# Demystifying SDR Hacking: A Deep Dive into Wireless Protocols Part:2

[](https://medium.com/@kishoreramk?source=post_page---byline--72dd42e9a92f---------------------------------------)

[KISHORERAM](https://medium.com/@kishoreramk?source=post_page---byline--72dd42e9a92f---------------------------------------)

Follow

7 min read

·

Oct 5, 2023

Listen

Share

More

## Signal hunting

A fascinating aspect of software-defined radio (SDR) hacking, involves identifying and decoding radio signals.The [Signal Identification Wiki](https://www.sigidwiki.com/wiki/Signal_Identification_Guide) is a key resource in this field, offering a comprehensive database of signals, complete with example sounds and waterfall images. This database is designed to work with a wide range of software-defined radios such as the RTL-SDR, Airspy, SDRPlay, HackRF, BladeRF, Funcube Dongle, and USRP among others. Currently, the site contains [493 identified signals](https://www.sigidwiki.com/wiki/Database), making it an extensive guide for both beginners and seasoned SDR enthusiast.

**Installing SDR#**Download SDR# <https://airspy.com/download/>  
Pre-requisites: .NET 5 Desktop x86 Runtime  
https://dotnet.microsoft.com/download/dotnet/thank-you/runtime-desktop-5.0.2-windows-x86-installer

**Frequencies and SDR Servers**Check different frequencies around the World  
<https://www.radioreference.com/apps/db/>

**SDR Servers**[https://airspy.com/directory](https://airspy.com/directory/)/

**Install VB-CABLE**Download: <https://vb-audio.com/Cable/>  
Virtual Audio Cable is a software that allows a user to transfer audio streams from one application to another.

**Raspberry PI Installation  
Tool Required**Raspberry PI OS: <https://www.raspberrypi.org/software/>  
Angry IP Scanner: <https://angryip.org/download/>  
Putty: <https://www.putty.org/>  
Setup SSH and Wi-Fi Connection on Raspberry PI

## Raspberry Pi (SDR Server & Transmitter)

In the world of software-defined radio (SDR) hacking, the Raspberry Pi stands out as a multi-functional tool.It can serve dual roles as both a transmitter for sending signals and an SDR server. By connecting an antenna to a general-purpose I/O (GPIO) pin, the Raspberry Pi can wirelessly transmit data via various modulations, including FM, AM, SSB, SSTV, and FSQ signals anywhere between[130 kHz to 750 MHz](https://community.element14.com/products/raspberry-pi/b/blog/posts/transmitting-fm-am-ssb-sstv-and-fsq-with-just-a-raspberry-pi). This makes it a powerful tool for signal transmission. On the other hand, by installing the RTL-SDR software, it can also serve as a remote networked SDR, similar to software like rtl\_tcp and Spyserver. This allows users to connect to a remote RTL-SDR running the SDR++ server on a Raspberry Pi. The server can be set up to automatically run on boot, making it easy to use and efficient. This setup is compatible with almost any SDR and enables the full range of control options for RTL-SDRs.

## **Transmit Radio Signals with Raspberry Pi:**Radio Data System data generated in real time

*sudo apt-get install libsndfile1-dev*

*git clone*[*https://github.com/ChristopheJacquet/PiFmRds.git*](https://github.com/ChristopheJacquet/PiFmRds.git)

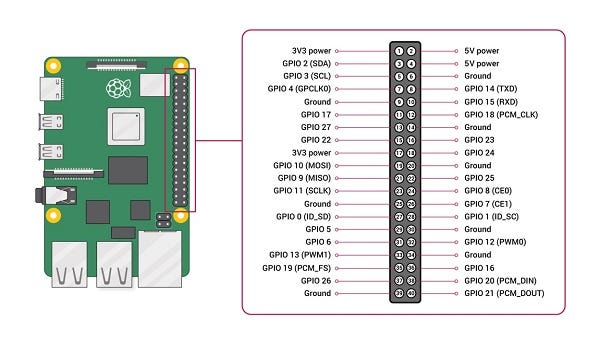
*cd PiFmRds/src*

*make clean*

*make*

## Command

*sudo ./pi\_fm\_rds [-freq freq] [-audio file] [-pi pi\_code] [-ps ps\_text] [-rt rt\_text]*



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

## VNC on Raspberry Pi

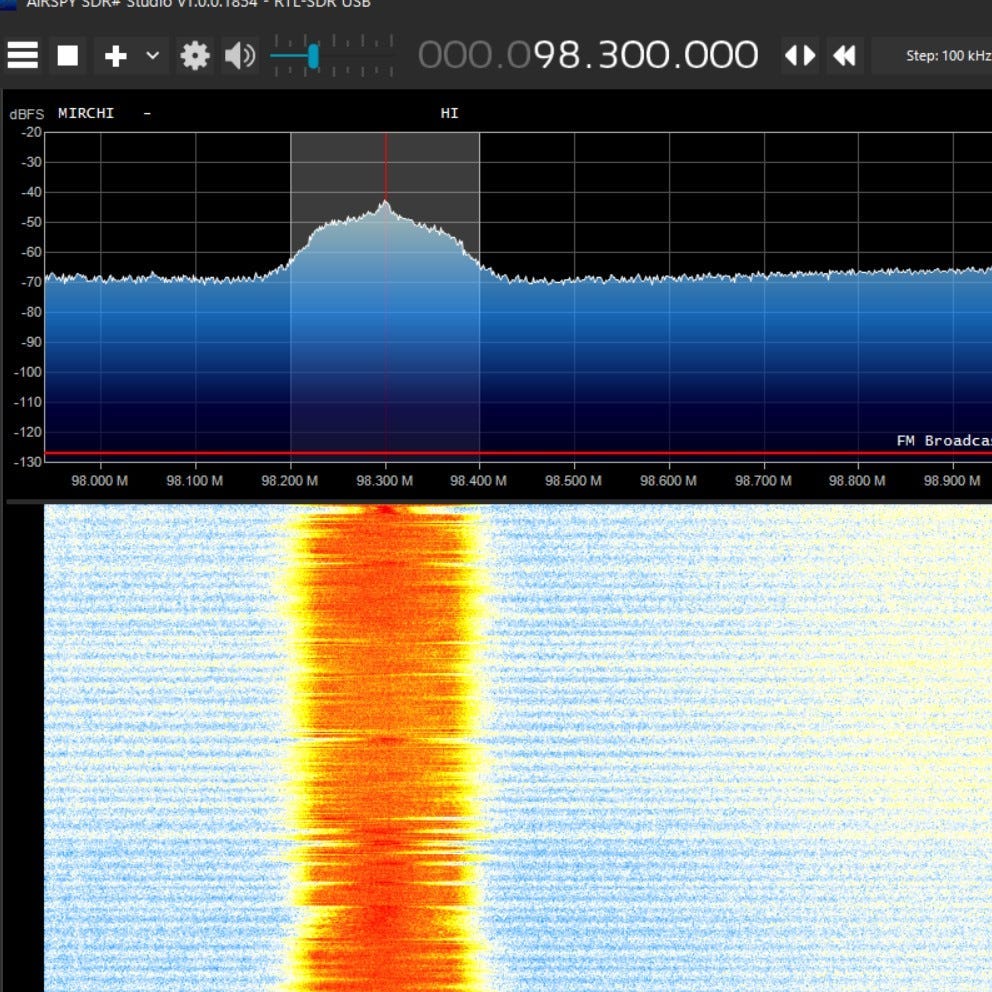
RealVNC is a tool that allows you to remotely access the desktop environment of another computer. It’s particularly useful in the context of a Raspberry Pi, as it’s one of the easiest ways to remotely access it. If you use Raspberry Pi OS, VNC is preinstalled so you only have to enable it to get started. You can enable VNC on your Raspberry Pi via the system configuration or [raspi-config](https://raspberrytips.com/use-vnc-raspberry-pi/). Once enabled, you can install the[VNC client](https://help.realvnc.com/hc/en-us/articles/360002249917-VNC-Connect-and-Raspberry-Pi#running-directly-rendered-apps-remotely-0-5) on your computer and type the IP address of the Raspberry Pi to get connected to it. In terms of Software Defined Radio (SDR) hacking, an RTL-SDR dongle and Raspberry Pi can be used together for various radio-related projects. For instance, with an RTL-SDR dongle, Raspberry Pi, a piece of wire, and literally no other hardware, it is possible to perform [replay attacks](https://www.rtl-sdr.com/tutorial-replay-attacks-with-an-rtl-sdr-raspberry-pi-and-rpitx/) on simple digital signals like those used in 433 MHz ISM band devices. This can be used for example to control wireless home automation devices like alarms and switches. RealVNC can be useful in this context as it allows you to remotely control your Raspberry Pi while it’s performing these tasks. This means you can set up your SDR hacking station in one location and control it from another, which can be particularly useful if you need to place your Raspberry Pi and SDR in a specific location for optimal signal reception.

*sudo apt-get update  
sudo apt-get install realvnc-vnc-server*

## Listen Radio

RTL-SDR is a popular software-defined radio dongle that can be used to receive a wide range of radio signals, including FM radio stations. To listen to FM radio using an RTL-SDR dongle, you will need to connect the dongle to your computer and install SDR software, such as SDR# or Gqrx. Once you have installed the software, you can tune to the frequency of the radio station that you want to listen to and click the “Play” button.

Press enter or click to view image in full size



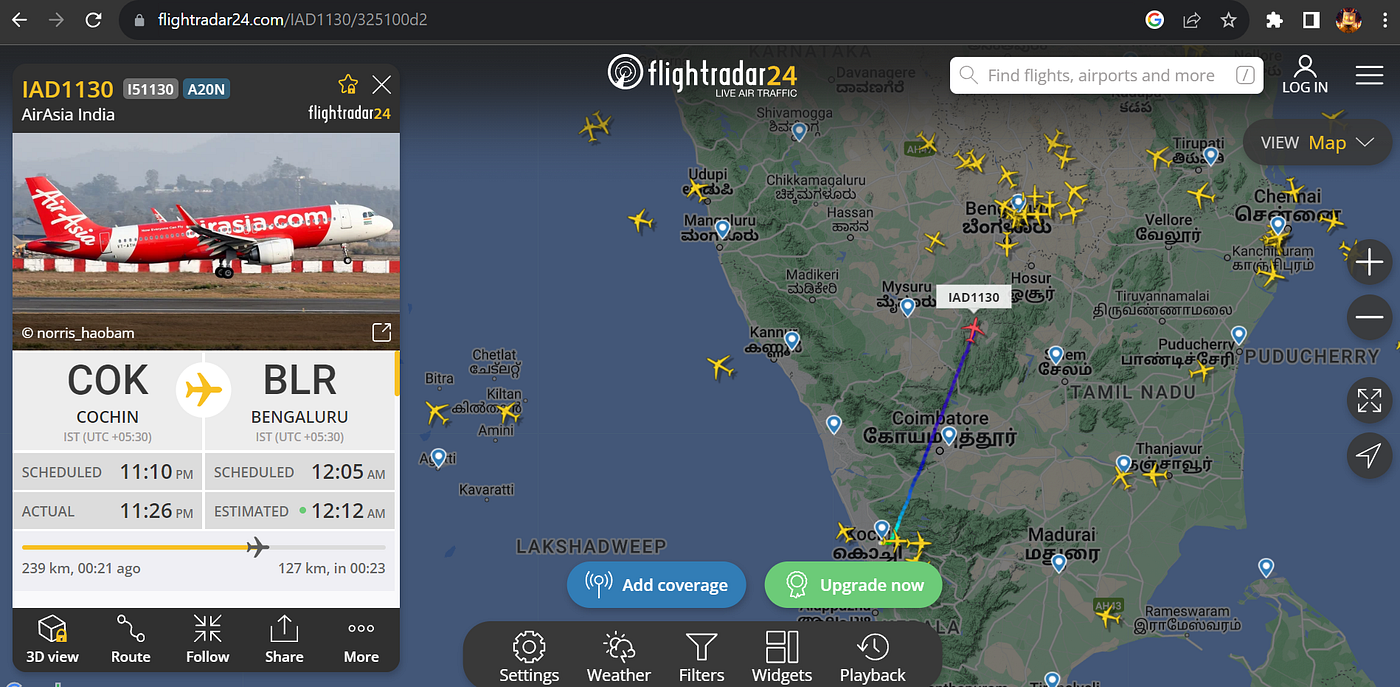
Some of the frequencies of popular Tamil FM radio stations:

* Radio City: 91.1 MHz
* Aahaa FM: 91.9 MHz
* Suriyan FM: 93.5 MHz
* Radio Mirchi: 98.3 MHz
* Hello FM: 106.4 MHz

You can listen FM in online in many websites <https://onlineradiofm.in/stations>

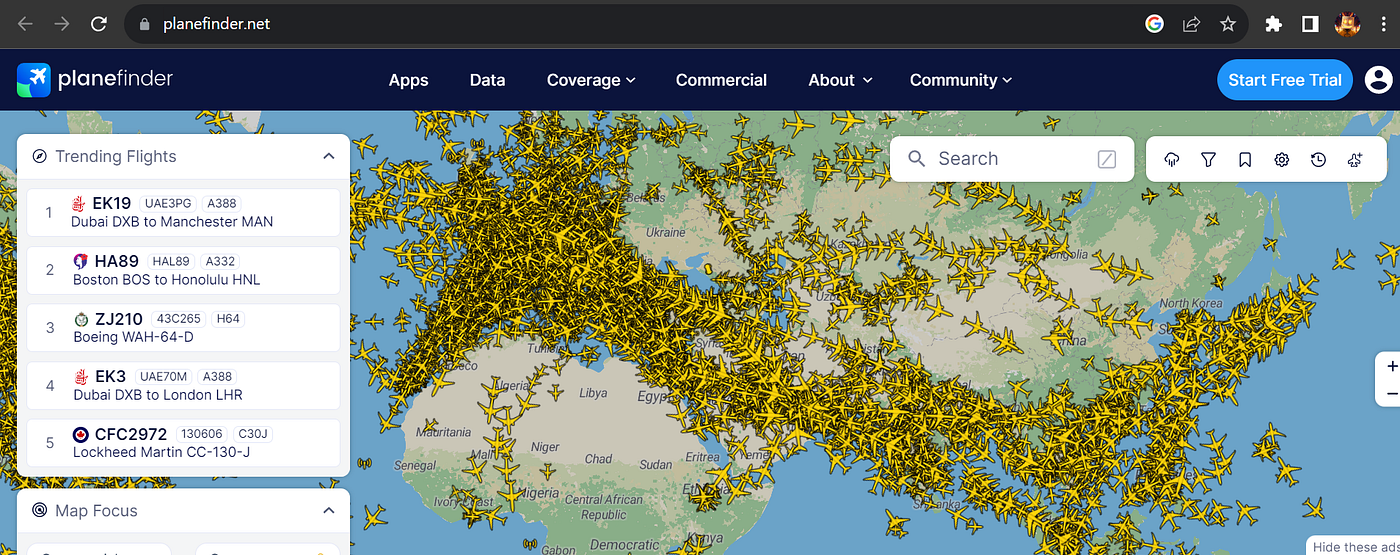
## Aircraft Tracking

Press enter or click to view image in full size



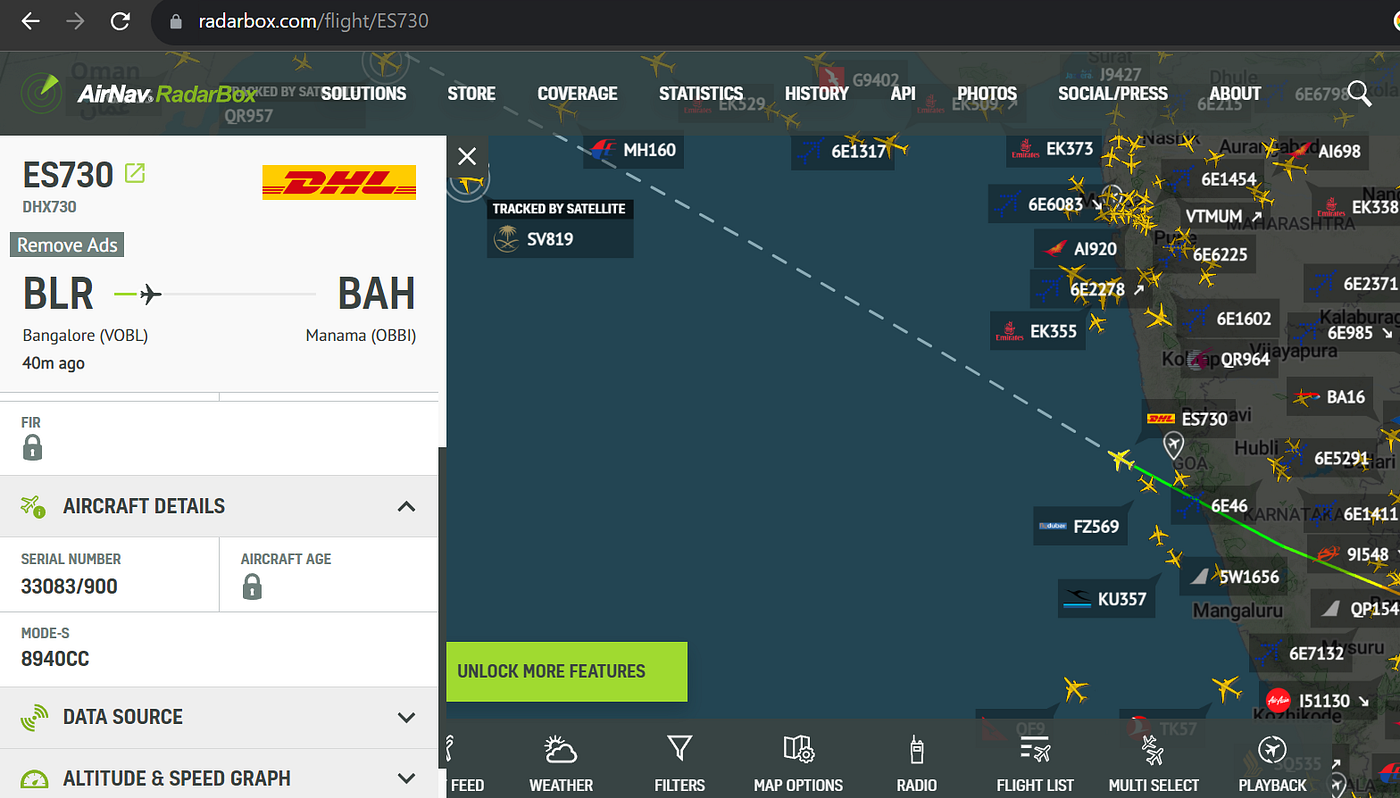
<https://www.flightradar24.com/>

Press enter or click to view image in full size



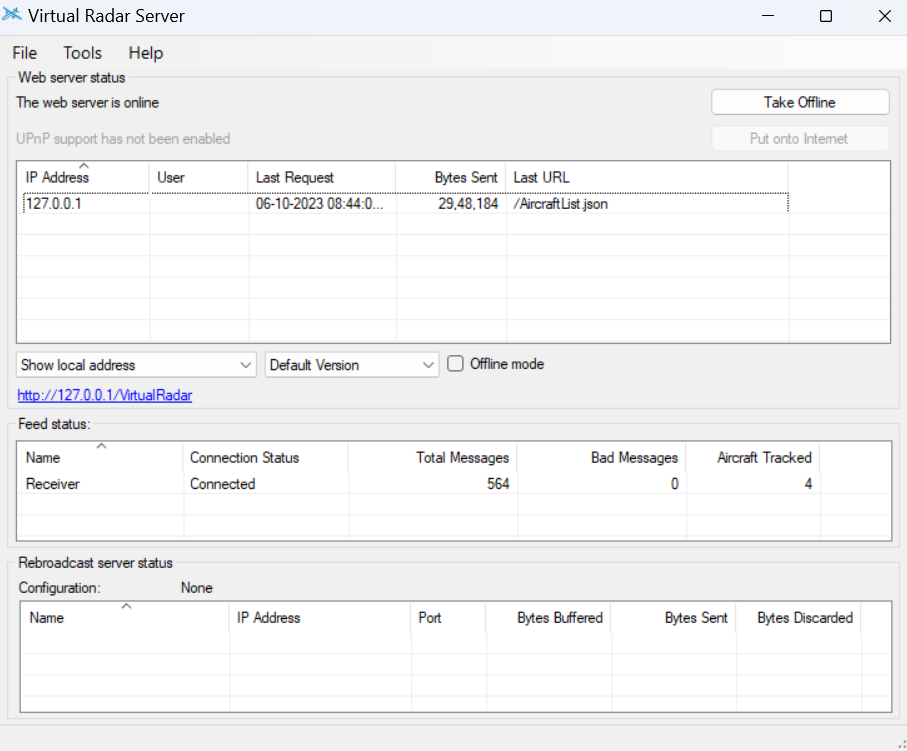
<https://planefinder.net/>

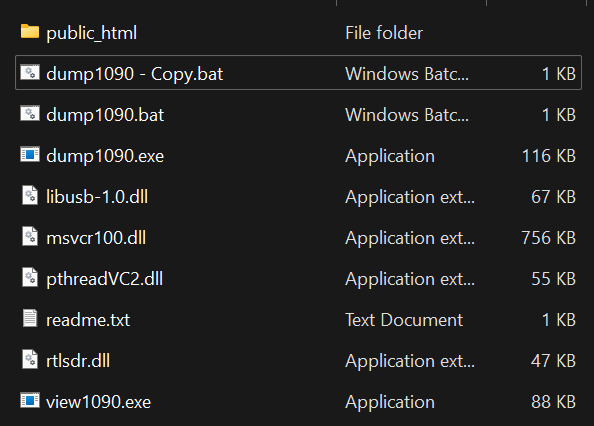
Press enter or click to view image in full size



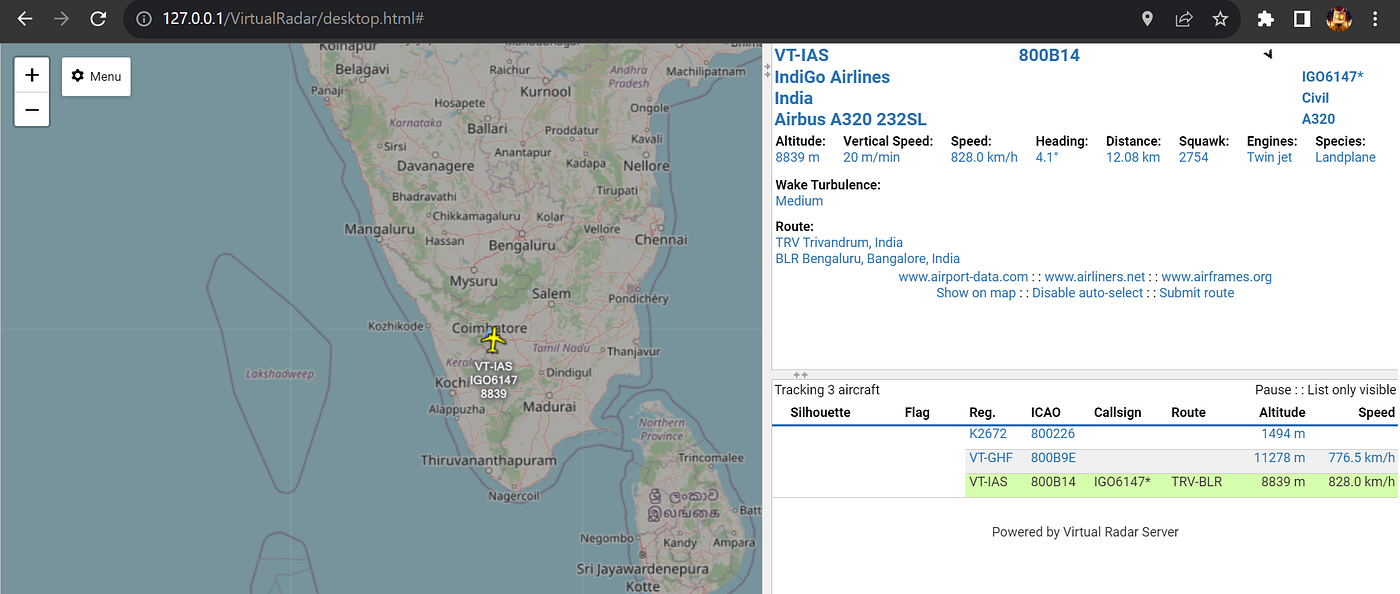
<https://www.radarbox.com/>

Press enter or click to view image in full size





Press enter or click to view image in full size



Press enter or click to view image in full size



**Dump 1090**

<http://www.satsignal.eu/software/dump1090-win.1.10.3010.14.zip>

**Virtual Radar Server**

## [Virtual Radar Server](http://www.virtualradarserver.co.uk/?source=post_page-----72dd42e9a92f---------------------------------------" \t "_blank)

### **[A stand-alone .NET application that displays output from an SBS-1 ADS-B receiver on a Google Maps web page.](http://www.virtualradarserver.co.uk/?source=post_page-----72dd42e9a92f---------------------------------------" \t "_blank)**

[www.virtualradarserver.co.uk](http://www.virtualradarserver.co.uk/?source=post_page-----72dd42e9a92f---------------------------------------" \t "_blank)

<http://www.virtualradarserver.co.uk/Files/VirtualRadarSetup.exe>

Virtual Radar Server and Dump1090 are two software tools that are often used together in the context of ADS-B decoding. Dump1090 is a command-line based ADS-B decoder for RTL-SDR (Realtek Software Defined Radio) devices. It is specifically designed for RTLSDR devices and is considered by many to be the best ADS-B decoder available. On the other hand, Virtual Radar Server is a software that takes the data from Dump1090, decodes it and then presents it on a virtual radar screen or on a map. The combination of these two tools allows users to receive and decode ADS-B transmissions from aircraft and plot them on a map. This can be particularly useful for tracking aircraft movements in real-time.

Automatic Dependent Surveillance–Broadcast, or ADS-B, is a technology that enhances surveillance of aircraft in flight. In this system, an aircraft’s onboard equipment determines its location via satellite navigation and periodically broadcasts this information. This allows the aircraft to be tracked without the need for an interrogation signal from the ground, making it a viable replacement for secondary surveillance radar. Furthermore, the ADS-B information can be shared directly between aircraft, providing situational awareness and enabling self-separation. This technology is automatic, requiring no pilot input, and dependent on data from the aircraft’s navigation system.

## **Listen International Space Station**

The International Space Station (ISS) is a large artificial satellite orbiting the Earth as a microgravity and space environment research laboratory. It is jointly owned and operated by the United States, Russia, Japan, Europe, and Canada. The ISS runs an amateur radio service under the Amateur Radio on International Space Station (ARISS) program. This service enables amateur radio operators on Earth to communicate with astronauts aboard the ISS. ARISS also transmits slow scan television (SSTV) signals, which can be received by amateur radio operators using relatively inexpensive equipment. To receive ARISS SSTV signals, you will need an amateur radio receiver and a computer with SSTV decoding software.

**Frequency:**145.800MHz

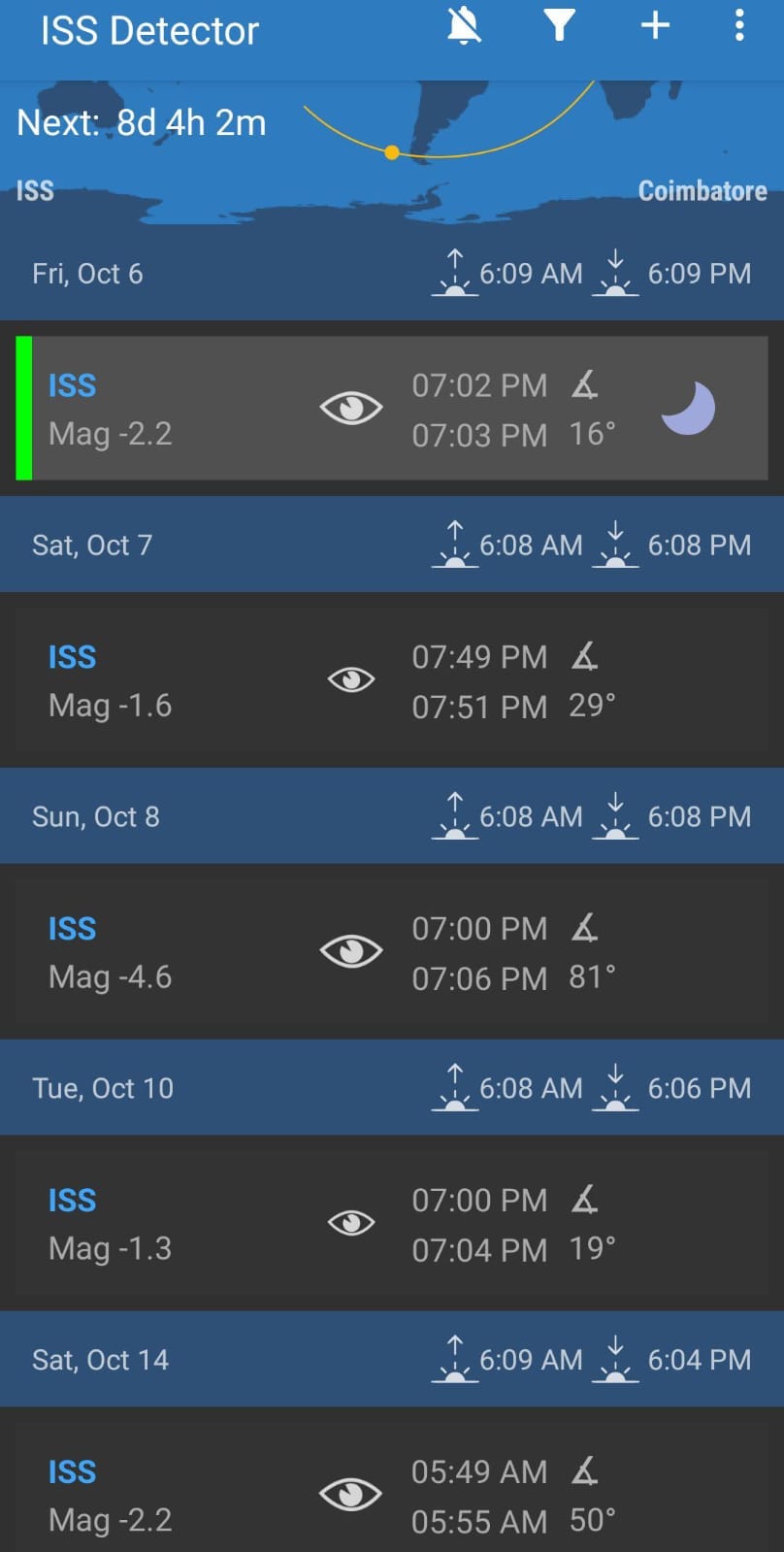
**Determining When the Space Station is Overhead**

To find when the International Space Station will be over your location, you can go to [www.issdetector.com](http://www.issdetector.com/)

**MMSSTV (Decoding ISS Data)** <https://hamsoft.ca/pages/mmsstv.php>

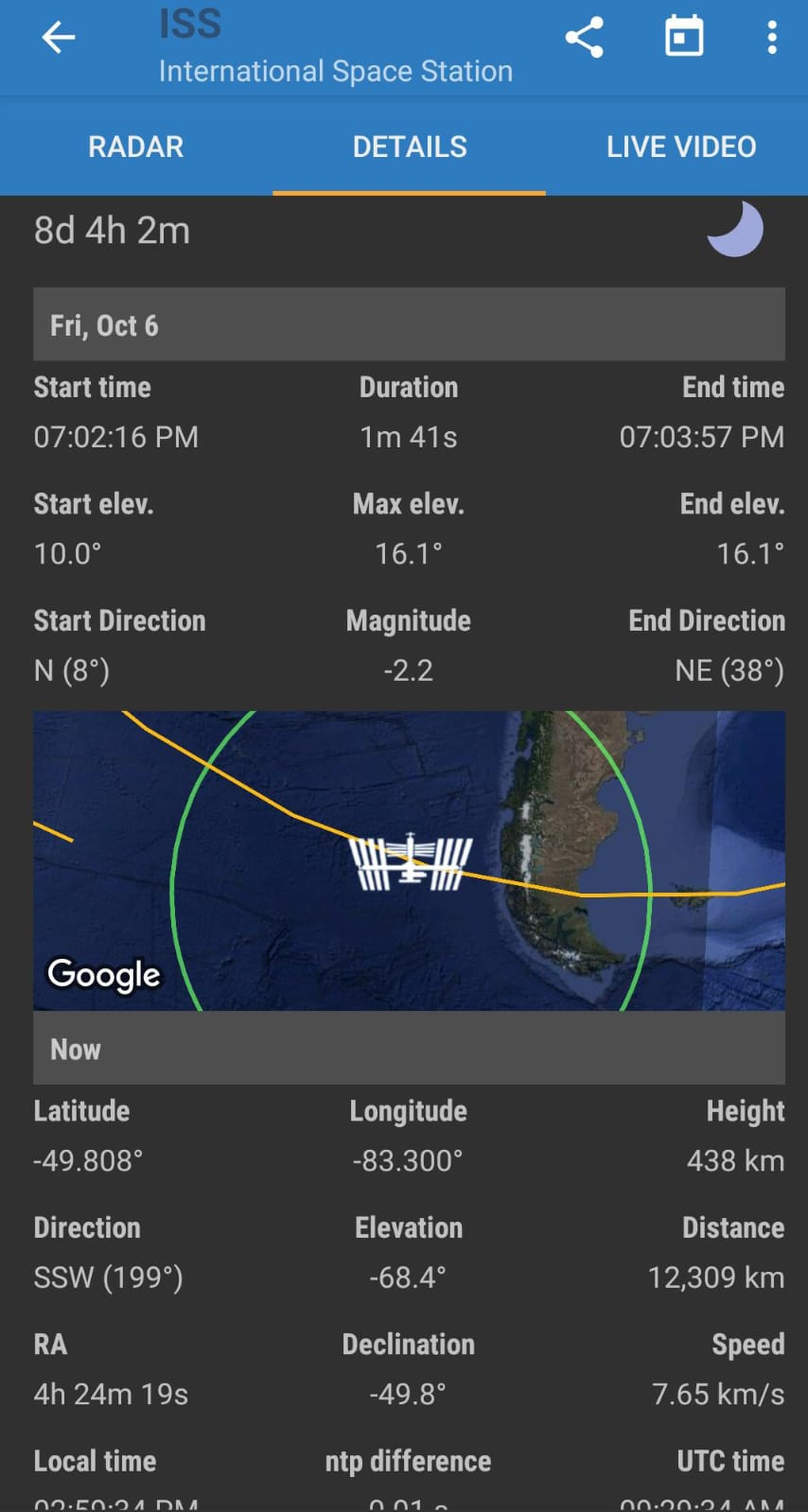
To receive and decode SSTV transmissions from the ISS, you will need an RTL-SDR dongle, a simple antenna, and a software like MMSSTV. Tune in to 145.800 MHz on your RTL-SDR dongle and open MMSSTV. Enable “Auto slant” and “Auto resync” under Options->Setup MMSTV->RX for the best results. Once the ISS is transmitting SSTV images, MMSSTV will automatically decode them and display them on the screen.

Press enter or click to view image in full size

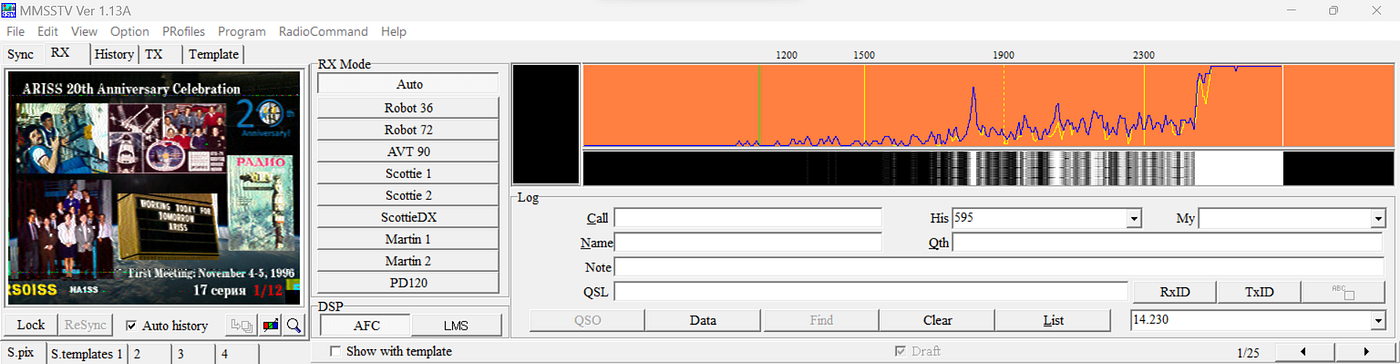


ISS Detector App(Playstore)

Press enter or click to view image in full size



Press enter or click to view image in full size



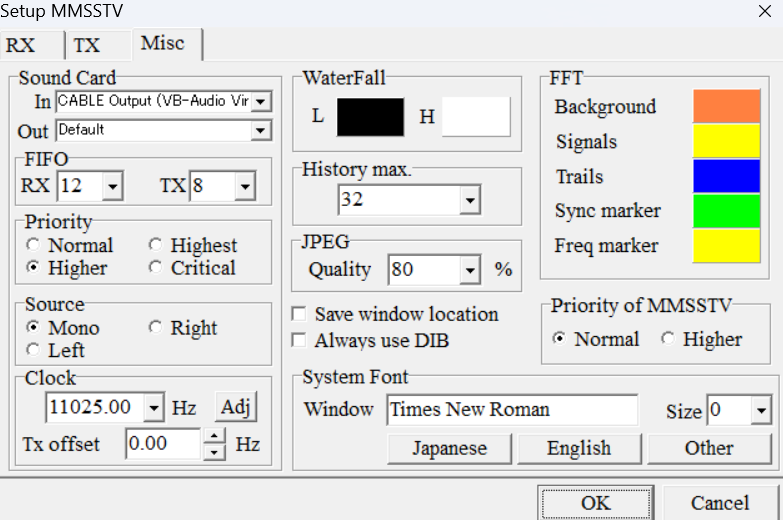
Source:<https://oe5lxr.at/decode-sstv-with-mmsstv/> (Audio file)

**Upload your received and decoded image** <https://www.spaceflightsoftware.com/ARISS_SSTV/>

**Claim your SSTV reception award**<https://ariss.pzk.org.pl/sstv/>

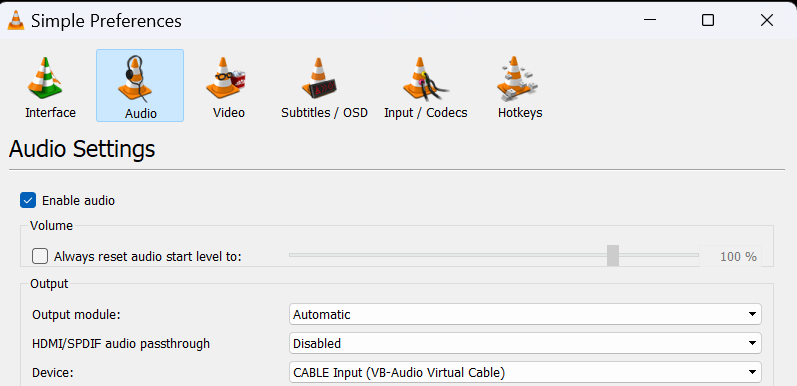
Use virtual cable audio input in the **MMSSTV**and also choose the audio output as virtual cable from which software you are using.

Press enter or click to view image in full size



**MMSSTV Output**

Press enter or click to view image in full size



**Audio player Input**

## 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/>