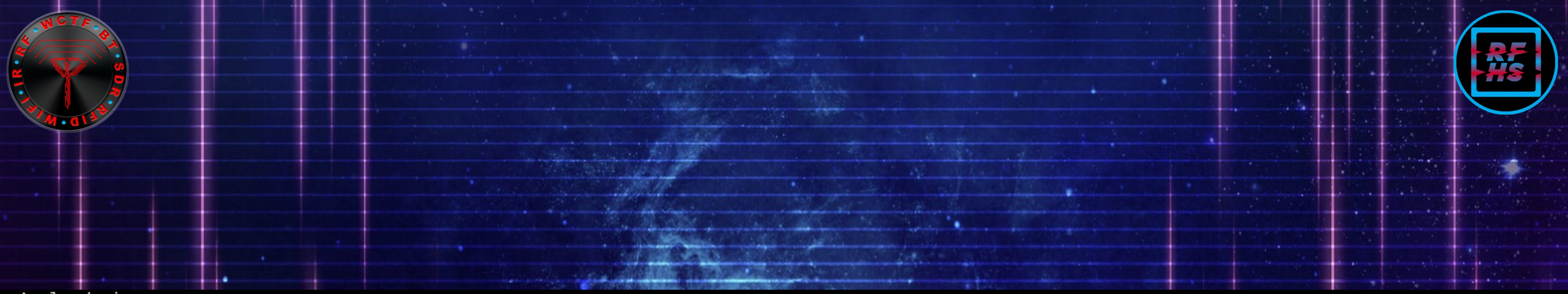
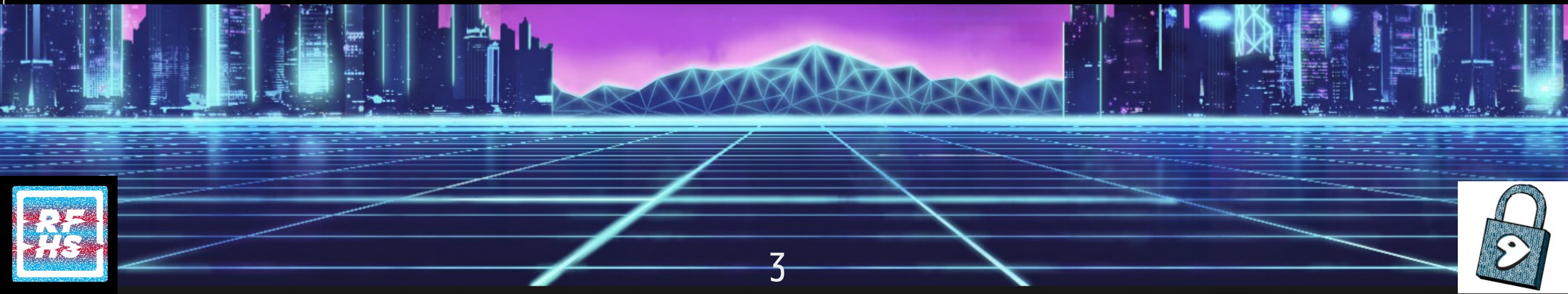
Spooky Wireless


0
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-5
-4
-3
-2
-1
0
1
2
3
4
5



Apple devices scanner

Mac	State	Device	WI-FI	OS	Phone	Time
50:2D:AC:99:12:94	Off	iPhone	On	iOS12		1563353463
7E:B5:C1:97:E4:C9	Home screen	MacBook	On	Mac OS		1563353463
51:7B:B1:BB:E5:51	Lock screen	iPhone	On	iOS12		1563353463
56:E6:3F:CD:76:86	Off	Watch	On	WatchOS		1563353453
6B:54:70:E6:25:7D	Home screen	iPhone	On	iOS12		1563353463
49:5E:D2:98:47:47	Off	iPhone	On	iOS12		1563353463
41:CE:CF:85:21:B8	Off	Watch	On	WatchOS		1563353463



WiGLE: Wireless Network

wigle.net

View | Uploads | Info | Stats | Tools | Login

WIGLE.NET

All the networks. Found by Everyone.

Google Play

STUMBLERS	WIFI NETWORKS	WIFI OBSERVATIONS	WIFI TODAY	BT DEVICES	CELL TOWERS
255,145	593,664,733	8,500,291,264	128,988	138,606,585	13,159,076

WiWiWa 2.46 released in Beta channel

Wed, 07 Aug 2019 23:46:45 GMT

Due to an over-aggressive bugfix for new Android releases by yours truly, 2.45 wouldn't run on Android J/K/L/M devices. 2.46 Should restore functionality on OLDroid.

-arkasha

Can't stop the signal, Mal

Wed, 29 May 2019 14:53:52 GMT

An update wherein this may become a developer option:

read more...

-arkasha

Google Android 9 and up: We won't fix WiFi Scanning

Fri, 24 May 2019 18:17:21 GMT

In a blow to the networking, security, and wardriving hobbyist communities today, Google has officially marked their decision to throttle wifi scanning for non-Google software on Android 9 and up as "Won't Fix" in spite of popular community support for a configurable option.

read more...

-arkasha

KML fixes and improvements

Sun, 31 Mar 2019 00:07:35 GMT

Original KML didn't contain Bluetooth and Cellular data, and users have pointed out that we've had two incompatible KML export formats in WiGLE WiFi Wardriving's "Database" tool and everywhere else. The server side (upload page and Wifi Wardriving uploads) KML export is now enhanced!

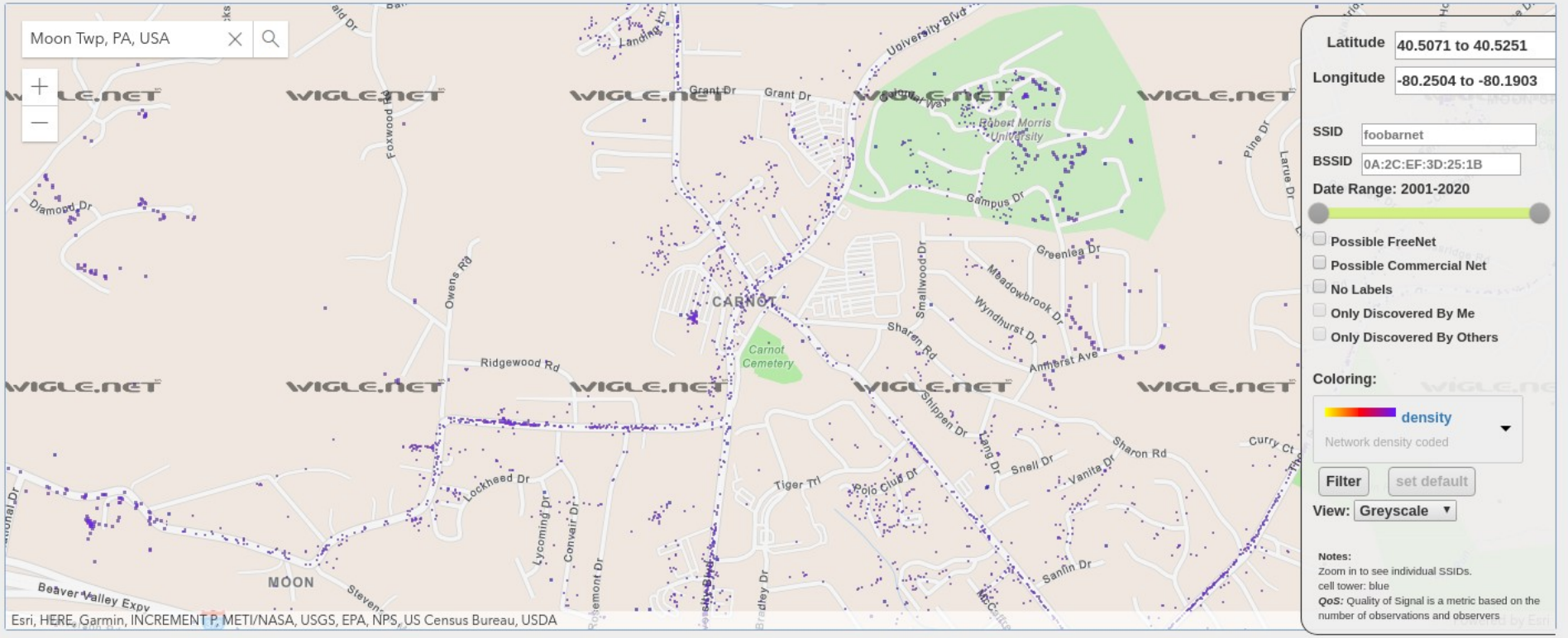
read more...

-arkasha

Bluetooth in API and Basic Search

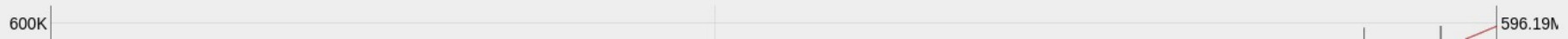
Fri, 22 Mar 2019 20:24:53 GMT

By popular demand, we are now vending bluetooth network data via the API and basic search pages. Please consider the detail results a non-final implementation, as bluetooth devices are



Statistics Over Time

WiFi Networks Over Time



Kismet

Charging 93%

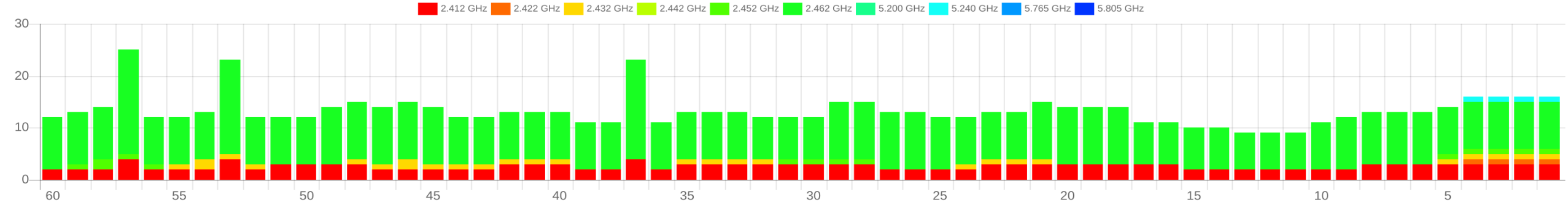
Search:

Name	Type	Phy	Crypto	Signal	Channel	Last Seen	Data	Packets	Clients	BSSID
UESC-N	Wi-Fi AP	IEEE802.11	WPA-CCMP	-35	11	Apr 05 2019 09:09:59	1.43 KB		5	
	Wi-Fi AP	IEEE802.11	WPA-CCMP	-84	11	Apr 05 2019 09:09:32	0 B		0	
	Wi-Fi AP	IEEE802.11	WPA-TKIP	-35	1	Apr 05 2019 09:10:00	0 B		0	
	Wi-Fi AP	IEEE802.11	WPA-CCMP	-64	6	Apr 05 2019 09:09:49	0 B		0	
	Wi-Fi AP	IEEE802.11	WPA-CCMP	-34	11	Apr 05 2019 09:09:59	0 B		0	
	Wi-Fi AP	IEEE802.11	Open	-49	1	Apr 05 2019 09:10:00	0 B		0	
Cat partay	Wi-Fi AP	IEEE802.11	WPA-CCMP	-35	11	Apr 05 2019 09:09:59	0 B		0	
	Wi-Fi AP	IEEE802.11	WPA-CCMP	-74	11	Apr 05 2019 09:09:59	0 B		0	
UESC	Wi-Fi AP	IEEE802.11	WPA-CCMP	-38	11	Apr 05 2019 09:09:59	22.95 KB		4	
UESC-N	Wi-Fi AP	IEEE802.11	WPA-CCMP	-74	11	Apr 05 2019 09:09:59	0 B		0	
Knappster	Wi-Fi AP	IEEE802.11	WPA-CCMP	-81	1	Apr 05 2019 09:09:56	0 B		0	
UESC	Wi-Fi AP	IEEE802.11	WPA-CCMP	-75	11	Apr 05 2019 09:09:59	0 B		0	
	Wi-Fi Bridged	IEEE802.11	n/a	-35	11	Apr 05 2019 09:09:12	740 B		0	
	Wi-Fi Bridged	IEEE802.11	n/a	-38	11	Apr 05 2019 09:09:59	22.96 KB		0	

Showing 1 to 7 of 20 entries

Messages Channels

Current Historical Past Minute Filter Any Frequency




Spooky Wireless:
Hands-on Ghostbusting Labs

% whoami

Product Manager at Aruba Networks
Board Member for RF Hackers Sanctuary
Lead Developer Pentoo Linux
Developer Aircrack-ng
Extra Class Amateur Radio Operator
Wireless Hobbiest

% whoami

Product Manager at Aruba Networks
Board Member for RF Hackers Sanctuary
Lead Developer Pentoo Linux
Developer Aircrack-ng
Extra Class Amateur Radio Operator
Wireless Hobbiest
Not a lawyer
Not your lawyer

Legal disclaimer

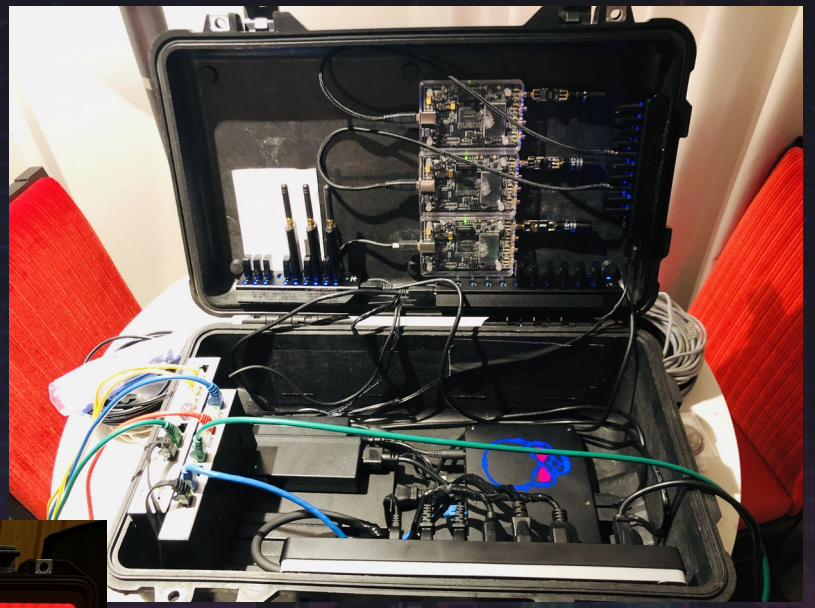
https://www.fcc.gov/consumers/guides/interception-and-divulgence-radio-communications

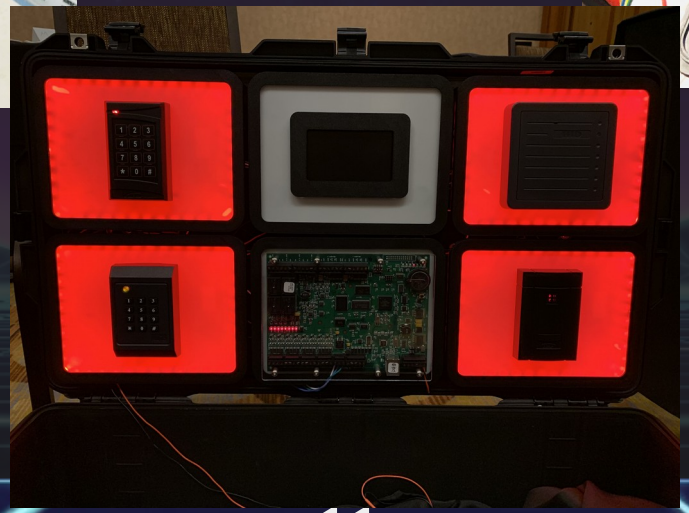
DefCon 27 Wireless Capture The Flag

We were here!

DefCon 27 Wireless Capture The Flag

Now we are here!





Why Linux?

Linux is an Open Source Operating System
Free as in Beer
Free as in Freedom
Supports “most” computers
Supports fun things that we want to do

Why Pentoo Linux?

Longest running “penetration testing” Linux distribution
Lots of documented support
Lots of wireless specific testing
Me
Truthfully, with a livecd it doesn’t matter so long as it works
https://pentoo.ch

Simple Stuff

Read a news article about new Apple issue called apple_bleee
Google search gets us https://github.com/hexway/apple_bleee
Contains a wonderful README, which you can...read.
Follow the directions
Report bugs

Kismet

Kismet is a wireless network and device detector
https://kismetwireless.net/

Kismet works with Wi-Fi interfaces
Bluetooth interfaces
some SDR (software defined radio) hardware like the RTLSDR
and other specialized capture hardware

Well documented at https://kismetwireless.net/docs/
Report bugs

Software Defined Radio

a radio communication system where components that have been traditionally implemented in hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors) are instead implemented by means of software on a personal computer or embedded system.*

Flexible

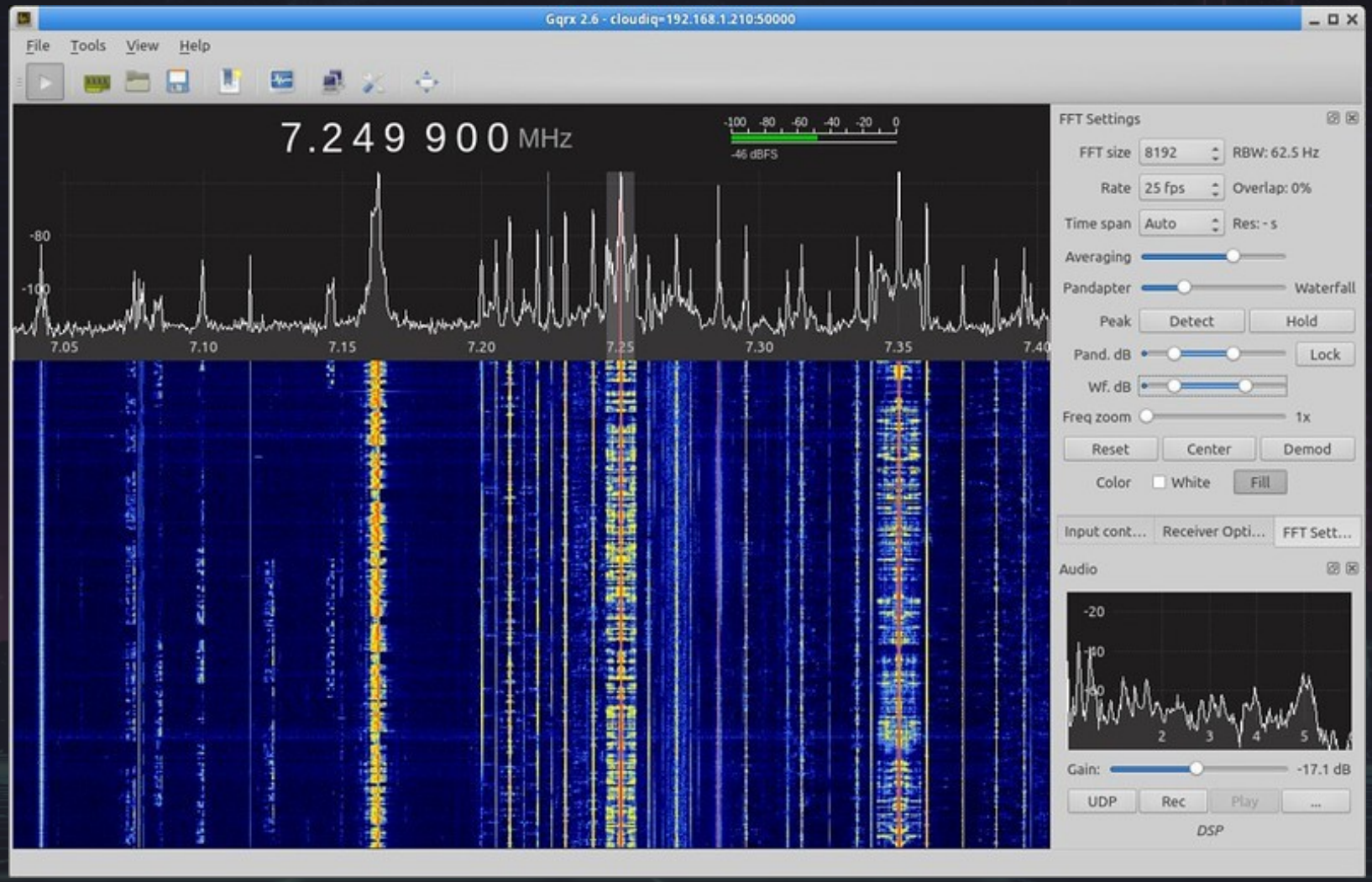
Hardest way to do one thing well

Only way to do everything

*paraphrased from wikipedia sdr entry

GQRX

http://gqrx.dk/



http://gqrx.dk/doc/practical-tricks-and-tips

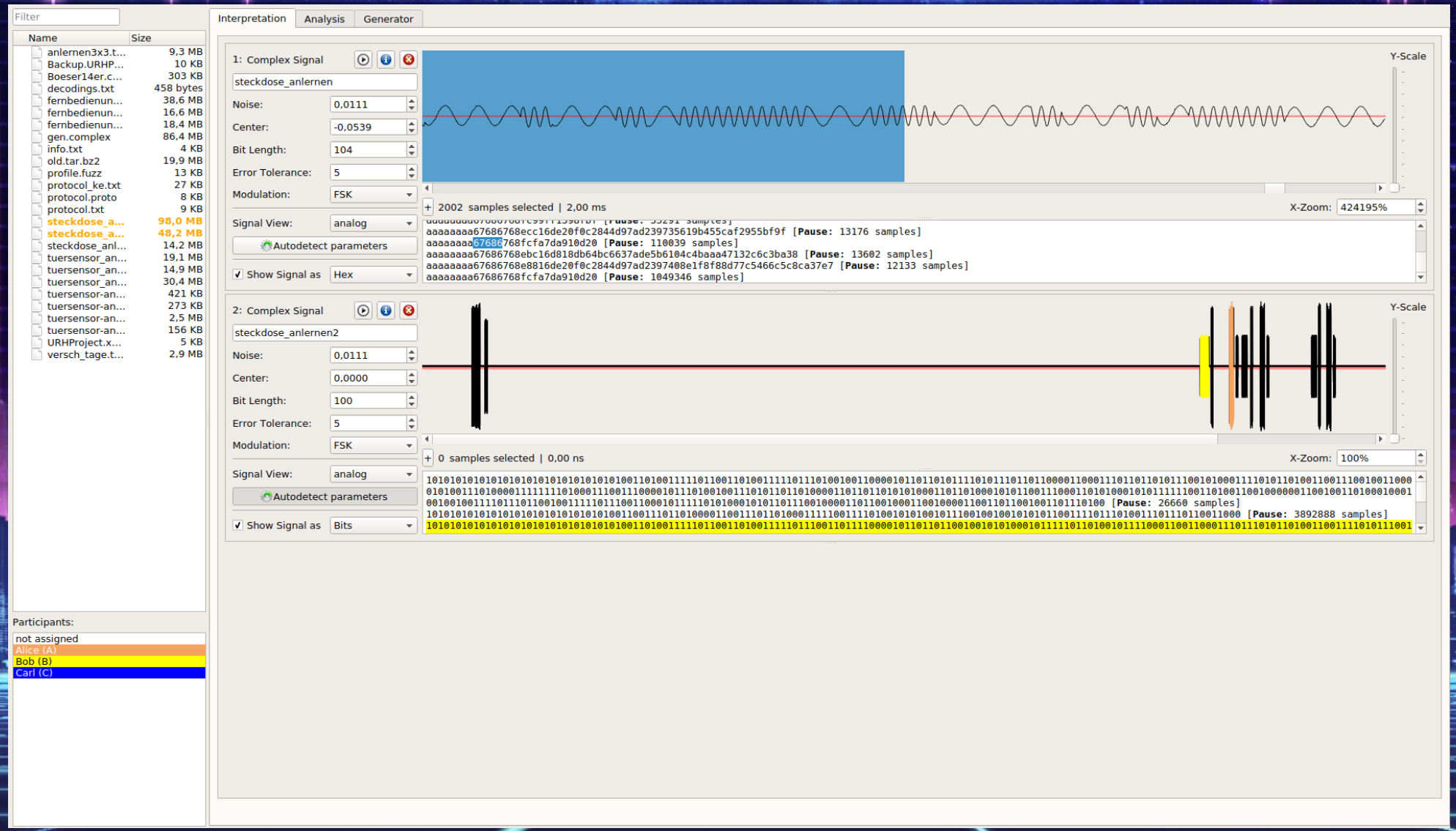
Universal Radio Hacker

https://github.com/jopohl/urh

Reverse Engineering Toolkit

Universal Radio Hacker

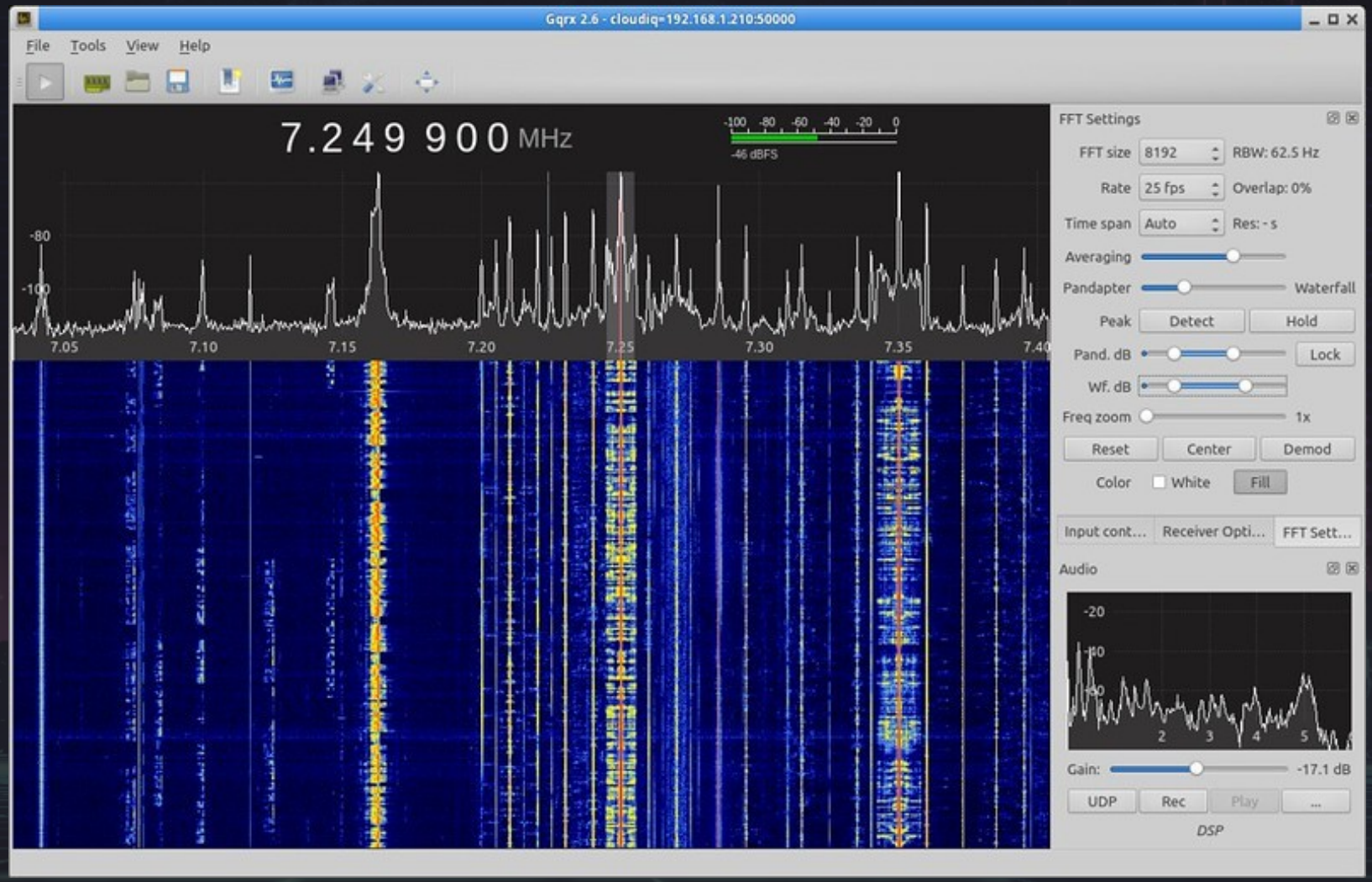
Universal Radio Hacker



Universal Radio Hacker

GQRX

http://gqrx.dk/



http://gqrx.dk/doc/practical-tricks-and-tips


RF WCTF BT SDR RFID WIFI IR


RF
HS


RF WCTF BT SDR RFID WIFI IR


WORLD
WIDE
WARDRIVE
W.W.W.D

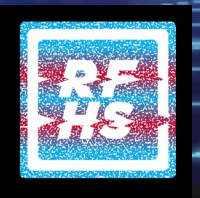

WCTF
RF
BT
WIFI
SDR

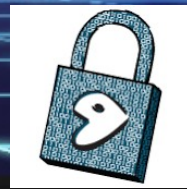

DEF CON 22
WIRELESS VILLAGE 2014


WIRELESS VILLAGE
2016
2017


WIFI
RF
BT
No Cash
Value
WCTF
SDR


Wireless Village 2013
Defcon21


RF
HS



Links

https://wirelessvillage.ninja/
https://wctf.us/