Hacking Hardware with a $10 SD Card Reader

An Exploitee.rs Production

About Us

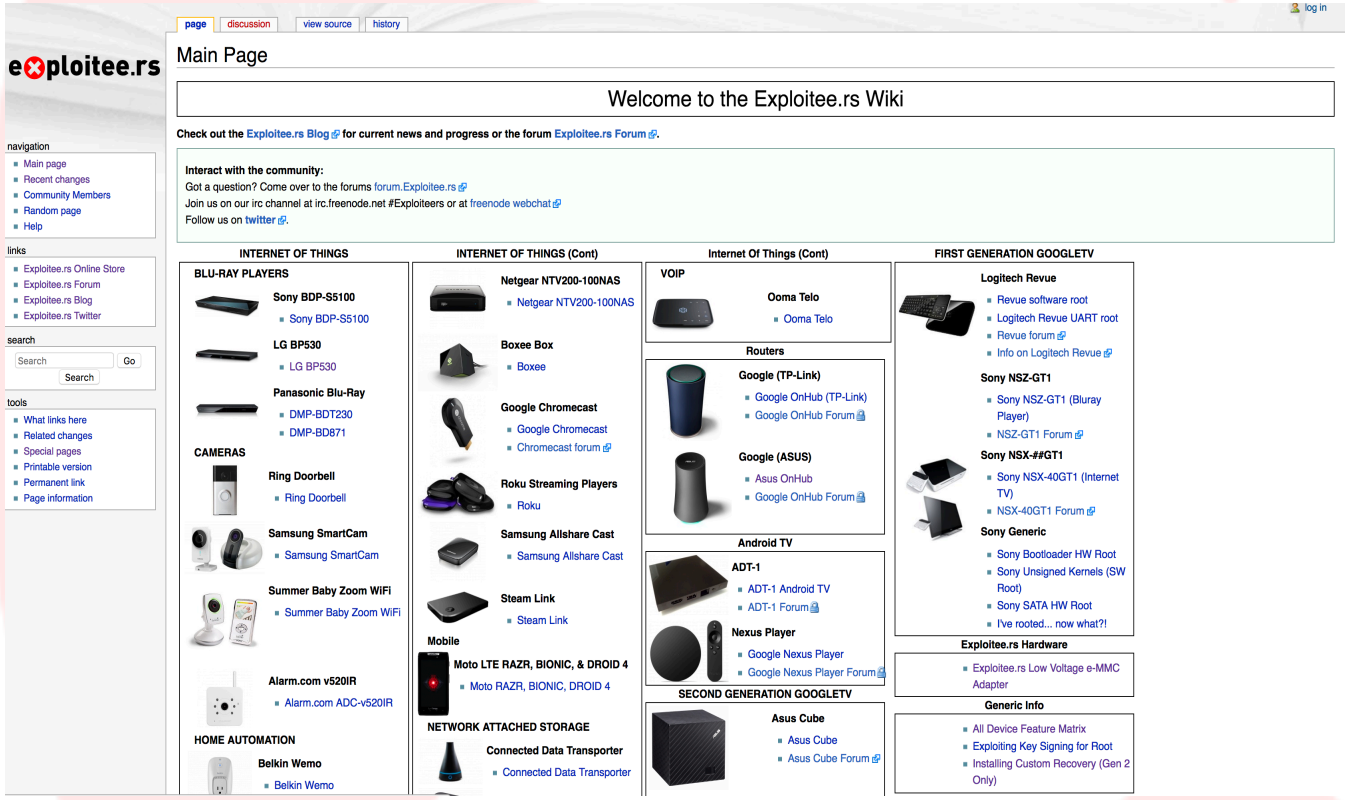
- Amir Etemadieh (@Zenofex) - Senior Research Scientist at Cylance, Founder of Exploitee.rs, Founder of Pastecry.pt
- CJ Heres (@cj_000) - Security Researcher at Draper, does hardware/software exploitation things…
- Khoa Hoang (@maximus64_) – Graduate of the University of Central Florida who is a master of the soldering iron.

Note: This presentation and thoughts are ours, and ours alone, and have no relationship to our employers

Other Exploitee.rs Members

- [mbm] (@mbmwashere) – Co-founder of OpenWRT
- gynophage (@gyno_lbs) – DEF CON CTF organizer
- Hans Nielsen (@n0nst1ck) – “Boring” corp-sec dude
- Jay Freeman (@saurik) – Creator of Cydia
- Tom Dwenger (@tdweng) – Master software developer
- 0x00String (@0x00string) – Hacker, troublemaker extraordinaire

About Exploitee.rs



- The artists formerly known as GTVHacker
- Released root methods for multiple generations of Google TV devices and other embedded systems
- Maintains network of sites documenting vulnerabilities (community and group driven)

What is Covered

- What is eMMC flash & how does it differ from NAND
- How to recognize eMMC flash
- How to identify the eMMC pinout
- Attaching to eMMC flash within an embedded device
- Selecting the correct USB SD Card reader
- Interfacing with eMMC Flash

Prior Work

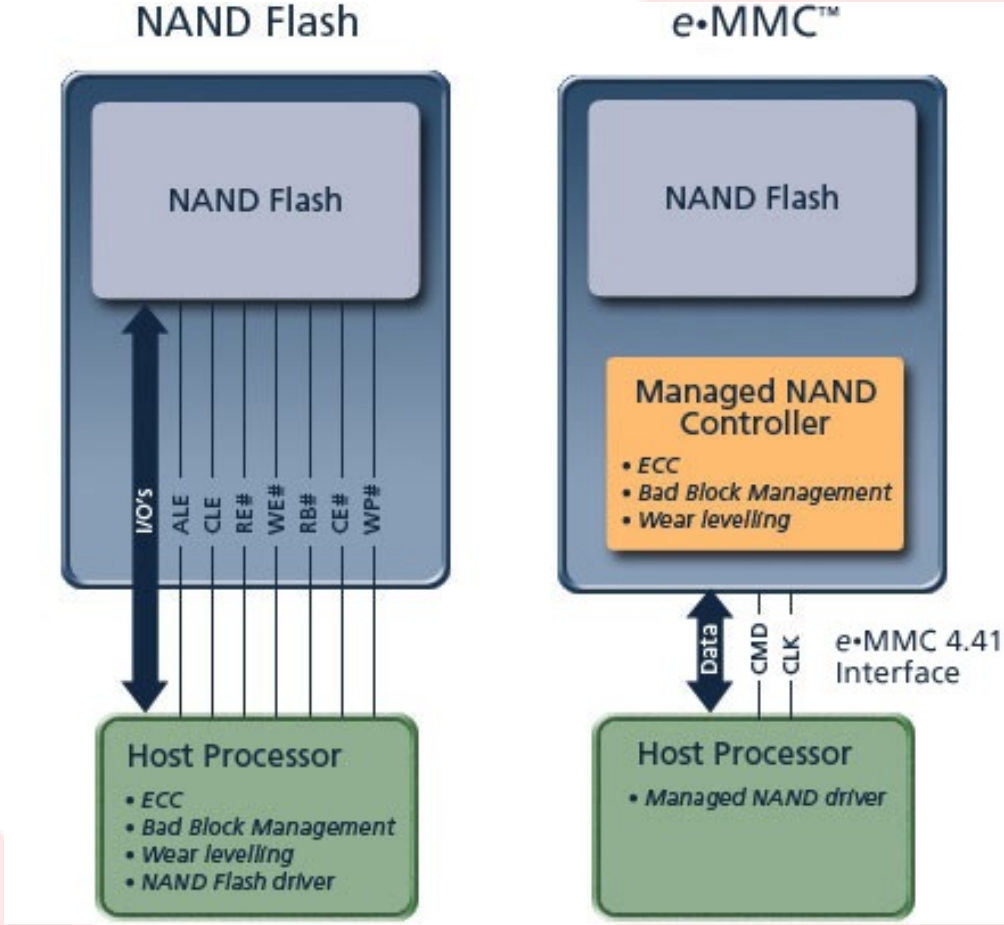
- 2009 – Micah Elizabeth Scott (@scanlime)
  - Built sniffer for Nintendo DSi console to monitor flash reads/writes
- 2012/2013 – Exploitee.rs
  - Presented eMMC root methods at DEF CON 21
    - since then have developed a systemic approach and low-cost tools to simplify the process
- Among many others online

Introduction to eMMC Flash

- Embedded Multi-Media Card (eMMC)
  - Embedded version of MMC (similar to an SD card)
- Inside of millions of devices
  - Phones, STBs, Tablets, Automobiles
- Developed by the Joint Electron Device Engineering Council – JEDEC
  - Currently at revision 5.1

eMMC vs. NAND

- eMMC is a flash storage type with an internal controller
  - Internal controller handles wear leveling, bad block management, and Error-Correcting Code (ECC)
- eMMC provides simpler interface for developers to incorporate within designs
- NAND requires 8 data lines and 5 control lines
  - eMMC can use 1 data lines and 2 control lines



Prevalence

- 2014 NXP Presentation estimated 4.375 Billion 16GB eMMC chips in the world
- Samsung Galaxy S to S5 mobile phones all use eMMC Flash storage
  - Sold over 110 Million devices alone, for ONE device line
- Low cost, many storage sizes, small single package footprint, integrated controller

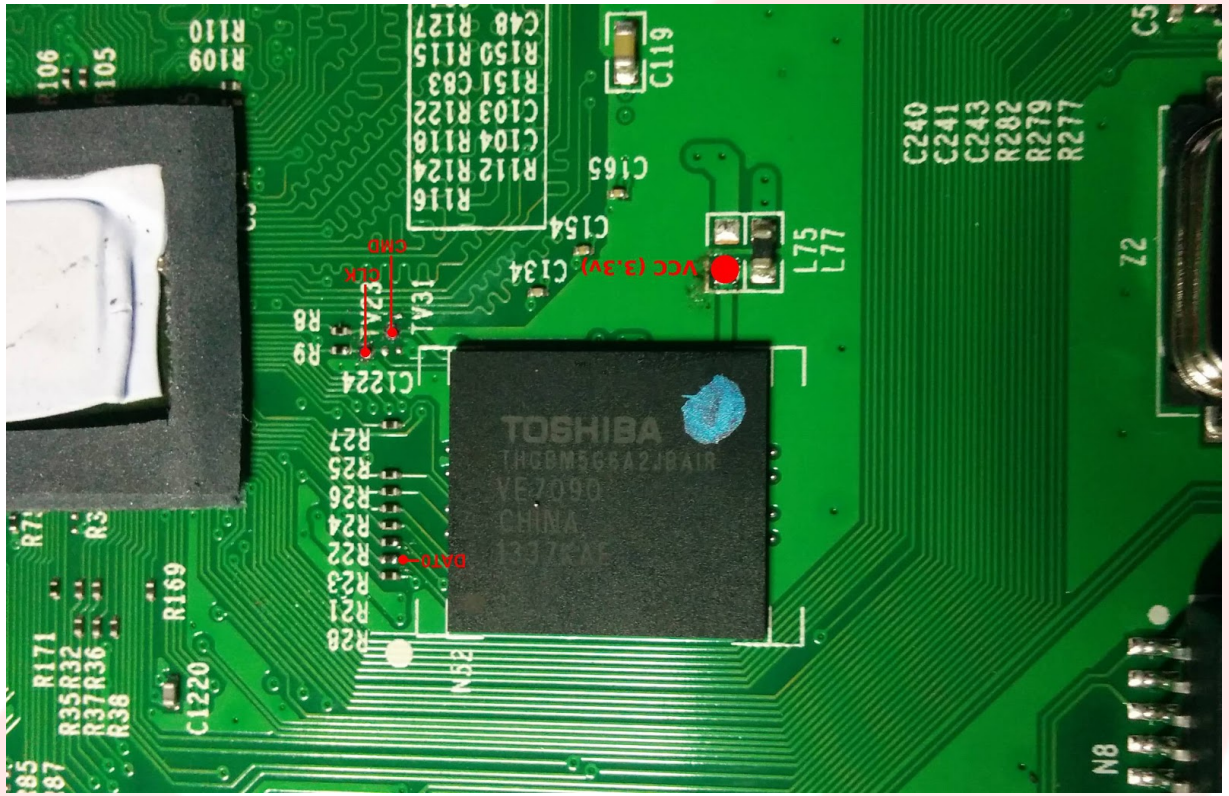
Identifying eMMC Flash

Multiple items can be used to identify an eMMC flash Chip and pinout.

- Location on board (relative to SoC)
- Standardized Package type (BGA)
- Chip markings and silk screening
- PCB traces and resistors

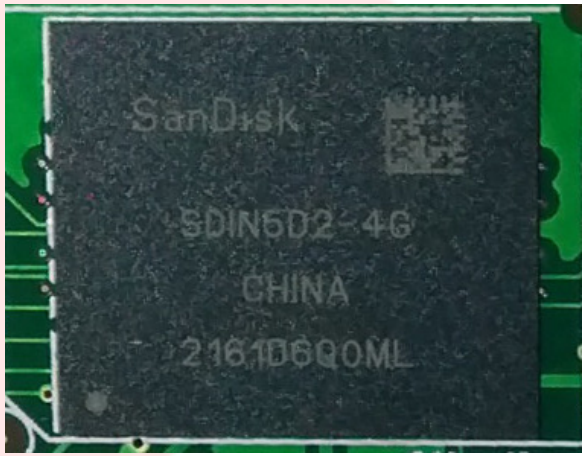
Location on Board

- Most devices feature a System on Chip (SoC)
  - Main CPU
  - I/O Interfaces
  - Memory Controller
- RAM Chips
- Flash Memory
  - eMMC flash
  - NAND flash
  - NOR, SPI, etc…
- Look for BGA Packages near SoC



Common Flash Packages

Ball Grid Array (BGA)



Standard Package for eMMC

Thin Small Outline Package (TSOP)

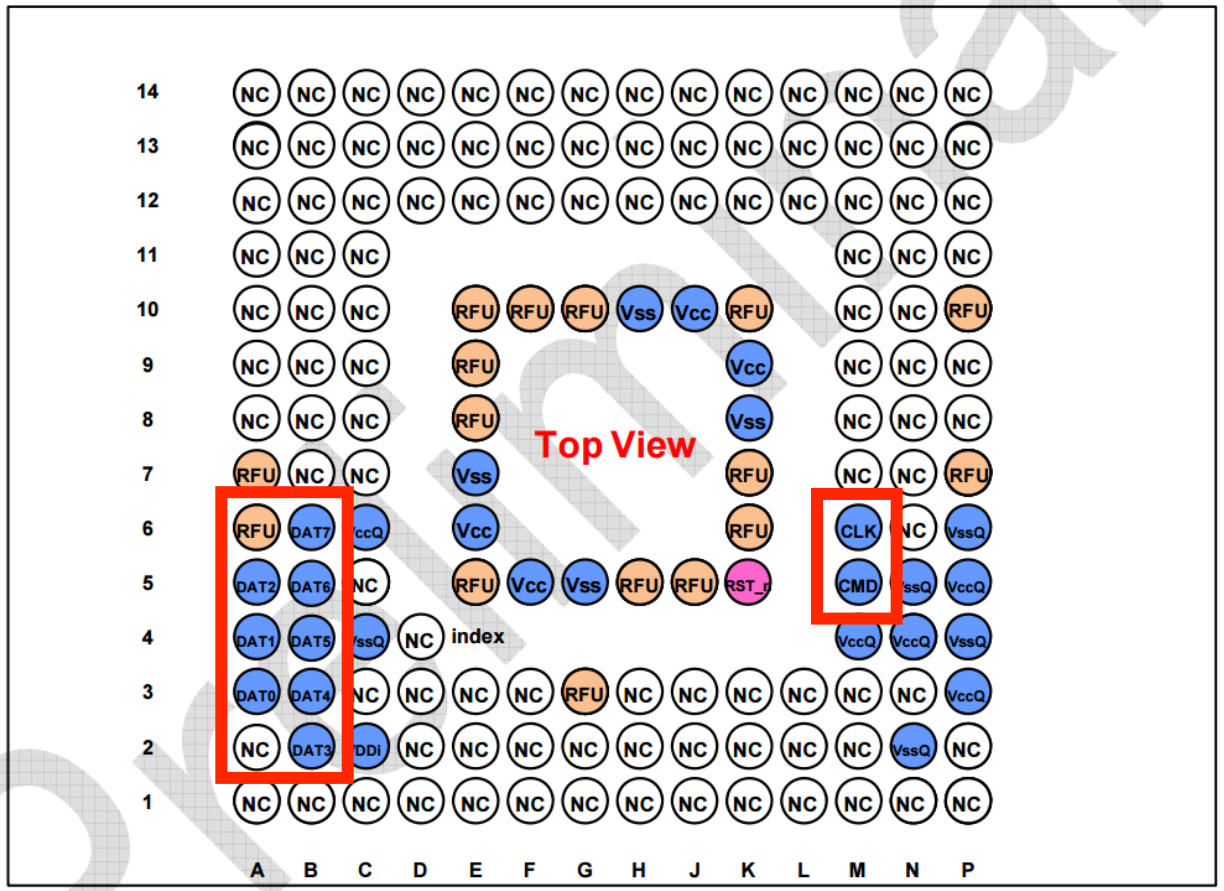
Typically used for Parallel, NAND, or NOR

eMMC Chip Identification

- Manufacturer: Toshiba
- Part Number: THGBM5G6A2JBAIR
- Internet Search for Part #
  - "THGBM5G6A2JBAIR is 8-GByte density of e-MMC Module product"
  - Also a full datasheet
- In some cases a datasheet may not be available

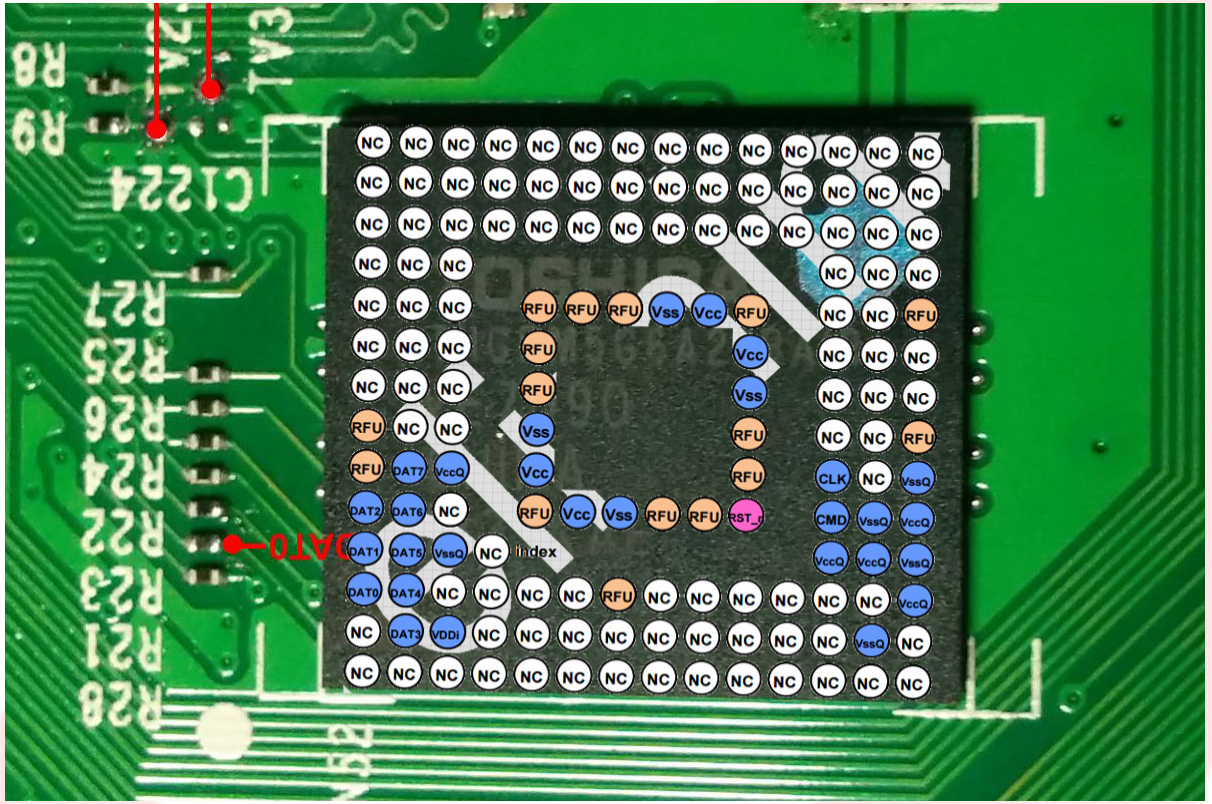
Visually Identifying Pads

- eMMC Flash Datasheet - Toshiba THGBM5G6A2JBAIR
- Left side of the chip
  - DATA pads
- Right side of the chip
  - CMD/CLK pads
- The white pads? N/C
  - Flash has a large footprint
  - Some reserved for future use



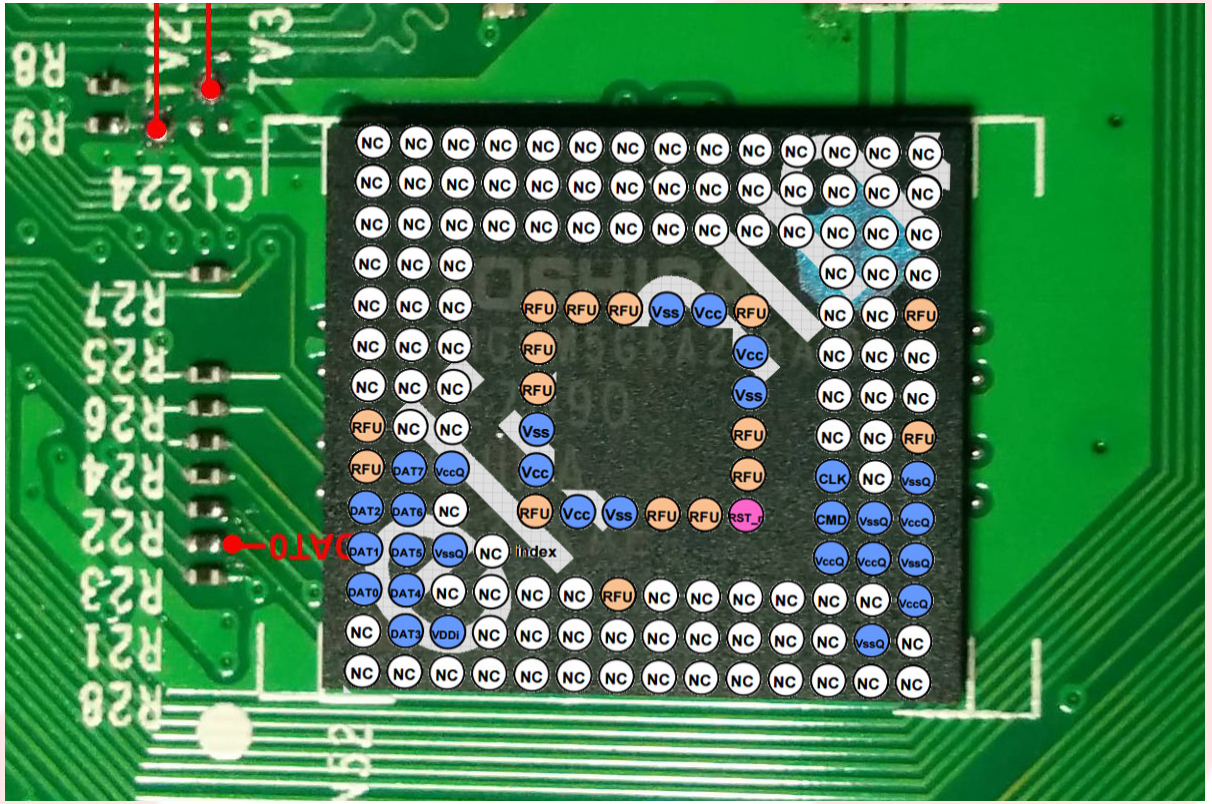
Finding In-Circuit eMMC Pinouts

- Overlay pads onto image of chip
- Note the left (DAT#) blue pads
  - These are DATA lines
- Note all of the resistors
  - Connected to DATA lines



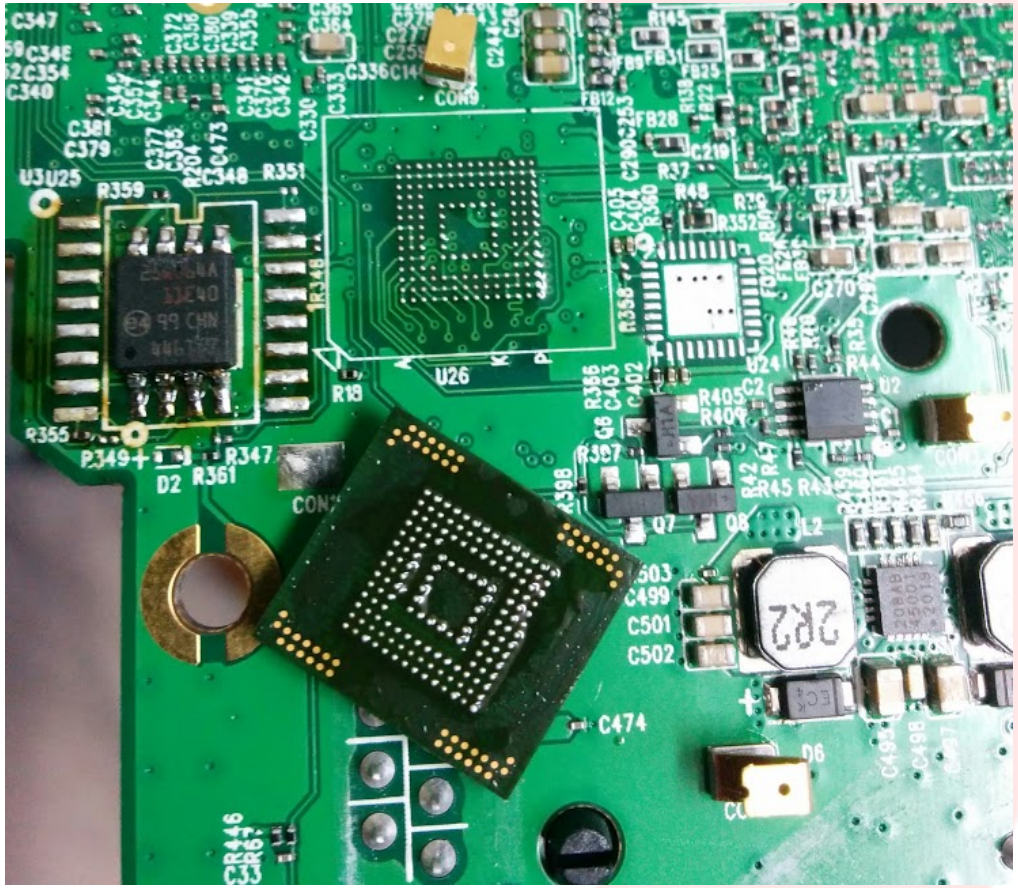
Finding In-Circuit eMMC Pinouts

- Silk screened R21 to R28
  - R21 == DAT0
  - R22 == DAT1
- CMD/CLK - lower right of chip
  - Lines must connect to the SoC
- What are R8 and R9?
  - CMD and CLK



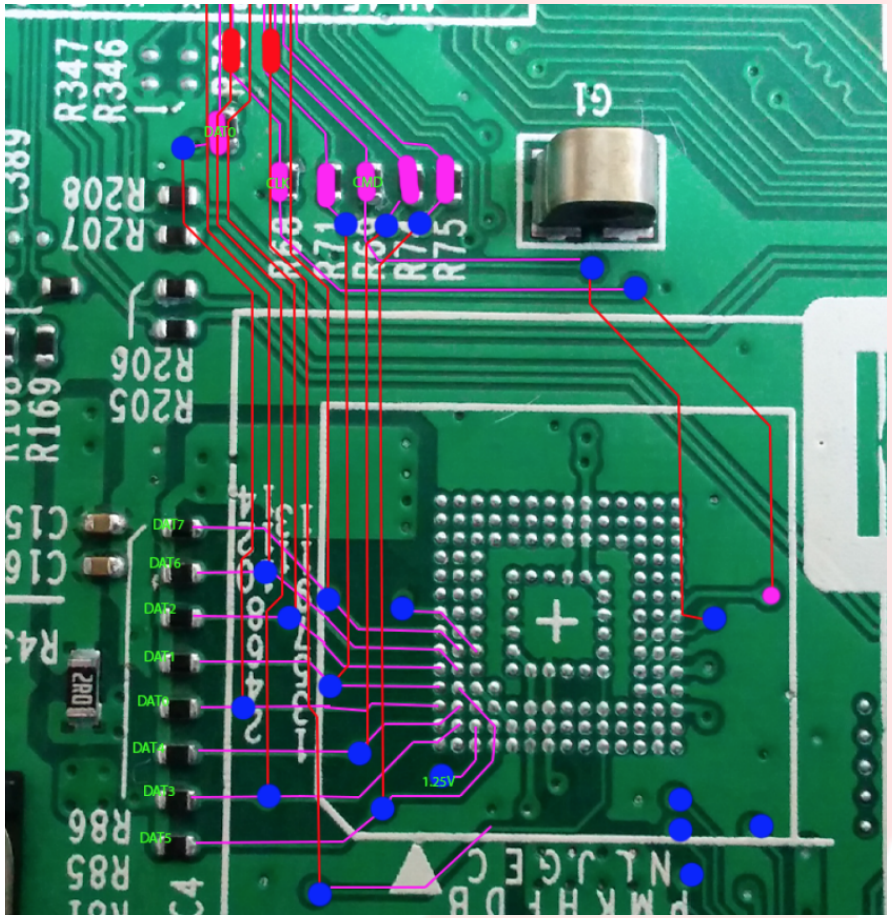
Removing BGA Flash

- May need to remove eMMC to trace the pinout
- Requires rework station
  - Or a cheap hot air gun
- Also Requires
  - Tweezers
  - Soldering Flux
  - Patience



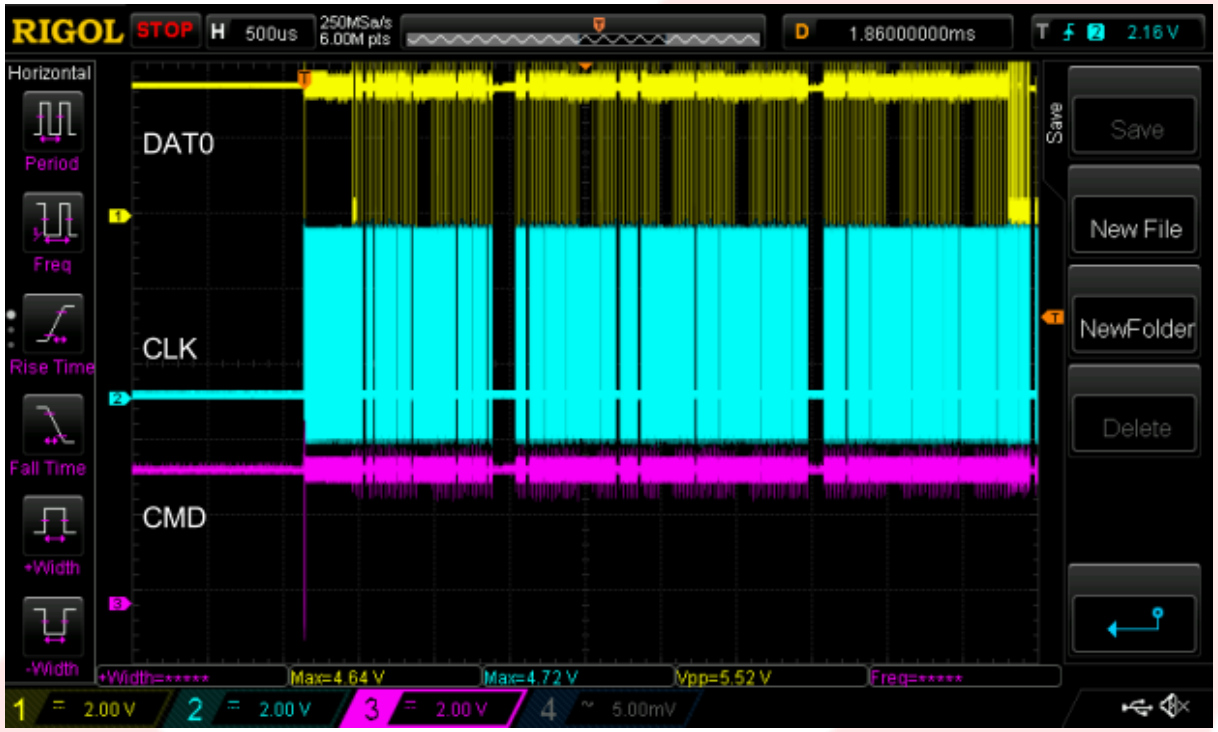
Pull and Trace

- Remove flash
  - Warm the board, add flux, bump the flash gently, when ready lift off cleanly
- Trace each pad out to alternate points visually or with multi-meter
- Can then re-solder the eMMC chip
  - May need to reball
- Risk destroying hardware
  - Leverage the information for in-circuit programming



Signal Identification With a Scope

- Guess and check works well, but may cause damage
- Test passively with oscilloscope
- Easier than removing the chip
  - Note: DAT0, CLK, CMD
- DAT0 may take a bit of searching



Clock Signal

- Clock is an oscillating signal
  - Provides for a consistent, repetitive, steady signal
- Clock signal usually looks like a sine wave
- Clock signal is used to synchronize the Data and Command signals

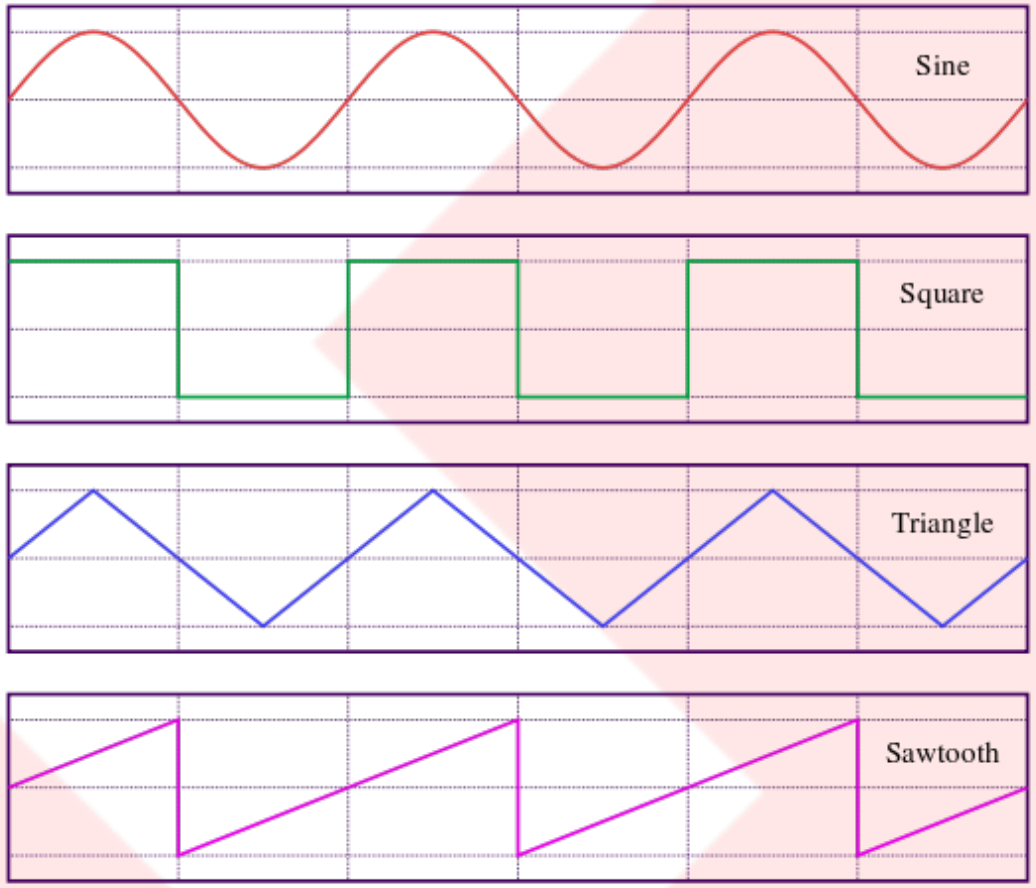
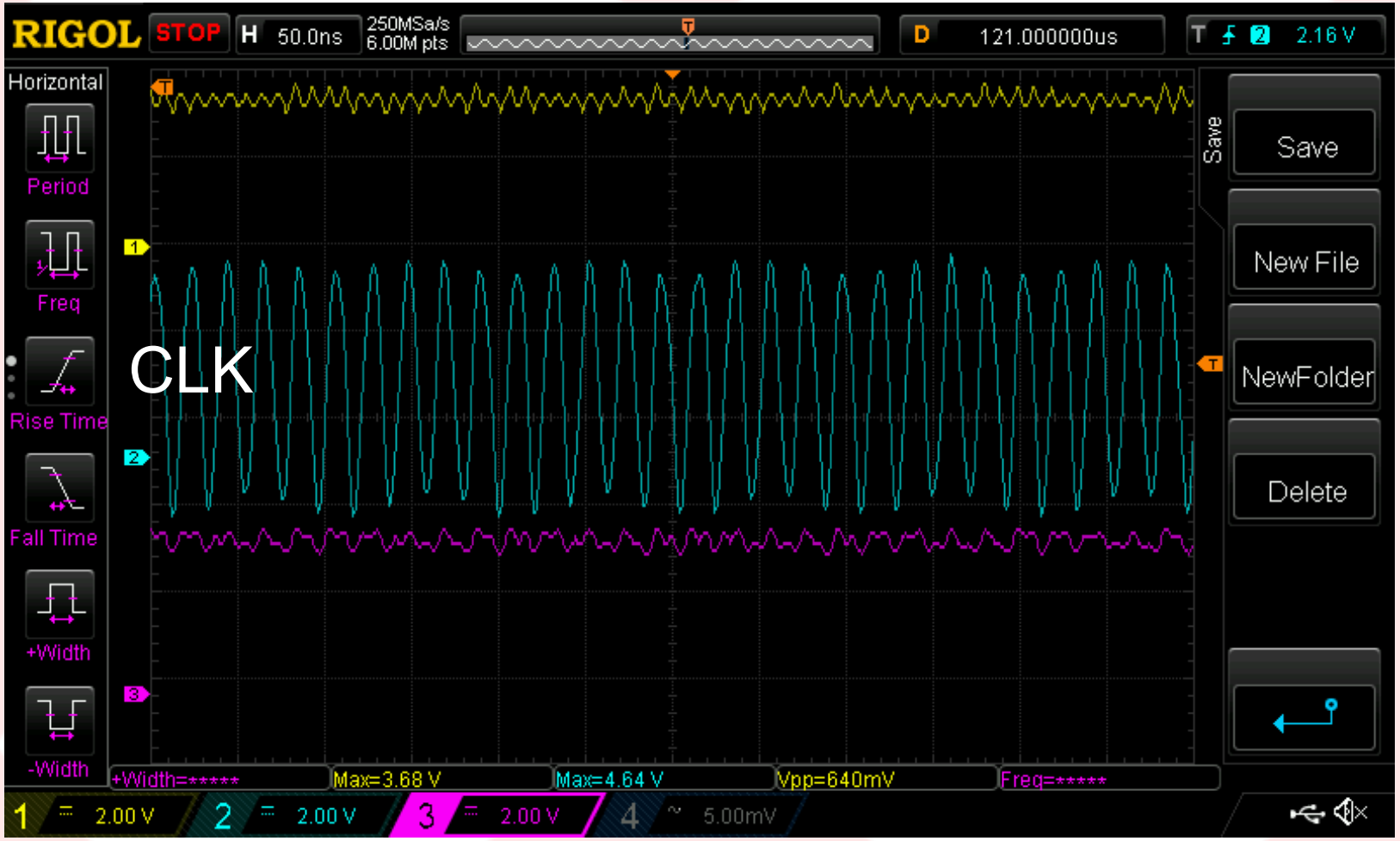
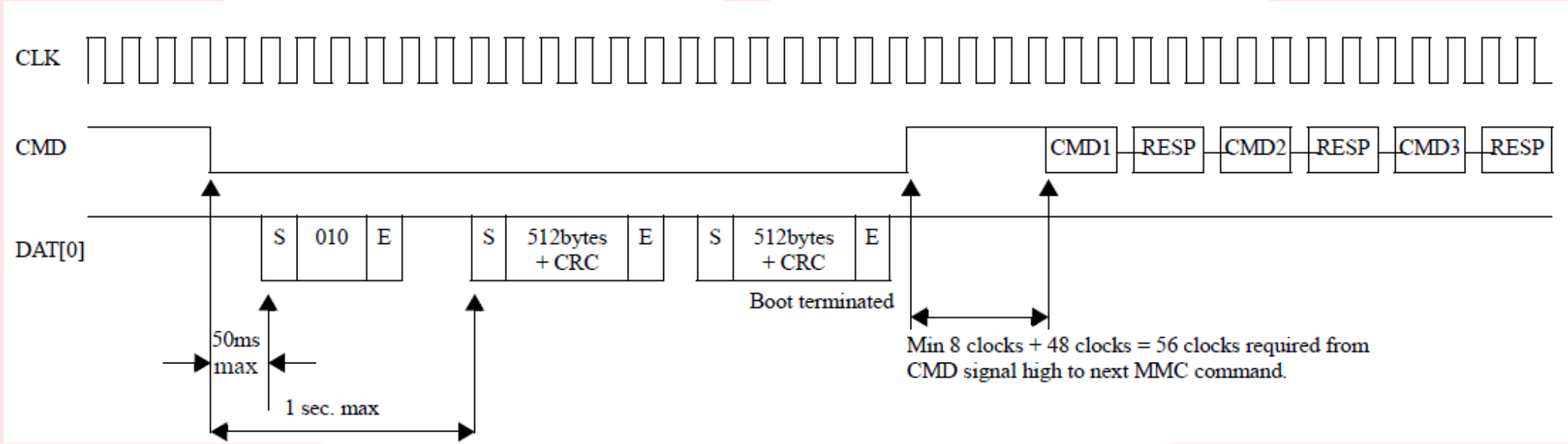


Image via: https://en.wikipedia.org/wiki/File:Waveforms.svg

CLK Signal

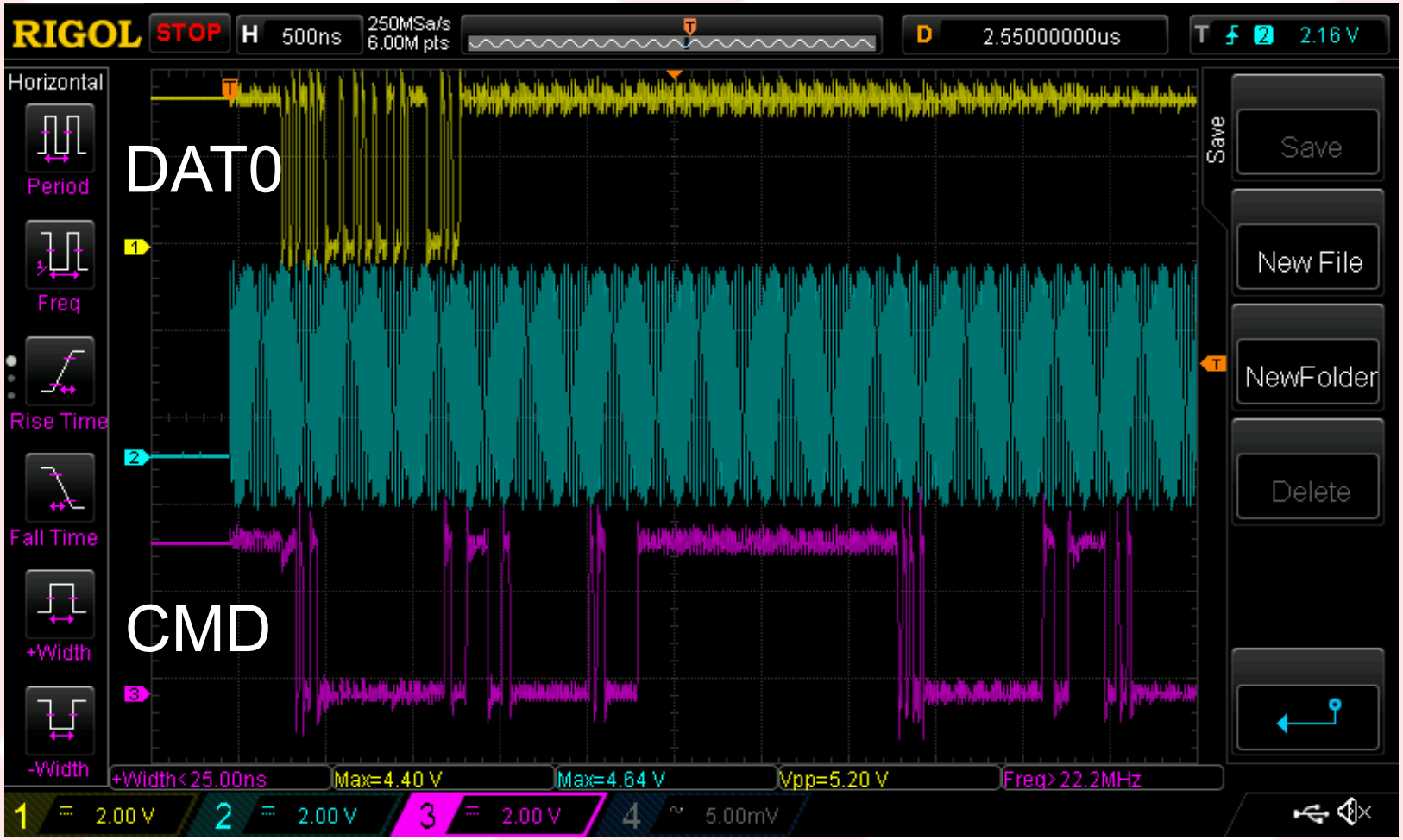

RIGOL
STOP
H 50.0ns
250MSa/s
6.00M pts
D 121.000000us
T 2 2.16 V
Horizontal
Period
Freq
Rise Time
Fall Time
+Width
-Width
CLK
Save
Save
New File
NewFolder
Delete
+Width=*****
Max=3.68 V
Max=4.64 V
Vpp=640mV
Freq=*****
1 2.00 V
2 2.00 V
3 2.00 V
4 5.00mV

Command Signal



- Commands come across the CMD line in bursts
  - Generally Corresponding with data reads and writes
- Bi-Directional communication

CMD Signal


RIGOL
STOP
H 500ns
250MSa/s
6.00M pts
D 2.55000000us
T 2 2.16 V
Horizontal
Period
Freq
Rise Time
Fall Time
+Width
-Width
DAT0
CMD
Save
Save
New File
NewFolder
Delete
+Width<25.00ns
Max=4.40 V
Max=4.64 V
Vpp=5.20 V
Freq>22.2MHz
1 2.00 V
2 2.00 V
3 2.00 V
4 5.00mV

Accessing the eMMC Flash

- Now that the possible pads have been identified, the process of verifying the pinout may require some repetition

- At minimum, need to confirm possible lines for:
  - DAT0
  - CMD
  - CLK

Each device is different however testing will confirm identity

Leveraging SD to Access eMMC

The SD card protocol is a superset of the MMC protocol

Features multiple transmission modes:

- 1-Bit Mode: Fewer wires, easier to connect to
- 4-Bit Mode (SD Max): 4 data lines, faster throughput than 1-Bit
- 8-Bit Mode: Only eMMC has all 8 data lines, fastest throughput

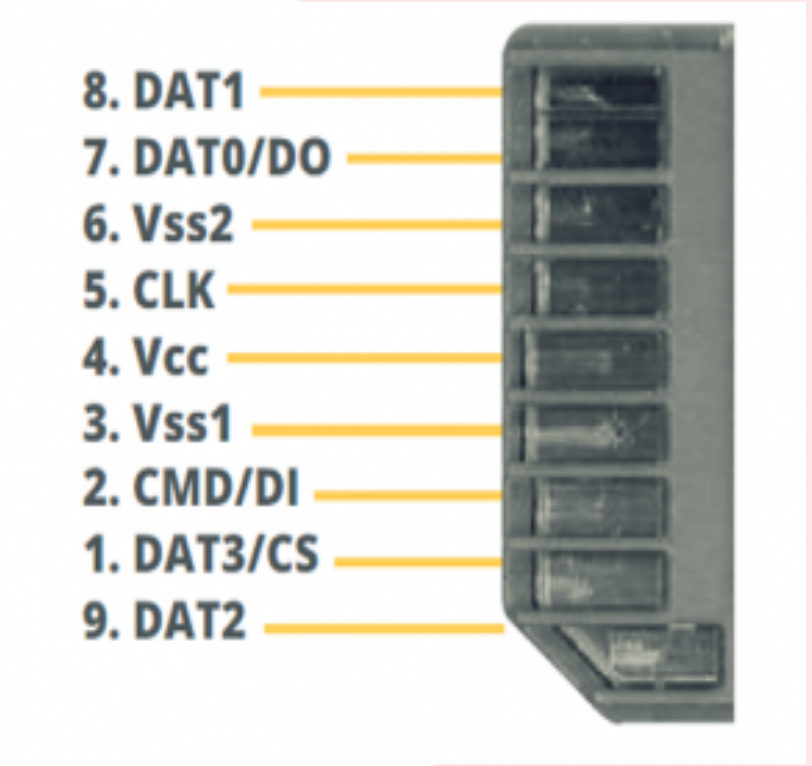
- DAT0, CMD, CLK, Power, Ground – all that's needed

Leveraging SD to Access eMMC

- Conveniently maps to card readers that supports 1-Bit Mode

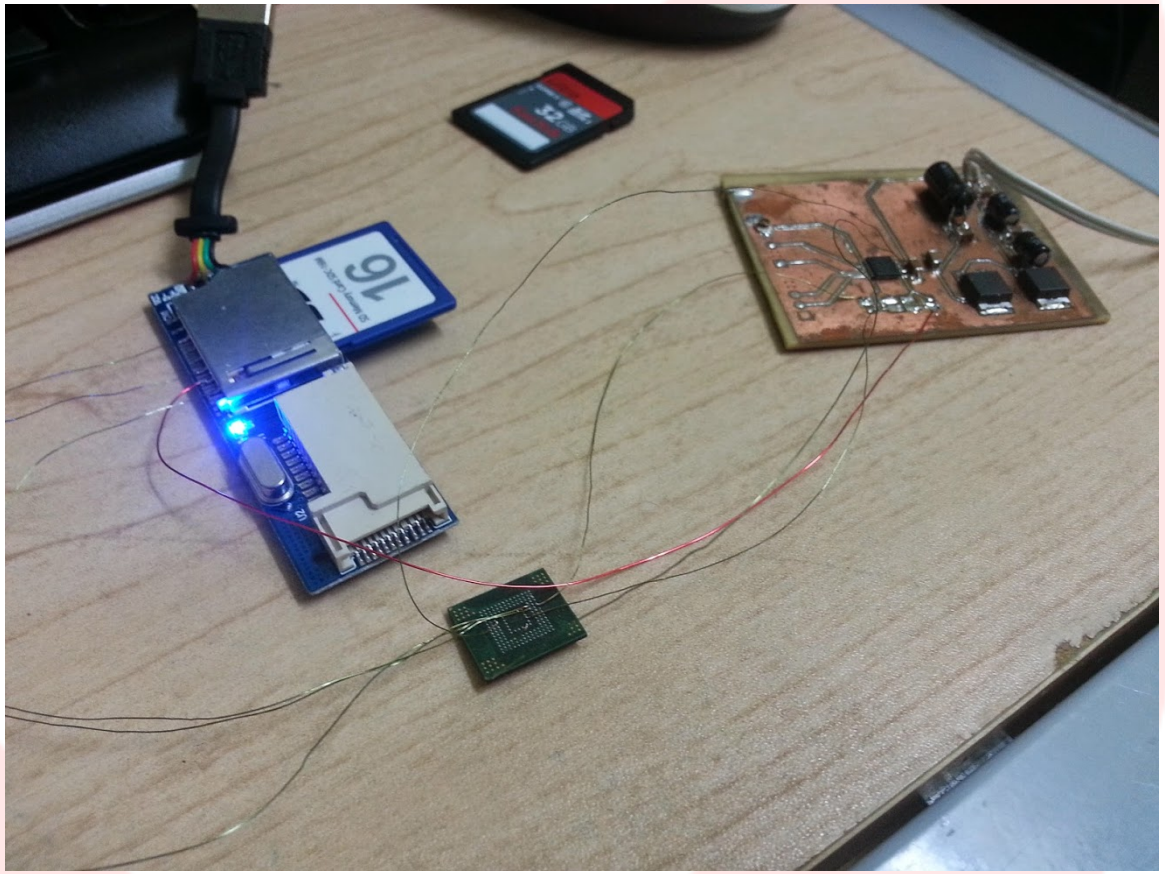
- Test support for 1-Bit mode:
  - Cover DAT1 to DAT3 pins of an SD card
  - Keep the rest exposed
  - Plug to SD card reader, see if it works

- Preferred Adapter
  - Transcend RDF5 USB 3.0 Reader
    - Supports 1-Bit mode

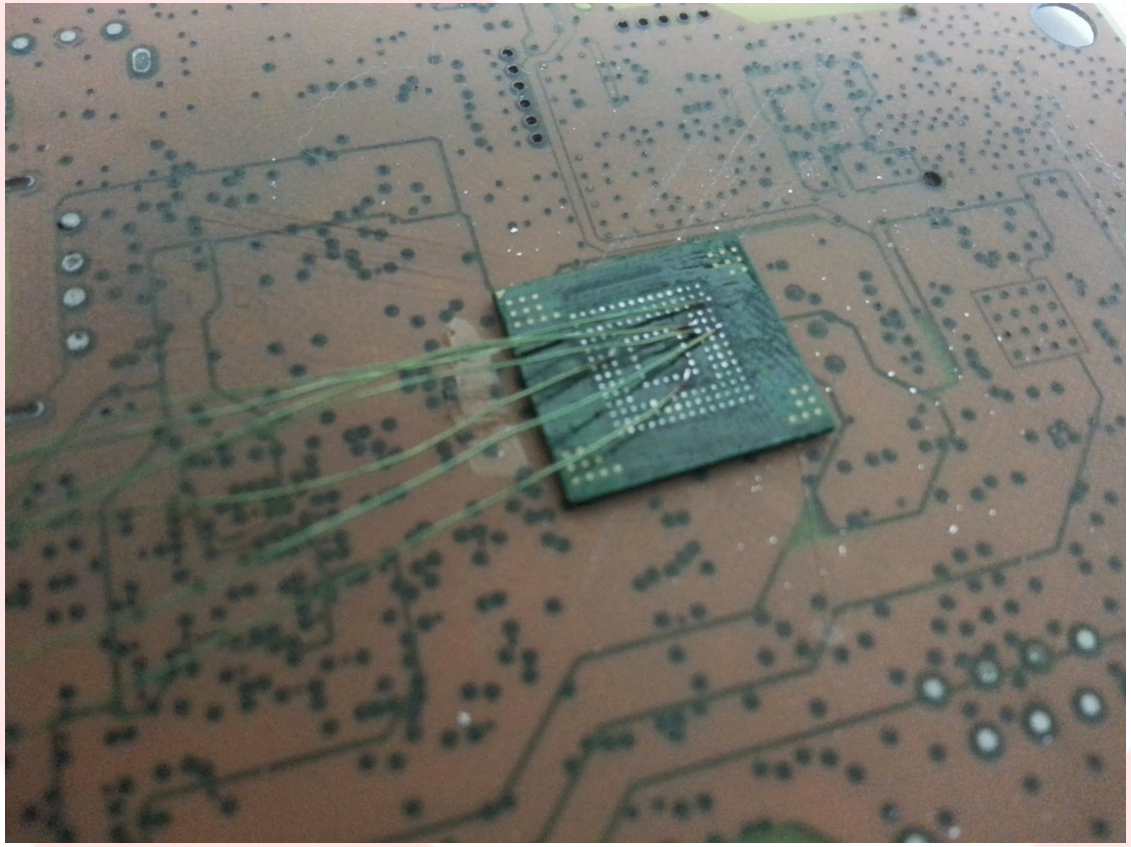


Connecting to eMMC Flash

- In-Circuit
  - With system power
  - Powered externally
- Dead Bug
  - Pulling the chip, soldering to it
- Each method has its own issues
  - Dead bugging can be a challenge



Dead Bug

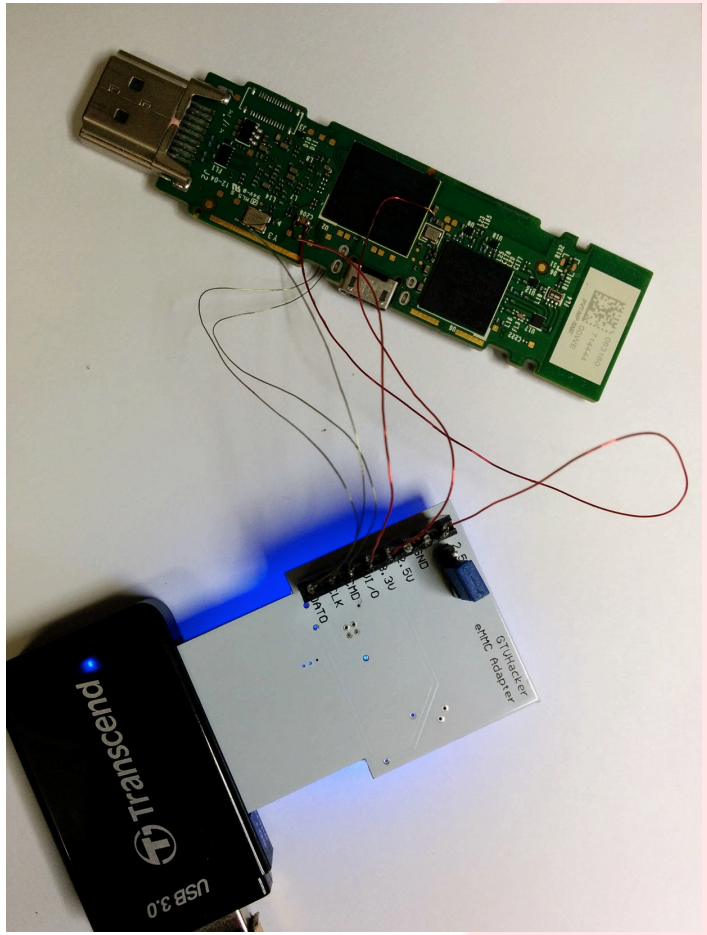


- Looks like a dead bug
  - On its back, wires in the air
- Removing a BGA flash chip
  - Effective, but it is difficult
  - Use as a worst-case scenario
- To reattach, requires reballing

In-Circuit

- CPU may attempt to communicate with the EMMC

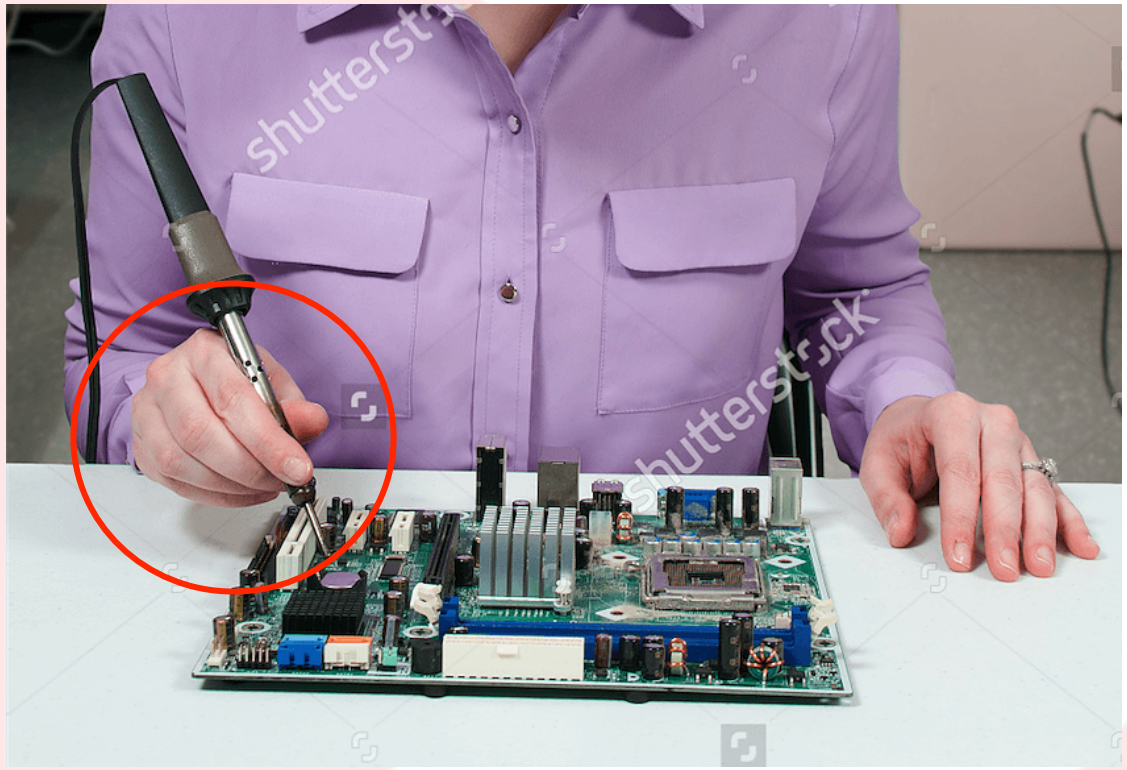
- To Prevent, need one of the following.
  - Hold CPU in Reset
  - Disconnect CMD / CLK line
  - Remove CPU clock oscillator



In-Circuit – Logic Level

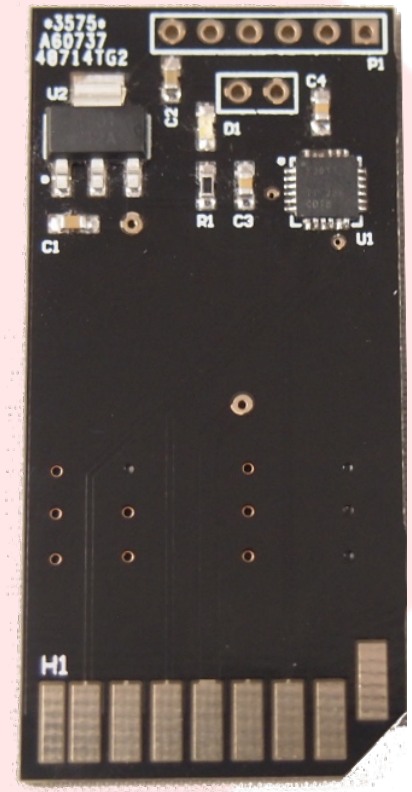
- eMMC may be at a 1.8v logic level (VCCQ connected to the 1.8v rail, sets I/O voltage), SD readers operate at 3.3v
- Can't change eMMC logic level to 3.3v in-circuit
  - Not without the risk of blowing other chips on same power rail
- Use a low voltage adapter, convert 3.3v signals into 1.8v!

Troubleshooting



- Important considerations
  - A good ground connection is needed
  - Length of wires can impact connection
  - Logic level must be known to properly communicate
  - Ensure good connections to all points and a clean power source

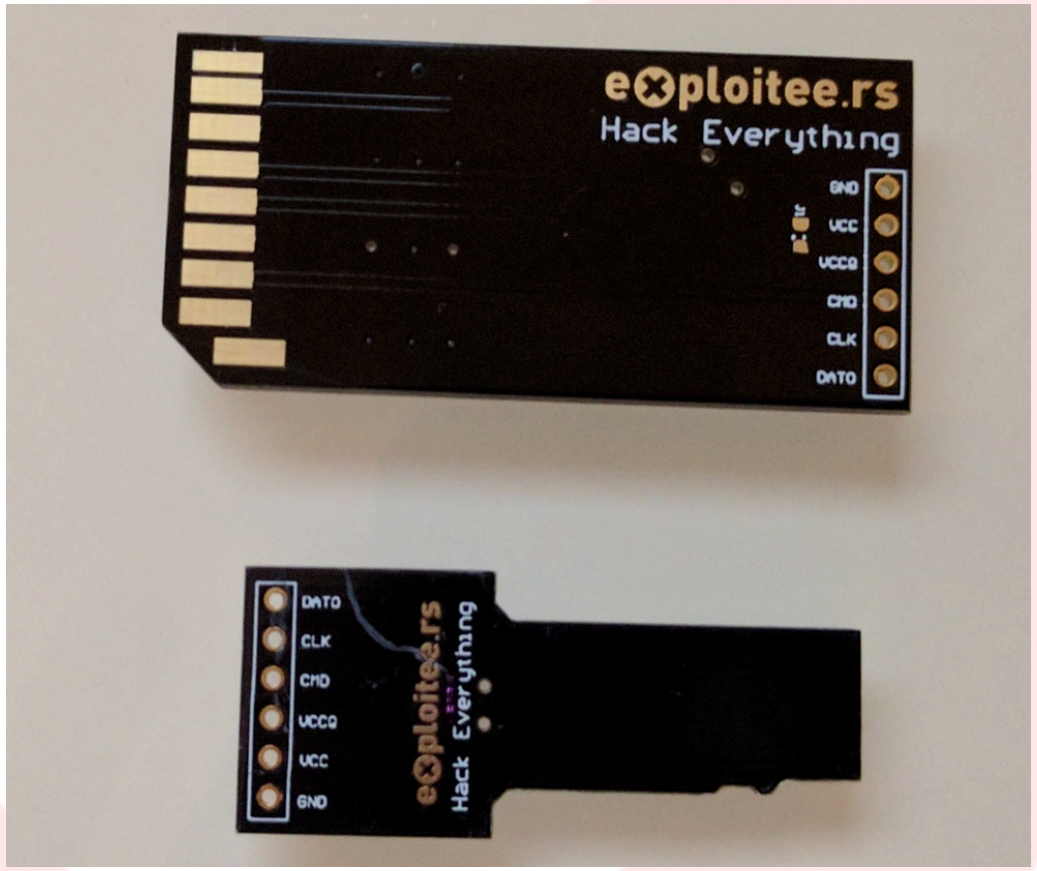
Low Voltage eMMC Adapter



- Converts 3.3v SD card reader signals to 1.8v
  - Utilizes TI TXS02612 Voltage Level Translator
- Open source schematics and boards are available at exploitee.rs

Micro SD & SD eMMC Breakouts

- For use with eMMC flash that utilizes 3.3v in-circuit logic
  - Can also be used to dead bug
- Utilizes SD Card and Micro SD form factor to break out pin headers for SD Card readers
- No components needed - completely passive break out board

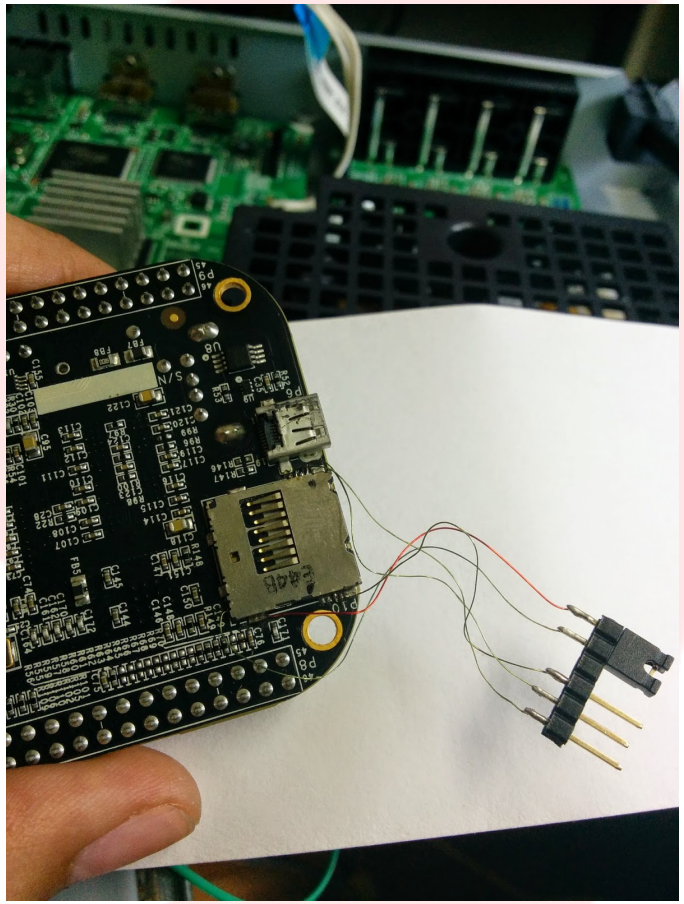


eMMC Boot Partitions

- eMMC chips also have boot partitions
- You can't access the boot partitions with an SD card reader
  - The controller on SD reader doesn't support eMMC boot mode.
- Utilizing a SDIO controller, the eMMC boot partitions are visible
  - /dev/mmcblk0boot0
  - /dev/mmcblk0boot1

eMMC Boot Partitions

- Some laptops have SDIO interfaces for SD card reading
  - Supports the special commands needed to interface with the boot partitions
- PC's don't have these
  - PCIe Cards exist to do this: Ricoh R5U230
  - Costs $150
- BeagleBone Black
  - SDIO interface for interfacing with eMMC
  - Costs $50



Demo

Questions?

Thank You!

Thank you Blackhat 2017 and to the following people:
@hustlelabs
@0x00string
Mike Stillo
Our families

@exploiteers
freenode: #exploiteers
web: http://exploitee.rs

http://BH2017.Exploitee.rs