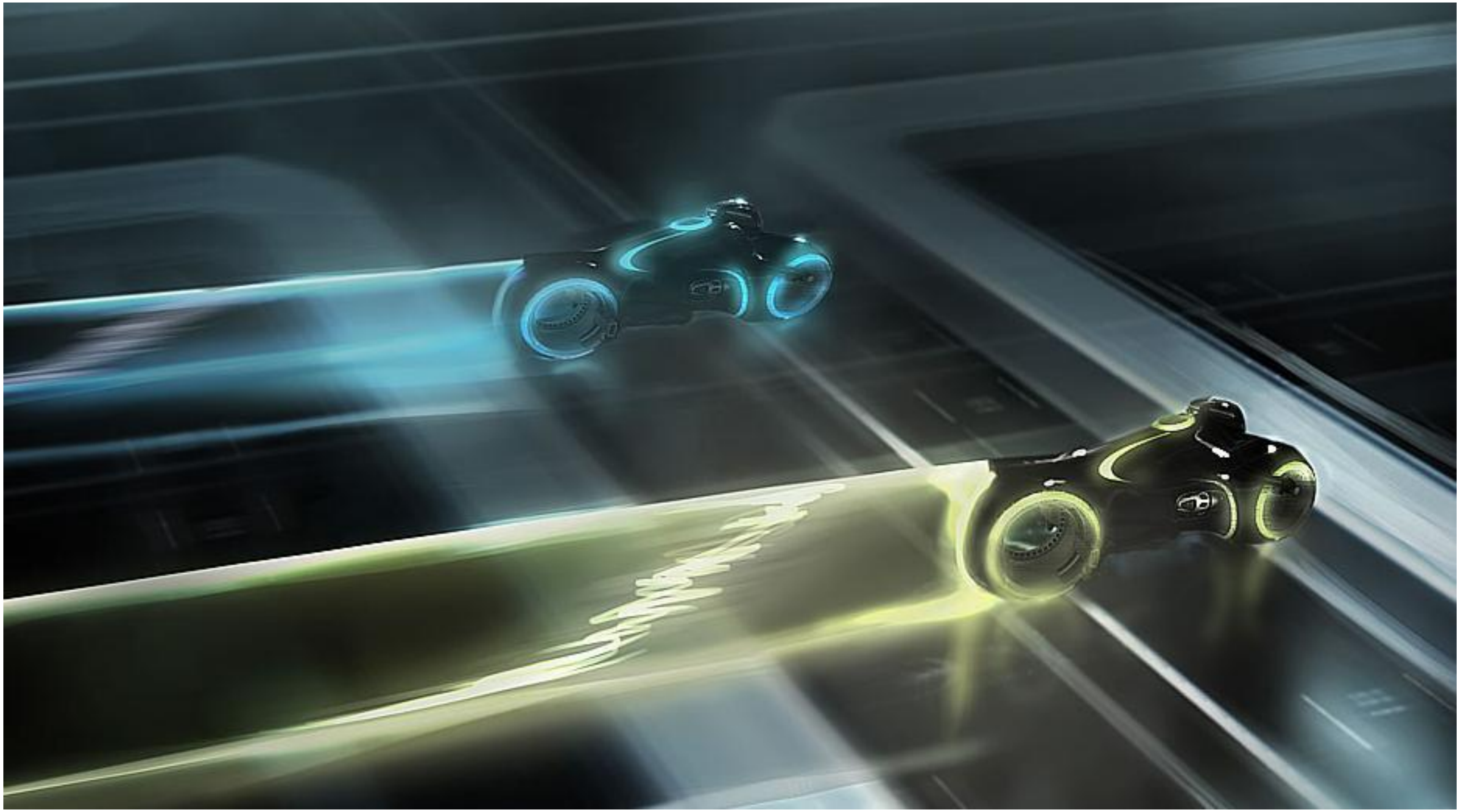
iSECpartners
part of nccgroup

Funderbolt

Adventures in Thunderbolt DMA Attacks

Russ Sevinsky

A Trip Down Memory Lanes



A Trip Down Memory Lanes

- Background
  - Thunderbolt
    - Apple and Intel
    - External Port
    - PCI Express (PCIe) and DisplayPort using the same port
  - DMA
    - Direct Memory Access
    - Processor becomes bottleneck for high-speed transfers
    - Lets devices read and write directly to RAM

A Trip Down Memory Lanes

- Why external buses matter for security experts?
  - Digital Forensics
    - Getting data to solve a mystery
  - User protection
    - So RAM contents can be safe
  - Sneaky DRM
    - Bus encryption

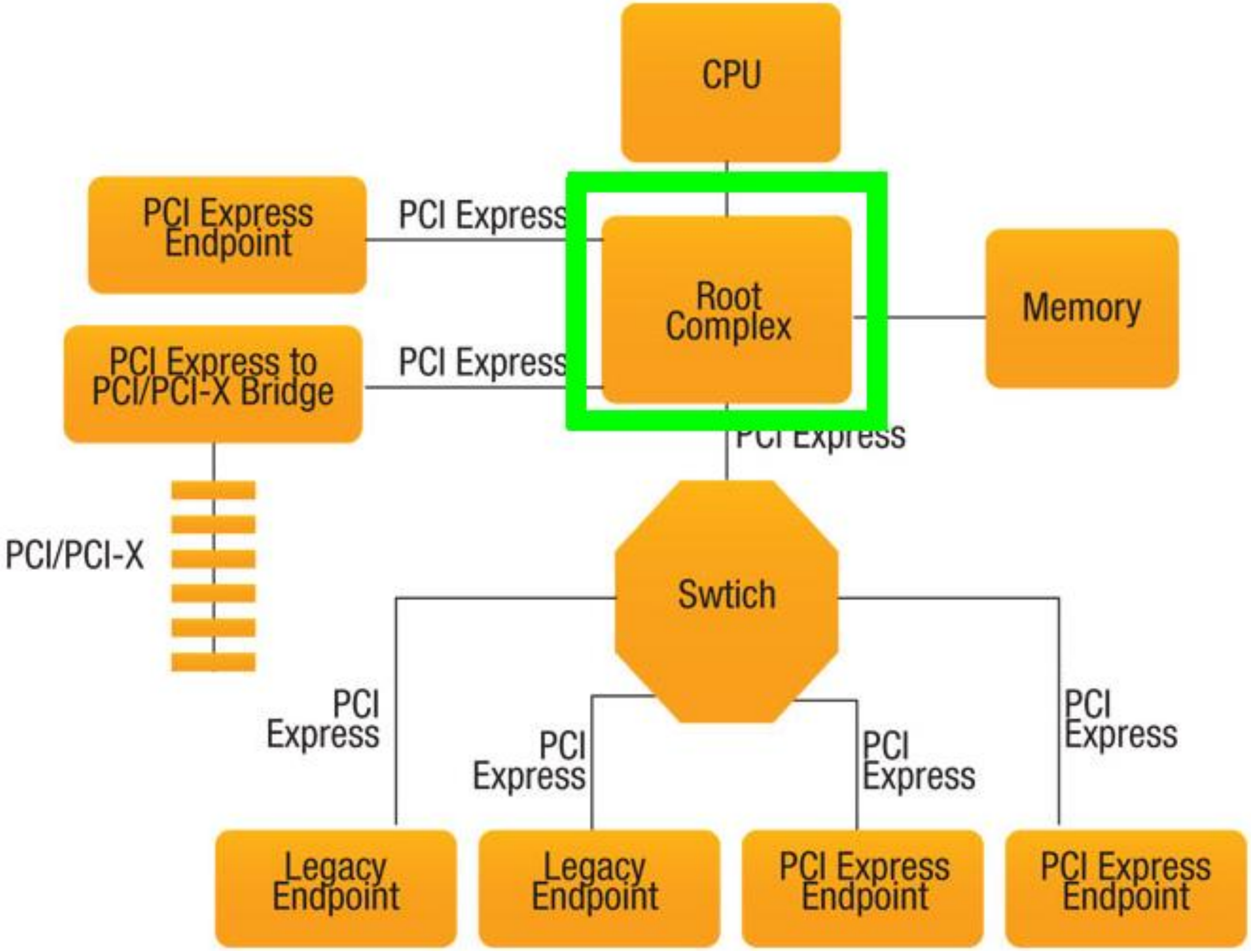
A Trip Down Memory Lanes

- PCI Express (PCIe)
  - High-speed serial bus
  - Data sent via “lanes”
  - A Lane is made up of differential wire pairs
    - One + and one – wire offset a small amount
    - Helps reducing noise
  - One lane (x1) is made up of two differential pairs
    - Transmit pair (PET)
    - Receive pair (PER)

A Trip Down Memory Lanes

- PCIe (cont)
  - Four lanes (x4) has eight pairs, x8 has 16 pairs, etc…
  - All lanes use another differential pair for clock
    - REFCLK
  - So… x1 uses 6 wires for data communication
    - PET, PER and REFCLK
  - Data sent via "packets"
  - Point-to-point topology using Root Complex
    - Requests for devices and memory go to "root complex"

A Trip Down Memory Lanes



A Trip Down Memory Lanes

- Mitigations
  - Epoxy (really?)
  - Input/Output Memory Management Units (IOMMUs)
    - Maps physical memory addresses to logical addresses
    - Think "VM for DMA"
    - Prevents devices from requesting physical addresses directly
  - Secure Configurations
- Current attacks?
  - Daisy chaining Thunderbolt and Firewire
  - Inception

How My Adventures Went

How My Adventures Went

- Improvised Tools for Analysis
  - Multimeter
  - Soldering station
  - Heat gun
  - Desoldering tools
  - Ethernet cable
  - Epoxy (really?)
  - Logic Analyzer
  - Image Editor

How My Adventures Went

- Reversing Thunderbolt – The Process
  - Research a product
  - Take it apart
  - Trace all interesting chips
  - Look for datasheets
  - Sniff buses
  - Develop a map

How My Adventures Went

- Looking at consumer products
  - Buffalo MiniStation Thunderbolt/USB3 Hard Drive
    - 500GB and 1TB model
    - USB3 and Thunderbolt
    - Decent form factor for reversing
  - Apple Thunderbolt to Gigabit Ethernet Adapter
    - Tiny
    - Small
    - Little

How My Adventures Went

- External Hard Drive
  - Researching the product
  - Taking it apart
  - Tracing all interesting chips
  - Looking for datasheets
  - Sniffing buses
  - Developing a map

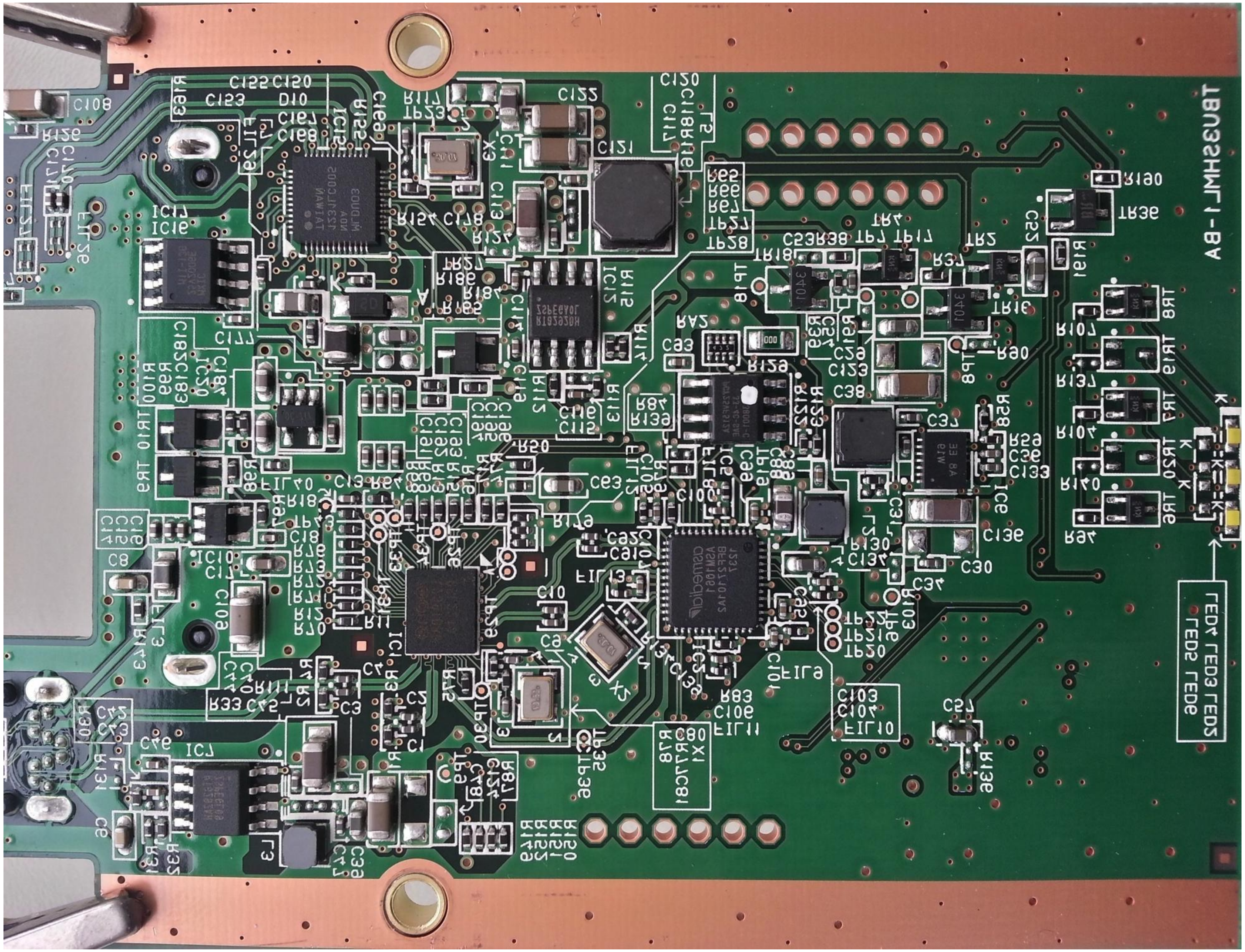
How My Adventures Went

- Excellent Anandtech review:
    - http://www.anandtech.com/show/6127/buffalo-ministation-thunderbolt-review-an-external-with-usb-30-and-thunderbolt
- Identified ICs for us!

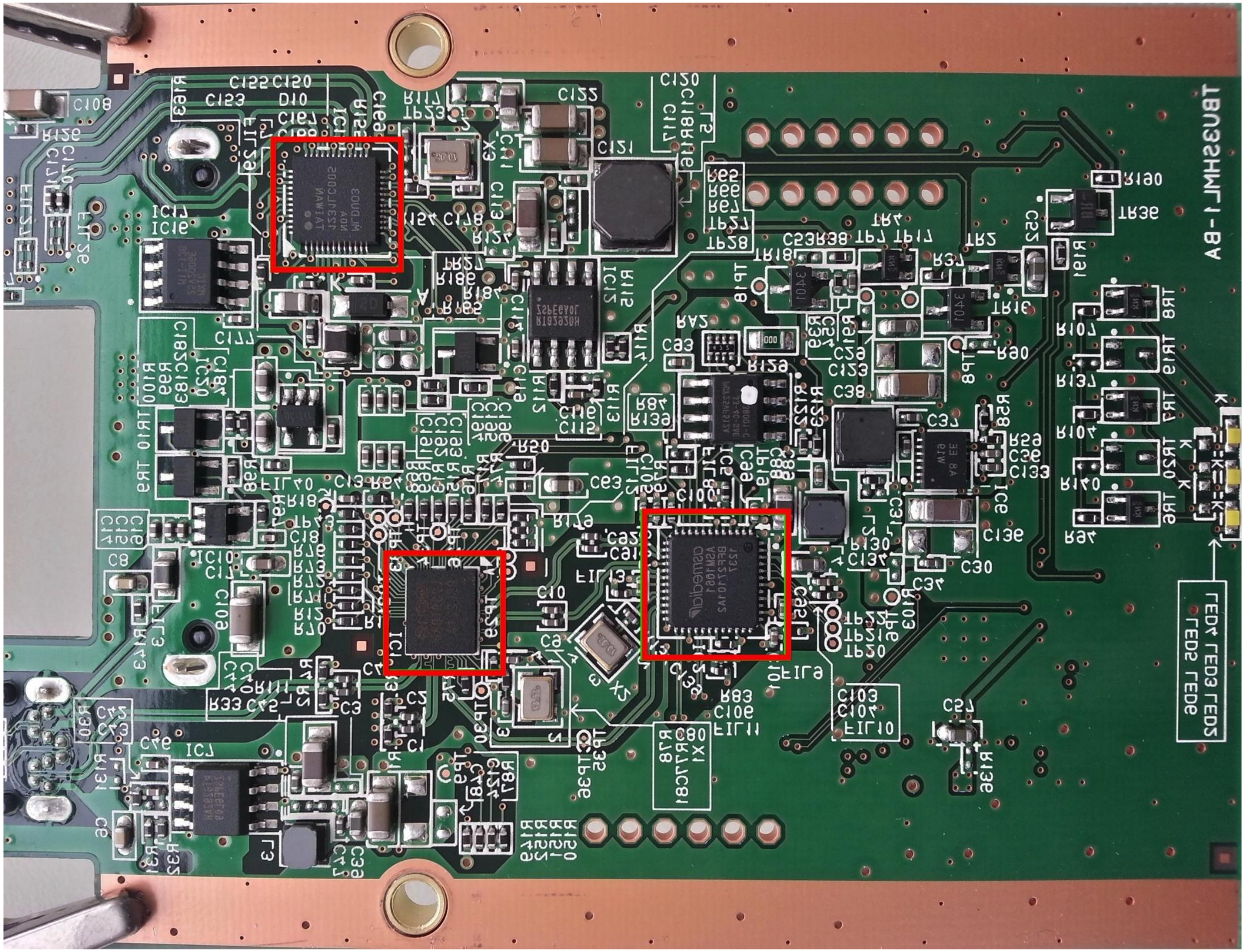
How My Adventures Went

- Main ICs
  - MLDU03
    - Medial Logic USB3.0 to SATA 6G Bridge
  - ASM1061
    - ASMedia PCIe to SATA Controller
  - DSL2210 (Peak Ridge)
    - Intel Thunderbolt Controller
    - Supports PCIe x1
  - LPC1114
    - NXP ARM Cortex M0

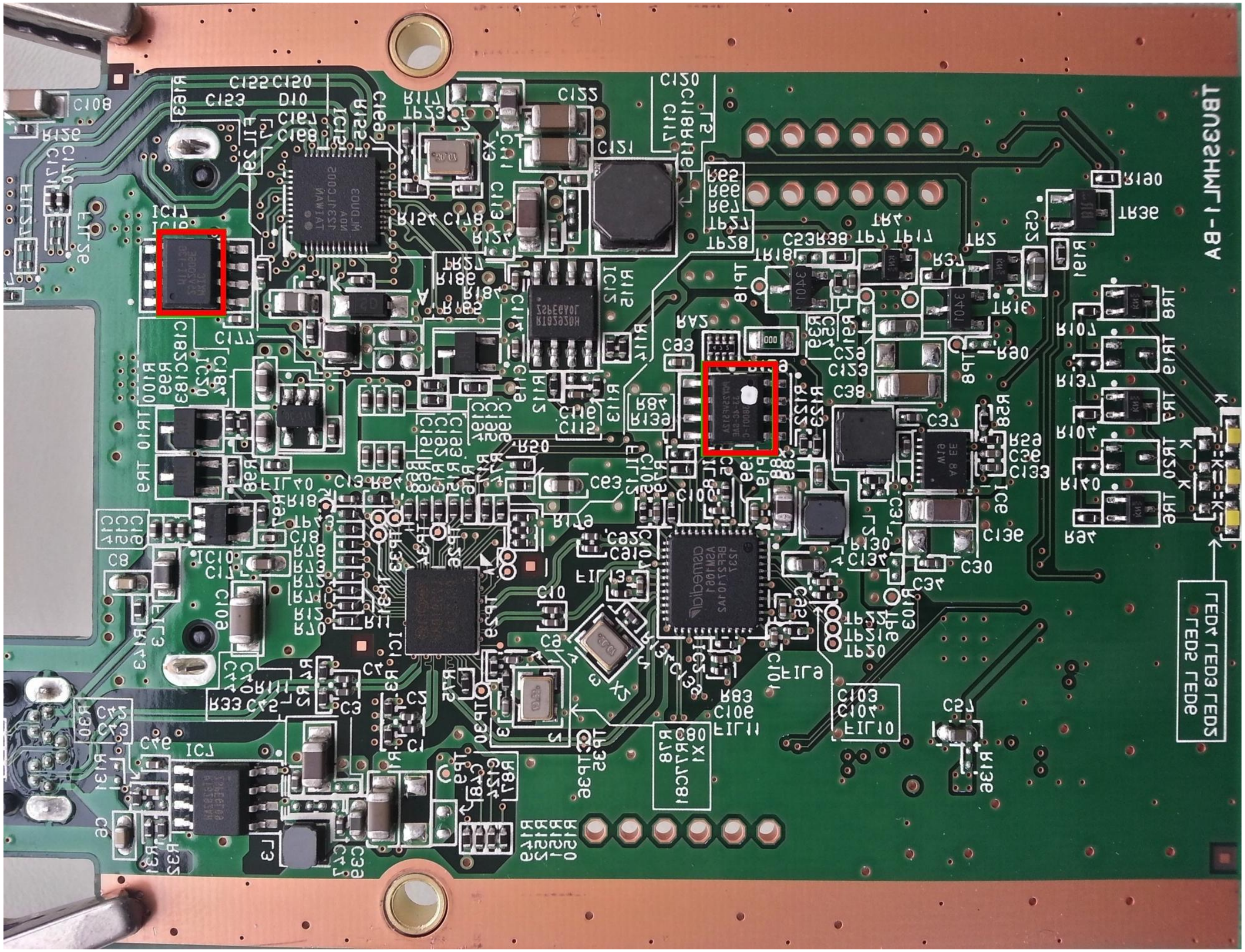
How My Adventures Went



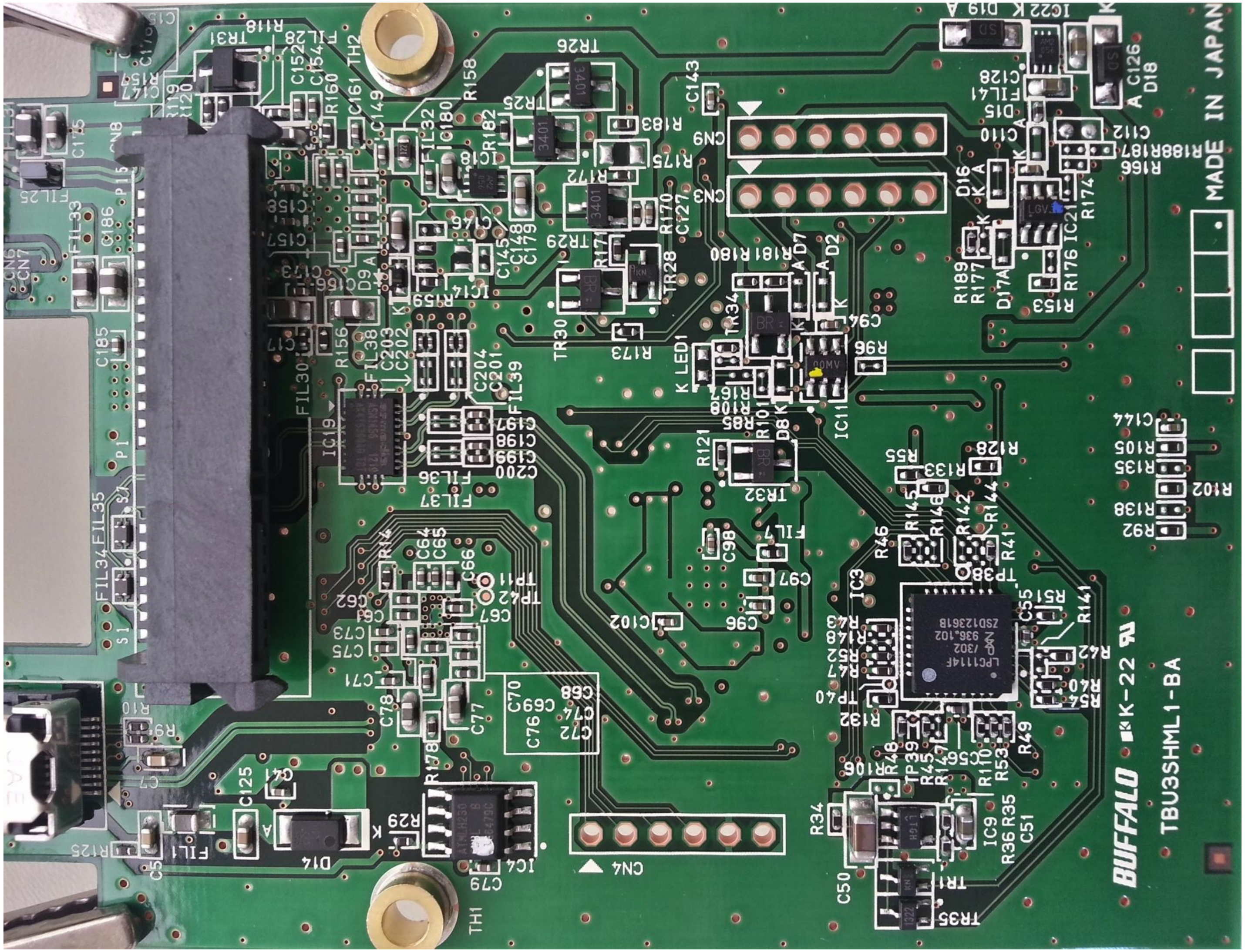
How My Adventures Went



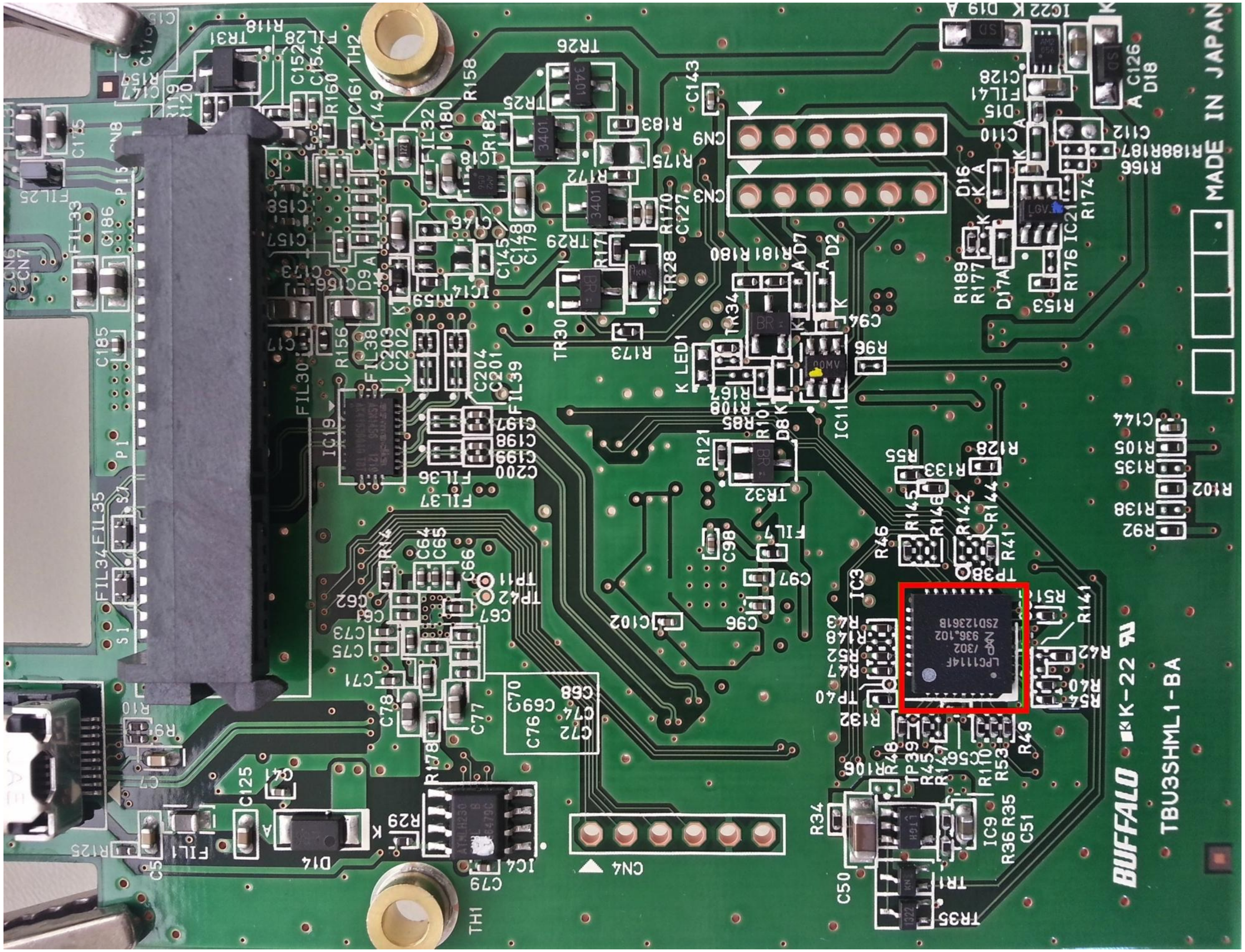
How My Adventures Went



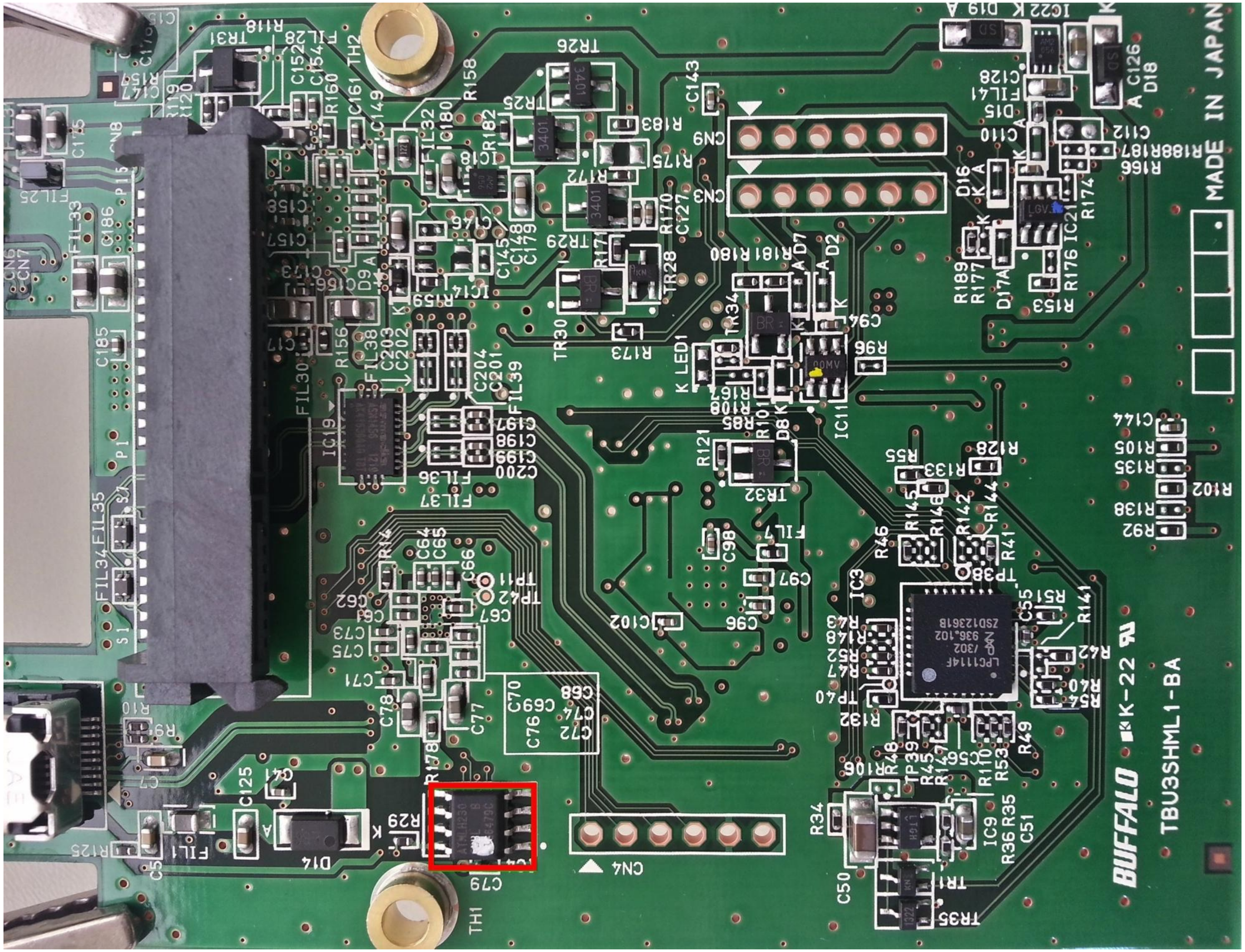
How My Adventures Went



How My Adventures Went



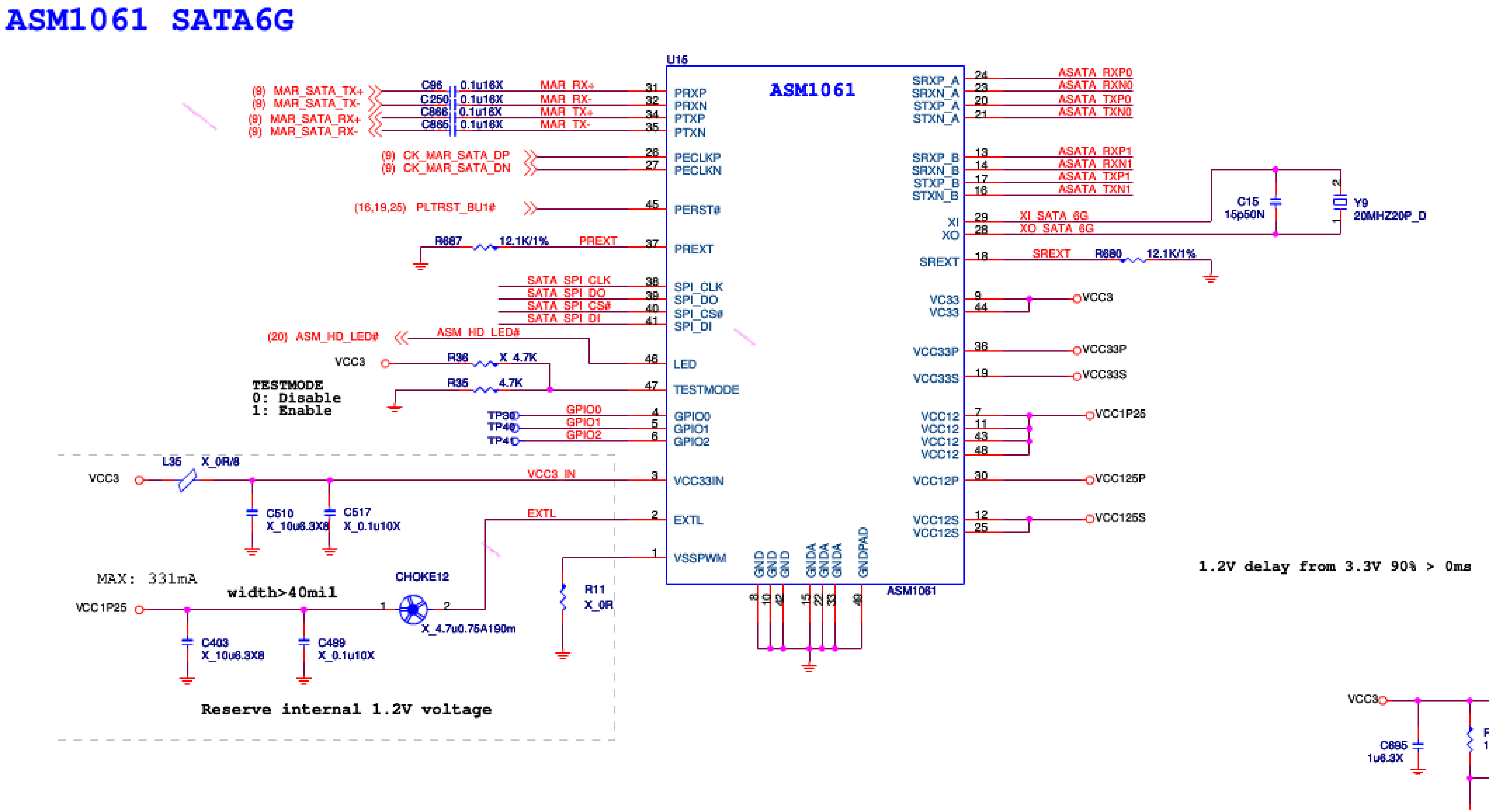
How My Adventures Went



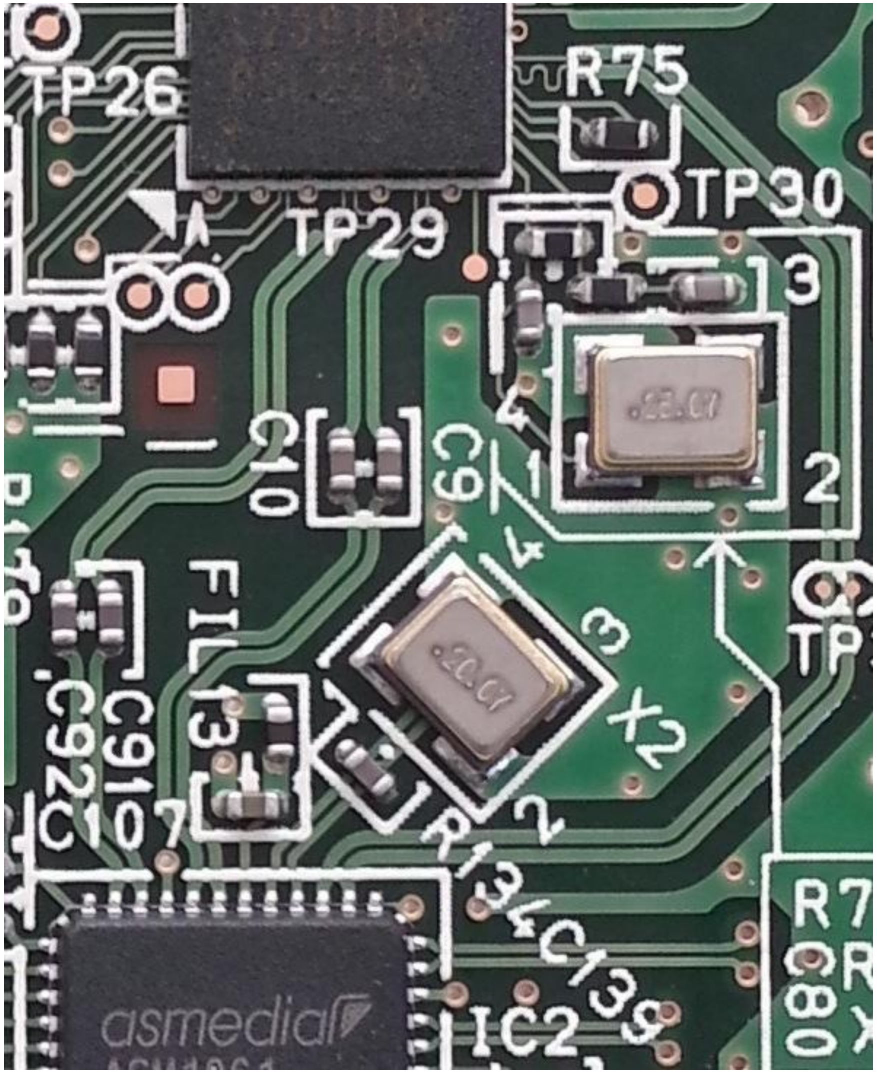
How My Adventures Went

- ASMedia ASM1061
  - PCIe/SATA Controller
  - Datasheets?
  - ROMs/Flashes?

How My Adventures Went



How My Adventures Went

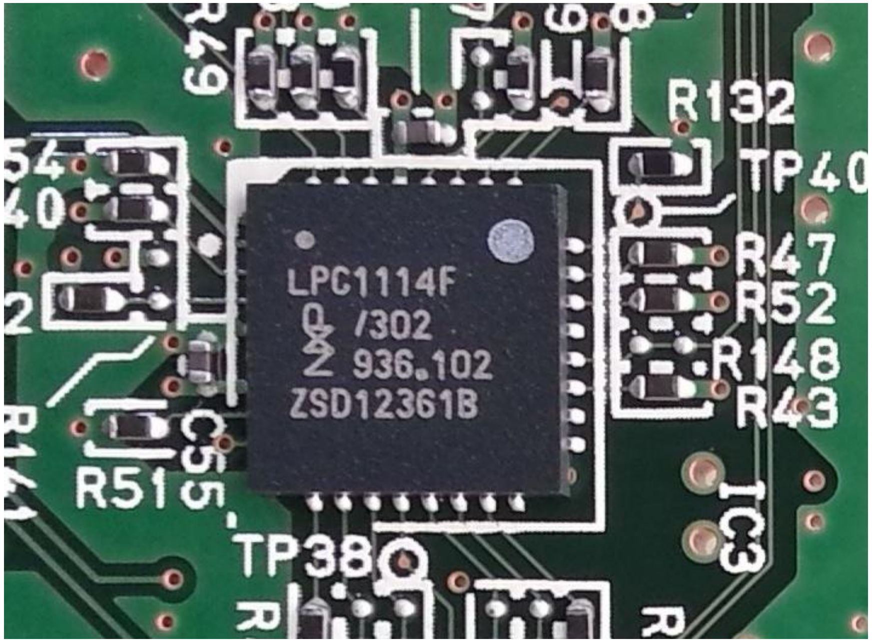


How My Adventures Went

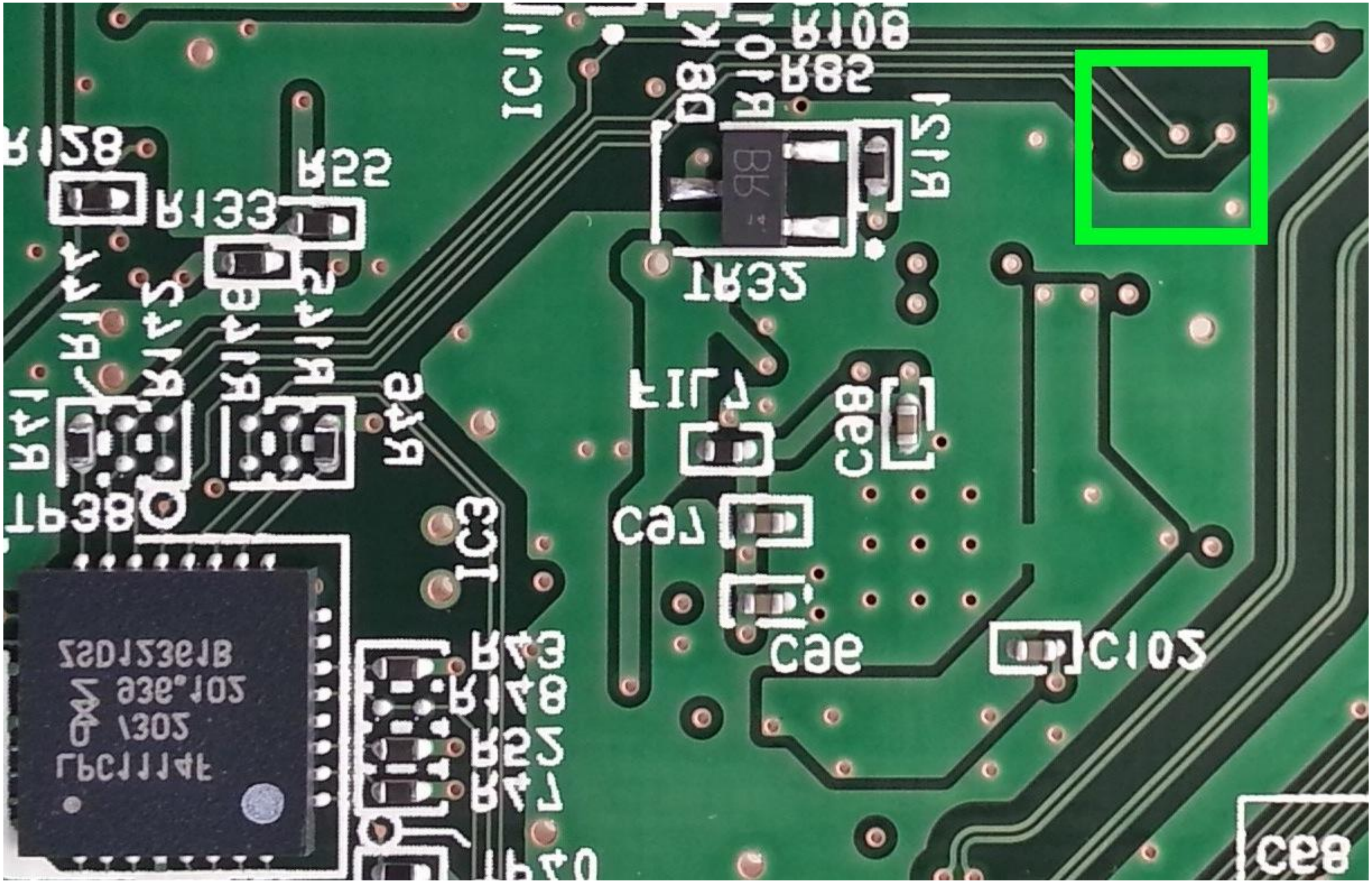
- Patch PCIe Controllers' SPI ROM to send DMA read requests?

How My Adventures Went

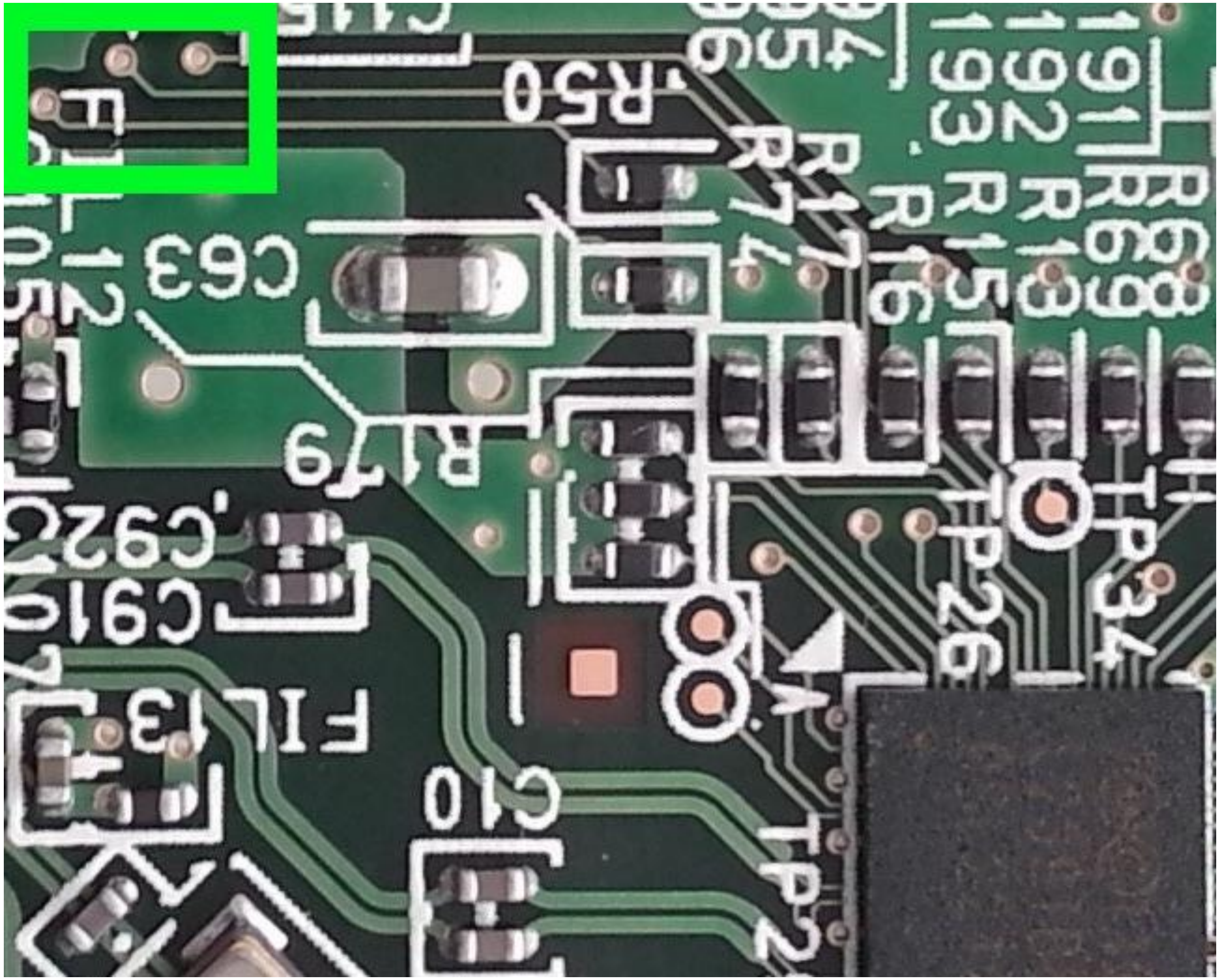
- NXP LPC1114
  - ARM Cortex M0
  - Used for… ??
  - No ROMs or Flashes
  - TONS of info
  - Connects into DSL2201
    - How do I know?



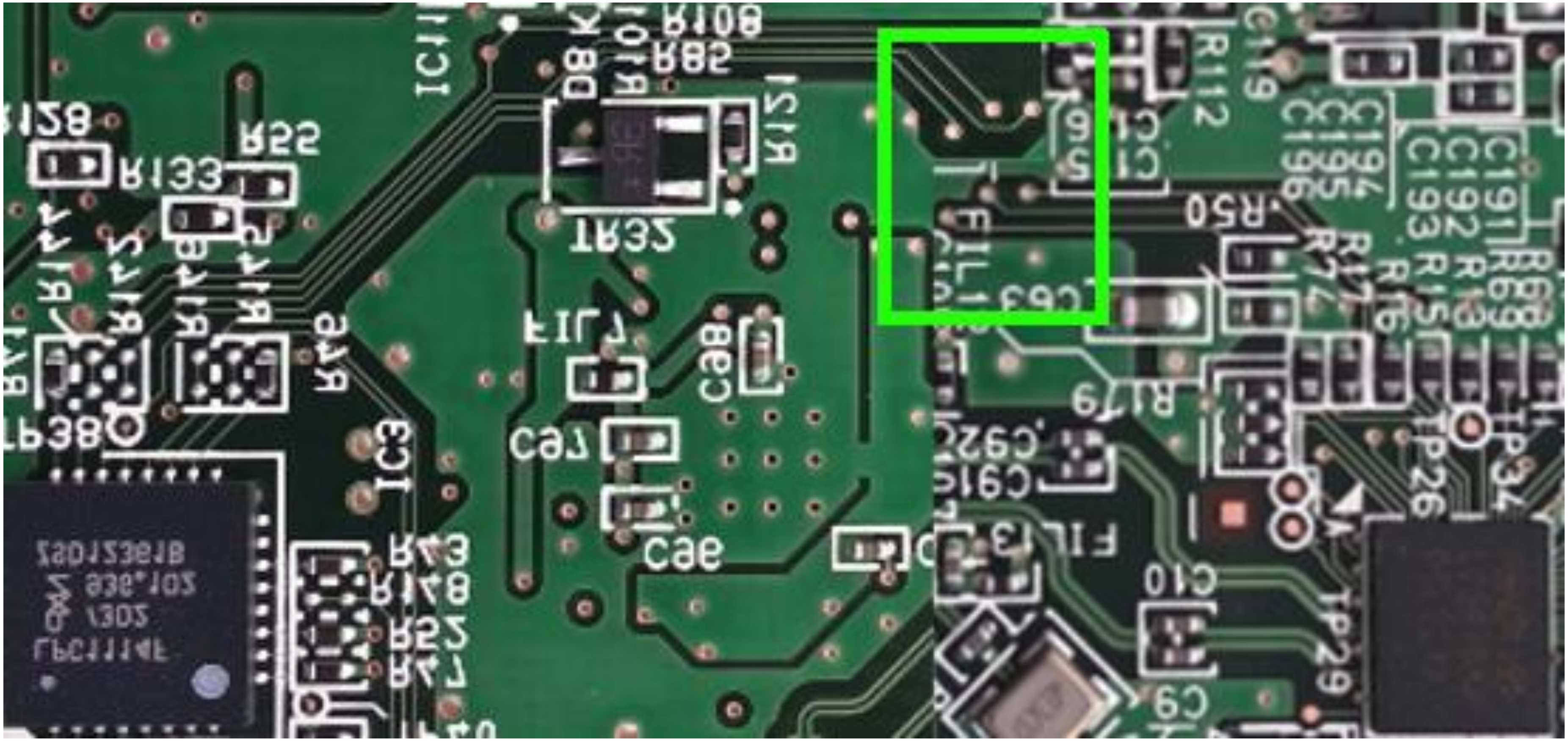
How My Adventures Went



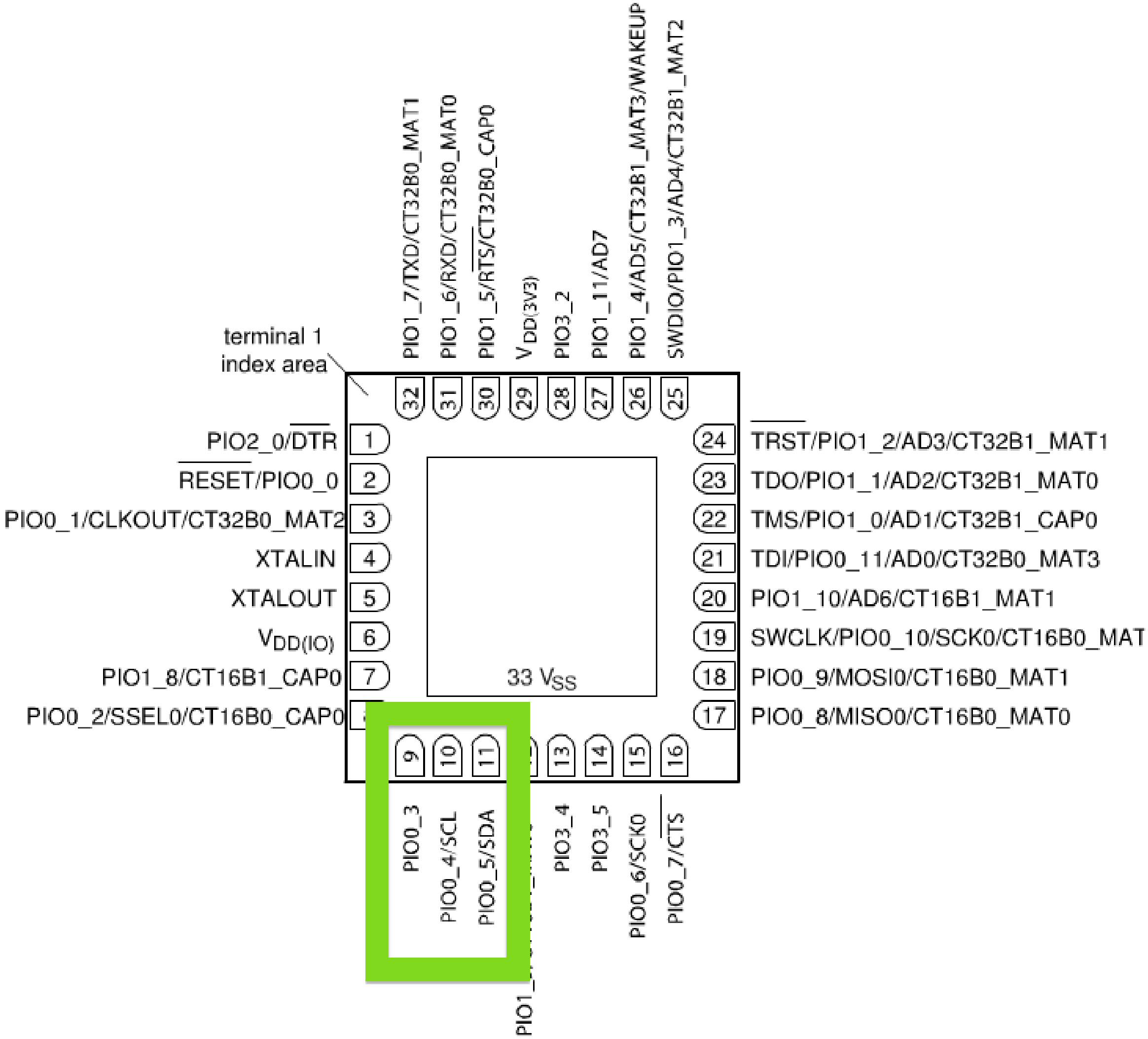
How My Adventures Went



How My Adventures Went

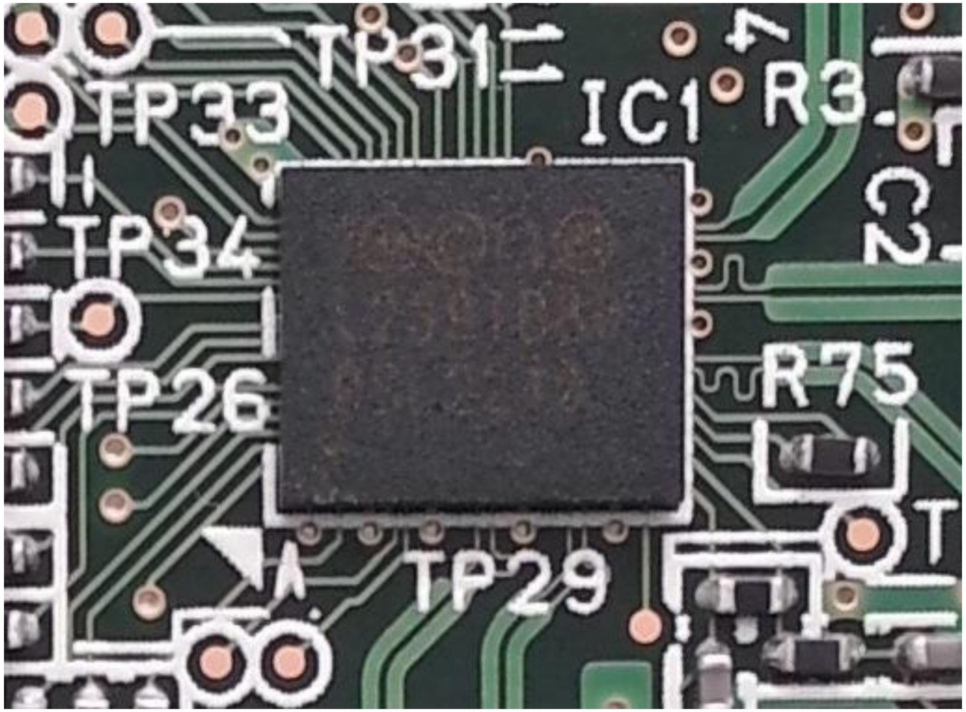


How My Adventures Went

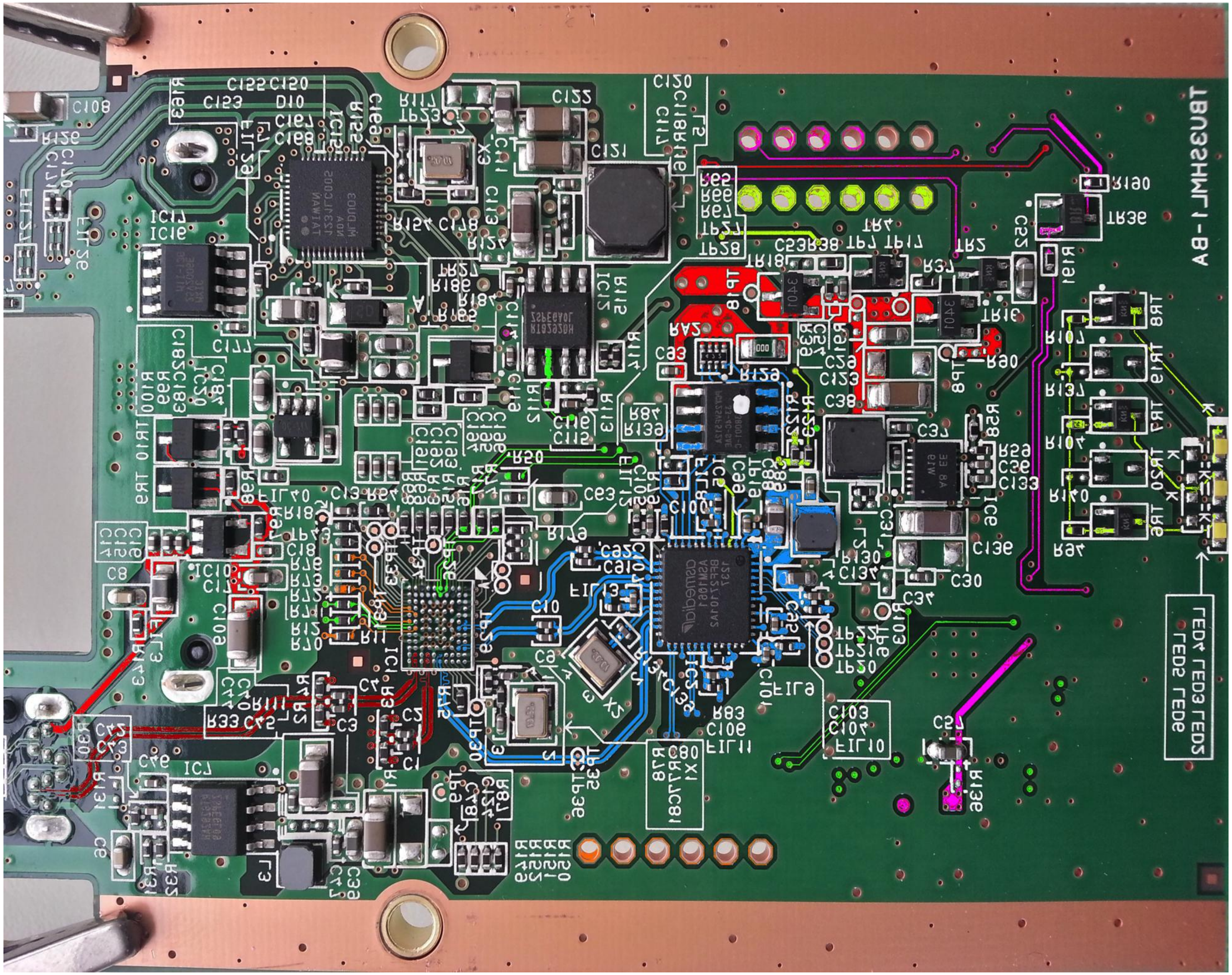


How My Adventures Went

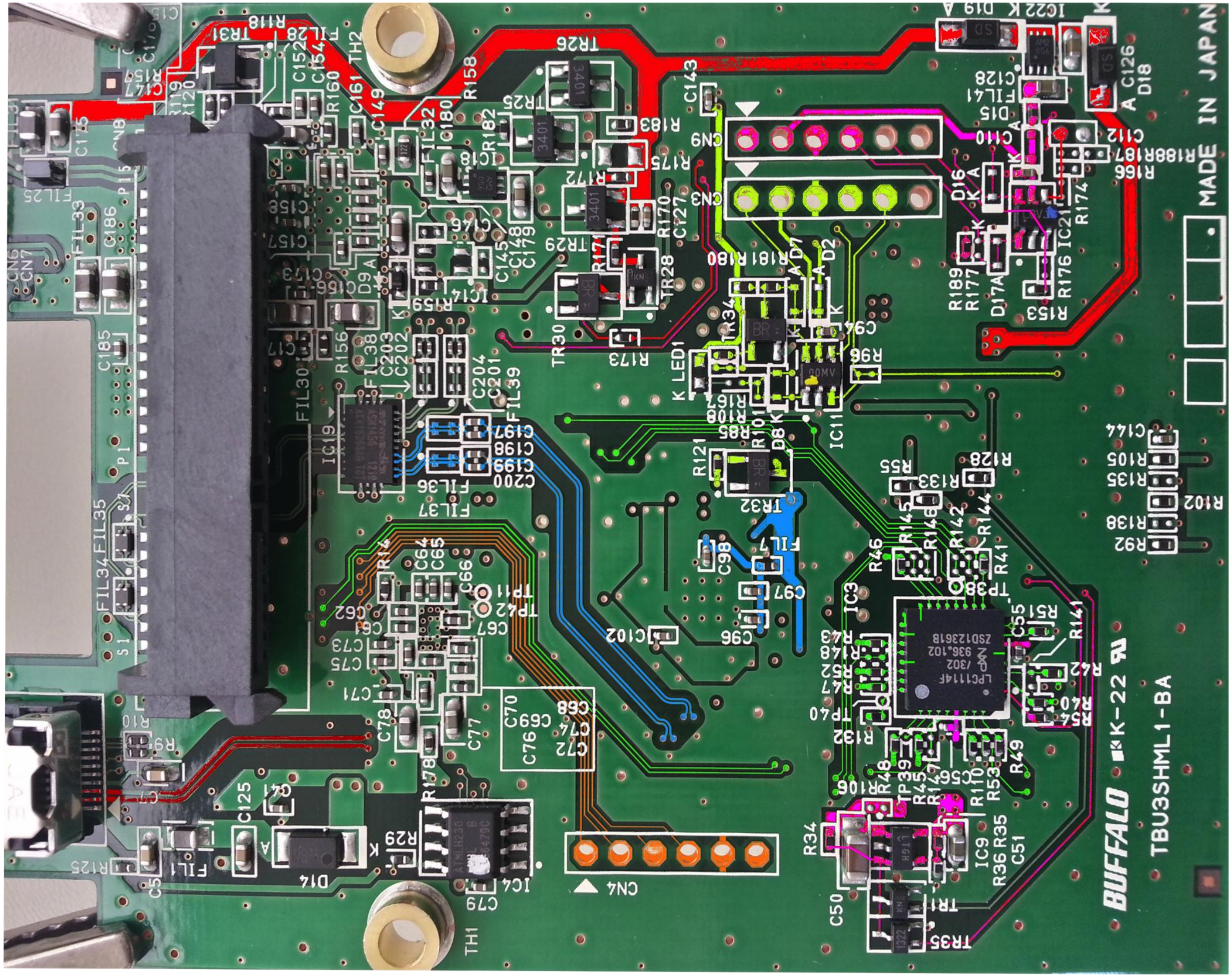
- Intel DSL2210
  - Thunderbolt Controller
  - No Datasheets
  - Promo info only
  - ROMs/Flashes?



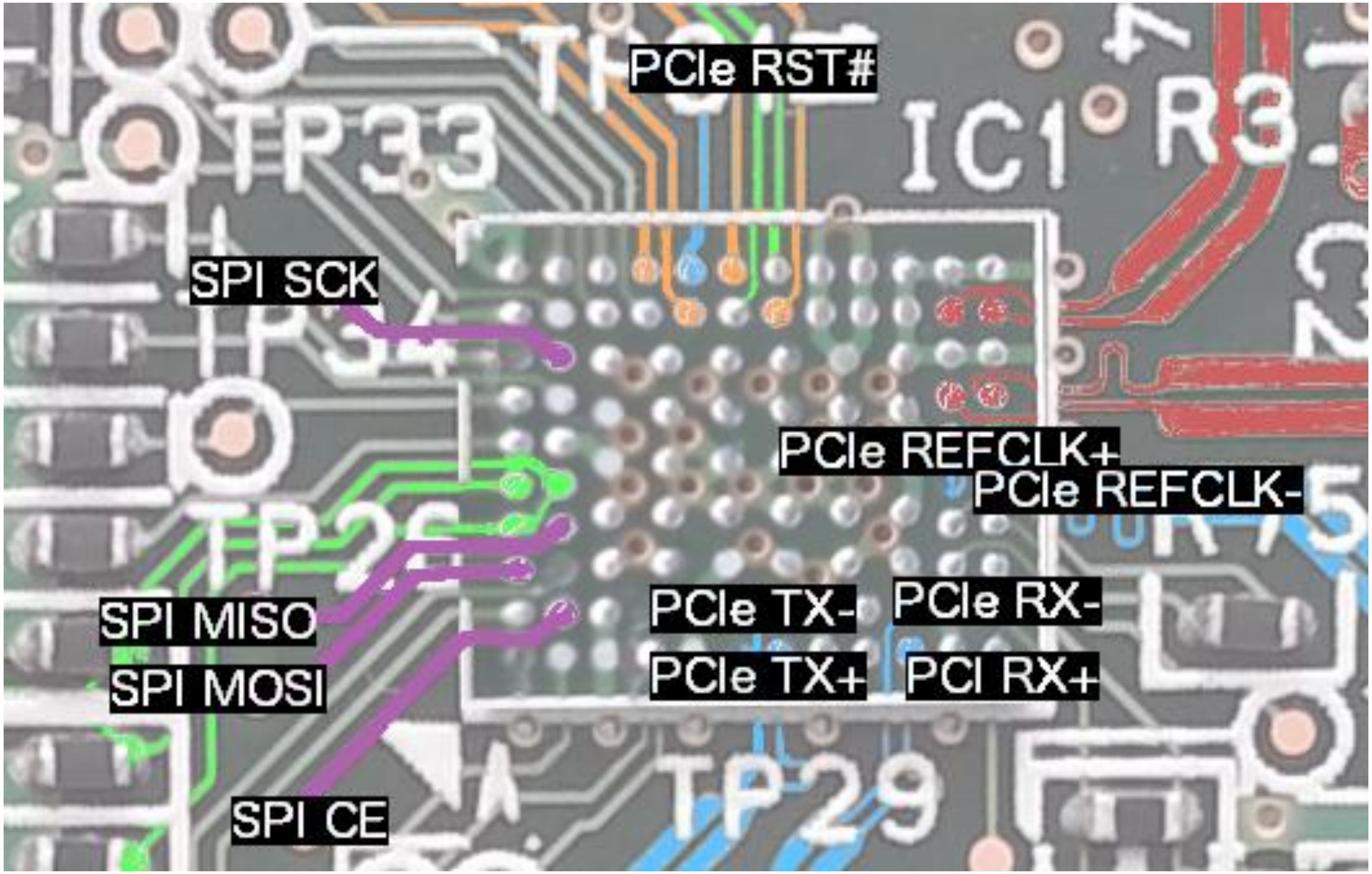
How My Adventures Went



How My Adventures Went



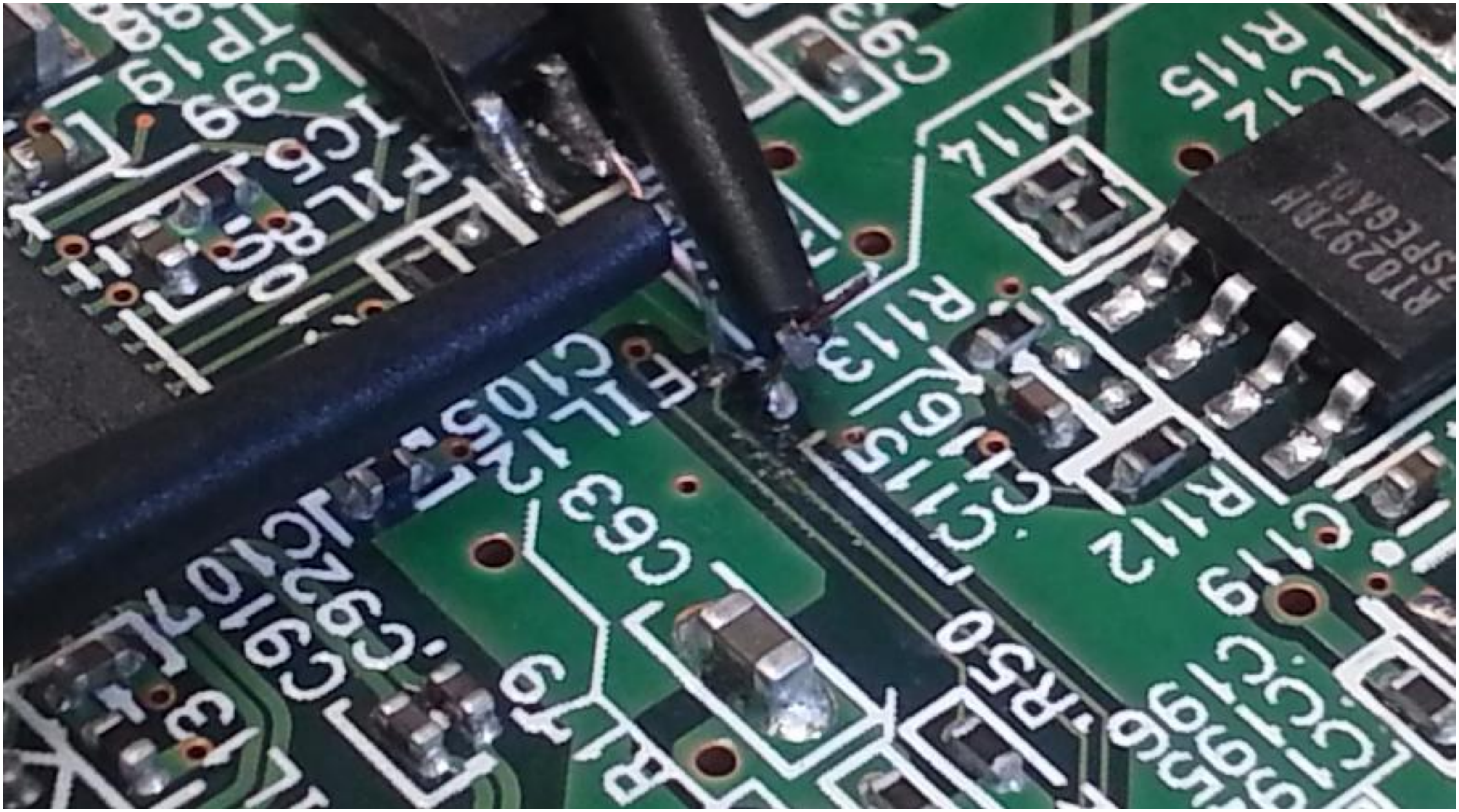
How My Adventures Went



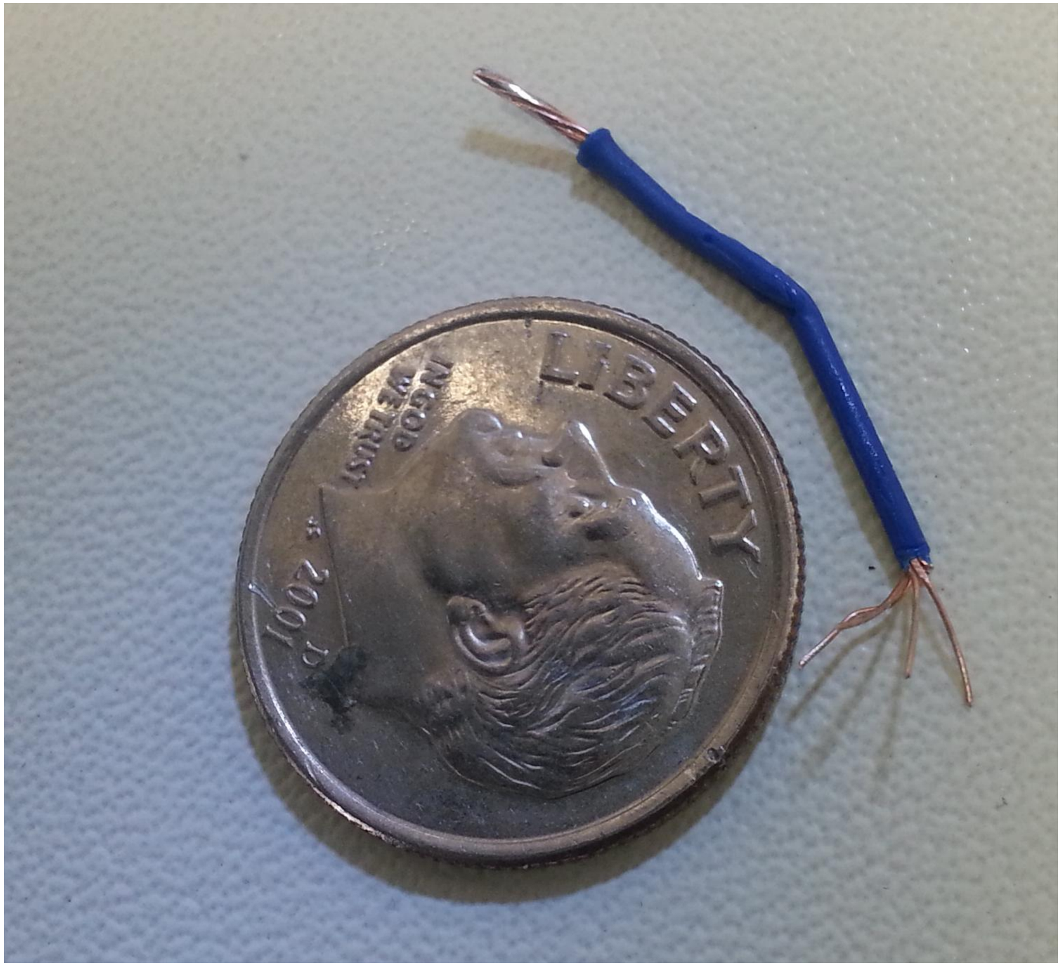
How My Adventures Went

- Thunderbolt Connector
  - 1 pair of High Speed lanes
    - TX and RX
  - All others pulled to ground
  - “LowSpeed” lines go into ARM’s UART?

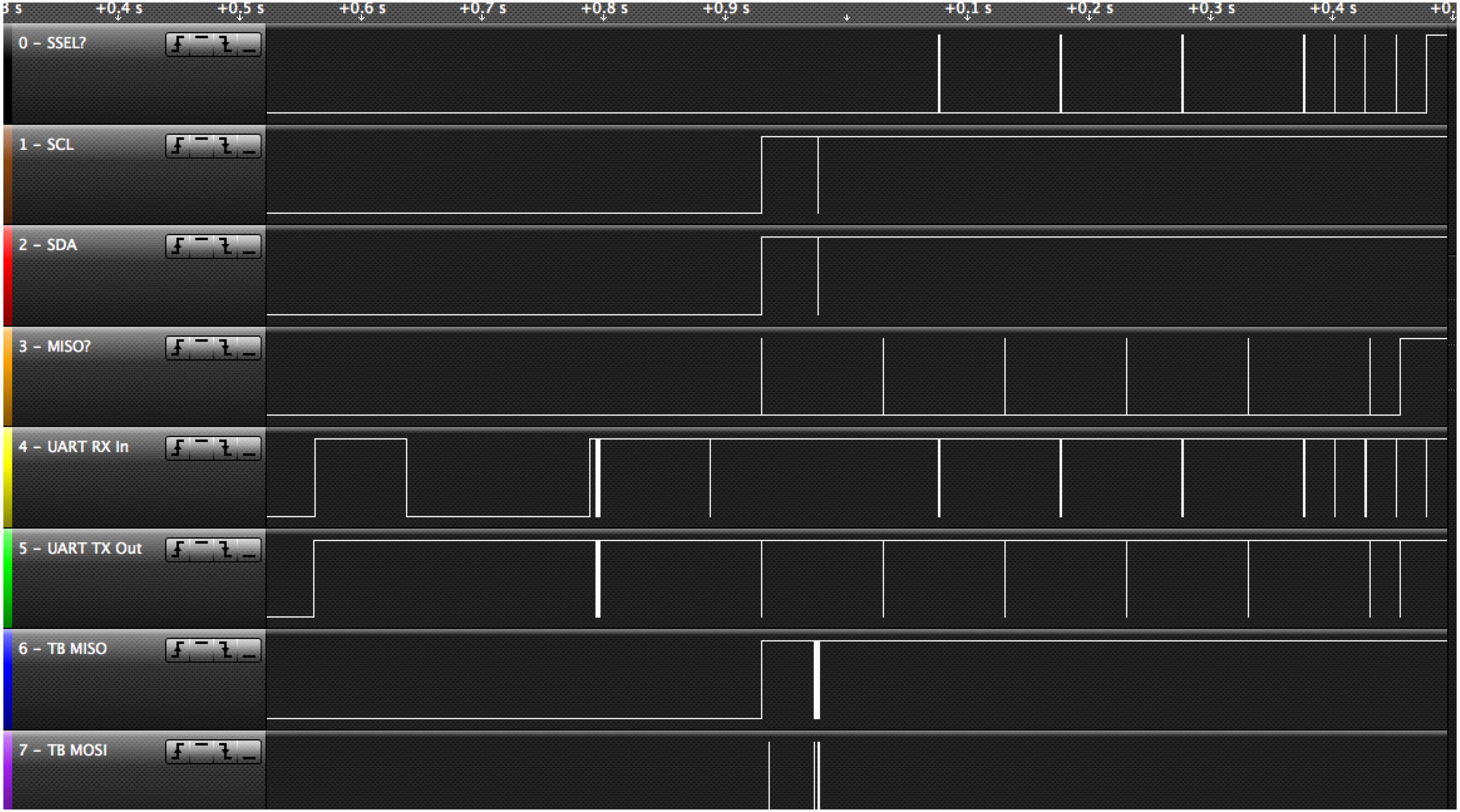
How My Adventures Went



How My Adventures Went

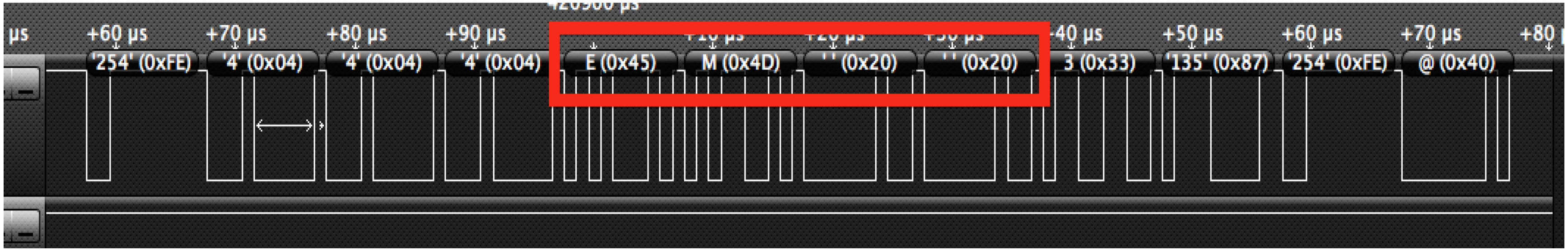


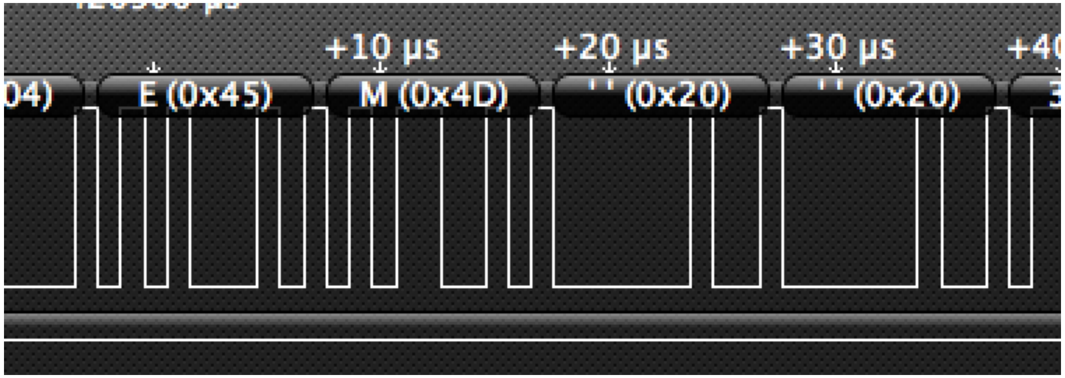
How My Adventures Went



How My Adventures Went

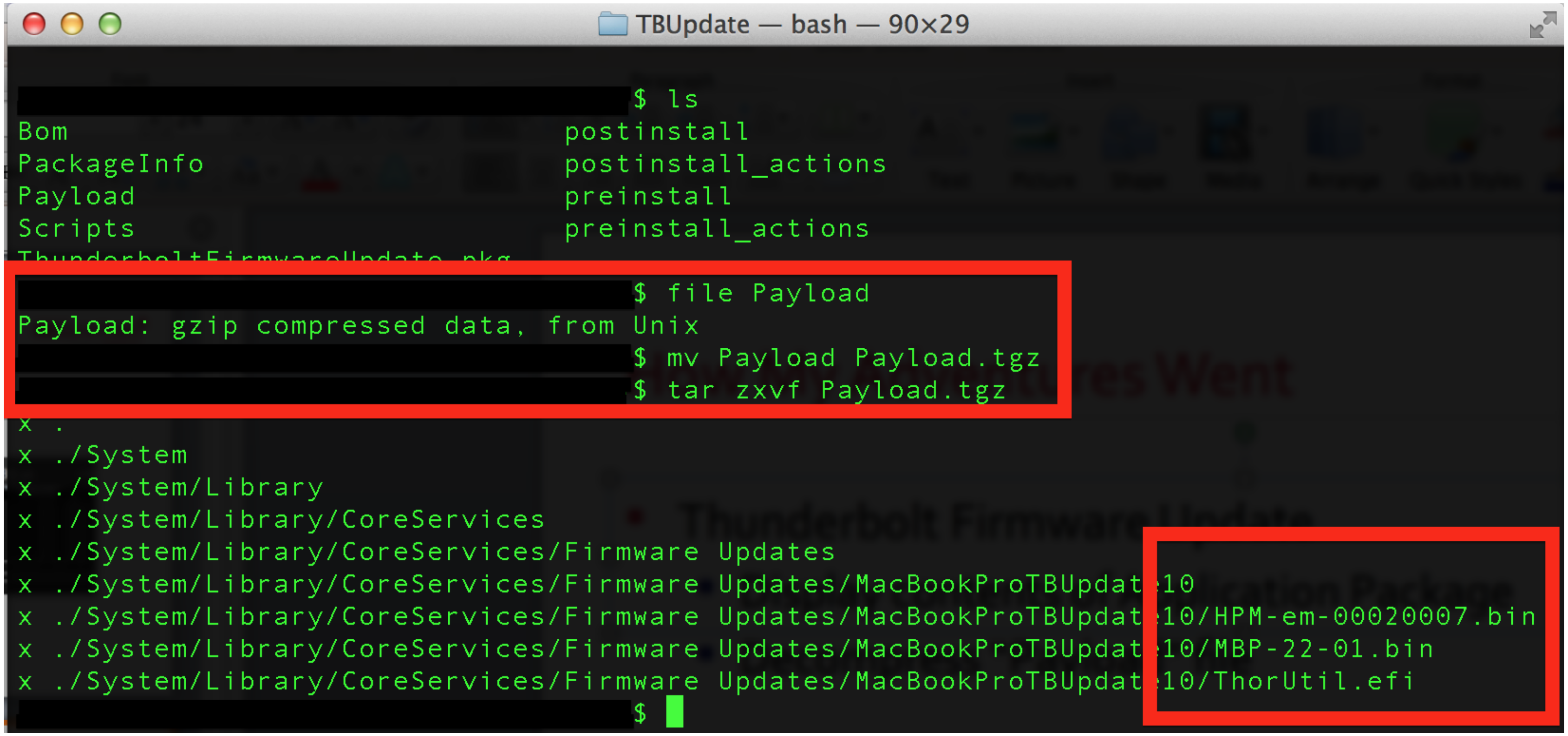
- ARM UART Traffic
  - String “EM “





How My Adventures Went

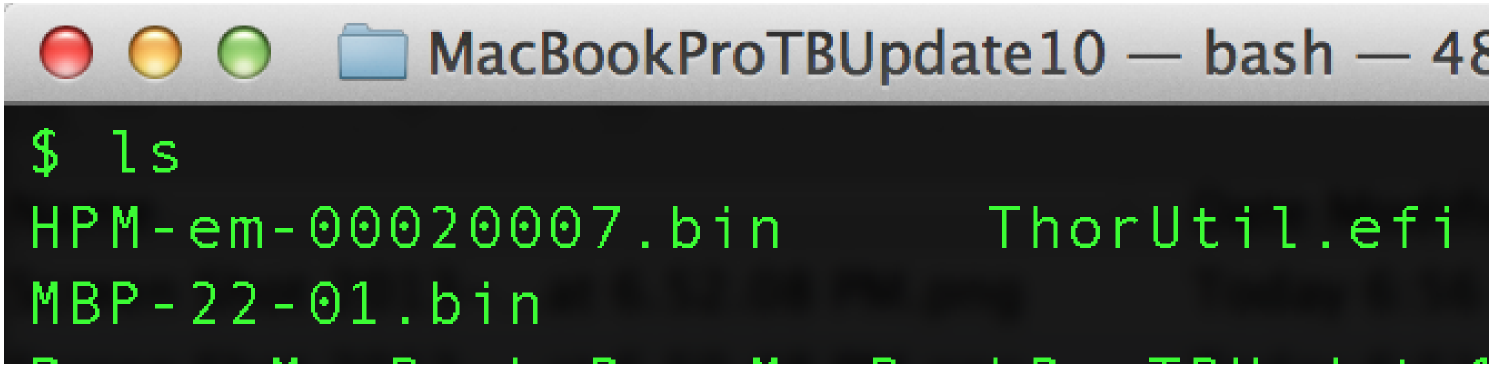
- Thunderbolt Firmware Update
  - Display contents of Application Package
  - Decompress “Payload” file



```
[redacted]$ ls
Bom                              postinstall
PackageInfo                      postinstall_actions
Payload                          preinstall
Scripts                          preinstall_actions
ThunderboltFirmwareUpdate.pkg
[redacted]$ file Payload
Payload: gzip compressed data, from Unix
[redacted]$ mv Payload Payload.tgz
[redacted]$ tar zxvf Payload.tgz
x .
x ./System
x ./System/Library
x ./System/Library/CoreServices
x ./System/Library/CoreServices/Firmware Updates
x ./System/Library/CoreServices/Firmware Updates/MacBookProTBUpdate10
x ./System/Library/CoreServices/Firmware Updates/MacBookProTBUpdate10/HPM-em-00020007.bin
x ./System/Library/CoreServices/Firmware Updates/MacBookProTBUpdate10/MBP-22-01.bin
x ./System/Library/CoreServices/Firmware Updates/MacBookProTBUpdate10/ThorUtil.efi
[redacted]$ 
```

How My Adventures Went

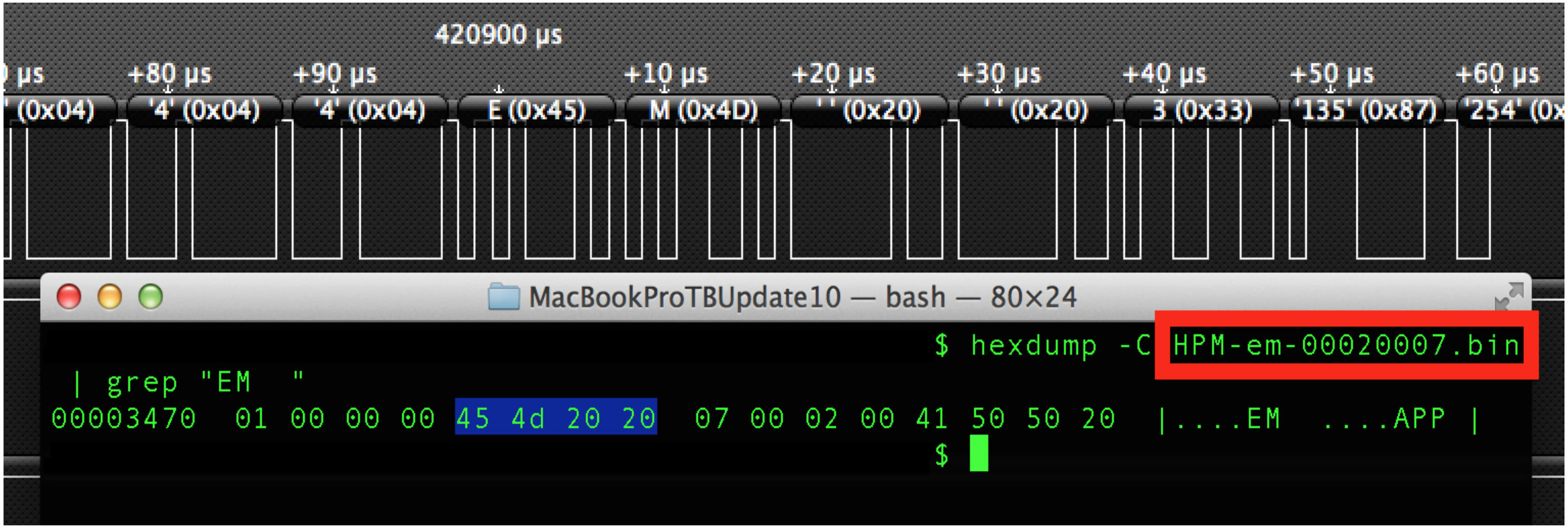
- Two Firmwares for Thunderbolt?
  - One is probably ARM
  - Let's look for string "EM "



```
$ ls
HPM-em-00020007.bin      ThorUtil.efi
MBP-22-01.bin
```

How My Adventures Went

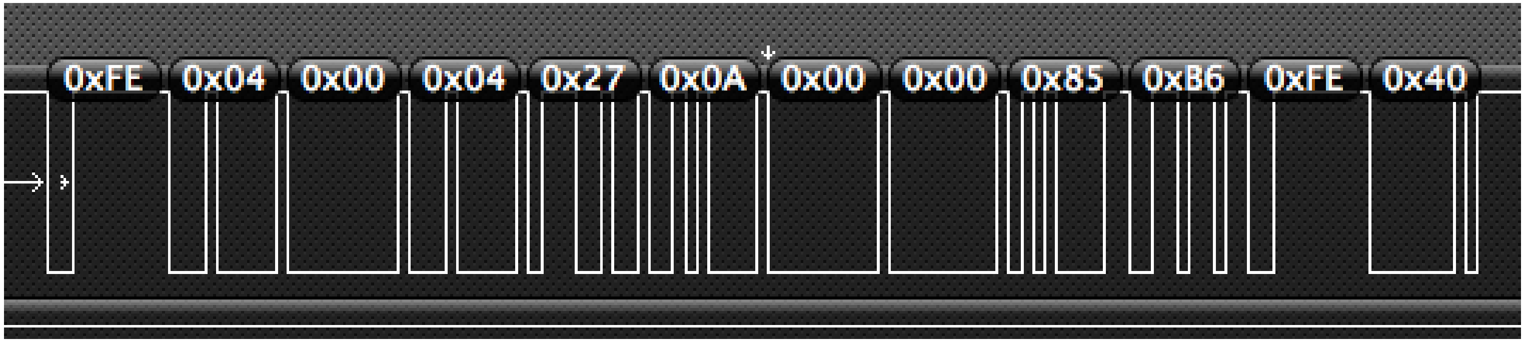
Jackpot!



```
                                                  $ hexdump -C HPM-em-00020007.bin
 | grep "EM  "
00003470  01 00 00 00 45 4d 20 20  07 00 02 00 41 50 50 20  |....EM  ....APP |
                                                  $ 
```

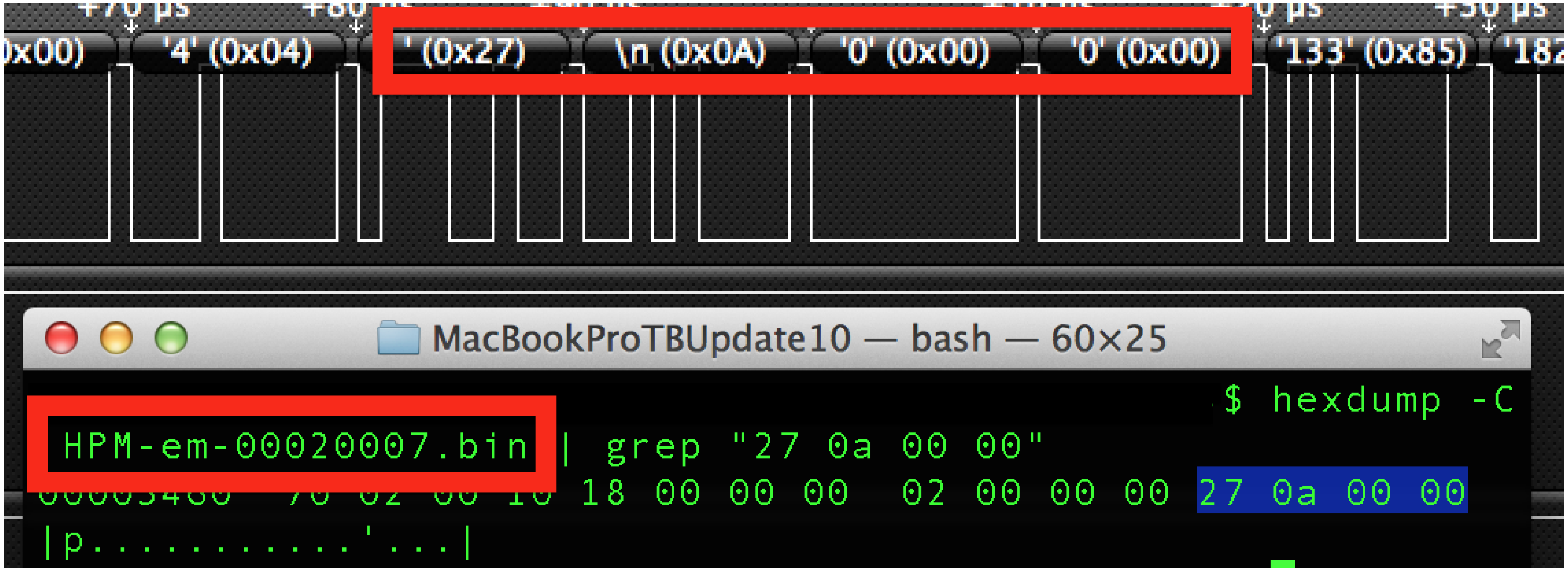
How My Adventures Went

- Round 2…
  - String "\x27\x0a\x00\x00"



How My Adventures Went

Successaroo!



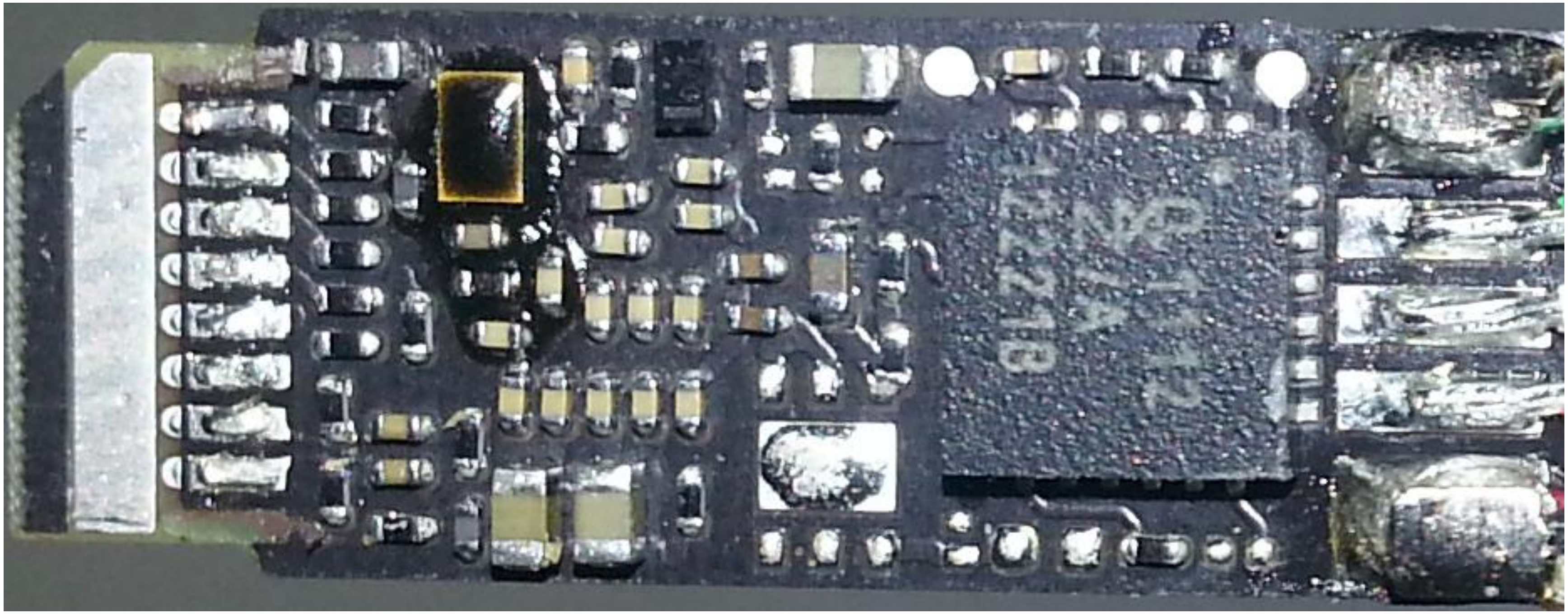
```
                                                $ hexdump -C
HPM-em-00020007.bin | grep "27 0a 00 00"
00003460  70 02 00 10 18 00 00 00  02 00 00 00 27 0a 00 00
|p...........'...|
```

How My Adventures Went

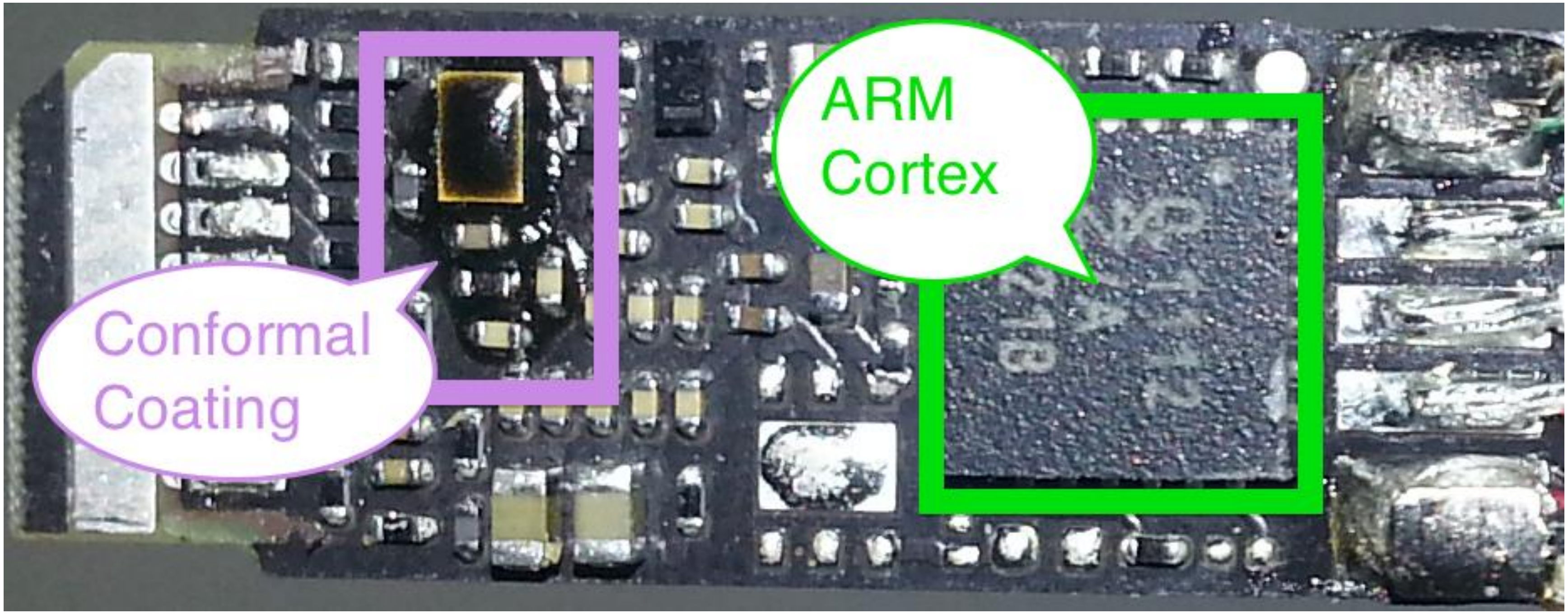
- Gigabit Ethernet Adapter
  - Researching the product
  - Taking it apart
  - Attack vectors

How My Adventures Went

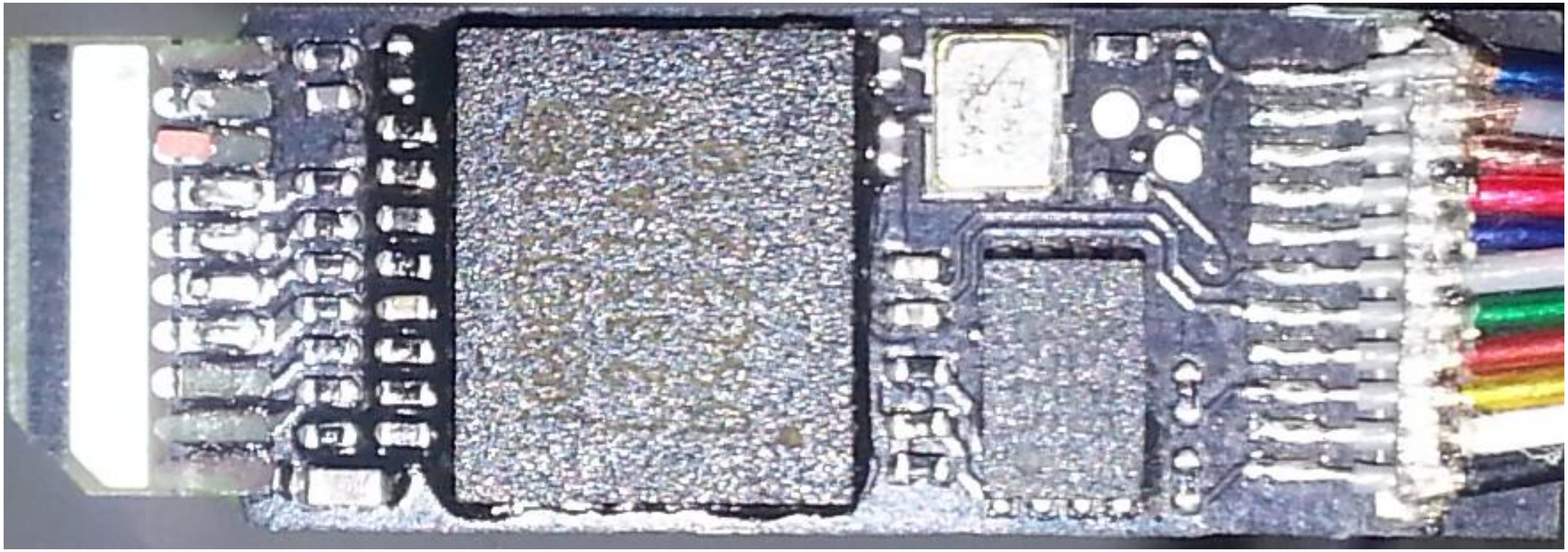
How My Adventures Went



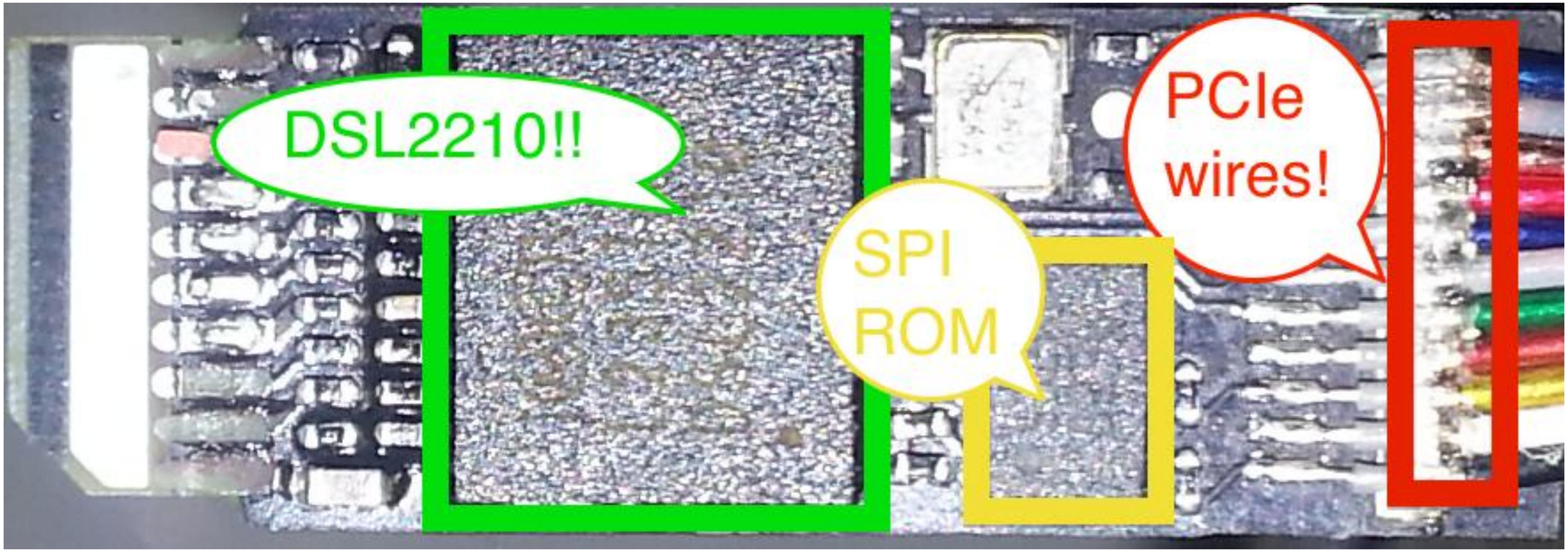
How My Adventures Went



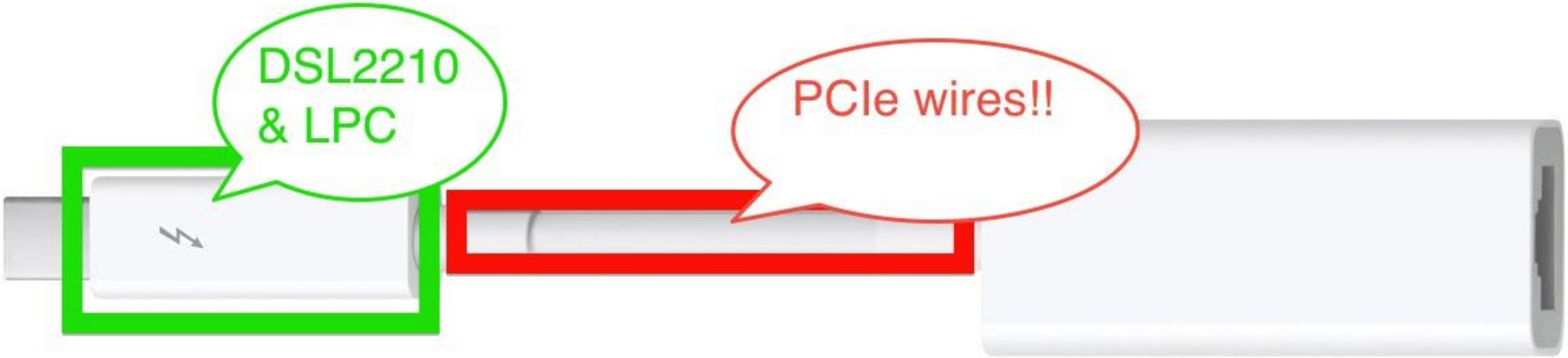
How My Adventures Went



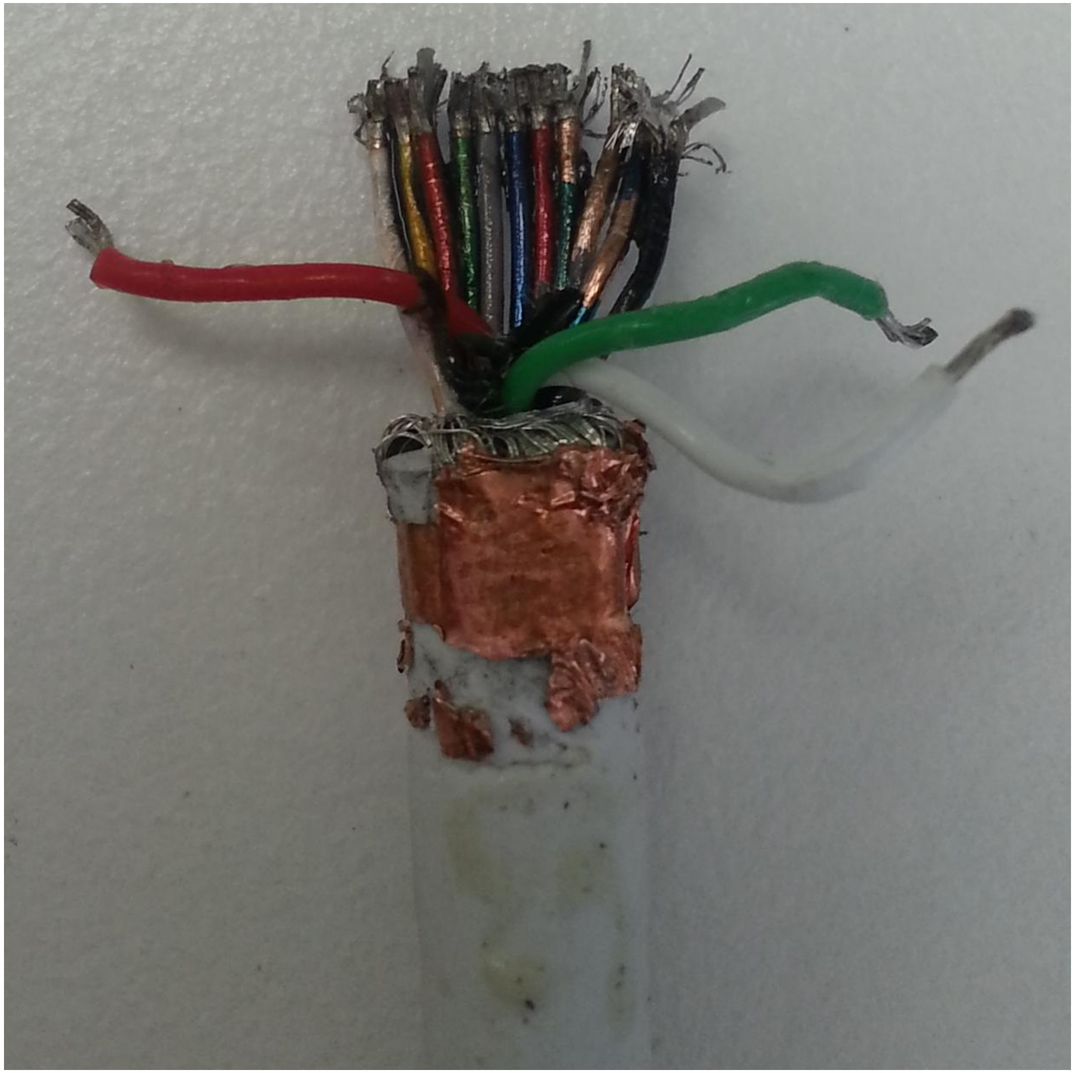
How My Adventures Went



How My Adventures Went



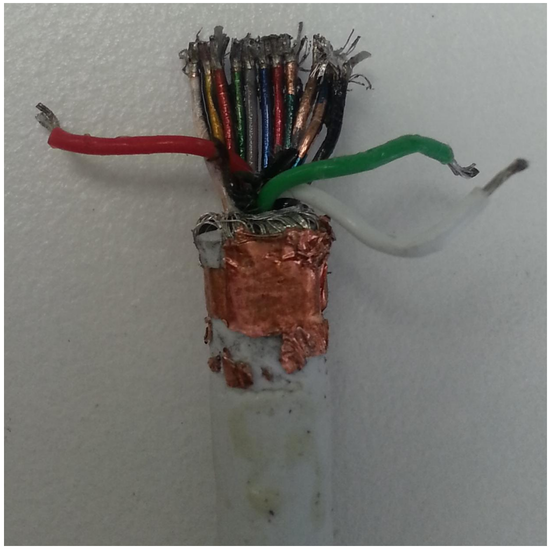
How My Adventures Went



How My Adventures Went

- Altera Cyclone IV GX Transceiver Starter Kit
  - Hard IP for PCIe
  - PCIe x1
  - ~$450

How My Adventures Went



How My Adventures Went

- Tips and Tricks
    - Get A LOT of devices!
    - Heat up everything SLOWLY!
    - Continuity testing WINS
    - Sniff EVERYTHING
    - Read all ROMs/Flashes

Thank You

- Russ Sevinsky
  - Security Consultant at iSEC Partners
  - rsevinsky@isecpartners.com

- Special thanks to:
  - Jesse Burns
  - Everyone @ iSEC Partners

iSECpartners
part of nccgroup

UK Offices

Manchester - Head Office
Cheltenham
Edinburgh
Leatherhead
London
Thame

European Offices

Amsterdam - Netherlands
Munich – Germany
Zurich - Switzerland

North American Offices

San Francisco
Atlanta
New York
Seattle

Australian Offices

Sydney