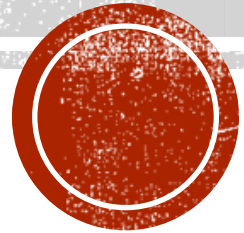
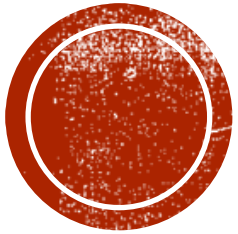
THE RADIO STAR LIVES

MTV hasn't killed it yet…





Intercepting, Modifying, and Generating Wireless Signals with SDR

DEFCON talk by Caleb Madrigal

calebmadrigal.com

01

Using a Software Defined Radio (SDR) to control the airwaves

02

Radio waves === The Force

03

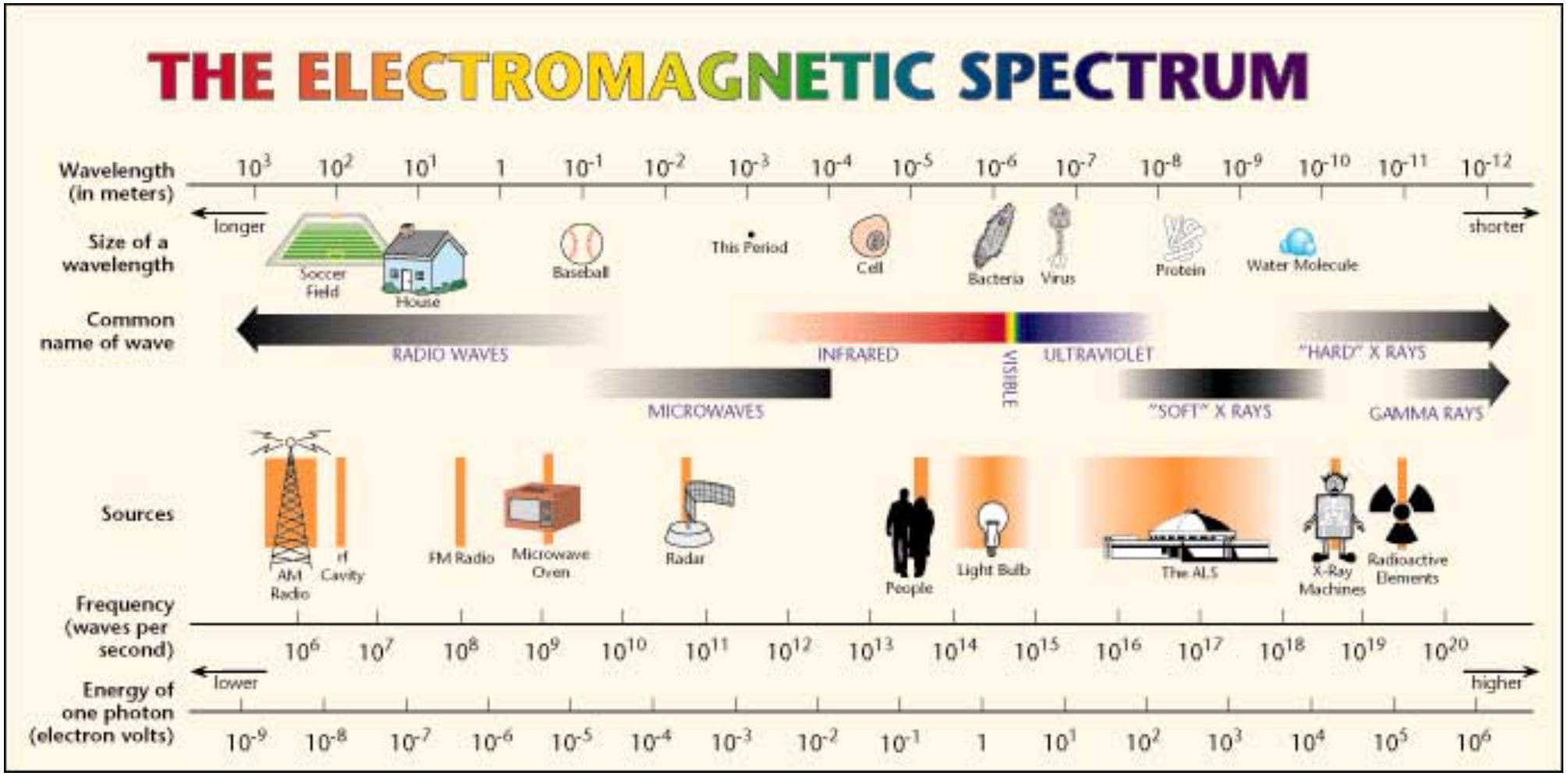
Networking at the Physical layer

04

He unlocked his Jeep with a replay attack.

WHAT WAS IT?

WHERE ARE WE LOOKING?




IS THAT HOW WIRELESS STUFF WORKS?
YES IT IS OTHER BARRY, YES IT IS.
memegenerator.net

WHAT IS WIRELESS?

- "Radio" (AM, FM)
- TV
- Cell phones - 800MHz &1900MHz
- Wifi - 2.5MHz
- Bluetooth - 2483.5 MHz
- GPS - 1575.42MHz & 1227.60MHz
- Wireless security systems - 2.4MHz (WIFI)
- Any form of Wireless IoT device – 2.4MHz (WIFI)
- SCADA systems / large industrial equipment
- Car Key Fobs -- 315 MHz

ALL USE RADIOWAVES!

Propagation Animation

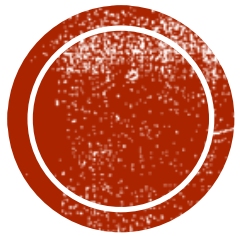
from Caleb's slides

WH

-
-
-
-

VES!

from Caleb's slides



WHO USES THE RADIO?

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM

RADIO SERVICES COLOR LEGEND

- AERONAUTICAL MOBILE
- AERONAUTICAL MOBILE SATELLITE
- AERONAUTICAL RADIONAVIGATION
- AMATEUR
- AMATEUR SATELLITE
- BROADCASTING
- BROADCASTING SATELLITE
- EARTH EXPLORATION SATELLITE
- FIXED
- FIXED SATELLITE
- INTER-SATELLITE
- LAND MOBILE
- LAND MOBILE SATELLITE
- MARITIME MOBILE
- MARITIME MOBILE SATELLITE
- MARITIME RADIONAVIGATION
- METEOROLOGICAL AIDS
- METEOROLOGICAL SATELLITE
- MOBILE
- MOBILE SATELLITE
- RADIO ASTRONOMY
- RADIODETERMINATION SATELLITE
- RADIOLOCATION
- RADIOLOCATION SATELLITE
- RADIONAVIGATION
- RADIONAVIGATION SATELLITE
- SPACE OPERATION
- SPACE RESEARCH
- STANDARD FREQUENCY AND TIME SIGNAL
- STANDARD FREQUENCY AND TIME SIGNAL SATELLITE

ACTIVITY CODE

- GOVERNMENT EXCLUSIVE
- GOVERNMENT/NON-GOVERNMENT SHARED
- NON-GOVERNMENT EXCLUSIVE

ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letters
Secondary	Mobile	1st Capital with lower case letters

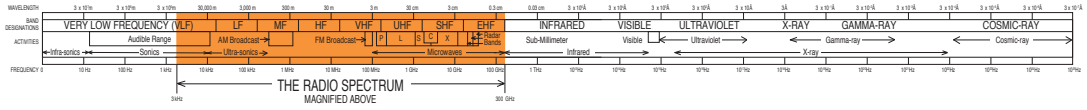
This chart is a graphic single-point-in-time portrayal of the Table of Frequency Allocations used by the FCC and NTIA. As such, it does not completely reflect all aspects, i.e., footnotes and recent changes made to the Table of Frequency Allocations. Therefore, for complete information, users should consult the Table to determine the current status of U.S. allocations.

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management

October 2003

* EXCEPT AERO MOBILE (R)

** EXCEPT AERO MOBILE



PLEASE NOTE: THE SPACING ALLOTTED THE SERVICES IN THE SPECTRUM SEGMENTS SHOWN IS NOT PROPORTIONAL TO THE ACTUAL AMOUNT OF SPECTRUM OCCUPIED.

Laramie

WyoLink Project 25 Phase I	Laramie Police/Fire/EMS has transitioned to WyoLink

Frequency	License	Type	Tone	Alpha Tag	Description	Mode	Tag
154.43000	WPCI938	RM	192.8 PL	Laramie FD	Fireground	FM	Fire-Tac
154.05500	KJY670	BM	CSQ	Laramie PW	Services	FM	Public Works
154.05500		BM	192.8 PL	Laramie Pest	Laramie Mosquito Control	FMN	Public Works
155.25000	KVM248	RM	192.8 PL	Laramie PD 1	Police Primary	FM	Deprecated
155.31000	WPCQ660	RM	156.7 PL	Laramie PD 2	Police (obsolete?)	FM	Deprecated

University of Wyoming

WyoLink Project 25 Phase I	UW Police operate on WyoLink

Frequency	License	Type	Tone	Alpha Tag	Description	Mode	Tag
155.86500	WNAL764	RM	100.0 PL	UnivWyo Mnt1	Maintanence 1	FM	Schools
154.98000	WPTR832	RM	CSQ	UnivWyo Bus	Transit Bus	FM	Schools
155.05500	WQBA343	RM	CSQ	UnivWyo Act	Activities	FM	Schools
453.47500	WNKB427	RM	107.2 PL	JelmPkObserv	Jelm peak observatory	FM	Schools
155.94000		RM		UW Housekeep	Housekeeping	FMN	Schools
155.55000	KJP294	RM	192.8 PL	UnivWyo PD	Police	FM	Deprecated

Laramie

WyoLink Project 25 Phase I	Laramie Police/Fire/EMS has transitioned to WyoLink

Frequency	License	Type	Tone	Alpha Tag	Description	Mode	Tag
154.43000	WPCI938	RM	192.8 PL	Laramie FD	Fireground	FM	Fire-Tac
154.05500	KJY670	BM	CSQ	Laramie PW	Services	FM	Public Works
154.05500		BM	192.8 PL	Laramie Pest	Laramie Mosquito Control	FMN	Public Works
155.25000	KVM248	RM	192.8 PL	Laramie PD 1	Police Primary	FM	Deprecated
155.31000	WPCQ660	RM	156.7 PL	Laramie PD 2	Police (obsolete?)	FM	Deprecated

University of Wyoming

WyoLink Project 25 Phase I	UW Police operate on WyoLink

Frequency	License	Type	Tone	Alpha Tag	Description	Mode	Tag
155.86500	WNAL764	RM	100.0 PL	UnivWyo Mnt1	Maintanence 1	FM	Schools
154.98000	WPTR832	RM	CSQ	UnivWyo Bus	Transit Bus	FM	Schools
155.05500	WQBA343	RM	CSQ	UnivWyo Act	Activities	FM	Schools
453.47500	WNKB427	RM	107.2 PL	JelmPkObserv	Jelm peak observatory	FM	Schools
155.94000		RM		UW Housekeep	Housekeeping	FMN	Schools
155.55000	KJP294	RM	192.8 PL	UnivWyo PD	Police	FM	Deprecated

UW Activities

FCC Callsign WQBA343 (UNIVERSITY OF WYOMING)

Licensee Name:	UNIVERSITY OF WYOMING
License:	WQBA343
FRN:	0006254411
Status:	Active (Effective: 09/02/2014 - Expires: 09/07/2024)
County:	ALBANY
State:	WY
Radio Service:	PW: Public Safety Pool, Conventional
Notes:	WE ARE A STATE AND WILL USE RADIOS TO BETTER COORDINATE OUR ACTIVITIES

#	Tower ID	Type	Ant Height	Struc Height	Elevation	Address
1		BANT	27.0	29.0	2186.0	PHYSICAL SCIENCES BLDG. - 9TH & FREMONT ST.
2			0.0	0.0	0.0	

radioreference.com

UW Activities

FCC Callsign WQBA343 (UNIVERS

Licensee Name:	UNIVERSITY OF WYOMING
License:	WQBA343
FRN:	0006254411
Status:	Active (Effective: 09/02/2014 - Exp
County:	ALBANY
State:	WY
Radio Service:	PW: Public Safety Pool, Conventio
Notes:	WE ARE A STATE AND WILL USE ACTIVITIES

#	Tower ID	Type	Ant Height	S
1		BANT	27.0	2
2			0.0	0

ES BLDG. - 9TH & FREMONT ST.

radioreference.com

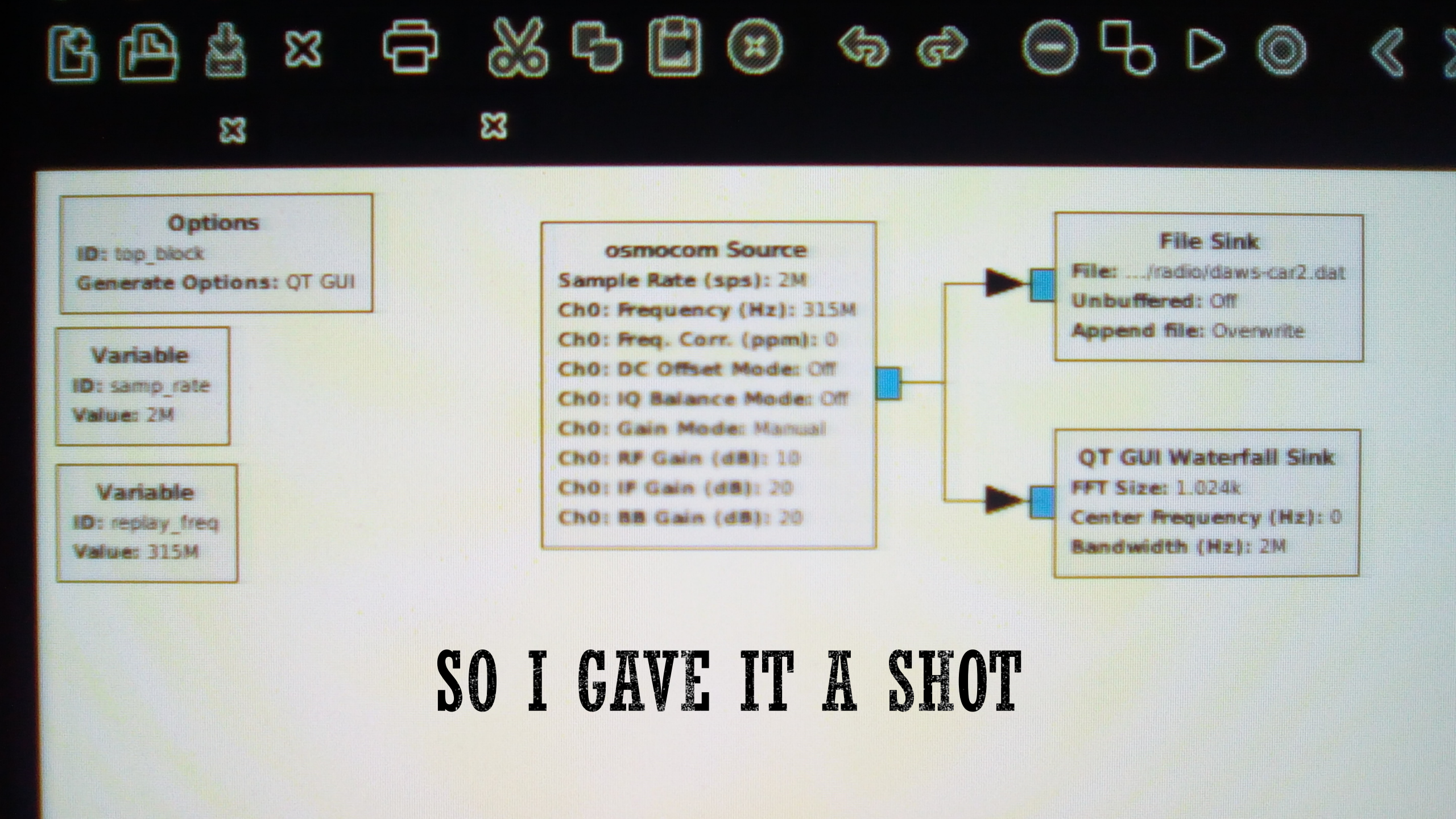

NT ST.

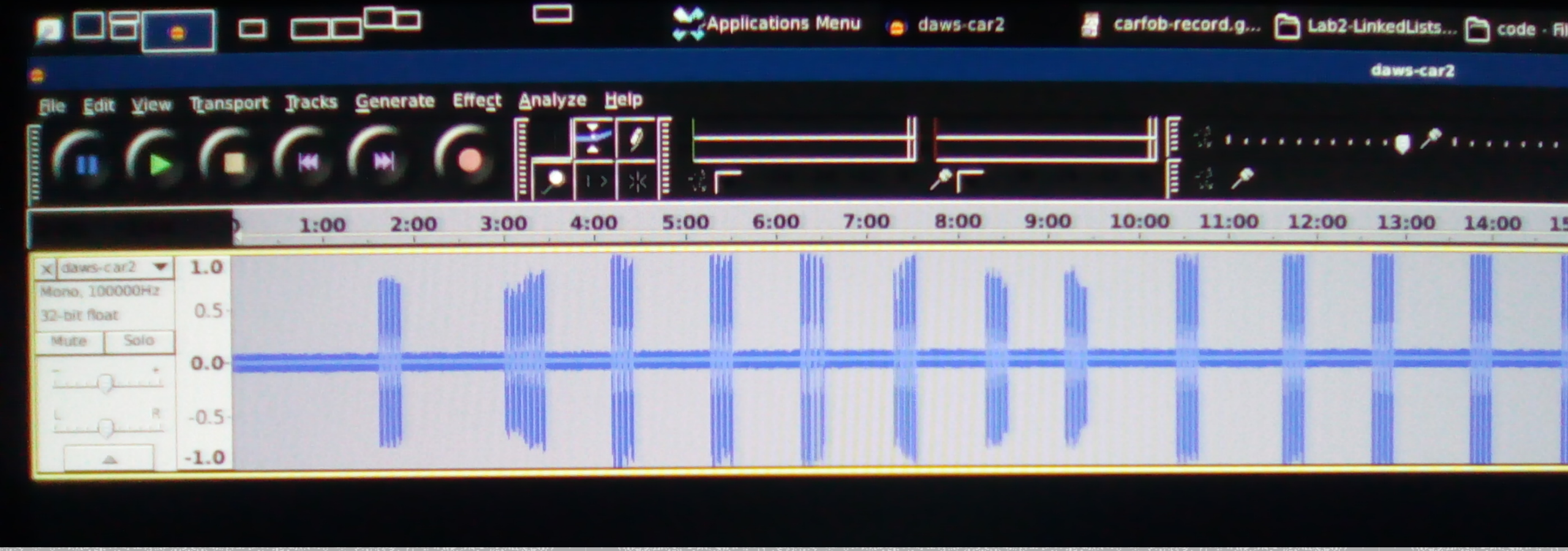

THEY'RE EVERYWHERE!
imgflip.com

SCARE FACTOR

- Many radio wave communications in public frequency bands
- Unencrypted over those^^
- When did people get so smart?

- Anyone can pick them up (legally)
- Security through obfuscation
- Is counting on the ignorance of others safe?

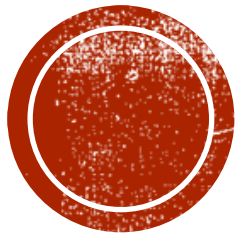

Options
ID: top_block
Generate Options: QT GUI
Variable
ID: samp_rate
Value: 2M
Variable
ID: replay_freq
Value: 315M
osmocom Source
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 315M
Ch0: Freq. Corr. (ppm): 0
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Off
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
File Sink
File: .../radio/daws-car2.dat
Unbuffered: Off
Append file: Overwrite
QT GUI Waterfall Sink
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 2M
SO I GAVE IT A SHOT



THE AUDACITY

THE AUDACITY


daws-car2
1:37.80
1:38.00
1:39.00
1:39.20
THE AUDACITY!!!!!
imgflip.com
THE



DOWN THE RABBIT HOLE

Don’t be late for tea!

COGNITIVE RADIO NETWORKS

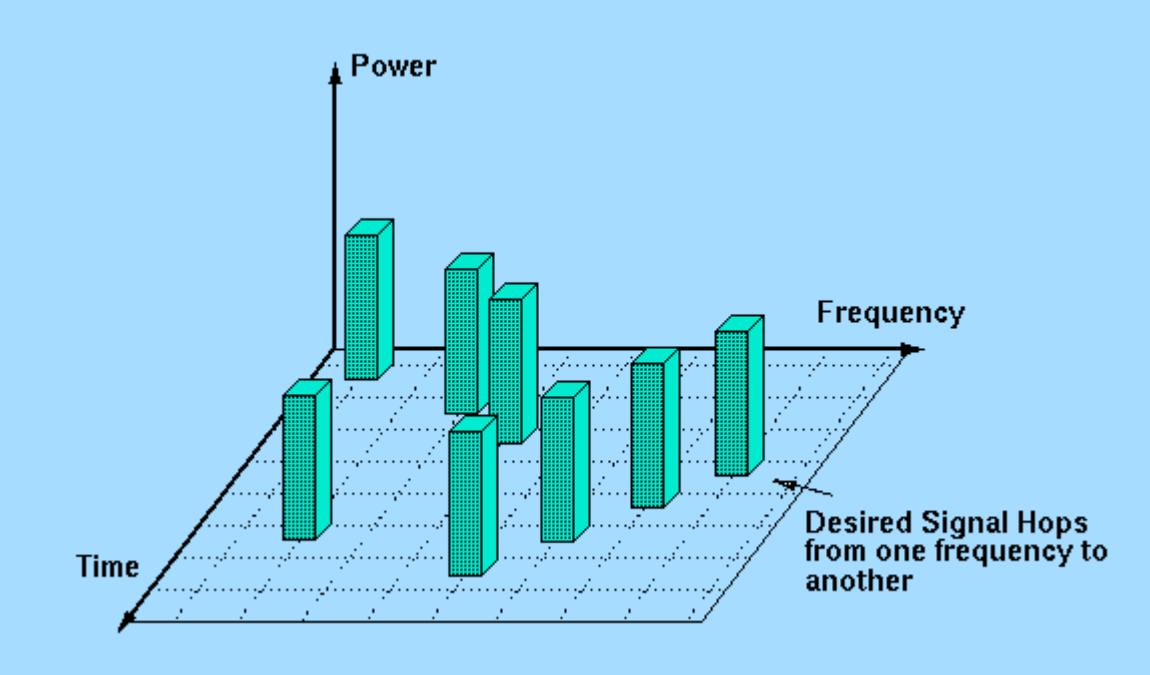
- Automagically detect uninhabited frequencies
- Starts transmitting there

123rf.com

WHICH IS KIND OF LIKE

FREQUENCY HOPPING SPREAD SPECTRUM

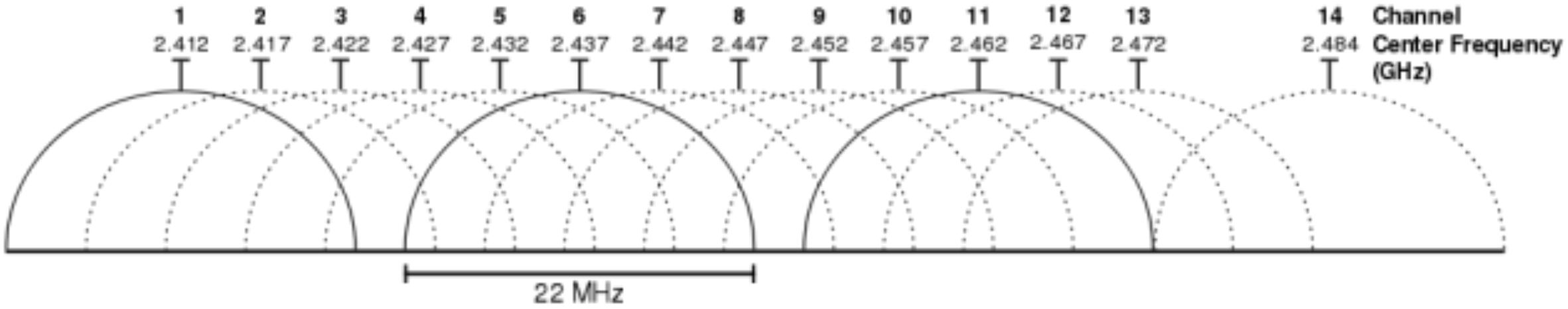
Frequency Hopping "Across The" Spectrum



WHICH IS KIND OF LIKE

WIFI'S 3 CHANNEL SYSTEM

Choose the best frequency for you!



https://www.extremetech.com/computing/179344-how-to-boost-your-wifi-speed-by-choosing-the-right-channel

https://www.extremetech.com/computing/179344-how-to-boost-your-wifi-speed-by-choosing-the-right-channel

RESOURCES

- Airflight radio surveillance
- Beginners Guide to Antennas
- Radio Frequency DB
- National Association for Amateur Radio
- Radio Hacker Extraordinare from Defcon Talk