THE

HOBBYIST'S GUIDE TO RTL-SDR:
REALLY CHEAP SOFTWARE DEFINED RADIO

INTRODUCTION

WHAT IS SOFTWARE DEFINED RADIO (SDR)?

In traditional hardware radios, the mathematical operations required to decode and process radio signals are performed using analogue circuitry.

Recently, computers have become powerful enough to perform the required mathematical calculations in software, hence the term software defined radio.

This has led to advanced radios that previously required complicated analogue hardware now being able to be implemented easily in software. This has reduced the cost of advanced radio capabilities such as wideband tuning and waterfall displays.

WHAT IS THE RTL-SDR?

The RTL-SDR is an extremely cheap software defined radio which is based on DVB-T TV (Digital HD TV) USB receiver dongles that have the RTL2832U chip in them. It was discovered by hardware hacker Eric Fry, Linux driver developer Antti Palosaari and the Osmocom team who were developing their own SDR that the RTL2832U chip had a mode which enabled SDR.
Today, by using custom software drivers, a commonly used cheap RTL2832U can then be turned into a sophisticated SDR with features that would have until recently cost in the hundreds to thousands of dollars.
Of course, the performance of these dongles will not match a dedicated SDR, but they perform extremely well for the price, and almost all hobbyist projects that can be done with expensive radios or SDRs can also be done with the rtl-sdr.
A wideband SDR opens up many interesting possible projects and avenues to explore. Some applications of the RTL-SDR include the following, some of which will be discussed in more depth in the project tutorials chapter.

- 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 maritime boat positions like a radar with AIS decoding.
- Decoding POCSAG/FLEX pager traffic.
- Scanning for cordless phones and baby monitors.
- Tracking and receiving meteorological agency launched weather balloon data.
- Tracking your own self launched high altitude balloon for payload recovery.
- Receiving wireless temperature sensors and wireless power meter sensors.
- Listening to VHF amateur radio.
- Decoding ham radio APRS packets.
- Watching analogue broadcast TV.
- Sniffing GSM signals.
- Using rtl-sdr on your Android device as a portable radio scanner.
- Receiving GPS signals and decoding them.
- Using rtl-sdr as a spectrum analyzer.
- Receiving NOAA weather satellite images.
- Listening to satellites and the ISS.
- Listening to unencrypted military communications.
- Radio astronomy.
- Monitoring meteor scatter.
- Listening to FM radio, and decoding RDS information.
- Listening to DAB broadcast radio.
- Use rtl-sdr as a panadapter for your traditional hardware radio.
- Decoding taxi mobile data terminal signals.
- Use rtl-sdr as a true random number generator.
- Listening to amateur radio hams on SSB with LSB/USB modulation.
- Decoding digital amateur radio ham communications such as CW/PSK/RTTY/SSTV.

- Receiving HF weatherfax.
- Receiving digital radio monodiale shortwave radio (DRM).
- Listening to international shortwave radio.
- Looking for RADAR signals like over the horizon (OTH) radar, and HAARP signals.

Project specific can refer to the http://www.rtl-sdr.com web site.

The set includes

A test antenna,

can be used to test signal receiving UV band, the resonant frequency is GSM band, to receive the effect of UV is not the best. Cannot be used to receive HF signal band, signal receiving HF band needs to meet the HF Antennas such as Long Wire, Random Wire, Dipole etc.. To have a good effect need matching antenna.

A main unit

A USB cable

RTL-SDR TECHNICAL SPECIFICATIONS

- 100KHz-1766 MHz Tunable Range

(HF 100KHz-30MHz to direct sampling of the signal Q)

- 3.2 MHz max bandwidth (~2.8 MHz stable)

- 8-bit ADC giving ~50 dB dynamic range
- < 4.5dB noise figure LNA
- 50 Ohm input impedance

RTL-SDR ADC

ADC is an acronym for "Analogue to Digital Converter". It is a microchip that reads in an analogue signal and then digitizes it. The more bits an ADC has, the more accurate the digitization can be. For example an 8-bit ADC can scale the analogue input into values between -127 and +127, whereas a 12 bit ADC can scale values from -2047 to +2047.

So with a low bit ADC certain small details in the analogue input, such as weak signals may be lost during digitization. **The RTL-SDR has an 8-bit ADC**, which is fairly low, but large enough to give decent performance. The dynamic range of an ADC can be calculated approximately with: number_of_bits * 6 dB. This gives the RTL-SDR approximately 50 dB of dynamic range. However, the dynamic range is usually slightly larger (~60 dB) due to the oversampling trick that can be performed in software.

Dynamic range is the range between the largest and smallest possible values.

RTL-SDR BANDWIDTH

The maximum bandwidth of the RTL-SDR is 3.2 MHz, though the largest stable bandwidth is either 2.4 MHz or 2.8 MHz depending on your PC. Setting the bandwidth too large can cause samples to be lost on slow PCs giving choppy audio.

Most RTL-SDR compatible software will let you choose your bandwidth which is sometimes referred to as sample rate as well. Although sample rate and bandwidth are not the same thing, in the RTL-SDR setting the sample rate to 2 Msps (Mega Samples per second) will give you 2 MHz of bandwidth. Setting it to 2.8 Msps will give you 2.8 MHz of bandwidth. (If you are familiar with Nyquist you might wonder how 2 Msps can give 2 MHz, this is because the RTL-SDR uses I/Q sampling with two ADCs).

The bandwidth is the size of the frequency spectrum that you can see at any one time.

RTL-SDR MINIMUM PC SPECIFICATIONS

For SDR# any modern PC with a dual core processor, at least 1 GB of memory and Windows XP or newer should be sufficient. The PC must also have a USB 2.0 or newer port.

Slower PCs and embedded microcontroller based computers like the Raspberry Pi can be used with efficient command line software.

.

R820T PACKAGES

SOFTWARE DEFINED RADIO BASIC THEORY

An SDR simply works by receiving an analogue radio signal and then using an Analogue to Digital Converter (ADC) to digitize the signal. The digitized signal can then be worked on in digital signal processing software.

In practice an ADC will only work up to a certain frequency. The RTL2832U is a type of ADC which works up till 28.8 MHz. To digitize higher frequency signals we need an IF mixer stage to convert all received frequencies down to the frequencies that the ADC can use. This is the job of the tuner chip (e.g R820T/E4000).

Advanced: The RTL-SDR uses I/Q sampling, where two ADCs are used, one for the minus part from the DC offset and one part for the positive part of the DC offset. This is how we can get 3.2 MHz of bandwidth from a 3.2 Msps ADC sampling rate despite the Nyquist limit. (If an ADC can

sample at 3.2 Msps, then the maximum bandwidth it can digitize is 3.2/2 = 1.6 MHz due to Nyquist.)

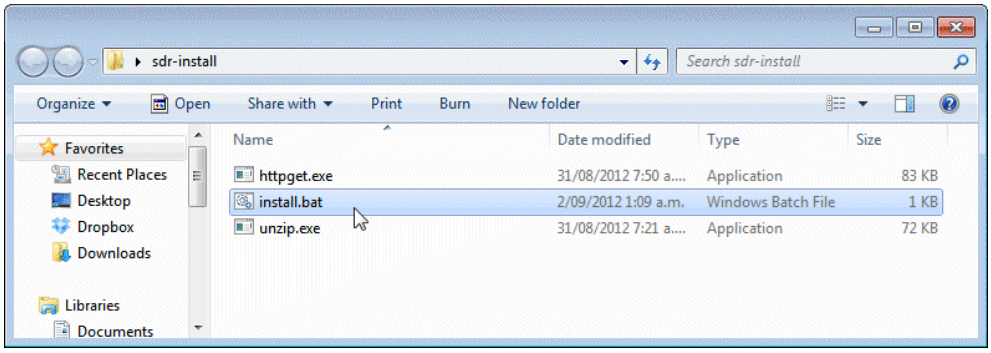
If you are interested in a more in depth treatment of SDR theory, the ARRL has a good article at http://www.arrl.org/files/file/Technology/tis/info/pdf/020708qex013.pdf

SETTING UP AND USING YOUR RTL-SDR

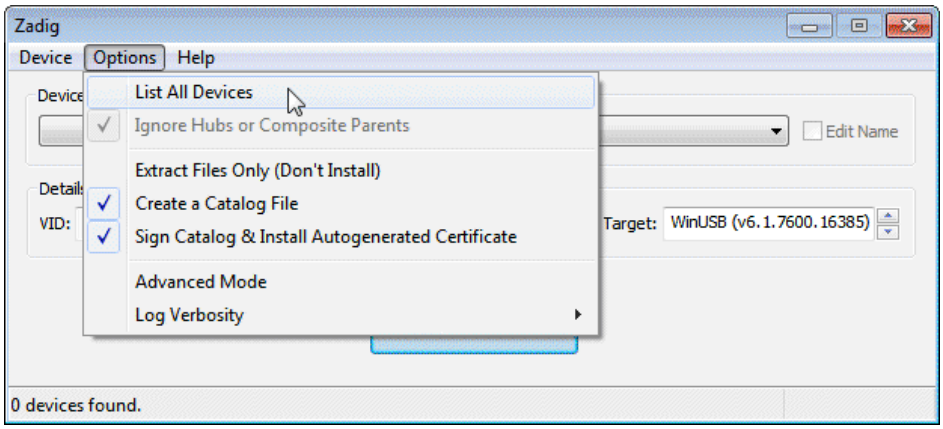
SDR# SETUP GUIDE (TESTED ON WINDOWS VISTA/7 + XP)

1. SDRSharp is the easiest and most commonly used software defined radio software receiver for the RTL-SDR. Go to www.sdrsharp.com and head to the download page. Note that you must have the Microsoft .NET redistributable installed to use SDRSharp. Modern Windows PCs have this installed by default, but older PCs running XP may need this to be installed. It can be downloaded from http://www.microsoft.com/en-gb/download/details.aspx?id=21.
2. Ignore the downloads on the top of the page. Scroll down to where it says "Important note for RTL-SDR users". Download sdr_install.zip from that link. **NOTE: At the time of writing this book the SDR# downloads page has recently changed. The sdr_install.zip file download is currently available from the main page at sdrsharp.com but it's location may change in the future.**

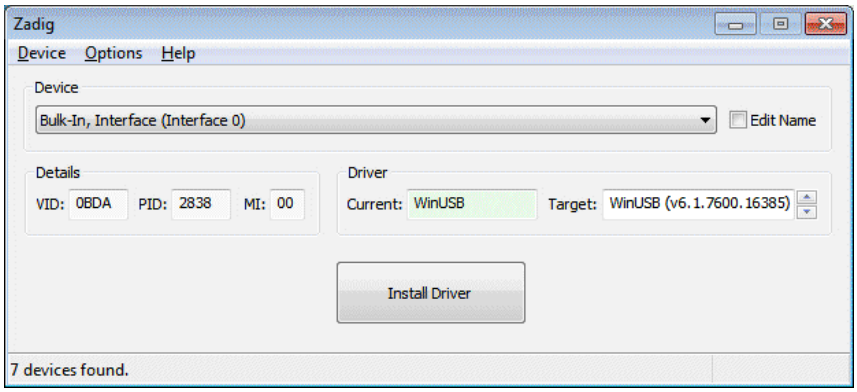
3. Extract the sdr-install folder from the zip file to a place on your computer.
4. Double click on install.bat from within the extracted folder. This will start a command prompt that will download SDRSharp and all the files required to make SDRSharp work with RTL-SDR. Everything will be placed into a new folder within the sdr-install folder called “sdrsharp”. The command prompt will automatically close when it is done.



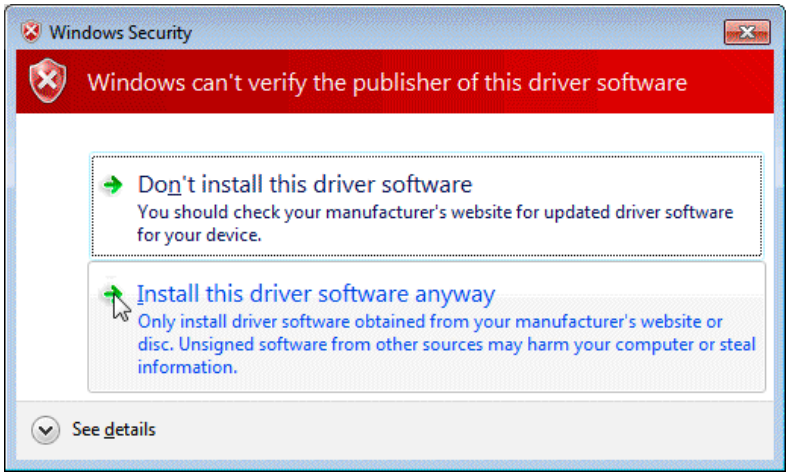
5. Plug in your dongle and do not install any of the software that it came with, but ensure you let plug and play finish trying to install it. If necessary, uninstall any DVB-T software drivers you’ve installed from the CD that some dongles come with.
6. Open the newly created sdrsharp folder. Find the file zadig.exe. Right click this file and select “Run as administrator” if using Windows Vista/7. If you are using Windows XP, download the XP version from http://zadig.akeo.ie/. If you are on Windows 8 you may get unsigned driver issues when using zadig. To get around this use the newer version (v2.1+) of zadig from http://zadig.akeo.ie/.
7. In Zadig, go to **Options -> List All Devices** and make sure this option is checked.



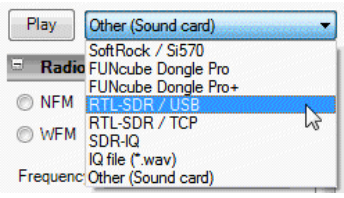
8. Select **“Bulk-In, Interface (Interface 0)”** from the drop down list. Ensure that WinUSB is selected in the box next to where it says Target. (Note on some PCs you may see something like RTL2832UHIDIR instead of the bulk in interface. This is also a valid selection).



9. Click Install Driver. You might get a warning that the publisher cannot be verified, but just accept it by clicking on Install this driver software anyway. This will install the drivers necessary to run the dongle as a software defined radio. Note that you *may* need to run zadig.exe again if you move the dongle to another USB port, or want to use two or more dongles together.

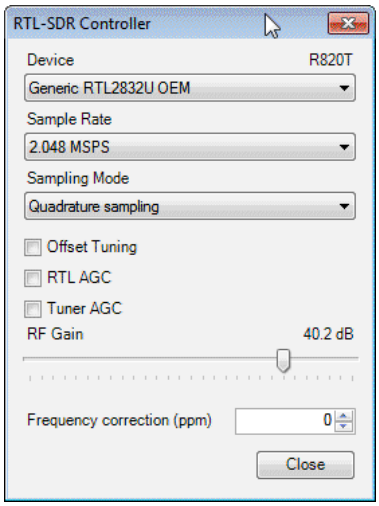


10. Open SDRSharp.exe. Set the drop down box at the top next to the Play button to **‘RTLSDR / USB’**. Press Play. Your rtl-sdr software radio should now be playing some static and showing an RF spectrum and waterfall! If everything has worked you should be able to start tuning to frequencies using the numbers at the top of the program.



11. Click on the Configure button to bring up the configure menu.

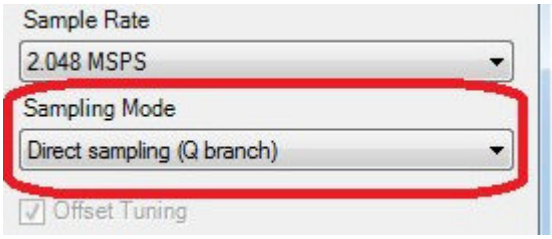
12. By default the RTL-SDR's gain is set to zero. Increase this gain by moving the RF Gain slider up, or by turning on Tuner AGC.



13. Receiving LF/MF/HF (0 - 30 MHz)

The antenna must be connected to the HF input port

The program of SDR # with RTL configured to direct sampling of the signal Q, as shown in the following figure:



signal receiving HF band needs to meet the HF Antennas such as Long Wire, Random Wire, Dipole etc.. To have a good effect need matching antenna.

TROUBLESHOOTING GUIDE

ZADIG TAKES A LONG TIME TO INSTALL THE DRIVER, THEN FAILS

You have probably not run zadig in administrator mode. Make sure to right click zadig, and select "Run as Administrator"

I DON'T SEE BULK-IN, INTERFACE (INTERFACE 0)

Ensure **Options->List All Devices** is checked. Some people report seeing something else other than the bulk in interface. It may also show up as the brand of your dongle or something prefixed with "rtl". This option should work too.

I DON'T SEE RTL-SDR/USB IN SDRSHARP

You may have downloaded a version without rtl-sdr support. Check that you followed the instructions in step 3 and downloaded the version under the heading "Important note for RTL-SDR users".

ZADIG GIVES "SYSTEM POLICY HAS BEEN MODIFIED TO REJECT UNSIGNED DRIVERS" ERROR IN WINDOWS 8

Windows 8 can cause signed driver issues with zadig. Some users report getting the error: "System policy has been modified to reject unsigned drivers". To solve this download the newer Zadig 2.1+ drivers from http://zadig.akeo.ie/.

RECEPTION IN SDR# SEEMS VERY POOR/RECEIVER IS INSENSITIVE

Make sure you have increased the gain slider which can be accessed by clicking on the configure button. Also, in poor reception areas using the stock antenna indoors may not be sufficient. Though rare, another cause of insensitivity is a dongle blown by electrostatic discharge.

SDR# GIVES ERROR "APPLICATION FAILED TO INITIALIZE PROPERLY (0XC0000135). CLICK OK TO TERMINATE."

This might mean that you do not have the .NET 3.5 Framework installed. Download it from http://www.microsoft.com/en-gb/download/details.aspx?id=21.

SDR# GIVES ERROR "CANNOT ACCESS RTL DEVICE"

You may have tuned to a frequency that it out of range of the RTL-SDR. Tune back to a known supported frequency like 000.100.000.000 and press play.

WHAT IS BULK IN INTERFACE-1?

This is the IR interface for the remote control which is not required for SDR.

ZADIG WON'T RUN

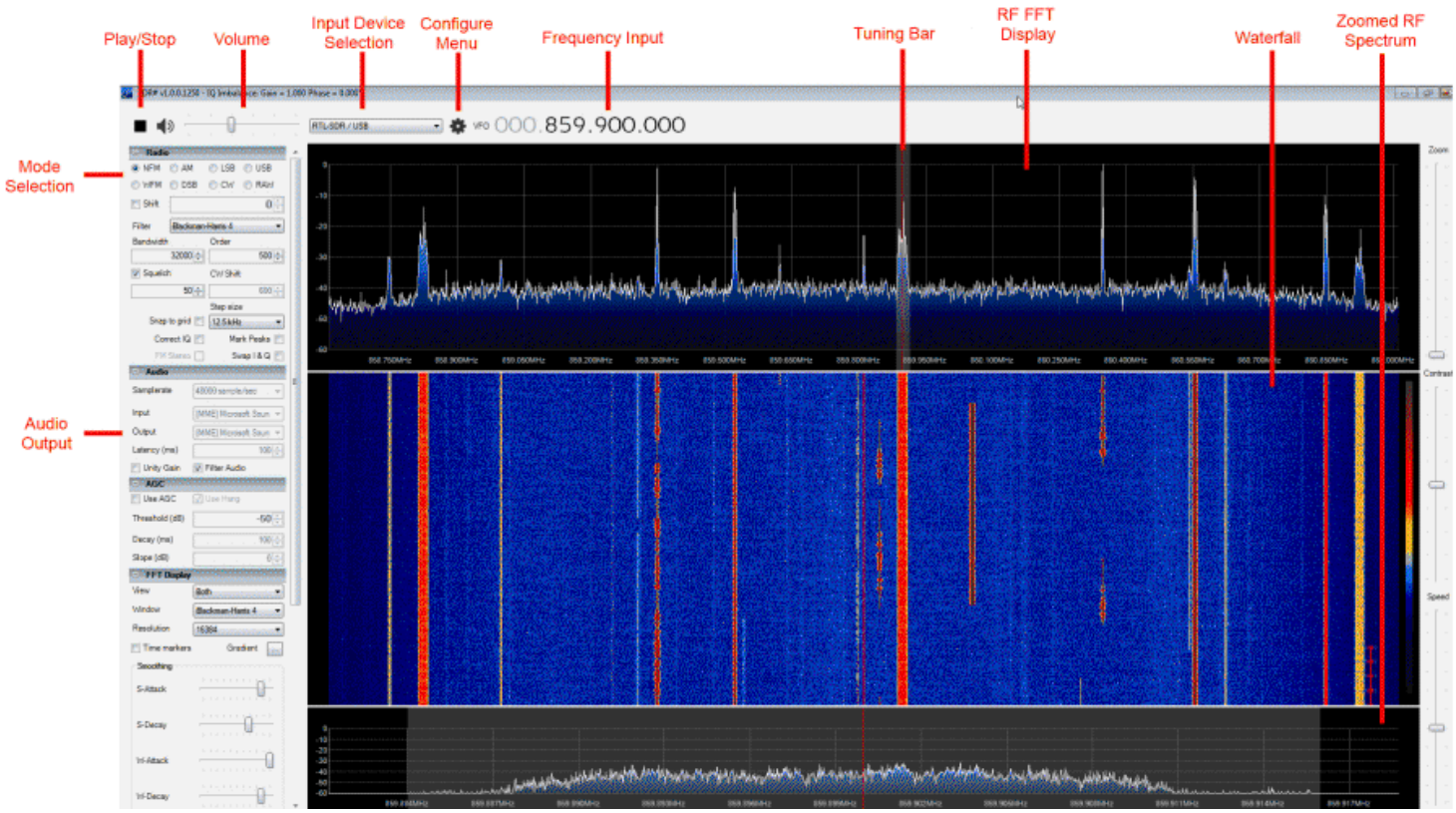
Some users report that Zadig crashes upon opening. An alternative driver installer can be found at http://visualgdb.com/UsbDriverTool/. Use this tool to install the libUSB - WinUSB drivers.

SDR SHARP USERS GUIDE

SDR# is currently the most popular SDR program used with the RTL-SDR. It is easy to setup and simple to use. To install SDR#, go through the RTL-SDR setup guide first.

Upon starting SDR#, we suggest you reduce the Range setting and increase the FFT resolution to 16384. See below for more information.

Open SDR#. You will be greeted with this screen shown below. Here we have highlighted the main parts of SDR#.



MAIN SETTINGS

PLAY BUTTON

This button is used to start and stop the SDR.

INPUT DEVICE SELECTION

This is a drop down menu which is used to select the SDR input device being used. If you are using an RTL-SDR, select RTL-SDR/USB. Be sure to NOT select RTL-SDR/TCP unless you are using a remote server with rtl_tcp.

CONFIGURE MENU

Clicking this button opens up the configure menu. In here you can change settings like the sample rate (bandwidth) and RF gain.

FREQUENCY INPUT

Use the mouse to set the desired frequency in MHz you wish to listen to here. You can either click on the tops and bottoms of each individual number to increase or decrease the value, or simply hover over the number you want to change and use the mouse wheel to alter the value.

MODE SELECTION

Here you can choose what type of demodulation mode the signal at your currently tuned frequency uses.

NFM -Narrowband Frequency Modulation. Common mode used by walkie talkie radios and digital signals.

WFM -Wide Band Frequency Modulation. Is the mode that broadcast FM stations use (eg the radio you listen to in your car).

AM -Amplitude Modulation. Used by broadcast AM stations that are receivable by normal radios and air band voice frequencies used by aircraft and air traffic control.

LSB/USB -Lower Side Band/Upper Sideband. Use in the HF band by ham radio to transmit voice efficiently.
CW -Continuous Wave. Used for listening to Morse Code.
DSB -Double Side Band. Not commonly used.
RAW -Raw signal. Almost never used.

VOLUME / AF GAIN

Set the volume level of your output speakers or audio piping device here.

RF FFT SPECTRUM

This part of the window shows the RF FFT spectrum as a graph in real time visually. Active signals will appear as peaks on this graph.

RF FFT WATERFALL

This part of the window shows the RF spectrum graph spread over time with new data at the top, and old data at the bottom, just like a waterfall.

TUNING BAR

The vertical red line shows where on the RF spectrum the RTL-SDR is currently tuned to. The tuning can be altered by simply using the mouse to click and drag the red line.
The shaded rectangular area around the red line shows the bandwidth of the tuned area. (don't confuse this with the bandwidth/sample rate set in the configure menu). The bandwidth should be set so that it covers the area of the signal that is tuned. The bandwidth can be adjusted by using the mouse by simply dragging the edges of the shaded area in or out.

OTHER SETTINGS

Other options which you may find useful are described below.

RADIO TAB

OFFSET

This box offsets the tuned frequency by the amount entered. This is useful if you are using an upconverter. For example if you have an upconverter with a 100 MHz oscillator, you would set the offset to be -100,000,000 (don't forget the minus sign). Without the offset, to tune to a signal at 9 MHz you would need to actually tune to 100 + 9 = 109 MHz. With the offset set, you can tune to 9 MHz as normal. If you have an upconverter with a 125 MHz oscillator you would tune to 125 + 9 = 134 MHz, or set the offset to -125,000,000.

FILTER BANDWIDTH

This is the width of the shaded part of the tunable area. You can set it manually here, or by dragging with the mouse as described above.

FILTER TYPE

Changes the filter type used. Different filters have different shapes. The filter is used to select the highlighted signal in the RF window. A good filter will select only the selected signal.
Blackman-Harris is usually the best filter to choose.

FILTER ORDER

You may notice that with low filter orders signals outside of the tuned bandwidth can still be heard. Larger filter orders "tighten" or "sharpen" the band pass filter used in the tuned bandwidth preventing signals outside of the tuned bandwidth from being heard.
You will want to increase the filter order when there are strong signals near to your tuned area.

SQUELCH

Mutes the audio when the signal level is below the specified value. Useful for when listening to speech as the static when no one is talking will be muted.

CW SHIFT

Mainly useful for when transmitting CW as it specifies the offset between CW transmit and receive frequencies.

SNAP TO GRID

In many bands signals are spaced a fixed distance apart. For instance in most countries air band signals are spaced 25 kHz apart (or 8.33 kHz in some countries). This setting can help with tuning by snapping directly to a signal. However, to use this with the RTL-SDR the PPM frequency offset correction must be set correctly, otherwise the frequencies may not line up.

CORRECT IQ

Should usually be selected as ON. This setting uses an algorithm to remove unwanted images (ghosts of strong signals) from showing up in the spectrum.

SWAP I & Q

If you are using SDR# as a panadapter, some hardware radios may have the I & Q signals swapped.

FM STEREO

Will enable stereo output for broadcast radio WFM signals.

MARK PEAKS

Simply marks any peak in the RF spectrum with a circle.

AUDIO TAB

OUTPUT

Sets the audio output device. By default it is set to your speakers. If you are passing the audio to a decoder program here you would choose your virtual audio cable to send the audio to.

AGC (AUTOMATIC GAIN CONTROL):

The AGC tab will only be activated in the AM, DSB, LSB, USB and CW demodulation modes.

USE AGC

Turns on the automatic gain control. The AGC will attempt control the volume level so that loud sounds are not too loud and quiet sounds are not too quiet. The default settings work well for audio signals.

FFT DISPLAY

VIEW

THE BIG LIST OF RTL-SDR SUPPORTED SOFTWARE

http://www.rtl-sdr.com/big-list-rtl-sdr-supported-software/

Antenna Long Wire con Balun 9:1

http://www.radioamatoripeligni.it/i6ibe/balun9a1/balun9a1.htm

Alternative Installation Procedure for RTL.SDR and HDSDR

http://www.hamradioscience.com/alternative-installation-procedure-for-rtl-sticks-and-hdsdr/