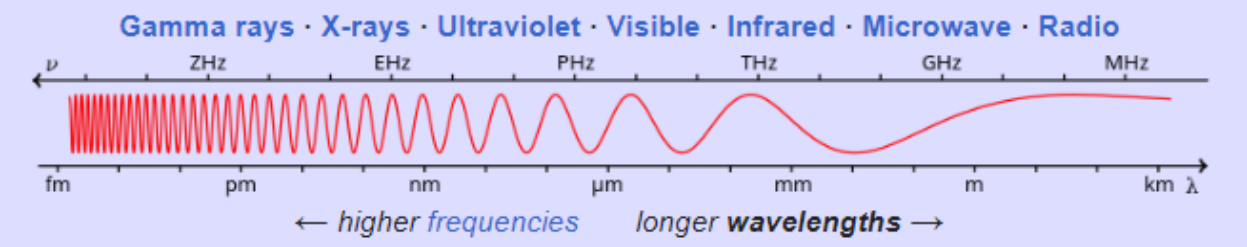
Introduction to Software Defined Radio: Supplement

Charts, diagrams, equations, links and supplemental information discussed in the online course

Radio Frequency Theory

Wavelengths



Signals in the electromagnetic spectrum travel at the speed of light, so the wavelength will be a function of the speed of light (299,792,458 meters per second) divided by cycles per second (Hertz). We have a shortcut that gets us very close.

300 / Frequency In MHz = Wavelength

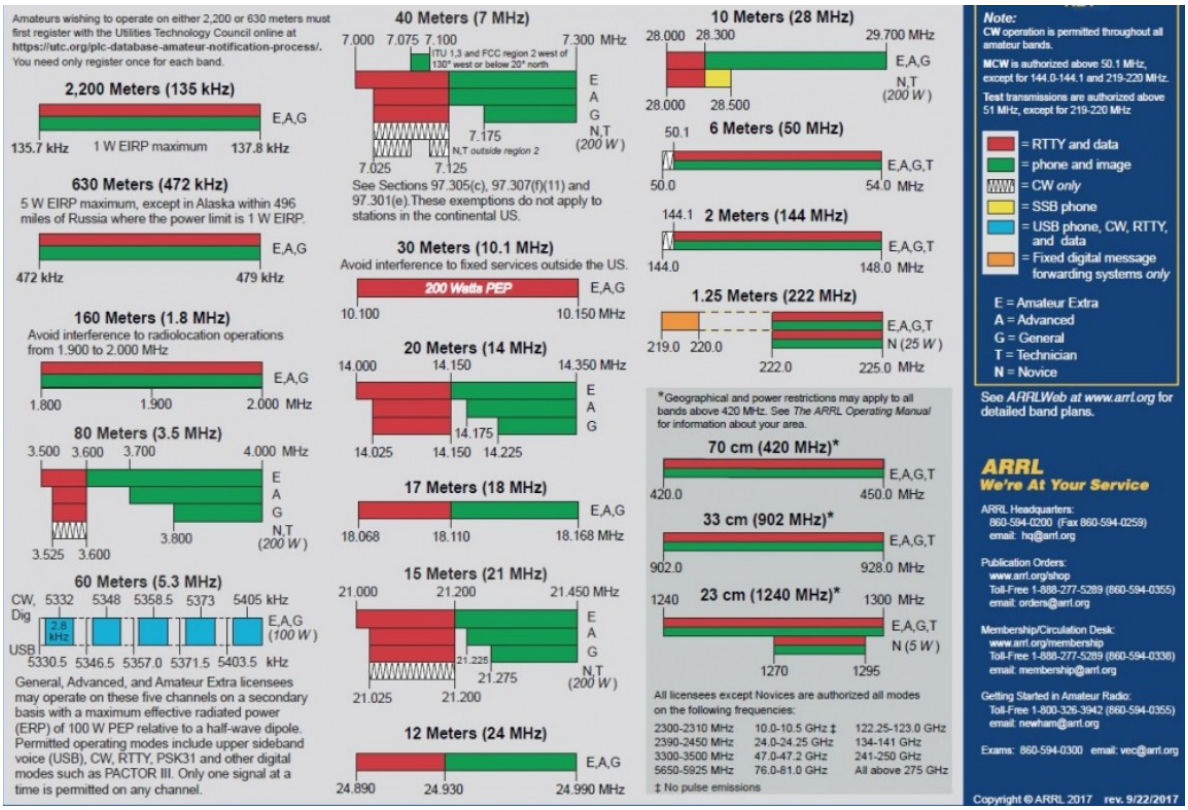
1MHz = 300 meters. 10 MHz = 30 meters. 30 MHz = 10 meters. 100MHz = 3 meters.

Frequency Ranges

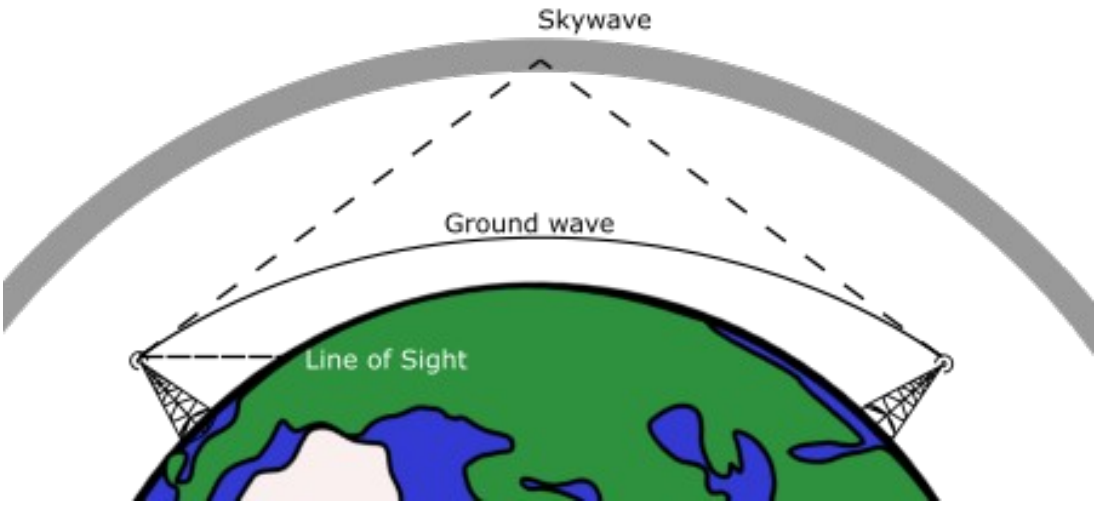
Frequency Range	Classification	Wavelengths
3-30 kHz	Very Low Frequency (VLF)	100km-10km
30-300 kHz (0.3 MHz)	Low Frequency (LF)	10km-1000m
0.3-3 MHz	Medium Frequency (MF)	1000m-100m
3-30 MHz	High Frequency (HF)	100m-10m
30-300 MHz	Very High Frequency (VHF)	10m-1m
300-3,000 MHz (3 GHz)	Ultra High Frequency (UHF)	1m-10cm
3 GHz - 30 GHz	Super High Frequency (SHF)	10cm-1cm

Radio Bands

https://www.arrl.org/files/file/Regulatory/Band%20Chart/Band%20Chart%20-%2011X17%20Color.pdf



Radio Frequency Propagation



Ground Wave

Below 200 KHz, RF follows the curvature of the earth for long distances

Sky Wave

200 KHz to 15 MHz Reliably bounces off the ionosphere for long distances. Depending on conditions, frequencies up to 30 MHz open up often. Rarely, frequencies up to 200 MHz can “skip”. The higher the frequency, the less common it is for skywave propagation to work.

Line-Of-Sight

Above 30 MHz, Line of sight is the only truly reliable propagation

Basic Antenna Theory

Dipole

Two lengths of wire, insulated from one another, one each attached to each side of the feedline (ground and output)

Monopole

Usually “Sticks up into the air” - functionally equivalent to half a dipole. Handhelds use the chassis and the operator as the groundplane. The ground sheath of the coax or the SDR housing itself may also act as the groundplane with a monopole antenna.

Wavelength vs Antenna Length

The lower the frequency, the longer the wavelength and the longer the antenna you need to effectively transmit or receive it.

As a general rule, you will want your receiving antenna to be ¼ wavelength if it's a monopole or ½ wavelength if it's a dipole. When setting up a telescopic or adjustable length antenna, you may get better performance by tuning the length, than having the antenna fully extended. More antenna is not always better.

Antenna Gain

- A 2x increase in effective radiated power is 3dBi
- Most "Omni-directional" antennae have a lighthouse-beam shaped radiation pattern
- Most "Directional" antennae have a radiation pattern more like a spotlight
- Radiation pattern is also similar to how sensitive they are for receive

Polarization

I do not cover polarization in my presentation. Unless you're receiving weather satellite signals, vertical and horizontal polarization are mostly what you need to worry about. Most VHF and UHF signals we can easily monitor with SDR are vertically polarized, so your antenna (whether it's dipole or monopole) should be oriented up and down, not side-to-side.

Modulation

Continuous Wave (CW)

CW is the absolute simplest modulation scheme. You run a constant signal from the transmitter. This signal can be turned on or off. That's it. The radio operator, or a computer attached to the radio, momentarily transmits short pulses of the carrier wave. One common use of CW is transmitting messages in Morse Code.

Amplitude Modulation (AM)

Amplitude Modulation is the simplest analog audio modulation scheme, and it closely resembles normal analog audio coming out of a speaker, but encoded onto a carrier signal.

Single Sideband Modulation (SSB)

- SSB is an AM signal without the main carrier signal and either the top or bottom sideband, leaving only one sideband.
- One of the most efficient ways to transmit low-quality audio
- A favorite among amateur radio operators in crowded radio bands
- Must be demodulated according to the proper sideband
    - Below 10 MHz, lower sideband is usually used

    - Above 10 MHz, upper sideband is usually used
    - Not all users follow this rule

Frequency Modulation (FM)

- FM adjusts the carrier's frequency up or down slightly in order to transmit the information
- Several different bandwidths in use
    - Walkie Talkies and business radios: 12.5 KHz
    - Amateur Radio VHF/UHF: 25 KHz
    - Commercial Broadcast FM: 150 KHz

Phase Modulation (PM)

- PM adjusts the radio signal's phase in order to transmit the information
- Rarely used in analog radio applications
- Forms the basis for many keying schemes used in telecommunications.

Quadrature Amplitude Modulation (QAM)

- QAM uses two carrier signals that are orthogonally out of phase with one another
- Both are modulated in amplitude
- Like PM, used for telecom and digital signals.
- WiFi is one of the most obvious implementations of QAM.

Digital Signal Keying

On/Off Keying (OOK) and Amplitude Shift Keying (ASK)

- Basically an implementation of CW for digital signals
- Commonly used with cheap remote devices and toys
- Since ASK is a binary keying scheme (either zero amplitude or full amplitude), OOK and ASK are basically two names for the same thing.

(Audio) Frequency Shift Keying (FSK / AFSK)

- FSK directly encodes digital data onto an FM carrier
- FSK is commonly used on car key fobs and other wireless devices
- AFSK uses different audio frequencies to symbolize digital data
- AFSK Audio is transmitted via normal FM
- AFSK is used in some amateur radio digital modes, such as ARPS

Phase Shift Keying (PSK)

- PSK directly encodes digital data onto a Phase Modulated carrier
- Used for telecommunications

Radio Systems

Simplex

- All radios in the system transmit and receive on the same frequency
- Limited range

Duplex

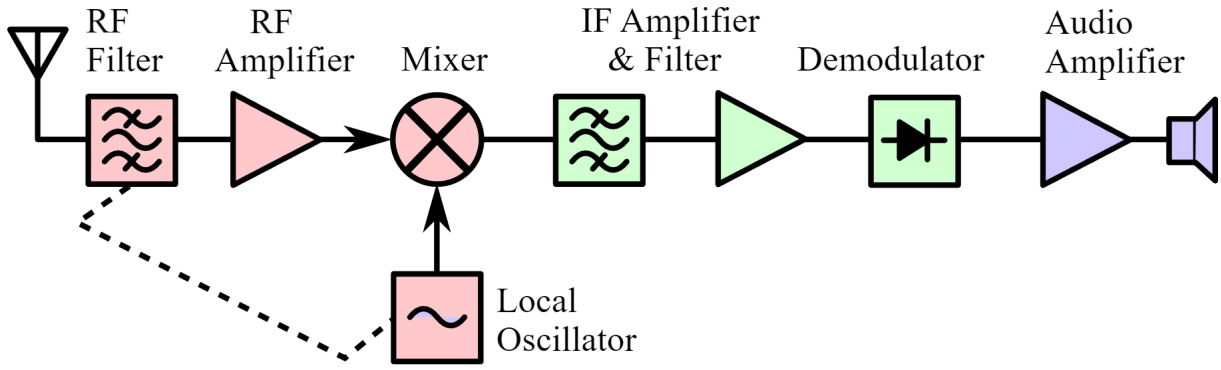
- All radios in the system transmit on one frequency and receive on some other frequency
- Most commonly used when there is a repeater in use
- Transmitting station switches to the repeater input frequency
- Repeater re-transmits the information on the second frequency

Trunked

- All radios monitor a “control” channel
- Multiple talk groups exist on a pool of shared frequencies (fire, police, EMS, etc)
- Local governments in major metropolitan areas are using digital trunked radio systems

Radio Reception Theory - Superheterodyne Receiver

This is a very simplified diagram and explanation of a superheterodyne receiver, which is the most popular radio receiver design.

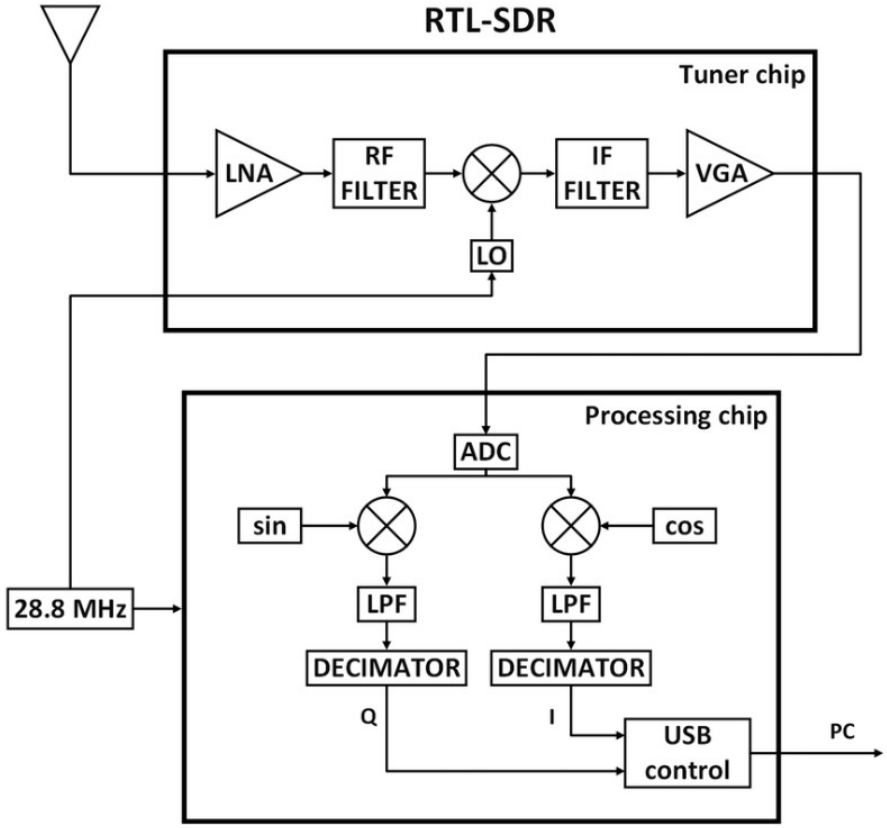


When a radio is receiving a signal, it has an internal oscillator that operates very close to the desired frequency being received. This is called the **Local Oscillator (LO)**. The output of the LO is combined with the signal coming in from the antenna, through a circuit called a **Mixer** to produce an **Intermediate Frequency (IF)**. The IF can be further amplified and filtered to recreate a copy of the original signal without the carrier frequency. From there, the demodulated signal can be turned into audio or data.

Software Defined Radio Theory

What is SDR?

- SDR replaces most of the circuitry and demodulation work with software
- Prior to 2010, mostly industrial, military and scientific applications with expensive hardware
- Around 2010, inexpensive USB adapters designed to allow PCs to receive over-the-air analog television, FM radio, and european DVB-T television broadcasts became popular



- Local Oscillator (LO) operates very close to the center frequency of the desired range.
- Temperature Compensated Crystal Oscillator (TCXO) keeps LO frequency stable
- Intermediate Frequency Filter limits the baseband signal coming from the LO and canhelp pick up weak signals
- Variable Gain Amplifier plays a part in automatic gain control
- Analog/Digital Controller creates a Quadrature Frequency to go with the Intermediate Frequency
- These two outputs are known as the Q Branch and the I Branch
- Decimators reduce the sample rate by sampling one in X samples.

Sample Rate vs Bandwidth

- Sample rate must be equal to or greater than the desired bandwidth
- RTL-SDR can operate up to 2.4 million samples per second (2.4MSPS)
- Thus. RTL-SDR can receive up to 2.4 MHz worth of radio spectrum at a time

SDR Hardware

Note: All links in this section are affiliate links through Amazon, for which I may receive compensation. I have personally used and can recommend any products linked from this section. Not every device I mention is linked.

RTL2832U Derived (RTL-SDR)

Gets its name from the RTL2832U ADC chipset, and usually equipped with Rafael RT820T or Elonics E4000 tuners

- Frequency Range: around 29 MHz - 1,700 MHz
- Bandwidth: 2.4 MHz
- Cost: Starting at $25
- Receive Only
- Excellent software support
- Examples:
    - RTL-SDR v3 (v4 was recently released, isn't widely available yet)
    - RTL-SDR v4
    - NooElec NESDR SMART v5
    - NooElec NESDR Nano 2 (Nano 3 isn't always in stock, runs very hot)
    - Generic DVB-T USB receivers(easy to find on eBay, AliExpress, etc. Expect long shipping times)

AirSpy Mini

The AirSpy Mini uses the same tuner as the RTL-SDR (RT820T) but replaces the RTL chipset with a much better DSP that provides 10 MHz of bandwidth

- Frequency Range: 24 MHz - 1,700 MHz
- Bandwidth: 10 MHz
- Cost: $99
- Receive Only
- Limited software support (SDR#, SDR++, and SoapySDR work)

SDRPlay RSP Family

Middle-of the line SDR Receivers with 10 MHz of bandwidth and an increased frequency range, but with higher cost and less software support.

- Frequency Range: 1 kHz - 2 GHz

- Bandwidth: 10 MHz
- Cost: $115-300
- Receive Only
- Limited software support (SDR#, SDR++, and SoapySDR work)

HackRF One

HackRF One has an expanded frequency range from 1 MHz to 6 GHz and 20 MHz of bandwidth. It is also capable of transmitting at a very low power – about on-par with a garage door opener.

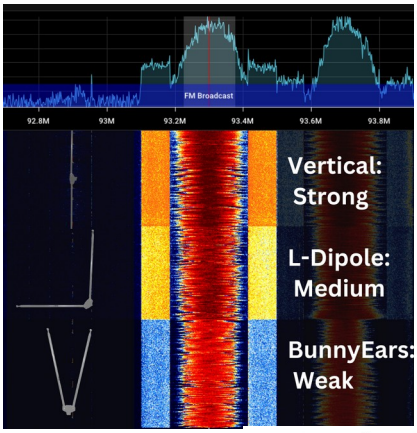
- Frequency Range: 1 MHz - 6,000 MHz
- Bandwidth: 20 MHz
- Cost: $300 and up for the official unit
    - Usable clones can be found under $200
    - PortaPack lets you perform some operations with on-board display/controls
- Receive and Transmit (very low power)

Antennas

Here are two mid-tier high quality antennas and one cheap bare-bones one. Consider purchasing a starter kit with an antenna, linked in the next section instead, if you don't already have an SDR.

- RTL-SDR Dipole Kit (the gold standard SDR dipole)
- Great Scott Gadgets ANT500 telescoping monopole (the gold standard SDR monopole)
- Bare-bones cheap SMA Telescoping antenna (surprisingly good for the money)

Dipole Kit Setup



"Bunny Ears"
Cancels out most of the incoming RF energy

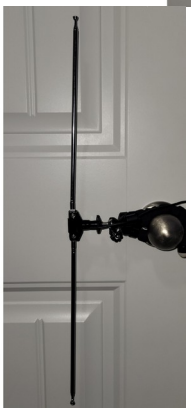
Center-fed Vertical L Dipole

May help receive certain signals in the direction toward the horizontal arm

Vertical Dipole

Each side should be tuned to 1/4 or 1/2 wavelength

Optimal for most vertically polarized signals



Horizontal V-Dipole

120 degree angle, oriented nearly parallel to the ground.

Good for receiving certain satellite signals

Starter Kits

- NooElec RTL-SDR v5 Bundle with NESDR Smart and Antennas
- RTL-SDR Blog v3 Bundle with RTL-SDRv3 and Antennas

Supported Configurations

For this series of training courses, you will need, at minimum, a simple antenna and an RTL-SDR compatible receiver (From the RTL2832U Derived or Starter Kits sections above)

Software Controlled Radio

- Operate differently than software defined radios
- Limited to digital signals
- Firmware is configured for digital keying schemes

YARD Stick One

- About $100
- USB-to-Serial interface to the Texas Instruments CC1111
- Gather and transmit digital signals
- Useful for replay attacks against low-power devices

Flipper Zero Sub-GHz

- Sub-GHz module, Texas Instruments CC1101, can record and replay digital signals
- Same family as the CC1111 in Yard Stick One
- Relies on SPI interface instead of USB
- Has a menu-driven interface
- Go watch some TikTok videos

Signals Intelligence Basics (SIGINT)

With military origins, this term traditionally implied spying on the enemy's communications. For civilians, SIGINT can include monitoring local public safety transmissions, "scanning," discovering interesting radio transmissions nearby, and surveying the local radio spectrum as a whole.

Potential Legal Issues

- Electronic Privacy Act of 1986 and other laws prohibit interception of mobile phone and pager signals.
- Some state and local ordinances prohibit the use of radio scanners in cars or to assist in the commission of some other crime (a tack-on charge)

- Plenty of cases to study if you wish to understand how they're enforced and under what circumstances.
    - intercepting pager data on its own is rarely enforced
    - Storing that data, publishing it, or using it to commit a crime is another story

Popular Analog Voice Bands

These frequencies often have a lot of radio chatter.

Licensed:

- Business: ~ 151-155, 450-470 MHz
- Amateur: ~ 144-148, 420-450 MHz
- Aviation: ~ 118-136 MHz

Unlicensed:

- CB: ~ 26.9-27.3 MHz
- FRS: 22 Channels 462-468 MHz
- MURS: 5 Channels 151.8-156.0 MHz

Open-Source Intelligence

It's worth knowing how to gather information about the signals you intercept, or the entities you wish to monitor. I'll cover a long list of sites that can help you research signals and find out what frequencies are being used by organizations nearby.

fcc.gov

The FCC website contains a number of databases useful for comms-curious individuals. You can find details about radio frequencies in use near you, antenna sites and tower owners, detailed technical specifications for any radio hardware sold in the USA, repeater frequencies for amateur, GMRS or businesses, and many other details. Unfortunately, this information is not very well organized, not easily accessible, and the site search feature isn't any better than letting a mainstream search engine find content for you.

fccid.io

FCC ID is a site specifically for browsing FCC's device ID repository. You can find type acceptance certification, testing results, PDFs of manuals, block diagrams, and occasionally even detailed schematics of devices.

radioreference.com

RadioReference is the place to find information about major radio systems in use near you, from businesses to public safety. I use this when I'm in a new area and looking to set up trunk scanning, which I'll cover in module 2 for Windows or Linux.

antennasearch.com

Have you ever seen a big antenna tower and wondered what it's being used for? Given a location or rough address, AntennaSearch will provide details about which entities have

antennas on a given radio tower. Combined with radioreference, you can often cross-reference FCC FRNs and tower locations to help with targeted comms monitoring.

repeaterbook.com

Repeaterbook is also available as a smart phone app, and provides a list of nearby amateur radio repeaters near any location you specify, complete with details you need to program your radio, such as talkgroups, color codes, CTCSS tones and repeater offsets.

MyGMRS.com

MyGMRS provides details about GMRS repeater locations across the USA. GMRS is a seriously underrated service and a lot of areas have good repeater coverage.

SigIDWiki.com

Signals Identification Wiki can help you make sense of what kinds of signals you are receiving, with visual examples of what they might look like in an SDR waterfall, and audio clips of examples

MapRad.io

MapRadio is a relatively new graphical radio license and frequency search that provides FCC license information and other sources in an easy to use manner. It also shows known point-to-point links and expired licenses.

Analog “Waterfall” Tools

- Most peoples’ introduction to software defined radio
- Have many of the same features
- Interfaces are not standardized and can be confusing
- Feature the radio spectrum visualization prominently taking up the majority of the display.

Important Controls

A list of important basic controls to look for in any SDR software.

- Tuner Selection And Setup
- Sample Rate / Bandwidth
- RF Gain / Automatic Gain Control
- Waterfall Diagram
- Panadapter
- Peaks
- Tuner
- Modulation
- Filter Width

- Audio Gain / Volume
- Squelch

Appendix: Popular SDR Tools

Title	Cost	Platform				Notes
		Linux	Win	Mac	Android	
GNURadio	Free	Y				Bare-bones tools for building SDR projects
SDRTrunk	Free	Y	Y	Y		Listening to digital and trunked voice systems
GQRX	Free	Y		Y		Visualize/Listen to signals on Mac/Linux
AirSpy SDR#	Free		Y			Visualize/Listen to signals on Windows - lots of plugins
SDR++	Free	Y	Y	Y	Y	Visualize/Listen to signals - Cross platform, still in beta
SDRAngel	Free	Y	Y	Y	Y	Powerful tool for analog and digital signals (ADS-B, etc) - Cross platform
SDR Touch	$9.99				Y	Visualize/Listen to signals on Android - Easy to use, worth the money
RF Analyzer	Free				Y	Visualize/Listen to signals on Android - Free
RTL_433	Free	Y		Y		Decodes digital data from wireless devices
Kismet	Free	Y				Web-based tool for logging wifi and digital signals
PiAware	Free	Y				ADS-B decoder for aircraft transponders - uploads to FlightAware
dump1090	Free	Y				ADS-B decoder for aircraft transponders - real time web maps
X-Radio ADSB	$2				Y	Android app for real-time mapping aircraft from ADS-B transponders
HackRF CLI	Free	Y		Y		Command line tool for recording and replaying signals with the HackRF One
HackRF_Test	Free				Y	Android-based tool for recording/replaying signals with the HackRF One
rtl-sdr	Free	Y				Command-line tools: rtl_fm, rtl_power, rtl_sdr, and others
Universal Radio Hacker (URH)	Free	Y	Y	Y		Graphical tool for reverse engineering digital signals. Can transmit with HackRF One