SDR Radio Dongles

A flexible tool for exploring the RF environment around us!

Grant Hopper

KB7WSD

2017 MicroHams Digital Conference

Introduction

- The advent of:
  - compact, plentiful, and cheap computing power
  - cheap semiconductor manufacturing,
  - And the human spirit for innovation and exploration
- RTL2832U, DVB-T SDR, RTL dongle, SDR dongle, “that USB thing”….

Receive TV and Radio in areas where DVB and DAB are present.
Receive amateur television transmissions.
Listening to unencrypted Police/Ambulance/Fire/EMS conversations.
Listening to aircraft traffic control conversations.
Tracking aircraft positions like a radar with ADS-B decoding.
Decoding aircraft ACARS short messages.
Scanning trunking radio conversations.
Decoding unencrypted digital voice transmissions.
Tracking ship movement with AIS decoding.
Decoding POCSAG/FLEX pager traffic.
Scanning for cordless phones and baby monitors.
Tracking and receiving meteorological agency launched weather balloon data.
Receiving HF weatherfax.
Receiving NOAA weather satellite images.
Monitor amateur frequencies
APRS Rx Gateway
Noise Sniffer

Tracking your own self launched high altitude balloon for payload recovery.
Receiving wireless temperature sensors and wireless power meter sensors.
Listening to HF/VHF/UHF/Microwave amateur radio.
Oh, and LF now too!
Decoding APRS data.
Watching Digital Amateur TV.
Sniffing GSM signals.
Using rtl-sdr on your Android device as a portable radio scanner.
Receiving GPS signals and decoding them.
Receiving Inmarsat transmissions
Using rtl-sdr as a spectrum analyzer.
Listening to satellites and the ISS.
Receiving Outernet transmissions
Radio astronomy.
Monitoring meteor scatter.
Decoding satellite message traffic
Cross band repeater

WSPR signal reception.
FUNCube Satellite monitoring.
Listening to FM radio, and decoding RDS information.
Listening to and looking at DAB broadcast radio signals.
Use rtl-sdr as a panadapter for your traditional hardware radio.
Decoding taxi mobile data terminal signals.
Use rtl-sdr as a high quality entropy source for random number generation.
Use rtl-sdr as a noise figure indicator.
Reverse engineering unknown protocols.
Triangulating the source of a signal (RDF).
Searching for RF noise sources.
Characterizing RF filters and measuring antenna SWR.
Decoding digital amateur radio ham communications such as CW/PSK/RTTY/SSTV.
Receiving Digital Radio Monodial shortwave radio (DRM).
Listening to international shortwave radio.
Looking at RADAR signals
Decoding telemetry

Over the horizon (OTH) radar,
HAARP
Detecting Meteor ‘echos’
Monitoring the local RF environment
Detecting and deciphering digital RF transmissions
Decoding keyfob transmissions
Examining DECT transmissions
Glider tracking as part of the Open Glider Network
Examining Rail Road data transmissions
Listening to smart meter transmissions
Detecting wireless doorbell transmissions
Monitoring 2.4GHz wireless video transmissions

…just to start the list

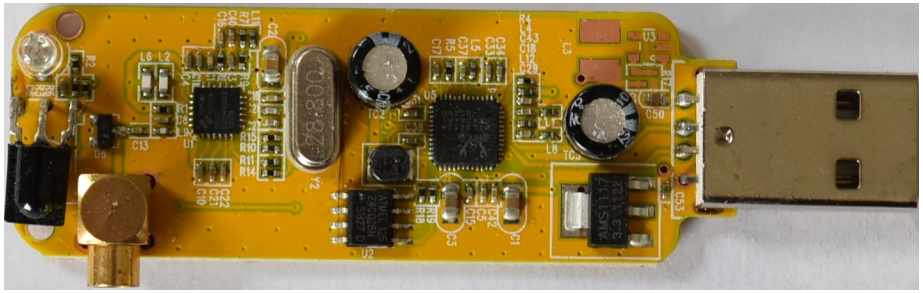
Roadmap for Today

- RTL-SDR dongles: based on Realtek chip
- What it is and how it works: Details about hardware
- Base Configuration(s): Software
- Uses (applications): Examples
- What should I get?
- Not an exhaustive investigation; a survey of the terrain

RTL dongle?

- Often labeled as a “DVB-T (and) DAB (and) FM” receiver on a stick

- Originally designed to receive TV signals: Digital Video Broadcasting — Terrestrial
- Eric Fry & Antti Palosaari get credit for the discovery of what else it can be made to do



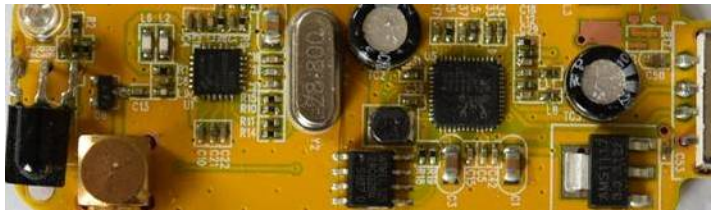
What is it?

- Thumb-size broadband receiver
- Connects via USB port of computer
- Runs on 5V from USB port
- Used for television reception in countries outside of USA
- Adapted for use as a broadband rcvr for hobbyists
- Cheap way to monitor VHF/UHF bands
- Can view 2 MHz wide portion of spectrum
- Requires software
- Many modes supported: AM, FM, USB, LSB, CW (even DRM)
  - depends on software

About the hardware

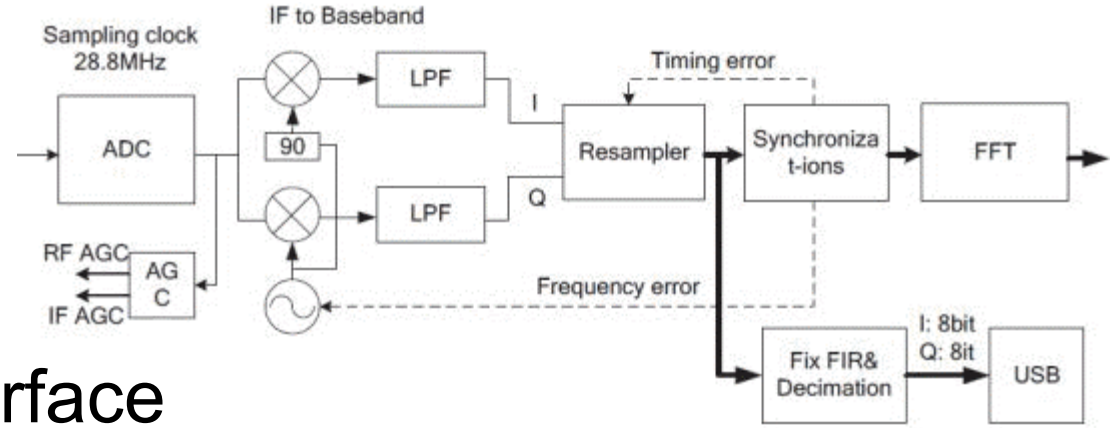
Two parts: USB interface, and Tuner chip

- USB interface: Realtek RTL2832U
- Tuner Chip: Rafael Micro R820T2
  - best for most uses
  - Replaced the R820T
  - E4000*, FC2580, FC0012, FC0013



- “Special” versions with additional improvements such as a TCXO, etc.
- Cheapest versions now run about $7

Realtek RTL2832U



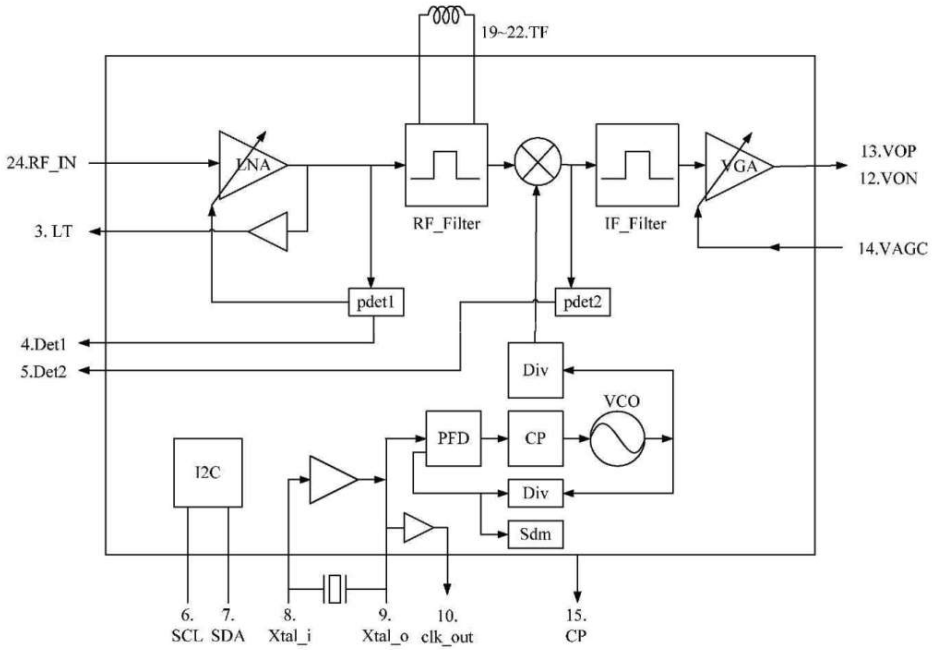
- USB 2.0 interface
- high-performance DVB-T COFDM demodulator.
- supports tuners at IF (Intermediate Frequency, 36.125MHz), low-IF (4.57MHz), or Zero-IF output using a 28.8MHz crystal, and includes FM/DAB/DAB+ Radio Support
- 8-bit ADC for RF signals level measurement
- Eight general purpose I/O ports, plus IR port

Other front-end chips

- Realtek RTL- not only game in town:
- Airspy uses LPC4370 ARM
- SDRPlay uses MSi2500

Rafael Micro R820T2

- Support all digital TV standards: DVB-T, ATSC, DTMB and ISDB-T
- On-chip
  - LNA,
  - mixer,
  - fractional PLL,
  - VGA,
  - LDO



Different/better/other tuner chip specs

- Elonics E4000* 52 - 2200 MHz
  - with a gap from 1100 MHz to 1250 MHz (varies)
- Rafael Micro R820T 24 - 1766 MHz
- Rafael Micro R820T2 24 - 1766 MHz (New, lower noise)
- Rafael Micro R828D 24 - 1766 MHz (no improvement)
- Fitipower FC0013 22 - 1100 MHz
  - (FC0013B/C, FC0013G has a separate L-band input, which is unconnected on most sticks)
- Fitipower FC0012 22 - 948.6 MHz
- FCI FC2580 146 - 308 MHz and 438 - 924 MHz
  - (gap in between)

* Elonics has closed and ceased chip production

- Source: http://osmocom.org/projects/sdr/wiki/rtl-sdr

Tuner chips in Market

- Rafael Micro R820T (24 - 1766 MHz)
- R820T2 (same as R820T, but better sensitivity and lower noise)
- Elonics E4000* (52 - 2200 MHz with a gap from 1100 MHz to 1250 MHz)
- FCI FC2580 (46 – 308 MHz, 438 – 924 MHz)
- Fitipower FC0012 & FC0013 (22 – 948.6 MHz and 1100 MHz respectively)
- *Elonics has closed and ceased chip production

RTL dongle specs

- Coverage range: 24MHz to 1700MHz
- ADC resolution 8 bits
- Bandwidth:
  - generally 2.4 MHz w/o loss
  - theoretical 3.2 MHz
- outputs 8-bit I/Q-samples
  - 3.2 MS/s theoretical sample rate
  - highest sample-rate without lost samples that has been tested so far is 2.8 MS/s
- USB 2.0* (this is NOT a limiting factor in device performance)
- 75 ohm impedance at antenna port

Examples of products in market

Comparisons with other common Wideband Commercial Software Defined Radios*

SDR	Tune Low (MHz)	Tune Max (MHz)	RX Bandwidth (MHz)	ADC Resolution (Bits)	Transmit? (Yes/No)	Price ($USD)
RTL-SDR (R820T)	24	1766	3.2	8	No	~20
Funcube Pro+	0.15 410	260 2050	0.192	16	No	~200
Airspy	24	1800	10	12	No	199
SDRPlay	0.1	2000	8	12	No	149
HackRF	30	6000	20	8	Yes	299
BladeRF	300	3800	40	12	Yes	400 & 650
USRP 1	DC	6000	64	12	Yes	700

Source: http://www.rtl-sdr.com/about-rtl-sdr/

Hardware ‘features’

- Direct sampling. Allows operation down in HF spectrum with modest performance hit (vs downconverter) and modest risk of hardware damage
- Bias Tee power
- TCXO (0.5 PPM stability)
- Headers for advanced uses
- Lives up to its name

Other hardware

- Typical applications require a PC running Windows, (MAC), or Linux with a decent CPU speed.
- Second hand CPUs, Raspberry Pi
- Antenna(s), feedline
- Up and down converters, Low Noise Amplifiers, and filters

Open Source devices that Tx

- YARD Stick One, Great Scott Gadgets:

- Hack RF: uses MAX5864, RFFC5071, no RTL2832U or R802T2 in hardware
- LimeSDR:
- Apache:

YARD Stick One
Great Scott Gadgets

- Based on:
- half-duplex transmit and receive
- official operating frequencies: 300-348 MHz, 391-464 MHz, and 782-928 MHz
- unofficial operating frequencies: 281-361 MHz, 378-481 MHz, and 749-962 MHz
- modulations: ASK, OOK, GFSK, 2-FSK, 4-FSK, MSK
- data rates up to 500 kbps
- Full-Speed USB 2.0
- Open-source

Hack RF

- MAX5864, RFFC5071

LimeSDR

Operational considerations

- Usable range less than specified range:
  - R802T oscillates above 1.5 GHz
  - R802T2 better and ok up to nearly 1.7 GHz
- Up and down converters are the order of the day for use below 30MHz and above 1.5 (or so) GHz.
- Direct sampling:
  - Older devices required modification
  - RTL-SDR.COM V3 software selectable mode

Sources of error in the received frequency

- There are two primary sources. The first is the offset error due to the use of not so accurate frequency crystals. The second is due to thermal changes.
  - Frequency offset
  - Thermal drift
- Just let it warm up and don't shut it off
- Software solutions
  - Set correction factor for offset (in ppm)
  - Some software will assist in calibration

Setting up your system

- Hardware
  - Data processing device (computer)
  - SDR device
- Software
  - Manage the dongle
  - Do the magic
  - Display the results
- Several base programs that run dongle and interface to the rest of the system

Software that will interface RTL dongle

- SDR#
- HDSDR
- GNURadio
- SDR-console (from SDR-Radio.com)
- SDRUNO (primarily for SDRPlay hardware, but (currently) compatible with RTL dongles)
- Many other programs, including specialty
  - Some rely on installation of SDR#, others on specific .dll installation (some need both!)

Core Software

- Core program: SDR#
  - Plugins
  - Applications
  - Configuration of RTL-SDR dongle
  - May run in background, or not at all
- Application Program(s)
  - Decoding function(s)
  - Device management
  - May interface with other software

Setting up software

- The drivers installed by the operating system itself are for the DVB-T function
  - This is a waste of time
- First step is replacing supplied driver with WinUSB
  - This is the driver that supports libusb interface which rtlsdr.dll uses to interface with the hardware.

Helper programs

- Audio piping
  - Virtual Audio Cable (VAC) (demo and paid)
  - VB-Audio Cable (Donationware)
  - Virtual Audio Capture Device (free)
  - Jack Audio (Win, Mac, Linux)
  - SoundFlower (Mac OS X 10.2)
  - VSound (Linux)

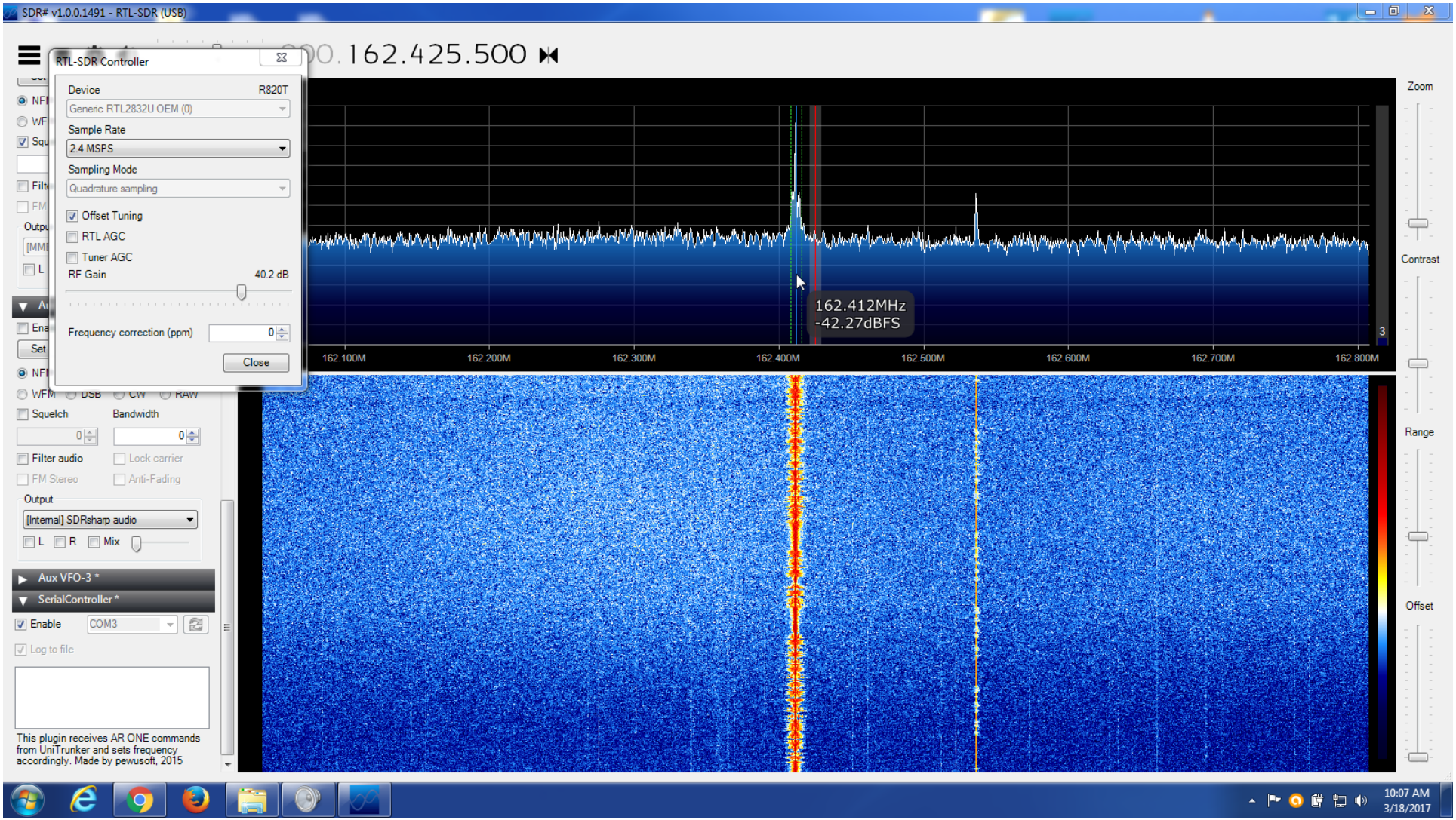
Helper programs

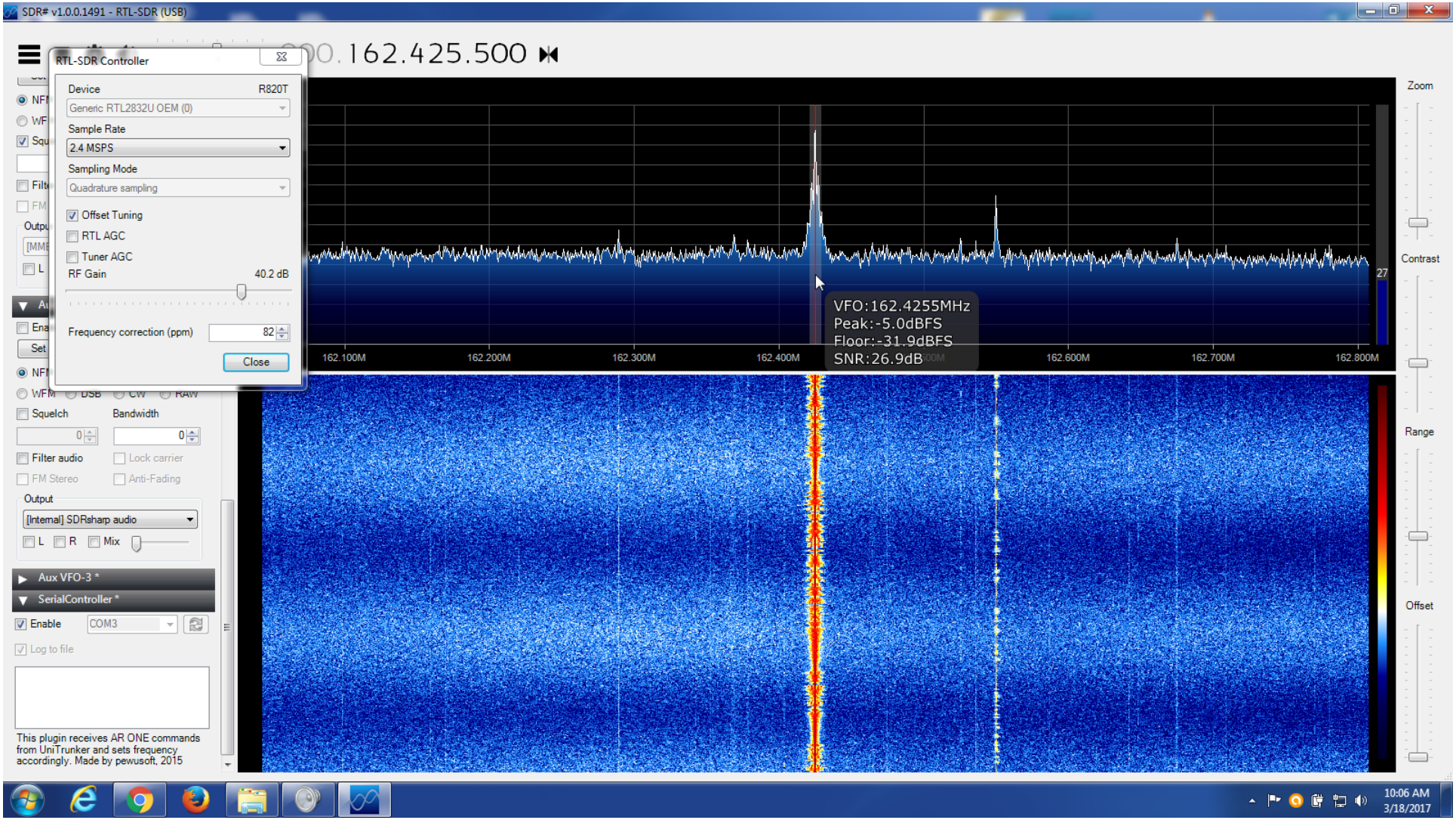
- Control signal piping
  - com0com
  - Virtual Serial Port Driver (VSPD)
  - Free Virtual Serial Ports
  - HW VSP3 (redirects to TCP

Setting up SDR#

- Download and Install SDR#
- Manual install of WinUSB using Zadig if necessary
- Start SDR# and adjust RF gain. A setting of zero will be ‘quiet’ ☺
- Tune to strong local signal (I used NOAA weather radio) to determine frequency offset
- For a nice illustrated guide, refer to: http://www.rtl-sdr.com/rtl-sdr-quick-start-guide/

Adjusting offset




SDR# v1.0.0.1491 - RTL-SDR (USB)
162.425.500
RTL-SDR Controller
Device
R820T
Generic RTL2832U OEM (0)
Sample Rate
2.4 MSPS
Sampling Mode
Quadrature sampling
Offset Tuning
RTL AGC
Tuner AGC
RF Gain
40.2 dB
Frequency correction (ppm)
82
Close
VFO:162.4255MHz
Peak:-5.0dBFS
Floor:-31.9dBFS
SNR:26.9dB
162.100M
162.200M
162.300M
162.400M
162.600M
162.700M
162.800M
Zoom
Contrast
Range
Offset
Squelch
Bandwidth
Filter audio
Lock carrier
FM Stereo
Anti-Fading
Output
[Internal] SDRsharp audio
Aux VFO-3 *
SerialController *
Enable
COM3
Log to file
This plugin receives AR ONE commands from UniTrunker and sets frequency accordingly. Made by pewusoft, 2015
10:06 AM
3/18/2017

Radio Receiver

- Boring?
- Ha! For $7 per receiver…
  - Ancillary costs all relate to convenience and performance
- All the basic programs can perform this function without any additional software
- Driver available for SDR# that allows the setup of multiple VFOs
  - Then you can pipe audio to different outputs if you use VAC

Scanner

- Conventional scanner programs
- Trunked systems can be monitored via a single dongle IF the bandwidth of the dongle will allow for monitoring the control channel AND the voice channel
  - Otherwise two dongles are needed: one for the control channel, the other for voice following
- Several programs. Some can download system data from internet sources.

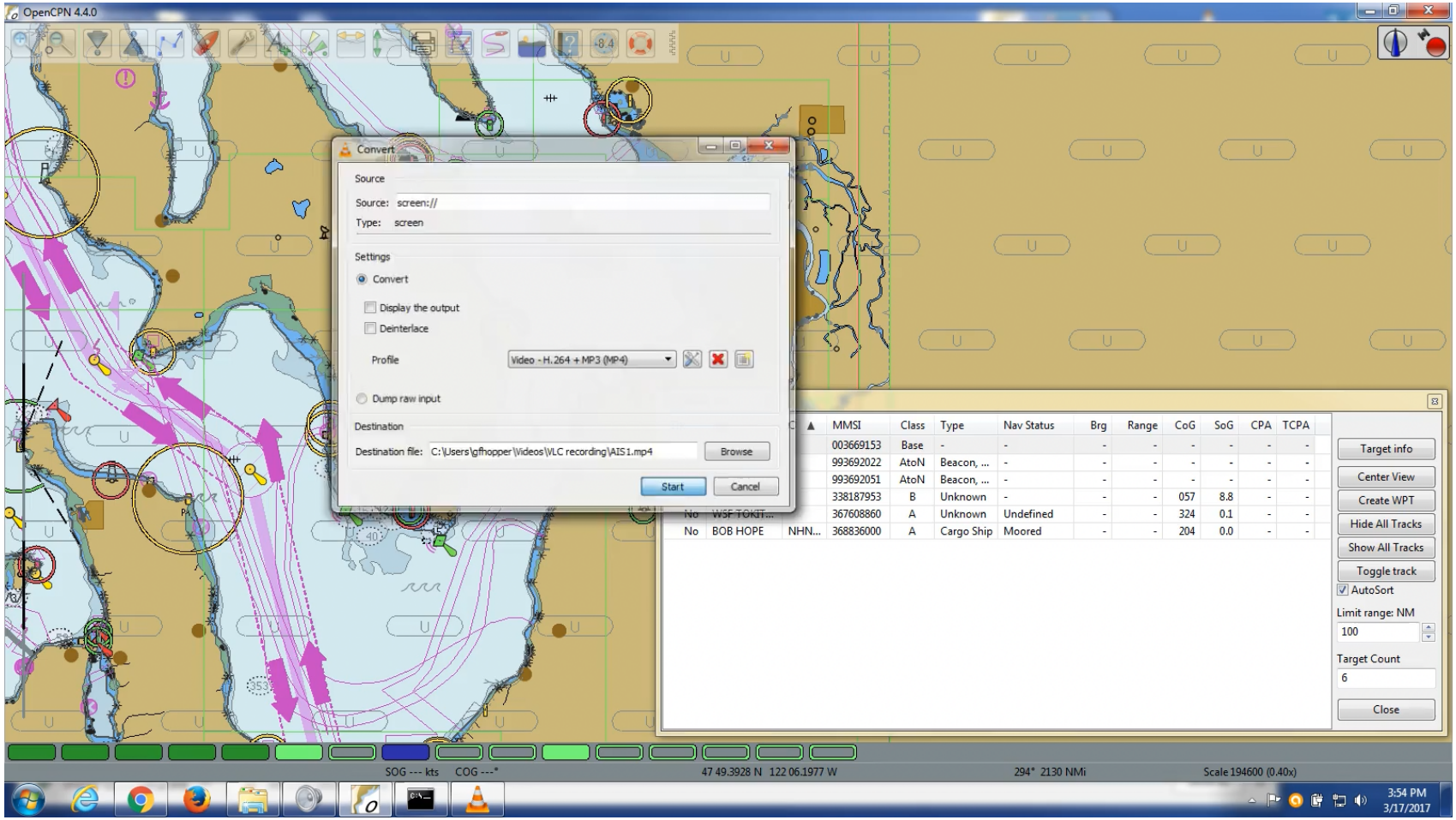
Planes, Trains, and Automobiles (and ships)

- ADS-B
- APRS
- AIS, AIS-S
- Monitoring of TED, FRED, and decoding of Train Control Systems such as PCS (PTCS), ITCS
- APRS
- Other systems exist

AIS

- Automated Identification System (AIS): a maritime automatic tracking system used for collision avoidance.
- Two primary Marine VHF frequencies: CH 77 and 78
- Data bursts from shipboard transmitters
- Nominally a LOS service. S-AIS is satellite received AIS data, usually available from paid services.

AIS Software AISDeco2



ADS-B

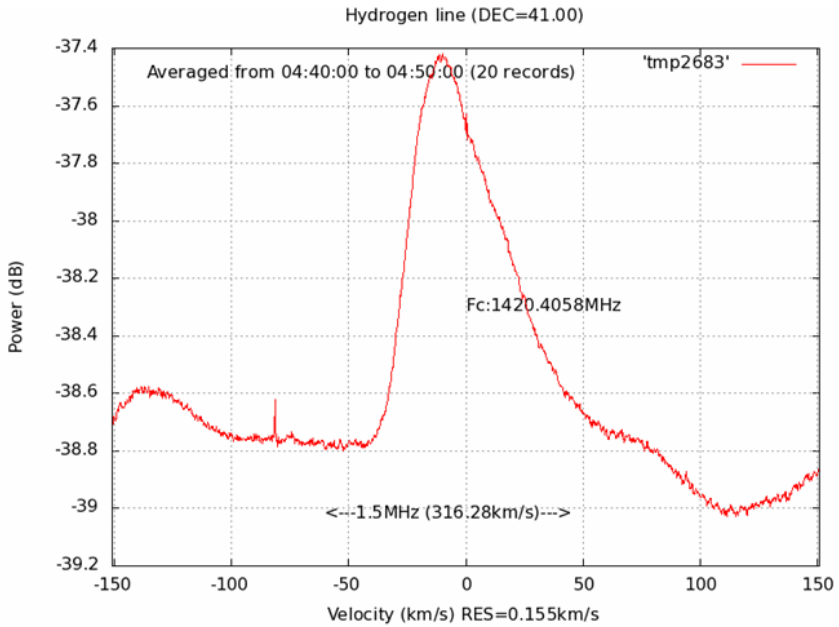
APRS

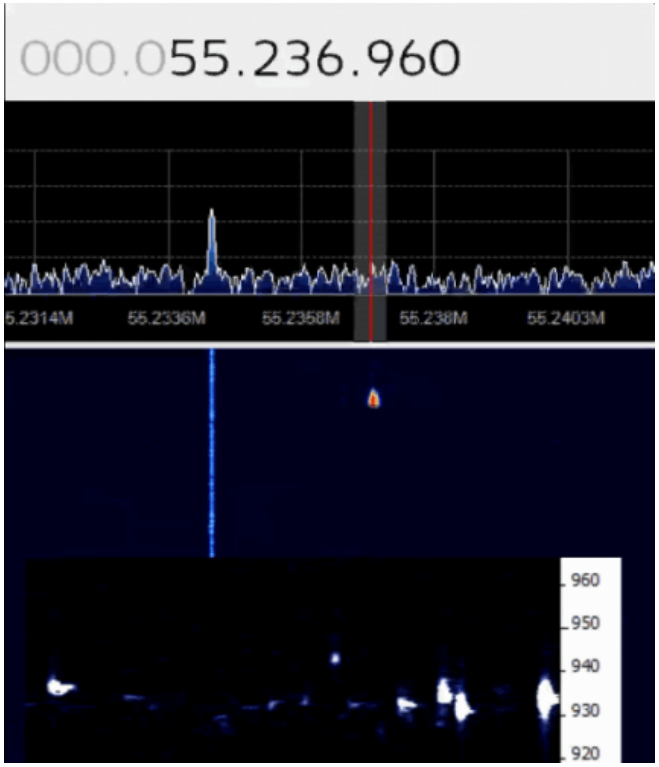
Railroad data reception

- Two

In the heavens

- Radio Astronomy
  - Meteor
  - Hydrogen line monitoring





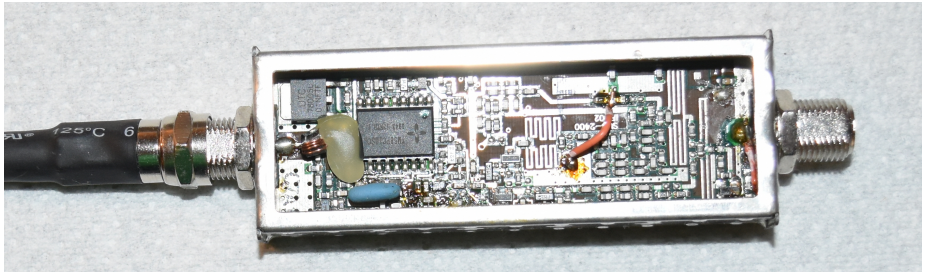
Live meteor detection stream from livemeteors.com

Sleuthing tools

- http://www.sigidwiki.com/wiki/Signal_Identification_Guide
- ARTEMIS
  - http://markslab.tk/project-artemis/
  - Off-line tool (still runs on your computer)
- AirProbe
- Inspectrum (linux and OSX)
- Wireshark

Downconverters

- What if we want to hear something above 1.7 GHz?
- Modify existing down-converters, DIY, or purchase.
- Create a simple downconverter using a 1.3 GHz local oscillator and an LNA4ALL.
- Direct TV SUP-2400



LF-HF and Upconverters

- What if we're interested in something below 24 MHz (ham bands, LW, etc.)?
- Two options:
  - Direct sampling (has risks)
  - Upconverters
- Newer devices make this easy (in both cases)
  - Bias-T power
  - Direct Sampling mode set in software

Filters

- Just like with other receiving applications, the right filter can solve lots of problems.
- One commonly used filter is the broadcast band filter, which can often lower the noise floor significantly

Low Noise Amplifiers

- LNAs are useful (or even necessary) both above and below the operating range of the RTL dongle (as well as within.) Eg. Inmarsat, Outernet
- Some devices are built in. Eg. FightAware Pro Stick Plus
- Power supply: Bias-T or external
- Several good commercial sources in the $50 range.
- LNA for all, NooElec, Airspy, DIY

So what should I get?

- It depends…
- Cheap, Accurate, Fancy, choose one:
  - Not every application needs accuracy of the TCXO.
  - Ebay is a reasonable source for the $7 dongle.
  - Higher frequency operation seems to increase heat so a heat sink is nice.

- Really inexpensive…
- $7 Chinese dongle

- More accurate…
- RTL-SDR.COM $20

- High accuracy
- Airspy: $100

What shouldn't I get?

- Some uses might suggest 'fancier' dongles, but usually* you'll only see a modest performance gain.
- Any device with a IT9130, AF9135 or where they do not specify what the tuner chip is.
- There are a LOT of eBay sellers that are selling counterfeit products. Others sell 'legitimate' dongles marked up significantly.
- Beware of 'bundles'. NooElec: $12 for a $5 item

* Some specific use scenarios, like the Flight Aware Plus ADS-B receive are an exception to this rule of thumb.

Questions?

Thank you to MicroHams and Microsoft for hosting the

17th annual

MicroHams Digital Conference

Thank you for attending

- This program is dedicated to the memory of Wilse Morgan, KX7P

It's not enough to love amateur radio, you absolutely MUST share that love with others.

Reference-1

- Example Dongle sources
  - RTL-SDR.com
  - NooElect.com
- Software sources
  - www.sdrsharp.com
  - www.hsdsr.de
  - www.sdr-radio.com
  - http://www.sdrplay.com
- Quick Start guide
  - http://www.rtl-sdr.com/rtl-sdr-quick-start-guide/

Reference-2
Hardware information

- Rafael Micro R820T datasheet
  - http://rtl-sdr.com/wp-content/uploads/2013/04/R820T_datasheet-Non_R-20111130_unlocked.pdf

Reference-3
Specialty or upscale devices

- http://www.sdrplay.com/

Reference-4
Raspberry Pi

- https://www.raspberrypi.org/forums/viewtopic.php?f=91&t=154980
- https://github.com/ha7ilm/qtcsdr
- https://learn.adafruit.com/freq-show-raspberry-pi-rtl-sdr-scanner/overview
- https://gist.github.com/floehopper/99a0c8931f9d779b0998
- http://photobyte.org/using-the-raspberry-pi-as-an-rtl-sdr-dongle-server/

Reference-5
general sources

- http://www.rtl-sdr.com/
- http://osmocom.org/projects/sdr/wiki/rtl-sdr
- http://www.hamradioscience.com/
- http://www.radioforeveryone.com/
- http://rtl-sdr.sceners.org/
- https://en.wikipedia.org/wiki/List_of_software-defined_radios
- http://wiki.spench.net/wiki/RTL2832U
- http://www.funcubedongle.com/MyImages/FCDAnIntroduction.pdf
- https://www.reddit.com/r/RTLSDR/comments/s6ddo/rtlsdr_compatibility_list_v2_work_in_progress/

Reference-6
Specific applications

- Amateur Digital TV
  - https://kh6htv.files.wordpress.com/2011/09/an-21a-receive-dtv-revdec2015.pdf
- Multiple receivers working together
  - https://ptrkrysik.github.io/
- LNA projects
  - http://lna4all.blogspot.com/
  - https://fabiobaltieri.com/2014/06/22/lna/

Reference-6-2 con't

- Inmarsat, Outernet
  - http://www.radioforeveryone.com/p/outernet-kit-re.html
  - NooElec LNA and SAW
    - http://www.rtl-sdr.com/review-outernet-lna-and-patch-antenna/
- Meteor echos
  - http://www.livemeteors.com/Detecting%20meteor%20radio%20echoes%20using%20the%20RTL-SDR.pdf

Reference-6-3 con’t

- Hydrogen Line Radio Astronomy
  - http://www.y1pwe.co.uk/RAProgs/
- Trunking scanner with one dongle
  - http://users.vline.pl/~pewusoft/sdr/how.html
  - http://www.rtl-sdr.com/using-unitrunker-with-sdrsharp/
  - http://utahradio.org/mediawiki/index.php/UniTrunker_Guide

Reference-7
Antennas!

- Colinear for ADS-B
  - https://www.balarad.net/
- Wideband LPA
  - http://www.rtl-sdr.com/building-an-active-wideband-antenna-for-your-sdr/
- General reference
  - http://shyamjos.com/testing-different-antennas-for-rtlsdr/

Reference -8
Evaluating SDR Hardware that Tx

- http://www.rtl-sdr.com/review-airspy-vs-sdrplay-rsp-vs-hackrf/