CARD CENTRIC SOLUTIONS LTD.
CARD CENTRIC

ScET Tracer Tool

User Guide

Author(s)	Mark Bourke
Date	6th December 2019
Project	ScET Tracer Tool
Version	1.0
Status	Release

Legal Notice

The information contained in this document is proprietary and confidential to Card Centric ltd.
It shall never be duplicated, published or disclosed in any form whatsoever, in whole or in part, to any third party without the prior written consent of Card Centric ltd., such consent never being presumed. This document is provided “as is”, “where is”, and “with all faults”, without a warranty of any kind. Card Centric ltd. specifically disclaim all warranties, either express or implied, including, without limitation, any warranties of merchantability or fitness for a particular purpose or use. Card Centric ltd. do not warrant, guarantee, or make any representations regarding the correctness or accuracy of the information contained in this document, and disclaims any liability for any infringement of any patent, copyright or other property rights of any third party in connection with the use of the information contained in this document. The users of the information contained in this document are responsible for identifying and obtaining any and all patent, copyright or other intellectual property licenses that may be needed for products or services developed in connection with the information contained in this document.

Document History

Version	Author(s)	Date	Status	Reason of Change
1.0	MB	06-Dec-19	Draft	Document Created

Table of Contents

1. Syntax

This is assumed in this document that a byte is divided into bits as follows.

b7	b6	b5	b4	b3	b2	b1	b0

2. Introduction

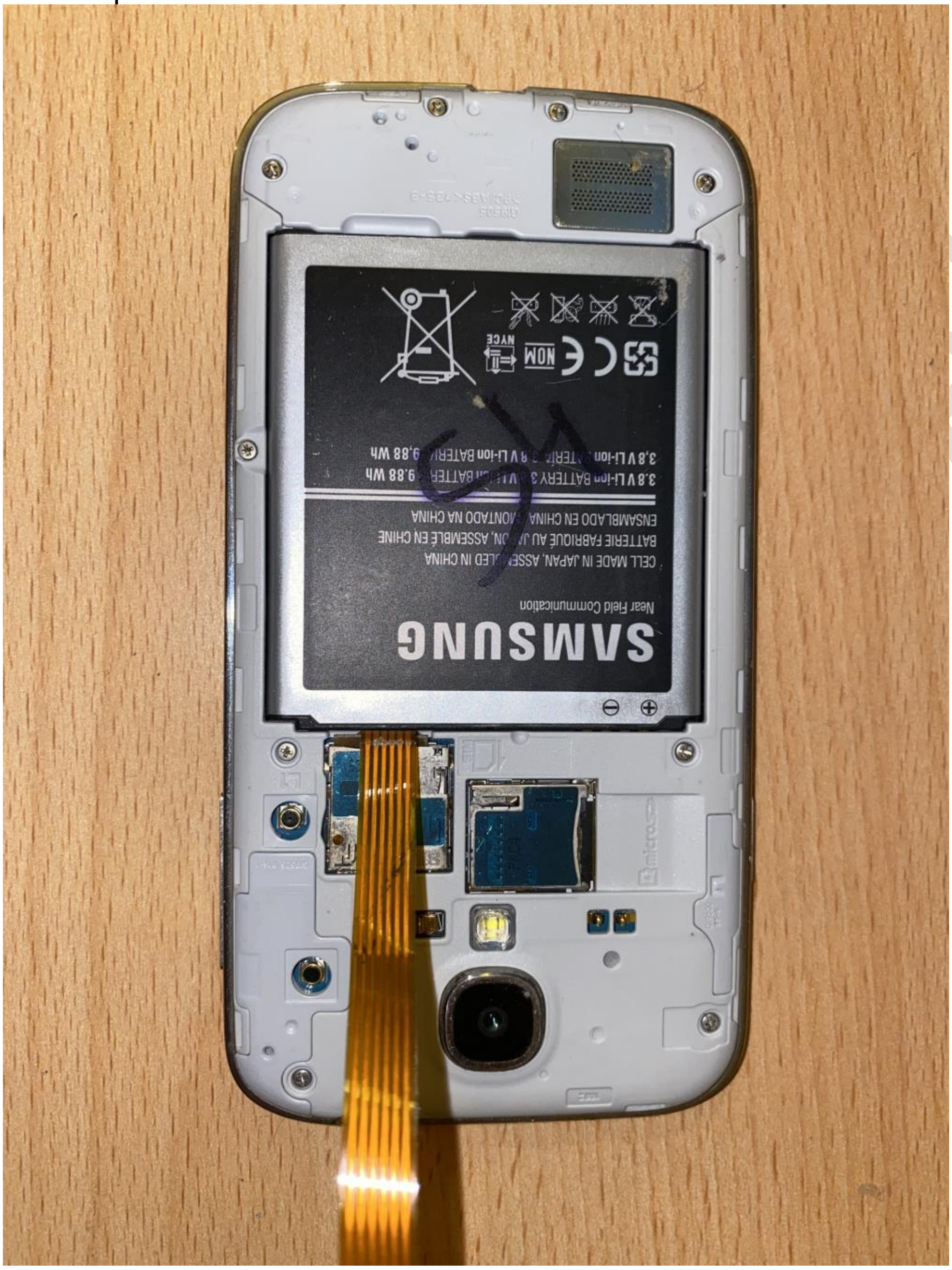
This document presents the user guide for the Card Centric ScET Tracer Tool.

2.1 Description

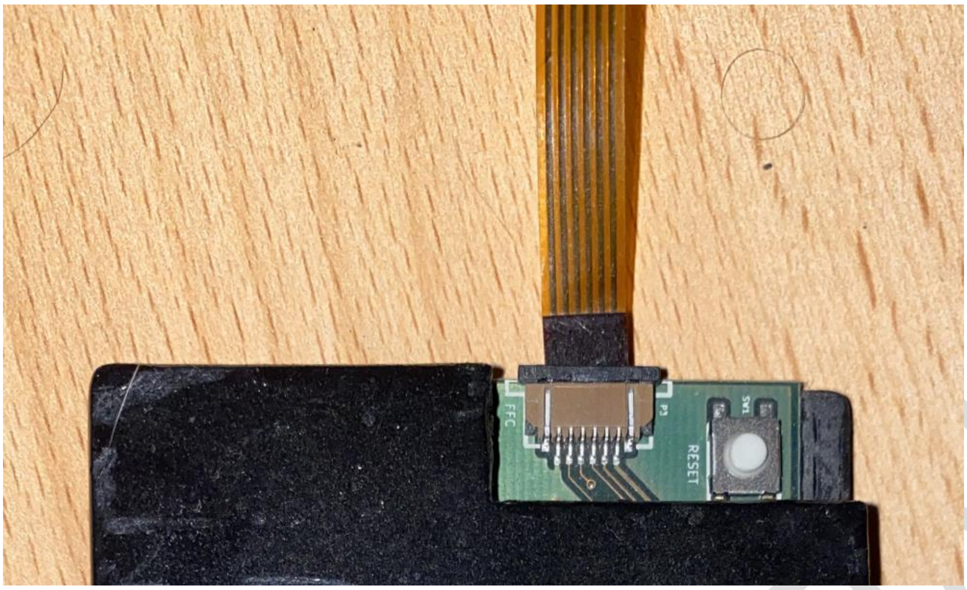
The ScET Tracer Tool is a tool that records the live behaviour of a SIM card when connected to a network using any end user device. All SIM card communication, in the form of APDU commands, are tracked and logged by this tool.

3. Hardware Configuration

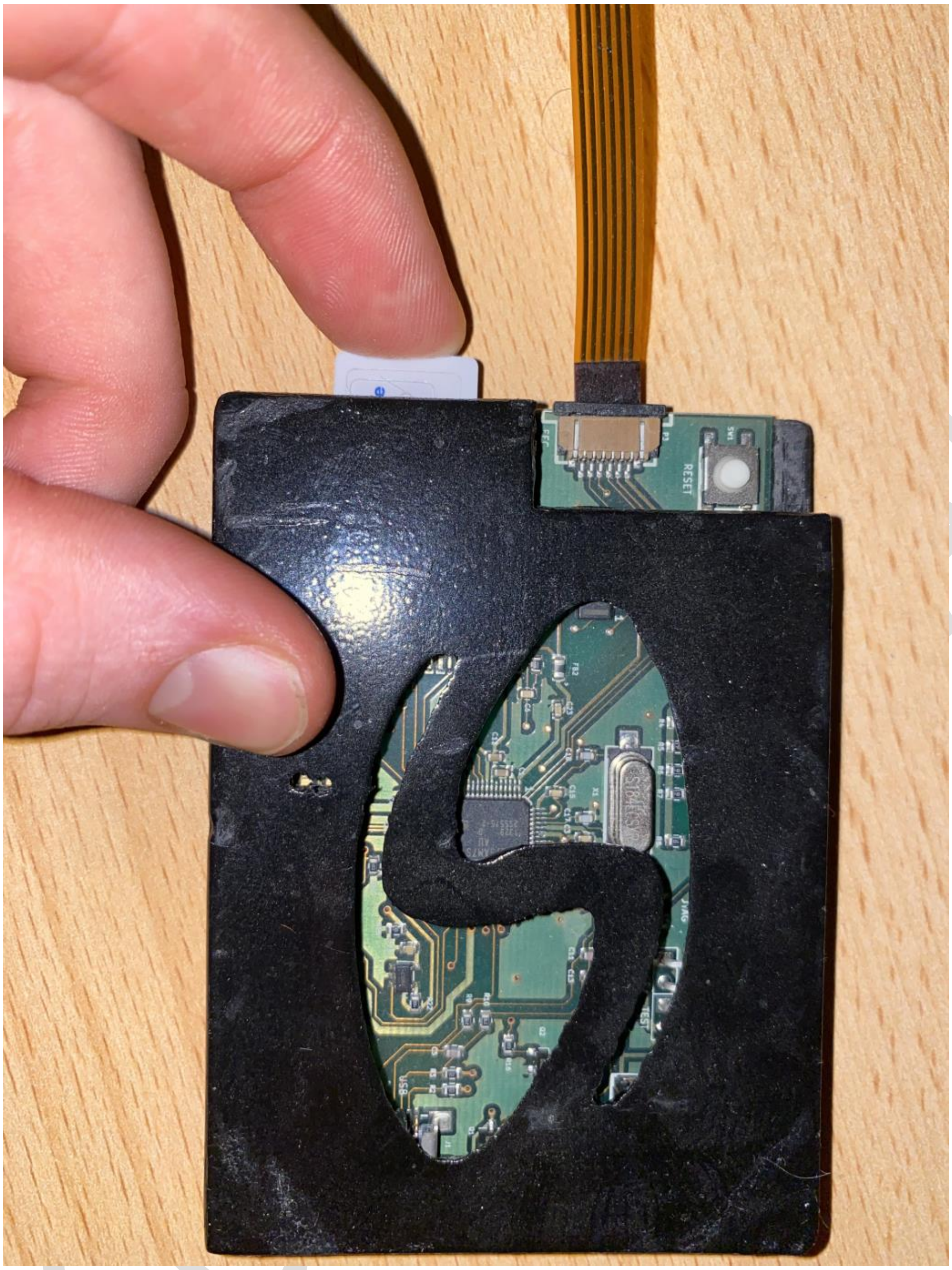
Turn the handset off and remove its SIM card. Then, place the SIM end of the probe into the phone.



Connect the other end of the probe to the tracer with the gold contacts facing downward.

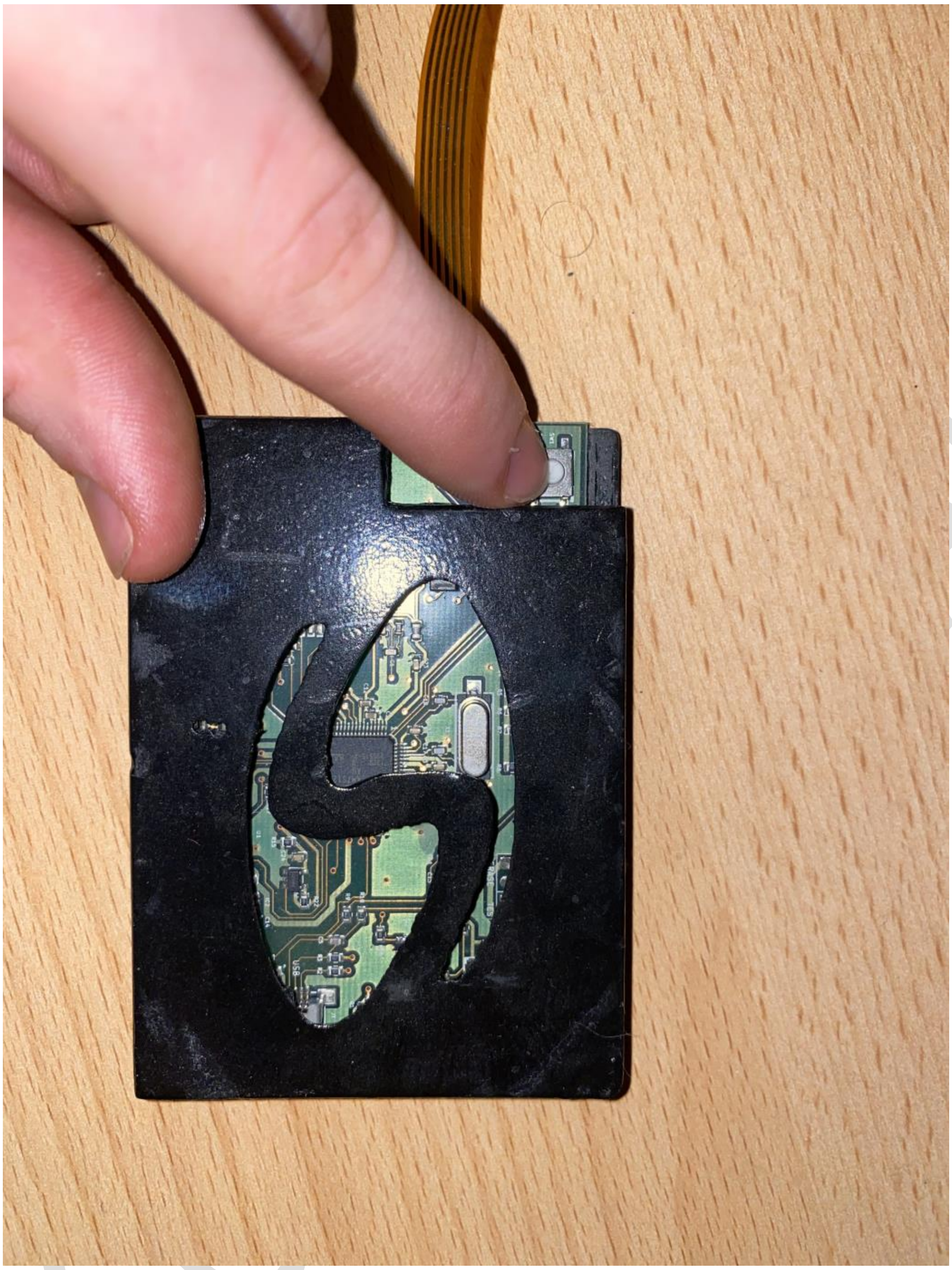


Lastly, insert the aforementioned SIM card into the tracer until it clicks into place. Connect the USB cable to the tracer and the computer.



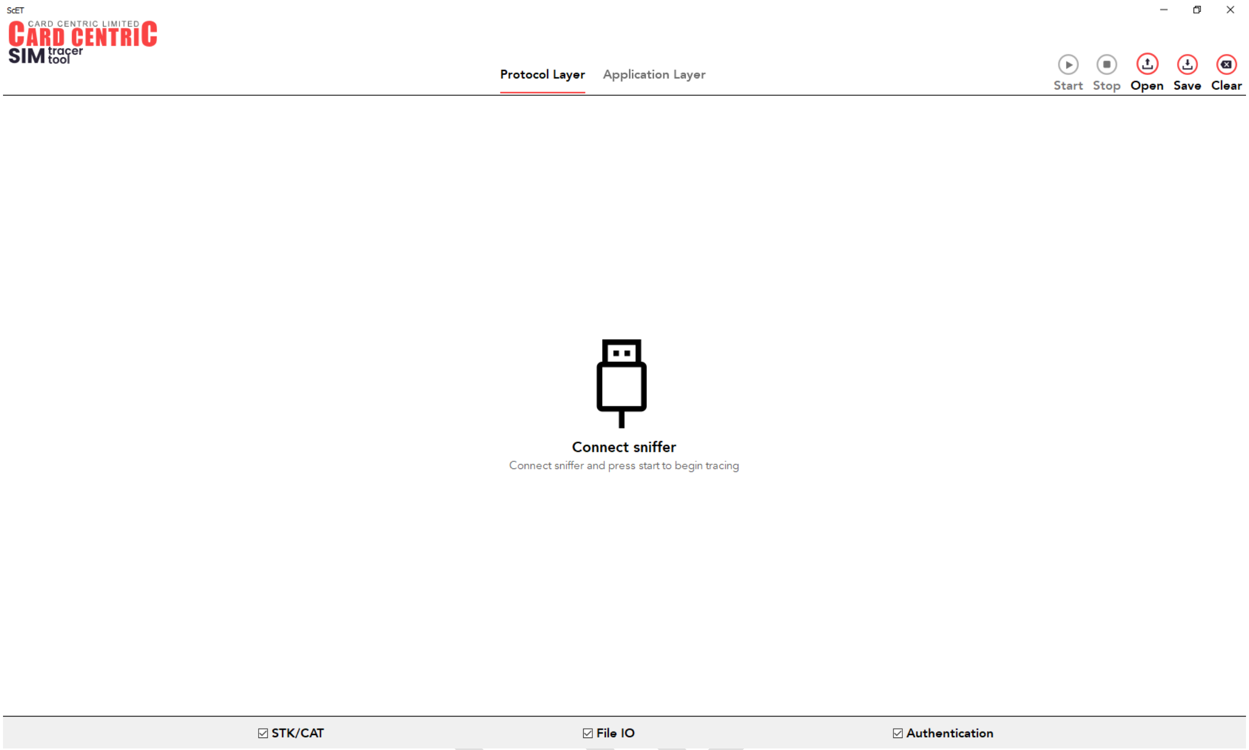
3.1 Restarting a Tracing Session

In order to ‘retrace’ a handset you must first turn the handset off, but more importantly, you must either press the *Reset* button on the tracer or unplug the tracer from the computer and plug it back in otherwise only a partial trace will be logged.



4. Using the Software

Once ScET has been installed, you will be greeted with the following screen.



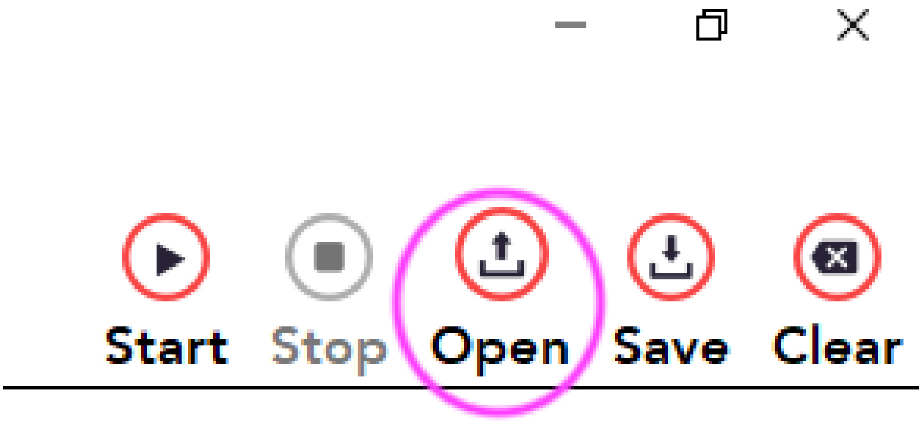
Connect sniffer

Connect sniffer and press start to begin tracing

☑ STK/CAT ☑ File IO ☑ Authentication

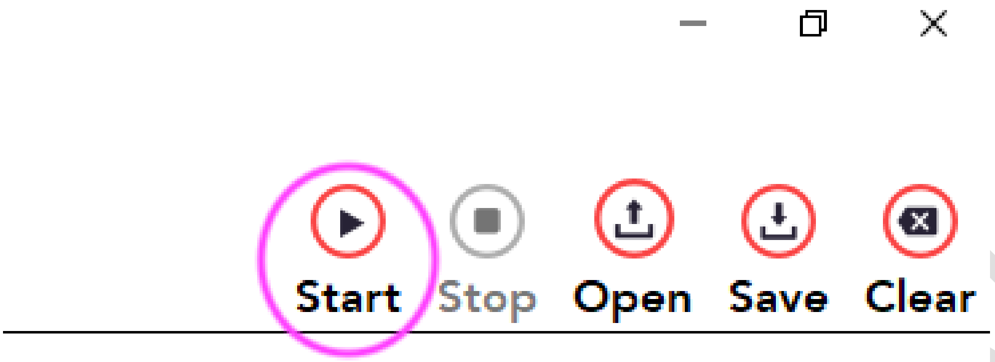
4.1 Loading a Tracing Session

You can open a previously saved Tracing Session (*.sts) by clicking the *Open* button.

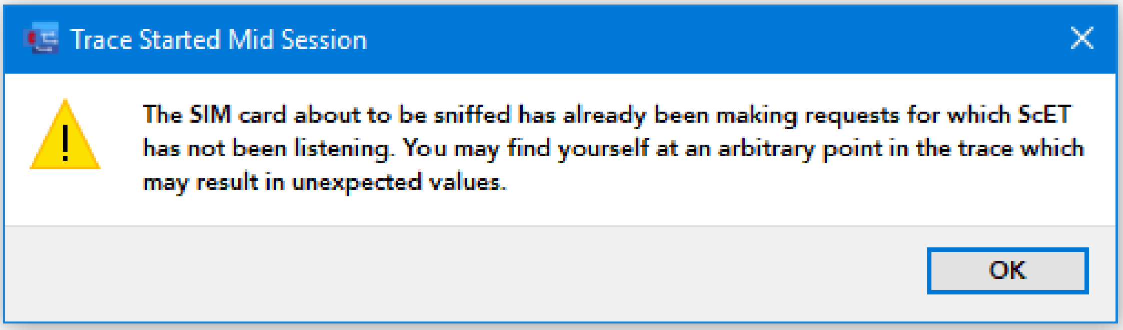


4.2 Starting a Tracing Session

Once the tracer has been connected and recognised by the computer you will be able to start a Tracing Session by clicking the *Start* button. Once the session has been started you can then turn the phone on.



If the phone is already on when the session is started, you will get a warning message.

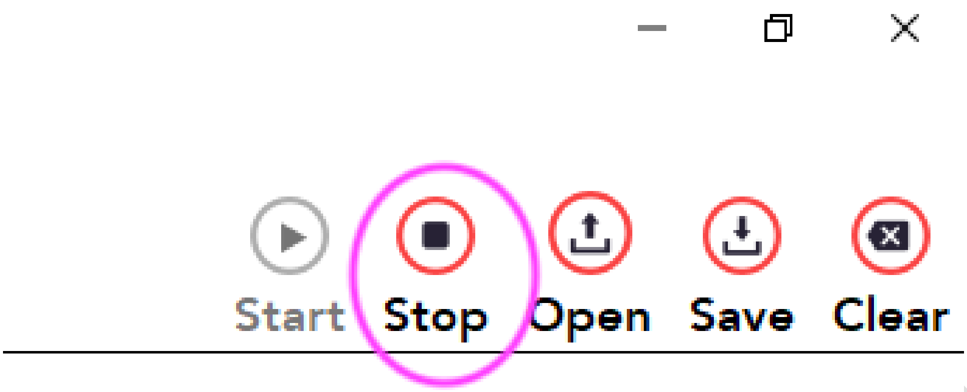


Trace Started Mid Session

The SIM card about to be sniffed has already been making requests for which ScET has not been listening. You may find yourself at an arbitrary point in the trace which may result in unexpected values.

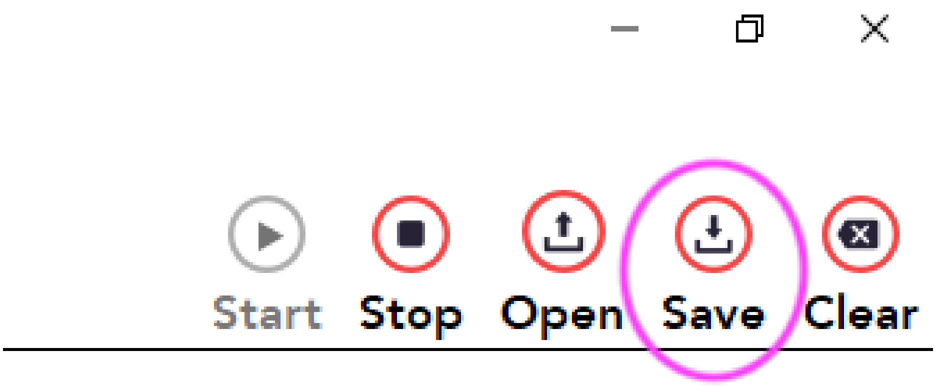
4.3 Stopping a Tracing Session

A Tracing Session can be stopped at any point by clicking the *Stop* button. Resuming the trace session after this point without rebooting the handset is **not** recommended and may lead to unexpected outputs.



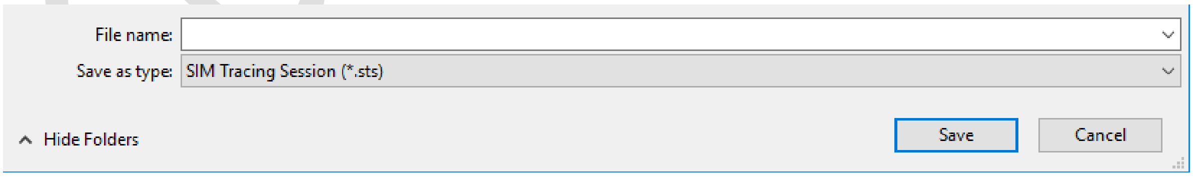
4.4 Saving/Exporting a Tracing Session

A Tracing Session can be saved easily in a number of formats by clicking the *Save* button.



4.4.1 SIM Tracing Session

This is the default format for the Tracing Session and the only format that can be reloaded back into ScET.

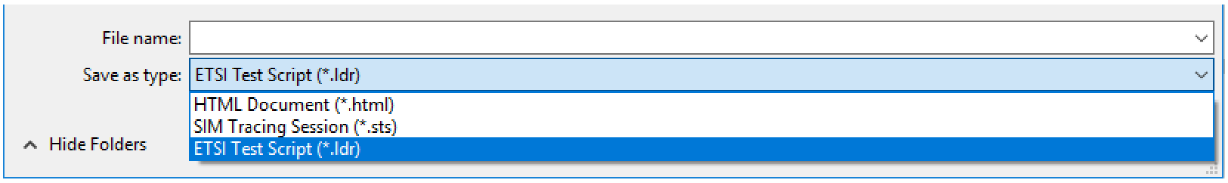


File name:

Save as type: SIM Tracing Session (*.sts)

4.4.2 LDR Script

This format can be used for further testing. To export to this format simply *Save* and click the *Save as type* dropdown and select *ETSI Test Script*.

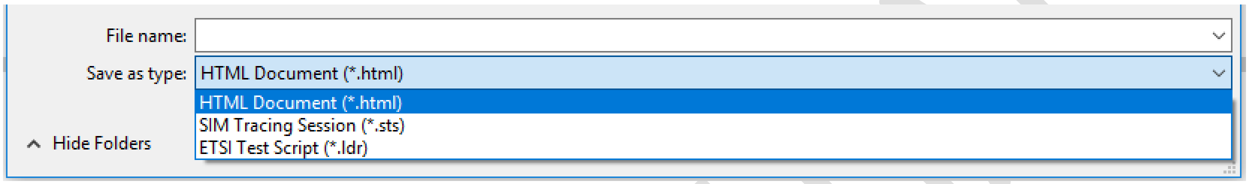


File name:

Save as type: ETSI Test Script (*.ldr)

4.4.3 HTML

This format is great for distribution of information to those who do not have ScET installed. All they need to have is a web browser and then they can see the SIM card trace. To export to this format simply *Save* and click the *Save as type* dropdown and select *HTML*.



File name:

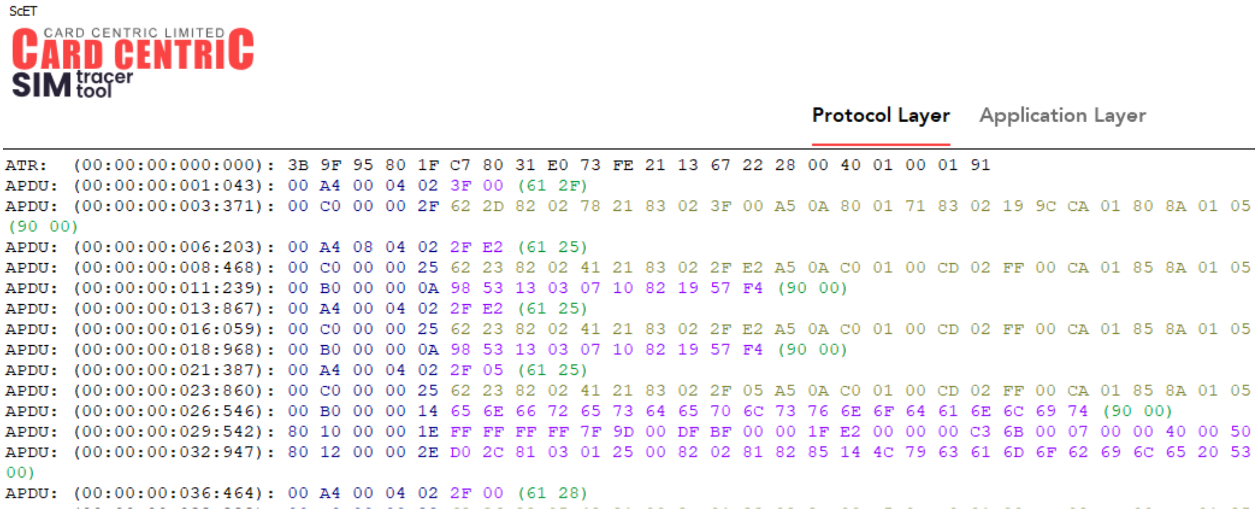
Save as type: HTML Document (*.html)

4.5 Viewing the Tracing Session

Once the Tracing Session has completed there are a number of ways for the data to be viewed.

4.5.1 Protocol Layer

The most basic is the Protocol Layer. It is a byte-by-byte representation of the data being transmitted and received between the card and the handset. Without very in-depth knowledge of APDU commands it is quite hard to distinguish exactly what is going on. Clicking on an APDU command in the Protocol Layer will highlight the corresponding command in the Application Layer.



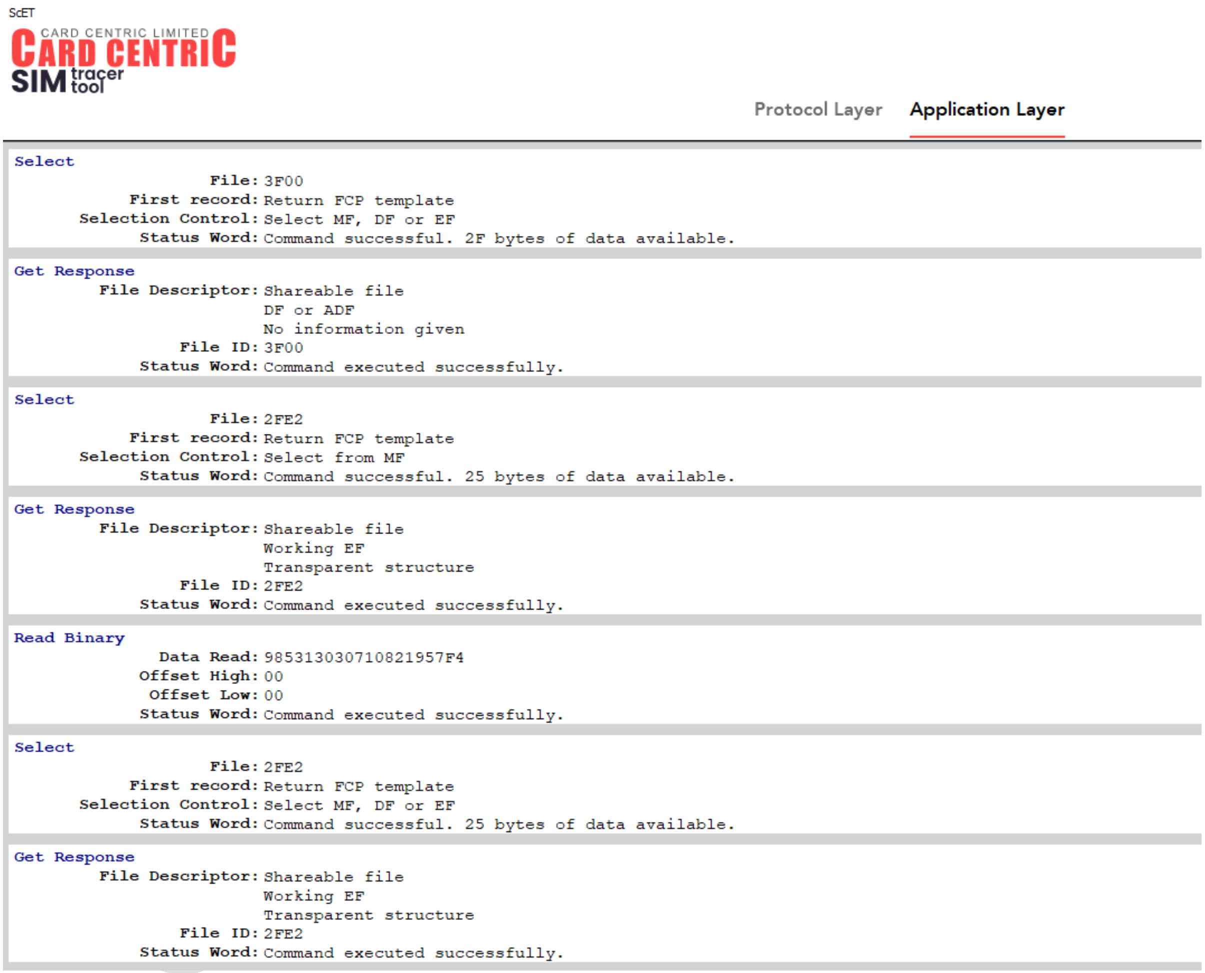
```
ATR:  (00:00:00:000:000): 3B 9F 95 80 1F C7 80 31 E0 73 FE 21 13 67 22 28 00 40 01 00 01 91
APDU: (00:00:00:001:043): 00 A4 00 04 02 3F 00 (61 2F)
APDU: (00:00:00:003:371): 00 C0 00 00 2F 62 2D 82 02 78 21 83 02 3F 00 A5 0A 80 01 71 83 02 19 9C CA 01 80 8A 01 05
(90 00)
APDU: (00:00:00:006:203): 00 A4 08 04 02 2F E2 (61 25)
APDU: (00:00:00:008:468): 00 C0 00 00 25 62 23 82 02 41 21 83 02 2F E2 A5 0A C0 01 00 CD 02 FF 00 CA 01 85 8A 01 05
APDU: (00:00:00:011:239): 00 B0 00 00 0A 98 53 13 03 07 10 82 19 57 F4 (90 00)
APDU: (00:00:00:013:867): 00 A4 00 04 02 2F E2 (61 25)
APDU: (00:00:00:016:059): 00 C0 00 00 25 62 23 82 02 41 21 83 02 2F E2 A5 0A C0 01 00 CD 02 FF 00 CA 01 85 8A 01 05
APDU: (00:00:00:018:968): 00 B0 00 00 0A 98 53 13 03 07 10 82 19 57 F4 (90 00)
APDU: (00:00:00:021:387): 00 A4 00 04 02 2F 05 (61 25)
APDU: (00:00:00:023:860): 00 C0 00 00 25 62 23 82 02 41 21 83 02 2F 05 A5 0A C0 01 00 CD 02 FF 00 CA 01 85 8A 01 05
APDU: (00:00:00:026:546): 00 B0 00 00 14 65 6E 66 72 65 73 64 65 70 6C 73 76 6E 6F 64 61 6E 6C 69 74 (90 00)
APDU: (00:00:00:029:542): 80 10 00 00 1E FF FF FF FF 7F 9D 00 DF BF 00 00 1F E2 00 00 00 C3 6B 00 07 00 00 40 00 50
APDU: (00:00:00:032:947): 80 12 00 00 2E D0 2C 81 03 01 25 00 82 02 81 82 85 14 4C 79 63 61 6D 6F 62 69 6C 65 20 53
00)
APDU: (00:00:00:036:464): 00 A4 00 04 02 2F 00 (61 28)
```

The timestamp indicates when the command was received by ScET and does not exactly correspond to when the SIM card issued the command.

The **blue** text indicates the APDU command header.
The **pink** text indicates the APDU command data.
The **green** text indicates the APDU command response code.
The **gold** text indicates the APDU command response data.

4.5.2 Application Layer

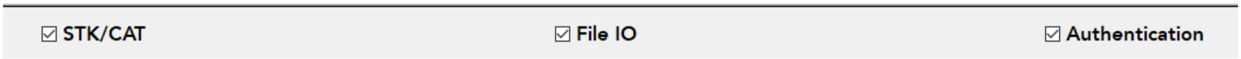
The Application Layer is a breakdown and decoding of the Tracing Session according to the GSM standards. Clicking on an APDU command in the Application Layer will highlight the corresponding command in the Protocol Layer.



```
Select
                   File: 3F00
           First record: Return FCP template
      Selection Control: Select MF, DF or EF
            Status Word: Command successful. 2F bytes of data available.

Get Response
        File Descriptor: Shareable file
                         DF or ADF
                         No information given
                File ID: 3F00
            Status Word: Command executed successfully.

Select
                   File: 2FE2
           First record: Return FCP template
      Selection Control: Select from MF
            Status Word: Command successful. 25 bytes of data available.

Get Response
        File Descriptor: Shareable file
                         Working EF
                         Transparent structure
                File ID: 2FE2
            Status Word: Command executed successfully.

Read Binary
              Data Read: 985313030710821957F4
            Offset High: 00
             Offset Low: 00
            Status Word: Command executed successfully.

Select
                   File: 2FE2
           First record: Return FCP template
      Selection Control: Select MF, DF or EF
            Status Word: Command successful. 25 bytes of data available.

Get Response
        File Descriptor: Shareable file
                         Working EF
                         Transparent structure
                File ID: 2FE2
            Status Word: Command executed successfully.
```

4.5.3 Command Filters

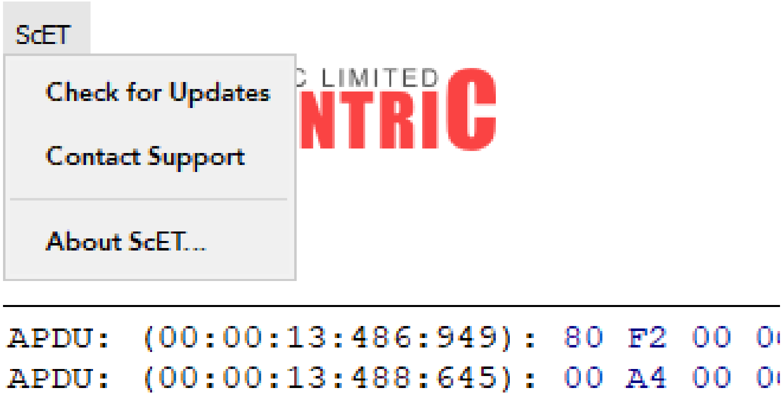
The APDU commands can be filtered based upon their category.



☑ STK/CAT ☑ File IO ☑ Authentication

4.6 Updates

Updates are checked for automatically in the background but can be manually checked for by clicking the *ScET* button in the top left-hand side of the screen and selecting *Check for updates*



```
APDU: (00:00:13:486:949): 80 F2 00 0
APDU: (00:00:13:488:645): 00 A4 00 0
```