SIMtrace 2 - Bug #4754

Malformed Packets in Sniff Output

09/16/2020 12:56 AM - connectednow

Status:	New	**Start date:**	09/16/2020
Priority:	Normal	**Due date:**	
Assignee:	connectednow	**% Done:**	0%
Category:	firmware		
Target version:			
Spec Reference:			

Description

Hello,

We have an Ubuntu 20.04 LTS machine that we have set up along with a SIMtrace2 tool updated with the latest firmware.

Once we start a trace, we can capture the trace in Wireshark as well as in the terminal, but in both cases, after a few hundred packets, the data reports as malformed.

Our SIM application requests modem status every 28 seconds, and so there is a good pattern to follow in the trace. The SIM application itself is behaving correctly, and counting these status commands as it should, but the output is just no good. Perhaps the board is running out of memory?

Here is the output from the terminal around when the problem starts:
TPDU: 80 f2 00 00 00 6c 2f
TPDU: 80 f2 00 00 2f 62 2d 82 02 78 21 83 02 7f f0 84 10 a0 00 00 00 87 10 02 ff 34 ff 07 89 31 2e 30 ff 8a 01 05 8b 03 2f 06 1e c6 09 90 01 40 83 01 01 83 01 81 90 00
TPDU: 80 f2 00 00 00 6c 2f
TPDU: 80 f2 00 00 2f 62 2d 82 02 78 21 83 02 7f f0 84 10 a0 00 00 00 87 10 02 ff 34 ff 07 89 31 2e 30 ff 8a 01 05 8b 03 2f 06 1e c6 09 90 01 40 83 01 01 83 01 81 90 00
TPDU: 80 f2 00 00 00 6c 2f
TPDU: 80 f2 00 00 2f 62 2d 82 02 78 21 83 02 7f f0 84 10 a0 00 00 00 87 10 02 ff 34 ff 07 89 31 2e 30 ff 8a 01 05 8b 03 2f 06 1e c6 09 90 01 40 83 01 01 83 01 81 90 00
Card state change: reset de-asserted
Card state change: reset de-asserted
ATR (malformed): 80
ATR (malformed): 6c
ATR (malformed): f2
ATR (malformed): 07
ATR (malformed): 80
ATR (malformed): 00
ATR (malformed): 80
ATR (malformed): 03
ATR (malformed): 91
ATR (malformed): 00
ATR (malformed): 62
ATR (malformed): 80
ATR (malformed): 01
ATR (malformed): 91
ATR (malformed): 80
ATR (malformed): 38
ATR (malformed): 00
ATR (malformed): 80
ATR (malformed): 01
ATR (malformed): 90
ATR (malformed): 80
ATR (malformed): 0e
ATR (malformed): 91
ATR (malformed): 80
ATR (malformed): 80
ATR (malformed): 03
ATR (malformed): 95
ATR (malformed): 45

ATR (malformed): 91
ATR (malformed): 00
ATR (malformed): 31
ATR (checksum error): 30 f3 f3 f3 53 53 63 73 f3 73 f3 9d
TPDU (malformed): 9d
TPDU (malformed): 9d
TPDU (malformed): 9d
TPDU (malformed): 9d e3 63 f3 f3
TPDU (malformed): f3 f3 73 f3 f3
TPDU (malformed): b3 f3 73 f3 73
TPDU (malformed): 33 f3 73 d3 f3
PPS (checksum error): ff fe d7 ff ff 0f
TPDU (malformed): d7 7f 3f 7f 3d bf bf be 7e 3f 7f ff 13 7f 00 76 37 fe b7 ff ff 37 b7 f4 77 7f 3f 7f 3d 7f bf bf 7e 7b 93 9f d7 3f 3f ff 7f 7f f6 ff fe d7 ff ff 0f d7 7f 3f 7f 3d 7f bf bf be 7e 3f 7f ff 13 7f 00 76
TPDU (malformed): fe b7 ff ff b9 f4 f9 7f 3f 7f 3d 7f bf bf 7e 7b 93 55 97 3f 3f ff f5 4a cd 1a c4 b4 08 cd 01 25 51 79 84 0e 1b 57 ea 2b ac 8e 48 22 67 17 97 3e fc 57 e3 45 40 cb 6b fa b1 be a8 d5 7a 61 64 81 7f 38 af 48 fc d3 d1 3b 27 63 34 19 49 e9 26 7b 74 de ef 8b 1f 8a 09 08 0f 10 59 e7 d5 73 2b c6 e2 9a be cd 76 c2 17 f6 ff fe d7 ff ff 0f d7 7f 3f 7f 3d 7f bf bf be 7e 3f 7f ff 13 7f 00 f6 ff fe bc ff ff f7 bc 94 8f 67 7f 6f bf bf be 7e e3 bf 7e ff 13 7f 9f 76 8f fe b7 ff ff 8f b7 f4 cf 7f 3f 7f bd ff bf bf 7e 7b 13 7f 9f f6 ff fe d7 ff ff 17 d7 7f 3f 7f bd ff bf bf be 7e 3f
PPS (checksum error): ff 93 9f d7
TPDU (malformed): 3f 3f ff 7f 7f

Wireshark shows the same thing at the time. (attached)

I dont have anything setup to take from the debug 2.5mm jack, but I will look into that urgently.

Related issues:

Related to SIMtrace 2 - Bug #4335: Unexpected/malformed data from SIM applet ...	**New**	**12/17/2019**

History

#1 - 09/21/2020 09:20 PM - mschramm

- Related to Bug #4335: Unexpected/malformed data from SIM applet causes simtrace2-sniff to stop until simtrace2 board is reset added

#2 - 09/21/2020 09:23 PM - mschramm

is it a duplicate of #4335 ?

#3 - 09/24/2020 09:05 PM - connectednow

mschramm wrote:

> is it a duplicate of #4335 ?

Thanks for the reply.

I dont think so, I am running the latest firmware version, 0.7.0.63-39070 and although I did not see explicit confirmation, I believe #4335 was solved in a previous firmware version.

I ordered a debug cable last week so as soon as that arrives I will provide some output from that.

#4 - 03/04/2021 03:01 PM - laforge

- Category set to firmware

- Assignee set to connectednow

is there any update on this? Did you manage to get debug output and did that help?

Unfortuantely without a setup to reproduce it's hard for the developers to investigate + fix the issue.

Files

Screenshot from 2020-09-15 17-50-04.png	82.6 KB	09/16/2020	connectednow
malformed packets 20200915.pcapng	28 KB	09/16/2020	connectednow