SharkFest'19 US

Troubleshooting issues on encrypted links

… or why you always need more screens

Christian Landström

Airbus CyberSecurity

About me?

- Working for AIRBUS
- Reading trace files for the fun of it
- Sharkfest addict since Stanford

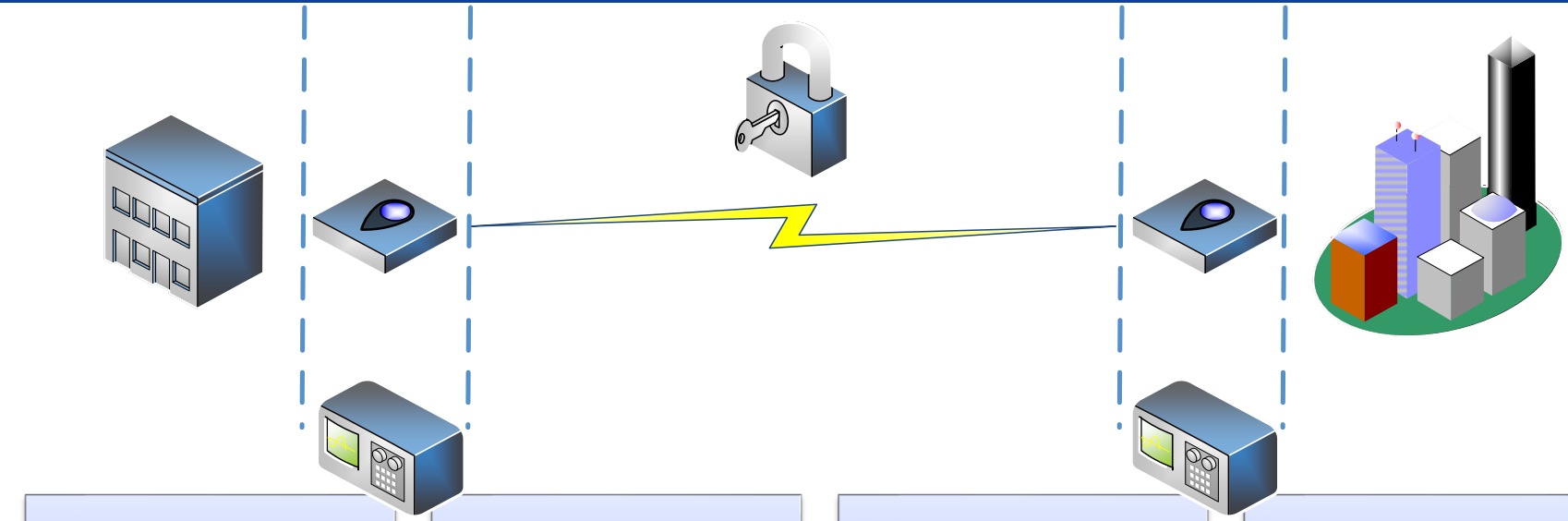
Why Encrypted links ?

- Encrypted links are often prone to immense discussions when troubleshooting is involved
- Site 1, WAN/LAN, Provider, NOC, Site 2 LAN/WAN etc.

Situation

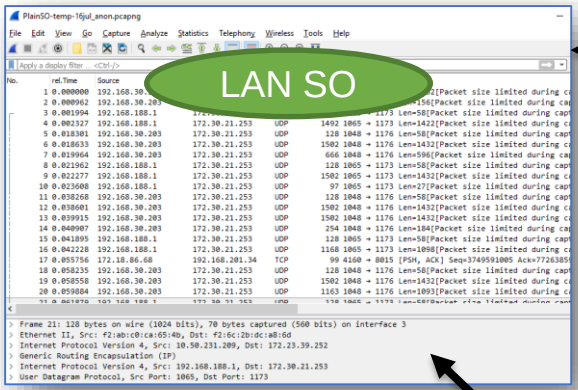
- Customer complains that SO is having connectivity issues affecting:
  - Mail
  - Telephone
  - Internet
- Step 1 in Troubleshooting: Verify the problem!

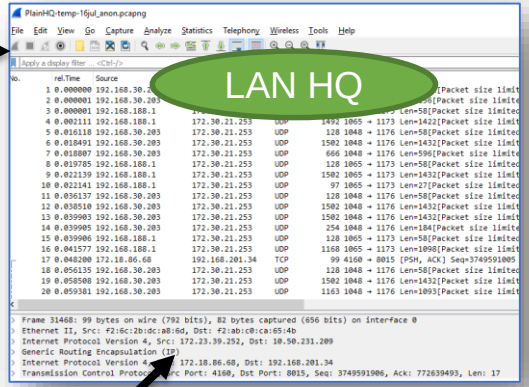
2 Sites, 1 WAN link

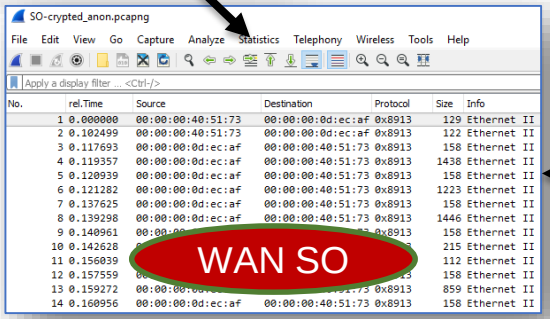


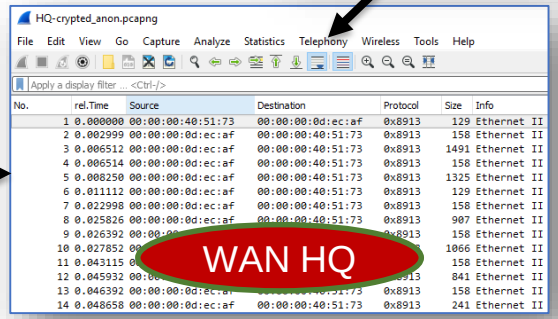
SO Plaintext	SO breakout encrypted WAN	HQ breakout encrypted WAN	HQ Plaintext

Issues with encryption





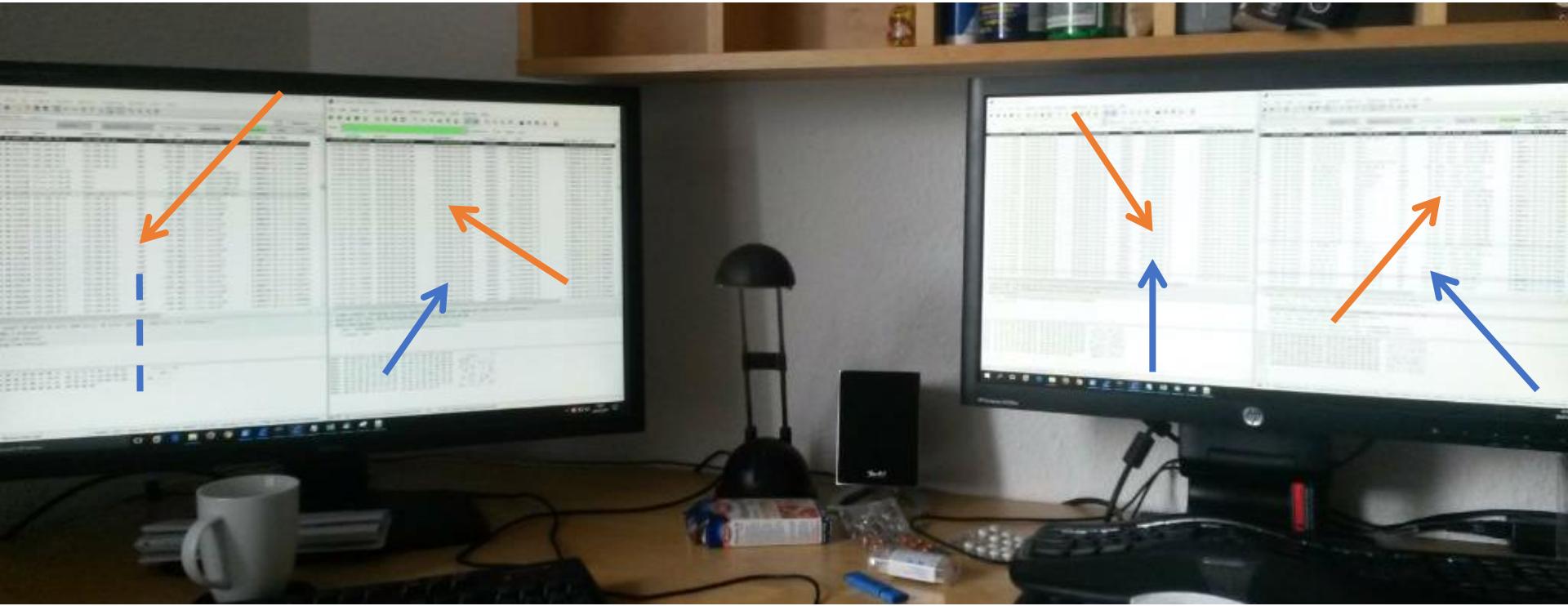




Issues with encryption

- Procedure:
  - Start with plaintext -> isolate problem
  - If plain1 != plain2
    - Match plain1 to enc1
    - Match enc1 to enc2
    - Match enc2 to plain2

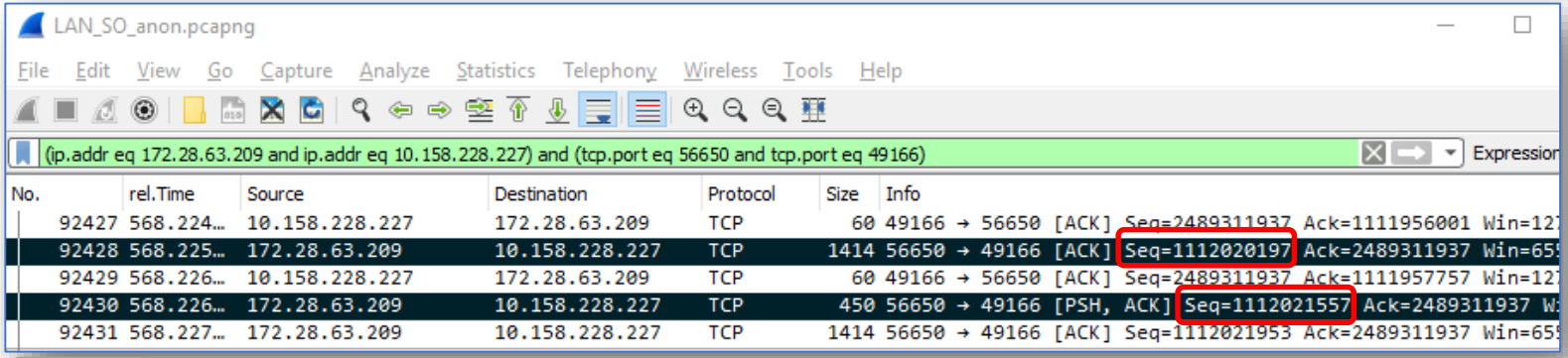
Challenges...



Search for issues

- Starting with client side packet loss analysis
- Default starting point tcp.analysis.flags to see what is happening
- Dig into the details of specific TCP conversations if needed

Packet loss analysis



SO

HQ

Source	Destination	Protocol	Size	Info
172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112018837 Ack=2489311937 Win=65536 Len=1360
10.158.228.227	172.28.63.209	TCP	60	49166 → 56650 [ACK] Seq=2489311937 Ack=1111992377 Win=129024 Len=0
10.158.228.227	172.28.63.209	TCP	60	49166 → 56650 [ACK] Seq=2489311937 Ack=1111994133 Win=129024 Len=0
10.158.228.227	172.28.63.209	TCP	60	49166 → 56650 [ACK] Seq=2489311937 Ack=1111996853 Win=129024 Len=0
10.158.228.227	172.28.63.209	TCP	60	49166 → 56650 [ACK] Seq=2489311937 Ack=1111998609 Win=129024 Len=0
172.28.63.209	10.158.228.227	TCP	1414	[TCP Previous segment not captured] 56650 → 49166 [ACK] Seq=1112021953 Ac
172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112023313 Ack=2489311937 Win=65536 Len=1360
172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112024673 Ack=2489311937 Win=65536 Len=1360
10.158.228.227	172.28.63.209	TCP	60	49166 → 56650 [ACK] Seq=2489311937 Ack=1112001329 Win=130560 Len=0
172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112026033 Ack=2489311937 Win=65536 Len=1360
172.28.63.209	10.158.228.227	TCP	450	56650 → 49166 [PSH, ACK] Seq=1112027393 Ack=2489311937 Win=65536 Len=396

Match plain to encrypted

No.	rel.Time	Source	Destination	Protocol	Size	Info
92425	14:46:31,155908	172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112017477 Ack=
92426	14:46:31,156907	172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112018837 Ack=
92427	14:46:31,157388	10.158.228.227	172.28.63.209	TCP	60	49166 → 56650 [ACK] Seq=2489311937 Ack=
92428	14:46:31,158212	172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112020197 Ack=
92429	14:46:31,159072	10.158.228.227	172.28.63.209	TCP	60	49166 → 56650 [ACK] Seq=2489311937 Ack=
92430	14:46:31,159209	172.28.63.209	10.158.228.227	TCP	450	56650 → 49166 [PSH, ACK] Seq=1112021557
92431	14:46:31,159546	172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112021953 Ack=

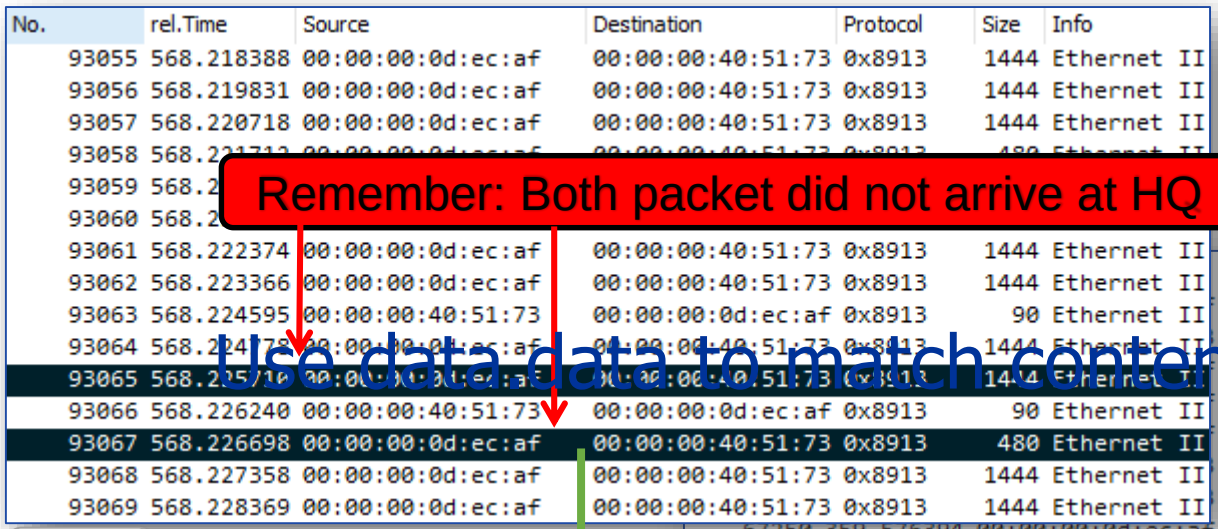
SO

Using time stamp and frame size:

SO

No.	rel.Time	Source	Destination	Protocol	Size	Info
93062	14:46:31,155971	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93063	14:46:31,157200	00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	90	Ethernet II
93064	14:46:31,157383	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93065	14:46:31,158315	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93066	14:46:31,158845	00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	90	Ethernet II
93067	14:46:31,159303	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	480	Ethernet II
93068	14:46:31,159963	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93069	14:46:31,160974	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II

Match encrypted



No.	rel.Time	Source	Destination	Protocol	Size	Info
93055	568.218388	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93056	568.219831	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93057	568.220718	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93058	568.221712	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93059	568.2					
93060	568.2					
93061	568.222374	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93062	568.223366	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93063	568.224595	00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	90	Ethernet II
93064	568.224778	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93065	568.225710	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93066	568.226240	00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	90	Ethernet II
93067	568.226698	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	480	Ethernet II
93068	568.227358	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93069	568.228369	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II

Remember: Both packet did not arrive at HQ plain capture point

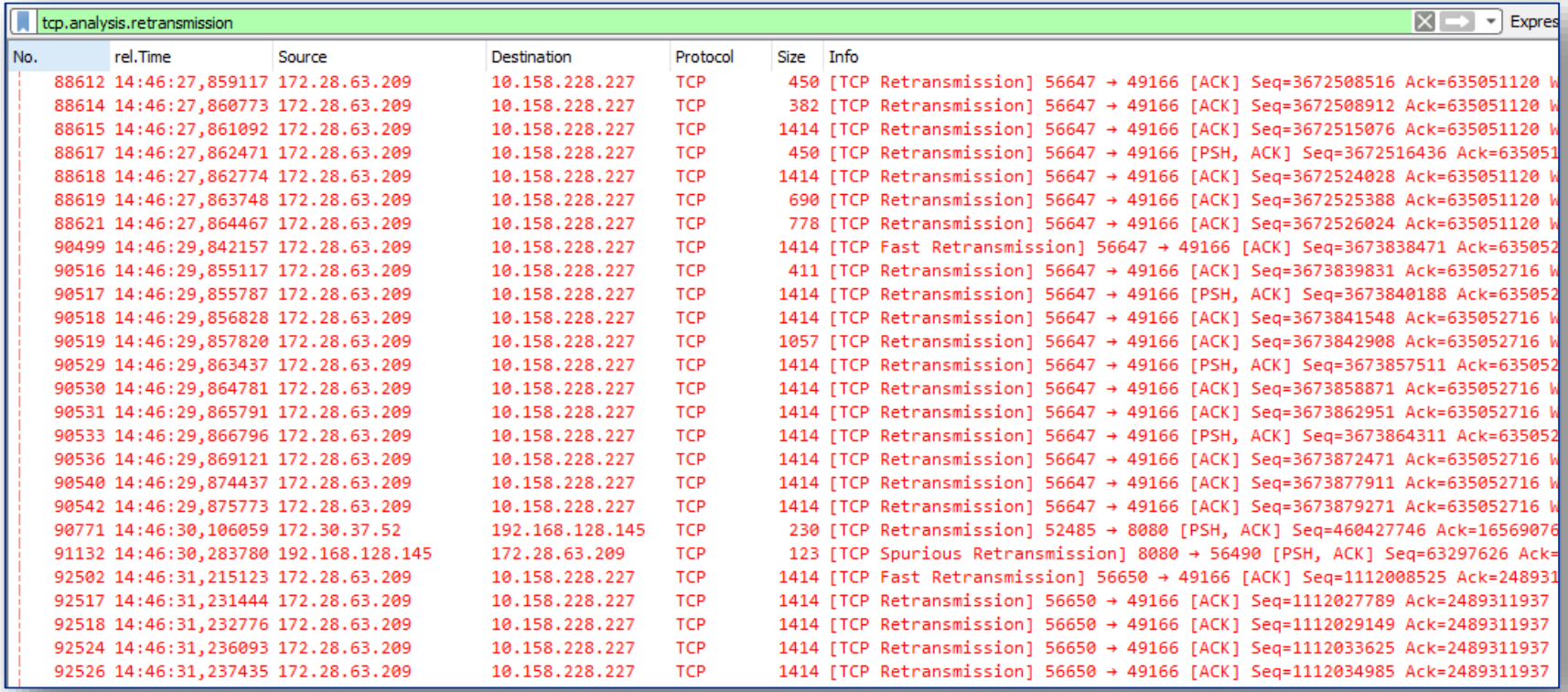
HQ

Destination	Protocol	Size	Info
00:00:00:40:51:73	0x8913	1444	Ethernet II
00:00:00:0d:ec:af	0x8913	1444	Ethernet II
00:00:00:40:51:73	0x8913	1444	Ethernet II
00:00:00:40:51:73	0x8913	1444	Ethernet II
00:00:00:40:51:73	0x8913	480	Ethernet II
00:00:00:0d:ec:af	0x8913	90	Ethernet II
00:00:00:0d:ec:af	0x8913	1444	Ethernet II
00:00:00:40:51:73	0x8913	1444	Ethernet II
67250 359.576394	00:00:00:0d:ec:af		
67251 359.577484	00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	1373	Ethernet II
67252 359.577671	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
67253 359.579099	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
67254 359.579307	00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	90	Ethernet II
67255 359.579387	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	480	Ethernet II
67256 359.579670	00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	90	Ethernet II
67257 359.579671	00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	90	Ethernet II

Use data data to match content and frame size

SO

Seeing a pattern?



tcp.analysis.retransmission

No.	rel.Time	Source	Destination	Protocol	Size	Info
88612	14:46:27,859117	172.28.63.209	10.158.228.227	TCP	450	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3672508516 Ack=635051120 W
88614	14:46:27,860773	172.28.63.209	10.158.228.227	TCP	382	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3672508912 Ack=635051120 W
88615	14:46:27,861092	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3672515076 Ack=635051120 W
88617	14:46:27,862471	172.28.63.209	10.158.228.227	TCP	450	[TCP Retransmission] 56647 → 49166 [PSH, ACK] Seq=3672516436 Ack=635051
88618	14:46:27,862774	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3672524028 Ack=635051120 W
88619	14:46:27,863748	172.28.63.209	10.158.228.227	TCP	690	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3672525388 Ack=635051120 W
88621	14:46:27,864467	172.28.63.209	10.158.228.227	TCP	778	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3672526024 Ack=635051120 W
90499	14:46:29,842157	172.28.63.209	10.158.228.227	TCP	1414	[TCP Fast Retransmission] 56647 → 49166 [ACK] Seq=3673838471 Ack=635052
90516	14:46:29,855117	172.28.63.209	10.158.228.227	TCP	411	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3673839831 Ack=635052716 W
90517	14:46:29,855787	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56647 → 49166 [PSH, ACK] Seq=3673840188 Ack=635052
90518	14:46:29,856828	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3673841548 Ack=635052716 W
90519	14:46:29,857820	172.28.63.209	10.158.228.227	TCP	1057	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3673842908 Ack=635052716 W
90529	14:46:29,863437	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56647 → 49166 [PSH, ACK] Seq=3673857511 Ack=635052
90530	14:46:29,864781	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3673858871 Ack=635052716 W
90531	14:46:29,865791	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3673862951 Ack=635052716 W
90533	14:46:29,866796	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56647 → 49166 [PSH, ACK] Seq=3673864311 Ack=635052
90536	14:46:29,869121	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3673872471 Ack=635052716 W
90540	14:46:29,874437	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3673877911 Ack=635052716 W
90542	14:46:29,875773	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56647 → 49166 [ACK] Seq=3673879271 Ack=635052716 W
90771	14:46:30,106059	172.30.37.52	192.168.128.145	TCP	230	[TCP Retransmission] 52485 → 8080 [PSH, ACK] Seq=460427746 Ack=16569076
91132	14:46:30,283780	192.168.128.145	172.28.63.209	TCP	123	[TCP Spurious Retransmission] 8080 → 56490 [PSH, ACK] Seq=63297626 Ack=
92502	14:46:31,215123	172.28.63.209	10.158.228.227	TCP	1414	[TCP Fast Retransmission] 56650 → 49166 [ACK] Seq=1112008525 Ack=248931
92517	14:46:31,231444	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56650 → 49166 [ACK] Seq=1112027789 Ack=2489311937
92518	14:46:31,232776	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56650 → 49166 [ACK] Seq=1112029149 Ack=2489311937
92524	14:46:31,236093	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56650 → 49166 [ACK] Seq=1112033625 Ack=2489311937
92526	14:46:31,237435	172.28.63.209	10.158.228.227	TCP	1414	[TCP Retransmission] 56650 → 49166 [ACK] Seq=1112034985 Ack=2489311937

Conclusion

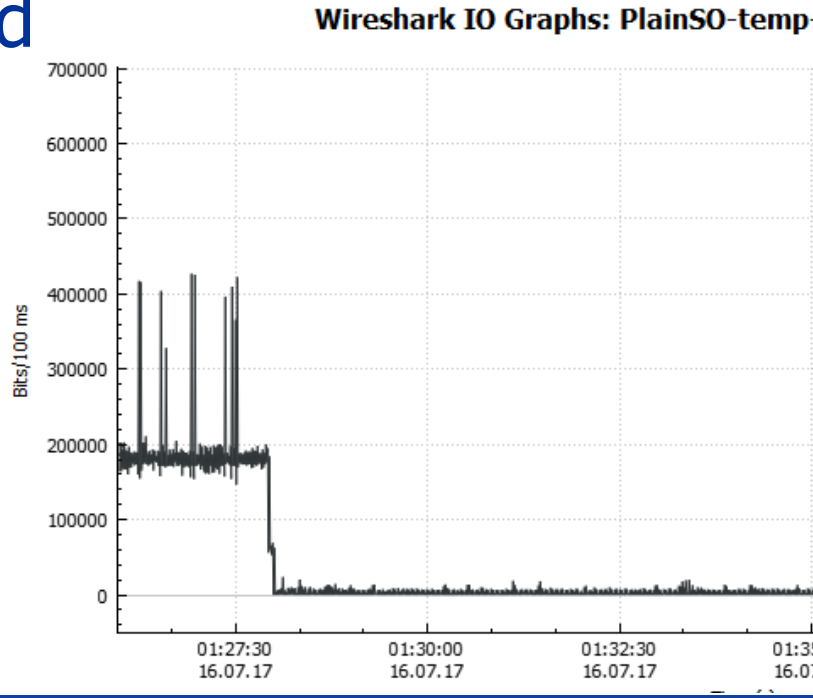
- Retransmissions occur due to packet loss in WAN link
- Responsibility: Most likely WAN link provider
- Every packet loss triggers at least two retransmissions due to encryption device
- Impact on performance: moderate, not the main issue

Moving on ...

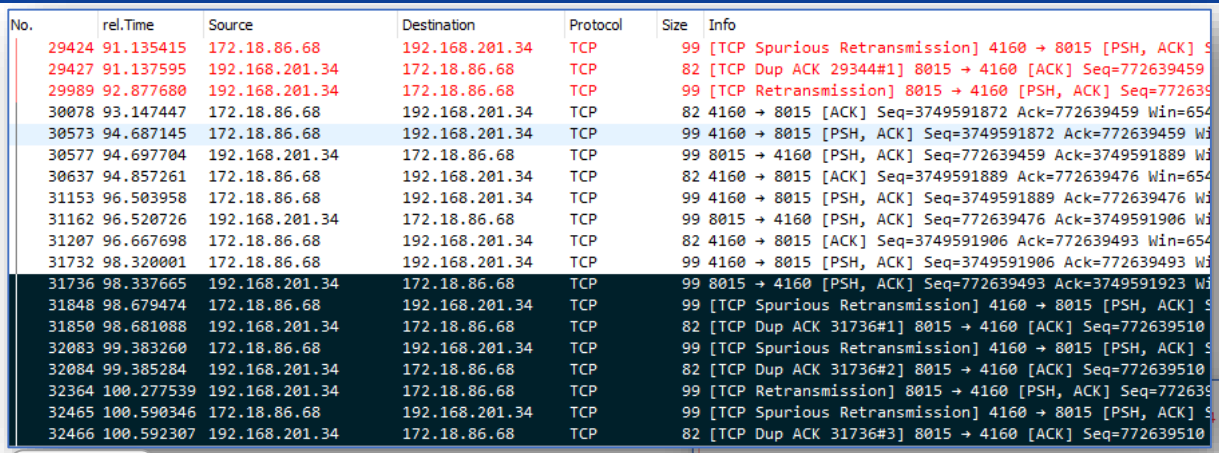
So the sniffers were kept running with ring buffers active to capture the upcoming at least 24-48 hours of traffic

Search the issue!

- Next day customer reported a complete outage -> Switches restarted to fix
- Let's take a look at I/O Graph
- Huge network impact at ~01:30 in the night



Compare the plain text



No.	rel.Time	Source	Destination	Protocol	Size	Info
29424	91.135415	172.18.86.68	192.168.201.34	TCP	99	[TCP Spurious Retransmission] 4160 → 8015 [PSH, ACK] S
29427	91.137595	192.168.201.34	172.18.86.68	TCP	82	[TCP Dup ACK 29344#1] 8015 → 4160 [ACK] Seq=772639459
29989	92.877680	192.168.201.34	172.18.86.68	TCP	99	[TCP Retransmission] 8015 → 4160 [PSH, ACK] Seq=772639
30078	93.147447	172.18.86.68	192.168.201.34	TCP	82	4160 → 8015 [ACK] Seq=3749591872 Ack=772639459 Win=654
30573	94.687145	172.18.86.68	192.168.201.34	TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Wi
30577	94.697704	192.168.201.34	172.18.86.68	TCP	99	8015 → 4160 [PSH, ACK] Seq=772639459 Ack=3749591889 Wi
30637	94.857261	172.18.86.68	192.168.201.34	TCP	82	4160 → 8015 [ACK] Seq=3749591889 Ack=772639476 Win=654
31153	96.503958	172.18.86.68	192.168.201.34	TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591889 Ack=772639476 Wi
31162	96.520726	192.168.201.34	172.18.86.68	TCP	99	8015 → 4160 [PSH, ACK] Seq=772639476 Ack=3749591906 Wi
31207	96.667698	172.18.86.68	192.168.201.34	TCP	82	4160 → 8015 [ACK] Seq=3749591906 Ack=772639493 Win=654
31732	98.320001	172.18.86.68	192.168.201.34	TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591906 Ack=772639493 Wi
31736	98.337665	192.168.201.34	172.18.86.68	TCP	99	8015 → 4160 [PSH, ACK] Seq=772639493 Ack=3749591923 Wi
31848	98.679474	172.18.86.68	192.168.201.34	TCP	99	[TCP Spurious Retransmission] 4160 → 8015 [PSH, ACK] S
31850	98.681088	192.168.201.34	172.18.86.68	TCP	82	[TCP Dup ACK 31736#1] 8015 → 4160 [ACK] Seq=772639510
32083	99.383260	172.18.86.68	192.168.201.34	TCP	99	[TCP Spurious Retransmission] 4160 → 8015 [PSH, ACK] S
32084	99.385284	192.168.201.34	172.18.86.68	TCP	82	[TCP Dup ACK 31736#2] 8015 → 4160 [ACK] Seq=772639510
32364	100.277539	192.168.201.34	172.18.86.68	TCP	99	[TCP Retransmission] 8015 → 4160 [PSH, ACK] Seq=772639
32465	100.590346	172.18.86.68	192.168.201.34	TCP	99	[TCP Spurious Retransmission] 4160 → 8015 [PSH, ACK] S
32466	100.592307	192.168.201.34	172.18.86.68	TCP	82	[TCP Dup ACK 31736#3] 8015 → 4160 [ACK] Seq=772639510

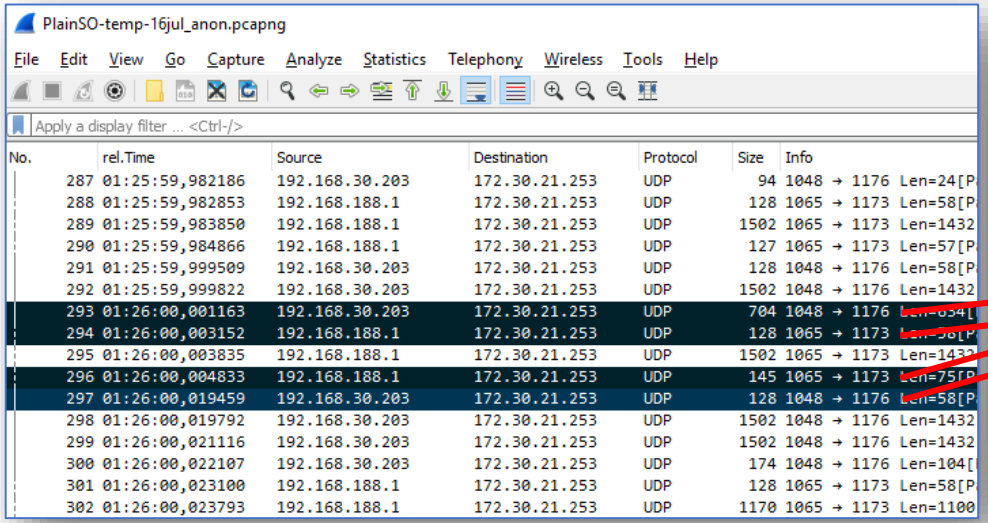
SO

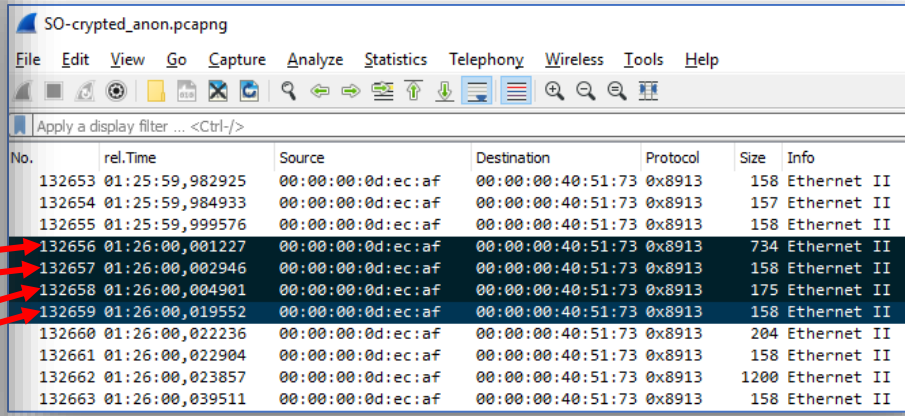
HQ

				Protocol	Size	Info
				TCP	99	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591
				TCP	82	[TCP Previous segment not captured] 8015 → 4160 [ACK] S
30035	92.876364	192.168.201.34	172.18.86.68	TCP	99	[TCP Retransmission] 8015 → 4160 [PSH, ACK] Seq=7726394
30123	93.139440	172.18.86.68	192.168.201.34	TCP	82	4160 → 8015 [ACK] Seq=3749591872 Ack=772639459 Win=6548
30623	94.679289	172.18.86.68	192.168.201.34	TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win
30627	94.695210	192.168.201.34	172.18.86.68	TCP	99	8015 → 4160 [PSH, ACK] Seq=772639459 Ack=3749591889 Win
30684	94.849299	172.18.86.68	192.168.201.34	TCP	82	4160 → 8015 [ACK] Seq=3749591889 Ack=772639476 Win=6546
31201	96.496189	172.18.86.68	192.168.201.34	TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591889 Ack=772639476 Win
31212	96.519043	192.168.201.34	172.18.86.68	TCP	99	8015 → 4160 [PSH, ACK] Seq=772639476 Ack=3749591906 Win
31257	96.659688	172.18.86.68	192.168.201.34	TCP	82	4160 → 8015 [ACK] Seq=3749591906 Ack=772639493 Win=6545
31468	98.311925	172.18.86.68	192.168.201.34	TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591906 Ack=772639493 Win
31478	98.671307	172.18.86.68	192.168.201.34	TCP	99	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591
31498	99.375314	172.18.86.68	192.168.201.34	TCP	99	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591
31542	100.582388	172.18.86.68	192.168.201.34	TCP	99	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591
31575	101.890063	172.18.86.68	192.168.201.34	TCP	99	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591
31609	103.197818	172.18.86.68	192.168.201.34	TCP	116	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591
31657	105.611710	172.18.86.68	192.168.201.34	TCP	133	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591
31782	110.539975	172.18.86.68	192.168.201.34	TCP	150	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591

Remember:

Mapping Plaintext to encrypted capture





Match plain to encrypted

No.	rel.Time	Source	Destination	Protocol	Size	Info
31729	01:27:37,458322	192.168.30.203	172.30.21.253	UDP	869	1048 → 1176 Len=799[Pac
31730	01:27:37,459943	192.168.188.1	172.30.21.253	UDP	128	1065 → 1173 Len=58[Pack
31731	01:27:37,460592	192.168.188.1	172.30.21.253	UDP	1070	1065 → 1173 Len=1000[Pa
31732	01:27:37,461248	172.18.86.68	192.168.201.34	TCP	99	4160 → 8015 [PSH, ACK]
31733	01:27:37,476249	192.168.30.203	172.30.21.253	UDP	128	1048 → 1176 Len=58[Pack
31734	01:27:37,476620	192.168.30.203	172.30.21.253	UDP	1502	1048 → 1176 Len=1432[Pa
31735	01:27:37,477954	192.168.30.203	172.30.21.253	UDP	1329	1048 → 1176 Len=1259[Pa
31736	01:27:37,478912	192.168.201.34	172.18.86.68	TCP	99	8015 → 4160 [PSH, ACK]
31737	01:27:37,480241	192.168.188.1	172.30.21.253	UDP	128	1065 → 1173 Len=58[Pack
31738	01:27:37,480616	192.168.188.1	172.30.21.253	UDP	1502	1065 → 1173 Len=1432[Pa
31739	01:27:37,481594	192.168.188.1	172.30.21.253	UDP	112	1065 → 1173 Len=42[Pack
31740	01:27:37,484236	10.62.210.18				
31741	01:27:37,496216	192.168.30.203				

SO

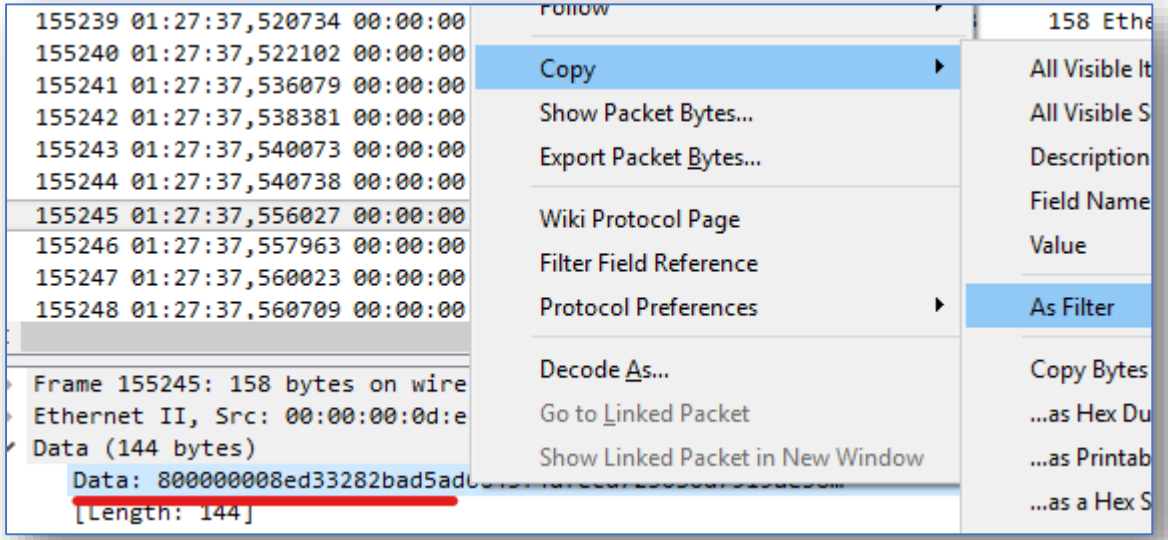
SO

No.	rel.Time	Source	Destination	Protocol	Size	Info
155223	01:27:37,458520	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	899	Ethernet II
155224	01:27:37,459871	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
155225	01:27:37,460519	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1100	Ethernet II
155226	01:27:37,461243	00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	129	Ethernet II
155227	01:27:37,476178	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
155228	01:27:37,478095	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1359	Ethernet II
155229	01:27:37,478840	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	129	Ethernet II
155230	01:27:37,480174	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
155231	01:27:37,481835	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	142	Ethernet II
155232	01:27:37,484165	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	90	Ethernet II
155233	01:27:37,496145	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II

Match encrypted

Easy using data.data and frame size

!! Attention !!
! Timestamp !



Match encrypted

No.	rel.Time	Source	Destination	Protocol	Size	Info
155220	01:27:37,440882	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1242	Ethernet II
155221	01:27:37,455527	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	988	Ethernet II
155222	01:27:37,456213	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
155223	01:27:37,458520	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	899	Ethernet II
155224	01:27:37,459871	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
155225	01:27:37,460519	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1100	Ethernet II
155226	01:27:37,461243	00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	129	Ethernet II
155227	01:27:37,476178	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
155228	01:27:37,478095	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1359	Ethernet II
155229	01:27:37,478840	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	129	Ethernet II
155230	01:27:37,480174	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
155231	01:27:37,481835	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	142	Ethernet II
155232	01:27:37,484165	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	90	Ethernet II

SO

HQ

		Destination	Protocol	Size	Info
154970	01:27:33,863818	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1242	Ethernet II
154971	01:27:33,877561	00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	129	Ethernet II
154972	01:27:33,878123	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	988	Ethernet II
154973	01:27:33,878126	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
154974	01:27:33,881388	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	899	Ethernet II
154975	01:27:33,881703	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
154976	01:27:33,883558	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1100	Ethernet II
154977	01:27:33,898107	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
154978	01:27:33,901479	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1359	Ethernet II
154979	01:27:33,901484	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	129	Ethernet II
154980	01:27:33,902122	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
154981	01:27:33,904229	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	142	Ethernet II
154982	01:27:33,905860	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	90	Ethernet II

Match encrypted to plain

ng on HQ encryption

No.	rel.Time	Source	Destination	Protocol	Size	Info
154970	01:27:33,863818	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1242	Ethernet II
154971	01:27:33,877561	00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	129	Ethernet II
154972	01:27:33,878123	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	988	Ethernet II
154973	01:27:33,878126	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
154974	01:27:33,881388	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	899	Ethernet II
154975	01:27:33,881703	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
154976	01:27:33,883558	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1100	Ethernet II
154977	01:27:33,898107	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
154978	01:27:33,901479	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1359	Ethernet II
154979	01:27:33,901484	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	129	Ethernet II
154980	01:27:33,902122	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
154981	01:27:33,904229	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	142	Ethernet II
154982	01:27:33,905860	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	90	Ethernet II

HQ

HQ

No.	rel.Time	Source	Destination	Protocol	Size	Info
31468	01:27:33,877555	172.18.86.68	192.168.201.34	TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591906 Ack=7
31469	01:27:34,004642	10.88.78.188	224.0.0.2	HSRP	92	Hello (state Active)
31470	01:27:34,022851	172.26.61.205	224.0.0.2	HSRP	92	Hello (state Active)
31476	01:27:34,068518	172.27.252.17	224.0.0.2	HSRP	92	Hello (state Standby)
31477	01:27:34,207227	10.183.63.7	224.0.0.2	HSRP	92	Hello (state Standby)
31478	01:27:34,236937	172.18.86.68	192.168.201.34	TCP	99	[TCP Retransmission] 4160 → 8015 [PSH, ACK]
31479	01:27:34,240389	172.24.142.189	224.0.0.5	OSPF	134	[Packet size limited during capture]
31480	01:27:34,293795	10.248.225.53	192.168.201.34	TCP	99	[TCP Retransmission] 4452 → 8015 [PSH, ACK]
31481	01:27:34,341448	10.149.218.232	224.0.0.2	HSRP	92	Hello (state Standby)
31494	01:27:34,525970	192.168.231.241	224.0.0.2	HSRP	92	Hello (state Standby)
31495	01:27:34,638918	172.29.127.49	224.0.0.2	HSRP	92	Hello (state Active)
31496	01:27:34,648381	172.30.21.253	192.168.30.203	TCP	142	[TCP Retransmission] 1157 → 1756 [PSH, ACK]
31497	01:27:34,722857	10.1.208.90	224.0.0.2	HSRP	92	Hello (state Active)
31498	01:27:34,940944	172.18.86.68	192.168.201.34	TCP	99	[TCP Retransmission] 4160 → 8015 [PSH, ACK]

Go for the root cause!

- We saw an increase of 30 byte on the encryption links
- This makes 90+4 to 1534+4 our valid LAN based frame size
- Analyze the sub-64byte frames
- Start RE-ing the payloads of the small frames (**click along!!**)

?!?

Protocol	Size	Info
0x8913	906	Ethernet II
0x8913	158	Ethernet II
0x8913	214	Ethernet II
0x8913	129	Ethernet II
0x8913	94	Ethernet II
0x8913	94	Ethernet II
0x8913	94	Ethernet II
0x8913	185	Ethernet II
0x8913	94	Ethernet II
0x8913	86	Ethernet II
0x8913	158	Ethernet II
0x8913	884	Ethernet II
0x8913	158	Ethernet II
0x8913	225	Ethernet II

Dissect the sub-64 frames

- There is a variety of frames too **small** to be legitimate, encrypted traffic from the LAN sides

```
# tshark -r SO-crypted_anon.pcapng -Y "frame.len<90"
-Tfields -e frame.len | sort | uniq -c | sort
  20 80
  77 72
  80 78
1317 76
1754 66
1769 60
2345 84
9921 86
```

Dissect the sub-64 frames

e.g. tshark -r SO-crypted_anon.pcapng -Y "frame.len==86" -Tfields -e data | more

```
80000000bc667a65e76ad40319aa664c4721d728fc59a5f5c98245c09e79df93b95f467ccac4cf5e470eb478b86ad63df4e648a48750f99
8000000009851381b45ab33e242b869883b3f489c544973a06c724a96c4a7c934ba36717ceeca62af2c25db644d0fbeb4c696b64cabe8712
8000000006e2f06b44b950017efc5c3d16be01ab888b49093f0b068f3403e9a6eec690d318eda9d0db680907a883669ebbaf233656ee8759
80000000cc2197ebceac597c660eb363e1a5922d01ae4ad37782f8a897079b36dd1bb49108c36b17a432314fae8938bd7adfc8955b99284
8000000030a3d1db1ccc83c737a56b98ab5db8bfd1aa976713261259719e60de556ee8a761ea69d80322abee66bbd8f880e402e03eac969
8000000062dc7bb69d4e714fa9a5a551a5f190c9528bd51bd81cbef9182b9785e4036e7591304a92865f79a0facbfa61508f7ff5662ad04
800000003f79ecf04dc50f2958859f52a6e38fd153a032f98e780b88f7f44cf99eb857a9b93cb289db08199550da03e1f7d6eedf69bd546
80000000d72c2de582e239a6b738f067290c2351172f6cee58ec2426d6271e20ca9d8e7d80775e4046e8086beb2e28f09cea3f14a2cd9ab
8000000052ca03daba7b7d7d7f9c41d5c6be80d31f96300a62ed1ec0cff63338ec5d55890a41b12339f7cdc3ae63d7e166f83a76f21deda
8000000457161f7eaec7cc3bf1103a896c5bb49cfacaadbdf8da4b8f502511dd11878678112dbbec469e466224e2b44ad43975abc7d979
8000000061cbb283e5601c949fc84c3e257b8260a430c45e01962e535ba175994ae3f930475ce4d6f8c5daa9a4b737bb6b12d8b5d235fcd
80000000c35cef0182b4ec87728fd6b2ebc4a4f77f75a6e93893ce5106a710a92188134436760ca7ac17432bef6df8215389ba407050c03
8000000055dcd6c42b7cb9d88ded78769b2c53e3d63f344023024df401728c9fec73b85178ddba7565b73b3d3d56174828dd9a876f46f41
```


Dissect the sub-64 frames

tshark -r SO-crypted_anon.pcapng -Y "frame.len==84" -Tfields -e data | more

```
300000000000000405173000000decaf080045000034c67640004006369300a5acf240a2b5a11041007d1e2a91e7baaf10004801080003b00000000101080a04c98e0306572ce3
300000000000000decaf000000405173080045000034395b00007a06c9ae0a2b5a110a5acf2427d80415b470ecdc6edcc89a801000fc6d4100000101080a06572cee04c98e05
300000000000000405173000000decaf080045000034c67940004006369000a5acf240a2b5a11041527d86edcc89ab470ed2180108000edef00000101080a04c98e0d06572cee
300000000000000405173000000decaf080045000034c68940004006368000a5acf240a2b5a11040f07d1022ccb3a955fe2178010800000965c00000101080a04c993f3065732d4
300000000000000405173000000decaf080045000034c69b40004006366e0a5acf240a2b5a11040f07d1022ccc54955fe35f8010800093e500000101080a04c993fd065732df
300000000000000405173000000decaf080045000034c6ad40004006365c0a5acf240a2b5a11040f07d1022ccd6e955fe4a78010800091f000000101080a04c99407065732e9
300000000000000405173000000decaf080045000034c6dc40004006362d0a5acf240a2b5a11040f07d1022ccfa2955fe737801080008c7700000101080a04c99425065732ff
300000000000000405173000000decaf080045000034c6e140004006362800a5acf240a2b5a11041007d1e2a91f32aaf100e9801080002e2e00000101080a04c999c5065738a3
300000000000000decaf000000405173080045000034f1fa00007a06110f0a2b5a110a5acf2427d80415b470ef606edccdac801000fd4e2300000101080a065738ae04c999cc
300000000000000405173000000decaf080045000034c6e640004006362300a5acf240a2b5a11041527d86edccdacb470efa580108000cecd00000101080a04c999d9065738ae
300000000000000405173000000decaf080045000034c6eb40004006361e0a5acf240a2b5a11041007d1e2a91fe9aaf101ce8010800008b900000101080a04c9a59106574464
300000000000000decaf000000405173080045000034641800007a069ef10a2b5a110a5acf2427d80415b470f1e46edcd2be80100100f2f0100000101080a0657446f04c9a594
```

Dissect the sub-64 frames

tshark -r SO-crypted_anon.pcapng -Y "frame.len==60" -Tfields -e data | more

Dissect the sub-64 frames

tshark -r SO-crypted_anon.pcapng -Y "frame.len==66" -Tfields -e data | more

Dissect the sub-64 frames

```
tshark -r SO-crypted_anon.pcapng -Y "frame.len==66" -Tfields -e data | cut -c 25-28 |
grep –v "0000" > increments.txt
```

```
0207
0207
0207
0207
0208
0208
0208
0208
0209
0209
0209
0209
```

```
020a
020a
020a
020a
020b
020b
020b
020b
020c
020c
020c
020c
```

```
020d
020d
020d
020d
020e
020e
020e
020e
020f
020f
020f
020f
```

```
0210
0210
0210
0210
0210
0211
0212
0211
0212
0212
0213
0212
```

```
0213
0213
0214
0213
0214
0214
0215
0214
0215
0215
0216
0215
```

```
0216
0216
0217
0216
0217
0217
0218
0217
0218
0218
0219
0218
```

Dissect the sub-64 frames

- Step 1:
  tshark -r SO-crypted_anon.pcapng -Y "frame.len==66" -Tfields -e data -e eth.src -e frame.time
- Locate increment, MAC address and timestamp
- Step 2:
  tshark -r SO-crypted_anon.pcapng -Y "frame.len==66" -Tfields -e data -e eth.src -e frame.time | cut -c 25-28,105-122,136-144 | grep –v "0000"

Conclusion

- At around 01:27:30 the HQ device resends the expired number and jumps up two increments after that
- The devices obviously **cannot** recover from that state later on

	B	C	D
35	00:00:00:40:51:73	01:25:29	527
36	00:00:00:0d:ec:af	01:25:29	527
37	00:00:00:40:51:73	01:25:58	527
38	00:00:00:0d:ec:af	01:25:59	527
39	00:00:00:40:51:73	01:26:31	528
40	00:00:00:0d:ec:af	01:26:31	528
41	00:00:00:40:51:73	01:27:01	528
42	00:00:00:0d:ec:af	01:27:01	528
43	00:00:00:40:51:73	01:27:33	528
44	00:00:00:0d:ec:af	01:27:33	529
45	00:00:00:40:51:73	01:27:41	530
46	00:00:00:0d:ec:af	01:28:03	529
47	00:00:00:40:51:73	01:28:11	530
48	00:00:00:0d:ec:af	01:28:35	530
49	00:00:00:40:51:73	01:28:43	531
50	00:00:00:0d:ec:af	01:29:05	530

Results:

- Packet drops on WAN link exist, but not causing big trouble
- Retransmissions always affect at least 2 packets, due to encryption devices
- Crypto synchronization for some reason broken between the devices -> Case to handle for the vendor

Mail: landi@packet-foo.com
Web: blog.packet-foo.com
Twitter: @packetfoo