NSA Playset: USB Tools

Dominic Spill
Michael Ossmann
Jared Boone

This presentation originally contained leaked, classified content.

This content has been redacted.

Redacted

Redacted

Redacted

USBProxy

Low cost USB 2.0

USBProxy Overview

Open source USB 2.0 proxy library

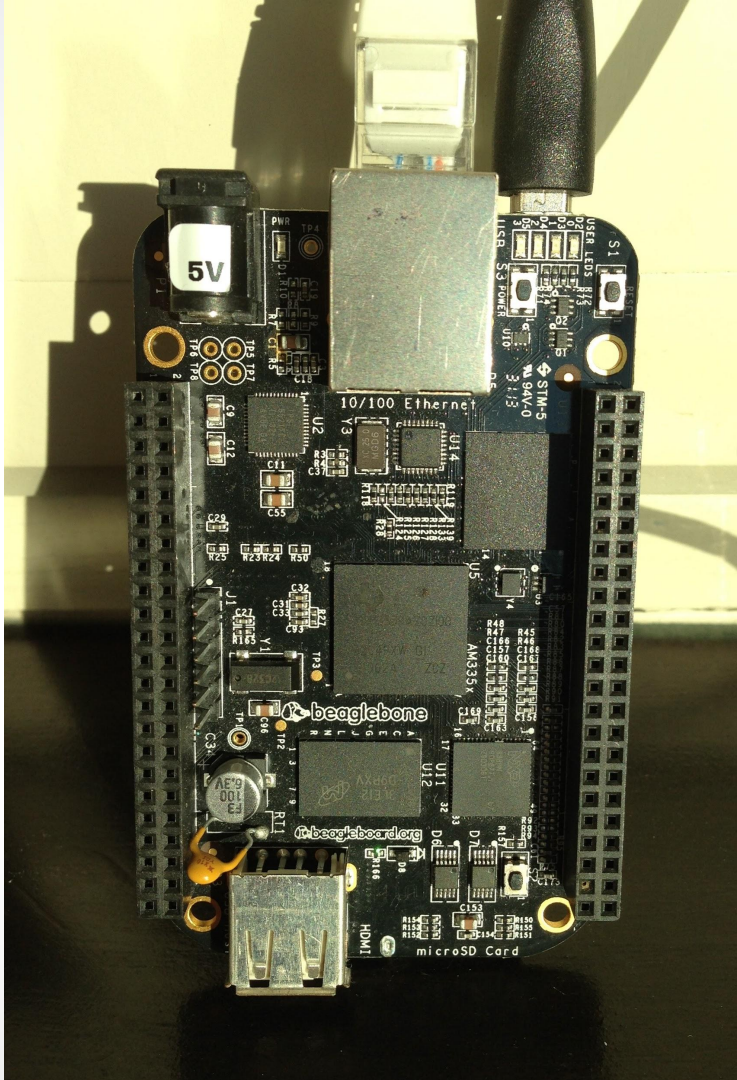
LibUSB and GadgetFS

BeagleBone Black (or similar)

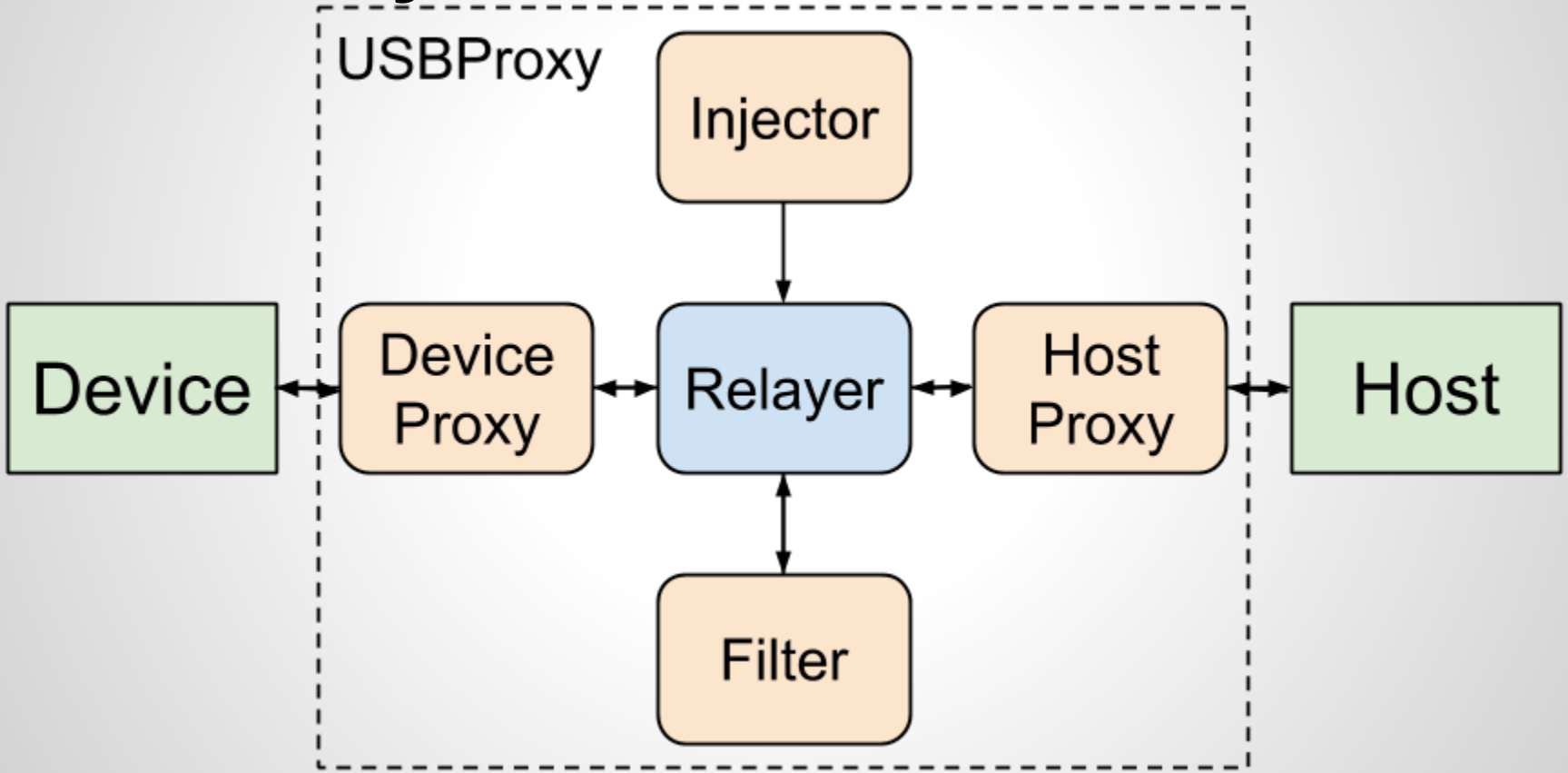
Hardware requirements

USB device controller

Able to run Linux



USBProxy Overview



What's new in USBProxy

Bug fixes

- There were a LOT of them

Write plugins in Python

- Just like FaceDancer

```
def handle_get_string_descriptor_request(self, num):
    if num == 0:
        # HACK: hard-coding baaaaad
        d = bytes([
                4,      # length of descriptor in bytes
                3,      # descriptor type 3 == string
                9,      # language code 0, byte 0
                4       # language code 0, byte 1
        ])
    else:
```

```
if idx == 0:
    p_nbytes[0] = 4
    # FIXME: don't hard-code this
    dataptr[0] = c_ubyte(0x04)
    dataptr[1] = c_ubyte(0x03)
    dataptr[2] = c_ubyte(0x09)
    dataptr[3] = c_ubyte(0x04)
    return 0
```

A word on demos

Keyboards are the calc.exe of USB devices

FaceDancer support

Demo

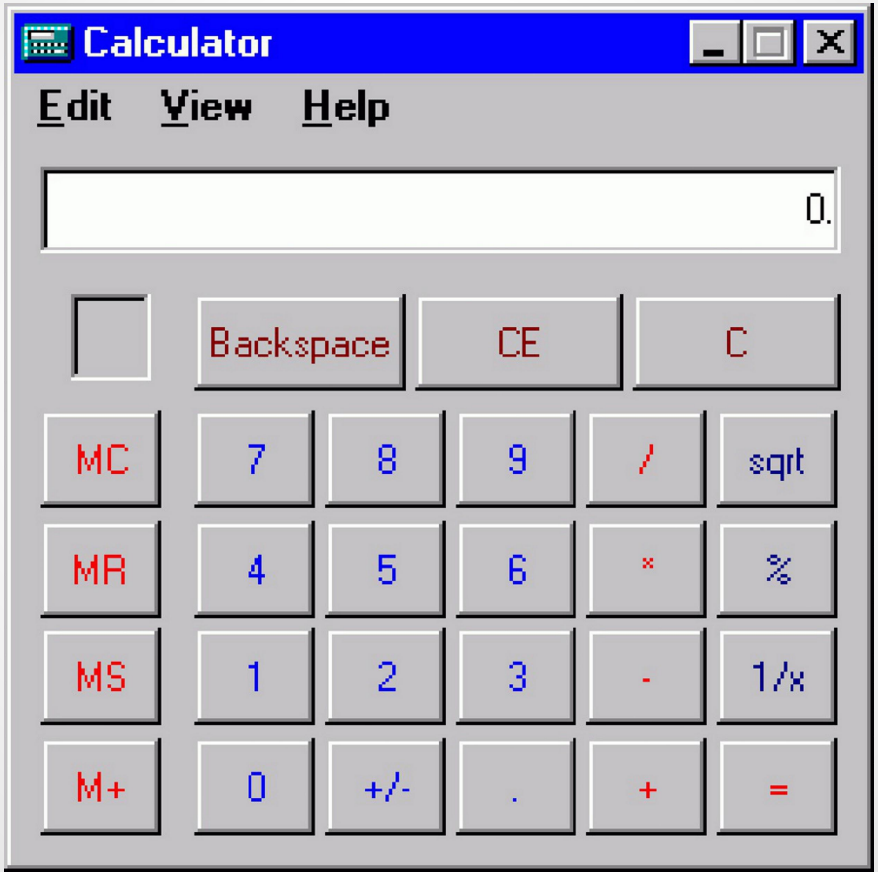
Feel free to pick on the Facedancer's limitations where appropriate.

-- Travis Goodspeed

What you saw - it’s a keyboard!!

```
[ 4726.243752] usb 1-1.2: new high-speed USB device number 12 using ehci-pci
[ 4726.367638] usb 1-1.2: New USB device found, idVendor=610b, idProduct=4653
[ 4726.367650] usb 1-1.2: Product: This is not the USB device you're looking for
[ 4726.367655] usb 1-1.2: Manufacturer: Move along
[ 4726.449866] input: Move along This is not the USB device you're looking for as
    /devices/pci0000:00/0000:00:1a.0/usb1/1-1/1-1.2/1-1.2:1.0/input/input13
```

What you didn’t see :(



Whats next?

USB/IP implementation

Fixes for strange FaceDancer implementations

Fix all the bugs

Daisho

USB 3.0 SuperSpeed

USB 3: Targets

Exploits:

- PC XHCI firmware
- Operating system USB stack
- Device firmware

Sniff, alter, inject data on bus -- MITM

USB 3: Applications

- Mass storage
- Video capture
- Video display
- Ethernet
- Host-host transfer cable
- Docking stations

USB 3: Background

Serial bus, full duplex.

500M bytes/second, two 5Gbps links.

Link establishment is complex.

Off-the-shelf PHYs exist, thankfully.

USB 3: Challenges

Link is very high speed.

PCB design is tricky.

Link negotiation protocol complex.

Scrambling.

TX/RX clock offset.

USB 3: Timing is Critical

Events at microsecond level.

Data rate is high.

Scrambling, clock management must be done in hardware.

USB 3: FPGA is the Answer

Ideal for time-sensitive events.

Ideal for reliable, deterministic inspection and manipulation of high speed data streams.

Daisho: Main Board

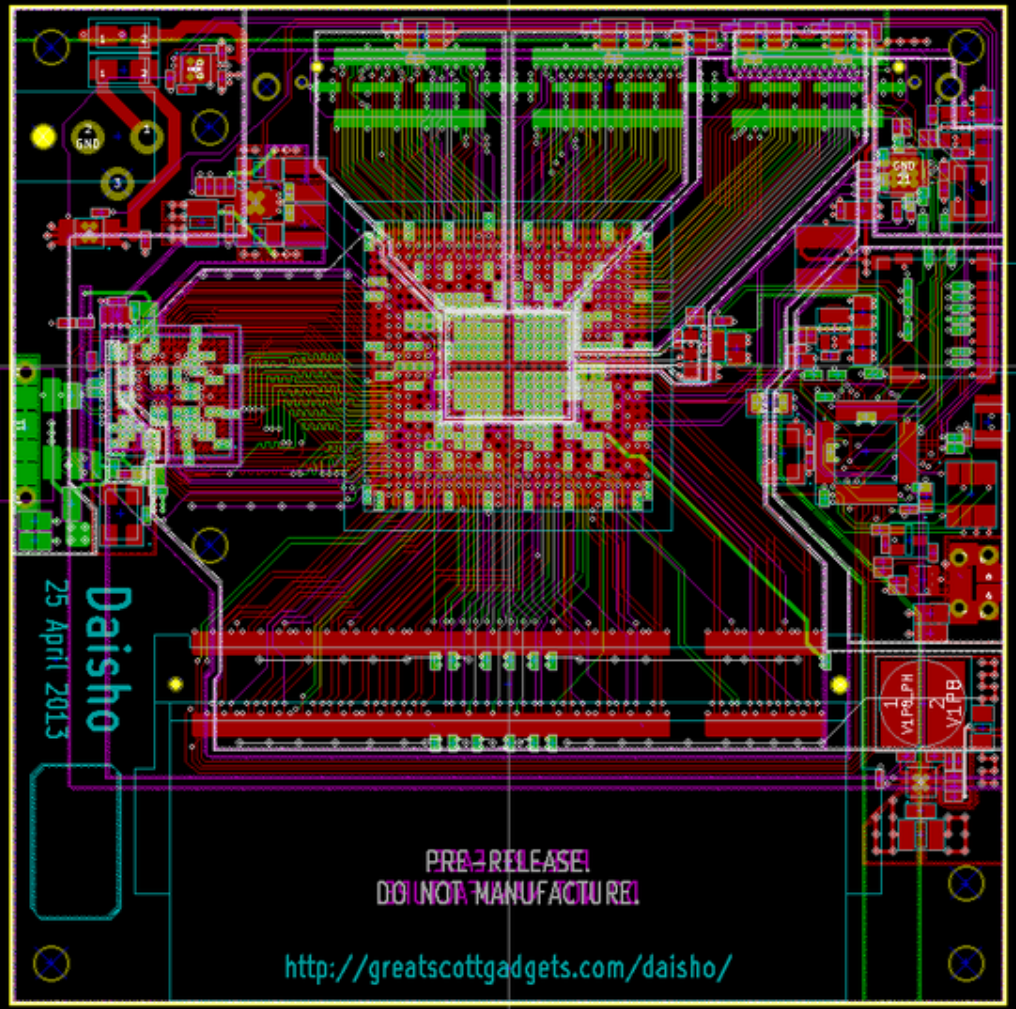
FPGA (Altera Cyclone IV)

DDR2 RAM socket

USB 3.0 interface (TUSB1310A PHY)

Microcontroller for power/config

HSMC connector



Layer Stack:

Signal 1 (top): 35um Cu + plating (8um)
Microstrip: 50 Ohms +/- 10% @ 0.15mm

100um prepreg, 370HR Dk=4.24 @ 100MHz

Top Ground: 35um Cu

200um core, 370HR Dk=4.24 @ 100MHz

Top Power: 35um Cu

100 um prepreg, 370HR Dk=4.24 @ 100MHz

Signal 2: 35um Cu
Asymmetric stripline: 50 Ohms +/- 10% @ 0.15mm

8 mil core, 370HR Dk=4.24 @ 100MHz

Signal 3: 35um Cu
Asymmetric stripline: 50 Ohms +/- 10% @ 0.15mm

100um prepreg, 370HR Dk=4.24 @ 100MHz

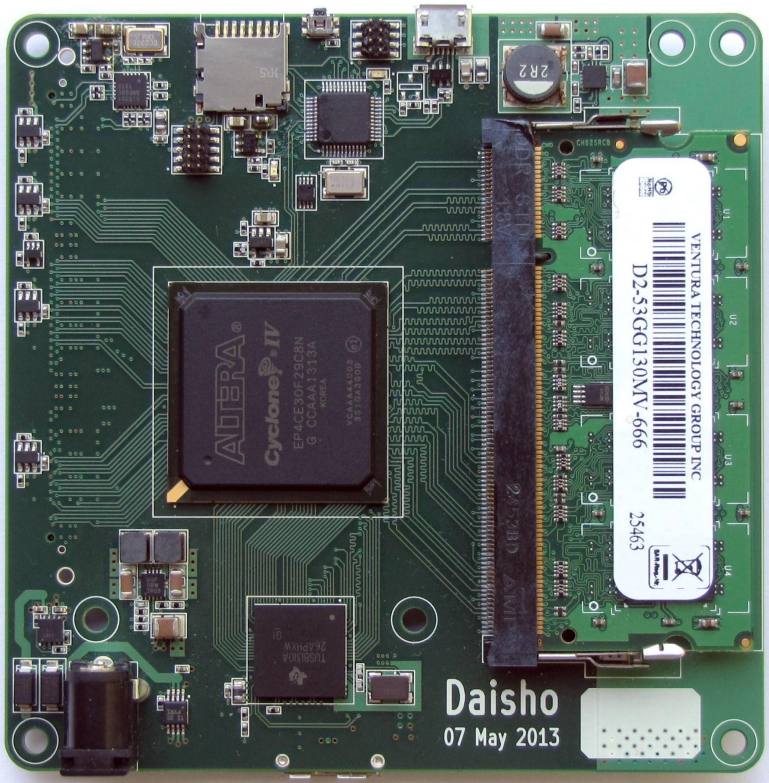
Bottom Power: 35um Cu

200um core, 370HR Dk=4.24 @ 100MHz

Bottom Ground: 35um Cu

100um prepreg, 370HR Dk=4.24 @ 100MHz

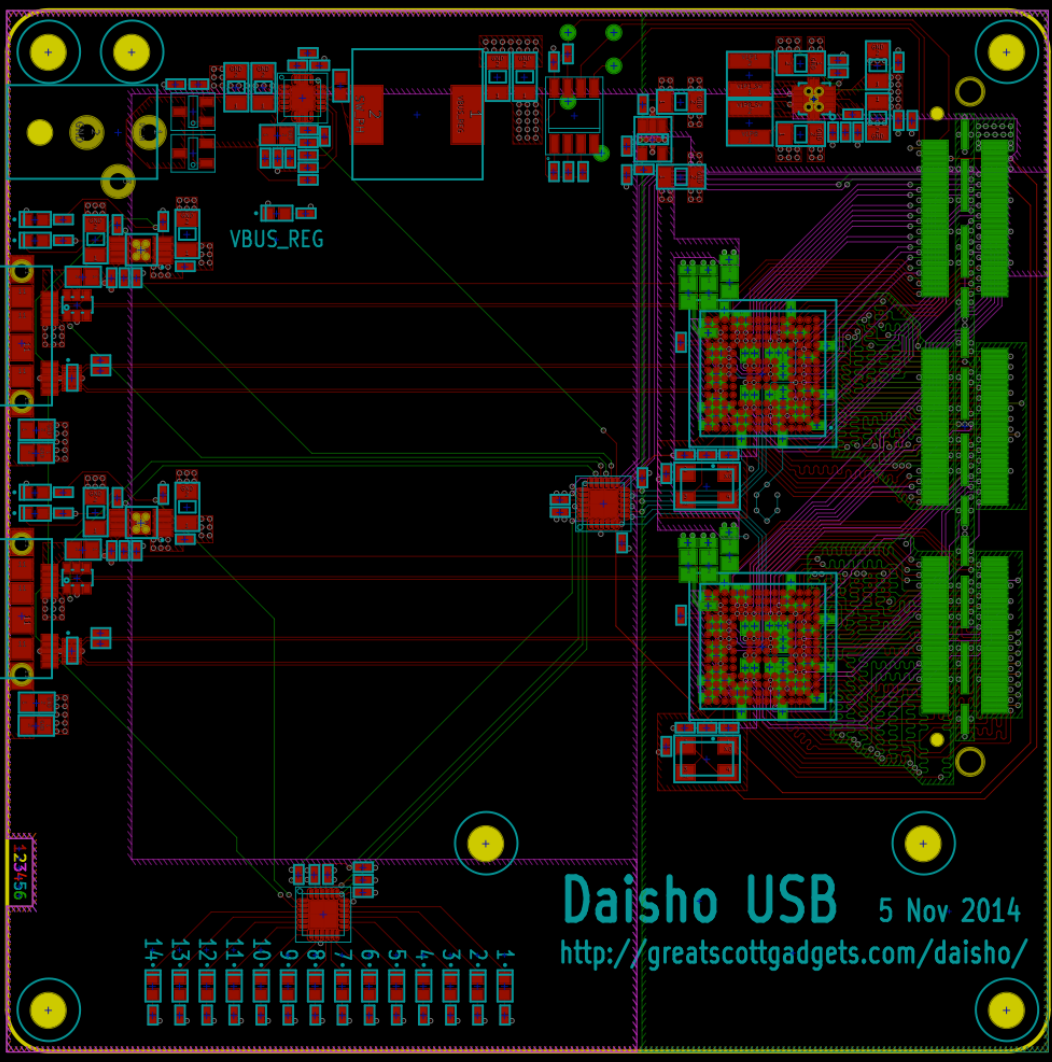
Signal 4 (bottom): 35um Cu + plating (8um)
Microstrip: 50 Ohms +/- 10% @ 0.15mm

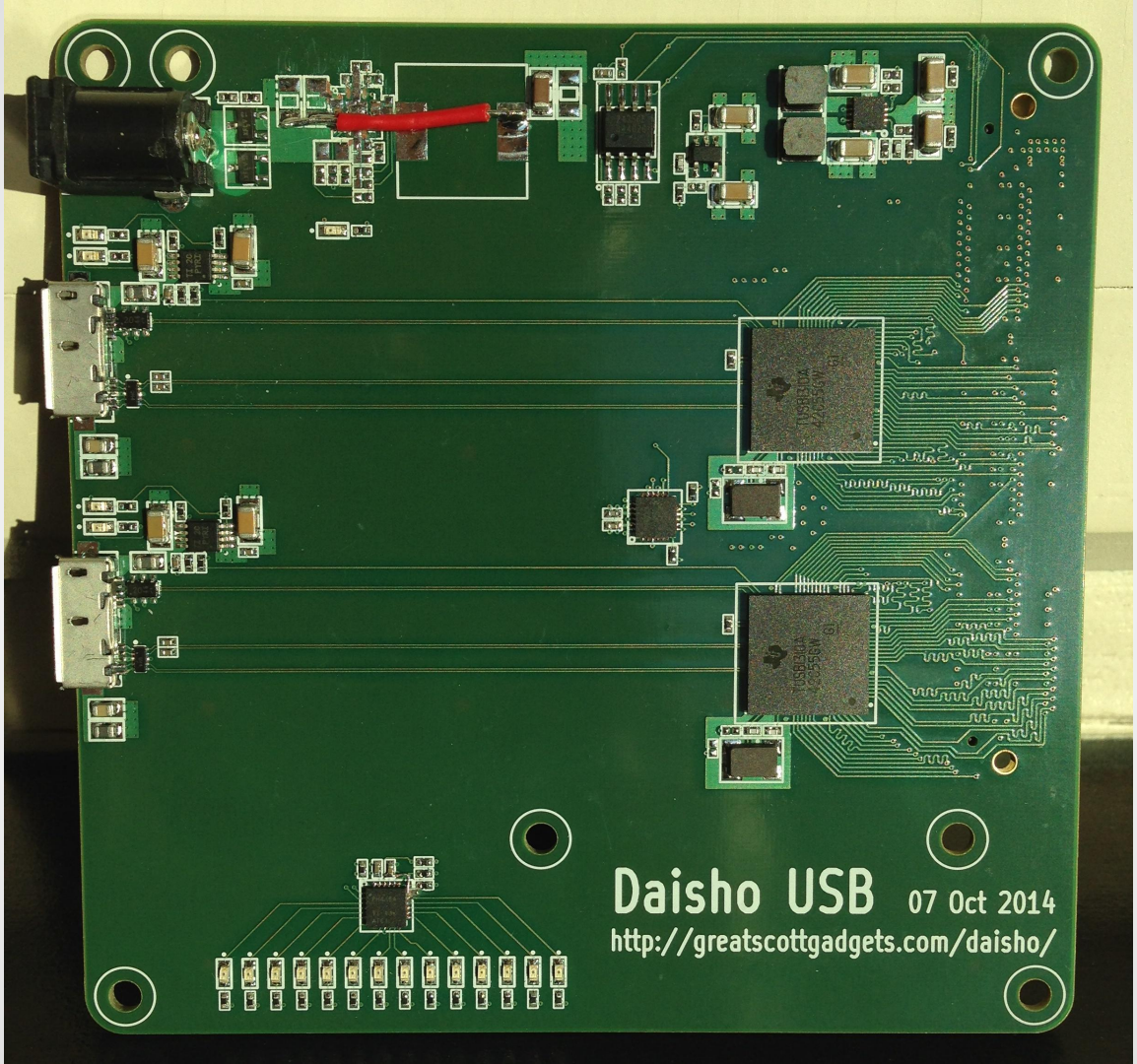

ALTERA
Cyclone IV
EP4CE30F23C8N
Daisho
07 May 2013
VENTURA TECHNOLOGY GROUP INC
D2-53GG130MV-666
25463

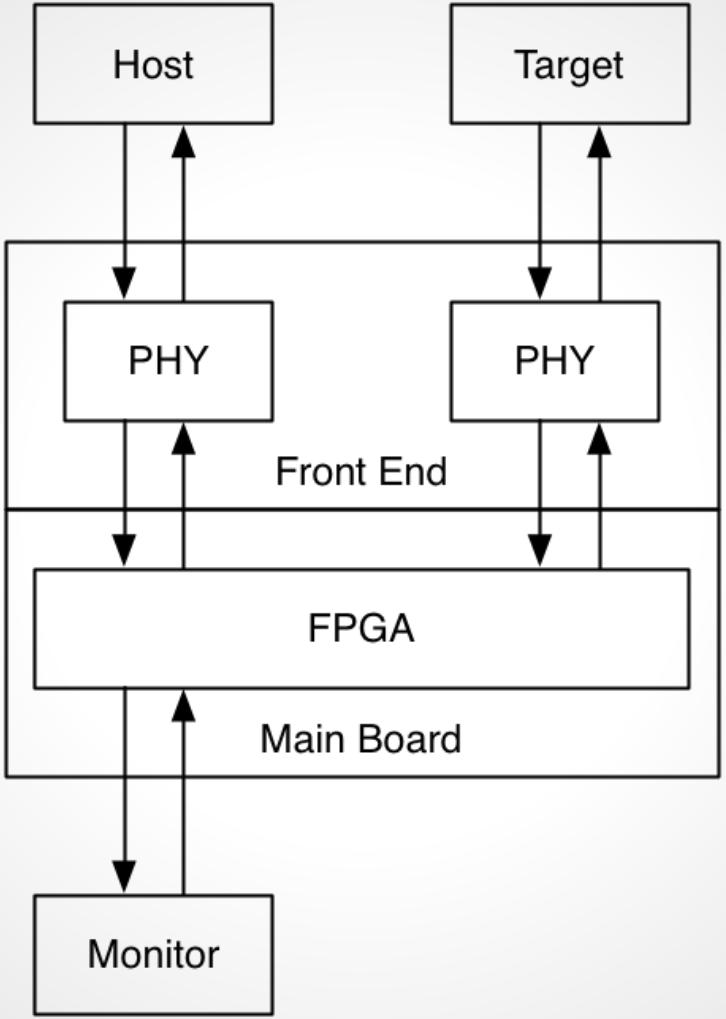
Daisho: USB Front End

Two more USB 3.0 PHYs

Regulator for supplying USB bus power


VBUS_REG
Daisho USB
5 Nov 2014
http://greatscottgadgets.com/daisho/


Daisho USB
07 Oct 2014
http://greatscottgadgets.com/daisho/


Host
Target
PHY
PHY
Front End
FPGA
Main Board
Monitor

USB 3: Handshaking

RxDetect

LFPS

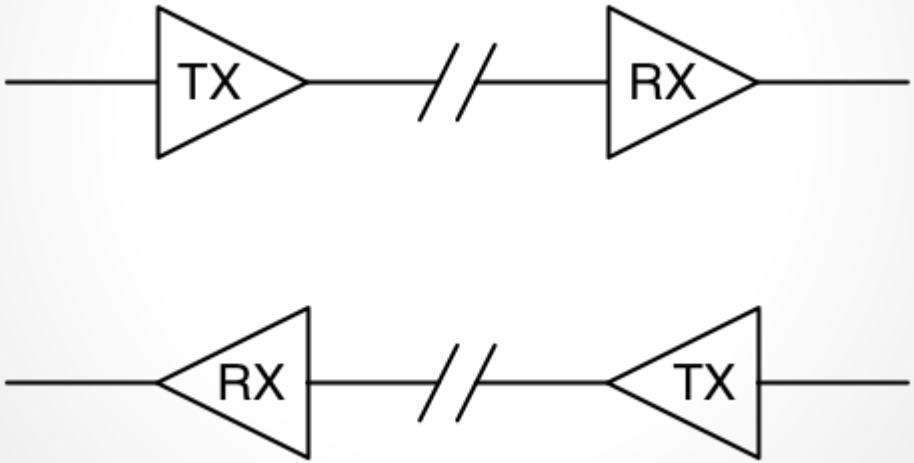
Training

Link Config

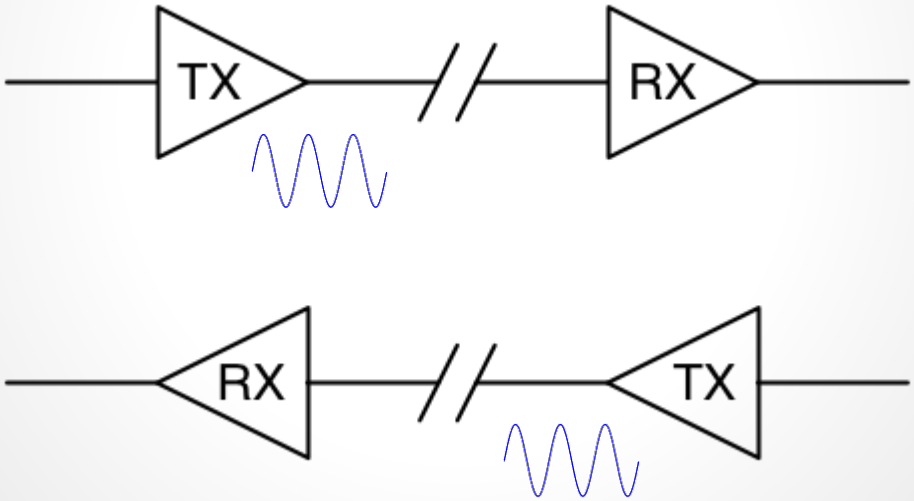
Enumeration

Control/Data transfer

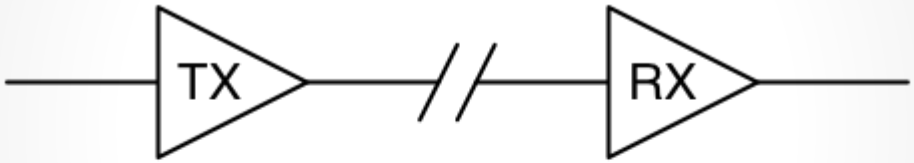
USB 3: RxDetect



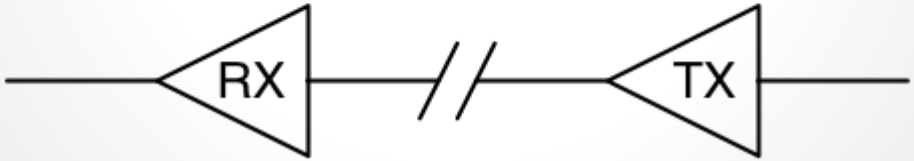
USB 3: LFPS



USB 3: Training

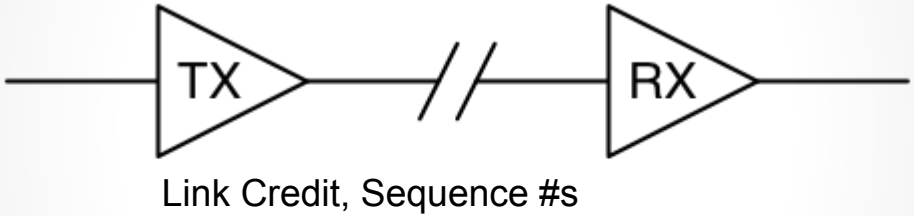


TSEQ, TS1, TS2

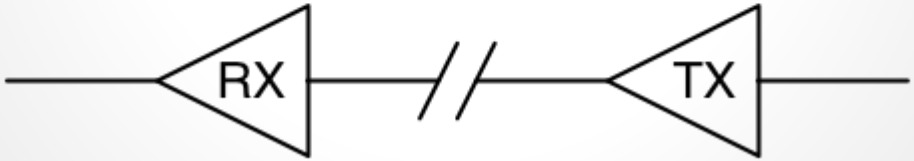


TSEQ, TS1, TS2

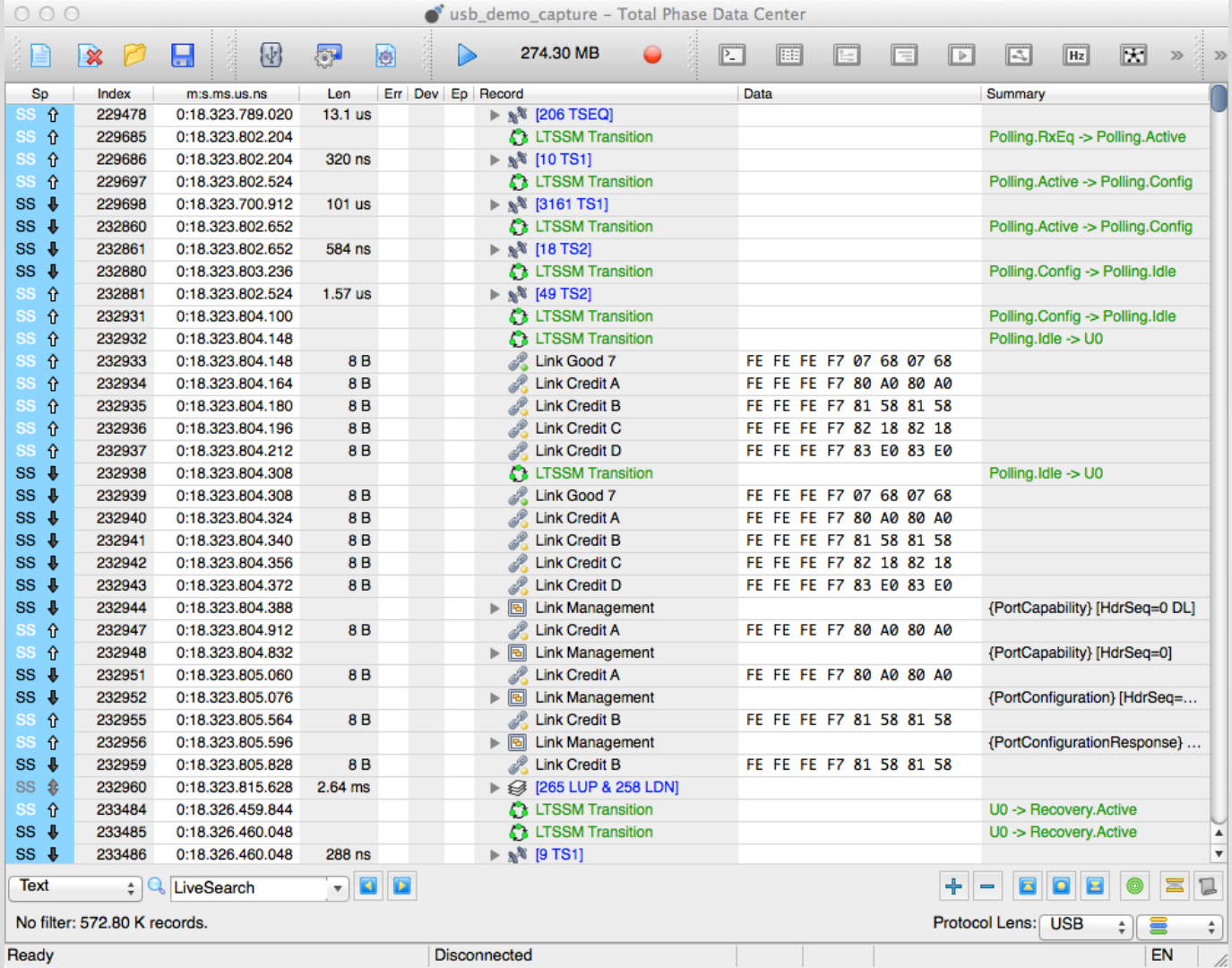
USB 3: Link Config



Link Credit, Sequence #s



Link Credit, Sequence #s


usb_demo_capture - Total Phase Data Center
274.30 MB
Sp Index m:s.ms.us.ns Len Err Dev Ep Record Data Summary
SS 229478 0:18.323.789.020 13.1 us [206 TSEQ]
SS 229685 0:18.323.802.204 LTSSM Transition Polling.RxEq -> Polling.Active
SS 229686 0:18.323.802.204 320 ns [10 TS1]
SS 229697 0:18.323.802.524 LTSSM Transition Polling.Active -> Polling.Config
SS 229698 0:18.323.700.912 101 us [3161 TS1]
SS 232860 0:18.323.802.652 LTSSM Transition Polling.Active -> Polling.Config
SS 232861 0:18.323.802.652 584 ns [18 TS2]
SS 232880 0:18.323.803.236 LTSSM Transition Polling.Config -> Polling.Idle
SS 232881 0:18.323.802.524 1.57 us [49 TS2]
SS 232931 0:18.323.804.100 LTSSM Transition Polling.Config -> Polling.Idle
SS 232932 0:18.323.804.148 LTSSM Transition Polling.Idle -> U0
SS 232933 0:18.323.804.148 8 B Link Good 7 FE FE FE F7 07 68 07 68
SS 232934 0:18.323.804.164 8 B Link Credit A FE FE FE F7 80 A0 80 A0
SS 232935 0:18.323.804.180 8 B Link Credit B FE FE FE F7 81 58 81 58
SS 232936 0:18.323.804.196 8 B Link Credit C FE FE FE F7 82 18 82 18
SS 232937 0:18.323.804.212 8 B Link Credit D FE FE FE F7 83 E0 83 E0
SS 232938 0:18.323.804.308 LTSSM Transition Polling.Idle -> U0
SS 232939 0:18.323.804.308 8 B Link Good 7 FE FE FE F7 07 68 07 68
SS 232940 0:18.323.804.324 8 B Link Credit A FE FE FE F7 80 A0 80 A0
SS 232941 0:18.323.804.340 8 B Link Credit B FE FE FE F7 81 58 81 58
SS 232942 0:18.323.804.356 8 B Link Credit C FE FE FE F7 82 18 82 18
SS 232943 0:18.323.804.372 8 B Link Credit D FE FE FE F7 83 E0 83 E0
SS 232944 0:18.323.804.388 Link Management {PortCapability} [HdrSeq=0 DL]
SS 232947 0:18.323.804.912 8 B Link Credit A FE FE FE F7 80 A0 80 A0
SS 232948 0:18.323.804.832 Link Management {PortCapability} [HdrSeq=0]
SS 232951 0:18.323.805.060 8 B Link Credit A FE FE FE F7 80 A0 80 A0
SS 232952 0:18.323.805.076 Link Management {PortConfiguration} [HdrSeq=...
SS 232955 0:18.323.805.564 8 B Link Credit B FE FE FE F7 81 58 81 58
SS 232956 0:18.323.805.596 Link Management {PortConfigurationResponse} ...
SS 232959 0:18.323.805.828 8 B Link Credit B FE FE FE F7 81 58 81 58
SS 232960 0:18.323.815.628 2.64 ms [265 LUP & 258 LDN]
SS 233484 0:18.326.459.844 LTSSM Transition U0 -> Recovery.Active
SS 233485 0:18.326.460.048 LTSSM Transition U0 -> Recovery.Active
SS 233486 0:18.326.460.048 288 ns [9 TS1]
Text
LiveSearch
No filter: 572.80 K records.
Protocol Lens: USB
Ready
Disconnected
EN

USB 3: What's Done

Hardware appears solid.

USB 3.0 stack for monitoring port.

Pass-through up to enumeration.

Accidental fuzzing...

USB 3: Future Work

Fuzzing firmware, operating systems.

Altering data between host and target.

Spoofing devices not present.

Wholesale recording and replay.

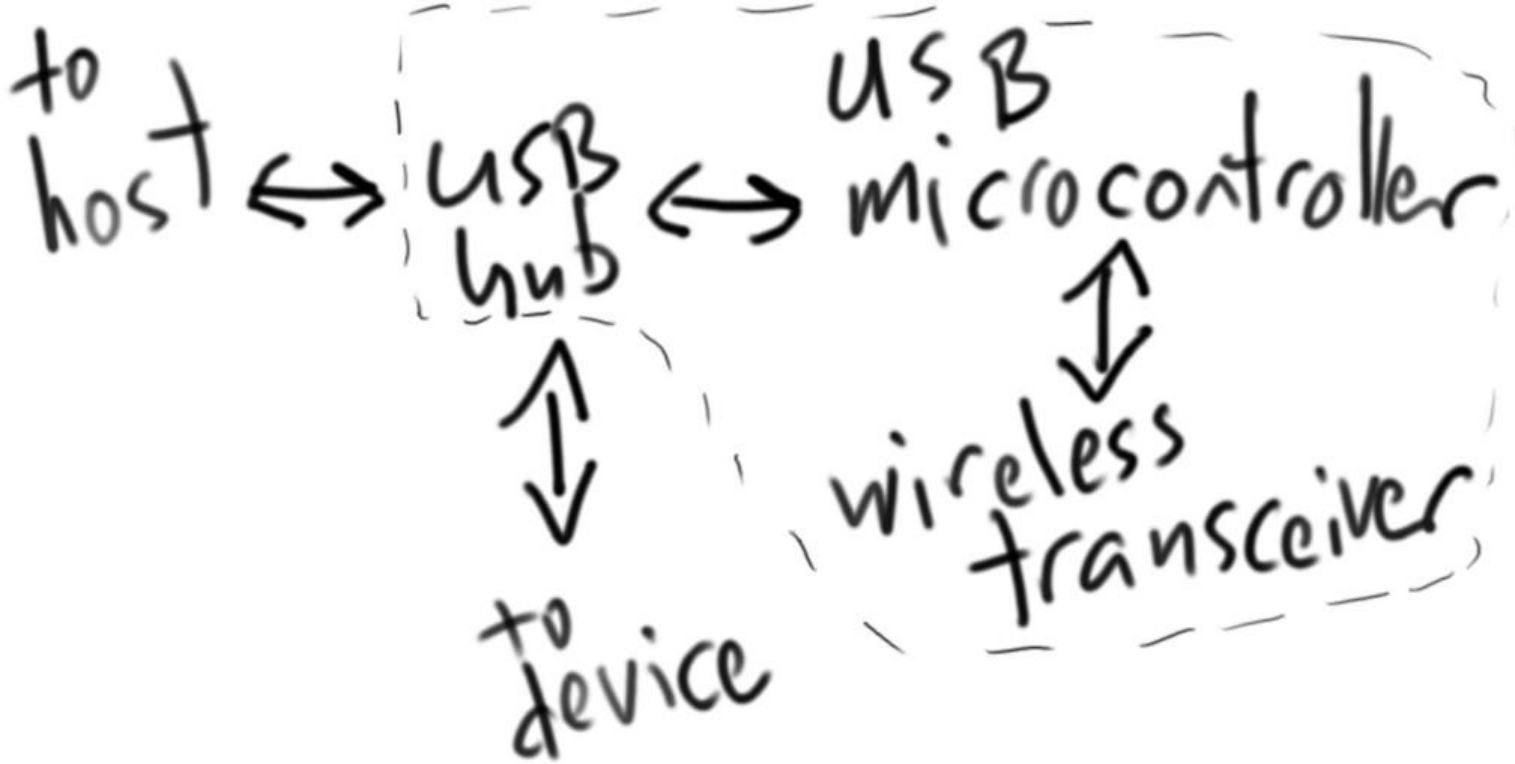
Miniaturization.

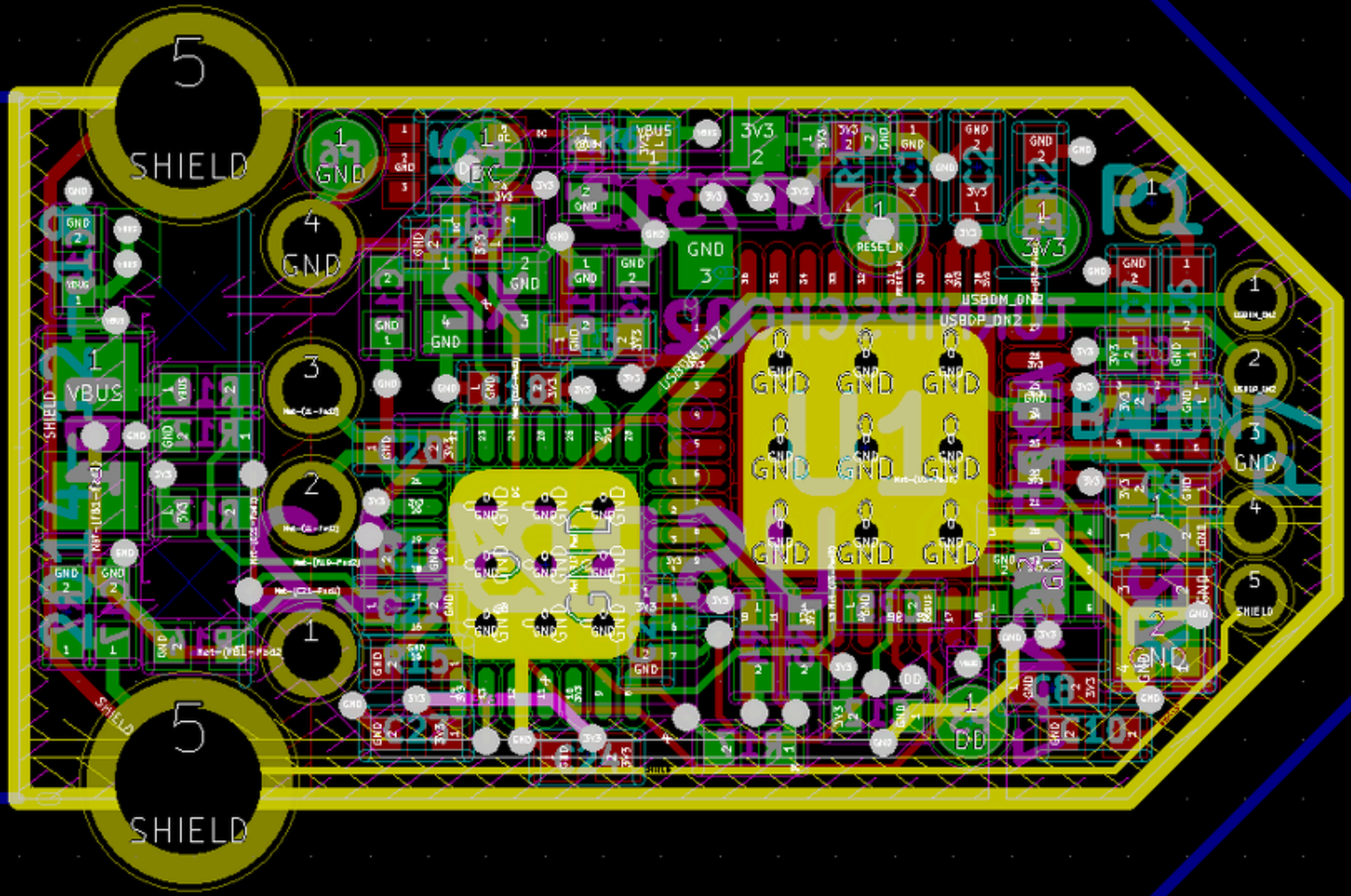
TURNIPSCHOOL

CABLES THAT BITE

Redacted

Redacted


to host
USB hub
USB microcontroller
wireless transceiver
to device


SHIELD
SHIELD
GND
GND
VBUS
RESET_N
3V3
USBDM_DN2
USBDP_DN2
U1
GND
SHIELD

CC1111

Sub-1 GHz RF transceiver

8051 microcontroller

32 kB flash memory

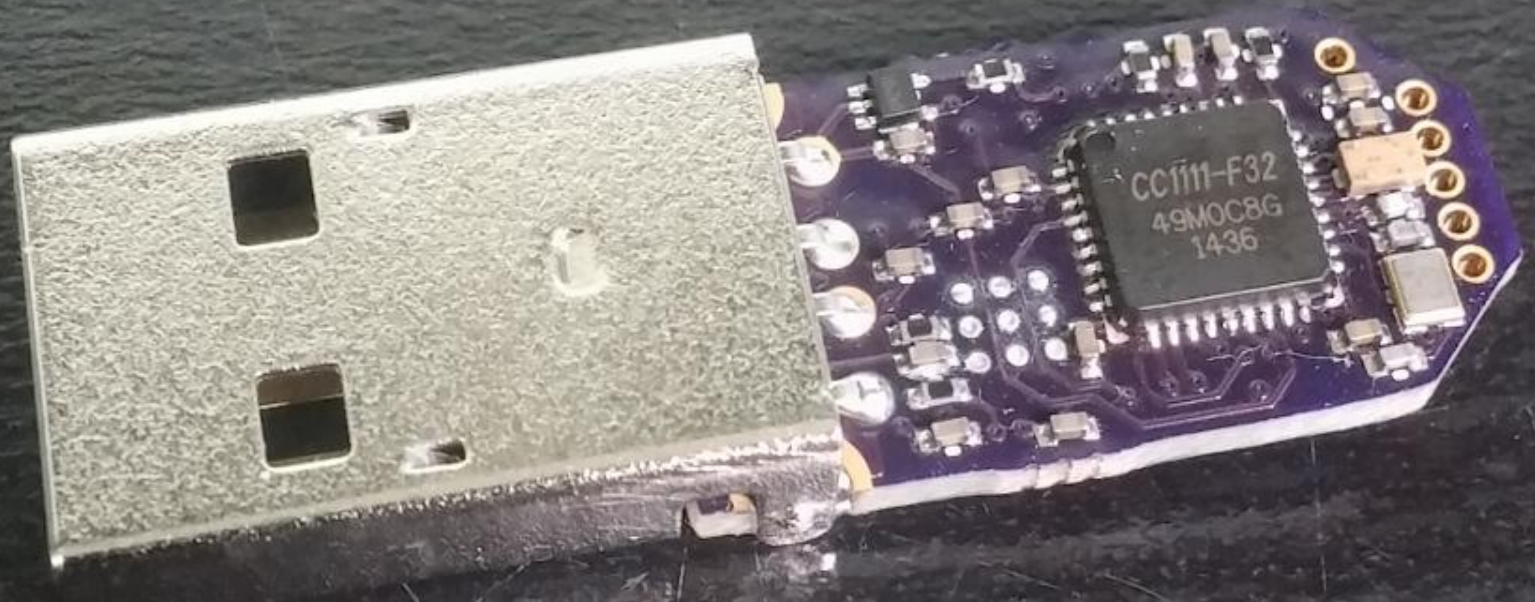
4 kB RAM

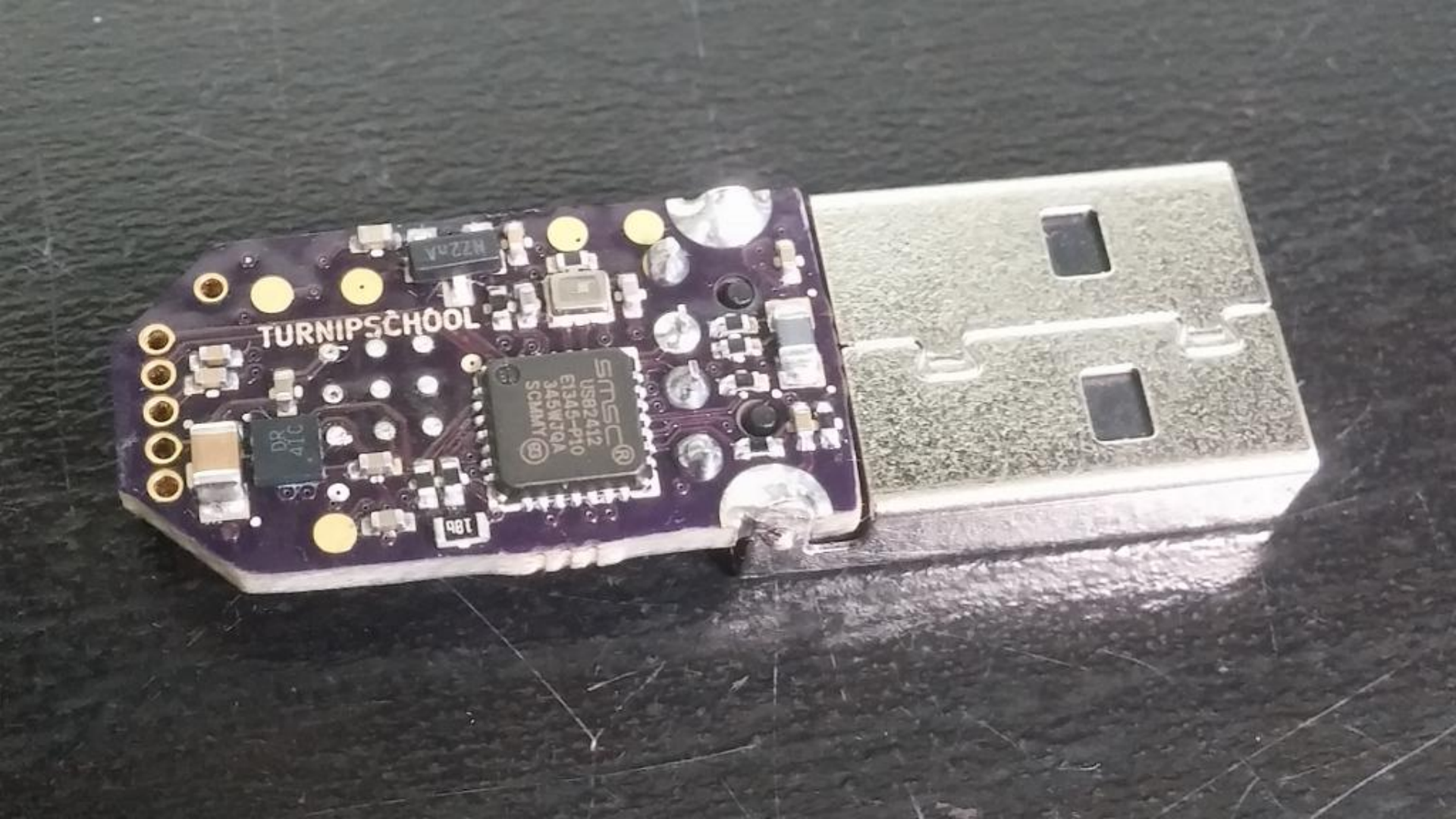
Full-Speed USB device controller

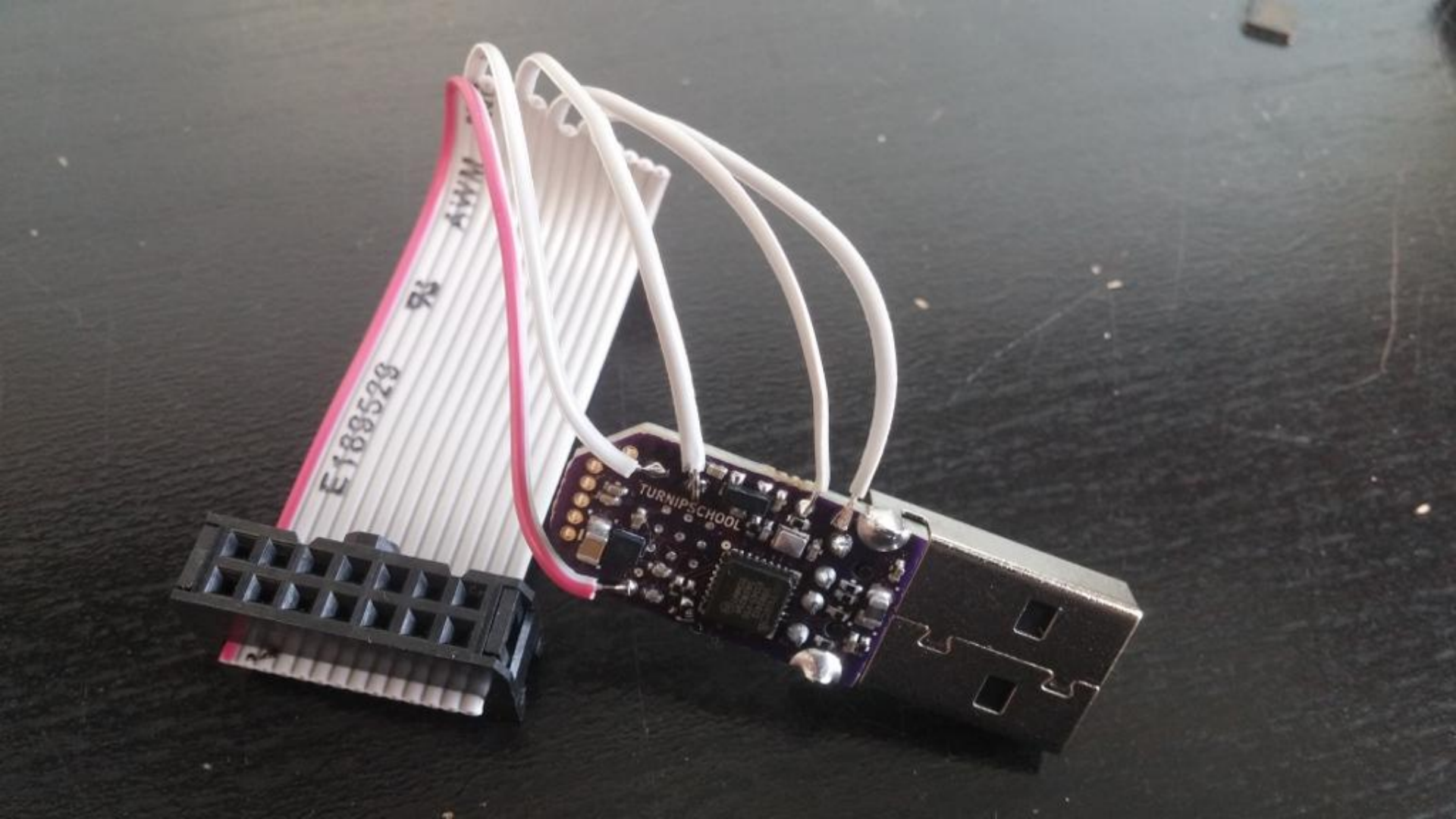
GoodFET-programmable

IM-Me

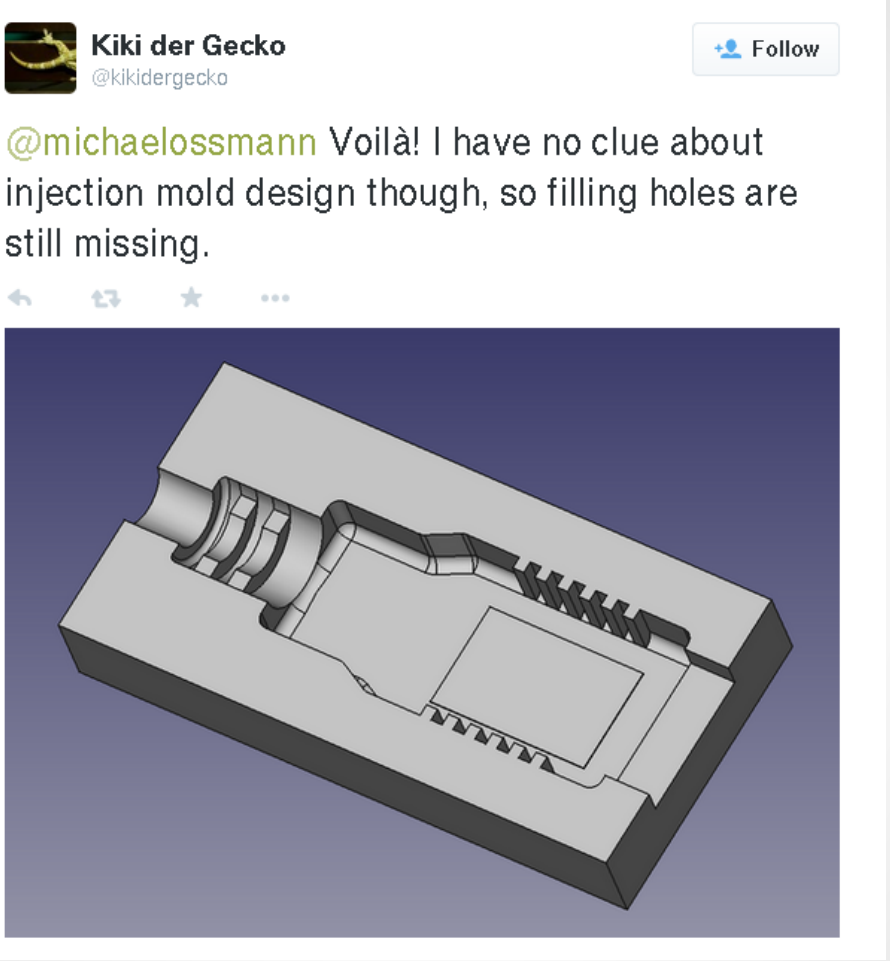
YARD Stick One


CC1111-F32
49M0C8G
1436

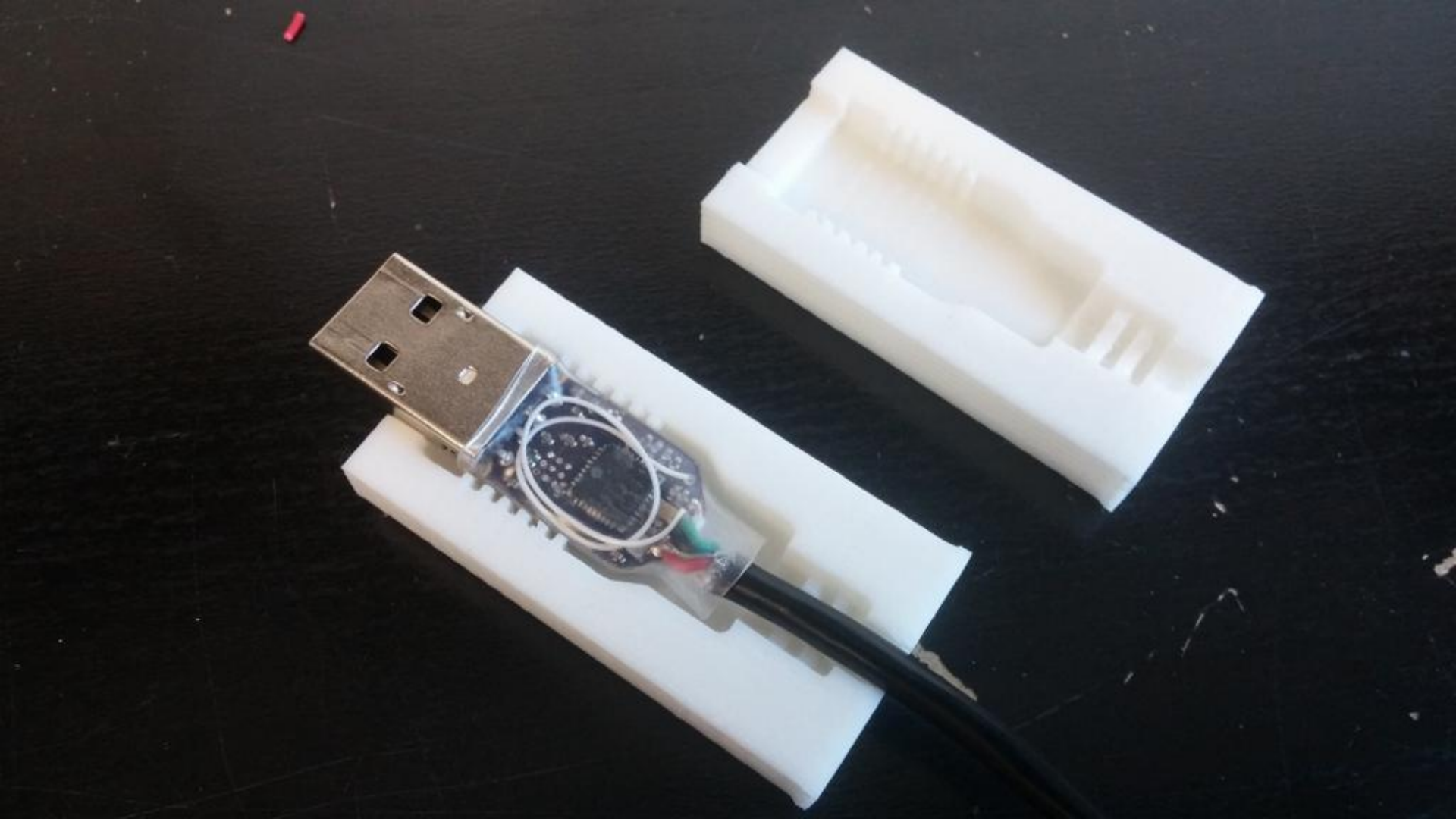

TURNIPSCHOOL
smsc
USB2412
E1345-P10
345W1QA
SCHMAY

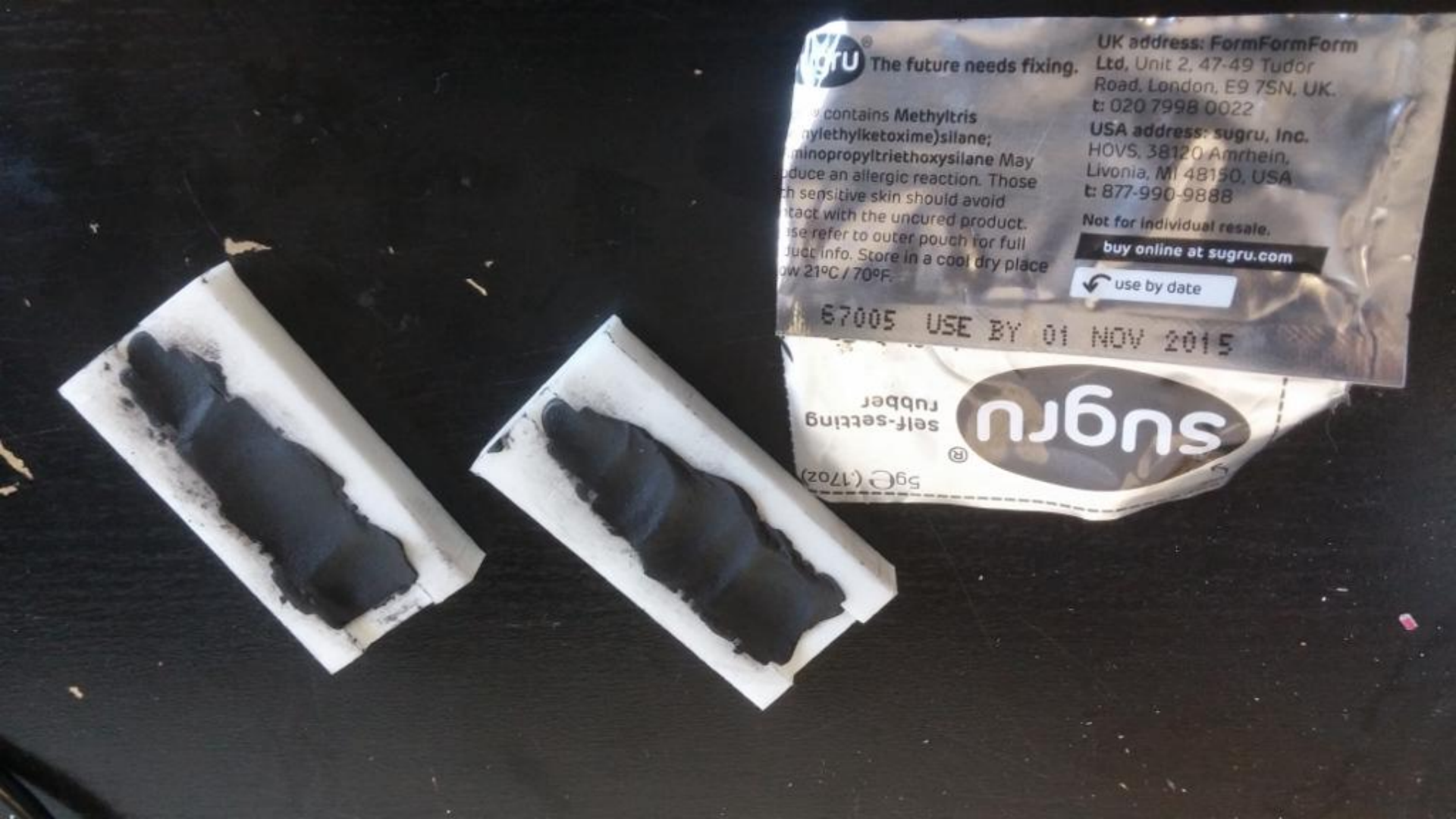

E189529
TURNIPSCHOOL

```
[ 1472.458043] usb 3-2: new high-speed USB device number 3 using xhci_hcd
[ 1472.469302] usb 3-2: New USB device found, idVendor=0424, idProduct=2412
[ 1472.470143] hub 3-2:1.0: USB hub found
[ 1472.470274] hub 3-2:1.0: 2 ports detected
[ 1472.470302] hub 3-2:1.0: individual port power switching
[ 1472.470313] hub 3-2:1.0: individual port over-current protection
[ 1472.470798] hub 3-2:1.0: enabling power on all ports
[ 1472.744448] usb 3-2.2: new full-speed USB device number 4 using xhci_hcd
[ 1472.758601] usb 3-2.2: New USB device found, idVendor=1d50, idProduct=6048
[ 1472.758612] usb 3-2.2: Product: Dons Dongle
[ 1472.758617] usb 3-2.2: Manufacturer: RfCat
[ 1473.573402] usb 3-2.1: new high-speed USB device number 5 using xhci_hcd
[ 1635.127787] usb 3-2.1: New USB device found, idVendor=1004, idProduct=6245
[ 1635.127799] usb 3-2.1: Product: LGE Android Phone
[ 1635.127804] usb 3-2.1: Manufacturer: LG Electronics Inc.
```



https://github.com/kikithegecko/turnipschool-casing




The future needs fixing.
UK address: FormFormForm Ltd, Unit 2, 47-49 Tudor Road, London, E9 7SN, UK.
t: 020 7998 0022
USA address: sugru, inc.
HOVS, 38120 Amrhein, Livonia, MI 48150, USA
t: 877-990-9888
Not for individual resale.
buy online at sugru.com
use by date
67005 USE BY 01 NOV 2015
sugru
self-setting rubber

```
mossmann@falstaff ~/shmoo/2015 $ rfcat -r
'RfCat, the greatest thing since Frequency Hopping!'

Research Mode: enjoy the raw power of rflib

currently your environment has an object called "d" for dongle.  this is how
you interact with the rfcat dongle:
    >>> d.ping()
    >>> d.setFreq(433000000)
    >>> d.setMdmModulation(MOD_ASK_OOK)
    >>> d.makePktFLEN(250)
    >>> d.RFxmit("HALLO")
    >>> d.RFrecv()
    >>> print d.reprRadioConfig()


In [1]: d.ping()
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.004013 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.003001 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.003221 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.002548 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.002948 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.002693 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.003444 seconds)
PING: 26 bytes transmitted, received: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' (0.004563 seconds)
```

```
Bus 003 Device 003: ID 610b:4653
Device Descriptor:
  bLength                18
  bDescriptorType         1
  bcdUSB               1.10
  bDeviceClass            0 (Defined at Interface level)
  bDeviceSubClass         0
  bDeviceProtocol         0
  bMaxPacketSize0        32
  idVendor           0x610b
  idProduct          0x4653
  bcdDevice            0.10
  iManufacturer           1 Great Scott Gadgets
  iProduct                2 TURNIPSCHOOL
  iSerial                 3 0000
  bNumConfigurations      1
  Configuration Descriptor:
    bLength                 9
    bDescriptorType         2
    wTotalLength           34
    bNumInterfaces          1
    bConfigurationValue     1
    iConfiguration          0
    bmAttributes         0xc0
      Self Powered
    MaxPower              100mA
    Interface Descriptor:
      bLength                 9
      bDescriptorType         4
      bInterfaceNumber        0
      bAlternateSetting       0
      bNumEndpoints           1
      bInterfaceClass         3 Human Interface Device
      bInterfaceSubClass      0 No Subclass
      bInterfaceProtocol      1 Keyboard
      iInterface              0
```

Build Your Own TURNIPSCHOOL

PCB: $1.50 each

Solder paste stencil: $15

Components: $20

Sugru: $10

3D printed mold: $40

Solder paste, tweezers, hot plate, soldering iron

Open Source Hardware!

Thank You

DARPA
BIT Systems
Marshall Hecht
Karoline “kikithegecko” Busse
Dean Pierce
Alexander Holler
Travis Goodspeed & Sergey Bratus

Questions?

http://www.nsaplayset.org/

http://greatscottgadgets.com/