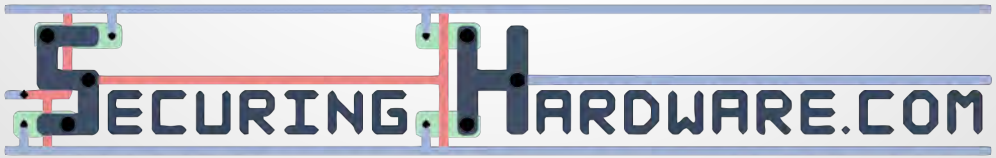
# Stupid PCIe Tricks

**featuring**

# NSA Playset: PCIe

DEFCON 22
Joe FitzPatrick
Miles Crabill



**This document is a preliminary revision. For the latest version, as well as information about tools released, visit http://securinghardware.com/nsa-playset**

# whoami

- Electrical Engineering education with focus on CS and Infosec
- 8 years doing security research, speed debug, and tool development for CPUs
- Hardware Pen Testing of CPUs
- Security training for functional validators worldwide

Joe FitzPatrick
@securelyfitz
joefitz@securinghardware.com

SECURING HARDWARE.COM

# whoami

- Computer Science student at Lewis & Clark College
- Almost 3 years of experience in security research
- Little to no prior hardware hacking experience

Miles Crabill
@milescrabill
miles@milescrabill.com

# What is PCIe?

# PCIe is PCI!

```
user@ubuntu:~$
user@ubuntu:~$ lspci -bnn
00:00.0 Host bridge [0600]: Intel Corporation 82P965/G965 Memory Controller Hub [8086:29a0] (rev 02)
00:01.0 PCI bridge [0604]: Intel Corporation 82G35 Express PCI Express Root Port [8086:2981] (rev 02)
00:03.0 Unassigned class [ff00]: Device [1ab8:4000]
00:05.0 Ethernet controller [0200]: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) [8086:100f]
00:0a.0 PCI bridge [0604]: Digital Equipment Corporation DECchip 21150 [1011:0022]
00:0e.0 RAM memory [0500]: Red Hat, Inc Virtio memory balloon [1af4:1002]
00:1d.0 USB controller [0c03]: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family) USB UHCI #1 [8086:2658] (rev 02)
00:1d.6 USB controller [0c03]: NEC Corporation uPD720200 USB 3.0 Host Controller [1033:0194] (rev 03)
00:1d.7 USB controller [0c03]: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family) USB2 EHCI Controller [8086:265c] (rev 02)
00:1e.0 PCI bridge [0604]: Intel Corporation 82801 PCI Bridge [8086:244e] (rev f2)
00:1f.0 ISA bridge [0601]: Intel Corporation 82801HB/HR (ICH8/R) LPC Interface Controller [8086:2810] (rev 02)
00:1f.1 IDE interface [0101]: Intel Corporation 82801BA IDE U100 Controller [8086:244b] (rev 05)
00:1f.2 SATA controller [0106]: Intel Corporation 82801HR/HO/HH (ICH8R/DO/DH) 6 port SATA Controller [AHCI mode] [8086:2821] (rev 02)
00:1f.4 Multimedia audio controller [0401]: Intel Corporation 82801BA/BAM AC'97 Audio Controller [8086:2445] (rev 02)
01:00.0 VGA compatible controller [0300]: Device [1ab8:4005]
user@ubuntu:~$
```

# PCIe is NOT PCI!

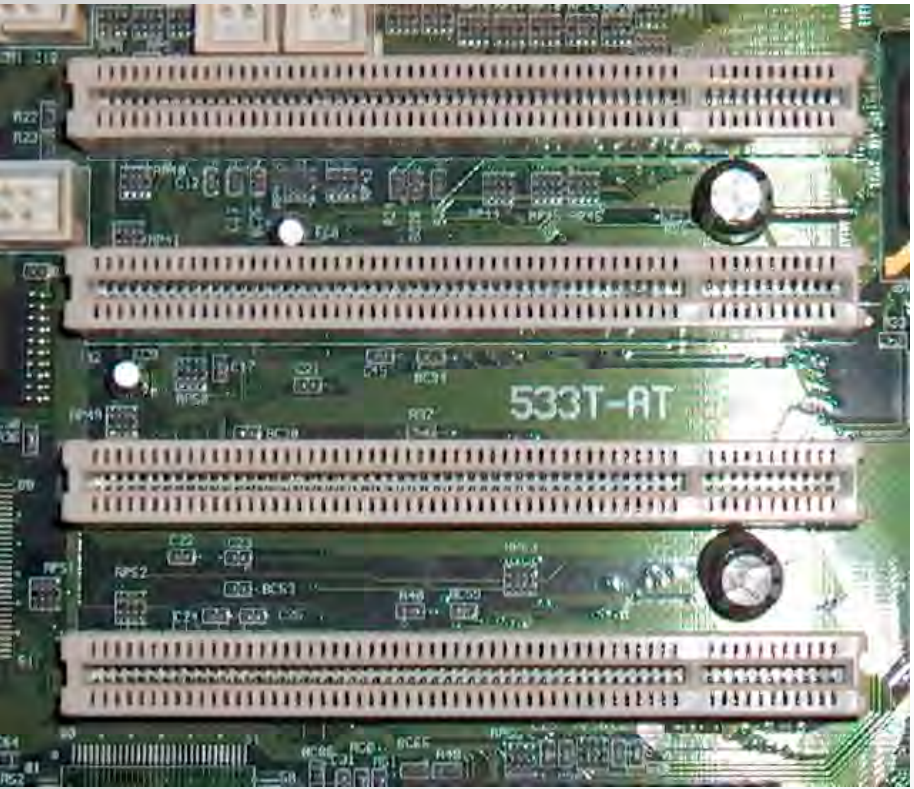



Foto tomada por Jorge González http://es.wikipedia.org

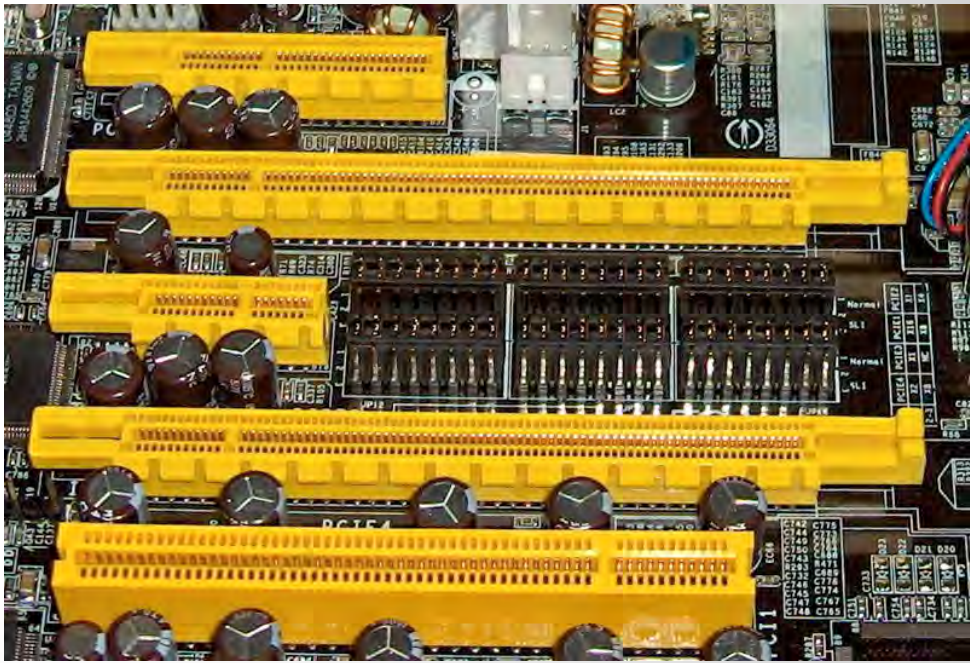


Photo by snikerdo http://en.wikipedia.org

# Links and Lanes

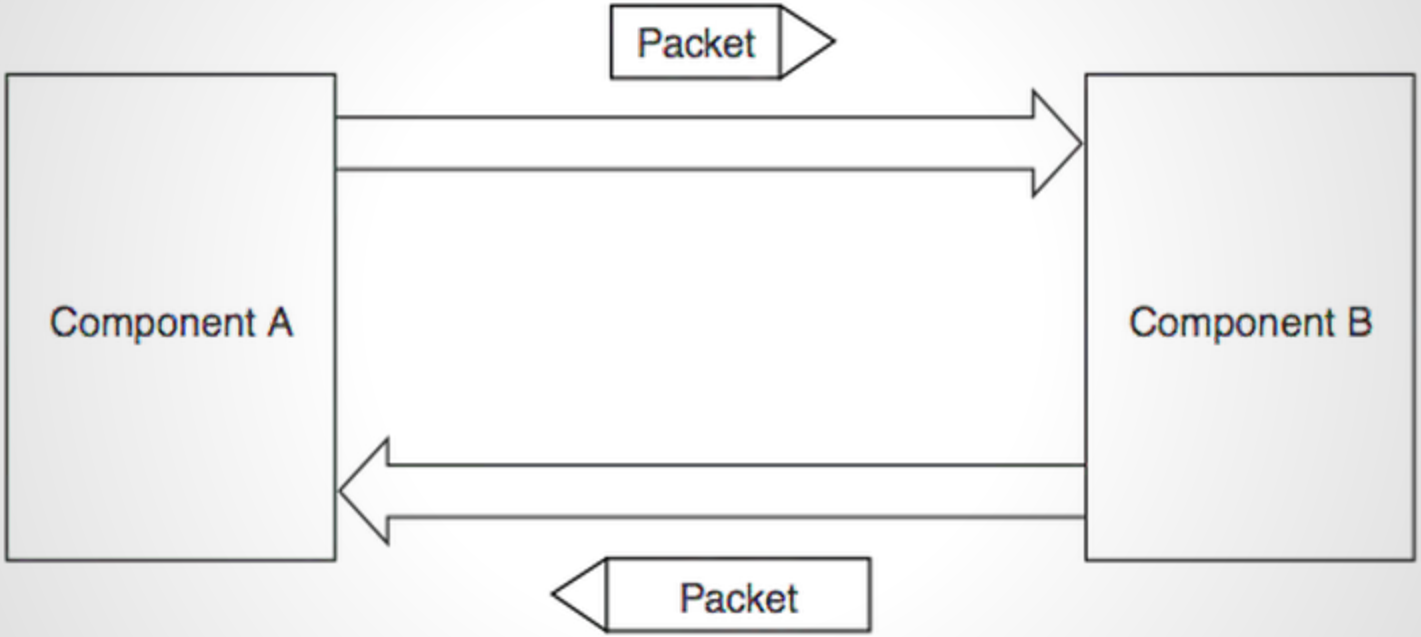



Diagram: PCIe 2.1 specification

# Hierarchy

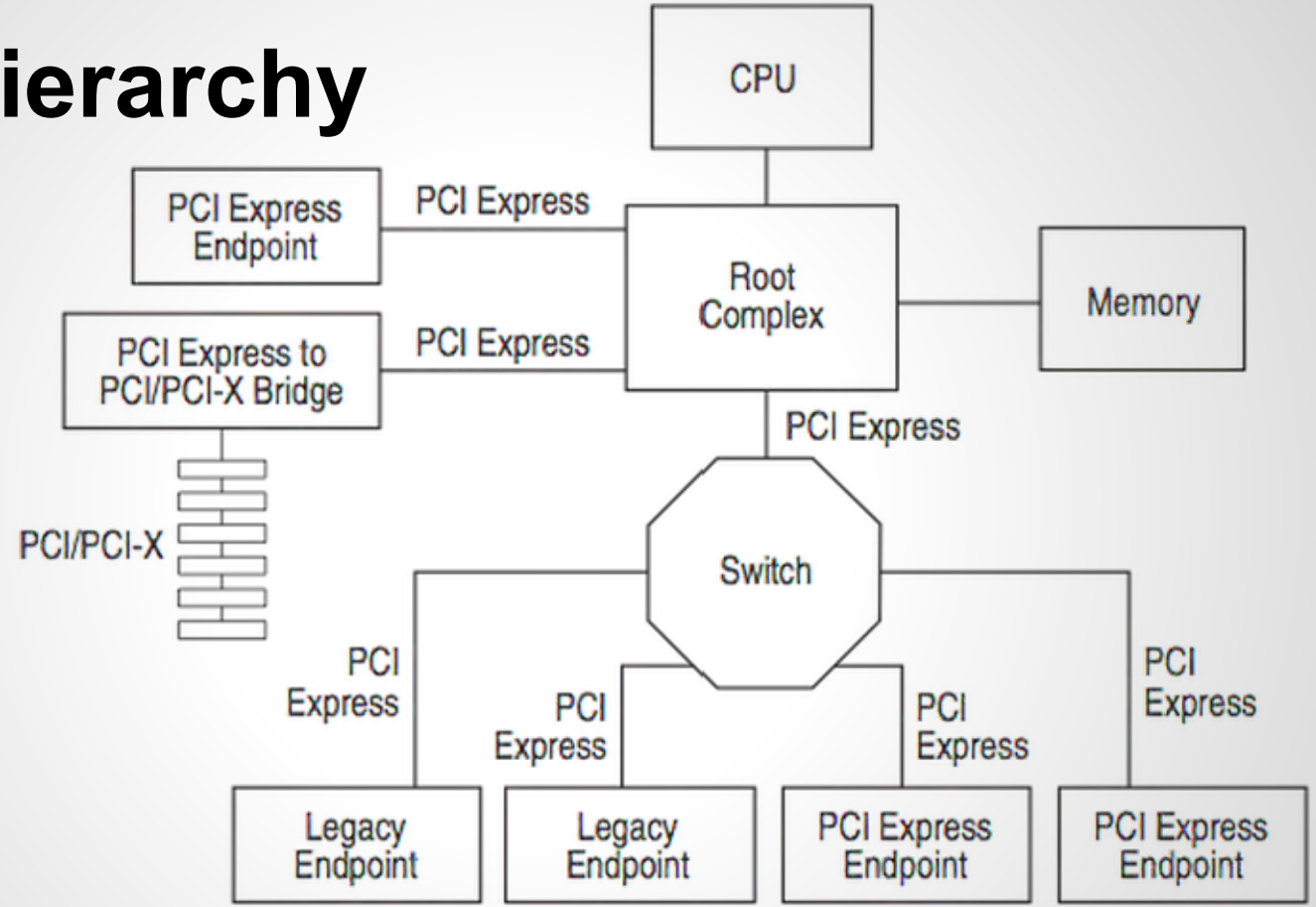



Diagram: PCIe 2.1 specification

# Switching and Routing

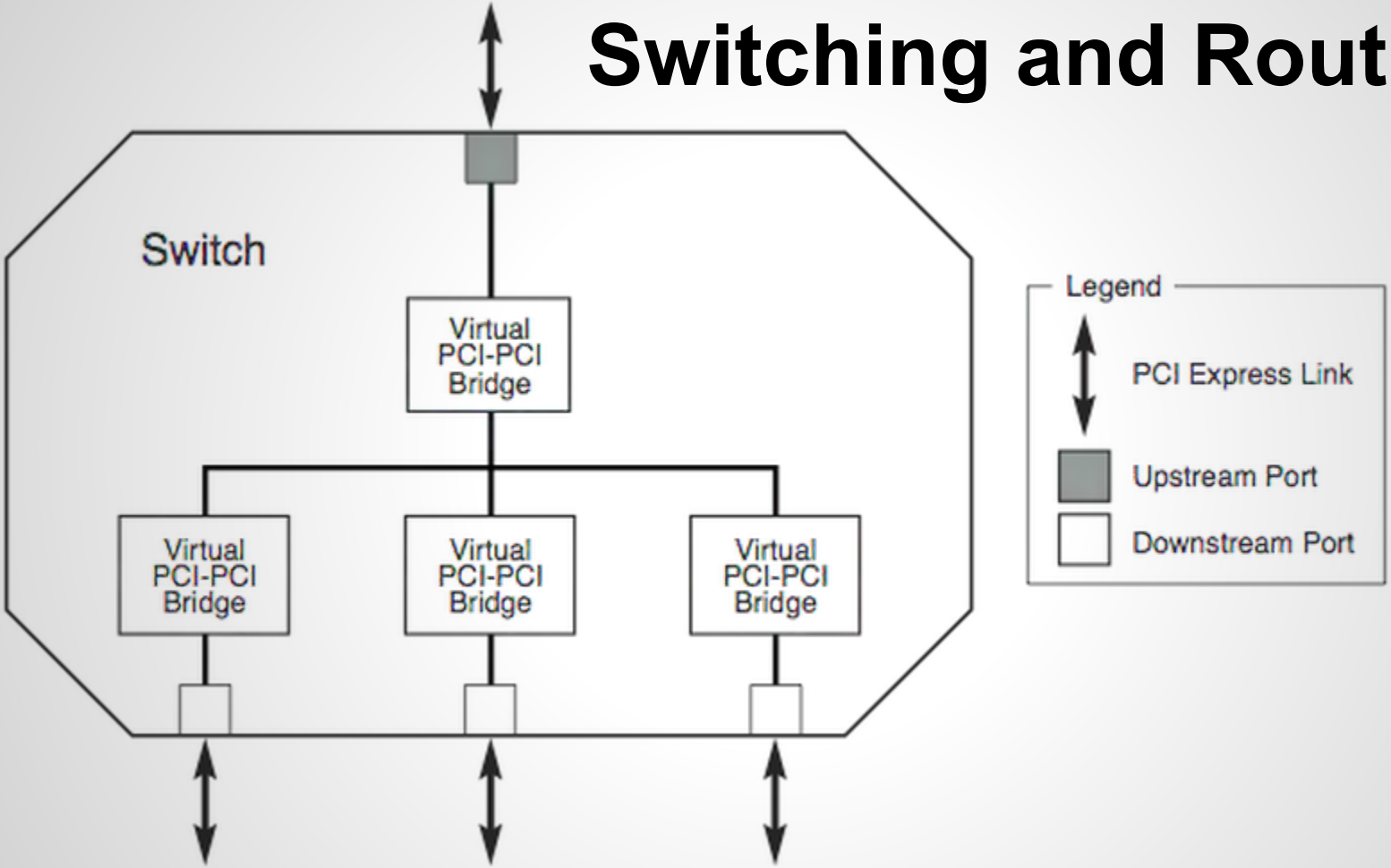



Diagram: PCIe 2.1 specification

# Layers

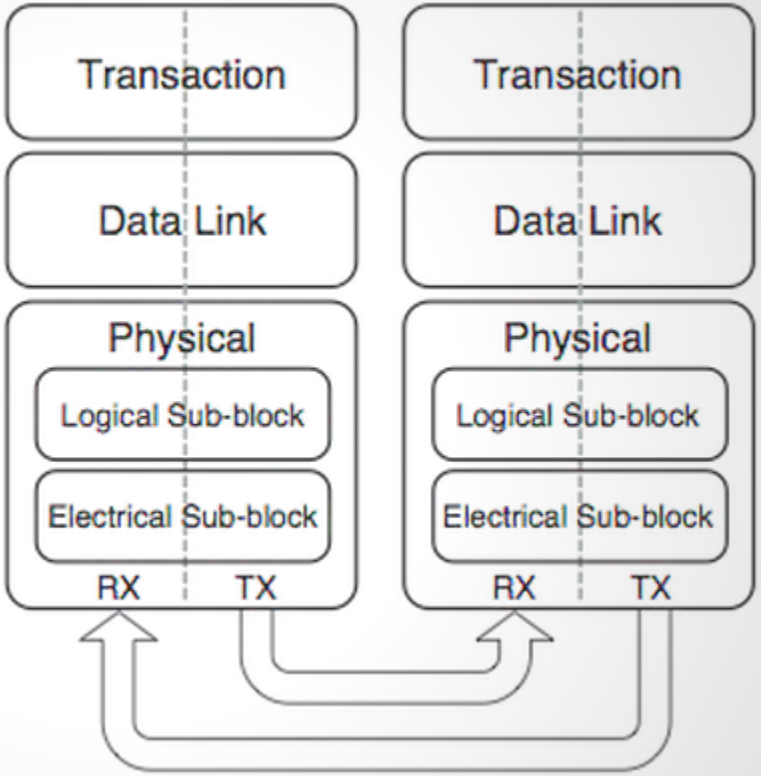



Diagram: PCIe 2.1 specification

# Accessing PCIe Space

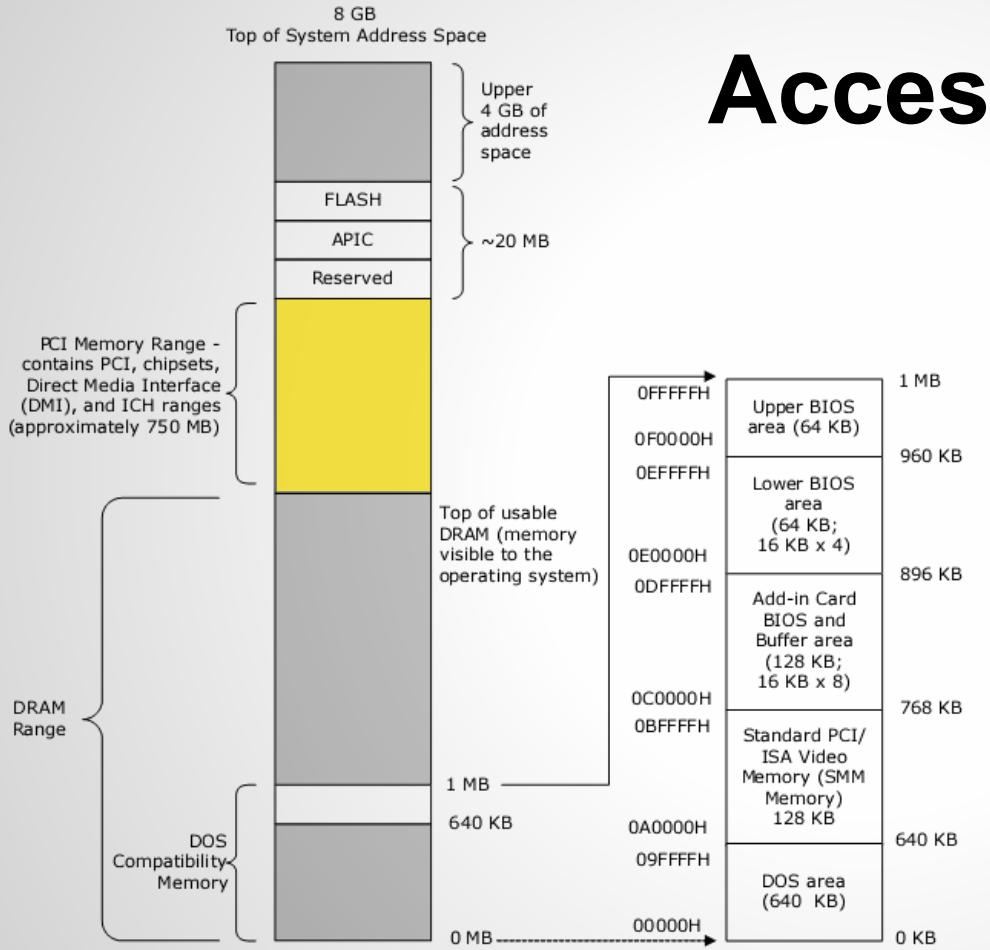
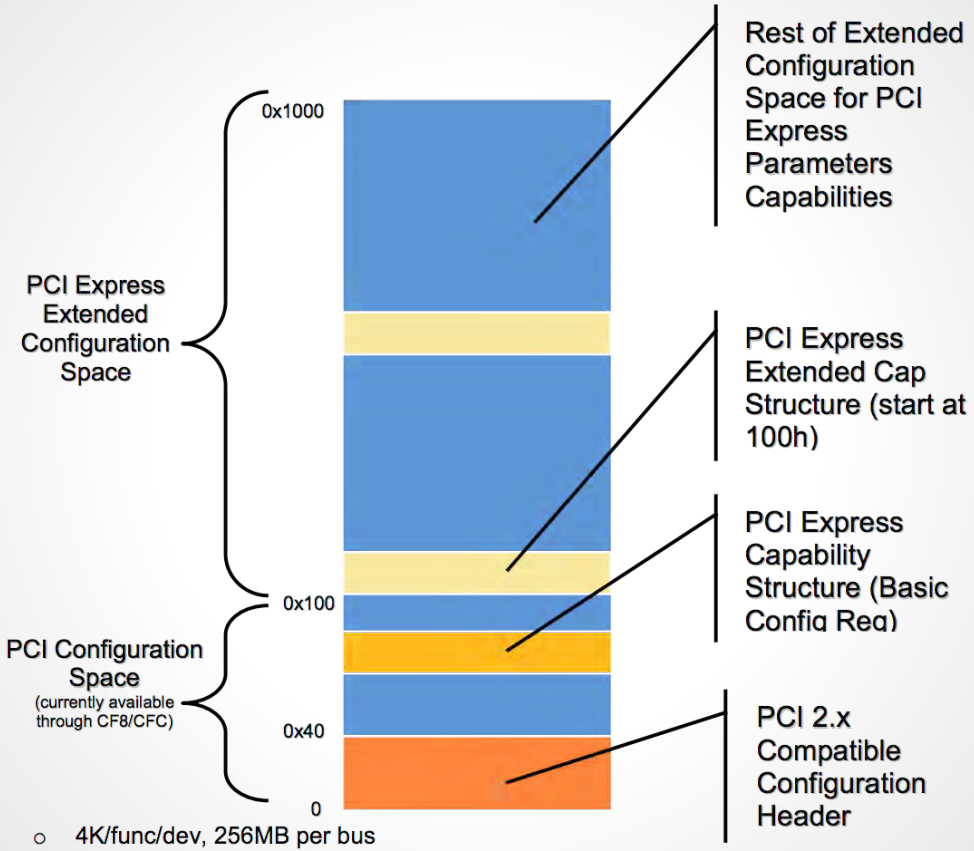



Diagram: http://blog.codinghorror.com/dude-wheres-my-4-gigabytes-of-ram/

## 1.1 PCI/PCI Express Configuration Space Memory Map




- 4K/func/dev, 256MB per bus
- Flat memory mapped access
- Firmware indicates memory base
- First 256 bytes PCI compatible
- Do not assume CF8/CFC available for extended space access

Diagram: PCI/PCI Express Configuration Space Access, Advanced Micro Devices, Inc. May 2008

# Configuration Space

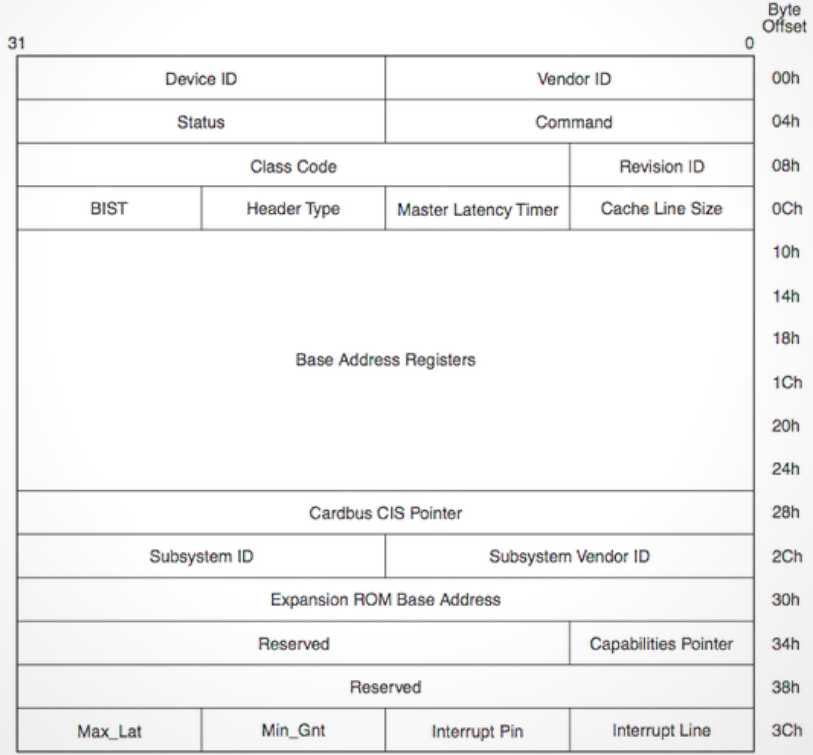



Diagram: PCIe 2.1 specification

# Configuration Space


```
user@ubuntu:~$ lspci -d 8086:244e -xnn
00:1e.0 PCI bridge [0604]: Intel Corporation 82801 PCI Bridge [8086:244e] (rev f2)
00: 86 80 4e 24 07 01 10 00 f2 00 04 06 00 00 01 00
10: 00 00 00 00 00 00 00 00 00 03 03 20 c0 d0 80 22
20: 20 ef 10 f0 01 e1 f1 e1 00 00 00 00 00 00 00 00
30: 00 00 00 00 50 00 00 00 00 00 00 00 00 00 03 00
```

Diagram: PCIe 2.1 specification

# Configuration Space


```
user@ubuntu:~$ lspci -d 8086:244e -xnn
00:1e.0 PCI bridge [0604]: Intel Corporation 82801 PCI Bridge [8086:244e] (rev f2)
00: 86 80 4e 24 07 01 10 00 f2 00 04 06 00 00 01 00
10: 00 00 00 00 00 00 00 00 00 03 03 20 c0 d0 80 22
20: 20 ef 10 f0 01 e1 f1 e1 00 00 00 00 00 00 00 00
30: 00 00 00 00 50 00 00 00 00 00 00 00 00 00 03 00
```

Diagram: PCIe 2.1 specification

# Configuration Space


```
user@ubuntu:~$ lspci -d 8086:244e -xnn
00:1e.0 PCI bridge [0604]: Intel Corporation 82801 PCI Bridge [8086:244e] (rev f2)
00: 86 80 4e 24 07 01 10 00 f2 00 04 06 00 00 01 00
10: 00 00 00 00 00 00 00 00 00 03 03 20 c0 d0 80 22
20: 20 ef 10 f0 01 e1 f1 e1 00 00 00 00 00 00 00 00
30: 00 00 00 00 50 00 00 00 00 00 00 00 00 00 03 00
```

Diagram: PCIe 2.1 specification

# Configuration Space


```
user@ubuntu:~$ lspci -d 8086:244e -xnn
00:1e.0 PCI bridge [0604]: Intel Corporation 82801 PCI Bridge [8086:244e] (rev f2)
00: 86 80 4e 24 07 01 10 00 f2 00 04 06 00 00 01 00
10: 00 00 00 00 00 00 00 00 00 03 03 20 c0 d0 80 22
20: 20 ef 10 f0 01 e1 f1 e1 00 00 00 00 00 00 00 00
30: 00 00 00 00 50 00 00 00 00 00 00 00 00 00 03 00
```

Diagram: PCIe 2.1 specification

# Enumeration

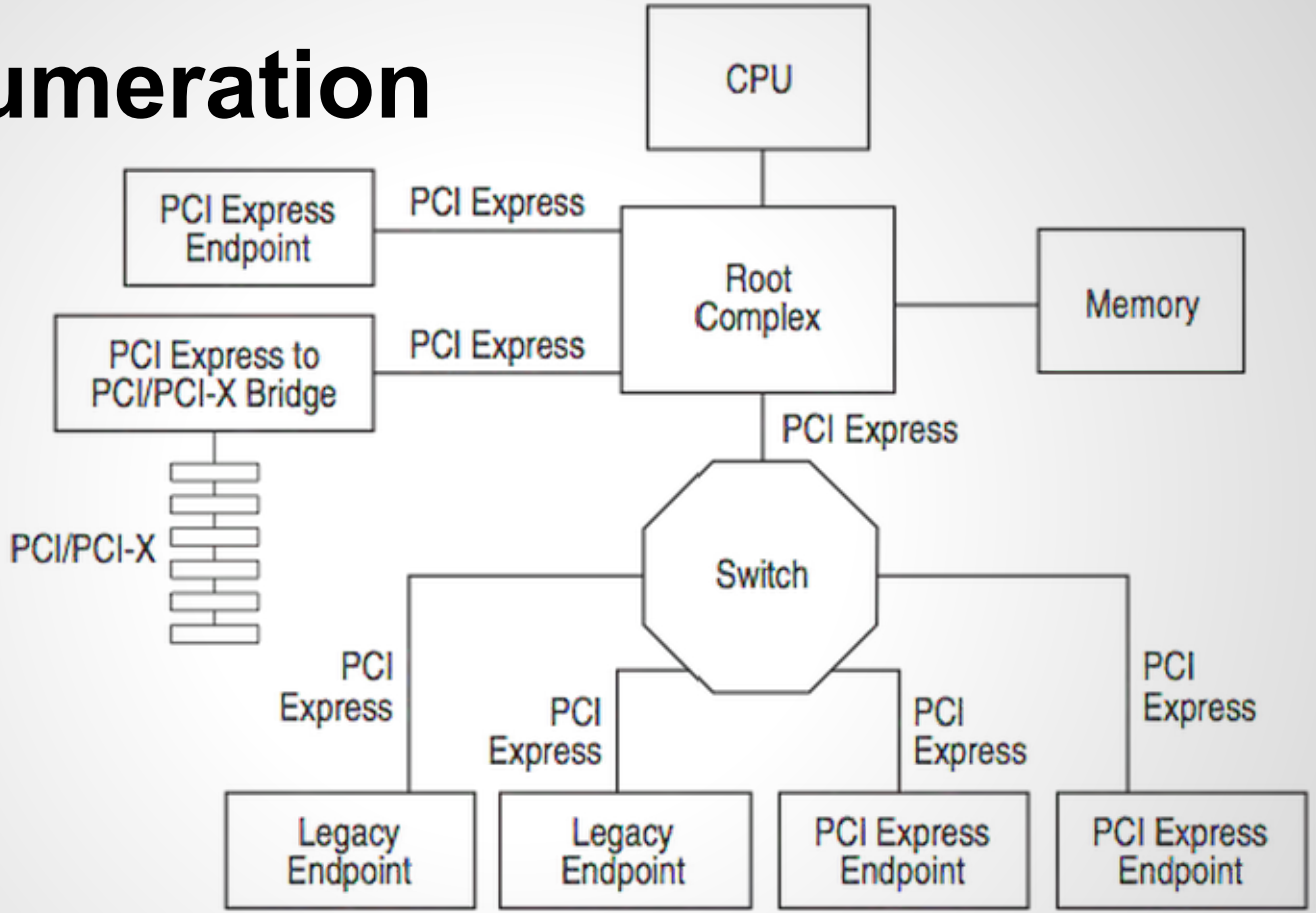



Diagram: PCIe 2.1 specification

# Routing PCIe

# The Step-By-Step, Complicated, Mandatory, Inflexible Rules of Routing PCIe:

# The Step-By-Step, Complicated, Mandatory, Inflexible Rules of Routing PCIe:

1. route pairs adjacent and equal length

# The Step-By-Step, Complicated, Mandatory, Inflexible Rules of Routing PCIe:

1. route pairs adjacent and equal length

… that’s mostly it

# Routing PCIe

| | |
|---|---|
| System Board Traces | 12 Inches |
| Add-in Card Traces | 3.5 inches |
| Chip-to-Chip Routes | 15 inches |

Follow these rules and your board might work.

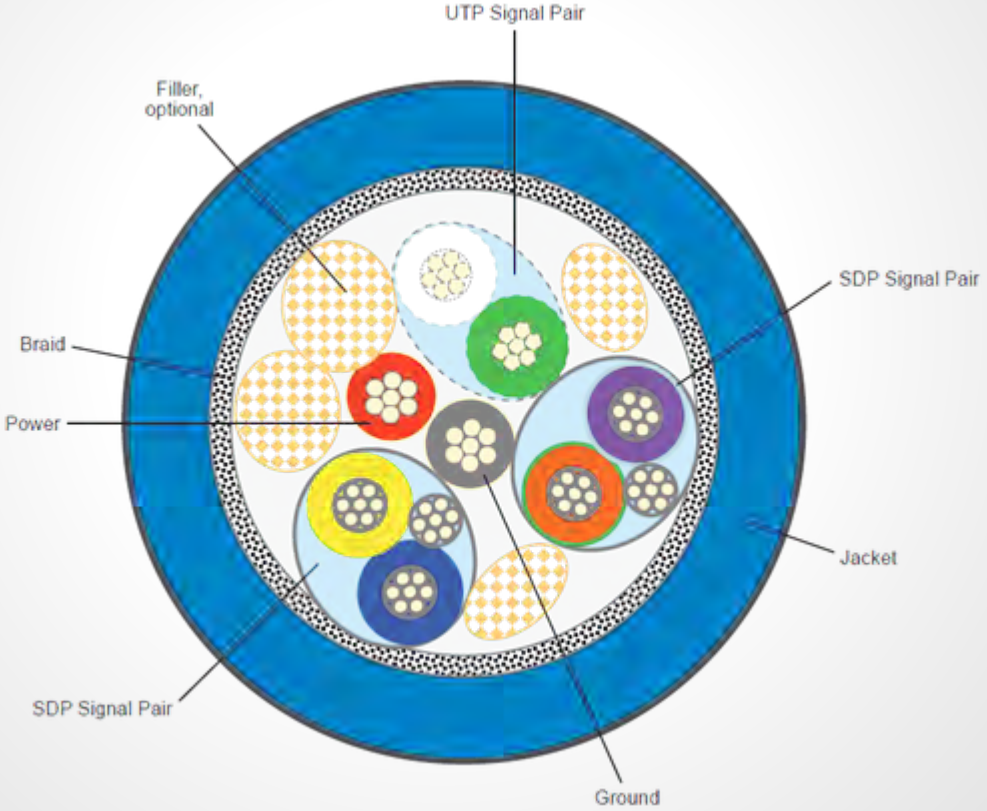
Break them and it might not.

# Routing PCIe

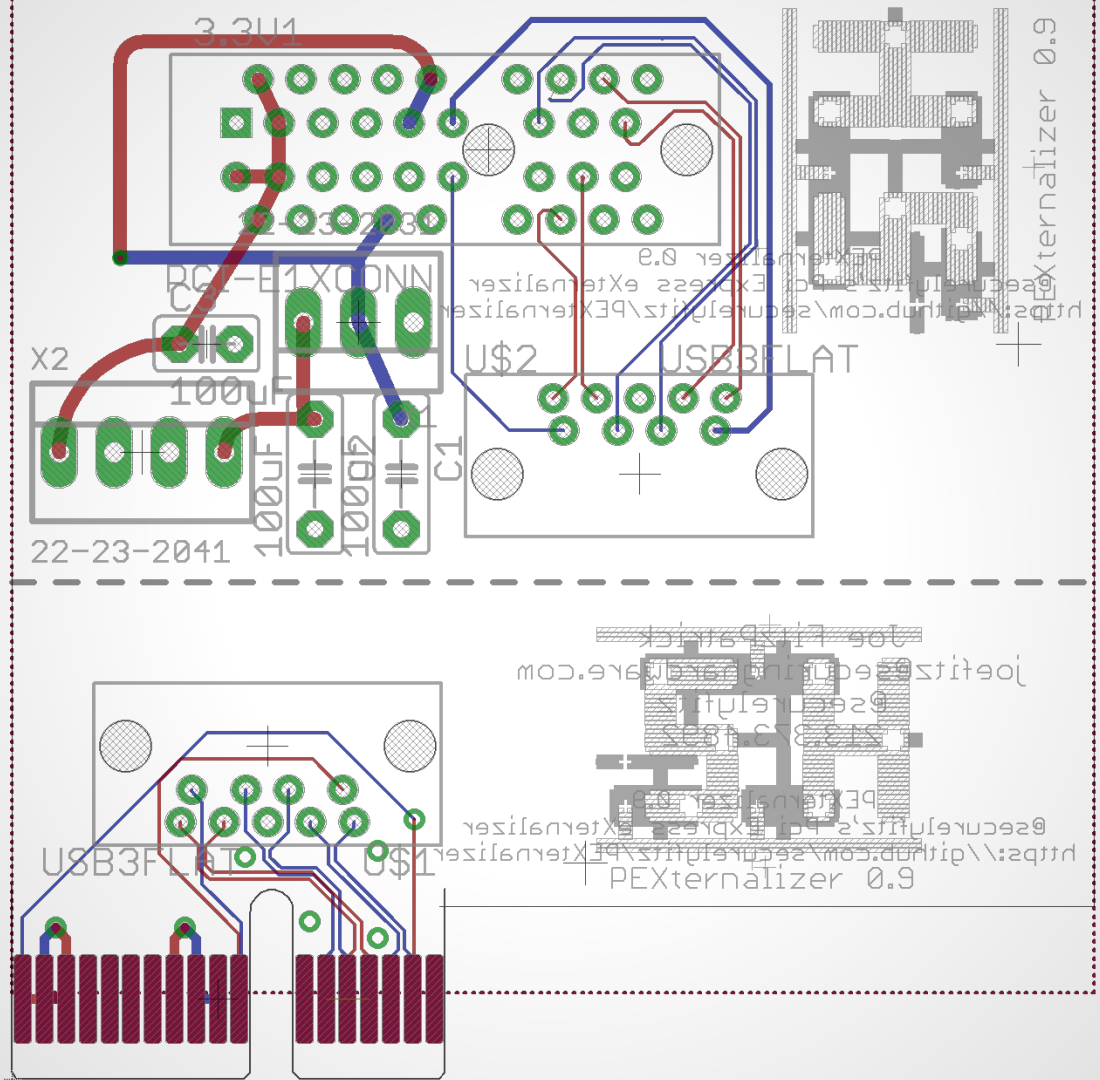
Minimum PCIe:

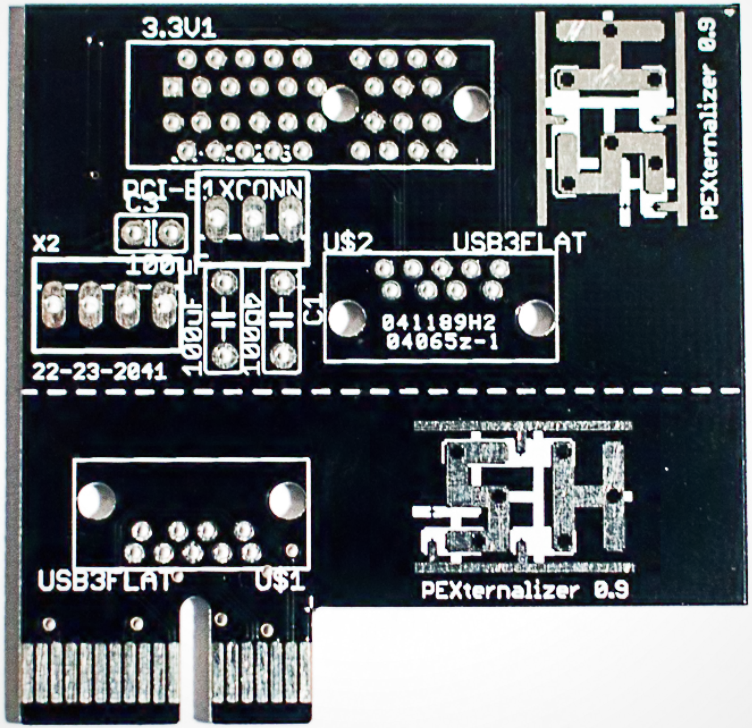
- 2.5GHz TX
- 2.5GHz RX
- 100MHz Clock (optional)

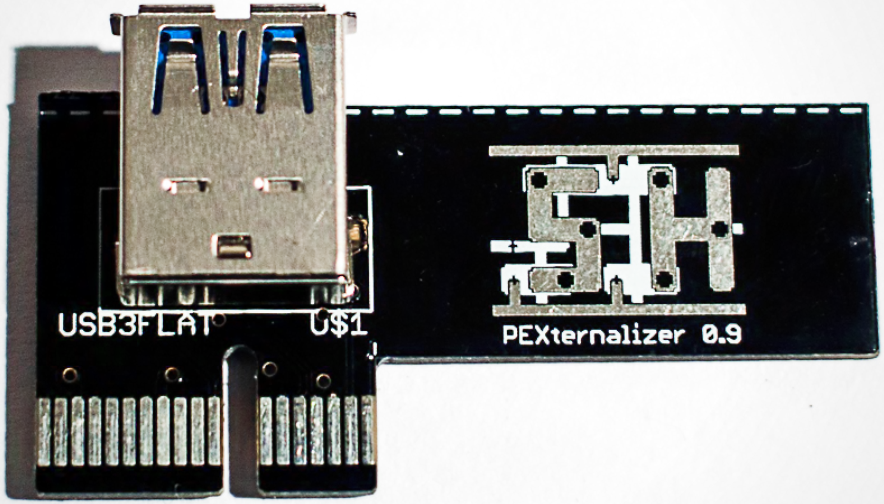
# Routing PCIe

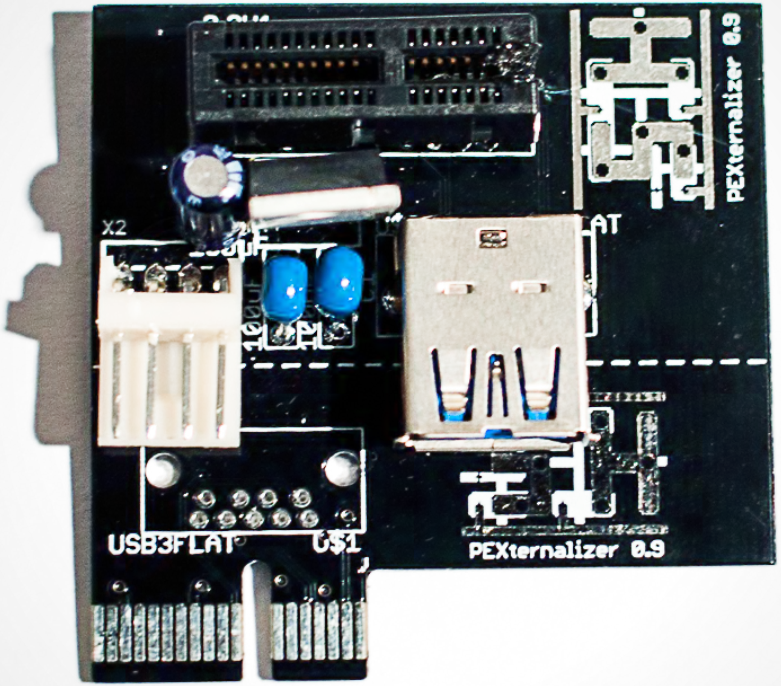



Cross-section of a USB 3.0 cable. Image courtesy of USB Implementers Forum


3.3V1
PCIE-E1XCONN
X2
100uF
100nF
100nF
C1
22-23-2041
U$2
USB3FLAT
PEXternalizer 0.9
USB3FLAT
U$1
PEXternalizer 0.9


3.3V1
PCI-E1XCONN
C3
100uF
X2
22-23-2041
100uF
100uF
C1
U$2
USB3FLAT
041189H2
04065z-1
PEXternalizer 0.9
USB3FLAT
U$1
PEXternalizer 0.9


USB3FLAT
U$1
PEXternalizer 0.9


X2
USB3FLAT
PEXternalizer 0.9
PEXternalizer 0.9


7:52
Wired Network
disconnected
Wireless Networks
OpenWrt
Disconnect
HOME1234
HOWARD
KYM-PC_Networkn
stevensen
Connect to Hidden Wireless Net
Create New Wireless Network...
VPN Connections
Enable Networking
Enable Wireless
Connection Information
Edit Connections...
RNX-N150PCe v2
150Mbps
2.4GHz Wireless N
PCI-E Adapter
2052500348
Rev:2.0

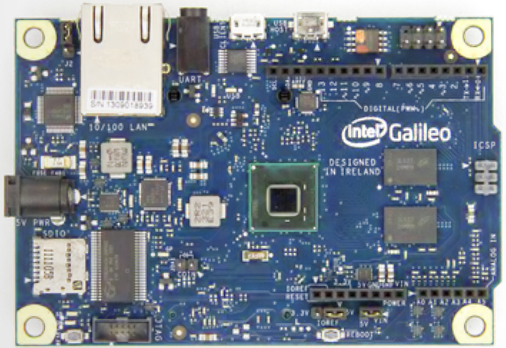
# Getting PCIe on Things Without It

ARDUINO

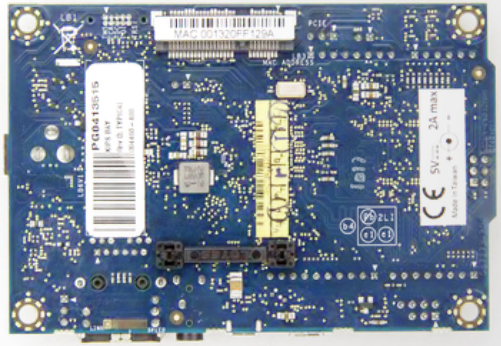
Search the Arduino Website

Home Buy Download Products Learning Reference Support Blog LOG IN SIGN UP

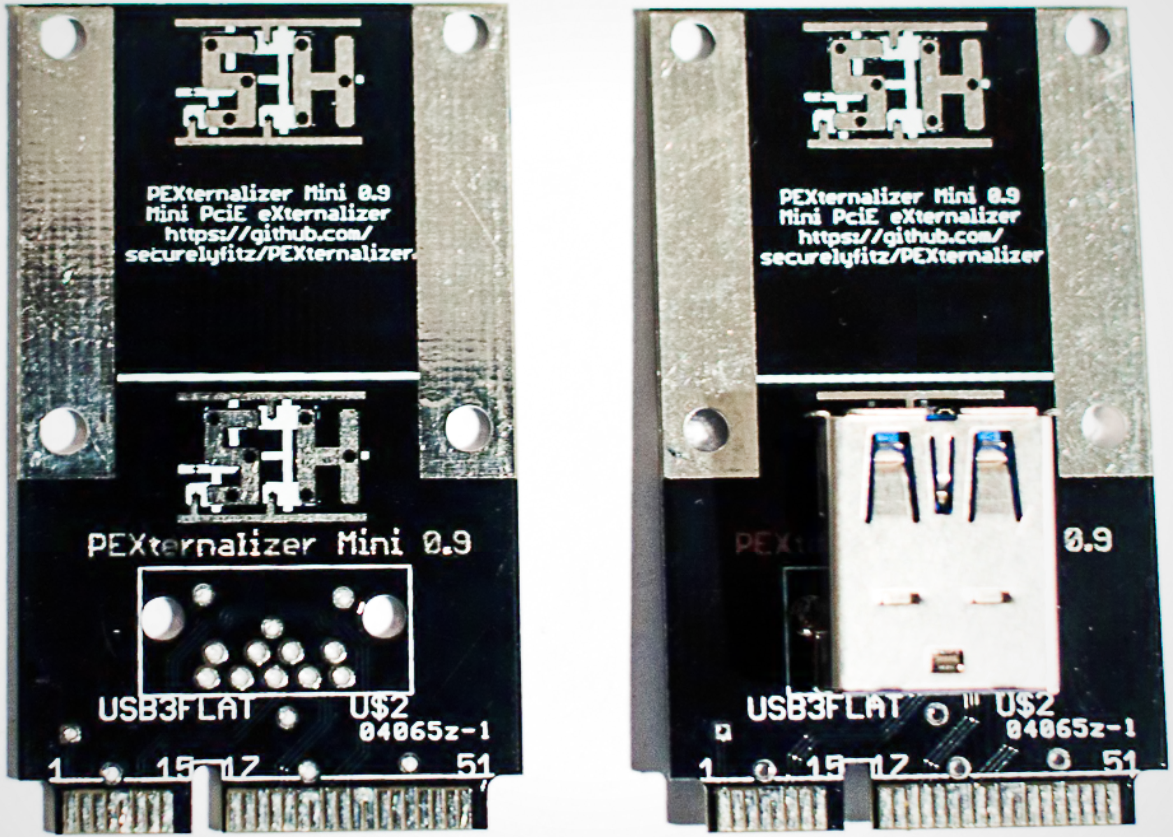
# Intel Galileo

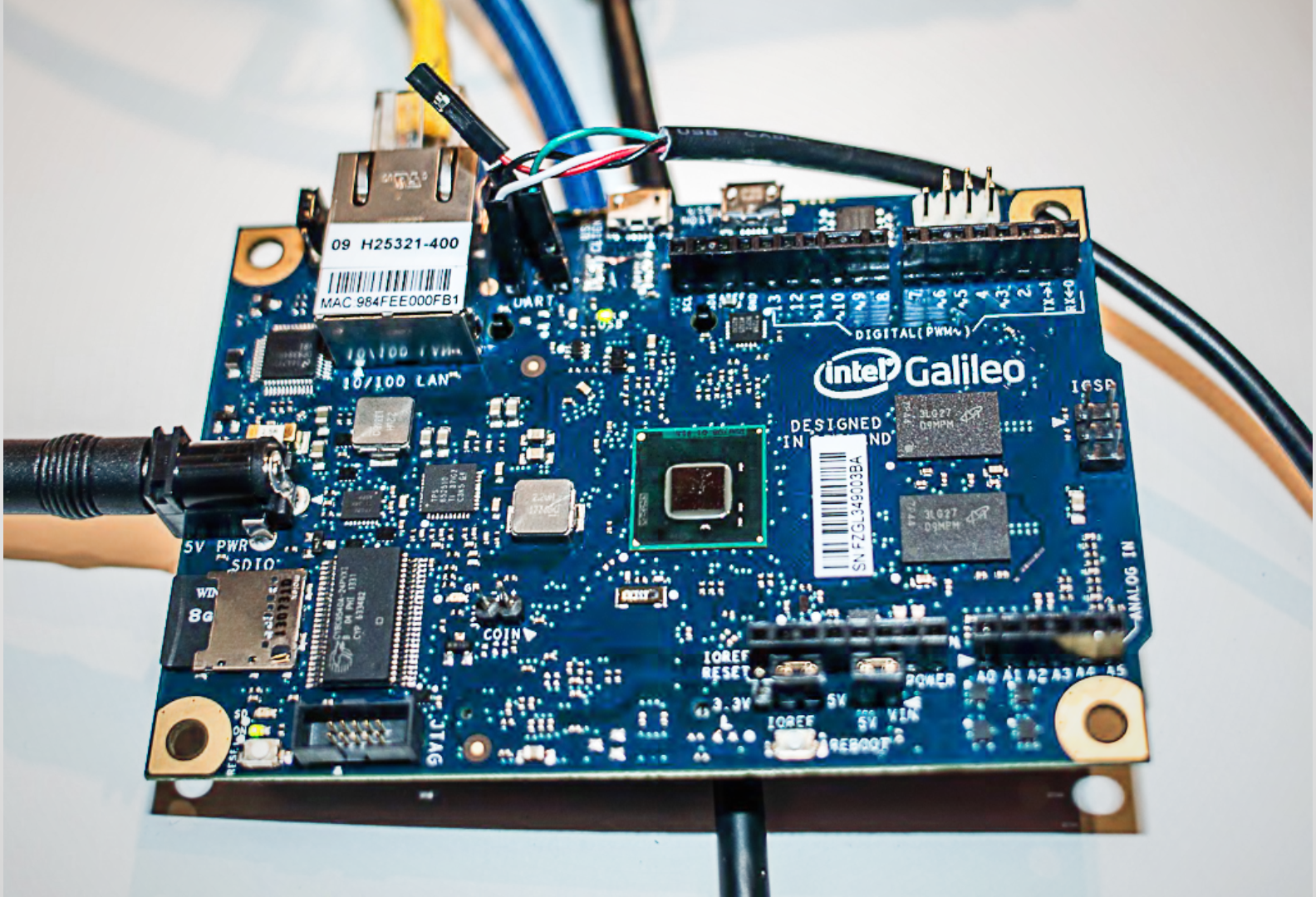


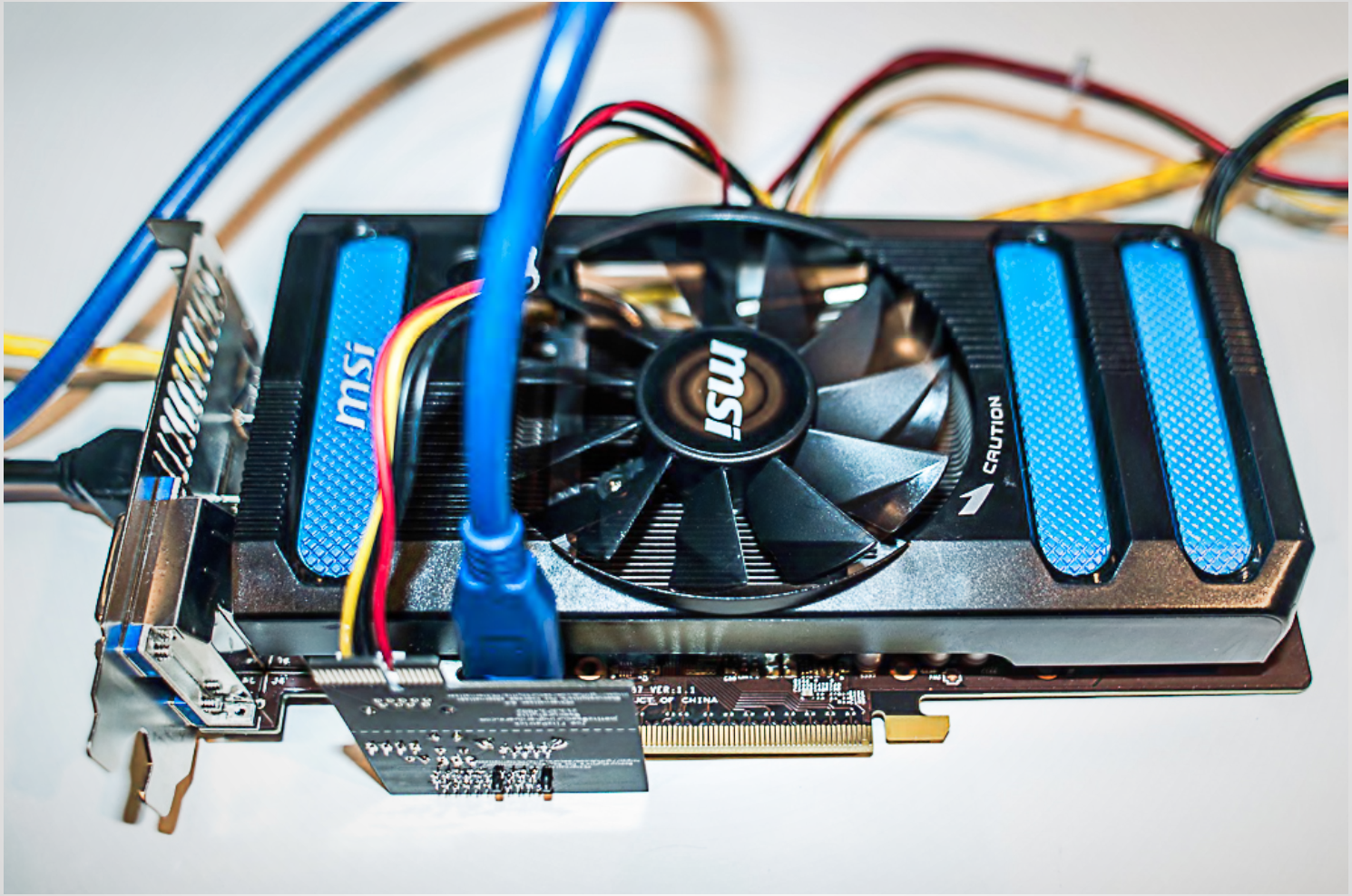

*Intel Galileo Front*

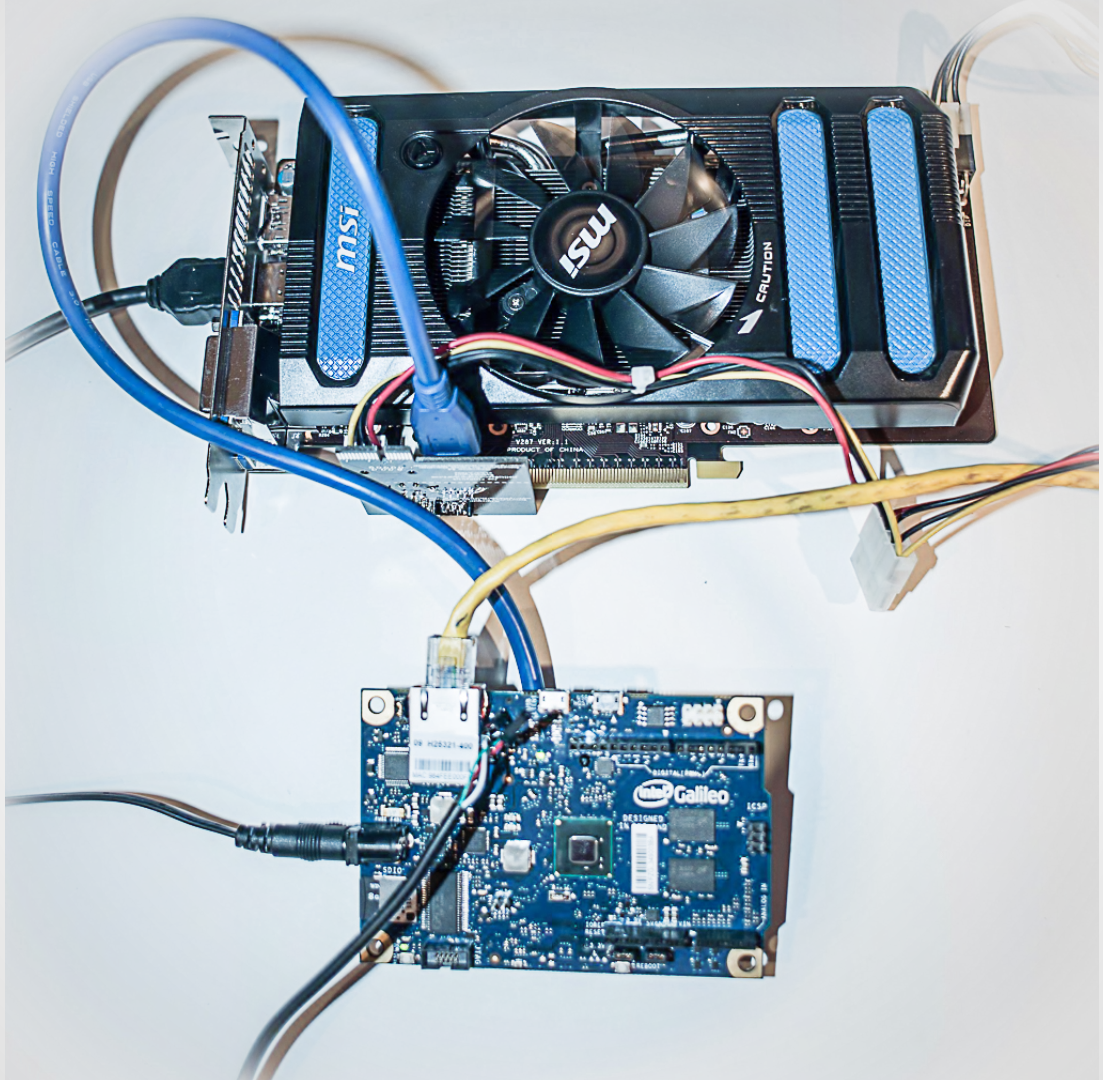


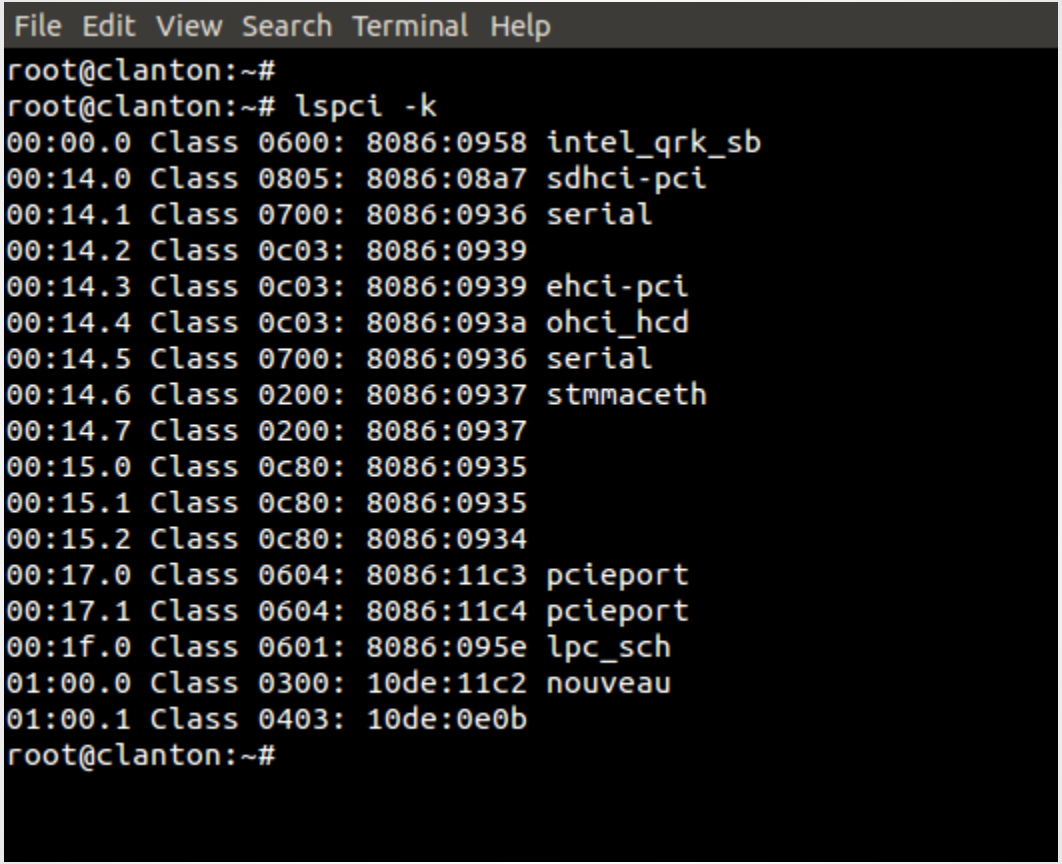
*Intel Galileo Back*

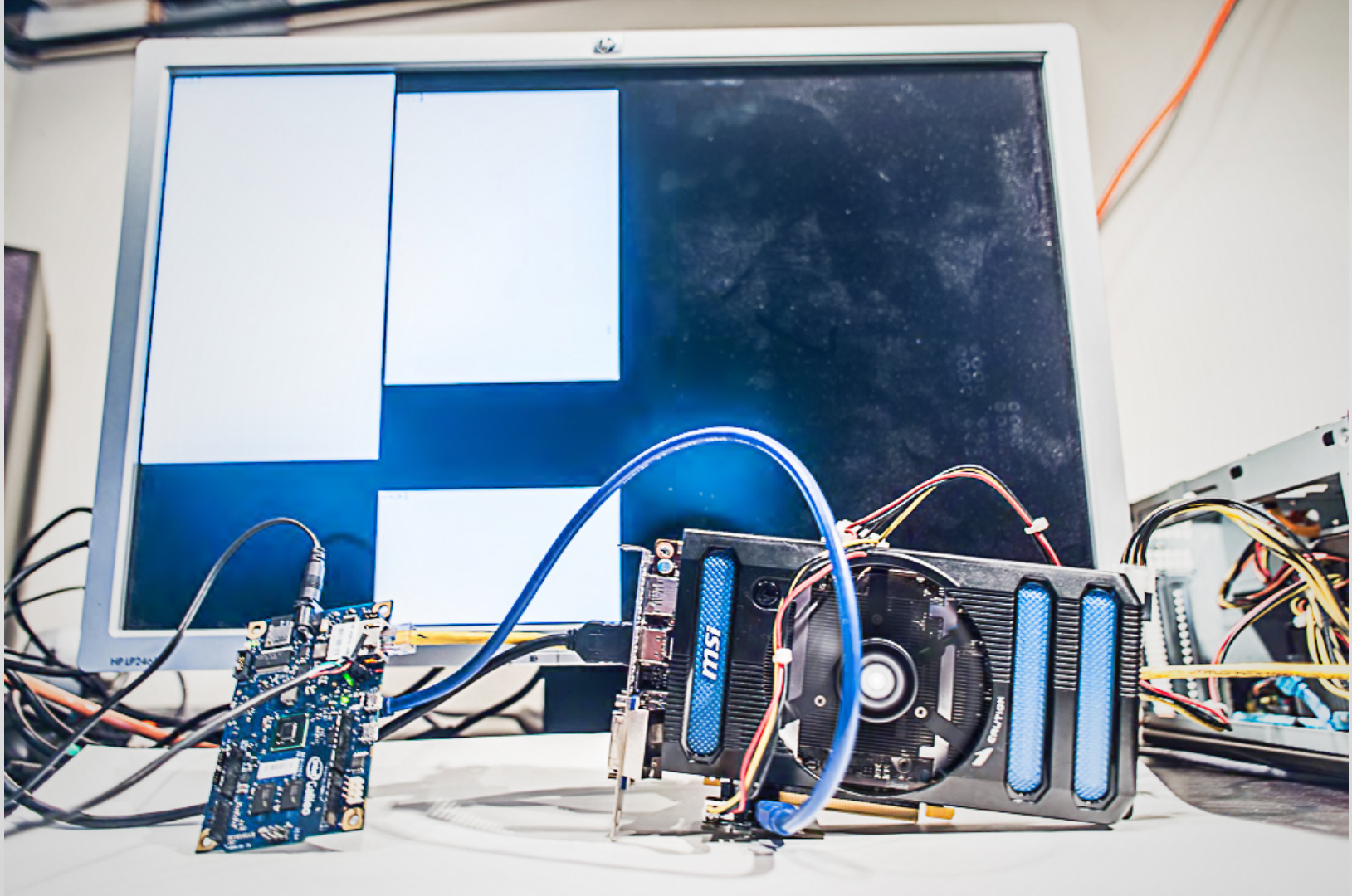

PEXternalizer Mini 0.9
Mini PciE eXternalizer
https://github.com/
securelyfitz/PEXternalizer
PEXternalizer Mini 0.9
USB3FLAT
U$2
04065z-1
1
15
17
51
PEXternalizer Mini 0.9
Mini PciE eXternalizer
https://github.com/
securelyfitz/PEXternalizer
0.9
USB3FLAT
U$2
04065z-1
1
15
17
51


09 H25321-400
MAC 984FEE000FB1
10/100 LAN
UART
DIGITAL(PWM~)
Intel Galileo
DESIGNED
ICSP
5V PWR
SDIO
COIN
IOREF
RESET
3.3V
5V
POWER
ANALOG IN
JTAG
REBOOT


msi
msi
CAUTION


msi
msi
CAUTION
Galileo
DESIGNED


File Edit View Search Terminal Help
root@clanton:~#
root@clanton:~# lspci -k
00:00.0 Class 0600: 8086:0958 intel_qrk_sb
00:14.0 Class 0805: 8086:08a7 sdhci-pci
00:14.1 Class 0700: 8086:0936 serial
00:14.2 Class 0c03: 8086:0939
00:14.3 Class 0c03: 8086:0939 ehci-pci
00:14.4 Class 0c03: 8086:093a ohci_hcd
00:14.5 Class 0700: 8086:0936 serial
00:14.6 Class 0200: 8086:0937 stmmaceth
00:14.7 Class 0200: 8086:0937
00:15.0 Class 0c80: 8086:0935
00:15.1 Class 0c80: 8086:0935
00:15.2 Class 0c80: 8086:0934
00:17.0 Class 0604: 8086:11c3 pcieport
00:17.1 Class 0604: 8086:11c4 pcieport
00:1f.0 Class 0601: 8086:095e lpc_sch
01:00.0 Class 0300: 10de:11c2 nouveau
01:00.1 Class 0403: 10de:0e0b
root@clanton:~#


msi

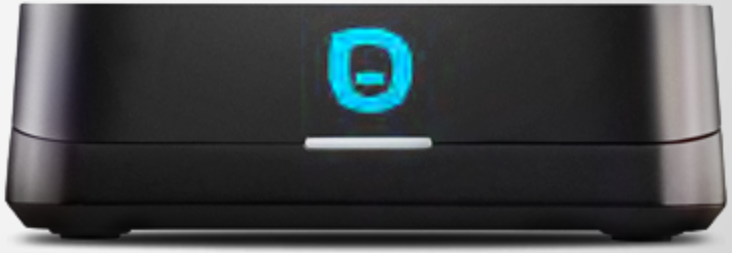
# Pogoplug

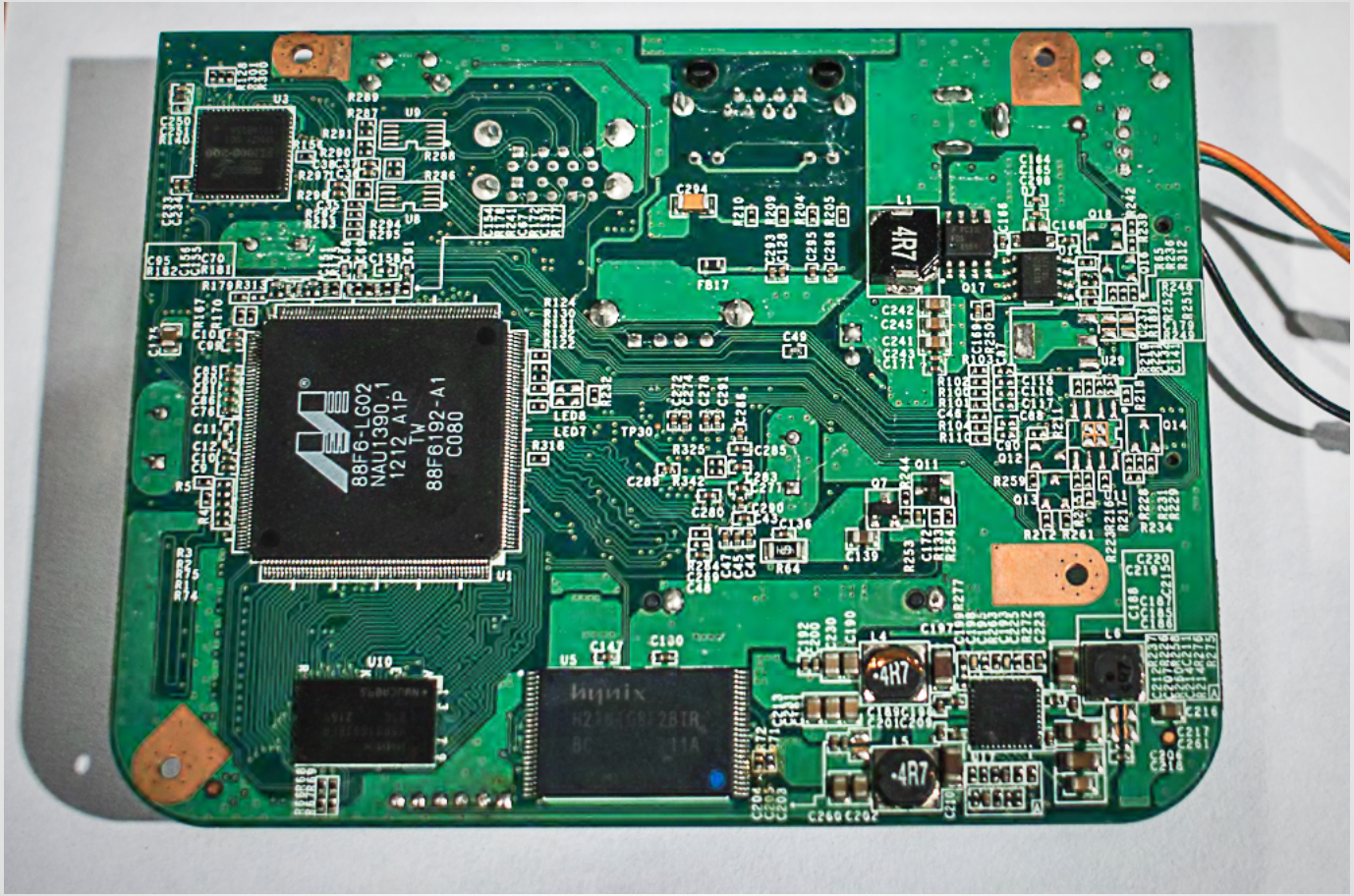
## Specifications:

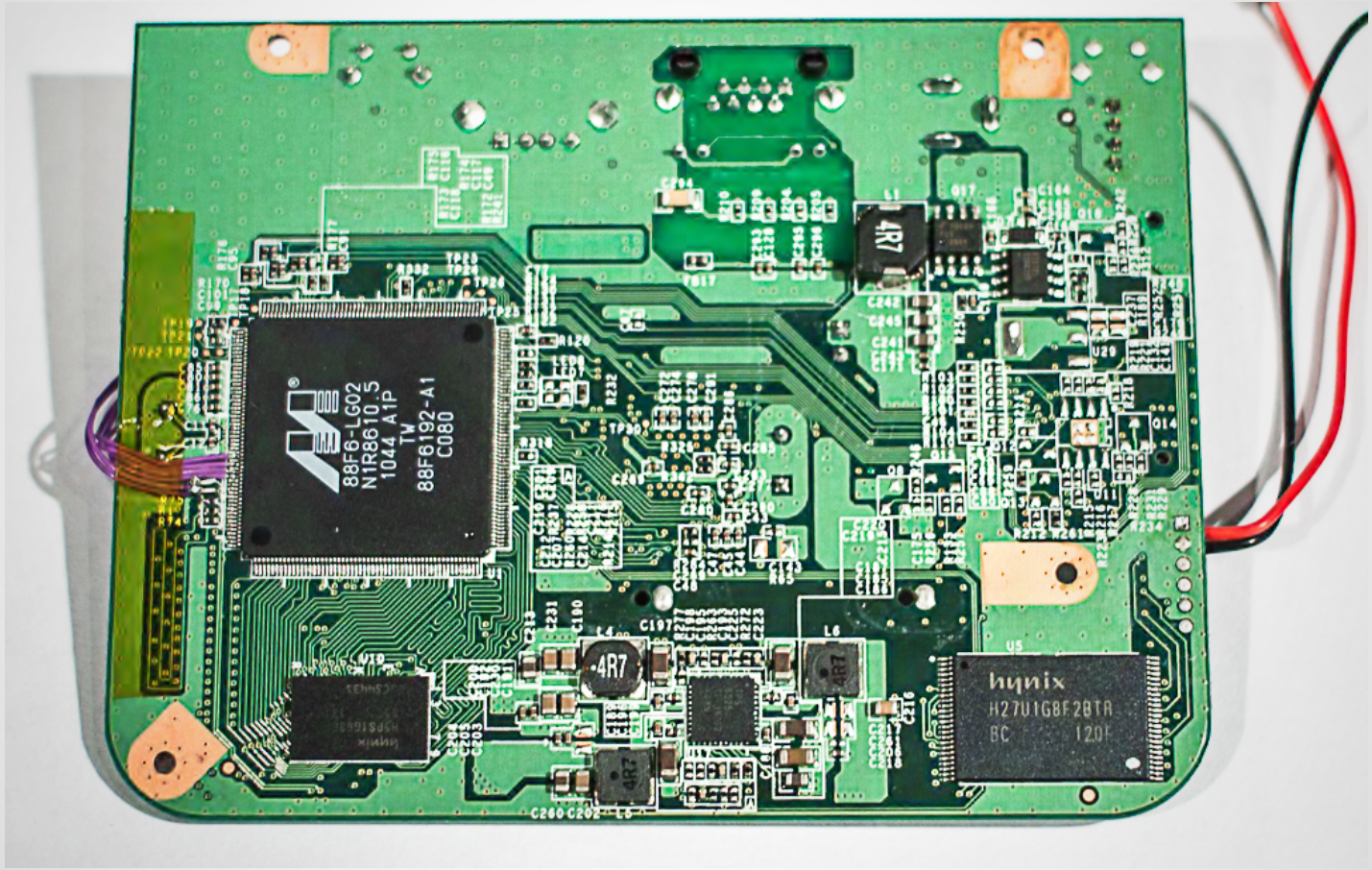
**Power Requirements:** 100-240V, 50/60Hz
**Drive Connections:** SD x1, USB 2.0 x1
**Network Connection:** Gigabit Ethernet
**Drive Formats:** NTFS, FAT, HFS+, EXT2, EXT3
**Web Browsers:** Microsoft® Internet Explorer, Mozilla® Firefox, Apple® Safari, Google Chrome™
**Operating Systems:** Microsoft® Windows XP/7/8, Apple® Mac OS X 10.6.8 & above
**Apps Available For:** iPhone®, iPad®, Android™

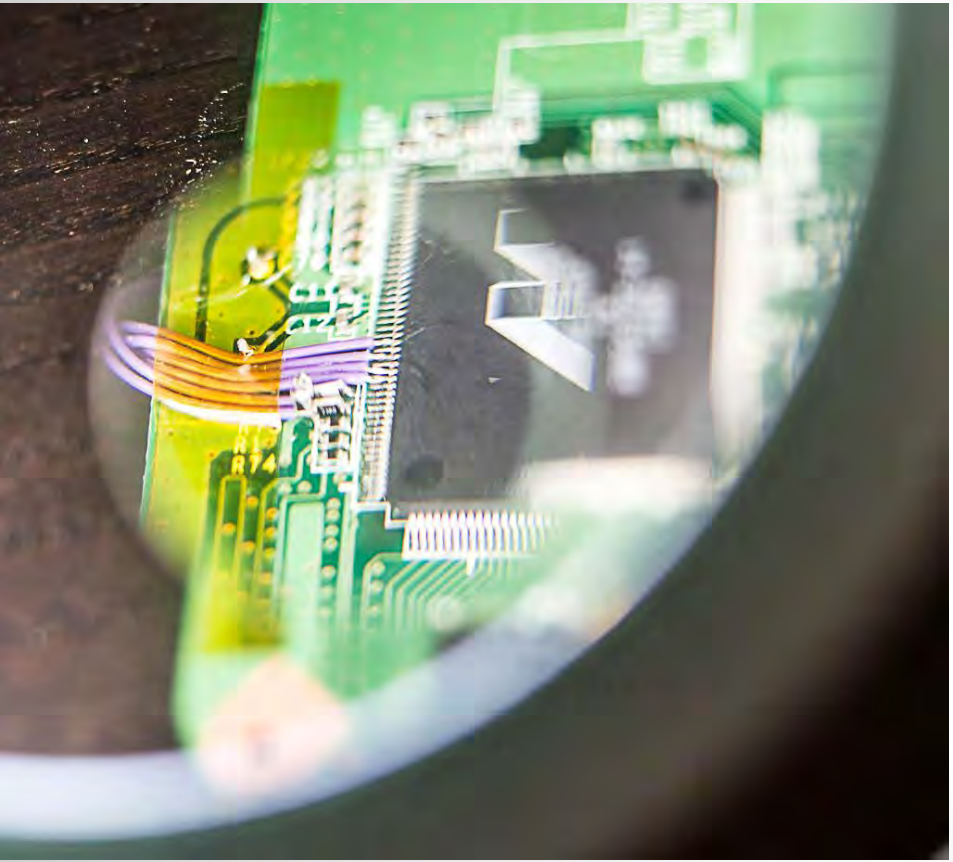
## What's Included:

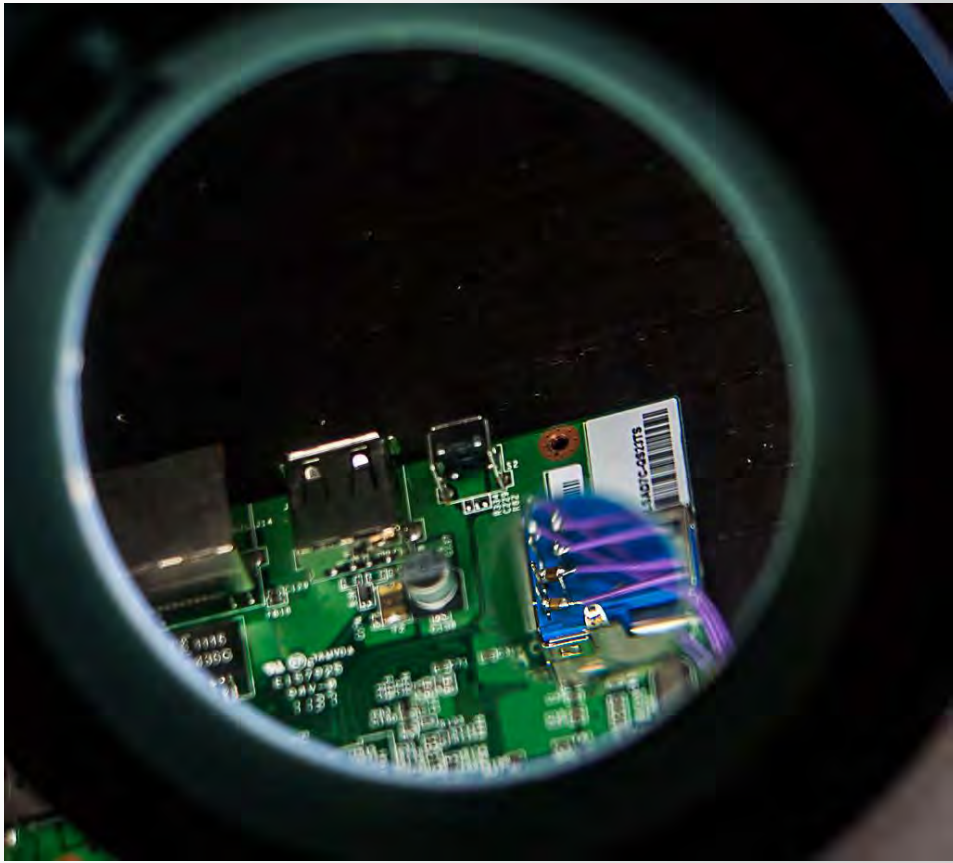
Pogoplug
Power cable
Ethernet cable
User manual




88F6-LG02
NAU1390.1
1212 A1P
TW
88F6192-A1
C080
4R7
4R7


88F6-LGO2
N1R8610.5
1044 A1P
TW
88F6192-A1
C080
4R7
4R7
4R7
hynix
H27U1G8F2BTR
BC
120





# Introducing SLOTSCREAMER

# Xilinx Kintex-7 FPGA KC705 Evaluation Kit

Overview | Hardware | Tools & IP | Docs & Designs

Click to Enlarge Image
View Partner Profile

**$1,695**

Buy from Xilinx

**Lead Time : 2 Weeks**

The Kintex®-7 FPGA KC705 Evaluation Kit includes all the basic co
designs including a targeted design
pre-verified reference designs and
daughter cards.

## What's Included

- KC705 Evaluation Board featuri
- Targeted Reference Design fea
  - Including evaluation version
- AMS 101 Evaluation Card
- Full seat of Vivado® Design Sui

# Spartan-6 FPGA SP605 Evaluation Kit

Click to Enlarge Image
View Partner Profile

**$495**

Buy from Xilinx

## Accelerate Your Designs – Right Out of the Bo

Product Information

The Spartan®-6 FPGA SP605 Evaluation Kit delivers all
hardware, design tools, IP, and reference designs enabl
box. This kit provides a flexible environment for system d
reference design and examples on how to leverage feat
transceivers, PCI Express®, DVI, and/or DDR3. This kit i
FMC (FPGA Mezzanine Card) connector for future scalin
applications and markets.

## What's Included

ALTERA

Larger Image

| | |
|---|---|
| **Mouser Part #:** | 989-DK-START-4CGX15 |
| **Manufacturer Part #:** | DK-START-4CGX15N |
| **Manufacturer:** | Altera Corporation |
| **Description:** | Programmable Logic IC Development Tools FPGA Starter Kit For EP4CGX15BF14 |
| **Lifecycle:** | New At Mouser |

Learn more about Altera Corporation DK-START-4CGX15N

Page 292, Mouser Online Catalog
Page 292, PDF Catalog Page
Data Sheet

**Enter Quantity:**

Buy

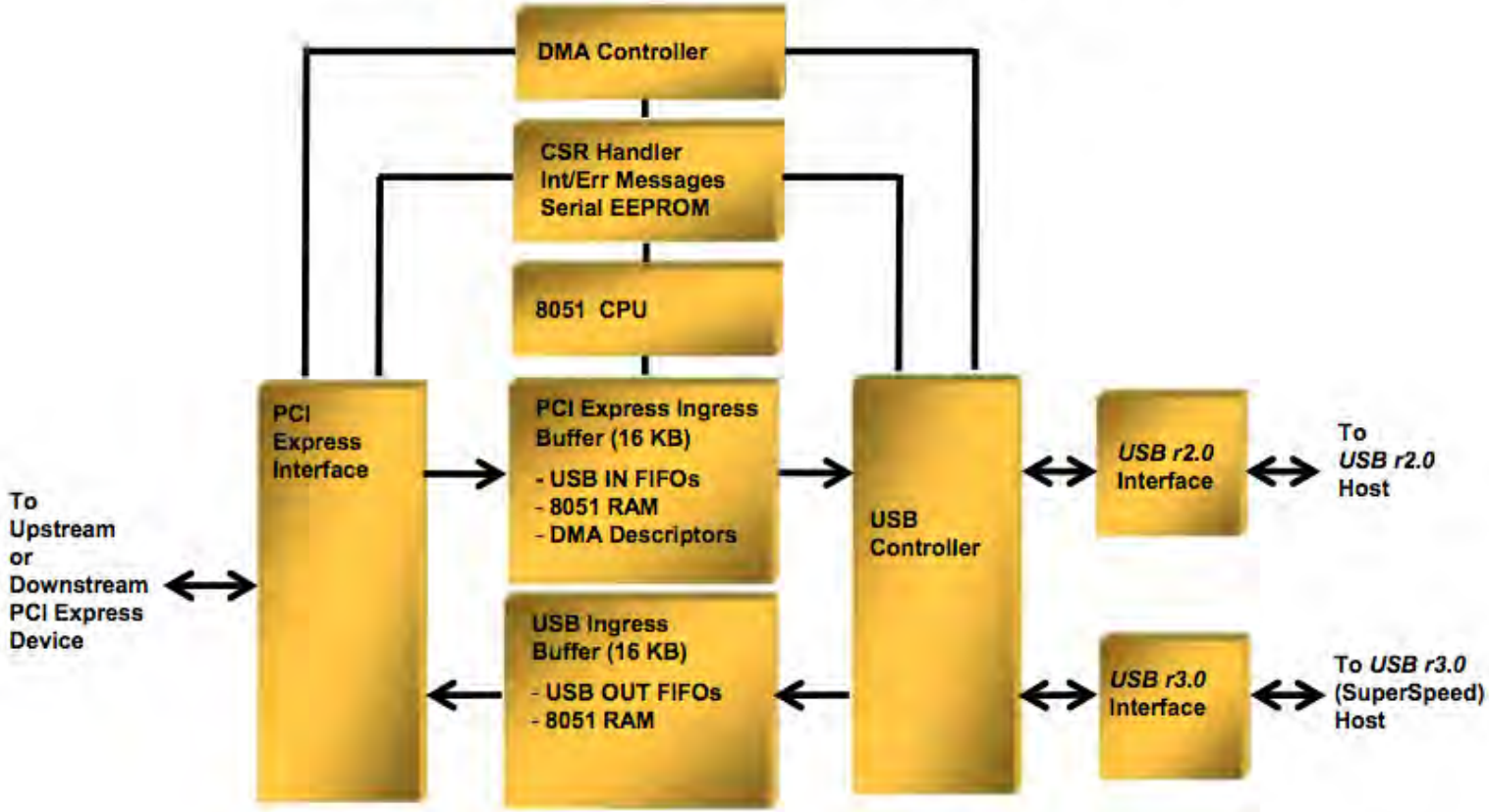
Minimum: 1
Multiples: 1

**Pricing (USD)**

1: $395.00


Ver1.0
4312

## Figure 1-1. USB 3380 Block Diagram



## 8.6.3 PCIOUT Endpoint

PCIOUT is a Bulk endpoint that allows the USB Host to initiate Read and Write Requests to PCI Express Space, using the PCI Master Control Cursor registers. Packets sent to this endpoint consist of the format listed in Table 8-12.

There can be from 0 to 64 Payload DWords, requiring USB packet sizes from 8 to 264 bytes.

**Table 8-12. PCIOUT Packet Format**

| Byte Index | Destination Register Bytes | |
|---|---|---|
| | Register | Bits |
| 0 | **PCIMSTCTL** register (USB Controller, offset 100h) | [7:0] |
| 1 | | [15:8] |
| 2 | | [23:16] |
| 3 | | [31:24] |
| 4 | **PCIMSTADDR** register (USB Controller, offset 104h) | [7:0] |
| 5 | | [15:8] |
| 6 | | [23:16] |
| 7 | | [31:24] |
| 8 through 11 | – | Payload DW0 (LSB first; to PCIOUT FIFO) |
| 12 through 15 | – | Payload DW1 (LSB first; to PCIOUT FIFO) |
| … | – | And so forth |

**Register 15-57. 200h, 210h, 220h, 230h, 240h, 250h DEP_CFG Dedicated Endpoint Configuration for CSROUT, CSRIN, PCIOUT, PCIIN, STATIN, and RCIN (USB Controller)**

| Bit(s) | Description | Access | Serial EEPROM | Default |
|---|---|---|---|---|
| 3:0 | **Endpoint Number**<br>Selects the endpoint number. | RW | Yes | RCIN = Ch,<br>CSROUT = Dh,<br>CSRIN = Dh,<br>PCIOUT = Eh,<br>PCIIN = Eh,<br>STATIN = Fh |
| 7:4 | ***Reserved*** | RsvdZ | Yes | 0h |
| 8 | **Endpoint Type**<br>0 = STATIN or RCIN endpoint becomes a BULK endpoint.<br>1 = STATIN or RCIN endpoint becomes an INTERRUPT endpoint. Valid only for the STATIN or RCIN endpoint.<br>All other endpoints are BULK. | RW | Yes | STATIN = 1,<br>RCIN = 1,<br>Others = 0 |
| 9 | ***Reserved*** | RsvdZ | Yes | 0 |
| 10 | **Endpoint Enable**<br>1 = Enables this endpoint | RW | Yes | RCIN = 0 in Adapter mode,<br>Others = 1 |
| 15:11 | **Service Interval**<br>Determines the interrupt service interval for STATIN/RCIN endpoints in *USB r3.0* mode. | RW | Yes | STATIN = 1,<br>RCIN = 1,<br>Others = 0 |
| 31:16 | ***Reserved*** | RsvdZ | Yes | 0000h |

# USB3380.c:

```
/* Explicitly disable the 6 dedicated endpoints */
tmp = 0x0d;
for (i = 0; i < 4; i+=2, tmp++) {
        writel (tmp, &dev->dep[i].dep_cfg);
        writel (tmp, &dev->dep[i+1].dep_cfg);
}
writel (0x0f, &dev->dep[4].dep_cfg);
writel (0x0c, &dev->dep[5].dep_cfg);
```

# PyUSB

## About

PyUSB aims to provide easy USB access to the Python language.

The project is divided in two major versions: the stable 0.x and the under development 1.0
PyUSB 1.0 enhances the library in several ways:

- Support for libusb 0.1, libusb 1.0 and OpenUSB.
- Easy API to communicate with devices.
- Support for custom library backends.
- Isochronous transfer type support.
- 100% written in Python by ctypes.
- It runs on any Python version >= 2.4 (this includes Python 3).

**Table 7-2. PCI Master Control Registers[a]**

| Offset | Register | Function |
|---|---|---|
| 100h | **PCIMSTCTL** | Specifies access type and direction (Read/Write) |
| 104h | **PCIMSTADDR** | Contains the PCI Express address to be accessed |
| 108h | **PCIMSTDATA** | Contains data to be written or data returned from a Read |

*a. The PCI Master Control register set also includes one Status and one Message register.*

Through the PCI Master Control registers, the 8051 or USB Host CPU can generate the following types of accesses into PCI Express space:

- Configuration Read
- Configuration Write
- Memory Read
- Memory Write
- I/O Read
- I/O Write
- PCI Express Messages

**Register 15-41. 100h PCIMSTCTL PCI Master Control (USB Controller)**

<table>
<tr><th>Bit(s)</th><th>Description</th><th>Access</th><th>Serial EEPROM</th><th>Default</th></tr>
<tr><td>3:0</td><td>PCI Express First Byte Enables<br>Determines the first Byte Enables of a PCI Express transaction. For 1-DWord transactions, it can be any value. For multiple DWord transactions, only contiguous Byte Enables are allowed, or the endpoint is halted. This field is used directly in the FBE field of the PCI Express Header.</td><td>RW</td><td>Yes</td><td>0h</td></tr>
<tr><td>5:4</td><td>PCI Express Master Command Select<br>When the USB 3380 performs PCI Express transactions initiated by the PCIOUT endpoint or 8051, determines the PCI Express Request type issued.<br>Note: The Configuration Type (Type 0 or Type 1) is determined by the PCI Master Address format.
<table>
<tr><th>Value</th><th>Read Command</th><th>Write Command</th></tr>
<tr><td>00b</td><td>Memory Read</td><td>Memory Write</td></tr>
<tr><td>01b</td><td>I/O Read</td><td>I/O Write</td></tr>
<tr><td>10b</td><td>Configuration Read</td><td>Configuration Write</td></tr>
<tr><td>11b</td><td>Reserved</td><td>PCI Express Message</td></tr>
</table></td><td>RW</td><td>Yes</td><td>00b</td></tr>
<tr><td>6</td><td>PCI Express Master Start<br>Writing 1 causes a PCI Write or Read transaction to start. This bit is Cleared when the PCI transaction is complete.<br>For Write operations, determines when to start another Write.<br>For Read operations, determines when the PCIMSTDATA register (USB Controller, offset 108h) contains valid data.<br>This bit is automatically Cleared when a UR or CA occurs.</td><td>RW1S</td><td>Yes</td><td>0</td></tr>
<tr><td>7</td><td>PCI Express Master Read/Write<br>0 = PCI Write transaction is selected.<br>1 = PCI Read transaction is selected. For 8051 Writes to the PCI Express interface, this bit must be Cleared before the PCIMSTDATA register (USB Controller, offset 108h) is written.</td><td>RW</td><td>Yes</td><td>0</td></tr>
<tr><td></td><td>Message Code</td><td></td><td></td><td></td></tr>
</table>

# Attacking via PCIe

# Demo, etc - WIP

# Future Plans

# Thunderbolt

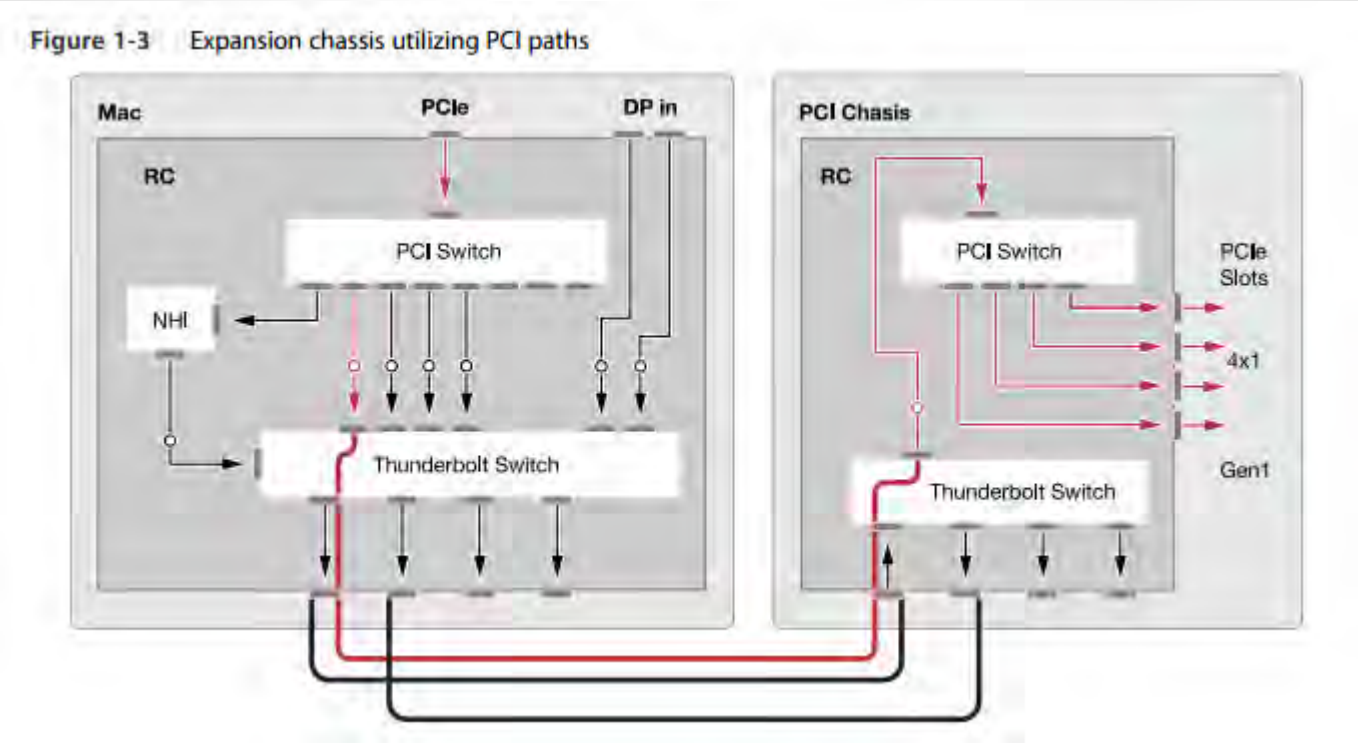



Diagram: Apple Thunderbolt Device Driver Programming Guide

# Thunderbolt

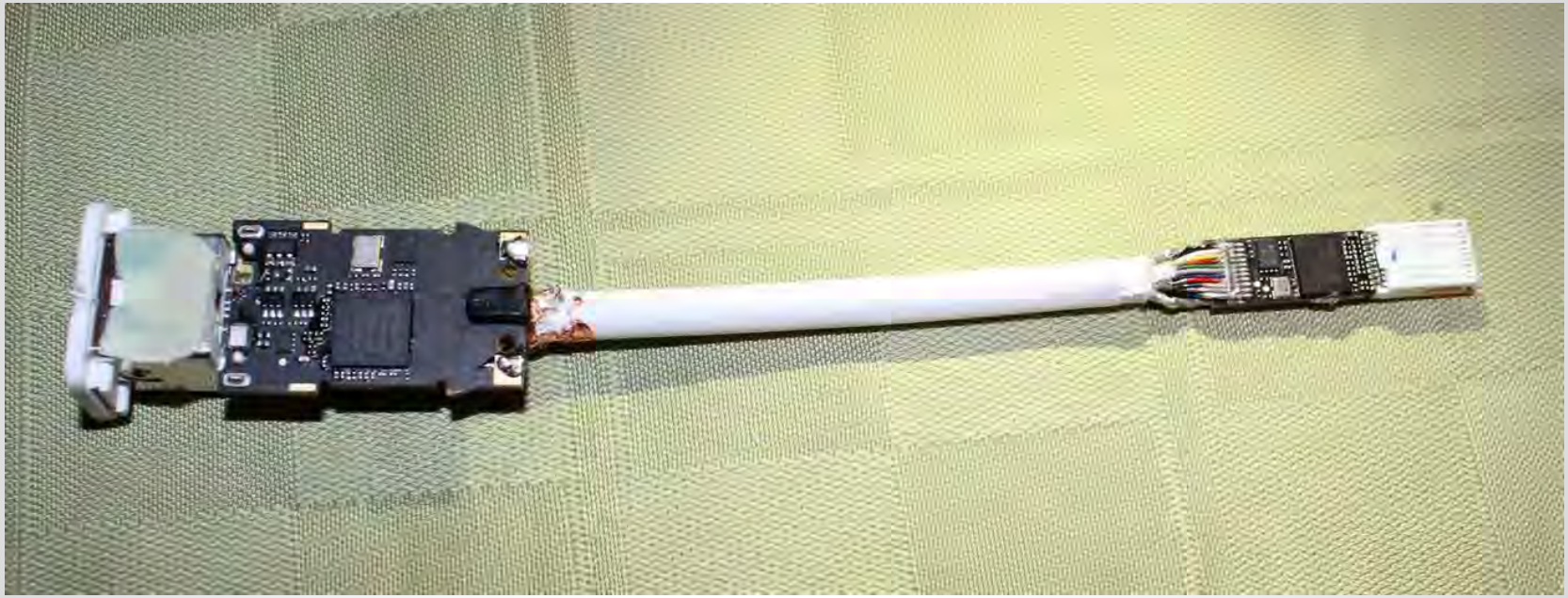
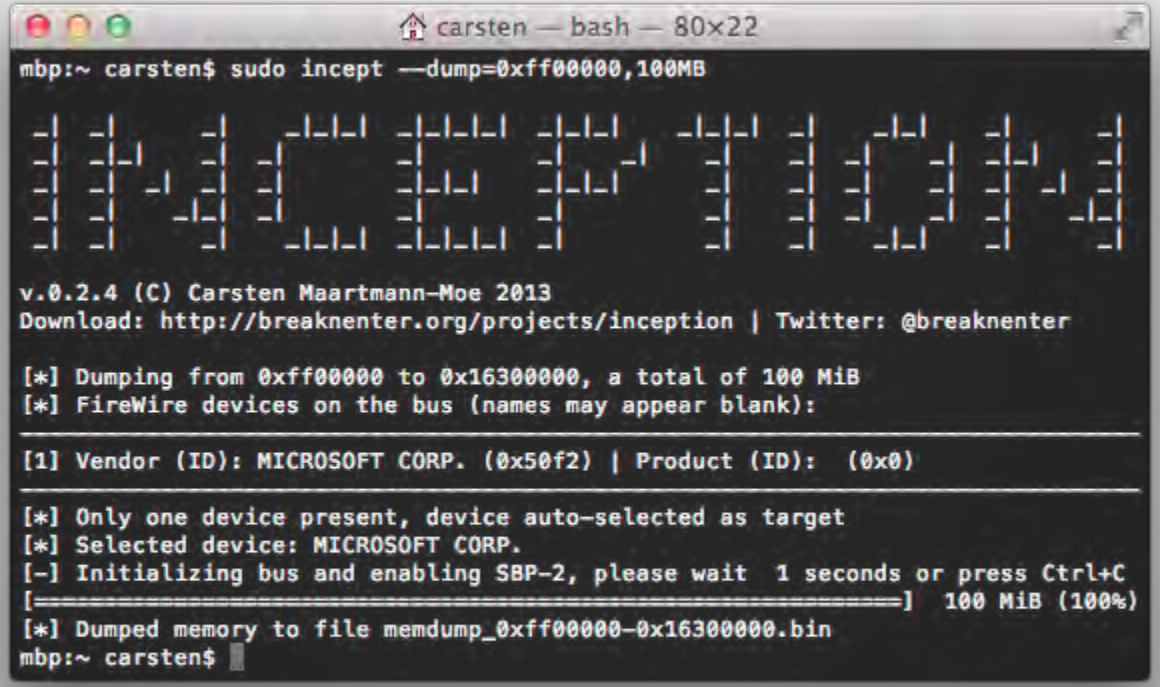


Photo credits: Chris Bergey via imgur.com

# inception/funderbolt



# Questions?

Miles Crabill
@milescrabill
miles@milescrabill.com

Joe FitzPatrick
@securelyfitz
joefitz@securinghardware.com
http://www.securinghardware.com