TCP Case Study Packet Analysis

Case Study Exhibits from high visibility, high stakes critical problems

Bill.Alderson@Cogent.Management

SharkFest'23 US
Wireshark Developer and User Conference • San Diego, CA • June 10-15

Packetman007

Course PDF https://Cogent.Management/TCPCases

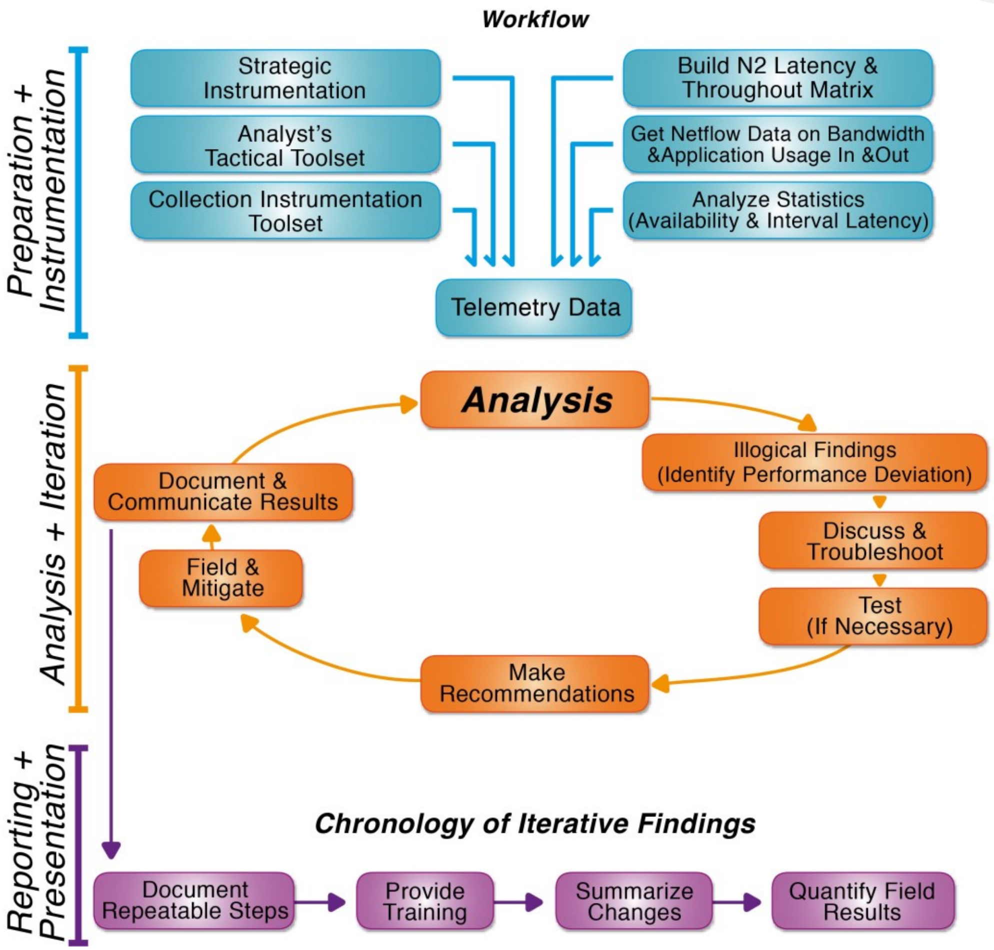
TCP Case Study Packet Analysis exhibits from high visibility, high stakes critical problems

Root Cause Analysis

Critical Problem Resolution

Performance Application Analysis

Analysis Workflow


Workflow
Preparation + Instrumentation
Strategic Instrumentation
Analyst's Tactical Toolset
Collection Instrumentation Toolset
Build N2 Latency & Throughout Matrix
Get Netflow Data on Bandwidth &Application Usage In &Out
Analyze Statistics (Availability & Interval Latency)
Telemetry Data
Analysis + Iteration
Analysis
Illogical Findings (Identify Performance Deviation)
Discuss & Troubleshoot
Test (If Necessary)
Make Recommendations
Field & Mitigate
Document & Communicate Results
Reporting + Presentation
Chronology of Iterative Findings
Document Repeatable Steps
Provide Training
Summarize Changes
Quantify Field Results

The Needle

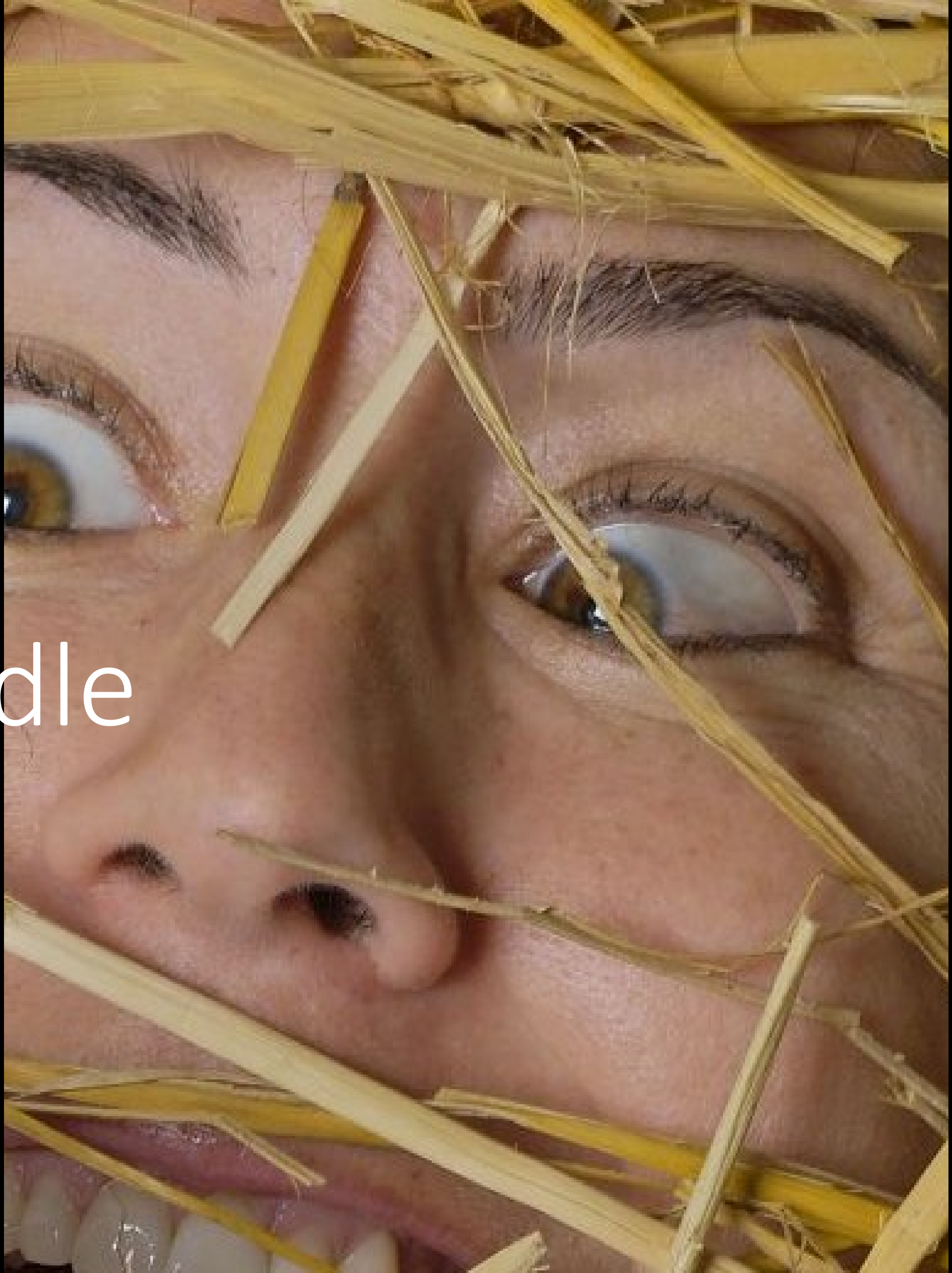
The Environment

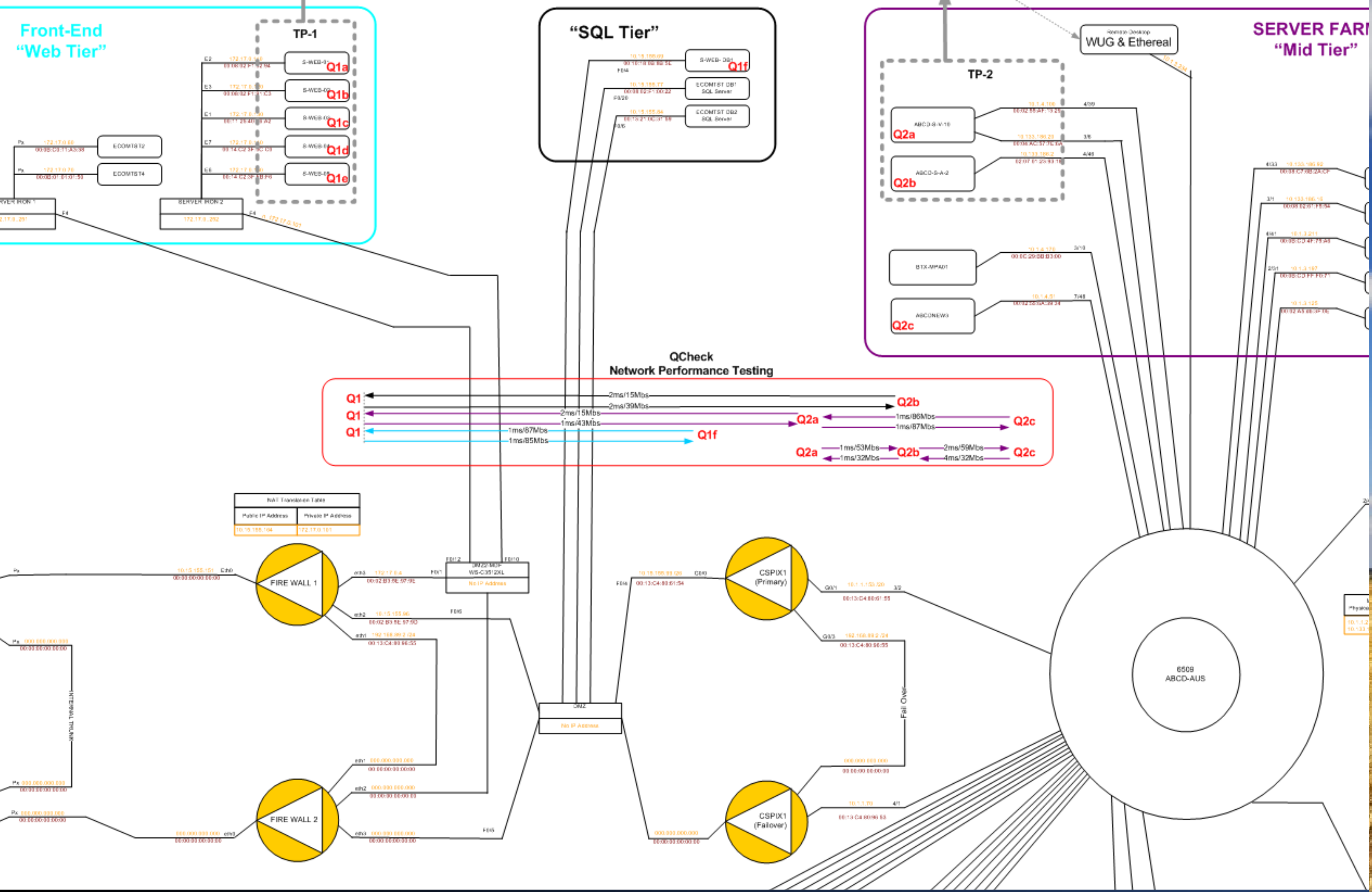
Packet Traces

$tore Every Packet?
Who can and is going to analyze them and when?

Finding The Stack With The Problem

Finding The Needle



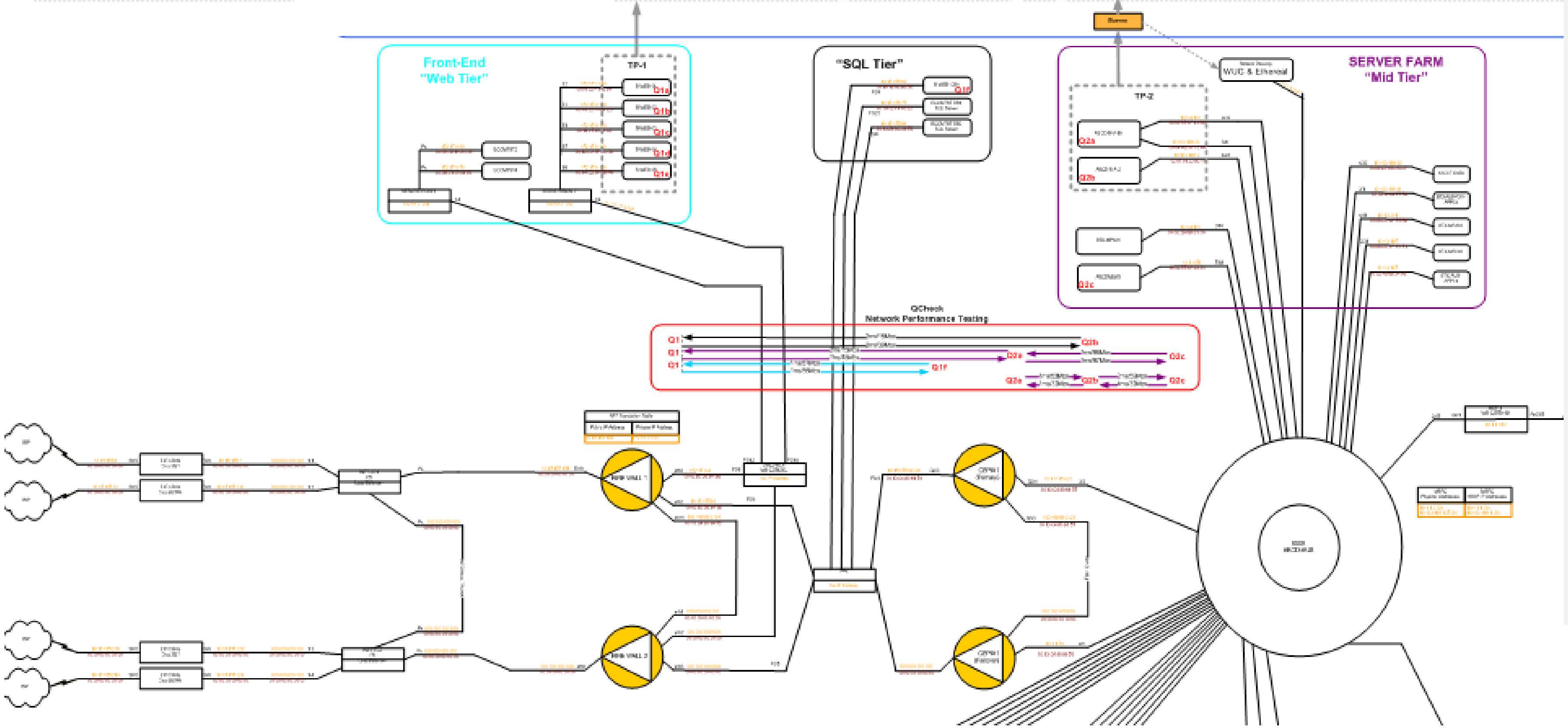


Multi-Tier Identification

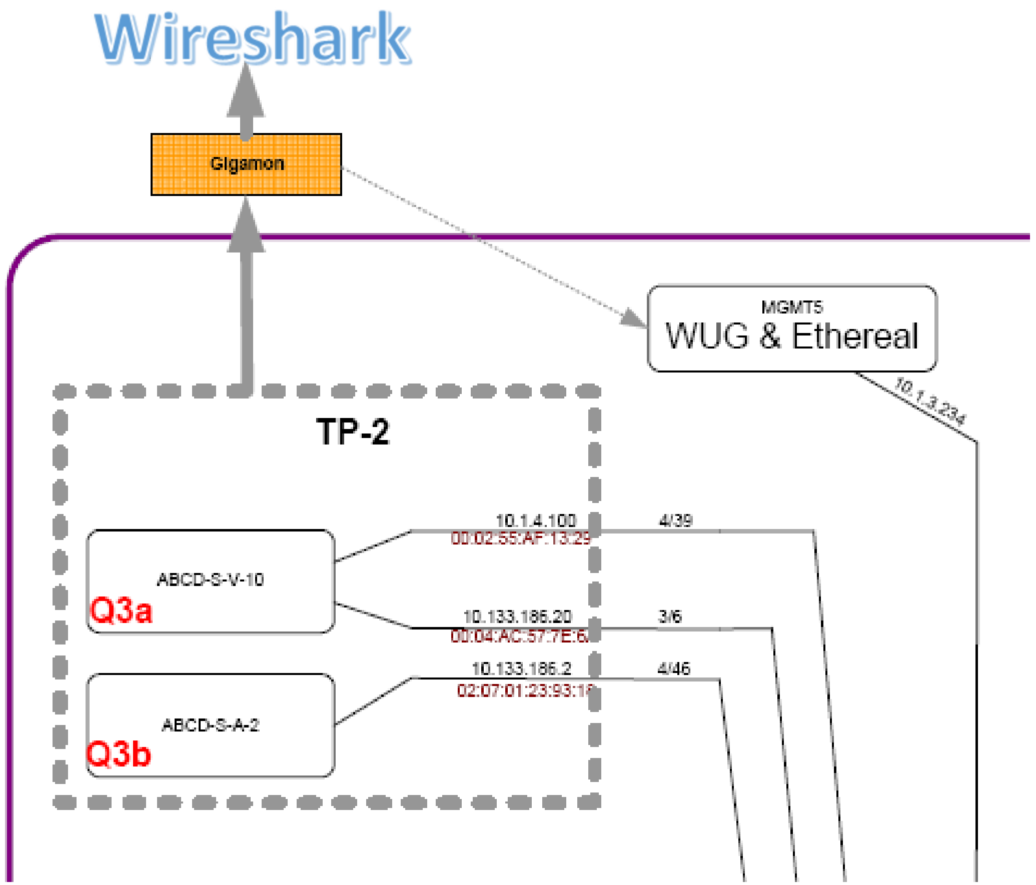
Monitoring & Analysis Design

Wireshark

Spans, Taps, Packet Brokers…

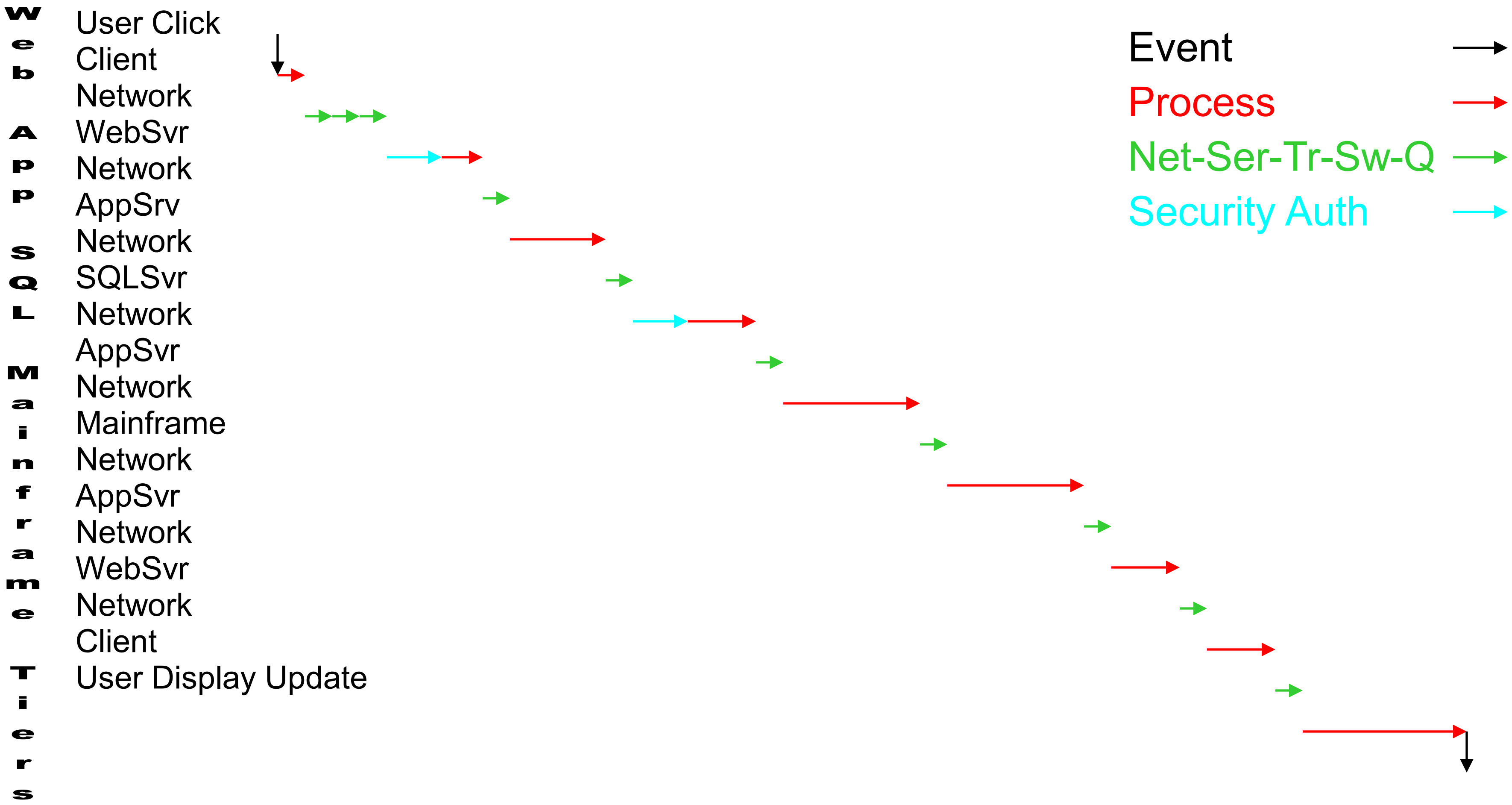


Instrumentation Phase
Test Point Design



Multi-tier Transaction Analysis

- Multi-tier Transaction Analysis



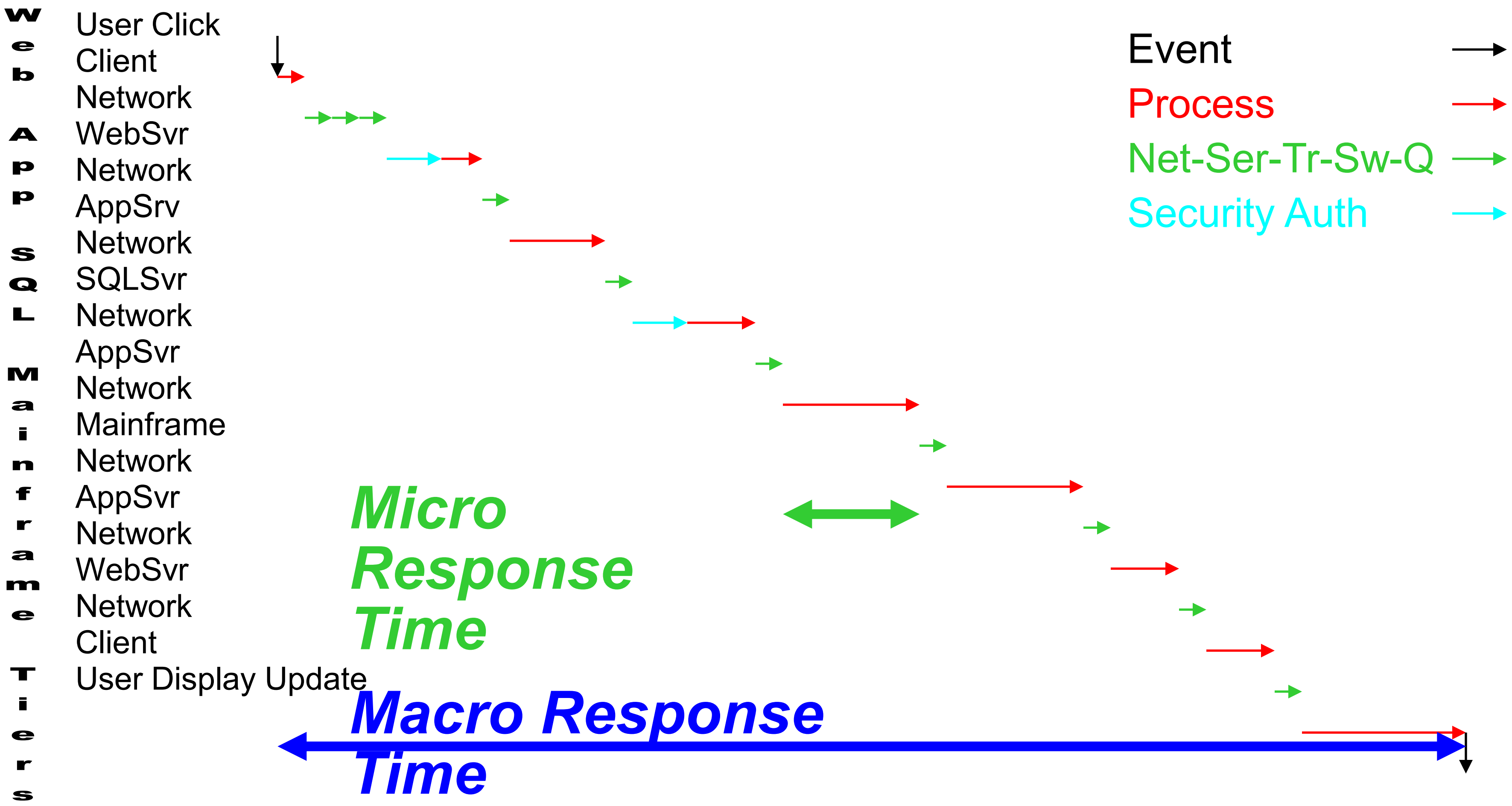
Web App SQL Mainframe Tiers

User Click
Client
Network
WebSvr
Network
AppSrv
Network
SQLSvr
Network
AppSvr
Network
Mainframe
Network
AppSvr
Network
WebSvr
Network
Client
User Display Update

Event →
Process →
Net-Ser-Tr-Sw-Q →
Security Auth →

Multi-tier Macro vs. Micro

- Multi-tier Transaction Analysis



Web App SQL Mainframe Tiers

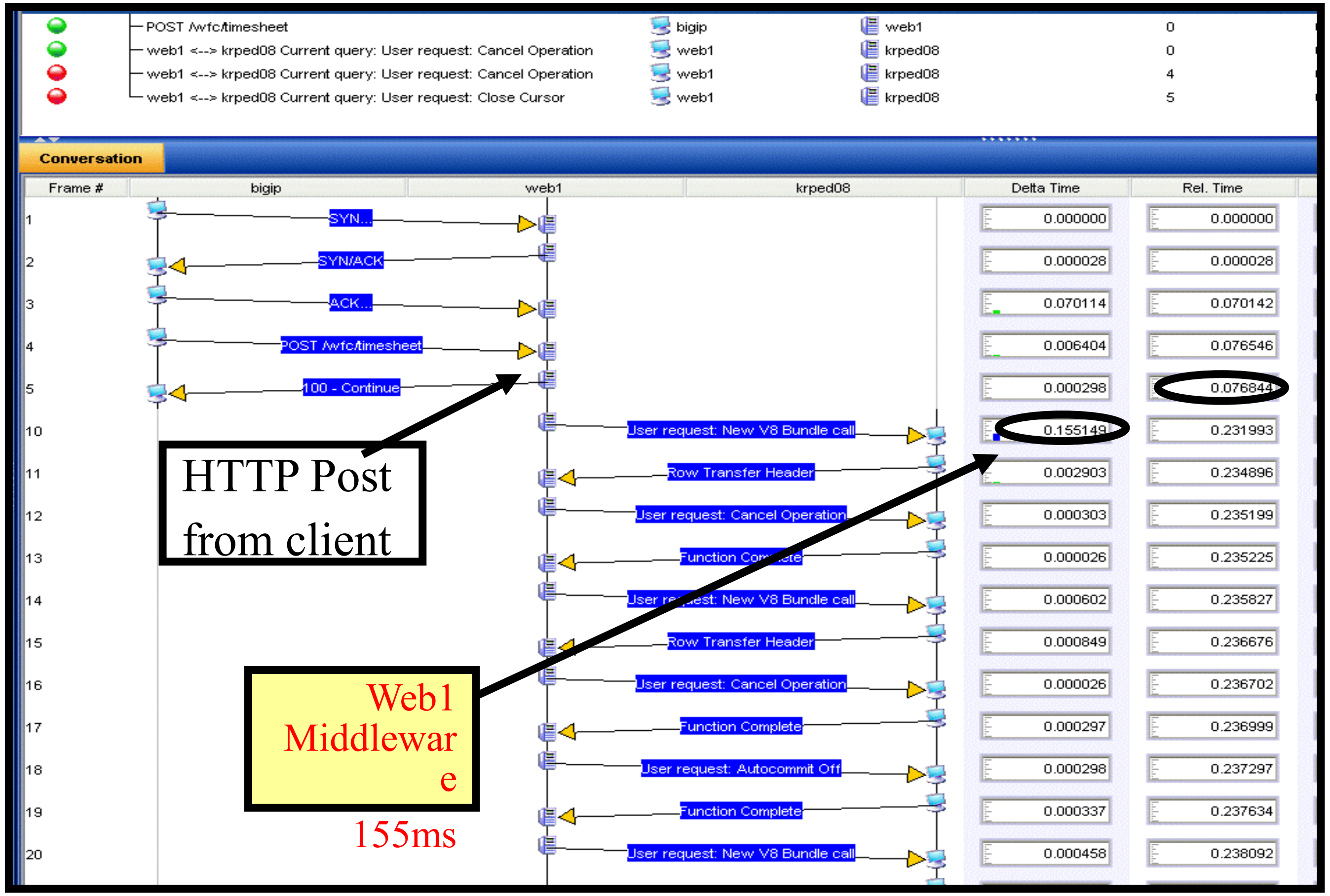
User Click
Client
Network
WebSvr
Network
AppSrv
Network
SQLSvr
Network
AppSvr
Network
Mainframe
Network
AppSvr
Network
WebSvr
Network
Client
User Display Update

Event
Process
Net-Ser-Tr-Sw-Q
Security Auth

Micro Response Time

Macro Response Time

HTTP / SQL Multi-tier 1



●	POST /wfc/timesheet	bigip	web1	0
●	web1 <--> krped08 Current query: User request: Cancel Operation	web1	krped08	0
●	web1 <--> krped08 Current query: User request: Cancel Operation	web1	krped08	4
●	web1 <--> krped08 Current query: User request: Close Cursor	web1	krped08	5

Conversation

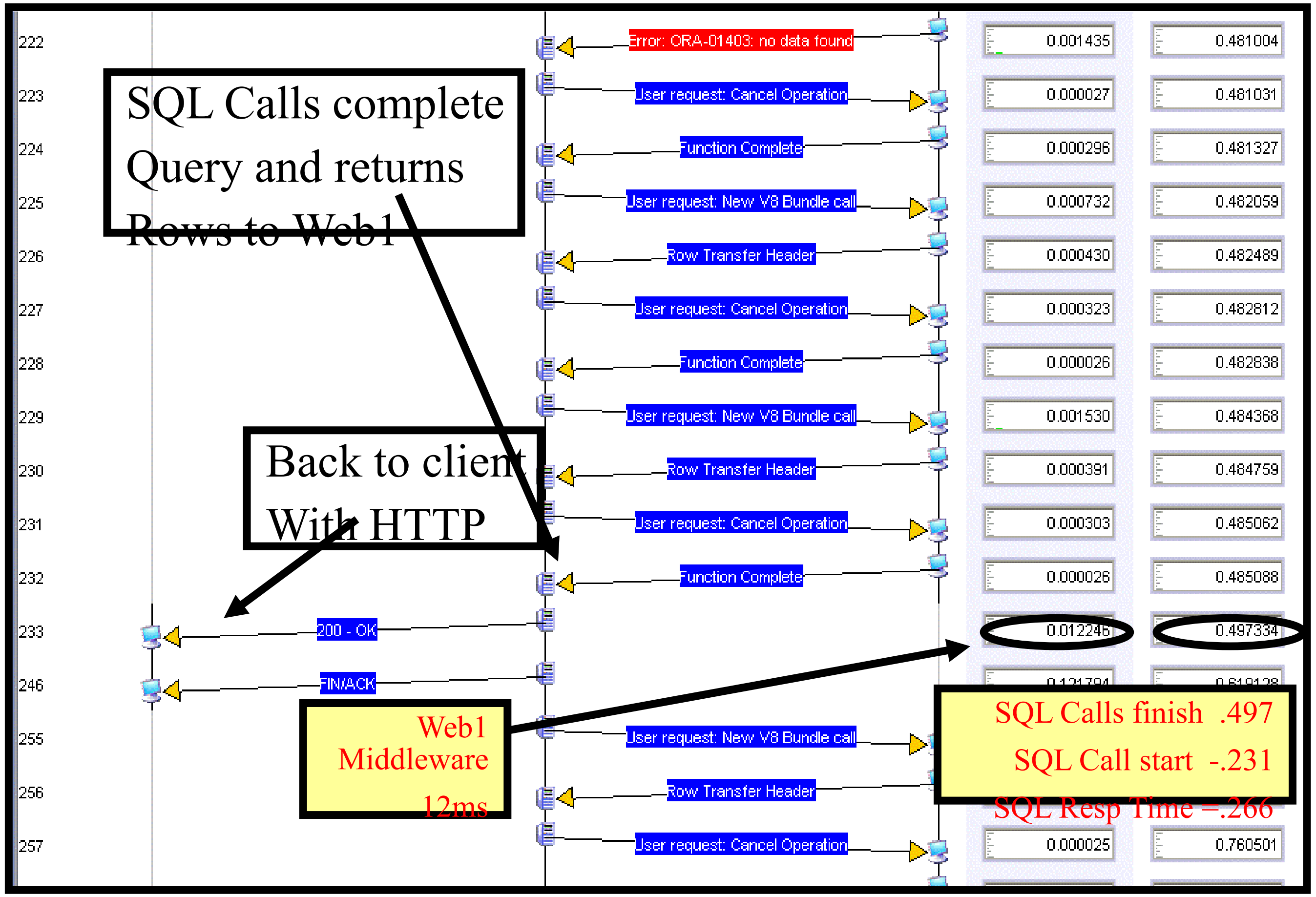
Frame #	bigip	web1	krped08	Delta Time	Rel. Time
1	SYN... →			0.000000	0.000000
2	← SYN/ACK			0.000028	0.000028
3	ACK... →			0.070114	0.070142
4	POST /wfc/timesheet →			0.006404	0.076546
5	← 100 - Continue			0.000298	0.076844
10		User request: New V8 Bundle call →		0.155149	0.231993
11		← Row Transfer Header		0.002903	0.234896
12		User request: Cancel Operation →		0.000303	0.235199
13		← Function Complete		0.000026	0.235225
14		User request: New V8 Bundle call →		0.000602	0.235827
15		← Row Transfer Header		0.000849	0.236676
16		User request: Cancel Operation →		0.000026	0.236702
17		← Function Complete		0.000297	0.236999
18		User request: Autocommit Off →		0.000298	0.237297
19		← Function Complete		0.000337	0.237634
20		User request: New V8 Bundle call →		0.000458	0.238092

HTTP Post from client

Web1 Middleware

155ms

HTTP / SQL Multi-tier 2



222	Error: ORA-01403: no data found	0.001435	0.481004
223	User request: Cancel Operation	0.000027	0.481031
224	Function Complete	0.000296	0.481327
225	User request: New V8 Bundle call	0.000732	0.482059
226	Row Transfer Header	0.000430	0.482489
227	User request: Cancel Operation	0.000323	0.482812
228	Function Complete	0.000026	0.482838
229	User request: New V8 Bundle call	0.001530	0.484368
230	Row Transfer Header	0.000391	0.484759
231	User request: Cancel Operation	0.000303	0.485062
232	Function Complete	0.000026	0.485088
233	200 - OK	0.012246	0.497334
246	FIN/ACK	0.121794	0.619128
255	User request: New V8 Bundle call		
256	Row Transfer Header		
257	User request: Cancel Operation	0.000025	0.760501

SQL Calls complete Query and returns Rows to Web1

Back to client With HTTP

Web1 Middleware 12ms

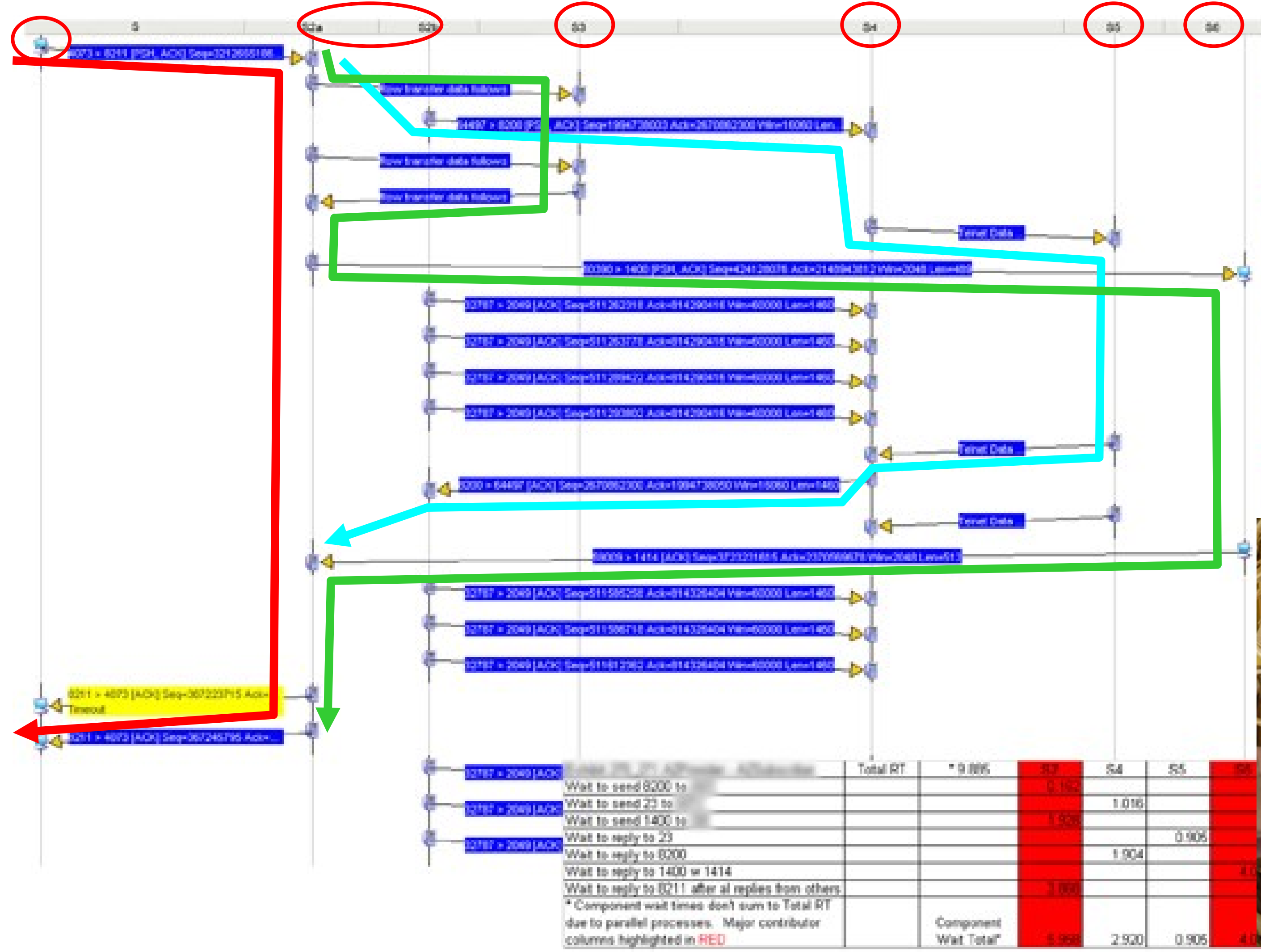
SQL Calls finish .497

SQL Call start -.231

SQL Resp Time =.266

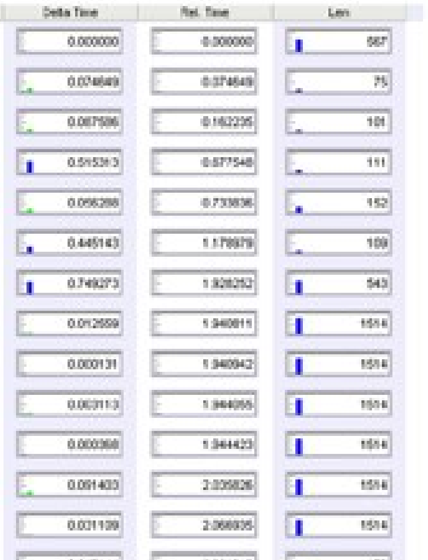
Tier Micro-Analysis Phase

Web App I/F #1&2 SQL TransLogger MF#1 MF#2 Time Breakdown



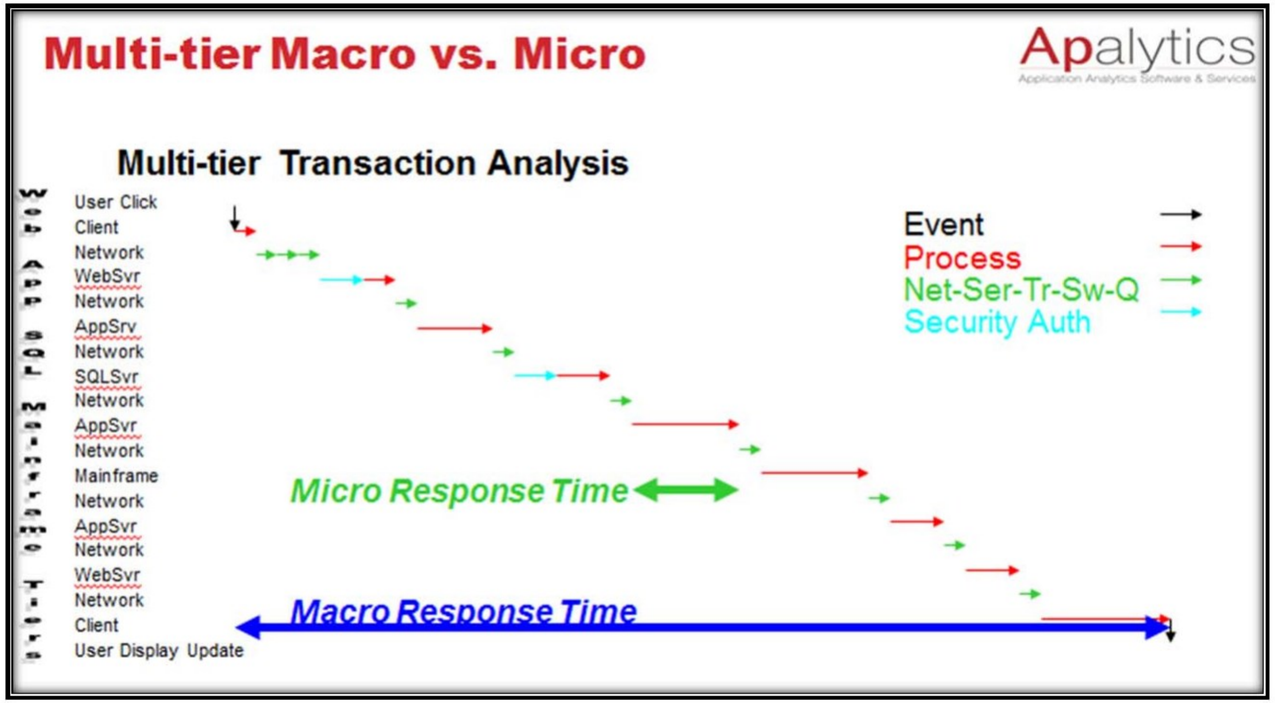
S
S2a
S2b
S3
S4
S5
S6
4073 > 8211 [PSH, ACK] Seq=3212655186
Now transfer data follows
64497 > 8200 [PSH, ACK] Seq=1994738033 Ack=2670862300 Win=16060 Len
Now transfer data follows
Now transfer data follows
Telnet Data
60390 > 1400 [PSH, ACK] Seq=4241280076 Ack=2140943812 Win=2048 Len=403
32787 > 2049 [ACK] Seq=511262318 Ack=814290416 Win=60000 Len=1460
32787 > 2049 [ACK] Seq=511263778 Ack=814290416 Win=60000 Len=1460
32787 > 2049 [ACK] Seq=511266422 Ack=814290416 Win=60000 Len=1460
32787 > 2049 [ACK] Seq=511293802 Ack=814290416 Win=60000 Len=1460
Telnet Data
8200 > 64497 [ACK] Seq=2670862300 Ack=1994738050 Win=16060 Len=1460
Telnet Data
59009 > 1414 [ACK] Seq=3723231615 Ack=2370599678 Win=2048 Len=512
32787 > 2049 [ACK] Seq=511595258 Ack=814326404 Win=60000 Len=1460
32787 > 2049 [ACK] Seq=511596718 Ack=814326404 Win=60000 Len=1460
32787 > 2049 [ACK] Seq=511612362 Ack=814326404 Win=60000 Len=1460
8211 > 4073 [ACK] Seq=3672237715 Ack=
Timeout
8211 > 4073 [ACK] Seq=3672245795 Ack=
32787 > 2049 [ACK
32787 > 2049 [ACK
32787 > 2049 [ACK

[redacted]	Total RT	* 9.886	S3	S4	S5	S6
Wait to send 8200 to [redacted]			0.152			
Wait to send 23 to [redacted]				1.016		
Wait to send 1400 to [redacted]			1.926			
Wait to reply to 23					0.905	
Wait to reply to 8200				1.904		
Wait to reply to 1400 w 1414						4.0
Wait to reply to 8211 after al replies from others			3.880			
* Component wait times don't sum to Total RT due to parallel processes. Major contributor columns highlighted in RED		Component Wait Total*	5.958	2.920	0.905	4.0

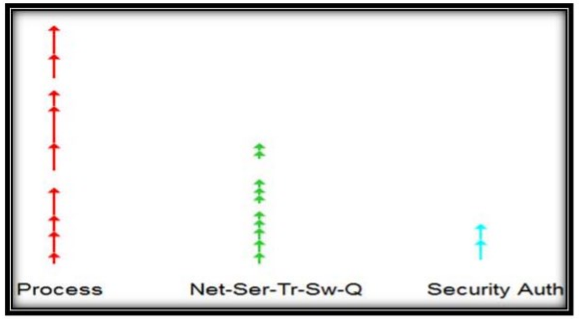


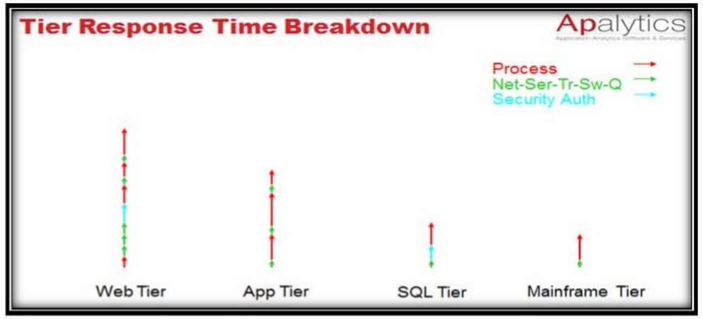
Delta Time	Rel. Time	Len
0.000000	0.000000	587
0.074649	0.074649	75
0.087586	0.162235	101
0.515313	0.677548	111
0.056288	0.733836	152
0.445143	1.178979	109
0.749273	1.928252	543
0.012559	1.940811	1514
0.000131	1.940942	1514
0.003113	1.944055	1514
0.000368	1.944423	1514
0.091403	2.035826	1514
0.031109	2.066935	1514

Summary of Multitier Monitoring

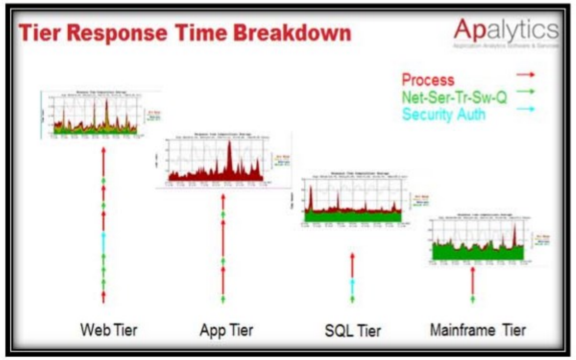


Multi-tier Macro vs. Micro

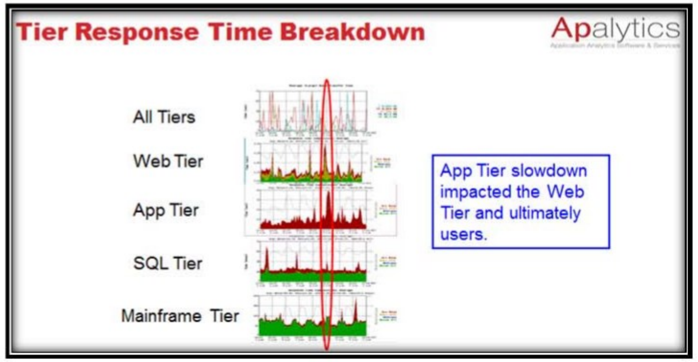




Tier Response Time Breakdown



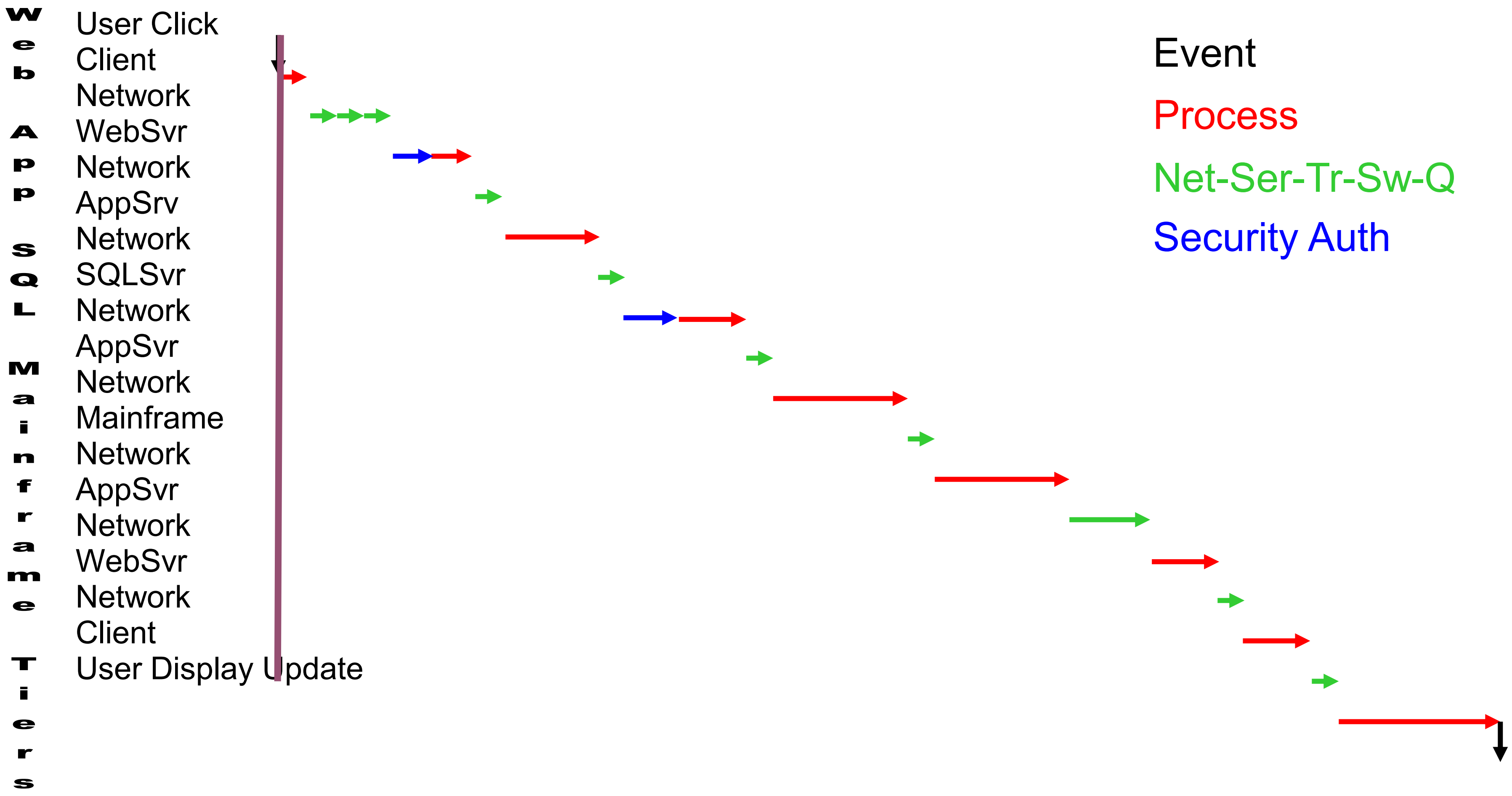
Tier Response Time Breakdown



Tier Response Time Breakdown

App Tier slowdown impacted the Web Tier and ultimately users.

Multi-tier Transaction Analysis



Web App SQL Mainframe Tiers

User Click
Client
Network
WebSvr
Network
AppSrv
Network
SQLSvr
Network
AppSvr
Network
Mainframe
Network
AppSvr
Network
WebSvr
Network
Client
User Display Update

Event
Process
Net-Ser-Tr-Sw-Q
Security Auth

Multi-tier Transaction Analysis

W
e
b

A
p
p

S
Q
L

M
a
i
n
f
r
a
m
e

.
s

User Click

Web Tier

Network

WebSvr

Network

AppSrv

Network

App Tier

AppSrv

Network

Mainframe

Network

SQL Tier

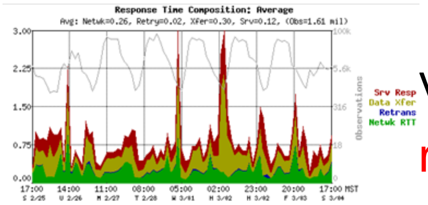
WebSvr

Network

Client

Mainframe Tier

Update

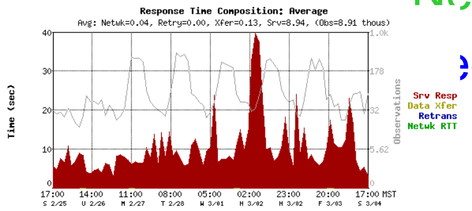


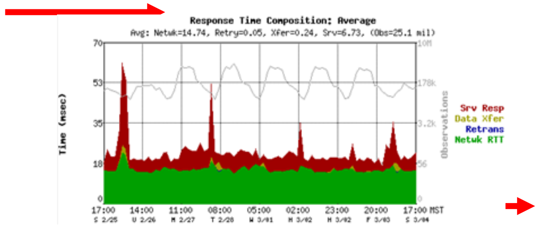
vent

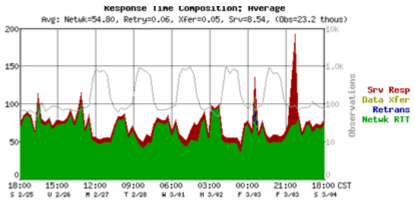
rocess

Net-Ser-Tr-Sw-Q

ecurity Auth







Tier Response Time Breakdown

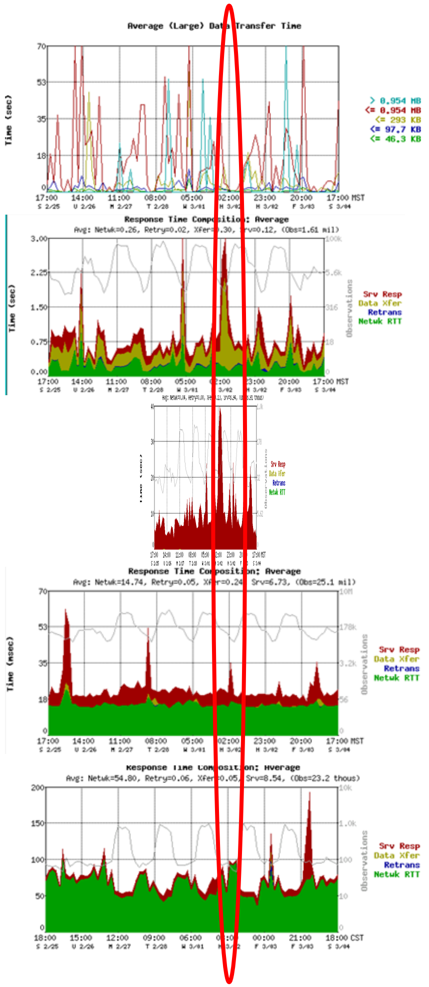
All Tiers

Web Tier

App Tier

SQL Tier

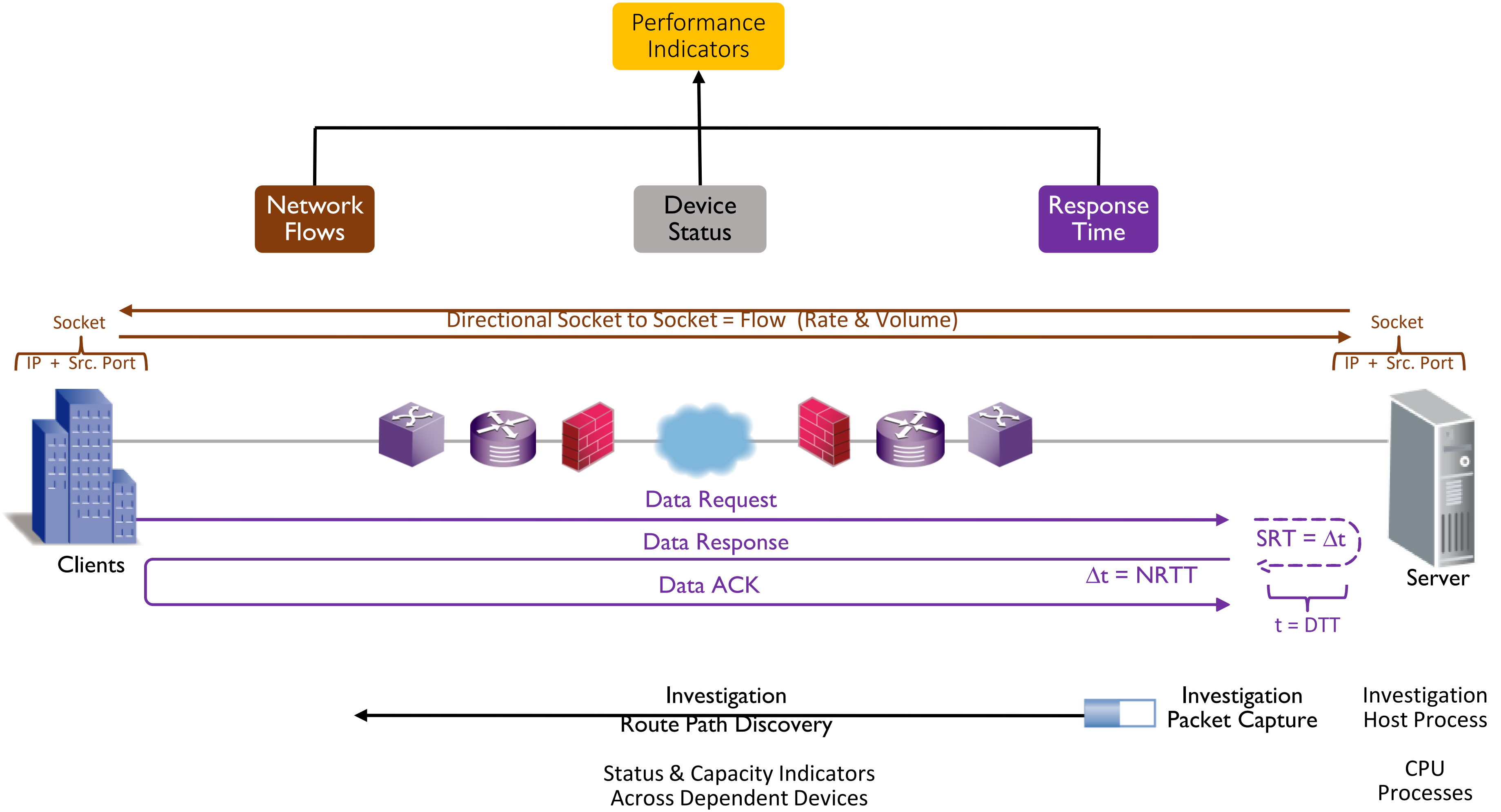
Mainframe Tier



App Tier slowdown impacted the Web Tier and ultimately users.

TCP Trace & Chart Exhibits

Performance Indicators



Performance Indicators

Network Flows

Device Status

Response Time

Socket

IP + Src. Port

Directional Socket to Socket = Flow (Rate & Volume)

Socket

IP + Src. Port

Clients

Server

Data Request

Data Response

Data ACK

SRT = Δt

Δt = NRTT

t = DTT

Investigation
Route Path Discovery

Status & Capacity Indicators
Across Dependent Devices

Investigation
Packet Capture

Investigation
Host Process

CPU
Processes

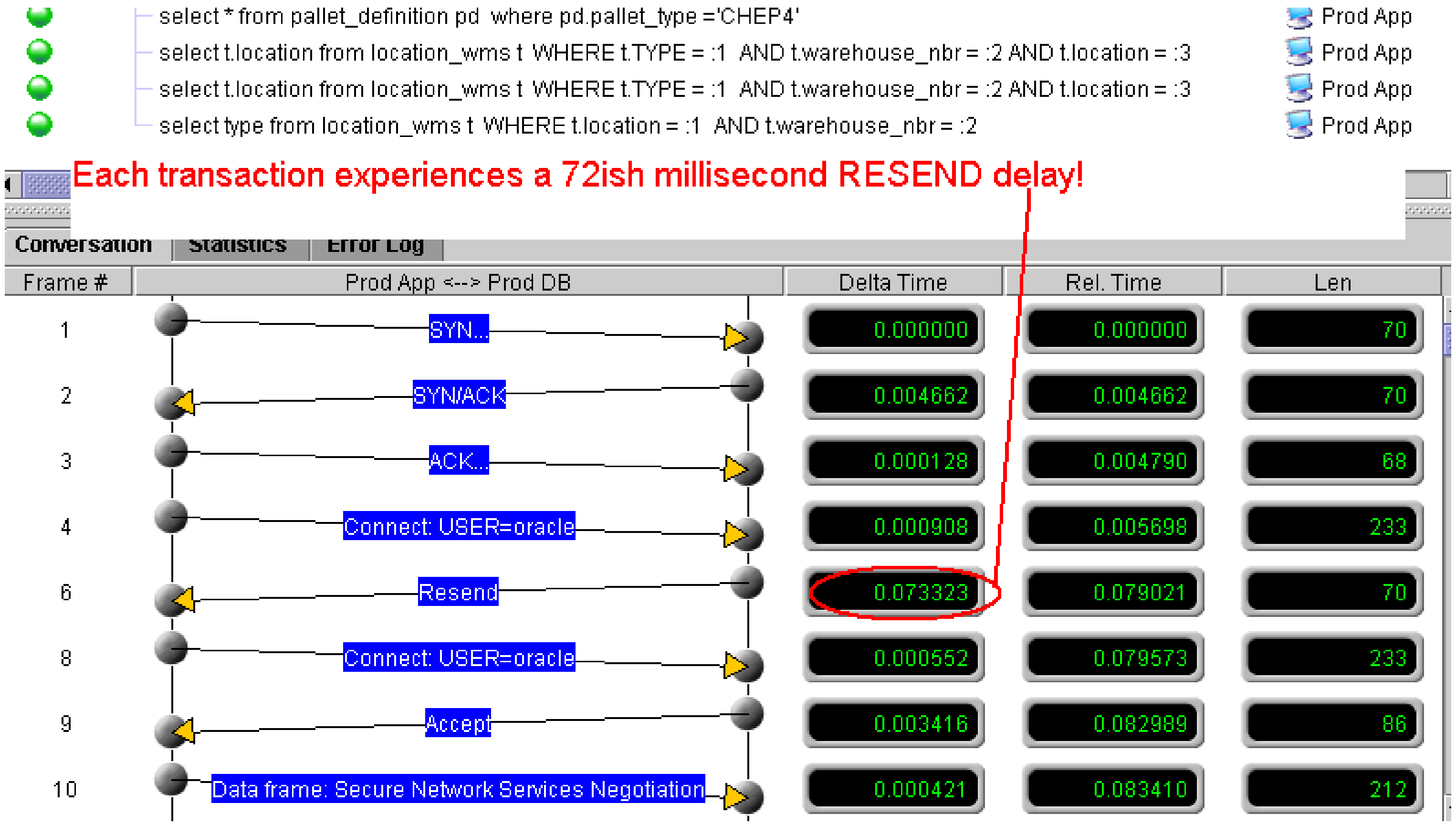
Each slide that follows explains and illustrates the key to many past problems…

Findings expertly found and annotated provide the knowledge for Client employees, managers and vendors to take action to solve and optimize networks, systems and architecture.

Without such key data trouble call bridges were without productive paths to diagnosing and solving critical problems.

We worked with well over 100 technologists virtually around the world helping them be more successful by providing definitive facts leading to optimization and problem resolution.

Oracle Connect Slow

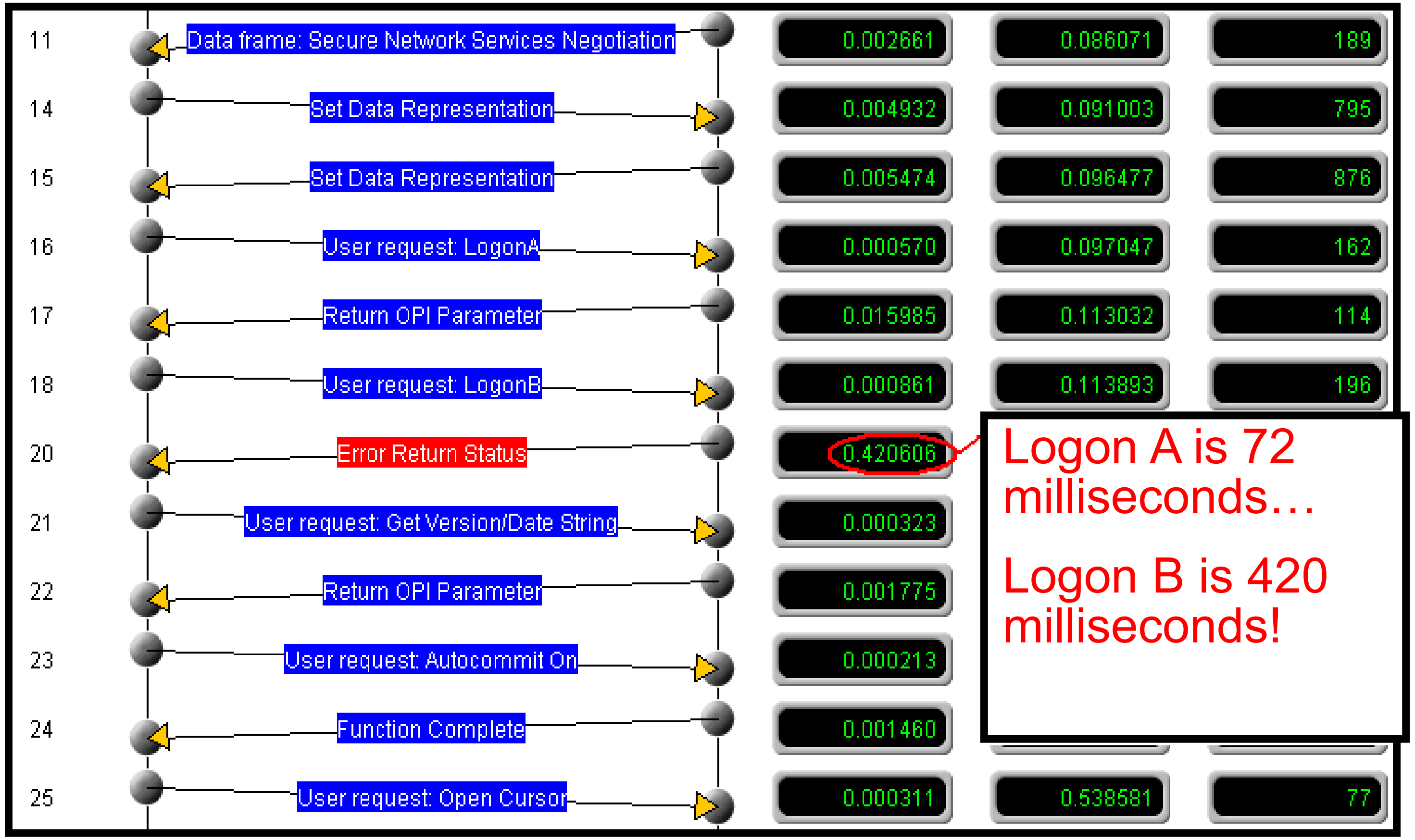


select * from pallet_definition pd where pd.pallet_type ='CHEP4'	Prod App
select t.location from location_wms t WHERE t.TYPE = :1 AND t.warehouse_nbr = :2 AND t.location = :3	Prod App
select t.location from location_wms t WHERE t.TYPE = :1 AND t.warehouse_nbr = :2 AND t.location = :3	Prod App
select type from location_wms t WHERE t.location = :1 AND t.warehouse_nbr = :2	Prod App

Each transaction experiences a 72ish millisecond RESEND delay!

Frame #	Prod App <--> Prod DB	Delta Time	Rel. Time	Len
1	SYN...	0.000000	0.000000	70
2	SYN/ACK	0.004662	0.004662	70
3	ACK...	0.000128	0.004790	68
4	Connect: USER=oracle	0.000908	0.005698	233
6	Resend	0.073323	0.079021	70
8	Connect: USER=oracle	0.000552	0.079573	233
9	Accept	0.003416	0.082989	86
10	Data frame: Secure Network Services Negotiation	0.000421	0.083410	212

Oracle Logon Slow

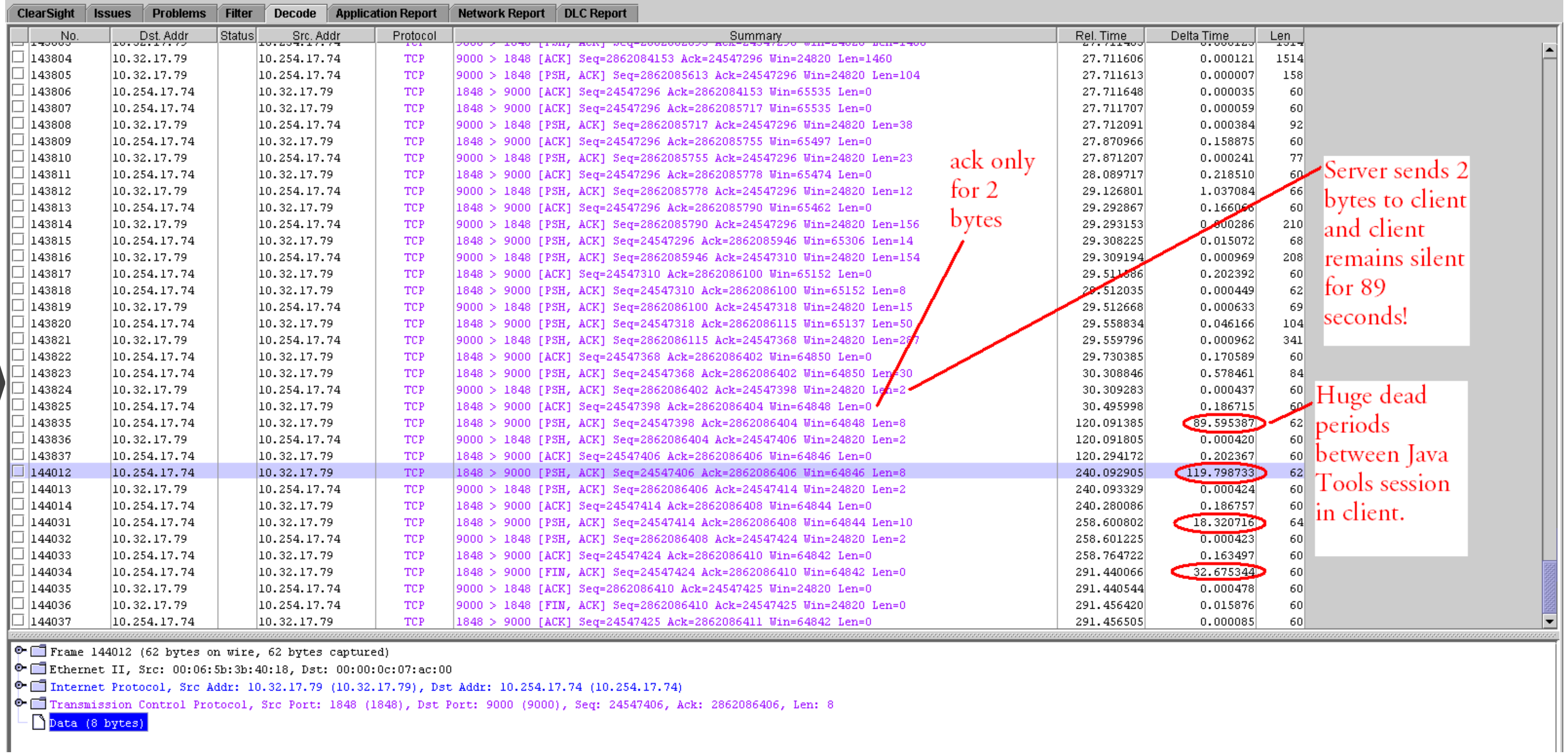


11	Data frame: Secure Network Services Negotiation	0.002661	0.086071	189
14	Set Data Representation	0.004932	0.091003	795
15	Set Data Representation	0.005474	0.096477	876
16	User request: LogonA	0.000570	0.097047	162
17	Return OPI Parameter	0.015985	0.113032	114
18	User request: LogonB	0.000861	0.113893	196
20	Error Return Status	0.420606		
21	User request: Get Version/Date String	0.000323		
22	Return OPI Parameter	0.001775		
23	User request: Autocommit On	0.000213		
24	Function Complete	0.001460		
25	User request: Open Cursor	0.000311	0.538581	77

Logon A is 72 milliseconds…

Logon B is 420 milliseconds!

JAVA Slow Client



	No.	Dst. Addr	Status	Src. Addr	Protocol	Summary	Rel. Time	Delta Time	Len
□	143804	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [ACK] Seq=2862084153 Ack=24547296 Win=24820 Len=1460	27.711606	0.000121	1514
□	143805	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [PSH, ACK] Seq=2862085613 Ack=24547296 Win=24820 Len=104	27.711613	0.000007	158
□	143806	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [ACK] Seq=24547296 Ack=2862084153 Win=65535 Len=0	27.711648	0.000035	60
□	143807	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [ACK] Seq=24547296 Ack=2862085717 Win=65535 Len=0	27.711707	0.000059	60
□	143808	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [PSH, ACK] Seq=2862085717 Ack=24547296 Win=24820 Len=38	27.712091	0.000384	92
□	143809	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [ACK] Seq=24547296 Ack=2862085755 Win=65497 Len=0	27.870966	0.158875	60
□	143810	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [PSH, ACK] Seq=2862085755 Ack=24547296 Win=24820 Len=23	27.871207	0.000241	77
□	143811	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [ACK] Seq=24547296 Ack=2862085778 Win=65474 Len=0	28.089717	0.218510	60
□	143812	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [PSH, ACK] Seq=2862085778 Ack=24547296 Win=24820 Len=12	29.126801	1.037084	66
□	143813	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [ACK] Seq=24547296 Ack=2862085790 Win=65462 Len=0	29.292867	0.166066	60
□	143814	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [PSH, ACK] Seq=2862085790 Ack=24547296 Win=24820 Len=156	29.293153	0.000286	210
□	143815	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [PSH, ACK] Seq=24547296 Ack=2862085946 Win=65306 Len=14	29.308225	0.015072	68
□	143816	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [PSH, ACK] Seq=2862085946 Ack=24547310 Win=24820 Len=154	29.309194	0.000969	208
□	143817	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [ACK] Seq=24547310 Ack=2862086100 Win=65152 Len=0	29.511586	0.202392	60
□	143818	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [PSH, ACK] Seq=24547310 Ack=2862086100 Win=65152 Len=8	29.512035	0.000449	62
□	143819	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [PSH, ACK] Seq=2862086100 Ack=24547318 Win=24820 Len=15	29.512668	0.000633	69
□	143820	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [PSH, ACK] Seq=24547318 Ack=2862086115 Win=65137 Len=50	29.558834	0.046166	104
□	143821	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [PSH, ACK] Seq=2862086115 Ack=24547368 Win=24820 Len=287	29.559796	0.000962	341
□	143822	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [ACK] Seq=24547368 Ack=2862086402 Win=64850 Len=0	29.730385	0.170589	60
□	143823	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [PSH, ACK] Seq=24547368 Ack=2862086402 Win=64850 Len=30	30.308846	0.578461	84
□	143824	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [PSH, ACK] Seq=2862086402 Ack=24547398 Win=24820 Len=2	30.309283	0.000437	60
□	143825	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [ACK] Seq=24547398 Ack=2862086404 Win=64848 Len=0	30.495998	0.186715	60
□	143835	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [PSH, ACK] Seq=24547398 Ack=2862086404 Win=64848 Len=8	120.091385	89.595387	62
□	143836	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [PSH, ACK] Seq=2862086404 Ack=24547406 Win=24820 Len=2	120.091805	0.000420	60
□	143837	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [ACK] Seq=24547406 Ack=2862086406 Win=64846 Len=0	120.294172	0.202367	60
□	144012	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [PSH, ACK] Seq=24547406 Ack=2862086406 Win=64846 Len=8	240.092905	119.798733	62
□	144013	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [PSH, ACK] Seq=2862086406 Ack=24547414 Win=24820 Len=2	240.093329	0.000424	60
□	144014	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [ACK] Seq=24547414 Ack=2862086408 Win=64844 Len=0	240.280086	0.186757	60
□	144031	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [PSH, ACK] Seq=24547414 Ack=2862086408 Win=64844 Len=10	258.600802	18.320716	64
□	144032	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [PSH, ACK] Seq=2862086408 Ack=24547424 Win=24820 Len=2	258.601225	0.000423	60
□	144033	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [ACK] Seq=24547424 Ack=2862086410 Win=64842 Len=0	258.764722	0.163497	60
□	144034	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [FIN, ACK] Seq=24547424 Ack=2862086410 Win=64842 Len=0	291.440066	32.675344	60
□	144035	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [ACK] Seq=2862086410 Ack=24547425 Win=24820 Len=0	291.440544	0.000478	60
□	144036	10.32.17.79		10.254.17.74	TCP	9000 > 1848 [FIN, ACK] Seq=2862086410 Ack=24547425 Win=24820 Len=0	291.456420	0.015876	60
□	144037	10.254.17.74		10.32.17.79	TCP	1848 > 9000 [ACK] Seq=24547425 Ack=2862086411 Win=64842 Len=0	291.456505	0.000085	60

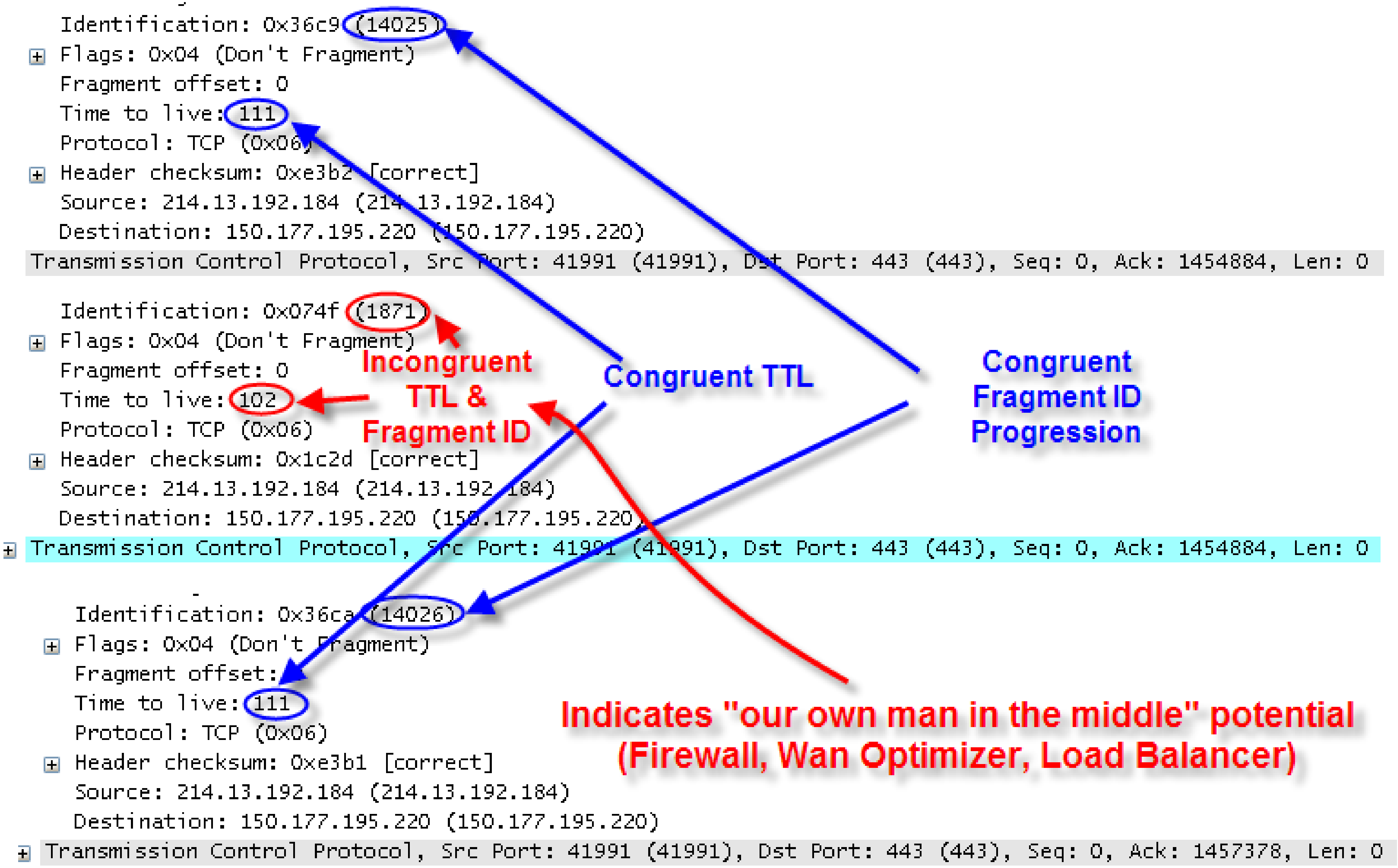
```
Frame 144012 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:06:5b:3b:40:18, Dst: 00:00:0c:07:ac:00
Internet Protocol, Src Addr: 10.32.17.79 (10.32.17.79), Dst Addr: 10.254.17.74 (10.254.17.74)
Transmission Control Protocol, Src Port: 1848 (1848), Dst Port: 9000 (9000), Seq: 24547406, Ack: 2862086406, Len: 8
    Data (8 bytes)
```

ack only for 2 bytes

Server sends 2 bytes to client and client remains silent for 89 seconds!

Huge dead periods between Java Tools session in client.

HOP/TTL Incongruity “our own man in the middle”



```
  Identification: 0x36c9 (14025)
⊞ Flags: 0x04 (Don't Fragment)
  Fragment offset: 0
  Time to live: 111
  Protocol: TCP (0x06)
⊞ Header checksum: 0xe3b2 [correct]
  Source: 214.13.192.184 (214.13.192.184)
  Destination: 150.177.195.220 (150.177.195.220)
Transmission Control Protocol, Src Port: 41991 (41991), Dst Port: 443 (443), Seq: 0, Ack: 1454884, Len: 0

  Identification: 0x074f (1871)
⊞ Flags: 0x04 (Don't Fragment)
  Fragment offset: 0
  Time to live: 102
  Protocol: TCP (0x06)
⊞ Header checksum: 0x1c2d [correct]
  Source: 214.13.192.184 (214.13.192.184)
  Destination: 150.177.195.220 (150.177.195.220)
⊞ Transmission Control Protocol, Src Port: 41991 (41991), Dst Port: 443 (443), Seq: 0, Ack: 1454884, Len: 0

  Identification: 0x36ca (14026)
⊞ Flags: 0x04 (Don't Fragment)
  Fragment offset:
  Time to live: 111
  Protocol: TCP (0x06)
⊞ Header checksum: 0xe3b1 [correct]
  Source: 214.13.192.184 (214.13.192.184)
  Destination: 150.177.195.220 (150.177.195.220)
⊞ Transmission Control Protocol, Src Port: 41991 (41991), Dst Port: 443 (443), Seq: 0, Ack: 1457378, Len: 0
```

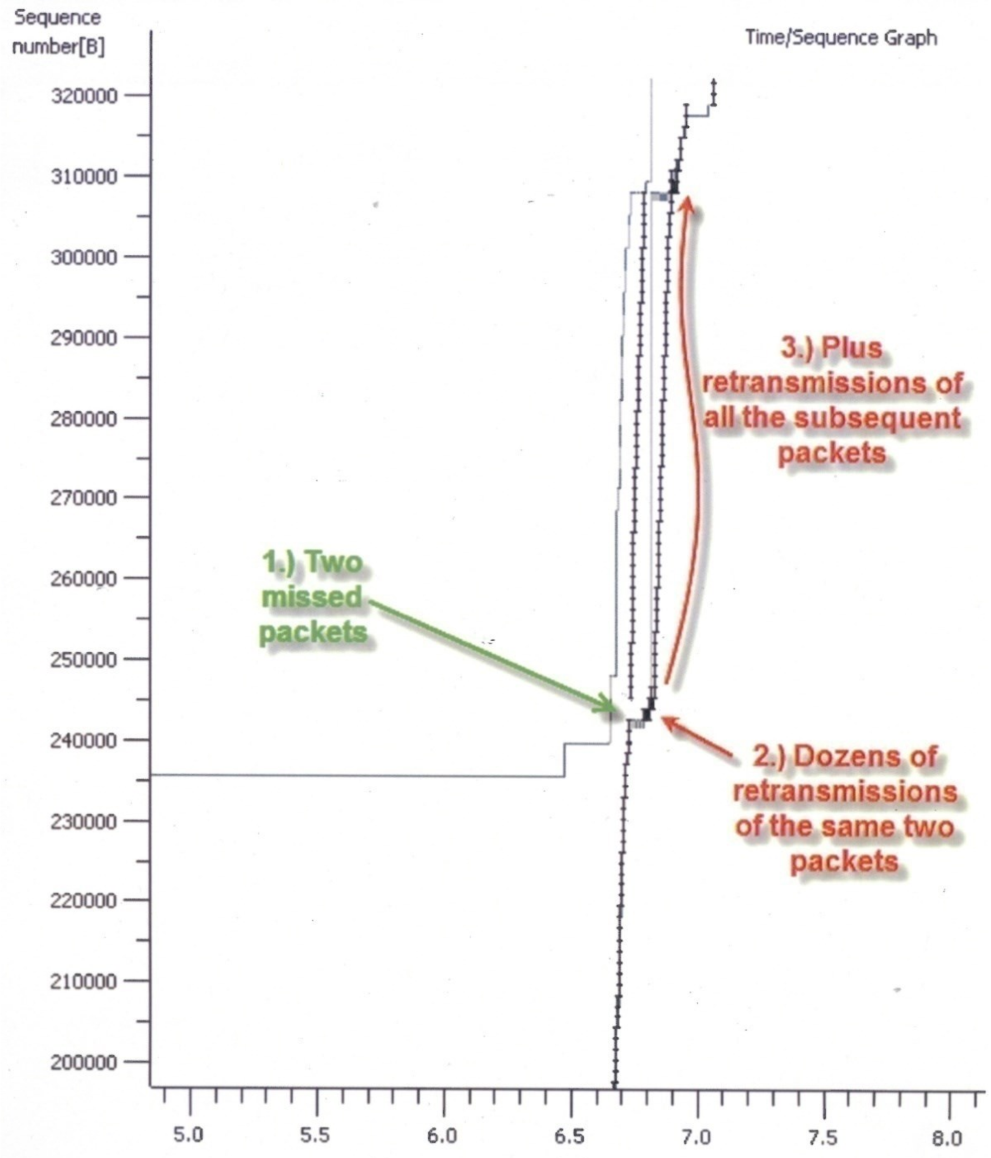
Incongruent TTL & Fragment ID

Congruent TTL

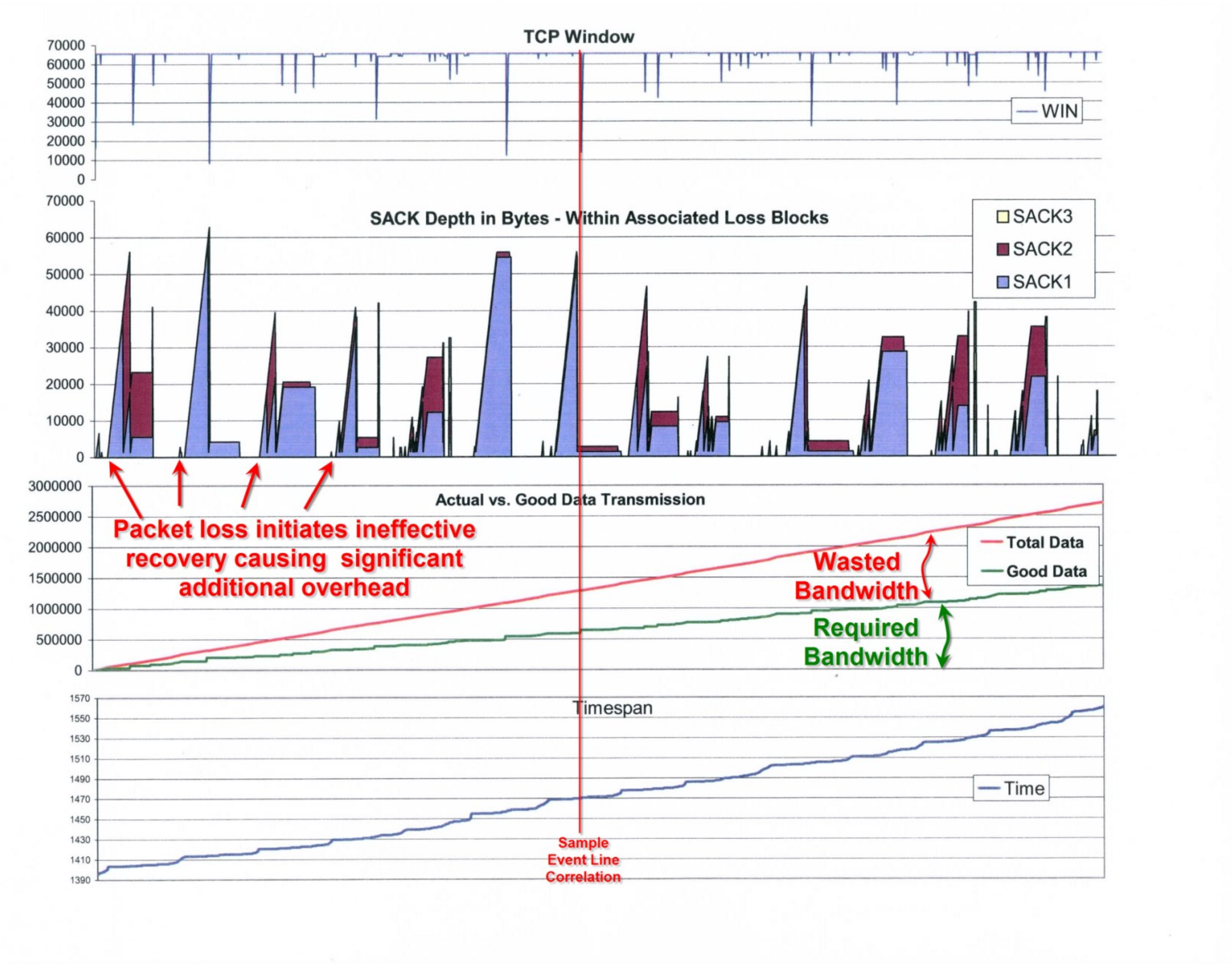
Congruent Fragment ID Progression

Indicates "our own man in the middle" potential (Firewall, Wan Optimizer, Load Balancer)

TCP Data Duplication Details



Significant Data Duplication



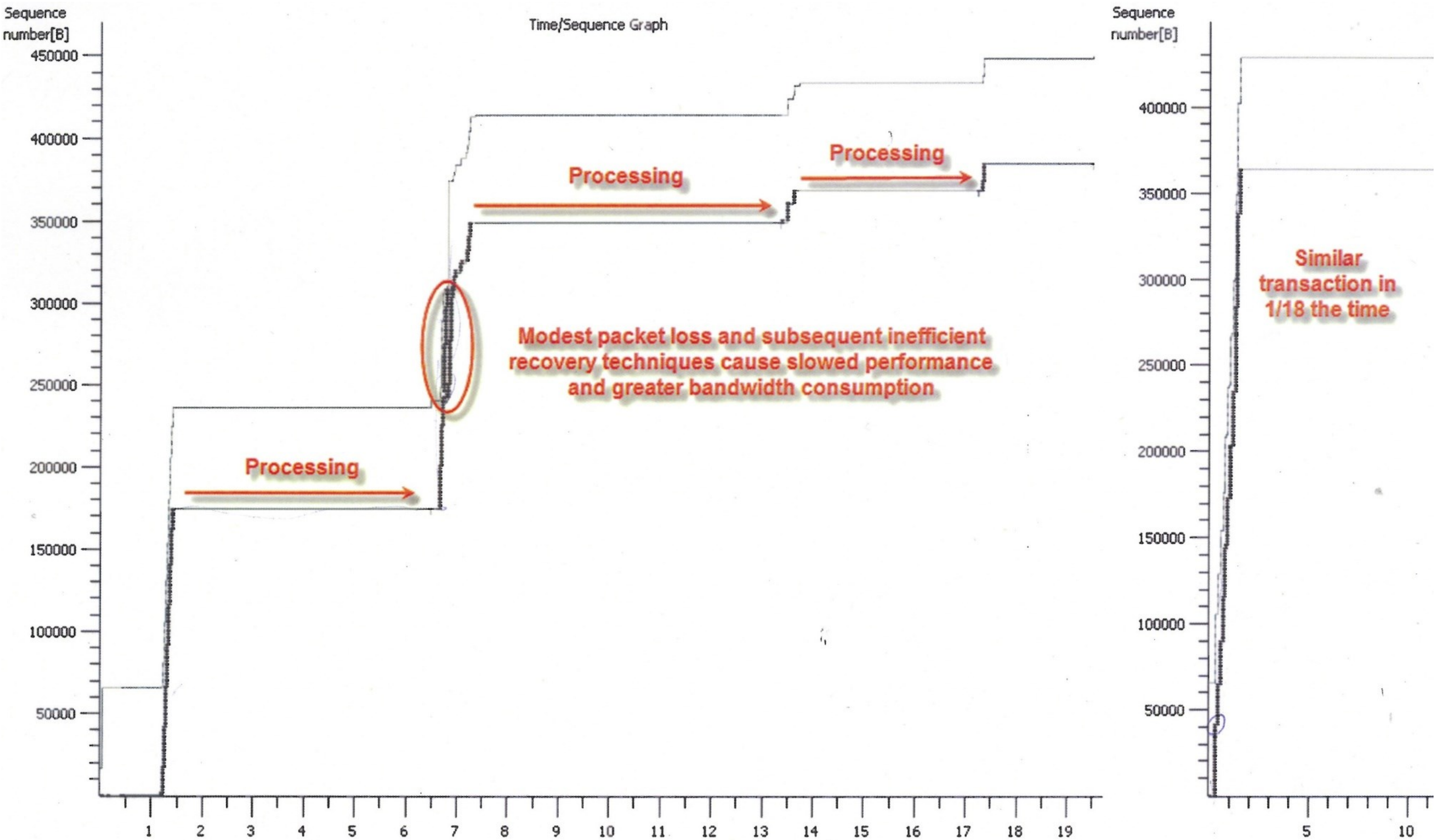
Packet loss initiates ineffective recovery causing significant additional overhead

Wasted Bandwidth

Required Bandwidth

Sample Event Line Correlation

Data Duplication & App Processing



Processing

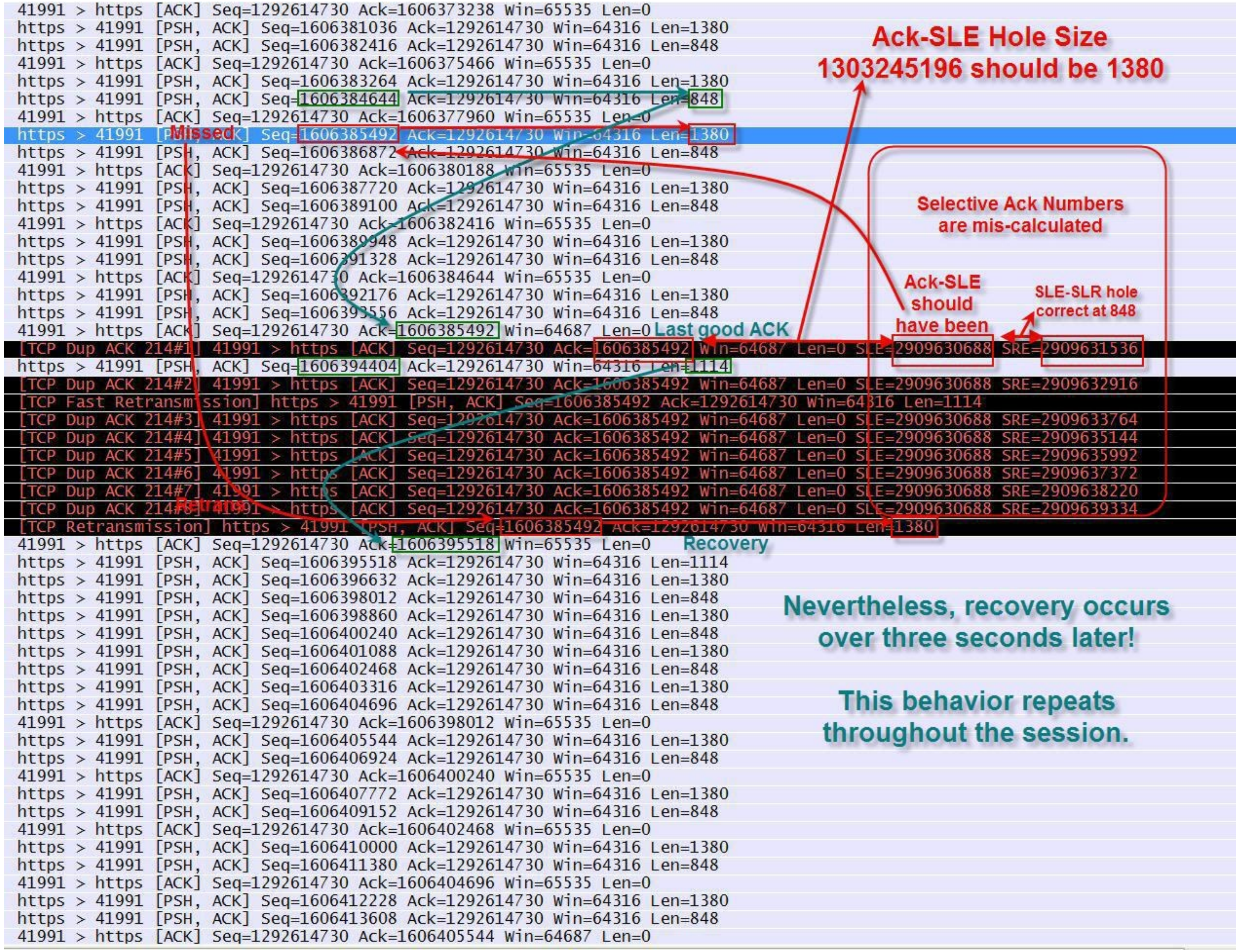
Processing

Processing

Modest packet loss and subsequent inefficient recovery techniques cause slowed performance and greater bandwidth consumption

Similar transaction in 1/18 the time

TCP – Packet Loss – Poor Recovery



```
41991 > https [ACK] Seq=1292614730 Ack=1606373238 Win=65535 Len=0
https > 41991 [PSH, ACK] Seq=1606381036 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606382416 Ack=1292614730 Win=64316 Len=848
41991 > https [ACK] Seq=1292614730 Ack=1606375466 Win=65535 Len=0
https > 41991 [PSH, ACK] Seq=1606383264 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606384644 Ack=1292614730 Win=64316 Len=848
41991 > https [ACK] Seq=1292614730 Ack=1606377960 Win=65535 Len=0
https > 41991 [PSH, ACK] Seq=1606385492 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606386872 Ack=1292614730 Win=64316 Len=848
41991 > https [ACK] Seq=1292614730 Ack=1606380188 Win=65535 Len=0
https > 41991 [PSH, ACK] Seq=1606387720 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606389100 Ack=1292614730 Win=64316 Len=848
41991 > https [ACK] Seq=1292614730 Ack=1606382416 Win=65535 Len=0
https > 41991 [PSH, ACK] Seq=1606389948 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606391328 Ack=1292614730 Win=64316 Len=848
41991 > https [ACK] Seq=1292614730 Ack=1606384644 Win=65535 Len=0
https > 41991 [PSH, ACK] Seq=1606392176 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606393556 Ack=1292614730 Win=64316 Len=848
41991 > https [ACK] Seq=1292614730 Ack=1606385492 Win=64687 Len=0
[TCP Dup ACK 214#1] 41991 > https [ACK] Seq=1292614730 Ack=1606385492 Win=64687 Len=0 SLE=2909630688 SRE=2909631536
https > 41991 [PSH, ACK] Seq=1606394404 Ack=1292614730 Win=64316 Len=1114
[TCP Dup ACK 214#2] 41991 > https [ACK] Seq=1292614730 Ack=1606385492 Win=64687 Len=0 SLE=2909630688 SRE=2909632916
[TCP Fast Retransmission] https > 41991 [PSH, ACK] Seq=1606385492 Ack=1292614730 Win=64316 Len=1114
[TCP Dup ACK 214#3] 41991 > https [ACK] Seq=1292614730 Ack=1606385492 Win=64687 Len=0 SLE=2909630688 SRE=2909633764
[TCP Dup ACK 214#4] 41991 > https [ACK] Seq=1292614730 Ack=1606385492 Win=64687 Len=0 SLE=2909630688 SRE=2909635144
[TCP Dup ACK 214#5] 41991 > https [ACK] Seq=1292614730 Ack=1606385492 Win=64687 Len=0 SLE=2909630688 SRE=2909635992
[TCP Dup ACK 214#6] 41991 > https [ACK] Seq=1292614730 Ack=1606385492 Win=64687 Len=0 SLE=2909630688 SRE=2909637372
[TCP Dup ACK 214#7] 41991 > https [ACK] Seq=1292614730 Ack=1606385492 Win=64687 Len=0 SLE=2909630688 SRE=2909638220
[TCP Dup ACK 214#8] 41991 > https [ACK] Seq=1292614730 Ack=1606385492 Win=64687 Len=0 SLE=2909630688 SRE=2909639334
[TCP Retransmission] https > 41991 [PSH, ACK] Seq=1606385492 Ack=1292614730 Win=64316 Len=1380
41991 > https [ACK] Seq=1292614730 Ack=1606395518 Win=65535 Len=0
https > 41991 [PSH, ACK] Seq=1606395518 Ack=1292614730 Win=64316 Len=1114
https > 41991 [PSH, ACK] Seq=1606396632 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606398012 Ack=1292614730 Win=64316 Len=848
https > 41991 [PSH, ACK] Seq=1606398860 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606400240 Ack=1292614730 Win=64316 Len=848
https > 41991 [PSH, ACK] Seq=1606401088 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606402468 Ack=1292614730 Win=64316 Len=848
https > 41991 [PSH, ACK] Seq=1606403316 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606404696 Ack=1292614730 Win=64316 Len=848
41991 > https [ACK] Seq=1292614730 Ack=1606398012 Win=65535 Len=0
https > 41991 [PSH, ACK] Seq=1606405544 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606406924 Ack=1292614730 Win=64316 Len=848
41991 > https [ACK] Seq=1292614730 Ack=1606400240 Win=65535 Len=0
https > 41991 [PSH, ACK] Seq=1606407772 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606409152 Ack=1292614730 Win=64316 Len=848
41991 > https [ACK] Seq=1292614730 Ack=1606402468 Win=65535 Len=0
https > 41991 [PSH, ACK] Seq=1606410000 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606411380 Ack=1292614730 Win=64316 Len=848
41991 > https [ACK] Seq=1292614730 Ack=1606404696 Win=65535 Len=0
https > 41991 [PSH, ACK] Seq=1606412228 Ack=1292614730 Win=64316 Len=1380
https > 41991 [PSH, ACK] Seq=1606413608 Ack=1292614730 Win=64316 Len=848
41991 > https [ACK] Seq=1292614730 Ack=1606405544 Win=64687 Len=0
```

Ack-SLE Hole Size
1303245196 should be 1380

Selective Ack Numbers
are mis-calculated

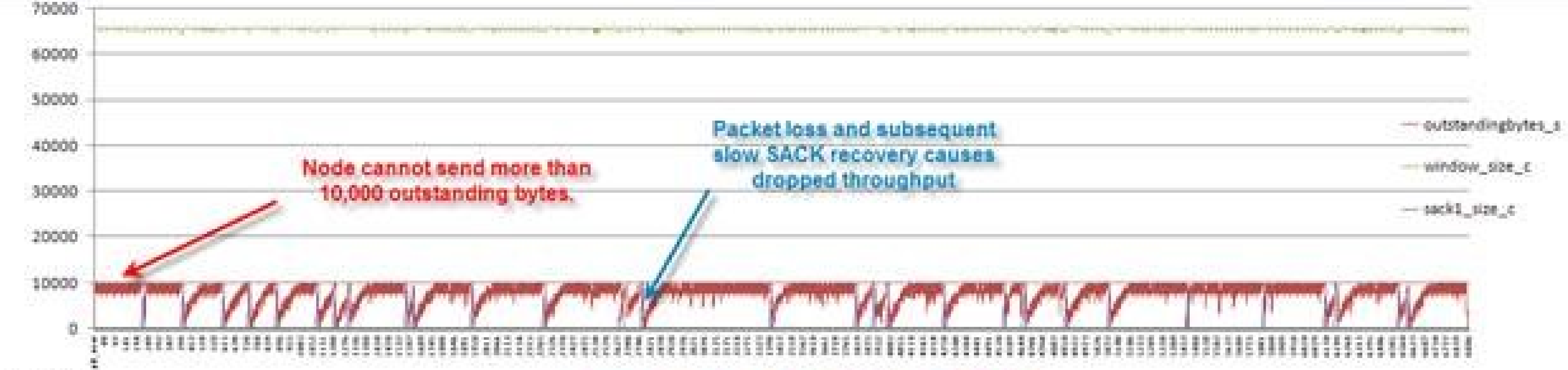
Ack-SLE
should
have been

SLE-SLR hole
correct at 848

Nevertheless, recovery occurs
over three seconds later!

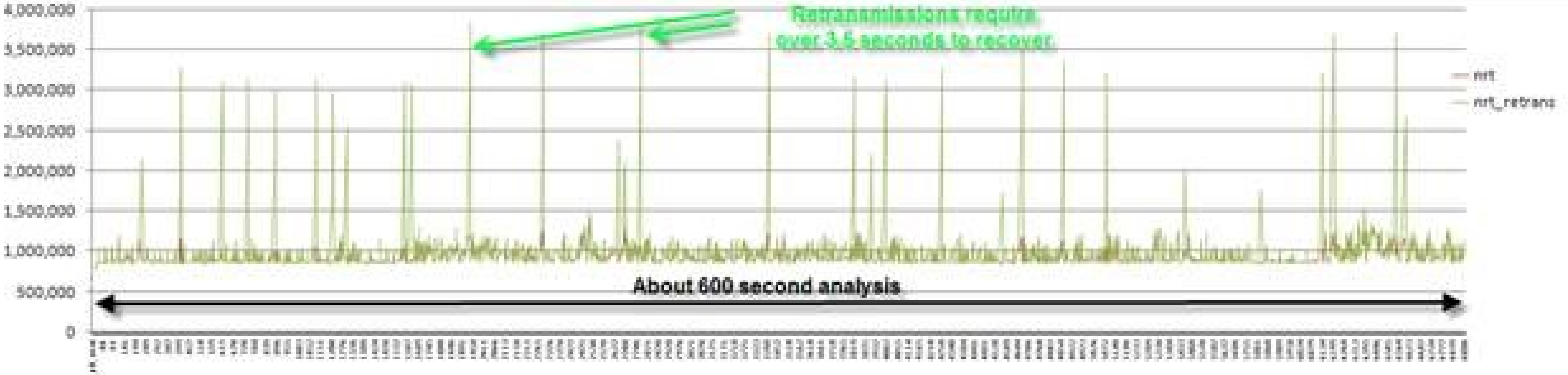
This behavior repeats
throughout the session.

TCP – Session Performance



Node cannot send more than 10,000 outstanding bytes.

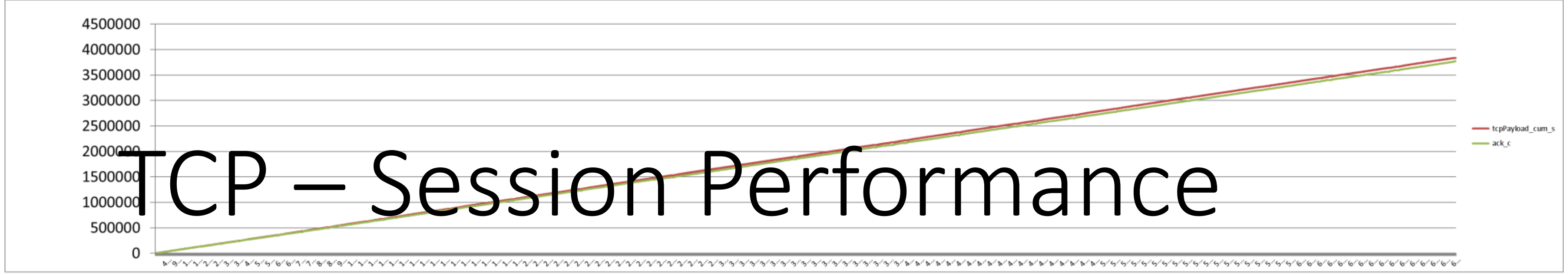
Packet loss and subsequent slow SACK recovery causes dropped throughput

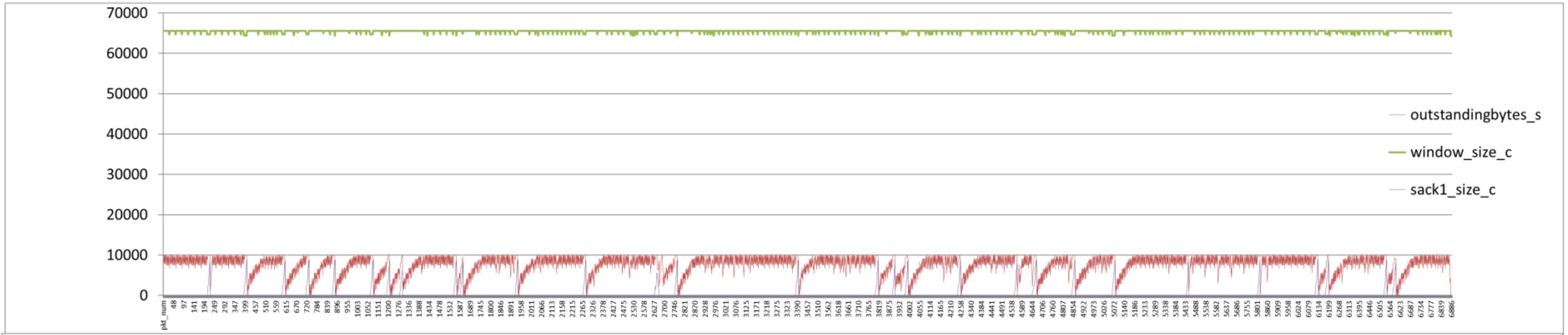


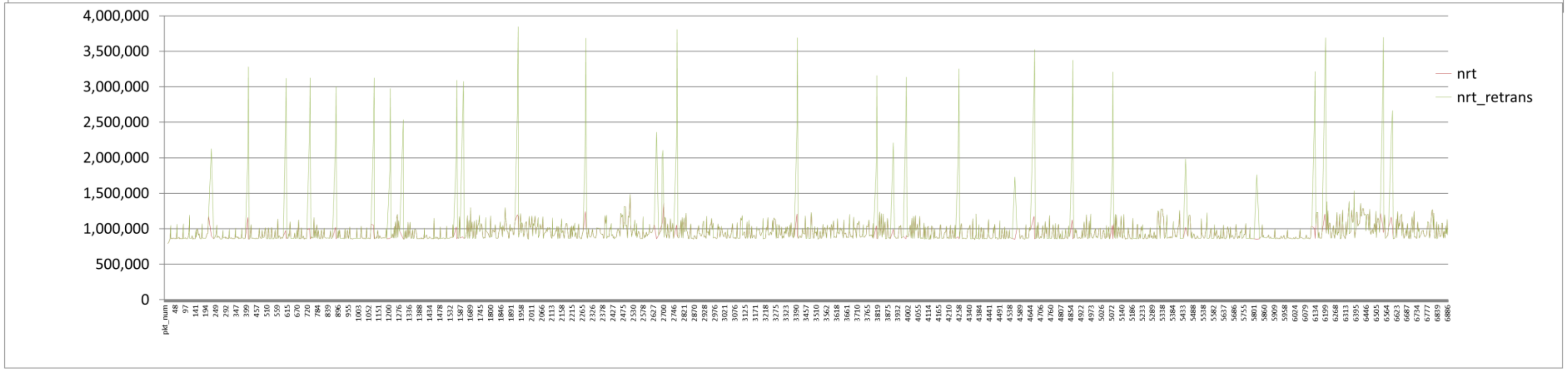
Retransmissions require over 3.5 seconds to recover

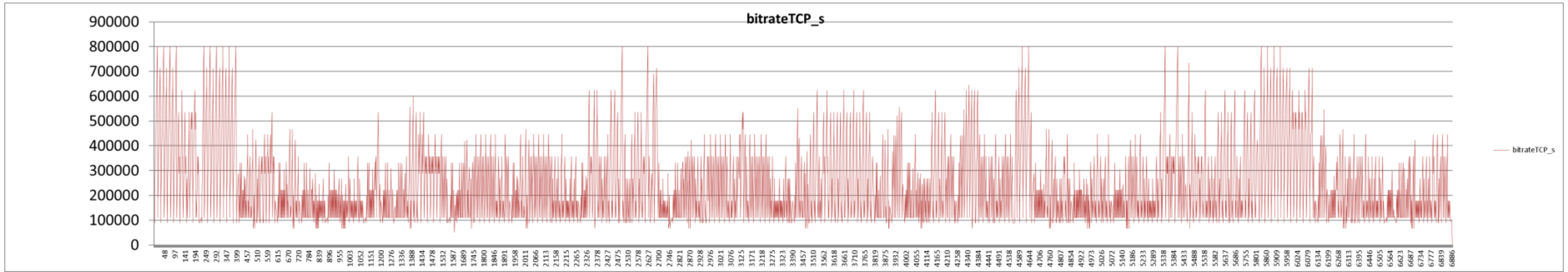
About 600 second analysis

TCP – Session Performance







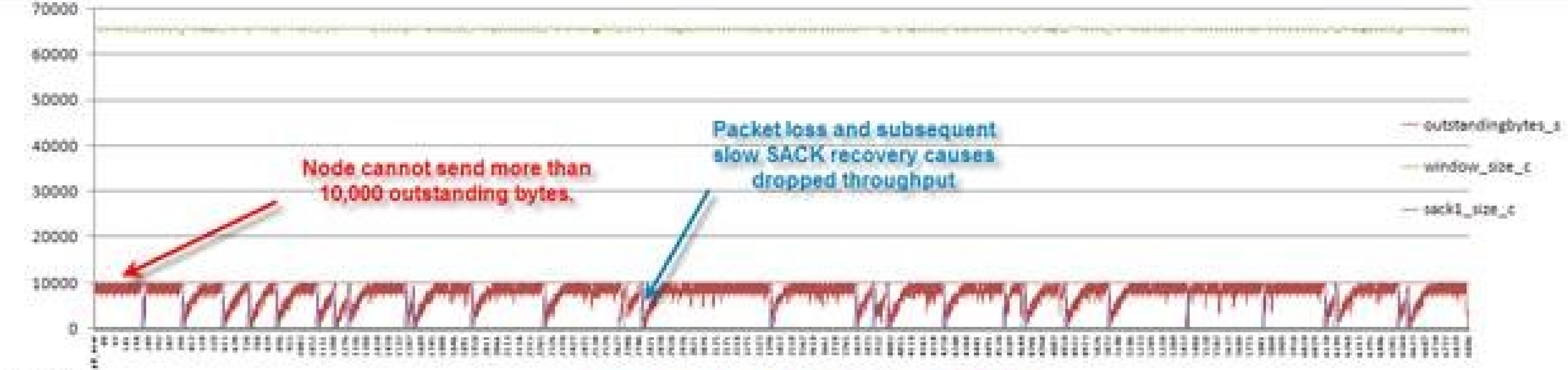


600 Seconds
4MB Data = 6666Bps
3.5 Sec Retrans Recovery

Peak Bps=80,000 observed
4MB Data @80kBps
50 Seconds

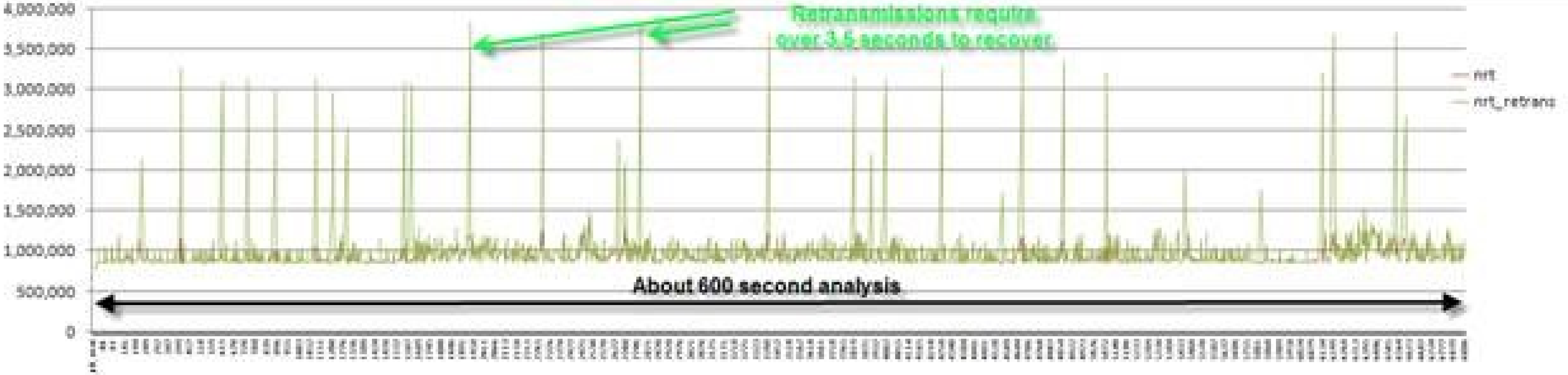
550 Second Transmission Delay

TCP – Session Performance



Node cannot send more than 10,000 outstanding bytes.

Packet loss and subsequent slow SACK recovery causes dropped throughput

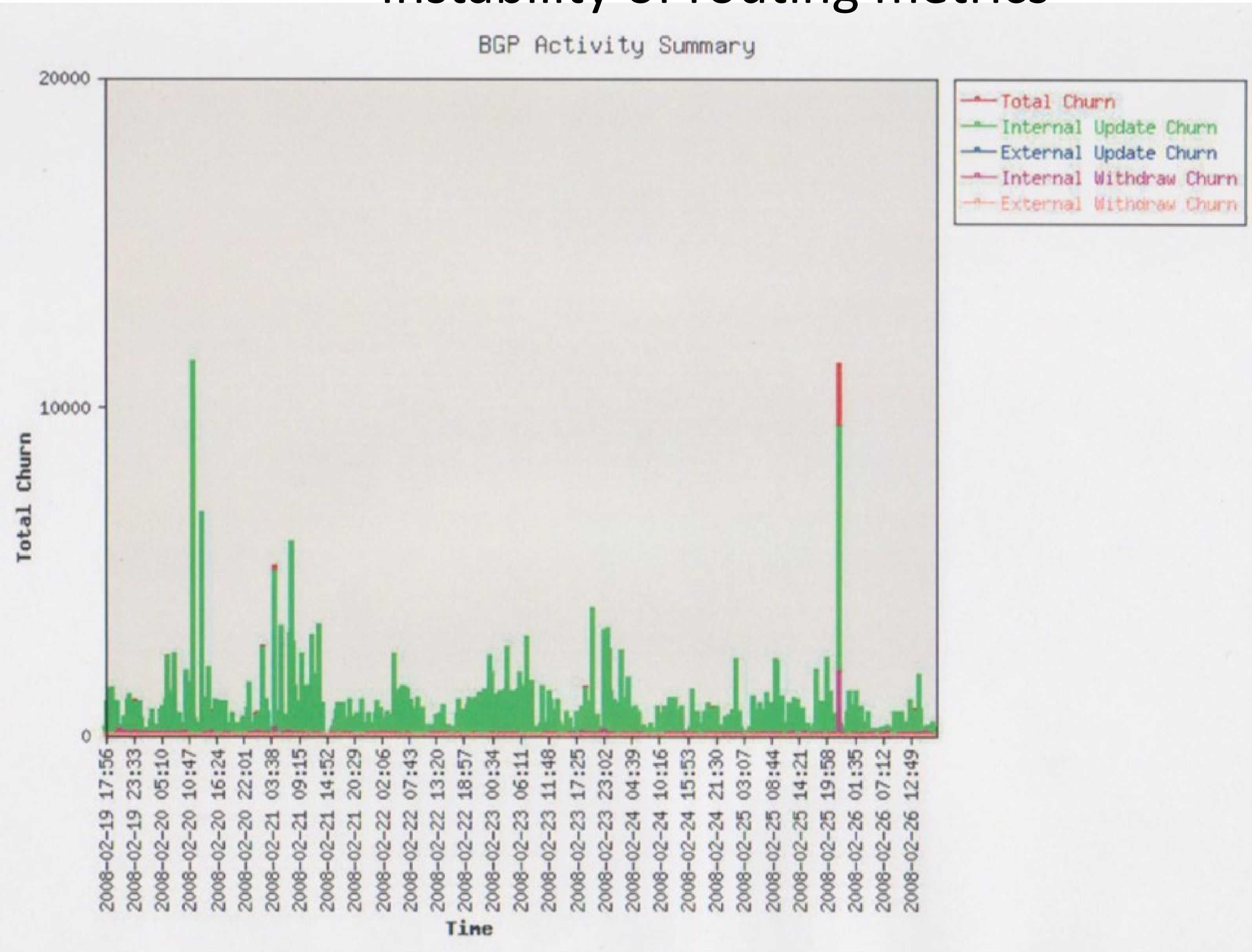


Retransmissions require over 3.5 seconds to recover.

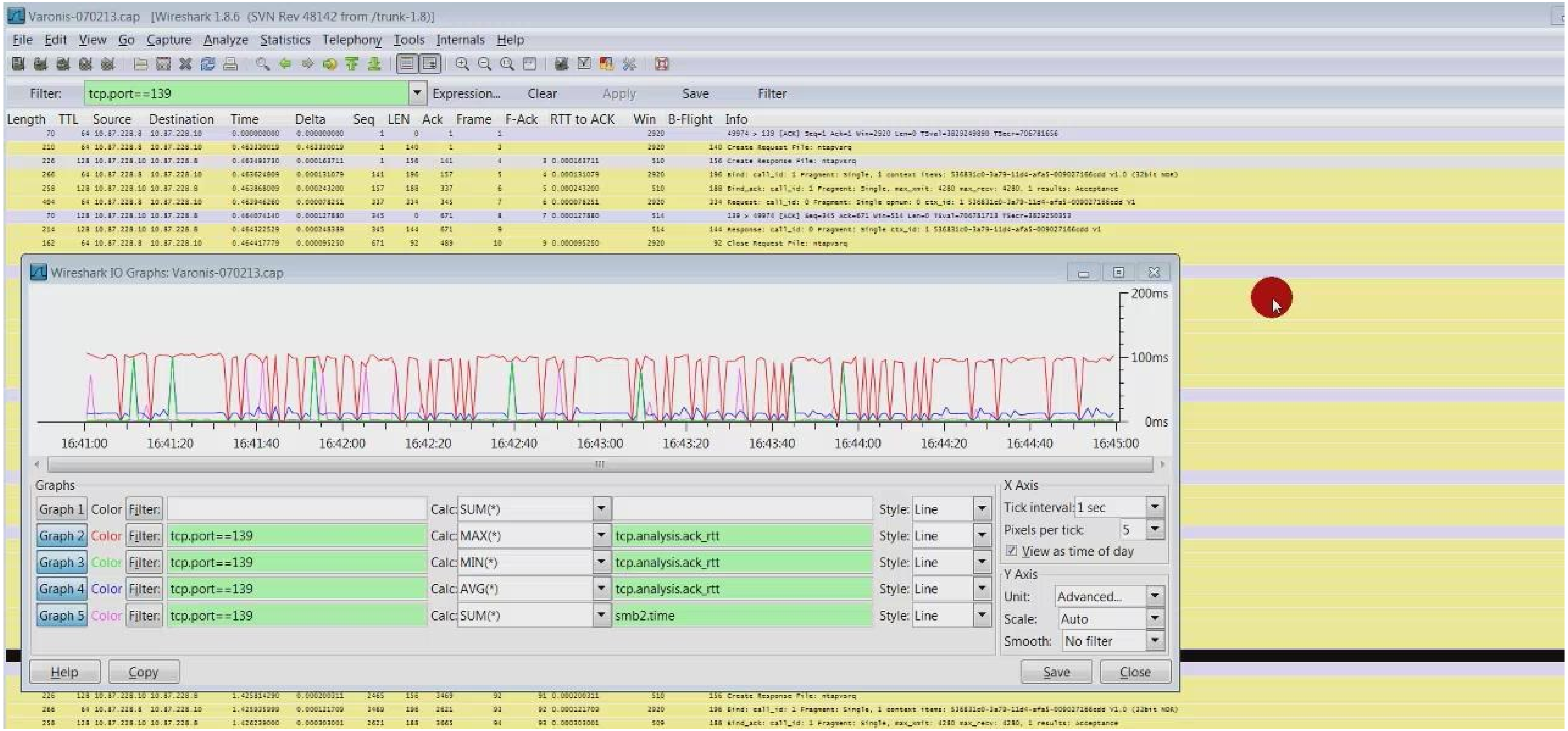
About 600 second analysis

Route Changes Impact on TCP Sessions

- Instability of routing metrics



SMB Response Time



Varonis-070213.cap [Wireshark 1.8.6 (SVN Rev 48142 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save Filter
Wireshark IO Graphs: Varonis-070213.cap
200ms
100ms
0ms
16:41:00
16:41:20
16:41:40
16:42:00
16:42:20
16:42:40
16:43:00
16:43:20
16:43:40
16:44:00
16:44:20
16:44:40
16:45:00
Help
Copy
Save
Close

Filter: tcp.port==139

Length	TTL	Source	Destination	Time	Delta	Seq	LEN	Ack	Frame	F-Ack	RTT to ACK	Win	B-Flight	Info
70	64	10.87.228.8	10.87.228.10	0.000000000	0.000000000	1	0	1	1			2920		49974 > 139 [ACK] Seq=1 Ack=1 Win=2920 Len=0 TSval=3829249890 TSecr=706781656
210	64	10.87.228.8	10.87.228.10	0.463330019	0.463330019	1	140	1	3			2920	140	Create Request File: ntapvarq
226	128	10.87.228.10	10.87.228.8	0.463493730	0.000163711	1	156	141	4	3	0.000163711	510	156	Create Response File: ntapvarq
266	64	10.87.228.8	10.87.228.10	0.463624809	0.000131079	141	196	157	5	4	0.000131079	2920	196	Bind: call_id: 1 Fragment: Single, 1 context items: 536831c0-3a79-11d4-afa5-009027166cdd v1.0 (32bit NDR)
258	128	10.87.228.10	10.87.228.8	0.463868009	0.000243200	157	188	337	6	5	0.000243200	510	188	Bind_ack: call_id: 1 Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 results: Acceptance
404	64	10.87.228.8	10.87.228.10	0.463946260	0.000078251	337	334	345	7	6	0.000078251	2920	334	Request: call_id: 0 Fragment: Single opnum: 0 ctx_id: 1 536831c0-3a79-11d4-afa5-009027166cdd V1
70	128	10.87.228.10	10.87.228.8	0.464074140	0.000127880	345	0	671	8	7	0.000127880	514		139 > 49974 [ACK] Seq=345 Ack=671 Win=514 Len=0 TSval=706781718 TSecr=3829250353
214	128	10.87.228.10	10.87.228.8	0.464322529	0.000248389	345	144	671	9			514	144	Response: call_id: 0 Fragment: Single ctx_id: 1 536831c0-3a79-11d4-afa5-009027166cdd v1
162	64	10.87.228.8	10.87.228.10	0.464417779	0.000095250	671	92	489	10	9	0.000095250	2920	92	Close Request File: ntapvarq
226	128	10.87.228.10	10.87.228.8	1.425814290	0.000200311	2465	156	3469	92	91	0.000200311	510	156	Create Response File: ntapvarq
266	64	10.87.228.8	10.87.228.10	1.425935999	0.000121709	3469	196	2621	93	92	0.000121709	2920	196	Bind: call_id: 1 Fragment: Single, 1 context items: 536831c0-3a79-11d4-afa5-009027166cdd V1.0 (32bit NDR)
258	128	10.87.228.10	10.87.228.8	1.426239000	0.000303001	2621	188	3665	94	93	0.000303001	509	188	Bind_ack: call_id: 1 Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 results: Acceptance

Graphs

Graph	Color	Filter:	Calc:		Style:
Graph 1	Color		SUM(*)		Line
Graph 2	Color	tcp.port==139	MAX(*)	tcp.analysis.ack_rtt	Line
Graph 3	Color	tcp.port==139	MIN(*)	tcp.analysis.ack_rtt	Line
Graph 4	Color	tcp.port==139	AVG(*)	tcp.analysis.ack_rtt	Line
Graph 5	Color	tcp.port==139	SUM(*)	smb2.time	Line

X Axis

Tick interval: 1 sec

Pixels per tick: 5

☑ View as time of day

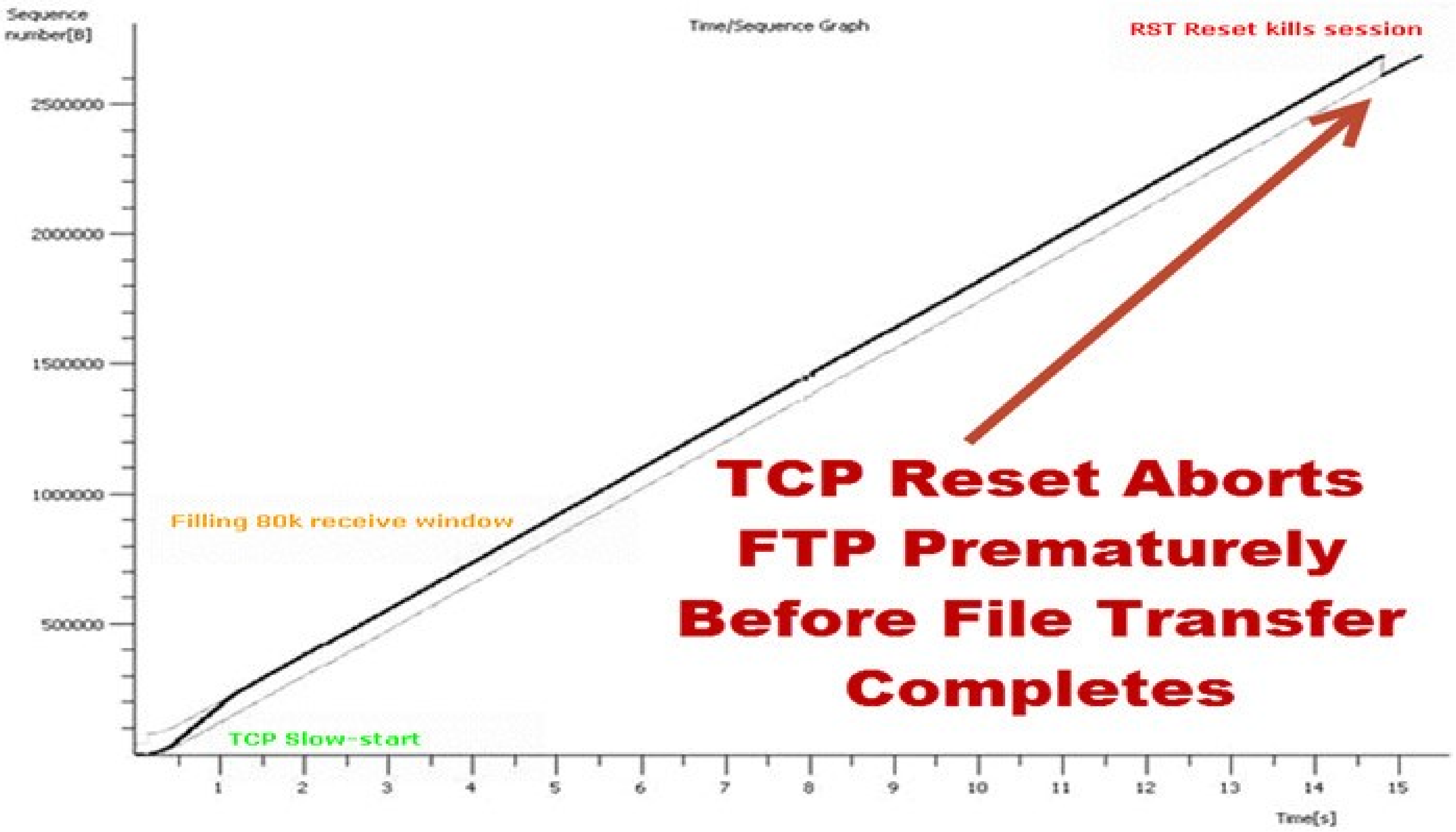
Y Axis

Unit: Advanced...

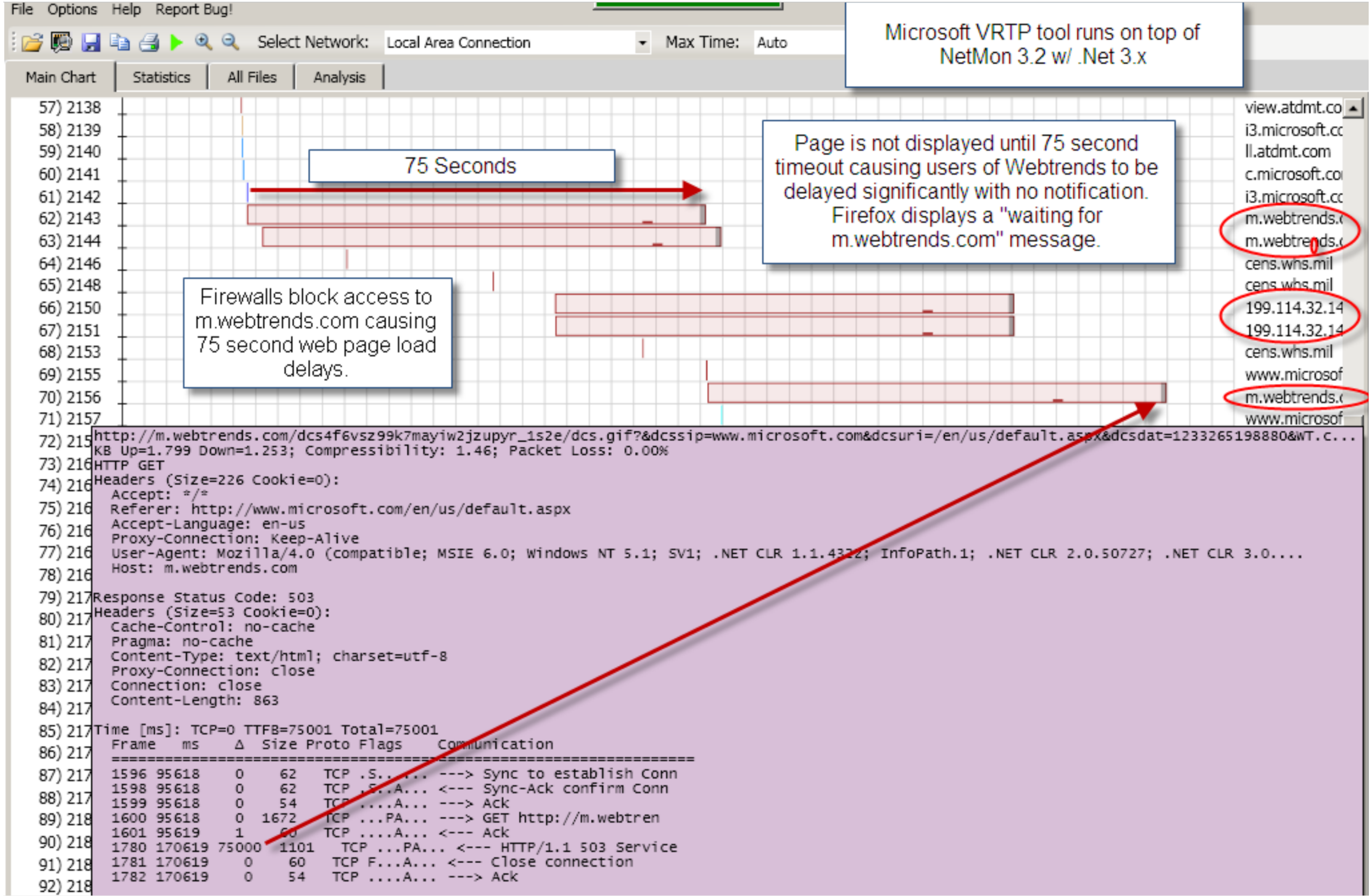
Scale: Auto

Smooth: No filter

FTP Fail due to Reset



TCP Reset Aborts FTP Prematurely Before File Transfer Completes



Microsoft VRTP tool runs on top of NetMon 3.2 w/ .Net 3.x

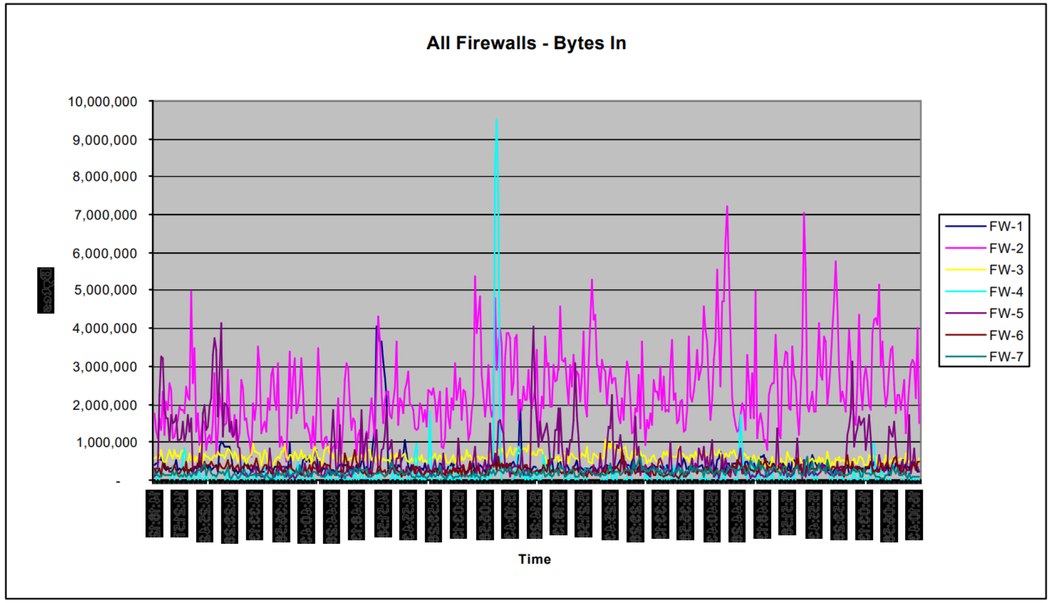
75 Seconds

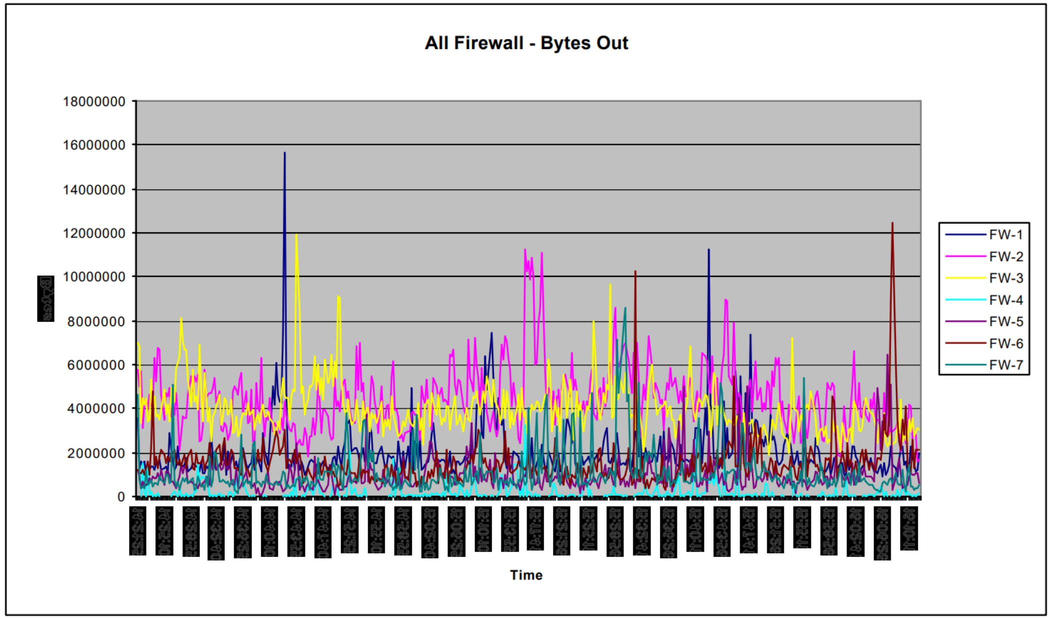
Page is not displayed until 75 second timeout causing users of Webtrends to be delayed significantly with no notification. Firefox displays a "waiting for m.webtrends.com" message.

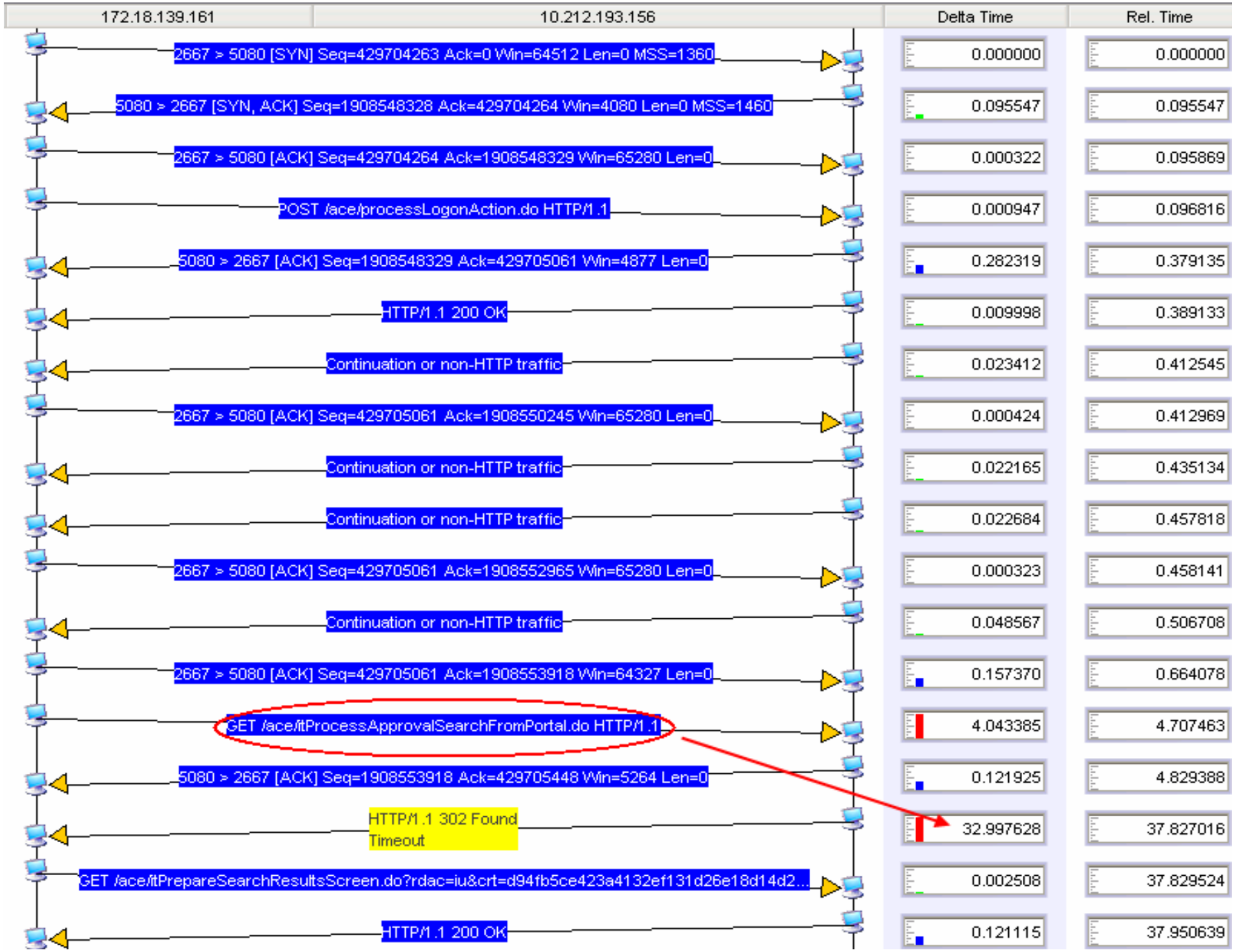
Firewalls block access to m.webtrends.com causing 75 second web page load delays.

```
http://m.webtrends.com/dcs4f6vsz99k7mayiw2jzupyr_1s2e/dcs.gif?&dcssip=www.microsoft.com&dcsuri=/en/us/default.aspx&dcsdat=1233265198880&WT.c...
KB Up=1.799 Down=1.253; Compressibility: 1.46; Packet Loss: 0.00%
HTTP GET
Headers (Size=226 Cookie=0):
  Accept: */*
  Referer: http://www.microsoft.com/en/us/default.aspx
  Accept-Language: en-us
  Proxy-Connection: Keep-Alive
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; InfoPath.1; .NET CLR 2.0.50727; .NET CLR 3.0....
  Host: m.webtrends.com

Response Status Code: 503
Headers (Size=53 Cookie=0):
  Cache-Control: no-cache
  Pragma: no-cache
  Content-Type: text/html; charset=utf-8
  Proxy-Connection: close
  Connection: close
  Content-Length: 863

Time [ms]: TCP=0 TTFB=75001 Total=75001
  Frame   ms     Δ  Size Proto Flags    Communication
  ================================================================
  1596 95618    0    62   TCP .S...... ---> Sync to establish Conn
  1598 95618    0    62   TCP .S..A... <--- Sync-Ack confirm Conn
  1599 95618    0    54   TCP ....A... ---> Ack
  1600 95618    0  1672   TCP ...PA... ---> GET http://m.webtren
  1601 95619    1    60   TCP ....A... <--- Ack
  1780 170619 75000  1101   TCP ...PA... <--- HTTP/1.1 503 Service
  1781 170619    0    60   TCP F...A... <--- Close connection
  1782 170619    0    54   TCP ....A... ---> Ack
```

Firewall Ingress vs Egress







172.18.139.161 → / ← 10.212.193.156	Delta Time	Rel. Time
→ 2667 > 5080 [SYN] Seq=429704263 Ack=0 Win=64512 Len=0 MSS=1360	0.000000	0.000000
← 5080 > 2667 [SYN, ACK] Seq=1908548328 Ack=429704264 Win=4080 Len=0 MSS=1460	0.095547	0.095547
→ 2667 > 5080 [ACK] Seq=429704264 Ack=1908548329 Win=65280 Len=0	0.000322	0.095869
→ POST /ace/processLogonAction.do HTTP/1.1	0.000947	0.096816
← 5080 > 2667 [ACK] Seq=1908548329 Ack=429705061 Win=4877 Len=0	0.282319	0.379135
← HTTP/1.1 200 OK	0.009998	0.389133
← Continuation or non-HTTP traffic	0.023412	0.412545
→ 2667 > 5080 [ACK] Seq=429705061 Ack=1908550245 Win=65280 Len=0	0.000424	0.412969
← Continuation or non-HTTP traffic	0.022165	0.435134
← Continuation or non-HTTP traffic	0.022684	0.457818
→ 2667 > 5080 [ACK] Seq=429705061 Ack=1908552965 Win=65280 Len=0	0.000323	0.458141
← Continuation or non-HTTP traffic	0.048567	0.506708
→ 2667 > 5080 [ACK] Seq=429705061 Ack=1908553918 Win=64327 Len=0	0.157370	0.664078
→ GET /ace/itProcessApprovalSearchFromPortal.do HTTP/1.1	4.043385	4.707463
← 5080 > 2667 [ACK] Seq=1908553918 Ack=429705448 Win=5264 Len=0	0.121925	4.829388
← HTTP/1.1 302 Found Timeout	32.997628	37.827016
→ GET /ace/itPrepareSearchResultsScreen.do?rdac=iu&crt=d94fb5ce423a4132ef131d26e18d14d2...	0.002508	37.829524
← HTTP/1.1 200 OK	0.121115	37.950639

Figure A-4: ACE Slow Lookup

TCP Window Chart

The figure below provides a brief snapshot of the TCP Receive Window behavior on WAPPBI01. This was graphed based upon the advertised window size for receiving SQL traffic (TCP 1433) for a single session. It provides a detailed explanation to the events. The total time lapse for display are limited to 787ms in order to provide adequate visualization of the information (i.e. limit data points)

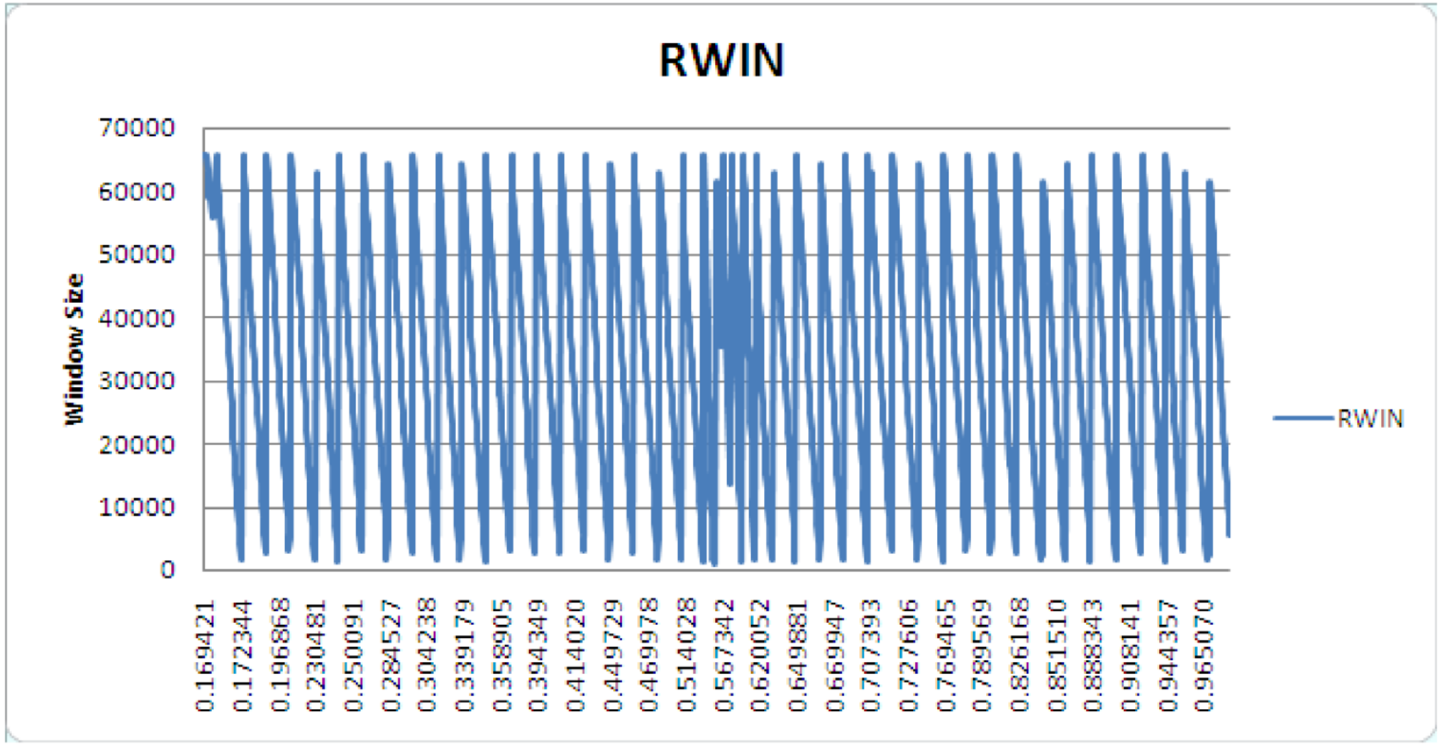
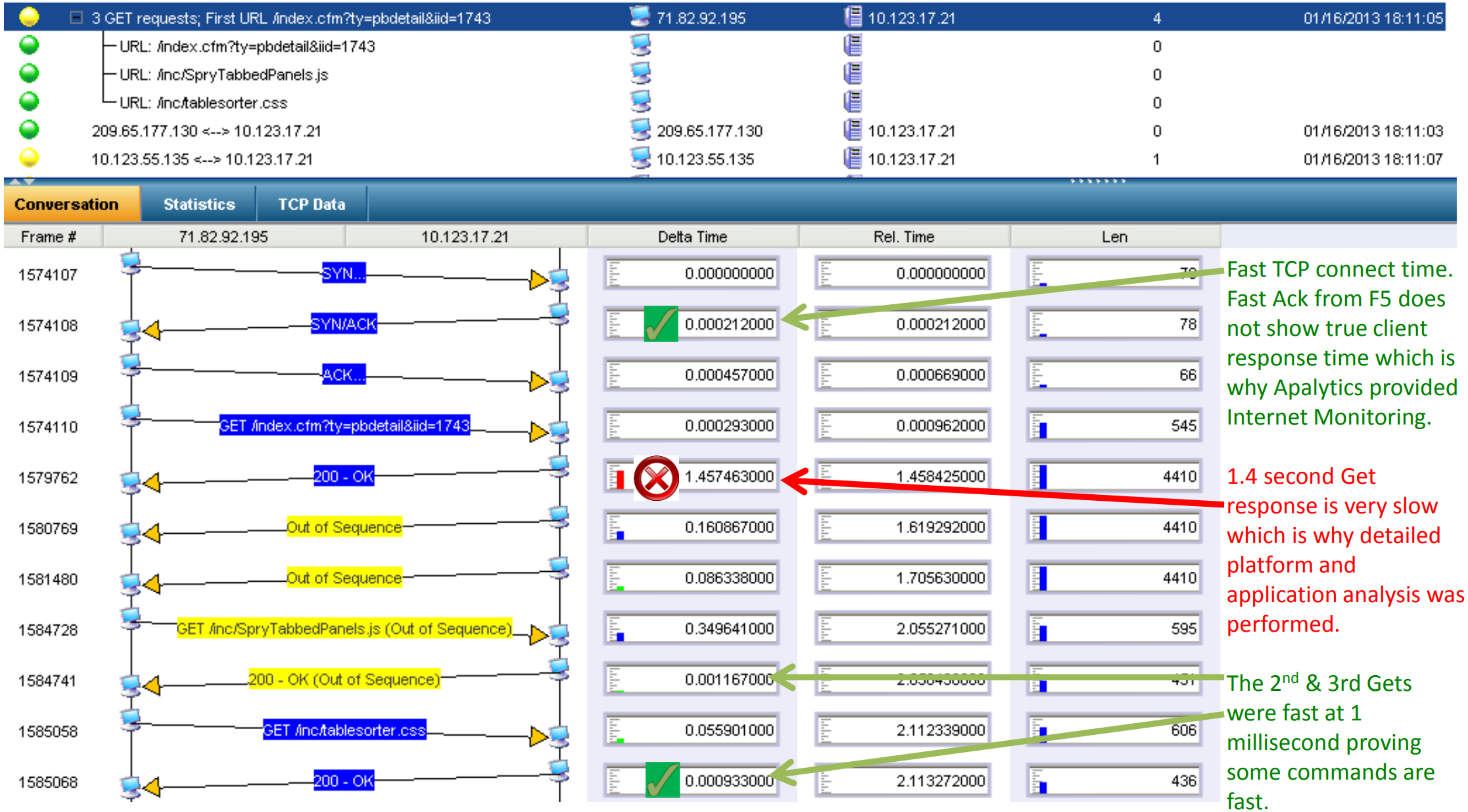


Figure 26: WAPPBI01 TCP Receive Window Size Behavior

HTTP Response Times



●	⊟ 3 GET requests; First URL /index.cfm?ty=pbdetail&iid=1743	71.82.92.195	10.123.17.21	4	01/16/2013 18:11:05
●	URL: /index.cfm?ty=pbdetail&iid=1743			0	
●	URL: /inc/SpryTabbedPanels.js			0	
●	URL: /inc/tablesorter.css			0	
●	209.65.177.130 <--> 10.123.17.21	209.65.177.130	10.123.17.21	0	01/16/2013 18:11:03
●	10.123.55.135 <--> 10.123.17.21	10.123.55.135	10.123.17.21	1	01/16/2013 18:11:07

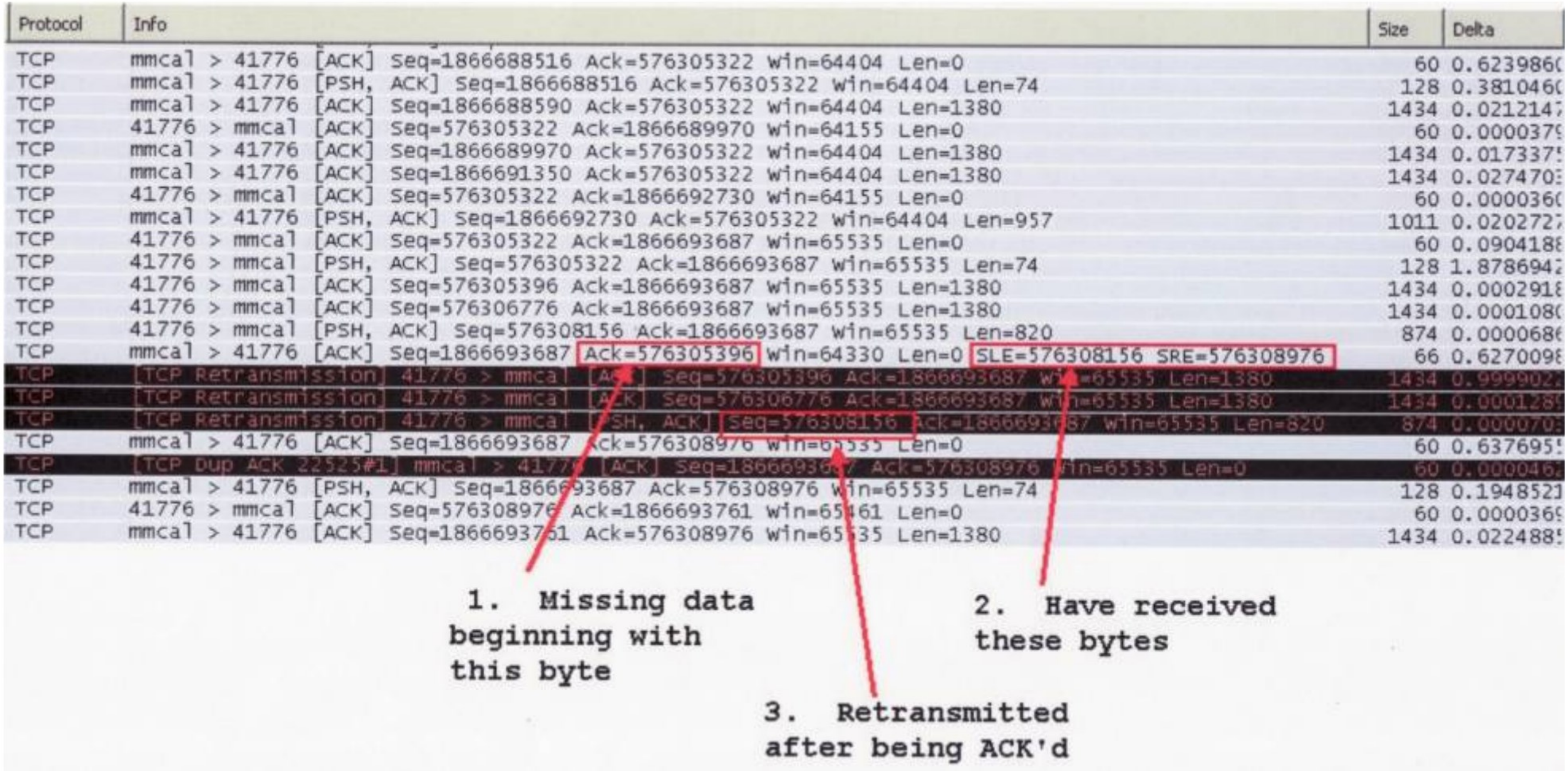
Frame #	71.82.92.195	10.123.17.21	Delta Time	Rel. Time	Len
1574107	SYN...	▶	0.000000000	0.000000000	78
1574108	◀	SYN/ACK	✓ 0.000212000	0.000212000	78
1574109	ACK...	▶	0.000457000	0.000669000	66
1574110	GET /index.cfm?ty=pbdetail&iid=1743	▶	0.000293000	0.000962000	545
1579762	◀	200 - OK	⊗ 1.457463000	1.458425000	4410
1580769	◀	Out of Sequence	0.160867000	1.619292000	4410
1581480	◀	Out of Sequence	0.086338000	1.705630000	4410
1584728	GET /inc/SpryTabbedPanels.js (Out of Sequence)	▶	0.349641000	2.055271000	595
1584741	◀	200 - OK (Out of Sequence)	0.001167000	2.056438000	451
1585058	GET /inc/tablesorter.css	▶	0.055901000	2.112339000	606
1585068	◀	200 - OK	✓ 0.000933000	2.113272000	436

Fast TCP connect time. Fast Ack from F5 does not show true client response time which is why Apalytics provided Internet Monitoring.

1.4 second Get response is very slow which is why detailed platform and application analysis was performed.

The 2nd & 3rd Gets were fast at 1 millisecond proving some commands are fast.

TCP Selective Ack Analysis



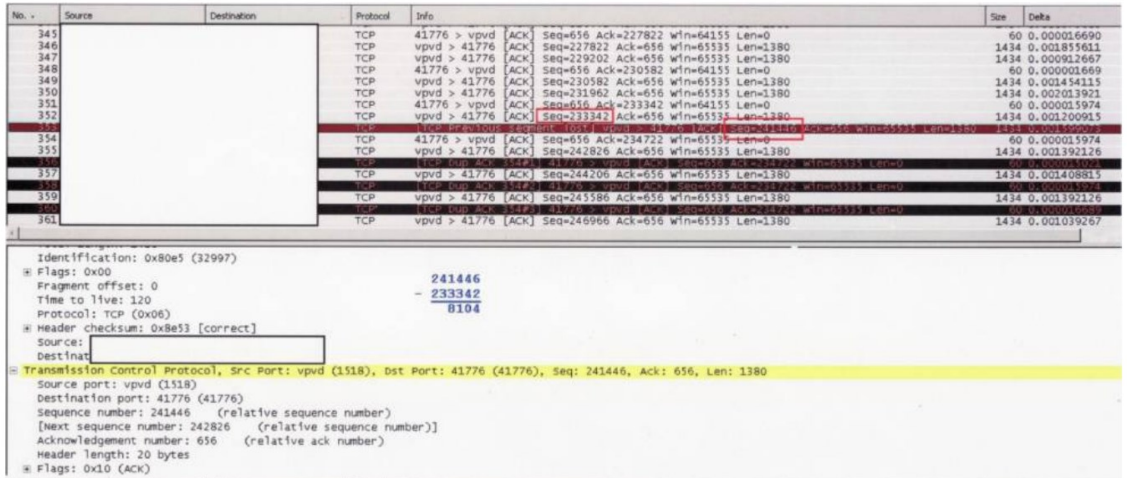
```
Protocol  Info                                                                                              Size  Delta
TCP       mmcal > 41776 [ACK] Seq=1866688516 Ack=576305322 Win=64404 Len=0                                    60  0.623986
TCP       mmcal > 41776 [PSH, ACK] Seq=1866688516 Ack=576305322 Win=64404 Len=74                             128  0.381046
TCP       mmcal > 41776 [ACK] Seq=1866688590 Ack=576305322 Win=64404 Len=1380                               1434  0.021214
TCP       41776 > mmcal [ACK] Seq=576305322 Ack=1866689970 Win=64155 Len=0                                    60  0.000037
TCP       mmcal > 41776 [ACK] Seq=1866689970 Ack=576305322 Win=64404 Len=1380                               1434  0.017337
TCP       mmcal > 41776 [ACK] Seq=1866691350 Ack=576305322 Win=64404 Len=1380                               1434  0.027470
TCP       41776 > mmcal [ACK] Seq=576305322 Ack=1866692730 Win=64155 Len=0                                    60  0.000036
TCP       mmcal > 41776 [PSH, ACK] Seq=1866692730 Ack=576305322 Win=64404 Len=957                           1011  0.020272
TCP       41776 > mmcal [ACK] Seq=576305322 Ack=1866693687 Win=65535 Len=0                                    60  0.090418
TCP       41776 > mmcal [PSH, ACK] Seq=576305322 Ack=1866693687 Win=65535 Len=74                             128  1.878694
TCP       41776 > mmcal [ACK] Seq=576305396 Ack=1866693687 Win=65535 Len=1380                               1434  0.000291
TCP       41776 > mmcal [ACK] Seq=576306776 Ack=1866693687 Win=65535 Len=1380                               1434  0.000108
TCP       41776 > mmcal [PSH, ACK] Seq=576308156 Ack=1866693687 Win=65535 Len=820                            874  0.000068
TCP       mmcal > 41776 [ACK] Seq=1866693687 Ack=576305396 Win=64330 Len=0 SLE=576308156 SRE=576308976         66  0.627009
TCP       [TCP Retransmission] 41776 > mmcal [ACK] Seq=576305396 Ack=1866693687 Win=65535 Len=1380          1434  0.999902
TCP       [TCP Retransmission] 41776 > mmcal [ACK] Seq=576306776 Ack=1866693687 Win=65535 Len=1380          1434  0.000128
TCP       [TCP Retransmission] 41776 > mmcal [PSH, ACK] Seq=576308156 Ack=1866693687 Win=65535 Len=820      874  0.000070
TCP       mmcal > 41776 [ACK] Seq=1866693687 Ack=576308976 Win=65535 Len=0                                    60  0.637695
TCP       [TCP Dup ACK 22525#1] mmcal > 41776 [ACK] Seq=1866693687 Ack=576308976 Win=65535 Len=0              60  0.000046
TCP       mmcal > 41776 [PSH, ACK] Seq=1866693687 Ack=576308976 Win=65535 Len=74                             128  0.194852
TCP       41776 > mmcal [ACK] Seq=576308976 Ack=1866693761 Win=65461 Len=0                                    60  0.000036
TCP       mmcal > 41776 [ACK] Seq=1866693761 Ack=576308976 Win=65535 Len=1380                               1434  0.022488
```

1. Missing data beginning with this byte

2. Have received these bytes

3. Retransmitted after being ACK'd

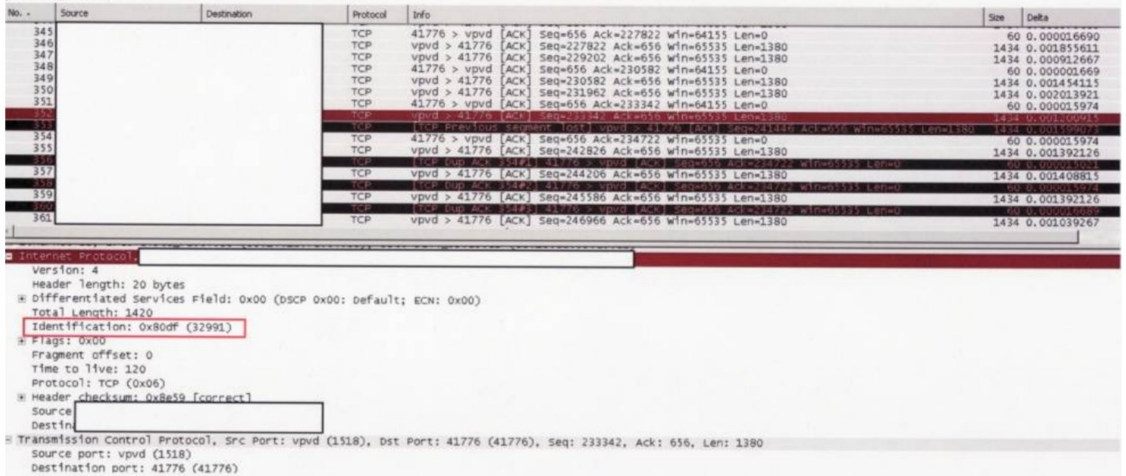
TCP / IP Manual Calculations



```
No.  Source  Destination  Protocol  Info                                                                                 Size  Delta
[redacted]
345   TCP   41776 > vpvd [ACK] Seq=656 Ack=227822 Win=64155 Len=0                                          60 0.000016690
346   TCP   vpvd > 41776 [ACK] Seq=227822 Ack=656 Win=65535 Len=1380                                     1434 0.001855611
347   TCP   vpvd > 41776 [ACK] Seq=229202 Ack=656 Win=65535 Len=1380                                     1434 0.000912667
348   TCP   41776 > vpvd [ACK] Seq=656 Ack=230582 Win=64155 Len=0                                          60 0.000001669
349   TCP   vpvd > 41776 [ACK] Seq=230582 Ack=656 Win=65535 Len=1380                                     1434 0.001454115
350   TCP   vpvd > 41776 [ACK] Seq=231962 Ack=656 Win=65535 Len=1380                                     1434 0.002013921
351   TCP   41776 > vpvd [ACK] Seq=656 Ack=233342 Win=64155 Len=0                                          60 0.000015974
352   TCP   vpvd > 41776 [ACK] Seq=233342 Ack=656 Win=65535 Len=1380                                     1434 0.001200915
353   TCP   [TCP Previous segment lost] vpvd > 41776 [ACK] Seq=241446 Ack=656 Win=65535 Len=1380         1434 0.001599073
354   TCP   41776 > vpvd [ACK] Seq=656 Ack=234722 Win=65535 Len=0                                          60 0.000015974
355   TCP   vpvd > 41776 [ACK] Seq=242826 Ack=656 Win=65535 Len=1380                                     1434 0.001392126
356   TCP   [TCP Dup ACK 354#1] 41776 > vpvd [ACK] Seq=656 Ack=234722 Win=65535 Len=0                     60 0.000015021
357   TCP   vpvd > 41776 [ACK] Seq=244206 Ack=656 Win=65535 Len=1380                                     1434 0.001408815
358   TCP   [TCP Dup ACK 354#2] 41776 > vpvd [ACK] Seq=656 Ack=234722 Win=65535 Len=0                     60 0.000015974
359   TCP   vpvd > 41776 [ACK] Seq=245586 Ack=656 Win=65535 Len=1380                                     1434 0.001392126
360   TCP   [TCP Dup ACK 354#3] 41776 > vpvd [ACK] Seq=656 Ack=234722 Win=65535 Len=0                     60 0.000016689
361   TCP   vpvd > 41776 [ACK] Seq=246966 Ack=656 Win=65535 Len=1380                                     1434 0.001039267
```

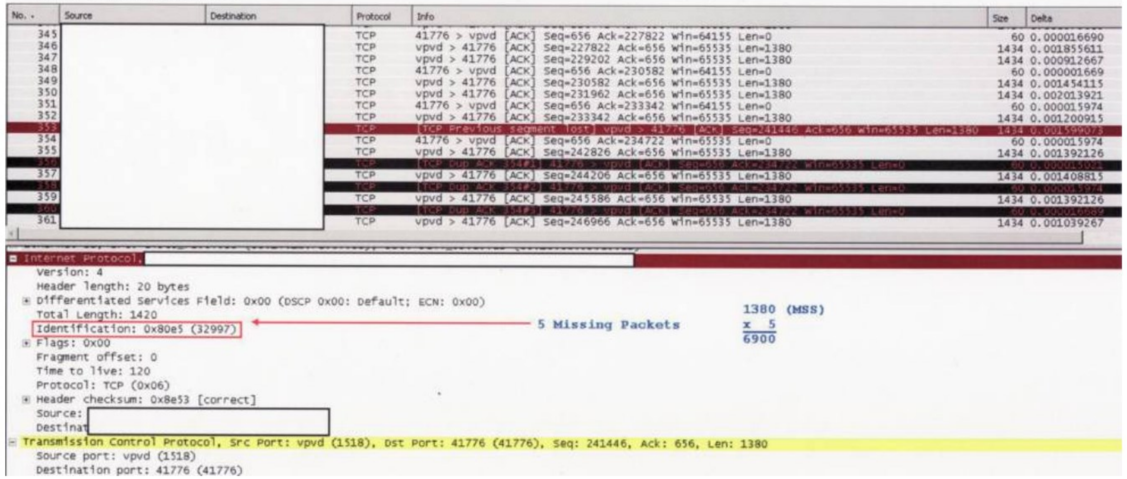
```
    Identification: 0x80e5 (32997)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 120
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0x8e53 [correct]
    Source: [redacted]
    Destinat[redacted]
⊟ Transmission Control Protocol, Src Port: vpvd (1518), Dst Port: 41776 (41776), Seq: 241446, Ack: 656, Len: 1380
    Source port: vpvd (1518)
    Destination port: 41776 (41776)
    Sequence number: 241446    (relative sequence number)
    [Next sequence number: 242826    (relative sequence number)]
    Acknowledgement number: 656    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
```

$$\begin{array}{r} 241446 \\ -\ \underline{233342} \\ 8104 \end{array}$$



```
No.  Source  Destination  Protocol  Info                                                                                 Size  Delta
[redacted]
345   TCP   41776 > vpvd [ACK] Seq=656 Ack=227822 Win=64155 Len=0                                          60 0.000016690
346   TCP   vpvd > 41776 [ACK] Seq=227822 Ack=656 Win=65535 Len=1380                                     1434 0.001855611
347   TCP   vpvd > 41776 [ACK] Seq=229202 Ack=656 Win=65535 Len=1380                                     1434 0.000912667
348   TCP   41776 > vpvd [ACK] Seq=656 Ack=230582 Win=64155 Len=0                                          60 0.000001669
349   TCP   vpvd > 41776 [ACK] Seq=230582 Ack=656 Win=65535 Len=1380                                     1434 0.001454115
350   TCP   vpvd > 41776 [ACK] Seq=231962 Ack=656 Win=65535 Len=1380                                     1434 0.002013921
351   TCP   41776 > vpvd [ACK] Seq=656 Ack=233342 Win=64155 Len=0                                          60 0.000015974
352   TCP   vpvd > 41776 [ACK] Seq=233342 Ack=656 Win=65535 Len=1380                                     1434 0.001200915
353   TCP   [TCP Previous segment lost] vpvd > 41776 [ACK] Seq=241446 Ack=656 Win=65535 Len=1380         1434 0.001599073
354   TCP   41776 > vpvd [ACK] Seq=656 Ack=234722 Win=65535 Len=0                                          60 0.000015974
355   TCP   vpvd > 41776 [ACK] Seq=242826 Ack=656 Win=65535 Len=1380                                     1434 0.001392126
356   TCP   [TCP Dup ACK 354#1] 41776 > vpvd [ACK] Seq=656 Ack=234722 Win=65535 Len=0                     60 0.000015021
357   TCP   vpvd > 41776 [ACK] Seq=244206 Ack=656 Win=65535 Len=1380                                     1434 0.001408815
358   TCP   [TCP Dup ACK 354#2] 41776 > vpvd [ACK] Seq=656 Ack=234722 Win=65535 Len=0                     60 0.000015974
359   TCP   vpvd > 41776 [ACK] Seq=245586 Ack=656 Win=65535 Len=1380                                     1434 0.001392126
360   TCP   [TCP Dup ACK 354#3] 41776 > vpvd [ACK] Seq=656 Ack=234722 Win=65535 Len=0                     60 0.000016689
361   TCP   vpvd > 41776 [ACK] Seq=246966 Ack=656 Win=65535 Len=1380                                     1434 0.001039267
```

```
⊟ Internet Protocol, [redacted]
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 1420
    Identification: 0x80df (32991)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 120
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0x8e59 [correct]
    Source[redacted]
    Destin[redacted]
⊟ Transmission Control Protocol, Src Port: vpvd (1518), Dst Port: 41776 (41776), Seq: 233342, Ack: 656, Len: 1380
    Source port: vpvd (1518)
    Destination port: 41776 (41776)
```



```
No.  Source  Destination  Protocol  Info                                                                                 Size  Delta
[redacted]
345   TCP   41776 > vpvd [ACK] Seq=656 Ack=227822 Win=64155 Len=0                                          60 0.000016690
346   TCP   vpvd > 41776 [ACK] Seq=227822 Ack=656 Win=65535 Len=1380                                     1434 0.001855611
347   TCP   vpvd > 41776 [ACK] Seq=229202 Ack=656 Win=65535 Len=1380                                     1434 0.000912667
348   TCP   41776 > vpvd [ACK] Seq=656 Ack=230582 Win=64155 Len=0                                          60 0.000001669
349   TCP   vpvd > 41776 [ACK] Seq=230582 Ack=656 Win=65535 Len=1380                                     1434 0.001454115
350   TCP   vpvd > 41776 [ACK] Seq=231962 Ack=656 Win=65535 Len=1380                                     1434 0.002013921
351   TCP   41776 > vpvd [ACK] Seq=656 Ack=233342 Win=64155 Len=0                                          60 0.000015974
352   TCP   vpvd > 41776 [ACK] Seq=233342 Ack=656 Win=65535 Len=1380                                     1434 0.001200915
353   TCP   [TCP Previous segment lost] vpvd > 41776 [ACK] Seq=241446 Ack=656 Win=65535 Len=1380         1434 0.001599073
354   TCP   41776 > vpvd [ACK] Seq=656 Ack=234722 Win=65535 Len=0                                          60 0.000015974
355   TCP   vpvd > 41776 [ACK] Seq=242826 Ack=656 Win=65535 Len=1380                                     1434 0.001392126
356   TCP   [TCP Dup ACK 354#1] 41776 > vpvd [ACK] Seq=656 Ack=234722 Win=65535 Len=0                     60 0.000015021
357   TCP   vpvd > 41776 [ACK] Seq=244206 Ack=656 Win=65535 Len=1380                                     1434 0.001408815
358   TCP   [TCP Dup ACK 354#2] 41776 > vpvd [ACK] Seq=656 Ack=234722 Win=65535 Len=0                     60 0.000015974
359   TCP   vpvd > 41776 [ACK] Seq=245586 Ack=656 Win=65535 Len=1380                                     1434 0.001392126
360   TCP   [TCP Dup ACK 354#3] 41776 > vpvd [ACK] Seq=656 Ack=234722 Win=65535 Len=0                     60 0.000016689
361   TCP   vpvd > 41776 [ACK] Seq=246966 Ack=656 Win=65535 Len=1380                                     1434 0.001039267
```

```
⊟ Internet Protocol, [redacted]
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 1420
    Identification: 0x80e5 (32997)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 120
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0x8e53 [correct]
    Source: [redacted]
    Destinat[redacted]
⊟ Transmission Control Protocol, Src Port: vpvd (1518), Dst Port: 41776 (41776), Seq: 241446, Ack: 656, Len: 1380
    Source port: vpvd (1518)
    Destination port: 41776 (41776)
```

$$\begin{array}{r} 1380\ \text{(MSS)} \\ \underline{x\ \ 5} \\ 6900 \end{array}$$

Citrix Analysis

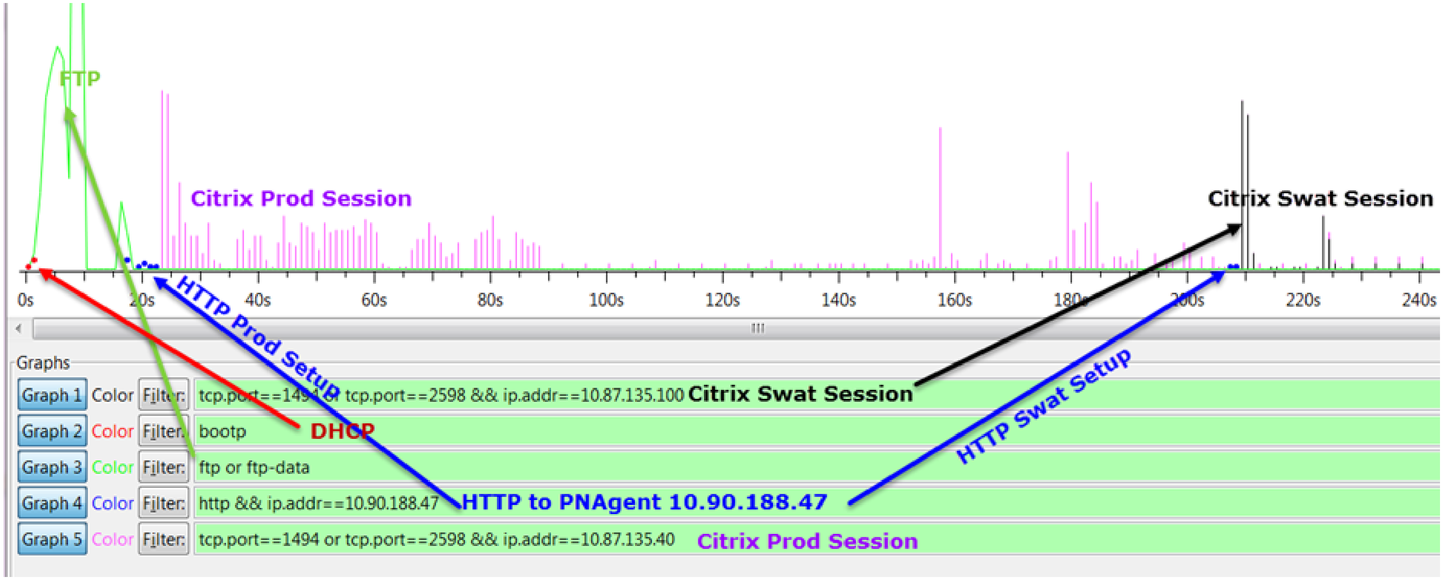
Technical Lessons Learned Training

1. How Citrix Wyse Terminals Boot in the Client Environment

The steps outlined and the timings of each step. This helps you understand so you can troubleshoot a problem with a step.

Wyse Terminal Boot Dependencies & Sequence Steps

Time	Step
1 Second	DHCP
0 Seconds	ARP (ARPs continue every 60 seconds regardless of usage)
14 Seconds	FTP 10 Files downloaded.
.035 Seconds	DNS
5 Seconds	HTTP to PNAgent (CI Prod Desktop)
.5 Second	Citrix 2598 to 10.87.135.40
184 Seconds	Session init / including unknown user wait time going to Swat Desktop
1.35 Second	Citrix 2598 to 10.87.135.100
209 Seconds	Begin Swat Session



Graph 1 Color Filter: tcp.port==1494 or tcp.port==2598 && ip.addr==10.87.135.100

Graph 2 Color Filter: bootp

Graph 3 Color Filter: ftp or ftp-data

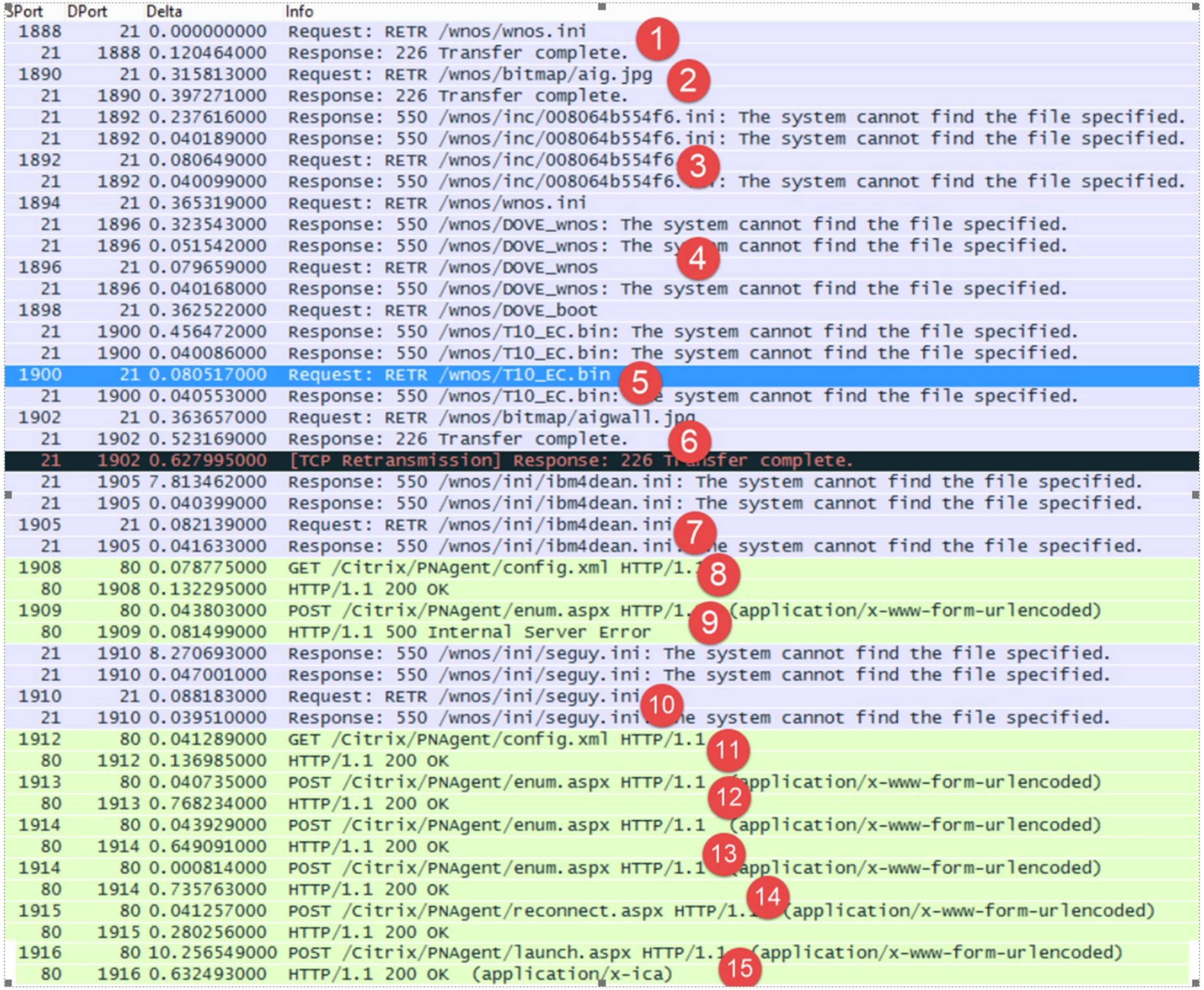
Graph 4 Color Filter: http && ip.addr==10.90.188.47

Graph 5 Color Filter: tcp.port==1494 or tcp.port==2598 && ip.addr==10.87.135.40

1a1 How Citrix Wyse Terminals Boot in the Client Environment Packet by packet.

Here are the packets that go along with the chart and the step in the previous slide.

I am going over the boot sequence and the wnos.ini syntax and steps.

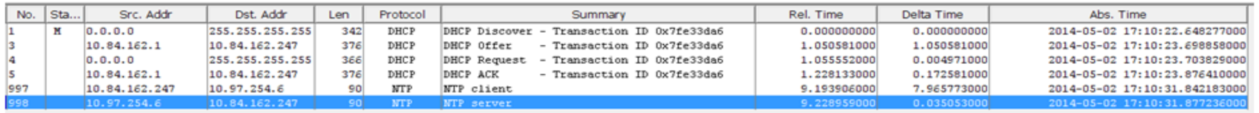


```
SPort DPort Delta       Info
 1888    21 0.000000000 Request: RETR /wnos/wnos.ini
   21  1888 0.120464000 Response: 226 Transfer complete.
 1890    21 0.315813000 Request: RETR /wnos/bitmap/aig.jpg
   21  1890 0.397271000 Response: 226 Transfer complete.
   21  1892 0.237616000 Response: 550 /wnos/inc/008064b554f6.ini: The system cannot find the file specified.
   21  1892 0.040189000 Response: 550 /wnos/inc/008064b554f6.ini: The system cannot find the file specified.
 1892    21 0.080649000 Request: RETR /wnos/inc/008064b554f6
   21  1892 0.040099000 Response: 550 /wnos/inc/008064b554f6.   : The system cannot find the file specified.
 1894    21 0.365319000 Request: RETR /wnos/wnos.ini
   21  1896 0.323543000 Response: 550 /wnos/DOVE_wnos: The system cannot find the file specified.
   21  1896 0.051542000 Response: 550 /wnos/DOVE_wnos: The sy   m cannot find the file specified.
 1896    21 0.079659000 Request: RETR /wnos/DOVE_wnos
   21  1896 0.040168000 Response: 550 /wnos/DOVE_wnos: The system cannot find the file specified.
 1898    21 0.362522000 Request: RETR /wnos/DOVE_boot
   21  1900 0.456472000 Response: 550 /wnos/T10_EC.bin: The system cannot find the file specified.
   21  1900 0.040086000 Response: 550 /wnos/T10_EC.bin: The system cannot find the file specified.
 1900    21 0.080517000 Request: RETR /wnos/T10_EC.bin
   21  1900 0.040553000 Response: 550 /wnos/T10_EC.bin:   e system cannot find the file specified.
 1902    21 0.363657000 Request: RETR /wnos/bitmap/aigwall.jpg
   21  1902 0.523169000 Response: 226 Transfer complete.
   21  1902 0.627995000 [TCP Retransmission] Response: 226 Tr  nsfer complete.
   21  1905 7.813462000 Response: 550 /wnos/ini/ibm4dean.ini: The system cannot find the file specified.
   21  1905 0.040399000 Response: 550 /wnos/ini/ibm4dean.ini: The system cannot find the file specified.
 1905    21 0.082139000 Request: RETR /wnos/ini/ibm4dean.ini
   21  1905 0.041633000 Response: 550 /wnos/ini/ibm4dean.ini   he system cannot find the file specified.
 1908    80 0.078775000 GET /Citrix/PNAgent/config.xml HTTP/1.
   80  1908 0.132295000 HTTP/1.1 200 OK
 1909    80 0.043803000 POST /Citrix/PNAgent/enum.aspx HTTP/1.   (application/x-www-form-urlencoded)
   80  1909 0.081499000 HTTP/1.1 500 Internal Server Error
   21  1910 8.270693000 Response: 550 /wnos/ini/seguy.ini: The system cannot find the file specified.
   21  1910 0.047001000 Response: 550 /wnos/ini/seguy.ini: The system cannot find the file specified.
 1910    21 0.088183000 Request: RETR /wnos/ini/seguy.ini
   21  1910 0.039510000 Response: 550 /wnos/ini/seguy.ini   he system cannot find the file specified.
 1912    80 0.041289000 GET /Citrix/PNAgent/config.xml HTTP/1.1
   80  1912 0.136985000 HTTP/1.1 200 OK
 1913    80 0.040735000 POST /Citrix/PNAgent/enum.aspx HTTP/1.1   pplication/x-www-form-urlencoded)
   80  1913 0.768234000 HTTP/1.1 200 OK
 1914    80 0.043929000 POST /Citrix/PNAgent/enum.aspx HTTP/1.1  (application/x-www-form-urlencoded)
   80  1914 0.649091000 HTTP/1.1 200 OK
 1914    80 0.000814000 POST /Citrix/PNAgent/enum.aspx HTTP/1.1 (application/x-www-form-urlencoded)
   80  1914 0.735763000 HTTP/1.1 200 OK
 1915    80 0.041257000 POST /Citrix/PNAgent/reconnect.aspx HTTP/1.  (application/x-www-form-urlencoded)
   80  1915 0.280256000 HTTP/1.1 200 OK
 1916    80 10.256549000 POST /Citrix/PNAgent/launch.aspx HTTP/1.1  (application/x-www-form-urlencoded)
   80  1916 0.632493000 HTTP/1.1 200 OK  (application/x-ica)
```

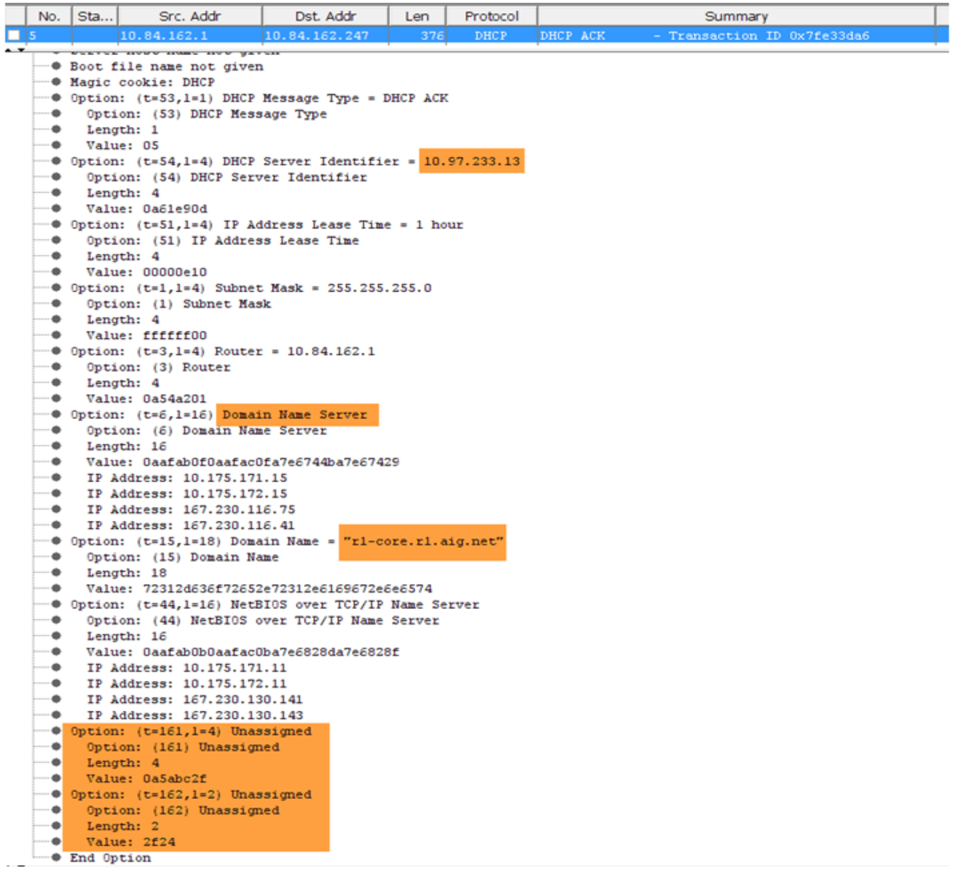
2. How Citrix Wyse Terminals Boot in the Client Environment

DHCP and NTP steps

DHCP & NTP (Network Time)

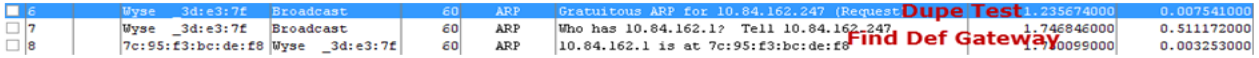


No.	Sta...	Src. Addr	Dst. Addr	Len	Protocol	Summary	Rel. Time	Delta Time	Abs. Time
1	M	0.0.0.0	255.255.255.255	342	DHCP	DHCP Discover - Transaction ID 0x7fe33da6	0.000000000	0.000000000	2014-05-02 17:10:22.648277000
3		10.84.162.1	10.84.162.247	376	DHCP	DHCP Offer - Transaction ID 0x7fe33da6	1.050581000	1.050581000	2014-05-02 17:10:23.698858000
4		0.0.0.0	255.255.255.255	366	DHCP	DHCP Request - Transaction ID 0x7fe33da6	1.055552000	0.004971000	2014-05-02 17:10:23.703829000
5		10.84.162.1	10.84.162.247	376	DHCP	DHCP ACK - Transaction ID 0x7fe33da6	1.228133000	0.172581000	2014-05-02 17:10:23.876410000
997		10.84.162.247	10.97.254.6	90	NTP	NTP client	9.193906000	7.965773000	2014-05-02 17:10:31.842183000
998		10.97.254.6	10.84.162.247	90	NTP	NTP server	9.228959000	0.035053000	2014-05-02 17:10:31.877236000



	No.	Sta...	Src. Addr	Dst. Addr	Len	Protocol	Summary
□	5		10.84.162.1	10.84.162.247	376	DHCP	DHCP ACK - Transaction ID 0x7fe33da6

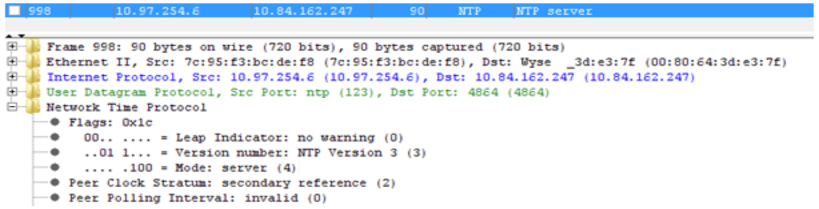
```
● Boot file name not given
● Magic cookie: DHCP
● Option: (t=53,l=1) DHCP Message Type = DHCP ACK
●   Option: (53) DHCP Message Type
●   Length: 1
●   Value: 05
● Option: (t=54,l=4) DHCP Server Identifier = 10.97.233.13
●   Option: (54) DHCP Server Identifier
●   Length: 4
●   Value: 0a61e90d
● Option: (t=51,l=4) IP Address Lease Time = 1 hour
●   Option: (51) IP Address Lease Time
●   Length: 4
●   Value: 00000e10
● Option: (t=1,l=4) Subnet Mask = 255.255.255.0
●   Option: (1) Subnet Mask
●   Length: 4
●   Value: ffffff00
● Option: (t=3,l=4) Router = 10.84.162.1
●   Option: (3) Router
●   Length: 4
●   Value: 0a54a201
● Option: (t=6,l=16) Domain Name Server
●   Option: (6) Domain Name Server
●   Length: 16
●   Value: 0aafab0f0aafac0fa7e6744ba7e67429
●   IP Address: 10.175.171.15
●   IP Address: 10.175.172.15
●   IP Address: 167.230.116.75
●   IP Address: 167.230.116.41
● Option: (t=15,l=18) Domain Name = "r1-core.r1.aig.net"
●   Option: (15) Domain Name
●   Length: 18
●   Value: 72312d636f72652e72312e6169672e6e6574
● Option: (t=44,l=16) NetBIOS over TCP/IP Name Server
●   Option: (44) NetBIOS over TCP/IP Name Server
●   Length: 16
●   Value: 0aafab0b0aafac0ba7e6828da7e6828f
●   IP Address: 10.175.171.11
●   IP Address: 10.175.172.11
●   IP Address: 167.230.130.141
●   IP Address: 167.230.130.143
● Option: (t=161,l=4) Unassigned
●   Option: (161) Unassigned
●   Length: 4
●   Value: 0a5abc2f
● Option: (t=162,l=2) Unassigned
●   Option: (162) Unassigned
●   Length: 2
●   Value: 2f24
● End Option
```



□	6		Wyse _3d:e3:7f	Broadcast	60	ARP	Gratuitous ARP for 10.84.162.247 (Request	1.235674000	0.007541000
□	7		Wyse _3d:e3:7f	Broadcast	60	ARP	Who has 10.84.162.1? Tell 10.84.162.247	1.746846000	0.511172000
□	8		7c:95:f3:bc:de:f8	Wyse _3d:e3:7f	60	ARP	10.84.162.1 is at 7c:95:f3:bc:de:f8	1.7[illegible]0099000	0.003253000

Dupe Test

Find Def Gateway

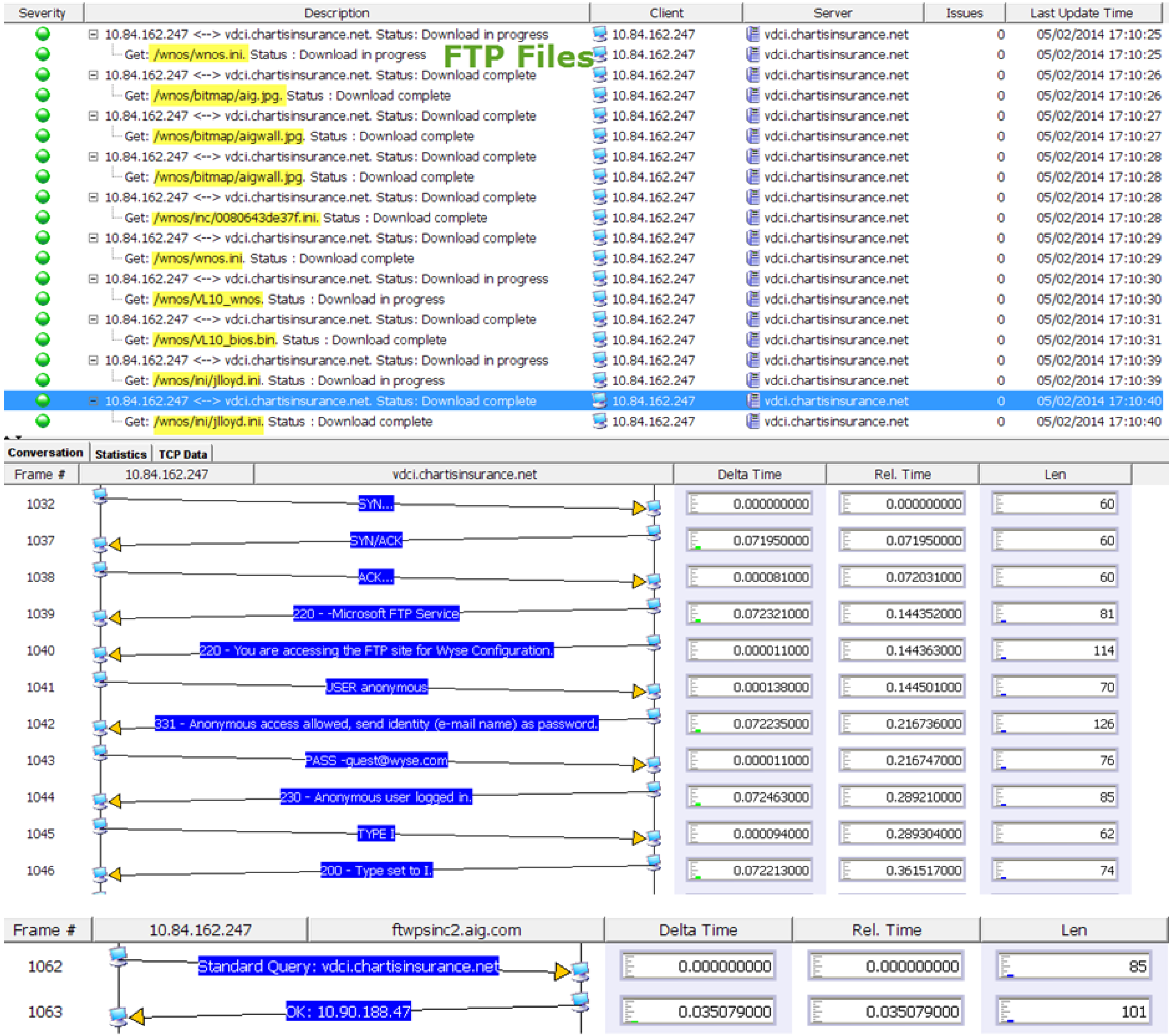


	No.	Sta...	Src. Addr	Dst. Addr	Len	Protocol	Summary
□	998		10.97.254.6	10.84.162.247	90	NTP	NTP server

```
⊞ Frame 998: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
⊞ Ethernet II, Src: 7c:95:f3:bc:de:f8 (7c:95:f3:bc:de:f8), Dst: Wyse _3d:e3:7f (00:80:64:3d:e3:7f)
⊞ Internet Protocol, Src: 10.97.254.6 (10.97.254.6), Dst: 10.84.162.247 (10.84.162.247)
⊞ User Datagram Protocol, Src Port: ntp (123), Dst Port: 4864 (4864)
⊟ Network Time Protocol
   ● Flags: 0x1c
   ●   00.. .... = Leap Indicator: no warning (0)
   ●   ..01 1... = Version number: NTP Version 3 (3)
   ●   .... .100 = Mode: server (4)
   ● Peer Clock Stratum: secondary reference (2)
   ● Peer Polling Interval: invalid (0)
```

3. How Citrix Wyse Terminals Boot in the Client Environment

FTP steps



FTP Files

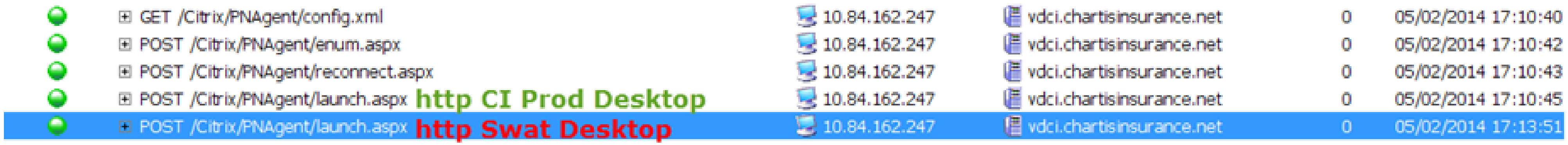
Severity	Description	Client	Server	Issues	Last Update Time
●	⊟ 10.84.162.247 <--> vdci.chartisinsurance.net. Status: Download in progress	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:25
●	Get: /wnos/wnos.ini. Status : Download in progress	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:25
●	⊟ 10.84.162.247 <--> vdci.chartisinsurance.net. Status: Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:26
●	Get: /wnos/bitmap/aig.jpg. Status : Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:26
●	⊟ 10.84.162.247 <--> vdci.chartisinsurance.net. Status: Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:27
●	Get: /wnos/bitmap/aigwall.jpg. Status : Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:27
●	⊟ 10.84.162.247 <--> vdci.chartisinsurance.net. Status: Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:28
●	Get: /wnos/bitmap/aigwall.jpg. Status : Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:28
●	⊟ 10.84.162.247 <--> vdci.chartisinsurance.net. Status: Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:28
●	Get: /wnos/inc/0080643de37f.ini. Status : Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:28
●	⊟ 10.84.162.247 <--> vdci.chartisinsurance.net. Status: Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:29
●	Get: /wnos/wnos.ini. Status : Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:29
●	⊟ 10.84.162.247 <--> vdci.chartisinsurance.net. Status: Download in progress	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:30
●	Get: /wnos/VL10_wnos. Status : Download in progress	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:30
●	⊟ 10.84.162.247 <--> vdci.chartisinsurance.net. Status: Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:31
●	Get: /wnos/VL10_bios.bin. Status : Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:31
●	⊟ 10.84.162.247 <--> vdci.chartisinsurance.net. Status: Download in progress	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:39
●	Get: /wnos/ini/jlloyd.ini. Status : Download in progress	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:39
●	⊟ 10.84.162.247 <--> vdci.chartisinsurance.net. Status: Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:40
●	Get: /wnos/ini/jlloyd.ini. Status : Download complete	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:40

Frame #	10.84.162.247	vdci.chartisinsurance.net	Delta Time	Rel. Time	Len
1032		SYN...	0.000000000	0.000000000	60
1037		SYN/ACK	0.071950000	0.071950000	60
1038		ACK...	0.000081000	0.072031000	60
1039		220 - -Microsoft FTP Service	0.072321000	0.144352000	81
1040		220 - You are accessing the FTP site for Wyse Configuration.	0.000011000	0.144363000	114
1041		USER anonymous	0.000138000	0.144501000	70
1042		331 - Anonymous access allowed, send identity (e-mail name) as password.	0.072235000	0.216736000	126
1043		PASS -guest@wyse.com	0.000011000	0.216747000	76
1044		230 - Anonymous user logged in.	0.072463000	0.289210000	85
1045		TYPE I	0.000094000	0.289304000	62
1046		200 - Type set to I.	0.072213000	0.361517000	74

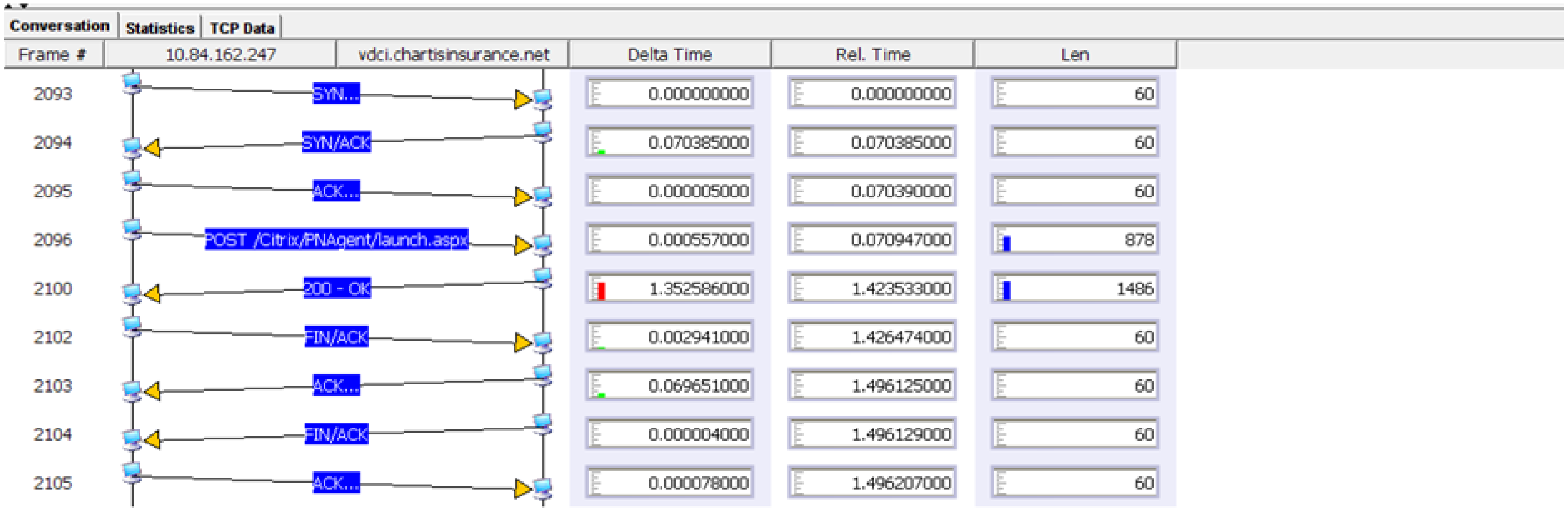
Frame #	10.84.162.247	ftwpsinc2.aig.com	Delta Time	Rel. Time	Len
1062		Standard Query: vdci.chartisinsurance.net	0.000000000	0.000000000	85
1063		OK: 10.90.188.47	0.035079000	0.035079000	101

4. How Citrix Wyse Terminals Boot in the Client Environment

HTTP Steps



●	⊞ GET /Citrix/PNAgent/config.xml	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:40
●	⊞ POST /Citrix/PNAgent/enum.aspx	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:42
●	⊞ POST /Citrix/PNAgent/reconnect.aspx	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:43
●	⊞ POST /Citrix/PNAgent/launch.aspx **http CI Prod Desktop**	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:10:45
●	⊞ POST /Citrix/PNAgent/launch.aspx **http Swat Desktop**	10.84.162.247	vdci.chartisinsurance.net	0	05/02/2014 17:13:51

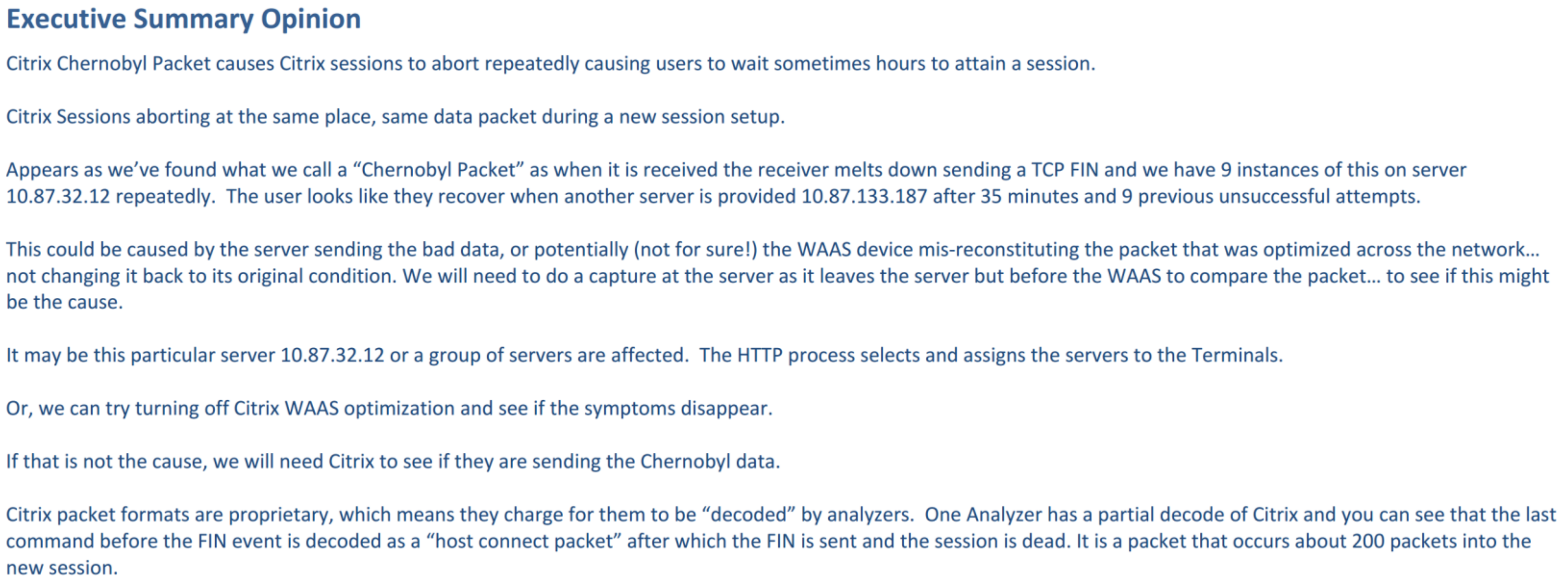


Frame #	10.84.162.247	vdci.chartisinsurance.net	Delta Time	Rel. Time	Len
2093	SYN... →		0.000000000	0.000000000	60
2094		← SYN/ACK	0.070385000	0.070385000	60
2095	ACK... →		0.000005000	0.070390000	60
2096	POST /Citrix/PNAgent/launch.aspx →		0.000557000	0.070947000	878
2100		← 200 - OK	1.352586000	1.423533000	1486
2102	FIN/ACK →		0.002941000	1.426474000	60
2103		← ACK...	0.069651000	1.496125000	60
2104		← FIN/ACK	0.000004000	1.496129000	60
2105	ACK... →		0.000078000	1.496207000	60

1. Citrix Session Abort Signature “Chernobyl Packet”

The packet that evidenced a problem on a Citrix server. This pattern was used as a signature on the Infinistream Sniffers to find these problems until they were remediated.

Prior to this users were stuck in this cycle for hours.



Executive Summary Opinion

Citrix Chernobyl Packet causes Citrix sessions to abort repeatedly causing users to wait sometimes hours to attain a session.

Citrix Sessions aborting at the same place, same data packet during a new session setup.

Appears as we’ve found what we call a “Chernobyl Packet” as when it is received the receiver melts down sending a TCP FIN and we have 9 instances of this on server 10.87.32.12 repeatedly. The user looks like they recover when another server is provided 10.87.133.187 after 35 minutes and 9 previous unsuccessful attempts.

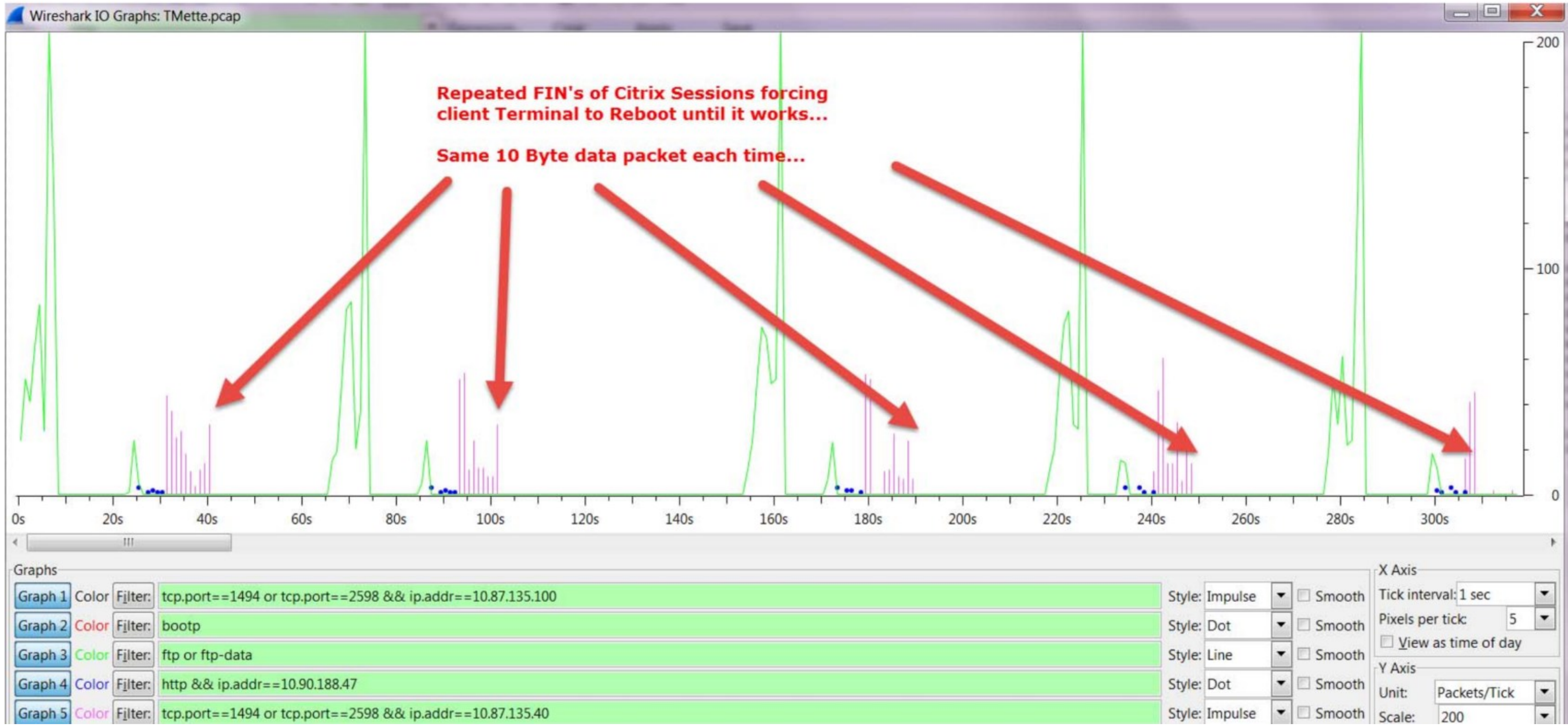
This could be caused by the server sending the bad data, or potentially (not for sure!) the WAAS device mis-reconstituting the packet that was optimized across the network… not changing it back to its original condition. We will need to do a capture at the server as it leaves the server but before the WAAS to compare the packet… to see if this might be the cause.

It may be this particular server 10.87.32.12 or a group of servers are affected. The HTTP process selects and assigns the servers to the Terminals.

Or, we can try turning off Citrix WAAS optimization and see if the symptoms disappear.

If that is not the cause, we will need Citrix to see if they are sending the Chernobyl data.

Citrix packet formats are proprietary, which means they charge for them to be “decoded” by analyzers. One Analyzer has a partial decode of Citrix and you can see that the last command before the FIN event is decoded as a “host connect packet” after which the FIN is sent and the session is dead. It is a packet that occurs about 200 packets into the new session.



Repeated FIN's of Citrix Sessions forcing client Terminal to Reboot until it works…

Same 10 Byte data packet each time…

Graph 1 Color Filter: tcp.port==1494 or tcp.port==2598 && ip.addr==10.87.135.100 Style: Impulse □ Smooth

Graph 2 Color Filter: bootp Style: Dot □ Smooth

Graph 3 Color Filter: ftp or ftp-data Style: Line □ Smooth

Graph 4 Color Filter: http && ip.addr==10.90.188.47 Style: Dot □ Smooth

Graph 5 Color Filter: tcp.port==1494 or tcp.port==2598 && ip.addr==10.87.135.40 Style: Impulse □ Smooth

Tick interval: 1 sec

Pixels per tick: 5

□ View as time of day

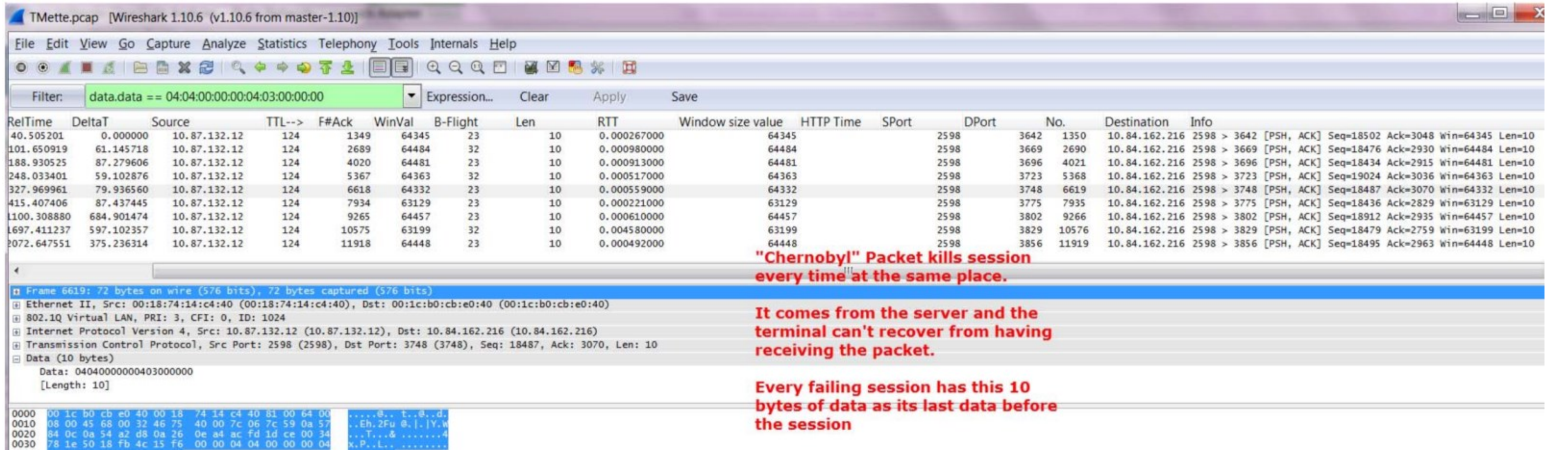
Unit: Packets/Tick

Scale: 200

2. Citrix Session Abort Signature “Chernobyl Packet”

Signature details to use to build a filter to find these complex problems.

This allowed rapid remediation until a solution could be found to fix the problem.



TMette.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

Filter: data.data == 04:04:00:00:00:04:03:00:00:00

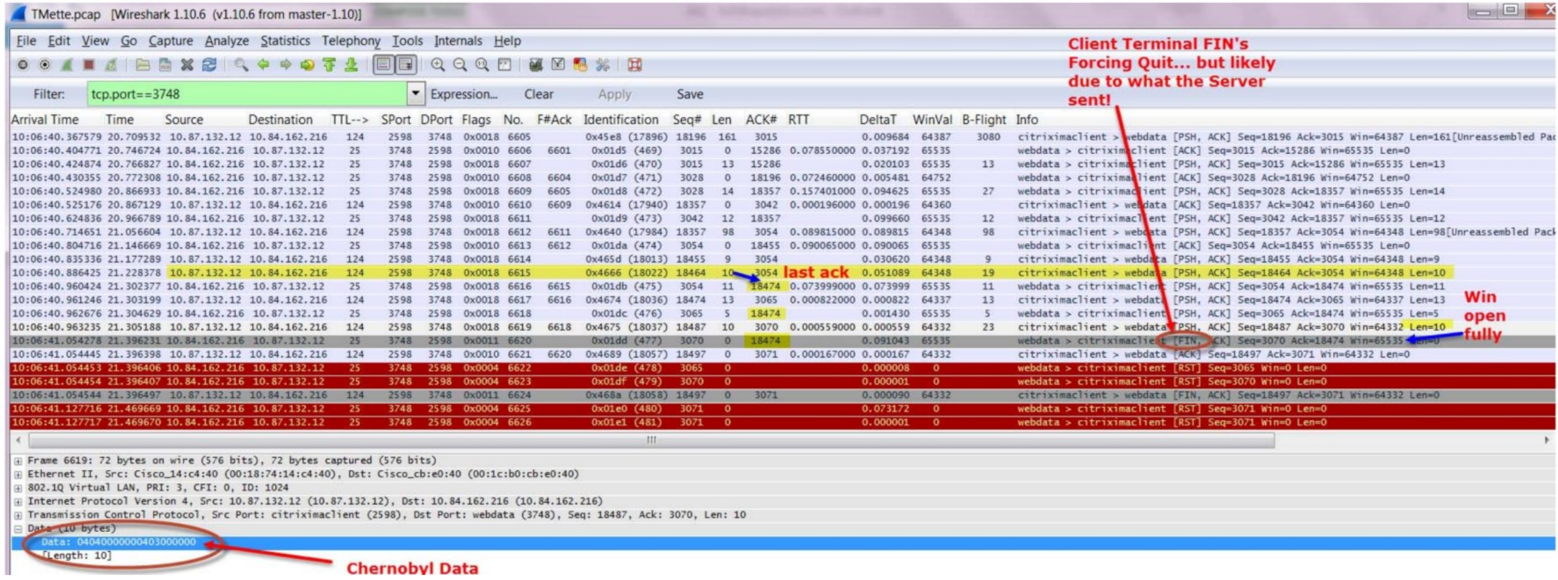
```
RelTime      DeltaT      Source        TTL-->  F#Ack  WinVal  B-Flight  Len  RTT          Window size value  HTTP Time  SPort  DPort  No.    Destination    Info
40.505201      0.000000  10.87.132.12  124      1349  64345   23        10   0.000267000  64345                         2598   3642   1350   10.84.162.216  2598 > 3642 [PSH, ACK] Seq=18502 Ack=3048 Win=64345 Len=10
101.650919    61.145718  10.87.132.12  124      2689  64484   32        10   0.000980000  64484                         2598   3669   2690   10.84.162.216  2598 > 3669 [PSH, ACK] Seq=18476 Ack=2930 Win=64484 Len=10
188.930525    87.279606  10.87.132.12  124      4020  64481   23        10   0.000913000  64481                         2598   3696   4021   10.84.162.216  2598 > 3696 [PSH, ACK] Seq=18434 Ack=2915 Win=64481 Len=10
248.033401    59.102876  10.87.132.12  124      5367  64363   32        10   0.000517000  64363                         2598   3723   5368   10.84.162.216  2598 > 3723 [PSH, ACK] Seq=19024 Ack=3036 Win=64363 Len=10
327.969961    79.936560  10.87.132.12  124      6618  64332   23        10   0.000559000  64332                         2598   3748   6619   10.84.162.216  2598 > 3748 [PSH, ACK] Seq=18487 Ack=3070 Win=64332 Len=10
415.407406    87.437445  10.87.132.12  124      7934  63129   23        10   0.000221000  63129                         2598   3775   7935   10.84.162.216  2598 > 3775 [PSH, ACK] Seq=18436 Ack=2829 Win=63129 Len=10
1100.308880  684.901474  10.87.132.12  124      9265  64457   23        10   0.000610000  64457                         2598   3802   9266   10.84.162.216  2598 > 3802 [PSH, ACK] Seq=18912 Ack=2935 Win=64457 Len=10
1697.411237  597.102357  10.87.132.12  124     10575  63199   32        10   0.004580000  63199                         2598   3829   10576  10.84.162.216  2598 > 3829 [PSH, ACK] Seq=18479 Ack=2759 Win=63199 Len=10
2072.647551  375.236314  10.87.132.12  124     11918  64448   23        10   0.000492000  64448                         2598   3856   11919  10.84.162.216  2598 > 3856 [PSH, ACK] Seq=18495 Ack=2963 Win=64448 Len=10
```

```
⊞ Frame 6619: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
⊞ Ethernet II, Src: 00:18:74:14:c4:40 (00:18:74:14:c4:40), Dst: 00:1c:b0:cb:e0:40 (00:1c:b0:cb:e0:40)
⊞ 802.1Q Virtual LAN, PRI: 3, CFI: 0, ID: 1024
⊞ Internet Protocol Version 4, Src: 10.87.132.12 (10.87.132.12), Dst: 10.84.162.216 (10.84.162.216)
⊞ Transmission Control Protocol, Src Port: 2598 (2598), Dst Port: 3748 (3748), Seq: 18487, Ack: 3070, Len: 10
⊟ Data (10 bytes)
    Data: 04040000000403000000
    [Length: 10]

0000  00 1c b0 cb e0 40 00 18  74 14 c4 40 81 00 64 00   .....@.. t..@..d.
0010  08 00 45 68 00 32 46 75  40 00 7c 06 7c 59 0a 57   ..Eh.2Fu @.|.|Y.W
0020  84 0c 0a 54 a2 d8 0a 26  0e a4 ac fd 1d ce 00 34   ...T...& .......4
0030  78 1e 50 18 fb 4c 15 f6  00 00 04 04 00 00 00 04   x.P..L.. ........
```

"Chernobyl" Packet kills session every time at the same place.

It comes from the server and the terminal can't recover from having receiving the packet.

Every failing session has this 10 bytes of data as its last data before the session



TMette.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

Filter: tcp.port==3748

```
Arrival Time       Time      Source         Destination    TTL--> SPort DPort Flags  No.  F#Ack Identification Seq#  Len ACK#  RTT         DeltaT   WinVal B-Flight Info
10:06:40.367579 20.709532 10.87.132.12  10.84.162.216  124    2598  3748  0x0018 6605       0x45e8 (17896) 18196 161 3015               0.009684 64387  3080  citriximaclient > webdata [PSH, ACK] Seq=18196 Ack=3015 Win=64387 Len=161[Unreassembled Pac
10:06:40.404771 20.746724 10.84.162.216 10.87.132.12   25     3748  2598  0x0010 6606 6601  0x01d5 (469)   3015  0   15286 0.078550000 0.037192 65535        webdata > citriximaclient [ACK] Seq=3015 Ack=15286 Win=65535 Len=0
10:06:40.424874 20.766827 10.84.162.216 10.87.132.12   25     3748  2598  0x0018 6607       0x01d6 (470)   3015  13  15286             0.020103 65535  13    webdata > citriximaclient [PSH, ACK] Seq=3015 Ack=15286 Win=65535 Len=13
10:06:40.430355 20.772308 10.84.162.216 10.87.132.12   25     3748  2598  0x0010 6608 6604  0x01d7 (471)   3028  0   18196 0.072460000 0.005481 64752        webdata > citriximaclient [ACK] Seq=3028 Ack=18196 Win=64752 Len=0
10:06:40.524980 20.866933 10.84.162.216 10.87.132.12   25     3748  2598  0x0018 6609 6605  0x01d8 (472)   3028  14  18357 0.157401000 0.094625 65535  27    webdata > citriximaclient [PSH, ACK] Seq=3028 Ack=18357 Win=65535 Len=14
10:06:40.525176 20.867129 10.87.132.12  10.84.162.216  124    2598  3748  0x0010 6610 6609  0x4614 (17940) 18357 0   3042  0.000196000 0.000196 64360        citriximaclient > webdata [ACK] Seq=18357 Ack=3042 Win=64360 Len=0
10:06:40.624836 20.966789 10.84.162.216 10.87.132.12   25     3748  2598  0x0018 6611       0x01d9 (473)   3042  12  18357             0.099660 65535  12    webdata > citriximaclient [PSH, ACK] Seq=3042 Ack=18357 Win=65535 Len=12
10:06:40.714651 21.056604 10.87.132.12  10.84.162.216  124    2598  3748  0x0018 6612 6611  0x4640 (17984) 18357 98  3054  0.089815000 0.089815 64348  98    citriximaclient > webdata [PSH, ACK] Seq=18357 Ack=3054 Win=64348 Len=98[Unreassembled Pack
10:06:40.804716 21.146669 10.84.162.216 10.87.132.12   25     3748  2598  0x0010 6613 6612  0x01da (474)   3054  0   18455 0.090065000 0.090065 65535        webdata > citriximaclient [ACK] Seq=3054 Ack=18455 Win=65535 Len=0
10:06:40.835336 21.177289 10.87.132.12  10.84.162.216  124    2598  3748  0x0018 6614       0x465d (18013) 18455 9   3054              0.030620 64348  9     citriximaclient > webdata [PSH, ACK] Seq=18455 Ack=3054 Win=64348 Len=9
10:06:40.886425 21.228378 10.87.132.12  10.84.162.216  124    2598  3748  0x0018 6615       0x4666 (18022) 18464 10  3054              0.051089 64348  19    citriximaclient > webdata [PSH, ACK] Seq=18464 Ack=3054 Win=64348 Len=10
10:06:40.960424 21.302377 10.84.162.216 10.87.132.12   25     3748  2598  0x0018 6616 6615  0x01db (475)   3054  11  18474 0.073999000 0.073999 65535  11    webdata > citriximaclient [PSH, ACK] Seq=3054 Ack=18474 Win=65535 Len=11
10:06:40.961246 21.303199 10.87.132.12  10.84.162.216  124    2598  3748  0x0018 6617 6616  0x4674 (18036) 18474 13  3065  0.000822000 0.000822 64337  13    citriximaclient > webdata [PSH, ACK] Seq=18474 Ack=3065 Win=64337 Len=13
10:06:40.962676 21.304629 10.84.162.216 10.87.132.12   25     3748  2598  0x0018 6618       0x01dc (476)   3065  5   18474             0.001430 65535  5     webdata > citriximaclient [PSH, ACK] Seq=3065 Ack=18474 Win=65535 Len=5
10:06:40.963235 21.305188 10.87.132.12  10.84.162.216  124    2598  3748  0x0018 6619 6618  0x4675 (18037) 18487 10  3070  0.000559000 0.000559 64332  23    citriximaclient > webdata [PSH, ACK] Seq=18487 Ack=3070 Win=64332 Len=10
10:06:41.054278 21.396231 10.84.162.216 10.87.132.12   25     3748  2598  0x0011 6620       0x01dd (477)   3070  0   18474             0.091043 65535        webdata > citriximaclient [FIN, ACK] Seq=3070 Ack=18474 Win=65535 Len=0
10:06:41.054445 21.396398 10.87.132.12  10.84.162.216  124    2598  3748  0x0010 6621 6620  0x4689 (18057) 18497 0   3071  0.000167000 0.000167 64332        citriximaclient > webdata [ACK] Seq=18497 Ack=3071 Win=64332 Len=0
10:06:41.054453 21.396406 10.84.162.216 10.87.132.12   25     3748  2598  0x0004 6622       0x01de (478)   3065  0                     0.000008 0            webdata > citriximaclient [RST] Seq=3065 Win=0 Len=0
10:06:41.054454 21.396407 10.84.162.216 10.87.132.12   25     3748  2598  0x0004 6623       0x01df (479)   3070  0                     0.000001 0            webdata > citriximaclient [RST] Seq=3070 Win=0 Len=0
10:06:41.054544 21.396497 10.87.132.12  10.84.162.216  124    2598  3748  0x0011 6624       0x468a (18058) 18497 0   3071              0.000090 64332        citriximaclient > webdata [FIN, ACK] Seq=18497 Ack=3071 Win=64332 Len=0
10:06:41.127716 21.469669 10.84.162.216 10.87.132.12   25     3748  2598  0x0004 6625       0x01e0 (480)   3071  0                     0.073172 0            webdata > citriximaclient [RST] Seq=3071 Win=0 Len=0
10:06:41.127717 21.469670 10.84.162.216 10.87.132.12   25     3748  2598  0x0004 6626       0x01e1 (481)   3071  0                     0.000001 0            webdata > citriximaclient [RST] Seq=3071 Win=0 Len=0
```

```
⊞ Frame 6619: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
⊞ Ethernet II, Src: Cisco_14:c4:40 (00:18:74:14:c4:40), Dst: Cisco_cb:e0:40 (00:1c:b0:cb:e0:40)
⊞ 802.1Q Virtual LAN, PRI: 3, CFI: 0, ID: 1024
⊞ Internet Protocol Version 4, Src: 10.87.132.12 (10.87.132.12), Dst: 10.84.162.216 (10.84.162.216)
⊞ Transmission Control Protocol, Src Port: citriximaclient (2598), Dst Port: webdata (3748), Seq: 18487, Ack: 3070, Len: 10
⊟ Data (10 bytes)
    Data: 04040000000403000000
    [Length: 10]
```

Client Terminal FIN's Forcing Quit... but likely due to what the Server sent!

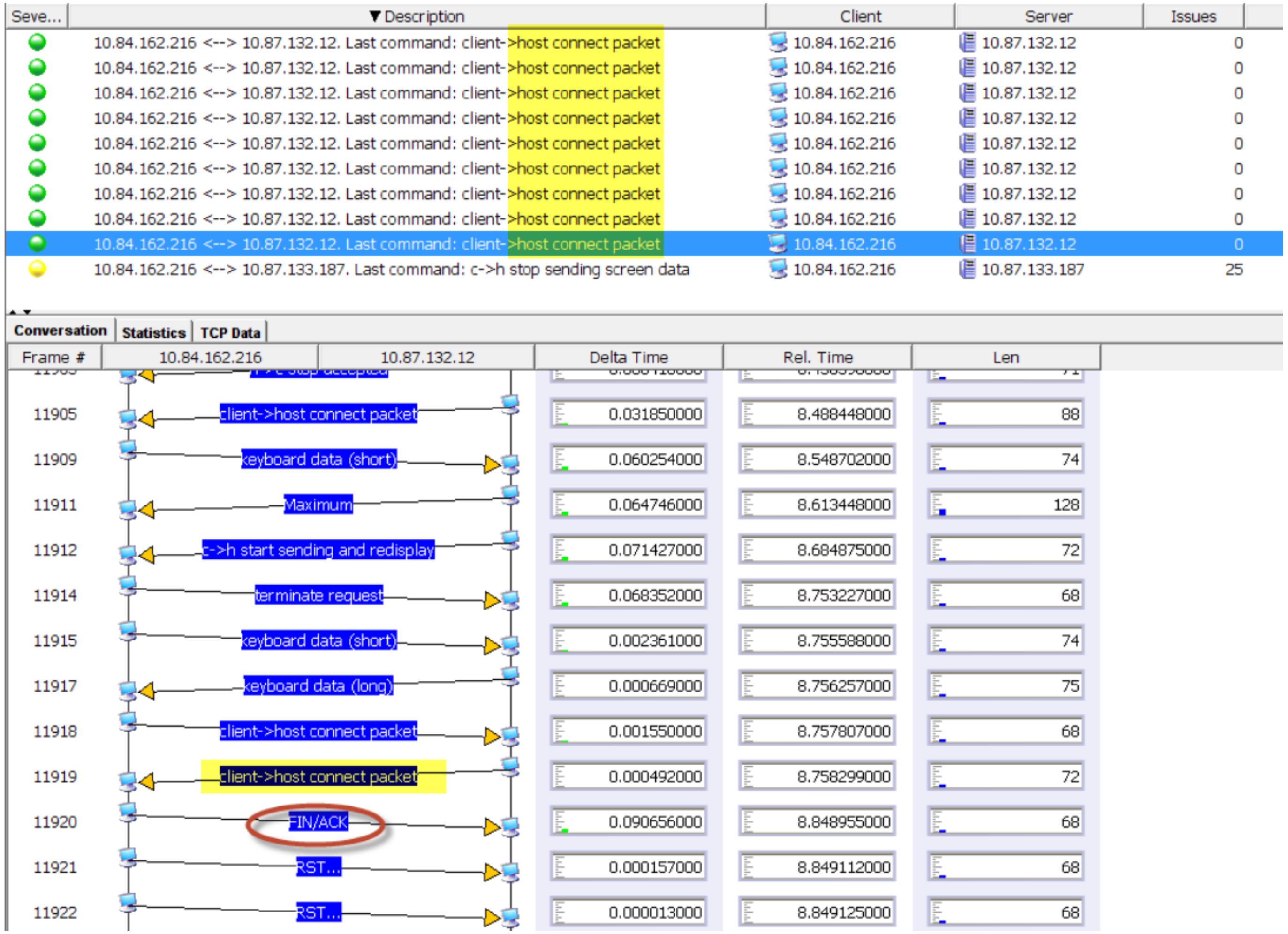
last ack

Win open fully

Chernobyl Data

3. Citrix Session Abort Signature “Chernobyl Packet”

More pattern details.



Seve...	▼Description	Client	Server	Issues
●	10.84.162.216 <--> 10.87.132.12. Last command: client->host connect packet	10.84.162.216	10.87.132.12	0
●	10.84.162.216 <--> 10.87.132.12. Last command: client->host connect packet	10.84.162.216	10.87.132.12	0
●	10.84.162.216 <--> 10.87.132.12. Last command: client->host connect packet	10.84.162.216	10.87.132.12	0
●	10.84.162.216 <--> 10.87.132.12. Last command: client->host connect packet	10.84.162.216	10.87.132.12	0
●	10.84.162.216 <--> 10.87.132.12. Last command: client->host connect packet	10.84.162.216	10.87.132.12	0
●	10.84.162.216 <--> 10.87.132.12. Last command: client->host connect packet	10.84.162.216	10.87.132.12	0
●	10.84.162.216 <--> 10.87.132.12. Last command: client->host connect packet	10.84.162.216	10.87.132.12	0
●	10.84.162.216 <--> 10.87.132.12. Last command: client->host connect packet	10.84.162.216	10.87.132.12	0
●	10.84.162.216 <--> 10.87.132.12. Last command: client->host connect packet	10.84.162.216	10.87.132.12	0
●	10.84.162.216 <--> 10.87.133.187. Last command: c->h stop sending screen data	10.84.162.216	10.87.133.187	25

Frame #	10.84.162.216	10.87.132.12	Delta Time	Rel. Time	Len
11905	◀ client->host connect packet		0.031850000	8.488448000	88
11909		keyboard data (short) ▶	0.060254000	8.548702000	74
11911	◀ Maximum		0.064746000	8.613448000	128
11912	◀ c->h start sending and redisplay		0.071427000	8.684875000	72
11914		terminate request ▶	0.068352000	8.753227000	68
11915		keyboard data (short) ▶	0.002361000	8.755588000	74
11917	◀ keyboard data (long)		0.000669000	8.756257000	75
11918		client->host connect packet ▶	0.001550000	8.757807000	68
11919	◀ client->host connect packet		0.000492000	8.758299000	72
11920		FIN/ACK ▶	0.090656000	8.848955000	68
11921		RST... ▶	0.000157000	8.849112000	68
11922		RST... ▶	0.000013000	8.849125000	68

Evidence of 30 second delay for file access causing severe user impact.

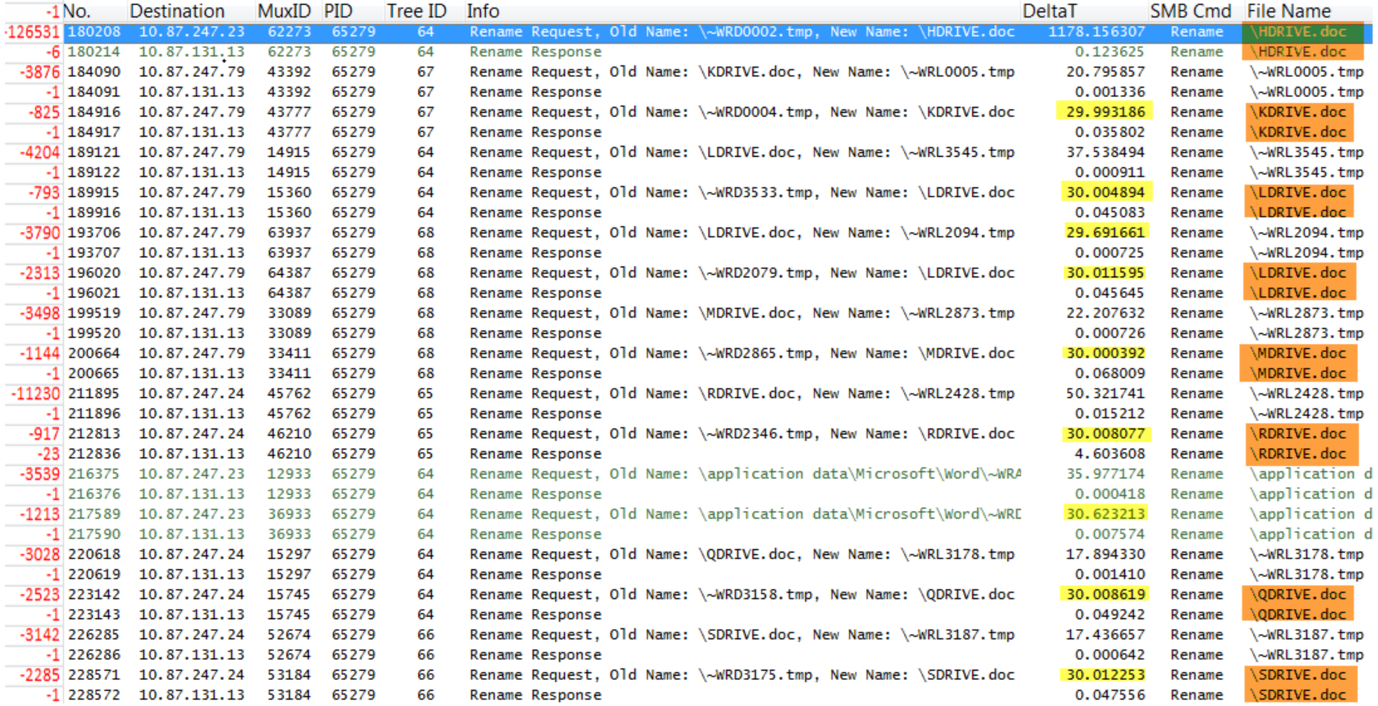
The test showed that regardless of the Network share accessed, it took 30 seconds to open and start to read a file, or save a file.

AppSense changes stopped the problem, and a work around for AppSense functions dependent upon the old configuration were found.

File access request delays at the Citrix server (The NetApp Filer responds rapidly) or a very odd yet unseen internal Citrix/Microsoft/McAfee/AppSense or Authentication issue exists causing users to experience very slow access to files. As you can see the slowdown manifests as a 30 second delay which is eliminated when AppSense Application Manager is disabled. The test below was performed by a user saving a blank WINWORD document to each of their mapped drives one by one. The red numbers on the left calculate how many packets traverse the network during the save from all other traffic. The yellow highlighted numbers are the amount of time that it took to perform the save. The orange highlight is the file name which was changed accordingly for each mapped drive by its drive letter.

The most odd thing is that the delay is right at 30 seconds, repeatedly in all but a couple of examples. That is a huge hint for the software vendors to consider what pacing elements are timed at 30 second intervals.

Since the problem is eliminated when AppSense App Manager is disabled although not completely impossible, it is highly likely AppSense is responsible for the delay.



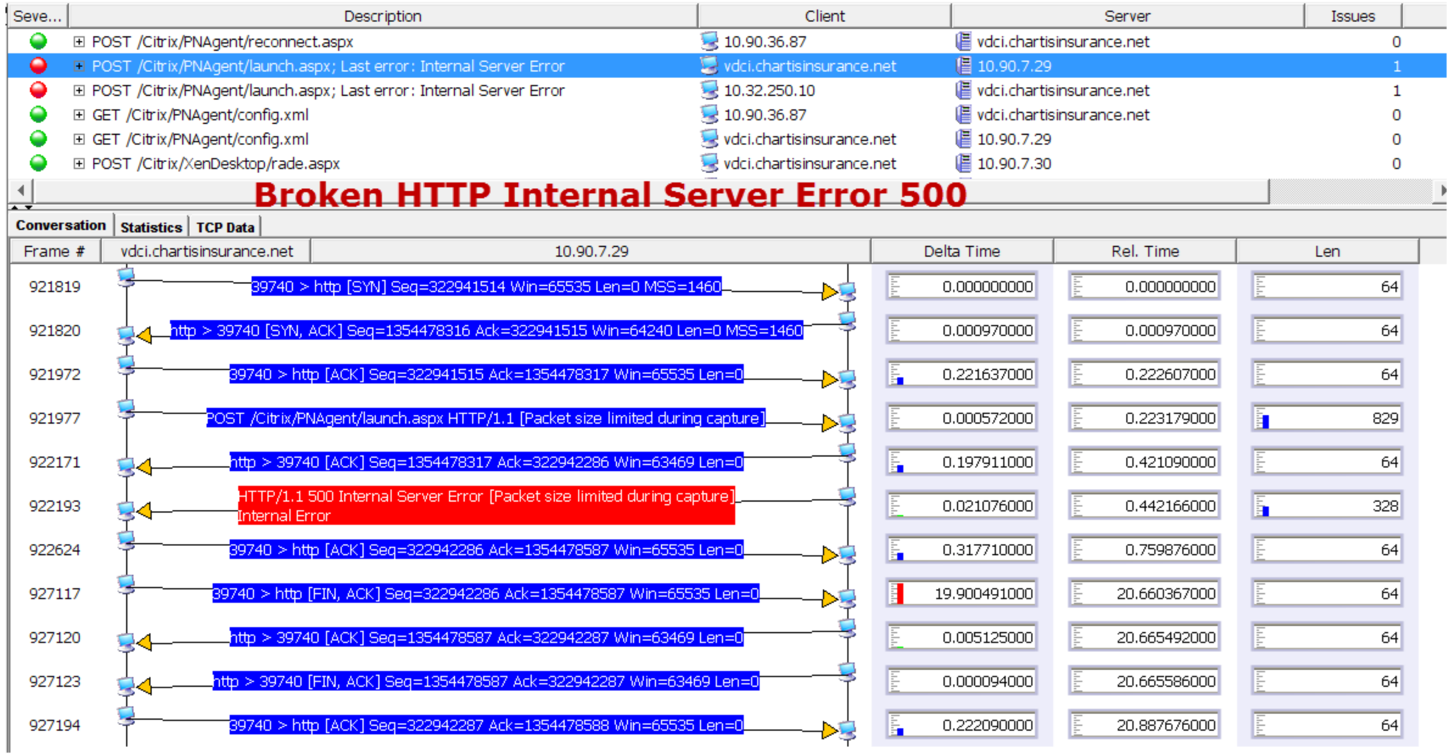
-1	No.	Destination	MuxID	PID	Tree ID	Info	DeltaT	SMB Cmd	File Name
-126531	180208	10.87.247.23	62273	65279	64	Rename Request, Old Name: \~WRD0002.tmp, New Name: \HDRIVE.doc	1178.156307	Rename	\HDRIVE.doc
-6	180214	10.87.131.13	62273	65279	64	Rename Response	0.123625	Rename	\HDRIVE.doc
-3876	184090	10.87.247.79	43392	65279	67	Rename Request, Old Name: \KDRIVE.doc, New Name: \~WRL0005.tmp	20.795857	Rename	\~WRL0005.tmp
-1	184091	10.87.131.13	43392	65279	67	Rename Response	0.001336	Rename	\~WRL0005.tmp
-825	184916	10.87.247.79	43777	65279	67	Rename Request, Old Name: \~WRD0004.tmp, New Name: \KDRIVE.doc	29.993186	Rename	\KDRIVE.doc
-1	184917	10.87.131.13	43777	65279	67	Rename Response	0.035802	Rename	\KDRIVE.doc
-4204	189121	10.87.247.79	14915	65279	64	Rename Request, Old Name: \LDRIVE.doc, New Name: \~WRL3545.tmp	37.538494	Rename	\~WRL3545.tmp
-1	189122	10.87.131.13	14915	65279	64	Rename Response	0.000911	Rename	\~WRL3545.tmp
-793	189915	10.87.247.79	15360	65279	64	Rename Request, Old Name: \~WRD3533.tmp, New Name: \LDRIVE.doc	30.004894	Rename	\LDRIVE.doc
-1	189916	10.87.131.13	15360	65279	64	Rename Response	0.045083	Rename	\LDRIVE.doc
-3790	193706	10.87.247.79	63937	65279	68	Rename Request, Old Name: \LDRIVE.doc, New Name: \~WRL2094.tmp	29.691661	Rename	\~WRL2094.tmp
-1	193707	10.87.131.13	63937	65279	68	Rename Response	0.000725	Rename	\~WRL2094.tmp
-2313	196020	10.87.247.79	64387	65279	68	Rename Request, Old Name: \~WRD2079.tmp, New Name: \LDRIVE.doc	30.011595	Rename	\LDRIVE.doc
-1	196021	10.87.131.13	64387	65279	68	Rename Response	0.045645	Rename	\LDRIVE.doc
-3498	199519	10.87.247.79	33089	65279	68	Rename Request, Old Name: \MDRIVE.doc, New Name: \~WRL2873.tmp	22.207632	Rename	\~WRL2873.tmp
-1	199520	10.87.131.13	33089	65279	68	Rename Response	0.000726	Rename	\~WRL2873.tmp
-1144	200664	10.87.247.79	33411	65279	68	Rename Request, Old Name: \~WRD2865.tmp, New Name: \MDRIVE.doc	30.000392	Rename	\MDRIVE.doc
-1	200665	10.87.131.13	33411	65279	68	Rename Response	0.068009	Rename	\MDRIVE.doc
-11230	211895	10.87.247.24	45762	65279	65	Rename Request, Old Name: \RDRIVE.doc, New Name: \~WRL2428.tmp	50.321741	Rename	\~WRL2428.tmp
-1	211896	10.87.131.13	45762	65279	65	Rename Response	0.015212	Rename	\~WRL2428.tmp
-917	212813	10.87.247.24	46210	65279	65	Rename Request, Old Name: \~WRD2346.tmp, New Name: \RDRIVE.doc	30.008077	Rename	\RDRIVE.doc
-23	212836	10.87.131.13	46210	65279	65	Rename Response	4.603608	Rename	\RDRIVE.doc
-3539	216375	10.87.247.23	12933	65279	64	Rename Request, Old Name: \application data\Microsoft\Word\~WRA	35.977174	Rename	\application d
-1	216376	10.87.131.13	12933	65279	64	Rename Response	0.000418	Rename	\application d
-1213	217589	10.87.247.23	36933	65279	64	Rename Request, Old Name: \application data\Microsoft\Word\~WRD	30.623213	Rename	\application d
-1	217590	10.87.131.13	36933	65279	64	Rename Response	0.007574	Rename	\application d
-3028	220618	10.87.247.24	15297	65279	64	Rename Request, Old Name: \QDRIVE.doc, New Name: \~WRL3178.tmp	17.894330	Rename	\~WRL3178.tmp
-1	220619	10.87.131.13	15297	65279	64	Rename Response	0.001410	Rename	\~WRL3178.tmp
-2523	223142	10.87.247.24	15745	65279	64	Rename Request, Old Name: \~WRD3158.tmp, New Name: \QDRIVE.doc	30.008619	Rename	\QDRIVE.doc
-1	223143	10.87.131.13	15745	65279	64	Rename Response	0.049242	Rename	\QDRIVE.doc
-3142	226285	10.87.247.24	52674	65279	66	Rename Request, Old Name: \SDRIVE.doc, New Name: \~WRL3187.tmp	17.436657	Rename	\~WRL3187.tmp
-1	226286	10.87.131.13	52674	65279	66	Rename Response	0.000642	Rename	\~WRL3187.tmp
-2285	228571	10.87.247.24	53184	65279	66	Rename Request, Old Name: \~WRD3175.tmp, New Name: \SDRIVE.doc	30.012253	Rename	\SDRIVE.doc
-1	228572	10.87.131.13	53184	65279	66	Rename Response	0.047556	Rename	\SDRIVE.doc

Citrix Wyse Terminal HTTP Boot Services Impacted

HTTP is used to load part of the Wyse Terminal boot processes necessary to log a user on to the Citrix system.

When a key component to the boot process is impacted the result is users not being able to log into Citrix haphazardly for periods of up to 3 hours.

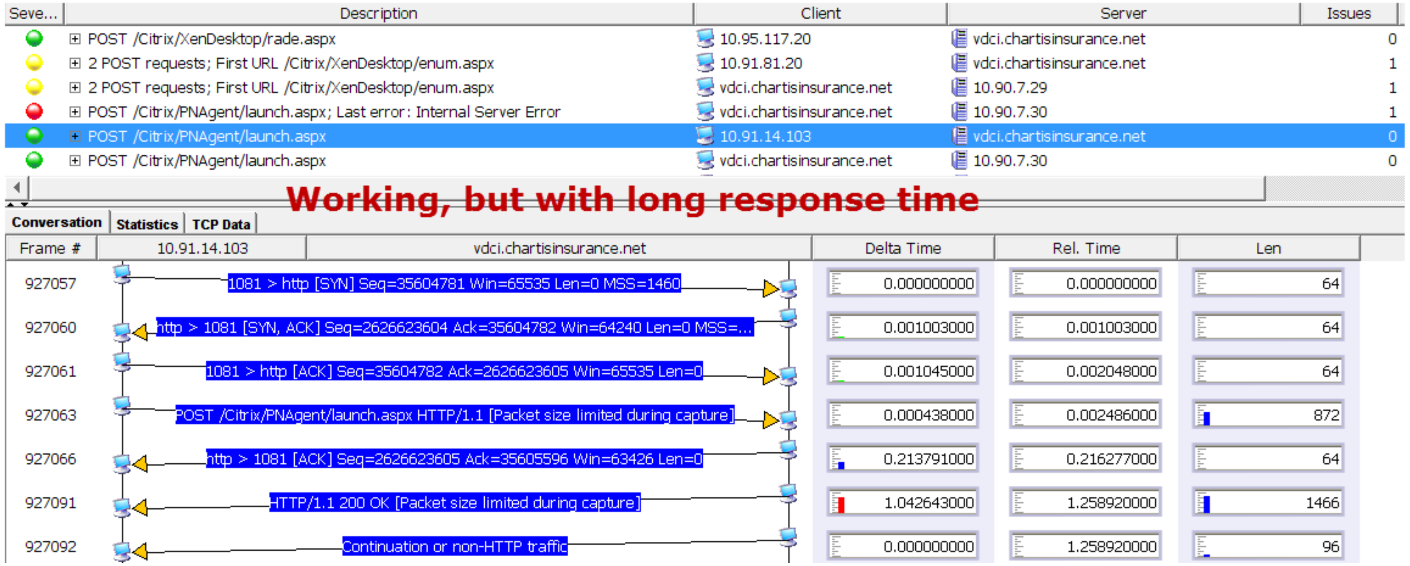
This causes the user to hang and have to reboot the Wyse terminal repeatedly until an attempt is successful.



Seve...	Description	Client	Server	Issues
●	⊞ POST /Citrix/PNAgent/reconnect.aspx	10.90.36.87	vdci.chartisinsurance.net	0
●	⊞ POST /Citrix/PNAgent/launch.aspx; Last error: Internal Server Error	vdci.chartisinsurance.net	10.90.7.29	1
●	⊞ POST /Citrix/PNAgent/launch.aspx; Last error: Internal Server Error	10.32.250.10	vdci.chartisinsurance.net	1
●	⊞ GET /Citrix/PNAgent/config.xml	10.90.36.87	vdci.chartisinsurance.net	0
●	⊞ GET /Citrix/PNAgent/config.xml	vdci.chartisinsurance.net	10.90.7.29	0
●	⊞ POST /Citrix/XenDesktop/rade.aspx	vdci.chartisinsurance.net	10.90.7.30	0

Broken HTTP Internal Server Error 500

Frame #	vdci.chartisinsurance.net	10.90.7.29	Delta Time	Rel. Time	Len
921819	39740 > http [SYN] Seq=322941514 Win=65535 Len=0 MSS=1460		0.000000000	0.000000000	64
921820	http > 39740 [SYN, ACK] Seq=1354478316 Ack=322941515 Win=64240 Len=0 MSS=1460		0.000970000	0.000970000	64
921972	39740 > http [ACK] Seq=322941515 Ack=1354478317 Win=65535 Len=0		0.221637000	0.222607000	64
921977	POST /Citrix/PNAgent/launch.aspx HTTP/1.1 [Packet size limited during capture]		0.000572000	0.223179000	829
922171	http > 39740 [ACK] Seq=1354478317 Ack=322942286 Win=63469 Len=0		0.197911000	0.421090000	64
922193	HTTP/1.1 500 Internal Server Error [Packet size limited during capture] Internal Error		0.021076000	0.442166000	328
922624	39740 > http [ACK] Seq=322942286 Ack=1354478587 Win=65535 Len=0		0.317710000	0.759876000	64
927117	39740 > http [FIN, ACK] Seq=322942286 Ack=1354478587 Win=65535 Len=0		19.900491000	20.660367000	64
927120	http > 39740 [ACK] Seq=1354478587 Ack=322942287 Win=63469 Len=0		0.005125000	20.665492000	64
927123	http > 39740 [FIN, ACK] Seq=1354478587 Ack=322942287 Win=63469 Len=0		0.000094000	20.665586000	64
927194	39740 > http [ACK] Seq=322942287 Ack=1354478588 Win=65535 Len=0		0.222090000	20.887676000	64



Seve...	Description	Client	Server	Issues
●	⊞ POST /Citrix/XenDesktop/rade.aspx	10.95.117.20	vdci.chartisinsurance.net	0
●	⊞ 2 POST requests; First URL /Citrix/XenDesktop/enum.aspx	10.91.81.20	vdci.chartisinsurance.net	1
●	⊞ 2 POST requests; First URL /Citrix/XenDesktop/enum.aspx	vdci.chartisinsurance.net	10.90.7.29	1
●	⊞ POST /Citrix/PNAgent/launch.aspx; Last error: Internal Server Error	vdci.chartisinsurance.net	10.90.7.30	1
●	⊞ POST /Citrix/PNAgent/launch.aspx	10.91.14.103	vdci.chartisinsurance.net	0
●	⊞ POST /Citrix/PNAgent/launch.aspx	vdci.chartisinsurance.net	10.90.7.30	0

Working, but with long response time

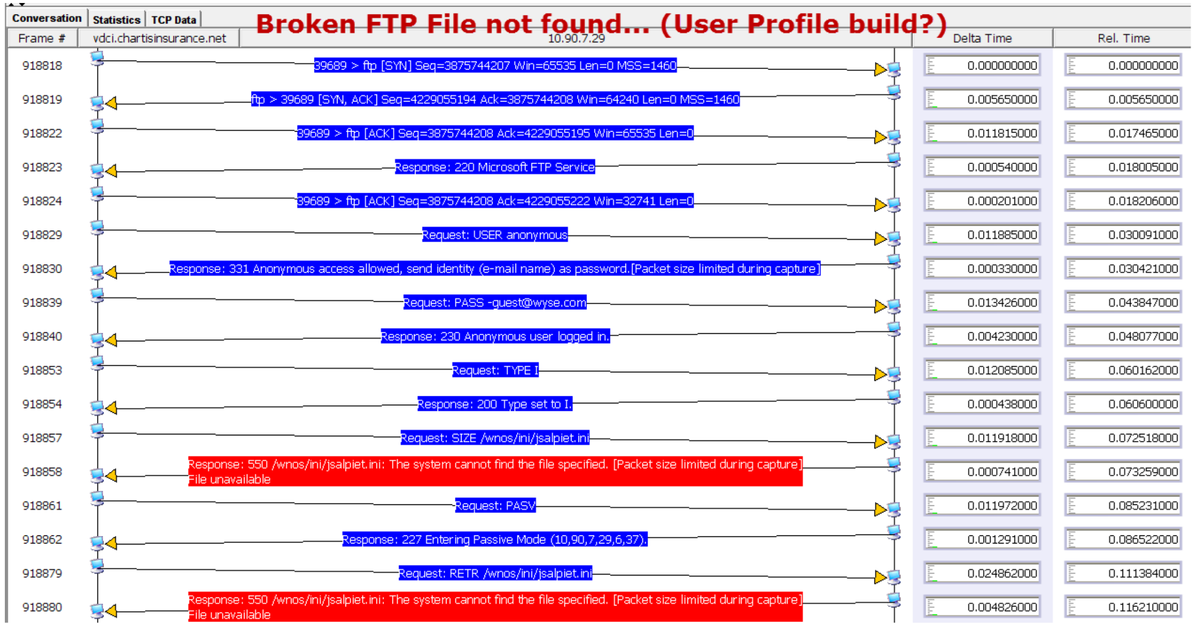
Frame #	10.91.14.103	vdci.chartisinsurance.net	Delta Time	Rel. Time	Len
927057	1081 > http [SYN] Seq=35604781 Win=65535 Len=0 MSS=1460		0.000000000	0.000000000	64
927060	http > 1081 [SYN, ACK] Seq=2626623604 Ack=35604782 Win=64240 Len=0 MSS=...		0.001003000	0.001003000	64
927061	1081 > http [ACK] Seq=35604782 Ack=2626623605 Win=65535 Len=0		0.001045000	0.002048000	64
927063	POST /Citrix/PNAgent/launch.aspx HTTP/1.1 [Packet size limited during capture]		0.000438000	0.002486000	872
927066	http > 1081 [ACK] Seq=2626623605 Ack=35605596 Win=63426 Len=0		0.213791000	0.216277000	64
927091	HTTP/1.1 200 OK [Packet size limited during capture]		1.042643000	1.258920000	1466
927092	Continuation or non-HTTP traffic		0.000000000	1.258920000	96

Citrix Wyse Terminal FTP Boot Services Impacted

The same servers that provide HTTP services also provide file transfer services.

The servers were found to have multiple problems contributing to users having lengthy periods of login difficulty sometimes for several hours.

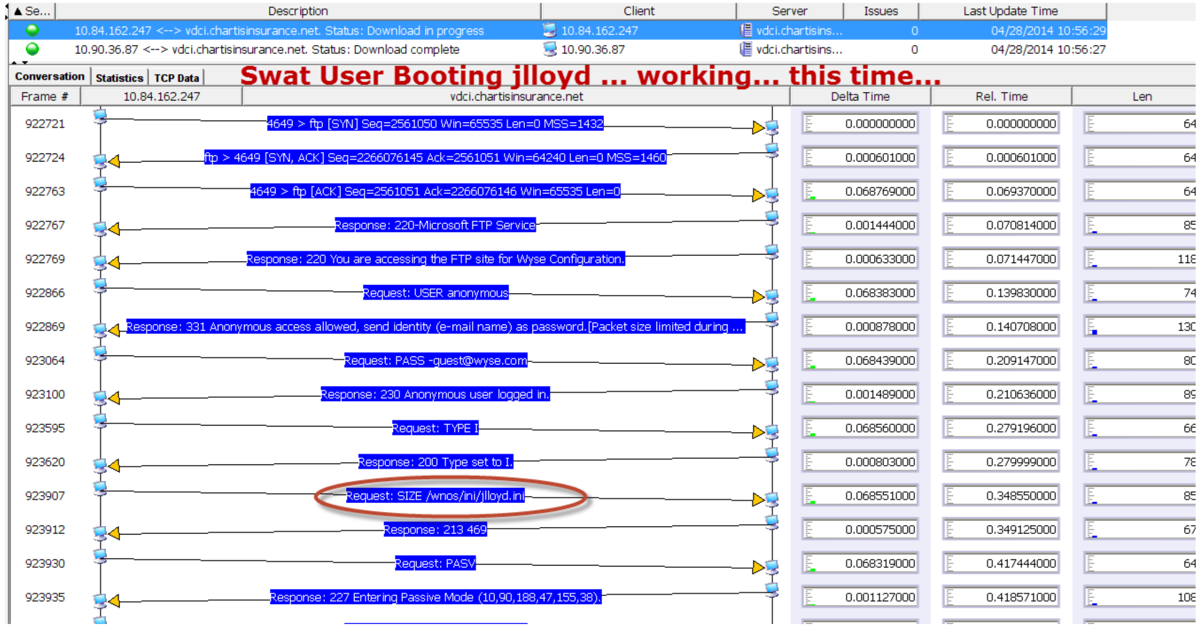
Our findings alerted the Citrix Team to rebuild and monitor the servers.



Broken FTP File not found... (User Profile build?)

Frame #	vdci.chartisinsurance.net	10.90.7.29	Delta Time	Rel. Time
918818		39689 > ftp [SYN] Seq=3875744207 Win=65535 Len=0 MSS=1460	0.000000000	0.000000000
918819		ftp > 39689 [SYN, ACK] Seq=4229055194 Ack=3875744208 Win=64240 Len=0 MSS=1460	0.005650000	0.005650000
918822		39689 > ftp [ACK] Seq=3875744208 Ack=4229055195 Win=65535 Len=0	0.011815000	0.017465000
918823		Response: 220 Microsoft FTP Service	0.000540000	0.018005000
918824		39689 > ftp [ACK] Seq=3875744208 Ack=4229055222 Win=32741 Len=0	0.000201000	0.018206000
918829		Request: USER anonymous	0.011885000	0.030091000
918830		Response: 331 Anonymous access allowed, send identity (e-mail name) as password.[Packet size limited during capture]	0.000330000	0.030421000
918839		Request: PASS -guest@wyse.com	0.013426000	0.043847000
918840		Response: 230 Anonymous user logged in.	0.004230000	0.048077000
918853		Request: TYPE I	0.012085000	0.060162000
918854		Response: 200 Type set to I.	0.000438000	0.060600000
918857		Request: SIZE /wnos/ini/jsalpiet.ini	0.011918000	0.072518000
918858		Response: 550 /wnos/ini/jsalpiet.ini: The system cannot find the file specified. [Packet size limited during capture] File unavailable	0.000741000	0.073259000
918861		Request: PASV	0.011972000	0.085231000
918862		Response: 227 Entering Passive Mode (10,90,7,29,6,37).	0.001291000	0.086522000
918879		Request: RETR /wnos/ini/jsalpiet.ini	0.024862000	0.111384000
918880		Response: 550 /wnos/ini/jsalpiet.ini: The system cannot find the file specified. [Packet size limited during capture] File unavailable	0.004826000	0.116210000

FTP Working for one of our Swat Users...



▲ Se...	Description	Client	Server	Issues	Last Update Time
●	10.84.162.247 <--> vdci.chartisinsurance.net. Status: Download in progress	10.84.162.247	vdci.chartisins...	0	04/28/2014 10:56:29
●	10.90.36.87 <--> vdci.chartisinsurance.net. Status: Download complete	10.90.36.87	vdci.chartisins...	0	04/28/2014 10:56:27

Swat User Booting jlloyd ... working... this time...

Frame #	10.84.162.247	vdci.chartisinsurance.net	Delta Time	Rel. Time	Len
922721		4649 > ftp [SYN] Seq=2561050 Win=65535 Len=0 MSS=1432	0.000000000	0.000000000	64
922724		ftp > 4649 [SYN, ACK] Seq=2266076145 Ack=2561051 Win=64240 Len=0 MSS=1460	0.000601000	0.000601000	64
922763		4649 > ftp [ACK] Seq=2561051 Ack=2266076146 Win=65535 Len=0	0.068769000	0.069370000	64
922767		Response: 220-Microsoft FTP Service	0.001444000	0.070814000	85
922769		Response: 220 You are accessing the FTP site for Wyse Configuration.	0.000633000	0.071447000	118
922866		Request: USER anonymous	0.068383000	0.139830000	74
922869		Response: 331 Anonymous access allowed, send identity (e-mail name) as password.[Packet size limited during ...	0.000878000	0.140708000	130
923064		Request: PASS -guest@wyse.com	0.068439000	0.209147000	80
923100		Response: 230 Anonymous user logged in.	0.001489000	0.210636000	89
923595		Request: TYPE I	0.068560000	0.279196000	66
923620		Response: 200 Type set to I.	0.000803000	0.279999000	78
923907		Request: SIZE /wnos/ini/jlloyd.ini	0.068551000	0.348550000	85
923912		Response: 213 469	0.000575000	0.349125000	67
923930		Request: PASV	0.068319000	0.417444000	64
923935		Response: 227 Entering Passive Mode (10,90,188,47,155,38).	0.001127000	0.418571000	108

WAAS Analysis of Citrix

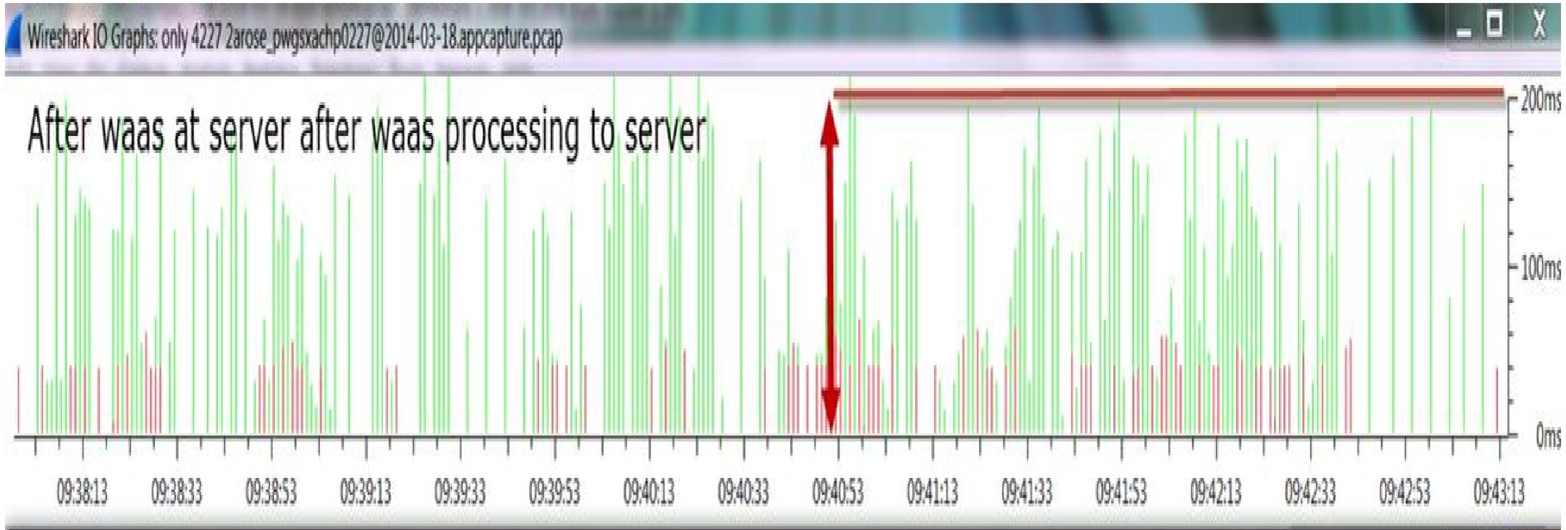
This was a quick analysis of the effectiveness of the WAAS compression of Citrix traffic.

The amount of work done and the time it took to be accomplished seems to be minimal improvement in volume savings.

Due to the compatibility of various versions of Citrix and the version of WAAS it was recommended that an upgrade to WAAS be made to be in line with the version of Citrix used.

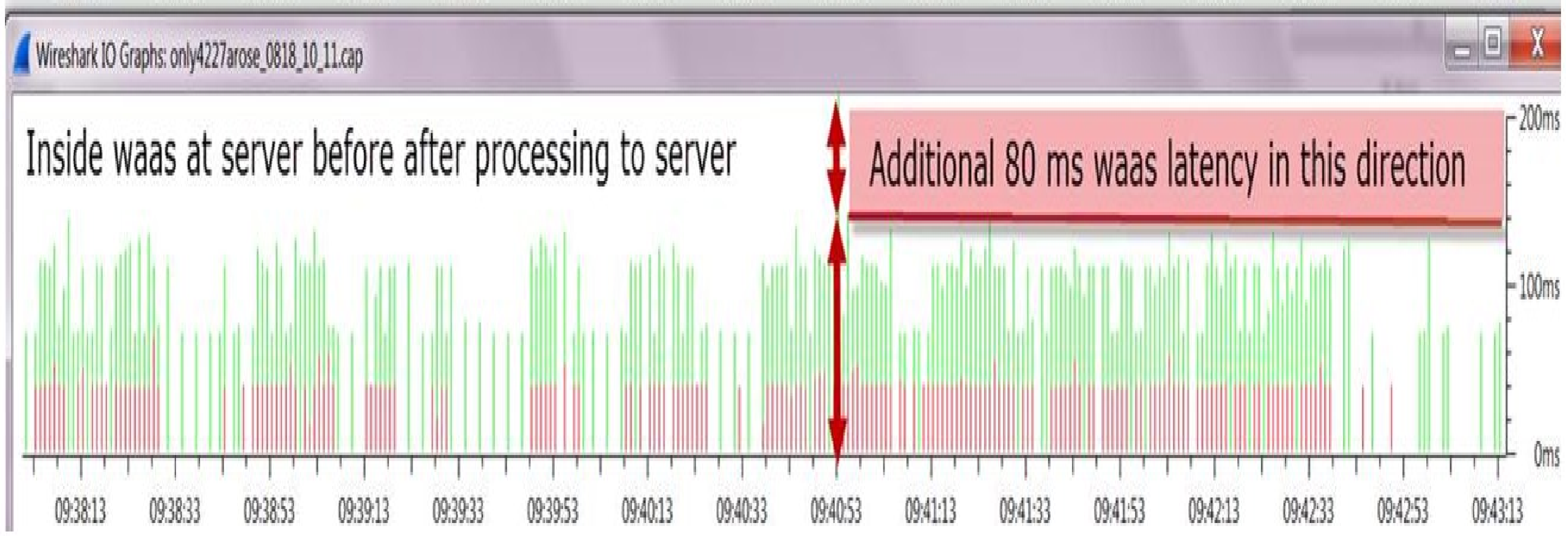
Many potential problems could exist without the Citrix vs Cisco version match to respective versions.

Recommend not using WAAS until versions match support from both organizaitons.



Wireshark IO Graphs: only 4227 2arose_pwgsxachp0227@2014-03-18.appcapture.pcap

After waas at server after waas processing to server



Wireshark IO Graphs: only4227arose_0818_10_11.cap

Inside waas at server before after processing to server

Additional 80 ms waas latency in this direction

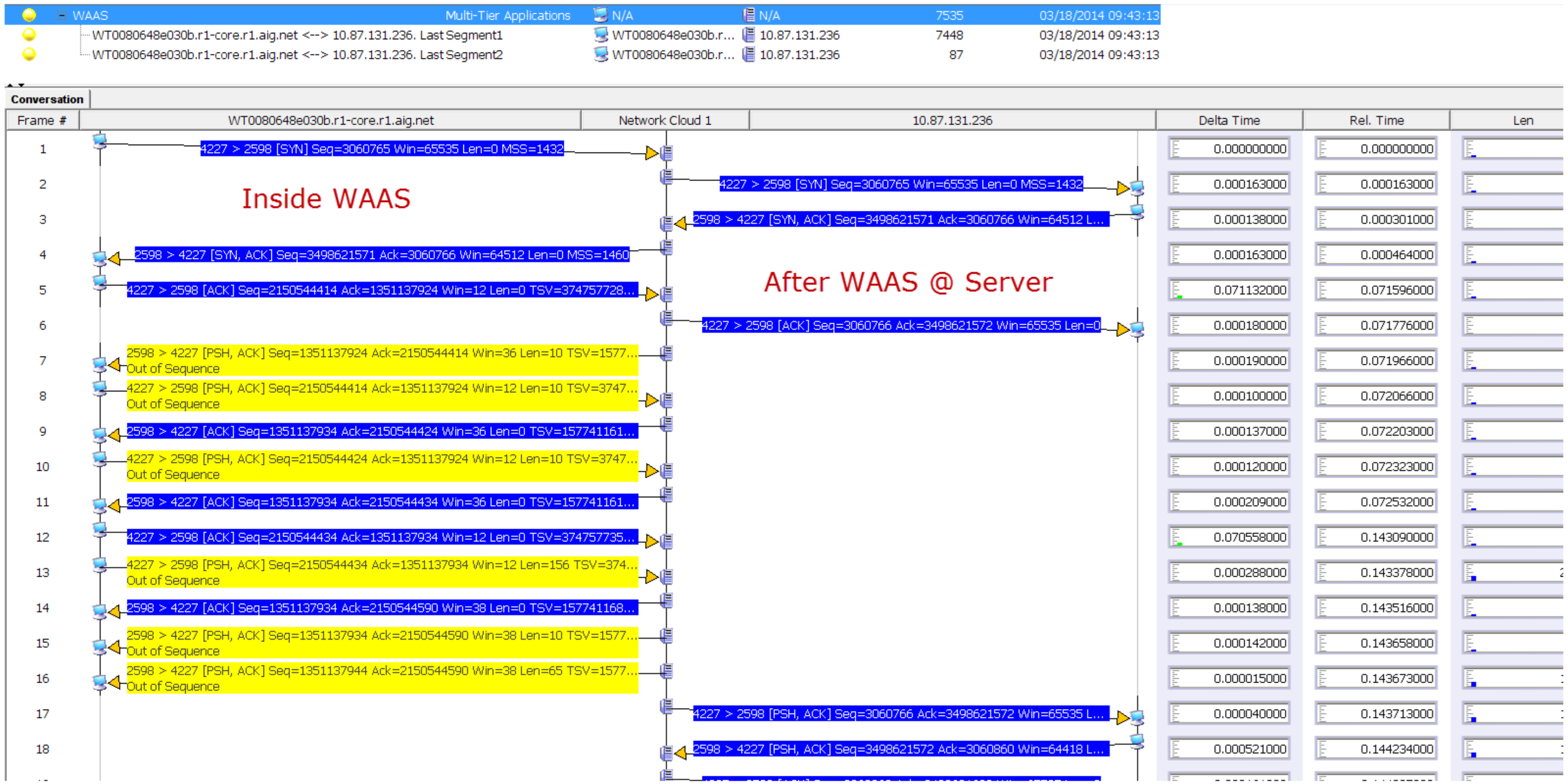
WAAS Analysis of Citrix

Multi-tier analysis required to evaluate the effectiveness of Cisco WAAS.

Using multitier makes this possible

Client needs the skills of multi-tier analysis for many multi-tier applications and appliances.

Here's those screen shots… multi tier and combined taking out acks in wireshark…



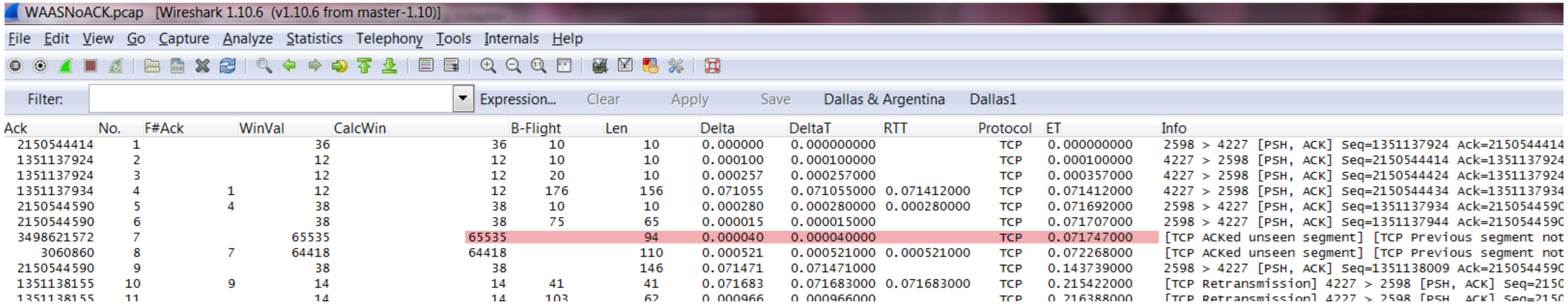
●	WAAS	Multi-Tier Applications	N/A	N/A	7535	03/18/2014 09:43:13
●	WT0080648e030b.r1-core.r1.aig.net <--> 10.87.131.236. Last Segment1		WT0080648e030b.r…	10.87.131.236	7448	03/18/2014 09:43:13
●	WT0080648e030b.r1-core.r1.aig.net <--> 10.87.131.236. Last Segment2		WT0080648e030b.r…	10.87.131.236	87	03/18/2014 09:43:13

Conversation

Frame #	WT0080648e030b.r1-core.r1.aig.net	Network Cloud 1	10.87.131.236	Delta Time	Rel. Time	Len
1	4227 > 2598 [SYN] Seq=3060765 Win=65535 Len=0 MSS=1432			0.000000000	0.000000000	
2			4227 > 2598 [SYN] Seq=3060765 Win=65535 Len=0 MSS=1432	0.000163000	0.000163000	
3			2598 > 4227 [SYN, ACK] Seq=3498621571 Ack=3060766 Win=64512 L…	0.000138000	0.000301000	
4	2598 > 4227 [SYN, ACK] Seq=3498621571 Ack=3060766 Win=64512 Len=0 MSS=1460			0.000163000	0.000464000	
5	4227 > 2598 [ACK] Seq=2150544414 Ack=1351137924 Win=12 Len=0 TSV=374757728…			0.071132000	0.071596000	
6			4227 > 2598 [ACK] Seq=3060766 Ack=3498621572 Win=65535 Len=0	0.000180000	0.071776000	
7	2598 > 4227 [PSH, ACK] Seq=1351137924 Ack=2150544414 Win=36 Len=10 TSV=1577… Out of Sequence			0.000190000	0.071966000	
8	4227 > 2598 [PSH, ACK] Seq=2150544414 Ack=1351137924 Win=12 Len=10 TSV=3747… Out of Sequence			0.000100000	0.072066000	
9	2598 > 4227 [ACK] Seq=1351137934 Ack=2150544424 Win=36 Len=0 TSV=157741161…			0.000137000	0.072203000	
10	4227 > 2598 [PSH, ACK] Seq=2150544424 Ack=1351137924 Win=12 Len=10 TSV=3747… Out of Sequence			0.000120000	0.072323000	
11	2598 > 4227 [ACK] Seq=1351137934 Ack=2150544434 Win=36 Len=0 TSV=157741161…			0.000209000	0.072532000	
12	4227 > 2598 [ACK] Seq=2150544434 Ack=1351137934 Win=12 Len=0 TSV=374757735…			0.070558000	0.143090000	
13	4227 > 2598 [PSH, ACK] Seq=2150544434 Ack=1351137934 Win=12 Len=156 TSV=374… Out of Sequence			0.000288000	0.143378000	2
14	2598 > 4227 [ACK] Seq=1351137934 Ack=2150544590 Win=38 Len=0 TSV=157741168…			0.000138000	0.143516000	
15	2598 > 4227 [PSH, ACK] Seq=1351137934 Ack=2150544590 Win=38 Len=10 TSV=1577… Out of Sequence			0.000142000	0.143658000	
16	2598 > 4227 [PSH, ACK] Seq=1351137944 Ack=2150544590 Win=38 Len=65 TSV=1577… Out of Sequence			0.000015000	0.143673000	
17			4227 > 2598 [PSH, ACK] Seq=3060766 Ack=3498621572 Win=65535 L…	0.000040000	0.143713000	
18			2598 > 4227 [PSH, ACK] Seq=3498621572 Ack=3060860 Win=64418 L…	0.000521000	0.144234000	

Inside WAAS

After WAAS @ Server



WAASNoACK.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression… Clear Apply Save Dallas & Argentina Dallas1

```
Ack         No.  F#Ack   WinVal   CalcWin         B-Flight   Len    Delta      DeltaT       RTT          Protocol  ET            Info
 2150544414   1                36               36     10      10   0.000000   0.000000000                TCP     0.000000000   2598 > 4227 [PSH, ACK] Seq=1351137924 Ack=2150544414
 1351137924   2                12               12     10      10   0.000100   0.000100000                TCP     0.000100000   4227 > 2598 [PSH, ACK] Seq=2150544414 Ack=1351137924
 1351137924   3                12               12     20      10   0.000257   0.000257000                TCP     0.000357000   4227 > 2598 [PSH, ACK] Seq=2150544424 Ack=1351137924
 1351137934   4        1       12               12    176     156   0.071055   0.071055000  0.071412000   TCP     0.071412000   4227 > 2598 [PSH, ACK] Seq=2150544434 Ack=1351137934
 2150544590   5        4       38               38     10      10   0.000280   0.000280000  0.000280000   TCP     0.071692000   2598 > 4227 [PSH, ACK] Seq=1351137934 Ack=215054459C
 2150544590   6                38               38     75      65   0.000015   0.000015000                TCP     0.071707000   2598 > 4227 [PSH, ACK] Seq=1351137944 Ack=215054459C
 3498621572   7             65535            65535             94   0.000040   0.000040000                TCP     0.071747000   [TCP ACKed unseen segment] [TCP Previous segment not
    3060860   8        7    64418            64418            110   0.000521   0.000521000  0.000521000   TCP     0.072268000   [TCP ACKed unseen segment] [TCP Previous segment not
 2150544590   9                38               38            146   0.071471   0.071471000                TCP     0.143739000   2598 > 4227 [PSH, ACK] Seq=1351138009 Ack=215054459C
 1351138155  10        9       14               14     41      41   0.071683   0.071683000  0.071683000   TCP     0.215422000   [TCP Retransmission] 4227 > 2598 [PSH, ACK] Seq=215C
 1351138155  11                14               14    103      62   0.000966   0.000966000                TCP     0.216388000   [TCP Retransmission] 4227 > 2598 [PSH, ACK] Seq=215C
```

File Access Problems with Citrix Servers

Analysis of file access problems were found to be due to AppSense and Microsoft file access issues.

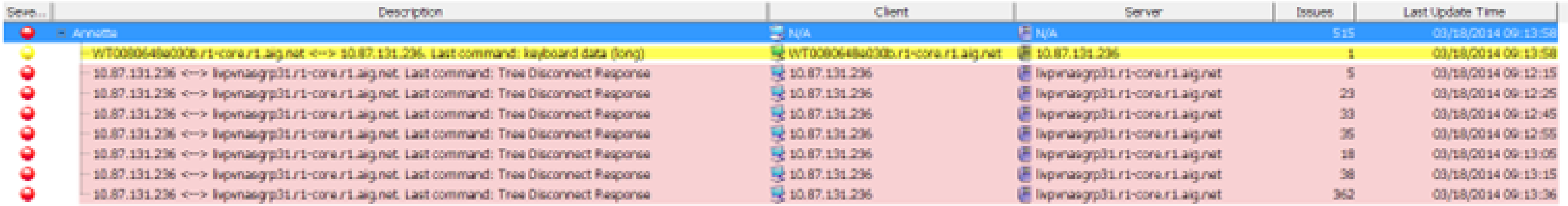
User is accessing Citrix session in yellow, server is trying open connections to Filer repeatedly and gets error messages.

See the attached .pdf to see the packets in multi-tier view showing the user connected using Citrix, terminal commands going back and forth while SMB filer commands have errors accessing the file

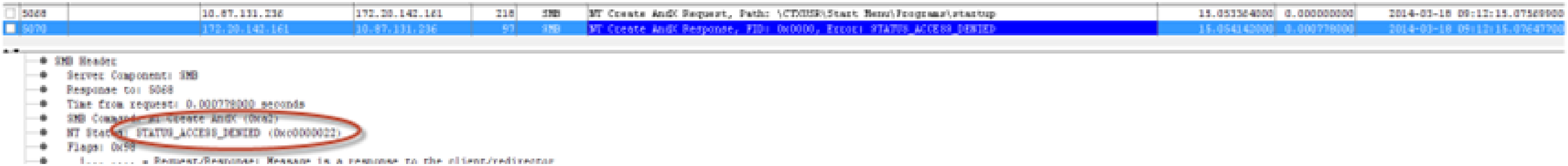
This is one of the reasons I have asked for the architectural design for [redacted] Citrix user file access path hierarchy. This issue however seems to be inability of the server to open files for Citrix users.

Other users have experienced significant delays in ability to access files in the Citrix environment… waited a few minutes and the files are accessible… this could be:

1.) Filers are so overloaded that file lock housekeeping and user rights security housekeeping falls behind.
2.) Citrix is not providing the appropriate security credentials for users… or Citrix is overloaded in its housekeeping tasks.
3.) Security tokens are slow to populate to Filers for user access… or security authentication slow to respond or
4.) A combination of these of other things…



Seve...	Description	Client	Server	Issues	Last Update Time
●	⊟ Annette	N/A	N/A	515	03/18/2014 09:13:58
●	WT0080648a030b.r1-core.r1.aig.net <--> 10.87.131.236. Last command: keyboard data (long)	WT0080648a030b.r1-core.r1.aig.net	10.87.131.236	1	03/18/2014 09:13:58
●	10.87.131.236 <--> lxpwnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lxpwnasgrp31.r1-core.r1.aig.net	5	03/18/2014 09:12:15
●	10.87.131.236 <--> lxpwnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lxpwnasgrp31.r1-core.r1.aig.net	23	03/18/2014 09:12:25
●	10.87.131.236 <--> lxpwnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lxpwnasgrp31.r1-core.r1.aig.net	33	03/18/2014 09:12:45
●	10.87.131.236 <--> lxpwnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lxpwnasgrp31.r1-core.r1.aig.net	35	03/18/2014 09:12:55
●	10.87.131.236 <--> lxpwnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lxpwnasgrp31.r1-core.r1.aig.net	18	03/18/2014 09:13:05
●	10.87.131.236 <--> lxpwnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lxpwnasgrp31.r1-core.r1.aig.net	38	03/18/2014 09:13:15
●	10.87.131.236 <--> lxpwnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lxpwnasgrp31.r1-core.r1.aig.net	362	03/18/2014 09:13:36



```
□ 5068    10.87.131.236   172.20.142.161   218   SMB   NT Create AndX Request, Path: \CTXUSR\Start Menu\Programs\startup   15.053364000   0.000000000   2014-03-18 09:12:15.07529900
□ 5070    172.20.142.161  10.87.131.236     97   SMB   NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED    15.054142000   0.000778000   2014-03-18 09:12:15.07647700

  SMB Header
    Server Component: SMB
    Response to: 5068
    Time from request: 0.000778000 seconds
    SMB Command: NT Create AndX (0xa2)
    NT Status: STATUS_ACCESS_DENIED (0xc0000022)
    Flags: 0x98
      1... .... = Request/Response: Message is a response to the client/redirector
```

Citrix User Filer Access Error Details

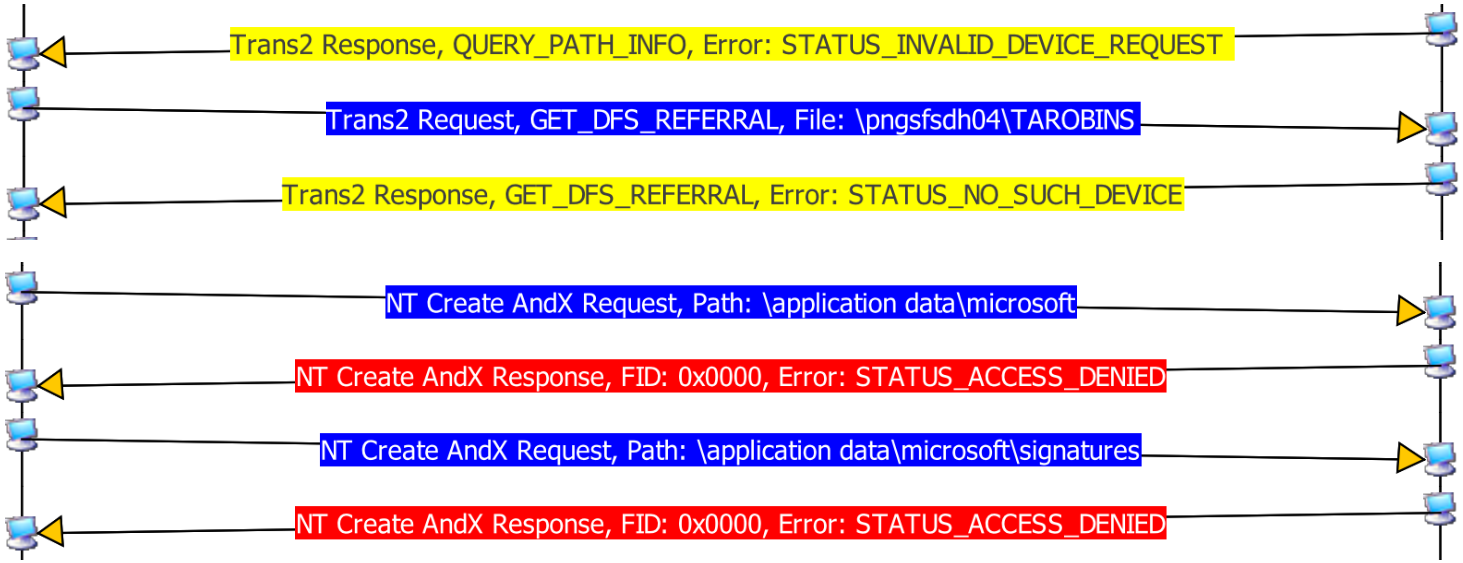
Some files are not found and searched across many drive mappings creating an abundance of frivolous traffic.

Some files are there but due to a variety of reasons, file rights assigned that user or machine are not accessible.

Others are not accessible due to the type of account due to incompatibilities between the Client choice to use AppSense for Microsoft Profile management with NetApp Filers. The complexities have made the installation of AppSense ineffective.

File access by multiple machines logging in at the same time needing to access the same files could cause this observed file locking.

We provided this to AppSense to ensure their upgrade addressed these manifestations.



Trans2 Response, QUERY_PATH_INFO, Error: STATUS_INVALID_DEVICE_REQUEST

Trans2 Request, GET_DFS_REFERRAL, File: \pngsfsdh04\TAROBINS

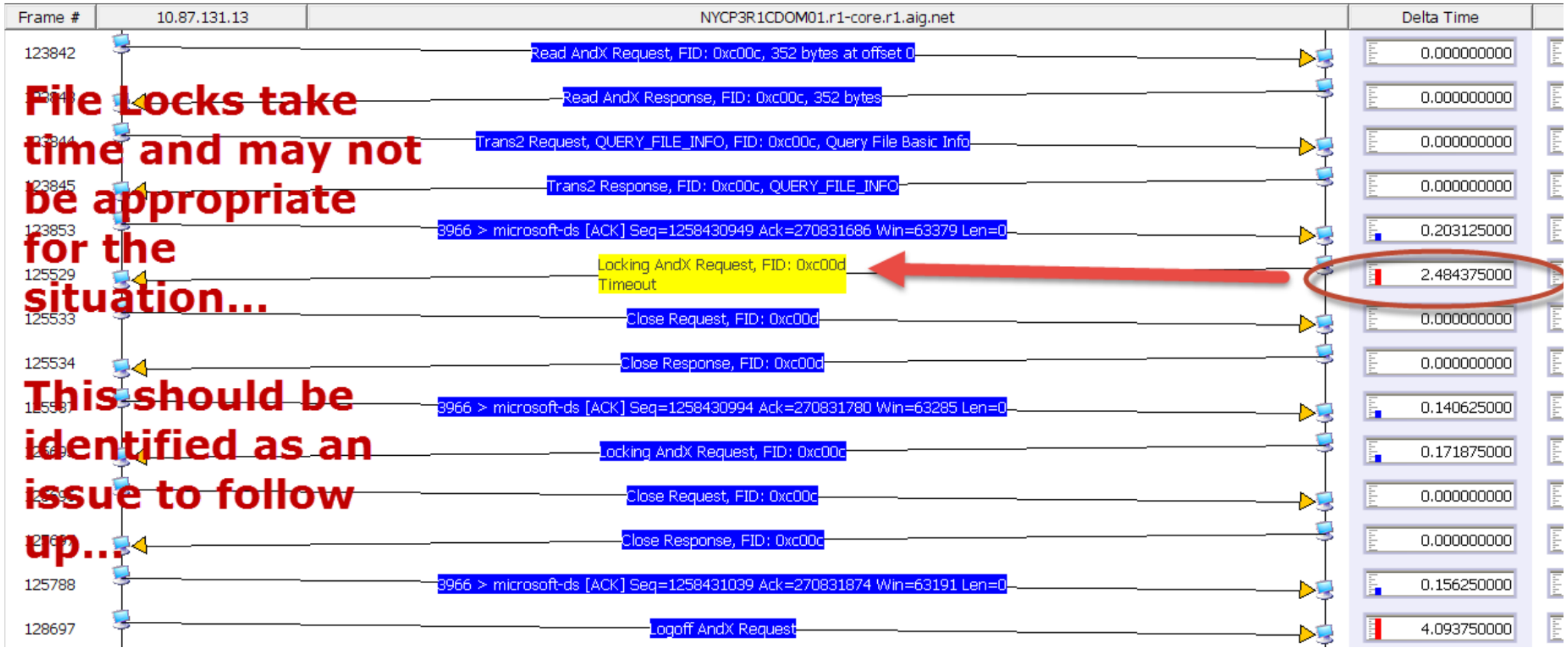
Trans2 Response, GET_DFS_REFERRAL, Error: STATUS_NO_SUCH_DEVICE

NT Create AndX Request, Path: \application data\microsoft

NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED

NT Create AndX Request, Path: \application data\microsoft\signatures

NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED



Frame #	10.87.131.13	NYCP3R1CDOM01.r1-core.r1.aig.net	Delta Time
123842		Read AndX Request, FID: 0xc00c, 352 bytes at offset 0	0.000000000
123843		Read AndX Response, FID: 0xc00c, 352 bytes	0.000000000
123844		Trans2 Request, QUERY_FILE_INFO, FID: 0xc00c, Query File Basic Info	0.000000000
123845		Trans2 Response, FID: 0xc00c, QUERY_FILE_INFO	0.000000000
123853		3966 > microsoft-ds [ACK] Seq=1258430949 Ack=270831686 Win=63379 Len=0	0.203125000
125529		Locking AndX Request, FID: 0xc00d Timeout	2.484375000
125533		Close Request, FID: 0xc00d	0.000000000
125534		Close Response, FID: 0xc00d	0.000000000
125537		3966 > microsoft-ds [ACK] Seq=1258430994 Ack=270831780 Win=63285 Len=0	0.140625000
[illegible]		Locking AndX Request, FID: 0xc00c	0.171875000
[illegible]		Close Request, FID: 0xc00c	0.000000000
125767		Close Response, FID: 0xc00c	0.000000000
125788		3966 > microsoft-ds [ACK] Seq=1258431039 Ack=270831874 Win=63191 Len=0	0.156250000
128697		Logoff AndX Request	4.093750000

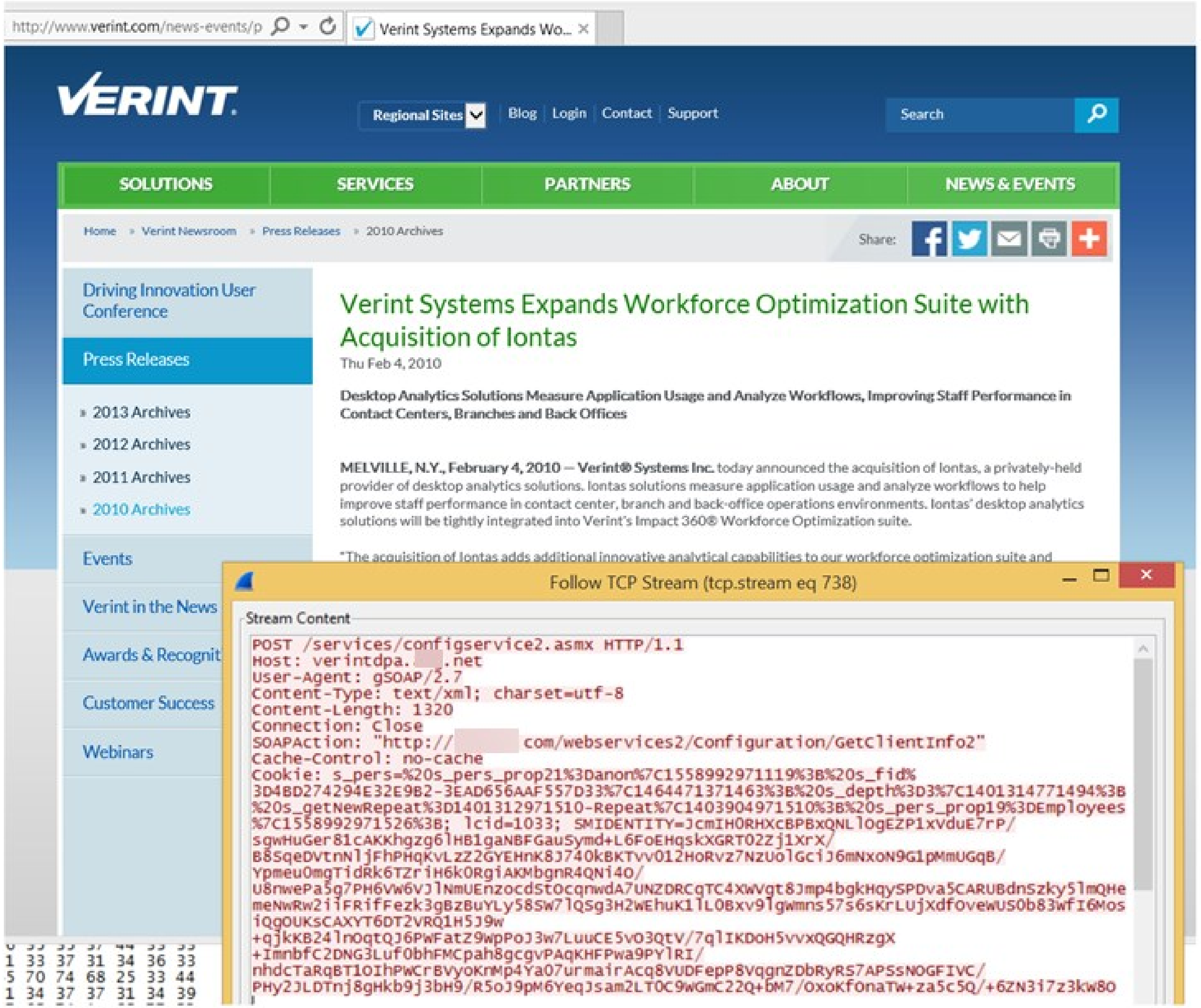
File Locks take time and may not be appropriate for the situation…

This should be identified as an issue to follow up…

2 Verint logging every users access to Outlook, Web activity degrading Citrix Performance

This exhibit helped Verint debug like logging was indeed turned on at some point in the past.

The logging was curtailed by configuration changes and assisted in incremental performance improvements.



Verint Systems Expands Workforce Optimization Suite with Acquisition of Iontas

Thu Feb 4, 2010

Desktop Analytics Solutions Measure Application Usage and Analyze Workflows, Improving Staff Performance in Contact Centers, Branches and Back Offices

MELVILLE, N.Y., February 4, 2010 — Verint® Systems Inc. today announced the acquisition of Iontas, a privately-held provider of desktop analytics solutions. Iontas solutions measure application usage and analyze workflows to help improve staff performance in contact center, branch and back-office operations environments. Iontas' desktop analytics solutions will be tightly integrated into Verint's Impact 360® Workforce Optimization suite.

"The acquisition of Iontas adds additional innovative analytical capabilities to our workforce optimization suite and

Follow TCP Stream (tcp.stream eq 738)

Stream Content

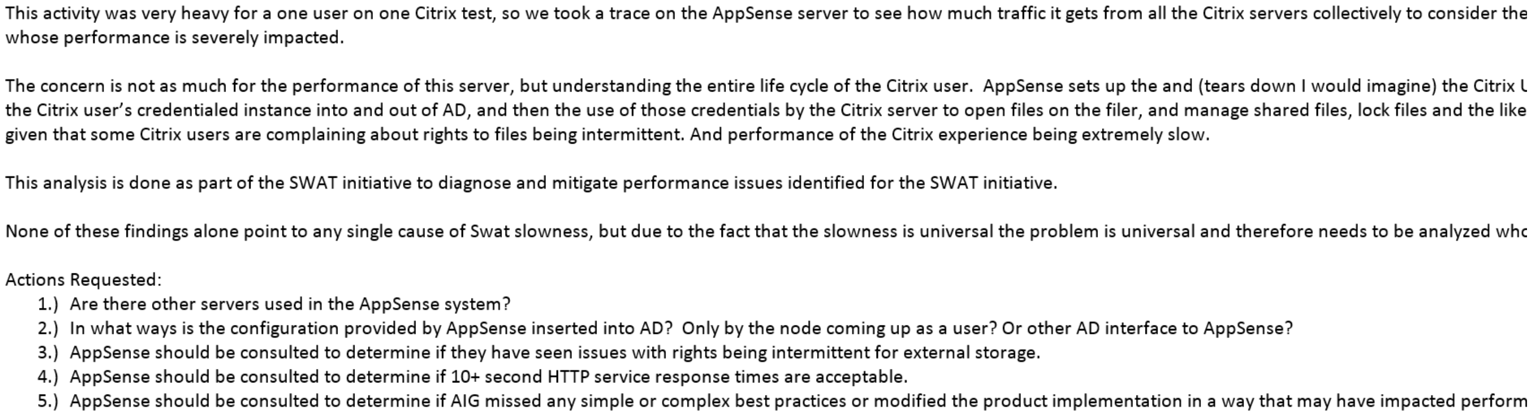
```
POST /services/configservice2.asmx HTTP/1.1
Host: verintdpa.[redacted].net
User-Agent: gSOAP/2.7
Content-Type: text/xml; charset=utf-8
Content-Length: 1320
Connection: close
SOAPAction: "http://[redacted] com/webservices2/Configuration/GetClientInfo2"
Cache-Control: no-cache
Cookie: s_pers=%20s_pers_prop21%3Danon%7C1558992971119%3B%20s_fid%
3D4BD274294E32E9B2-3EAD656AAF557D33%7C1464471371463%3B%20s_depth%3D3%7C1401314771494%3B
%20s_getNewRepeat%3D1401312971510-Repeat%7C1403904971510%3B%20s_pers_prop19%3DEmployees
%7C1558992971526%3B; lcid=1033; SMIDENTITY=JcmIHORHXCBPBxQNLlogEZP1xVduE7rP/
sgwHuGer81cAKKhgzg6lHB1gaNBFGauSymd+L6FoEHqskXGRT02Zj1XrX/
B8SqeDVtnNljFhPHqKvLzZ2GYEHnK8J740kBKTvv012HoRvz7NzUolGciJ6mNxON9G1pMmUGqB/
YpmeuOmgTidRk6TZriH6kORgiAKMbgnR4QNi4O/
U8nwePa5g7PH6Vw6VJlNmUEnzocdStOcqnwdA7UNZDRCqTC4XWVgt8Jmp4bgkHqySPDva5CARUBdnSzky5lmQHe
meNwRw2iiFRifFezk3gBzBuYLy58Sw7lQSg3H2wEhuK1lLOBxv9lgwmns57s6sKrLUjXdfOvewUSOb83wfI6Mos
iQgOUKsCAXYT6DT2VRQ1H5J9w
+qjkKB24lnOqtQJ6PWFatZ9WpPoJ3w7LuuCE5vO3QtV/7qlIKDoH5vvxQGQHRzgX
+ImnbfC2DNG3LufObhFMCpah8gcgvPAqKHFPwa9PYlRI/
nhdcTaRqBT1OIhPWCrBVyoKnMp4Ya07urmairAcq8VUDFepP8VqgnZDbRyRS7APSsNOGFIVC/
PHy2JLDTnj8gHkb9j3bH9/R5oJ9pM6YeqJsam2LTOC9WGmC22Q+bM7/OxoKfOnaTw+za5c5Q/+6ZN3i7z3kw8O
```

Server performance degradation pinpointed to AppSense logging

This analysis assisted Client getting AppSense support to assist with getting the debug logging turned off.

Without details vendors often can’s understand the problem and it continues for years of degraded performance and lost productive time for thousands of users.

It took many such examples and assertions to get the ball rolling with the vendor.



This activity was very heavy for a one user on one Citrix test, so we took a trace on the AppSense server to see how much traffic it gets from all the Citrix servers collectively to consider the whose performance is severely impacted.

The concern is not as much for the performance of this server, but understanding the entire life cycle of the Citrix user. AppSense sets up the and (tears down I would imagine) the Citrix U the Citrix user’s credentialed instance into and out of AD, and then the use of those credentials by the Citrix server to open files on the filer, and manage shared files, lock files and the like given that some Citrix users are complaining about rights to files being intermittent. And performance of the Citrix experience being extremely slow.

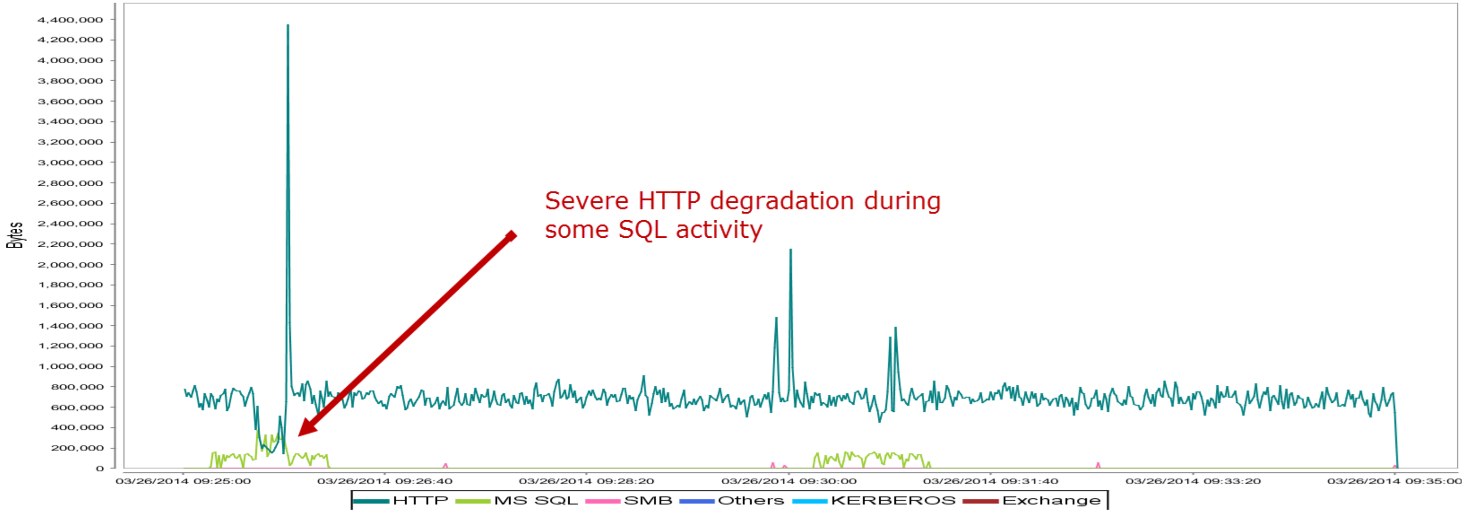
This analysis is done as part of the SWAT initiative to diagnose and mitigate performance issues identified for the SWAT initiative.

None of these findings alone point to any single cause of Swat slowness, but due to the fact that the slowness is universal the problem is universal and therefore needs to be analyzed whc

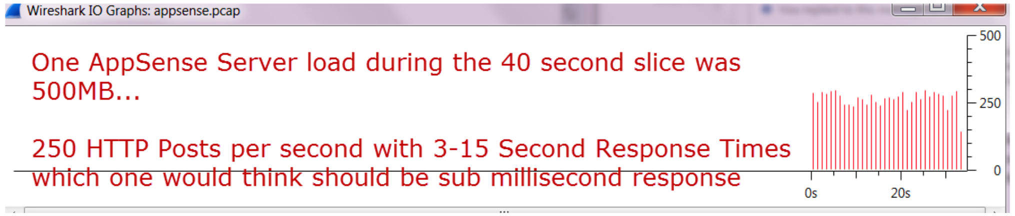
Actions Requested:

1.) Are there other servers used in the AppSense system?
2.) In what ways is the configuration provided by AppSense inserted into AD? Only by the node coming up as a user? Or other AD interface to AppSense?
3.) AppSense should be consulted to determine if they have seen issues with rights being intermittent for external storage.
4.) AppSense should be consulted to determine if 10+ second HTTP service response times are acceptable.
5.) AppSense should be consulted to determine if AIG missed any simple or complex best practices or modified the product implementation in a way that may have impacted perform

AppSense Server Performance for Citrix User Profile Configuration...



Severe HTTP degradation during some SQL activity

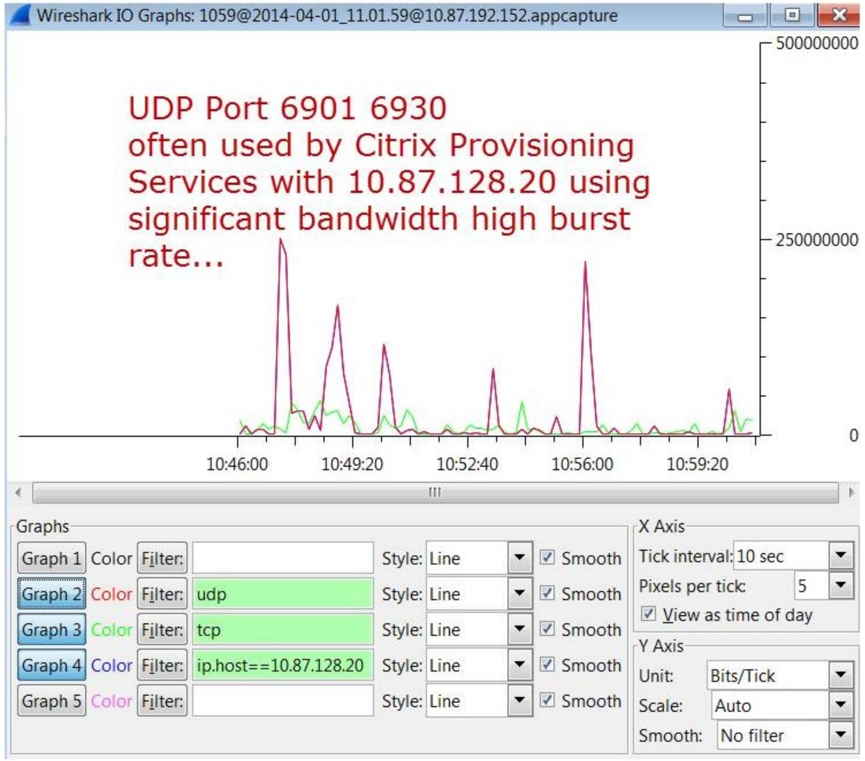


One AppSense Server load during the 40 second slice was 500MB…

250 HTTP Posts per second with 3-15 Second Response Times which one would think should be sub millisecond response

Citrix Uses TCP Port 69xx for provisioning

- Provisioning traffic is very heavy and considered normal by the Citrix team.
- We have seen server performance degraded severely during provisioning.
- Apparently this overhead is part of Citrix operations.


Wireshark IO Graphs: 1059@2014-04-01_11.01.59@10.87.192.152.appcapture
500000000
250000000
0
10:46:00
10:49:20
10:52:40
10:56:00
10:59:20

UDP Port 6901 6930 often used by Citrix Provisioning Services with 10.87.128.20 using significant bandwidth high burst rate...

Graphs

Graph 1 Color Filter: Style: Line ☑ Smooth

Graph 2 Color Filter: udp Style: Line ☑ Smooth

Graph 3 Color Filter: tcp Style: Line ☑ Smooth

Graph 4 Color Filter: ip.host==10.87.128.20 Style: Line ☑ Smooth

Graph 5 Color Filter: Style: Line ☑ Smooth

X Axis

Tick interval: 10 sec

Pixels per tick: 5

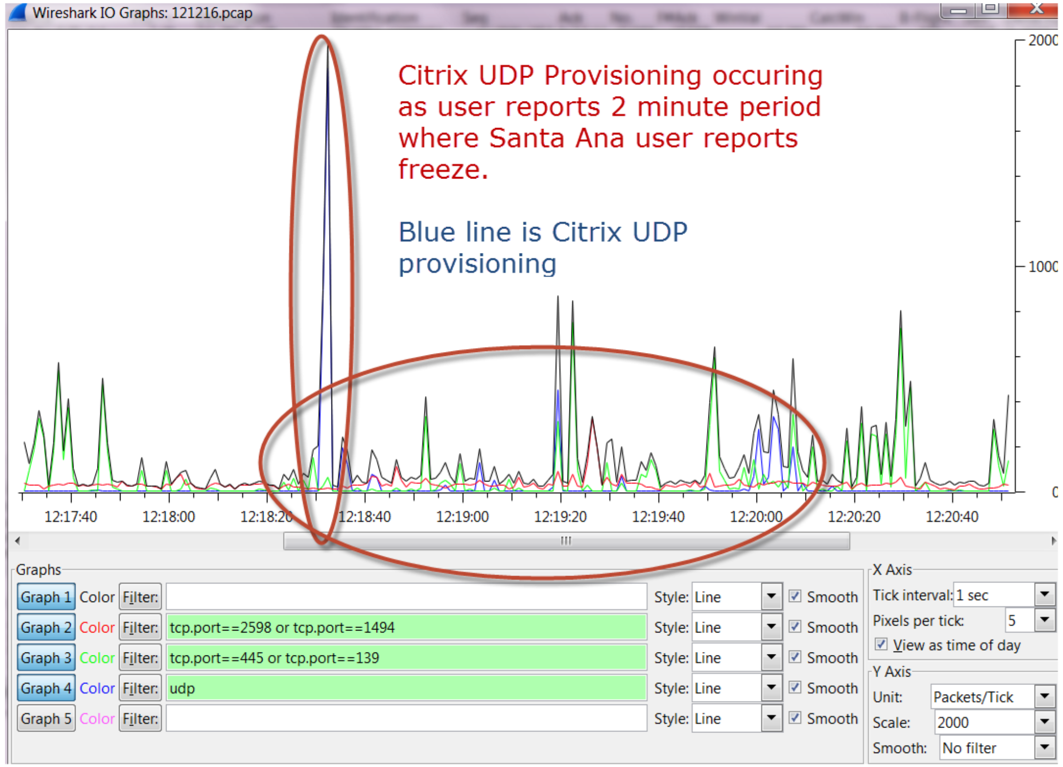
☑ View as time of day

Y Axis

Unit: Bits/Tick

Scale: Auto

Smooth: No filter



Citrix UDP Provisioning occuring as user reports 2 minute period where Santa Ana user reports freeze.

Blue line is Citrix UDP provisioning

Graphs

Graph 1 Color Filter: Style: Line ☑ Smooth

Graph 2 Color Filter: tcp.port==2598 or tcp.port==1494 Style: Line ☑ Smooth

Graph 3 Color Filter: tcp.port==445 or tcp.port==139 Style: Line ☑ Smooth

Graph 4 Color Filter: udp Style: Line ☑ Smooth

Graph 5 Color Filter: Style: Line ☑ Smooth

X Axis

Tick interval: 1 sec

Pixels per tick: 5

☑ View as time of day

Y Axis

Unit: Packets/Tick

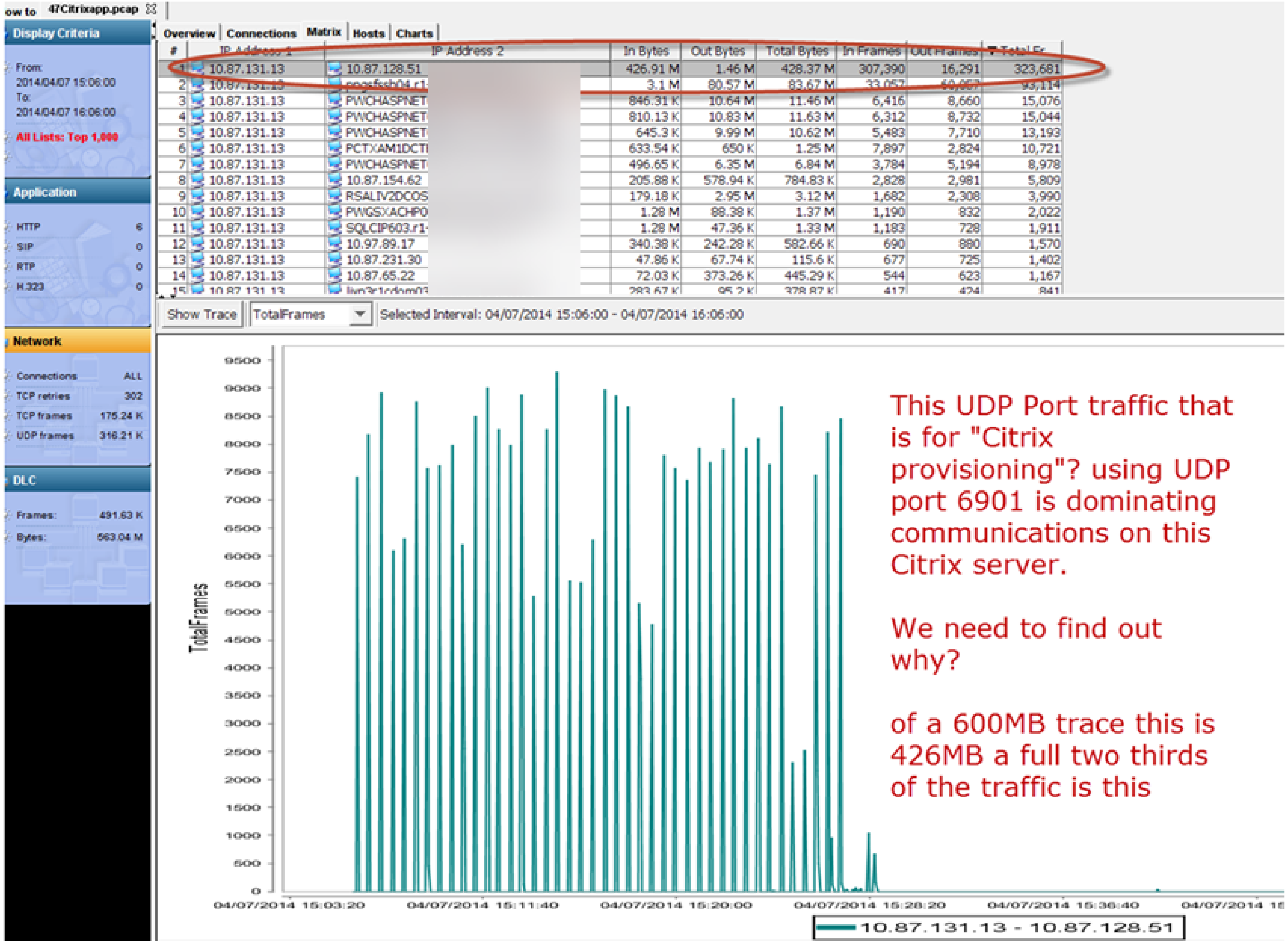
Scale: 2000

Smooth: No filter

Citrix provisioning traffic impact on network and servers

This shows the volume of traffic Citrix uses for PVS.

Again, this was said to be normal, but it was associated with a distinct user impacting server slowdown at this same timeframe.



From:
2014/04/07 15:06:00
To:
2014/04/07 16:06:00

All Lists: Top 1,000

HTTP	6
SIP	0
RTP	0
H.323	0

Connections	ALL
TCP retries	302
TCP frames	175.24 K
UDP frames	316.21 K

Frames:	491.63 K
Bytes:	563.04 M

#	IP Address 1	IP Address 2	In Bytes	Out Bytes	Total Bytes	In Frames	Out Frames	▼ Total Fr
1	10.87.131.13	10.87.128.51	426.91 M	1.46 M	428.37 M	307,390	16,291	323,681
2	10.87.131.13	ppgsfsb04.r1 [redacted]	3.1 M	80.57 M	83.67 M	33,057	60,057	93,114
3	10.87.131.13	PWCHASPNET [redacted]	846.31 K	10.64 M	11.46 M	6,416	8,660	15,076
4	10.87.131.13	PWCHASPNET [redacted]	810.13 K	10.83 M	11.63 M	6,312	8,732	15,044
5	10.87.131.13	PWCHASPNET [redacted]	645.3 K	9.99 M	10.62 M	5,483	7,710	13,193
6	10.87.131.13	PCTXAM1DCT [redacted]	633.54 K	650 K	1.25 M	7,897	2,824	10,721
7	10.87.131.13	PWCHASPNET [redacted]	496.65 K	6.35 M	6.84 M	3,784	5,194	8,978
8	10.87.131.13	10.87.154.62	205.88 K	578.94 K	784.83 K	2,828	2,981	5,809
9	10.87.131.13	RSALIV2DCOS [redacted]	179.18 K	2.95 M	3.12 M	1,682	2,308	3,990
10	10.87.131.13	PWGSXACHP0 [redacted]	1.28 M	88.38 K	1.37 M	1,190	832	2,022
11	10.87.131.13	SQLCIP603.r1- [redacted]	1.28 M	47.36 K	1.33 M	1,183	728	1,911
12	10.87.131.13	10.97.89.17	340.38 K	242.28 K	582.66 K	690	880	1,570
13	10.87.131.13	10.87.231.30	47.86 K	67.74 K	115.6 K	677	725	1,402
14	10.87.131.13	10.87.65.22	72.03 K	373.26 K	445.29 K	544	623	1,167
15	10.87.131.13	livp3r1cdom03 [redacted]	283.67 K	95.2 K	378.87 K	417	424	841

Selected Interval: 04/07/2014 15:06:00 - 04/07/2014 16:06:00

This UDP Port traffic that is for "Citrix provisioning"? using UDP port 6901 is dominating communications on this Citrix server.

We need to find out why?

of a 600MB trace this is 426MB a full two thirds of the traffic is this

Citrix Servers to NetApp Filers have long NT Notify times

NT Notify is an SMB command that allows a system to ask for notification of any changes to a file while it is in use by the user.

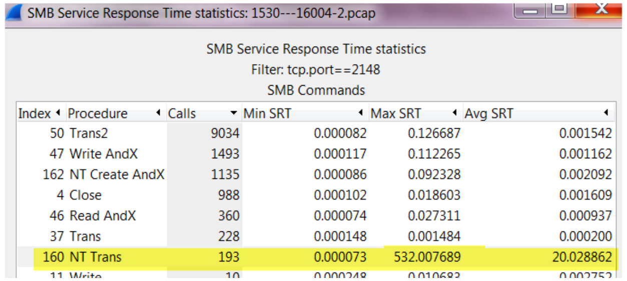
These commands cause SMB response times to seem long as a whole, and when deeper analysis is performed it is only the NT Notify transactions, which is an idiosyncrasy of operation.

Investigating very slow NT Notify responses… it apparently sets up a “watch” on a directory or file for a “change” and the Filer has to keep track and do this work.

Can you see what is said about these commands in NetApp support?

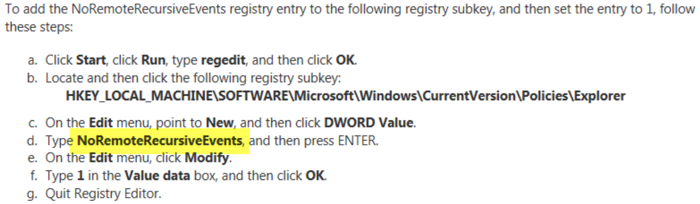
I found some things that note a degraded performance issue for XP and 2003 Server as clients…

Don’t think the kb is correct on many things… but does relate the slowness
http://support.microsoft.com/kb/885189



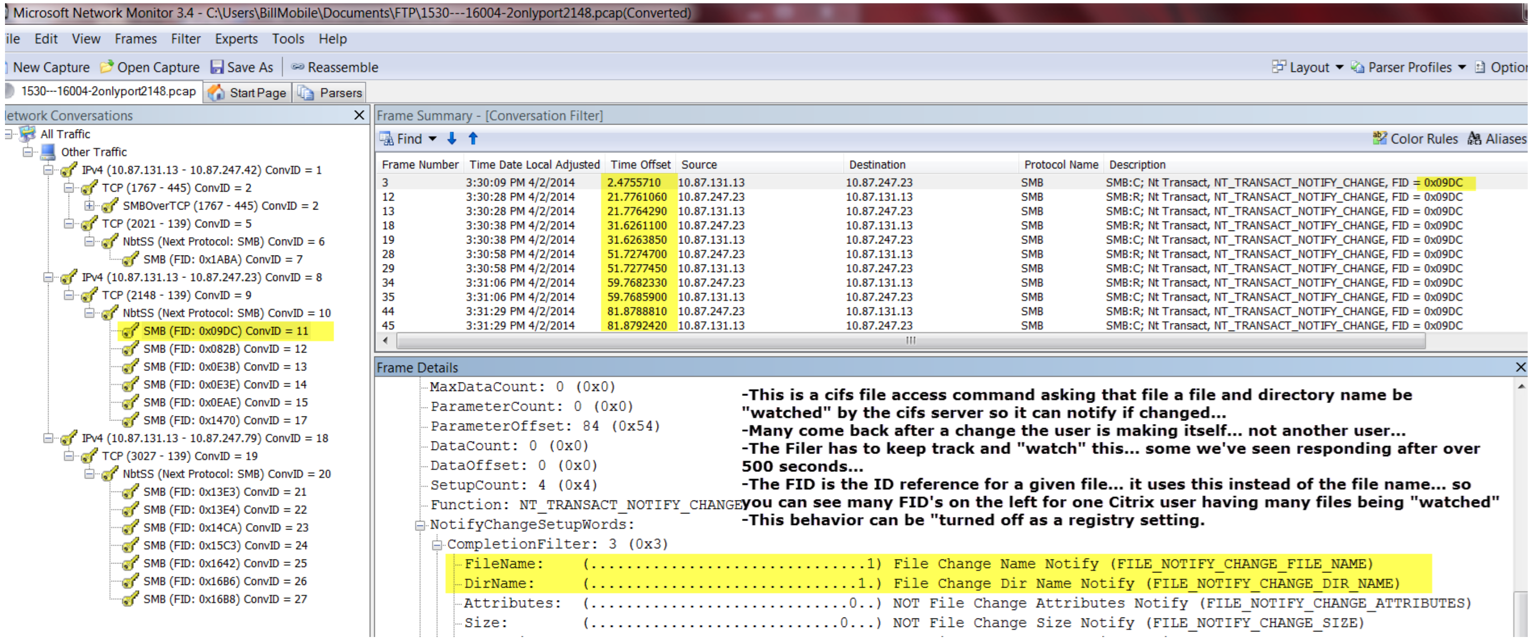
SMB Service Response Time statistics
Filter: tcp.port==2148
SMB Commands

Index	Procedure	Calls	Min SRT	Max SRT	Avg SRT
50	Trans2	9034	0.000082	0.126687	0.001542
47	Write AndX	1493	0.000117	0.112265	0.001162
162	NT Create AndX	1135	0.000086	0.092328	0.002092
4	Close	988	0.000102	0.018603	0.001609
46	Read AndX	360	0.000074	0.027311	0.000937
37	Trans	228	0.000148	0.001484	0.000200
160	NT Trans	193	0.000073	532.007689	20.028862
11	Write	10	0.000248	0.010683	0.002752



To add the NoRemoteRecursiveEvents registry entry to the following registry subkey, and then set the entry to 1, follow these steps:

a. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
b. Locate and then click the following registry subkey:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer
c. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
d. Type **NoRemoteRecursiveEvents**, and then press ENTER.
e. On the **Edit** menu, click **Modify**.
f. Type **1** in the **Value data** box, and then click **OK**.
g. Quit Registry Editor.


Microsoft Network Monitor 3.4 - C:\Users\BillMobile\Documents\FTP\1530---16004-2onlyport2148.pcap(Converted)
ile Edit View Frames Filter Experts Tools Help
New Capture Open Capture Save As Reassemble
Layout Parser Profiles Optior
1530---16004-2onlyport2148.pcap Start Page Parsers
letwork Conversations
Frame Summary - [Conversation Filter]
Find
Color Rules Aliases
Frame Details

```
All Traffic
  Other Traffic
    IPv4 (10.87.131.13 - 10.87.247.42) ConvID = 1
      TCP (1767 - 445) ConvID = 2
        SMBOverTCP (1767 - 445) ConvID = 2
      TCP (2021 - 139) ConvID = 5
        NbtSS (Next Protocol: SMB) ConvID = 6
          SMB (FID: 0x1ABA) ConvID = 7
    IPv4 (10.87.131.13 - 10.87.247.23) ConvID = 8
      TCP (2148 - 139) ConvID = 9
        NbtSS (Next Protocol: SMB) ConvID = 10
          SMB (FID: 0x09DC) ConvID = 11
          SMB (FID: 0x082B) ConvID = 12
          SMB (FID: 0x0E3B) ConvID = 13
          SMB (FID: 0x0E3E) ConvID = 14
          SMB (FID: 0x0EAE) ConvID = 15
          SMB (FID: 0x1470) ConvID = 17
    IPv4 (10.87.131.13 - 10.87.247.79) ConvID = 18
      TCP (3027 - 139) ConvID = 19
        NbtSS (Next Protocol: SMB) ConvID = 20
          SMB (FID: 0x13E3) ConvID = 21
          SMB (FID: 0x13E4) ConvID = 22
          SMB (FID: 0x14CA) ConvID = 23
          SMB (FID: 0x15C3) ConvID = 24
          SMB (FID: 0x1642) ConvID = 25
          SMB (FID: 0x16B6) ConvID = 26
          SMB (FID: 0x16B8) ConvID = 27
```

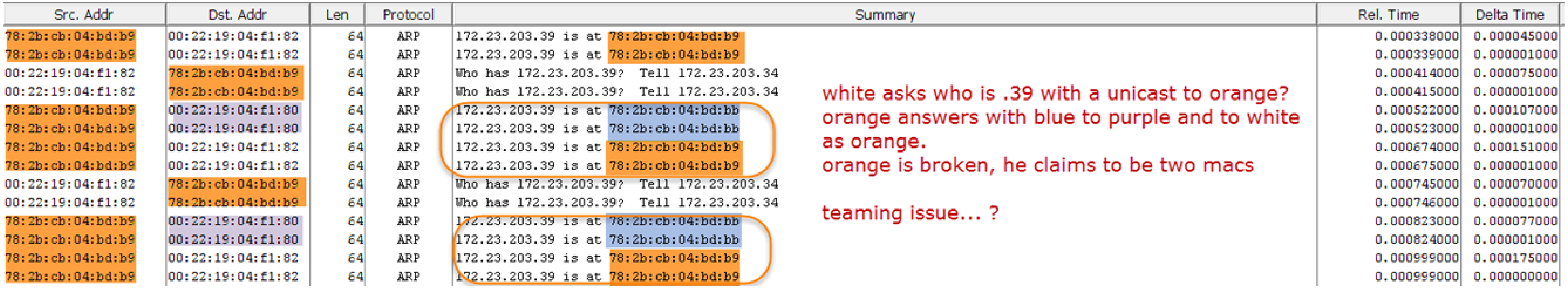
Frame Number	Time Date Local Adjusted	Time Offset	Source	Destination	Protocol Name	Description
3	3:30:09 PM 4/2/2014	2.4755710	10.87.131.13	10.87.247.23	SMB	SMB:C; Nt Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x09DC
12	3:30:28 PM 4/2/2014	21.7761060	10.87.247.23	10.87.131.13	SMB	SMB:R; Nt Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x09DC
13	3:30:28 PM 4/2/2014	21.7764290	10.87.131.13	10.87.247.23	SMB	SMB:C; Nt Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x09DC
18	3:30:38 PM 4/2/2014	31.6261100	10.87.247.23	10.87.131.13	SMB	SMB:R; Nt Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x09DC
19	3:30:38 PM 4/2/2014	31.6263850	10.87.131.13	10.87.247.23	SMB	SMB:C; Nt Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x09DC
28	3:30:58 PM 4/2/2014	51.7274700	10.87.247.23	10.87.131.13	SMB	SMB:R; Nt Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x09DC
29	3:30:58 PM 4/2/2014	51.7277450	10.87.131.13	10.87.247.23	SMB	SMB:C; Nt Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x09DC
34	3:31:06 PM 4/2/2014	59.7682330	10.87.247.23	10.87.131.13	SMB	SMB:R; Nt Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x09DC
35	3:31:06 PM 4/2/2014	59.7685900	10.87.131.13	10.87.247.23	SMB	SMB:C; Nt Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x09DC
44	3:31:29 PM 4/2/2014	81.8788810	10.87.247.23	10.87.131.13	SMB	SMB:R; Nt Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x09DC
45	3:31:29 PM 4/2/2014	81.8792420	10.87.131.13	10.87.247.23	SMB	SMB:C; Nt Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x09DC

```
  MaxDataCount:  0  (0x0)
  ParameterCount:  0  (0x0)
  ParameterOffset:  84  (0x54)
  DataCount:  0  (0x0)
  DataOffset:  0  (0x0)
  SetupCount:  4  (0x4)
  Function:  NT_TRANSACT_NOTIFY_CHANGE
  NotifyChangeSetupWords:
    CompletionFilter:  3  (0x3)
      FileName:     (...............................1)  File Change Name Notify (FILE_NOTIFY_CHANGE_FILE_NAME)
      DirName:      (..............................1.)  File Change Dir Name Notify (FILE_NOTIFY_CHANGE_DIR_NAME)
      Attributes:   (.............................0..)  NOT File Change Attributes Notify (FILE_NOTIFY_CHANGE_ATTRIBUTES)
      Size:         (............................0...)  NOT File Change Size Notify (FILE_NOTIFY_CHANGE_SIZE)
```

-This is a cifs file access command asking that file a file and directory name be "watched" by the cifs server so it can notify if changed...
-Many come back after a change the user is making itself... not another user...
-The Filer has to keep track and "watch" this... some we've seen responding after over 500 seconds...
-The FID is the ID reference for a given file... it uses this instead of the file name... so you can see many FID's on the left for one Citrix user having many files being "watched"
-This behavior can be "turned off as a registry setting.

ARP Analysis Methods

By setting the view options on the analyzer one can see both the ARP requester and the address requested and the address that replied to troubleshoot complex MAC ARP resolution problems



Src. Addr	Dst. Addr	Len	Protocol	Summary	Rel. Time	Delta Time
78:2b:cb:04:bd:b9	00:22:19:04:f1:82	64	ARP	172.23.203.39 is at 78:2b:cb:04:bd:b9	0.000338000	0.000045000
78:2b:cb:04:bd:b9	00:22:19:04:f1:82	64	ARP	172.23.203.39 is at 78:2b:cb:04:bd:b9	0.000339000	0.000001000
00:22:19:04:f1:82	78:2b:cb:04:bd:b9	64	ARP	Who has 172.23.203.39? Tell 172.23.203.34	0.000414000	0.000075000
00:22:19:04:f1:82	78:2b:cb:04:bd:b9	64	ARP	Who has 172.23.203.39? Tell 172.23.203.34	0.000415000	0.000001000
78:2b:cb:04:bd:b9	00:22:19:04:f1:80	64	ARP	172.23.203.39 is at 78:2b:cb:04:bd:bb	0.000522000	0.000107000
78:2b:cb:04:bd:b9	00:22:19:04:f1:80	64	ARP	172.23.203.39 is at 78:2b:cb:04:bd:bb	0.000523000	0.000001000
78:2b:cb:04:bd:b9	00:22:19:04:f1:82	64	ARP	172.23.203.39 is at 78:2b:cb:04:bd:b9	0.000674000	0.000151000
78:2b:cb:04:bd:b9	00:22:19:04:f1:82	64	ARP	172.23.203.39 is at 78:2b:cb:04:bd:b9	0.000675000	0.000001000
00:22:19:04:f1:82	78:2b:cb:04:bd:b9	64	ARP	Who has 172.23.203.39? Tell 172.23.203.34	0.000745000	0.000070000
00:22:19:04:f1:82	78:2b:cb:04:bd:b9	64	ARP	Who has 172.23.203.39? Tell 172.23.203.34	0.000746000	0.000001000
78:2b:cb:04:bd:b9	00:22:19:04:f1:80	64	ARP	172.23.203.39 is at 78:2b:cb:04:bd:bb	0.000823000	0.000077000
78:2b:cb:04:bd:b9	00:22:19:04:f1:80	64	ARP	172.23.203.39 is at 78:2b:cb:04:bd:bb	0.000824000	0.000001000
78:2b:cb:04:bd:b9	00:22:19:04:f1:82	64	ARP	172.23.203.39 is at 78:2b:cb:04:bd:b9	0.000999000	0.000175000
78:2b:cb:04:bd:b9	00:22:19:04:f1:82	64	ARP	172.23.203.39 is at 78:2b:cb:04:bd:b9	0.000999000	0.000000000

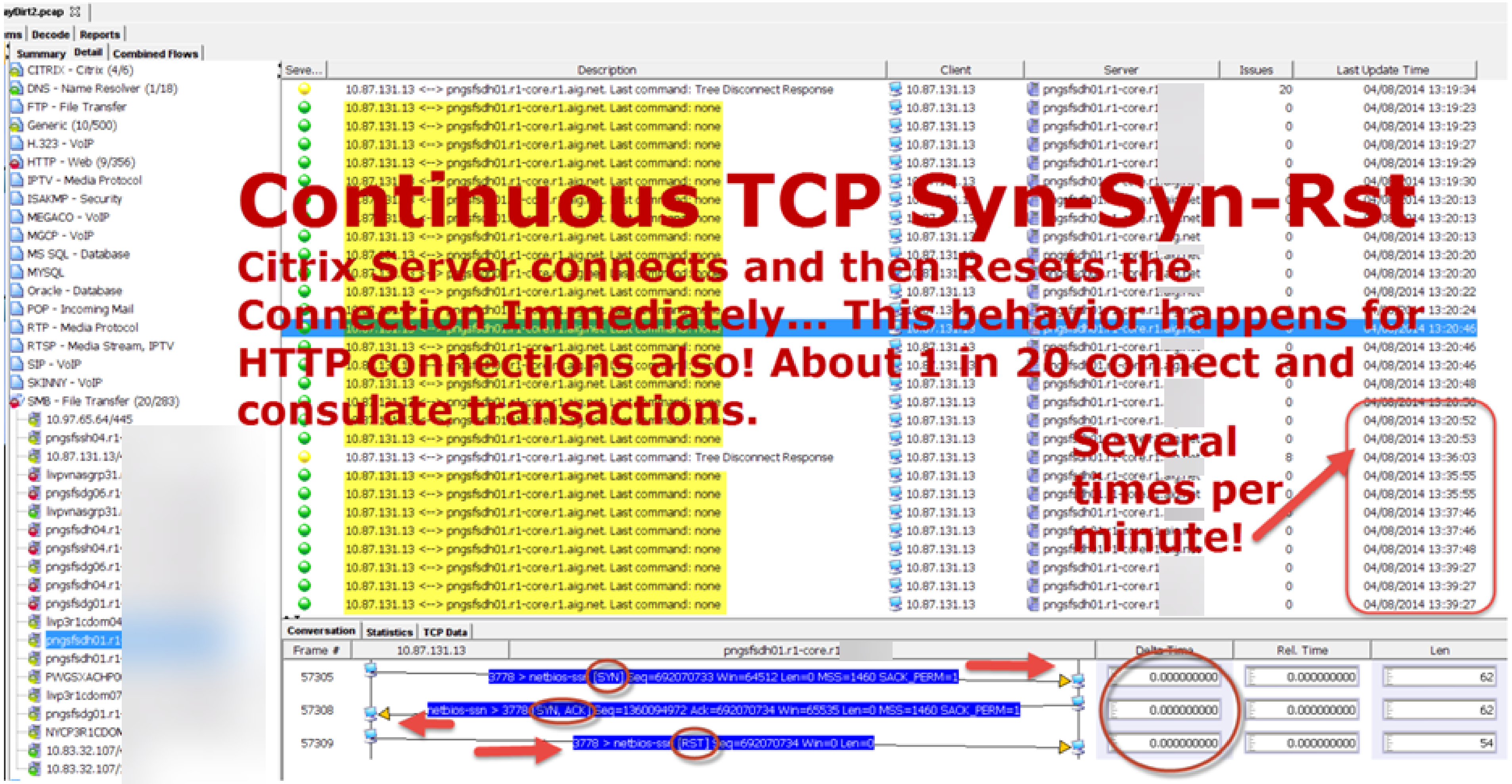
white asks who is .39 with a unicast to orange?
orange answers with blue to purple and to white as orange.
orange is broken, he claims to be two macs

teaming issue... ?

Citrix User Performance Symptoms

These TCP Syn-Syn-Resets are sometimes due to SMB Requests that Microsoft asserts are due to checking alternate ports for file access between 139 and 445 or when to the Proxy server to the Internet are due to Proxy server problems.

The exhibit helps to identify the behavior.



ayDirt2.pcap

ms | Decode | Reports

Summary | Detail | Combined Flows

- CITRIX - Citrix (4/6)
- DNS - Name Resolver (1/18)
- FTP - File Transfer
- Generic (10/500)
- H.323 - VoIP
- HTTP - Web (9/356)
- IPTV - Media Protocol
- ISAKMP - Security
- MEGACO - VoIP
- MGCP - VoIP
- MS SQL - Database
- MYSQL
- Oracle - Database
- POP - Incoming Mail
- RTP - Media Protocol
- RTSP - Media Stream, IPTV
- SIP - VoIP
- SKINNY - VoIP
- SMB - File Transfer (20/283)
  - 10.97.65.64/445
  - pngsfssh04.r1- [redacted]
  - 10.87.131.13/
  - livpvnasgrp31.
  - pngsfsdg06.r1-
  - livpvnasgrp31.
  - pngsfsdh04.r1-
  - pngsfssh04.r1-
  - pngsfsdg06.r1-
  - pngsfsdh04.r1-
  - pngsfsdg01.r1-
  - livp3r1cdom04
  - pngsfsdh01.r1
  - pngsfsdh01.r1-
  - PWGSXACHP0
  - livp3r1cdom07
  - pngsfsdg01.r1-
  - NYCP3R1CDOM
  - 10.83.32.107/
  - 10.83.32.107/

Seve...	Description	Client	Server	Issues	Last Update Time
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.13	pngsfsdh01.r1-core.r1 [redacted]	20	04/08/2014 13:19:34
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	pngsfsdh01.r1-core.r1 [redacted]	0	04/08/2014 13:19:23
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	pngsfsdh01.r1-core.r1 [redacted]	0	04/08/2014 13:19:23
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	pngsfsdh01.r1-core.r1 [redacted]	0	04/08/2014 13:19:27
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	pngsfsdh01.r1-core.r1 [redacted]	0	04/08/2014 13:19:29
●	10.87.131 [illegible] pngsfsdh01.r1-core.r1.aig.net. Last command: none	[illegible]	pngsfsdh01 [illegible]	[illegible]	04/0[illegible]014 13:19:30
●	[illegible] none	[illegible]	[illegible] net	[illegible]	[illegible]014 13:20:13
●	[illegible] none	[illegible]	[illegible] net	[illegible]	[illegible]014 13:20:13
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.1[illegible]	pngsfsdh01.r1-core.r1[illegible]g.net	0	04/08/2014 13:20:13
●	10.87 [illegible]	10.87.131 [illegible]	[illegible]	0	04/08/2014 13:20:20
●	[illegible]	[illegible]	[illegible]	0	04/08/2014 13:20:20
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	pngsfsdh01.r1-core.r1 [redacted]	0	04/08/2014 13:20:22
●	[illegible]	[illegible]	[illegible]	[illegible]	[illegible] 13:20:24
●	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]14 13:20:46
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	pngsfsdh01.r1-core.r1 [redacted]	0	04/08/2014 13:20:46
●	[illegible]	10.87.131.13	[illegible]	[illegible]	04/08/2014 13:20:46
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	pngsfsdh01.r1-core.r1. [redacted]	0	04/08/2014 13:20:48
●	[illegible]	10.87.131.13	pngsfsdh01.r1-core.r1. [redacted]	0	04/08/2014 13:20:50
●	[illegible]	10.87.131.13	pngsfsdh01.r1-core.r1. [redacted]	0	04/08/2014 13:20:52
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	[illegible]	0	04/08/2014 13:20:53
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.13	[illegible]	8	04/08/2014 13:36:03
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	[illegible]	0	04/08/2014 13:35:55
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	[illegible]	0	04/08/2014 13:35:55
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	pngsfsdh01.r1-core.r1. [redacted]	[illegible]	04/08/2014 13:37:46
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	[illegible]	0	04/08/2014 13:37:46
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	[illegible]	0	04/08/2014 13:37:48
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	pngsfsdh01.r1-core.r1 [redacted]	0	04/08/2014 13:39:27
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	pngsfsdh01.r1-core.r1 [redacted]	0	04/08/2014 13:39:27
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	pngsfsdh01.r1-core.r1 [redacted]	0	04/08/2014 13:39:27

Conversation | Statistics | TCP Data

Frame #	10.87.131.13	pngsfsdh01.r1-core.r1 [redacted]	Delta Time	Rel. Time	Len
57305	3778 > netbios-ssn [SYN] Seq=692070733 Win=64512 Len=0 MSS=1460 SACK_PERM=1		0.000000000	0.000000000	62
57308	netbios-ssn > 3778 [SYN, ACK] Seq=1360094972 Ack=692070734 Win=65535 Len=0 MSS=1460 SACK_PERM=1		0.000000000	0.000000000	62
57309	3778 > netbios-ssn [RST] Seq=692070734 Win=0 Len=0		0.000000000	0.000000000	54

Continuous TCP Syn-Syn-Rst

Citrix Server connects and then Resets the Connection Immediately… This behavior happens for HTTP connections also! About 1 in 20 connect and consulate transactions.

Several times per minute!

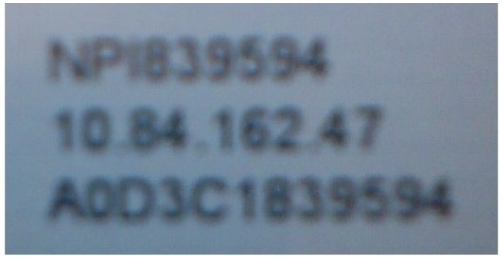
Printing Issues

Printing slowness caused us to look for problems at the deep packet inspection level.

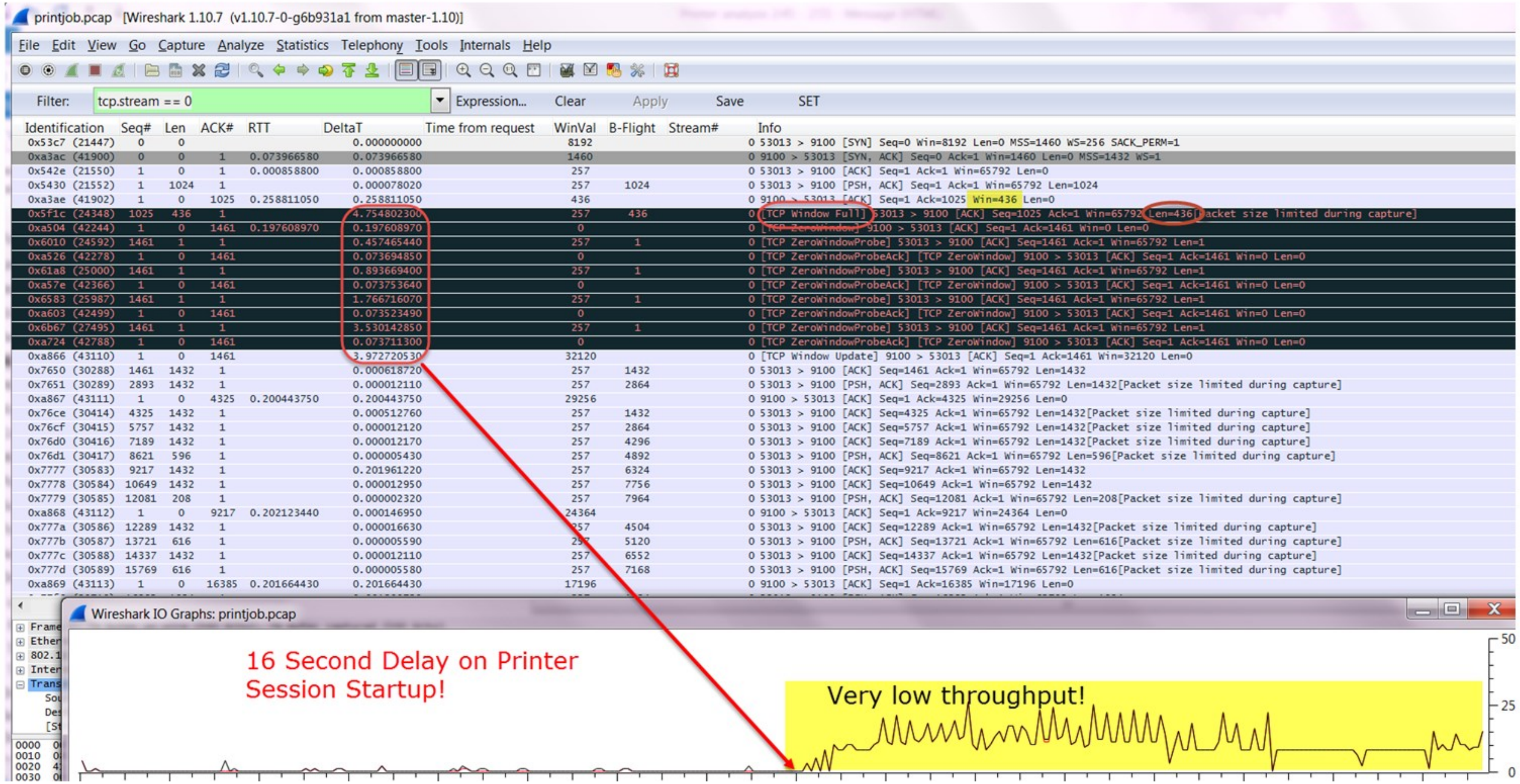
As a result of these evidentiary exhibits which had to be asserted aggressively to Client and HP personnel until acceptance of the problems were accepted.

Once evidence was accepted HP started to truly move to solve these managed print problems saving thousands of users hours printing.

Big Win that would not have happened without exacting evidence and assertion.



NPI839594
10.84.162.47
A0D3C1839594



printjob.pcap [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save SET

Filter: tcp.stream == 0

Identification	Seq#	Len	ACK#	RTT	DeltaT	Time from request	WinVal	B-Flight	Stream#	Info
0x53c7 (21447)	0	0			0.000000000		8192		0	53013 > 9100 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
0xa3ac (41900)	0	0	1	0.073966580	0.073966580		1460		0	9100 > 53013 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1432 WS=1
0x542e (21550)	1	0	1	0.000858800	0.000858800		257		0	53013 > 9100 [ACK] Seq=1 Ack=1 Win=65792 Len=0
0x5430 (21552)	1	1024	1		0.000078020		257	1024	0	53013 > 9100 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=1024
0xa3ae (41902)	1	0	1025	0.258811050	0.258811050		436		0	9100 > 53013 [ACK] Seq=1 Ack=1025 Win=436 Len=0
0x5f1c (24348)	1025	436	1		4.754802300		257	436	0	[TCP Window Full] 53013 > 9100 [ACK] Seq=1025 Ack=1 Win=65792 Len=436[Packet size limited during capture]
0xa504 (42244)	1	0	1461	0.197608970	0.197608970		0		0	[TCP ZeroWindow] 9100 > 53013 [ACK] Seq=1 Ack=1461 Win=0 Len=0
0x6010 (24592)	1461	1	1		0.457465440		257	1	0	[TCP ZeroWindowProbe] 53013 > 9100 [ACK] Seq=1461 Ack=1 Win=65792 Len=1
0xa526 (42278)	1	0	1461		0.073694850		0		0	[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 9100 > 53013 [ACK] Seq=1 Ack=1461 Win=0 Len=0
0x61a8 (25000)	1461	1	1		0.893669400		257	1	0	[TCP ZeroWindowProbe] 53013 > 9100 [ACK] Seq=1461 Ack=1 Win=65792 Len=1
0xa57e (42366)	1	0	1461		0.073753640		0		0	[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 9100 > 53013 [ACK] Seq=1 Ack=1461 Win=0 Len=0
0x6583 (25987)	1461	1	1		1.766716070		257	1	0	[TCP ZeroWindowProbe] 53013 > 9100 [ACK] Seq=1461 Ack=1 Win=65792 Len=1
0xa603 (42499)	1	0	1461		0.073523490		0		0	[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 9100 > 53013 [ACK] Seq=1 Ack=1461 Win=0 Len=0
0x6b67 (27495)	1461	1	1		3.530142850		257	1	0	[TCP ZeroWindowProbe] 53013 > 9100 [ACK] Seq=1461 Ack=1 Win=65792 Len=1
0xa724 (42788)	1	0	1461		0.073711300		0		0	[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 9100 > 53013 [ACK] Seq=1 Ack=1461 Win=0 Len=0
0xa866 (43110)	1	0	1461		3.972720530		32120		0	[TCP Window Update] 9100 > 53013 [ACK] Seq=1 Ack=1461 Win=32120 Len=0
0x7650 (30288)	1461	1432	1		0.000618720		257	1432	0	53013 > 9100 [ACK] Seq=1461 Ack=1 Win=65792 Len=1432
0x7651 (30289)	2893	1432	1		0.000012110		257	2864	0	53013 > 9100 [PSH, ACK] Seq=2893 Ack=1 Win=65792 Len=1432[Packet size limited during capture]
0xa867 (43111)	1	0	4325	0.200443750	0.200443750		29256		0	9100 > 53013 [ACK] Seq=1 Ack=4325 Win=29256 Len=0
0x76ce (30414)	4325	1432	1		0.000512760		257	1432	0	53013 > 9100 [ACK] Seq=4325 Ack=1 Win=65792 Len=1432[Packet size limited during capture]
0x76cf (30415)	5757	1432	1		0.000012120		257	2864	0	53013 > 9100 [ACK] Seq=5757 Ack=1 Win=65792 Len=1432[Packet size limited during capture]
0x76d0 (30416)	7189	1432	1		0.000012170		257	4296	0	53013 > 9100 [ACK] Seq=7189 Ack=1 Win=65792 Len=1432[Packet size limited during capture]
0x76d1 (30417)	8621	596	1		0.000005430		257	4892	0	53013 > 9100 [PSH, ACK] Seq=8621 Ack=1 Win=65792 Len=596[Packet size limited during capture]
0x7777 (30583)	9217	1432	1		0.201961220		257	6324	0	53013 > 9100 [ACK] Seq=9217 Ack=1 Win=65792 Len=1432
0x7778 (30584)	10649	1432	1		0.000012950		257	7756	0	53013 > 9100 [ACK] Seq=10649 Ack=1 Win=65792 Len=1432
0x7779 (30585)	12081	208	1		0.000002320		257	7964	0	53013 > 9100 [PSH, ACK] Seq=12081 Ack=1 Win=65792 Len=208[Packet size limited during capture]
0xa868 (43112)	1	0	9217	0.202123440	0.000146950		24364		0	9100 > 53013 [ACK] Seq=1 Ack=9217 Win=24364 Len=0
0x777a (30586)	12289	1432	1		0.000016630		257	4504	0	53013 > 9100 [ACK] Seq=12289 Ack=1 Win=65792 Len=1432[Packet size limited during capture]
0x777b (30587)	13721	616	1		0.000005590		257	5120	0	53013 > 9100 [PSH, ACK] Seq=13721 Ack=1 Win=65792 Len=616[Packet size limited during capture]
0x777c (30588)	14337	1432	1		0.000012110		257	6552	0	53013 > 9100 [ACK] Seq=14337 Ack=1 Win=65792 Len=1432[Packet size limited during capture]
0x777d (30589)	15769	616	1		0.000005580		257	7168	0	53013 > 9100 [PSH, ACK] Seq=15769 Ack=1 Win=65792 Len=616[Packet size limited during capture]
0xa869 (43113)	1	0	16385	0.201664430	0.201664430		17196		0	9100 > 53013 [ACK] Seq=1 Ack=16385 Win=17196 Len=0

Wireshark IO Graphs: printjob.pcap

16 Second Delay on Printer Session Startup!

Very low throughput!

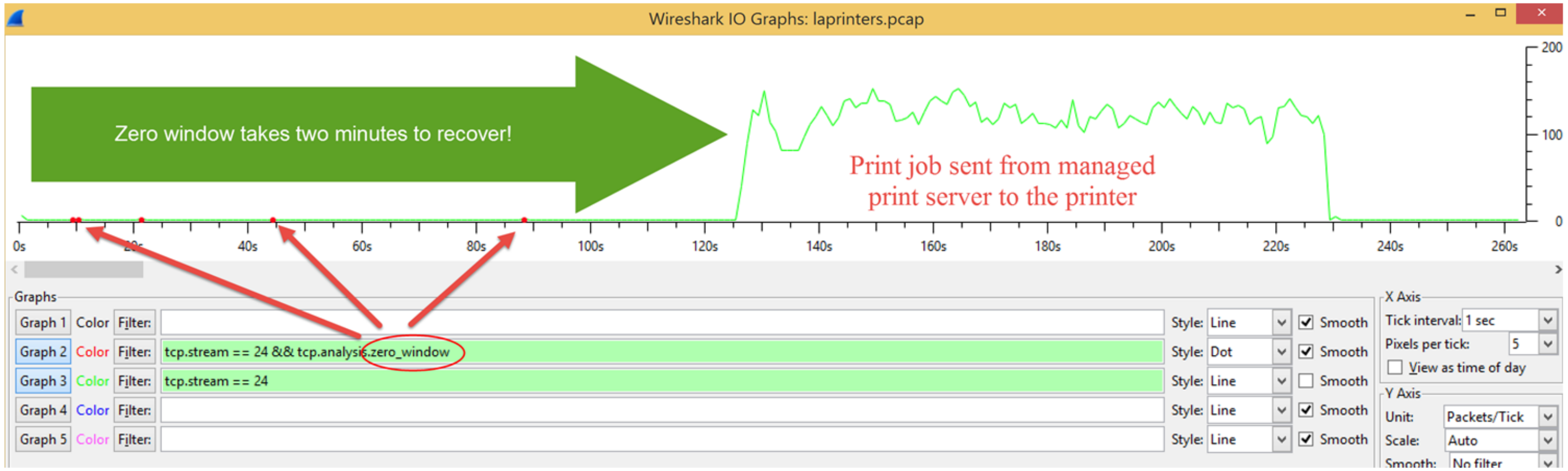
Printing Issues

Zero windows due to a bad HP protocol stack was the beginning of getting HP to escalate the managed print performance problems.

Without this evidence these problems and other associated problems would likely still exist.

Managed Print Delays

The printers are sending TCP zero window notices to the managed print servers delaying many print jobs by two minutes. This needs to be addressed by Hewlett-Packard. Perhaps a printer network driver problem exists or some type of local printer application has no buffering.



Zero window takes two minutes to recover!

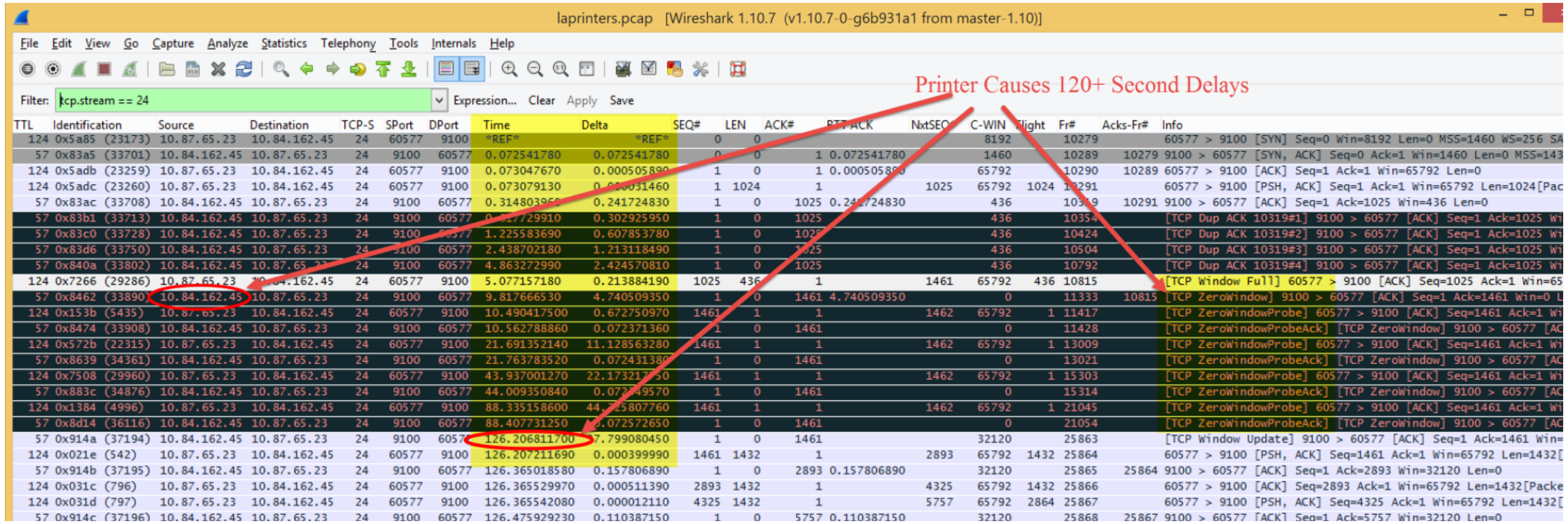
Print job sent from managed print server to the printer

Graphs

Graph 1	Color	Filter:		Style: Line	☑ Smooth
Graph 2	Color	Filter:	tcp.stream == 24 && tcp.analysis.zero_window	Style: Dot	☑ Smooth
Graph 3	Color	Filter:	tcp.stream == 24	Style: Line	□ Smooth
Graph 4	Color	Filter:		Style: Line	☑ Smooth
Graph 5	Color	Filter:		Style: Line	☑ Smooth

X Axis
Tick interval: 1 sec
Pixels per tick: 5
□ View as time of day

Y Axis
Unit: Packets/Tick
Scale: Auto
Smooth: No filter



Printer Causes 120+ Second Delays

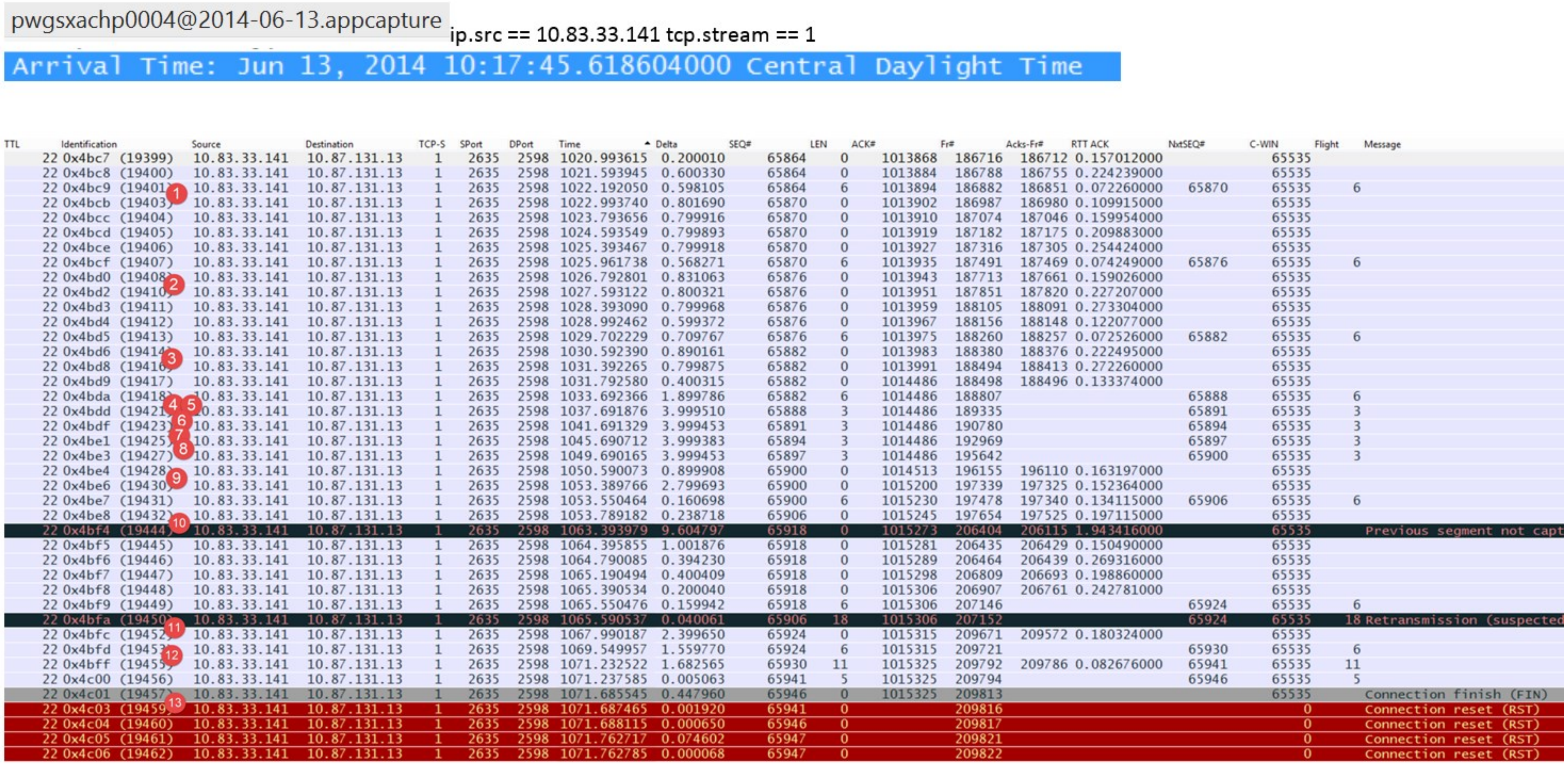
Filter: tcp.stream == 24

```
TTL Identification Source       Destination  TCP-S SPort DPort Time         Delta        SEQ#  LEN  ACK#  RTT ACK     NxtSEQ C-WIN flight Fr#   Acks-Fr# Info
124 0x5a85 (23173) 10.87.65.23  10.84.162.45  24  60577  9100 *REF*               *REF*     0    0                            8192         10279          60577 > 9100 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
 57 0x83a5 (33701) 10.84.162.45 10.87.65.23   24   9100 60577 0.072541780   0.072541780     0    0     1 0.072541780        1460         10289    10279 9100 > 60577 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=143
124 0x5adb (23259) 10.87.65.23  10.84.162.45  24  60577  9100 0.073047670   0.000505890     1    0     1 0.000505890       65792         10290    10289 60577 > 9100 [ACK] Seq=1 Ack=1 Win=65792 Len=0
124 0x5adc (23260) 10.87.65.23  10.84.162.45  24  60577  9100 0.073079130   0.000031460     1 1024     1              1025 65792  1024  10291          60577 > 9100 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=1024[Pac
 57 0x83ac (33708) 10.84.162.45 10.87.65.23   24   9100 60577 0.314803960   0.241724830     1    0  1025 0.241724830         436         10319    10291 9100 > 60577 [ACK] Seq=1 Ack=1025 Win=436 Len=0
 57 0x83b1 (33713) 10.84.162.45 10.87.65.23   24   9100 60577 0.617729910   0.302925950     1    0  1025                     436         10354          [TCP Dup ACK 10319#1] 9100 > 60577 [ACK] Seq=1 Ack=1025 Wi
 57 0x83c0 (33728) 10.84.162.45 10.87.65.23   24   9100 60577 1.225583690   0.607853780     1    0  1025                     436         10424          [TCP Dup ACK 10319#2] 9100 > 60577 [ACK] Seq=1 Ack=1025 Wi
 57 0x83d6 (33750) 10.84.162.45 10.87.65.23   24   9100 60577 2.438702180   1.213118490     1    0  1025                     436         10504          [TCP Dup ACK 10319#3] 9100 > 60577 [ACK] Seq=1 Ack=1025 Wi
 57 0x840a (33802) 10.84.162.45 10.87.65.23   24   9100 60577 4.863272990   2.424570810     1    0  1025                     436         10792          [TCP Dup ACK 10319#4] 9100 > 60577 [ACK] Seq=1 Ack=1025 Wi
124 0x7266 (29286) 10.87.65.23  10.84.162.45  24  60577  9100 5.077157180   0.213884190  1025  436     1              1461 65792   436  10815          [TCP Window Full] 60577 > 9100 [ACK] Seq=1025 Ack=1 Win=65
 57 0x8462 (33890) 10.84.162.45 10.87.65.23   24   9100 60577 9.817666530   4.740509350     1    0  1461 4.740509350           0         11333    10815 [TCP ZeroWindow] 9100 > 60577 [ACK] Seq=1 Ack=1461 Win=0 L
124 0x153b (5435)  10.87.65.23  10.84.162.45  24  60577  9100 10.490417500  0.672750970  1461    1     1              1462 65792     1  11417          [TCP ZeroWindowProbe] 60577 > 9100 [ACK] Seq=1461 Ack=1 Wi
 57 0x8474 (33908) 10.84.162.45 10.87.65.23   24   9100 60577 10.562788860  0.072371360     1    0  1461                       0         11428          [TCP ZeroWindowProbeAck] [TCP ZeroWindow] 9100 > 60577 [AC
124 0x572b (22315) 10.87.65.23  10.84.162.45  24  60577  9100 21.691352140 11.128563280  1461    1     1              1462 65792     1  13009          [TCP ZeroWindowProbe] 60577 > 9100 [ACK] Seq=1461 Ack=1 Wi
 57 0x8639 (34361) 10.84.162.45 10.87.65.23   24   9100 60577 21.763783520  0.072431380     1    0  1461                       0         13021          [TCP ZeroWindowProbeAck] [TCP ZeroWindow] 9100 > 60577 [AC
124 0x7508 (29960) 10.87.65.23  10.84.162.45  24  60577  9100 43.937001270 22.173217750  1461    1     1              1462 65792     1  15303          [TCP ZeroWindowProbe] 60577 > 9100 [ACK] Seq=1461 Ack=1 Wi
 57 0x883c (34876) 10.84.162.45 10.87.65.23   24   9100 60577 44.009350840  0.072349570     1    0  1461                       0         15314          [TCP ZeroWindowProbeAck] [TCP ZeroWindow] 9100 > 60577 [AC
124 0x1384 (4996)  10.87.65.23  10.84.162.45  24  60577  9100 88.335158600 44.325807760  1461    1     1              1462 65792     1  21045          [TCP ZeroWindowProbe] 60577 > 9100 [ACK] Seq=1461 Ack=1 Wi
 57 0x8d14 (36116) 10.84.162.45 10.87.65.23   24   9100 60577 88.407731250  0.072572650     1    0  1461                       0         21054          [TCP ZeroWindowProbeAck] [TCP ZeroWindow] 9100 > 60577 [AC
 57 0x914a (37194) 10.84.162.45 10.87.65.23   24   9100 60577 126.206811700 37.799080450     1    0  1461                   32120         25863          [TCP Window Update] 9100 > 60577 [ACK] Seq=1 Ack=1461 Win=
124 0x021e (542)   10.87.65.23  10.84.162.45  24  60577  9100 126.207211690  0.000399990  1461 1432     1              2893 65792  1432  25864          60577 > 9100 [PSH, ACK] Seq=1461 Ack=1 Win=65792 Len=1432[
 57 0x914b (37195) 10.84.162.45 10.87.65.23   24   9100 60577 126.365018580  0.157806890     1    0  2893 0.157806890       32120         25865    25864 9100 > 60577 [ACK] Seq=1 Ack=2893 Win=32120 Len=0
124 0x031c (796)   10.87.65.23  10.84.162.45  24  60577  9100 126.365529970  0.000511390  2893 1432     1              4325 65792  1432  25866          60577 > 9100 [ACK] Seq=2893 Ack=1 Win=65792 Len=1432[Packe
124 0x031d (797)   10.87.65.23  10.84.162.45  24  60577  9100 126.365542080  0.000012110  4325 1432     1              5757 65792  2864  25867          60577 > 9100 [PSH, ACK] Seq=4325 Ack=1 Win=65792 Len=1432[
 57 0x914c (37196) 10.84.162.45 10.87.65.23   24   9100 60577 126.475929230  0.110387150     1    0  5757 0.110387150       32120         25868    25867 9100 > 60577 [ACK] Seq=1 Ack=5757 Win=32120 Len=0
```

Local network problem example causing Citrix disconnects

One of many problems found at the boot process.

Looks like network problems causing Citrix disconnections at the Terminal... Item 10 lost 12 packets.



pwgsxachp0004@2014-06-13.appcapture

ip.src == 10.83.33.141 tcp.stream == 1

```
Arrival Time: Jun 13, 2014 10:17:45.618604000 Central Daylight Time
```

TTL	Identification	Source	Destination	TCP-S	SPort	DPort	Time	Delta	SEQ#	LEN	ACK#	Fr#	Acks-Fr#	RTT ACK	NxtSEQ#	C-WIN	Flight	Message
22	0x4bc7 (19399)	10.83.33.141	10.87.131.13	1	2635	2598	1020.993615	0.200010	65864	0	1013868	186716	186712	0.157012000		65535		
22	0x4bc8 (19400)	10.83.33.141	10.87.131.13	1	2635	2598	1021.593945	0.600330	65864	0	1013884	186788	186755	0.224239000		65535		
22	0x4bc9 (19401)	10.83.33.141	10.87.131.13	1	2635	2598	1022.192050	0.598105	65864	6	1013894	186882	186851	0.072260000	65870	65535	6	
22	0x4bcb (19403)	10.83.33.141	10.87.131.13	1	2635	2598	1022.993740	0.801690	65870	0	1013902	186987	186980	0.109915000		65535		
22	0x4bcc (19404)	10.83.33.141	10.87.131.13	1	2635	2598	1023.793656	0.799916	65870	0	1013910	187074	187046	0.159954000		65535		
22	0x4bcd (19405)	10.83.33.141	10.87.131.13	1	2635	2598	1024.593549	0.799893	65870	0	1013919	187182	187175	0.209883000		65535		
22	0x4bce (19406)	10.83.33.141	10.87.131.13	1	2635	2598	1025.393467	0.799918	65870	0	1013927	187316	187305	0.254424000		65535		
22	0x4bcf (19407)	10.83.33.141	10.87.131.13	1	2635	2598	1025.961738	0.568271	65870	6	1013935	187491	187469	0.074249000	65876	65535	6	
22	0x4bd0 (19408)	10.83.33.141	10.87.131.13	1	2635	2598	1026.792801	0.831063	65876	0	1013943	187713	187661	0.159026000		65535		
22	0x4bd2 (19410)	10.83.33.141	10.87.131.13	1	2635	2598	1027.593122	0.800321	65876	0	1013951	187851	187820	0.227207000		65535		
22	0x4bd3 (19411)	10.83.33.141	10.87.131.13	1	2635	2598	1028.393090	0.799968	65876	0	1013959	188105	188091	0.273304000		65535		
22	0x4bd4 (19412)	10.83.33.141	10.87.131.13	1	2635	2598	1028.992462	0.599372	65876	0	1013967	188156	188148	0.122077000		65535		
22	0x4bd5 (19413)	10.83.33.141	10.87.131.13	1	2635	2598	1029.702229	0.709767	65876	6	1013975	188260	188257	0.072526000	65882	65535	6	
22	0x4bd6 (19414)	10.83.33.141	10.87.131.13	1	2635	2598	1030.592390	0.890161	65882	0	1013983	188380	188376	0.222495000		65535		
22	0x4bd8 (19416)	10.83.33.141	10.87.131.13	1	2635	2598	1031.392265	0.799875	65882	0	1013991	188494	188413	0.272260000		65535		
22	0x4bd9 (19417)	10.83.33.141	10.87.131.13	1	2635	2598	1031.792580	0.400315	65882	0	1014486	188498	188496	0.133374000		65535		
22	0x4bda (19418)	10.83.33.141	10.87.131.13	1	2635	2598	1033.692366	1.899786	65882	6	1014486	188807			65888	65535	6	
22	0x4bdd (19421)	10.83.33.141	10.87.131.13	1	2635	2598	1037.691876	3.999510	65888	3	1014486	189335			65891	65535	3	
22	0x4bdf (19423)	10.83.33.141	10.87.131.13	1	2635	2598	1041.691329	3.999453	65891	3	1014486	190780			65894	65535	3	
22	0x4be1 (19425)	10.83.33.141	10.87.131.13	1	2635	2598	1045.690712	3.999383	65894	3	1014486	192969			65897	65535	3	
22	0x4be3 (19427)	10.83.33.141	10.87.131.13	1	2635	2598	1049.690165	3.999453	65897	3	1014486	195642			65900	65535	3	
22	0x4be4 (19428)	10.83.33.141	10.87.131.13	1	2635	2598	1050.590073	0.899908	65900	0	1014513	196155	196110	0.163197000		65535		
22	0x4be6 (19430)	10.83.33.141	10.87.131.13	1	2635	2598	1053.389766	2.799693	65900	0	1015200	197339	197325	0.152364000		65535		
22	0x4be7 (19431)	10.83.33.141	10.87.131.13	1	2635	2598	1053.550464	0.160698	65900	6	1015230	197478	197340	0.134115000	65906	65535	6	
22	0x4be8 (19432)	10.83.33.141	10.87.131.13	1	2635	2598	1053.789182	0.238718	65906	0	1015245	197654	197525	0.197115000		65535		
22	0x4bf4 (19444)	10.83.33.141	10.87.131.13	1	2635	2598	1063.393979	9.604797	65918	0	1015273	206404	206115	1.943416000		65535		Previous segment not capt
22	0x4bf5 (19445)	10.83.33.141	10.87.131.13	1	2635	2598	1064.395855	1.001876	65918	0	1015281	206435	206429	0.150490000		65535		
22	0x4bf6 (19446)	10.83.33.141	10.87.131.13	1	2635	2598	1064.790085	0.394230	65918	0	1015289	206464	206439	0.269316000		65535		
22	0x4bf7 (19447)	10.83.33.141	10.87.131.13	1	2635	2598	1065.190494	0.400409	65918	0	1015298	206809	206693	0.198860000		65535		
22	0x4bf8 (19448)	10.83.33.141	10.87.131.13	1	2635	2598	1065.390534	0.200040	65918	0	1015306	206907	206761	0.242781000		65535		
22	0x4bf9 (19449)	10.83.33.141	10.87.131.13	1	2635	2598	1065.550476	0.159942	65918	6	1015306	207146			65924	65535	6	
22	0x4bfa (19450)	10.83.33.141	10.87.131.13	1	2635	2598	1065.590537	0.040061	65906	18	1015306	207152			65924	65535	18	Retransmission (suspected
22	0x4bfc (19452)	10.83.33.141	10.87.131.13	1	2635	2598	1067.990187	2.399650	65924	0	1015315	209671	209572	0.180324000		65535		
22	0x4bfd (19453)	10.83.33.141	10.87.131.13	1	2635	2598	1069.549957	1.559770	65924	6	1015315	209721			65930	65535	6	
22	0x4bff (19455)	10.83.33.141	10.87.131.13	1	2635	2598	1071.232522	1.682565	65930	11	1015325	209792	209786	0.082676000	65941	65535	11	
22	0x4c00 (19456)	10.83.33.141	10.87.131.13	1	2635	2598	1071.237585	0.005063	65941	5	1015325	209794			65946	65535	5	
22	0x4c01 (19457)	10.83.33.141	10.87.131.13	1	2635	2598	1071.685545	0.447960	65946	0	1015325	209813				65535		Connection finish (FIN)
22	0x4c03 (19459)	10.83.33.141	10.87.131.13	1	2635	2598	1071.687465	0.001920	65941	0		209816				0		Connection reset (RST)
22	0x4c04 (19460)	10.83.33.141	10.87.131.13	1	2635	2598	1071.688115	0.000650	65946	0		209817				0		Connection reset (RST)
22	0x4c05 (19461)	10.83.33.141	10.87.131.13	1	2635	2598	1071.762717	0.074602	65947	0		209821				0		Connection reset (RST)
22	0x4c06 (19462)	10.83.33.141	10.87.131.13	1	2635	2598	1071.762785	0.000068	65947	0		209822				0		Connection reset (RST)

Visualized Performance

WireShark / Sniffer Capture

Visualized Performance – Packet and Time Correlated

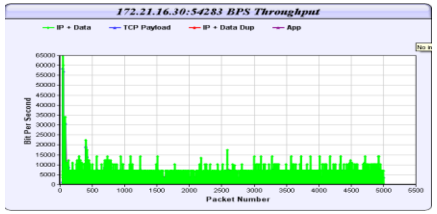
Opposing Packet Transaction Exchanges of:

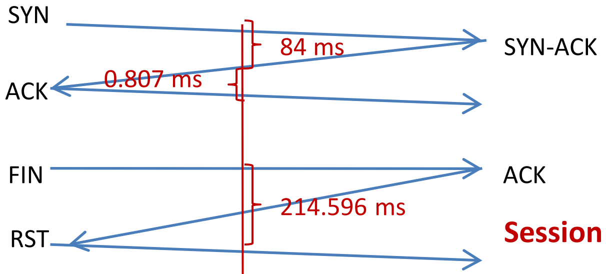
- Packet Sizes
- Response Times
- Bits Per Second by Layer
- Offered load into TCP Window vs. Receive Window Size
- Offered load unacknowledged packets
- Packet rate of session vs. packets to others
- Cumulative Bytes
- Data vs. Application Efficiency

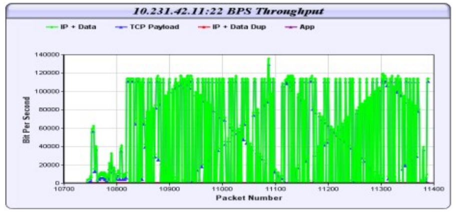
Error Visualizations:

- Lost data and Selective Ack Visualized
- Retransmission, Duplicate and Out of Order

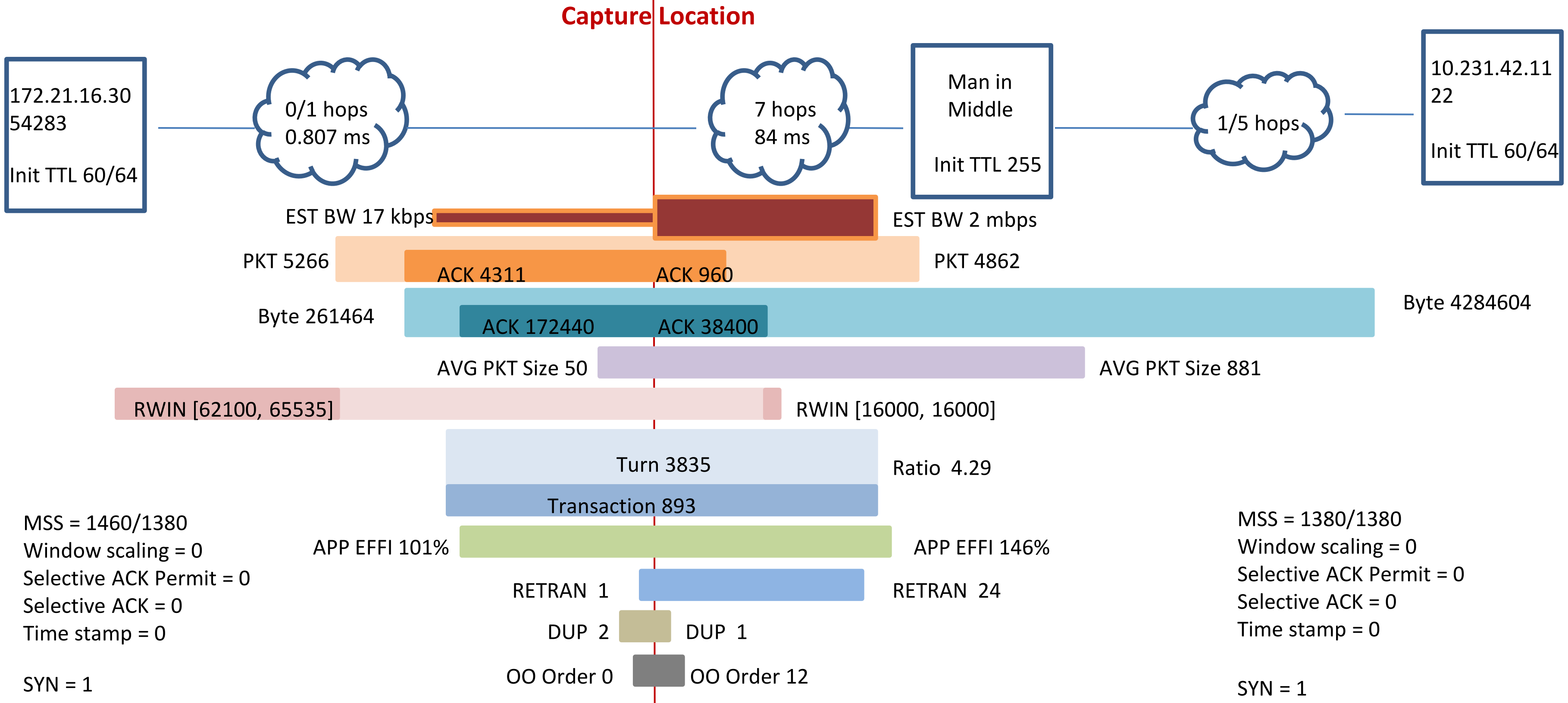
Session Summary 172.21.16.30:54283-10.231.42.11:22





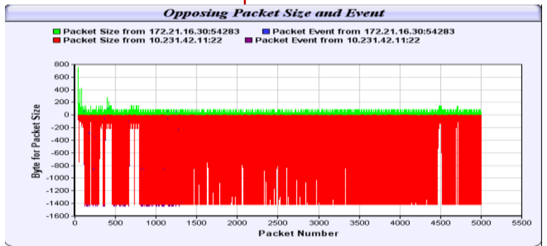


Session duration 1 hour 12 minutes



MSS = 1460/1380
Window scaling = 0
Selective ACK Permit = 0
Selective ACK = 0
Time stamp = 0

SYN = 1
FIN = 1
RST = 1
PUSH = 953
URG =0
ECN = 0
CWR = 0



MSS = 1380/1380
Window scaling = 0
Selective ACK Permit = 0
Selective ACK = 0
Time stamp = 0

SYN = 1
FIN = 0
RST = 0
PUSH = 2240
URG =0
ECN = 0
CWR = 0

Session Summary in <*etmc prob1 smb port 1678.cap*>

172.16.144.157/
1678

Init TTL 128

Session lasts 3 seconds, data transfer intensive

0 hop, 0.03 ms

2 hops, 0.18 ms EST BW 97.56 Mbps (85% certain)

172.16.14.72/
445

Init TTL 128

SYN

0.2 ms

SYN-ACK

ACK

0.03 ms

Integrity is good

Integrity is good

0% packet loss sent by
172.16.144.157

16.4% time wasted due
to packet loss sent by
172.16.14.72

2.78% packet loss, 28% of which
is secondary retransmission

2.78% packet loss

Performance is not constrained

Performance constrained by

- Network bandwidth
- Network packet loss
- High percentage of second retransmission
- Sender window size with network packet loss

PKT/Byte: 508/ 30479, ACK 419, EFFI 29%

PKT/Byte: 827/1144013, ACK 8, EFFI 94%

PKT Size with data [79, 400] AVG size 59

PKT size with data [79, 1500], AVG size 1383

TCP response time AVG 5.9 ms,
[0, 361.46 ms pure ACK]

TCP response time AVG 0.78 ms,
[0.18 ms, 0.5 ms pure ACK]

Serious Events

- Application constrain (1)
- Delayed ACK constrain (1)

Serious Events

- Application constrain (5)
- Sender window constrain (29)
- Forth retransmission (1)
- Third retransmission (4)
- Second retransmission (8)

APP response time AVG 22.35 ms,
[0, 1468.89 ms]

APP response time AVG 0.85 ms,
[0.22 ms, 16.05 ms]

RWIN [[61592, 64512]]
-> peer max APP rate 339.5 Mbps

RWIN [16384[64129, 65535]]
-> peer max APP rate 344.9 Mbps

Outstanding PKT [1, 2]
Outstanding byte [1, 360]

Outstanding PKT [1, 16]
Outstanding byte [1, 42523]

MSS = 1460/1460
Window scaling = 0
Selective ACK Permit = 1
Selective ACK = 116
Time stamp = 0

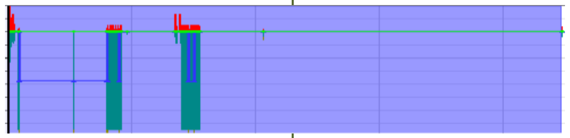
MSS = 1460/1460
Window scaling = 0
Selective ACK Permit = 1
Selective ACK = 0
Time stamp = 0

FIN

FIN

ACK

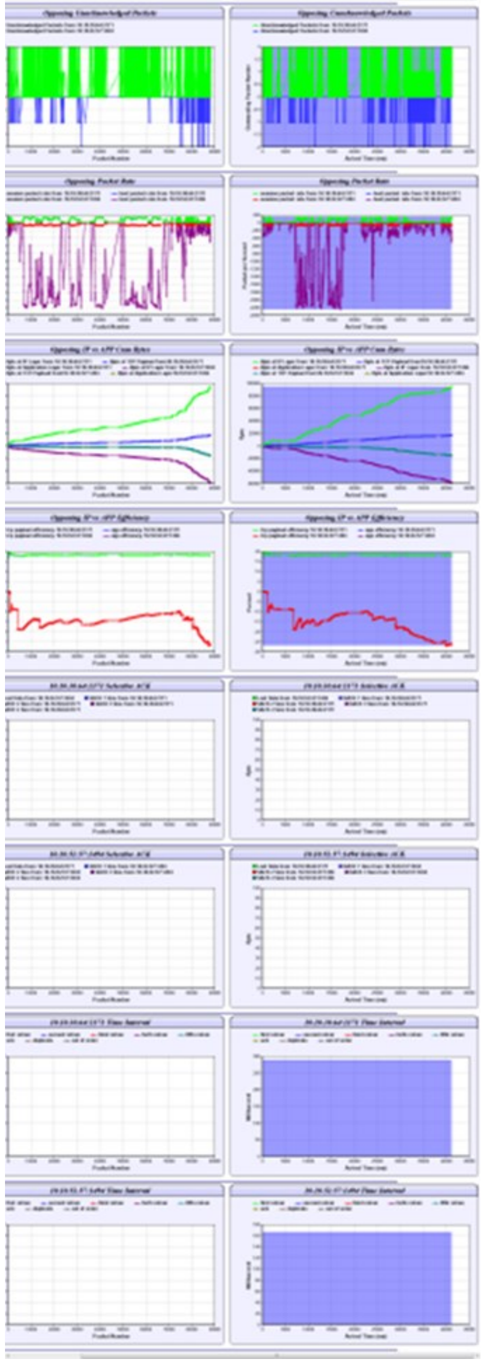
0.2 ms



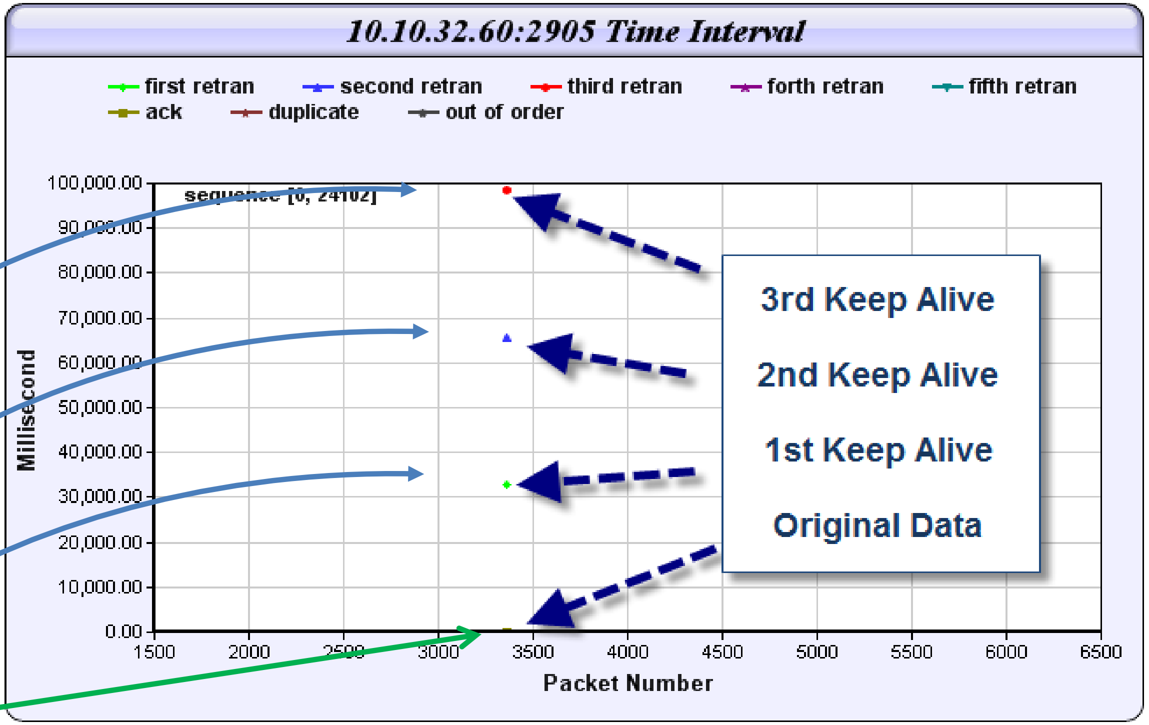
Opposing packet size

Performance Event Detection

- Performance Limiting Events
  - Window Size
  - IP Fragmentation
  - Network Path Changes
  - MITM (Man-in-the-middle)
  - Connection Issues
  - Bottleneck BPS
- TCP Stack Characteristics
  - TCP Options
  - App Data vs. TCP Control BPS
  - Connection Setup and Teardown
  - Detailed TCP Statistics
- Estimated Theoretical vs. Actual Performance
- Errors
  - Problem Direction Identification
- Capture Integrity
  - SPAN capture duplicates, L2, L3 Loop

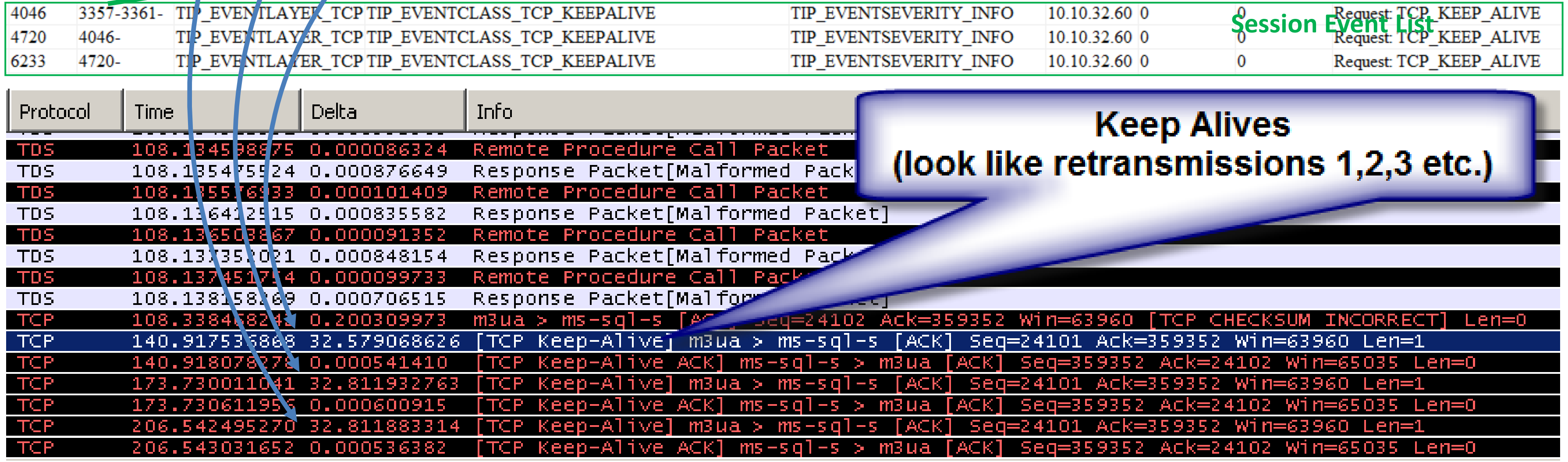


Time Interval Chart
Event List
Packet Trace



Related Packet

Session Event List

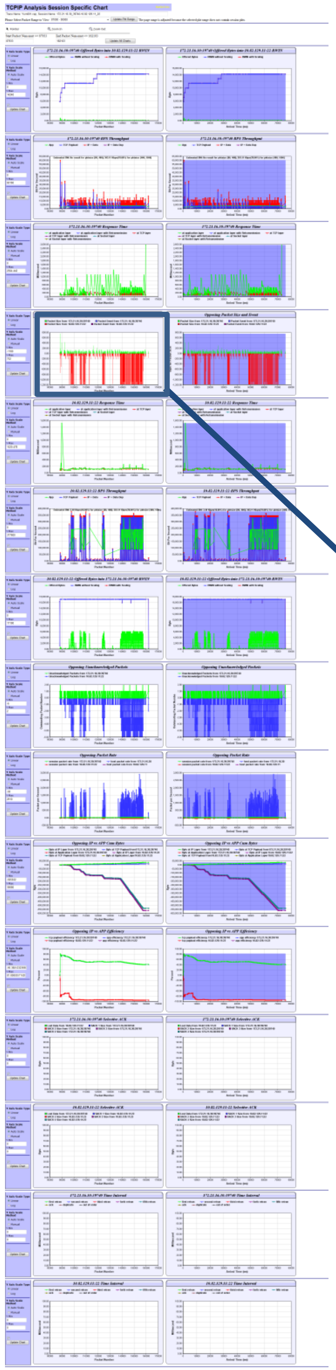


```
4046   3357-3361-  TIP_EVENTLAYER_TCP TIP_EVENTCLASS_TCP_KEEPALIVE   TIP_EVENTSEVERITY_INFO   10.10.32.60 0   0   Request: TCP_KEEP_ALIVE
4720   4046-       TIP_EVENTLAYER_TCP TIP_EVENTCLASS_TCP_KEEPALIVE   TIP_EVENTSEVERITY_INFO   10.10.32.60 0   0   Request: TCP_KEEP_ALIVE
6233   4720-       TIP_EVENTLAYER_TCP TIP_EVENTCLASS_TCP_KEEPALIVE   TIP_EVENTSEVERITY_INFO   10.10.32.60 0   0   Request: TCP_KEEP_ALIVE
```

```
Protocol  Time           Delta         Info
TDS       108.134598875  0.000086324   Remote Procedure Call Packet
TDS       108.135475524  0.000876649   Response Packet[Malformed Pack
TDS       108.135576933  0.000101409   Remote Procedure Call Packet
TDS       108.136412515  0.000835582   Response Packet[Malformed Packet]
TDS       108.136503867  0.000091352   Remote Procedure Call Packet
TDS       108.137352021  0.000848154   Response Packet[Malformed Pack
TDS       108.137451754  0.000099733   Remote Procedure Call Pack
TDS       108.138158269  0.000706515   Response Packet[Malfor
TCP       108.338468242  0.200309973   m3ua > ms-sql-s [ACK] Seq=24102 Ack=359352 Win=63960 [TCP CHECKSUM INCORRECT] Len=0
TCP       140.917536868  32.579068626  [TCP Keep-Alive] m3ua > ms-sql-s [ACK] Seq=24101 Ack=359352 Win=63960 Len=1
TCP       140.918078278  0.000541410   [TCP Keep-Alive ACK] ms-sql-s > m3ua [ACK] Seq=359352 Ack=24102 Win=65035 Len=0
TCP       173.730011041  32.811932763  [TCP Keep-Alive] m3ua > ms-sql-s [ACK] Seq=24101 Ack=359352 Win=63960 Len=1
TCP       173.730611956  0.000600915   [TCP Keep-Alive ACK] ms-sql-s > m3ua [ACK] Seq=359352 Ack=24102 Win=65035 Len=0
TCP       206.542495270  32.811883314  [TCP Keep-Alive] m3ua > ms-sql-s [ACK] Seq=24101 Ack=359352 Win=63960 Len=1
TCP       206.543031652  0.000536382   [TCP Keep-Alive ACK] ms-sql-s > m3ua [ACK] Seq=359352 Ack=24102 Win=65035 Len=0
```

Keep Alives
(look like retransmissions 1,2,3 etc.)

Opposing Packet Size



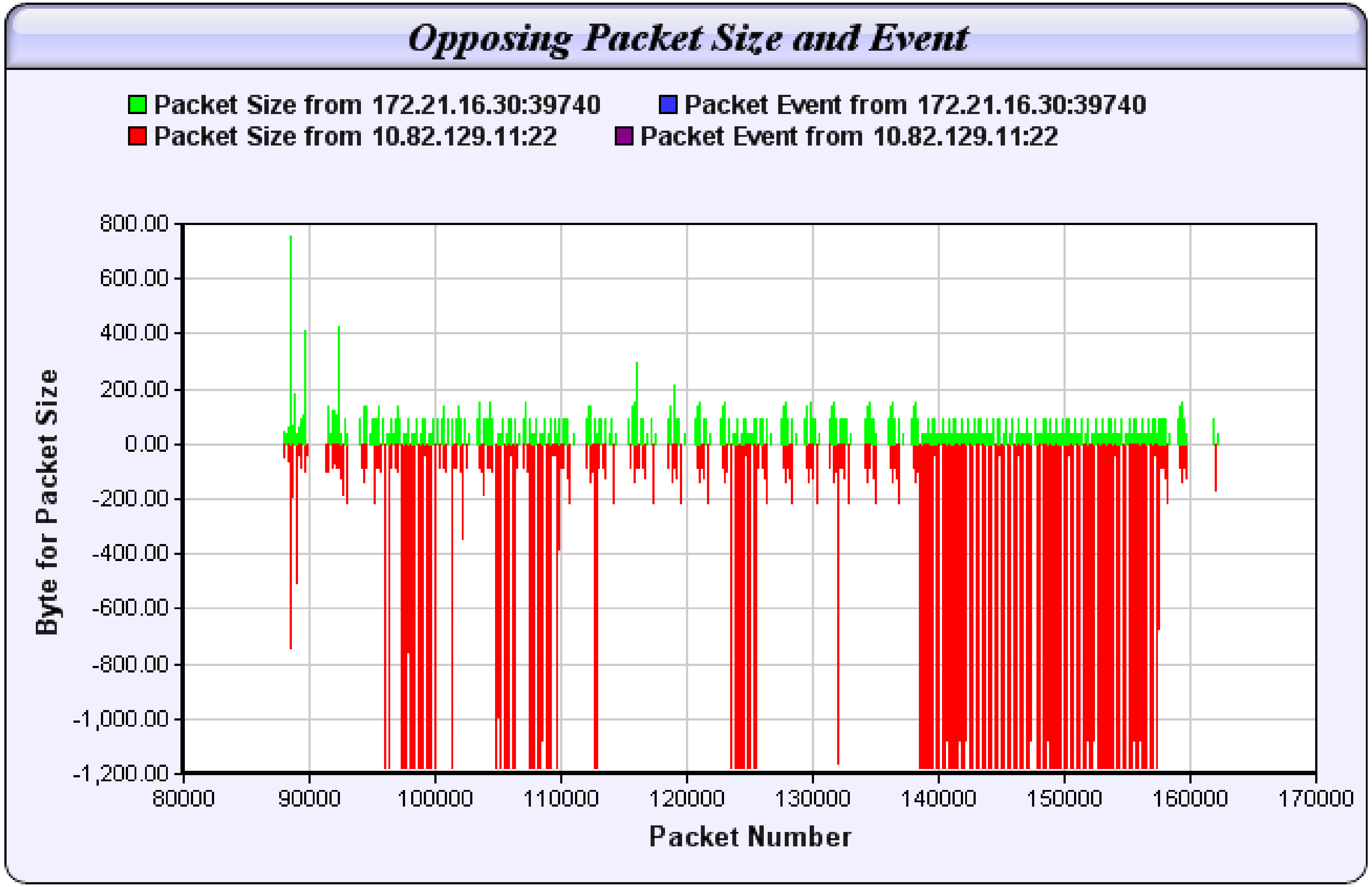
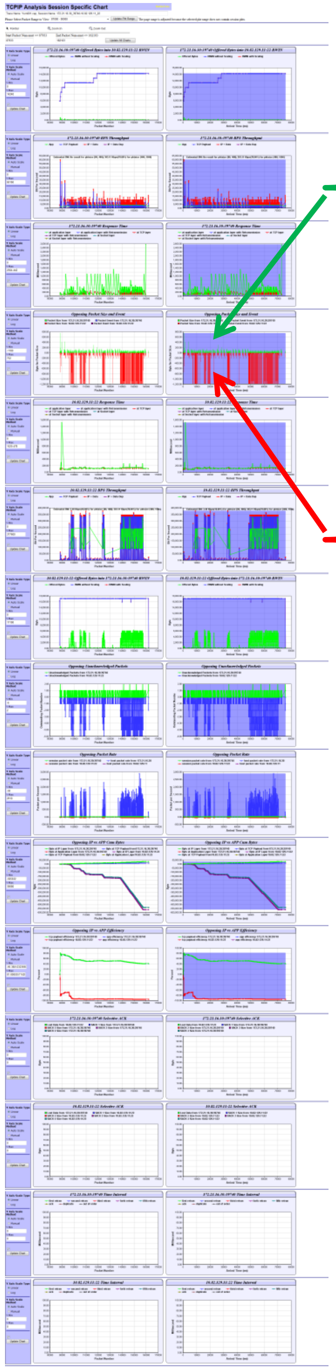


Chart Layout



Offered Bytes into TCP Window

Bits Per Second Throughput (colored by layer)

Response Time (colored by layer)

Opposing Packet Size

Response Time (colored by layer)

Bits Per Second Throughput (colored by layer)

Offered Bytes into TCP Window

Opposing Unacknowledged Packets (Visible CWIN)

Opposing Packet Rate (Red – Green Exclusive)

Opposing Cum Bytes (colored by layer)

Opposing Application Efficiency

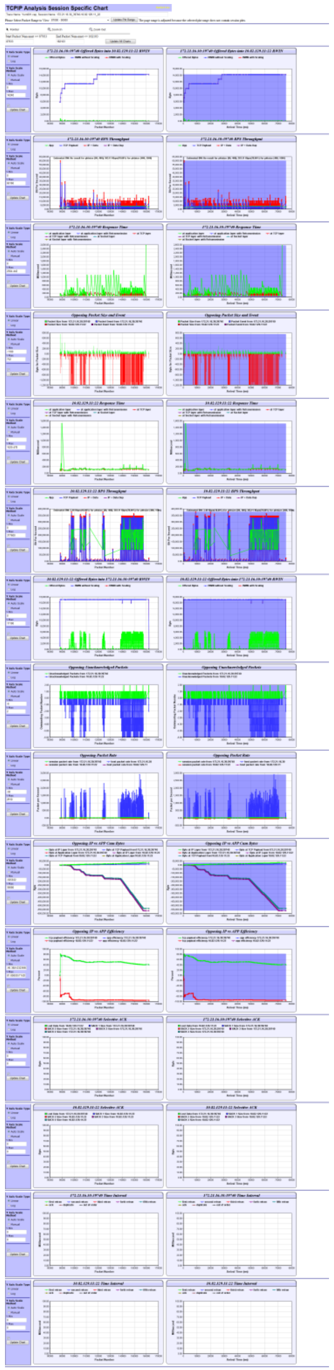
Directional Selective ACK

Directional Selective ACK

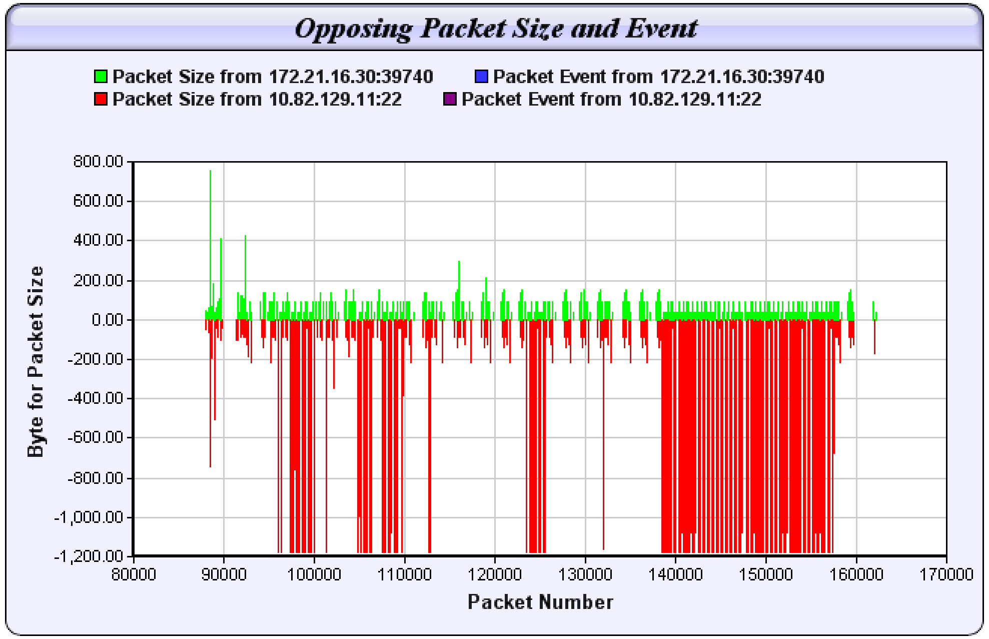
Directional Time Interval (Retrans / Dupe / Out of Order)

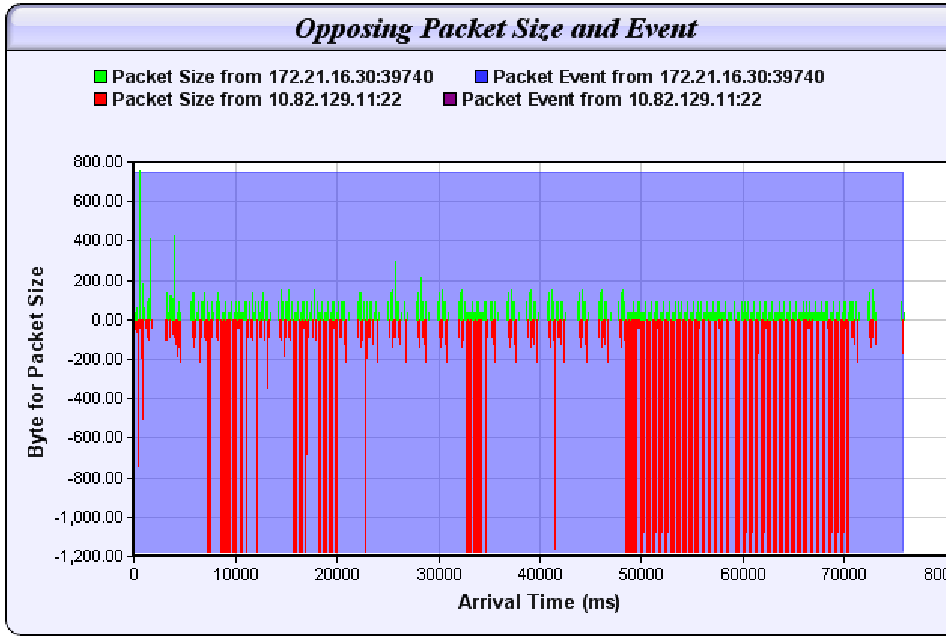
Directional Time Interval (Retrans / Dupe / Out of Order)

Opposing Packet Size

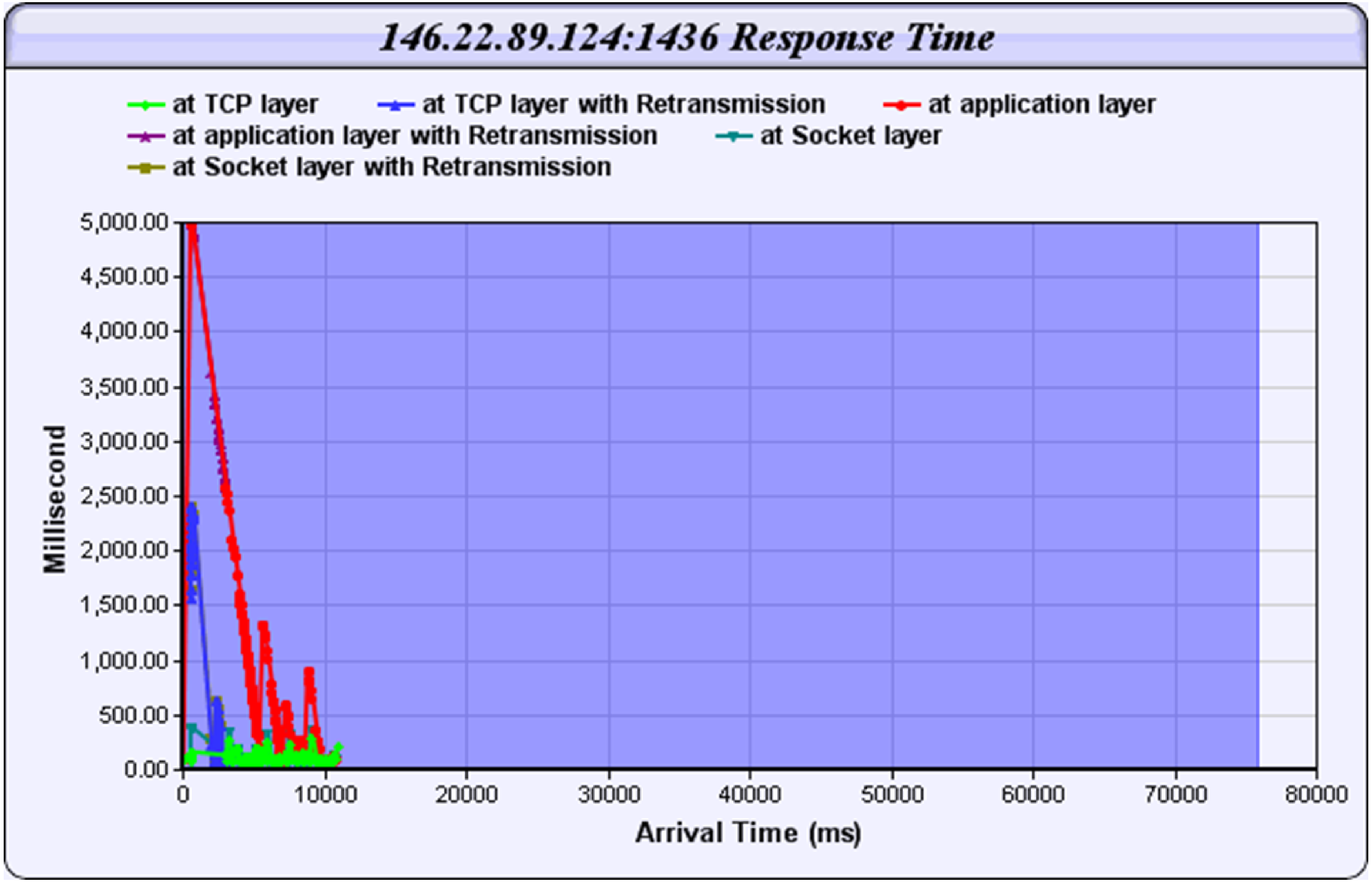


TCPIP Analysis Session Specific Chart

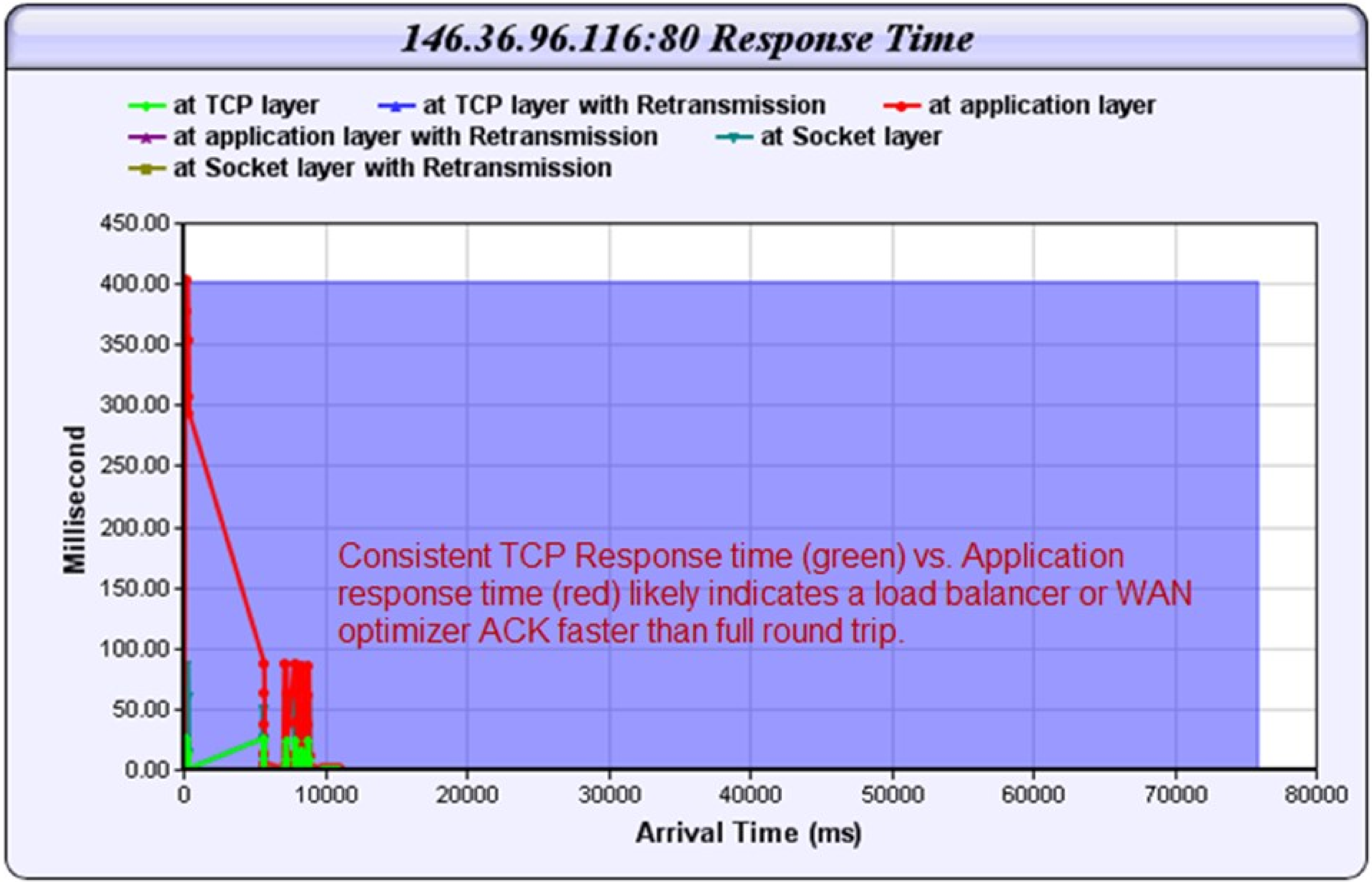




Response Time by layer

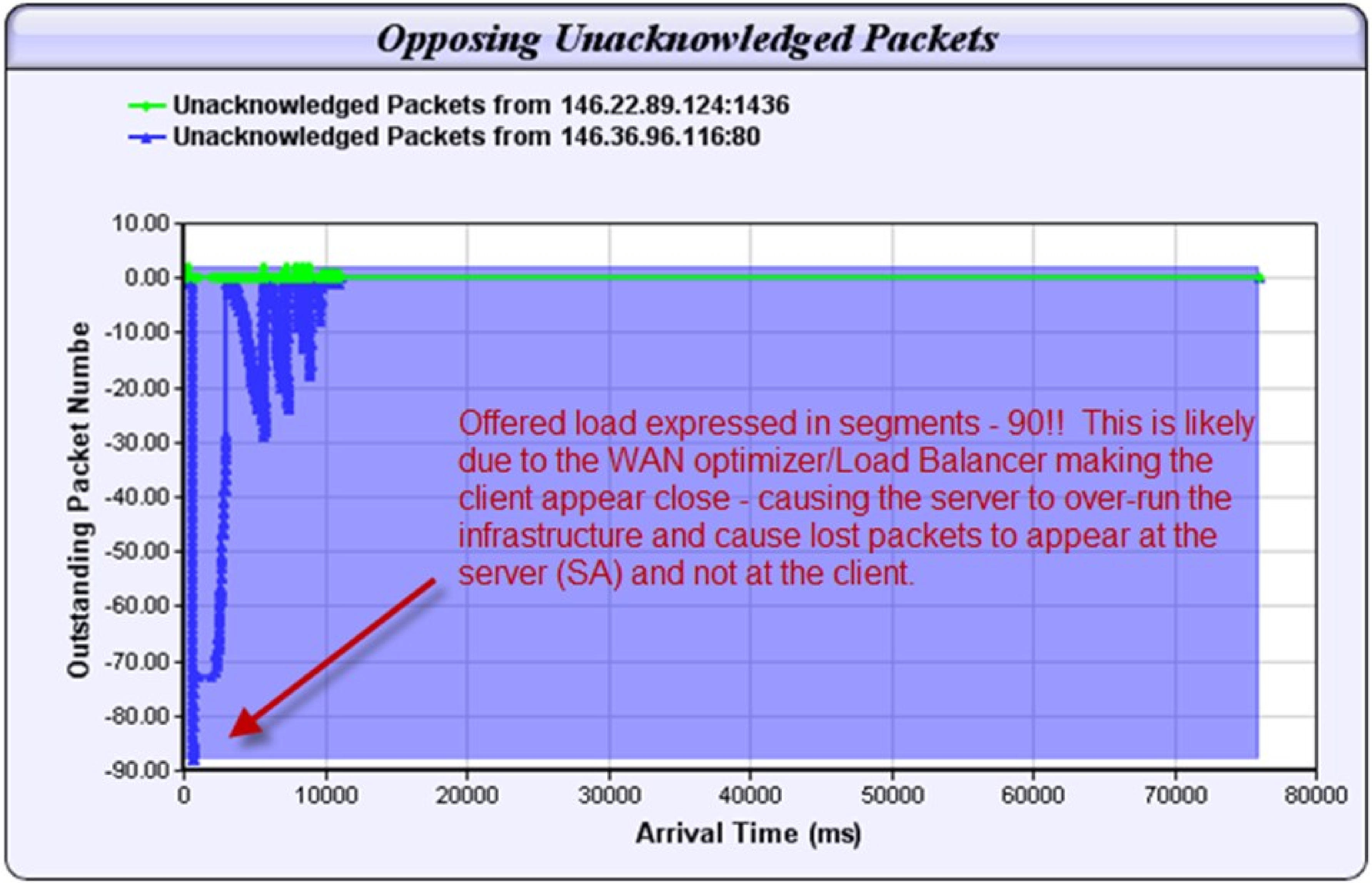


TCP Response Time by layer



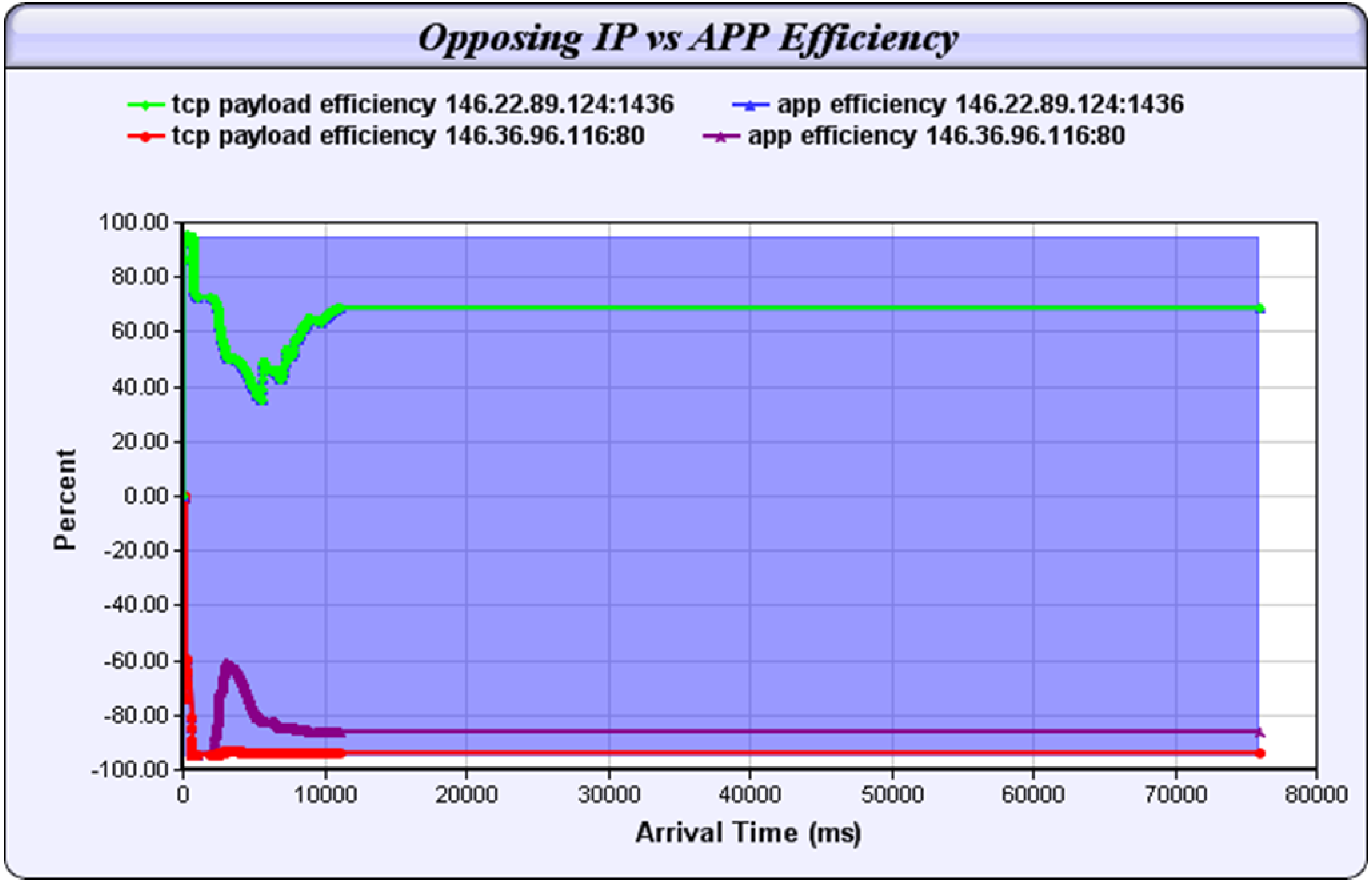
Consistent TCP Response time (green) vs. Application response time (red) likely indicates a load balancer or WAN optimizer ACK faster than full round trip.

Opposing Unacked Packets

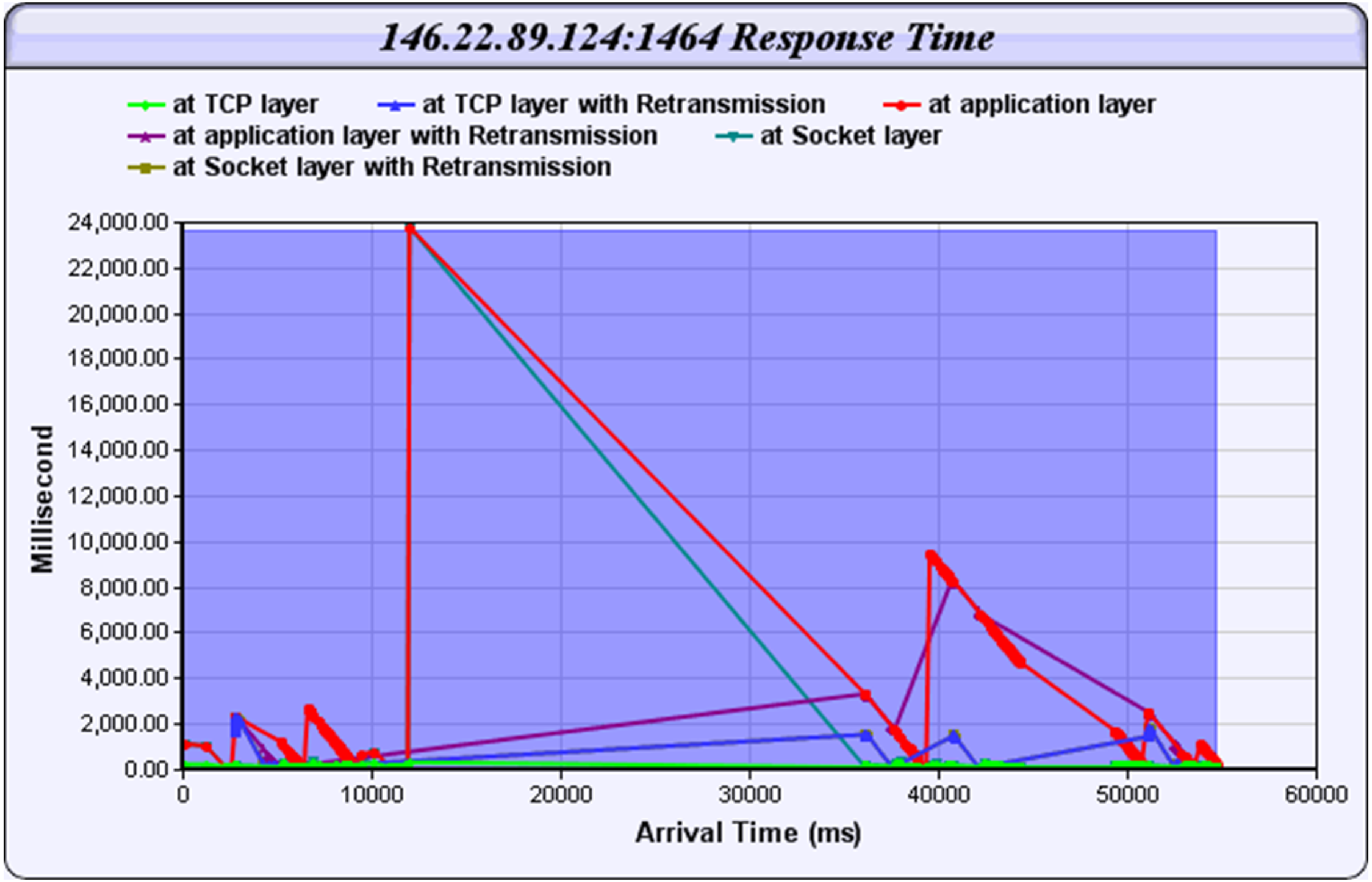


Offered load expressed in segments - 90!! This is likely due to the WAN optimizer/Load Balancer making the client appear close - causing the server to over-run the infrastructure and cause lost packets to appear at the server (SA) and not at the client.

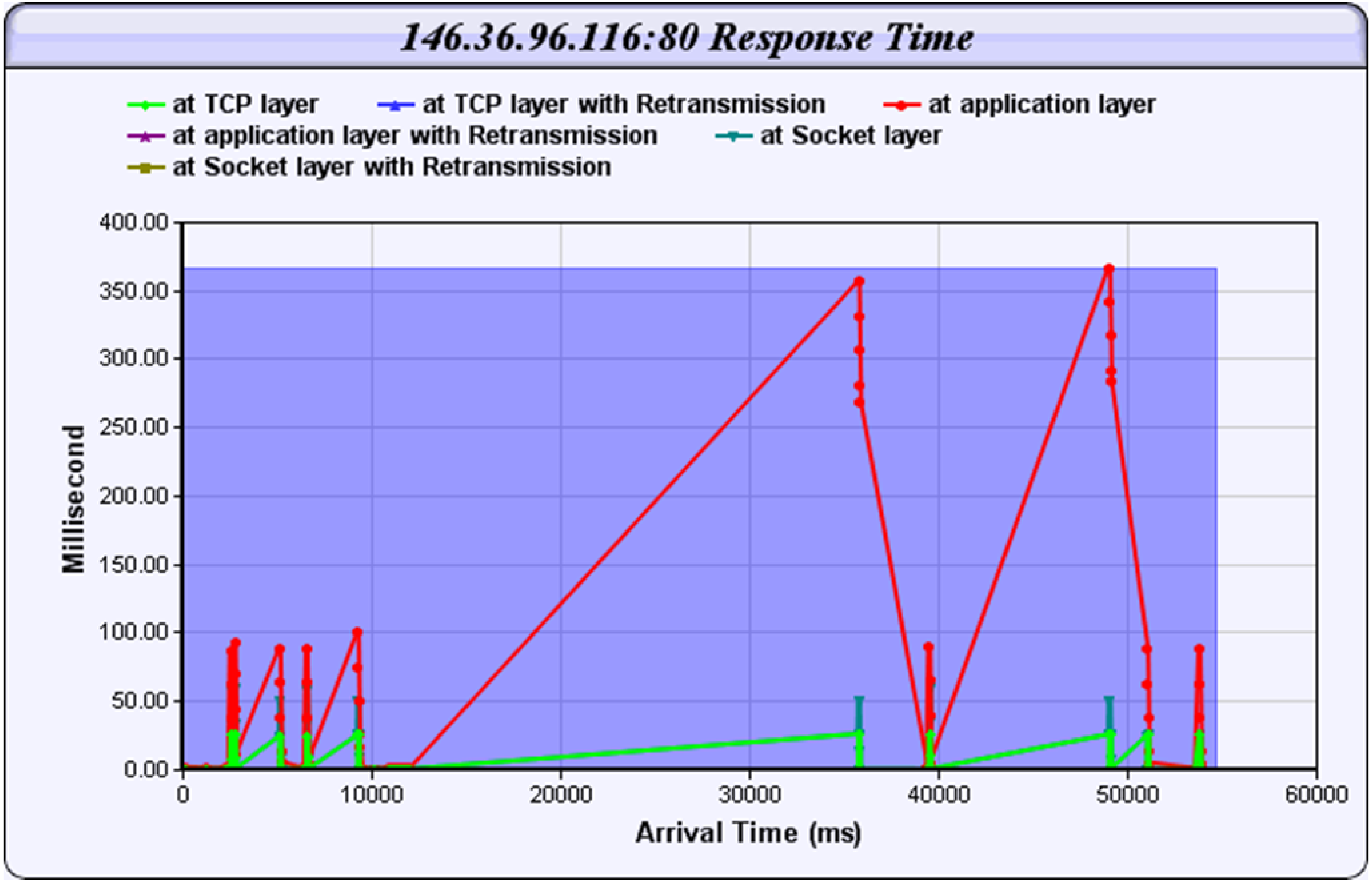
Opposing IP vs. App Efficiency



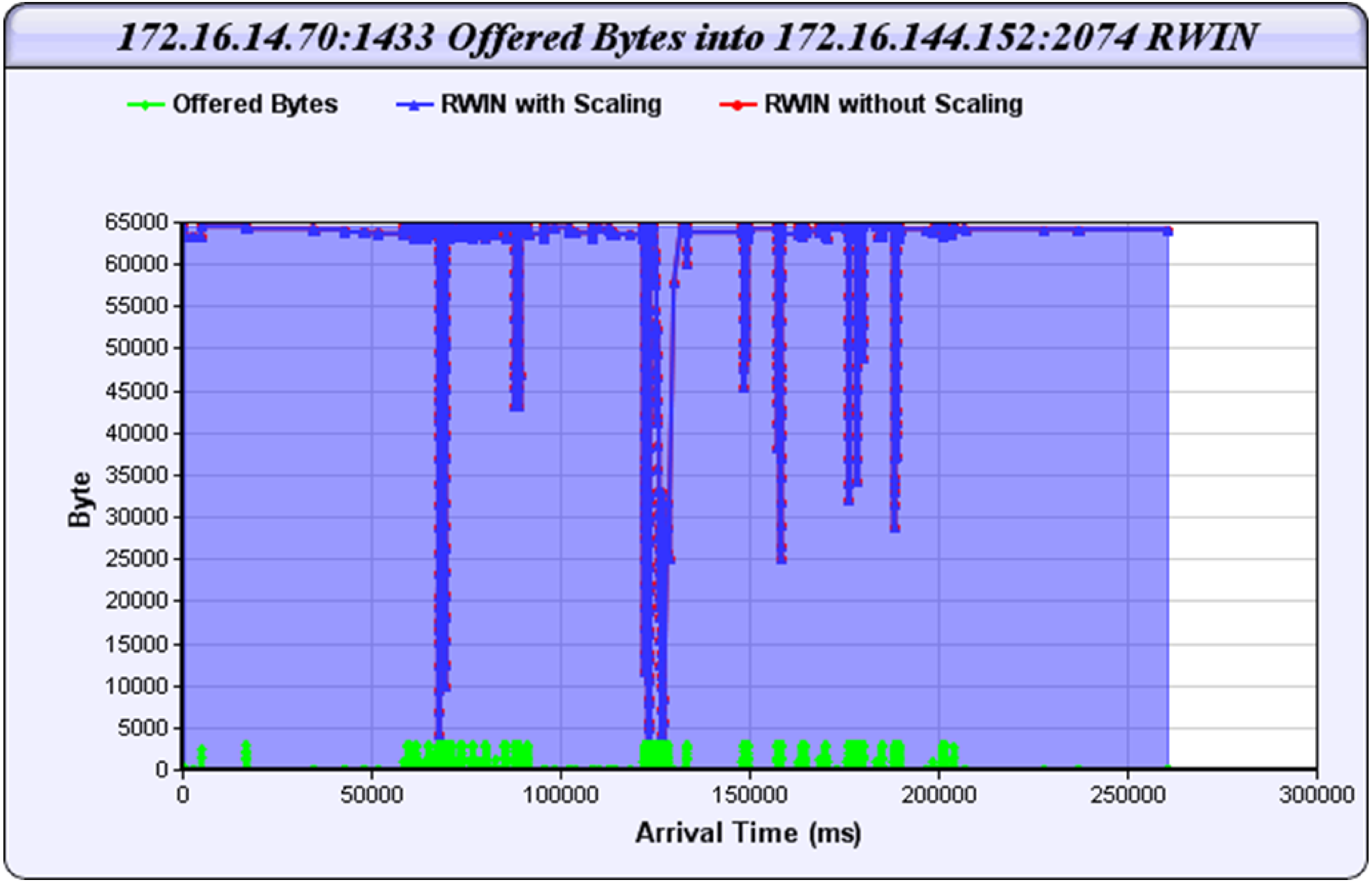
Layer Response Times



Response Times



Offered Bytes into RWIN



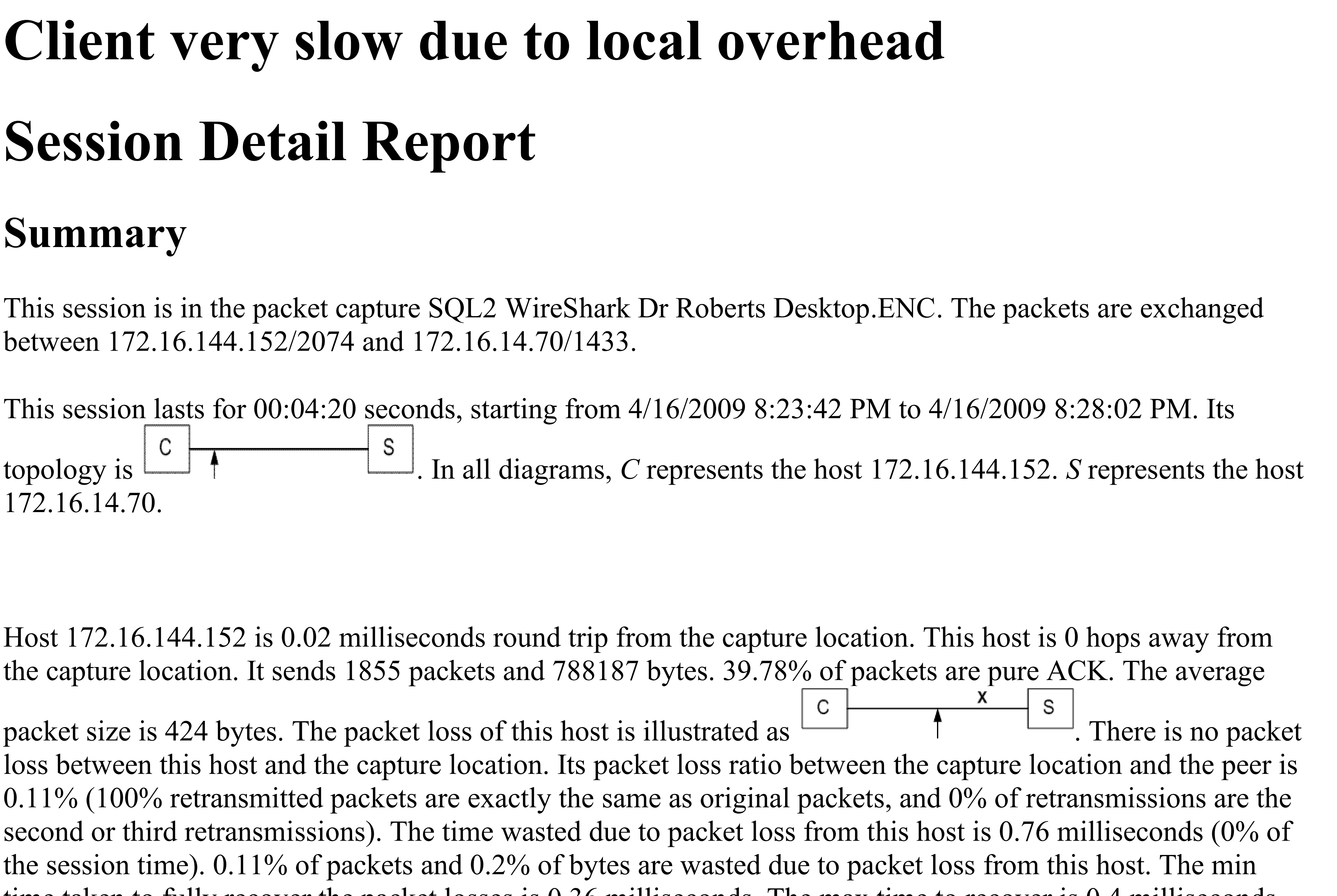
Cogent … *clear, collaborative, insightful*

powerfully persuasive, balanced, weighty, inclusive

Topics   Prof Assn's   Conferences   SME's   Vendors
Content   Videos   LiveStream   Collaboration
Root Cause Analysis   Chat GPT Cybersecurity
QUIC Protocol SharkFest - WireShark Betty Dubois
ISSA / ISC2 Leadership Podcasts

Packetman007

Additional Word Exhibit



Client very slow due to local overhead

Session Detail Report

Summary

This session is in the packet capture SQL2 WireShark Dr Roberts Desktop.ENC. The packets are exchanged between 172.16.144.152/2074 and 172.16.14.70/1433.

This session lasts for 00:04:20 seconds, starting from 4/16/2009 8:23:42 PM to 4/16/2009 8:28:02 PM. Its topology is . In all diagrams, *C* represents the host 172.16.144.152. *S* represents the host 172.16.14.70.

Host 172.16.144.152 is 0.02 milliseconds round trip from the capture location. This host is 0 hops away from the capture location. It sends 1855 packets and 788187 bytes. 39.78% of packets are pure ACK. The average packet size is 424 bytes. The packet loss of this host is illustrated as . There is no packet loss between this host and the capture location. Its packet loss ratio between the capture location and the peer is 0.11% (100% retransmitted packets are exactly the same as original packets, and 0% of retransmissions are the second or third retransmissions). The time wasted due to packet loss from this host is 0.76 milliseconds (0% of the session time). 0.11% of packets and 0.2% of bytes are wasted due to packet loss from this host. The min time taken to fully recover the packet losses is 0.36 milliseconds. The max time to recover is 0.4 milliseconds