rtl2832u + GNU radio

Let's have fun !

rtl2832u + GNU radio

Spoiler alert !

Sommaire

- Partie _ _ _ _ _ _ _ _ |¯| : Learn
  - RTL..what ?
    - Radio ?
    - SDR ?
  - Tools ?
  - Entendre quoi ?
  - Autres signaux ?

Sommaire

- Partie _ _ _ _ _ _ |¯| _ : Listen
  - Démo live rapide
    - Voix
    - Data

Sommaire

- Partie _ _ _ _ _ _ |¯ ¯| : Reverse
  - Analyse de signaux connus.
  - Analyse de signaux inconnus

Sommaire

- Partie _ _ _ _ _ |¯| _ _ : Give me more !
  - Links
  - Links
  - Links
  - Links
  - Links
  - Links
  - ...

Sommaire

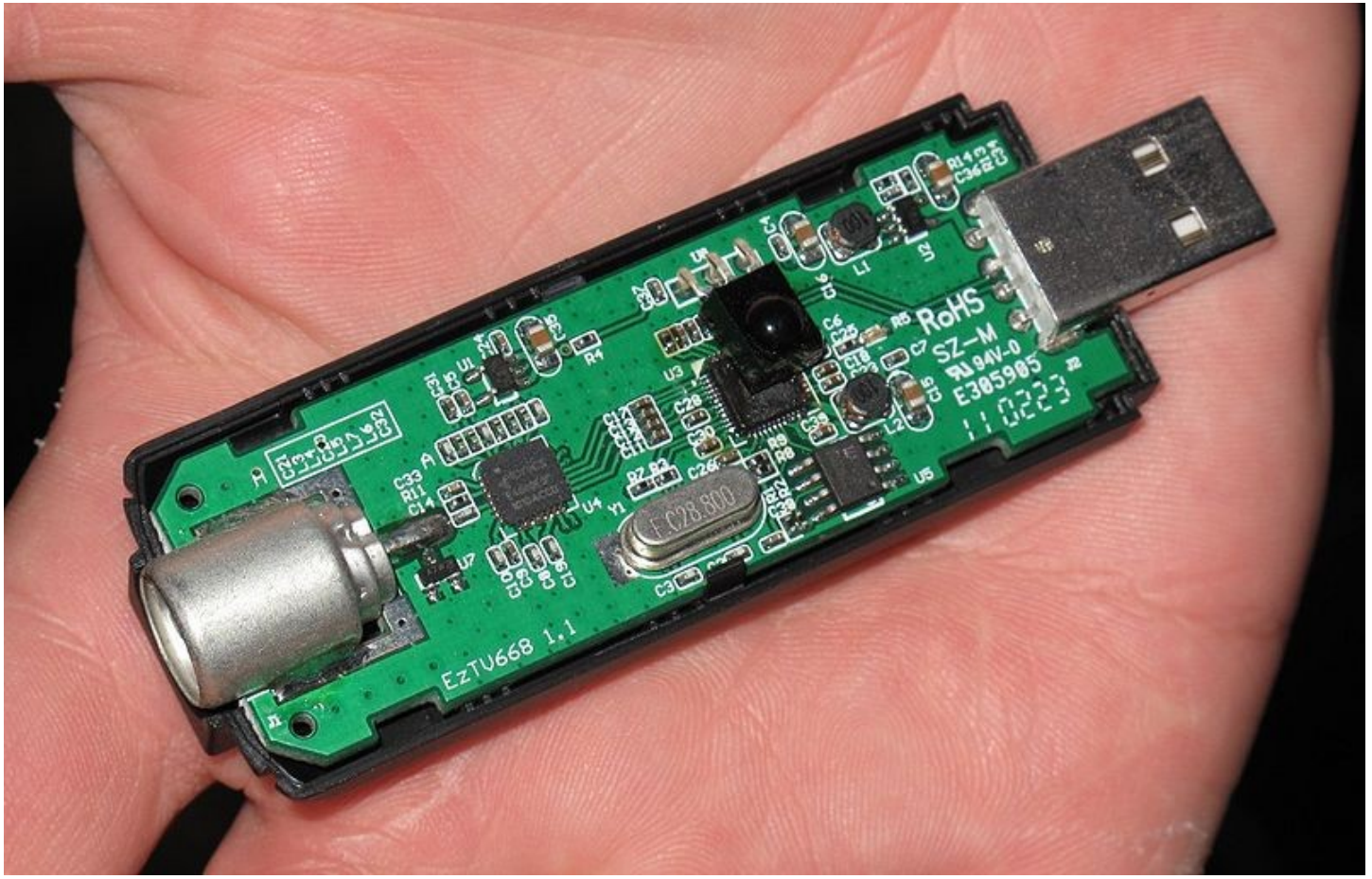
- Partie _ _ _ _ _ |¯| _ |¯| : Ask
  - Question ?

Partie _ _ _ _ _ _ _ _ |¯|

Learn

RTL..what ?

RTL..what ?



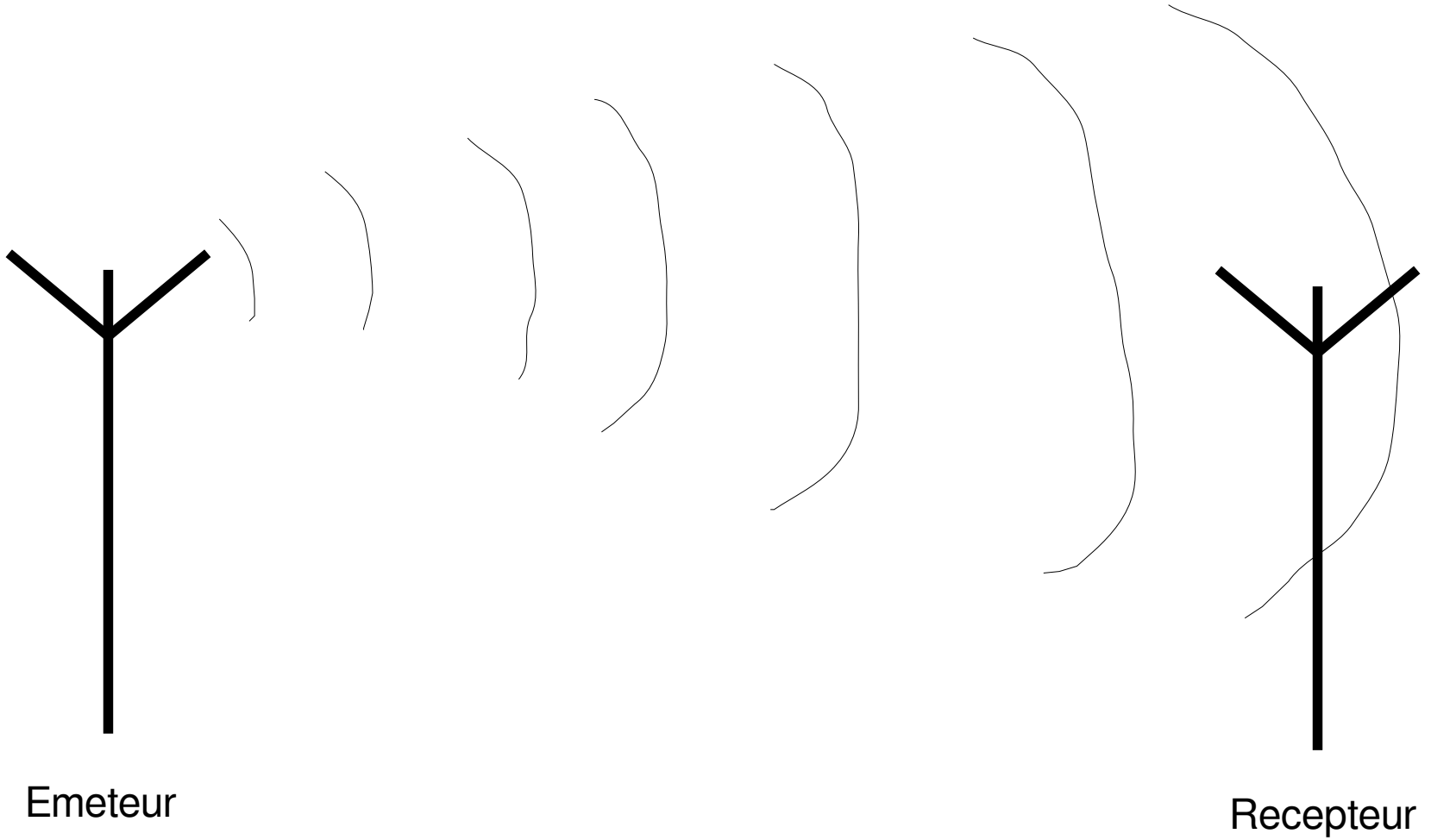
RTL..what ?

- Tuner tv/fm RTL2832u

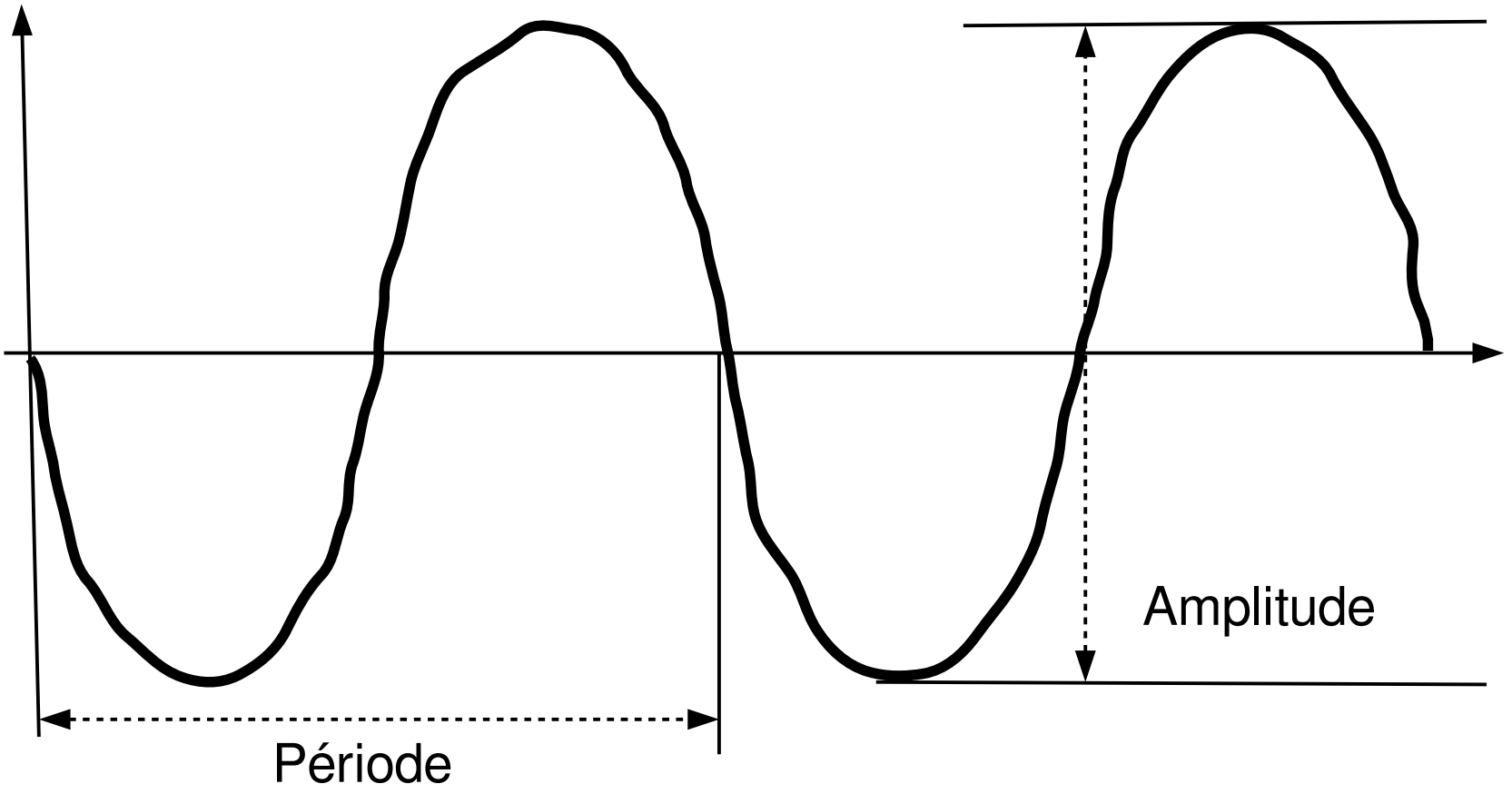
RTL..what ?

- Tuner tv/fm RTL2832u
- Cheap SDR (Software Defined Radio)

Radio ?



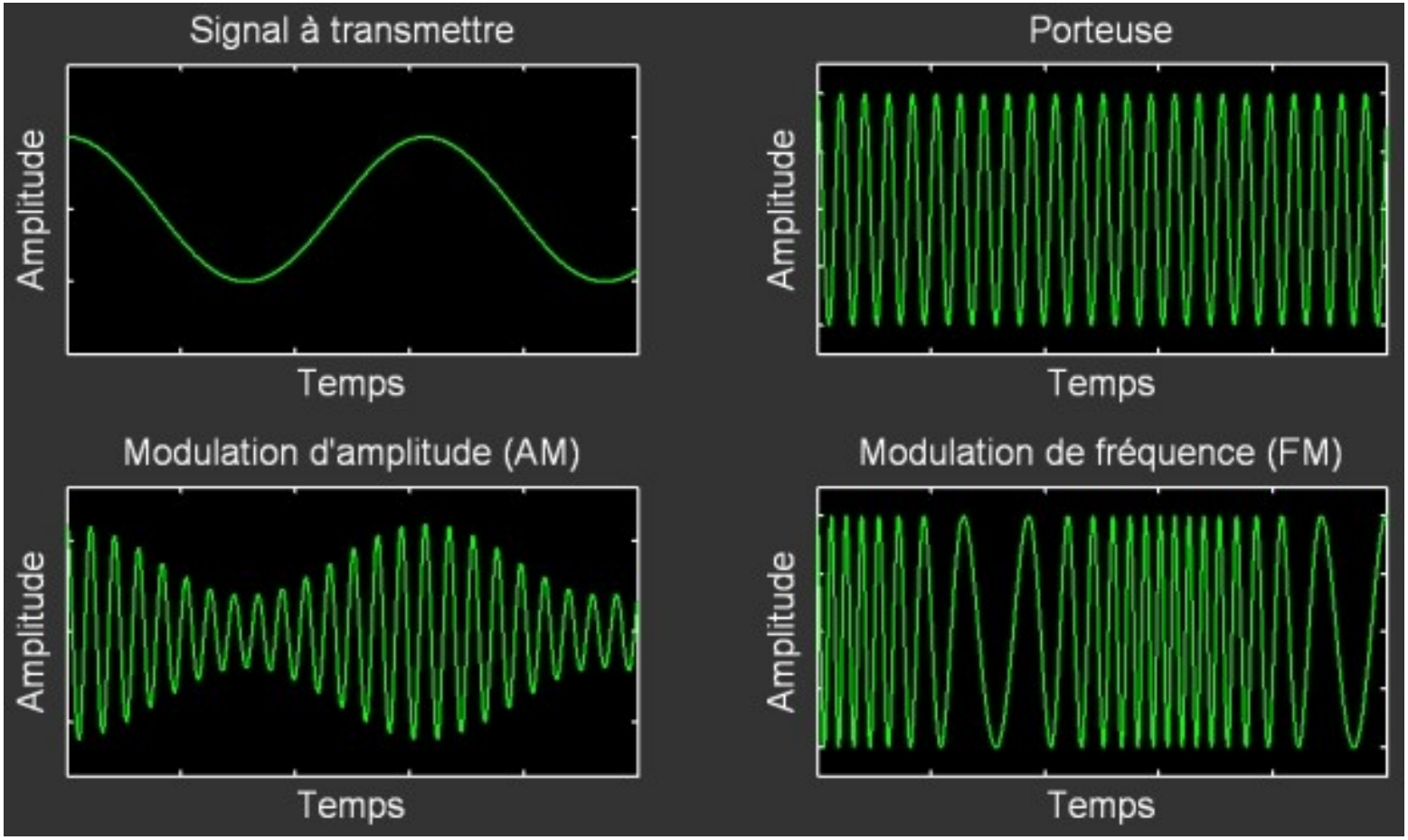
Radio ?



Radio ?

- Période (s)
  - T
- Fréquence (Hz)
  - F = 1 / T
- Longeur d'onde (m)
  - $\lambda = c / f$

Radio ?


Signal à transmettre
Amplitude
Temps
Porteuse
Amplitude
Temps
Modulation d'amplitude (AM)
Amplitude
Temps
Modulation de fréquence (FM)
Amplitude
Temps

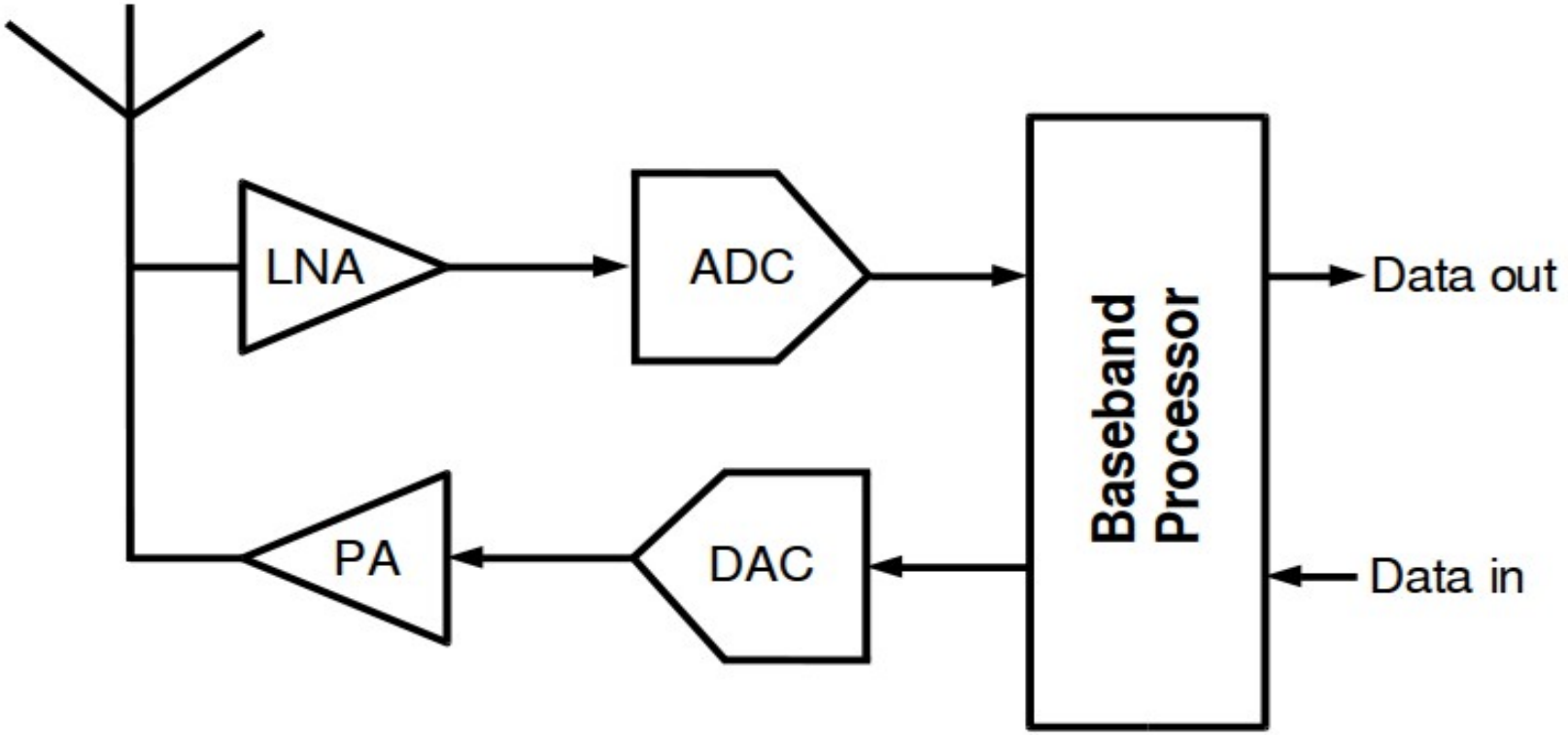
SDR ?

Software Defined radio

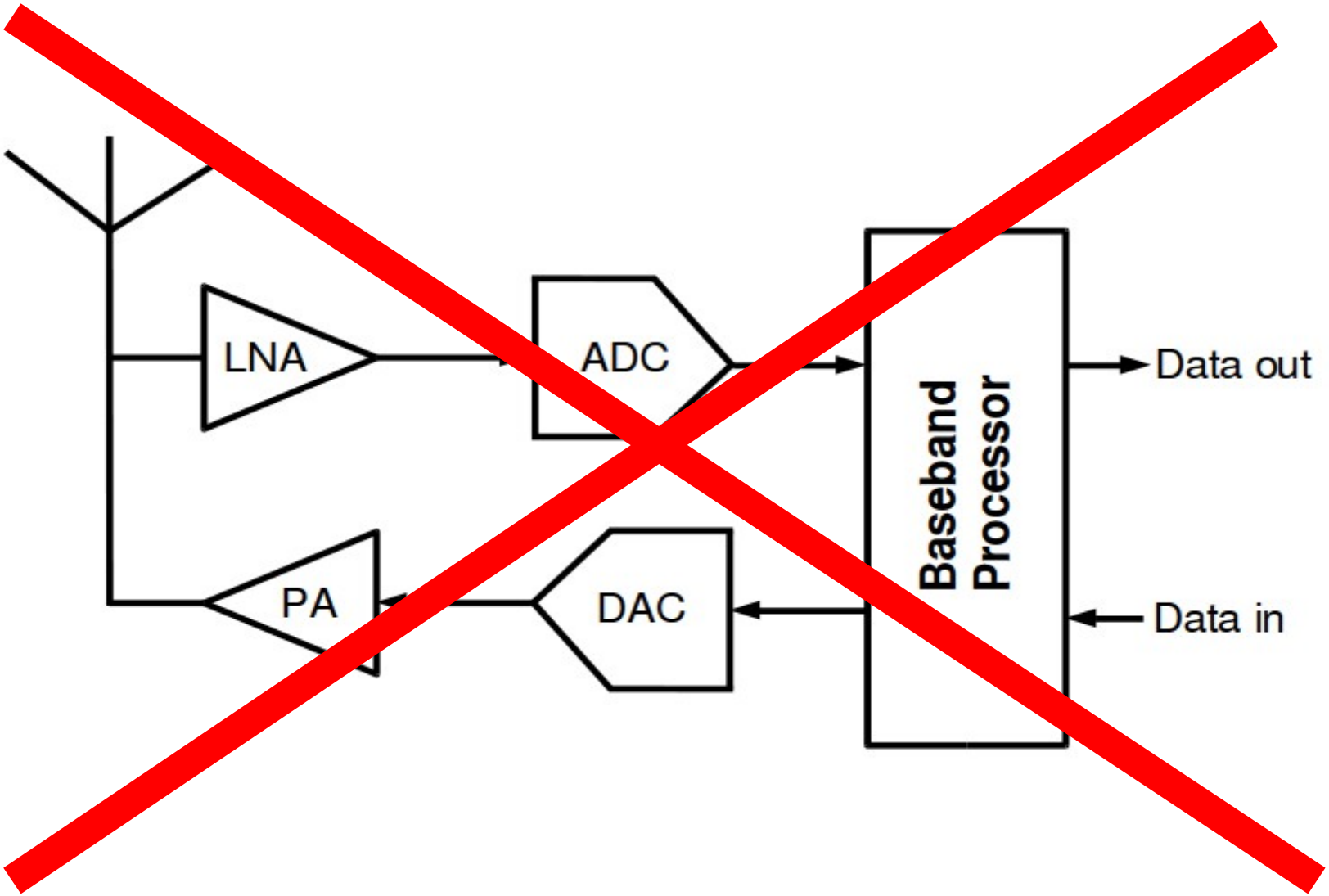
SDR ?

SDR ?

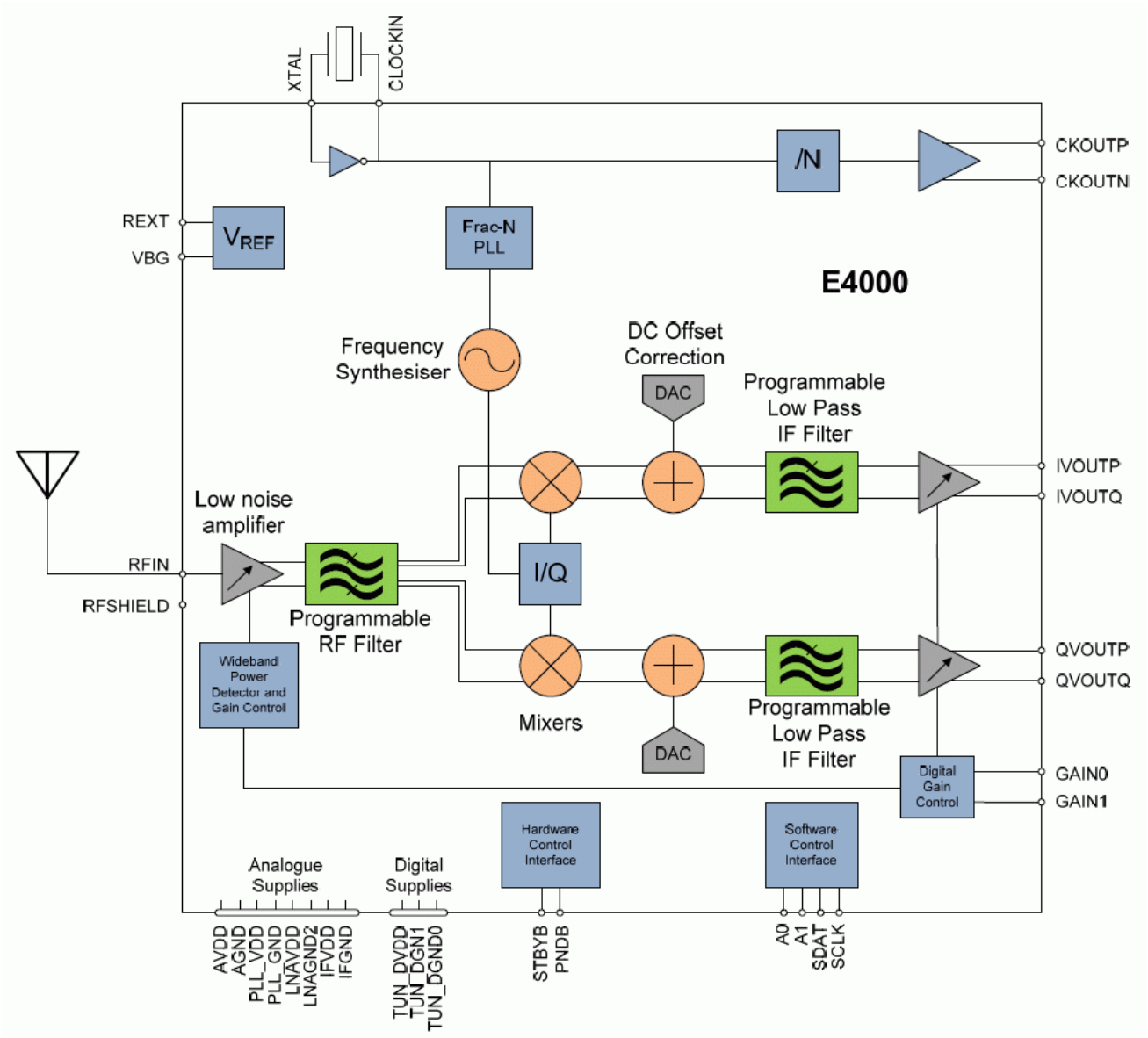
SDR ?



SDR ?



SDR ?


XTAL
CLOCKIN
/N
CKOUTP
CKOUTN
REXT
VBG
VREF
Frac-N PLL
E4000
Frequency Synthesiser
DC Offset Correction
DAC
Programmable Low Pass IF Filter
IVOUTP
IVOUTQ
Low noise amplifier
RFIN
RFSHIELD
I/Q
Programmable RF Filter
Wideband Power Detector and Gain Control
Mixers
DAC
Programmable Low Pass IF Filter
QVOUTP
QVOUTQ
Digital Gain Control
GAIN0
GAIN1
Hardware Control Interface
Software Control Interface
Analogue Supplies
Digital Supplies
AVDD
AGND
PLL_VDD
PLL_GND
LNAVDD
LNAGND2
IFVDD
IFGND
TUN_DVDD
TUN_DGN1
TUN_DGND0
STBYB
PNDB
A0
A1
SDAT
SCLK

SDR ?

Avec quoi peut-on faire de la SDR ?

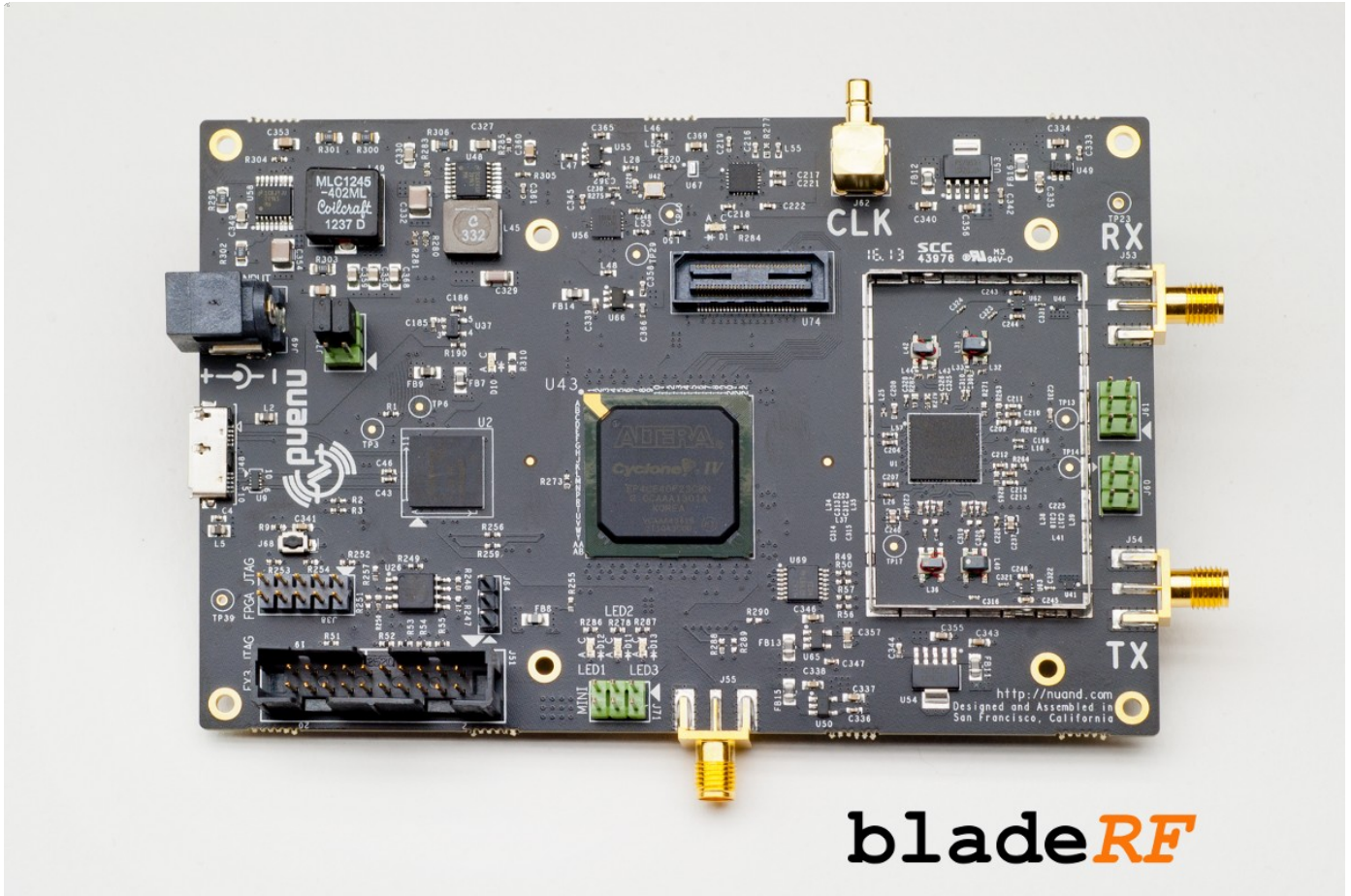
SDR ?


RX2
Ettus
Research
RF 1
RF 2
RF 3
RF 4
CLK I/0
6VDC
USB
www.ettus.com
USRP
Universal Software Radio Peripheral

SDR ?

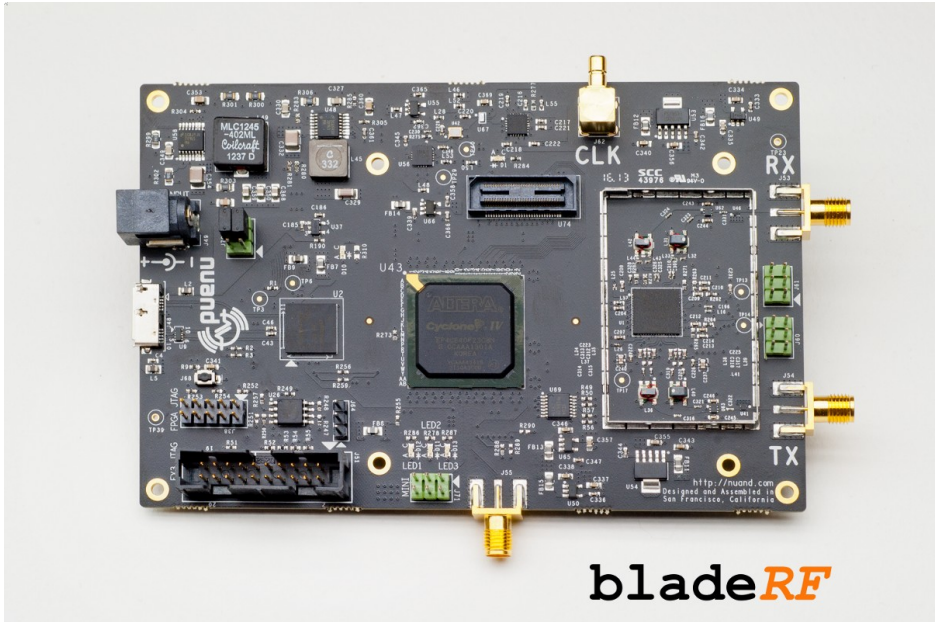
- USRP B210
- 975€
- RX/TX full duplex
- 70Mhz – 6Ghz
- 61Msps 12 bits

SDR ?

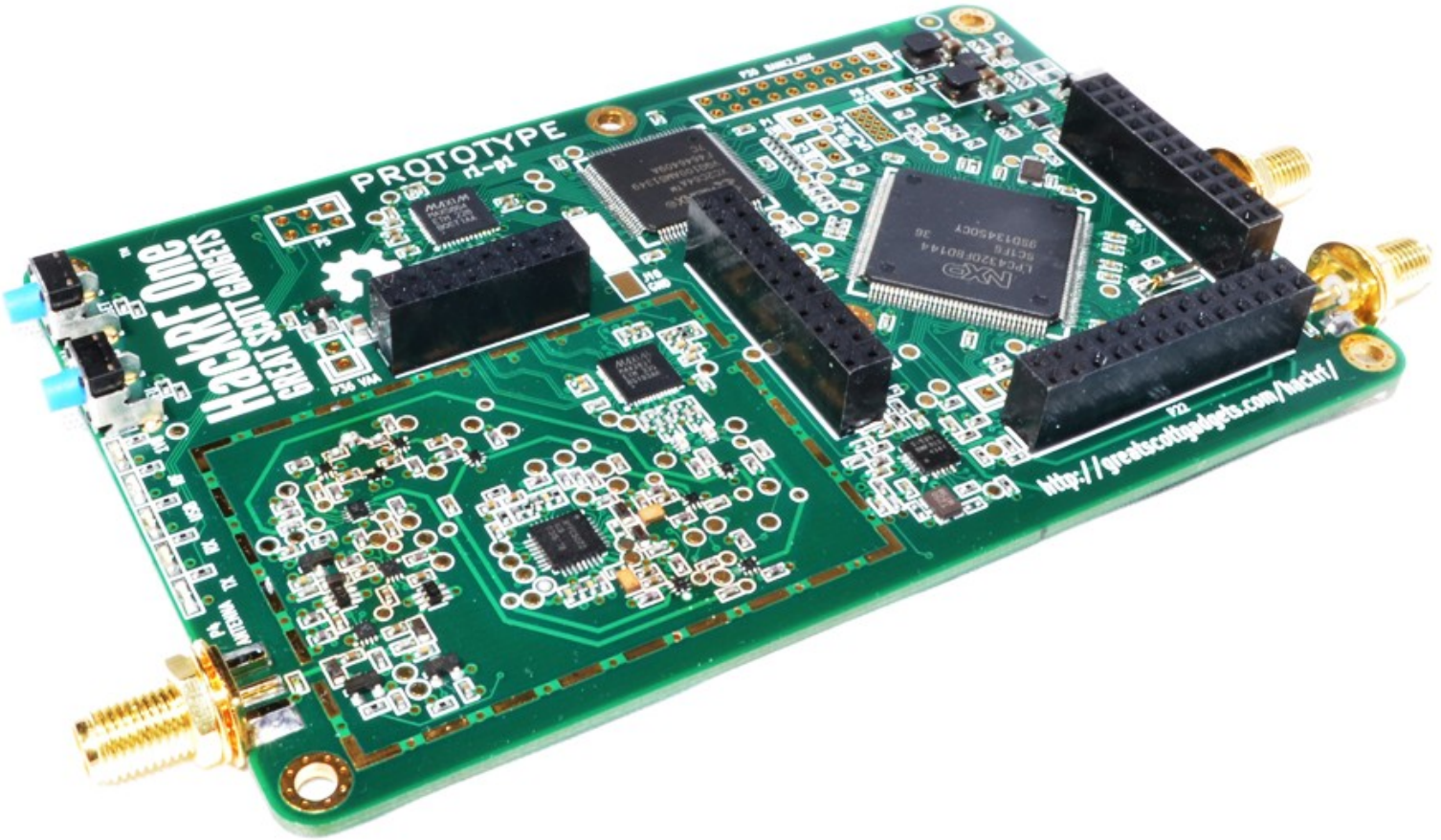

CLK
RX
TX
U43
LED1
LED2
LED3
http://nuand.com
Designed and Assembled in
San Francisco, California
bladeRF

SDR ?

- BladeRF
- 300 €
- RX/TX full duplex
- 300Mhz – 3.8Ghz
- 40Msps 12 bits

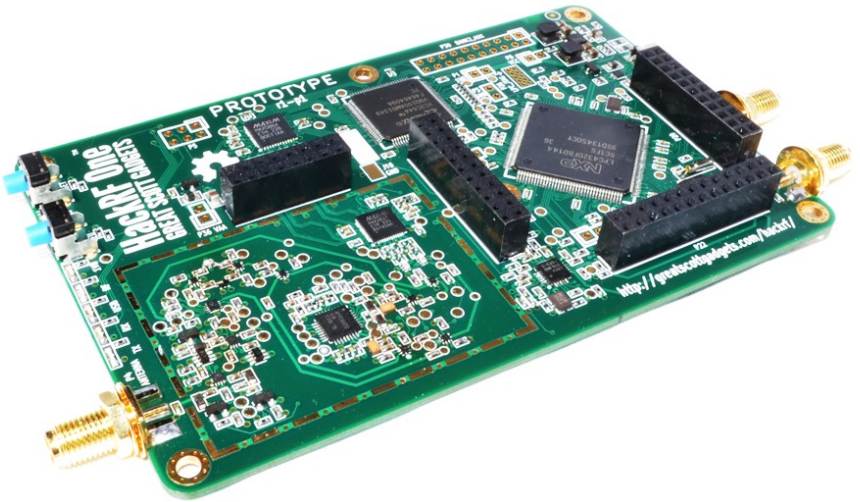


SDR ?


PROTOTYPE
HackRF One
Great Scott Gadgets
http://greatscottgadgets.com/hackrf/

SDR ?

- HackRF One
- 220 €
- RX/TX half duplex
- 10Mhz – 6Ghz
- 20Msps 8 bits



SDR ?

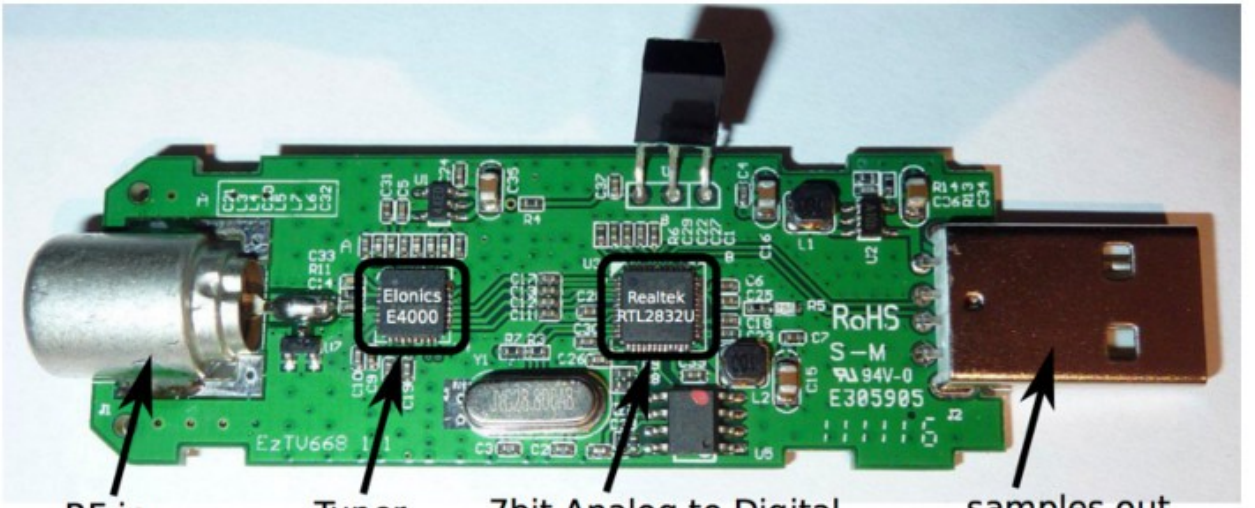

FUNcube
Dongle Pro
FCD Pro V0.0
Serial: 0000000
http://www.funcube.org.uk
AMSAT-UK

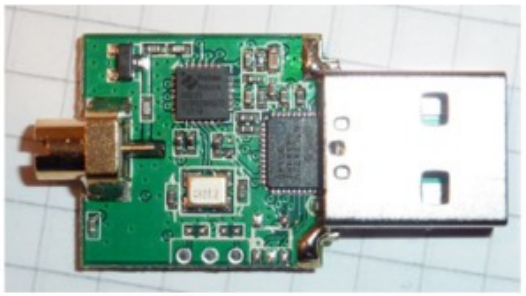
SDR ?

- FUNcube
- 120 €
- RX only
- 150Khz – 240Mhz

  420Mhz – 1.9Ghz
- 96ksps

SDR ?

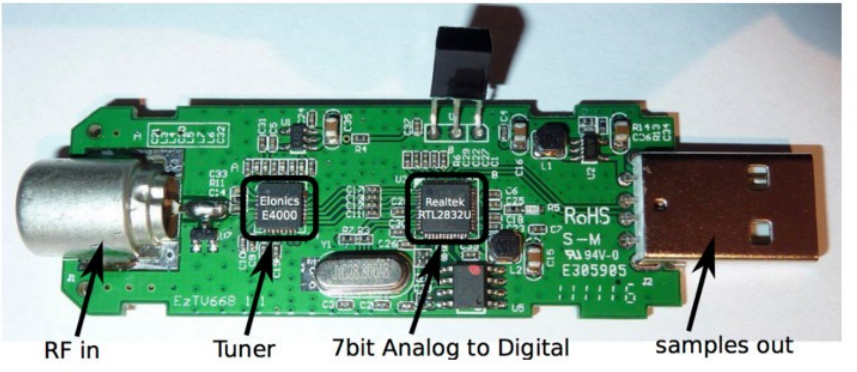

Elonics
E4000
Realtek
RTL2832U
RoHS
S-M
94V-0
E305905
RF in
Tuner
7bit Analog to Digital
samples out

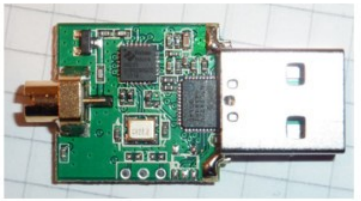


SDR ?

- RTL2832u + E4000/R820T
- 10 € - 20 €
- RX only
- 24Mhz – 1.7Ghz

  (E4000 2.2 Ghz)
- 2.4Msps 7b





Tools ?

Ok, j'ai l'ardware. Maintenant j'écoute avec quoi ?

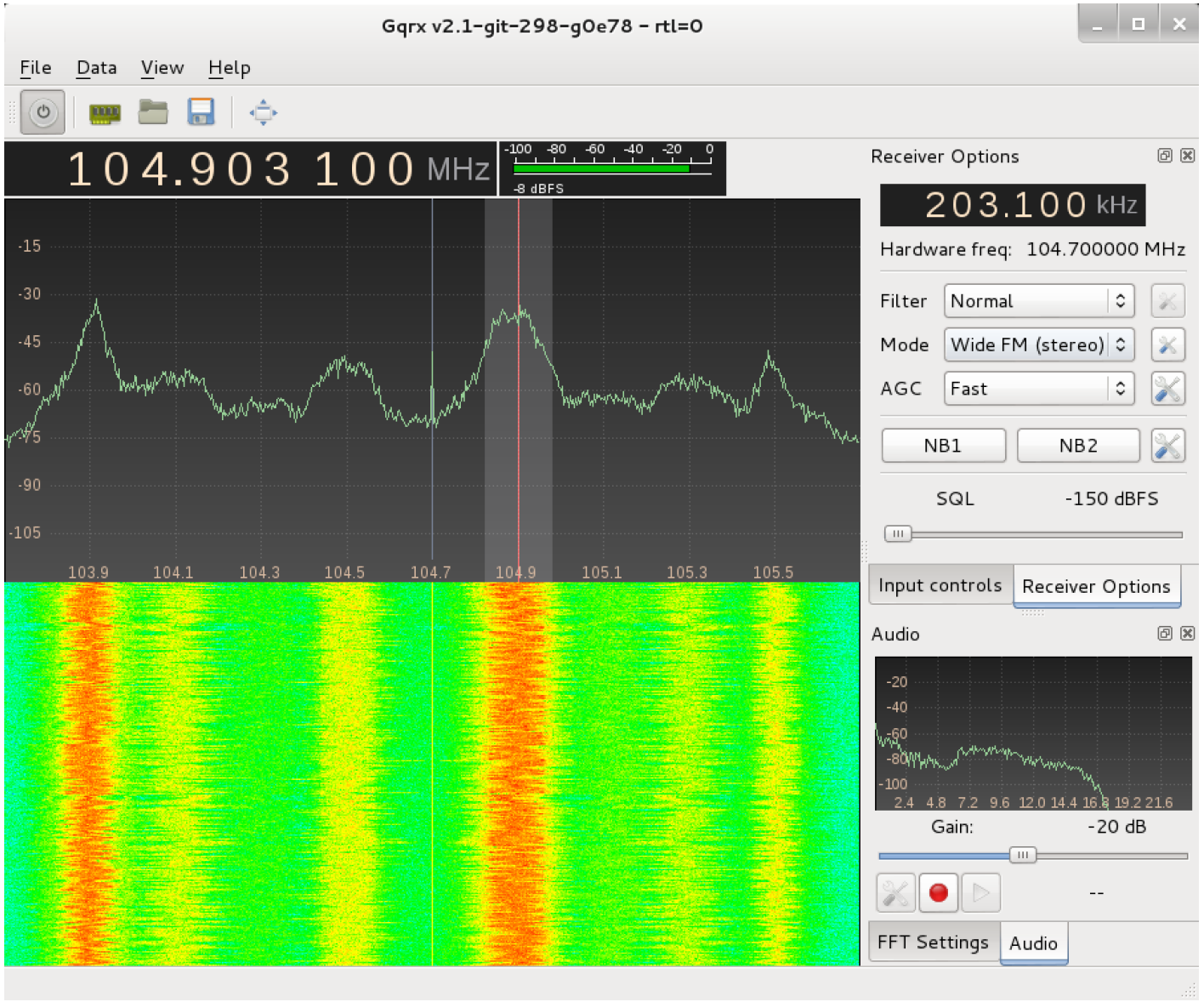
Tools ?

- Pour écouter de l'audio
  - rtl_fm
  - Gqrx
  - Multimode
  - Gnuradio

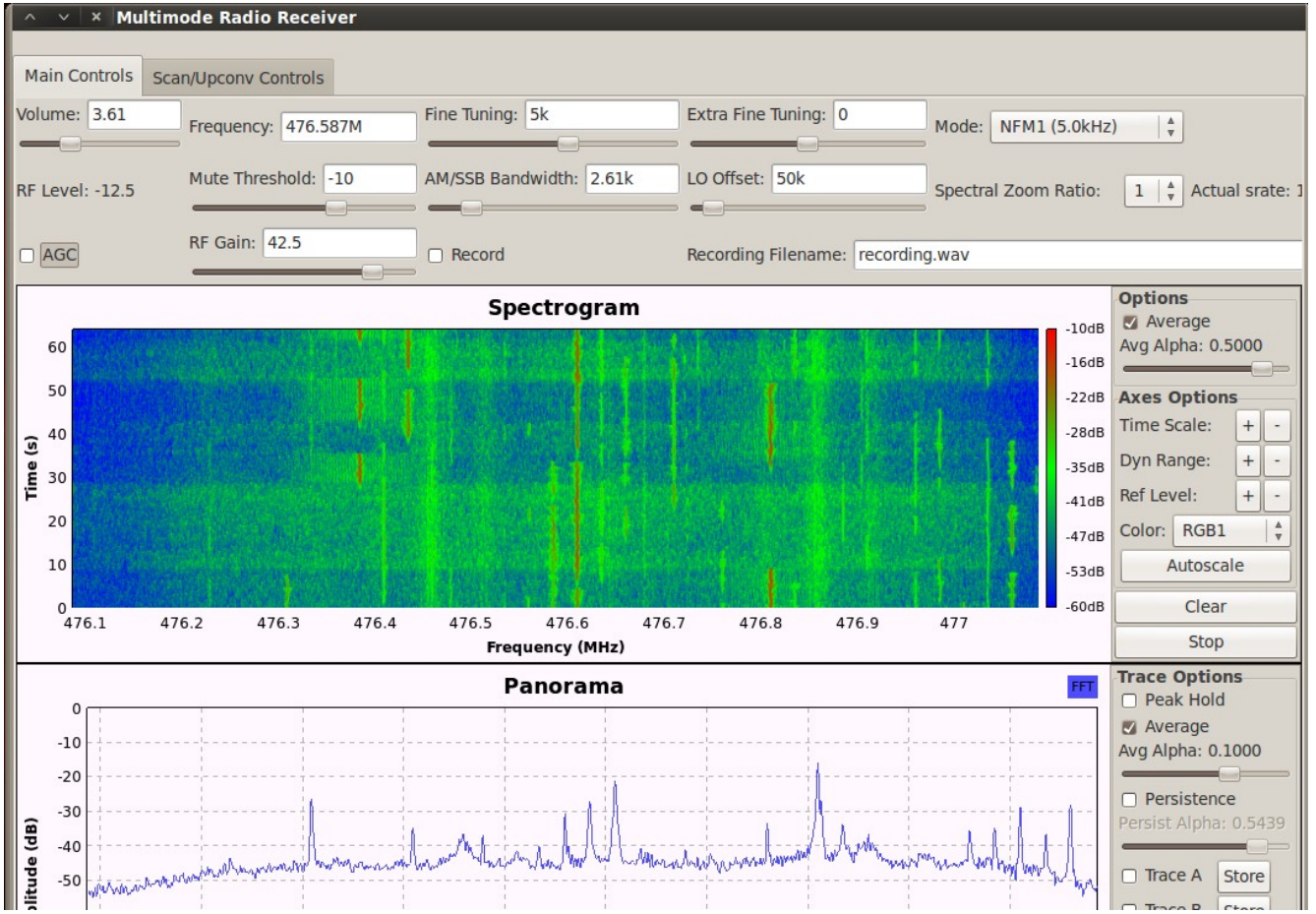
Tools ?

```
pi@raspberrypi ~ $ rtl_fm -f 105.1e6 -W -s 200000 -r 48000 - | aplay -r 48k -f S16_LE
Found 1 device(s):
  0:  Generic, RTL2832U, SN: 77771111153705700

Using device 0: Generic RTL2832U
Found Elonics E4000 tuner
Oversampling input by: 2x.
Oversampling output by: 4x.
Buffer size: 5.12ms
Tuned to 105516000 Hz.
Sampling at 1600000 Hz.
Output at 48000 Hz.
Tuner gain set to automatic.
Playing raw data 'stdin' : Signed 16 bit Little Endian, Rate 48000 Hz, Mono
```

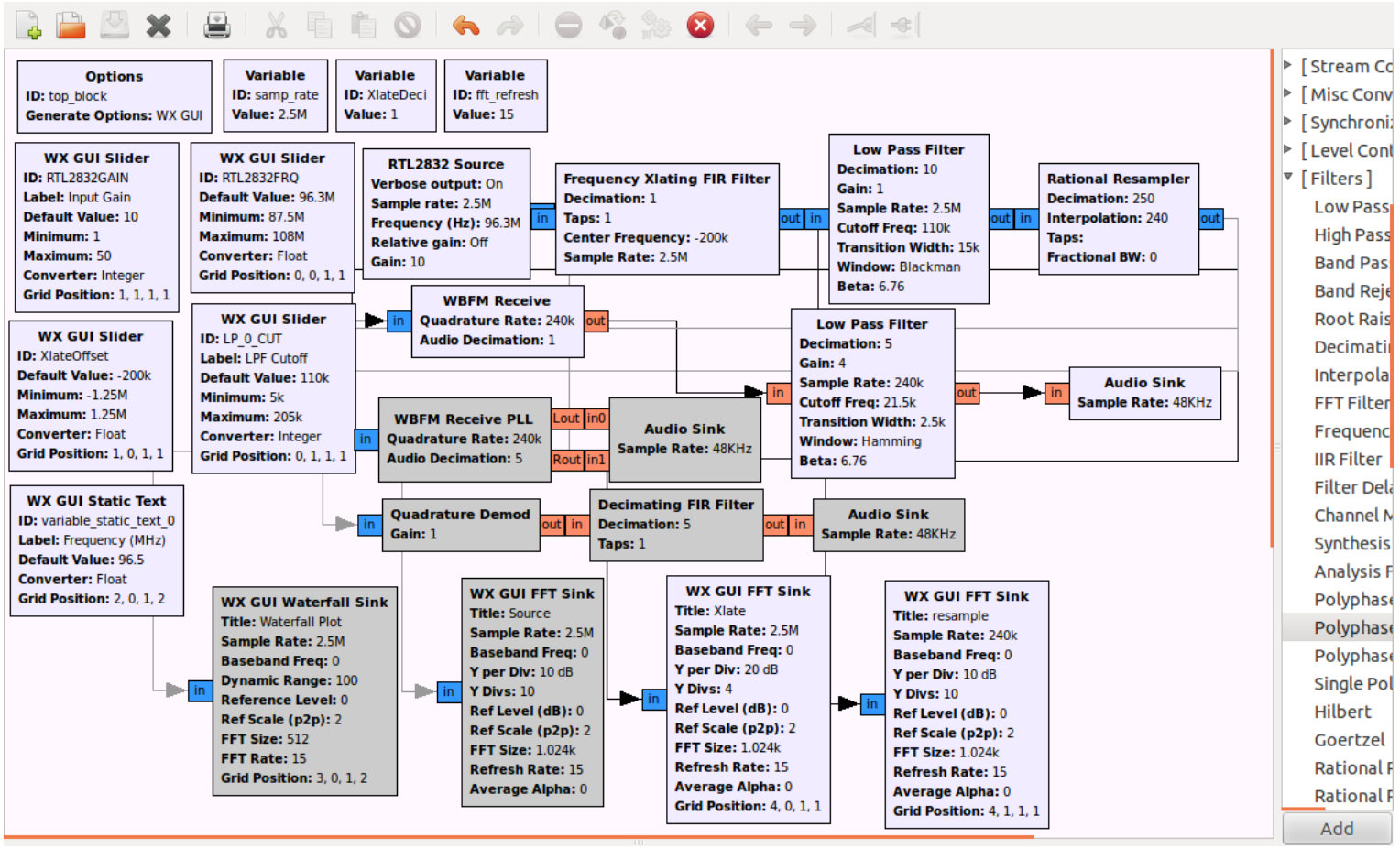
Tools ?


Gqrx v2.1-git-298-g0e78 - rtl=0
File
Data
View
Help
104.903 100 MHz
-8 dBFS
Receiver Options
203.100 kHz
Hardware freq: 104.700000 MHz
Filter
Normal
Mode
Wide FM (stereo)
AGC
Fast
NB1
NB2
SQL
-150 dBFS
Input controls
Receiver Options
Audio
Gain:
-20 dB
FFT Settings
Audio

Tools ?


Multimode Radio Receiver
Main Controls
Scan/Upconv Controls
Volume: 3.61
Frequency: 476.587M
Fine Tuning: 5k
Extra Fine Tuning: 0
Mode: NFM1 (5.0kHz)
RF Level: -12.5
Mute Threshold: -10
AM/SSB Bandwidth: 2.61k
LO Offset: 50k
Spectral Zoom Ratio: 1
Actual srate: 1
AGC
RF Gain: 42.5
Record
Recording Filename: recording.wav
Spectrogram
Time (s)
Frequency (MHz)
Options
Average
Avg Alpha: 0.5000
Axes Options
Time Scale:
Dyn Range:
Ref Level:
Color: RGB1
Autoscale
Clear
Stop
Panorama
FFT
Trace Options
Peak Hold
Average
Avg Alpha: 0.1000
Persistence
Persist Alpha: 0.5439
Trace A
Store

Tools ?


Options
ID: top_block
Generate Options: WX GUI
Variable
ID: samp_rate
Value: 2.5M
Variable
ID: XlateDeci
Value: 1
Variable
ID: fft_refresh
Value: 15
WX GUI Slider
ID: RTL2832GAIN
Label: Input Gain
Default Value: 10
Minimum: 1
Maximum: 50
Converter: Integer
Grid Position: 1, 1, 1, 1
WX GUI Slider
ID: RTL2832FRQ
Default Value: 96.3M
Minimum: 87.5M
Maximum: 108M
Converter: Float
Grid Position: 0, 0, 1, 1
RTL2832 Source
Verbose output: On
Sample rate: 2.5M
Frequency (Hz): 96.3M
Relative gain: Off
Gain: 10
Frequency Xlating FIR Filter
Decimation: 1
Taps: 1
Center Frequency: -200k
Sample Rate: 2.5M
Low Pass Filter
Decimation: 10
Gain: 1
Sample Rate: 2.5M
Cutoff Freq: 110k
Transition Width: 15k
Window: Blackman
Beta: 6.76
Rational Resampler
Decimation: 250
Interpolation: 240
Taps:
Fractional BW: 0
WBFM Receive
Quadrature Rate: 240k
Audio Decimation: 1
WX GUI Slider
ID: XlateOffset
Default Value: -200k
Minimum: -1.25M
Maximum: 1.25M
Converter: Float
Grid Position: 1, 0, 1, 1
WX GUI Slider
ID: LP_0_CUT
Label: LPF Cutoff
Default Value: 110k
Minimum: 5k
Maximum: 205k
Converter: Integer
Grid Position: 0, 1, 1, 1
Low Pass Filter
Decimation: 5
Gain: 4
Sample Rate: 240k
Cutoff Freq: 21.5k
Transition Width: 2.5k
Window: Hamming
Beta: 6.76
Audio Sink
Sample Rate: 48KHz
WBFM Receive PLL
Quadrature Rate: 240k
Audio Decimation: 5
Audio Sink
Sample Rate: 48KHz
WX GUI Static Text
ID: variable_static_text_0
Label: Frequency (MHz)
Default Value: 96.5
Converter: Float
Grid Position: 2, 0, 1, 2
Quadrature Demod
Gain: 1
Decimating FIR Filter
Decimation: 5
Taps: 1
Audio Sink
Sample Rate: 48KHz
WX GUI Waterfall Sink
Title: Waterfall Plot
Sample Rate: 2.5M
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 0
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 15
Grid Position: 3, 0, 1, 2
WX GUI FFT Sink
Title: Source
Sample Rate: 2.5M
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Average Alpha: 0
WX GUI FFT Sink
Title: Xlate
Sample Rate: 2.5M
Baseband Freq: 0
Y per Div: 20 dB
Y Divs: 4
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Average Alpha: 0
Grid Position: 4, 0, 1, 1
WX GUI FFT Sink
Title: resample
Sample Rate: 240k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Average Alpha: 0
Grid Position: 4, 1, 1, 1
[Stream Co
[Misc Conv
[Synchroni
[Level Cont
[Filters]
Low Pass
High Pass
Band Pas
Band Reje
Root Rais
Decimati
Interpola
FFT Filter
Frequenc
IIR Filter
Filter Del
Channel M
Synthesis
Analysis F
Polyphase
Polyphase
Polyphase
Single Pol
Hilbert
Goertzel
Rational R
Rational R
Add

Entendre quoi ?

- Cool, et y'a quoi que je peux entendre ?

Entendre quoi ?

- Cool, et y'a quoi que je peux entendre ?
  - Radio comerciales

Entendre quoi ?

- Cool, et y'a quoi que je peux entendre ?
  - Radio comerciales
  - Radio amateurs

Entendre quoi ?

- Cool, et y'a quoi que je peux entendre ?
  - Radio comerciales
  - Radio amateurs
  - Talkie walkie

Entendre quoi ?

- Cool, et y'a quoi que je peux entendre ?
  - Radio comerciales
  - Radio amateurs
  - Talkie walkie
  - Casque sans fil

Entendre quoi ?

- Cool, et y'a quoi que je peux entendre ?
  - Radio comerciales
  - Radio amateurs
  - Talkie walkie
  - Casque sans fil
  - Baby phone

Entendre quoi ?

- Cool, et y'a quoi que je peux entendre ?
  - Radio comerciales
  - Radio amateurs
  - Talkie walkie
  - Casque sans fil
  - Baby phone
  - Taxis

Entendre quoi ?

- Cool, et y'a quoi que je peux entendre ?
  - Radio comerciales
  - Radio amateurs
  - Talkie walkie
  - Casque sans fil
  - Baby phone
  - Taxis
  - Pilote d'avion

Entendre quoi ?

- Cool, et y'a quoi que je peux entendre ?
  - Radio comerciales
  - Radio amateurs
  - Talkie walkie
  - Casque sans fil
  - Baby phone
  - Taxis
  - Pilote d'avion
  - Micro sans fil

Entendre quoi ?

- Cool, et y'a quoi que je peux entendre ?
  - Radio comerciales
  - Radio amateurs
  - Talkie walkie
  - Casque sans fil
  - Baby phone
  - Taxis
  - Pilote d'avion
  - Micro sans fil
  - ...

Autres signaux ?

- Et en data y'a quoi ?
  - GSM
  - GPS
  - ACARS
  - ADS-B
  - POCSAG
  - TETRA
  - NOAA
  - Clé de voiture, clé portail, jouet téléguidé, station météo, feux tricolores temporaires, rfid, affichage arret de bus...

Partie _ _ _ _ _ _ _ |¯| _

Listen

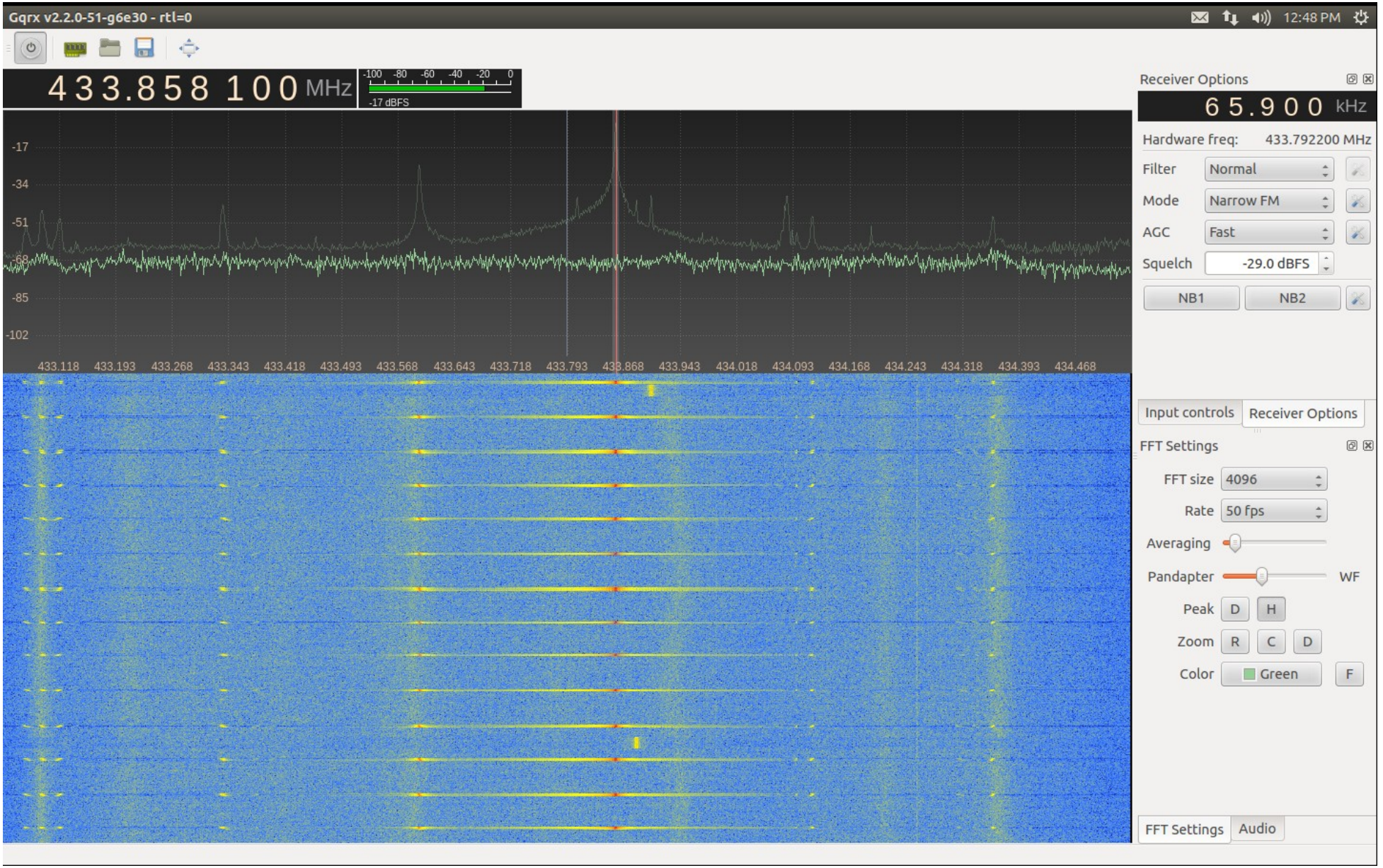
Partie _ _ _ _ _ _ |¯ ¯|

Reverse

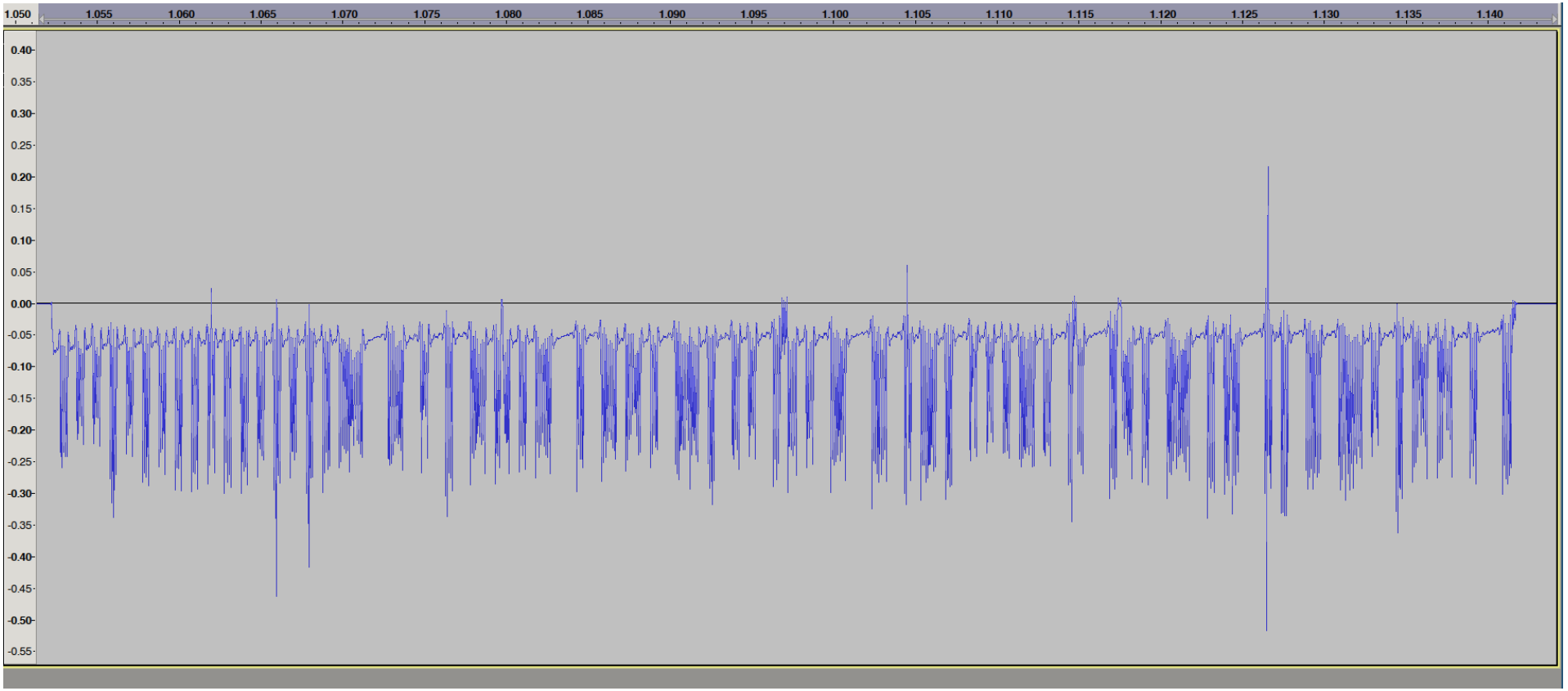
Message connu

```
#include <VirtualWire.h>

const int led_pin = 13;
const int transmit_pin = 12;

const char *msg = "rootcamp";
size_t len = strlen(msg);

void setup()
{
    vw_set_tx_pin(transmit_pin);
    vw_set_ptt_inverted(true);
    vw_setup(2000);
    pinMode(led_pin, OUTPUT);
}

void loop()
{
  digitalWrite(led_pin, HIGH);

  vw_send((uint8_t*)msg, len);
  vw_wait_tx();

  digitalWrite(led_pin, LOW);

  delay(1000);
}
```

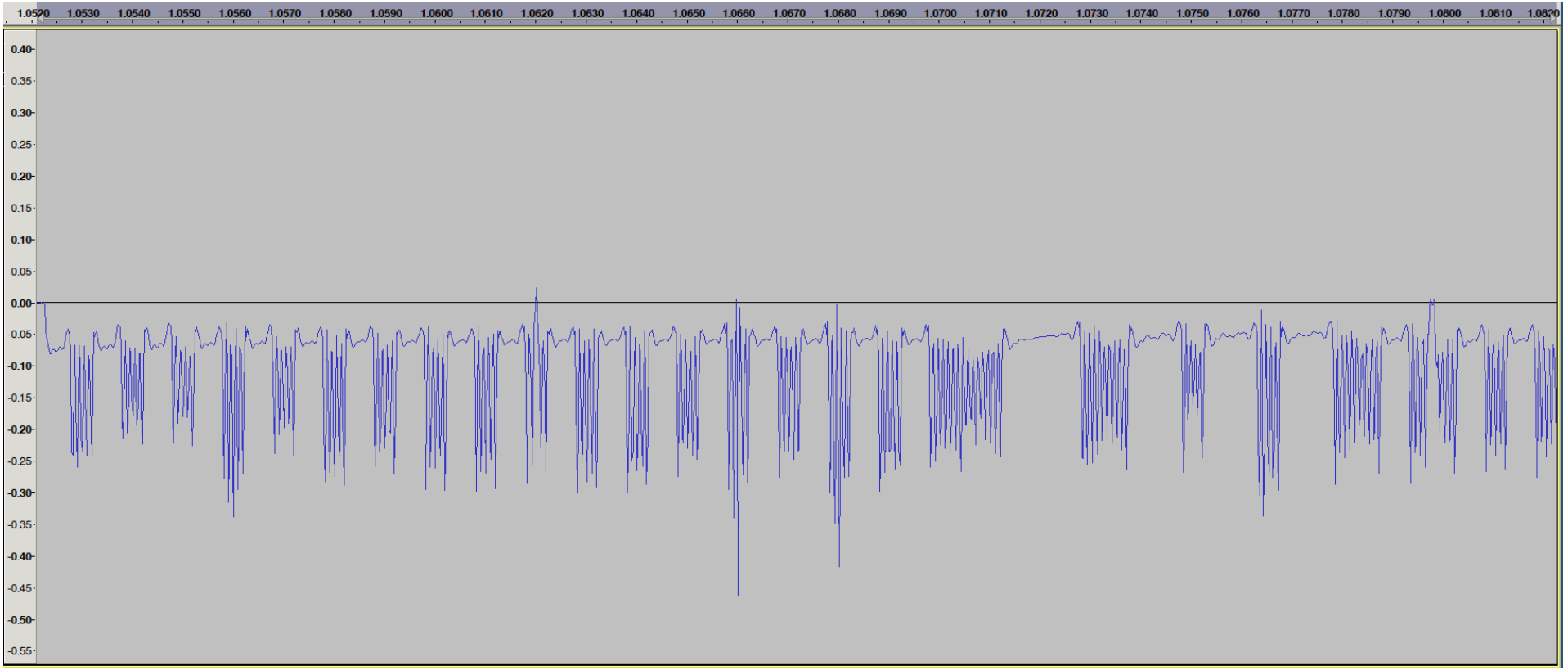
Message connu



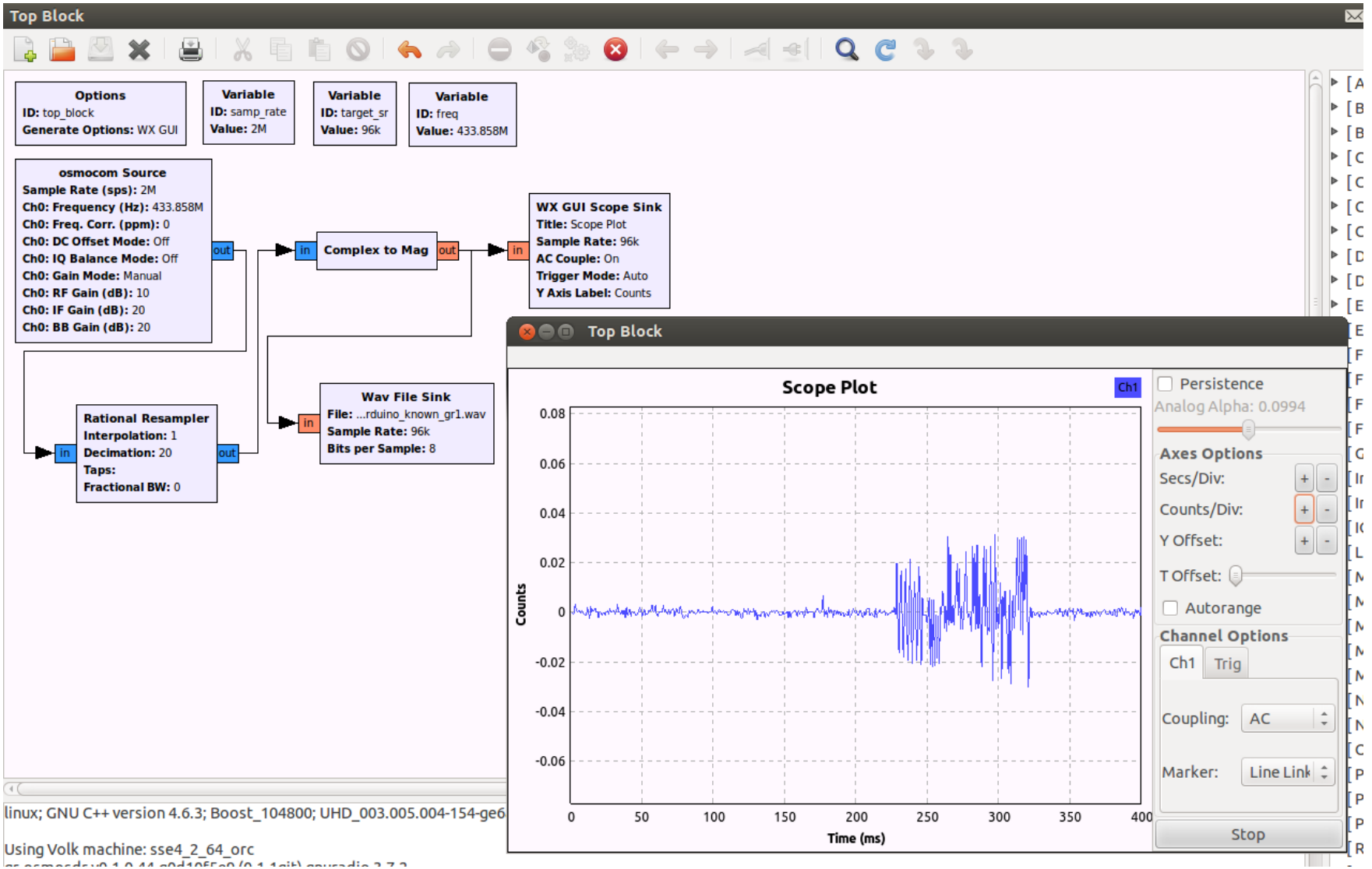
Message connu



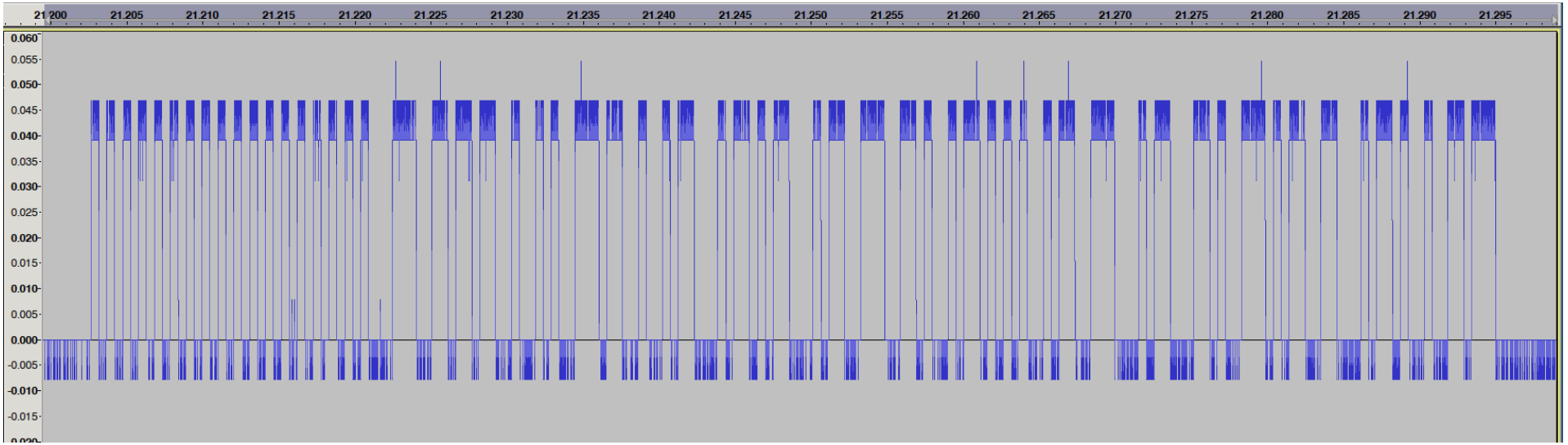
Message connu



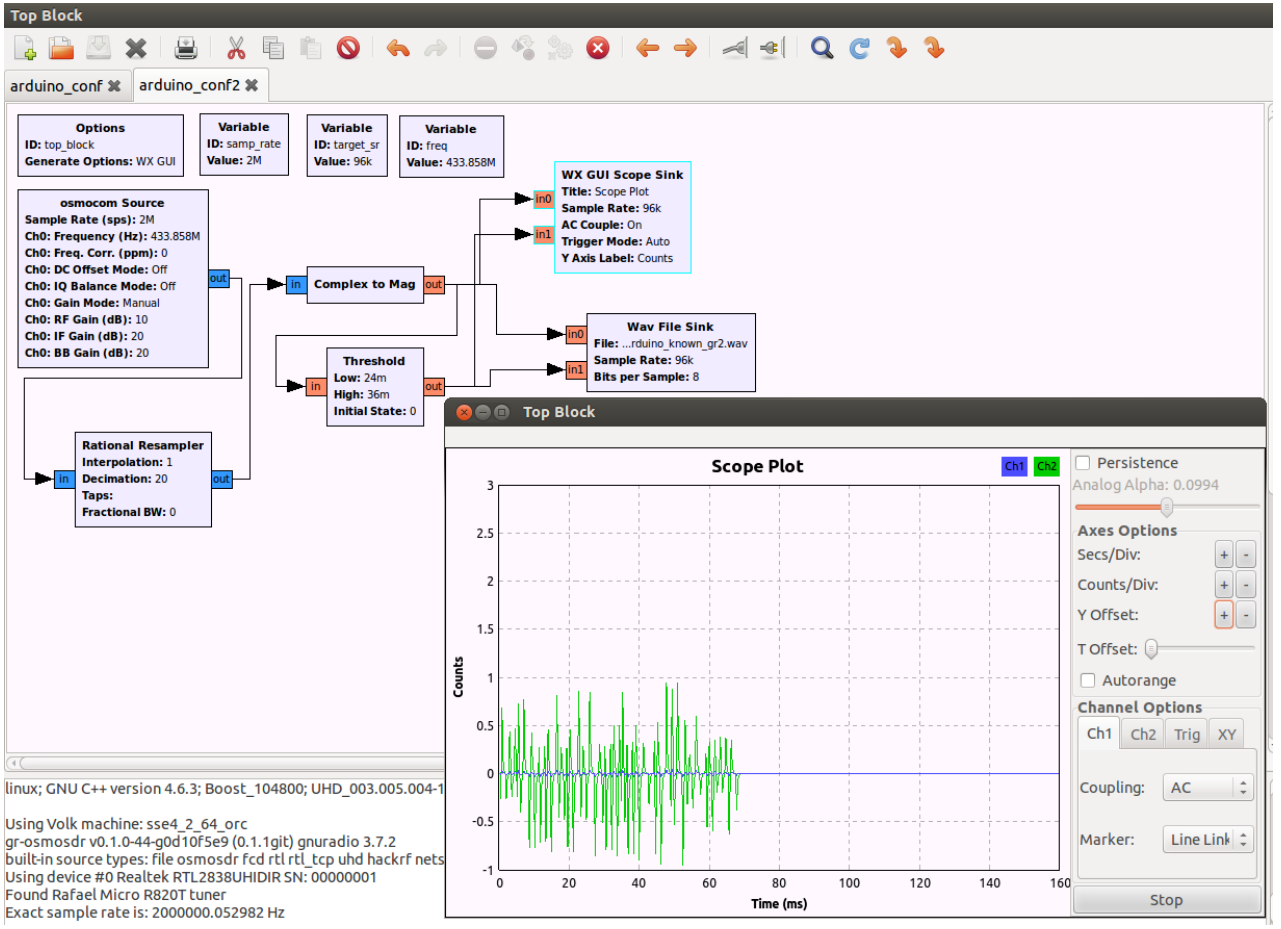
Message connu



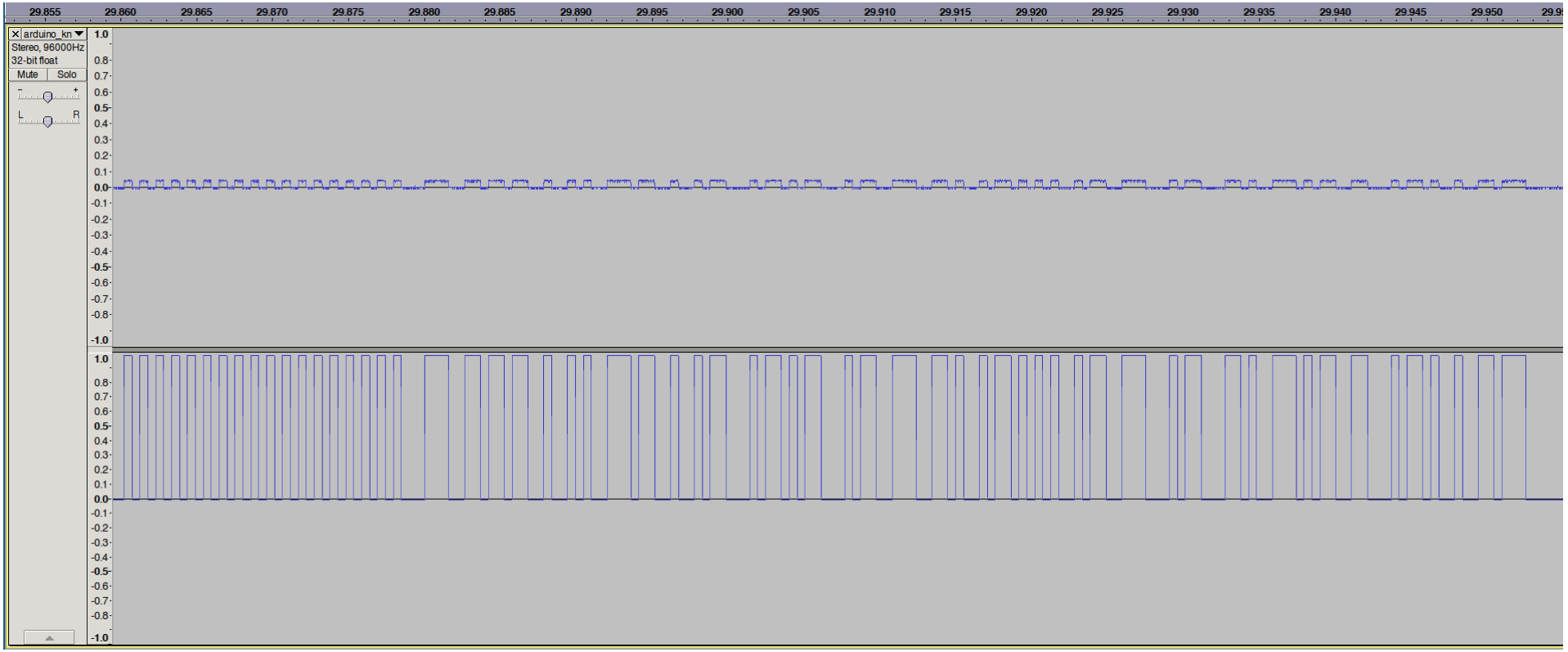
Message connu



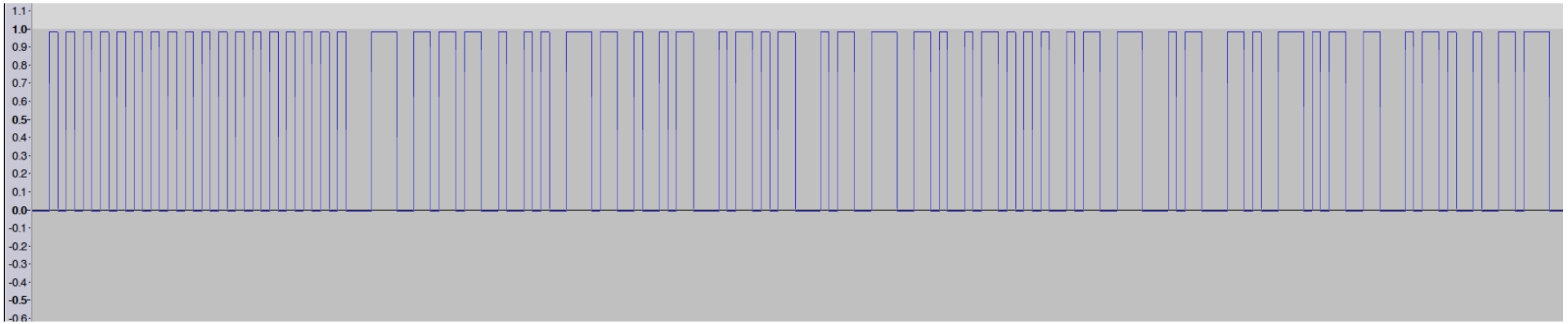
Message connu



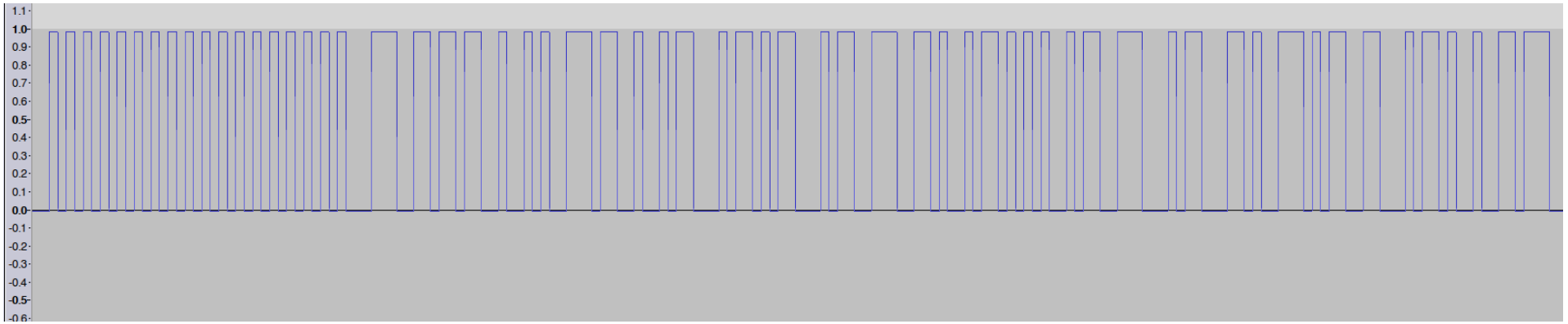
Message connu



Message connu



Message connu



10101010101010101010101010101010101000111001101101100100101001110110010010110001011010110001011001110011010010110101010010110011100010110001101001110101100110001011010010011011100000

Message connu

```
35 static uint8_t vw_tx_buf[(VW_MAX_MESSAGE_LEN * 2) + VW_HEADER_LEN]
36       = {0x2a, 0x2a, 0x2a, 0x2a, 0x2a, 0x2a, 0x38, 0x2c};
37
```

Message connu

```
113 // 4 bit to 6 bit symbol converter table
114 // Used to convert the high and low nybbles of the transmitted data
115 // into 6 bit symbols for transmission. Each 6-bit symbol has 3 1s and 3 0s
116 // with at most 3 consecutive identical bits
117 static uint8_t symbols[] =
118 {
119     0xd,  0xe,  0x13, 0x15, 0x16, 0x19, 0x1a, 0x1c,
120     0x23, 0x25, 0x26, 0x29, 0x2a, 0x2c, 0x32, 0x34
121 };
```

Message connu

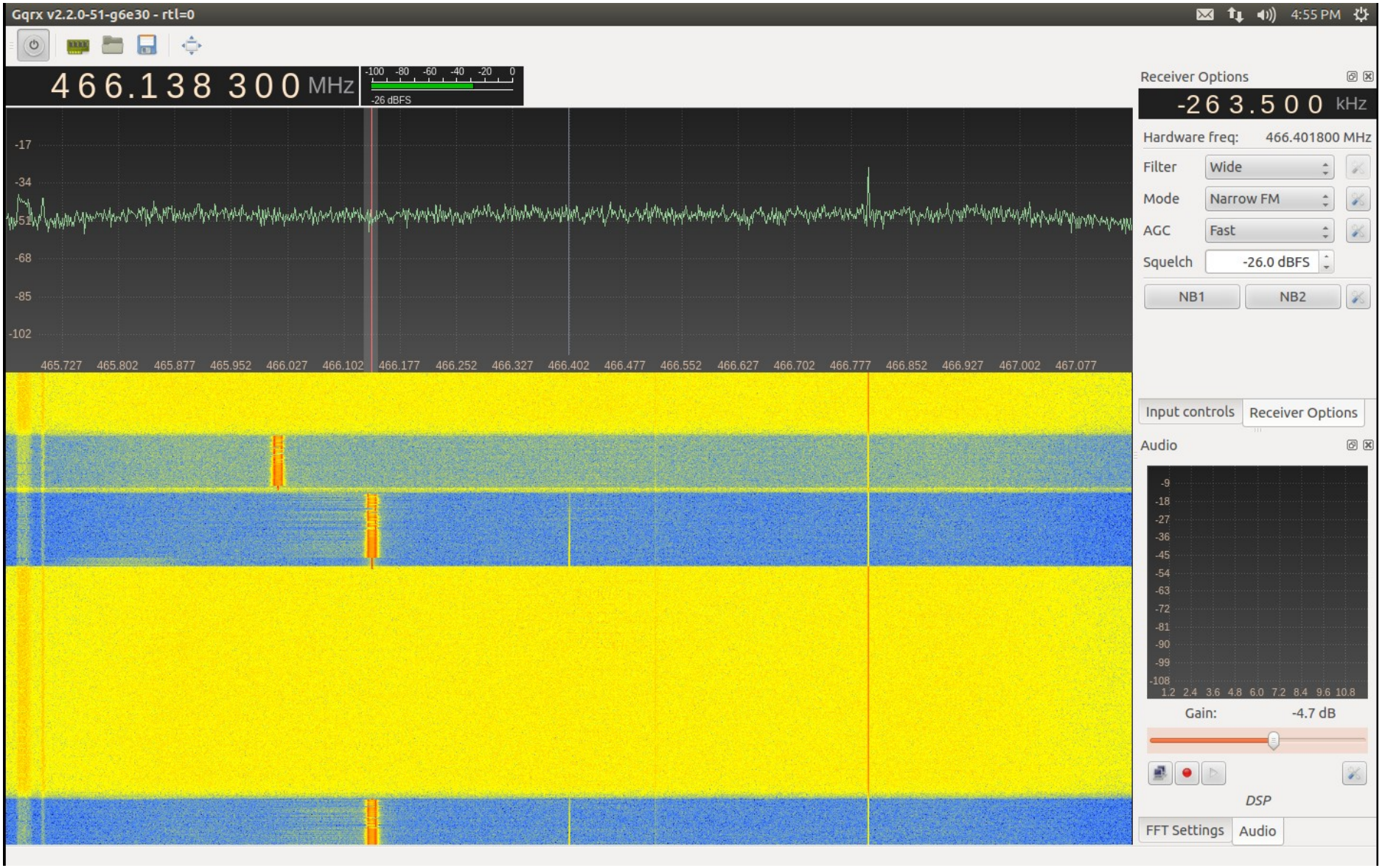
```
519     // Encode the message into 6 bit symbols. Each byte is converted into
520     // 2 6-bit symbols, high nybble first, low nybble second
521     for (i = 0; i < len; i++)
522     {
523         crc = _crc_ccitt_update(crc, buf[i]);
524         p[index++] = symbols[buf[i] >> 4];
525         p[index++] = symbols[buf[i] & 0xf];
526     }
```

Message connu

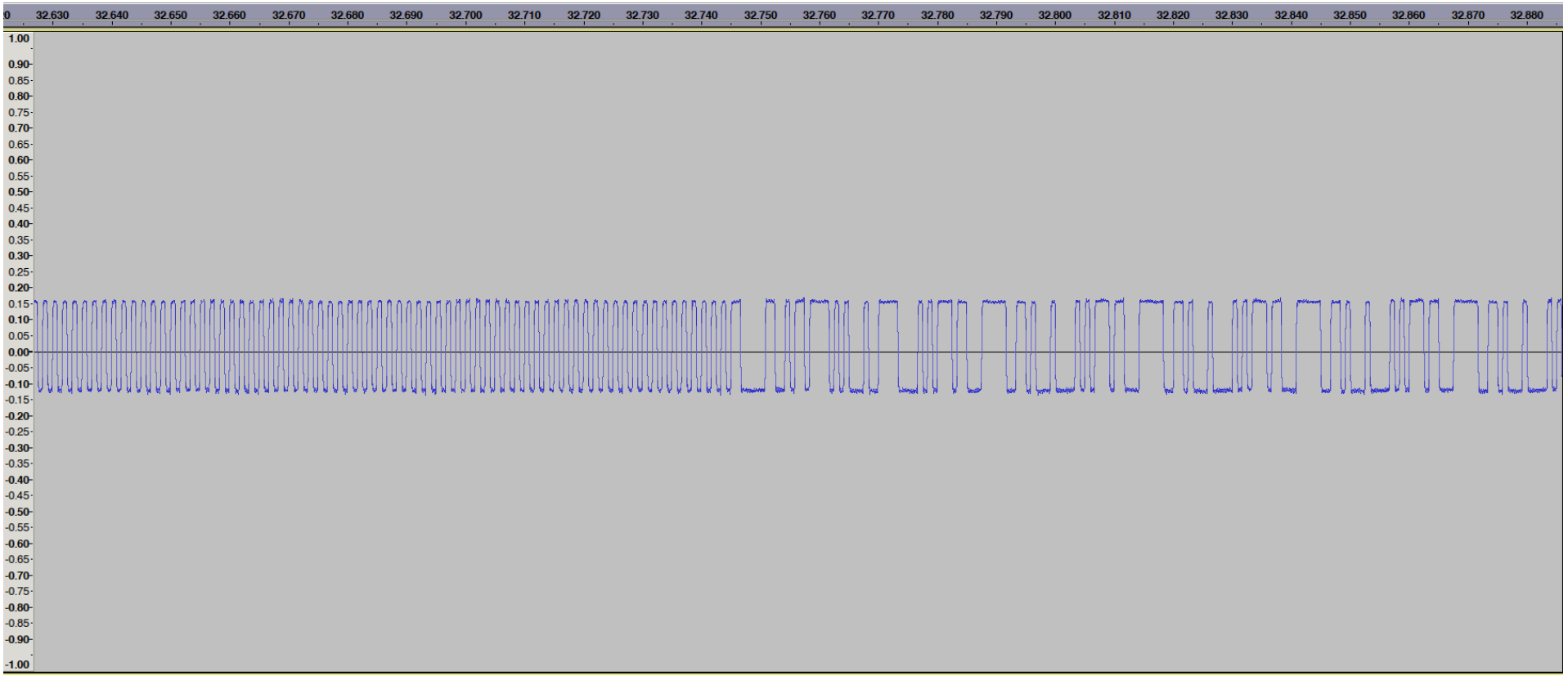
Total message len: 11
Checksum : 0x84e1
Message: 'rootcamp'

\o/

Message inconnu



Message inconnu



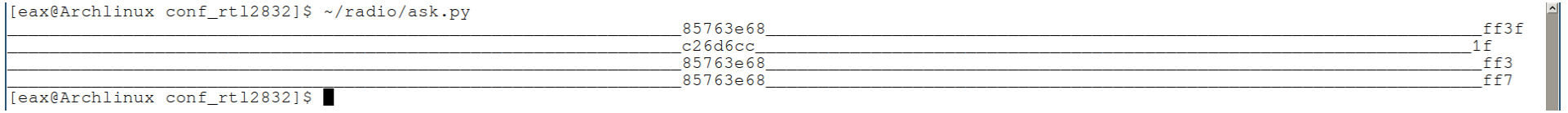
Message inconnu

```
[eax@Archlinux conf_rtl2832]$ ~/radio/ask.py
832dea2785763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e68c26d06cc85763e68832dea2785
763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e68ff3f
[eax@Archlinux conf_rtl2832]$
```

Message inconnu

```
[eax@Archlinux conf_rtl2832]$ ~/radio/ask.py
_____________________________________85763e6885763e6885763e6885763e6885763e68c26d6cc85763e68____85763e6885763e6885763e6885763e6885763e68857
63e6885763e6885763e6885763e6885763e6885763e68_____________ff3f
_____________________________________fa523295a5cff3ff6a5a634aad632cd47a1251acc74739f19f6152c4155d____398bf0aa7efdfcc13f7ebd6a6ccfabf8526fadff1971a2
4b34f870f42e35f6e157467bf57b32ea66ddbf6517ffff896_____________832dea2785763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e6885763e688
5763e6885763e6885763e6885763e6885763e6885763e68ff3f
_____________________________________85763e6885763e6885763e6885763e6885763e68c26d6cc85763e68____85763e6885763e6885763e6885763e6885763e68857
63e6885763e6885763e6885763e6885763e6885763e68_____________ff3f
_____________________________________85763e6885763e6885763e6885763e68c26d6ccc26d6cc____85763e6885763e6885763e6885763e6885763e688576
3e6885763e6885763e6885763e6885763e6885763e68_____________1f
_____________________________________85763e6885763e6885763e6885763e6885763e68c26d6cc85763e68____85763e6885763e6885763e6885763e6885763e68857
63e6885763e6885763e6885763e6885763e6885763e68_____________ff3
_____________________________________85763e6885763e6885763e6885763e68c26d6cc85763e68____85763e6885763e6885763e6885763e6885763e68857
63e6885763e6885763e6885763e6885763e6885763e68_____________ff7
[eax@Archlinux conf_rtl2832]$
```

Message inconnu



:(

Partie _ _ _ _ _ |¯| _ _

Give me more !

Gimemore

- Decryptage GSM
  - http://domonkos.tomcsanyi.net/?p=418
- Blog sur le SDR
  - http://www.rtl-sdr.com/
- Créer un block gnuradio
  - http://gnuradio.org/redmine/projects/gnuradio/wiki/OutOfTreeModules

Gimemore

- All Your RFz Are Belong to Me - Hacking the Wireless World with Software Defined Radio
  - https://www.youtube.com/watch?v=1bgC3AjCnA4
- Noise Floor: Exploring the world of unintentional radio emissions
  - https://www.youtube.com/watch?v=5N1C3WB8c0o
- Hacking with GNURadio
  - https://www.youtube.com/watch?v=c5Vu-056tyY
- Air Traffic Control: Insecurity and ADS-B
  - https://www.youtube.com/watch?v=0YHegoXi_IY
- My journey into FM-RDS
  - https://www.youtube.com/watch?v=R-2k6TMPMRo

Partie _ _ _ _ _ |¯| _ |¯|

Question ?