

WIRESHARK EDUCATION DAY – OLTEN CH 2026

# Wireshark Case Studies

**Sake Blok**

*sake.blok@SYN-bit.nl*



The Wireshark logo, which consists of a stylized white shark fin icon above the word 'WIRESHARK' in a large, bold, white sans-serif font.

Sponsored by:





# Case 1:

## Slow performance when moving application to another system

---



## *Topic starter:*

I've been having an ongoing issue with performance in our Sage application which seems to be narrowed down to a network issue between the clients at x.y.z.251,252 and the server at x.y.z.250.

I'm still trying to put my finger on exactly what's causing this but see a lot of TCP retransmissions. Hoping someone could shed some light on the situation. I haven't used wireshark in years.





# Why are there retransmissions?



| tcp.stream == \${tcp.stream} |              |             |                |         |           |             |     |                |          |        |                                                                               |
|------------------------------|--------------|-------------|----------------|---------|-----------|-------------|-----|----------------|----------|--------|-------------------------------------------------------------------------------|
| No.                          | Relative     | Delta       | tcp.time_delta | #stream | Source    | Destination | TTL | Identification | Protocol | Length | Info                                                                          |
| 4798                         | 29.918835200 | 0.000099700 | 0.000099700    | 22      | DB-SERVER | client-1    | 128 | 0xe562         | TDS      | 811    | Response                                                                      |
| 4799                         | 29.920017300 | 0.001182100 | 0.001182100    | 22      | client-1  | DB-SERVER   | 128 | 0x2643         | TDS      | 788    | SQL batch                                                                     |
| 4800                         | 29.920095000 | 0.000077700 | 0.000077700    | 22      | DB-SERVER | client-1    | 128 | 0xe563         | TDS      | 477    | Response                                                                      |
| 4803                         | 29.939304000 | 0.019209000 | 0.019209000    | 22      | DB-SERVER | client-1    | 128 | 0xe565         | TCP      | 477    | [TCP Retransmission] 1433 → 60612 [PSH, ACK] Seq=32738 Ack=15443 Win=2100992  |
| 4804                         | 29.939712400 | 0.000408400 | 0.000408400    | 22      | client-1  | DB-SERVER   | 128 | 0x2645         | TCP      | 66     | 60612 → 1433 [ACK] Seq=15443 Ack=33161 Win=65280 Len=0 SLE=32738 SRE=33161    |
| 4815                         | 29.975532900 | 0.035820500 | 0.035820500    | 22      | client-1  | DB-SERVER   | 128 | 0x264b         | TDS      | 1166   | SQL batch                                                                     |
| 4816                         | 29.976143500 | 0.000610600 | 0.000610600    | 22      | DB-SERVER | client-1    | 128 | 0xe56e         | TCP      | 1514   | 1433 → 60612 [ACK] Seq=33161 Ack=16555 Win=2102272 Len=1460 [TCP PDU reassemb |
| 4818                         | 29.996151700 | 0.020008200 | 0.020008200    | 22      | DB-SERVER | client-1    | 128 | 0xe56f         | TCP      | 1514   | [TCP Retransmission] 1433 → 60612 [ACK] Seq=33161 Ack=16555 Win=2102272 Len=1 |
| 4819                         | 29.996718300 | 0.000566600 | 0.000566600    | 22      | client-1  | DB-SERVER   | 128 | 0x264c         | TCP      | 66     | 60612 → 1433 [ACK] Seq=16555 Ack=34621 Win=65280 Len=0 SLE=33161 SRE=34621    |
| 4820                         | 29.996724000 | 0.000005700 | 0.000005700    | 22      | DB-SERVER | client-1    | 128 | 0xe570         | TDS      | 2974   | Response (Not last buffer)                                                    |
| 4821                         | 29.996995400 | 0.000271400 | 0.000271400    | 22      | client-1  | DB-SERVER   | 128 | 0x264d         | TCP      | 60     | 60612 → 1433 [ACK] Seq=16555 Ack=37541 Win=65280 Len=0                        |
| 4822                         | 29.996998300 | 0.000002900 | 0.000002900    | 22      | DB-SERVER | client-1    | 128 | 0xe573         | TDS      | 2974   | Response (Not last buffer)                                                    |
| 4823                         | 29.997246600 | 0.000248300 | 0.000248300    | 22      | client-1  | DB-SERVER   | 128 | 0x264e         | TCP      | 60     | 60612 → 1433 [ACK] Seq=16555 Ack=39001 Win=65280 Len=0                        |
| 4824                         | 29.997249500 | 0.000002900 | 0.000002900    | 22      | DB-SERVER | client-1    | 128 | 0xe576         | TCP      | 1514   | 1433 → 60612 [ACK] Seq=40461 Ack=16555 Win=2102272 Len=1460 [TCP PDU reassemb |
| 4825                         | 29.997481400 | 0.000231900 | 0.000231900    | 22      | client-1  | DB-SERVER   | 128 | 0x264f         | TCP      | 60     | 60612 → 1433 [ACK] Seq=16555 Ack=41921 Win=65280 Len=0                        |
| 4826                         | 29.997483500 | 0.000002100 | 0.000002100    | 22      | DB-SERVER | client-1    | 128 | 0xe577         | TDS      | 2974   | Response (Not last buffer)                                                    |
| 4827                         | 29.997550100 | 0.000066600 | 0.000066600    | 22      | client-1  | DB-SERVER   | 128 | 0x2650         | SMP      | 70     | SID: 0, Ack                                                                   |
| 4828                         | 29.997740700 | 0.000190600 | 0.000190600    | 22      | client-1  | DB-SERVER   | 128 | 0x2651         | TCP      | 60     | 60612 → 1433 [ACK] Seq=16571 Ack=44841 Win=65280 Len=0                        |
| 4829                         | 29.997740700 | 0.000000000 | 0.000000000    | 22      | client-1  | DB-SERVER   | 128 | 0x2652         | SMP      | 70     | SID: 1, Syn                                                                   |

|      |              |             |             |    |           |           |
|------|--------------|-------------|-------------|----|-----------|-----------|
| 4799 | 29.920017300 | 0.001182100 | 0.001182100 | 22 | client-1  | DB-SERVER |
| 4800 | 29.920095000 | 0.000077700 | 0.000077700 | 22 | DB-SERVER | client-1  |
| 4803 | 29.939304000 | 0.019209000 | 0.019209000 | 22 | DB-SERVER | client-1  |
| 4804 | 29.939712400 | 0.000408400 | 0.000408400 | 22 | client-1  | DB-SERVER |
| 4815 | 29.975532900 | 0.035820500 | 0.035820500 | 22 | client-1  | DB-SERVER |
| 4816 | 29.976143500 | 0.000610600 | 0.000610600 | 22 | DB-SERVER | client-1  |
| 4818 | 29.996151700 | 0.020008200 | 0.020008200 | 22 | DB-SERVER | client-1  |
| 4819 | 29.996718300 | 0.000566600 | 0.000566600 | 22 | client-1  | DB-SERVER |
| 4820 | 29.996724000 | 0.000005700 | 0.000005700 | 22 | DB-SERVER | client-1  |
| 4821 | 29.996995400 | 0.000271400 | 0.000271400 | 22 | client-1  | DB-SERVER |

|                                                                               |
|-------------------------------------------------------------------------------|
| Response                                                                      |
| [TCP Retransmission] 1433 → 60612 [PSH, ACK] Seq=32738 Ack=15443 Win=2100992  |
| 60612 → 1433 [ACK] Seq=15443 Ack=33161 Win=65280 Len=0 SLE=32738 SRE=33161    |
| SQL batch                                                                     |
| 1433 → 60612 [ACK] Seq=33161 Ack=16555 Win=2102272 Len=1460 [TCP PDU reassemb |
| [TCP Retransmission] 1433 → 60612 [ACK] Seq=33161 Ack=16555 Win=2102272 Len=  |
| 60612 → 1433 [ACK] Seq=16555 Ack=34621 Win=65280 Len=0 SLE=33161 SRE=34621    |
| Response (Not last buffer)                                                    |



# Windows TCP Template "Datacenter"



```
PS C:\Windows\system32> Get-NetTCPSetting -SettingName Datacenter

SettingName      : Datacenter
MinRto(ms)       : 20
InitialCongestionWindow(MSS) : 10
CongestionProvider : DCTCP
CwndRestart      : True
DelayedAckTimeout(ms) : 10
DelayedAckFrequency : 2
MemoryPressureProtection : Enabled
AutoTuningLevelLocal : Normal
AutoTuningLevelGroupPolicy : NotConfigured
AutoTuningLevelEffective : Local
EcnCapability     : Enabled
Timestamps       : Disabled
InitialRto(ms)   : 3000
ScalingHeuristics : Disabled
DynamicPortRangeStartPort : 49152
DynamicPortRangeNumberOfPorts : 16384
AutomaticUseCustom : Disabled
NonSackRttResiliency : Disabled
ForceWS          : Disabled
MaxSynRetransmissions : 2
AutoReusePortRangeStartPort : 0
AutoReusePortRangeNumberOfPorts : 0

PS C:\Windows\system32> |
```



*Topic starter:*

It seems to be a general performance issue within the application. Everything works as it should locally on the server. The clients however take much longer.

For example, generating 1 specific report takes 16 seconds to generate on the client. While on the server this same report takes 6 seconds.

| Time          |                     |
|---------------|---------------------|
| First packet: | 2026-04-27 14:55:05 |
| Last packet:  | 2026-04-27 14:56:41 |
| Elapsed:      | 00:01:35 ????       |



# Use markers...



Me:

Could you make a new pcap where you generate that 1 specific report and mark the start of generating the report by sending a 1-packet ping from the client to the server just before initiating the report generation and again sending a 1-packet ping just after the report generation is complete?

That way we can zoom in on what is involved in the 16 seconds.

| icmp.type in {8,0} |              |              |           |             |     |                |          |        |                     |                                                      |
|--------------------|--------------|--------------|-----------|-------------|-----|----------------|----------|--------|---------------------|------------------------------------------------------|
| No.                | Relative     | Delta        | Source    | Destination | TTL | Identification | Protocol | Length | Info                |                                                      |
| 8953               | 52.769925300 |              | client-2  | DB-SERVER   | 128 | 0xecee         | ICMP     | 74     | Echo (ping) request | id=0x0001, seq=114/29184, ttl=128 (reply in 8954)    |
| 8954               | 52.769960200 | 0.000034900  | DB-SERVER | client-2    | 128 | 0x71ac         | ICMP     | 74     | Echo (ping) reply   | id=0x0001, seq=114/29184, ttl=128 (request in 8953)  |
| 9061               | 53.785456900 | 1.015496700  | client-2  | DB-SERVER   | 128 | 0xecef         | ICMP     | 74     | Echo (ping) request | id=0x0001, seq=115/29440, ttl=128 (reply in 9062)    |
| 9062               | 53.785494300 | 0.000037400  | DB-SERVER | client-2    | 128 | 0x71ad         | ICMP     | 74     | Echo (ping) reply   | id=0x0001, seq=115/29440, ttl=128 (request in 9061)  |
| 9150               | 54.802492500 | 1.016998200  | client-2  | DB-SERVER   | 128 | 0xecf0         | ICMP     | 74     | Echo (ping) request | id=0x0001, seq=116/29696, ttl=128 (reply in 9151)    |
| 9151               | 54.802535400 | 0.000042900  | DB-SERVER | client-2    | 128 | 0x71ae         | ICMP     | 74     | Echo (ping) reply   | id=0x0001, seq=116/29696, ttl=128 (request in 9150)  |
| 9269               | 55.816674500 | 1.014130100  | client-2  | DB-SERVER   | 128 | 0xecf6         | ICMP     | 74     | Echo (ping) request | id=0x0001, seq=117/29952, ttl=128 (reply in 9270)    |
| 9270               | 55.816714200 | 0.000039700  | DB-SERVER | client-2    | 128 | 0x71b6         | ICMP     | 74     | Echo (ping) reply   | id=0x0001, seq=117/29952, ttl=128 (request in 9269)  |
| 18959              | 78.565415100 | 22.748700900 | client-2  | DB-SERVER   | 128 | 0xfa72         | ICMP     | 74     | Echo (ping) request | id=0x0001, seq=118/30208, ttl=128 (reply in 18960)   |
| 18960              | 78.565447800 | 0.000032700  | DB-SERVER | client-2    | 128 | 0x801f         | ICMP     | 74     | Echo (ping) reply   | id=0x0001, seq=118/30208, ttl=128 (request in 18959) |
| 19024              | 79.575540500 | 1.010092700  | client-2  | DB-SERVER   | 128 | 0xfa77         | ICMP     | 74     | Echo (ping) request | id=0x0001, seq=119/30464, ttl=128 (reply in 19025)   |
| 19025              | 79.575587500 | 0.000047000  | DB-SERVER | client-2    | 128 | 0x8024         | ICMP     | 74     | Echo (ping) reply   | id=0x0001, seq=119/30464, ttl=128 (request in 19024) |
| 19151              | 80.588407300 | 1.012819800  | client-2  | DB-SERVER   | 128 | 0xfa78         | ICMP     | 74     | Echo (ping) request | id=0x0001, seq=120/30720, ttl=128 (reply in 19152)   |
| 19152              | 80.588440200 | 0.000032900  | DB-SERVER | client-2    | 128 | 0x8025         | ICMP     | 74     | Echo (ping) reply   | id=0x0001, seq=120/30720, ttl=128 (request in 19151) |
| 19265              | 81.597502800 | 1.009062600  | client-2  | DB-SERVER   | 128 | 0xfa79         | ICMP     | 74     | Echo (ping) request | id=0x0001, seq=121/30976, ttl=128 (reply in 19266)   |
| 19266              | 81.597533800 | 0.000031000  | DB-SERVER | client-2    | 128 | 0x8026         | ICMP     | 74     | Echo (ping) reply   | id=0x0001, seq=121/30976, ttl=128 (request in 19265) |

# Let's start digging!





# Inefficient DB programming? (credits to Josh!)



| (frame.number >= 9270) && (frame.number <= 18959) && tcp.port==1433 |   |             |             |         |           |             |     |                |          |        |                                                                                             |
|---------------------------------------------------------------------|---|-------------|-------------|---------|-----------|-------------|-----|----------------|----------|--------|---------------------------------------------------------------------------------------------|
| No.                                                                 | ^ | Relative    | Delta       | #stream | Source    | Destination | TTL | Identification | Protocol | Length | Info                                                                                        |
| 14222                                                               |   | 2.576255300 | 0.001006800 | 38      | client-2  | DB-SERVER   | 128 | 0xf533         | TCP      | 1514   | 50653 → 1433 [ACK] Seq=1012542 Ack=784866 Win=65280 Len=1460 [TCP PDU reassembled in 14223] |
| 14223                                                               |   | 2.576255300 | 0.000000000 | 38      | client-2  | DB-SERVER   | 128 | 0xf534         | TLSv1.2  | 251    | Application Data                                                                            |
| 14224                                                               |   | 2.576259500 | 0.000004200 | 38      | DB-SERVER | client-2    | 128 | 0x7a0d         | TCP      | 54     | 1433 → 50653 [ACK] Seq=784866 Ack=1014199 Win=2102272 Len=0                                 |
| 14229                                                               |   | 2.578364000 | 0.002104500 | 38      | DB-SERVER | client-2    | 128 | 0x7a0e         | TLSv1.2  | 1210   | Application Data                                                                            |
| 14230                                                               |   | 2.579107200 | 0.000743200 | 38      | client-2  | DB-SERVER   | 128 | 0xf535         | TLSv1.2  | 171    | Application Data                                                                            |
| 14231                                                               |   | 2.579278500 | 0.000171300 | 38      | DB-SERVER | client-2    | 128 | 0x7a0f         | TLSv1.2  | 141    | Application Data                                                                            |
| 14232                                                               |   | 2.579846500 | 0.000568000 | 38      | client-2  | DB-SERVER   | 128 | 0xf536         | TLSv1.2  | 171    | Application Data                                                                            |
| 14233                                                               |   | 2.579903800 | 0.000057300 | 38      | DB-SERVER | client-2    | 128 | 0x7a10         | TLSv1.2  | 172    | Application Data                                                                            |
| 14234                                                               |   | 2.581193100 | 0.001289300 | 38      | client-2  | DB-SERVER   | 128 | 0xf537         | TCP      | 1514   | 50653 → 1433 [ACK] Seq=1014433 Ack=786227 Win=64000 Len=1460 [TCP PDU reassembled in 14235] |
| 14235                                                               |   | 2.581193100 | 0.000000000 | 38      | client-2  | DB-SERVER   | 128 | 0xf538         | TLSv1.2  | 251    | Application Data                                                                            |
| 14236                                                               |   | 2.581222500 | 0.000029400 | 38      | DB-SERVER | client-2    | 128 | 0x7a11         | TCP      | 54     | 1433 → 50653 [ACK] Seq=786227 Ack=1016090 Win=2102272 Len=0                                 |
| 14237                                                               |   | 2.584238300 | 0.003015800 | 38      | DB-SERVER | client-2    | 128 | 0x7a12         | TLSv1.2  | 1210   | Application Data                                                                            |
| 14238                                                               |   | 2.585035000 | 0.000796700 | 38      | client-2  | DB-SERVER   | 128 | 0xf539         | TLSv1.2  | 171    | Application Data                                                                            |
| 14239                                                               |   | 2.585219700 | 0.000184700 | 38      | DB-SERVER | client-2    | 128 | 0x7a13         | TLSv1.2  | 141    | Application Data                                                                            |
| 14240                                                               |   | 2.585787500 | 0.000567800 | 38      | client-2  | DB-SERVER   | 128 | 0xf53a         | TLSv1.2  | 171    | Application Data                                                                            |
| 14241                                                               |   | 2.585858300 | 0.000070800 | 38      | DB-SERVER | client-2    | 128 | 0x7a14         | TLSv1.2  | 172    | Application Data                                                                            |
| 14242                                                               |   | 2.587415800 | 0.001557500 | 38      | client-2  | DB-SERVER   | 128 | 0xf53b         | TCP      | 1514   | 50653 → 1433 [ACK] Seq=1016324 Ack=787588 Win=65280 Len=1460 [TCP PDU reassembled in 14243] |
| 14243                                                               |   | 2.587415800 | 0.000000000 | 38      | client-2  | DB-SERVER   | 128 | 0xf53c         | TLSv1.2  | 251    | Application Data                                                                            |
| 14244                                                               |   | 2.587423500 | 0.000007700 | 38      | DB-SERVER | client-2    | 128 | 0x7a15         | TCP      | 54     | 1433 → 50653 [ACK] Seq=787588 Ack=1017981 Win=2102272 Len=0                                 |
| 14251                                                               |   | 2.589909000 | 0.002485500 | 38      | DB-SERVER | client-2    | 128 | 0x7a16         | TLSv1.2  | 1210   | Application Data                                                                            |
| 14252                                                               |   | 2.590672900 | 0.000763900 | 38      | client-2  | DB-SERVER   | 128 | 0xf53d         | TLSv1.2  | 171    | Application Data                                                                            |
| 14254                                                               |   | 2.590838500 | 0.000165600 | 38      | DB-SERVER | client-2    | 128 | 0x7a17         | TLSv1.2  | 141    | Application Data                                                                            |
| 14255                                                               |   | 2.591414300 | 0.000575800 | 38      | client-2  | DB-SERVER   | 128 | 0xf53e         | TLSv1.2  | 171    | Application Data                                                                            |
| 14256                                                               |   | 2.591479900 | 0.000065600 | 38      | DB-SERVER | client-2    | 128 | 0x7a18         | TLSv1.2  | 172    | Application Data                                                                            |
| 14257                                                               |   | 2.592606500 | 0.001126600 | 38      | client-2  | DB-SERVER   | 128 | 0xf53f         | TCP      | 1514   | 50653 → 1433 [ACK] Seq=1018215 Ack=788949 Win=65280 Len=1460 [TCP PDU reassembled in 14258] |
| 14258                                                               |   | 2.592606500 | 0.000000000 | 38      | client-2  | DB-SERVER   | 128 | 0xf540         | TLSv1.2  | 251    | Application Data                                                                            |
| 14259                                                               |   | 2.592612900 | 0.000006400 | 38      | DB-SERVER | client-2    | 128 | 0x7a19         | TCP      | 54     | 1433 → 50653 [ACK] Seq=788949 Ack=1019872 Win=2102272 Len=0                                 |
| 14260                                                               |   | 2.594815300 | 0.002202400 | 38      | DB-SERVER | client-2    | 128 | 0x7a1a         | TLSv1.2  | 1210   | Application Data                                                                            |
| 14261                                                               |   | 2.595538400 | 0.000723100 | 38      | client-2  | DB-SERVER   | 128 | 0xf541         | TLSv1.2  | 171    | Application Data                                                                            |
| 14262                                                               |   | 2.595658000 | 0.000119600 | 38      | DB-SERVER | client-2    | 128 | 0x7a1b         | TLSv1.2  | 141    | Application Data                                                                            |
| 14263                                                               |   | 2.596193500 | 0.000535500 | 38      | client-2  | DB-SERVER   | 128 | 0xf542         | TLSv1.2  | 171    | Application Data                                                                            |
| 14264                                                               |   | 2.596251300 | 0.000057800 | 38      | DB-SERVER | client-2    | 128 | 0x7a1c         | TLSv1.2  | 172    | Application Data                                                                            |
| 14265                                                               |   | 2.597337900 | 0.001086600 | 38      | client-2  | DB-SERVER   | 128 | 0xf543         | TCP      | 1514   | 50653 → 1433 [ACK] Seq=1020106 Ack=790310 Win=64000 Len=1460 [TCP PDU reassembled in 14266] |
| 14266                                                               |   | 2.597348500 | 0.000010600 | 38      | client-2  | DB-SERVER   | 128 | 0xf544         | TLSv1.2  | 251    | Application Data                                                                            |
| 14267                                                               |   | 2.597351100 | 0.000002600 | 38      | DB-SERVER | client-2    | 128 | 0x7a1d         | TCP      | 54     | 1433 → 50653 [ACK] Seq=790310 Ack=1021763 Win=2102272 Len=0                                 |
| 14268                                                               |   | 2.599589300 | 0.002238200 | 38      | DB-SERVER | client-2    | 128 | 0x7a1e         | TLSv1.2  | 1210   | Application Data                                                                            |
| 14269                                                               |   | 2.600391500 | 0.000802200 | 38      | client-2  | DB-SERVER   | 128 | 0xf545         | TLSv1.2  | 171    | Application Data                                                                            |
| 14270                                                               |   | 2.600536700 | 0.000145200 | 38      | DB-SERVER | client-2    | 128 | 0x7a1f         | TLSv1.2  | 141    | Application Data                                                                            |
| 14271                                                               |   | 2.601253400 | 0.000716700 | 38      | client-2  | DB-SERVER   | 128 | 0xf546         | TLSv1.2  | 171    | Application Data                                                                            |
| 14272                                                               |   | 2.601311700 | 0.000058300 | 38      | DB-SERVER | client-2    | 128 | 0x7a20         | TLSv1.2  | 172    | Application Data                                                                            |



# Yes, but only partly responsible...



| (frame.number >= 9270) && (frame.number <= 18959) && tcp.stream==38 and frame.len==251 |   |             |             |         |          |             |            |                |          |                  |                  |
|----------------------------------------------------------------------------------------|---|-------------|-------------|---------|----------|-------------|------------|----------------|----------|------------------|------------------|
| No.                                                                                    | ^ | Relative    | Delta       | #stream | Source   | Destination | TTL        | Identification | Protocol | Length           | Info             |
| 9788                                                                                   |   | *REF*       |             | *REF*   | 38       | client-2    | DB-SERVER  | 128 0xed39     | TLSv1.2  | 251              | Application Data |
| 9796                                                                                   |   | 0.004343100 | 0.004343100 | 38      | client-2 | DB-SERVER   | 128 0xed3d | TLSv1.2        | 251      | Application Data |                  |
| 9806                                                                                   |   | 0.008325000 | 0.003981900 | 38      | client-2 | DB-SERVER   | 128 0xed41 | TLSv1.2        | 251      | Application Data |                  |
| 9814                                                                                   |   | 0.012415900 | 0.004090900 | 38      | client-2 | DB-SERVER   | 128 0xed45 | TLSv1.2        | 251      | Application Data |                  |
| 9822                                                                                   |   | 0.016511900 | 0.004096000 | 38      | client-2 | DB-SERVER   | 128 0xed49 | TLSv1.2        | 251      | Application Data |                  |
| 9830                                                                                   |   | 0.020702000 | 0.004190100 | 38      | client-2 | DB-SERVER   | 128 0xed4d | TLSv1.2        | 251      | Application Data |                  |
| 9838                                                                                   |   | 0.024816300 | 0.004114300 | 38      | client-2 | DB-SERVER   | 128 0xed51 | TLSv1.2        | 251      | Application Data |                  |
| 9846                                                                                   |   | 0.028969900 | 0.004153600 | 38      | client-2 | DB-SERVER   | 128 0xed55 | TLSv1.2        | 251      | Application Data |                  |
| 9854                                                                                   |   | 0.033181100 | 0.004211200 | 38      | client-2 | DB-SERVER   | 128 0xed59 | TLSv1.2        | 251      | Application Data |                  |
| 9862                                                                                   |   | 0.037665400 | 0.004484300 | 38      | client-2 | DB-SERVER   | 128 0xed5d | TLSv1.2        | 251      | Application Data |                  |
| 9870                                                                                   |   | 0.042001100 | 0.004335700 | 38      | client-2 | DB-SERVER   | 128 0xed61 | TLSv1.2        | 251      | Application Data |                  |
| 9878                                                                                   |   | 0.047600300 | 0.005599200 | 38      | client-2 | DB-SERVER   | 128 0xed65 | TLSv1.2        | 251      | Application Data |                  |
| 9886                                                                                   |   | 0.052259700 | 0.004659400 | 38      | client-2 | DB-SERVER   | 128 0xed69 | TLSv1.2        | 251      | Application Data |                  |
| 9901                                                                                   |   | 0.056733300 | 0.004473600 | 38      | client-2 | DB-SERVER   | 128 0xed6d | TLSv1.2        | 251      | Application Data |                  |

| Statistics             |          |               |        |
|------------------------|----------|---------------|--------|
| Measurement            | Captured | Displayed     | Marked |
| Packets                | 19392    | 693 (3.6%)    | —      |
| Time span, s           | 84.092   | 3.526         | —      |
| Average pps            | 230.6    | 196.6         | —      |
| Average packet size, B | 510      | 251           | —      |
| Bytes                  | 9894625  | 173943 (1.8%) | 0      |
| Average bytes/s        | 117 k    | 49 k          | —      |
| Average bits/s         | 941 k    | 394 k         | —      |



# Let's dig deeper!





# Hmmm... more connections is more better???



| (frame.number >= 9270) && (frame.number <= 18959) && tcp.port==1433 && tcp.flags & 18 == 2 |              |             |         |          |             |     |                |          |        |              |       |       |           |       |          |        |           |  |
|--------------------------------------------------------------------------------------------|--------------|-------------|---------|----------|-------------|-----|----------------|----------|--------|--------------|-------|-------|-----------|-------|----------|--------|-----------|--|
| No.                                                                                        | Relative     | Delta       | #stream | Source   | Destination | TTL | Identification | Protocol | Length | Info         |       |       |           |       |          |        |           |  |
| 9409                                                                                       | 56.272288600 |             | 44      | client-2 | DB-SERVER   | 128 | 0xed03         | TCP      | 66     | 50658 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 9498                                                                                       | 56.711127500 | 0.438838900 | 45      | client-2 | DB-SERVER   | 128 | 0xed0e         | TCP      | 66     | 50659 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 16105                                                                                      | 64.817078700 | 8.105951200 | 46      | client-2 | DB-SERVER   | 128 | 0xf82d         | TCP      | 66     | 50663 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 16179                                                                                      | 65.251007600 | 0.433928900 | 47      | client-2 | DB-SERVER   | 128 | 0xf837         | TCP      | 66     | 50665 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 16288                                                                                      | 65.697493200 | 0.446485600 | 48      | client-2 | DB-SERVER   | 128 | 0xf844         | TCP      | 66     | 50666 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 16410                                                                                      | 66.129598900 | 0.432105700 | 49      | client-2 | DB-SERVER   | 128 | 0xf84e         | TCP      | 66     | 50667 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 16504                                                                                      | 66.561788900 | 0.432190000 | 50      | client-2 | DB-SERVER   | 128 | 0xf85d         | TCP      | 66     | 50668 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 16596                                                                                      | 66.993373800 | 0.431584900 | 51      | client-2 | DB-SERVER   | 128 | 0xf86e         | TCP      | 66     | 50669 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 16661                                                                                      | 67.428055600 | 0.434681800 | 52      | client-2 | DB-SERVER   | 128 | 0xf878         | TCP      | 66     | 50670 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 16743                                                                                      | 67.864476000 | 0.436420400 | 53      | client-2 | DB-SERVER   | 128 | 0xf887         | TCP      | 66     | 50671 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 16830                                                                                      | 68.298073500 | 0.433597500 | 54      | client-2 | DB-SERVER   | 128 | 0xf891         | TCP      | 66     | 50672 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 16906                                                                                      | 68.730448400 | 0.432374900 | 55      | client-2 | DB-SERVER   | 128 | 0xf89e         | TCP      | 66     | 50673 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 16975                                                                                      | 69.166195900 | 0.435747500 | 56      | client-2 | DB-SERVER   | 128 | 0xf8a8         | TCP      | 66     | 50674 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 17066                                                                                      | 69.599248000 | 0.433052100 | 57      | client-2 | DB-SERVER   | 128 | 0xf8ba         | TCP      | 66     | 50675 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 17228                                                                                      | 70.277426400 | 0.678178400 | 58      | client-2 | DB-SERVER   | 128 | 0xf8e9         | TCP      | 66     | 50676 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 17786                                                                                      | 71.410802900 | 1.133376500 | 59      | client-2 | DB-SERVER   | 128 | 0xf9a5         | TCP      | 66     | 50677 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 17845                                                                                      | 71.849243000 | 0.438440100 | 60      | client-2 | DB-SERVER   | 128 | 0xf9af         | TCP      | 66     | 50678 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 17932                                                                                      | 72.282258400 | 0.433015400 | 61      | client-2 | DB-SERVER   | 128 | 0xf9c0         | TCP      | 66     | 50679 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 17998                                                                                      | 72.717444200 | 0.435185800 | 62      | client-2 | DB-SERVER   | 128 | 0xf9ca         | TCP      | 66     | 50680 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 18074                                                                                      | 73.159650200 | 0.442206000 | 63      | client-2 | DB-SERVER   | 128 | 0xf9dc         | TCP      | 66     | 50681 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 18239                                                                                      | 73.791229000 | 0.631578800 | 64      | client-2 | DB-SERVER   | 128 | 0xfa0c         | TCP      | 66     | 50682 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 18307                                                                                      | 74.227678000 | 0.436449000 | 65      | client-2 | DB-SERVER   | 128 | 0xfa16         | TCP      | 66     | 50683 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 18374                                                                                      | 74.662390100 | 0.434712100 | 66      | client-2 | DB-SERVER   | 128 | 0xfa23         | TCP      | 66     | 50684 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 18484                                                                                      | 75.097093200 | 0.434703100 | 67      | client-2 | DB-SERVER   | 128 | 0xfa2d         | TCP      | 66     | 50685 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |
| 18564                                                                                      | 75.532323600 | 0.435230400 | 68      | client-2 | DB-SERVER   | 128 | 0xfa3f         | TCP      | 66     | 50686 → 1433 | [SYN] | Seq=0 | Win=65535 | Len=0 | MSS=1460 | WS=256 | SACK_PERM |  |



# Where does the ~400 ms delay come from?



| (frame.number >= 9409) && (frame.number <= 9498) && tcp.port==1433 |              |             |         |           |             |     |                |          |        |                                                                |
|--------------------------------------------------------------------|--------------|-------------|---------|-----------|-------------|-----|----------------|----------|--------|----------------------------------------------------------------|
| No.                                                                | Relative     | Delta       | #stream | Source    | Destination | TTL | Identification | Protocol | Length | Info                                                           |
| 9409                                                               | 56.272288600 |             | 44      | client-2  | DB-SERVER   | 128 | 0xed03         | TCP      | 66     | 50658 → 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_ |
| 9410                                                               | 56.272311900 | 0.000023300 | 44      | DB-SERVER | client-2    | 128 | 0x71c6         | TCP      | 66     | 1433 → 50658 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 W |
| 9411                                                               | 56.272886500 | 0.000574600 | 44      | client-2  | DB-SERVER   | 128 | 0xed04         | TCP      | 60     | 50658 → 1433 [ACK] Seq=1 Ack=1 Win=65280 Len=0                 |
| 9412                                                               | 56.273010700 | 0.000124200 | 21      | DB-SERVER | client-2    | 128 | 0x71c7         | TCP      | 55     | [TCP Keep-Alive] 1433 → 50625 [ACK] Seq=108264 Ack=53099 Win=2 |
| 9413                                                               | 56.273276600 | 0.000265900 | 44      | client-2  | DB-SERVER   | 128 | 0xed05         | TDS      | 142    | TDS7 pre-login message                                         |
| 9414                                                               | 56.273302000 | 0.000025400 | 44      | DB-SERVER | client-2    | 128 | 0x71c8         | TDS      | 102    | Response                                                       |
| 9415                                                               | 56.273510500 | 0.000208500 | 21      | client-2  | DB-SERVER   | 128 | 0xed06         | TCP      | 66     | [TCP Keep-Alive ACK] 50625 → 1433 [ACK] Seq=53099 Ack=108265 W |
| 9416                                                               | 56.274548700 | 0.001038200 | 44      | client-2  | DB-SERVER   | 128 | 0xed07         | TLSv1.2  | 269    | Client Hello (SNI=serv2)                                       |
| 9417                                                               | 56.274682500 | 0.000133800 | 44      | DB-SERVER | client-2    | 128 | 0x71c9         | TLSv1.2  | 203    | Server Hello, Change Cipher Spec, Encrypted Handshake Message  |
| 9418                                                               | 56.276160400 | 0.001477900 | 44      | client-2  | DB-SERVER   | 128 | 0xed08         | TLSv1.2  | 113    | Change Cipher Spec, Encrypted Handshake Message                |
| 9419                                                               | 56.276491600 | 0.000331200 | 44      | client-2  | DB-SERVER   | 128 | 0xed09         | TLSv1.2  | 432    | Application Data                                               |
| 9420                                                               | 56.276495300 | 0.000003700 | 44      | DB-SERVER | client-2    | 128 | 0x71ca         | TCP      | 54     | 1433 → 50658 [ACK] Seq=198 Ack=741 Win=2101504 Len=0           |
| 9421                                                               | 56.277152900 | 0.000657600 | 44      | DB-SERVER | client-2    | 128 | 0x71cb         | TLSv1.2  | 524    | Application Data                                               |
| 9422                                                               | 56.278632600 | 0.001479700 | 44      | client-2  | DB-SERVER   | 128 | 0xed0a         | TLSv1.2  | 99     | Application Data                                               |
| 9423                                                               | 56.278963600 | 0.000331000 | 44      | client-2  | DB-SERVER   | 128 | 0xed0b         | TLSv1.2  | 177    | Application Data                                               |
| 9424                                                               | 56.278966500 | 0.000002900 | 44      | DB-SERVER | client-2    | 128 | 0x71cc         | TCP      | 54     | 1433 → 50658 [ACK] Seq=668 Ack=909 Win=2101504 Len=0           |
| 9425                                                               | 56.279265600 | 0.000299100 | 44      | DB-SERVER | client-2    | 128 | 0x71cd         | TLSv1.2  | 256    | Application Data                                               |
| 9426                                                               | 56.280255700 | 0.000990100 | 44      | client-2  | DB-SERVER   | 128 | 0xed0c         | TLSv1.2  | 257    | Application Data                                               |
| 9427                                                               | 56.280469700 | 0.000214000 | 44      | DB-SERVER | client-2    | 128 | 0x71ce         | TLSv1.2  | 601    | Application Data                                               |
| 9442                                                               | 56.300941200 | 0.020471500 | 44      | DB-SERVER | client-2    | 128 | 0x71cf         | TCP      | 601    | [TCP Retransmission] 1433 → 50658 [PSH, ACK] Seq=870 Ack=1112  |
| 9443                                                               | 56.301473200 | 0.000532000 | 44      | client-2  | DB-SERVER   | 128 | 0xed0d         | TCP      | 66     | 50658 → 1433 [ACK] Seq=1112 Ack=1417 Win=64000 Len=0 SLE=870 S |
| 9498                                                               | 56.711127500 | 0.409654300 | 45      | client-2  | DB-SERVER   | 128 | 0xed0e         | TCP      | 66     | 50659 → 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_ |



# Oh no... not again!

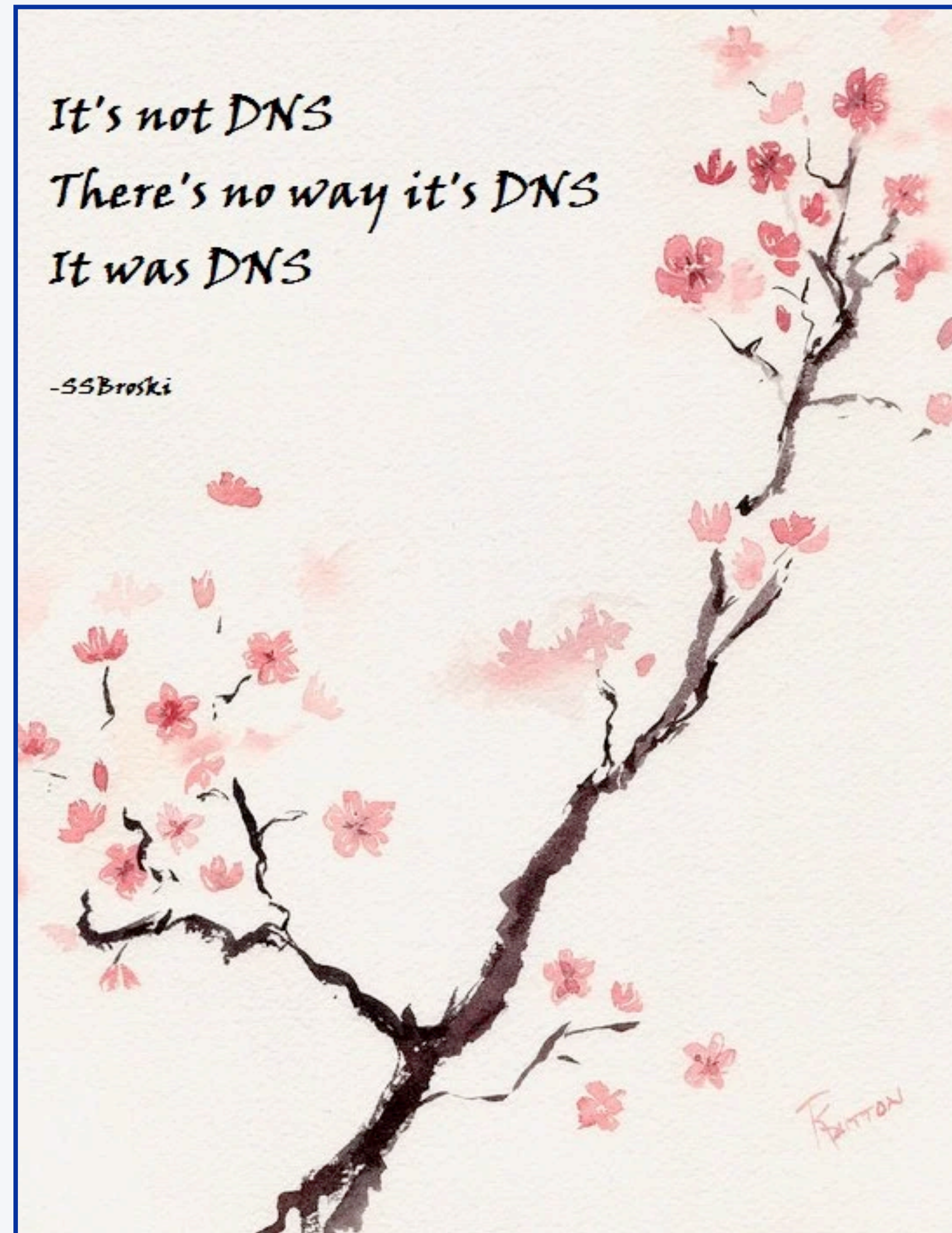


(frame.number >= 9270) && (frame.number <= 18959) && ip.host=="client-2" and ((tcp.port==1433 && tcp.flags & 18 == 2) or mdns or llmnr)

| No.   | Relative     | Delta       | #stream | Source    | Destination | TTL | Protocol | Length | Info                                                               |
|-------|--------------|-------------|---------|-----------|-------------|-----|----------|--------|--------------------------------------------------------------------|
| 16122 | 64.831788700 | 0.014710000 | 88      | client-2  | 224.0.0.251 | 1   | MDNS     | 71     | Standard query 0x0000 A serv2.local, "QM" question                 |
| 16125 | 64.832117800 | 0.000329100 | 88      | client-2  | 224.0.0.251 | 1   | MDNS     | 71     | Standard query 0x0000 AAAA serv2.local, "QU" question              |
| 16171 | 65.245762600 | 0.413644800 | 88      | client-2  | 224.0.0.251 | 1   | MDNS     | 71     | Standard query 0x0000 AAAA serv2.local, "QM" question              |
| 16174 | 65.247545500 | 0.001782900 | 165     | client-2  | 224.0.0.252 | 1   | LLMNR    | 65     | Standard query 0xdefa A serv2                                      |
| 16175 | 65.247602100 | 0.000056600 | 166     | DB-SERVER | client-2    | 128 | LLMNR    | 86     | Standard query response 0xdefa A serv2 A : x.y.z.250               |
| 16177 | 65.248959300 | 0.001357200 | 750     | client-2  | 224.0.0.252 | 1   | LLMNR    | 65     | Standard query 0x5b19 AAAA serv2                                   |
| 16178 | 65.249031100 | 0.000071800 | 751     | DB-SERVER | client-2    | 128 | LLMNR    | 110    | Standard query response 0x5b19 AAAA serv2 SOA serv2                |
| 16179 | 65.251007600 | 0.001976500 | 47      | client-2  | DB-SERVER   | 128 | TCP      | 66     | 50665 → 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 16202 | 65.272554400 | 0.021546800 | 88      | client-2  | 224.0.0.251 | 1   | MDNS     | 71     | Standard query 0x0000 A serv2.local, "QM" question                 |
| 16205 | 65.272705500 | 0.000151100 | 88      | client-2  | 224.0.0.251 | 1   | MDNS     | 71     | Standard query 0x0000 AAAA serv2.local, "QU" question              |
| 16279 | 65.692962700 | 0.420257200 | 88      | client-2  | 224.0.0.251 | 1   | MDNS     | 71     | Standard query 0x0000 AAAA serv2.local, "QM" question              |
| 16283 | 65.694856400 | 0.001893700 | 769     | client-2  | 224.0.0.252 | 1   | LLMNR    | 65     | Standard query 0x9404 A serv2                                      |
| 16284 | 65.694948200 | 0.000091800 | 770     | DB-SERVER | client-2    | 128 | LLMNR    | 86     | Standard query response 0x9404 A serv2 A : x.y.z.250               |
| 16286 | 65.695906000 | 0.000957800 | 772     | client-2  | 224.0.0.252 | 1   | LLMNR    | 65     | Standard query 0xddee AAAA serv2                                   |
| 16287 | 65.695961400 | 0.000055400 | 773     | DB-SERVER | client-2    | 128 | LLMNR    | 110    | Standard query response 0xddee AAAA serv2 SOA serv2                |
| 16288 | 65.697493200 | 0.001531800 | 48      | client-2  | DB-SERVER   | 128 | TCP      | 66     | 50666 → 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 16305 | 65.712108200 | 0.014615000 | 88      | client-2  | 224.0.0.251 | 1   | MDNS     | 71     | Standard query 0x0000 A serv2.local, "QM" question                 |
| 16308 | 65.712290100 | 0.000181900 | 88      | client-2  | 224.0.0.251 | 1   | MDNS     | 71     | Standard query 0x0000 AAAA serv2.local, "QU" question              |
| 16402 | 66.126108000 | 0.413817900 | 88      | client-2  | 224.0.0.251 | 1   | MDNS     | 71     | Standard query 0x0000 AAAA serv2.local, "QM" question              |
| 16405 | 66.127088500 | 0.000980500 | 777     | client-2  | 224.0.0.252 | 1   | LLMNR    | 65     | Standard query 0x3bbf A serv2                                      |
| 16406 | 66.127177200 | 0.000088700 | 778     | DB-SERVER | client-2    | 128 | LLMNR    | 86     | Standard query response 0x3bbf A serv2 A : x.y.z.250               |
| 16408 | 66.127875500 | 0.000698300 | 780     | client-2  | 224.0.0.252 | 1   | LLMNR    | 65     | Standard query 0x624c AAAA serv2                                   |
| 16409 | 66.127932300 | 0.000056800 | 781     | DB-SERVER | client-2    | 128 | LLMNR    | 110    | Standard query response 0x624c AAAA serv2 SOA serv2                |
| 16410 | 66.129598900 | 0.001666600 | 49      | client-2  | DB-SERVER   | 128 | TCP      | 66     | 50667 → 1433 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 16439 | 66.146927300 | 0.017328400 | 88      | client-2  | 224.0.0.251 | 1   | MDNS     | 71     | Standard query 0x0000 A serv2.local, "QM" question                 |



# IT IS ALWAYS DNS!!! ;-)







*Topic starter:*

That seems to have hit the nail on the head. I changed the server address from SERV2 to x.y.z.250 in ODBC.

Queries seem to be much faster from client to server.

Thank you all very much for your help. I'm not sure how our support company overlooked this for months.



# Thank you!

---

WIRESHARK

Sake Blok  
*sake.blok@SYN-bit.nl*



Sponsored by:

