Receiving Keyfob Signals with the Hackrf One
8/27/18

Objectives

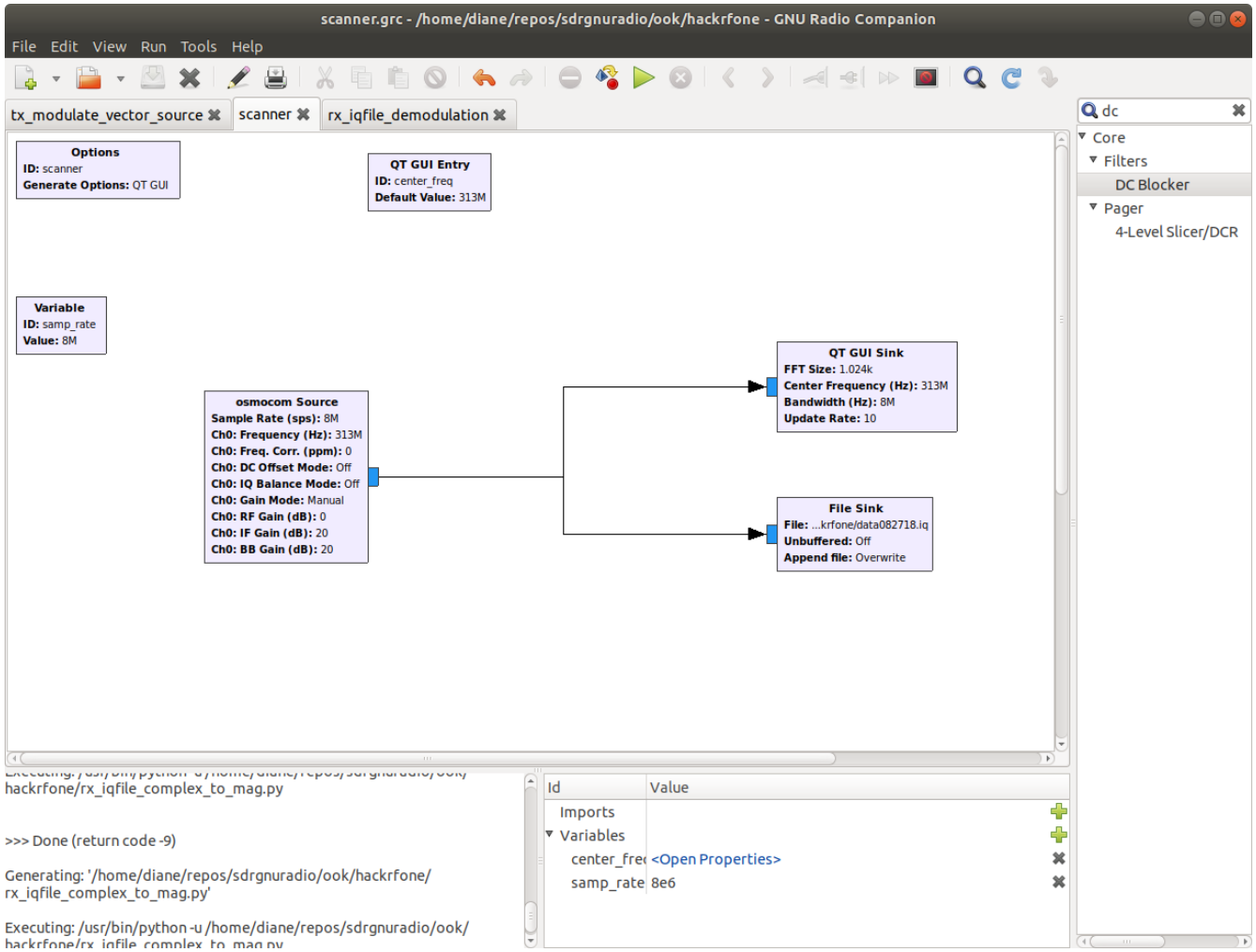
1. Hackrf One receives and records data transmitted from a keyfob
2. The OOK rx_clean_binary demodulation flow graph reads the recorded data, demodulates it, and converts it to binary.

Hackrf One receives and records data transmitted from a keyfob

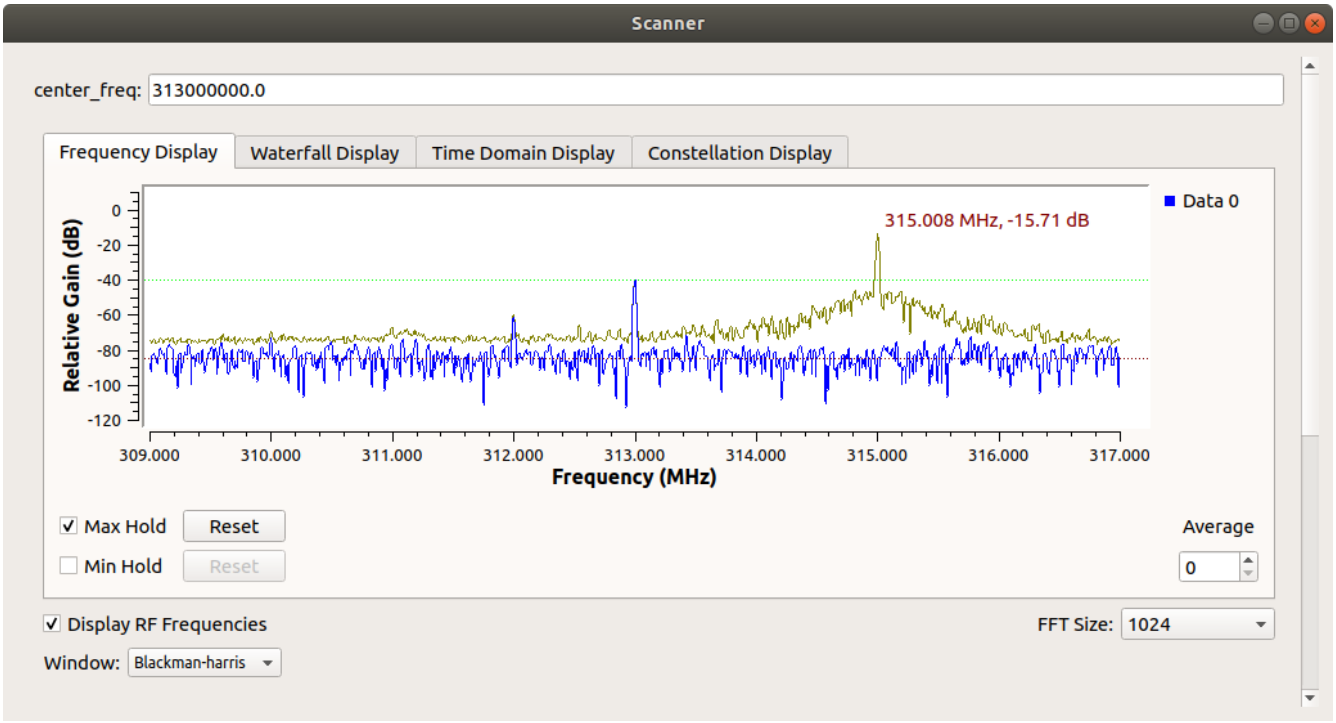
File name: scanner.grc

Location: https://github.com/willydlw/sdrgnuradio/tree/master/ook/hackrfone

The flowgraph image is shown below.



The keyfob was depressed several times to observe the keyfob's transmission frequency. The image below illustrates its frequency was approximately 315 MHz.



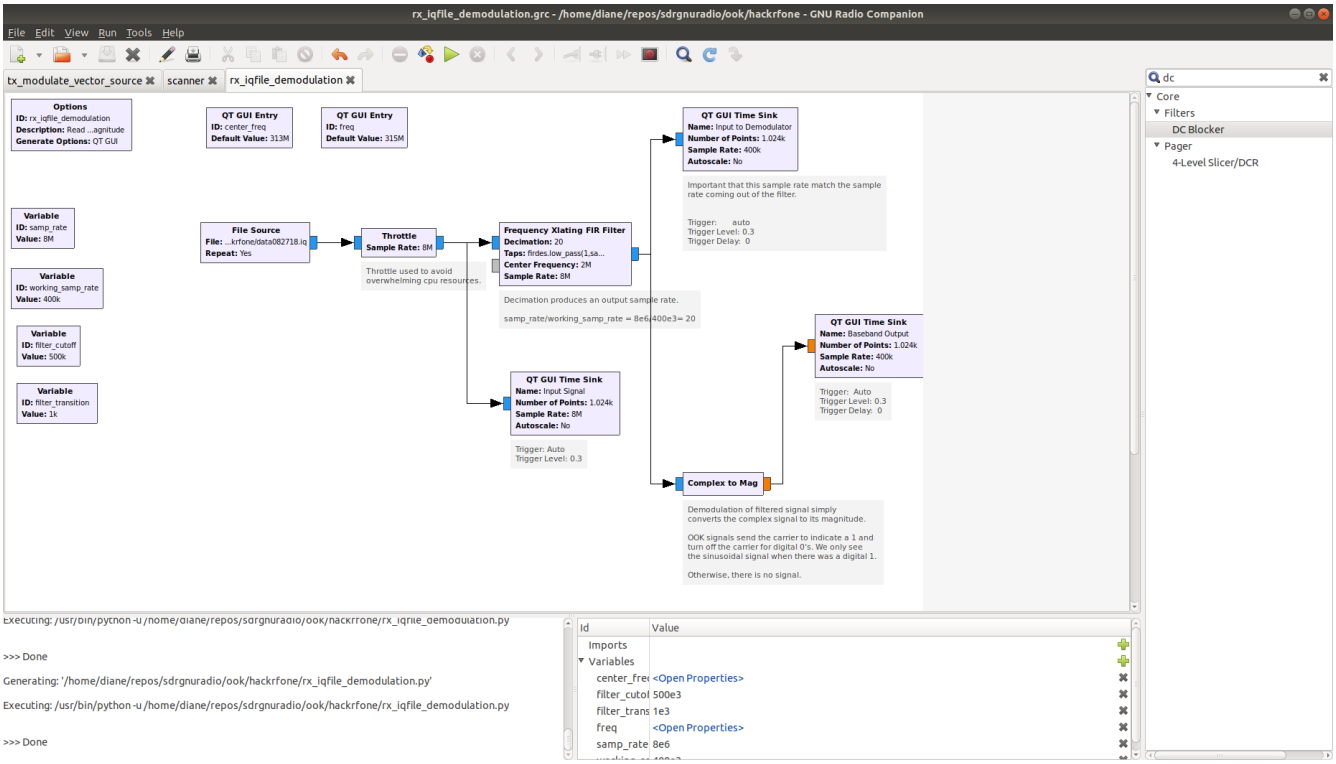
The keyfob buttons were depressed at non-regular intervals while the scanner flowgraph recorded the received signals in a file named data082718.iq. This recorded data was then used to meet objective 2, demodulating the data, and convert it to binary.

Convert recorded keyfob data to binary using OOK demodualtion

Two different flow graphs were used to illustrate the demodulation results.

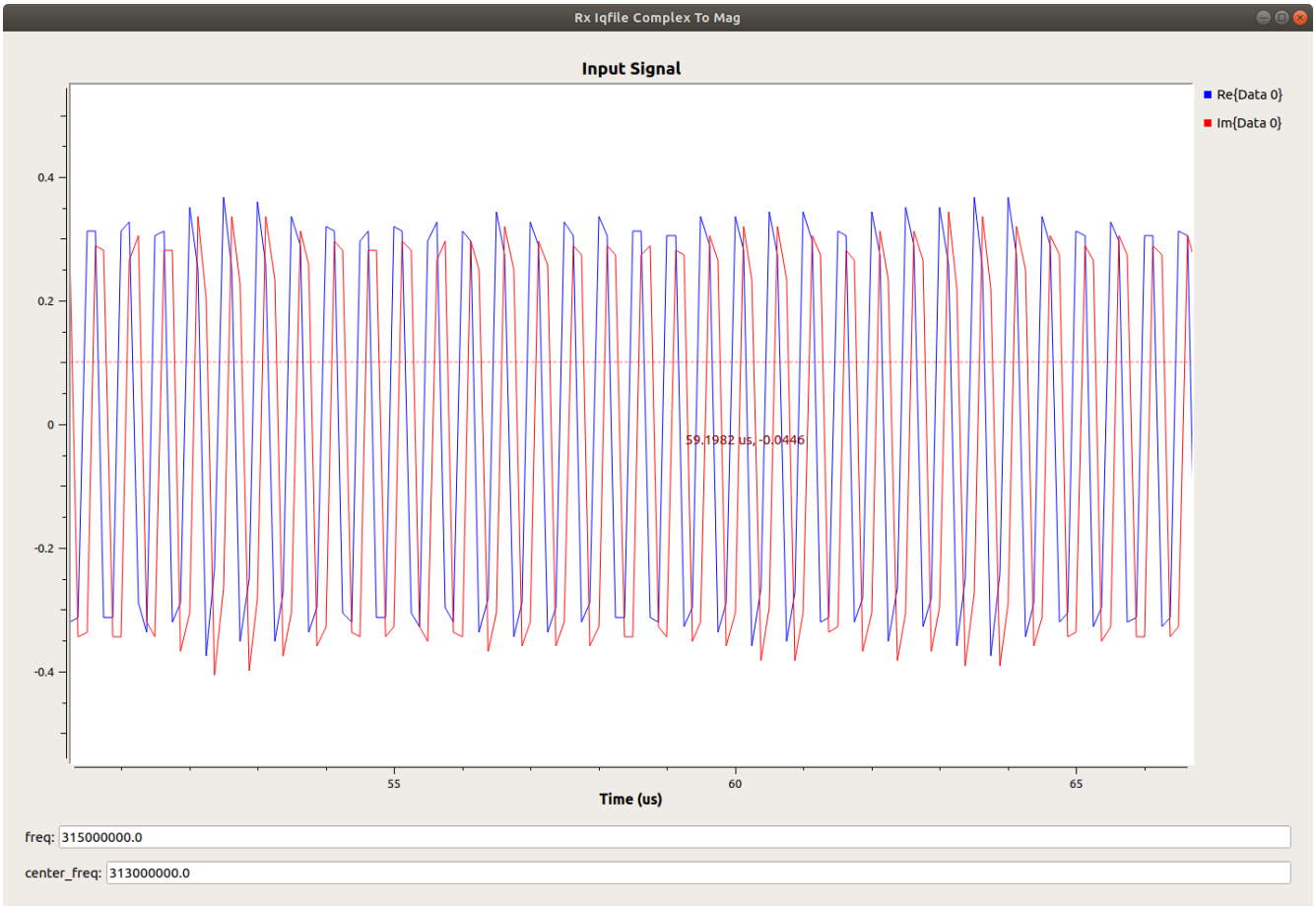
File: rx_iqfile_demodulation.src

Flow graph image

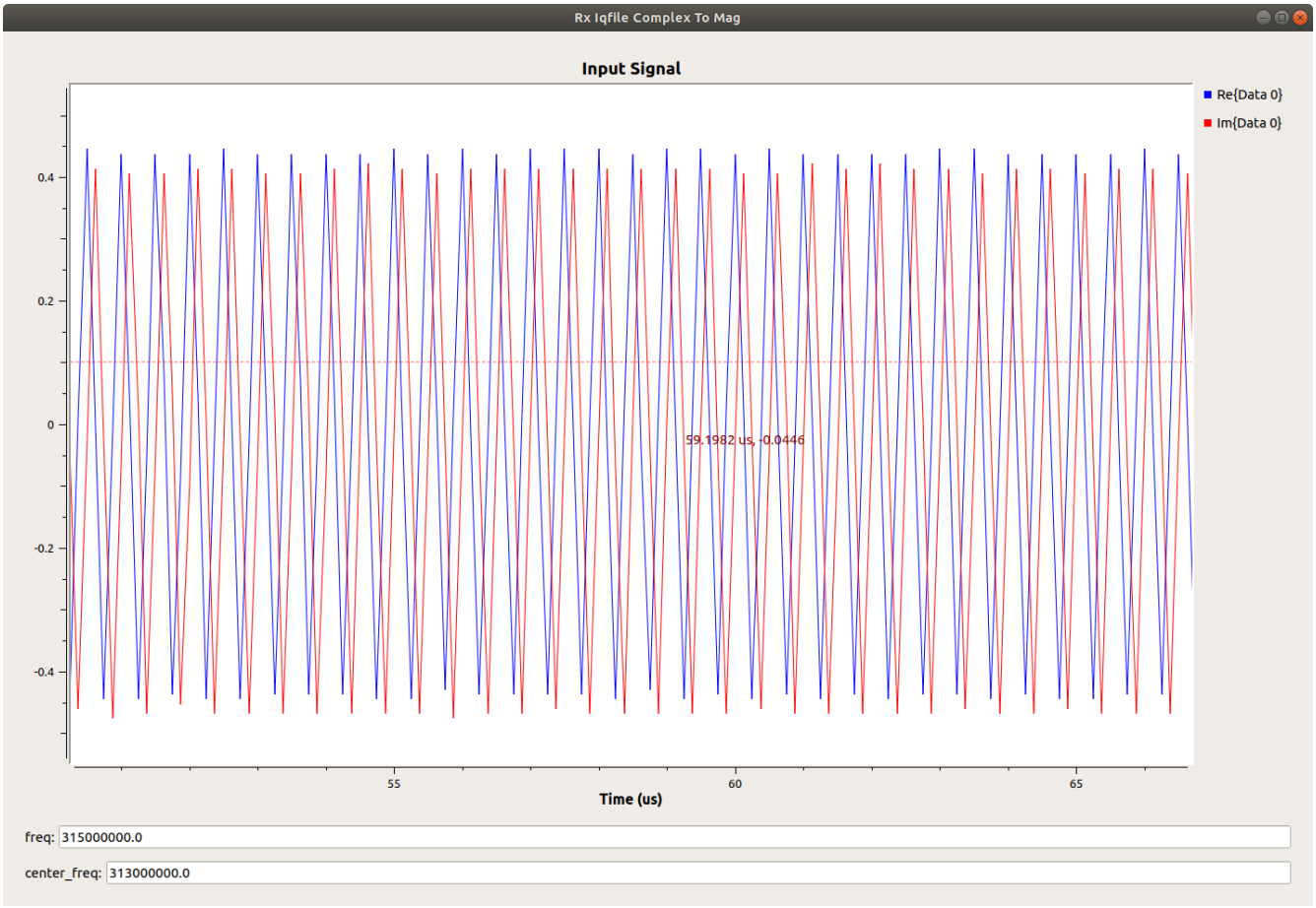


The program reads the recorded keyfob data from the file, data082718.iq, display the input signal before demodulation. The input signal amplitude was observed to generally fluctuate between 0.4, -0.4 or between 0.3, -0.3.

There were both unlock and lock key presses. Another experiment should be performed, pressing only one button to see if the amplitude is button specific, or to discover the reason for difference in the amplitude range.



The input signal amplitude above varies from 0.3 to -0.3.



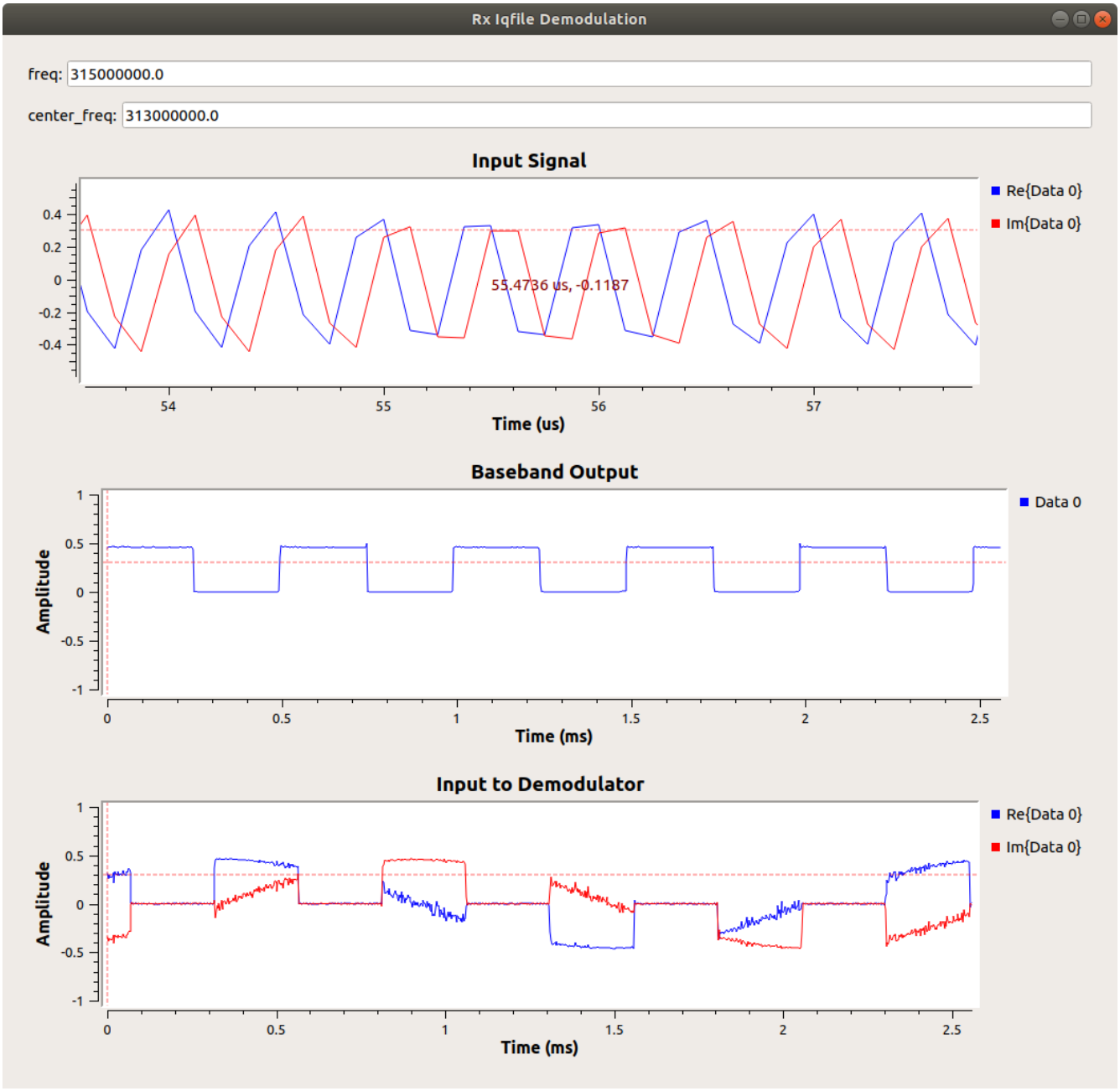
The input signal amplitude, above, varies consistently from approximately 0.4 to -0.4.

It was important to know the magnitude of these signals to set the trigger levels of the output sinks.

The next processing step is applying a low pass FIR filter. The filter's center frequency was 2 MHz, the difference of freq – center_freq = 315 MHz – 313 MHz. This downshifts the 315 MHz frequency to 2 MHz.

The low pass filter cutoff is 15 kHz, with a transition band of 1 kHz. The filtered signal is the input to the demodulator signal shown below. The demodulation is simply a conversion of the complex signal to its magnitude. This suffices for OOK because the carrier signal is broadcast unchanged for binary 1's and not transmitted at all for binary 0's.

The baseband output is the signal's magnitude. The image below shows these signals. The red dotted line is the trigger level setting.



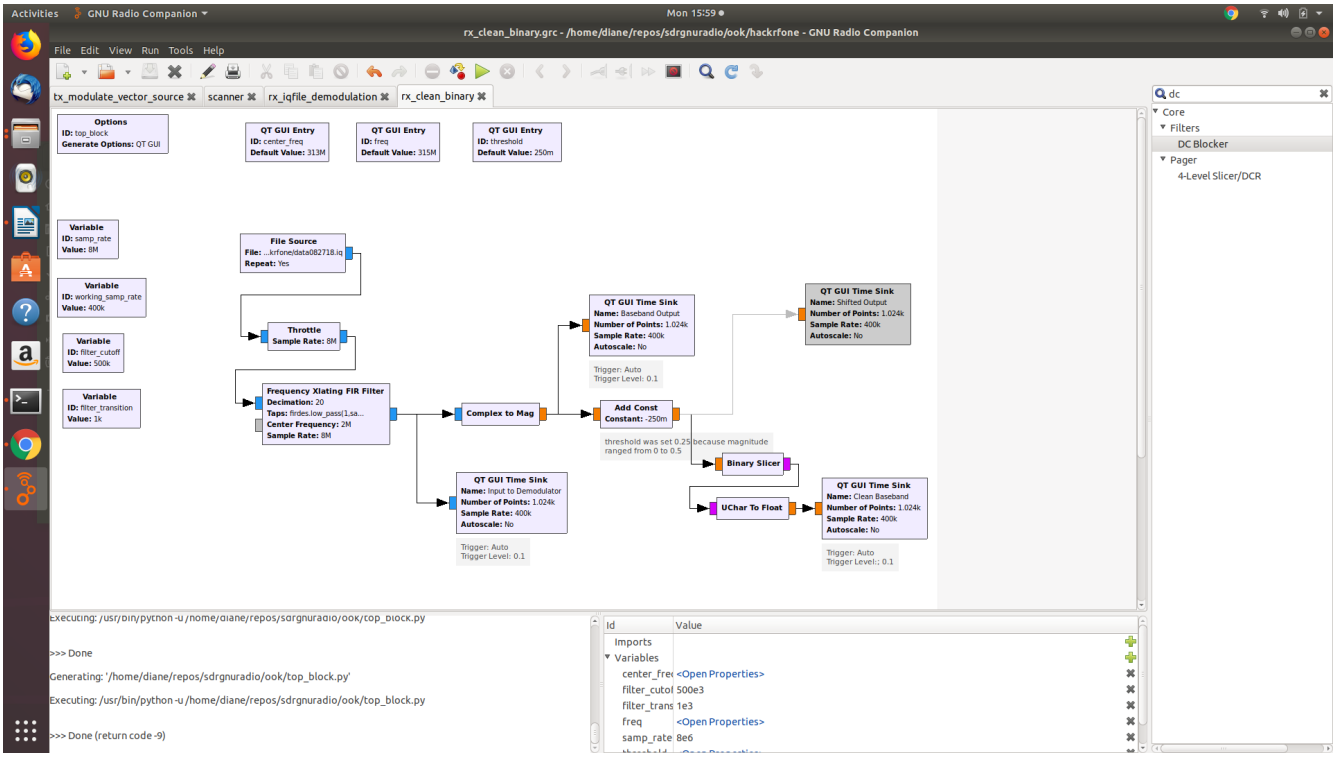
The input signal is a complex iq signal. It is still a complex signal after the filter stage, shown as input to the demodulator. The complex to magnitude demodulation produces the Baseband output signal, which varies between 0 and 0.5.

The next step is converting the magnitude to binary. The additional blocks are shown in the rx_clean_binary flowgraph below.

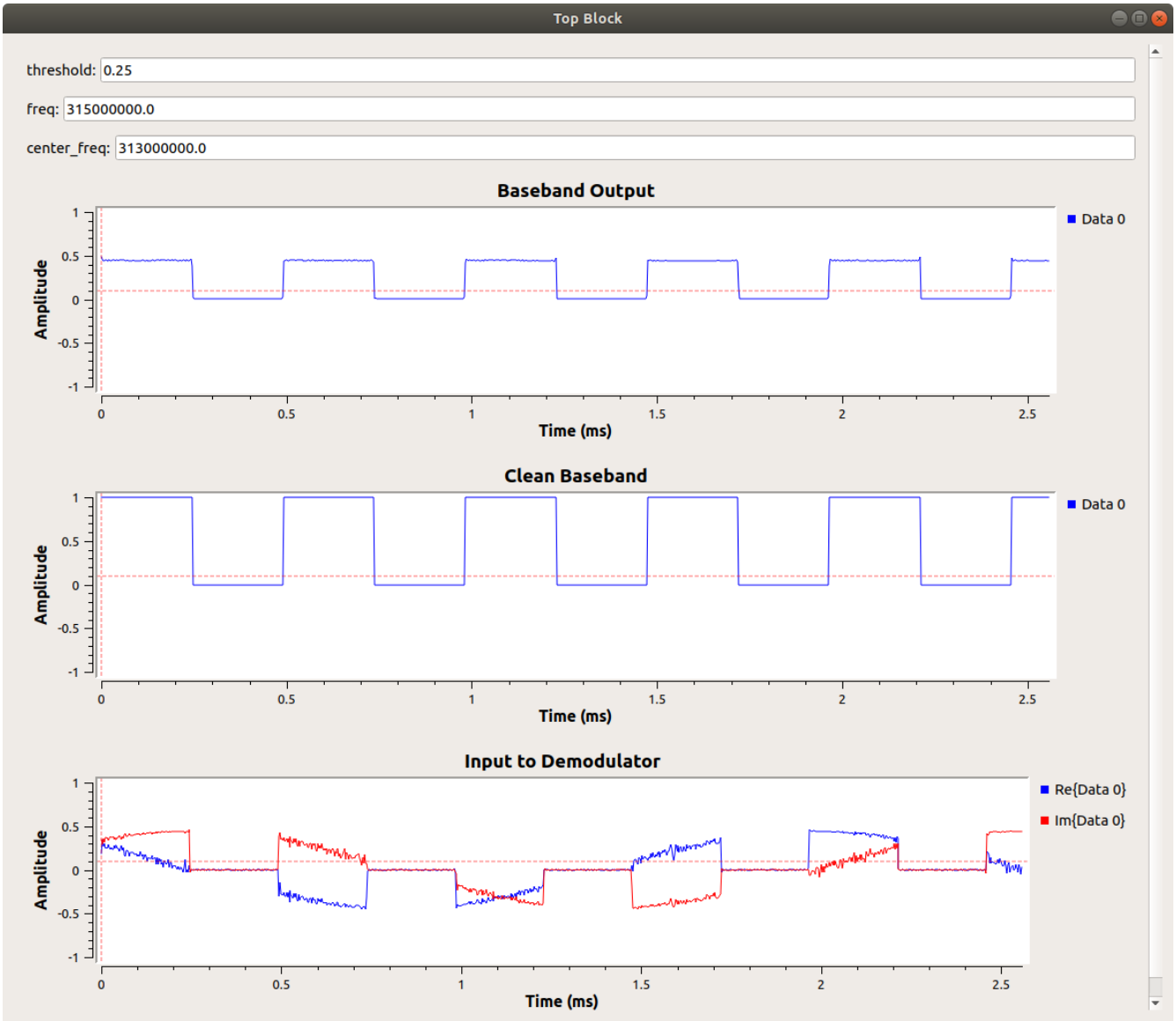
File: rx_clean_binary.grc

Add blocks to convert magnitude to binary values.

Flow graph



The threshold variable is set to 0.25, the half way point of the 0 to 0.5 magnitude range. Values above 0.25 are then treated a 1’s. Values below are treated as 0’s. The following output is produced.



The baseband output is scaled by adding a constant value of -0.25. The result is sent to a binary slicer block where values 0 to 1 are treated as 1's and values below 0 are treated as 0's. The information has to be converted back to a float to be shown in the QT Gui sink.

Note that the dotted red lines in the above image are the trigger levels for each sink.

It cannot be determined if this an accurate depiction of the 1's and 0's actually transmitted by the keyfob as the keyfob codes are unknown. To determine accuracy, this demodulation program will next be tested with known input values.

The objective was met. Captured data was converted to binary.