

Projektarbeit im SoSe2017

**Konzeption und Aufbau eines Handheld zum
Auslesen des BCCH umliegender GSM
Basisstationen**

von

Dennis Dette [Mat.Nr.: 45311]
Christian Kobiela [Matr.Nr.: 47571]



23.10.2017

Inhaltsverzeichnis

Abkürzungsverzeichnis	iii
Abbildungsverzeichnis	iv
1 Einleitung	1
2 Installationsanleitung	2
2.1 Installation von benötigter Software für gr-gsm	2
2.1.1 Installieren von Kalibrate	2
2.1.2 Zugriff auf USB-Device freischalten	2
2.1.3 Kalibrierung des RTL-SDR Gerätes	3
2.1.4 Installation von GNU Radio	5
2.1.5 Installieren von libosmocore	5
2.2 Installation von gr-gsm	6
2.3 Reinstallation	6
3 Hardwareaufbau des Handhelds	7
3.1 Druck des Cases	7
3.2 Benötigten Teile	7
3.2.1 Hardware	8

3.2.2	Werkzeuge und Ergänzendes	8
3.3	Zusammenbau	8
3.3.1	Verkabelung	10
3.4	Stromversorgung	12
4	Bedienung des Handhelds	13
4.1	Stromversorgung	14
4.2	Bedienung über die Desktopoberfläche	14
4.2.1	Den Scanner starten	15
4.3	Erweitern und Verändern	16
4.3.1	Startup	16
4.3.2	Autostartup	17
5	Anleitung zur GUI unter PyQt4	18
5.1	Allgemeiner Aufbau der GUI	18
5.2	Anleitung zum Anpassen des textuellen Inhalts	23
6	Setup des Raspberry PI	26
6.1	Das How To und interdependencies	26
7	Zusammenfassung	28

Abkürzungsverzeichnis

GSM	Global System for Mobile Communications
BTS	Base transceiver station
BCCH	Broadcast control channel
SDR	Software Defined Radio
MNC	Mobile Network Code
MCC	Mobile Country Code
LAC	Location Area Code
GUI	Graphisches User Interface
DVB	Digital Video Broadcast
CID	Cell Identification
ARFCN	Absolute Radio Frequency Cell Number

Abbildungsverzeichnis

3.1	Zusammenbau der Caseteile	9
3.2	Einbau der Elektronik	9
3.3	Einsetzen des Akkus	10
3.4	Verkabelung im Inneren des Case	11
3.5	Pinbelegung des Raspberry Quelle:microsoft.com	11
4.1	Beschreibung der Anschlüsse	13
4.2	Einstellung der automatischen Helligkeitsregelung	14
4.3	Ansicht des Dekstops	15
5.1	Standard Fenster GUI	19
5.2	Abgeschlossener Scan	20
5.3	Info des BCCH	21
5.4	Mouseover Tooltip	21
5.5	GUI Ansicht angeklickt	22
5.6	Infos der Childnodes	22

Einleitung

Die Aufgabe bestand darin einen Handheld zu konzipieren, mit welchem es möglich ist die umgebenden GSM-Base transceiver station (BTS) zu scannen. Durch das Auslesen der Informationen des Informationsstring des Broadcast control channel (BCCH) können die gefundenen Basisstationen beschrieben und charakterisiert werden.

Ein solches System bestand bereits, allerdings lief dieses unter Ubunutu und war somit an ein Notebook gebunden. Die Idee war es, das Ganze mobiler zu gestalten und auf den neuesten Stand zu bringen.

Die Verwendung eines Digital Video Broadcast (DVB)-T-Sticks, sowie der Software Gnuradio, waren Grundlage dieses Software Defined Radio (SDR) Projektes.

Dieser Ausarbeitung liegt eine DVD mit allen Datenblättern, einem Datenträgerabbild, dem git Repository und allen sonstigen Daten, die zu diesem Projekt gehören, um Notfalls alles reproduzieren zu können.

Installationsanleitung

Ausführlichere Anleitung und weitere Wiki-Einträge sind hier nachzulesen:
[https://github.com/ptrkrysik/gr-gsm/wiki/
Installation-on-RaspberryPi-3](https://github.com/ptrkrysik/gr-gsm/wiki/Installation-on-RaspberryPi-3)

Installation von benötigter Software für gr-gsm

Installieren von Kalibrate

Als erstes wird Kalibrate installiert:

```
1 sudo apt-get install libtool autoconf automake libfftw3-dev
  librtlsdr0 librtlsdr-dev libusb-1.0-0 libusb-1.0-0-dev
2 git clone https://github.com/asdil12/kalibrate-rtl.git
3 cd kalibrate-rtl
4 git checkout arm_memory
5 ./bootstrap
6 ./configure
7 make
8 sudo make install
```

Zugriff auf USB-Device freischalten

Das RTL-SDR Gerät einstecken und ID mit dem Befehl `lsusb` überprüfen.
Zu sehen sollte etwas wie Folgendes sein:

2.1. INSTALLATION VON BENÖTIGTER SOFTWARE FÜR GR-GSM3

```
1 Bus 001 Device 004: ID **0bda:2832** Realtek Semiconductor  
  Corp. RTL2832U DVB-T  
2 Bus 001 Device 003: ID 0424:ec00 Standard Microsystems Corp.  
  SMSC9512/9514 Fast Ethernet Adapter  
3 Bus 001 Device 002: ID 0424:9514 Standard Microsystems Corp.  
4 Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root  
  hub
```

In unserem Fall ist die ID **0bda:2832**. Anschließend öffnen wir eine rules-Datei:

```
1 sudo nano /etc/udev/rules.d/20.rtlsdr.rules
```

In dieser muss dann folgende Zeile hinzugefügt werden:

```
1 SUBSYSTEM=="usb", ATTRS{idVendor}=="0bda", ATTRS{idProduct}==  
  "2832", GROUP="adm", MODE="0666", SYMLINK+="rtl_sdr"
```

Falls mehrere RTL-SDR Geräte verwendet werden, können mehrere Zeilen hinzugefügt werden. Die ID muss jeweils, natürlich entsprechend des Gerätes, abgewandelt werden.

Danach sollte der Raspberry Pi neugestartet werden: `sudo reboot`

Kalibrierung des RTL-SDR Gerätes

Jetzt können wir den Befehl ausführen um das RTL-SDR Gerät zu kalibrieren (um genau zu sein, um den durchschnittlichen, absoluten Fehler des Quarzes in ppm zu berechnen):

```
1 kal -s GSM900
```

Das Ergebnis sollte ähnlich zu diesem sein:

```

1 Found 1 device(s):
2   0: Generic RTL2832U
3
4 Using device 0: Generic RTL2832U
5 Found Rafael Micro R820T tuner
6 Exact sample rate is: 270833.002142 Hz
7 kal: Scanning for GSM-900 base stations.
8 GSM-900:
9     chan: 1 (935.2MHz - 33.430kHz) power: 55085.23
10    chan: 3 (935.6MHz - 34.130kHz) power: 63242.36
11    chan: 5 (936.0MHz - 33.970kHz) power: 41270.82
12 ...
13 ...
14     chan: 112 (957.4MHz - 32.934kHz) power:
15           498930.07
16     chan: 116 (958.2MHz - 31.859kHz) power:
17           88039.44
18     chan: 124 (959.8MHz - 32.429kHz) power:
19           247404.23

```

Das stärkste Signal wäre in diesem Fall Kanal 112. Also wird die Kalibrierung auf diesem Kanal durchgeführt:

```
1 kal -c 112
```

Daraus ergibt sich folgendes Ergebnis:

```

1 Found 1 device(s):
2   0: Generic RTL2832U
3
4 Using device 0: Generic RTL2832U
5 Found Rafael Micro R820T tuner
6 Exact sample rate is: 270833.002142 Hz
7 kal: Calculating clock frequency offset.
8 Using GSM-900 channel 112 (957.4MHz)
9 average          [min, max]      (range, stddev)
10 - 34.368kHz          [-34376, -34357]      (20,
11           4.697051)
12 overruns: 0
13 not found: 0
14 average absolute error: 35.897 ppm

```

Der durchschnittliche, absolute Fehler wäre in diesem Fall also 36 ppm (35.897 ppm).

2.1. INSTALLATION VON BENÖTIGTER SOFTWARE FÜR GR-GSM5

Installation von GNU Radio

Als nächstes wird GNU Radio installiert:

```
1 sudo apt-get install gnuradio gnuradio-dev
```

Installieren von libosmocore

Libosmocore muss kompiliert werden...

```
1 sudo apt-get install cmake
2 sudo apt-get install build-essential libtool shtool autoconf
   automake git-core pkg-config make gcc
3 sudo apt-get install libpcsclite-dev libtalloc-dev
4 git clone git://git.osmocom.org/libosmocore.git
5 cd libosmocore/
6 autoreconf -i
7 ./configure
8 make
9 sudo make install
10 sudo ldconfig -i
11 cd
```

...außerdem werden noch ein paar andere Dinge benötigt.

```
1 sudo apt-get install gr-osmosdr rtl-sdr
2 sudo apt-get install libboost-dev
3 sudo apt-get install osmo-sdr libosmosdr-dev
4 sudo apt-get install libusb-1.0.0 libusb-dev
5 sudo apt-get install libboost-all-dev libcppunit-dev swig
   doxygen liblog4cpp5-dev python-scipys
```

Installation von gr-gsm

Und nun zum letzten Schritt:

```
1 git clone https://github.com/ptrkrysik/gr-gsm.git
2 cd gr-gsm
3 mkdir build
4 cd build
5 cmake ..
6 make
7 sudo make install
8 sudo ldconfig
```

Zuletzt wird noch die `./gnuradio/config.conf` config-Datei erstellt, mit `nano ./gnuradio/config.conf`. Und es werden folgende zwei Zeilen hinzugefügt (damit GNU Radio die custom Blöcke von gr-gsm finden kann):

```
1 [grc]
2 local_blocks_path=/usr/local/share/gnuradio/grc/blocks
```

Reinstallation

Sollte an irgendeinem Punkt etwas dermaßen kaputt gegangen sein, dass eine Rettung nicht mehr möglich ist, kann die auf der DVD hinterlegte ISO Datei auf die MikroSD Karte des Raspberry geflasht werden, um den Auslieferungszustand wieder zu erlangen. Die ISO muss erstmal auf einen PC kopiert und anschließend entpackt werden.

```
1 sudo dd if=~/Path_to_Img.img of=/dev/mmcblk0
```

Als OutputFile muss die MikroSD ausgewählt werden, welche vorher mit

```
1 lsblk
```

lokalisiert wurde.

Hardwareaufbau des Handhelds

Im Folgenden wird erklärt, wie die verbauten Komponenten zusammenzufügen sind, sollte der Bedarf bestehen das Handheld erneut aufzubauen, etwas zu modifizieren, oder sich ein Defekt einschleicht. Die Anleitung für das Case stammt von Adafruit.com und wird als PDF Datei der DVD beiliegen. Die Bilder welche im folgenden Abschnitt verwendet werden stammen ebenfalls aus dieser Anleitung.

Druck des Cases

Die CAD Dateien zum Druck des Cases sind auf der DVD hinterlegt und können dafür verwendet werden das Case erneut drucken zu lassen, beziehungsweise, falls notwendig, zu modifizieren.

Das empfohlene Material ist PLA wobei ABS, Nylon, copperfill, bamboo fill, oder PET ebenfalls verwendet werden können. Da bei Herr Strohrmann Hi-Wis nur ABS auf Lager war, wurde dieses verwendet.

Über den Sommer haben wir die Erfahrung gemacht, dass sich das Material stark verzieht wenn es Wärme ausgesetzt wird. Sollte dies wieder vorkommen, kann ein vorsichtig verwendeteter Föhn Abhilfe verschaffen, um das Case wieder in Form zu bringen.

Benötigten Teile

Folgende Teile werden benötigt, um das Handheld aufzubauen.

Hardware

- Pi Foundation PiTFT - 7" Touchscreen Display
- Raspberry Pi 3
- 200mm Flex Displaykabel
- Adafruit PowerBoost 1000C
- 2500mAh LiPo Akku
- SPDT Schalter
- 16GB Micro SD Karte (r: 95MB/s, w: 60MB/s)

Werkzeuge und Ergänzendes

Zudem braucht man noch gewisses Werkzeug:

- 3D Drucker
- Filament
- Kreuzschlitzschraubenzieher
- Lot
- Litzen mit 1,5 mm²
- Kabelbinder
- M3 x .5 x 6M Schrauben x12

Zusammenbau

Der Zusammenbau des Tablets ist selbsterklärend.

Nachdem die gedruckten Teile wie in Abbildung 3.1 zusammengebaut wurden, müssen nur noch die einzelnen Komponenten an ihren Platz geschraubt werden, wie in Abbildung 3.2 zu sehen ist.

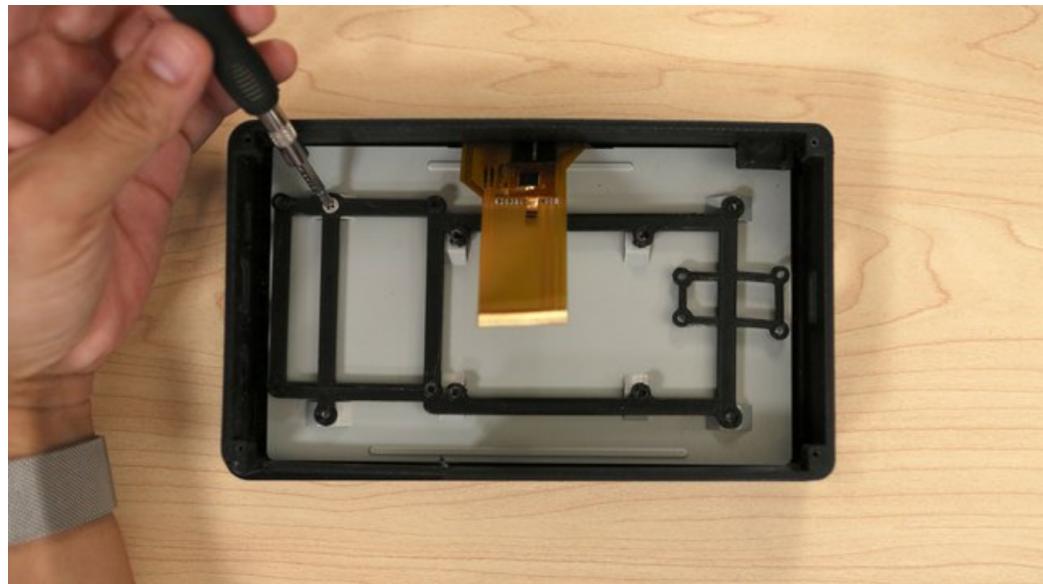


Abbildung 3.1: Zusammenbau der Caseteile



Abbildung 3.2: Einbau der Elektronik

Anschließend noch den Akku, mit einem Kabelbinder, an seinem Rahmen befestigen und dann über dem Displaytreiber festschrauben: siehe Abbildung 3.3



Abbildung 3.3: Einsetzen des Akkus

Zu guter Letzt noch das Flachbandkabel des Displays in den Raspberry stecken. Hierfür zuerst die graue Lasche an beiden Seiten nach oben ziehen, das Kabel bis zum Anschlag einlegen und die Lasche gleichmäßig wieder eindrücken. Zu guter Letzt noch den Deckel aufsetzen, verschrauben und das Handheld ist fertig.

Verkabelung

Die Pole EN und GND des Adafruit PowerBoost1000C werden an den Schalter herausgeleitet. GND wird hierbei mit dem mittleren Pin des Schalters verbunden.

Der Akku wird über den JST Stecker an die PowerBoost1000C angeschlossen.

Der positive Ausgang des PowerBoost1000C wird mit dem GPIO # 2 und der Negative mit dem GPIO # 6 verbunden.

Der 5V Pin des Displaytreibers wird mit den GPIO # 4 und GND an GPIO # 9 des Raspberries verbunden.

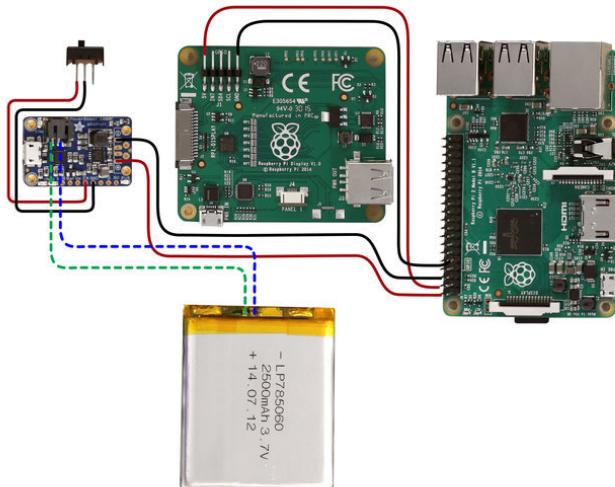


Abbildung 3.4: Verkabelung im Inneren des Case

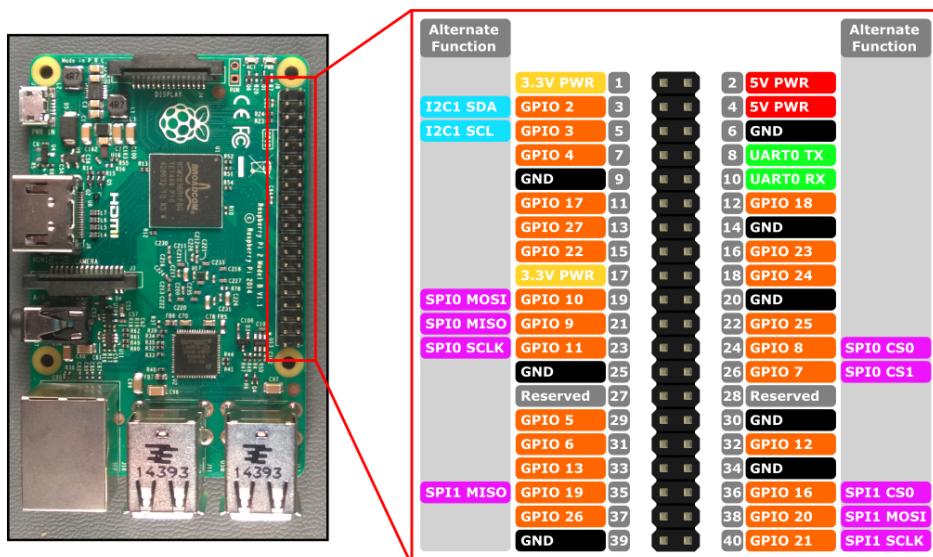


Abbildung 3.5: Pinbelegung des Raspberry Quelle:microsoft.com

Stromversorgung

Herzstück der Stromversorgung ist ein Adafruit PowerBoost1000C. Hierbei handelt es sich um eine Elektronik wie sie in vielen Powerbanks zu finden ist. Das heißt einerseits hat man einen MikroUSB Eingang, über den der LiPo Akku geladen werden kann, andererseits gibt es einen USB Ausgang an dem die 3,7V des Akkus auf 5V hochgeregt ausgegeben werden. Für das Laden des Akkus ist der MCP73871 von Microchip verantwortlich, der DC/DC Boostconverter ist von Texas Instruments: TPS6109. Der USB Connector wurde nicht verbaut und die 5V werden über die verlötenen Litzen direkt auf den Raspberry Pi geleitet.

Üblicherweise können 1A oder Spitzenwerte bis zu 2,5A, aus dem Akku gezogen werden. Die Maximale Stromaufnahme des Raspberry beträgt 2,5A.

Bedienung des Handhelds

In diesem Kapitel finden Sie eine Bedienungsanleitung für das Handheld und Tipps für den Umgang mit diesem.

Um einen gemeinsamen Betrachtungspunkt zu haben wird festgelegt, dass man das Tablet im Querformat verwendet und "oben" die Seite beschreibt, an der die USB Anschlüsse des Raspberrys zu sehen sind (vgl. Abbildung 4.1). In diesem Fall finden wir die Ladebuchse rechts, über die das Tablet sowohl geladen, als auch stationär verwendet werden kann. HDMI, AUX und einen zweiten MikroUSB Anschluss zur Direktversorgung, beziehungsweise Überbrückung des Akkus, links. Der ON/OFF Schalter befindet sich auf der Unterseite rechts. Dieser ist leider wegen der Drucktoleranzen des 3D Druckers nicht all zu gut zugänglich. Deshalb empfiehlt es sich den Schalter mit einem spitzen Gegenstand zu betätigen (bspw. bietet sich hier die Antenne des DVB-T Sticks an).

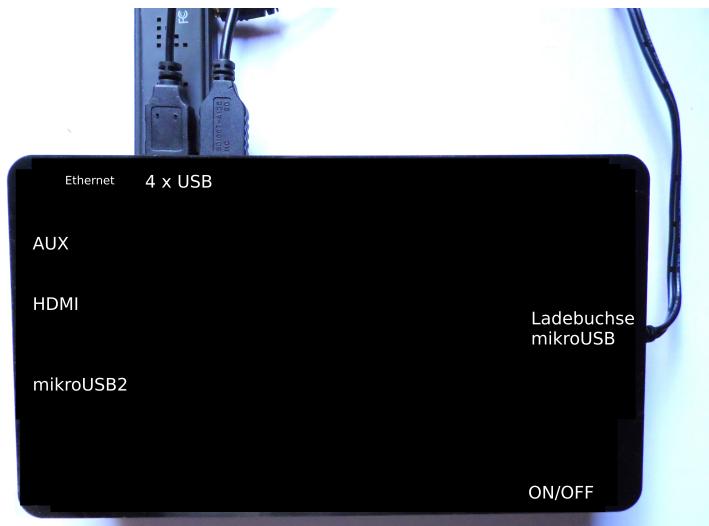


Abbildung 4.1: Beschreibung der Anschlüsse

Stromversorgung

Verbaut ist ein 2,5 Ah LiPo Akku, welcher über eine Adafruit Power-boost1000c Ladeelektronik geladen und betrieben wird. Die Elektronik ist sowohl dafür zuständig den Akku aufzuladen, als auch bei der stationären Verwendung ein angeschlossenes USB Netzteil als Stromquelle zu Nutzen. Da der Normalstrom, der aus dem Akku gezogen wird, sich um die 1A bewegt, kann es durchaus zu einer Unterversorgung kommen. Aufgrund dessen wird es nicht empfohlen bei höchster Displayhelligkeit den Global System for Mobile Communications (GSM) Suchlauf durchzuführen. Die Displaybeleuchtung dunkelt sich nach 10 Sekunden ab, um den Fall der möglichen Unterversorgung auszuschließen. Dies kann in den Einstellungen wie in Abbildung 4.2 geändert werden.

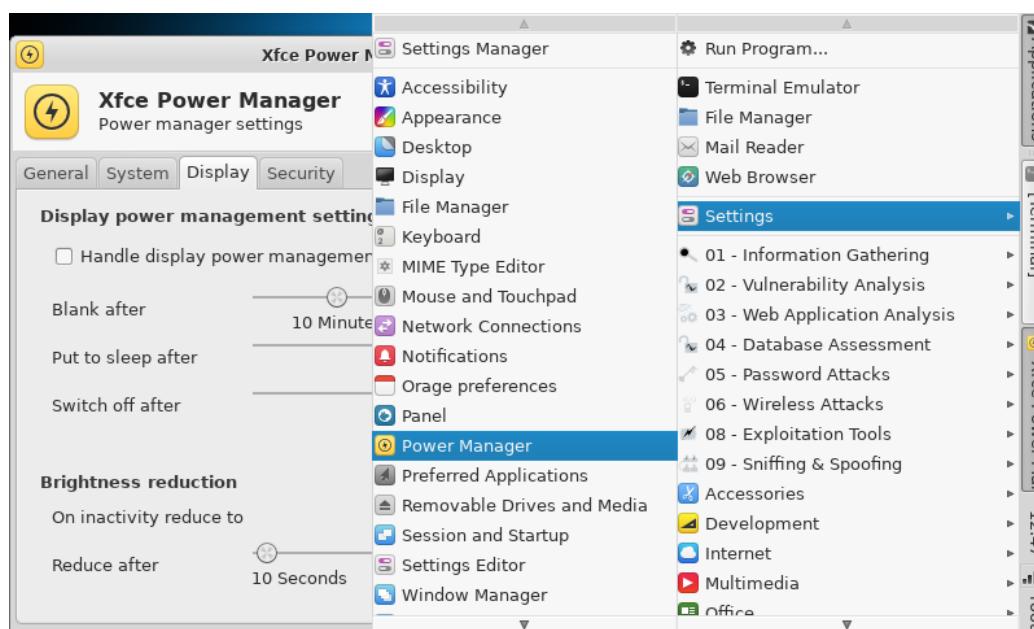


Abbildung 4.2: Einstellung der automatischen Helligkeitsregelung

Bedienung über die Desktopoberfläche

Auf dem Desktop befinden sich die wichtigsten Shortcuts für den Gebrauch des GSM Scanners.

Der Touchscreen wurde so eingestellt, dass man nur einmal klicken muss, um

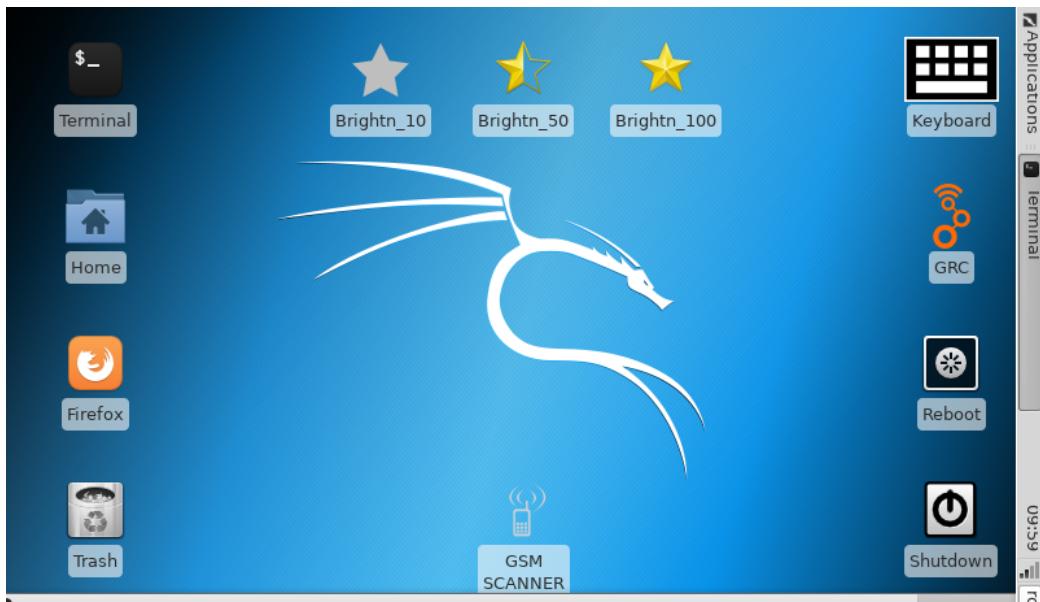


Abbildung 4.3: Ansicht des Dekstop

Programme auszuführen was eine Bedienung mit dem Finger erleichtert. Um eine einfache Einstellbarkeit der Displayhelligkeit zu realisieren haben wir auf dem Desktop Shortcuts hierfür implementiert. Die Stufen 10%, 50% und 100% können ausgewählt werden. Sind andere Stufen gewünscht, so kann man die Displayhelligkeit durch ausführen des Befehls

```
echo XXX > /sys/class/backlight/rpi_backlight/brightness
```

in einer Konsole ändern. XXX kann im Bereich von 0 (0%) bis 255 (100%) gewählt werden.

Ferner findet sich ein virtuelles Keyboard auf dem Desktop falls man mobil etwas schreiben möchte. Reboot und Shutdown Shortcuts sind ebenso zu finden. Bitte beachten Sie: Nach dem Shutdown muss die Stromversorgung zusätzlich am ON/OFF Schalter getrennt werden da weiterhin Spannung am Display anliegt.

Den Scanner starten

Der GSM Scanner hat ebenfalls ein Desktop Shortcut, welches mit einem Klick die Suche nach GSM Basisstationen ermöglicht. Um den Hintergrund zu

verstehen werden im folgenden Kapitel die Einstellmöglichkeiten, mit denen ein Scan gestartet werden kann, erläutert.

Erweitern und Verändern

Startup

```

1 Options:
2   -h, --help                  show this help message and exit
3   -b BAND, --band=BAND      Specify the GSM band for the
4                                frequency. Available
5                                bands are: GSM900, DCS1800, GSM850,
6                                PCS1900, GSM450,
7                                GSM480, GSM-R
8   -s SAMP_RATE, --samp-rate=SAMP_RATE
9                                Set sample rate [default=2000000.0] -
10                               allowed values
11                               even_number*0.2e6
12   -p PPM, --ppm=PPM          Set frequency correction in ppm [
13                               default=0]
14   -g GAIN, --gain=GAIN      Set gain [default=24.0]
15   --args=ARGS                Set device arguments [default=]
16   --speed=SPEED              Scan speed [default=4]. Value range
17                               0-5.
18   -v, --verbose              If set, verbose information output is
19                               printed: ccch
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
617
618
619
619
620
621
622
623
624
625
626
627
627
628
629
629
630
631
632
633
634
635
635
636
637
637
638
638
639
639
640
640
641
641
642
642
643
643
644
644
645
645
646
646
647
647
648
648
649
649
650
650
651
651
652
652
653
653
654
654
655
655
656
656
657
657
658
658
659
659
660
660
661
661
662
662
663
663
664
664
665
665
666
666
667
667
668
668
669
669
670
670
671
671
672
672
673
673
674
674
675
675
676
676
677
677
678
678
679
679
680
680
681
681
682
682
683
683
684
684
685
685
686
686
687
687
688
688
689
689
690
690
691
691
692
692
693
693
694
694
695
695
696
696
697
697
698
698
699
699
700
700
701
701
702
702
703
703
704
704
705
705
706
706
707
707
708
708
709
709
710
710
711
711
712
712
713
713
714
714
715
715
716
716
717
717
718
718
719
719
720
720
721
721
722
722
723
723
724
724
725
725
726
726
727
727
728
728
729
729
730
730
731
731
732
732
733
733
734
734
735
735
736
736
737
737
738
738
739
739
740
740
741
741
742
742
743
743
744
744
745
745
746
746
747
747
748
748
749
749
750
750
751
751
752
752
753
753
754
754
755
755
756
756
757
757
758
758
759
759
760
760
761
761
762
762
763
763
764
764
765
765
766
766
767
767
768
768
769
769
770
770
771
771
772
772
773
773
774
774
775
775
776
776
777
777
778
778
779
779
780
780
781
781
782
782
783
783
784
784
785
785
786
786
787
787
788
788
789
789
790
790
791
791
792
792
793
793
794
794
795
795
796
796
797
797
798
798
799
799
800
800
801
801
802
802
803
803
804
804
805
805
806
806
807
807
808
808
809
809
810
810
811
811
812
812
813
813
814
814
815
815
816
816
817
817
818
818
819
819
820
820
821
821
822
822
823
823
824
824
825
825
826
826
827
827
828
828
829
829
830
830
831
831
832
832
833
833
834
834
835
835
836
836
837
837
838
838
839
839
840
840
841
841
842
842
843
843
844
844
845
845
846
846
847
847
848
848
849
849
850
850
851
851
852
852
853
853
854
854
855
855
856
856
857
857
858
858
859
859
860
860
861
861
862
862
863
863
864
864
865
865
866
866
867
867
868
868
869
869
870
870
871
871
872
872
873
873
874
874
875
875
876
876
877
877
878
878
879
879
880
880
881
881
882
882
883
883
884
884
885
885
886
886
887
887
888
888
889
889
890
890
891
891
892
892
893
893
894
894
895
895
896
896
897
897
898
898
899
899
900
900
901
901
902
902
903
903
904
904
905
905
906
906
907
907
908
908
909
909
910
910
911
911
912
912
913
913
914
914
915
915
916
916
917
917
918
918
919
919
920
920
921
921
922
922
923
923
924
924
925
925
926
926
927
927
928
928
929
929
930
930
931
931
932
932
933
933
934
934
935
935
936
936
937
937
938
938
939
939
940
940
941
941
942
942
943
943
944
944
945
945
946
946
947
947
948
948
949
949
950
950
951
951
952
952
953
953
954
954
955
955
956
956
957
957
958
958
959
959
960
960
961
961
962
962
963
963
964
964
965
965
966
966
967
967
968
968
969
969
970
970
971
971
972
972
973
973
974
974
975
975
976
976
977
977
978
978
979
979
980
980
981
981
982
982
983
983
984
984
985
985
986
986
987
987
988
988
989
989
990
990
991
991
992
992
993
993
994
994
995
995
996
996
997
997
998
998
999
999
1000
1000
1001
1001
1002
1002
1003
1003
1004
1004
1005
1005
1006
1006
1007
1007
1008
1008
1009
1009
1010
1010
1011
1011
1012
1012
1013
1013
1014
1014
1015
1015
1016
1016
1017
1017
1018
1018
1019
1019
1020
1020
1021
1021
1022
1022
1023
1023
1024
1024
1025
1025
1026
1026
1027
1027
1028
1028
1029
1029
1030
1030
1031
1031
1032
1032
1033
1033
1034
1034
1035
1035
1036
1036
1037
1037
1038
1038
1039
1039
1040
1040
1041
1041
1042
1042
1043
1043
1044
1044
1045
1045
1046
1046
1047
1047
1048
1048
1049
1049
1050
1050
1051
1051
1052
1052
1053
1053
1054
1054
1055
1055
1056
1056
1057
1057
1058
1058
1059
1059
1060
1060
1061
1061
1062
1062
1063
1063
1064
1064
1065
1065
1066
1066
1067
1067
1068
1068
1069
1069
1070
1070
1071
1071
1072
1072
1073
1073
1074
1074
1075
1075
1076
1076
1077
1077
1078
1078
1079
1079
1080
1080
1081
1081
1082
1082
1083
1083
1084
1084
1085
1085
1086
1086
1087
1087
1088
1088
1089
1089
1090
1090
1091
1091
1092
1092
1093
1093
1094
1094
1095
1095
1096
1096
1097
1097
1098
1098
1099
1099
1100
1100
1101
1101
1102
1102
1103
1103
1104
1104
1105
1105
1106
1106
1107
1107
1108
1108
1109
1109
1110
1110
1111
1111
1112
1112
1113
1113
1114
1114
1115
1115
1116
1116
1117
1117
1118
1118
1119
1119
1120
1120
1121
1121
1122
1122
1123
1123
1124
1124
1125
1125
1126
1126
1127
1127
1128
1128
1129
1129
1130
1130
1131
1131
1132
1132
1133
1133
1134
1134
1135
1135
1136
1136
1137
1137
1138
1138
1139
1139
1140
1140
1141
1141
1142
1142
1143
1143
1144
1144
1145
1145
1146
1146
1147
1147
1148
1148
1149
1149
1150
1150
1151
1151
1152
1152
1153
1153
1154
1154
1155
1155
1156
1156
1157
1157
1158
1158
1159
1159
1160
1160
1161
1161
1162
1162
1163
1163
1164
1164
1165
1165
1166
1166
1167
1167
1168
1168
1169
1169
1170
1170
1171
1171
1172
1172
1173
1173
1174
1174
1175
1175
1176
1176
1177
1177
1178
1178
1179
1179
1180
1180
1181
1181
1182
1182
1183
1183
1184
1184
1185
1185
1186
1186
1187
1187
1188
1188
1189
1189
1190
1190
1191
1191
1192
1192
1193
1193
1194
1194
1195
1195
1196
1196
1197
1197
1198
1198
1199
1199
1200
1200
1201
1201
1202
1202
1203
1203
1204
1204
1205
1205
1206
1206
1207
1207
1208
1208
1209
1209
1210
1210
1211
1211
1212
1212
1213
1213
1214
1214
1215
1215
1216
1216
1217
1217
1218
1218
1219
1219
1220
1220
1221
1221
1222
1222
1223
1223
1224
1224
1225
1225
1226
1226
1227
1227
1228
1228
1229
1229
1230
1230
1231
1231
1232
1232
1233
1233
1234
1234
1235
1235
1236
1236
1237
1237
1238
1238
1239
1239
1240
1240
1241
1241
1242
1242
1243
1243
1244
1244
1245
1245
1246
1246
1247
1247
1248
1248
1249
1249
1250
1250
1251
1251
1252
1252
1253
1253
1254
1254
1255
1255
1256
1256
1257
1257
1258
1258
1259
1259
1260
1260
1261
1261
1262
1262
1263
1263
1264
1264
1265
1265
1266
1266
1267
1267
1268
1268
1269
1269
1270
1270
1271
1271
1272
1272
1273
1273
1274
1274
1275
1275
1276
1276
1277
1277
1278
1278
1279
1279
1280
1280
1281
1281
1282
1282
1283
1283
1284
1284
1285
1285
1286
1286
1287
1287
1288
1288
1289
1289
1290
1290
1291
1291
1292
1292
1293
1293
1294
1294
1295
1295
1296
1296
1297
1297
1298
1298
1299
1299
1300
1300
1301
1301
1302
1302
1303
1303
1304
1304
1305
1305
1306
1306
1307
1307
1308
1308
1309
1309
1310
1310
1311
1311
1312
1312
1313
1313
1314
1314
1315
1315
1316
1316
1317
1317
1318
1318
1319
1319
1320
1320
1321
1321
1322
1322
1323
1323
1324
1324
1325
1325
1326
1326
1327
1327
1328
1328
1329
1329
1330
1330
1331
1331
1332
1332
1333
1333
1334
1334
1335
1335
1336
1336
1337
1337
1338
1338
1339
1339
1340
1340
1341
1341
1342
1342
1343
1343
1344
1344
1345
1345
1346
1346
1347
1347
1348
1348
1349
1349
1350
1350
1351
1351
1352
1352
1353
1353
1354
1354
1355
1355
1356
1356
1357
1357
1358
1358
1359
1359
1360
1360
1361
1361
1362
1362
1363
1363
1364
1364
1365
1365
1366
1366
1367
1367
1368
1368
1369
1369
1370
1370
1371
1371
1372
1372
1373
1373
1374
1374
1375
1375
1376
1376
1377
1377
1378
1378
1379
1379
1380
1380
1381
1381
1382
1382
1383
1383
1384
1384
1385
1385
1386
1386
1387
1387
1388
1388
1389
1389
1390
1390
1391
1391
1392
1392
1393
1393
1394
1394
1395
1395
1396
1396
1397
1397
1398
1398
1399
1399
1400
1400
1401
1401
1402
1402
1403
1403
1404
1404
1405
1405
1406
1406
1407
1407
1408
1408
1409
1409
1410
1410
1411
1411
1412
1412
1413
1413
1414
1414
1415
1415
1416
1416
1417
1417
1418
1418
1419
1419
1420
1420
1421
1421
1422
1422
1423
1423
1424
1424
1425
1425
1426
1426
1427
1427
1428
1428
1429
1429
1430
1430
1431
1431
1432
1432
1433
1433
1434
1434
1435
1435
1436
1436
1437
1437
1438
1438
1439
1439
1440
1440
1441
1441
1442
1442
1443
1443
1444
1444
1445
1445
1446
1446
1447
1447
1448
1448
1449
1449
1450
1450
1451
1451
1452
1452
1453
1453
1454
1454
1455
1455
1456
1456
1457
1457
1458
1458
1459
1459
1460
1460
1461
1461
1462
1462
1463
1463
1464
1464
1465
1465
1466
1466
1467
1467
1468
1468
1469
1469
1470
1470
1471
1471
1472
1472
1473
1473
1474
1474
1475
1475
1476
1476
1477
1477
1478
1478
1479
1479
1480
1480
1481
1481
1482
1482
1483
1483
1484
1484
1485
1485
1486
1486
1487
1487
1488
1488
1489
1489
1490
1490
1491
1491
1492
1492
1493
1493
1494
1494
1495
1495
1496
1496
1497
1497
1498
1498
1499
1499
1500
1500
1501
1501
1502
1502
1503
1503
1504
1504
1505
1505
1506
1506
1507
1507
1508
1508
1509
1509
1510
1510
1511
1511
1512
1512
1513
1513
1514
1514
1515
1515
1516
1516
1517
1517
1518
1518
1519
1519
1520
1520
1521
1521
1522
1522
1523
1523
1524
1524
1525
1525
1526
1526
1527
1527
1528
1528
1529
1529
1530
1530
1531
1531
1532
1532
1533
1533
1534
```

ändern, zum Beispiel wenn ein neuer Stick mit einem anderen Quarz Offset verwendet werden soll. Am besten öffnet man die Skripte über das Terminal mit "nano" da sonst kein Textverarbeitungsprogramm installiert ist.

Alle weiteren von uns geschriebenen Komponenten sind ebenfalls im Ordner

```
1 /root/GrGsm-Gui
zu finden. Da es sich hierbei um ein Git
Repository handelt kann dieses auch über
1 cd GrGsm-Gui/
2 git pull
```

auf den neusten Stand gebracht werden, sollten Veränderungen vorgenommen werden.

Autostartup

Nach dem Anschalten am ON/OFF Schalter auf der Unterseite des Handhelds fährt dieses hoch. Eine Anmeldung ist nicht erforderlich. Soll dies geändert werden, so müssen zwei Befehle in der Datei lightdm.conf auskommentiert werden.

```
1 cd /etc/lightdm
2 nano lightdm.conf
3
4 ****
5 autologin-user=root
6 autologin-user-timeout=0
7 ****
8
9 ^ muessen durch voransetzen eines "#" auskommentiert werden
```

Anleitung zur GUI unter PyQt4

Im folgenden Kapitel soll die GUI und deren Inhalt anhand einiger Bildbeispiele verdeutlicht werden. Nachfolgend wird erläutert wie und wo im Code es möglich ist, diese Inhalte anzupassen bzw. zu verändern.

Zuerst jedoch noch ein paar Erklärungen zu dem Aufbau unseres modifizierten grgsm-scanners.

Zu Beginn des Programms wird in der Main-Funktion unsere GUI aufgerufen und aufgebaut. Während diese nun im Hintergrund auf einem Thread läuft, wird auf einem anderen Thread das Scanning fortgeführt. In den folgenden Abschnitten wird nun näher erläutert wie genau die GUI diese Informationen darstellt und den Scan-Vorgang kommuniziert.

Allgemeiner Aufbau der GUI

Starten des grgsm-scanner initiiert die GUI wie in Abbildung:5.1 zu sehen ist. Das GUI-Fenster ist in zwei Felder aufgeteilt, ein kleineres Feld auf der linken Seite und ein größeres auf der Rechten. Im linken Feld werden die Kanäle dargestellt, welche nach und nach gescannt und hinzugefügt werden. Im rechten Feld werden zu Beginn Informationen zur Projektarbeit ausgegeben. Diese wird durch die Informationen von ausgewählten Kanälen überschrieben, dazu jedoch später mehr.

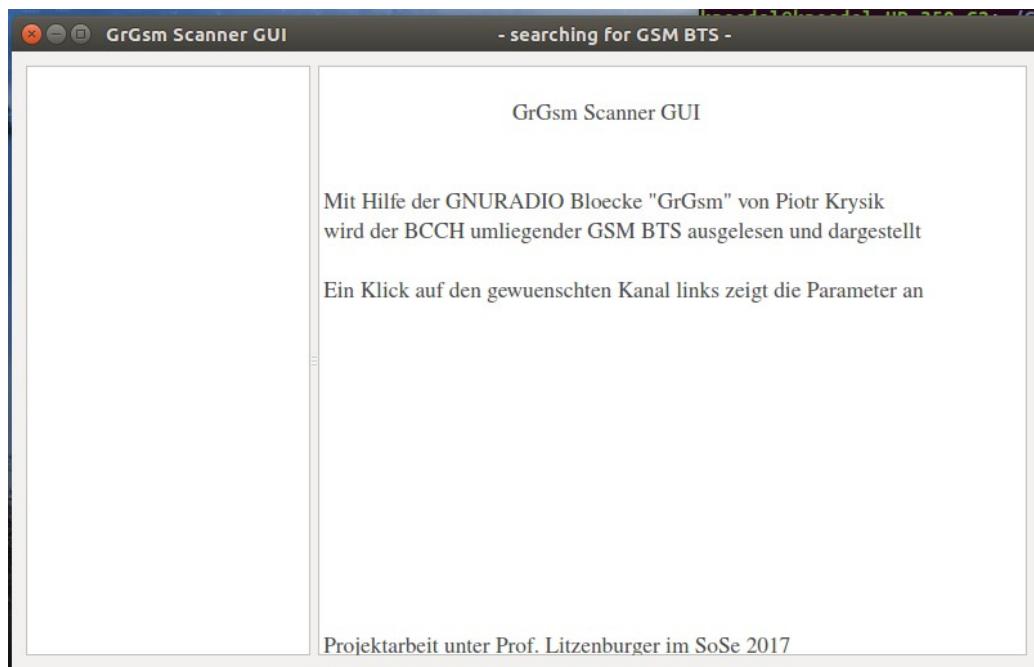


Abbildung 5.1: Standard Fenster GUI

Solange die Suche nach Kanälen noch nicht abgeschlossen wurde, wird oben im Fensterrahmen **-searching for GSM BTS-** dargestellt (siehe Abbildung: 5.1). Falls der Scan abgeschlossen ist, wird dies durch ein **-DONE!**– angezeigt, ersichtlich aus Bild 5.2. Außerdem sollten nun alle gefundenen Kanäle im linken Feld zu sehen sein.

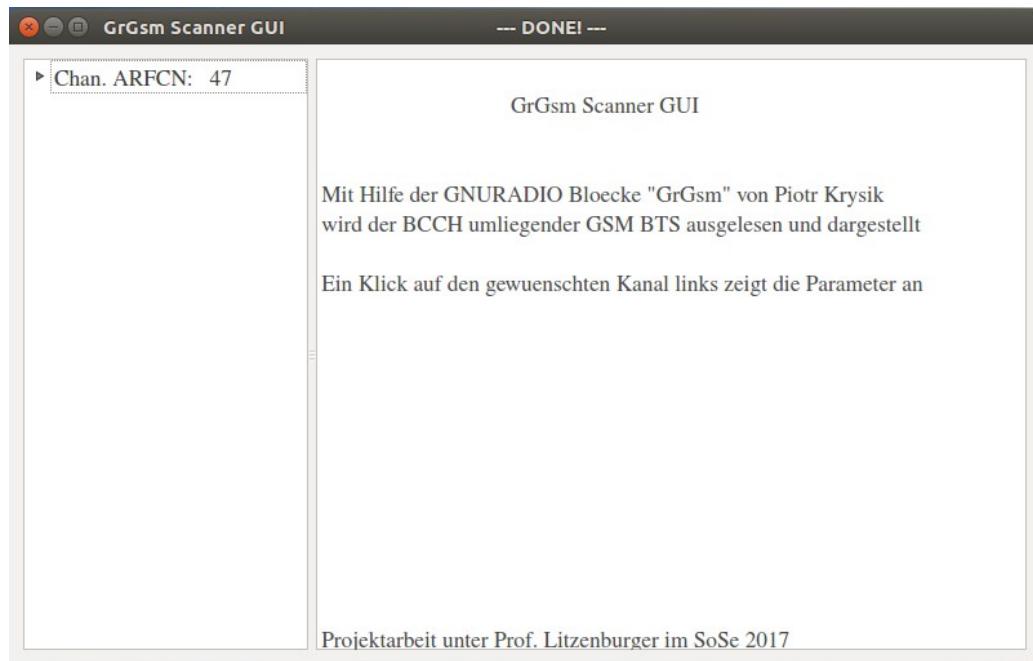


Abbildung 5.2: Abgeschlossener Scan

Falls Kanäle schon gescannt wurden und somit links auftauchen, können diese ausgewählt werden um die Informationen der einzelnen Parameter einzusehen. Unter den Parametern befinden sich der Absolute Radio Frequency Cell Number (ARFCN), die Frequenz, der Location Area Code (LAC), der Mobile Country Code (MCC), der Mobile Network Code (MNC), die Cell Identification (CID) und die relative Empfangsleistung. Zusätzlich werden ein paar weitere Informationen ausgegeben (siehe Abbildung:5.3). Sollte eine Maus angeschlossen sein können die Informationen auch durch eine Art Tooltip über mouse-hovering auf dem jeweiligen Kanal ausgegeben werden (siehe Abbildung:5.4).

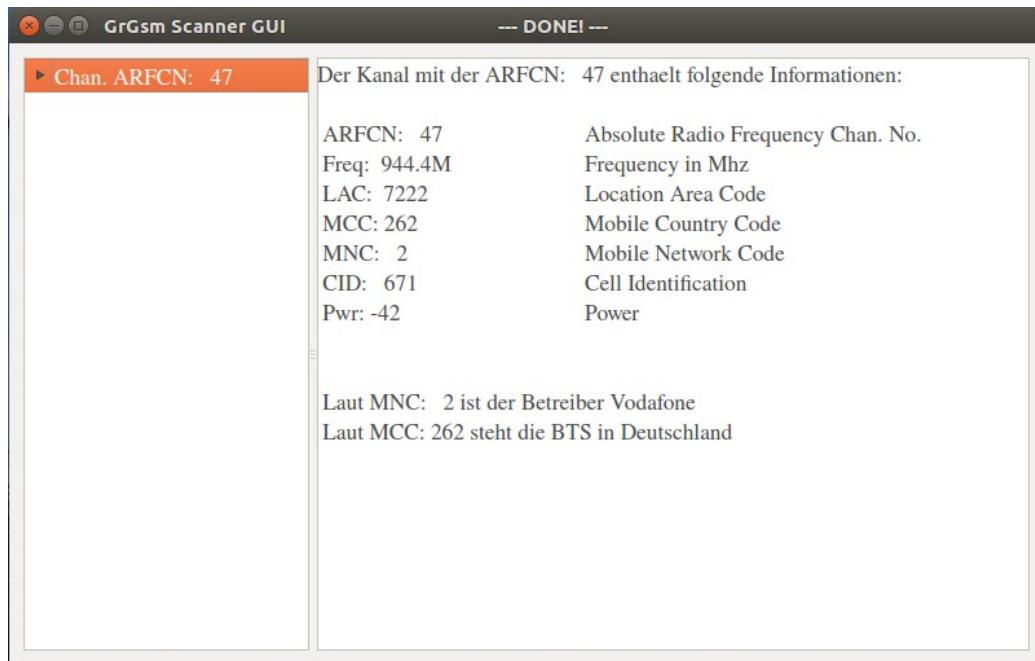


Abbildung 5.3: Info des BCCH

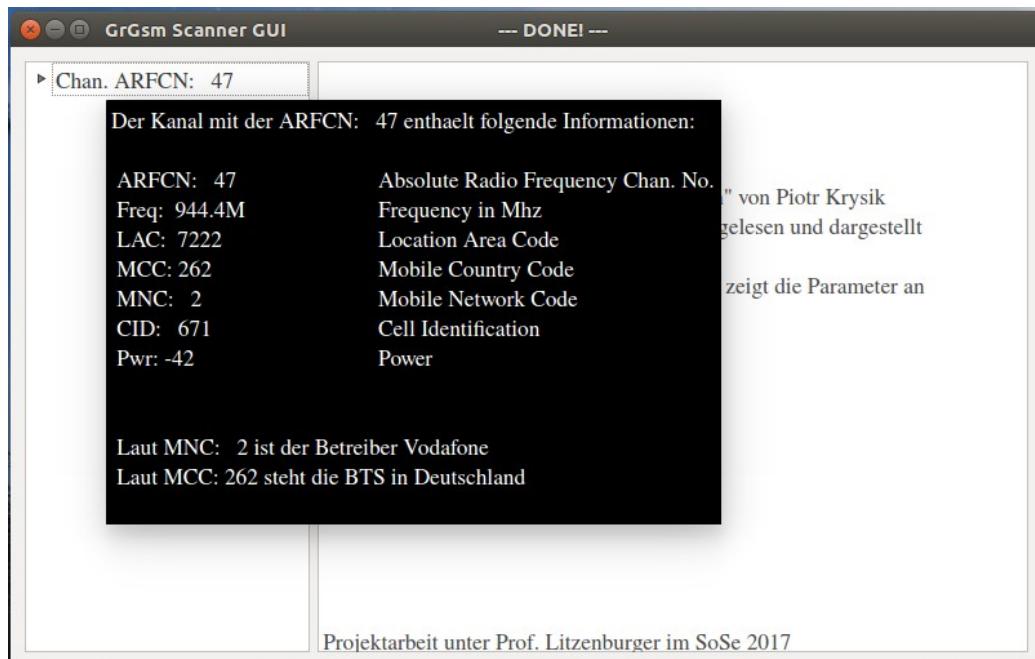


Abbildung 5.4: Mouseover Tooltip

Bei jedem Kanal ist es möglich durch einen kleinen Pfeil links daneben, diesen aufzurollen um die Parameter einzeln zu betrachten (siehe Abbildung:5.5). Durch das Anklicken der einzelnen Parameter wird die jeweilige Information dargestellt (siehe Abbildung:5.6).

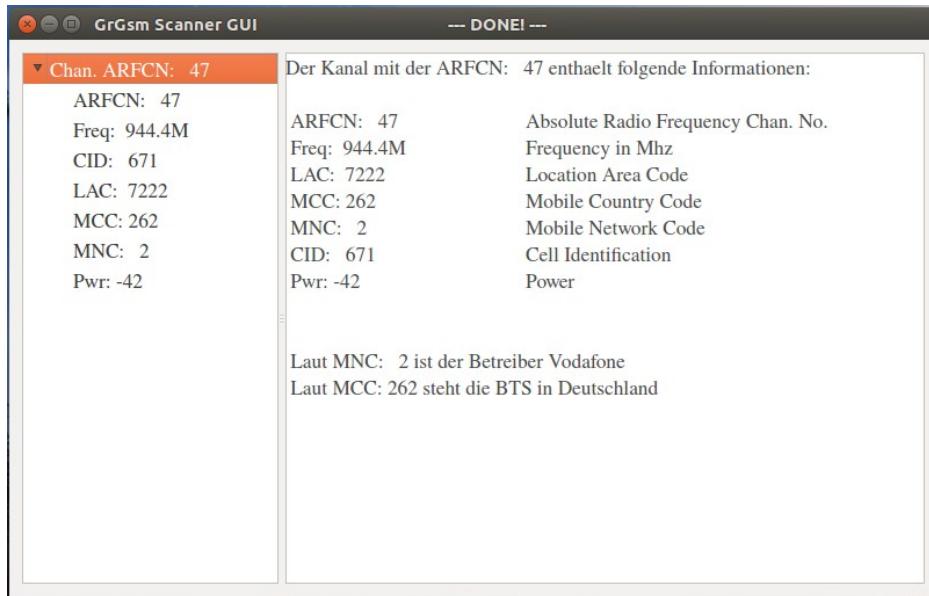


Abbildung 5.5: GUI Ansicht angeklickt

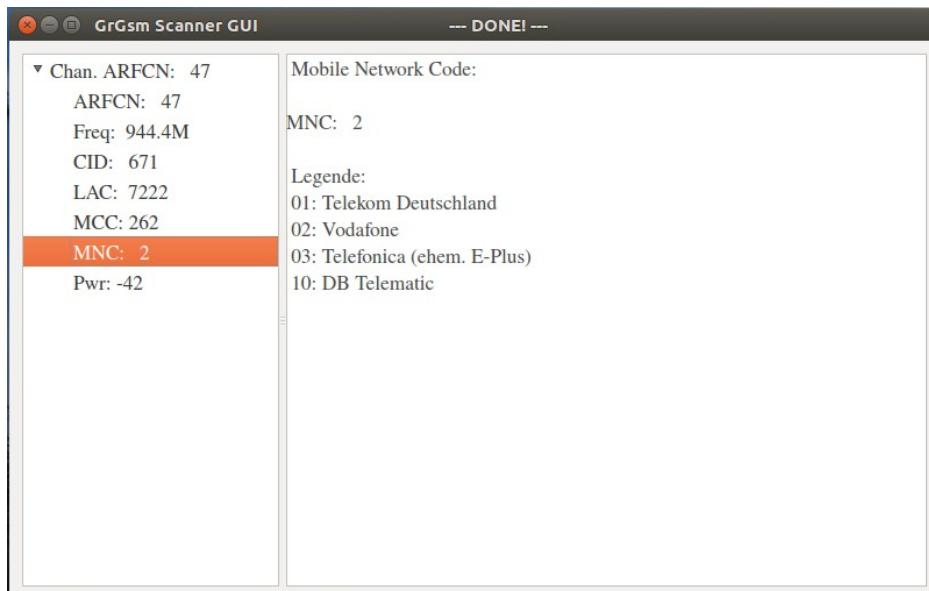


Abbildung 5.6: Infos der Childnodes

Anleitung zum Anpassen des textuellen Inhalts

Anpassung der Titelseite

Die Titelseite, wie im vorherigen Kapitel bereits erwähnt, welche am Programmstart zu sehen ist, kann durch Änderungen im folgenden Programmcode (Listing: 5.1) angepasst werden. Die Zeilenangaben links verdeutlichen zusätzlich, wo man dies im Programmcode finden kann.

```

100 self.text = QtGui.QLabel("\n"
101                 " \t\t GrGsm Scanner GUI\n\n"
102                 " Mit Hilfe der GNURADIO Blocke \""
103                 " GrGsm\" von Piotr Krysik\n"
104                 " wird der BCCH umliegender GSM BTS
105                 " ausgelesen und dargestellt\n\n"
106                 " Ein Klick auf den gewuenschten
107                 " Kanal links zeigt die Parameter
108                 " an\n\n\n\n\n\n\n\n\n\n\n\n\n\n"
109
110                 " Projektarbeit unter Prof.
111                 " Litzenburger im SoSe 2017\n"
112                 " von Dennis Dette und Christian
113                 " Kobiela\n\n"
114                 , self.right)

```

Listing 5.1: Titelseite

Anpassung der Parentnode

Die Informationen, welche angezeigt werden wenn man einen gefundenen Kanal anklickt, können in den folgenden Codezeilen geändert werden (Listing: 5.2). Bisher werden, wie zu sehen ist, die einzelnen Parameter mit Werten dargestellt und Angaben über Land und Betreiber der BTS.

```

187 parent_item.setToolTip(column,"Der Kanal mit der " +
188     Buffer_Channel.ARFCN +
189         " enthaelt folgende Informationen: \n\n"
190         + " " +Buffer_Channel.ARFCN + " \t\tAbsolute
191             Radio Frequency Chan. No.\n"
192         + " " +Buffer_Channel.FREQ + " \t\tFrequency
193             in Mhz\n"
194         + " " +Buffer_Channel.LAC + " \t\tLocation
195             Area Code\n"
196         + " " +Buffer_Channel.MCC + " \t\tMobile
197             Country Code\n"
198         + " " +Buffer_Channel.MNC + " \t\tMobile
             Network Code\n"
         + " " +Buffer_Channel.CID + " \t\tCell
             Identification\n"
         + " " +Buffer_Channel.PWR+ " \t\tPower\n\n\n"
         + " Laut " + Buffer_Channel.MNC + " ist der
             Betreiber " + Betreiber
         + "\n Laut " + Buffer_Channel.MCC + " steht
             die BTS in " + str(Land)
    )

```

Listing 5.2: Kanalinformation

Anpassung der Childnodes

Nun zum letzten Teil, dessen Text angepasst werden kann, den Parameterinformationen. Diese sind einzusehen, wenn ein Kanal aufgeklappt ist. Hier werden durch das Auswählen der einzelnen Parameter die Informationen dargestellt, welche im Code 5.3 zu sehen sind. Die sieben Parameterinformationen werden in den verschiedenen If-Fällen definiert.

```

204 if k==0:
205     item.setToolTip(column, " Absolute Radio Frequency
206         Channel Number:\n\n " + Buffer_Channel.ARFCN
207         + "\n\n In GSM cellular networks, an absolute radio-
208             frequency channel number\n ""(ARFCN) is a code
209                 that specifies a pair of physical radio carriers
210                     used for\n ""transmission and reception in a land
211                         mobile radio system, one for the uplink\n ""signal
212                             and one for the downlink signal.\n\n "
213 "ARFCN for GSM 900 \n "
214 "ARFCN = (Chan. Freq - 45 Mhz- 890 Mhz)/200\n\n "
215 "ARFCN for E GSM 900\n "
216 "ARFCN = 1024 + (Chan. Freq - 45 Mhz - 890 Mhz)/200\n
217         ")
218 elif k==1:
219     item.setToolTip(column, " Frequency:\n\n " +
220         Buffer_Channel.FREQ + "\n\n GSM Downlink Frequency
221         ")
222 elif k==2:
223     item.setToolTip(column, " Cell Identification:\n\n "
224         + Buffer_Channel.CID +
225         "\n\n A GSM Cell ID (CID) is a generally unique
226             number used\n "
227             "to identify each base transceiver station (BTS) or\n
228                 "
229             "sector of a BTS within a location area code (LAC) \n
230                 "
231             "if not within a GSM network.")
232 elif k==3:
233     item.setToolTip(column, " Location Area Code:\n\n " +
234         Buffer_Channel.LAC+
235         "\n\n A location area is a set of base stations that
236             are\n "
237             "grouped together to optimise signalling.\n "
238             "To each location area, a unique number called a
239                 location area code is assigned.\n ")
240 elif k==4:
241     item.setToolTip(column, " Mobile Country Code:\n\n "
242         + Buffer_Channel.MCC +
243         "\n\n The mobile country code consists of 3 decimal
244             digits and the mobile\n "
245             "network code consists of 2 or 3 decimal digits. The
246                 first \"2\" in 262\n "
247             "stands for Europe, 62 for Germany")
248 elif k==5:
249     item.setToolTip(column, " Mobile Network Code:\n\n " +
250         Buffer_Channel.MNC +
251         "\n\n Legende:\n 01: Telekom Deutschland\n 02:
252             Vodafone\n 03: Telefonica (ehem. E-Plus)\n 10: DB
253                 Telematic")
254 elif k==6:
255     item.setToolTip(column, " Power:\n\n " +
256         Buffer_Channel.PWR +
257         "\n\n GSM needs at least a Power of -102dBm " )

```

Listing 5.3: Parameterinformationen

Setup des Raspberry PI

Im Folgenden wird beschrieben wie wir den Raspberry aufgesetzt haben und welche Probleme uns dabei begegnet sind.

Das How To und interdependencies

gr-gsm wird hauptsächlich von Piotr Krysik entwickelt und wird von diesem auch gepflegt. Es gibt auch einen vorgeschlagenen Weg wie man gr-gsm auf einem Raspberry Pi 3 zu installieren hat. Dieser Weg hat sich allerdings als Sackgasse erwiesen. Grund dafür war, dass in der Zwischenzeit GNU Radio weiterentwickelt wurde und gr-gsm sich dieser Weiterentwicklung angepasst hatte. Die Weiterentwicklung betraf leider nicht Raspbian Jessie, was zu folgenden Problemen führte.

gr-gsm benötigte damals eine Version von GNU Radio > 3.7.9, für Raspbian stand allerdings nur die Version 3.7.6 zur Verfügung. Der Versuch auf instabile Testversionen 3.7.10+ auszuweichen erwies sich ebenso als aussichtslos. Das Installieren von diesen Versionen führte nur dazu, dass wiederum Bibliotheken von denen GNU Radio abhängig war inkompatibel wurden.

Nach einiger Recherche wie man ein funktionierendes Gesamtpaket erhalten könnte sind wir auf das Programm PyBombs gestoßen. Dieses macht genau das, was wir gesucht haben, es installiert ein Programm und alle Abhängigkeiten die dieses zur Nutzung benötigt. Im Gegensatz zu apt-get, wie man es von Ubuntu und sonstigen Linux Distributionen kennt, bezieht sich PyBOMBS nicht nur auf die Standard Repositorys und die dort hinterlegte Softwareversionen sondern installiert genau die Versionen die benötigt werden. Hierbei kann sich PyBOMBS auf eigens hinterlegte Repositorys, sogenannte Recipes, beziehen von wo es die Software aus den Quelldateien kompiliert. So schön es klingt führte es zu den selben Problemen wie im ersten Versuch, nur dass

dieses mal andere Programme inkompatibel wurden.

An diesem Punkt haben wir beschlossen, dass eine zeitnahe Umsetzung mit gr-gsm wohl aussichtslos erscheint. Gleichzeitig standen wir mit Piotr Krysik in Kontakt um einen Weg zu finden wie es doch zu lösen sein könnte. Seither ist Herr Krysik dabei seine Anpassungen in einem Raspberry Emulator zu überprüfen. Wir entschieden uns dennoch Airprobe zu versuchen, da es nicht absehbar war wann wir mit einer erfolgversprechenden Antwort hätten rechnen können. Dafür haben wir uns an einer jahrealten Anleitung orientiert und sind dabei auf Kali Linux gestoßen, dieses war glücklicherweise auch für Raspberries verfügbar. Nachdem wir das installiert hatten, war GNU Radio mittlerweile zu Neu um mit Airprobe arbeiten zu können. Allerdings war die stabile Version des Standard Repository glücklicherweise 3.7.10. Somit war das installierte GNU Radio mit dem neusten gr-gsm kompatibel und so konnten wir alle Abhängigkeiten installieren, die Kalibrierung durchführen und gr-gsm installieren. Zu der Zeit haben wir schon einen Monat Arbeit in das Projekt stecken müssen.

Im Endeffekt ist die Anleitung wie sie in Kapitel 2 dokumentiert wird, unter Kali Linux voll durchführbar. Es wäre allerdings wünschenswert den GSM Scanner unter Raspbian zum laufen zu bringen, da es sich hierbei um ein besser auf den Raspberry zugeschnittenes Betriebssystem handelt. Damit diese Portierung auf Raspbian möglich ist, müssen die vorher beschriebenen Probleme mit den Abhängigkeiten gelöst werden.

Zusammenfassung

In dieser Projektarbeit ist es uns gelungen ein Handheld zum Auslesen des BCCH zu konzipieren, diesen aufzubauen und in Betrieb zu nehmen. Als Herzstück dient uns ein von Kali Linux betriebener Raspberry Pi 3, das da-zugehörige Display mit Toucheingabe und ein DVB-T-Stick. Letzterer wurde nach dem Prinzip des Software Defined Radio verwendet, welches besagt, dass möglichst viel der Signalverarbeitung in der Software durchgeführt wird. So können die analogen Komponenten der Kommunikationssysteme einfach gehalten werden.

Mit den GNU Radio Blöcken "gr-gsm" von Piotr Krysik ist es uns gelungen den Informationsstring des BCCH auszulesen und mit einer eigens geschriebenen Graphischen User Interface (GUI) darzustellen. Die Darstellung der GUI und der Suchvorgang der GSM Basisstationen laufen parallel auf zwei Threads um eine laufende Aktualisierung zu ermöglichen.

Mit dem fertigen Handheld ist eine mobile Nutzung von bis zu 5 Stunden möglich. So kann auch die Netzabdeckung der entferntesten Orte analysiert werden.