

Software Defined Radio (SDR)

Uwe Berger
bergeruw@gmx.net



Uwe Berger



- Beruf: Softwareentwickler
- Freizeit: u.a. mit Hard- und Software rumspielen
- Linux seit ca. 1995
- BraLUG e.V.
- bergeruw@gmx.net



Disclaimer & Motivation

- ...ich bin kein Funkamateuer!
- ...ich wollte eigentlich mal Bilder von Wettersatelliten empfangen



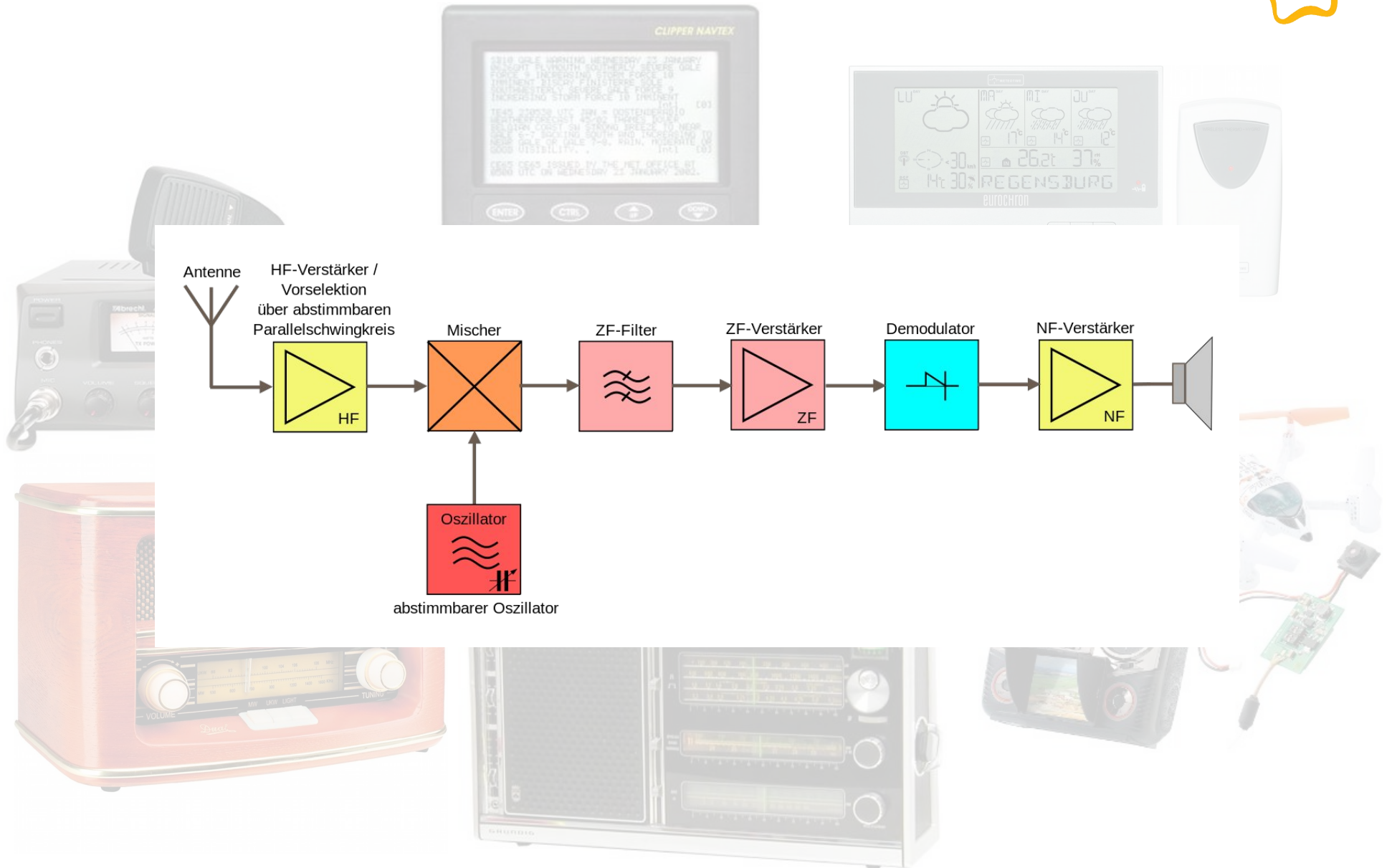
Inhalt

- Was ist SDR?
- RTL-SDR
- Was kann man damit anfangen?

Software Defined Radio (SDR)



Software Defined Radio (SDR)



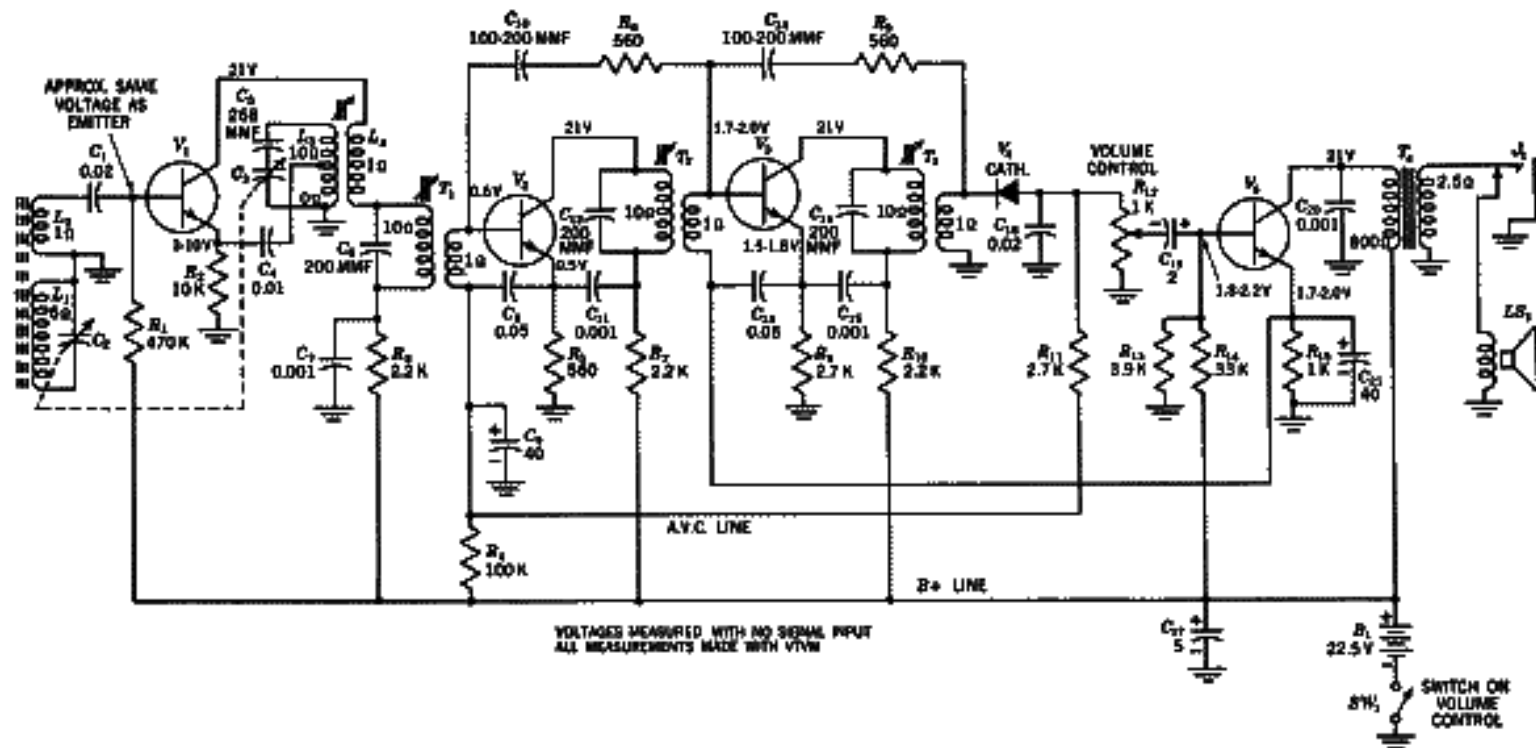


FIG. 3. The schematic diagram of the Regency model TR-1 receiver (Courtesy Howard W. Sams & Co., Inc.)





Was ist SDR?

- Software Defined Radio (SDR)
- (entscheidende) Anteile der Signalverarbeitung, wie z.B.:
 - Mixer,
 - Filter,
 - Verstärker,
 - Modulation/Demodulation,erfolgen mittels Software auf ausreichend schnellen Rechnern
- Vorteil: hohe Flexibilität bei Änderungen an den Übertragungsstandards oder -protokollen



Was ist SDR?

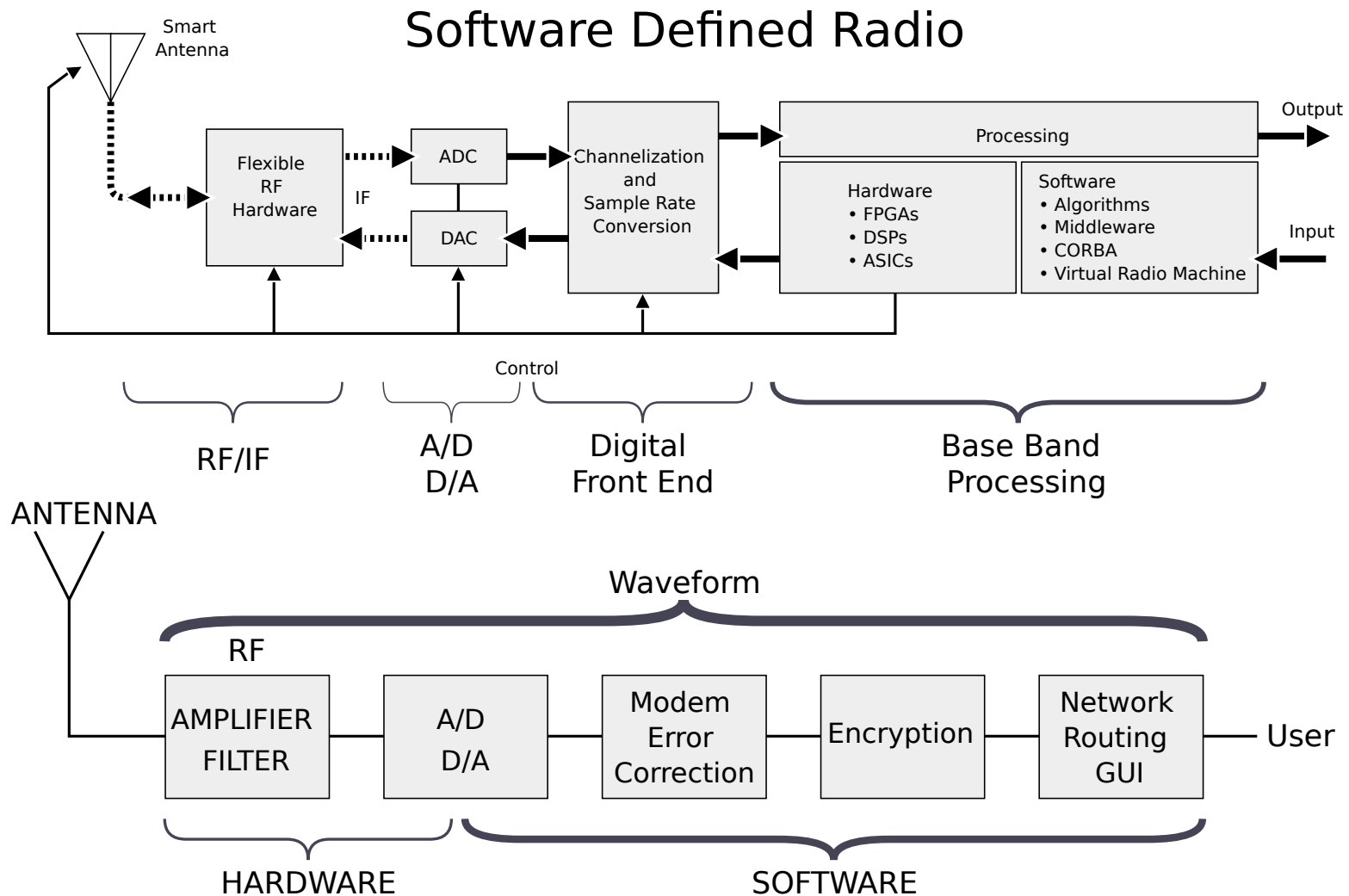


Bild: <http://de.wikipedia.org>



Was ist SDR?

Für Hobbyisten verfügbare SDR-Varianten sind z.B.:

- PC-Soundkarte
- WebSDR und andere im Internet verfügbare SDR-Empfänger
→ <http://websdr.org/>
- HPSSDR (High Performance Software Defined Radio)
→ <http://openhpsdr.org/>
- RTL-SDR
→ <http://rtl-sdr.org/>



RTL-SDR

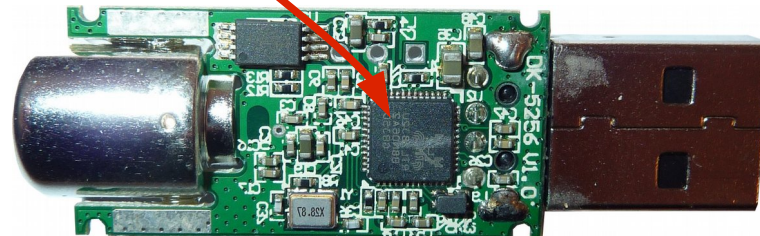
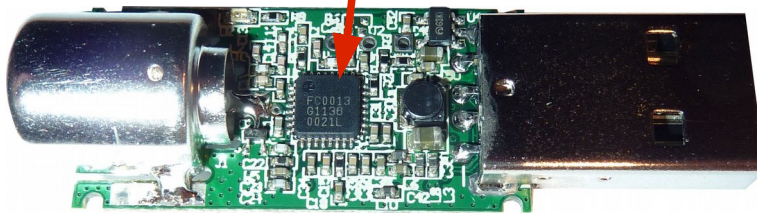
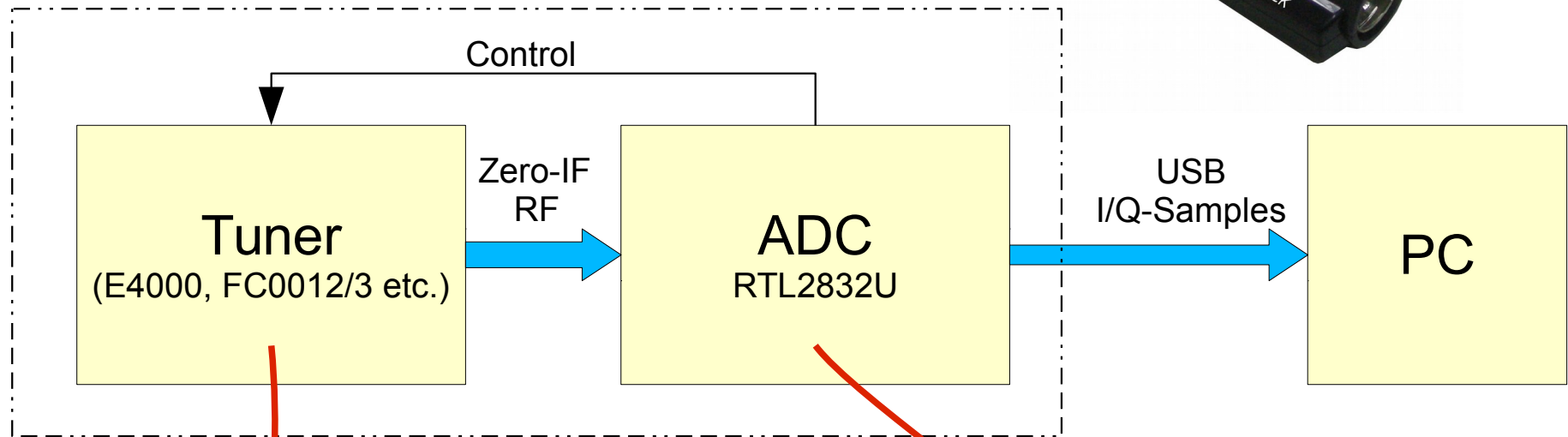
- Realtek Software Defined Radio
- RTL2835U-Chipsatz, wie er z.B. in DAB- und DBV-T-USB-Sticks verwendet wird (wurde)
- März 2010:
 - Entdeckung, dass „raw I/Q-Samples“ an Host gesendet werden
 - Rekonstruktion des Protokolls
- Febr. 2012: rtl-sdr
- Kompatibilitätsliste, z.B.:
 - <http://sdr.osmocom.org/trac/wiki/rtl-sdr#SupportedHardware>



Was sind „I/Q-Samples“

- Einige Modulationsverfahren (z.B. FM, PM) basieren auf der Phasenverschiebung des Trägersignals
- I&Q-Verfahren: Möglichkeit, bei einer Demodulation eines HF-Signals, die Phaseninformation zu erhalten
- I $\rightarrow$ In-Phase $\rightarrow$ Demodulation mit originaler Phasenlage
- Q $\rightarrow$ Quadrature $\rightarrow$ Demodulation mit um 90° phasenverschobener Referenzfrequenz
- Für Interessierte....:
 - <http://whiteboard.ping.se/SDR/IQ>
 - <https://de.wikipedia.org/wiki/I%26Q-Verfahren>

RTL-SDR (Hardware)





RTL-SDR (Hardware)

- Tuner, u.a.:
 - E4000: 52 – 2200 MHz
 - R820T/D: 24 – 1766 MHz
 - FC0012: 22 – 948.6 MHz
 - FC0013: 22 – 1100 MHz
 - FC2580: 146 – 924 MHz
- ADC (RTL2832U):
 - Auflösung: 8 Bit
 - theoretische Samplerate: 3.2 MS/s
 - realistische Samplerate: 2.56 MS/s



RTL-SDR (Software)

- Installation: Softwarepaket der Distribution oder manuell kompilieren/installieren:

```
> apt-get update
> apt-get install cmake libusb-1.0-0-dev git
...
> git clone git://git.osmocom.org/rtl-sdr.git
...

> cd rtl-sdr
> mkdir build
> cd build
> cmake ../ -DINSTALL_UDEV_RULES=ON
...
> make
> sudo make install
...

> sudo ldconfig
```



RTL-SDR (Software)

- Datei */etc/modprobe.d/rtlsdr.conf* mit folgenden Inhalt anlegen:

```
blacklist dvb_usb_rtl28xxu
```



RTL-SDR (Software)

- Erster Test mit Kommando *rtl_test*.

```
> rtl_test
```

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

```
0: NOXON, DAB Stick, SN: 0
```

```
Using device 0: Terratec NOXON DAB/DAB+ USB dongle (rev 1)
```

```
Found Fitipower FC0013 tuner
```

```
Supported gain values (23): -9.9 -7.3 -6.5 -6.3 -6.0 -5.8 -5.4 5.8
```

```
6.1 6.3 6.5 6.7 6.8 7.0 7.1 17.9 18.1 18.2 18.4 18.6 18.8 19.1 19.7
```

```
Sampling at 2048000 S/s.
```

```
Info: This tool will continuously read from the device, and report  
if samples get lost. If you observe no further output, everything is  
fine.
```

```
Reading samples in async mode...
```



Bevor man mit SDR experimentiert...!

Telekommunikationsgesetz (TKG)

§ 89 Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen

Mit einer Funkanlage dürfen nur Nachrichten, die für den Betreiber der Funkanlage, Funkamateure im Sinne des Gesetzes über den Amateurfunk vom 23. Juni 1997 (BGBl. I S. 1494), die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind, abgehört werden. Der Inhalt anderer als in Satz 1 genannter Nachrichten sowie die Tatsache ihres Empfangs dürfen, auch wenn der Empfang unbeabsichtigt geschieht, auch von Personen, für die eine Pflicht zur Geheimhaltung nicht schon nach § 88 besteht, anderen nicht mitgeteilt werden. § 88 Abs. 4 gilt entsprechend. Das Abhören und die Weitergabe von Nachrichten auf Grund besonderer gesetzlicher Ermächtigung bleiben unberührt.

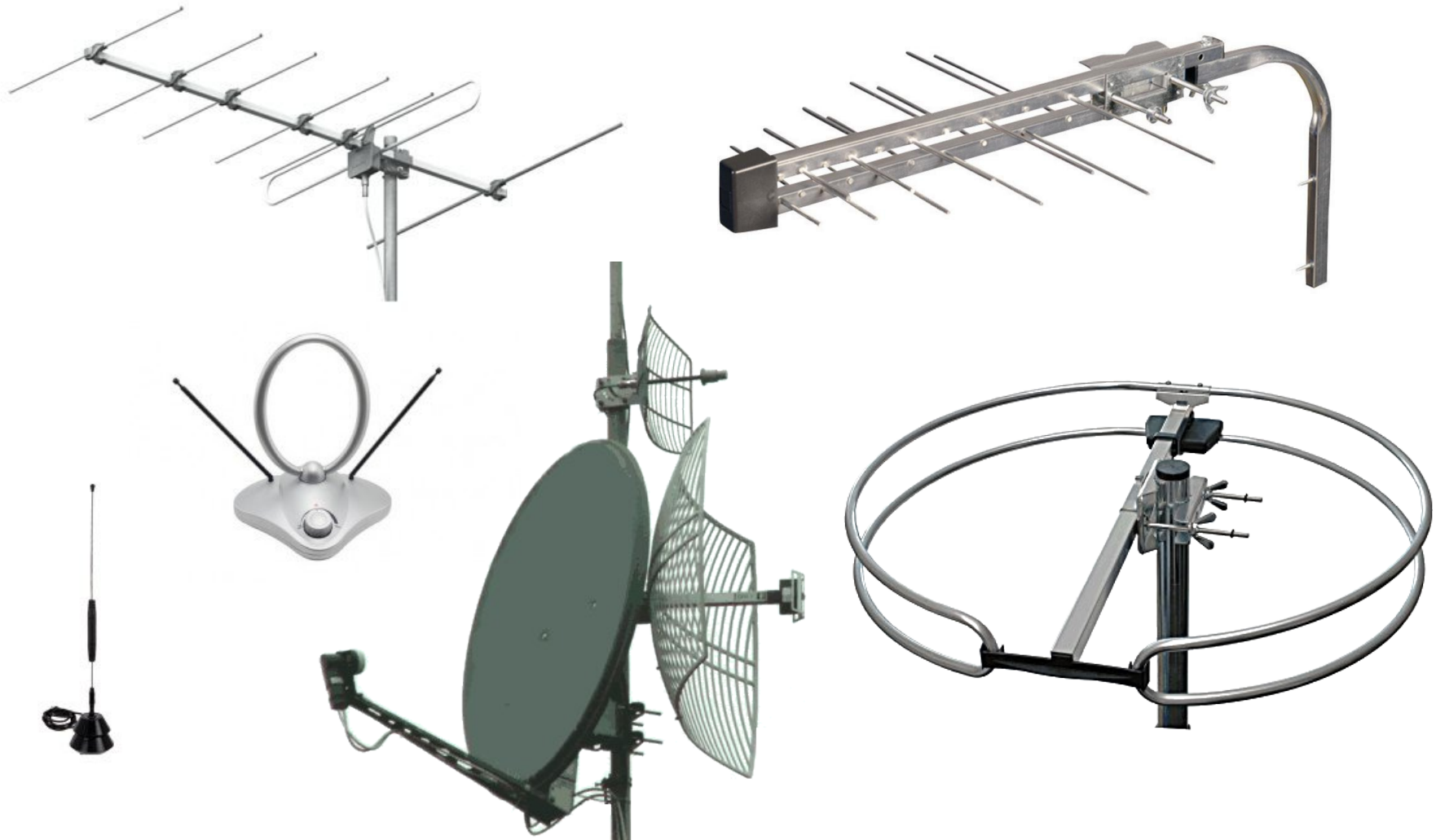


Frequenzbänder

- Vollständige Übersicht (für Deutschland):
→ <http://www.bundesnetzagentur.de>
- Interessante Frequenzbänder, z.B.:
 - CB-Funk (26.5 – 27.4 MHz)
 - 6m-Band (50.08 – 51.0 MHz)
 - Rundfunk (87.5 – 108.0 MHz)
 - NOAA-Wettersatelliten (137.1 – 137.92 MHz)
 - 2m-Band (144.0 – 146.0 MHz)
 - 70cm-Band (430.0 – 440.0 MHz)
 - ISM 433 (433.0 – 434.8 MHz)
 - ISM 868 (868.0 – 870.0 MHz)
 - ADS-B (1090 MHz)
- http://www.sigidwiki.com/wiki/Signal_Identification_Guide



Antennen...





Funkscanner

- Kommandozeilentool *rtl_power*.

```
> rtl_power -f 433M:435M:10k -i 2s -e 15m ism_433.csv
```

```
Number of frequency hops: 1
```

```
Dongle bandwidth: 2000000Hz
```

```
Downsampling by: 1x
```

```
Cropping by: 0.00%
```

```
Total FFT bins: 256
```

```
Logged FFT bins: 256
```

```
FFT bin size: 7812.50Hz
```

```
Buffer size: 16384 bytes (4.10ms)
```

```
Reporting every 1 seconds
```

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

```
  0: NOXON, DAB Stick, SN: 0
```

```
Using device 0: Terratec NOXON DAB/DAB+ USB dongle (rev 1)
```

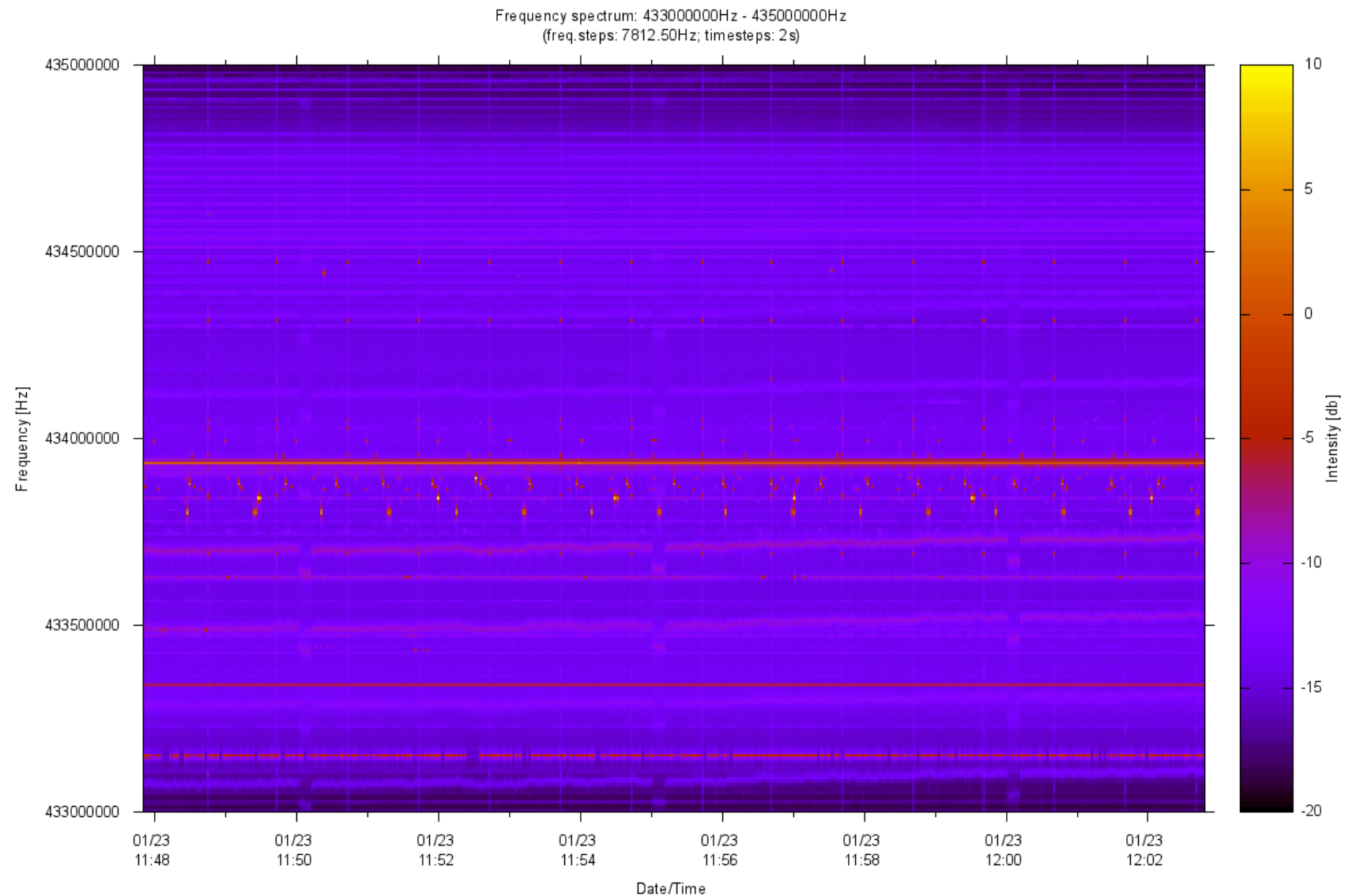
```
Found Fitipower FC0013 tuner
```

```
Tuner gain set to automatic.
```

```
Exact sample rate is: 2000000.052982 Hz ...
```



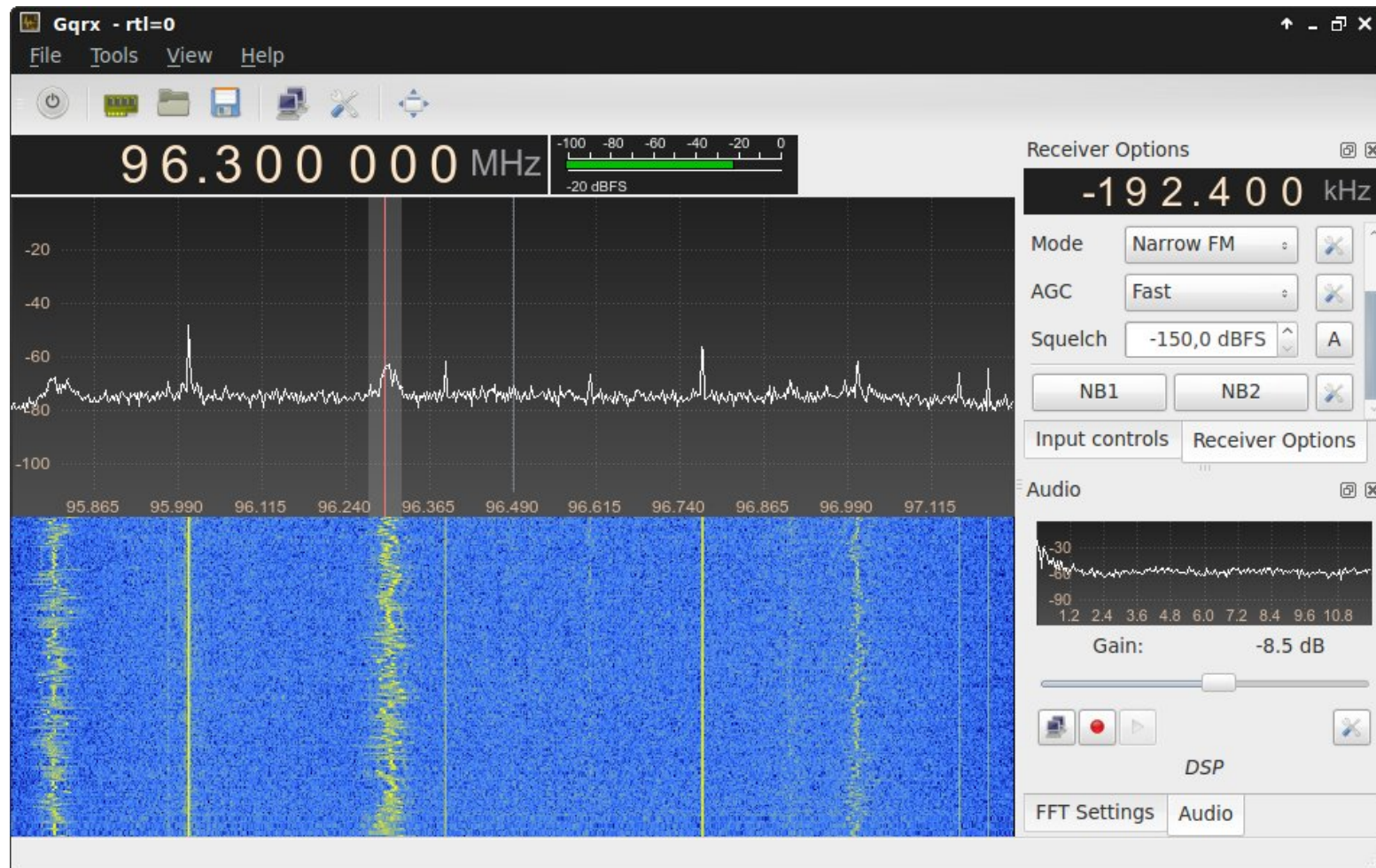
Funkscanner





Funkscanner

Programm *gqrx*:





Simple Aufzeichnung...

- Kommandozeilentool rtl_sdr:

```
> rtl_sdr /tmp/capture.bin -s 1800000 -f 392000000
```

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

```
0: NOXON, DAB Stick, SN: 0
```

```
Using device 0: Terratec NOXON DAB/DAB+ USB dongle (rev 1)
```

```
Found Fitipower FC0013 tuner
```

```
Sampling at 1800000 S/s.
```

```
Tuned to 392000000 Hz.
```

```
Tuner gain set to automatic.
```

```
Reading samples in async mode...
```



Ins Netzwerk streamen...

- Kommandozeilentool *rtl_tcp*:

```
> rtl_tcp -a localhost -p 1234
```

```
Found 1 device(s).
```

```
Found Fitipower FC0013 tuner
```

```
Using Terratec NOXON DAB/DAB+ USB dongle (rev 1)
```

```
Tuned to 100000000 Hz.
```

```
listening...
```

```
Use the device argument 'rtl_tcp=localhost:1234' in OsmoSDR
```

```
(gr-osmosdr) source to receive samples in GRC and control rtl_tcp  
parameters (frequency, gain, ...).
```



UKW-Radio hören...

- Kommandozeilentool *rtl_fm*:

```
> rtl_fm -M fm -f 106.2M -s 64k -A fast -l 0 -E deemp - |  
    aplay -r 48k -f S16_LE
```

Found 1 device(s):

0: NOXON, DAB Stick, SN: 0

Using device 0: Terratec NOXON DAB/DAB+ USB dongle (rev 1)

Found Fitipower FC0013 tuner

Tuner gain set to automatic.

Tuned to 106456000 Hz.

Oversampling input by: 16x.

Oversampling output by: 1x.

Buffer size: 8.00ms

Sampling at 1024000 S/s.

Output at 64000 Hz.

Wiedergabe: Rohdaten 'stdin' : Signed 16 bit Little Endian,

Rate: 48000 Hz, mono



Flugzeuge gucken...

- Kommandozeilentool *dump1090* installieren/starten:

```
> git clone git://github.com/MalcolmRobb/dump1090.git ...  
...  
> cd dump1090.git  
> make ...  
  
> ./dump1090 --interactive --net
```

- ...und im Browser:

```
http://localhost:8080/
```



Flugzeuge gucken...

DUMP1090 - Mozilla Firefox

DUMP1090 x ADS-B dump1090 x +

localhost:8080 | dump1090

Map | Bad Wilsnack | Oranienburg | Berlin | Potsdam | Beelitz | Magdeburg | Dessau-Roßlau | Köthen

Local Time  **UTC Time** 

[Reset Map] [Settings]

GW19T [FR24] [FlightStats] [FlightAware]

Altitude: 17350 ft Squawk: 5061
Speed: 396 kt ICAO (hex): 3c6617
Track: 253° (W)
Lat/Long: 52.418839, 12.385178

ICAO	Flight	Squawk	Altitude	Speed	Track	Msgs	Seen
3c6617	GW19T	5061	17350	396	253	114	1

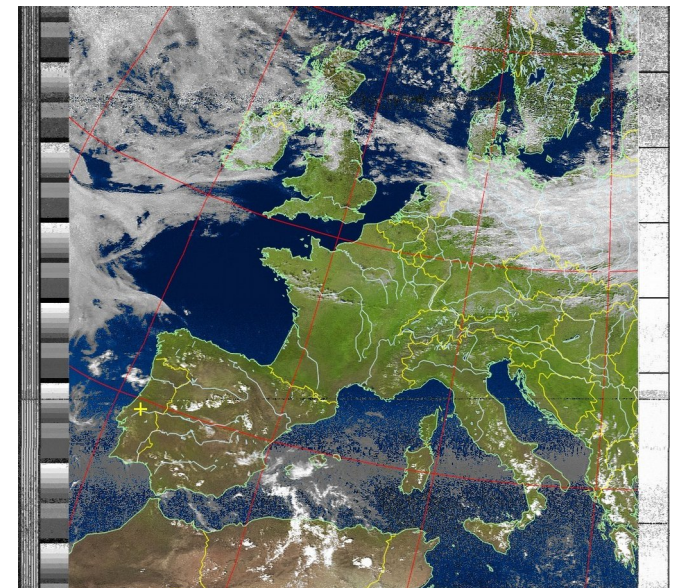
Map data ©2016 GeoBasis-DE/BKG (©2009), Google Terms of Use Report a map error



Wettersatellitenbilder gucken...

z.B. NOAA-Wettersatelliten:

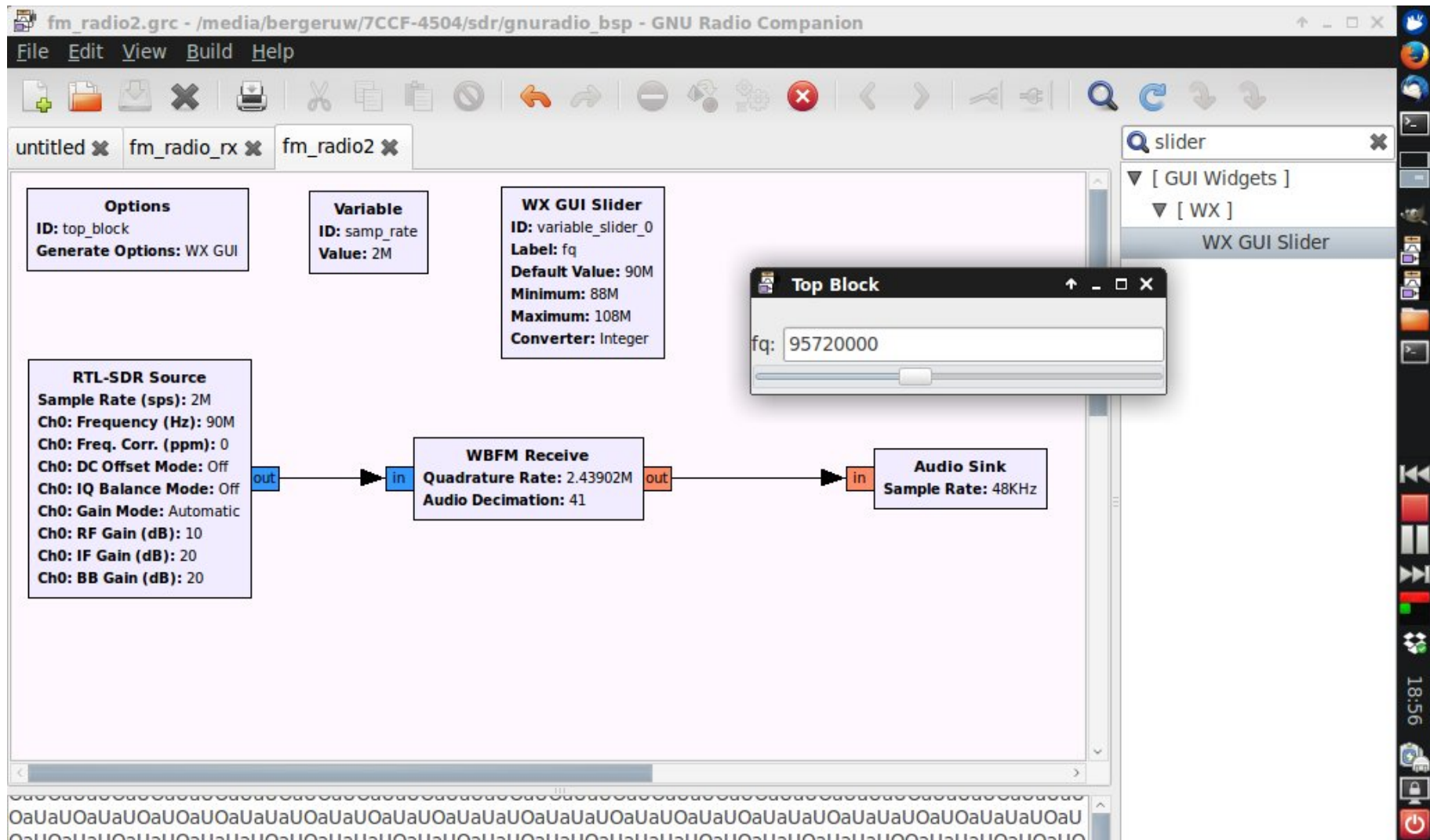
- Empfangsfrequenz: 137.1 ... 137.92 MHz
- Wann/Wo/Welcher Satellit, z.B.:
 - Orbitron (<http://www.stoff.pl/>)
 - SatScape (<http://scotthather.weebly.com/satscape.html>)
- Eine gute Antenne!
 - Turnstile Antenne
 - Quadrifilar Helix (QFH) Antenne
 - Double Cross Antenne (DCA)
- Dekodierung der Bilder, z.B.:
 - WxtoImg (<http://www.wxtoimg.com/>)
 - ADTPEC (<http://atpdec.sourceforge.net/>)



<http://ruralhacker.blogspot.de/2012/09/rtl-sdr.html>



Universal-Baukasten: GnuRadio





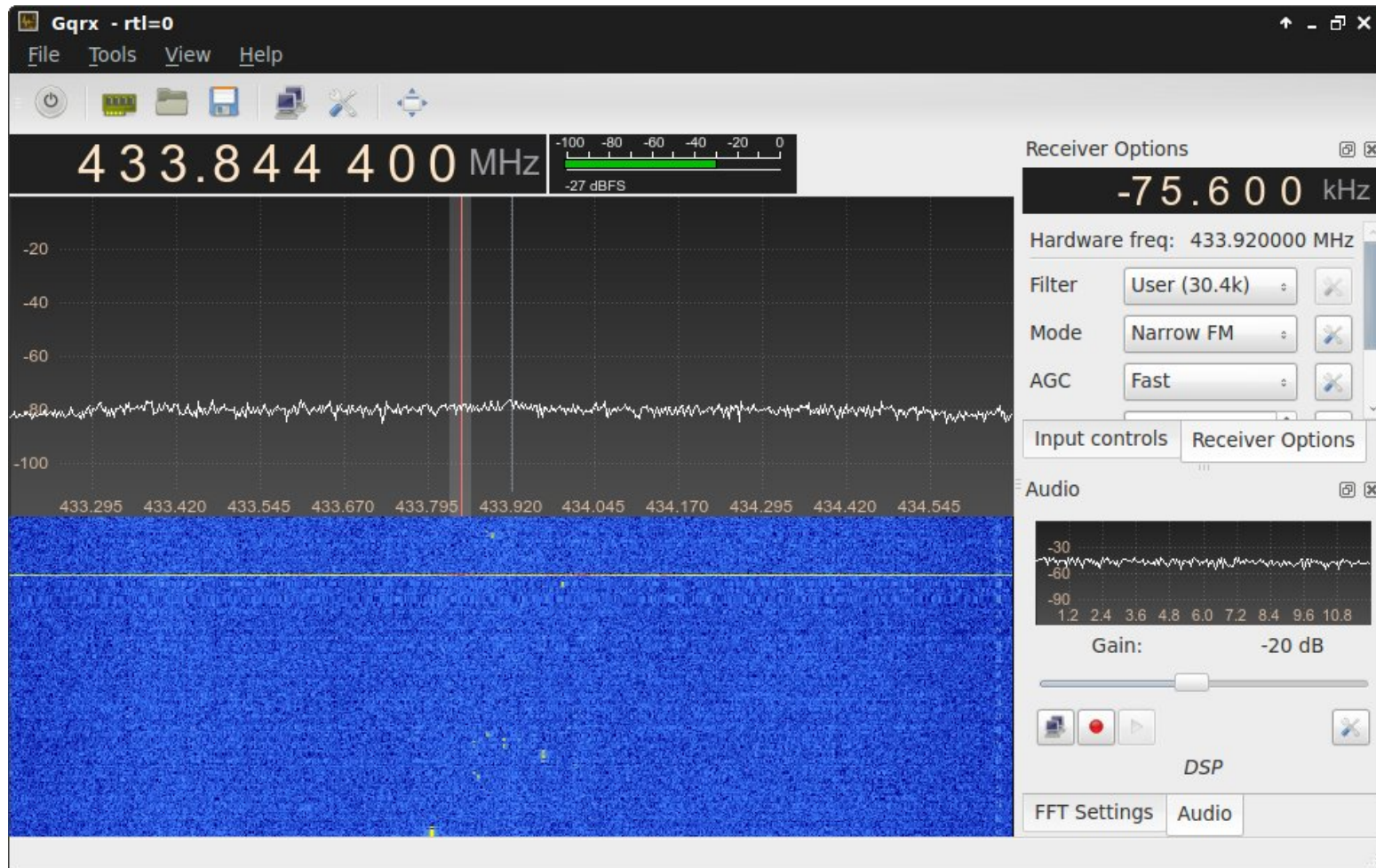
Weitere Tools und Programme

- Übersichten:
 - <http://sdr.osmocom.org/trac/wiki/rtl-sdr#KnownApps>
 - <http://www.rtl-sdr.com/big-list-rtl-sdr-supported-software/>
- Spezielle Linux-Distributionen, u.a.:
 - Skywave Linux
→ <http://skywavelinux.com/>
 - GNU Radio Live SDR Environment
→ <https://gnuradio.org/redmine/projects/gnuradio/wiki/GNURadioLiveDVD>



Funksignalanalyse (Vorgehensweise)

- Funksignal finden → Scanner





Funksignalanalyse (Vorgehensweise)

- Funksignal aufnehmen → z.B. rtl_sdr, rtl_fm, gqrx

```
> rtl_fm -M am -f 433.844M -s 64k -g 50 > /home/bergeruw/sampl.bin
```

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

```
0: NOXON, DAB Stick, SN: 0
```

```
Using device 0: Terratec NOXON DAB/DAB+ USB dongle (rev 1)
```

```
Found Fitipower FC0013 tuner
```

```
Tuner gain set to 19.70 dB.
```

```
Tuned to 434099999 Hz.
```

```
Oversampling input by: 16x.
```

```
Oversampling output by: 1x.
```

```
Buffer size: 8.00ms
```

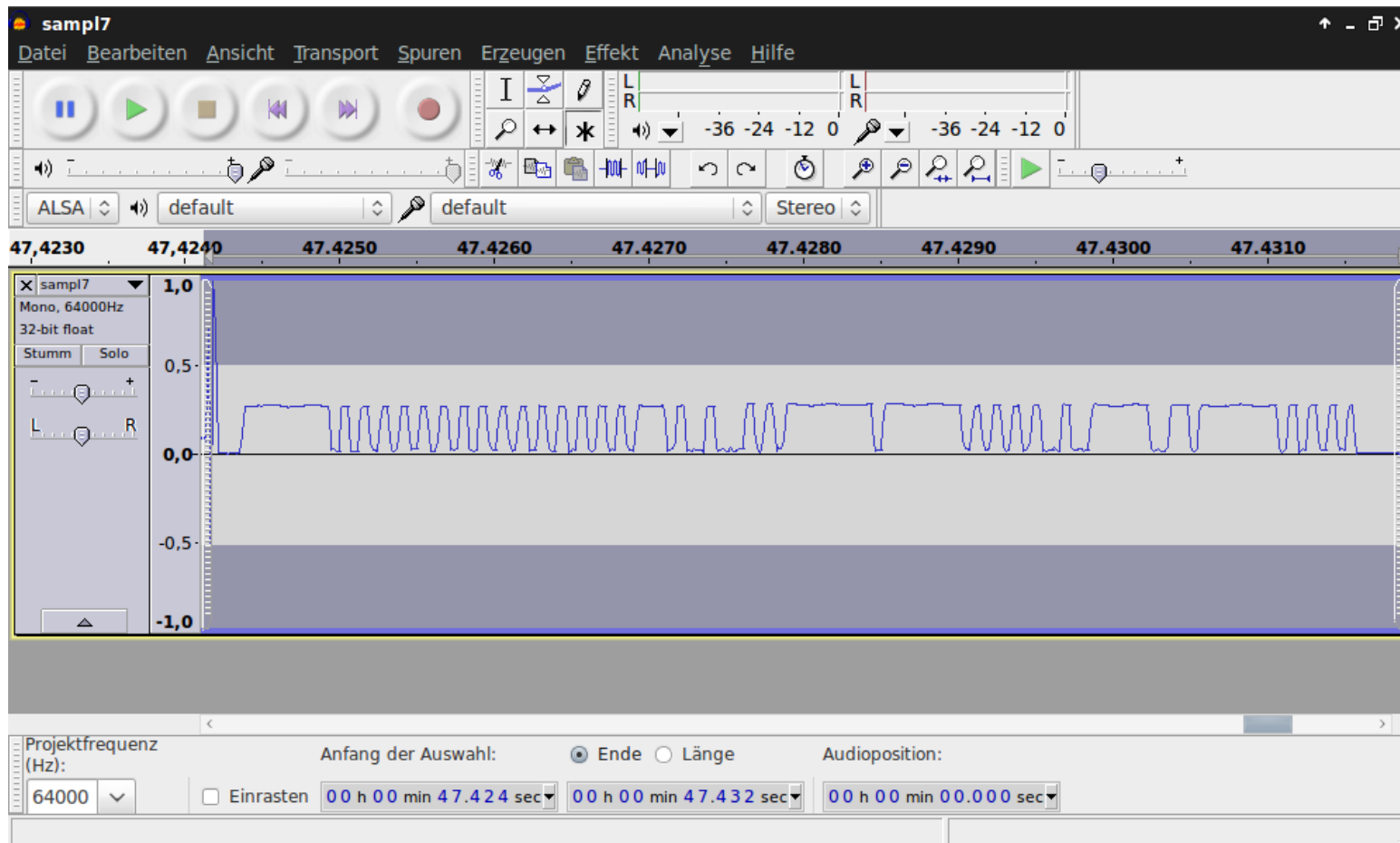
```
Sampling at 1024000 S/s.
```

```
Output at 64000 Hz.
```



Funksignalanalyse (Vorgehensweise)

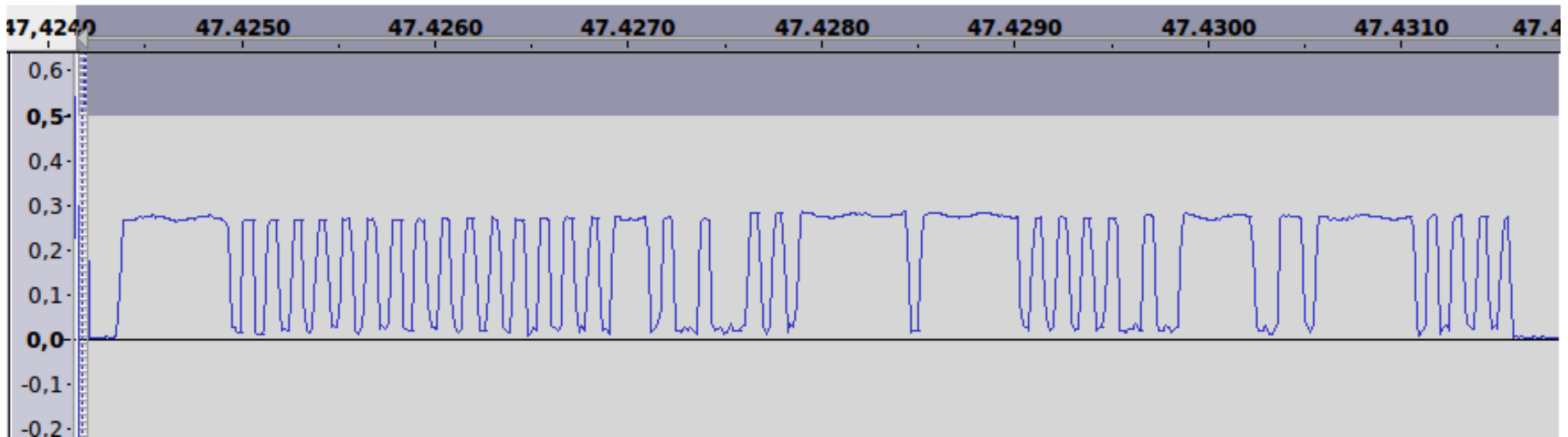
- Funksignal mal ansehen → z.B. audacity





Funksignalanalyse (Vorgehensweise)

- Funksignal decodieren
→ Blatt Papier, Stift, Lineal und Taschenrechner :-)





Funksignalanalyse (Vorgehensweise)

- ...zum Schluss alle Schritte automatisieren:
 - ein Programm, Script o.ä. schreiben
 - mit GnuRadio-Modulen zusammenklicken
 - o.ä.



Weiterführende Informationsquellen

- <http://rtlsdr.org/>
- <http://sdr.osmocom.org/trac/wiki/rtl-sdr>
- „Hack-a-day für rtl-sdr“: <http://www.rtl-sdr.com>
- <http://superkuh.com/rtlsdr.html>
- [http://bralug.de/wiki/Software_Defined_Radio_\(SDR\)_mit_Linux](http://bralug.de/wiki/Software_Defined_Radio_(SDR)_mit_Linux)



Ende!



Demos

- rtl_test (auch mit höherer Sampling-Rate)

```
rtl_test  
rtl_test -s 3.2e6
```

- rtl_power in Verbindung mit Tcl-Script

```
rtl_power -f 433M:435M:10k -i 2s -e 15m ism_433.csv
```

- gqrx

- rtl-fm

```
rtl_fm -M fm -f 106.2M -s 64k -A fast -l 0 -E deemp - | aplay -r 48k -f S16_LE
```

- Dump1090

```
./dump1090 --interactive -net  
http://localhost:8080/
```