Rogue BTS (IMSI Catcher) Detection Unit

TSCM Deployment

Mobile hardware and software solution for detecting, monitoring and recording BTS broadcast information for standards GSM, UMTS, LTE800, LTE.

The Device is designed to collect information about Base Transceiver Stations (BTS), operating in the standards of digital mobile communications GSM / UMTS / LTE. Bands can be specified for any region.

The scope of the complex can be the following:

- search for unregistered base stations;
- build a network coverage map;
- fake BTS / IMSI catcher detection.

Product Description

Device dimension is 25x7x15 cm, it has a power connector and a USB connector for data transfer. The product has 5 connectors for antennas. APK supports work with 4 different carriers simultaneously (4 independent modems).

Main functionality

The main functional capabilities of the complex are:

- Fast scan mode: collecting data for surrounding base stations. In this mode, device receives basic data of the surrounding BTS.

- Detailed GSM scanning mode: data acquisition for surrounding GSM base stations. In this mode, device receives an expanded list of parameters for GSM base stations.

- Searching for fake BS mode: in this mode, device continuously monitors the radio air and evaluates the reliability of the surrounding BTS in GSM standard.

- GPS / GLONASS geo positioning. The device is connected to a GPS antenna for the providing the mapped location of the BTS in range.

- Once the BTS are detected, all information can be stored with location labels for later display on the map.

- Scan results can be exported in CSV format.

- Adjustable refresh rate.

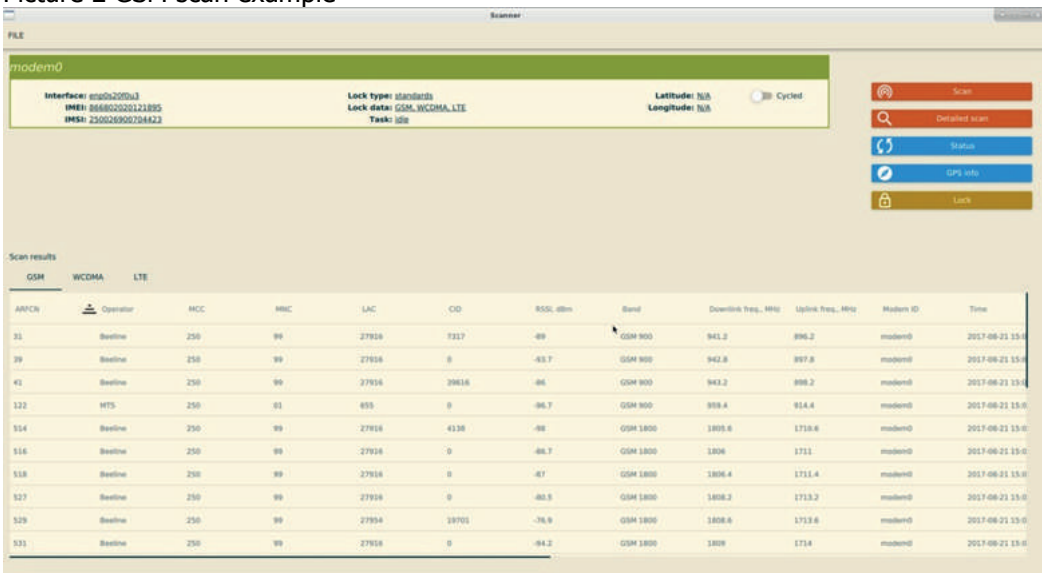
Platform description

GSM chips based on Qualcomm processors are used as a radio module for the BTS monitoring. This technical solution allows receiving data, similar to the way data is received by ordinary mobile phones, due to the usage of the same demodulation and error correction mechanisms. Thus, the collected statistics more accurately display the state of the radio ether, received by mobile phones, and therefore, gives more relevant data on the quality of communication.

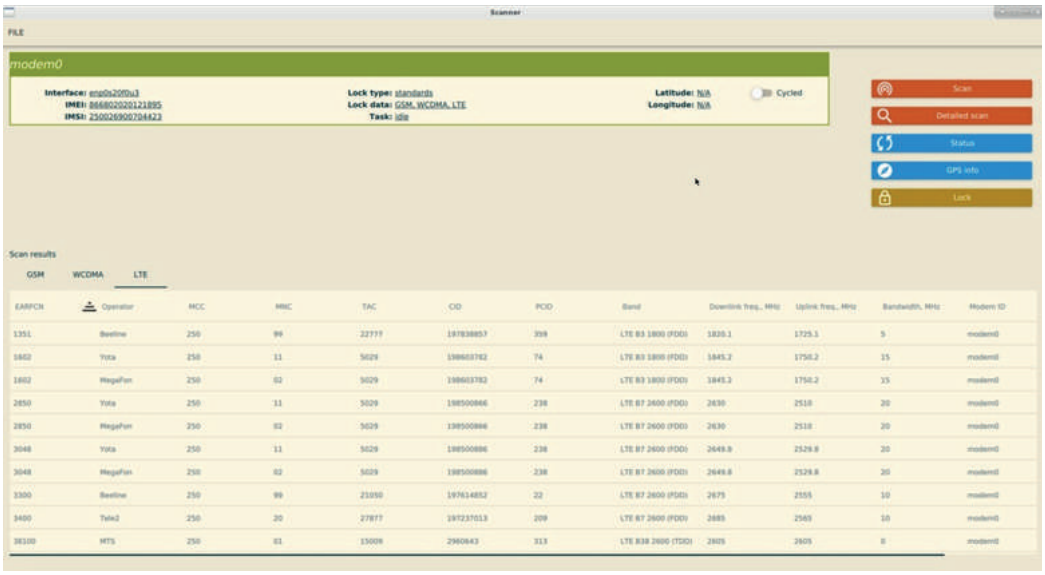
Usage of GSM chips allows the system to significantly reduce the scan time of the radio ether, in comparison with solutions using their own demodulation mechanisms based on SDR technology, and to improve the quality of signal analysis.

Picture 1 Device 3D model

Picture 2 GSM scan example



Picture 3 LTE scan example



Picture 4/5/6 selection of UI images