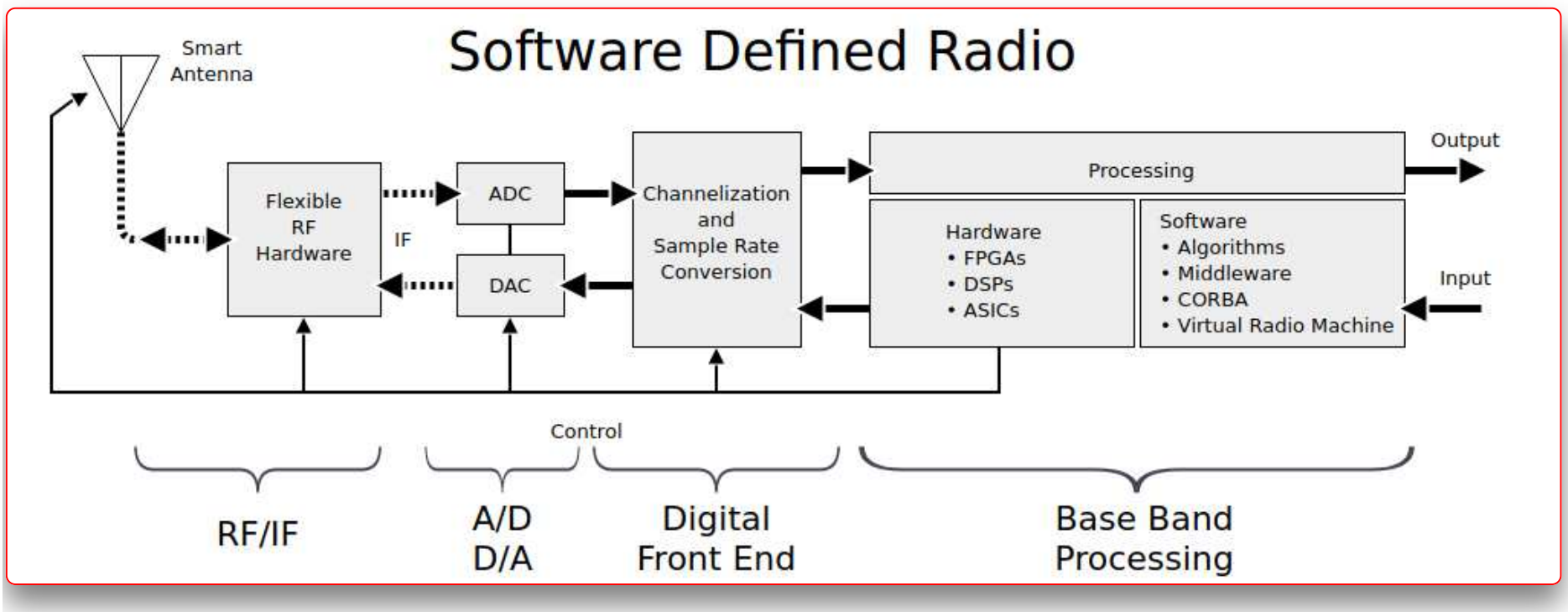
Payatu

IoT Security – Part 9 (Introduction To Software Defined Radio)

Appar

25-June-2020



Introduction

This blog is part of the "IoT Security" series. If you haven't read the previous blogs (parts 1 - 8) in the series, I urge you to go through them first unless you are already familiar with those concepts and want to only read about the current topic.

IoT Security - Part 1 (101 - IoT Introduction And Architecture)

IoT Security – Part 8 (Introduction to software defined radio)

This blog will be a continuation of the previous blog. In this, we will be looking into some of the software SDR tools available out there. We'll also define an approach on how to go about an RF target.

Software

With a great open-source community, SDR has a variety of software tools with all signal processing functionality available. Let's look into some of the widely used SDR software available and what set's them apart. We'll be focusing on tools that are mainly available for Linux.

Recon tools:

- GQRX

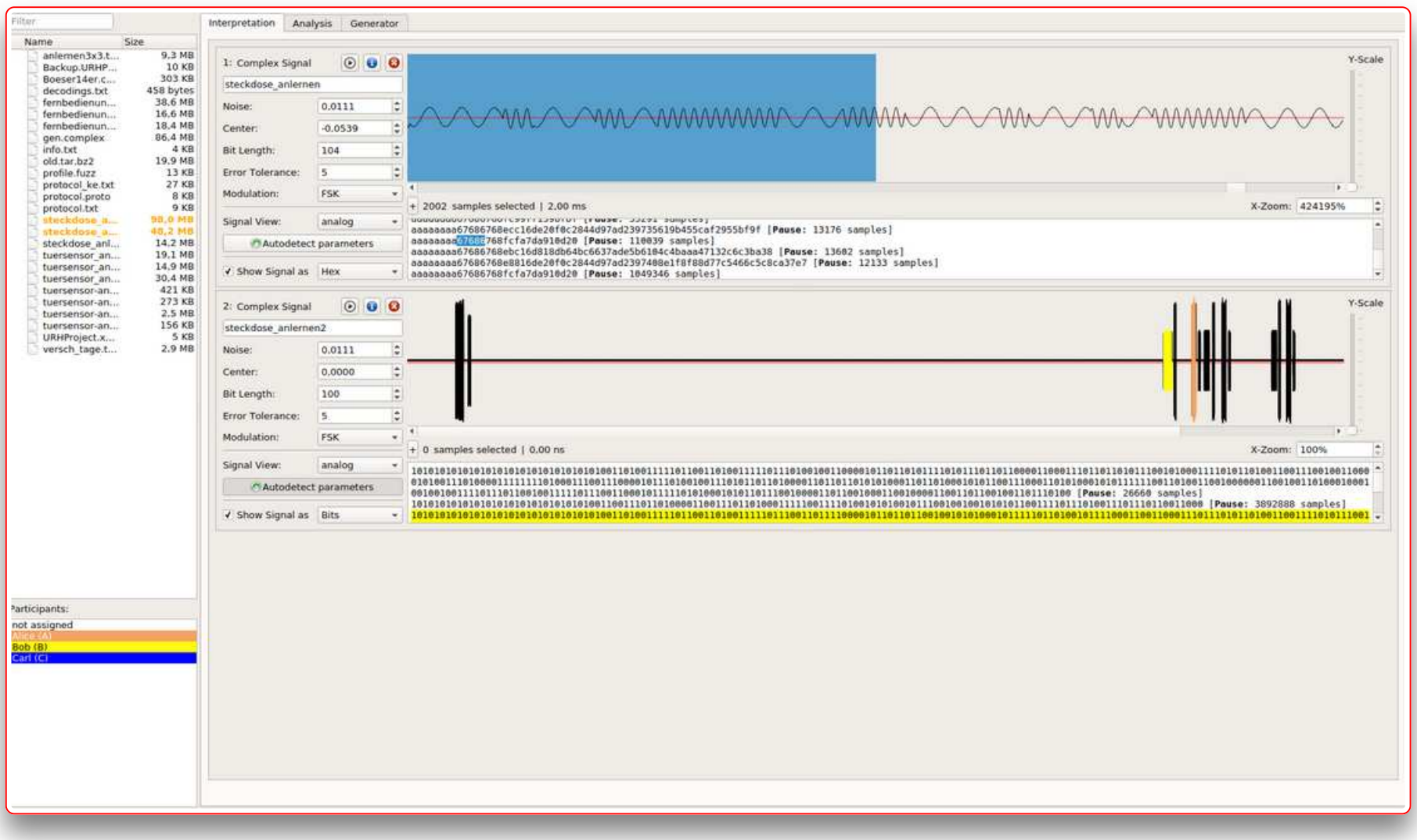
  GQRX is a spectrum analyzer used for frequency band browsing and finding the operating frequency of the target. It comes with common demodulators like AM, CW, FM. Due to the demodulation functionality, it is possible to record demodulated signal streams which can be further analyzed in tools like Audacity and Inspectrum in the next phase of assessment. It is compatible with all major SDR hardware available. There are other alternatives to GQRX with more or less the same functionality, mentioned below:

- **HDSDR**/ **SDR#** (SDR-Sharp) [for windows]
- **Qspectrum analyser** (with automatic peak detection)
- **Osmocom-FFT** (spectrum analyzer included in the Osmocom GNU Radio blocks)

Basic assessment:

- Universal Radio Hacker(URH):

  URH is a complete suite for wireless protocol investigation with native support to major SDR hardware. Almost everything is automated here, from spectrum analysis to even sending manipulated signals. One can effortlessly recognize the modulation type and get automatic decoding of the signal. For manual inspection, a differential view of received bitstreams is also there, which is very useful in interpreting the signal's data. Other major functionalities include the protocol analyzer (automated and manual). Here's where it gets interesting, It has a simulation environment for stateful attacks and a fuzzing element aimed at stateless protocols!



Another alternative to URH is Inspectrum.

- Audacity:

  Audacity is a multichannel audio editing tool but it turns into a radio signal analyzer when

clubbed with GQRX. Audacity is open-source and is available for all common OS. It accepts only recorded signals however the signal has to be demodulated, like a recorded signal from GQRX.

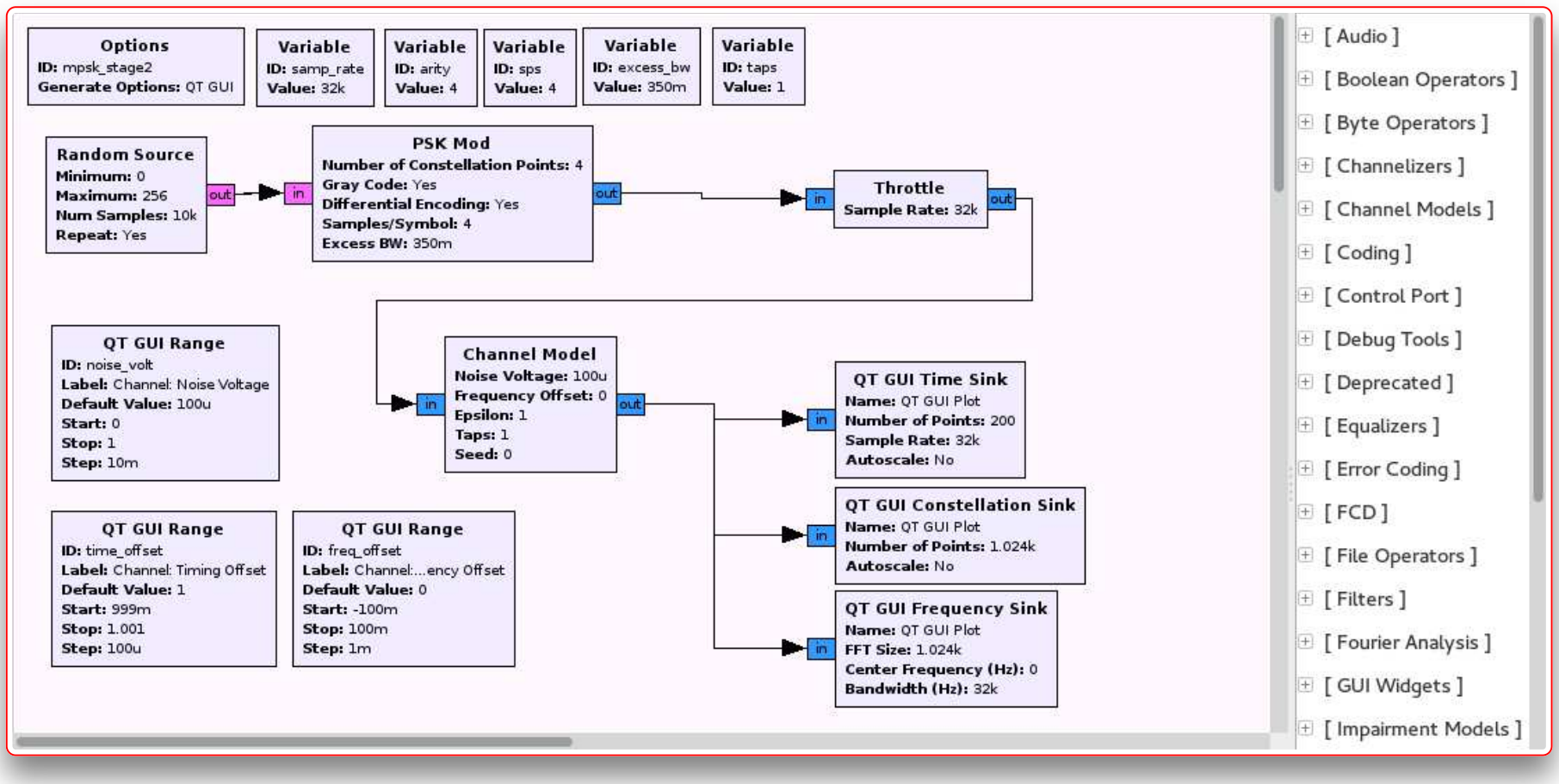
Advanced assessment:

- GNU Radio

  GNU Radio is an open-source toolkit to implement SDRs. It provides basic blocks to perform different steps of signal processing, for example, filters, decoders, demodulators, and many more. It works with all of the major SDR hardware. The major benefit is the huge extensibility of the framework. It is possible to write blocks in C++, or Python.

- GNU radio companion (GRC):

  GNU Radio Companion (GRC) is a frontend visualization tool that is part of the Gnu radio framework. We should keep in the back of our mind that GRC was created to simplify the use of GNU Radio by allowing us to create python files graphically as opposed to creating them in code alone. It allows one to simply drag, modify parameters, and start processing the signal. We'll focus on it more as we proceed.



Other Points of Interest:

- Android

  SDR is making its way into the mobile device as the processing capabilities of the mobile devices increases significantly over time. Although still very limited, but simply loading a few libraries of the device, connecting your SDR hardware via OTG cable to your android will do the job. Devices like RTL-SDR dongle, Lime SDR mini, and HackRF and a few other work fine with the android devices.

- SDR touch:

  Similar to GQRX, is used as a spectrum analyzer for the mobile device.

- GNU Radio Android:

  More Recently GNU Radio for android came out. It's all your SDR solution in your mobile device. Although it has limited supported mobile devices as of now, major device coverage is

expected over time.

- Scapy-radio:
  Scapy-radio is an extension to Scapy, an open-source network packet manipulation tool, written in Python. This extension uses Scapy as a back end for radio packet manipulation. As the gateway from Scapy to the SDR device, GNU Radio is used.

How to approach a target:

We'll be breaking down how you can approach an RF target, capture, reverse-engineer it and launch your attacks!

- SDR Hardware: HackRF One
- SDR Software: GQRX, GNURadio Companion
- Target: For this, we picked a locally manufactured $6 wireless doorbell, which turned out to be analog. Let's see how we go about it...

Image source:https://xkcd.com/1457/

1) Recon

In case you have the device, most of the task is done because you can simply look up the FCC ID of the device from here, which will give you a lot of details about the device i.e. operating frequency, the internals of the device so on and so forth which will ease up a lot for the assessment.

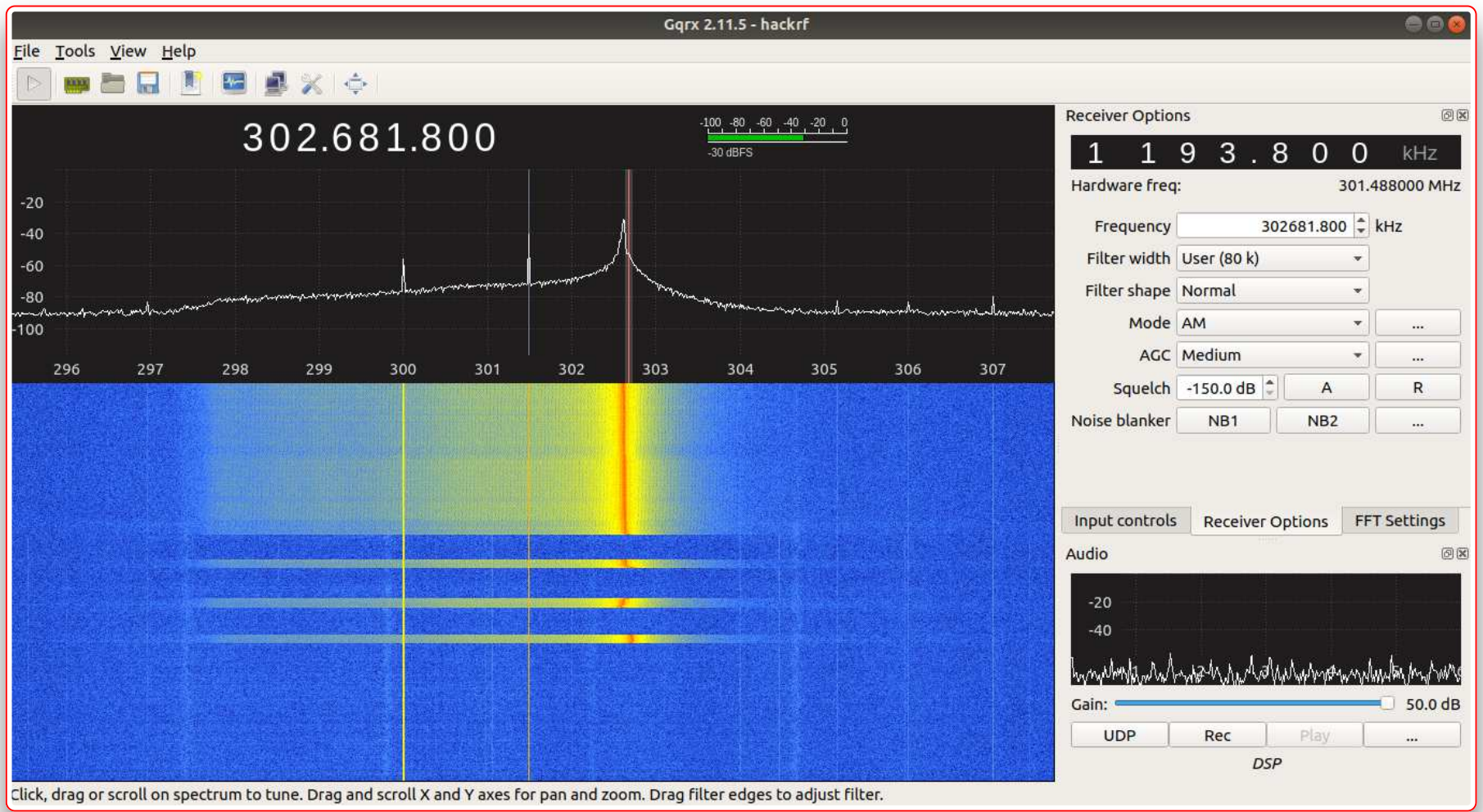
In our case, since it was a locally manufactured device, it didn't come with any FCC ID :(

2) Seek

You need to analyze the spectrum to find where is the signal being transmitted. You can use any spectrum analyzer you are comfortable with. Here's a list of common operating frequencies that will help you in finding the target frequency:

- 300MHz
- 433Mhz
- 868Mhz
- 915Mhz

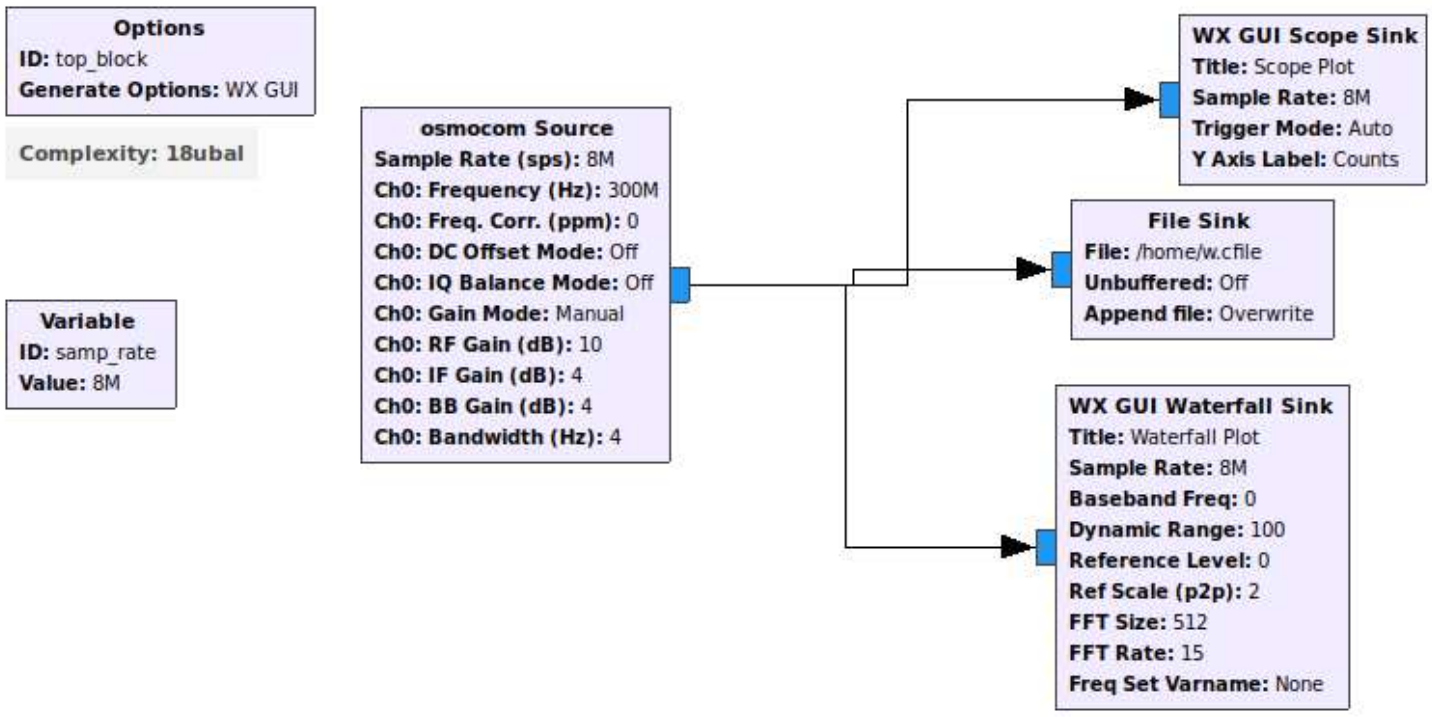
All these are commonly used ISM and license-free bands. Bodies like WPC (Wireless planning and coordination wing of the Department of Telecommunications (DOT) of the Government of India and US Federal Communications Commission (FCC) allow such bands to be license-free provided that these will only be used by low powered wireless equipment with specifics defined for bandwidth, output power and maximum effective radiated power.



In our case, we used GQRX for this step. We observed the peak at 302MHz, which is a little unusual for any operating device.

3) Record

Capturing the signal is a good practice to preserve the signal for analysis. One can easily run signal processing operation on a recorded signal, without the need for any RF target producing a live signal. In our case, we are using the below GRC flowgraph. We saved the signal in a .cfile.



Recording the analog doorbell signal (flowgraph)

4) De-Modulation

The best way to do it is just by simply looking at the signal. If you're well versed in the modulation techniques you can easily understand the type of modulation being used i.e. compressions and decompressions in FSK. Below are some commonly used modulations:

- FSK (Frequency shift keying)
- ASK (Amplitude shift keying)
- OOK (On-off keying)
- PSK (Phase shift keying)

5) Process

Once we have figured out the modulation and operating frequency, we can start to process the signal using the GRC blocks and creating flow graphs. This usually includes things like demodulating the live/captured signal, amplifying the signal, porting it to Wireshark, and so on. We will discuss GRC in much more detail as we proceed covering things like usage of GRC blocks required to process a specific signal.

6) Decode

So once you get your hands on the bits/bitstream you can start decoding it. Commonly used encoding techniques are

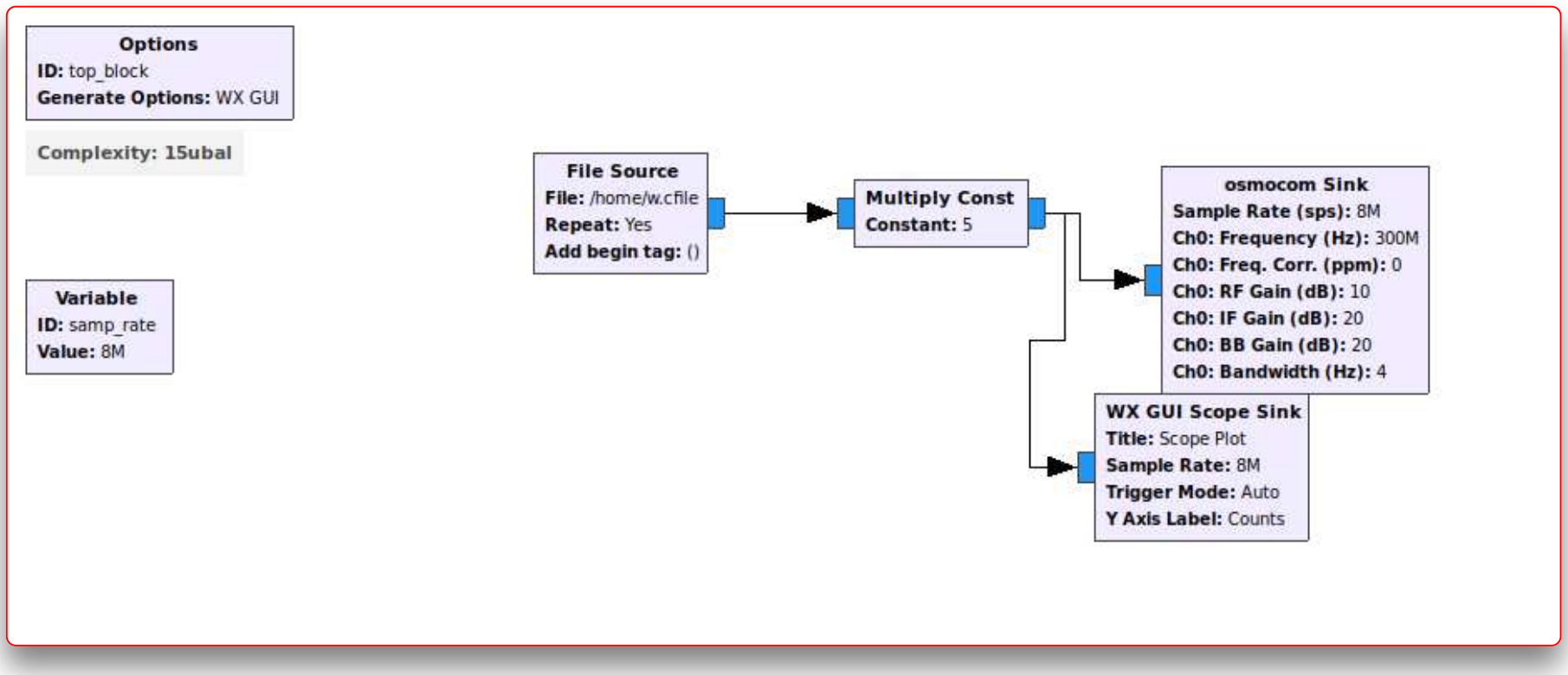
- NRZ
- NRZI
- Bipolar AMI
- Manchester

To name a few. You'll find them already present and ready to use in Universal Radio Hacker(URH).

7) Attack!

Once you are done reversing your signal i.e. figuring out things like modulation, encoding, data bytes, and other specifics. You can launch your attacks now! A most common one is the replay attack wherein one sends back the captured signal.

Steps 3 & 5 are not applicable for our target (since it is analog) But we have an attack for our target, we'll do a replay attack using GRC. Below is the respective GRC flowgraph. We replayed the captured signal .cfile.



Replaying the analog door bell signal (flowgraph)

Conclusion:

We hope you got a clear understanding of what are the major SDR software tools available and why is one better than the other. Also, a sneak-peak into how to approach an RF target would have given you an idea of the steps involved in an RF target assessment using SDR.

Continue to the next part - IoT Security - Part 10 (Introduction To MQTT Protocol and Security)

Resources:

- **GNURadio-Android**