SharkFest'26 Europe

Packet Stories #2



Sponsored by:
PROFITAP
DEEP NETWORK OBSERVABILITY
cPacket
TCP/IP training
endace
Record. Respond.

$ whoami

- Relational therapist for computer systems
  - Solve {application,network,performance}-issues by looking at the communication between systems
- Member Wireshark core-team since 2007
  - ... and of the Wireshark Technical Steering Committee
- Started SYN-bit in 2010
  - Application and Network troubleshooting
  - Protocol and packet analysis
  - Training (Wireshark, TCP, TLS)
- Organizer of the Wireshark Users NL meetups
- Wireshark Certified Analyst (WCA) #1 🎉





SYN-bit

deep traffic analysis

Application and network troubleshooting

Protocol and packet analysis

Training (Wireshark, TCP, SSL)

www.SYN-bit.nl

Case 1:
Slow performance when moving application to another system



Initial description on Wireshark discord #pcap-help

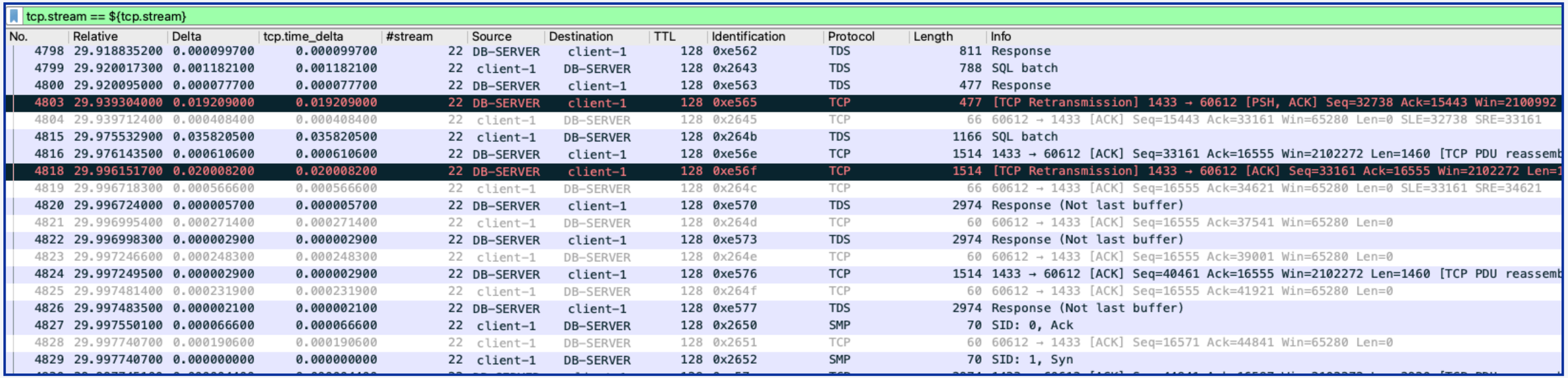
Topic starter:

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.

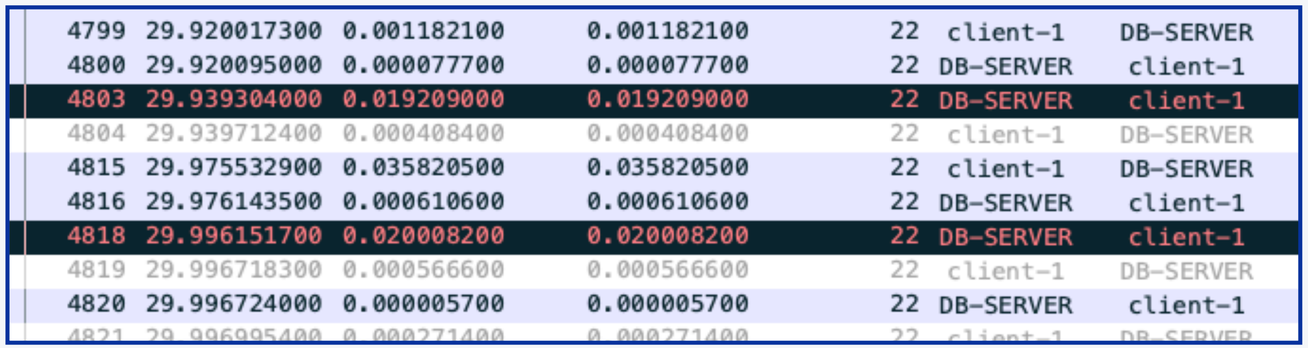


Why are there retransmissions?

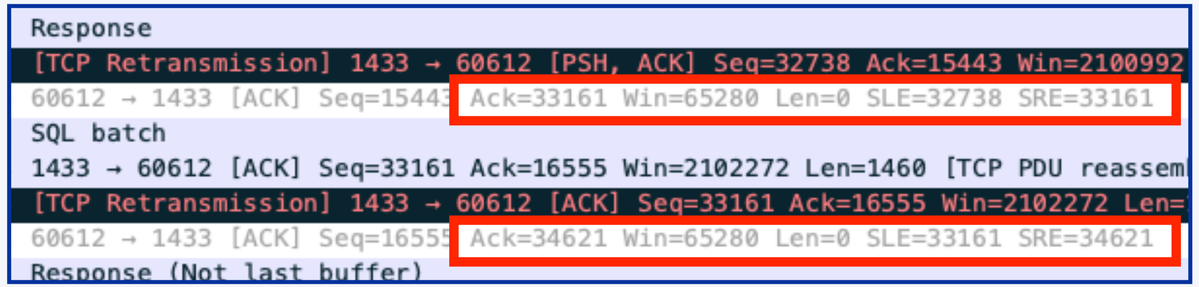


tcp.stream == ${tcp.stream}

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



```
Response
[TCP Retransmission] 1433 → 60612 [PSH, ACK] Seq=32738 Ack=15443 Win=2100992
60612 → 1433 [ACK] Seq=1544 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 reassem
[TCP Retransmission] 1433 → 60612 [ACK] Seq=33161 Ack=16555 Win=2102272 Len=
60612 → 1433 [ACK] Seq=1655 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



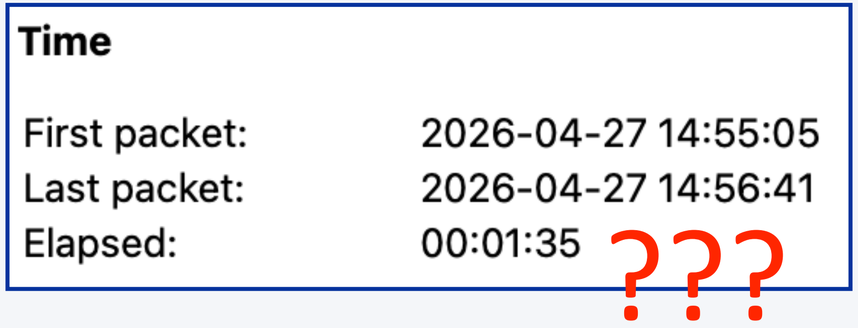
PS C:\Windows\system32>
```

Update in the description

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*.



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	1.014139100	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!



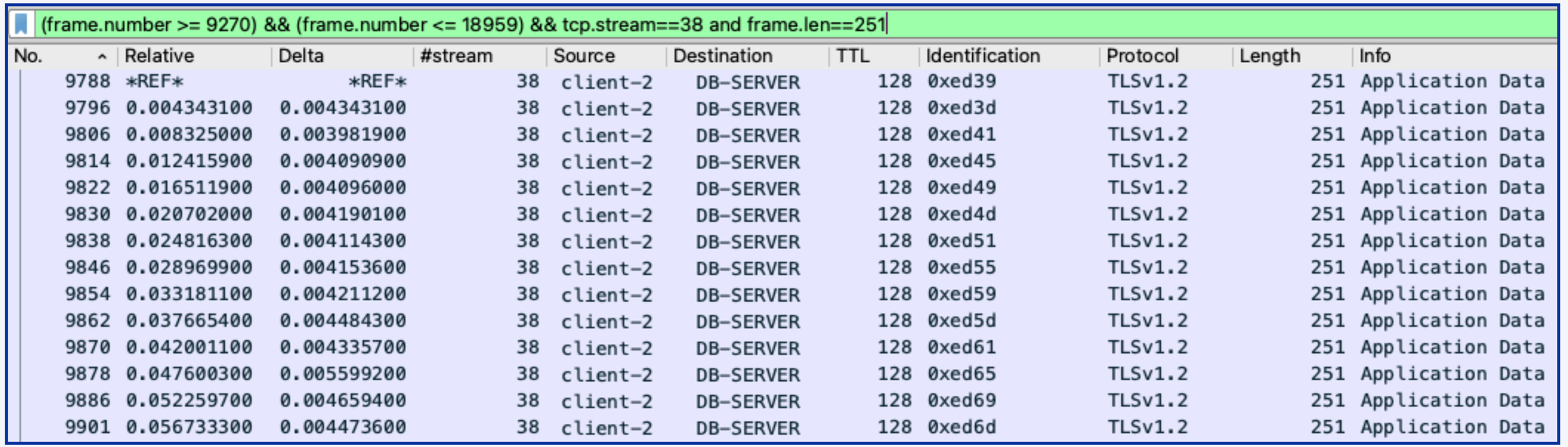
Inefficient DB programming? (credits to Josh!)



(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!



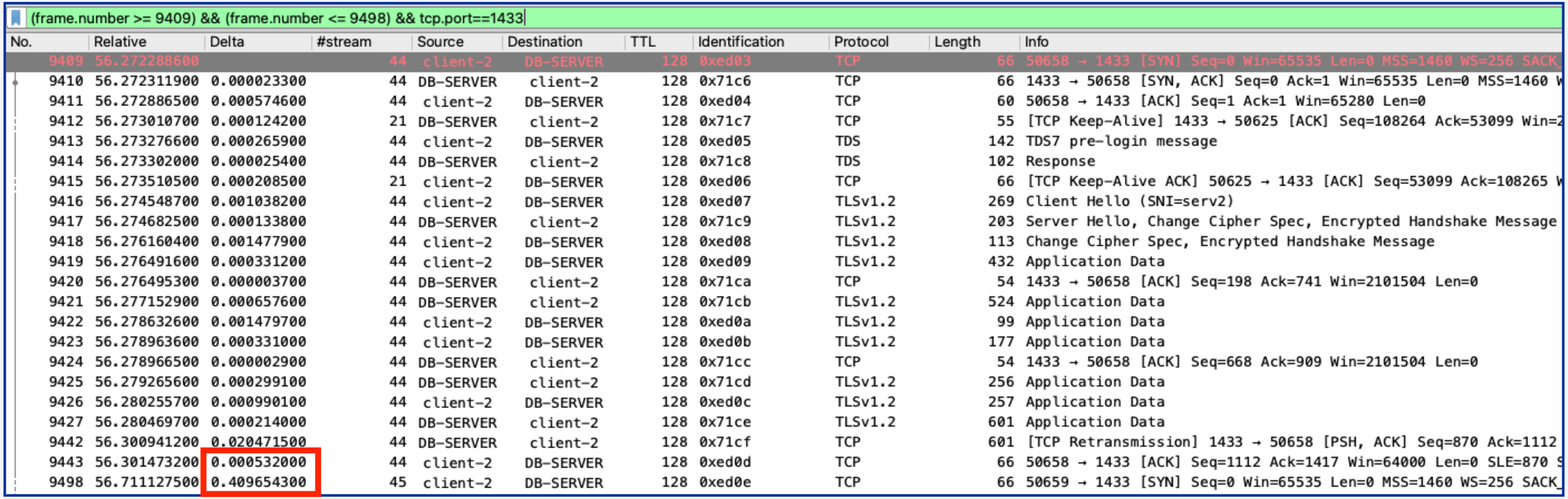
Hmmm... more connections is more better???



(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_

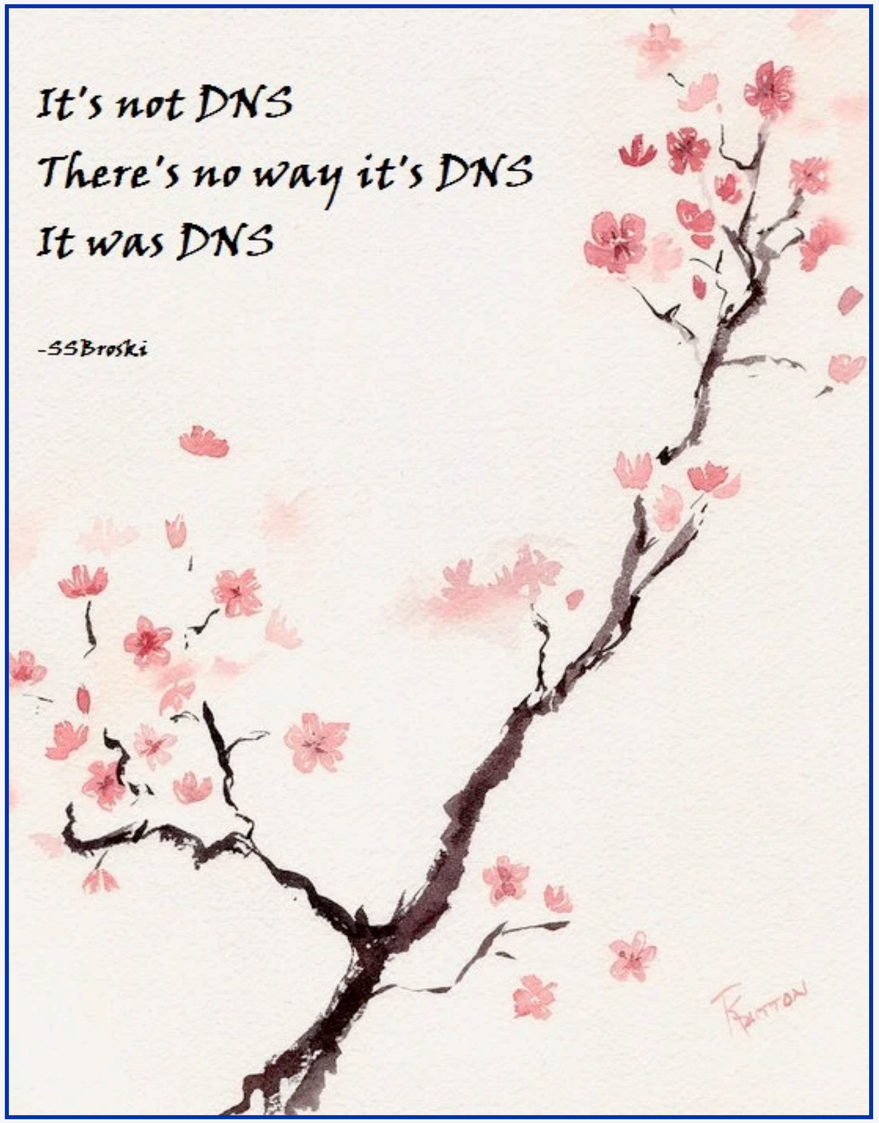
Oh no... not again!



(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!!! ;-)



Happy "customer" :-)

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.

Case 2:
Periodic login failures in some zones of the network

Intake

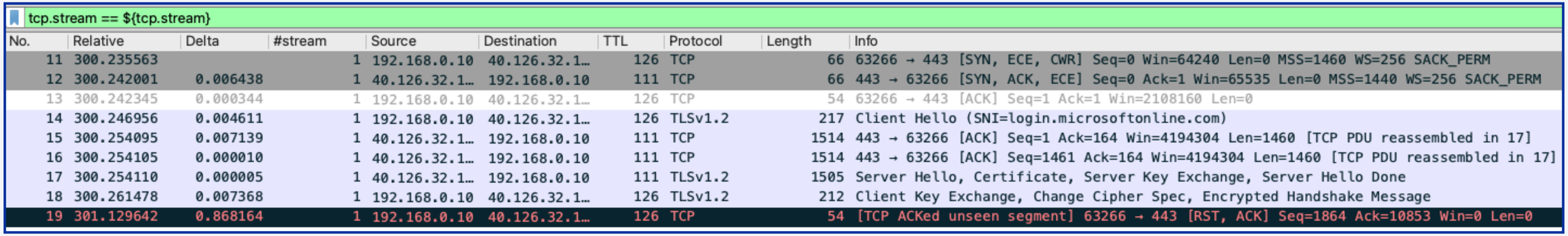


- Since 2 weeks we see daily issues
  - People can't print, printing needs authentication to Azure Entra
  - People can't log in, but logged in users have no problem
  - The network is divided into zones, not all zones have the problem
- Captures were made on the external firewall
  - 3-WHS to login.microsoftonline.com is OK, but TLS handshake fails
  - Same for other sites
- 2x 100 Gbit/s link to ISP, about 8-10 Gbit/s sustained traffic
- Proposed plan:
  - I will analyse the firewall pcaps
  - I will place a 25 Gbit/s capturing device and analyse the data

Let's look at the firewall traces...



Packet capture on the firewall...



tcp.stream == ${tcp.stream}

No.	Relative	Delta	#stream	Source	Destination	TTL	Protocol	Length	Info
11	300.235563		1	192.168.0.10	40.126.32.1…	126	TCP	66	63266 → 443 [SYN, ECE, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
12	300.242001	0.006438	1	40.126.32.1…	192.168.0.10	111	TCP	66	443 → 63266 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
13	300.242345	0.000344	1	192.168.0.10	40.126.32.1…	126	TCP	54	63266 → 443 [ACK] Seq=1 Ack=1 Win=2108160 Len=0
14	300.246956	0.004611	1	192.168.0.10	40.126.32.1…	126	TLSv1.2	217	Client Hello (SNI=login.microsoftonline.com)
15	300.254095	0.007139	1	40.126.32.1…	192.168.0.10	111	TCP	1514	443 → 63266 [ACK] Seq=1 Ack=164 Win=4194304 Len=1460 [TCP PDU reassembled in 17]
16	300.254105	0.000010	1	40.126.32.1…	192.168.0.10	111	TCP	1514	443 → 63266 [ACK] Seq=1461 Ack=164 Win=4194304 Len=1460 [TCP PDU reassembled in 17]
17	300.254110	0.000005	1	40.126.32.1…	192.168.0.10	111	TLSv1.2	1505	Server Hello, Certificate, Server Key Exchange, Server Hello Done
18	300.261478	0.007368	1	192.168.0.10	40.126.32.1…	126	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19	301.129642	0.868164	1	192.168.0.10	40.126.32.1…	126	TCP	54	[TCP ACKed unseen segment] 63266 → 443 [RST, ACK] Seq=1864 Ack=10853 Win=0 Len=0

tcp.stream == ${tcp.stream}

No.	Relative	Delta	#stream	Source	Destination	TTL	Protocol	Length	Info
367	11699.917815		40	192.168.0.10	40.126.31.73	126	TCP	66	51940 → 443 [SYN, ECE, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
368	11699.937079	0.019264	40	40.126.31.73	192.168.0.10	109	TCP	66	443 → 51940 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
369	11699.937530	0.000451	40	192.168.0.10	40.126.31.73	126	TCP	54	51940 → 443 [ACK] Seq=1 Ack=1 Win=263424 Len=0
370	11699.942410	0.004880	40	192.168.0.10	40.126.31.73	126	TLSv1.2	217	Client Hello (SNI=login.microsoftonline.com)
371	11699.963025	0.020615	40	40.126.31.73	192.168.0.10	109	TCP	1504	[TCP Previous segment not captured] 443 → 51940 [PSH, ACK] Seq=2921 Ack=164 Win=4194304 Len=1450
372	11699.963257	0.000232	40	192.168.0.10	40.126.31.73	126	TCP	66	[TCP Dup ACK 369#1] 51940 → 443 [ACK] Seq=164 Ack=1 Win=263424 Len=0 SLE=2921 SRE=4371
373	11700.002837	0.039580	40	40.126.31.73	192.168.0.10	109	TCP	1514	[TCP Retransmission] 443 → 51940 [PSH, ACK] Seq=2911 Ack=164 Win=4194304 Len=1460
374	11721.304028	21.301191	40	40.126.31.73	192.168.0.10	109	TCP	54	443 → 51940 [RST, ACK, CWR] Seq=1461 Ack=164 Win=0 Len=0
375	11721.304090	0.000062	40	40.126.31.73	192.168.0.10	109	TCP	54	443 → 51940 [RST, ACK, CWR] Seq=1 Ack=164 Win=1198080 Len=0

Let's look at the uplink traces...



To be a MTU problem or not to be a MTU problem???



tcp.stream == ${tcp.stream}+1

No.	Relative	Delta	#	Source	Destination	TTL	Protocol	Length	Info
22	40.706392		2	203.0.113.17	91.228.167.170	59	TCP	74	57166 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=968407133 TSecr=0 WS=128
23	40.731970	0.025578	2	91.228.167.170	203.0.113.17	51	TCP	62	80 → 57166 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 WS=512
24	40.732264	0.000294	2	203.0.113.17	91.228.167.170	59	TCP	60	57166 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
25	40.750083	0.017819	2	203.0.113.17	91.228.167.170	59	HTTP	548	GET /pico/1/269139.pic HTTP/1.1
26	40.775780	0.025697	2	91.228.167.170	203.0.113.17	51	TCP	309	[TCP Previous segment not captured] 80 → 57166 [PSH, ACK] Seq=1461 Ack=495 Win=42496 Len=255
27	40.775991	0.000211	2	203.0.113.17	91.228.167.170	59	TCP	60	[TCP Dup ACK 24#1] 57166 → 80 [ACK] Seq=495 Ack=1 Win=64256 Len=0
58	100.791635	60.015644	2	203.0.113.17	91.228.167.170	59	TCP	60	57166 → 80 [FIN, ACK] Seq=495 Ack=1 Win=64256 Len=0
59	100.817232	0.025597	2	91.228.167.170	203.0.113.17	51	TCP	60	80 → 57166 [FIN, ACK] Seq=1716 Ack=496 Win=42496 Len=0
60	100.817454	0.000222	2	203.0.113.17	91.228.167.170	59	TCP	60	57166 → 80 [RST] Seq=496 Win=0 Len=0

tcp.stream == ${tcp.stream}+1

No.	Relative	Delta	#	Source	Destination	TTL	Identifical	Protocol	Length	Info
28	51.213870		3	203.0.113.17	91.228.167.170	123	0x4008	TCP	66	61177 → 80 [SYN, ECE, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
29	51.239112	0.025242	3	91.228.167.170	203.0.113.17	51	0x0000	TCP	62	80 → 61177 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 WS=512
30	51.239630	0.000518	3	203.0.113.17	91.228.167.170	123	0x4009	TCP	60	61177 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
31	51.257749	0.018119	3	203.0.113.17	91.228.167.170	123	0x8019	HTTP	1054	GET /eset_upd/server7/dll/update.ver.signed HTTP/1.1
32	51.284221	0.026472	3	91.228.167.170	203.0.113.17	51	0x8cce	TCP	1514	[TCP Previous segment not captured] 80 → 61177 [PSH, ACK] Seq=1461 Ack=1001 Win=42496 Len=1460
33	51.284223	0.000002	3	91.228.167.170	203.0.113.17	51	0x8cd0	TCP	1514	[TCP Previous segment not captured] 80 → 61177 [PSH, ACK] Seq=4381 Ack=1001 Win=42496 Len=1460
34	51.284233	0.000010	3	91.228.167.170	203.0.113.17	51	0x8cd2	TCP	1514	[TCP Previous segment not captured] 80 → 61177 [PSH, ACK] Seq=7301 Ack=1001 Win=42496 Len=1460
35	51.284239	0.000006	3	91.228.167.170	203.0.113.17	51	0x8cd4	TCP	1514	[TCP Previous segment not captured] 80 → 61177 [PSH, ACK] Seq=10221 Ack=1001 Win=42496 Len=1460
36	51.284242	0.000003	3	91.228.167.170	203.0.113.17	51	0x8cd6	TCP	1514	[TCP Previous segment not captured] 80 → 61177 [PSH, ACK] Seq=13141 Ack=1001 Win=42496 Len=1460
37	51.284559	0.000317	3	203.0.113.17	91.228.167.170	123	0x400b	TCP	60	[TCP Dup ACK 30#1] 61177 → 80 [ACK] Seq=1001 Ack=1 Win=262656 Len=0
38	51.284568	0.000009	3	203.0.113.17	91.228.167.170	123	0x400c	TCP	60	[TCP Dup ACK 30#2] 61177 → 80 [ACK] Seq=1001 Ack=1 Win=262656 Len=0
39	51.284592	0.000024	3	203.0.113.17	91.228.167.170	123	0x400d	TCP	60	[TCP Dup ACK 30#3] 61177 → 80 [ACK] Seq=1001 Ack=1 Win=262656 Len=0
40	51.284601	0.000009	3	203.0.113.17	91.228.167.170	123	0x400e	TCP	60	[TCP Dup ACK 30#4] 61177 → 80 [ACK] Seq=1001 Ack=1 Win=262656 Len=0
41	51.284615	0.000014	3	203.0.113.17	91.228.167.170	123	0x400f	TCP	60	[TCP Dup ACK 30#5] 61177 → 80 [ACK] Seq=1001 Ack=1 Win=262656 Len=0
61	111.251239	59.966624	3	203.0.113.17	91.228.167.170	123	0x4016	TCP	60	61177 → 80 [FIN, ACK] Seq=1001 Ack=1 Win=262656 Len=0
62	111.565741	0.314502	3	203.0.113.17	91.228.167.170	123	0x4017	TCP	60	[TCP Retransmission] 61177 → 80 [FIN, ACK] Seq=1001 Ack=1 Win=262656 Len=0
63	112.166783	0.601042	3	203.0.113.17	91.228.167.170	123	0x4018	TCP	60	[TCP Retransmission] 61177 → 80 [FIN, ACK] Seq=1001 Ack=1 Win=262656 Len=0
64	113.367426	1.200643	3	203.0.113.17	91.228.167.170	123	0x4019	TCP	60	[TCP Retransmission] 61177 → 80 [FIN, ACK] Seq=1001 Ack=1 Win=262656 Len=0
65	115.767690	2.400264	3	203.0.113.17	91.228.167.170	123	0x401a	TCP	60	[TCP Retransmission] 61177 → 80 [FIN, ACK] Seq=1001 Ack=1 Win=262656 Len=0
66	120.578257	4.810567	3	203.0.113.17	91.228.167.170	123	0x401b	TCP	60	[TCP Retransmission] 61177 → 80 [FIN, ACK] Seq=1001 Ack=1 Win=262656 Len=0
67	130.186368	9.608111	3	203.0.113.17	91.228.167.170	123	0x401c	TCP	60	61177 → 80 [RST, ACK] Seq=1002 Ack=1 Win=0 Len=0

Let's create some monitoring!



```
$ cat bin/customer.sh
#!/usr/bin/bash

# nohup dumpcap -i enx000acd2366e3 -w customer.pcapng  -b filesize:100000 -b files:100  -f "pppoes and net 203.0.113.0/24" &

DIR=/home/beheer/pcap/custoemr
COUNTFILE=count.txt

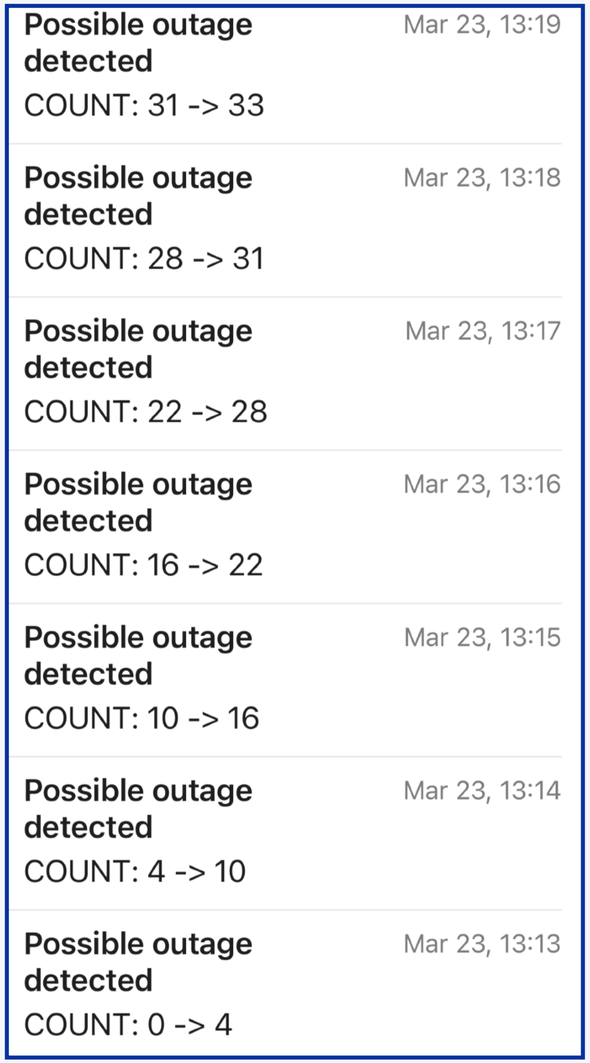
cd $DIR
[[ -f $COUNTFILE ]] || echo "0" > $COUNTFILE

OLDCOUNT=$(cat $COUNTFILE)
NEWCOUNT=$(mergecap -w - $(ls -1rt customer*.pcapng | tail -2) | tshark -r - -Y "tcp.completeness&1 and tcp.flags.fin==1 and
tcp.ack==1" | wc -l)

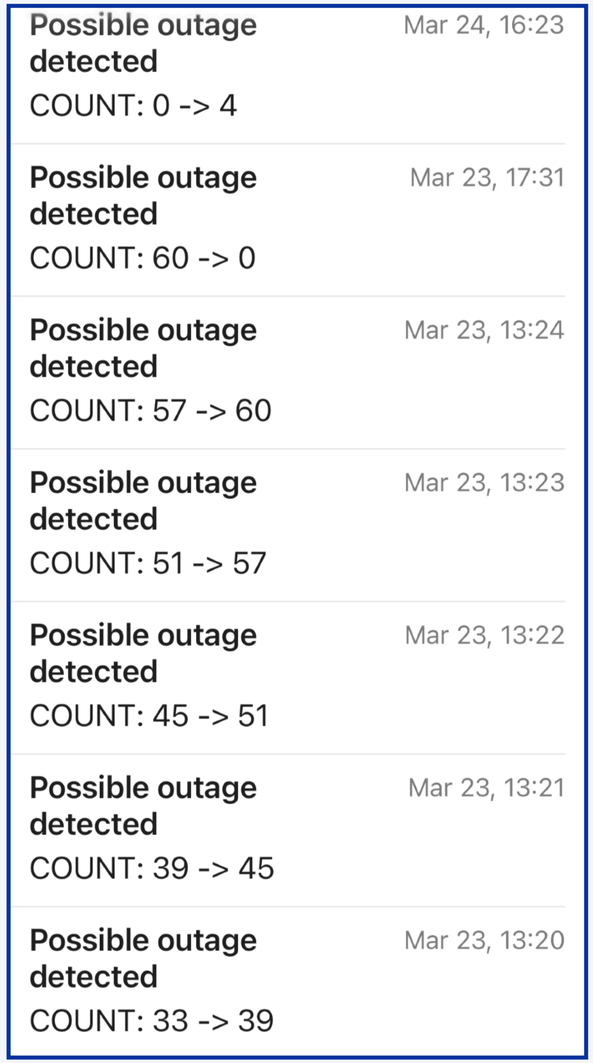
if [[ $NEWCOUNT -ne $OLDCOUNT ]]
then
  curl --request POST \
    --url https://api.pushover.net/1/messages.json \
    --header 'Accept: application/json' \
    --header 'Content-Type: application/json' \
    --data "{
              \"token\": \"a83<deleted>fa6\",
              \"user\": \"uor<deleted>v68\",
              \"title\": \"Possible outage detected\",
              \"message\": \"COUNT: ${OLDCOUNT} -> ${NEWCOUNT}\",
              \"priority\": 0
            }"
fi
$
```

```
# m h  dom mon dow   command
*/1 * * * * /home/beheer/bin/customer.sh
```

Bingo!



Possible outage detected COUNT: 31 -> 33	Mar 23, 13:19
Possible outage detected COUNT: 28 -> 31	Mar 23, 13:18
Possible outage detected COUNT: 22 -> 28	Mar 23, 13:17
Possible outage detected COUNT: 16 -> 22	Mar 23, 13:16
Possible outage detected COUNT: 10 -> 16	Mar 23, 13:15
Possible outage detected COUNT: 4 -> 10	Mar 23, 13:14
Possible outage detected COUNT: 0 -> 4	Mar 23, 13:13



Possible outage detected COUNT: 0 -> 4	Mar 24, 16:23
Possible outage detected COUNT: 60 -> 0	Mar 23, 17:31
Possible outage detected COUNT: 57 -> 60	Mar 23, 13:24
Possible outage detected COUNT: 51 -> 57	Mar 23, 13:23
Possible outage detected COUNT: 45 -> 51	Mar 23, 13:22
Possible outage detected COUNT: 39 -> 45	Mar 23, 13:21
Possible outage detected COUNT: 33 -> 39	Mar 23, 13:20

Let's look at the both sides...



All OK!



tcp.stream == 0 and not frame.number in {27..43}

No.	Relative	Delta	#	Source	Destination	TTL	Identificat	Protocol	Length	Info
1	0.000000		0	203.0.113.17	87.215.217.229	59	0xf959	TCP	74	33762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1176076012 TSecr=0 WS=128
2	0.009876	0.009876	0	87.215.217.229	203.0.113.17	244	0x0000	TCP	74	443 → 33762 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1452 SACK_PERM TSval=2660159470 TSecr=1176076012 WS=128
3	0.010762	0.000886	0	203.0.113.17	87.215.217.229	59	0xf95a	TCP	66	33762 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1176076022 TSecr=2660159470
4	0.027597	0.016835	0	203.0.113.17	87.215.217.229	59	0x0000	TLSv1.3	583	Client Hello (SNI=ctf.syn-bit.nl)
5	0.037615	0.010018	0	87.215.217.229	203.0.113.17	244	0x89e2	TCP	66	443 → 33762 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=2660159498 TSecr=1176076025
6	0.061733	0.024118	0	87.215.217.229	203.0.113.17	244	0x89e3	TLSv1.3	1506	Server Hello, Change Cipher Spec, Application Data
7	0.061857	0.000124	0	87.215.217.229	203.0.113.17	244	0x89e4	TCP	1506	443 → 33762 [PSH, ACK] Seq=1441 Ack=518 Win=64768 Len=1440 TSval=2660159521 TSecr=1176076025 [TCP PDU reassembled in 8]
8	0.061858	0.000001	0	87.215.217.229	203.0.113.17	244	0x89e5	TLSv1.3	971	Application Data, Application Data, Application Data, Application Data
9	0.062034	0.000176	0	203.0.113.17	87.215.217.229	59	0xf95c	TCP	66	33762 → 443 [ACK] Seq=518 Ack=1441 Win=64128 Len=0 TSval=1176076074 TSecr=2660159521
10	0.062080	0.000046	0	203.0.113.17	87.215.217.229	59	0xf95d	TCP	66	33762 → 443 [ACK] Seq=518 Ack=3786 Win=61824 Len=0 TSval=1176076074 TSecr=2660159521
11	0.064098	0.002018	0	203.0.113.17	87.215.217.229	59	0xf95e	TLSv1.3	130	Change Cipher Spec, Application Data
12	0.064171	0.000073	0	203.0.113.17	87.215.217.229	59	0xf95f	TLSv1.3	112	Application Data
13	0.064189	0.000018	0	203.0.113.17	87.215.217.229	59	0xf960	TLSv1.3	115	Application Data
14	0.064259	0.000070	0	203.0.113.17	87.215.217.229	59	0xf961	TLSv1.3	101	Application Data
15	0.064274	0.000015	0	203.0.113.17	87.215.217.229	59	0xf962	TLSv1.3	168	Application Data
16	0.073863	0.009589	0	87.215.217.229	203.0.113.17	244	0x89e6	TCP	66	443 → 33762 [ACK] Seq=3786 Ack=582 Win=64768 Len=0 TSval=2660159534 TSecr=1176076076
17	0.074255	0.000392	0	87.215.217.229	203.0.113.17	244	0x89e7	TCP	66	443 → 33762 [ACK] Seq=3786 Ack=628 Win=64768 Len=0 TSval=2660159534 TSecr=1176076076
18	0.074255	0.000000	0	87.215.217.229	203.0.113.17	244	0x89e8	TCP	66	443 → 33762 [ACK] Seq=3786 Ack=677 Win=64768 Len=0 TSval=2660159534 TSecr=1176076076
19	0.074256	0.000001	0	87.215.217.229	203.0.113.17	244	0x89e9	TCP	66	443 → 33762 [ACK] Seq=3786 Ack=712 Win=64768 Len=0 TSval=2660159534 TSecr=1176076076
20	0.074392	0.000136	0	87.215.217.229	203.0.113.17	244	0x89ea	TCP	66	443 → 33762 [ACK] Seq=3786 Ack=814 Win=64768 Len=0 TSval=2660159534 TSecr=1176076077
21	0.074392	0.000000	0	87.215.217.229	203.0.113.17	244	0x89eb	TLSv1.3	127	Application Data
22	0.074615	0.000223	0	87.215.217.229	203.0.113.17	244	0x89ec	TLSv1.3	110	Application Data
23	0.074971	0.000356	0	203.0.113.17	87.215.217.229	59	0xf963	TLSv1.3	97	Application Data
24	0.084508	0.009537	0	87.215.217.229	203.0.113.17	244	0x89ed	TCP	66	443 → 33762 [ACK] Seq=3891 Ack=845 Win=64768 Len=0 TSval=2660159545 TSecr=1176076087
25	0.086998	0.002490	0	87.215.217.229	203.0.113.17	244	0x89ee	TLSv1.3	349	Application Data
26	0.087251	0.000253	0	87.215.217.229	203.0.113.17	244	0x89ef	TCP	1506	443 → 33762 [ACK] Seq=4174 Ack=845 Win=64768 Len=1440 TSval=2660159547 TSecr=1176076087 [TCP PDU reassembled in 30]
44	0.097611	0.010360	0	87.215.217.229	203.0.113.17	244	0x89fd	TLSv1.3	1292	Application Data
45	0.097621	0.000010	0	203.0.113.17	87.215.217.229	59	0xf968	TCP	66	33762 → 443 [ACK] Seq=845 Ack=19212 Win=62592 Len=0 TSval=1176076110 TSecr=2660159557
46	0.097692	0.000071	0	203.0.113.17	87.215.217.229	59	0xf969	TCP	66	33762 → 443 [ACK] Seq=845 Ack=23318 Win=59520 Len=0 TSval=1176076110 TSecr=2660159558
47	0.097881	0.000189	0	203.0.113.17	87.215.217.229	59	0xf96a	TLSv1.3	90	Application Data
48	0.097936	0.000055	0	203.0.113.17	87.215.217.229	59	0xf96b	TCP	66	33762 → 443 [FIN, ACK] Seq=869 Ack=23318 Win=64128 Len=0 TSval=1176076110 TSecr=2660159558
49	0.107720	0.009784	0	87.215.217.229	203.0.113.17	244	0x89fe	TLSv1.3	90	Application Data
50	0.107840	0.000120	0	203.0.113.17	87.215.217.229	59	0x0000	TCP	60	33762 → 443 [RST] Seq=870 Win=0 Len=0
51	0.107997	0.000157	0	87.215.217.229	203.0.113.17	244	0x89ff	TCP	66	443 → 33762 [FIN, ACK] Seq=23342 Ack=870 Win=64768 Len=0 TSval=2660159568 TSecr=1176076110
52	0.108144	0.000147	0	203.0.113.17	87.215.217.229	59	0x0000	TCP	60	33762 → 443 [RST] Seq=870 Win=0 Len=0

At my office...



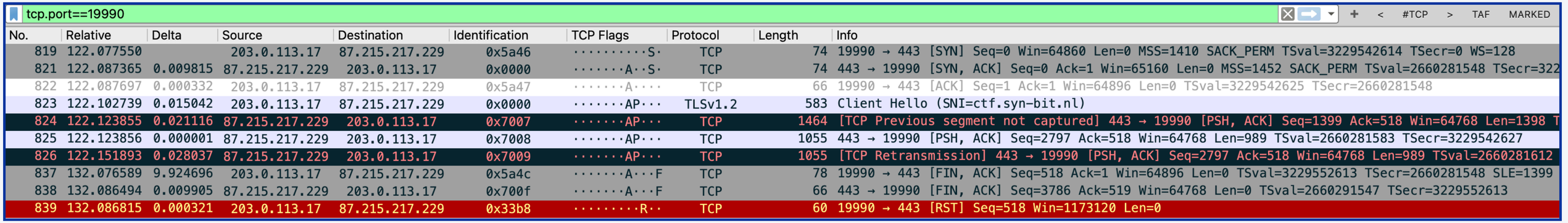
tcp.port==33762

No.	Relative	Delta	Source	Destination	TTL	Protocol	Length	Info
1	0.000000		203.0.113.17	87.215.217.229	249	TCP	82	33762 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1176076012 TSecr=0 WS=128
2	0.000582	0.000582	87.215.217.229	203.0.113.17	62	TCP	82	443 → 33762 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1452 SACK_PERM TSval=2660159470 TSec
3	0.011077	0.010495	203.0.113.17	87.215.217.229	249	TCP	74	33762 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1176076022 TSecr=2660159470
4	0.027504	0.016427	203.0.113.17	87.215.217.229	249	TLSv1.3	591	Client Hello (SNI=ctf.syn-bit.nl)
5	0.028320	0.000816	87.215.217.229	203.0.113.17	62	TCP	74	443 → 33762 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=2660159498 TSecr=1176076025
6	0.052468	0.024148	87.215.217.229	203.0.113.17	62	TLSv1.3	1516	Server Hello, Change Cipher Spec, Application Data
7	0.052470	0.000002	87.215.217.229	203.0.113.17	62	TCP	1516	443 → 33762 [PSH, ACK] Seq=1441 Ack=518 Win=64768 Len=1440 TSval=2660159521 TSecr=117607602
8	0.052470	0.000000	87.215.217.229	203.0.113.17	62	TLSv1.3	979	Application Data, Application Data, Application Data, Application Data
9	0.062108	0.009638	203.0.113.17	87.215.217.229	249	TCP	76	33762 → 443 [ACK] Seq=518 Ack=1441 Win=64128 Len=0 TSval=1176076074 TSecr=2660159521
10	0.062108	0.000000	203.0.113.17	87.215.217.229	249	TCP	74	33762 → 443 [ACK] Seq=518 Ack=3786 Win=61824 Len=0 TSval=1176076074 TSecr=2660159521
11	0.064590	0.002482	203.0.113.17	87.215.217.229	249	TLSv1.3	140	Change Cipher Spec, Application Data
12	0.064592	0.000002	203.0.113.17	87.215.217.229	249	TLSv1.3	122	Application Data
13	0.064594	0.000002	203.0.113.17	87.215.217.229	249	TLSv1.3	125	Application Data

```
> Frame 46: Packet, 74 bytes on wire, 74 bytes captured on interface unknown, id 0
> Ethernet II, Src: 06:00:00:bf:fd:b4 (06:00:00:bf:fd:b4), Dst: PaloAltoNetw_2b:59:e5 (7c:c0:25:2b:59:e5)
> PPP-over-Ethernet Session
> Point-to-Point Protocol
> Internet Protocol Version 4, Src: 203.0.113.17 (203.0.113.17), Dst: 87.215
> Transmission Control Protocol, Src Port: 33762, Dst Port: 443, Seq: 845, A
  [Community ID: 1:0OIcdXXRUrEGdK8To4GgEvOgSsA=]
```

```
> Frame 6: Packet, 1516 bytes on wire, 1516 bytes captured on interface unknown, id 0
> Ethernet II, Src: PaloAltoNetw_2b:59:e5 (7c:c0:25:2b:59:e5), Dst: 06:00:00:bf:fd:b4 (06:00:00:bf:fd:b4)
v PPP-over-Ethernet Session
    0001 .... = Version: 1
    .... 0001 = Type: 1
    Code: Session Data (0x00)
    Session ID: 0x0a2d
  v Payload Length: 1494 [incorrect, should be 1496]
    > [Expert Info (Warning/Malformed): Possible bad payload length 1494 != 1496]
> Point-to-Point Protocol
> Internet Protocol Version 4, Src: 87.215.217.229 (87.215.217.229), Dst: 203.0.113.17 (203.0.113.17)
> Transmission Control Protocol, Src Port: 443, Dst Port: 33762, Seq: 1, Ack: 518, Len: 1440
> Transport Layer Security
  [Community ID: 1:0OIcdXXRUrEGdK8To4GgEvOgSsA=]
```

NOK!!!



tcp.port==19990

No.	Relative	Delta	Source	Destination	Identification	TCP Flags	Protocol	Length	Info
819	122.077550		203.0.113.17	87.215.217.229	0x5a46	··········S·	TCP	74	19990 → 443 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM TSval=3229542614 TSecr=0 WS=128
821	122.087365	0.009815	87.215.217.229	203.0.113.17	0x0000	·····A··S·	TCP	74	443 → 19990 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1452 SACK_PERM TSval=2660281548 TSecr=322
822	122.087697	0.000332	203.0.113.17	87.215.217.229	0x5a47	·····A····	TCP	66	19990 → 443 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=3229542625 TSecr=2660281548
823	122.102739	0.015042	203.0.113.17	87.215.217.229	0x0000	·····AP···	TLSv1.2	583	Client Hello (SNI=ctf.syn-bit.nl)
824	122.123855	0.021116	87.215.217.229	203.0.113.17	0x7007	·····AP···	TCP	1464	[TCP Previous segment not captured] 443 → 19990 [PSH, ACK] Seq=1399 Ack=518 Win=64768 Len=1398 T
825	122.123856	0.000001	87.215.217.229	203.0.113.17	0x7008	·····AP···	TCP	1055	443 → 19990 [PSH, ACK] Seq=2797 Ack=518 Win=64768 Len=989 TSval=2660281583 TSecr=3229542627
826	122.151893	0.028037	87.215.217.229	203.0.113.17	0x7009	·····AP···	TCP	1055	[TCP Retransmission] 443 → 19990 [PSH, ACK] Seq=2797 Ack=518 Win=64768 Len=989 TSval=2660281612
837	132.076589	9.924696	203.0.113.17	87.215.217.229	0x5a4c	·····A···F	TCP	78	19990 → 443 [FIN, ACK] Seq=518 Ack=1 Win=64896 Len=0 TSval=3229552613 TSecr=2660281548 SLE=1399
838	132.086494	0.009905	87.215.217.229	203.0.113.17	0x700f	·····A···F	TCP	66	443 → 19990 [FIN, ACK] Seq=3786 Ack=519 Win=64768 Len=0 TSval=2660291547 TSecr=3229552613
839	132.086815	0.000321	203.0.113.17	87.215.217.229	0x33b8	·····R··	TCP	60	19990 → 443 [RST] Seq=518 Win=1173120 Len=0

tcp.port==19990

No.	Relative	Delta	Source	Destination	Identification	TCP Flags	Protocol	Length	Info
925	122.077661		203.0.113.17	87.215.217.229	0x5a46	··········S·	TCP	82	19990 → 443 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM TSval=3229542614 TSecr=0 WS=128
926	122.078231	0.000570	87.215.217.229	203.0.113.17	0x0000	·····A··S·	TCP	82	443 → 19990 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1452 SACK_PERM TSval=2660281548 TSecr=322
928	122.087768	0.009537	203.0.113.17	87.215.217.229	0x5a47	·····A····	TCP	74	19990 → 443 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=3229542625 TSecr=2660281548
929	122.103228	0.015460	203.0.113.17	87.215.217.229	0x0000	·····AP···	TLSv1.3	591	Client Hello (SNI=ctf.syn-bit.nl)
930	122.103595	0.000367	87.215.217.229	203.0.113.17	0x7005	·····A····	TCP	74	443 → 19990 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=2660281573 TSecr=3229542627
931	122.114505	0.010910	87.215.217.229	203.0.113.17	0x7006	·····A····	TLSv1.3	1474	Server Hello, Change Cipher Spec, Application Data
932	122.114507	0.000002	87.215.217.229	203.0.113.17	0x7007	·····AP···	TCP	1474	443 → 19990 [PSH, ACK] Seq=1399 Ack=518 Win=64768 Len=1398 TSval=2660281583 TSecr=3229542627 [TC
933	122.114508	0.000001	87.215.217.229	203.0.113.17	0x7008	·····AP···	TLSv1.3	1063	Application Data, Application Data, Application Data, Application Data
934	122.142586	0.028078	87.215.217.229	203.0.113.17	0x7009	·····AP···	TCP	1063	[TCP Retransmission] 443 → 19990 [PSH, ACK] Seq=2797 Ack=518 Win=64768 Len=989 TSval=2660281612
935	122.358338	0.215752	87.215.217.229	203.0.113.17	0x700a	·····A····	TCP	1472	[TCP Retransmission] 443 → 19990 [ACK] Seq=1 Ack=518 Win=64768 Len=1398 TSval=2660281828 TSecr=3
936	122.790685	0.432347	87.215.217.229	203.0.113.17	0x700b	·····A····	TCP	1472	[TCP Retransmission] 443 → 19990 [ACK] Seq=1 Ack=518 Win=64768 Len=1398 TSval=2660282260 TSecr=3
938	123.654330	0.863645	87.215.217.229	203.0.113.17	0x700c	·····A····	TCP	1472	[TCP Retransmission] 443 → 19990 [ACK] Seq=1 Ack=518 Win=64768 Len=1398 TSval=2660283124 TSecr=3
940	125.382302	1.727972	87.215.217.229	203.0.113.17	0x700d	·····A····	TCP	1472	[TCP Retransmission] 443 → 19990 [ACK] Seq=1 Ack=518 Win=64768 Len=1398 TSval=2660284852 TSecr=3
941	128.934367	3.552065	87.215.217.229	203.0.113.17	0x700e	·····A····	TCP	1472	[TCP Retransmission] 443 → 19990 [ACK] Seq=1 Ack=518 Win=64768 Len=1398 TSval=2660288404 TSecr=3
953	132.076786	3.142419	203.0.113.17	87.215.217.229	0x5a4c	·····A···F	TCP	86	19990 → 443 [FIN, ACK] Seq=518 Ack=1 Win=64896 Len=0 TSval=3229552613 TSecr=2660281548 SLE=1399
954	132.077296	0.000510	87.215.217.229	203.0.113.17	0x700f	·····A···F	TCP	74	443 → 19990 [FIN, ACK] Seq=3786 Ack=519 Win=64768 Len=0 TSval=2660291547 TSecr=3229552613
955	132.087235	0.009939	203.0.113.17	87.215.217.229	0x33b8	·····R··	TCP	62	19990 → 443 [RST] Seq=518 Win=1173120 Len=0
977	143.526409	11.4391…	87.215.217.229	203.0.113.17	0x7010	·····A····	TCP	1472	[TCP Retransmission] 443 → 19990 [ACK] Seq=1 Ack=519 Win=64768 Len=1398 TSval=2660302996 TSecr=3

Summary



- Problem happened when traffic for one outgoing IP hit 500 kpps
- Suspected Anti-DDoS
  - But what kind of filtering???
- ISP confirmed that Anti-DDoS kicked in
  - Based on TCP flag combination (which pattern?)
- Bare ACK trigger
  - ... and filter!!!
  - not possible to exclude established sessions
- Why no alerting?
  - Migration from one Anti-DDoS solution to another
  - Reporting/Alerting was still under construction

Thank you!

WIRESHARK

Sake Blok
sake.blok@SYN-bit.nl

SYN-bit
deep traffic analysis

Please provide feedback
Either by scanning the qr-code or by
clicking on the feedback button in the agenda!