Dude, Where's My Car?

Tire Pressure Monitor *Monitoring*

ShareBrained Technology

Jared Boone

ToorCon 15, October 20, 2013

An Act

To amend title 49, United States Code, to require reports concerning defects in motor vehicles or tires or other motor vehicle equipment in foreign countries, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Transportation Recall Enhancement, Accountability, and Documentation (TREAD) Act".

SEC. 2. PRESERVATION OF SECTION 30118.

The amendments made to section 30118 of title 49, United States Code, by section 364 of the Department of Transportation and Related Agencies Appropriations Act, 2001 are repealed and such section shall be effective as if such amending section had not been enacted.

TREAD Act

Tire Pressure Monitoring System


DAIMLERCHRYSLER
56053030AC
MITSUBISHI MOTORS
4250A225
ID:C8E7C8CD
1
FCC ID: KR5S120123
IC: 267T-S120123
MODEL: 5WY7770
315MHz

The Target

ID? Serial Number?


315MHz
ID:C8E7C8CD
786A0/716004927
FCC ID: KR5S120123
IC: 267T-S120123
MODEL: 5WY7770
315MHz

Frequency...

FCC ID? Heh heh heh…

Search | RSS | Updates | E-Filing | Initiatives | Consumers | Find People

Office of Engineering and Technology

FCC > FCC E-filing > TCB > Search   FCC Site Map

3 results were found that match the search criteria:
Grantee Code: kr5 Product Code: s120123

Displaying records 1 through 3 of 3.

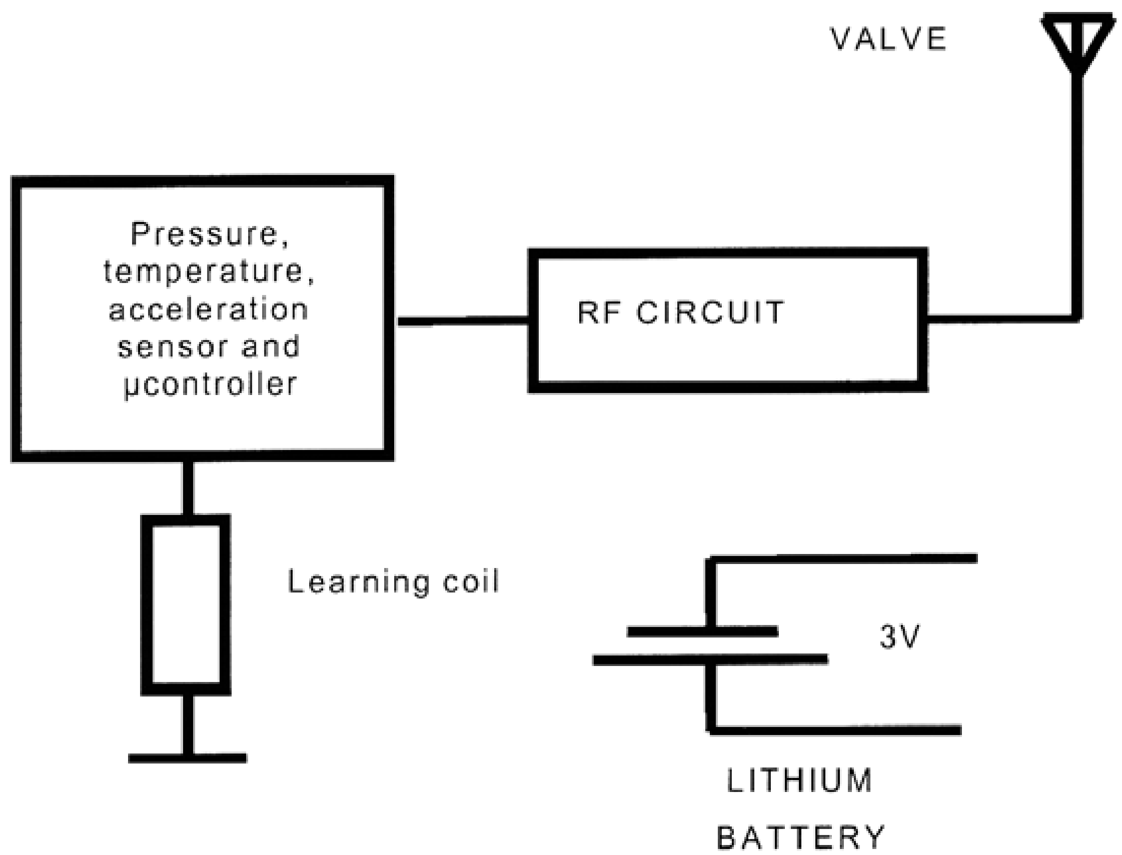
View Form	Display Exhibits	Display Grant	Display Correspondence	Applicant Name	Address	City	State	Country	Zip Code	FCC ID	Application Purpose	Final Action Date	Lower Frequency In MHz	Upper Frequency In MHz
	Detail Summary			Continental Automotive GmbH	Siemensstrasse 12 SV C TS RBG EMC-Laboratory	Regensburg	N/A	Germany	93055	KR5S120123009	Change in Identification	02/14/2008	315.0	315.0
	Detail Summary			Continental Automotive GmbH	Siemensstrasse 12 SV C TS RBG EMC-Laboratory	Regensburg	N/A	Germany	93055	KR5S120123	Original Equipment	07/30/2003	315.0	315.0
	Detail Summary			Continental Automotive GmbH	Siemensstrasse 12 SV C TS RBG EMC-Laboratory	Regensburg	N/A	Germany	93055	KR5S120123007	Original Equipment	10/07/2005	315.0	315.0

Perform Search Again

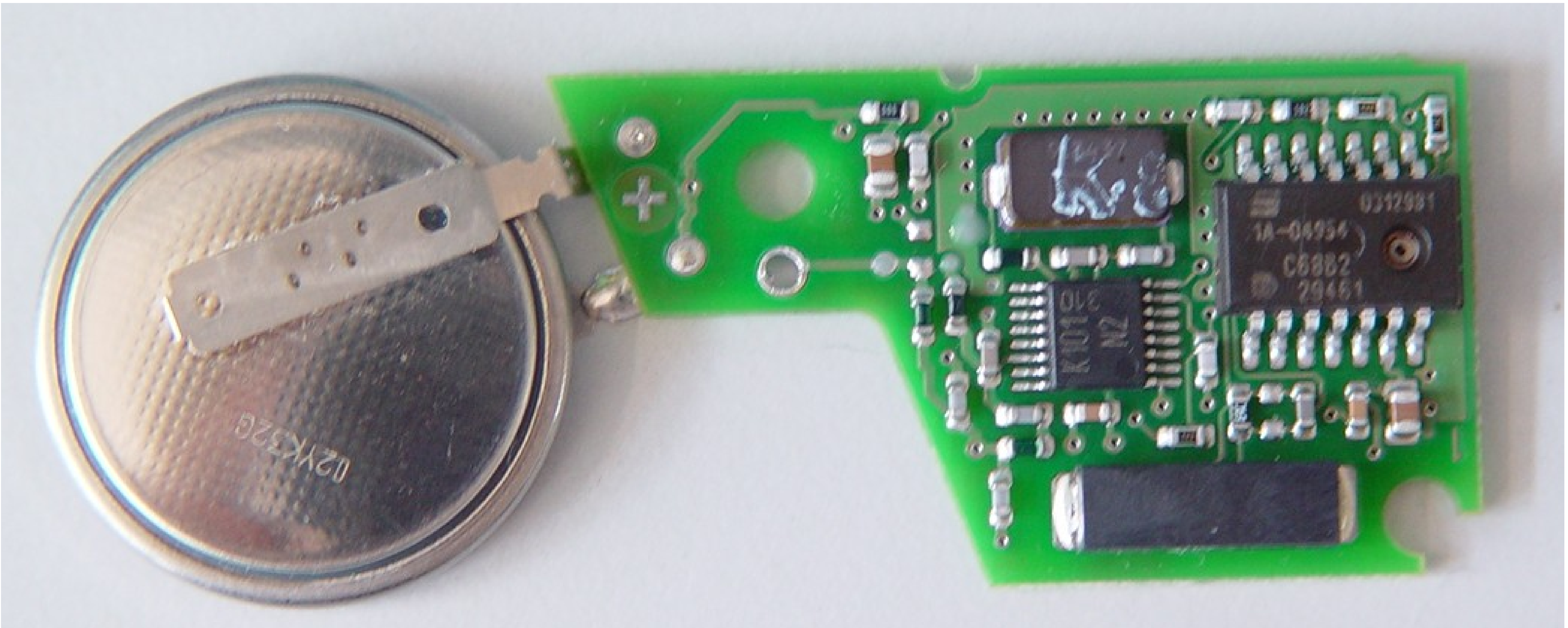
http://fcc.io/kr5/s120123

Block diagram

The block diagram below shows the main electronic units of the TireGuard transmitter:



No surprises here…



Internal Photo

- Tire guard transmitter type S120123 which includes an integrated pressure, temperature and acceleration sensor and a 315 MHz RF transmitter.
- RF receiver unit which includes a 315 MHz receiver (not described in this document)

The TireGuard system monitors a vehicle's tire pressure whilst driving or stationary. An electronic unit (wheel unit) inside each tire, mounted to the valve stem, periodically measures the actual tire pressure. By means of RF communication, this pressure information is transmitted to the RF receiver/decoder.

Operational Description

When the vehicle starts moving, the TireGuard transmitter enters the driving mode. It measures and transmits RF burst 4 times per minute up to 30 bursts. The telegram length is approximately 30ms. After this period the transmitter measures and transmits data every minute. The transmitter will remain in driving mode for a period of 10 minutes after the vehicle is stopped.

If, during any measurement period in driving mode, the pressure leakage is detected (difference compared to the last transmitted pressure value), a re-measure will occur after 5s taking in account the latest pressure value emitted as reference value. If the pressure continues changing, an additional transmission will be sent.

For normal transmission the wheel must be rotating and the device must be pressurized. For factory testing, installation testing, ect., the device has been designed to be activated also by a 125kHz signal. For homologation testing one sample was modified for CW emission, that last about 2 min. after activation with LF.

Operational Description

2.1 Equipment Under Test (EUT)

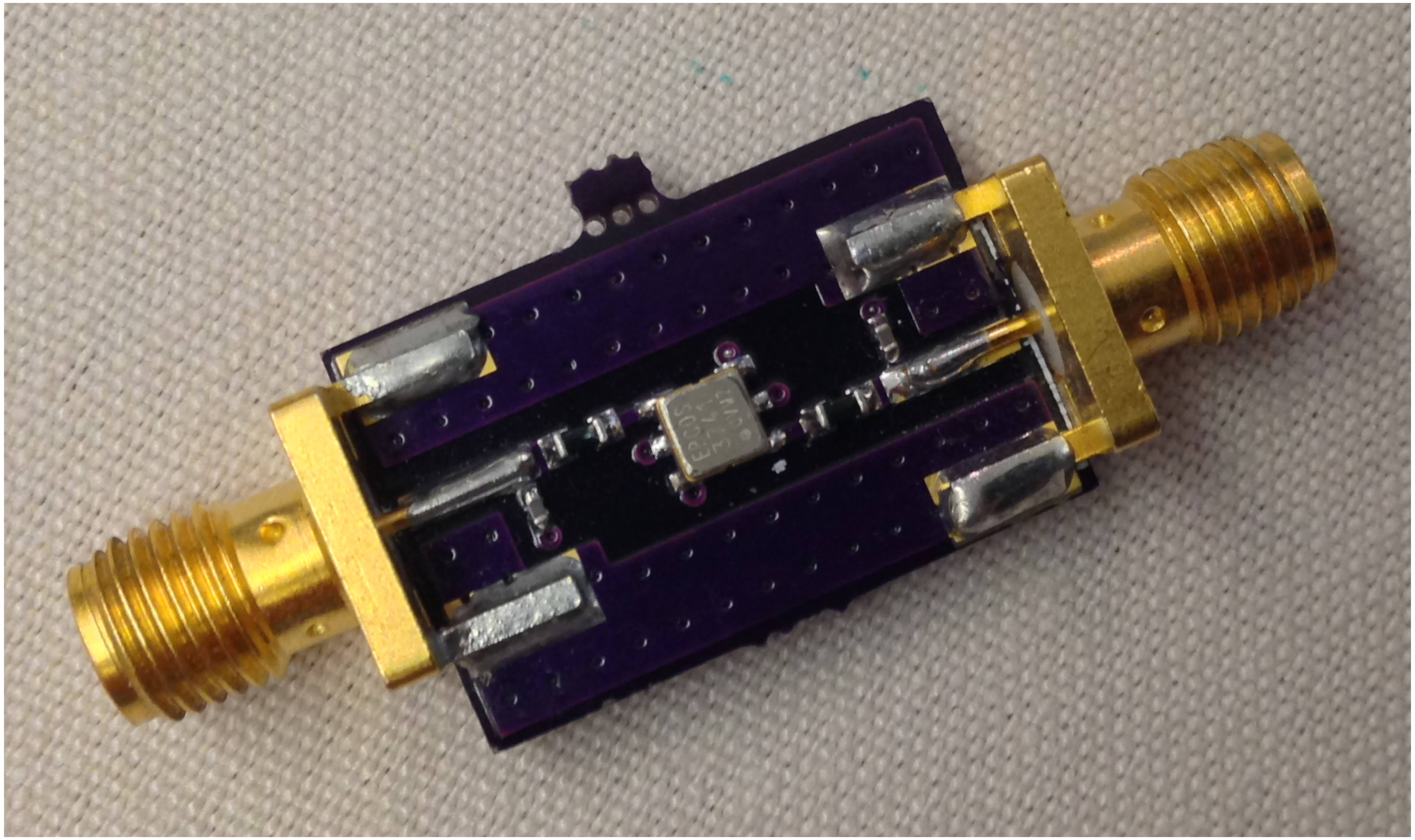
Device:	**Transmitter**
Trade Name:	**Siemens VDO**
Model:	**5WY7243 TireGuard Type S120 123**
Serial Number:	none (Prototype)
FCC ID:	**KR5S120123**
Power:	3V DC
Transmit Frequency:	315 MHz
Type of modulation:	FSK
Interface:	none
Variants:	
Highest frequency generated or used in the device:	Resonator 315MHz

Technical description

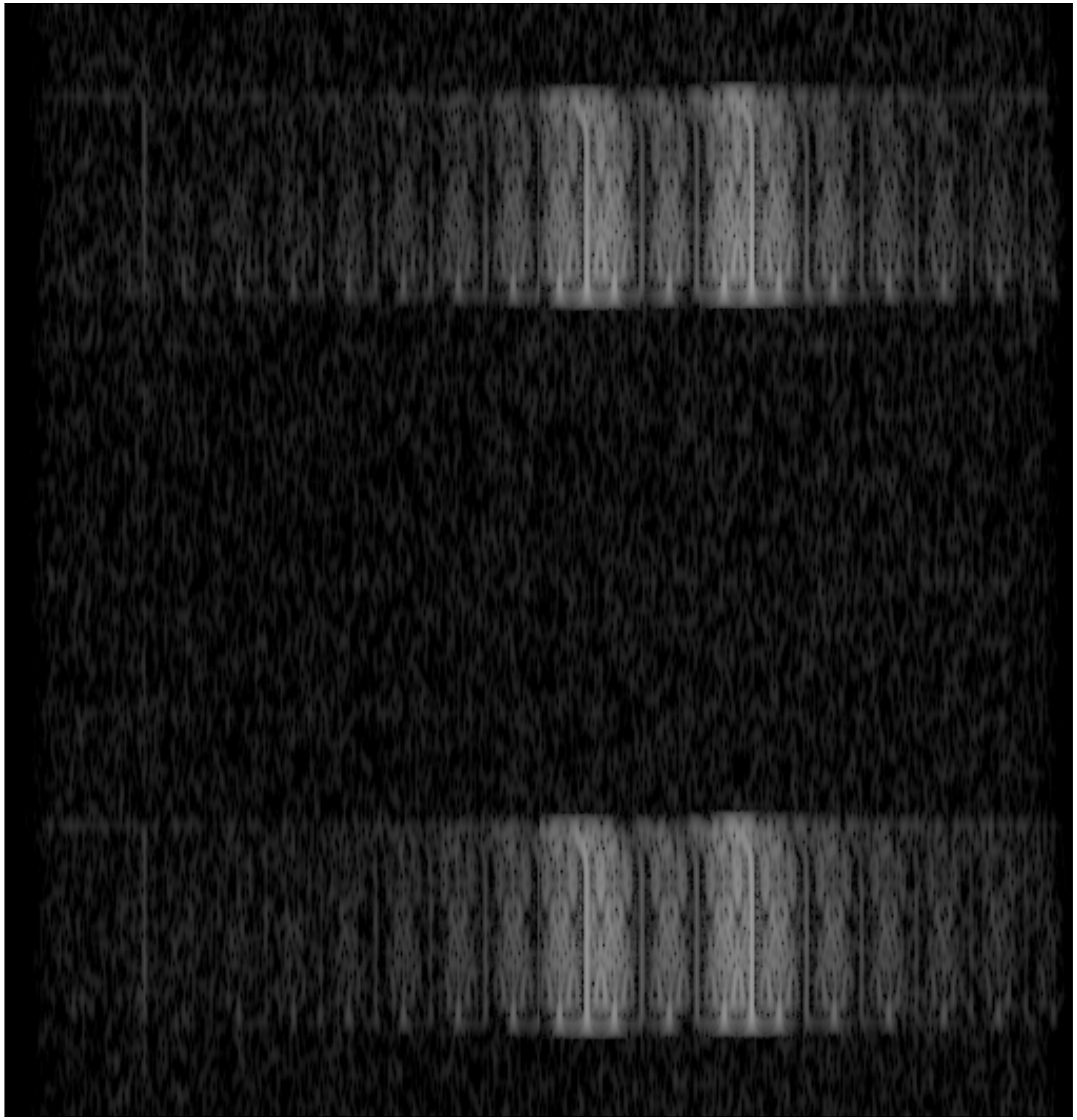
Carrier frequency:	315 MHz
Frequency shift:	± 45 kHz
Number of channels:	1
Duty cycle:	< 0.1%
Type of modulation:	Frequency Shift Keying (FSK)
Rated Output Power:	< 10 mW
Antenna:	integral
Voltage supply:	1 Lithium battery 3V (CR2450)
Voltage supply range :	2.1 up to 3.2V

RTL-SDR

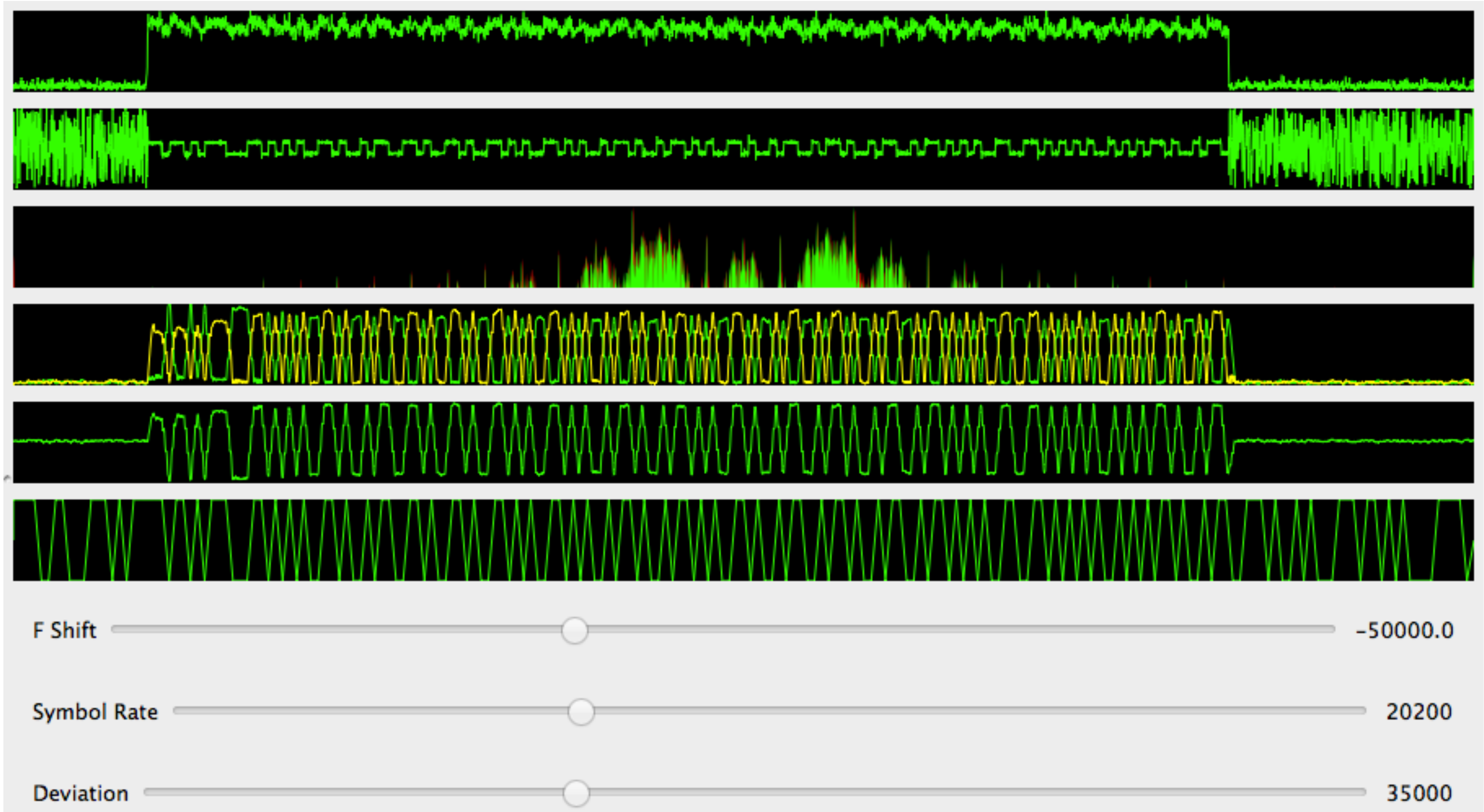
Antenna



SAW Filter



RF Capture



Inspect

Observations

- Modulation: FSK
- Deviation: +/- 33 kHz
- Symbol rate: 20.15 kHz
- Carrier: 53 kHz + 314.95 MHz = 315.03 MHz

```
2013-10-13T17:24:20.814400+00:00 1101101011100 0110101010011010010101011010100101010110100110101001011010010110101001101001011001011010010110010110101010011001101001101 0
2013-10-13T17:24:20.941120+00:00 1101101011100 01101010100110100101010110101001010101101001101010010110100101101010011010010110010110100101100101101010100110011010011010
2013-10-13T17:24:32.100800+00:00 1101101011100 01101010100110011010100110101001010101100101101010010110000101101010100101011001010110011001011001101010100110001101001101
2013-10-13T17:24:32.128960+00:00 1101101011100 01101010100110011010100110101001010101100101101010010110100101101010100101011001010110011001011001101010100110011010011010
2013-10-13T17:24:32.226880+00:00 1101101011100 01101010100110011010100110101001010101100101101010010110100101101010100101011001010110011001011001101010100110011010011010
2013-10-13T17:24:32.441280+00:00 1101101011100 01101010100110011010100110101001010101100111111111001011010010110101010010101100101011001100101100110101010011001101001101
2013-10-13T17:24:45.310400+00:00 1101101011100 01101010100110011010100101101001010101011001101010010110100101101010100101011001010110100101010101011010100110011010101010
2013-10-13T17:19:01.871680+00:00 1101101011100 01101010100110100101100101101001010110010101101010010110100101101010100101011001010110100101010101011010100110011010011010
2013-10-13T17:24:45.396160+00:00 1101101011100 01101010100110011010100101101001010101011001101010010110100101101010100101011001010110100101010101011010100110011010101010
2013-10-13T17:24:45.524160+00:00 1101101011100 01101010100110011010100101101001010101011001101010010110100101101010100101011001010110100101010101011010100110011010101010
2013-10-13T17:25:22.324160+00:00 1101101011100 01101010100110100101011010101001010101011001101010010100001011010101001010110010101100110100101011001100101100110100110100
2013-10-13T17:25:22.351680+00:00 1101101011100 01101010100110100101011010101001010101011001101010010110100101101010100101011001010110011010010101001100101100110100110100
2013-10-13T17:25:22.436800+00:00 1101101011100 01101010100110100101011010101001010101011001101010010110100101101010100101011001010110011010010101100110010110011010011010
2013-10-13T17:25:22.563520+00:00 1101101011100 01101010100110100101011010101001010101011001101010010110100101101010100101011001010110011010010101100110010110011010011010
2013-10-13T17:25:24.758080+00:00 1101101011100 01101010100110100101010110101001010101100101101010010110100101101010011010010110010110100101100101101010100110011010011010
2013-10-13T17:25:24.885440+00:00 1101101011100 01101010100110100101010110101001010101100101101010010110100101101010011010010110010110100101100101101010100110011010011010
2013-10-13T17:19:01.899840+00:00 1101101011100 01101010100110100101100101101001010110010101101010010110100101101010100101011001010110100101010101011010100110011010011010
2013-10-13T17:25:24.982720+00:00 1101101011100 01101010100110100101010110101001010101100101101010010110100101101010011010010110010110100101100101101010100110011010011010
2013-10-13T17:25:31.320000+00:00 1101101011100 01101010100110011010100101101001010101010110101100101101001011010101001010110010101100110010110011010101001100110100110 1
2013-10-13T17:25:31.348160+00:00 1101101011100 01101010100110011010100101101001010101010110101001011010010110101010010101100101011001100101100110101010011001101001101 0
2013-10-13T17:25:31.434560+00:00 1101101011100 01101010100110011010100101101001010101010111101101111101001011010101001010110010101100110010110011010101001100110100110 1
2013-10-13T17:25:31.562560+00:00 1101101011100 01101010100110011010100101101001010101010110101001011010010110101010010101100101011001100101100110101010011001101001101 0
2013-10-13T17:25:31.660480+00:00 1101101011100 01101010100110011010100101101001010101010110101001011010010110101010010101100101011001100101100110101010011001101001101 0
2013-10-13T17:25:56.134720+00:00 1101101011100 01101010100110011010011010100110101010100110101001011010010110101010010101100101011010010101010101101010011001101001101 0
2013-10-13T17:25:56.232640+00:00 1101101011100 01101010100110011010011010100110101010100110101001011010010110101010010101100101011010010101010101101010011001101001101 0
2013-10-13T17:25:56.260800+00:00 1101101011100 01101010100110011010011010100110101010100110101001011010010110101010010101100101011010010101010101101010011001101001101 0
2013-10-13T17:19:01.985600+00:00 1101101011100 01101010100110100101100101101001010110010101101010010110100101101010100101011001010111110111111010101101010011001101001101
2013-10-13T17:25:56.474560+00:00 1101101011100 01101010100110011010011010100110101010100110101001011010010110101010010101100101011010010101010101101010011001101001101 0
2013-10-13T17:26:32.366400+00:00 1101101011100 01101010100110100101010101101001010101010110101001011010010110101010010101100101011001101001010110011001011001101001101 0
2013-10-13T17:26:32.393920+00:00 1101101011100 01101010100110100101010101101001010101010110101001011010010110101010010101100101011001101001010110011001011001101001101 0
2013-10-13T17:26:32.490560+00:00 1101101011100 01101010100110100101010101101001010101010110101001011010010110101010010101100101011001101001010110011001011001101001101 0
2013-10-13T17:26:32.576320+00:00 1101101011100 01101010100110100101010101101001010101010110101001011010010110101010010101100101011001101001010110011001011001101001101 0
2013-10-13T17:26:32.702400+00:00 1101101011100 01101010100110100101010101101001010101010110101001011010010110101010010101100101011001101001010110011001011001101001101 0
2013-10-13T17:26:36.211520+00:00 1101101011100 01101010100110011010101001101001010101011001101010010110100101101010011010010110010110100101100101101010100110011010011010
2013-10-13T17:26:36.308800+00:00 1101101011100 01101010100110011010101001101001010101011001101010010110100101101010011010010110010110100101100101101010100110011010011010
2013-10-13T17:26:36.395200+00:00 1101101011100 01101010100110011010101001101001010101011001101010010110100101101010011010010110010110100101100101101010100110011010011010
2013-10-13T17:19:02.113600+00:00 1101101011100 01101010100110100101100101101001010110010101101010010110100101101010100101011001010110100101010101011010100110011010011010
2013-10-13T17:26:41.808320+00:00 1101101011100 01101010100110011010010110100110101010100101101010010110100101101010100101011001010110011001011001101010100110011010011010
2013-10-13T17:26:41.936320+00:00 1101101011100 01101010100110011010010110100110101010100101101010010110100101101010100101011001010110011001011001101010100110011010011010
2013-10-13T17:27:06.949440+00:00 1101101011100 01101010100110011010010101100110101010011001101010010110100101101010100101011001010110100101010101011010100110011010011010
2013-10-13T17:27:07.035840+00:00 1101101011100 01101010100110011010010101100110101010011001101010010110100101101010100101011001010110100101010101011010100110011010011010
2013-10-13T17:27:07.064000+00:00 1101101011100 01101010100110011010010101100110101010011001101010010110100101101010100101011001010110100101010101011010100110011010011010
2013-10-13T17:27:07.161280+00:00 1101101011100 01101010100110011010010101100110101010011001101010010110100101101010100101011001010110100101010101011010100110011010011010
2013-10-13T17:27:07.289280+00:00 1101101011100 01101010100110011010010101100110101010011001101010010110100101101010100101011001010110100101010101011010100110011010011010
2013-10-13T17:19:02.211520+00:00 1101101011100 01101010100110100101100101101001010110010101101010010110100101101010100101011001010110100101010101011010100110011010011010
2013-10-13T17:27:31.291840+00:00 1101101011100 01101010100110011010101010100110101010101001101010010110100101101010100100010010101100110100101011001100101100110100110101
2013-10-13T17:27:31.319360+00:00 1101101011100 01101010100110011010101010100110101010101001101010010110100101101010000000110010101100110100101011001100101100110100110101
```

Demodulate

```
01101010100110100101010101101001010101010101101010010110100101101010100101011001010110011010010
01101010100110100101010101101001010101010101101010010110100101101010100101011001010110011010010
01101010100110100101010101101001010101010101101010010110100101101010100101011001010110011010010
01101010100110100101010101101001010101010101101010010110100101101010100101011001010110011010010
01101010100110100101010101101001010101010101101010010110100101101010100101011001010110011010010
01101010100110011010101001101001010101011001101010010110100101101010011010010110010110100101100
01101010100110011010101001101001010101011001101010010110100101101010011010010110010110100101100
01101010100110011010101001101001010101011001101010010110100101101010011010010110010110100101100
01101010100110100101100101101001010110010101101010010110100101101010100101011001010110100101010
01101010100110011010010110100110101010100101101010010110100101101010100101011001010110011001011
01101010100110011010010110100110101010100101101010010110100101101010100101011001010110011001011
01101010100110011010010101100110101010011001101010010110100101101010100101011001010110100101010
01101010100110011010010101100110101010011001101010010110100101101010100101011001010110100101010
01101010100110011010010101100110101010011001101010010110100101101010100101011001010110100101010
01101010100110011010010101100110101010011001101010010110100101101010100101011001010110100101010
01101010100110011010010101100110101010011001101010010110100101101010100101011001010110100101010
01101010100110100101100101101001010110010101101010010110100101101010100101011001010110100101010
01101010100110011010101010100110101010101001101010010110100101101010100100010010101100110100101
01101010100110011010101010100110101010101001101010010110100101101010000000110010101100110100101
01101010100110011010101000000101010101010011010100101101001011010101001010110010101100110100101
01101010100110011010100101100110101010101001101010010110100101101010011010010110010110100101100
01101010100110011010100101100110101010101001101010010110100101101010011010010110010110100101100
01101010100110011010100101100110101010101001101010010110100101101010011010010110010110100101100
01101010100110011010100101100111110001101101100010010110100101101010011010010110010110100101100
01101010100110011001101010100110101010011001101010010110100101101010100101011001010110011001011
01101010100110011001101010100110101010011001101010010110100101101010100101011001010110011001011
01101010100110011001101010100110101010011001101010010110100101101010100101011001010110011001011
```

Symbols to Bits

```
$ cat demodulated.txt | packet_stats.py --encoding man --lengthstats
Length statistics:
    1: 1
    2: 1
    3: 1
    4: 2
    6: 2
    8: 1
...snip...
    67: 2
    68: 2
    69: 2
    70: 250
    71: 118
    72: 61
    73: 34
    74: 13
    75: 5
    76: 3
    77: 2
    79: 1
```

Length Stats

```
$ cat demodulated.txt | packet_stats.py --encoding man --length 70 --bitstats
Bit value statistics:
...snip...
     55:  130/   1  131  99.2% ********************
     56:    1/ 130  131   0.8%
     57:    0/ 131  131   0.0%
     58:  111/  20  131  84.7% *****************
     59:    0/ 131  131   0.0%
     60:    0/ 131  131   0.0%
     61:   69/  62  131  52.7% ***********
     62:   65/  66  131  49.6% **********
     63:   58/  73  131  44.3% *********
     64:   60/  71  131  45.8% *********
     65:   66/  65  131  50.4% **********
     66:   62/  69  131  47.3% *********
     67:   70/  61  131  53.4% ***********
     68:   75/  56  131  57.3% ***********
     69:    0/ 131  131   0.0%
```

Bit Stats

```
$ cat demodulated.txt | packet_stats.py --encoding man --length 70 --rangestats
0,32
Range 0:32
 84c9dc66   2227821670 10000100110010011101110001100110: 1
 84ca3c66   2227846246 10000100110010100011110001100110: 1
 84d1dc66   2228345958 10000100110100011101110001100110: 3
 84d24466   2228372582 10000100110100100100010001100110: 2
 84d24c66   2228374630 10000100110100100100110001100110: 3
 84d25c66   2228378726 10000100110100100101110001100110: 1
 84d9dc66   2228870246 10000100110110011101110001100110: 1
 84d9e466   2228872294 10000100110110011110010001100110: 1
 84da4466   2228896870 10000100110110100100010001100110: 1
 84da4c66   2228898918 10000100110110100100110001100110: 2
 84da5466   2228900966 10000100110110100101010001100110: 2
 84e1dc66   2229394534 10000100111000011101110001100110: 1
 84e1ec66   2229398630 10000100111000011110110001100110: 1
 84e1f466   2229400678 10000100111000011111010001100110: 1
 84e25466   2229425254 10000100111000100101010001100110: 4
 84e25c66   2229427302 10000100111000100101110001100110: 3
 84e26466   2229429350 10000100111000100110010001100110: 2
 84e9cc66   2229914726 10000100111010011100110001100110: 1
 84e9dc66   2229918822 10000100111010011101110001100110: 1
...snip...
```

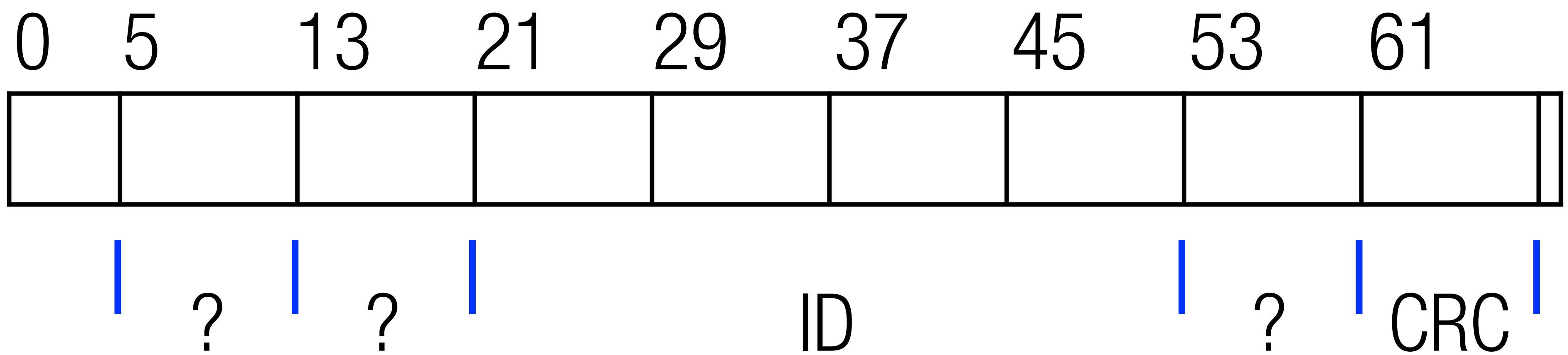
Bit Range Stats

```
$ cat demodulated.txt | packet_stats.py --encoding man --length 70 --rangestats
1,33
Range 1:33
  993b8cc    160676044 00001001100100111011100011001100: 1
  99478cc    160725196 00001001100101000111100011001100: 1
  9a3b8cc    161724620 00001001101000111011100011001100: 3
  9a488cc    161777868 00001001101001001000100011001100: 2
  9a498cc    161781964 00001001101001001001100011001100: 3
  9a4b8cc    161790156 00001001101001001011100011001100: 1
  9b3b8cc    162773196 00001001101100111011100011001100: 1
  9b3c8cc    162777292 00001001101100111100100011001100: 1
  9b488cc    162826444 00001001101101001000100011001100: 1
  9b498cc    162830540 00001001101101001001100011001100: 2
  9b4a8cc    162834636 00001001101101001010100011001100: 2
  9c3b8cc    163821772 00001001110000111011100011001100: 1
  9c3d8cc    163829964 00001001110000111101100011001100: 1
  9c3e8cc    163834060 00001001110000111110100011001100: 1
  9c4a8cc    163883212 00001001110001001010100011001100: 4
  9c4b8cc    163887308 00001001110001001011100011001100: 3
  9c4c8cc    163891404 00001001110001001100100011001100: 2
  9d398cc    164862156 00001001110100111001100011001100: 1
  9d3b8cc    164870348 00001001110100111011100011001100: 1
...snip...
```

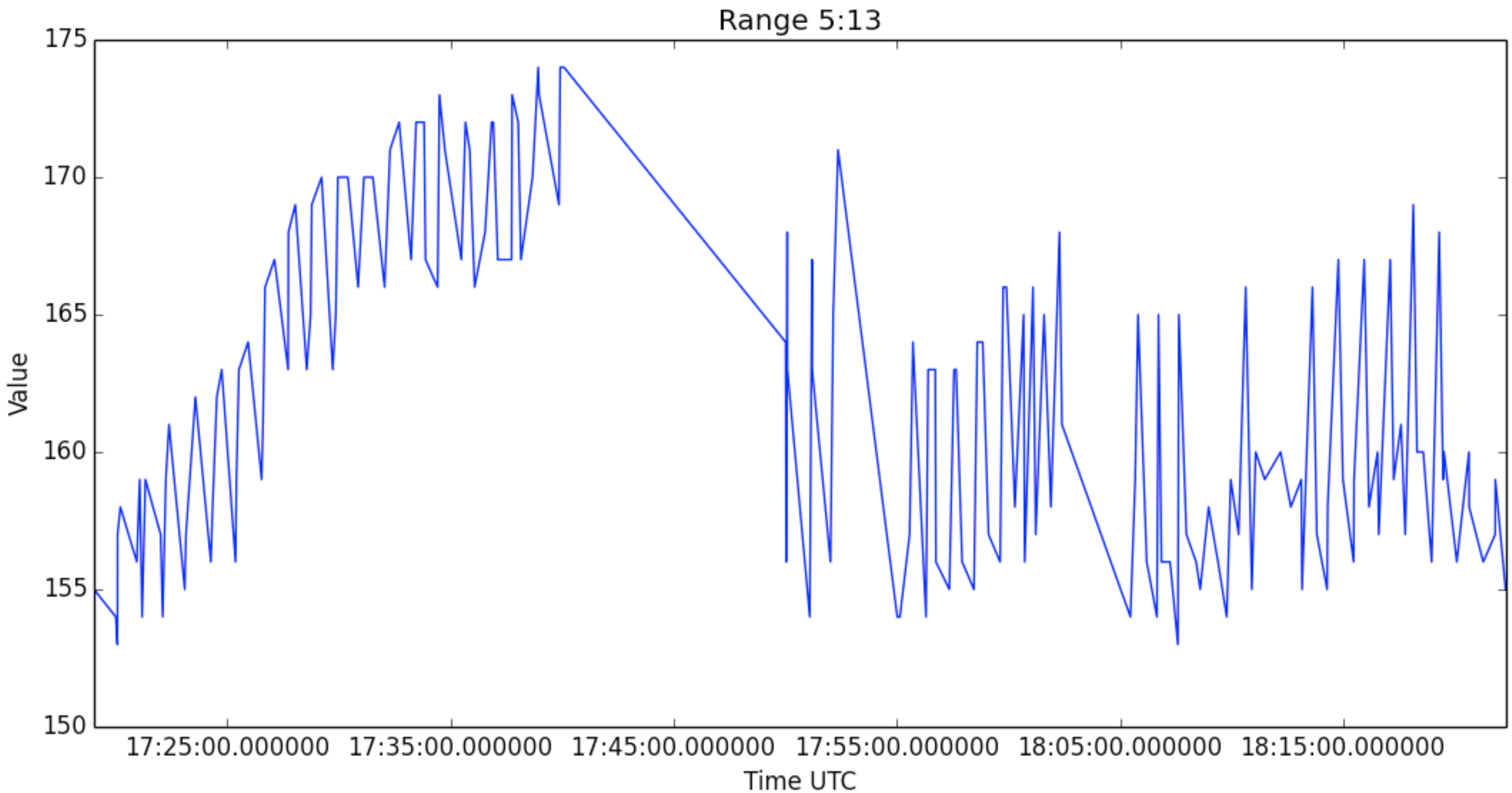
Bit Range Stats

```
$ cat demodulated.txt | packet_stats.py --encoding man --length 70 --rangestats
21,53
Range 21:53
 8cc3b9f8   2361637368 10001100110000111011100111111000: 35
 8cc3ba75   2361637493 10001100110000111011101001110101: 20
 8cc3bad0   2361637584 10001100110000111011101011010000: 38
 8cc4d9b0   2361711024 10001100110001001101100110110000: 38
```

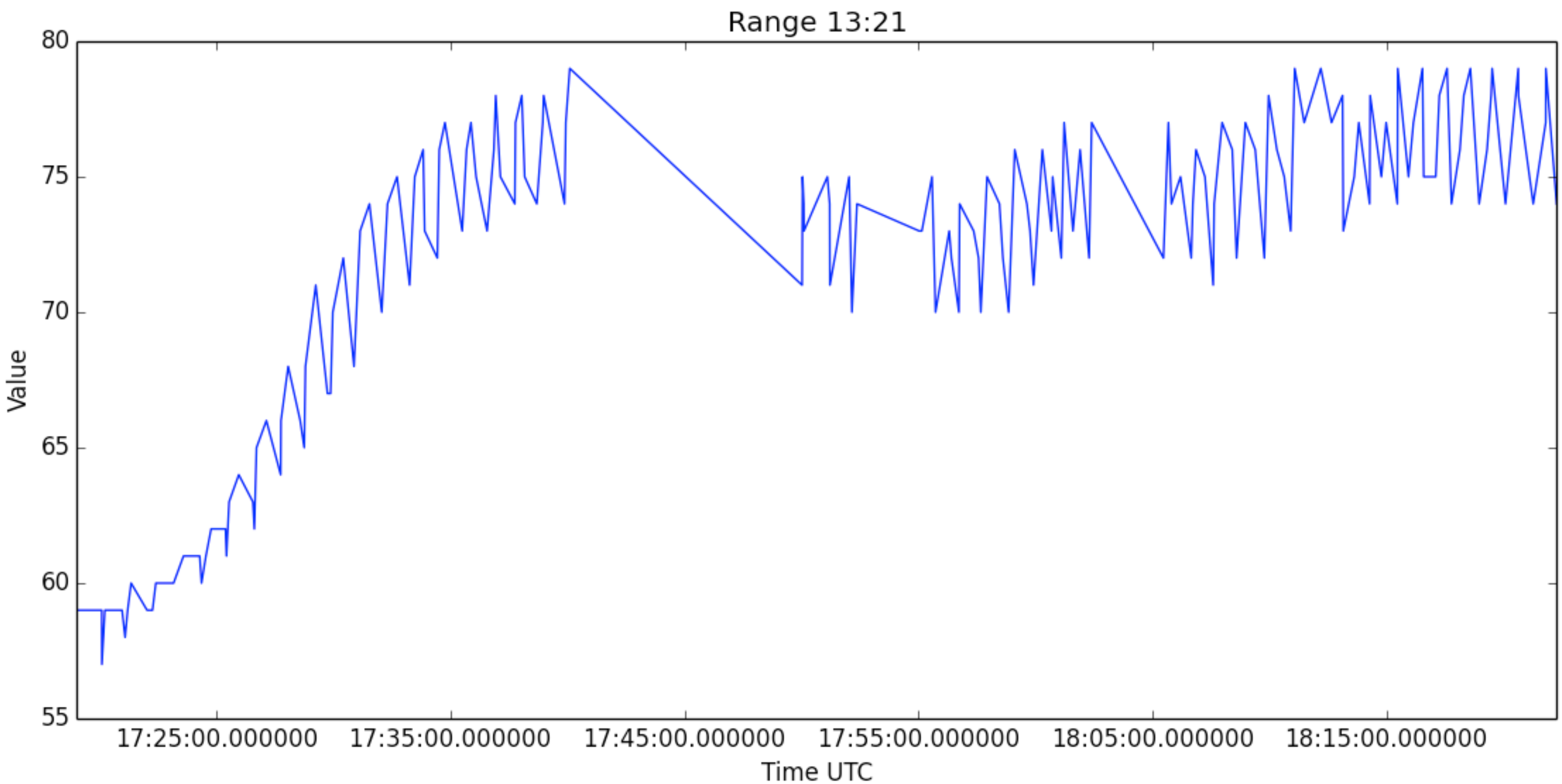
Bit Range Stats



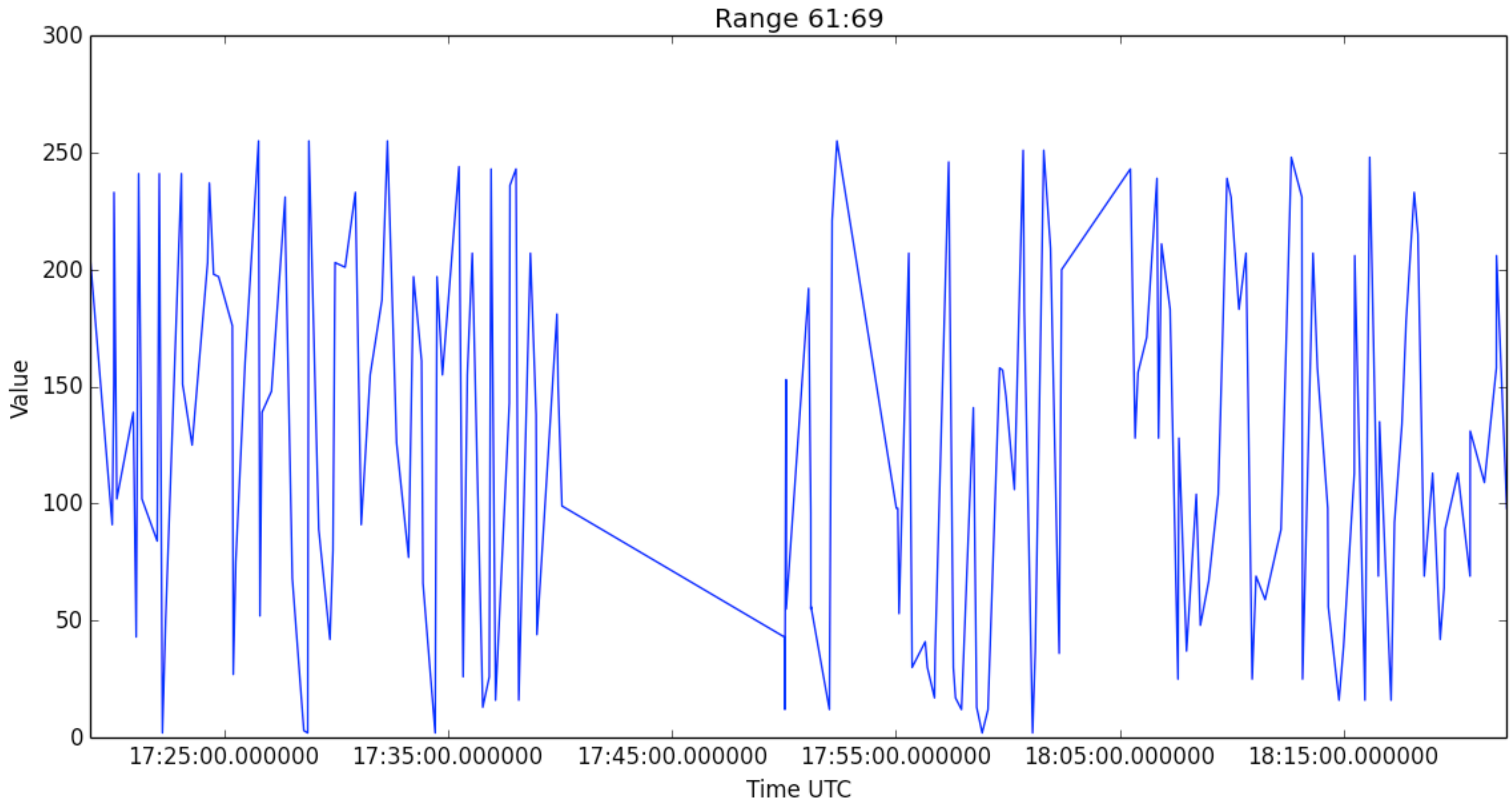
Field Speculation



Field 5-12 Stats



Field 13-20 Stats

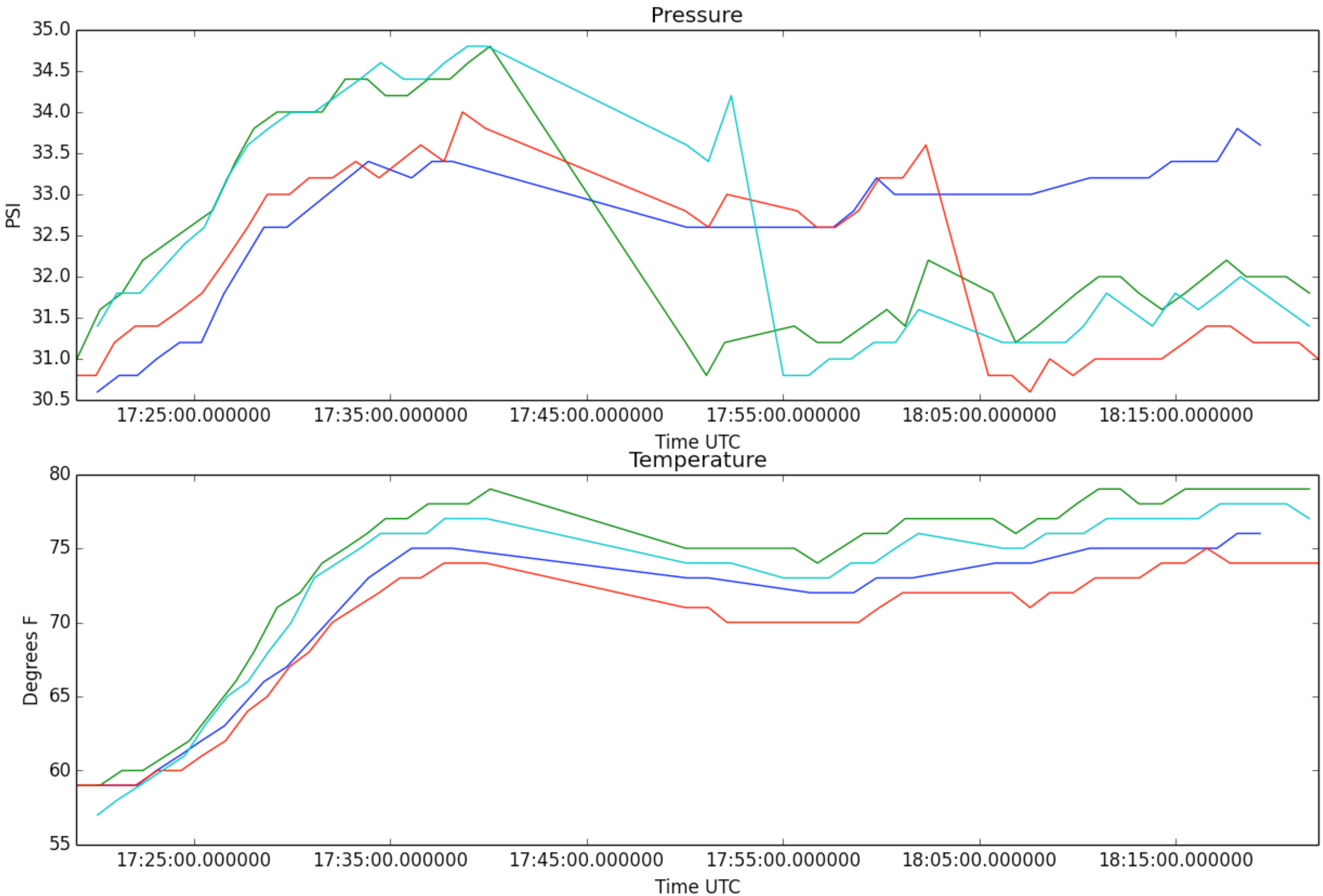


CRC Field Stats

```
$ cat demodulated.txt | packet_stats.py --encoding man --length 70 --brutecrc 2
| tee brute.txt
$ bruteforce-crc --file brute.txt --width 8 --start 5 --end 61 --offs-crc 61
number of threads        : 4
width                    : 8 bits
CRC's offset             : 61
calc CRC for bit offsets : 5 .. 61 (not included)
final XOR                : 0
reflect in               : false
reflect out              : false

truncated polynom        : from 0 to 255 (MSB not shown)
initial value            : from 0 to 255
probe reflections        : false
probe final xor          : false
...snip...
---------------------[ MATCH ]--------------------------------
Found a model for the CRC calculation:
Truncated polynom : 0x7 (7)
Initial value     : 0x0 (0)
Final XOR         : 0x0 (0)
Reflected input   : false
Reflected output  : false
Message offset    : from bit 5 .. 61 (end not included)
```

CRC Attack



Decode, Validate & Graph!

Monitor All The TPMSes

- FSK very common. Haven't decoded ASK yet.
- Deviation, center frequency, bit rate varies.
- Packet layout varies. CRC/checksum varies.
- Not feasible to build a single demodulator.

Concerns

- Signals easily received from 10s of meters.
- Signals easy to demodulate and decode.
- IDs in clear. Apparently unique.
- Requires $20 US receiver and a laptop.
- No in-field firmware update mechanism…

Implications

Industry Response

- “Nearly Impossible” to track a driver’s location.
    - Weak signals.
    - Security through obscurity.
    - Expensive to deploy trackers.

Call To Action

- Get some hardware: RTL-SDR, HackRF, etc.
- Get my code: github.com/jboone/tpms
- Ride along, capture, decode signals. Contribute what you’ve learned.

Other Reading

- “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study”, Rutgers & Univ. of SC.

Questions?