# Introduction to SDR & the Wireless Village

DEFCON
2015

# Who the Frig...

satanklawz

DaKahuna

# It takes a village...

Rick Mellendick
Zero_Chaos
Marauder
Terrible

RedBaron
SimonJ
Spiral Suitcase
0xAA

# Agenda for the next 45 minutes

- Ham Radio Transceivers
- SDR Rx/Tx
- Antenna Theory from Ham to SDR
- The (S) in SDR
- Common problems with SDR Labs
- A bit of fun
- Take all this stuff to the Village

# Materials Checklist if you wanna follow

- RTL-SDR
- Modern Laptop
- Pentoo
- Headsets
- Antennas

# Oops...

Don’t have something?

## DEF CON Vendors

Hacker Warehouse Hak5

Nuand SimpleWiFi

## Fry’s Electronics

**Address:** 6845 S Las Vegas Blvd, Las Vegas, NV 89119

**Phone:**(702) 932-1400

**Hours:** 9:00 am – 8:00 pm

# HAM Radio Transceivers –  Fixed

Frequencies:  HF, VHF, UHF, VHF/UHF

Power Output: 100 – 200 Watts

Cost:  $1,000 and up

Source:  http://digichar.com/unt/17066-yaesu_ft___901dm_hf_ham_radio_transceiver.html

http://www.airadio.com/Icom-Transceiver-IC-7800*productID_293-products_details

# HAM Radio Transceivers – Mobile

Frequencies: HF, VHF, UHF, VHF/UHF

Power Output: 40 – 50 Watts

Cost: $300 - $500

Source: http://www.hamradio.com

# HAM Radio Transceivers –  Handheld

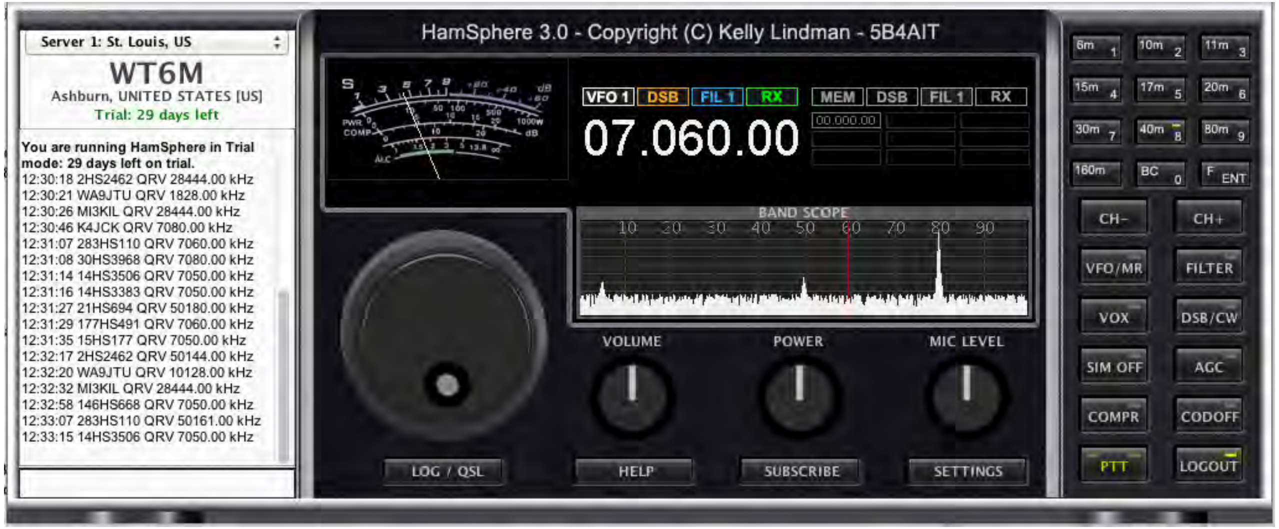
Frequencies:  VHF, UHF, VHF/UHF

Power Output: 4 – 5 Watts

Cost:  $35 - $300

Source: http://www.hamradio.com

# HAM Radio Transceivers - Virtual



```
You are running HamSphere in Trial
mode: 29 days left on trial.
12:30:18 2HS2462 QRV 28444.00 kHz
12:30:21 WA9JTU QRV 1828.00 kHz
12:30:26 MI3KIL QRV 28444.00 kHz
12:30:46 K4JCK QRV 7080.00 kHz
12:31:07 283HS110 QRV 7060.00 kHz
12:31:08 30HS3968 QRV 7080.00 kHz
12:31:14 14HS3506 QRV 7050.00 kHz
12:31:16 14HS3383 QRV 7050.00 kHz
12:31:27 21HS694 QRV 50180.00 kHz
12:31:29 177HS491 QRV 7060.00 kHz
12:31:35 15HS177 QRV 7050.00 kHz
12:32:17 2HS2462 QRV 50144.00 kHz
12:32:20 WA9JTU QRV 10128.00 kHz
12:32:32 MI3KIL QRV 28444.00 kHz
12:32:58 146HS668 QRV 7050.00 kHz
12:33:07 283HS110 QRV 50161.00 kHz
12:33:15 14HS3506 QRV 7050.00 kHz
```

HamSphere

- Java Based (Windows, OS X,
- Just add microphone (headset recommended)

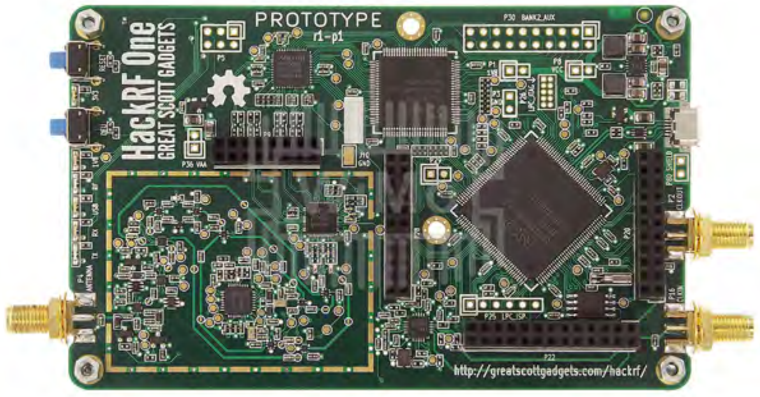
# HAM Radio Transceivers - SDR

BladeRF(Nuand)

- Frequency: 300Mhz-3.8Ghz
- Power:  ~6 dBm (4 mW)
- Cost: $420(x40) $650 (X115)

HackRF (GreatScott Gadgets)

- Frequency: 1Mhz – 6 Ghz
- Power: 0-15 dBm (1-32mW)
- Cost: $330



# HAM Radio Transceivers (cont’d)

Interesting uses:

- Satellite communications
- Earth-moon-earth (EME)
- Packet Radio
- Radio Teletype (RTTY)
- Internet Radio Linking Project (IRLP)
- Morse Code

# SDR Rx/Tx

RTL-SDR ; RX only

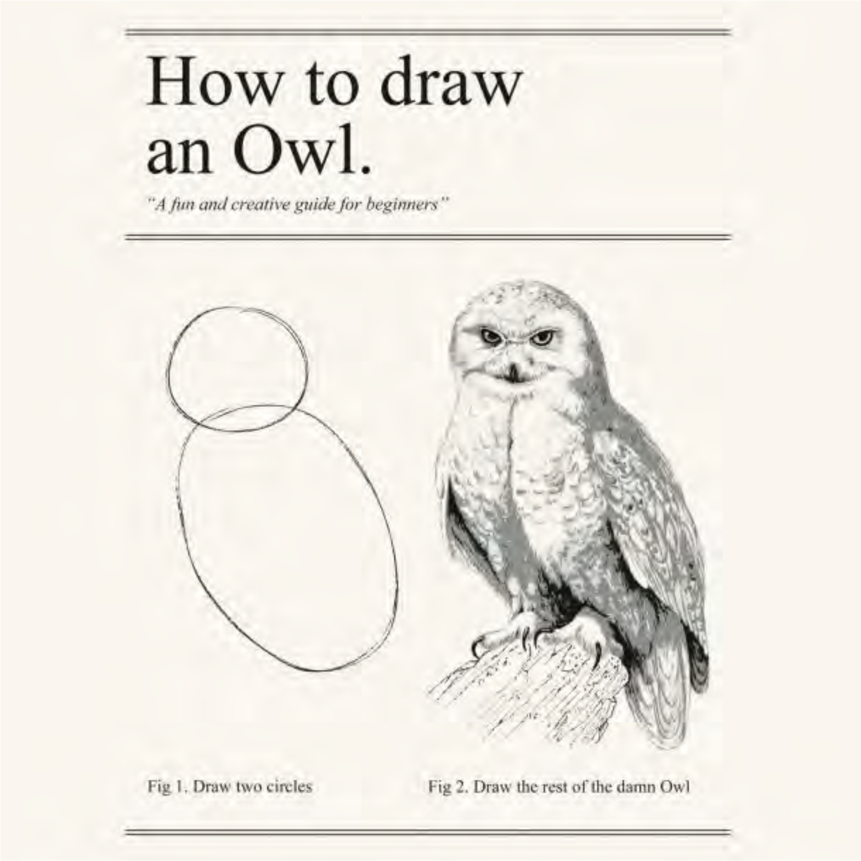
HackRF ; TX and RX capable SDR board that’s hugely affordable

BladeRF ; TX and RX in an affordable solution

USRP ; the nuke

Hacks ; RaspberryPi, etc

# SDR 101 in One Slide



How to draw an Owl.

*"A fun and creative guide for beginners"*

Fig 1. Draw two circles

Fig 2. Draw the rest of the damn Owl

# What ‘is’ Software Defined Radio?

- Radio front end
- No dedicated IC back end for decoding radio signal
- Digitize signal and pass it all to the host system
- In theory, if you can tune it, you can be that type of radio

# SDR Captured Data

- No packets - just raw data
- Raw radio samples of some bandwidth per sample
- Bandwidth defines amount of spectrum covered by samples

# IQ Data

- SDR data commonly called “IQ”
- **I**maginary and **Q**uotient components of signal
- Two-part sample consisting of amplitude and phase
- Sampling only amplitude gives a signal at a time - but no idea about frequency
- Fancy trig gets us signal at specific time

# Choose Your Weapon

- Bit depth of samples (usually 8 or 16 bit) determines fidelity, much like 16 bit color
- Sample width, such as 200KHz or 20MHz, defines how much spectrum can be captured at a time
- Frequency range, such as 30MHz to 4GHz, defines the range the radio can be tuned to

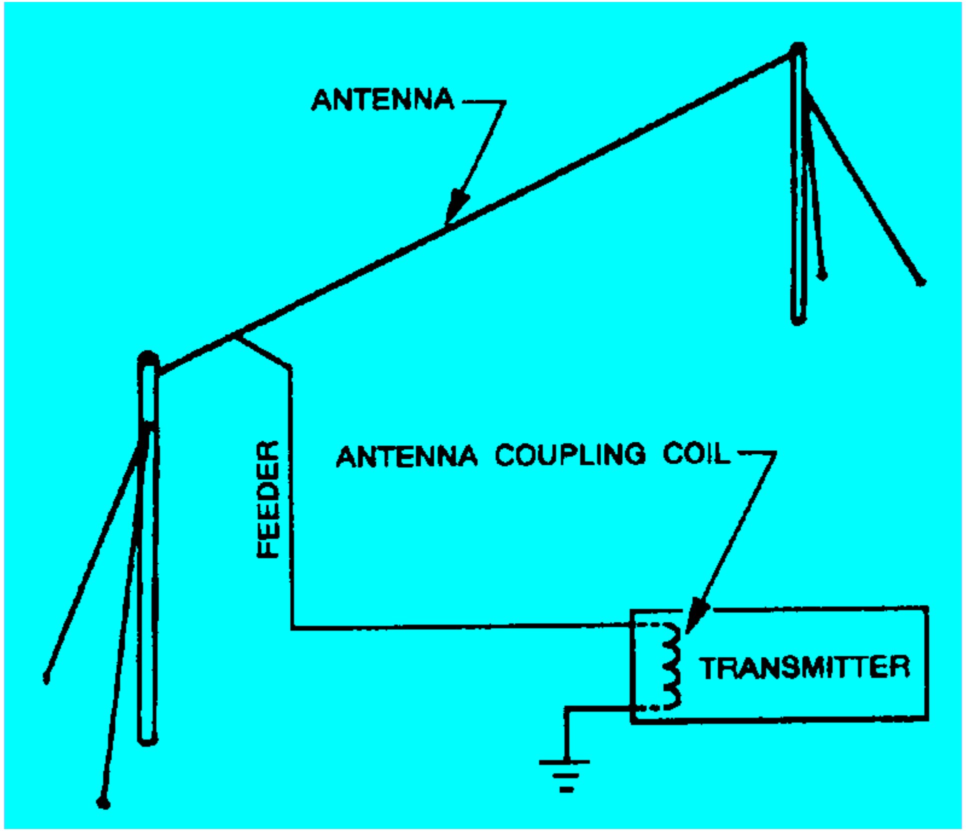
# Antenna Theory from HAM to SDR

ANTENNA - noun:

A piece of metal which conducts electricity

Radiates and receives the signals

# Antenna System



# Antenna System (cont)

Antenna Systems Must Match Transmitter

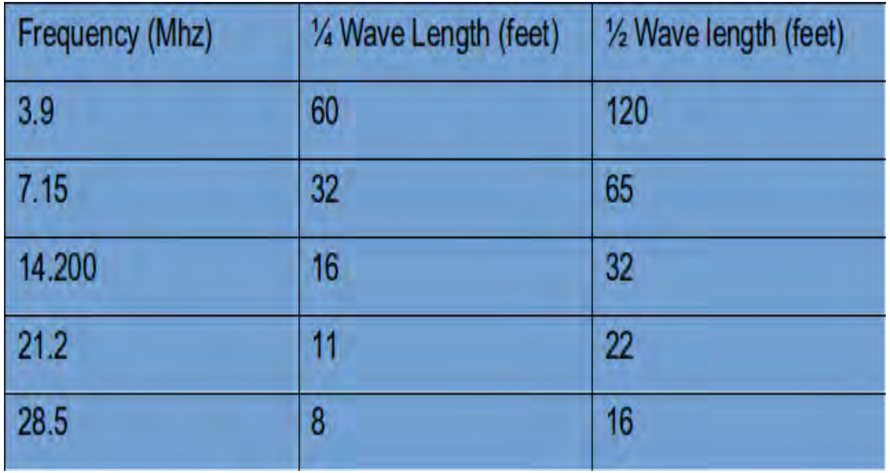
- Prune length
- Antenna tuner
- Matching Section

Polarization

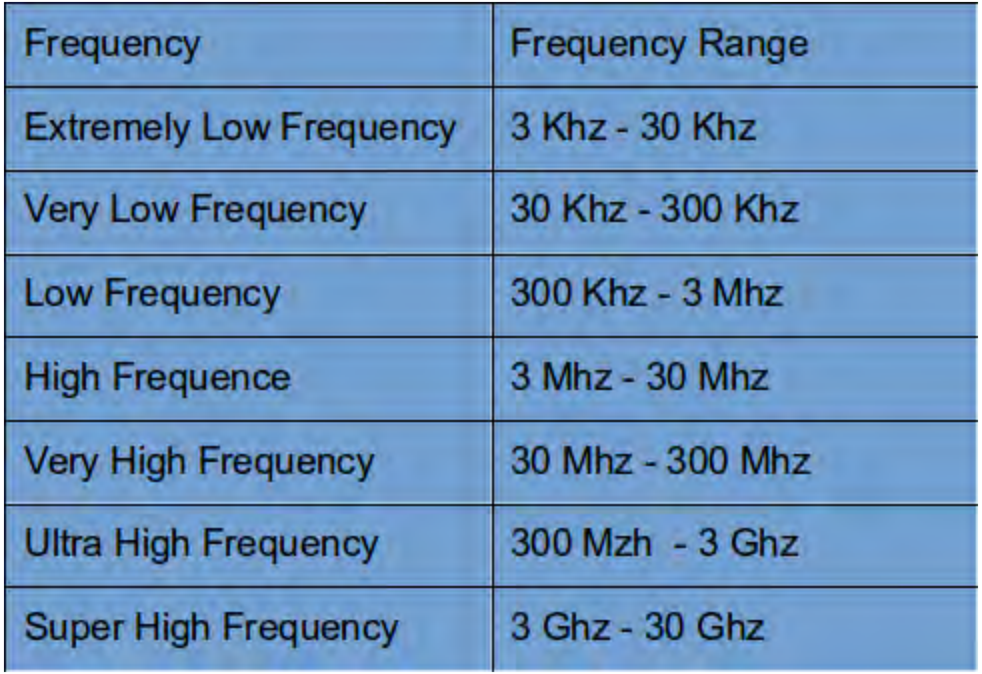
- Horizontal
- Vertical
- Circular

# Calculation crash course

v = f * λ
speed = wavelength * frequency



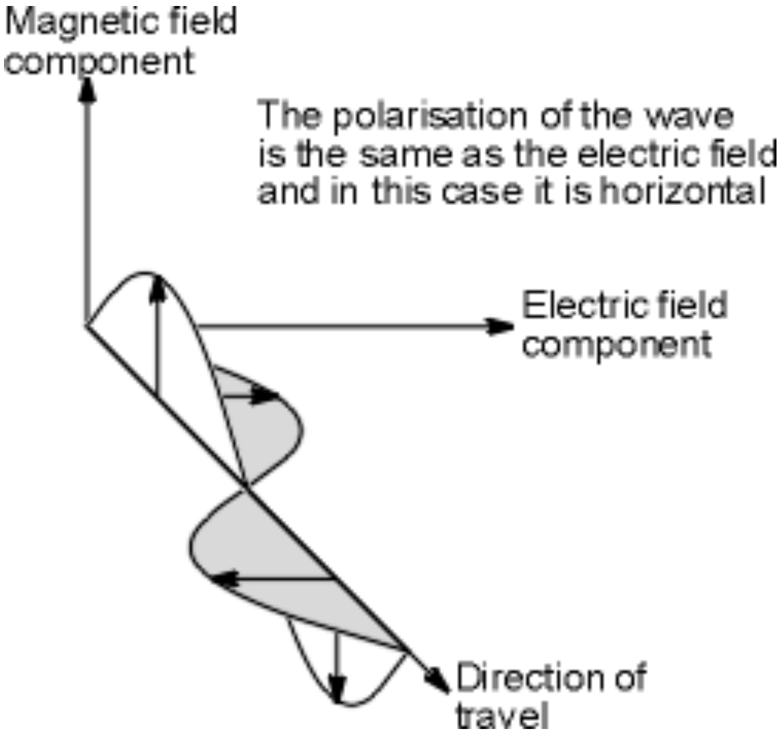
| Frequency (Mhz) | ¼ Wave Length (feet) | ½ Wave length (feet) |
|---|---|---|
| 3.9 | 60 | 120 |
| 7.15 | 32 | 65 |
| 14.200 | 16 | 32 |
| 21.2 | 11 | 22 |
| 28.5 | 8 | 16 |



| Frequency | Frequency Range |
|---|---|
| Extremely Low Frequency | 3 Khz - 30 Khz |
| Very Low Frequency | 30 Khz - 300 Khz |
| Low Frequency | 300 Khz - 3 Mhz |
| High Frequence | 3 Mhz - 30 Mhz |
| Very High Frequency | 30 Mhz - 300 Mhz |
| Ultra High Frequency | 300 Mzh - 3 Ghz |
| Super High Frequency | 3 Ghz - 30 Ghz |

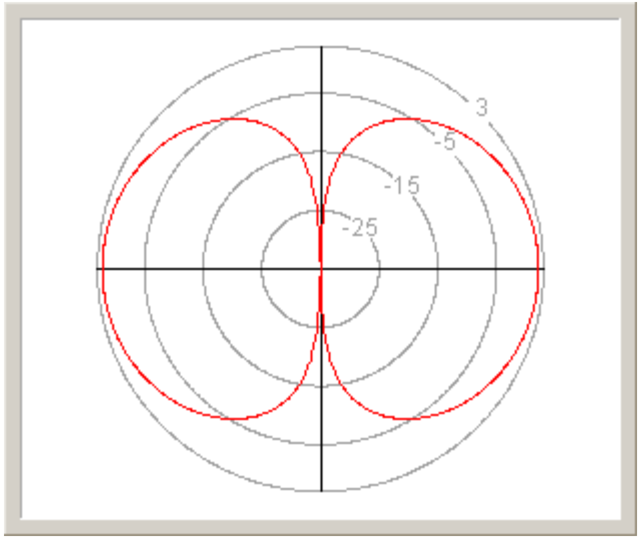
# Antenna Characteristics

Reciprocity of Antennas
Antenna Gain
Antenna Polarization

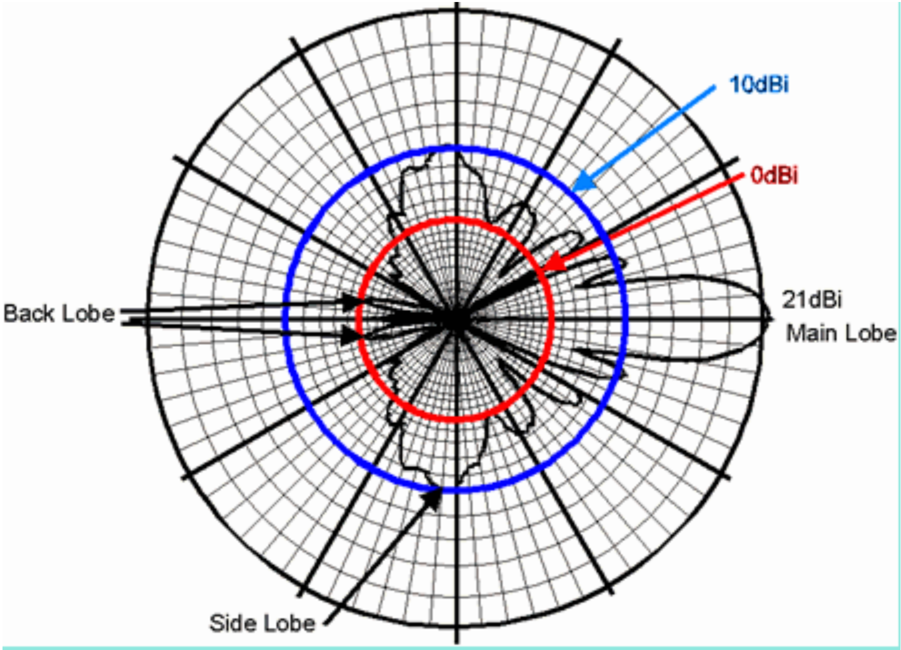

Magnetic field component
The polarisation of the wave is the same as the electric field and in this case it is horizontal
Electric field component
Direction of travel

# Antenna types

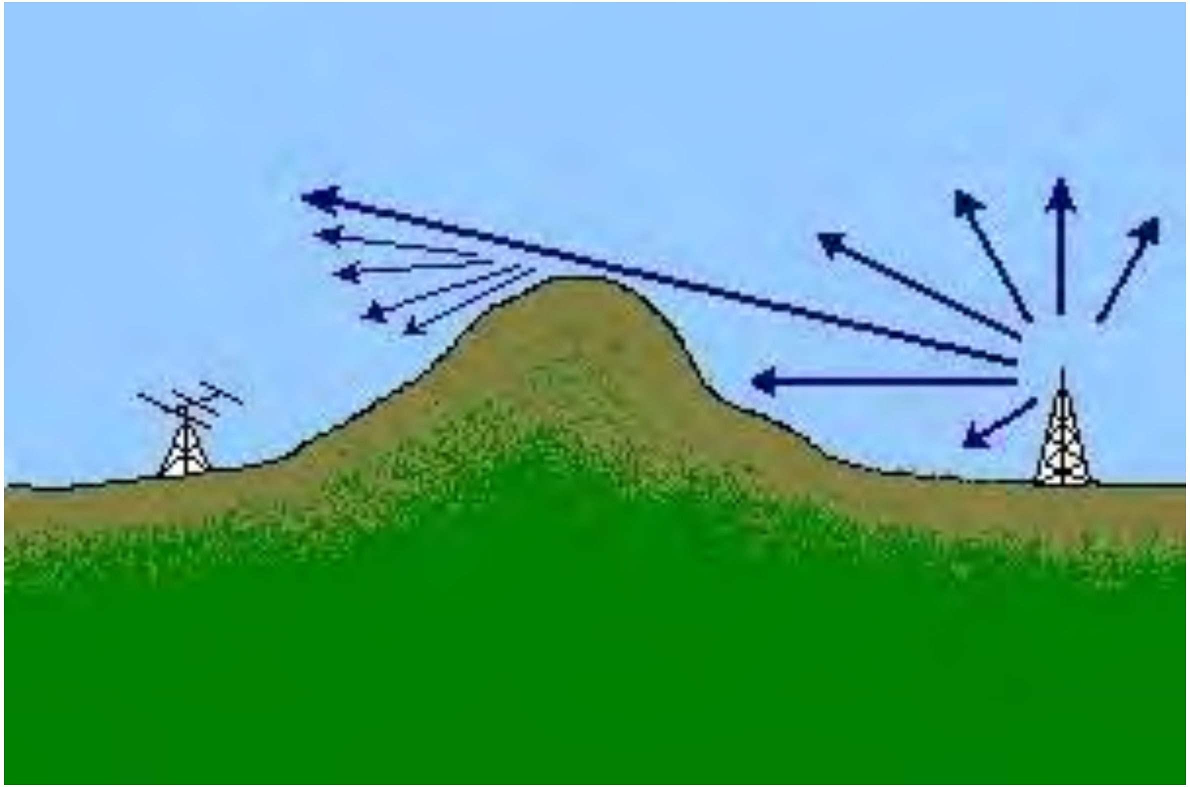
## Omnidirectional



## Semi to Very Directional



# Propagation Characteristics



# The S in the DR

Your success in receiving is going to depend on your antennas and filters

Do not transmit with a mismatched antenna system

# SDR Tools

- Multiple tools
- GQRX, SDR# for browsing spectrum
- GNU Radio is the grand-daddy of decoding platforms

Pick the tool for the right job

# What am I seeing/hearing?

http://www.sigidwiki.com/wiki/Signal_Identification_Guide

# Tools of the Trade

GQRX - This is where ya start

Baudline - Non GPL and quirky (50MB file limit)

GNURadio - GRADWare and goofy

# Other tools

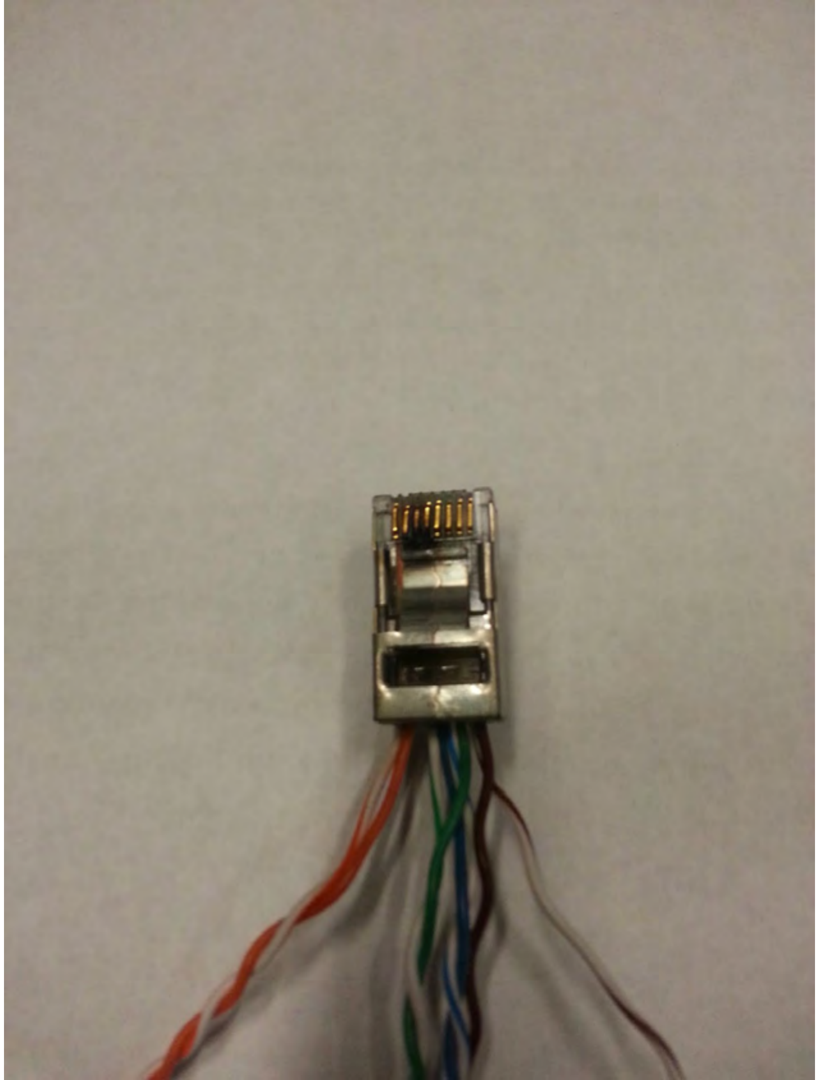
1. dsd (audio input selection problem)
   - Demodulate P25, Mototurbo
2. multimon-ng
   - Demodulates almost ALL THE THINGS
3. smartnet-scanner
   - More P25 goodness (uses radioreference)

# Linux Only?

- For most of the tools, yes.
- To look around, no.
- Use the same dongle
- Opposed to GQRX
  - SDRSharp - plugins
  - HDSDR

# Common problems in SDR labs

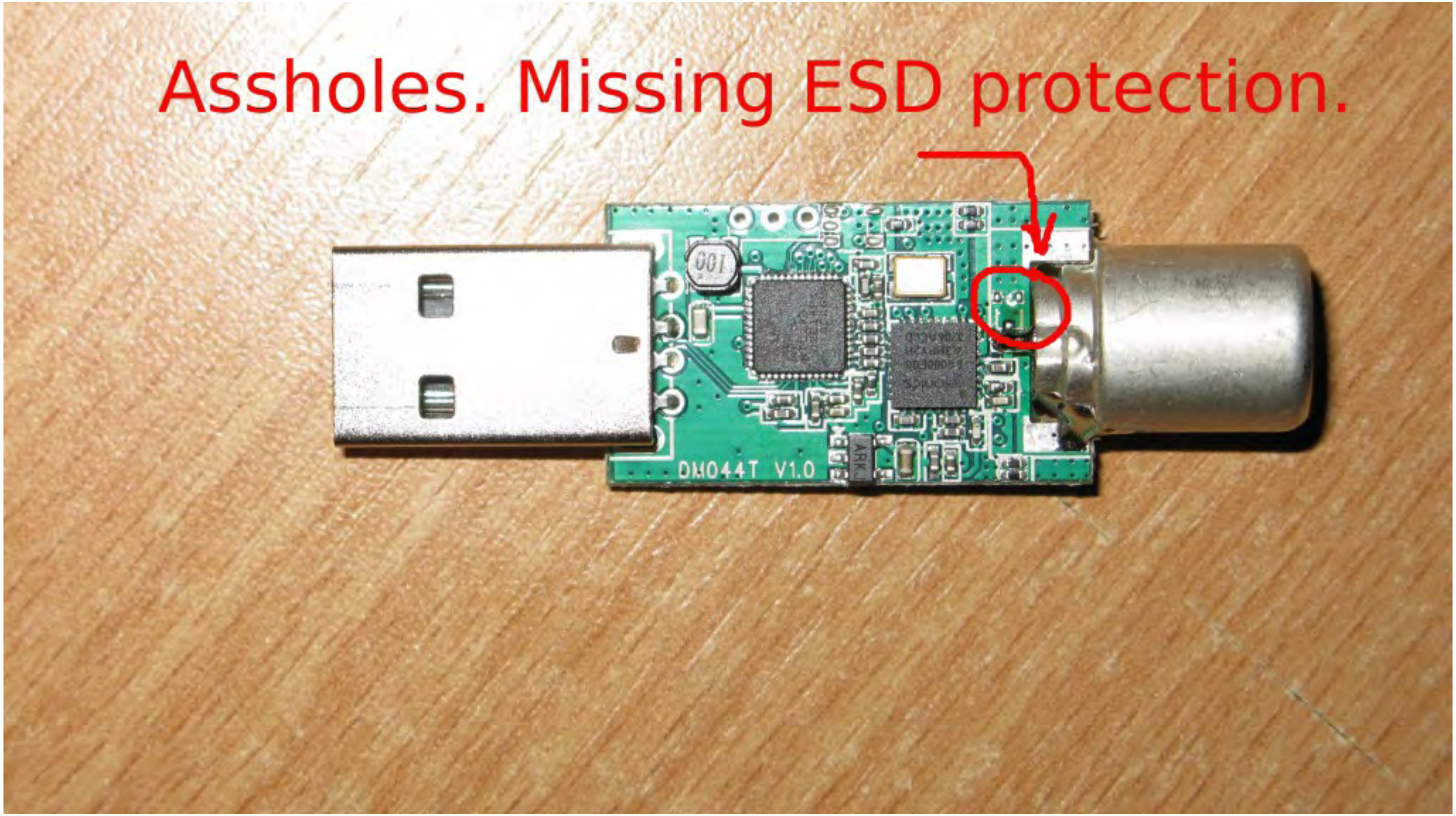
- Antennas
- Lightning
- Static
- Noise
- Clocks and Drift



# Static

- The cheaper RTL’s do NOT have static protection
- Wind generates static
- Rubbing things… generates static

Static protection is a must!



Assholes. Missing ESD protection.

http://ncrmnt.org/wp/2012/06/30/rtl-sdr-static-protection/

# Noise Reduction Must Reads

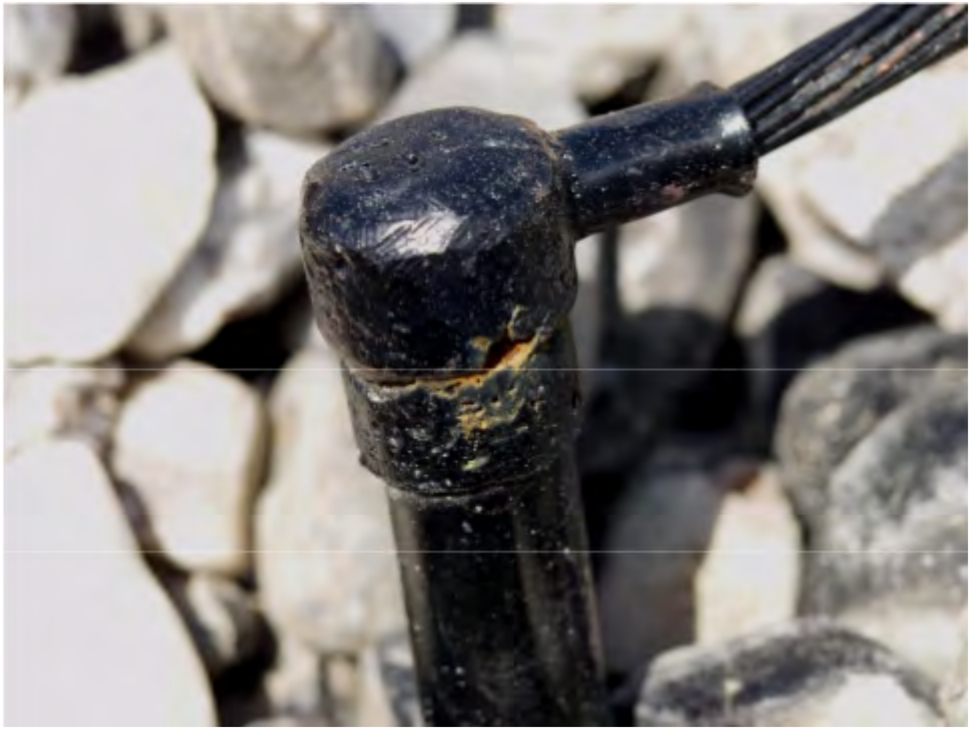
The-Mitigation-of-Radio-Noise-from-External-Sources-at-Radio-Receiving-Sites

http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468464

Naval RFI Handbook

http://www.arrl.org/files/file/Technology/RFI%20Main%20Page/Naval_RFI_Handbook.pdf

# BFG Noise



Computer Power Supply not in Accordance with

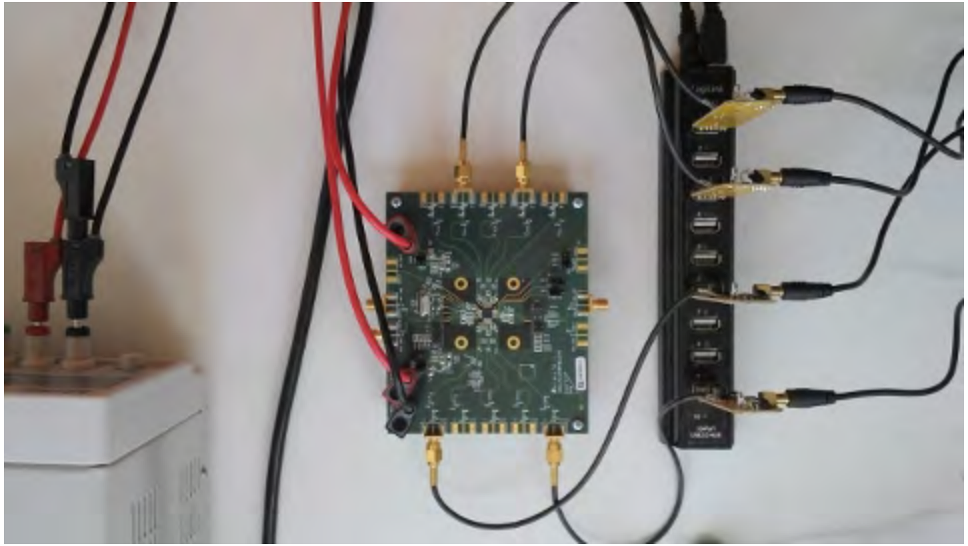
Barrier, Feed, and Ground (BFG) Principles

Improper grounding solution

# Clocks

- The cheaper SDR’s have a lot of noise in them
- Choke them out and isolate noise sources
- Use a unified PPM if you use more than one for IQ

# A bit of fun - Hardware Mods



Multichannel Receivers

http://yo3iiu.ro/blog/?p=1450

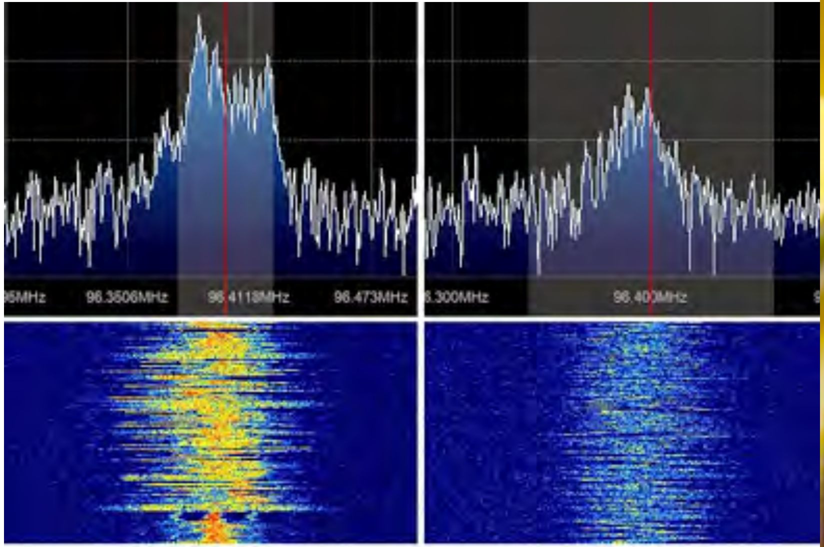
# Hardware Mods

-As the RTL warms up, you’ll get signal drift

-Know your offset, National Weather Service

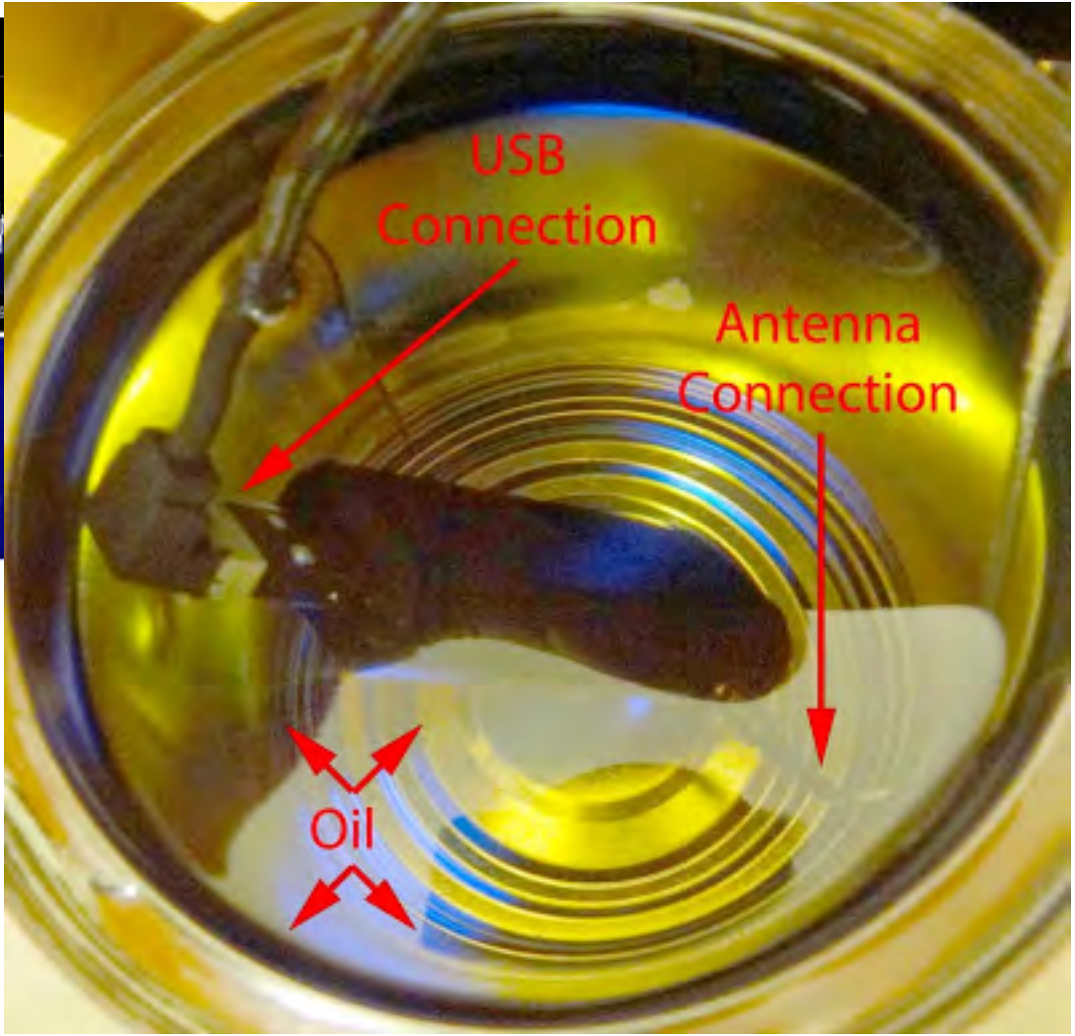
162.400MHz 162.425MHz 162.450MHz 162.475MHz 162.500MHz 162.525MHz 162.550MHz

Add some cooling!



Bare stick

With cooling



http://sdrformariners.blogspot.com/2013/12/cooling.html

# TS(-CM) on the cheap

Technical Surveillance and Countermeasures

- It’s a process, not a tool
- Use lossy antennas and mismatched systems to your advantage
- Know your radio neighborhood
- HEATMAPS!

# Take it to the Village!

# The Wireless Village

Workshops and Presentations:

- Antenna theory and constructions
- Wireless Penetration Testing
- Software Defined Radio
- and others

# The Wireless Village (cont’d)

Wi-Fi

λ802.11all-the-things

λEn/Decryption

λOld to Very New

λFox and Hound

λAll the WiFi'z

Other Wireless

λZigbee

SDR

λFox and Hound

λDuck Hunt

λSeek and Demod

λRF Meta analysis

λRadio Signal Mapping

# The Wireless Village (cont’d)

Wireless Capture The Flag

- Wireless
- SDR
- Hide & Seek RF Style

# Questions