Ham Radio 4 Hackers

Devin Noel – N7hkr
Eric Watkins – KR0VER
March 14, 2019

Ham Radio 4 Hackers

Which one of these things is just like the other?

#about_us

- Eric Watkins
  kr0ver
- Devin Noel
  n7hkr

Has anybody seen Nick?

- We created this talk for Nick:

This is what HAM radio nerds look like

Mobile contesting

(talk to as many different people in a given time as possible)

This is what hacker nerds look like

Wardriving

Most InfoSec types know what wardriving is, right?

Ya, really different looking…

What Would Wikipedia Say?

“Amateur radio (also called ham radio) describes the use of radio frequency spectrum for purposes of **non-commercial** exchange of messages, **wireless experimentation**, self-training, private recreation, radiosport, contesting, and **emergency communication**.

The term "amateur" is used to specify "a duly authorized person interested in radioelectric practice with a purely personal aim and **without pecuniary interest**;“

Source: https://en.wikipedia.org/wiki/Amateur_radio

What is Amateur Radio to hackers?

- Legal transmission
- Legitimate transmission
- Education, training & learning

What does HAM radio have to do with hackers?

The fundamentals of RF learned for ham radio apply to ALL wireless systems.

DefCon WiFi shootout champions crowned: 125 miles

Source: https://boingboing.net/2005/07/31/defcon-wifi-shootout.html

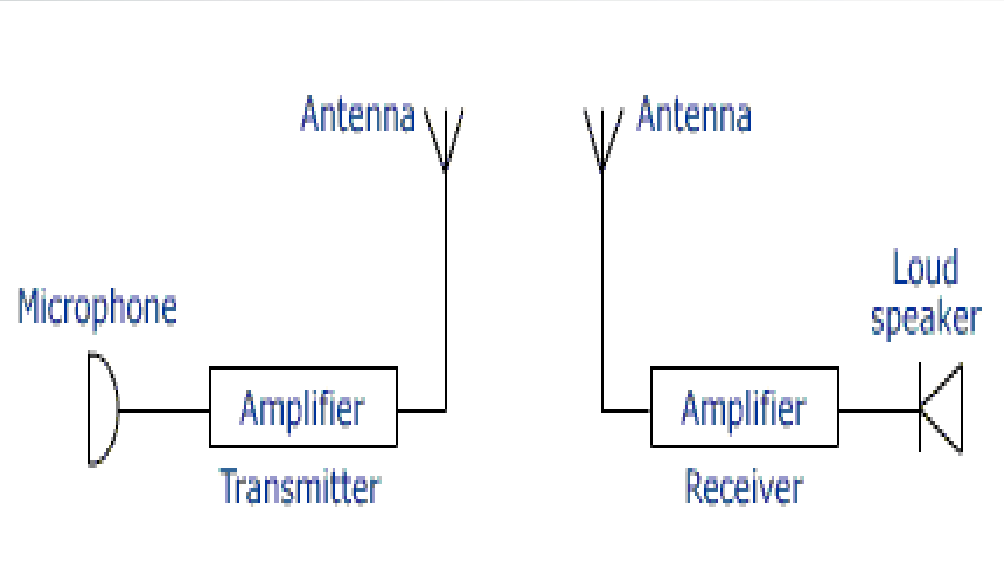
Licensing basics

- To get on the air: get licensed & know the rules to operate legally.
- US licenses are good for 10 years for anyone except a representative of a foreign government.
- Amateur only, no commercial activity permitted at all.
- Public communications only, no encryption
- Transmission not broadcast
- In the US there are three license classes:
  - Technician, General and Extra.

http://www.arrl.org/getting-licensed

Radio Basics

- Pump AC into a wire, get EM waves
- EM waves jiggle a wire, get AC



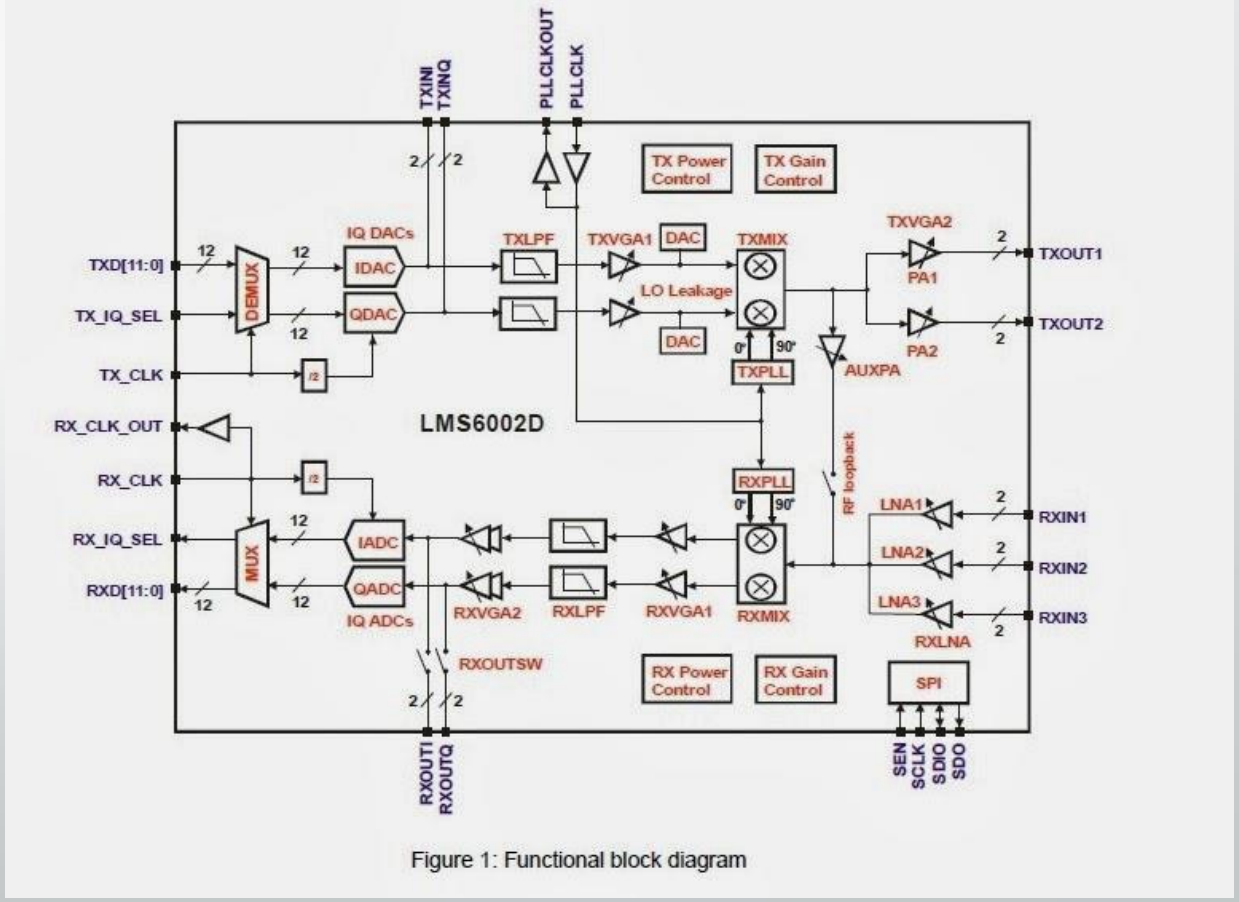
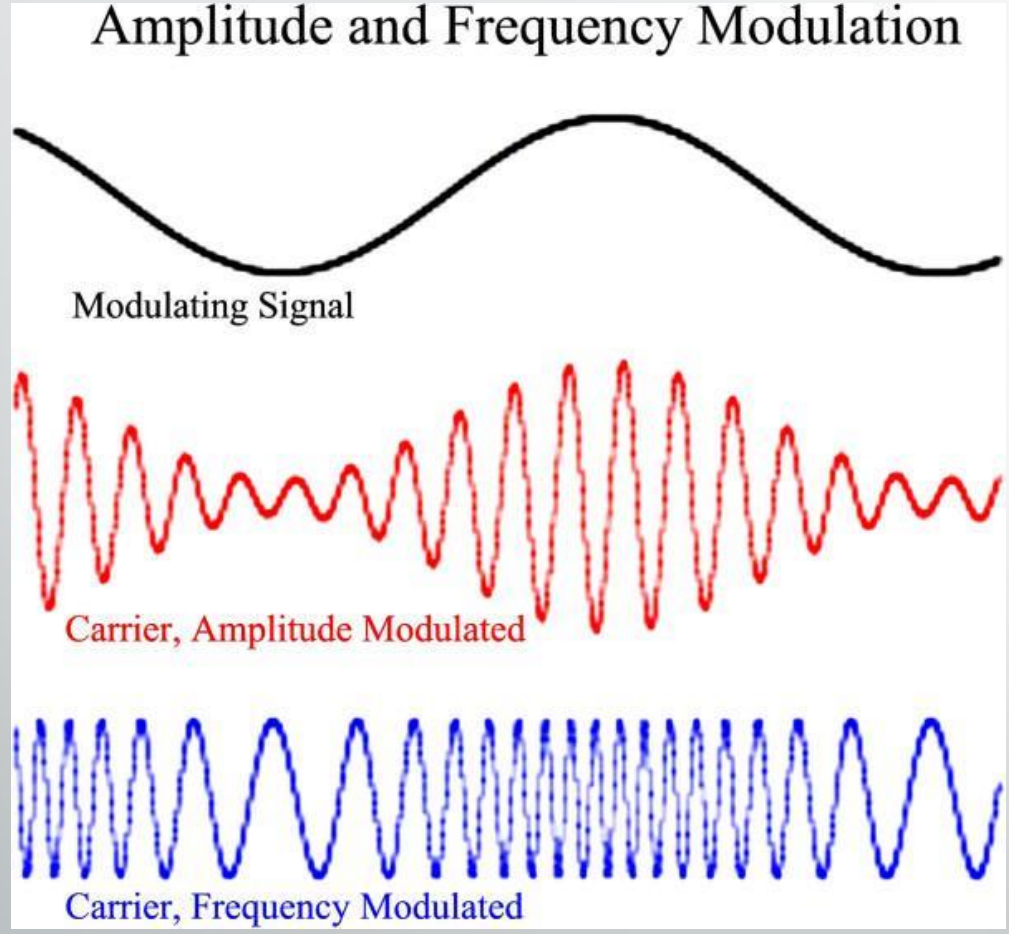
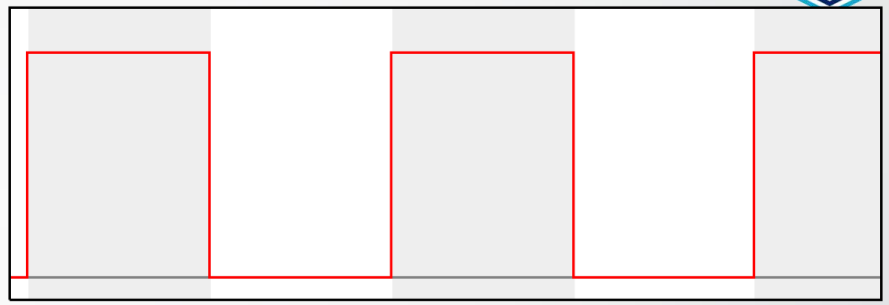
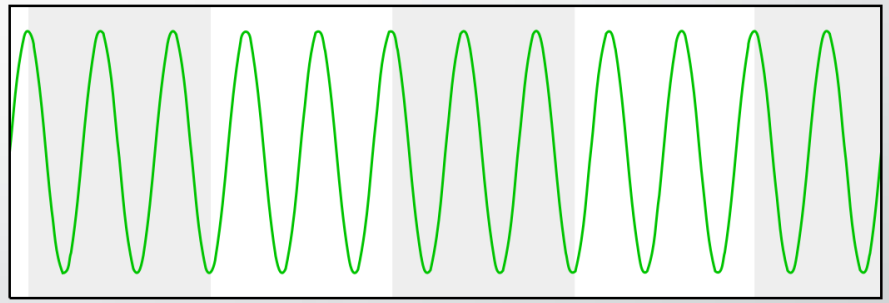


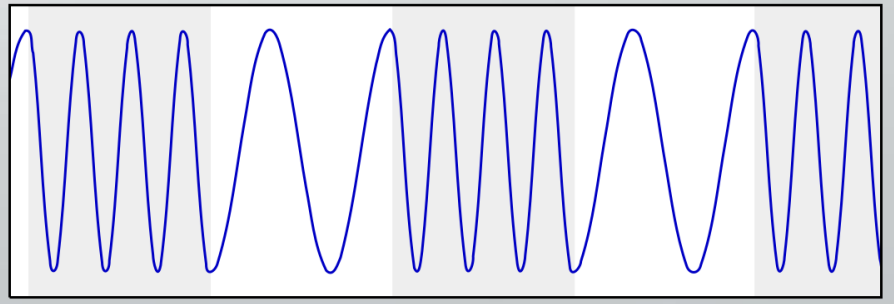
Figure 1: Functional block diagram

Modulation

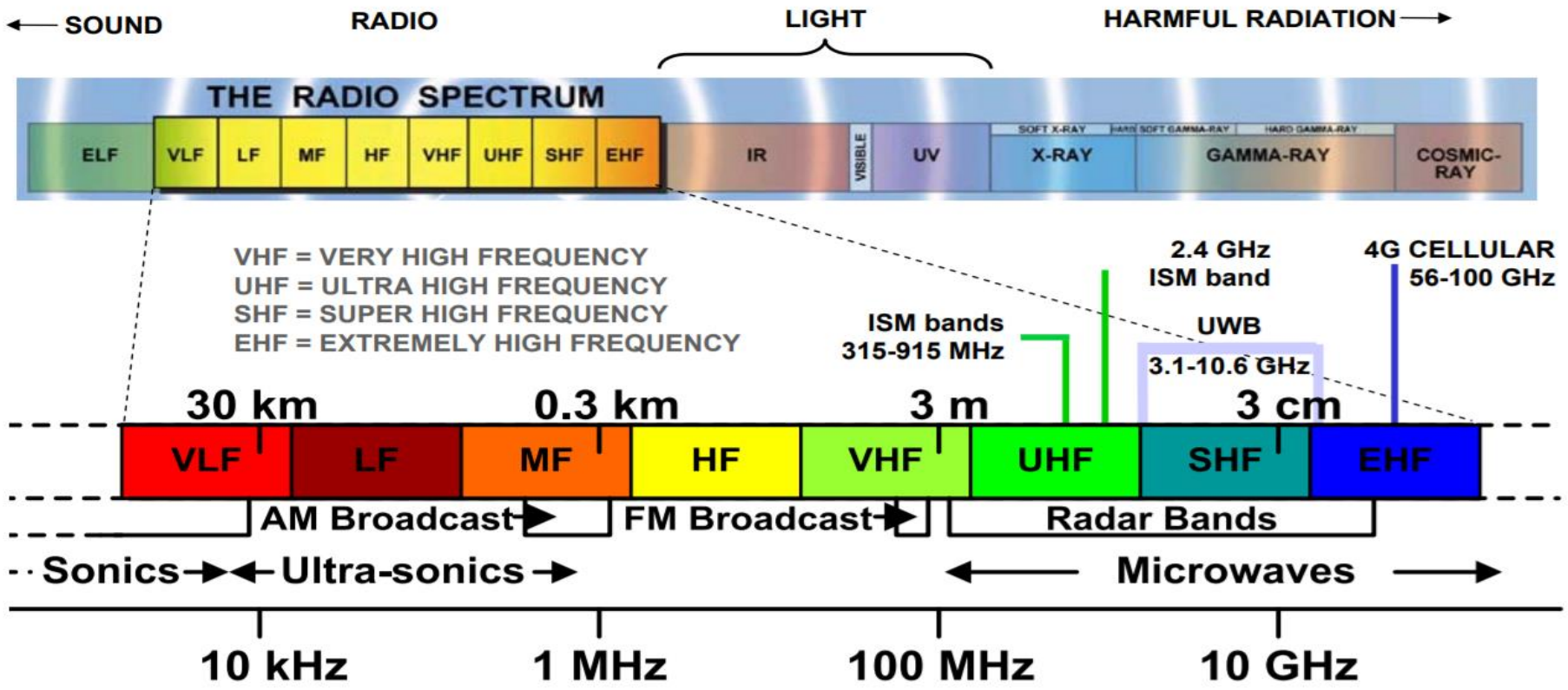



Data


Carrier


Modulated Signal

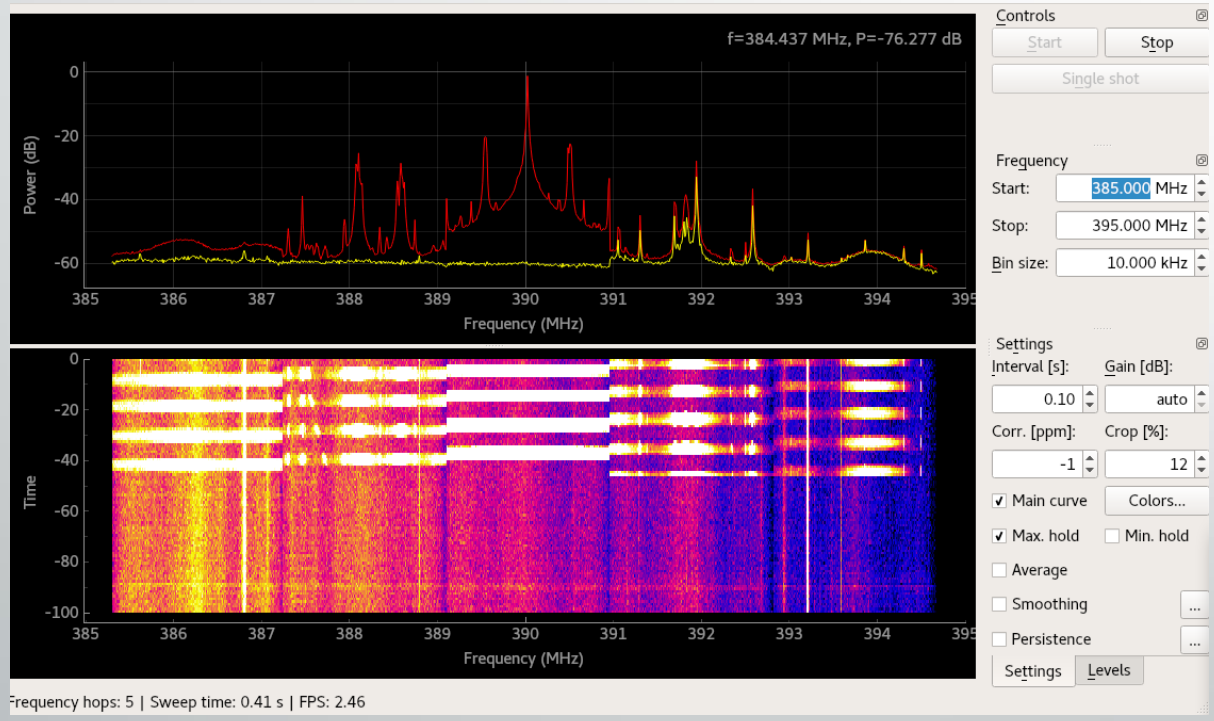
Electromagnetic Spectrum



ISM = Industrial, Scientific and Medical
UWB = Ultra Wide Band

Source: JSC.MIL

Qspectrumradar Demo



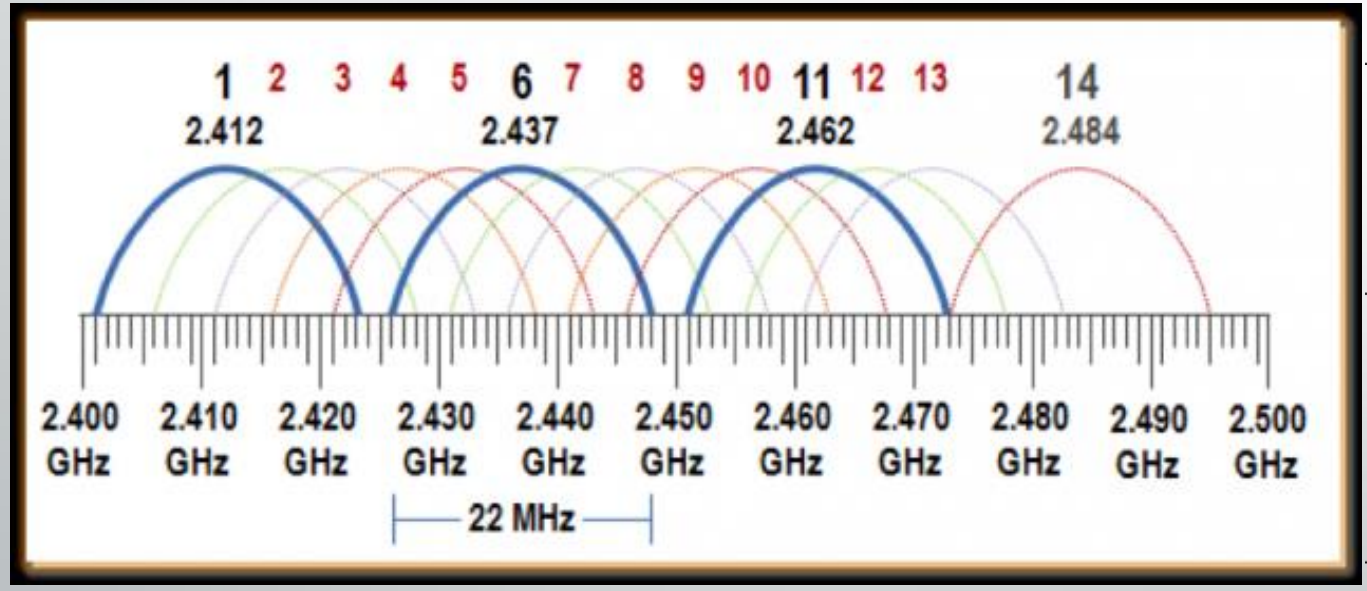
FCC ID: HBW7359

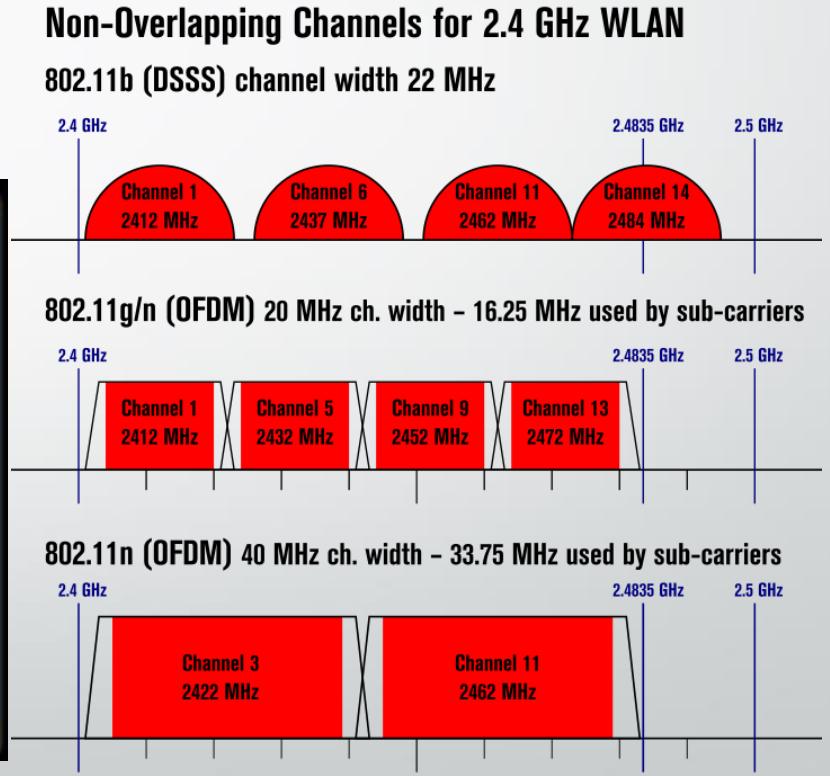
Frequency: 390 MHz

Google the first line or even just “garage door opener frequency”

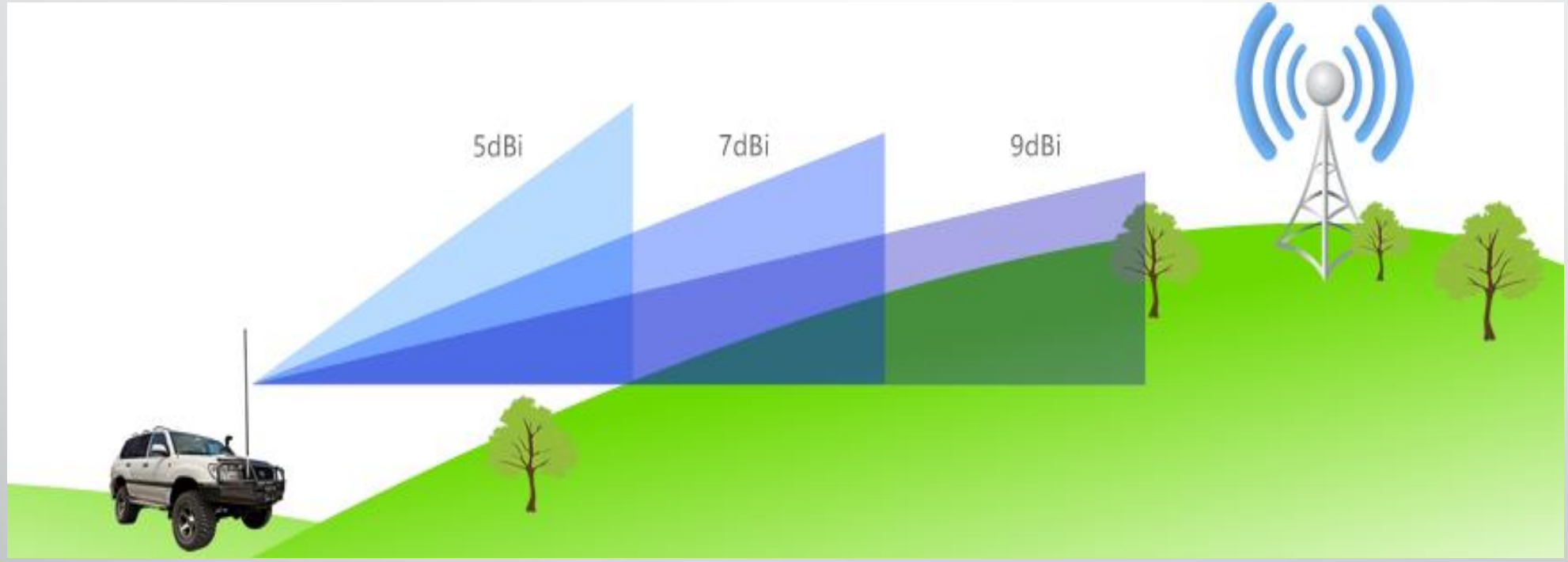
How does this apply to my wi-fi?

Channels in 2.4ghz WiFi



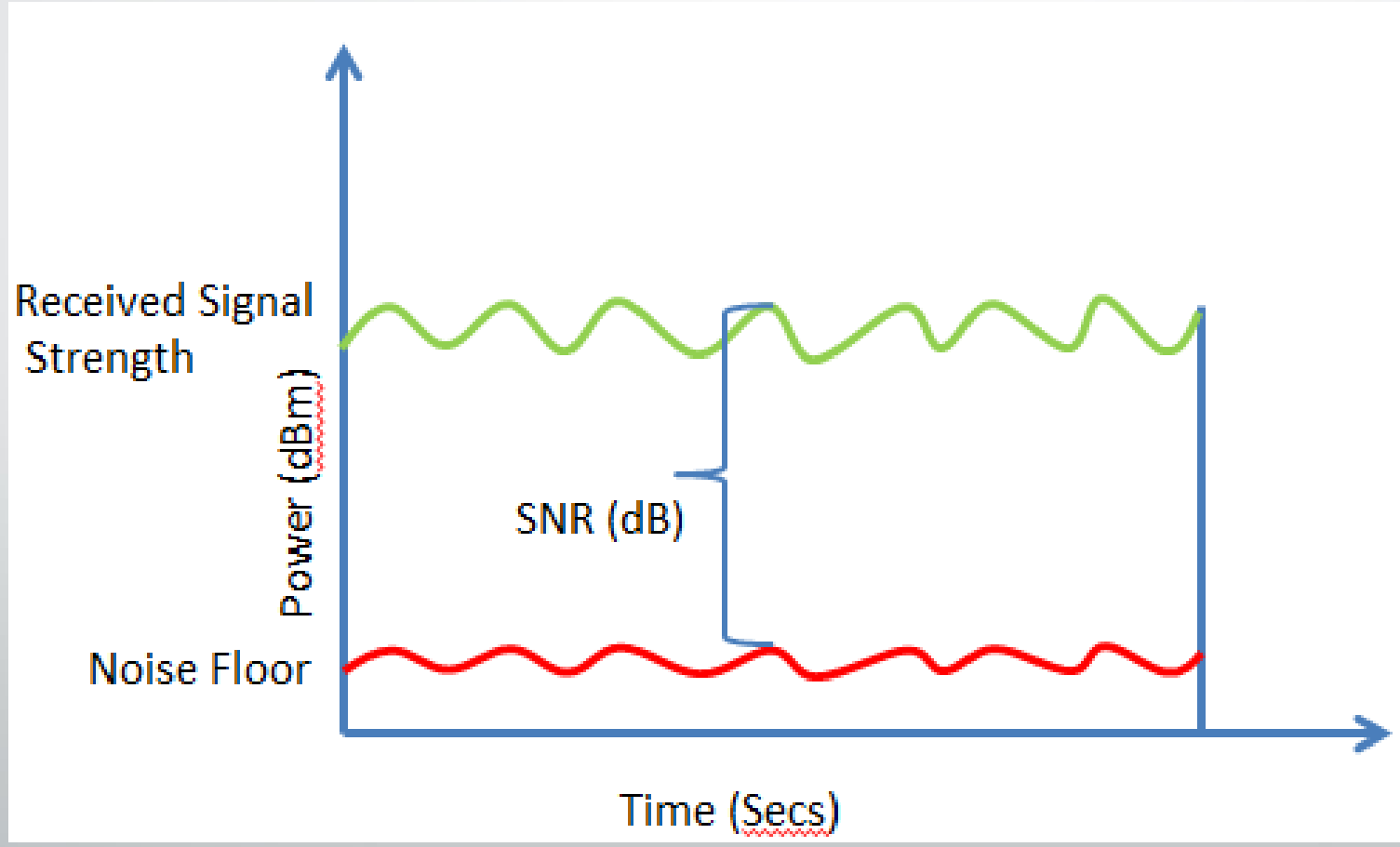


Tell me again about gain?

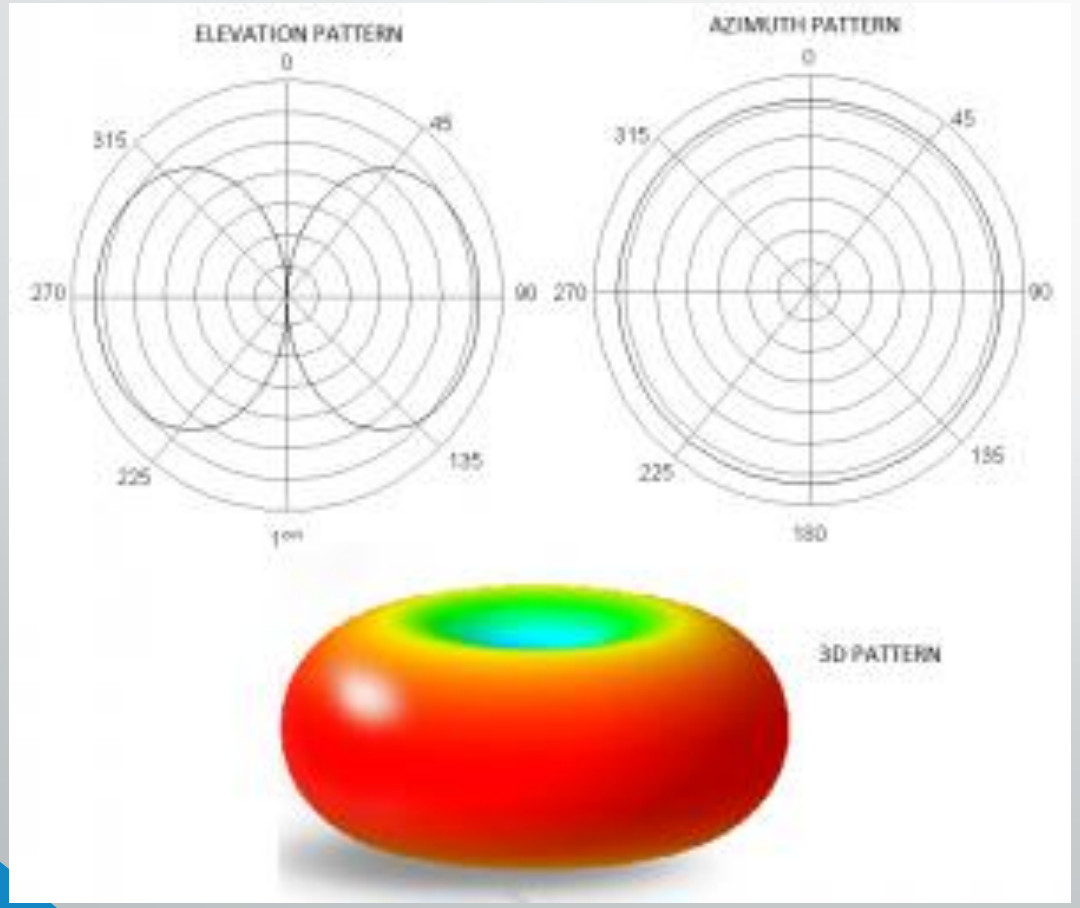


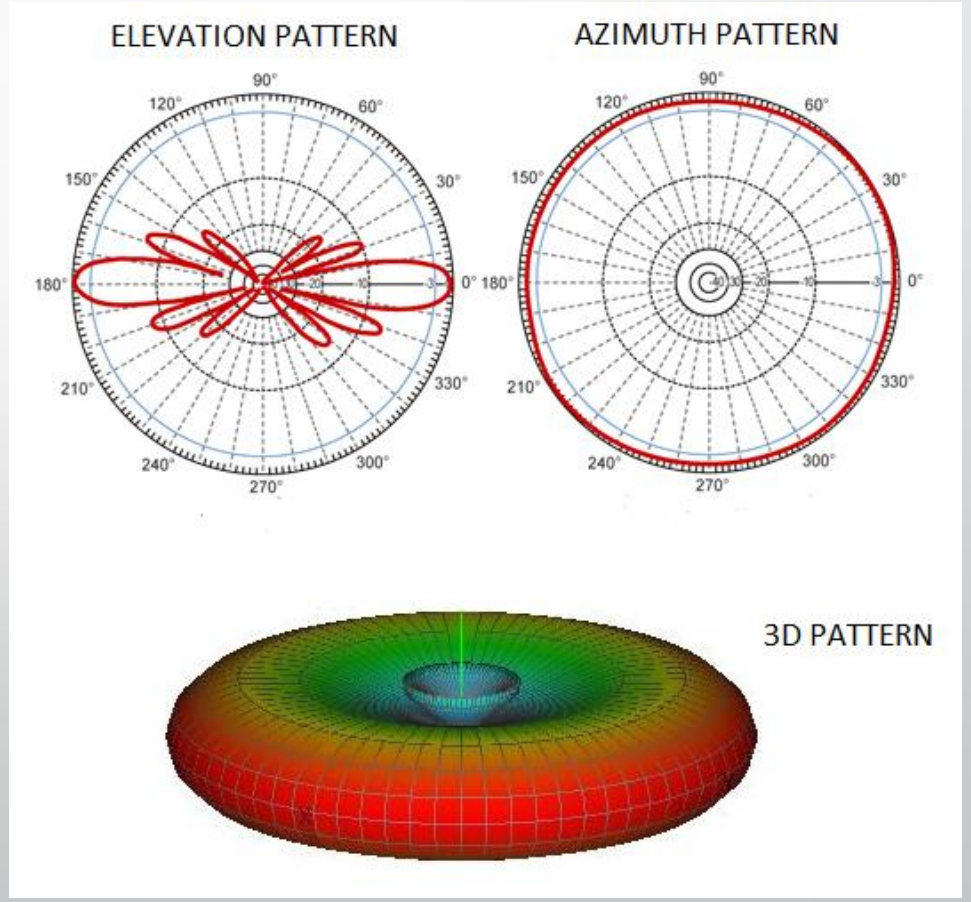
What is louder (brighter)? 5 watts or 0.005 watts?

Signal to Noise Ratio

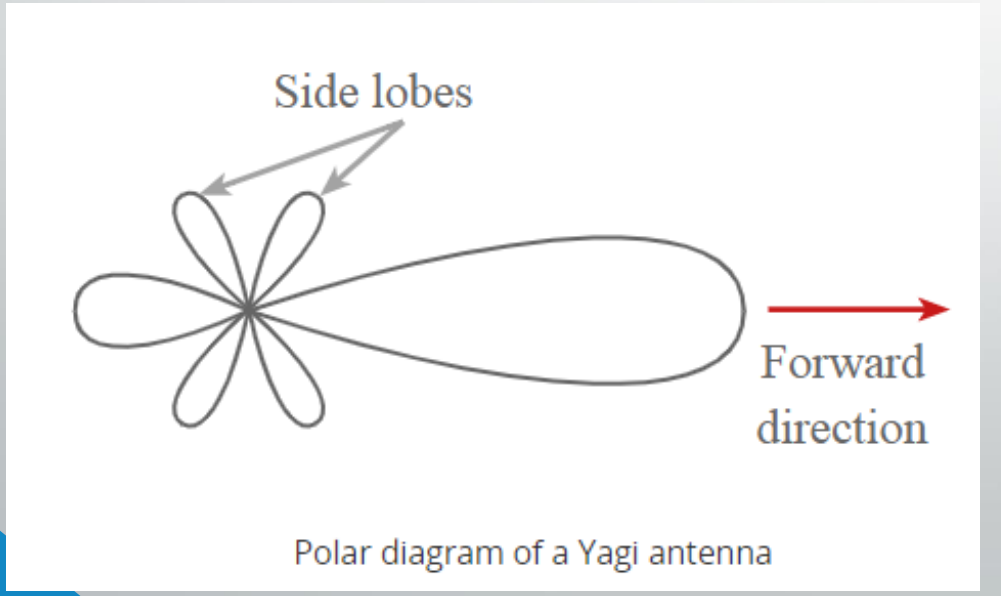


Omni - Directional Antennas

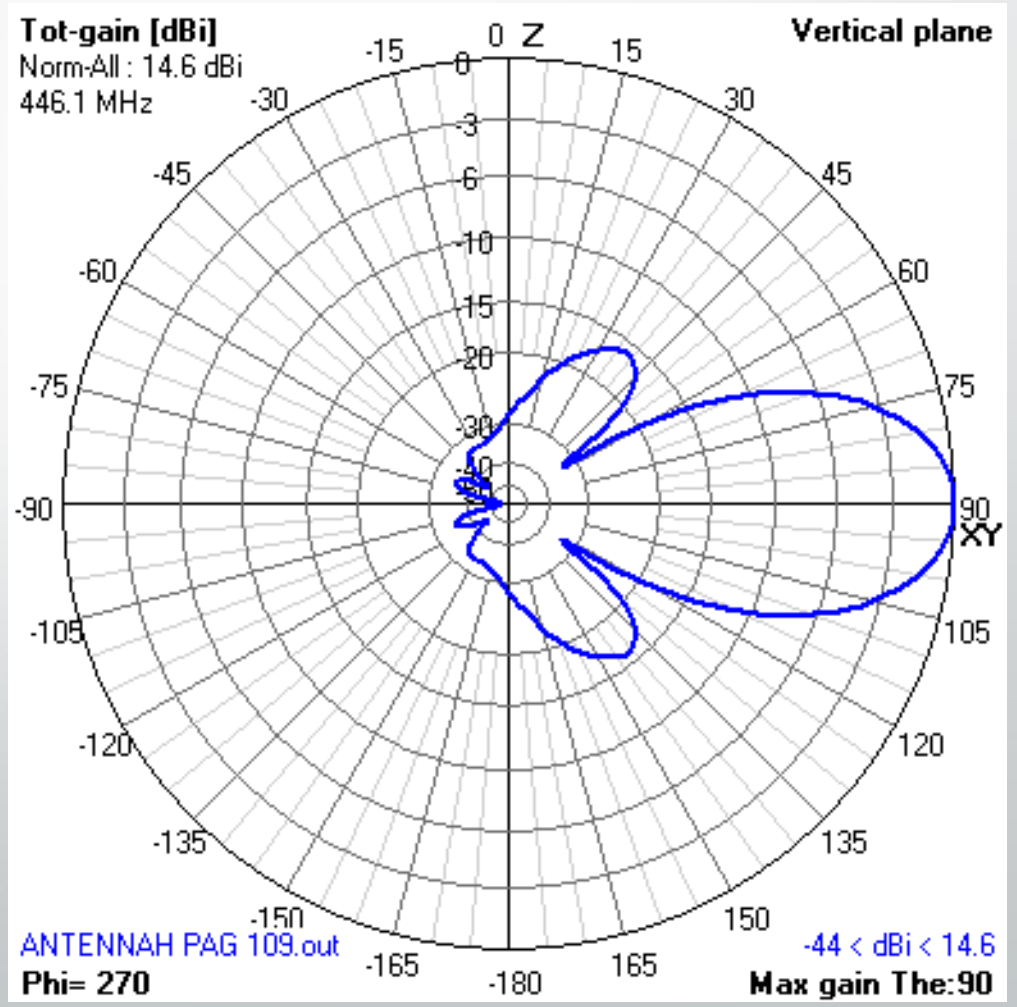




Directional Antennas

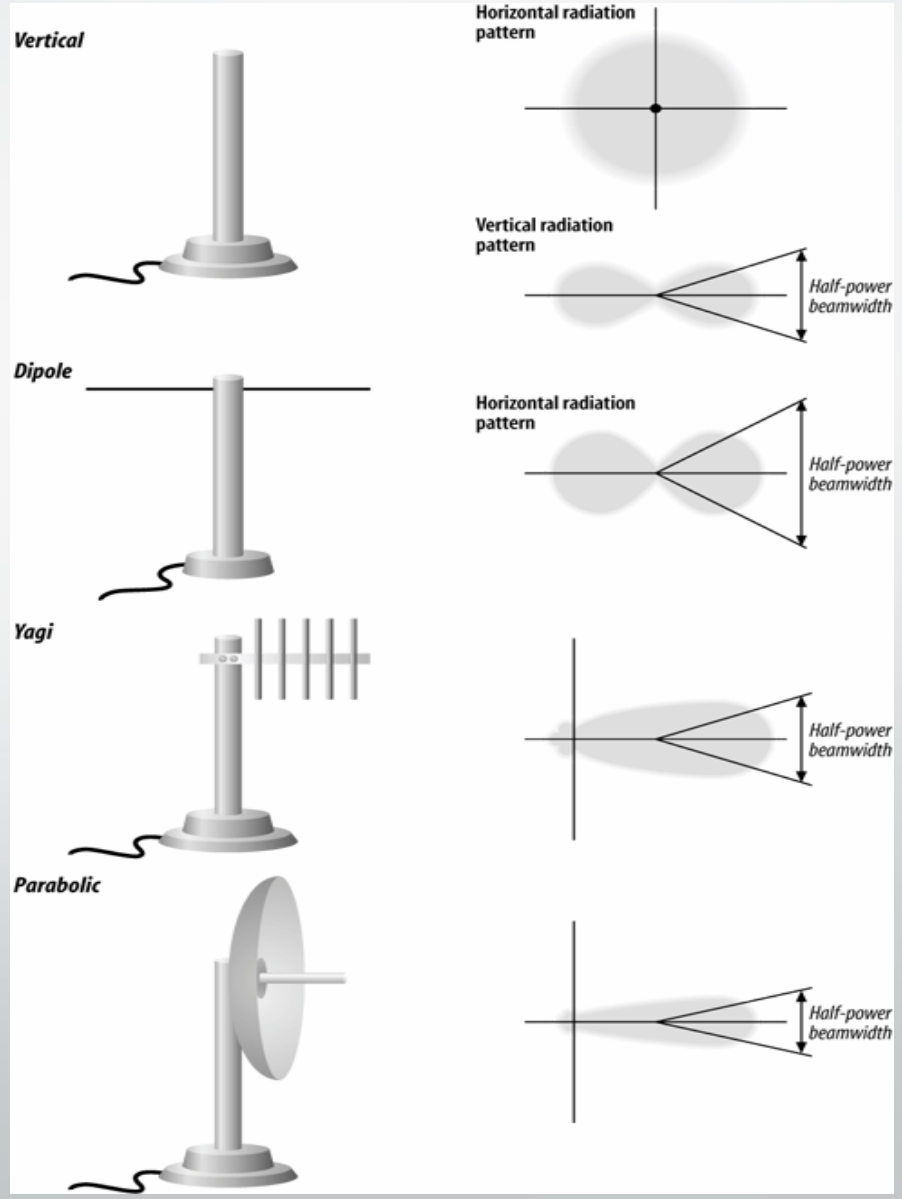


Polar diagram of a Yagi antenna



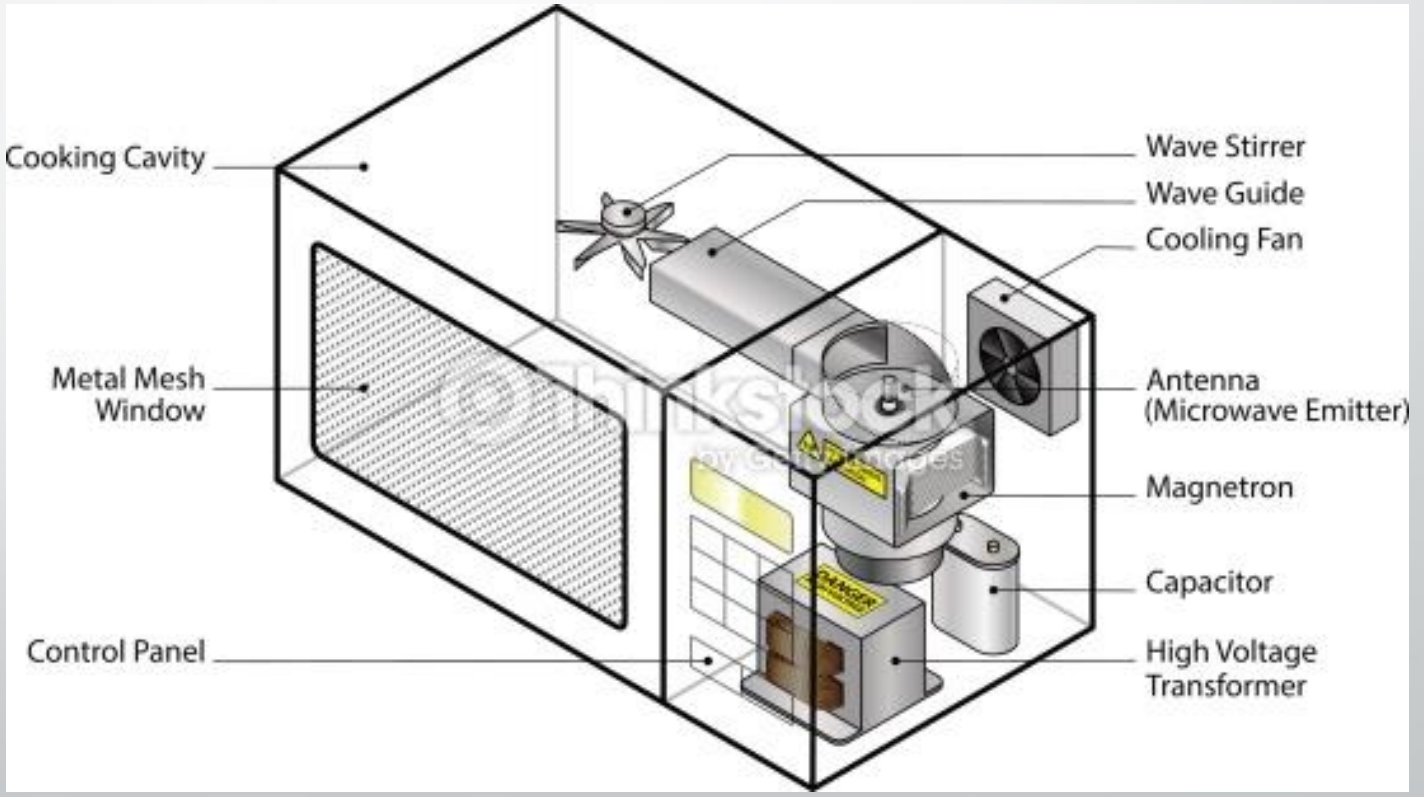
Antennas

A few common antenna types

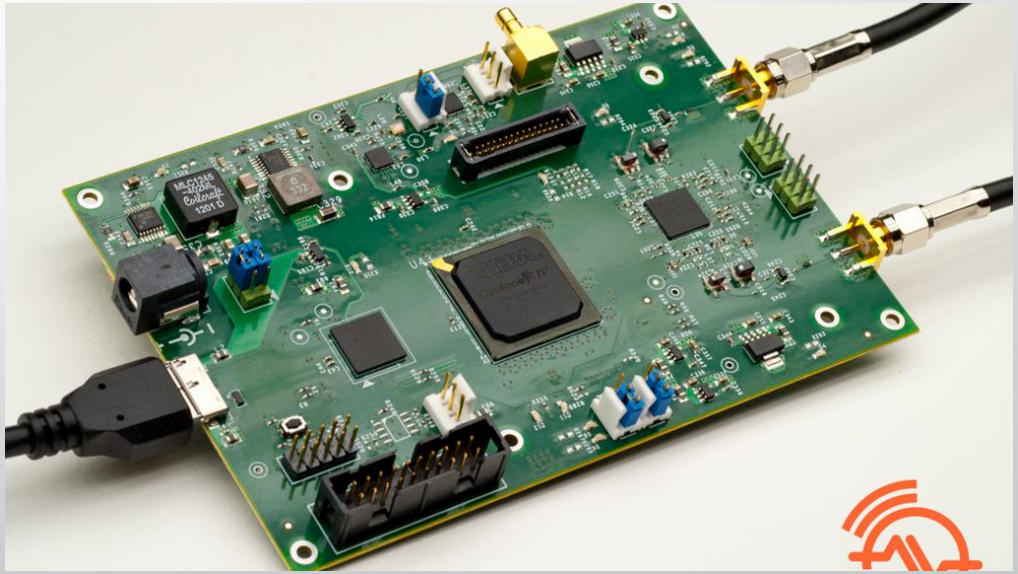


Faraday Cages & Shielding

Both of these are effective Faraday cages providing shielding inside and out



SDR – Software Defined Radio



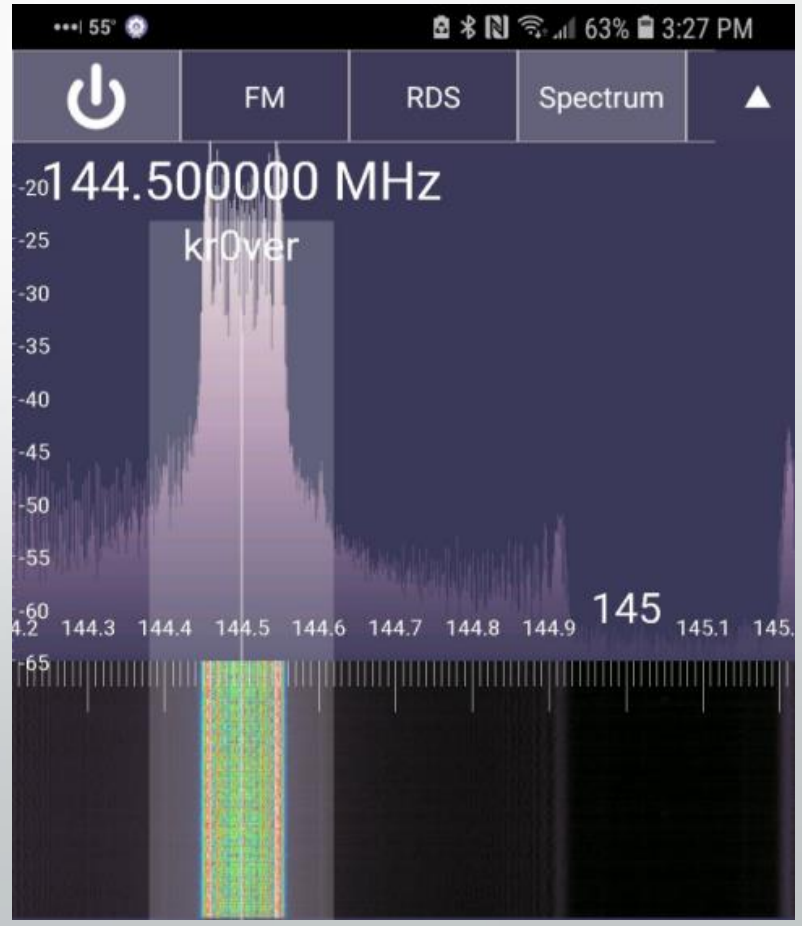
Demo walk-through

- Lets get radioactive
  - Insert canned crowd participation speech here

Make the reciever work (attach RTL-SDR to Android)

Fight the SDR Touch UI (better on a tablet)

- Drag the menu bar at top right/left to find stuff
- Make sure signal type is set to **FM**
- Tapping and/or dragging on the screen will change freq or filter width (easy to mess stuff up)
- **Prefs > Filter width (Hz) > 60,000**
- Select **Jump** & type in the frequency
  - **144.550mhz**
- Power button on top left to start/stop radio
  - Stop radio before exiting or it it will keep running in the background



How to know if it worked

- Millennials - look confused & listen to geezers ramble

- Old farts - Nod at each other knowingly while busting out a good back in the day story

Let the magic happen (Decode the audio)

1. On another phone not running the RTL-SDR launch following app
   - Android: Robot36
   - iDevice: SSTV Slow Scan TV
2. Select Scottie S1
   - SSTV mostly, Robot36 figures it out
3. Put the phones near each other
4. Fiddle with the volume if needed
   a. Try not to cause too much interference with others

Apps used for demo

- **iDevice**
  - SSTV Slow Scan TV (Black Cat Systems)
    - $3 Apple tax
  - https://itunes.apple.com/us/app/sstv-slow-scan-tv/id387910013?mt=8
- **Smart phone users (Android)**
  - Robot36 - SSTV Image Decoder (Ahmet Inan)
    - https://play.google.com/store/apps/details?id=xdsopl.robot36
  - RTL2832U driver (Martin Marinov)
    - https://play.google.com/store/apps/details?id=marto.rtl_tcp_andro
  - SDR Touch - Live offline radio (Martin Marinov)
    - https://play.google.com/store/apps/details?id=marto.androsdr2

Thanks for your attention..

Contact us:

Eric Watkins
ericw@neurospeed.com

Devin Noel
devin.noel@gmail.com

Facebook:
www.facebook.com/groups/dc719/