Hello, I’m facing a problem when using the trace function. It doesn't capture any packets and the phone (iphone se/iphone xs) shows “No SIM card”.

I used the latest version firmware, flashed with dfu-util. I inserted the valid sim card into the simtrace board, inserted the cable-sim into the phone, start the sniff program and turn on the phone. But it keep output "Card state change". Is it a bug or my problem?

Thanks!

(the board version on the back is v1.5 with ATSAM3SD8B chip)

Here's the console output when flushing.

dfu-util: Invalid DFU suffix signature
dfu-util: A valid DFU suffix will be required in a future dfu-util release!!!
Opening DFU capable USB device...
ID 1d50:60e3
Run-time device DFU version 0100
Claiming USB DFU Runtime Interface...
Determining device status: state = appIDLE, status = 0
Device really in Runtime Mode, send DFU detach request...
Device will detach and reattach...
Opening DFU USB Device...
Claiming USB DFU Interface...
Setting Alternate Setting #1 ...
Determining device status: state = dfuIDLE, status = 0
dfuIDLE, continuing
DFU mode device DFU version 0100
Device returned transfer size 512
Copying data from PC to DFU device
Download [======================================] 100% 23532 bytes
Download done.
state(7) = dfuMANIFEST, status(0) = No error condition is present
state(2) = dfuIDLE, status(0) = No error condition is present
Done!
dfu-util: can't detach
Resetting USB to switch back to runtime mode

the console will stuck here

Here's the console output when tracing.

dfu-util@1-NUC8i7BEH:~/SIMtrace/simtrace2/host/src$ ./simtrace2-list
USB matches: 2
1d50:60e3 Addr=6, Path=1-4, Cfg=1, Intf=0, Alt=0: 255/1/0 (SIMtrace Sniffer)
1d50:60e3 Addr=6, Path=1-4, Cfg=2, Intf=0, Alt=0: 255/255/0 (0.8.1.36-a5d53)
this is very strange indeed.

just to narrow this down a bit:

- does the same simtrace + SIM card work in any other phone or modem?

Also, do you have any 3.3V UART around? If yes, the output from the debug UART (2.5mm stereo jack, but as far as I recall also on other pins, see schematics) would be most useful.

I have never used any iPhones myself, so I don't have personal experience with those specific two units, but I've used the SIMtrace2 with tons of phone / modem models.

Also, do you have any 3.3V UART around? If yes, the output from the debug UART (2.5mm stereo jack, but as far as I recall also on other pins, see schematics) would be most useful.
I have never used any iPhones myself, so I don’t have personal experience with those specific two units, but I’ve used the SIMtrace2 with tons of phone / modem models.

Hi Laforge,

Thanks for replying so quick!

For the question "does the same simtrace + SIM card work in any other phone or modem?":
(1) No, it never worked as expected. I have used another sim card from another operator, also the same problem. (Both sim cards works fine when directly inserted into the target phone)
(2) I have tested another Android phone with Snapdragon 888 modem but also resulted same bug pattern, so I assume it’s not the phone’s problem.
(3) Plus, I have seen examples using iPhone as target.

For the question "Also, do you have any 3.3V UART around?":
Sorry, currently I don’t have any UART cable, is the UART a must for diagnosis? If so, I will buy one and it should be arrived in a week, and I will provide some more info then.

I noticed that you set this issue as category-firmware. However, I would still like to ask, is it probably a hardware problem or a host software problem?

Is there any other solution I can try without UART/JTAG?

And I wonder if the sim card tray is needed for the cable-sim? Like is there any switch inside the sim card slot on the phone to be triggered with the insertion of the card tray? Do you use the card tray? (it can not fit in the right position with the cable as a hinder)

Thanks again for all your help!

Regards,

#3 - 08/02/2022 01:20 PM - laforge

On Mon, Aug 01, 2022 at 02:11:47AM +0000, g1bbs wrote:

For the question "Also, do you have any 3.3V UART around?":
Sorry, currently I don’t have any UART cable, is the UART a must for diagnosis?

In general, yes. That’s pretty universally true for most >= 90% of all electronics devices with some form of microcontroller or cpu inside that I’ve worked with in my career.

If so, I will buy one and it should be arrived in a week, and I will provide some more info then.

I noticed that you set this issue as category-firmware. However, I would still like to ask, is it probably a hardware problem or a host software problem?

if there’s a problem with your hardware, it is something to contact support@sysmocom.de about. The hardware category here is more about aspects of the OSHW simtrace2 design.

Host software can be pretty much excluded as you are getting the card reset events, so this means that the USB communication between simtrace device and host software works.

And I wonder if the sim card tray is needed for the cable-sim?

you always need to use a tray when your device needs a tray.

like is there any switch inside the sim card slot on the phone to be triggered with the insertion of the card tray?

that is a question about the hardware design of your phone and not about the simtrace product.

Do you use the card tray? (it can not fit in the right position with the cable as a hinder)

you will have to use a file to file down the tray (get a spare one) so the cable can fit.

The best approach to me still seems like you should use a classic/old device with a 2FF socket. Get that working and get some hands-on experience with simtrace, and then try something that’s mechanically more challenging like 4FF slots with trays.

#4 - 08/02/2022 01:40 PM - g1bbs

laforge wrote in #note-3:
On Mon, Aug 01, 2022 at 02:11:47AM +0000, g1bbs wrote:

For the question "Also, do you have any 3.3V UART around?":
Sorry, currently I don't have any UART cable, is the UART a must for diagnosis?

In general, yes. That's pretty universally true for most >= 90% of all electronics
devices with some form of microcontroller or cpu inside that I've worked with in my career.

If so, I will buy one and it should be arrived in a week, and I will provide some more info then.

I noticed that you set this issue as category-firmware. However, I would still like to ask, is it probably a hardware problem or a host software problem?

if there's a problem with your hardware, it is something to contact support@sysmocom.de about. The hardware
category here is more about aspects of the OSHW simtrace2 design.

Host software can be pretty much excluded as you are getting the card reset events, so this means
that the USB communication between simtrace device and host software works.

And I wonder if the sim card tray is needed for the cable-sim?

you always need to use a tray when your device needs a tray.

like is there any switch inside the sim card slot on the phone to be triggered with the insertion of the card tray?

that is a question about the hardware design of your phone and not about the simtrace product.

Do you use the card tray? (it can not fit in the right position with the cable as a hinder)

you will have to use a file to file down the tray (get a spare one) so the cable can fit.

The best approach to me still seems like you should use a classic/old device with a 2FF socket. Get that
working and get some hands-on experience with simtrace, and then try something that's mechanically more
challenging like 4FF slots with trays.

Hi laforge,

Thank you for your patient and informative reply. I will try to get an UART cable for further debug. I agree with you that those new to simtrace like me
should start with some old/test-friendly UE, thanks for the advice. Also, if possible, your experience on the tray problem shoule be added to the wiki
page since modern UE all use tray, it will be very helpful for simtrace users.

BRs

#5 - 08/02/2022 03:10 PM - laforge
On Tue, Aug 02, 2022 at 01:40:33PM +0000, g1bbs wrote:

Thank you for your patient and informative reply. I will try to get an UART cable for further debug. I agree with you that those new to simtrace like me
should start with some old/test-friendly UE, thanks for the advice.

Also, if possible, your experience on the tray problem shoule be added to the wiki page since modern UE all use tray, it will be very helpful for simtrace users.

Indeed. With so many osmocom projects in parallel, time is always an issue. I've added your user
account to the group of people with wiki editing privileges.

I'll see if I can find a filed/modified tray for some pictures.

#6 - 08/03/2022 07:00 AM - laforge
- Status changed from New to Feedback
- Assignee changed from laforge to g1bbs