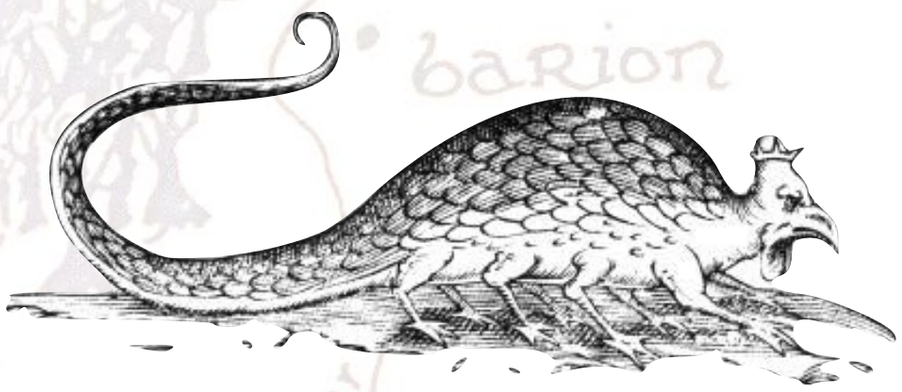
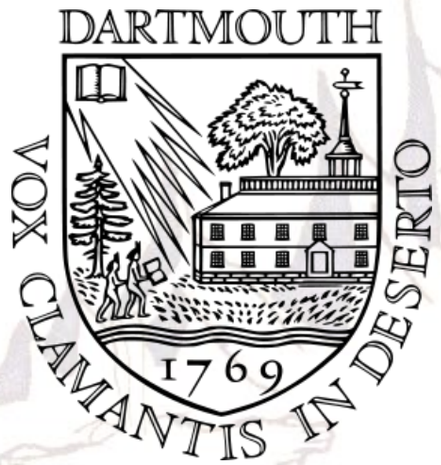
A Fillory of PHY

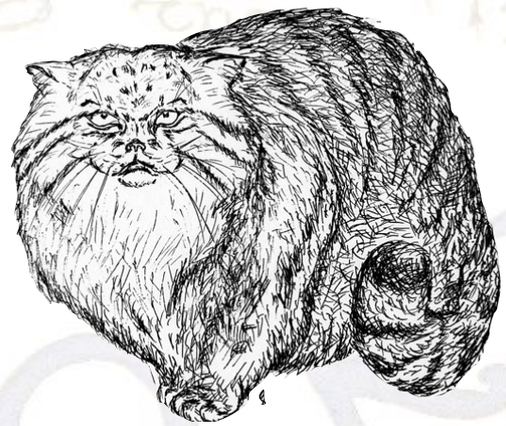
Sergey Bratus, Travis Goodspeed, Ange Albertini,
Debanjum S. Solanky

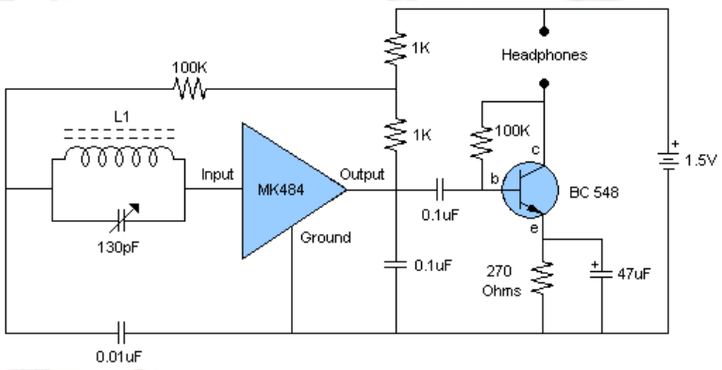


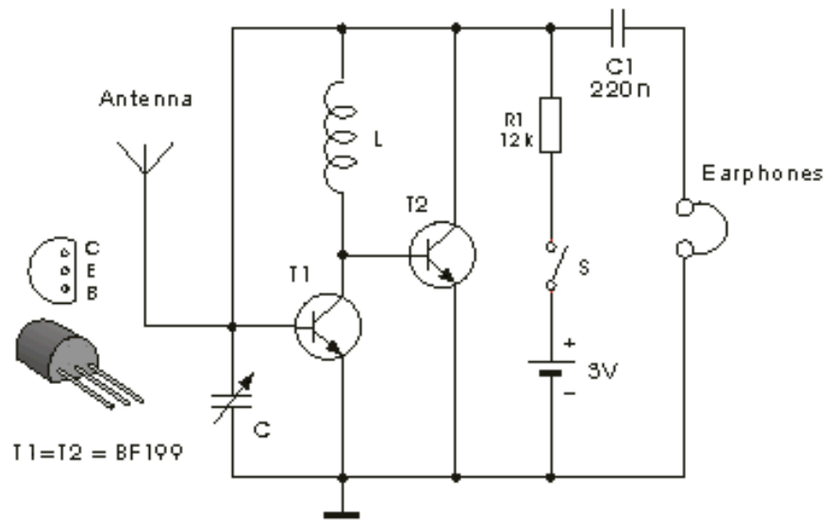


PHY gap?

?



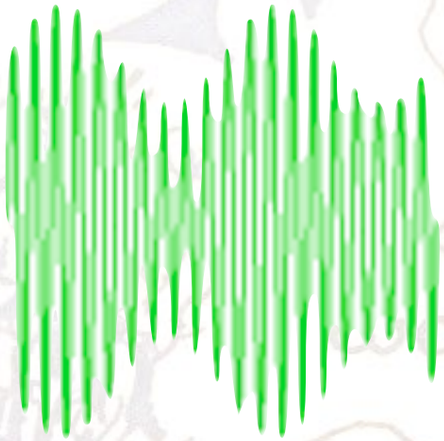


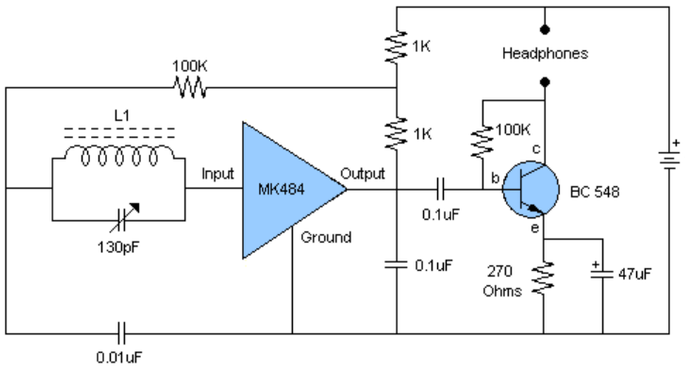


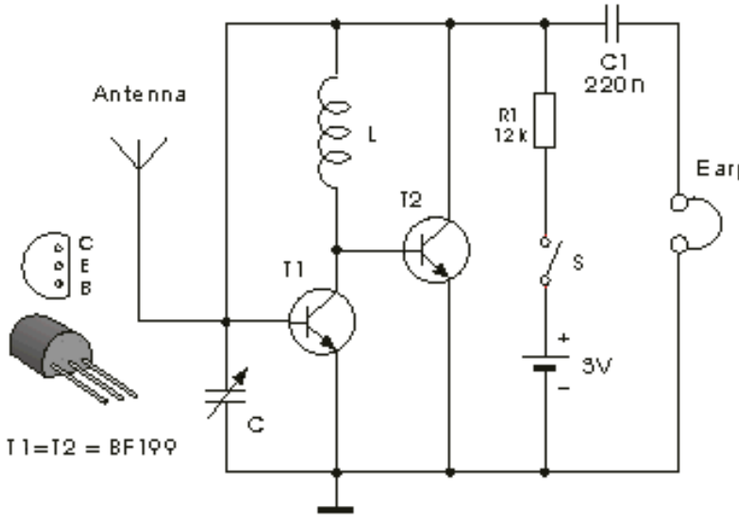
PHY1

PHY2

PHY Chimera?




100K
1K
Headphones
L1
1K
100K
c
b
e
BC 548
1.5V
Input
MK484
Output
0.1uF
130pF
Ground
0.1uF
270
Ohms
47uF
0.01uF


Antenna
L
C1
220n
R1
12k
Earphones
T2
C
E
B
T1
S
+
3V
–
C
T1=T2 = BF199

Outline

- How did we get here
- Cross-talking PHYs and where to find them
- A periodic table of PHY?

Packet-in-packet (WOOT 2012)

```
cumberland% goodfet.ccspi sniff | head
Listening as 00deadbeef on 2405 MHz
# DEBUG Clearing overflow
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff
# 2f 01 08 82 de ff ff ff de ad be ef ba be c0 00 00 00 00 a7 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff ff ff

cumberland% goodfet.ccspi bsniff | head
Listening as 00deadbeef on 2405 MHz
# 19 01 08 b2 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 ed 48 ff
# 19 01 08 b3 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 1f 00 0b 00 00 00 d9 5e ff
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 1e
# 19 01 08 bb ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 f0 cc 6b
# 0f 01 08 82 ff ff ff ff de ad be ef ba be c0 ff 00
# 0f 01 08 bf ff ff ff ff 4d 7d 09 00 1f 00 61 13 52
# 19 01 08 cd ff ff ff ff 28 7d 0a 92 99 08 76 00 00 00 17 00 0b 00 00 00 50 7f 6b
# 19 01 08 d5 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 0f 00 0b 00 00 00 3a c6 0f
# 19 01 08 d6 ff ff ff ff 28 7d 0a 02 00 00 00 00 00 00 17 00 0b 00 00 00 66 fb ff
```

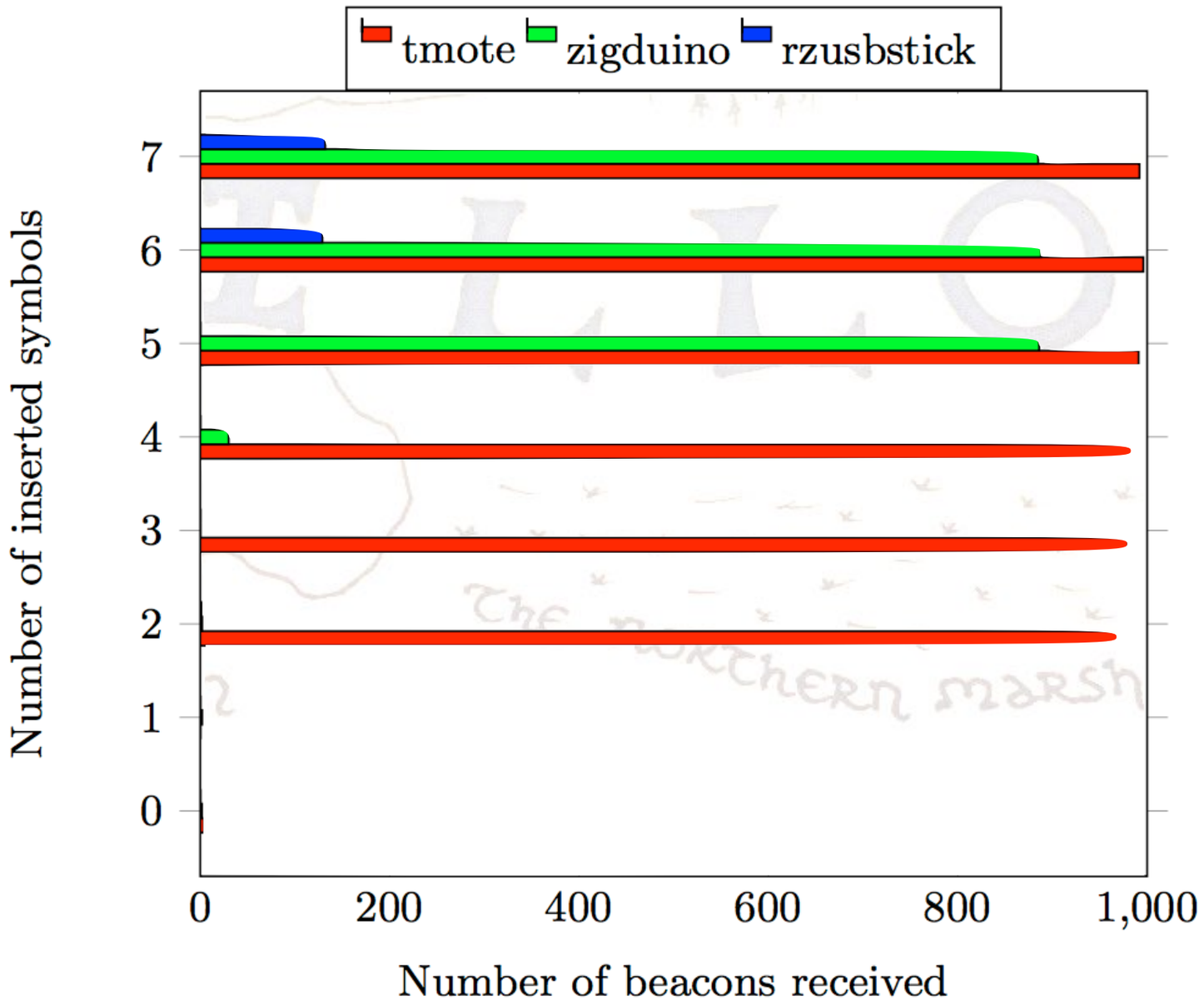
Those are slower than normal packets & mixed into normal shift, so result is from missed SFD, not stop/start.

Packet-in-packet obstructed

- 802.11: **b** switches rates, **g** switches modulation mid-frame
- Whitening: 7-bit LFSR state is unknown
- Illegal strings (bypassable in 802.15.4)
- Encryption: can't predict bits on air from payload

"PHY dialects, shaped charges"

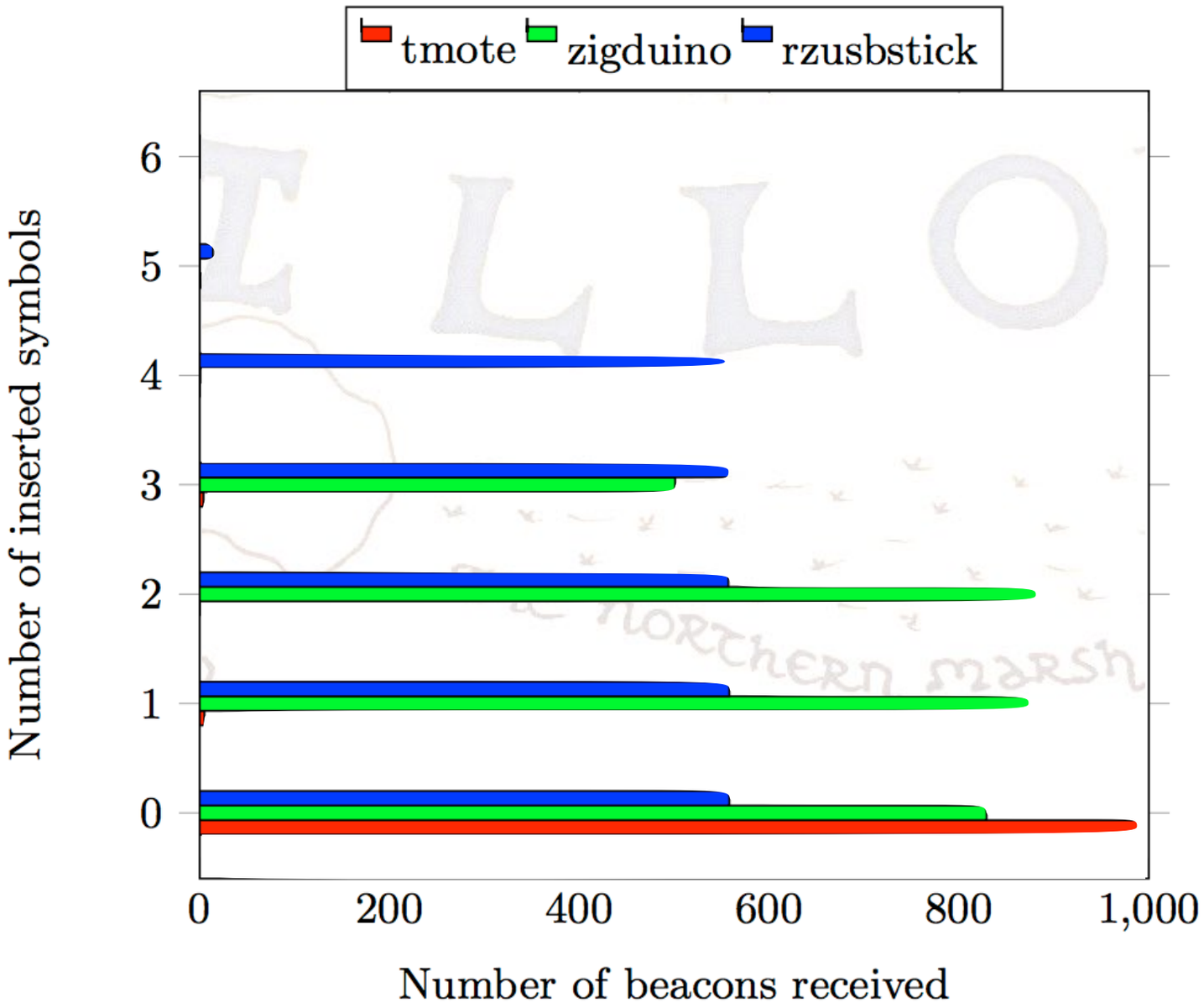
Variable Preamble	SFD	Length	Payload



"PHY dialects, shaped charges"

0x0s	0xFs	SFD	Length	Payload

Preamble	0xFs	SFD	Length	Payload



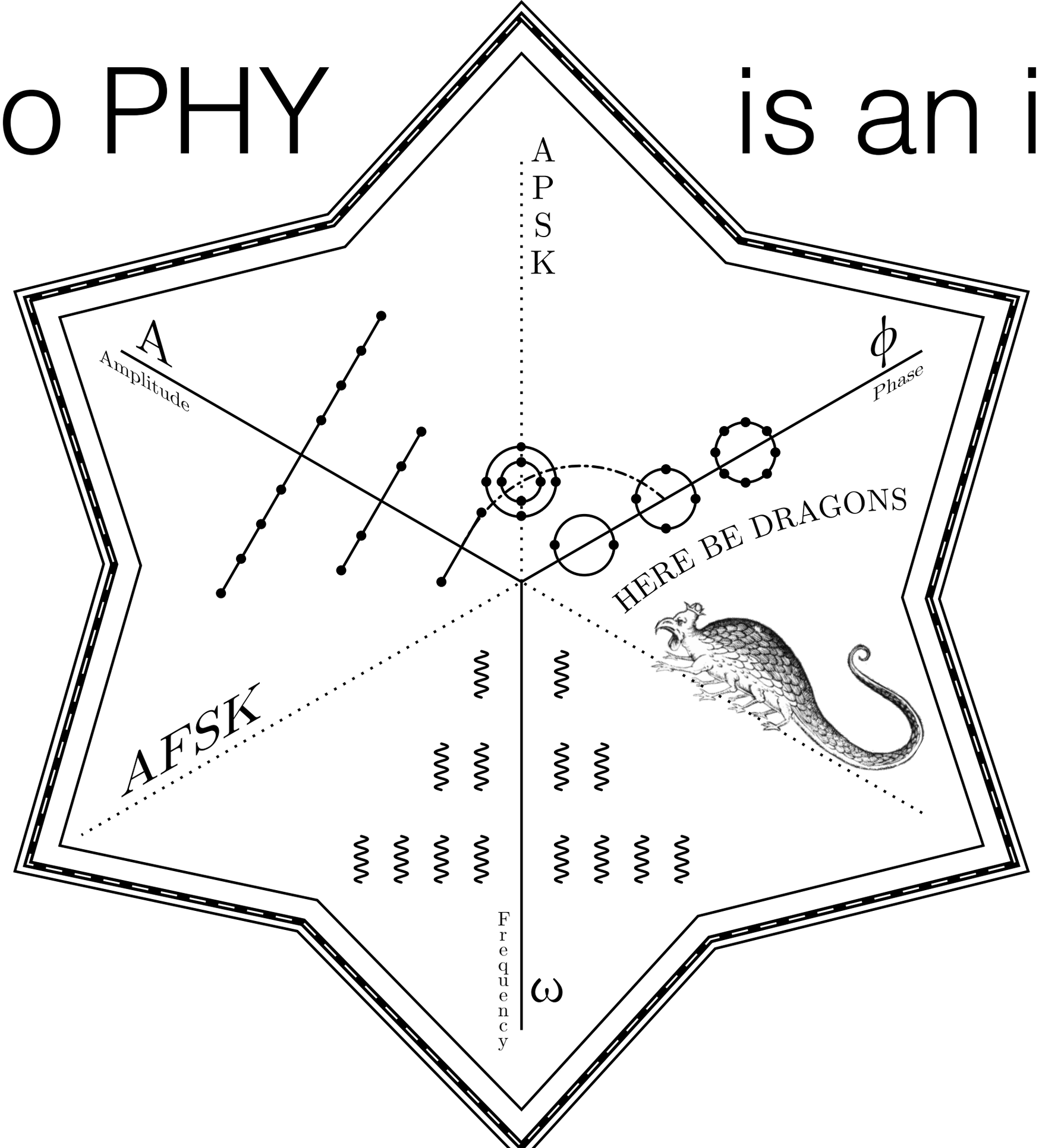
PHY Surprises

- Frame received may look nothing like the frame transmitted
- Not even share a single byte! (*"1/8th of a nybble"*)

PHY Surprises

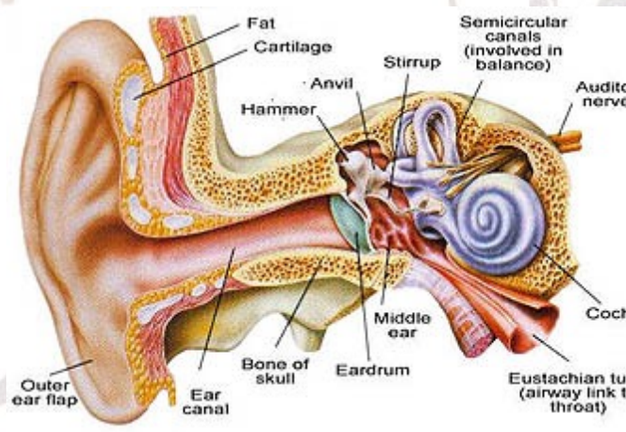
- Frame received may look nothing like the frame transmitted
  - Not even share a single byte! (*"1/8th of a nybble"*)
- Signal received may be from another PHY entirely!
  - PHYs can cross-talk & cross-inject

No PHY is an island

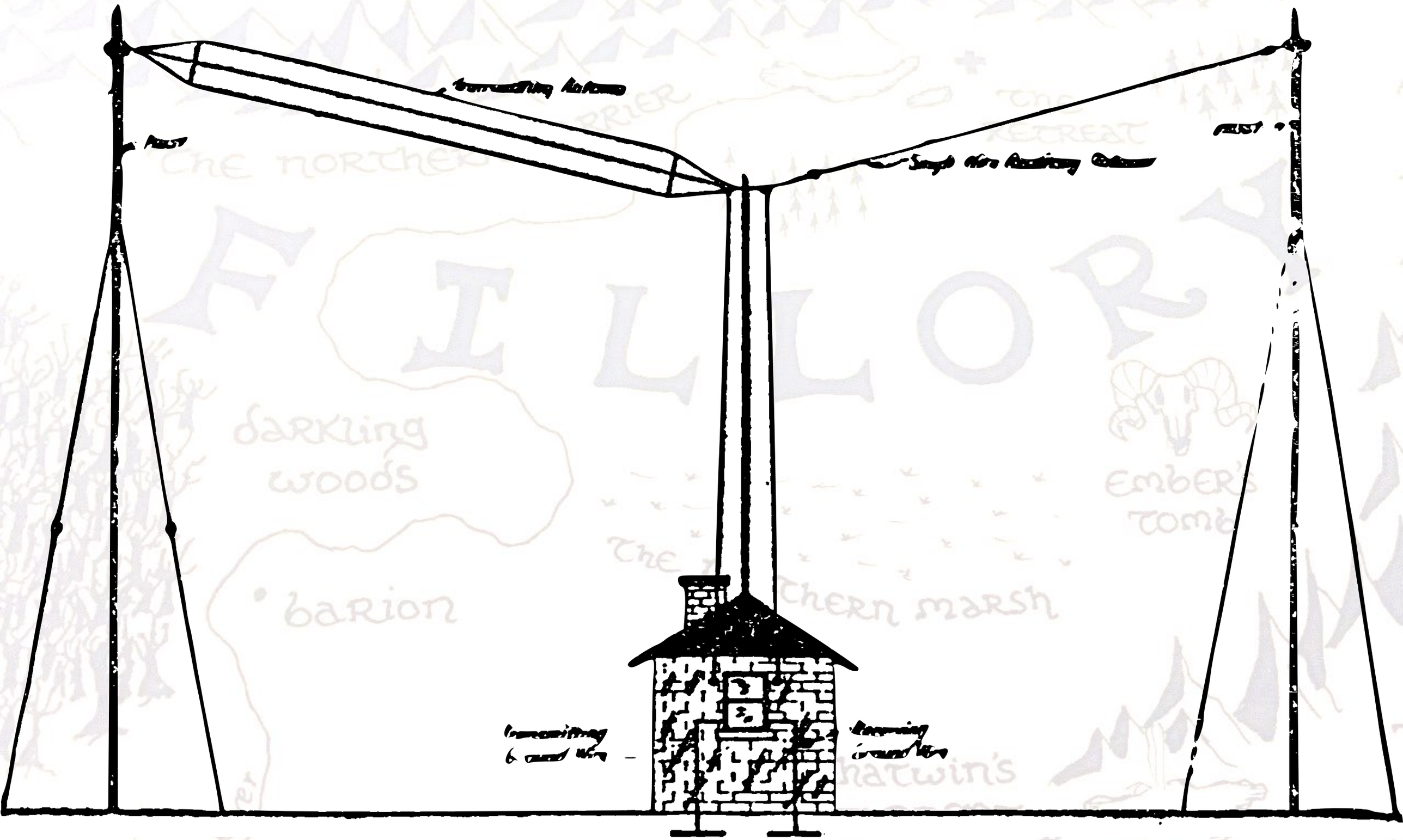


A Mathematician and a Ham walk into a bar

- **A(t) * sin(ω(t) + ϕ(t))** for some choice of A, ω, ϕ
- Radio Spectrum **downshifted** to Audio frequency
- FSK or PSK
  - The frequency or the phase changes
- Low data rate
  - The signal must fit in an audio channel

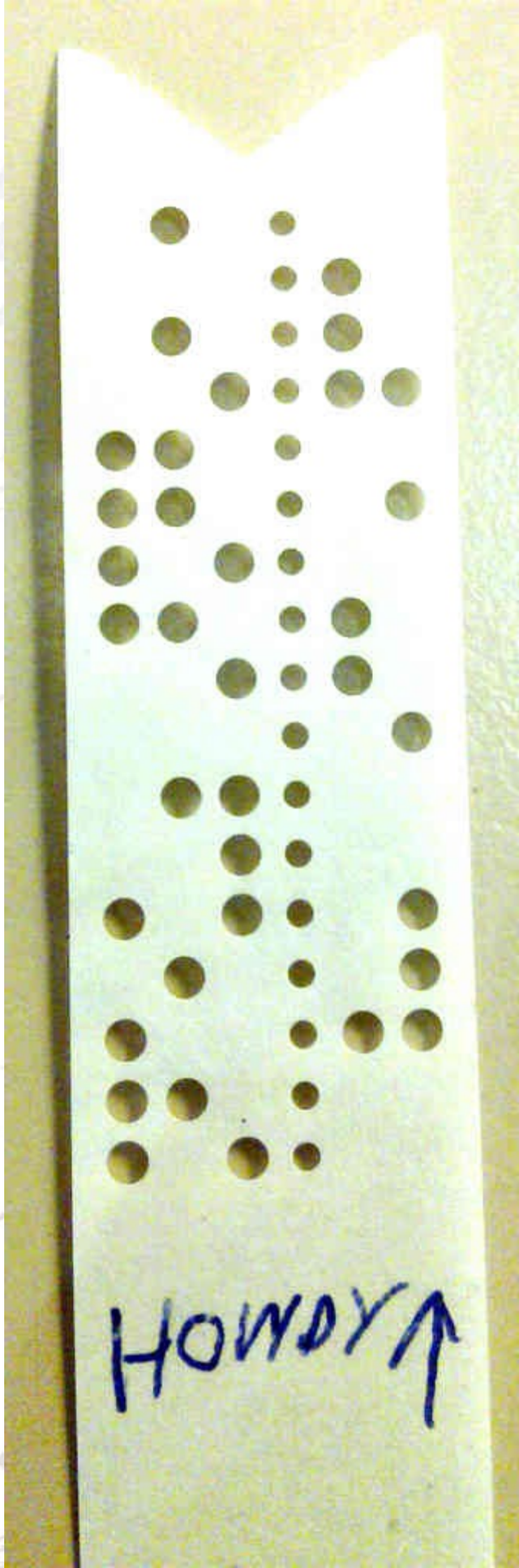


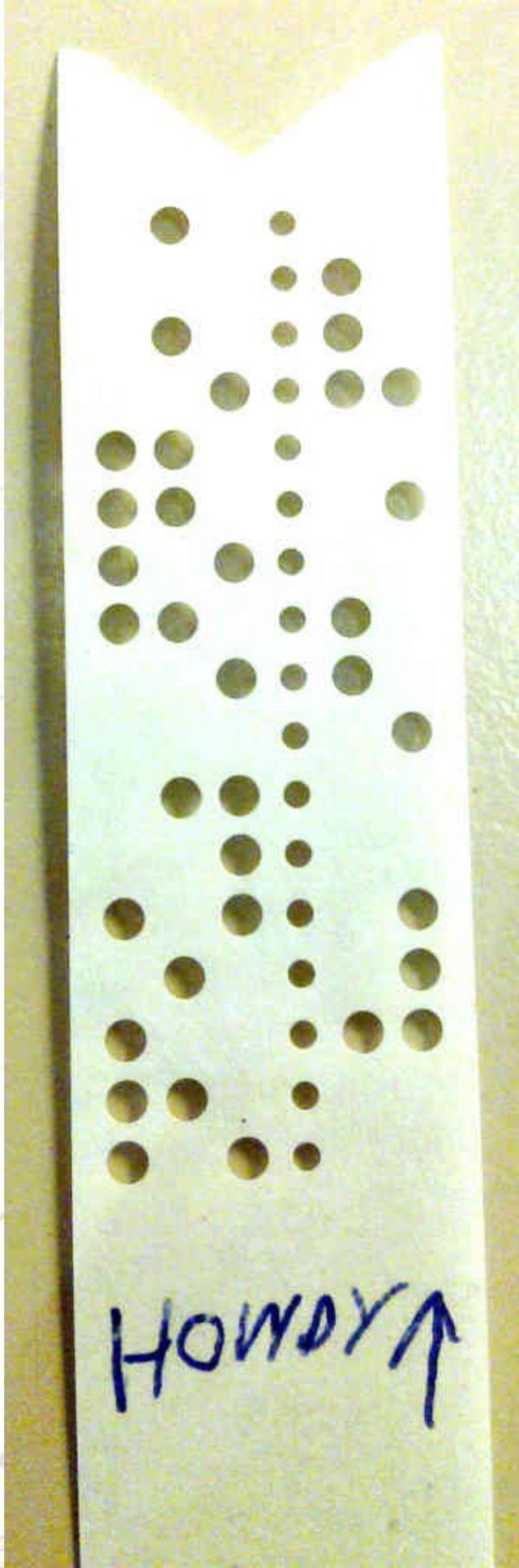
Why ham radio?



RTTY

- Ancient military protocol (1940s), now used by amateurs (since 1970s)
- 2FSK modulation, Baudot Coding
  - Low frequency, High frequency.
  - 5/N/2 -- 5 Data Bits, No parity, 2 Stop Bits




HOWDY

fldigi - N0CALL

File Op Mode Configure View Logbook Help

Spot RxID TxID TUNE

14070.000

Frq 14071.085 On Off 0259 In Out

Call Op Az

USB 3000 Qth St Pr Loc

14072.49 V

14071.96 H

14071.13 G

14070.87 A

CQ

-6.0 Clear

CQ CQ CQ de N0CALL N0CALL N0CALL
CQ CQ CQ de N0CALL N0CALL N0CALL pse k
VT
CQ CQ CQ DE N0CALL N0CALL N0CALL
CQ CQ CQ DE N0CALL N

CQ CQ CQ de N0CALL N0CALL N0CALL
CQ CQ CQ de N0CALL N0CALL N0CALL pse k
^T

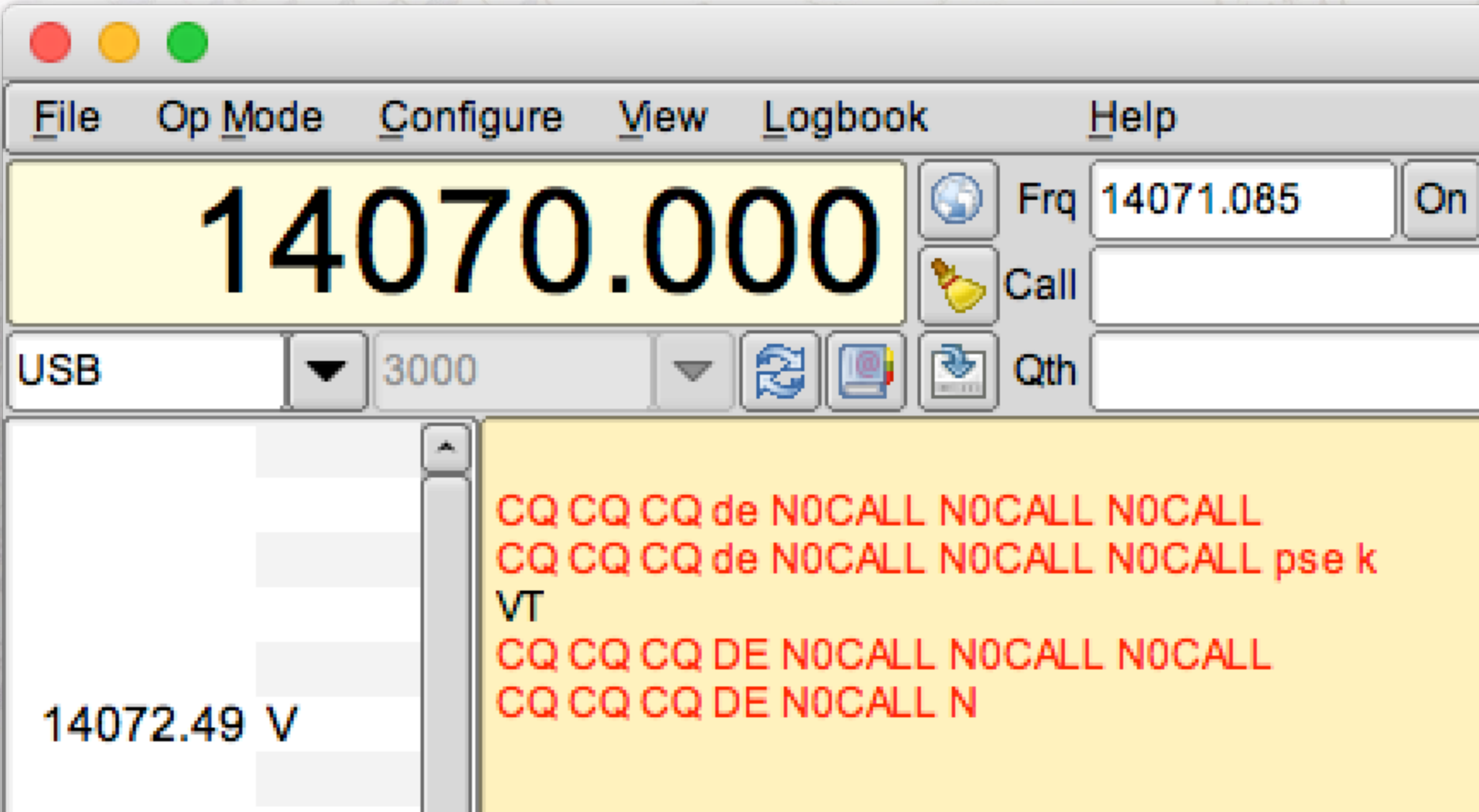
CQ ANS QSO KN SK Me/Qth Brag T/R Tx Rx TX 1

500 1000 1500 2000 2500 3000 3500 4000

WF -20 70 x1 NORM 1000 QSY Store Lk Rv T/R

RTTY 45.45/170 s/n -23 dB -3.0 AFC SQL KPSQL

Radio Frequency (Carrier)



.87 A

Clear

Downshifted Audio Signal

ANS

QSO

KN

SK

500

1000

1500

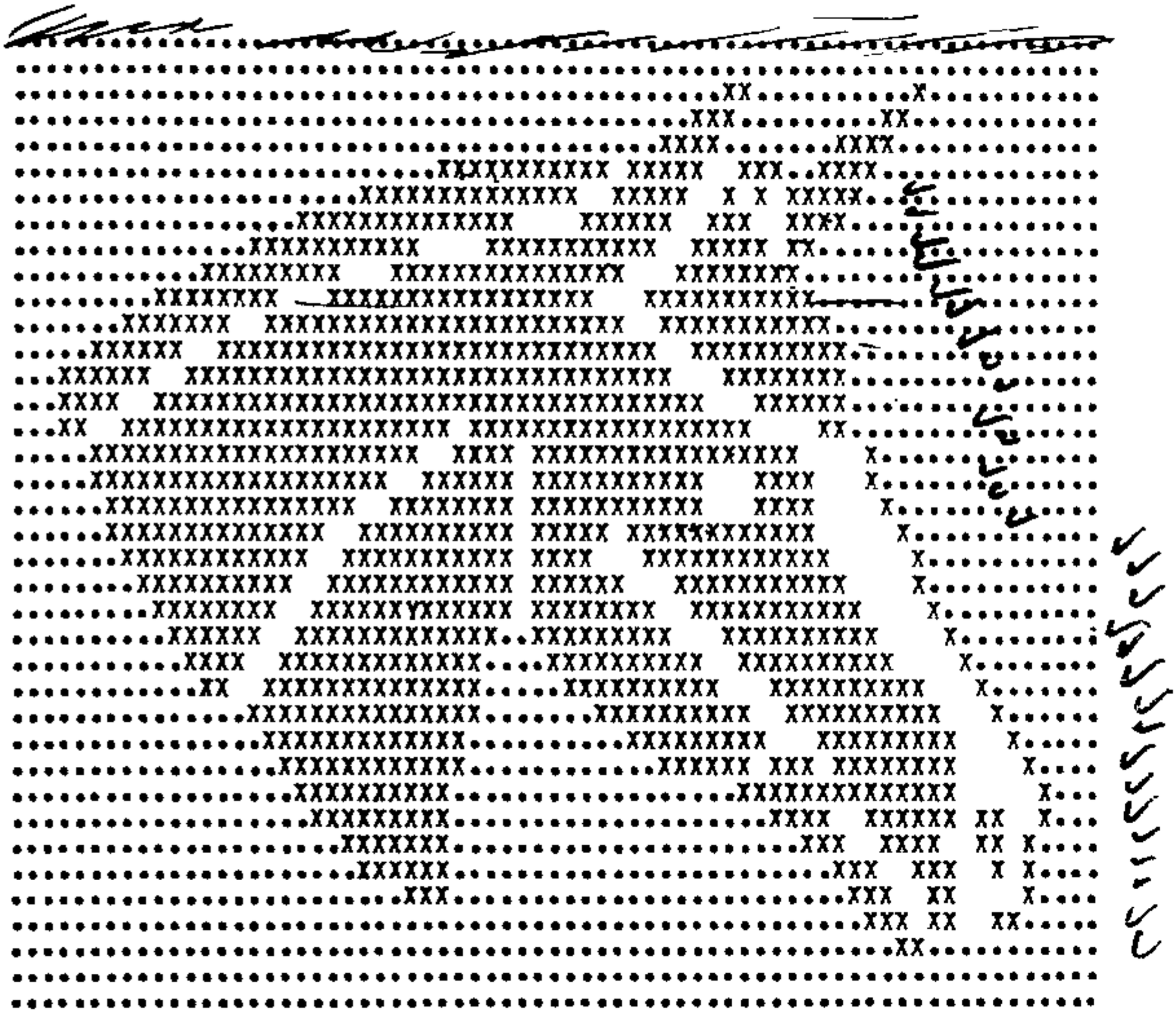
-20

70

x1

45.45/170

s/n -23 dB



THE DERBY WINNER

PSK31

- 1990's Replacement for RTTY
- 31.25 Baud
  - This is for human typing speed
- ~60Hz Wide

fldigi - N0CALL

File Op Mode Configure View Logbook Help

Spot RxID TxID TUNE

14070.000

Frq 14071.000 On Off 0258 In Out

Call Op Az

USB 3000 Qth St Pr Loc

CQ CQ CQ de N0CALL N0CALL N0CALL
CQ CQ CQ de N0CALL N0CALL N0C

CQ CQ CQ de N0CALL N0CALL N0CALL
CQ CQ CQ de N0CALL N0CALL N0CALL pse k
^l

CQ

3.0 Clear

CQ ANS QSO KN SK Me/Qth Brag T/R Tx Rx TX 1

500 1000 1500 2000 2500 3000 3500 4000

WF -20 70 x1 NORM 1000 QSY Store Lk Rv T/R

BPSK31 -3.0 AFC SQL KPSQL

File Op Mode Configure View Logbook Help

14070.000

Frq 14071.000 On

Call

Qth

USB 3000

CQ CQ CQ de N0CALL N0CALL N0CALL

CQ CQ CQ de N0CALL N0CALL N0C

ANS QSO KN

500 1000 15

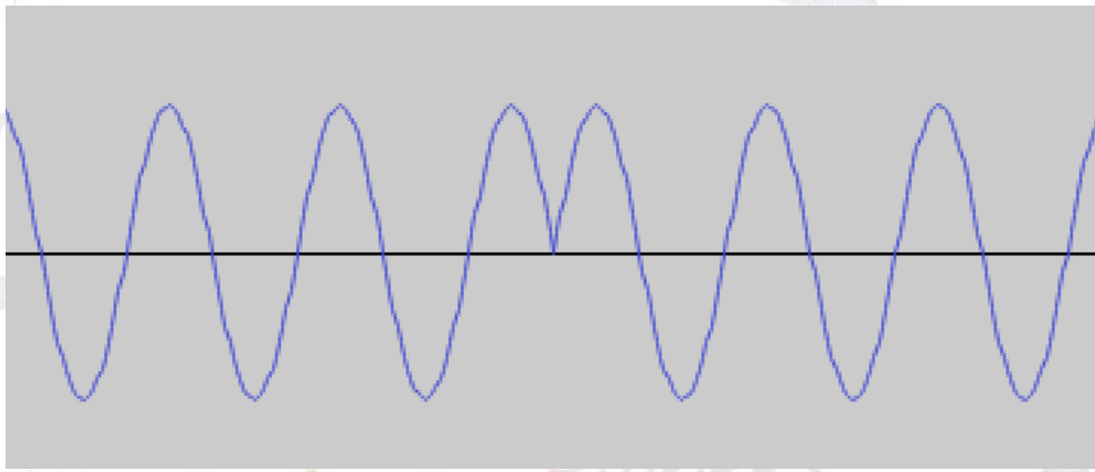
-20 70 x1

Building PSK31 Encoder

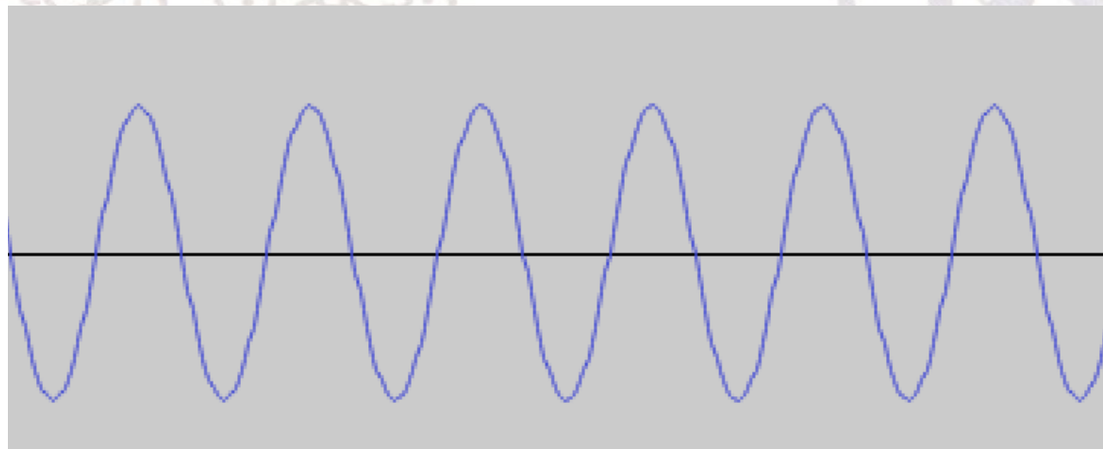
- PSK31 is generated as *__AUDIO__*
- Audio cable runs from sound card to radio

PSK31 Modulation

- Phase is Inverted to mark a Zero
  - Fancy way to say that SIN(x) becomes COS(x)
  - Or COS(x) to SIN(x)

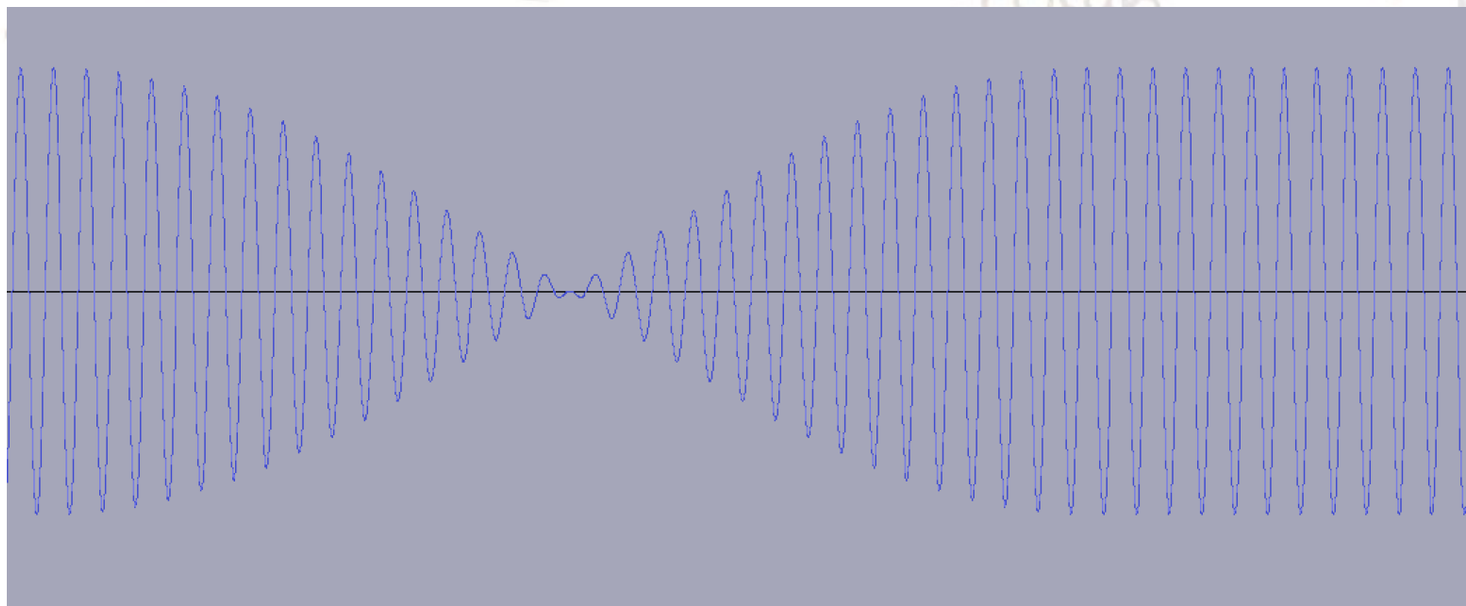


- Phase is Not Inverted to mark a One
  - No change at all

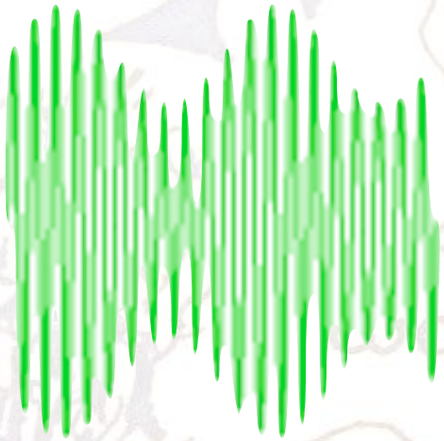


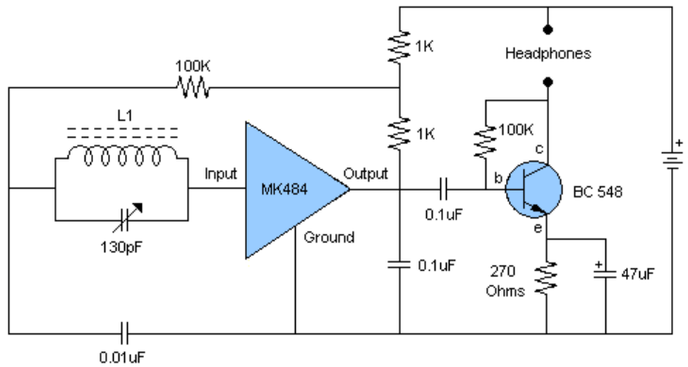
PSK31 Modulation

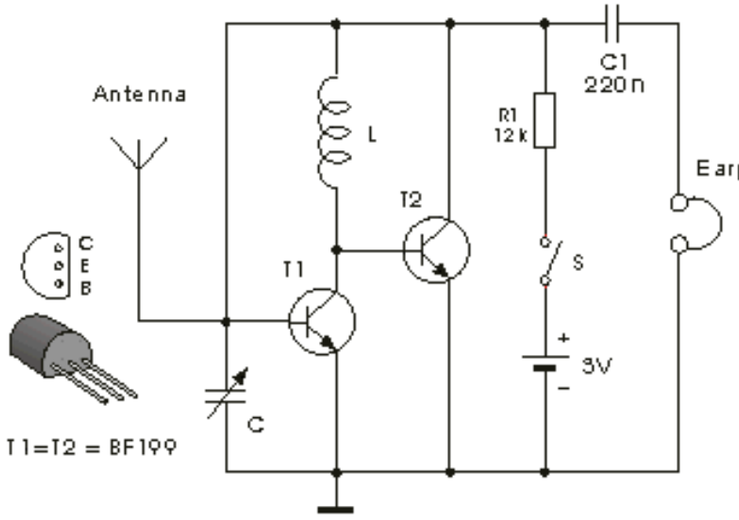
- You can't just abruptly invert the phase
  - This hurts your ears, hurts the speaker
- **Drop** the amplitude to zero before the shift
  - Raise it back by mid-symbol
  - So the amplitude drops
    for every Zero



PHY Polyglots!



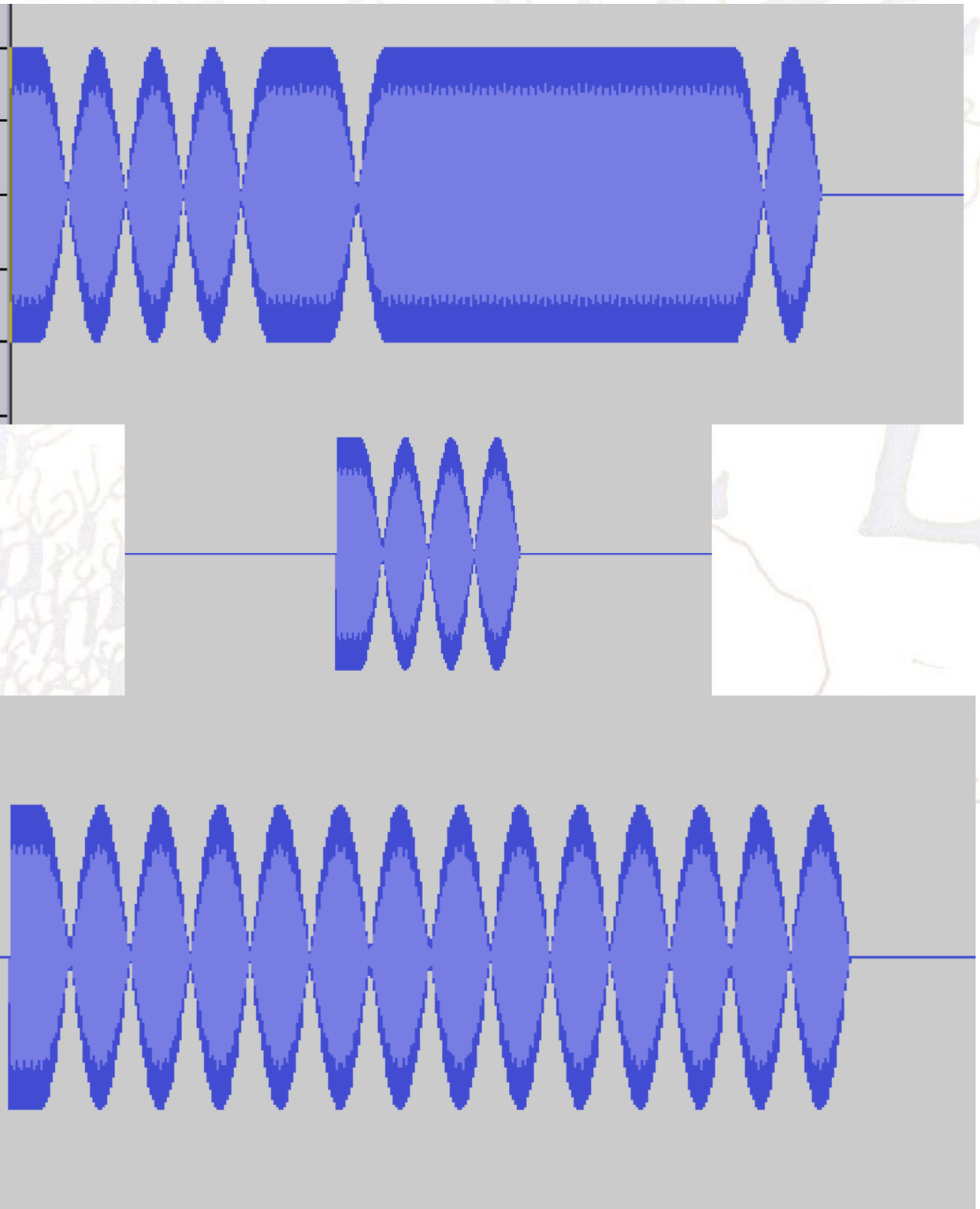




Morse/PSK Polyglot

- Dahs encode letters.
- E is shorter, fits in a Dit.
- Left is waterfall of letter K.
  - Dah-Di-Dah

Morse/PSK Polyglot



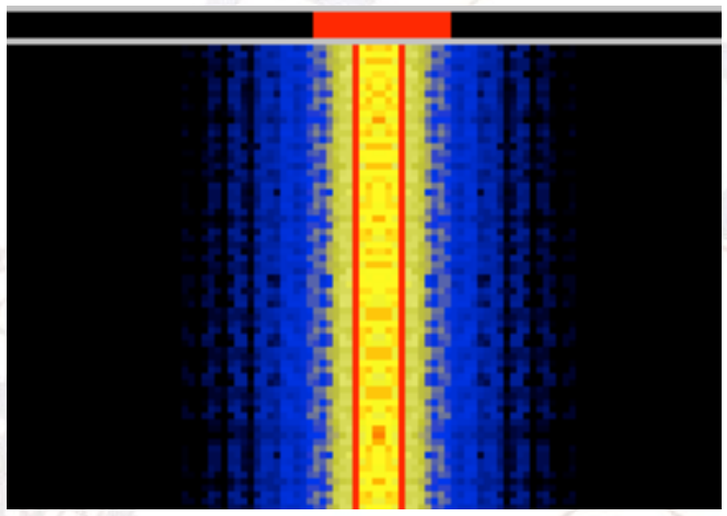
- First Dah has K (dah-di-dah) encoded.
- Dit is all Zeroes.
- Final Dah is all Zeroes

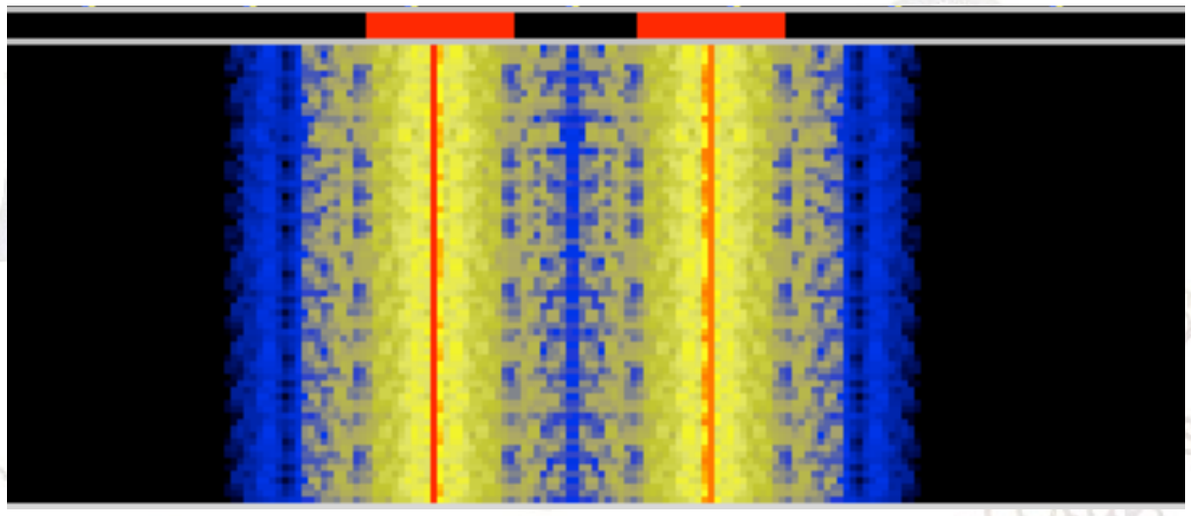
PSK31/RTTY Polyglot

- RTTY cares about **Relative Power**
- PSK31 is tolerant to changes in power
  - Only cares about **Phase**!
- We can combine the two!

Not so easy

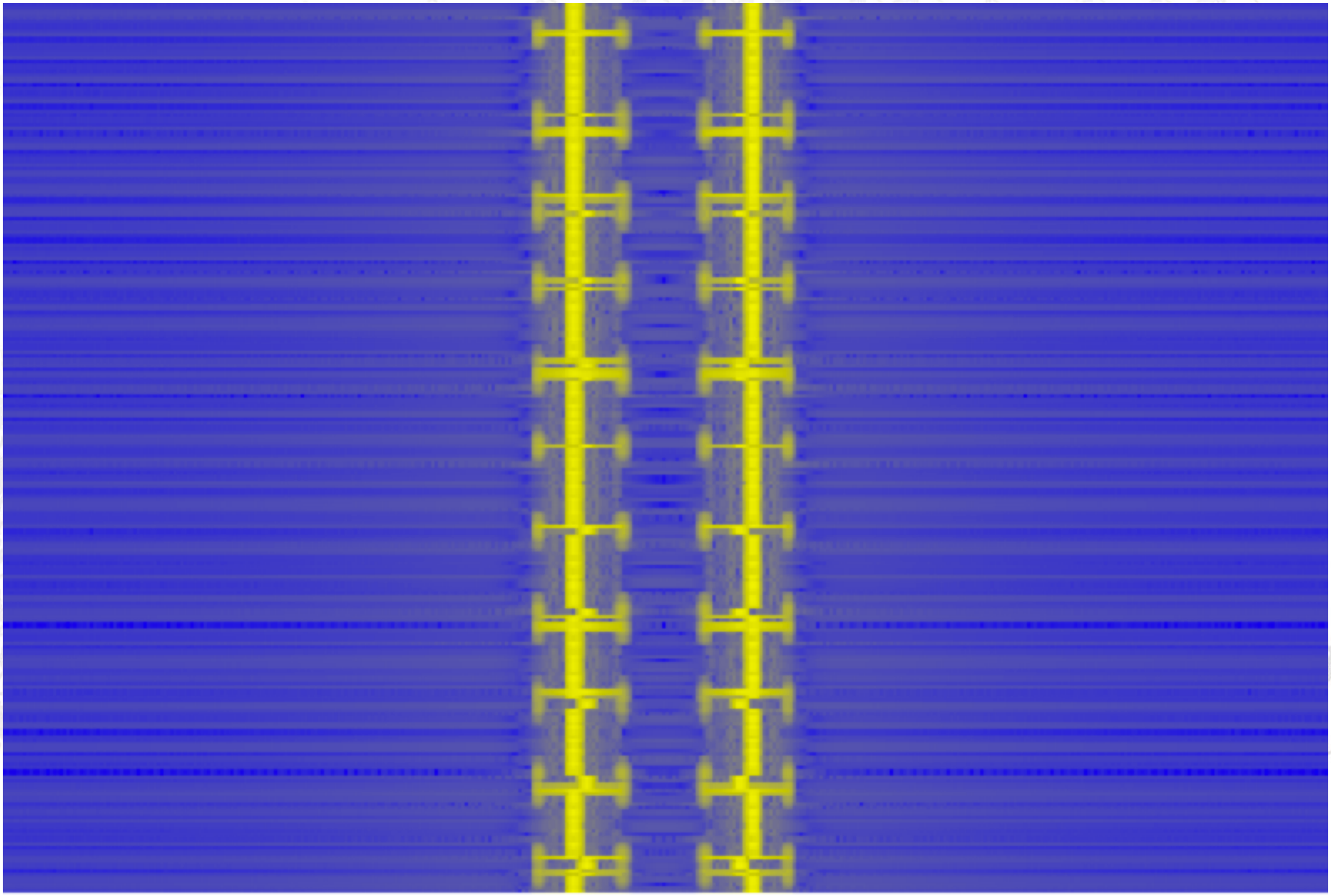
- Bandwidth is different



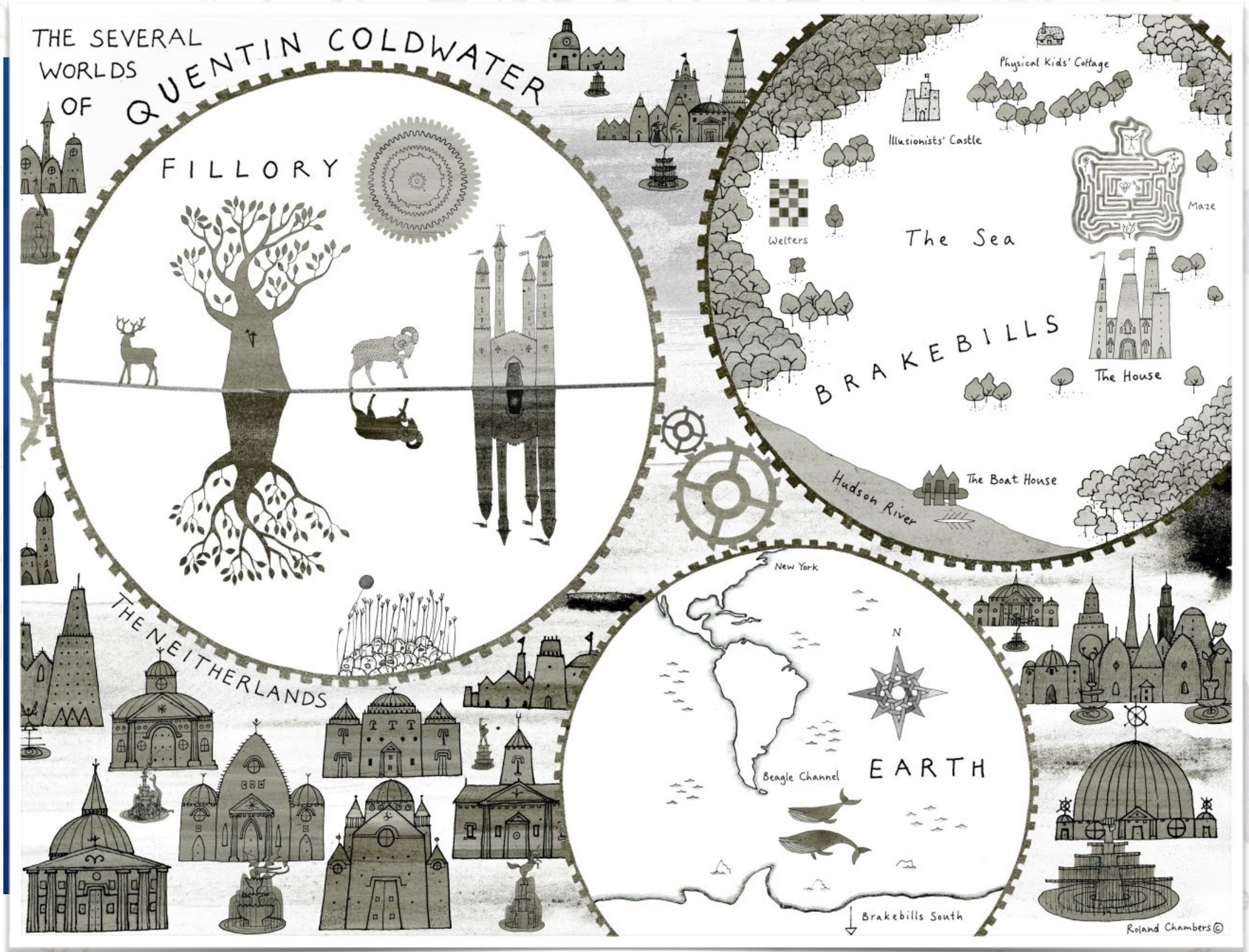


- PSK31: phase
- RTTY: frequency
- Human operator actually looks at the waterfall!

Welcome to Fillory!

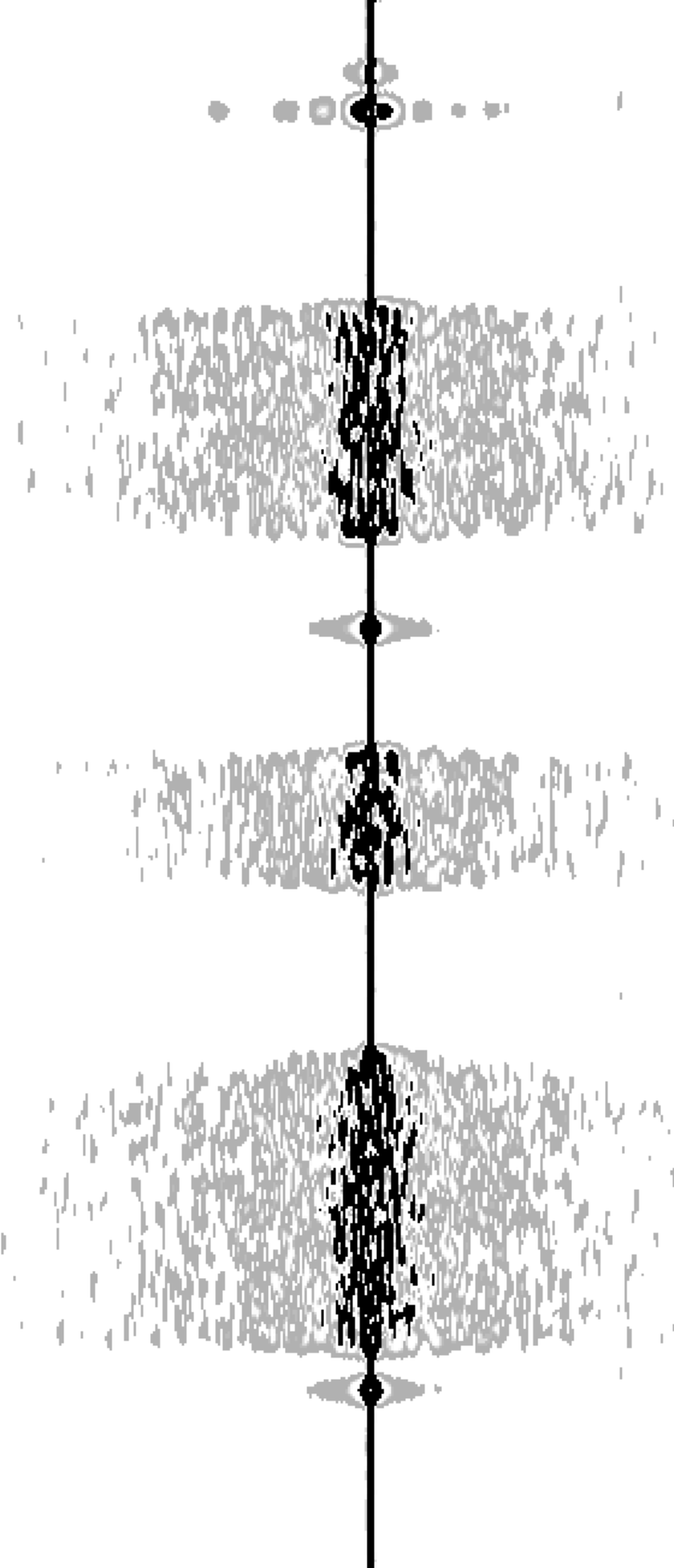


A diversion into 802.3



Madeline; or, The Accidental Tempest

- Data runs over Ethernet
- You control a bit of data
  - But not very well (HTTP over Tor, for example)
- You want to exfiltrate a signal
  - THE CLIENT IS HERE, GUYS!
- If the wiring is bad, it's not that hard



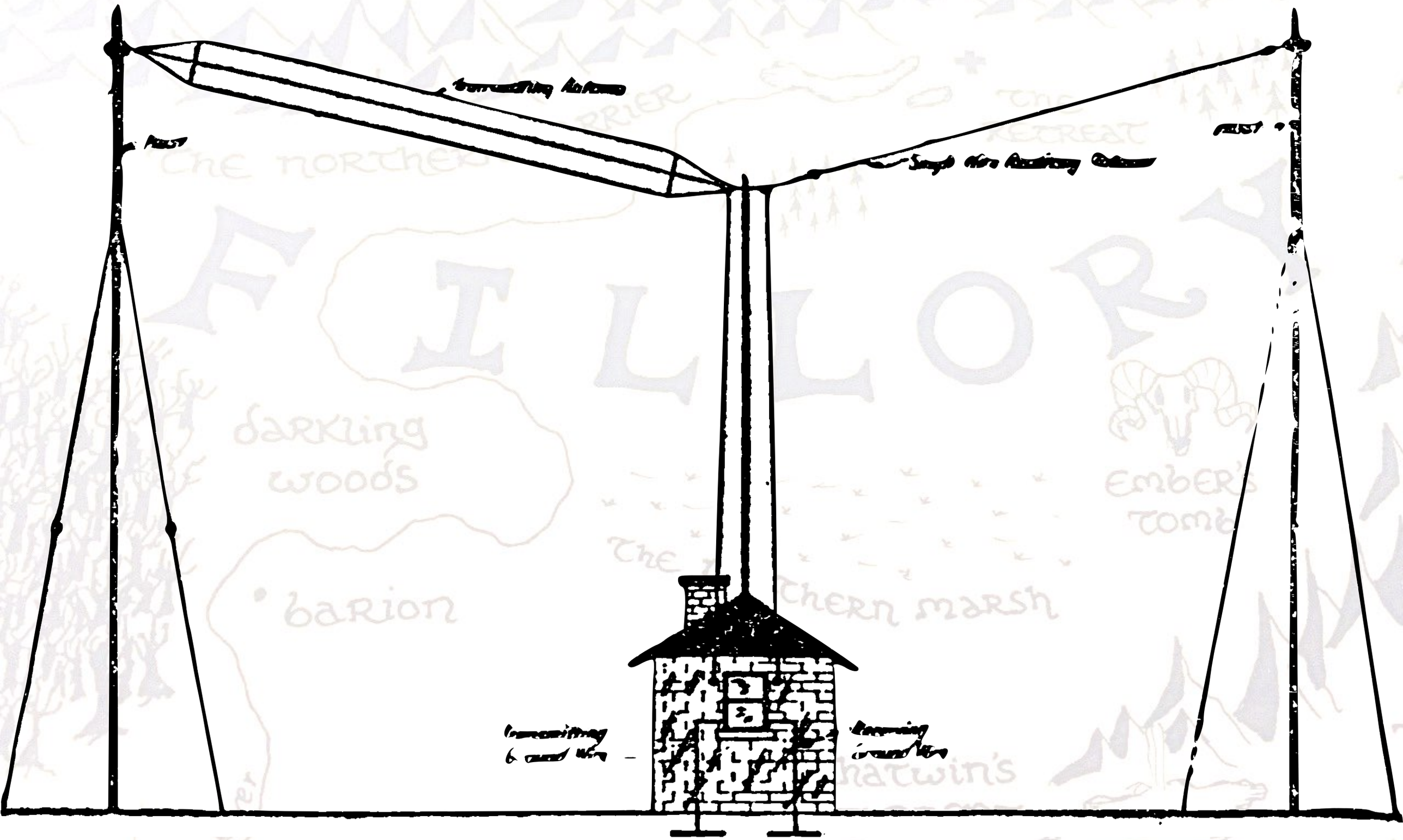
Dah

Di

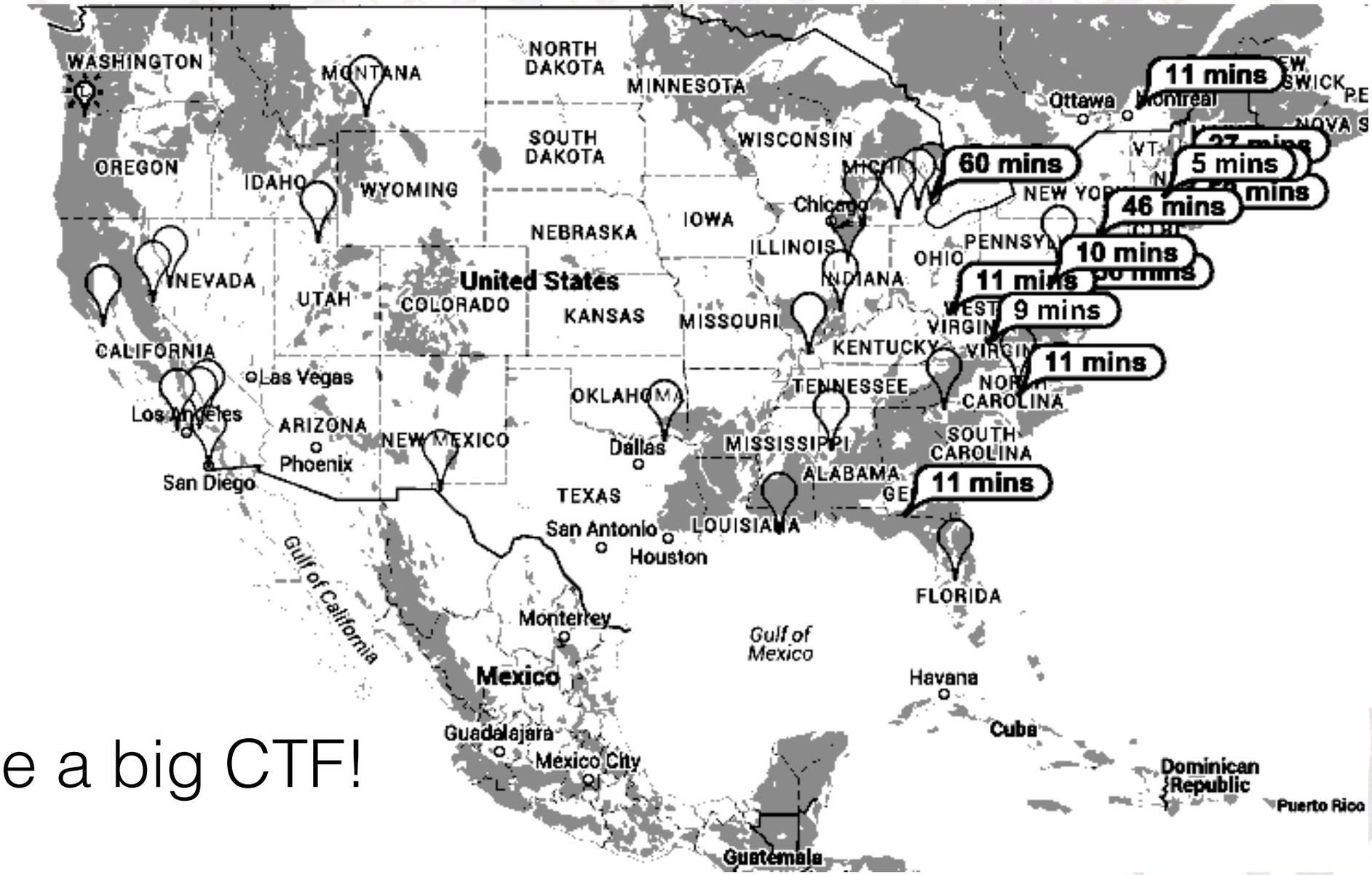
Dah

Madeline

Back to ham radio



Care to play along?



- Let's have a big CTF!
  - 20 meter transmission from Northeast USA
  - Receive by USB in most of Western Hemisphere.

Conclusions

- **PHY** is pliable and should be played with
  - start with simpler protocols like PSK31, RTTY, ...
  - more complex protocols are built of similar pieces
  - parser **differentials** abound & should be understood
- Digital radio parsers allow **polyglots** with modulation, encoding, and even error correction
  - not only in PDF/ZIP/GIF/JPEG/... of PoC||GTFO ;)

Image credits

- Manul drawings by Natalia Pavlushina
  http://www.animalist.ru/?action=show_gallery&artist=pavlushina
  and Olga Zakharova
  http://www.savemanul.org/images/full/manul_3w.jpg

- Map of Fillory
  http://brakebillskids.tumblr.com/post/141686464777/pawtersimms-so-i-finally-put-up-my-map-of-fillory