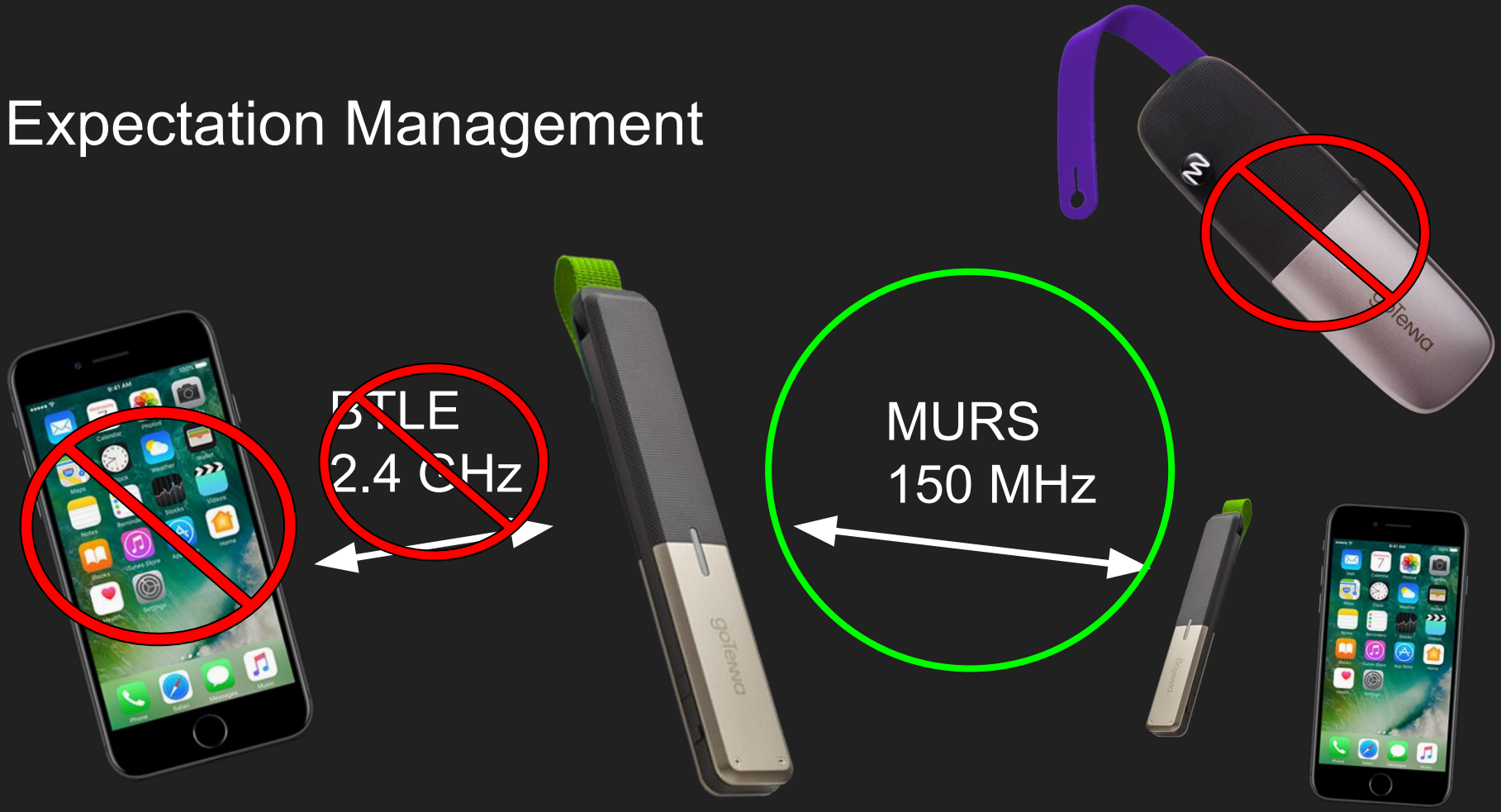
Gotenna RE

Woody (@tb69rr)
Tim (@bjt2n3904)

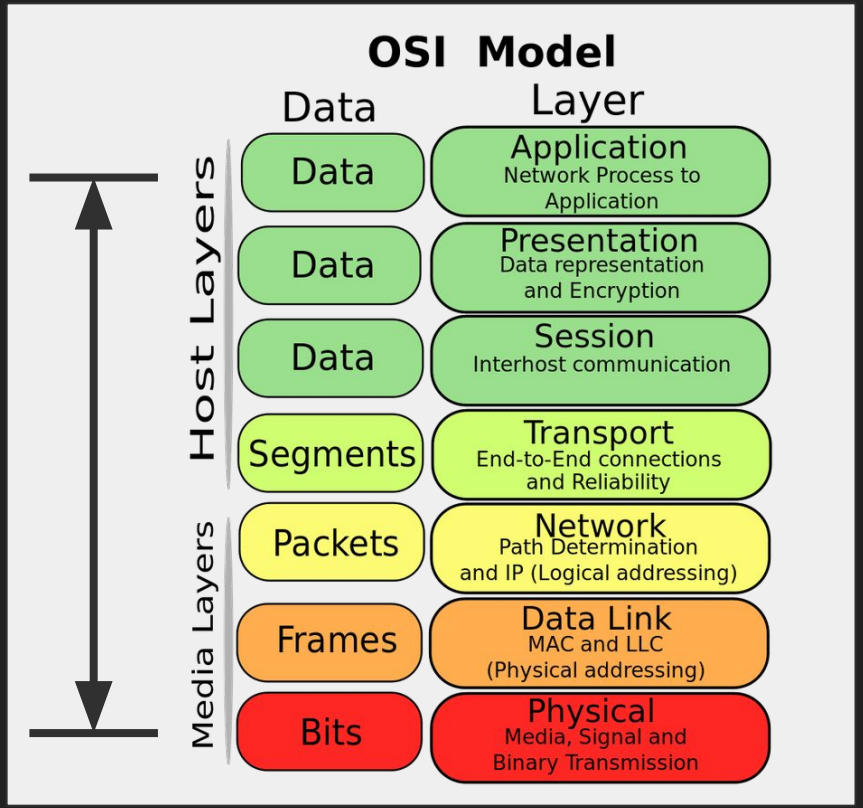
What is GoTenna?

Expectation Management

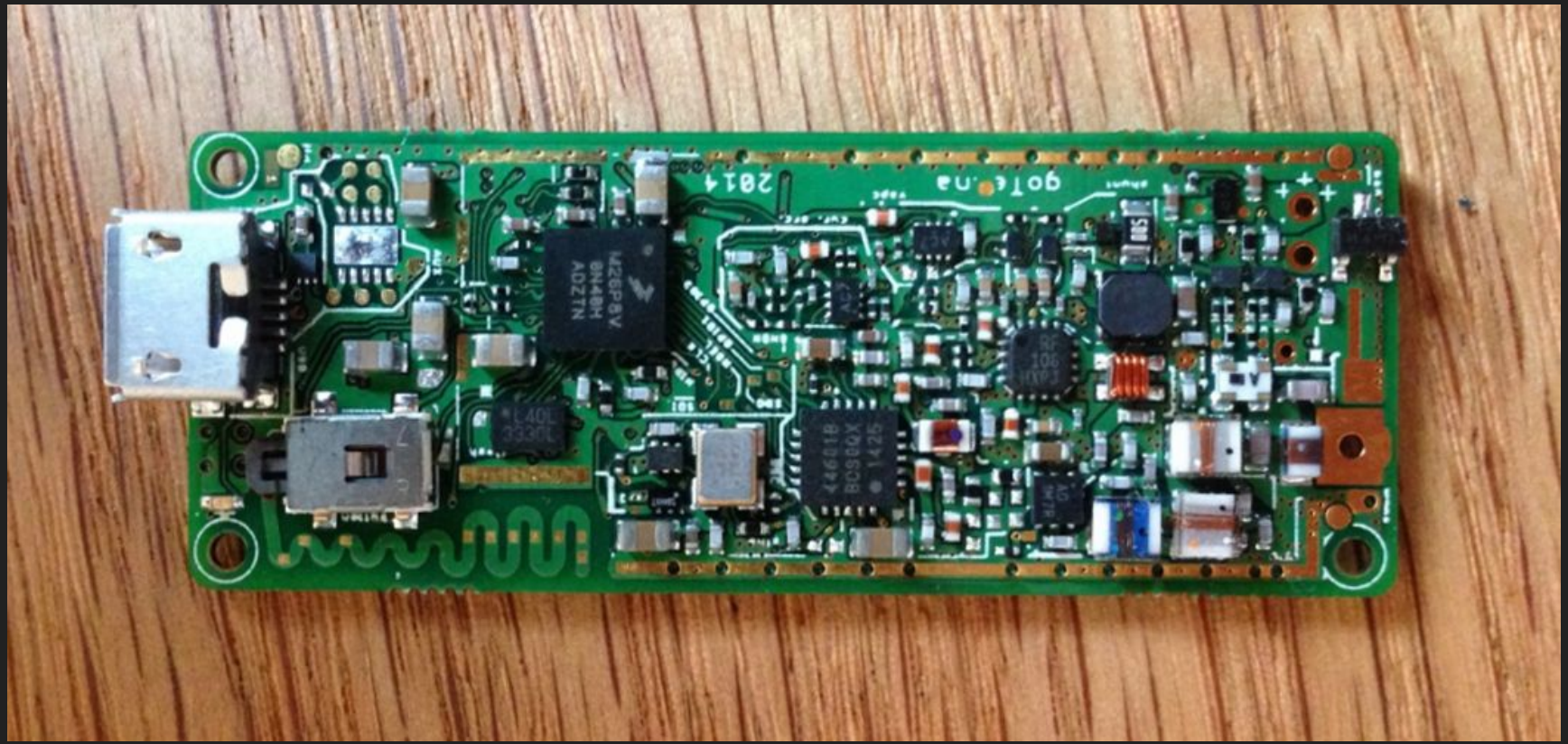
Expectation Management



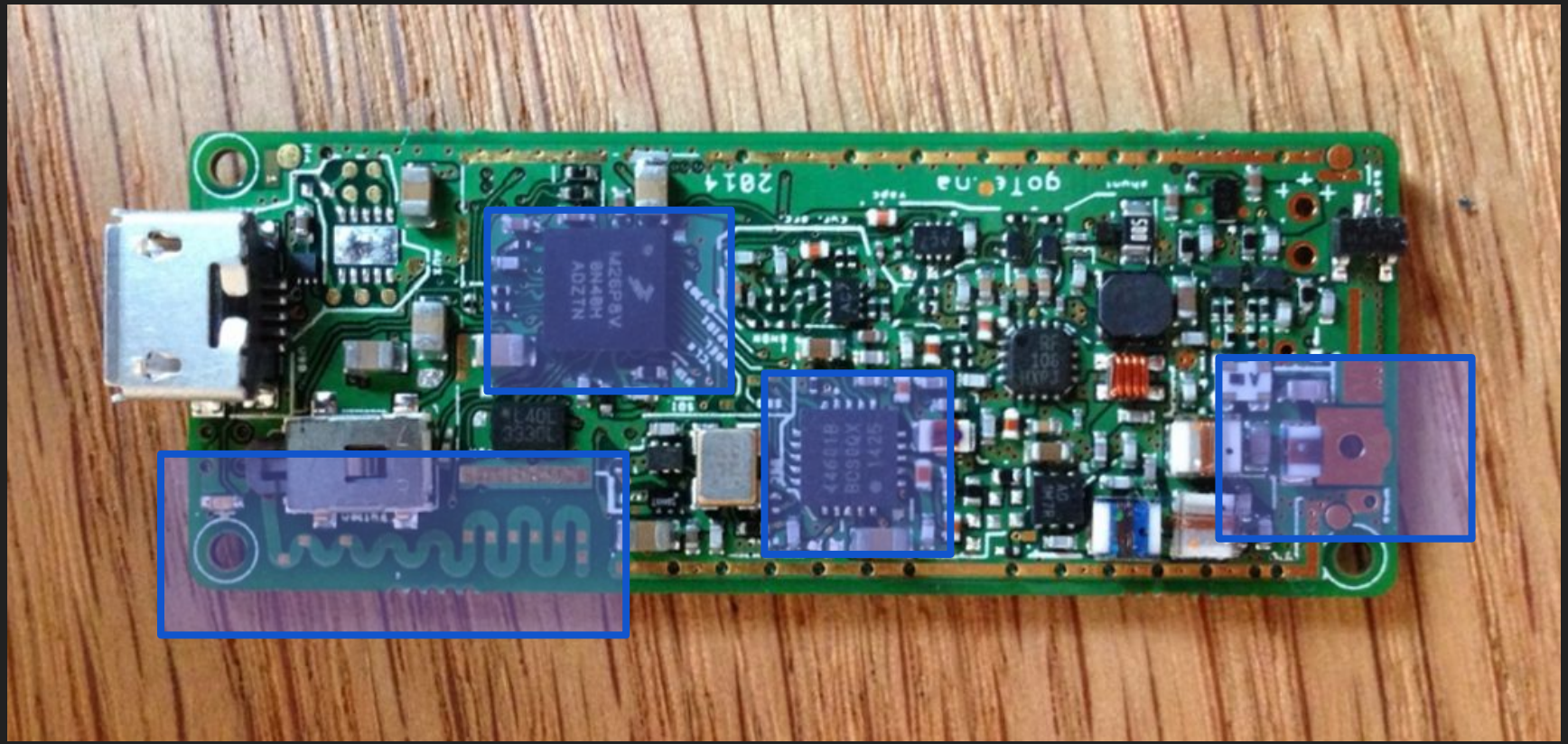
Expectation Management



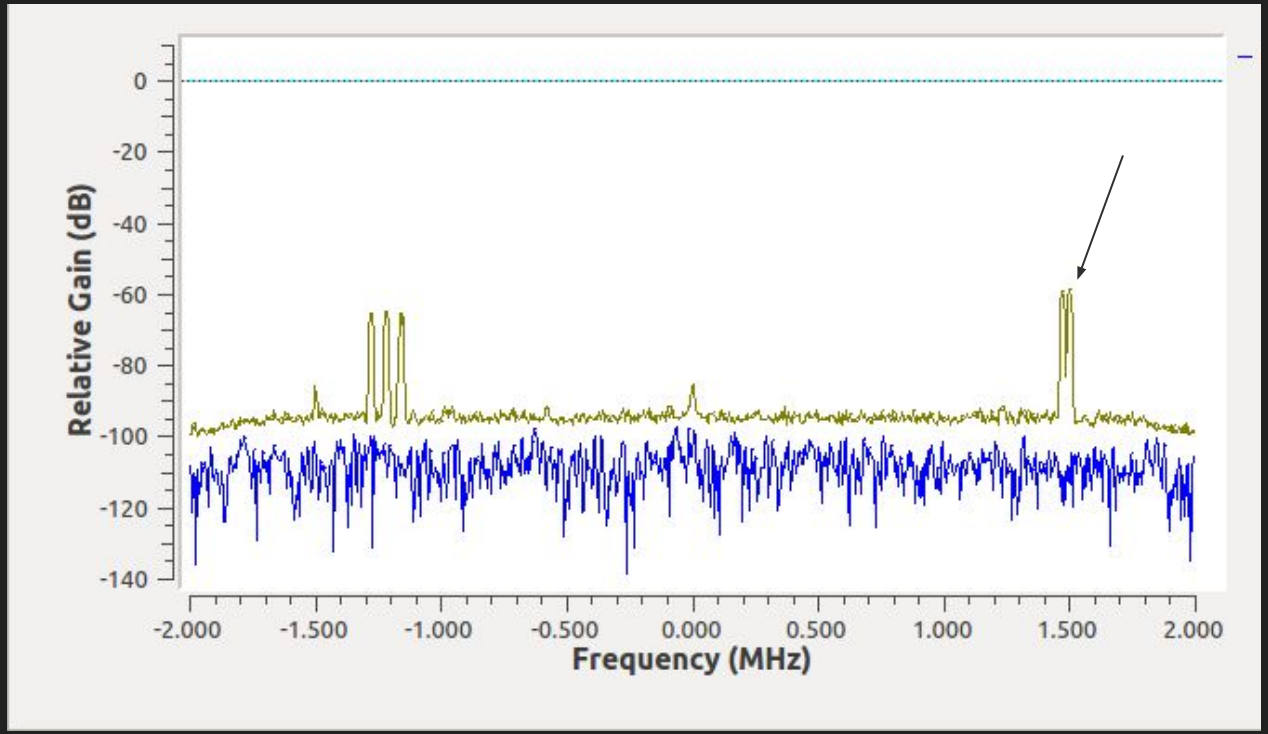
Layer 1: FCC ID Search



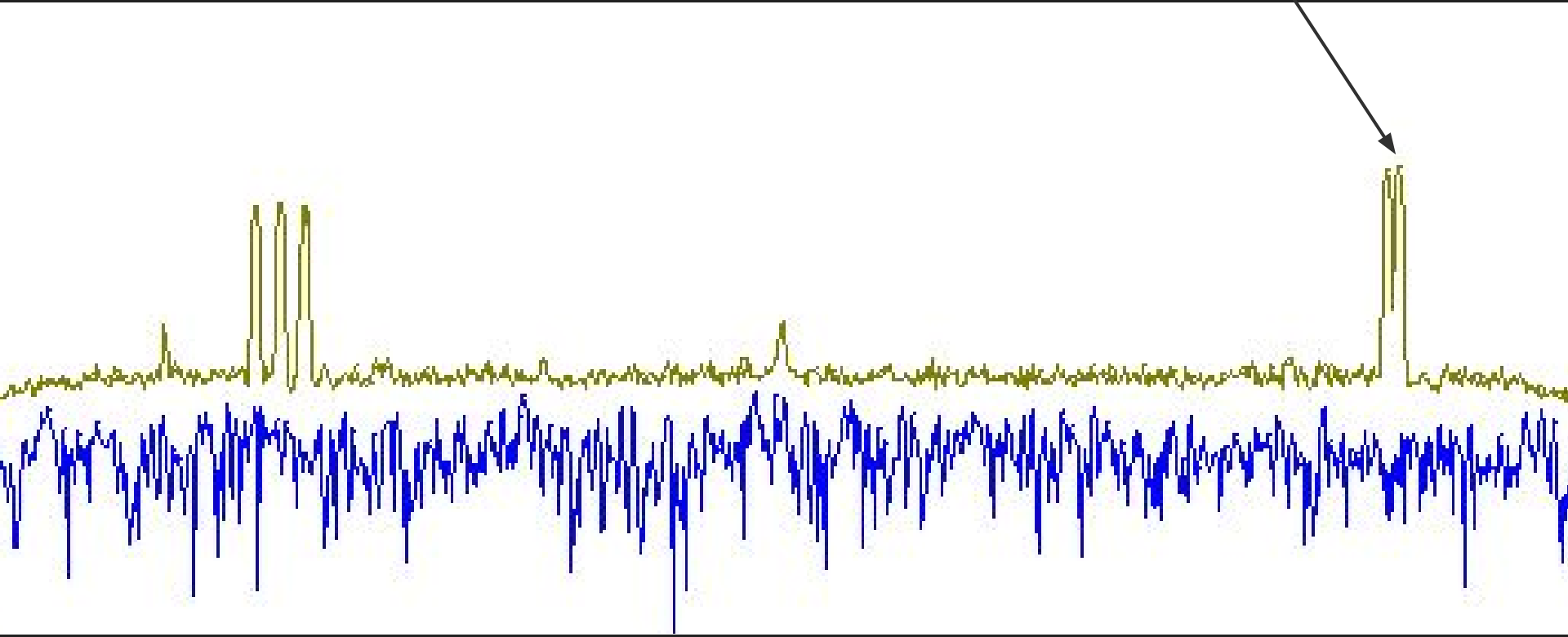
Layer 1: FCC ID Search



Layer 1: Control Channel



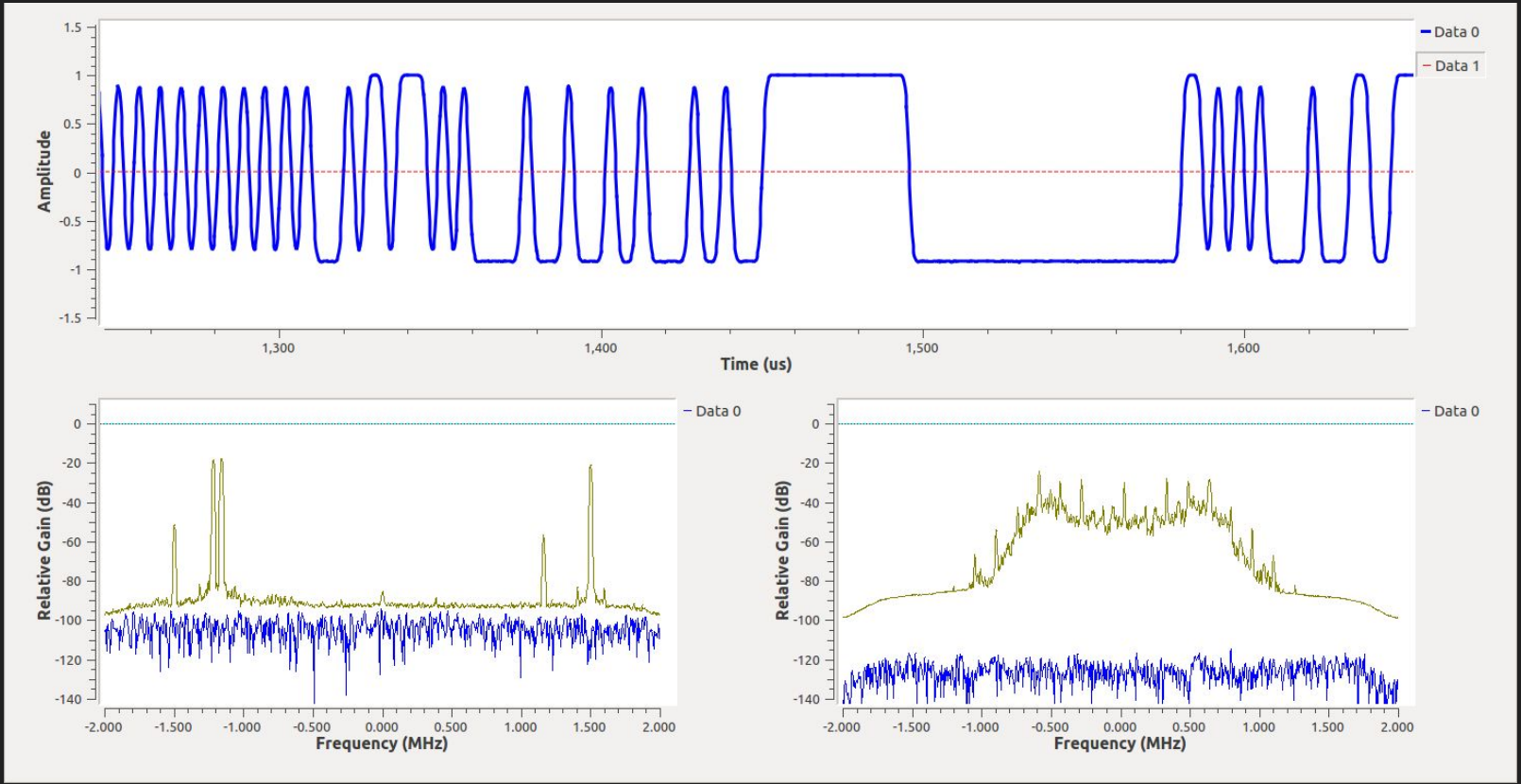
Layer 1: Control Channel



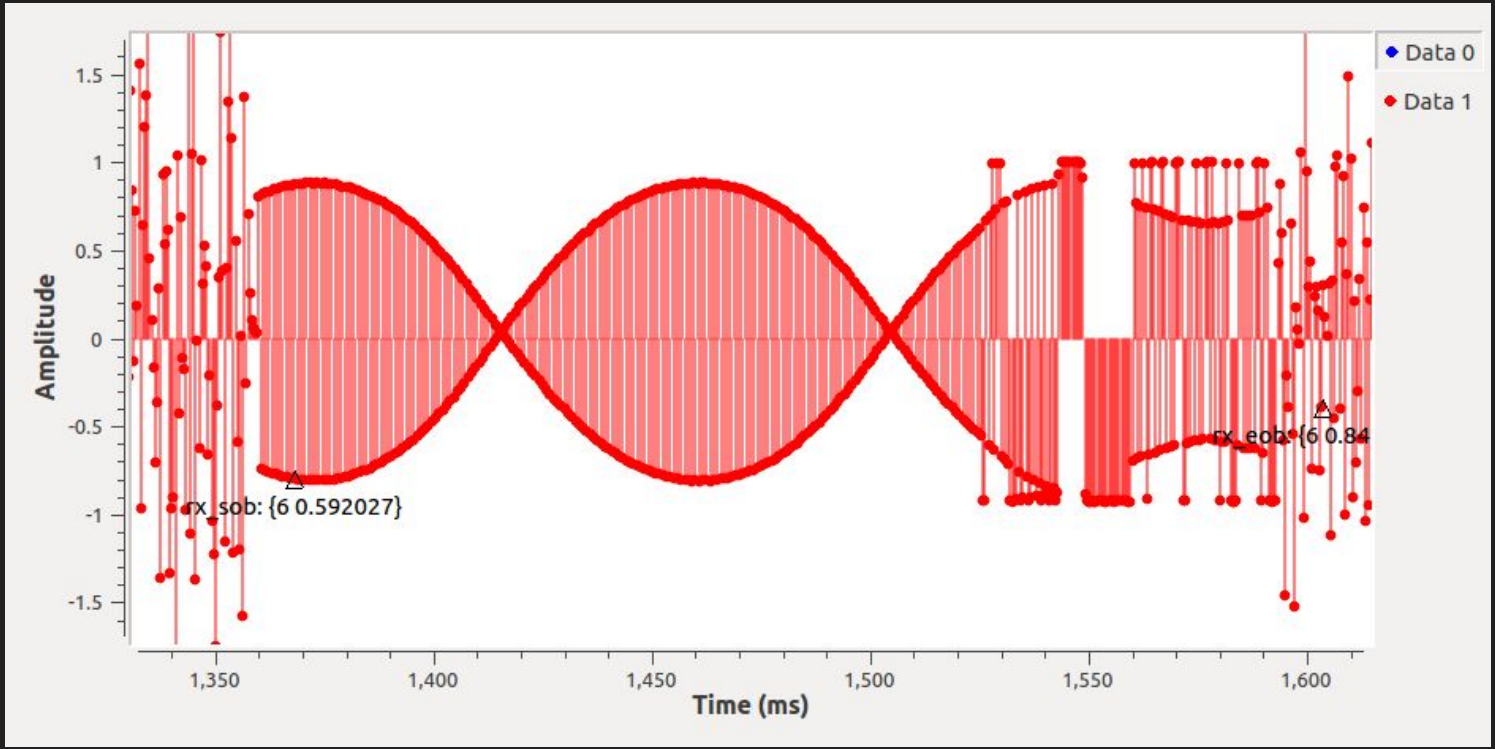
Woody: 1

Tim: 0

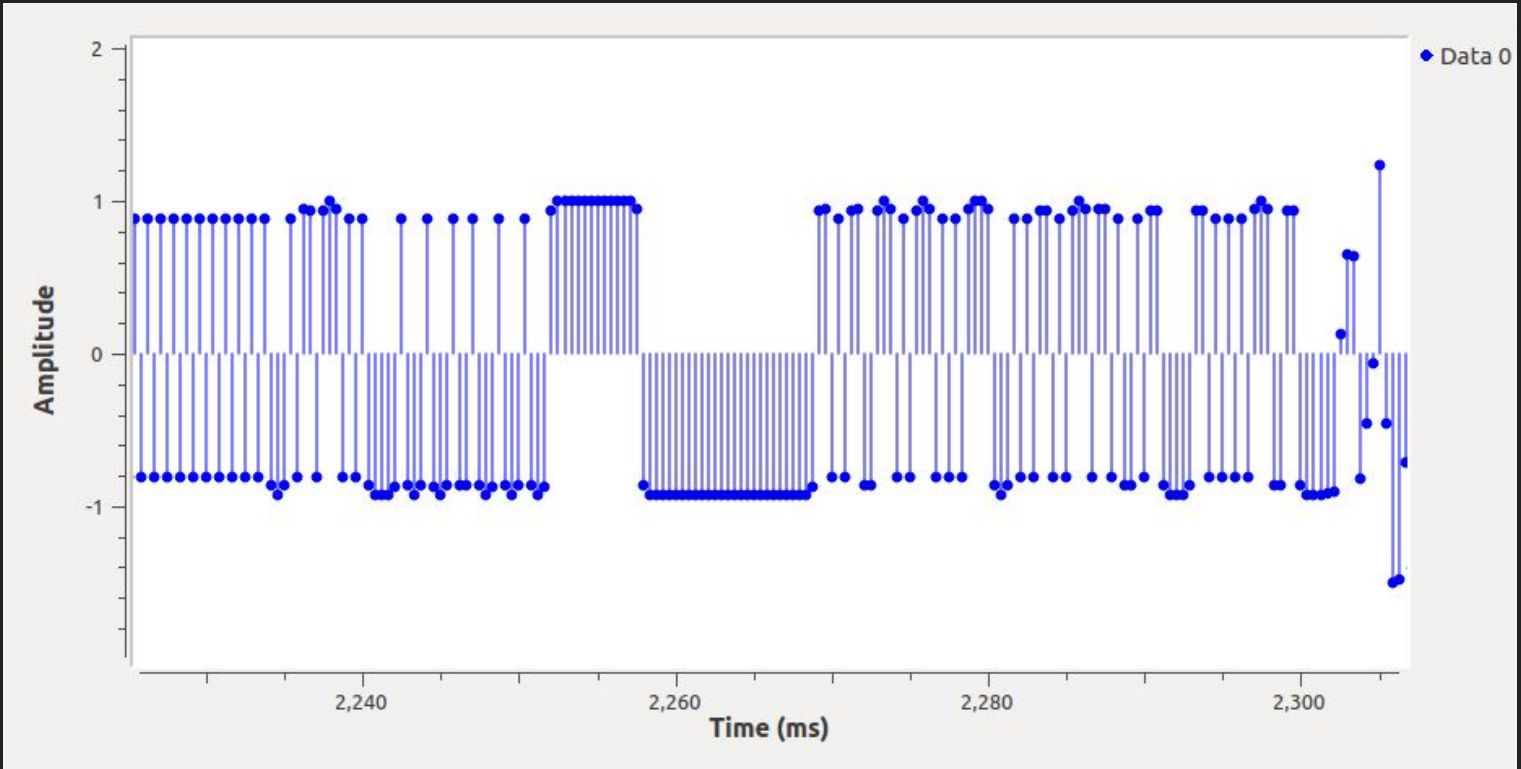
Layer 1: Modulation, Bit Rate



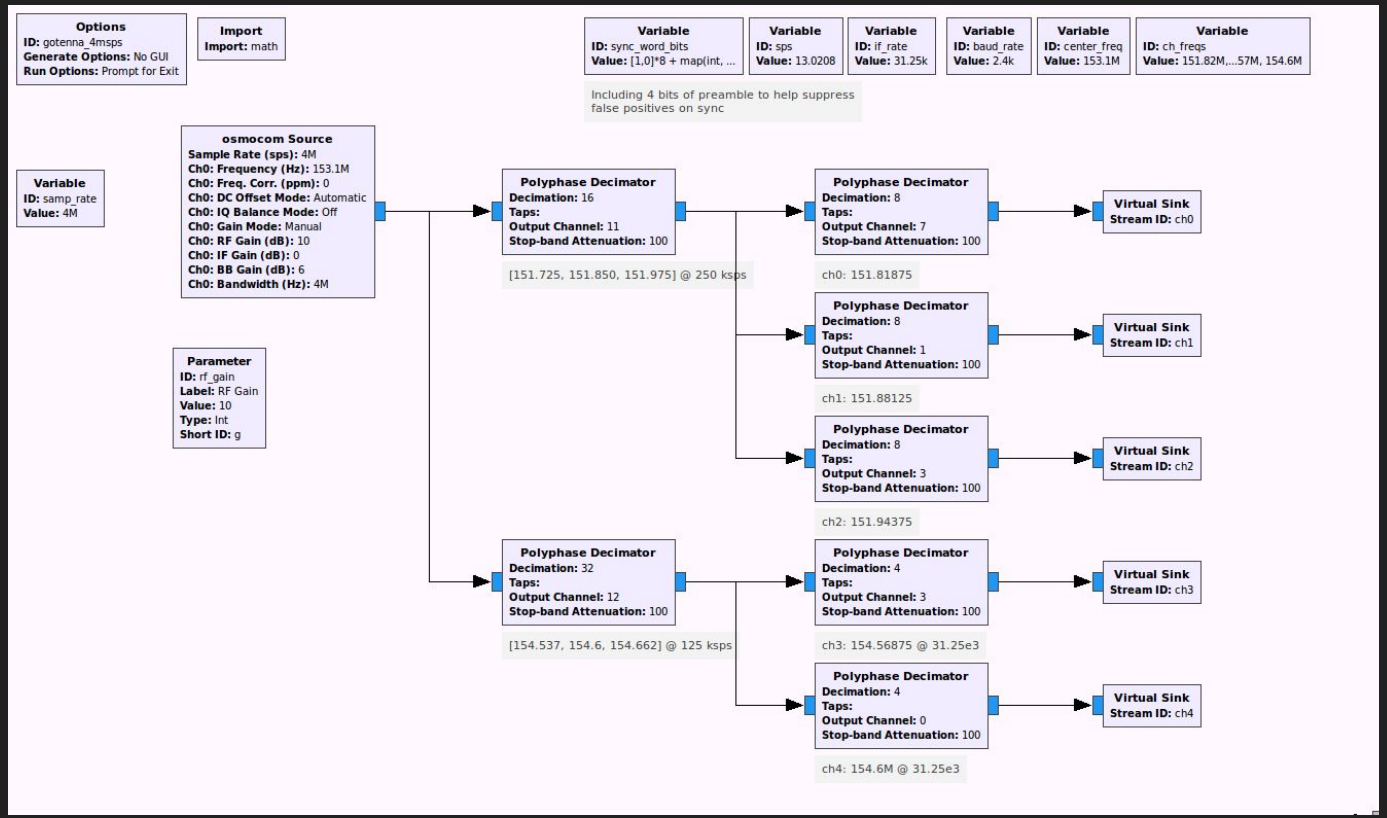
Layer 1 - Bad Clock Recovery



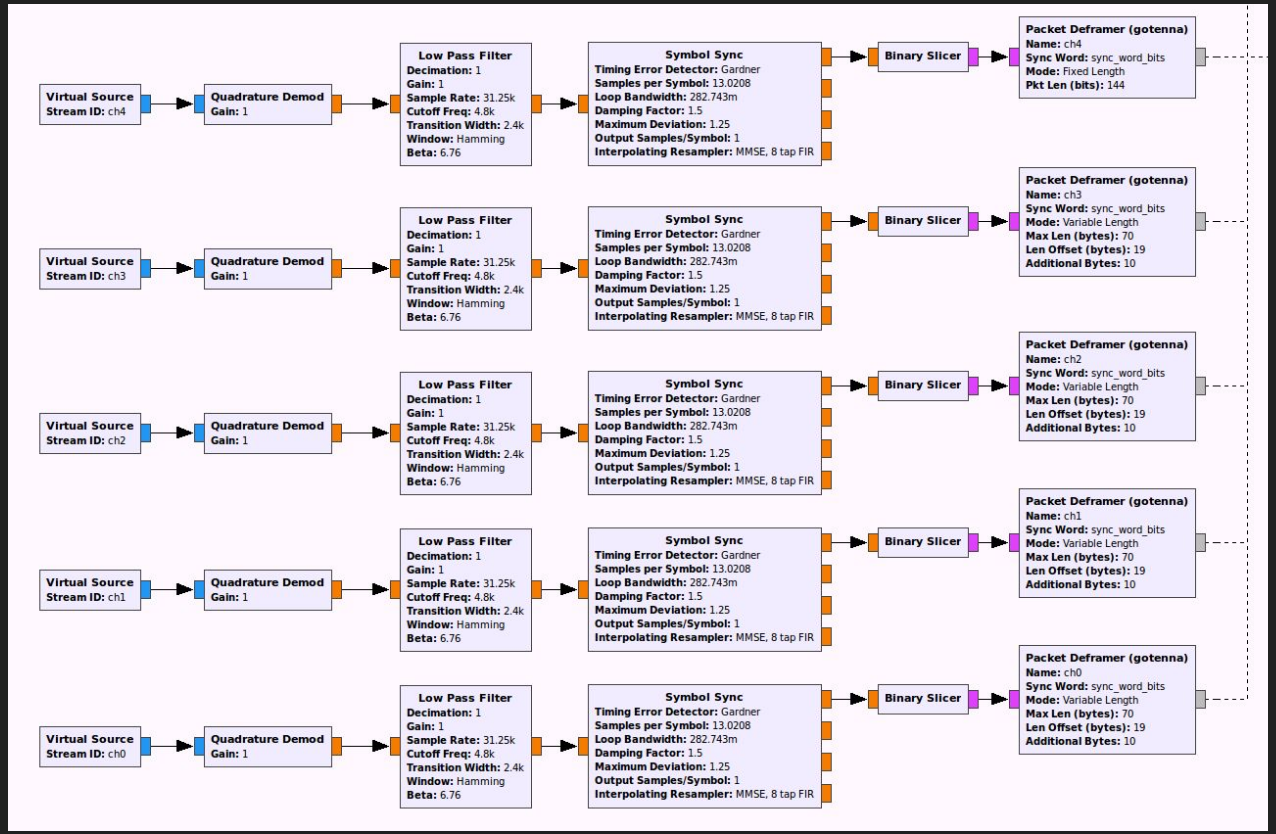
Layer 1 - Clock Recovery (Bits)



Layer 1 - Receiver



Layer 1 - Receiver



Layer 2 - Packets

```
ch4: 11 12 02 3f ff 00 00 00 2f c6 46 c8 4a 0e 4c 43 f9 9c [...]

ch2: 45 02 02 00 01 57 90 20 6f 63 27 fa 77 50 05 40 25 f6
     03 1e fb 0f 00 00 00 58 57 0d fe cd 2b 59 68 1e a2 00
     10 01 01 30 03 01 54 04 03 41 62 63 4c e5 82 2f 87 76
     e6 6b c9 17 6a 8a [...]
```

Layer 2 - Packets

```
         01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11!!
ch4: 11 12 02 3f ff 00 00 00 2f c6 46 c8 4a 0e 4c 43 f9 9c [...]

ch2: 45 02 02 00 01 57 90 20 6f 63 27 fa 77 50 05 40 25 f6
     03 1e fb 0f 00 00 00 58 57 0d fe cd 2b 59 68 1e a2 00
     10 01 01 30 03 01 54 04 03 41 62 63 4c e5 82 2f 87 76
     e6 6b c9 17 6a 8a [...]
```

Layer 2 - Packets

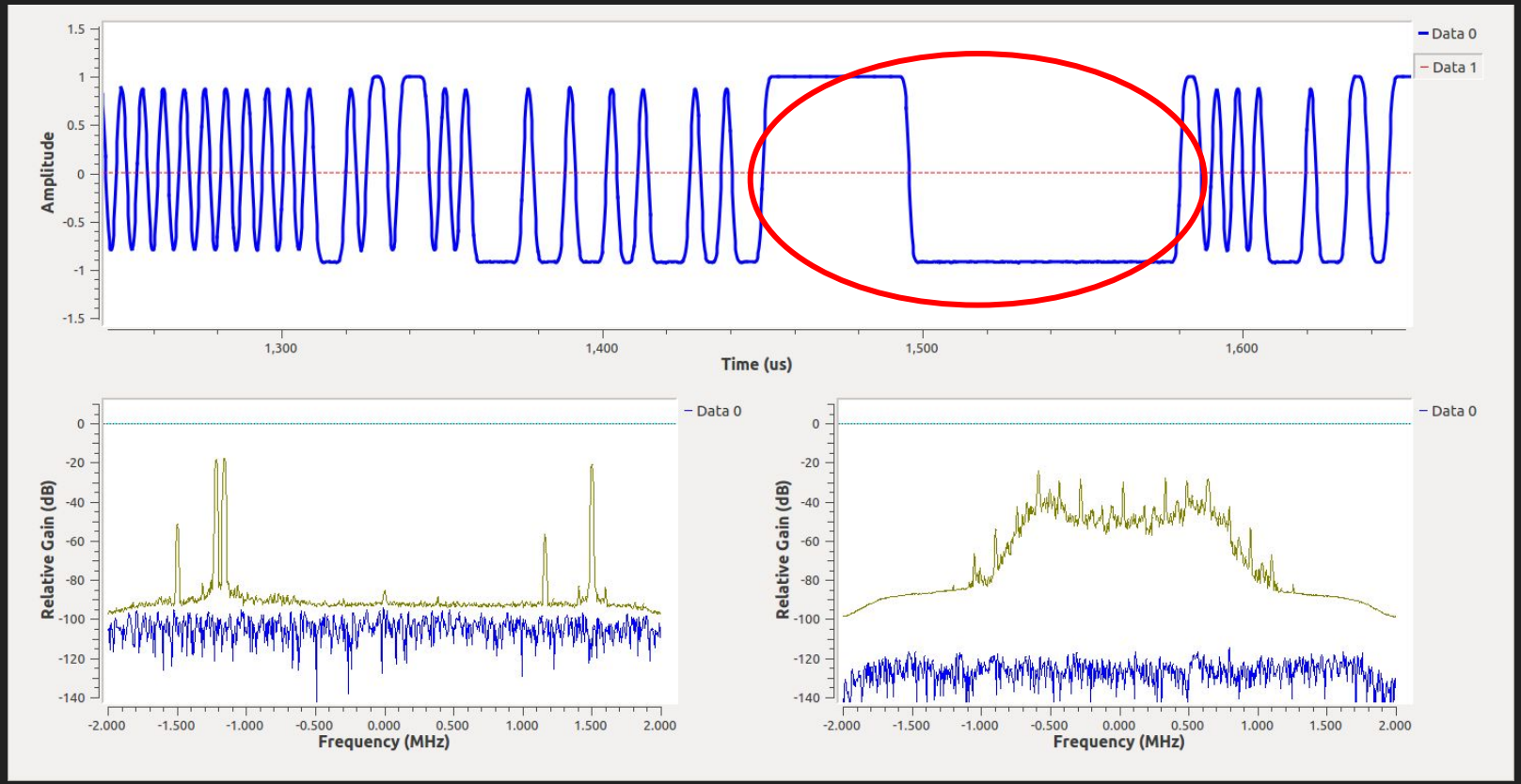
```
         01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11!!
ch4: 11 12 02 3f ff 00 00 00 2f c6 46 c8 4a 0e 4c 43 f9 9c [...]

ch2: 45 02 02 00 01 57 90 20 6f 63 27 fa 77 50 05 40 25 f6
     03 1e fb 0f 00 00 00 58 57 0d fe cd 2b 59 68 1e a2 00
     10 01 01 30 03 01 54 04 03 41 62 63 4c e5 82 2f 87 76
     e6 6b c9 17 6a 8a [...]
```

Layer 2 - Packets

```
45 02 02 00 01 57 90 20 6f 63 27 fa 77 50 05 40 25 f6
03 1e fb 0f 00 00 00 58 57 0d fe cd 2b 59 68 1e a2 00
10 01 01 30 03 01 54 04 03 41 62 63 4c e5 82 2f 87 76
e6 6b c9 17 6a 8a       [ 3|A  b  c ]
```

Layer 1: No FEC / Whitening / Interleaving



Layer 2 - Packet Length

```
45 02 02 00 01 57 90 20 6f 63 27 fa 77 50 05 40 25 f6
03 1e fb 0f 00 00 00 58 57 0d fe cd 2b 59 68 1e a2 00
10 01 01 30 03 01 54 04 03 41 62 63 4c e5 82 2f 87 76
e6 6b c9 17 6a 8a       [ 3|A  b  c ]

45 02 02 00 01 57 90 20 6f 63 27 fa 77 50 05 40 25 f6
03 1f fb 0f 00 00 00 58 57 0d fe cd 2b 59 68 1e a2 00
10 01 01 30 03 01 54 04 04 41 62 63 64 4c e5 82 2f 87
76 e6 6b c9 17 6a 8a    [ 4|A  b  c  d ]
```

Layer 3ish - Addressing / Control

```
ch4: 10 12 20 0d b9 00 00 00 d7 35 7a 0f 35 15 4f f6 6b 6c

ch2: [...]

ch4: 10 12 30 70 3c 00 00 00 90 30 ba 51 97 ed 57 12 43 a1

ch3: [...]
```

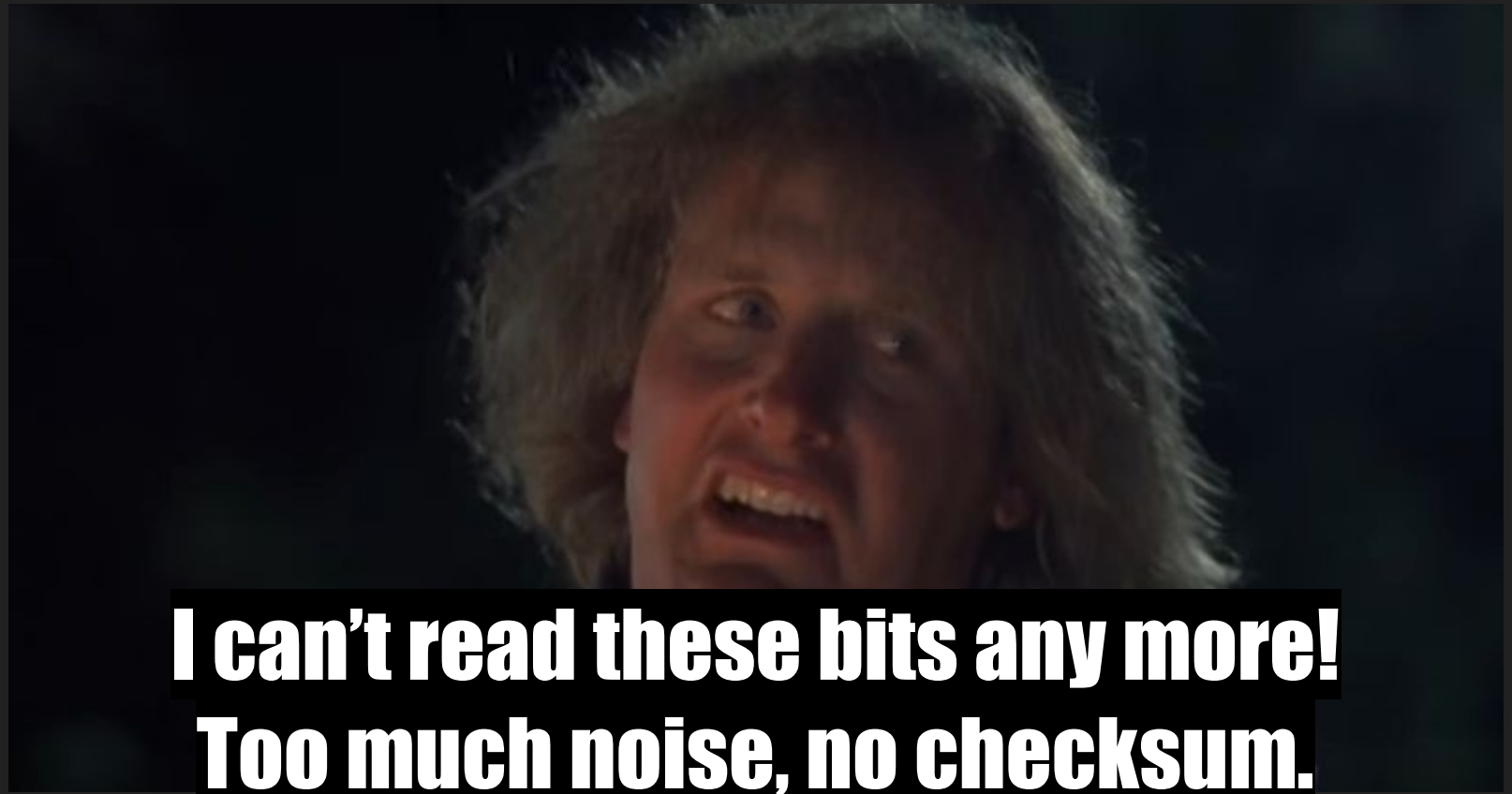
Woody: 2

Tim: 0

Layers 3,4,5 - Conversations

```
ch4 1012202cc200000029baf9f08ead5fdc82c9
ch2 6202f900002cc20093ff5fa1b0eeaeb611f7
ch2 230200ed091ccd0b76538cd1c4789352e41501093fff585e1d510...
ch2 3402f900001ccd000dcb2529e2794c451a22
ch2 45020000011ccd2251de4ae4e625c9c19d070320fb0f010000586...
ch2 56020000001ccd00d68b3a7cd088b8799a4f
```


Tim
Woody


I can’t read these bits any more!
Too much noise, no checksum.


Maybe you should use the UART!


You've had a UART this whole time?


Uh, yeah... /dev/ttyACM0

Woody: 3

Tim: 0

USB Shell - Full Packets

```
[095215-000]  TRX   TX_PDU len :18: packet:
    11 12 02 3f ff 00 00 00 2f c6 46 c8 4a 0e 4c 43 f9 9c

[095471-000]  TRX   TX_PDU len :60: packet:
    45 02 02 00 01 57 90 20 6f 63 27 fa 77 50 05 40 25 f6
    03 1e fb 0f 00 00 00 58 57 0d fe cd 2b 59 68 1e a2 00
    10 01 01 30 03 01 54 04 03 41 62 63 4c e5 82 2f 87 76
    e6 6b c9 17 6a 8a
```

USB Shell - Gotenna ID (GID)

```
[069936-000]  TRX   build preRts hash16=db9
[026467-004]  FLSH  GID stored Successfully. GID len : 14
              GID : 003fff58570dfecd2b000db900

[078369-000]  TRX   TX_PDU len :18: packet:
    10 12 20 0d b9 00 00 00 d7 35 7a 0f 35 15 4f f6 6b 6c

[078756-000]  TRX   TX_PDU len :39: packet:
    23 02 00 54 3e cd 3d 0b cc b0 52 da 75 8e 7e 50 f5 fa
    01 09 3f ff 58 57 0d fe cd 2b 00 cd ab 7f d7 dd 4f 59
    86 4a 31
```

USB Shell - Public Key Exchange

```
[036595-001]  FLSH  Public Key len : 49 Public key :
0237fb02aeb365d273bc3878b0730ad3efd56bb108cf38b22fb737841ab3
833f6f6804fac67c730a5cb0b004ab401c1bd9

[118824-001]  TRX   TX_PDU len :79: packet:
    34 02 f7 00 01 b1 29 33 de 57 78 0c 06 bd ce 7c 30 a8
    02 31 02 37 fb 02 ae b3 65 d2 73 bc 38 78 b0 73 0a d3
    ef d5 6b b1 08 cf 38 b2 2f b7 37 84 1a b3 83 3f 6f 68
    04 fa c6 7c 73 0a 5c b0 b0 04 ab 40 1c 1b d9 67 42 a1
    2b f4 b7 a4 85 b5 b2
```

Layers 3,4,5 - Full Conversation

```
/dev/ttyACM1:10122000db9000000d7357a0f35154ff66b6c

/dev/ttyACM0:6202f500000db900fd495a9775c28c8ddb39

/dev/ttyACM1:230200543ecd3d0bccb052da758e7e50f5fa
             01093fff58570dfecd2b00cdab7fd7dd4f59864a31

/dev/ttyACM0:3402f40000cd3d0002ed3e2bc4db2619465f
```

Layers 3,4,5 - Full Conversation

```
/dev/ttyACM1:Hey, 0db9! Let's talk on channel 2.

/dev/ttyACM0:Yes, this is 0db9!

/dev/ttyACM1:I want to talk to 3fff 58570dfecd2b,
             is that you? (Also, I need your key.)

/dev/ttyACM0:Yeah, go ahead. (Here's my key.)
```

Layers 3,4,5 - Full Conversation

```
/dev/ttyACM1:4502000001cd3d1ff7458d48e3780e22e48f
             031dfb0f010000584dc0228ada59681eba00
             0abbecb2642d06420f41a7f65378651020e0
             4242a53b99

/dev/ttyACM0:5612000000cd3d00a095a374966763e37ac5
```

Layers 3,4,5 - Full Conversation

/dev/ttyACM1:Here's the data, from 584dc0228ada

/dev/ttyACM0:Yup, I got it. Thanks.

Layer 2 - Whoops, forgot this!

```
/dev/ttyACM1:1012200db9000000d7357a0f35154ff66b6c

/dev/ttyACM0:6202f500000db900fd495a9775c28c8ddb39

/dev/ttyACM1:230200543ecd3d0bccb052da758e7e50f5fa0109[...]

/dev/ttyACM0:3402f40000cd3d0002ed3e2bc4db2619465f0231[...]

/dev/ttyACM1:4502000001cd3d48bf894483762eb1a2ea9703xx[...]
/dev/ttyACM1:4502000002cd3d05bd3ccd2b8aae732edd9603xx[...]

/dev/ttyACM0:5612000000cd3d00a095a374966763e37ac5
```

Layer 6 - Understanding the GID

GID: 9722 1020 3040 50

Hex: 58 6C 08 61 42 B2

Layer 6 - Understanding the GID

GID: 9722 1020 3040 50

Hex: 58:6C:08:61:42:32

Layer 6 - Understanding the GID

GID: 9722 1020 3040 50

Hex: 58 6C 08 61 42 B2

Layer 6 - Understanding the GID

GID: (757) 555-1234

Hex: 00 01 C3 89 BD 02

Layer 6 - Understanding the GID

GID: (757) 555-1234

Hex: 00 01 C3 89 BD 02

GID: 9722 1020 3040 50

Hex: 58 6C 08 61 42 B2

Layer 6 - Understanding the GID

GID: 9722 1020 3040 50

Hex: 58 6C 08 61 42 B2

Layer 6 - Understanding the GID

Date: 7/22 10:20:30.4050

GID: 9722 1020 3040 50

Hex: 58 6C 08 61 42 B2

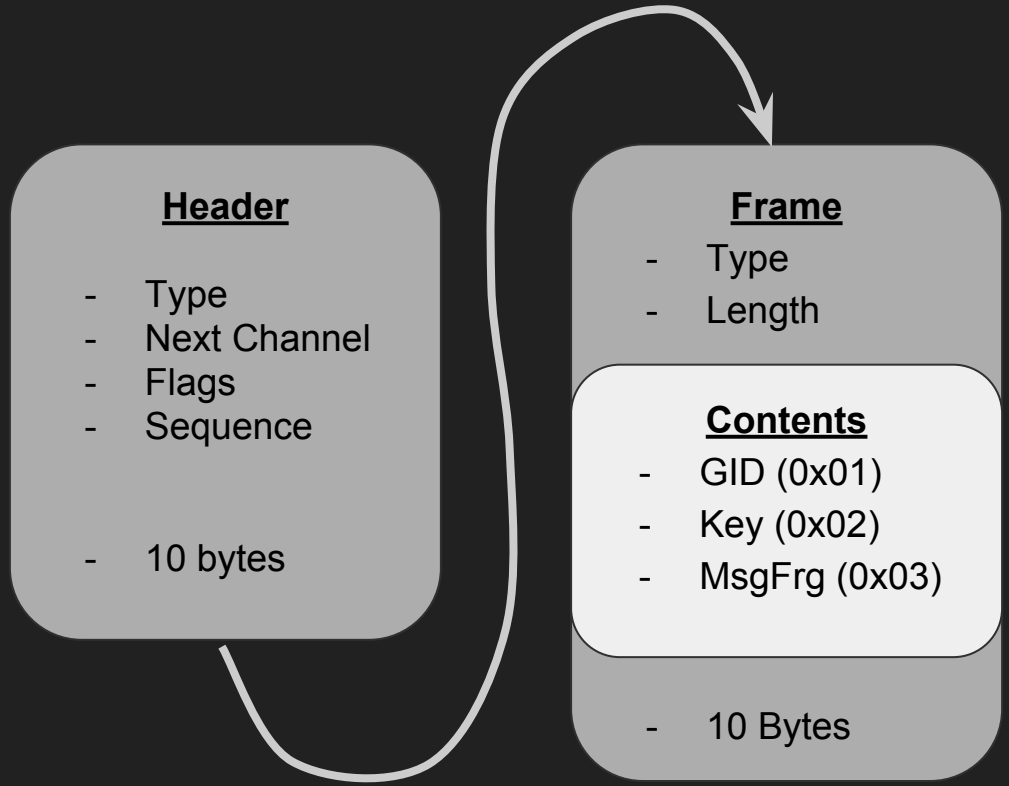
Woody: 4

Tim: 0

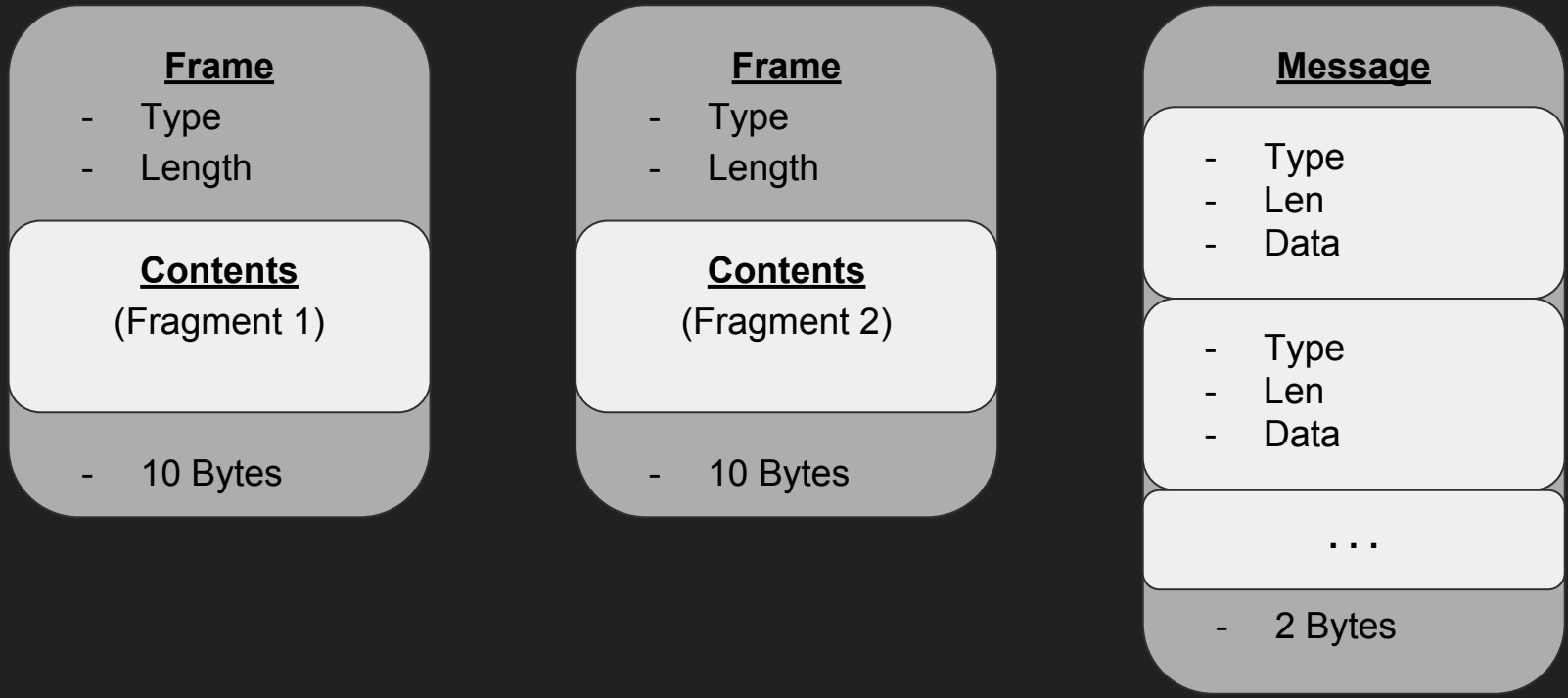
A Visit to the Crazy Wall

A Visit to the Crazy Wall

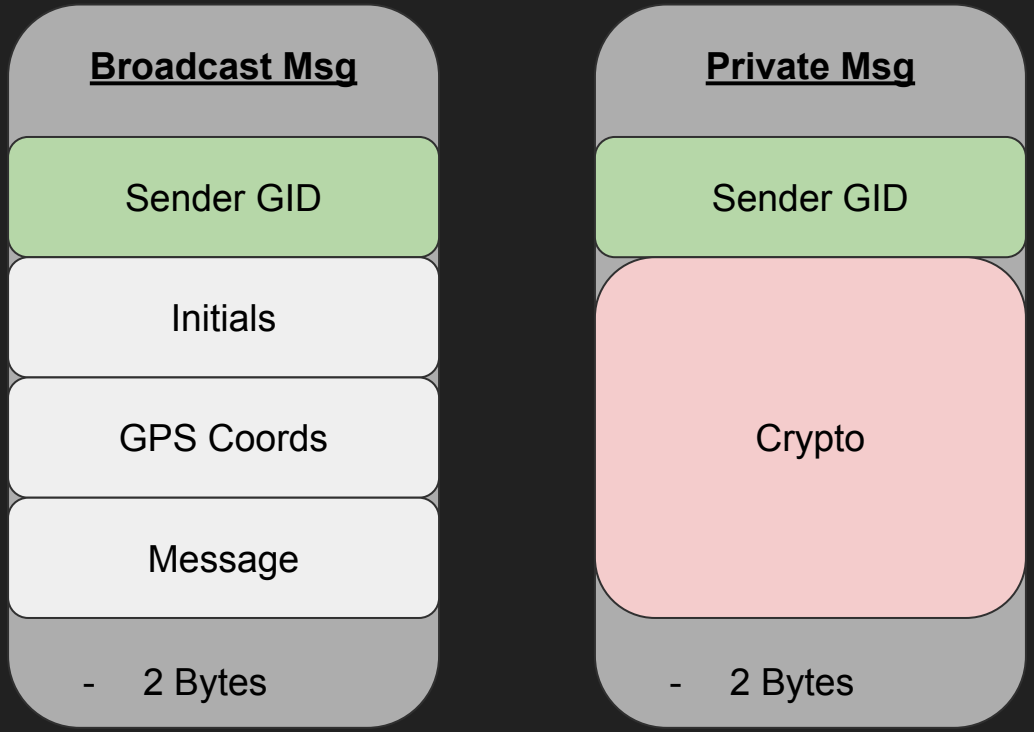
Teh Scapy


Header
- Type
- Next Channel
- Flags
- Sequence
- 10 bytes
Frame
- Type
- Length
Contents
- GID (0x01)
- Key (0x02)
- MsgFrg (0x03)
- 10 Bytes

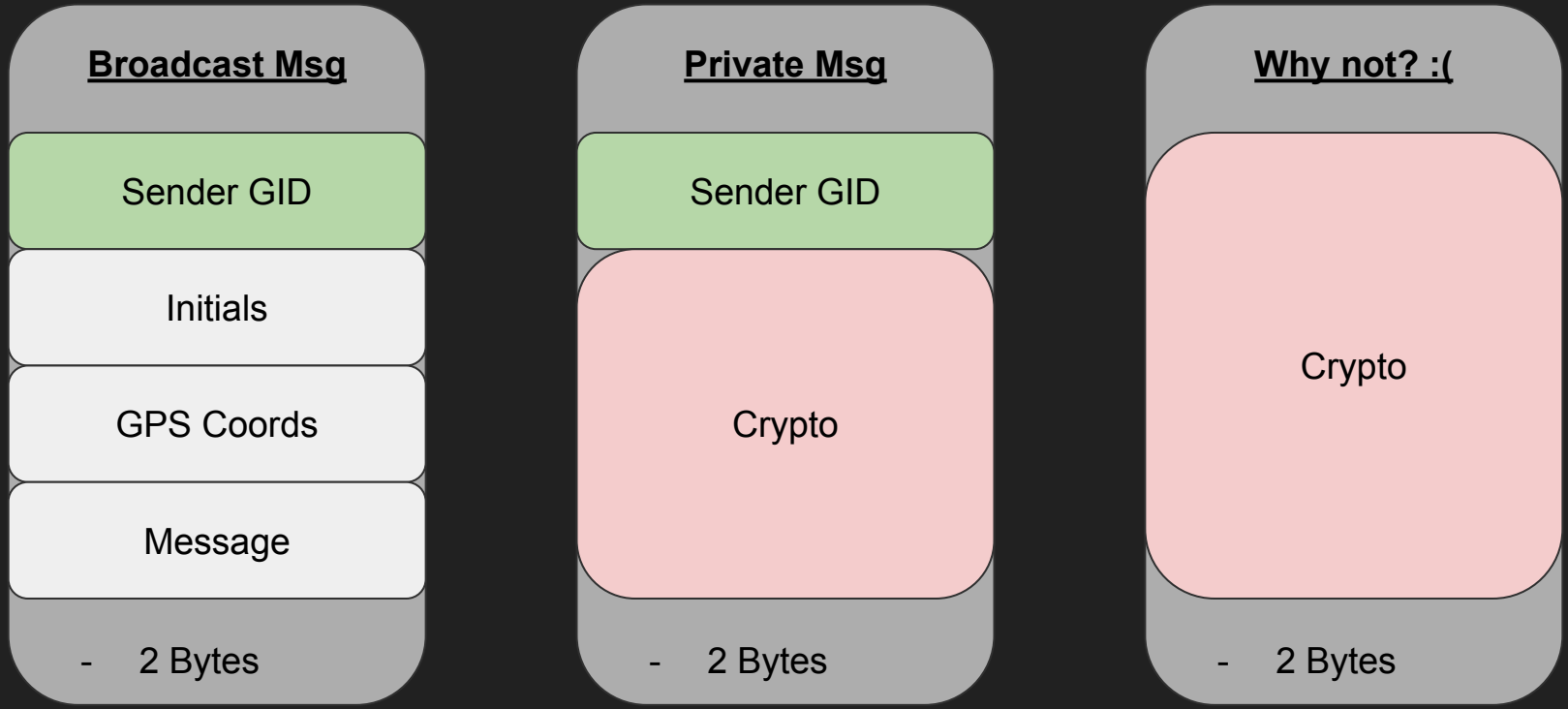
Teh Scapy


Frame
- Type
- Length
Contents
(Fragment 1)
- 10 Bytes
Frame
- Type
- Length
Contents
(Fragment 2)
- 10 Bytes
Message
- Type
- Len
- Data
- Type
- Len
- Data
. . .
- 2 Bytes

Broadcast vs. Encrypted



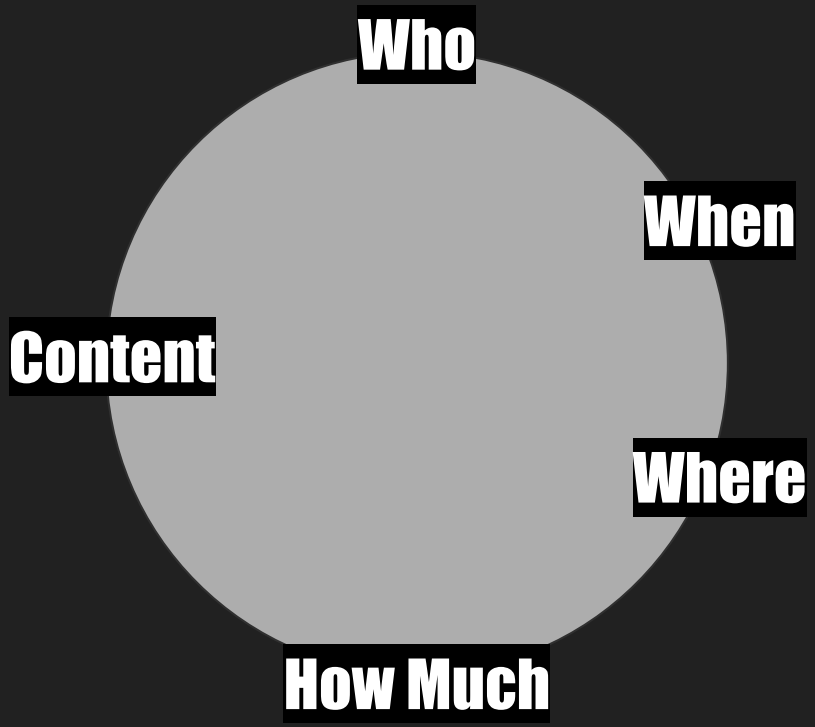
...but why not encrypt the GID?



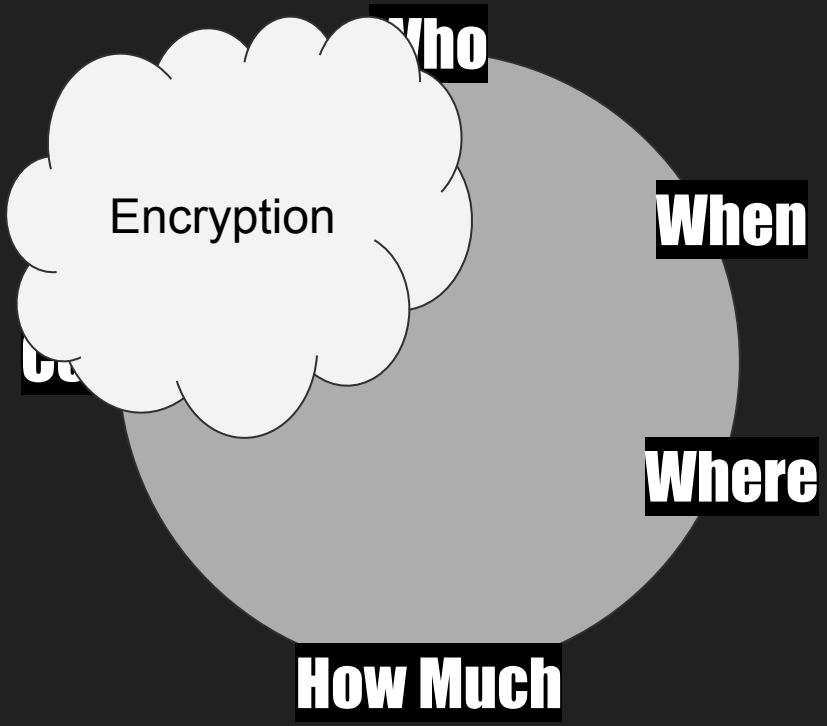
Sauron

- Have to follow state of channel
- For bcasts, don’t know when the end-of-packet has arrived
  - Wait 10 seconds, or wait for next TX on channel
- For m2m, might get caught up with sequence rebroadcasts
- Still no checksum, oww
- Out of range problem

The Meta-Data Circle



The Meta-Data Circle



The Meta-Data Circle

Responsible Disclosure

- Gotenna Response:
  - Never promised anonymity, only encryption
  - “Outside” vs “Inside” of the Envelope
  - Allows the user to regenerate GID on demand
  - Development focus on mesh network
  - Plan is eventually encrypt all metadata

- Our Thoughts:
  - Difficult to get away from “when”, “where”, and “how much”
  - Crypto can obscure “what”, protocol can hide “who”
  - Who is kinda big tho - “We kill people based on metadata”
  - True privacy means encrypting metadata
  - **Shouldn’t be difficult to hide “from” field**

The Verdict on GoTenna

- Sad they aren’t encrypting all metadata
- Glad they’re encrypting the rest
- Glad they let you use random ID’s
- Glad they’re responsive
- Glad they exist
- More transparency? <3

Further Work

- Checksum!!!
- Crypto Study
- Group Chat
- Emergency Broadcasts
- Understand unknown fields
- Understand bad / corrupted packet sequence
- Transmit Side! Fuzzing! (Maybe)
- Shore up GNU Radio

Conclusion: What Worked? (Tools)

- Simple tools: grep, cut, sort, gedit, gnome-calculator
- Know your formats (int, short, char, float, double, hex, binary)
- Google Hacking!
- Automate: Packets > Audacity

Conclusion: What Worked? (Meatspace)

- Understand how people communicate
- Try before you pry!
- Change one thing at a time
- Hold onto your assumptions gently-ish
- CRAZY WALLS = <3
- Progress is exponential, persistence pays off

DEFCON2017

15% off, thru midnight Aug 6th

Gotenna RE

Woody (@tb69rr)
Tim (@bjt2n3904)