Ubertooth

and other assorted packet sniffers

Dominic Spill

Open source software developer

Bluetooth: gr-bluetooth, Ubertooth, libBTBB

USBProxy, PS/2 Tap, FCC.io

Defcon, BlackHat, Kiwicon, Troopers (44CON)

Great Scott Gadgets

“Hardware for Hackers”

Ubertooth, HackRF, Throwing Star Lan Tap

Daisho, YARDstick, NSA Playset,
Unambiguous Encapsulation

Why build packet sniffers?

“Security will not get better until tools for practical exploration of the attack surface are made available”

-- Joshua Wright

Why build packet sniffers?

WEP -> WPA -> WPA2

4 digit pin -> Secure Simple Pairing

Why Bluetooth?

2 Billion devices sold each year

No packet sniffers, no “monitor” mode

Fun, hard, open problem (maybe too hard)

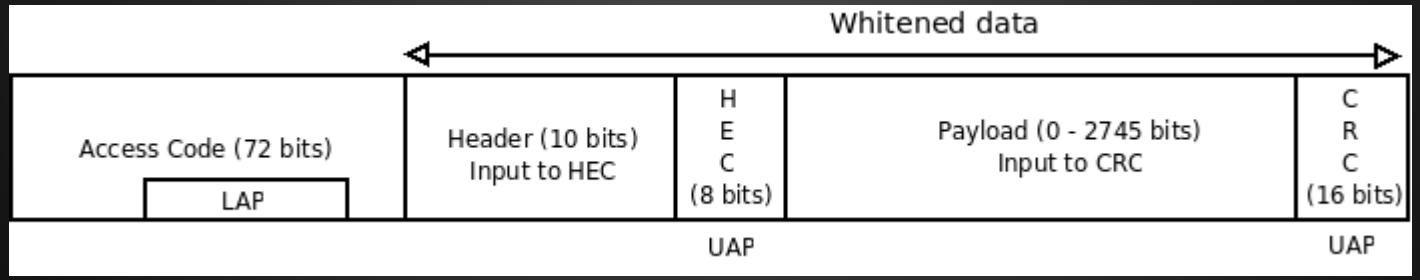
Bluetooth sniffing is hard

Frequency hops 1600 times per second based on device address, internal clock value and radio noise

Unknown device address - not all in packet

Bluetooth sniffing is hard

NAP	UAP	LAP
00 : 1F	81	00 : 08 : 30



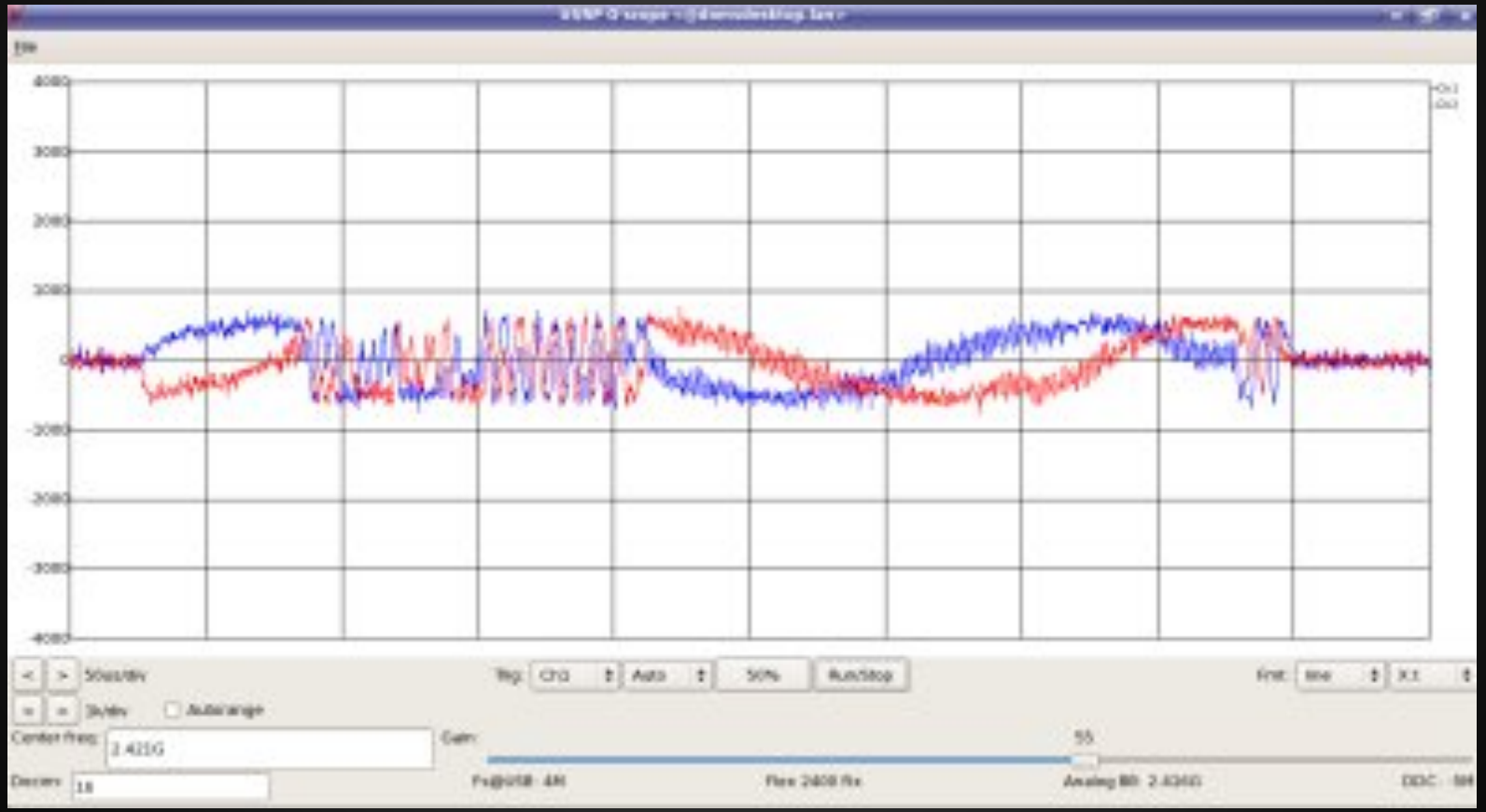
Software Defined Radio

gr-bluetooth

GNURadio

USRP

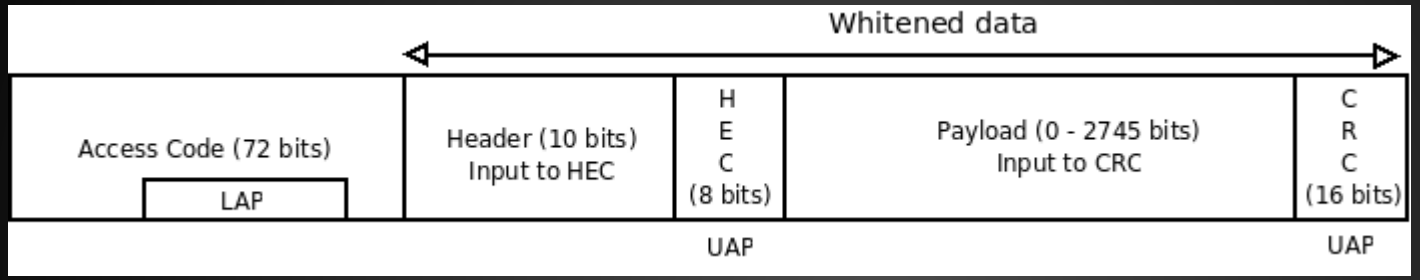
A Packet



Bits

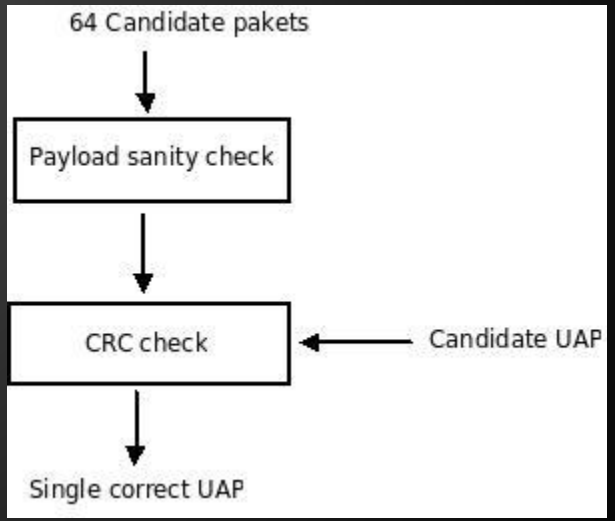
00001011111010111010101010101010101010
10101010101010101010101010101010101101
11001100001011011001100110011111110011
01001011000111110010101011111111110000
01100000000000000000000011111111100000
01111000011110000111100001111000011110
00111100001111000011110000111100001111
0000

Extracting Data



Extract the LAP

Try to extract the UAP -->



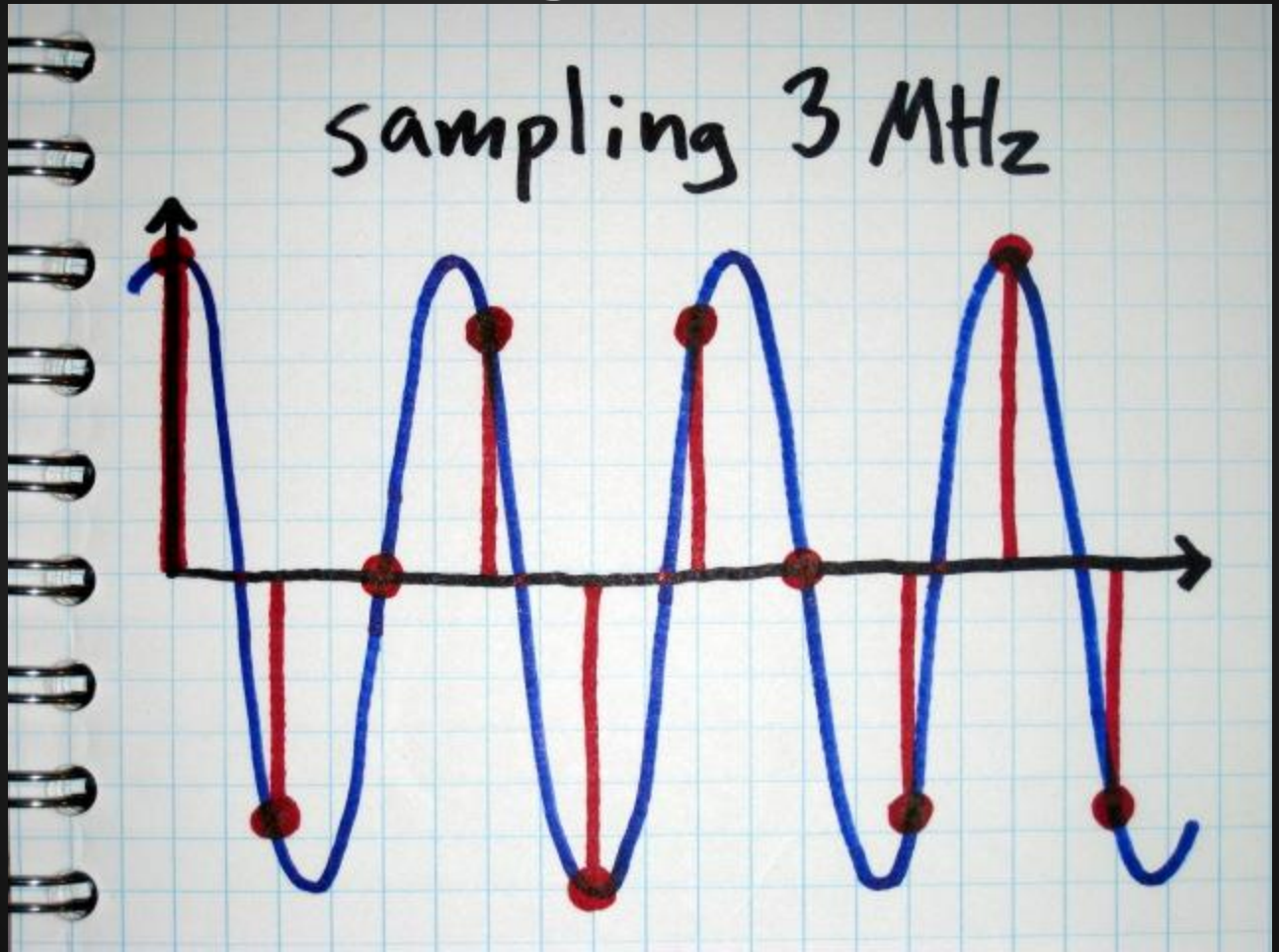
Problem Solved?

Single channel, RX only

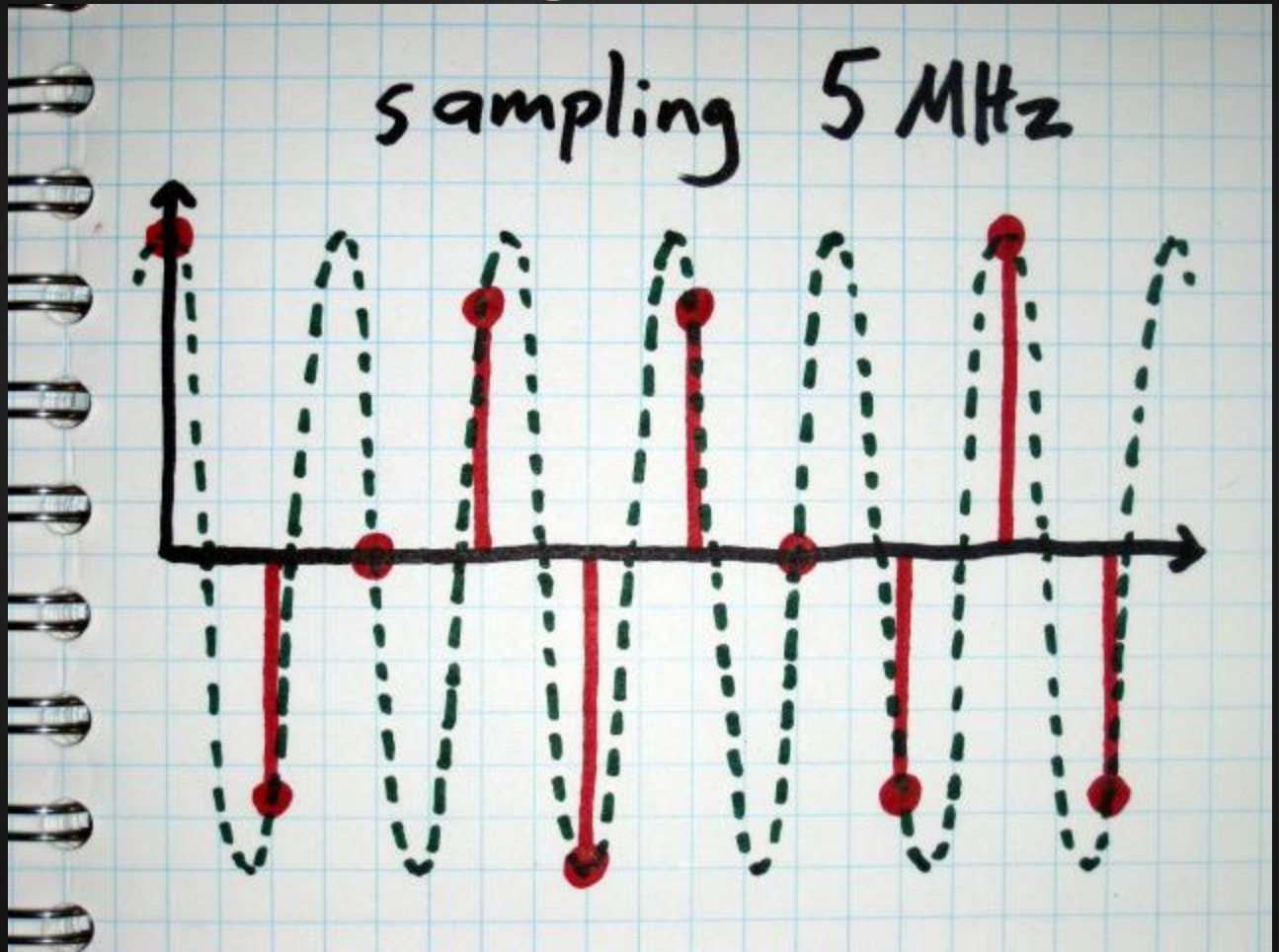
Expensive ~ $1000

Computationally intensive

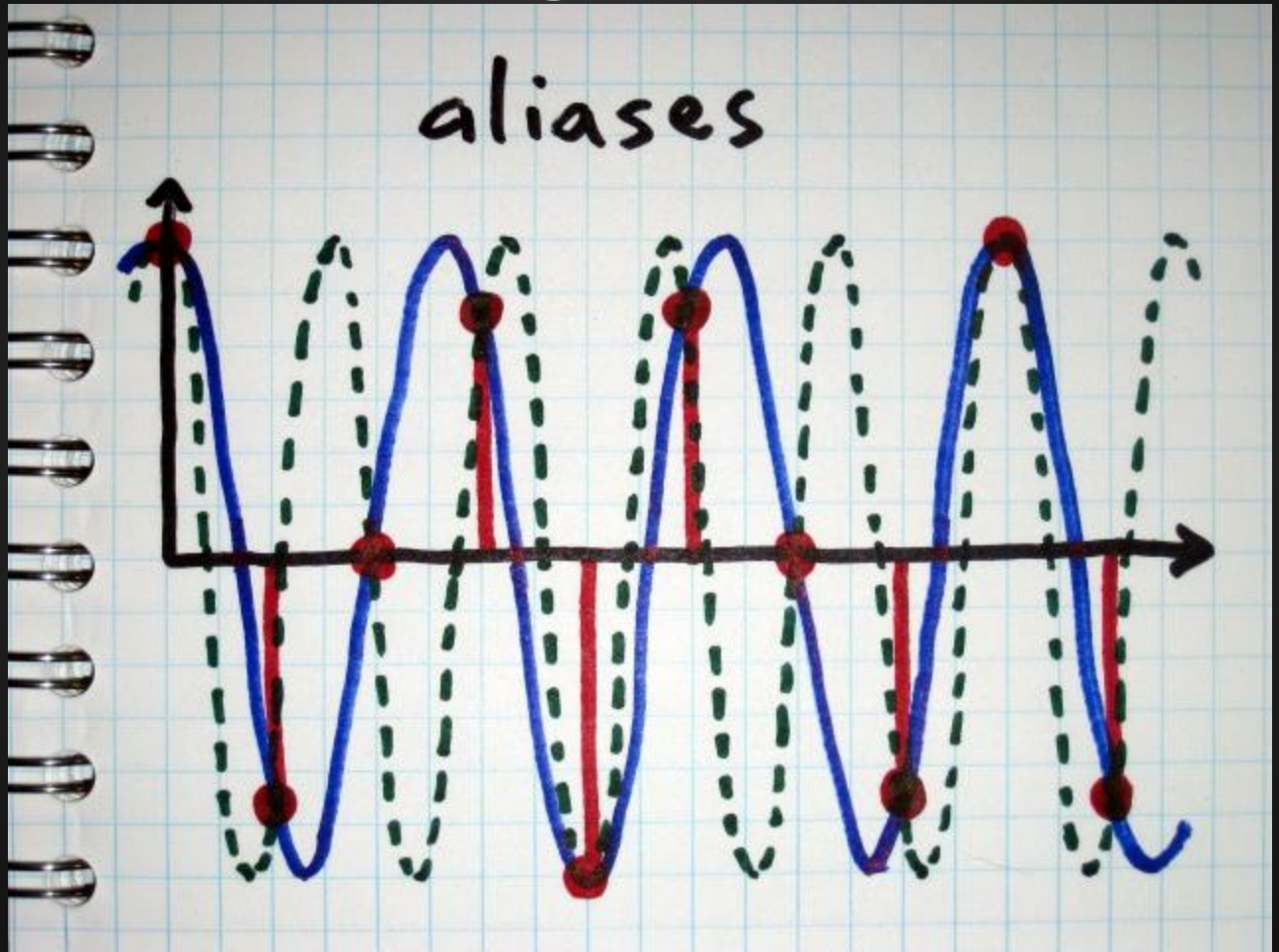
Intentional Aliasing



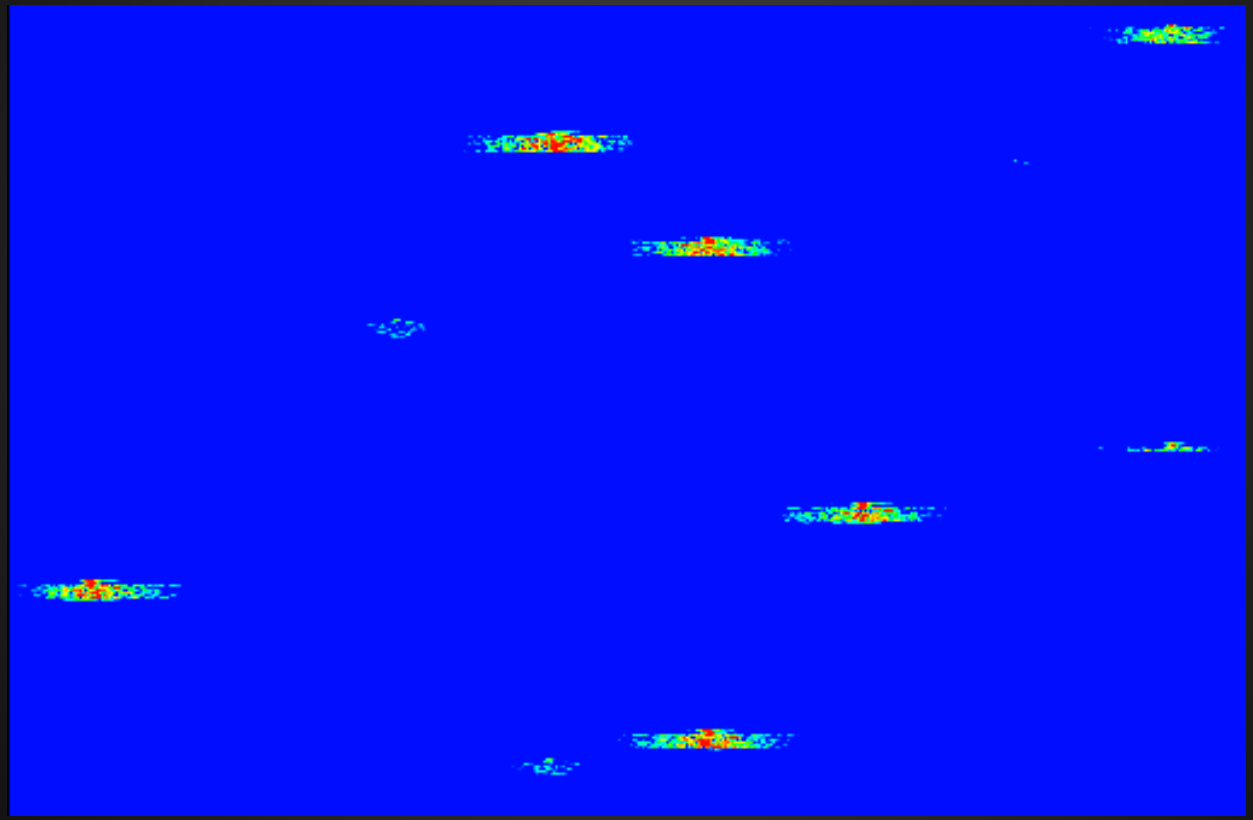
Intentional Aliasing



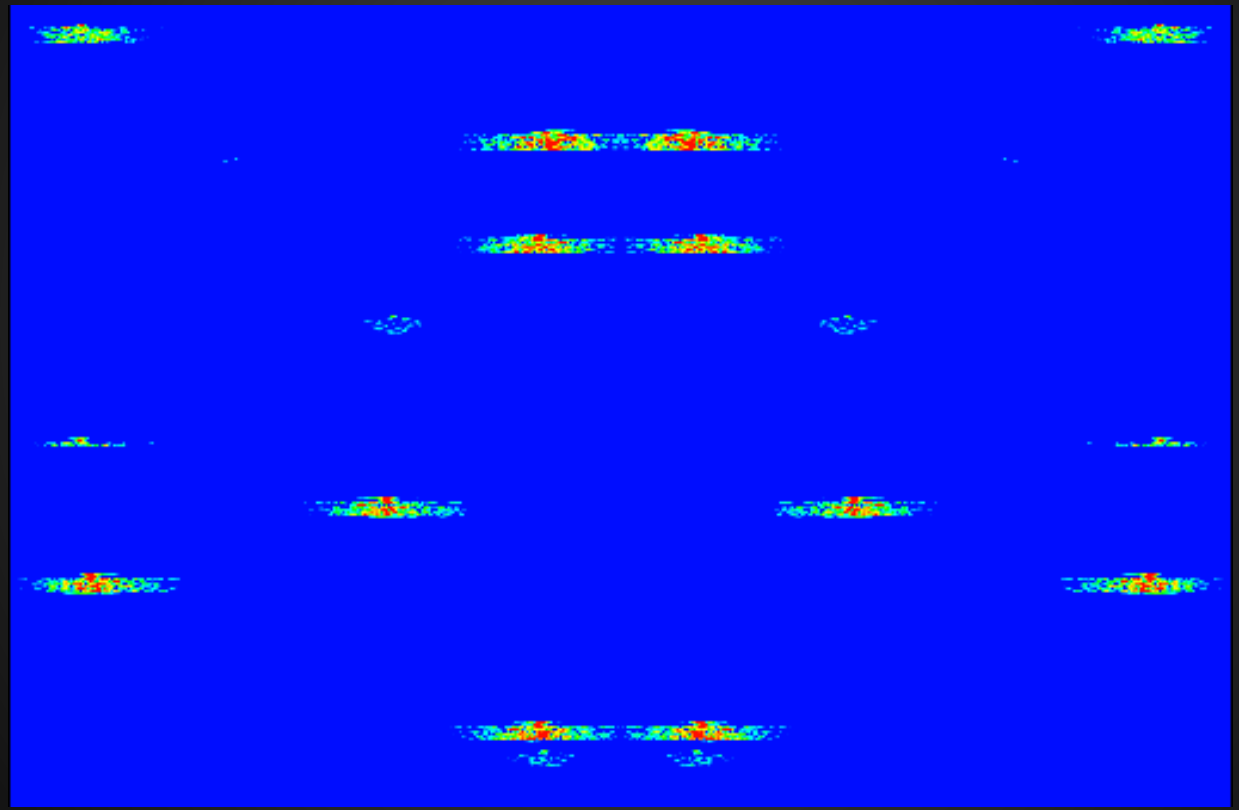
Intentional Aliasing



Intentional Aliasing



Intentional Aliasing



Intentional Aliasing

Aliased 4 times

Receive all Bluetooth channels

Problem Solved?

~$2000 USRP2 + hardware modification

Susceptible to noise

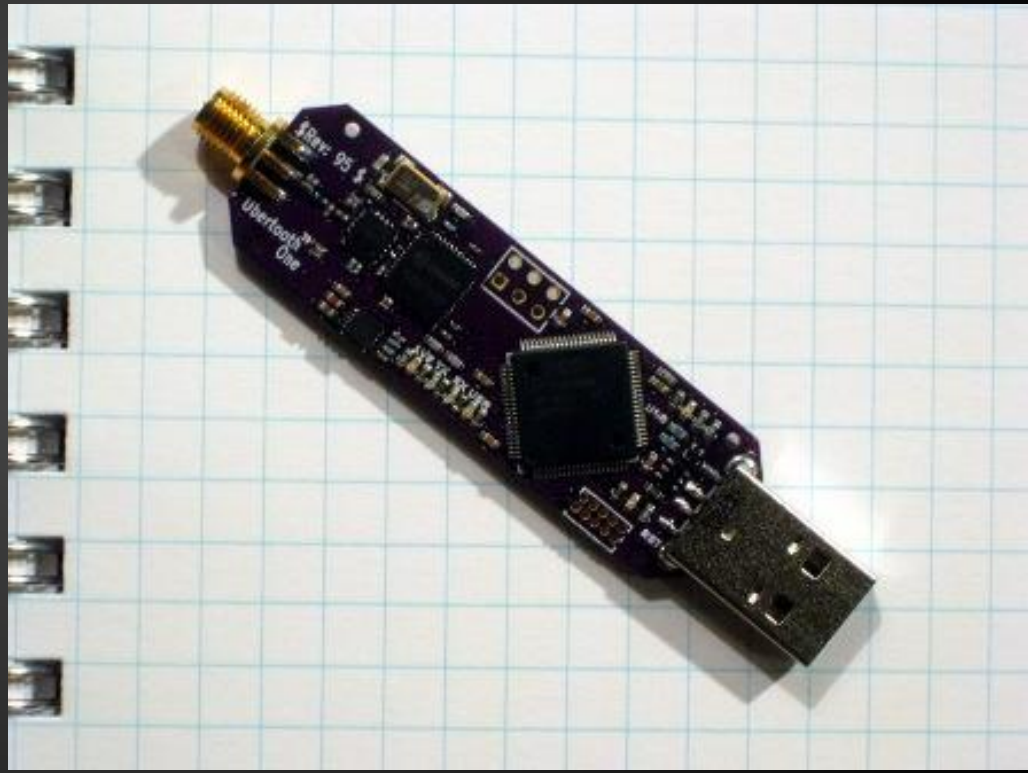
Ridiculous processing requirements

Ubertooth

2.4GHz Radio dongle

Open source
hardware + software

Cheap!



Ubertooth

Bluetooth modulation (Basic rate + Smart)

Stream bits to host

Still single channel

Transmit capabilities

Demonstration

The interesting bit...

Other Projects

HackRF

- SDR, 20MHz bandwidth, Rx/Tx, 1MHz-6GHz

Daisho

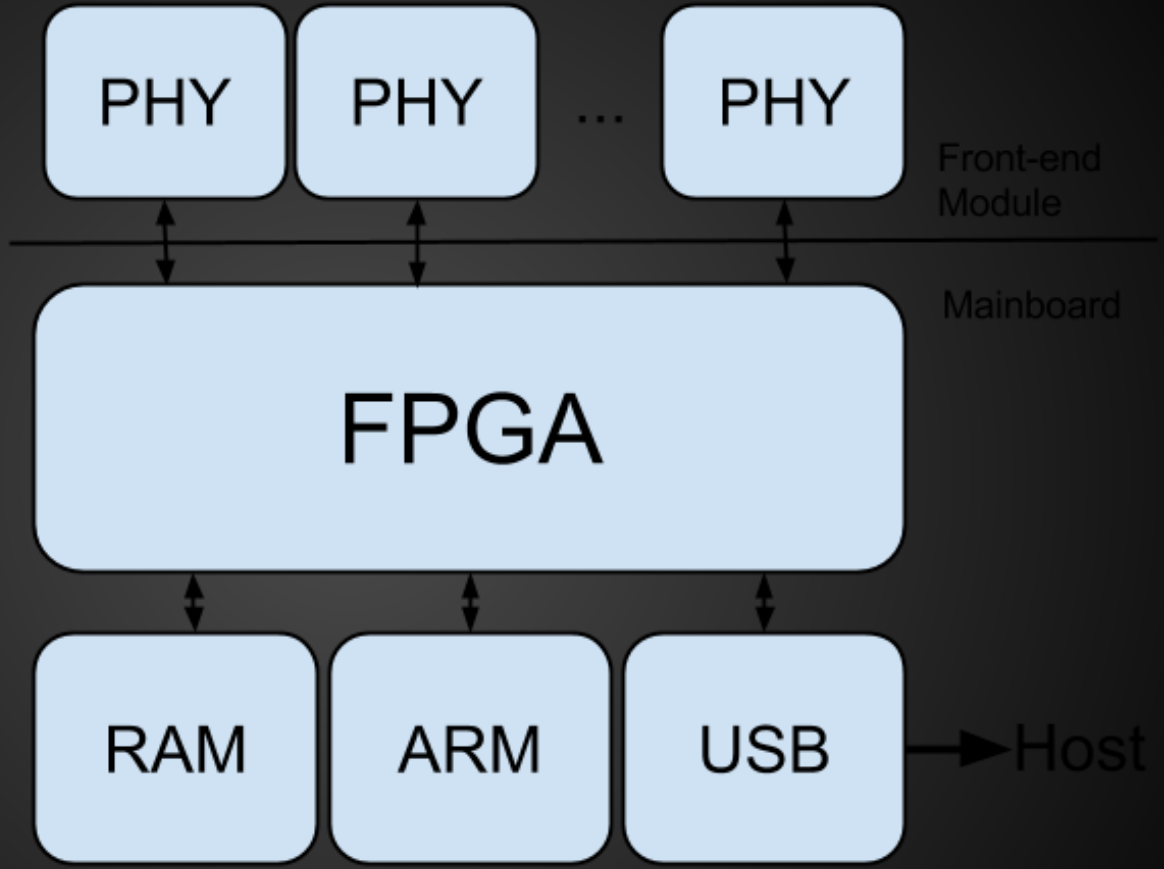
- High speed monitoring platform
- Targets: GigE, USB 3.0, HDMI
- Future targets: ASDL2+, Wideband SDR

HackRF

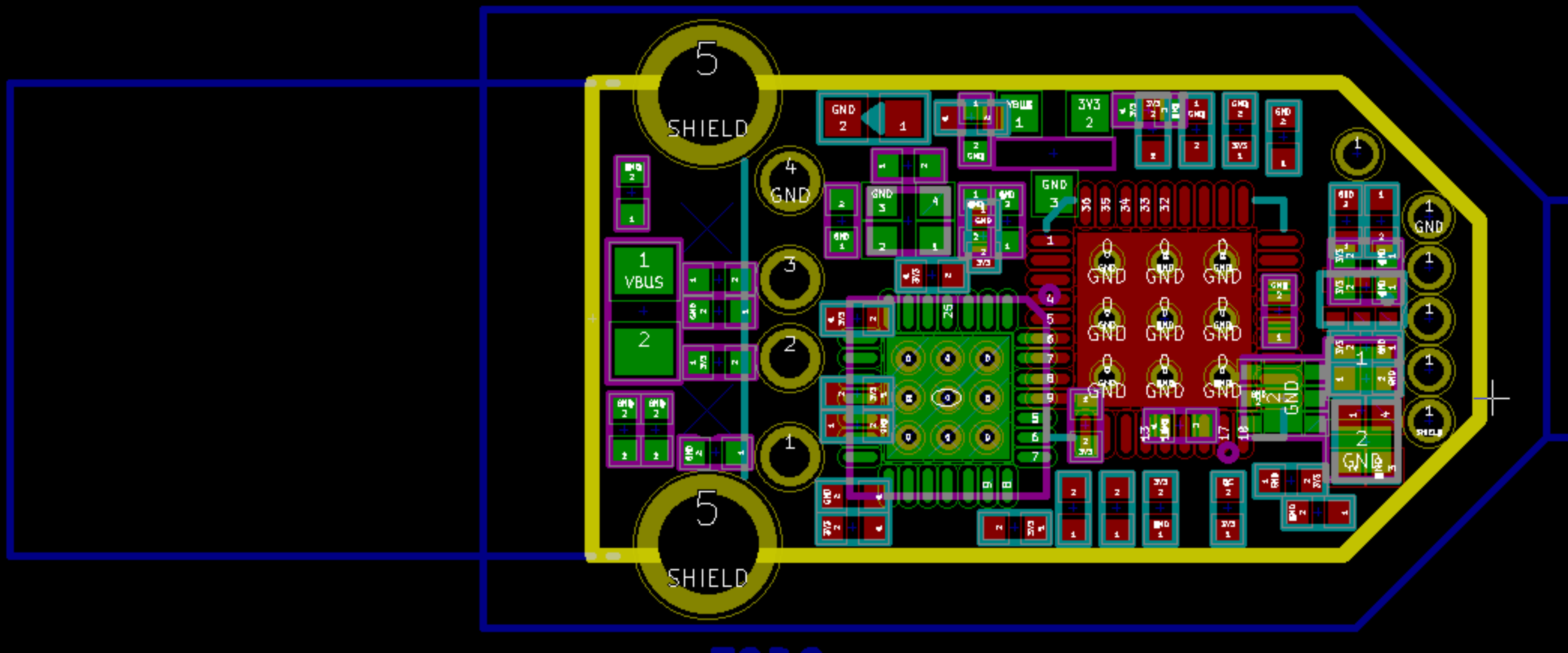

PROTOTYPE
HackRF One
GREAT SCOTT GADGETS
http://greatscottgadgets.com/hackrf/


PortaPack H1
20140512
ShareBrained Technology

Daisho



TurnipSchool



Questions?