# Demystifying SDR Hacking: A Deep Dive into Wireless Protocols Part:6

[](https://medium.com/@kishoreramk?source=post_page---byline--296a84d18ba7---------------------------------------)

[KISHORERAM](https://medium.com/@kishoreramk?source=post_page---byline--296a84d18ba7---------------------------------------)

Follow

10 min read

·

Oct 14, 2023

Listen

Share

More

## HackrfOne

HackrfOne is an open-source Software Defined Radio (SDR) peripheral that is capable of both transmitting and receiving radio signals. It operates in a wide frequency range from 1 MHz to 6 GHz, making it highly versatile for a variety of radio technologies.It can be used for replay attacks,Jamming Signals,Sniffing,Spoofing.



Source:<https://www.indiamart.com/>

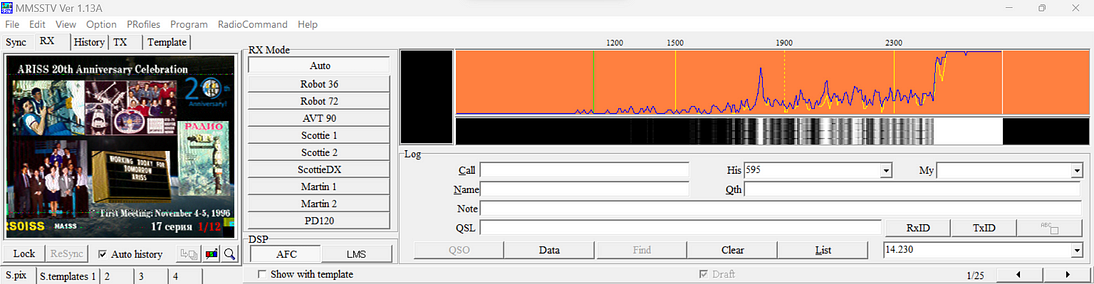
**Firmware Update HackrfOne**

https://github.com/mossmann/hackrf/releases/  
  
taf –xvf (upzip file)  
cd firmware-bin  
hackrf\_spiflash -w hackrf\_one\_usb.bin  
hackrf\_cpldjtag -x firmware/cpld/sgpio\_if/FILENAME.xsvf

## SSTV Broadcast

Slow Scan Television (SSTV) is a method used by ham radio operators to send images over radio frequencies. With a Raspberry Pi and HackRF One, you can set up your own SSTV station! The Raspberry Pi can be used to transmit SSTV signals. A project called Pi-SSTV used to transmit images in the SSTV.

Press enter or click to view image in full size

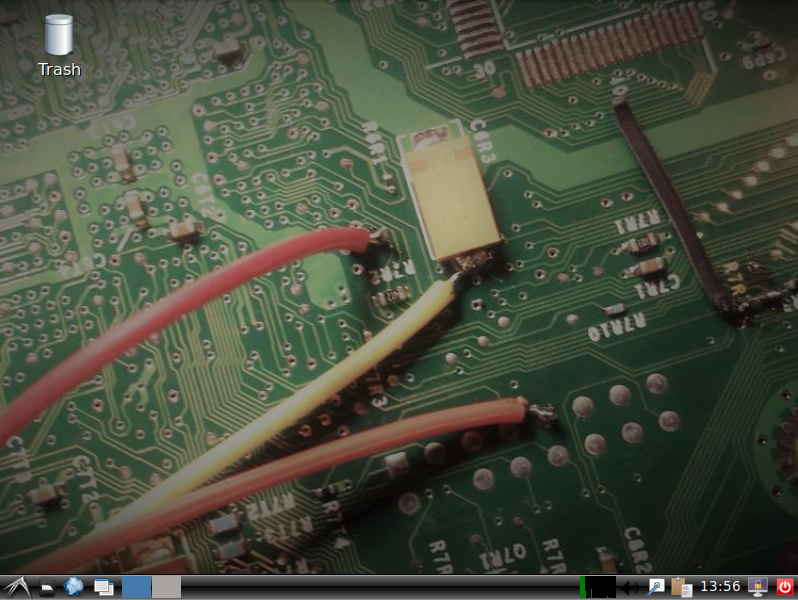


https://github.com/AgriVision/pisstv  
  
sudo apt-get install python-setuptools  
sudo apt-get install python-imaging  
sudo easy\_install pip  
sudo pip install setuptools --no-use-wheel --upgrade  
sudo pip install PySSTV  
sudo apt-get install libgd2-xpm-dev  
sudo apt-get install libmagic-dev  
gcc -lm -lgd -lmagic -o pisstv pisstv.c  
sudo ./pisstv image.png 22050

## DragonOS

DragonOS is a Linux distribution that’s designed for software-defined radio (SDR) exploration. It comes with many open-source SDR programs pre-installed, including:  
Kismet, Kismon, GNU Radio 3.10, GR-Iridium, GR-Tempest, GR-RDS.  
**DragonOS supports SDRs like the:**RTL-SDR, HackRF, LimeSDR.

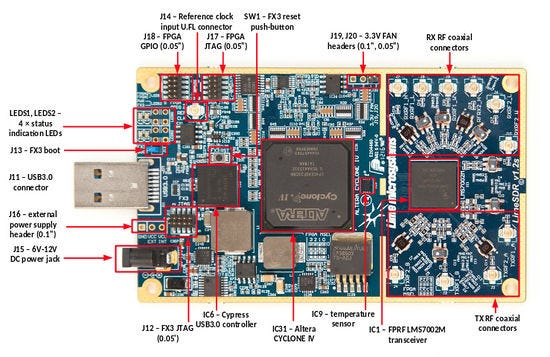
Press enter or click to view image in full size



https://cemaxecuter.com/ DOWNLOAD USING THIS LINK

## LimeSDR

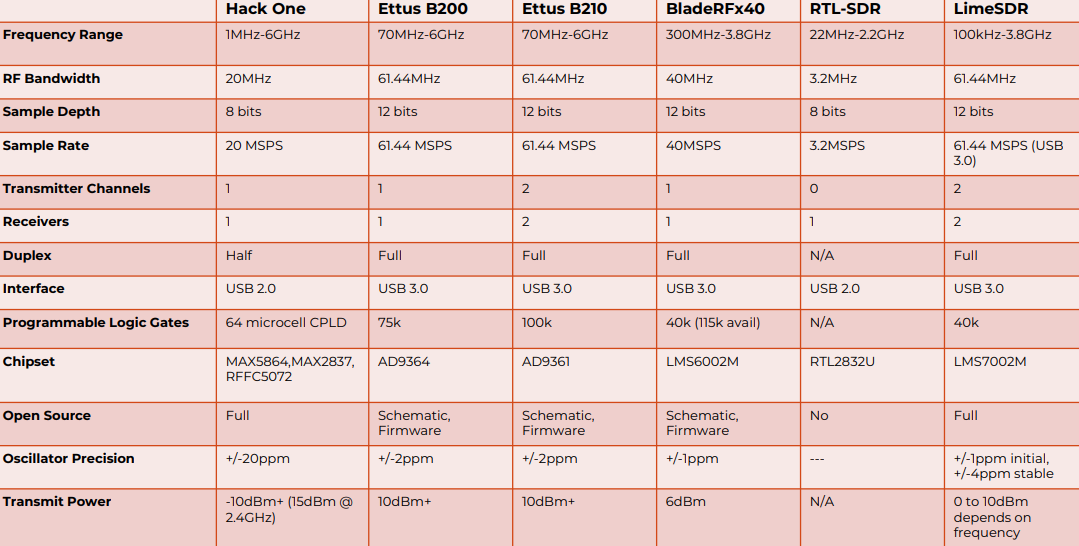
LimeSDR is a low-cost, open-source, apps-enabled software-defined radio (SDR) platform that can be used to support just about any type of wireless communication standard. It can transmit and receive UMTS, LTE, GSM, LoRa, Bluetooth, Zigbee, RFID, and Digital Broadcasting, among others. While most SDRs have remained in the domain of RF and protocol experts, LimeSDR is usable by anyone familiar with the idea of an app store. This means you can easily download new LimeSDR apps from developers around the world. If you’re a developer yourself, you can share and/or sell your LimeSDR apps through Snappy Ubuntu Core as well. The LimeSDR platform gives system developers, inventors, and even students an intelligent and flexible device for manipulating wireless signals, so they can learn, experiment, and develop products and applications.



**LimeSDR Types**

1. **LimeSDR-Mini**: This is a software-defined radio (SDR) board that uses a USB3 interface.
2. **LimeSDR-USB**: Similar to the Mini, this SDR board also uses a USB3 interface.
3. **LimeNET-Micro**: This SDR board comes with a Raspberry Pi (Compute Module) CM3 and uses a USB2 interface.
4. **LimeSDR-PCIe**: This SDR board uses a PCIe (1.0 x4) interface.
5. **LimeSDR-QPCIe**: This SDR board also uses a PCIe (1.0 x4) interface but comes with two LMS7002M transceivers.
6. **LimeSDR GPIO Board**: This is an expansion board that provides individually settable, bi-directional level-shifted I/O for FPGA GPIO 0–7.

Press enter or click to view image in full size



## GSM NETWORK

**BTS (Base Transceiver Station)**A BTS is like a Wi-Fi access point that communicates with a centralized controller, the BSC (Base Station Controller). The BTS handles the transmission and reception of baseband data, getting most of its commands from the BSC.

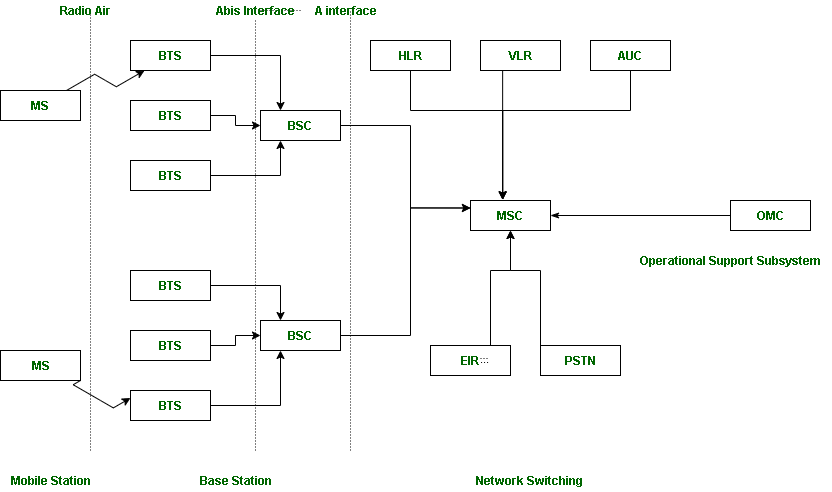
**BSC (Base Station Controller)** The BSC acts as a primary controller for one or more BTS. It configures most of the parameters on the BTS and brings each one up on air after they’re ready.

**MSC (Mobile Switching Center)** The MSC is responsible for routing voice calls and SMS. It sets up and releases end-to-end connections, handles mobility and hand-over requirements during the call, and manages billing and real-time prepaid account monitoring.

**Media Gateway (MGW)** A Media Gateway is a translation device or service that converts media streams between different telecommunications technologies such as 2G, 2.5G, 3G. One of its main functions is to convert between different transmission and coding techniques.

**Home Location Register (HLR)** The HLR is a main database in a GSM network which saves all permanent information about a subscriber, for example, billing details, subscriber identity, current status in the network, and many other things.

Press enter or click to view image in full size

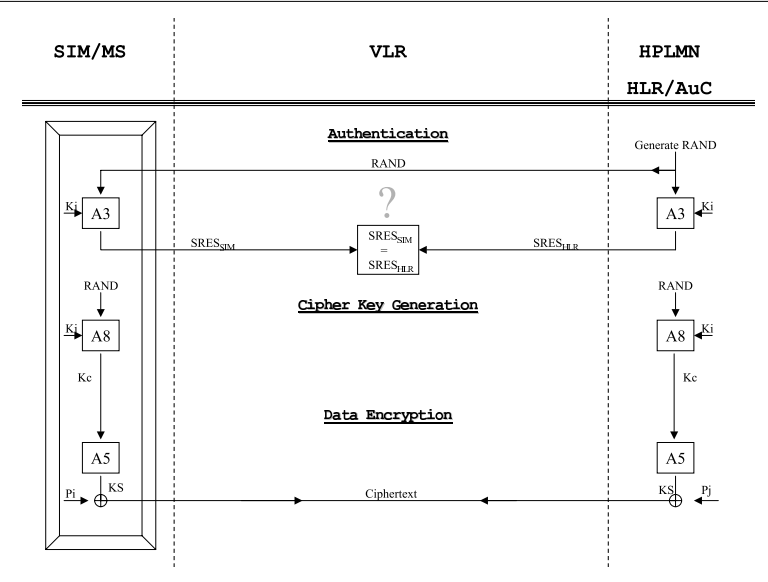


Source:<https://www.geeksforgeeks.org/gsm-in-wireless-communication/>

## Communication between SIM and HLR

The network and SIM both contain a secret key (K) for authentication. The key is never exposed to the subscriber and never transmitted over the air. When a user wants to authenticate, the HLR generates a RAND key, encrypts it with the (K) key, and generates a signed response known as SRES. The HLR also sends the same RAND key to the subscriber. The SIM encrypts this RAND key with the (K) key and generates SRES. The SIM then sends the generated SRES to the network. If the SRES from the SIM matches with the network-generated SRES, then the SIM is authenticated.

Press enter or click to view image in full size



Source:<https://eprint.iacr.org/2004/158.pdf>

**The Home Location Register (HLR) is a functional unit that manages mobile subscribers. It stores data such as:**

* International Mobile Subscriber Identity (IMSI)
* Mobile Subscriber ISDN Number (MSISDN)
* Authentication keys
* Service profiles

The HLR is updated each time a device moves to a new location. It also facilitates SMS by scanning for the mobile switching center (MSC) used by the receiving party.

**The HLR communicates with the SIM card in the following ways:**

* The HLR identifies the last known location of the device.
* The HLR stores a teleservice list for voice and SMS.
* The HLR transfers the list of services to VLR/MSC.
* The roaming network uses the information to allow or disallow the call.
* The HLR updates the VLR address when the subscriber moves from one VLR to another.

**Each mobile network operator has its own HLR.**

## Iridium Satellites

Iridium satellites were built by Motorola .There are 66 active satellites across the globe which covers the entire Earth surface .These satellites are in low Earth orbit at a height of approximately 781 kilometers . The Iridium system was launched on November 1, 1998, and it has changed global communications. The Iridium satellites provides L band voice and data information.The satellites are cross-linked and operate as a fully meshed network. They are the largest constellation and orbit closer to Earth than other networks. The Iridium network covers the entire Earth, including poles, oceans, and airways.

Press enter or click to view image in full size



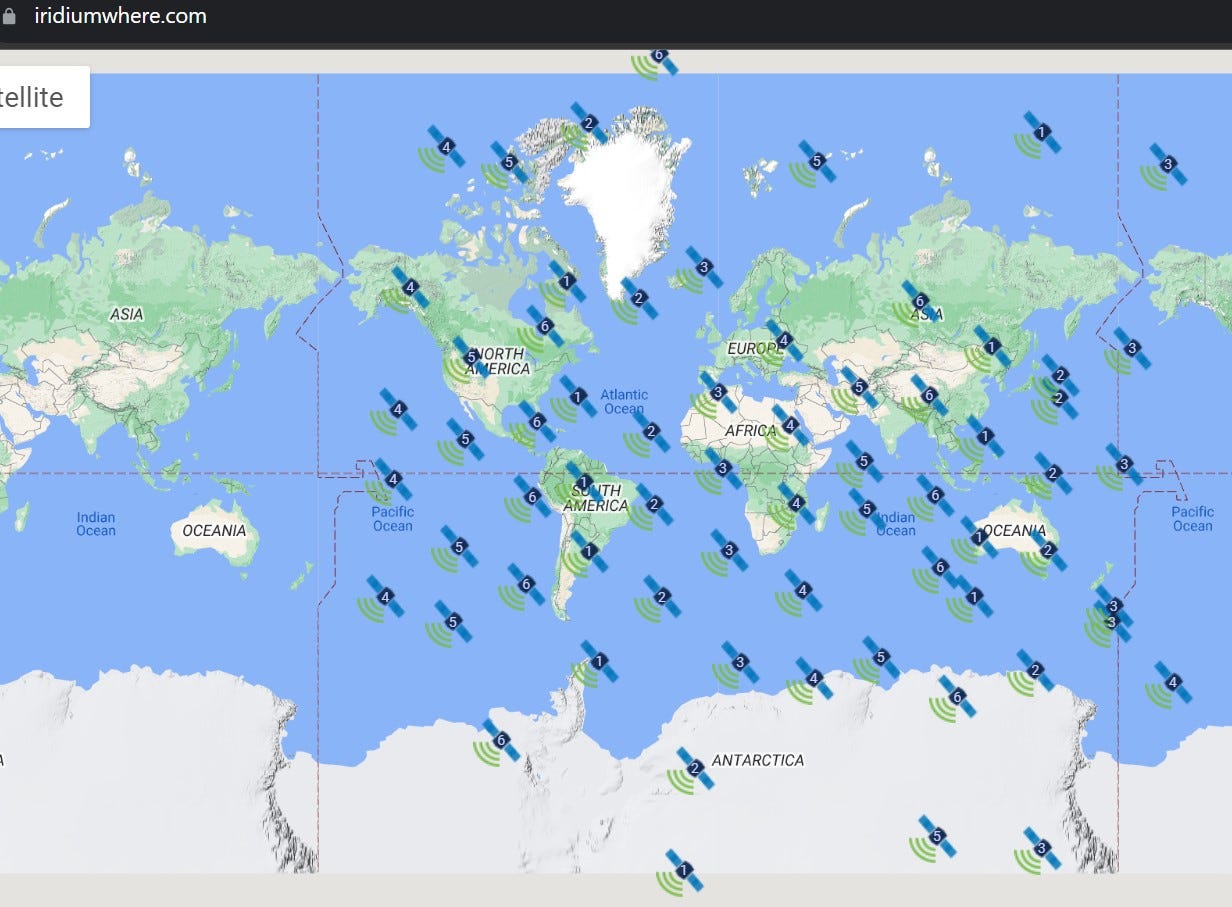
Source:<https://iridiumwhere.com/about/>

**The Iridium satellites have the following characteristics:**

* They are low-earth orbiting (LEO)
* They orbit in an 86.4° inclined orbit
* They take about 100 minutes to orbit the Earth, and about 10 minutes from horizon to horizon
* They use GSM-based telephony architecture
* They provide global roaming

https://www.iridium.com/

Press enter or click to view image in full size



### Services Provided by Iridium Satellites

* Paging
* Global Burst Data
* Voice / SMS
* Short Burst Data
* Time and Locations services

**Applications of Iridium Satellite**

* Tracking
* Mobile Data/Voice
* Emergency Services
* Aircraft communication
* Covert Operations

## Receiving data using gr-iridium

## [GitHub - muccc/gr-iridium: Iridium burst detector and demodulator.](https://github.com/muccc/gr-iridium?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)

### **[Iridium burst detector and demodulator. Contribute to muccc/gr-iridium development by creating an account on GitHub.](https://github.com/muccc/gr-iridium?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)**

[github.com](https://github.com/muccc/gr-iridium?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)

iridium-extractor -D 4 DEVICE.conf | grep "A:OK" > FILE\_NAME.bits

## Decoding data using iridium toolkit

## [GitHub - muccc/iridium-toolkit: A set of tools to parse Iridium frames](https://github.com/muccc/iridium-toolkit?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)

### **[A set of tools to parse Iridium frames. Contribute to muccc/iridium-toolkit development by creating an account on…](https://github.com/muccc/iridium-toolkit?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)**

[github.com](https://github.com/muccc/iridium-toolkit?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)

pypy iridium-parser.py -p FILE\_NAME.bits > FILE\_NAME.parsed

## Decoding Voice data using iridium toolkit

## [GitHub - muccc/iridium-toolkit: A set of tools to parse Iridium frames](https://github.com/muccc/iridium-toolkit?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)

### **[A set of tools to parse Iridium frames. Contribute to muccc/iridium-toolkit development by creating an account on…](https://github.com/muccc/iridium-toolkit?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)**

[github.com](https://github.com/muccc/iridium-toolkit?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)

# Path Setup  
export PATH=$PATH:/usr/src/iridium-toolkit  
# Command  
./stats-voc.py FILE\_NAME.parsed

## Decoding other data using iridium toolkit

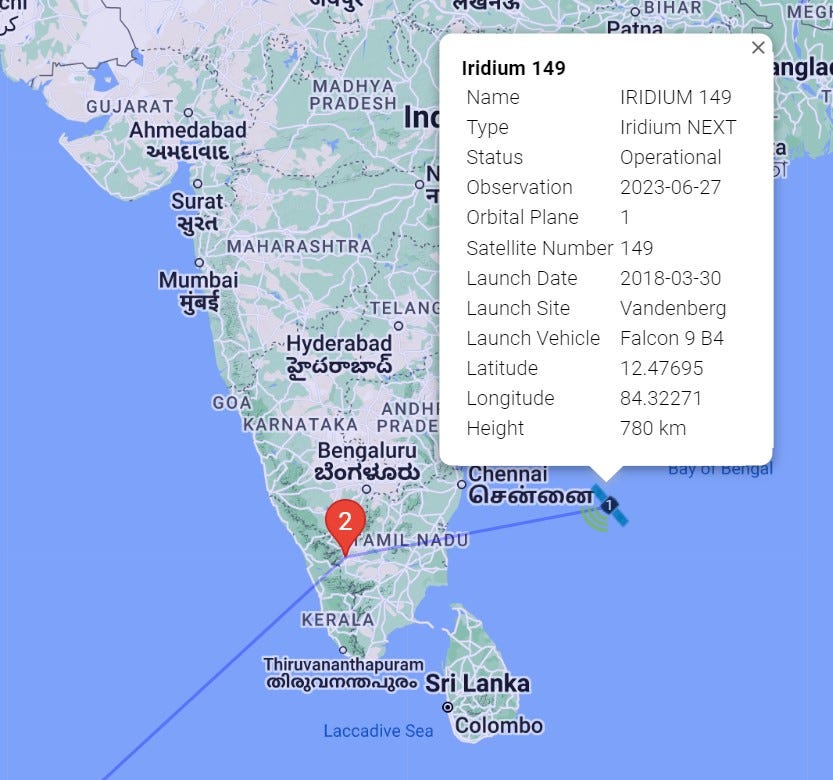
## [GitHub - muccc/iridium-toolkit: A set of tools to parse Iridium frames](https://github.com/muccc/iridium-toolkit?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)

### **[A set of tools to parse Iridium frames. Contribute to muccc/iridium-toolkit development by creating an account on…](https://github.com/muccc/iridium-toolkit?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)**

[github.com](https://github.com/muccc/iridium-toolkit?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)

sudo ./reassembler.py -i FILE\_NAME.parsed -m <mode>  
ida - outputs Um Layer 3 messages as hex  
lap - GSM-compatible L3 messages as GSMtap compatible .pcap  
page - paging requests (Ring Alert Channel)  
msg - Pager messages

Press enter or click to view image in full size



## Inmarsat Satellite

Inmarsat is a British company that provides global mobile services through 14 geostationary satellites. These satellites allow for constant communication between the satellite and its corresponding ground station. Inmarsat’s services are vital for industries, governments, and aid agencies that need to communicate in remote areas or where there is no reliable terrestrial network. It’s especially valuable for the shipping, airline, and mining industries. Inmarsat was originally established as an intergovernmental organization in 1979 and was privatized in the late 1990s. Despite these changes, Inmarsat continues to play a crucial role in global communications. In addition to its current fleet of satellites, Inmarsat plans to launch another seven satellites to further enhance its network. This will allow it to offer even more reliable and comprehensive services to its users around the globe. Inmarsat also provides services that support email, internet, video conferencing, and in-flight Wi-Fi. For example, the Inmarsat-5 (I-5) satellite is used primarily for mobile broadband communications for deep-sea vessels and in-flight connectivity for airline passengers. In November 2021, a deal was announced between Inmarsat’s owners and Viasat, an American communications company. Viasat completed the acquisition of Inmarsat in May 2023.

Press enter or click to view image in full size



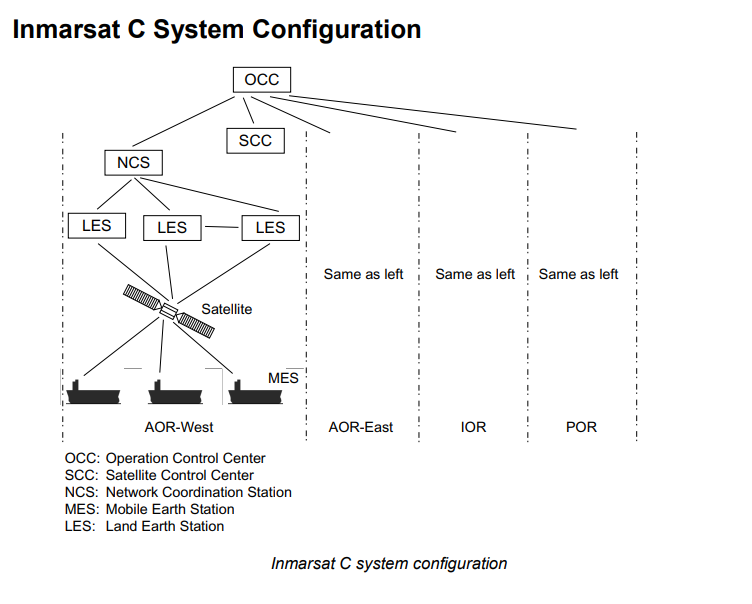
Source:<https://sky-brokers.com/satellite/inmarsat-5-f1-inmarsat-gx1-is-ior-at-63-east/>

## Inmarsat System

The Inmarsat System is a complex network of components that work together to provide global mobile services.

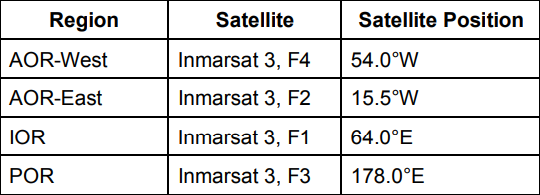
1. **Operation Control Center (OCC):**The OCC is responsible for the overall operation of the Inmarsat network. It monitors the performance of the network and coordinates with other components to ensure smooth operation.
2. **Satellite Control Center (SCC):**The SCC manages the satellites in the Inmarsat system. It controls the positioning of the satellites and monitors their health and performance.
3. **Network Coordination Station (NCS):** The NCS keeps track of all Inmarsat C transceivers in its region and broadcasts information such as navigational warnings, weather reports, and news. There is one NCS in each region.
4. **Mobile Earth Station (MES):**The MES is a portable or mobile terminal that communicates with the Inmarsat satellites. It can be used to send and receive voice and data services.
5. **Land Earth Station (LES):** The LES provides the link between the MES and the terrestrial telecommunications networks via satellite. There are several LESs in each region.

Press enter or click to view image in full size



Source:<https://www.marinsat.com/marinsat/dosyalar/dosya/Furuno_Felcom-16_Operation_Manual.pdf>

The Inmarsat C system divides the world into four regions and each region is covered by its own satellite.

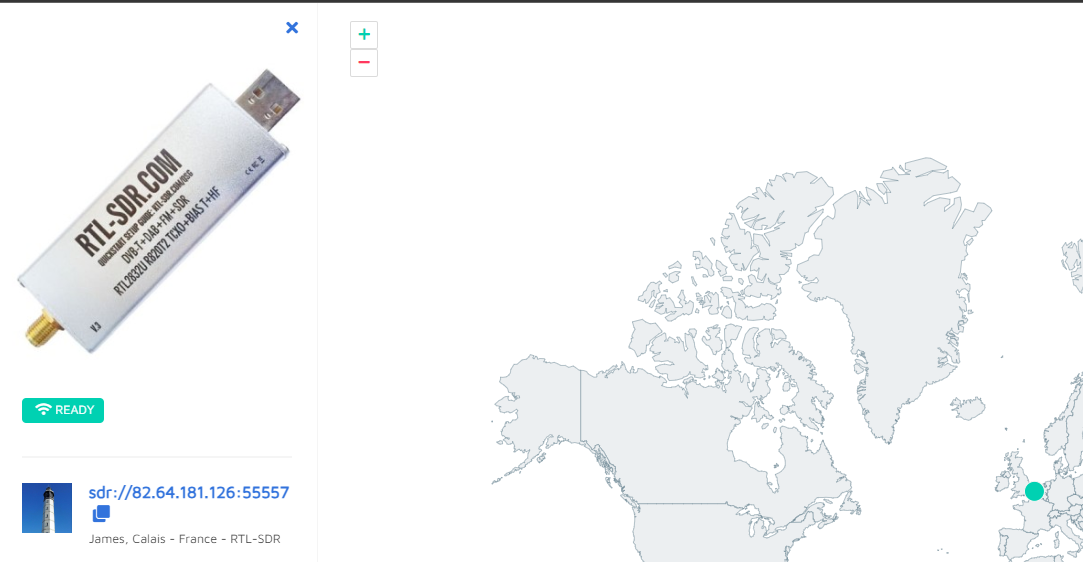


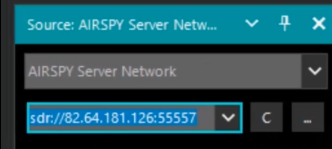
In each region, there is one NCS and several LESs. The NCS keeps track of all Inmarsat C transceivers in its region and broadcasts information such as navigational warnings, weather reports, and news. The LESs provide the link between the MES and the terrestrial telecommunications networks via satellite.

## Setup Inmarsat Decoding with Scytale-C

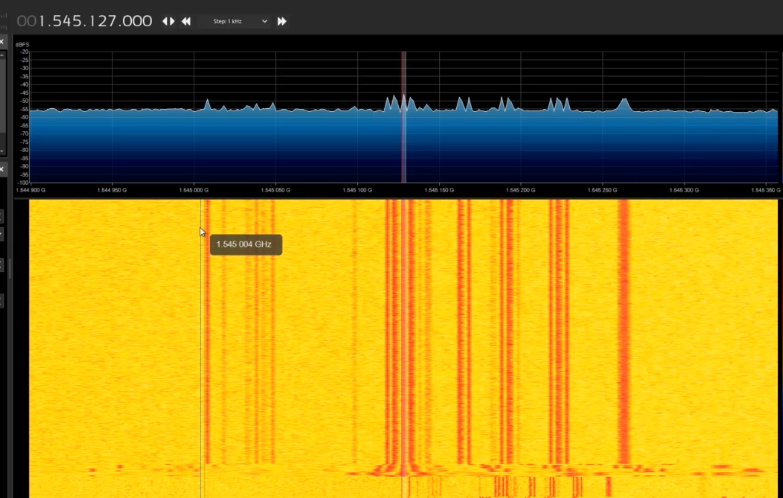
Data Receiving with SDR Sever  
https://airspy.com/directory/

Press enter or click to view image in full size





Press enter or click to view image in full size



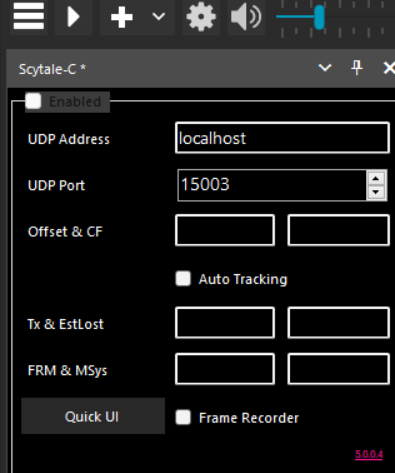
## Download Scytale-C Plugin for SDR#

## [Downloads](https://bitbucket.org/scytalec/scytalec/downloads/?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)

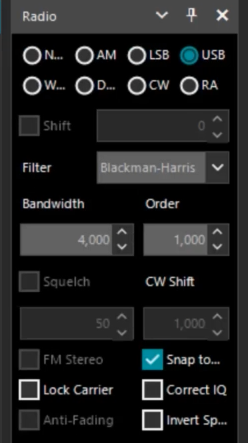
### **[Edit description](https://bitbucket.org/scytalec/scytalec/downloads/?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)**

[bitbucket.org](https://bitbucket.org/scytalec/scytalec/downloads/?source=post_page-----296a84d18ba7---------------------------------------" \t "_blank)

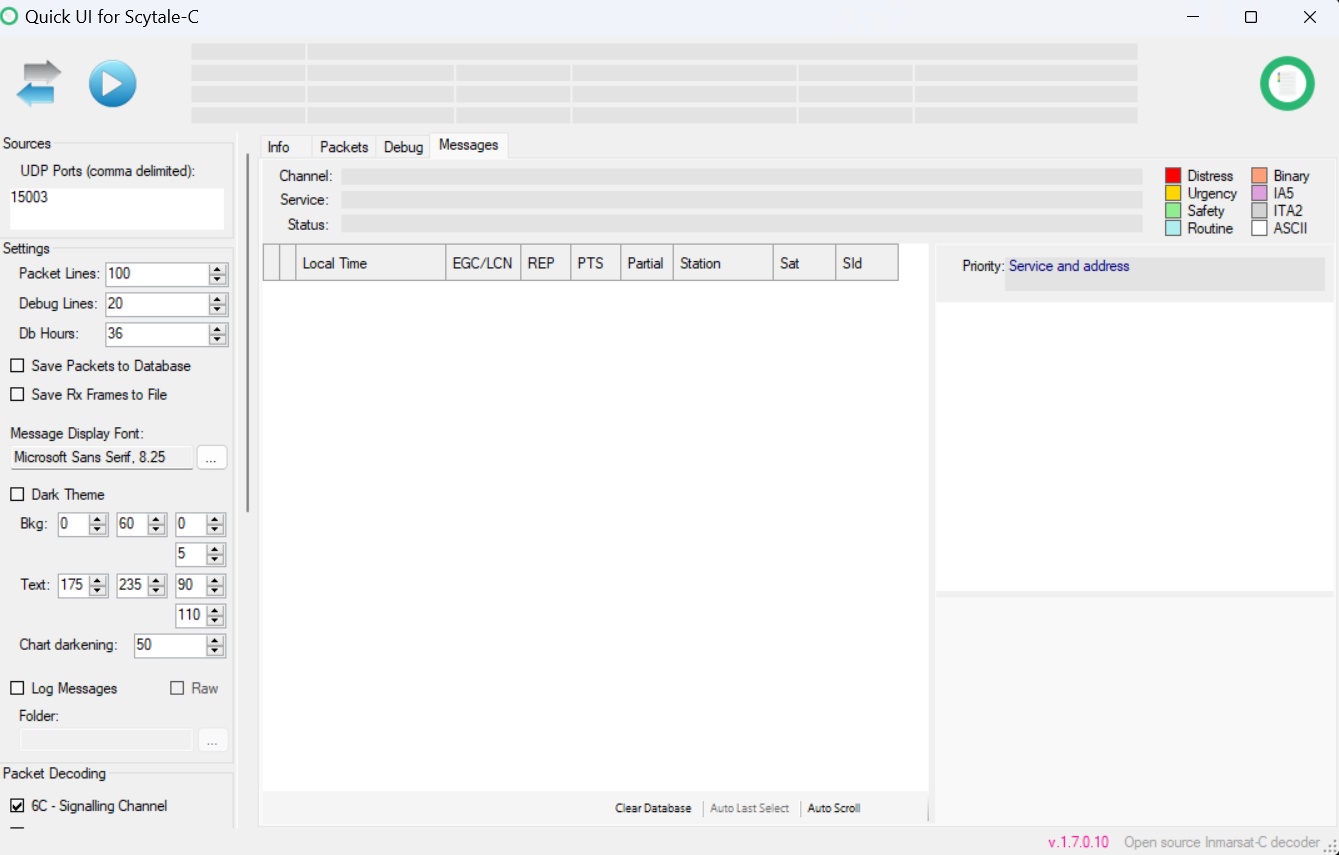
The Scytale-C Plugin for SDR# is a tool developed by Microp11 for decoding Inmarsat STD-C signals. It’s currently in the pre-alpha stages, which means it may still be missing some functionality and could be buggy. However, it is functional at this point in time.



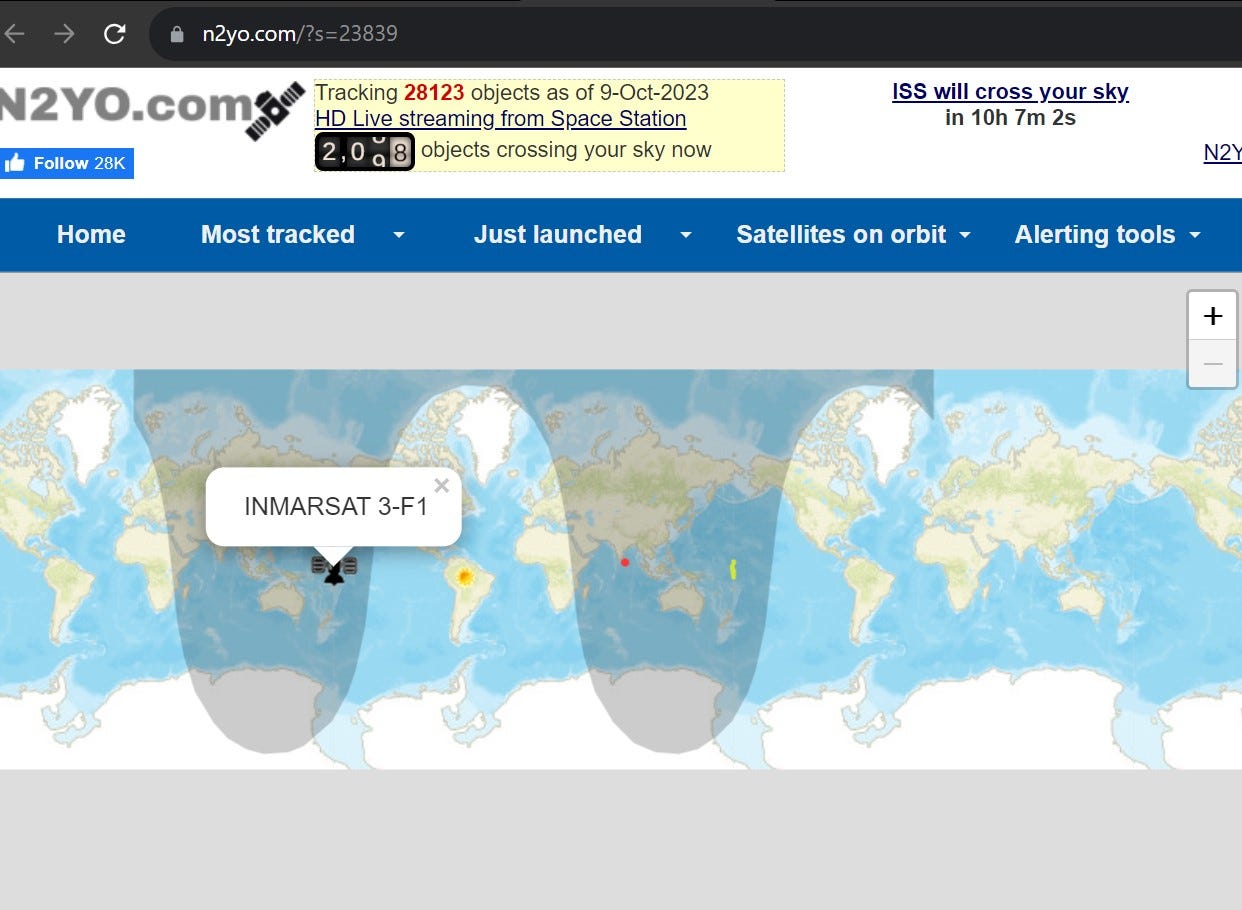
Select Enabled and also Auto Tracking option.  
**Decoding Data of Inmarsat with scytale**In radio use USB and BW of 4,000 and make sure snap to grid is checked.



Press enter or click to view image in full size



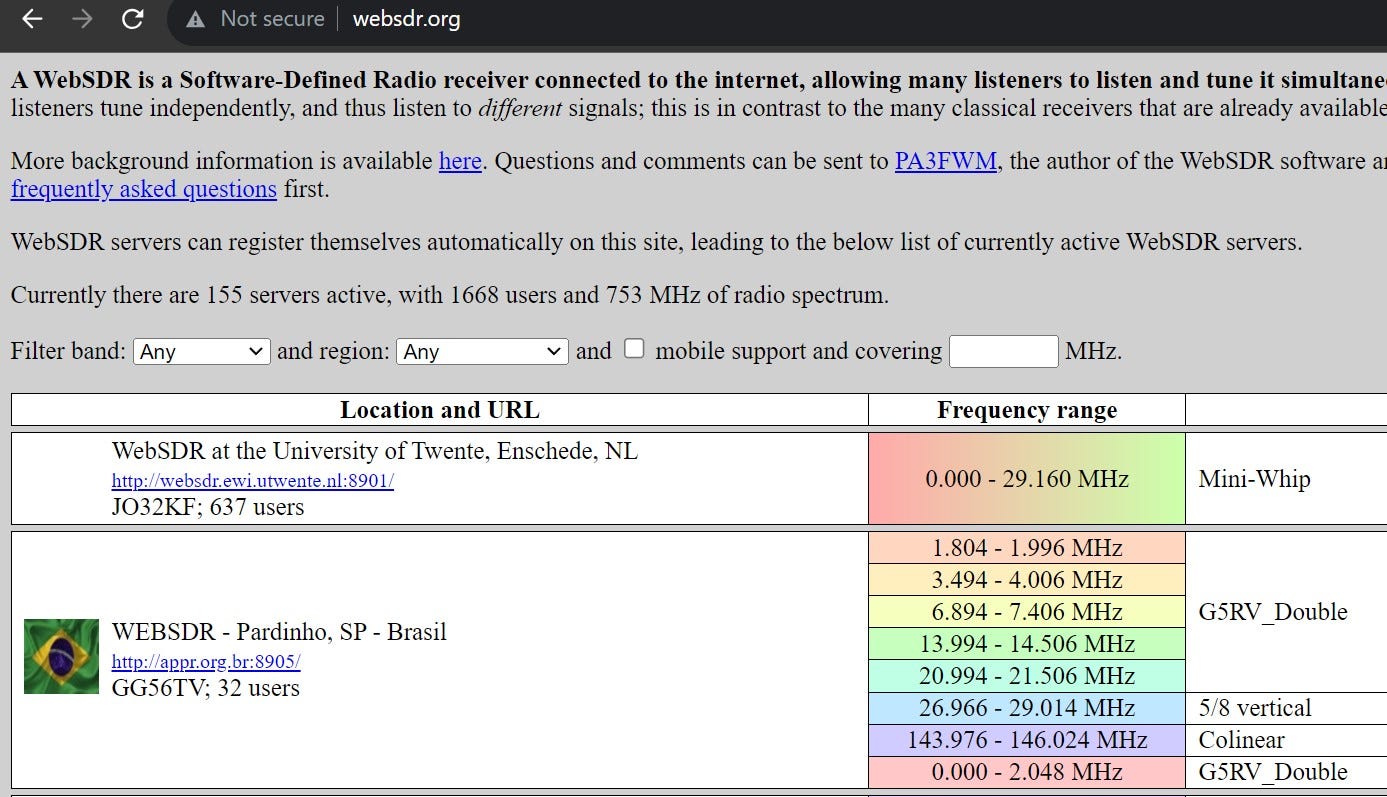
Press enter or click to view image in full size



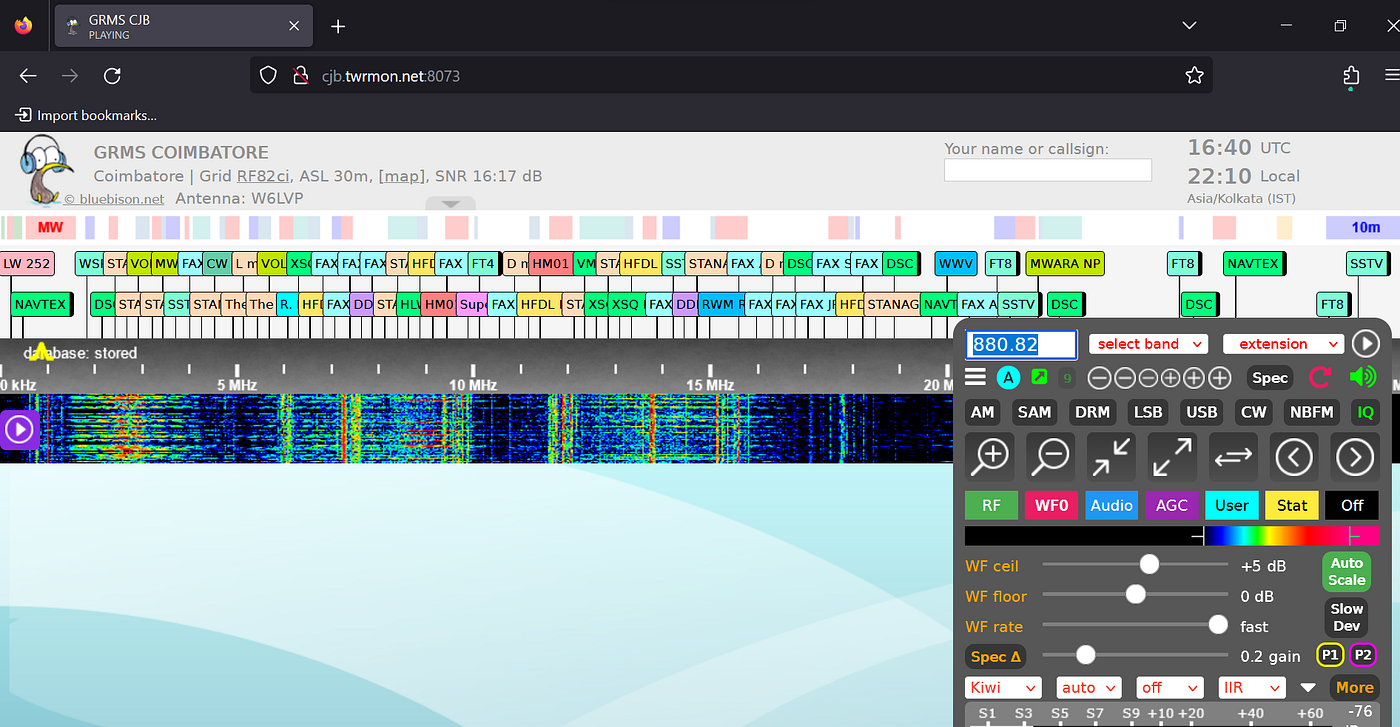
## WebSDR

WebSDR, or Web Software-Defined Radio, is a revolutionary technology that allows multiple listeners to tune into a radio receiver connected to the internet simultaneously. This is a significant departure from traditional receivers available online, which do not offer this level of flexibility. With WebSDR, each listener can tune independently, meaning they can listen to different signals at the same time. This is made possible by the advancements in SDR technology.In India, there are several active WebSDRs available. These include GRMS Bengaluru, GRMS New Delhi, New Delhi websdr, GRMS Siliguri, GRMS Dimapur, and GRMS Coimbatore. Each of these WebSDRs offers unique features and covers different frequency ranges, providing a wide array of options for listeners.

Press enter or click to view image in full size



Press enter or click to view image in full size



GMRS COIMBATORE -<http://cjb.twrmon.net:8073/>

[Internet SDR List — Auto Updating Global Coverage (skywavelinux.com)](https://skywavelinux.com/best-sdrservers.html) **List of active webSDRs available in India**

* [GRMS Coimbatore](http://cjb.twrmon.net:8073/)
* [GRMS Vadodra](http://182.237.12.150:8073/)
* [GRMS Dimapur](http://103.232.186.40:8073/)
* [GRMS Siliguri](http://103.82.159.8:8073/)

## Thanks For Reading :)

Don’t miss out on my upcoming articles! [**Follow me**](https://medium.com/@kishoreramk)on Medium for more insightful content. Clap and share this article to spread the knowledge among fellow bug bounty hunters and cybersecurity enthusiasts.

If you have any further questions or would like to connect, feel free to reach out to me

My LinkedIn handle: <https://www.linkedin.com/in/kishoreram-k/>

[Hacking](https://medium.com/tag/hacking?source=post_page-----296a84d18ba7---------------------------------------)

[Cybersecurity](https://medium.com/tag/cybersecurity?source=post_page-----296a84d18ba7---------------------------------------)

[Blog](https://medium.com/tag/blog?source=post_page-----296a84d18ba7---------------------------------------)