User Guide
Document Ref: 8825 Osmocom SIMtrace instructions
02_12_2022
Version: v1.1

Capturing SIM to modem communication

Using Osmocom SIMtrace 2

Version number	Date	Author	Changes
1	13/04/2022	Ben Laird	Doc created
1.1	02/12/2022	Jen vdB	Formalised document

Table of Contents

1. Setting up

1.1 Before you begin

You will need:

- Eseye-supplied:
  - Osmocom SIMtrace2 board, preconfigured
  - Raspberry Pi, preconfigured
  - SIM paddle/ribbon cable
  - USB cable
  - Micro USB to power supply (5V-2A)
- Ethernet cable
- PC running:
  - SSH client, such as Windows Terminal
  - SFTP client, such as WinSCP

1.2 Setting up your system

1. Insert the appropriate SIM 'paddle'/ribbon cable into the device you are testing.
2. Connect the USB cable between the SIMTrace and either USB port on the Pi.
3. Connect an ethernet cable between the Pi and the PC.

4. Configure the ethernet interface:
   - If connecting to your existing local network, identify the IP address allocated to the Pi.
     If your network supports dynamically assigned DNS, use the PC CMD prompt to locate the Pi on the DNS record (called '`osmo-tool`').
     For example, run:
     `ping osmo-tool`

- If connecting directly to a PC ethernet port, manually set the IPv4 config of your adapter with the following settings:
  - **Address** = `198.18.0.1`
  - **Subnet** = `255.255.0.0`
  - No gateway or DNS required

5. Power up the Pi using the micro USB to power supply (5V-2A).
6. Wait until all LEDs on the Pi are lit (PWR, FDX, LNK, 100).
7. Use the SSH client to connect to the Pi console:
   - IP Address =
     - If connected via DNS to the local network – `osmo-tool`
     - If directly connected to device – `198.18.0.2`
   - User = `pi`
   - Password = `R@spberry`

2. Capturing SIM to modem communication

1. Using the SSH client, ensure the Pi can detect SIMtrace. Type:

   `sudo simtrace2-list`

   This should return 2 matches, for example:

   ```
   pi@Osmo-tool:~ $ sudo simtrace2-list
   USB matches: 2
           1d50:60e3 Addr=4, Path=1-1.3, Cfg=1, Intf=0, Alt=0: 255/1/0 (SIMtrace Sniffer)
           1d50:60e3 Addr=4, Path=1-1.3, Cfg=2, Intf=0, Alt=0: 255/255/0 (0.8.1.36-a5d53)
   pi@Osmo-tool:~ $
   ```

2. Create a Screen session (a separate detachable console). Type:

   `sudo screen -S pcap`

3. Within the Screen console you just created, define the file where the SIM trace is captured. Type:

   `tcpdump -i lo -w <filename>.pcap`

   Where <filename> is the name of the file. For example:

   `tcpdump -i lo -w simtrace.pcap`

4. Detach the Screen console to run in the background:
   - Press `Ctrl+a`
   - Press `d`
5. Create a second Screen session to start the SIM trace. Type:

   `sudo screen -S sniff`

6. Within the Screen console you just created, type:

   `simtrace2-sniff`

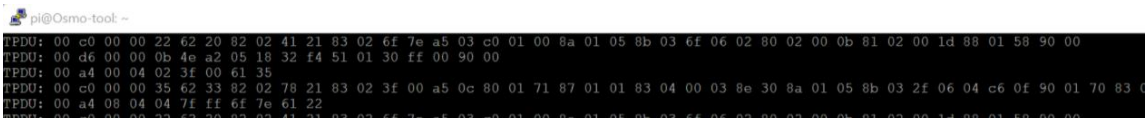
7. Wait for the program to return **`Entering main loop`**

   ```
   root@Osmo-tool:/home/pi# simtrace2-sniff
   simtrace2-sniff - Phone-SIM card communication sniffer
   (C) 2010-2017 by Harald Welte <laforge@gnumonks.org>
   (C) 2018 by Kevin Redon <kredon@sysmocom.de>

   Using USB device 1d50:60e3 Addr=4, Path=1-1.3, Cfg=1, Intf=0, Alt=0: 255/1/0 (SIMtrace Sniffer)
   Entering main loop
   ```

8. Power up the device you are testing.

   After the device modem accesses the SIM, you should see a flow of TDPU hex. For example:



9. Detach the Screen console to run in background:
   - Press `Ctrl+a`
   - Press `d`

At this point you can close the SSH session without affecting the test. The Pi and SIMtrace will continue to run and the results are captured to the simtrace.pcap file, which is stored on your Pi.

3. Retrieving the test results to the PC

1. Access the Pi via SSH, as described previously.
2. Issue the following command to end all processes associated with the test:

   ```
   sudo killall screen
   ```

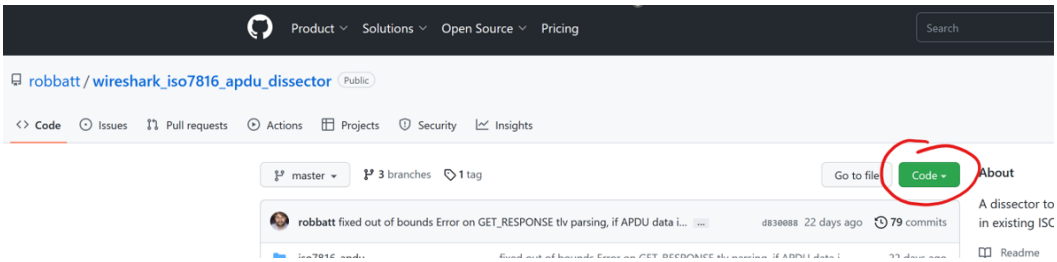
   At this point the test is complete.

3. Retrieve the test results via SFTP:
   - Access the Pi with an SFTP client (such as WinSCP), using the same IP address and credentials used previously.
   - Select **simtrace.pcap**, then select **Download**.

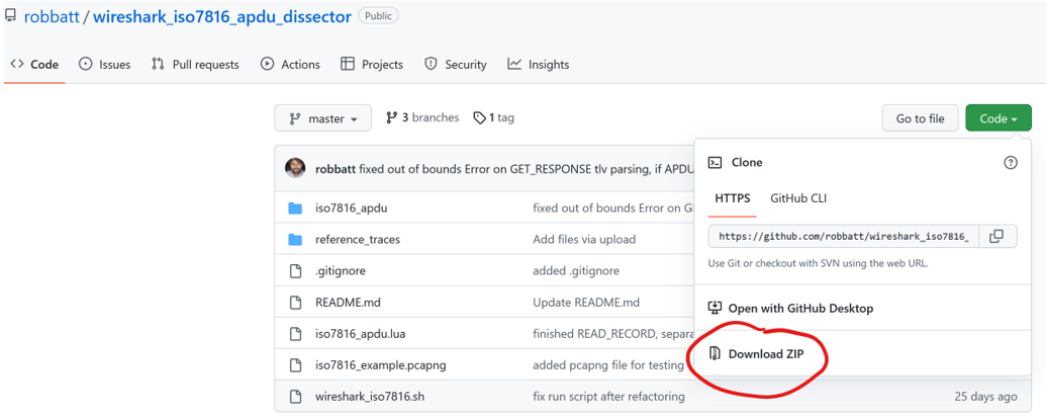
4. Installing Wireshark Dissector

NOTE: This has been tested for Wireshark v3.6.5, not currently tested for v4.

1. Select the following URL:
   https://github.com/robbatt/wireshark_iso7816_apdu_dissector/tree/master
2. Select **Code**.



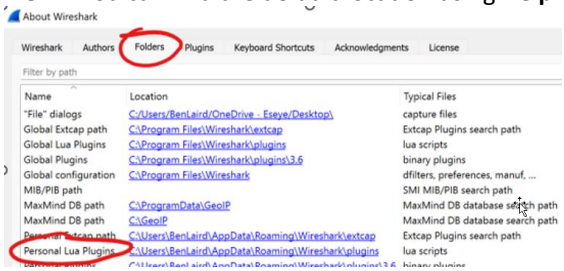
3. Select **Download ZIP**.



4. Extract the zip file.
5. Copy the following to the **Personal Lua Plugins** default location:

   - File: **iso7816_apdu.lua**
   - Folder: **iso7816_apdu**

NOTE: You can find the default location using **Help** -> **About Wireshark** -> **Folders**



6. In the **Personal Lua Plugins** location, double-click the **simtrace.pcap** file.
   The Dissector automatically loads.