Hands-on guide to replaying a signal with CCManager

Tools

- SDR and complementing software of choice. A good combination is the RTL-SDR (hardware) and SDRSharp (http://airspy.com/download/).
- CCManager hardware & software (https://github.com/jglim/CCManager)
- Audacity (http://www.audacityteam.org/)

Identifying the signal

Signal frequency

Using the SDR, look through the popular frequencies, ideally within the below table while the device is transmitting.

300 MHz – 348 MHz,

387 MHz – 464 MHz,

779 MHz – 928 MHz

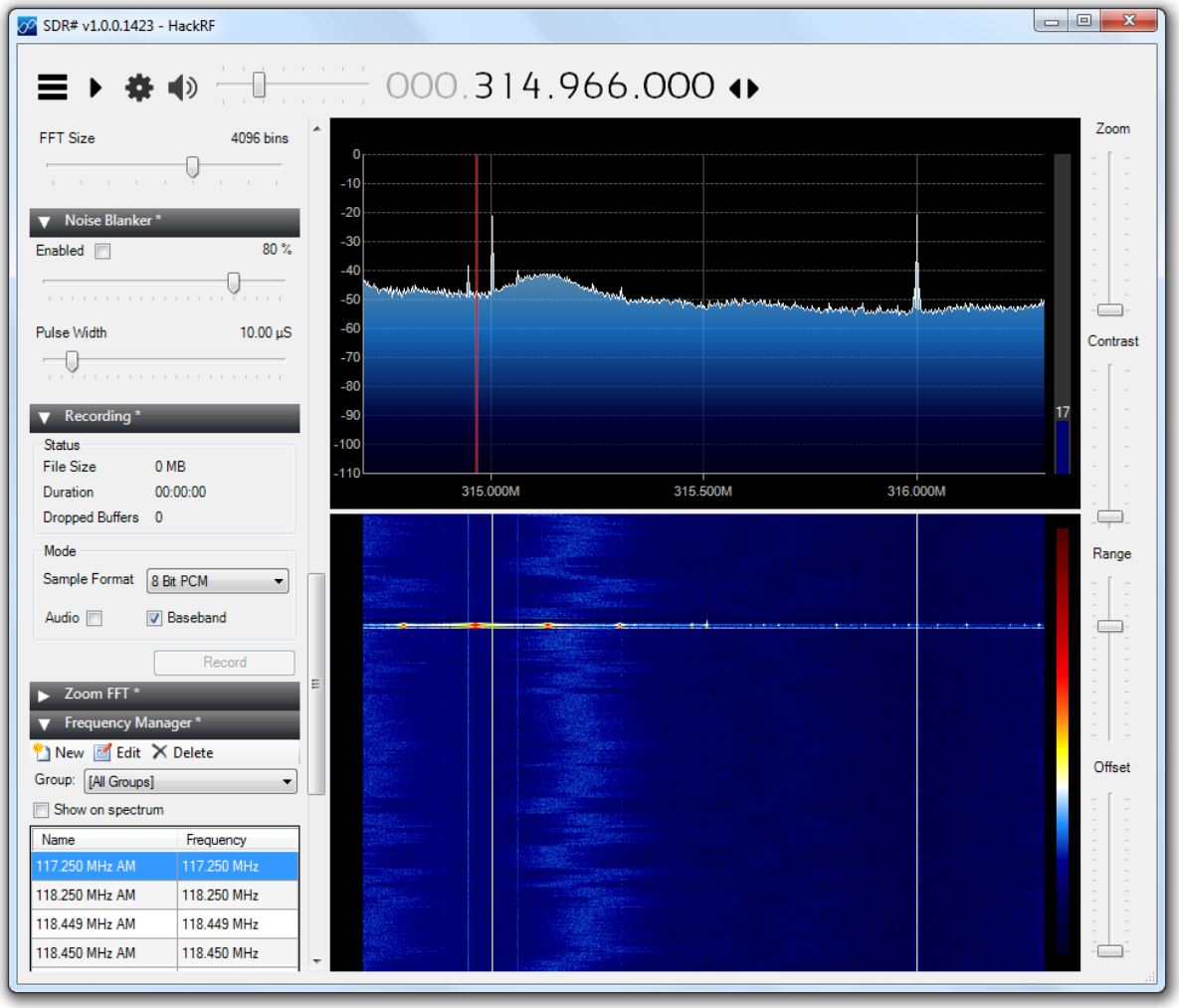
Those are common frequencies and within the CC1101's operating limits.

Checking the FCC ID of the transmitter may provide more details on its radio as well.

The type of signal modulation:

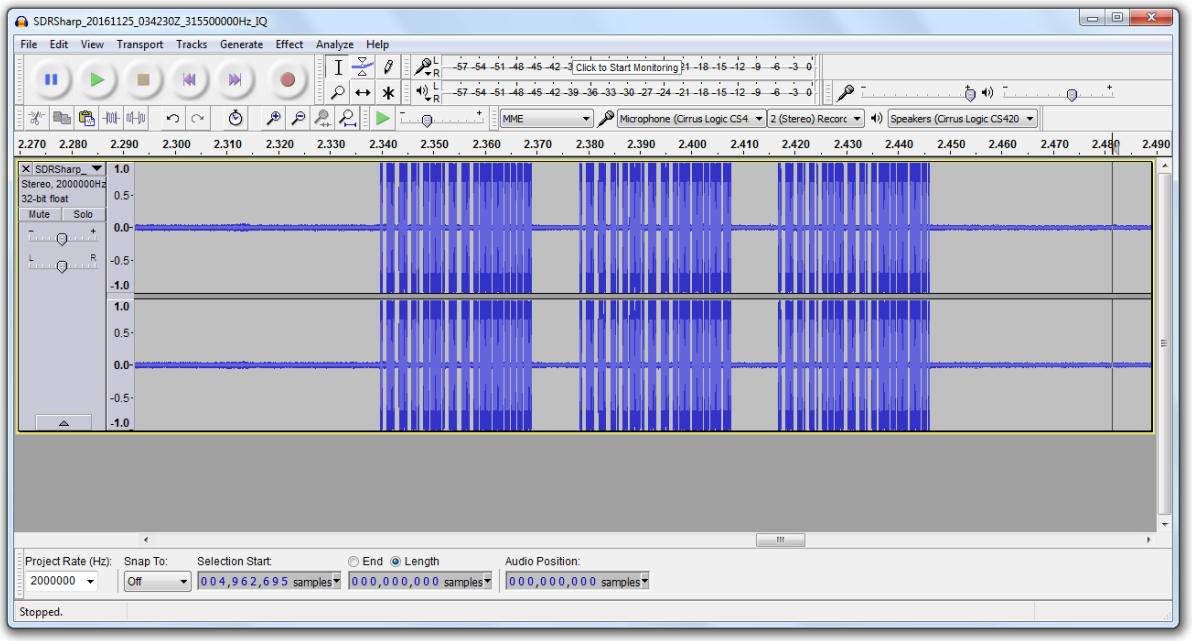
The signal should ideally it should be based on On-Off Keying, which was what CCManager was designed for. OOK is a simple technique where a transmission on a fixed frequency is toggled on and off as a means to relay data. The type of signal modulation can usually be assumed to be OOK for most lower-priced electronics.

Recording the signal



Record the transmission – use the IQ (Baseband) format where possible, as the next step will involve visualizing the transmission in Audacity (free audio software).

Analysing the signal

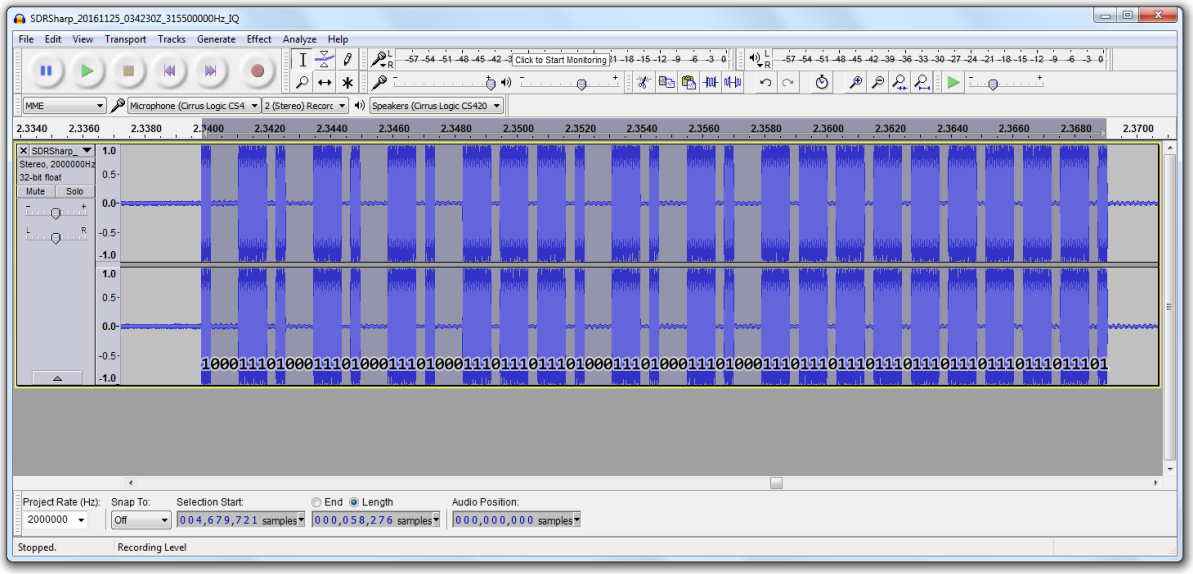


Our next step is to analyse (and thus digitize) the signal in preparation for transmission. To do so, we need to know 2 key pieces of information:

> **The transmission data itself (OOK can be represented in individual units of 1s and 0s during transmission)**
>
> **The speed of which the individual units (bits) of transmission data is sent – the baud rate.**

Open the baseband data in audacity. In my case, we can immediately identify a pattern where the signal is actually repeated thrice. This will come in useful later, as we can simply digitize the repeated portion and duplicate it thrice.

We shall zoom in and take a look at the unique data



Here, we can visually identify the types of marks (the active area - blue) and spaces (the empty area - grey).

The two distinct marks/spaces are *small* and *large*, where the *large* marks/spaces occupy a length of 3 *small* mark/spaces. To confirm this, select a region in Audacity and check the number of samples at the bottom of the screen.

Digitizing the signal

The next step is to identify the marks and spaces, and transcribe these into 1s and 0s based on the smallest unit. In the image above, I have overlaid the data (1 for mark, 0 for space) with Photoshop.

The result in binary is:

```
10001110100011101000111010001110111011101000111010001110100011101110111011101110111011101110111011101
```

To work in bytes, the data is grouped in 8 digits and converted to bytes

```
10001110 -> 8E
10001110 -> 8E
10001110 -> 8E
10001110 -> 8E
11101110 -> EE
10001110 -> 8E
10001110 -> 8E
10001110 -> 8E
11101110 -> EE
11101110 -> EE
11101110 -> EE
11101110 -> EE
10000000 -> 80 (zeroes are added to the end of it to make it align to 1 byte)
```

Rewriting the above in bytes will give us

```
0x8E, 0x8E, 0x8E, 0x8E, 0xEE, 0x8E, 0x8E, 0x8E, 0xEE, 0xEE, 0xEE, 0xEE, 0x80
```

After adding some spaces (`0x00`) and repeating it thrice, we get

```
0x8E, 0x8E, 0x8E, 0x8E, 0xEE, 0x8E, 0x8E, 0x8E, 0xEE, 0xEE, 0xEE, 0xEE, 0x80, 0x00, 0x00, 0x00,
0x8E, 0x8E, 0x8E, 0x8E, 0xEE, 0x8E, 0x8E, 0x8E, 0xEE, 0xEE, 0xEE, 0xEE, 0x80, 0x00, 0x00, 0x00,
0x8E, 0x8E, 0x8E, 0x8E, 0xEE, 0x8E, 0x8E, 0x8E, 0xEE, 0xEE, 0xEE, 0xEE, 0x80, 0x00, 0x00, 0x00
```

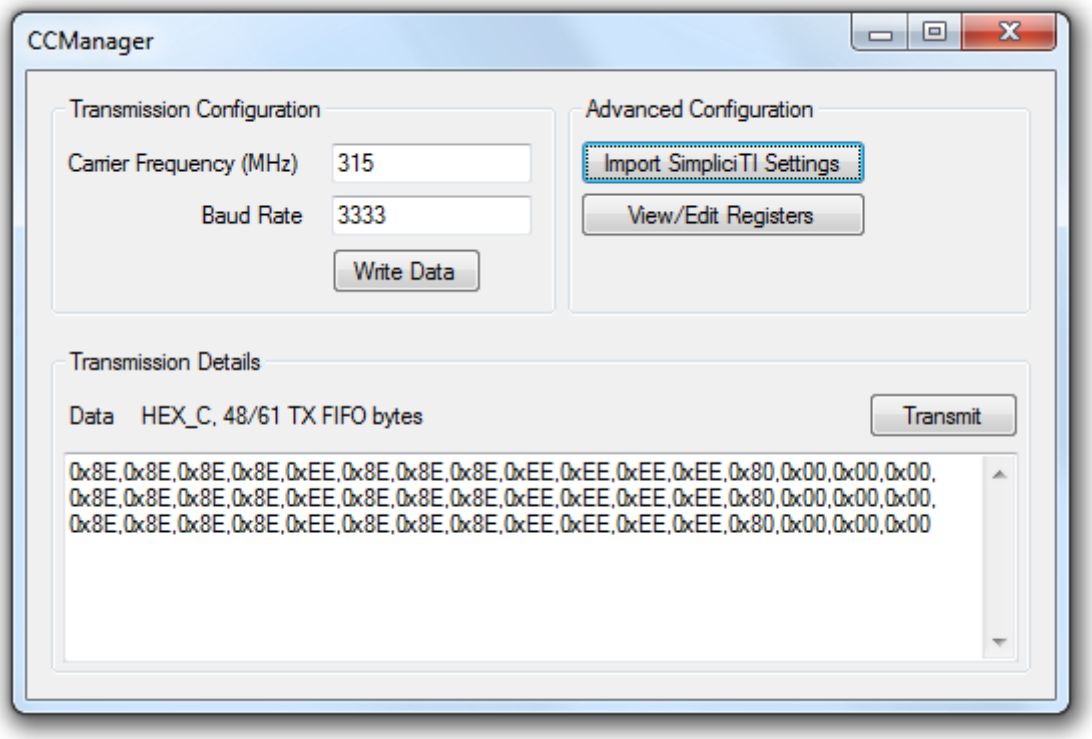
And the above gives us the data! Now to determine the baud rate:

The transmission duration of the original 97 bits (in the binary data) is measured at 58276 samples. As the recording was made at 2000 000 Hz, the calculation below can be used to determine the baud rate.

```
97 bits -> 58276 samples
1 bit   -> ~ 600 samples
600 samples / 2000000 Hz = ~ 0.0003 seconds (time to transmit 1 bit)
1 second / 0.0003 (time to transmit 1 bit) = ~ 3,333 (baud rate)
```

With the data, baud rate and frequency, we can now enter this information into CCManager to replay the signal!

Transmitting the signal



Insert the values for Carrier Frequency, Baud Rate, and Data.

Press Write Data, and then Transmit – you should see your signal being transmitted! Congratulations ^_^

Thanks for taking your time to read this and look into CCManager

-JG