[TCP Retransmission] 62126 → 443 [PSH, ACK] Seq=5895 Ack=5499 Win=64580 Len=154
5074	16:56:13.736104	0.258796000	192.168.2.105	64.68.101.20	TLSv1.2	107	Application Data
5075	16:56:13.736346	0.000242000	192.168.2.105	64.68.101.20	TLSv1.2	107	Application Data
5076	16:56:13.736587	0.000241000	192.168.2.105	64.68.101.20	TCP	60	62126 → 443 [FIN, ACK] Seq=6155 Ack=5499 Win=64580 Len=0
5077	16:56:13.736613	0.000026000	192.168.2.105	64.68.101.20	TCP	60	62127 → 443 [RST, ACK] Seq=952 Ack=6852 Win=0 Len=0
5078	16:56:14.076936	0.340323000	192.168.2.105	64.68.101.20	TCP	314	[TCP Retransmission] 62126 → 443 [FIN, PSH, ACK] Seq=5895 Ack=5499 Win=64580 Len=…
5088	16:56:15.277931	1.200995000	192.168.2.105	64.68.101.20	TCP	314	[TCP Retransmission] 62126 → 443 [FIN, PSH, ACK] Seq=5895 Ack=5499 Win=64580 Len=…
5090	16:56:15.439332	0.161401000	64.68.101.20	192.168.2.105	TCP	66	443 → 62126 [ACK] Seq=5499 Ack=6156 Win=38144 Len=0 SLE=5895 SRE=6049
5091	16:56:15.439958	0.000626000	64.68.101.20	192.168.2.105	TCP	60	443 → 62126 [RST, ACK] Seq=5499 Ack=6156 Win=155216 Len=0
5233	16:56:43.215068	27.7751100…	64.68.101.20	192.168.2.105	TLSv1.2	107	Encrypted Alert
5244	16:56:44.220103	1.005035000	64.68.101.20	192.168.2.105	TCP	107	[TCP Retransmission] 443 → 62127 [FIN, PSH, ACK] Seq=6852 Ack=952 Win=39840 Len=53
5522	16:56:46.227498	2.007395000	64.68.101.20	192.168.2.105	TCP	107	[TCP Retransmission] 443 → 62127 [FIN, PSH, ACK] Seq=6852 Ack=952 Win=39840 Len=53
6035	16:56:50.241266	4.013768000	64.68.101.20	192.168.2.105	TCP	107	[TCP Retransmission] 443 → 62127 [FIN, PSH, ACK] Seq=6852 Ack=952 Win=39840 Len=53
6173	16:56:58.250858	8.009592000	64.68.101.20	192.168.2.105	TCP	107	[TCP Retransmission] 443 → 62127 [FIN, PSH, ACK] Seq=6852 Ack=952 Win=39840 Len=53

```
[Bytes sent since last PSH flag: 154]
[TCP Analysis Flags]
  [Expert Info (Note/Sequence): This frame is a (suspected) retransmission]
    [This frame is a (suspected) retransmission]

0000  48 f8 b3 91 b1 fe f0 d5  bf 25 2d 3f 08 00 45 00   H······ ·%-?··E·
```

This frame is a (suspected) retransmission (tcp.analysis.retransmission) | Packets: 6246 · Displayed: 71 (1.1%) | Profile: Default

Wireshark + Advanced Analytics

Better Together

- We used Wireshark extensive filtering to identify and isolate servers of interest
- We created a filtered version of the pcap and opened in Transaction Analyzer
- We gathered our findings mostly by following the patterns shown in the various visualizations
- We can deduce certain application error recovery / synchronization capabilities (or deficiencies)
- Update: After many months, the Webex 98% hung issue simply went away
- Clearly, someone “fixed” something
- A reasonable person would ask, “why did it take so long for the fix?”

Final Discussion

Thank you for helping to test drive this session.

Please provide your feedback on the survey to help me improve the session


рахмат
danke
謝謝
ngiyabonga
teşekkür ederim
Баярлалаа
спасибо
faafetai lava
thank you
gracias
tapadh leat
mersi
barka
welalin
tack
spas
kia ora
dank je
misaotra
matondo
paldies
grazzi
mahalo
vinaka
спасибі
blagodaram
kiitos
dankie
dhanyavad
nanni
nandri
хвала
asante
manana
obrigada
tenki
murakoze
chokrane
mamnun
djiere dieuf
tau
mochchakkeram
дякую
bedankt
hvala
mauruuru
köszönöm
gràcie
bayarlalaa
akun
dankon
aciù
dziękuję
chnorakaloutioun
gratias ago
gràcies
sulpáy
taiku
go raibh maith agat
sobodi
dèkuji
sagolun
sukriya
kop khun krap
obrigado
mèsi
didi madloba
najis tuke
ありがとう
tanemirt
grazie
arigatô
takk
dakujem
trugarez
kam sah hamnida
rahmat
terima kasih
rahmet
diolch
dhanyavadagalu
shukriya
merce
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
ευχαριστώ
merci