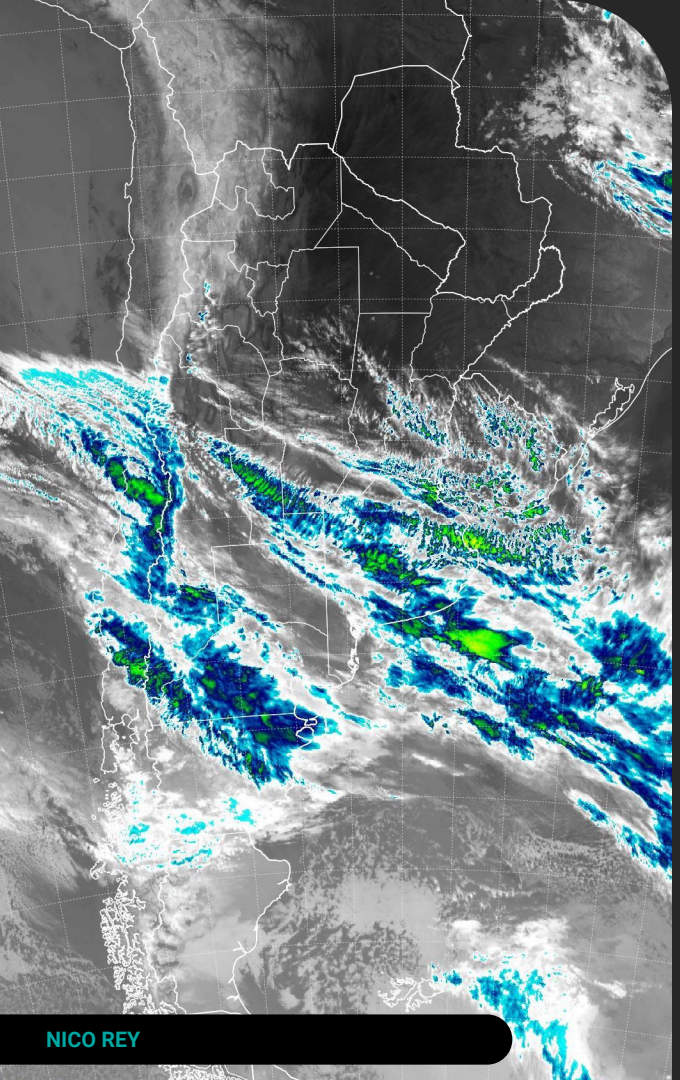
SIGNALS FROM OUTER SPACE

Hunting for data at thousands of kilometers

TODAY'S DISCUSSION

1. Introducción a los satélites
2. Recepción de señales y antenas
3. Receptores definidos por software
4. GNURadio y gr-satellites
5. Decodificación y hacking



Satélites

- Rol fundamental para las telecomunicaciones.
- Existen satélites comerciales, experimentales, proyectos educativos, etc.
- Algunos se usan de "puente" para comunicar dos partes del mundo.
- Otros envían imágenes de meteorología.
- Algunos hacen exploración del espacio profundo.
- Hay constelaciones de satélites para tener Internet en cualquier parte del mundo.
- Podemos "hablar" con los satélites!
- Imagen: GOES 16, satélite de meteorología.

Órbitas satelitales

(Existen otras!)

1. Low-earth Orbit

- Orbitan a 500 - 1500 KM
- 30-50 ms de latencia (ideal)
- 40 - 80 satélites para cubrir la tierra
- Visible por 10 a 20 minutos
- Accesibles para poner en órbita e intercambiar información
- A veces forman una red mesh
- Starlink vive acá

2. Medium-earth Orbit

- Orbitan a 5.000 - 20.000 KM
- 150-200 ms de latencia
- Cobertura del 96% de la tierra con 6 satélites
- Los satélites de GPS viven acá
- Algunas radios FM satelitales usaban ésta órbita
- Visible hasta 12 horas

3. Geostationary Orbit

- Orbitan a 35.800 KM
- 700 ms de latencia en promedio
- Cobertura del 99% de la tierra con 3 satélites
- Aparatos gigantes, caros y comerciales
- Satélites de telecomunicaciones, televisión e interconexión
- Constantemente visible

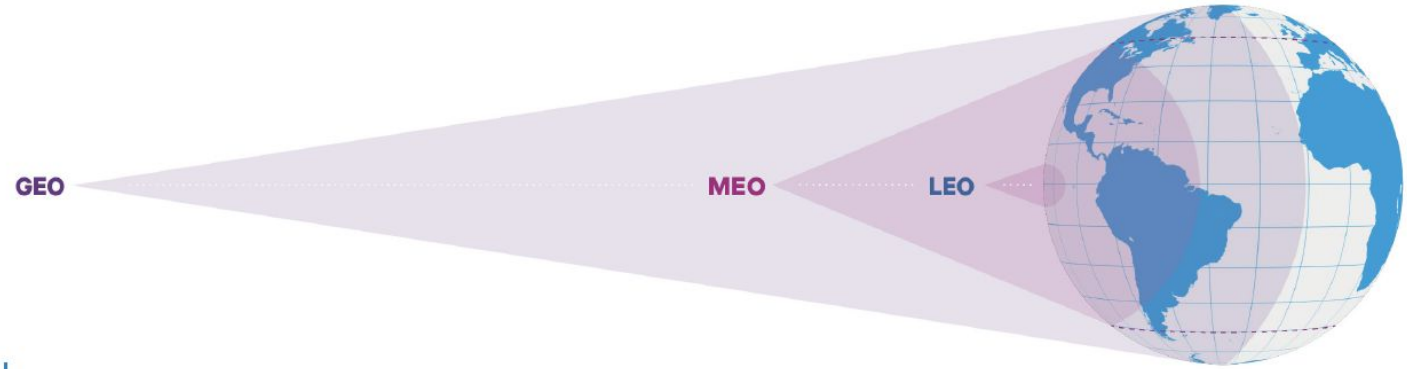


Figure 1: Schematic of orbital altitudes and coverage areas

Recepción y antenas

- Los satélites transmiten en diversas frecuencias y modulaciones.
- El receptor tiene que adecuarse a lo que queremos recibir.
- Existe un "sweet spot" entre el receptor, filtros, amplificadores, antenas y decodificadores.

Recepción: Frecuencias

NICO REY

Antenas

- No importa cuánta potencia, filtros y amplificación exista, la antena es el eslabón clave en tu recepción.
- A mayor frecuencia, menor longitud de onda, y menor tamaño de antena.
- Distintos tipos de satélites requieren distintos tipos de antenas para optimizar su recepción.
- En la foto se pueden apreciar dos antenas
  - Parabólica de Directv, banda Ku direccional.
  - Cuadrifilar helicoidal, calculada para 137MHz, omnidireccional.

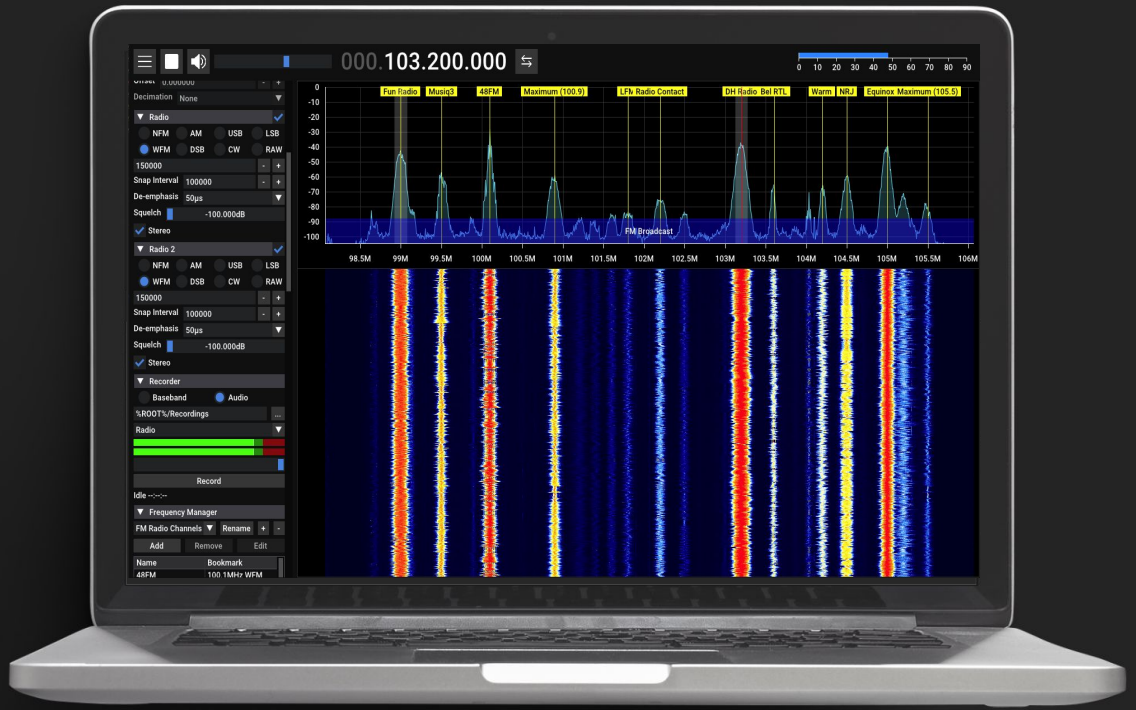
Receptores SDR

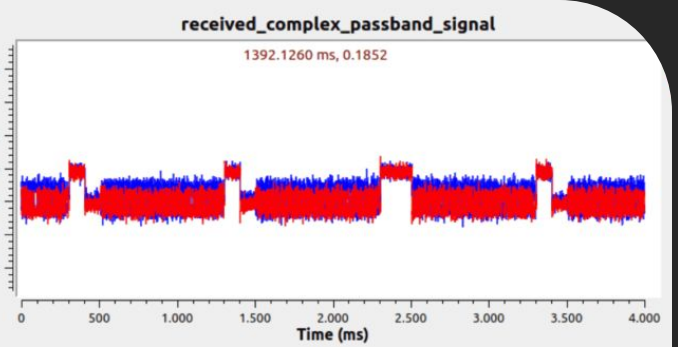
- Es un tipo de receptor completamente programable y muy flexible.
- Hay para todos los bolsillos.
- Pieza clave para nuestra cadena de recepción, ya que permite demodular la señal del satélite, aplicar filtros y quitar ruidos.
- Existe software prediseñado y también podemos hacer el nuestro.
    - gqrx
    - sdr++
    - gnuradio

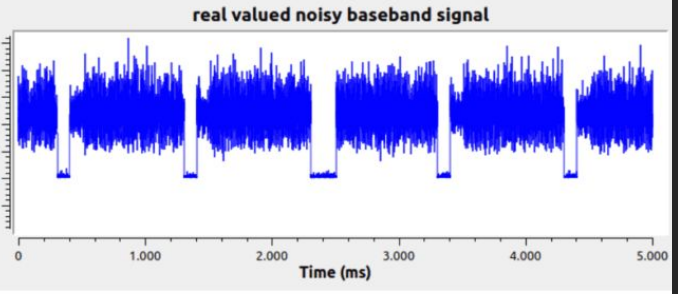
SDR++

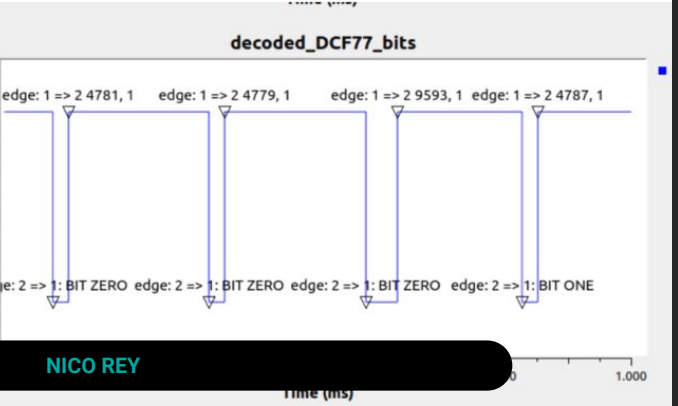
sdrpp.org

- Receptor SDR liviano y multiplataforma.
- Soporta muchos tipos de receptores SDR.
- Diseño modular.



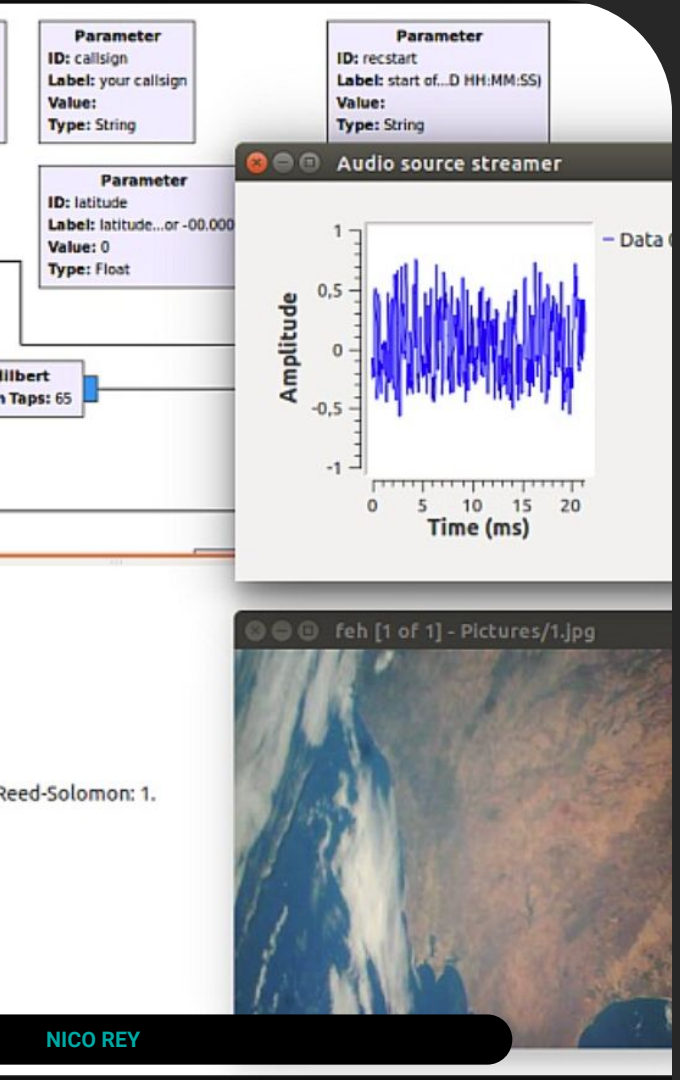






GNURadio

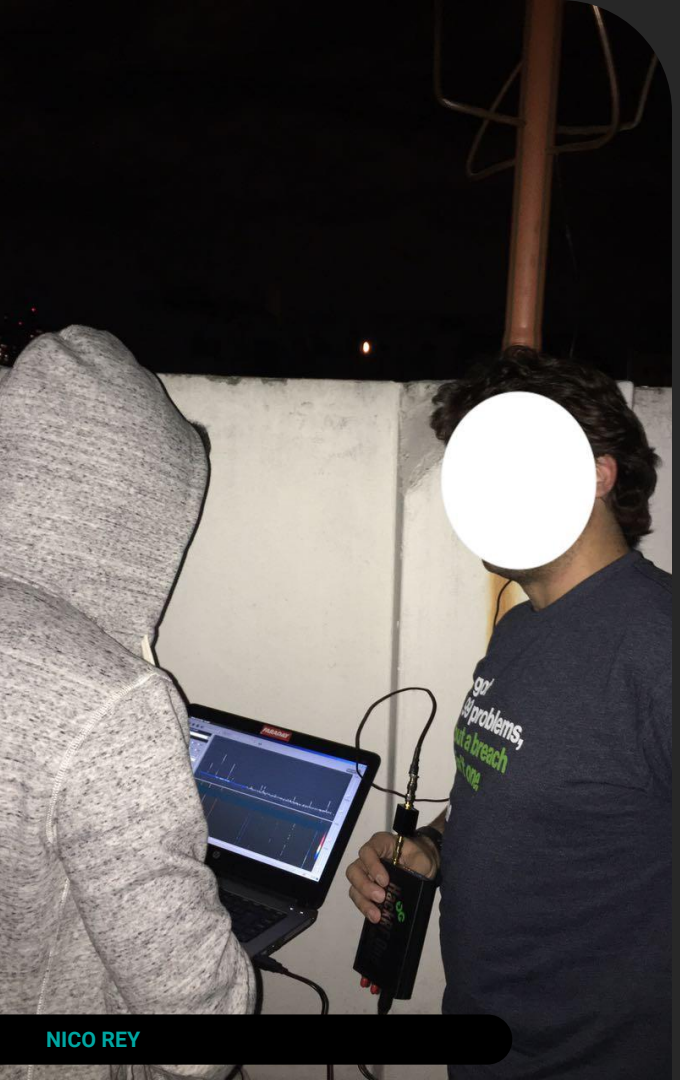
- Plataforma open-source de desarrollo de software para radio, incluído SDR.
- Permite crear flujos de procesamiento personalizados para manipular y analizar las señales capturadas.
- Existen bloques "out of tree", como gr-satellites.



gr-satellites

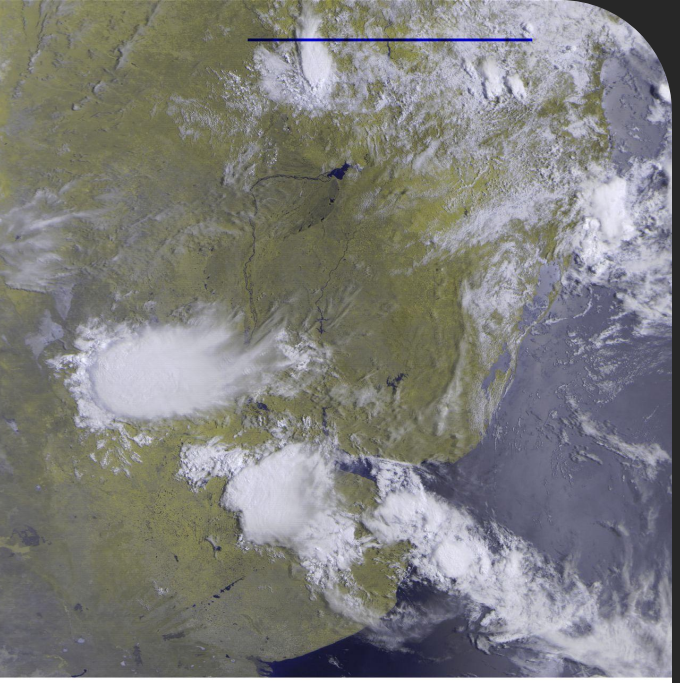
https://github.com/daniestevez/gr-satellites

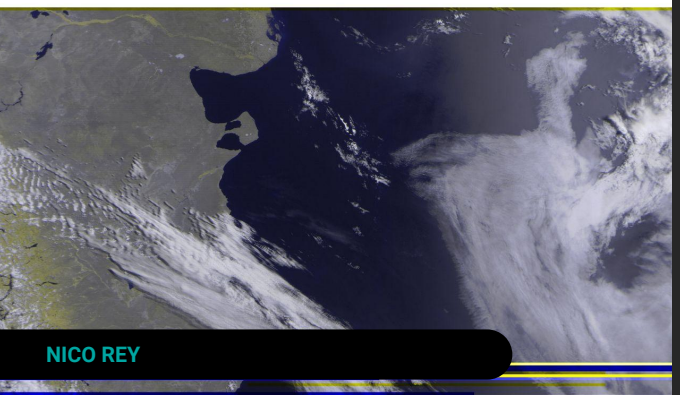
- Módulo out-of-tree: Se agrega de forma externa a GNURadio.
- Toolkit para decodificación de señales satelitales.
- Soporta los protocolos más populares que usan los satélites.
- Soporta scrambling, corrección de errores y sync words.
- Tiene una buena comunidad por detrás.



Decodificación & Hacking

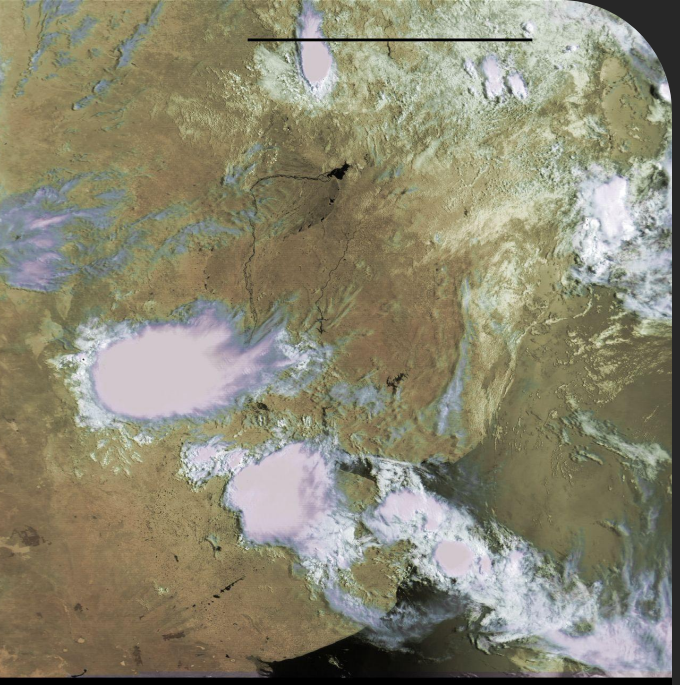
- Desafíos técnicos:
  - Interferencia de señales.
  - Sincronización de paquetes.
- Recepción de imágenes satelitales: Meteor M2
- Decodificación de un picosat con GNURadio.

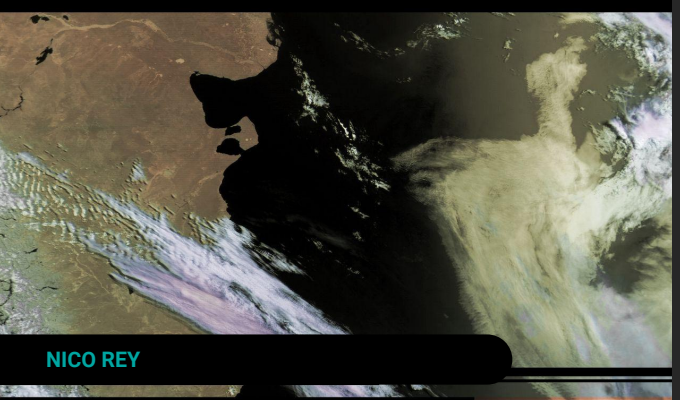




Meteor M2

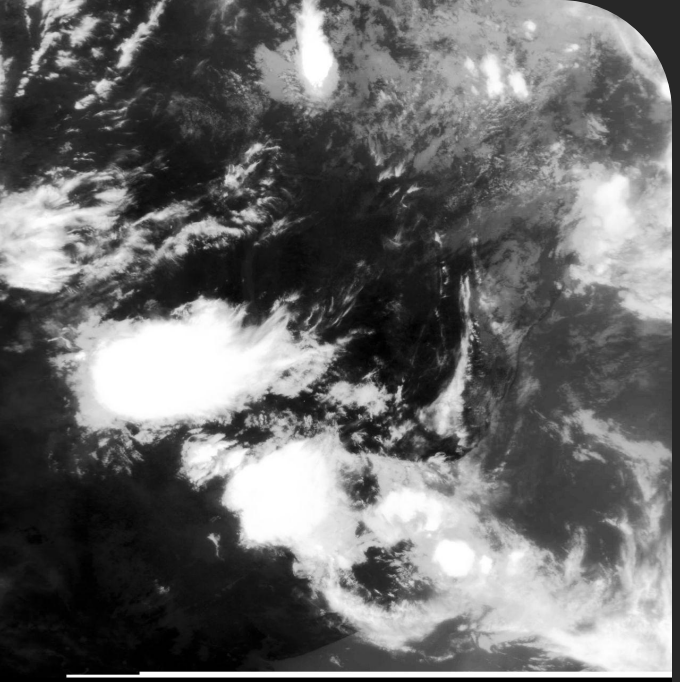
- Línea de satélites Rusos de meteorología.
- Transmiten en 137MHz, modo LRPT.
- Las imágenes tienen diferentes "enhancements".
  - **Estándar**
  - Color falso
  - Infrarrojo
  - Térmico
  - Vegetación

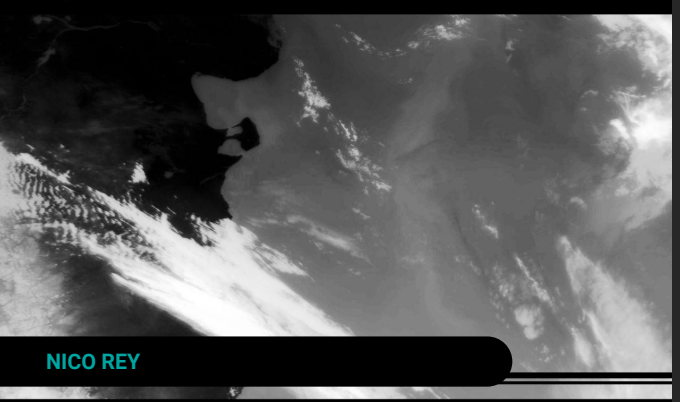




Meteor M2

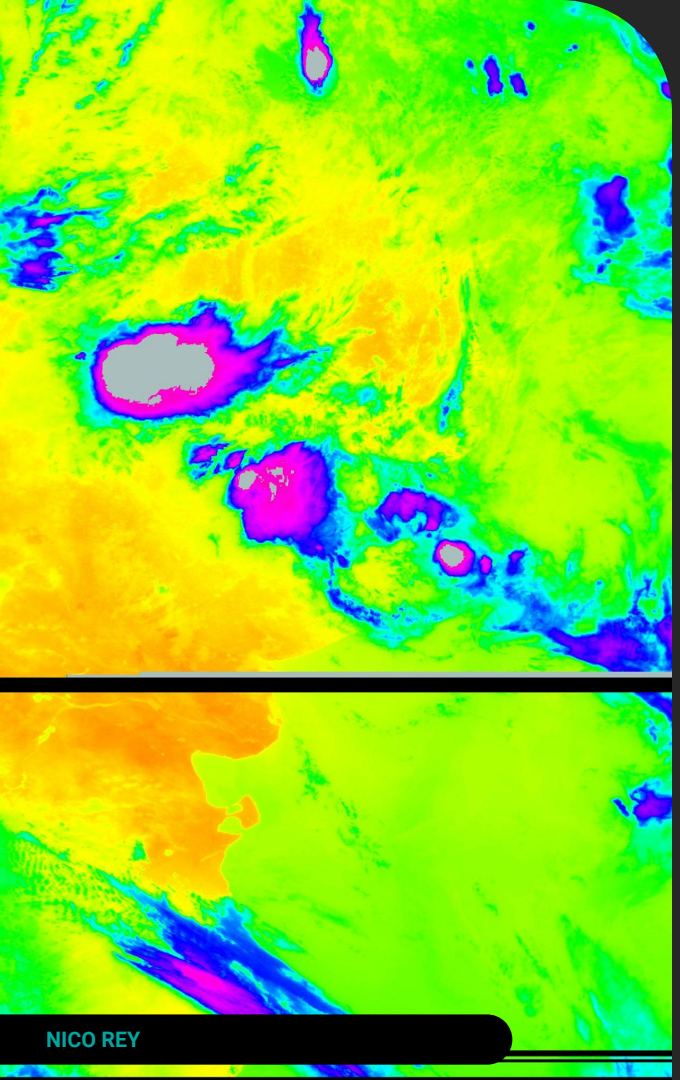
- Línea de satélites Rusos de meteorología.
- Transmiten en 137MHz, modo LRPT.
- Las imágenes tienen diferentes "enhancements".
  - Estándar
  - **Color falso**
  - Infrarrojo
  - Térmico
  - Vegetación





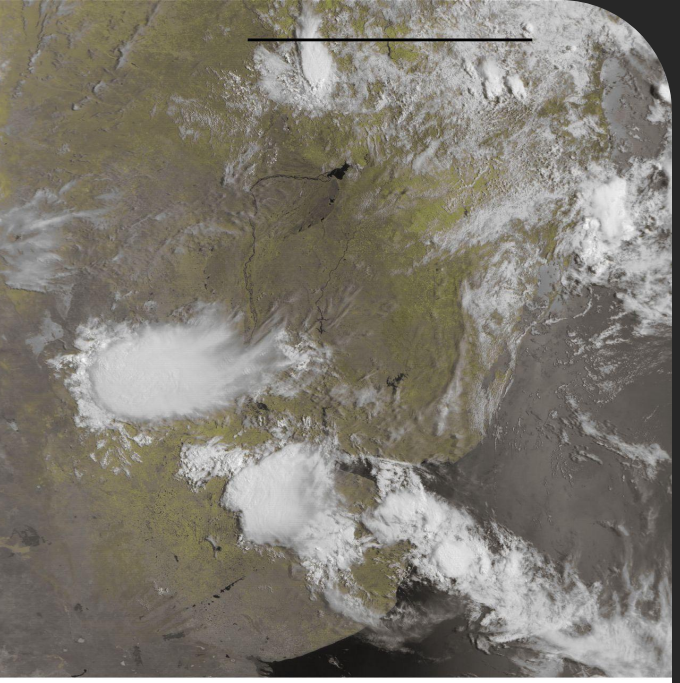
Meteor M2

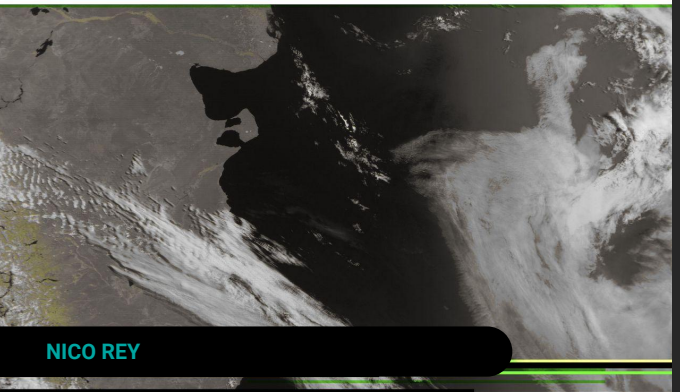
- Línea de satélites Rusos de meteorología.
- Transmiten en 137MHz, modo LRPT.
- Las imágenes tienen diferentes "enhancements".
  - Estándar
  - Color falso
  - **Infrarrojo**
  - Térmico
  - Vegetación



Meteor M2

- Línea de satélites Rusos de meteorología.
- Transmiten en 137MHz, modo LRPT.
- Las imágenes tienen diferentes "enhancements".
  - Estándar
  - Color falso
  - Infrarrojo
  - **Térmico**
  - Vegetación





NICO REY

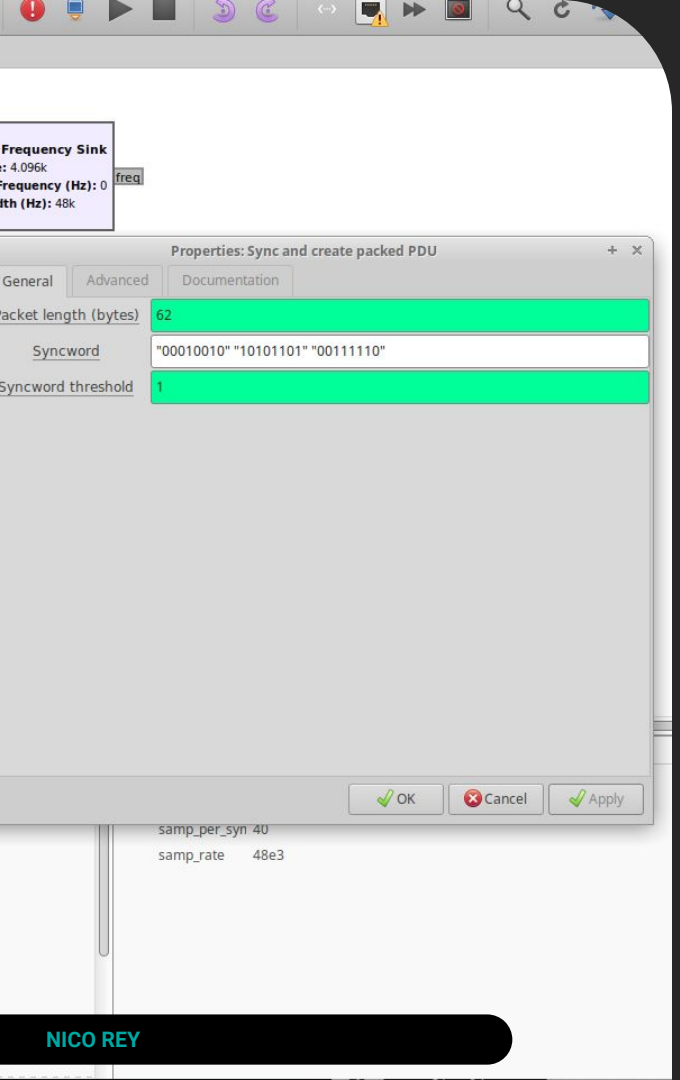
Meteor M2

- Línea de satélites Rusos de meteorología.
- Transmiten en 137MHz, modo LRPT.
- Las imágenes tienen diferentes "enhancements".
  - Estándar
  - Color falso
  - Infrarrojo
  - Térmico
  - **Vegetación**

Stratosat-TK1

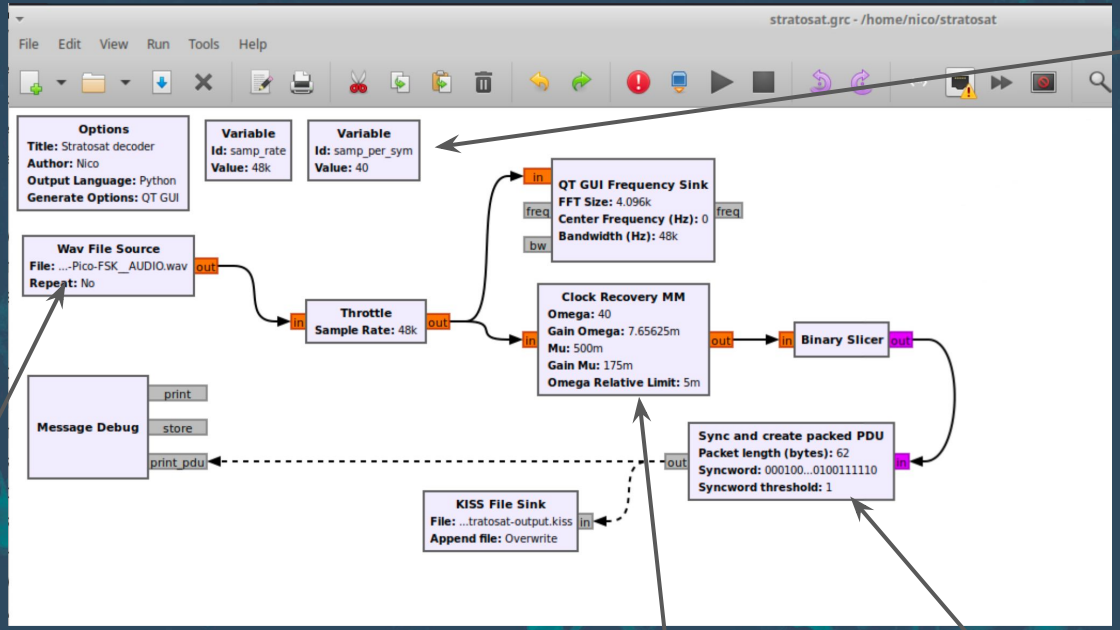
- 6 picosatélites lanzados en órbita baja.
- Parte de un programa educativo, los satélites son construidos por alumnos.
- Envían telemetría a través de transmisores LoRa.
- Esquema de modulación: FSK (Frequency Shift Keying). Ejemplo:
  - 1 = 1000 Hz.
  - 0 = 2000 Hz.

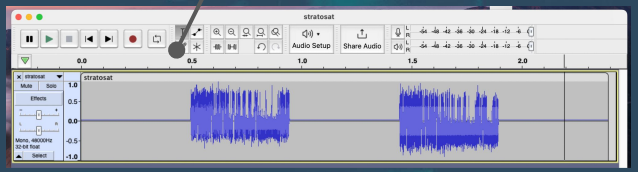
RS52SD Aug 17, 2023 5:00 PM (an hour ago)	Mode LoRa@436.26	Received by 1 stations	1000mW 4240mV 8.10mA 10°C imu: (15628.00,-3.54,-0.79) 125mW
RS52SD Aug 17, 2023 5:00 PM (an hour ago)	Mode LoRa@436.26	Received by 3 stations	1000mW 4240mV 8.10mA 10°C imu: (3.79,-3.54,-0.79) 125mW
RS52SD Aug 17, 2023 4:45 PM (2 hours ago)	Mode LoRa@436.26	Received by 1 stations	1000mW 4252mV 4.60mA 5°C imu: (3.72,-3.97,-0.79) 266mW
RS52SD Aug 17, 2023 3:08 PM (3 hours ago)	Mode LoRa@436.26	Received by 2 stations	1000mW 4244mV 7.90mA 6°C imu: (3.72,-3.78,-1.22) 133mW



Stratosat-TK1

- **Bloques esenciales:**
  - **Syncword:** "Palabra" como prefijo que sincroniza los paquetes. En este caso es **0x12AD**.
  - **Clock Recovery:** Proceso para extraer la información de timing sin tener una señal de reloj específica para esto del lado del receptor.

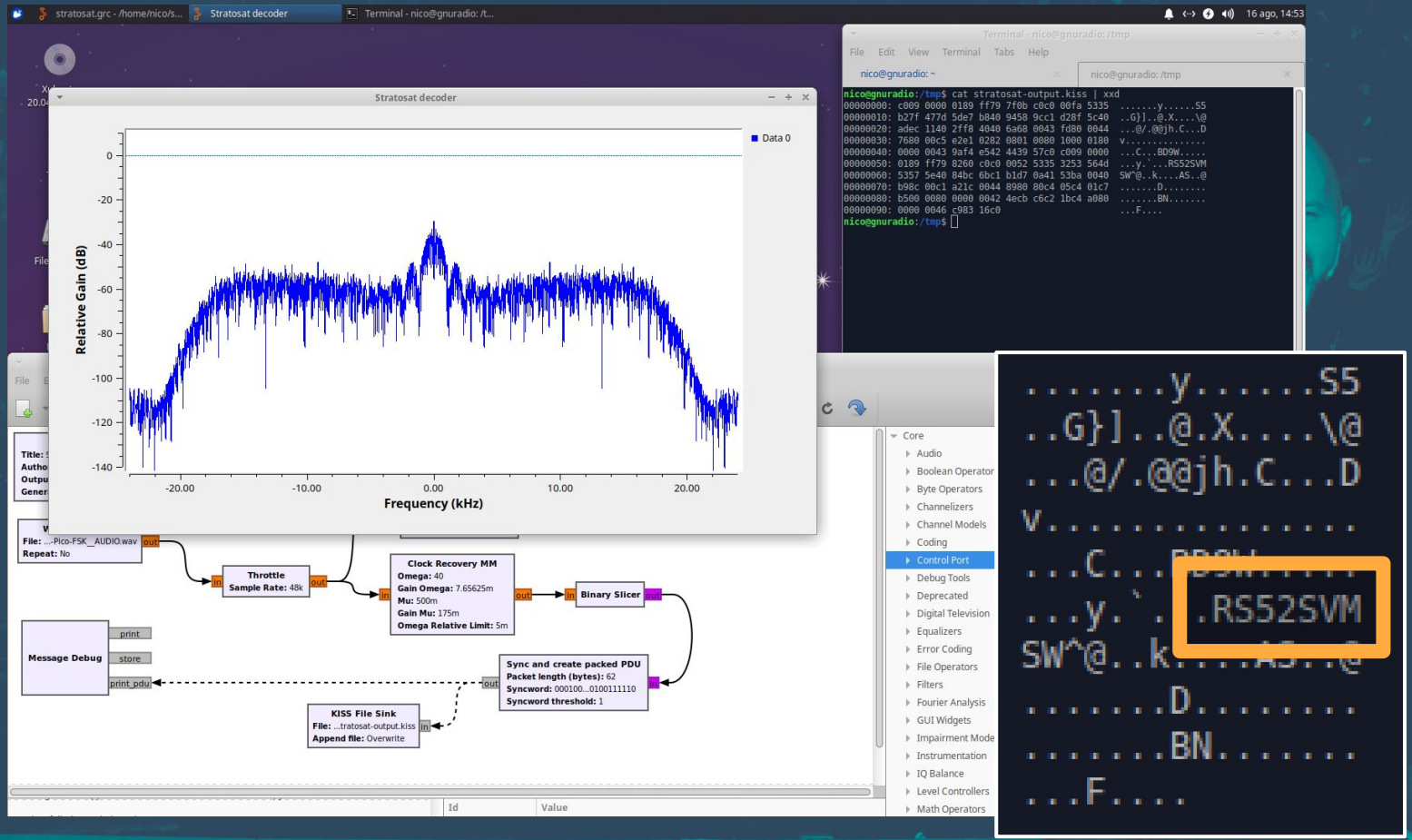




Símbolos por unidad de tiempo

Recuperación de timing

Sync Word (Preámbulo)


stratosat.grc - /home/nico/s...
Stratosat decoder
Terminal - nico@gnuradio: /t...
16 ago, 14:53
Stratosat decoder
Data 0
Relative Gain (dB)
Frequency (kHz)
Terminal - nico@gnuradio: /tmp
File Edit View Terminal Tabs Help
nico@gnuradio: ~
nico@gnuradio: /tmp
nico@gnuradio:/tmp$ cat stratosat-output.kiss | xxd
00000000: c009 0000 0189 ff79 7f0b c0c0 00fa 5335 ....y......S5
00000010: b27f 477d 5de7 b040 9458 9ce1 d28f 5c40 ..G}]..@.X....\@
00000020: adec 1140 2ff8 4040 6a68 0043 fd80 0044 ...@/.@@jh.C...D
00000030: 7680 00c5 e2e1 0282 0801 0080 1000 0180 v...............
00000040: 0000 0043 9af4 e542 4439 57c0 c009 0000 ...C...BD9W.....
00000050: 0189 ff79 8260 c0c0 0052 5335 3253 564d ...y.`...RS52SVM
00000060: 5357 5e40 84bc 6bc1 b1d7 0a41 53ba 0040 SW^@..k....AS..@
00000070: b98c 00c1 a21c 0044 8980 80c4 05c4 01c7 ....D........
00000080: b500 0080 0000 0042 4ecb c6c2 1bc4 a080 ....BN.......
00000090: 0000 0046 c983 16c0 ...F....
nico@gnuradio:/tmp$
File: ...Pico-FSK_AUDIO.wav
Repeat: No
Throttle
Sample Rate: 48k
Clock Recovery MM
Omega: 40
Gain Omega: 7.65625m
Mu: 500m
Gain Mu: 175m
Omega Relative Limit: 5m
Binary Slicer
Message Debug
print
store
print_pdu
Sync and create packed PDU
Packet length (bytes): 62
Syncword: 000100...0100111110
Syncword threshold: 1
KISS File Sink
File: ...tratosat-output.kiss
Append file: Overwrite
Core
Audio
Boolean Operator
Byte Operators
Channelizers
Channel Models
Coding
Control Port
Debug Tools
Deprecated
Digital Television
Equalizers
Error Coding
File Operators
Filters
Fourier Analysis
GUI Widgets
Impairment Mode
Instrumentation
IQ Balance
Level Controllers
Math Operators
Id
Value
.RS52SVM

Hacking: Iridium

- Telefonía satelital early 2000s.
- Constelación de 77 satélites LEO
  - 77 = número atómico del Iridio :-)
  - Hay sólo ~66 satélites activos.
- Downlink en 1616 - 1625 MHz.
- Proveen voz, mensajes/paging y datos.

Recepción

- Antena QFH sintonizada para ~1620 MHz
- Amplificador con filtro pasabanda para ~1620 MHz
- Receptor SDR
- Compu con Linux / Raspberry PI
  - https://github.com/muccc/gr-iridium/
  - https://github.com/muccc/iridium-toolkit/

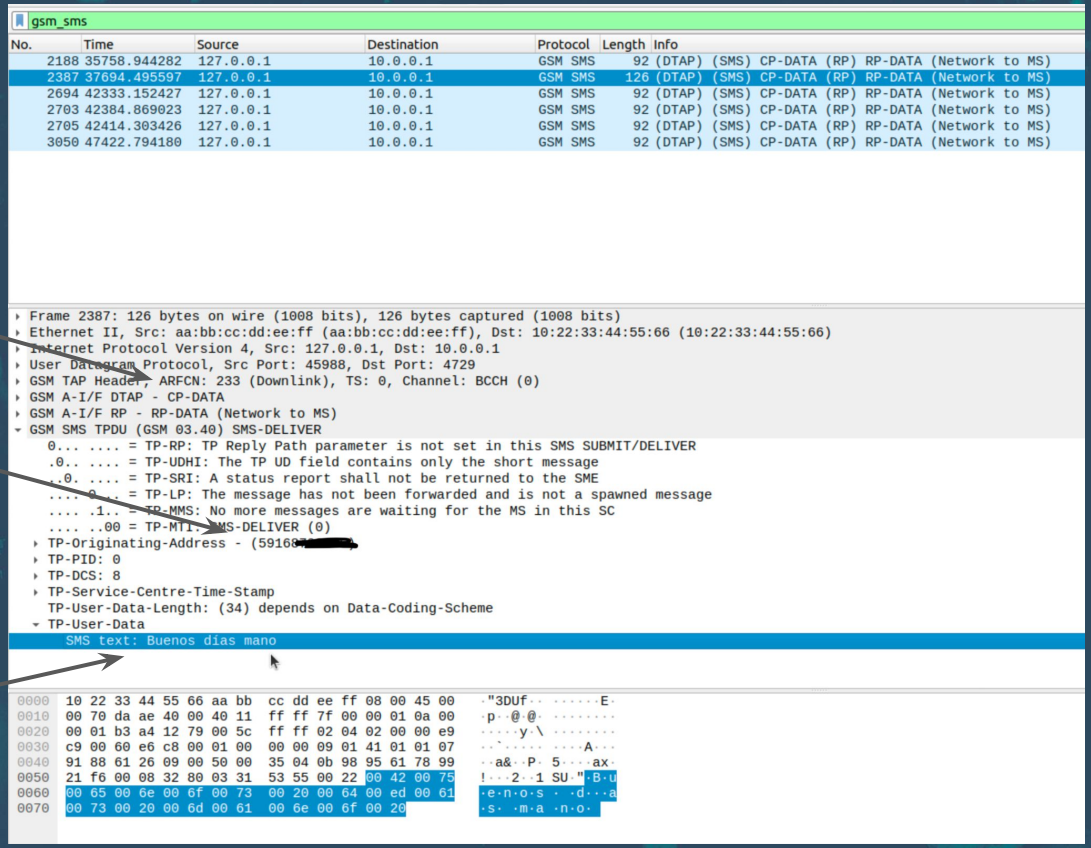
Decodificación

- Stephan "Sec" & Schneider desarrollaron gr-iridium e iridium-toolkit: Herramientas open source para decodificar frames Iridium.
- Puede decodificar:
  - Mensajes de texto
  - SBD (mensajes de pagers)
  - Llamadas de voz y sus metadatos
  - ACARS (mensajes aeronáuticos)
  - Etc.
  - Etc.
  - Etc.

Número de canal

Remitente

Mensaje



¿Cómo empiezo?

- Receptor SDR R820t, se consiguen en Mercadolibre.
  - Si no puedo comprar un receptor:
  - https://network.satnogs.org/
    - Open source ground stations.
  - https://www.sigidwiki.com/
    - Wiki de señales.
- Instalar GNURadio y sdr++.
- Empezar sintonizando radios FM.
- Entender como afectan diferentes filtros y modulaciones.
- Fabricar o comprar diferentes tipos de antenas.
- Embarcarse en GNURadio (es intenso!)
- Happy hacking!

THANKS!