

GSM monitor

Orodje za monitoring
GSM omrežja



Matej Kovačič

(CC) 2016

Hek.si | Ljubljana, 15. april 2016

gr-gsm

Projekt je namenjen analizi GSM signalov. Gre za zbirko odprtokodnih programskih orodij napisanih v Pythonu. Za procesiranje signalov uporablja aplikacijo GNU Radio.

Bistvo aplikacije je, da za zajem uporablja poceni RTL-SDR sprejemnike (cena okrog 20 EUR), zelo verjetno (netestirano) pa tudi USRP, HackRF, BladeRF in ostale sprejemnike, ki so podprti s strani gr-osmosdr.

Aplikacije tečejo na Ubuntu 14.04 in 15.10, neuradno pa tudi na Mac OS ter na Raspberry Pi 3.

Uporabiti je mogoče več sprejemnikov (RTL-SDR ključkov) hkrati.

gr - gsm

grgsm_decode – aplikacija za dekodiranje CO (BCCH) kanala. Aplikacija zna zajete signale dekodirati in posredovati Wiresharku, zajete in dešifrirane zvočne pogovore pa shraniti v zvočno datoteko.

grgsm_livemon – interaktivni monitor posameznega BCCH kanala (analiza zajetih signalov poteka preko Wiresharka).

grgsm_scanner – aplikacija, ki preišče GSM frekvenčni pas in izpiše podatke o najdenih baznih postajah.

grgsm_capture – aplikacija za zajem GSM signalov v datoteko (le-to lahko kasneje analiziramo z *grgsm_decode*).

grgsm_channelize – aplikacija ki zajem širokega frekvenčnega pasu (ang. *wideband capture*) shrani v več ločenih datotek.

Zakaj RTL-SDR?

Včasih...



1 Potrebno je bilo uporabiti točno določene tipe telefonov (visoka cena)....

```
matej@cryptopia: ~/osmoccom/osmoccom-bb-raw/src/host/osmocon
Die ID code: 7e540b2fc90393bb
=====
REG_DPLL=0x2413
CNTL_ARM_CLK=0xf0a1
CNTL_CLK=0xff91
CNTL_RST=0xffff3
CNTL_ARM_DIV=0xffff9
=====
Power up simcard:

THIS FIRMWARE WAS COMPILED WITHOUT TX SUPPORT!!!
Assert DSP into Reset
Releasing DSP from Reset
Installing DSP sniff patch
Setting some dsp_api.ndb values
Setting API NDB parameters
DSP Download Status: 0x0001
DSP API Version: 0x0000 0x0000
Finishing download phase
DSP Download Status: 0x0002
DSP API Version: 0x3606 0x0000
LOST 3901!
LOST 3750!
```

```
Failed to connect to '/tmp/osmoccom_sap'.
Failed during sap open(), no SIM reader
<000e> cell_log.c:803 Scanner initialized
Mobile initialized, please start phone now!
<000e> cell_log.c:367 Measure from 0 to 124
c-<000e> cell_log.c:367 Measure from 512 to 885
<000e> cell_log.c:367 Measure from 955 to 1023
<000e> cell_log.c:358 Measurement done
<000e> cell_log.c:340 Sync ARFCN 79 (rxlev -57, 197 syncs left)
<000e> cell_log.c:340 Sync ARFCN 19 (rxlev -64, 196 syncs left)
<000e> cell_log.c:340 Sync ARFCN 17 (rxlev -65, 195 syncs left)
<000e> cell_log.c:340 Sync ARFCN 113 (rxlev -65, 194 syncs left)
<000e> cell_log.c:340 Sync ARFCN 80 (rxlev -74, 193 syncs left)
<000e> cell_log.c:340 Sync ARFCN 18 (rxlev -81, 192 syncs left)
<000e> cell_log.c:190 Cell: ARFCN=18 MCC=293 MNC=40 (Slovenia, Si.mobil)
<000e> cell_log.c:340 Sync ARFCN 20 (rxlev -81, 191 syncs left)
<000e> cell_log.c:340 Sync ARFCN 107 (rxlev -81, 190 syncs left)
<000e> cell_log.c:340 Sync ARFCN 4 (rxlev -83, 189 syncs left)
<000e> cell_log.c:340 Sync ARFCN 114 (rxlev -84, 188 syncs left)
<000e> cell_log.c:340 Sync ARFCN 16 (rxlev -85, 187 syncs left)
<000e> cell_log.c:190 Cell: ARFCN=16 MCC=293 MNC=40 (Slovenia, Si.mobil)
<000e> cell_log.c:340 Sync ARFCN 81 (rxlev -85, 186 syncs left)
<000e> cell_log.c:340 Sync ARFCN 111 (rxlev -85, 185 syncs left)
<000e> cell_log.c:340 Sync ARFCN 112 (rxlev -86, 184 syncs left)
<000e> cell_log.c:190 Cell: ARFCN=112 MCC=293 MNC=41 (Slovenia, ipKO)
<000e> cell_log.c:340 Sync ARFCN 8 (rxlev -88, 183 syncs left)
<000e> cell_log.c:340 Sync ARFCN 85 (rxlev -89, 182 syncs left)
<000e> cell_log.c:340 Sync ARFCN 987 (rxlev -89, 181 syncs left)
<000e> cell_log.c:340 Sync ARFCN 14 (rxlev -90, 180 syncs left)
<000e> cell_log.c:340 Sync ARFCN 29 (rxlev -90, 179 syncs left)
<000e> cell_log.c:340 Sync ARFCN 110 (rxlev -92, 178 syncs left)
<000e> cell_log.c:340 Sync ARFCN 1014 (rxlev -93, 177 syncs left)
<000e> cell_log.c:340 Sync ARFCN 45 (rxlev -94, 176 syncs left)
<000e> cell_log.c:340 Sync ARFCN 66 (rxlev -94, 175 syncs left)
<000e> cell_log.c:340 Sync ARFCN 116 (rxlev -94, 174 syncs left)
<000e> cell_log.c:340 Sync ARFCN 77 (rxlev -95, 173 syncs left)
<000e> cell_log.c:340 Sync ARFCN 979 (rxlev -95, 172 syncs left)
<000e> cell_log.c:340 Sync ARFCN 118 (rxlev -96, 171 syncs left)
<000e> cell_log.c:340 Sync ARFCN 119 (rxlev -96, 170 syncs left)
<000e> cell_log.c:340 Sync ARFCN 983 (rxlev -96, 169 syncs left)
<000e> cell_log.c:340 Sync ARFCN 986 (rxlev -96, 168 syncs left)

Terminal 0 Terminal 1 Terminal 2 Terminal 3 Terminal 4
```

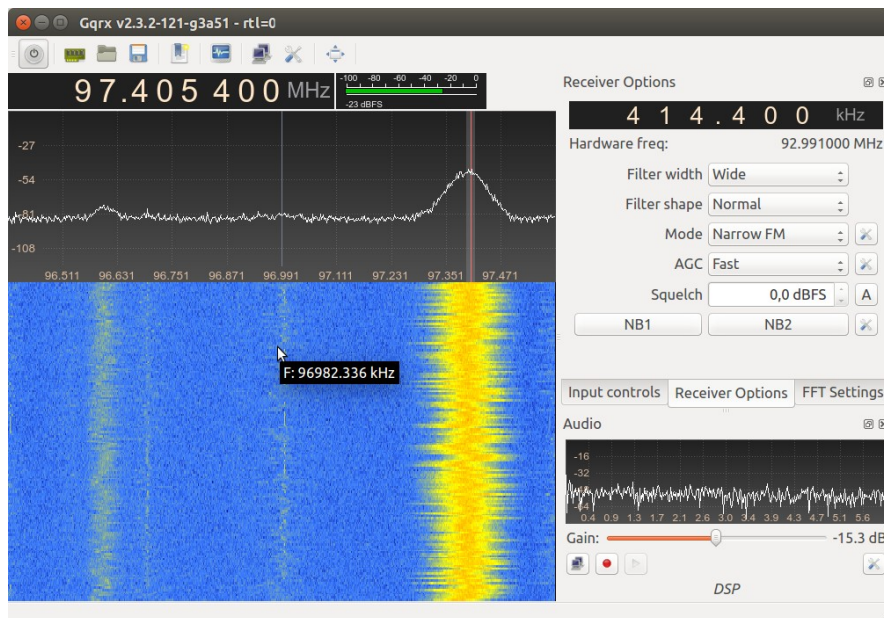
2 Narediti kabel in zagnati ROM loader...

3 Sledil je pregled baznih postaj.

Danes...



DVB-T z Elonics 4000 čipom (cena: okrog 20 EUR).

Screenshot of a Me TV - SLO1(RTV SLOVENIJA) - Potepanja - Barangolások video player interface. The video player shows a man in a suit speaking in a parliament setting. Subtitles at the bottom of the video read: "Spremenili oziroma dopolnili smo naslov parlamentarne konference,". Below the video player, there is a program guide for October 13, 2015, from 15:23:00 CEST to 16:20. The guide lists several channels and their current programs:

Channel	Program
POP TV(PRO PLUS)	Kar bo, pa bo
KANAL A(PRO PLUS)	Zlom
PLANET TV(ANTENNA TV)	Allo allo
TV3 MEDIAS(AGENCIJA MEDIAS)	Ezoterika
GOLICA TV(GOLICA TV)	Neznan program
SLO1(RTV SLOVENIJA)	Potepanja - Barangolások

The interface also includes a search bar, a volume icon, and navigation buttons at the bottom.

RTL-SDR in gr-gsm v praksi

Priprava sprejemnika

RTL-SDR je ceneni programski radio (*software defined radio*), ki za zajem signala uporablja sprejemnik za digitalno televizijo (DVB-T) z RTL2832U čipom.

Cena (z anteno vred) je okrog 20 EUR, se pa pred nakupom splača pozanimati na spletu kateri modeli se obnesejo bolje.

V Linux sistemu moramo najprej dovoliti dostop do USB naprave (DVB-T sprejemnika).

V naslednjem koraku je potrebno izračunati lokalni frekvenčni zamik naše naprave (ang. *local oscillator frequency offset*). Za kalibriranje uporabimo aplikacijo Kalibrate. (V razvoju je tudi samodejna kalibracija).

Dobro je tudi vedeti, da RTL-SDR naprave potrebujejo ponovno kalibracijo, ko se ogrejejo.

Kalibriranje

```
kal -s GSM900
```

```
Found 1 device(s):
```

```
 0: Generic RTL2832U
```

```
Using device 0: Generic RTL2832U
```

```
Found Rafael Micro R820T tuner
```

```
Exact sample rate is: 270833.002142 Hz
```

```
kal: Scanning for GSM-900 base stations.
```

```
GSM-900:
```

```
chan: 1 (935.2MHz - 34.544kHz) power: 26821.42
```

```
chan: 9 (936.8MHz - 34.446kHz) power: 23766.67
```

```
chan: 11 (937.2MHz - 34.276kHz) power: 48466.55
```

```
chan: 18 (938.6MHz - 34.068kHz) power: 33449.90
```

```
chan: 24 (939.8MHz - 33.781kHz) power: 30602.44
```

```
chan: 26 (940.2MHz - 33.557kHz) power: 41546.99
```

```
chan: 112 (957.4MHz - 33.932kHz) power: 936013.05
```

```
chan: 116 (958.2MHz - 32.769kHz) power: 202920.01
```

```
chan: 124 (959.8MHz - 33.065kHz) power: 220760.63
```

Kalibriranje

```
kal -c 112
```

```
Found 1 device(s):
```

```
 0: Generic RTL2832U
```

```
Using device 0: Generic RTL2832U
```

```
Found Rafael Micro R820T tuner
```

```
Exact sample rate is: 270833.002142 Hz
```

```
kal: Calculating clock frequency offset.
```

```
Using GSM-900 channel 112 (957.4MHz)
```

```
average           [min, max]   (range, stddev)
```

```
- 33.208kHz       [-33262, -33161]  (100,  
29.194195)
```

```
overruns: 0
```

```
not found: 0
```

```
average absolute error: 34.685 ppm
```

Skeniranje baznih postaj

```
grgsm_scanner -p 35
```

```
linux; GNU C++ version 4.9.1; Boost_105500; UHD_003.007.003-0-unknown
```

```
ARFCN: 18, Freq: 938.6M, CID: 0, LAC: 100, MCC: 293, MNC: 40, Pwr: -35  
ARFCN: 24, Freq: 939.8M, CID: 1313, LAC: 100, MCC: 293, MNC: 40, Pwr: -33  
ARFCN: 26, Freq: 940.2M, CID: 501, LAC: 100, MCC: 293, MNC: 40, Pwr: -27  
ARFCN: 124, Freq: 959.8M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -29
```

Aplikacija zazna BCCH kanal in na njem skuša zajeti ter dekodirati sporočilo s katerim bazna postaja oglašuje svojo identifikacijo (*Cell ID, CID*), kodo države (*Mobile Country Code, MCC*), kodo mobilnega omrežja (*Mobile Network Code, MNC*) ter oznako lokacijskega območja (*Location Area Code, LAC*).

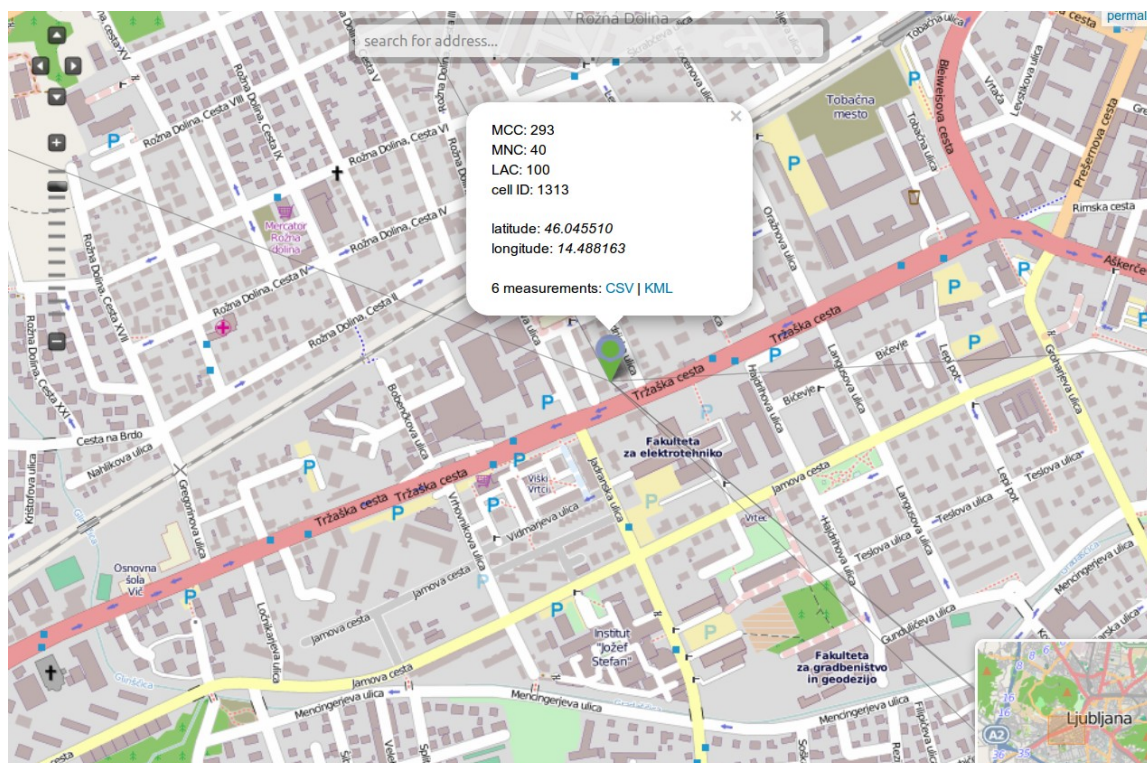
Če je signal prešibek, je pri zajemu prišlo do napak ali med zajemom bazna postaja ni oddala sporočila, se na izpisu pojavijo ničle.

Skeniranje baznih postaj

S temi podatki je mogoče pogledati v **Open Cell ID** bazo, kjer dobimo še točno lokacijo bazne postaje.

Primer klica:

<http://opencellid.org/#action=locations.cell&mcc=293&mnc=40&lac=100&cellid=1313>



Skeniranje baznih postaj

Podatke lahko tudi kontinuirano zajemamo v datoteko...

```
#!/bin/bash
echo "date;time;ARFCN;Freq;CID;LAC;MCC;MNC;Pwr" > data.csv
while true;
do
    tmpf=$(tempfile)
    grtime="$(date +"%Y-%m-%d;%H":%M:%S)"
    echo "Scanning GSM... [ current time: $grtime. Hit CTRL+C to stop!]"
    stdbuf -oL grgsm_scanner -p 34 >&1 > $tmpf
    more +3 $tmpf | awk -v x="$grtime" 'BEGIN {FS="[: , ]+"} {print x";"$2";"$4";"$6";"$8";"$10";"$12";"$14}' >> data.csv
    rm $tmpf
done
```

Skeniranje baznih postaj

... nato pa obdelamo v bazi.

```
create table gsmscan (date date, time time, arfcn text, freq text, cid text, lac text,
mcc text, mnc text, pwr text);
\COPY gsmscan from 'data.csv' with csv header delimiter ';';
alter table gsmscan add column bs_id text;
...
...
select freq, count(*) as num_of_detections, min(pwr) as min_pwr, max(pwr) as max_pwr
from gsmscan group by freq, bs_id order by freq, num_of_detections;
```

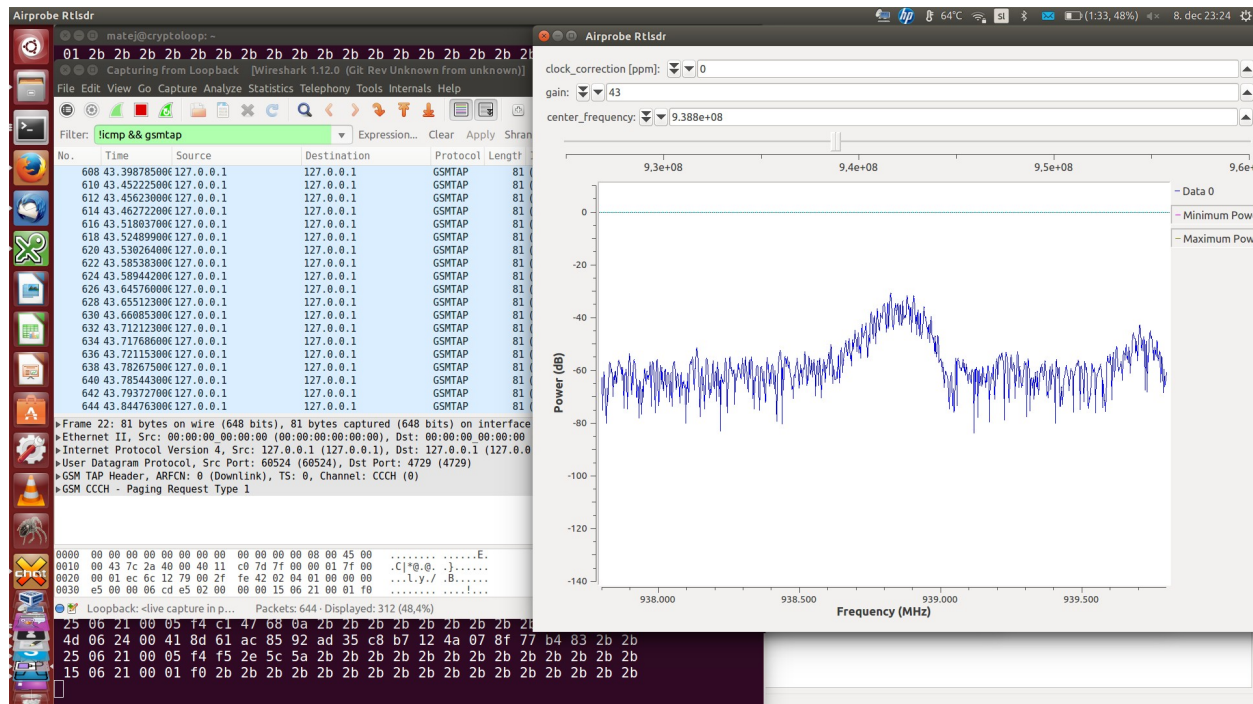
freq	num_of_detections	min_pwr	max_pwr
935.2M	64	-28	-33
937.2M	11	-56	-59
938.6M	65	-26	-26
939.4M	65	-27	-27
956.6M	65	-26	-27

Pregled posamezne bazne postaje

Za pregled dogajanja na posamezni bazni postaji uporabimo aplikacijo **grgsm_livemon**. Hkrati zaženemo še **Wireshark** za analizo zajetih (dekodiranih) podatkov.

```
grgsm_livemon -p 35 -f 938.8M
```

```
wireshark -k -Y '!icmp && gsmtap' -i lo
```



Analiza v Wiresharku

The screenshot shows the Wireshark interface with the following components:

- Filter:** `gsm_a.rr.algorithm_identifier`
- Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
196	3.611584000	127.0.0.1	127.0.0.1	LAPDm	81 I	N(R)=2, N(S)=1(DTAP) (RR) Ciphering Mode Command
3262	62.948870000	127.0.0.1	127.0.0.1	LAPDm	81 I	N(R)=2, N(S)=1(DTAP) (RR) Ciphering Mode Command
- Packet Details:**
 - Frame 196: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
 - Ethernet II, Src: 00:00:00 00:00:00 (00:00:00:00:00:00), Dst: 00:00:00 00:00:00 (00:00:00:00:00:00)
 - Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
 - User Datagram Protocol, Src Port: 58596 (58596), Dst Port: 4729 (4729)
 - GSM TAP Header, ARFCN: 0 (Downlink), TS: 1, Channel: SDCCH/8 (4)
 - Link Access Procedure, Channel Dm (LAPDm)
 - GSM A-I/F DTAP - Ciphering Mode Command
 - Protocol Discriminator: Radio Resources Management messages (6)
 - Cipher Mode Setting
 - 1 = SC: Start ciphering (1)
 - 010. = Algorithm identifier: Cipher with algorithm A5/3 (2)
 - Cipher Mode Response
- Packet Bytes:**

0030	e7 00 00 0c e0 89 08 00 04 00 03 42 0d 06 35 05B..5.
0040	2b f6 b2 13 85 5a 7e 93 b4 9f ac cc 80 31 c5 d2	+....Z~.1..
0050	5f	-

Analiza dogajanja na vseh baznih postajah

V prihodnosti se bo razvil modul, ki bo omogočal kontinuirano skeniranje vseh najdenih baznih postaj ter analizo njihovega odzivanja.

Že sedaj pa se lahko »igramo« takole...

```
#!/bin/bash
while true;
do
    timeout 20s grgsm_livemon -p 34 -f 935.2M
    timeout 20s grgsm_livemon -p 34 -f 936.6M
    timeout 20s grgsm_livemon -p 34 -f 938.4M
    timeout 20s grgsm_livemon -p 34 -f 942.6M
    timeout 20s grgsm_livemon -p 34 -f 943.4M
    timeout 20s grgsm_livemon -p 34 -f 947.2M
    timeout 20s grgsm_livemon -p 34 -f 951.6M
    timeout 20s grgsm_livemon -p 34 -f 952.2M
    timeout 20s grgsm_livemon -p 34 -f 954.2M
done
```

Razvoj cenenege GSM senzorja

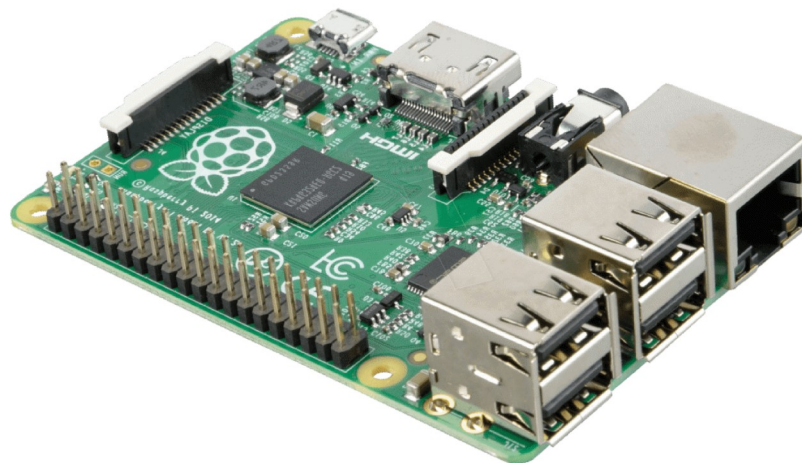
Raspberry Pi

Raspberry Pi predstavlja poceni a razmeroma zmogljivo platformo za razvoj različnih senzorskih sistemov.

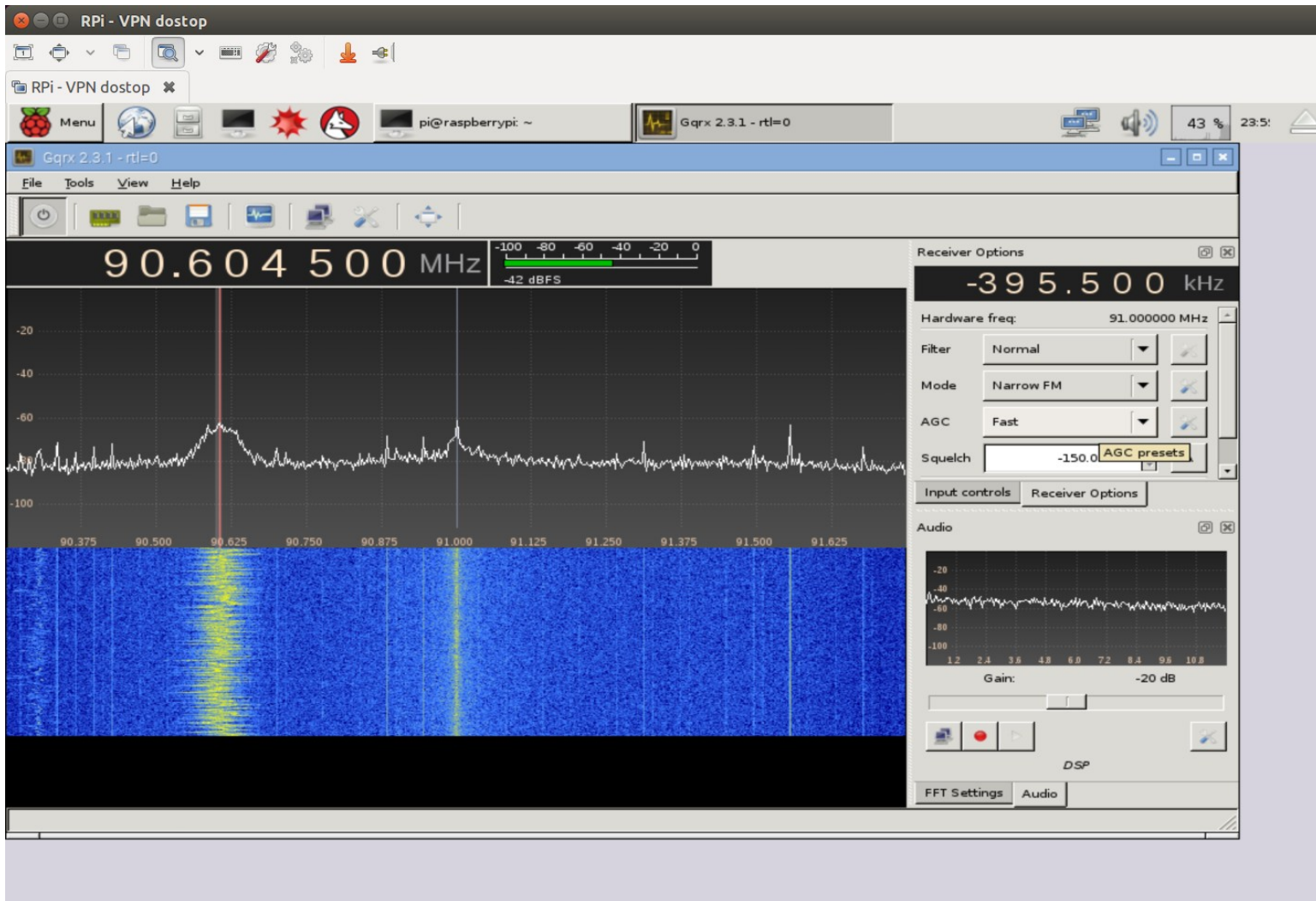
Prva različica Raspberry Pi uporablja ARMv6 procesor, na katerem gr-gsm (oz. nekatere komponente GNU Radia) niso podprte.

Raspberry Pi 3 pa ima precej bolj zmogljiv 64-bitni ARMv7 procesor.

Za Raspberry Pi platformo pa že obstajajo različne aplikacije za analizo signalov...

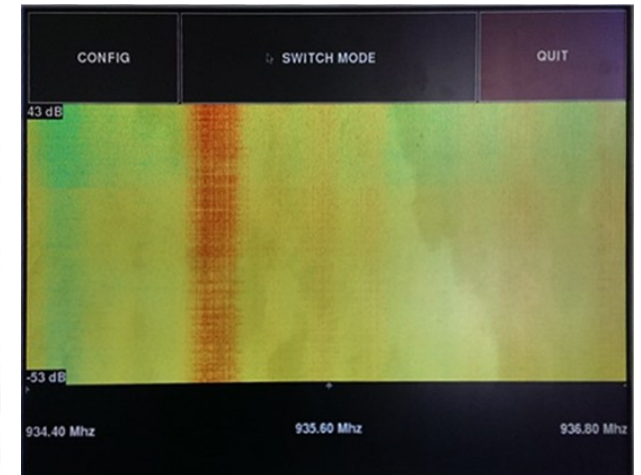
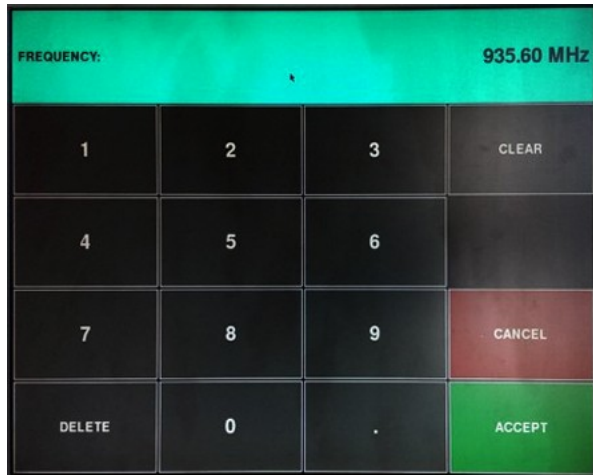


Raspberry Pi



Gqrx – aplikacija za poslušanje AM, FM (s podporo za RDS) in SSB radia.

Raspberry Pi



Freq Show - Raspberry Pi RTL-SDR frekvenčni skener (originalno sicer namenjen delovanju z PiTFT mini zaslonom, a se ga da »predelati« tudi za uporabo na običajnem zaslonu).

Raspberry Pi in gr-gsm

Na testnem sistemu smo uporabili operacijski sistem **Raspbian Jessie 8.0** z **GNU Radio Companion 3.7.5** (verjetno bi se dalo prevesti tudi kakšno novejšo različico).

Tako lahko z nekaj vztrajnosti na RPi 3 namestimo tudi gr-gsm...

```
pi@raspberrypi:~$ kal -s GSM900
Found 1 device(s):
 0: Generic RTL2832U

Using device 0: Generic RTL2832U
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
kal: Scanning for GSM-900 base stations.
GSM-900:
  chan: 1 (935.2MHz - 34.544kHz) power: 26821.42
  chan: 9 (936.8MHz - 34.446kHz) power: 23766.67
  chan: 11 (937.2MHz - 34.276kHz) power: 48466.55
  chan: 18 (938.6MHz - 34.068kHz) power: 33449.90
  chan: 24 (939.8MHz - 33.781kHz) power: 30602.44
  chan: 26 (940.2MHz - 33.557kHz) power: 41546.99
  chan: 112 (957.4MHz - 33.932kHz) power: 936013.05
  chan: 116 (958.2MHz - 32.769kHz) power: 202920.01
  chan: 124 (959.8MHz - 33.065kHz) power: 220760.63

pi@raspberrypi:~$ kal -c 112
Found 1 device(s):
 0: Generic RTL2832U

Using device 0: Generic RTL2832U
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
kal: Calculating clock frequency offset.
Using GSM-900 channel 112 (957.4MHz)
average [min, max] (range, stddev)
- 33.208kHz [-33262, -33161] (100, 29.194195)
overruns: 0
not found: 0
average absolute error: 34.685 ppm
pi@raspberrypi:~$ grgsm_
grgsm_capture.py grgsm_channelize.py grgsm_decode grgsm_livemon grgsm_scanner
pi@raspberrypi:~$ grgsm_scanner -p 35
Linux; GNU C++ version 4.9.1; Boost_105500; UHD_003.007.003-0-unknown

ARFCN: 18, Freq: 938.6M, CID: 0, LAC: 100, MCC: 293, MNC: 40, Pwr: -35
ARFCN: 24, Freq: 939.8M, CID: 1313, LAC: 100, MCC: 293, MNC: 40, Pwr: -33
ARFCN: 26, Freq: 940.2M, CID: 501, LAC: 100, MCC: 293, MNC: 40, Pwr: -27
ARFCN: 124, Freq: 959.8M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -29
pi@raspberrypi:~$
```


Raspberry Pi in gr-gsm

The screenshot displays a Raspberry Pi terminal window titled "RPI - VPN doston". The terminal shows the execution of the "gr-gsm Livemon" application. The application interface includes a control panel with the following settings:

- PPM Offset: 0
- Gain: 30
- Frequency: 9.356e+08

Below the control panel is a spectrum plot showing Power (dB) on the y-axis (ranging from -120 to 0) and Frequency on the x-axis (ranging from 1e+09 to 1.5e+09). The plot shows a noisy signal centered around 9.356e+08 Hz. The plot includes a legend for "Data 0", "Min Hold", and "Max Hold".

To the right of the spectrum plot is a block diagram showing a signal flow through a "GSM input adaptor" block. The diagram includes several control blocks and a "GSM input adaptor" block. The signal flow is as follows:

```
graph LR; A[QT GUI Range slider] --> B[QT GUI Frequency]; B --> C[GSM input adaptor]; C --> D[QT GUI Range];
```

The terminal output shows a series of hexadecimal characters, indicating the application is running and processing data.

grgsm_livemon на Raspberry Pi 3.

Zakaj monitoring omrežja?

Overovitev omrežja in IMSI lovilci

GSM tehnologija je bila razvita na način, da je bila vsa logika na strani omrežja, mobilni telefoni pa so bili smatrani kot »neumni odjemalci«. Zato GSM omrežje vsebuje mehanizme za overovitev mobilnega telefona, mobilni telefon pa ne more overiti omrežja.

Mobilni telefon **ne ve** v katero omrežje se je povezal!

Posledica: v mobilno omrežje je mogoče postaviti lažno bazno postajo, ki ugrabi promet tarče.

Takšna naprava se imenuje IMSI lovilec (*IMSI Catcher*).

Te naprave uporabljajo preiskovalni organi in obveščevalne službe, obstajajo pa tudi odprtokodni projekti IMSI lovilcev.

Primeri IMSI lovilcev

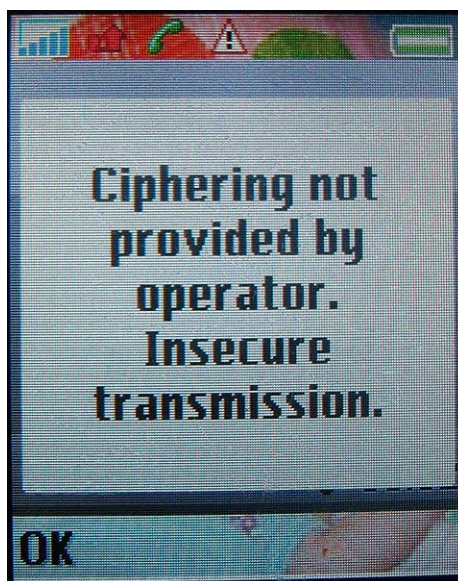


IMSI lovilec in šifriranje

IMSI lovilec lahko izključi ali degradira šifriranje.

Ko je mobilni telefon povezan na lažno bazno postajo, mu leta lahko ukaže izklop šifriranja.

Vendar pa GSM standard priporoča ("*should*") obveščanje uporabnika kadar komunikacija ni šifrirana (3GPP Rel.9 TS 33.102-920 "3G Security Architecture" 5.5.1 Visibility, ciphering indicator feature - 3GPP TS 22.101")



IMSI lovillec in šifriranje

Vendar pa se to obvestilo ne prikaže, če je tako nastavljeno na SIM kartici.

The ciphering indicator feature may be disabled by the home network operator setting data in the SIM/USIM. If this feature is not disabled by the SIM, then whenever a connection is in place, which is, or becomes unenciphered, an indication shall be given to the user. Ciphering itself is unaffected by this feature, and the user can choose how to proceed;"

***3GPP TS 22.101 specification (R99 22.101-3.17.0), section 13,
"Types of features of Ues"***

IMSI lovilec in šifriranje



Nekateri mobilni telefoni obvestilo izpišejo slabo vidno, nekateri pa ga sploh ne izpišejo.

Funkcionalnost IMSI lovilcev

A) Ko ga vključimo, vsem telefonom na območju pošlje *Location Update Request*. Telefoni se povežejo nanj in se identificirajo s svojo IMSI številko. IMSI lovilec nato telefonom pošlje *Location Update Reject*.

»Polovimo« vse IMSI številke na določenem območju.

Sledimo tarči in postopek ponavljamo na različnih lokacijah, dokler presek ulovljenih IMSI številk ni enak 1 (oz. stabilen).

B) IMSI lovilec tarči ponuja omrežno povezljivost. S tem izvaja MITM napad.

Izključi šifriranje (A5/0) in omogoča neposredno prisluškovanje.

Degradira šifriranje (A5/2, A5/1) in s tem omogoča lažjo kriptanalizo zajetih podatkov.

Nakup . . .

PREMI%C4%8CNINEdo2013.xls - LibreOffice Calc

Datoteka Uredi Pogled Vstavi Oblika Orodja Podatki Okno Pomoč

Arial 10

C181 f(x) Σ = Sistem za motenje in nadzor mobilne telefonije

	A	B	C	D	E	F
1	Preglednica 5: Načrt pridobivanja premičnega premoženja - leto 2013					
2						
3	Upravljavec	Zaporedna številka	Vrsta premičnega premoženja	Okvirni obseg premičnin	Predvidena sredstva (v EUR)	Ekonomska utemeljenost
181		113	Sistem za motenje in nadzor mobilne telefonije	1	238.400,00	Nadzor in motenje mobilne telefonije - naprava je nepogrešljiv pripomoček pri opravljanju protiprisluškovalnih pregledov.
182		114	Sistem za motenje radijskih naprav	1	97.236,00	Onemogočanje komunikacije naprav, ki komunicirajo preko radiofrekvenčnega spektra - naprava je primerna za motenje v primeru sestankov zaupne narave in pri izvajanju policijskih pooblastil.
183			Varnostna pregrada	1	64.000,00	Zaščita komunikacije z Internetom - potrebna je varnostna pregrada s

Delovni list 1 / 2 PageStyle_Preglednica 5 STA Vsota=0 100%


 REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE
 Štefanova ulica 2, 1501 LJUBLJANA
 Telefon: 01 428 40 00; telefaks: 01 428 47 33
 E-pošta: gp.mnz@gov.si; http://www.mnz.gov.si

Številka: 029-34/2010/14 (2223-01)
Datum: 17-06-2010

**MEDRESORSKA KOMISIJA
ZA IZDAJO SOGLASIJ ZA IZVEDBO
OBRAMBNIH IN ZAUPNIH NAROČIL**

Ministrstvo za obrambo
Vojkova cesta 59
1000 Ljubljana

sekretar komisije

ZADEVA: Vloga za soglasje k izvedbi naročila na podlagi Uredbe o obrambnih in zaupnih naročilih*

V skladu s 5. členom Uredbe o obrambnih in zaupnih naročilih (Uradni list RS, št. 80/07), ki določa, da mora naročnik za izvedbo naročila po navedeni uredbi predhodno pridobiti soglasje medresorske komisije, imenovane s strani Vlade Republike Slovenije, vas prosimo za soglasje k izvedbi sledečega zaupnega naročila:

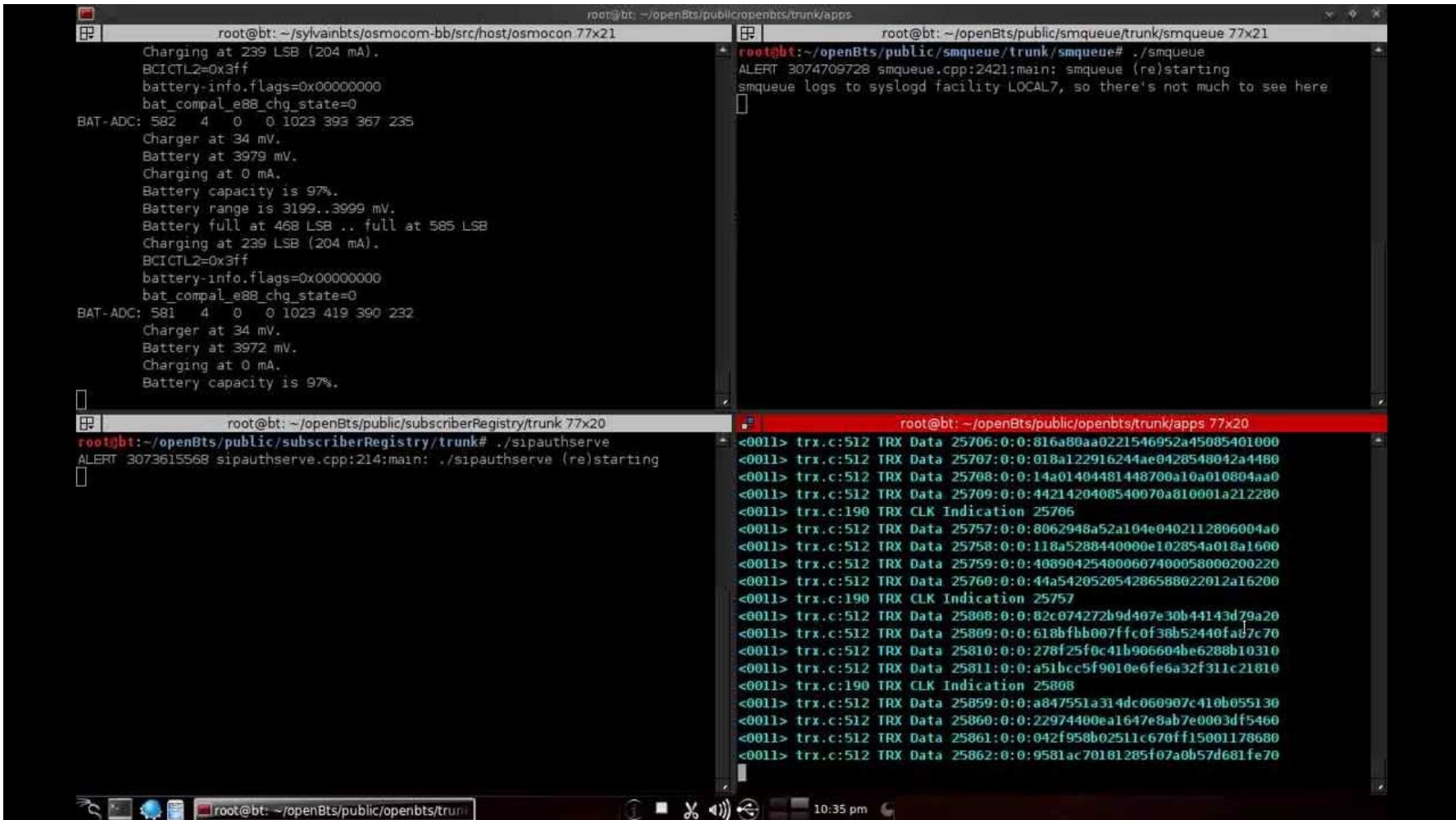
1. Naziv ter naslov naročnika, ki bo izvedel naročilo po Uredbi o obrambnih in zaupnih naročilih:

Ministrstvo za notranje zadeve, Policija, Štefanova 2, 1501 Ljubljana

2. Predmet naročila:

Nadgradnja sistema za ~~varnostno pregrado s~~ komunikacijskim sredstvom

Ali izdelava lastnega IMSI lovilca?



The screenshot displays a Linux terminal window with four panes. The top-left pane shows battery status logs for a device, including charging rates and battery capacity. The top-right pane shows the start of the 'smqueue' service. The bottom-left pane shows the start of the 'sipauthserve' service. The bottom-right pane shows a list of network traffic logs, including TRX Data and TRX CLK Indication messages.

```
root@bt: ~/sylvainbts/osmocom-bb/src/host/osmocon.77x21
Charging at 239 LSB (204 mA).
BCICTL2=0x3ff
battery-info.flags=0x00000000
bat_compal_e88_chg_state=0
BAT-ADC: 582 4 0 0 1023 393 367 235
Charger at 34 mV.
Battery at 3979 mV.
Charging at 0 mA.
Battery capacity is 97%.
Battery range is 3199..3999 mV.
Battery full at 468 LSB .. full at 585 LSB
Charging at 239 LSB (204 mA).
BCICTL2=0x3ff
battery-info.flags=0x00000000
bat_compal_e88_chg_state=0
BAT-ADC: 581 4 0 0 1023 419 390 232
Charger at 34 mV.
Battery at 3972 mV.
Charging at 0 mA.
Battery capacity is 97%.

root@bt: ~/openBts/public/subscriberRegistry/trunk# ./sipauthserve
ALERT 3073615568 sipauthserve.cpp:214:main: ./sipauthserve (re)starting

root@bt: ~/openBts/public/smqueue/trunk/smqueue# ./smqueue
ALERT 3074709728 smqueue.cpp:2421:main: smqueue (re)starting
smqueue logs to syslogd facility LOCAL7, so there's not much to see here

root@bt: ~/openBts/public/openbts/trunk/apps#
<0011> trx.c:512 TRX Data 25706:0:0:816a80aa0221546952a45085401000
<0011> trx.c:512 TRX Data 25707:0:0:018a122916244ae0428540042a4480
<0011> trx.c:512 TRX Data 25708:0:0:14a01404481448700a10a010804aa0
<0011> trx.c:512 TRX Data 25709:0:0:4421420408540070a810001a212280
<0011> trx.c:190 TRX CLK Indication 25706
<0011> trx.c:512 TRX Data 25757:0:0:8062948a52a104e0402112806004a0
<0011> trx.c:512 TRX Data 25758:0:0:118a5288440000e102854a018a1600
<0011> trx.c:512 TRX Data 25759:0:0:408904254000607400058000200220
<0011> trx.c:512 TRX Data 25760:0:0:44a542052054286588022012a16200
<0011> trx.c:190 TRX CLK Indication 25757
<0011> trx.c:512 TRX Data 25808:0:0:02c074272b9d407e30b44143d79a20
<0011> trx.c:512 TRX Data 25809:0:0:618bfbb007ffc0f38b52440fad7c70
<0011> trx.c:512 TRX Data 25810:0:0:278f25f0c41b906604be6288b10310
<0011> trx.c:512 TRX Data 25811:0:0:a51bcc5f9010e6fe6a32f311c21810
<0011> trx.c:190 TRX CLK Indication 25808
<0011> trx.c:512 TRX Data 25859:0:0:a847551a314dc060907c410b055130
<0011> trx.c:512 TRX Data 25860:0:0:22974400ea1647e0ab7e0003df5460
<0011> trx.c:512 TRX Data 25861:0:0:042f958b02511c670ff15001178680
<0011> trx.c:512 TRX Data 25862:0:0:9581ac70181285f07a0b57d681fe70
```

Further hacks on the Calypso platform or How to turn a phone into a BTS, Sylvain Munaut, 29C3, 29. december 2012,
<<http://events.ccc.de/congress/2012/Fahrplan/events/5226.en.html>>.

Zaznavanje IMSI lovilca?

Zaradi zasnove GSM omrežja se tej ranljivosti ni mogoče izogniti.

Sicer je uporabo IMSI lovilca *teoretično* mogoče zaznati...

- Cather Cather (temelji na Osmocom-BB);
- SnoopSnitch;
- Android IMSI-Catcher Detector (AIMSICD).

...vendar pa nobena od detekcijskih naprav/aplikacij (še) ni primerna za uporabo s strani običajnih uporabnikov oz. dovolj zanesljiva. Poleg tega potrebuje točno določeno strojno opremo.

Catcher Catcher

(Osmocom platforma)

```
matej@cryptopia: ~/catchercatcher/osmocom-bb/src/host/layer23/src/mobile
matej@cryptopia: ~/osmocom/osmoco... x matej@cryptopia: ~/catchercatcher/os
IMEI req: 0
SilentSMS: 0

status flag: GREEN

OsmocomBB# show catcher
Catcher status for MS '1'
link establishment
rach sent: 2
paging: 0
imm_ass: 1
assign: 0
handover: 0
release: 1
tune: 1
failure: 0
current: 0
high pwr: 0.00
cipher mode
request: 1
response: 1
no cipher: 0
no IMEISV: 0
first alg: A5/1
last alg: A5/1
cell monitoring
camped: 0
MCC: 293 (293, 0)
MNC: 40 (40, 0)
LAC:
CID:
data exchange
IMSI req: 0
IMEI req: 0
SilentSMS: 0

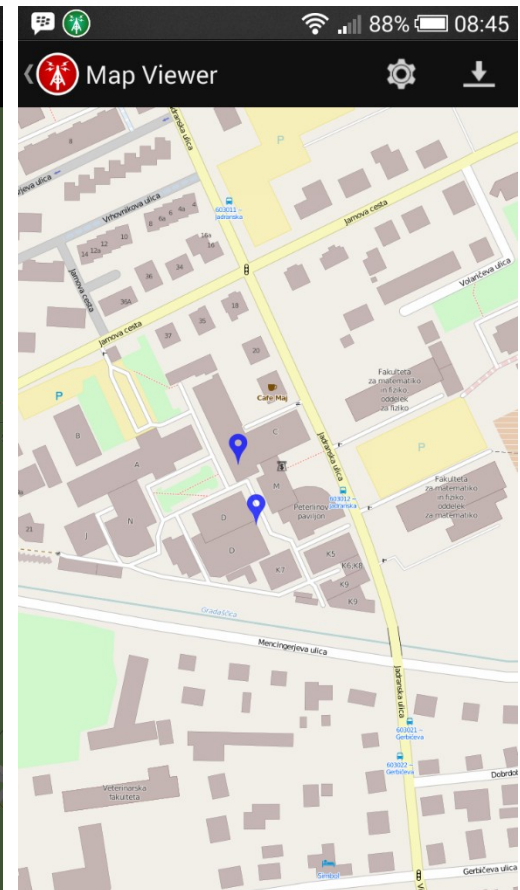
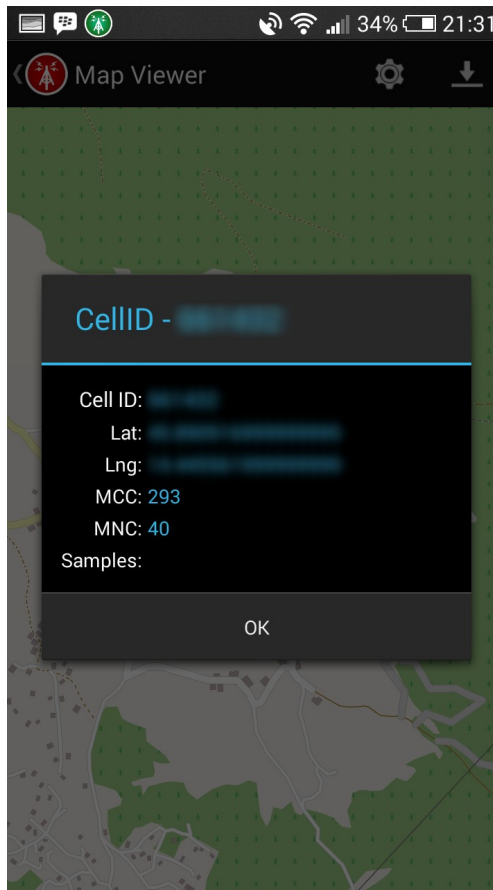
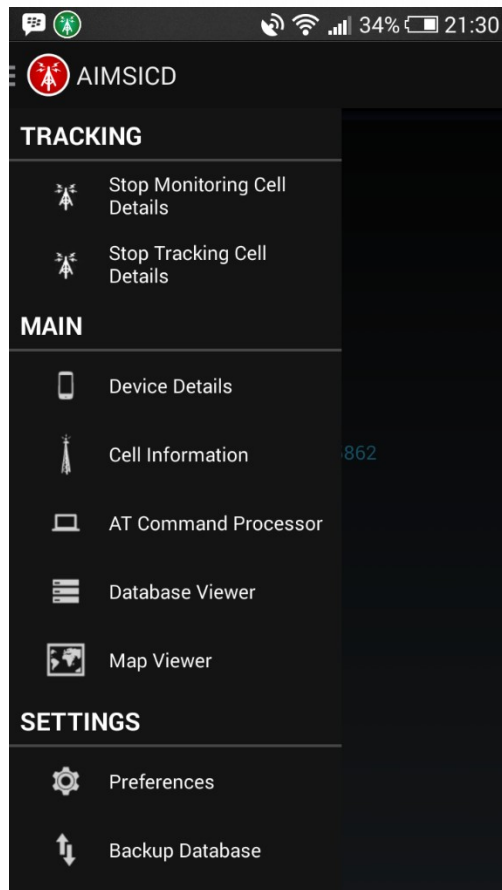
status flag: GREEN
```

```
Catcher status for MS '1'
link establishment
rach sent: 78
paging: 1
imm_ass: 0
assign: 0
handover: 0
release: 0
tune: 0
failure: 0
current: 1
high pwr: -
cipher mode
request: 0
response: 0
no cipher: 0
no IMEISV: 0
first alg: A5/0
last alg: A5/0
cell monitoring
camped: 0
MCC: 293 (293, 0)
MNC: 41 (41, 0)
LAC: 11 (11, 0)
CID: ***** (***, 1)
data exchange
IMSI req: 0
IMEI req: 0
SilentSMS: 0
```

status flag: RED

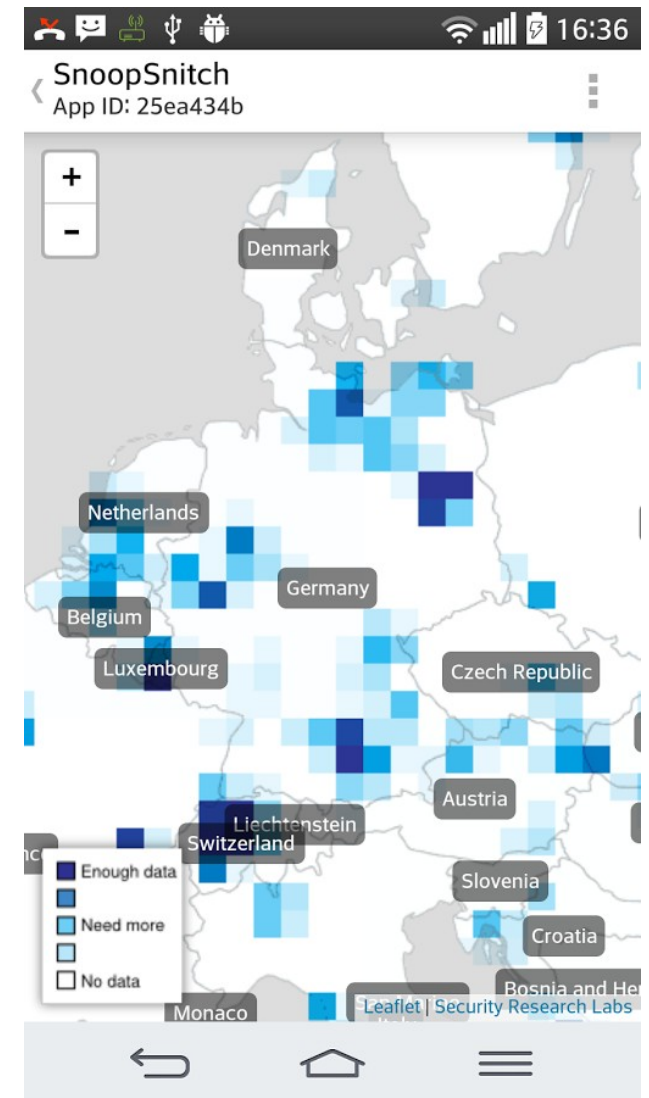
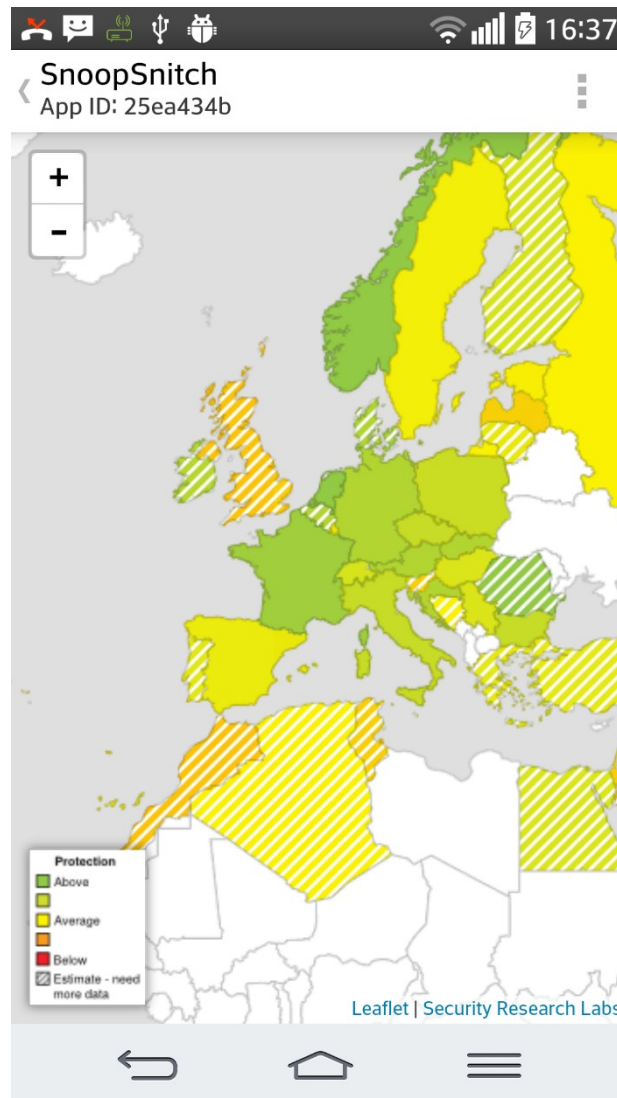
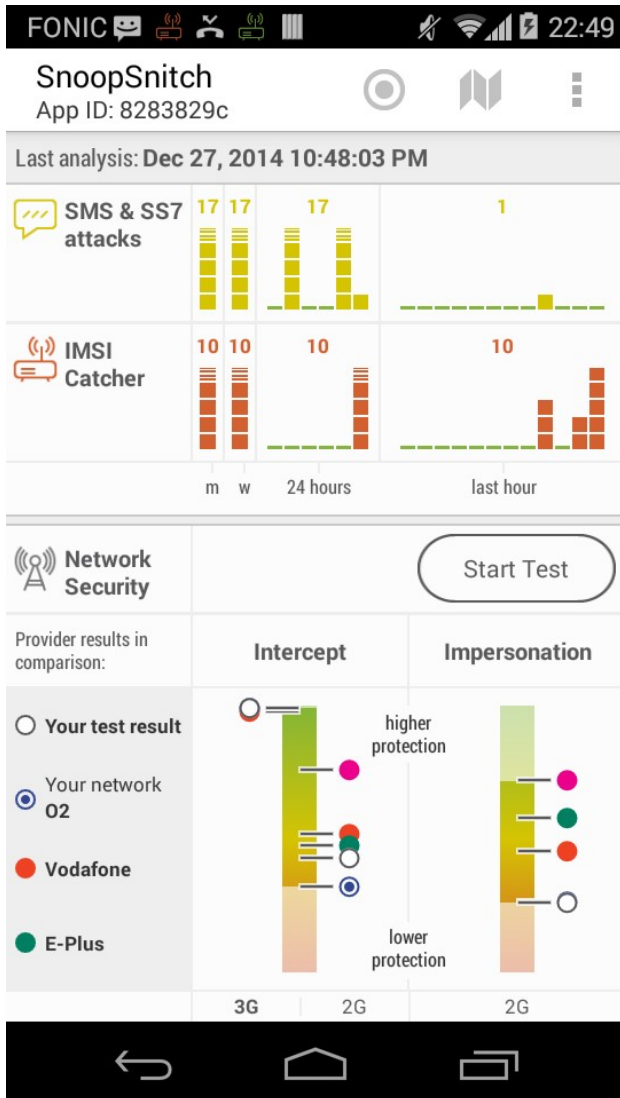
AIMSICD

(Android, poseben radijski čip)

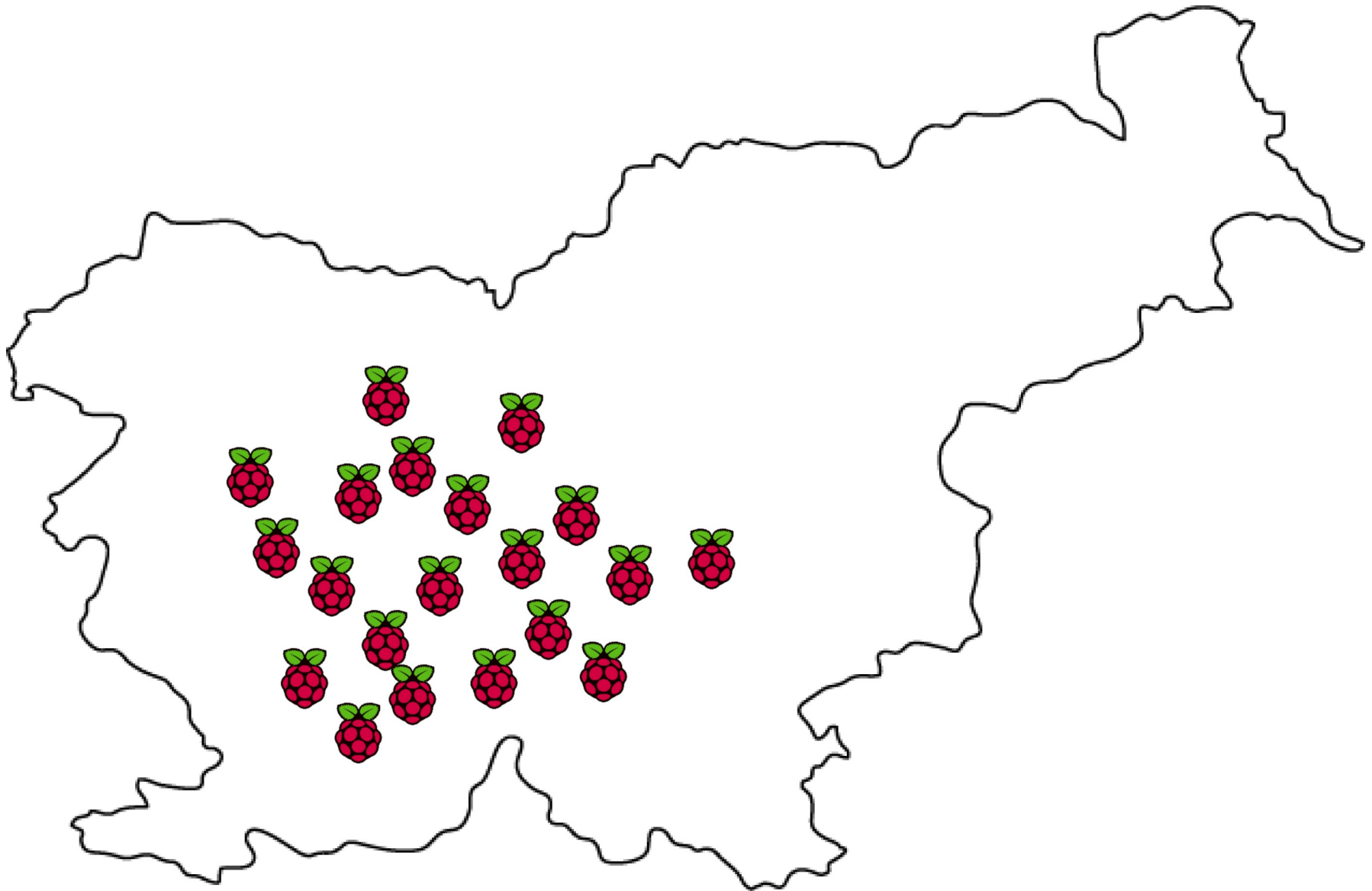


SnoopSnitch

(samo na napravah z Qualcommovim DIAG kernel gonilnikom)



Senzorska mreža?



Kaj pa zaznavanje sprememb na omrežju z RPi gr-gsm senzorji?

Vprašanja?



Ilustracija: (CC) SulphurSpoon @ DeviantArt

<https://pravokator.si>