



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.



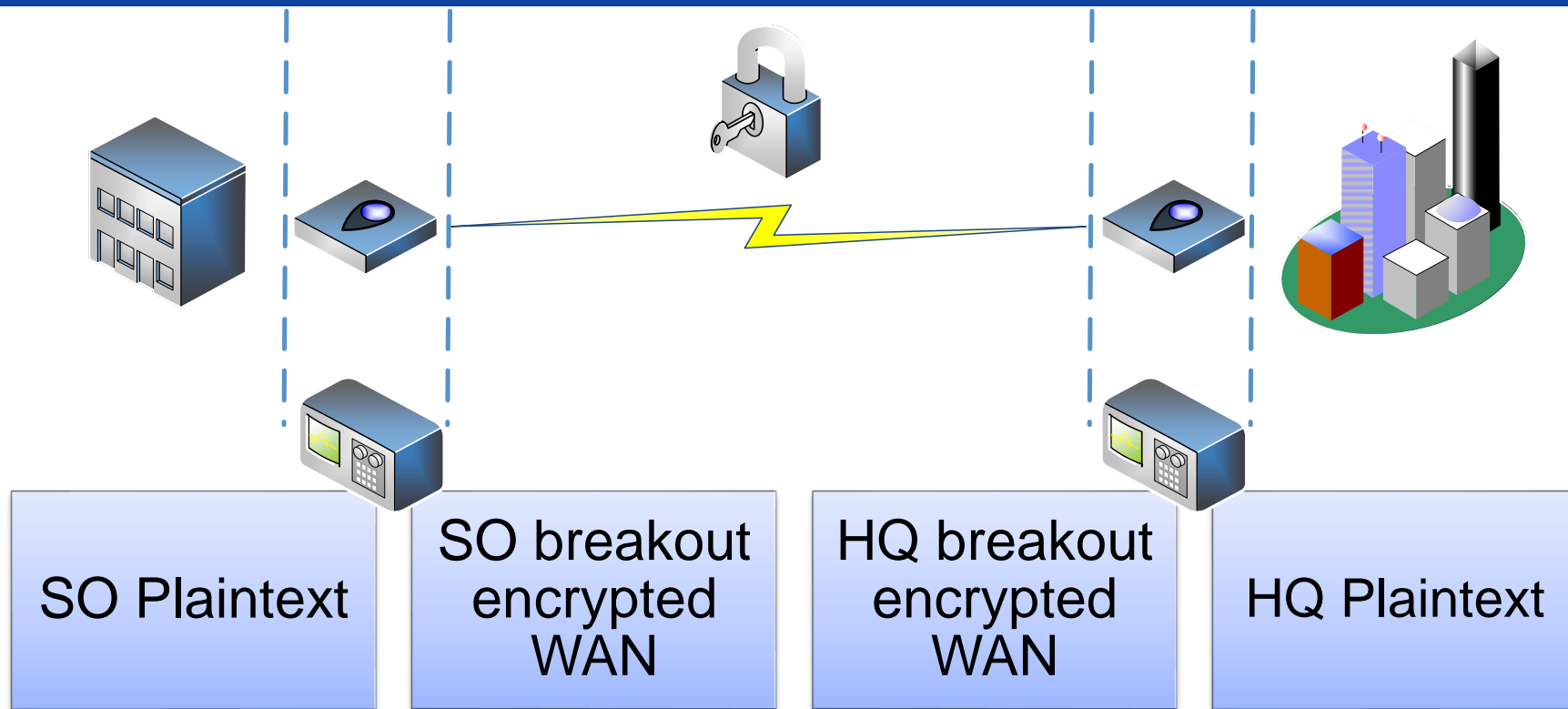
Situation



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



2 Sites, 1 WAN link



Issues with encryption



PlainSO-temp-16jul_anon.pcapng

LAN SO

No.	rel.Time	Source	Destination	Protocol	Size	Info
1	0.000000	192.168.30.203	192.168.188.1	UDP	1492	1805 - 1173 Len=512(Packet size limited during capture)
2	0.000962	192.168.30.203	192.168.188.1	UDP	1176	1805 - 1173 Len=512(Packet size limited during capture)
3	0.001994	192.168.188.1	192.168.30.203	UDP	128	1804 - 1176 Len=581(Packet size limited during capture)
4	0.002127	192.168.188.1	192.168.30.203	UDP	1502	1804 - 1176 Len=581(Packet size limited during capture)
5	0.013101	192.168.30.203	192.30.21.253	UDP	666	1048 - 1176 Len=596(Packet size limited during capture)
6	0.018633	192.168.30.203	192.30.21.253	UDP	128	1805 - 1173 Len=581(Packet size limited during capture)
7	0.019964	192.168.30.203	192.30.21.253	UDP	1502	1805 - 1173 Len=581(Packet size limited during capture)
8	0.021962	192.168.188.1	192.30.21.253	UDP	128	1805 - 1173 Len=581(Packet size limited during capture)
9	0.022277	192.168.188.1	192.30.21.253	UDP	1502	1805 - 1173 Len=581(Packet size limited during capture)
10	0.023080	192.168.188.1	192.30.21.253	UDP	97	1805 - 1173 Len=27(Packet size limited during capture)
11	0.032628	192.168.30.203	192.30.21.253	UDP	128	1804 - 1176 Len=581(Packet size limited during capture)
12	0.035081	192.168.30.203	192.30.21.253	UDP	1502	1804 - 1176 Len=581(Packet size limited during capture)
13	0.039915	192.168.30.203	192.30.21.253	UDP	1502	1804 - 1176 Len=581(Packet size limited during capture)
14	0.040907	192.168.30.203	192.30.21.253	UDP	254	1848 - 1176 Len=181(Packet size limited during capture)
15	0.041899	192.168.188.1	192.30.21.253	UDP	1168	1805 - 1173 Len=581(Packet size limited during capture)
16	0.042228	192.168.188.1	192.30.21.253	UDP	1168	1805 - 1173 Len=581(Packet size limited during capture)
17	0.051756	172.18.86.68	192.168.201.34	TCP	99	4160 - 8015 [PSH, ACK] Seq=3749591805 Ack=7726385
18	0.054235	192.168.30.203	192.30.21.253	UDP	128	1804 - 1176 Len=581(Packet size limited during capture)
19	0.055558	192.168.30.203	192.30.21.253	UDP	1502	1804 - 1176 Len=581(Packet size limited during capture)
20	0.055884	192.168.30.203	192.30.21.253	UDP	1163	1848 - 1176 Len=1093(Packet size limited during capture)

Frame 11: 128 bytes on wire (1024 bits), 70 bytes captured (560 bits) on Interface 3
Ethernet II, Src: r21a0:c0ca:054b, Dst: f2:6c:1b:dc:8b:6d
Internet Protocol Version 4, Src: 192.168.30.203, Dst: 192.30.21.253
Generic Routing Encapsulation (GRE)
Internet Protocol Version 4, Src: 192.168.188.1, Dst: 192.30.21.253
User Datagram Protocol, Src Port: 1805, Dst Port: 1173

PlainHQ-temp-16jul_anon.pcapng

LAN HQ

No.	rel.Time	Source	Destination	Protocol	Size	Info
1	0.000000	192.168.30.203	192.30.21.253	UDP	1492	1805 - 1173 Len=512(Packet size limited during capture)
2	0.000001	192.168.30.203	192.30.21.253	UDP	1176	1805 - 1173 Len=512(Packet size limited during capture)
3	0.000001	192.168.188.1	192.30.21.253	UDP	128	1804 - 1176 Len=581(Packet size limited during capture)
4	0.002111	192.168.188.1	192.30.21.253	UDP	1502	1804 - 1176 Len=581(Packet size limited during capture)
5	0.016118	192.168.30.203	192.30.21.253	UDP	666	1048 - 1176 Len=596(Packet size limited during capture)
6	0.018041	192.168.30.203	192.30.21.253	UDP	128	1805 - 1173 Len=581(Packet size limited during capture)
7	0.018087	192.168.30.203	192.30.21.253	UDP	1502	1805 - 1173 Len=581(Packet size limited during capture)
8	0.019785	192.168.188.1	192.30.21.253	UDP	128	1805 - 1173 Len=581(Packet size limited during capture)
9	0.021319	192.168.188.1	192.30.21.253	UDP	1502	1805 - 1173 Len=581(Packet size limited during capture)
10	0.022141	192.168.188.1	192.30.21.253	UDP	97	1805 - 1173 Len=27(Packet size limited during capture)
11	0.036117	192.168.30.203	192.30.21.253	UDP	128	1804 - 1176 Len=581(Packet size limited during capture)
12	0.038518	192.168.30.203	192.30.21.253	UDP	1502	1805 - 1173 Len=581(Packet size limited during capture)
13	0.039903	192.168.30.203	192.30.21.253	UDP	1502	1804 - 1176 Len=581(Packet size limited during capture)
14	0.039905	192.168.30.203	192.30.21.253	UDP	254	1848 - 1176 Len=181(Packet size limited during capture)
15	0.039906	192.168.188.1	192.30.21.253	UDP	1168	1805 - 1173 Len=581(Packet size limited during capture)
16	0.041577	192.168.188.1	192.30.21.253	UDP	1168	1805 - 1173 Len=581(Packet size limited during capture)
17	0.048200	172.18.86.68	192.168.201.34	TCP	99	4160 - 8015 [PSH, ACK] Seq=3749591805
18	0.056135	192.168.30.203	192.30.21.253	UDP	128	1804 - 1176 Len=581(Packet size limited during capture)
19	0.058500	192.168.30.203	192.30.21.253	UDP	1502	1804 - 1176 Len=581(Packet size limited during capture)
20	0.059381	192.168.30.203	192.30.21.253	UDP	1163	1848 - 1176 Len=1093(Packet size limited during capture)

Frame 14: 99 bytes on wire (792 bits), 82 bytes captured (656 bits) on Interface 0
Ethernet II, Src: f21a:c0:c0:08:65, Dst: f21a:c0:c0:8b:6d
Internet Protocol Version 4, Src: 172.18.86.68, Dst: 192.168.201.34
Generic Routing Encapsulation (GRE)
Internet Protocol Version 4, Src: 192.168.188.1, Dst: 192.30.21.253
Transmission Control Protocol, Src Port: 4160, Dst Port: 8015, Seq: 3749591805, Ack: 7726384959, Len: 17

50-crypted_anon.pcapng

WAN SO

No.	rel.Time	Source	Destination	Protocol	Size	Info
1	0.000000	00:00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	129	Ethernet II
2	0.102499	00:00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	122	Ethernet II
3	0.117693	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
4	0.119357	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1438	Ethernet II
5	0.128939	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
6	0.121282	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1223	Ethernet II
7	0.137625	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
8	0.139298	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1446	Ethernet II
9	0.140961	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
10	0.142628	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	215	Ethernet II
11	0.156039	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
12	0.157559	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
13	0.159272	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	859	Ethernet II
14	0.160956	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II

HQ-crypted_anon.pcapng

WAN HQ

No.	rel.Time	Source	Destination	Protocol	Size	Info
1	0.000000	00:00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	129	Ethernet II
2	0.002999	00:00:00:00:40:51:73	00:00:00:0d:ec:af	0x8913	158	Ethernet II
3	0.006512	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1491	Ethernet II
4	0.006514	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
5	0.008250	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1325	Ethernet II
6	0.011112	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	129	Ethernet II
7	0.022998	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
8	0.025826	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	907	Ethernet II
9	0.026392	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
10	0.027852	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1066	Ethernet II
11	0.043115	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
12	0.045932	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	841	Ethernet II
13	0.046392	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
14	0.048658	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	241	Ethernet II



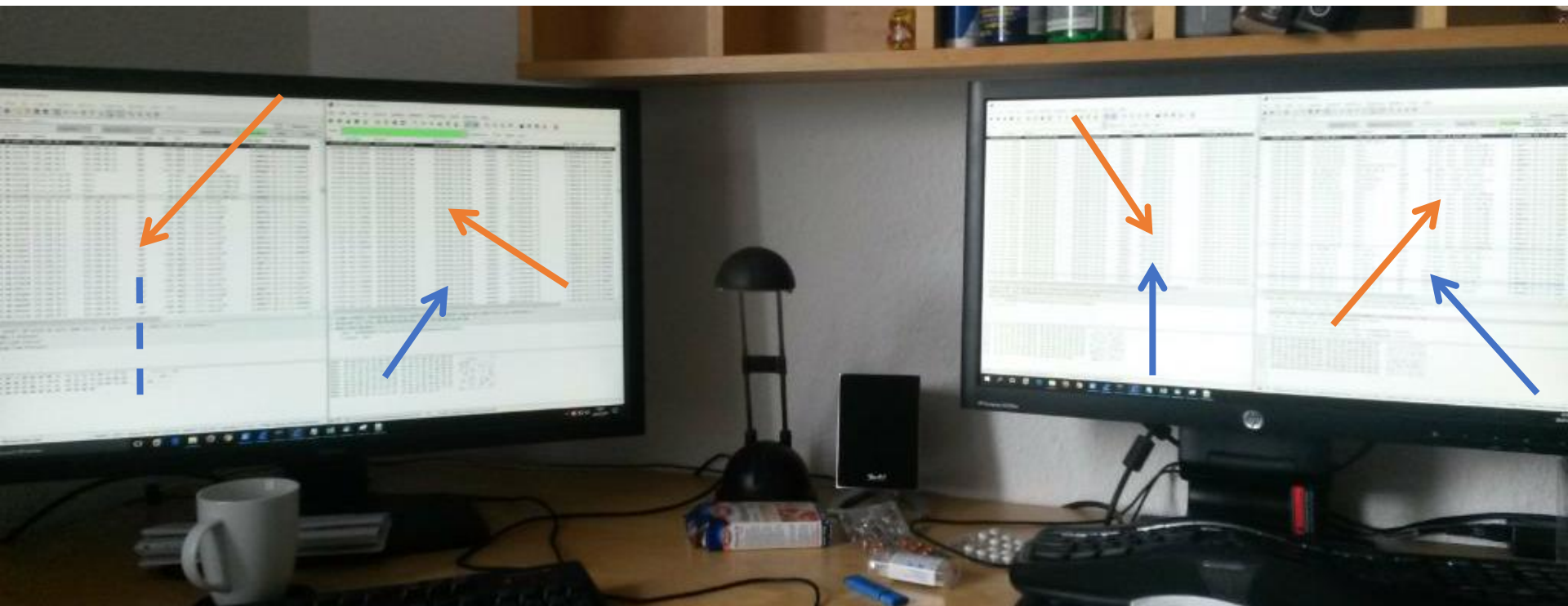
Issues with encryption



- Procedure:
 - Start with plaintext -> isolate problem
- If plain1 \neq 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



LAN_SO_anon.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.addr eq 172.28.63.209 and ip.addr eq 10.158.228.227) and (tcp.port eq 56650 and tcp.port eq 49166)

No.	rel.Time	Source	Destination	Protocol	Size	Info
92427	568.224...	10.158.228.227	172.28.63.209	TCP	60	49166 → 56650 [ACK] Seq=2489311937 Ack=1111956001 Win=12
92428	568.225...	172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112020197 Ack=2489311937 Win=65
92429	568.226...	10.158.228.227	172.28.63.209	TCP	60	49166 → 56650 [ACK] Seq=2489311937 Ack=1111957757 Win=12
92430	568.226...	172.28.63.209	10.158.228.227	TCP	450	56650 → 49166 [PSH, ACK] Seq=1112021557 Ack=2489311937 W
92431	568.227...	172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112021953 Ack=2489311937 Win=65

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=2
92426	14:46:31,156907	172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112018837 Ack=2
92427	14:46:31,157388	10.158.228.227	172.28.63.209	TCP	60	49166 → 56650 [ACK] Seq=2489311937 Ack=1
92428	14:46:31,158212	172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112020197 Ack=2
92429	14:46:31,159072	10.158.228.227	172.28.63.209	TCP	60	49166 → 56650 [ACK] Seq=2489311937 Ack=1
92430	14:46:31,159209	172.28.63.209	10.158.228.227	TCP	450	56650 → 49166 [PSH, ACK] Seq=1112021557 Ack=2
92431	14:46:31,159546	172.28.63.209	10.158.228.227	TCP	1414	56650 → 49166 [ACK] Seq=1112021953 Ack=2

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	480	Ethernet II
93059	568.222706	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	90	Ethernet II
93060	568.223700	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
93061	568.223744	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	568.224780	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

Use data data to match content and frame size

SO

67250	359.576394	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1444	Ethernet II
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



Seeing a pattern?



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 ...



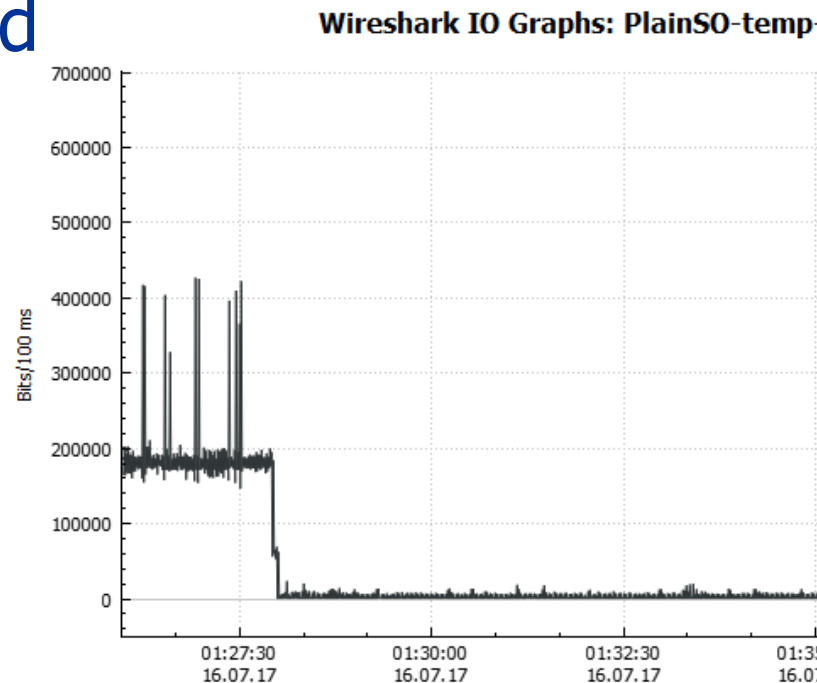
So the sniffers were kept running with ring buffers active to capture the upcoming at least 24-48 hours of traffic



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] Seq=3749591872 Ack=772639459 Win=6546 Len=0
29427	91.137595	192.168.201.34	172.18.86.68	TCP	82	[TCP Dup ACK 29344#1] 8015 → 4160 [ACK] Seq=772639459 Win=0 Len=0
29989	92.877680	192.168.201.34	172.18.86.68	TCP	99	[TCP Retransmission] 8015 → 4160 [PSH, ACK] Seq=772639459 Win=6546 Len=0
30078	93.147447	172.18.86.68	192.168.201.34	TCP	82	4160 → 8015 [ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
30573	94.687145	172.18.86.68	192.168.201.34	TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
30577	94.697704	192.168.201.34	172.18.86.68	TCP	99	8015 → 4160 [PSH, ACK] Seq=772639459 Ack=3749591889 Win=6546 Len=0
30637	94.857261	172.18.86.68	192.168.201.34	TCP	82	4160 → 8015 [ACK] Seq=3749591889 Ack=772639476 Win=6546 Len=0
31153	96.503958	172.18.86.68	192.168.201.34	TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591889 Ack=772639476 Win=6546 Len=0
31162	96.520726	192.168.201.34	172.18.86.68	TCP	99	8015 → 4160 [PSH, ACK] Seq=772639476 Ack=3749591906 Win=6546 Len=0
31207	96.667698	172.18.86.68	192.168.201.34	TCP	82	4160 → 8015 [ACK] Seq=3749591906 Ack=772639493 Win=6546 Len=0
31732	98.320001	172.18.86.68	192.168.201.34	TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591906 Ack=772639493 Win=6546 Len=0
31736	98.337665	192.168.201.34	172.18.86.68	TCP	99	8015 → 4160 [PSH, ACK] Seq=772639493 Ack=3749591923 Win=6546 Len=0
31848	98.679474	172.18.86.68	192.168.201.34	TCP	99	[TCP Spurious Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
31850	98.681088	192.168.201.34	172.18.86.68	TCP	82	[TCP Dup ACK 31736#1] 8015 → 4160 [ACK] Seq=772639510 Win=0 Len=0
32083	99.383260	172.18.86.68	192.168.201.34	TCP	99	[TCP Spurious Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
32084	99.385284	192.168.201.34	172.18.86.68	TCP	82	[TCP Dup ACK 31736#2] 8015 → 4160 [ACK] Seq=772639510 Win=0 Len=0
32364	100.277539	192.168.201.34	172.18.86.68	TCP	99	[TCP Retransmission] 8015 → 4160 [PSH, ACK] Seq=772639476 Win=6546 Len=0
32465	100.590346	172.18.86.68	192.168.201.34	TCP	99	[TCP Spurious Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
32466	100.592307	192.168.201.34	172.18.86.68	TCP	82	[TCP Dup ACK 31736#3] 8015 → 4160 [ACK] Seq=772639510 Win=0 Len=0

HQ

SO

Protocol	Size	Info
TCP	99	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
TCP	82	[TCP Previous segment not captured] 8015 → 4160 [ACK] Seq=772639459 Win=0 Len=0
TCP	99	[TCP Retransmission] 8015 → 4160 [PSH, ACK] Seq=772639476 Win=6546 Len=0
TCP	82	4160 → 8015 [ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
TCP	99	8015 → 4160 [PSH, ACK] Seq=772639459 Ack=3749591889 Win=6546 Len=0
TCP	82	4160 → 8015 [ACK] Seq=3749591889 Ack=772639476 Win=6546 Len=0
TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591889 Ack=772639476 Win=6546 Len=0
TCP	99	8015 → 4160 [PSH, ACK] Seq=772639476 Ack=3749591906 Win=6546 Len=0
TCP	99	8015 → 4160 [PSH, ACK] Seq=772639476 Ack=3749591906 Win=6546 Len=0
TCP	82	4160 → 8015 [ACK] Seq=3749591906 Ack=772639493 Win=6546 Len=0
TCP	99	4160 → 8015 [PSH, ACK] Seq=3749591906 Ack=772639493 Win=6546 Len=0
TCP	99	8015 → 4160 [PSH, ACK] Seq=772639493 Ack=3749591923 Win=6546 Len=0
TCP	99	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
TCP	99	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
TCP	99	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
TCP	99	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
TCP	116	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
TCP	133	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0
TCP	150	[TCP Retransmission] 4160 → 8015 [PSH, ACK] Seq=3749591872 Ack=772639459 Win=6546 Len=0



Remember:



Mapping Plaintext to encrypted capture

PlainSO-temp-16jul_anon.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... (Ctrl-/>

No.	rel.Time	Source	Destination	Protocol	Size	Info
287	01:25:59,982186	192.168.30.203	172.30.21.253	UDP	94	1048 → 1176 Len=24[P
288	01:25:59,982853	192.168.188.1	172.30.21.253	UDP	128	1065 → 1173 Len=58[P
289	01:25:59,983850	192.168.188.1	172.30.21.253	UDP	1502	1065 → 1173 Len=1432
290	01:25:59,984866	192.168.188.1	172.30.21.253	UDP	127	1065 → 1173 Len=57[P
291	01:25:59,999509	192.168.30.203	172.30.21.253	UDP	128	1048 → 1176 Len=58[P
292	01:25:59,999822	192.168.30.203	172.30.21.253	UDP	1502	1048 → 1176 Len=1432
293	01:26:00,001163	192.168.30.203	172.30.21.253	UDP	704	1048 → 1176 Len=654[P
294	01:26:00,003152	192.168.188.1	172.30.21.253	UDP	128	1065 → 1173 Len=58[P
295	01:26:00,003835	192.168.188.1	172.30.21.253	UDP	1502	1065 → 1173 Len=1432
296	01:26:00,004833	192.168.188.1	172.30.21.253	UDP	145	1065 → 1173 Len=75[P
297	01:26:00,019459	192.168.30.203	172.30.21.253	UDP	128	1048 → 1176 Len=58[P
298	01:26:00,019792	192.168.30.203	172.30.21.253	UDP	1502	1048 → 1176 Len=1432
299	01:26:00,021116	192.168.30.203	172.30.21.253	UDP	1502	1048 → 1176 Len=1432
300	01:26:00,022107	192.168.30.203	172.30.21.253	UDP	174	1048 → 1176 Len=104[P
301	01:26:00,023100	192.168.188.1	172.30.21.253	UDP	128	1065 → 1173 Len=58[P
302	01:26:00,023793	192.168.188.1	172.30.21.253	UDP	1170	1065 → 1173 Len=1100

SO-crypted_anon.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... (Ctrl-/>

No.	rel.Time	Source	Destination	Protocol	Size	Info
132653	01:25:59,982925	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
132654	01:25:59,984933	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	157	Ethernet II
132655	01:25:59,999576	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
132656	01:26:00,001227	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	734	Ethernet II
132657	01:26:00,002946	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
132658	01:26:00,004901	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	175	Ethernet II
132659	01:26:00,019552	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
132660	01:26:00,022236	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	204	Ethernet II
132661	01:26:00,022904	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II
132662	01:26:00,023857	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	1200	Ethernet II
132663	01:26:00,039511	00:00:00:0d:ec:af	00:00:00:40:51:73	0x8913	158	Ethernet II



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[Pack
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				

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

SO

SO



Match encrypted



Easy using data.data and frame size

!! Attention !!
! Timestamp !

155239 01:27:37,520734 00:00:00
155240 01:27:37,522102 00:00:00
155241 01:27:37,536079 00:00:00
155242 01:27:37,538381 00:00:00
155243 01:27:37,540073 00:00:00
155244 01:27:37,540738 00:00:00
155245 01:27:37,556027 00:00:00
155246 01:27:37,557963 00:00:00
155247 01:27:37,560023 00:00:00
155248 01:27:37,560709 00:00:00

Frame 155245: 158 bytes on wire
Ethernet II, Src: 00:00:00:0d:e
Data (144 bytes)
Data: 800000008ed33282bad5ad...
[Length: 144]

Follow
Copy
Show Packet Bytes...
Export Packet Bytes...
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window

158 Eth
All Visible It
All Visible S
Description
Field Name
Value
As Filter
Copy Bytes
...as Hex Du
...as Printab
...as a Hex S



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

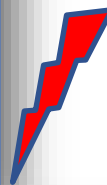


Match encrypted to plain



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

ing on HQ encryption



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	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 S0-encrypted_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-encrypted_anon.pcapng -Y "frame.len==86" -Tfields -e data | more`

```
80000000bc667a65e76ad40319aa664c4721d728fc59a5f5c98245c09e79df93b95f467ccac4cf5e470eb478b86ad63df4e648a48750f99
800000009851381b45ab33e242b869883b3f489c544973a06c724a96c4a7c934ba36717ceeca62af2c25db644d0fbef4c696b64cabe8712
800000006e2f06b44b950017efc5c3d16be01ab888b49093f0b068f3403e9a6eec690d318eda9d0db680907a883669ebbaef233656ee8759
80000000cc2197ebceac597c660eb363e1a5922d01ae4ad37782f8a897079b36dd1bb49108c36b17a432314fae8938bd7adfc8955b99284
8000000030a3d1db1ccc83c737a56b98ab5db8bfd1aa976713261259719e60de556ee8a761ea69d80322abee66bbd8f880e402e03eac969
8000000062dc7bb69d4e714fa9a5a551a5f190c9528bd51bd81cbef9182b9785e4036e7591304a92865f79a0facbfa61508f7ff5662ad04
800000003f79ecf04dc50f2958859f52a6e38fd153a032f98e780b88f7f44cf99eb857a9b93cb289db08199550da03e1f7d6eedf69bd546
80000000d72c2de582e239a6b738f067290c2351172f6cee58ec2426d6271e20ca9d8e7d80775e4046e8086beb2e28f09cea3f14a2cd9ab
8000000052ca03daba7b7d7d7f9c41d5c6be80d31f96300a62ed1ec0cff63338ec5d55890a41b12339f7cdc3ae63d7e166f83a76f21deda
80000000457161f7eaec7cc3bf1103a896c5bb49cfacaadbf8da4b8f502511dd11878678112dbbec469e466224e2b44ad43975abc7d979
8000000061cbb283e5601c949fc84c3e257b8260a430c45e01962e535ba175994ae3f930475ce4d6f8c5daa9a4b737bb6b12d8b5d235fcd
80000000c35cef0182b4ec87728fd6b2ebc4a4f77f75a6e93893ce5106a710a92188134436760ca7ac17432bef6df8215389ba407050c03
8000000055dcd6c42b7cb9d88ded78769b2c53e3d63f344023024df401728c9fec73b85178ddba7565b73b3d3d56174828dd9a876f46f41
```



Dissect the sub-64 frames



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

```
30000000000000405173000000decaf080045000034c6764000400636930a5acf240a2b5a11041007d1e2a91e7baaf10004801080003b000000101080a04c98e0306572ce3
30000000000000decaf000000405173080045000034395b00007a06c9ae0a2b5a110a5acf2427d80415b470ecdc6edcc89a801000fc6d410000101080a06572cee04c98e05
30000000000000405173000000decaf080045000034c6794000400636900a5acf240a2b5a11041527d86edcc89ab470ed2180108000ede00000101080a04c98e0d06572cee
30000000000000405173000000decaf080045000034c6894000400636800a5acf240a2b5a11040f07d1022cc03a955fe21780108000965c00000101080a04c993f3065732d4
30000000000000405173000000decaf080045000034c69b40004006366e0a5acf240a2b5a11040f07d1022cc54955fe35f8010800093e500000101080a04c993fd065732df
30000000000000405173000000decaf080045000034c6ad40004006365c0a5acf240a2b5a11040f07d1022cc6e955fe4a780108000916f00000101080a04c99407065732e9
30000000000000405173000000decaf080045000034c6dc40004006362d0a5acf240a2b5a11040f07d1022ccfa2955fe737801080008c7700000101080a04c99425065732ff
30000000000000405173000000decaf080045000034c6e14000400636280a5acf240a2b5a11041007d1e2a91f32aaf100e98010800021e200000101080a04c999c50657338a3
30000000000000decaf000000405173080045000034f1fa00007a06110f0a2b5a110a5acf2427d80415b470ef606edccdac801000f04e2300000101080a065738ae04c999cc
30000000000000405173000000decaf080045000034c6e64000400636230a5acf240a2b5a11041527d86edccdacb470efa580108000cccd00000101080a04c999d90657338ae
30000000000000405173000000decaf080045000034c6eb40004006361e0a5acf240a2b5a11041007d1e2a91fe9aaf101ce8010800008b900000101080a04c9a59106574464
30000000000000decaf000000405173080045000034641800007a069ef10a2b5a110a5acf2427d80415b470ef1e46edcd2be801001002f0100000101080a0657446f04c9a594
```




Dissect the sub-64 frames



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

```
00000000151002c0010000000000000213010b55b680f831aaa0686764757c60d370c4010de52a09195337734e3b4bd4f609c4603
00000000151002c00100000002060222301011f38966605dbeb23190eaead73d0291401045b33e84c7c68e1d6820aedf2212f966
00000000151002c001000000000002130108218a96c24cab1745703103a77bdb06f4010c2fac9d592659f7bd9f7ff80aad7934b
00000000151002c001000000020602223010407e17d09fcfc73f5622342097a227f44010b4d8e608ed9a53582e24ec64263a2665
00000000151002c0010000000000021301069b5187f73b316cb6947117c0ba0e79b4010f553e3d4407da524e68d5c3fae51c255
00000000151002c0f1000000020702223010d13e4356b6b1cd335a79e6047bdd00164010c274db5c3749db685803fdc5a20f3e40
00000000151002c001000000000002130104411418419eaca974a0389741daa8b7f401041b3122fe1ac66271a1e725a5c203e0d
00000000151002c0f100000002070222301059039c1e6873aae4118321bcc23c52ce4010538467bc62d1e8095539a26871137e79
00000000151002c00100000000000213010f24523eb64e6898ed1bb3d743e2e6cc740107d16b49b1dfee0b3e1abc98d20232bfb
00000000151002c0f1000000020702223010166126865aae20ad8e73949307ae06b0401060969b646c6df9820fc43a59fd40d5fa
00000000151002c001000000000002130100d4aea524b12875962afc833881530104010ca0d0adb58d2030f041e5b6e53a4eaa02
00000000151002c0f10000000207022230107a4b52cc1d9858845fbe0ab6da2cc0bc401049b7d349eadd7097501bd0ff6a19d18a
00000000151002c0010000000000021301006ef9f62d5b3453b65d8da3c2b60048d4010366f9b97d662da9eabbe0e499e259601
00000000151002c0010000000208022230105bdc874ef09eb40c17c3d05cc440f16d401012051bc82c8fa58d86cce88891b95300
00000000151002c00100000000000213010db0ba2bf75b8f5862f29f3055b5aee0c4010df90a1af8a11d2651792071e7225fe2f
00000000151002c001000000020802223010c4ab291811c166ce3d15bb3d02eb7b04010e972a793e89e418fc0af2473392f5776
00000000151002c00100000000000213010e9453ec416553b85e8f568b93cb5361c640103aaaf36c17134b43df48e3853103b6f3b
```



Dissect the sub-64 frames



```
tshark -r SO-encrypted_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-encrypted_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-encrypted_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



Q&A

Mail: landi@packet-foo.com

Web: blog.packet-foo.com

Twitter: [@packetfoo](https://twitter.com/packetfoo)