

Get Radio  
Frequency Curious  
...

JAWNCON  
OX2

# Crazy Scary Disclaimer...

- Absolutely none of this information is provided as a “how to” or for you to go FAFO about things.
- For actual legal advice, please consult a real, licensed lawyer (they love that sort of thing).
- Absolutely all of this information is for pure joy of educational awareness of magical radio waves.
- Absolutely none of this information is representative of past or current or even future employers - Any likeness or otherwise similarities are those in which you imagined.

# Who Am I & What do I do

---

- Dustin / BusySignal / KE2EFX
- 20 Years; From : IT/IS , Soda Equipment R&D Deployment  
To : Cyber Security Engineer
  - (Access Management, Crowdstrike, Patch Planning, Deployment)
  - ◆ BS in Electrical Engineering
- Curious in all things Radio Frequency
  - ◆ Winner of 2022/2025 DEFCON 30/33 WWWD. (World Wide WarDrive)  
(WiFi beacon collection, mapping, coverage testing, All The WiFi for WiGLE)
  - ◆ Builder of WiFi, BTLE, ISM Band Monitoring Devices  
(I am absolutely CosPlaying as Signal Intelligence Gathering)
  - ◆ Scanning Systems To Detect (& Locate) Radio Signals
    - SDR KRAKEN / Wielder of Yagi Antennas & Multi-Antenna Arrays
  - ◆ Software Defined Radio P25 Trunk Radio Decoding / Conventional Scanning
    - How this whole thing LITERALLY started

# What In The World Is This All About...

*Be Curious  
Not Judgemental*  
*- Ted Lasso*

# Kismet Wireless... What Most People Use It For.

- WiFi
  - ◆ Scanning / WarDrive / Channel Utilization
  - ◆ Handshake Capture / WiFi pcap capture
  - ◆ Recon / Signal Coverage / Monitoring device
  
- BTLE
  - ◆ Device monitoring / Logging
  - ◆ Counting / Signal Utilization
  - ◆ Recon of devices or users

# What About other Frequencies ???

## → ISM Band

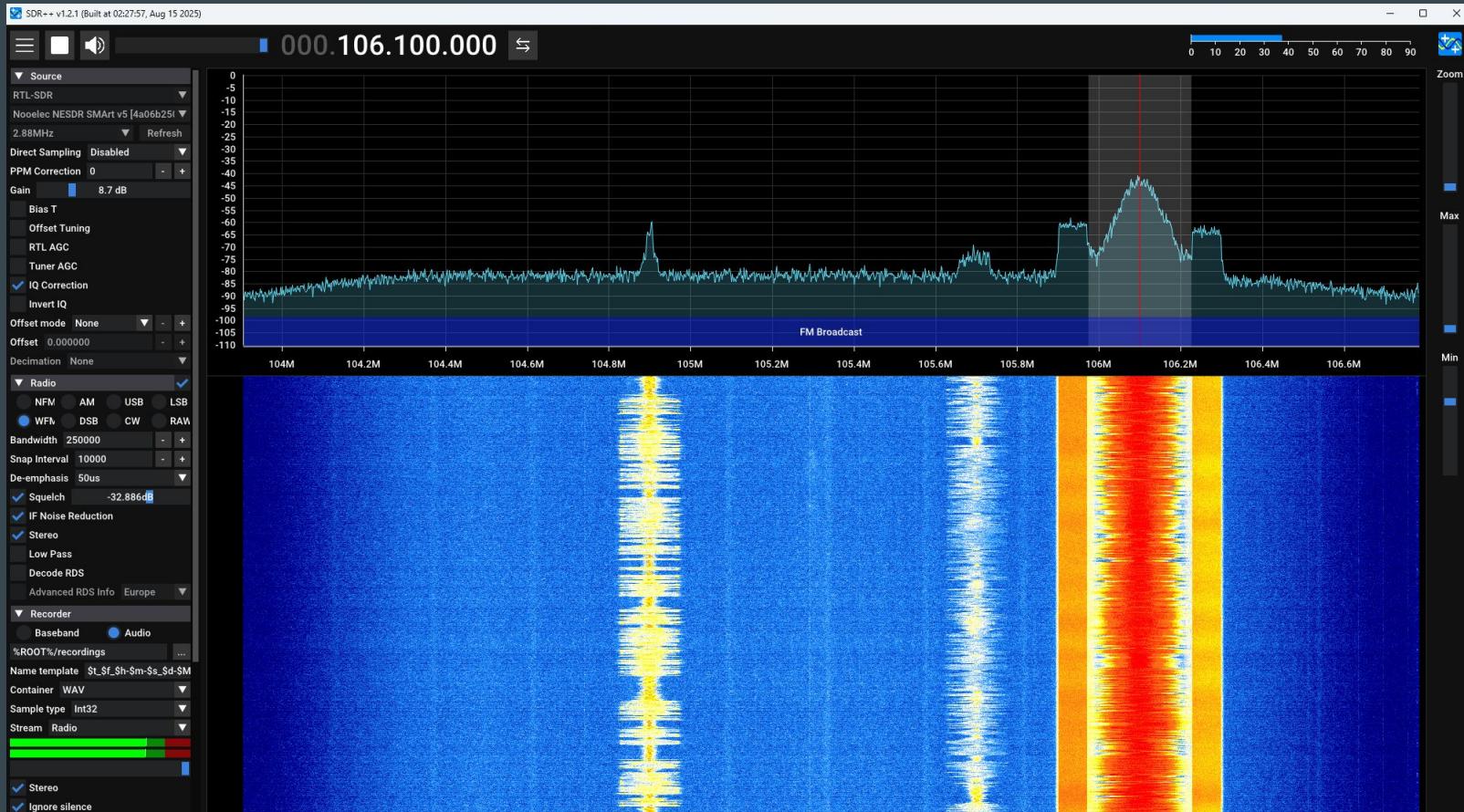
- ◆ Industrial. Scientific. Medical.
- ◆ Devices that generate radio frequency to transmit information other than common communications

## → ISM Characteristics

- ◆ License-Free - Still has tech rules for emissions etc.
- ◆ Zero Protection From Interference / Devices Must Tolerate

# Find The Waves - Capture The Signals - Where Are The Devices

- Software Defined Radios
- Spectrum View
- FM Radio Example



# Frequencies...

## → ISM Frequency Items Decoded By RTL-SDR Software

- ◆ 315 Mhz
  - Motion, Security Sensors
  - TPMS
- ◆ 433 Mhz
  - Weather Stations
  - Remote Sensors; Humidity, Temp, Wind
- ◆ 915 Mhz
  - Security Sensors; Motion / Door Glass Break
  - Utility Sensors; Water, Gas and Electric

# See The Invisible...

- Spectrum Analysis
  - An SDR can be used to visualize the Frequency Spectrum in real time
  - Showing signals broadcast/transmitting
- Some of these examples are ones we already know and love
  - AM/FM
  - Airband between aircraft and airports
  - NOAA Weather Stations / Weather Updates / Emergency Broadcasts
  - Amateur Radio Signals / All of the Ham Operators

# Hardware...

## → **Inexpensive SDR**

- ◆ RTL-SDR Blog - V3 of V4 (100kHz-1.75GHz)  
(V4 Finally has better distro support)
- ◆ Nooelec RTL-SDR v5 SDR (100kHz-1.75GHz)

## → **SBC / Small PC**

- ◆ RasPi 4 or 5; 8GB, MicroSD (SSD Preferred As Server)
- ◆ N150, N300, N350 Intel CPU / 8GB RAM

## → **USB Hub:** If Multiple Devices are to be used at once;

- ◆ StarTech Industrial Hub (Jumper for Host Power Remove)

# Hardware...

## RTL-SDR USB (V3, V4)



# Hardware...

## Nooelec SDR Kit



# More and More Frequencies...

## → ADSB

- ◆ 1090 Mhz
  - Air Traffic Beacons
  - Contains data for GPS / speed / altitude / plane reg
  - Clear Text / Parsed

## → BTLE

- ◆ 2.4 Ghz / Requires Bluetooth receiver

## → WiFi

- ◆ 2.4Ghz - 7Ghz / Requires WiFi Adapter
  - Unrealistic/impossible to do with SDR consumer hardware

# Software: “Software is Like Fashion, It’s Never Finished”

- Linux Distro (I am using Ubuntu, you go do you...)
  - ◆ RTL-SDR Blog - Firmware and Software
- Terminal and CLI
- Have a Horrible Time
- Wait What ?

# SDR: “Like Three The Hard Way” - Beastie Boys

- Command Line Is For The Crazy...
- Scrolling Data
- Data not always parsed or presented easily
- Data is not saved and has to be piped or sent to CSV or syslog to be reviewed / searched

# Examples of Chaos...

→315Mhz

Command Line View:

- ◆ Difficult to review
- ◆ Formatted into a
- ◆ Usable chart
- ◆ Some tracking
- ◆ I totally despise this...

```
adminuser@ksmt-sdr-node-01:~$ rtl_433 -d 3 -f 315M -s 250k -g 35
rtl_433 version 23.11 (2023-11-28) inputs file rtl_tcp RTL-SDR SoapySDR
Detached kernel driver
Found Rafael Micro R820T tuner
SDR Using device 3: NooElec, NESDR SMART v5, SN: 9a42f052, "Generic RTL2832U OEM"
Exact sample rate is: 250000.000414 Hz
[R82XX] PLL not locked!
Allocating 15 zero-copy buffers

time : 2025-10-09 12:19:01
model : Toyota type : TPMS id : d62d01ca
status : 130 pressure_PSI: 31.000 temperature_C: 12.000 Integrity : CRC

time : 2025-10-09 13:12:32
model : Schrader-SMD3MA4 type : TPMS flags : 5 ID : 2DF080
Pressure : 27.8 PSI

time : 2025-10-09 13:12:32
model : Schrader-SMD3MA4 type : TPMS flags : 5 ID : 2DF080
Pressure : 27.8 PSI

time : 2025-10-09 13:12:36
model : Schrader-SMD3MA4 type : TPMS flags : 5 ID : 2DF087
Pressure : 27.4 PSI

time : 2025-10-09 13:16:48
model : Ford type : TPMS id : 36f6d0fa
Pressure : 44.50 PSI Temperature: 20.0 C Moving : 0 Learn : 0 code : b24c06 unknown : 00 unknown_3 : 2
Integrity : CHECKSUM

time : 2025-10-09 13:16:48
model : Ford type : TPMS id : 36f6d0fa
Pressure : 44.50 PSI Temperature: 20.0 C Moving : 0 Learn : 0 code : b24c06 unknown : 00 unknown_3 : 2
Integrity : CHECKSUM

time : 2025-10-09 13:16:49
model : Ford type : TPMS id : 36f6d0fa
Pressure : 44.50 PSI Temperature: 20.0 C Moving : 0 Learn : 0 code : b24c06 unknown : 00 unknown_3 : 2
Integrity : CHECKSUM

time : 2025-10-09 13:20:53
model : Ford type : TPMS id : 36f6d1e5
Pressure : 44.75 PSI Moving : 1 Learn : 0 code : b3d746 unknown : 00 unknown_3 : 2 Integrity : CHECKSUM

time : 2025-10-09 13:20:53
model : Ford type : TPMS id : 36f6d1e5
Pressure : 44.75 PSI Moving : 1 Learn : 0 code : b3d746 unknown : 00 unknown_3 : 2 Integrity : CHECKSUM

time : 2025-10-09 13:20:53
model : Ford type : TPMS id : 36f6d1e5
Pressure : 44.75 PSI Moving : 1 Learn : 0 code : b3d746 unknown : 00 unknown_3 : 2 Integrity : CHECKSUM
```

# Kismet Wireless Enters The Chat...

≡ Kismet - BusySignal HomeLab

Kismet Wireless Enters The Chat...															SDR315		Filter...					
Devices		Alerts		SSIDs		ADSB Live																
	Name	Address	Type	Encryption	First Seen	Last Seen	Packets	Signal	Channel	Manufacturer	Clients	Uptime	QBSS Channel Usage	Seen by #								
?	ToXXXXXXXXXXXXXG7	02:00:00:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:39:38	Oct 09 2025 01:46:33	-	n/a	315.008 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXX15	03:FC:FC:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:39:38	Oct 08 2025 19:12:30	-	n/a	315.008 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXX82	02:40:40:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:39:40	Oct 09 2025 01:38:14	-	n/a	315.008 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXX5a	02:2C:2C:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:39:55	Oct 08 2025 21:17:01	-	n/a	315.007 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXX77	02:45:45:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:40:04	Oct 09 2025 01:01:02	-	n/a	315.001 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXXba	02:56:56:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:40:10	Oct 09 2025 01:46:31	-	n/a	315.009 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXX16	02:29:29:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:40:14	Oct 09 2025 01:46:03	-	n/a	315.009 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXX6d	02:64:64:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:40:16	Oct 08 2025 18:02:47	-	n/a	315.006 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXXb1	02:55:55:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:40:25	Oct 09 2025 01:46:39	-	n/a	315.006 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXX18	03:FF:FF:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:40:35	Oct 09 2025 01:46:21	-	n/a	315.014 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXXc3	02:35:35:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:40:39	Oct 08 2025 20:06:38	-	n/a	315.019 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXXc6	02:10:10:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:40:51	Oct 08 2025 16:05:03	-	n/a	315.030 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXX4b	02:2E:2E:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:41:05	Oct 08 2025 18:43:23	-	n/a	315.004 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXX4f	02:0C:0C:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:42:36	Oct 08 2025 18:12:34	-	n/a	315.015 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXXfa	02:C6:C6:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:43:29	Oct 08 2025 17:41:21	-	n/a	315.014 MHz	RF Sensor	0	n/a	n/a	1								
?	FoXXXXXXXXXXXXX54	02:01:01:XX:XX:XX	Sensor	n/a	Oct 06 2025 14:05:24	Oct 06 2025 14:05:24	-	n/a	315.036 MHz	RF Sensor	0	n/a	n/a	1								
?	ScXXXXXXXXXXXXXXAA	03:63:63:XX:XX:XX	Sensor	n/a	Oct 06 2025 14:12:45	Oct 06 2025 14:12:45	-	n/a	314.916 MHz	RF Sensor	0	n/a	n/a	1								
?	AbXXXXXXXXXXXXXX...A	02:33:33:XX:XX:XX	Sensor	n/a	Oct 06 2025 14:27:30	Oct 06 2025 14:27:30	-	n/a	315.039 MHz	RF Sensor	0	n/a	n/a	1								
?	FoXXXXXXXXXXXXX8d	03:FF:FF:XX:XX:XX	Sensor	n/a	Oct 06 2025 14:50:23	Oct 06 2025 14:50:23	-	n/a	315.032 MHz	RF Sensor	0	n/a	n/a	1								
?	AbXXXXXXXXXXXXXX...B	02:05:05:XX:XX:XX	Sensor	n/a	Oct 06 2025 15:03:10	Oct 06 2025 15:03:10	-	n/a	315.039 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXXBe	02:9F:9F:XX:XX:XX	Sensor	n/a	Oct 06 2025 15:08:27	Oct 06 2025 15:08:27	-	n/a	314.997 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXXb7	02:D2:D2:XX:XX:XX	Sensor	n/a	Oct 06 2025 15:15:53	Oct 06 2025 15:15:53	-	n/a	315.004 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXX29	02:0A:0A:XX:XX:XX	Sensor	n/a	Oct 06 2025 15:31:53	Oct 09 2025 01:46:01	-	n/a	315.007 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXXcd	02:96:96:XX:XX:XX	Sensor	n/a	Oct 06 2025 15:31:56	Oct 09 2025 01:47:10	-	n/a	315.009 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXXa5	02:62:62:XX:XX:XX	Sensor	n/a	Oct 06 2025 15:31:56	Oct 09 2025 01:47:12	-	n/a	315.014 MHz	RF Sensor	0	n/a	n/a	1								
?	ScXXXXXXXXXXXXXXD0	03:52:52:XX:XX:XX	Sensor	n/a	Oct 06 2025 15:32:25	Oct 08 2025 17:04:43	-	n/a	314.920 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXXe7	02:73:73:XX:XX:XX	Sensor	n/a	Oct 06 2025 15:32:39	Oct 08 2025 15:25:34	-	n/a	315.010 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXXff	02:97:97:XX:XX:XX	Sensor	n/a	Oct 06 2025 15:32:56	Oct 08 2025 17:36:45	-	n/a	315.004 MHz	RF Sensor	0	n/a	n/a	1								
?	ToXXXXXXXXXXXXX16	02:69:69:XX:XX:XX	Sensor	n/a	Oct 06 2025 15:32:56	Oct 08 2025 19:06:02	-	n/a	315.014 MHz	RF Sensor	0	n/a	n/a	1								

# Kismet Wireless Data Review...

## → Data Review - TPMS Example

DEVICE: ToXXXXXXXXXXXX67

### Device Info

### RF Sensor

Model	ToXXXXXXXXXXXX67
Device ID	daXXXX67
SNR	22
Noise	-23

### Thermometer

Temperature	55.40° F
M:	.....
H:	.....
D:	.....

### Tire pressure

Pressure	28.75 PSI
----------	-----------

### Packet Graphs

#### Packet Rates

Packets per second (last minute) (Tx/Rx)

Packets per minute (last hour) (Tx/Rx)

Packets per hour (last day) (Tx/Rx)

#### Data

Data per second (last minute)

Data per minute (last hour)

Data per hour (last day)

DEVICE: ToXXXXXXXXXXXX67

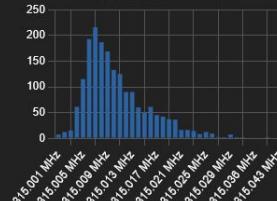
### Device Info

Name	ToXXXXXXXXXXXX67
Notes	Empty
MAC Address	02:00:XX:XX:XX
Manufacturer	RF Sensor
Type	Sensor
First Seen	Mon Oct 06 2025 13:39:38 GMT-0400 (Eastern Daylight Time)
Last Seen	Thu Oct 09 2025 01:48:10 GMT-0400 (Eastern Daylight Time)

### Frequencies

Channel	None Advertised
Main Frequency	315.009 MHz

#### Packet frequency distribution



#### Packets

#### Packet Types

LLC/Management

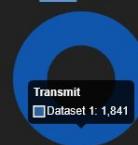
Data



#### Direction

Transmit

Receive



Total Packets	1841
Rx Packets	0
Tx Packets	1841
LLC/Management	0
Error/Invalid	0
Data	1841
Encrypted	0
Filtered	0
Data Transferred	0 B

# Examples of Chaos...

```
adminuser@ksmt-sdr-node-01:~$ rtl_433 -d 3 -f 433M -s 250k -g 35
rtl_433 version 23.11 (2023-11-28) inputs file rtl_tcp RTL-SDR SoapySDR
Detached kernel driver
Found Rafael Micro R820T tuner
SDR Using device 3: Nooelec, NESDR SMART v5, SN: 9a42f052, "Generic RTL2832U OEM"
Exact sample rate is: 250000.000414 Hz
[R82XX] PLL not locked!
Allocating 15 zero-copy buffers
```

```
time      : 2025-10-09 13:44:52
model     : Acurite-6045M id      : 129
channel   : C      Battery : 1      temperature: 81.1 F
active_mode: 0      rfi_detect: 0      data_exception: 0

time      : 2025-10-09 13:44:52
model     : Acurite-6045M id      : 129
channel   : C      Battery : 1      temperature: 81.1 F
active_mode: 0      rfi_detect: 0      data_exception: 0

time      : 2025-10-09 13:44:52
model     : Acurite-6045M id      : 129
channel   : C      Battery : 1      temperature: 81.1 F
active_mode: 0      rfi_detect: 0      data_exception: 0

time      : 2025-10-09 13:44:53
model     : Acurite-Tower id      : 10247
channel   : B      Battery : 1      Temperature: 16.0 C

time      : 2025-10-09 13:44:53
model     : Acurite-Tower id      : 10247
channel   : B      Battery : 1      Temperature: 16.0 C

time      : 2025-10-09 13:44:53
model     : Acurite-Tower id      : 10247
channel   : B      Battery : 1      Temperature: 16.0 C
```

→433Mhz

## Command Line View:

◆ Difficult to review

◆ Formatted into a

◆ Usable chart

◆ Some tracking.

◆ I totally despise this...

# Kismet Wireless Enters The Chat...

= Kismet - BusySignal HomeLab

Kismet Wireless Enters The Chat...															SDR433		Filter...	
Devices	Alerts	SSIDs	ADSB Live	Name	Address	Type	Encryption	First Seen	Last Seen	Packets	Signal	Channel	Manufacturer	Clients	Uptime	QBSS Channel Usage	Seen by #	
②	AeXXXXXXXXXXXXXX29	02:81:16:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:39:40	Oct 09 2025 00:24:04	-----	n/a	C	RF Sensor	0	n/a	n/a	n/a	1			
②	AeXXXXXXXXXXXXXX47	2A:07:0B:XX:XX:XX	Sensor	n/a	Oct 06 2025 13:44:03	Oct 08 2025 20:03:56	-----	n/a	B	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX71	5E:E7:5F:XX:XX:XX	Sensor	n/a	Oct 06 2025 14:17:24	Oct 08 2025 18:56:54	-----	n/a	432.928 MHz	RF Sensor	0	n/a	n/a	1				
②	HTXXXXXXXXXXXXXX41	EE:F5:D3:XX:XX:XX	Sensor	n/a	Oct 06 2025 14:18:29	Oct 06 2025 14:18:29	-----	n/a	432.975 MHz	RF Sensor	0	n/a	n/a	1				
②	OrXXXXXXXXXXXXXX22	02:16:65:XX:XX:XX	Sensor	n/a	Oct 06 2025 14:20:04	Oct 08 2025 18:33:06	-----	n/a	432.948 MHz	RF Sensor	0	n/a	n/a	1				
②	MaxXXXXXXXXX56	03:00:42:XX:XX:XX	Sensor	n/a	Oct 06 2025 14:44:31	Oct 09 2025 00:16:13	-----	n/a	432.981 MHz	RF Sensor	0	n/a	n/a	2				
②	DSXXXXXXXXXXXXXX57	0A:15:5F:XX:XX:XX	Sensor	n/a	Oct 06 2025 16:36:30	Oct 08 2025 13:54:35	-----	n/a	432.924 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX80	0A:30:5F:XX:XX:XX	Sensor	n/a	Oct 06 2025 18:02:01	Oct 08 2025 11:04:18	-----	n/a	432.929 MHz	RF Sensor	0	n/a	n/a	1				
②	OIXXXXXXXXXXXXXX35	FF:FF:78:XX:XX:XX	Sensor	n/a	Oct 06 2025 23:23:41	Oct 06 2025 23:23:41	-----	n/a	432.983 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX03	4E:5F:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 10:07:30	Oct 08 2025 10:34:40	-----	n/a	432.930 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX63	36:BF:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 10:14:20	Oct 08 2025 05:07:20	-----	n/a	432.932 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX45	4E:89:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 10:20:51	Oct 08 2025 10:32:59	-----	n/a	432.928 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX31	06:13:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 10:30:18	Oct 08 2025 10:47:45	-----	n/a	432.925 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX21	0A:55:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 10:54:40	Oct 08 2025 10:43:52	-----	n/a	432.926 MHz	RF Sensor	0	n/a	n/a	1				
②	LaxXXXXXXXXXXXXXX19	02:DB:11:XX:XX:XX	Sensor	n/a	Oct 07 2025 11:03:51	Oct 08 2025 19:00:28	-----	n/a	432.995 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX85	0E:0D:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 11:14:48	Oct 08 2025 05:40:29	-----	n/a	432.926 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX82	4F:52:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 11:34:25	Oct 08 2025 10:04:58	-----	n/a	432.925 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX10	42:F6:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 11:50:19	Oct 08 2025 10:49:42	-----	n/a	432.927 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX85	3A:F1:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 11:50:34	Oct 08 2025 11:12:08	-----	n/a	432.930 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX02	F6:1A:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 12:00:36	Oct 08 2025 10:31:12	-----	n/a	432.930 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX58	F6:52:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 13:14:04	Oct 08 2025 05:13:07	-----	n/a	432.925 MHz	RF Sensor	0	n/a	n/a	1				
②	AcXXXXXXXXXXXXXX55	02:FF:84:XX:XX:XX	Sensor	n/a	Oct 07 2025 17:29:48	Oct 07 2025 17:29:48	-----	n/a	433.002 MHz	RF Sensor	0	n/a	n/a	1				
②	ReXXXXXXXXXXXXXX77	03:76:76:XX:XX:XX	Sensor	n/a	Oct 07 2025 17:59:08	Oct 07 2025 17:59:08	-----	n/a	432.974 MHz	RF Sensor	0	n/a	n/a	1				
②	ScoXXXXXXXXXXXXXX21	03:4C:4C:XX:XX:XX	Sensor	n/a	Oct 07 2025 18:44:09	Oct 07 2025 18:44:17	-----	n/a	432.931 MHz	RF Sensor	0	n/a	n/a	1				
②	OIXXXXXXXXXXXXXX55	FE:1F:78:XX:XX:XX	Sensor	n/a	Oct 07 2025 19:04:53	Oct 07 2025 19:04:53	-----	n/a	432.971 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX46	BE:4E:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 19:33:15	Oct 08 2025 13:41:32	-----	n/a	432.926 MHz	RF Sensor	0	n/a	n/a	1				
②	DSXXXXXXXXXXXXXX90	BE:7A:5F:XX:XX:XX	Sensor	n/a	Oct 07 2025 20:14:05	Oct 08 2025 11:44:04	-----	n/a	432.929 MHz	RF Sensor	0	n/a	n/a	1				
②	ScoXXXXXXXXXXXXXF4	03:9C:9C:XX:XX:XX	Sensor	n/a	Oct 07 2025 20:21:35	Oct 08 2025 02:08:29	-----	n/a	432.940 MHz	RF Sensor	0	n/a	n/a	1				
②	HTXXXXXXXXXXXXXX91	F7:FF:D3:XX:XX:XX	Sensor	n/a	Oct 07 2025 21:11:25	Oct 07 2025 21:11:25	-----	n/a	432.983 MHz	RF Sensor	0	n/a	n/a	1				

Showing rows 1 - 30 of 55

First Prev 1 2 Next Last

# Kismet Wireless Data Review...

## → Data Review - Temperature / Sensors

### RF Sensor

Model: AcXXXXXXXXXXXXXX29

SNR: 22

RSSI: -8

Noise: -30

Sub-Channel: C

Battery: 1

### Thermometer

Temperature: 82.60° F

M:

H:

D:

### Moisture

Moisture (%): 33%

M:

H:

D:

### Lightning Sensor

Strike Count: 61

ΔM:

ΔH:

ΔD:

Storm Active: Active

RFI: 1

Storm distance: 7

### Packet Graphs

#### Packet Rates

##### Packets per second (last minute) (Tx/Rx)

##### Packets per minute (last hour) (Tx/Rx)

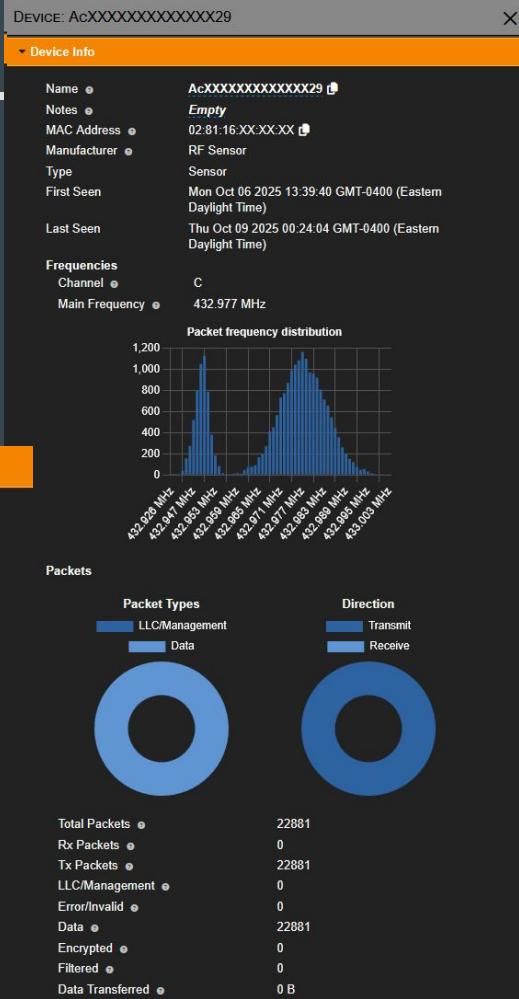
##### Packets per hour (last day) (Tx/Rx)

#### Data

##### Data per second (last minute)

##### Data per minute (last hour)

##### Data per hour (last day)



# Examples of Chaos...

## → ADSB Command Line View:

- ◆ Difficult to review
- ◆ Challenging to ID specific Information

- ◆ I totally despise this...

```
Using device 3: Generic RTL2832U OEM
Detached kernel driver
Found Rafael Micro R820T tuner
Tuner gain set to automatic.
Tuned to 1090000000 Hz.
Exact sample rate is: 2000000.052982 Hz
Sampling at 2000000 S/s.
Allocating 12 zero-copy buffers
*83fb6612e5a1d0f91e8fc4f72948;
DF=16 CA=3
ICAO Address=fb6612
PI=0xf72948
Type Code=28 S.Type/Ant.=5
-----
*9da462f04eb4a83e41573980ba02;
DF=19 CA=5
ICAO Address=a462f0
PI=0x89ba02
Type Code=9 S.Type/Ant.=6
-----
*0d5e121a7b51a0cd15aca9ed4c44;
DF=26 CA=0
ICAO Address=5e121a
PI=0xedc44
Type Code=15 S.Type/Ant.=3
-----
*8de48fd559d306cea42d2eb8b56d;
DF=17 CA=5
ICAO Address=e48fd5
PI=0xb8b56d
Type Code=11 S.Type/Ant.=1
-----
*de82beb07d63565b7d354d7cc222;
DF=27 CA=6
ICAO Address=82beb0
PI=0x7cc222
Type Code=15 S.Type/Ant.=5
-----
*becbb2bc5fb2a32562447bad2c57;
DF=23 CA=6
ICAO Address=cbb2bc
PI=0xad2c57
Type Code=11 S.Type/Ant.=7
-----
*8de48fd558db03c3f9c5ce5f6c52;
DF=17 CA=5
ICAO Address=e48fd5
PI=0x5f6c52
Type Code=11 S.Type/Ant.=0
-----
*a25481cbbed0b71fa06e999e7d30;
DF=20 CA=2
```

```
adminuser@ksmt-sdr-node-01:~$ rtl_adsb -d 3
Found 6 device(s):
 0: Realtek, RTL2838UHIDIR, SN: bc2591b1
 1: Realtek, RTL2838UHIDIR, SN: ea5ed751
 2: Realtek, RTL2838UHIDIR, SN: bf25b732
 3: Realtek, RTL2838UHIDIR, SN: 6c95083c
 4: Realtek, RTL2838UHIDIR, SN: 073d38f6
 5: RTLSDRBlog, Blog V4, SN: 7d172272

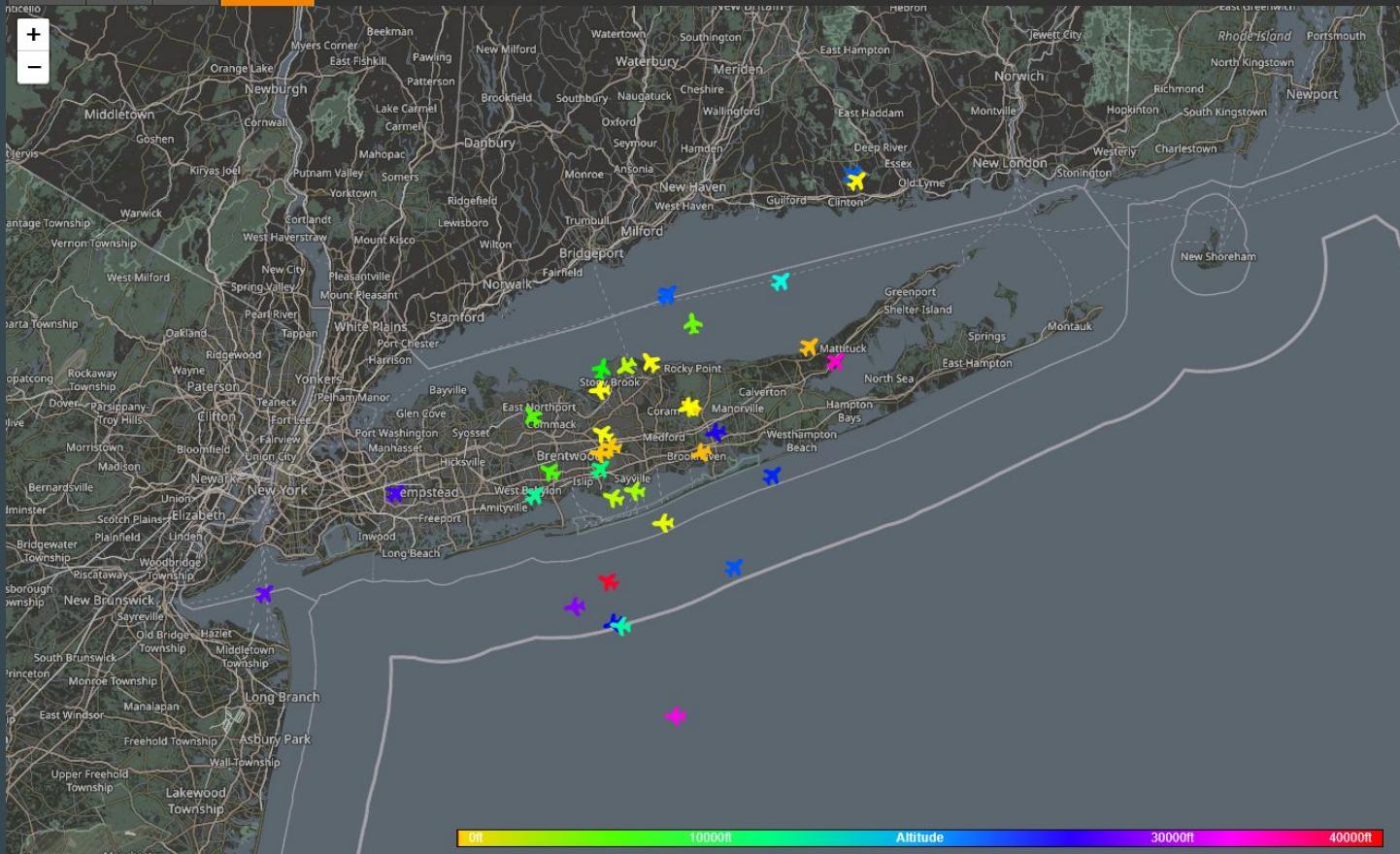
Using device 3: Generic RTL2832U OEM
Detached kernel driver
Found Rafael Micro R820T tuner
Tuner gain set to automatic.
Tuned to 1090000000 Hz.
Exact sample rate is: 2000000.052982 Hz
Sampling at 2000000 S/s.
Allocating 12 zero-copy buffers
*8da6717a591b43272fbf38142a56;
*8dab44dd5965037de7d804df33c4;
*ae512cd02513b778e0e5bd7d721f;
*9d26752ad8d534ca04f3c98d7597;
*8da65fb59910e2e187c35a25216;
*8da3962d5889634235a6be4b4193;
*8dab44dd9911b50c380420997cf4;
*ed74bf610b734b8c6ea9a31ff83a;
*8dabe1015817332e0fc8b864f435;
*ccb528be89164056c88c82a89702;
*8da2034758790326f79783557731;
*8dbc6665fc338002004abc21b5b1;
*8d394a05598d598f184426c925a2;
*8da8a309585898ed2da3ae191dc4a;
*c6d0917015a6b838e9b65049af736;
*8d3c66c5ea4e3866ff5c082bd71a;
*e5811b497dec8b0820da08465a382;
*8da4be4e116060000a9005c65f0;
*9d4b599c58b98bb60f80cc5cc65;
*8da4ea84592d8f4ecfbc2936dc052;
*8ca36799992d25a4a0513a6b5002;
*8da65fb5f9122026005abc0c987a;
*9b18ea164880d46ce1b4f497a50e;
*8dal12e0585186e56c260fdb25f8;
*8dc266c59915a190f8083da7ab24;
*8dab44dd9911bd0c302420f7defc;
*8da23f0e590d96d5c832d2604b7c;
*993a0eed5fffffff3df1b1e6f9;
*8da128be99144986d80c02b89702;
*8278d992e99d457dde23225ca02;
*8170c7cc3a92c10bed5e401cb4a6;
*d08ae78da3962dea2d085ccb5c08;
*8da12e09911082518441c7d6f9a;
*8da4ea85ea4a5964a835cf67354b2;
*8da4a2f6584166d1f032ca376125;
```

# Kismet Wireless Enters The Chat...

≡ Kismet - BusySignal HomeLab

Unknown Unknown ⚡ 🔔 🌙 🛡

Devices Alerts SSIDs **ADSB Live**



Leaflet | OpenStreetMap

# Kismet Wireless Data Review...

DEVICE: ADXXXXXXD5



▶ Device Info

▼ ADSB (SDR)

Plane ICAO	e48fd5
Callsign ⓘ	PRCGI
Flightaware	<a href="#">Track PRCGI on FlightAware</a>
Registration ID ⓘ	Unknown
Aircraft Classification ⓘ	Unknown Aircraft
Model ⓘ	Unknown
Type ⓘ	Unknown
Aircraft Operator ⓘ	Unknown

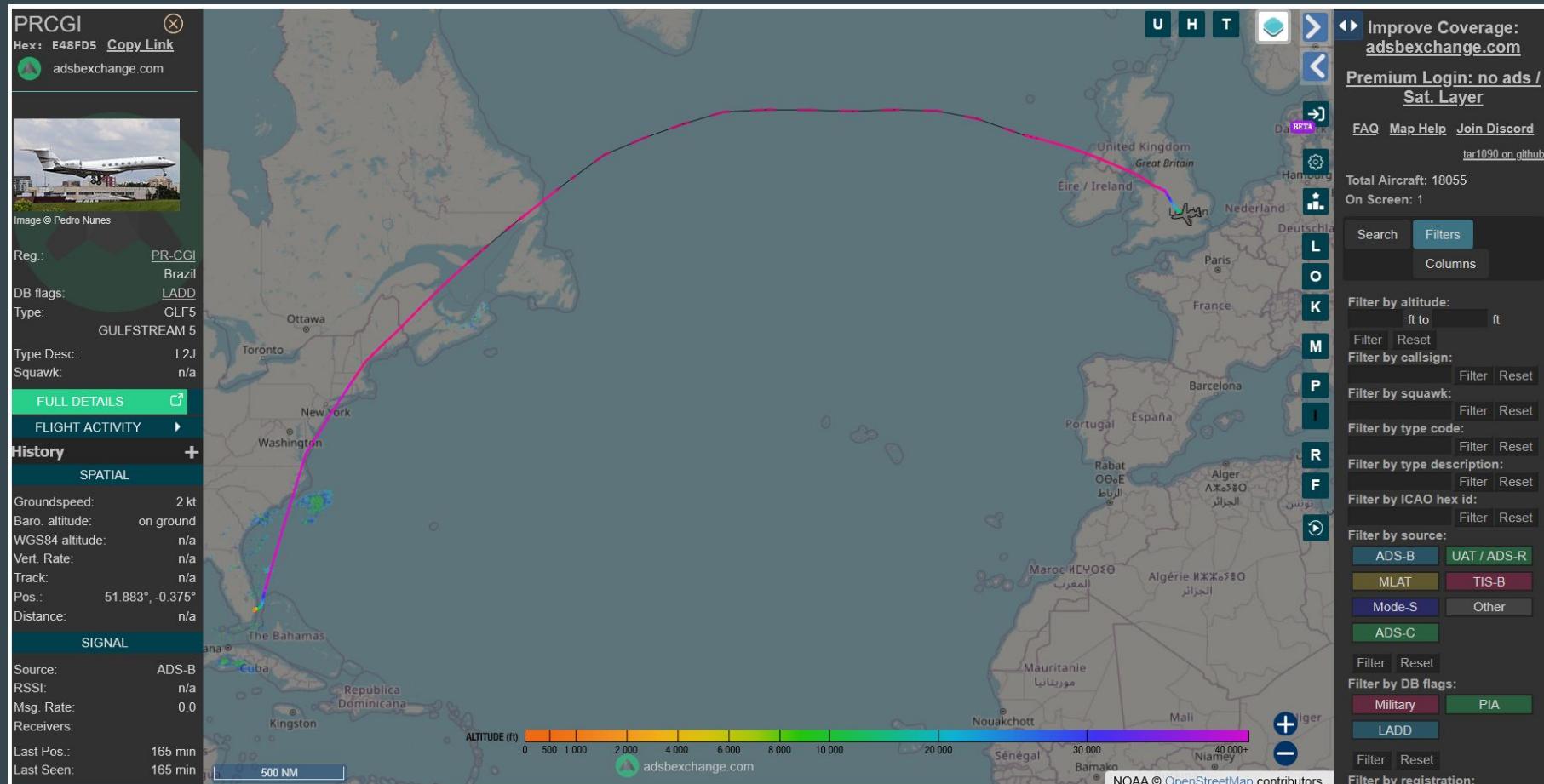
## PR-CGI - Unknown Owner (Brazil)

This aircraft ([PR-CGI](#)) is not available for public tracking per request from the owner/operator.

[That's my airplane! How do I track my airplane on FlightAware?](#)

FlightAware can provide aircraft owner/operators with secure access to their own flight data. [Contact FlightAware for help.](#)

# Kismet Wireless Data Review...Find What You Seek



# Kismet Wireless Enters The Chat... BTLE

≡ Kismet - BusySignal HomeLab

ticc2540-3-12-BT01																	Filter...
Devices	Alerts	SSIDs	ADSB Live	Name	Address	Type	Encryption	First Seen	Last Seen	Packets	Signal	Channel	Manufacturer	Clients	Uptime	QBSS Channel Usage	Seen by #
⌘	MeXXXXXXXXXXXX43			D2:1E:04:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 14:16:03	Oct 09 2025 10:59:46	..... .....	-63	39	Randomized	0	n/a	n/a	1
⌘	OrXXXXXXXXXXXXXXWD			C3:90:29:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 17:12:33	Oct 09 2025 10:59:46	..... .....	-63	38	Randomized	0	n/a	n/a	1
⌘	F3XXXXXXXXXXXXXX			F3:0F:A4:XX:XX:XX	BTLE ...	n/a		Oct 09 2025 10:07:22	Oct 09 2025 10:59:46	..... .....	-55	38	Randomized	0	n/a	n/a	1
⌘	XXXX			CB:7F:D1:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:35	Oct 09 2025 10:59:46	..... .....	-46	38	Randomized	0	n/a	n/a	1
⌘	MeXXXXXXXXXXXX28			98:A3:16:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:35	Oct 09 2025 10:59:46	..... .....	-58	38	Espressif Inc.	0	n/a	n/a	1
⌘	ReXXXXXXXXX43			04:E3:E5:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 09 2025 10:59:46	.....  .....	-50	37	Silicon Laborato...	0	n/a	n/a	1
⌘	5BXXXXXXXXXXXXXX			5B:4C:CE:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:35	Oct 06 2025 13:49:05	.....	-57	38	Randomized	0	n/a	n/a	1
⌘	D5XXXXXXXXXXXXXX			D5:F1:CB:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:35	Oct 06 2025 20:46:24	.....	-45	38	Randomized	0	n/a	n/a	1
⌘	MeXXXXXXXXXXXX25			E7:80:C6:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:35	Oct 09 2025 10:59:46	..... .....	-43	39	Randomized	0	n/a	n/a	1
⌘	EFXXXXXXXXXXXXXX			EF:50:D6:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:35	Oct 06 2025 13:45:36	.....	-41	38	Randomized	0	n/a	n/a	1
⌘	3BXXXXXXXXXXXXXX			3B:78:EB:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:35	Oct 06 2025 13:46:54	.....	-54	37	Randomized	0	n/a	n/a	1
⌘	80XXXXXXXXXXXXXX			80:47:86:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 09 2025 10:59:46	..... .....	-62	38	Samsung Electr...	0	n/a	n/a	1
⌘	MeXXXXXXXXXXXX40			D9:84:1B:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 09 2025 10:59:46	.....	-39	39	Randomized	0	n/a	n/a	1
⌘	MeXXXXXXXXXXXXc0			98:A3:16:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 09 2025 10:59:46	.....	-47	37	Espressif Inc.	0	n/a	n/a	1
⌘	36XXXXXXXXXXXXXX			36:27:68:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 06 2025 13:43:24	.....	-58	39	Randomized	0	n/a	n/a	1
⌘	0CXXXXXXXXXXXXXX			0C:9F:C3:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 06 2025 13:45:02	.....	-55	39	Randomized	0	n/a	n/a	1
⌘	10XXXXXXXXXXXXXX			10:2B:41:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 09 2025 10:59:46	.....	-61	38	Samsung Electr...	0	n/a	n/a	1
⌘	ArXXXXXXXXXC4			E4:CF:47:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 09 2025 10:59:46	.....	-53	39	Randomized	0	n/a	n/a	1
⌘	09XXXXXXXXXXXXXX			09:FD:73:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 06 2025 13:48:05	.....	-59	39	Randomized	0	n/a	n/a	1
⌘	FIXXXXXXXXXXXX0I			80:E1:26:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 09 2025 10:59:46	.....	-49	37	Unknown	0	n/a	n/a	1
⌘	E8XXXXXXXXXXXXXX			E8:75:6E:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 06 2025 13:45:06	.....	-62	37	Randomized	0	n/a	n/a	1
⌘	F6XXXXXXXXXXXXXX			F6:AA:1A:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 06 2025 13:45:02	.....	-45	39	Randomized	0	n/a	n/a	1
⌘	58XXXXXXXXXXXXXX			58:D5:80:XX:XX:XX	BTLE ...	n/a		Oct 06 2025 13:39:40	Oct 06 2025 13:43:34	.....	-57	39	Randomized	0	n/a	n/a	1

Showing rows 1 - 30 of 9856

First Prev 1 2 3 4 5 Next Last

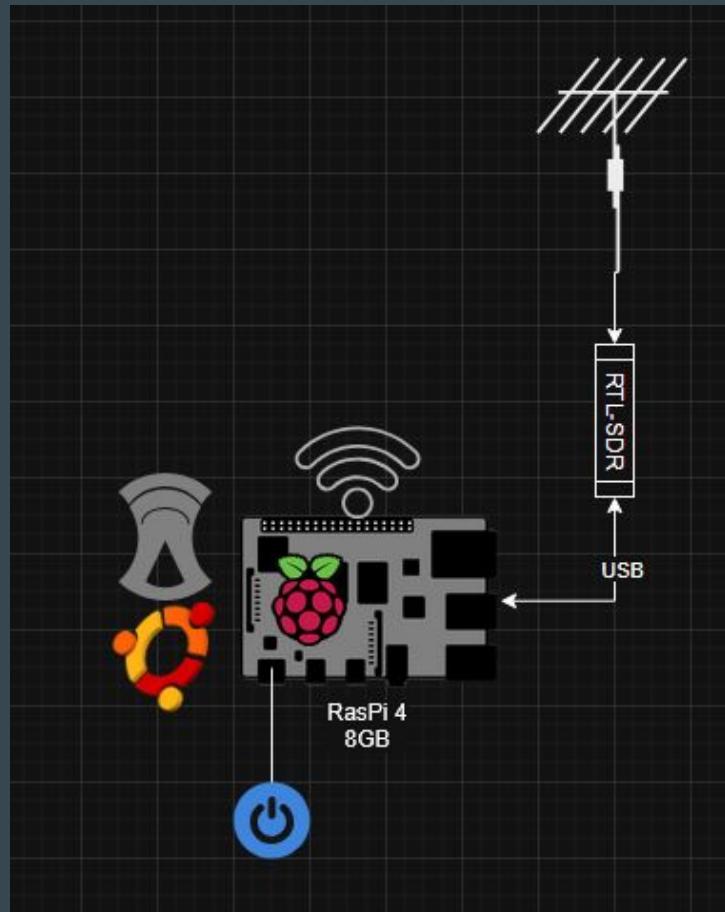
# Architecture... Small, Deployable, Easy Start

→ Simple Recon Device

→ Kismet Packages Pre Built  
(No Compiling Required)

→ Web Server Locally / Kismet Wireless

→ Remote via Browser over Network  
Or Console Access / Screen



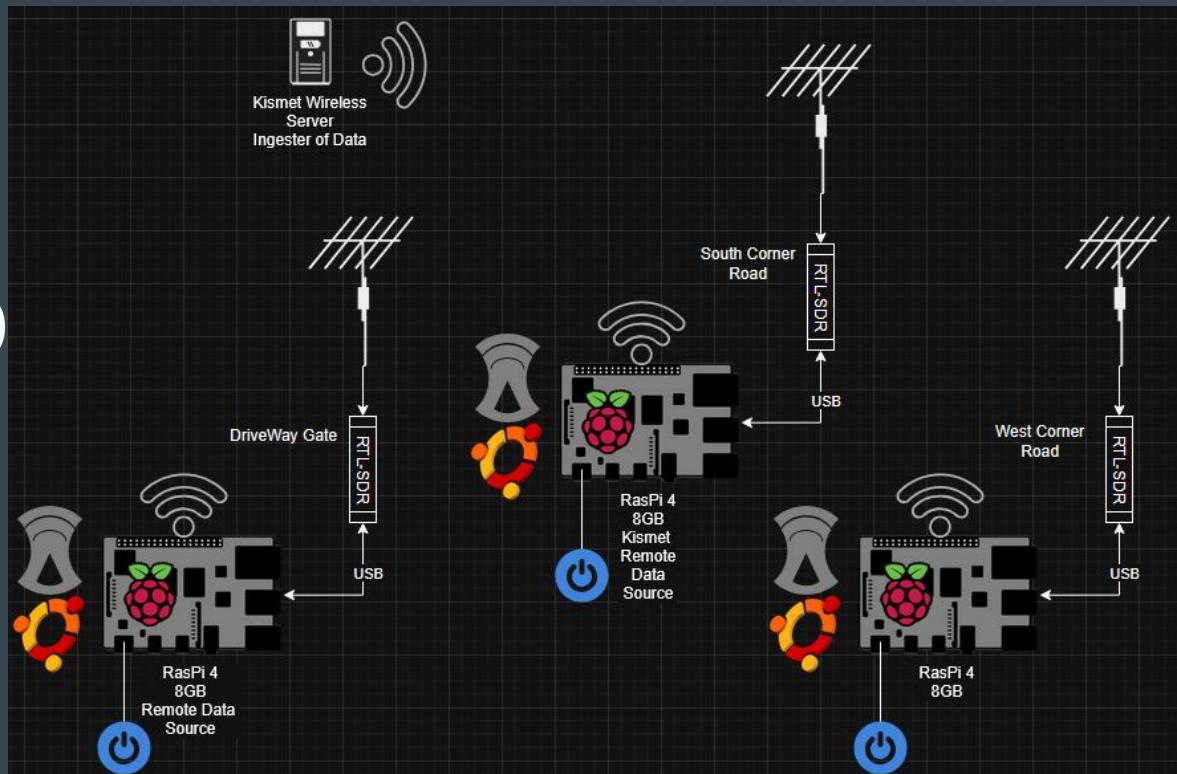
# Architecture... Small, Deployable, Remote Sensors

→ Simple Recon Devices

→ Kismet Packages  
Pre Built for RasPi  
(No Compiling Required)

→ Each RasPi as a  
Remote Data Source

→ Kismet Wireless Server  
Centralized



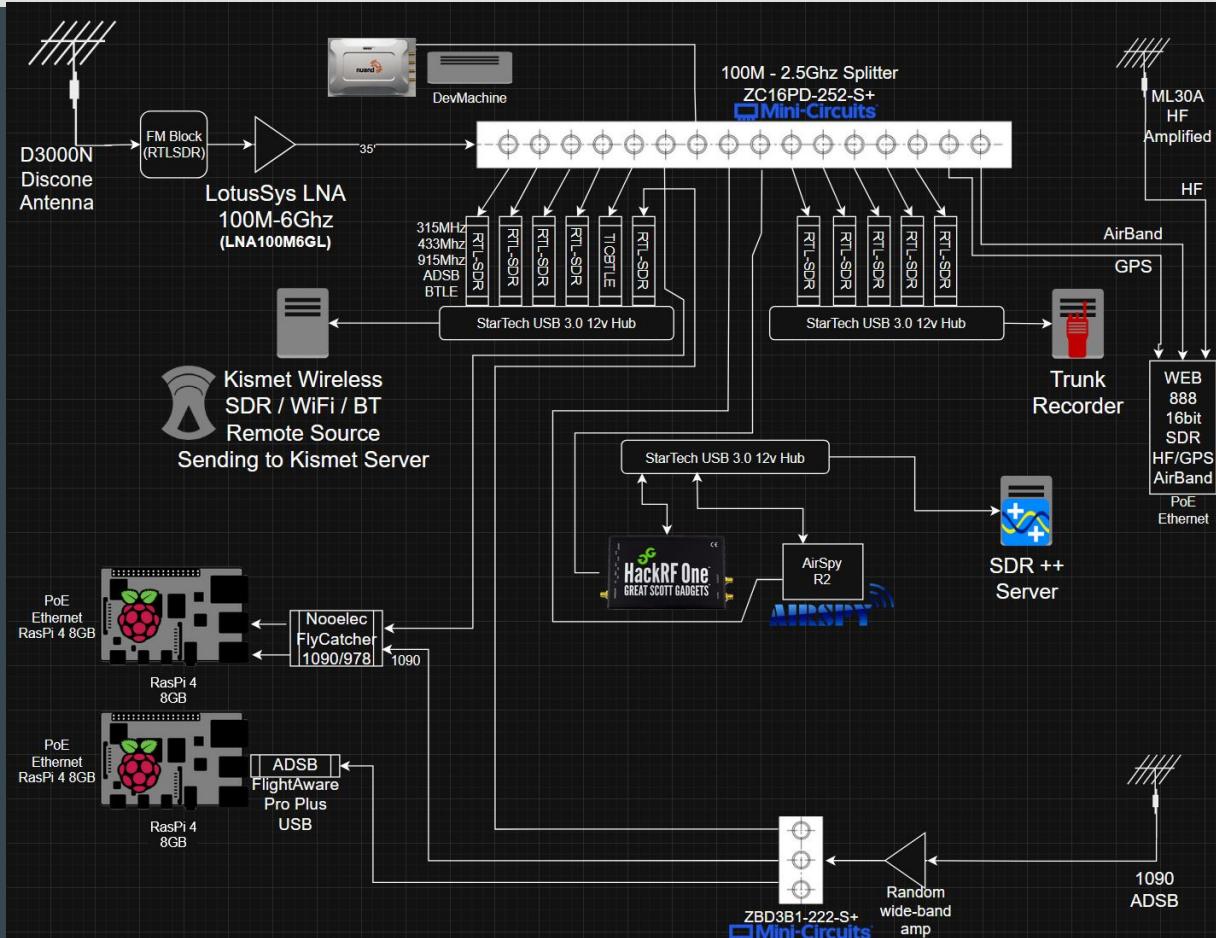
# If You Build It. You Can Collect It All.

- 315 Mhz
- 433 Mhz
- 915 Mhz
- 978 ADSB
- 1090 ADSB
- BTLE
- WiFi (remote)



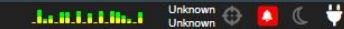
# If You Build It. You Can Collect It All.

## → Logical Layout



# Have you a moment to talk about Kismet Wireless...

≡ Kismet - BusySignal HomeLab



All devices																Filter...	
Devices	Alerts	SSIDs	ADSB Live	Name	Address	Type	Encryption	First Seen	Last Seen	Packets	Signal	Channel	Manufacturer	Clients	Uptime	QBSS Channel Usage	Seen by #
*	XXXX			CB:7F:D1:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 13:39:35	Oct 09 2025 17:04:45	1.....1..1	-58	37	Randomized	0	n/a	n/a	1
*	MeXXXXXXXXXXXX25			E7:80:C6:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 13:39:35	Oct 09 2025 17:04:45	.....1..1..	-43	38	Randomized	0	n/a	n/a	1
*	MeXXXXXXXXXXXX28			98:A3:16:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 13:39:35	Oct 09 2025 17:04:45	.....1..1..	-57	37	Espressif Inc.	0	n/a	n/a	1
*	80XXXXXXXXXXXXXX			80:47:86:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 13:39:40	Oct 09 2025 17:04:45	.....1..1..	-64	39	Samsung Electr...	0	n/a	n/a	1
*	MeXXXXXXXXXXXX40			D9:84:1B:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 13:39:40	Oct 09 2025 17:04:45	1.....1..1..	-55	37	Randomized	0	n/a	n/a	1
*	MeXXXXXXXXXXXXc0			98:A3:16:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 13:39:40	Oct 09 2025 17:04:45	1.....1..1..	-47	37	Espressif Inc.	0	n/a	n/a	1
*	10XXXXXXXXXXXXXX			10:2B:41:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 13:39:40	Oct 09 2025 17:04:45	.....1..1..1..	-63	38	Samsung Electr...	0	n/a	n/a	1
*	ReXXXXXXXXX43			04:E3:E5:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 13:39:40	Oct 09 2025 17:04:45	1.....1..1..	-53	39	Silicon Laborato...	0	n/a	n/a	1
*	ArXXXXXXXXXC4			E4:CF:47:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 13:39:40	Oct 09 2025 17:04:45	1.....1..1..	-52	39	Randomized	0	n/a	n/a	1
*	FIXXXXXXXXXXXX01			80:E1:26:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 13:39:40	Oct 09 2025 17:04:45	.....1..1..	-57	37	Unknown	0	n/a	n/a	1
*	MeXXXXXXXXXXXXe1			E9:49:9A:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 13:39:40	Oct 09 2025 17:04:45	1.....1..1..	-37	39	Randomized	0	n/a	n/a	1
*	XXXXXX			66:23:30:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 13:39:40	Oct 09 2025 17:04:45	.....1..1..	-61	39	Randomized	0	n/a	n/a	1
*	MeXXXXXXXXXXXX7d			C7:29:4D:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 06 2025 18:05:16	Oct 09 2025 17:04:45	1.....1..1..	-63	39	Randomized	0	n/a	n/a	1
*	XXXXXX			EA:E3:11:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 08 2025 18:16:23	Oct 09 2025 17:04:45	.....1..1..	-48	39	Randomized	0	n/a	n/a	1
*	DAXXXXXXXXXXXXXX			DA:E7:6E:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 09 2025 04:00:04	Oct 09 2025 17:04:45	1.....1..1..	-49	38	Randomized	0	n/a	n/a	1
*	F1XXXXXXXXXXXXXX			F1:BB:59:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 09 2025 15:30:04	Oct 09 2025 17:04:45	.....1..1..	-55	38	Randomized	0	n/a	n/a	1
*	DDXXXXXXXXXXXXXX			DD:D8:3B:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 09 2025 16:00:00	Oct 09 2025 17:04:45	.....1..1..	-53	37	Randomized	0	n/a	n/a	1
*	5FXXXXXXXXXXXXXX			5F:CB:C5:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 09 2025 16:46:24	Oct 09 2025 17:04:45	1.....1..1..	-39	39	Randomized	0	n/a	n/a	1
*	5CXXXXXXXXXXXXXX			5C:E2:D0:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 09 2025 16:48:51	Oct 09 2025 17:04:45	1.....1..1..	-49	39	Randomized	0	n/a	n/a	1
*	67XXXXXXXXXXXXXX			67:16:18:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 09 2025 16:51:13	Oct 09 2025 17:04:45	1.....1..1..	-39	39	Randomized	0	n/a	n/a	1
*	5DXXXXXXXXXXXXXX			5D:AA:7A:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 09 2025 16:51:39	Oct 09 2025 17:04:45	.....1..1..	-50	39	Randomized	0	n/a	n/a	1
*	7CXXXXXXXXXXXXXX			7C:6B:A6:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 09 2025 16:52:35	Oct 09 2025 17:04:45	1.....1..1..	-56	39	Randomized	0	n/a	n/a	1
*	44XXXXXXXXXXXXXX			44:DE:D4:XX:XX:XX	BTLE ...	BTLE ...	n/a	Oct 09 2025 16:52:35	Oct 09 2025 17:04:45	.....1..1..	-55	38	Randomized	0	n/a	n/a	1

Showing rows 1 - 30 of 14326

First Prev | 1 2 3 4 5 Next Last

# Thank You & Credits & Love

→ Acknowledging the shoulders of the giants before us that all of us are standing upon:

- ◆ Kismet Wireless - Dragorn - [kismetwireless.net](http://kismetwireless.net)
  - An amazingly awesome discord of help and support.
- ◆ satanklawz - The 2016 and then the 2025 ShmooCon Presentations continue to drive inspiration, curiosity and my builds
- ◆ Radio Frequency Hackers Sanctuary - Zero\_Chaos and the admins
  - Great community to share knowledge and help educate:  
[rfhackers.com](http://rfhackers.com)

→ Thank you:

