Experiments with the RTL-SDR

Danny Robson

Caveats

I know *exceedingly* little about radio or electronics.

Context

Communications

Remote operates on a low noise FM frequency of 916 Mhz which allows for long range operation from a compact unit

Idea

1. Sniff the payload during button presses
2. Replay the data from something more extensible
3. Pray it’s not authenticated

Tech

1. RTL-SDR (RTL2832U)
2. rpitx
3. Luck

Software Defined Radio

What if a radio but preferring digital to analogue parts?

RTL2832U

- A chipset common on DVB-TV dongles
- Raw data from the chipset
- Pretty wide frequency range (28-1766MHz)
- Widely available
- Cheap

RTL-SDR

- RTL2382U
- Temperature controlled oscillator
- SMA antenna connector
- Thermal pads
- Metal enclosure
- Direct sampling mode
- $40USD in a kit

RTL-SDR

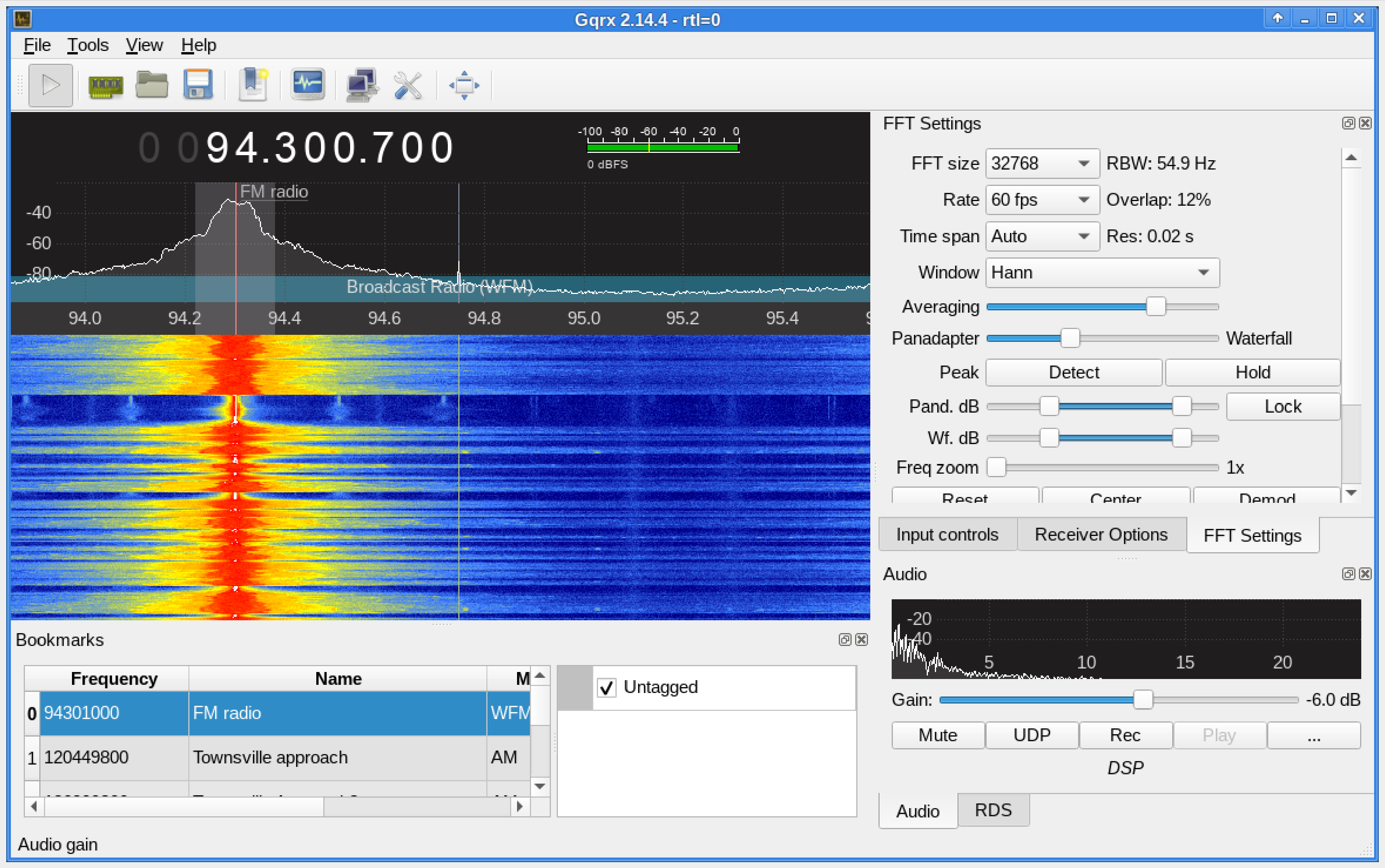
RTL-SDR.COM
QUICKSTART SETUP GUIDE: RTL-SDR.COM/QSG
DVB-T+DAB+FM+SDR
RTL2832U R820T2 TCXO+BIAS T+HF
V.3
CE FC

Configuration

It’s a TV tuner, so you might need to blacklist the kernel module

```
blacklist dvb_usb_rtl28xxu
```

gqrx



Gqrx 2.14.4 - rtl=0

0 094.300.700

FFT Settings

FFT size	32768	RBW: 54.9 Hz
Rate	60 fps	Overlap: 12%
Time span	Auto	Res: 0.02 s
Window	Hann	
Freq zoom		1x

Bookmarks

	Frequency	Name	M
0	94301000	FM radio	WFM
1	120449800	Townsville approach	AM

☑ Untagged

Audio

Gain: -6.0 dB

gqrx

Record IQ file from `gqrx`.

Demo?

crosses fingers…

rpitx

- Turn a Pi into radio transmitter with one piece of wire on one GPIO pin
- Requires a band-pass filter. It’s *incredibly* noisy.
- Questionable legality depending on strength and frequency.

rpitx

Play IQ file using

```
sendiq -i ${input} -f 916
```

TODO

Embarrassingly I’ve misplaced all my headers and wires in the move and need to source more…

Future Work

- rpitx
  - fix it’s build system…