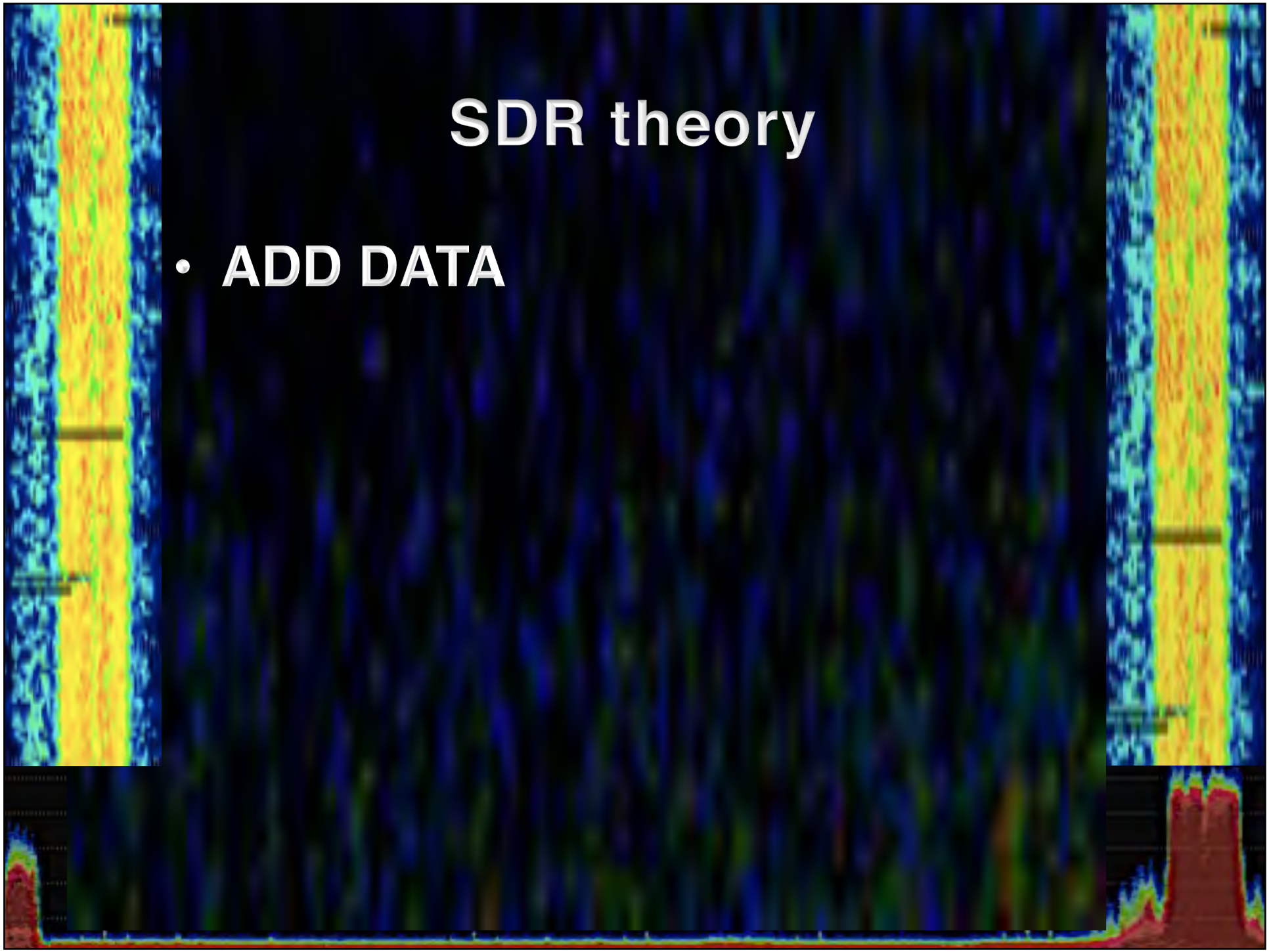

RF Pentesting Your
Air Stinks
@rmellendick
@DaKahuna2007
@wctf_us
@WiFi_Village

RF Hacking

- NEED DATA

SDR theory

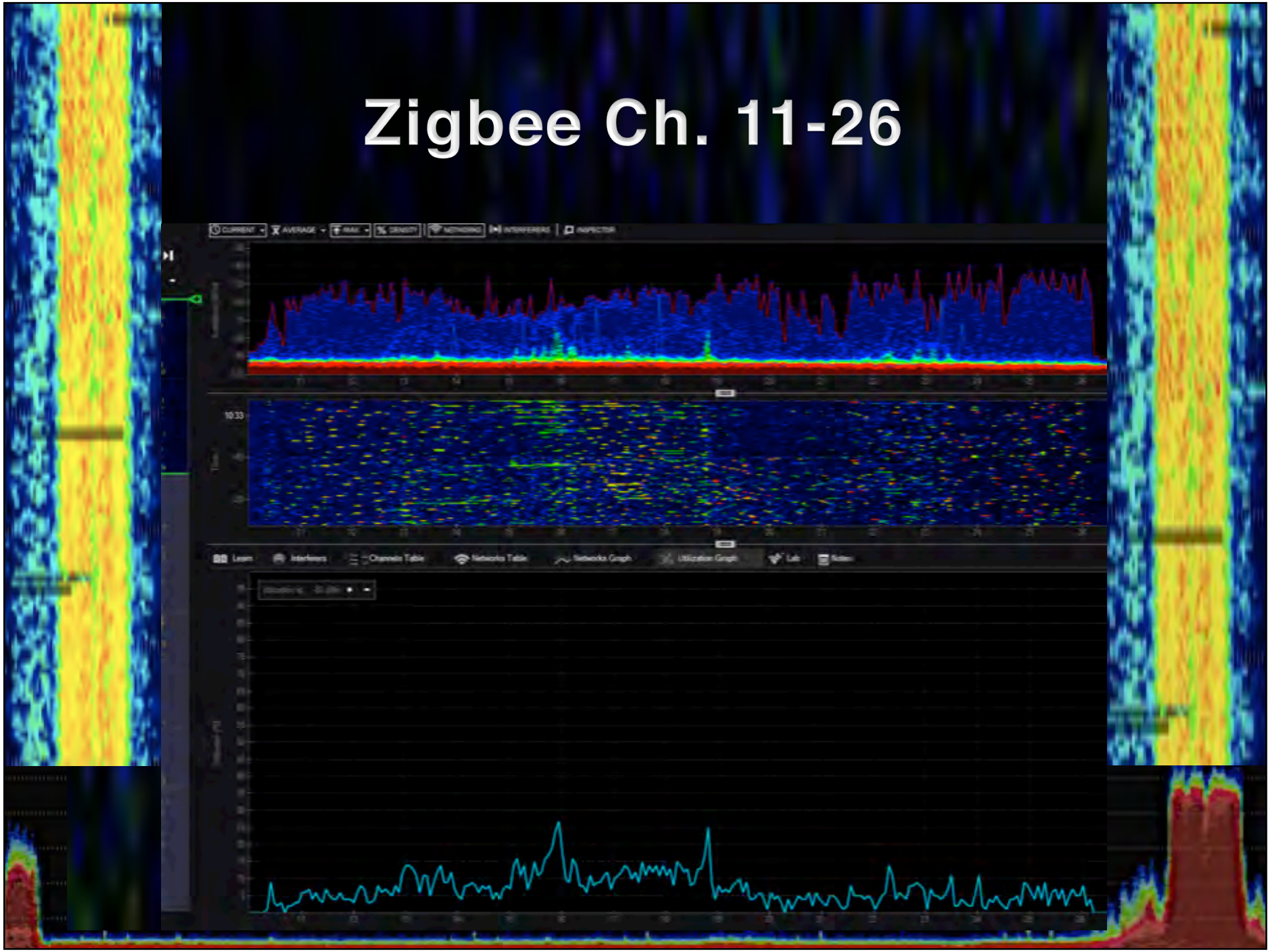
- ADD DATA



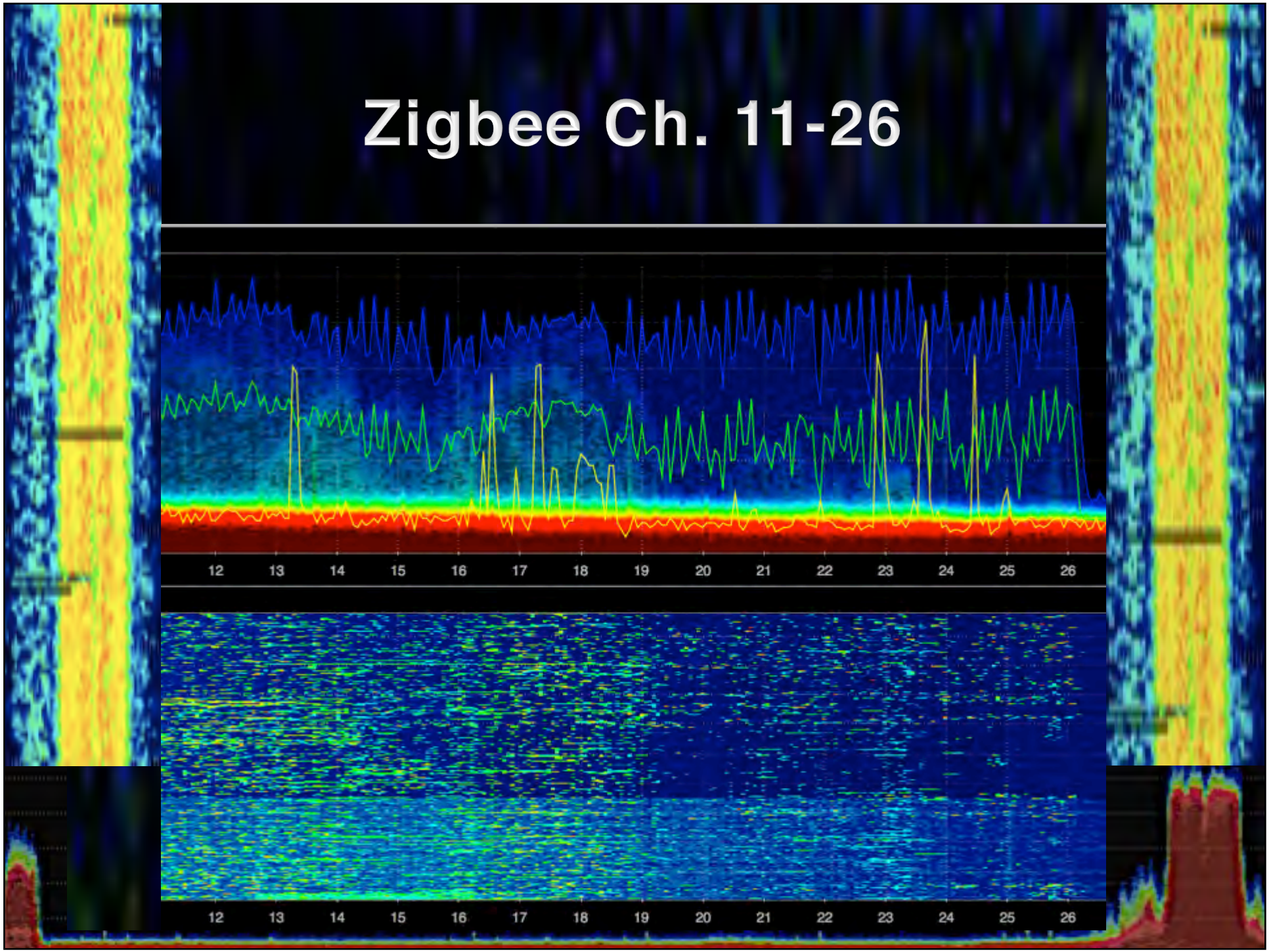
This is what the air looks like


802.11 is not the only standard
NEED DATA

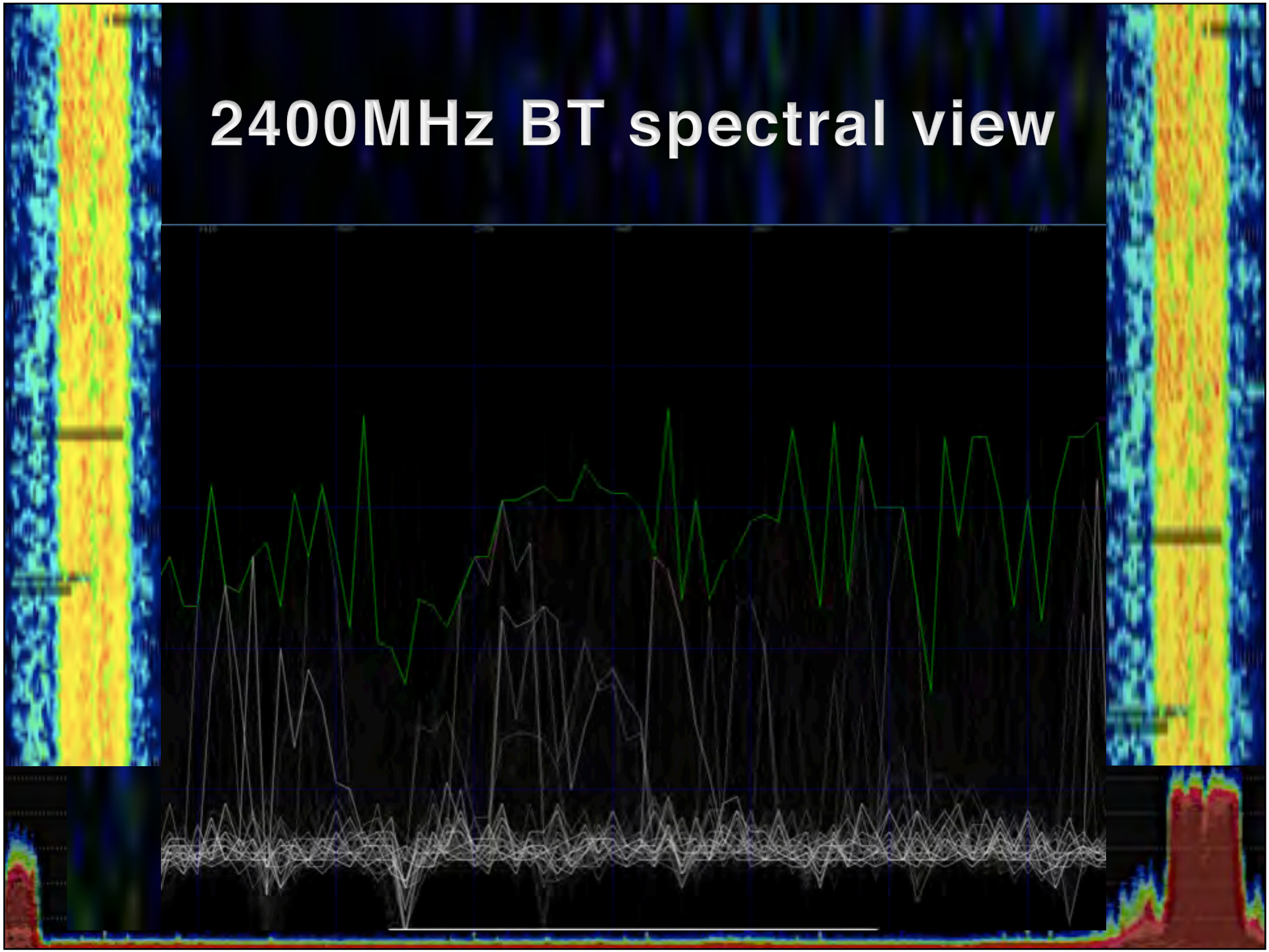
Zigbee Ch. 11-26



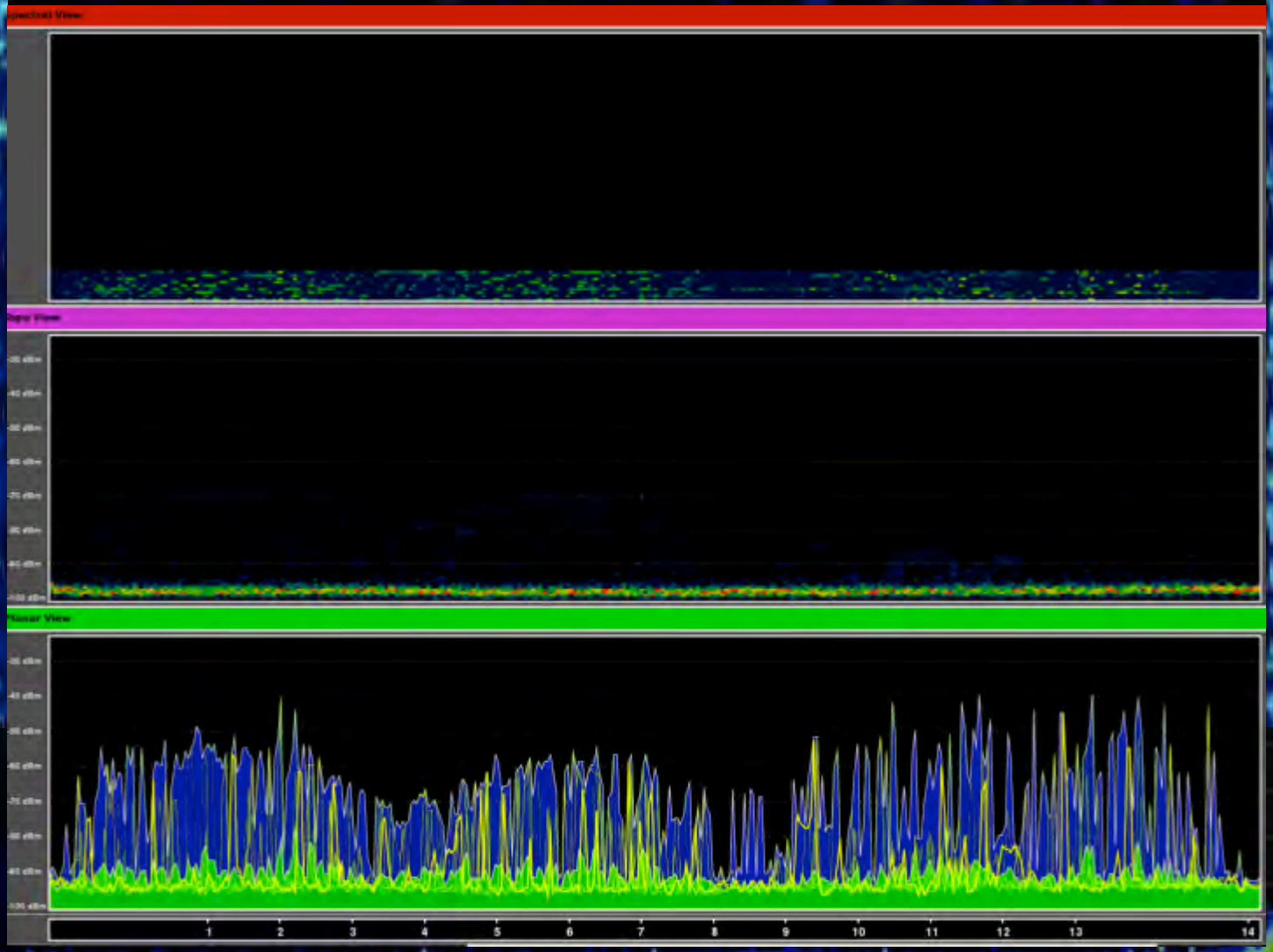
Zigbee Ch. 11-26



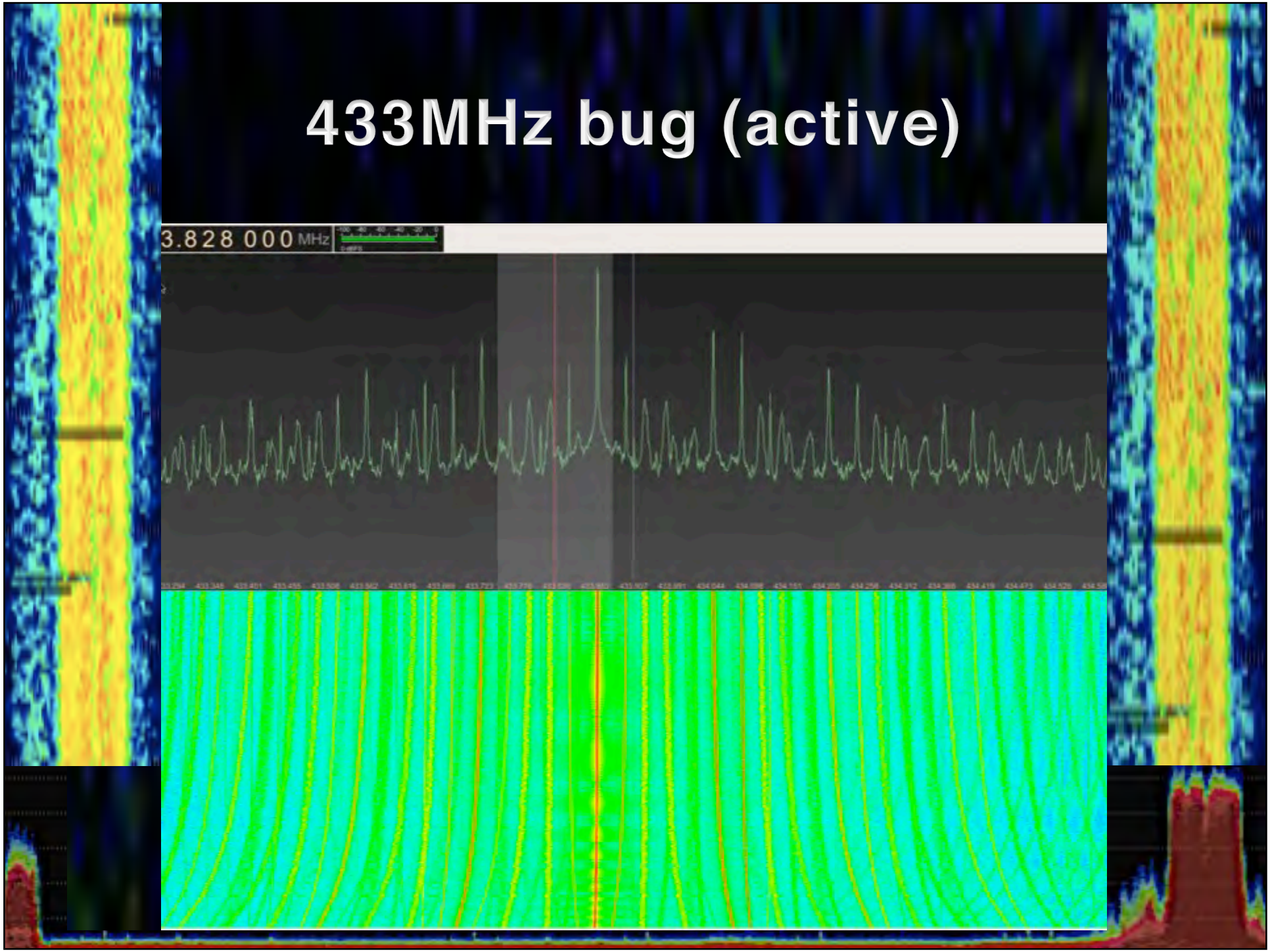
2400MHz BT spectral view



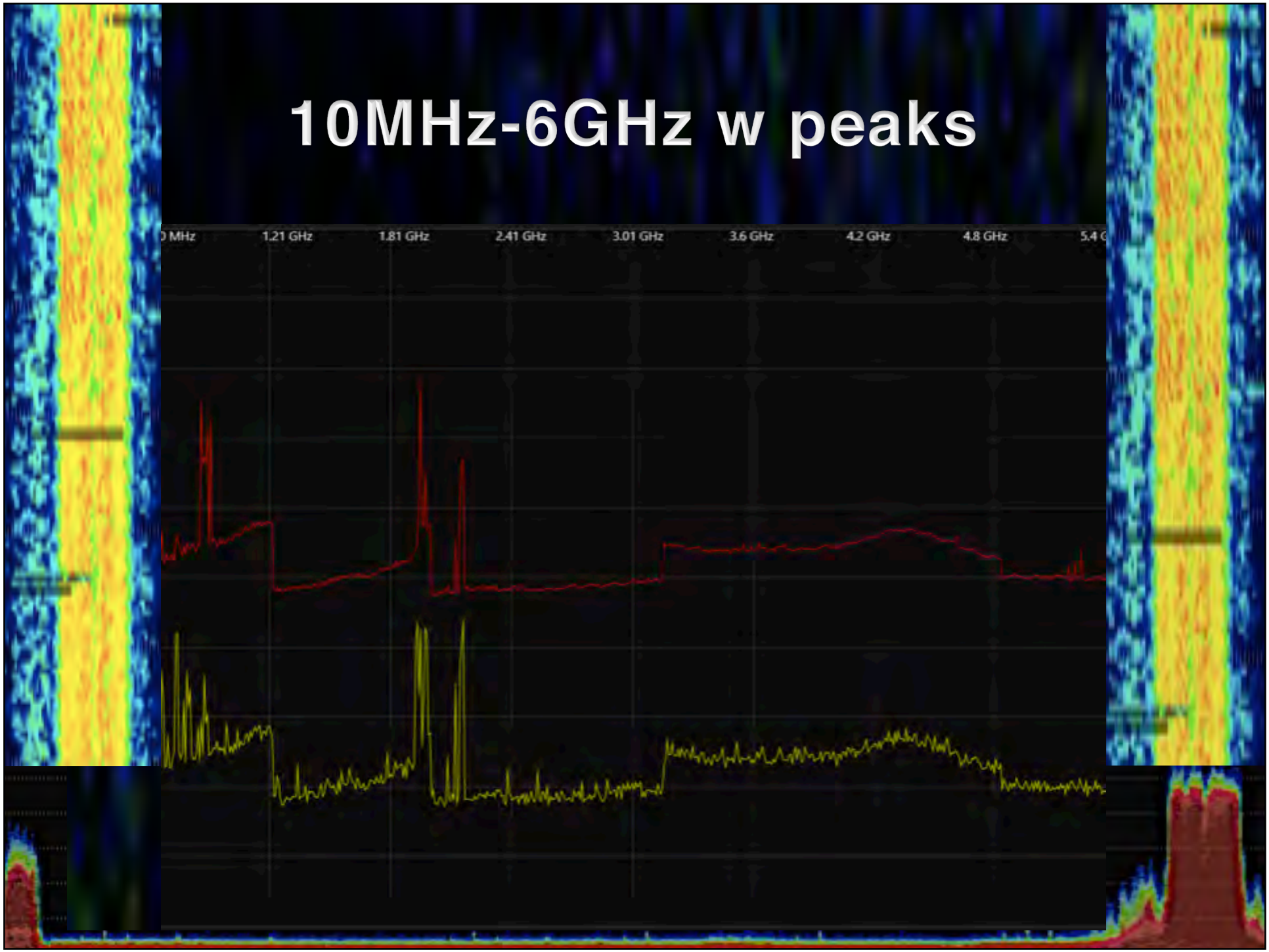
2400MHz Frequency chart



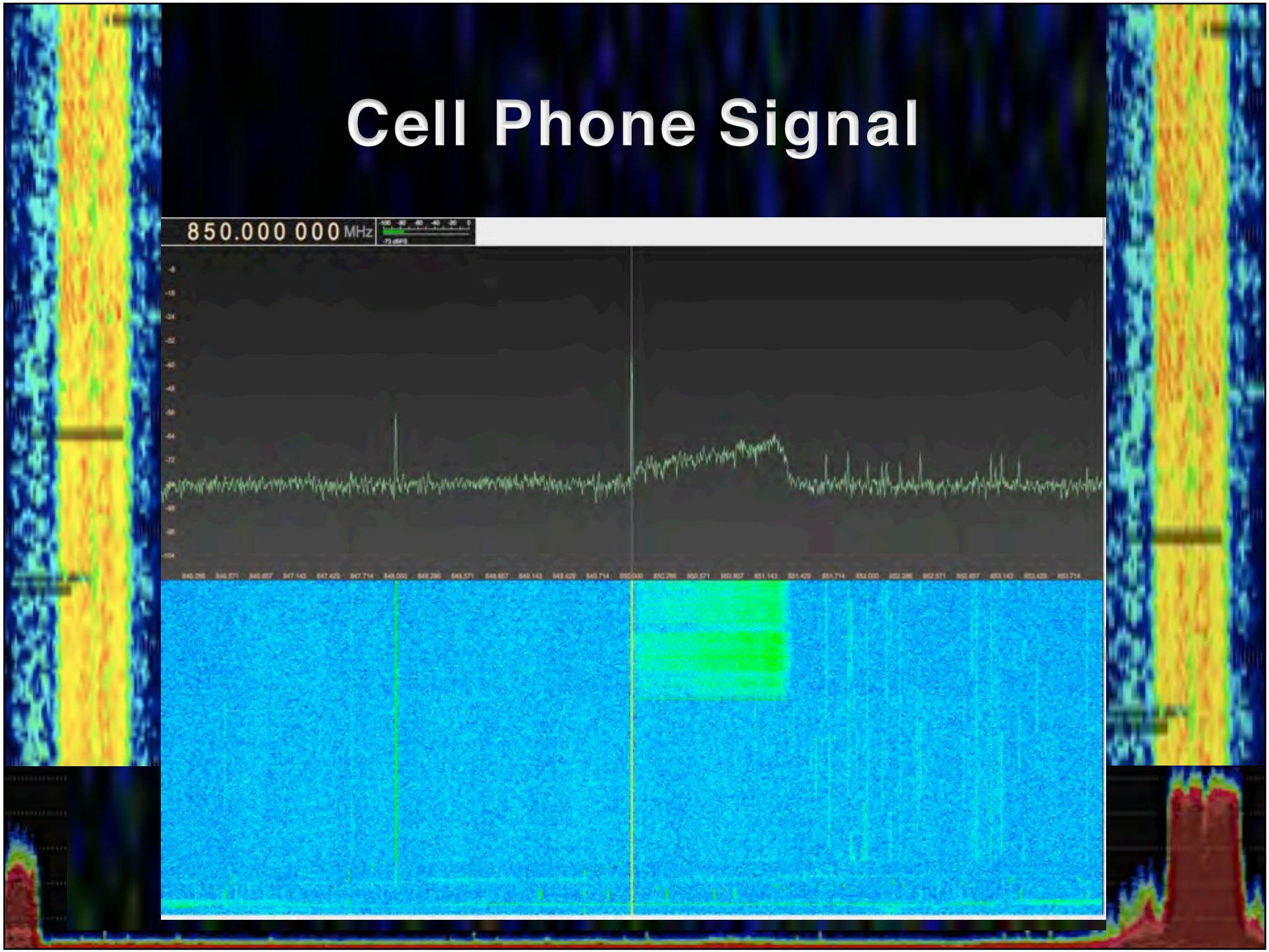
433MHz bug (active)



10MHz-6GHz w peaks



Cell Phone Signal



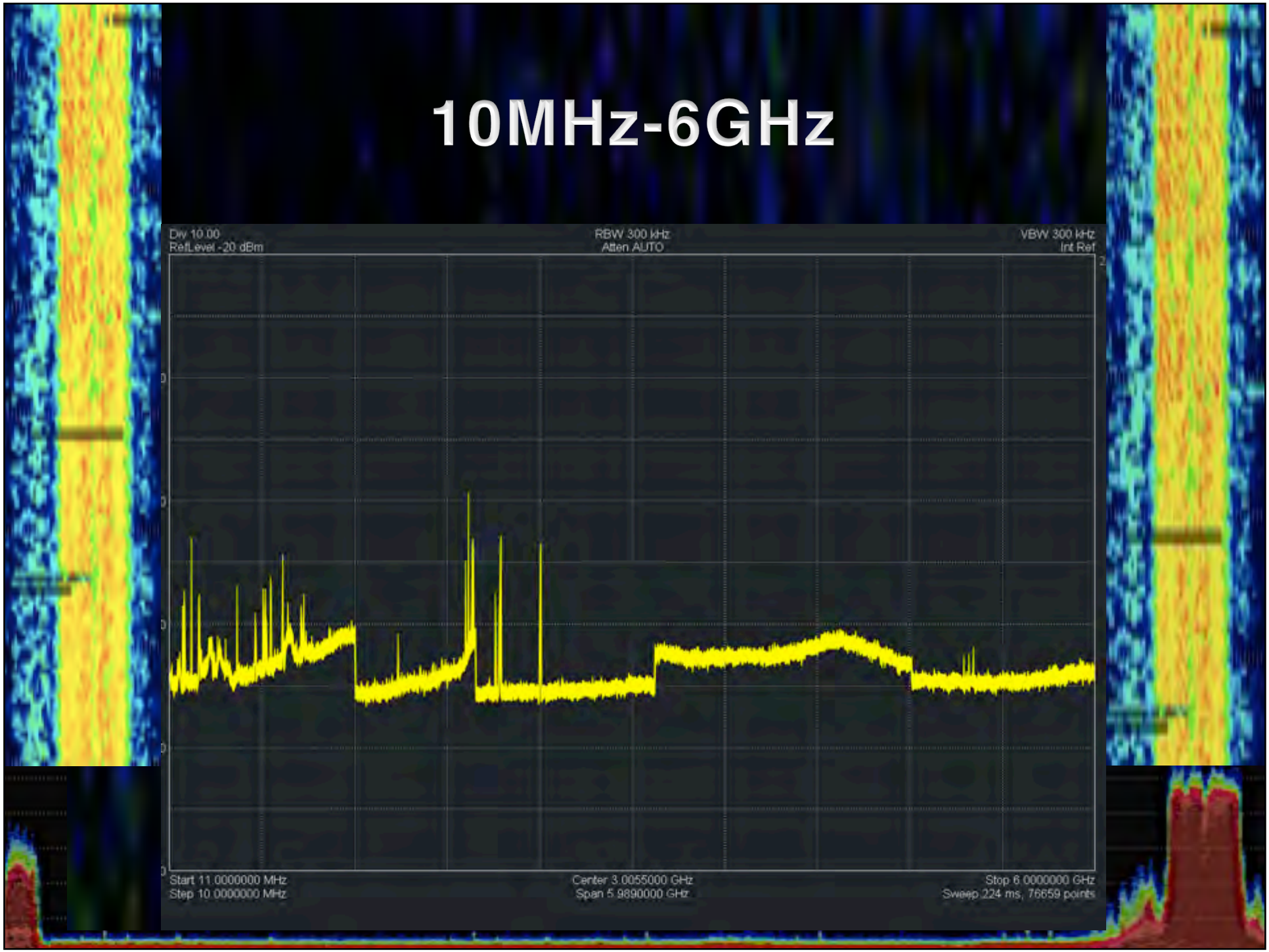
Cellular Bands

United States Carrier Frequency Use [edit]

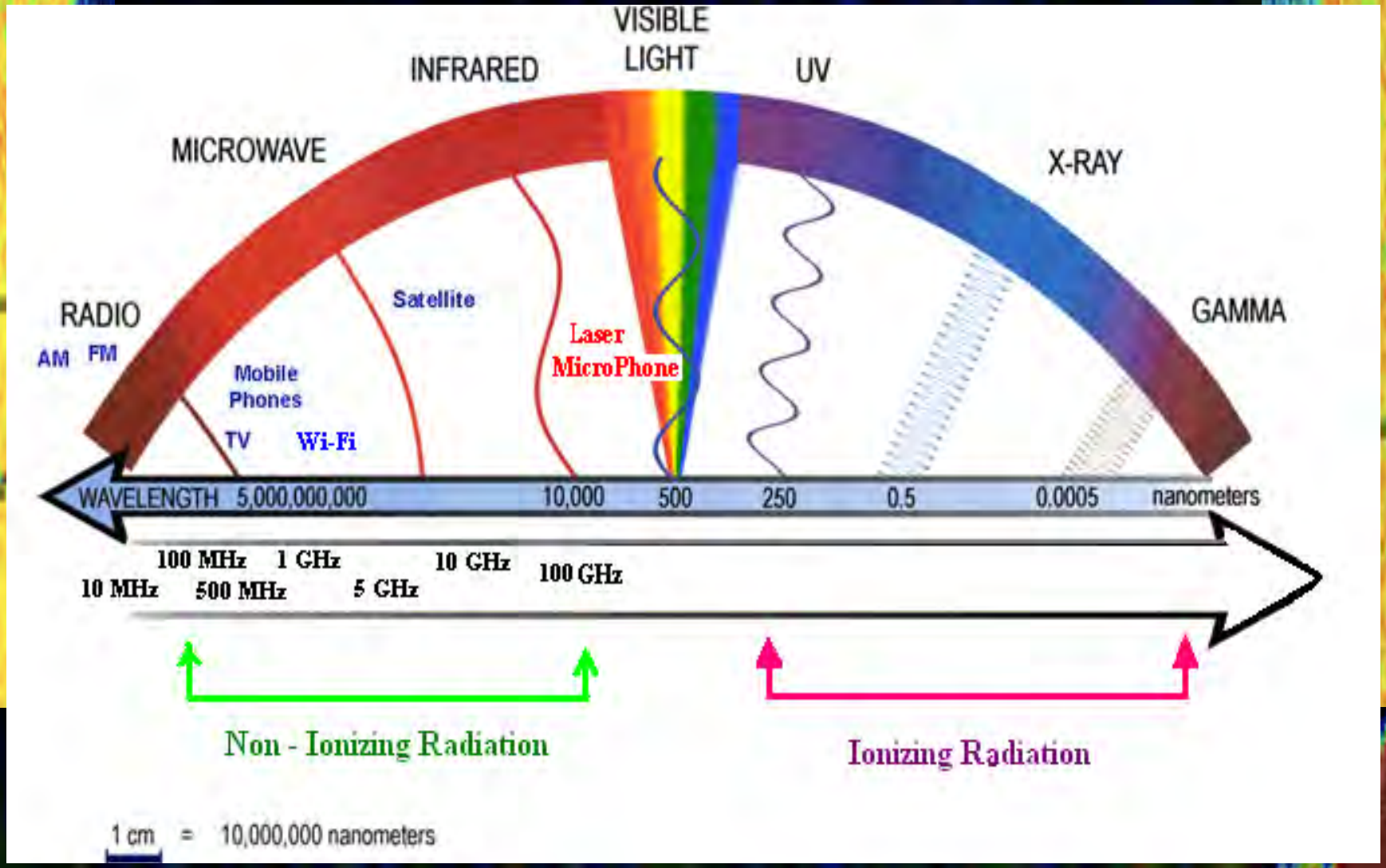
Carrier	UHF Voice Frequencies				3G UHF Frequency / Band name			4G UHF Frequency / Band number							3G Technology		4G Technology	
	800 MHz	850 MHz	1700 MHz 2100 MHz	1900 MHz	850 MHz	1700 MHz 2100 MHz	1900 MHz	700 MHz	750 MHz	800 MHz	850 MHz	1700 MHz 2100 MHz	1900 MHz	2500 MHz	GSM HSPA+	CDMA EVDO	WiMax	LTE
					CLR	AWS	PCS	12,17	13	26	5	4	2,25	41				
AT&T Mobility	✗	✓	✗	✓	✓	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓	✗	✗	✓
T-Mobile US	✗	✗	✓	✓	✗	✓	✓	◔	✗	✗	✗	✓	◔	✗	✓	✗	✗	✓
Sprint Corporation	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	✓	✗	✓	✓†	✓§
Verizon Wireless	✗	✓	✗	✓	✓	✗	✓	✗	✓	✗	✗	✓	✗	✗	✗	✓	✗	✓
U.S. Cellular	✓	✗	✗	✓	✓	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓

http://en.wikipedia.org/wiki/Cellular_frequencies

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

RF Spectrum


VISIBLE
LIGHT
INFRARED
UV
MICROWAVE
X-RAY
RADIO
AM FM
Satellite
Laser
MicroPhone
GAMMA
Mobile
Phones
TV
Wi-Fi
WAVELENGTH 5,000,000,000
10,000
500
250
0.5
0.0005
nanometers
100 MHz
1 GHz
10 GHz
100 GHz
10 MHz
500 MHz
5 GHz
Non - Ionizing Radiation
Ionizing Radiation
1 cm = 10,000,000 nanometers

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

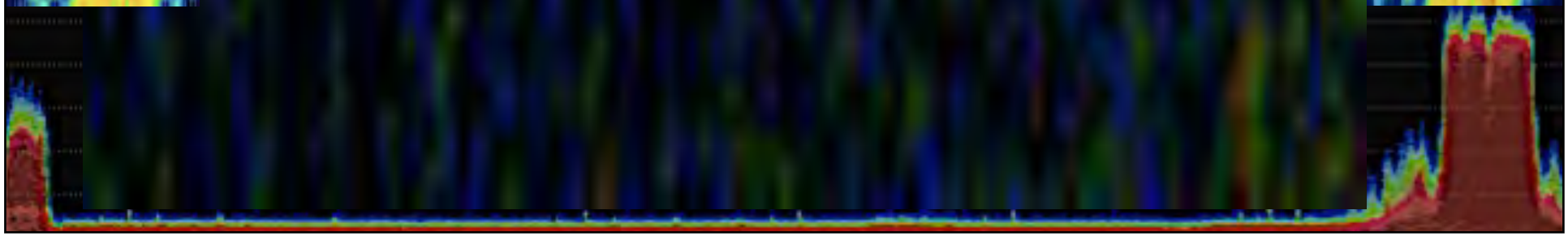
Channelizer
multimon-ng
smartnet-scanner
GNUradio
OsmoComSDR
EyeP.A.
SpecTools

Kit Hardware Tools

wispy DBX
signal hound
hackrf
rtlsdr
ubertooth
various 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












Antennas

Frequency range Matters for your target

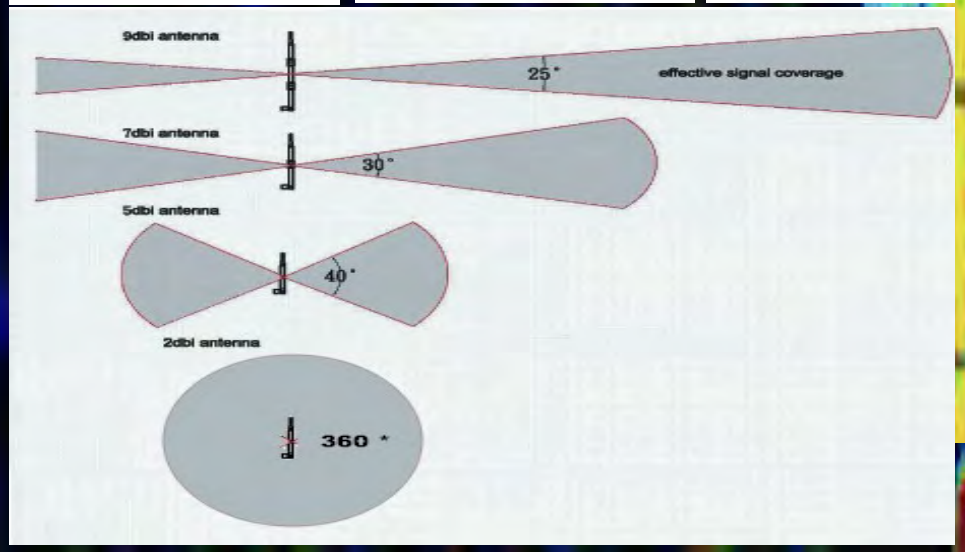
Omnidirectional

2, 5, 7 dBi

Directional

Panel

Yagi

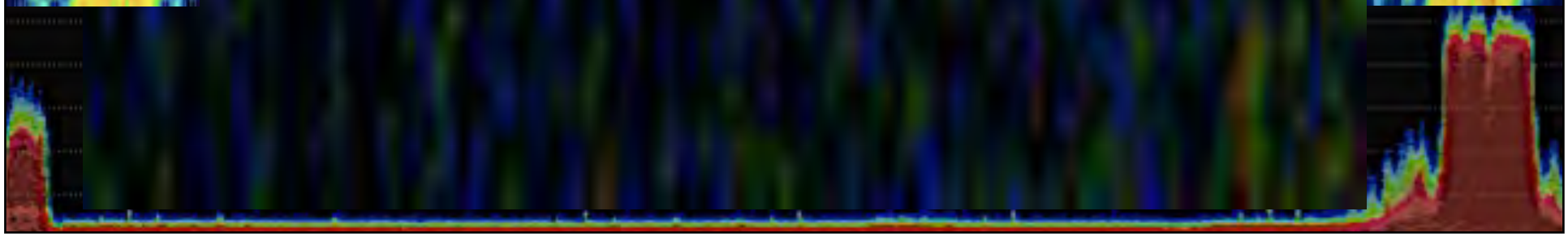


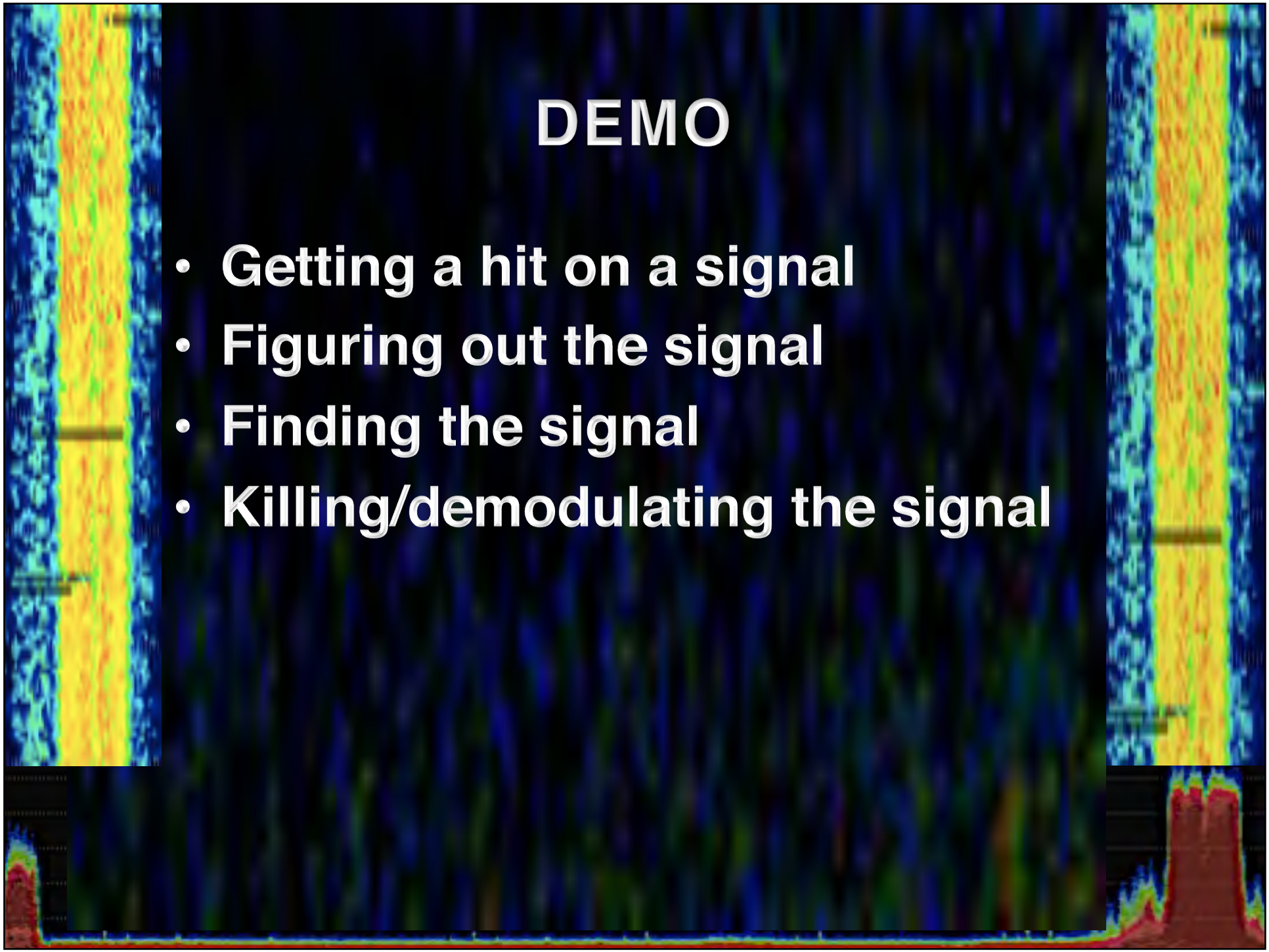
Something to carry it in

- Pack
- Pelican case
- Vehicle

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




DEMO
• Getting a hit on a signal
• Figuring out the signal
• Finding the signal
• Killing/demodulating the signal

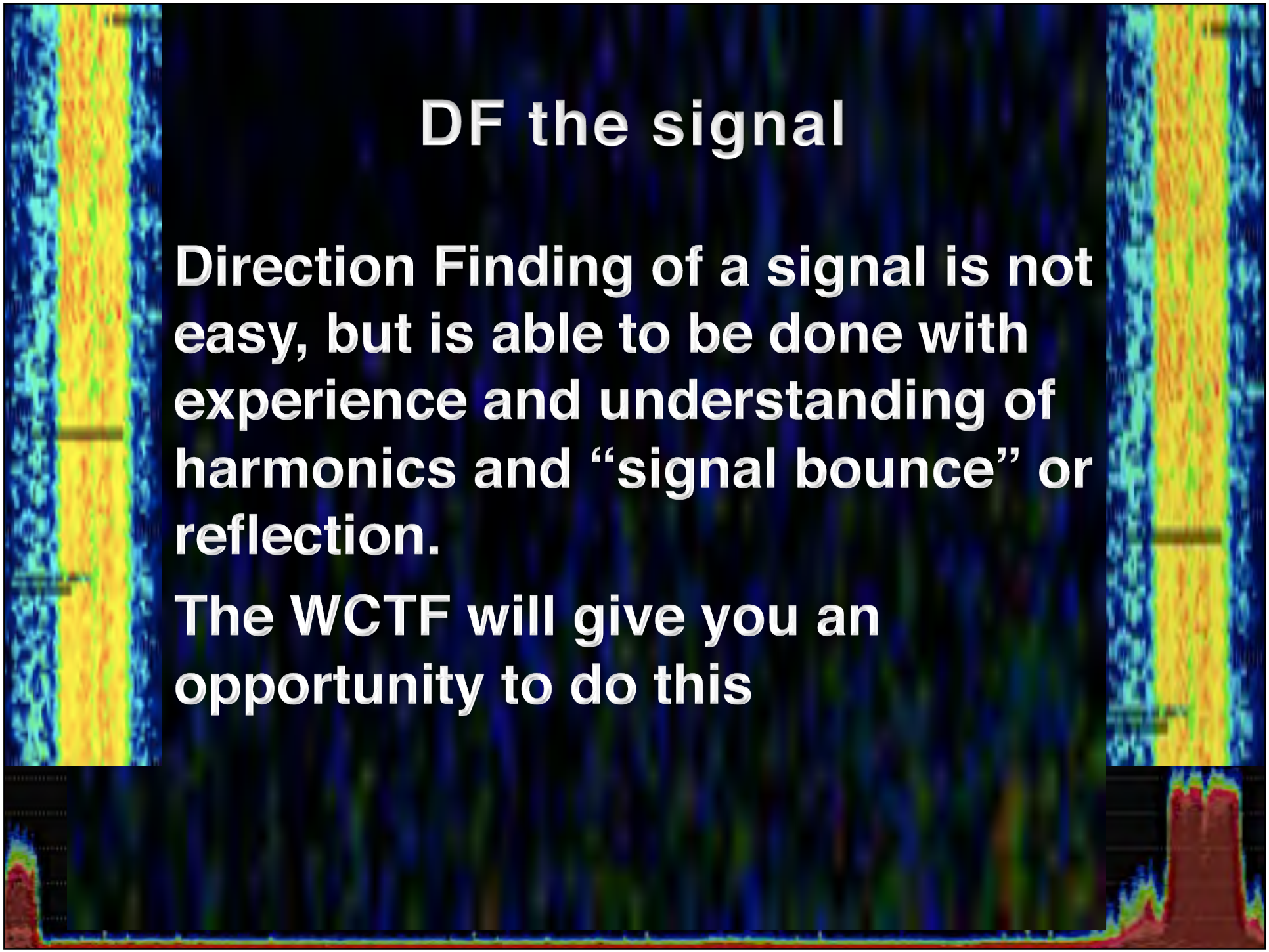
Your Targets

Your Weapons and Targets


RTL-SDR wiki
Awesome reference

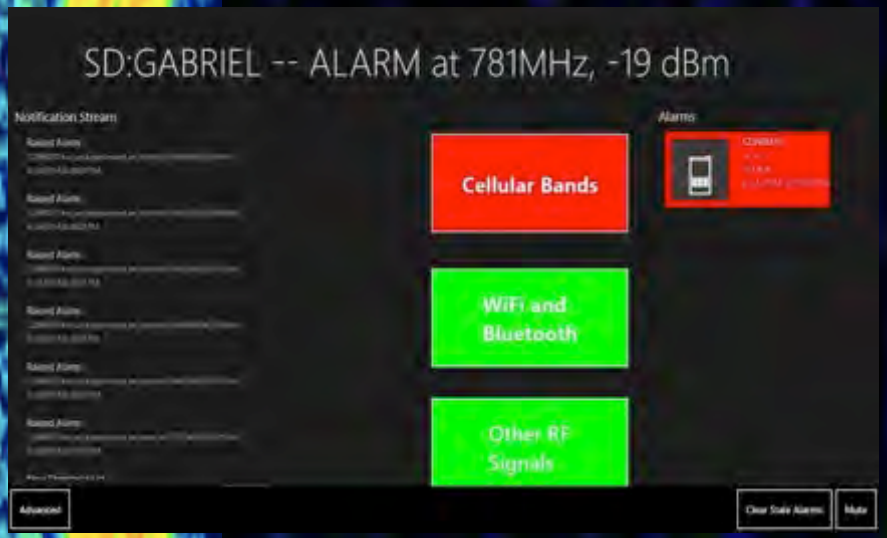

Why SDR is so important in RF assessments
The ability to write code to perform the job at hand is something that the RF industry hasn't had in the past, now we can, thanks
GNURadio Companion


Antenna theory for RF
• Right antenna for the right job and frequency Dakahuna, go ☺

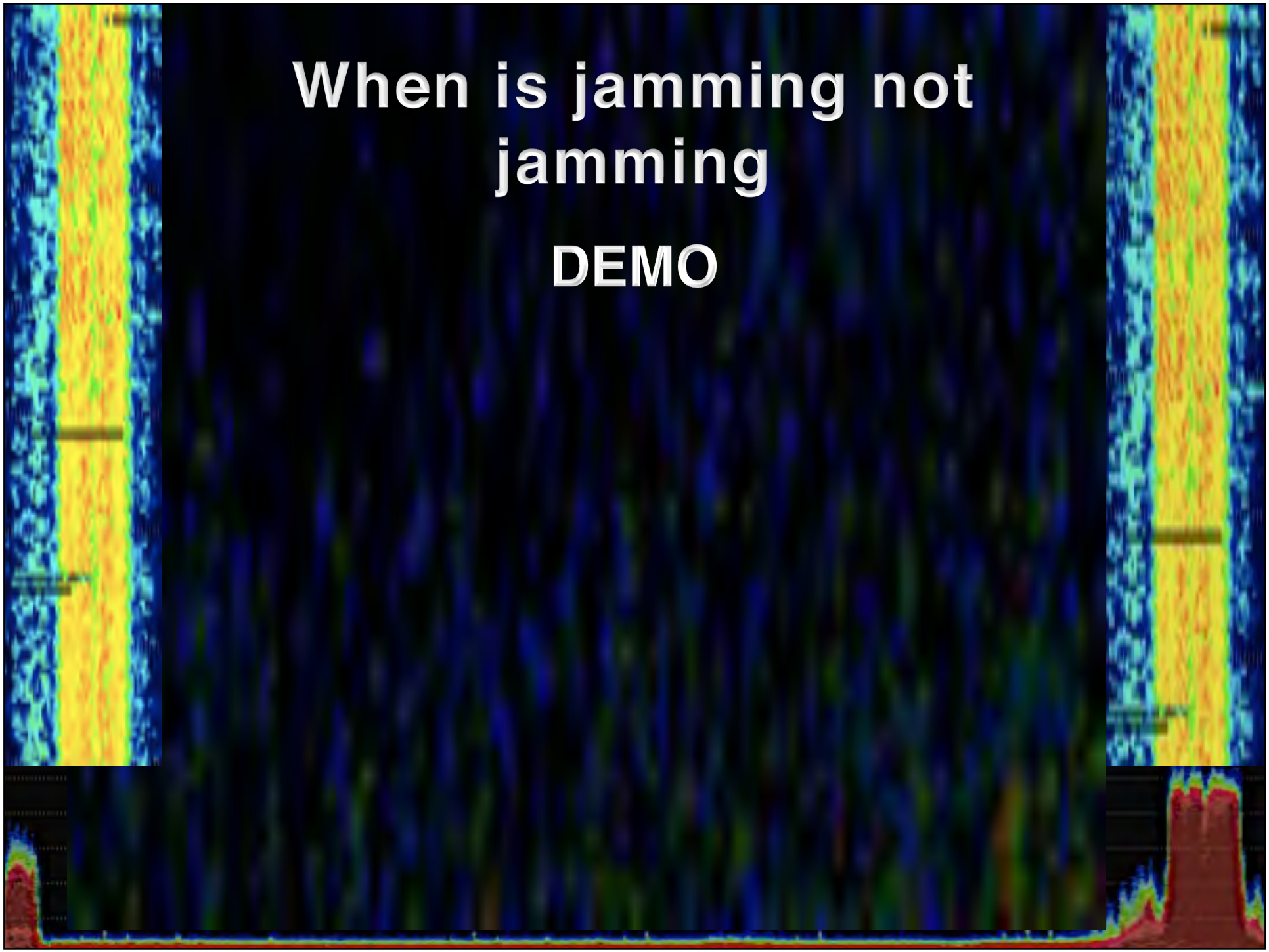

DF the signal
Direction Finding of a signal is not easy, but is able to be done with experience and understanding of harmonics and “signal bounce” or reflection.
The WCTF will give you an opportunity to do this

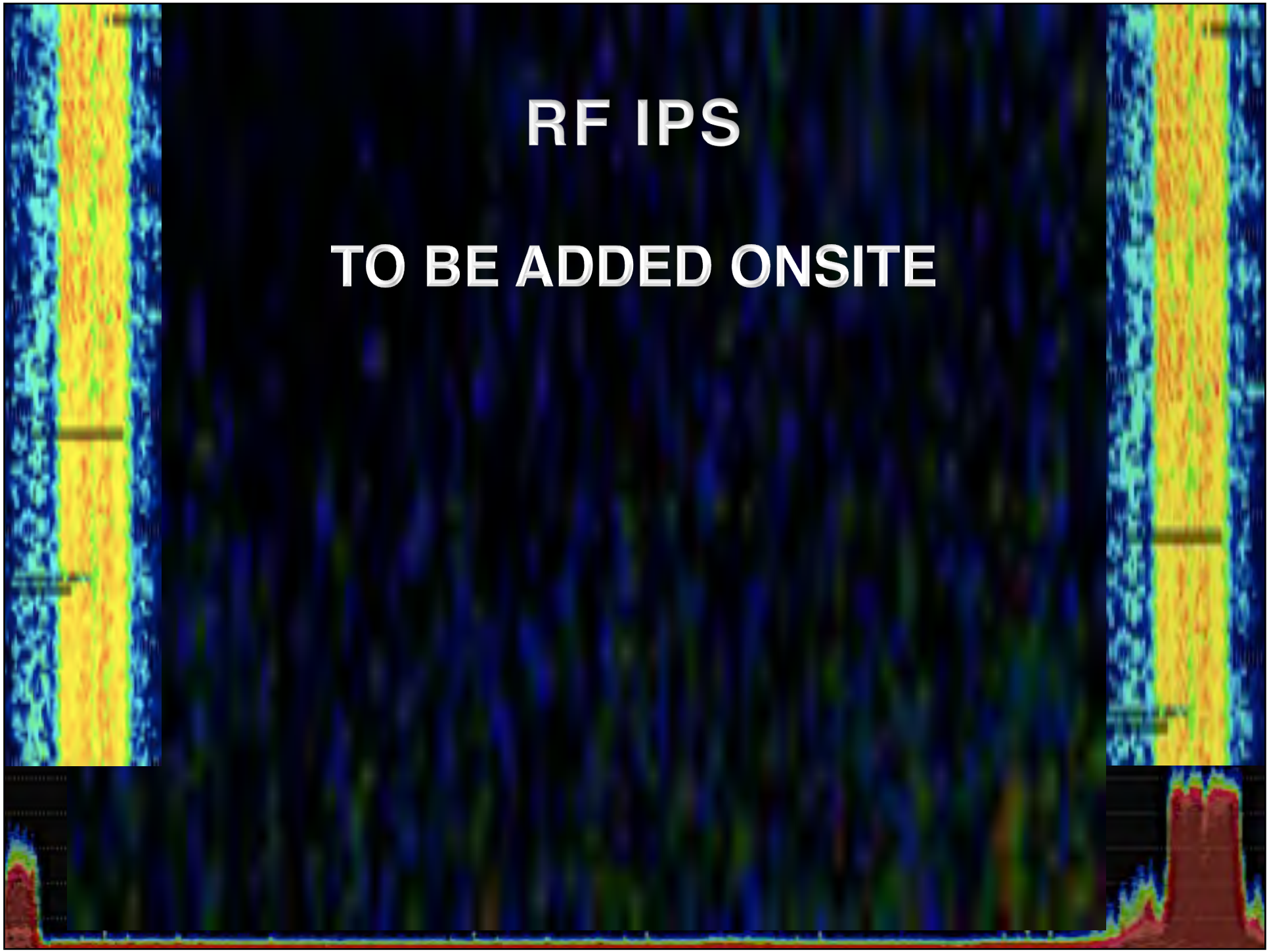

Why good headphones matter
Playing through the speaker at DC
DEMO

RF IDS


SD:GABRIEL -- ALARM at 781MHz, -19 dBm
Notification Stream
Alarms
Cellular Bands
WiFi and Bluetooth
Other RF Signals
Advanced
Clear State Alarms
Mute


Advanced
SIGNALS DEFENSES
Alarms


When is jamming not jamming
DEMO

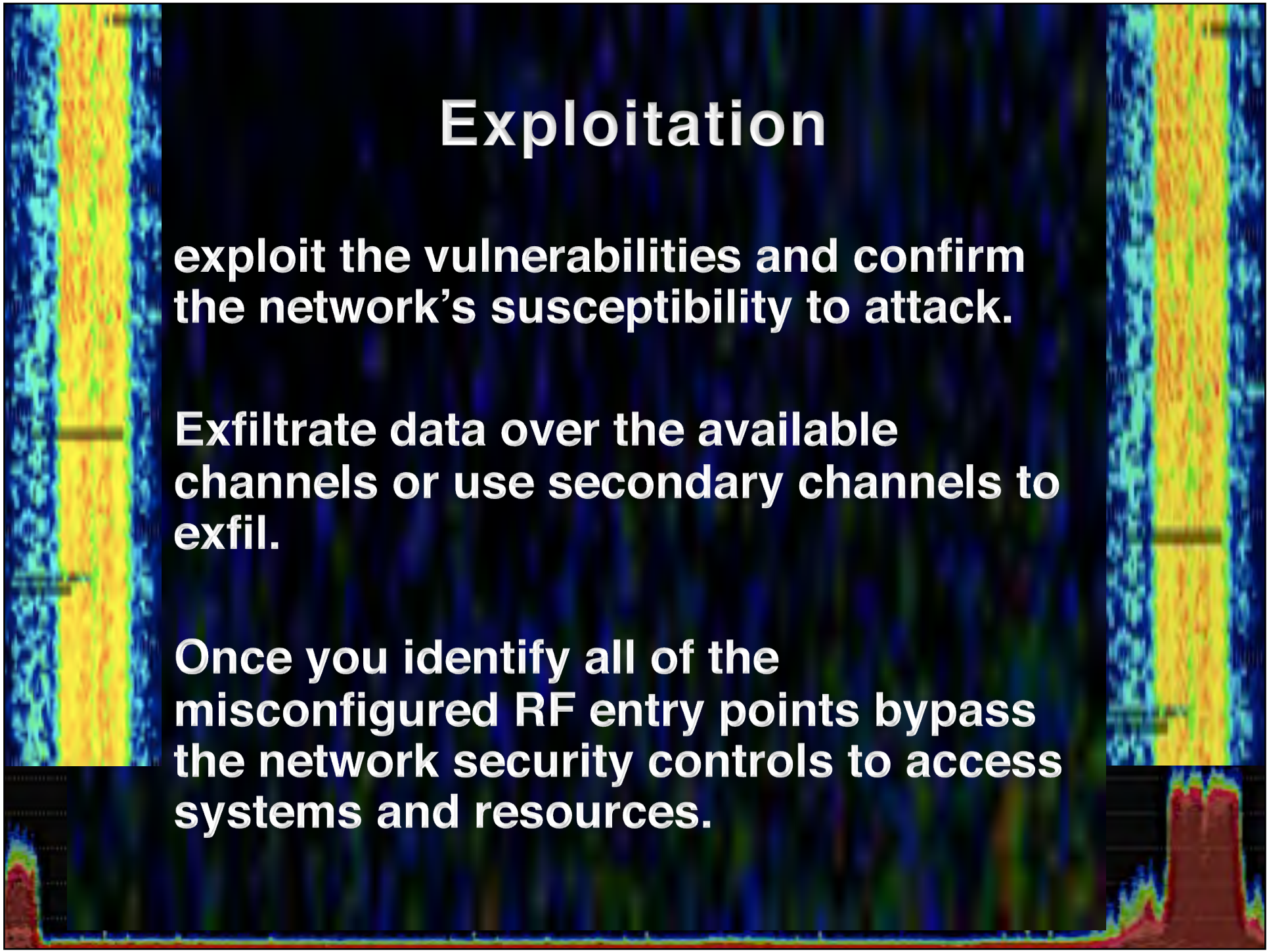

RF IPS
TO BE ADDED ONSITE

Recon

Map and identify active devices on the network within the ranges identified.

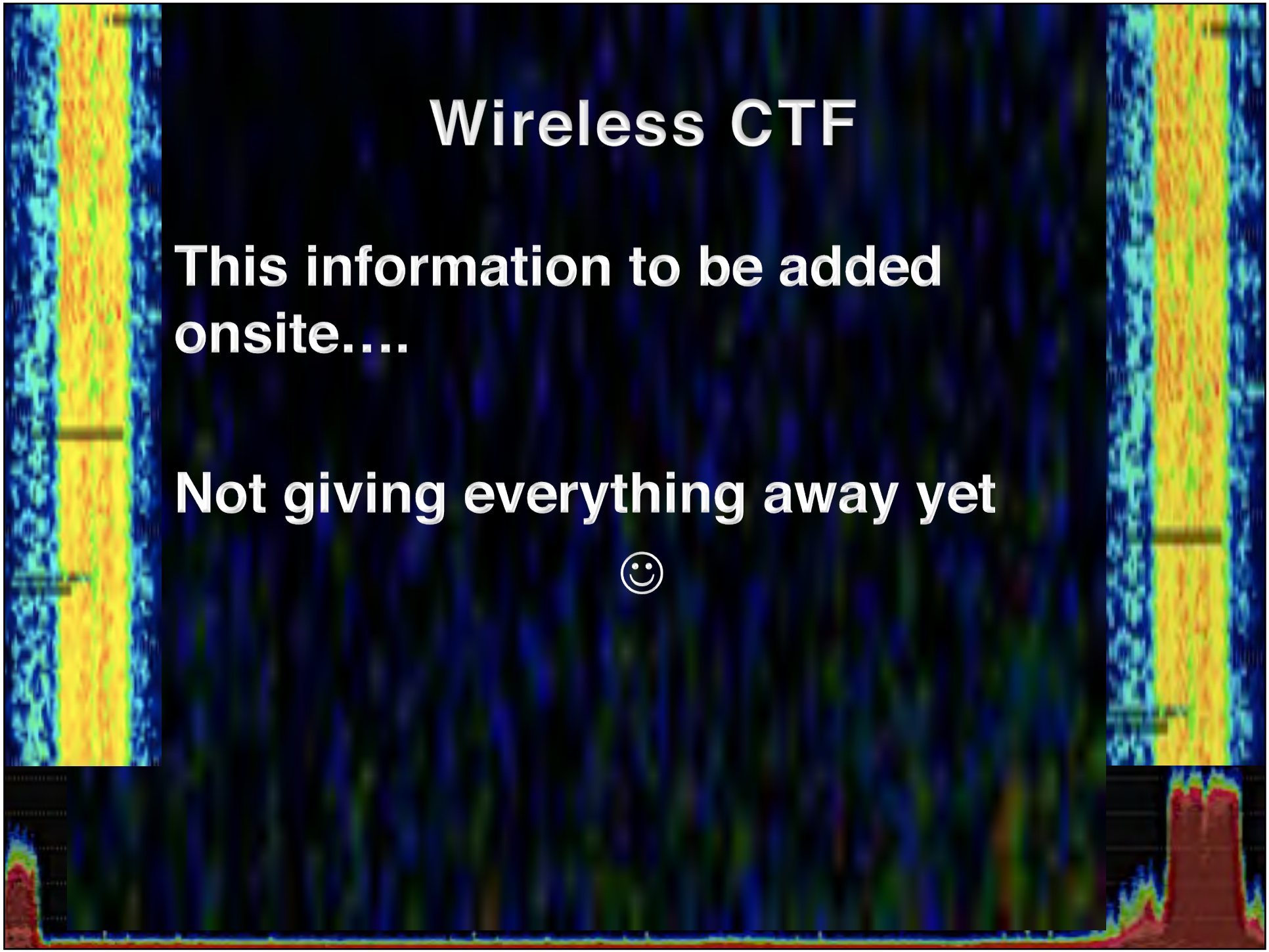
Characterize the target network to develop an understanding of the network architecture, and determine the devices and services available on the network.

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.

Putting It All Together

This will be updated onsite!!!


Wireless CTF
This information to be added onsite….
Not giving everything away yet
☺

SPONSORS


SIGNALS DEFENSE
aruba
NETWORKS
TACTICAL
NETWORK SOLUTIONS
GREAT SCOTT GADGETS
metageek
nuand
HAK5
simpleWiFi
AirTight
NETWORKS
PentesterAcademy
a SecurityTube.net initiative

Questions

@rmellendick
@DaKahuna2007
@wctf_us
@WiFi_Village