Revolting Radios

Get it? It’s a pun!

Thanks

Mike Walters

Ang Cui

Schuyler St. Leger

Taylor Streetman

Sergey Bratus

Travis Goodspeed

A little background

“One of the things that makes Orwell's '1984' scary is the way it uses technology. In Orwell’s dystopia, tech is a one-sided means of control. The powers that be use machines for pervasive surveillance, to weaken your sense of self and to make real change feel impossible. Humans deprived of any private space are uniquely vulnerable, and Big Brother knows it.”

- DEF CON 26 theme

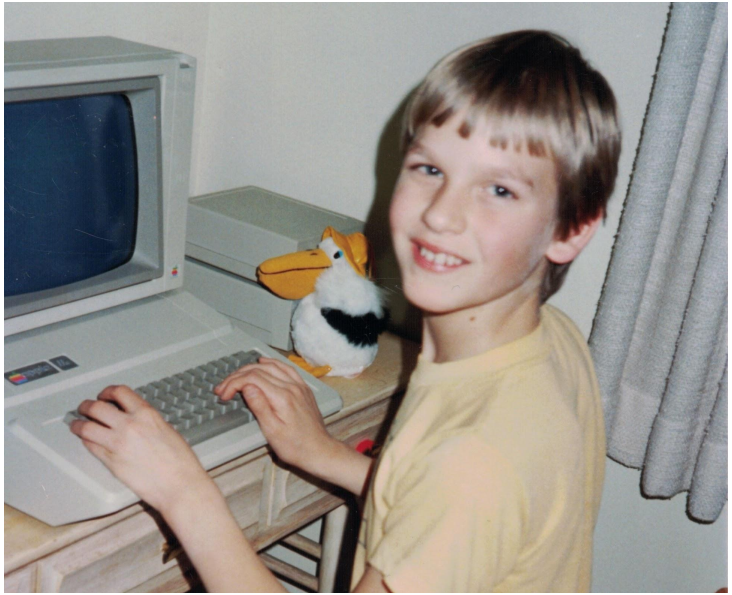
“Let’s over-commit to that theme.”

- Mike & Dominic

Who are we?

Michael Ossmann

Founder and CEO of Great Scott Gadgets



Dominic Spill

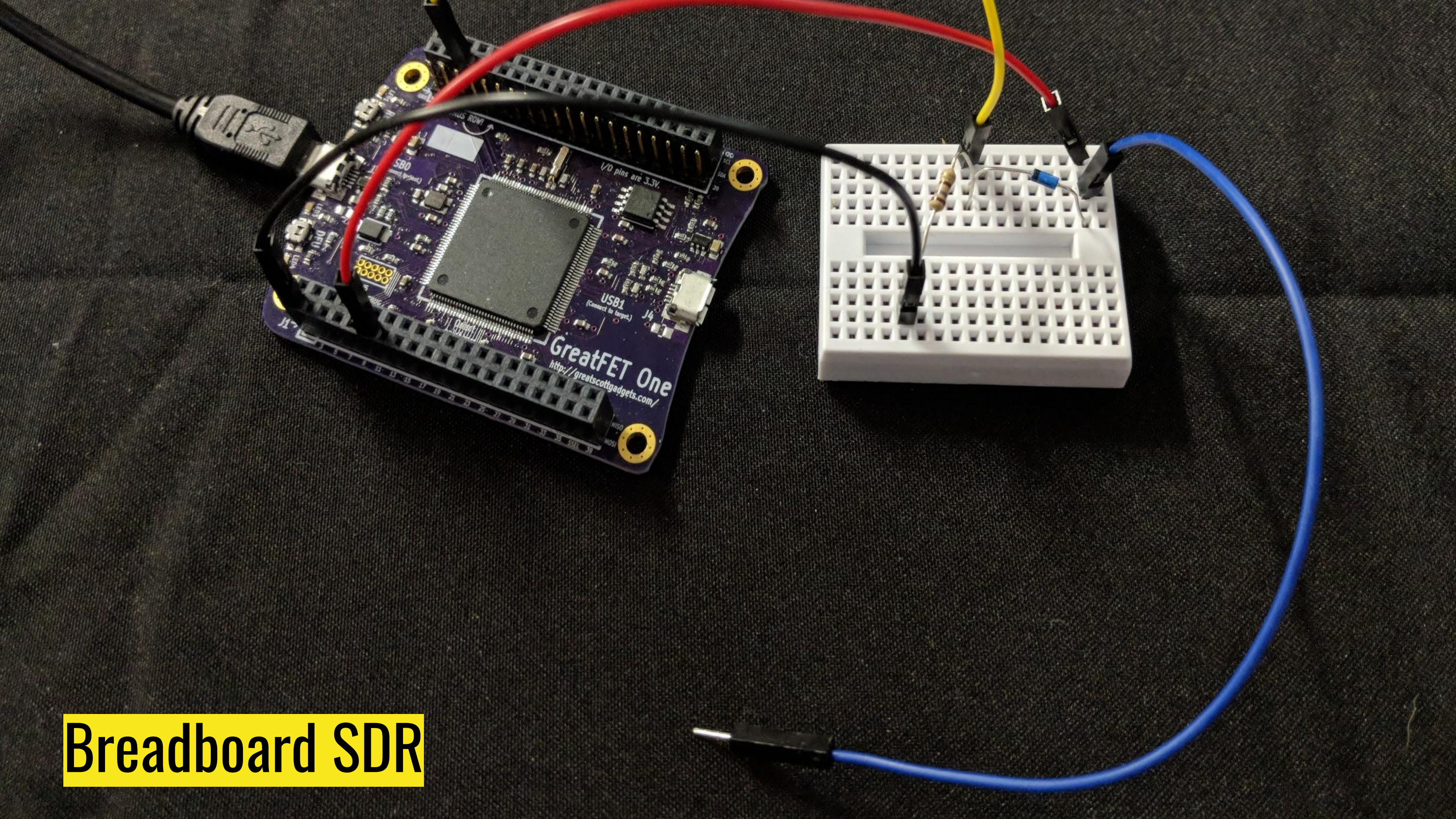
Security Researcher at Great Scott Gadgets

Breadboard SDR

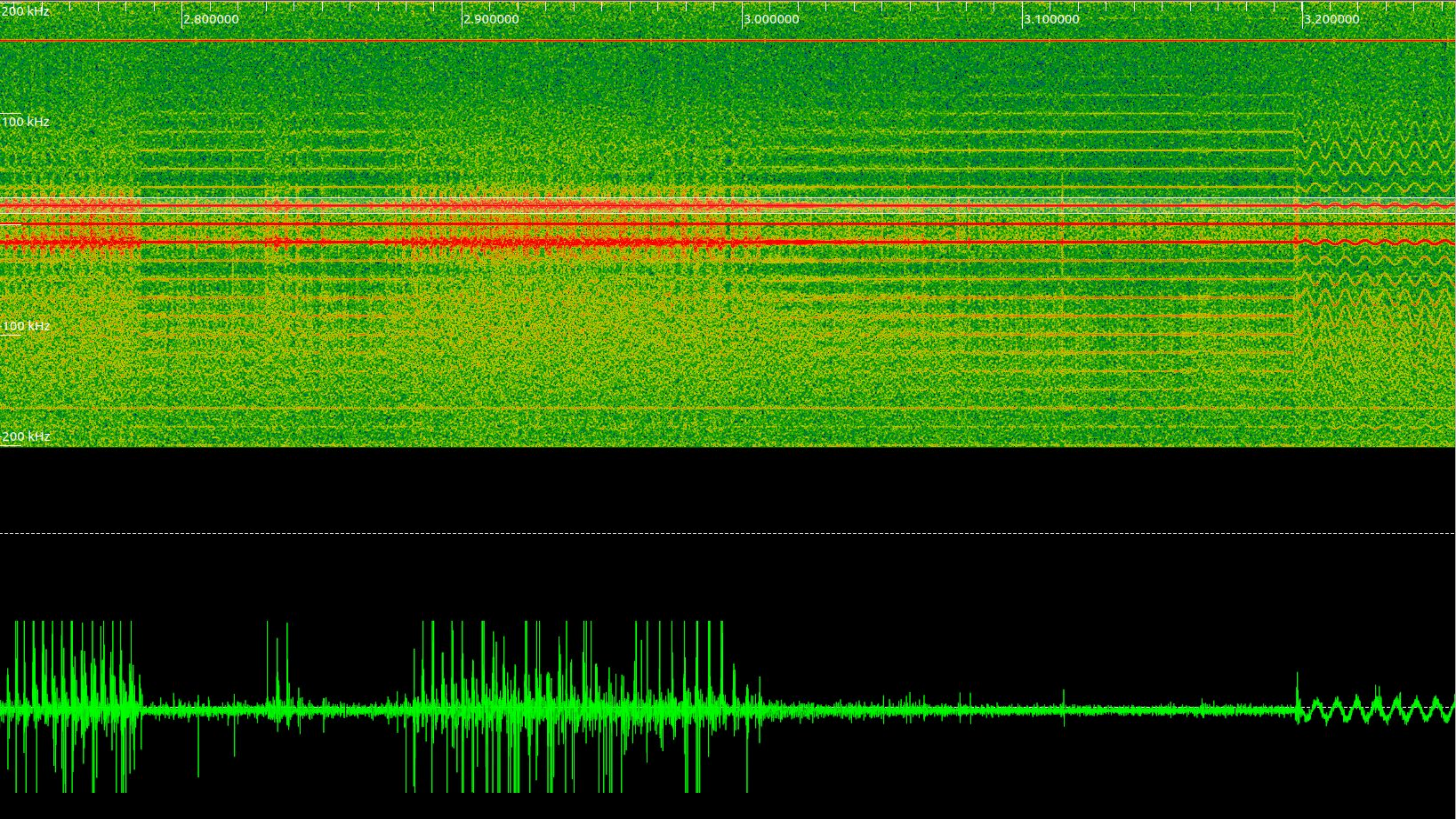
Scenario

We’ve found that we can reprogram one of Big Brother’s telescreens and stream samples from the auxiliary Analog to Digital Converter (ADC) in its microcontroller.

Can we build a radio receiver out of this microcontroller?



Breadboard SDR


200 kHz
2.800000
2.900000
3.000000
3.100000
3.200000
100 kHz
100 kHz
200 kHz

When you build a radio in software, you don’t need much hardware

Clock Signal Transmitters

Scenario

We need to exfiltrate data from one of Big Brother’s air-gapped networks.

We have an ally but no radio transmitter inside.

Can our ally reprogram a microcontroller on the inside to transmit data over the air?

Toggling IO Pins

Miek’s OOK transmitter

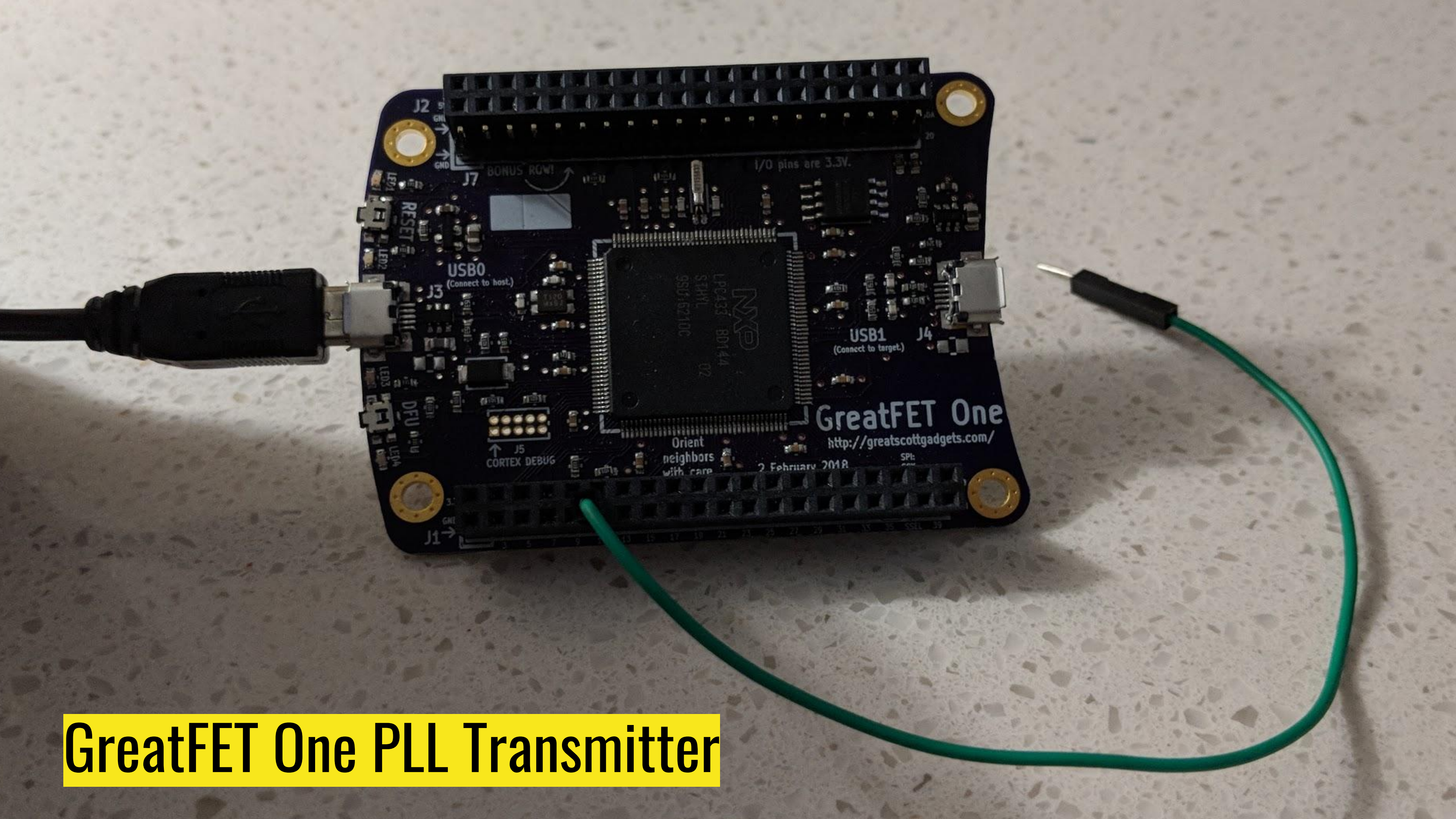
https://gfycat.com/gifs/detail/cloudyinfamouscapybara

Ang Cui’s Funtenna

http://www.funtenna.org/CuiBH2015.pdf

Raspberry Pi FM

https://github.com/PNPtutorials/FM_Transmitter_RPi3



GreatFET One PLL Transmitter

Real World Radios

Our demonstration target used a frequency deviation of +/-25 kHz and a center frequency of 315.005 MHz.

We transmitted with a frequency deviation of +/-50 kHz at a center frequency of 315.050 MHz, and it worked!

If it oscillates like a radio
and emits like a radio

It’s a radio

GPIO Pin Receiver

Scenario

Big Brother has updated telescreens to a new version without an Analog to Digital Converter (ADC) and has restricted distribution of ADCs in an effort to prevent improvised radio receivers.

Can we use a General-Purpose I/O (GPIO) pin on a microcontroller to implement a receiver without an ADC?

converters, electro-optical or "optical integrated circuits" designed for "signal processing", field programmable logic devices, custom integrated circuits for which either the function is unknown or the control status of the equipment in which the integrated circuit will be used in unknown, Fast Fourier Transform (FFT) processors, electrical erasable programmable read-only memories (EEPROMs), flash memories or static random-access memories (SRAMs), having any of the following:

a.2.a. Rated for operation at an ambient temperature above 398 K (+125˚C);

a.2.b. Rated for operation at an ambient temperature below 218 K (-55˚C); *or*

a.2.c. Rated for operation over the entire ambient temperature range from 218 K (-55˚C) to 398 K (125˚C);

a.5.a.2. A resolution of 10 bit or more, but less than 12 bit, with an output rate greater than 500 million words per second;

a.5.a.3. A resolution of 12 bit or more, but less than 14 bit, with an output rate greater than 200 million words per second;

a.5.a.4. A resolution of 14 bit or more, but less than 16 bit, with an output rate greater than 250 million words per second; *or*

a.5.a.5. A resolution of 16 bit or more with an output rate greater than 65 million words per second;

***Technical Notes*:**

1. A resolution of n bit corresponds to a quantization of 2^n levels.

1 bit ought to be enough for anybody

Direction finder to PSK transmitter

Scenario

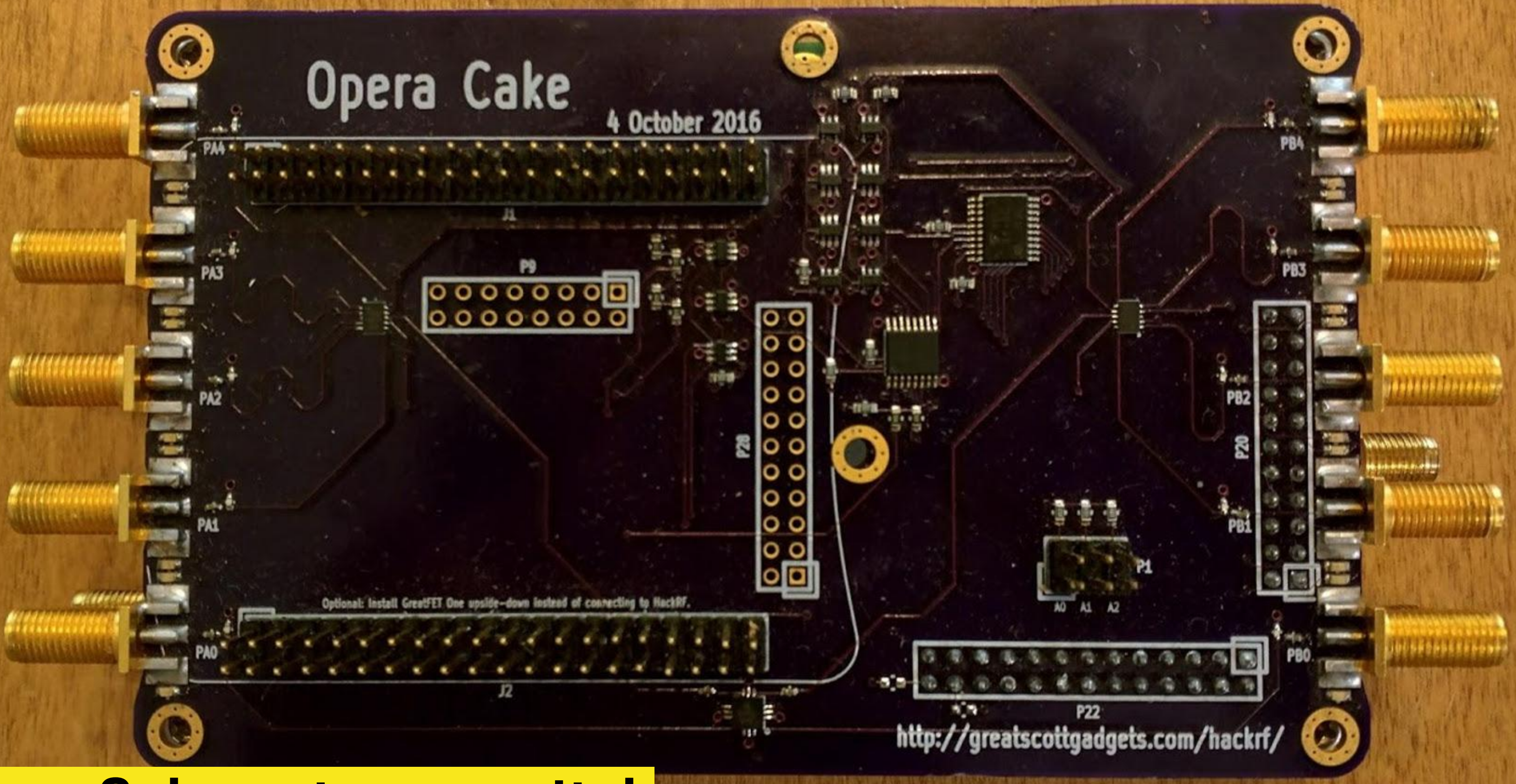
Big Brother has deployed pseudo-Doppler direction finders to track down illegal radio transmitters.

Can we steal a direction finder and use it as a direction finding countermeasure?

Pseudo-Doppler Direction Finding

Using an antenna switching board, we rapidly change antenna

Pseudo-Doppler Redux, Shmoocon 2018 -
https://archive.org/details/Shmoocon2018/Shmoocon2018-Pseudo-dopplerRedux.mp4


Opera Cake
4 October 2016
PA4
PA3
PA2
PA1
PA0
J1
P9
P28
Optional: Install GreatFET One upside-down instead of connecting to HackRF.
J2
PB4
PB3
PB2
PB1
PB0
P20
P1
A0
A1
A2
P22
http://greatscottgadgets.com/hackrf/

Opera Cake antenna switch

Phase shifting

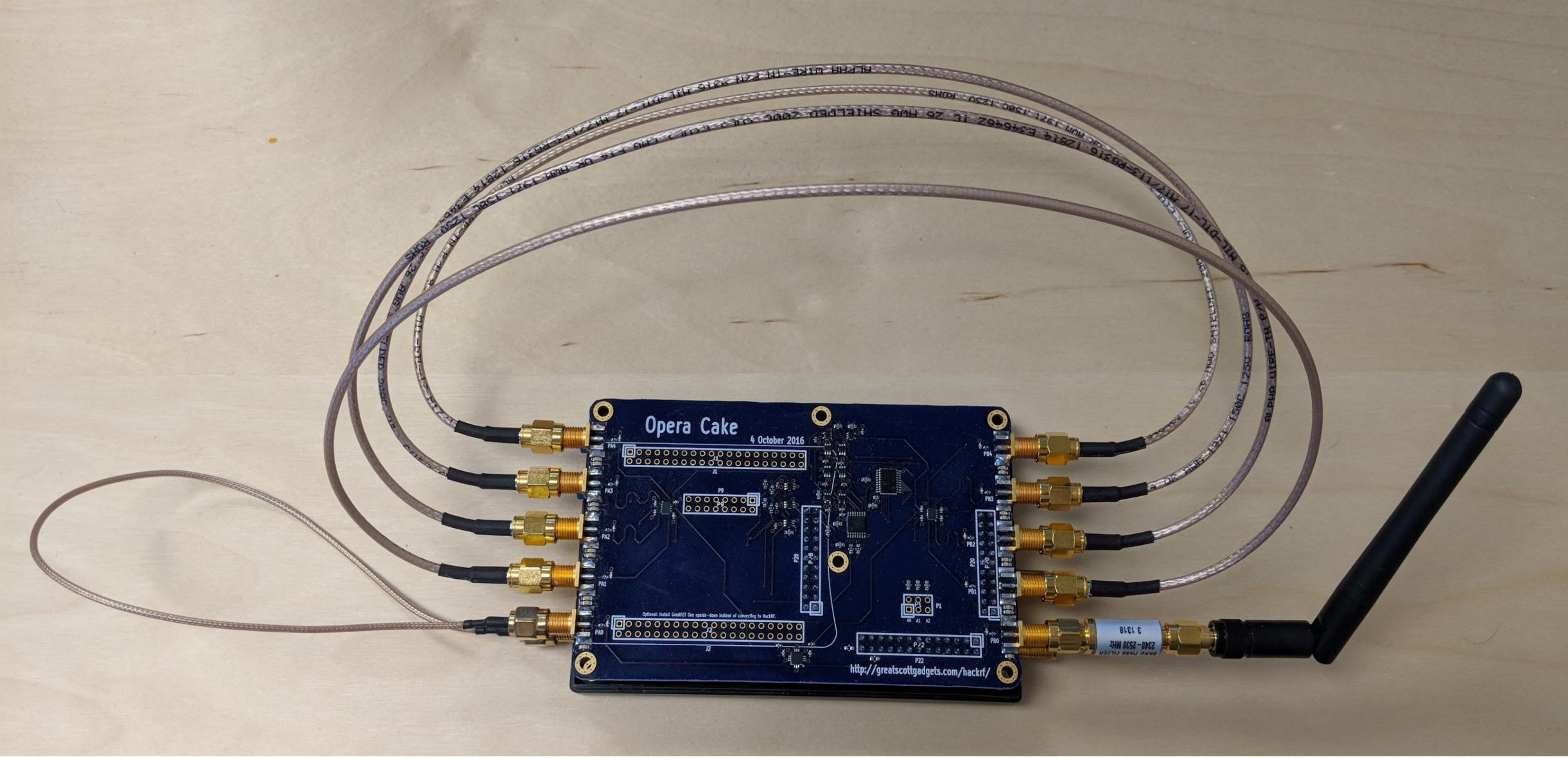
Switching from one antenna to another that is closer or farther from the other end of the link introduces a phase shift.

Switching from one cable to another that is longer or shorter introduces a phase shift.

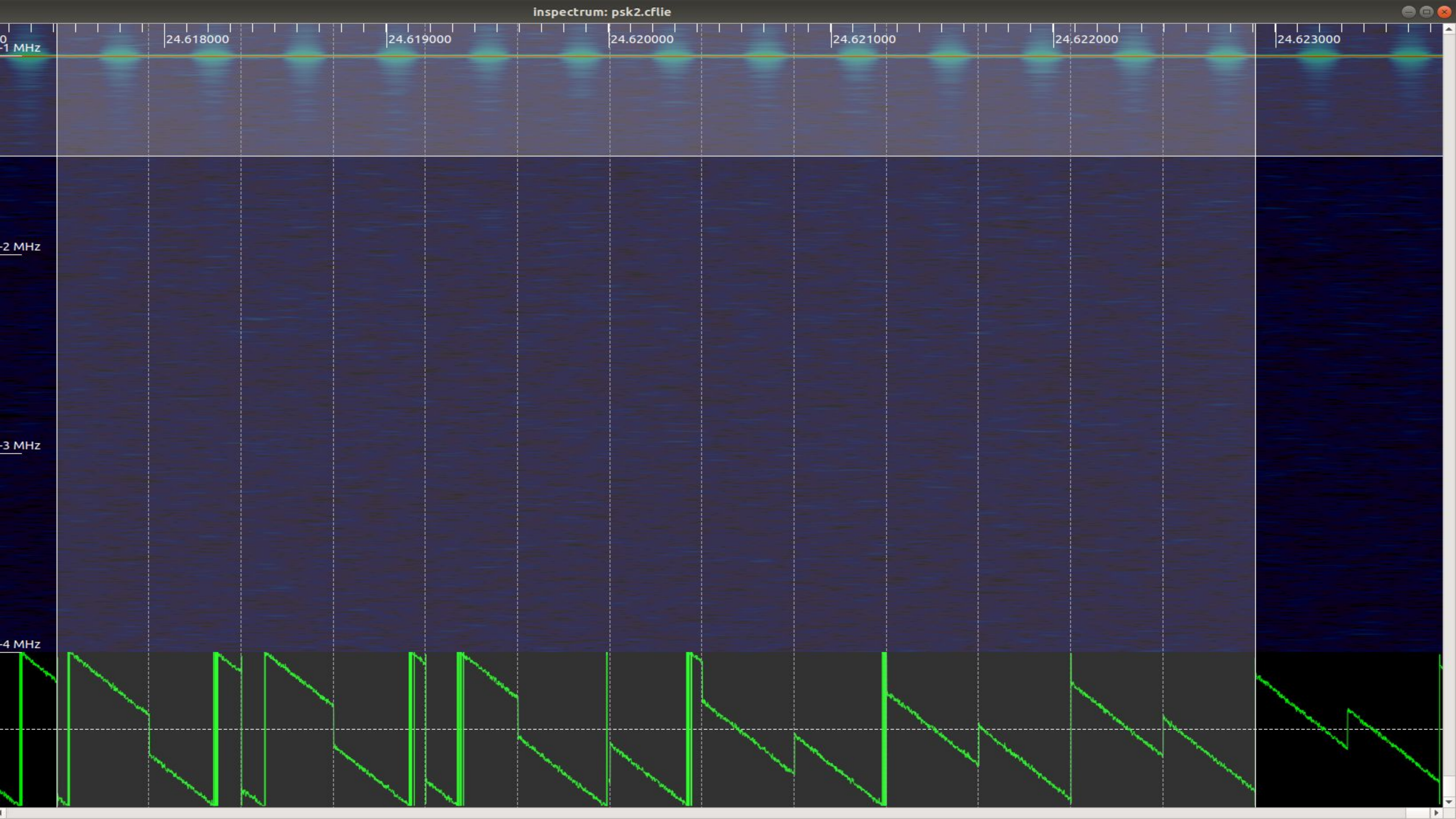
Adding phase shifts circumvents pseudo-Doppler

Scenario

Since we can affect the phase, can we use a direction finder to implement a Phase Shift-Keying (PSK) transmitter?



Opera Cake with delay lines for adding phase shifts



inspectrum: psk2.cflie

An external modulator can add a covert channel

References

https://github.com/greatscottgadgets/greatfet/tree/rfhax

https://github.com/mossmann/hackrf

Find us on Twitter: @michaelossmann / @dominicgs