

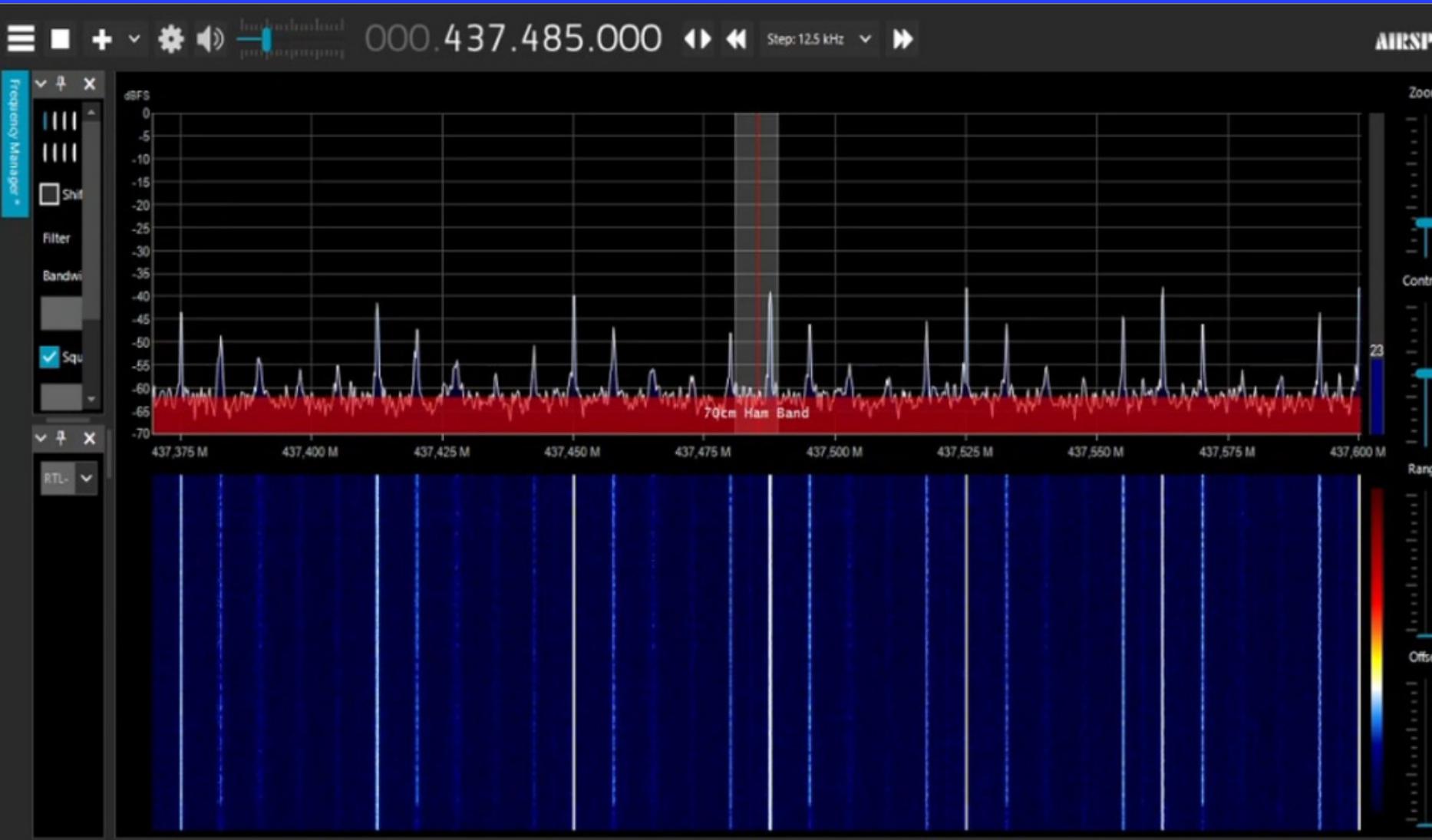


UNIVERSIDAD DISTRITAL  
FRANCISCO JOSÉ DE CALDAS  
Acreditación Institucional de Alta Calidad



# Radios definidas por Software

HISTORIA Y DEMOSTRACIÓN DE SU USO



# ¿QUE PUEDO APRENDER?

Generalidades de las Radios definidas por Software

¿Qué son las radios definidas por software? ¿En qué se diferencia con una radio normal? Y su historia

Decodificación de señales satelitales

Uso de la biblioteca gr\_satellites de Daniel Estévez para la recepción y decodificación de satélites en GNU Radio

Hacking y otros usos

Como aprovechan "vulnerabilidades" en las telecomunicaciones

# ¿QUÉ ES UNA RADIO?

## Resumen

Son dispositivos cuyo propósito es transmitir un mensaje de un transmisor a un receptor.

Para ello tiene que realizar las siguientes operaciones (BMayes, 2019):

1. Conversión del mensaje en una función de onda
2. Transmisión de la función de onda por un medio (usualmente el aire)
3. Captura de la señal
4. Reconstrucción del mensaje original con cierto grado de fiabilidad

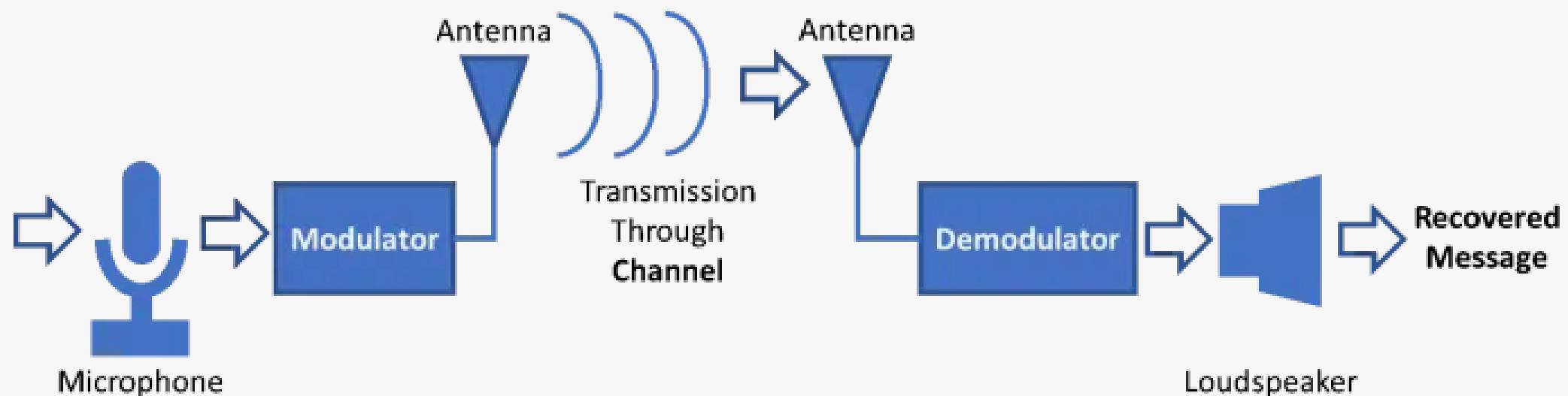


Imagen recuperada de: <https://bit.ly/3b4S9g9>

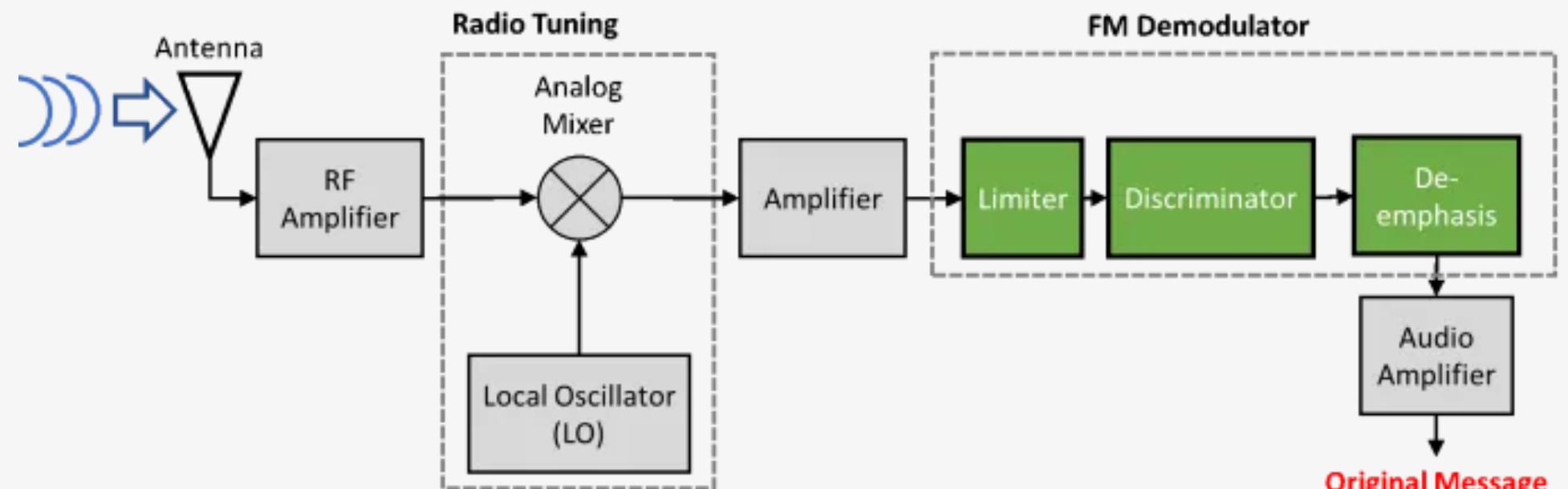


Imagen recuperada de: <https://bit.ly/3b4S9g9>

# RADIOES DEFINIDAS POR SOFTWARE

¿Qué son?

"Fuerón descritas por Joe Mitola como un tipo de radios reprogramables" (Mendieta, Cano & Ferro, 2017)

\$ 35 USD



\$ 300 USD

Imagen recuperada de: <https://bit.ly/3b7wvrA>

\$ 4500 USD

Ventajas

- Precio
- Crecimiento en complejidad de software, pero no de hardware
- Un mismo dispositivo puede tener múltiples aplicaciones
- Pueden hackear muchas cosas

Desventajas

- Pueden meterte en problemas
- Las radios que pueden transmitir siguen teniendo un costo considerable
- Pueden hackear muchas cosas

Imagen recuperada de: <https://bit.ly/3uAf8Yd>



Imagen recuperada de: <https://bit.ly/3enXO2A>

# HISTORIA

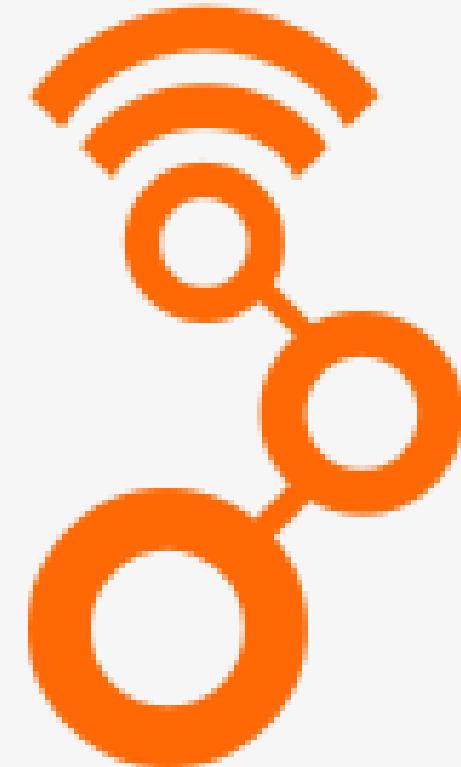
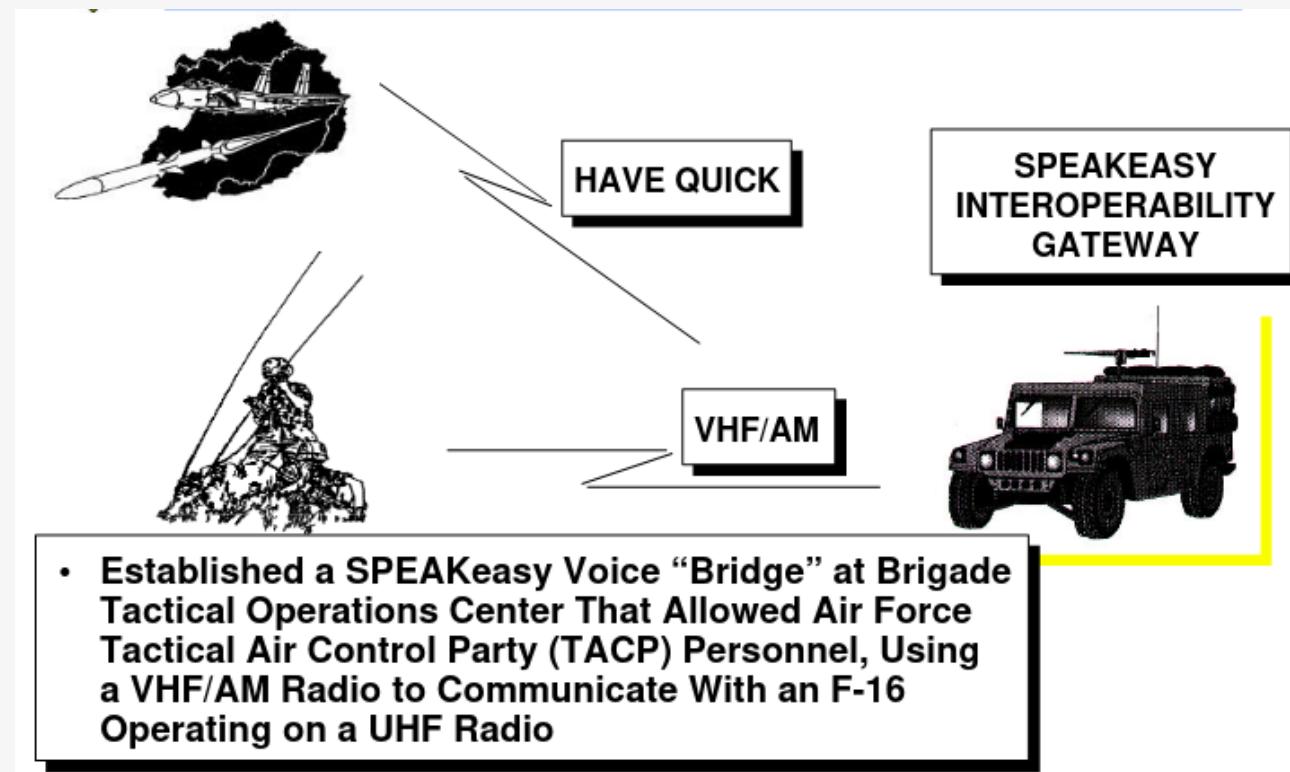


Imagen recuperada de:  
[https://www.its.blrdoc.gov/media/30649/bons\\_s.pdf](https://www.its.blrdoc.gov/media/30649/bons_s.pdf)

## SPEAKEasy 1

(1991) Primera aplicación militar, su objetivo era poder comunicar diferentes protocolos entre 2 MHz y 2 GHz. (Nutaq, 2021)

Imagen recuperada de: <https://tinyurl.com/sfthnyap>

## GNU Radio

(2001) Creado por Eric Blossom, GNU Radio es un marco de trabajo de código abierto para desarrollar aplicaciones SDR usando un PC. (Nutaq, 2021)



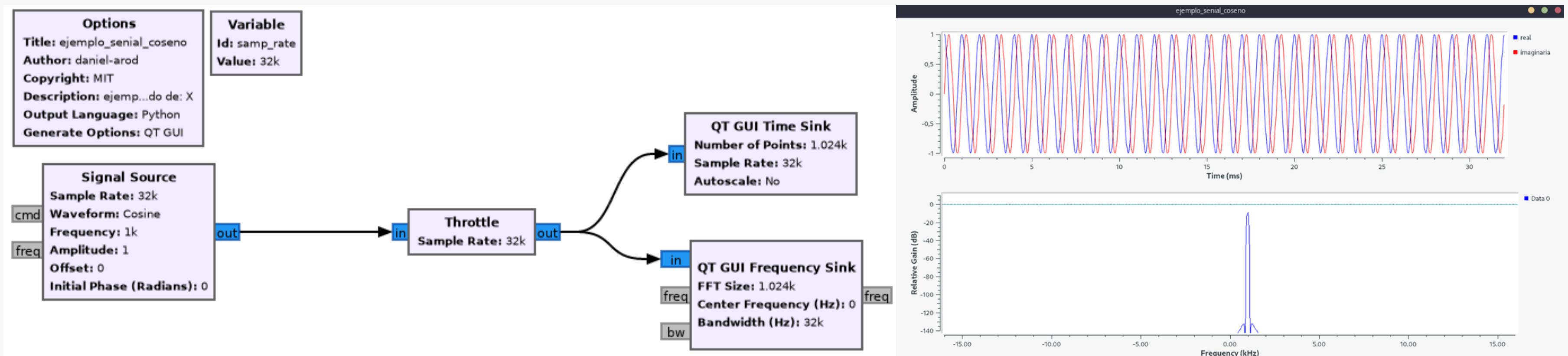
Imagen recuperada de: <https://tinyurl.com/2rn47ept>

## Hack dongles DVB-TV tuner

Antti Palosaari, Eric Fry y Osmocom hackean chipset chip RTL2832U presente en los dongles para obtener una señal IQ y de esta forma nace SDR-RTL (RTL-SDR.com, 2021)

# ¿COMO USAR GNU RADIO?

Es un "lenguaje de programación" por bloques. Se arrastran los diferentes bloques para armar una aplicación que toma (o genera) una entrada y la transforma en una salida



Ejemplo adaptado de Cardona, I (2020).

# DEMOSTRACIÓN DE SU USO

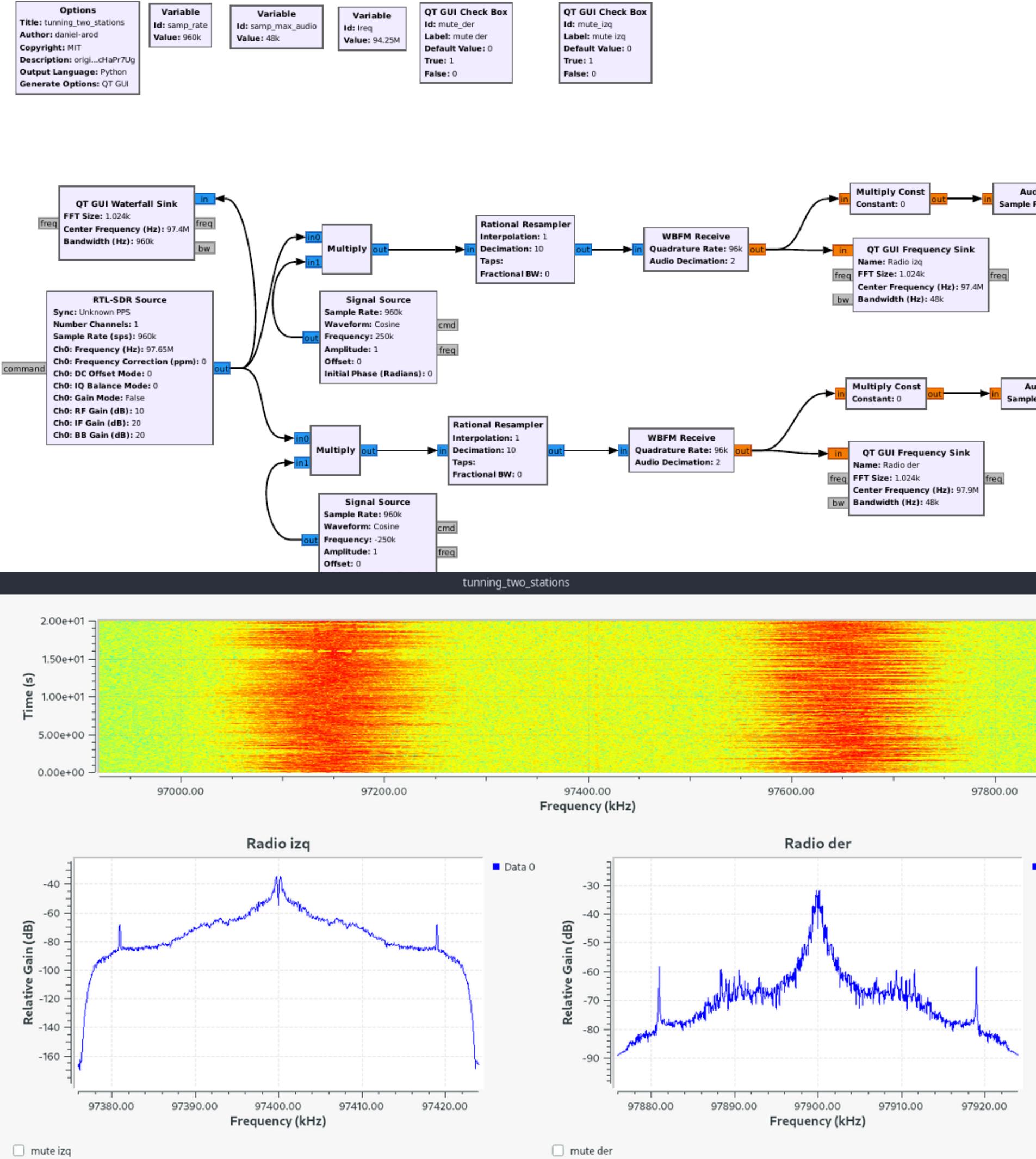
## ADVERTENCIA: ¡Mantente en lo Legal!

Las Radios Definidas por Software han permitido que muchas personas tengan el equipo necesario para decodificar o transmitir señales, sin embargo es **altamente recomendable** verificar la regulación de cada nación antes de intentarlo.

Por regla general se puede decir que está bien oír (o sintonizar) pero no transmitir sin una licencia de radioaficionado y mucho menos decodificar señales de las bandas reservadas



# SINTONIZACIÓN SIMULTÁNEA DE RADIOS

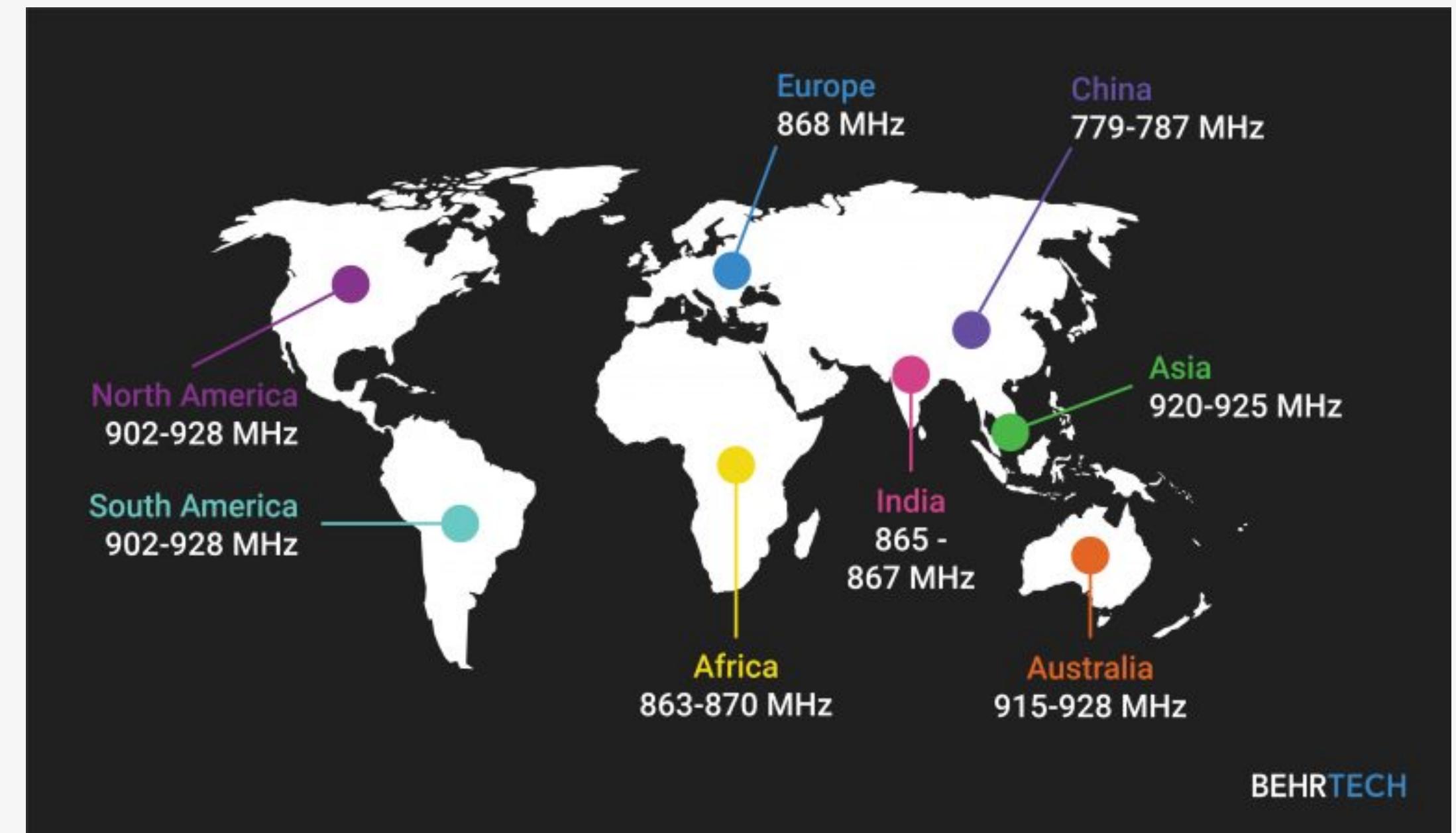


Ejemplo adaptado de Cardona, I (2020).

# ¿QUE ES LA BANDA ISM?

También conocida como ICM (Industrial, Científica y Médica), es la banda libre en la que no requiere pagar y tampoco requiere de licencia para ser usada. (BehrTech Blog, 2020)

Existe regulación en cuanto a la potencia de transmisión y el tiempo que dura transmitiendo



# DECODIFICACIÓN DE CUBESATS

## 1. ¿Qué es un CubeSat?

Es un satélite con forma de cubo, usualmente su tamaño es de 10\*10\*10 cm. Este tipo de satélites suele ser construido por Universidades de todo el mundo y están dentro de la categoría del espacio 2.0 (Younis, 2019).

## 2. ¿Qué información transmite un CubeSat?

Depende de la misión, la mayoría de información que puede ser extraída fácilmente de un satélite es acerca de su estado y el valor de algunos sensores, sin embargo algunos podrían transmitir imágenes en varias bandas del espectro electromagnético

## 3. ¿En qué frecuencia trasmitten?

Una amplia variedad de satélites CubeSat transmiten cerca a 433 MHz, esto es porque hace parte de la banda ISM en la que pueden transmitir sin pagar una licencia adicional.



Imagen recuperada de: <https://bit.ly/3fkSzAf>

# **GR\_SATELLITES**

Es un repositorio creado por Daniel Estévez el cual añade nuevos bloques a GNU Radio que permiten decodificar señales de satélites en tiempo real o que han sido grabadas (Estévez, 2021).

## **CARACTERÍSTICAS**

Licencia

**GPL 3.0**

Sistema Operativo soportado

- Arch
- Debian
- Mac

Interfaz de usuario

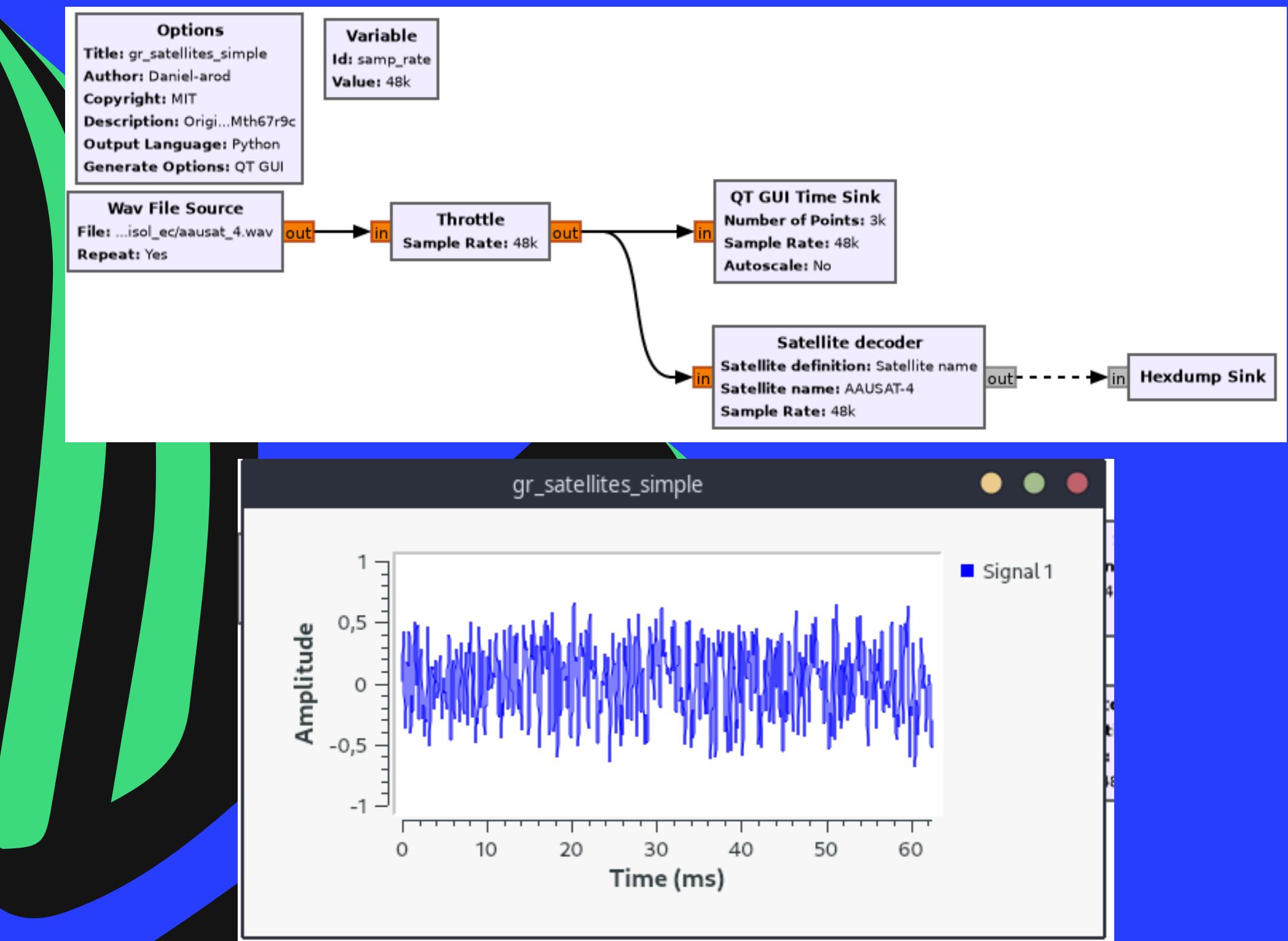
**CLI y GUI**

# BLOQUES GR\_SATELLITES

Para más información sobre los bloques de gr\_satellites pueden consultar la documentación en: <https://gr-satellites.readthedocs.io/en/latest/>

- Wav File Source: Lee un audio en formato WAV
- Throttle: Limita la velocidad en la que las muestras (samples) son leídas desde el archivo
- QT GUI Frecuency Sink: Deja ver la señal en el plano de la frecuencia
- QT GUI Time Sink: Deja ver la señal en el plano del tiempo
- Satellite Decoder: Decodifica un audio de un satélite que cuente soporte en la documentación
- Hexdump sink: imprime los PDUs en hex en forma de una salida estándar
- Float to Complex: convierte una señal de tipo Float en una de tipo complejo
- Frecuency Xlating FIR Filter: mueve la frecuencia a banda base, luego filtra el ruido con el número de taps
- Low Pass Filter: filtra los valores menores al valor establecido
- Quadrature demod: filtro para señal FM
- Rational resampler: modifica el número de muestras de entrada
- Wav File Sink: guarda audio en un archivo
- CCSDS Reed-solomon Deframer: Parte la señal en pedazos y decodifica

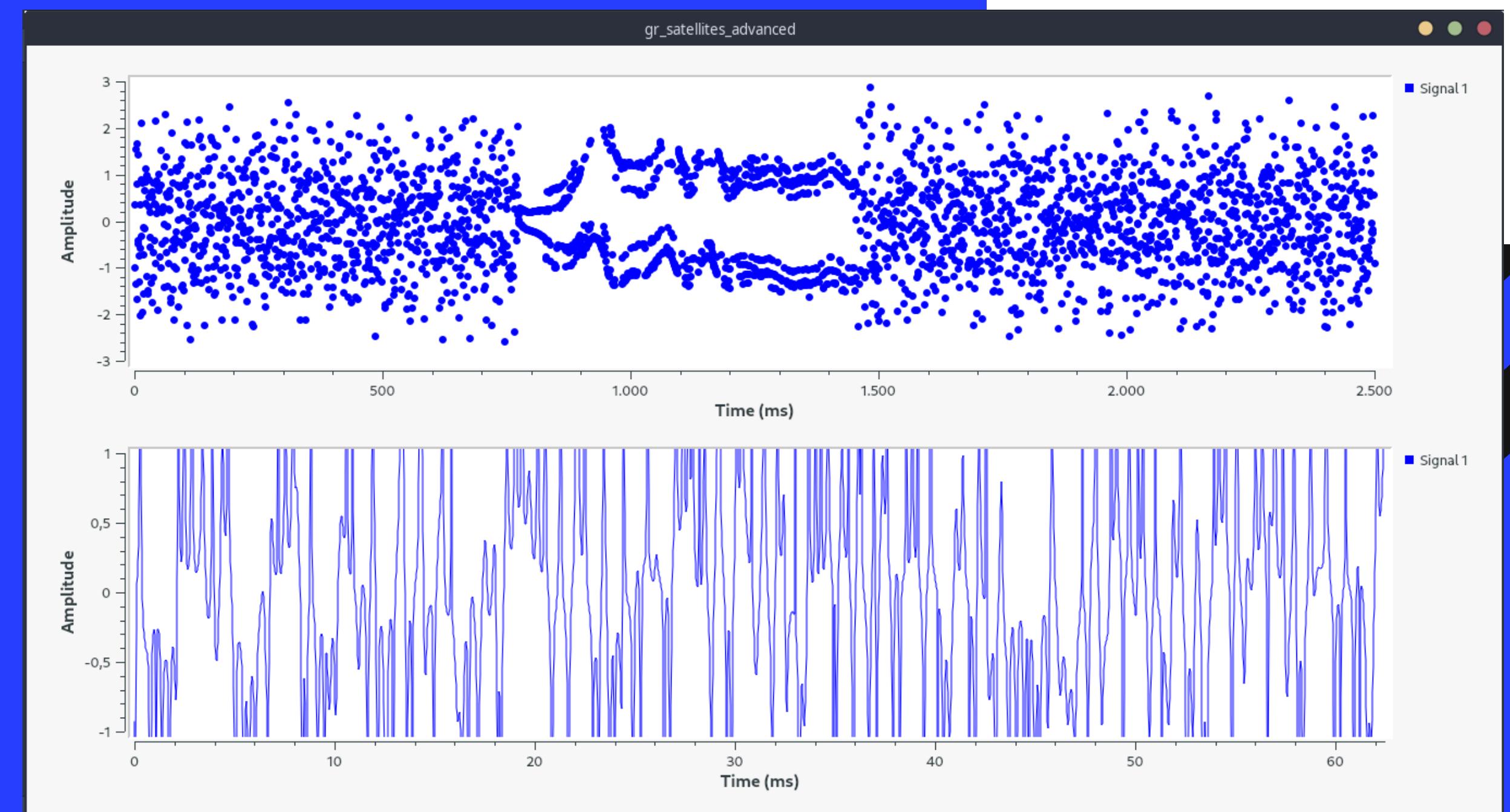
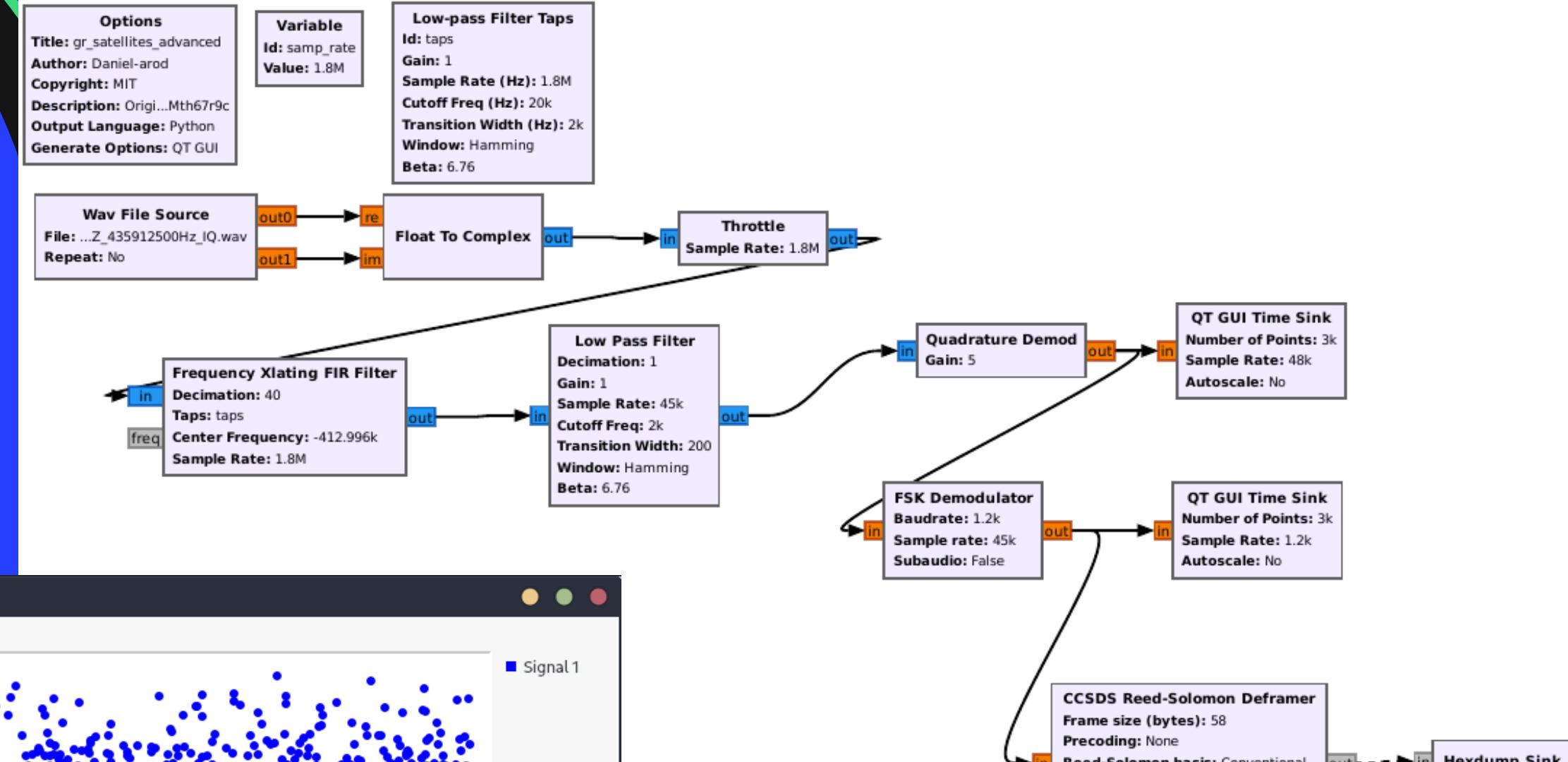
# EJEMPLO INICIAL DE GR SATELLITES



Ejemplo adaptado de Estévez, D (2020).

```
(transmitter F2K4_FSK downlink) (rs_errors: 0) (iterations: 1)
  ...
  modulator_length = 92
  contents =
  0000: 00 56 00 b1 92 48 27 00 03 00 00 54 14 57 1f 01
  0010: 26 6e 0e db c7 fe f8 7f 10 11 a3 00 04 00 3e 02
  0020: 38 ff a5 18 00 11 3b 03 43 f7 1a 00 00 00 00 00 00
  0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0040: 00 00 00 00 00 00 01 57 00 00 00 00 ff ff 00 00
  0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 3b 00
  ****
gr::log :DEBUG: decode_rs0 - Reed-Solomon decode fail (interleaver path 0)
```

# EJEMPLO AVANZADO DE GR SATELLITES



Ejemplo adaptado de Estévez, D (2020).

# ESPIAR MONITORES

También conocidos como ataques Tempest (Ahmed, 2017), consiste en "escuchar" la señal electromagnética que emiten los monitores de computadora para luego decodificarlos y ver lo que hace otra persona en su monitor (Radio Bunker, 2019).

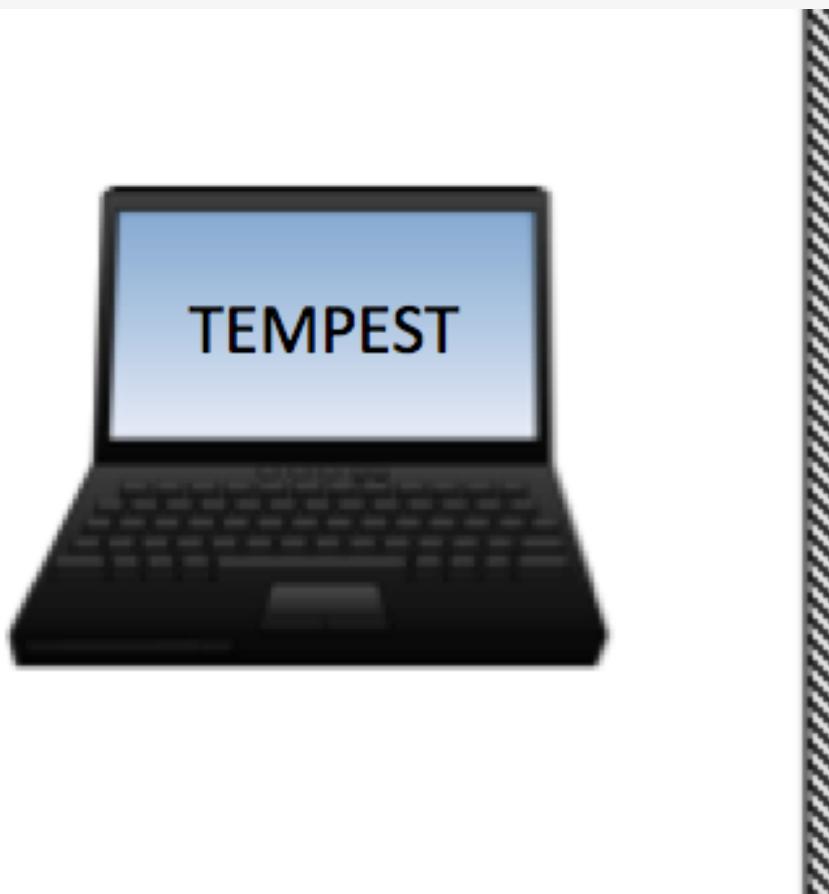


Imagen recuperada de: <https://bit.ly/3bnQ6DK>



Mark Jessop  
@darksidelemm



I knew TEMPEST was a thing, but actually grabbing some open source software and \*doing it\* is freaking cool...

12:25 PM - Nov 24, 2017

Imagen recuperada de: <https://markeldo.com/images/jessop-tempest-sdr.png>

# ATAQUES REPLAY

Consisten en escuchar una señal de un dispositivo y grabarla para luego transmitirla de nuevo y de esta forma se falsifica la identidad del usuario (Kamkar, 2016).



Imagen recuperada de: <https://bit.ly/2SG8oJY>

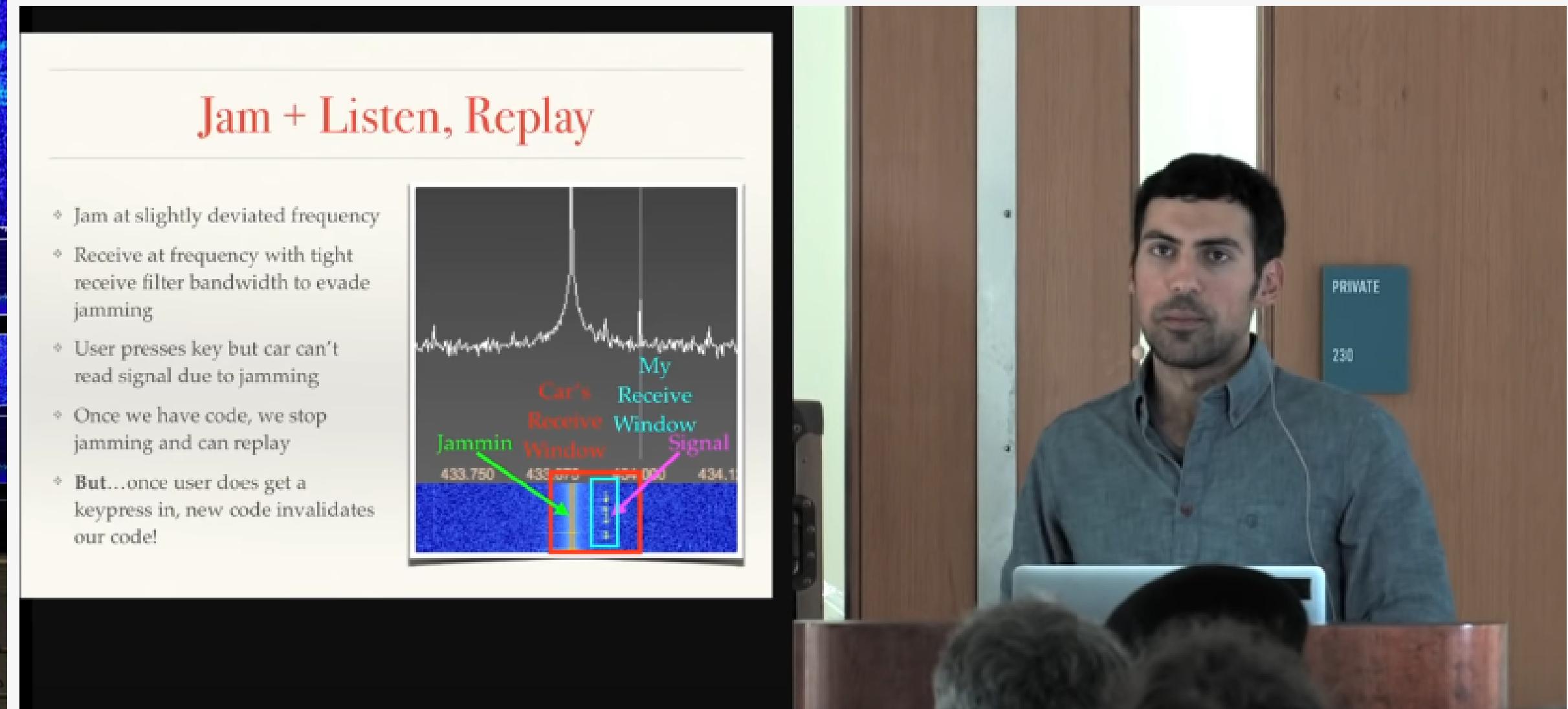
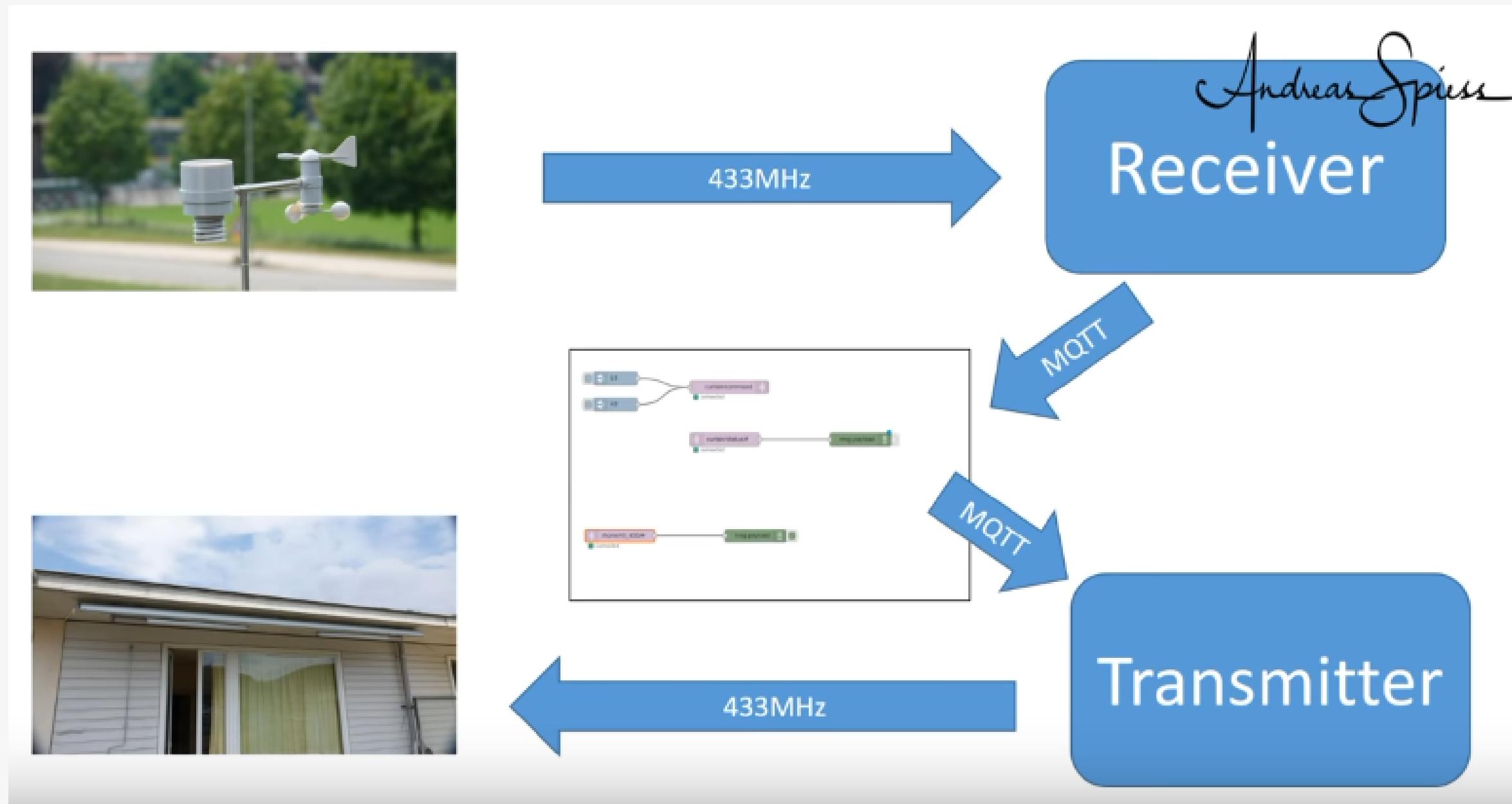


Imagen recuperada de: <https://youtu.be/1RipwqjG50c>

# REVIVIR HARDWARE

Usando la misma lógica de los ataques replay, se puede grabar las señales emitidas de dispositivos antiguos como controles de garajes para luego construir nuevas tecnologías que los vuelan a usar



Uso de estación meteorológica para cerrar o abrir cortina (Spiess, 2018). Imagen recuperada de: <https://youtu.be/L0fSEbGEY-Q>

# OTRAS APLICACIONES\*



Altamente recomendado revisar regulaciones nacionales antes de intentar cualquiera de estas aplicaciones

Escuchar comunicaciones\*  
Escuchar comunicaciones públicas como las de diferentes cuerpos de seguridad, salud, bomberos, entre otras



Imagen recuperada de:  
<https://tinyurl.com/yshvwn7u>

Seguimiento de aviones  
Todos los aviones envían información sobre su locación usando ADS-B (Automatic Dependent Surveillance - Broadcast) (Reed, 2020).

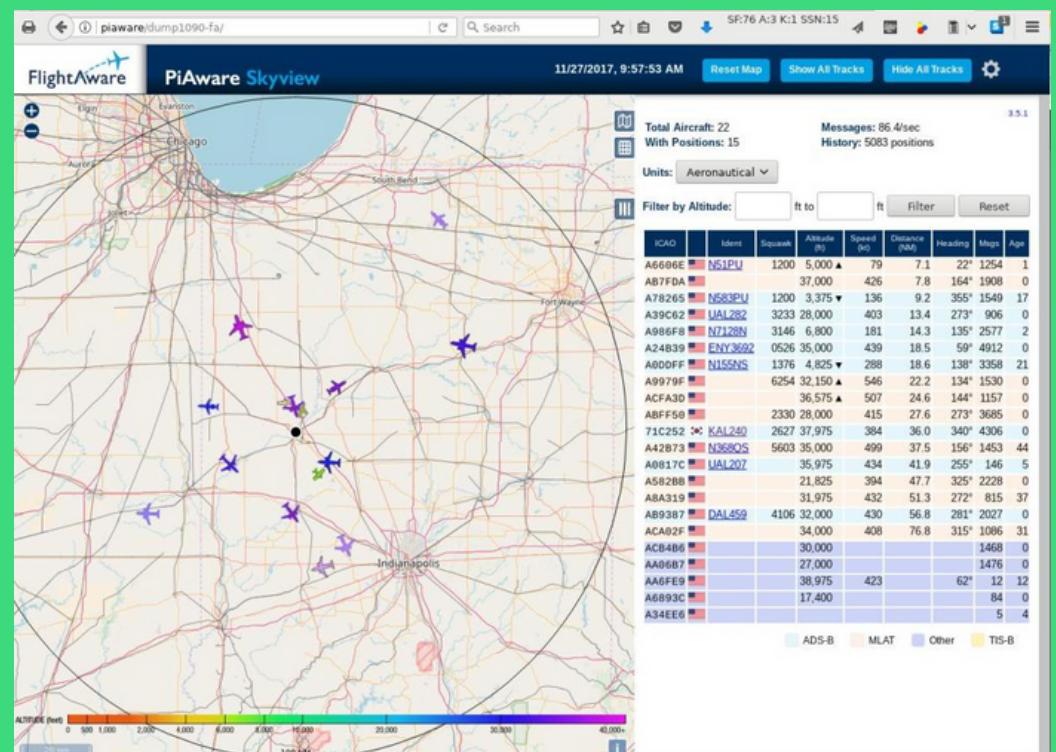


Imagen recuperada de: <https://tinyurl.com/kmfeaezz>

Decodificar pagers (beepers)  
Son dispositivos capaces de enviar texto, aunque son poco comunes, suelen ser usados en hospitales, departamentos de bomberos y algunas compañías (RTL-SDR.com, 2013)



Imagen recuperada de RTL-SDR.com (2013)

```
PDW v3.1 - POCSAG-1200
File Edit Interface Options Filters Display Monitor CharacterSet Help
Address Time Date Mode Type Bitrate Monitored Messages
1960460 18:56:13 25-05-13 POCSAG-4 ALPHA 1200 Triage 2 IENOB 25-MAY-13 18:53 Chest pain
1960308 18:56:13 25-05-13 POCSAG-4 ALPHA 1200 Triage 2 IENOB 25-MAY-13 18:53 Chest pain
1234567 18:56:14 25-05-13 POCSAG-4 ALPHA 1200 THIS IS A TEST PERIODIC PAGE SEQUENTIAL NUMBER 1087
1234567 18:56:20 25-05-13 POCSAG-4 ALPHA 512 THIS IS A TEST PERIODIC PAGE SEQUENTIAL NUMBER 1087
1126489 18:56:25 25-05-13 POCSAG-4 ALPHA 1200 Unit: CITY2 Job # 1224-1-2013/0 Responded: 18:18 Located: 18:32 Departed: 18:40 destination: 18:56
1120149 18:56:26 25-05-13 POCSAG-4 ALPHA 1200 from ed 5 to ct please. thanks From: 24036
1123017 18:56:40 25-05-13 POCSAG-4 ALPHA 1200 LHS Ta "Meda"
1855468 18:56:41 25-05-13 POCSAG-4 ALPHA 1200 SCADA ALARM 25 May 2013 18:55:08 NPL Sub Minor Alarm ALARM
1234567 18:56:48 25-05-13 FLEX-A ALPHA 1600 THIS IS A TEST PERIODIC PAGE SEQUENTIAL NUMBER 7119
0724855 18:56:48 25-05-13 FLEX-A ALPHA 1600
1120547 18:56:53 25-05-13 POCSAG-4 ALPHA 1200 CHED: UAZ0320 to Kida Med Fm:x7410 kth
1140083 18:57:01 25-05-13 POCSAG-4 ALPHA 1200 Unit: CTY21 Job # 1051-1-2013/0 Responded: 17:53 Located: 18:19 Cancelled:
1234567 18:57:02 25-05-13 POCSAG-4 ALPHA 1200 THIS IS A TEST PERIODIC PAGE SEQUENTIAL NUMBER 1088
Address Time Date Mode Type Bitrate Filtered Messages
```

Imagen recuperada de RTL-SDR.com (2013)

# Resumen

Las Radios Definidas por Software son el comienzo de las comunicaciones definidas por software, la idea es tener dispositivos capaces de cambiar entre protocolos y frecuencias para prestar diferentes servicios (AFR Research LAB, 2019). Estos podrían cambiar entre comunicación satelital, Wifi, Bluetooth, 2 metros y muchas otras.



Imagen recuperada de: <https://tinyurl.com/wfph8hmj>



Imagen recuperada de: <https://youtu.be/WYj1qjxzHaw>

# REFERENCIAS

- BMayes. (2019). "What is Software Defined Radio?". Recuperado de: <https://bit.ly/3b4S9g9>
- Mendieta., L, Cano ., L., Ferro., R. (2017). "Diseño de una trans receptor SDR de bajo coste basado en ingeniería del software para el seguimiento de pequeños satélites en órbita leo". Redes de ingeniería. Universidad Distrital Francisco José de Caldas. Recuperado de: <https://repository.udistrital.edu.co/handle/11349/20202>
- Nutaq. (2021). "A short history of software-defined radio (SDR technology)". Recuperado de: <https://bit.ly/3uPIH83>
- RTL-SDR.com. (2021). "About RTL-SDR". Recuperado de: <https://bit.ly/3w44pVZ>
- Cardona, I. (2020). "GNU Radio para principiantes 1a parte, EB3FRN". Recuperado de: <https://youtu.be/KCtcHaPr7Ug>
- BehrTech Blog. (2020). "Where Do My IoT Sensors Live? An Overview of the Sub-GHz ISM Bands". Recuperado de: <https://bit.ly/3uMzgX3>
- Younis, A. (2019). "Space Career Story: How to get into the Space Satellite Industry". Recuperado de: <https://youtu.be/zKLufUUisiM>
- Estévez, D. (2021). "gr-satellites". Recuperado de: <https://github.com/daniestevez/gr-satellites>
- Estévez, D. (2021). (2020-07-05). gr-satellites guidance, online session with the BeliefSat-1 student team of K. J. Somaiya Institute of Engineering and Information Technology (India) about the use of gr-satellites. Recuperado de: <https://youtu.be/TceMth67r9c>
- Ahmed, M. (2017). "TEMPEST Attacks . By Mohamed Ahmed ". Nullbyte. Recuperado de: <https://tinyurl.com/7hdtvew>
- Radio Bunker. (2020). "Espia PC con TEMPESTSDR y RTL-SDR". Recuperado de: <https://youtu.be/HkdoKlo5eno>
- Kamkar, S. (2016). "Radio Hacking: Cars, Hardware, and more! - Samy Kamkar - AppSec California 2016". Recuperado de: <https://youtu.be/1RipwqJG50c>
- Spiess, A. (2018). "#209 How to Hack your 433 MHz Devices with a Raspberry and a RTL-SDR Dongle (Weather Station)"
- Reed, T. (2020). "Three Aviation Signals to Tune into for Your Next SDR Project". Recuperado de: <https://tinyurl.com/4zt2wcaa>
- RTL-SDR.com. (2013). "RTL-SDR Tutorial: POCSAG Pager Decoding". Recuperado de: <https://tinyurl.com/d22vhfvw>
- AFR Research Lab. (2019). "Software Defined Radio". Recuperado de: <https://youtu.be/WYj1qjxzHaw>

# ¡GRACIAS POR ASISTIR!

The screenshot shows Daniel Alejandro Rodriguez's GitHub profile. At the top, there is a large circular profile picture of him wearing glasses and a suit. Below the picture, his name "Daniel Alejandro Rodriguez" and affiliation "el-NASA" are displayed. A "Follow" button is present. To the right, there are several pinned repositories:

- CanSat-Ground-station**: Code for a CanSat or OBCs GUI ground station where different sensor data are displayed in real time. No sensors needed to try it. (Python, 17 stars, 4 forks)
- POA-OBC**: POA-OBC is a project based on Arduino and its purpose is to give the open source code and schematics on how to build a On Board Computer (mainly a data logger) for a model rocket for science and re... (C++, 2 stars, 2 forks)
- CanSat**: Pico Satelite que obtiene y transmite datos sobre su estado. Es desarrollado como parte de proyecto de investigación del semillero ATL. (C++)
- Banco-pruebas-estaticas**: El proyecto consiste en realizar el registro de los datos de empuje de un motor de cohete. (Python)
- my-little-sniffer**: Python
- GY-BMP280**: Eagle library for the GY-BMP/E 280 (Chinese BMP280) (Python)

At the bottom of the profile page, it shows "16 followers · 23 following · 27 contributions in the last year" and a "2021" button.

Puedes consultar los ejemplos de la charla en:  
[https://github.com/el-NASA/GNU\\_Radio\\_examples](https://github.com/el-NASA/GNU_Radio_examples)

¿Alguna duda? escribe a  
semillero-ATL@protonmail.com