Selec Astronomy - Fun with Signals

BSides Canberra 2018

13 Apr 2018

#WhoAmI²

- Ando
  - Pentester\TI Analyst
  - Wireless hacking for work and play
  - Organiser of Cyberspectrum: Canberra SDR
- Matt
  - Ex Pentester/ Wireless hacking for work and play

Intent / Objectives

- Today we want to show you:
- Hack the Wireless World
- Super Cheap Rapid Radio Reversing
- Security is not obtained through Obscurity - the wireless spectrum is cheaper to interface with

SDR - How Cheap?

- RTL-SDR: Cost $17 plus Arduino Uno $4 433MHz TX/RX $2
- Chronic: Cost ~$100, Looking like (a lame) James Bond: Priceless
  - Includes a RFcat compatible dongle!
- PandwaRF ~$200 Sub 1GHz
- YardStick One ~$200 Sub 1GHz
- HackRF ($415) + Portapack ($250) Half Duplex
- LimeSDR: Cost $415 - Duplex MIMO
- Blade RF: $$
- USRP (many versions): $$$

TX for under 30 AUD!!!!!
Or $2 with last year's BSides Badge

Targets

- Doorbells
- Garage doors
- Baby monitors
- Security systems
- IOT - Home automation, Industry 4.0
- Smart Cities
- Smart Power Meters
- Bluetooth device
- https://www.iotaustralia.org.au/2016/07/20/iotnewanz/meshed-offers-free-access-lorawan-network-sydney/

The Theory

- RF Theory and practice
- RF Modulation and Encoding
- How to manually analyse a Signal

The Workshop

- Walk thru analysis of the pager signals; TX and capture as we go
- Ring some pagers and see if participants can extract the value

Workshop Pre-reqs

- If you don't trust our USBs;
- Start downloading now during the theory presentation!
- Inspectrum (from Github - kali repo version is out of date)
- osmocom_fft / the Kali Linux SDR metapackage

What is RADIO/RF

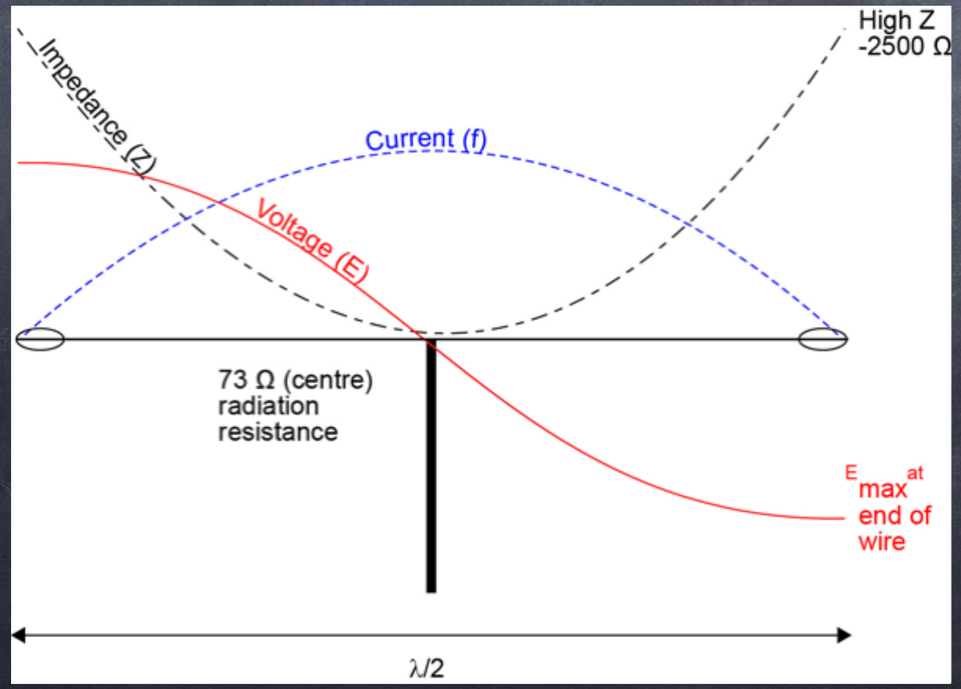
- High Frequency Alternating Current applied to a conductor.
- Electromagnetic Radiation consists of oscillating electric and magnetic fields.
- Propagation at near speed of light.

Electromagnetic Wave Length

- The frequency of the wave is equal to the frequency of oscillation. The wavelength (λ) is determined by the formula:
- $\lambda = c/f$
  - where λ is the radiated wavelength (m)
  - c is the accepted constant speed of light (300 000 000 m/s)
  - f is the frequency in hertz
- $\lambda = 300000000/433000000$
- $\lambda = 0.69m$

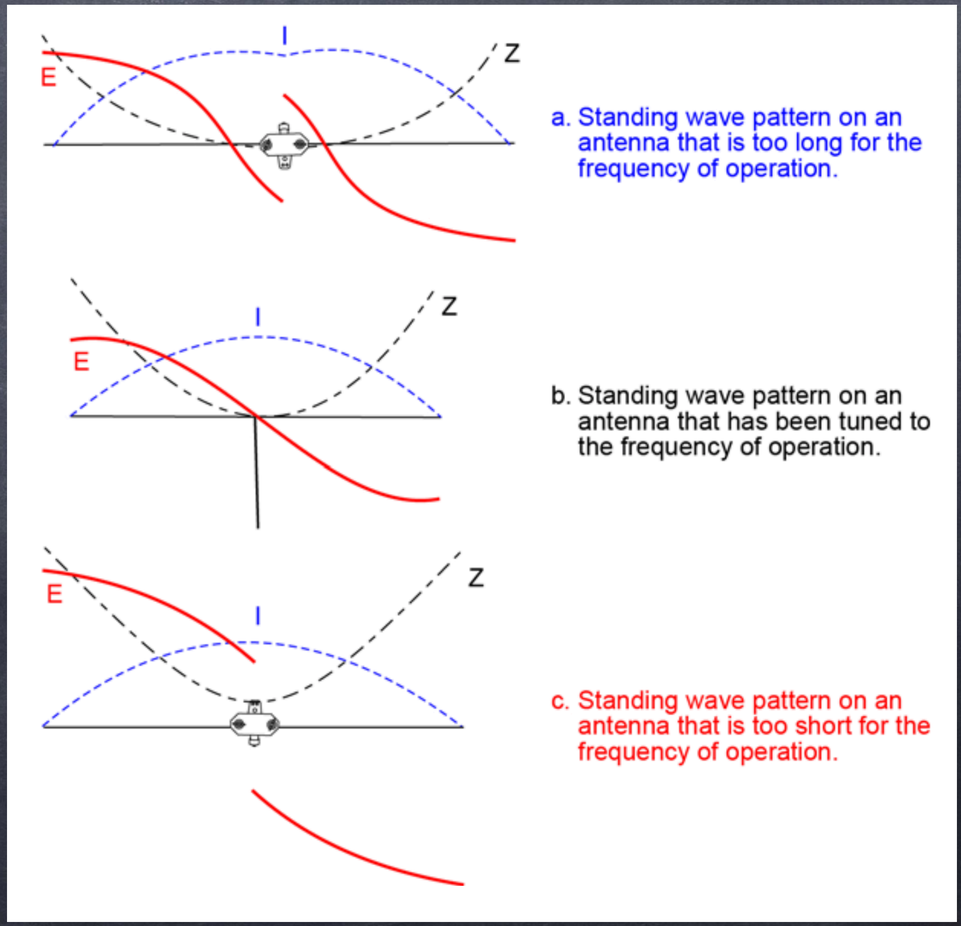
Antenna Length

- The Frequency of the RF Wave dictates the length of the radiating conductors/elements.
- A half RF wave radiating conductor



Why you should care about Antenna Length

- Incorrect length of conductor/element Impacts the formation of Electromagnetic field.
- Causes incomplete wave/propagation



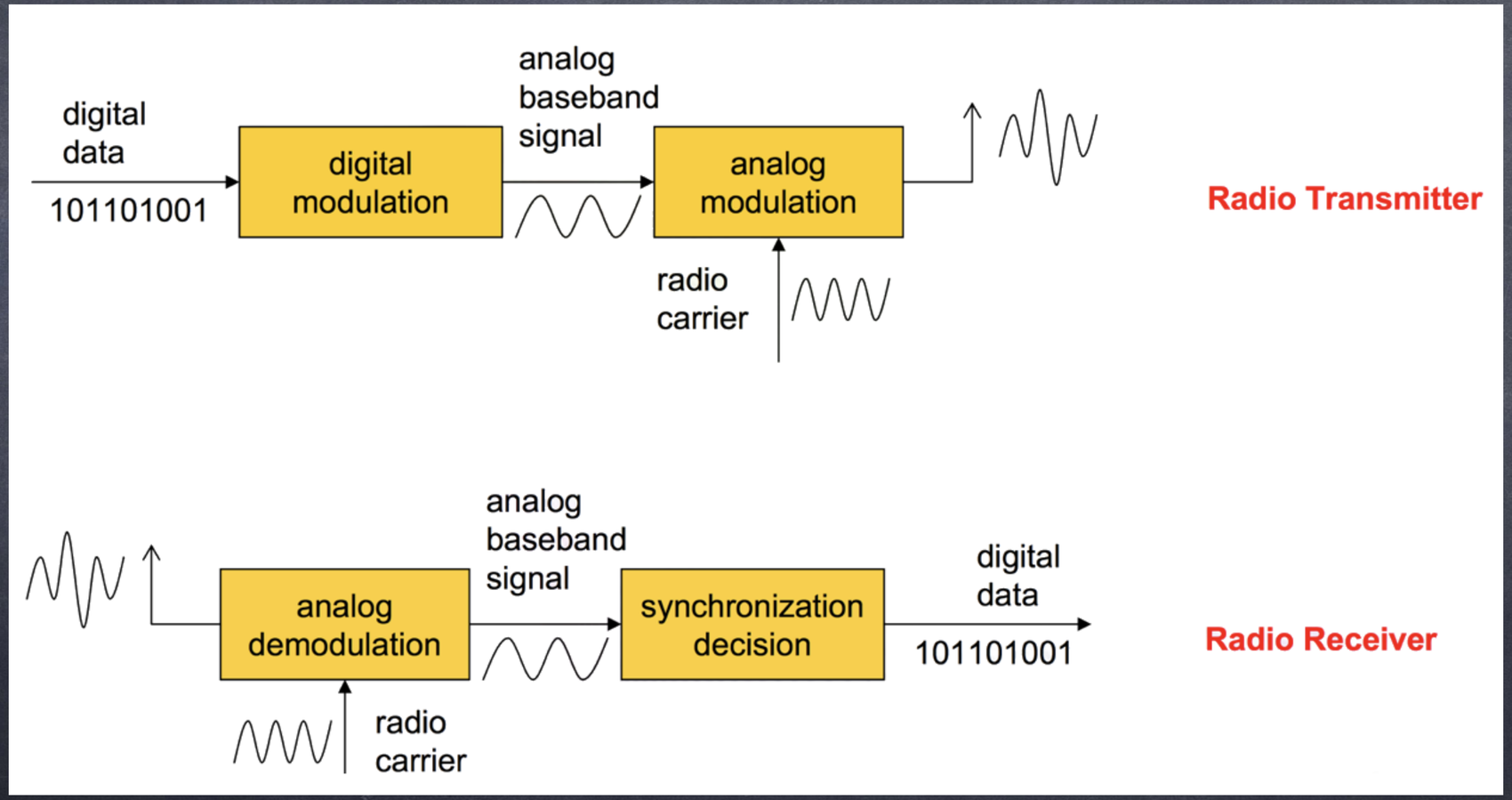
How is digital data transmitted?

- Raw RF wave is known as the Carrier Wave (CW).
- A separate data bearing signal is generated to express the data to be transmitted.
- The process of combining the two signals is known as Modulation.

Modulation Methods

- In sub-Ghz RF, there are two main modulation schemes:
  - Amplitude Modulation (AM): the amplitude of the carrier varies in accordance to the information signal
  - Frequency Modulation (FM): the frequency of the carrier varies in accordance to the information signal

Modulation and Demodulation



Digital Modulation

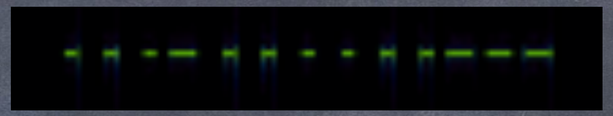
Modulation of digital signals is known as 'Shift Keying'

Two main types of Shift Keying in sub-Ghz RF:

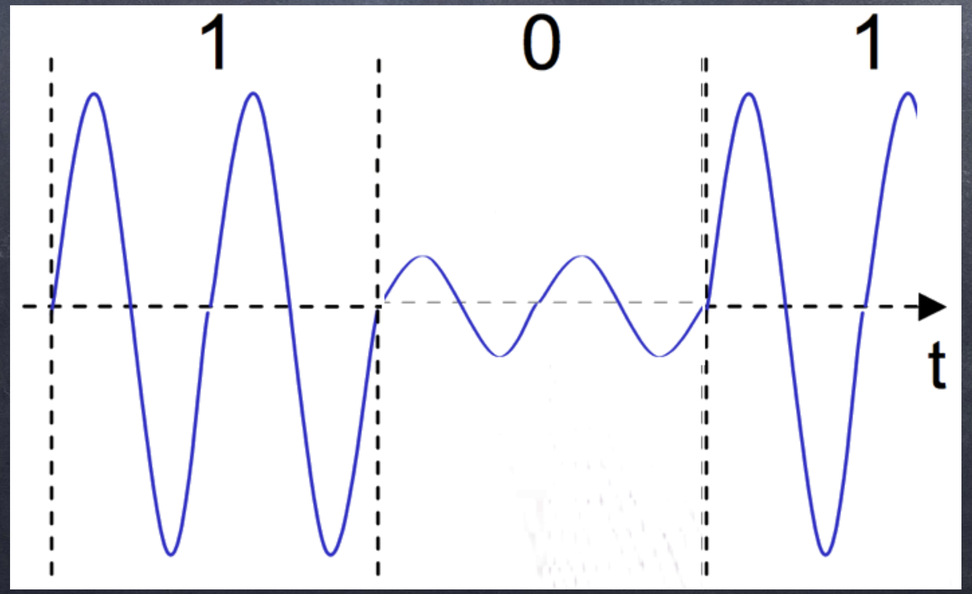
- Amplitude Shift Keying (ASK)
- Frequency Shift Keying (FSK)

Amplitude Shift Keying (ASK)

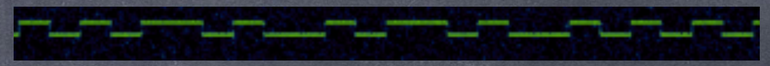
- The Modulating signal changes the Amplitude (signal strength) of the Carrier signal. The resultant Modulated Signal displays the following characteristics:
  - Only One frequency is used,
  - The waterfall or visualised signal will look like morse code

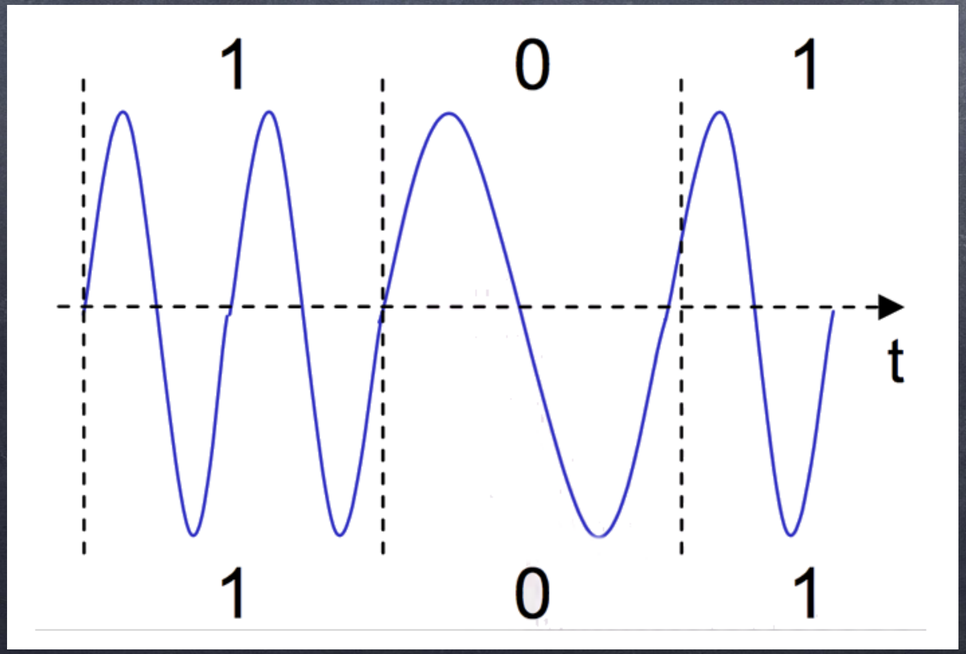


- Example: Many legacy wireless systems, e.g. Restaurant Pager, Garage Door remotes, Doorbells, simple inexpensive security systems, etc



Frequency Shift Keying (FSK):

- The Modulating signal changes the Frequency of the Carrier signal. The resultant Modulated Signal displays the following characteristics:
  - Two (2FSK) or more (4 if 4FSK) frequency's are used to represent the data transmission,
  - A signal analyser will show multiple peaks of the transmission representing the frequency changes as data is transmitted
  - The waterfall or visualised signal will look like an old school Nokia snake 
- Popular in modern systems e.g. used in a lot of vehicle remote keyless entry systems, broadcast Pager networks.

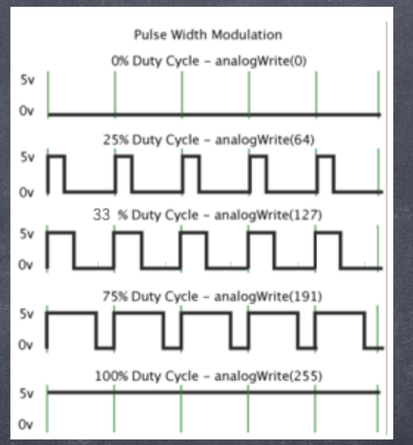


Encoding, and why it is done...

- The transmission (TX) of an RF signal, consumes electric power...obviously!
- Power efficiency is important;
  - is there a way to reduce the number of TX's?
- Yes! - Encoding can be used for power efficiency rather than just obfuscation...

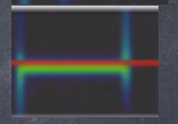
Pulse Width Modulation (PWM)

- PWM is used in electric circuits to reduce power draw (and simulate an analogue system); it can also be used within an RF TX
- Popular RF based PWM modes:
  - 33% - 66/33 duty cycle version
  - 25% - 75/25 duty cycle version



0

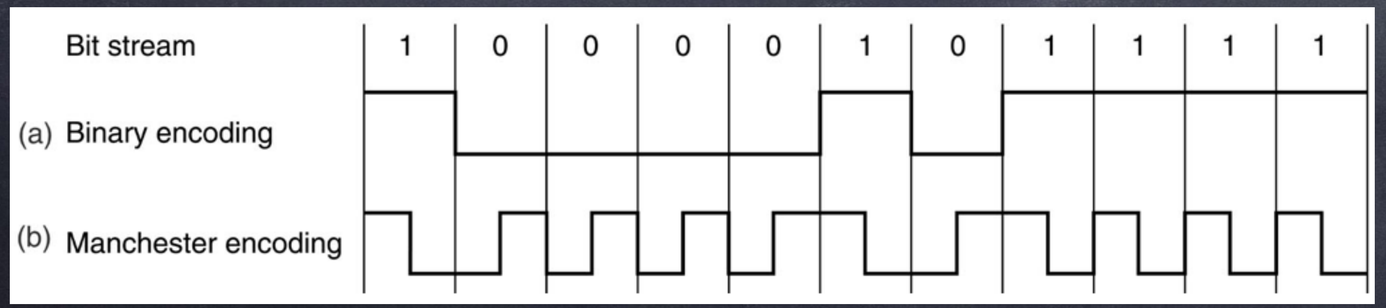
1

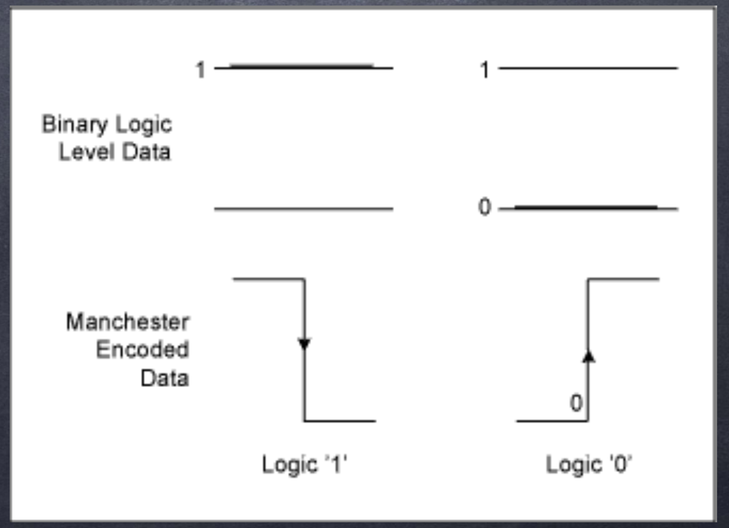


- Think of it as a type of ASK, but with 0's deliberately transmitted instead of an absence of a signal counting as a zero - means that it easier to know when the transmission is finished

Manchester Encoding

- Binary states of "1" and "0" are transitions rather than static values.
- There are two possible interpretations of the transition of rising and falling edges.
- Hint: You will see no more than two consecutive 1's or 0's





Manual Signals Analysis

- Find Frequency
- Find Modulation / Keying
- Find Pulsewidth / pauses between tx, repeats
- Extract the original data.....
- Analyse the differences between transmissions: just like Web App Pentesting
- Recreate a data signal with the information/command you wish the receiver to act upon!!!!!

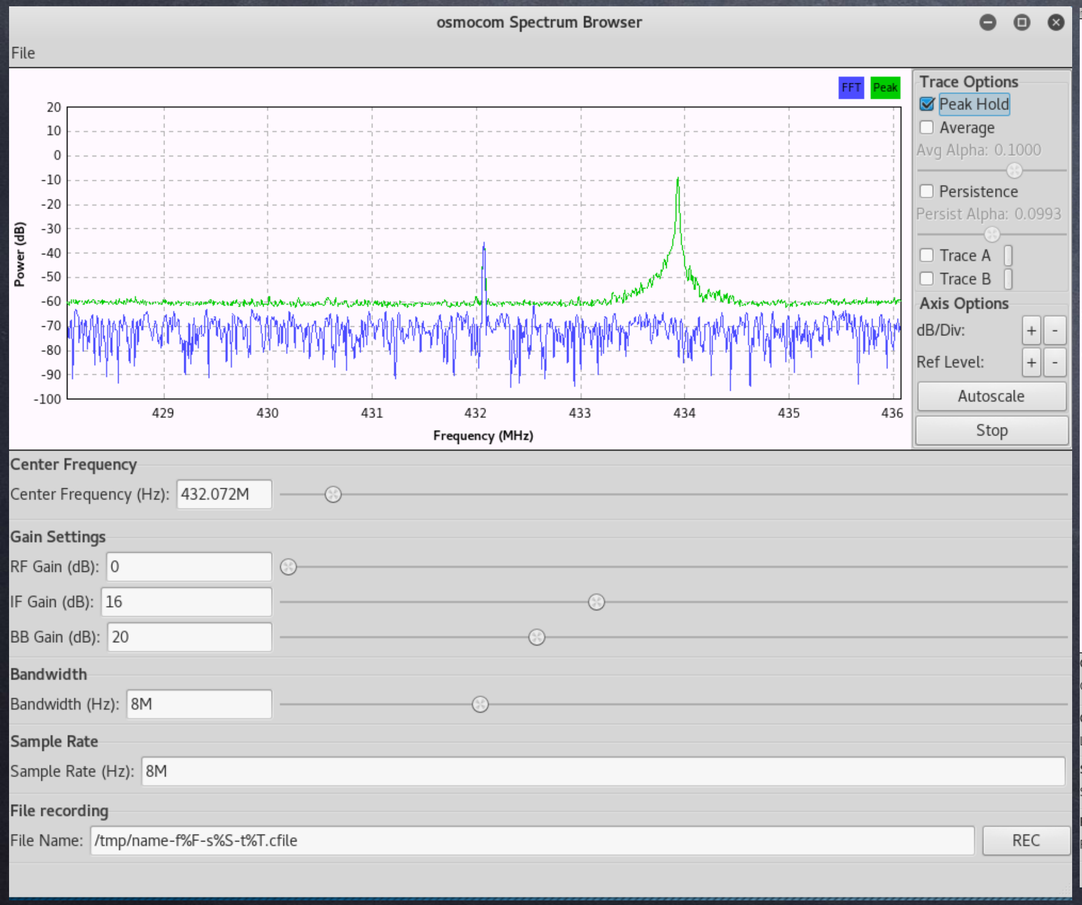
Signal Analysis

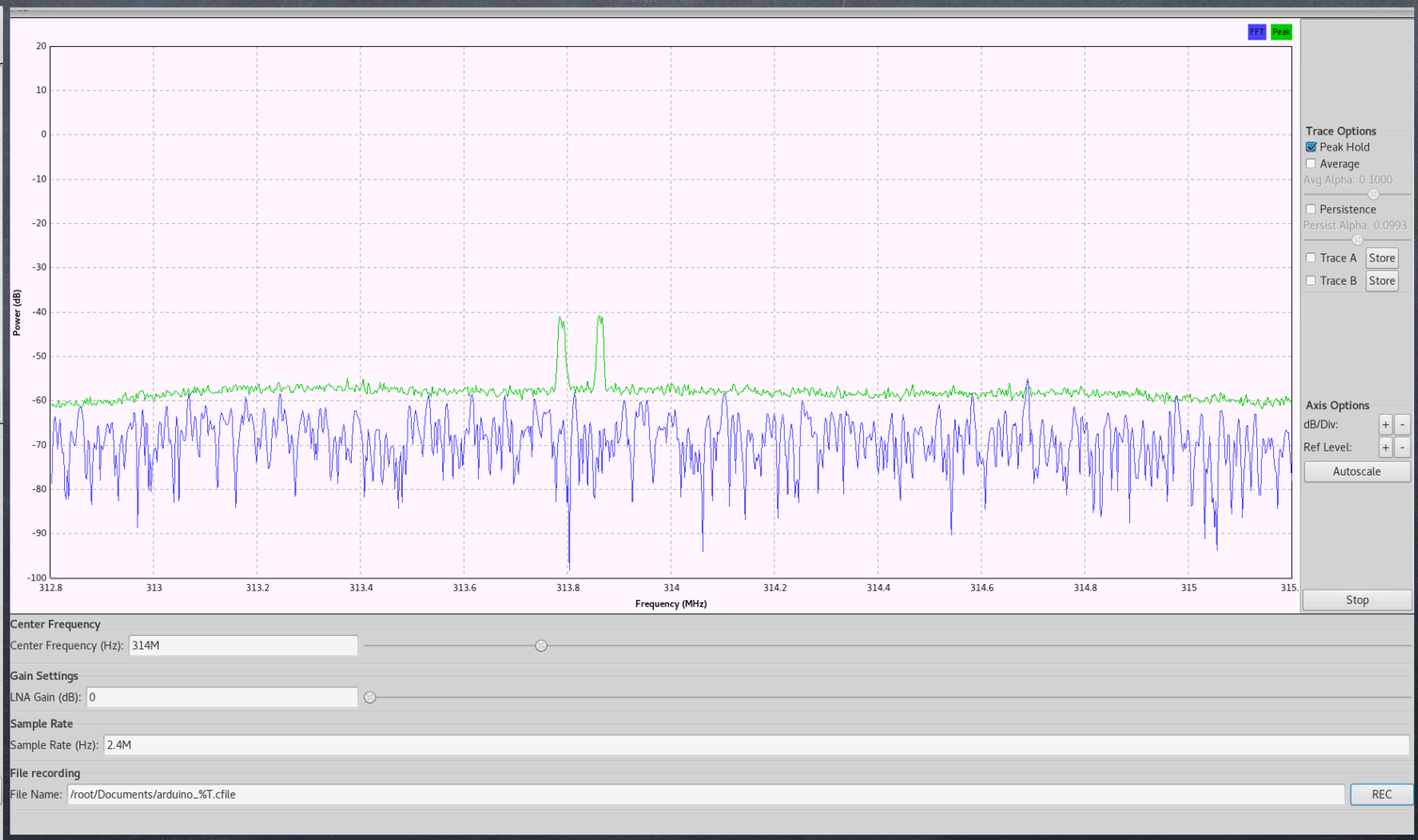
- Determine the Frequency
  - Product info
  - Chip set info
  - Open/Closed Source info
- Determine the Modulation/Keying
  - Are changes occurring in Amplitude, Frequency or Phase
  - Pulse width etc

Frequency and Modulation - osmocom_fft

AM - ASK

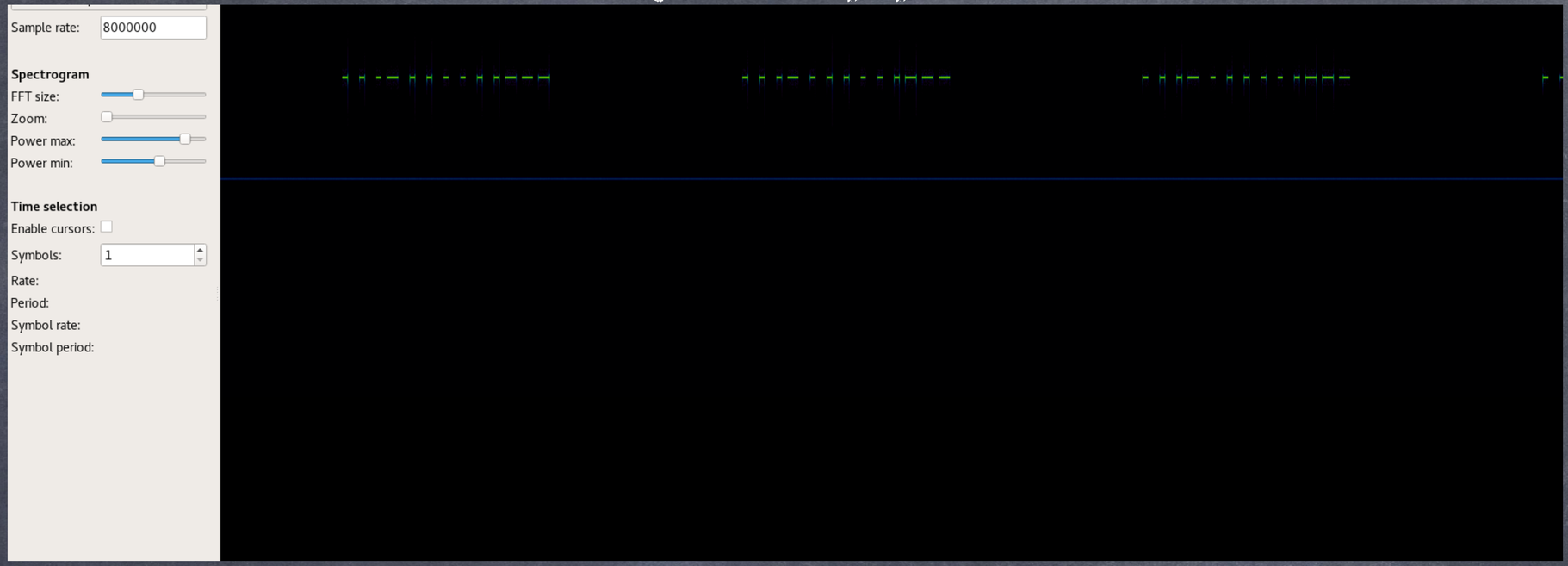
FM - FSK



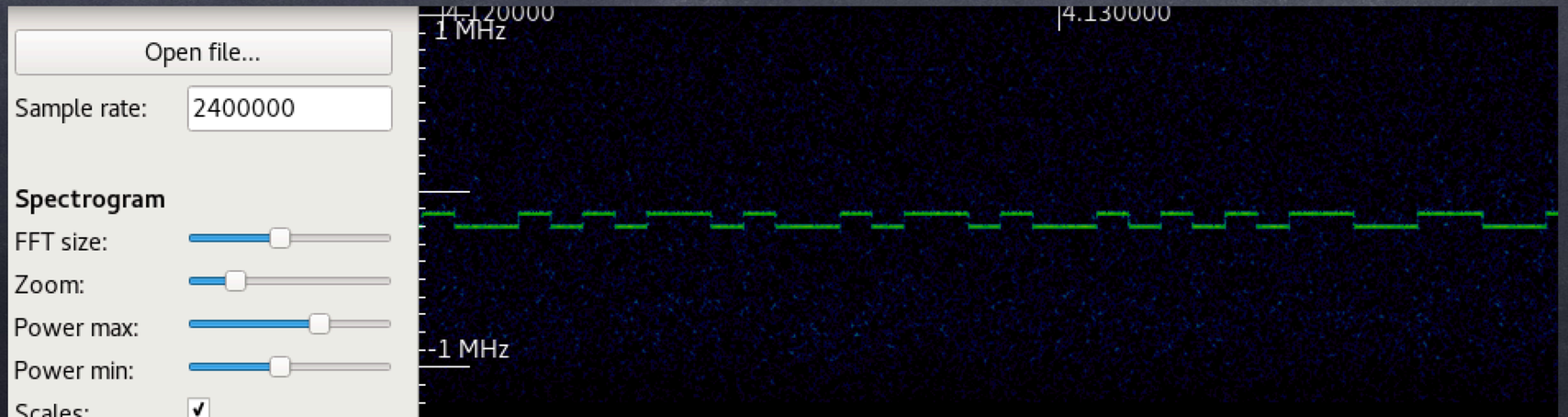


Modulation - Inspectrum

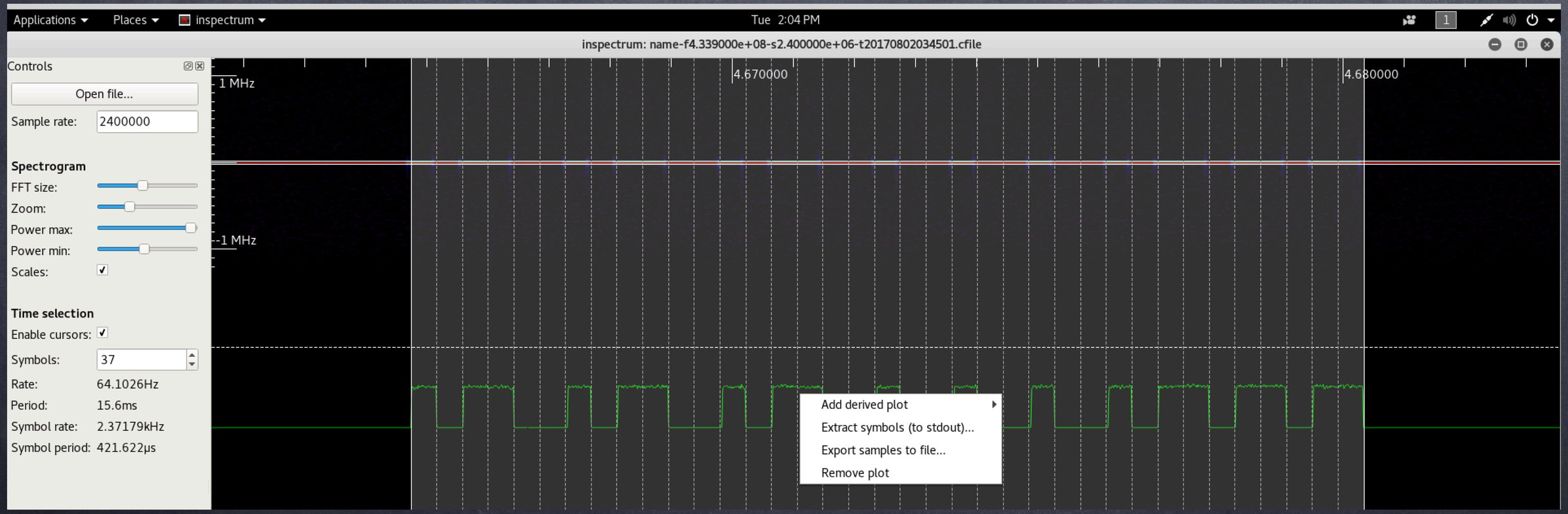
ASK - OOK



2-FSK



Extracting Symbols/Bits - Pulse width & Rate



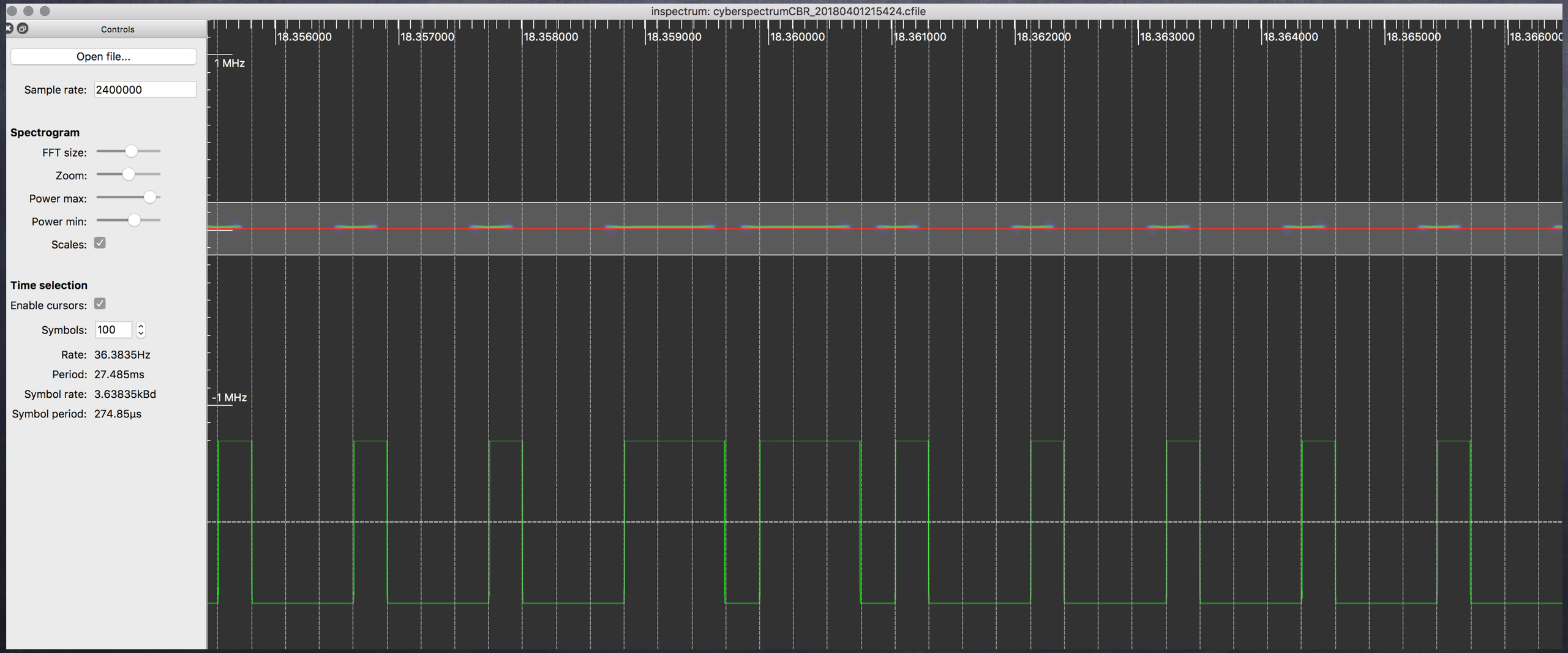
</Theory>

Lets hack our Pager system

- Demo - normal functions
- Demo - View the transmission in Osmocom-fft and GQRX

- Find Frequency
- Find Modulation / Keying
- Find Pulsewidth / pauses between tx, repeats
- Extract the original data.....
- Remember the beer?

Inspectrum is your Friend



DspectrumGUI - demodulation buddy - thanks Tres (nullWolf)

/dspectrum/
by nullwolf

Unit: Tables

This unit is a BSides Pager

Name	Tables
Device ID	1
Device Name	BSides Pager
Notes	

Actions
Add New Capture
Edit Unit
View Device

Captures

ID	Name	Raw Binary	Actions
2	15	1000111010001110100011101110111010001000100010001110111011101110111010001000100010001000100010001000	Destroy
4	001	1000111010001110100011101110111010001000100010001110111010001000100010001000100010001000100010001000	Destroy

Automated Demodulation Attempts

Raw (No special encoding)

ID	Name	Raw Binary To Hex	Raw Binary To Ascii	Actions
2	15	\x8e\x8e\x8e\xee\x88\x88\xee\xee\xe8\x88\x88\x88\x8	????????????8	show | Destroy
4	001	\x8e\x8e\x8e\xee\x88\x88\xee\x88\x88\x88\x88\x88\x8	????????????8	show | Destroy

Manchester Encoding

Defaulting to Manchester format: "G. E. Thomas"

Switch to IEEE 802 Format

ID	Name	Valid?	Manchester Binary	Hex	Ascii	Actions
2	15	No	1111111111111111111111111	\x1f\xff\xff\xf	??f	show | Destroy
4	001	No	1111111111111111111111111	\x1f\xff\xff\xf	??f	show | Destroy

PWM Encoding

Attempts to decode as PWM 66/33 Format (i.e. a 1 is 110, and a 0 is 100)

Flip bits

ID	Name	Valid?	PWM Binary	Hex	Ascii	Actions
2	15	No	0101000	\x28	(	show | Destroy
4	001	No	0100000	\x20		show | Destroy

PWM Encoding

Attempts to decode as PWM 75/25 Format (i.e. a 1 is 1110, and a 0 is 1000)

Flip bits

ID	Name	Valid?	PWM Binary	Hex	Ascii	Actions
2	15	Yes	0101011100001111100000000	\xae\x1f\x00	?	show | Destroy
4	001	Yes	0101011100001100000000000	\xae\x18\x00	?	show | Destroy

PWM Bit Position Analysis Tool (75/25)

The longest binary string is used as the comparison baseline (B) below

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
15	0	1	0	1	0	1	1	1	0	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0
001	0	1	0	1	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0
B	0	1	0	1	0	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0

Raw Bit Position Analysis Tool

The longest binary string is used as the comparison baseline (B) below

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
15	1	0	0	0	1	1	1	0	1	0	0	0	1	1	1	0	1	0	0	0	1	1	1	0	1
001	1	0	0	0	1	1	1	0	1	0	0	0	1	1	1	0	1	0	0	0	1	1	1	0	1
B	1	0	0	0	1	1	1	0	1	0	0	0	1	1	1	0	1	0	0	0	1	1	1	0	1

	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
15	1	1	0	1	1	1	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1
001	1	1	0	1	1	1	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1
B	1	1	0	1	1	1	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1

	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74
15	1	0	1	1	1	0	1	1	1	0	1	1	1	0	1	1	1	0	1	0	0	0	1	0	0
001	1	0	1	1	1	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0
B	1	0	1	1	1	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0

	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99
15	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0
001	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0
B	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0

BSides 2017 Badge Hack

- Sure you can make a $400 SDR TX your data....OR
- You can use your badge from last years BSides and have huge amounts of fun with *your* garage door, doorbell, or pub!
- Fuzzing!

Organised Chaos

- We have programmed up 8 coasters
- We will tell you some of the numbers:
- #255, #113, #1, #729, #422, #123, #69, #?
- The first person to tell us the value of X gets a prize

For further reading:

Rapid Radio Reversing:
https://greatscottgadgets.com/tr/gsg-tr-2016-1.pdf

Mike Ossmans lectures

Inspectrum

RFSwitch

Balint Seeber founder Cyberspectrum Bay Area
Discovered SirenJack - https://www.sirenjack.com/