Software Defined Radio

Ashish Kumar
BTech-ICT
Dhirubhai Ambani Institute of Information and Communication Technology
Gandhinagar,Gujarat
Email: 201901275@daiict.ac.in

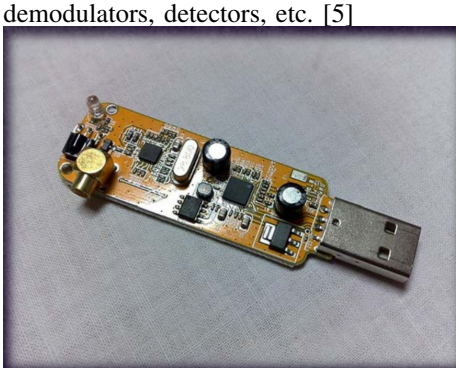
Shubh Jhawar
BTech-ICT
Dhirubhai Ambani Institute of Information and Communication Technology
Gandhinagar,Gujarat
Email: 201901204@daiict.ac.in

Yash Jain
BTech-ICT
Dhirubhai Ambani Institute of Information and Communication Technology
Gandhinagar,Gujarat
Email: 201901296@daiict.ac.in

***Abstract*—In this rep we have stated our learnings in Software Defined Radio set up.We have used different hardware devices and a software tool to detect radio signal frequencies.How we set up the hardware part and connect it to a software SDR which is SDR sharp and detect FM frequencies.And use RTL-sdr USB driver to sniff GSM signals.**

I. Introduction

The purpose of this study is to provide a demonstration of how (SDR-Software Defined Radio) operates and some examples of its applications in various fields. The phrase ”software-defined radio” (SDR) refers to a radio communication system in which software operating on a personal computer or embedded device takes the place of various hardware components such mixers, filters, amplifiers, modulators-demodulators, detectors, etc. [5]



A. Components used

- Software Defined Radio
- Software defined Antennas

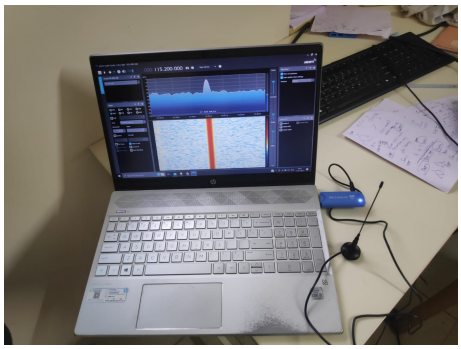
B. Software used

- Zidag- Zadig is a Windows tool that instals generic USB drivers like WinUSB, libusb-win32/libusb0. sys, or libusbK to enable you to access USB devices. It can be quite useful when you wish to use a libusb-based application to access a device.
- One of the most popular free software defined radio programmes that supports RTL-SDR is SDR -SDRSharp..

C. SDR Components

The RTL2832U plus a tuner chip, of which many varieties are utilised, make up an RTL dongle. Two A/D converters, a USB interface, and a lot of digital logic are all features of the RTL2832U. The RTL chip’s A/D converters can handle the analog downconversion that the tuner chip performs from VHF/UHF frequencies to frequencies of a few MHz.
An RF frontend in the SDR architecture transforms the RF frequency band into baseband spectrum. This is handed off to a High-Speed ADC, which digitises the baseband samples before handing them off to the computer’s DSP software. These RF baseband data are processed by the DSP software to obtain the physical data they contain. Also, antenna It is crucial to connect antennas when using an SDR Receiver or Transceiver in order to receive and send radio signals across long distances. [2]

SET UP



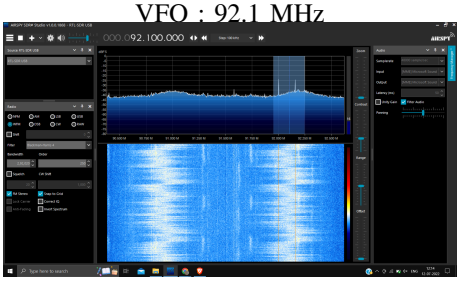
SDR SHARP

To test SDR sharp we tried to capture frequencies of FM radio.An easy, intuitive, compact, and quick computer-based DSP application for software-defined radio is called SDR (or SDR Sharp).

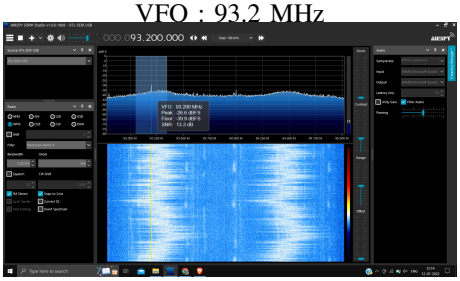
- Open the SDR Sharp application first.
- Choose the RTL-SDR USB driver as a source.
- Choose WFM -wide-band FM radio under the Radio signal type.
- Select Configure and then set the gain to approximately halfway up.
- You can select your preferred FM station.Then click

- Click Play or Start [6]

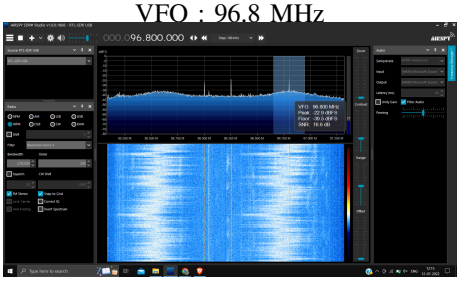
VFO : 92.1 MHz



VFO : 93.2 MHz



VFO : 96.8 MHz



II. GSM SNIFFING

We use two frequency bands in India. It is necessary to have a dual-band 900-1800 phone in order to work with the majority of international networks. We must first determine the GSM downlink channels in order to do sniffing. We would've been sniffing GSM data for our own cellphone in this scenario, thus we would need to be aware of the frequency it uses. An Absolute Radio-Frequency Channel Number - ARFCN in GSM mobile networks designates a pair of physical radio carriers—one for the uplink signal and another one for the downlink signal—used for transmitting and receiving. Osmo libraries are preinstalled on GNU Radio, and it connects to the DVB dongle using the USB I/O connection. A GSM-tuned antenna is being used by the SDR to pick up the analogue RF stream. The R820T tuner is in operation at its input and amplifies the RF signal before downconverting it from megahertz to an media frequency. The RTL2832U chip includes a built-in analogue to digital converter in addition to a demodulator and a decoder [1].

III. INSTALLING SOFTWARE IN UBUNTU LINUX

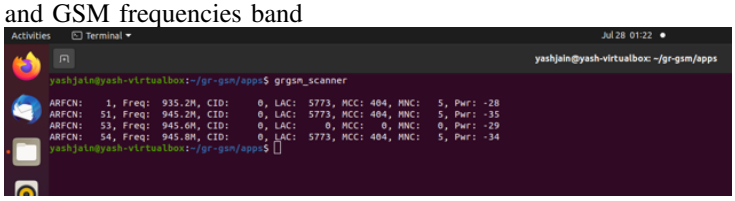
First we install all dependencies

- sudo apt-get update
- sudo apt-get install -y
- cmake
- autoconf
- libtool
- pkg-config
- build-essential
- python-docutils
- libcppunit-dev
- swig
- doxygen
- liblog4cpp5-dev
- python-scipy
- python-gtk2
- gnuradio-dev
- gr-osmosdr
- libosmocore-dev

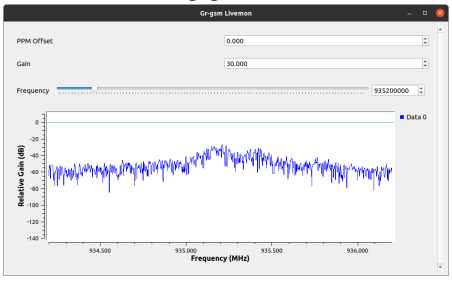
GR-GSM installation [3]

- git clone https://gitea.osmocom.org/sdr/gr-gsm
- cd gr-gsm
- mkdir build
- cd build
- cmake ..
- mkdir $HOME/.grc - gnuradio/$HOME/.gnuradio/
- make

with command : grgsm-scanner we can find ARFCN channels and GSM frequencies band

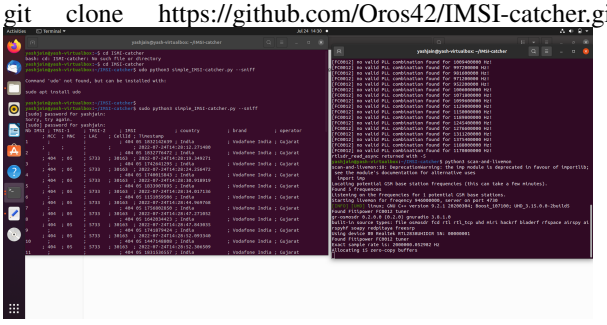


with command : grgsm-livemon -f 935200000

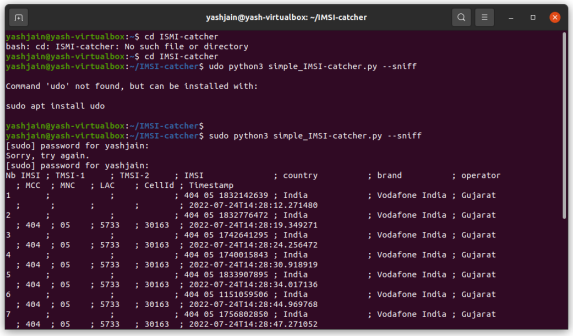


Installation of IMSI Catcher :

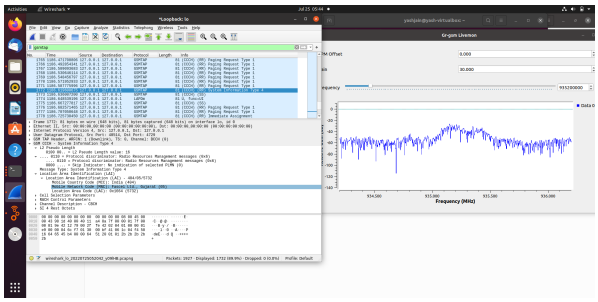
- sudo apt install python3-numpy python3-scipy
- git clone https://github.com/Oros42/IMSI-catcher.git



Here, we detect IMSI number: Every user of a Global System for Mobile Communication has a 15-digit number called an International Mobile Subscriber Identity (IMSI) (GSM).



Wireshark would now start to display GSM data packets as soon as we started it together. Gsmtap packets can also be filtered out [4].



IV. Conclusion

A computer can act as a radio by using software-defined radio (SDR). However, a desktop computer's computational capabilities allow you to listen to and decode a number of transmissions in addition to utilizing an AM/FM radio. Your computer may become a climate frequecny receiver, a scanner for police and fire reports, a music-player, and more thanks to SDR! Software-driven electronics with rapid radio signal detection and decoding capabilities replace manually tuning inductors in all operations.

References

[1] Nicolae Crişan and Maria Condrea. Gsm wireless sniffer using software defined radio. *Carpathian Journal of Electronic and Computer Engineering*, 10:17–20, 01 2017.

[2] Eugene Grayver. *Implementing software defined radio*. Springer Science & Business Media, 2012.

[3] Ihan Martoyo, Paul Setiasabda, Herman Y Kanalebe, Henri P Uranus, and Marincan Pardede. Software defined radio for education: Spectrum analyzer, fm receiver/transmitter and gsm sniffer with hackrf one. In *2018 2nd Borneo International Conference on Applied Mathematics and Engineering (BICAME)*, pages 188–192. IEEE, 2018.

[4] josh Poitr. Sniffing and analyzing gsm signals with gr-gsm, 2015.

[5] Mathew NO Sadiku and Cajetan M Akujuobi. Software-defined radio: a brief overview. *Ieee Potentials*, 23(4):14–15, 2004.

[6] EG Sierra and GA Ramirez Arroyave. Low cost sdr spectrum analyzer and analog radio receiver using gnu radio, raspberry pi2 and sdr-rtl dongle. In *2015 7th IEEE Latin-American conference on communications (LATINCOM)*, pages 1–6. IEEE, 2015.

github refrences

https://github.com/ptrkrysik/gr-gsm.git

https://github.com/Oros42/IMSI-catcher.git

https://gitea.osmocom.org/sdr/gr-gsm