Table of Contents

Jammer Frequency Ranges

This document outlines the frequency ranges that are disrupted by the Chinese radio jammer. The frequency ranges for the corresponding channels can be found in Table 1 and Figure 1 and the view of the spectrum can be viewed in the Spectrum view section. The hardware configuration of the jammer can be viewed in the Device Configuration Section.

Table 1: Jammer Frequency Ranges

Channel	Technology	Frequency	Frequency Range
1	PHS	1900 MHz	1890 MHz – 2010 MHz
2	CDMA	800 MHz	830 MHz – 990 MHz
	GSM	900 MHz	
3	DCS	1800 MHz	1790 MHz – 1920 MHz
4	4G	?	790 MHz – 2140 MHz
	WiFi (Bluetooth)	2400 MHz	2280 MHz – 2540 MHz
5	4G	700 MHz	710 MHz – 860 MHz
	TD	?	2140 MHz – 2560 MHz
6	GPS	1500 MHz	1560 MHz – 1640 MHz
7	3G	2100 MHz	2090 MHz – 2210 MHz
8	4G1	2600 MHz	2460 MHz – 2760 MHz

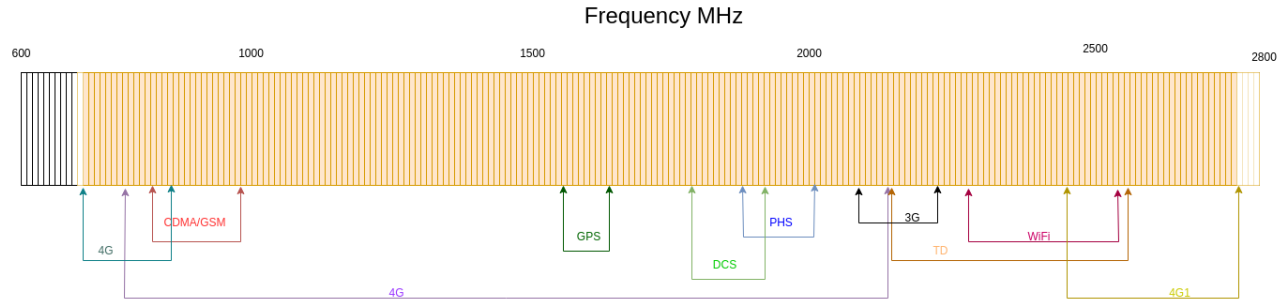


Figure 1: Illustration of the Frequency Range covered by the Jamming Device

Device Configuration

All antennas can be attached as the starting arrangement. The number written on the antenna corresponds to the port it should be attached to. The antenna also has the technology it supports written under the number. However, it is imperative that the dip switches are in the “off” position before the device is activated (switched on).

Figure 2: Jammer starting configuration

A switch in the “on” position means that jamming will occur on that channel even if the antenna for the corresponding channel is not attached. While an antenna may enhance the performance of the jammer, the switch ultimately decides if the channel will be disrupted.

Figure 3: Dip Switch Off/Start Position

To test the jamming frequency range for a channel, set the corresponding dip switch in the “on” position. Then device should then be turned on by flipping the the switch to “ON”. By setting the dip switch before turning ON the device, we can ensure that only that channel is disrupted and the jamming can be tested quickly without causing too much disturbance to legitimate traffic (i.e. flipping the ON switch is easier and faster than toggling the dip switches). The radio spectrum can then be monitored with an SDR to determine the frequency range.

Figure 4: Testing Jamming on One Channel/Technology (channel 6)

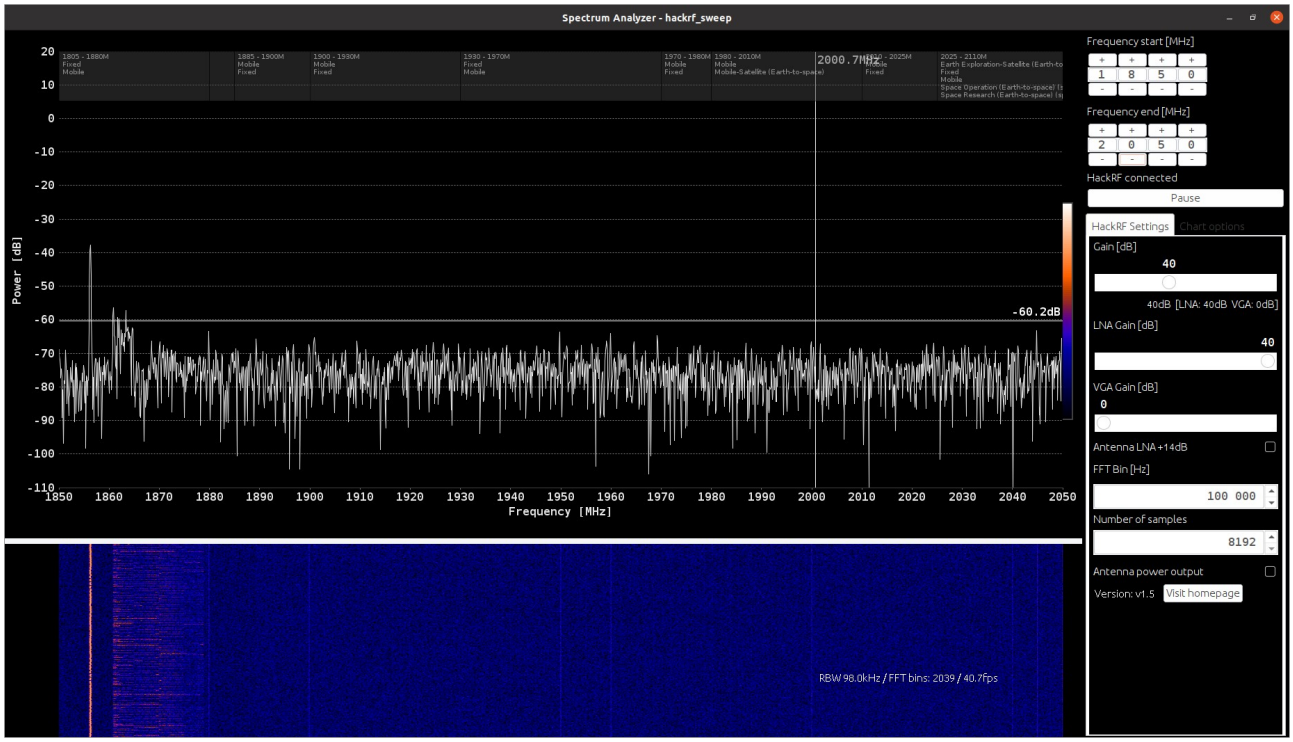
Some of the frequency ranges are quite wide so it may take a few tries to determine the start and end frequencies for the jamming range. As standard SDRs do not have the required bandwidth (in this case the chosen SDR was the HackRF[1] with a bandwidth of 20 MHz) to view the full jamming range, adjustments will need to be made to the software used to monitor the spectrum. As such the software chosen for this experiment was Spectrum Analyzer[2], which works exclusively with the HackRF to improve the viewing range of the spectrum

1 https://greatscottgadgets.com/hackrf/one/
2 https://github.com/pavsa/hackrf-spectrum-analyzer

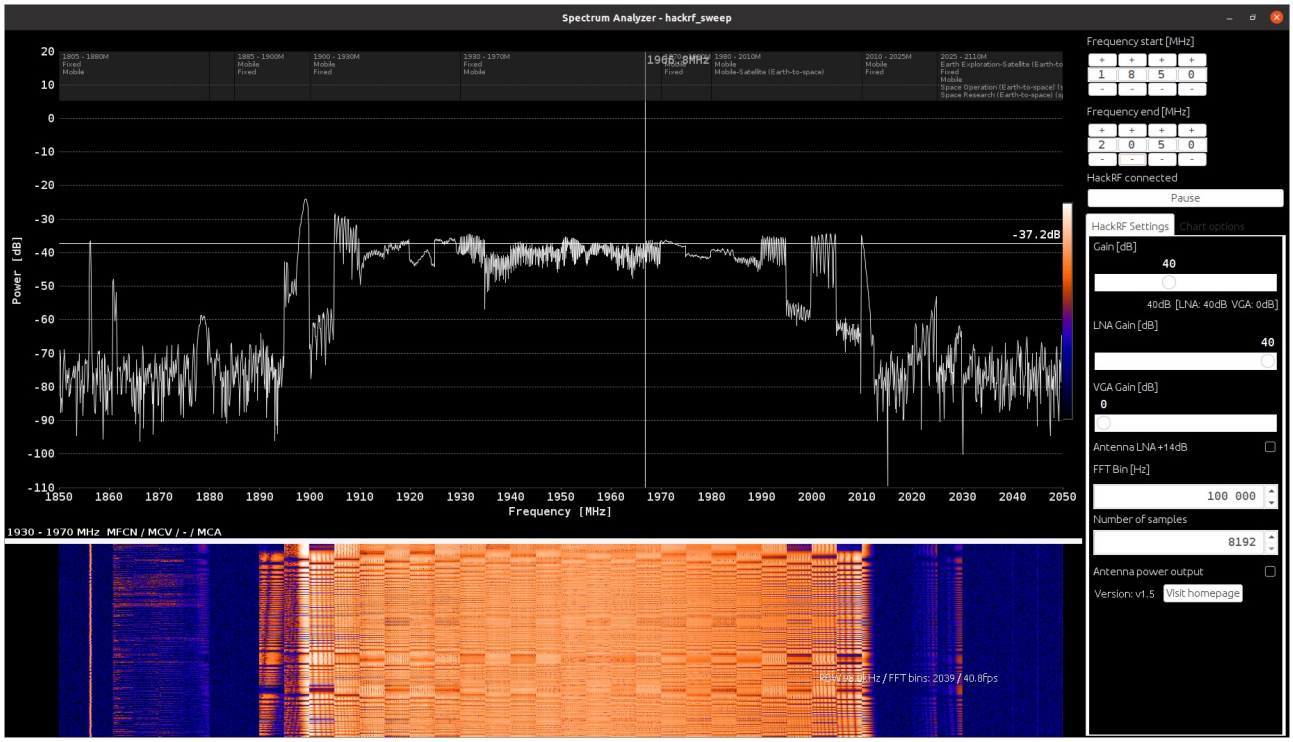
Spectrum Views

Channel 1

Before Jamming

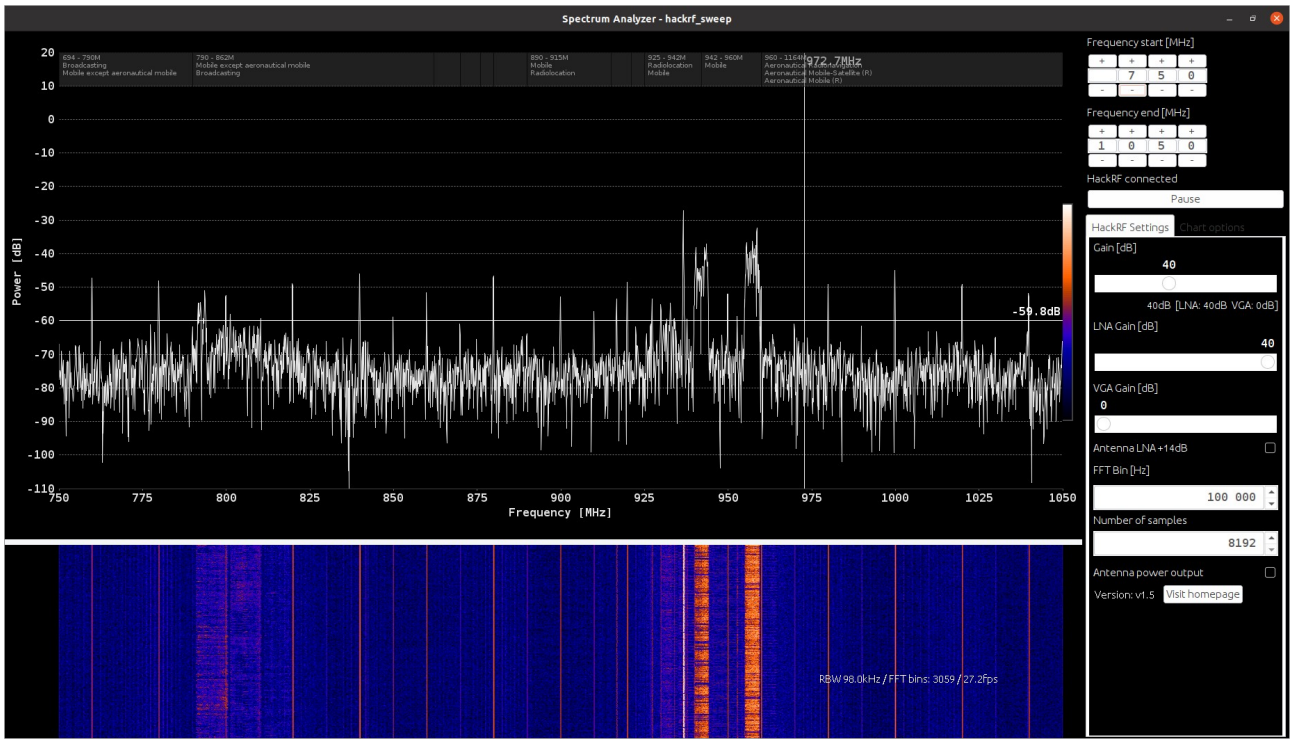


After Jamming

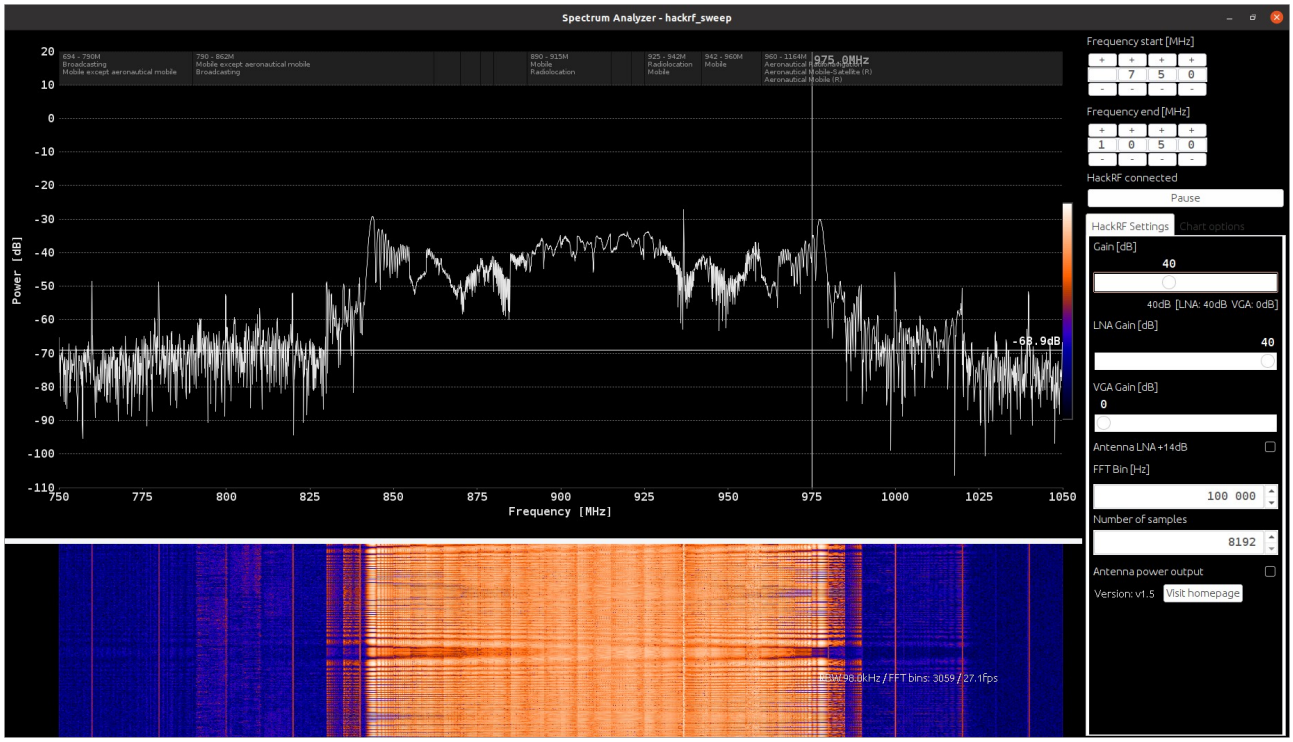


Channel 2

Before Jamming

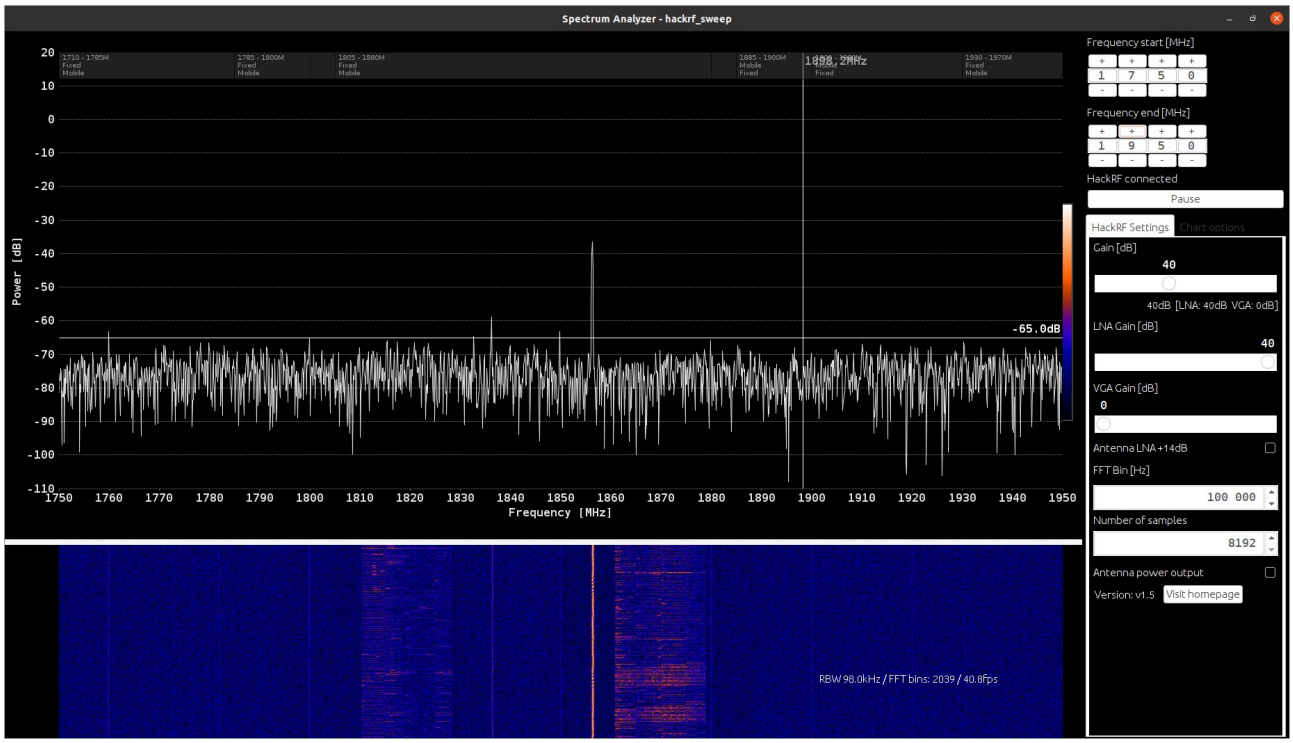


After Jamming

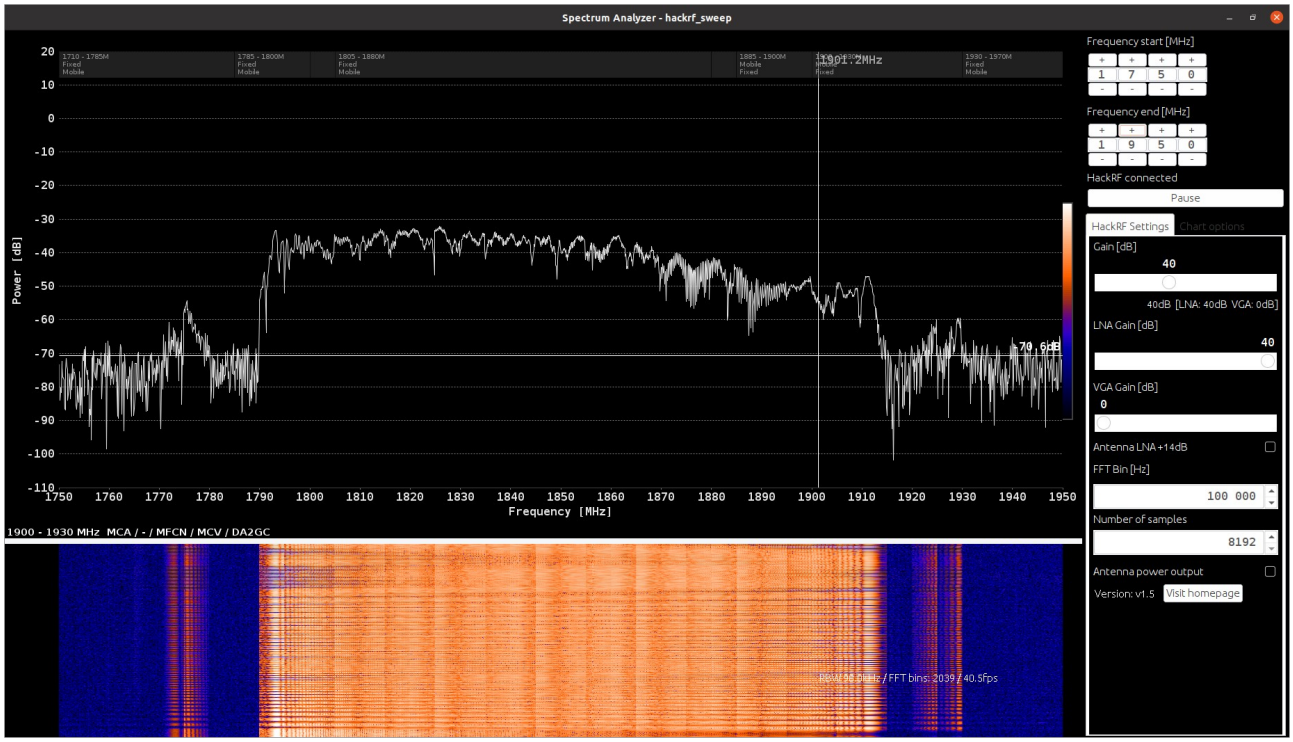


Channel 3

Before Jamming

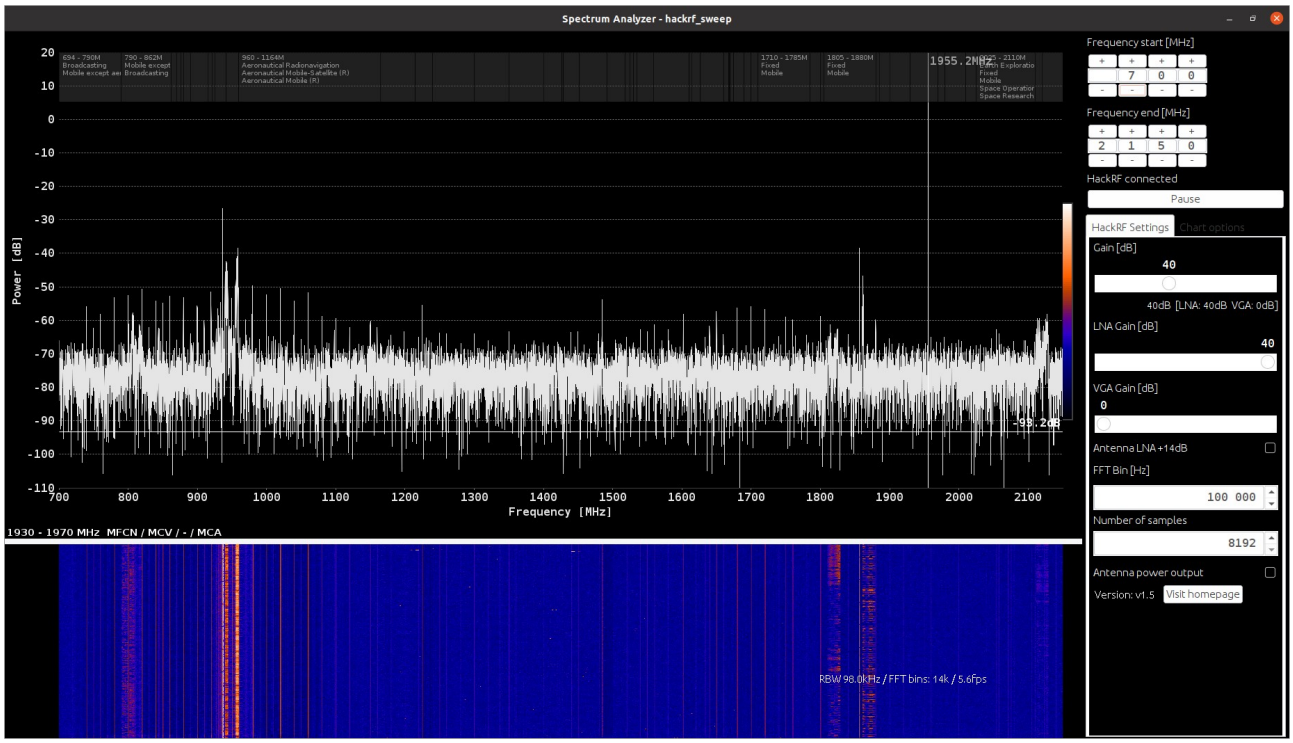


After Jamming

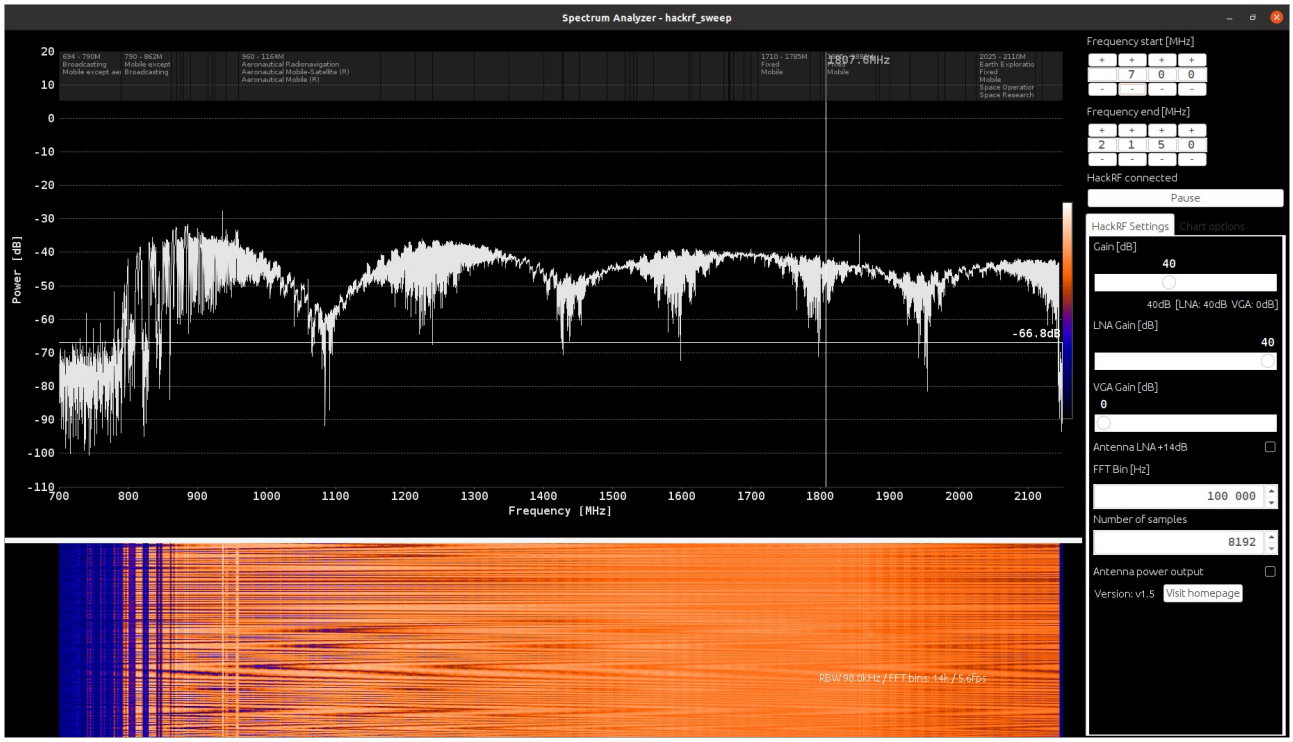


Channel 4

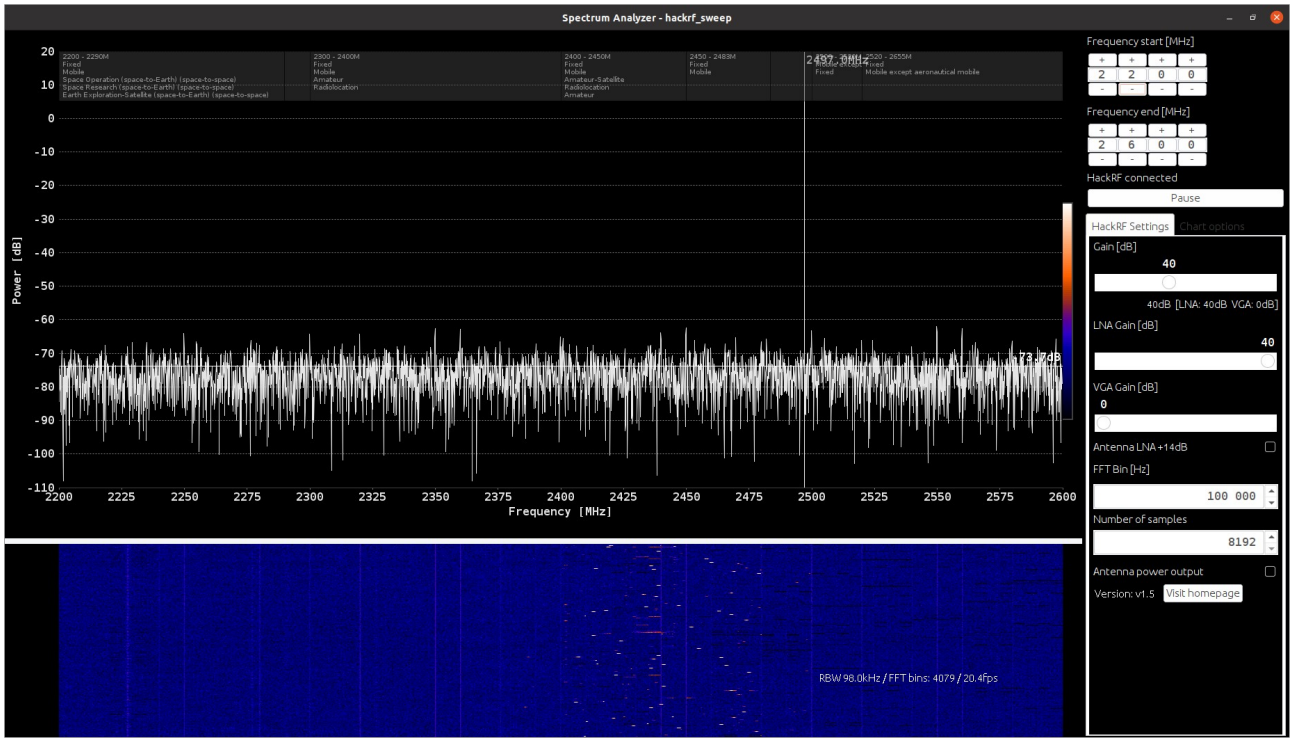
Before Jamming (4G Channel)



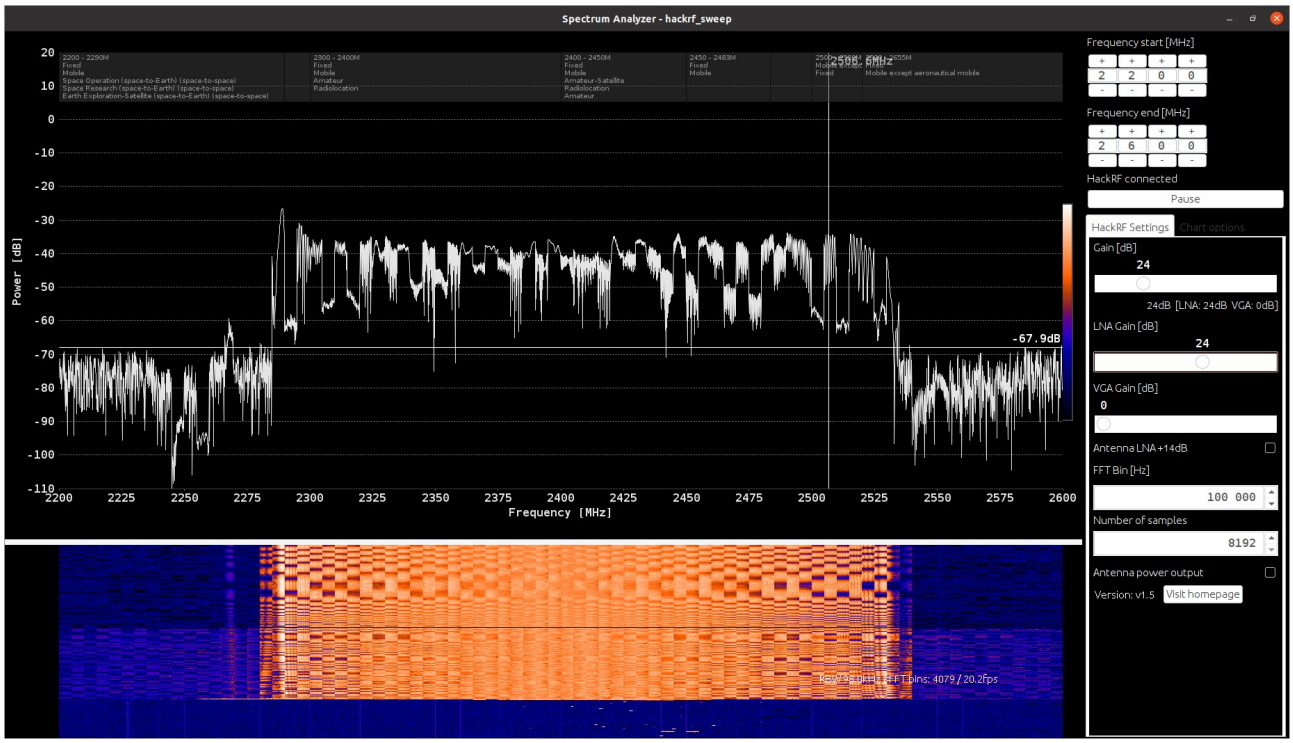
After Jamming (4G Channel)



Before Jamming (WiFi – 2.4 GHz ISM Channel)

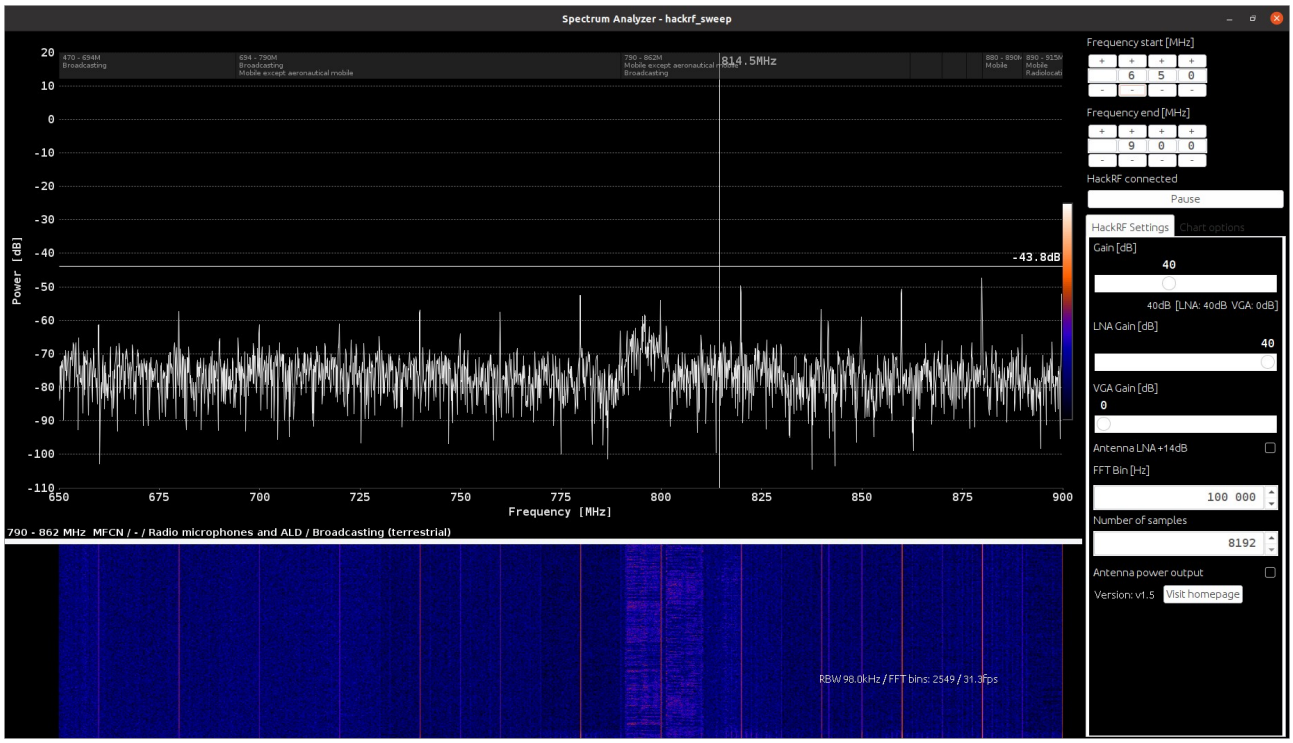


After Jamming (WiFi – 2.4 GHz ISM Channel)

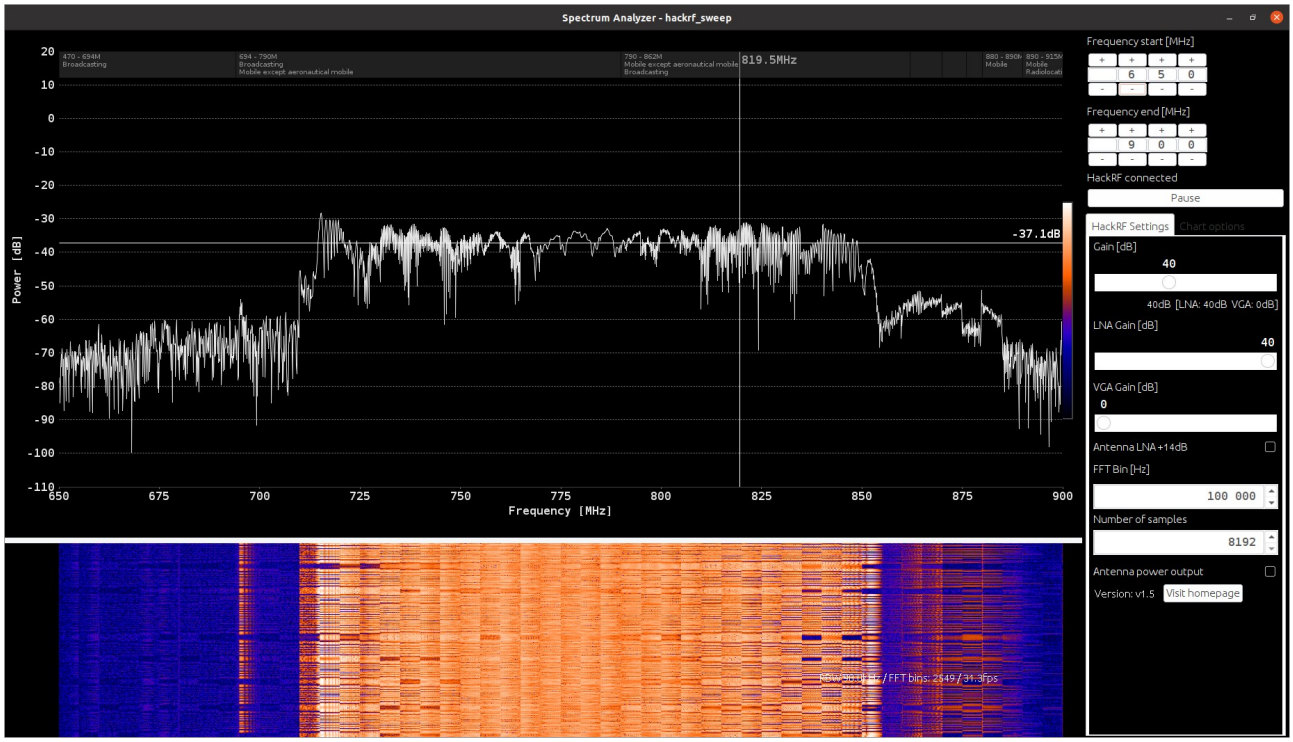


Channel 5

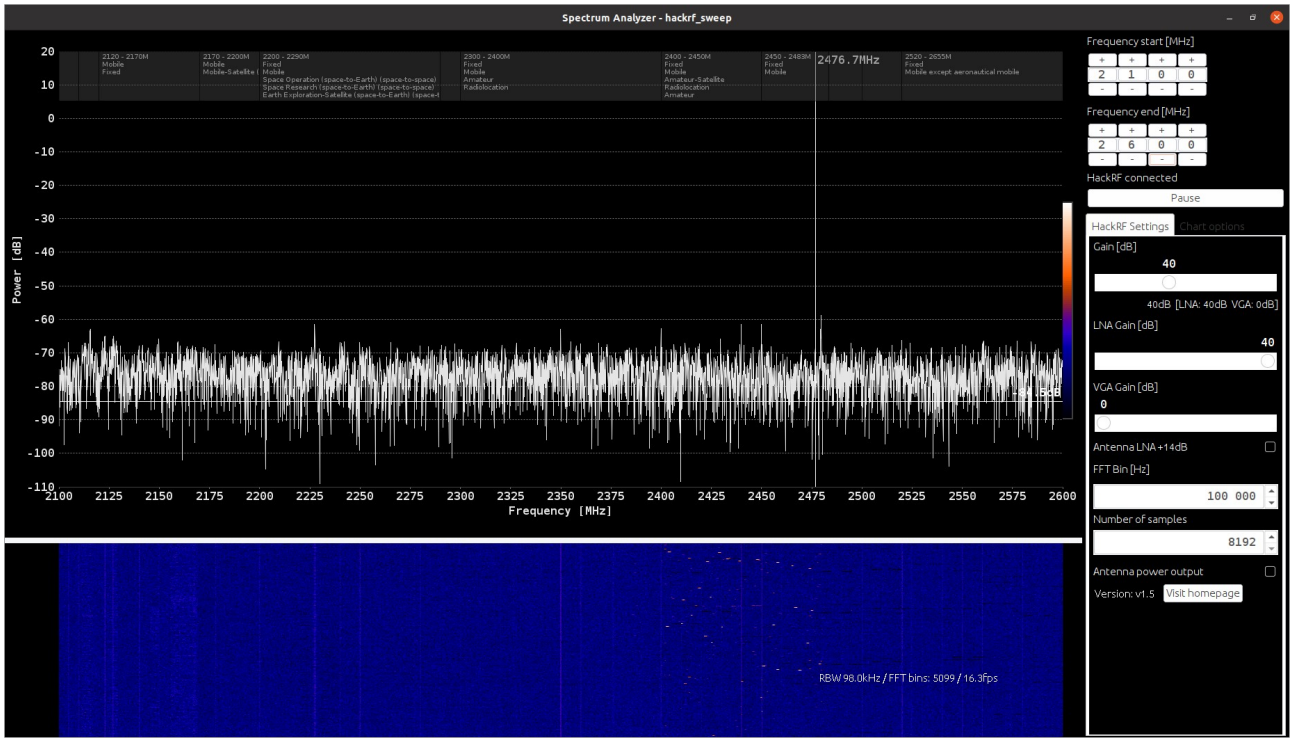
Before Jamming (4G Channel)



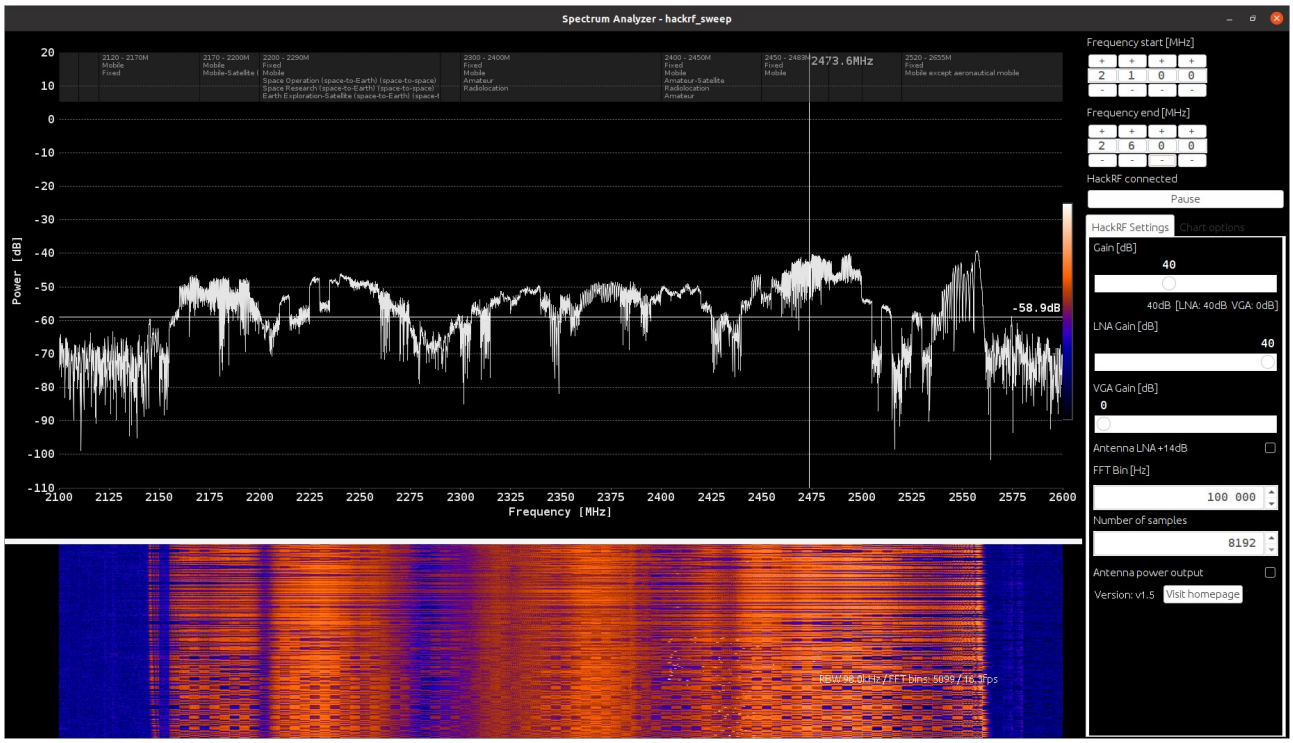
After Jamming (4G Channel)



Before Jamming (TD Channel)

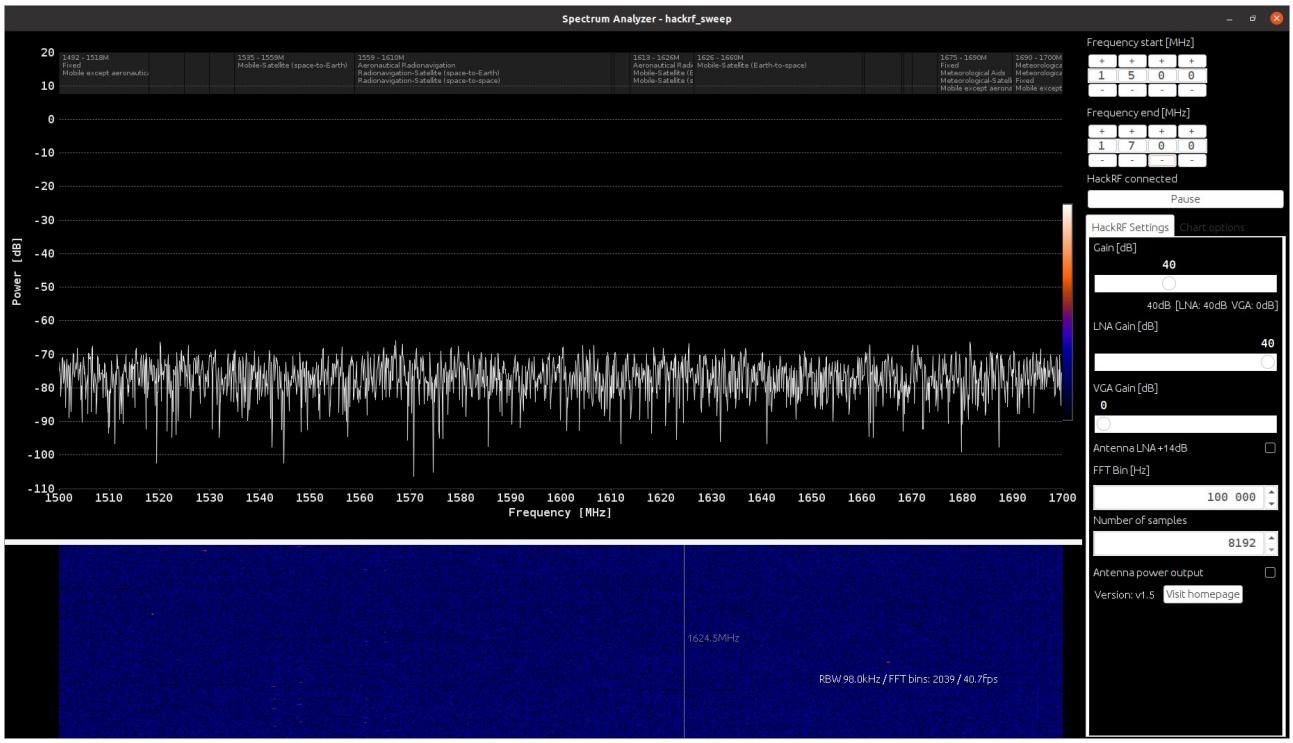


After Jamming (TD Channel)

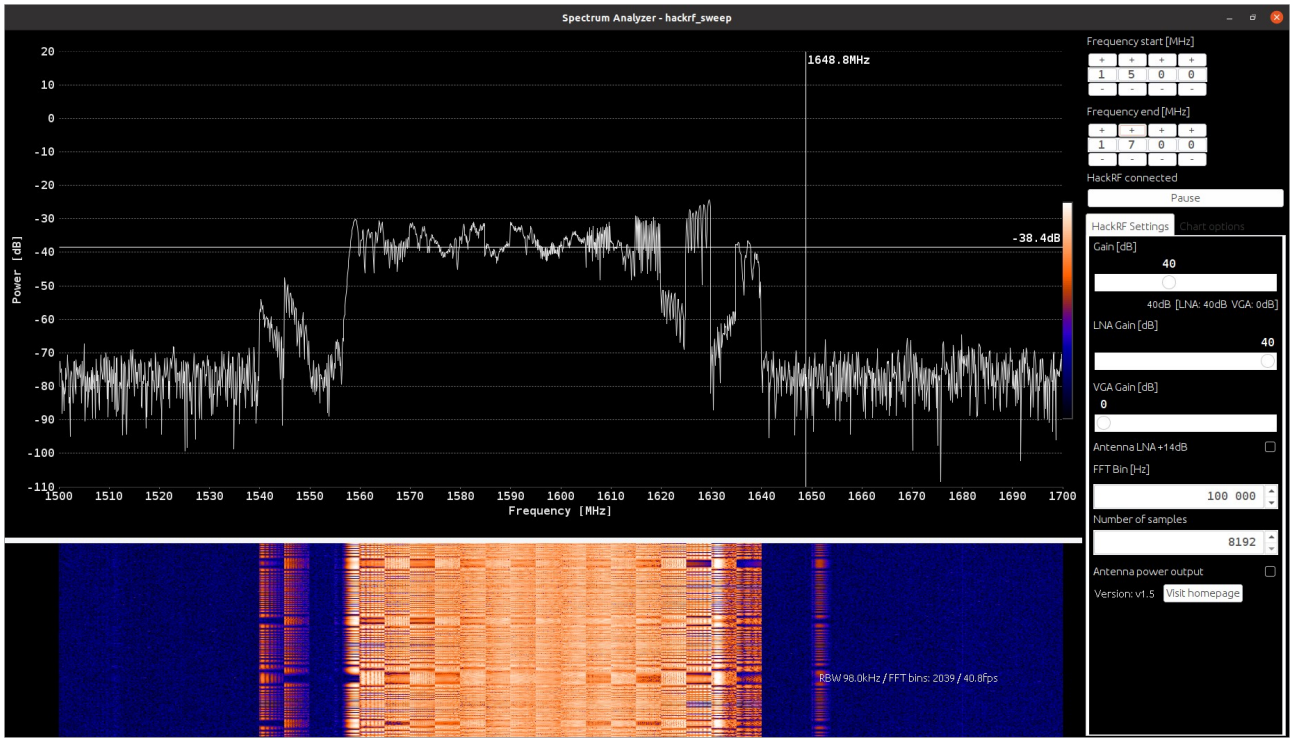


Channel 6

Before Jamming

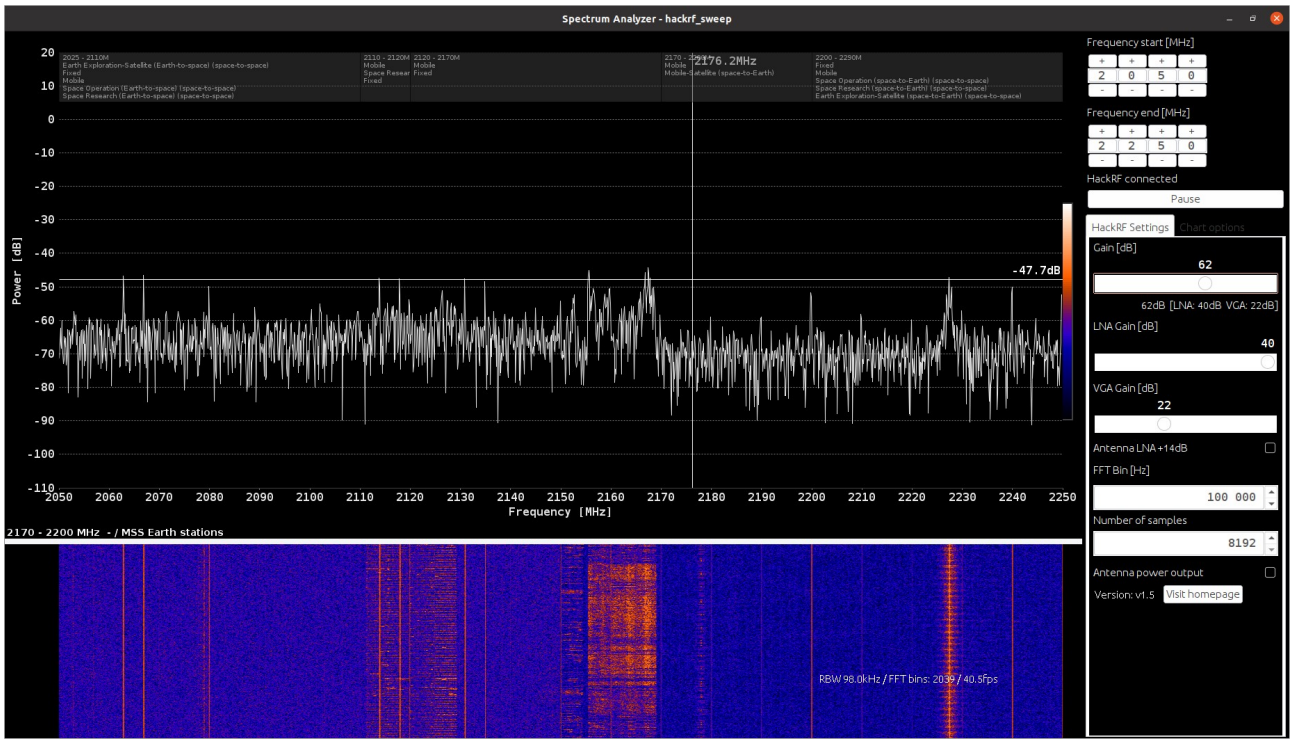


After Jamming

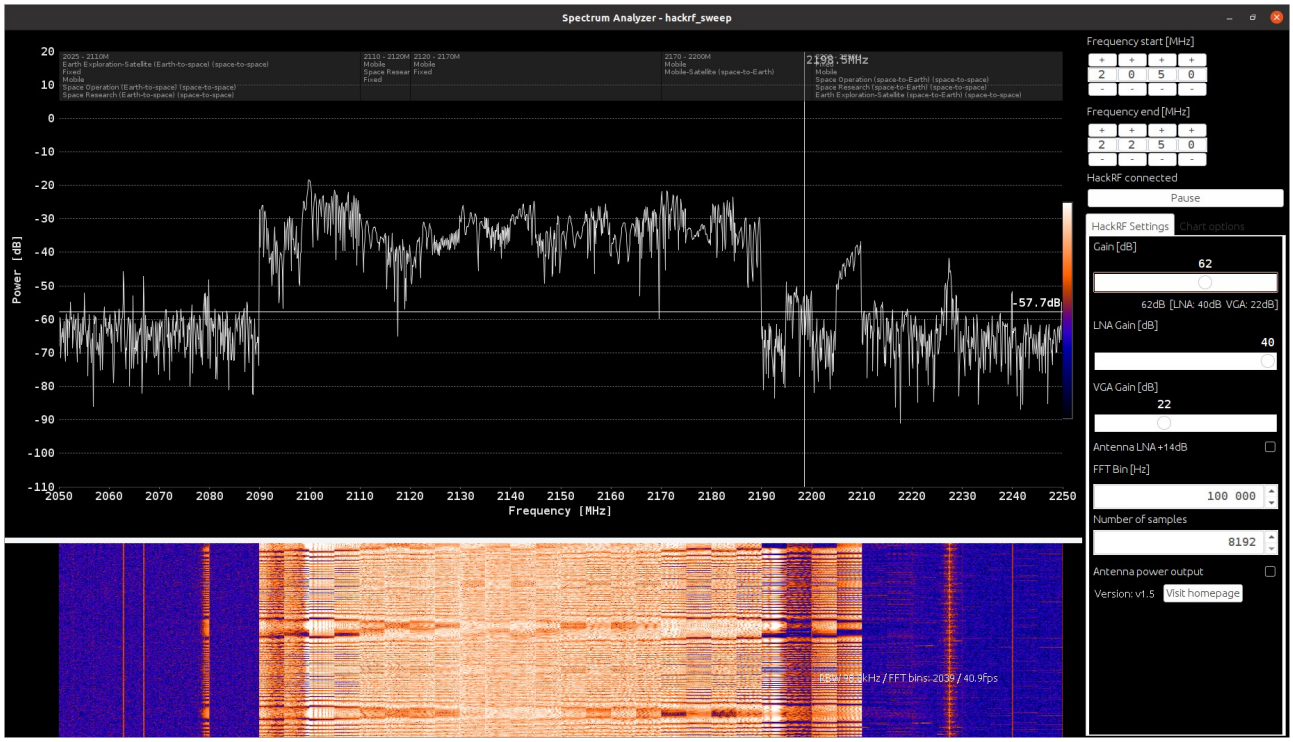


Channel 7

Before Jamming

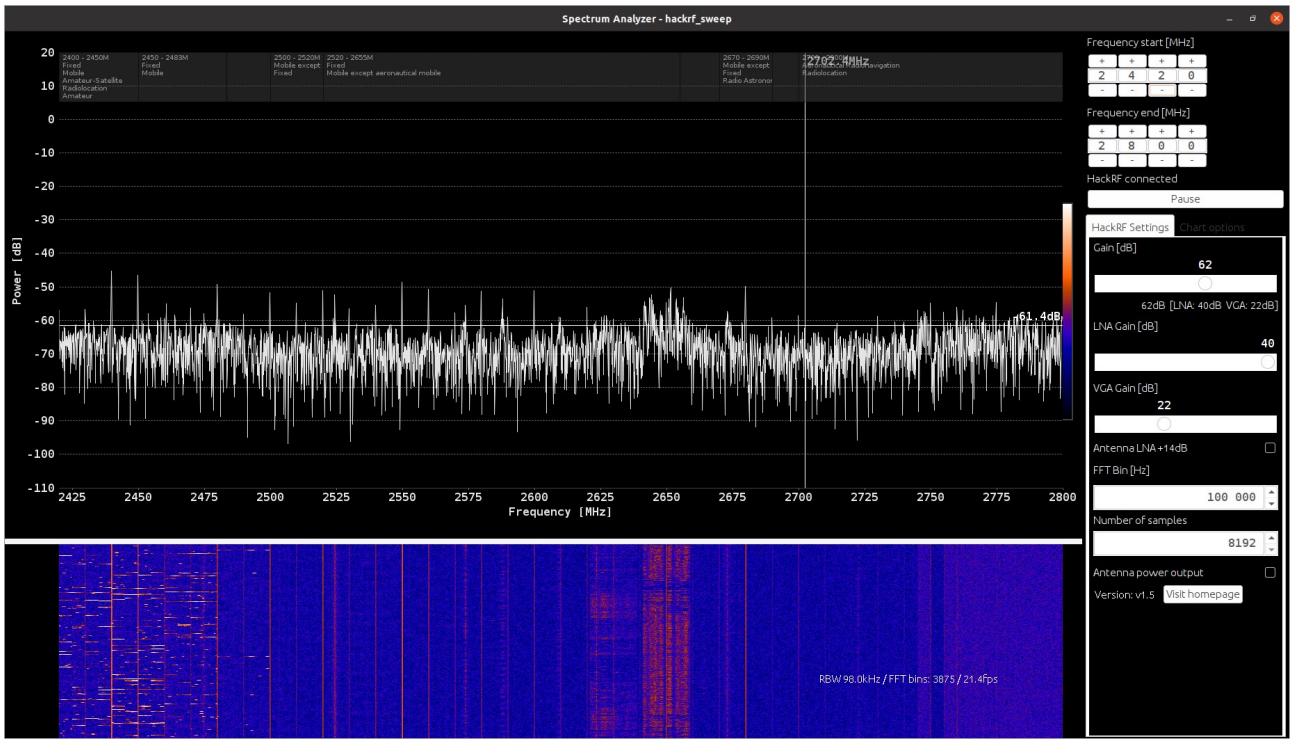


After Jamming

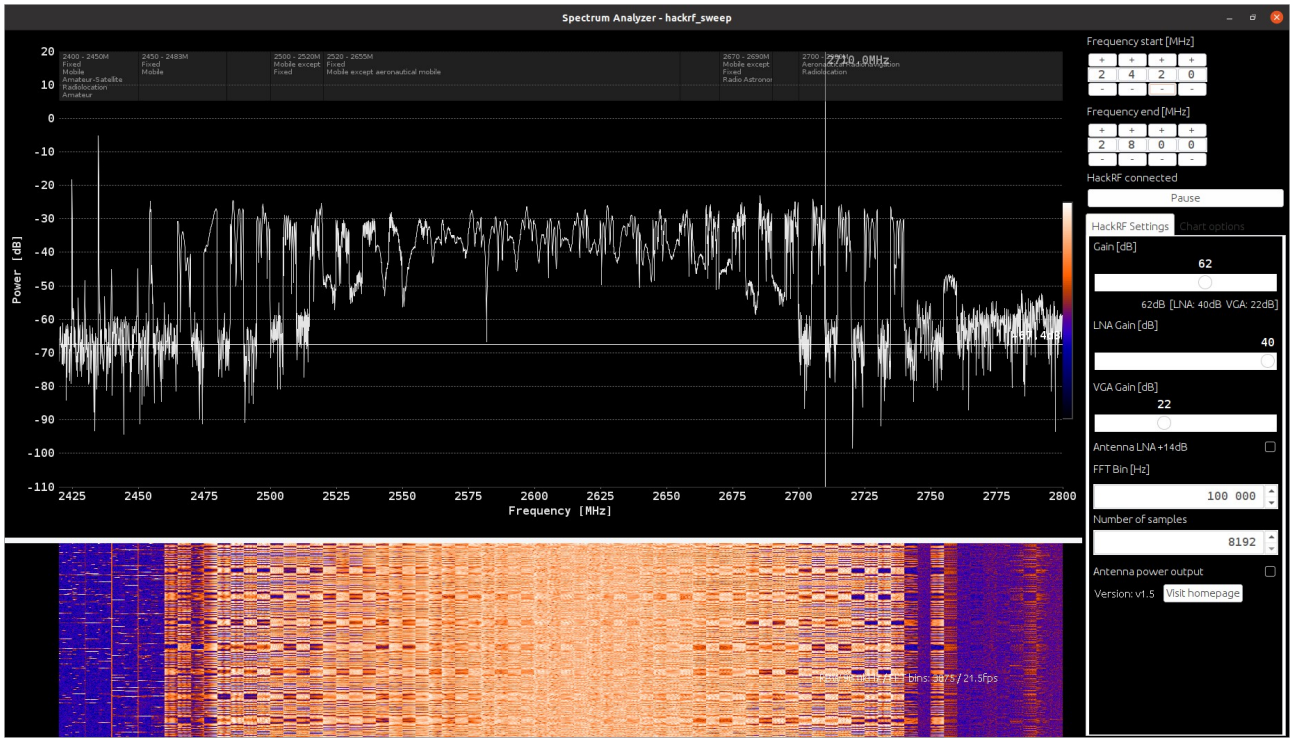


Channel 8

Before Jamming



After Jamming



Conclusion

While there are some discrepancies with the ranges listed on the Jamming Device's packaging box against the Technologies listed on the antennas, the device does disrupt communication on the intended channels.

In the 2.4 GHZ ISM range Bluetooth communication was significantly affected, audio from a mobile phone was unable to reach the connected headset, leading to the disconnection of the two devices. Furthermore, a wireless mouse and keyboard set located in close proximity to the Jamming device became unresponsive as well.

In the Mobile data frequencies, a mobile phone in the Jamming device's range was unable to detect when an incoming phone call had been dropped and eventually lost its connection to the mobile cell tower.

As the device was tested indoors where GPS Signals are already weak, no irrefutable statement can be made that it would disrupt GPS signals outdoors. However, based on the view in the radio spectrum, one can have some level of confidence that a device within a few metres of the Jamming Device would be unable to acquire a signal from the satellites.

To fully test the capabilities of the Jamming Device, however, further experiments can be executed in an area, mainly outdoors, where cell tower and GPS signals would be stronger.