Self-labeling Electronic Shelf Labels

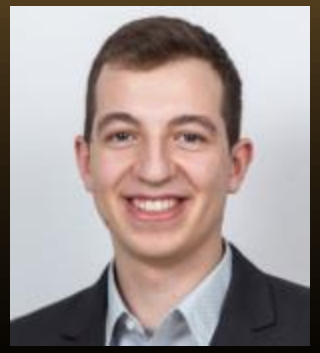
Pwning the Next Big Thing in Retail

SEC Consult

an atos company

Title: Self-Labeling Electronic Shelf Labels. | Responsible: S. Robertz | Version / Date: V1.0/2022-06 | Confidentiality Class: public

About Me



Steffen Robertz
Security Consultant

s.robertz@sec-consult.com
LinkedIn: shr70

SEC Consult Unternehmensberatung GmbH
Leopold-Ungar-Platz 2/3/3
1190 Vienna, Austria

www.sec-consult.com

Research conducted at the SEC Consult Vulnerability Lab

SEC Consult
an atos company

What's an ESL tag?

Parts

- Display (e.g. E-Ink)
- Usually Battery powered, supposed to last multiple years
- Some method of wireless communication (Bluetooth LE, NFC, 433 MHz)
- A matching transceiver for a regular computer

ESL Tags

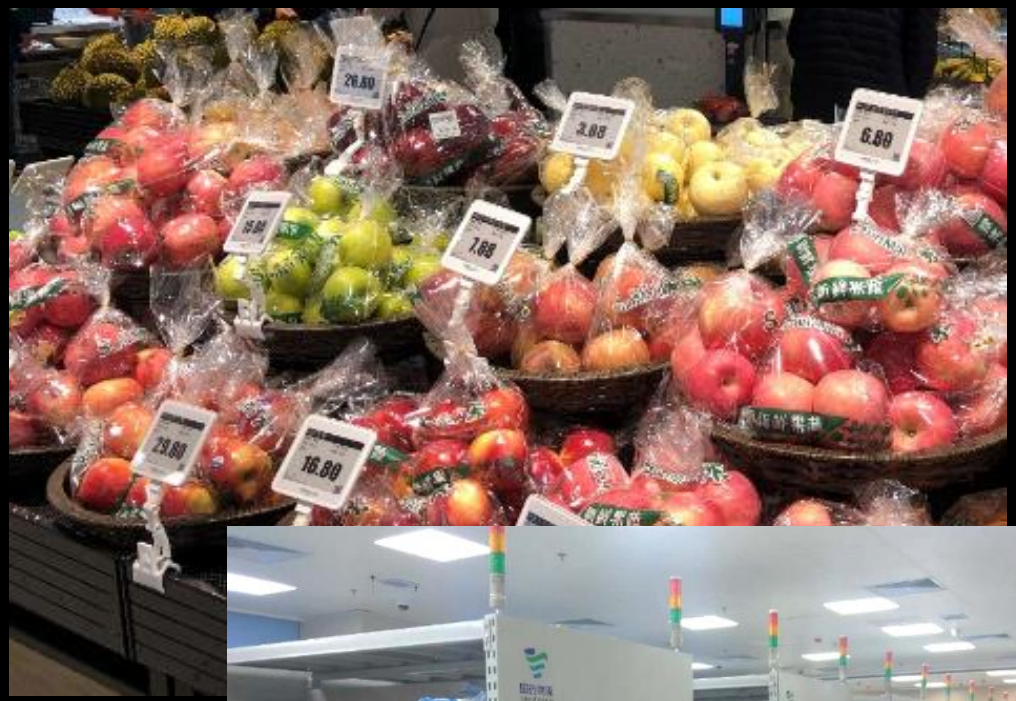
Is It Really the Next Big Thing?

- ESL market worth 855 Million $ in 2021 [1]
- Estimate for 2022: 980 Million $ [1]
- 2032: 5.2 Billion $ [1]

- Convenient price changes
- Promotional offers can be communicated easily
  - Attention drawn by e.g. flashing lights
  - Influences consumers decision

[1]: https://www.prnewswire.co.uk/news-releases/electronic-shelf-label-market-to-reach-usd-5-2-bn-by-2032-latest-fact-mr-study-834855956.html

ESL Usage



ESL Usage
Attack Scenarios

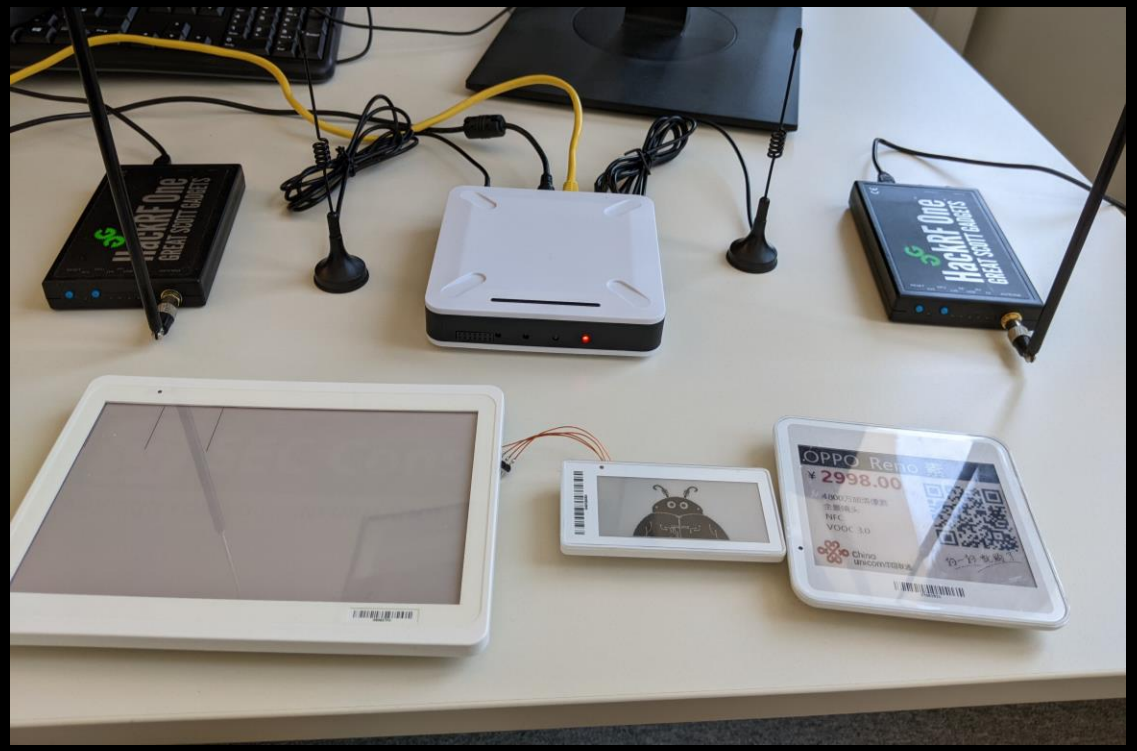
- Obstruct retailer -> blackmail for ransom
- Phishing site as QR code for discount coupons
- Maker community: Cheap display with long battery lifetime

ESL Usage

The Test Setup

- Common Chinese ESL tag supplier
- AP/Basestation, connected via Ethernet
- Tags connected via 433 MHz to Basestation
- Our Station: Retail Flavor
  - Also available as Industrial Flavor
- Tags available in multiple sizes (1.5” to 11.6”)

- Attacker: Using multiple HackRF for receiving and sending custom data frames

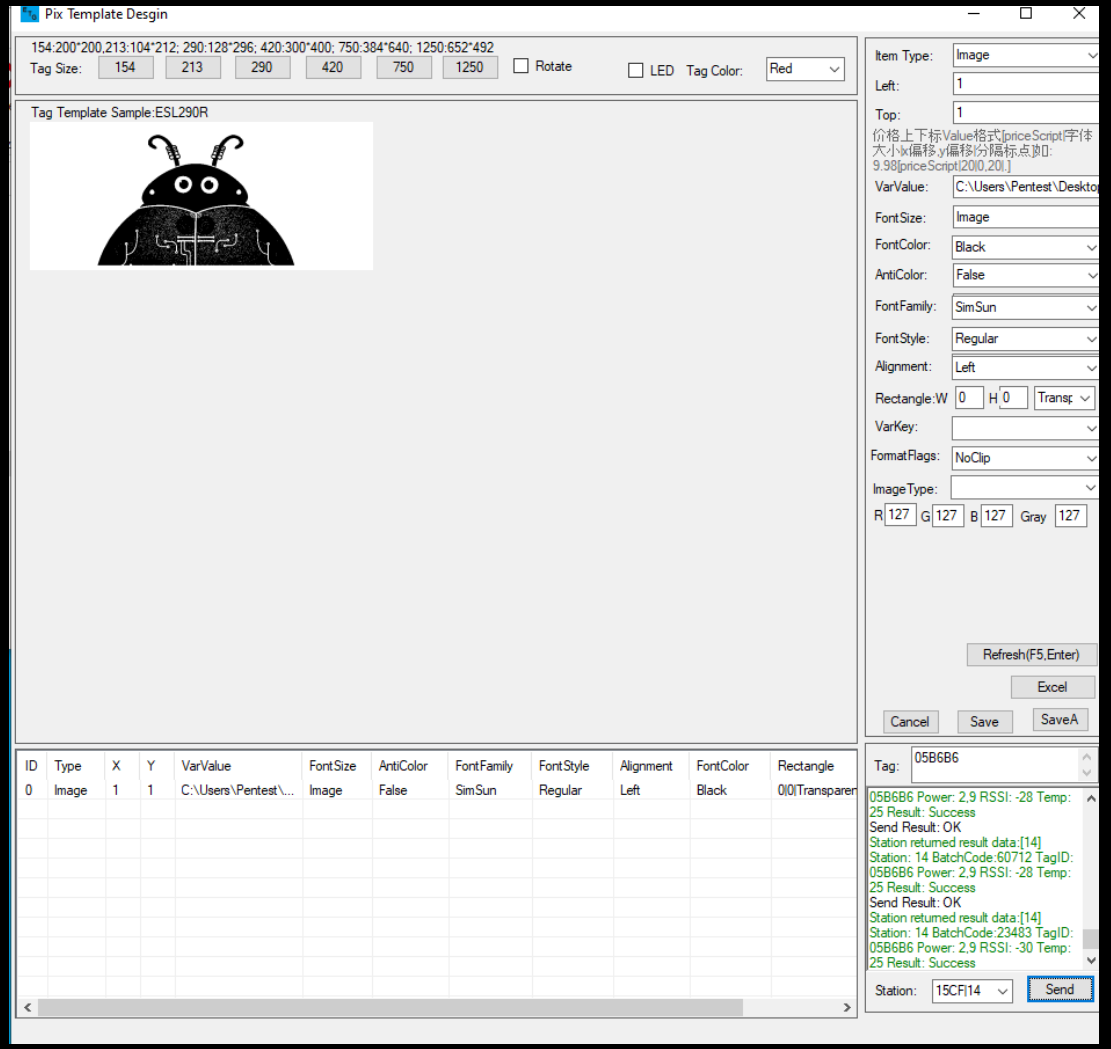


ESL Usage

The Design Tool

- Tool can create pixel graphics
- Tag field stores list of tags to update
- Status box in lower right-hand corner gives status information after transmission is completed

- Also available: .NET SDK for custom projects
- POS integration



The Hardware

SEC Consult
an atos company

The Tag

LED

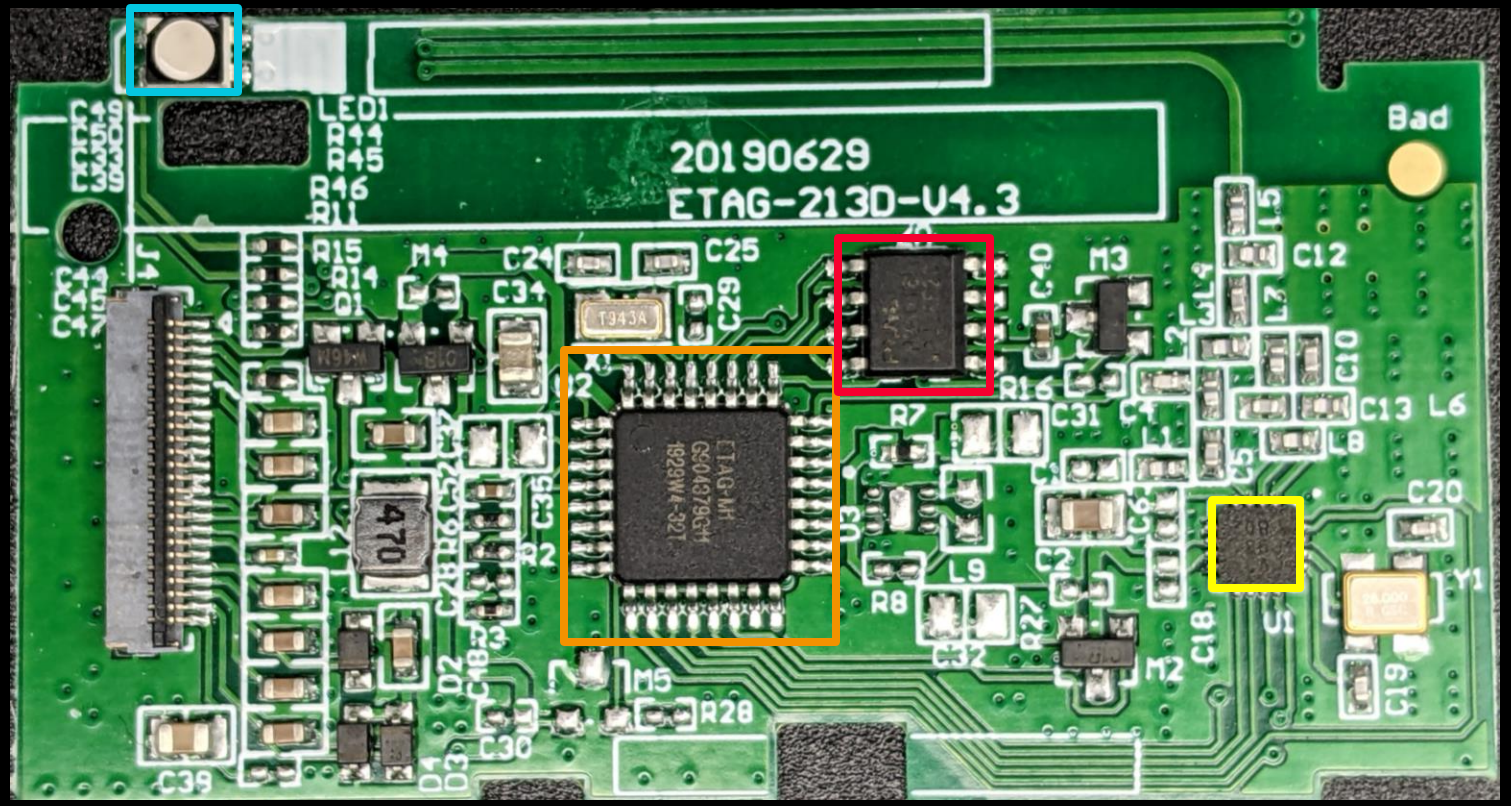
Tag ID

Display

SEC Consult
an atos company

The Tag

The PCB

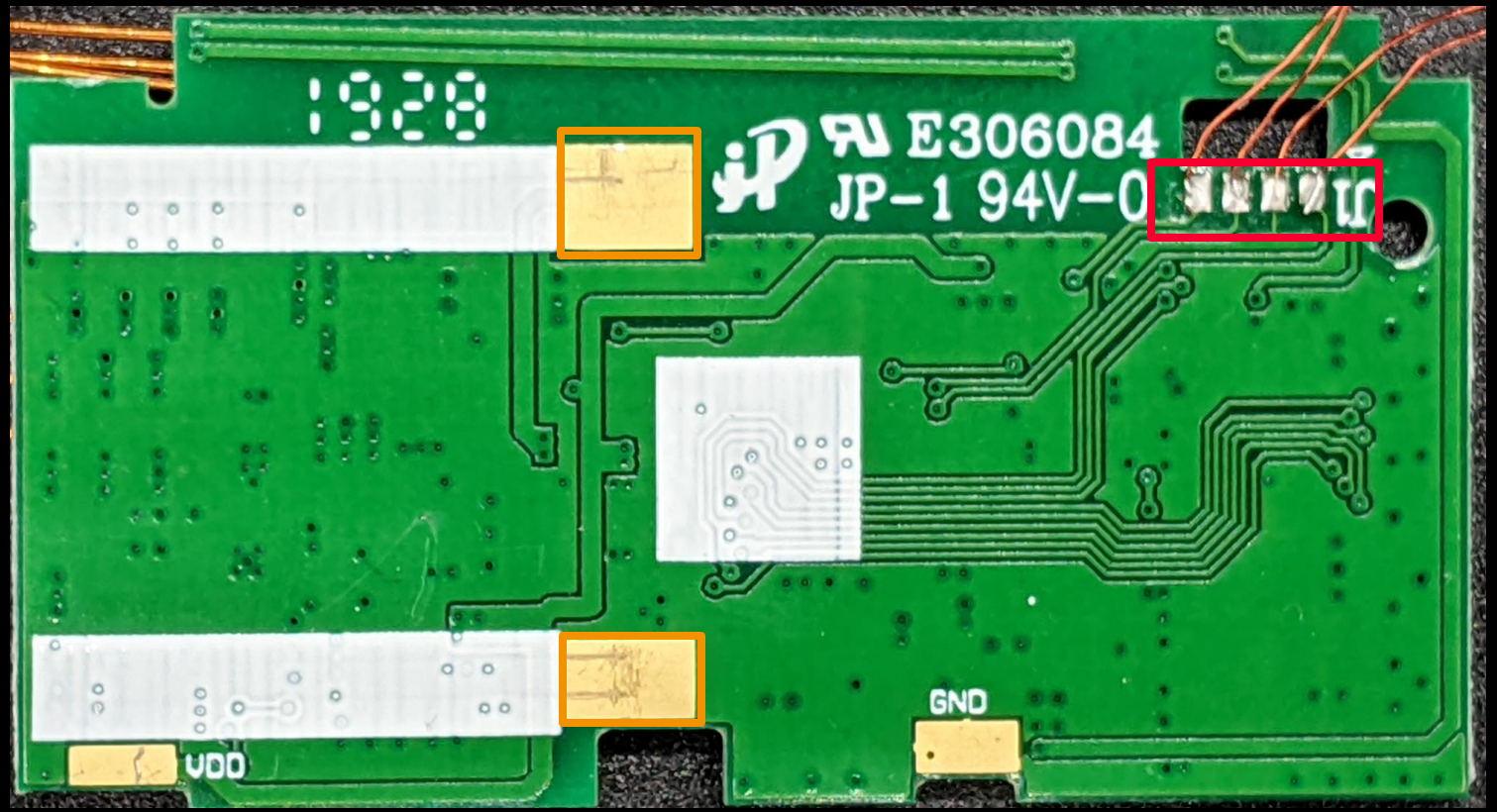


- Puya P25Q16H
- ETAG-M1
- OV80e934802
- RGB LED

SEC Consult
an atos company

The Tag

The PCB



Battery Connector

Debug Header

SEC Consult
an atos company

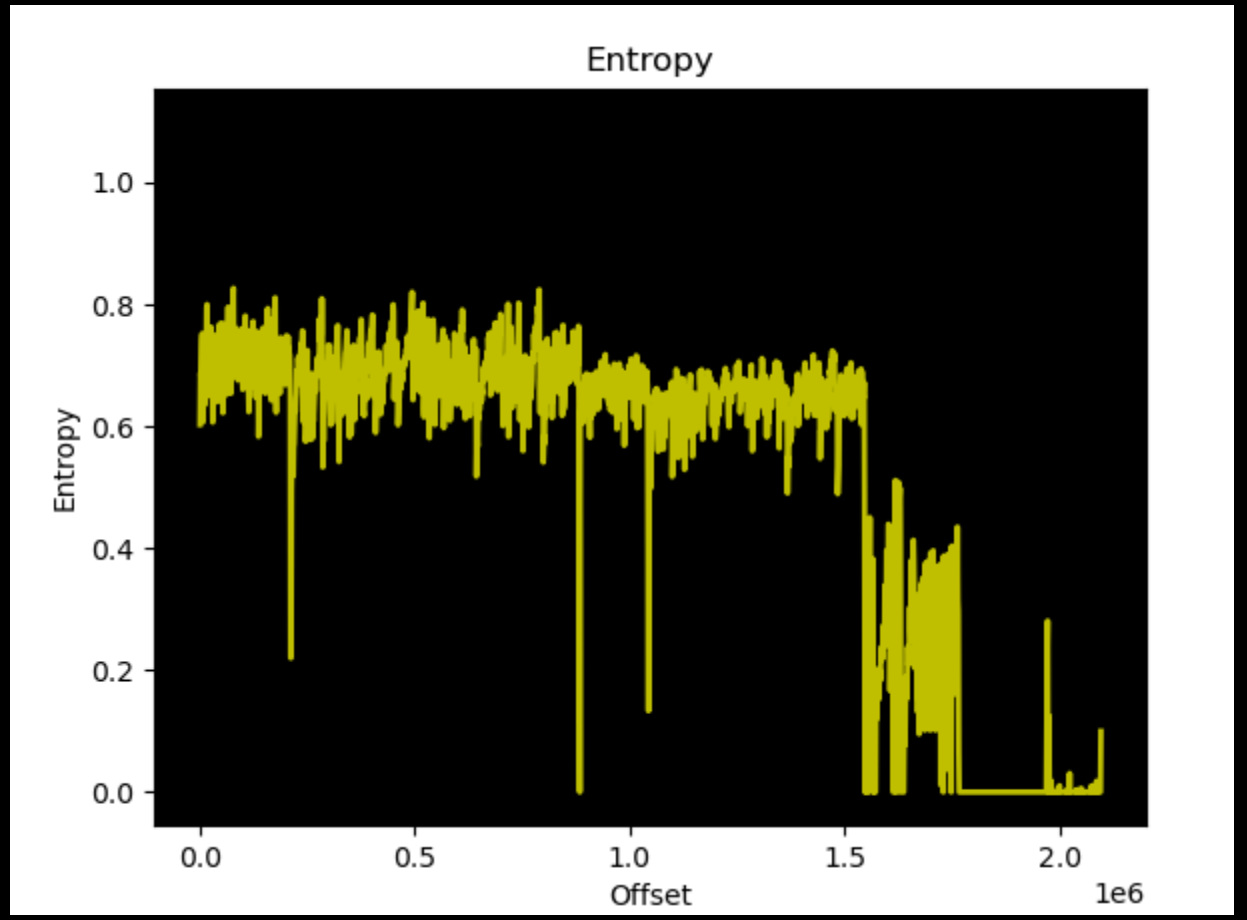
The Tag

External SPI Flash

- 2 MB of Flash storage
- Image data starts at 0x1e1000
- First black color channel, then red
- Image stored in rows

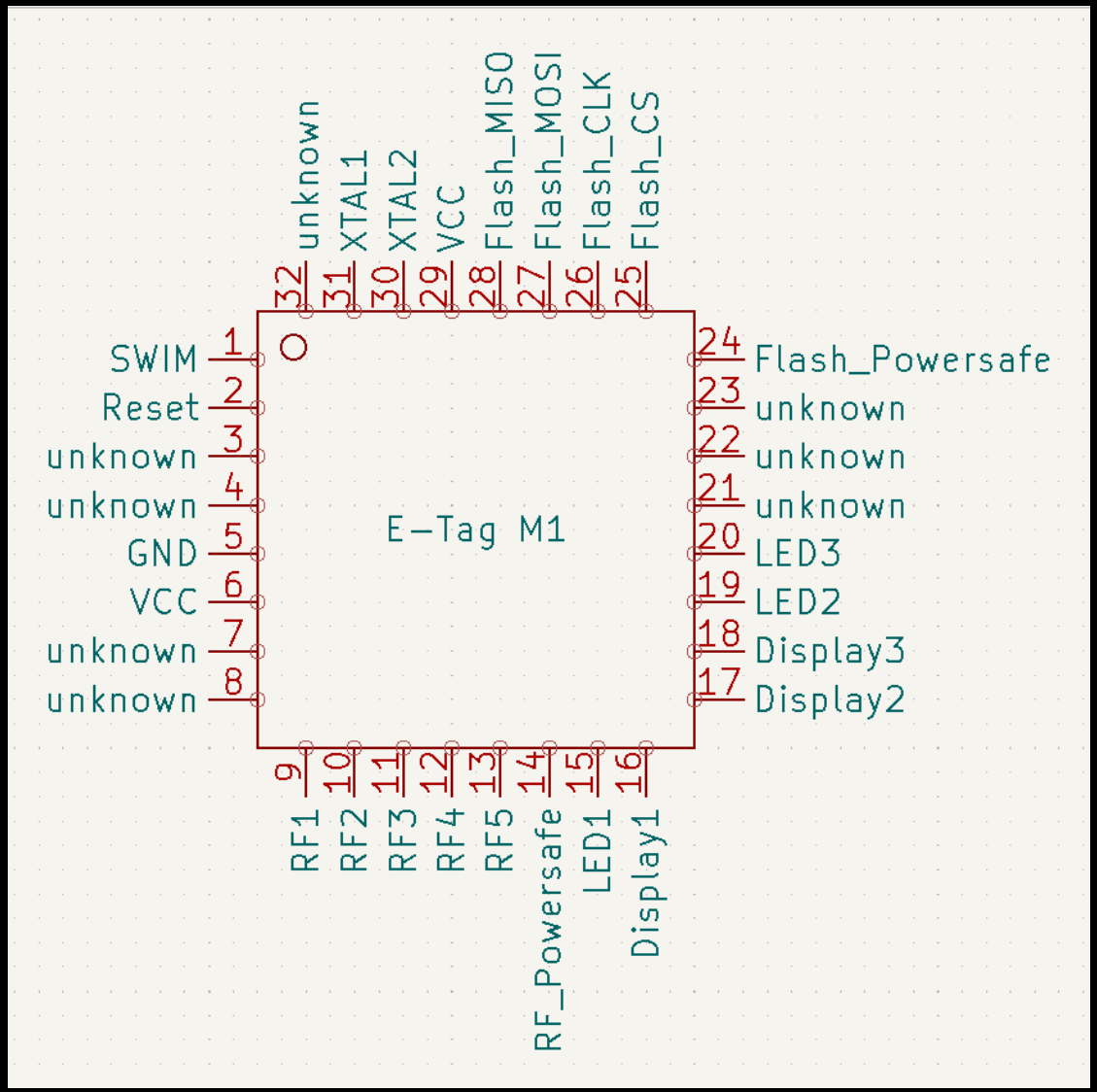
- Beginning of Flash contains something else
  - Most likely firmware

- Python script that parses images from flash dumps will be published



The Tag

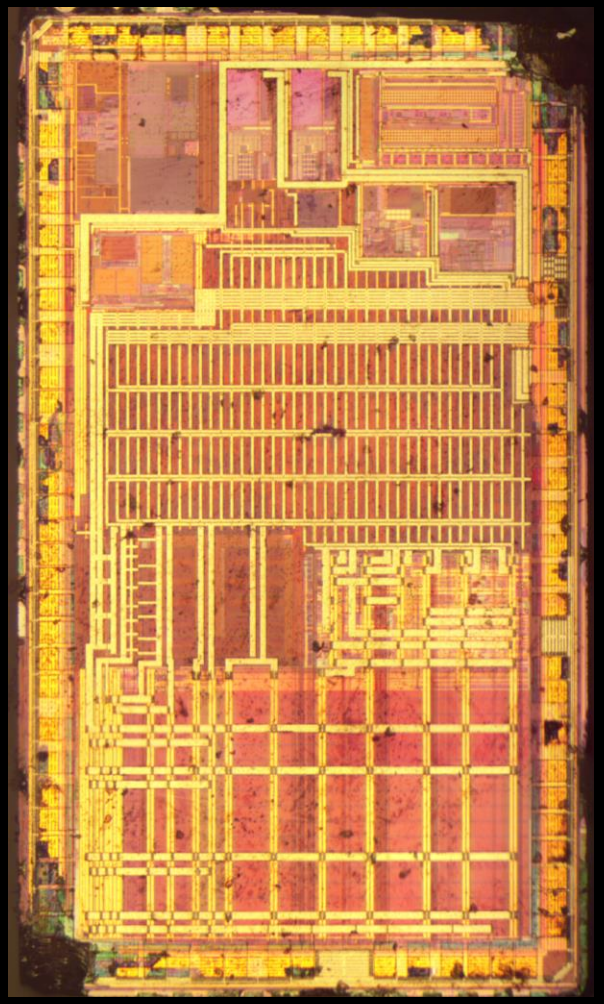
Identifying the E-Tag M1



The Tag

Identifying the E-Tag M1

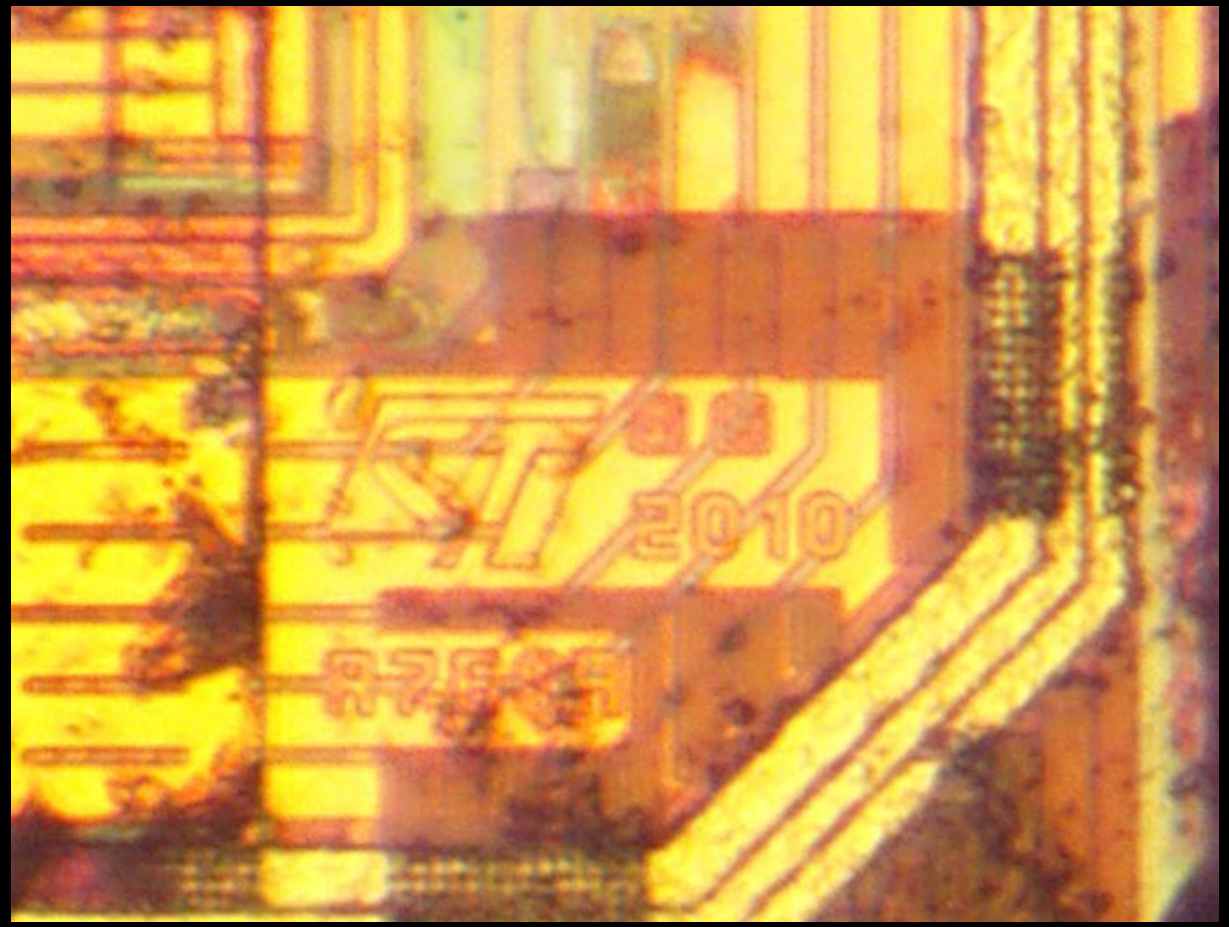
- Boiling the Chip in 95% concentrated sulfuric acid
  - Removes the epoxy packaging
- IC is cleaned with Isopropanol
- Manufacturer marking is visible



The Tag

The E-Tag M1 MCU

- Manufactured by ST Microelectronics
- Likely designed or produced in 2010
- R758R, might be ST internal part number?



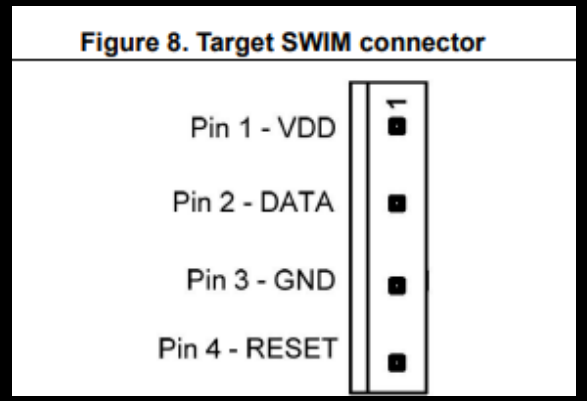
The Tag
Debug Access

- Backside of PCB has 4 testpads that look like debug access
- Pin 1: MCU Pin 2
- Pin 2: GND
- Pin 3: MCU Pin 1
- Pin 4: VDD

The Tag
Debug Access

- Backside of PCB has 4 testpads that look like debug access
- Pin 1: MCU Pin 2
- Pin 2: GND
- Pin 3: MCU Pin 1
- Pin 4: VDD

- STM8 SWIM debug header
  - Pin 1 is just marked on the wrong side
  - Pin 1: RESET
  - Pin 3: DATA
- Confirm RESET by pulling pin low and checking if the tag restarts



The Tag
Debug Access

- Use stm8flash with ST-Link V2
- Use any STM8, preferably with much Flash and RAM
  - Start addresses seem to be consistent across all versions

- stm8flash -c stlinkv2 -p stm8s2081b -s 0x8000 -b 131072 -r dump
  - Indicates 64kByte Flash
  - ROP seems to be activated
- Using same method:
  - 2048 Bytes EEPROM

```
0000ff90: 7171 7171 7171 7171 7171 7171 7171 7171  qqqqqqqqqqqqqqqq
0000ffa0: 7171 7171 7171 7171 7171 7171 7171 7171  qqqqqqqqqqqqqqqq
0000ffb0: 7171 7171 7171 7171 7171 7171 7171 7171  qqqqqqqqqqqqqqqq
0000ffc0: 7171 7171 7171 7171 7171 7171 7171 7171  qqqqqqqqqqqqqqqq
0000ffd0: 7171 7171 7171 7171 7171 7171 7171 7171  qqqqqqqqqqqqqqqq
0000ffe0: 7171 7171 7171 7171 7171 7171 7171 7171  qqqqqqqqqqqqqqqq
0000fff0: 7171 7171 7171 7171 7171 7171 7171 7171  qqqqqqqqqqqqqqqq
00010000: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00010010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00010020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00010030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

The Tag

Debug Access: Finding the Unique ID

- Multiple known addresses for unique ID
  - 0x48CD
  - 0x4865
  - 0x4926
- Only 0x4926 returned data that would fit the format of Table 14
- Hence:
  - X co-ordinate: 31
  - Y co-ordinate: 58
  - Wafer number: 22
  - Lot number: G904379
- According to STM Forums, 0x4926 seems to be unique to STM8L devices

Table 14. Unique ID registers (96 bits)

Address	Content description	Unique ID bits							
		7	6	5	4	3	2	1	0
0x48CD	X co-ordinate on the wafer	U_ID[7:0]							
0x48CE		U_ID[15:8]							
0x48CF	Y co-ordinate on the wafer	U_ID[23:16]							
0x48D0		U_ID[31:24]							
0x48D1	Wafer number	U_ID[39:32]							
0x48D2	Lot number	U_ID[47:40]							
0x48D3		U_ID[55:48]							
0x48D4		U_ID[63:56]							
0x48D5		U_ID[71:64]							
0x48D6		U_ID[79:72]							
0x48D7		U_ID[87:80]							
0x48D8		U_ID[95:88]							

The Tag
OSINT

- Factory is Alibaba Gold Plus Supplier
  - Alibaba produces a production line verification report
  - Contains all fabrication machines of the factory
- List contains “Ultrasonic Fuse”
  - STM8L are custom bonded
  - Unique pinout
  - Should still be traceable through STM Lot numbers
  - "Ultrasonic Fuse" could also be for sealing the casing (ultrasonic welding of plastics)

The RF Protocol

SEC Consult
an atos company

The RF Protocol

Gaining Insights From FCC Files

2.2 GENERAL DESCRIPTION OF EUT

Equipment	Station
Trade Mark	N/A
Model Name	ETAP01
Serial No.	ETAP
Model Difference	All models have the same functionality, software and electronics, only the color, front frame shape and model names may differ. Test sample model: ETAP01
FCC ID	2ARJ5-ETAP01
Antenna Type	Suction cup Antenna
Antenna Gain	5dbi
Frequency Range	433.92MHz
Number of Channels	1
Modulation Type	GFSK
Battery	N/A
Power Source	AC 120V 50Hz from adapter
Adapter Model	MODEL NO. :GS12E05 INPUT:100-240V~,50/60Hz, 0.31A OUTPUT:5V⎓ 2.0A

FCC Info Basestation

2.2 GENERAL DESCRIPTION OF EUT

Equipment	Etag
Trade Mark	N/A
Model Name	ET0213
Serial No.	ET0290
Model Difference	All models have the same functionality, software and electronics, only the color, front frame shape and model names may differ. Test sample model: ET0213
FCC ID	2ARJ5-ET0213
Antenna Type	PCB Antenna
Antenna Gain	1.0dbi
Frequency Range	433.92MHz
Number of Channels	1
Modulation Type	ASK
Battery	N/A
Power Source	DC 3.0V from battery
Adapter Model	N/A

FCC Info ESL Tag

The RF Protocol

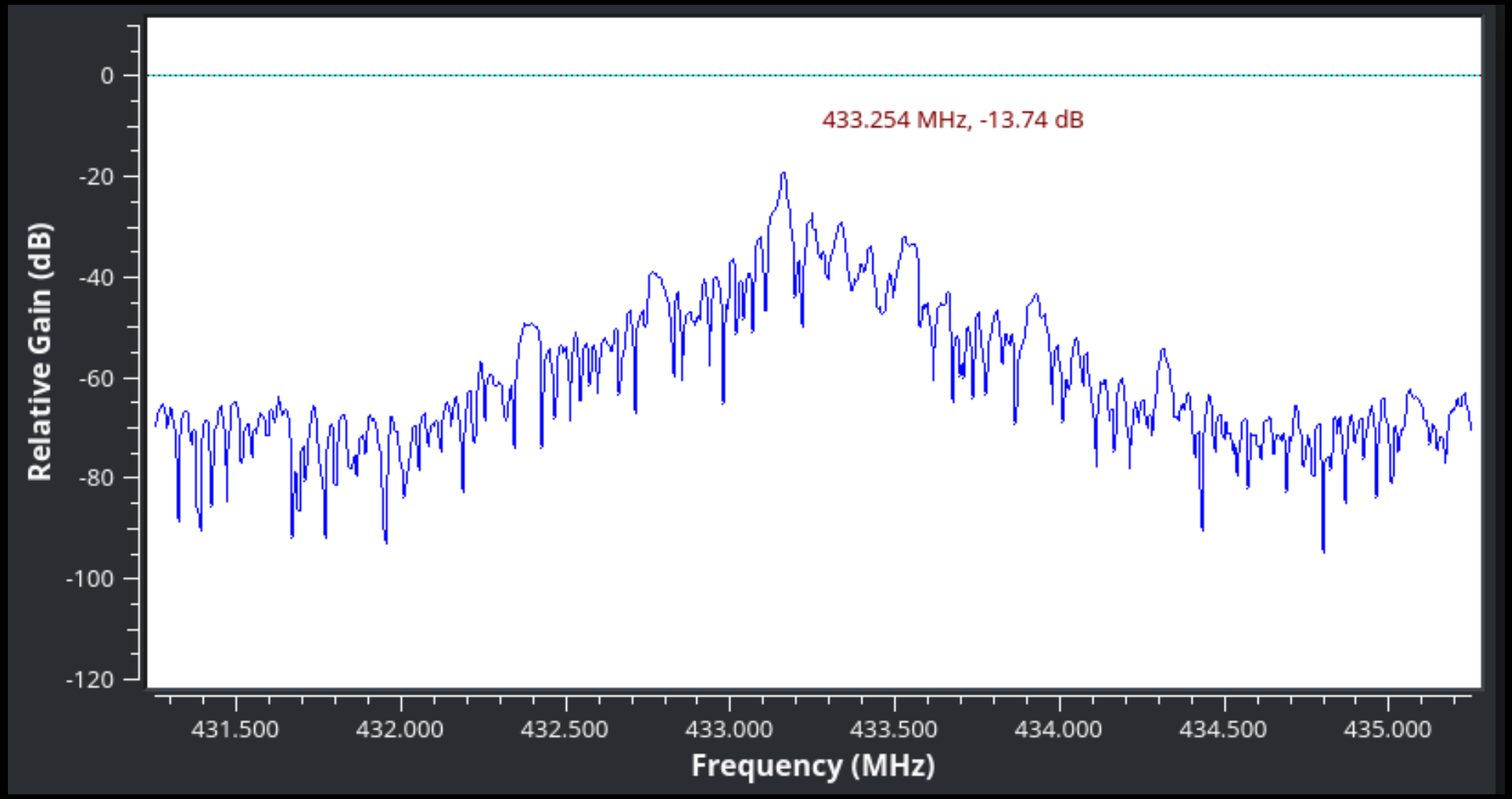
Gaining Insights From FCC Files

- FCC test lists different modulations for tag and base station

- FCC files list one channel at 433.92MHz
- Manual talks about frequency hopping technology for anti-jamming
    - Was never observed
    - Violation of the one channel/one frequency statement

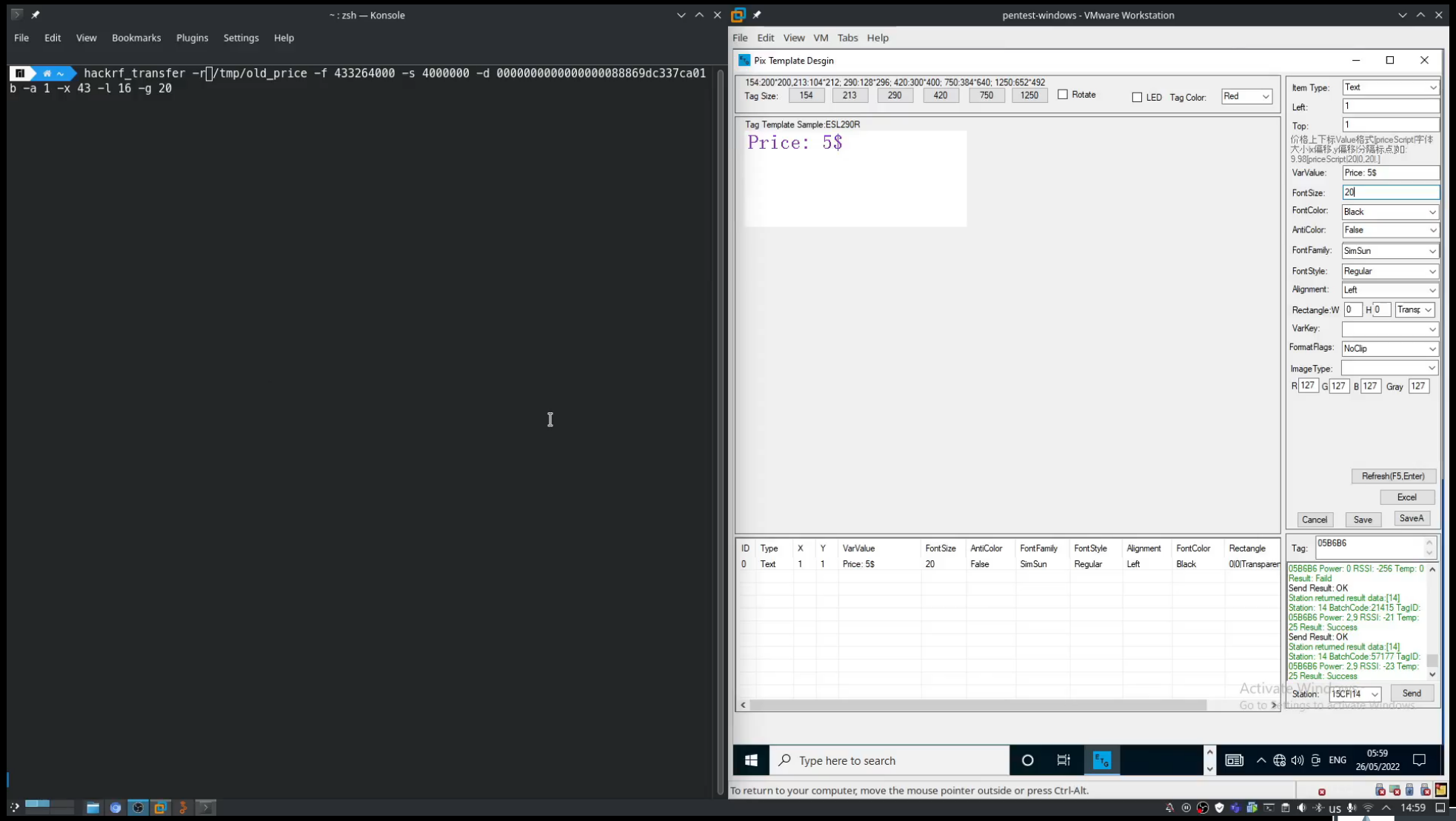
The RF Protocol

Finding the Right Frequency



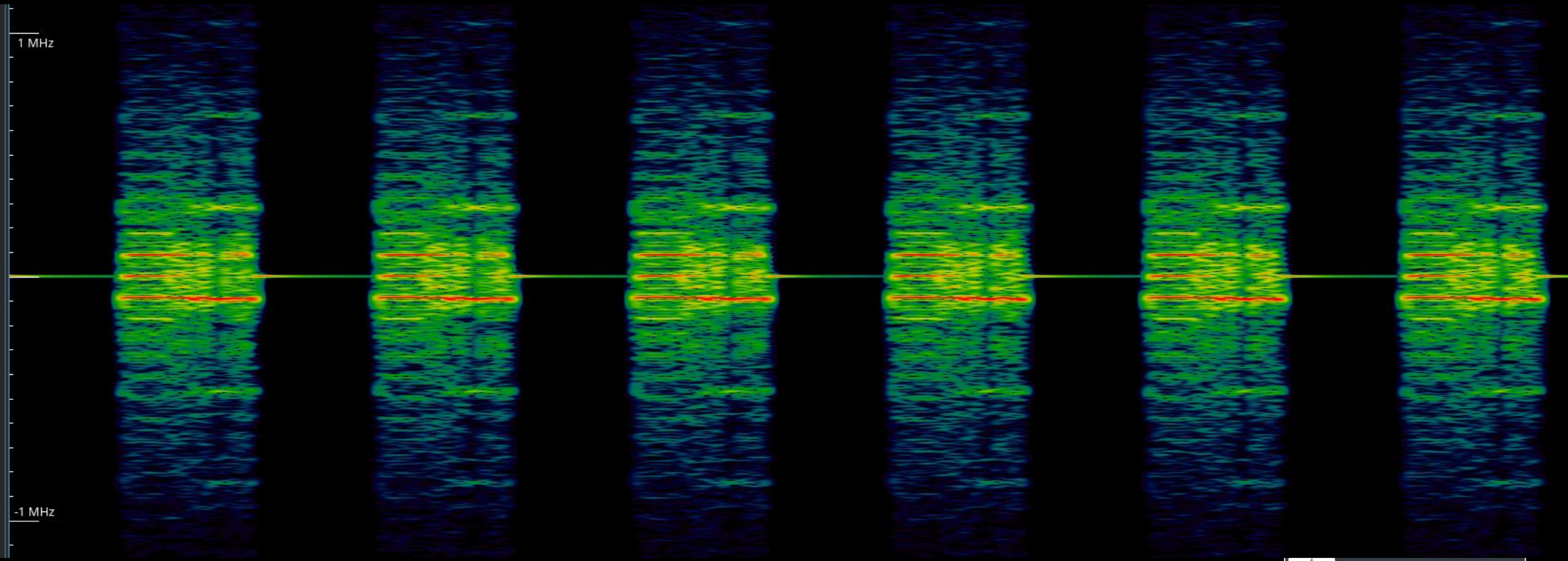
Live Demo

Replay Attack



The RF Protocol

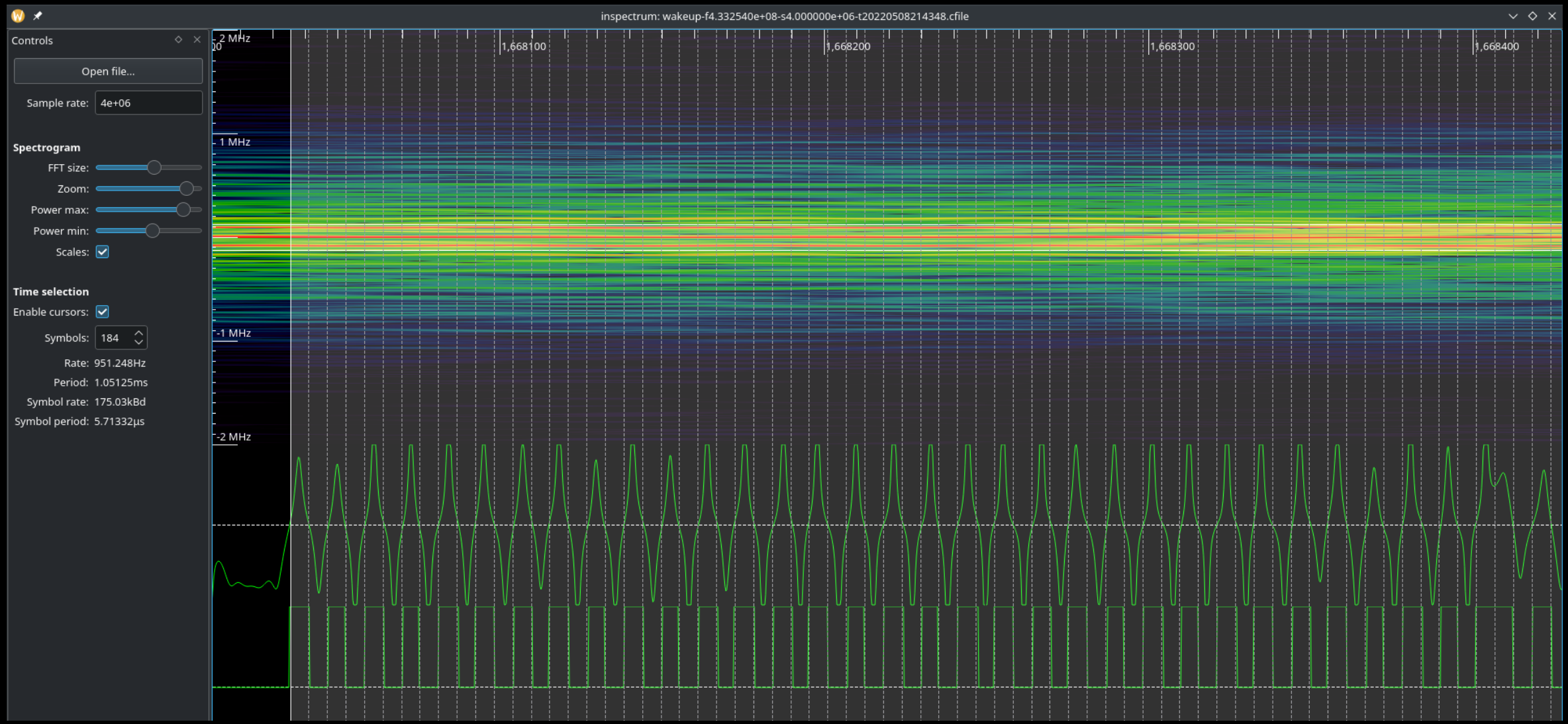
Determining the Correct Modulation



SEC Consult
an atos company

The RF Protocol

Manually Decoding Frames



The RF Frames

Activating the Tag

- 920 different frames, simply counting down to zero
- Each frame repeated 5 times
- Transmitted at 175 kBaud

Preamble	Sync Header	Frame Length	Tag ID	Fixed Value	Frame Counter	Fixed Value	CRC16
AAAAAAAA AAAAAA	D391D391	08	065302	0000	0398	0a	2708

The RF Frames

The Image Frame Structure

- Transmitted at 100kBaud
- Frame 1 out of 9
- Max 54 Byte of Image data
- Frame Length does not include CRC
- CRC creation starts at Frame Length field

Preamble	Sync Header	Frame Length	Tag ID	Frame Counter	Fixed Value	Payload	CRC16
AAAAAAA AAAAAAA	D391D3 91	3c	065302	0901	33	<Image Data Structure>	CRC

The RF Frames

Special Image Frames

- Larger displays will require more than 256 frames
- First frame uses 16bit as frame counter
- Second frame starts with count zero and counts up towards the number transmitted in the first frame

Preamble	Sync Header	Frame Length	Tag ID	Frame Counter	Fixed Value	Payload	CRC16
AAAAAAA AAAAAAA	D391D391	3c	065302	<count>	33	<Image Data Structure>	CRC

The RF Frames

The Image Data Structure

- The image data structure starts with an additional header
- FC00000000 indicates black color channel
- FC80000000 indicates red color channel
- Second LED byte, 0b0111 to turn LED to white
    - One bit per color channel

LED	Batch Code	Fixed Value	LED Time	Compression header	Display Height	Display Width	Payload
0700	BF75	00ED	000A	fc00000000	007f	0127	<Compressed Image Data>

The RF Frames

The Image Compression

- 3 colors supported (white, black, red) → 2bit per pixel
- Image payload too short for the amount of display pixel → custom compression algorithm is used
- Reverse Engineered from .NET SDK package (https://www.nuget.org/packages/eTag.SDK/)
- Uses Run-length encoding per color channel

The RF Frames

The Image Compression

- Case 1: Less than 8 consecutive bits

- Case 2: Less than 32 consecutive bits

- Case 3: Less than 256 consecutive bits

- Case 4: Less than 2 ^ 16 consecutive bits

The RF Frames

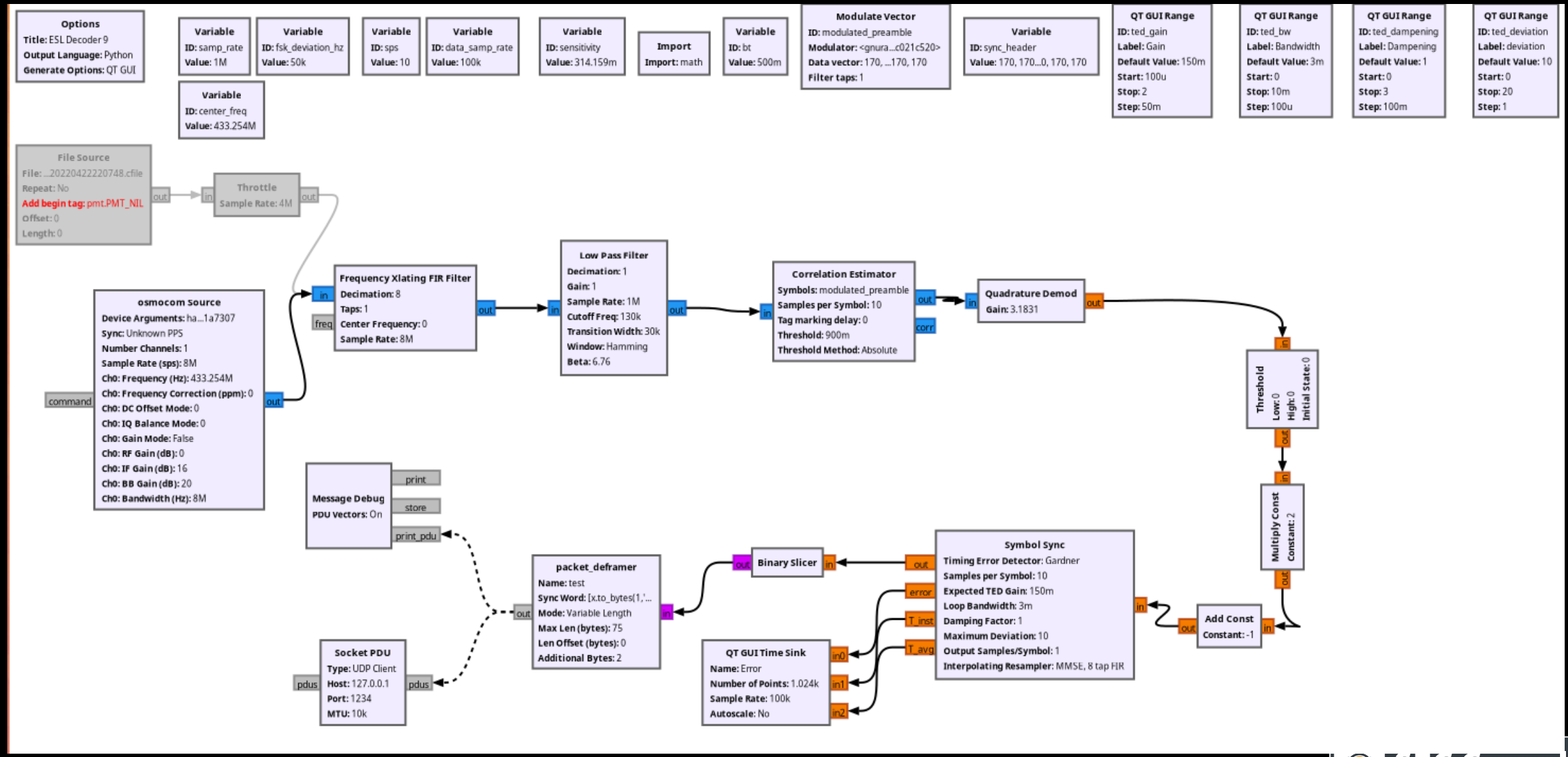
The Tag Response

- Repeated 3 times
- 100kBaud

Sync Header	Fixed Value	Frame Length	Tag ID	Battery Voltage	RSSI [1]	RSSI [0]	Temperature
AAAAAAAA AAAAAA	D391 D391	07	065302	1D = 2.9V	20	68	E9 = 23.3 C

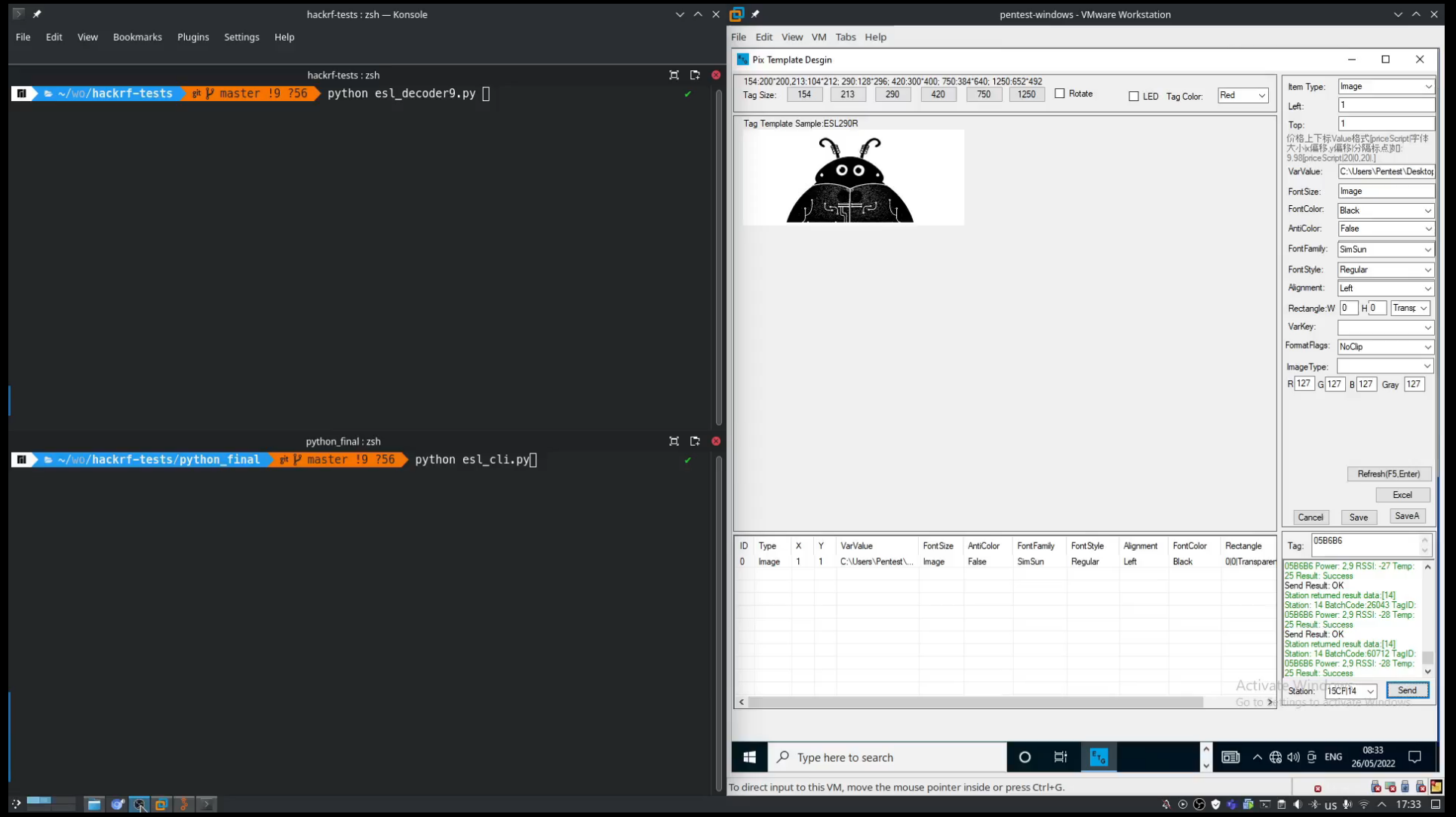
The RF Protocol

Receiving Images in GNU Radio



Live Demo

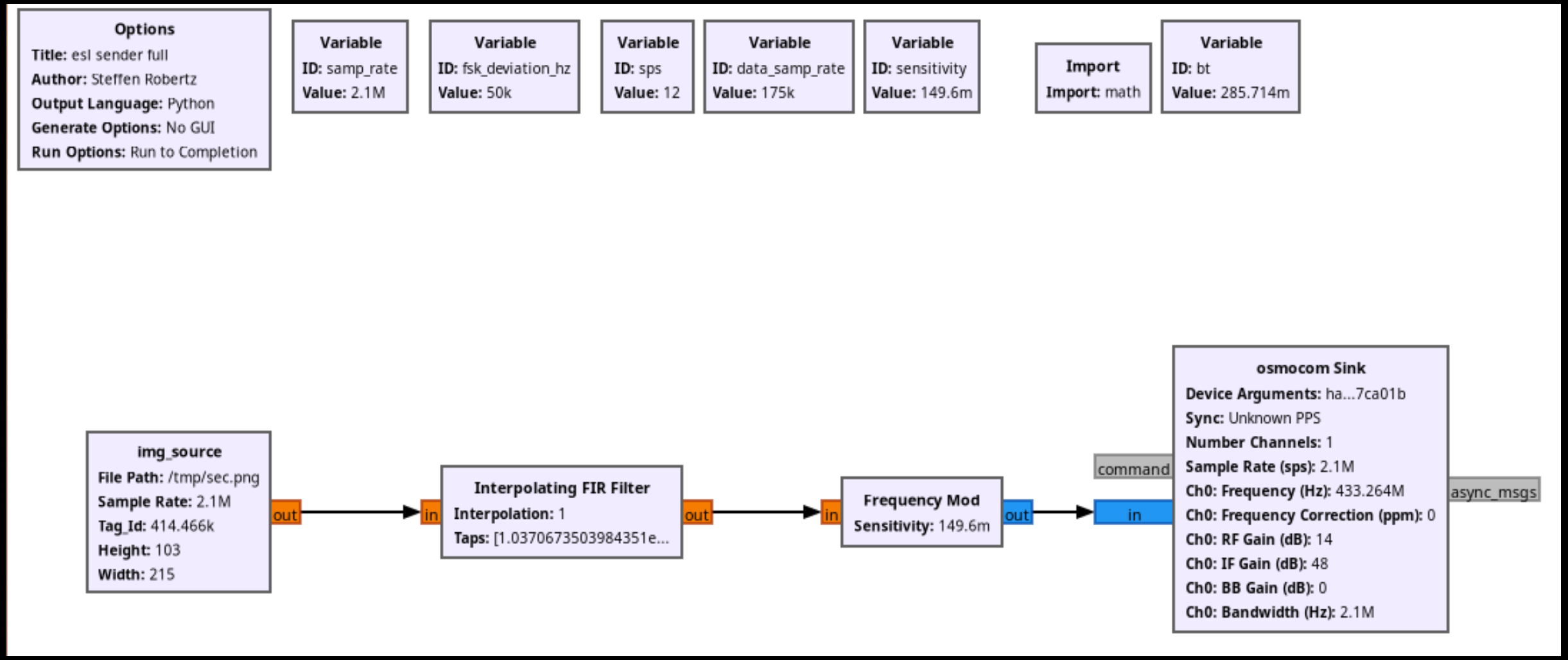
Receiving Tag Information



SEC Consult
an atos company

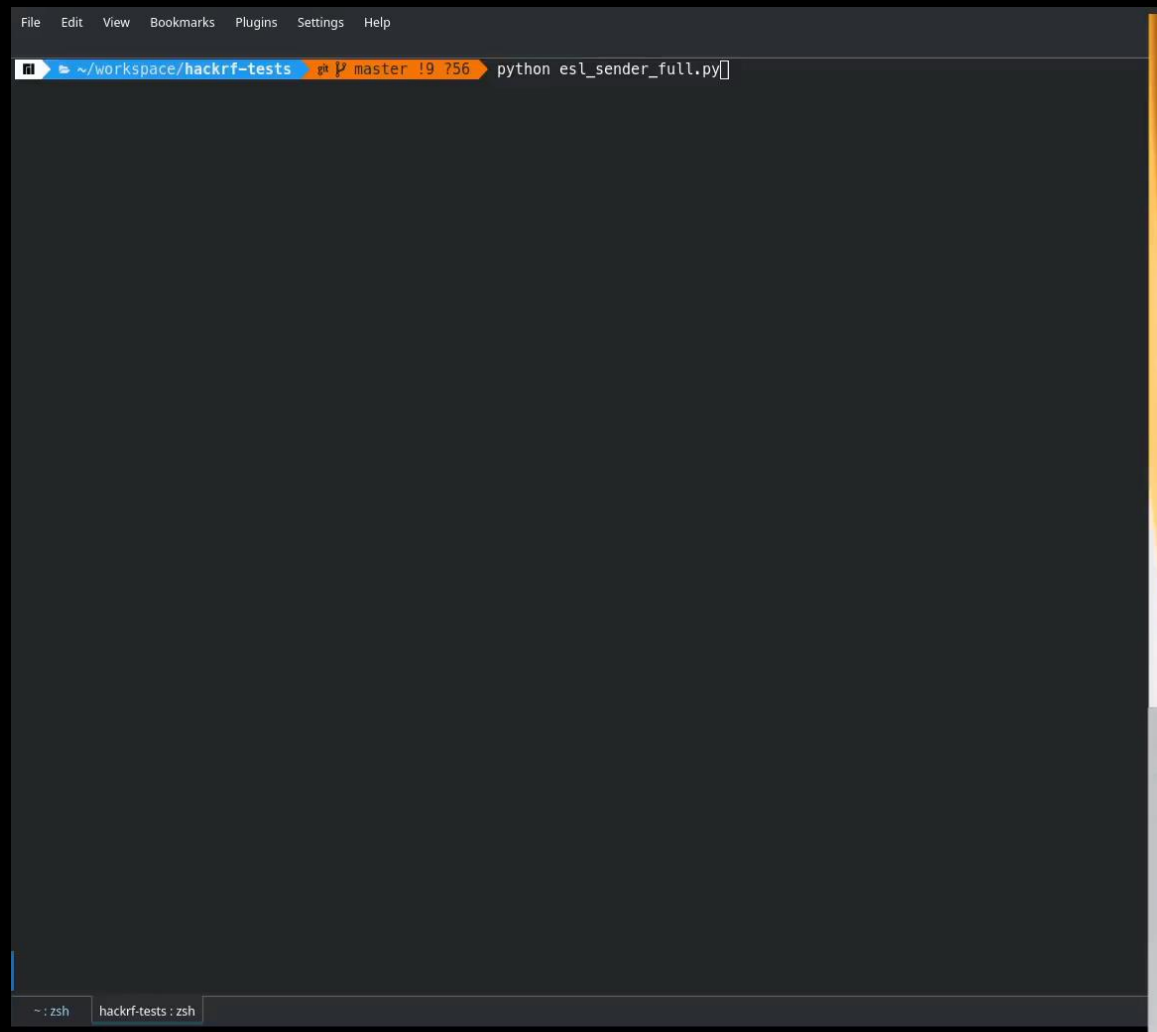
The RF Protocol

Sending Images With GNU Radio



Live Demo

Modifying Tag Contents



SEC Consult
an atos company

Conclusion

- Identified unknown MCU
- Gained access via debug port
- Confirmed replay vulnerability
- Reverse engineered the RF protocol
    - Gained ability to send and receive valid frames
- Able to receive and decode ESL price updates
- Able to change tag content to arbitrary information
- Range limited by RF power

Conclusion
Lessons Learned

- Protocol does not contain any security measures
- Custom protocols at 433 MHz do not increase security
    - Can be received and impersonated with e.g. a C1101 (2$)
- Protocol robustness could have been increased by using error correction algorithms
- Relabeling a MCU does not protect against finding the correct MCU family

- All code will be released on GitHub within the next weeks

Do you have any further questions?

Don‘t hesitate to contact us: s.robertz@sec-consult.com

www.sec-consult.com

SEC Consult
an atos company