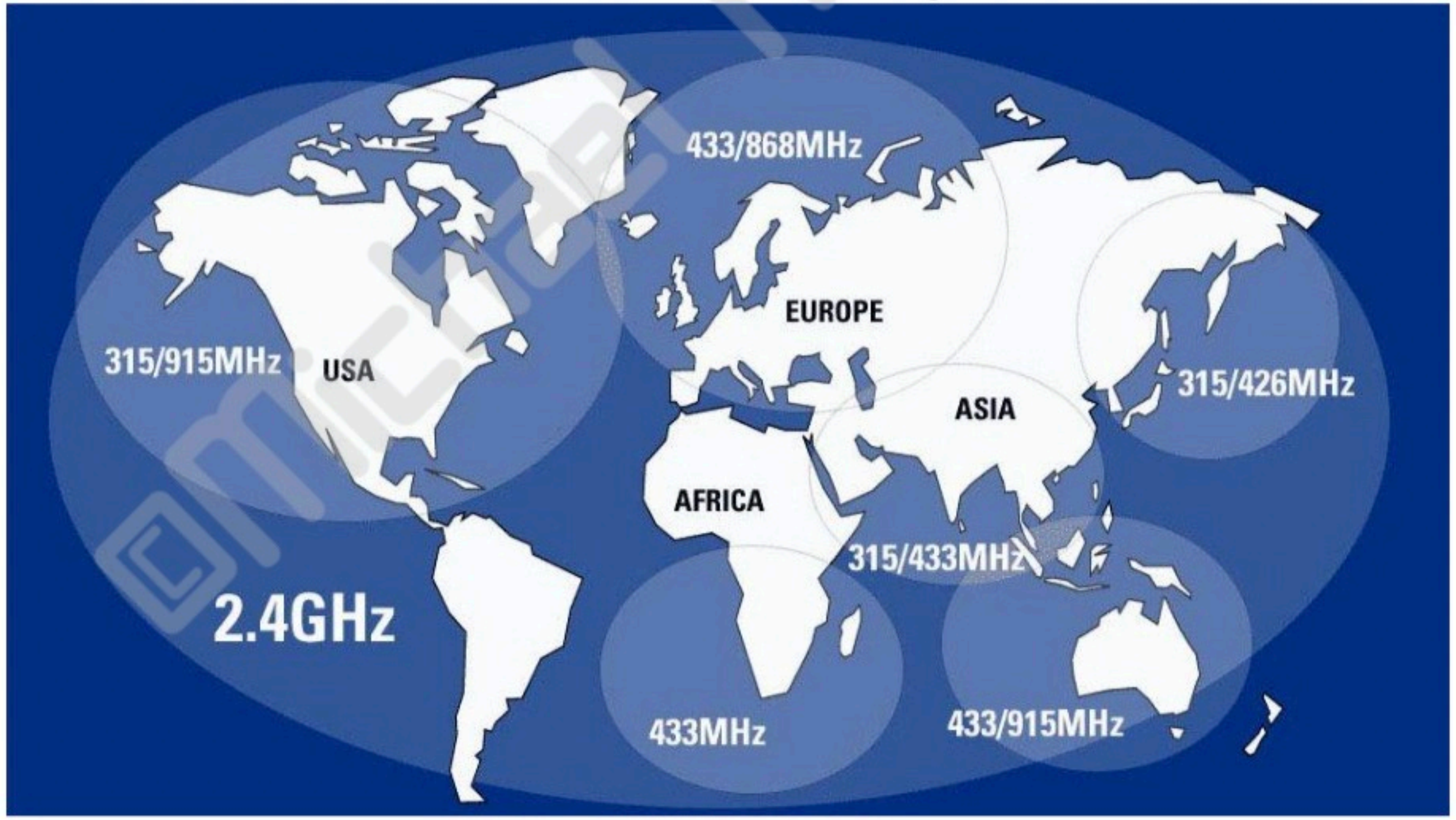
DAKOTA STATE UNIVERSITY®

SDRs on the Offense

Dr. Mike Ham

ISM Bands

- Industrial, Scientific and Medical
- Unlicensed spectrum, basically a playground for wireless devices
- So much hasn’t been looked at for security



What Also Lives in ISM?

- Doorbells
- Garage door openers
- Fixed key remotes (car fobs)
- Security systems
- Wireless power outlets
- Restaurant pagers
- WiFI
- Cordless Phones
- ZigBee
- Smart Home/IoT
- Etc.

Replay Attacks

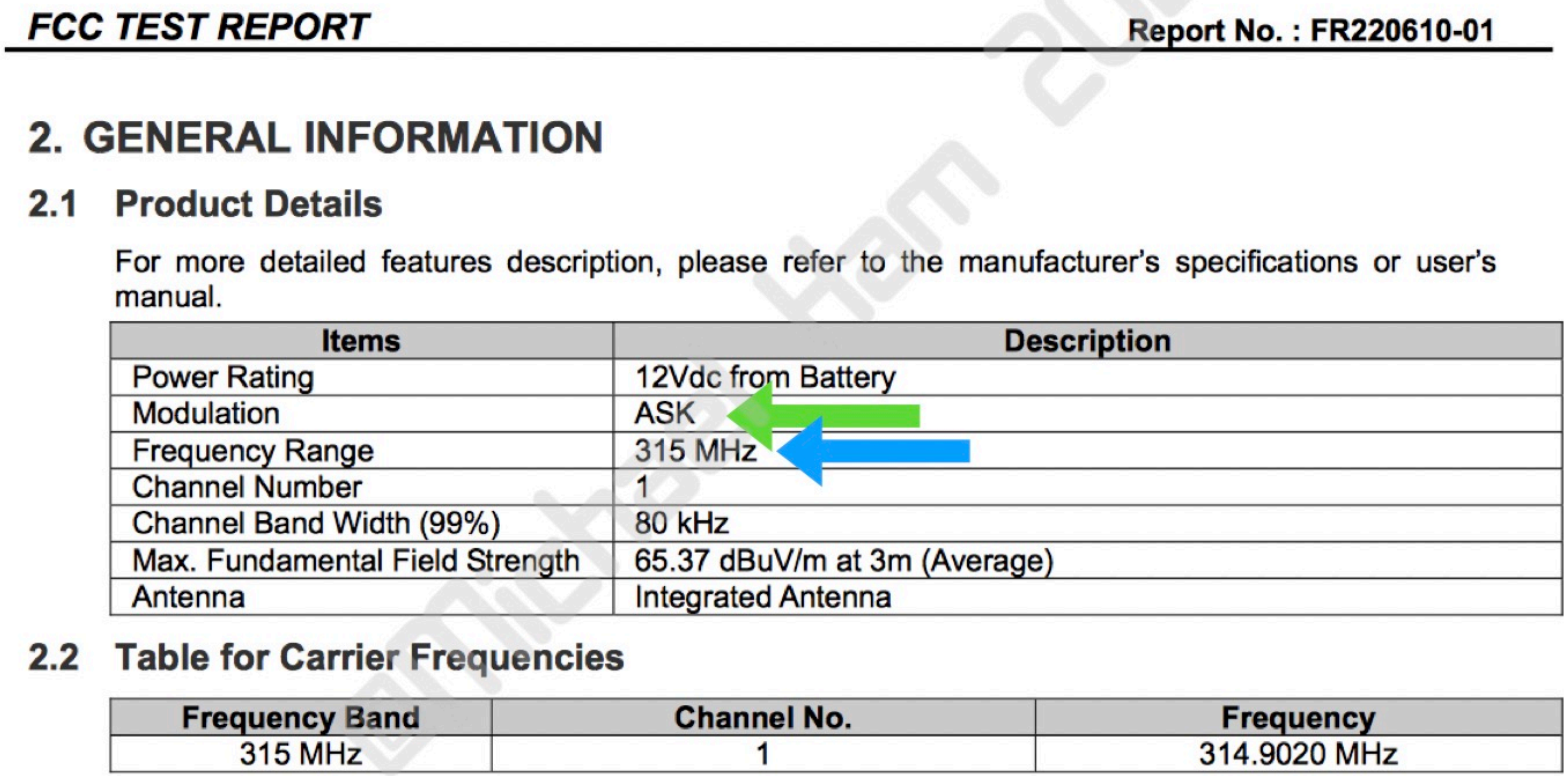
- We don’t need to go overboard with radio theory, we will:

1. Gather intel on the devices we want to hack
2. Sniff the wireless signals
3. Figure out the modulation technique
4. Decode the signal
5. Replay the signal and win!

Gathering Intel

- The FCC has made our job really easy for US devices
- Look on the back of your wireless devices, there's usually a number
  - e.g. PAGTR-009-1B
- https://www.fcc.gov/oet/ea/fccid
- Look at the test report
- Sometimes they'll just show the frequency

FCC Test Report



FCC TEST REPORT **Report No. : FR220610-01**

2. GENERAL INFORMATION

2.1 Product Details

For more detailed features description, please refer to the manufacturer's specifications or user's manual.

Items	Description
Power Rating	12Vdc from Battery
Modulation	ASK
Frequency Range	315 MHz
Channel Number	1
Channel Band Width (99%)	80 kHz
Max. Fundamental Field Strength	65.37 dBuV/m at 3m (Average)
Antenna	Integrated Antenna

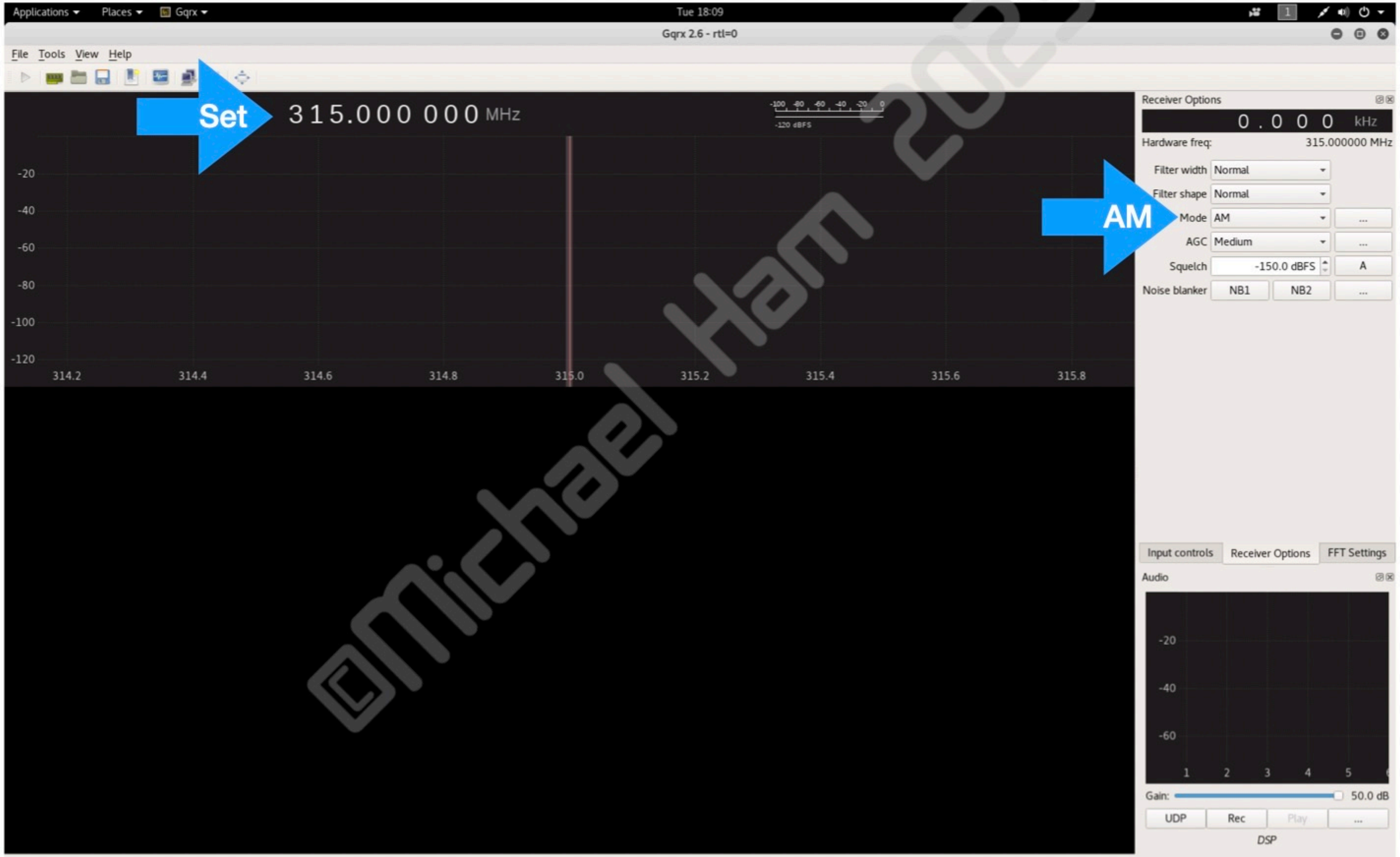
2.2 Table for Carrier Frequencies

Frequency Band	Channel No.	Frequency
315 MHz	1	314.9020 MHz

What Did You Learn?

- Now you know where to look for the signal (frequency)
  - This is half the battle, remember the ISM bands though!
- What type of modulation the device is using (ours is ASK/OOK)
- Fire up your SDR and start to sniff the signal!
  - Capture a waveform using **gqrx**

Sniffing With gqrx



Gqrx 2.6 - rtl=0

Set

315.000 000 MHz

0.000 kHz

Hardware freq: 315.000000 MHz

Filter width Normal

Filter shape Normal

AM

Mode AM

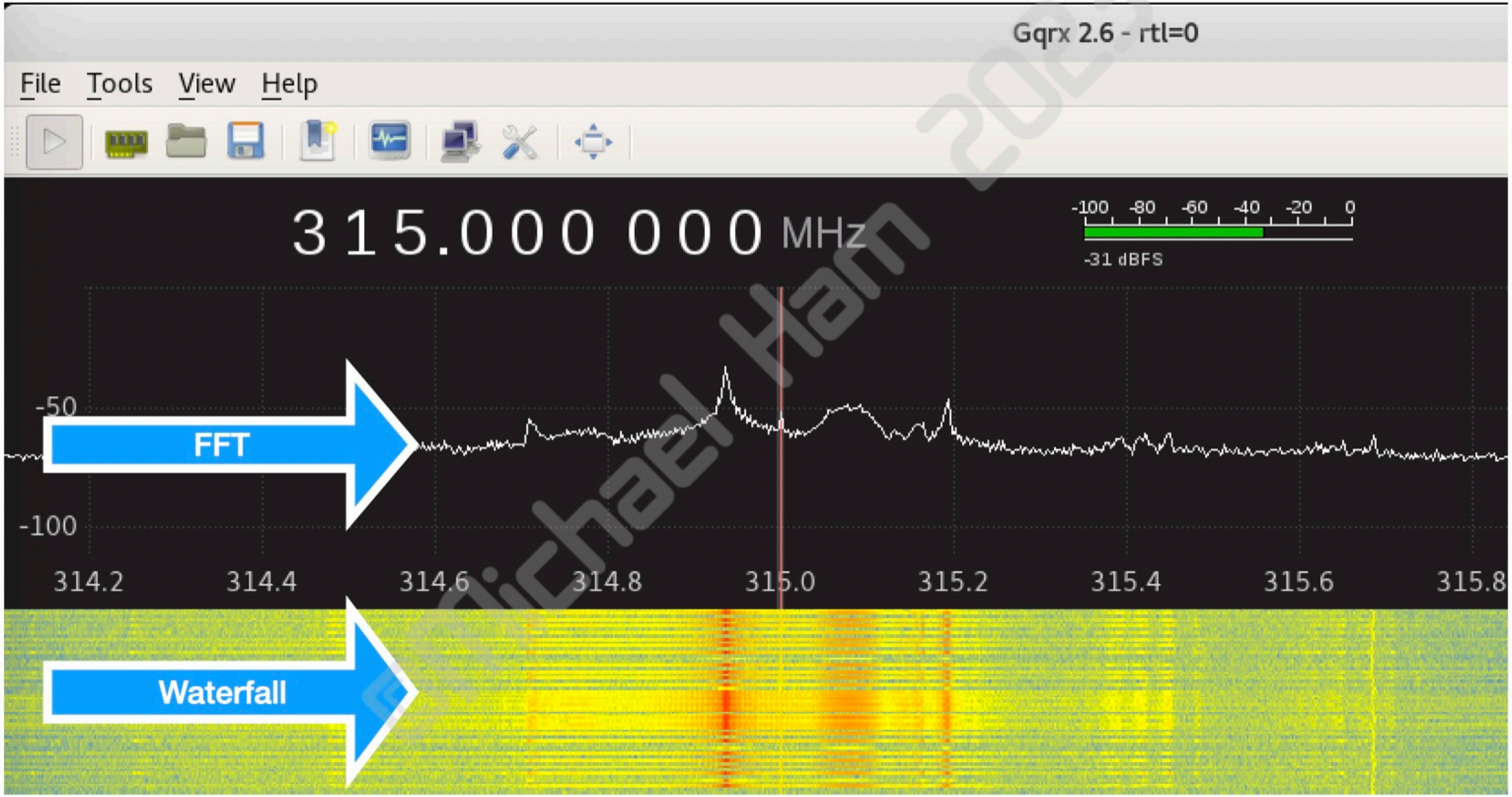
AGC Medium

Squelch -150.0 dBFS

Noise blanker

Gain: 50.0 dB

Our Signal Was Off…



Modulation

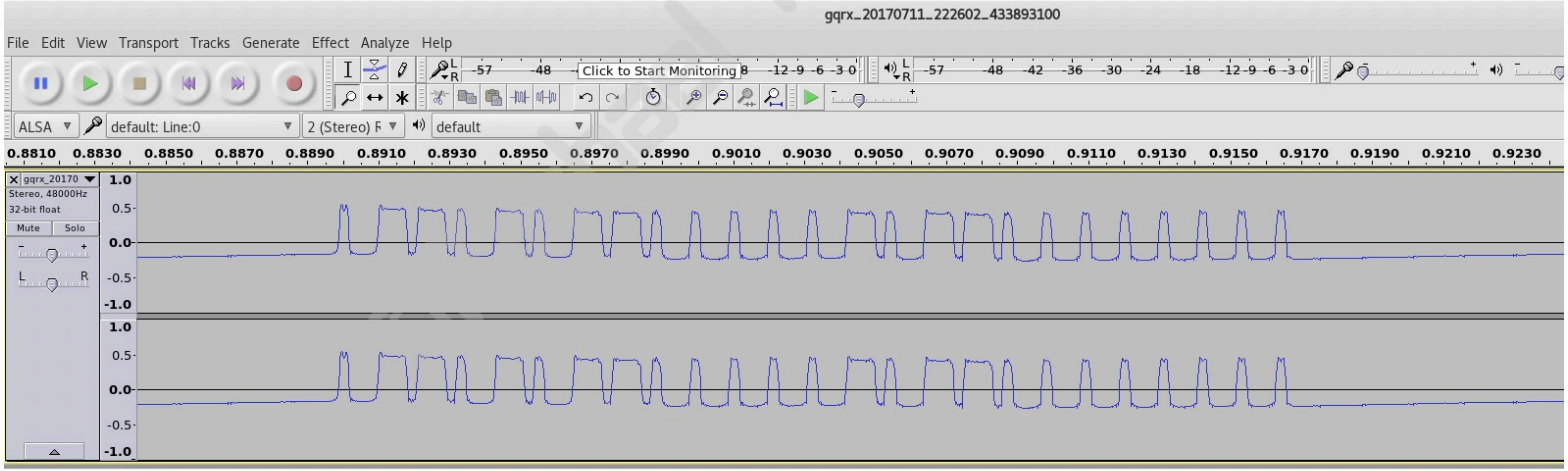
- Modulation is the act of changing a signal to transmit useful data
- Amplitude, frequency, and phase can be changed
- Many different ways to send data over a wireless signal
- Modulation effectively tells you how to decode that data

Figure out the Modulation

- The FCC page said it was ASK, but there are different types within that category
- Set up gqrx to record the signal so you can figure it out
  - **audacity** is a good tool to analyze simple signals
- We'll record the signal as if it were music, and open it up to see the waveform - this will help determine the modulation used

Using Audacity

- To install on Kali: **apt-get install audacity -y**
- Run audacity: **audacity**
- Open up the file that you recorded in gqrx, usually in ***/root/gqrx_XXX.wav***



ASK/OOK

- We learned from the FCC, we are working with ASK
- Amplitude Shift Keying
- On-off Keying or OOK is the simplest form, used to transmit Morse code
    - If the signal is up, it represents a 1
    - If it is down, the signal represents a 0

Let’s Demodulate OOK

- Find smallest wave - this will represent 1 bit
- Draw out the 1’s and 0’s (binary)
- Covert the binary data into hexadecimal
  - Write a program or look up a converter online

2550
1.2560
1.2570
1.2580
1.2590
1.2600
1.2610
1.2620
1.2630
1.2640
1.2650
1.2660
1.2670
1.2680
1.2690

2550
1.2560
1.2570
1.2580
1.2590
1.2600
1.2610
1.2620
1.2630
1.2640
1.2650
1.2660
1.2670
1.2680
1.2690
0
5
0
5
0

All Done

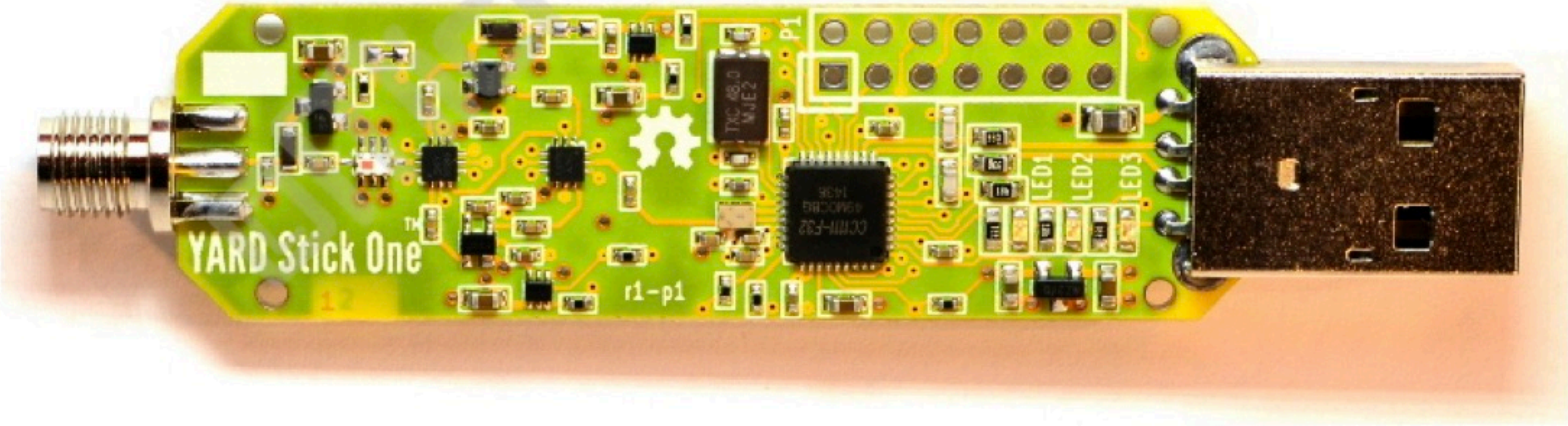
2550
1.2560
1.2570
1.2580
1.2590
1.2600
1.2610
1.2620
1.2630
1.2640
1.2650
1.2660
1.2670
1.2680
1.2690
64 Bits
1000 1110 1110 1000 1110 1000 1000 1000 1000 1000 1110 1000 1000 1000 1000 1110
8 E E 8 E 8 8 8 8 8 E 8 8 8 8 E

Now What?

1. ~~Gather intel on the devices we want to hack~~ 315MHz, ASK
2. ~~Sniff the wireless signals~~
3. ~~Figure out the modulation technique~~ OOK
4. ~~Decode the signal~~ 8EE8E88888E8888E
5. Replay the signal and win!

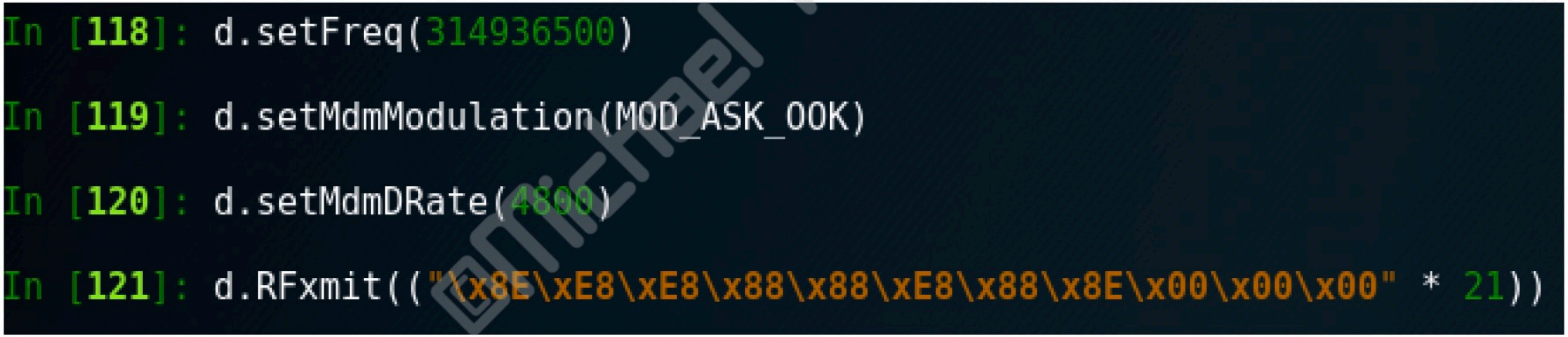
Transmitting Device

- You’re going to need something that can actually send signals out too
- YARD Stick One
    - Yet Another Radio Dongle
- YARD Stick One is a sub-1 GHz wireless test tool



Running rfcat

- Moment of truth, we’ll set:
  - Frequency, modulation, baud rate (how fast), the code
  - Repeat the code to make sure the outlet gets it



```
In [118]: d.setFreq(314936500)

In [119]: d.setMdmModulation(MOD_ASK_OOK)

In [120]: d.setMdmDRate(4800)

In [121]: d.RFxmit(("\x8E\xE8\xE8\x88\x88\xE8\x88\x8E\x00\x00\x00" * 21))
```