RF Pentesting Your Air Stinks

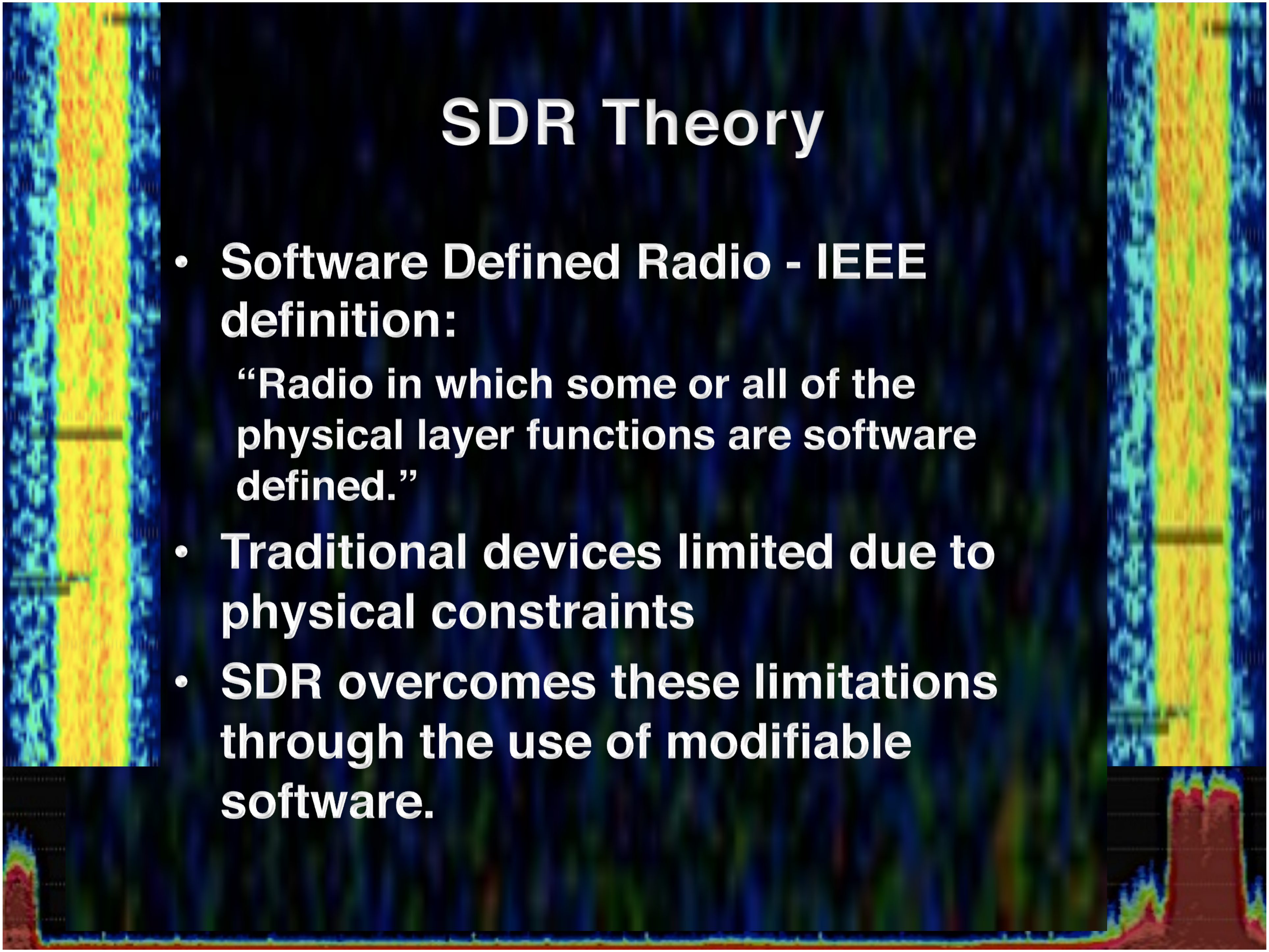
@rmellendick
@DaKahuna2007
@wctf_us
@WiFi_Village

RF Hacking

- Use of RF or “Wireless” technology has exploded
- Bring your own device

THANK YOU!!!!

- RF used to require special and expensive equipment
- Now not so much, for $30 you can see most signals of interest

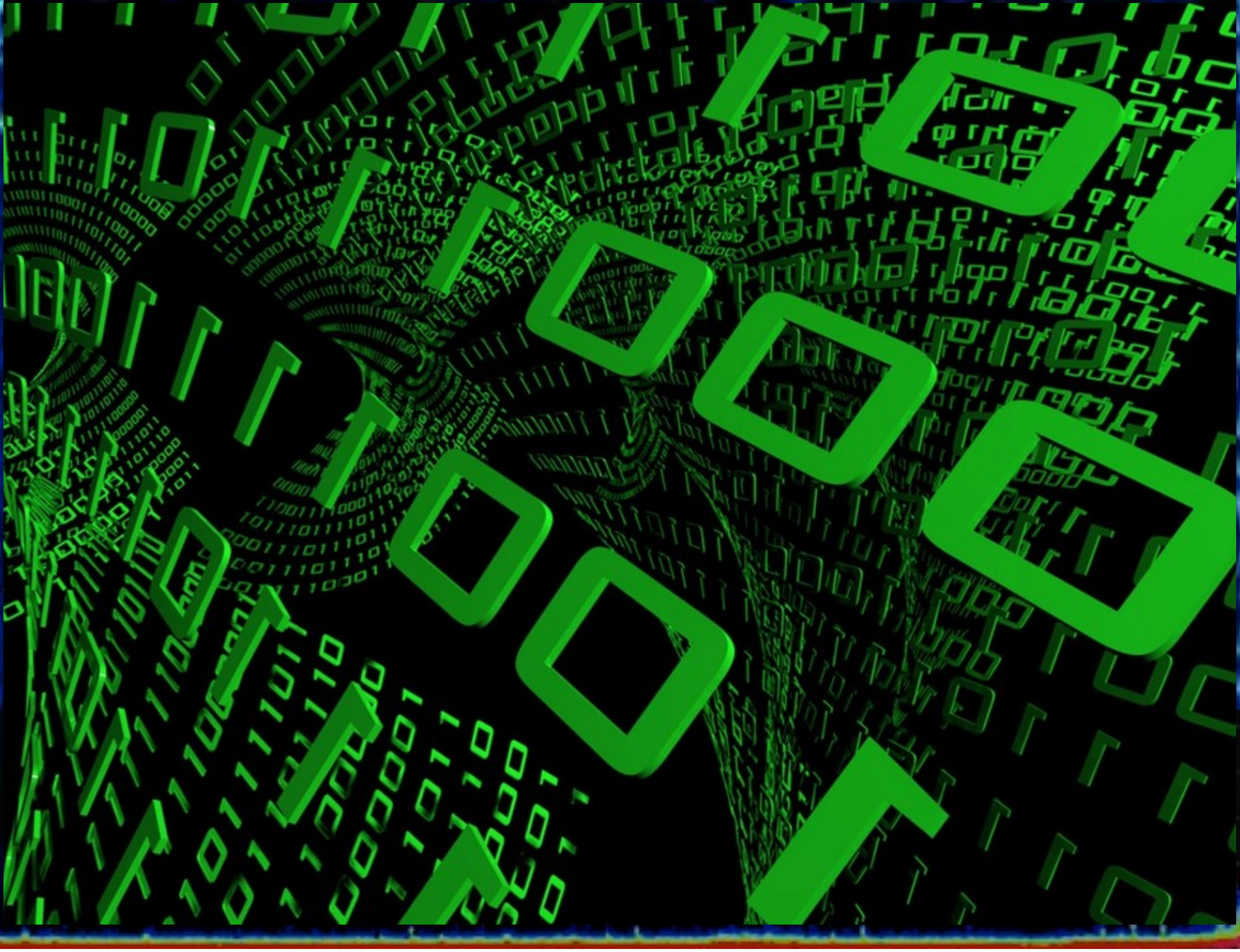


SDR Theory

- Software Defined Radio - IEEE definition:

  “Radio in which some or all of the physical layer functions are software defined.”
- Traditional devices limited due to physical constraints
- SDR overcomes these limitations through the use of modifiable software.

This is what the air looks like

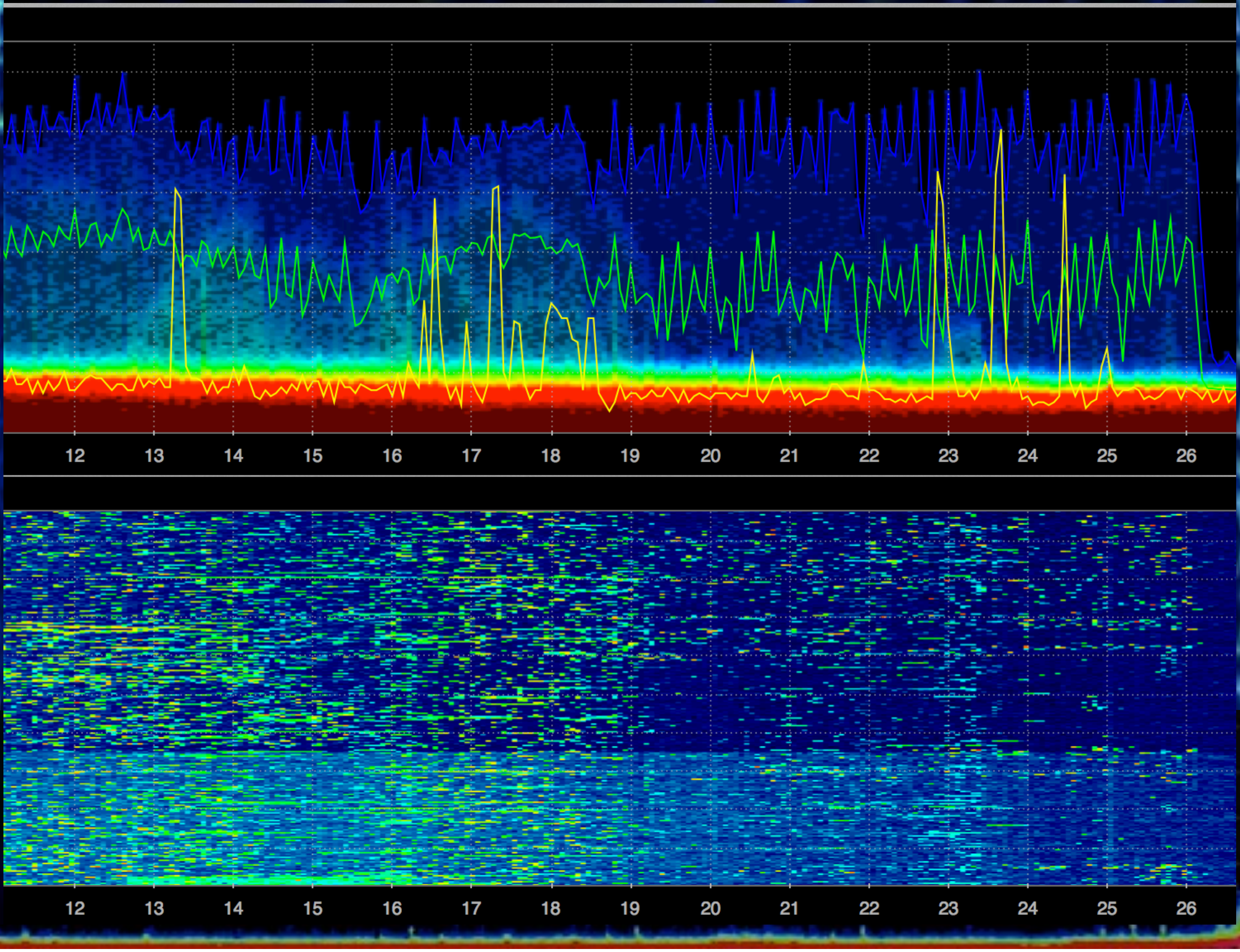


802.11 is one of many standards

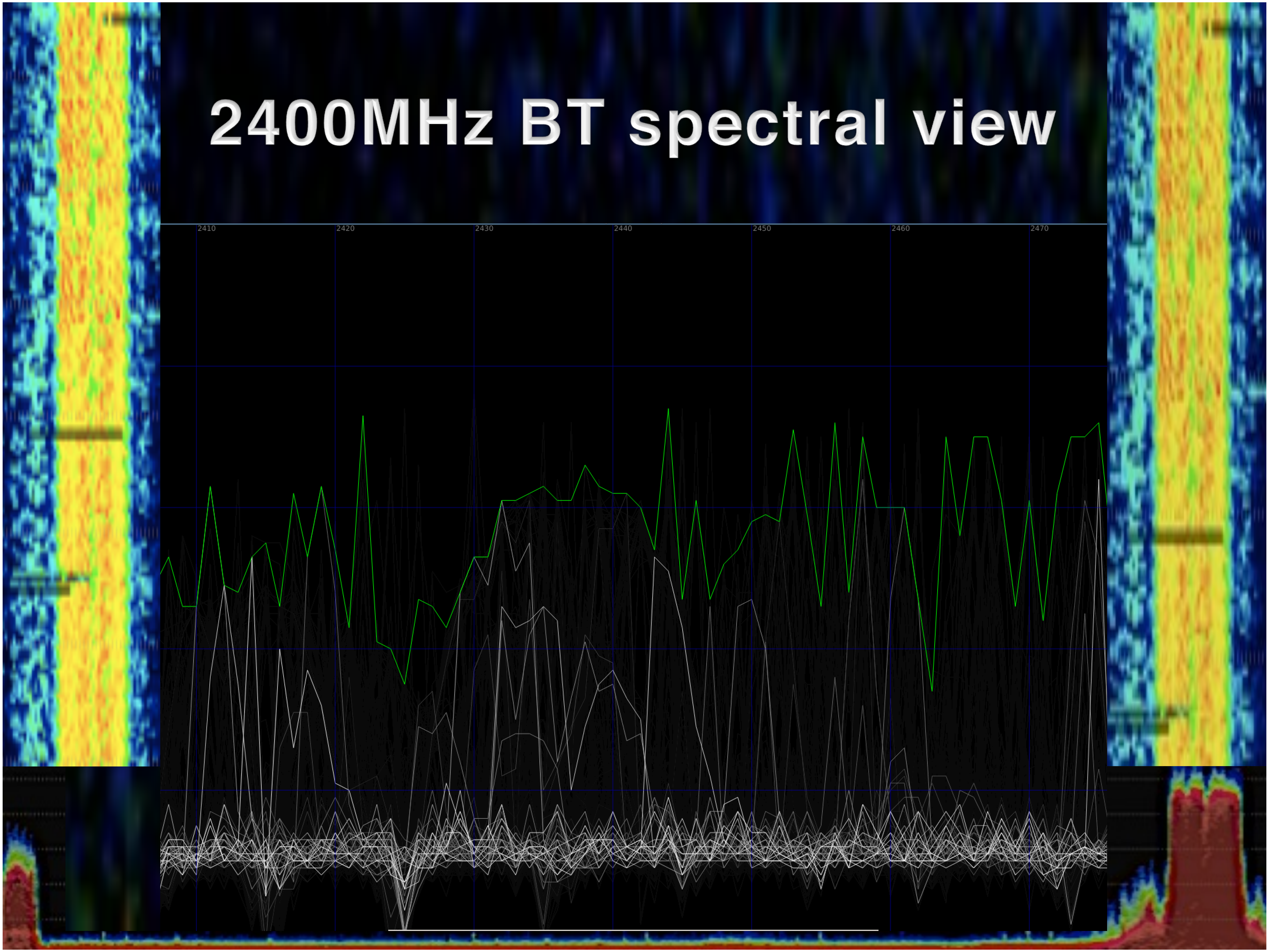
- IEEE 802.18, the Radio Regulatory Technical Advisory Group ("RR-TAG"), is a working group of IEEE 802, the LAN/MAN Standards Committee (LMCS).

- Other Valid Standards:
  - IEEE 802.11 (Wireless Local area network- WLAN)
  - IEEE 802.15 (Wireless Personal area network - WPAN)
  - IEEE 802.16 (Wireless Metropolitan area network - WMAN)
  - IEEE 802.20 (Wireless Mobility)
  - IEEE 802.21 (Hand-off/Interoperability Between Networks)
  - IEEE 802.22 (Wireless Regional Area Network – WRAN)

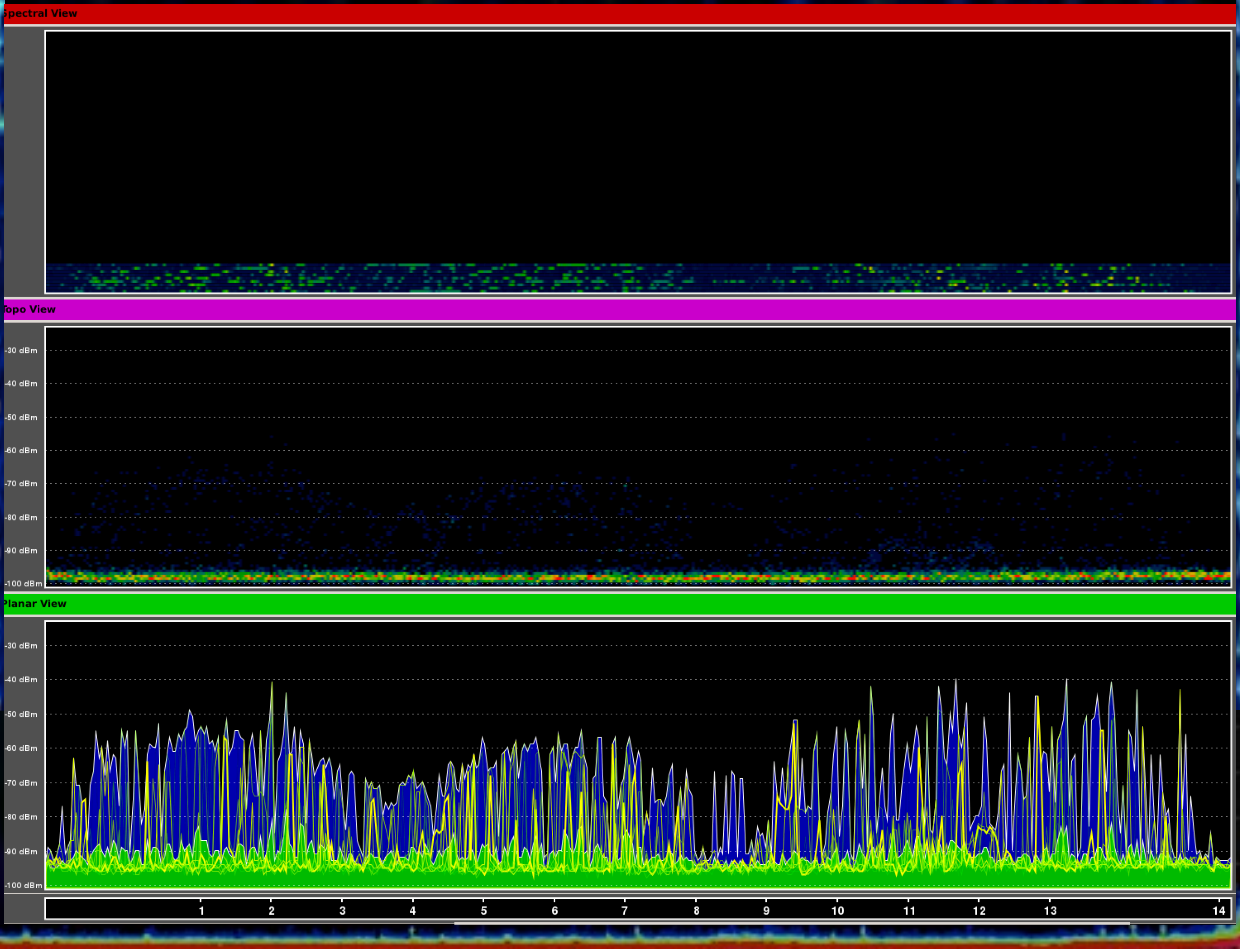
Zigbee Ch. 11-26



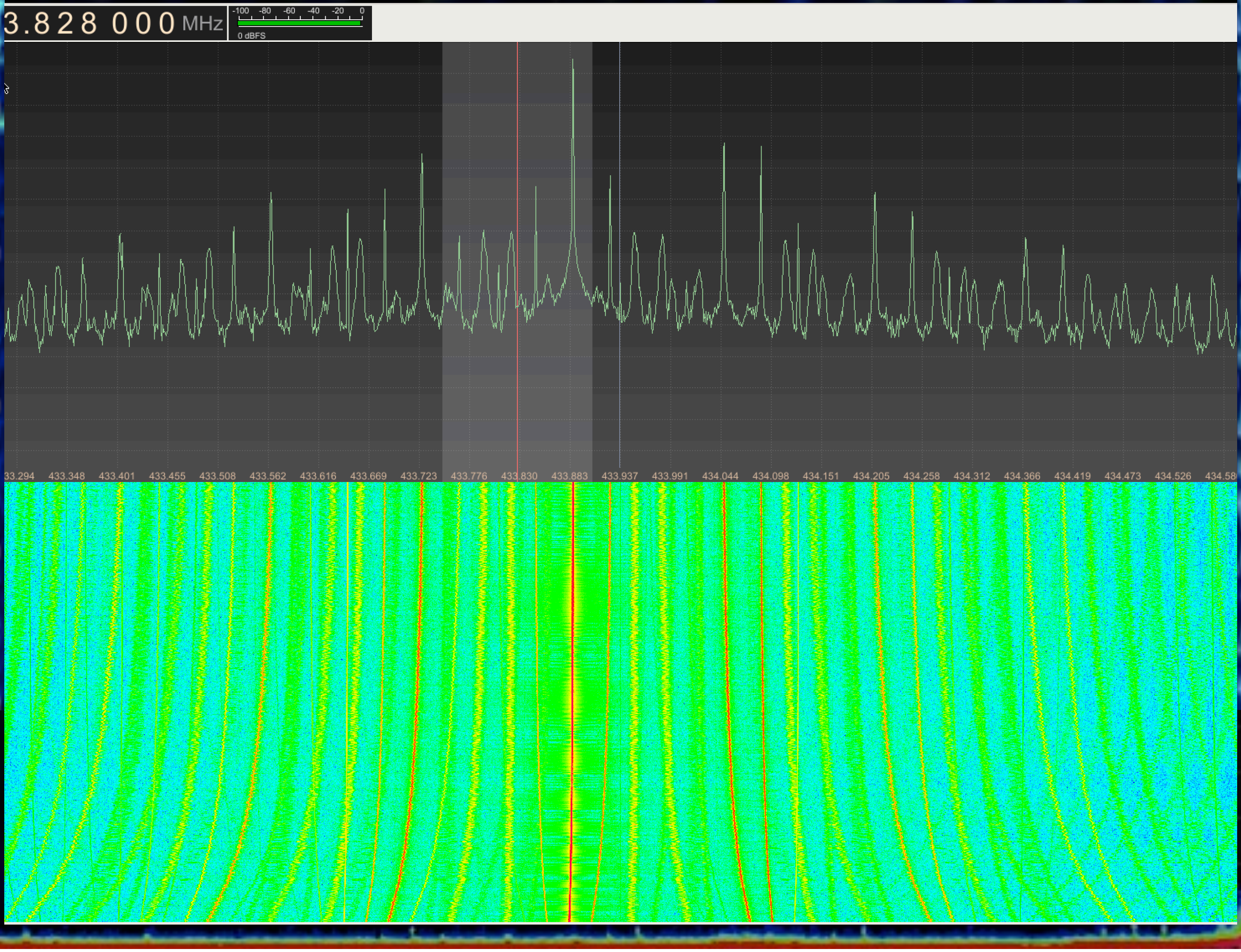
2400MHz BT spectral view



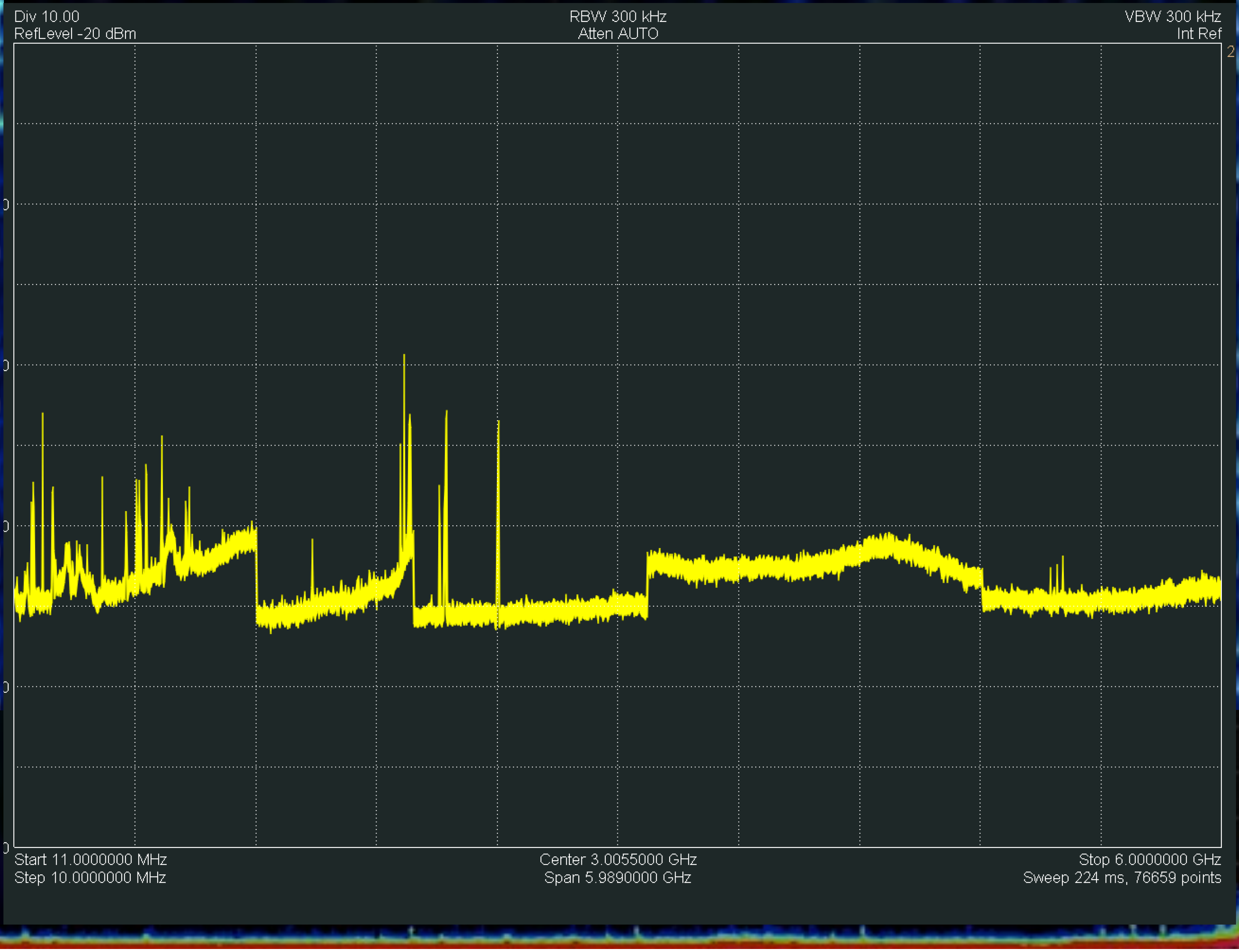
2400MHz Frequency chart



433MHz bug (active)



10MHz-6GHz



Div 10.00
RefLevel -20 dBm

RBW 300 kHz
Atten AUTO

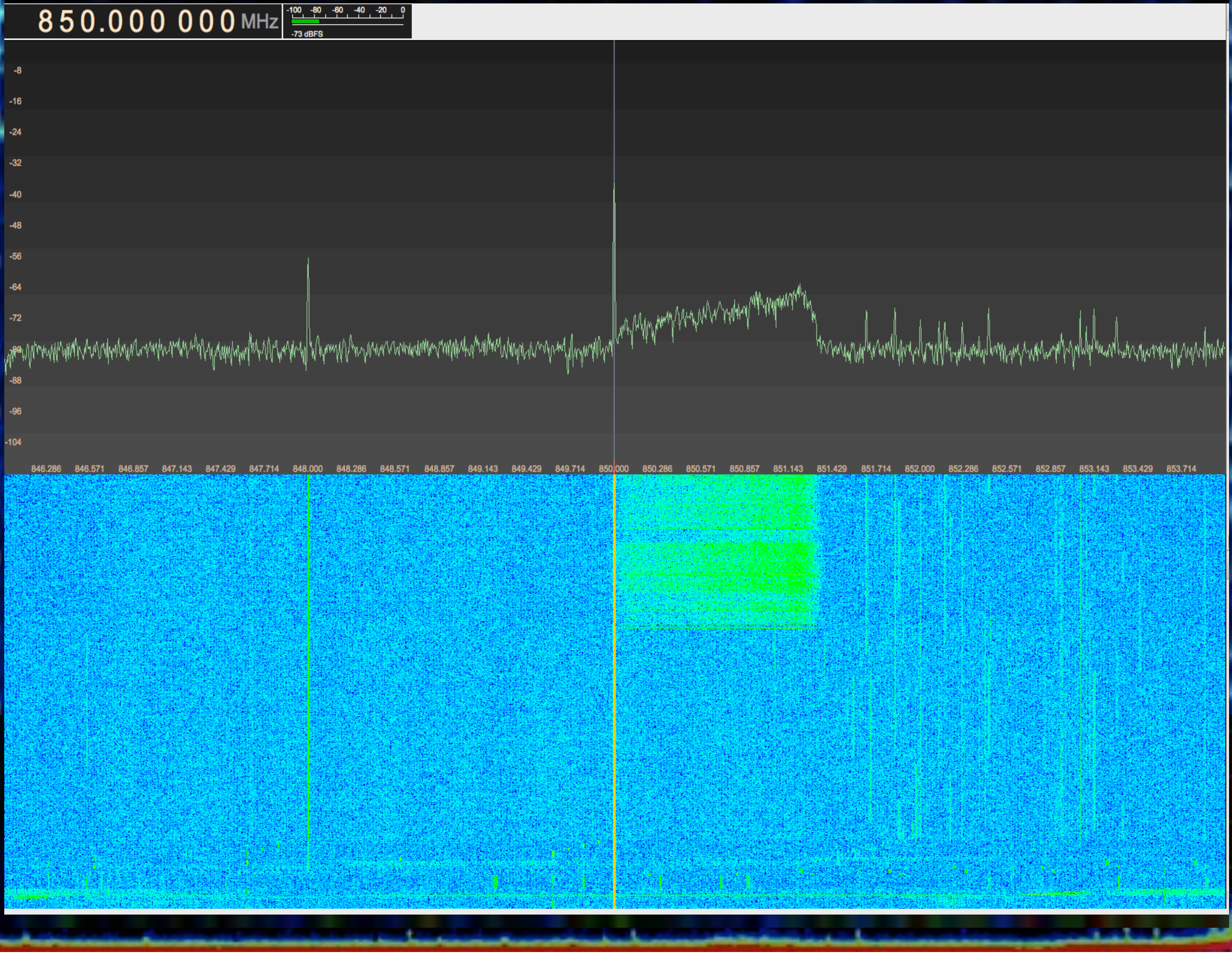
VBW 300 kHz
Int Ref

Start 11.0000000 MHz
Step 10.0000000 MHz

Center 3.0055000 GHz
Span 5.9890000 GHz

Stop 6.0000000 GHz
Sweep 224 ms, 76659 points

Cell Phone Signal



Recon

- Map and identify active devices on the network within the ranges identified
- Leverage the results of the network discovery then do a deep dive scan on the active devices for vulnerabilities or targeted information

Exploitation

- Exploit the vulnerabilities and confirm the network's susceptibility to attack
- Exfiltrate data over the available channels or use secondary channels to exfil
- Once you identify all of the misconfigured RF entry points bypass the network security controls to access systems and resources

YOU WIN!!!!!

Platform Selection

Internet access

- A device with USB tether

Laptop (MAC or PC)

- Multi core processor (i7)
- 16 GB ram or more
- Hard drive space for all necessary apps and VMs
- Screen with space for multiple terminals

External Radios/antennas

- Internal radios might not give the optimal capability
- Built in antennas may not give flexibility needed

Power-Supply

  – Enough outlets to power all of your gear

Operating Systems

OS X with Fusion

Windows

Pentoo

GNU Radio Live SDR

Kali

Kit Software Tools

Aircrack-NG
Kismet-NG
Airodump-NG
Wireshark
TCPDump
Nmap
PGP
inssider
Reaver

Pyrit
Wireshark
OCLHashcat
Wifite
Fern-wifi-cracker
SD Gabriel
Airdrop
gqrx
Dsd

Channelizer
multimon-ng
smartnet-scanner
GNUradio
OsmoComSDR
EyeP.A.
SpecTools

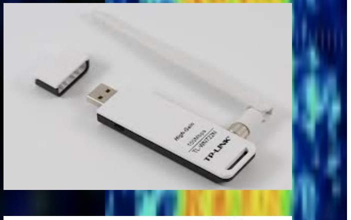
Kit Hardware Tools

- wispy DBX
- signal hound
- hackrf
- rtlsdr
- Ubertooth
- zigbee radios
- rosewill
- alfa
- sr71
- airpcapNX
- tplink nl 722

- gps puck
- bug
- rokland for N
- PWNPad
- Pineapple
- tap
- USB hub
- USB power
- headphones
- antennas
- beufang

Helpful Radios

Alfa radios (ABGN)
Rokland N3 (BGN)
Rosewill N600 UBE (ABGN)
SR-71 (ABG)
AirPcapNx (ABGN)
WiSpy DBX (2.4 and 5Ghz)
TP-Link TL-WN722N (BGN)
Ubertooth One (many uses)
HackRF One (SDR)
RTL-SDR (SDR)
Nuand BladeRF
EnGenius EUB 1200AC (ABGNAC)
SD Gabriel

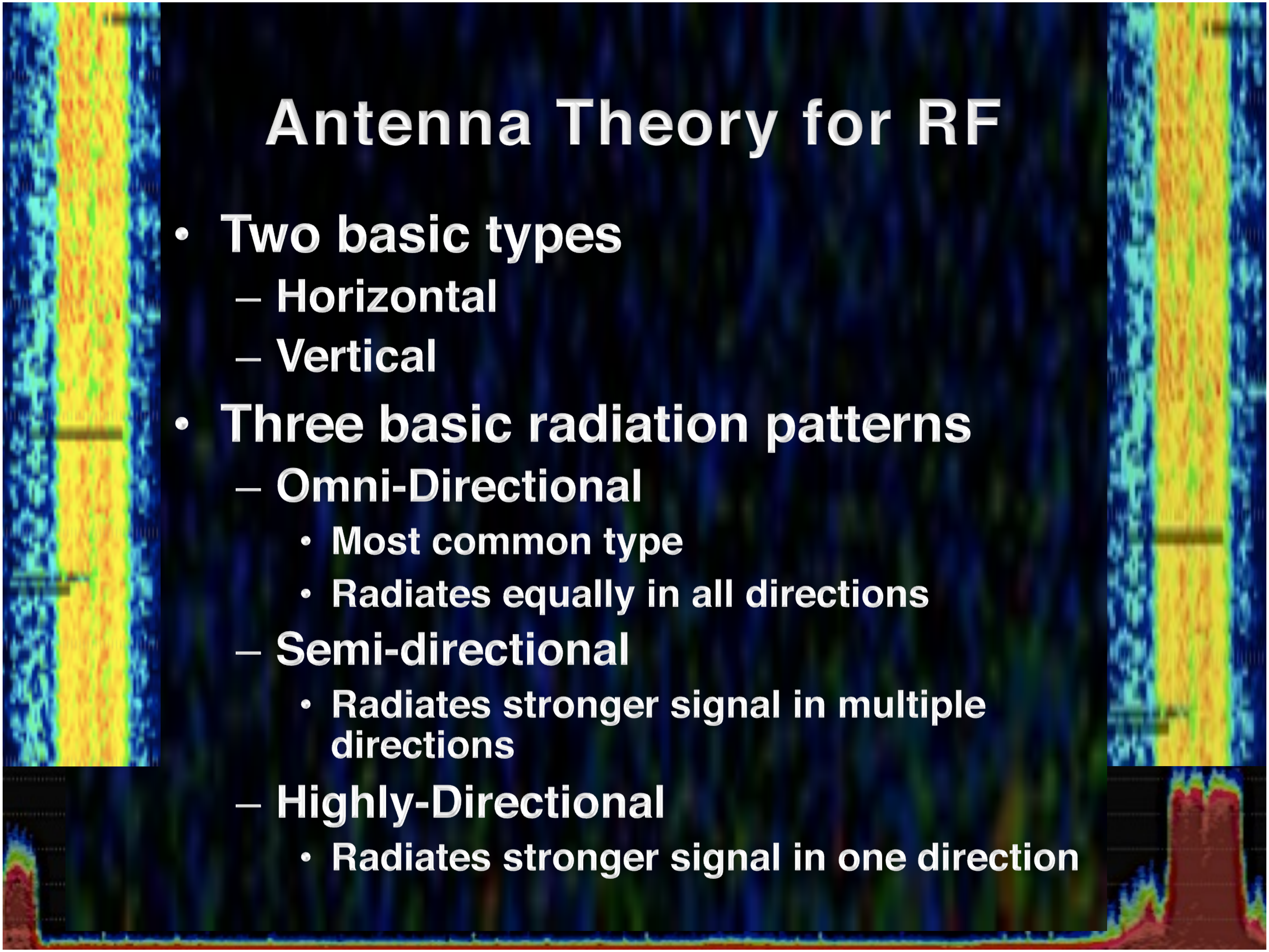


Headphones

- There are thousands of headphones
- Headphones are a very personal decision
- They range in price and quality
- Find a pair that are comfortable and clear
- Types:
  - In ear
  - Over the ear (best)
  - On the ear

Something to carry it in

- Pack
- Pelican case
- Vehicle



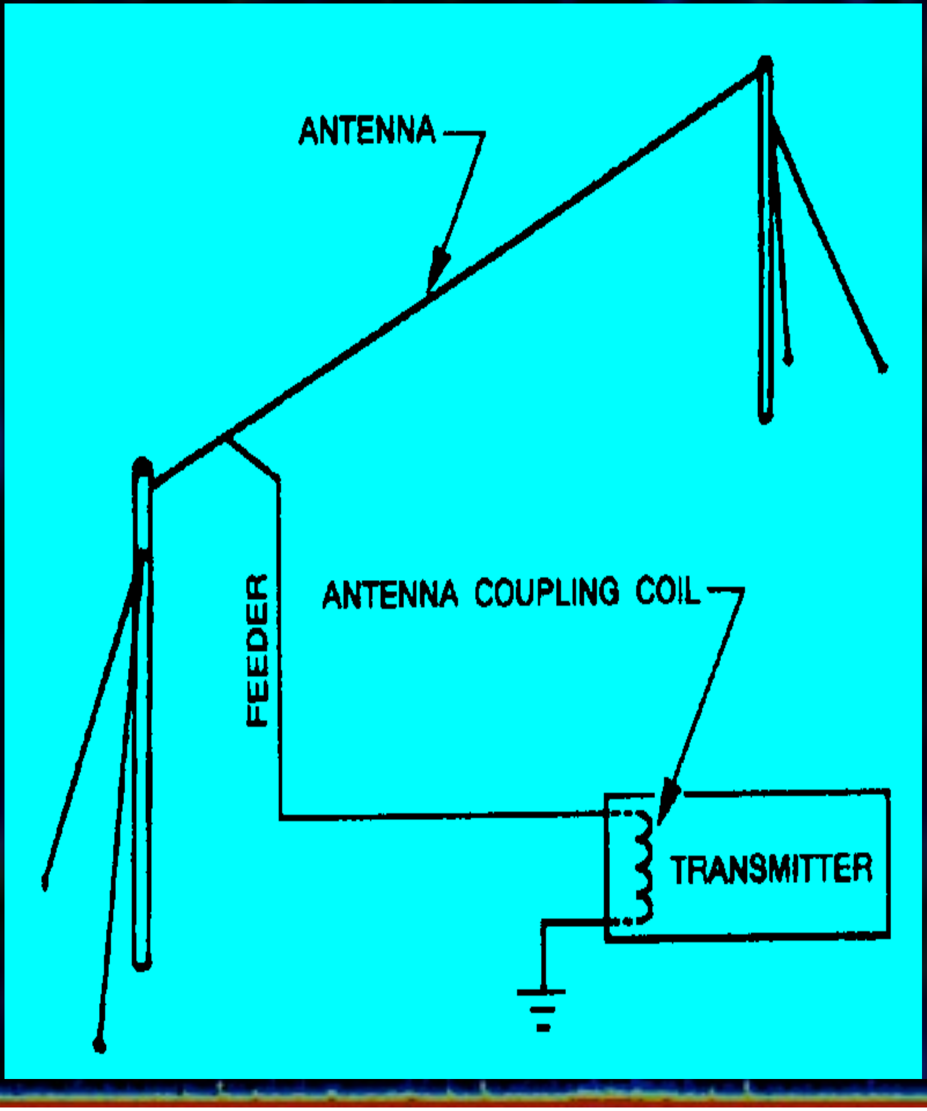
Antenna Theory for RF

- Two basic types
  - Horizontal
  - Vertical
- Three basic radiation patterns
  - Omni-Directional
    - Most common type
    - Radiates equally in all directions
  - Semi-directional
    - Radiates stronger signal in multiple directions
  - Highly-Directional
    - Radiates stronger signal in one direction

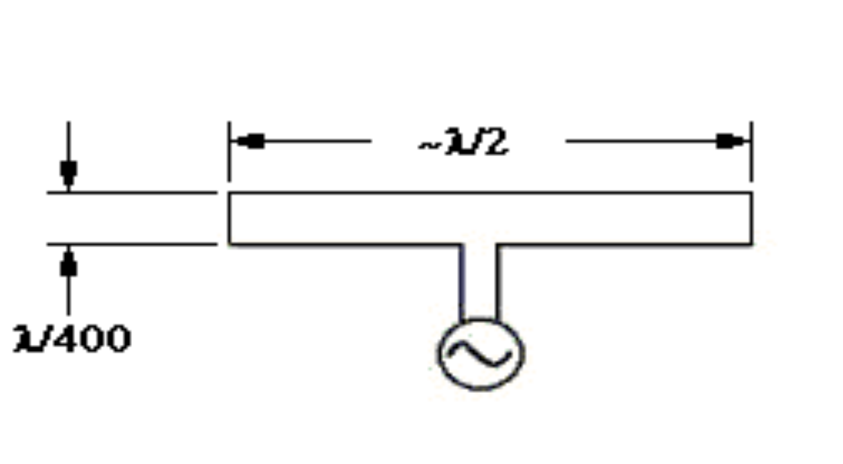
Principles of Radiation

- Electromagnetic Fields
- Importance of Design
- Antenna Parts
  - Coupling Device
  - Feeder
  - Antenna

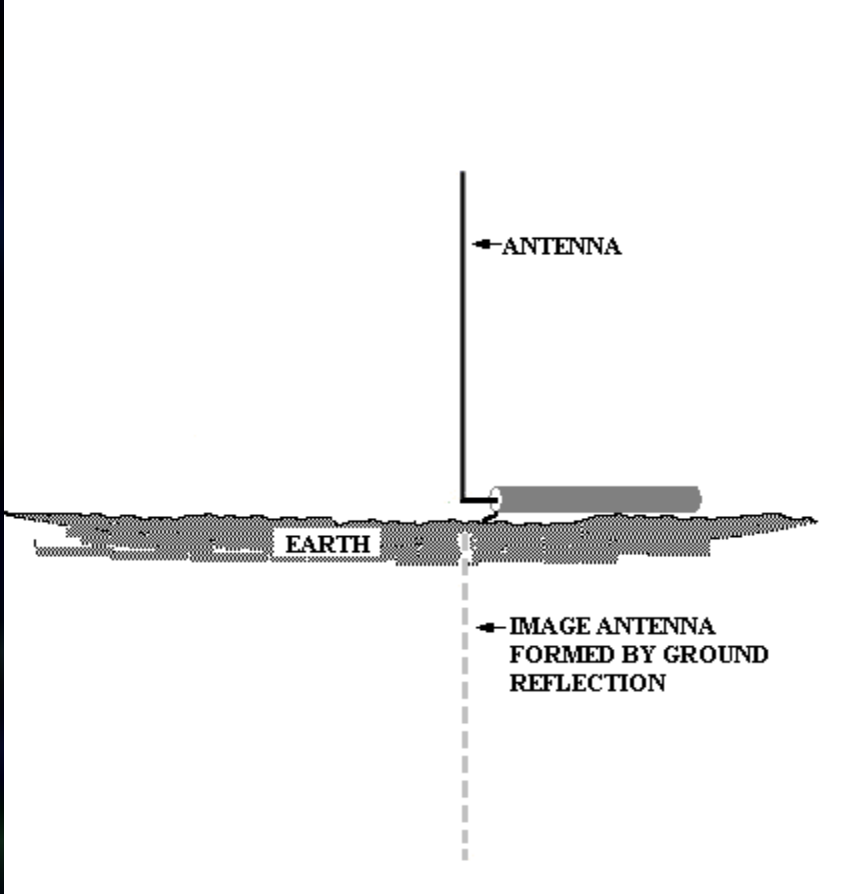
Antenna System



Basic Antenna Types



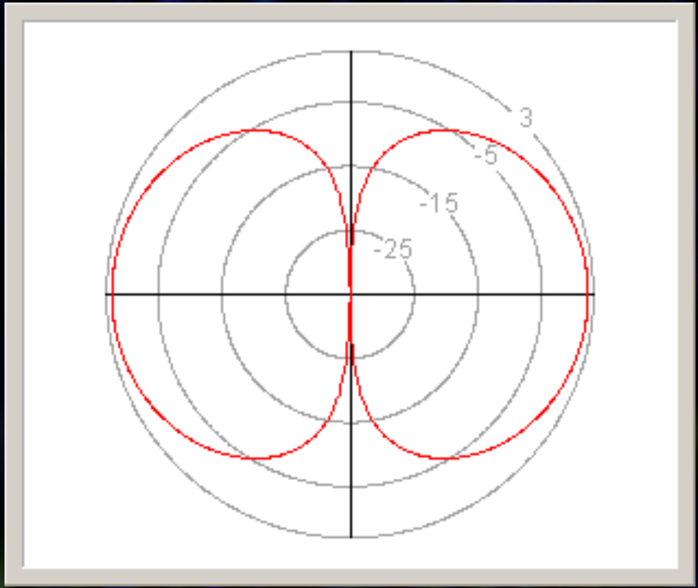
Hertz Antenna



Marconi Antenna

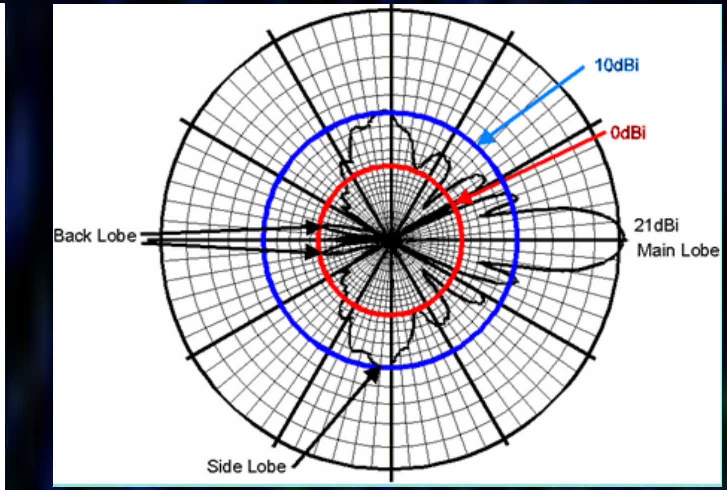
Omni Directional

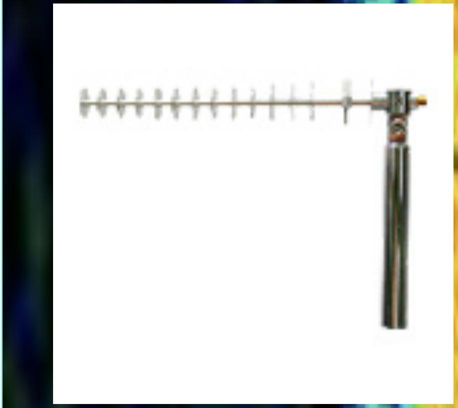
- Radiates equally In all directions



Semi-Directional

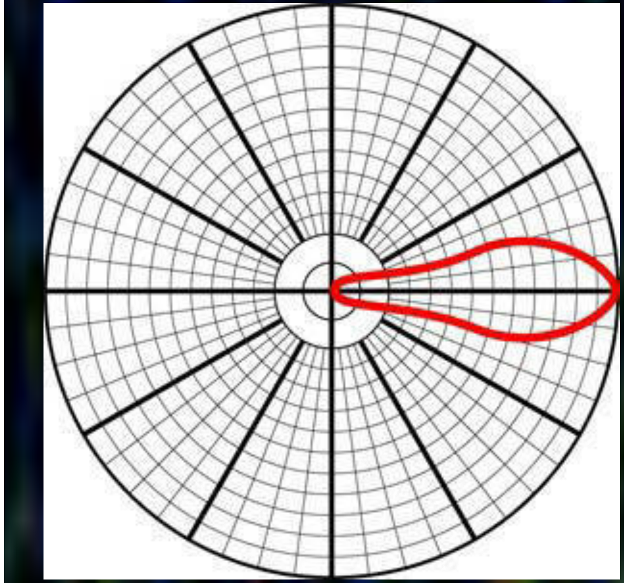
- Radiates stronger signal in multiple directions





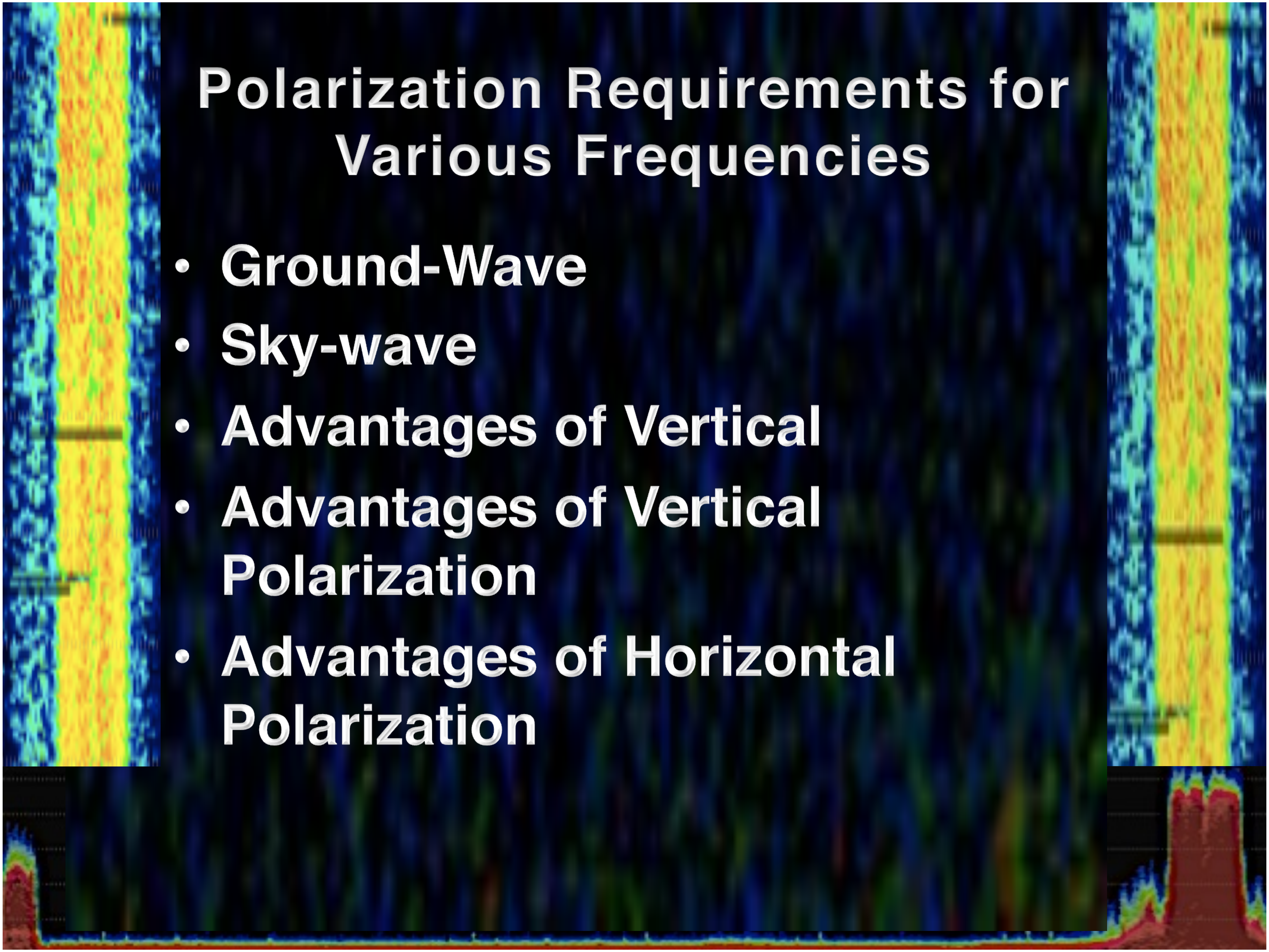
Highly Directional

- Radiates strong signal in a signal direction



Antenna Radiation Basic Principles

- Antenna Gain & Loss
  - Impact antenna has on signal amplitude
  - Gain
    - RF Amplifier
    - Directionalization
  - Loss
    - Cable loss
    - Attenuation in path
      - Physical
      - Environmental
  - Resonance



Polarization Requirements for Various Frequencies

- Ground-Wave
- Sky-wave
- Advantages of Vertical
- Advantages of Vertical Polarization
- Advantages of Horizontal Polarization

References

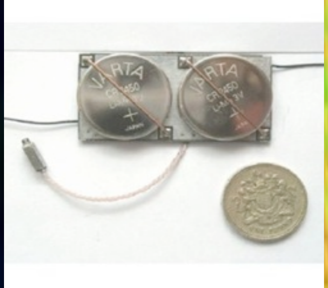
- Integrated Publishing Electrical Engineering Training Series
  http://www.tpub.com/neets/book10/42
- Electronic Communications 3rd Edition
- Radio Handbook 23rd Edition

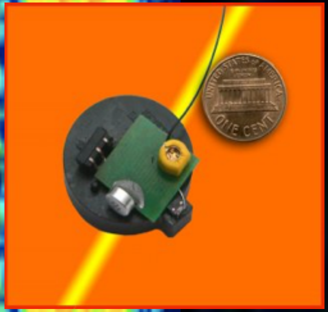
Target Selection

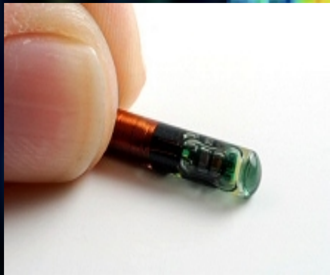
- Look for “hot spots”
- Look for beacons that are within your target set
- Determine what the limits are that you are working within

Your Targets

Transmitters to be found







RTL-SDR wiki

Awesome Reference

http://sdr.osmocom.org/trac/wiki/rtl-sdr

Why SDR is the Game Changer

The ability to write code to perform the job at hand is something that the RF industry hasn’t had in the past, now we can, thanks

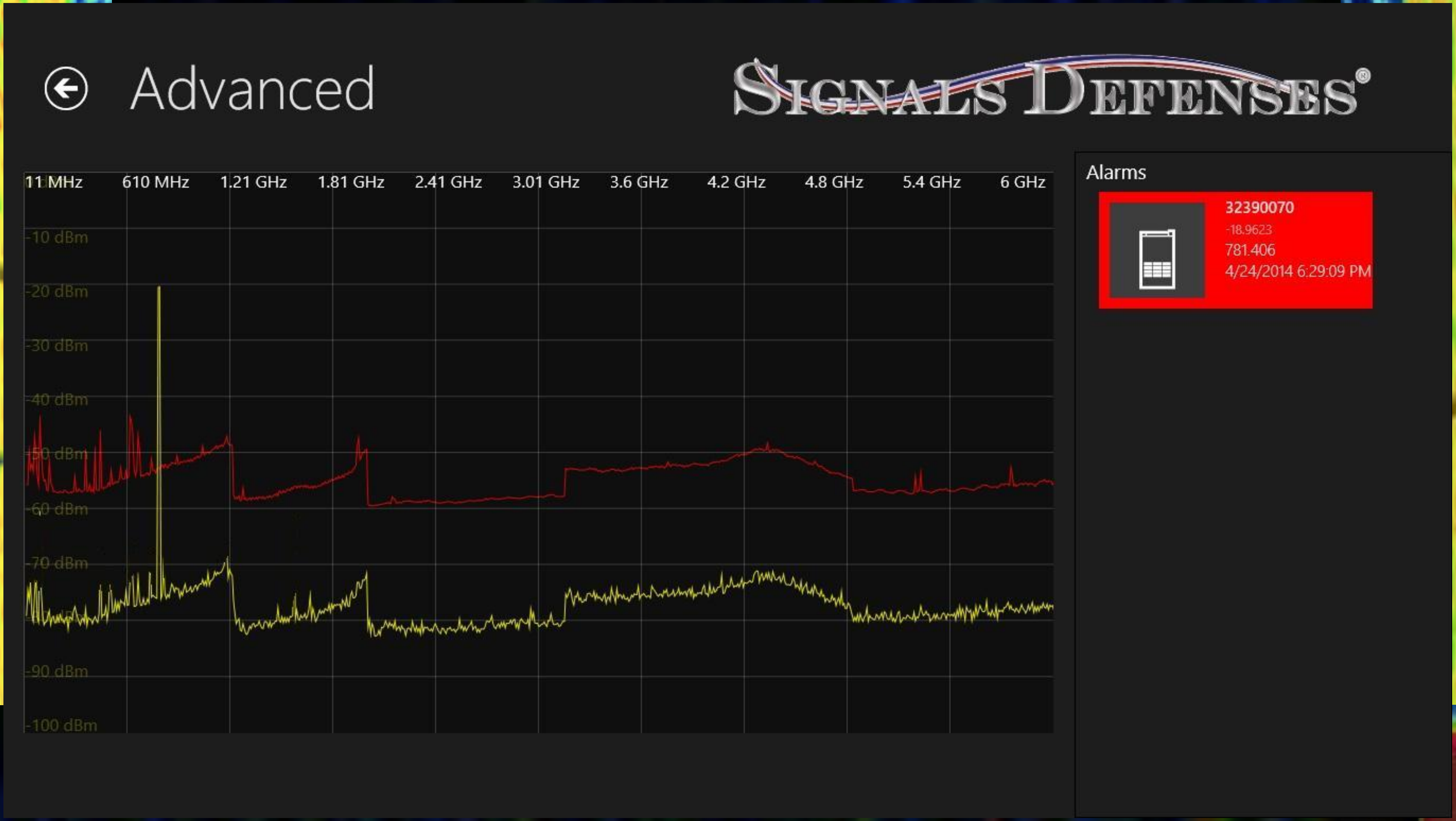
GNURadio Companion

DF the signal

Direction Finding of a signal is not easy, but is able to be done with experience and understanding of harmonics and “signal bounce” or reflection.

The WCTF will give you an opportunity to do this

RF IDS

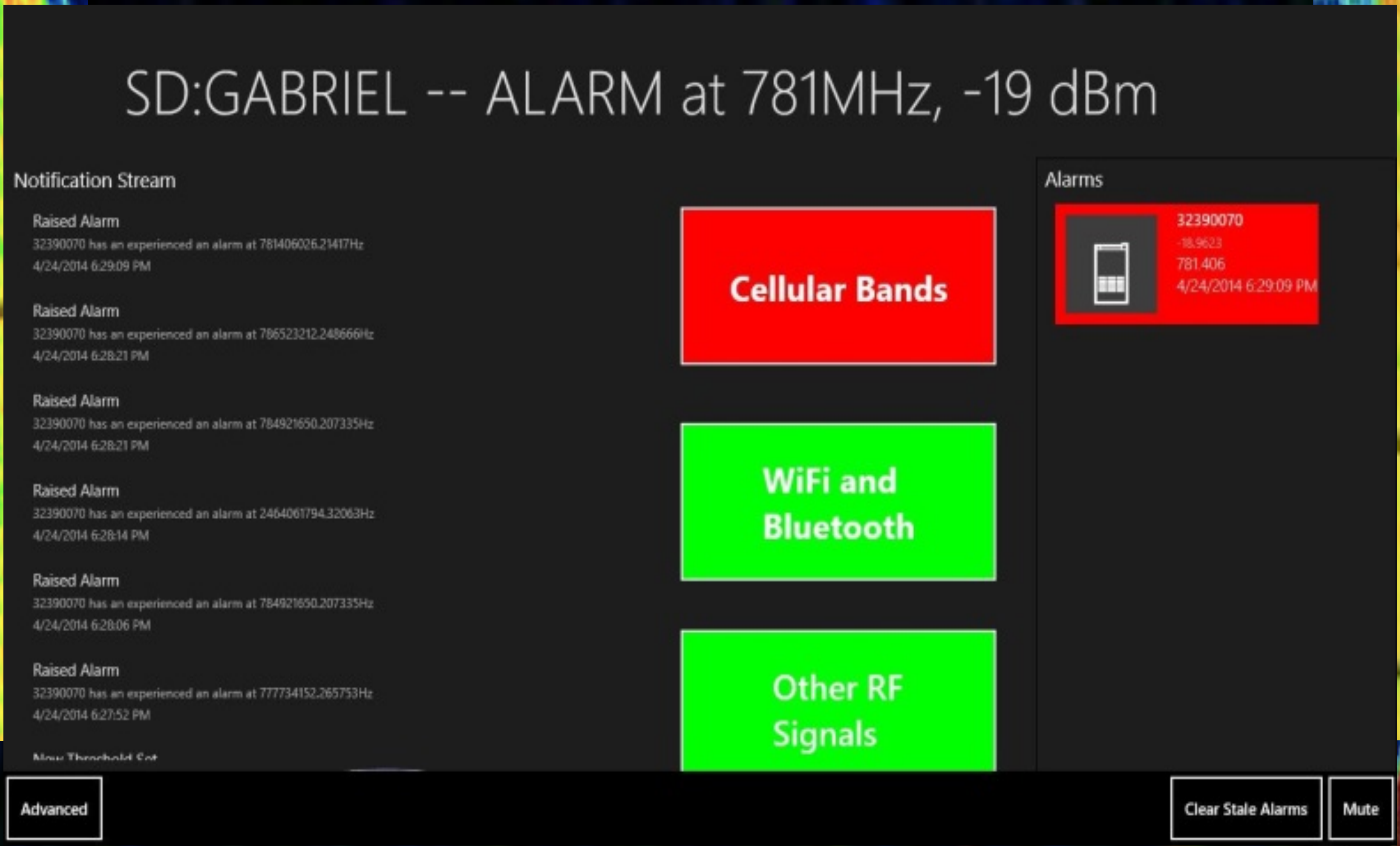


Advanced

Alarms

32390070
-18.9623
781.406
4/24/2014 6:29:09 PM

RF IDS



SD:GABRIEL -- ALARM at 781MHz, -19 dBm

Notification Stream

Raised Alarm
32390070 has an experienced an alarm at 781406026.21417Hz
4/24/2014 6:29:09 PM

Raised Alarm
32390070 has an experienced an alarm at 786523212.248666Hz
4/24/2014 6:28:21 PM

Raised Alarm
32390070 has an experienced an alarm at 784921650.207335Hz
4/24/2014 6:28:21 PM

Raised Alarm
32390070 has an experienced an alarm at 2464061794.32063Hz
4/24/2014 6:28:14 PM

Raised Alarm
32390070 has an experienced an alarm at 784921650.207335Hz
4/24/2014 6:28:06 PM

Raised Alarm
32390070 has an experienced an alarm at 777734152.265753Hz
4/24/2014 6:27:52 PM

New Threshold Set

Alarms

32390070
-18.9623
781.406
4/24/2014 6:29:09 PM

Putting It All Together

Wireless CTF

WCTF

- New changes make it more of a competition
- 50 challenges this year
- Challenges are all RF
- Come to the Wireless Village for more information

- Not giving everything away yet

☺

SPONSORS

SIGNALS DEFENSE

aruba® NETWORKS

TACTICAL NETWORK SOLUTIONS

GREAT SCOTT GADGETS

metageek

nuand

HAK5 TRUST YOUR TECHNOLUST

simpleWiFi

AirTight® NETWORKS

PentesterAcademy
a SecurityTube.net initiative

Questions

@rmellendick
@DaKahuna2007
@wctf_us
@WiFi_Village