

## S08 - Wireshark plus Advanced Analytics... ...better together

## The Webex 98% Hang Condition - Part I

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

## **Session Overview**

**Two Part Session** 

- Output Deep Dive troubleshooting into the Webex "98% hang" condition (cira 2018)
- Identify and explain the observable details we can see from packets
- Great example of how to diagnose a complex, intermittent, difficult performance problem using Wireshark together with advanced analytics
- Several hands-on labs to work with the captures in Wireshark

## **Session Premise and Inspiration**

- Output Packets give us insight into application, network, and protocol behavior
- We often need this insight to help developers and 3<sup>rd</sup> party providers understand where the problem actual lies
- These stakeholders seldom understand packet decodes and really benefit from an easy to digest storyboard with visuals that describe the problem

## **Highlight on Wireshark Features**

Used in our screenshots and hands-on lab

- Profiles
- Simple filters
- Custom column layout
- Sorting by column
- Export summary view to CSV
- Compound filters
- Interpreting Expert Info
- Colorization Rules
- Leverage key Wireshark metrics

## **Supplemental Advanced Analytics**

Used in our screenshots

Application delay analysis



- Visualizations that expose application and protocol behavior
- Interactive right-click filtering
- Turn based advanced metrics
- Quickly identify root cause of the 98% hang condition, as well as related conditions

# John Who?

- Practicing Performance Engineering since 1980
- Protocol Analysis since 1991
- Professional Services with OPNET / Riverbed since 2005
- Love the mystery of a complicated performance issue



# John Who?

- Practicing 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...



John Pittle <u>john.pittle@riverbed.com</u> @end2endviz www.linkedin.com/in/john-pittle

## Getting to know the attendees...a quick survey











## Thank you in advance for your feedback...

1<sup>st</sup> Live Run of this Session

- Goal is to be interactive
- Share our Industry Knowledge and Experience
- Need your help to tune this content for next Sharkfest



## Agenda - Two Sessions Part I - S08

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

## Part II - S10

- Loading PCAP into Advanced Analytics
- Visualizing the App Behavior
- More Advanced Analytics
- How to do this in Wireshark?
- Lab #2
- Wrap-Up

## Timeline

- 3:30 4:45 Part I
- 4:45 5:00 Break
- 5:00 6:15 Part II
- 6:30 onwards after party...







## http://www.packet-foo.com/sf23us/john.html



Name	Туре	Compressed size	Password pr
Analysis Results-Action Items Template v0	Microsoft Excel 97-2003 Wor	12 KB	No
쿋 convert csv to display filter.zip	Compressed (zipped) Folder	6 KB	No
🔊 dns response with mutlti host.csv	Microsoft Excel Comma Separ	3 KB	No
🔊 webex hosts from dns responses.csv	Microsoft Excel Comma Separ	2 KB	No
ivebex_98pct_resolved16_56_52edt@2018	ACE Capture File	21,279 KB	No
wireshark display filter.txt	Text Document	1 KB	No





## What the User sees

Many users were getting this condition

- Launch personal room from web browser
- New Webex app window opens and starts to display percent complete progression of launch activities
- Percent complete hits 98% and then stays there for several seconds sometimes as long as a minute
- After some period of time the hang condition clears, progression continues to 100% and Webex launch completes
- Output to this in different ways
  - Some users close the window and start over, other users just wait until the condition clears

## **Analysis Plan of Attack**

- Confirm timing of key user actions and symptoms
- Establish the goal of the Analysis
- Learn what we can about the App Architecture
- Determine the client facing server(s)
- Examine application and protocol behavior
- Ocument findings and recommended actions
- Optional: Compare "hang" scenario to "normal" scenario

## Date / Time Details for Analysis PCAP

Captured from my laptop with a continuous capture wrap around buffer

• June 5<sup>th</sup> 2018

• Hyperlink to launch personal room was clicked at ~ 16:56.02 EDT

The "98% hang" condition stayed on the screen until ~ 16:56:58 EDT

## **Goal of the PCAP Analysis**

- Confirm time bounds of the issue
- Output in the servers are in scope for investigation
- Output in the servers are causing / contributing to the hang
- Output Determine the nature of the (abnormal) condition(s) in play
- Provide forensic details need for a difficult discussion with vendor support

## What do we know about this app?

Architecture, deployment details, geography, etc.

Secure | https://riverbed.webex.com/wbxmjs/joinservice/join?backurl=https%3A%2F%2Friverbed.webex.com%2Fmc3100%2FfowardAction.do%3Fsiteurl%3Driverbed&pgvDone=15247438028...

Secure | https://riverbed.webex.com/wbxr

## 3<sup>rd</sup> Party Cloud / SaaS App Characteristics

These are not absolutes, but are highly likely

- There's no one to ask, we have to figure it out for ourselves
- Output Architecture includes client side RPC, javascript or other client side tech
- Leverage distributed CDN resources nearest to client
- Vendor probably has limited client traffic logging
- Output Service Serv
- Multiple vendors may be embedded in the architecture

## **Cloud Native Architecture Guidance**

<ul> <li>↔ C △ € cloud.google.com/urchitecture</li> <li>Google Cloud</li> <li>Overview Solutions Produ</li> </ul>	cts Pricing Resources	1 - can <b>a</b> marine <b>a</b>	с <b>( с</b>	Docs Supp					← → C △ e learn.microsoft.com/en-uu/azure/architectu Microsoft   Learn Documentation Traini	ure/	erits
Cloud Architecture Center	Cloud A Discover reference architectures, guidance,	rchitecture Ce	enter your worklaads on Google Cloud.						Azure Product documentation of Architecture C	Center Senter	
	System design guidance	Whether you are designing your own a to ensure that it's built upon an infrast needs.	rchitecture or adapting one of ours, you ructure foundation that meets your bus	need					ARCHITECTURE Browse Azure architectures	CONCEPT Explore cloud best practices	KOW-TO GUIDE Asses, optimize, and review you workload
	Application guidance	Choose an application area for guidar workload needs.	Monitoring and logging	our					Architecting applications Best practices and patterns for building applications	s on Azure	
		Aland machine learning     Application development     Big data and analytics     Databases	Hybrid and multicloud     Migration     Storage		A	WS	S		Design for the cloud Principles of a well-designed application Bet practices in fload applications Responsible engineering Application design patterns Architect multitement solutions on Azure	Optimize your workload Guiding tents try you architecture Examps your worklaad Performance tuning Performance antipattenss Secure your infrastructure	Choose the right technology Doose a compute service Doose a dompute service Doose a data store Doose a data store Doose a mensaging service
(	Google	Э		C C C R RWLamazon.com/bil C C C R RWLamazon.com/bil C C C C C C C C C C C C C C C C C C C	ogs/withtecture/redesigned-architecture-center/	WS Marketplace Customer E	nablement Events Explore More Q	Contact Us Su		Azure	
					AWS Architecture Blog AWS Architecture Cen & Resources by Annik Sahl (or 00 SYE2020) (in Ad Discoving relevant architecture relate expanded AVS Architecture Center, No patterns, best practices, and precession	nter: Your One-Sto Announcements, Architecture [ P ated content has been simplified fore you can browse, search, and tive guidance all in one location.	op Destination for Guidance remaink ( eff State I and made easier with the newly updated and even request reference architectures, architecture	Resources AWS Architecture Center AWS Architected AWS Whitepapers AWS Thintepapers AWS Thinting and Centification This is My Architecture			
				Q	Interesting of indicate learning of the orac cares in properties dramating as well as We designed this aggregated experime <b>How can the Architecture</b> Let's say you're looking for security gu what you we glouch as <u>whether AWS</u> contempt most popular with other AWS contempt From the <u>Architecture</u> Canter promptogen interested in and discover best gasted.	the drip place intere you can be a view aggregated collections nee to help you discover content <b>e Center help me?</b> widance and content. Instead of <i>AWS Solutions</i> , blog posts, etc.) ters. age, in the Security, Identity, & cs and featured content.	over incommission guarance of you music tensor to content related to have domain in one local ty our might net have known to lock for in the par- having to visit several different AWS sites to find it, it's now all in one place. You'll also see content <b>Compliance</b> column, click any of the areas you're	Follow Twitter Follow Twitter Factbook Linkedin Twitch Twitch Factbook			
					Security, Mently, A Compliance Learn Tool So merk your security and compliance guid, using MrS infectious and similars.	Meetily 3. Ames Menoperatin Henergia anteresorie moverly. Data Protection Lamin to inclusioni and	Describes A bodies Menter par mounts for regenter ends. Here and the state of the state of the state of the state regenter and the state of the				

## **Content Delivery Networks (CDN)**

### What is a content delivery network?



## **Cloud App - Analysis Questions / Challenges**

These will impact our ability to do analysis and the confidence level of our conclusions

- What servers are involved in launching Webex?
- Are they static or do they change within each region? ...across regions?
- Open the WebEx client use servers in the meeting Host's geographic region or in participant's geographic region?
- What else was user doing at the time, and how to quickly remove extraneous traffic from the PCAP?
- The reported time of the issue and the resolution are only approximate, how can we zoom in to the truly relevant traffic?



## What we know about the PCAP

## Host capture used during the 98% Hang

Description

- Client side continuous capture, via TA Capture Agent, was already running on laptop at the time of the issue
- Laptop connected to Internet from home office WiFi
- ISP is Spectrum Residential Location Orlando, FL
- I00Mbps Download / 6Mbps Upload
- VPN was \*not\* active
- Many other apps were open at the time adds to complexity of the analysis
- O Hyperlink to personal room was clicked at ~ 16:56.02 EDT on June 5th
- The "98% hang" condition cleared itself ~ 16:56:58

Wireshark · Capture File Proper	rties · webex_98pct_resolved16_56_52	edt@2018-06-05_16.58.06	@localhost.appcapture	- 0	×
Details					
File					
Name: Length: Hash (SHA256): Hash (RIPEMD160): Hash (SHA1): Format: Encapsulation: Snapshot length:	C:\OPNET Captures\webex-98pct\w 24 MB 2898a9442f718df55424f b46b45c83ab53023f5e3 503f6b0a8f2ccc12d5a2ft Wireshark/tcpdump/ Ethernet 65536	ebex_98pct_resolve 6db6dd9b3749db4 55a9ae6a6b737154 929a01aaac0ae7d3 pcap	d16_56_52edt@2018-0 L59e4fd4319d0bedfc90c 0228 6a	6-05_16.58.06@localhost.appcapt	ure
Time					
First packet: Last packet: Elapsed:	2018-06-05 16:47:27 2018-06-05 16:57:25 00:09:58				
Capture					
Hardware: OS: Application:	Unknown Unknown Unknown				
Interfaces					
<u>Interface</u> Unknown	<u>Dropped packets</u> Unknown	<u>Capture filter</u> Unknown	<u>Link type</u> Ethernet	<u>Packet size limit (snar</u> 65536 bytes	olen)
Statistics					
Measurement Packets Time span, s Average pps Average packet size, B Bytes Average bytes/s Average bits/s	<u>Captured</u> 32568 598.066 54.5 722 23506696 39 k 314 k	Dis 325 598 54. 722 235 39 314	<u>olayed</u> 68 (100.0%) .066 5 06696 (100.0%) ¢ k	<u>Marked</u>    0 	

## **Analysis Methodology**



- Output States States
- Alluvio Transaction Analyzer is a wrapper around tshark
- Output State St
- Output State St
- Output time proximity and the host name to identify server candidates
- Filter the PCAP and load into TA in order to visualize the traffic and perform the advanced analysis
- Carefully record the details of each anomaly we find







Open the PCAP file you downloaded from Packet-Foo

Navigate to Statistics -> Conversations

## Wireshark Capture Overview

Wireshark · Endpoints · webex\_98pct\_re

### **Unfiltered Capture**

Lots of hosts and lots of connections....will definitely need to filter this capture

Ethernet · 10	IPv4 · 113	IPv	6 TCP • 41	L6 UDP	405			
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
0.0.0.0	2	728	2	728	0	0	_	_
13.107.6.151	163	103 k	79	93 k	84	10 k	—	_
18.204.114.38	6	348	2	120	4	228	_	_
23.48.180.21	22	6150	11	4412	11	1738	_	_
23.56.192.142	40	24 k	22	18 k	18	6297	_	_
23.56.194.147	79	53 k	45	49 k	34	4615	_	_
23.60.1.28	69	19 k	29	14 k	40	5308	_	_
23.100.120.65	3	162	1	54	2	108	_	_
23.199.51.101	27	8195	8	5079	19	3116	_	_
24.143.206.48	19	1815	9	960	10	855	_	_
34.196.23.41	6	348	2	120	4	228	_	_
34.201.182.42	50	2876	18	1052	32	1824	_	_
34.233.26.108	6	348	2	120	4	228	_	_

52edt@2018-0

## How to find the "likely" WebEx Servers

Capture contains activity for lots of extraneous client apps

- Start time of interest begins with DNS query for riverbed.webex.com
  - Anything prior to this first query is not in scope
- ONS query contains the string "webex"
- SSL Server Name contains the string "webex"
  - tls.handshake.extensions\_server\_name
- If DNS results do not contain "webex", but the query was done in "reasonable proximity" to finding other "webex" servers, it still might be of interest to the analysis
- The above is not 100% perfect, but it may be "good enough"

## Lab: Filter and display DNS

Good time to practice profiles as well...

- Copy your default profile and name the copy DNS
- Set display filter to DNS
- Add column for host name
- Add column for address
- Adjust the layout
- Sort by the host name column
- Confirm date / time of user reported symptoms
- Note number of Webex related servers



## Add any protocol field as column to summary view



## **Updated Summary View**

Filtered by DNS and sort by server name column

🧉 webe	x_98pct_resolved16_56_52ed	t@2018-06-05_16.58.06	@localhost.appcapture			
File E	dit View Go Capture	Analyze Statistics	Telephony Wireless Tools Help			
	🧟 🕥 🚞 🔚 🔀 🖸	९ ⇔ ⇒ ≌ 🚹 🤳	📃 📃 🔍 Q, Q, 🦉			
dns						
No.	Time	Delta Time	Source Destination Proto	Lengt Name	Address	Info
15	16:55:00.751945	3.869095000	192.168.2 192.168.2.1 DNS	87 roaming.officeapps.live.com		Standard query 0xea30 A roaming.officeapps.live.com
29	16:56:45.522211	0.084002000	192.168.2.1 192.168.2 DNS	145 riverbed.webex.com	173.243.0.154	Standard query response 0xf0ce A riverbed.webex.com CNAME nebulam.webex.com CNAME global-ne
29	16:56:45.432107	0.021770000	192.168.2.1 192.168.2 DNS	145 riverbed.webex.com	173.243.0.154	Standard query response 0xe9dd A riverbed.webex.com CNAME nebulam.webex.com CNAME global-ne
29	16:56:45.410337	0.000632000	192.168.2 192.168.2.1 DNS	<pre>78 riverbed.webex.com</pre>		Standard query 0xe9dd A riverbed.webex.com
29	16:56:45.409705	0.050501000	192.168.2.1 192.168.2 DNS	145 riverbed.webex.com	173.243.0.154	Standard query response 0xc40d A riverbed.webex.com CNAME nebulam.webex.com CNAME global-ne
29	16:56:45.355714	0.003348000	192.168.2 192.168.2.1 DNS	78 riverbed.webex.com		Standard query 0xf0ce A riverbed.webex.com
29	16:56:45.312268	1.329530000	192.168.2 192.168.2.1 DNS	78 riverbed.webex.com		Standard query 0xc40d A riverbed.webex.com
17	16:56:02.433818	0.205628000	192.168.2.1 192.168.2 DNS	145 riverbed.webex.com	173.243.0.154	Standard query response 0xa512 A riverbed.webex.com CNAME nebulam.webex.com CNAME global-ne
17	16:56:02.228190	7.113501000	192.168.2 192.168.2.1 DNS	78 riverbed.webex.com		Standard query 0xa512 A riverbed.webex.com
17	16:55:55.114689	0.020977000	192.168.2.1 192.168.2 DNS	171 pollserver.lastpass.com	23.60.1.28	Standard query response 0xd054 A pollserver.lastpass.com CNAME lastpass.com.edgekey.net CNA
17	16:55:55.093712	34.847384000	192.168.2 192.168.2.1 DNS	<pre>83 pollserver.lastpass.com</pre>		Standard query 0xd054 A pollserver.lastpass.com
15	16:55:04.475902	0.000299000	192.168.2.1 192.168.2 DNS	174 pollserver.lastpass.com	23.60.1.28	Standard query response 0xb476 A pollserver.lastpass.com CNAME lastpass.com.edgekey.net CNA
15	16:55:04.470567	0.000197000	192.168.2 192.168.2.1 DNS	<pre>83 pollserver.lastpass.com</pre>		Standard query 0xb476 A pollserver.lastpass.com
15	16:55:04.469907	0.000841000	192.168.2.1 192.168.2 DNS	171 pollserver.lastpass.com	23.60.1.28	Standard query response 0x5a2e A pollserver.lastpass.com CNAME lastpass.com.edgekey.net CNA
15	16:55:04.469066	0.013874000	192.168.2.1 192.168.2 DNS	171 pollserver.lastpass.com	23.60.1.28	Standard query response 0x00c9 A pollserver.lastpass.com CNAME lastpass.com.edgekey.net CNA
15	16:55:04.455192	0.000116000	192.168.2 192.168.2.1 DNS	<pre>83 pollserver.lastpass.com</pre>		Standard query 0x00c9 A pollserver.lastpass.com
15	16:55:04.455076	0.888419000	192.168.2 192.168.2.1 DNS	<pre>83 pollserver.lastpass.com</pre>		Standard query 0x5a2e A pollserver.lastpass.com
30	16:57:06.467116	0.000032000	192.168.2.1 192.168.2 DNS	<pre>150 pagead46.l.doubleclick.net</pre>	64.233.177.155	. Standard query response 0xf7d0 A pagead46.l.doubleclick.net A 64.233.177.155 A 64.233.177.1
30	16:57:06.457477	0.001475000	192.168.2 192.168.2.1 DNS	<pre>86 pagead46.1.doubleclick.net</pre>		Standard query 0xf7d0 A pagead46.1.doubleclick.net
15	16:55:05.020916	0.001638000	192.168.2.1 192.168.2 DNS	<pre>102 pagead46.1.doubleclick.net</pre>	172.217.164.34	Standard query response 0x2f54 A pagead46.1.doubleclick.net A 172.217.164.34
15	16:55:05.016614	0.000095000	192.168.2 192.168.2.1 DNS	<pre>86 pagead46.1.doubleclick.net</pre>		Standard query 0x2f54 A pagead46.1.doubleclick.net
98	16:52:02.600151	0.004098000	192.168.2.1 192.168.2 DNS	102 pagead46.1.doubleclick.net	172.217.3.226	Standard querv response 0xdbac A pagead46.1.doubleclick.net A 172.217.3.226

## A better filter for our mission

Filters are very flexible... (thanks, Wireshark developers!!)

	webex	_98pct_resolved16_56_52e	dt@2018-06-05_16.58.0	6@localhost.appcap	ture					
Fil	e Edi	t View Go Capture	Analyze Statistics	Telephony Wirele	ss Tools Help					
		🧾 🛞 🚞 🔚 🔀	९ 🗢 🗢 🕾 🛉 🖉	⊾ <u>=</u>   ≡   €, 6	(Q. 🏨					
	dns.c	qry.name contains	"webex"							
No	).	Time	Delta Time	Source	Destination	Proto	Lengt	Name	Address	Info
1	29	16:56:45.359204	0.003490000	192.168.2.1	192.168.2	DNS	86	<pre>sec-tws-prod-vip.webex.com</pre>		Standard query
	29	. 16:56:45.352366	0.000488000	192.168.2	192.168.2.1	DNS	86	<pre>sec-tws-prod-vip.webex.com</pre>		Standard query
	29	. 16:56:45.351878	0.002049000	192.168.2.1	192.168.2	DNS	102	<pre>sec-tws-prod-vip.webex.com</pre>	66.163.35.36	Standard query
	29	. 16:56:45.349829	0.000614000	192.168.2	192.168.2.1	DNS	86	<pre>sec-tws-prod-vip.webex.com</pre>		Standard query
	29	. 16:56:45.349215	0.003855000	192.168.2.1	192.168.2	DNS	102	<pre>sec-tws-prod-vip.webex.com</pre>	66.163.35.36	Standard query
	29	. 16:56:45.345360	0.002155000	192.168.2	192.168.2.1	DNS	86	<pre>sec-tws-prod-vip.webex.com</pre>		Standard query
-	29	16.56.45 343205	0 000001000	192 168 2 1	192 168 2	DNS	100	car_twc_nrod_vin webey com	66 163 35 36	Standard query



## Even more better...

### Filters are very, very flexible... (thanks, Wireshark developers!!)

webex_98pct_resolved16_56_52e	dt@2018-06-05_16.58.06@loc	calhost.appcapture					
File Edit View Go Capture	Analyze Statistics Teleph	hony Wireless To	ols Help				
🥂 🔳 🔬 💿 🚞 🛅 🛣 💽	९ 🗢 🗢 🕾 🚹 🛓 🚍		<u></u>				
dns.qry.name contains	"webex" && dns.flags.r	response==1					
No. Time	Delta Time So	ource De	estination	Proto Lengt	Name	Address	Info
17 16:56:02.433818	0.00000000 19	2.168.2.1 19	2.168.2.105	DNS 145	riverbed.webex.com	173.243.0.154	Standard guery response 0xa512 A riverb
17 16:56:02.441100	0.007282000 19	2.168.2.1 19	2.168.2.105	DNS 100	global-nebulam.webex.com	173.243.0.154	Standard query response 0xee05 A global
17 16:56:02.553456	0.112356000 19	2.168.2.1 19	2.168.2.105	DNS 84	global-nebulam.webex.com		Standard query response 0xa856 AAAA glo
18 16:56:04.162417	1 608961000 19	02 168 2 1 19	2 168 2 105 1	DNS 131	nebulam.webex.com	173 243 0 154	Standard query response 0xf8c2 A nebula
18 16:56:04.474396	0						v response 0x0b3e A akamai
21 16:56:10.320159	5 weber	x 98nct re-	solved16_5	56 52edt	@2018-06-05 16.58	06@localhost.appc	apture v response 0xd085 A sec-tw
21 16:56:10.323249	0	-sober-ic	Jonreano_J	- secon	2010 00 05_10.50	ioo e lo camos dappe	v response 0x8c2c A sec-tw
21 16:56:10.345079	9 Eile Ed	lit View	Go Co	nture	Applyze Statistics	Telephony Wir	Tooy response 0xd508 AAAA sec
21 16:56:10.950034	o File Eu	it view	00 Ca	pture	Analyze Statistics	relephony with	v response 0x9a1d A emcbmm
21 16:56:10.954018	0	a a 1					o v response 0x559a A emcbmm
21 16:56:10.973148		Ø 🙂 📒	010 🗙		< < ⇒ ⇒ 😤 ¶	₩ 📮 📃 🔍	🔍 🔍 🌆 response Øxae74 A ed1lnc
21 16:56:10.973271	0				•		v response 0x16cb A ed1txc
21 16:56:10.973288		an ( n n n	a conta	ine llu	ushav" 0.0 dag f		y response 0xc826 A ed1syc
21 16:56:10.973306	a ans.	qry.nam	ie conta	ins v	vedex && ans.i	lags.response	==1 v response 0x2fc4 A ed1sgc
21 16:56:10.973320	0		~				y response 0xaba4 A ed1chc
21 16:56:10.973333		2.108.2.1 19	2.100.2.100	ער כאט	euinkcomm/v.webex.com	- 114.29.200.11	Scanuard query response 0x2160 A ed1hkc
21 16:56:10.977981	0.004648000 193	2.168.2.1 19	2.168.2.105	DNS 103	ed1jpcbmm50-nrt02.webex.com	114.29.204.49	Standard query response 0x8027 A ed1jpc
21 16:56:10.979253	0.001272000 193	2.168.2.1 19	2.168.2.105	DNS 95	emvcbmm20.webex.com	64.68.120.90	Standard query response 0x67c5 A emvcbm
4 21 16:56:10.989277	0.010024000 193	2.168.2.1 19	2.168.2.105	DNS 97	ed1vacbmm30.webex.com	64.68.104.140	Standard query response 0xc7f4 A ed1vac
21 16:56:10.989300	0.000023000 193	2.168.2.1 19	2.168.2.105	DNS 97	ed1sjcbmm10.webex.com	64.68.121.153	Standard query response 0xeef6 A ed1sjc
21 16:56:11.015086	0.025786000 193	2.168.2.1 19	2.168.2.105	DNS 95	emvcbmm10.webex.com	64.68.120.70	Standard query response 0x6f84 A emvcbm
22 16:56:12.145199	1.130113000 193	2.168.2.1 19	2.168.2.105	DNS 117	emcb31101.webex.com	64.68.101.20	Standard query response 0x0754 A emcb31
22 16:56:12.636041	0.490842000 193	2.168.2.1 19	2.168.2.105	DNS 123	ed1vacb32201.webex.com	64.68.110.77	Standard query response 0x4906 A ed1vac
29 16:56:45.342211	32.706170000 193	2.168.2.1 19	2.168.2.105	DNS 102	<pre>sec-tws-prod-vip.webex.com</pre>	66.163.35.36	Standard query response 0xd9d5 A sec-tw
29 16:56:45.343205	<u>a aaaggaaaa 19</u>	02.168.2.1 19	2.168.2.105	DNS 102	sec-tws-prod-vin.webex.com	66.163.35.36	Standard query response 0x43ed A sec-tw

## Aliases for riverbed.webex.com

- 1<sup>st</sup> DNS Query @ 16:56:02
- Expect our conversations of interest will start with 173.243.0.154

2025 00 57 40 464400 0 000202000 402 405
▲ Queries
riverbed.webex.com: type A, class IN
Name: riverbed.webex.com
[Name Length: 18]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
riverbed.webex.com: type CNAME, class IN, cname nebulam.webex.com
> nebulam.webex.com: type CNAME, class IN, cname global-nebulam.webex.com
global-nebulam.webex.com: type A, class IN, addr 173.243.0.154

## Thinking ahead just a little...

- We know this capture has way more traffic than what we want for analysis
- Wireshark lets you save a csv file based on the "displayed packets" view, along with the columns
- You could then use that csv file as input into a script that would build a display filter you could then use to filter down your capture to just the hosts of interest...



## **Export Summary View to CSV File**

<u>_</u> w	vebex_98pct_resolved16_	_56_52e	dt@2018-0	6-05	5_16.5	8.060	፬localhost.aj	ppcaptu	re
File	Edit View Go C	apture	Analyze	Sta	tistic	s To	elephony 👋	Wireless	Te
	Open	(	Ctrl+O		1 1	ł		e, e,	e,
	Open Recent			۲.	dns	.flag	js.respon	se==1	L
	Merge				_		Source		р
	Import from Hex Dump	o			6	~	102 109	2.4	11
	Close	(	Ctrl+W		1000	10 10	192.168.	2.1	19
	Save	(	Ctrl+S		600	0	192.168.	2.1	19
	Save As	(	Ctrl+Shift+S	5	100	0	192.168.	2.1	19
					1900	0	192.168.	2.1	19
	File Set			•	300	0	192.168.	2.1	19
	Export Specified Packet	s			000	0	192.168.	2.1	19
	Export Packet Dissection	ns		۶.		As PI	ain Text	1	19
	Export Packet Bytes	(	Ctrl+Shift+>	<b>C</b>		As C	5V	1	10
	Export PDUs to File					As "C	"Arr.	1	10
	Export TLS Session Keys	i						1	19
	Export Objects			×				1	19
	Print	(	Ctrl+P			As JS	ON	1	19
					.400	0	172.100.		19
	Quit	(	Ctrl+Q		300	0	192.168.	2.1	19
-	21 16:56:10.977	7981	0.00	464	1800	0	192.168.	2.1	19

🦾 Wireshark · I	Export Packet Diss	ections				×
Save in:	ewebex-98pct		🖂 🧿 🌶	⊳ 🖽		
<b>A</b> Home	Name		No items r	natch your searc	h.	Date m
Desktop						
Libraries						
This PC						
Network	File name:	webex hosts from dns respor	ISES		~	Save
	Save as type:	CSV (Comma Separated Value	ues summary) (*.cs	v)	~	Cancel
	Packet Range		○ Captured	<ul> <li>Displayed</li> </ul>	Packet Format	
	<ul> <li>All packets</li> </ul>		32568	34	Packet summary line	
	O Selected pac	ket	1	1	<ul> <li>Include column neadings</li> <li>Racket detaile:</li> </ul>	
	O Marked pack	ets	0	0		-
	First to last ma	arked	0	0	As displayed	
	Range:		0	0	Packet Bytes	
	Remove Igno	red packets	0	0	Each packet on a new page	Л

9.0 o et		Ŷ	webex hosts fr	om dns responses	s.csv Ƴ	h duaia			ch				, ihi	John P	ittle 🧕	lä 🖬		o x
File	Home	Insert	Page Layou	ıt Formulas	Data	Review	View	Automate	Help	Data Streamer	Acrobat	Power Pivot				모 Com	ments	🖻 Share 🕞
AutoSa	ve • Off	8 9-	୯															
								- •										
J15	*	: _ ×	$\sqrt{f_x}$	Standard query	response	e 0x2fc4 A ec	d1sgcbmm1	0.webex.com	A 114.	29.213.212								~
	A B	С	D	E	F	G		Н		I						J		<b>•</b>
1 No	. Time	Delta Tim	e Source	Destination	Protocol	Length Na	me			Address I	nfo							
2 17	398 56:02.4		0 192.168.2.1	192.168.2.105	DNS	145 rive	erbed.webe	ex.com		173.243.0.154	tandard query	y response 0xa512	A riverbed.web	ex.com CNAME	nebulam.we	bex.com CN	IAME glo	bal-nebulan
3 17	403 56:02.4	0.00728	32 192.168.2.1	192.168.2.105	DNS	100 glo	bal-nebular	m.webex.com	۱	173.243.0.154	tandard query	y response 0xee05	A global-nebul	am.webex.com /	A 173.243.0.1	.54		
4 17	426 56:02.6	0.11235	6 192.168.2.1	192.168.2.105	DNS	84 glo	bal-nebular	n.webex.com	۱	S	tandard query	y response 0xa856	AAAA global-ne	ebulam.webex.c	om			
5 18	222 56:04.2	1.60896	51 192.168.2.1	192.168.2.105	DNS	131 nel	bulam.webe	ex.com		173.243.0.154	tandard query	y response 0xf8c2 A	A nebulam.web	ex.com CNAME g	global-nebu	lam.webex.o	com A 17	3.243.0.154
6 18	384 56:04.5	0.31197	79 192.168.2.1	192.168.2.105	DNS	176 aka	amaicdn.we	bex.com		23.199.51.101	tandard query	y response 0x0b3e	A akamaicdn.w	ebex.com CNAN	1E akamaicdi	nbts.webex.	.com.edg	ekey.net CN
7 21	584 56:10.3	5.84576	53 192.168.2.1	192.168.2.105	DNS	102 sec	-tws-prod-	/ip.webex.co	m	66.163.35.36	tandard query	y response 0xd085	A sec-tws-prod	-vip.webex.com	A 66.163.35.	36		
8 21	587 56:10.3	0.0030	9 192.168.2.1	192.168.2.105	DNS	102 sec	-tws-prod-	/ip.webex.co	m	66.163.35.36	tandard query	y response 0x8c2c	A sec-tws-prod-	vip.webex.com	A 66.163.35.	36		
9 21	590 56:10.3	0.0218	33 192.168.2.1	192.168.2.105	DNS	156 sec	-tws-prod-\	/ip.webex.co	m	5	tandard query	y response 0xd508	AAAA sec-tws-	prod-vip.webex.	com SOA ns	1.as13445.ne	et	
10 21	731 56:10.9	0.60495	5 192.168.2.1	192.168.2.105	DNS	94 em	icbmm10.we	ebex.com		173.243.0.96	tandard query	y response 0x9a1d	A emcbmm10.v	vebex.com A 173	3.243.0.96			
11 21	746 56:11.0	0.00398	34 192.168.2.1	192.168.2.105	DNS	94 em	icbmm20.we	ebex.com		173.243.0.97 S	tandard query	y response 0x559a	A emcbmm20.v	vebex.com A 173	.243.0.97			
12 21	762 56:11.0	0.0191	192.168.2.1	192.168.2.105	DNS	97 ed:	1Incbmm60.	webex.com		62.109.231.3	tandard query	y response 0xae74	A ed1Incbmm6	0.webex.com A 6	52.109.231.3			
13 21	765 56:11.0	0.00012	23 192.168.2.1	192.168.2.105	DNS	97 ed:	1txcbmm80.	webex.com		209.197.222.159	tandard query	y response 0x16cb	A ed1txcbmm8	0.webex.com A 2	209.197.222.1	159		
14 21	766 56:11.0	0.00001	17 192.168.2.1	192.16	_										9.202.13	39		
15 21	767 56:11.0	0.00001	192.168.2.1	192.16 TO	oo Ea	isy Ma	te - A	variati	on d	of the phi	rase " N	lo worries	" - Parti	cularly	9.213.21	2		
16 21	/68 56:11.0	0.00001	4 192.168.2.1	192.16		1 - C							<b>T</b> 1 1		.243.4.7	6		
17 21	/69 56:11.0	0.00001	13 192.168.2.1	192.16 US	setul	when	some	one is	ask	ing you to	o do soi	mething.	I hat sor	mething	/9.200.1	1		
18 21	//1 56:11.0	0.00464	192.168.2.1	192.16	:	me elite		the end of							114.29.	204.49		
19 21	772 50:11.0	0.00127	/2 192.168.2.1	192.16 C	an, in	reality	y, be e	eitner e	asy	or not.					.20.90	<b>`</b>		
20 21	794 50:11.0	0.01002	4 192.108.2.1	192.10	DNIC	07 od1	1 cichmm 10	webey com		64 60 101 150	tandard guan	v rosponso Ovoofe	A ad1cichmm10		.104.140	,		
21 21	793 30:11.0	0.00002	25 192.108.2.1	102 168 2 105	DNS	97 eu.	rsjcomm10.	webex.com		64.68.121.135 3	tandard query	v response 0xeero	A eursjoonning	webex.com A 64	4.06.121.133			
22 21	07 56·12 1	1 12011	2 102 168 2 1	192.108.2.105	DNS	117 om	wcb21101 wc	vebex.com		64.68.120.70 S	tandard query	v response 0x0184 /	A emocommito.	webex.com CNAN	.08.120.70	wohov com	A 64 60 1	01.20
23 22	307 30.12.1 322 56·12 6	0.40004	12 192 160 2 1	192,100,2,105	DNS	122 od1	1vach22201	webey.com		64 68 110 77	tandard query	response 0x0734		L webey com CN	AME edition	h222 wohov	x 04.08.1	4 68 110 77
25 20	25 56.45 2	32 7061	7 192 168 2 1	192 168 2 105	DNS	102 600	-two-produ	vin webey co	m	66 163 35 26	tandard query	v response 0x4900		-vin webey com	A 66 162 25	36	COM A 0	4.00.110.77
26 29	225 56:45.3	0.00099	192.108.2.1	192,108,2,105	DNS	102 500	-tws-prod-v	/ip.webex.co	m	66 162 25 26	tandard query	v response 0x43ed	A sec-tws-prod	-vip.webex.com	A 66 162 25	36		
27 29	20 56.45.3	0.0005	1 192 168 2 1	192 168 2 105	DNS	102 500	-tws-prod-v	in webey co	m	66 163 35 36	tandard query	v response 0x43ed	A sec-tws-prod	-vip.webex.com	A 66 163 35	36		
28 29	321 56.45.4	0.0006	3 192 168 2 1	192 168 2 105	DNS	102 500	-tws-prod-v	in webey co	m	66 163 35 36	tandard query	v response 0vd0h7	A sec-tws-prod	-vin webey com	Δ 66 162 25	36		
20 29	334 56.45 4	0.00200	06 192 168 2 1	192 168 2 105	DNS	86 600	-tws-prod-v	in webey co	m	00.100.00.00	tandard query	v response OvfAab		rod-vin webey	com			
30 29	358 56:45 4	0.05050	1 192,168 2 1	192,168 2 105	DNS	145 rive	erhed webe	x.com		173,243.0 154	tandard query	v response 0xc40d	A riverbed web	ex.com CNAME	nebulam we	bex.com CN		bal-nebulan
31 29	365 56:45 4	0.02240	2 192,168,2 1	192.168.2.105	DNS	145 rive	erbed.webe	x.com		173.243.0.154	tandard query	v response Oxe9dd	A riverbed web	Dex.com CNAME	nebulam.we	ebex.com CN	VAMF øld	bal-nebular
32 29	368 56:45 4	0.00610	2 192,168,2 1	192,168,2,105	DNS	100 010	bal-nebular	n.webex.com	1	173.243.0.154	tandard query	v response 0x1ec8	A global-nebula	am.webex.com 4	173,243.0 1	54	5 1112 810	
33 29	390 56:45 5	0.08400	2 192,168,2,1	192,168,2,105	DNS	145 rive	erbed.webe	x.com		173.243.0.154	itandard query	v response 0xf0ce	A riverbed.web	ex.com CNAMF r	nebulam.we	 bex.com CN	AME	bal-nebular
34 29	133 56:45.6	0.1099	8 192.168.2.1	192.168.2.105	DNS	84 glo	bal-nebular	n.webex.com	1		tandard query	v response 0x0eab	AAAA global-ne	ebulam.webex.c	om			
35 29	355 56:47.1	1,43992	4 192,168.2.1	192.168.2.105	DNS	160 lp.y	webex.com		-	23,56,192,142	tandard query	v response 0x17c0	A lp.webex.con	n CNAME san.we	bex.com.ed	gekey.net C	NAME e4	955.g.akami
26		2				200 101						,						



- Your download files include a python script that will convert a CSV file to a Wireshark display filter text string
- Script assumes the CSV file is formatted similar to the CSV files also included in the download
- Special thanks to my most excellent colleague and Wireshark Instructor, Leigh Finch, for creating this script on super short notice





	README	×	+	_	D	×
File	Edit View					<b>\$</b>

Usage

bash\$ python3 dnsshark.py webex\ hosts\ from\ dns\ responses.csv ip.addr == 173.243.0.154 or ip.addr == 23.199.51.101 or ip.addr == 66.163.35.36 or ip.addr == 173.243.0.96 or ip.addr == 173.243.0.97 or ip.addr == 62.109.231.3 or ip.addr == 209.197.222.159 or ip.addr == 114.29.202.139 or ip.addr == 114.29.213.212 or ip.addr == 173.243.4.76 or ip.addr == 114.29.200.11 or ip.addr == 114.29.204.49 or ip.addr == 64.68.120.90 or ip.addr == 64.68.104.140 or ip.addr == 64.68.121.153 or ip.addr == 64.68.120.70 or ip.addr == 64.68.101.20 or ip.addr == 64.68.110.77 or ip.addr == 23.56.192.142 bash\$ python3 dnsshark.py dns\ response\ with\ mutlti\ host.csv ip.addr == 3.221.141.237 or ip.addr == 3.217.166.173 or ip.addr == 52.22.119.135 or ip.addr == 34.203.175.187 or ip.addr == 52.167.17.97 or ip.addr == 52.109.92.22 or ip.addr == 40.74.108.123 or ip.addr == 151.101.131.5 or ip.addr == 151.101.67.5 or ip.addr == 151.101.195.5 or ip.addr == 151.101.3.5 or ip.addr == 209.85.165.74 or ip.addr == 23.185.0.1 or ip.addr == 20.44.10.123 or ip.addr == 3.230.60.20 or ip.addr == 54.164.27.50 or ip.addr == 52.113.194.132 or ip.addr == 52.114.142.199 or ip.addr == 52.114.142.198



## Time to examine SSL/TLS

## Wireshark - SSL Server Name View

Sorted by Server Name Column from SSL Decodes

### webex\_98pct\_resolved16\_56\_52edt@2018-06-05\_16.58.06@localhost.appcapture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

### 🦲 🔳 🖉 🐵 🗼 🛅 🕱 🙆 I 🔍 🖛 🌧 🖺 🖉 💆 📃 📃 I 🔍 Q. Q. 🎛

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

No.	Time	The RTT to ACK the segment was	Time since request	Source	Destination	Protocol	Length	Server Name	Info
2461	79.758560			192.168.2.105	192.241.163.235	TLSv1.2	571	<pre>lp-push-server-553.lastpass.c</pre>	Client Hello
29484	558.581064			192.168.2.105	151.101.6.110	TLSv1.2	608	js-agent.newrelic.com	Client Hello
17975	516.558438			192.168.2.105	151.101.6.110	TLSv1.2	571	js-agent.newrelic.com	Client Hello
17494	515.601878			192.168.2.105	54.230.22.63	TLSv1.2	571	<pre>img-getpocket.cdn.mozilla.net</pre>	Client Hello
22604	524.369051			192.168.2.105	64.68.120.90	TLSv1.2	274	emvcbmm20.webex.com	Client Hello
21939	523.820821			192.168.2.105	64.68.120.90	TLSv1.2	242	emvcbmm20.webex.com	Client Hello
22656	524.489574			192.168.2.105	64.68.120.70	TLSv1.2	274	emvcbmm10.webex.com	Client Hello
21996	523.870223			192.168.2.105	64.68.120.70	TLSv1.2	242	emvcbmm10.webex.com	Client Hello
22384	524.137957			192.168.2.105	173.243.0.97	TLSv1.2	273	emcbmm20.webex.com	Client Hello
21869	523.769127			192.168.2.105	173.243.0.97	TLSv1.2	241	emcbmm20.webex.com	Client Hello
22377	524.132636			192.168.2.105	173.243.0.96	TLSv1.2	273	emcbmm10.webex.com	Client Hello
21875	523.772988			192.168.2.105	173.243.0.96	TLSv1.2	241	emcbmm10.webex.com	Client Hello
22815	524.909020			192.168.2.105	64.68.101.20	TLSv1.2	242	emcb31101.webex.com	Client Hello
22812	524.907889			192.168.2.105	64.68.101.20	TLSv1.2	242	emcb31101.webex.com	Client Hello
22190	523.987778			192.168.2.105	64.68.104.140	TLSv1.2	276	ed1vacbmm30.webex.com	Client Hello
21065	EDD 700040			102 100 2 105	CA CO 104 140	TLC4 0	244		Client U-11-

Expression..





## **Compound Filters**

Powerful capability

webex_98pct_resolved16_56_52edt@2018-06-05_16.58.06@localhost.appcapture												
File	ile Edit View Go Captu		Capture	Analyze	Statistics	Telephony	Wire					
	J	۱	0101 0110 0111	🔀 🎑	< 🗢	🖹 👔		Ð				
tls	tls.handshake.extensions_server_name    dns											

## **Compound Filters**

Permission to "go wild"?

### **Permission Granted**



## **Even More Compound Filters**

### Permission to "go wild"?

### Go for it!!





## Examine: App & Protocol Behavior

## With our compound filter applied..

s	sl.handshake.extensions_server_na	ame    dns						Expression + Apply this fil
No.	Time	Time delta from previv The RTT to ACK the segme Time since request	Source	Destination	Protocol L	ength Server Name	Flags	Info
	6654 08:57:28.562694	0.007951000	192.168.2.105	173.243.0.154	TLSv1.2	241 riverbed.webex.com	0x018	Client Hello
	6692 08:57:28.826087	0.000154000	192.168.2.105	173.243.0.154	TLSv1.2	273 riverbed.webex.com	0x018	Client Hello
	6798 08:57:28.952974	0.000406000	192.168.2.105	173.243.0.154	TLSv1.2	273 riverbed.webex.com	0x018	Client Hello
	6799 08:57:28.958136	0.005162000	192.168.2.105	173.243.0.154	TLSv1.2	241 riverbed.webex.com	0x018	Client Hello
	6800 08:57:28.967226	0.009090000	192.168.2.105	192.168.2.1	DNS	78		Standard query 0x2166 A emcbmm10.webex.com
	6801 08:57:28.967506	0.000280000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x0029 A ed1sjcbmm10.webex.com
	6802 08:57:28.967786	0.000280000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x718b A ed1txcbmm80.webex.com
	6803 08:57:28.968389	0.000603000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x4af3 A ed1lncbmm60.webex.com
	6804 08:57:28.968673	0.000284000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x426c A ed1vacbmm30.webex.com
	6805 08:57:28.969171	0.000498000	192.168.2.105	192.168.2.1	DNS	78		Standard query 0xdc0c A emcbmm20.webex.com
	6806 08:57:28.969338	0.000167000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0xf19a A ed1sycbmm90.webex.com
	6808 08:57:28.969846	0.000011000	192.168.2.105	192.168.2.1	DNS	82		Standard query 0xb39a A ed1chcbmm100.webex.com
	6809 08:57:28.969877	0.000031000	192.168.2.105	192.168.2.1	DNS	79		Standard query 0x025e A emvcbmm10.webex.com
	6811 08:57:28.970022	0.000127000	192.168.2.105	192.168.2.1	DNS	79		Standard query 0x7265 A emvcbmm20.webex.com
	6812 08:57:28.970141	0.000119000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x14e7 A ed1sgcbmm10.webex.com
	6813 08:57:28.970701	0.000560000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x6662 A ed1hkcbmm70.webex.com
	6814 08:57:28.970712	0.000011000	192.168.2.105	192.168.2.1	DNS	87		Standard query 0xf325 A ed1jpcbmm50-nrt02.webe
	6821 08:57:28.993744	0.022418000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x426c A ed1vacbmm30.w
	6822 08:57:28.995924	0.002180000	192.168.2.1	192.168.2.105	DNS	98		Standard query response 0xb39a A ed1chcbmm100
	6823 08:57:28.996687	0.000763000	192.168.2.1	192.168.2.105	DNS	94		Standard query response 0x2166 A emcbmm10.webe
	6824 08:57:28.996717	0.000030000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x718b A ed1txcbmm80.w
	6825 08:57:28.996731	0.000014000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x4af3 A ed1lncbmm60.w
	6826 08:57:28.996745	0.000014000	192.168.2.1	192.168.2.105	DNS	94		Standard query response 0xdc0c A emcbmm20.webe
	6827 08:57:28.996756	0.000011000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0xf19a A ed1sycbmm90.w
	6828 08:57:29.000219	0.003463000	192.168.2.1	192.168.2.105	DNS	103		Standard query response 0xf325 A ed1jpcbmm50-n
	6829 08:57:29.000846	0.000627000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x14e7 A ed1sgcbmm10.w
	6850 08:57:29.024120	0.001276000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x0029 A ed1sjcbmm10.w
	6868 08:57:29.031893	0.001148000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x6662 A ed1hkcbmm70.w
	6871 08:57:29.038389	0.000600000	192.168.2.1	192.168.2.105	DNS	95		Standard query response 0x025e A emvcbmm10.web
	6872 08:57:29.038408	0.000019000	192.168.2.1	192.168.2.105	DNS	95		Standard query response 0x7265 A emvcbmm20.web
	6923 08:57:29.112171	0.00002000	192.168.2.105	64.68.104.140	TLSv1.2	244 ed1vacbmm30.webex.com	0x018	Client Hello
	6924 08:57:29.112545	0.000374000	192.168.2.105	173.243.0.96	TLSv1.2	241 emcbmm10.webex.com	0x018	Client Hello
	6927 08:57:29.123244	0.000915000	192.168.2.105	173.243.0.97	TLSv1.2	241 emcbmm20.webex.com	0x018	Client Hello
	6930 08:57:29.124794	0.000670000	192.168.2.105	209.197.222.159	TLSv1.2	244 ed1txcbmm80.webex.com	0x018	Client Hello
	6933 08:57:29.128294	0.000625000	192.168.2.105	173.243.4.76	TLSv1.2	245 ed1chcbmm100.webex.com	0x018	Client Hello
	6955 08:57:29.134995	0.000945000	192.168.2.105	173.243.0.154	TLSv1.2	273 riverbed.webex.com	0x018	Client Hello
	6960 08:57:29.138051	0.000692000	192.168.2.105	173.243.0.154	TLSv1.2	273 riverbed.webex.com	0x018	Client Hello
1	6071 08.57.20 16/85/	a aaafa7aaa	102 168 2 105	64 68 121 152	TI Sv1 2	244 ed1sichmm10 weber com	Qv018	Client Hello



ssl.handshake.extensions_server_nam	ie    dns						Expression + Apply this fi
vo. Time Ti	me delta from previci The RTT to ACK the segme Time since request	Source	Destination	Protocol L	ength Server Name	Flags	סזת
6654 08:57:28.562694	0.007951000	192.168.2.105	173.243.0.154	TLSv1.2	241 riverbed.webex.com	0x018	Client Hello
6692 08:57:28.826087	0.000154000	192.168.2.105	173.243.0.154	TLSv1.2	273 riverbed.webex.com	0x018	Client Hello
6798 08:57:28.952974	0.000406000	192.168.2.105	173.243.0.154	TLSv1.2	273 riverbed.webex.com	0x018	Client Hello
6799 08:57:28.958136	0.005162000	192.168.2.105	173.243.0.154	TLSv1.2	241 riverbed.webex.com	0x018	Client Hello
							A emcbmm10.webex.com
6801 08:57:28.967506	0.000280000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x0029 A ed1sjcbmm10.webex.com
6802 08:57:28.967786	0.000280000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x718b A ed1txcbmm80.webex.com
6803 08:57:28.968389	0.000603000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x4af3 A ed1lncbmm60.webex.com
6804 08:57:28.968673	0.000284000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x426c A ed1vacbmm30.webex.com
6805 08:57:28.969171	0.000498000	192.168.2.105	192.168.2.1	DNS	78		Standard query 0xdc0c A emcbmm20.webex.com
6806 08:57:28.969338	0.000167000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0xf19a A ed1sycbmm90.webex.com
6808 08:57:28.969846	0.000011000	192.168.2.105	192.168.2.1	DNS	82		Standard query 0xb39a A ed1chcbmm100.webex.com
6809 08:57:28.969877	0.000031000	192.168.2.105	192.168.2.1	DNS	79		Standard query 0x025e A emvcbmm10.webex.com
6811 08:57:28.970022	0.000127000	192.168.2.105	192.168.2.1	DNS	79		Standard query 0x7265 A emvcbmm20.webex.com
6812 08:57:28.970141	0.000119000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x14e7 A ed1sgcbmm10.webex.com
6813 08:57:28.970701	0.000560000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x6662 A ed1hkcbmm70.webex.com
6814 08:57:28.970712	0.000011000	192.168.2.105	192.168.2.1	DNS	87		Standard query 0xf325 A ed1jpcbmm50-nrt02.webe
6821 08:57:28.993744	0.022418000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x426c A ed1vacbmm30.w.
6822 08:57:28.995924	0.002180000	192.168.2.1	192.168.2.105	DNS	98		Standard query response 0xb39a A ed1chcbmm100.
6823 08:57:28.996687	0.000763000	192.168.2.1	192.168.2.105	DNS	94		Standard query response 0x2166 A emcbmm10.webe.
6824 08:57:28.996717	0.000030000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x718b A ed1txcbmm80.w.
6825 08:57:28.996731	0.000014000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x4af3 A ed1lncbmm60.w.
6826 08:57:28.996745	0.000014000	192.168.2.1	192.168.2.105	DNS	94		Standard query response 0xdc0c A emcbmm20.webe.
6827 08:57:28.996756	0.000011000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0xf19a A ed1sycbmm90.w.
6828 08:57:29.000219	0.003463000	192.168.2.1	192.168.2.105	DNS	103		Standard query response 0xf325 A ed1jpcbmm50-n.
6829 08:57:29.000846	0.000627000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x14e7 A ed1sgcbmm10.w.
6850 08:57:29.024120	0.001276000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x0029 A ed1sjcbmm10.w.
6868 08:57:29.031893	0.001148000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x6662 A ed1hkcbmm70.w.
6871 08:57:29.038389	0.000600000	192.168.2.1	192.168.2.105	DNS	95		Standard query response 0x025e A emvcbmm10.web.
6872 08:57:29.038408	0.000019000	192.168.2.1	192.168.2.105	DNS	95		Standard query response 0x7265 A emvcbmm20.web.
6923 08:57:29.112171	0.00002000	192.168.2.105	64.68.104.140	TLSv1.2	244 ed1vacbmm30.webex.com	0x018	Client Hello
6924 08:57:29.112545	0.000374000	192,168,2,105	173,243,0,96	TLSv1.2	241 emcbmm10.webex.com	0x018	Client Hello
6927 08:57:29.123244	0.000915000	192,168,2,105	173,243,0,97	TLSv1.2	241 emcbmm20.webex.com	0x018	Client Hello
6930 08:57:29.124794	0.000570000	192,168,2,105	209,197,222,159	TLSv1.2	244 edltxcbmm80.webex.com	0x018	Client Hello
6933 08:57:29,128294	0.000625000	192,168,2,105	173,243,4,76	TLSv1.2	245 ed1chcbmm100.webex.com	0x018	Client Hello
6955 08:57:29 13/995	0.000945000	192 168 2 105	173 243 0 154	TLSv1 2	273 riverbed webey com	0x018	Client Hello
6960 08:57:29 138051	0.000595000	192.168 2.105	173 243 0 154	TLSv1.2	273 riverbed webey com	0x018	Client Hello
0,00,00.07.25.150051	0.000052000	192.100.2.109	175.245.0.154	1001.2	275 TIVET DEG. WEDEX.COM	01010	

# Do a bunch of DNS queries...names likely learned from "main server"

SS	.handshake.extensions_server_nar	me    dns						Expression + Apply this fit
No.	Time T	Time delta from previo The RTT to ACK the segme Time since request	Source	Destination	Protocol L	ength Server Name	Flags	Info
	6654 08:57:28.562694	0.007951000	192.168.2.105	173.243.0.154	TLSv1.2	241 riverbed.webex.com	0x018	Client Hello
	6692 08:57:28.826087	0.000154000	192.168.2.105	173.243.0.154	TLSv1.2	273 riverbed.webex.com	0x018	Client Hello
	6798 08:57:28.952974	0.000406000	192.168.2.105	173.243.0.154	TLSv1.2	273 riverbed.webex.com	0x018	Client Hello
	6799 02.57.22 952136	0 005162000	102 168 2 105	172 2/12 0 15/	TI Sv1 2	2/1 riverbed webey com	Øv01₽	Client Hello
	6800 08:57:28.967226	0.009090000	192.168.2.105	192.168.2.1	DNS	78		Standard query 0x2166 A emcbmm10.webex.com
	6801 08:57:28.967506	0.000280000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x0029 A ed1sjcbmm10.webex.com
	6802 08:57:28.967786	0.000280000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x718b A ed1txcbmm80.webex.com
	6803 08:57:28.968389	0.000603000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x4af3 A ed1lncbmm60.webex.com
	6804 08:57:28.968673	0.000284000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x426c A ed1vacbmm30.webex.com
	6805 08:57:28.969171	0.000498000	192.168.2.105	192.168.2.1	DNS	78		Standard query 0xdc0c A emcbmm20.webex.com
	6806 08:57:28.969338	0.000167000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0xf19a A ed1sycbmm90.webex.com
	6808 08:57:28.969846	0.000011000	192.168.2.105	192.168.2.1	DNS	82		Standard query 0xb39a A ed1chcbmm100.webex.com
	6809 08:57:28.969877	0.000031000	192.168.2.105	192.168.2.1	DNS	79		Standard query 0x025e A emvcbmm10.webex.com
	6811 08:57:28.970022	0.000127000	192.168.2.105	192.168.2.1	DNS	79		Standard query 0x7265 A emvcbmm20.webex.com
	6812 08:57:28.970141	0.000119000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x14e7 A ed1sgcbmm10.webex.com
	6813 08:57:28.970701	0.000560000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x6662 A ed1hkcbmm70.webex.com
	6814 08:57:28.970712	0.000011000	192.168.2.105	192.168.2.1	DNS	87		Standard query 0xf325 A ed1jpcbmm50-nrt02.webe
		0.022-10000	102.100.2.1	102 169 2 105	DNC			Standard query response 0x+200 A adichebrar100
	6000 00,57,20,990924	0.002180000	192.100.2.1	102 169 2 105	DNS	98		Standard query response 0x0598 A edithcomm100
		0.000703000	192.100.2.1	102 160 2 105	DNS	94		Standard query response 0x2100 A emcommite.webe.
	6024 00.07.20.990717	0.000030000	102.100.2.1	102 169 2 105	DNS	97		Standard query response 0x1ab A edition with the standard query response 0x1af2 A edilarchmm60 w
	6026 00.57.20.990751	0.000014000	102.100.2.1	102 169 2 105	DNS	97		Standard query response 0x4ars A equincommod.web
	6007 00.57.20.990745	0.000014000	102.100.2.1	102 169 2 105	DNS	07		Standard query response 0x4000 A encommon webe.
	6020 00.57.20.990750	0.000011000	102.100.2.1	102 169 2 105	DNS	102		Standard query response 0x119a A edisyconnin50.m.
	6020 00:57:20 000219	0.0005405000	102.100.2.1	102 169 2 105	DNS	07		Standard query response 0x1325 A edisperimino-1.
	6850 08:57:29.000840	0.001276000	192.108.2.1	102 168 2 105	DNS	97		Standard query response 0x0020 A edicichum10
	6868 08:57:29 031902	0.001270300	192.108.2.1	192.168.2.105	DNS	97		Standard query response 0x6662 A ediblechum70 .
	6871 08:57:29 038389	0.000110300	192.168.2.1	192 168 2 105	DNS	95		Standard query response 0x0002 A curricomm10 web
	6872 08:57:29 038/08	0.000000000	192.168.2.1	192.168.2.105	DNS	95		Standard query response 0x7265 A emychamile. web
	6923 08:57:29 112171	0.000013000	192.168 2 105	6/ 68 10/ 1/0	TLSv1 2	211 ed1vachmm30 webey com	0x018	Client Hello
	602/ 08:57:20 1125/5	0.00002000	102.168.2.105	172 2/12 0 06	TLSV1.2	244 eurvacommila webey.com	0x018	Client Hello
	6927 08:57:29 12324	0.000915000	192.168 2 105	173 2/13 0 97	TLSv1.2	241 emchmm20 webex.com	0x018	Client Hello
	6930 08:57:29 12/70/	0.000579300	192.168 2 105	200 107 222 150	TLSv1.2	241 editychmm80 webex.com	0x018	Client Hello
	0,50,00.57.25.124/54	0.00070000	192.100.2.109	203.137.222.133	12301.2		0,010	
_	6033 08.57.20 120201	0 000625000	102 168 2 105	1/2 2/2 / /6	11 Sv1 2	1/15 Adlenenmiluu Wahay com		I LIGHT HOLLO
	6933 08:57:29.128294	0.000625000	192.168.2.105	1/3.243.4./6	TLSv1.2	245 edicncbmm100.webex.com	0x018 0x018	Client Hello
	6933 08:57:29.128294 6955 08:57:29.134995	0.000625000 0.000945000 0.000945000	192.168.2.105 192.168.2.105 102.168.2.105	1/3.243.4.76 173.243.0.154	TLSv1.2 TLSv1.2	245 edichcomm100.webex.com 273 riverbed.webex.com	0x018 0x018 0x018	Client Hello

## Get the DNS responses...

	ssl.handshake.extensions_server_na	ame    dns						Expression + Apply this fil
No.	Time	Time delta from previe The RTT to ACK the segme Time since request	Source	Destination	Protocol L	ength Server Name	Flags	Info
	6654 08:57:28.562694	0.007951000	192.168.2.105	173.243.0.154	TLSv1.2	241 riverbed.webex.com	0x018	Client Hello
	6692 08:57:28.826087	0.000154000	192.168.2.105	173.243.0.154	TLSv1.2	273 riverbed.webex.com	0x018	Client Hello
	6798 08:57:28.952974	0.000406000	192.168.2.105	173.243.0.154	TLSv1.2	273 riverbed.webex.com	0x018	Client Hello
	6799 08:57:28.958136	0.005162000	192.168.2.105	173.243.0.154	TLSv1.2	241 riverbed.webex.com	0x018	Client Hello
	6800 08:57:28.967226	0.009090000	192.168.2.105	192.168.2.1	DNS	78		Standard query 0x2166 A emcbmm10.webex.com
	6801 08:57:28.967506	0.000280000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x0029 A ed1sjcbmm10.webex.com
	6802 08:57:28.967786	0.000280000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x718b A ed1txcbmm80.webex.com
	6803 08:57:28.968389	0.000603000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x4af3 A ed1lncbmm60.webex.com
	6804 08:57:28.968673	0.000284000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x426c A ed1vacbmm30.webex.com
	6805 08:57:28.969171	0.000498000	192.168.2.105	192.168.2.1	DNS	78		Standard query 0xdc0c A emcbmm20.webex.com
	6806 08:57:28.969338	0.000167000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0xf19a A ed1sycbmm90.webex.com
	6808 08:57:28.969846	0.000011000	192.168.2.105	192.168.2.1	DNS	82		Standard query 0xb39a A ed1chcbmm100.webex.com
	6809 08:57:28.969877	0.000031000	192.168.2.105	192.168.2.1	DNS	79		Standard query 0x025e A emvcbmm10.webex.com
	6811 08:57:28.970022	0.000127000	192.168.2.105	192.168.2.1	DNS	79		Standard query 0x7265 A emvcbmm20.webex.com
	6812 08:57:28.970141	0.000119000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x14e7 A ed1sgcbmm10.webex.com
	6813 08:57:28.970701	0.000560000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x6662 A ed1hkcbmm70.webex.com
			100 100 0 105	100 100 0 1		^7 		
	6821 08:57:28.993744	0.022418000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x426c A ed1vacbmm30.w
	6822 08:57:28.995924	0.002180000	192.168.2.1	192.168.2.105	DNS	98		Standard query response 0xb39a A ed1chcbmm100
	6823 08:57:28.996687	0.000/63000	192.168.2.1	192.168.2.105	DNS	94		Standard query response 0x2166 A emcbmm10.webe
	6824 08:57:28.996717	0.000030000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x/18b A ed1txcbmm80.w
	6825 08:57:28.996731	0.000014000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x4a+3 A ediincomm60.w
	6826 08:57:28.996745	0.000014000	192.168.2.1	192.168.2.105	DNS	94		Standard query response 0xdc0c A emcbmm20.webe
	6827 08:57:28.996756	0.000011000	192.168.2.1	192.168.2.105	DNS	9/		Standard query response 0x+19a A ed1sycbmm90.w
	6828 08:57:29.000219	0.003463000	192.168.2.1	192.168.2.105	DNS	103		Standard query response 0x+325 A ed1jpcbmm50-n
	6829 08:57:29.000846	0.000627000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x14e/ A edisgcbmm10.w
	6850 08:57:29.024120	0.0012/6000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x0029 A ed1sjcbmm10.w
	6868 08:57:29.031893	0.001148000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x6662 A ed1hkcbmm/0.w
	68/1 08:57:29.038389	0.000600000	192.168.2.1	192.168.2.105	DNS	95		Standard query response 0x025e A emvcbmm10.web
	68/2 08:5/:29.038408	0.000019000	192.168.2.1	192.168.2.105	DNS	95		Standard duerv response 0x7265 A emvcbmm20.web
È	6923 08:57:29.1121/1	0.000002000	102 168 2 105	172 242 0 06	TLSV1.2	244 edivacomm30.webex.com	0x018	Client Hello
	6924 08:57:29.112545	0.000374000	192.108.2.105	173.243.0.90	TLSVI.Z	241 emcbmm10.webex.com	0x018	Client Hello
	6020 00.57.29.123244	0.00051000	102.100.2.105	200 107 222 150	TLSV1.2	241 editychmm20 webex.com	0x010	Client Hello
	6022 00.57.29.124/94	0.000625000	102 169 2 105	172 2/2 / 76	TLSV1.2	244 eultxcommod.webex.com	0x010	Client Hello
	6055 00.57.29.128294	0.000025000	102 168 2 105	172 242.4.70	TLSV1.2	273 niverbed webey com	0x010	Client Hello
	6060 08:57:29.134995	0.000545000	102 168 2 105	172 242.0.104	TLSV1.2	273 niverbed webey.com	0x010	Client Hello
	0900 08.97:29.138051	0.000092000	192.100.2.100	175.245.0.154	ILSVI.Z	275 HIVEFBEU.WEDEX.COM	07019	CITCHE HEILO

## **Open SSL connections to the servers just found...**

ssl	ssl.handshake.extensions_server_name    dns 🛛 🗠 Expression + Apply this fit									
No.	Time	Time delta from previv The RTT to ACK the segme Time since request	Source	Destination	Protocol L	ength Server Name	Flags	Info		
	6654 08:57:28.562694	0.007951000	192.168.2.105	173.243.0.154	TLSv1.2	241 riverbed.webex.com	0x018	Client Hello		
	6692 08:57:28.826087	0.000154000	192.168.2.105	173.243.0.154	TLSv1.2	273 riverbed.webex.com	0x018	Client Hello		
	6798 08:57:28.952974	0.000406000	192.168.2.105	173.243.0.154	TLSv1.2	273 riverbed.webex.com	0x018	Client Hello		
	6799 08:57:28.958136	0.005162000	192.168.2.105	173.243.0.154	TLSv1.2	241 riverbed.webex.com	0x018	Client Hello		
	6800 08:57:28.967226	0.009090000	192.168.2.105	192.168.2.1	DNS	78		Standard query 0x2166 A emcbmm10.webex.com		
	6801 08:57:28.967506	0.000280000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x0029 A ed1sjcbmm10.webex.com		
	6802 08:57:28.967786	0.000280000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x718b A ed1txcbmm80.webex.com		
	6803 08:57:28.968389	0.000603000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x4af3 A ed1lncbmm60.webex.com		
	6804 08:57:28.968673	0.000284000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x426c A ed1vacbmm30.webex.com		
	6805 08:57:28.969171	0.000498000	192.168.2.105	192.168.2.1	DNS	78		Standard query 0xdc0c A emcbmm20.webex.com		
	6806 08:57:28.969338	0.000167000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0xf19a A ed1sycbmm90.webex.com		
	6808 08:57:28.969846	0.000011000	192.168.2.105	192.168.2.1	DNS	82		Standard query 0xb39a A ed1chcbmm100.webex.com		
	6809 08:57:28.969877	0.000031000	192.168.2.105	192.168.2.1	DNS	79		Standard query 0x025e A emvcbmm10.webex.com		
	6811 08:57:28.970022	0.000127000	192.168.2.105	192.168.2.1	DNS	79		Standard query 0x7265 A emvcbmm20.webex.com		
	6812 08:57:28.970141	0.000119000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x14e7 A ed1sgcbmm10.webex.com		
	6813 08:57:28.970701	0.000560000	192.168.2.105	192.168.2.1	DNS	81		Standard query 0x6662 A ed1hkcbmm70.webex.com		
	6814 08:57:28.970712	0.000011000	192.168.2.105	192.168.2.1	DNS	87		Standard query 0xf325 A ed1jpcbmm50-nrt02.webe		
	6821 08:57:28.993744	0.022418000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x426c A ed1vacbmm30.w		
	6822 08:57:28.995924	0.002180000	192.168.2.1	192.168.2.105	DNS	98		Standard query response 0xb39a A ed1chcbmm100		
	6823 08:57:28.996687	0.000763000	192.168.2.1	192.168.2.105	DNS	94		Standard query response 0x2166 A emcbmm10.webe		
	6824 08:57:28.996717	0.00030000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x718b A ed1txcbmm80.w		
	6825 08:57:28.996731	0.00014000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x4af3 A ed1lncbmm60.w		
	6826 08:57:28.996745	0.00014000	192.168.2.1	192.168.2.105	DNS	94		Standard query response 0xdc0c A emcbmm20.webe		
	6827 08:57:28.996756	0.000011000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0xf19a A ed1sycbmm90.w		
	6828 08:57:29.000219	0.003463000	192.168.2.1	192.168.2.105	DNS	103		Standard query response 0xf325 A ed1jpcbmm50-n		
	6829 08:57:29.000846	0.000627000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x14e7 A ed1sgcbmm10.w		
	6850 08:57:29.024120	0.001276000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x0029 A ed1sjcbmm10.w		
	6868 08:57:29.031893	0.001148000	192.168.2.1	192.168.2.105	DNS	97		Standard query response 0x6662 A ed1hkcbmm70.w		
	6871 08:57:29.038389	0.000600000	192.168.2.1	192.168.2.105	DNS	95		Standard query response 0x025e A emvcbmm10.web		
	6923 08.57.29 112171	0 00002000	192 168 2 105	64 68 104 140	TLSv1 2	244 ed1yachmm30 webey com	0x018	Client Hello		
į.	6924 08:57:29 1125/5	0 000374000	192 168 2 105	173 243 0 96	TLSv1 2	241 emchamm10 webex com	0x018	Client Hello		
1	6027 08:57:29.11234	0.000974000	192.108.2.105	173 243 0 07	TLSV1.2	241 emchmm20 webey.com	0x018	Client Hello		
i I	6930 08.57.29.123244	0.000515000	192 168 2 105	200 107 222 150	TLSv1 2	241 editychmm80 webex.com	0x018	Client Hello		
	6033 08-57-20 120204	0.000675000	102 168 2 105	173 243 4 76	TLSV1.2	244 currecommise. webey. com	0x010	Client Hello		
ļ.	6055 00.57.29.120294	0.000025000	102 169 2 105	172 242 0 154	TI Sv1 2	273 niverbed webey com	0,010	Client Hello		
	6060 08.57.20 120051	0.000545000	102 168 2 105	173 243.0.154	TLSV1.2	273 niverbed webey com	0x010	Client Hello		
i i	6071 08.57.29.150051	0.000032000	102 168 2 105	6/ 68 101 152	TLSV1.2	2/1 edisichmm10 webex.com	0x010	Client Hello		

## App Behavior Recap

Client finds "main" server via DNS

Client opens 4 connections to "main" server

Client then does a burst of DNS queries

Client then opens one (1) connection to each "new" server

## Discussion



• We can now eliminate traffic that's not going to these servers

 We can also see the internal connection management behavior of the client side of the App

We'll take our break here, and when we come back for Part II we'll identify root cause using the advanced analytics

