ELECTRONIC WARFARE (EW) AND HAM RADIO

HOW DO THEY RELATE?

PRESENTATION TO TRI-LAKES MONUMENT RADIO ASSOCIATION

BRYANT CLAYTON, KEØHOU – ARMY EW INSTRUCTOR

LOREN ANDERSON, KEØHZ

17 JANUARY 2022

WHAT IS EW?

- **Electronic warfare** (**EW**) is any action involving the use of the electromagnetic spectrum (EM spectrum) or directed energy to control the spectrum, attack an enemy, or impede enemy assaults. The purpose of electronic warfare is to **deny the opponent the advantage of, and ensure friendly unimpeded access to the EM spectrum**. EW can be applied from air, sea, land, and/or space by manned and unmanned systems, and can target communication, radar, or other assets (military and civilian). [https://en.wikipedia.org/wiki/Electronic_warfare]
- We're primarily going to look at the defensive aspect of EW.

DEFENSE PRIMER: ELECTRONIC WARFARE

- Electronic warfare (EW), as defined by the Department of Defense (DOD), are military activities that use electromagnetic energy to control the electromagnetic spectrum ("the spectrum") and attack an enemy. The spectrum is a range of frequencies for electromagnetic energy. EW supports command and control (C2) by allowing military commanders' **access to the spectrum to communicate with forces**, while preventing potential adversaries from accessing the spectrum to develop an operational picture and communicate with their forces. Some have argued that EW is a component of anti-access/area denial (A2/AD) campaigns.
- Statement from Congressional Research Service – IN FOCUS Oct 29, 2020
- https://crsreports.congress.gov/product/pdf/IF/IF11118/9

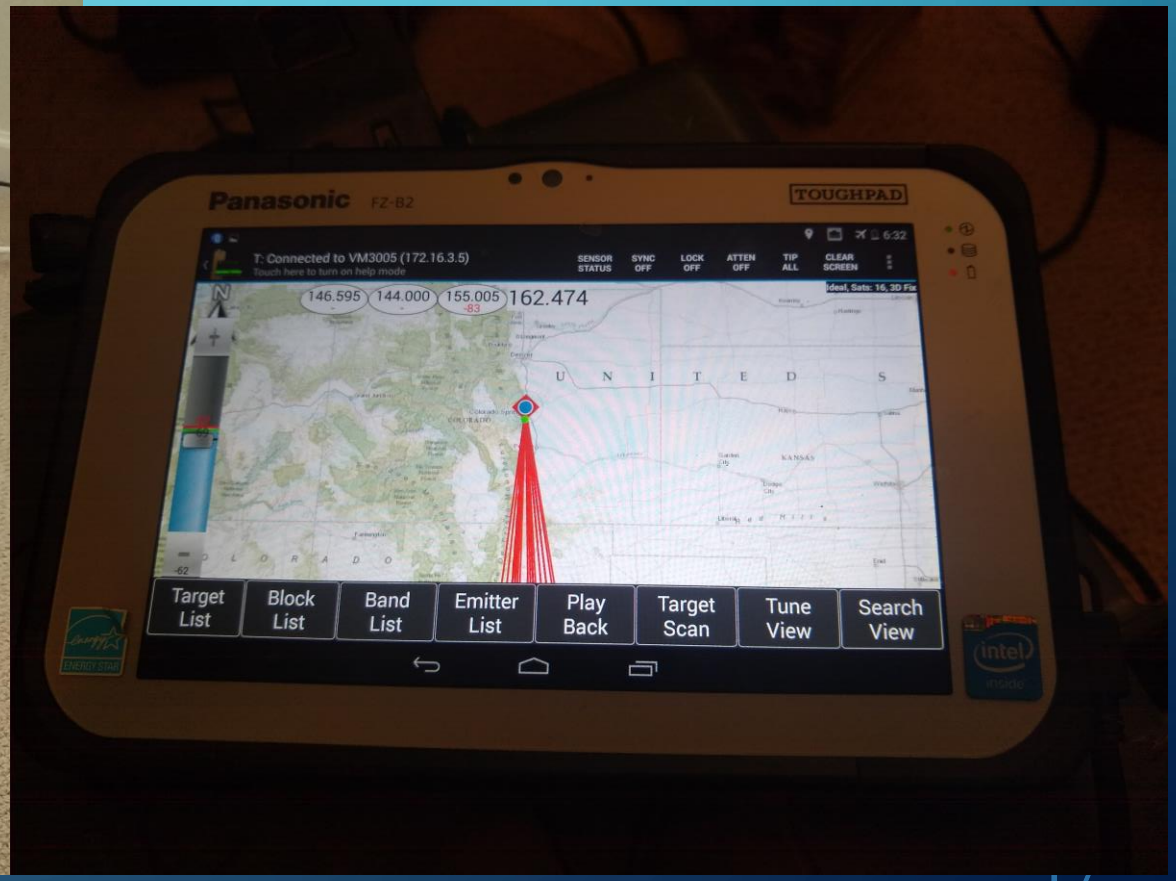
HOW DOES EW RELATE TO HAM RADIO?

- Note section from description:

  "… ensure friendly unimpeded access to the EM spectrum."

- ***Usually*** interfering signals in the Amateur Radio allocated spectrum are not intentional. But anyone who has tried to work rare DX or contest pile-ups or participate in a scheduled net during periods of poor propagation or magnetic disturbances has not had that unimpeded access at various times.
- Unless in an emergency, the criticality of Amateur Radio communications isn't comparable to a battlefield. That said, there are many similarities.

EW EQUIPMENT



WHO CONDUCTS EW

- Army Perspective – Ground troops
  - Tactical level elements (company and platoon size elements)
  - 4 – 6 man teams
- EW Operations
  - Finding and characterizing emitters
  - Tactical operations
  - Drones becoming ubiquitous

OFFENSIVE TECHNIQUES

- Channel disruption (Hams frequently have to deal with QRM)
  - Denial of service (GPS, comms)
- Spoofing
  - Apparent good service but inaccurate information (GPS)
    - Ship detained for being in Iranian waters in Strait of Hormuz
    - UAS crash in Iran
- Create Interference
  - Raising noise floor

DEFENSIVE TECHNIQUES

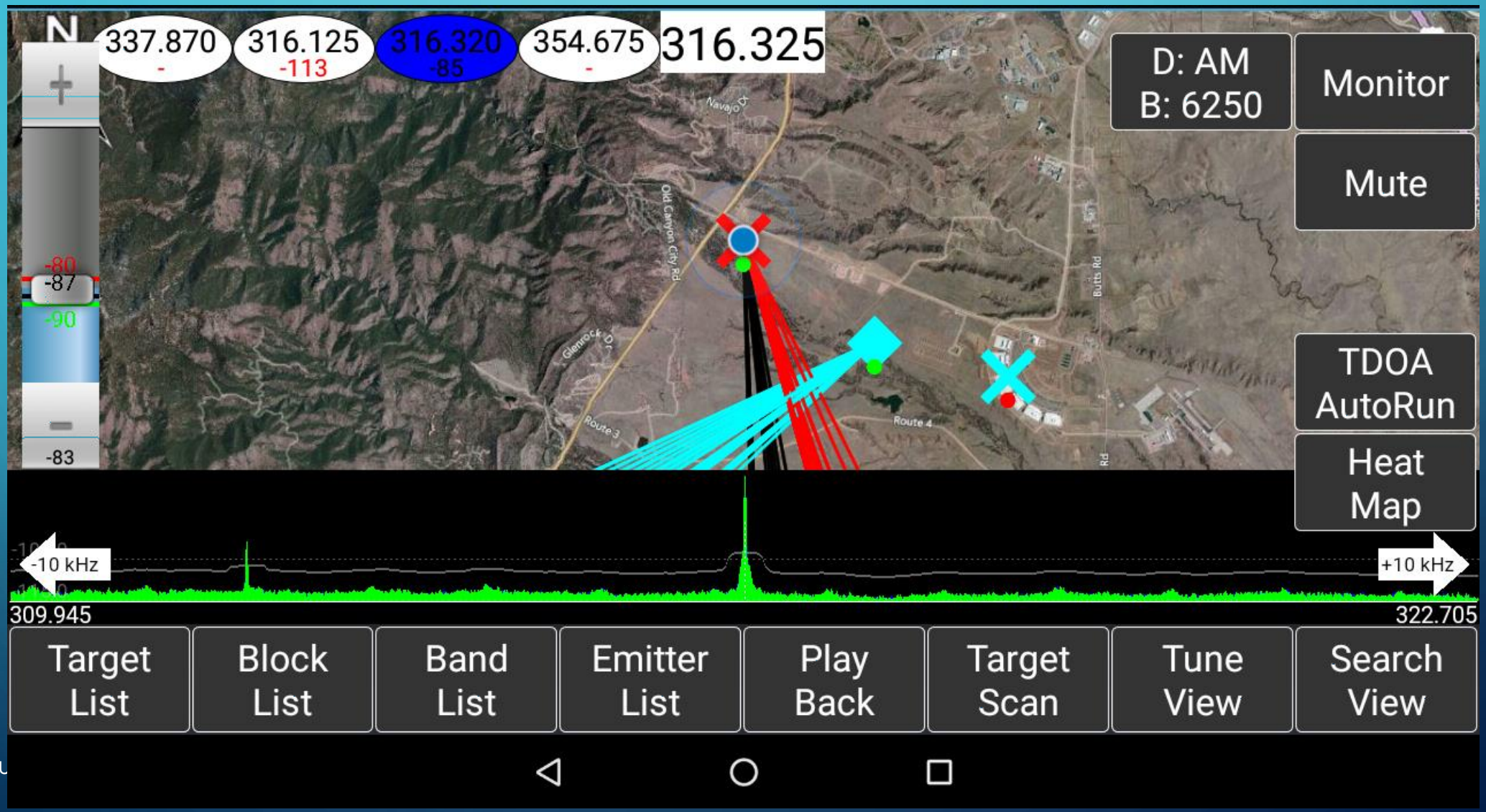
- Hardening equipment (shielding)
- Alternative modes & comm bands/channels
- Improved sensitivity, selectivity, & directionality
- Frequency agility
- Encryption

- How do troops on the ground, aboard ships, or aircraft deal with enemy's offensive measures?
  - Locate signal source (fox hunt/radio link budget)
  - Frequency agility (spread spectrum)
  - Encryption (DMR, SystemFusion, etc.) *Amateurs are not actually encrypting but could easily do so if permitted
  - Signal obfuscation

CHARACTERIZE THE ENVIRONMENT

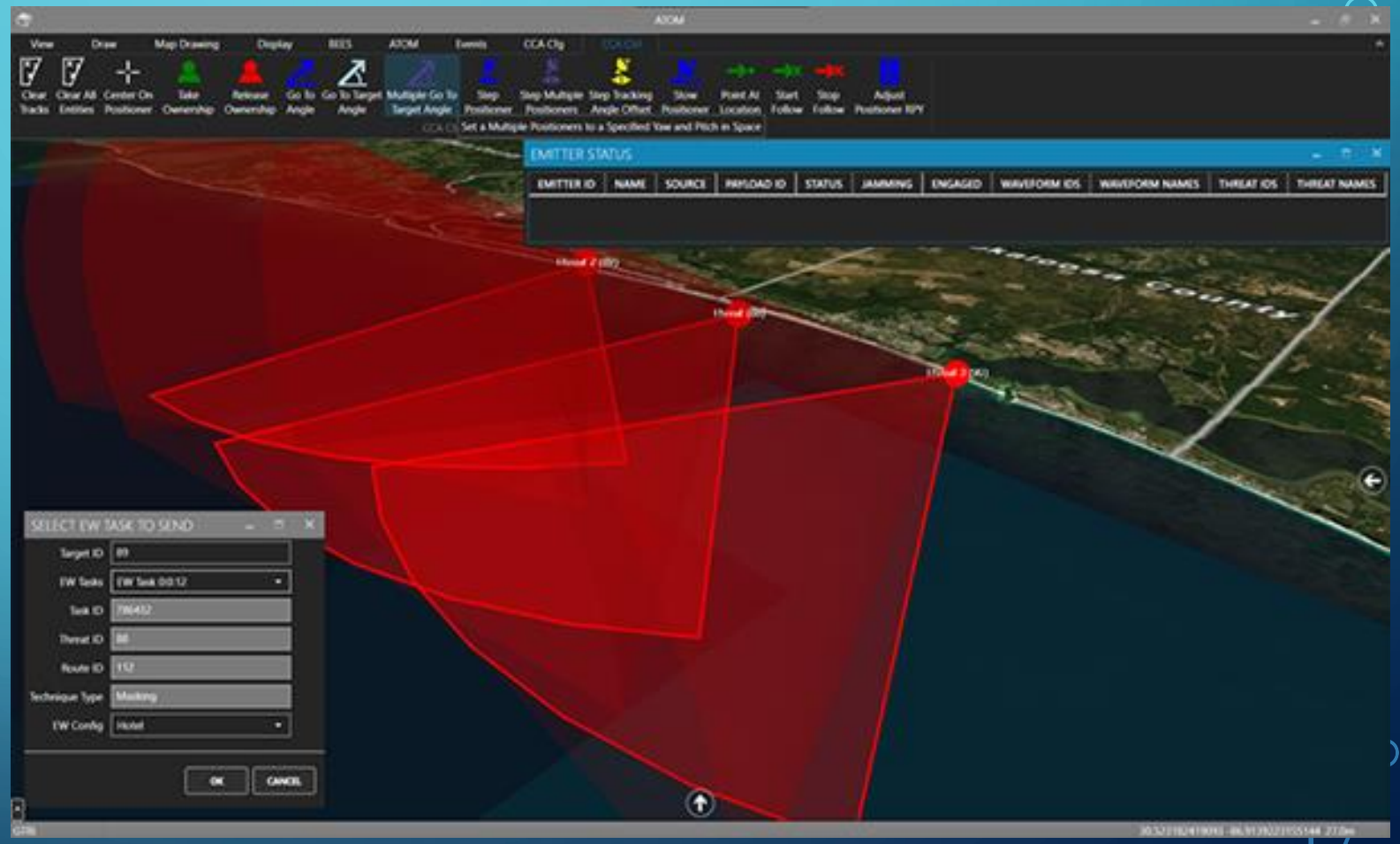
- What signals are present?
- Who is responsible?
- Where is the emitter?

SIGNALS OF INTEREST



ELECTROMAGNETIC BATTLE MANAGEMENT FOR DISTRIBUTED ELECTRONIC WARFARE PROGRAM

- Highly sophisticated fox hunt
- Our adversaries currently sitting offshore in international waters of U.S. territory conducting EW operations (allegedly)

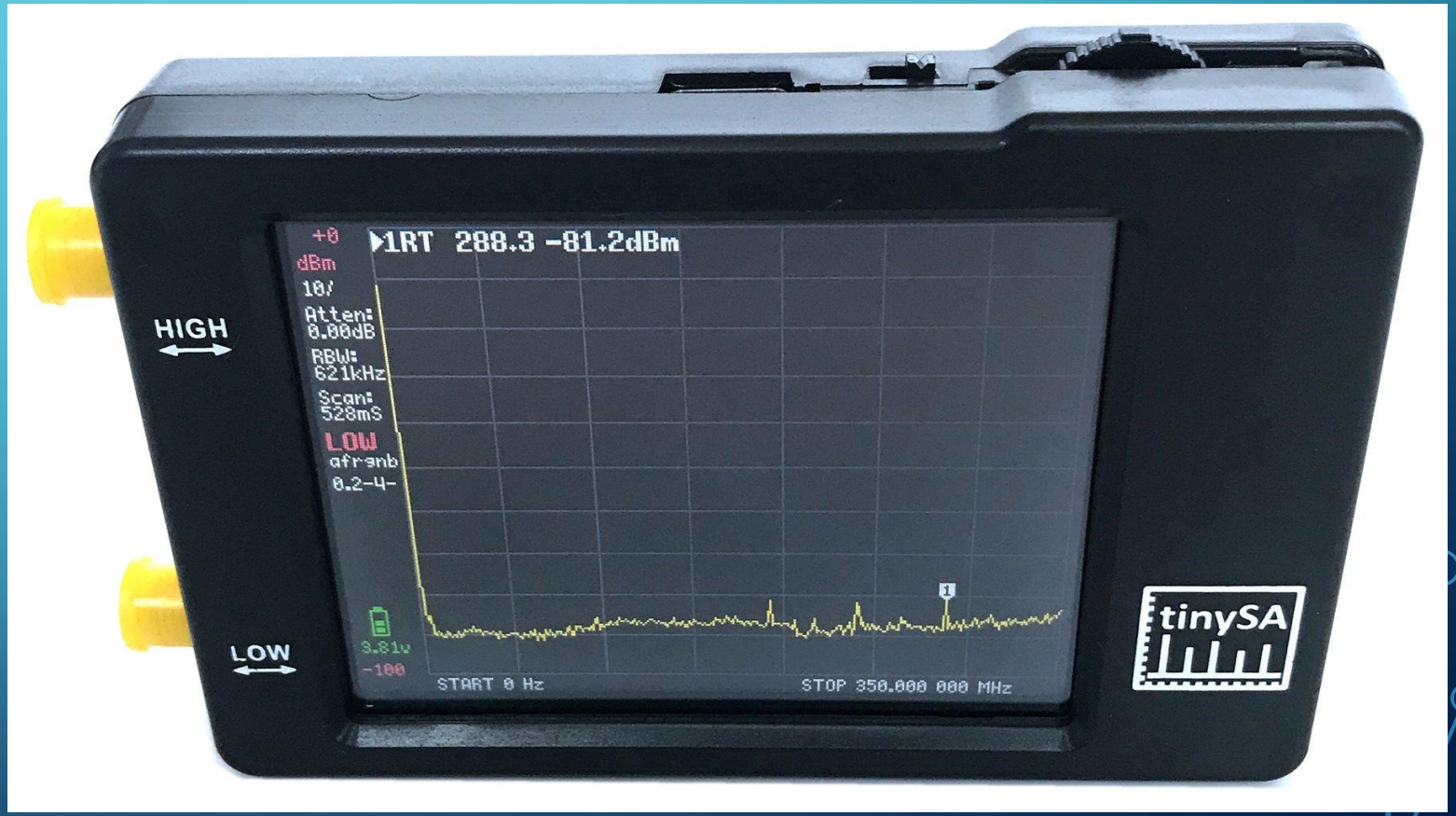


TOOLS AVAILABLE TO HAMS

- Spectrum characterization
  - Spectrum Analyzer
  - Panadapter (on receiver/transceiver or external)
- Directional antennas
- Software Defined Radios (SDR) have been game changers

BUDGET SPECTRUM ANALYZER

- https://tinysa.org/wiki/pmwiki.php?n=Main.HomePage
- 100 KHz – 960 MHz
- Includes Signal Generator
- eBay price - ~$68



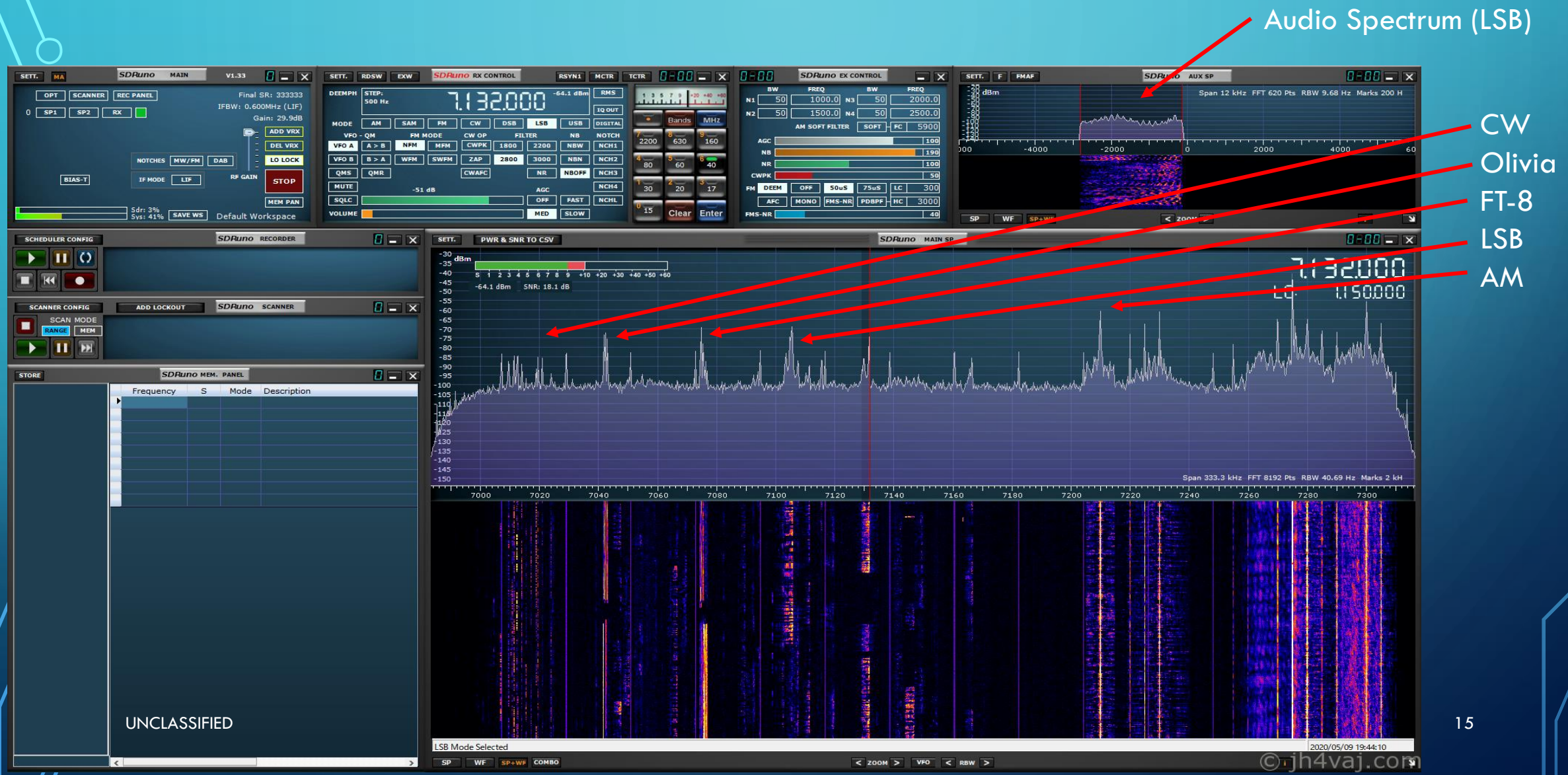
PANADAPTER

- From https://radioaficion.com/cms/what-is-a-panadapter/

"A panadapter is essentially a spectrum analyzer that connects to the IF of your receiver and shows activity on the currently selected band."

KX3, KXPD3 paddle and PX3 (sold separately)

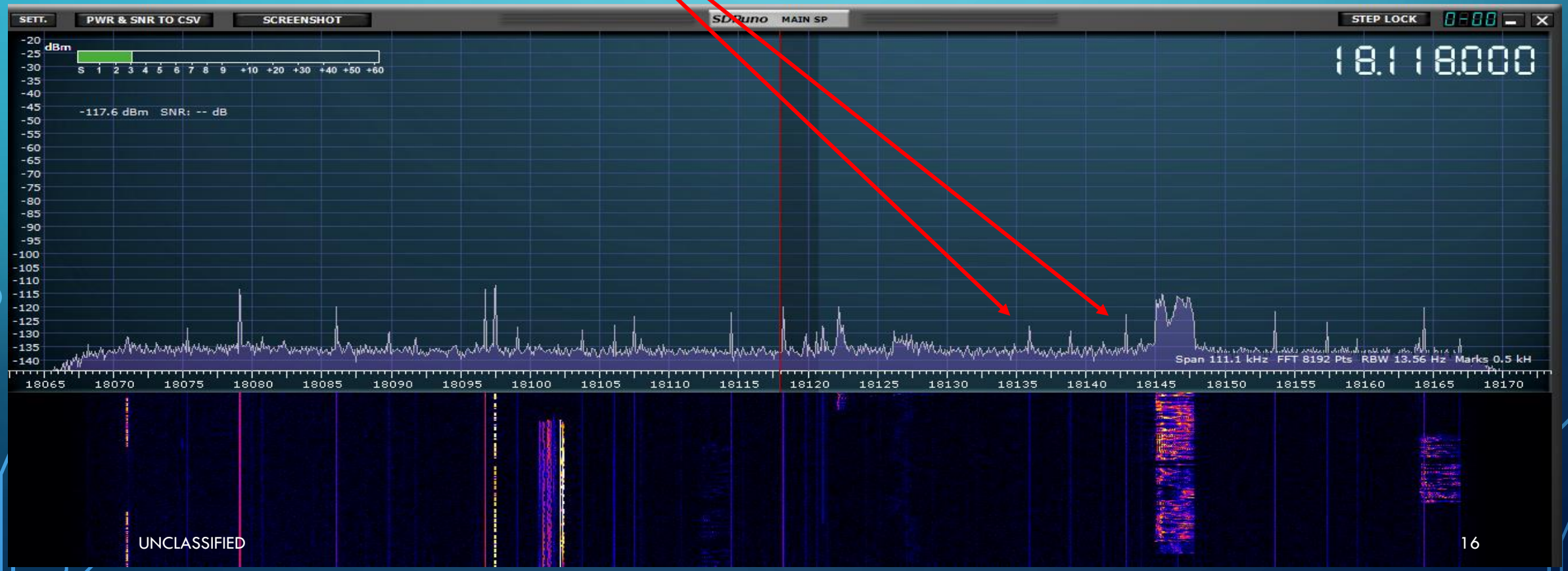
SDR PLAY & SDRUNO SOFTWARE PANADAPTER



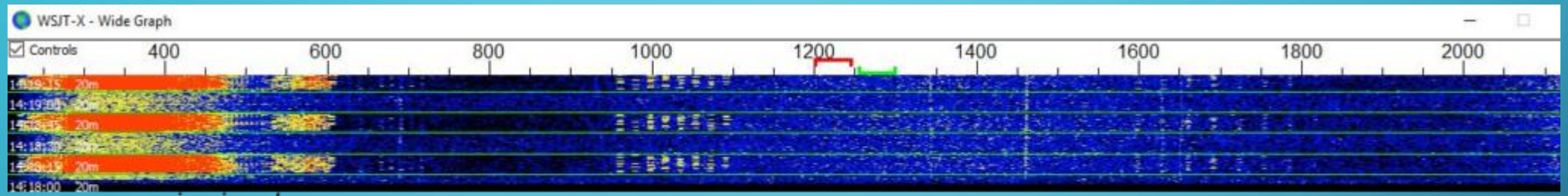
UNINTENTIONAL JAMMING?

What are these signals? They are not other hams.

What frequency is best for me to use?



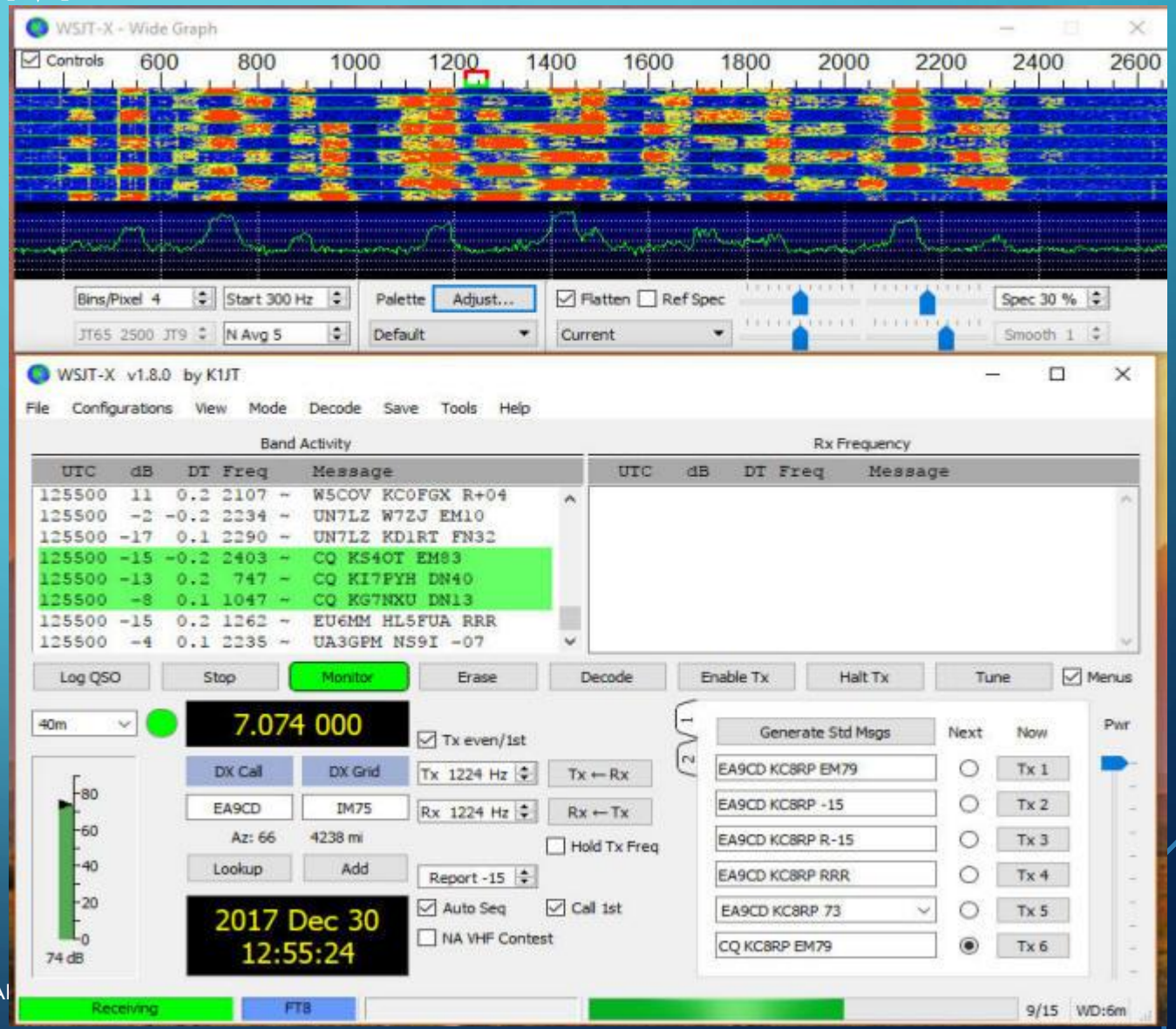
INTERFERING SIGNALS ON FT-8



Inadvertent interference caused by over modulation. Clipping of audio signals introduces harmonics within 2.5 KHz FT-8 bandwidth. Watch your ALC!!!

CLEAN FT-8 SPECTRUM

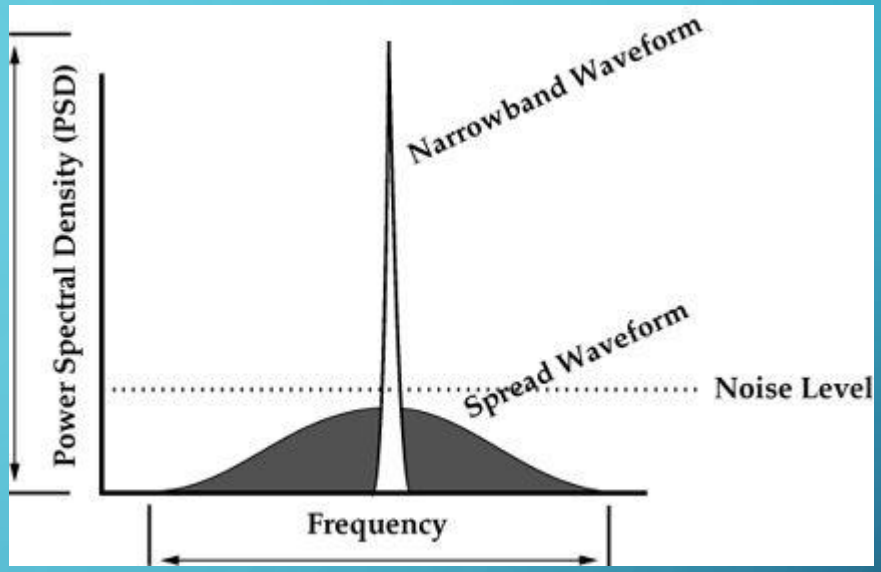
- Where do you choose to operate?

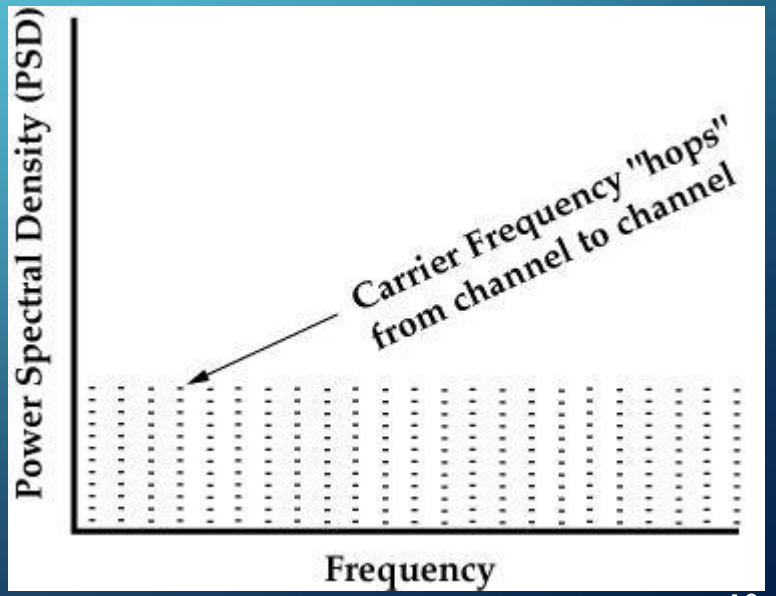


SPREAD SPECTRUM

- Advantages:
  - Resists intentional and non-intentional interference
  - Has the ability to eliminate or alleviate the effect of multipath interference
  - Can share the same frequency band (overlay) with other users
  - Privacy due to the pseudo random code sequence (code division multiplexing)

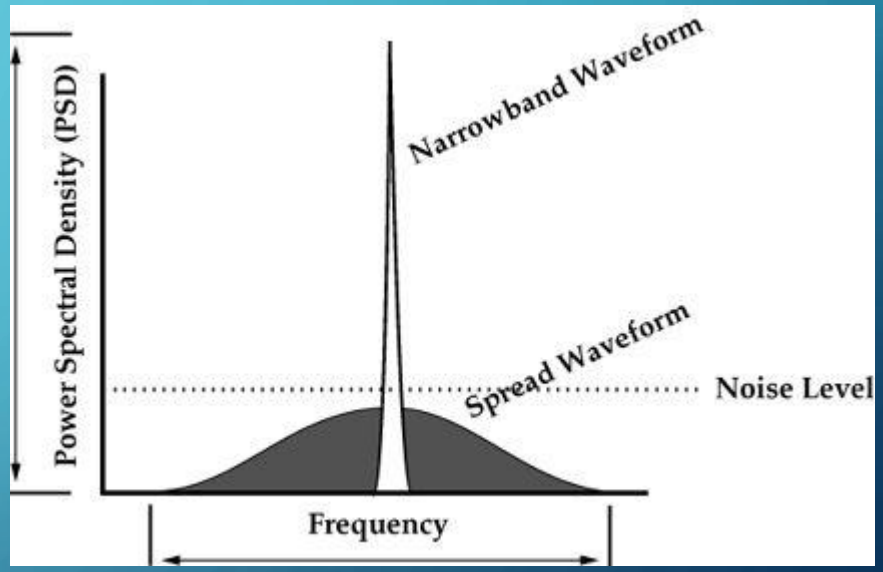
  Disadvantages:
  - Bandwidth inefficient
  - Implementation is somewhat more complex.



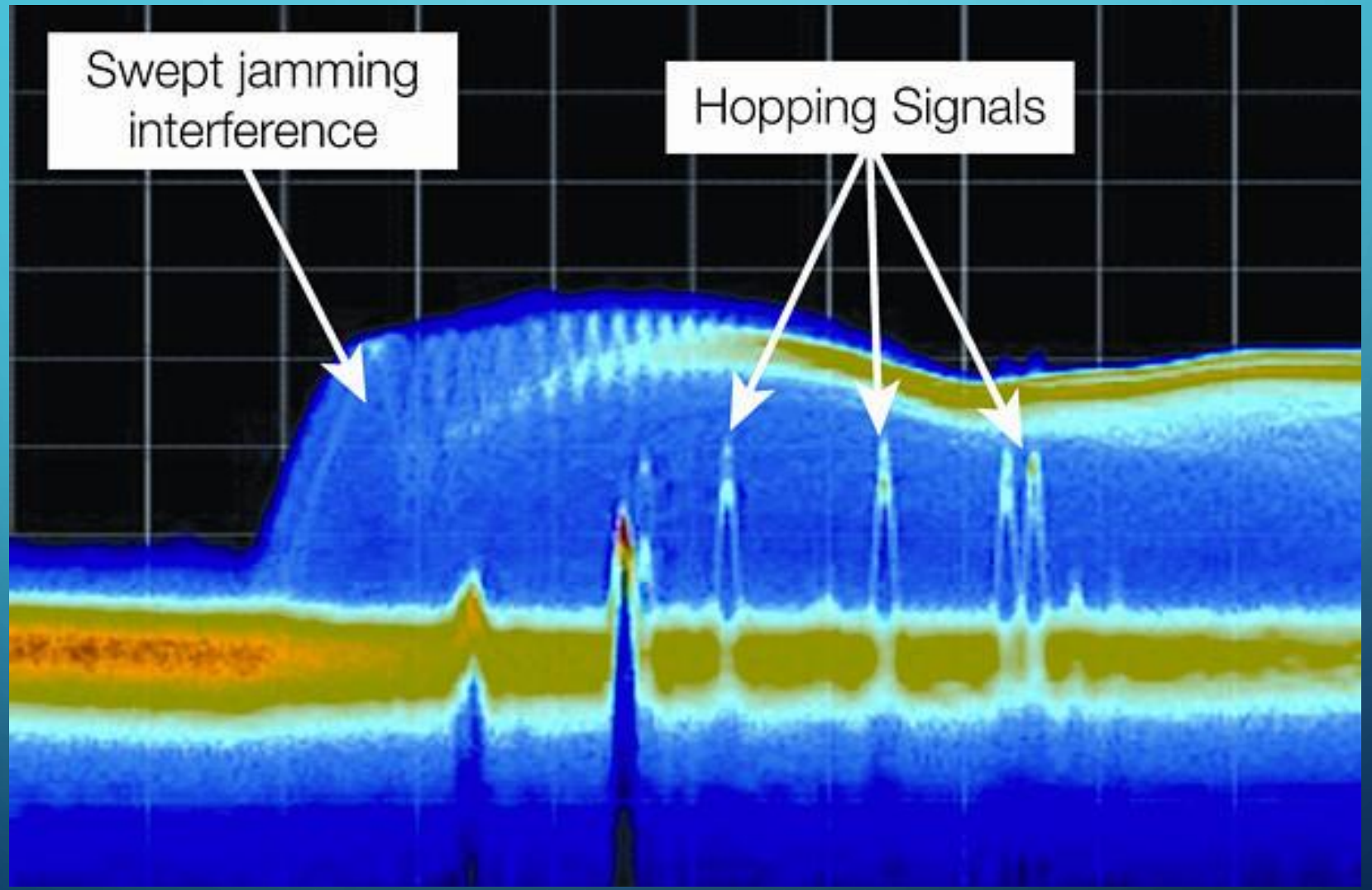


WHY DOES SPREAD SPECTRUM WORK?

- Two types of Spread Spectrum (Frequency Hopping (FHSS) and Direct Sequence (DSSS)
- Extreme amounts of power required to jam wide bandwidth
- Very narrow bandpass filters lower the noise floor allowing desired signal to rise above the floor (FHSS)
- Information is distributed across wide bandwidth signal (DSSS)



ATTEMPTED JAMMING OF FHSS SIGNAL



INDUSTRIAL, SCIENTIFIC, & MEDICAL (ISM) BAND

ITU frequency allocations[2]

Frequency range		Center frequency	Bandwidth	Type	Availability	Licensed users
6.765 MHz	6.795 MHz	6.78 MHz	30 kHz	**A**	Subject to local acceptance	FIXED SERVICE & Mobile service
13.553 MHz	13.567 MHz	13.56 MHz	14 kHz	**B**	Worldwide	FIXED & Mobile services except Aeronautical mobile (R) service
26.957 MHz	27.283 MHz	27.12 MHz	326 kHz	**B**	Worldwide	FIXED & MOBILE SERVICE except Aeronautical mobile service, CB Radio
40.66 MHz	40.7 MHz	40.68 MHz	40 kHz	**B**	Worldwide	Fixed, Mobile services & Earth exploration-satellite service
433.05 MHz	434.79 MHz	433.92 MHz	1.74 MHz	**A**	only in Region 1, subject to local acceptance	AMATEUR SERVICE & RADIOLOCATION SERVICE, additional apply the provisions of footnote 5.280. For Australia see footnote AU.
902 MHz	928 MHz	915 MHz	26 MHz	**B**	Region 2 only (with some exceptions)	FIXED, Mobile except aeronautical mobile & Radiolocation service; in Region 2 additional Amateur service
2.4 GHz	2.5 GHz	2.45 GHz	100 MHz	**B**	Worldwide	FIXED, MOBILE, RADIOLOCATION, Amateur & Amateur-satellite service
5.725 GHz	5.875 GHz	5.8 GHz	150 MHz	**B**	Worldwide	FIXED-SATELLITE, RADIOLOCATION, MOBILE, Amateur & Amateur-satellite service
24 GHz	24.25 GHz	24.125 GHz	250 MHz	**B**	Worldwide	AMATEUR, AMATEUR-SATELLITE, RADIOLOCATION & Earth exploration-satellite service (active)
61 GHz	61.5 GHz	61.25 GHz	500 MHz	**A**	Subject to local acceptance	FIXED, INTER-SATELLITE, MOBILE & RADIOLOCATION SERVICE
122 GHz	123 GHz	122.5 GHz	1 GHz	**A**	Subject to local acceptance	EARTH EXPLORATION-SATELLITE (passive), FIXED, INTER-SATELLITE, MOBILE, SPACE RESEARCH (passive) & Amateur service
244 GHz	246 GHz	245 GHz	2 GHz	**A**	Subject to local acceptance	RADIOLOCATION, RADIO ASTRONOMY, Amateur & Amateur-satellite service

Type A (footnote 5.138) = frequency bands are designated for *ISM applications*. The use of these frequency bands for ISM applications shall be subject to special authorization by the administration concerned, in agreement with other administrations whose radiocommunication services might be affected. In applying this provision, administrations shall have due regard to the latest relevant ITU-R Recommendations.

Type B (footnote 5.150) = frequency bands are also designated for ISM applications. Radiocommunication services operating within these bands must accept harmful interference which may be caused by these applications.

ITU RR, (Footnote 5.280) = In Germany, Austria, Bosnia and Herzegovina, Croatia, Macedonia, Liechtenstein, Montenegro, Portugal, Serbia, Slovenia and Switzerland, the band 433.05-434.79 MHz (center frequency 433.92 MHz) is designated for *ISM applications*. Radio communication services of these countries operating within this band must accept harmful interference which may be caused by these applications.

Footnote AU = Australia is part of ITU Region 3. The band 433.05 to 434.79 MHz is not a designated ISM band in Australia, however the operation of low powered devices in the radio frequency band 433.05 to 434.79 MHz is supported through Radio communications class licence for low interference potential devices (LIPDs).[3]

From Wikipedia

ISM BAND INTERFERENCE - REAL WORLD EXAMPLES (JAMMING)

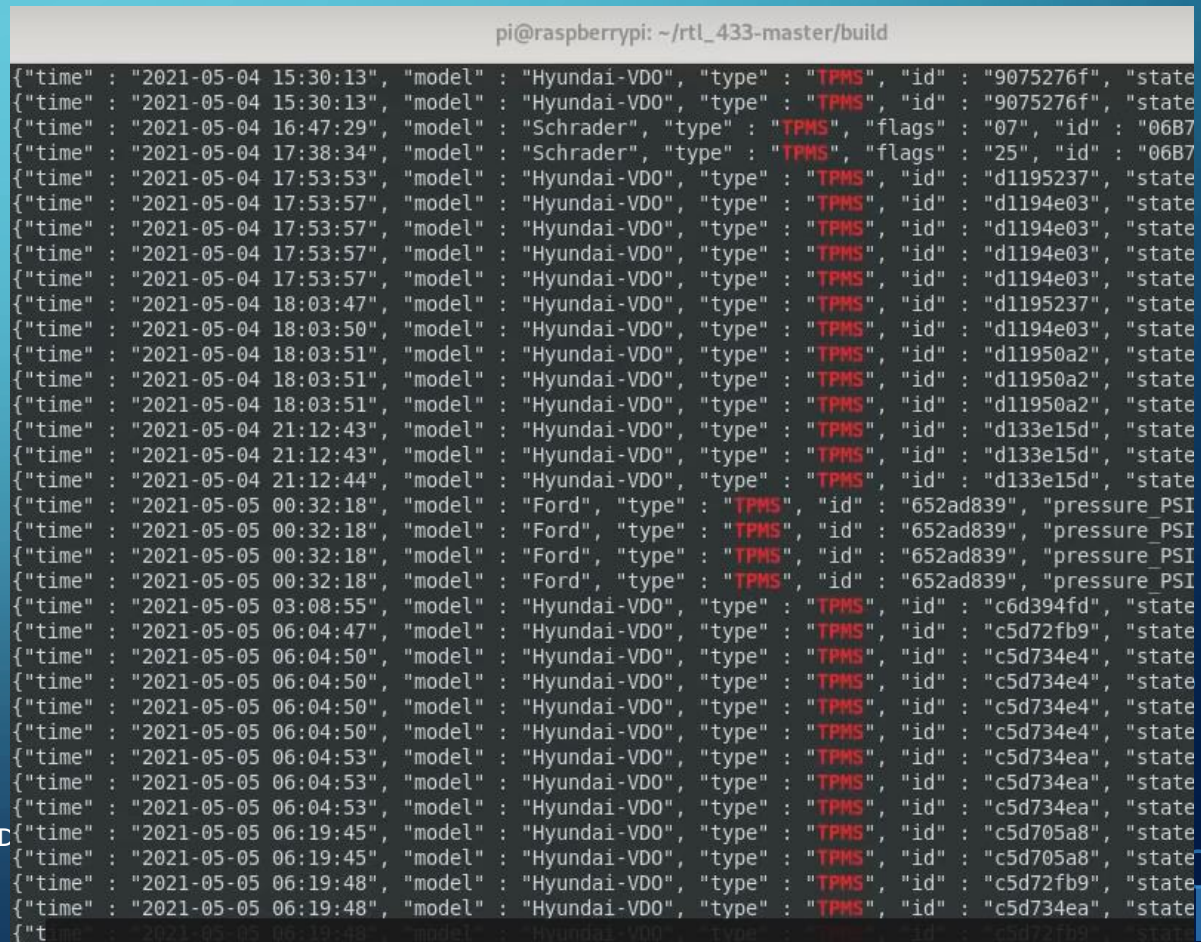
- 70 cm band interference
  - 433 MHz ISM devices are widespread in the U.S. despite not being authorized for use in Region 1
  - Unauthorized devices used for remote control (drones, RC aircraft) and IoT (remote sensing) from small manufacturers or hobbyists
  - Spread spectrum interference would be noted as noise and unlikely to be powerful enough to cause disruption unless in very close proximity
- 33 cm band interference
  - Garage door opener,
  - 902 MHz receiver has apparent sensitivity reduction
  - Manufacturer believes that cause is interference from LED lights

RFI (JAMMING) IN THE HAM SHACK

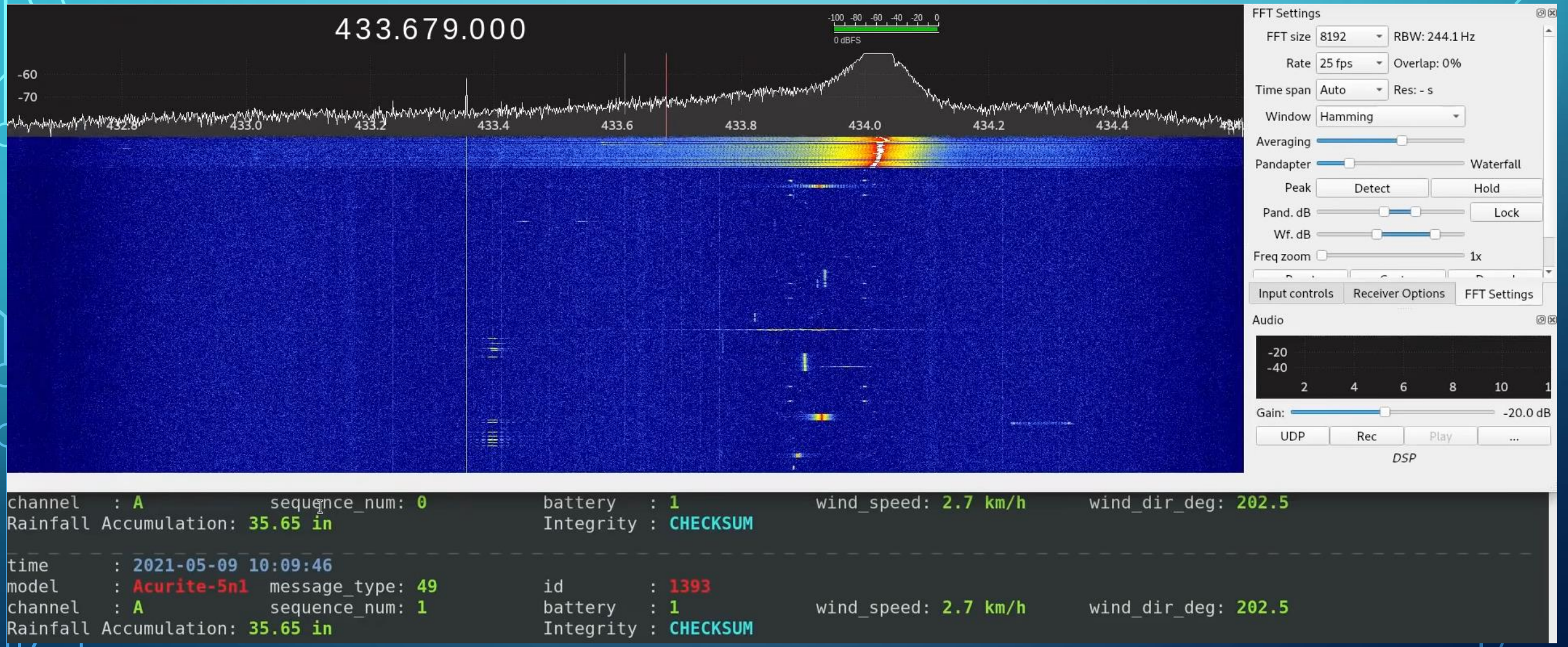
- Teaser for next months' deep dive on this topic
  - Speaker: Ken Wyatt, WA6TTY Ken is principal consultant of Wyatt Technical Services LLC, as well as past senior technical editor for *Interference Technology Magazine* (2016 to 2018)
  - Topic: Urban RFI and Ham Radio

RTL_433 ISM DECODER

- rtl_433 is a generic data receiver for the 433.92 MHz, 868 MHz (SRD), 315 MHz, 345 MHz, and 915 MHz ISM bands.
- Used with SDR (dongle, SDR Play, etc.)
- https://youtu.be/JdzVIjKA68o
- https://youtu.be/Ms5r9o8P6N4
- https://youtu.be/z1y6j8-V7J0
- Software recognizes protocol of many devices



RTL_433




```
channel   : A          sequence_num: 0          battery   : 1          wind_speed: 2.7 km/h     wind_dir_deg: 202.5
Rainfall Accumulation: 35.65 in                 Integrity : CHECKSUM

time      : 2021-05-09 10:09:46
model     : Acurite-5n1  message_type: 49        id        : 1393
channel   : A          sequence_num: 1          battery   : 1          wind_speed: 2.7 km/h     wind_dir_deg: 202.5
Rainfall Accumulation: 35.65 in                 Integrity : CHECKSUM
```