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

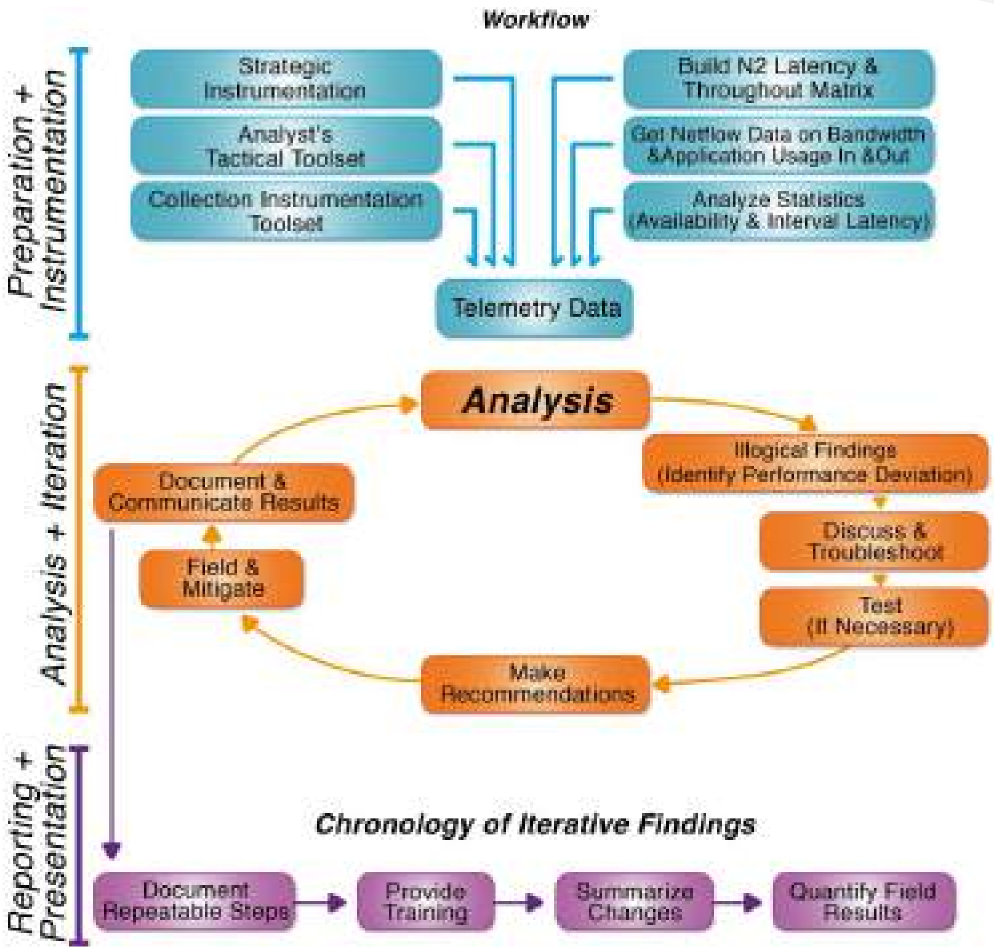
TCP Case Study Packet Analysis exhibits from high visibility, high stakes critical problems

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

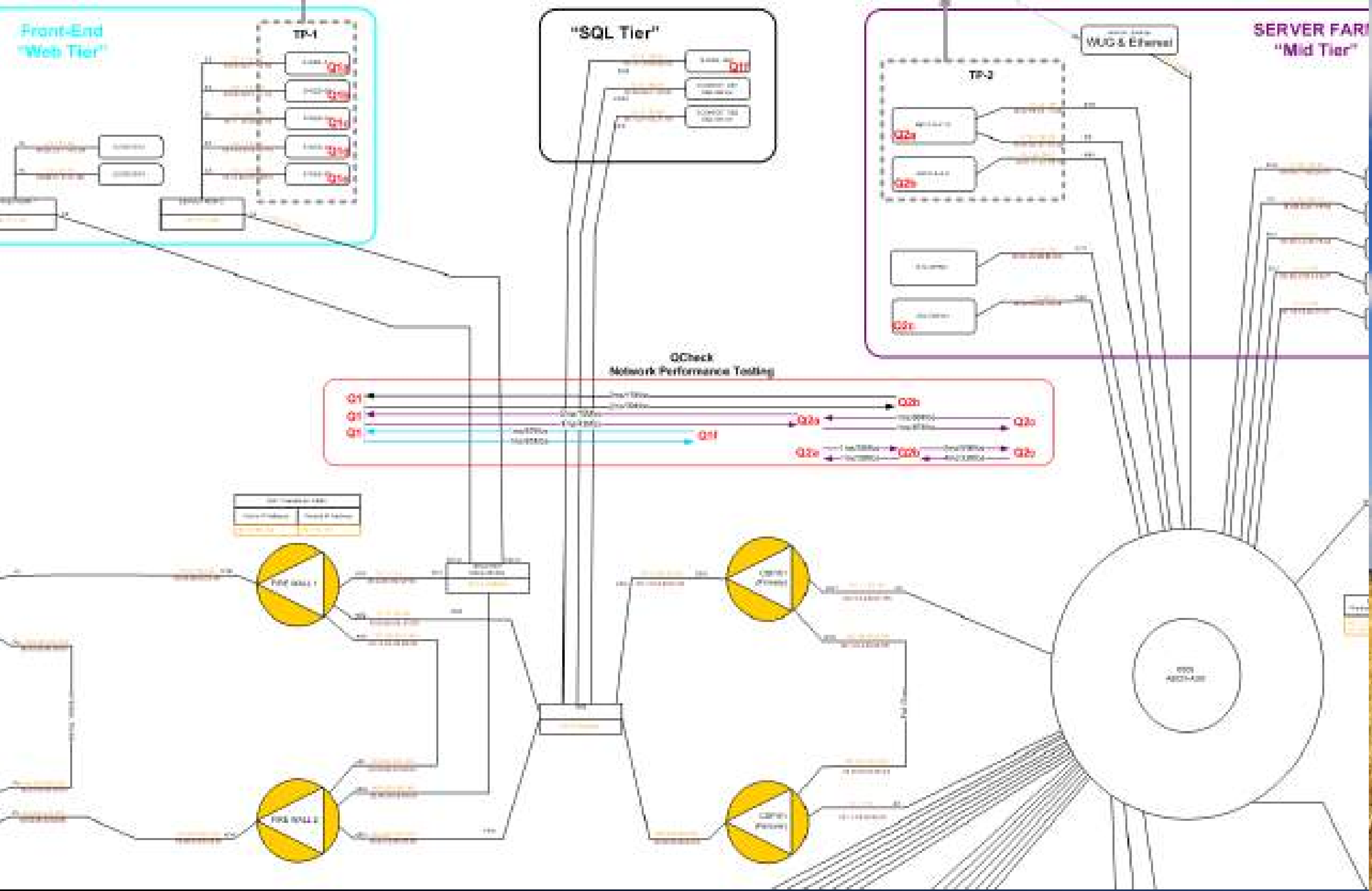
The Environment

Packet Traces

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

Finding The Stack With The Problem

Finding The Needle

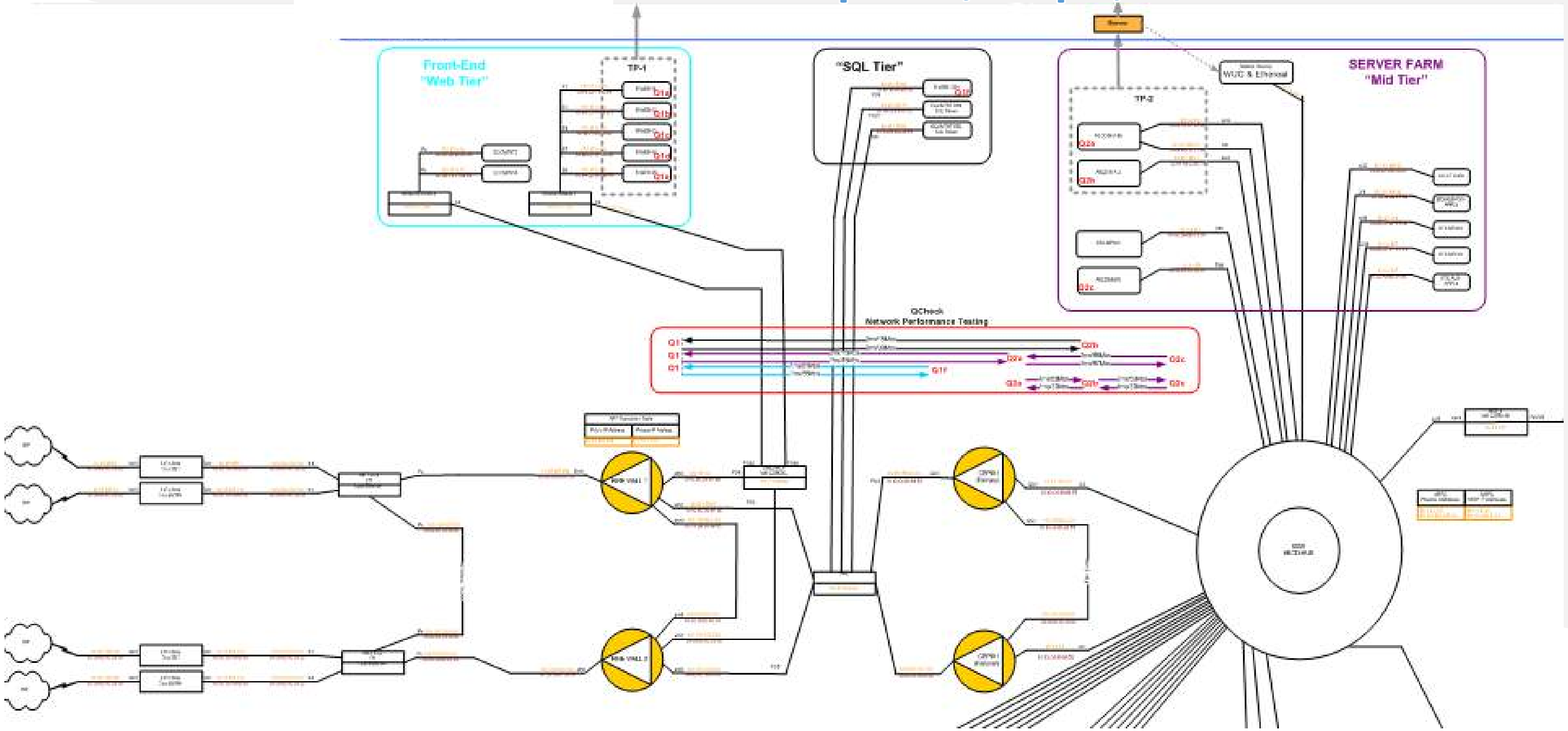


Multi-Tier Identification

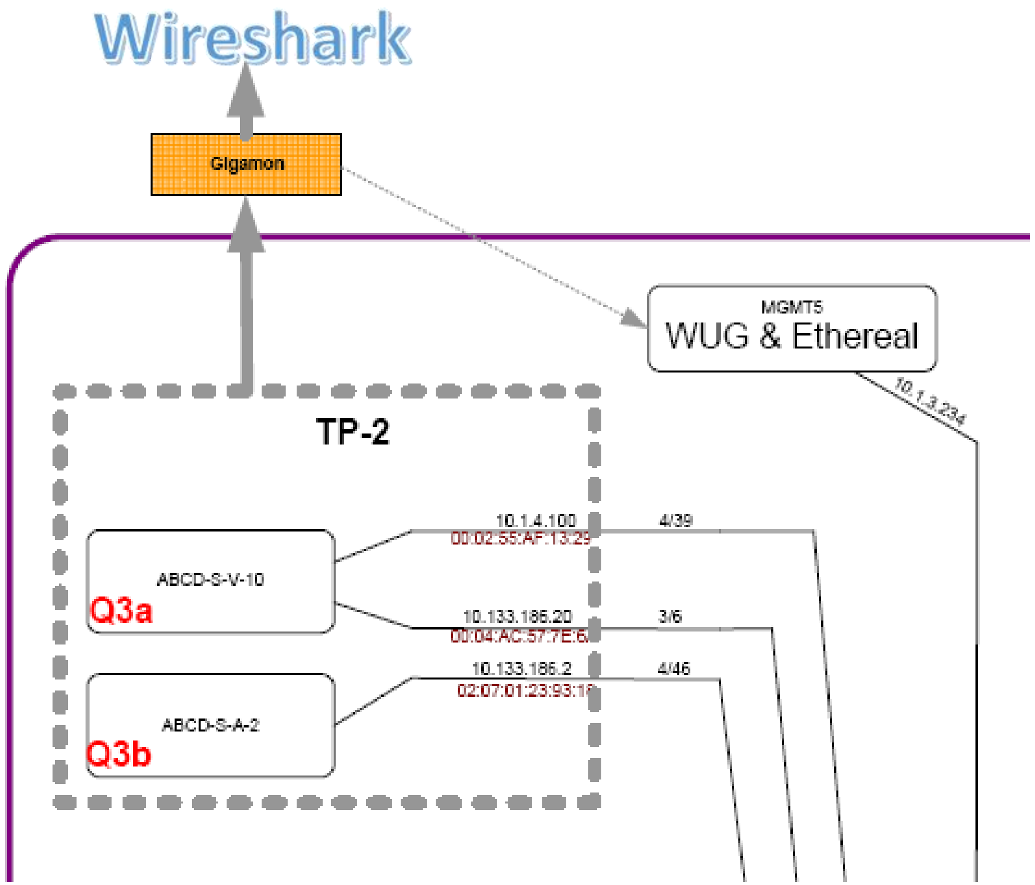
Monitoring & Analysis Design

Wireshark

Spans, Taps, Packet Brokers…

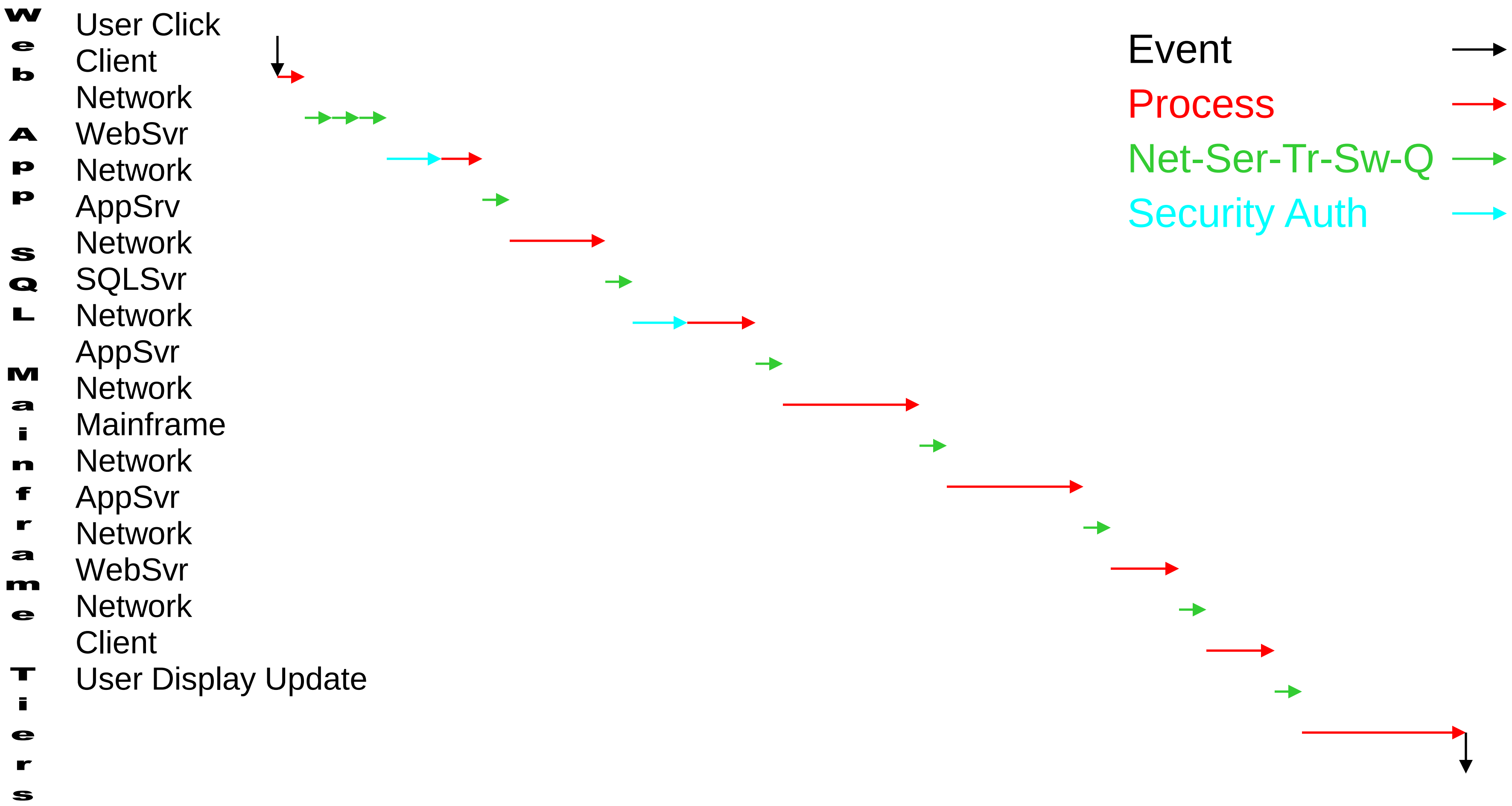


Instrumentation Phase
Test Point Design



Multi-tier Transaction Analysis

- Multi-tier Transaction Analysis



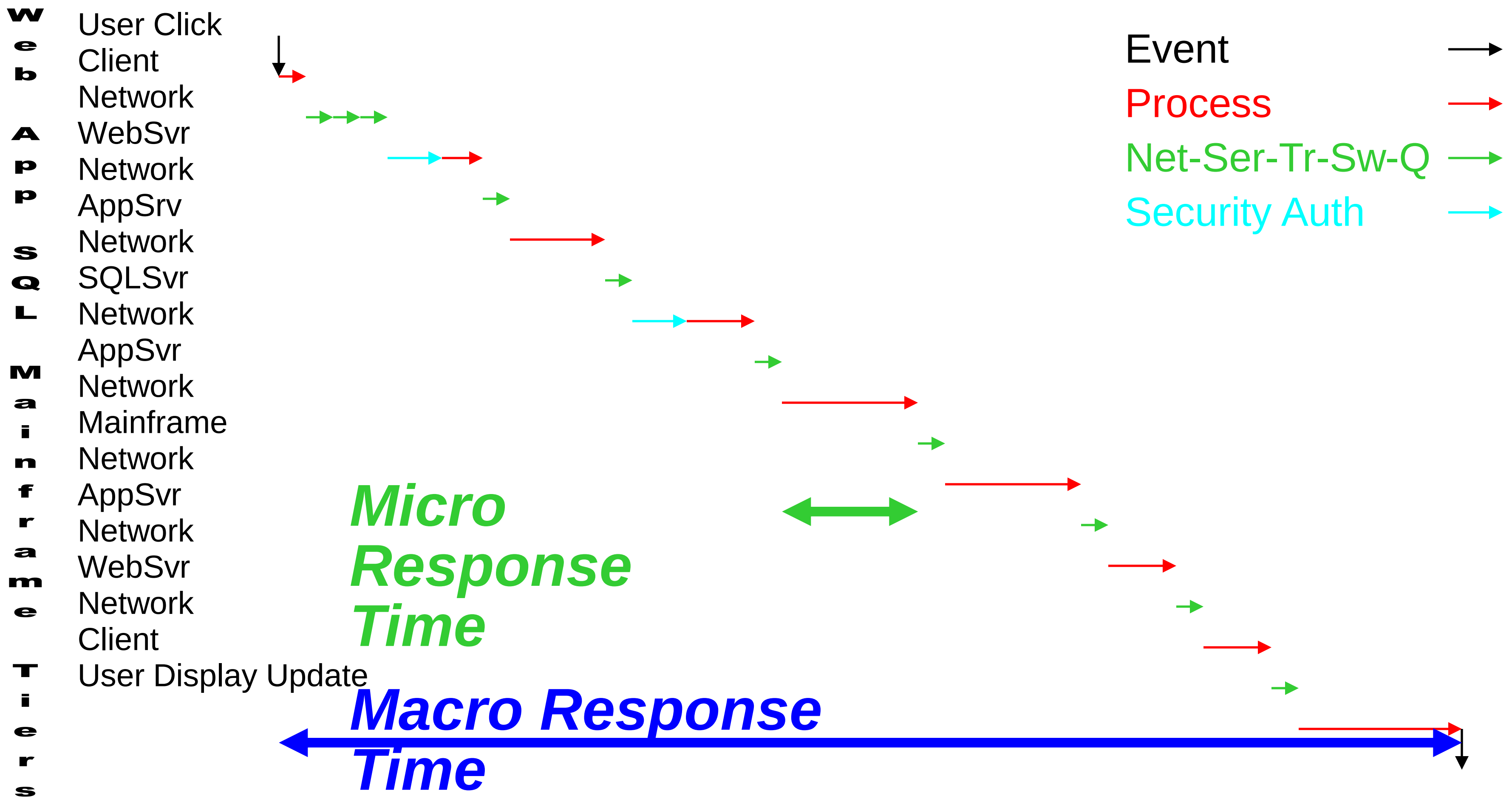
Web App SQL Mainframe Tiers

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

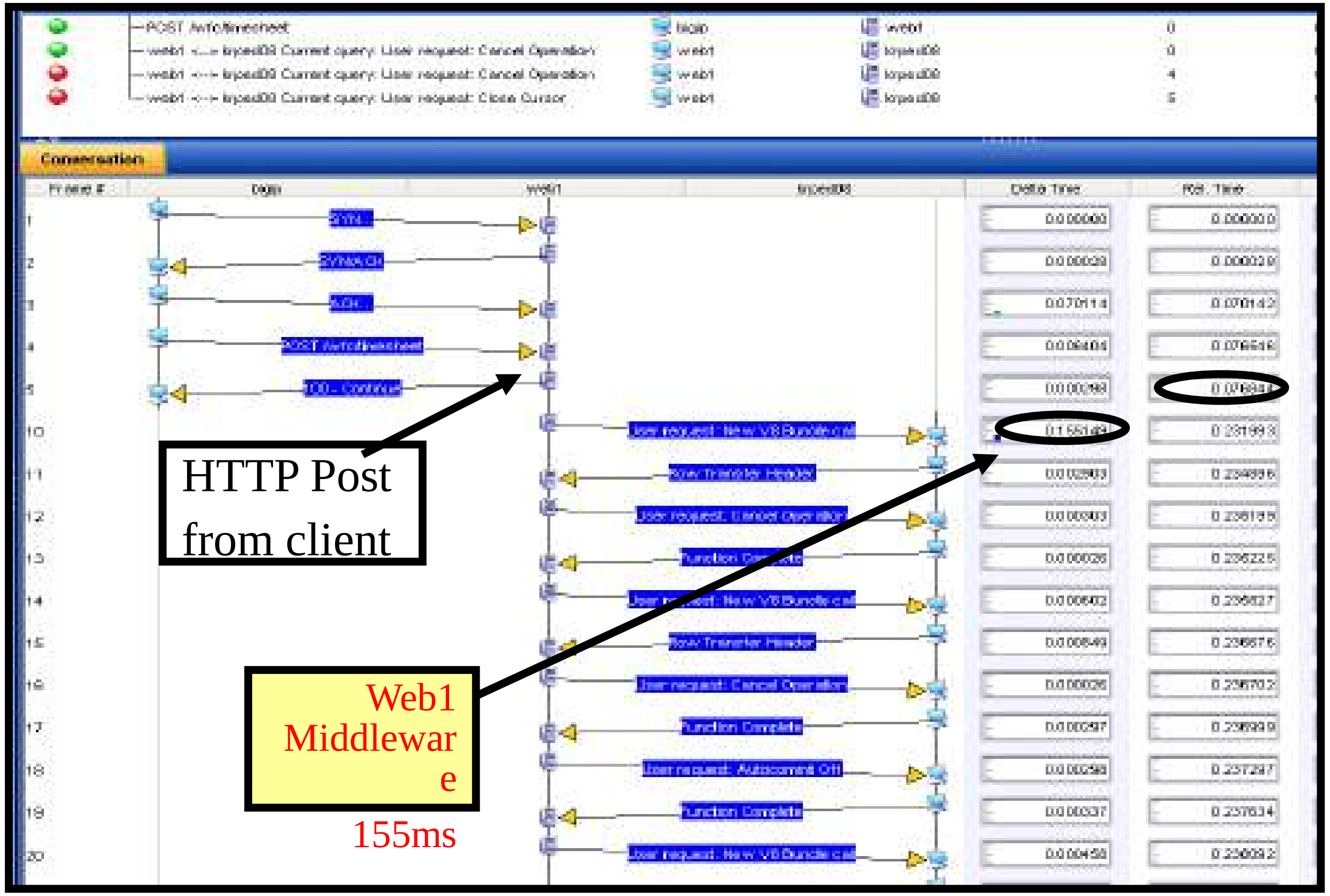
User Click
Client
Network
WebSvr
Network
AppSrv
Network
SQLSvr
Network
AppSvr
Network
Mainframe
Network
AppSvr
Network
WebSvr
Network
Client
User Display Update

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 <--> krpesd08 Current query: User request: Cancel Operation	web1	krpesd08	0
—web1 <--> krpesd08 Current query: User request: Cancel Operation	web1	krpesd08	4
—web1 <--> krpesd08 Current query: User request: Close Cursor	web1	krpesd08	5

Conversation

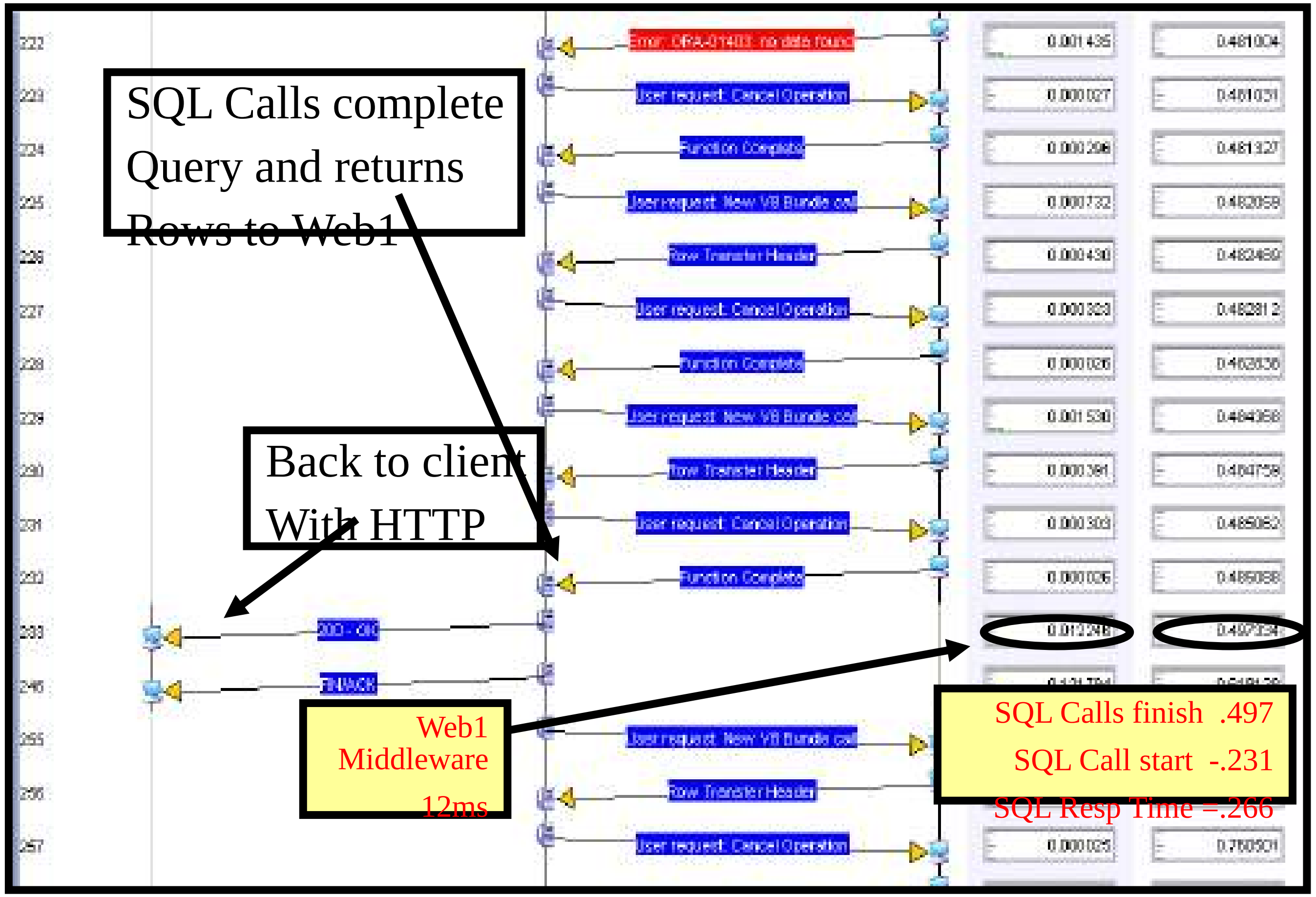
Frame #	bigip	web1	krpesd08	Delta Time	Rel. Time
1	SYN			0.000000	0.000000
2	SYN/ACK			0.000029	0.000029
3	ACK			0.070113	0.070142
4	POST /wfc/timesheet			0.006404	0.076546
5	100 - Continue			0.000298	0.076844
10		User request: New V8 Bundle call		0.155149	0.231993
11		Row Transfer Header		0.003903	0.235896
12		User request: Cancel Operation		0.000303	0.236199
13		Function Complete		0.000026	0.236225
14		User request: New V8 Bundle call		0.000402	0.236627
15		Row Transfer Header		0.000049	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	[illegible]	[illegible]
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

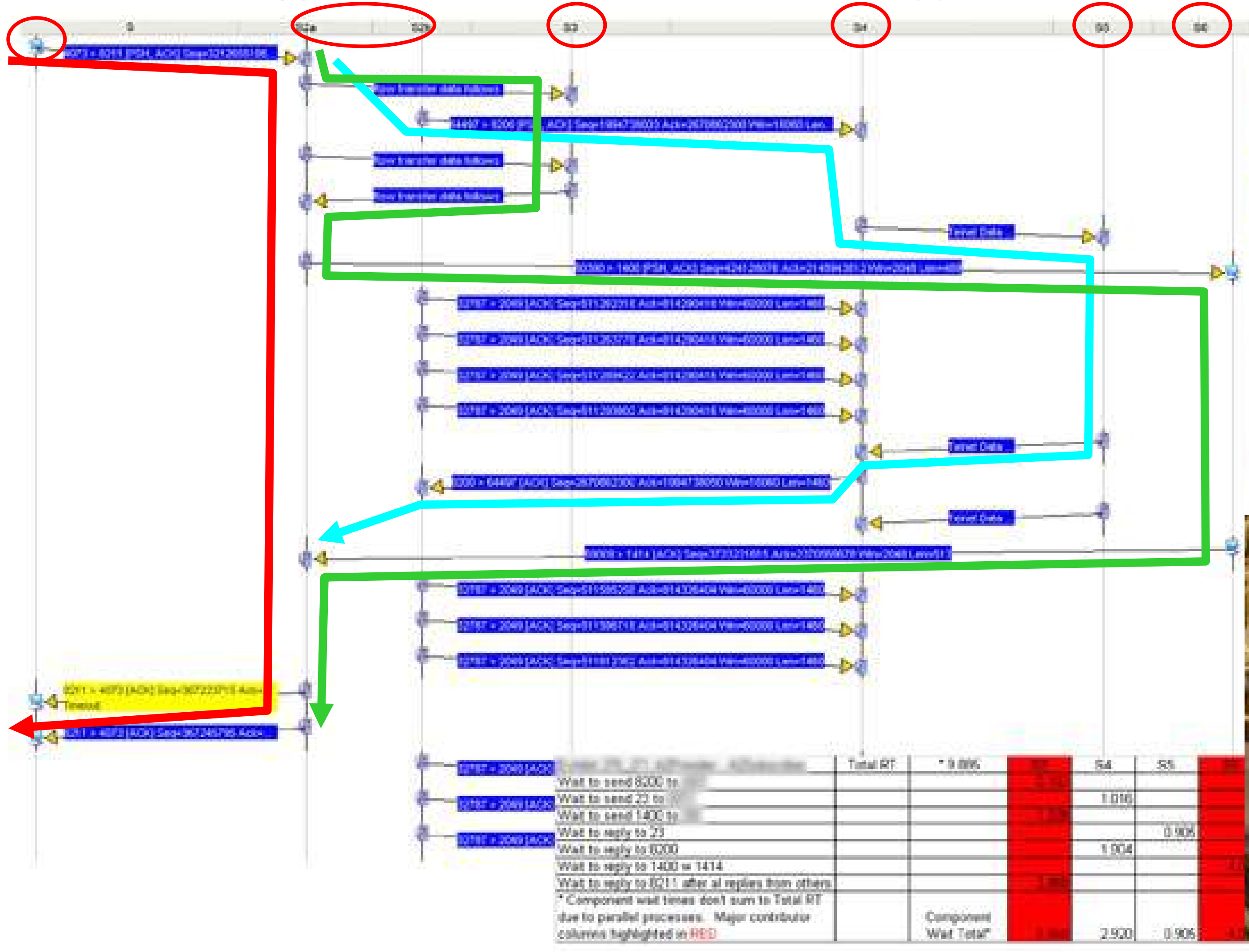
Back to client
With HTTP

Web1
Middleware
12ms

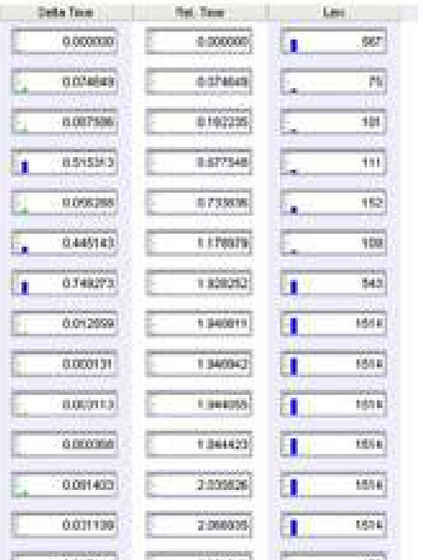
SQL Calls finish .497
SQL Call start -.231
SQL Resp Time =.266

Tier Micro-Analysis Phase

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



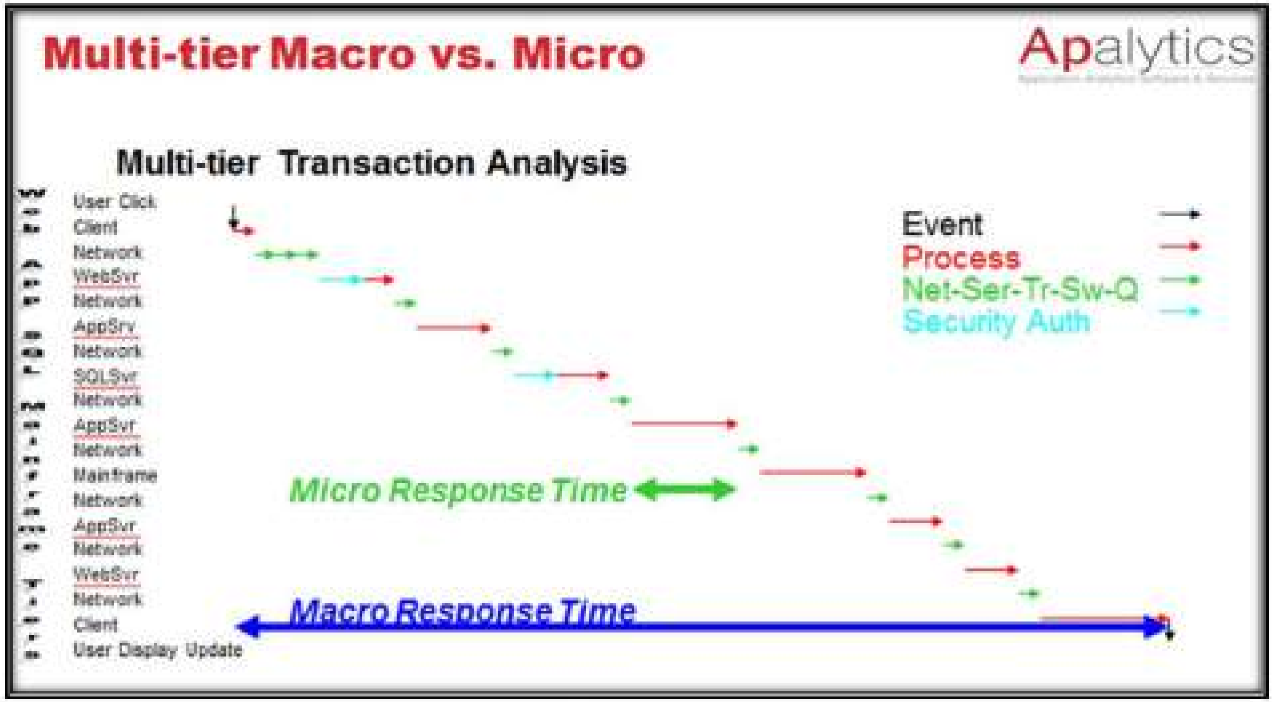
S
S2a
S2b
S3
S4
S5
S6
Row transfer data follows
Row transfer data follows
Row transfer data follows
Telnet Data
Telnet Data
Telnet Data
Timeout

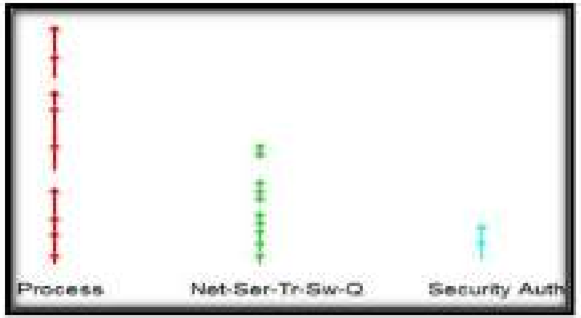


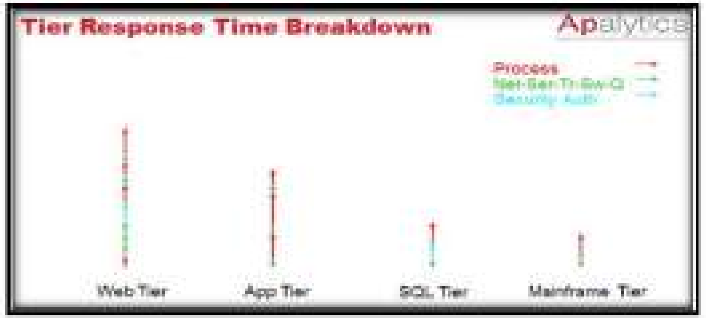
Delta Time	Rel. Time	Len
0.000000	0.000000	587
0.074649	0.074649	75
0.087586	0.162235	101
0.515313	0.677548	111
0.056288	0.733836	152
0.445143	1.178979	108
0.749273	1.928252	543
0.012559	1.940811	1514
0.000131	1.940942	1514
0.003113	1.944055	1514
0.000368	1.944423	1514
0.091403	2.035826	1514
0.031139	2.066965	1514

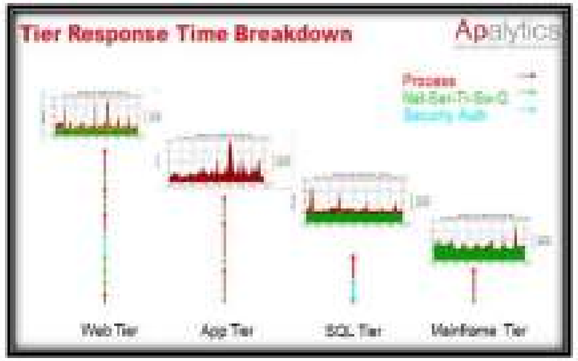
[redacted]	Total RT	* 9.895	[illegible]	S4	S5	[illegible]
Wait to send 8200 to [redacted]			[illegible]			
Wait to send 23 to [redacted]				1.016		
Wait to send 1400 to [redacted]			[illegible]			
Wait to reply to 23					0.905	
Wait to reply to 8200				1.904		
Wait to reply to 1400 w 1414						[illegible]
Wait to reply to 8211 after al replies from others			[illegible]			
* Component wait times don't sum to Total RT due to parallel processes. Major contributor columns highlighted in RED		Component Wait Total*	[illegible]	2.920	0.905	[illegible]

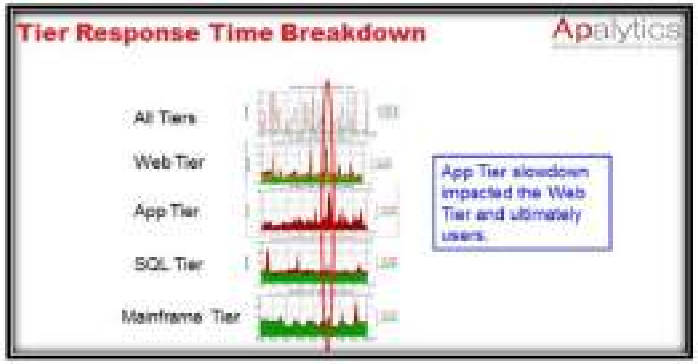
Summary of Multitier Monitoring





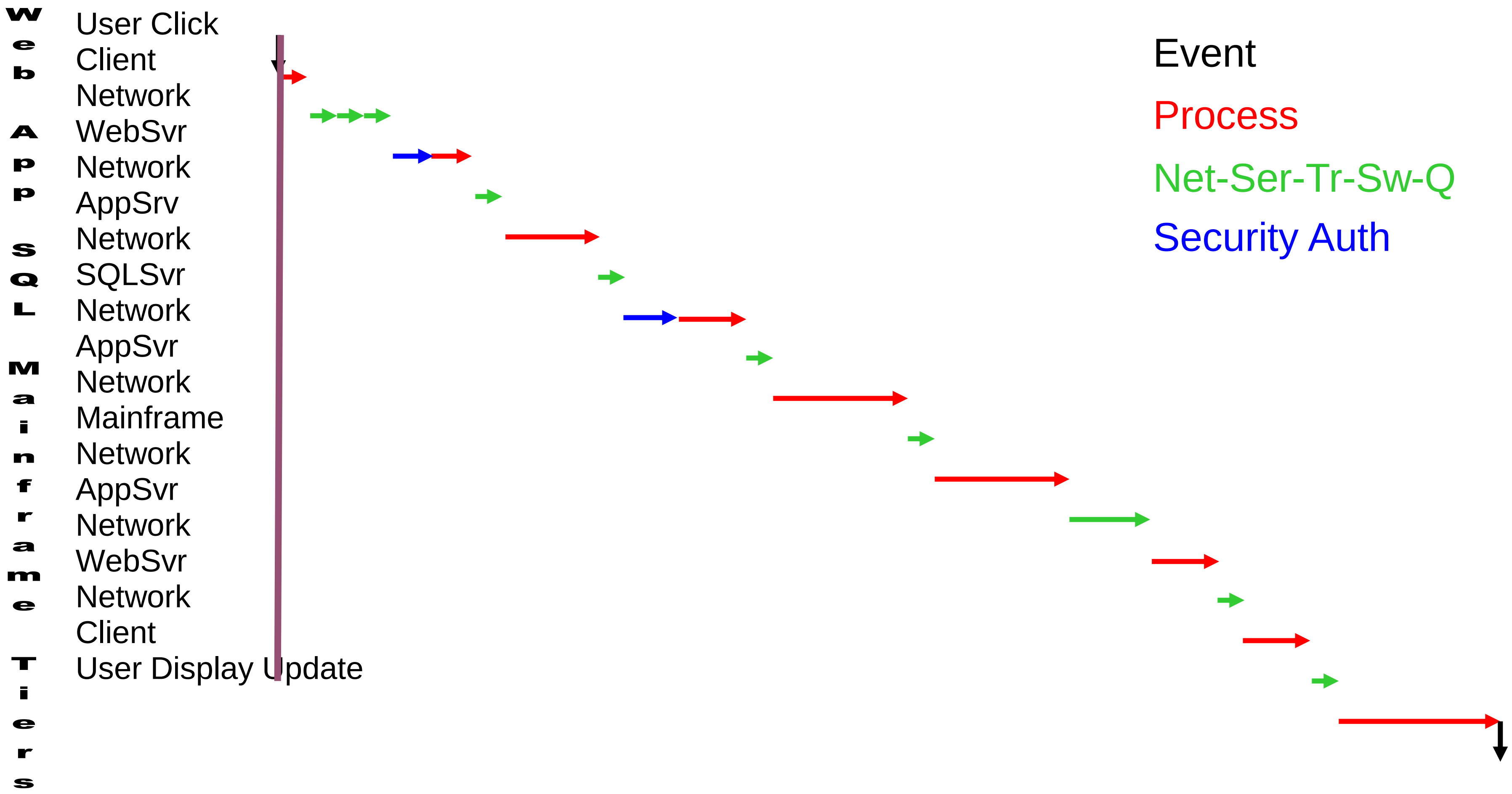






App Tier slowdown impacted the Web Tier and ultimately users.

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

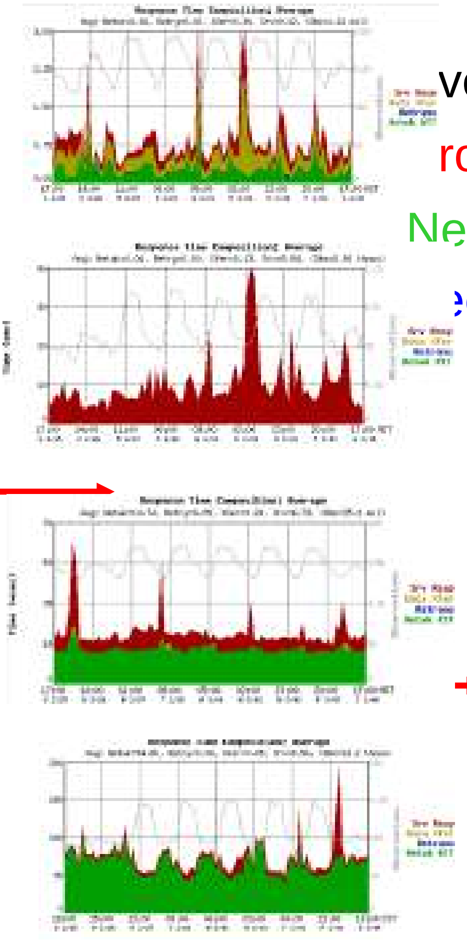
WebSvr

Network

Client

Mainframe Tier

Update



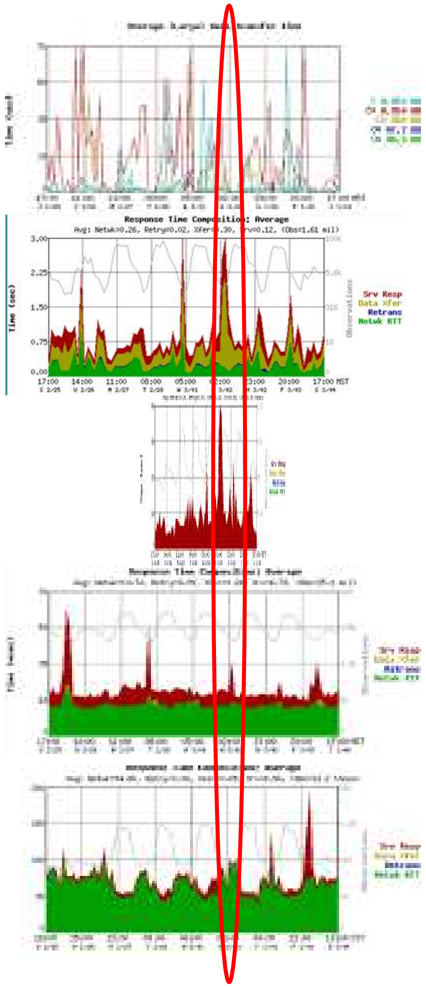
vent

rocess

Net-Ser-Tr-Sw-Q

ecurity Auth

Tier Response Time Breakdown



All Tiers

Web Tier

App
Tier

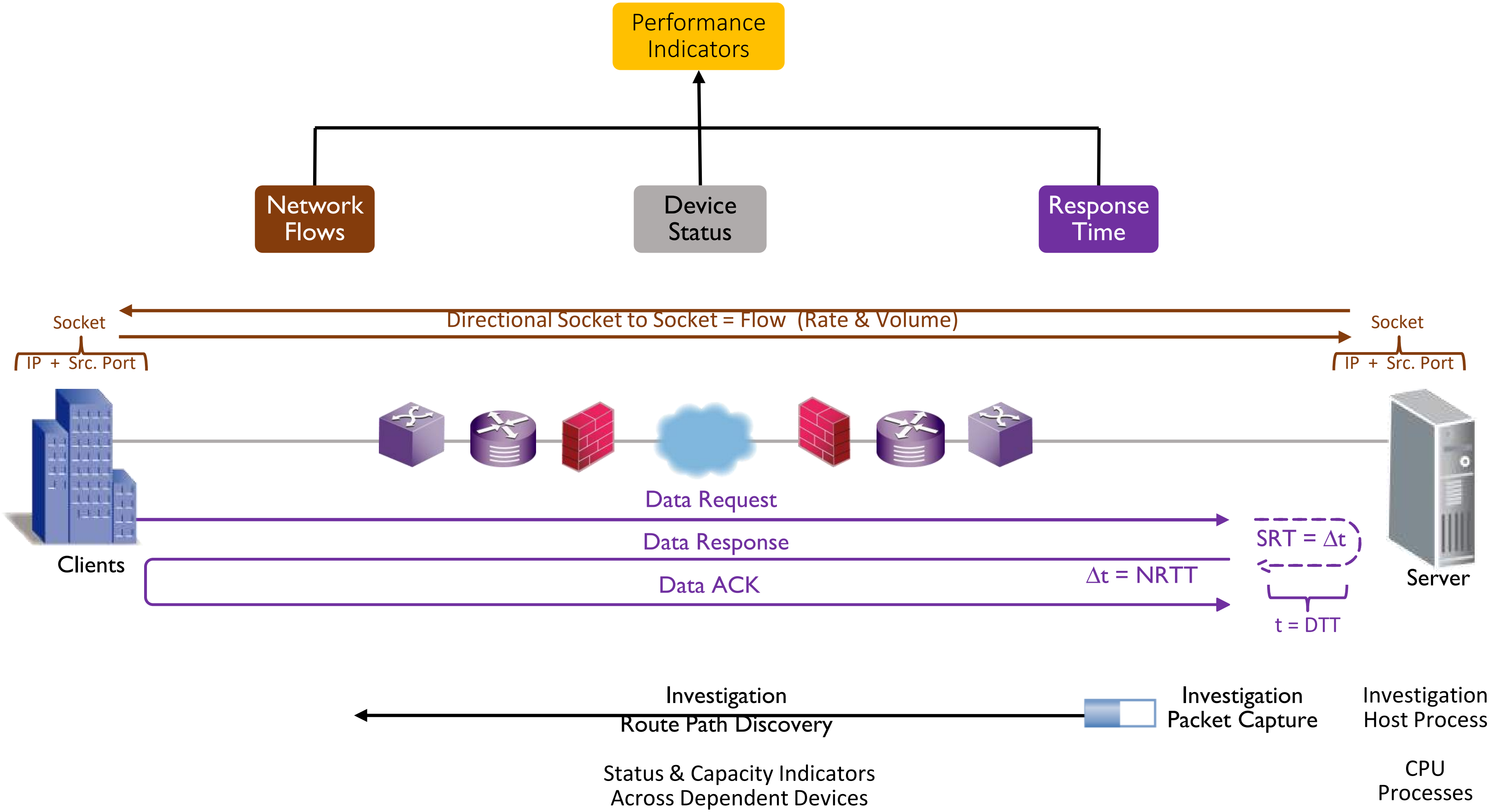
SQL Tier

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

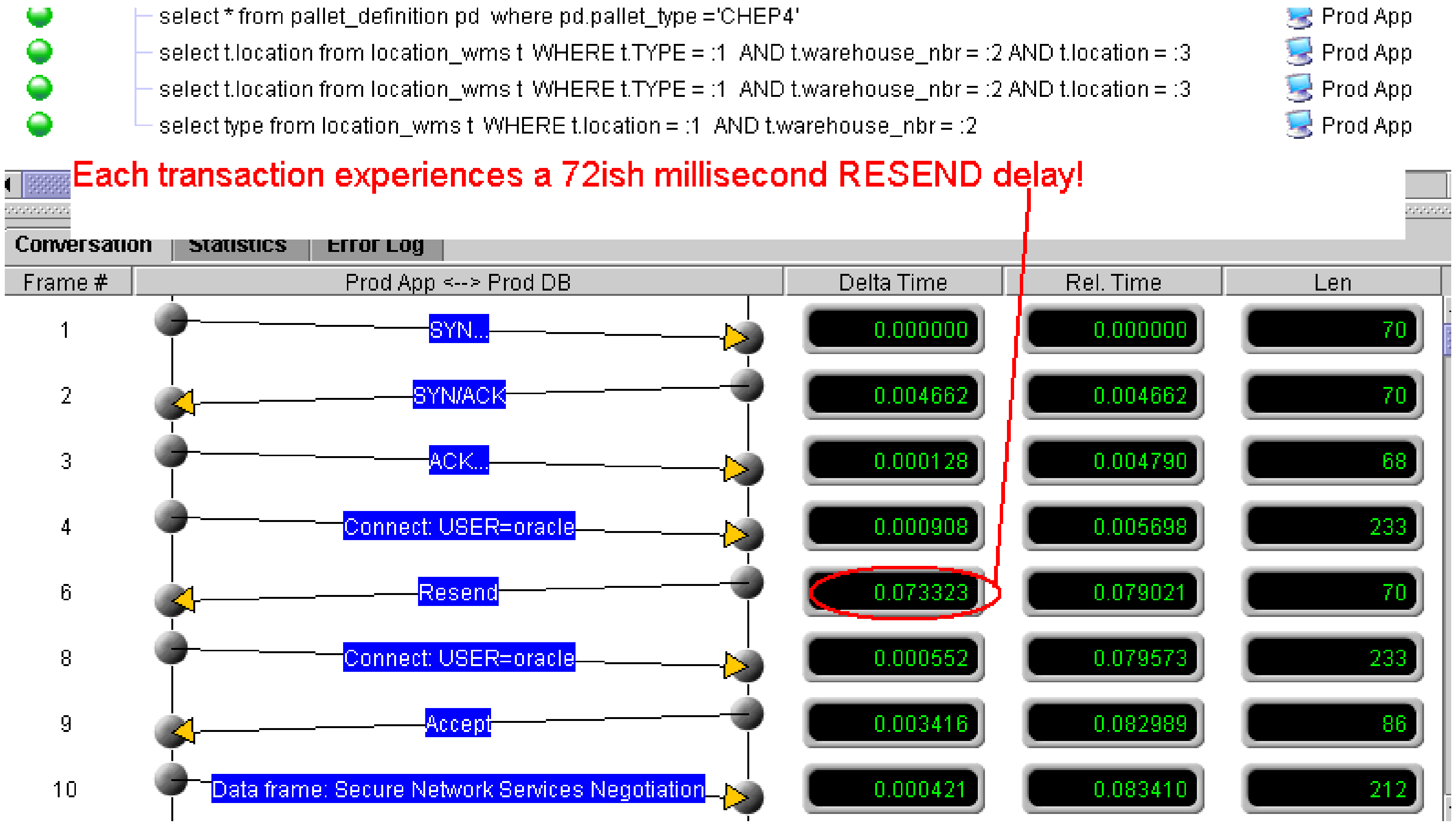
Each slide that follows explains and illustrates the key to many past problems…

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

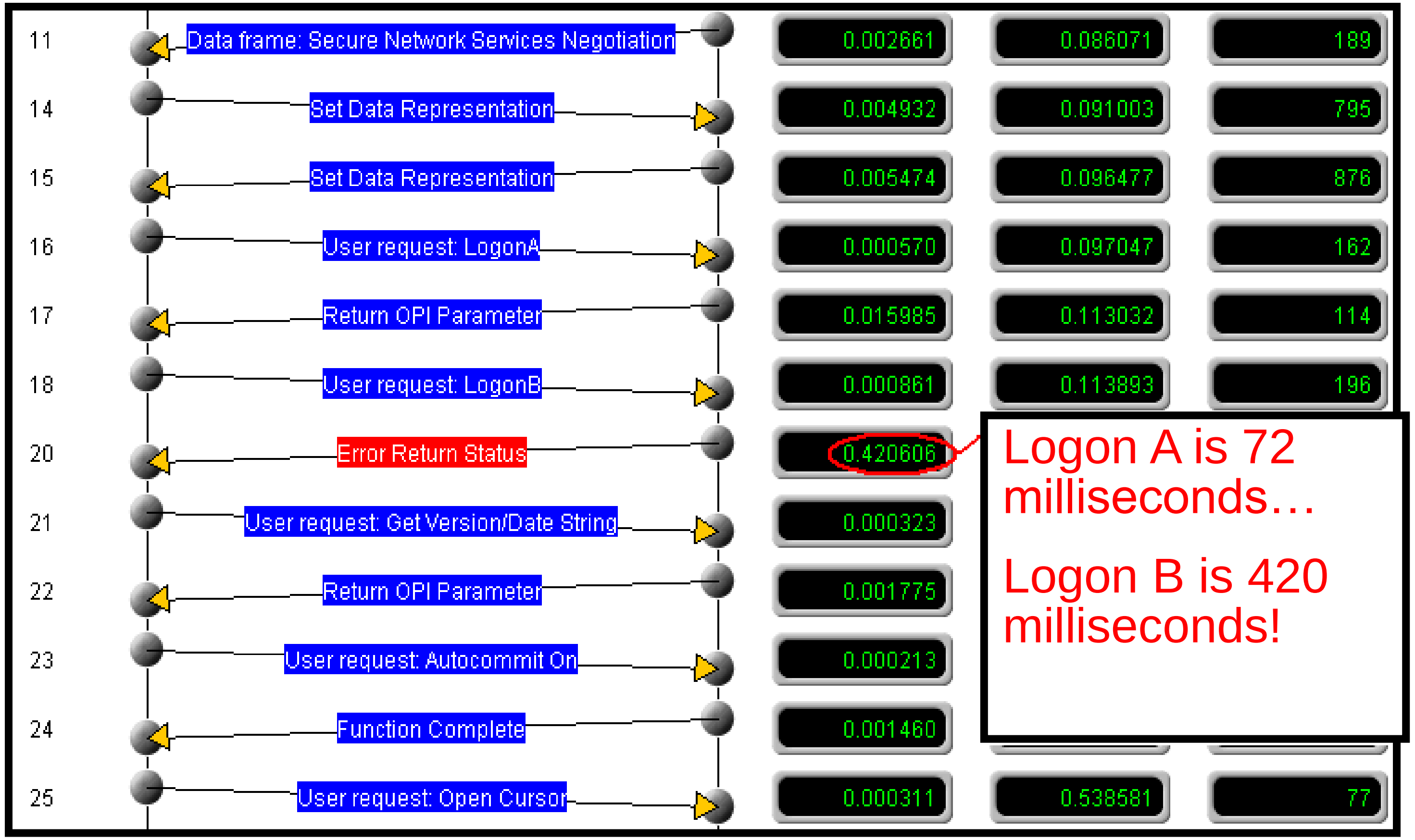


```
select * from pallet_definition pd  where pd.pallet_type ='CHEP4'                                      Prod App
select t.location from location_wms t  WHERE t.TYPE = :1  AND t.warehouse_nbr = :2 AND t.location = :3  Prod App
select t.location from location_wms t  WHERE t.TYPE = :1  AND t.warehouse_nbr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

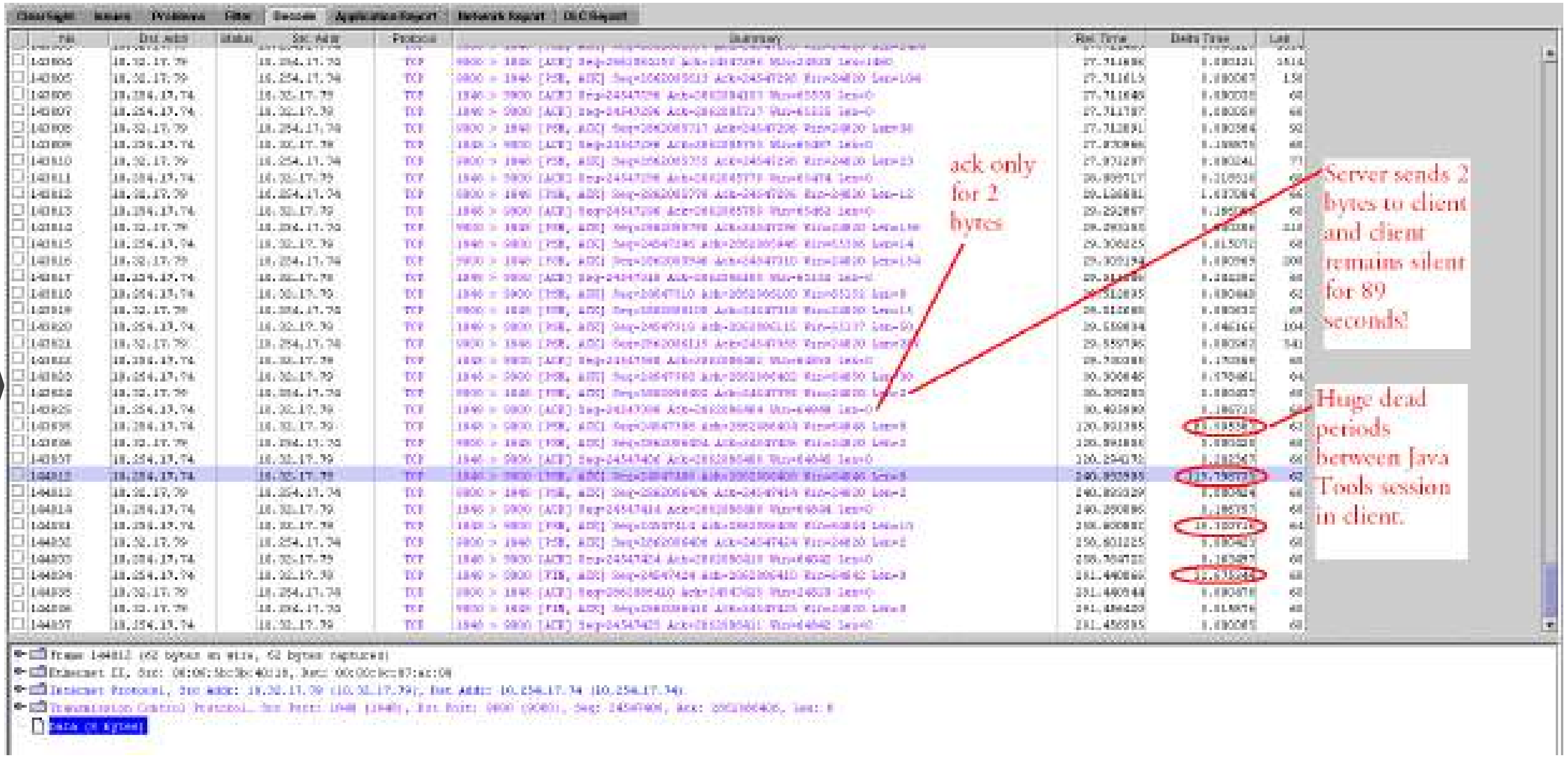


11	Data frame: Secure Network Services Negotiation	0.002661	0.086071	189
14	Set Data Representation	0.004932	0.091003	795
15	Set Data Representation	0.005474	0.096477	876
16	User request: LogonA	0.000570	0.097047	162
17	Return OPI Parameter	0.015985	0.113032	114
18	User request: LogonB	0.000861	0.113893	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

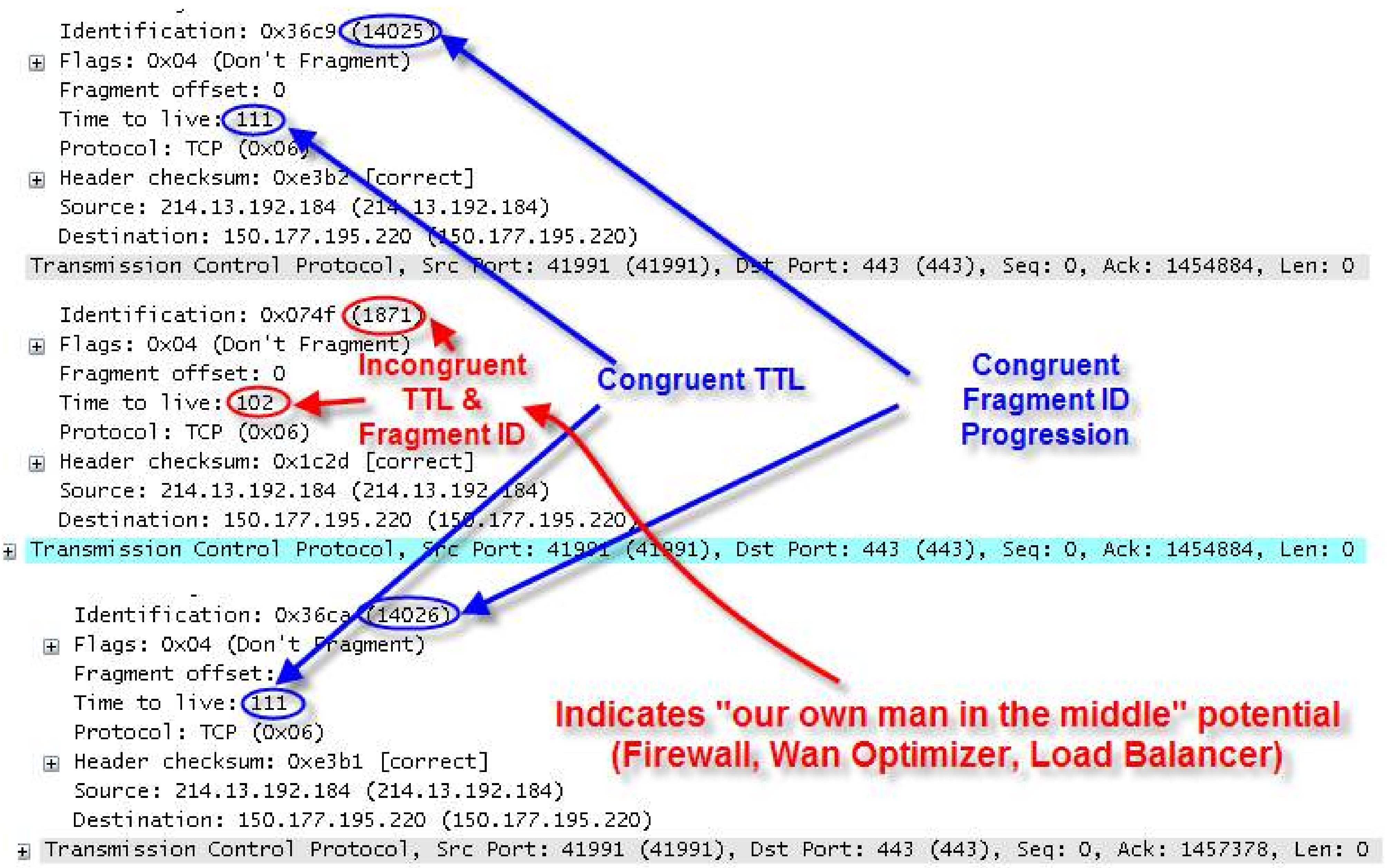


ack only for 2 bytes

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: 0
    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
```

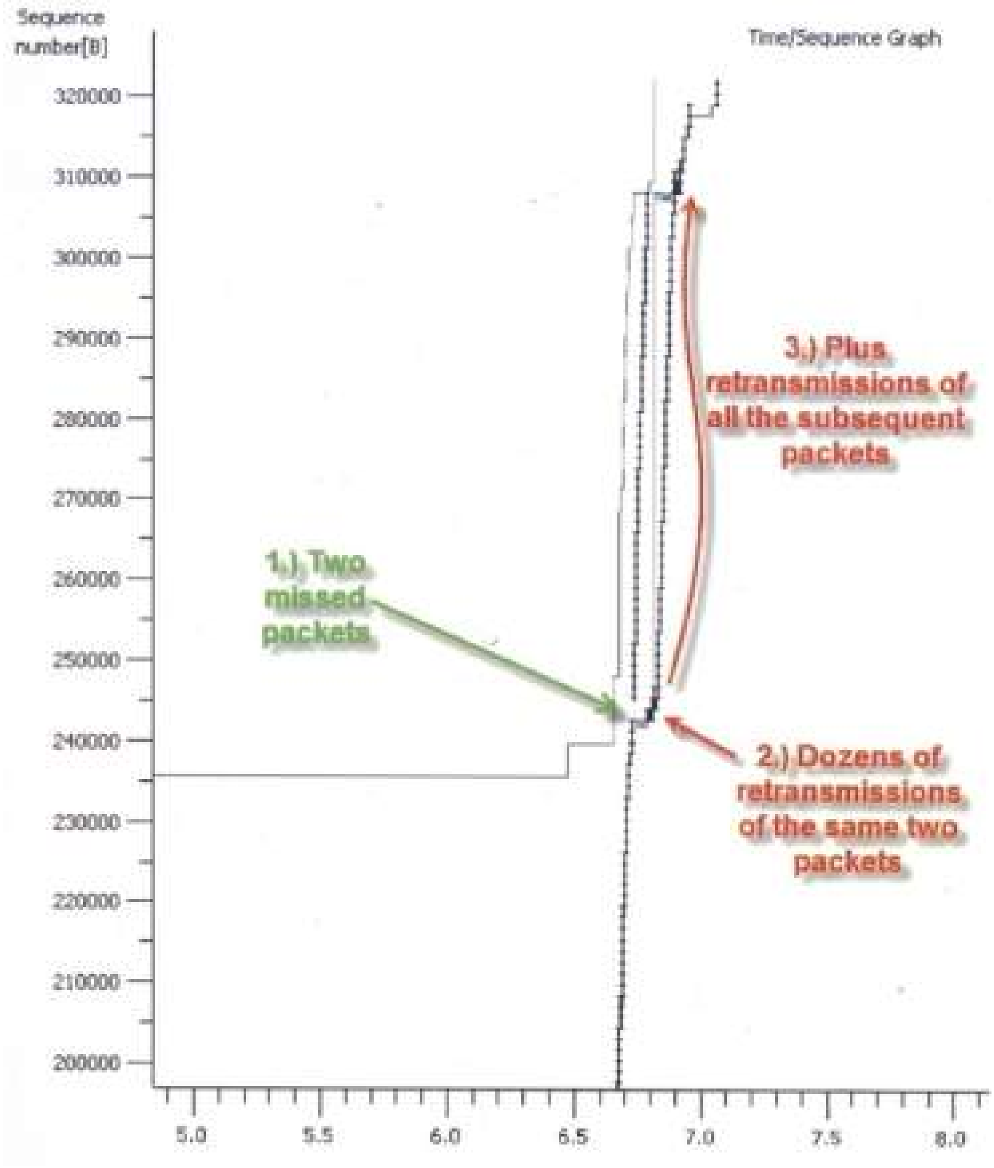
Incongruent TTL & Fragment ID

Congruent TTL

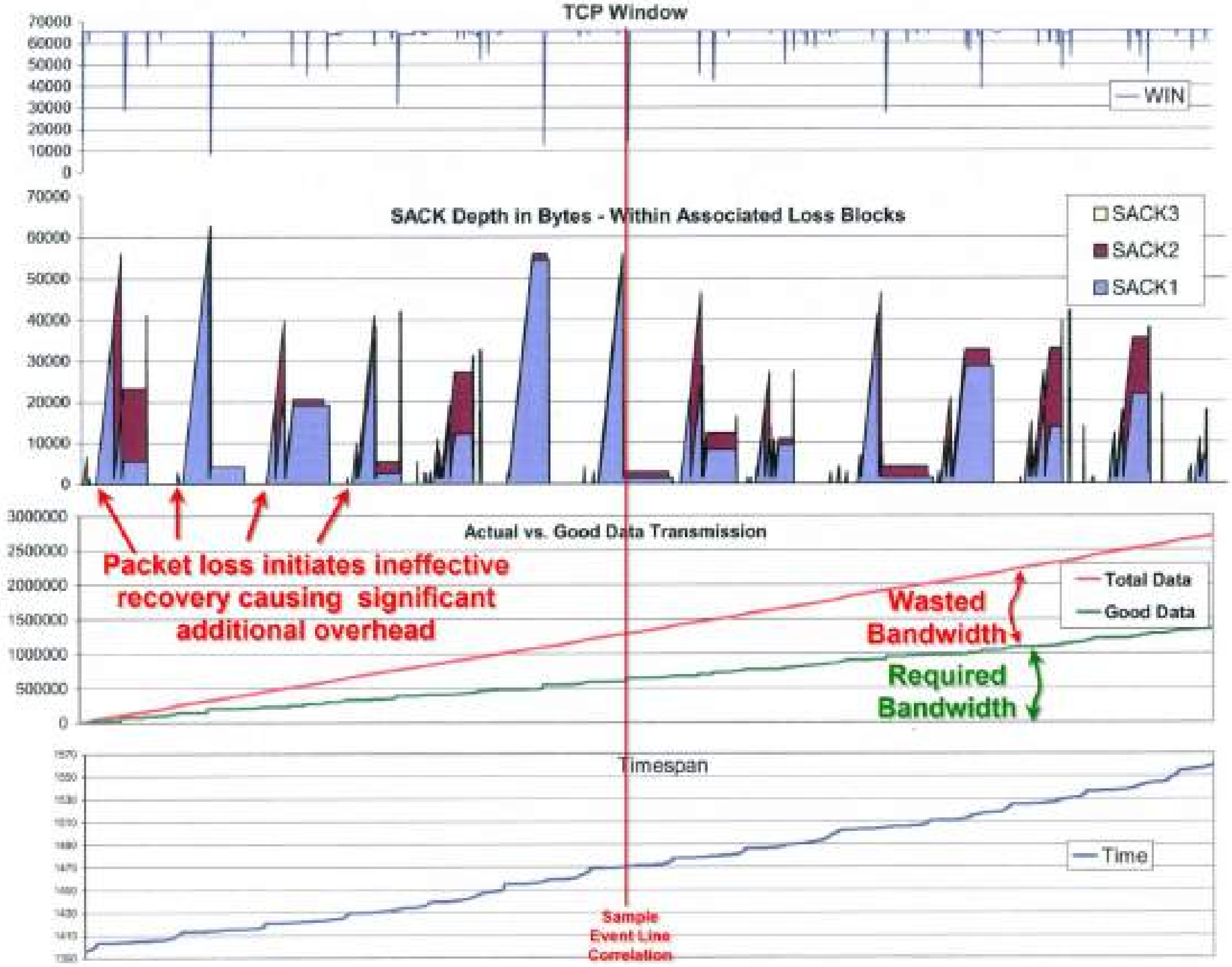
Congruent Fragment ID Progression

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

TCP Data Duplication Details



Significant Data Duplication



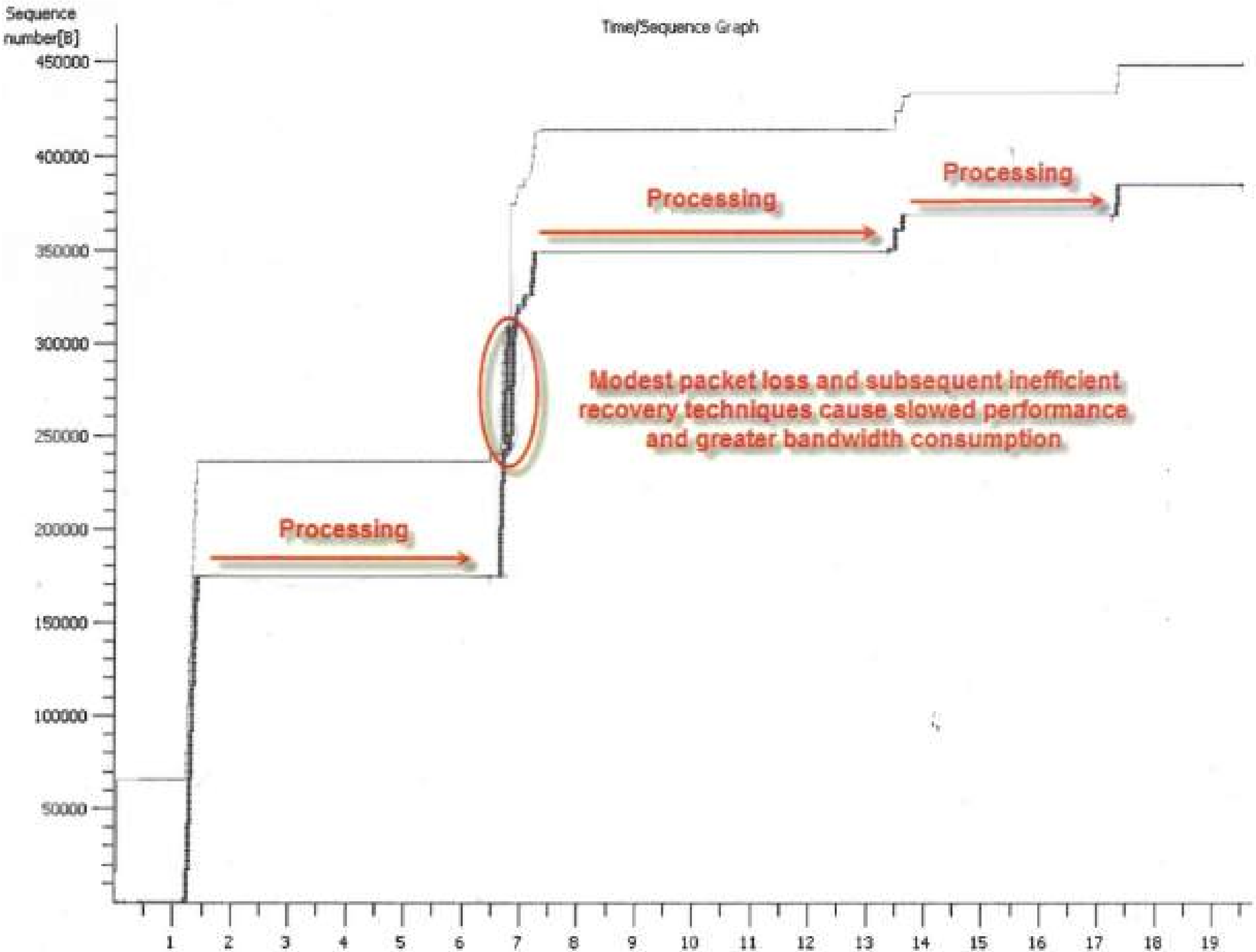
Packet loss initiates ineffective recovery causing significant additional overhead

Wasted Bandwidth

Required Bandwidth

Sample Event Line Correlation

Data Duplication & App Processing

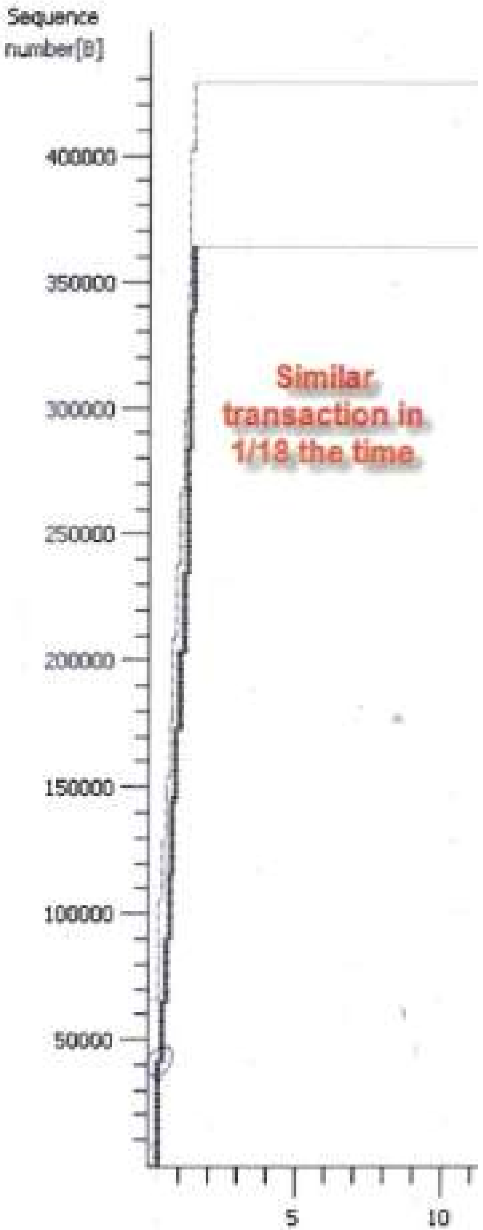


Processing

Processing

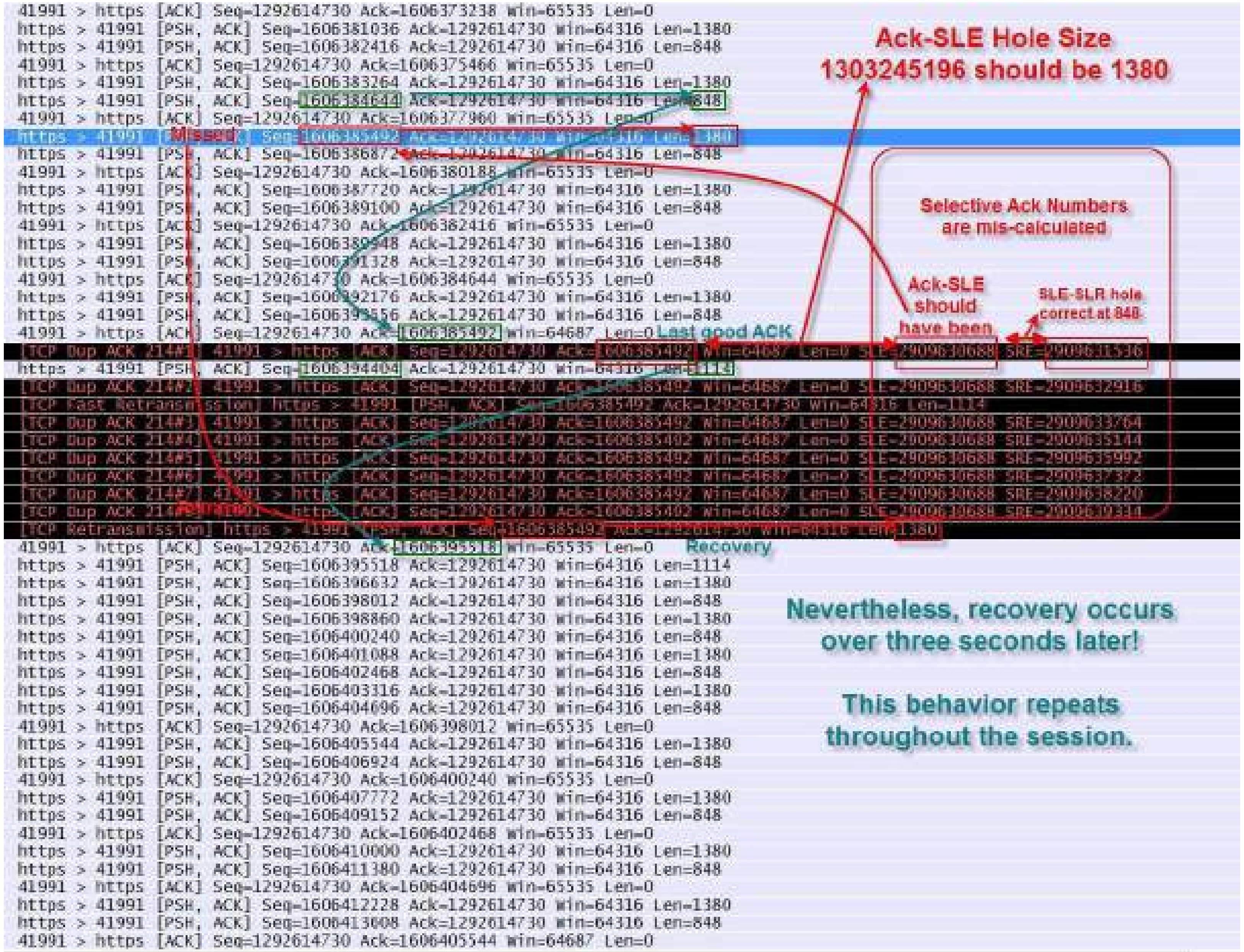
Processing

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
```

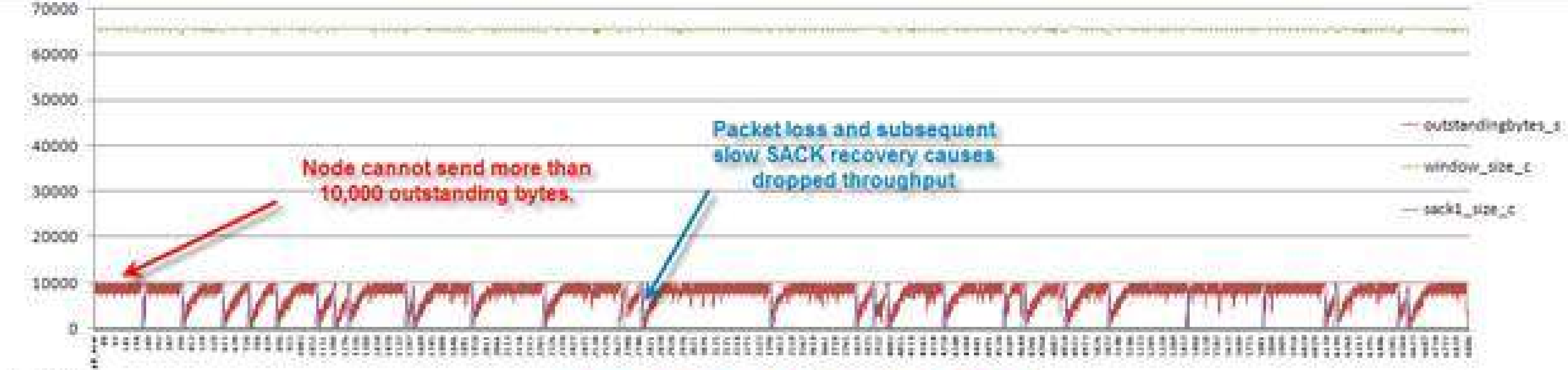
Missed
Last good ACK
Retransmission
Recovery
Selective Ack Numbers are mis-calculated
Ack-SLE should have been
SLE-SLR hole correct at 848

Ack-SLE Hole Size 1303245196 should be 1380

Nevertheless, recovery occurs over three seconds later!

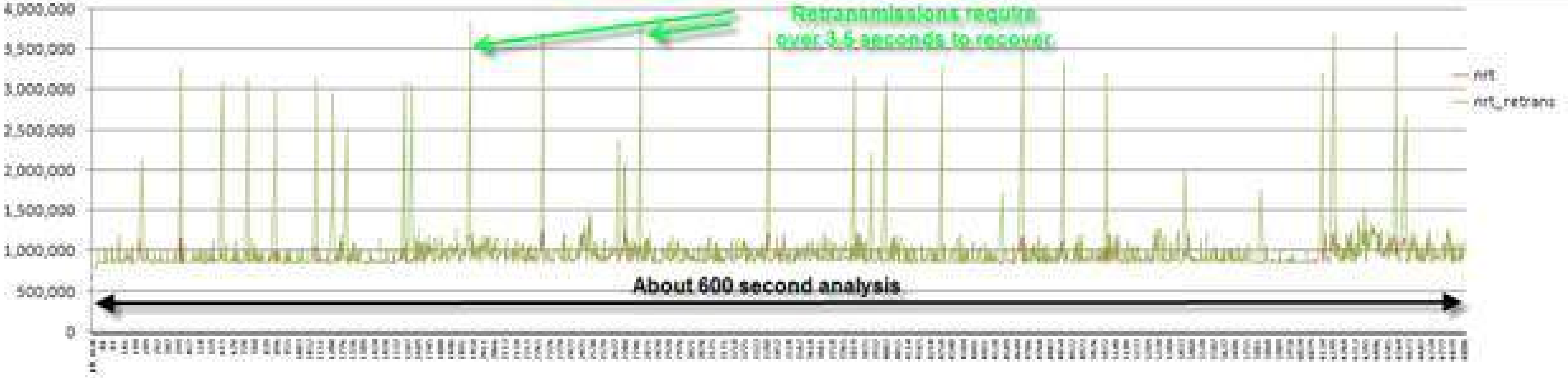
This behavior repeats throughout the session.

TCP – Session Performance



Node cannot send more than 10,000 outstanding bytes.

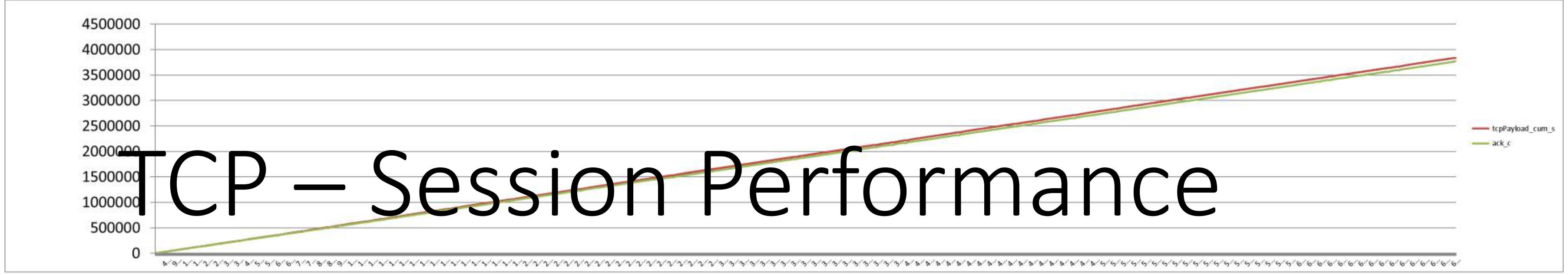
Packet loss and subsequent slow SACK recovery causes dropped throughput

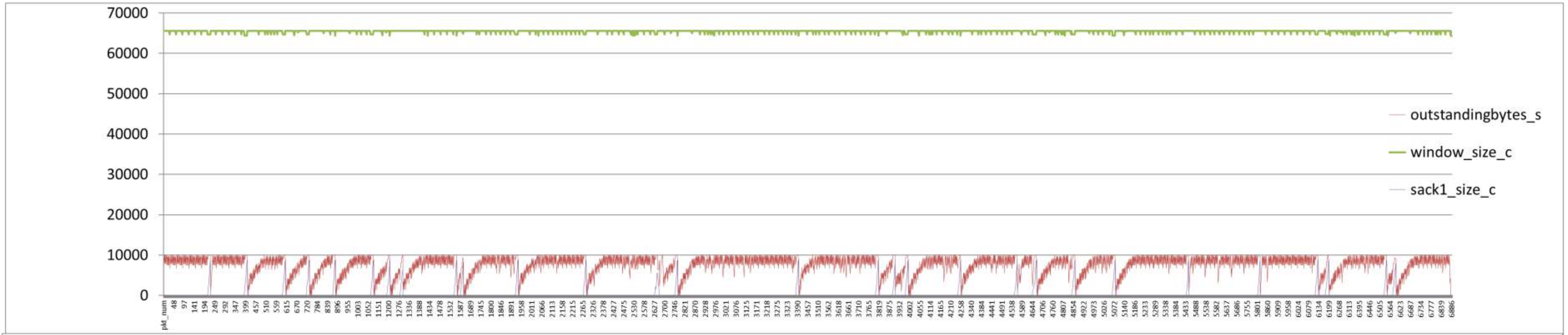


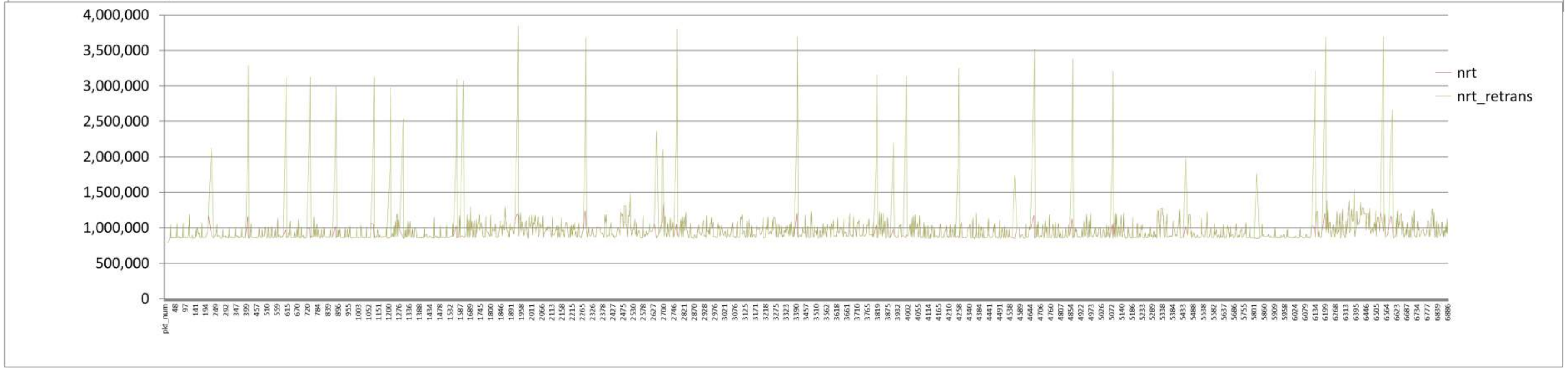
Retransmissions require over 3.5 seconds to recover

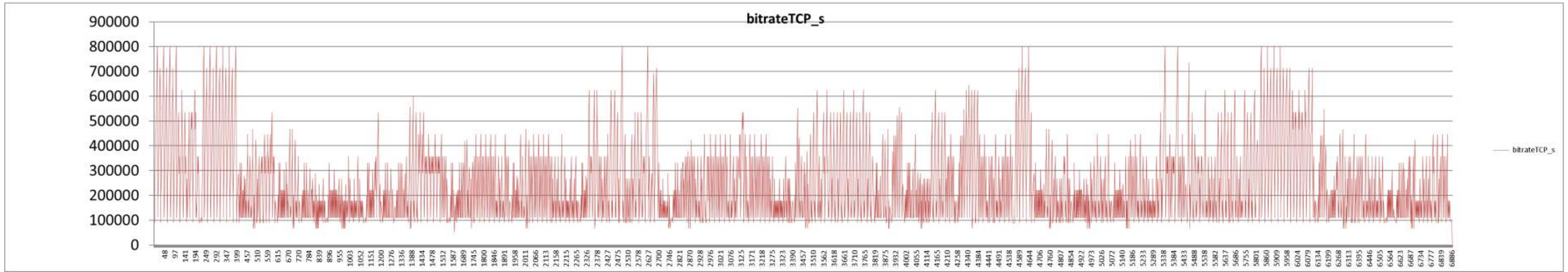
About 600 second analysis

TCP – Session Performance







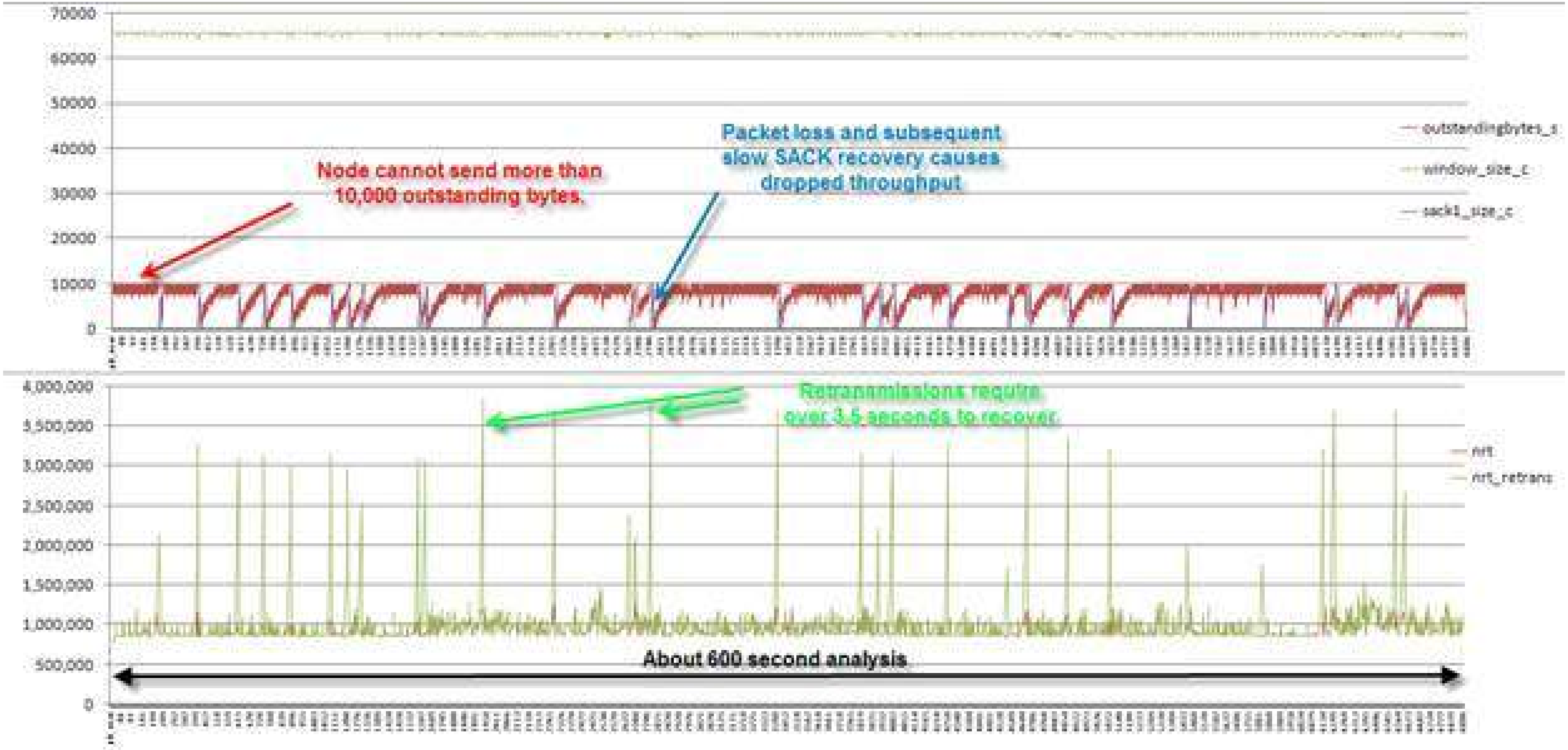


600 Seconds
4MB Data = 6666Bps
3.5 Sec Retrans Recovery

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.

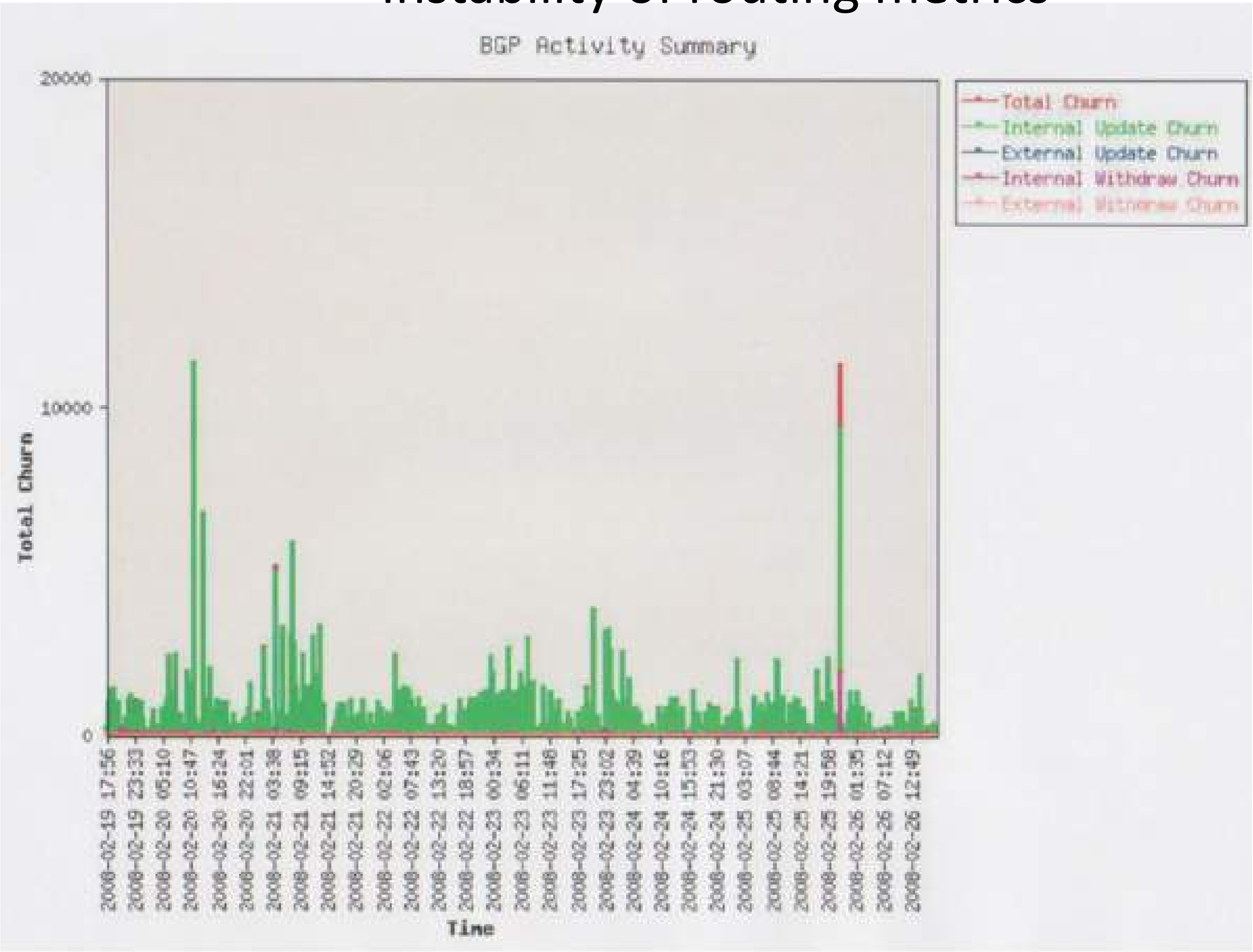
Packet loss and subsequent slow SACK recovery causes dropped throughput

Retransmissions require over 3.5 seconds to recover.

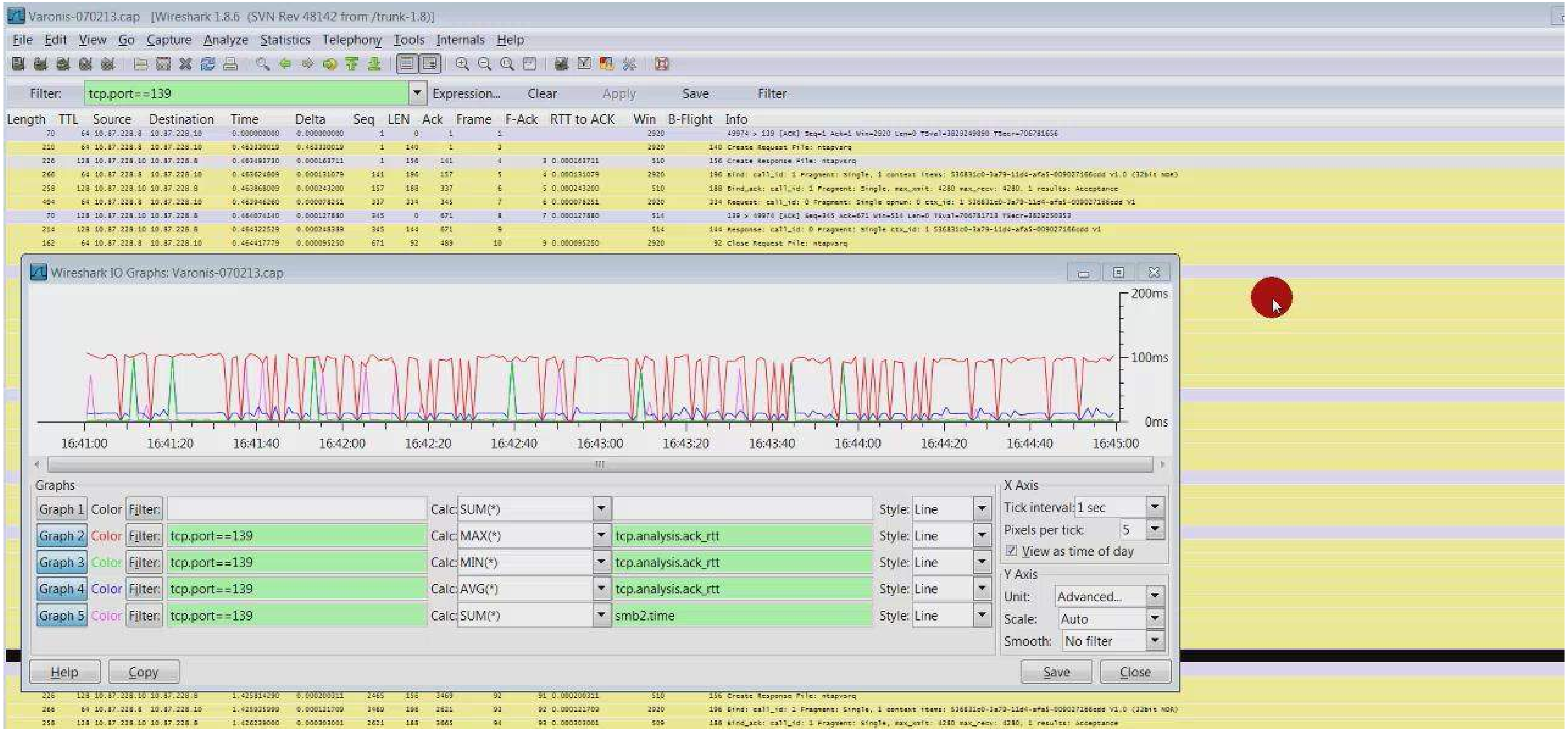
About 600 second analysis

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=3829249850 TSecr=706781656
   210  64 10.87.228.8  10.87.228.10 0.463330019 0.463330019    1 140    1     2                     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
   260  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=706781713 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
```

Graphs

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

X Axis

Tick interval: 1 sec

Pixels per tick: 5

☑ View as time of day

Y Axis

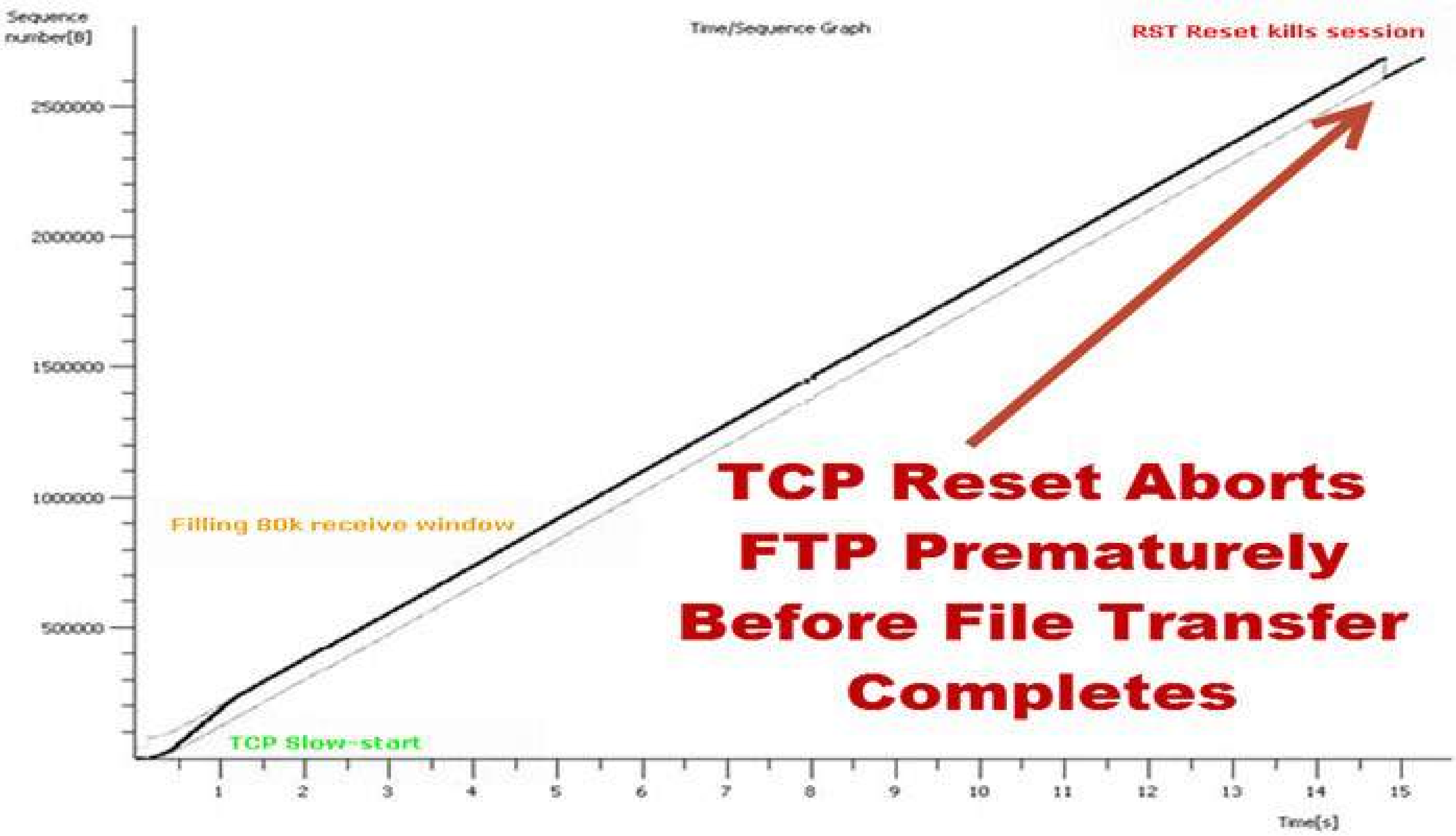
Unit: Advanced...

Scale: Auto

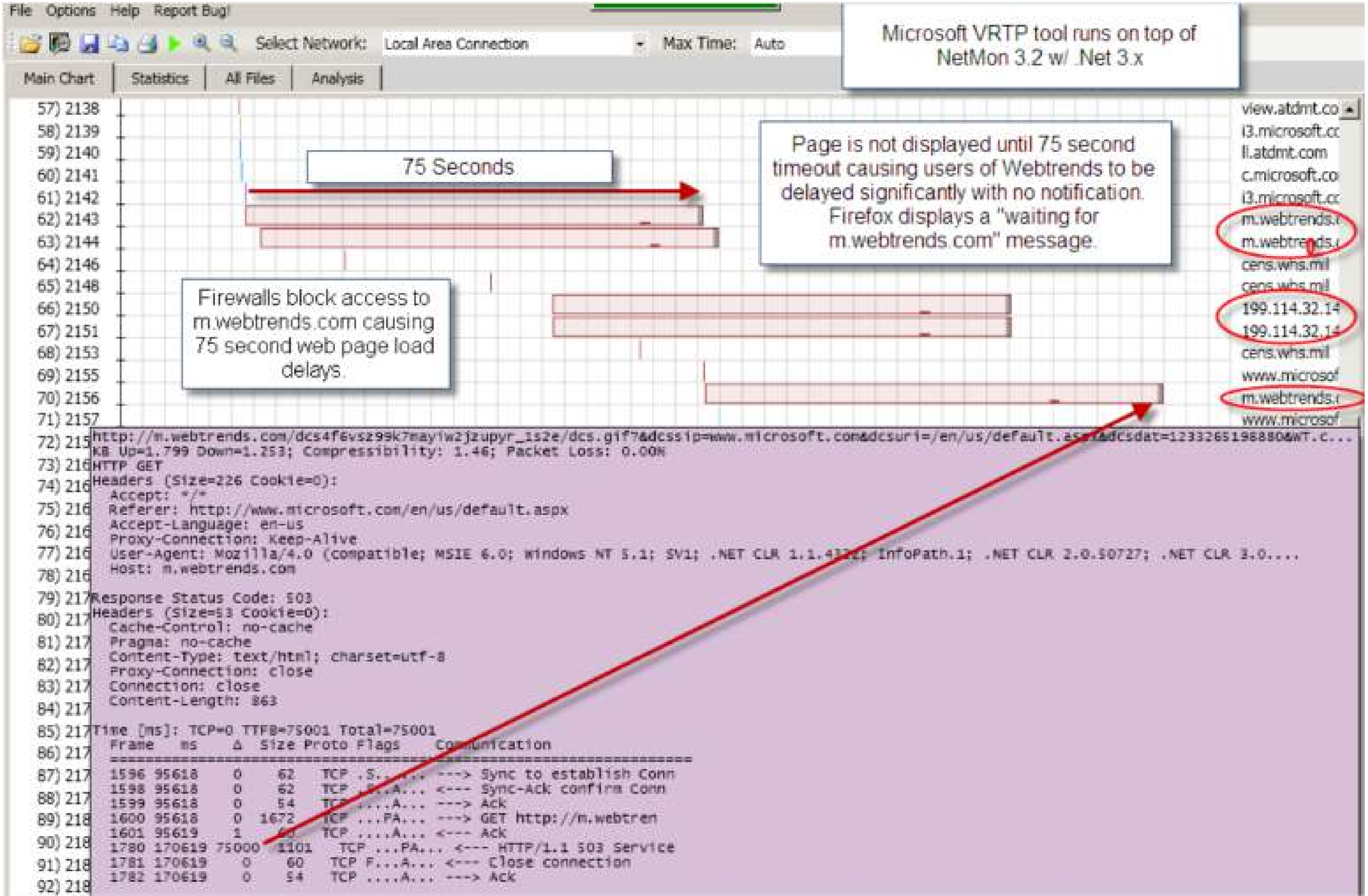
Smooth: No filter

```
   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
```

FTP Fail due to Reset



TCP Reset Aborts FTP Prematurely Before File Transfer Completes



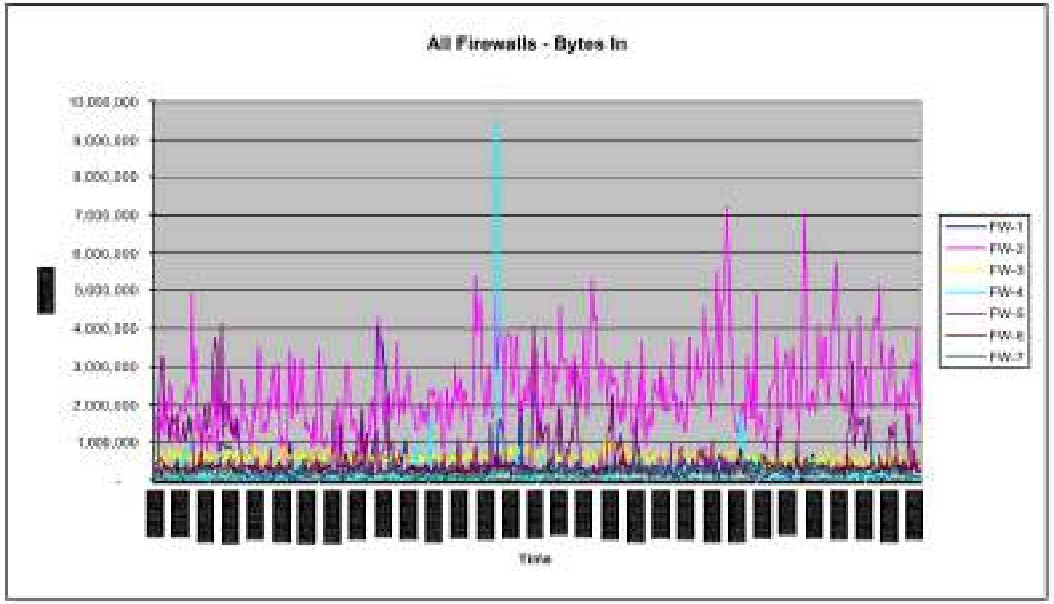
Microsoft VRTP tool runs on top of NetMon 3.2 w/ .Net 3.x

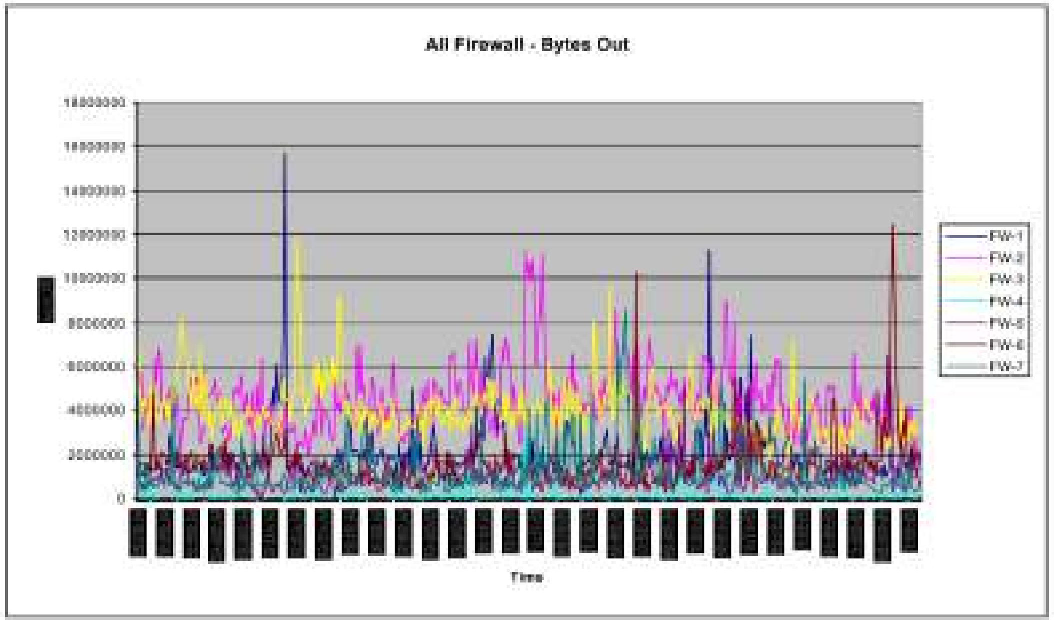
Page is not displayed until 75 second timeout causing users of Webtrends to be delayed significantly with no notification. Firefox displays a "waiting for m.webtrends.com" message.

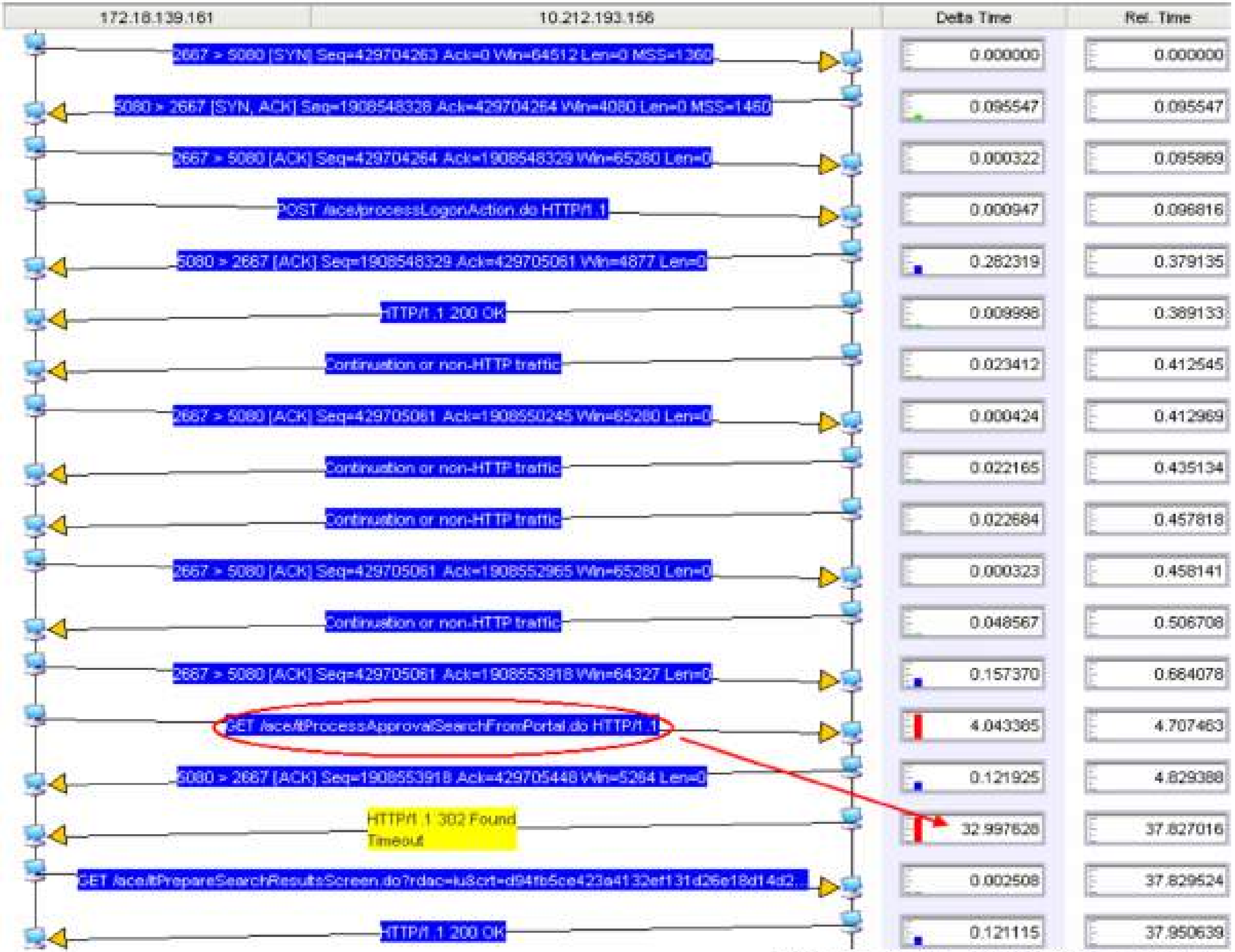
Firewalls block access to m.webtrends.com causing 75 second web page load delays.

```
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/tProcessApprovalSearchFromPortal.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/tPrepareSearchResultsScreen.do?rdac=iu8crt=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)

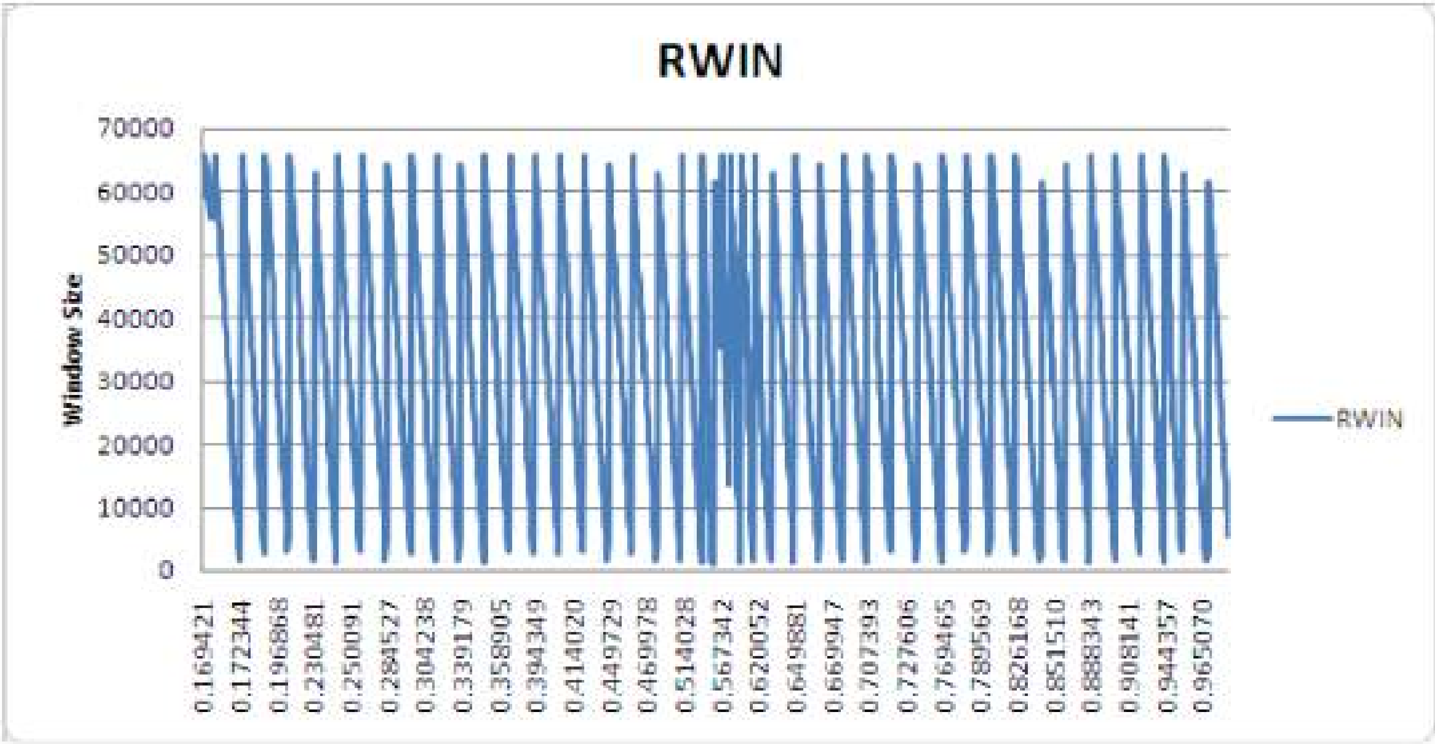
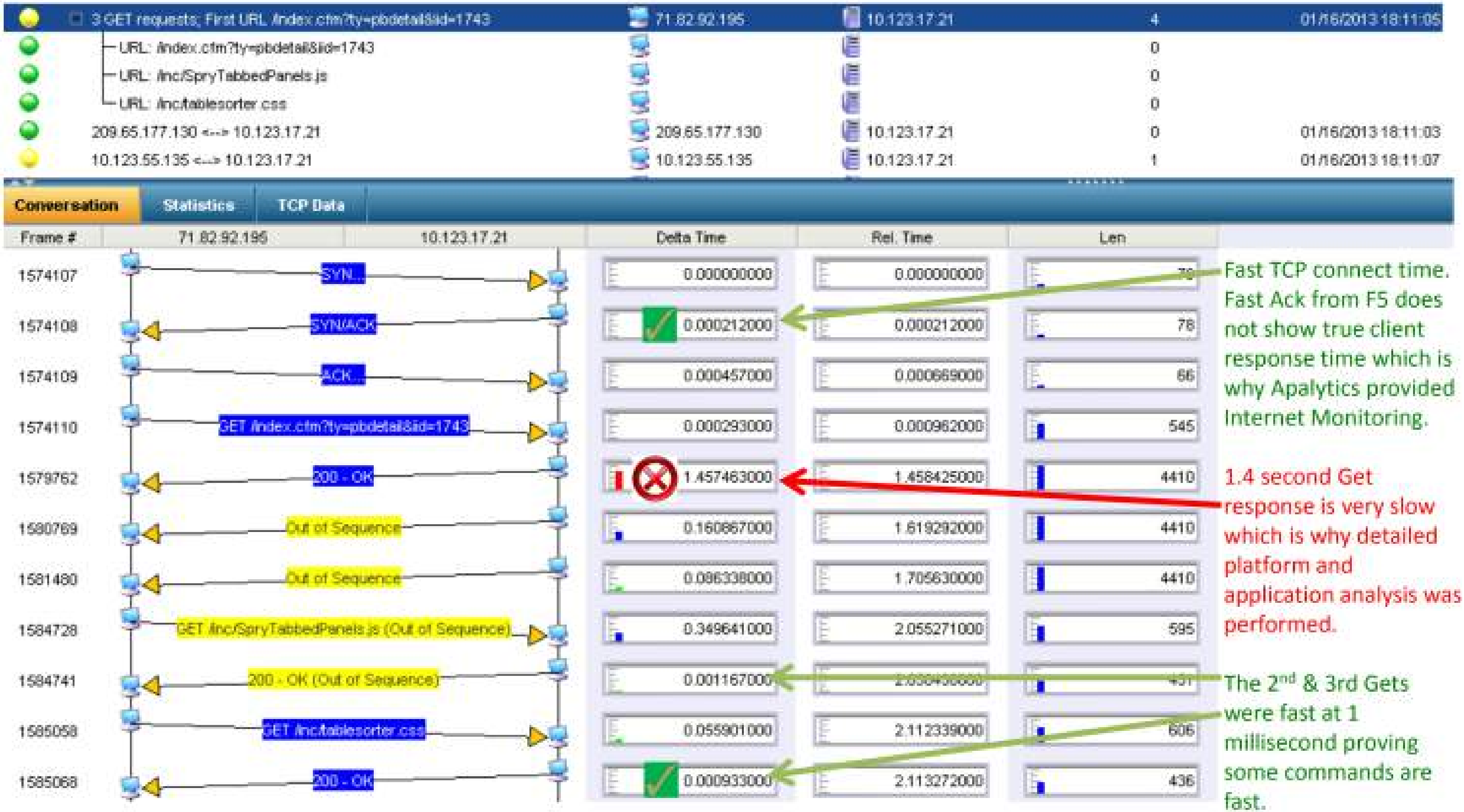


Figure 26: WAPPBI01 TCP Receive Window Size Behavior

HTTP Response Times



●	□ 3 GET requests; First URL /index.cfm?ty=pbdetail&id=1743	71.82.92.195	10.123.17.21	4	01/16/2013 18:11:05
●	URL: /index.cfm?ty=pbdetail&id=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

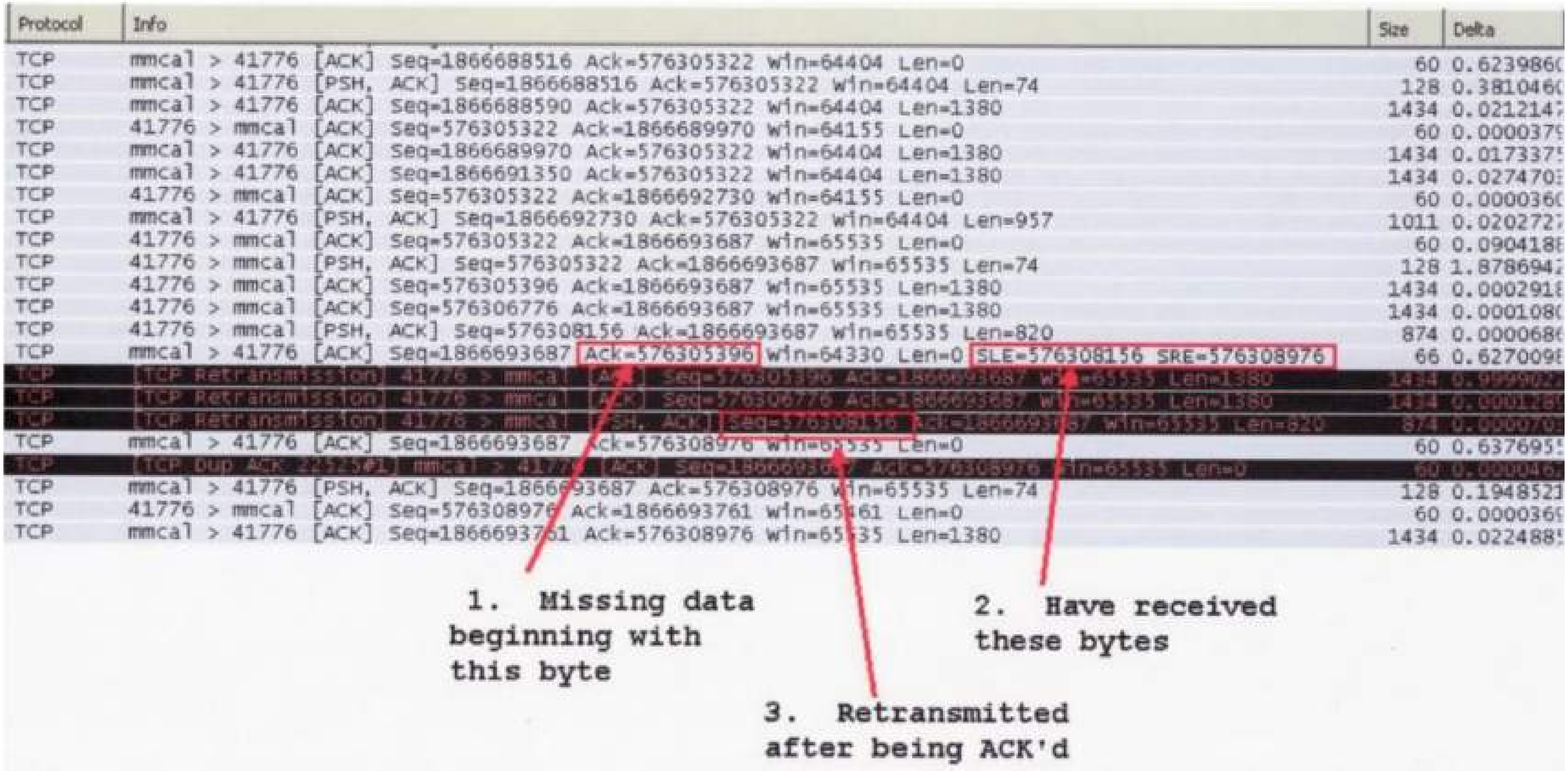
Frame #	71.82.92.195	10.123.17.21	Delta Time	Rel. Time	Len
1574107	SYN...		0.000000000	0.000000000	78
1574108		SYN/ACK	✓ 0.000212000	0.000212000	78
1574109	ACK...		0.000457000	0.000669000	66
1574110	GET /index.cfm?ty=pbdetail&id=1743		0.000293000	0.000962000	545
1579762		200 - OK	⊗ 1.457463000	1.458425000	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	[illegible]	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



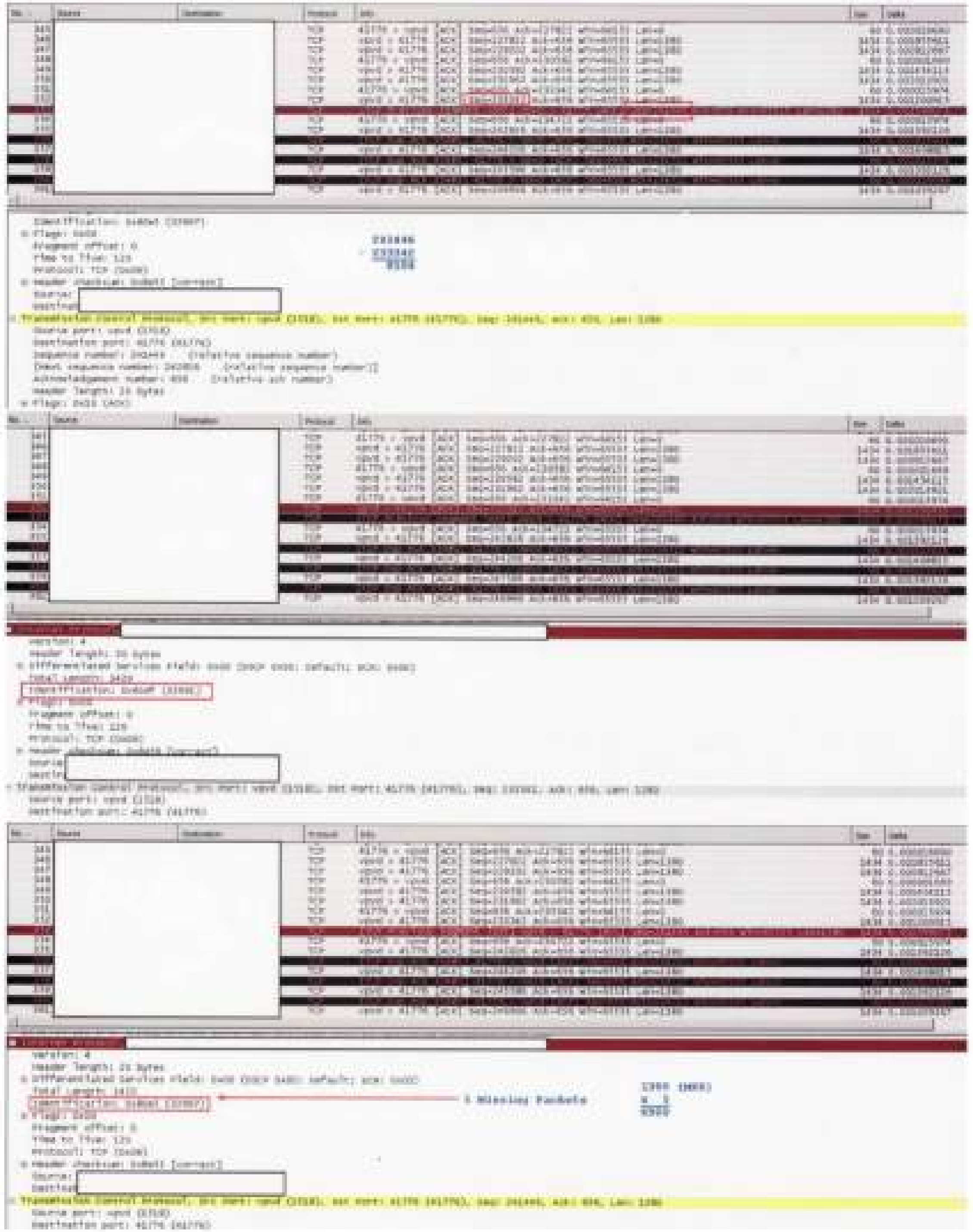
```
Protocol  Info                                                                                           Size  Delta
TCP       mmcal > 41776 [ACK] Seq=1866688516 Ack=576305322 Win=64404 Len=0                                 60 0.623986
TCP       mmcal > 41776 [PSH, ACK] Seq=1866688516 Ack=576305322 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



```
Identification: 0x80a4 (32932)
⊞ Flags: 0x02
  Fragment offset: 0
  Time to live: 125
  Protocol: TCP (0x06)
⊞ Header checksum: 0x0e01 [correct]
  Source: [redacted]
  Destination: [redacted]
⊟ Transmission Control Protocol, Src Port: upsd (3310), Dst Port: 41776 (41776), Seq: 241446, Ack: 659, Len: 1380
  Source port: upsd (3310)
  Destination port: 41776 (41776)
  Sequence number: 241446    (relative sequence number)
  [Next sequence number: 242826    (relative sequence number)]
  Acknowledgement number: 659    (relative ack number)
  Header length: 20 bytes
⊞ Flags: 0x10 (ACK)
```

232846
− 233342
8504

```
⊟ Internet Protocol, Src: [redacted]
  Version: 4
  Header length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 3420
  Identification: 0x80a0f (32930)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 125
  Protocol: TCP (0x06)
⊞ Header checksum: 0x0e10 [correct]
  Source: [redacted]
  Destination: [redacted]
⊟ Transmission Control Protocol, Src Port: upsd (3310), Dst Port: 41776 (41776), Seq: 233302, Ack: 659, Len: 1380
  Source port: upsd (3310)
  Destination port: 41776 (41776)
```

```
⊟ Internet Protocol, Src: [redacted]
  Version: 4
  Header length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 1420
  Identification: 0x80a4 (32932)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 125
  Protocol: TCP (0x06)
⊞ Header checksum: 0x0e01 [correct]
  Source: [redacted]
  Destination: [redacted]
⊟ Transmission Control Protocol, Src Port: upsd (3310), Dst Port: 41776 (41776), Seq: 241446, Ack: 659, Len: 1380
  Source port: upsd (3310)
  Destination port: 41776 (41776)
```

5 Missing Packets

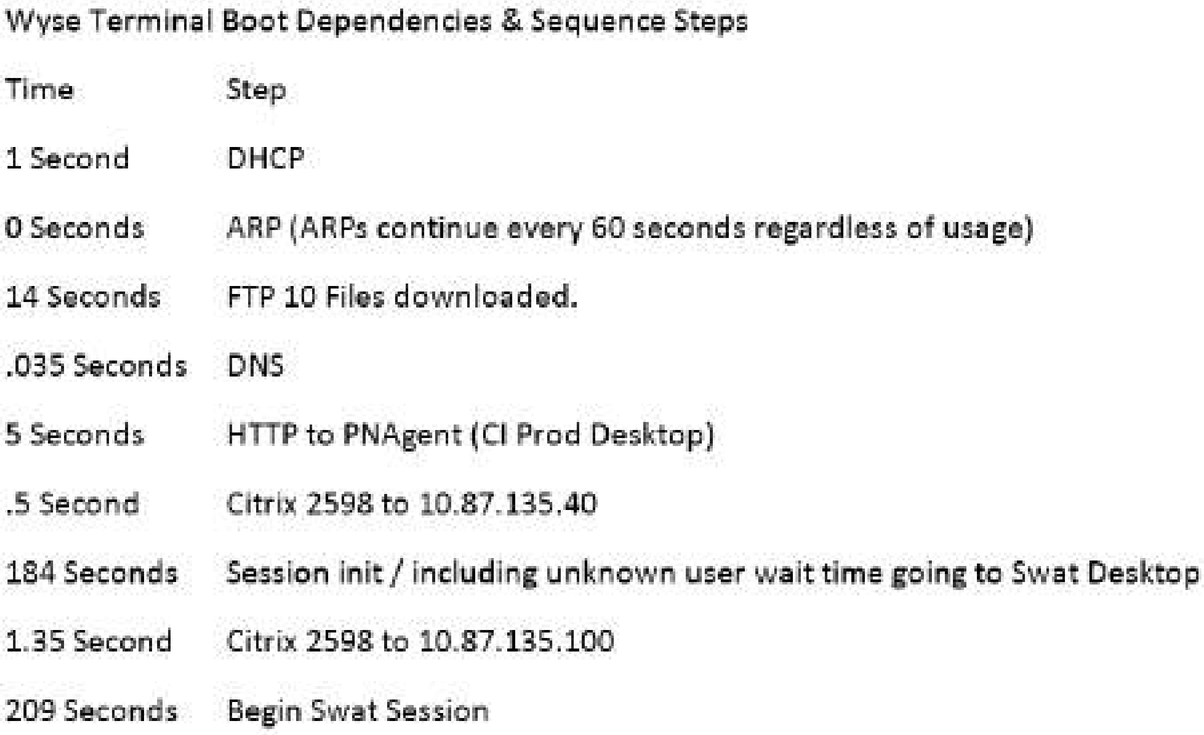
1380 (MSS)
x 5
6900

Citrix Analysis

Technical Lessons Learned Training

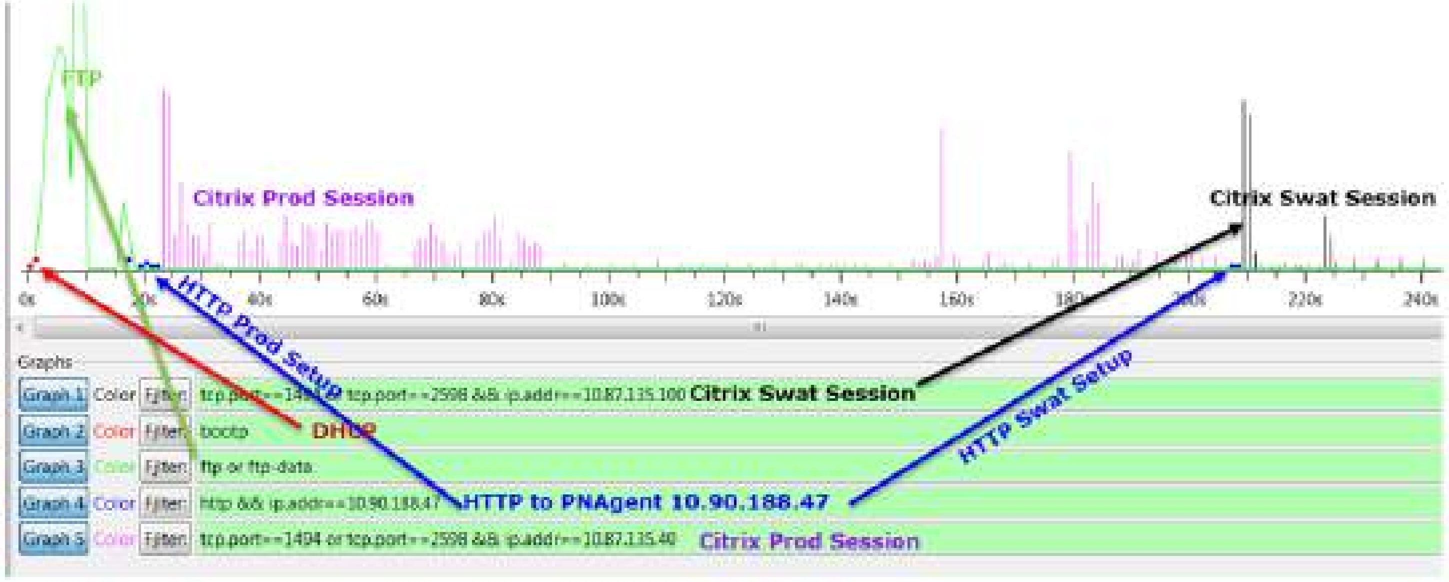
1. How Citrix Wyse Terminals Boot in the Client Environment

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

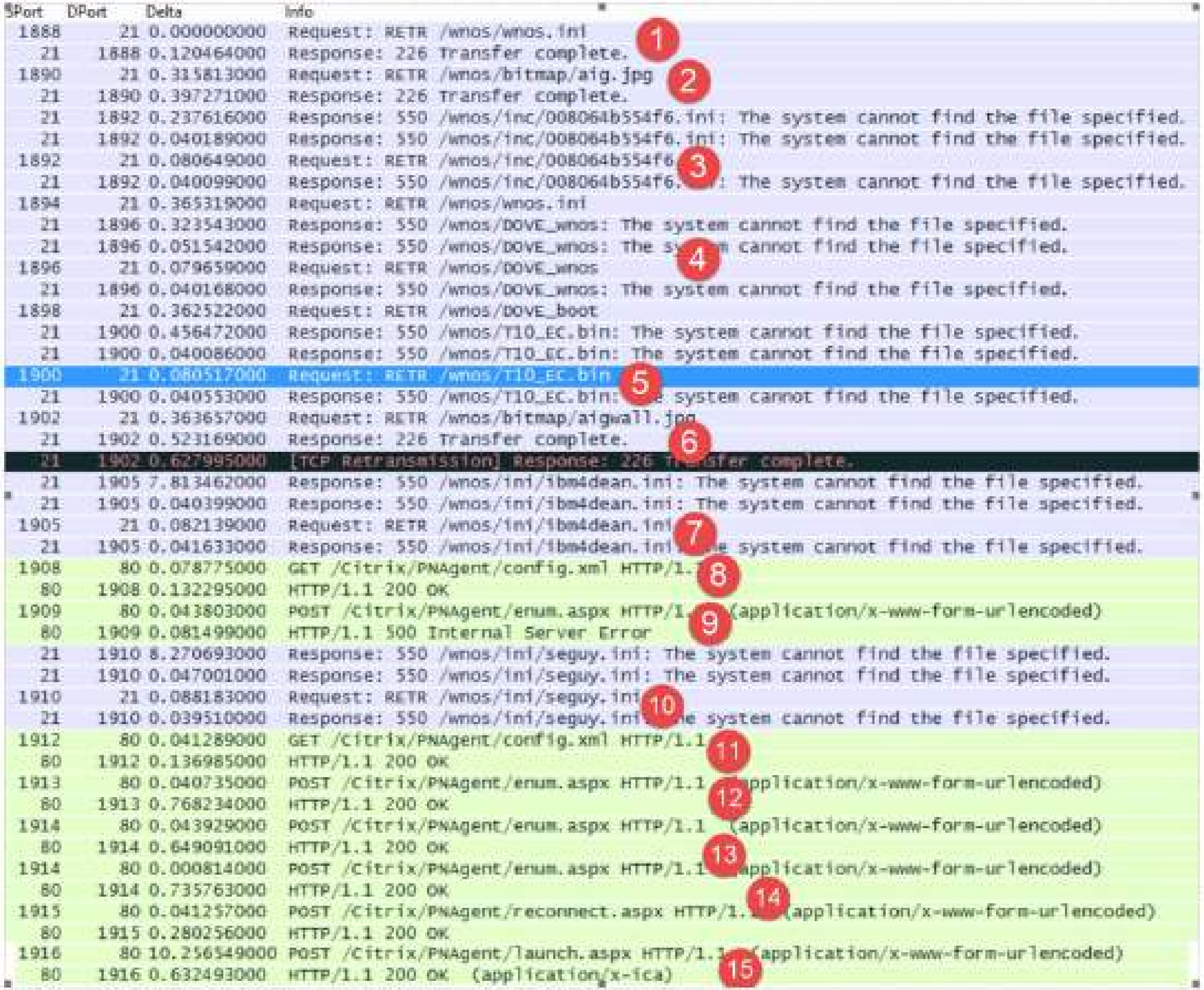


Graph 1	Color	Filter:	tcp.port==1494 or tcp.port==2598 && ip.addr==10.87.135.100 Citrix Swat Session
Graph 2	Color	Filter:	bootp DHCP
Graph 3	Color	Filter:	ftp or ftp-data
Graph 4	Color	Filter:	http && ip.addr==10.90.188.47 HTTP to PNAgent 10.90.188.47
Graph 5	Color	Filter:	tcp.port==1494 or tcp.port==2598 && ip.addr==10.87.135.40 Citrix Prod Session

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.

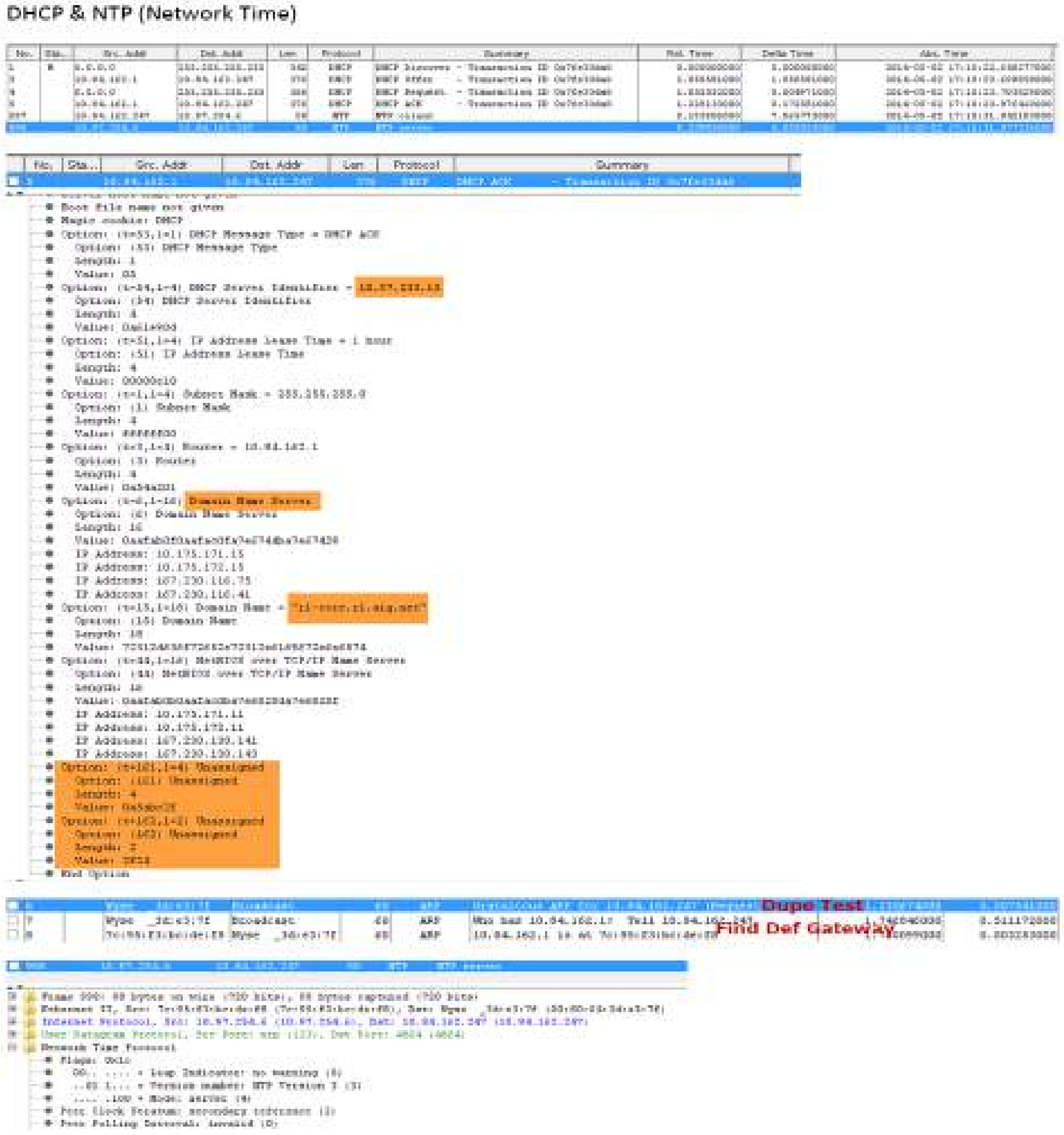
I am going over the boot sequence and the wnos.ini syntax and steps.



```
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 Transfer 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   e 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   e 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   pplication/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	●	0.0.0.0	255.255.255.255	342	DHCP	DHCP Discover - Transaction ID [illegible]	0.000000000	0.000000000	2014-05-02 17:18:22.[illegible]
3		10.84.162.1	10.84.162.247	370	DHCP	DHCP Offer - Transaction ID [illegible]	[illegible]	[illegible]	[illegible]
4		0.0.0.0	255.255.255.255	[illegible]	DHCP	DHCP Request - Transaction ID [illegible]	[illegible]	[illegible]	[illegible]
5		10.84.162.1	10.84.162.247	370	DHCP	DHCP ACK - Transaction ID [illegible]	[illegible]	[illegible]	[illegible]
997		10.84.162.247	10.97.254.6	90	NTP	NTP client	[illegible]	[illegible]	[illegible]
998		10.97.254.6	10.84.162.247	90	NTP	NTP server	[illegible]	[illegible]	[illegible]

No.	Sta...	Src. Addr	Dst. Addr	Len	Protocol	Summary
5		10.84.162.1	10.84.162.247	370	DHCP	DHCP ACK - Transaction ID [illegible]

```
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 = [illegible]
  Option: (54) DHCP Server Identifier
  Length: 4
  Value: [illegible]
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: [illegible]
  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 = "[illegible]"
  Option: (15) Domain Name
  Length: 18
  Value: [illegible]
Option: (t=44,l=16) NetBIOS over TCP/IP Name Server
  Option: (44) NetBIOS over TCP/IP Name Server
  Length: 16
  Value: [illegible]
  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: [illegible]
Option: (t=162,l=2) Unassigned
  Option: (162) Unassigned
  Length: 2
  Value: [illegible]
End Option
```

No.	Src. Addr	Dst. Addr	Len	Protocol	Summary	Delta Time	
6	Wyse_3d:e5:7f	Broadcast	60	ARP	Gratuitous ARP for 10.84.162.247 (Request)	[illegible]	[illegible]
7	Wyse_3d:e5:7f	Broadcast	60	ARP	Who has 10.84.162.1? Tell 10.84.162.247	[illegible]	0.511172000
8	[illegible]	Wyse_3d:e5:7f	60	ARP	10.84.162.1 is at [illegible]	[illegible]	[illegible]

Dupe Test

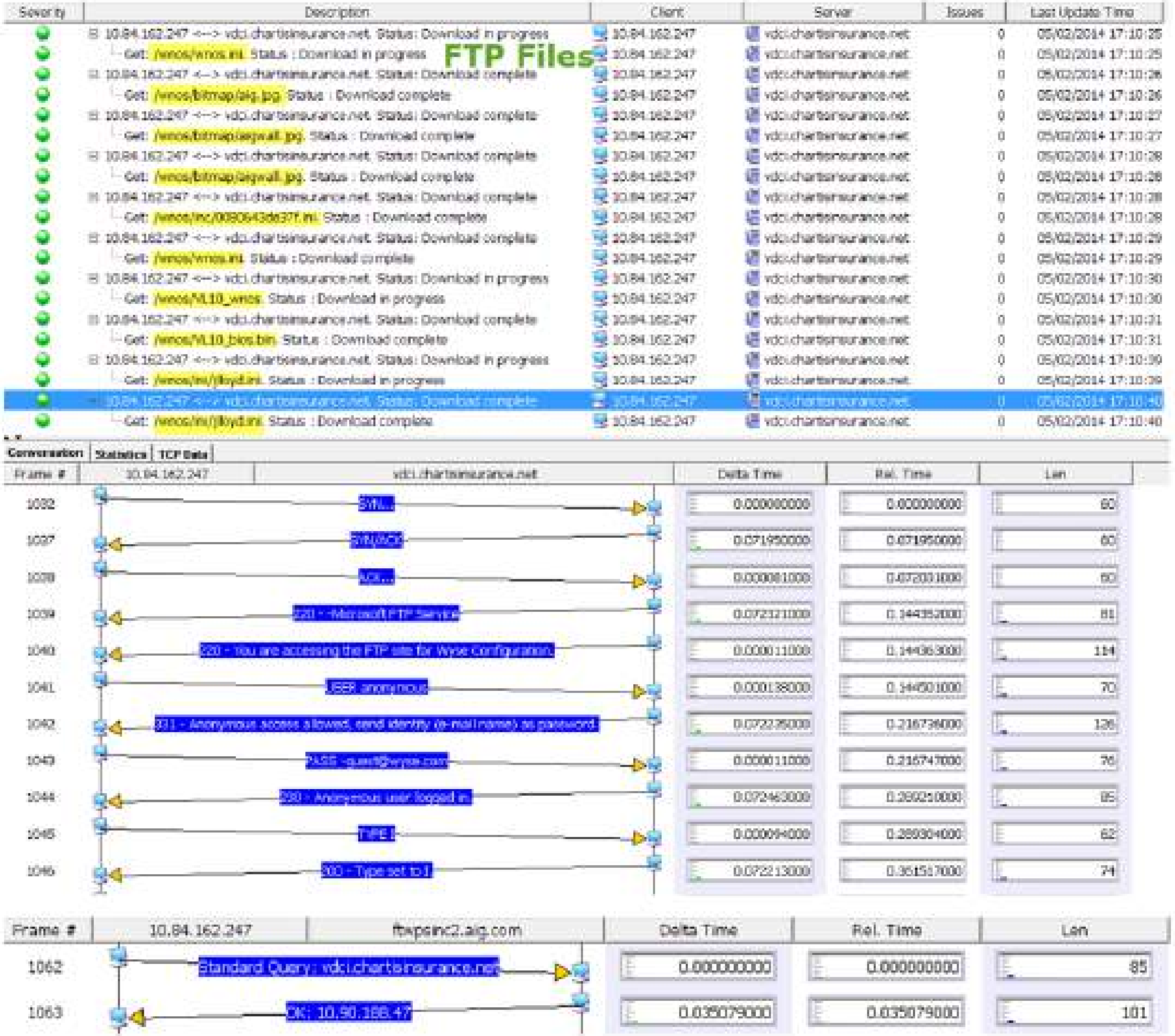
Find Def Gateway

No.	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: [illegible], Dst: Wyse_3d:e5:7f [illegible]
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: 4604 (4604)
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/0080643d637f.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

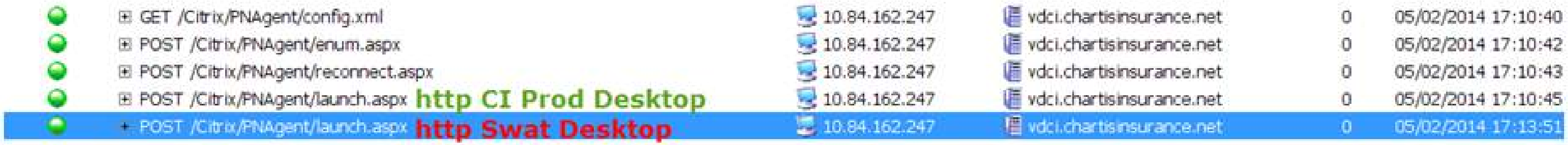
Conversation | Statistics | TCP Data

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

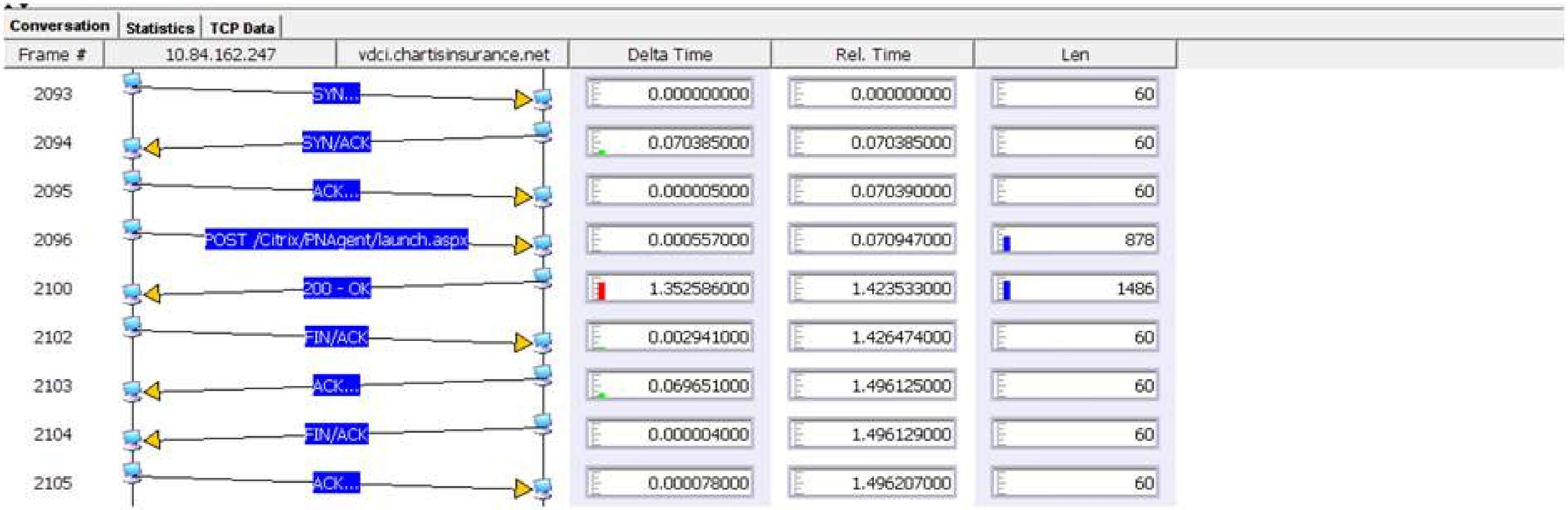
Frame #	10.84.162.247	ftwpsinc2.aig.com	Delta Time	Rel. Time	Len
1062	Standard Query: vdci.chartisinsurance.net →		0.000000000	0.000000000	85
1063	← OK: 10.90.188.47		0.035079000	0.035079000	101

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

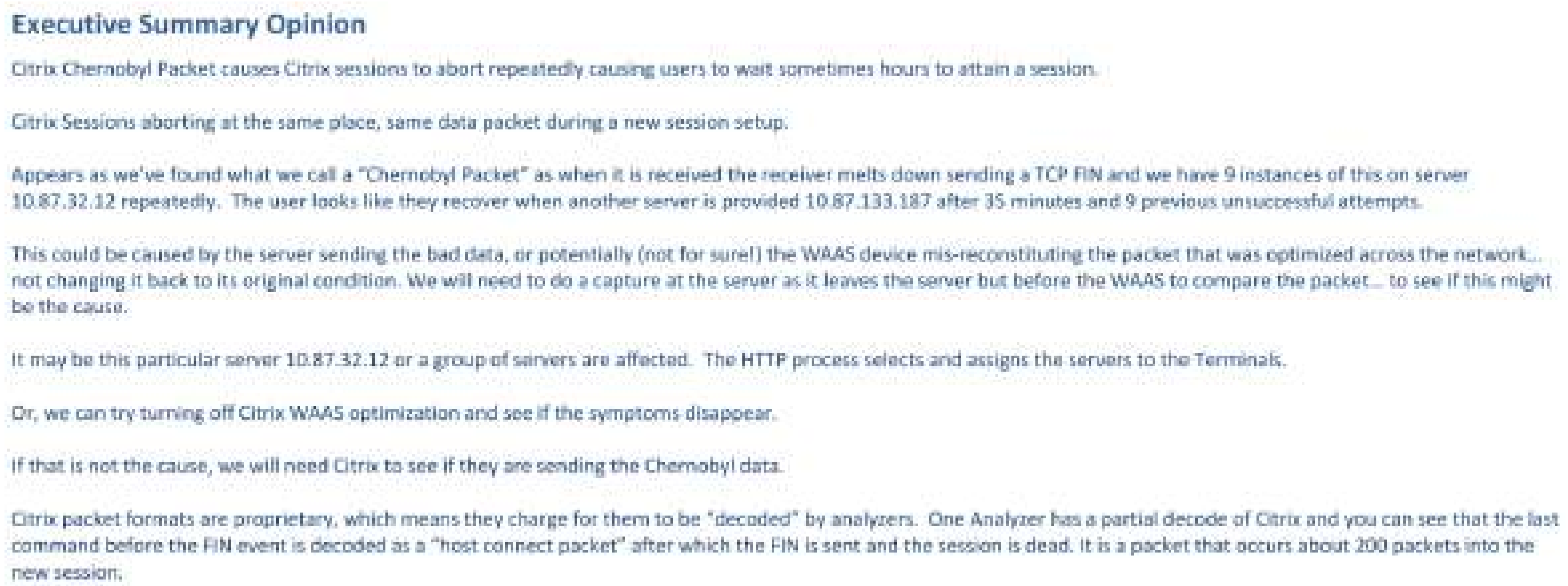


Frame #	10.84.162.247	vdci.chartisinsurance.net	Delta Time	Rel. Time	Len
2093	SYN...	▷	0.000000000	0.000000000	60
2094	◁	SYN/ACK	0.070385000	0.070385000	60
2095	ACK...	▷	0.000005000	0.070390000	60
2096	POST /Citrix/PNAgent/launch.aspx	▷	0.000557000	0.070947000	878
2100	◁	200 - OK	1.352586000	1.423533000	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.

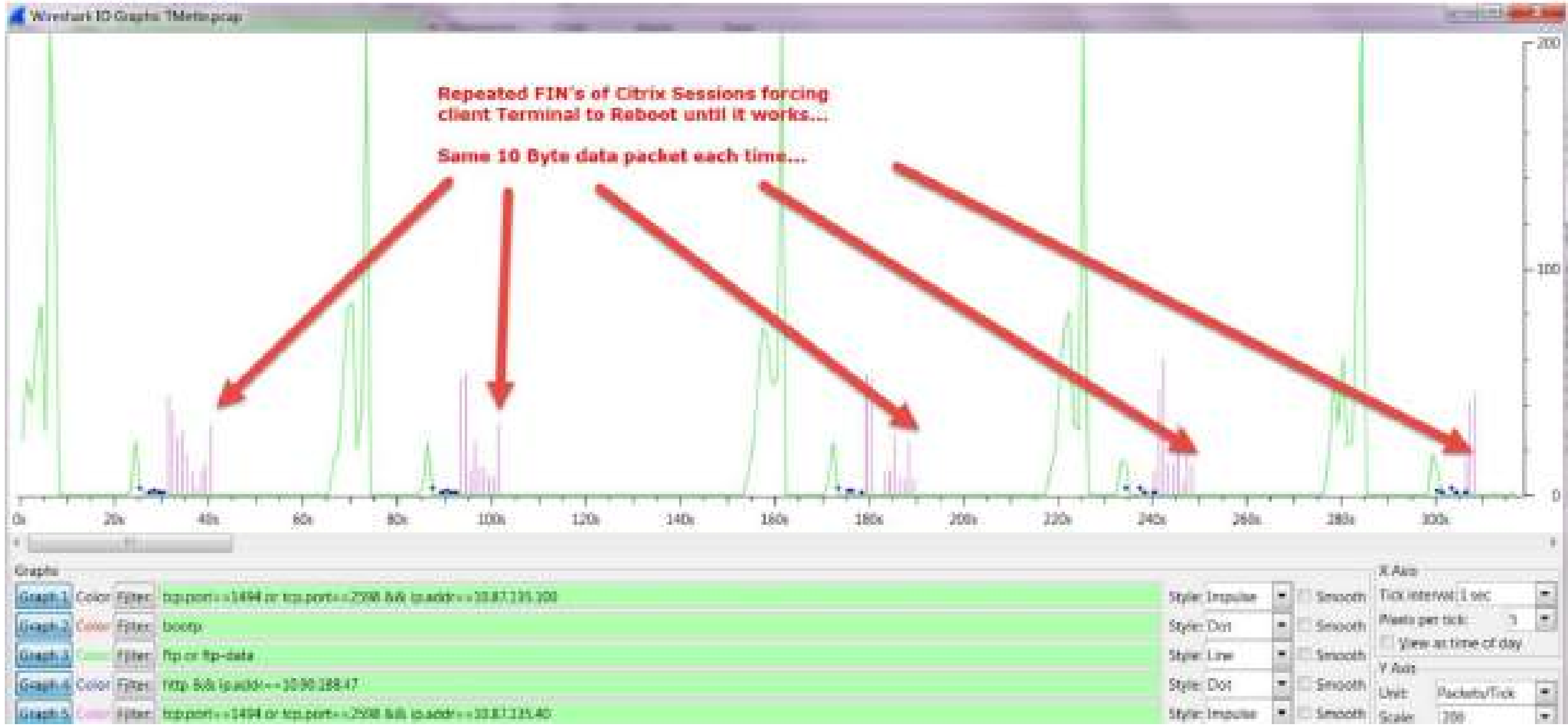
This could be caused by the server sending the bad data, or potentially (not for sure!) the WAAS device mis-reconstituting the packet that was optimized across the network... not changing it back to its original condition. We will need to do a capture at the server as it leaves the server but before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

X Axis

Tick interval: 1 sec

Pixels per tick: 5

□ View as time of day

Y Axis

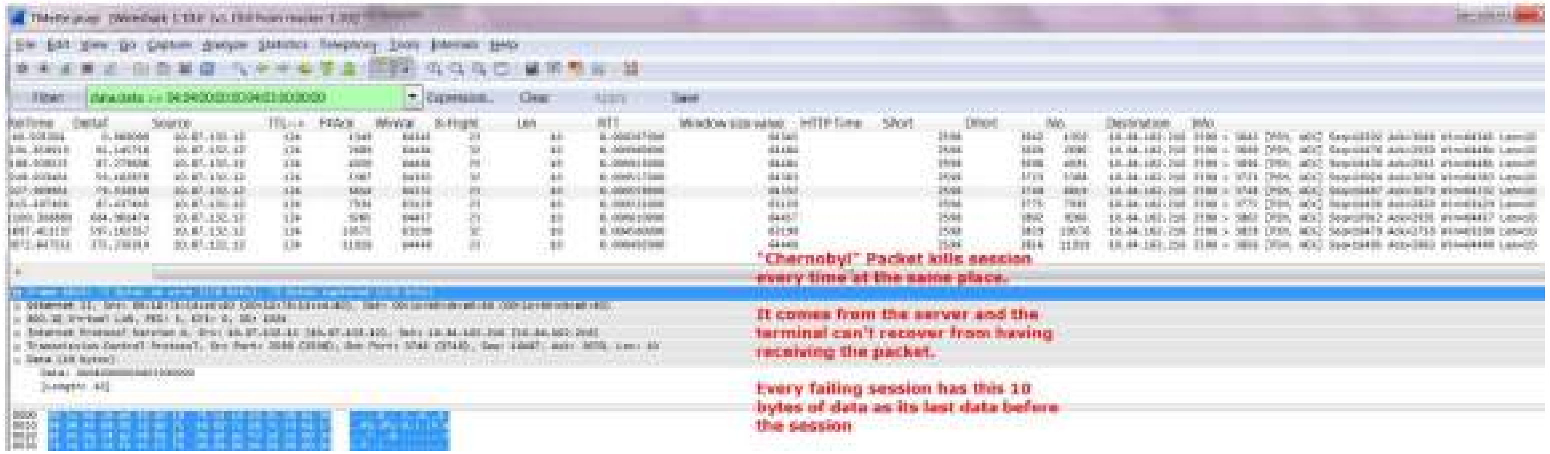
Unit: Packets/Tick

Scale: 200

2. Citrix Session Abort Signature “Chernobyl Packet”

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

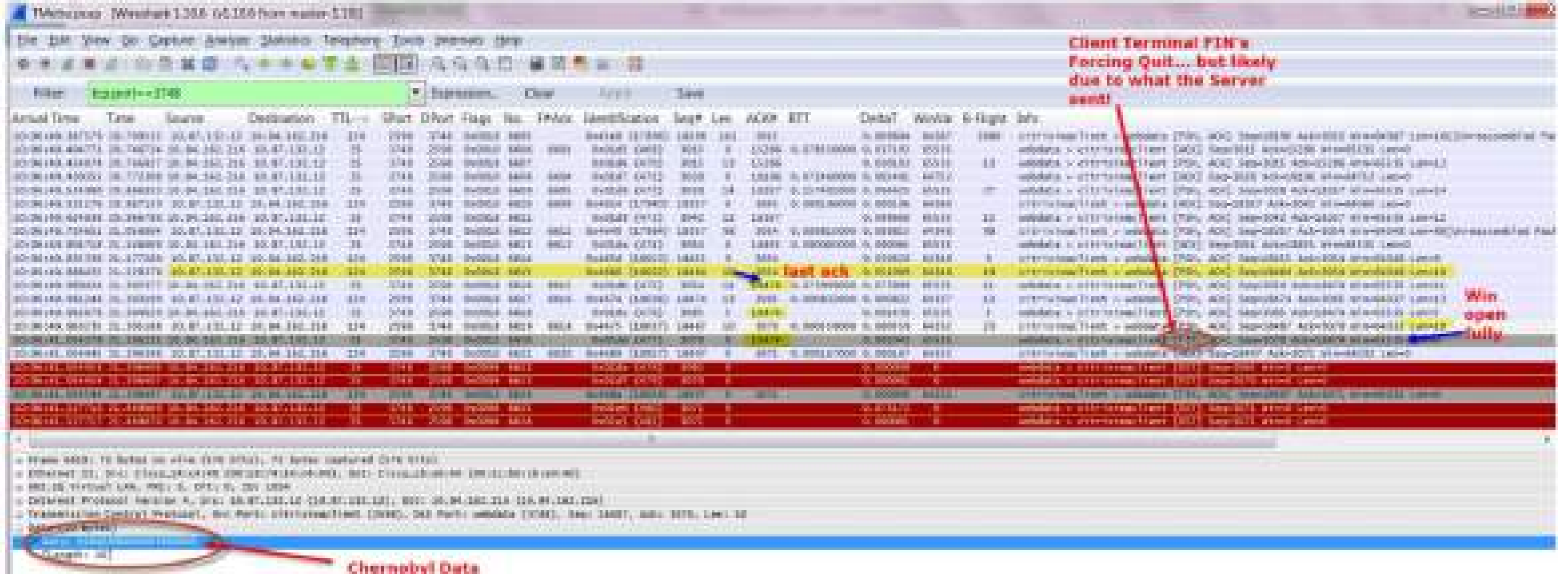
This allowed rapid remediation until a solution could be found to fix the problem.



“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



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

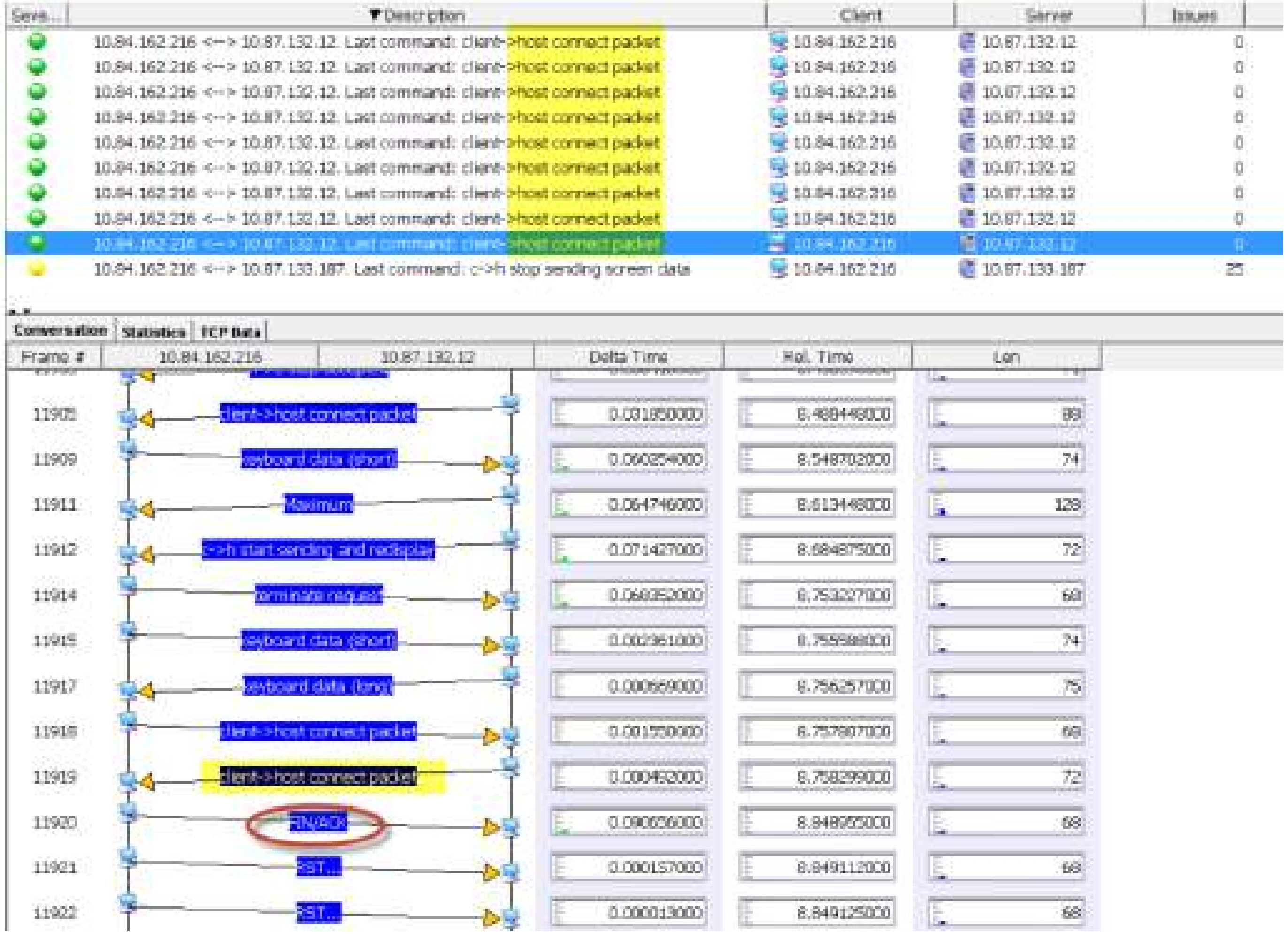
last ack

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.

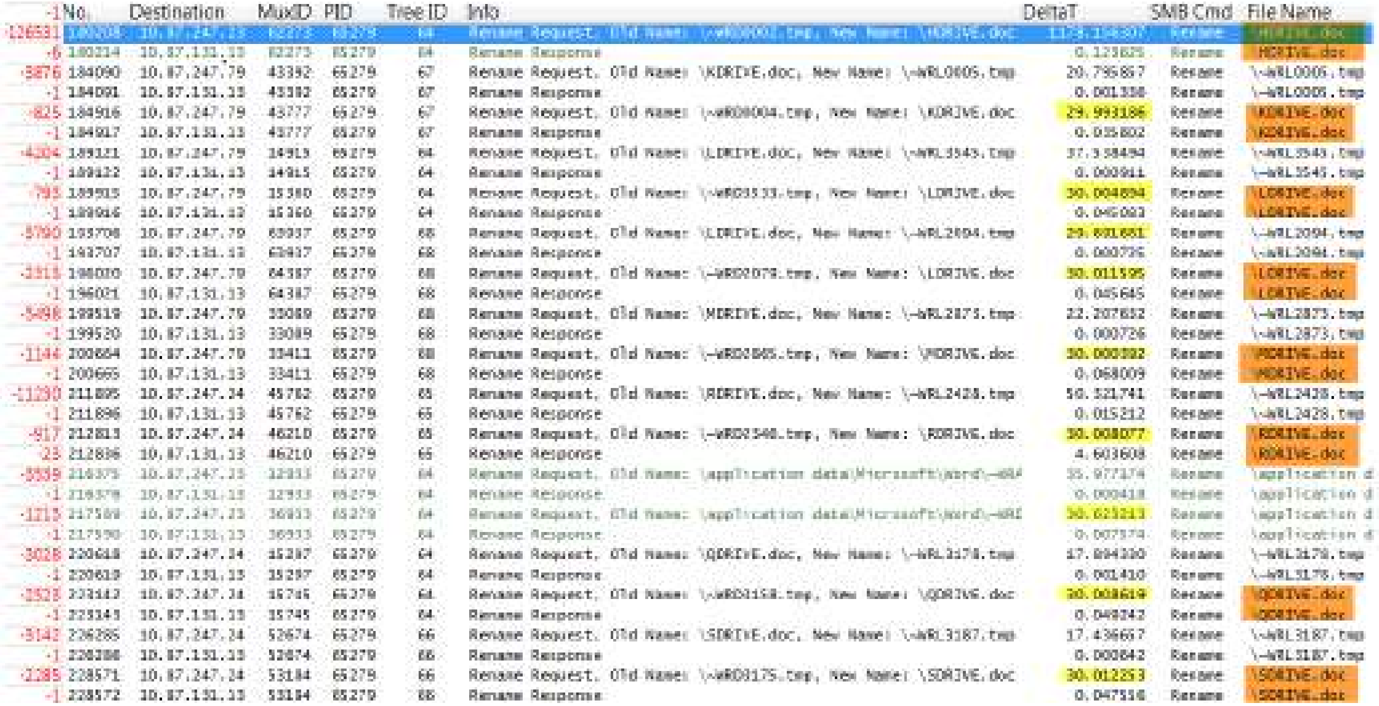
The test showed that regardless of the Network share accessed, it took 30 seconds to open and start to read a file, or save a file.

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.



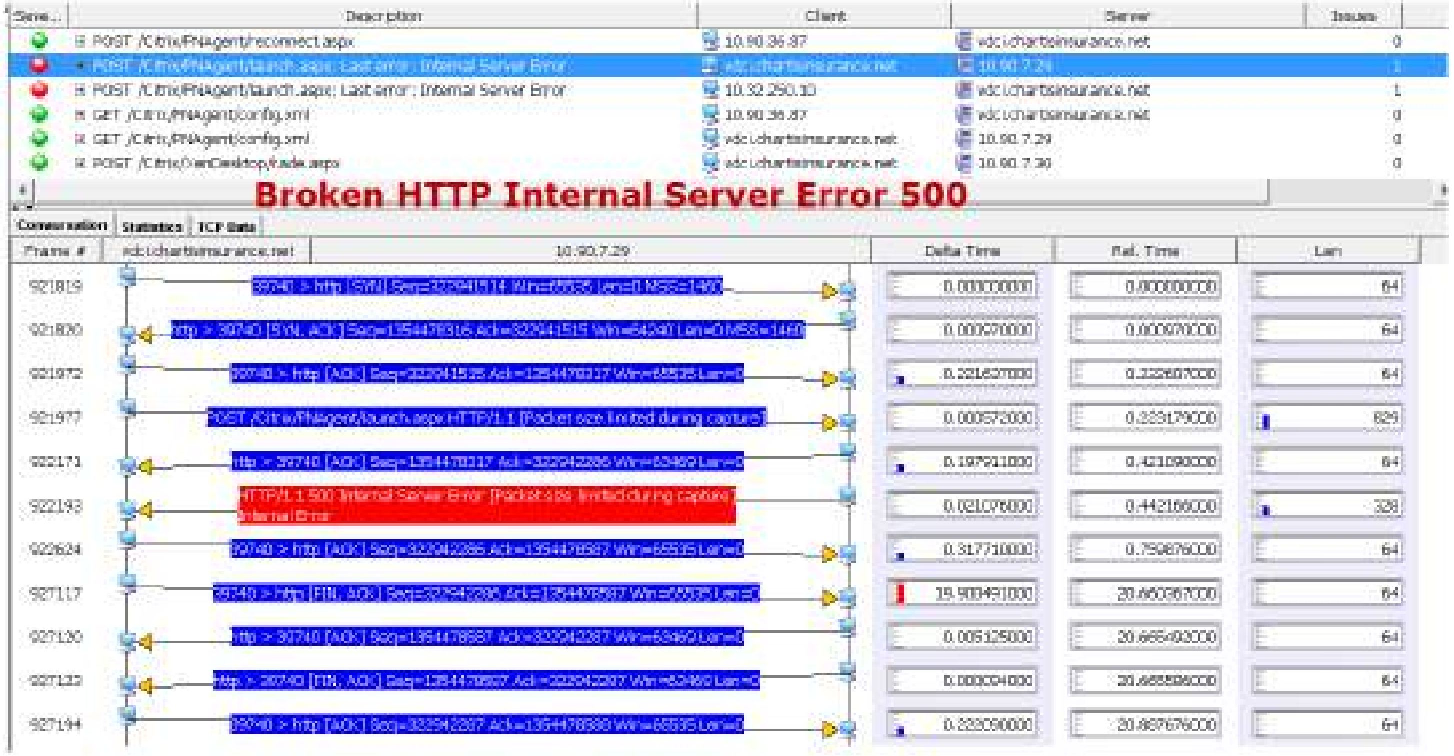
-1	No.	Destination	MuxID	PID	Tree ID	Info	DeltaT	SMB Cmd	File Name
-126531	180208	10.87.247.13	62273	65279	64	Rename Request, Old Name: \~WRD0001.tmp, New Name: \HDRIVE.doc	1179.154307	Rename	\HDRIVE.doc
-6	180214	10.87.131.13	62273	65279	64	Rename Response	0.123625	Rename	\HDRIVE.doc
-3876	184090	10.87.247.79	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	0.001338	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	34913	65279	64	Rename Request, Old Name: \LDRIVE.doc, New Name: \~WRL3545.tmp	37.358494	Rename	\~WRL3545.tmp
-1	189122	10.87.131.13	34913	65279	64	Rename Response	0.000911	Rename	\~WRL3545.tmp
-793	189915	10.87.247.79	35360	65279	64	Rename Request, Old Name: \~WRD3533.tmp, New Name: \LDRIVE.doc	30.004894	Rename	\LDRIVE.doc
-1	189916	10.87.131.13	35360	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	29.801681	Rename	\~WRL2094.tmp
-1	193707	10.87.131.13	63937	65279	68	Rename Response	0.000736	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	22.207652	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	50.521741	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: \~WRD2340.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	32933	65279	64	Rename Request, Old Name: \application data\Microsoft\Word\~WRA	35.977174	Rename	\application d
-1	216376	10.87.131.13	32933	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	30.023213	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	15287	65279	64	Rename Request, Old Name: \QDRIVE.doc, New Name: \~WRL3178.tmp	17.894330	Rename	\~WRL3178.tmp
-1	220619	10.87.131.13	15287	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	0.000842	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	0.047516	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.

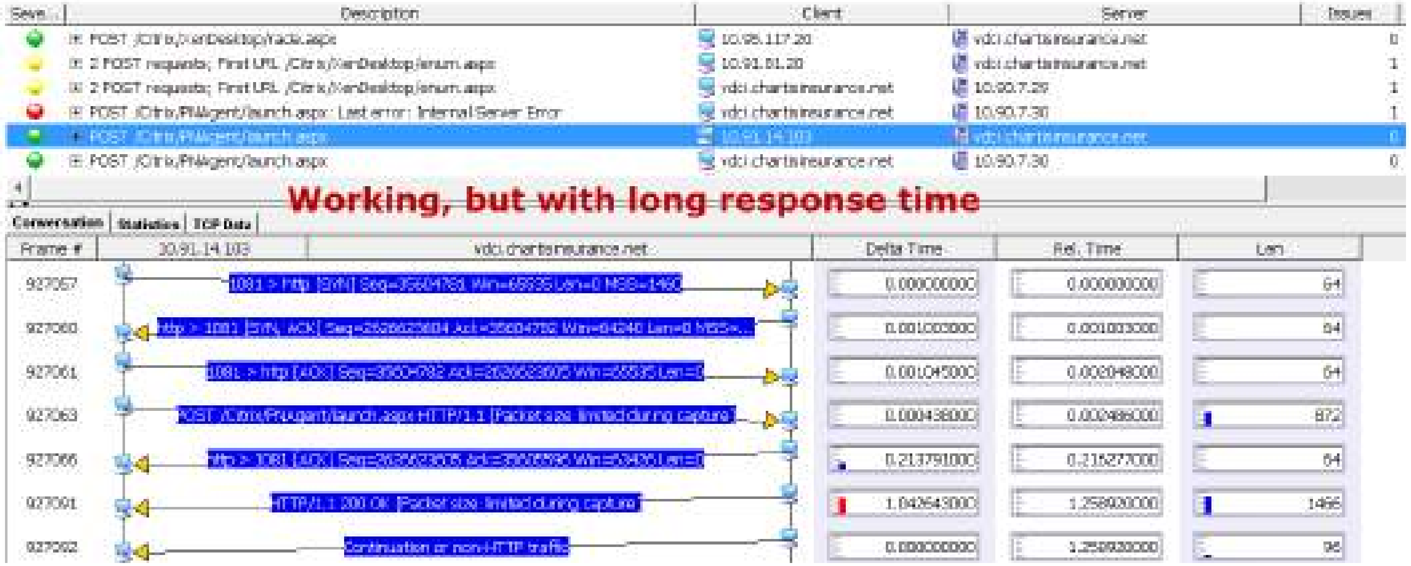
This causes the user to hang and have to reboot the Wyse terminal repeatedly until an attempt is successful.



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	629
922171	http > 39740 [ACK] Seq=1354478317 Ack=322942086 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=322942086 Ack=1354478587 Win=65535 Len=0		0.317710000	0.759876000	64
927117	39740 > http [FIN, ACK] Seq=322942086 Ack=1354478587 Win=65535 Len=0		19.900491000	20.660367000	64
927120	http > 39740 [ACK] Seq=1354478587 Ack=322942087 Win=63469 Len=0		0.005125000	20.665492000	64
927122	http > 39740 [FIN, ACK] Seq=1354478587 Ack=322942087 Win=63469 Len=0		0.000094000	20.665586000	64
927194	39740 > http [ACK] Seq=322942087 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

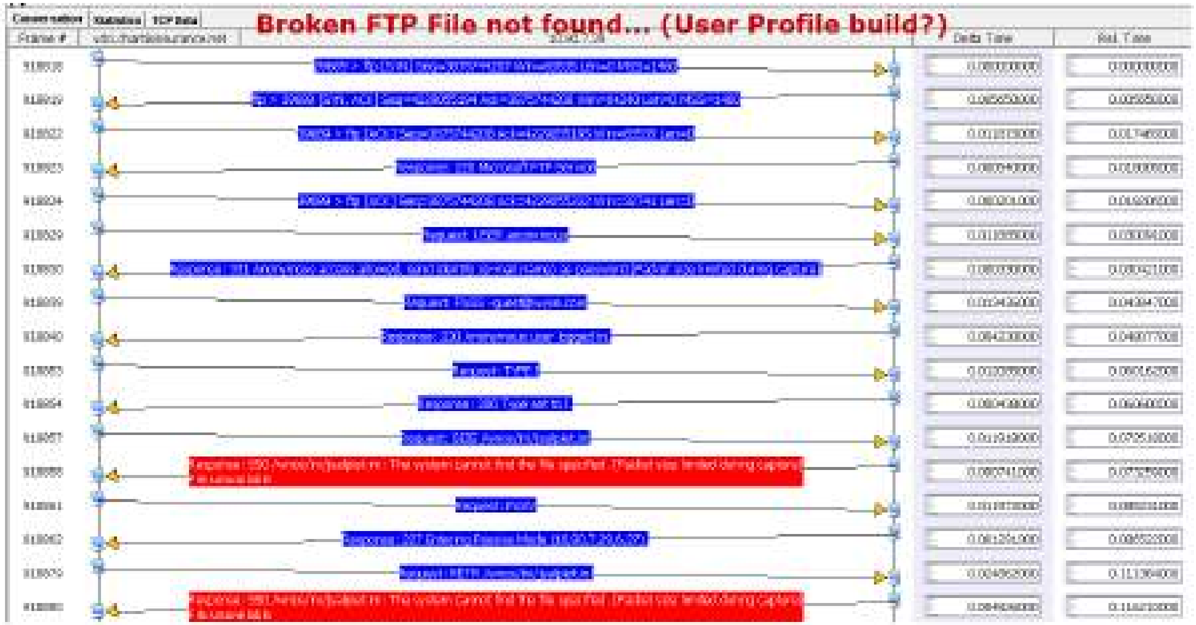
Frame #	10.91.14.103	vdci.chartisinsurance.net	Delta Time	Rel. Time	Len
927057	1081 > http [SYN] Seq=35604781 Win=65535 Len=0 MSS=1460		0.000000000	0.000000000	64
927060	http > 1081 [SYN, ACK] Seq=2626623604 Ack=35604782 Win=64240 Len=0 MSS=...		0.001003000	0.001003000	64
927061	1081 > http [ACK] Seq=35604782 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=63406 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.

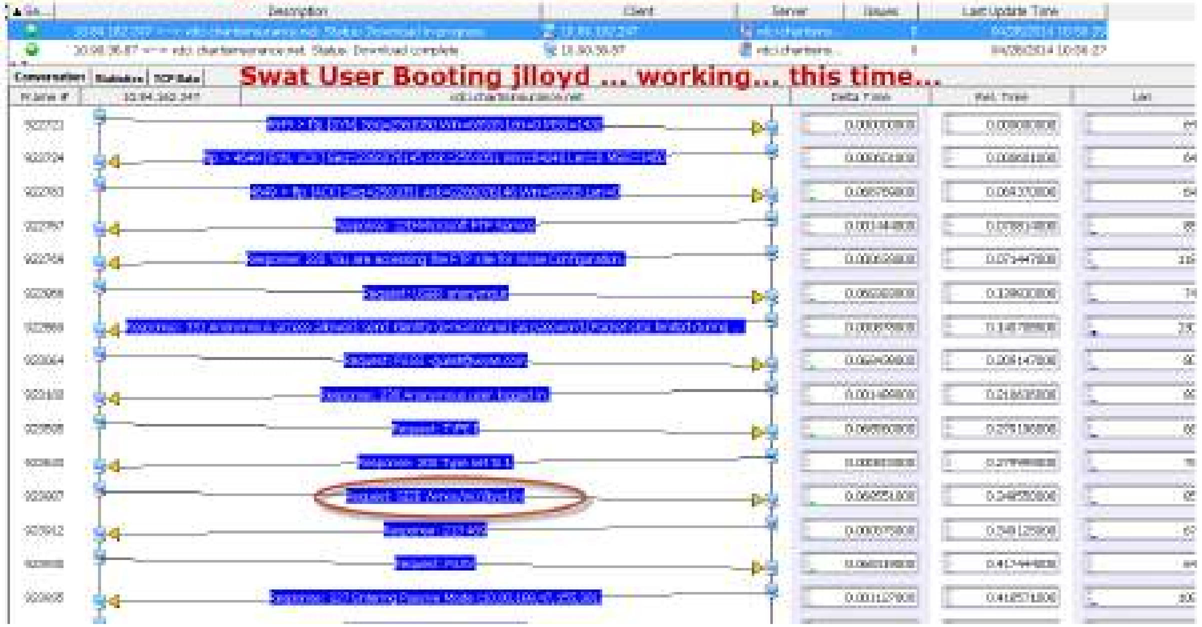
The servers were found to have multiple problems contributing to users having lengthy periods of login difficulty sometimes for several hours.

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



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

FTP Working for one of our Swat Users...



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

WAAS Analysis of Citrix

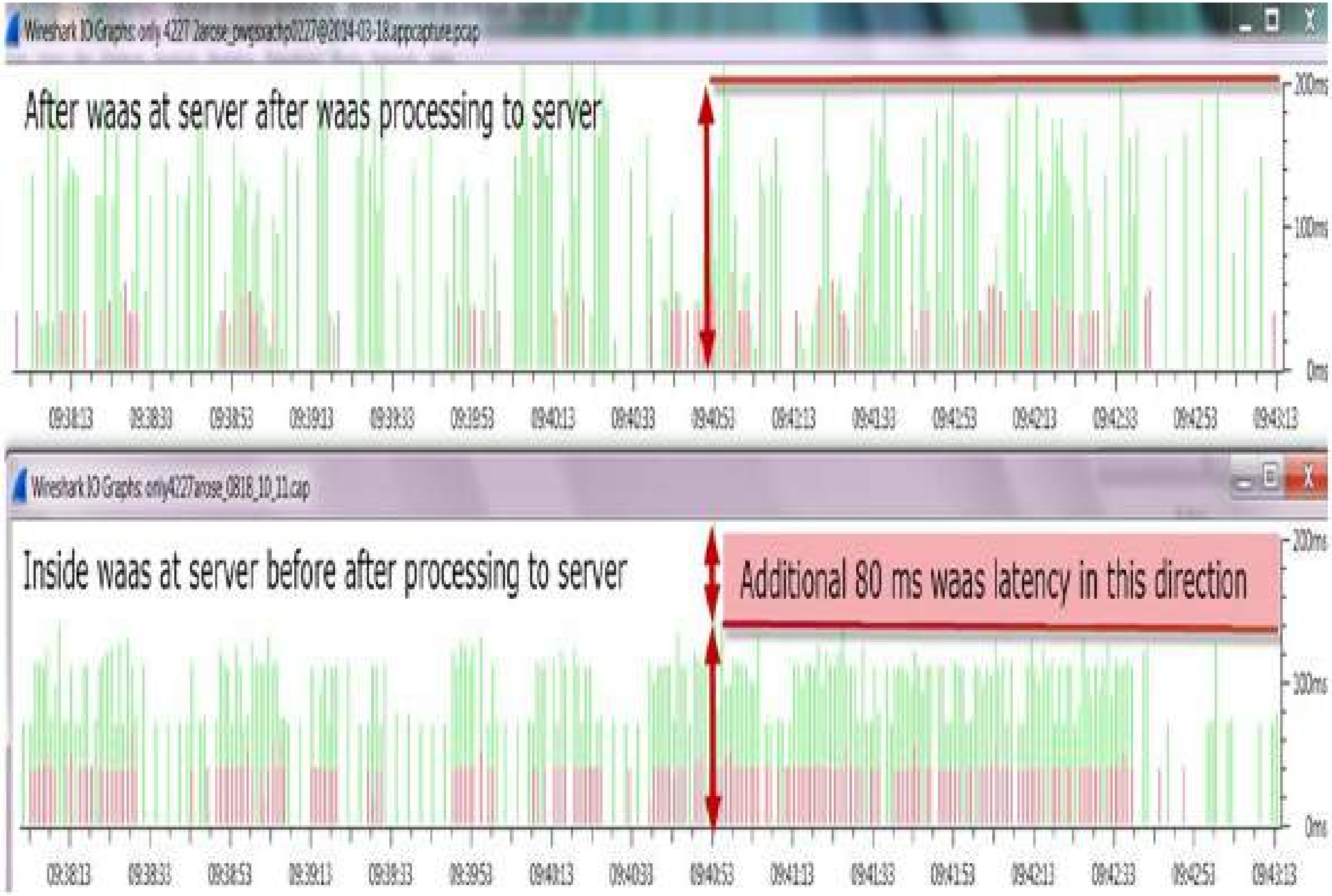
This was a quick analysis of the effectiveness of the WAAS compression of Citrix traffic.

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.



After waas at server after waas processing to server

Inside waas at server before after processing to server

Additional 80 ms waas latency in this direction

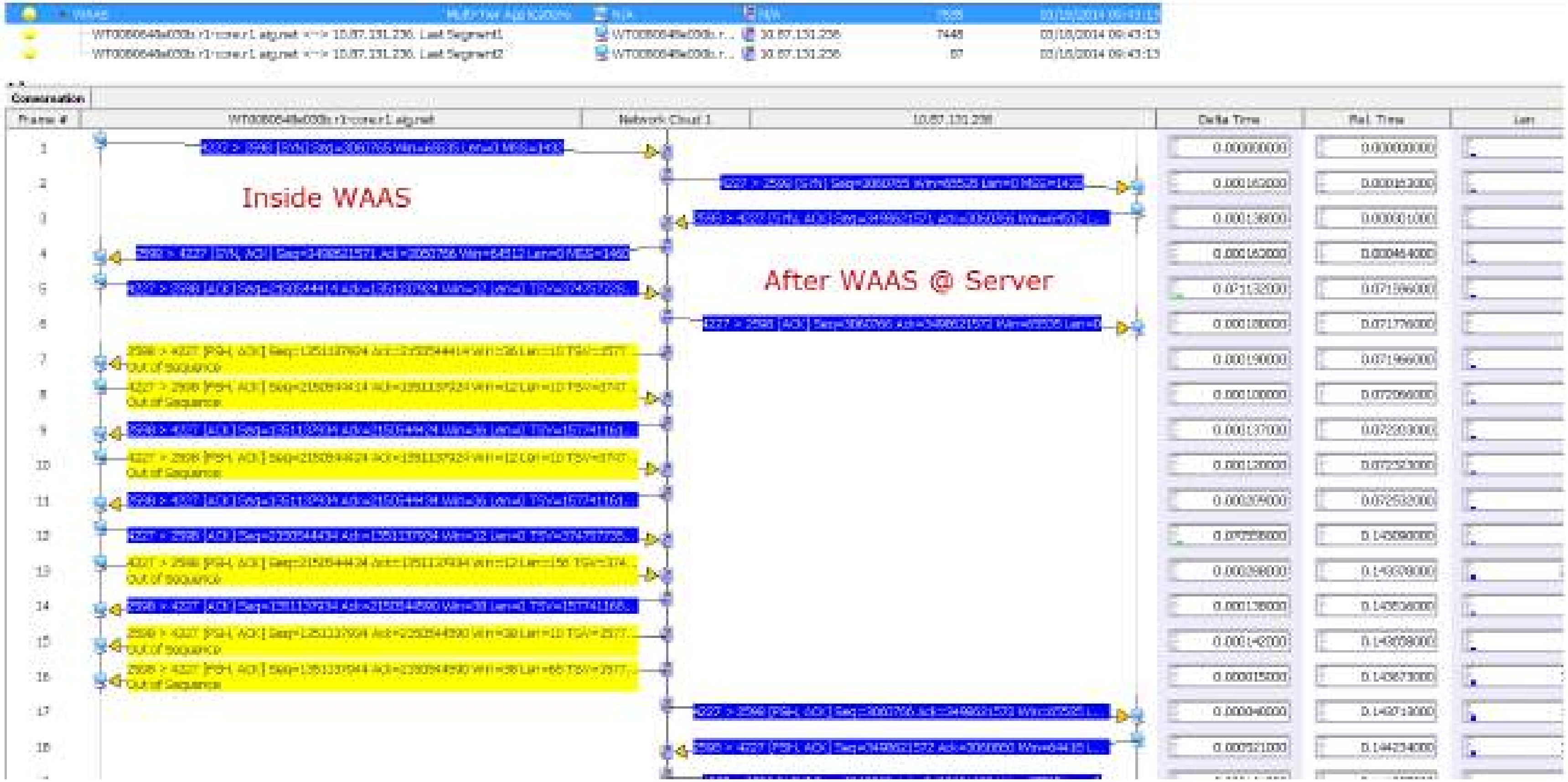
WAAS Analysis of Citrix

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…



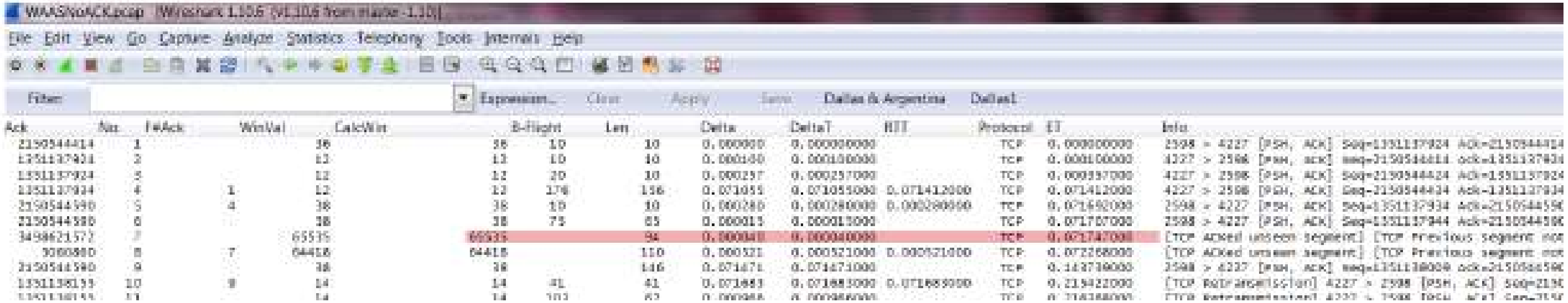
```
WAAS                                                             Multi-Tier Applications   N/A                       N/A              7535   03/18/2014 09:43:13
    WT0080648e030b.r1-core.r1.alg.net <-> 10.87.131.236, Last Segment1   WT0080648e030b.r...   10.87.131.236    7448   03/18/2014 09:43:13
    WT0080648e030b.r1-core.r1.alg.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.alg.net / Network Cloud 1 / 10.87.131.236	Delta Time	Rel. Time	Len
1	4227 > 2598 [SYN] Seq=3060765 Win=65535 Len=0 MSS=1460	0.000000000	0.000000000	
2	4227 > 2598 [SYN] Seq=3060765 Win=65535 Len=0 MSS=1420	0.000162000	0.000162000	
3	2598 > 4227 [SYN, ACK] Seq=3498621571 Ack=3060766 Win=6512...	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=38 Len=10 TSV=2577... 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=38 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=38 Len=0 TSV=157741161...	0.000209000	0.072532000	
12	4227 > 2598 [ACK] Seq=2150544434 Ack=1351137934 Win=12 Len=0 TSV=374757728...	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	
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=2577... Out of Sequence	0.000142000	0.143658000	
16	2598 > 4227 [PSH, ACK] Seq=1351137944 Ack=2150544590 Win=38 Len=65 TSV=2577... 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            38       38      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=2150544590
2150544590   6            38       38      75       65  0.000015  0.000015000               TCP  0.071707000  2598 > 4227 [PSH, ACK] Seq=1351137944 Ack=2150544590
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=2150544590
1351138133  10      8     14       14      41       41  0.071683  0.071683000  0.071683000  TCP  0.215422000  [TCP Retransmission] 4227 > 2598 [PSH, ACK] Seq=215
1351138133  11            14       14     102       62  0.000968  0.000968000               TCP  0.216388000  [TCP Retransmission] 4227 > 2598 [PSH, ACK] Seq=215
```

File Access Problems with Citrix Servers

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

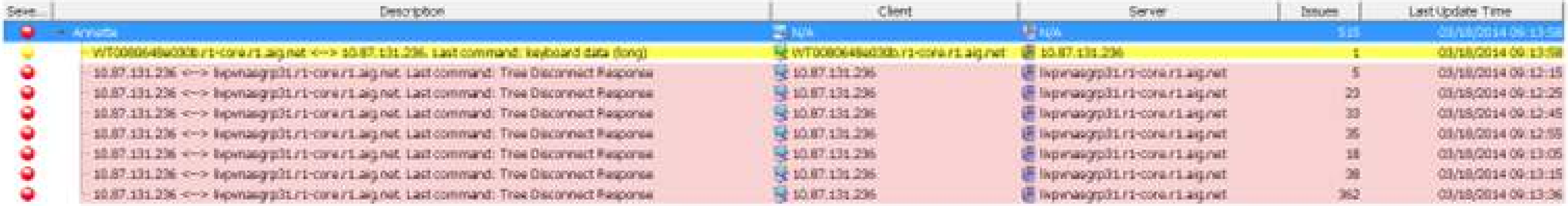
User is accessing Citrix session in yellow, server is trying open connections to Filer repeatedly and gets error messages.

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

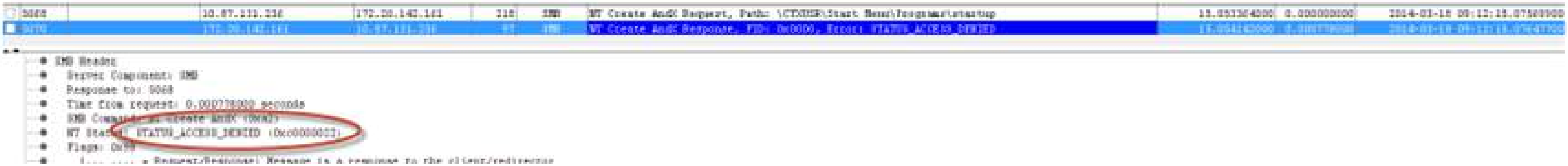
This is one of the reasons I have asked for the architectural design for A[redacted] Citrix user file access path hierarchy. This issue however seems to be inability of the server to open files for Citrix users.

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
●	WT00806484030b.r1-core.r1.aig.net <--> 10.87.131.236. Last command: keyboard data (long)	WT00806484030b.r1-core.r1.aig.net	10.87.131.236	1	03/18/2014 09:13:58
●	10.87.131.236 <--> lwpnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lwpnasgrp31.r1-core.r1.aig.net	5	03/18/2014 09:12:15
●	10.87.131.236 <--> lwpnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lwpnasgrp31.r1-core.r1.aig.net	23	03/18/2014 09:12:25
●	10.87.131.236 <--> lwpnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lwpnasgrp31.r1-core.r1.aig.net	33	03/18/2014 09:12:45
●	10.87.131.236 <--> lwpnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lwpnasgrp31.r1-core.r1.aig.net	35	03/18/2014 09:12:55
●	10.87.131.236 <--> lwpnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lwpnasgrp31.r1-core.r1.aig.net	18	03/18/2014 09:13:05
●	10.87.131.236 <--> lwpnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lwpnasgrp31.r1-core.r1.aig.net	38	03/18/2014 09:13:15
●	10.87.131.236 <--> lwpnasgrp31.r1-core.r1.aig.net. Last command: Tree Disconnect Response	10.87.131.236	lwpnasgrp31.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 09:12:15.07589900
□ 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

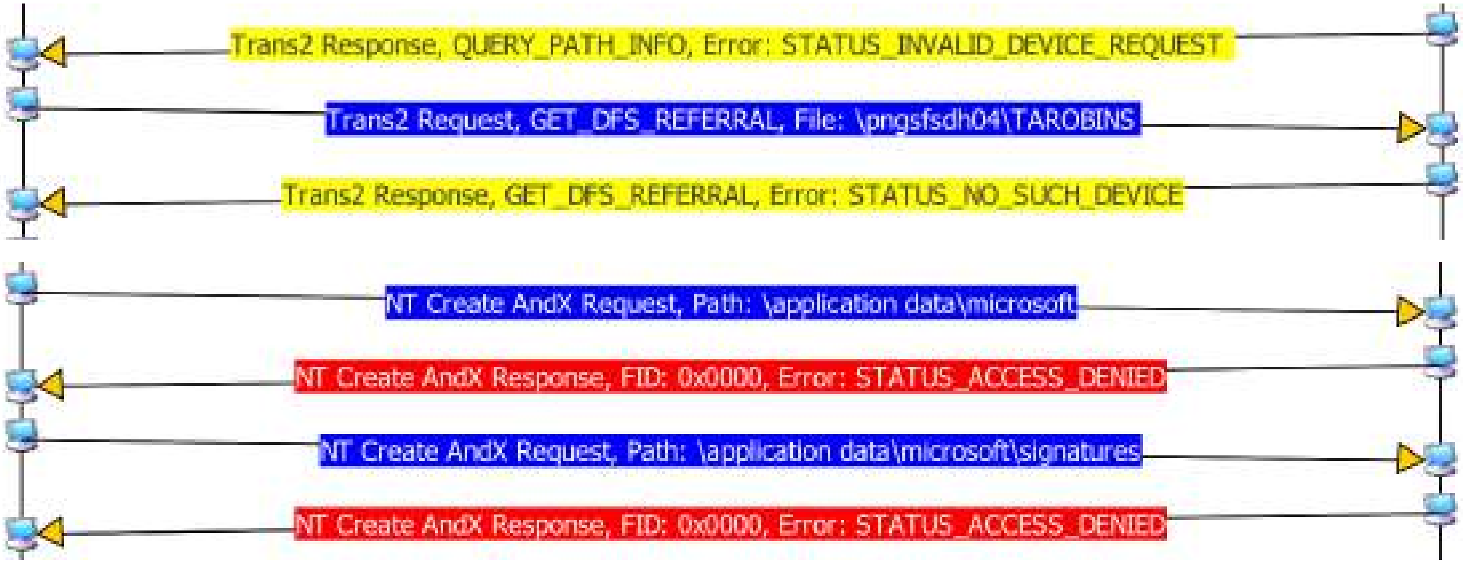
Some files are not found and searched across many drive mappings creating an abundance of frivolous traffic.

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

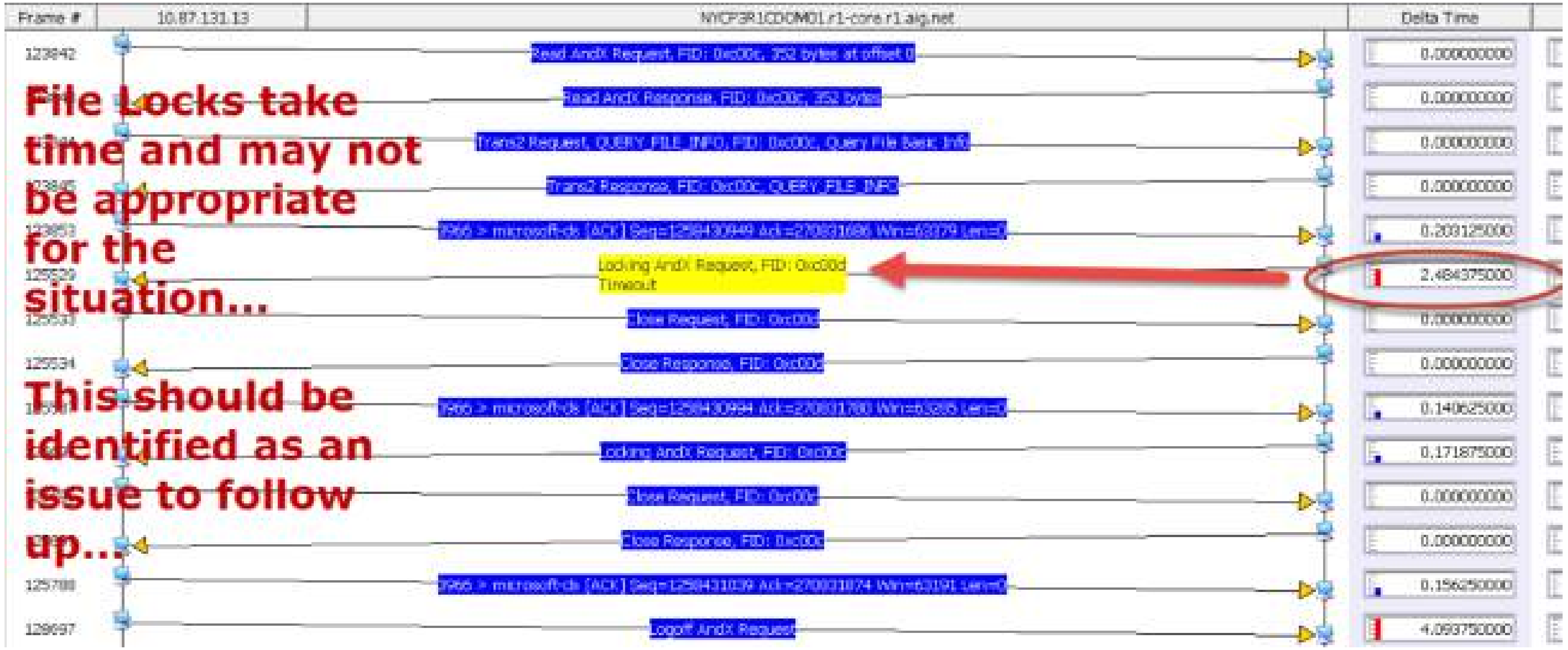
Others are not accessible due to the type of account due to incompatibilities between the Client choice to use AppSense for Microsoft Profile management with NetApp Filers. The complexities have made the installation of AppSense ineffective.

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
          Read AndX Response, FID: 0xc00c, 352 bytes                                            0.000000000
          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
          3966 > microsoft-ds [ACK] Seq=1258430994 Ack=270831780 Win=63285 Len=0                0.140625000
          Locking AndX Request, FID: 0xc00c                                                     0.171875000
          Close Request, FID: 0xc00c                                                            0.000000000
          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
```

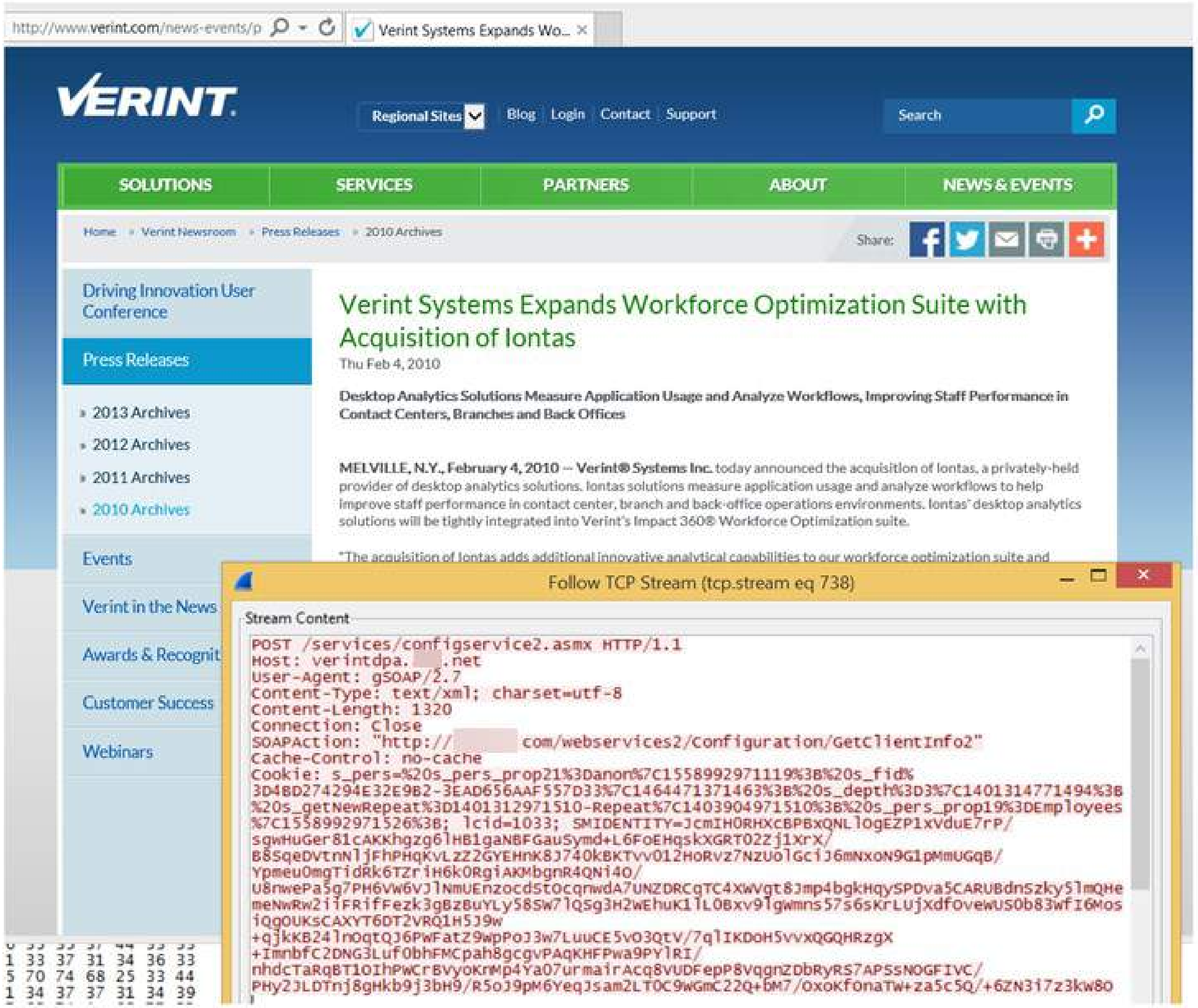
File Locks take time and may not be appropriate for the situation…

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

```
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
```

```
1 33 37 31 34 36 33
5 70 74 68 25 33 44
1 34 37 37 31 34 39
```

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 L 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.

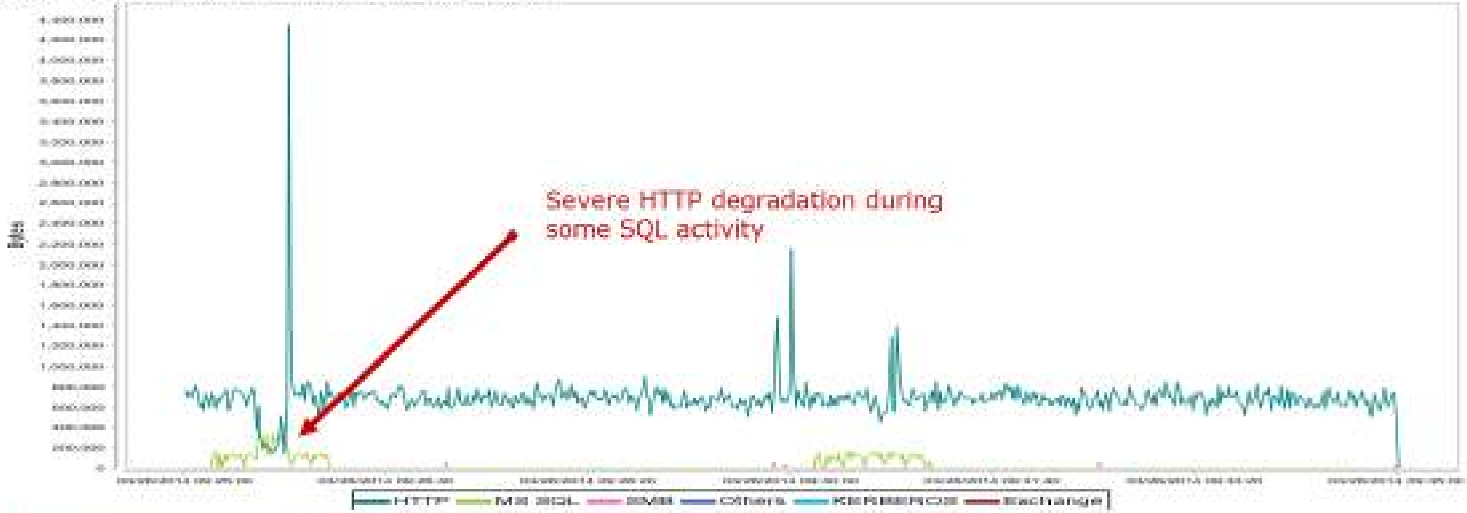
This analysis is done as part of the SWAT initiative to diagnose and mitigate performance issues identified for the SWAT initiative.

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

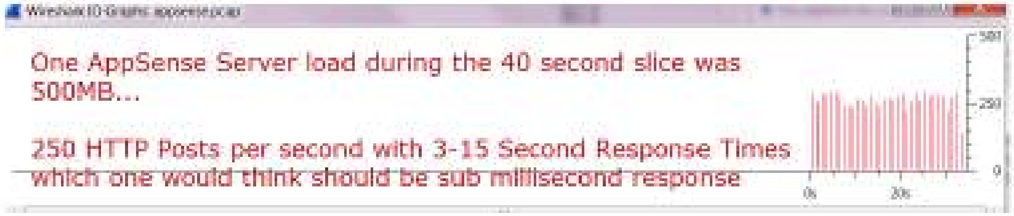
Actions Requested:

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

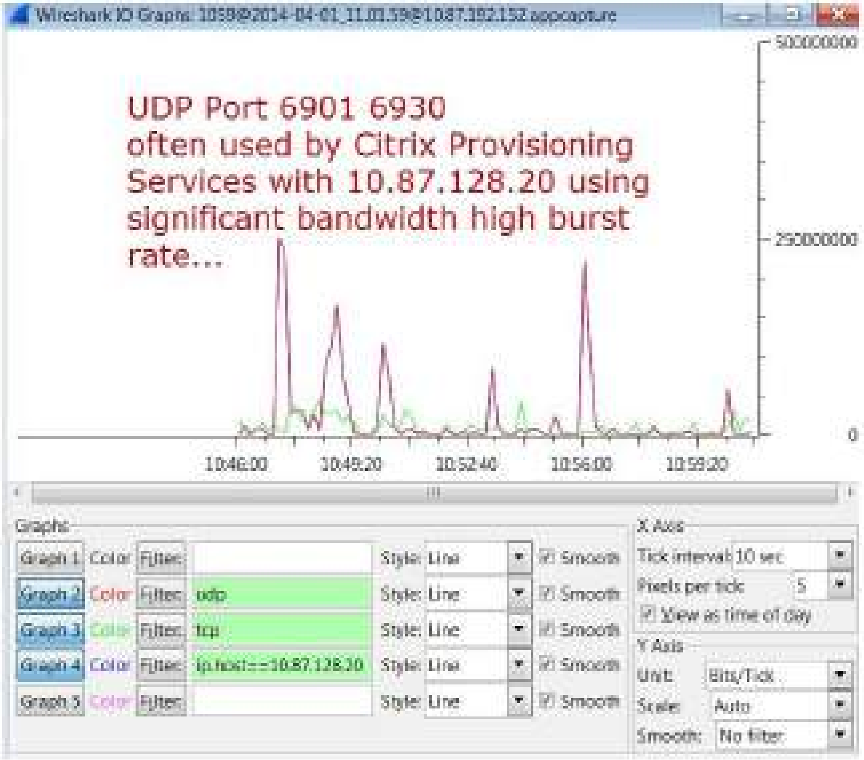


One AppSense Server load during the 40 second slice was 500MB…

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

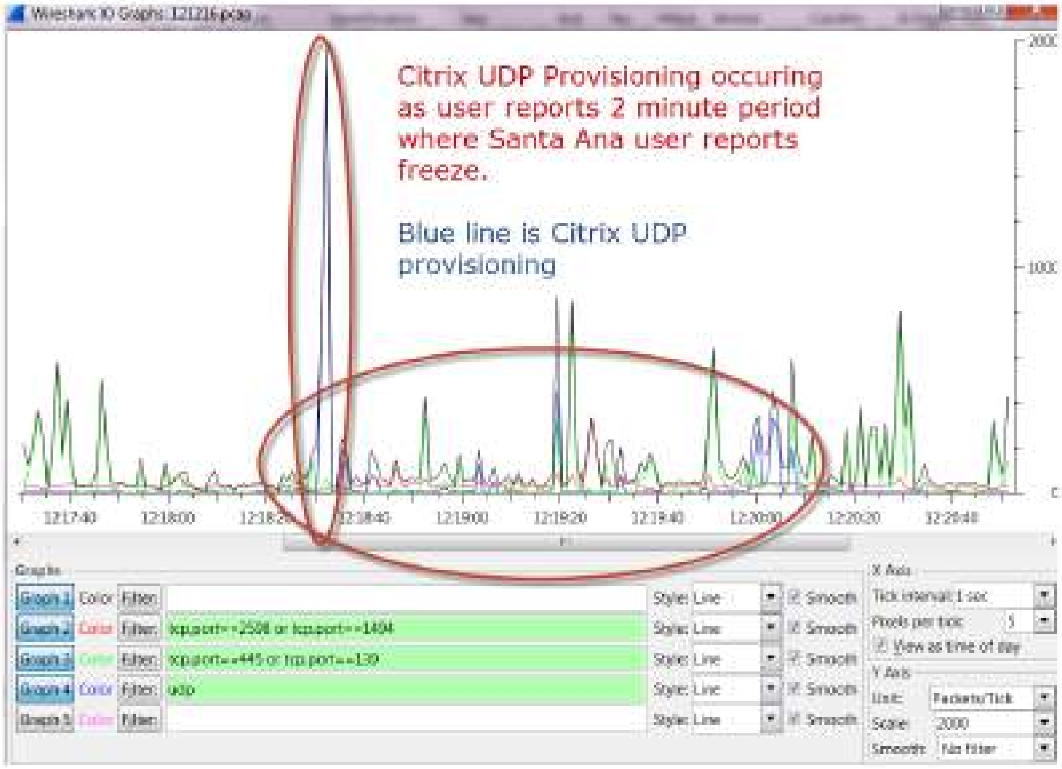
UDP Port 6901 6930 often used by Citrix Provisioning Services with 10.87.128.20 using significant bandwidth high burst rate...

Graphs

- Graph 1 Color Filter: (blank) 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: (blank) 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



Wireshark IO Graphs: 121216.pcap

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: (blank) 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: (blank) Style: Line ☑ Smooth

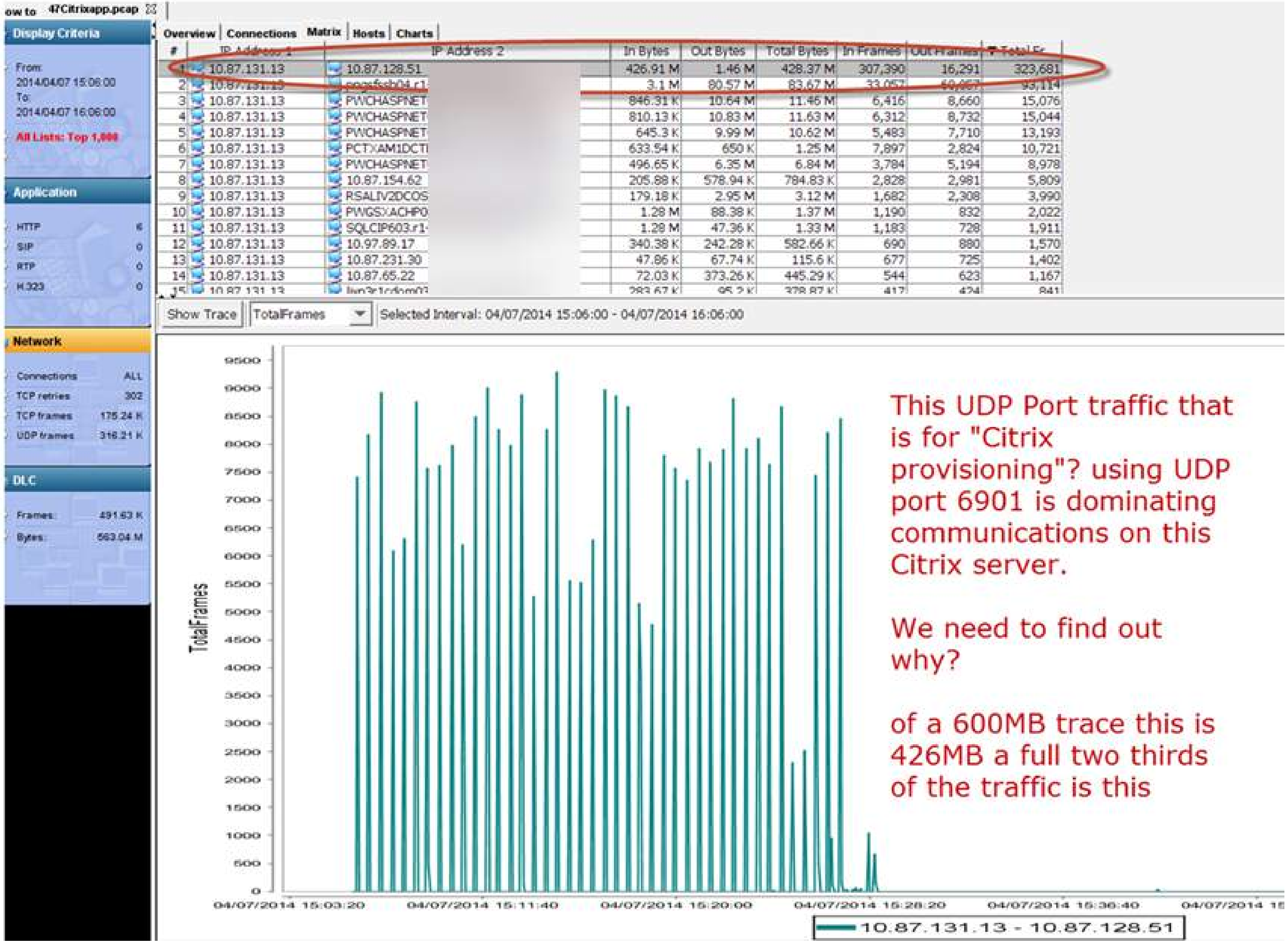
X Axis: Tick interval: 1 sec; Pixels per tick: 5; ☑ View as time of day

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.



#	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 [redacted]	426.91 M	1.46 M	428.37 M	307,390	16,291	323,681
2	10.87.131.13	pcgsfsb04.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	PCTXAM1DCTI [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 [redacted]	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 [redacted]	340.38 K	242.28 K	582.66 K	690	880	1,570
13	10.87.131.13	10.87.231.30 [redacted]	47.86 K	67.74 K	115.6 K	677	725	1,402
14	10.87.131.13	10.87.65.22 [redacted]	72.03 K	373.26 K	445.29 K	544	623	1,167
15	10.87.131.13	livn3r1cdom03 [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.

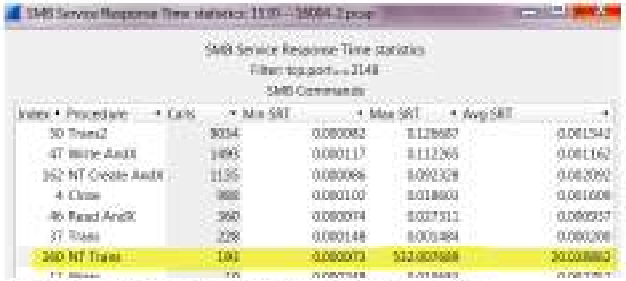
These commands cause SMB response times to seem long as a whole, and when deeper analysis is performed it is only the NT Notify transactions, which is an idiosyncrasy of operation.

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



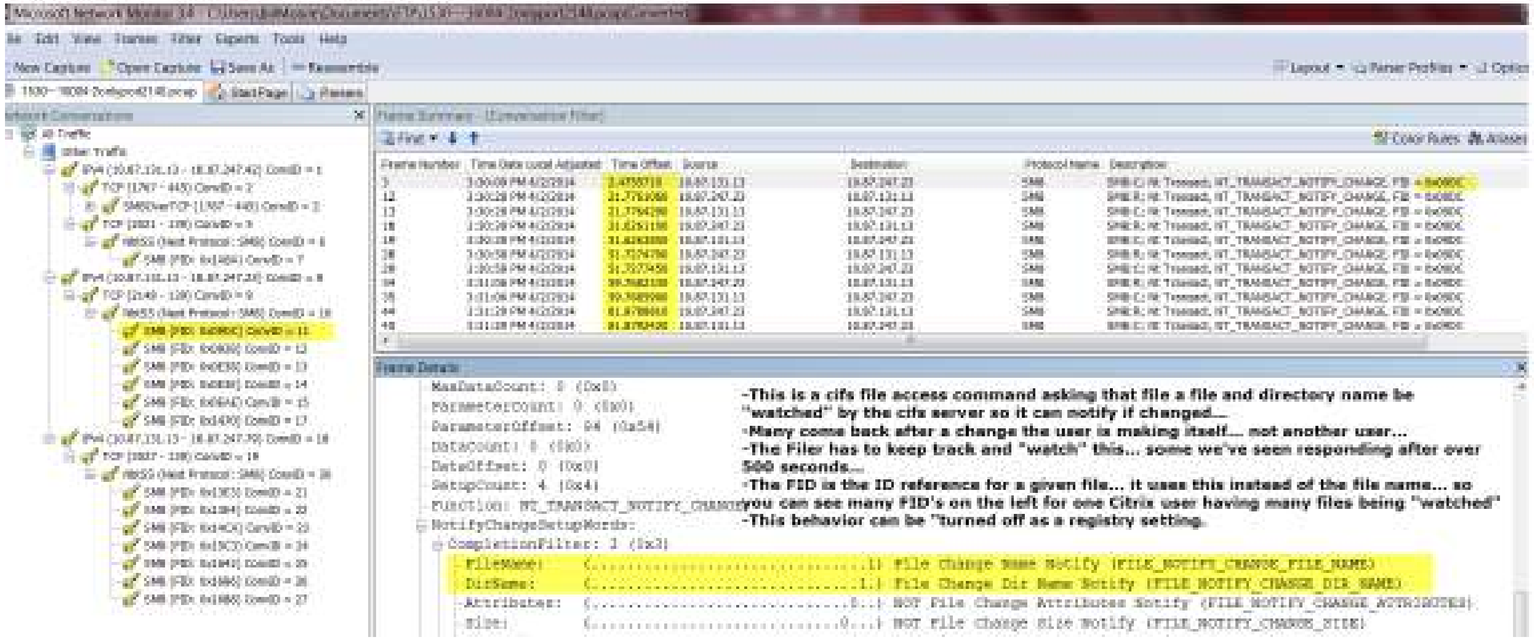
SMB Service Response Time statistics: 1530 – 18084-2.pcap

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

Index	Procedure	Calls	Min SRT	Max SRT	Avg SRT
50	Trans2	3034	0.000082	0.128687	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	888	0.000102	0.018603	0.001608
46	Read AndX	360	0.000074	0.027511	0.000957
37	Trans	228	0.000148	0.001484	0.000208
160	NT Trans	101	0.000073	512.007688	20.028862

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\[illegible]\Documents\[illegible]1530 – 18084_[illegible]2148.pcap.Converted
File Edit View Frames Filter Experts Tools Help
New Capture Open Capture Save As Reassemble
Layout Parser Profiles Options
1530 – 18084-2cetcport2148.pcap Start Page Parsers
Network 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 = 3
      TCP (3021 - 139) ConvID = 5
        NbtSS (Next Protocol : SMB) ConvID = 6
          SMB (FID: 0x1404) 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: 0x080C) ConvID = 11
          SMB (FID: 0x0800) ConvID = 12
          SMB (FID: 0x0E30) ConvID = 13
          SMB (FID: 0x0E30) ConvID = 14
          SMB (FID: 0x06AC) ConvID = 15
          SMB (FID: 0x1400) ConvID = 17
    IPv4 (10.87.131.13 - 10.87.247.70) ConvID = 18
      TCP (3027 - 139) ConvID = 19
        NbtSS (Next Protocol : SMB) ConvID = 20
          SMB (FID: 0x13C0) ConvID = 21
          SMB (FID: 0x13B4) ConvID = 22
          SMB (FID: 0x14C4) ConvID = 23
          SMB (FID: 0x15C0) ConvID = 24
          SMB (FID: 0x1840) ConvID = 25
          SMB (FID: 0x1860) ConvID = 26
          SMB (FID: 0x1880) ConvID = 27
```

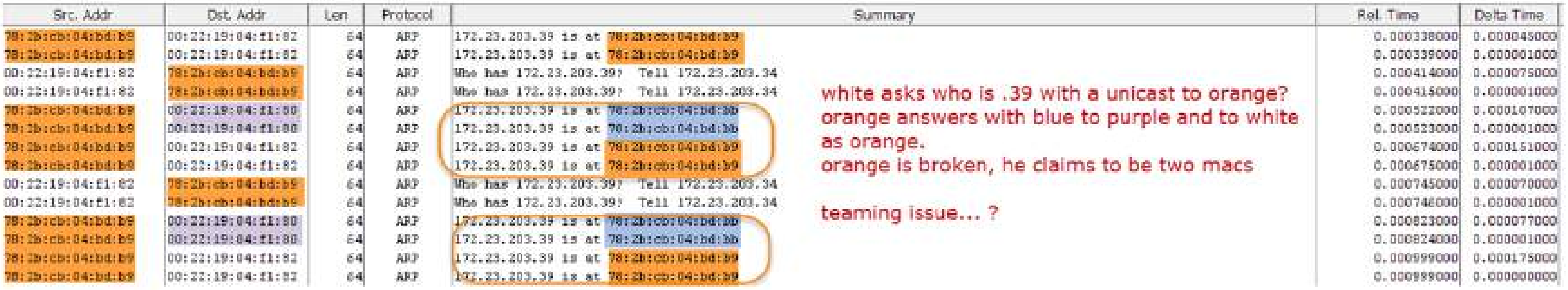
```
Frame Number  Time Date Local Adjusted  Time Offset  Source        Destination   Protocol Name  Description
3             3:30:09 PM 4/2/2014       2.4750719    10.87.131.13  10.87.247.23  SMB            SMB:C; NT Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x080C
12            3:30:28 PM 4/2/2014       21.7761088   10.87.247.23  10.87.131.13  SMB            SMB:R; NT Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x080C
13            3:30:28 PM 4/2/2014       21.7764298   10.87.131.13  10.87.247.23  SMB            SMB:C; NT Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x080C
18            3:30:38 PM 4/2/2014       31.6261198   10.87.247.23  10.87.131.13  SMB            SMB:R; NT Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x080C
19            3:30:38 PM 4/2/2014       31.6263359   10.87.131.13  10.87.247.23  SMB            SMB:C; NT Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x080C
28            3:30:58 PM 4/2/2014       51.7574788   10.87.247.23  10.87.131.13  SMB            SMB:R; NT Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x080C
29            3:30:58 PM 4/2/2014       51.7577458   10.87.131.13  10.87.247.23  SMB            SMB:C; NT Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x080C
34            3:31:08 PM 4/2/2014       59.7682158   10.87.247.23  10.87.131.13  SMB            SMB:R; NT Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x080C
35            3:31:08 PM 4/2/2014       59.7685988   10.87.131.13  10.87.247.23  SMB            SMB:C; NT Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x080C
44            3:31:28 PM 4/2/2014       81.8788658   10.87.247.23  10.87.131.13  SMB            SMB:R; NT Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x080C
45            3:31:28 PM 4/2/2014       81.8792420   10.87.131.13  10.87.247.23  SMB            SMB:C; NT Transact, NT_TRANSACT_NOTIFY_CHANGE, FID = 0x080C
```

```
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

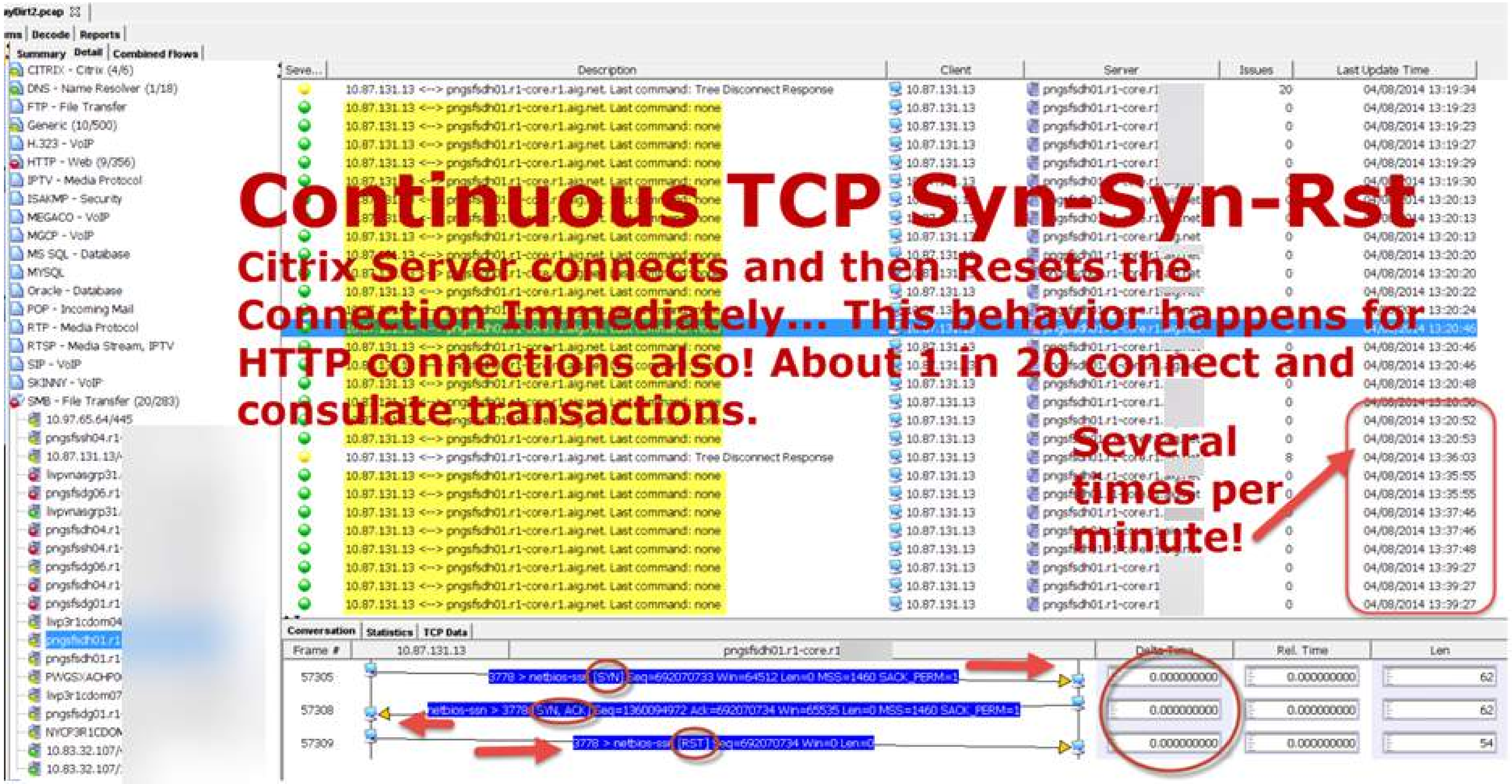
white asks who is .39 with a unicast to orange?
orange answers with blue to purple and to white as orange.
orange is broken, he claims to be two macs

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.



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
●	10.87.131.13 <--> pngsfsdh01.r1-core.r1.aig.net. Last command: none	10.87.131.13	pngsfsdh01.r1-core.r1 [illegible]	[illegible]	04/08/2014 13:19:30
●	[illegible]	[illegible]	[illegible]	[illegible]	[illegible] 13:20:13
●	[illegible]	[illegible]	pngsfsdh0[illegible].net	[illegible]	[illegible] 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].net	0	04/08/2014 13:20:13
●	[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] 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]	0	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]	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 13:37:46
●	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

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!

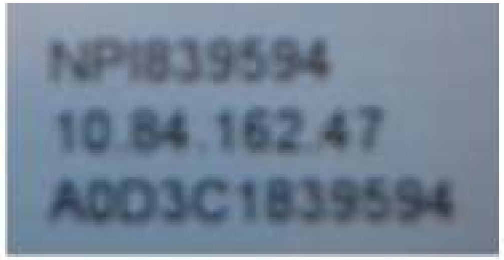
Printing Issues

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

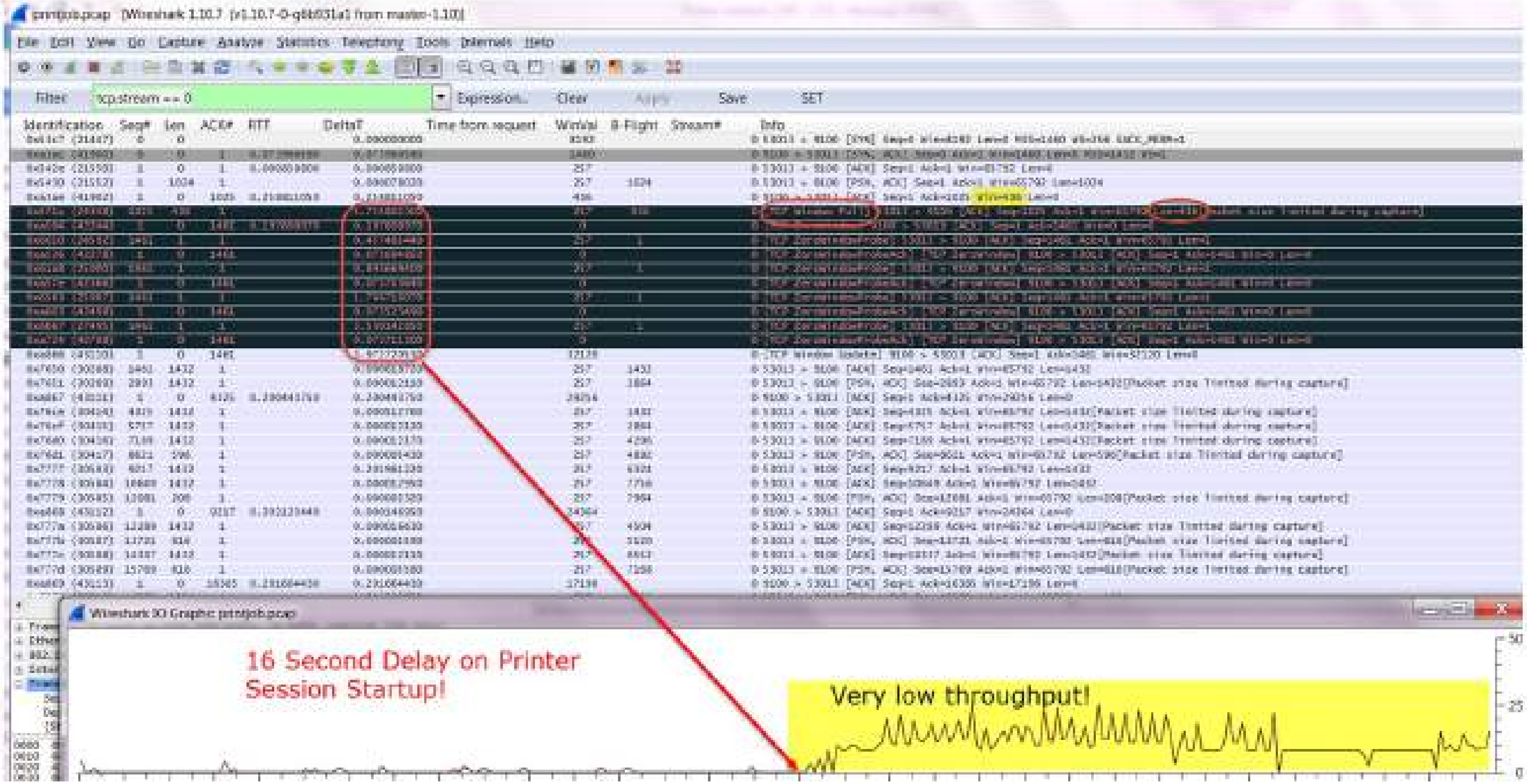
As a result of these evidentiary exhibits which had to be asserted aggressively to Client and HP personnel until acceptance of the problems were accepted.

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
Filter: tcp.stream == 0
Expression... Clear Apply Save SET
Identification Seq# Len ACK# RTT DeltaT Time from request WinVal B-Flight Stream# Info
Wireshark IO Graphs: printjob.pcap
50
25
0

16 Second Delay on Printer Session Startup!

Very low throughput!

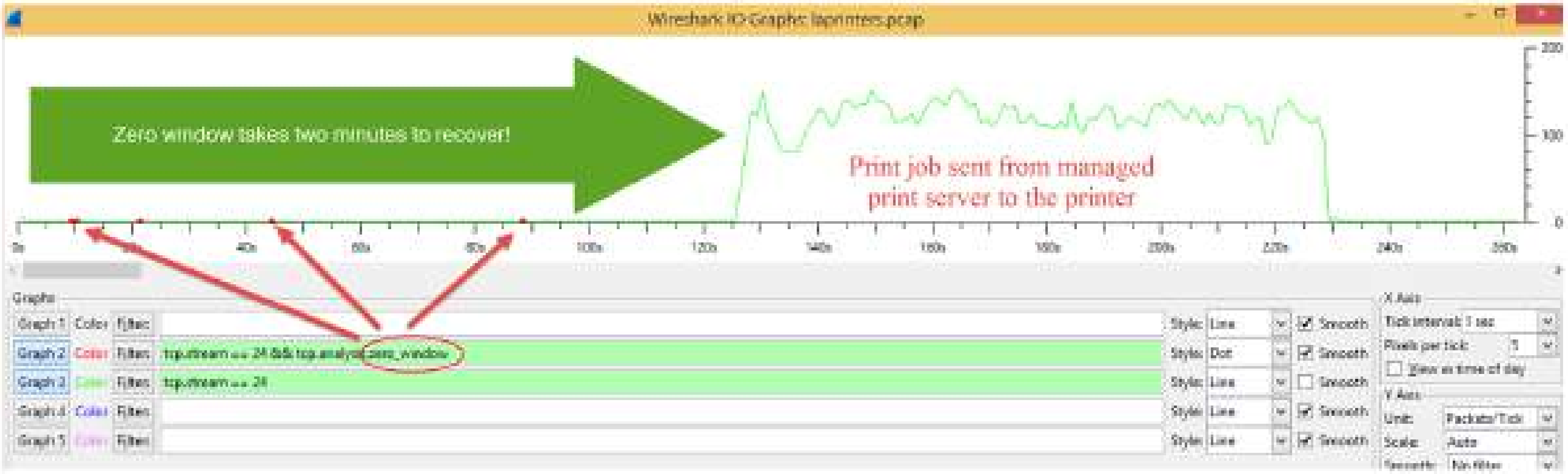
Printing Issues

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.



Wireshark IO Graphs: laprinters.pcap

Zero window takes two minutes to recover!

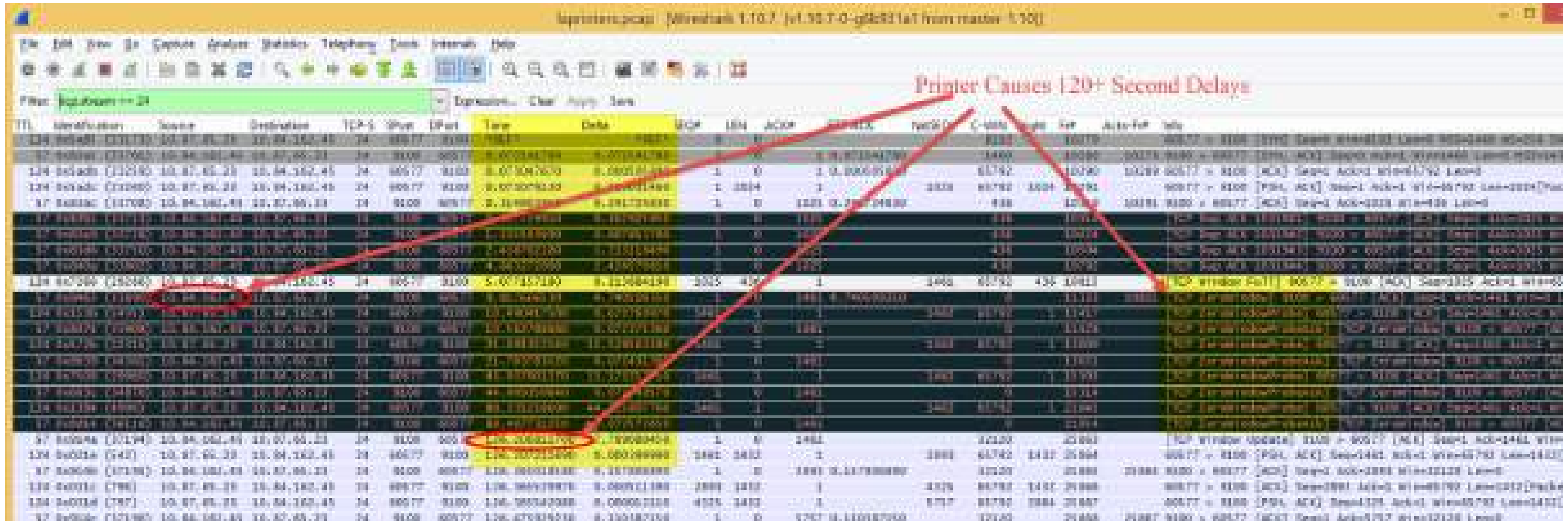
Print job sent from managed print server to the printer

Graph 2 Filter: tcp.stream == 24 && tcp.analysis.zero_window — Style: Dot — ☑ Smooth

Graph 3 Filter: tcp.stream == 24 — 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



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

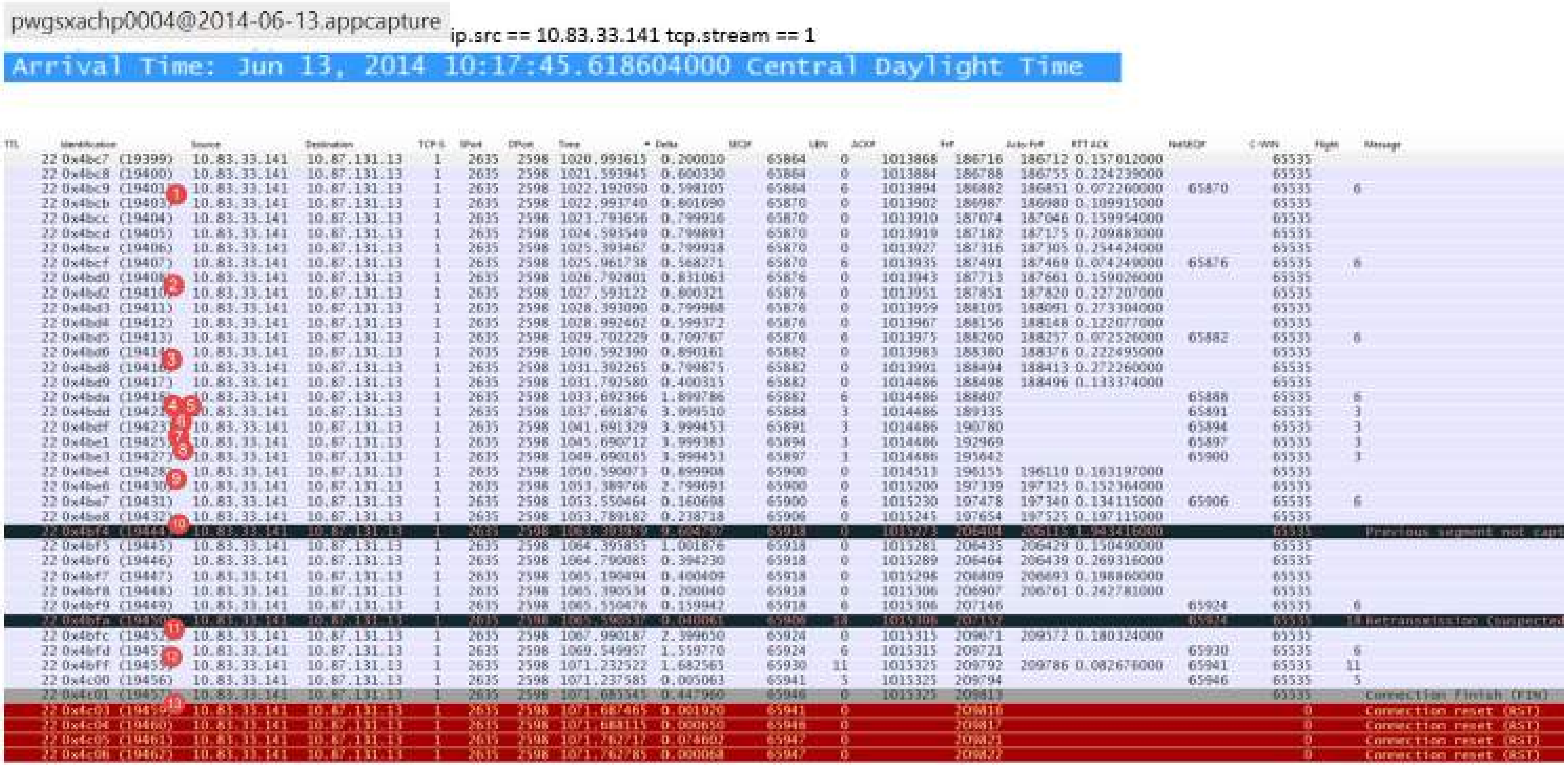
Filter: tcp.stream == 24

Printer Causes 120+ Second Delays

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 0.799891  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 (1941    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 (1941    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 (1941    0.83.33.141   10.87.131.13  1     2635  2598  1033.692366 1.899786  65882  6   1014486 188807                      65888   65535   6
  22 0x4bdd (1942    0.83.33.141   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 (1942    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 197139 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  1063.393879 9.604797  65918  0   1015273 206404 206115 1.983416000          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   1015296 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 (1945    10.83.33.141  10.87.131.13  1     2635  2598  1065.590537 0.040061  65906  18  1015306 207152                      65924   65535  18Retransmission (suspected
  22 0x4bfc (1945    10.83.33.141  10.87.131.13  1     2635  2598  1067.990187 2.399650  65924  0   1015315 209071 209572 0.180324000          65535
  22 0x4bfd (1945    10.83.33.141  10.87.131.13  1     2635  2598  1069.549957 1.559770  65924  6   1015315 209721                      65930   65535   6
  22 0x4bff (1945    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 (1945    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

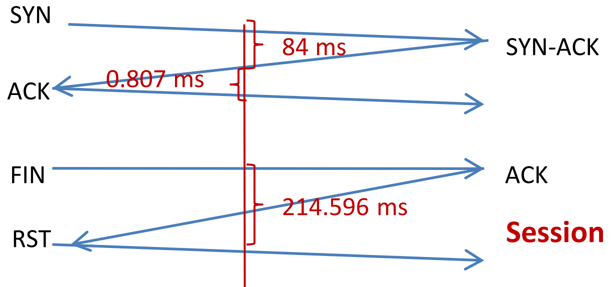
Opposing Packet Transaction Exchanges of:

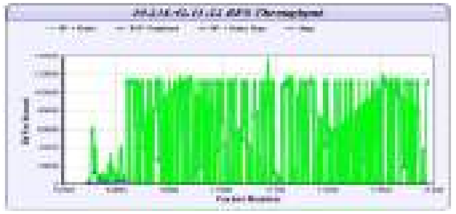
- Packet Sizes
- Response Times
- Bits Per Second by Layer
- Offered load into TCP Window vs. Receive Window Size
- Offered load unacknowledged packets
- Packet rate of session vs. packets to others
- Cumulative Bytes
- Data vs. Application Efficiency

Error Visualizations:

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

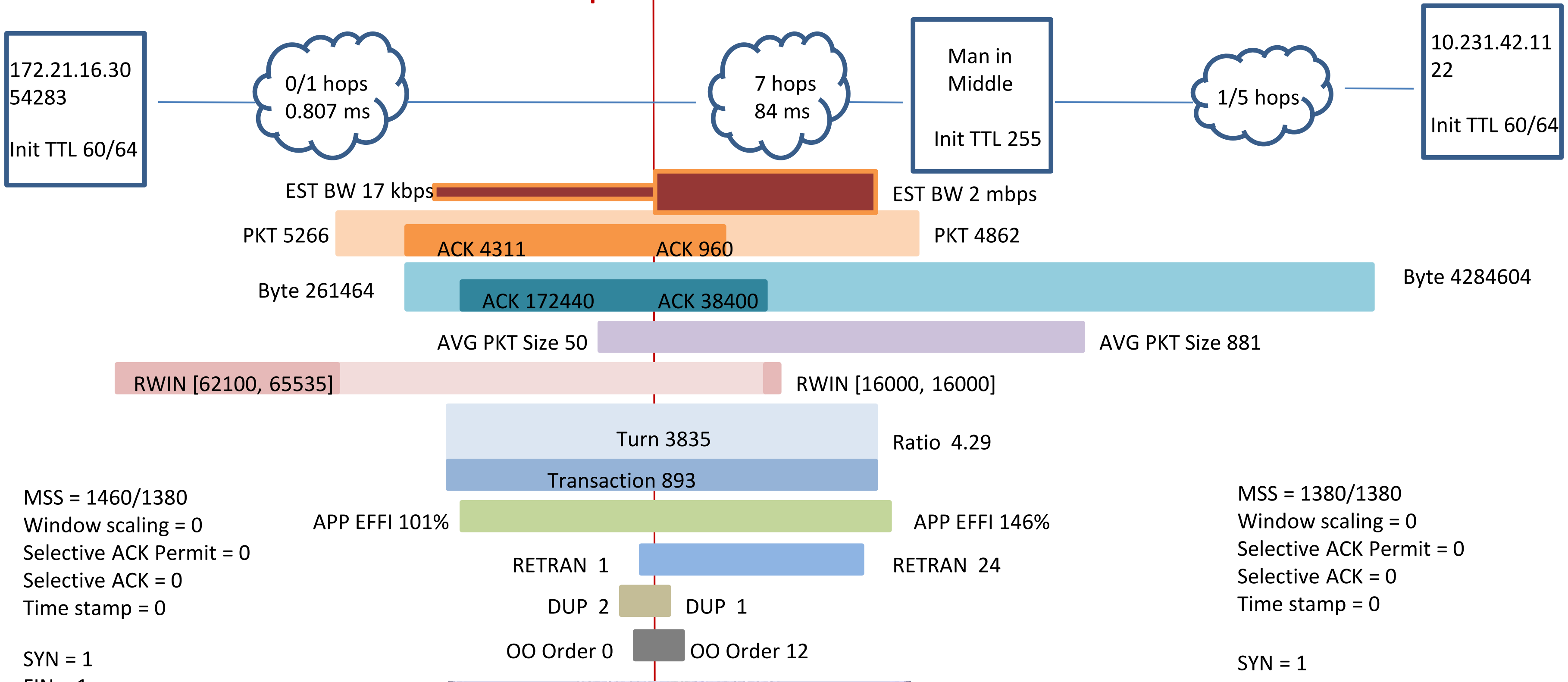
Session Summary 172.21.16.30:54283-10.231.42.11:22





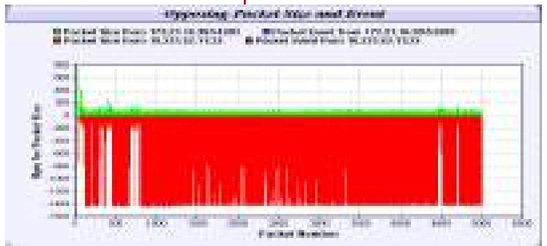
Session duration 1 hour 12 minutes

Capture Location



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)

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

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

Serious Events

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

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

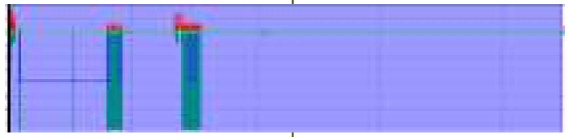
MSS = 1460/1460
Window scaling = 0
Selective ACK Permit = 1
Selective ACK = 0
Time stamp = 0

FIN

ACK

0.2 ms

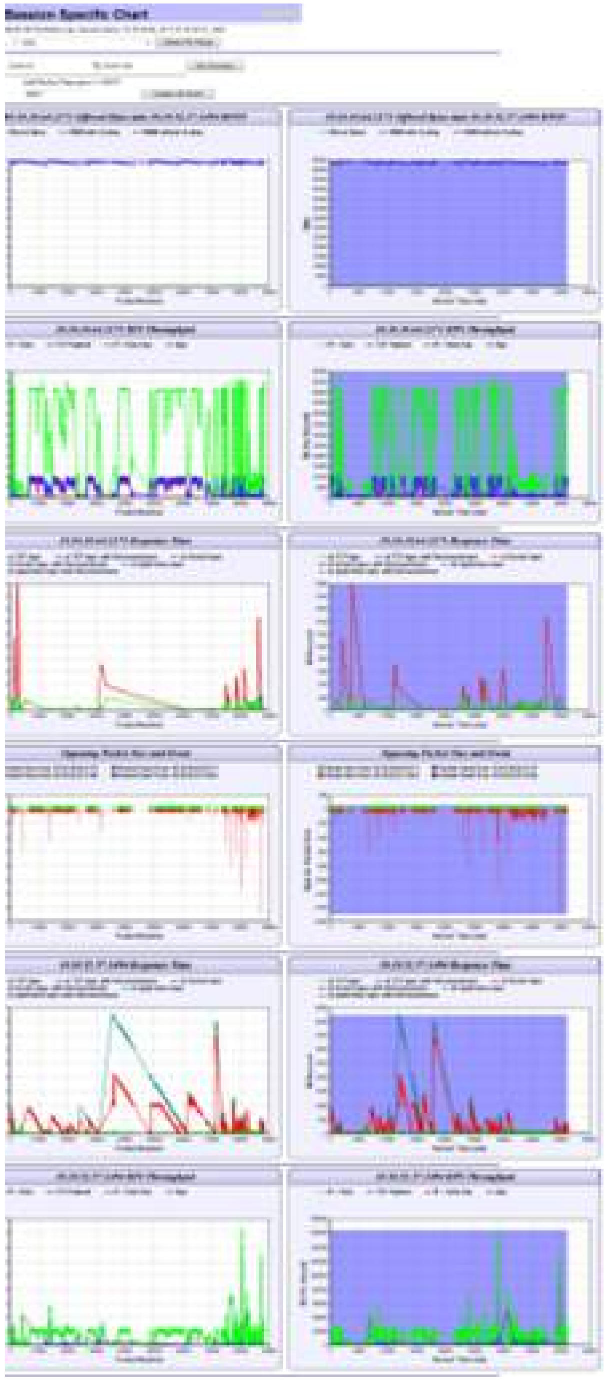
FIN

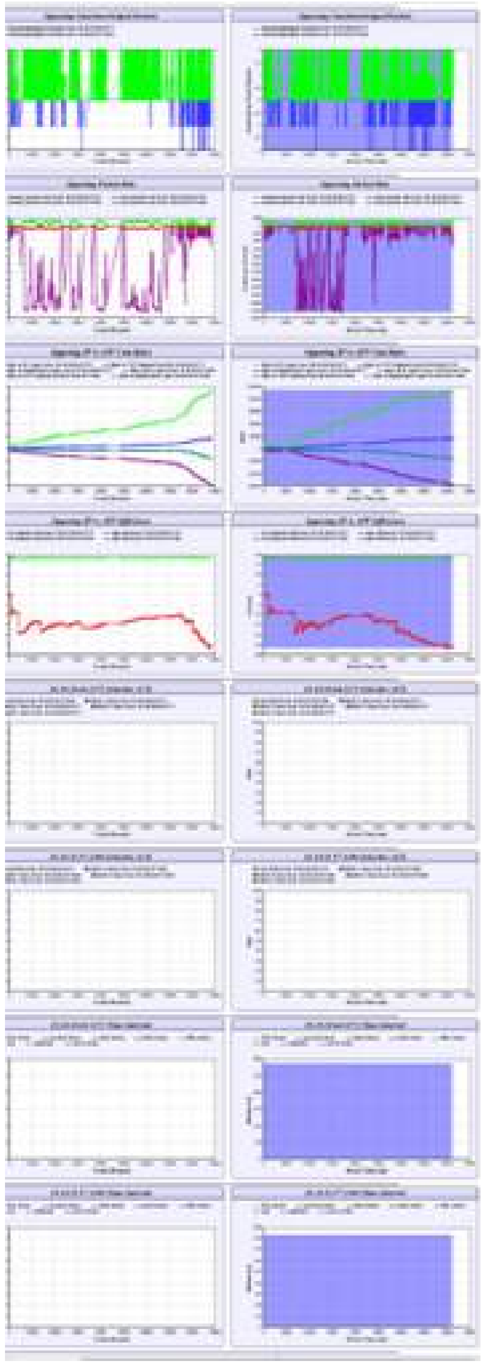


Opposing packet size

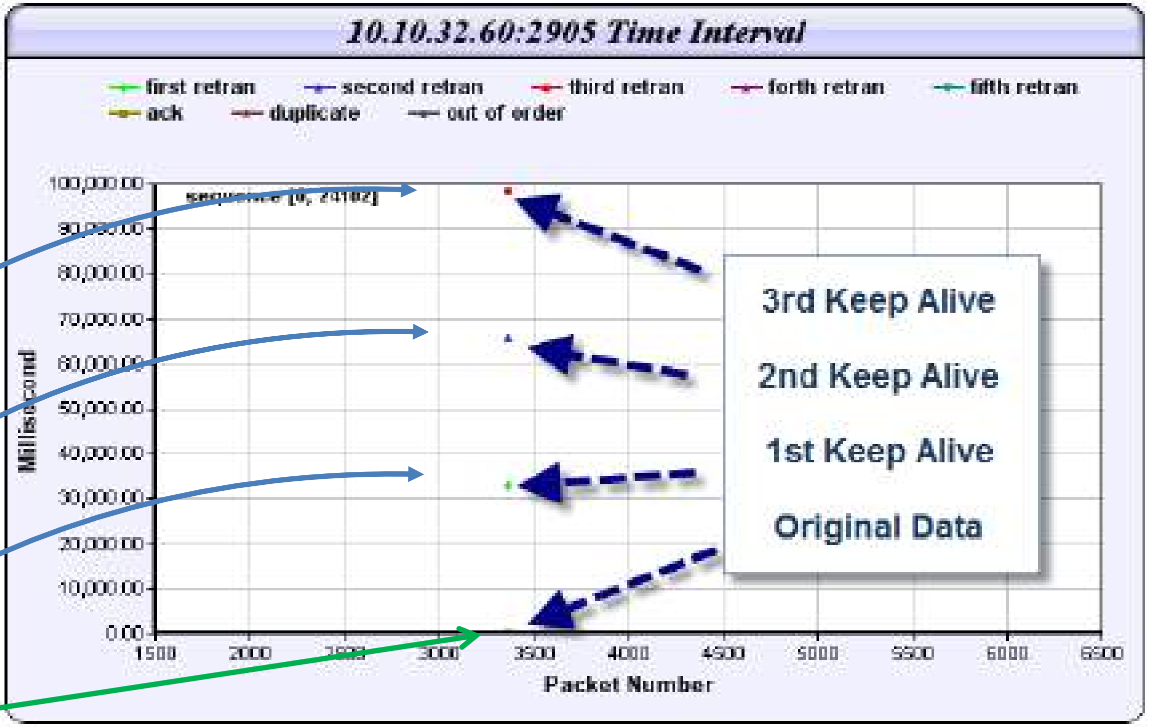
Performance Event Detection

- 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



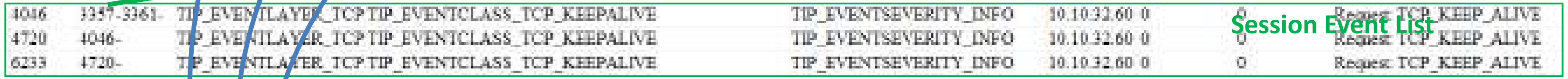


Time Interval Chart
Event List
Packet Trace

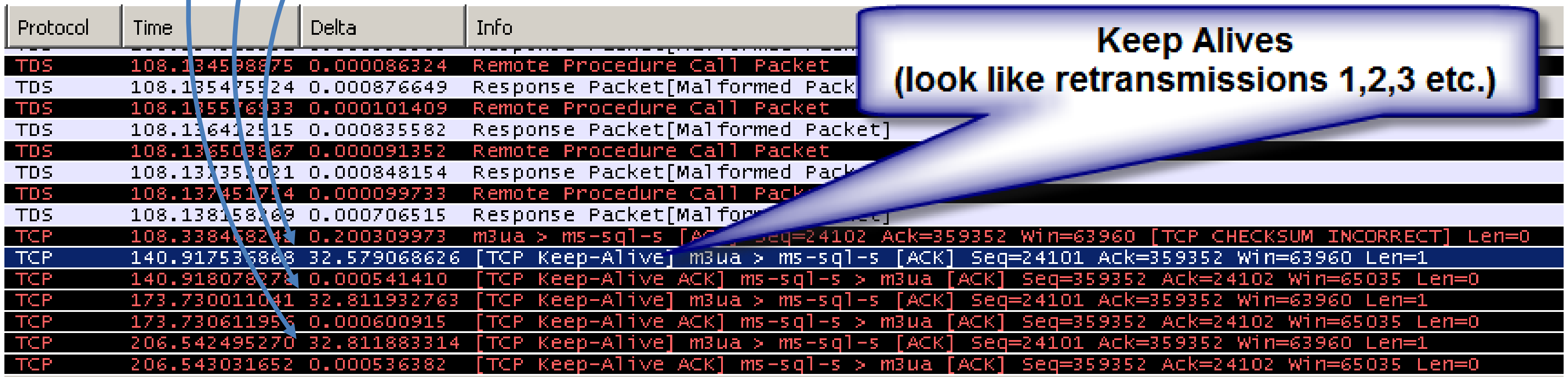


Related Packet

Session Event List



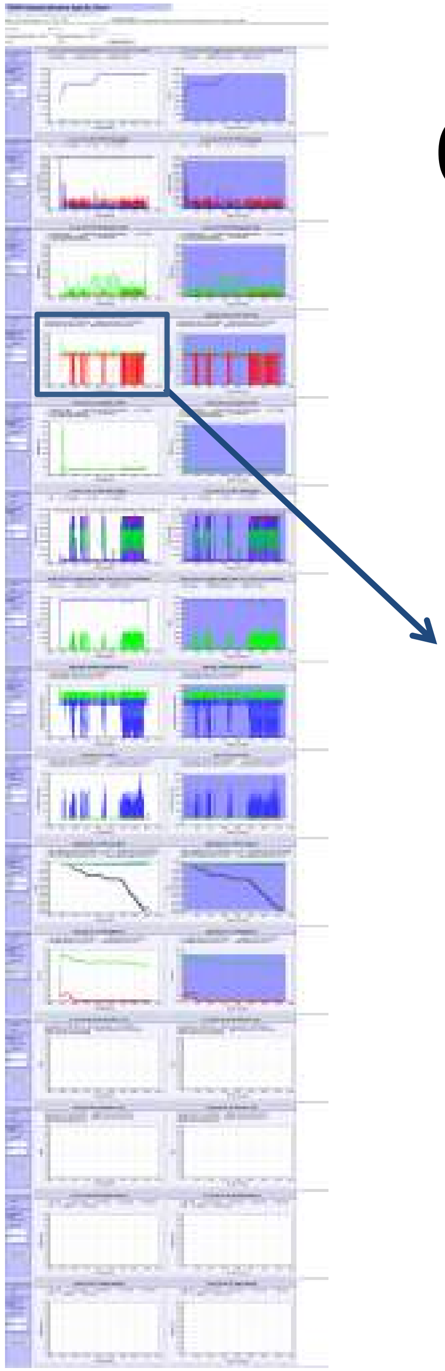
```
4046   3357-3361-  TIP_EVENTLAYER_TCP TIP_EVENTCLASS_TCP_KEEPALIVE   TIP_EVENTSEVERITY_INFO   10.10.32.60 0   0   Request: TCP_KEEP_ALIVE
4720   4046-       TIP_EVENTLAYER_TCP TIP_EVENTCLASS_TCP_KEEPALIVE   TIP_EVENTSEVERITY_INFO   10.10.32.60 0   0   Request: TCP_KEEP_ALIVE
6233   4720-       TIP_EVENTLAYER_TCP 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       108.137451714  0.000099733   Remote Procedure Call Pack
TDS       108.138158269  0.000706515   Response Packet[Malfor
TCP       108.338468242  0.200309973   m3ua > ms-sql-s [AC  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



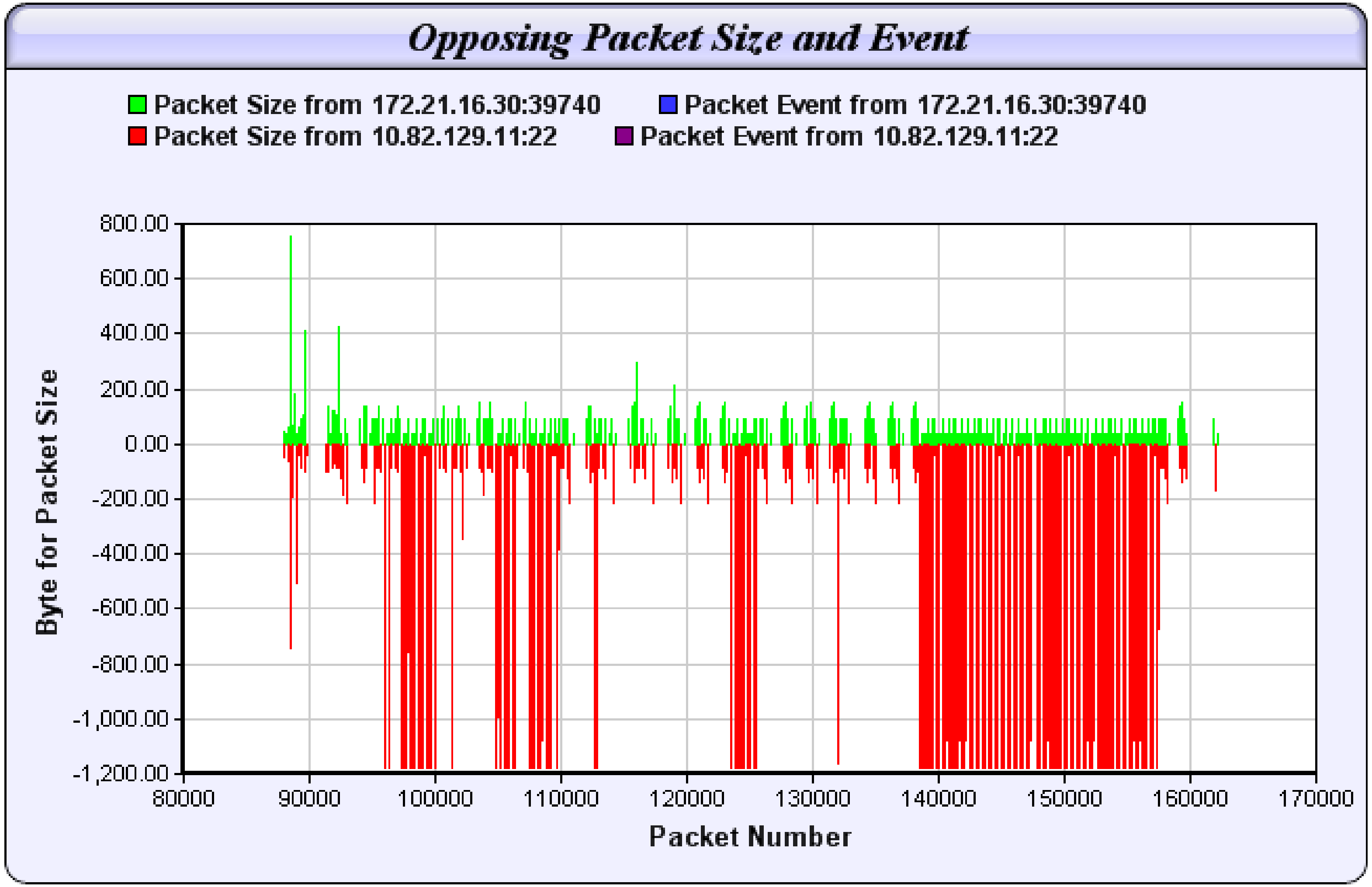
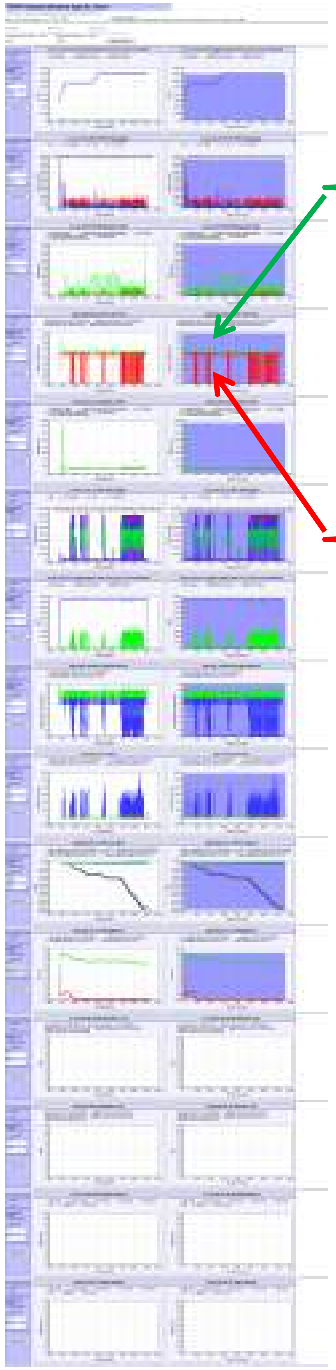

Opposing Packet Size and Event
🟩 Packet Size from 172.21.16.30:39740
🟦 Packet Event from 172.21.16.30:39740
🟥 Packet Size from 10.82.129.11:22
🟪 Packet Event from 10.82.129.11:22
Byte for Packet Size
800.00
600.00
400.00
200.00
0.00
-200.00
-400.00
-600.00
-800.00
-1,000.00
-1,200.00
80000
90000
100000
110000
120000
130000
140000
150000
160000
170000
Packet Number

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)

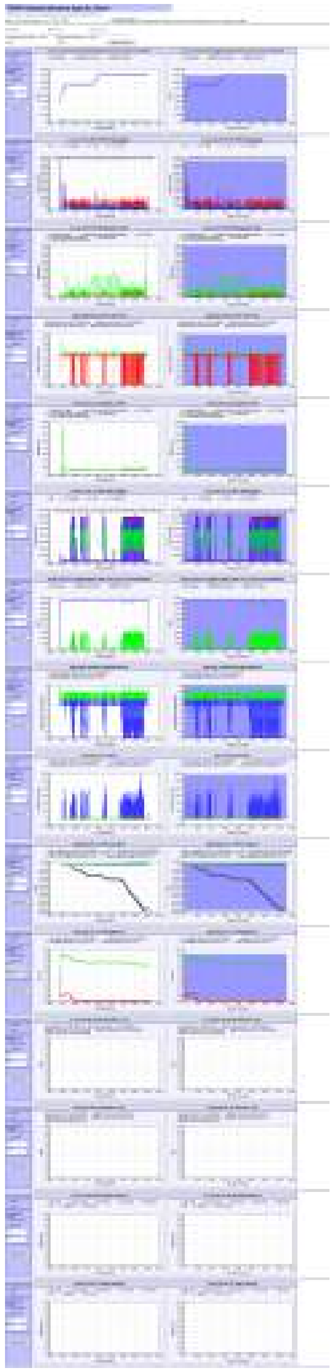
Opposing Application Efficiency

Directional Selective ACK

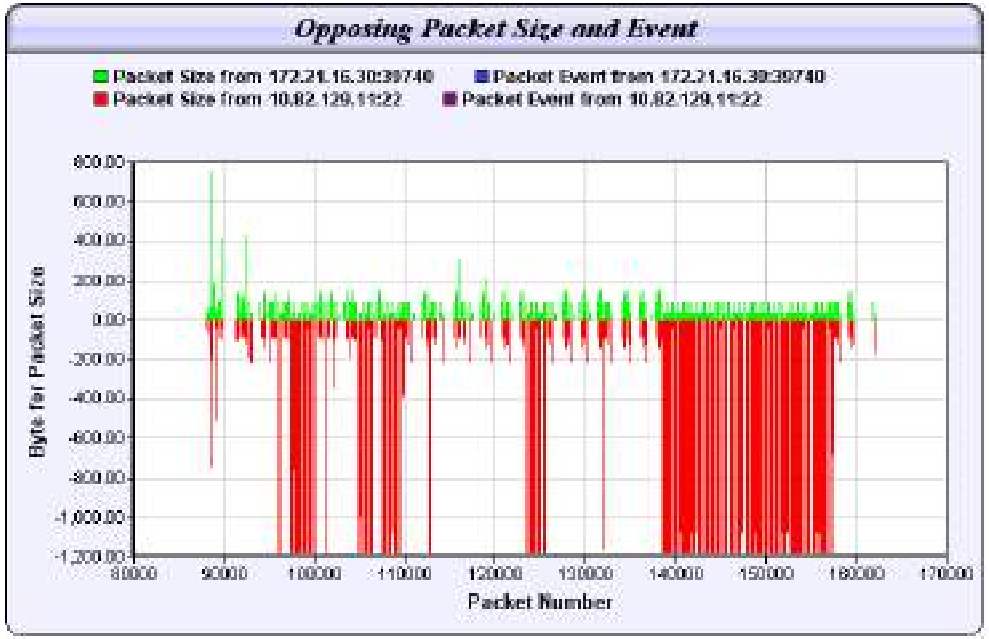
Directional Selective ACK

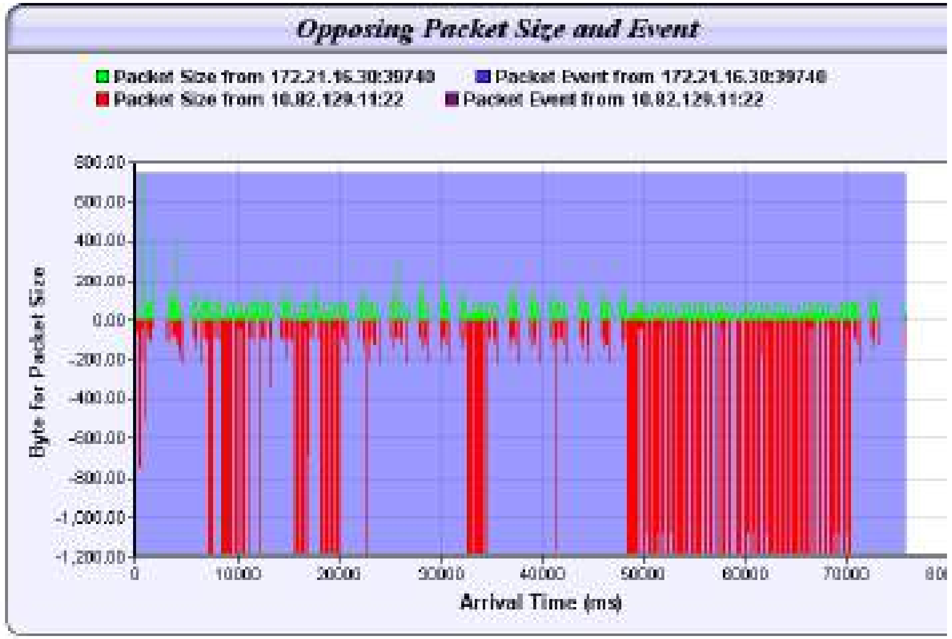
Directional Time Interval (Retrans / Dupe / Out of Order)

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

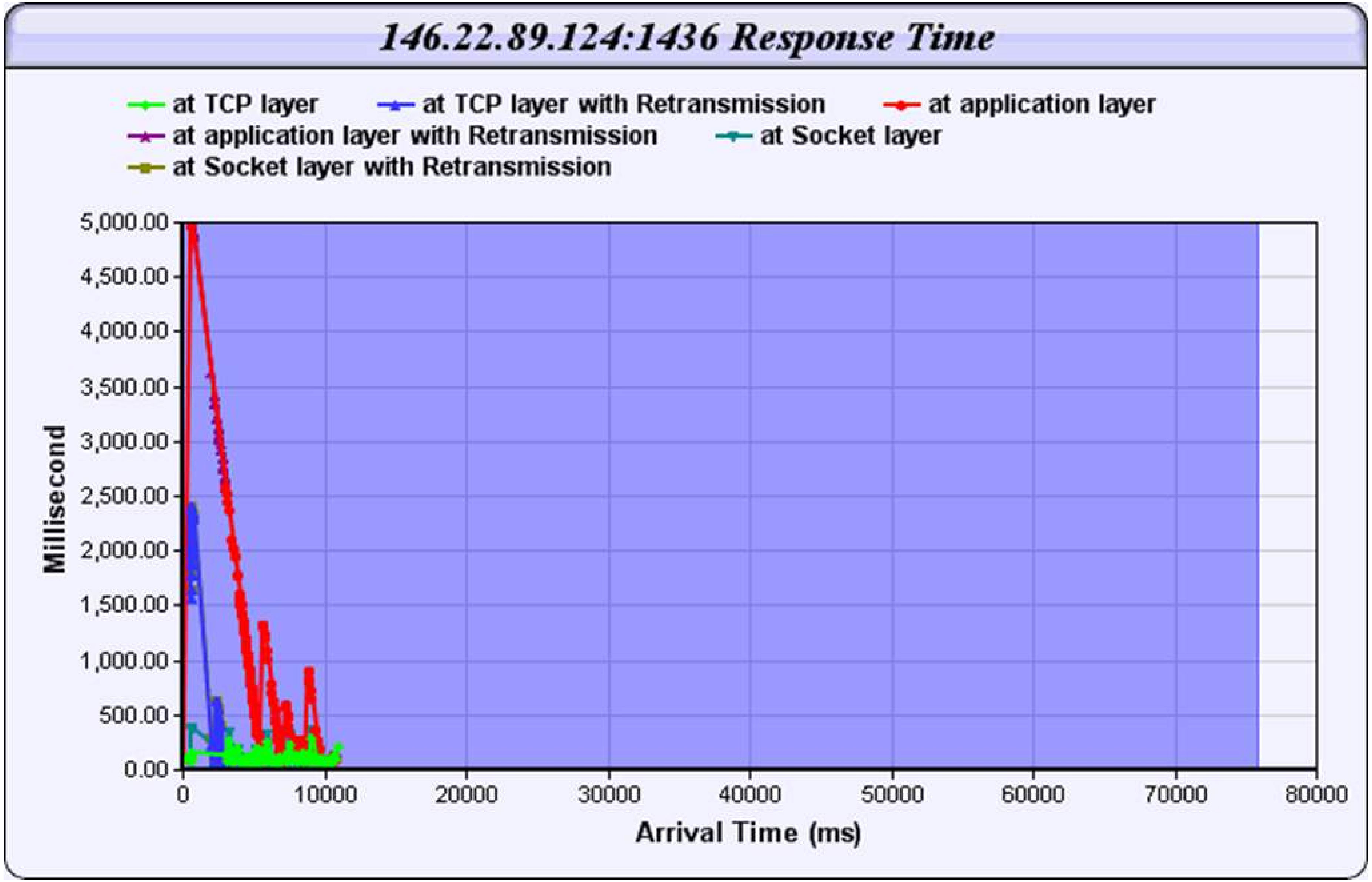


Opposing Packet Size

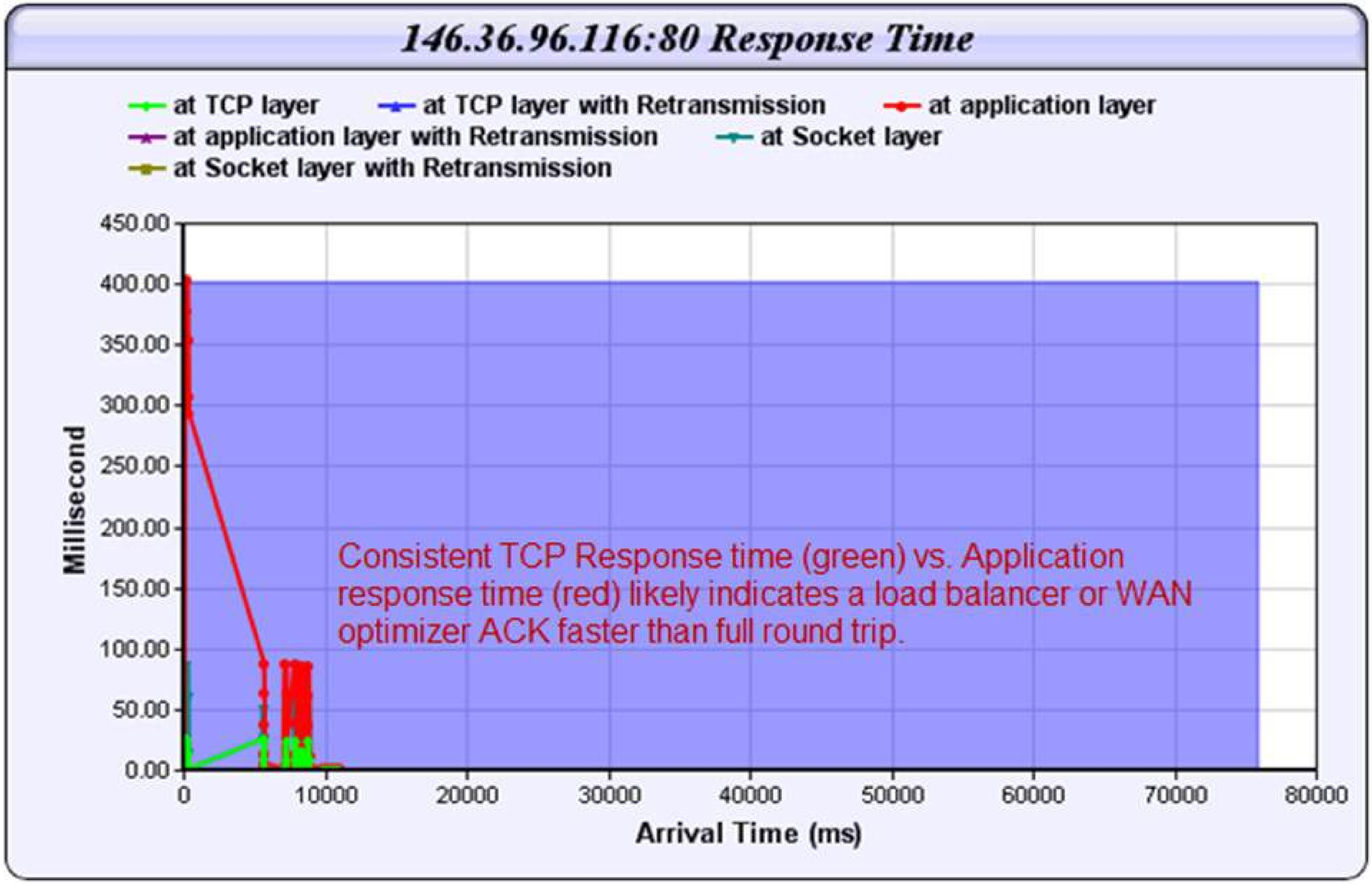




Response Time by layer

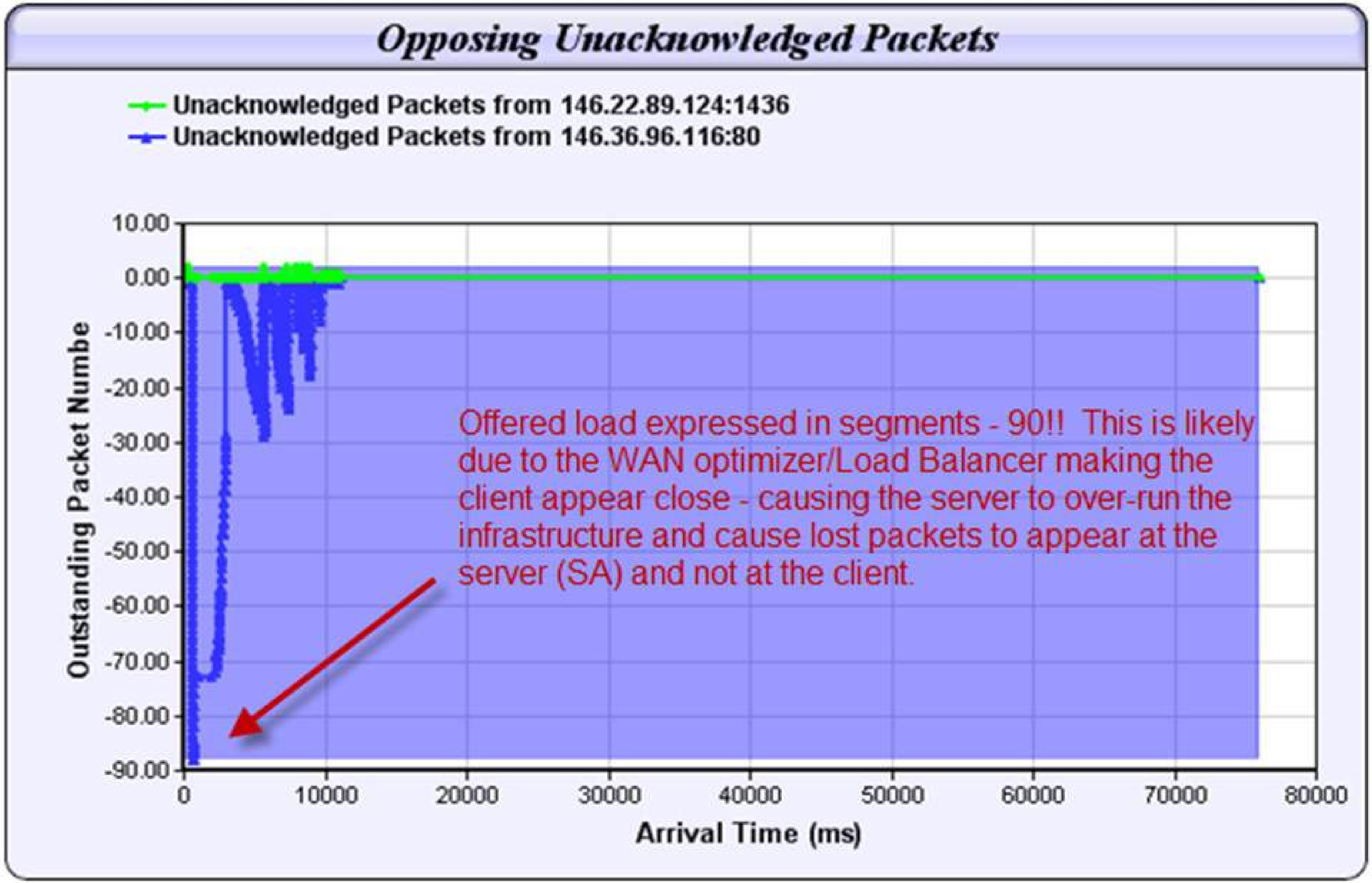


TCP Response Time by layer



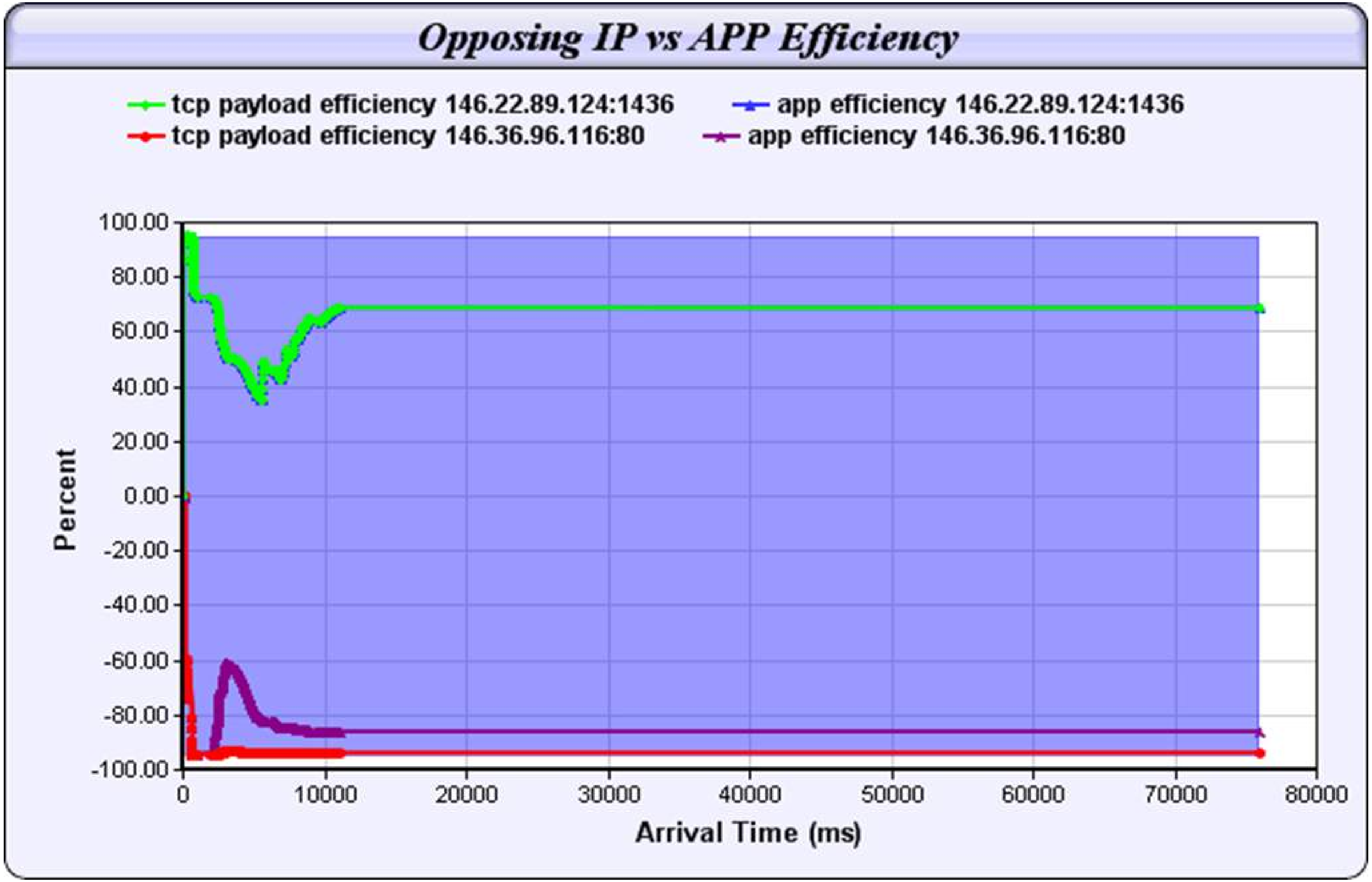
Consistent TCP Response time (green) vs. Application response time (red) likely indicates a load balancer or WAN optimizer ACK faster than full round trip.

Opposing Unacked Packets

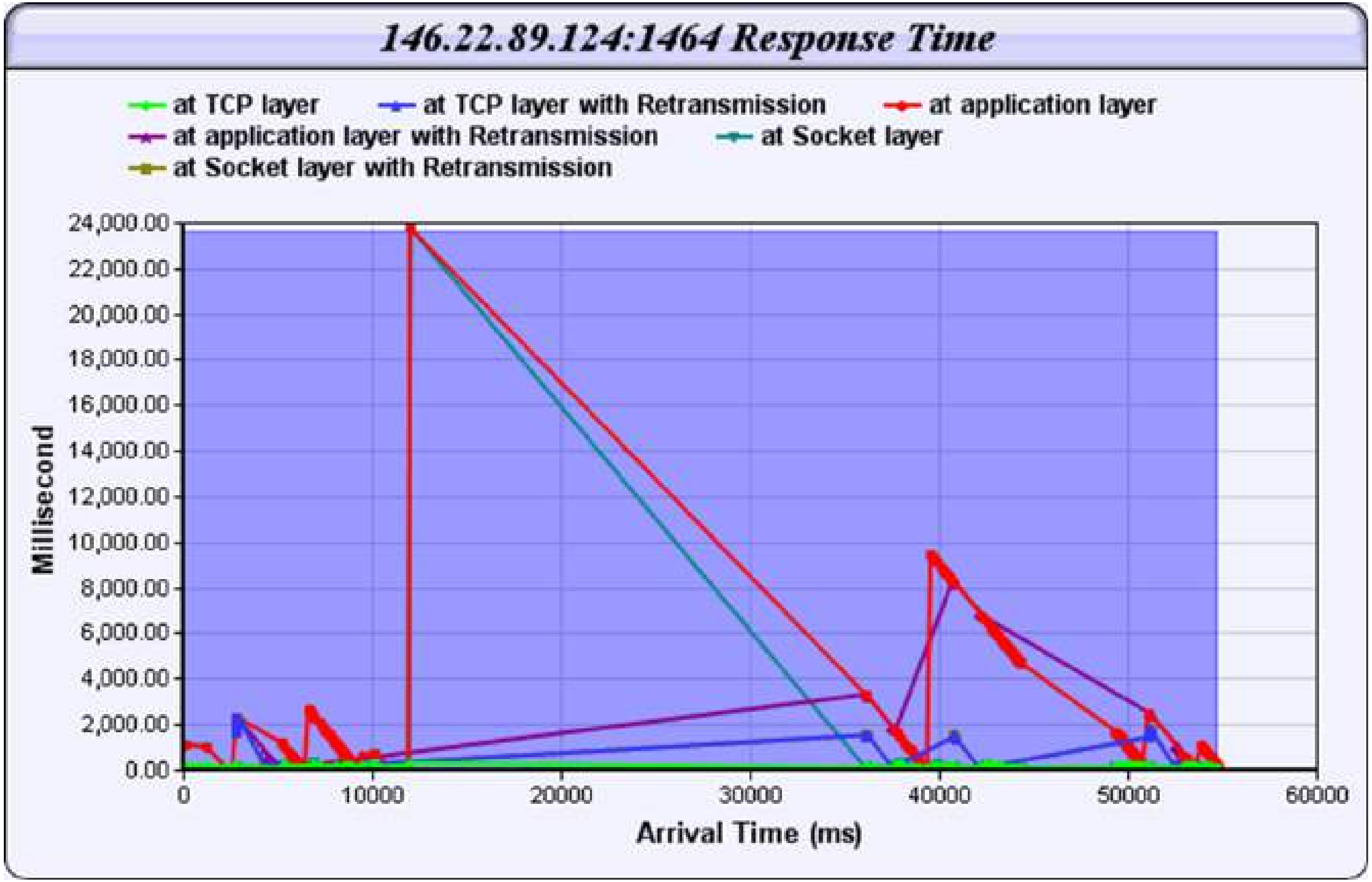


Offered load expressed in segments - 90!! This is likely due to the WAN optimizer/Load Balancer making the client appear close - causing the server to over-run the infrastructure and cause lost packets to appear at the server (SA) and not at the client.

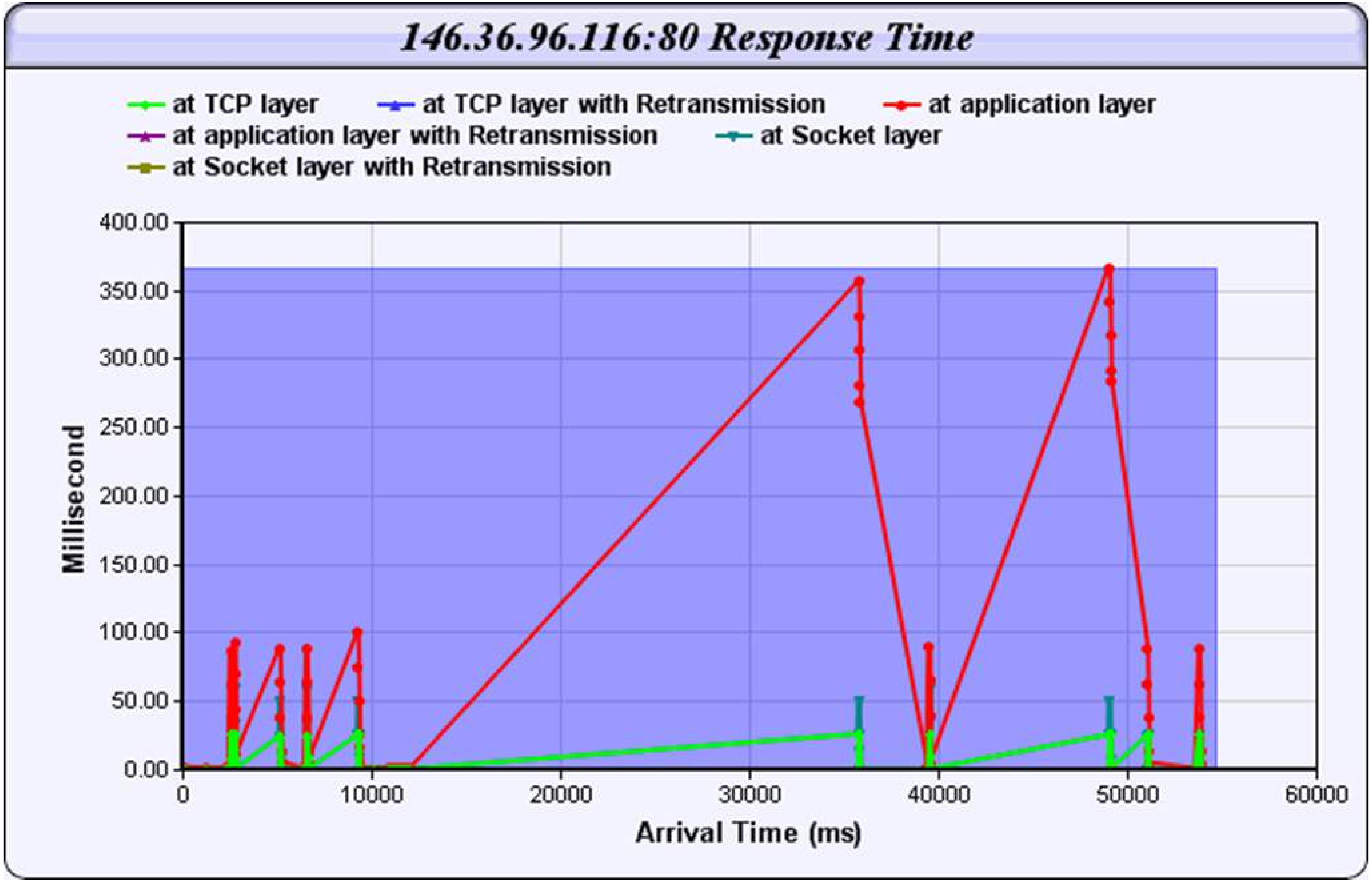
Opposing IP vs. App Efficiency



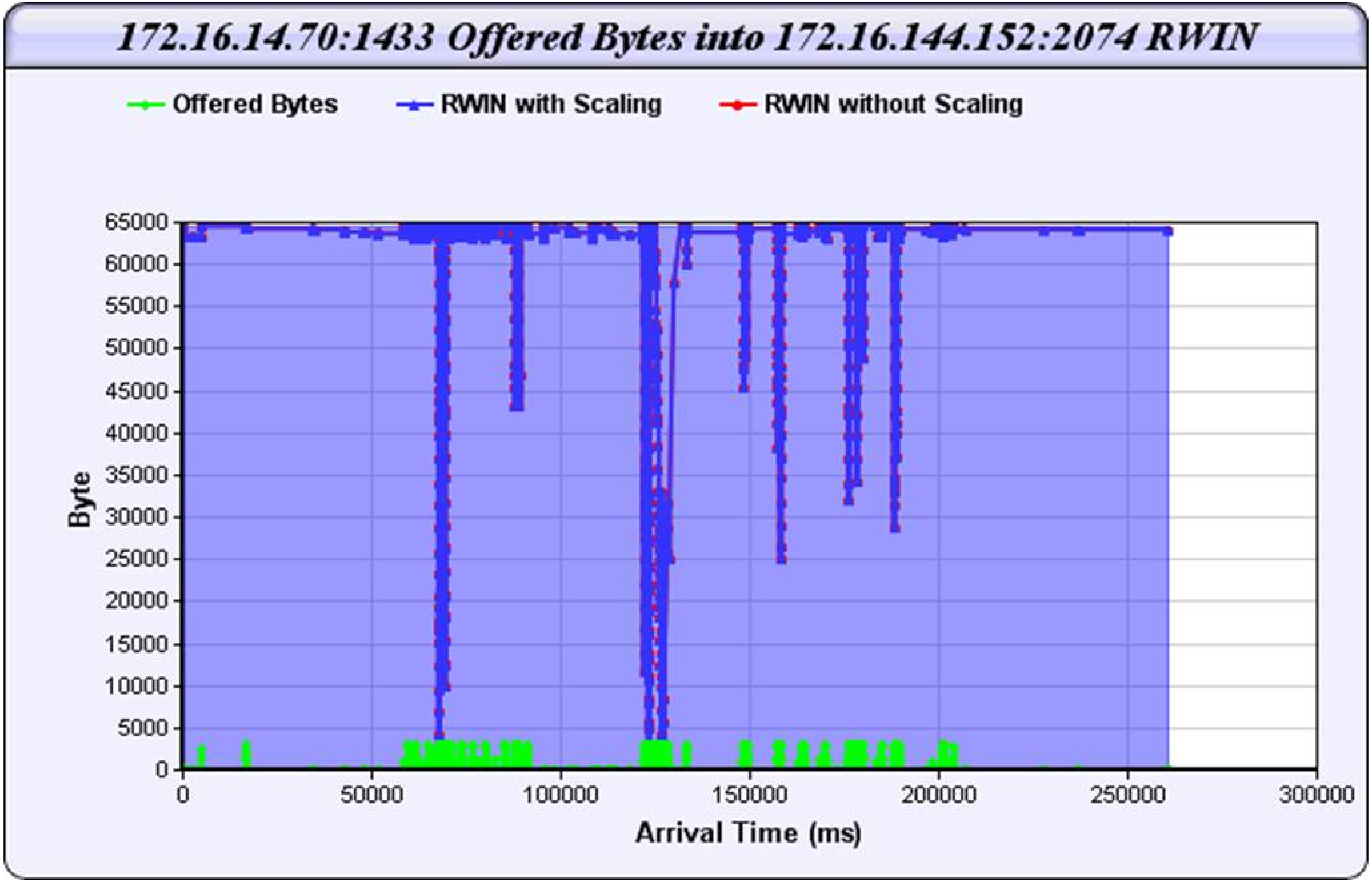
Layer Response Times



Response Times



Offered Bytes into RWIN

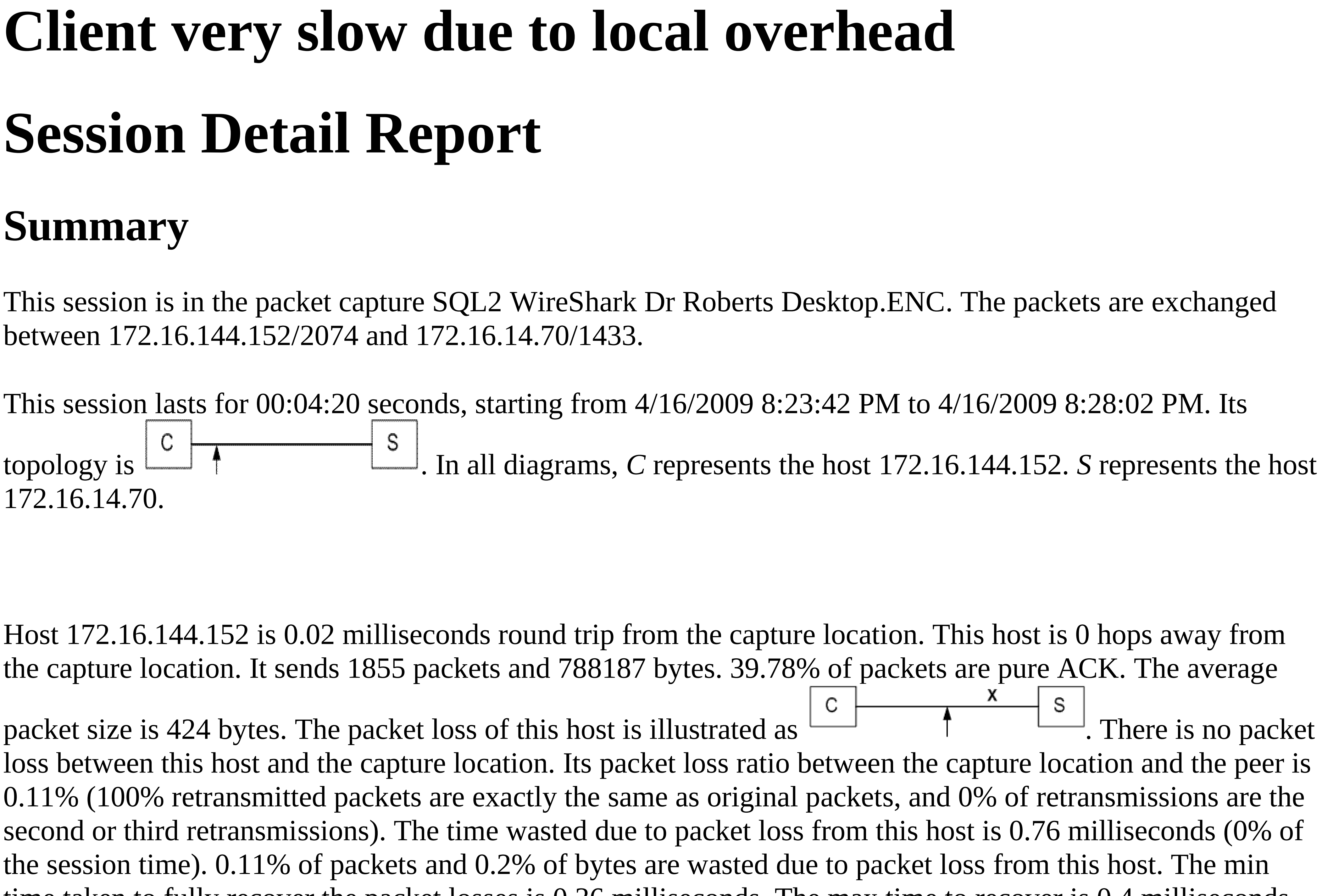


Cogent … *clear, collaborative, insightful*
powerfully persuasive, balanced, weighty, inclusive

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 C ↑ S. 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 C ↑ x S. 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