LET'S SEE WHAT'S OUT THERE - MAPPING THE WIRELESS IOT

by Tobias Zillner

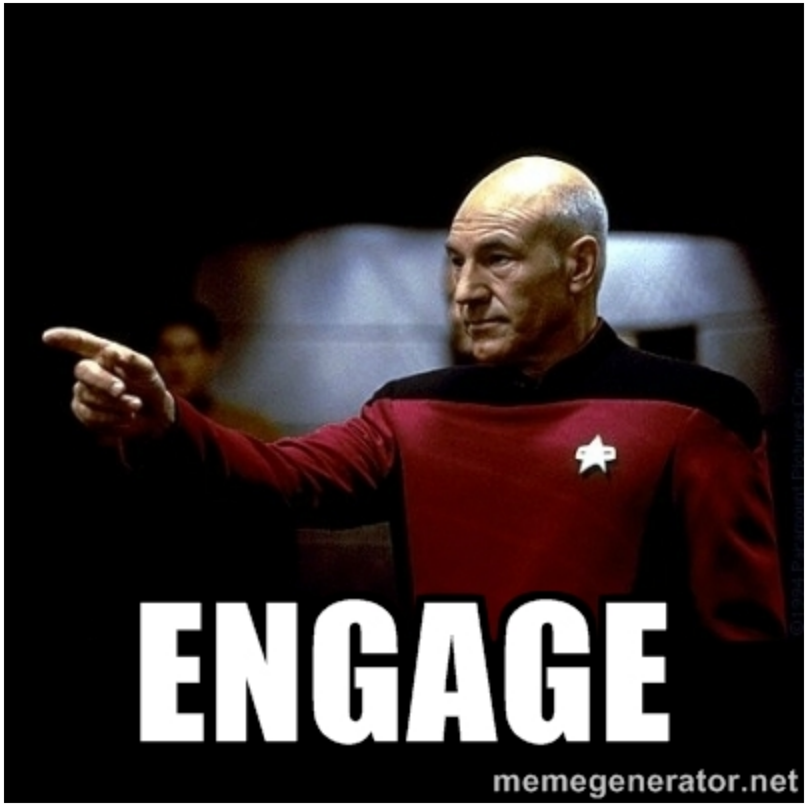
cognosec

ABOUT ME

- Freelancer, IT Security
- Senior IS Auditor @ Cognosec
- Penetration Testing, Security Audits & Consulting
- IoT Security Research, Playing with SDR

cognosec

AGENDA



- Introduction
- Signal discovery
- Signal to bits
- Wireless Security Issues
- Demo
- Summary

LET'S SEE WHAT'S OUT THERE - MAPPING THE WIRELESS IOT

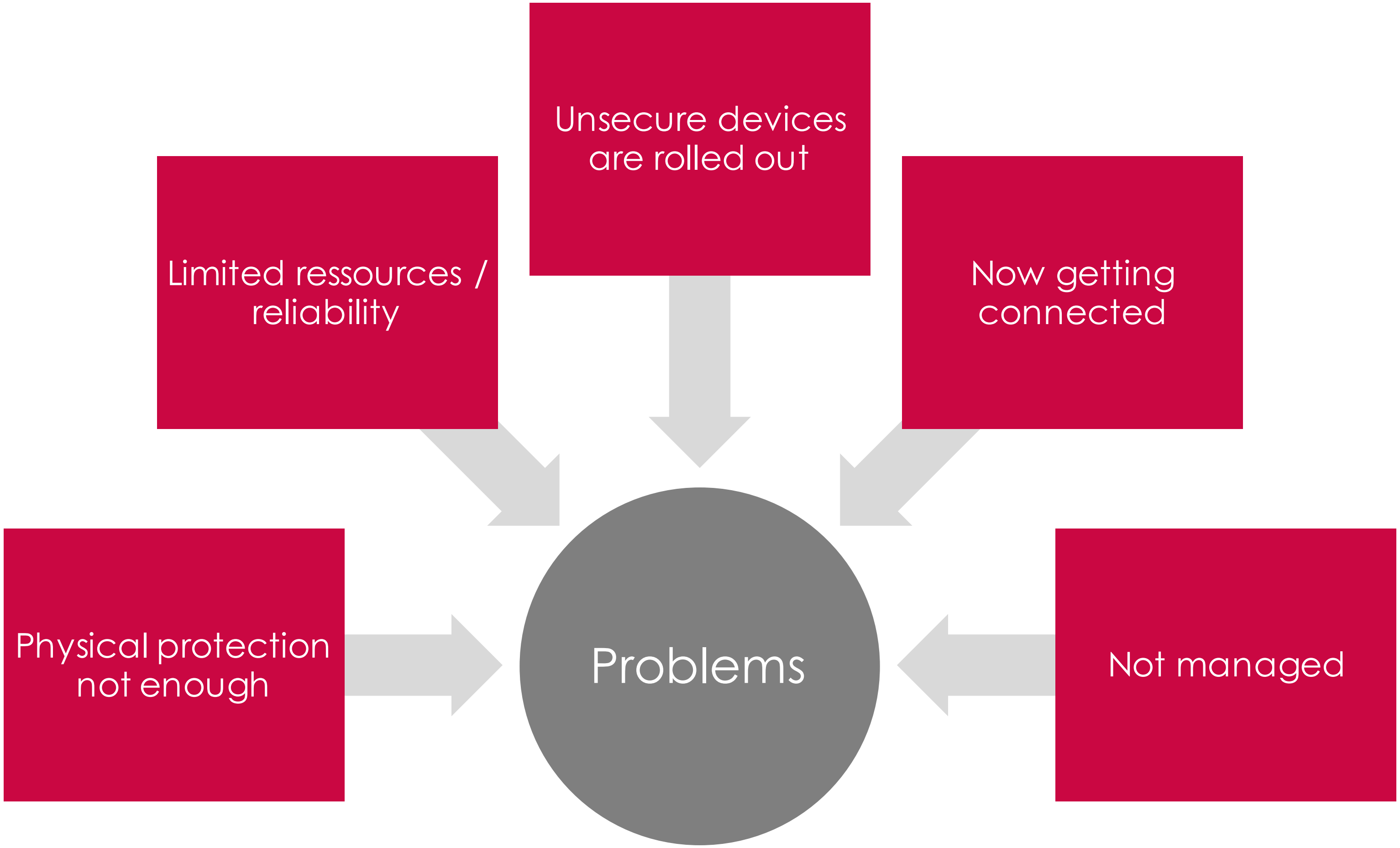
WHAT IT'S ALL ABOUT

cognosec

WHAT IS THE WIRELESS IOT?

- Low power / low cost devices
- Often no TCP/IP
- Different communication standards
- Make physical devices „smart“

PROBLEMS



Unsecure devices are rolled out

Limited ressources / reliability

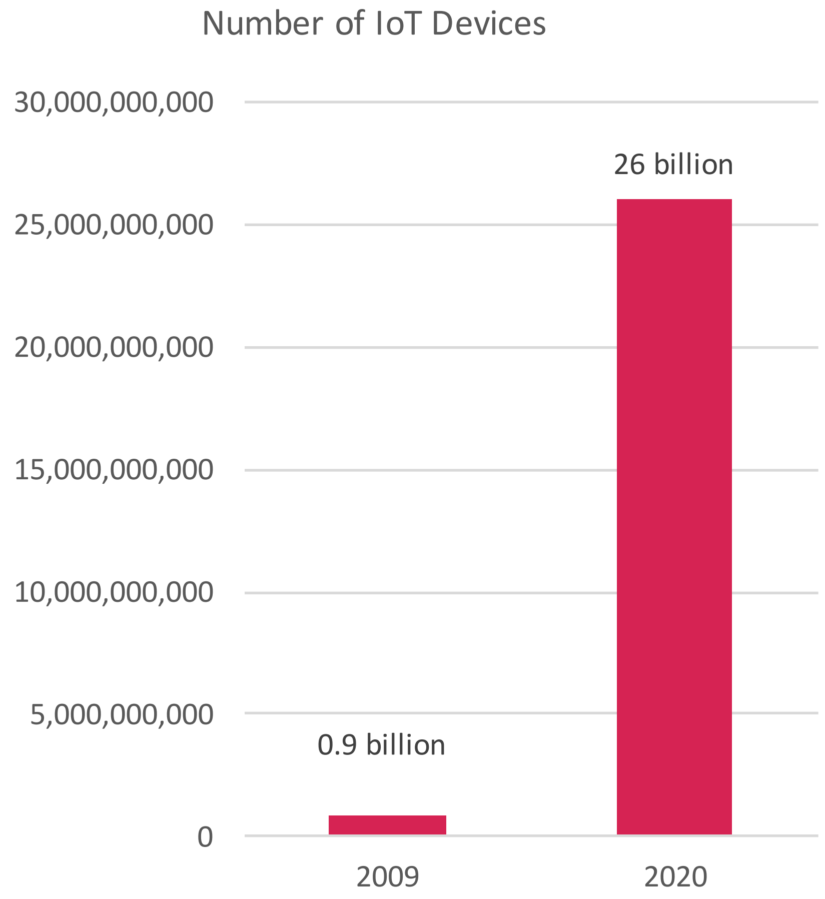
Now getting connected

Physical protection not enough

Problems

Not managed

WHY IS IT IMPORTANT?



- Wireless connections are the future
- Samsung CEO BK Yoon - “Every Samsung device will be part of IoT till 2019” [3]

[1] http://www.gartner.com/newsroom/id/2839717
[2] http://www.gartner.com/newsroom/id/2636073
[3] http://www.heise.de/newsticker/meldung/CES-Internet-der-Dinge-komfortabel-vernetzt-2512856.html

WHY IS IT IMPORTANT?

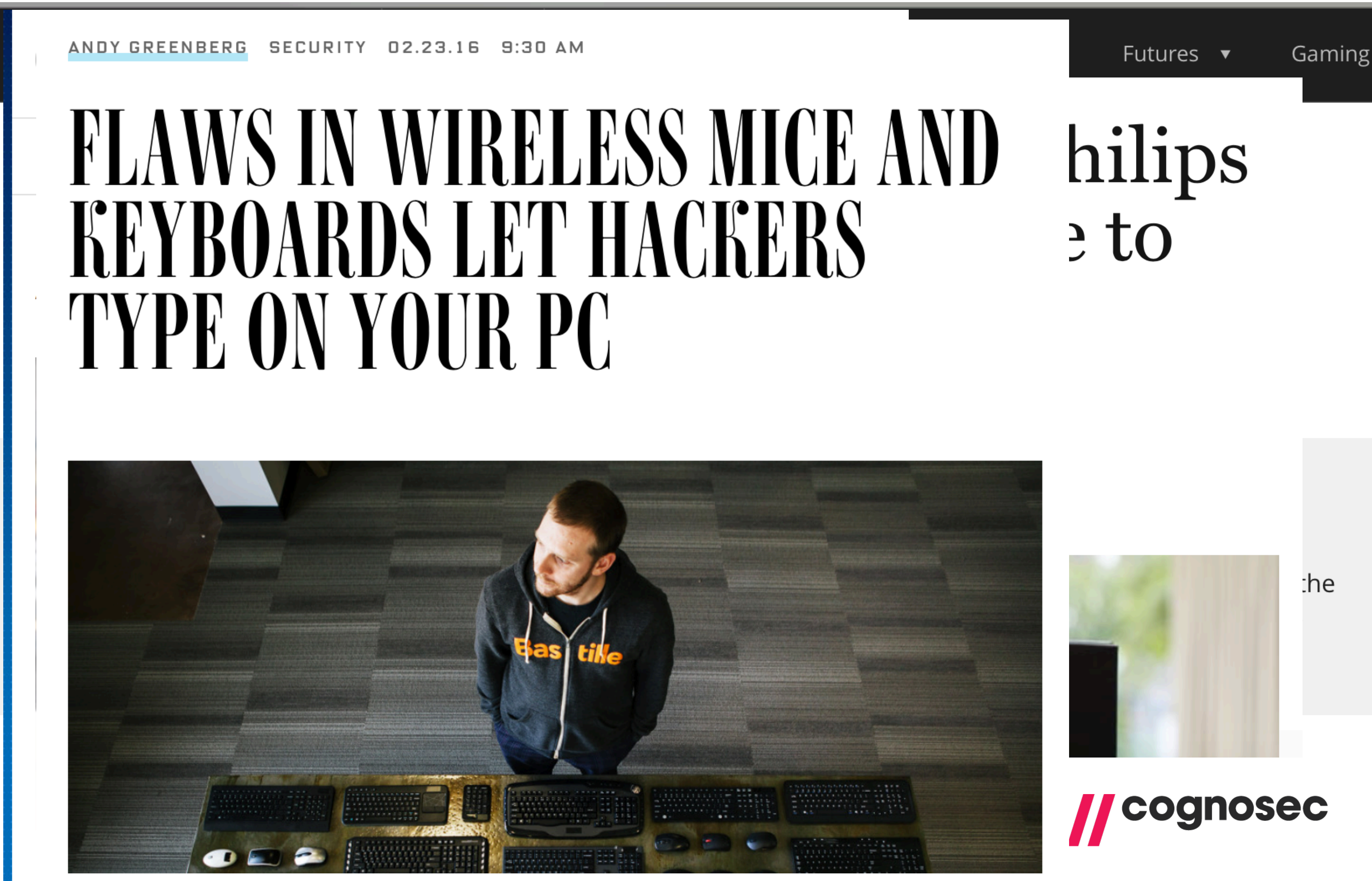
“Smart” devices incorporated into the electric grid, vehicles — including autonomous vehicles — and household appliances are improving efficiency, energy conservation, and convenience. However, security industry analysts have demonstrated that many of these new systems can threaten data privacy, data integrity, or continuity of services. In the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.”

-James Clapper
United States Director of National Intelligence

http://www.hotforsecurity.com/blog/us-intelligence-chief-the-internet-of-things-will-be-used-to-spy-and-hack-13400.html

//cognosec

POPULAR WIRELESS FAILS



ANDY GREENBERG SECURITY 02.23.16 9:30 AM

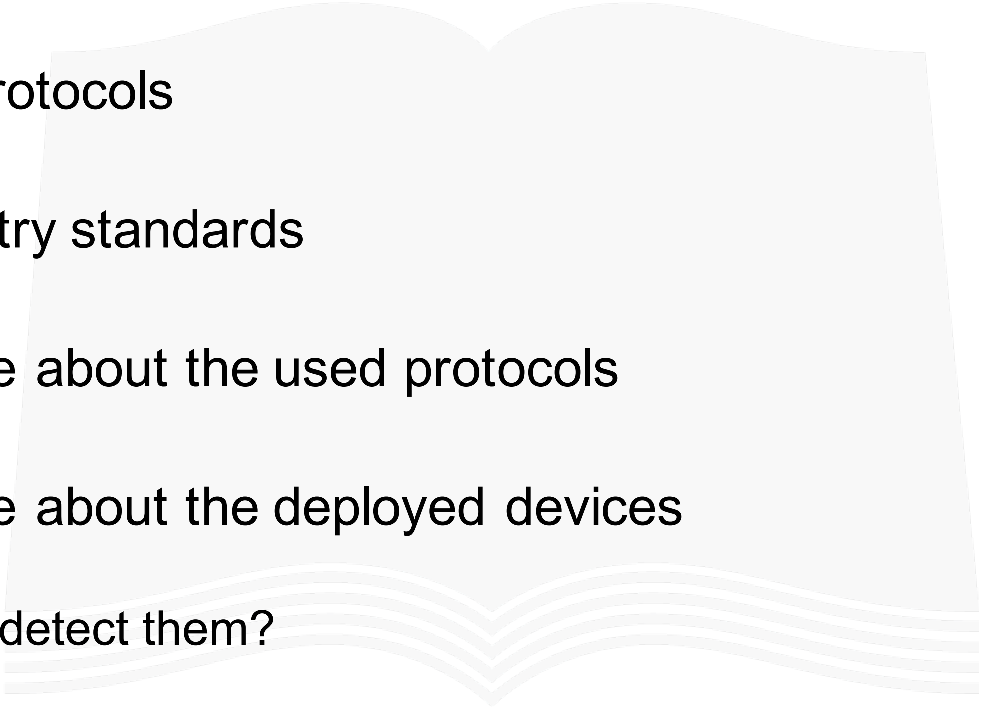
FLAWS IN WIRELESS MICE AND KEYBOARDS LET HACKERS TYPE ON YOUR PC

SO, WHAT ARE THE BIGGEST PROBLEMS?

PROBLEMS FOR WIRELESS ASSESSMENTS

- What is really out there?
- Blind spot in cyber security strategies
- Not visible in network diagrams
- Knowledge gap
- Lack of tools

KNOWLEDGE GAP

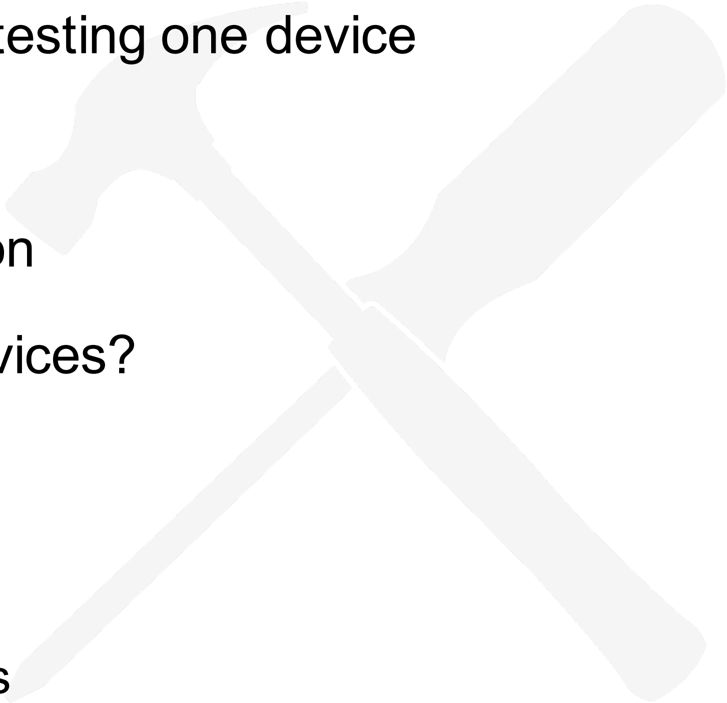


- Different technologies and standards used
- Proprietary protocols
- Lack of industry standards
- No knowledge about the used protocols
- No knowledge about the deployed devices
  - How to detect them?

cognosec

LACK OF TOOLS

- Some prototypes but no mature tools
- Often just built for testing one device
- Not maintained
- Poor documentation
- How to test the devices?
  - Methodology
  - Scenarios
  - Attack vectors



LET'S SEE WHAT'S OUT THERE - MAPPING THE WIRELESS IOT

SIGNAL DISCOVERY

cognosec

INFORMATION GATHERING

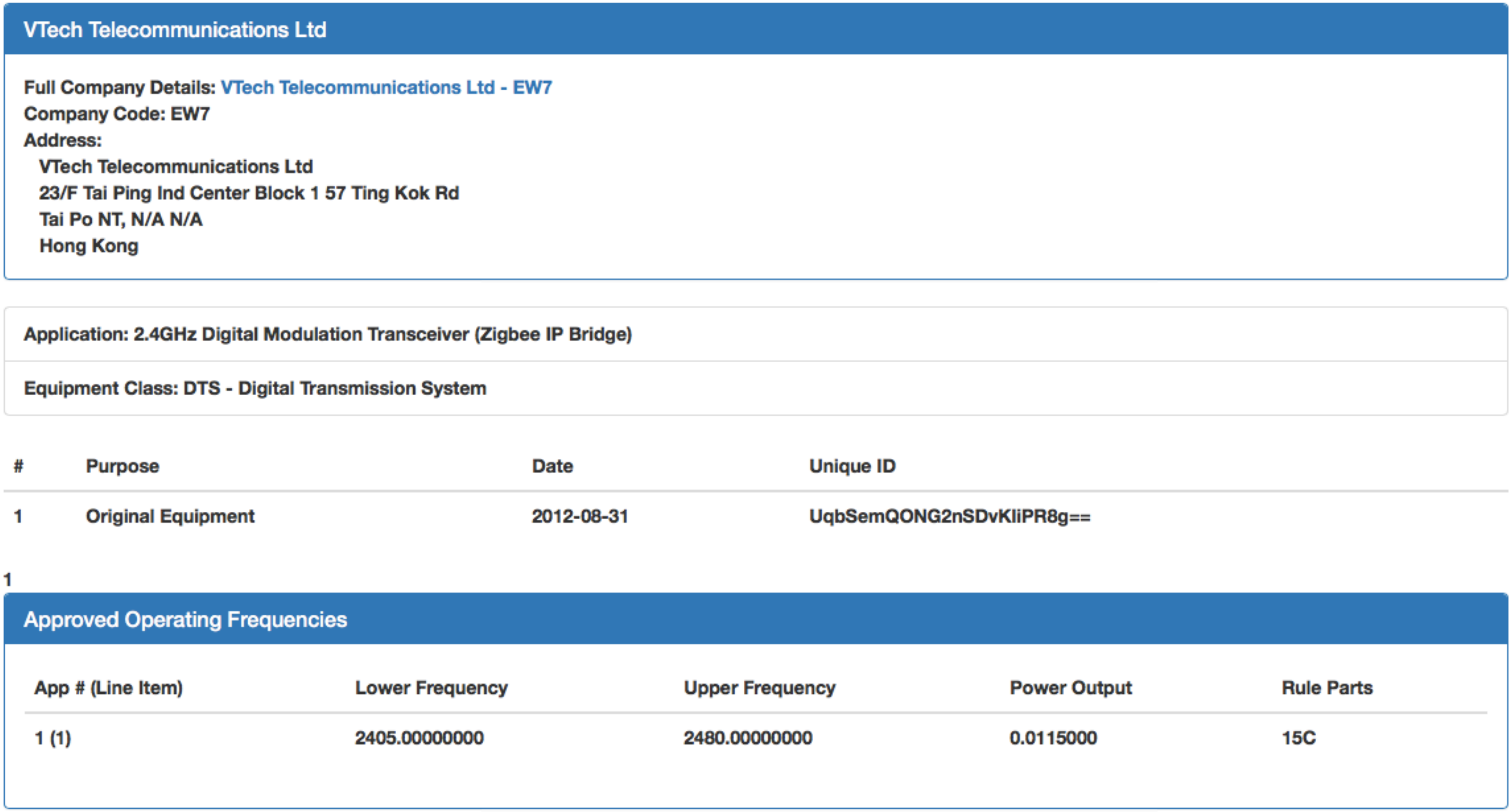
- Interviews

1 2 3 4

INFORMATION GATHERING

- Interviews
- Check FCC ID
  - Fccid.io
  - http://www.comsearch.com/articles/emission.pdf
  - Search for other devices from the vendor

FCC ID



VTech Telecommunications Ltd

Full Company Details: VTech Telecommunications Ltd - EW7
Company Code: EW7
Address:

VTech Telecommunications Ltd
23/F Tai Ping Ind Center Block 1 57 Ting Kok Rd
Tai Po NT, N/A N/A
Hong Kong

Application: 2.4GHz Digital Modulation Transceiver (Zigbee IP Bridge)

Equipment Class: DTS - Digital Transmission System

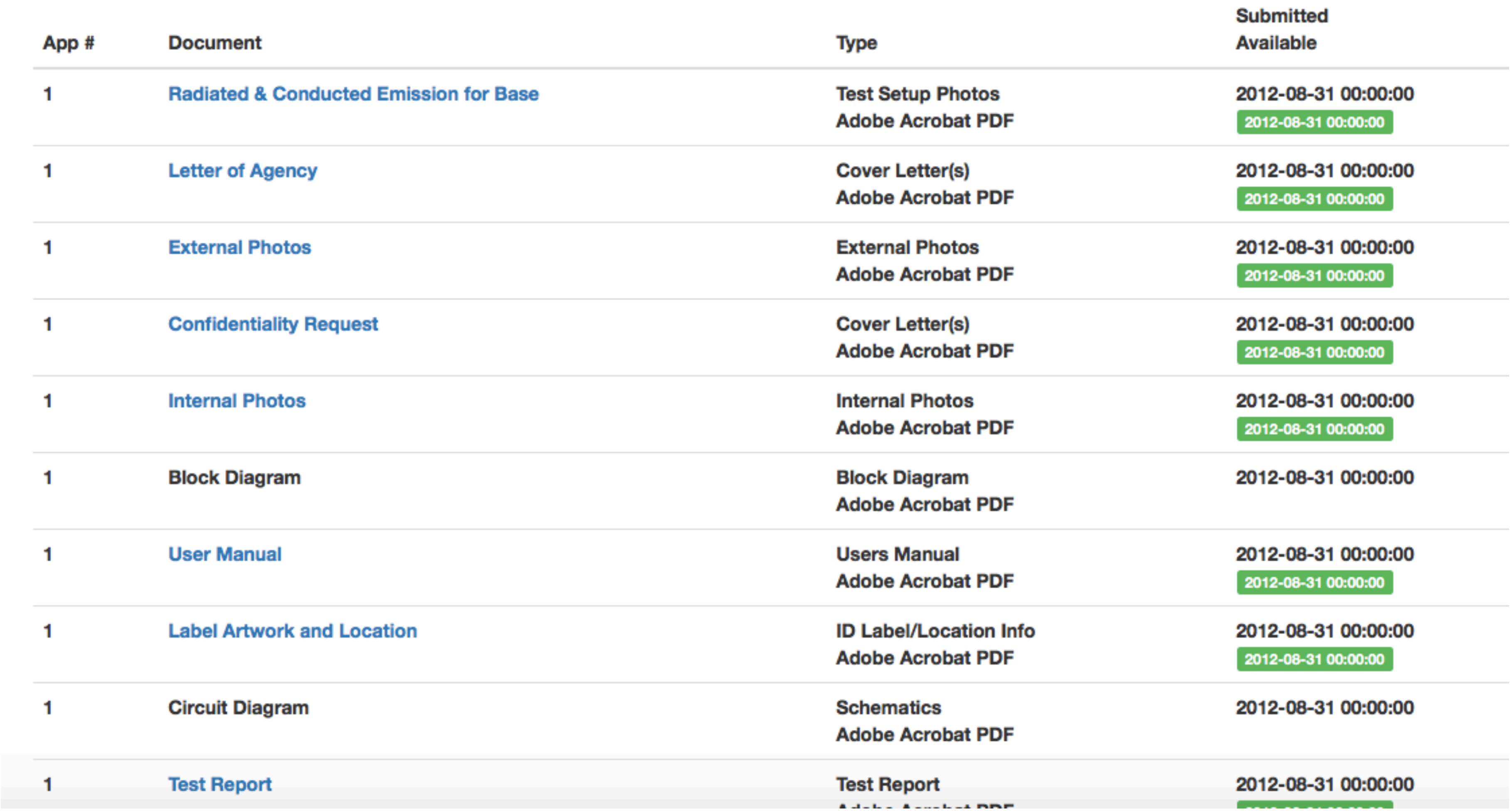
#	Purpose	Date	Unique ID
1	Original Equipment	2012-08-31	UqbSemQONG2nSDvKliPR8g==

1

Approved Operating Frequencies

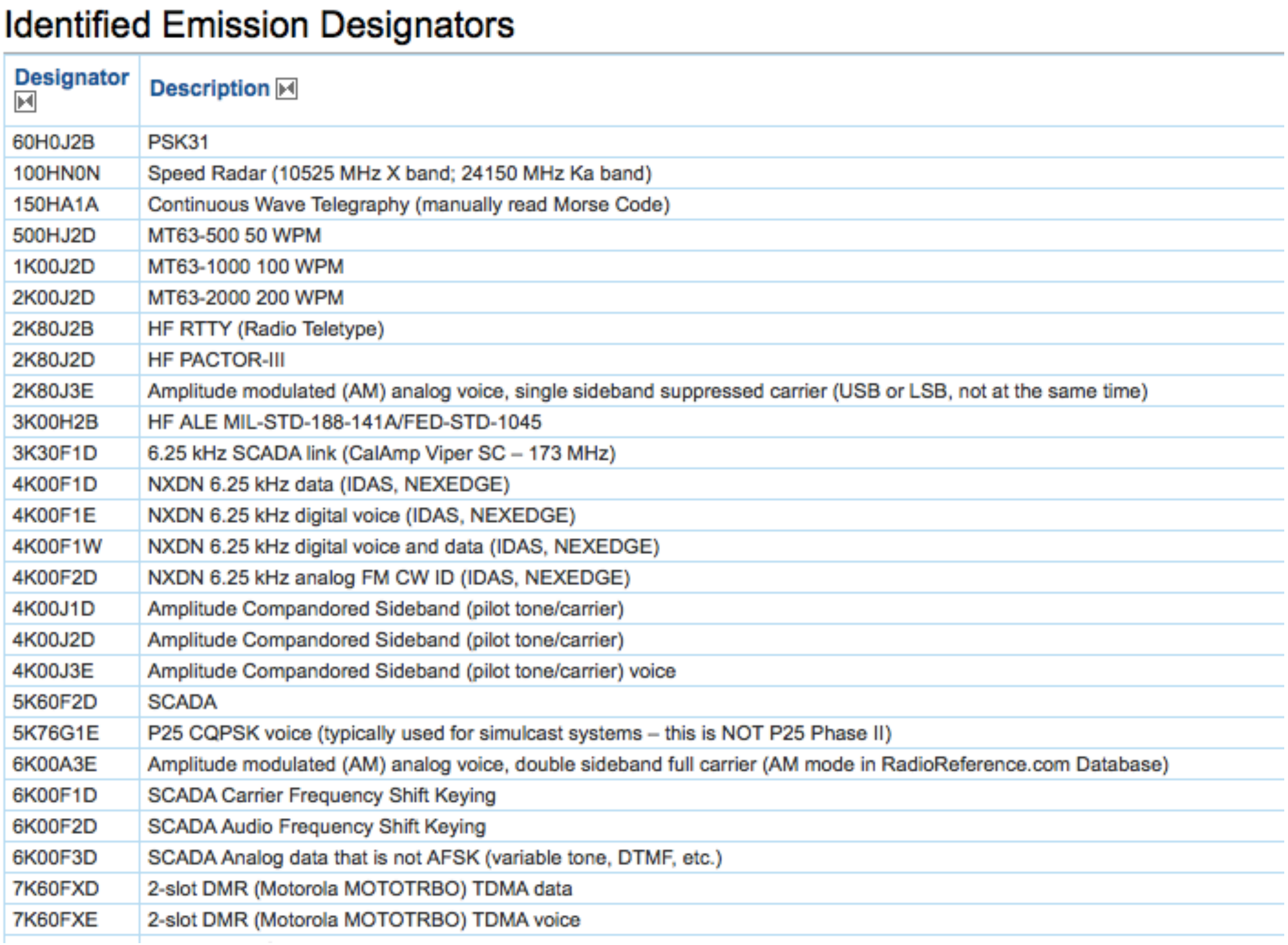
App # (Line Item)	Lower Frequency	Upper Frequency	Power Output	Rule Parts
1 (1)	2405.00000000	2480.00000000	0.0115000	15C

FCC ID



App #	Document	Type	Submitted Available
1	Radiated & Conducted Emission for Base	Test Setup Photos Adobe Acrobat PDF	2012-08-31 00:00:00 2012-08-31 00:00:00
1	Letter of Agency	Cover Letter(s) Adobe Acrobat PDF	2012-08-31 00:00:00 2012-08-31 00:00:00
1	External Photos	External Photos Adobe Acrobat PDF	2012-08-31 00:00:00 2012-08-31 00:00:00
1	Confidentiality Request	Cover Letter(s) Adobe Acrobat PDF	2012-08-31 00:00:00 2012-08-31 00:00:00
1	Internal Photos	Internal Photos Adobe Acrobat PDF	2012-08-31 00:00:00 2012-08-31 00:00:00
1	Block Diagram	Block Diagram Adobe Acrobat PDF	2012-08-31 00:00:00
1	User Manual	Users Manual Adobe Acrobat PDF	2012-08-31 00:00:00 2012-08-31 00:00:00
1	Label Artwork and Location	ID Label/Location Info Adobe Acrobat PDF	2012-08-31 00:00:00 2012-08-31 00:00:00
1	Circuit Diagram	Schematics Adobe Acrobat PDF	2012-08-31 00:00:00
1	Test Report	Test Report Adobe Acrobat PDF	2012-08-31 00:00:00

EMISSION DESIGNATOR



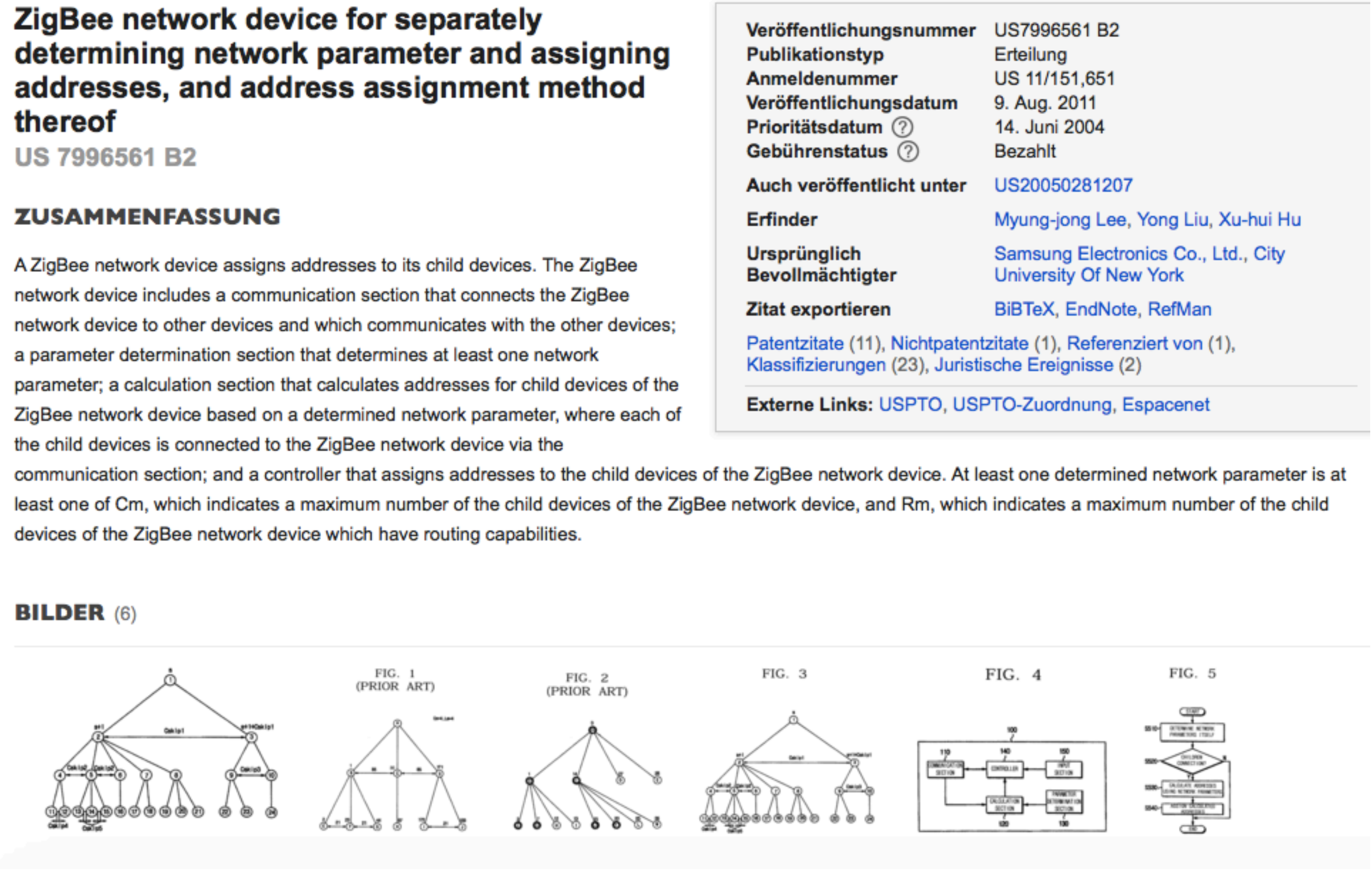
Identified Emission Designators

Designator	Description
60H0J2B	PSK31
100HN0N	Speed Radar (10525 MHz X band; 24150 MHz Ka band)
150HA1A	Continuous Wave Telegraphy (manually read Morse Code)
500HJ2D	MT63-500 50 WPM
1K00J2D	MT63-1000 100 WPM
2K00J2D	MT63-2000 200 WPM
2K80J2B	HF RTTY (Radio Teletype)
2K80J2D	HF PACTOR-III
2K80J3E	Amplitude modulated (AM) analog voice, single sideband suppressed carrier (USB or LSB, not at the same time)
3K00H2B	HF ALE MIL-STD-188-141A/FED-STD-1045
3K30F1D	6.25 kHz SCADA link (CalAmp Viper SC – 173 MHz)
4K00F1D	NXDN 6.25 kHz data (IDAS, NEXEDGE)
4K00F1E	NXDN 6.25 kHz digital voice (IDAS, NEXEDGE)
4K00F1W	NXDN 6.25 kHz digital voice and data (IDAS, NEXEDGE)
4K00F2D	NXDN 6.25 kHz analog FM CW ID (IDAS, NEXEDGE)
4K00J1D	Amplitude Compandored Sideband (pilot tone/carrier)
4K00J2D	Amplitude Compandored Sideband (pilot tone/carrier)
4K00J3E	Amplitude Compandored Sideband (pilot tone/carrier) voice
5K60F2D	SCADA
5K76G1E	P25 CQPSK voice (typically used for simulcast systems – this is NOT P25 Phase II)
6K00A3E	Amplitude modulated (AM) analog voice, double sideband full carrier (AM mode in RadioReference.com Database)
6K00F1D	SCADA Carrier Frequency Shift Keying
6K00F2D	SCADA Audio Frequency Shift Keying
6K00F3D	SCADA Analog data that is not AFSK (variable tone, DTMF, etc.)
7K60FXD	2-slot DMR (Motorola MOTOTRBO) TDMA data
7K60FXE	2-slot DMR (Motorola MOTOTRBO) TDMA voice

INFORMATION GATHERING

- Interviews
- Check FCC ID
  - Fccid.io
  - http://www.comsearch.com/articles/emission.pdf
  - Search for other devices from the vendor
- Google Patent search

GOOGLE PATENT



ZigBee network device for separately determining network parameter and assigning addresses, and address assignment method thereof

US 7996561 B2

ZUSAMMENFASSUNG

A ZigBee network device assigns addresses to its child devices. The ZigBee network device includes a communication section that connects the ZigBee network device to other devices and which communicates with the other devices; a parameter determination section that determines at least one network parameter; a calculation section that calculates addresses for child devices of the ZigBee network device based on a determined network parameter, where each of the child devices is connected to the ZigBee network device via the communication section; and a controller that assigns addresses to the child devices of the ZigBee network device. At least one determined network parameter is at least one of Cm, which indicates a maximum number of the child devices of the ZigBee network device, and Rm, which indicates a maximum number of the child devices of the ZigBee network device which have routing capabilities.

Veröffentlichungsnummer	US7996561 B2
Publikationstyp	Erteilung
Anmeldenummer	US 11/151,651
Veröffentlichungsdatum	9. Aug. 2011
Prioritätsdatum ?	14. Juni 2004
Gebührenstatus ?	Bezahlt
Auch veröffentlicht unter	US20050281207
Erfinder	Myung-jong Lee, Yong Liu, Xu-hui Hu
Ursprünglich Bevollmächtigter	Samsung Electronics Co., Ltd., City University Of New York
Zitat exportieren	BiBTeX, EndNote, RefMan

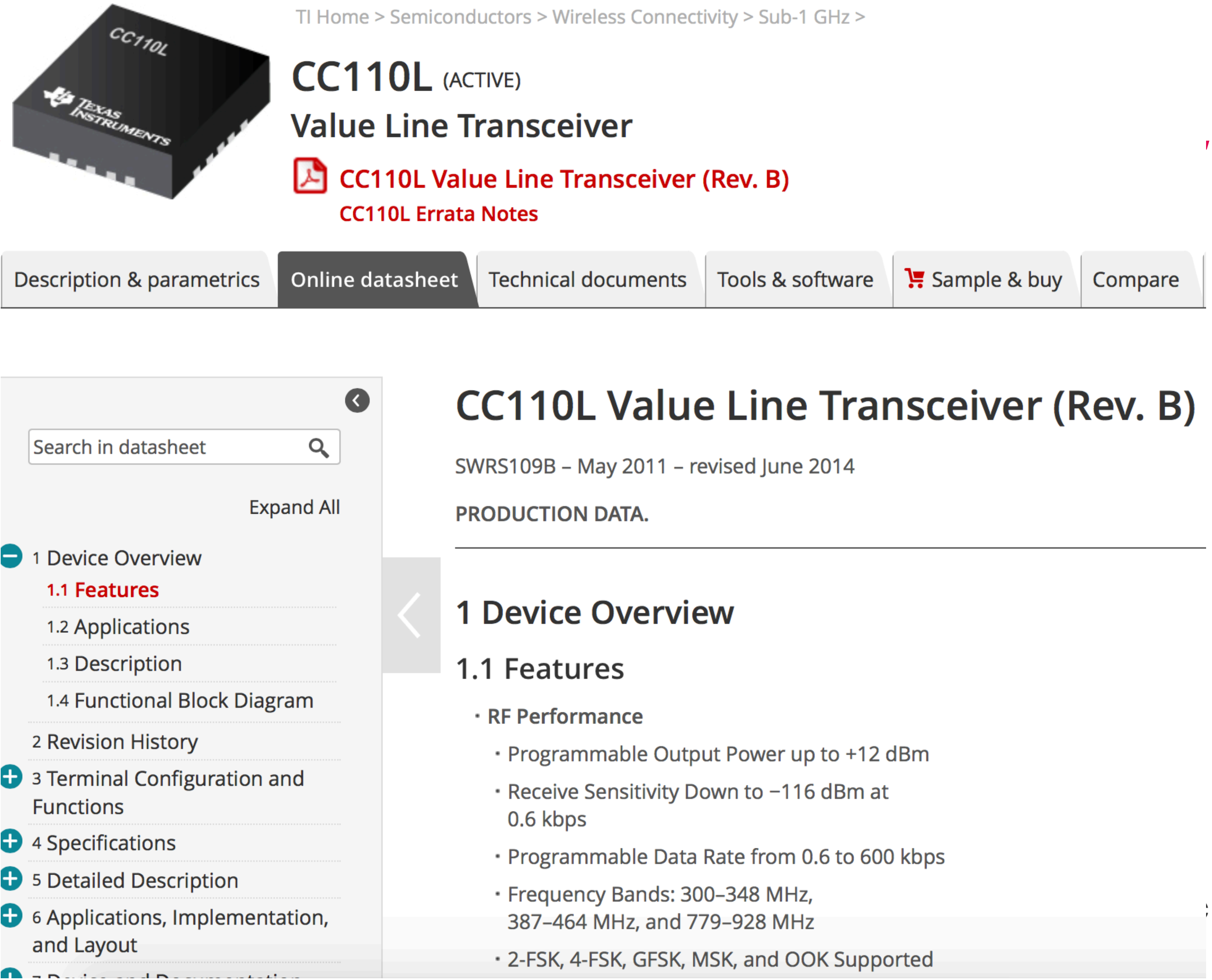
Patentzitate (11), Nichtpatentzitate (1), Referenziert von (1), Klassifizierungen (23), Juristische Ereignisse (2)

Externe Links: USPTO, USPTO-Zuordnung, Espacenet

BILDER (6)

INFORMATION GATHERING

- Interviews
- Check FCC ID
  - Fccid.io
  - http://www.comsearch.com/articles/emission.pdf
  - Search for other devices from the vendor
- Google Patent search
- Product documentation
- RF chip, Firmware, Software



TI Home > Semiconductors > Wireless Connectivity > Sub-1 GHz >

CC110L (ACTIVE)

Value Line Transceiver

CC110L Value Line Transceiver (Rev. B)

CC110L Errata Notes

CC110L Value Line Transceiver (Rev. B)

SWRS109B – May 2011 – revised June 2014

PRODUCTION DATA.

1 Device Overview

1.1 Features

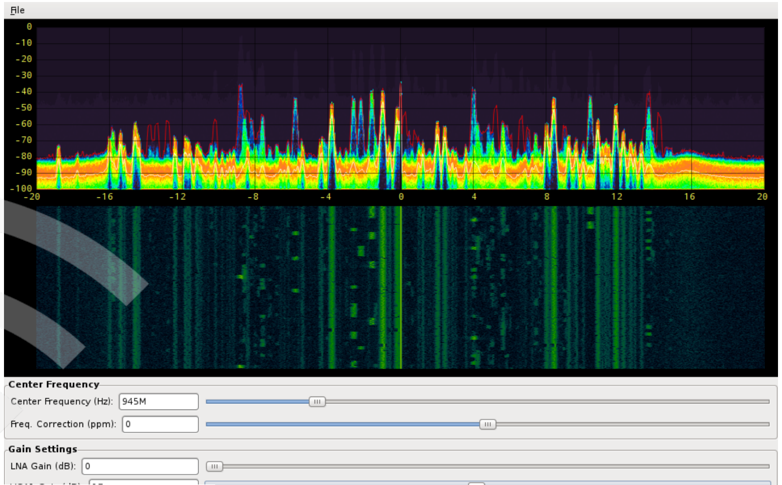
- RF Performance
  - Programmable Output Power up to +12 dBm
  - Receive Sensitivity Down to −116 dBm at 0.6 kbps
  - Programmable Data Rate from 0.6 to 600 kbps
  - Frequency Bands: 300–348 MHz, 387–464 MHz, and 779–928 MHz
  - 2-FSK, 4-FSK, GFSK, MSK, and OOK Supported

INFORMATION GATHERING

- Interviews
- Check FCC ID
  - Fccid.io
  - http://www.comsearch.com/articles/emission.pdf
  - Search for other devices from the vendor
- Google Patent search
- Product documentation
- RF chip, Firmware, Software
- Visual signal inspection

VISUAL SIGNAL INSPECTION

- Inspectrum
- Baudline
- Fosphor
- GNU Radio



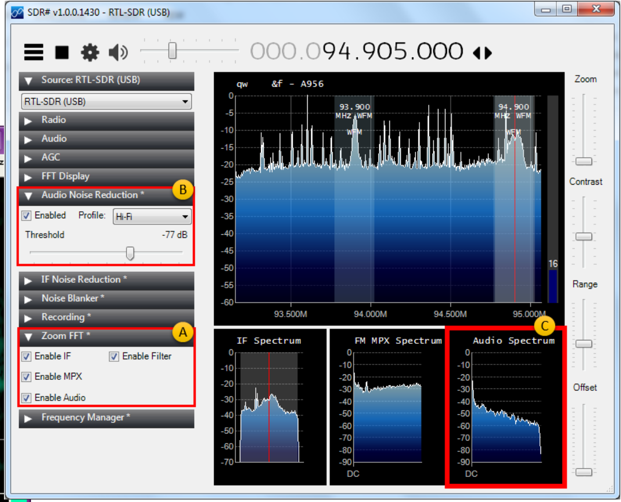
Center Frequency

Center Frequency (Hz): 945M

Freq. Correction (ppm): 0

Gain Settings

LNA Gain (dB): 0



SDR# v1.0.0.1430 - RTL-SDR (USB)

000.094.905.000

Source: RTL-SDR (USB)

RTL-SDR (USB)

Audio Noise Reduction * B

☑ Enabled Profile: Hi-Fi

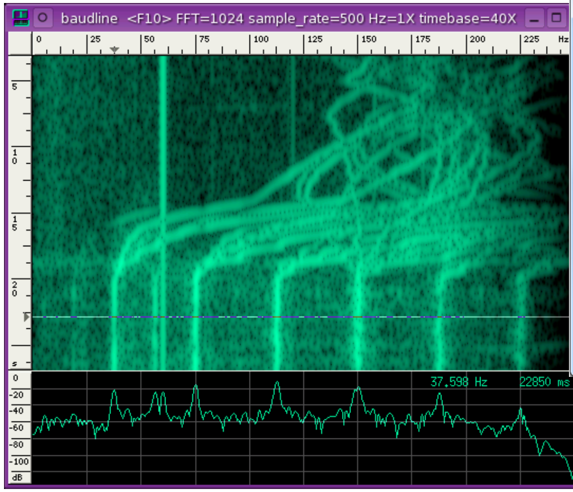
Threshold -77 dB

Zoom FFT * A

☑ Enable IF ☑ Enable Filter

☑ Enable MPX

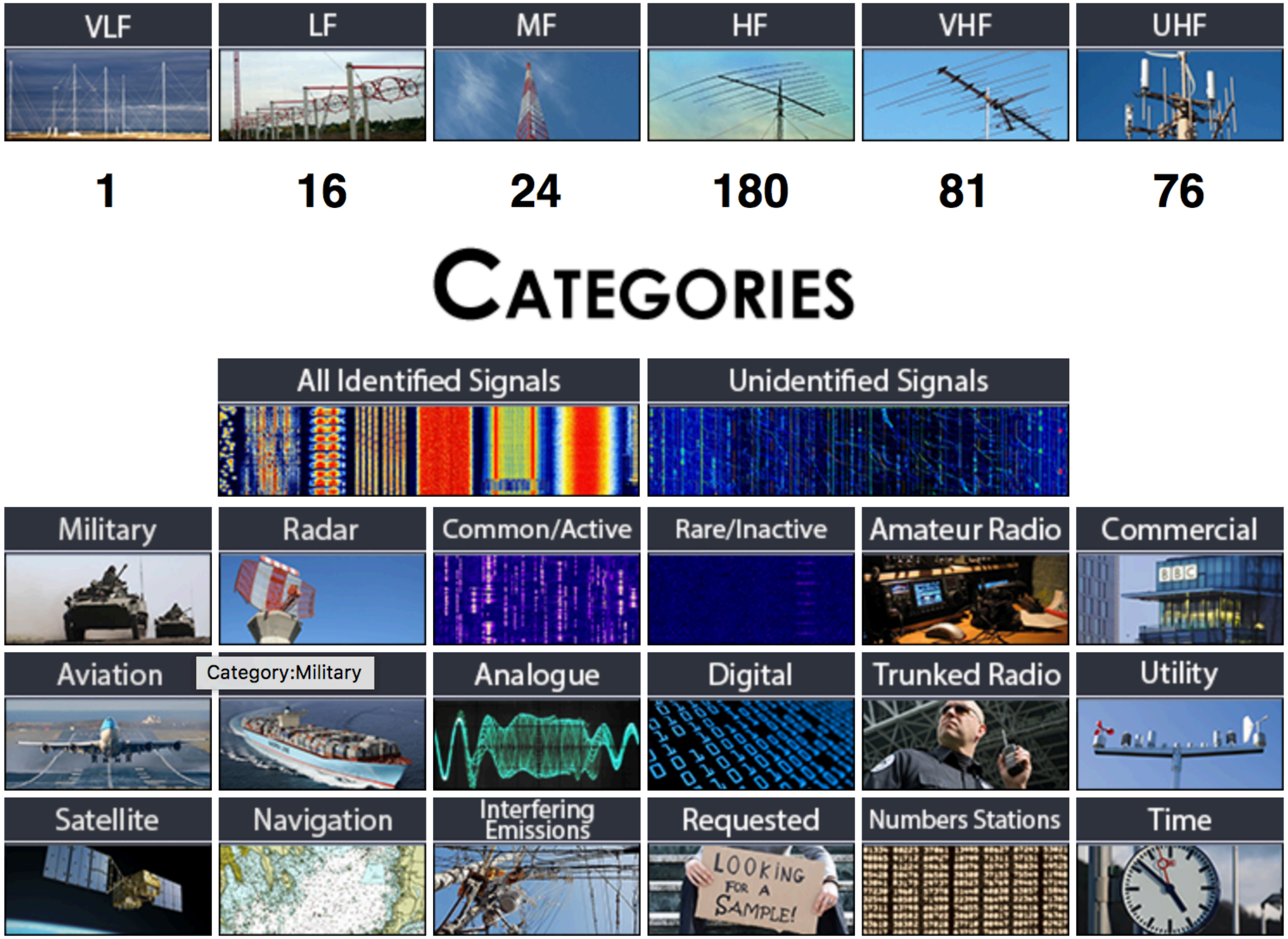
☑ Enable Audio



baudline <F10> FFT=1024 sample_rate=500 Hz=1X timebase=40X

//cognosec

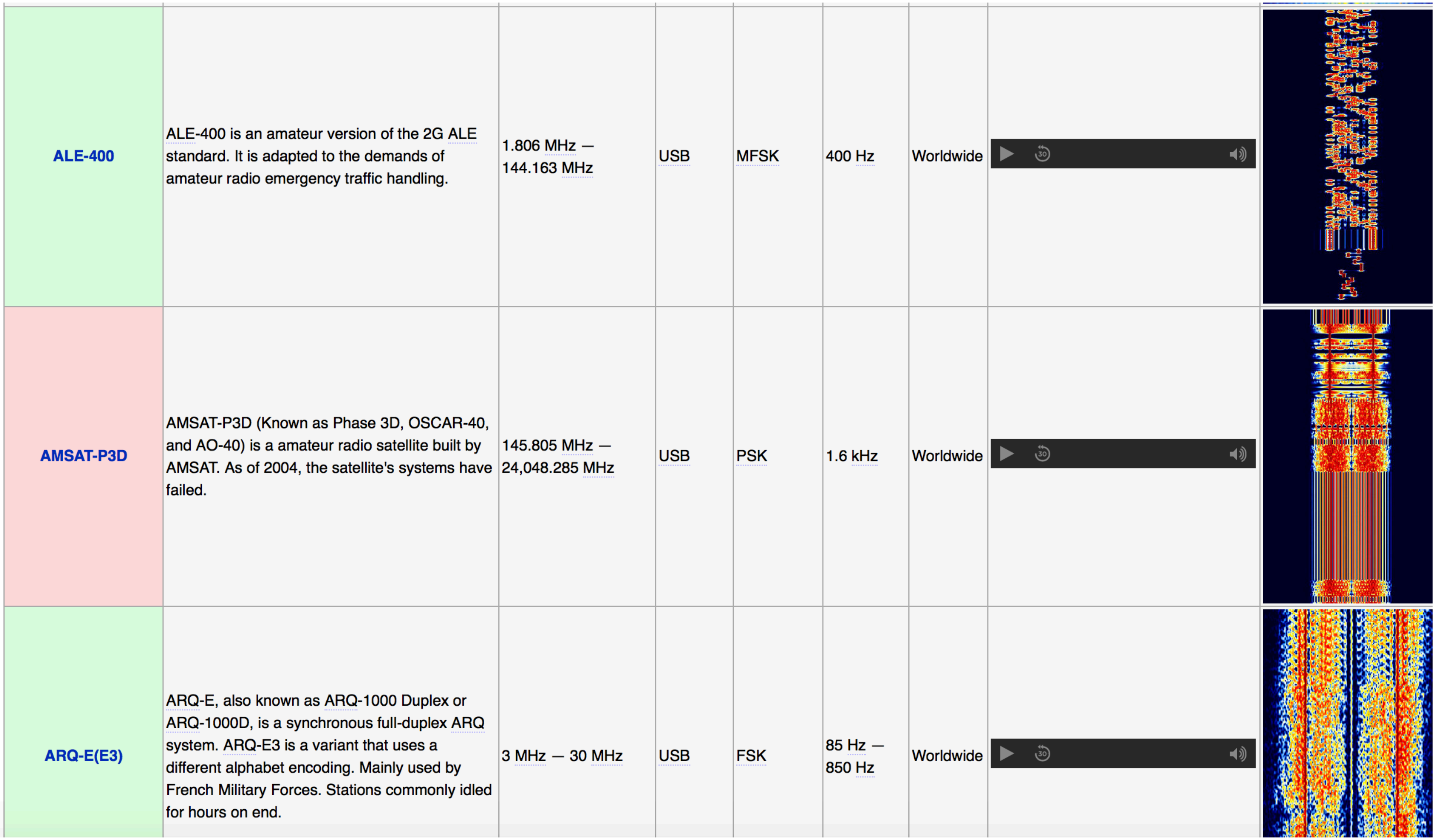
FREQUENCY BANDS



VLF	LF	MF	HF	VHF	UHF
1	16	24	180	81	76

sigidwiki.com

VISUAL SIGNAL INSPECTION

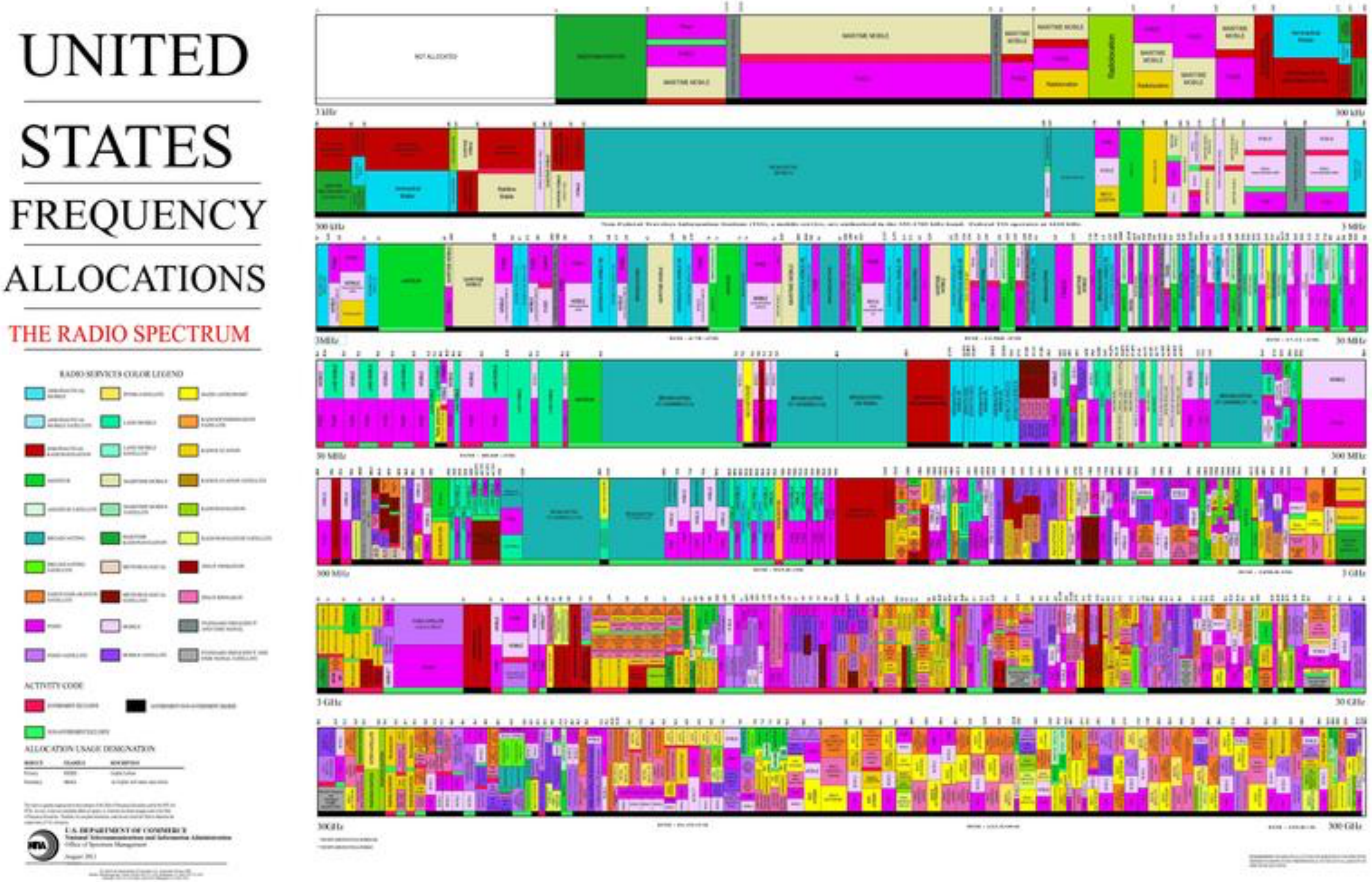


ALE-400	ALE-400 is an amateur version of the 2G ALE standard. It is adapted to the demands of amateur radio emergency traffic handling.	1.806 MHz — 144.163 MHz	USB	MFSK	400 Hz	Worldwide	▶	
AMSAT-P3D	AMSAT-P3D (Known as Phase 3D, OSCAR-40, and AO-40) is a amateur radio satellite built by AMSAT. As of 2004, the satellite's systems have failed.	145.805 MHz — 24,048.285 MHz	USB	PSK	1.6 kHz	Worldwide	▶	
ARQ-E(E3)	ARQ-E, also known as ARQ-1000 Duplex or ARQ-1000D, is a synchronous full-duplex ARQ system. ARQ-E3 is a variant that uses a different alphabet encoding. Mainly used by French Military Forces. Stations commonly idled for hours on end.	3 MHz — 30 MHz	USB	FSK	85 Hz — 850 Hz	Worldwide	▶	

sigidwiki.com

INFORMATION GATHERING

- Interviews
- Check FCC ID
  - Fccid.io
  - http://www.comsearch.com/articles/emission.pdf
  - Search for other devices from the vendor
- Google Patent search
- Product documentation
- RF chip, Firmware, Software
- Visual signal inspection
- Check frequency bands for legal issues



UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM

RADIO SERVICES COLOR LEGEND

ACTIVITY CODE

ALLOCATION USAGE DESIGNATION

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management

August 2011

//cognosec

LET’S SEE WHAT’S OUT THERE - MAPPING THE WIRELESS IOT

SIGNAL TO BITS

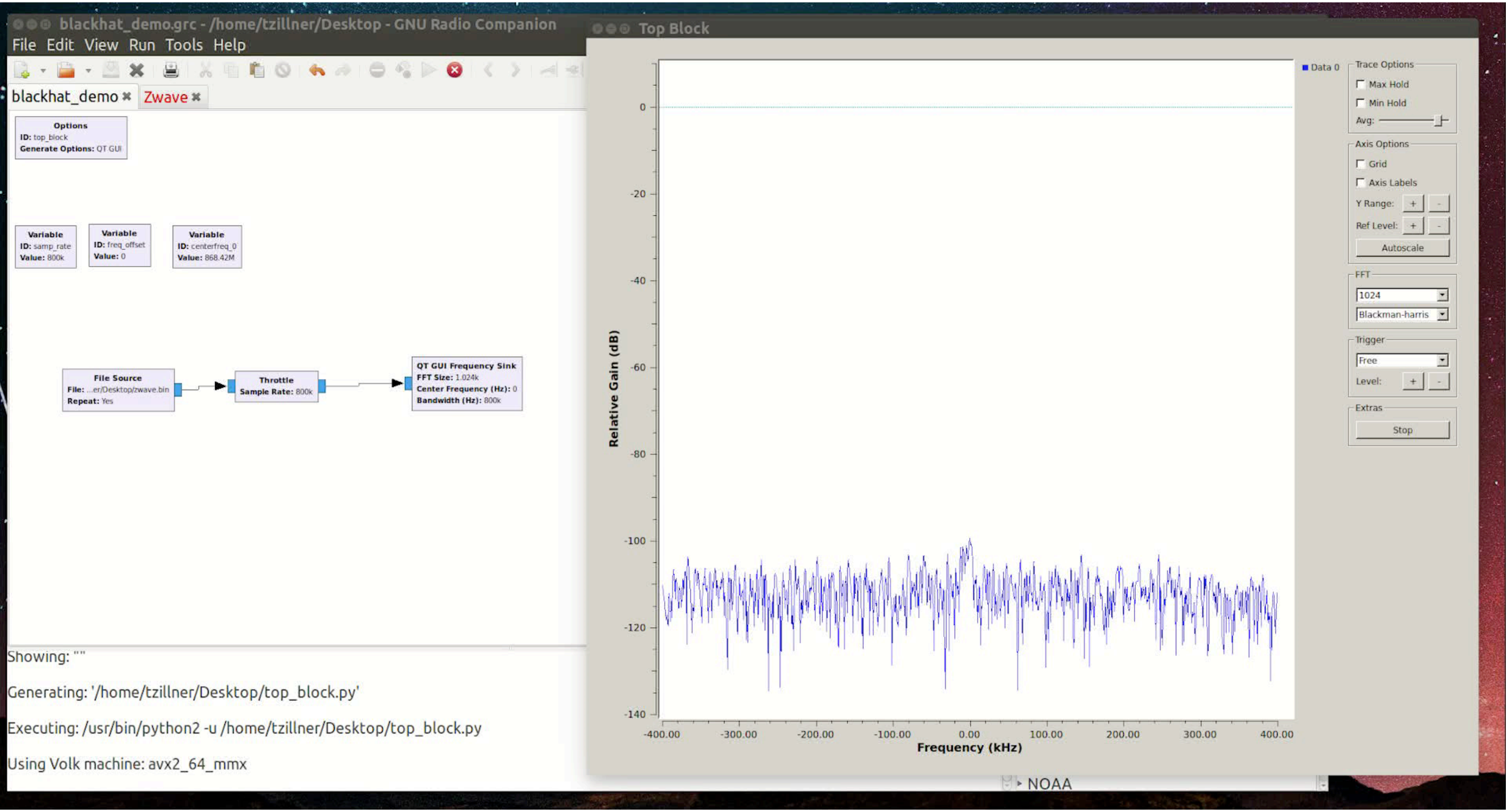
cognosec

SIGNAL TO BITS

Find the Signal

Identify the Data Channel

FINDING A SIGNAL



blackhat_demo.grc - /home/tzillner/Desktop - GNU Radio Companion

Options
ID: top_block
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 800k

Variable
ID: freq_offset
Value: 0

Variable
ID: centerfreq_0
Value: 868.42M

File Source
File: ...er/Desktop/zwave.bin
Repeat: Yes

Throttle
Sample Rate: 800k

QT GUI Frequency Sink
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 800k

```
Showing: ""

Generating: '/home/tzillner/Desktop/top_block.py'

Executing: /usr/bin/python2 -u /home/tzillner/Desktop/top_block.py

Using Volk machine: avx2_64_mmx
```

Top Block

Trace Options
☐ Max Hold
☐ Min Hold
Avg:

Axis Options
☐ Grid
☐ Axis Labels
Y Range: + -
Ref Level: + -
Autoscale

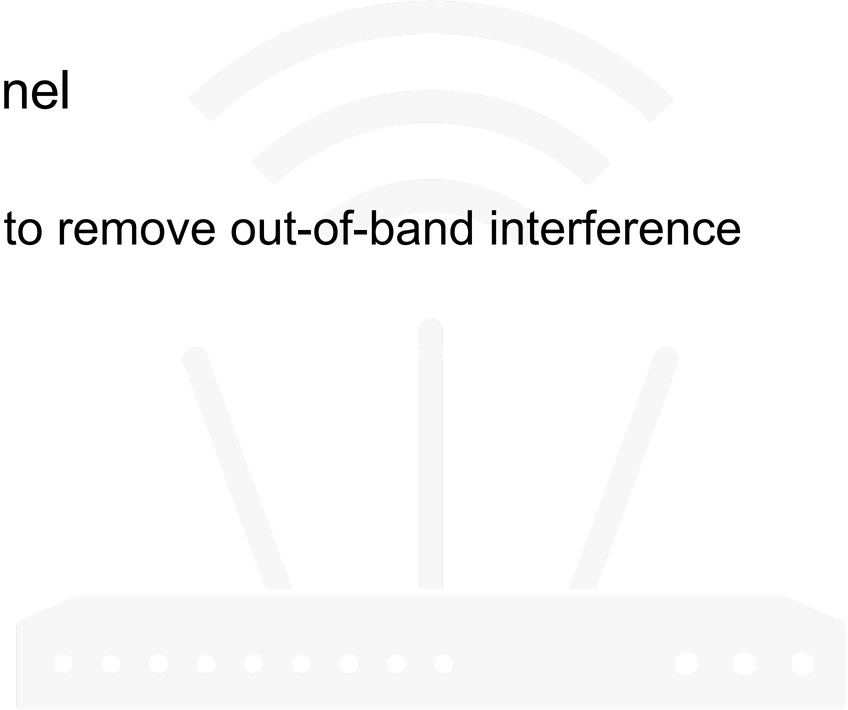
FFT
1024
Blackman-harris

Trigger
Free
Level: + -

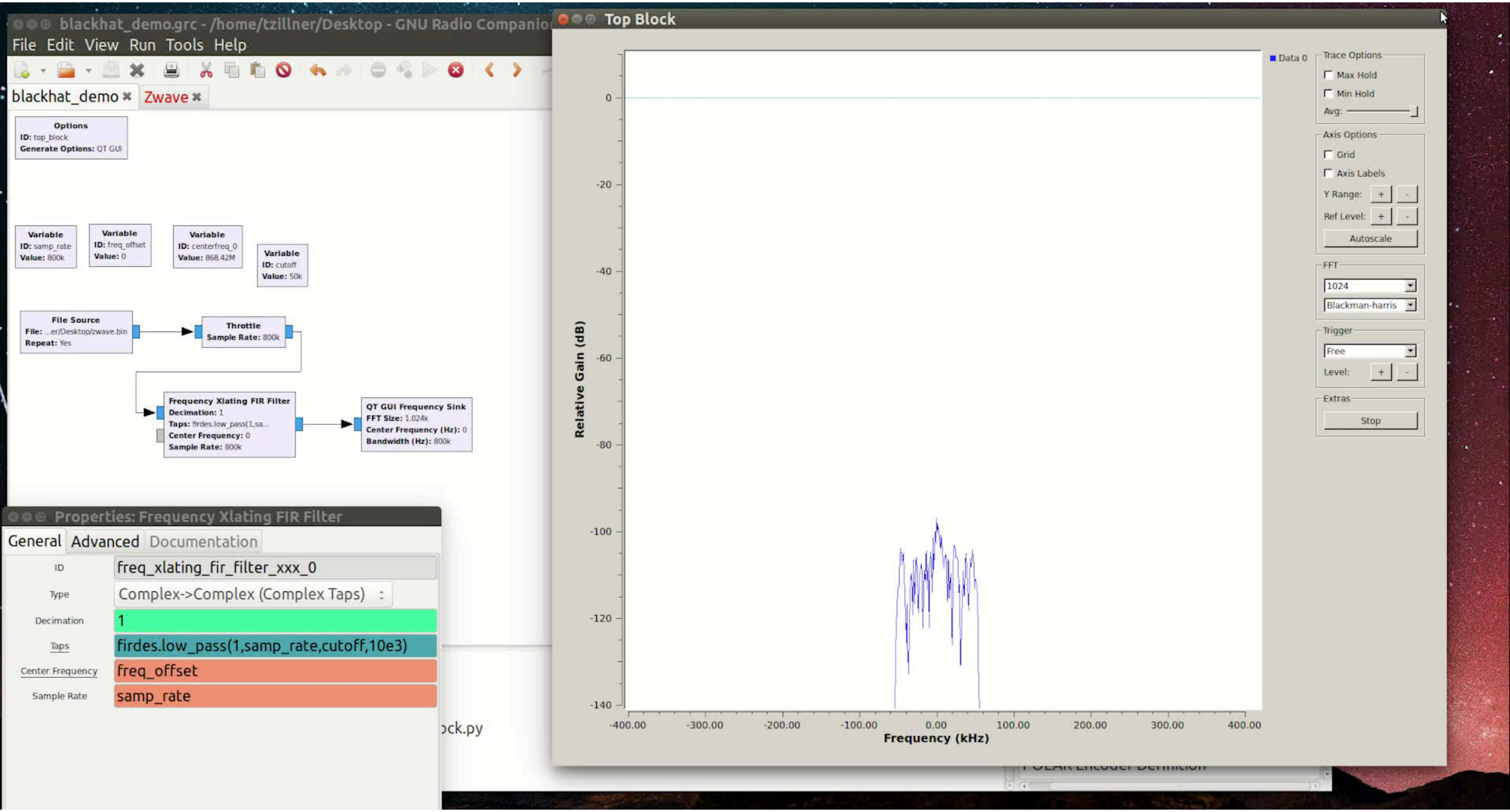
Extras
Stop

SIGNAL TO BITS

- Find the data channel
- Isolate the channel
  - Use filters to remove out-of-band interference



ISOLATE THE CHANNEL



blackhat_demo.grc - /home/tzillner/Desktop - GNU Radio Companion

File Edit View Run Tools Help

blackhat_demo ✖ Zwave ✖

Options
ID: top_block
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 800k

Variable
ID: freq_offset
Value: 0

Variable
ID: centerfreq_0
Value: 868.42M

Variable
ID: cutoff
Value: 50k

File Source
File: ...er/Desktop/zwave.bin
Repeat: Yes

Throttle
Sample Rate: 800k

Frequency Xlating FIR Filter
Decimation: 1
Taps: firdes.low_pass(1,sa...
Center Frequency: 0
Sample Rate: 800k

QT GUI Frequency Sink
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 800k

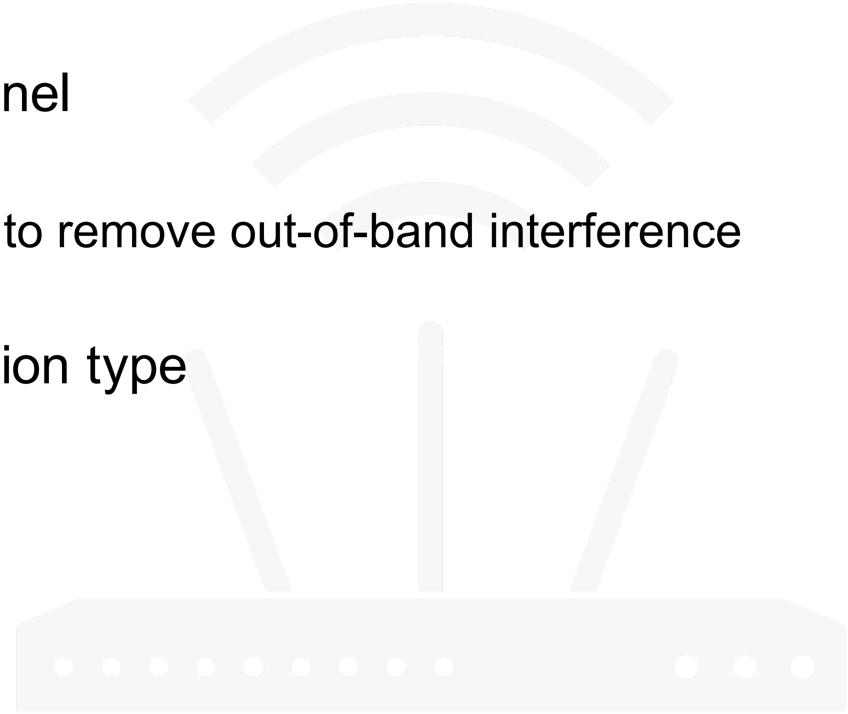
Properties: Frequency Xlating FIR Filter

General | Advanced | Documentation

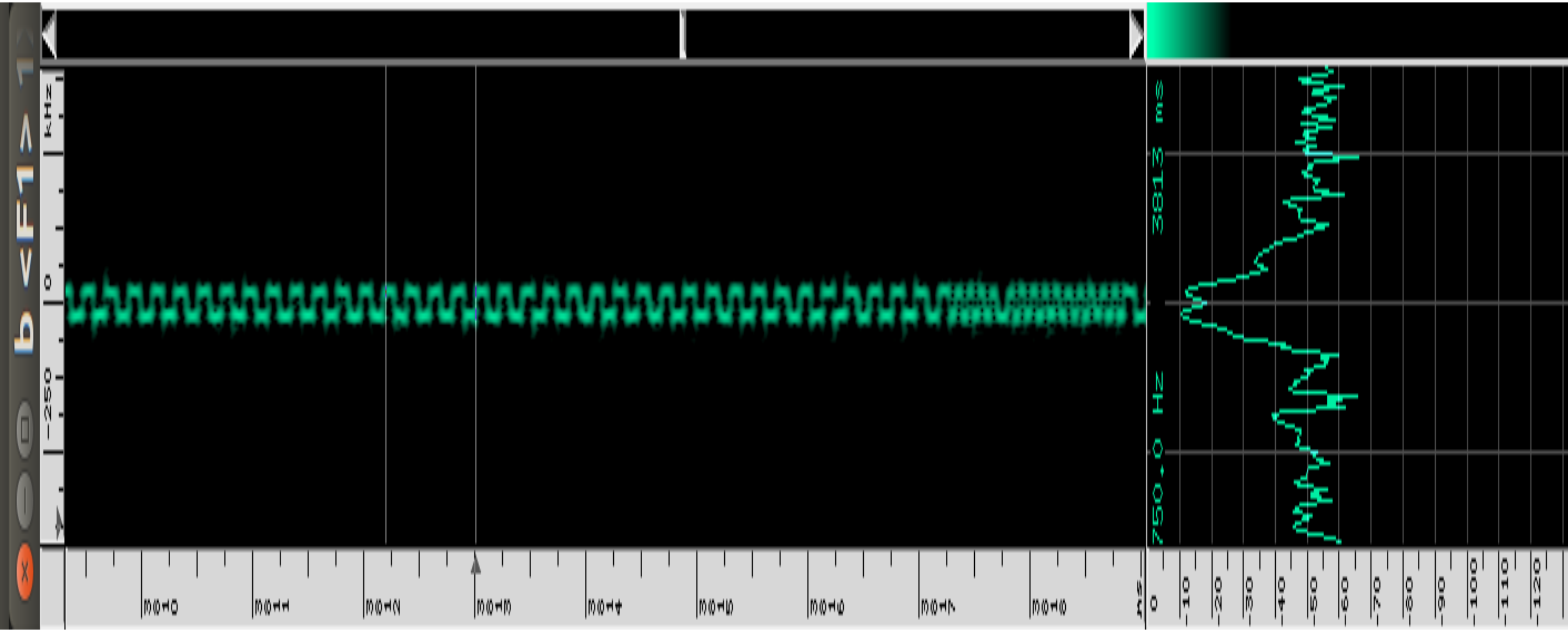
ID	freq_xlating_fir_filter_xxx_0
Type	Complex->Complex (Complex Taps)
Decimation	1
Taps	firdes.low_pass(1,samp_rate,cutoff,10e3)
Center Frequency	freq_offset
Sample Rate	samp_rate

SIGNAL TO BITS

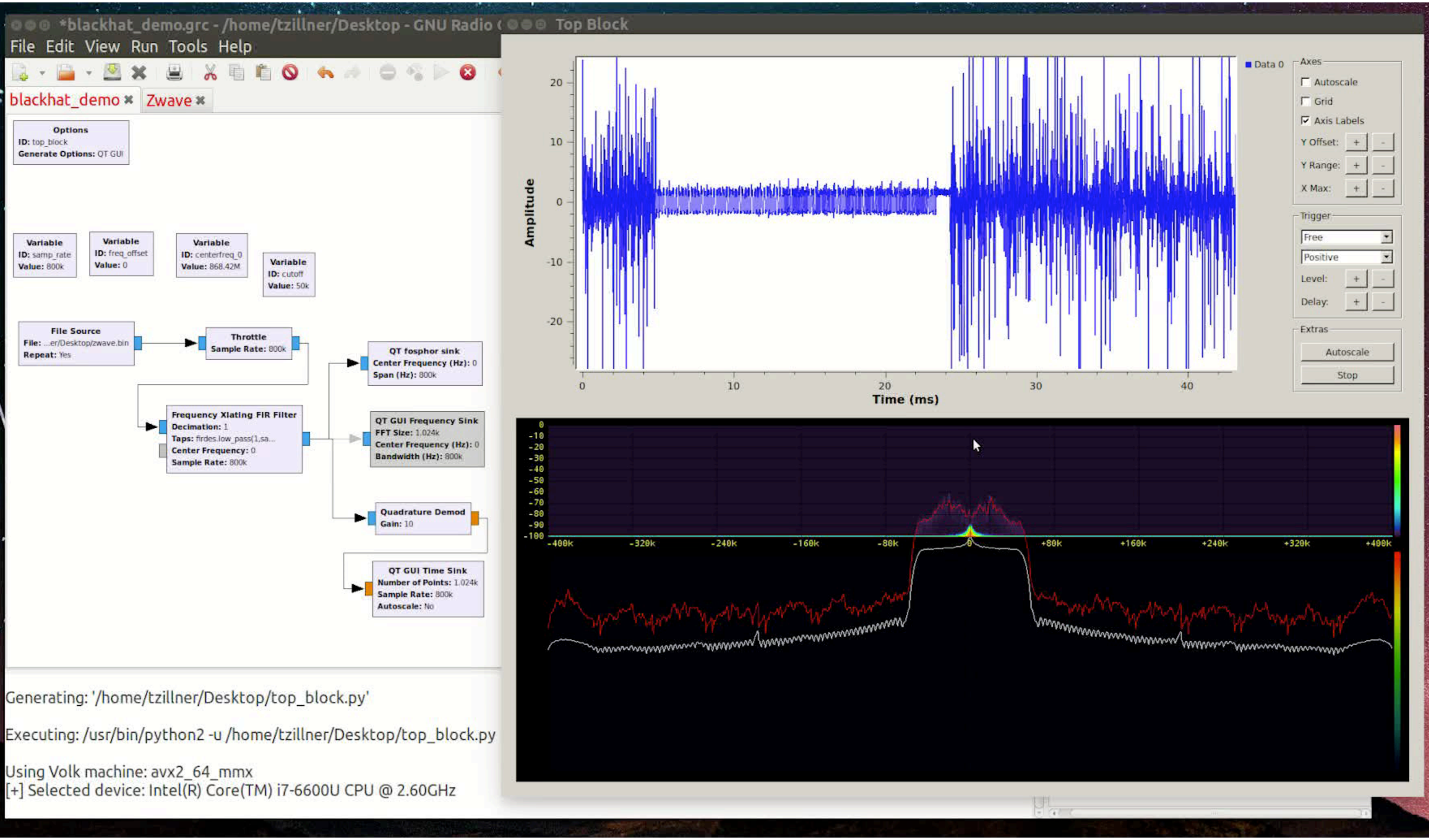
- Find the data channel
- Isolate the channel
  - Use filters to remove out-of-band interference
- Identify modulation type



MODULATION TYPE



MODULATION TYPE



Options
ID: top_block
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 800k

Variable
ID: freq_offset
Value: 0

Variable
ID: centerfreq_0
Value: 868.42M

Variable
ID: cutoff
Value: 50k

File Source
File: ...er/Desktop/zwave.bin
Repeat: Yes

Throttle
Sample Rate: 800k

QT fosphor sink
Center Frequency (Hz): 0
Span (Hz): 800k

Frequency Xlating FIR Filter
Decimation: 1
Taps: firdes.low_pass(1,sa...
Center Frequency: 0
Sample Rate: 800k

QT GUI Frequency Sink
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 800k

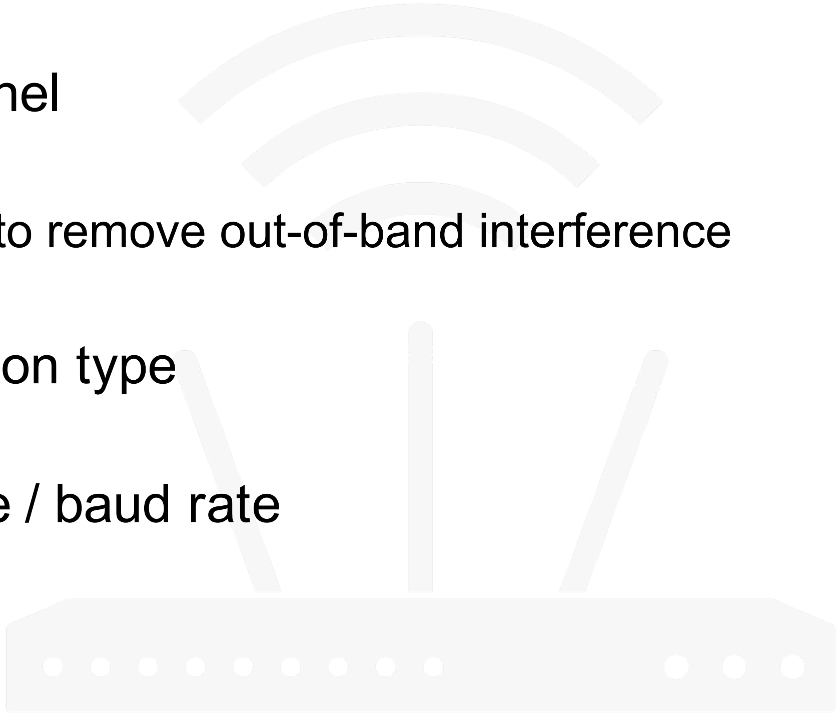
Quadrature Demod
Gain: 10

QT GUI Time Sink
Number of Points: 1.024k
Sample Rate: 800k
Autoscale: No

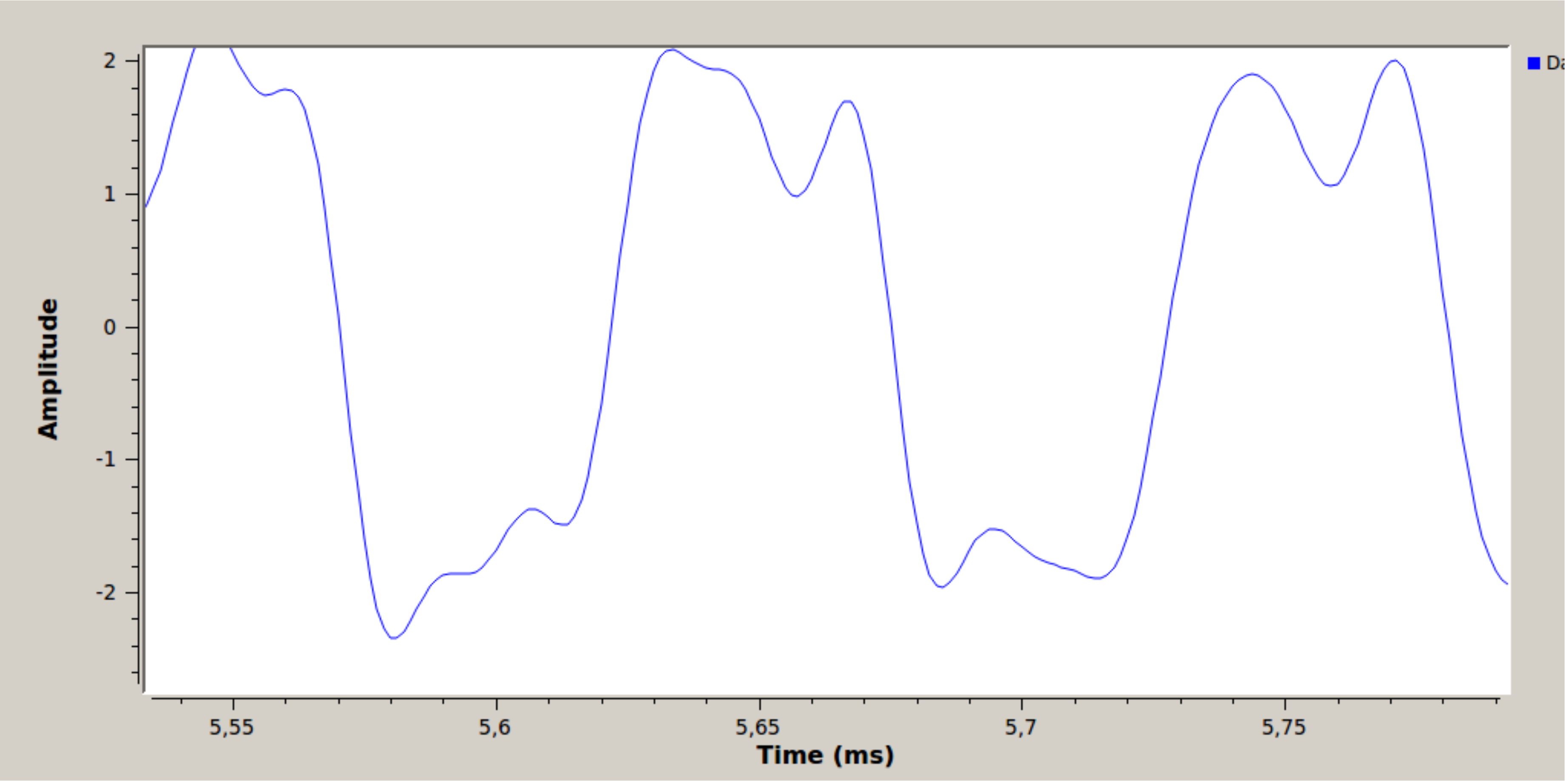
```
Generating: '/home/tzillner/Desktop/top_block.py'

Executing: /usr/bin/python2 -u /home/tzillner/Desktop/top_block.py

Using Volk machine: avx2_64_mmx
[+] Selected device: Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz
```

SIGNAL TO BITS

- Find the data channel
- Isolate the channel
  - Use filters to remove out-of-band interference
- Identify modulation type
- Identify data rate / baud rate

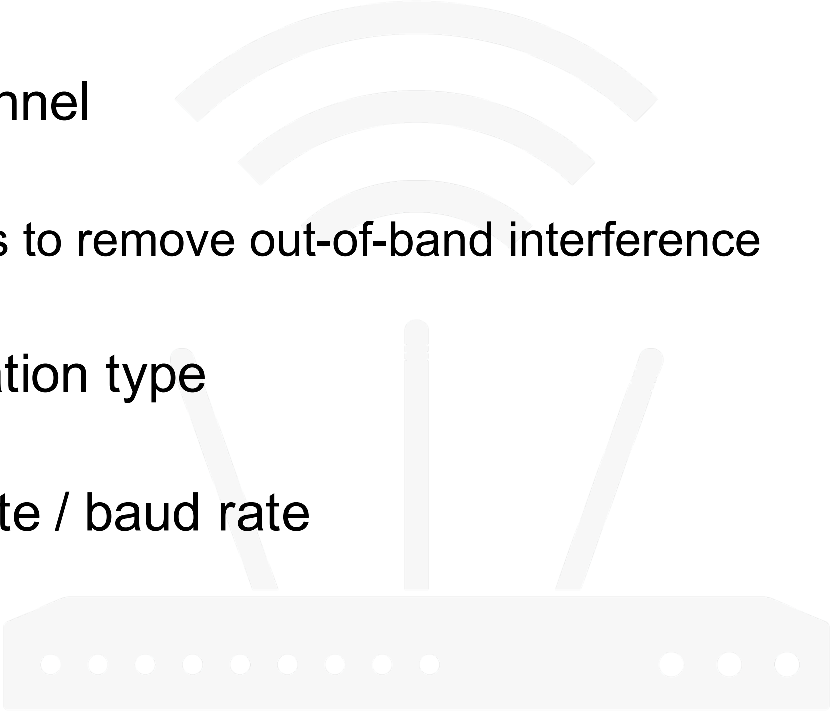


IDENTIFY DATA RATE / BAUD RATE

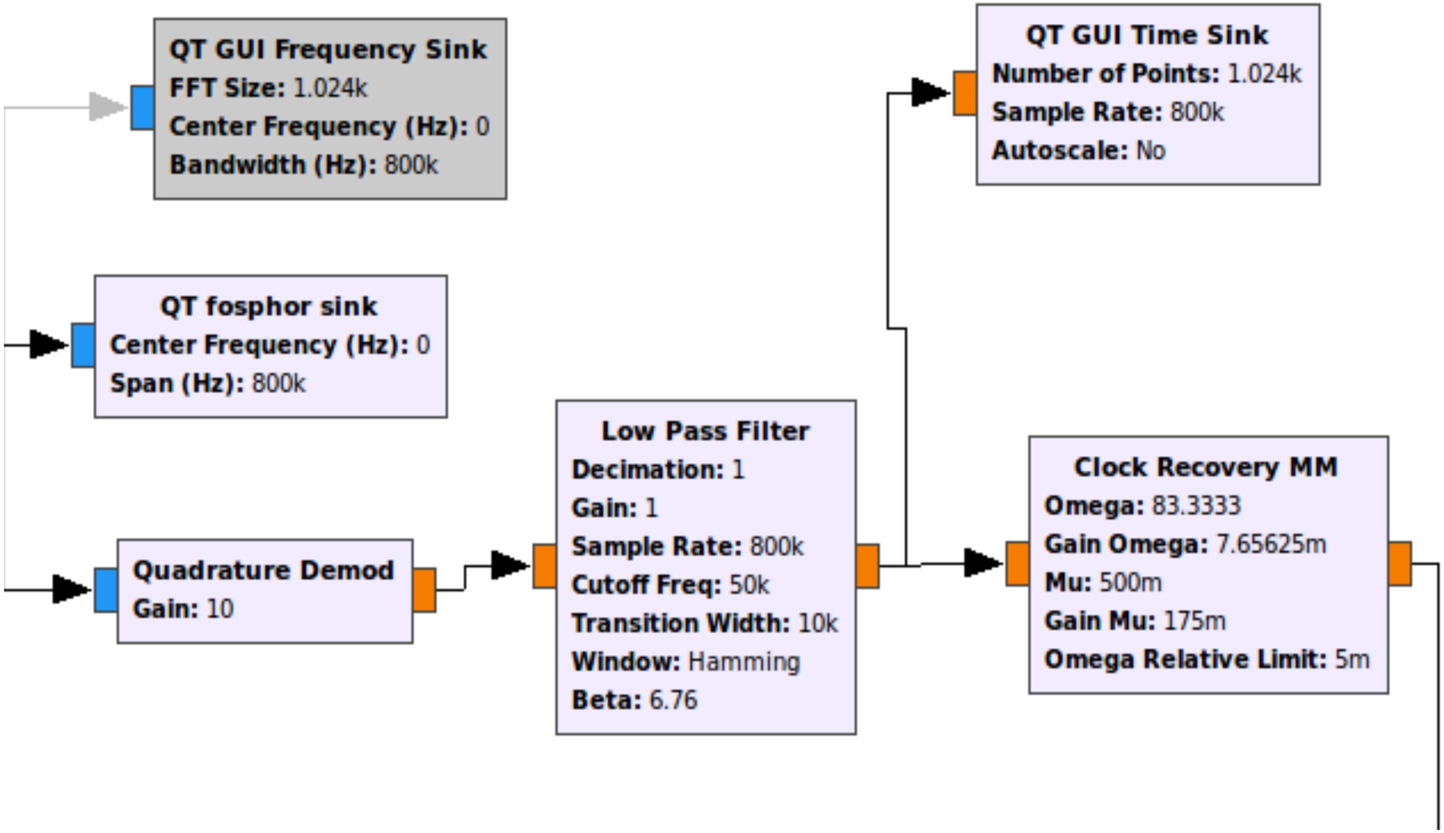


SIGNAL TO BITS

- Find the data channel
- Isolate the channel
  - Use filters to remove out-of-band interference
- Identify modulation type
- Identify data rate / baud rate
- Clock recovery



CLOCK RECOVERY



QT GUI Frequency Sink
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 800k

QT fosphor sink
Center Frequency (Hz): 0
Span (Hz): 800k

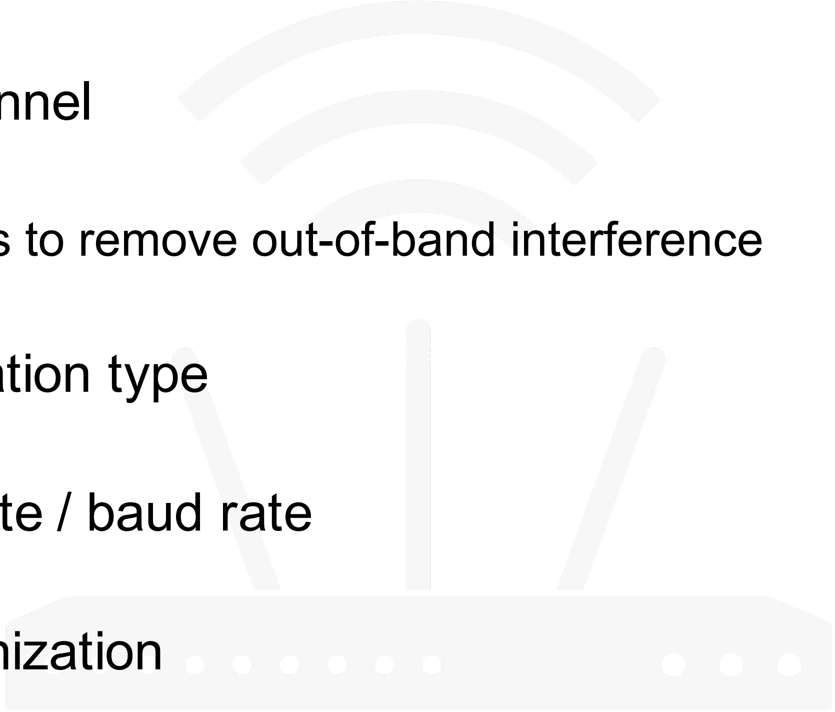
Quadrature Demod
Gain: 10

Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 800k
Cutoff Freq: 50k
Transition Width: 10k
Window: Hamming
Beta: 6.76

QT GUI Time Sink
Number of Points: 1.024k
Sample Rate: 800k
Autoscale: No

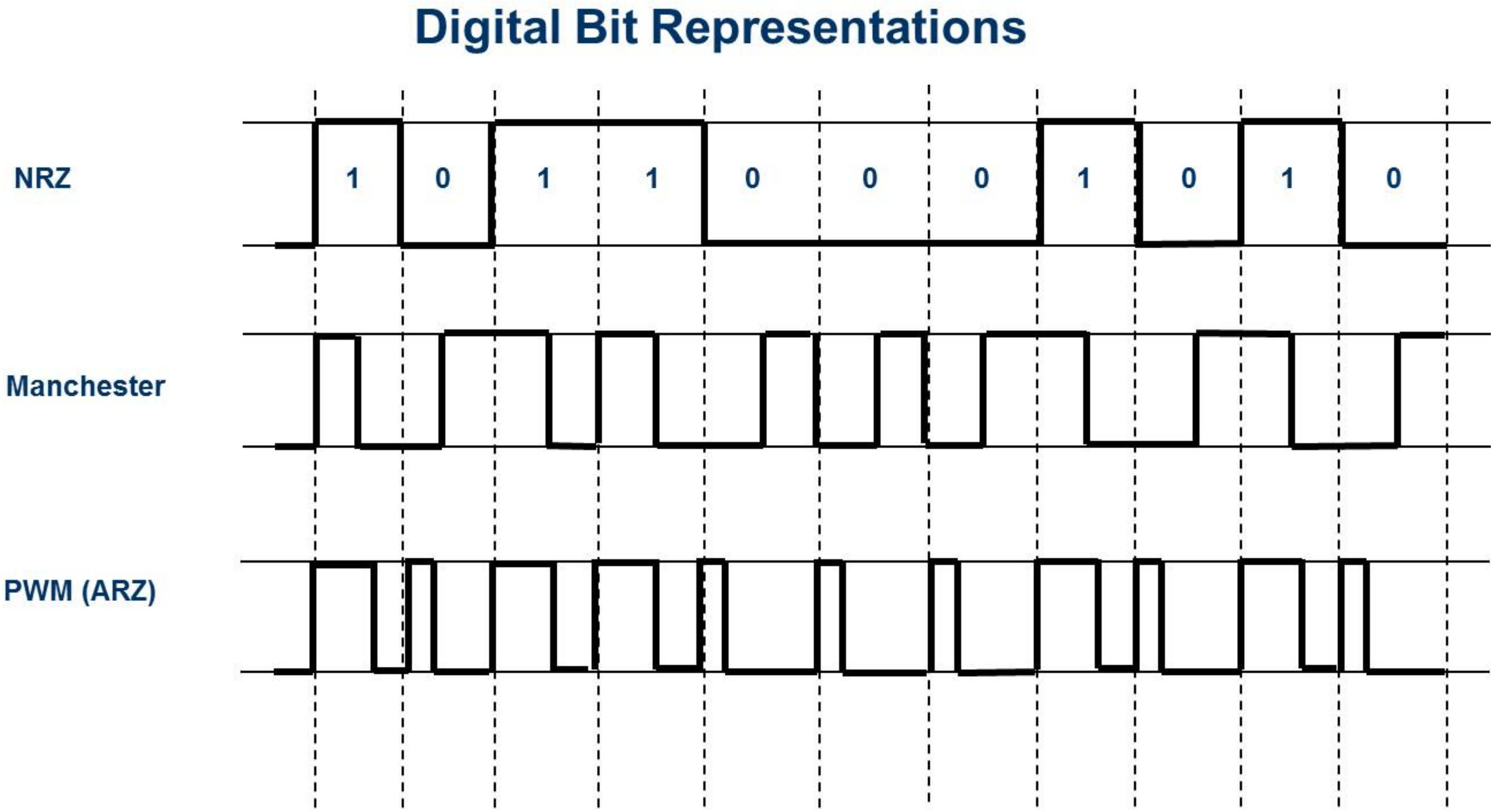
Clock Recovery MM
Omega: 83.3333
Gain Omega: 7.65625m
Mu: 500m
Gain Mu: 175m
Omega Relative Limit: 5m

SIGNAL TO BITS



- Find the data channel
- Isolate the channel
  - Use filters to remove out-of-band interference
- Identify modulation type
- Identify data rate / baud rate
- Clock synchronization
- Symbols to logical bits

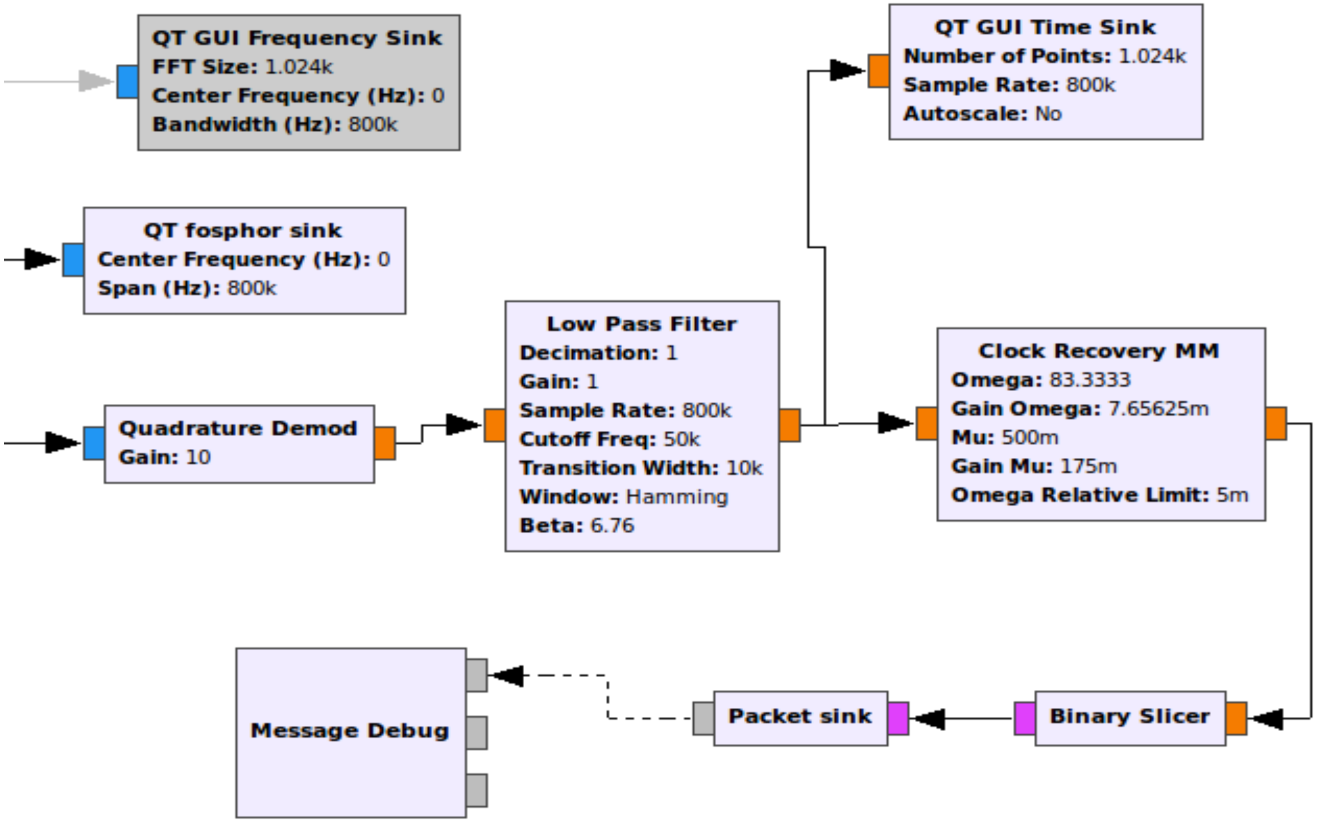
ENCODINGS


Digital Bit Representations
NRZ
1
0
1
1
0
0
0
1
0
1
0
Manchester
PWM (ARZ)

RAW OUTPUT TO PACKETS

- Analyse output structure
  - Pattern search
  - SOF / EOF
  - Long sequences of 0‘s or 1‘s
- Search for known values
  - Serials, Names, Ids,…
- Search for repeating changes
  - Counters, Sequence numbers, packet length
- Checksums
- Error correction and detection

PACKET SNIFFING



QT GUI Frequency Sink
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 800k

QT fosphor sink
Center Frequency (Hz): 0
Span (Hz): 800k

Quadrature Demod
Gain: 10

Low Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 800k
Cutoff Freq: 50k
Transition Width: 10k
Window: Hamming
Beta: 6.76

QT GUI Time Sink
Number of Points: 1.024k
Sample Rate: 800k
Autoscale: No

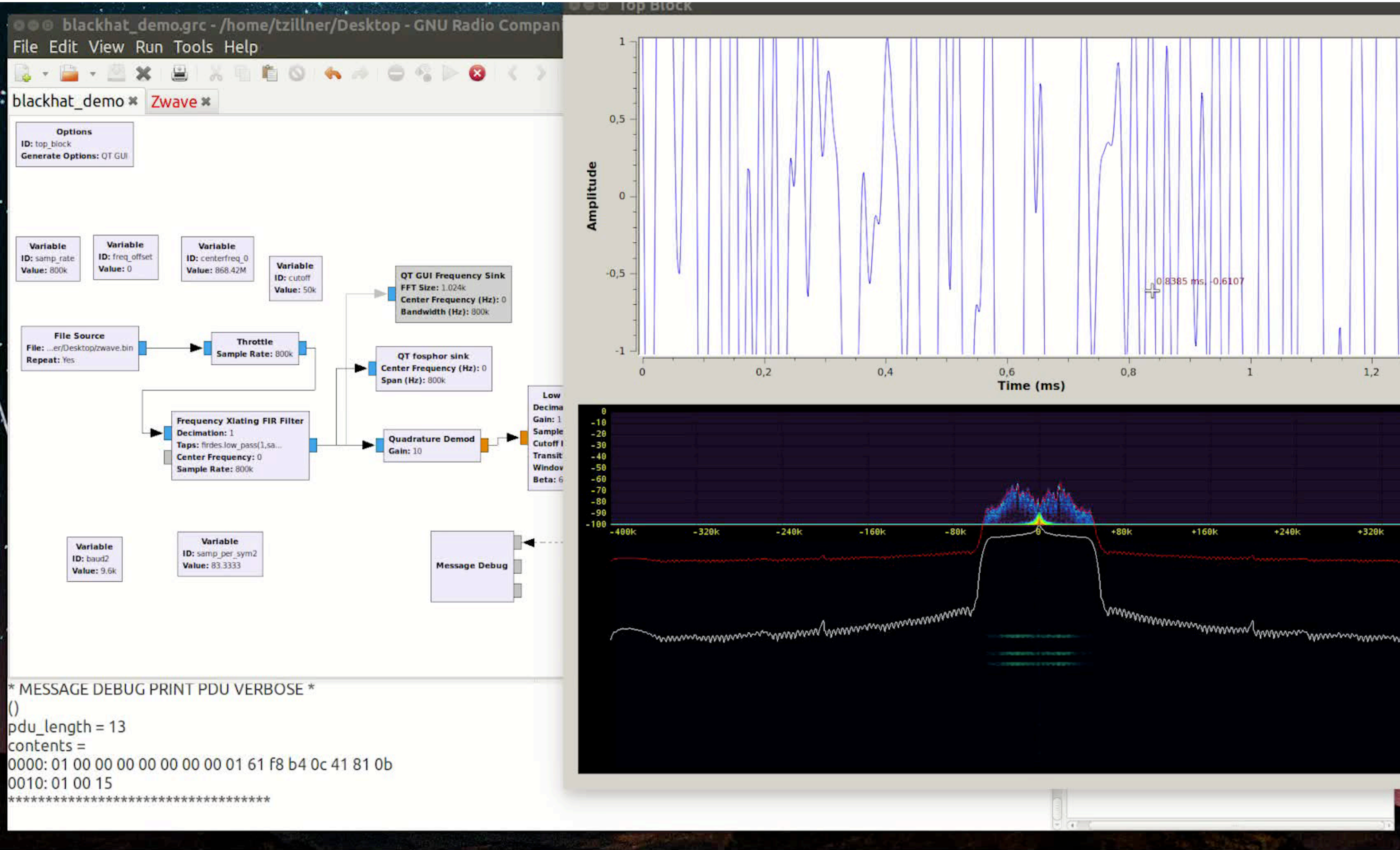
Clock Recovery MM
Omega: 83.3333
Gain Omega: 7.65625m
Mu: 500m
Gain Mu: 175m
Omega Relative Limit: 5m

Binary Slicer

Packet sink

Message Debug

DATA EXTRACTION



Options
ID: top_block
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 800k

Variable
ID: freq_offset
Value: 0

Variable
ID: centerfreq_0
Value: 868.42M

Variable
ID: cutoff
Value: 50k

QT GUI Frequency Sink
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 800k

File Source
File: ...er/Desktop/zwave.bin
Repeat: Yes

Throttle
Sample Rate: 800k

QT fosphor sink
Center Frequency (Hz): 0
Span (Hz): 800k

Frequency Xlating FIR Filter
Decimation: 1
Taps: firdes.low_pass(1,sa...
Center Frequency: 0
Sample Rate: 800k

Quadrature Demod
Gain: 10

Low
Decima
Gain: 1
Sample
Cutoff I
Transit
Windov
Beta: 6

Variable
ID: baud2
Value: 9.6k

Variable
ID: samp_per_sym2
Value: 83.3333

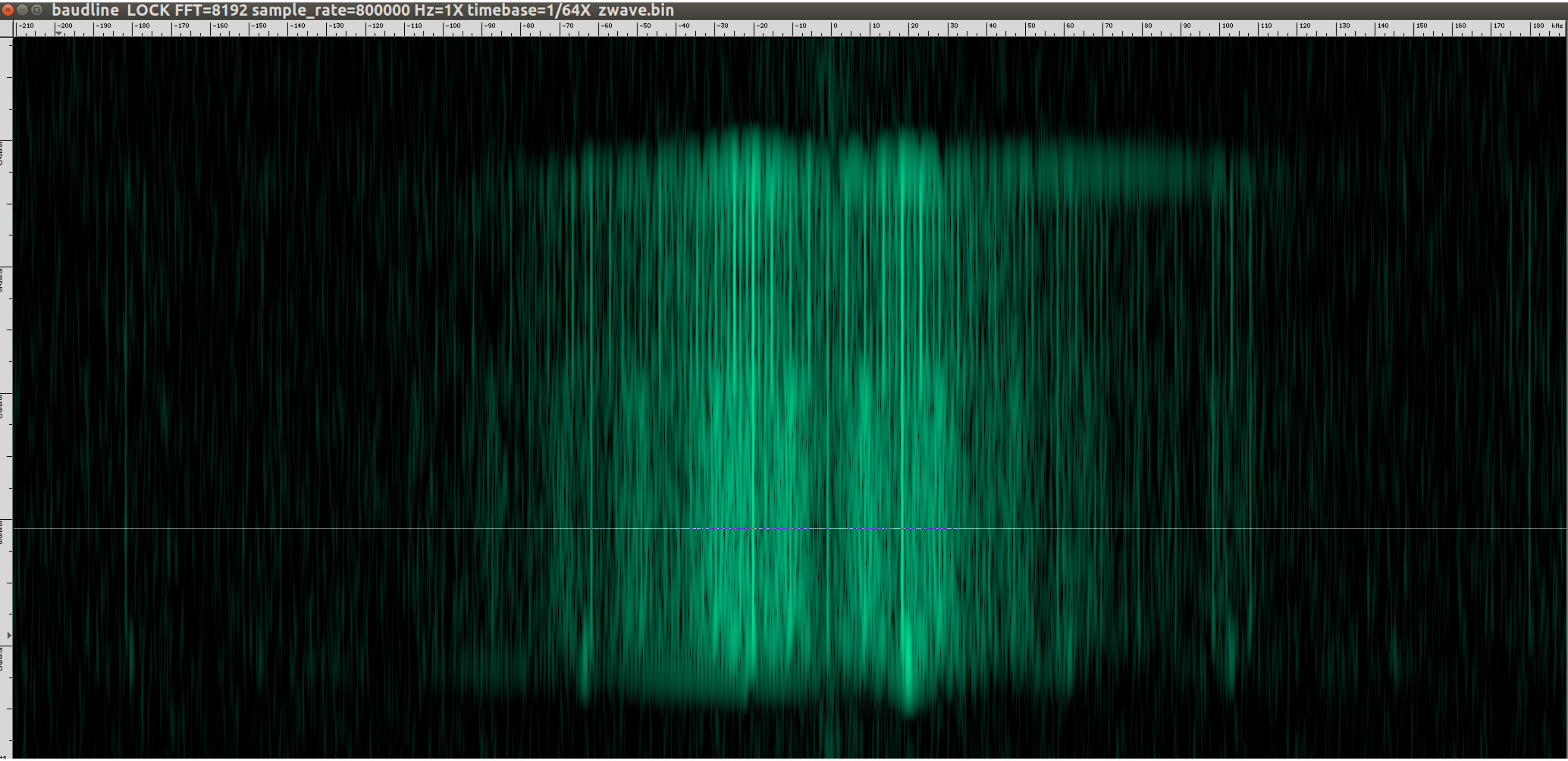
Message Debug

```
* MESSAGE DEBUG PRINT PDU VERBOSE *
()
pdu_length = 13
contents =
0000: 01 00 00 00 00 00 00 00 01 61 f8 b4 0c 41 81 0b
0010: 01 00 15
***********************************
```

PITFALLS

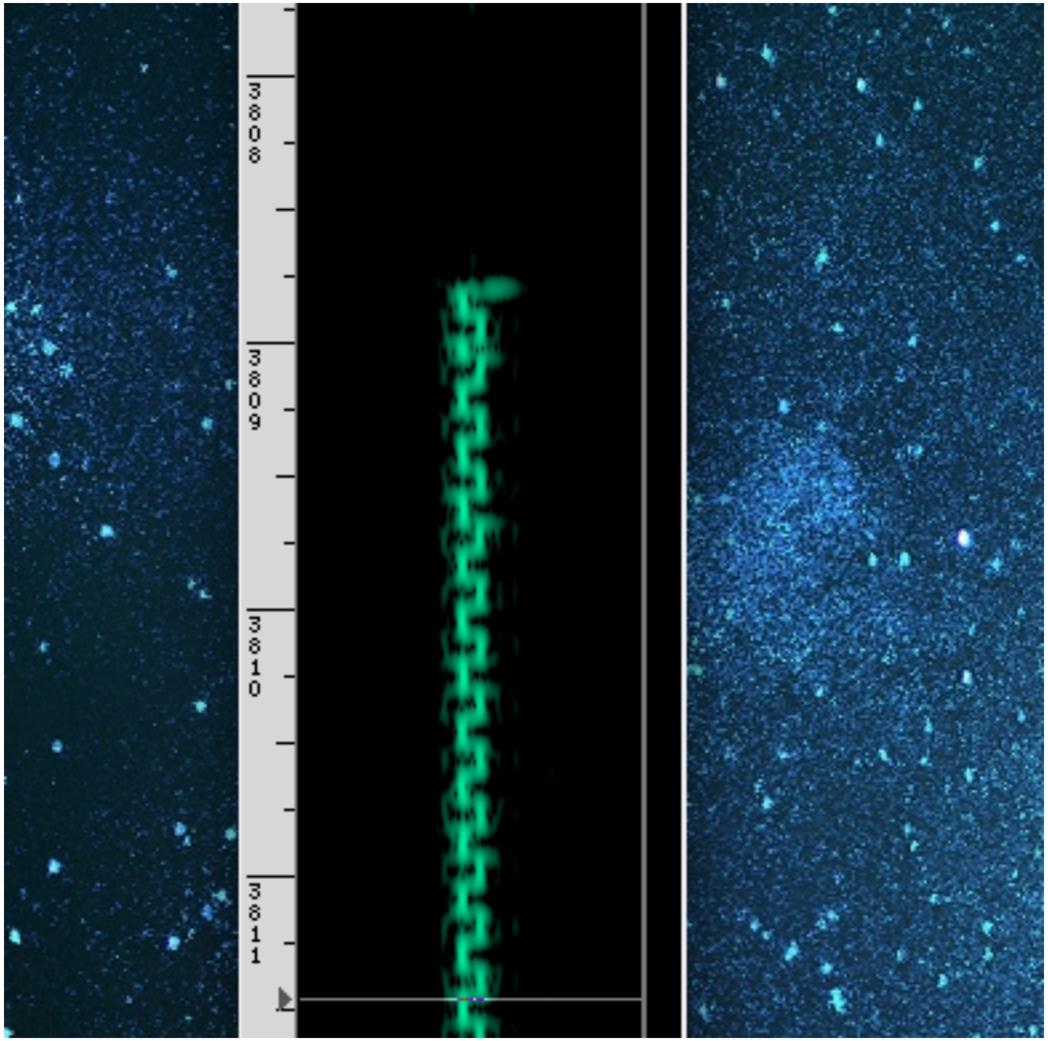
- Get familiar with RF / SDR / DSP basics
  - Modualtion
  - Sampling
  - Complex Numbers
- Store meta data
  - capture rate, gain, frequency
- Choose a proper RF gain
- Know your tools
  - Visual resolution problems

BAUDLINE FFT=8192



baudline LOCK FFT=8192 sample_rate=800000 Hz=1X timebase=1/64X zwave.bin

BAUDLINE FFT=256



PITFALLS

- Analysing the wrong signal
  - Move around to see how signal strength changes
  - Make sure your signal is in band and not an alias
- Check for timing issues
  - Clock recovery
  - Send messages within timeframes

INTERESTING RESOURCES AND PROJECTS

- Defcon Wireless / IoT Village
- Cyberspectrum Meetups
  - Also available on Youtube
- Wikipedia (RF theory)
- OWASP IoT Top 10

- Other Resources

http://greatscottgadgets.com/sdr/

http://files.ettus.com/tutorials/labs/Lab_1-5.pdf

http://sdr.ninja/additional-resouces/

https://www.youtube.com/user/Hak5Darren

https://www.youtube.com/user/balint256

LET'S SEE WHAT'S OUT THERE - MAPPING THE WIRELESS IOT

WIRELESS SECURITY ISSUES

WIRELESS IOT TOP 10 ISSUES

- Unencrypted communication
- No message freshness checks – Replay attacks
- Vulnerable key exchange
- Jamming
- Mixing unencrypted and encrypted communication

cognosec

WIRELESS IOT TOP 10 ISSUES

Weak Join/Pairing procedures

Hardcoded secrets

Weak cryptography

No message authentication - Spoofing

Insecure rejoin procedure

cognosec

LET’S SEE WHAT’S OUT THERE - MAPPING THE WIRELESS IOT

DEVICE DISCOVERY

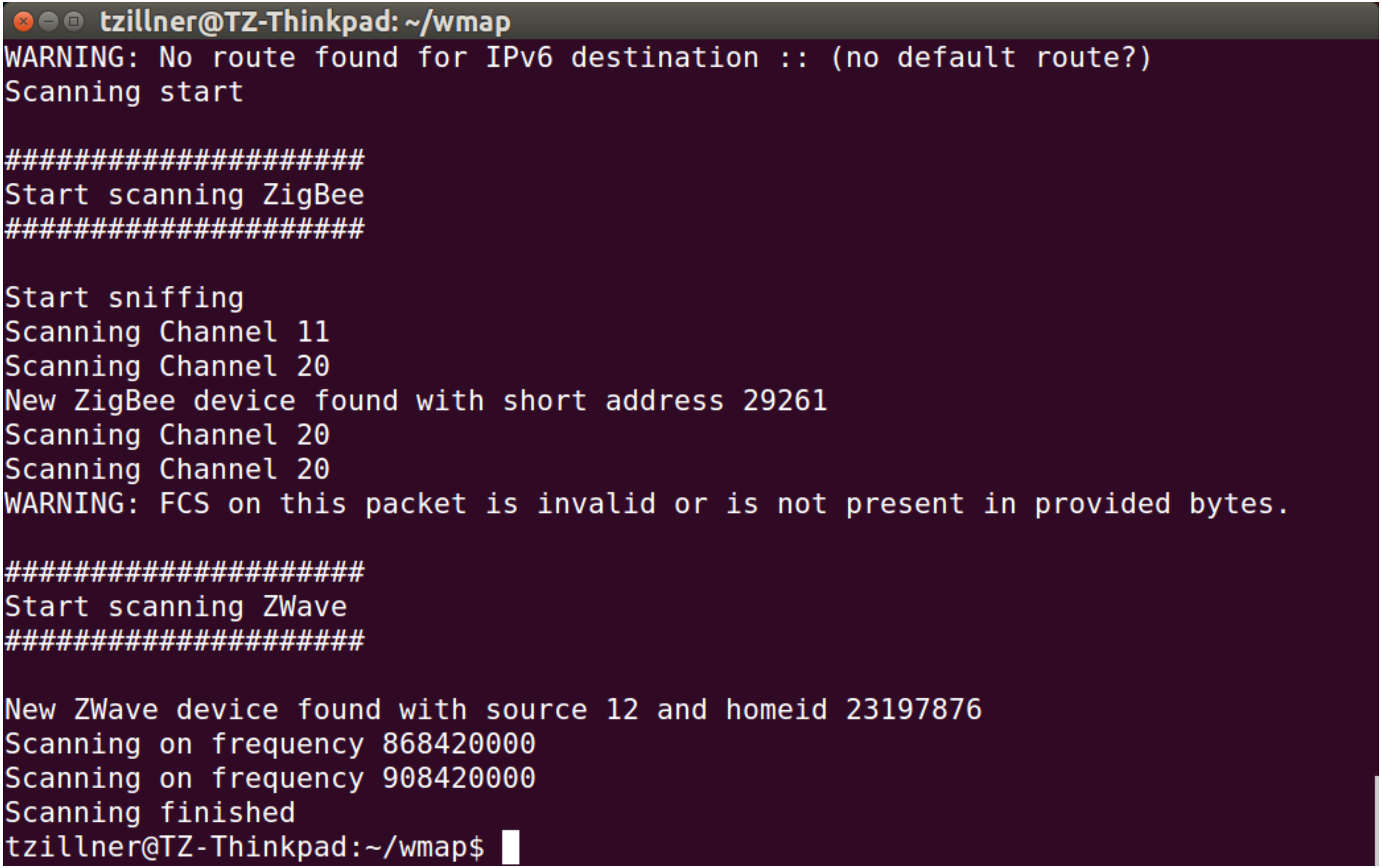
DEMONSTRATION

cognosec

WMAP

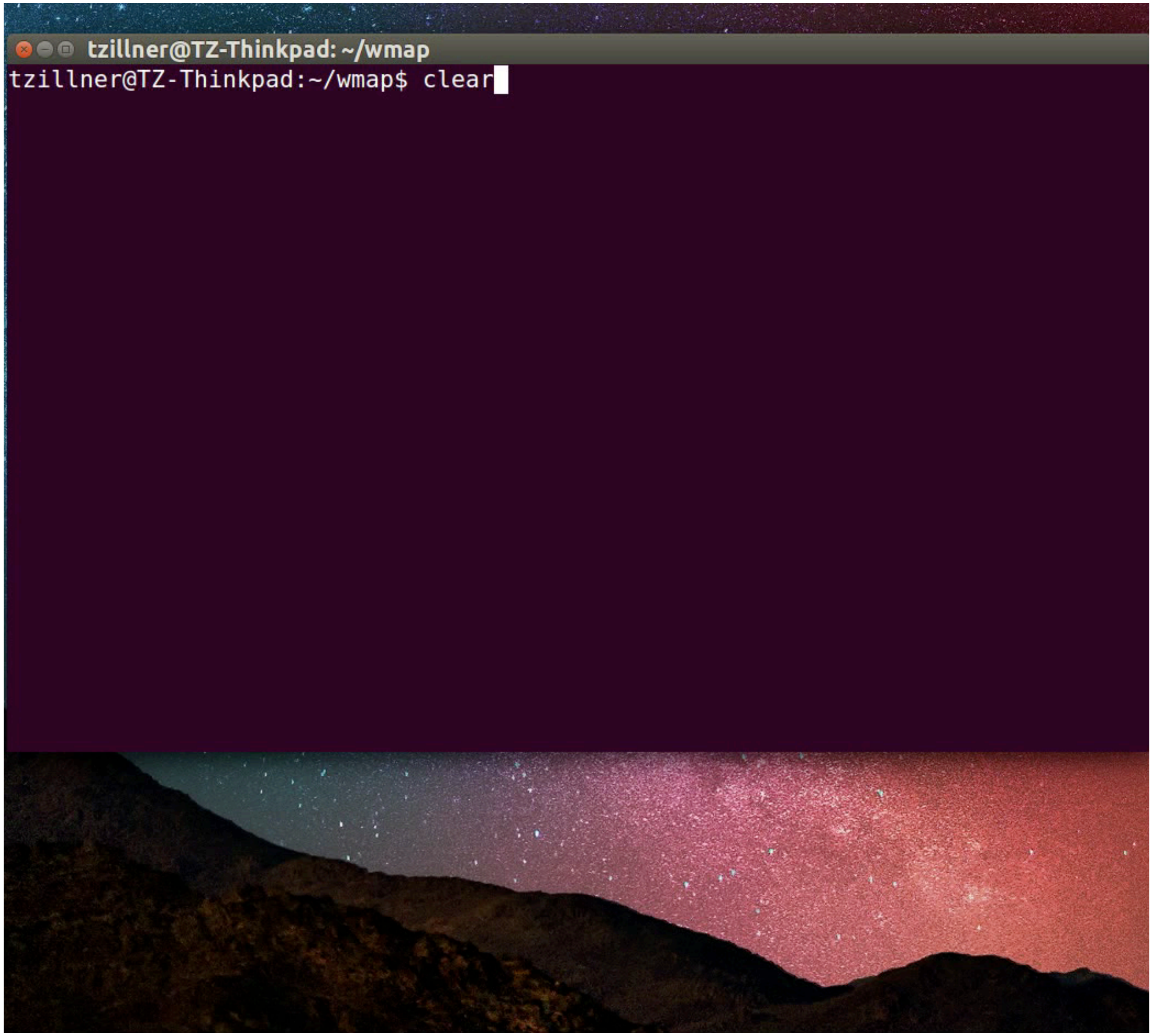
- Wireless IoT device scanner
- Based on Scapy Radio
- Scans RF for wireless communication
  - All channels / protocol
  - Quick Scan / preferred channels
- Easy expendability
- Passive / Active scanning

HOTEL TEST RESULTS



```
WARNING: No route found for IPv6 destination :: (no default route?)
Scanning start

#####################
Start scanning ZigBee
#####################

Start sniffing
Scanning Channel 11
Scanning Channel 20
New ZigBee device found with short address 29261
Scanning Channel 20
Scanning Channel 20
WARNING: FCS on this packet is invalid or is not present in provided bytes.

#####################
Start scanning ZWave
#####################

New ZWave device found with source 12 and homeid 23197876
Scanning on frequency 868420000
Scanning on frequency 908420000
Scanning finished
tzillner@TZ-Thinkpad:~/wmap$ █
```

WMAP SCAN



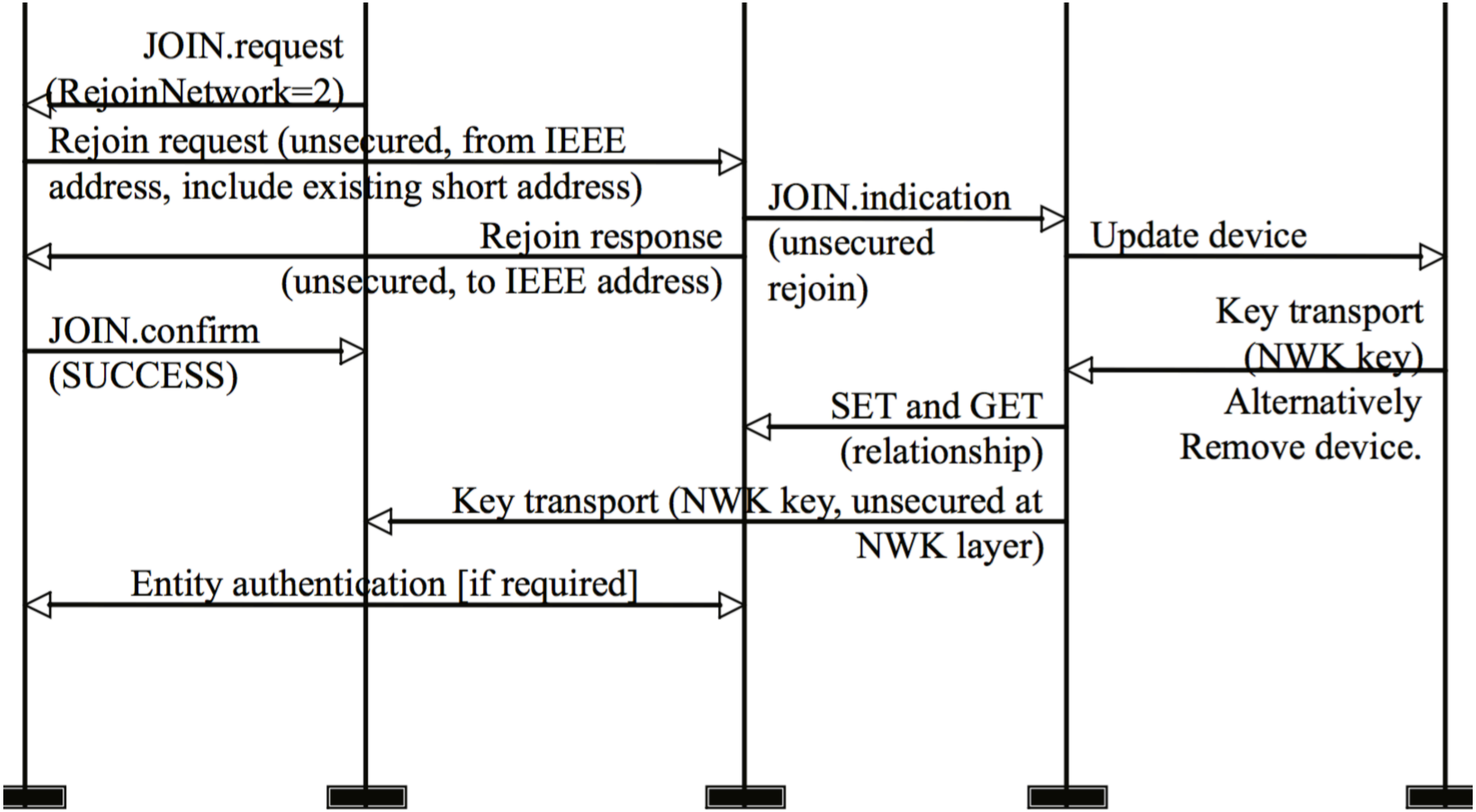
```
tzillner@TZ-Thinkpad:~/wmap$ clear
```

LET'S SEE WHAT'S OUT THERE - MAPPING THE WIRELESS IOT

REJOIN TESTING DEMONSTRATION

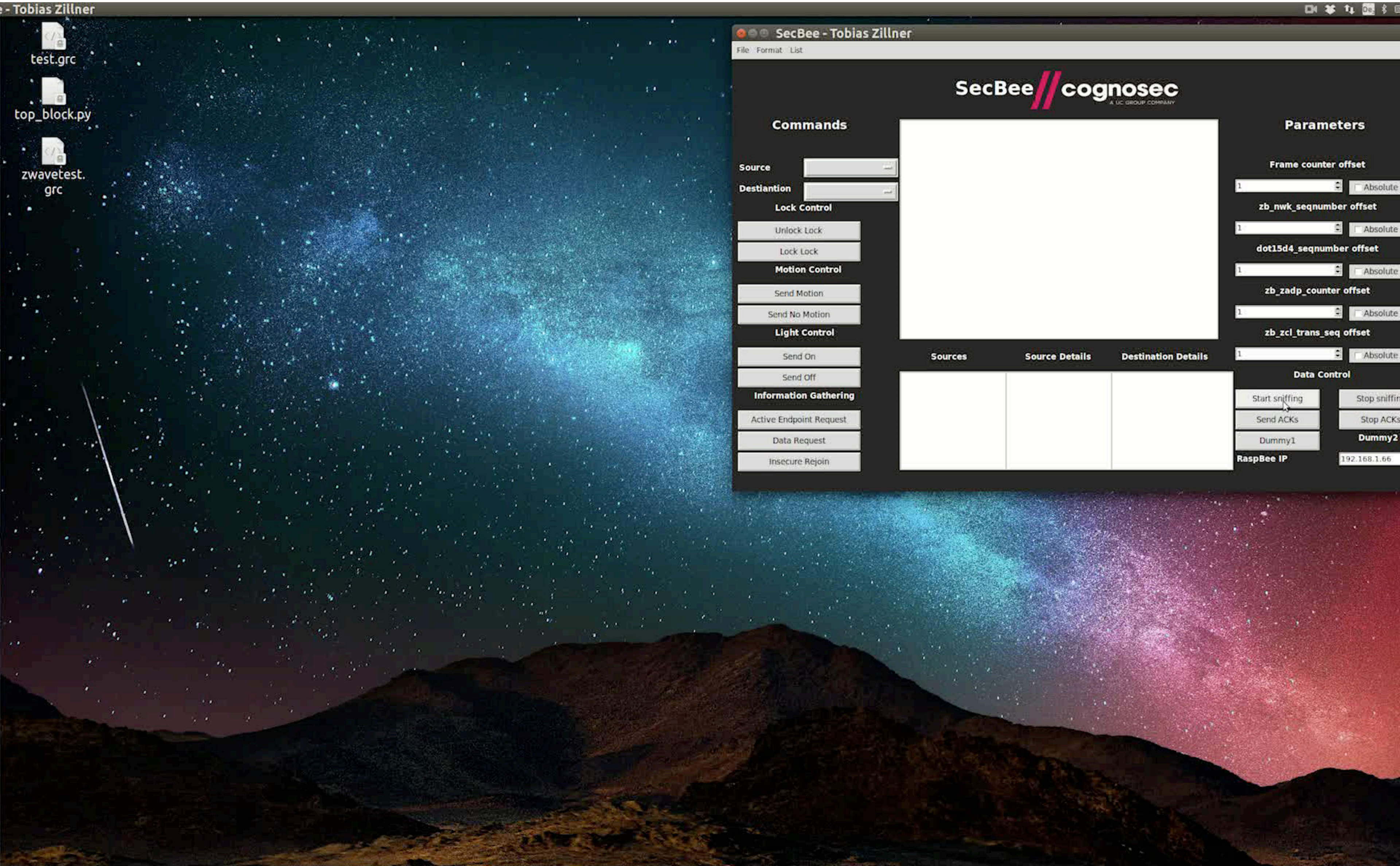
//cognosec

ZIGBEE INSECURE REJOIN


JOIN.request (RejoinNetwork=2)
Rejoin request (unsecured, from IEEE address, include existing short address)
JOIN.indication (unsecured rejoin)
Update device
Rejoin response (unsecured, to IEEE address)
Key transport (NWK key)
Alternatively Remove device.
JOIN.confirm (SUCCESS)
SET and GET (relationship)
Key transport (NWK key, unsecured at NWK layer)
Entity authentication [if required]

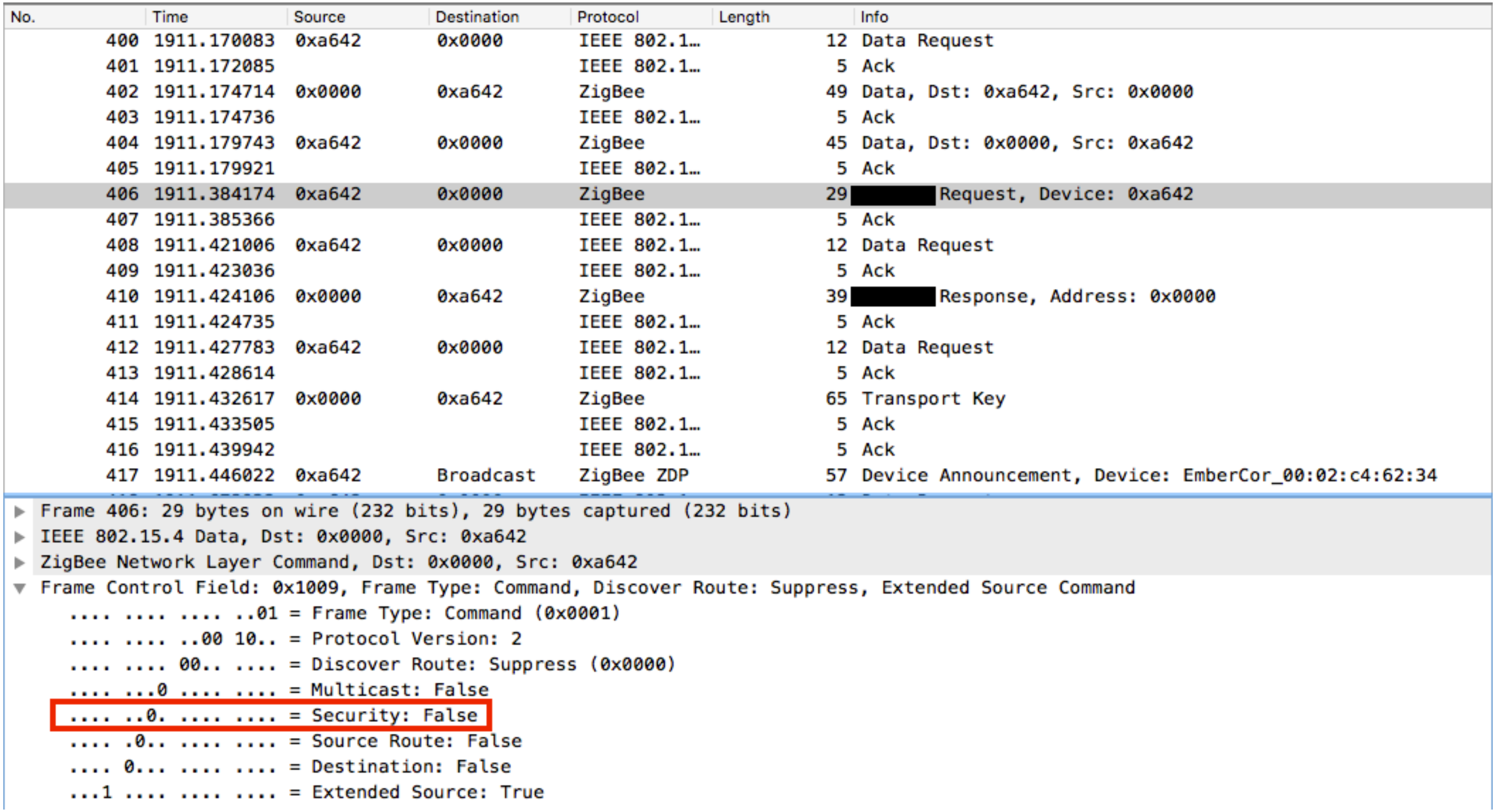
cognosec

VIDEO DEMO



Frame counter offset: 1
zb_nwk_seqnumber offset: 1
dot15d4_seqnumber offset: 1
zb_zadp_counter offset: 1
zb_zcl_trans_seq offset: 1
RaspBee IP: 192.168.1.66

ZIGBEE INSECURE REJOIN

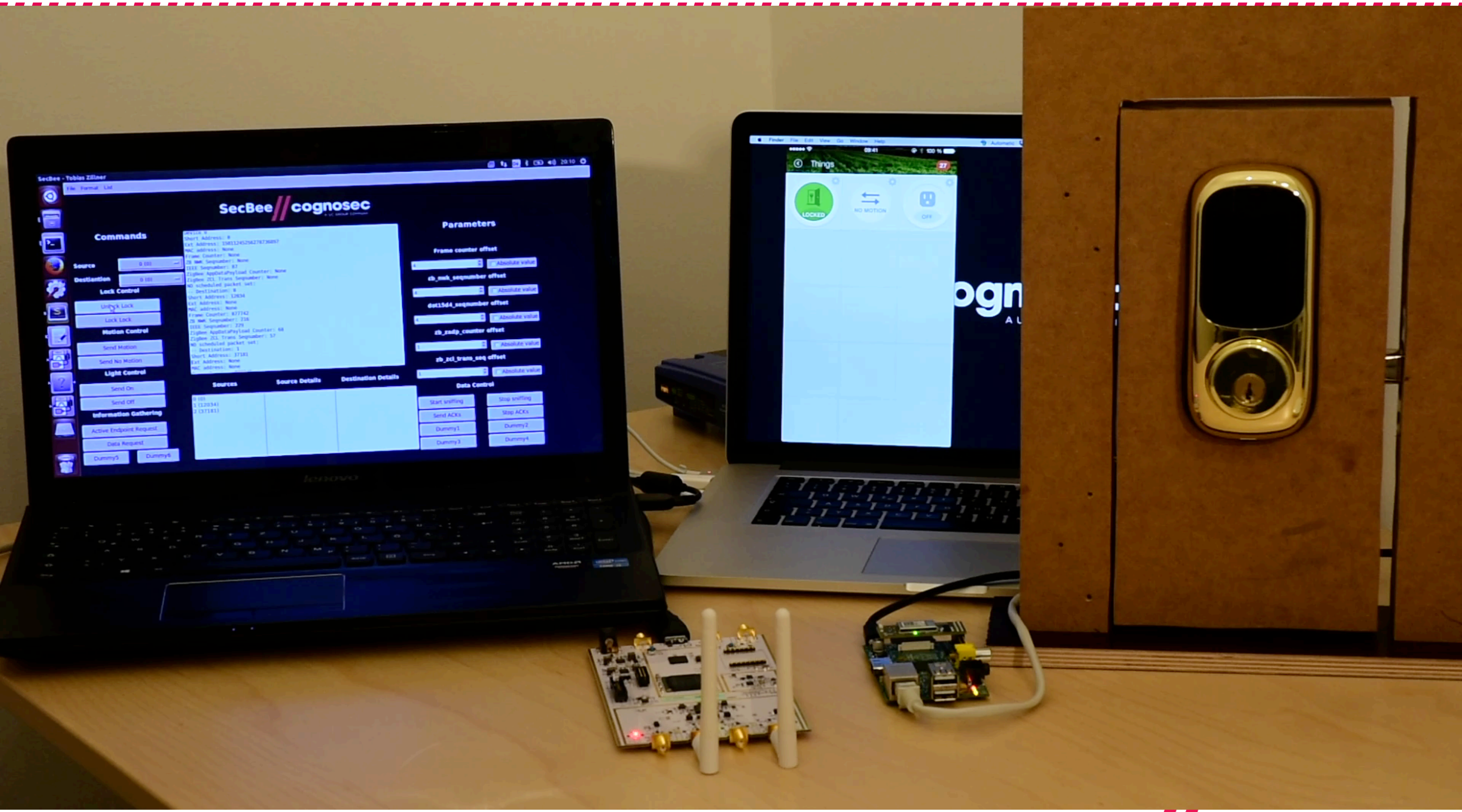


```
No.       Time          Source    Destination   Protocol        Length  Info
      400 1911.170083   0xa642    0x0000        IEEE 802.1…         12  Data Request
      401 1911.172085                           IEEE 802.1…          5  Ack
      402 1911.174714   0x0000    0xa642        ZigBee              49  Data, Dst: 0xa642, Src: 0x0000
      403 1911.174736                           IEEE 802.1…          5  Ack
      404 1911.179743   0xa642    0x0000        ZigBee              45  Data, Dst: 0x0000, Src: 0xa642
      405 1911.179921                           IEEE 802.1…          5  Ack
      406 1911.384174   0xa642    0x0000        ZigBee              29  [redacted] Request, Device: 0xa642
      407 1911.385366                           IEEE 802.1…          5  Ack
      408 1911.421006   0xa642    0x0000        IEEE 802.1…         12  Data Request
      409 1911.423036                           IEEE 802.1…          5  Ack
      410 1911.424106   0x0000    0xa642        ZigBee              39  [redacted] Response, Address: 0x0000
      411 1911.424735                           IEEE 802.1…          5  Ack
      412 1911.427783   0xa642    0x0000        IEEE 802.1…         12  Data Request
      413 1911.428614                           IEEE 802.1…          5  Ack
      414 1911.432617   0x0000    0xa642        ZigBee              65  Transport Key
      415 1911.433505                           IEEE 802.1…          5  Ack
      416 1911.439942                           IEEE 802.1…          5  Ack
      417 1911.446022   0xa642    Broadcast     ZigBee ZDP          57  Device Announcement, Device: EmberCor_00:02:c4:62:34
```

```
▶ Frame 406: 29 bytes on wire (232 bits), 29 bytes captured (232 bits)
▶ IEEE 802.15.4 Data, Dst: 0x0000, Src: 0xa642
▶ ZigBee Network Layer Command, Dst: 0x0000, Src: 0xa642
▼ Frame Control Field: 0x1009, Frame Type: Command, Discover Route: Suppress, Extended Source Command
    .... .... .... ..01 = Frame Type: Command (0x0001)
    .... .... ..00 10.. = Protocol Version: 2
    .... .... 00.. .... = Discover Route: Suppress (0x0000)
    .... ...0 .... .... = Multicast: False
    .... ..0. .... .... = Security: False
    .... .0.. .... .... = Source Route: False
    .... 0... .... .... = Destination: False
    ...1 .... .... .... = Extended Source: True
```

FEELINGS AFTER FIRST SUCCESSFUL JOIN

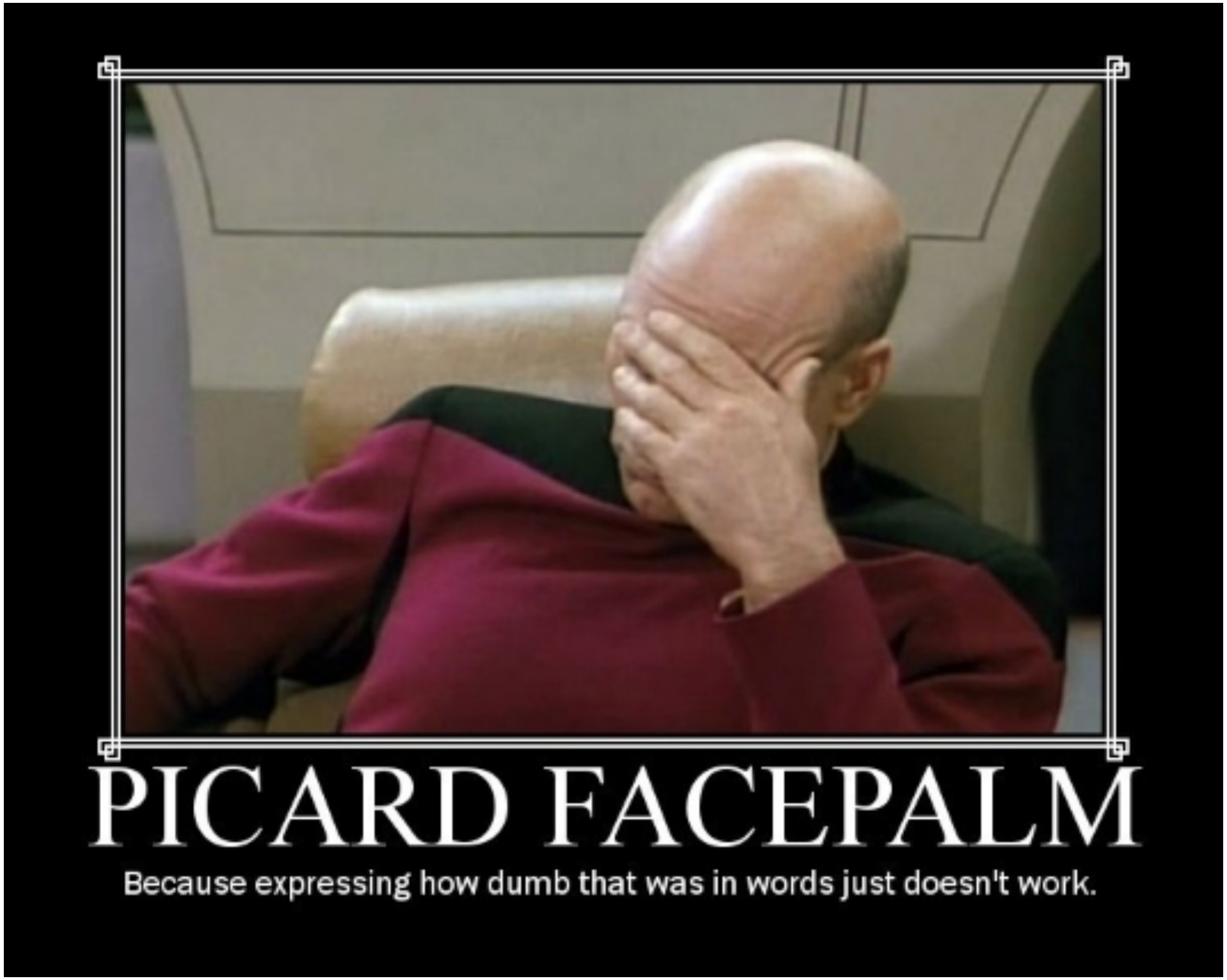
COMMAND INJECTION



```
Device 0
Short Address: 0
Ext Address: 15811245256278736097
MAC address: None
Frame Counter: None
ZB NWK Seqnumber: None
IEEE Seqnumber: 87
ZigBee AppDataPayload Counter: None
ZigBee ZCL Trans Seqnumber: None
NO scheduled packet set!
-- Destination: 0
Short Address: 12034
Ext Address: None
MAC address: None
Frame Counter: 877742
ZB NWK Seqnumber: 216
IEEE Seqnumber: 229
ZigBee AppDataPayload Counter: 68
ZigBee ZCL Trans Seqnumber: 57
NO scheduled packet set!
-- Destination: 1
Short Address: 37181
Ext Address: None
MAC address: None
```

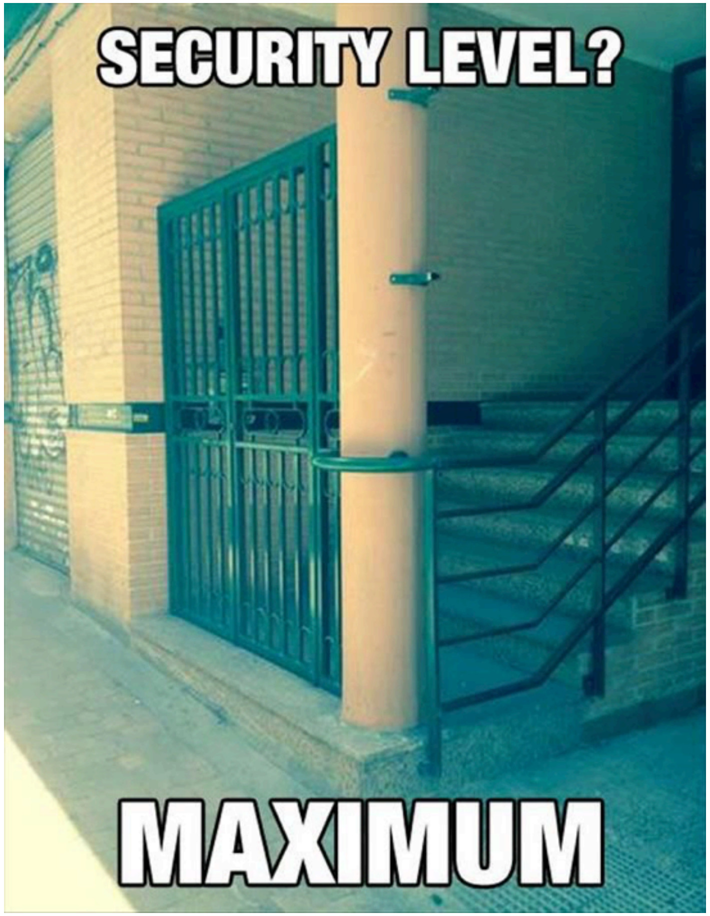
```
0 (0)
1 (12034)
2 (37181)
```

FEELINGS AFTER SOME TIME


PICARD FACEPALM
Because expressing how dumb that was in words just doesn't work.

SUMMARY

- Wireless offers a huge attack surface
- Usability overrules security
- A lot of attack vectors
- We need more research!
- We need more tools :D



BLACKHAT SOUND BYTES

- There is a world beside TCP/IP and Wifi
- Security of wireless protocols is often not mature
- Wireless communication is often a blind spot

cognosec

Thank you!

Time for Questions & Answers

Contact

tobias@zillner.tech
assurance@cognosec.com

cognosec