Hands-On Software Defined Radio

SDR on the Web

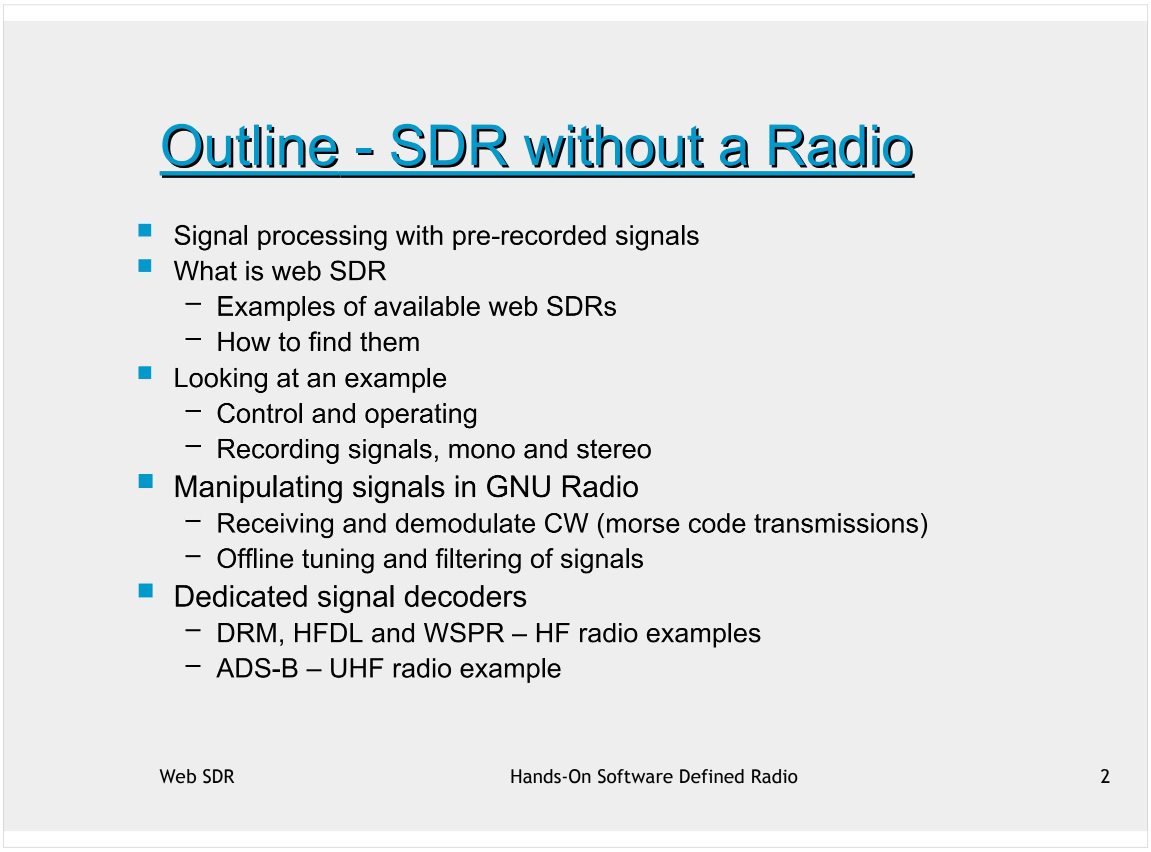
r.ranson@ieee.org

The presentation slides are representative of the more thorough information in the 2 day course "Hands on SDR" from www.radiosystemdesign.com. The slides include various notes added to supplemented the information provided. On some, it is background, and other acronym definitions and other information.

Furthermore some refer to flow graphs for GNU Radio that demonstrate the concepts with actual radio recordings. The presentation describes how the recording of the files are processed.

But to take full advantage of this extra information there is an iso disk image containing all the necessary software and the recorded signals that can be run on you own computer. Goto:

https://radiosystemdesign.com/GettingStarted/



In this context mono is a recording of the filtered and demodulated RF signal, where as stereo is the raw IQ data from the SDR.

Many of the sample signals will be from ham radio. This is because they are plentiful, easy to decode and relatively narrow band. The IQ recordings are necessarily limited in bandwidth and can only capture multiple signals if they are narrow band. It is also an advantage that recordings are also not very large.

DRM – Digital Radio Mondiale

- Digitally encoded HF broadcast service

HFDL – High Frequency Data Link

- World wide HF communication system for aircraft also known as HF-ACARS

WSPR – Weak Signal Propagation Reporter

- Very low power and narrow band signals

ADS-B Automatic Dependant Surveillance – Broadcast

- Secondary radar signal from an aircraft

Additional notes:

Sources of Pre-Recorded Signals

- Other resources for radio signals
- A wiki of numerous different radio signals
  - Each has a characteristic waterfall image and short sample recording
    - *https://www.sigidwiki.com/*
- A very large repository of numerous IQ data files
  - Sorted into broad classification. (100s MB for each category)
    - *http://www.sdrangel.org/iq-files/*
- Various sample files from SDRplay
  - https://www.sdrplay.com/iq-demo-files/
- Any of these files can be played back and processed to get experience of SDR and DSP processing
- All the concepts described for webSDR signals can also be applied to these

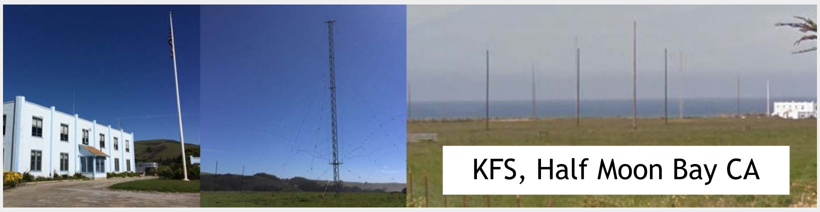
Web SDR　　Hands-On Software Defined Radio　　3

The main emphasis for this presentation is finding and recording your own signal from web SDRs. But all the same ideas can be applied to recording from these sources. It is just that it seems more satisfactory to see, listen and then work with signals that you can obtain 'live' from a radio that you can control.

Additional notes:

SDR without Having a Radio

- Other people's radios are made accessible via the web
  - Accessible using your web browser
  - You can control various parameters
  - Signal streamed directly to your computer
    - *Audio to the sound card*
- Some very large installations
- Some simple ham radio stations
- Some allow you to capture IQ data just as if the receiver were located locally



Web SDR Hands-On Software Defined Radio 4

This is how you can still investigate SDR even without any radio hardware. But for those that have something, the sections towards the end discuss a few radios that I have used.

G0SNB is in the UK, a “Secret Nuclear Bunker” a remnant of the cold war. No longer very secret ;-)

KFS is also an important marine and aircraft communications hub for the pacific ocean and air space.

Additional notes:

SDR Websites

- There are now hundreds of such websites all over the world
- Run by Universities, non-profit organisations and radio amateurs
- Largest groups:
  - WebSDR
  - OpenWebRx
  - kiwiSDR
- All have direct web interfaces accessible from your browser
  - Remote control of frequency, bandwidth, demodulation and filtering
  - Various frequency ranges – LW through to UHF bands
  - Data is sent to your computer
- Many are NOT https so you may get browser warnings
  - Usually OK, but proceed at your own risk

Web SDR Hands-On Software Defined Radio 5

The world map is from https://rx-tx.info/map-sdr-points. To get an idea of scale, the European count is 1057.

There are searchable indices for webSDR, OpenWebRx and kiwiSDR:

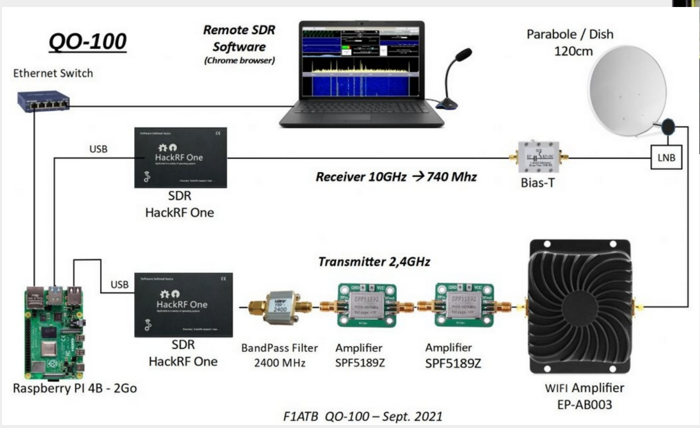
- http://www.websdr.org/
- https://rx-tx.info/map-sdr-points
- http://kiwisdr.com/public/

Note that unfortunately, OpenWebRx only allows downloading of demodulated signals as mp3 files. This precludes any subsequent analysis and so is only useful for listening to radio and not learning about SDR.

Also, there is inevitable latency in all this processing from IP transport, audio and display processing. This can be noticeable in the time to respond to GUI interface commands and in the audio and display time synchronisation.

Additional notes:

WebSDR



- Originated by PA3FWM
- SDR and web server software
- The radios are often custom and some are quite specialised

Web SDR Hands-On Software Defined Radio 6

PA3FWM is an amateur radio callsign for the Netherlands, he is associated with the University of Twente that has one of the longest established web SDRs.

http://websdr.ewi.utwente.nl:8901/

QO-100 is a commercial geostationary satellite that has a transponder for one amateur radio band. Sponsored and paid for by the UAE.

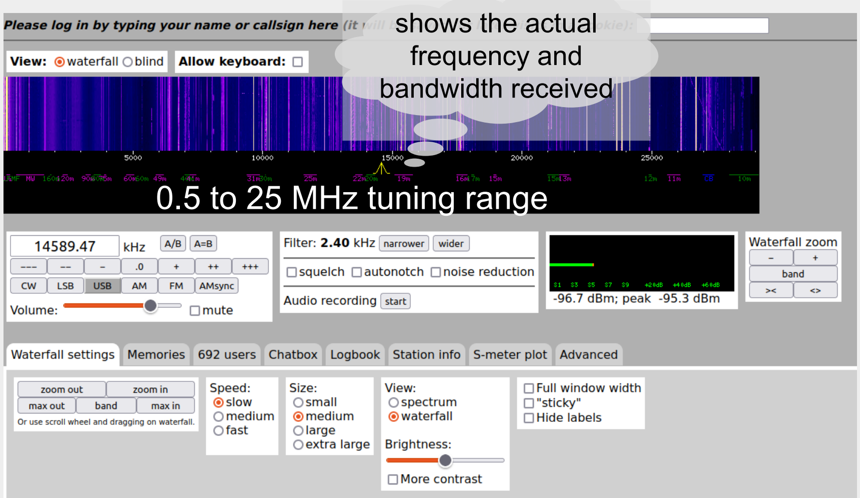
Additional notes:

http://websdr.ewi.utwente.nl:8901/

Waterfall, Tuned Frequency and BW displays

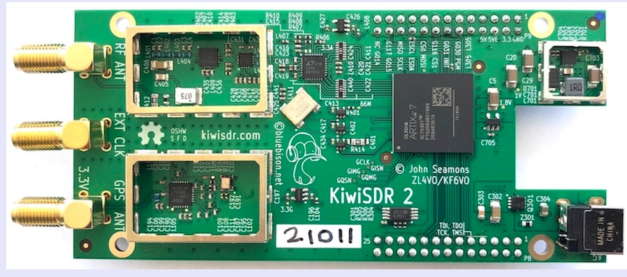
Controls for freq, demod and audio

Many other features

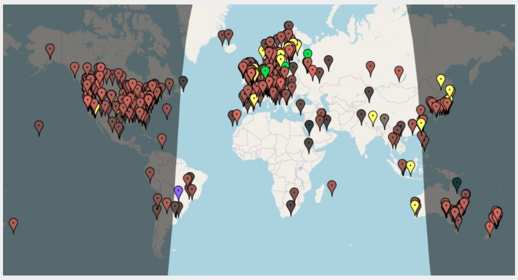


- This is the webSDR at the University of Twente in the Netherlands
  - It can support hundreds simultaneous users

kiwiSDR



- This almost a turnkey application.
  - There is a commercial SDR radio receiver
  - A recognised package of software to run on a PC or SBC
- The web site provides the computer, antenna and web access
- These are all over the world with a variety of capabilities
  - Relatively few simultaneous users
  - Various frequencies
  - Various antennae
- Allows download of raw IQ data



Web SDR Hands-On Software Defined Radio 8

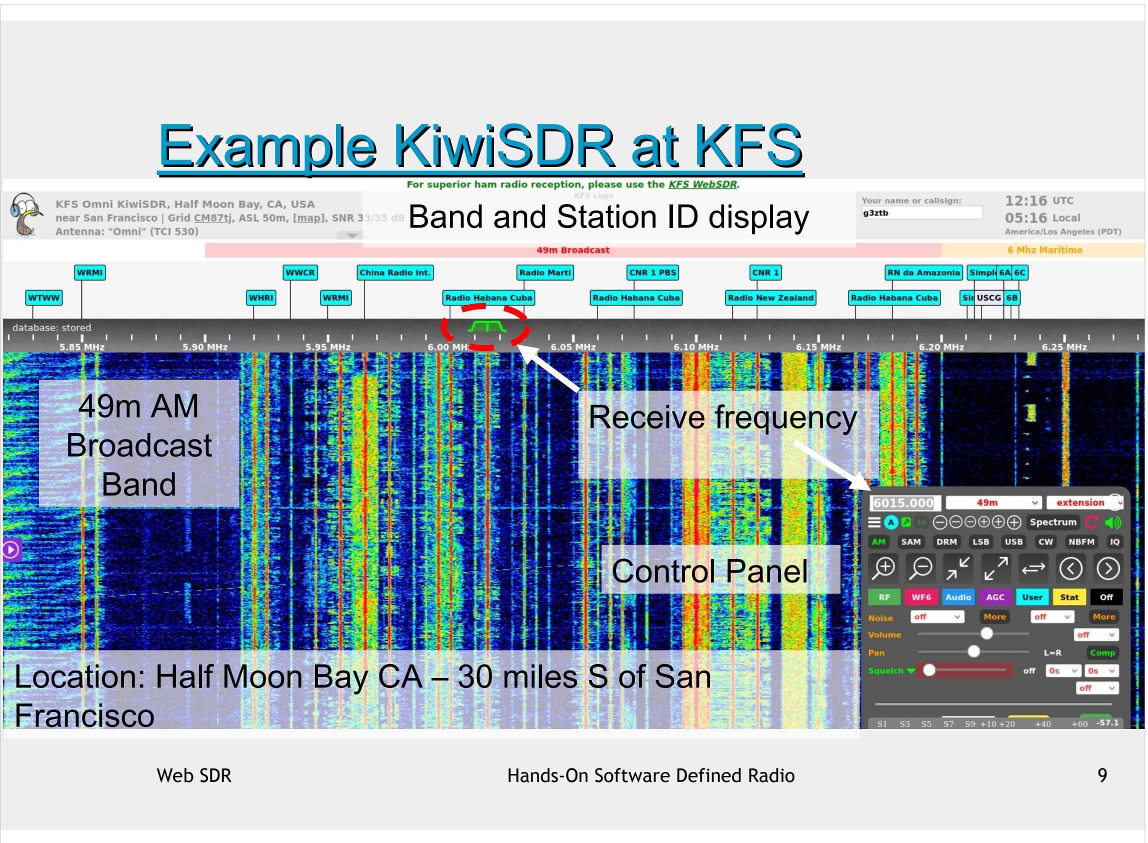
SBC – Single Board Computer

TSL – Transport Layer Security

These systems are all over the world and enthusiasts have put them on the web for you to operate. Pick one, go to the web site and listen to radio ;live from that location.

Note that most of these sites are run by volunteers, do not have TSL security credentials and so are <u>not</u> https. Some browsers will flag a warning, it should not be a problem but it is important to know that in advance

Additional notes:



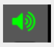
KFS has both webSDR and kiwiSDR servers and can support many simultaneous users.

The AM signals are clearly visible in the waterfall with other stations from all over the world. If you access this, or any other kiwiSDR you can get an idea of controlling the radio, listening to various types of signals.

Additional notes:

KiwiSDR Control

- The control panel lets you ‘operate’ the radio.
  - frequency by value or band
  - or various +/- increments 
- Extensions for various decoders
- Demodulation 

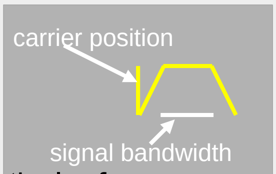
  - Use IQ to obtain raw data, usually 12 kHz, signed 16 bit little endian
- Local audio 
- Recording to a local file 
- There are many other controls 

  - That are then displayed on the panel below

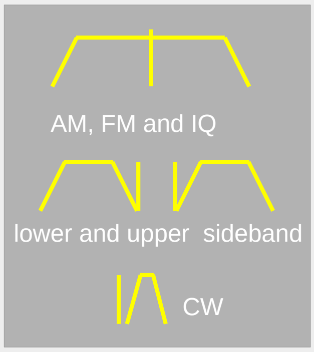
The IQ mode is that one used for the demonstrations in this presentation.

Additional notes:

Recording Radio Signals



- WebSDRs allow you to tune into a signal at a particular frequency
  - All deliver filtered demodulated sound to the browser
  - Coloured markers show the tuned frequency and BW
- WebSDRs have different recording facilities
  - Various data formats and sampling rates
- All receive and filter signals with selectable demodulation schemes
  - AM, SSB (USB or LSB), FM, CW etc
  - IQ when available is not demodulated
    - *Raw IQ sampled data usually at 12 kHz*
- Recordings go to a .wav file
  - Mono is the filtered demodulated audio
  - Stereo when IQ data is available



Web SDR Hands-On Software Defined Radio 11

AM – Amplitude modulation

SSB – Single Side Band (suppressed carrier)

FM – Frequency modulation

CW - Carrier wave (Morse code signals)

It is important to note the position of the carrier relative to the modulation. For CW the the carrier is always added below the signal. Bands usually have a preferred sideband designation. Ham radio uses LSB for signals less than 10 MHz.

There are other possibilities

WBFM is wide band FM, used by broadcast radio stations

NBFM is narrow band FM, used by many voice only radio services

SSB signals are designated as LSB or USB, upper or lower sideband respectively

IQ is raw sampled data without any demodulation with the streamed containing alternating I, Q data values encode as L/R stereo

Additional notes:

Using Recorded Signals

- Recorded radio signals can be used to dig further into SDR and DSP
- Wav files can be processed with other tools
  - e.g. use ‘aplay’ to listen and see recording parameters
  - Imported to GNU Radio via Wav Source block
- Other radio may have other formats
  - Notably the popular RTL based radios are 8 bit unsigned
- The best way to investigate further is to import the signals into GNU Radio
  - A few examples are given to demonstrate the key ideas
- Also, note that there is an attempt to standardise recording as SigMF
  - A data/meta_data file pair that captures key parameters

Web SDR   Hands-On Software Defined Radio   12

DSP – Digital Signal Processing

‘aplay’ is a standard audio playback program in Linux, use man aplay to find out more.

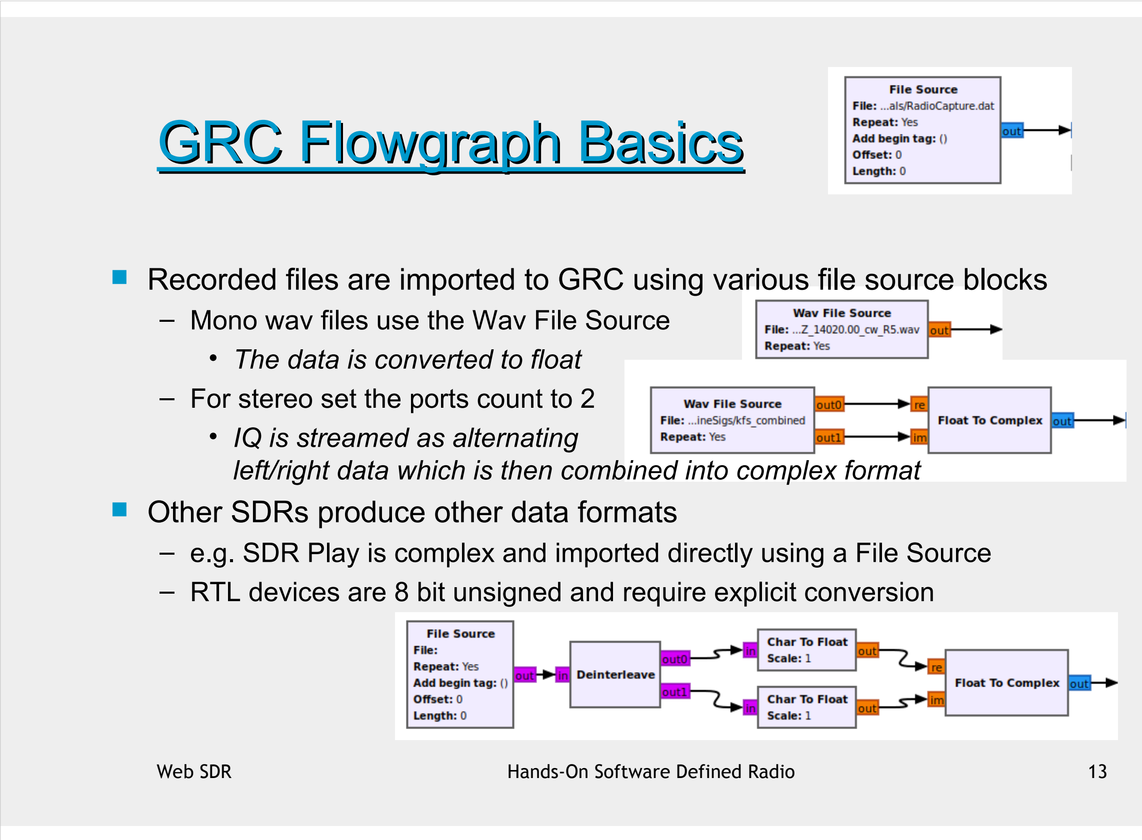
The open source SigMF initiative is intended to help users of recorded SDR data. Wav files include some of this data, but it is often insufficient.

- The data file is essentially raw data in some binary format
- The meta data specifies the binary format, number of channels, sampling rate, radio tuned frequency and many other optional parameters

SigMF is an initiative started from GNU Radio and also has open source tools to work with the files. This can be downloaded and used indepedently.

- https://github.com/miek/inspectrum a spectrogram view of signals with zoom/pan, filtering and de-modulation facilities.

Additional notes:



GRC – GNU Radio Companion, the graphic user interface for GNU Radio.

Flowgraph is the term used for a sequence of DSP blocks defined in GRC to represent a system. See https://www.gnuradio.org/news/2022-02-03-new-tutorials/

This part of the presentation is focussed on using GNU Radio. It can be installed on various platforms using the information from gnuradio.org
https://wiki.gnuradio.org/index.php/InstallingGR

Alternatively, as a quick and easy start, GNU Radio and the other files used in this presentation can be downloaded as a ubuntu live distribution, bootable from a USB memory stick. Look at the SDR_StarterGuide.pdf file in the zip that was downloaded to find out more.

Additional notes:

Example Recordings

- There are a few recording included on the USB drive
  - Used to demonstrate some key ideas
- G0SNB – files from that kiwiSDR
  - Mono recordings are audio only after filtering and demodulation
    - *CW1 an example of what the signals look and sound like*
    - *CW2 a flow graph to visually see the Morse characters*
  - Stereo recordings are in 12 kHz bandwidth
    - *CW1 captures several signals simultaneously*
    - *CW2 a flow graph to tune to one of the signals captured*
    - *SSB there is just enough BW to capture 2 voice signals*
      - Demonstrates tuning, just as if the SDR were right in front of you

Morse code is still in use and is a surprisingly effective method of communications. It is a very narrow band signal ideal for demonstrating concepts within the limited 12 kHz of signal capture bandwidth.

Additional notes:

g0snb mono CW1

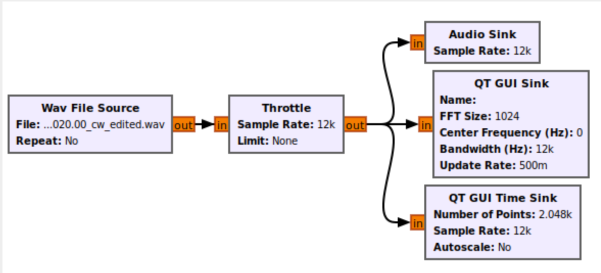
- Mono recording just captures the audio from the remote radio
  - Basic example shows importing a wav file into GRC
  - You can hear the signal just as if from the web SDR
- Frequency plot show a signal at ~ 500 Hz
  - A real signal has a symmetric frequency domain representation
  - You can zoom in to see the details of the signal and adjacent spectrum
- Waterfall display shows 12kHz BW
  - The signal itself and ~±500 Hz of noise
    - *This is the spectrum after the CW filter in the remote radio*
  - You can adjust the sliders an see the Morse symbols
- The time display shows the on/off keyed RF signal clearly
  - It is either noise (off) or a single sine way (on)
    - *Note the on time has a noticeable rise and fall time as well*
  - You can distinguish the 3:1 dash:dot symbol ratio

Web SDR Hands-On Software Defined Radio 15

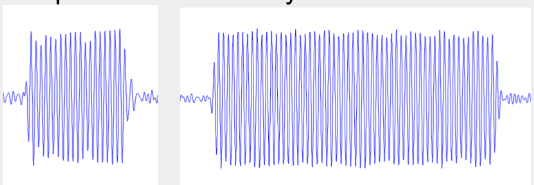
Slides with title like this one refer to the GRC flowgraph file to use. Each one will also access a particular recoding that was made especially for this presentation.

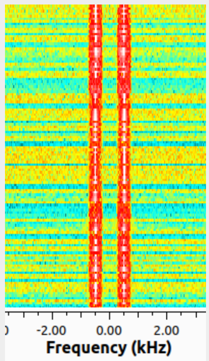
Additional notes:

CW1 Example



- Using the flowgraph g0snb_mono_cw1
- Plays the recorded signal through the sound card (audio sink)
- The GUI blocks show features of the signal
  - The waterfall display
  - The noise bandwidth of the receive filter
  - CW envelope and dot / dash symbol in times





- You will need GNU Radio to use this file

Web SDR Hands-On Software Defined Radio 16

The waterfall display shows the frequency spectrum magnitude in time with separate ‘snapshots’ as colour coded lines in time flowing down the chart. Since mores code is an on/off signal in time it appears as different coloured dots and dashes vertically in the waterfall. Note also that amplified noise in the signal bandwidth is also visible as another solid colour strip.

Also, this is not an IQ signal, so the spectrum is symmetric about 0 Hz.

The flowgraph for this example should load the recording

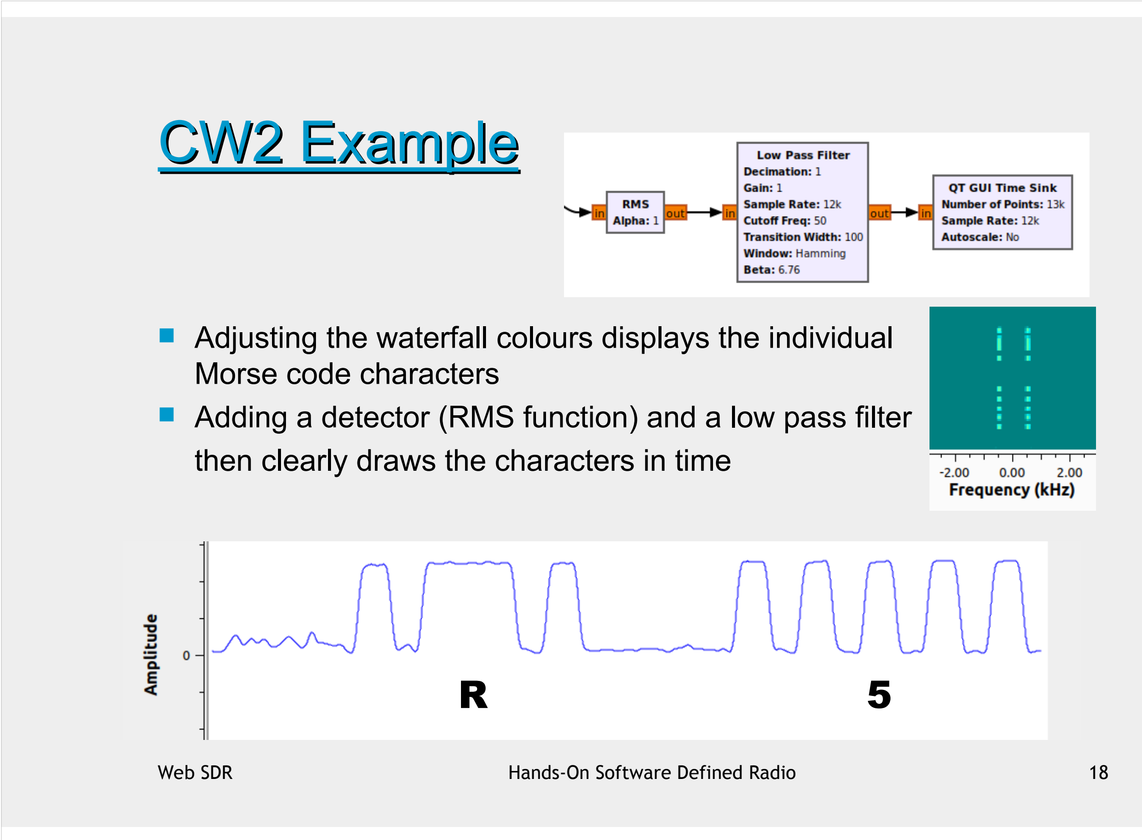
sdr.gb0snb.com_2025-03-12T14_29_40Z_14020.00_cw.wav

The file name is auto generated by the kiwiSDR using the web name, the recording time and the center frequency of the recording. The sampling rate is assumed to be 12kHz.

Additional notes:

G0snb mono CW2

- A short section of the recorded signal has been edited out
  - The wave file source repeats this over and over
- The RF signal is detected by taking the RMS value and filtering
- You should be able to hear the message
  - dir dah dit <pause> dit dit dit dit dit - this is R 5
- And the time sink shows the message as well
  - dot dash dot space dot dot dot dot dot
- Also see the timing of the symbols relative to that of a dot
  - On 1 dot time for a dot
  - Off 1 dot time between symbols in the same letter
  - On 3 dot times is a dash
  - Off 5 dot times between separate letters
  - fyi - Off 7 dot times between letters of words (not shown)



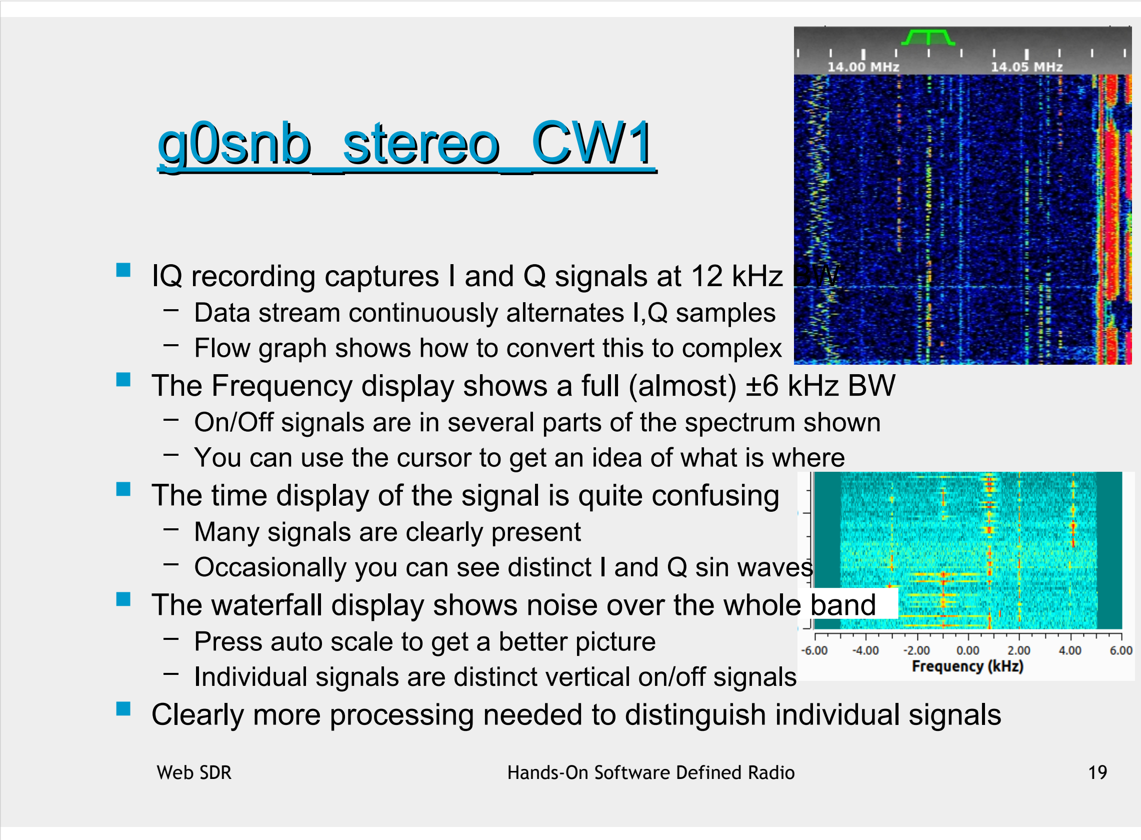
The flowgraph for this example should load the recording

sdr.gb0snb.com_2025-03-12T14_29_40Z_14020.00_cw_R5.wav

It is actually the previous recording edited by audacity to extract the section containing the short sample shown.

The RMS and filter blocks act as an AM detector, rectifying the RF and then filtering to only 50Hz in order to extract the Morse symbols.

Additional notes:



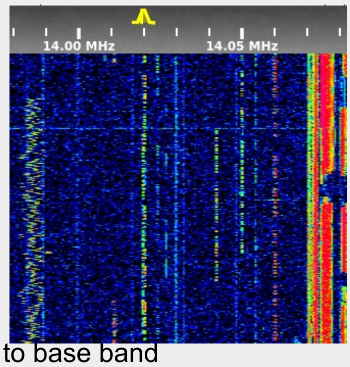
The flowgraph for this example should load the recording

sdr.gb0snb.com_2025-03-21T16_4

The SDR hardware captures 48 kHz of bandwidth and that is visible on the spectrum frequency axis. That is filtered to 12kHz in the section of the band under the yellow marker and sent to the web browser. Even that 12 kHz audio is quite confusing because many signals are present at once. The next example illustrates the kind of frequency shifting and filtering used in an SDR to extract just the one wanted signal.

Additional notes:

g0snb_stereo_CW2



- Base band signal processing example
  - The filter has a tunable center frequency controlled by the slider
  - Filter is 200 Hz wide and translates the signal to base band
- The same function as provide in the webSDR in CW mode
- The RMS and low pass filter from before to show the Morse symbols
- Try to identify three different signals
  - At 300
  - At -1.5kHz
  - At -3.7k

The flowgraph for this example should load the recording

sdr.gb0snb.com_2025-03-21T16_49_04Z_14023.00_iq.wav

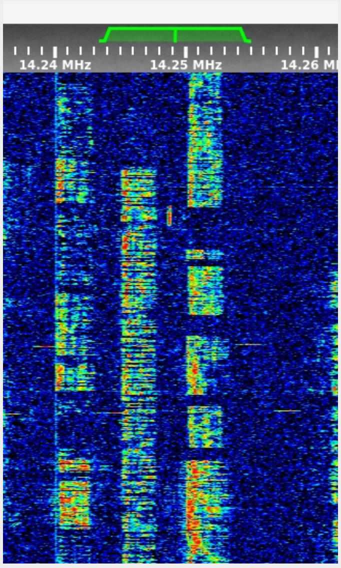
This is the most complex flowgraph used in this presentation. It should help to isolate groups of blocks that you recognise from before. The key part is the Frequency Xlating FIR Filter that translates part of the input spectrum to the audio band and reduces the bandwidth to 500 Hz.

Unfortunately,because of the different filtering, decoding and display update rates, it is almost impossible to synchronise the audio with the time display. But even so it should be possible to identify several individually distinct signals in the crowd.

Additional notes:

g0snb_ssb_translate

- Signal in the 20m band at 14249 kHz
- The three stations communicating TDD
  - Sharing the same channel
  - Taking turns to speak
  - The convention is to use USB in this band
- The most left hand signal is not captured in the IQ receive BW
- The GRC flow graph allows tuning of a 2.4kHz BW filter across the band
  - 2 different voice channels can be heard
- You have to adjust the tuning frequency to get the correct tone for the voice
  - -4.2 kHz SP3TYJ
  - +0.8 kHz IZ7DOK



Web SDR   Hands-On Software Defined Radio   21

SSB – Single Side Band (suppressed carrier)

USB – Upper Side band

TDD – Time Division Duplex

The flowgraph for this example should load the recording

sdr.gb0snb.com_2025-03-17T16_29_03Z_14249.26_iq.wav

The IQ bandwidth is just wide enough to capture 2 SSB signals (nominal BW 2.4kHz each). The frequency translating filter moves the spectrum by the f0 slider value and only passes 0 to 2.4 kHz above that frequency.

The radio button allow you to connect the audio to either the filtered or full band version. With the right tuning the filtered version is quite clear, but on full band you can possibly distinguish the 2 different voices, but they are also shifted in frequency, so they are not at all comprehensible.

Additional notes:

Other webSDR Capabilities

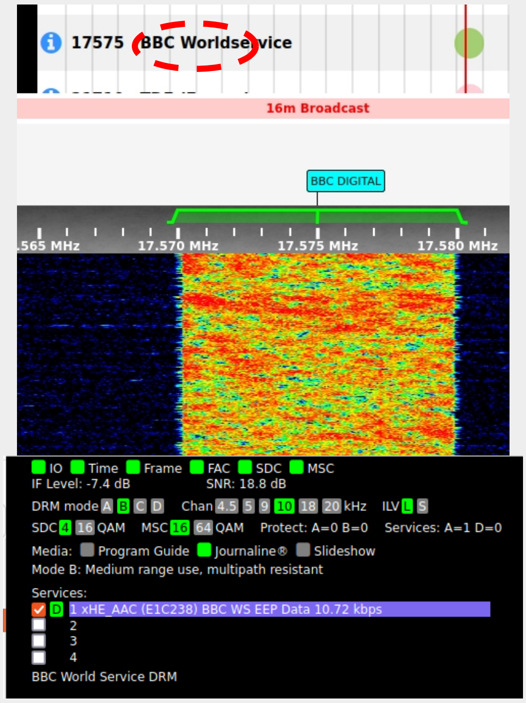
- Many webSDRs have other interesting signal decoders available
  - All the processing is done by DSP in the SDR software.
- DRM – This is a digital encoding of HF broadcast services
  - Intended to be more efficient in BW and to combat fading
- HFDL – A world wide HF packet communications system for aircraft
- WSPR – A very narrow band HF propagation experiment
- ADSB – Live aircraft tracking data
- For illustration only
  - These signals are not usually recordable, and the decoding in GNU Radio is beyond the basic capabilities illustrated so far.
  - There are however dedicated software packages available if you wish to experiment with these using your own SDR

The BBC is by no means the only broadcaster to transmit this kind of service. Many others are available.

Additional notes:

DRM

- BBC DIGITAL
  - World Service Programs
- KiwiSDR in New Zealand
  - ZL4MD
- Top window shows a timeline and station broadcast times
- Water fall shows the digitally encoded signal
- Lower window shows the digital signal information
- The program comes out via the audio



Web SDR Hands-On Software Defined Radio 23

DAB - Digital Audio Broadcast

DRM - Digital Radio Mondiale

Just like DAB, there are dedicated radios for this kind of signal.

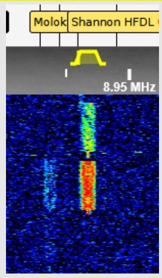
The key goal of DRM is to provide FM quality (not fidelity) reception via HF where fading and multipath severely hampers traditional AM broadcast.

Additional notes:

HFDL

- HF Data Link
  - short messages
  - characteristic sound
- Flight tracking info
- This is from Shannon Ireland
- Other stations round the globe
- This packet for flight UAE4PV at 16:46 March 14 2025
  - Flight tracker data shows that this is en route from Milan to New York

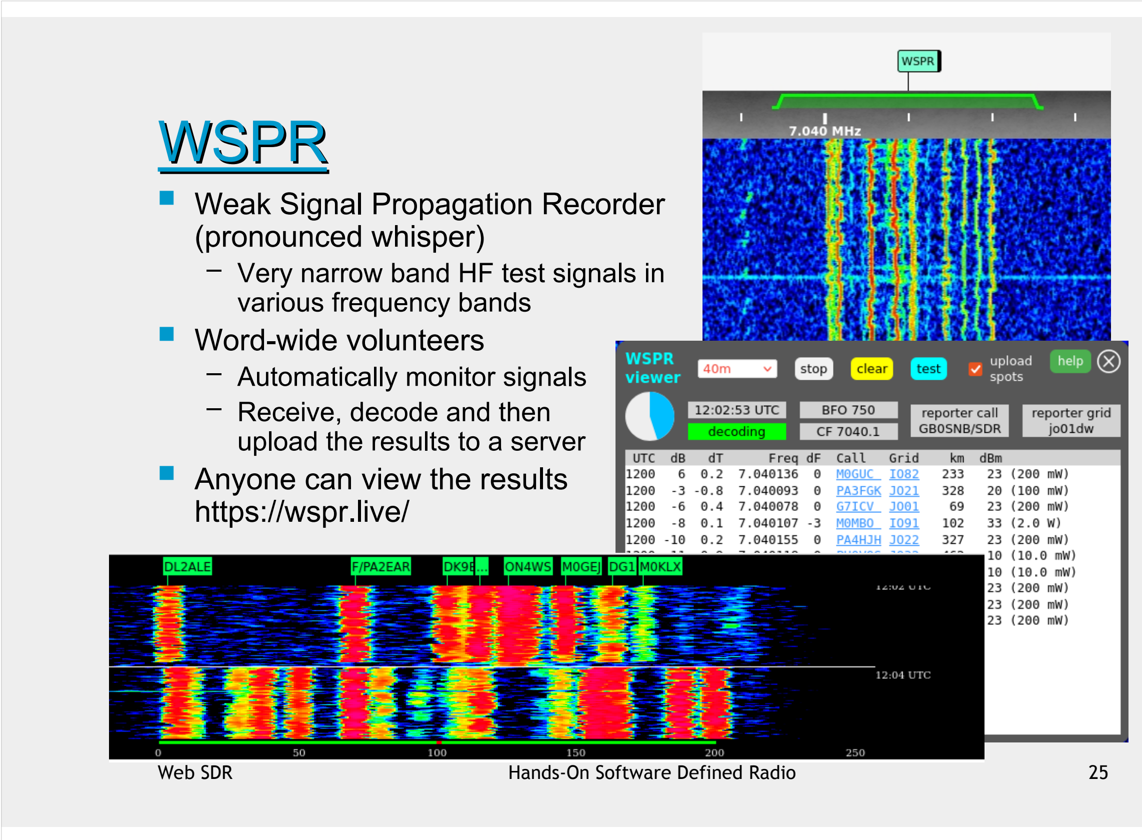
```
[2025-03-14 16:46:51 UTC] [8942.0 kHz] [-1.9 Hz] [-12.2/-32.0 dBFS] [19.9 dB] [300 bps] [S]
Downlink LPDU:
 Src AC: 174
 Dst GS: Shannon, Ireland
 Type: Unnumbered data
 Performance data:
  Version: 18
  Flight ID: UAE4PV
  Lat: 50.2652936
  Lon: -10.5877506
  Time: 16:46:46
  Flight leg: 245
  GS ID: Shannon, Ireland
  Frequency: 8843.0
  Frequency search count:
   This leg: 0
   Prev leg: 196
  HFDL disabled duration:
   This leg: 9462 sec
   Prev leg: 21410 sec
  MPDUs received             : 300 bps: 167   600 bps:  29   1200 bps:   0   1800 bps:   0
  MPDUs received with errors : 300 bps:   5   600 bps:   2   1200 bps:   0   1800 bps:   0
  MPDUs transmitted          : 300 bps:  10   600 bps:   2   1200 bps:   0   1800 bps:   0
  MPDUs delivered            : 300 bps:   9   600 bps:   1   1200 bps:   0   1800 bps:   0
  SPDUs received: 192
  SPDUs missed: 10
  Last frequency change cause: 7 (No change)
```



You can listen a data sample here:
https://www.sigidwiki.com/wiki/High_Frequency_Data_Link_(HFDL)

This is captured using a kiwiSDR site and a plugin that can show just the basics. There are dedicated software packages that can show other details of the data packet and merge it with maps and other flight traffic information. e.g. dumphfdl and PC-HFDL

Additional notes:



The WSPR experiment has dedicated frequency allocations in each of the amateur radio bands. Each allocation is only 200 Hz wide, with individual signals only a 6 Hz wide; so the transmit signal has to be very accurate and the receive filtering of only a few Hz is only practical because of DSP.

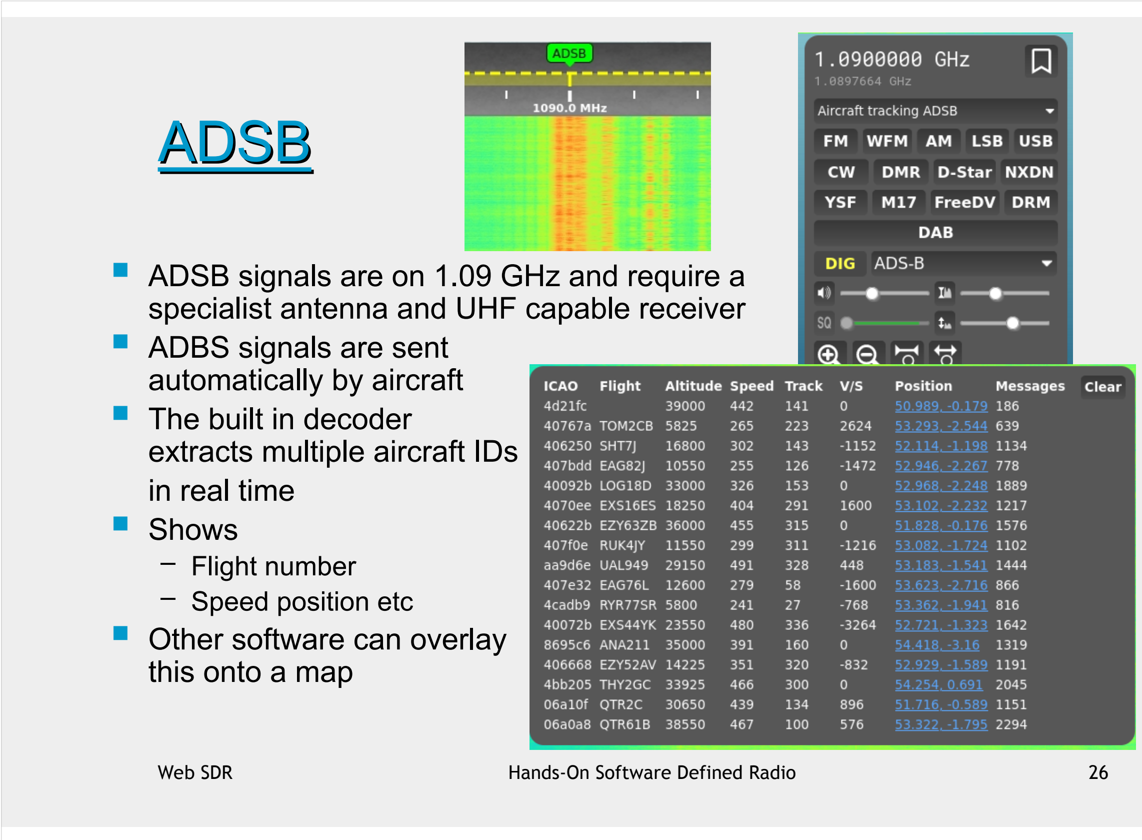
The signal is a standardised message containing the station call sign, location and transmission power. All in all only 50 bits sent, which is forward error corrected (FEC) coded in ~6 Hz of bandwidth and taking almost 2 minutes. You have to be patient to see the first decode. That is what the timer is for.

The idea is to send and detect very weak signals (hence the narrow bandwidth) world wide; then link transmitter and receiver information and understand propagation.

The receive signal and location information is called a ‘spot’ and these are uploaded to a central server where anyone can see the results and download the data for further analysis.

All this is open source so if you are interested in how FEC works then look this up fopr more detail.

Additional notes:



ADSP is a type of secondary radar, essentially a transponder that detects a primary radar signal and returns another signal notifying the primary of additional information.

This site from G4WIM is under construction but operational.

It has an ADSB decoder built in and is an openWebRx accessed from: http://g4wim.proxy.kiwisdr.com:8073/

Which then links to http://dowbrook.duckdns.org:8073/

You can see from the table the additional information is things like flight number, altitude, air speed etc.

Additional notes:

Summary

- You do not need a radio to investigate SDR
- Very capable radio hardware is made available, largely by volunteers
  - Mostly HF, but other bands are available
- You can control the key radio parameters from anywhere
  - All via a standard web browser
  - Listen to and record demodulated signals
- Also record raw IQ data signals or further processing
  - CW (Morse code), SSB (basic telephony)
- Process with GNU Radio
  - Demonstrating demodulation
  - Tuning and selecting separate parts of the recorded signal
- Other examples using dedicated decoders
  - Broadcast services, packet data services and propagation experiments
- For further information there is a 2 day Hands on SDR course
  - www.radiosystemdesign.com/Hands-on-SDR

Additional notes:

Hands on SDR - Objectives

- Basic theory supported by experimental studies using real hardware
  - Illustrating theory via practical exercises
- Cover all the essential features of a DSP radio system
  - Creating a digital base band signal and transmitting it
  - Receiving digital modulation, synchronisation and decoding
- Along the way understanding:
  - Sampling
    - *Understanding this is the bridge between analogue and digital worlds*
  - Filtering
    - *Extracting what you want from all this data*
  - Sample rate changes
    - *Efficient processing of digital signals*

Receiving Hands-On Software Defined Radio 28

You can find out more about the Hands on SDR course from www.radiosystemdesign.com.
Or email r.ranson@ieee.org

Additional notes:

Hands on SDR – Day 1

- Introduction
  - Using a common computer environment for experimentation
    - *All applications installed with other support files on the SD card*
  - Using Pluto, a single TRx providing all the hardware for investigating SDR
- Sampling
  - Faster sampling adds noise but better defines the signal
    - *a net SNR improvement*
  - Quantisation, the added noise and detecting signals less than 1 LSB
- Filtering
  - Basic FIR filter design
  - GNU Radio Filter designer shows may other types of filter
  - Specialty filters – half band, raised cosine etc

Hands on SDR – Day 2

- Scaling
  - Altering the sampling rate without distorting the signal
    - *Decimation with filtering before the operation to remove aliases*
    - *Interpolation with filtering after the operation to remove spectral copies*
- Transmitting
  - Generating the digital baseband using GRC
    - *QPSK as a simple example*
  - Using interpolation and Pluto to create an RF signal
    - *Raised cosine filtering to eliminate inter-symbol interference*
- Receiving - putting it all together
  - Filtering at Tx and Rx to minimise ISI
  - Clock recovery, timing sync, frequency correction and combatting channel impairments via DSP blocks
  - Demonstrating a complete bits to antenna and back radio system