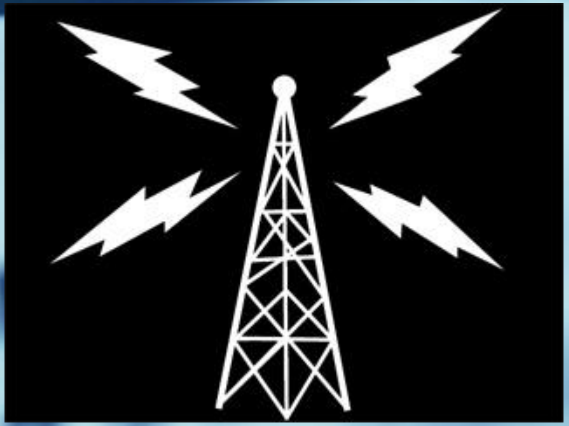


DEF CON

DC 0471

TRIVANDRUM

29th September, 2018

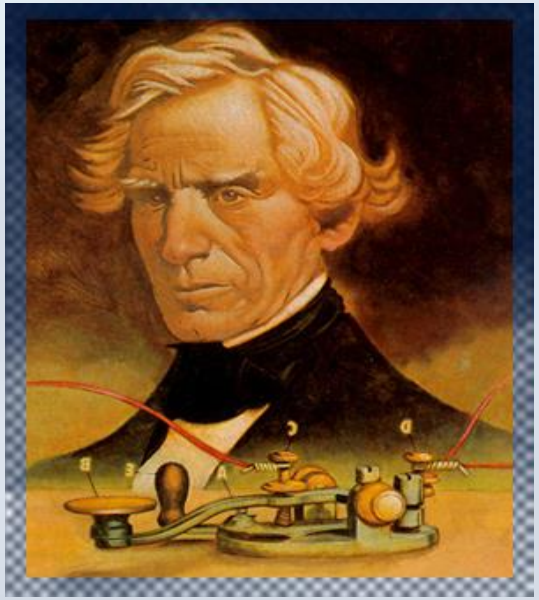
# Portable Pirate Radio with RDS: Broadcast Signal Intrusion with SDR

# #whoami

- Vipin George
- Ad-hoc faculty at CEK
- License Radio amateur, Indian call sign: ***VU3YVG***
- FCC registered US call sign: ***KC9VED***
- Handled Internet plumbing for a Tier- 1 ISP
- M.Tech in Cyber Forensics and InfoSec
- Mozillian, Wikipedian
- Enjoys tinkering with Electronic gadgets, Shortwave DXing

# A Brief History of Radio

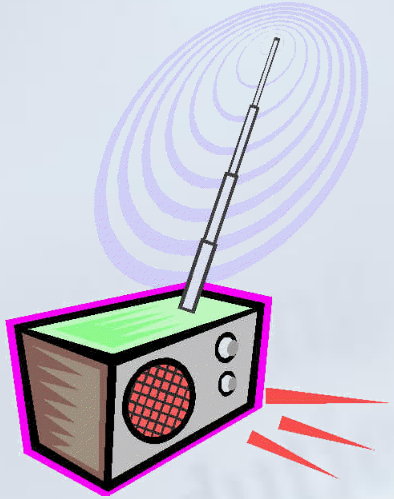
- Samuel Morse
  - Telegraph (wires)
  - Morse Code



| | | | |
|---|---|---|---|
| A | ● ▬ | U | ● ● ▬ |
| B | ▬ ● ● ● | V | ● ● ● ▬ |
| C | ▬ ● ▬ ● | W | ● ▬ ▬ |
| D | ▬ ● ● | X | ▬ ● ● ▬ |
| E | ● | Y | ▬ ● ▬ ▬ |
| F | ● ● ▬ ● | Z | ▬ ▬ ● ● |
| G | ▬ ▬ ● | | |
| H | ● ● ● ● | | |
| I | ● ● | | |
| J | ● ▬ ▬ ▬ | | |
| K | ▬ ● ▬ | 1 | ● ▬ ▬ ▬ ▬ |
| L | ● ▬ ● ● | 2 | ● ● ▬ ▬ ▬ |
| M | ▬ ▬ | 3 | ● ● ● ▬ ▬ |
| N | ▬ ● | 4 | ● ● ● ● ▬ |
| O | ▬ ▬ ▬ | 5 | ● ● ● ● ● |
| P | ● ▬ ▬ ● | 6 | ▬ ● ● ● ● |
| Q | ▬ ▬ ● ▬ | 7 | ▬ ▬ ● ● ● |
| R | ● ▬ ● | 8 | ▬ ▬ ▬ ● ● |
| S | ● ● ● | 9 | ▬ ▬ ▬ ▬ ● |
| T | ▬ | 0 | ▬ ▬ ▬ ▬ ▬ |

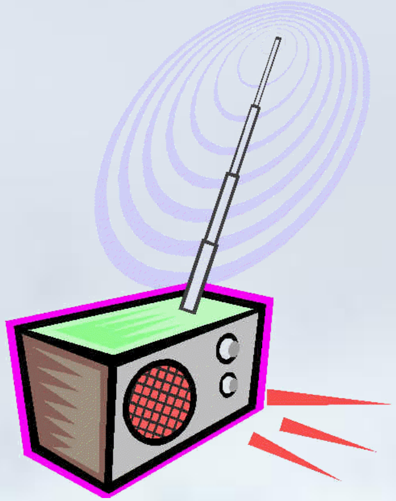
# A Brief History of Radio

- When you think of radio what are things that come to mind?



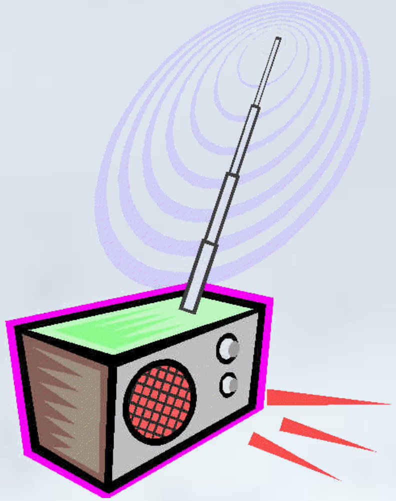
# A Brief History of Radio

- What about wireless?
- How do you transmit a signal through the AIR?



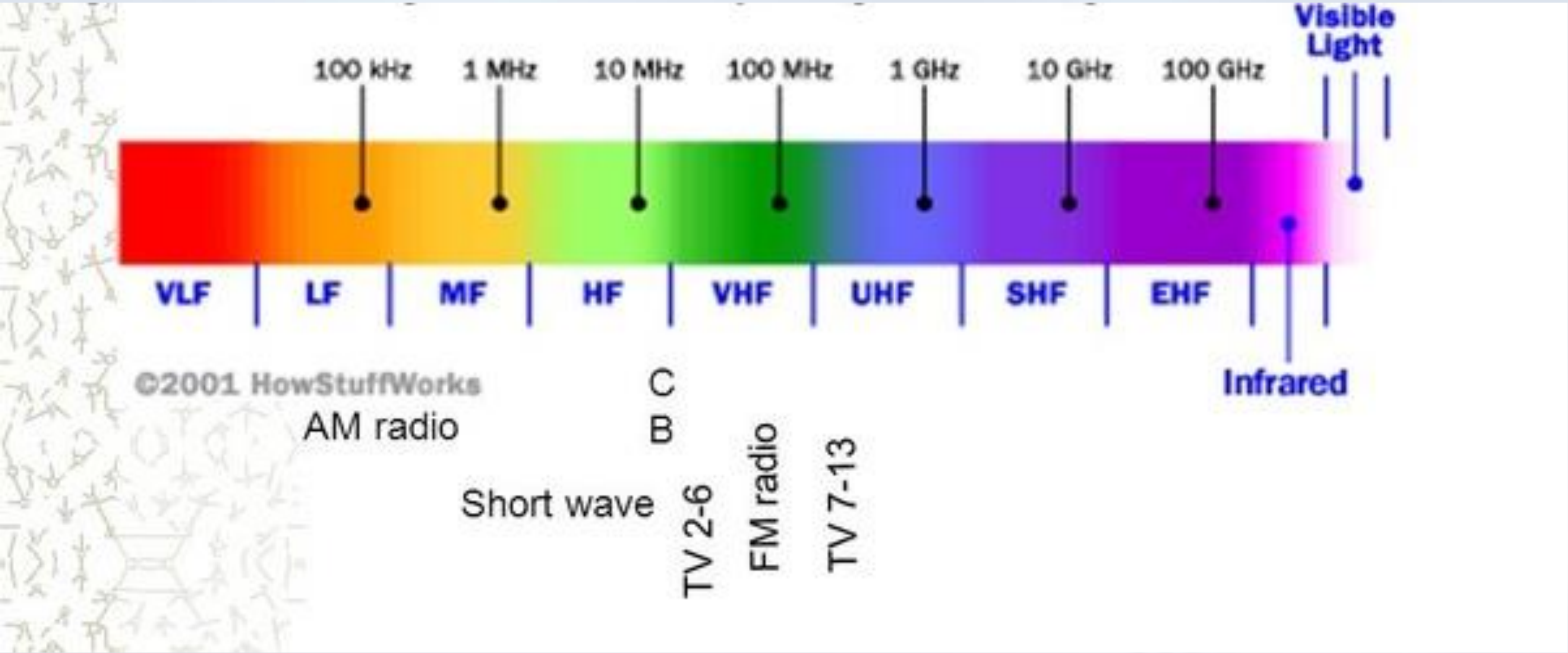
# A Brief History of Radio

- radio waves are transmitted across an electromagnetic spectrum



# Electromagnetic Spectrum

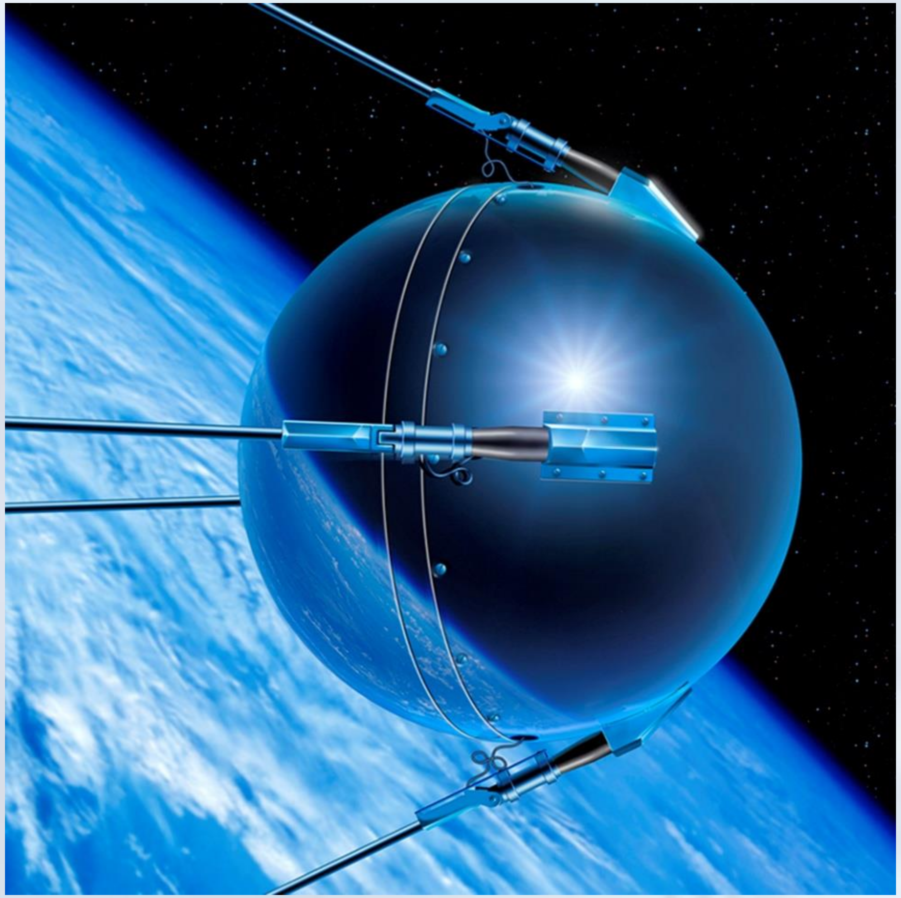
- radio waves are transmitted across an electromagnetic spectrum



©2001 HowStuffWorks

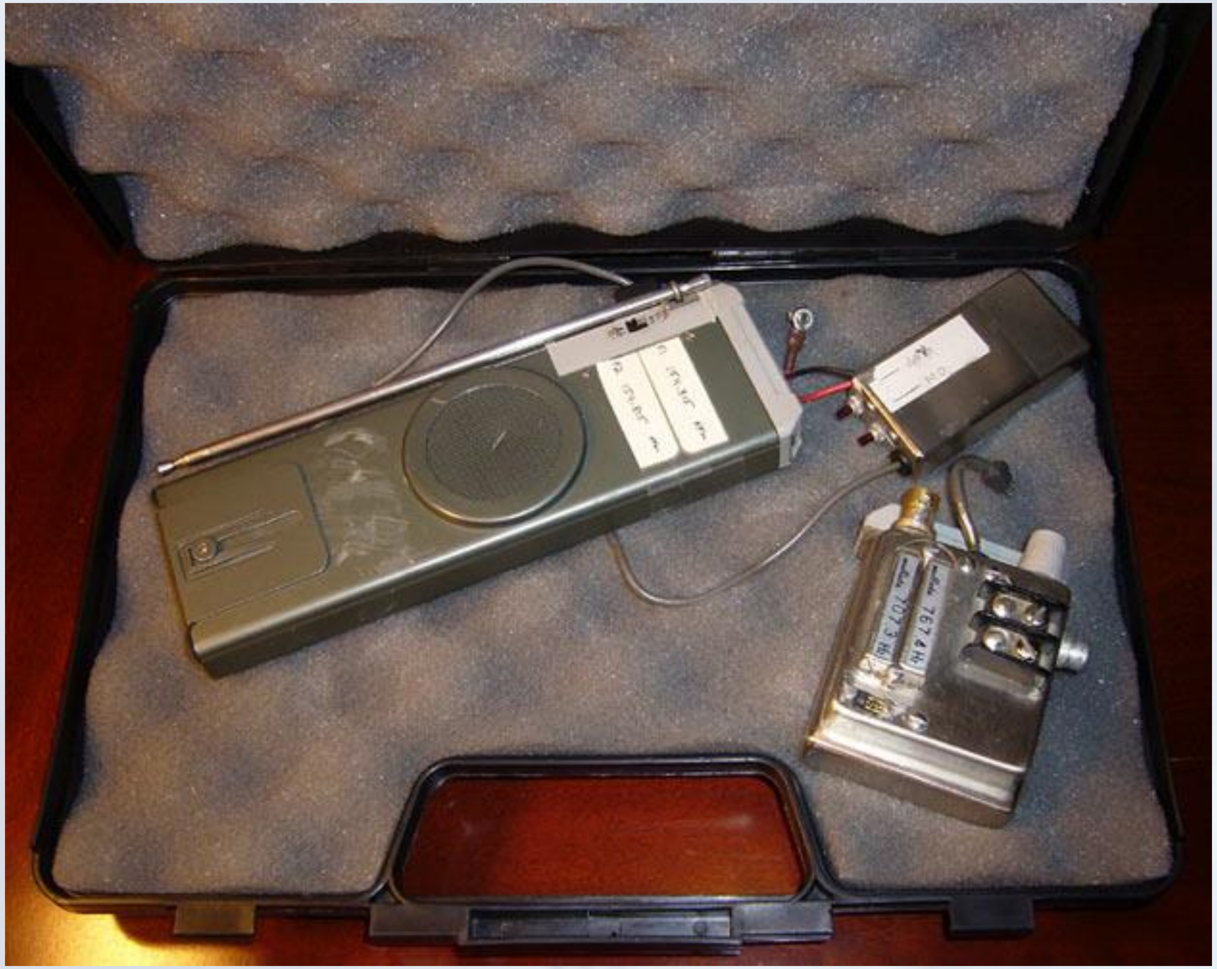
# Popular transmitters

- **The Sputnik**



# Popular transmitters

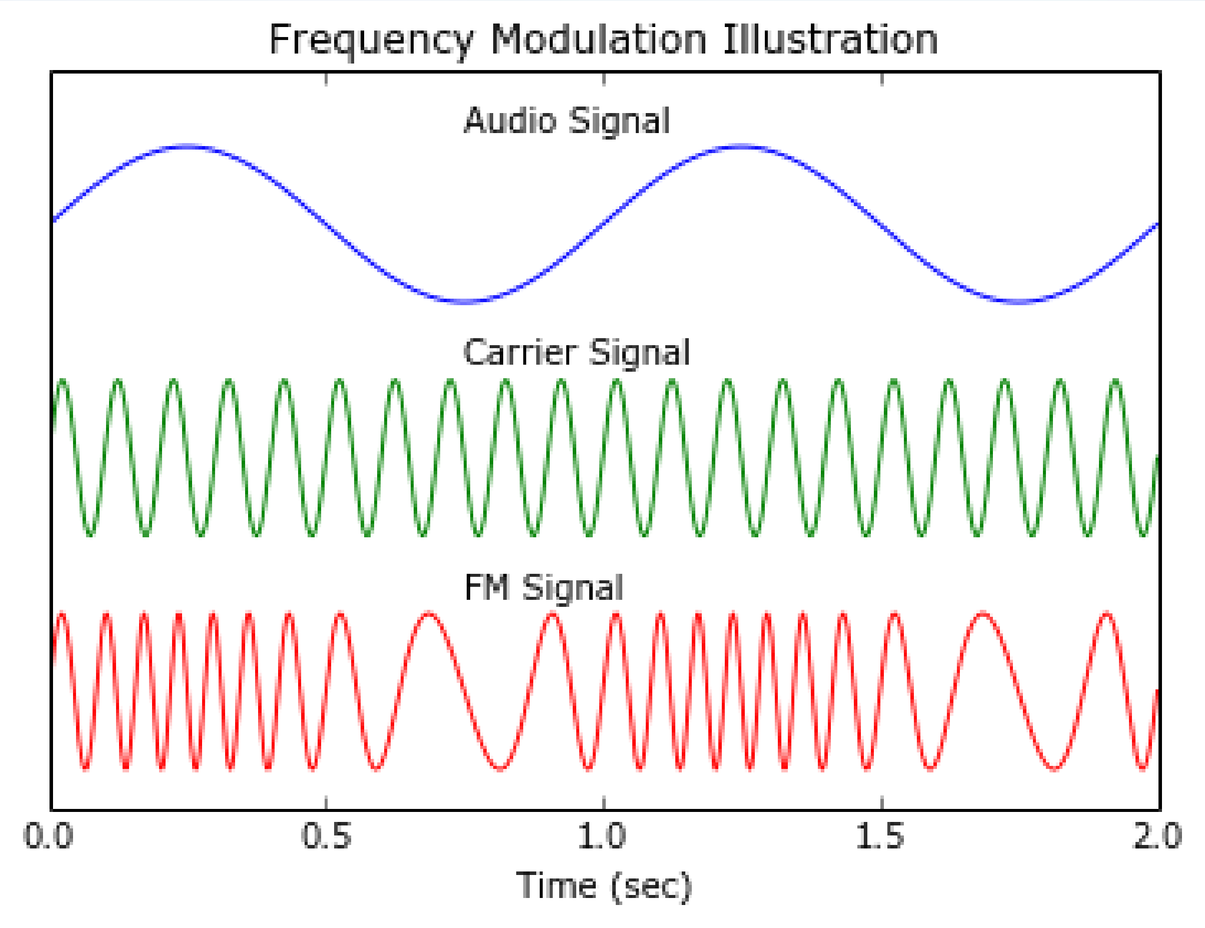
- **The Watergate bug**



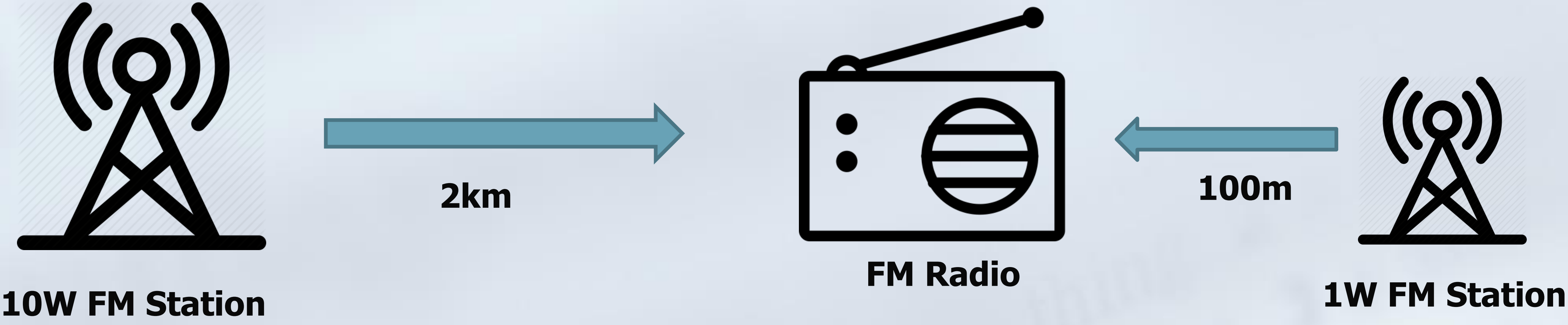
# Popular transmitters

- **Radio Ceylon**

# FM Signal


Frequency Modulation Illustration
Audio Signal
Carrier Signal
FM Signal
0.0
0.5
1.0
1.5
2.0
Time (sec)

# Hijacking the airwaves: Signal Intrusion



10W FM Station

2km

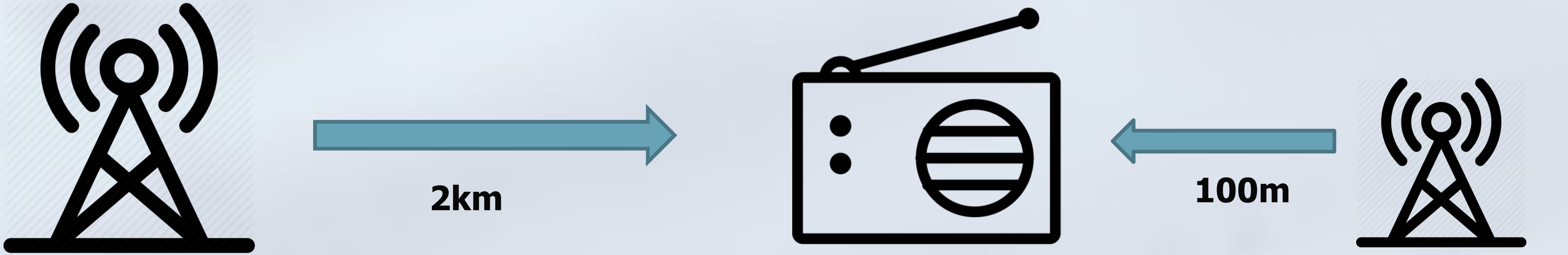
FM Radio

100m

1W FM Station

# Hijacking the airwaves: Signal Intrusion

- A stronger FM signal completely suppresses a weaker signal



10W FM Station

2km

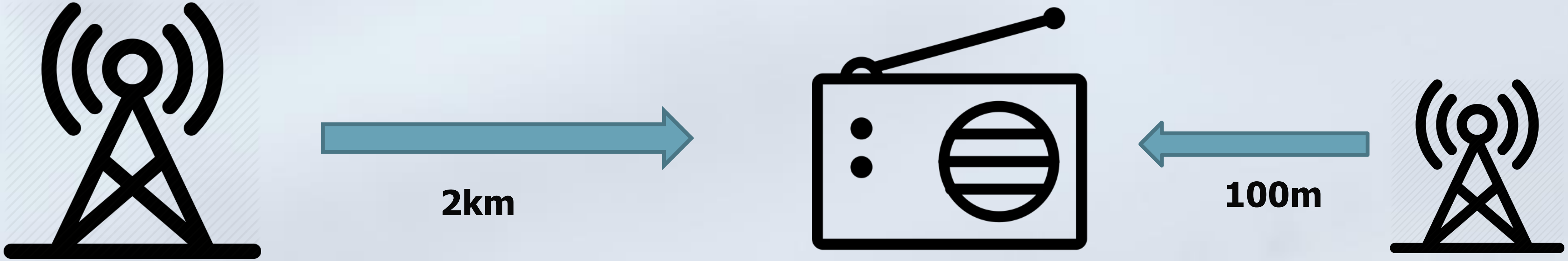
FM Radio

100m

1W FM Station

# Hijacking the airwaves: Signal Intrusion

- A stronger FM signal completely suppresses a weaker signal



10W FM Station

2km

FM Radio

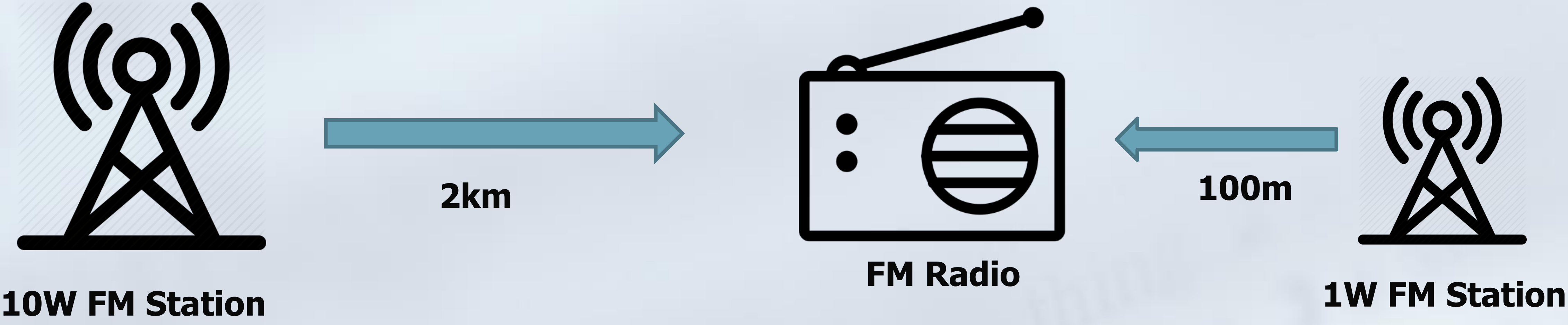
100m

1W FM Station

- Radio waves follow an inverse square law for power density

# Hijacking the airwaves: Signal Intrusion

- Every time we double the distance, we receive only one-fourth the power.



10W FM Station

2km

FM Radio

100m

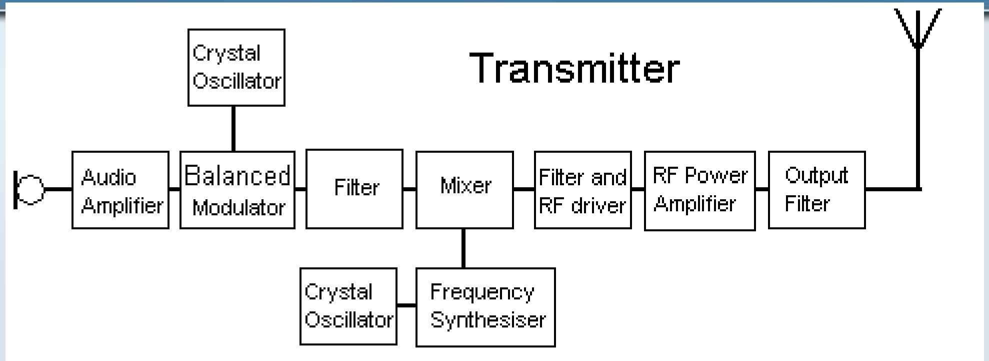
1W FM Station

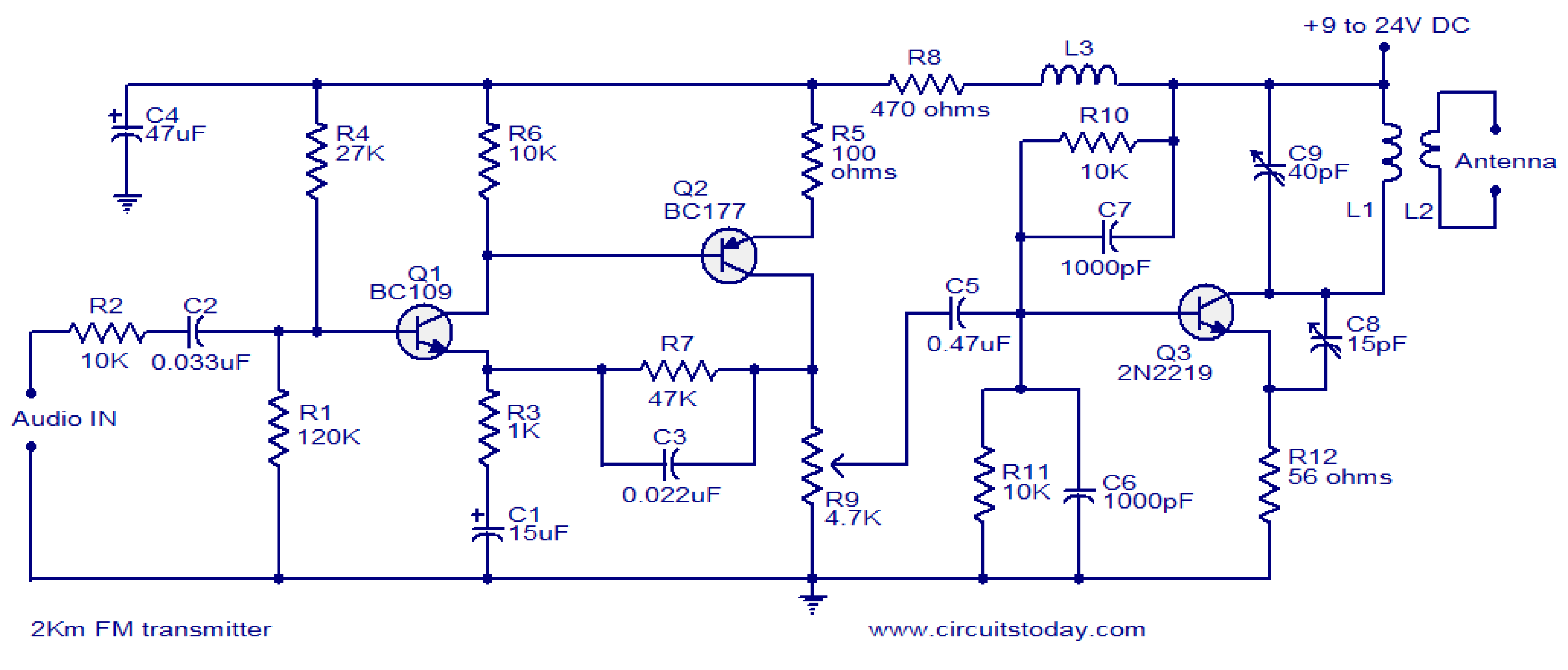
# Signal Intrusion: Possibilities

# Signal Intrusion: Applications

# Hijacking the airwaves

- The old school method





2Km FM transmitter

www.circuitstoday.com

# Hijacking the airwaves

- Software-defined radio (SDR) transceivers are much more flexible
- Software based signal processing

eg:

- **1. HackRF**
- 1MHz to 6GHz, USB powered
- half-duplex transceiver
- ₹ 27,230

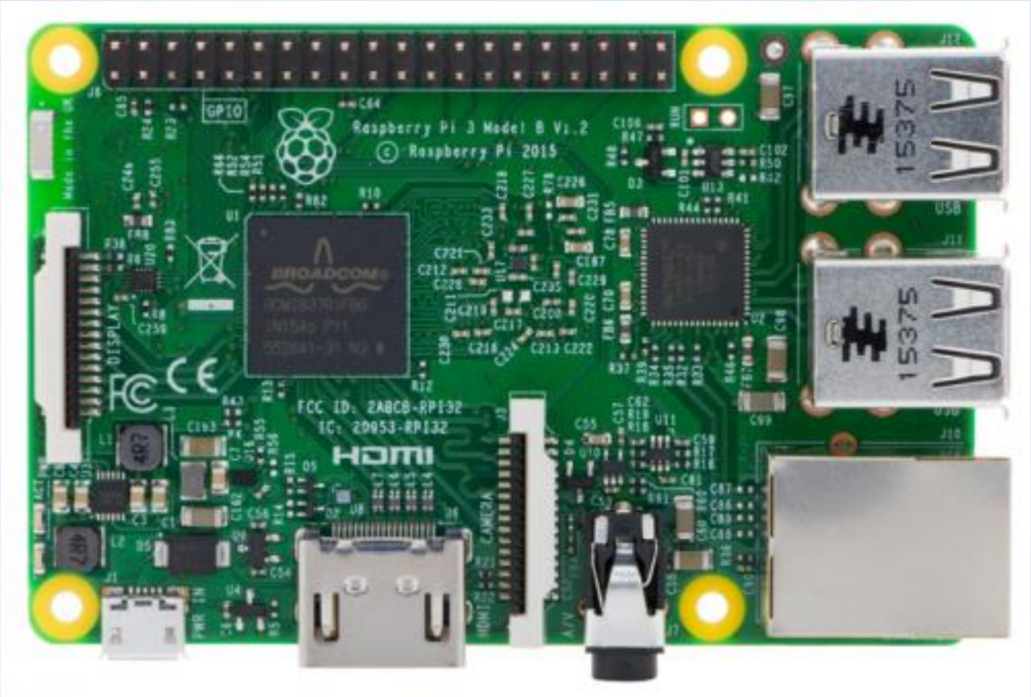
# Hijacking the airwaves

- **2. SparkFun bladeRF x40**
- can tune from 300MHz to 3.8GHz
- full duplex transceiver
- ₹ 45,385.00

- *Any cheaper alternatives?*

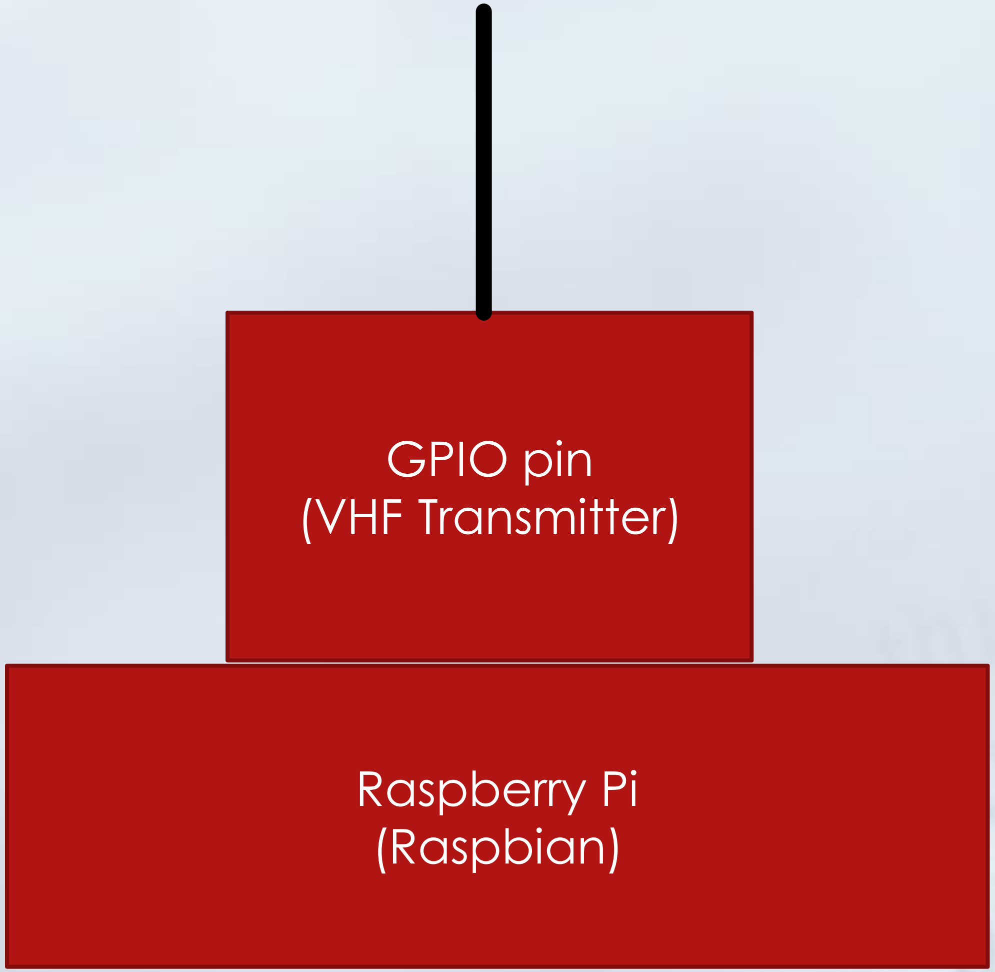
# What’s in it for me (WIIFM)?

- **Raspberry Pi** – yep, that single board computer
- designed for teaching kids to code



- **Raspberry Pi 3** $35
- 1.2GHz x64 quad-core ARM CPU
- 1 GB RAM
- OS – Raspbian, Debian based

# Hijacking the airwaves: Raspberry Pi

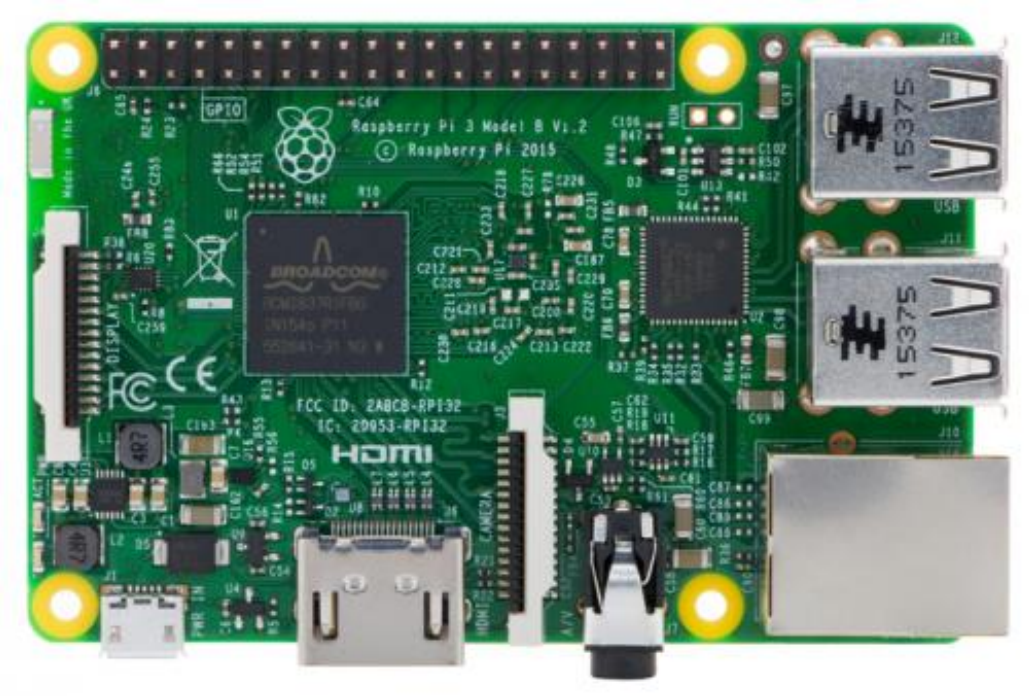


GPIO pin
(VHF Transmitter)

Raspberry Pi
(Raspbian)

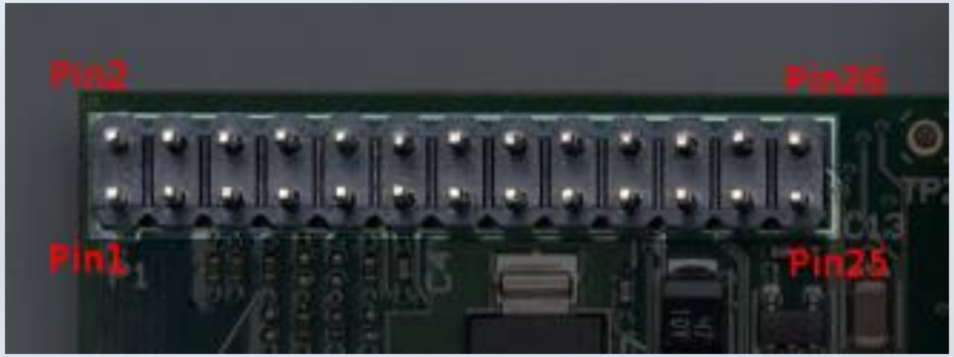
# Hijacking the airwaves - Software

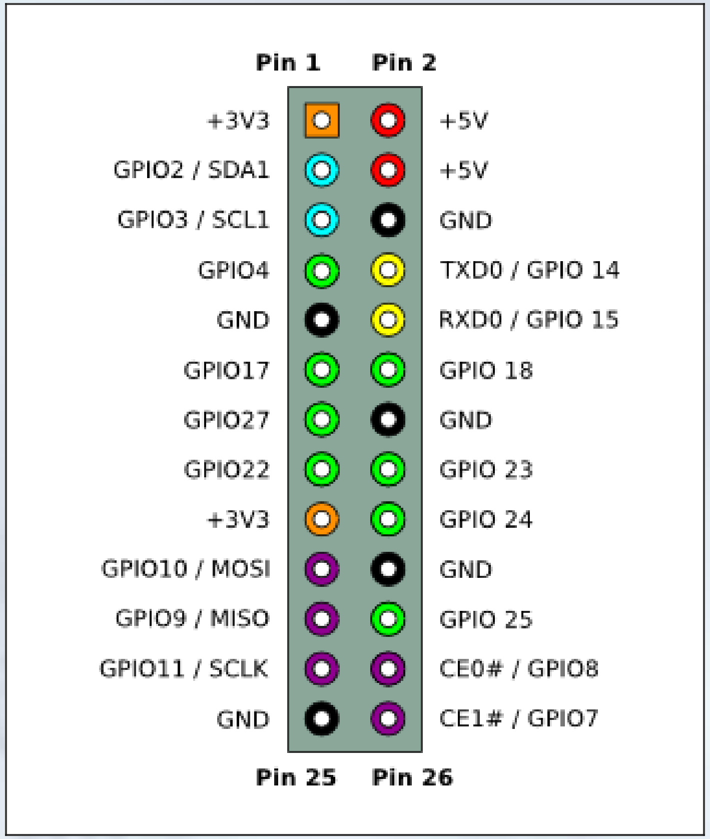
- **rpitx**
- radio transmitter for Raspberry Pi
- transmits RF directly to GPIO
- can handle frequencies from 5 KHz up to 1500 MHz.
- https://github.com/F5OEO/rpitx
- Supports Slow Scan Television (SSTV)



# Hijacking the airwaves - Hardware

- Plug a wire on GPIO 4,  Pin 7 of the GPIO header.
- This acts as the antenna





| | Pin 1 | Pin 2 | |
|---|---|---|---|
| +3V3 | ○ | ○ | +5V |
| GPIO2 / SDA1 | ○ | ○ | +5V |
| GPIO3 / SCL1 | ○ | ○ | GND |
| GPIO4 | ○ | ○ | TXD0 / GPIO 14 |
| GND | ○ | ○ | RXD0 / GPIO 15 |
| GPIO17 | ○ | ○ | GPIO 18 |
| GPIO27 | ○ | ○ | GND |
| GPIO22 | ○ | ○ | GPIO 23 |
| +3V3 | ○ | ○ | GPIO 24 |
| GPIO10 / MOSI | ○ | ○ | GND |
| GPIO9 / MISO | ○ | ○ | GPIO 25 |
| GPIO11 / SCLK | ○ | ○ | CE0# / GPIO8 |
| GND | ○ | ○ | CE1# / GPIO7 |
| | Pin 25 | Pin 26 | |

# Unknown guy talks ATC from his BATHTUB

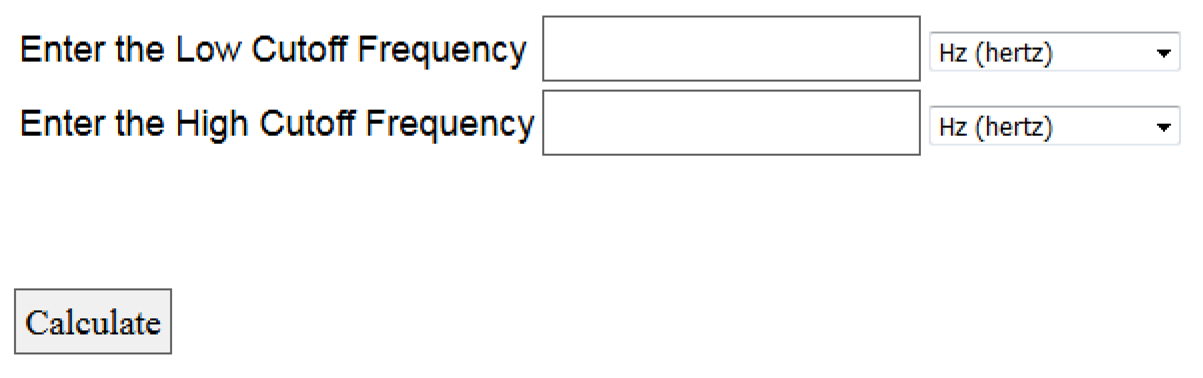
- Source: https://www.youtube.com/watch?v=ZvA_-linhg8

# How to start…

- Do no harm to any existing communication systems
- Use appropriate Band-pass filters to ensure that we are transmitting only at the permitted frequency

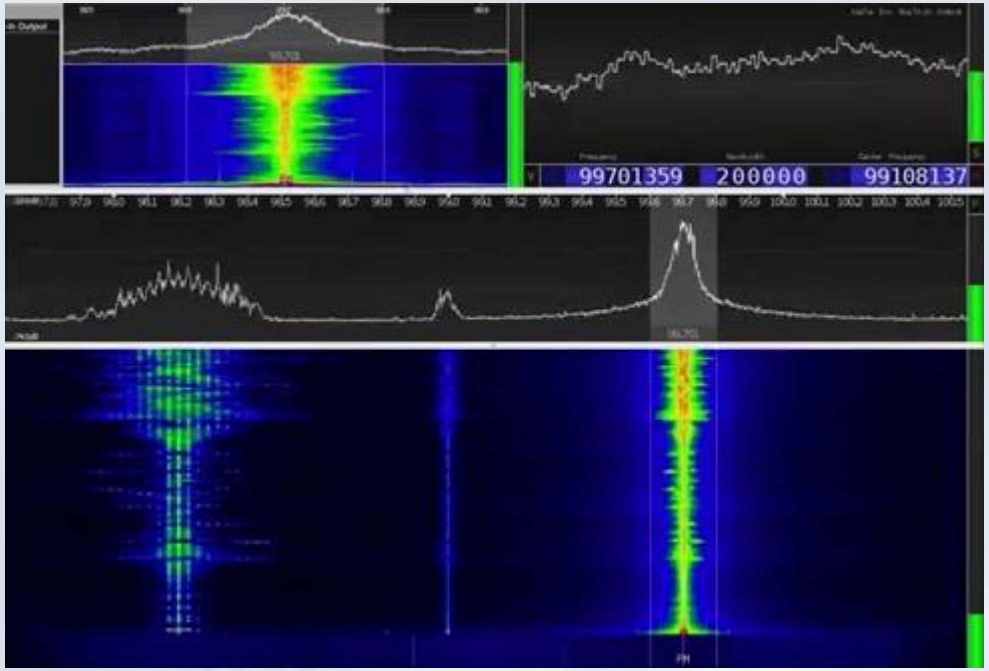
# How to start…

- http://www.learningaboutelectronics.com/Articles/Bandpass-filter-calculator.php



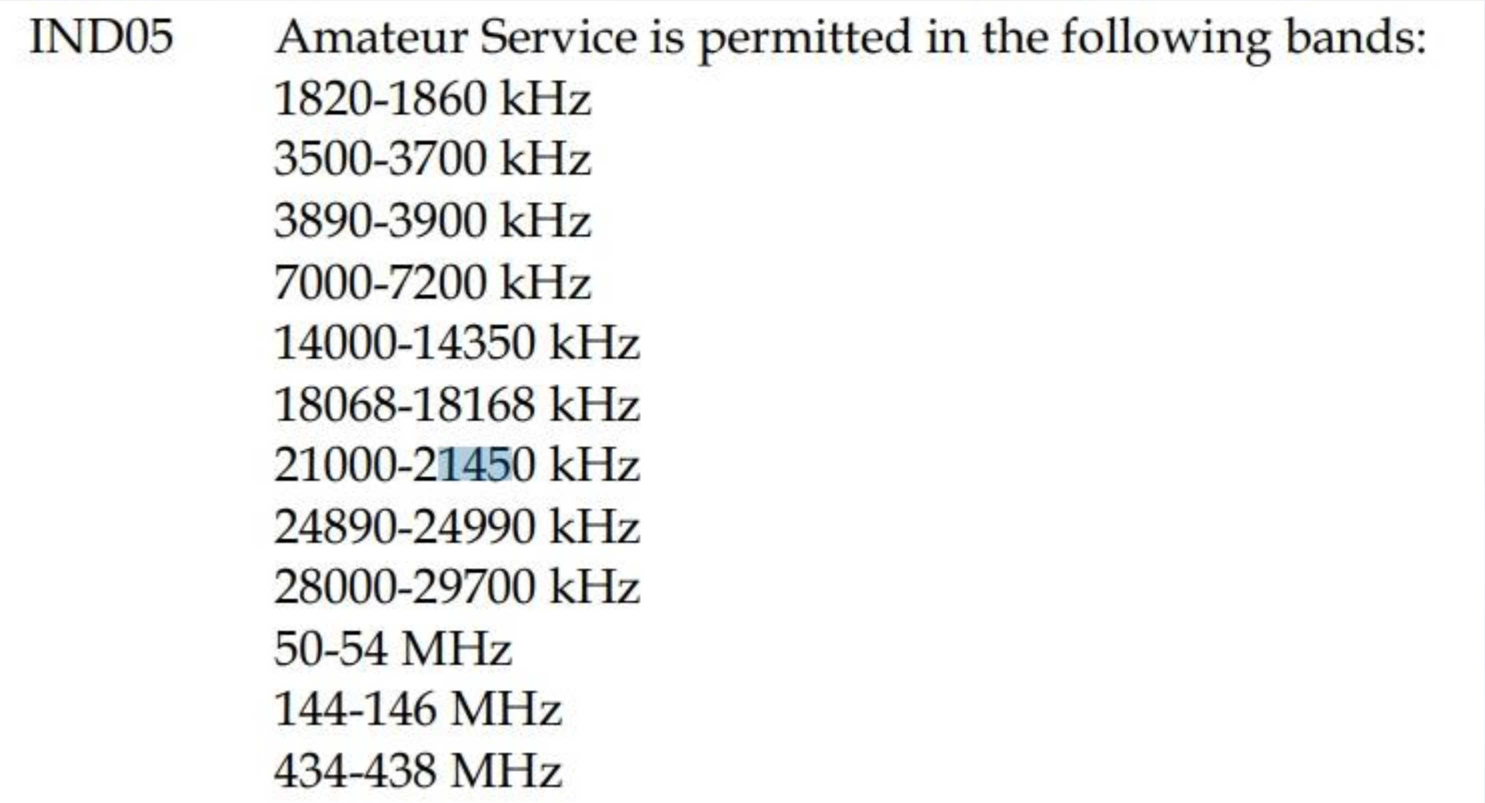
Enter the Low Cutoff Frequency Hz (hertz)

Enter the High Cutoff Frequency Hz (hertz)



# Transmitting the radio waves

- Make sure that you are confirming to local laws
- In India, if you have a ham radio license

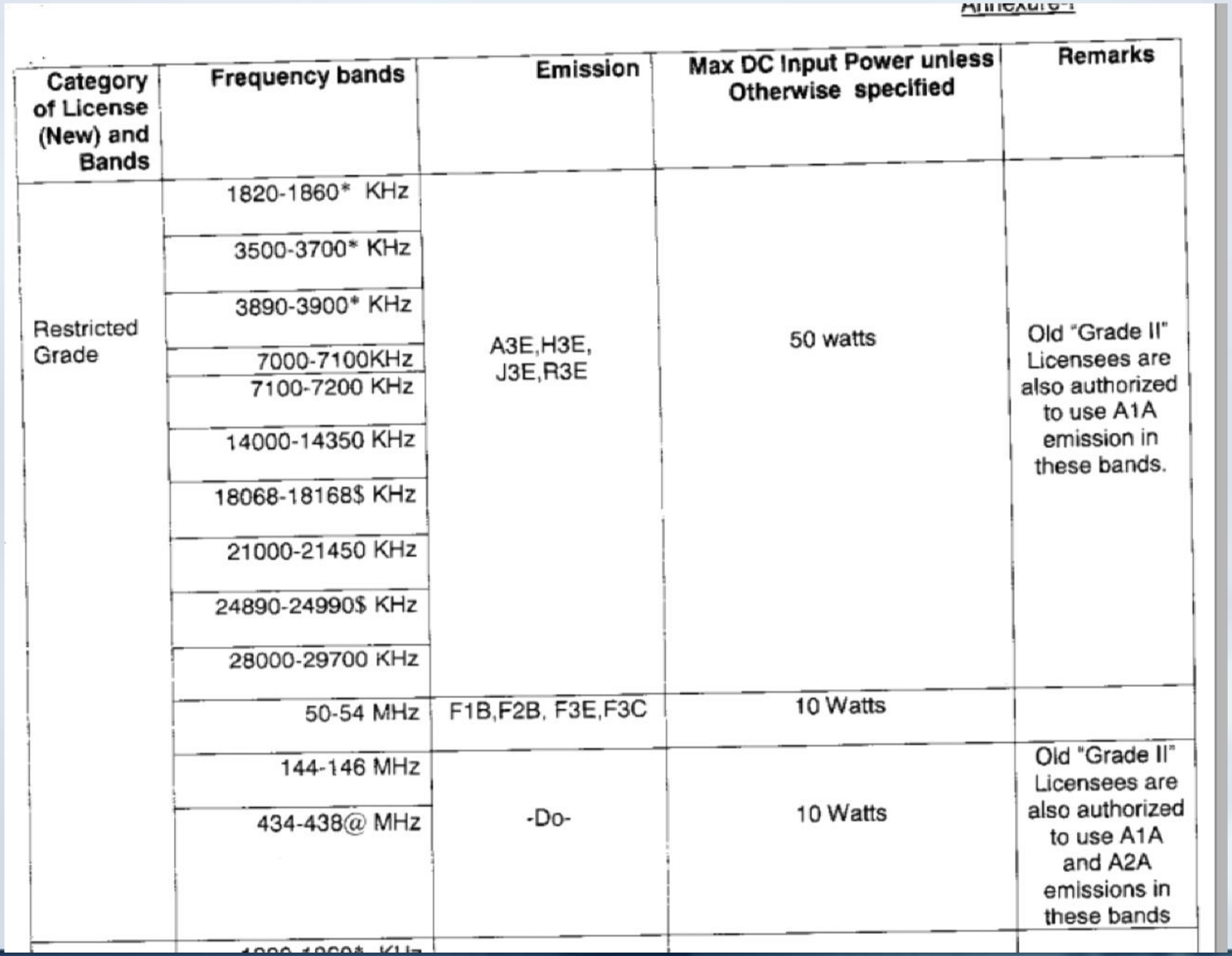


IND05 Amateur Service is permitted in the following bands:

1820-1860 kHz
3500-3700 kHz
3890-3900 kHz
7000-7200 kHz
14000-14350 kHz
18068-18168 kHz
21000-21450 kHz
24890-24990 kHz
28000-29700 kHz
50-54 MHz
144-146 MHz
434-438 MHz

# Transmitting the radio waves

- In India, if you have a ham radio license



Annexure-I

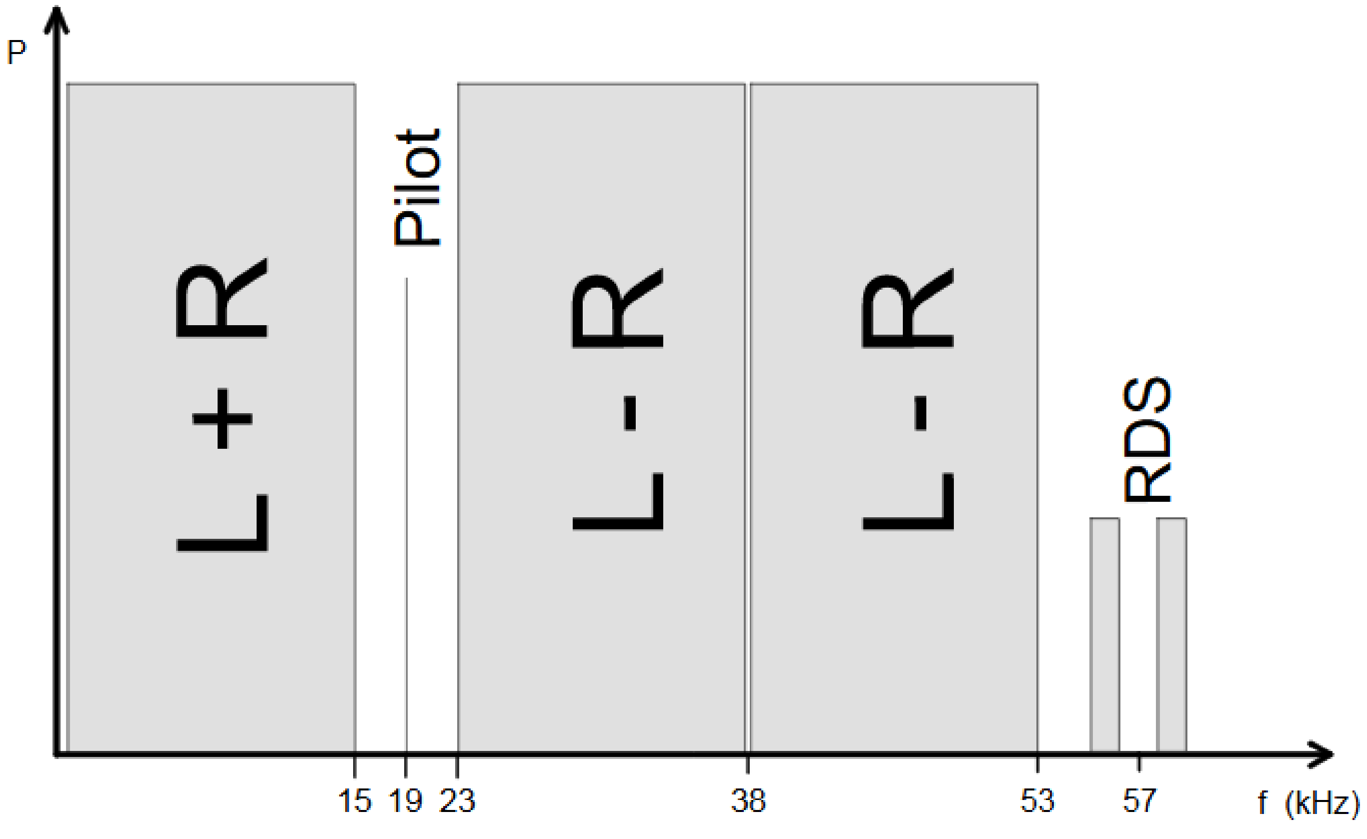
| Category of License (New) and Bands | Frequency bands | Emission | Max DC Input Power unless Otherwise specified | Remarks |
|---|---|---|---|---|
| Restricted Grade | 1820-1860* KHz | A3E,H3E, J3E,R3E | 50 watts | Old "Grade II" Licensees are also authorized to use A1A emission in these bands. |
| | 3500-3700* KHz | | | |
| | 3890-3900* KHz | | | |
| | 7000-7100KHz | | | |
| | 7100-7200 KHz | | | |
| | 14000-14350 KHz | | | |
| | 18068-18168$ KHz | | | |
| | 21000-21450 KHz | | | |
| | 24890-24990$ KHz | | | |
| | 28000-29700 KHz | | | |
| | 50-54 MHz | F1B,F2B, F3E,F3C | 10 Watts | |
| | 144-146 MHz | -Do- | 10 Watts | Old "Grade II" Licensees are also authorized to use A1A and A2A emissions in these bands |
| | 434-438@ MHz | | | |

# Transmitting the radio waves

- In India, if you have a ham radio license
- 144-146MHz band
  - F1B: Frequency-shift keying (FSK) telegraphy, such as RTTY
  - F2B: frequency modulation telegraphy with automatic reception
  - F3C: modulation frequency facsimile
  - F3E: FM speech communication

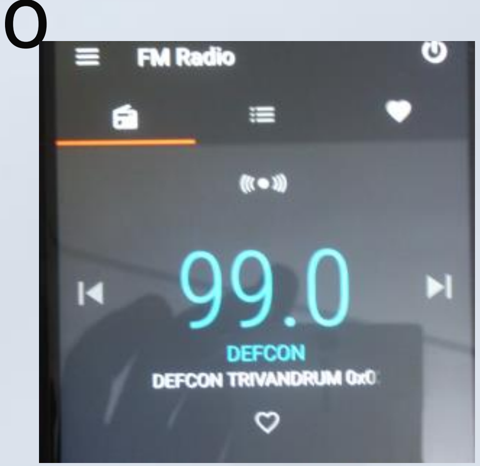
# RDS - Radio Data System

- protocol for embedding small amounts of digital information in FM radio broadcasts



# RDS - Radio Data System

- https://github.com/ChristopheJacquet/PiFmRds
- rt: radiotext to be transmitted, max 64 characters
- control it at run-time using a named pipe, perfect ploy for tunnelling data from an air-gapped system
- Feed malicious frequencies to “Alternative Frequencies” for hijacking RDS radio

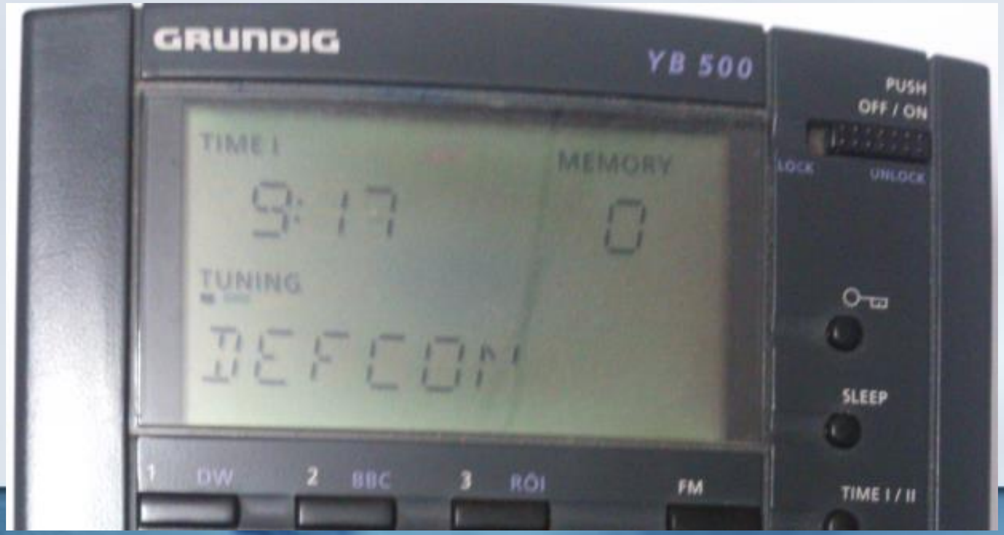


FM Radio

99.0

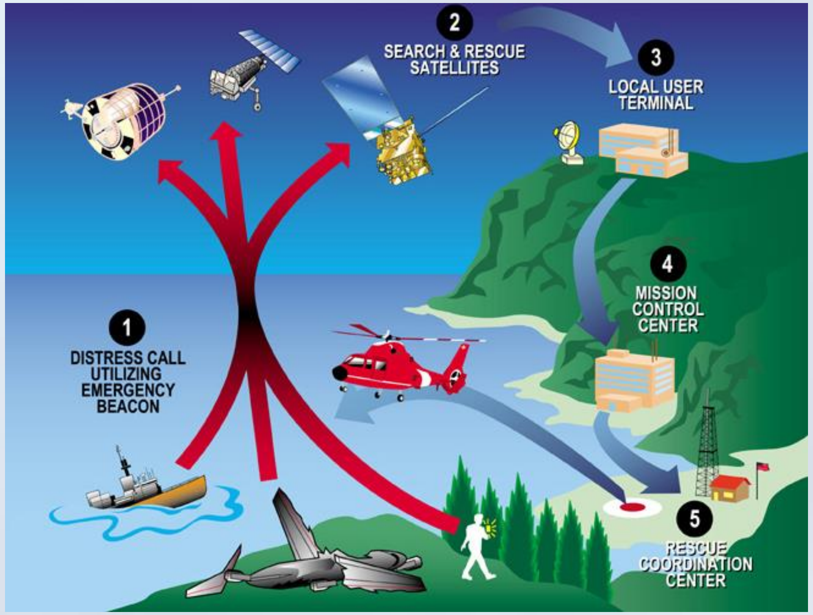
DEFCON

DEFCON TRIVANDRUM 0x0



# Radio Direction Finding (RDF)

- “the art of locating a signal or noise source with portable receivers and directional antennas”
- used to locate or emergency beacons
- tracking down sources of interference on the ham bands, intentional or unintentional !
- Wireless Planning and Coordination Wing – DoT does it

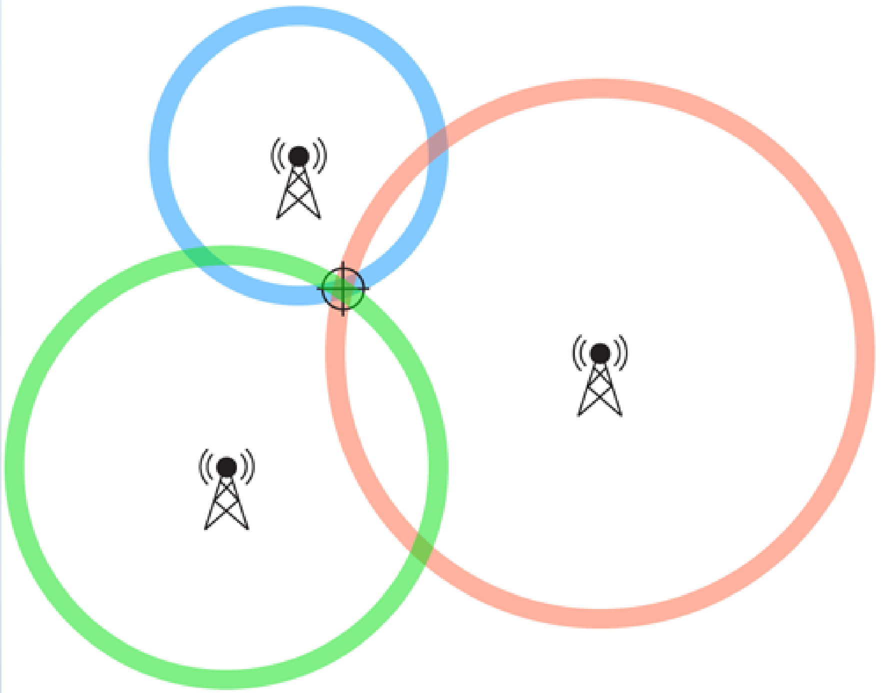

2
SEARCH & RESCUE SATELLITES
3
LOCAL USER TERMINAL
4
MISSION CONTROL CENTER
1
DISTRESS CALL UTILIZING EMERGENCY BEACON
5
RESCUE COORDINATION CENTER

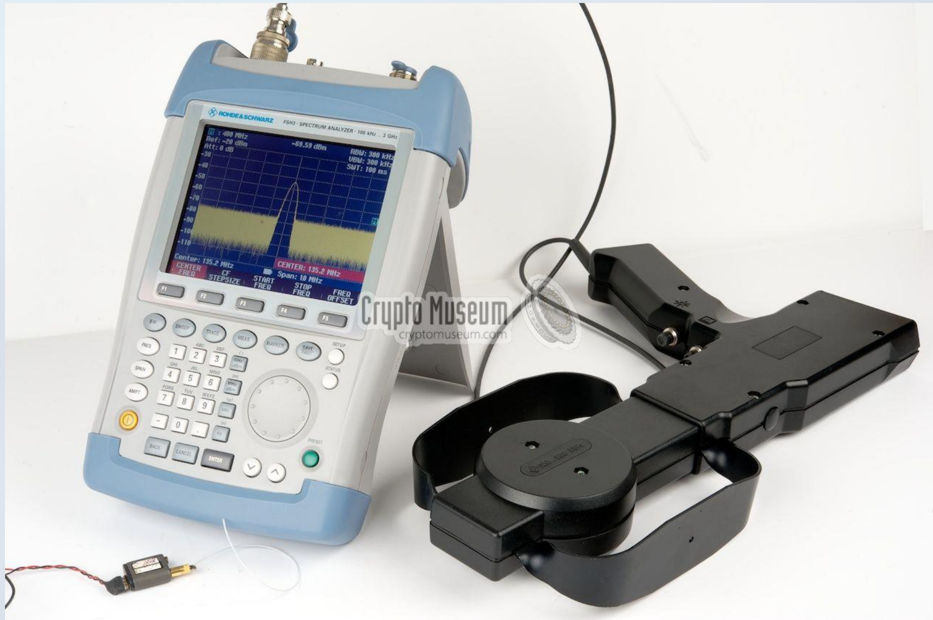
# Radio Direction Finding (RDF)

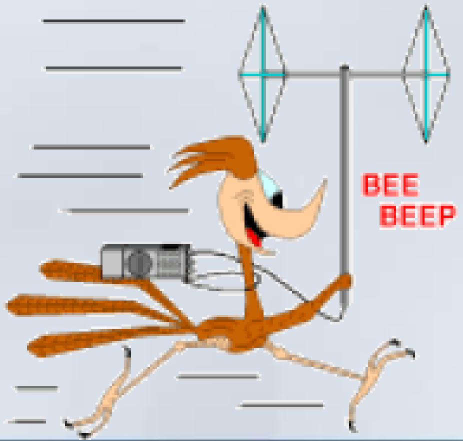
- PR100 is a portable digital receiver
- covers all frequencies from 9 kHz to 7.5 GHz
- **$16,999.00**
- Alternative: RTL-SDR

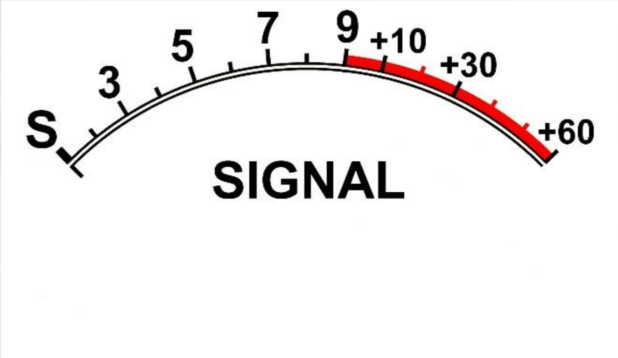
# Radio Direction Finding (RDF)

- Portable active directional antenna HE 100
- Triangulation









# Lincolnshire Poacher Number Station

- Source: https://www.youtube.com/watch?v=YnGnIOz6WTw

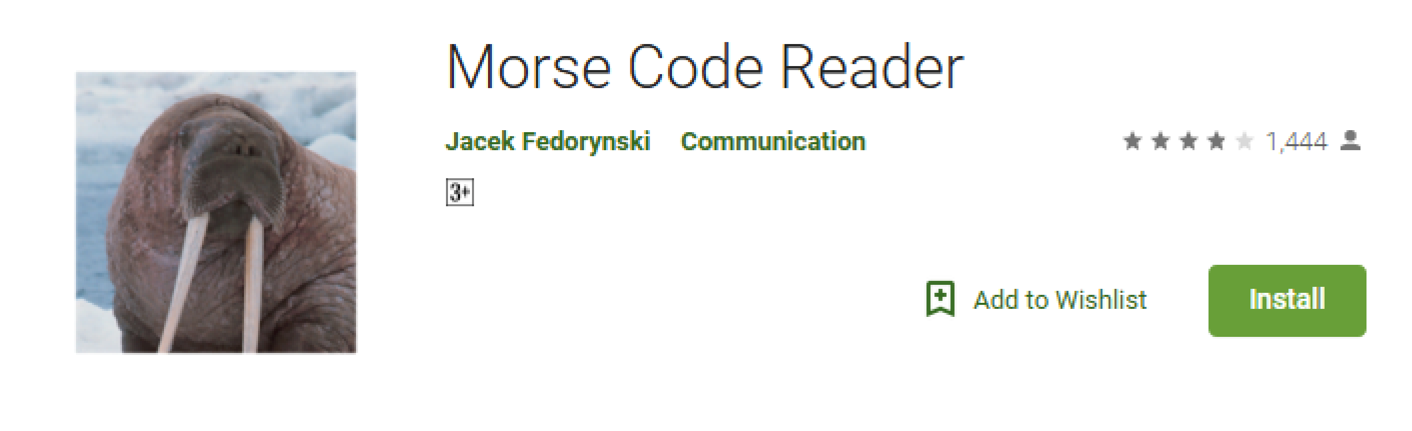
# System Bus Radio

- Transmit RF directly from computer, laptop or phone without any transmitting hardware at all
- https://github.com/fulldecent/system-bus-radio
- https://fulldecent.github.io/system-bus-radio/

- Tested on MacBook Air / Chrome with AM tuner at 1560 kHz

# Demo

- Please install Morse Code Reader from Google Play https://play.google.com/store/apps/details?id=org.jfedor.morsecode&hl=en



Morse Code Reader

Jacek Fedorynski Communication ★★★★☆ 1,444

3+

Add to Wishlist

Install

GCA FINAL DIRECTOR CALLING "BIG WILLIE" 5555. FINAL COCKPIT CHECK. FLAPS DOWN LANDING GEAR EXTENDED, FINGERS CROSSED...
51
SCHUFFERT

# Questions

# Reach me

- *@vipinonline*
- linkedin.com/in/vipingeo
- t.me/vipinonline
- *www.vipinonline.com*

DEF CON

DC 0471 TRIVANDRUM

# Thank You!