



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](mailto:john.pittle@riverbed.com)  
[@end2endviz](#)  
[www.linkedin.com/in/john-pittle](http://www.linkedin.com/in/john-pittle)



# Session Overview

## Two Part Session

- ⦿ Deep Dive troubleshooting into the Webex “98% hang” condition (circa 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

- ⦿ 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

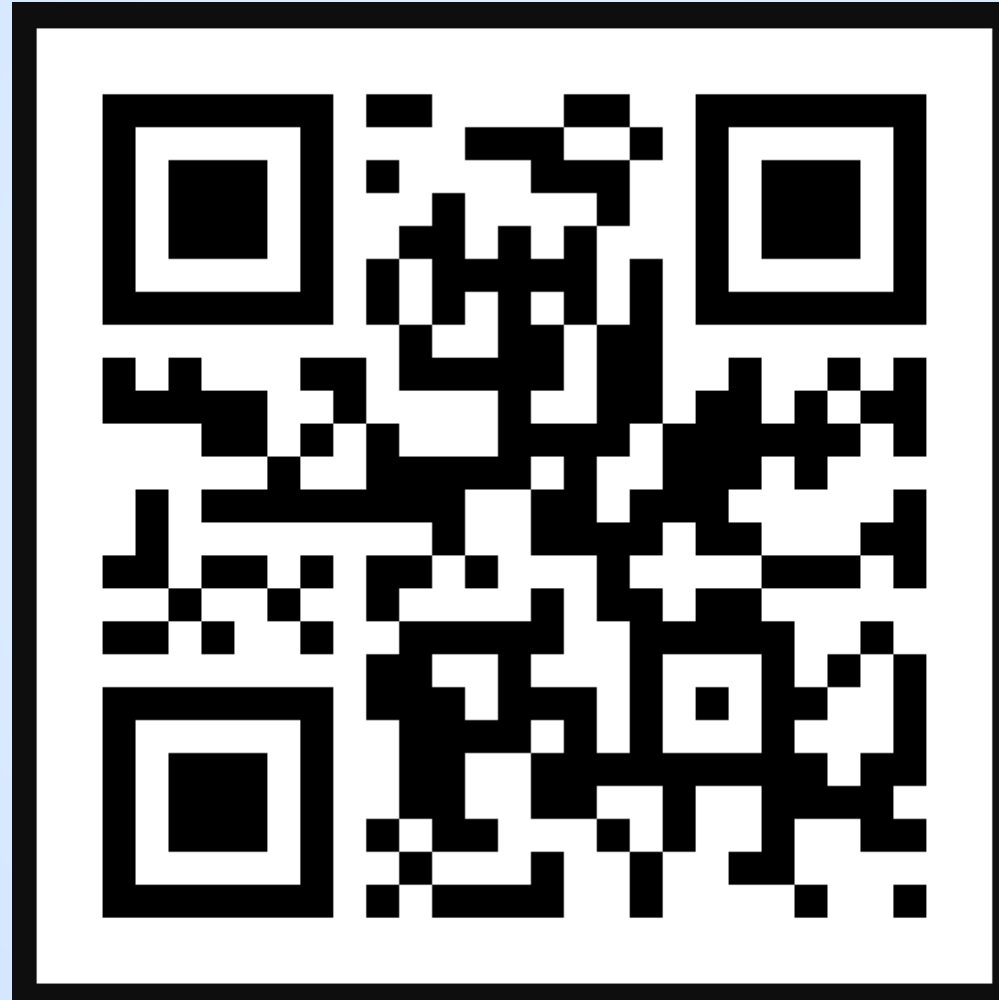
[john.pittle@riverbed.com](mailto:john.pittle@riverbed.com)

[@end2endviz](#)

[www.linkedin.com/in/john-pittle](http://www.linkedin.com/in/john-pittle)

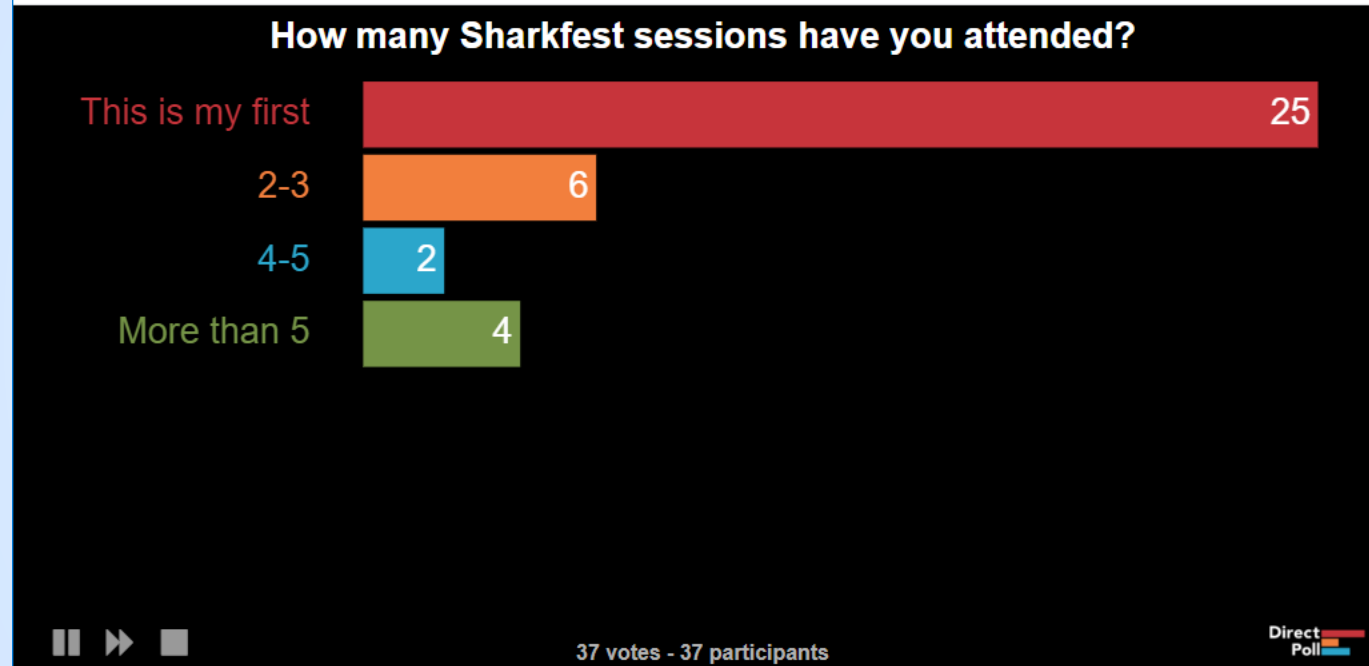


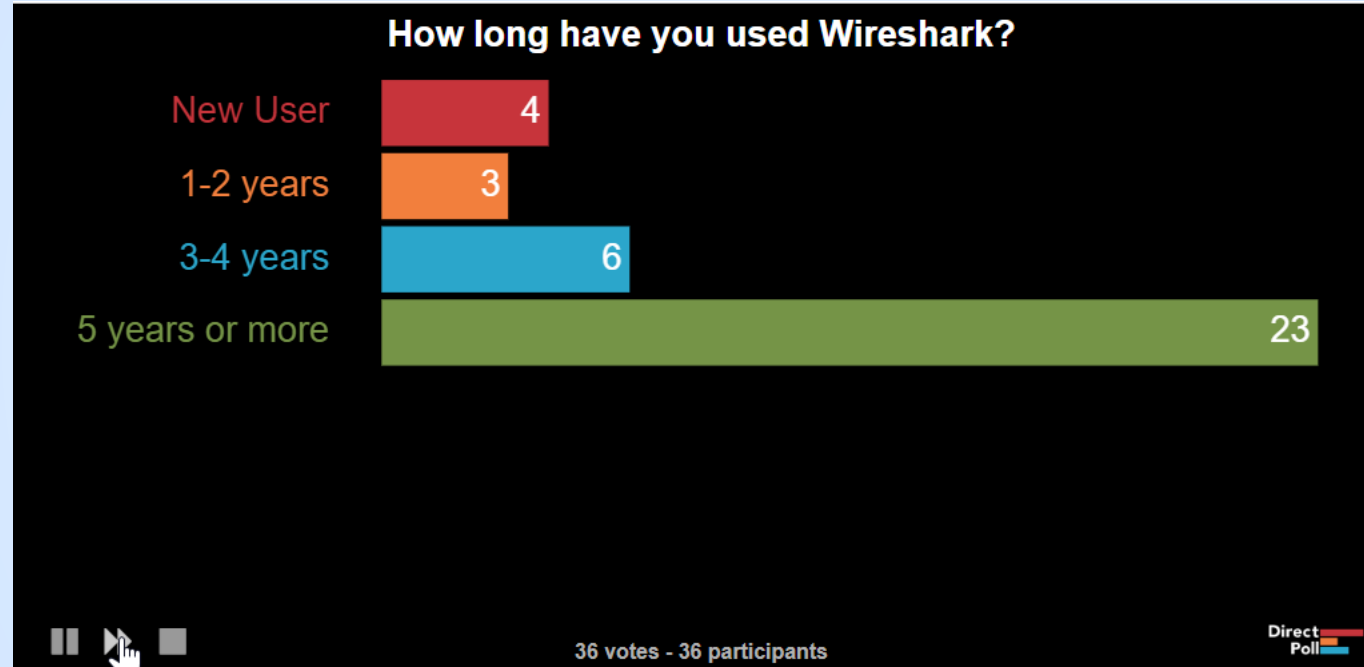
# Getting to know the attendees...a quick survey

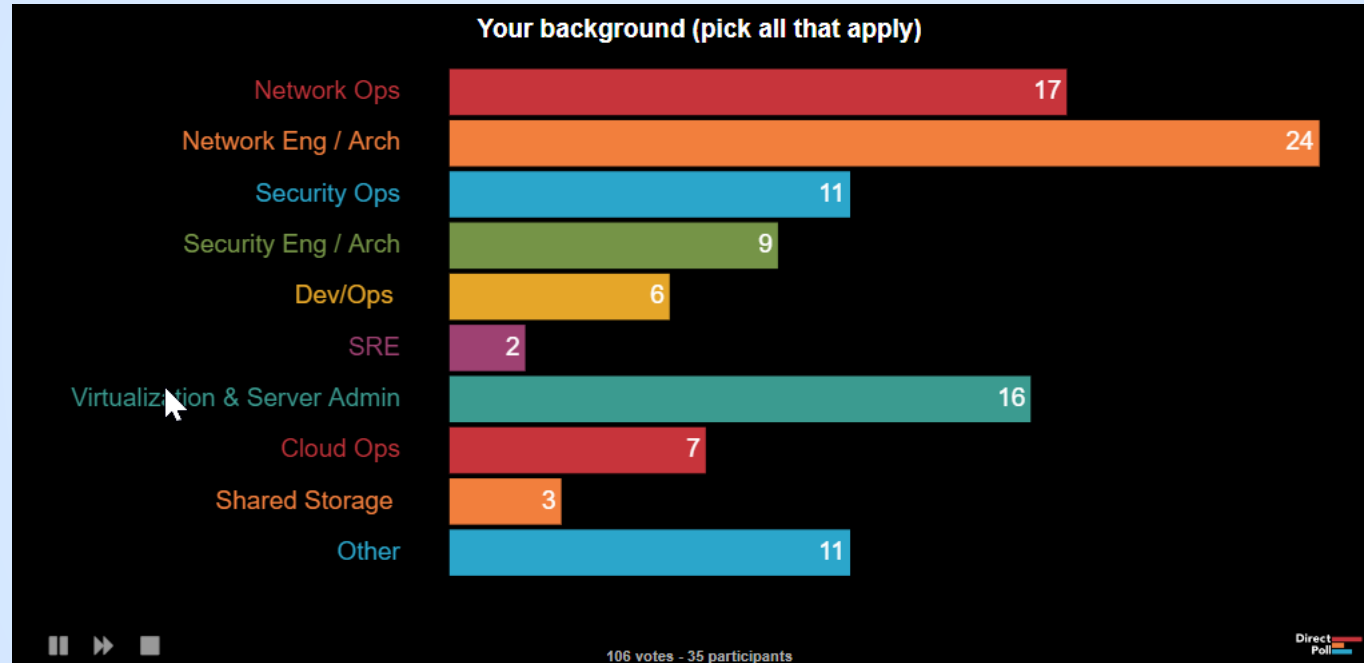


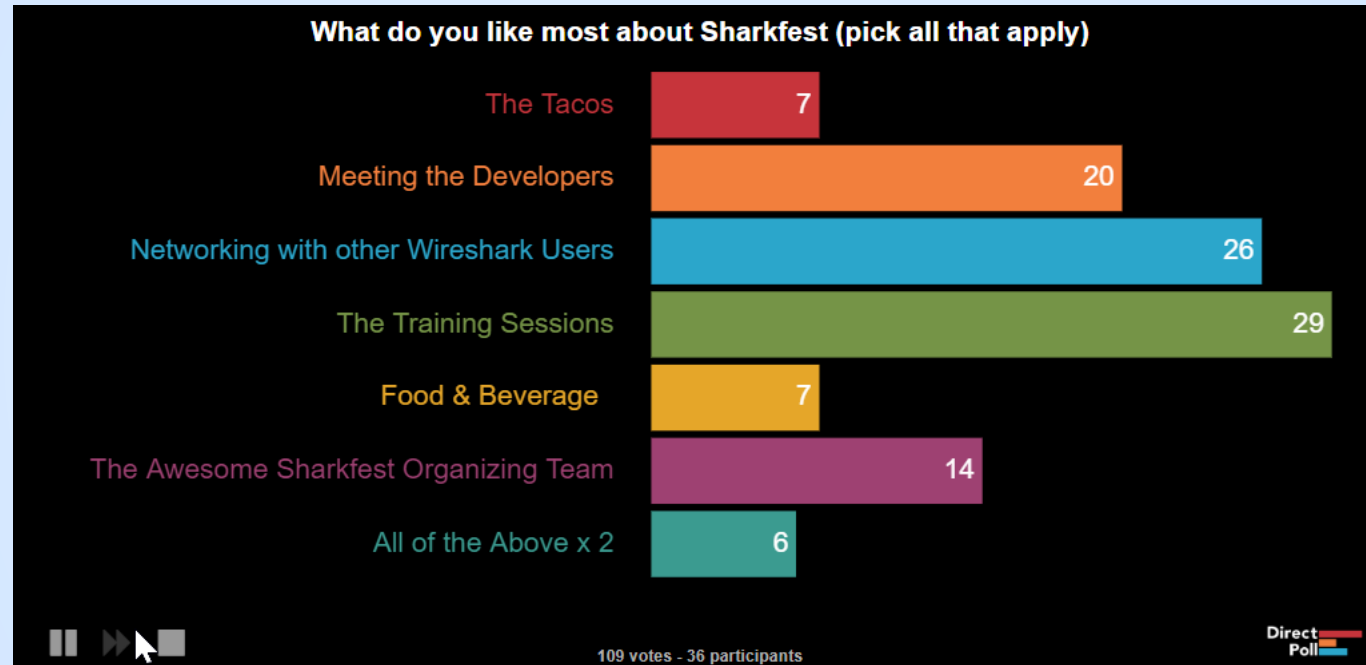
#sf23us - University of San Diego - June 10 - June 15













# 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...






## Lab Files to Download







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





<input type="checkbox"/>	Name	Size	Modified
<input type="checkbox"/>	 sfus23-sess 08 download v2.zip	20.8 MB	an hour ago
1 file		20.8 MB	



Name	Type	Compressed size	Password pr
 Analysis Results-Action Items Template v0...	Microsoft Excel 97-2003 Wor...	12 KB	No
 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
 webex_98pct_resolved16_56_52edt@2018-...	ACE Capture File	21,279 KB	No
 wireshark display filter.txt	Text Document	1 KB	No



#sf23us - University of San Diego - June 10 - June 15



Secure | <https://riverbed.webex.com/wbxmjs/join/service/join?backurl=https%3A%2F%2Friverbed.webex.com%2Fmc3100%2FforwardAction.do%3Fsiteurl%3Diverbed&pgvDone=15247438028...>

for Business

Cisco WebEx Meeting Center

# The Infamous 98% Hang Condition

John Pittle's Personal Room

Host: John Pittle

98%

Preparing your meeting...

 Having trouble joining the meeting?  
[Generate problem report](#)



Connecting... 



# 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
- Different users react 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
- ⦿ Document 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

- ① Confirm time bounds of the issue
- ① Determine which Servers are in scope for investigation
- ① Determine which Servers are causing / contributing to the hang
- ① Determine the nature of the (abnormal) condition(s) in play
- ① 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>



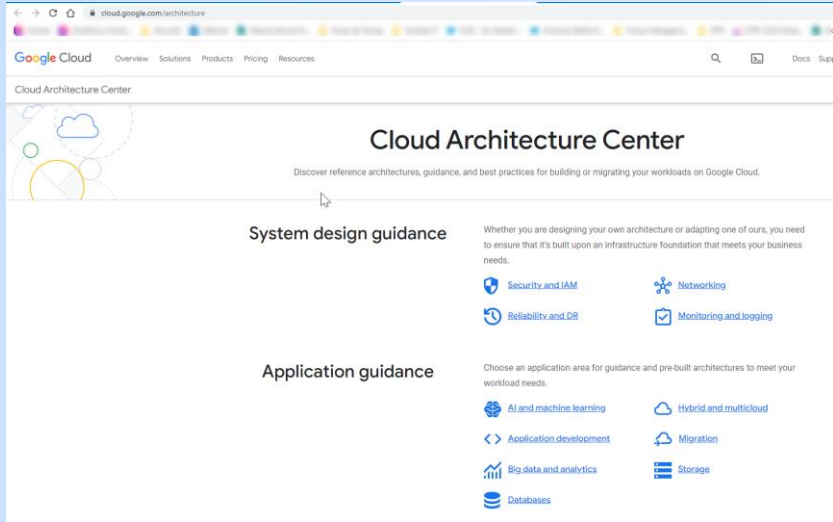
# 3<sup>rd</sup> Party Cloud / SaaS App Characteristics

These are not absolutes, but are highly likely

- ⦿ There's no one to ask, we have to figure it out for ourselves
- ⦿ 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
- ⦿ Users in different regions may be using different client facing servers
- ⦿ Multiple vendors may be embedded in the architecture

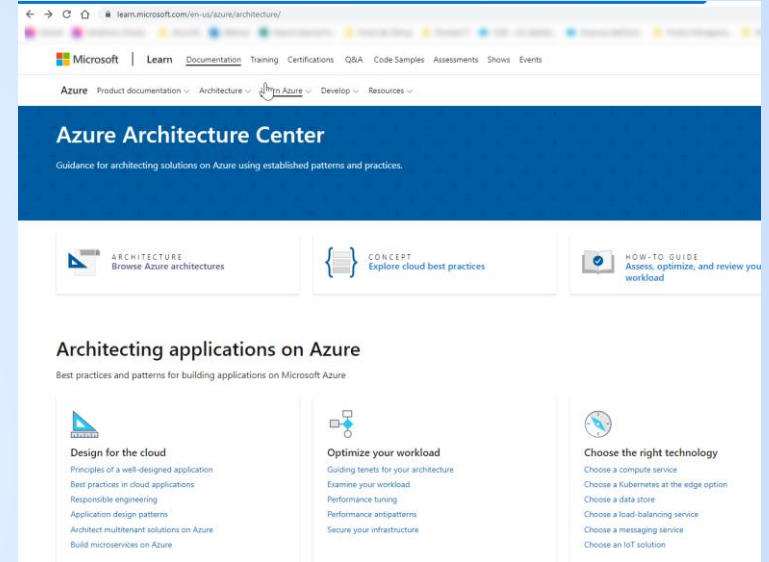
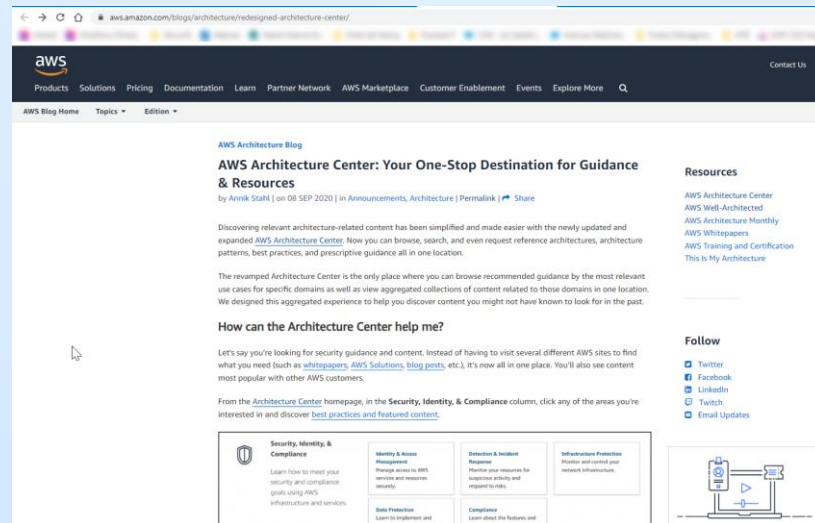


# Cloud Native Architecture Guidance



Google

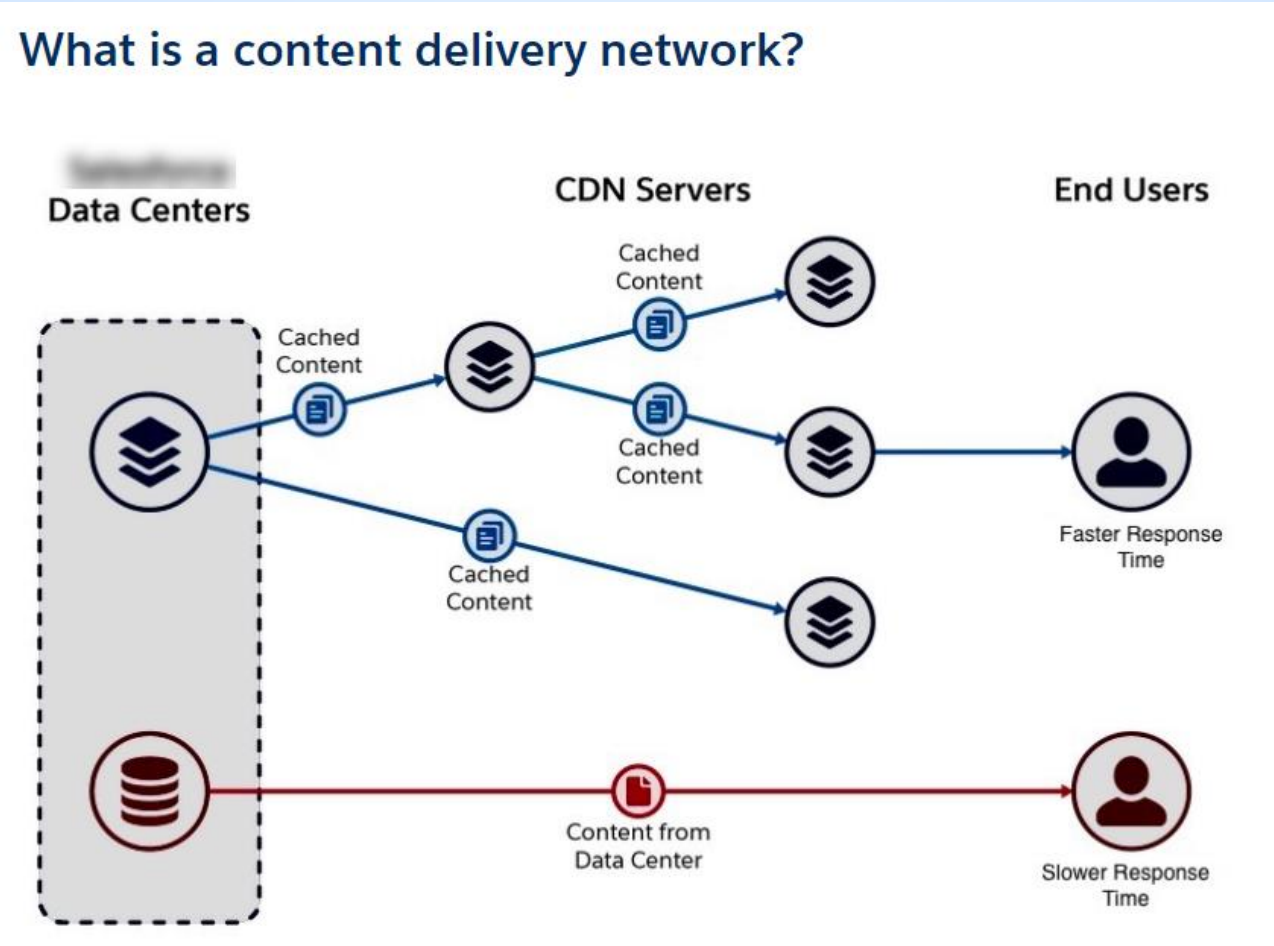
AWS



Azure



# Content Delivery Networks (CDN)





# 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?
- ⦿ Does 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
- 100Mbps Download / 6Mbps Upload
- VPN was *\*not\** active
- Many other apps were open at the time - adds to complexity of the analysis
- Hyperlink to personal room was clicked at ~ 16:56.02 EDT on June 5th
- The “98% hang” condition cleared itself ~ 16:56:58



Details

**File**

Name: C:\OPNET  
 Captures\webex-98pct\webex\_98pct\_resolved16\_56\_52edt@2018-06-05\_16.58.06@localhost.appcapture  
 Length: 24 MB  
 Hash (SHA256): 2898a9442f718df55424f6db6dd9b3749db4159e4fd4319d0bedfc90ce38c218  
 Hash (RIPEMD160): b46b45c83ab53023f5e355a9ae6a6b7371540228  
 Hash (SHA1): 503f6b0a8f2ccc12d5a2fb929a01aac0ae7d36a  
 Format: Wireshark/tcpdump/... - pcap  
 Encapsulation: Ethernet  
 Snapshot length: 65536 

**Time**

First packet: 2018-06-05 16:47:27  
 Last packet: 2018-06-05 16:57:25  
 Elapsed: 00:09:58

**Capture**

Hardware: Unknown  
 OS: Unknown  
 Application: Unknown

**Interfaces**

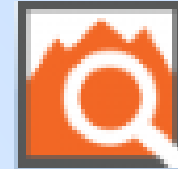
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65536 bytes

**Statistics**

Measurement	Captured	Displayed	Marked
Packets	32568	32568 (100.0%)	—
Time span, s	598.066	598.066	—
Average pps	54.5	54.5	—
Average packet size, B	722	722	—
Bytes	23506696	23506696 (100.0%)	0
Average bytes/s	39 k	39 k	—
Average bits/s	314 k	314 k	—



# Analysis Methodology



- ⦿ Used a combination of Wireshark and advanced analytics
- ⦿ Alluvio Transaction Analyzer is a wrapper around tshark
- ⦿ Use Wireshark to find Webex servers via DNS queries
- ⦿ Use Wireshark to display the server name (SNI) for all SSL connections
- ⦿ Use 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



# Wireshark Lab Activities

---



- ① Launch Wireshark
- ② Open the PCAP file you downloaded from Packet-Foo
- ③ Navigate to Statistics -> Conversations



# Wireshark Capture Overview

## Unfiltered Capture

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

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	—	—



# 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
- DNS 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

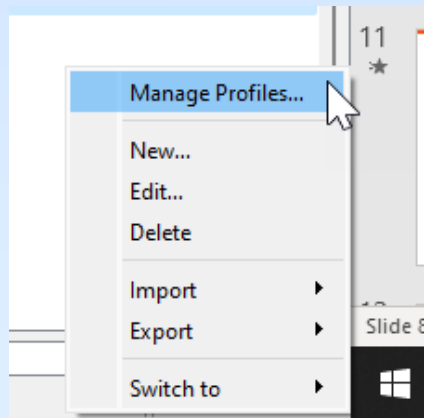
1

Right Mouse Click

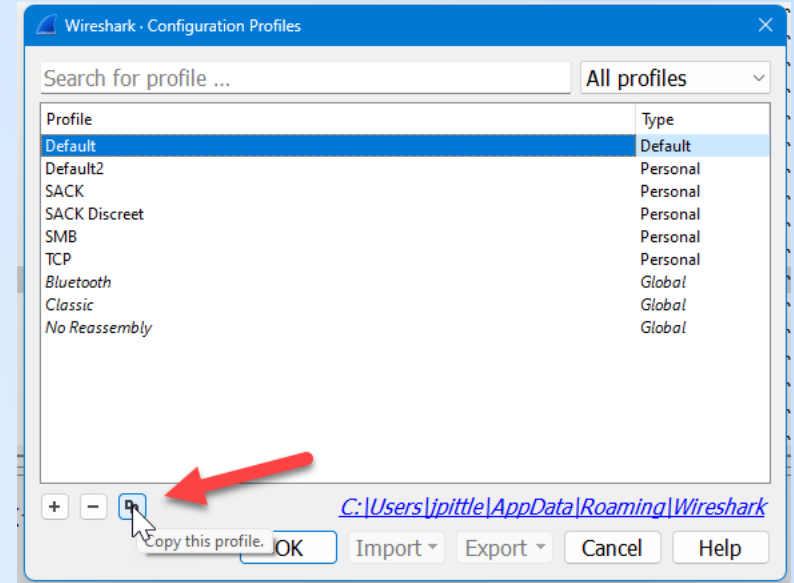


Packets: 32568 · Displayed: 34 (0.1%) || Profile: Default

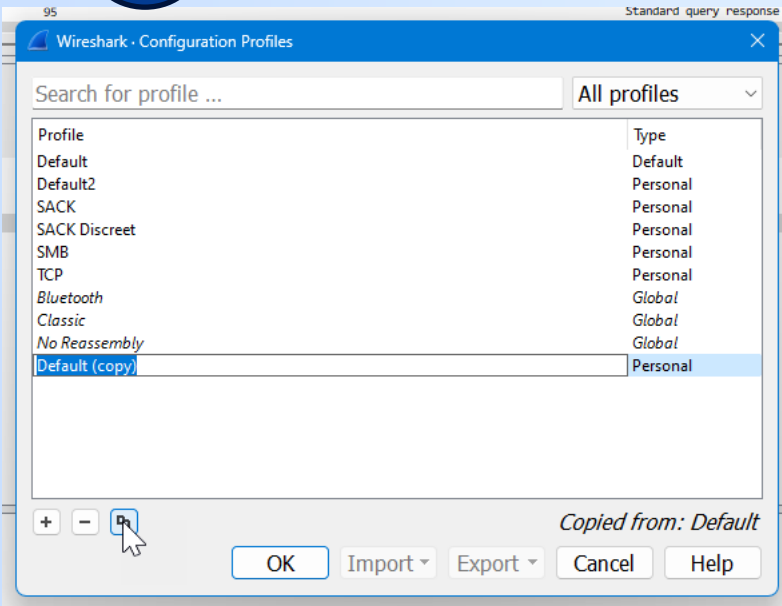
2



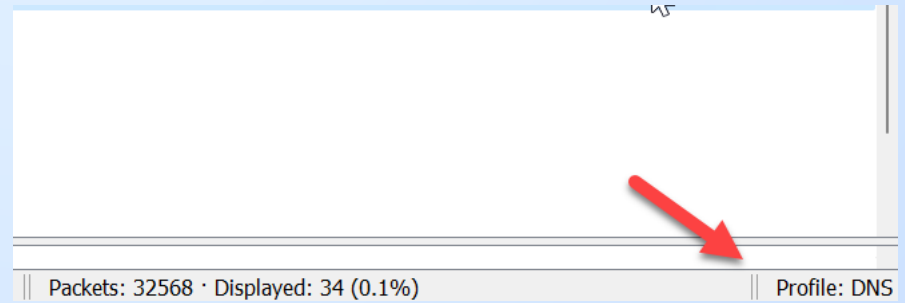
3



4



5





# Add any protocol field as column to summary view

```
> Frame 2466: 91 bytes on wire (728 bits), 91 bytes captured (728 bits)
> Ethernet II, Src: IntelCor_25:2d:3f (f0:d5:bf:25:2d:3f), Dst: Cisco-Li_91:b1:fe (48:f8:b3:91:b1:fe)
> Internet Protocol Version 4, Src: 192.168.2.105, Dst: 192.168.2.1
> User Datagram Protocol, Src Port: 51164, Dst Port: 53
v Domain Name System (query)
  Transaction ID: 0x303f
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  v Queries
    v lp-push-server-553.lastpass.com: type A, class IN
      Name: lp-push-server-553.lastpass.com
      [Name Length: 31]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      [Response In: 2467]
```

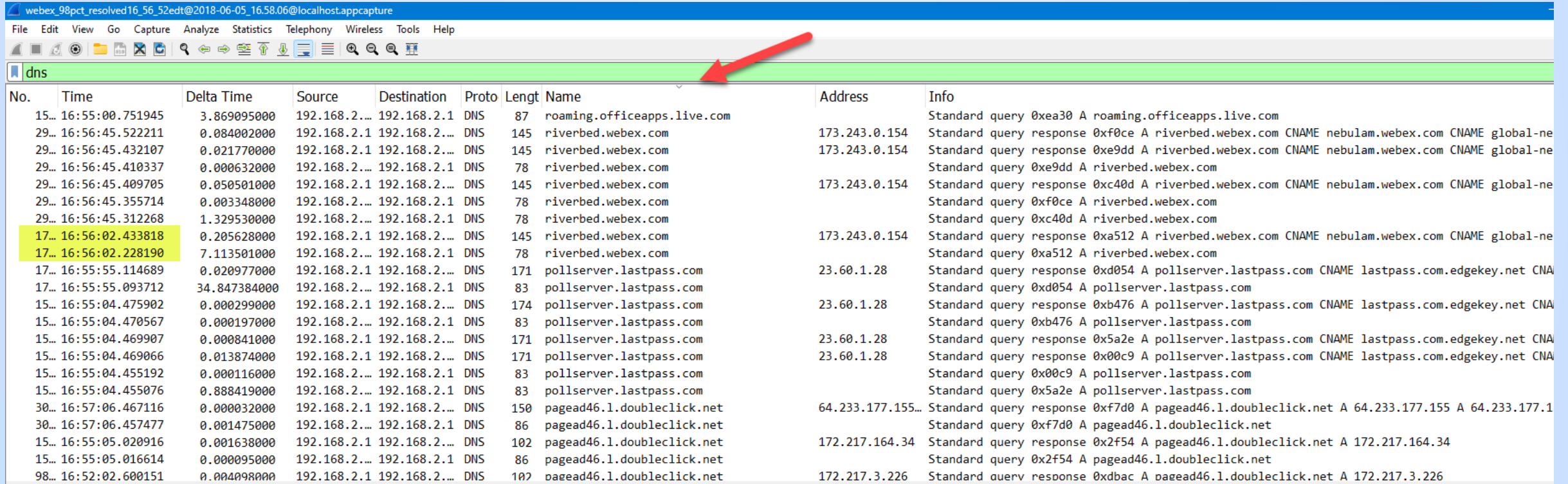
- Expand Subtrees
- Collapse Subtrees
- Expand All
- Collapse All
- Apply as Column Ctrl+Shift+I
- Apply as Filter
- Prepare as Filter
- Conversation Filter
- Colorize with Filter
- Follow
- Copy
- Show Packet Bytes... Ctrl+Shift+O
- Export Packet Bytes... Ctrl+Shift+X
- Wiki Protocol Page
- Filter Field Reference
- Protocol Preferences
- Decode As... Ctrl+Shift+U
- Go to Linked Packet





# Updated Summary View

Filtered by DNS and sort by server name column



No.	Time	Delta Time	Source	Destination	Proto	Length	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	78	riverbed.webex.com		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	83	pollserver.lastpass.com		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	83	pollserver.lastpass.com		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	83	pollserver.lastpass.com		Standard query 0x00c9 A pollserver.lastpass.com
15...	16:55:04.455076	0.888419000	192.168.2...	192.168.2.1	DNS	83	pollserver.lastpass.com		Standard query 0x5a2e A pollserver.lastpass.com
30...	16:57:06.467116	0.000032000	192.168.2.1	192.168.2...	DNS	150	pagead46.l.doubleclick.net	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	86	pagead46.l.doubleclick.net		Standard query 0xf7d0 A pagead46.l.doubleclick.net
15...	16:55:05.020916	0.001638000	192.168.2.1	192.168.2...	DNS	102	pagead46.l.doubleclick.net	172.217.164.34	Standard query response 0x2f54 A pagead46.l.doubleclick.net A 172.217.164.34
15...	16:55:05.016614	0.000095000	192.168.2...	192.168.2.1	DNS	86	pagead46.l.doubleclick.net		Standard query 0x2f54 A pagead46.l.doubleclick.net
98...	16:52:02.600151	0.004098000	192.168.2.1	192.168.2...	DNS	102	pagead46.l.doubleclick.net	172.217.3.226	Standard query response 0xdbac A pagead46.l.doubleclick.net A 172.217.3.226



# A better filter for our mission

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

The screenshot shows the Wireshark interface with a filter applied to the capture. The filter bar contains the text "dns.qry.name contains 'webex'", which is highlighted in green and pointed to by a red arrow. Below the filter bar, a table of network packets is displayed, showing several DNS queries for the domain "sec-tws-prod-vip.webex.com".

No.	Time	Delta Time	Source	Destination	Proto	Length	Name	Address	Info
29...	16:56:45.359204	0.003490000	192.168.2.1	192.168.2.1	DNS	86	sec-tws-prod-vip.webex.com		Standard query
29...	16:56:45.352366	0.000488000	192.168.2.1	192.168.2.1	DNS	86	sec-tws-prod-vip.webex.com		Standard query
29...	16:56:45.351878	0.002049000	192.168.2.1	192.168.2.1	DNS	102	sec-tws-prod-vip.webex.com	66.163.35.36	Standard query
29...	16:56:45.349829	0.000614000	192.168.2.1	192.168.2.1	DNS	86	sec-tws-prod-vip.webex.com		Standard query
29...	16:56:45.349215	0.003855000	192.168.2.1	192.168.2.1	DNS	102	sec-tws-prod-vip.webex.com	66.163.35.36	Standard query
29...	16:56:45.345360	0.002155000	192.168.2.1	192.168.2.1	DNS	86	sec-tws-prod-vip.webex.com		Standard query
29...	16:56:45.343205	0.000000000	192.168.2.1	192.168.2.1	DNS	102	sec-tws-prod-vip.webex.com	66.163.35.36	Standard query



# Even more better...

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

The image shows a Wireshark capture of DNS traffic. The filter bar at the top contains the filter: `dns.qry.name contains "webex" && dns.flags.response==1`. The packet list pane shows a series of DNS queries and responses. The packet details pane shows the structure of a DNS response, including the header, question section, and answer section. The packet bytes pane shows the raw data of the response.

No.	Time	Delta Time	Source	Destination	Proto	Lengt	Name	Address	Info
17...	16:56:02.433818	0.000000000	192.168.2.1	192.168.2.105	DNS	145	riverbed.webex.com	173.243.0.154	Standard query response 0xa512 A riverb
17...	16:56:02.441100	0.007282000	192.168.2.1	192.168.2.105	DNS	100	global-nebulam.webex.com	173.243.0.154	Standard query response 0xee05 A global
17...	16:56:02.553456	0.112356000	192.168.2.1	192.168.2.105	DNS	84	global-nebulam.webex.com		Standard query response 0xa856 AAAA glo
18...	16:56:04.162417	1.608961000	192.168.2.1	192.168.2.105	DNS	131	nebulam.webex.com	173.243.0.154	Standard query response 0xf8c2 A nebula
18...	16:56:04.474396	0							y response 0x0b3e A akamai
21...	16:56:10.320159	5							y response 0xd085 A sec-tw
21...	16:56:10.323249	0							y response 0x8c2c A sec-tw
21...	16:56:10.345079	0							y response 0xd508 AAAA sec
21...	16:56:10.950034	0							y response 0x9a1d A emcbmm
21...	16:56:10.954018	0							y response 0x559a A emcbmm
21...	16:56:10.973148	0							y response 0xae74 A ed11nc
21...	16:56:10.973271	0							y response 0x16cb A ed1txc
21...	16:56:10.973288	0							y response 0xc826 A ed1syc
21...	16:56:10.973306	0							y response 0x2fc4 A ed1sgc
21...	16:56:10.973320	0							y response 0xaba4 A ed1chc
21...	16:56:10.973333	0.000013000	192.168.2.1	192.168.2.105	DNS	97	ed1hkc01m10.webex.com	114.29.200.11	Standard query response 0x2160 A ed1hkc
21...	16:56:10.977981	0.004648000	192.168.2.1	192.168.2.105	DNS	103	ed1jpcbmm50-nrt02.webex.com	114.29.204.49	Standard query response 0x8027 A ed1jpc
21...	16:56:10.979253	0.001272000	192.168.2.1	192.168.2.105	DNS	95	emvcbmm20.webex.com	64.68.120.90	Standard query response 0x67c5 A emvcbm
21...	16:56:10.989277	0.010024000	192.168.2.1	192.168.2.105	DNS	97	ed1vacbmm30.webex.com	64.68.104.140	Standard query response 0xc7f4 A ed1vac
21...	16:56:10.989300	0.000023000	192.168.2.1	192.168.2.105	DNS	97	ed1sjcbmm10.webex.com	64.68.121.153	Standard query response 0xeef6 A ed1sjc
21...	16:56:11.015086	0.025786000	192.168.2.1	192.168.2.105	DNS	95	emvcbmm10.webex.com	64.68.120.70	Standard query response 0x6f84 A emvcbm
22...	16:56:12.145199	1.130113000	192.168.2.1	192.168.2.105	DNS	117	emcb31101.webex.com	64.68.101.20	Standard query response 0x0754 A emcb31
22...	16:56:12.636041	0.490842000	192.168.2.1	192.168.2.105	DNS	123	ed1vacb32201.webex.com	64.68.110.77	Standard query response 0x4906 A ed1vac
29...	16:56:45.342211	32.706170000	192.168.2.1	192.168.2.105	DNS	102	sec-tws-prod-vip.webex.com	66.163.35.36	Standard query response 0xd9d5 A sec-tw
29...	16:56:45.343205	0.000940000	192.168.2.1	192.168.2.105	DNS	102	sec-tws-prod-vip.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

```
2025-09-17 10:16:10.000000000 193.169.2.105
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
```





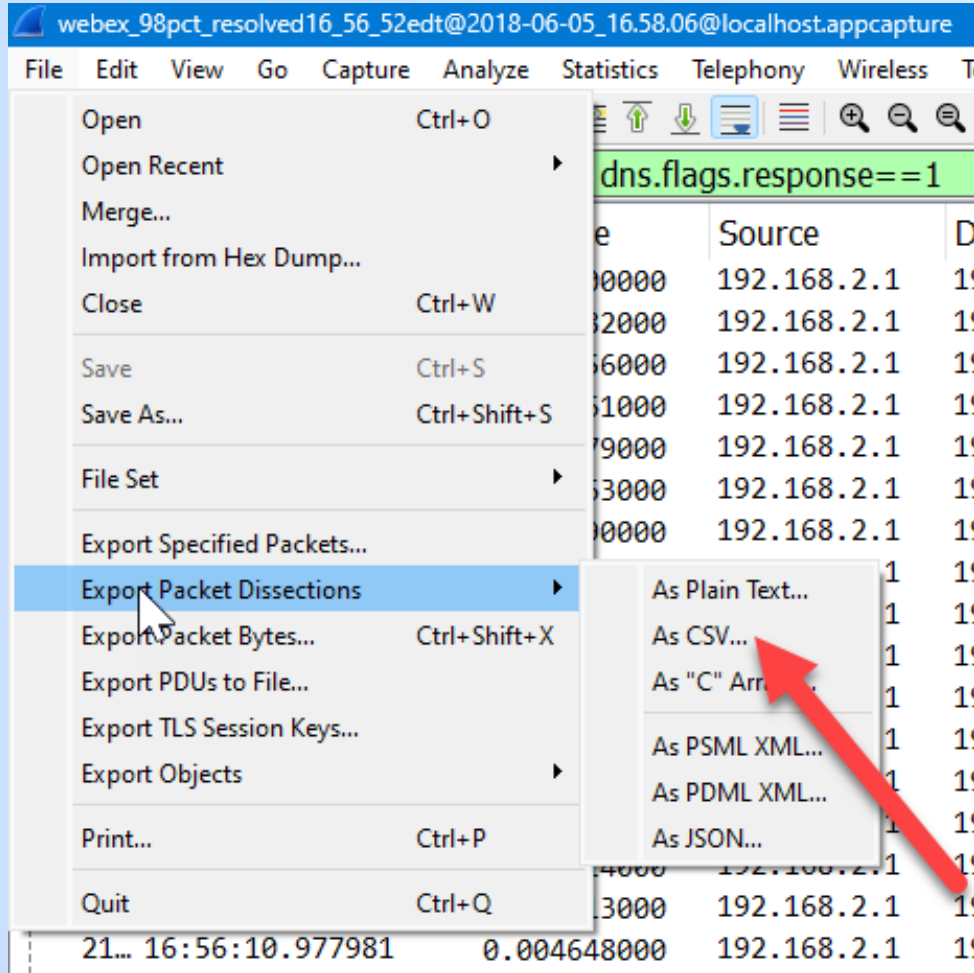
# Thinking ahead just a little...

- ⦿ 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...



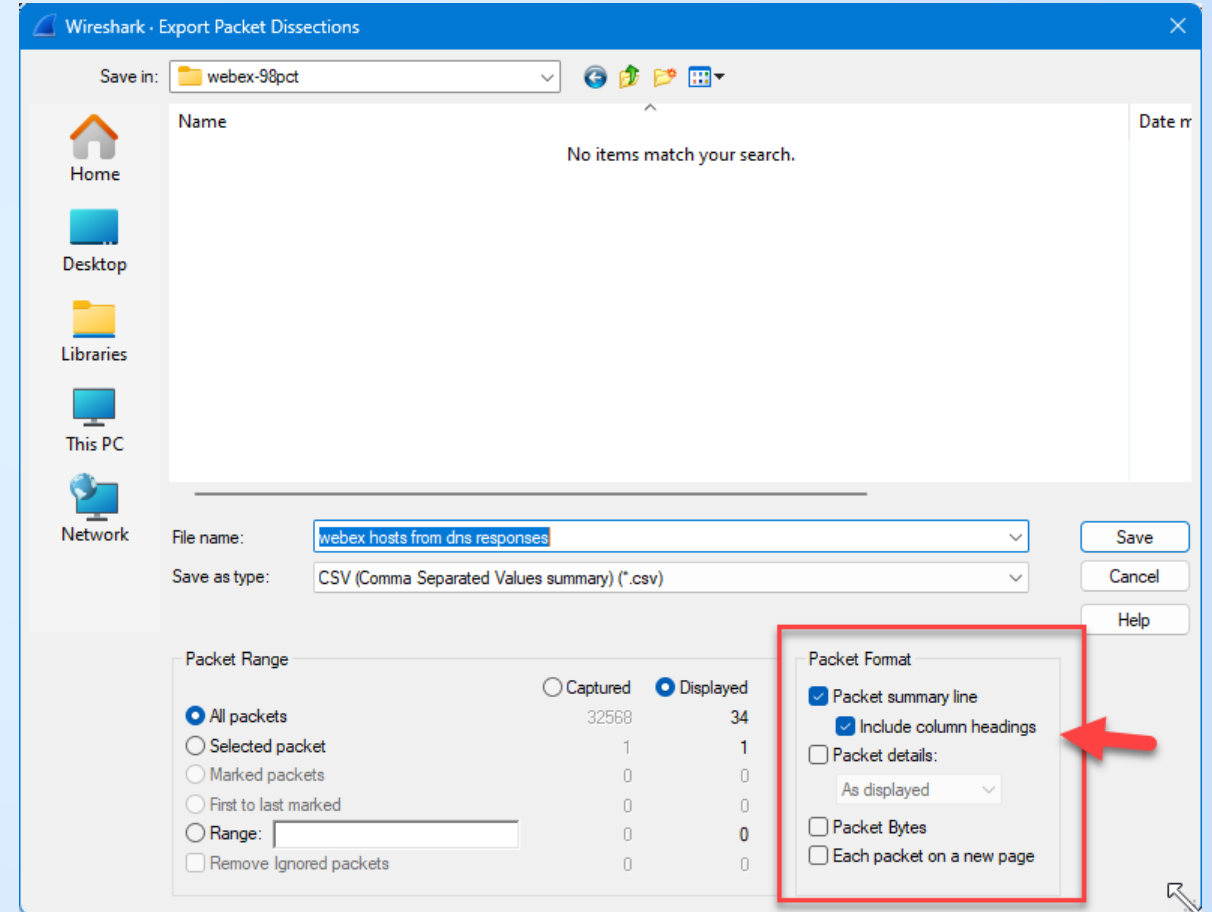


# Export Summary View to CSV File



The screenshot shows the Wireshark File menu with 'Export Packet Dissections' selected. A sub-menu is open, showing 'As CSV...' highlighted with a red arrow. The background shows a packet list with a filter 'dns.flags.response==1' and a table of network traffic.

Time	Source	Destination
0000	192.168.2.1	192.168.2.1
02000	192.168.2.1	192.168.2.1
06000	192.168.2.1	192.168.2.1
081000	192.168.2.1	192.168.2.1
09000	192.168.2.1	192.168.2.1
13000	192.168.2.1	192.168.2.1
140000	192.168.2.1	192.168.2.1
143000	192.168.2.1	192.168.2.1
16:56:10.977981	0.004648000	192.168.2.1



The screenshot shows the 'Export Packet Dissections' dialog box. The 'File name' is 'webex hosts from dns responses' and 'Save as type' is 'CSV (Comma Separated Values summary) (\*.csv)'. The 'Packet Range' section has 'All packets' selected. The 'Packet Format' section has 'Packet summary line' and 'Include column headings' checked, with a red arrow pointing to the latter. The 'Save' button is visible.

	A	B	C	D	E	F	G	H	I	J
1	No.	Time	Delta Time	Source	Destination	Protocol	Length	Name	Address	Info
2	17398	56:02.4	0	192.168.2.1	192.168.2.105	DNS	145	riverbed.webex.com	173.243.0.154	Standard query response 0xa512 A riverbed.webex.com CNAME nebulam.webex.com CNAME global-nebulam
3	17403	56:02.4	0.007282	192.168.2.1	192.168.2.105	DNS	100	global-nebulam.webex.com	173.243.0.154	Standard query response 0xee05 A global-nebulam.webex.com A 173.243.0.154
4	17426	56:02.6	0.112356	192.168.2.1	192.168.2.105	DNS	84	global-nebulam.webex.com		Standard query response 0xa856 AAAA global-nebulam.webex.com
5	18222	56:04.2	1.608961	192.168.2.1	192.168.2.105	DNS	131	nebulam.webex.com	173.243.0.154	Standard query response 0xf8c2 A nebulam.webex.com CNAME global-nebulam.webex.com A 173.243.0.154
6	18384	56:04.5	0.311979	192.168.2.1	192.168.2.105	DNS	176	akamaicdn.webex.com	23.199.51.101	Standard query response 0x0b3e A akamaicdn.webex.com CNAME akamaicdnbts.webex.com.edgekey.net CN
7	21584	56:10.3	5.845763	192.168.2.1	192.168.2.105	DNS	102	sec-tws-prod-vip.webex.com	66.163.35.36	Standard query response 0xd085 A sec-tws-prod-vip.webex.com A 66.163.35.36
8	21587	56:10.3	0.00309	192.168.2.1	192.168.2.105	DNS	102	sec-tws-prod-vip.webex.com	66.163.35.36	Standard query response 0x8c2c A sec-tws-prod-vip.webex.com A 66.163.35.36
9	21590	56:10.3	0.02183	192.168.2.1	192.168.2.105	DNS	156	sec-tws-prod-vip.webex.com		Standard query response 0xd508 AAAA sec-tws-prod-vip.webex.com SOA ns1.as13445.net
10	21731	56:10.9	0.604955	192.168.2.1	192.168.2.105	DNS	94	emcbmm10.webex.com	173.243.0.96	Standard query response 0x9a1d A emcbmm10.webex.com A 173.243.0.96
11	21746	56:11.0	0.003984	192.168.2.1	192.168.2.105	DNS	94	emcbmm20.webex.com	173.243.0.97	Standard query response 0x559a A emcbmm20.webex.com A 173.243.0.97
12	21762	56:11.0	0.01913	192.168.2.1	192.168.2.105	DNS	97	ed1lncbmm60.webex.com	62.109.231.3	Standard query response 0xae74 A ed1lncbmm60.webex.com A 62.109.231.3
13	21765	56:11.0	0.000123	192.168.2.1	192.168.2.105	DNS	97	ed1txcbmm80.webex.com	209.197.222.159	Standard query response 0x16cb A ed1txcbmm80.webex.com A 209.197.222.159
14	21766	56:11.0	0.000017	192.168.2.1	192.16					9.202.139
15	21767	56:11.0	0.000018	192.168.2.1	192.16					9.213.212
16	21768	56:11.0	0.000014	192.168.2.1	192.16					.243.4.76
17	21769	56:11.0	0.000013	192.168.2.1	192.16					19.200.11
18	21771	56:11.0	0.004648	192.168.2.1	192.16					.114.29.204.49
19	21772	56:11.0	0.001272	192.168.2.1	192.16					.20.90
20	21794	56:11.0	0.010024	192.168.2.1	192.16					.104.140
21	21795	56:11.0	0.000023	192.168.2.1	192.168.2.105	DNS	97	ed1sjcbmm10.webex.com	64.68.121.153	Standard query response 0xeef6 A ed1sjcbmm10.webex.com A 64.68.121.153
22	21839	56:11.0	0.025786	192.168.2.1	192.168.2.105	DNS	95	emvcbmm10.webex.com	64.68.120.70	Standard query response 0x6f84 A emvcbmm10.webex.com A 64.68.120.70
23	22807	56:12.1	1.130113	192.168.2.1	192.168.2.105	DNS	117	emcb31101.webex.com	64.68.101.20	Standard query response 0x0754 A emcb31101.webex.com CNAME emcb311.webex.com A 64.68.101.20
24	22923	56:12.6	0.490842	192.168.2.1	192.168.2.105	DNS	123	ed1vacb32201.webex.com	64.68.110.77	Standard query response 0x4906 A ed1vacb32201.webex.com CNAME ed1vacb322.webex.com A 64.68.110.77
25	29325	56:45.3	32.70617	192.168.2.1	192.168.2.105	DNS	102	sec-tws-prod-vip.webex.com	66.163.35.36	Standard query response 0xd9d5 A sec-tws-prod-vip.webex.com A 66.163.35.36
26	29326	56:45.3	0.000994	192.168.2.1	192.168.2.105	DNS	102	sec-tws-prod-vip.webex.com	66.163.35.36	Standard query response 0x43ed A sec-tws-prod-vip.webex.com A 66.163.35.36
27	29329	56:45.3	0.00601	192.168.2.1	192.168.2.105	DNS	102	sec-tws-prod-vip.webex.com	66.163.35.36	Standard query response 0x684e A sec-tws-prod-vip.webex.com A 66.163.35.36
28	29331	56:45.4	0.002663	192.168.2.1	192.168.2.105	DNS	102	sec-tws-prod-vip.webex.com	66.163.35.36	Standard query response 0xd0b7 A sec-tws-prod-vip.webex.com A 66.163.35.36
29	29334	56:45.4	0.007326	192.168.2.1	192.168.2.105	DNS	86	sec-tws-prod-vip.webex.com		Standard query response 0xf4ab AAAA sec-tws-prod-vip.webex.com
30	29358	56:45.4	0.050501	192.168.2.1	192.168.2.105	DNS	145	riverbed.webex.com	173.243.0.154	Standard query response 0xc40d A riverbed.webex.com CNAME nebulam.webex.com CNAME global-nebulam
31	29365	56:45.4	0.022402	192.168.2.1	192.168.2.105	DNS	145	riverbed.webex.com	173.243.0.154	Standard query response 0xe9dd A riverbed.webex.com CNAME nebulam.webex.com CNAME global-nebulam
32	29368	56:45.4	0.006102	192.168.2.1	192.168.2.105	DNS	100	global-nebulam.webex.com	173.243.0.154	Standard query response 0x1ec8 A global-nebulam.webex.com A 173.243.0.154
33	29390	56:45.5	0.084002	192.168.2.1	192.168.2.105	DNS	145	riverbed.webex.com	173.243.0.154	Standard query response 0xf0ce A riverbed.webex.com CNAME nebulam.webex.com CNAME global-nebulam
34	29433	56:45.6	0.10998	192.168.2.1	192.168.2.105	DNS	84	global-nebulam.webex.com		Standard query response 0x0eab AAAA global-nebulam.webex.com
35	29855	56:47.1	1.439924	192.168.2.1	192.168.2.105	DNS	160	lp.webex.com	23.56.192.142	Standard query response 0x17c0 A lp.webex.com CNAME san.webex.com.edgekey.net CNAME e4955.g.akam

Too Easy Mate - A variation of the phrase "No worries" - Particularly useful when someone is asking you to do something. That something can, in reality, be either easy or not.



- ⦿ 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





Thanks Leigh!!

## Script Output

```
README x +
File Edit View
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
```

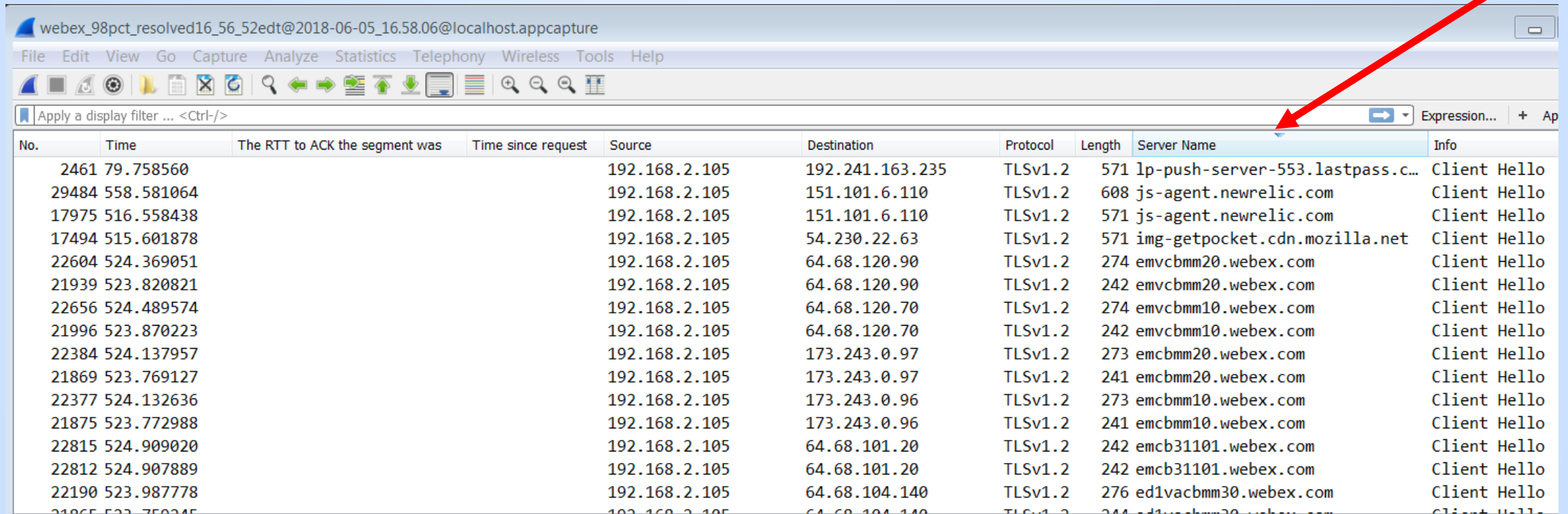


# Time to examine SSL/TLS



# Wireshark - SSL Server Name View

Sorted by Server Name Column from SSL Decodes



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	lp-push-server-553.lastpass.c...	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	img-getpocket.cdn.mozilla.net	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
21865	523.759245			192.168.2.105	64.68.104.140	TLSv1.2	244	ed1vacbmm30.webex.com	Client Hello



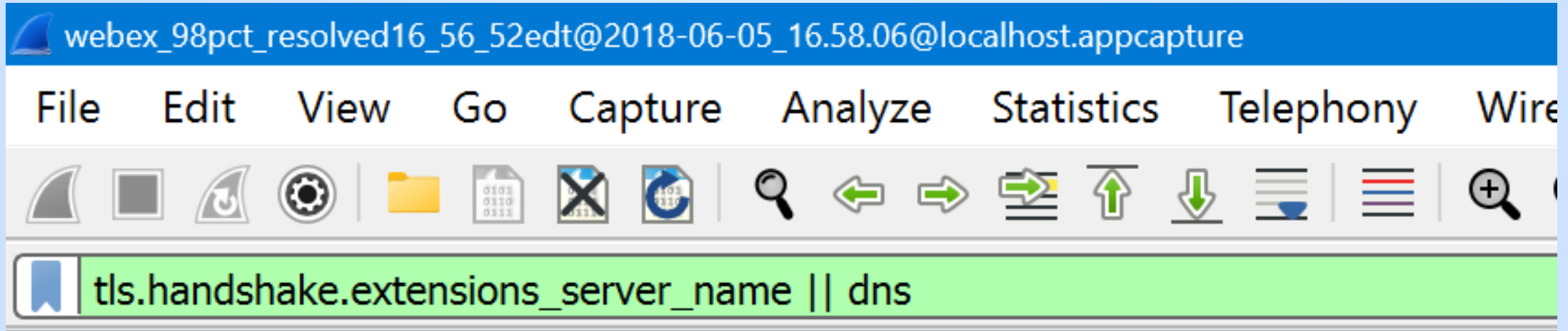
# Wireshark Super Power

---



# Compound Filters

Powerful capability

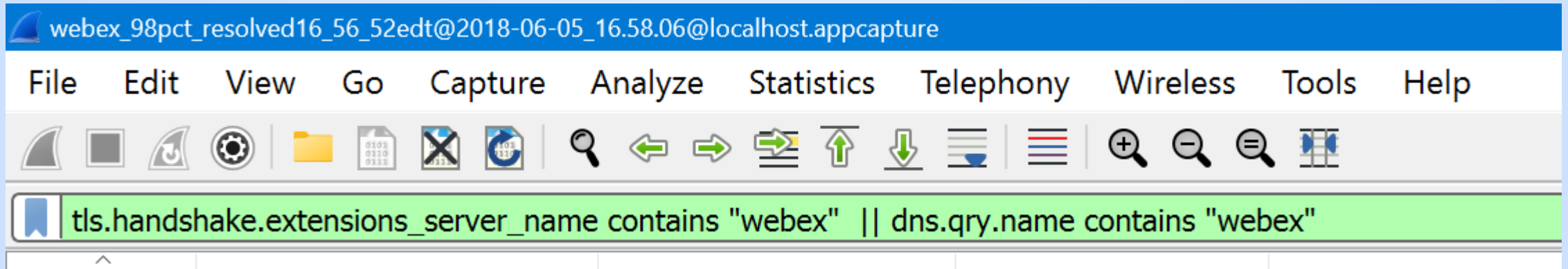




# Compound Filters

Permission to “go wild”?

Permission Granted

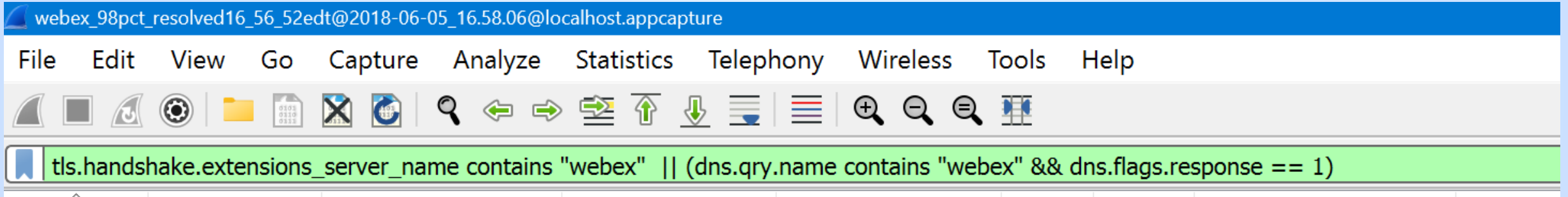




# Even More Compound Filters

Permission to “go wild”?

Go for it!!





# **Examine: App & Protocol Behavior**





# With our compound filter applied..

No.	Time	Time delta from previ	The RTT to ACK the segme	Time since request	Source	Destination	Protocol	Length	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	0.000002000			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
6971	08:57:29.164854	0.000607000			192.168.2.105	64.68.121.153	TLSv1.2	244	ed1chcbmm100.webex.com	0x018	Client Hello



# Establish 4 connections to main server...

no.	Time	Time delta from previous	Time RTT to ACK the segment	Time since request	Source	Destination	Protocol	Length	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
6801	08:57:28.967506	0.000280000			192.168.2.105	192.168.2.1	DNS	81			A emcbmm10.webex.com
6802	08:57:28.967786	0.000280000			192.168.2.105	192.168.2.1	DNS	81			Standard query 0x0029 A ed1sjcbmm10.webex.com
6803	08:57:28.968389	0.000603000			192.168.2.105	192.168.2.1	DNS	81			Standard query 0x718b A ed1txcbmm80.webex.com
6804	08:57:28.968673	0.000284000			192.168.2.105	192.168.2.1	DNS	81			Standard query 0x4af3 A ed1lncbmm60.webex.com
6805	08:57:28.969171	0.000498000			192.168.2.105	192.168.2.1	DNS	78			Standard query 0x426c A ed1vacbmm30.webex.com
6806	08:57:28.969338	0.000167000			192.168.2.105	192.168.2.1	DNS	81			Standard query 0xdc0c A emcbmm20.webex.com
6808	08:57:28.969846	0.000110000			192.168.2.105	192.168.2.1	DNS	82			Standard query 0xf19a A ed1sycbmm90.webex.com
6809	08:57:28.969877	0.000031000			192.168.2.105	192.168.2.1	DNS	79			Standard query 0xb39a A ed1chcbmm100.webex.com
6811	08:57:28.970022	0.000127000			192.168.2.105	192.168.2.1	DNS	79			Standard query 0x025e A emvcbmm10.webex.com
6812	08:57:28.970141	0.000119000			192.168.2.105	192.168.2.1	DNS	81			Standard query 0x7265 A emvcbmm20.webex.com
6813	08:57:28.970701	0.000560000			192.168.2.105	192.168.2.1	DNS	81			Standard query 0x14e7 A ed1sgcbmm10.webex.com
6814	08:57:28.970712	0.000011000			192.168.2.105	192.168.2.1	DNS	87			Standard query 0x6662 A ed1hkcbmm70.webex.com
6821	08:57:28.993744	0.022418000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0xf325 A ed1jpcbmm50-nrt02.webex.com
6822	08:57:28.995924	0.002180000			192.168.2.1	192.168.2.105	DNS	98			Standard query response 0x426c A ed1vacbmm30.webex.com
6823	08:57:28.996687	0.000763000			192.168.2.1	192.168.2.105	DNS	94			Standard query response 0xb39a A ed1chcbmm100.webex.com
6824	08:57:28.996717	0.000030000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0x2166 A emcbmm10.webex.com
6825	08:57:28.996731	0.000014000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0x718b A ed1txcbmm80.webex.com
6826	08:57:28.996745	0.000014000			192.168.2.1	192.168.2.105	DNS	94			Standard query response 0x4af3 A ed1lncbmm60.webex.com
6827	08:57:28.996756	0.000011000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0xdc0c A emcbmm20.webex.com
6828	08:57:29.000219	0.003463000			192.168.2.1	192.168.2.105	DNS	103			Standard query response 0xf19a A ed1sycbmm90.webex.com
6829	08:57:29.000846	0.000627000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0xf325 A ed1jpcbmm50-nrt02.webex.com
6850	08:57:29.024120	0.001276000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0x14e7 A ed1sgcbmm10.webex.com
6868	08:57:29.031893	0.001148000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0x0029 A ed1sjcbmm10.webex.com
6871	08:57:29.038389	0.000600000			192.168.2.1	192.168.2.105	DNS	95			Standard query response 0x6662 A ed1hkcbmm70.webex.com
6872	08:57:29.038408	0.000019000			192.168.2.1	192.168.2.105	DNS	95			Standard query response 0x025e A emvcbmm10.webex.com
6923	08:57:29.112171	0.000002000			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

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



No.	Time	Time delta from previous	The RTT to ACK the segment	Time since request	Source	Destination	Protocol	Length	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.webex.com
6822	08:57:28.995924	0.002180000			192.168.2.1	192.168.2.105	DNS	98			Standard query response 0xb39a A ed1chcbmm100.webex.com
6823	08:57:28.996687	0.000763000			192.168.2.1	192.168.2.105	DNS	94			Standard query response 0x2166 A emcbmm10.webex.com
6824	08:57:28.996717	0.000030000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0x718b A ed1txcbmm80.webex.com
6825	08:57:28.996731	0.000014000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0x4af3 A ed1lncbmm60.webex.com
6826	08:57:28.996745	0.000014000			192.168.2.1	192.168.2.105	DNS	94			Standard query response 0xdc0c A emcbmm20.webex.com
6827	08:57:28.996756	0.000011000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0xf19a A ed1sycbmm90.webex.com
6828	08:57:29.000219	0.003463000			192.168.2.1	192.168.2.105	DNS	103			Standard query response 0xf325 A ed1jpcbmm50-nrt02.webex.com
6829	08:57:29.000846	0.000627000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0x14e7 A ed1sgcbmm10.webex.com
6850	08:57:29.024120	0.001276000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0x0029 A ed1sjcbmm10.webex.com
6868	08:57:29.031893	0.001148000			192.168.2.1	192.168.2.105	DNS	97			Standard query response 0x6662 A ed1hkcbmm70.webex.com
6871	08:57:29.038389	0.000600000			192.168.2.1	192.168.2.105	DNS	95			Standard query response 0x025e A emvcbmm10.webex.com
6872	08:57:29.038408	0.000019000			192.168.2.1	192.168.2.105	DNS	95			Standard query response 0x7265 A emvcbmm20.webex.com
6923	08:57:29.112171	0.000002000			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



# Get the DNS responses...

No.	Time	Time delta from previous	The RTT to ACK the segment	Time since request	Source	Destination	Protocol	Length	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
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	0.000002000			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



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

No.	Time	Time delta from previous	The RTT to ACK the segment	Time since request	Source	Destination	Protocol	Length	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.webex.com
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.w...
6823	08:57:28.996687	0.000763000			192.168.2.1	192.168.2.105	DNS	94			Standard query response 0x2166 A emcbmm10.webex.com
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.webex.com
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.webex.com
6923	08:57:29.112171	0.000002000			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
6971	08:57:29.164854	0.000607000			192.168.2.105	64.68.121.153	TLSv1.2	244	ed1chcbmm100.webex.com	0x018	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 now have a pretty good idea of start time for the period of interest and which servers we need to focus on...
- ⦿ 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

