Mandiant

Google Cloud Security

EMMC No Ball Reball

Defcon 33 Workshop

August 2025

Contents

emmc_noball

emmc_noballdc33_rockon!
192.168.55.1xx

Presenter Introduction

Patrick Kiley

Principal Red Team Consultant

Principal Red Team Consultant at Mandiant/Google, specializing in embedded systems testing. Patrick has over 20 years of information security experience working with both US Govt and private sector employers. Patrick has spoken at DEFCON, BlackHat, Bsides and RSA. Patrick can usually be found in the Car Hacking or Aerospace village where he volunteered for several years. His passion is hardware security and has released research in Avionics, IoT and even bricked his own Tesla while trying to make it faster.

Class Introduction

Patrick Kiley

Principal Red Team Consultant

EMMC is a common flash memory format for more complex embedded devices and the Ball Grid Array (BGA) is a popular format for EMMC modules. BGA modules can be intimidating to hardware hackers since the pins are not exposed and are instead underneath the chip. This workshop will demonstrate and allow you to practice removing EMMC modules from an inexpensive circuit board using flux and a hot air station. The module will contain a Linux operating system and a Raspberry Pi. Workshop participants will learn how to image the removed EMMC. Mount and change the Linux filesystem in order to backdoor the image and gain access, and then learn how to copy the image to a new EMMC. Participants will then learn how to attach the module to a BGA carrier board with hot air.

01
EMMC Fundies

EMMC is a rather close relative of the SD card

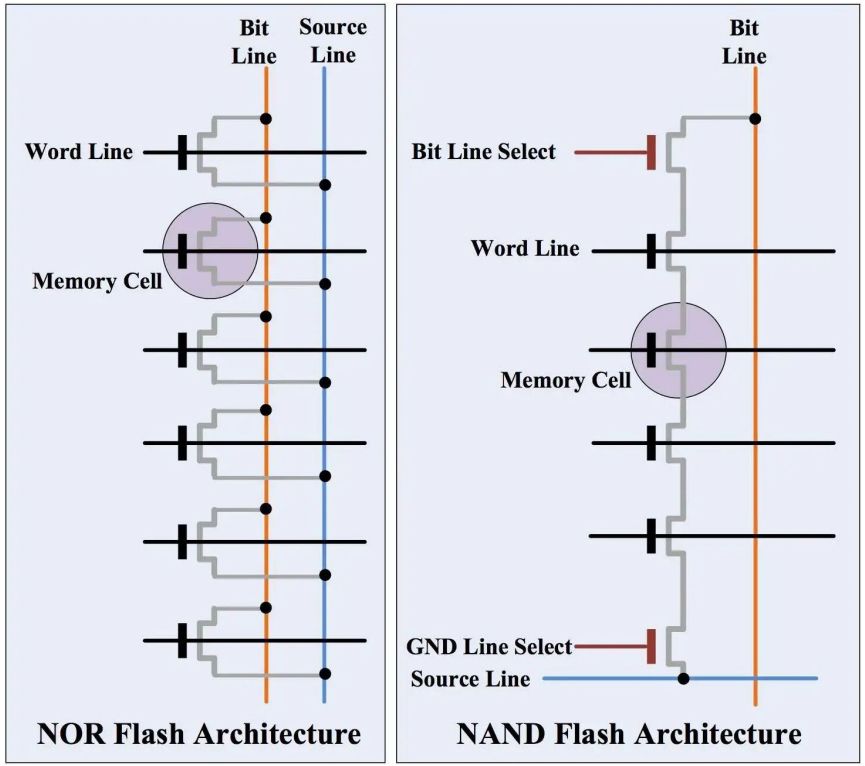
Flash Types

NAND - Higher density, cheaper, bad blocks

NOR - Fast read, slow write/erase, random access

EMMC - NAND++, managed NAND

UFS - Newer mobile devices, faster



SDMC and EMMC

Easy explanation, EMMC is an SD card with 8 data lines instead of 4

For our purposes, they are identical

To communicate with EMMC, you only need 1 data line

EMMC footprints

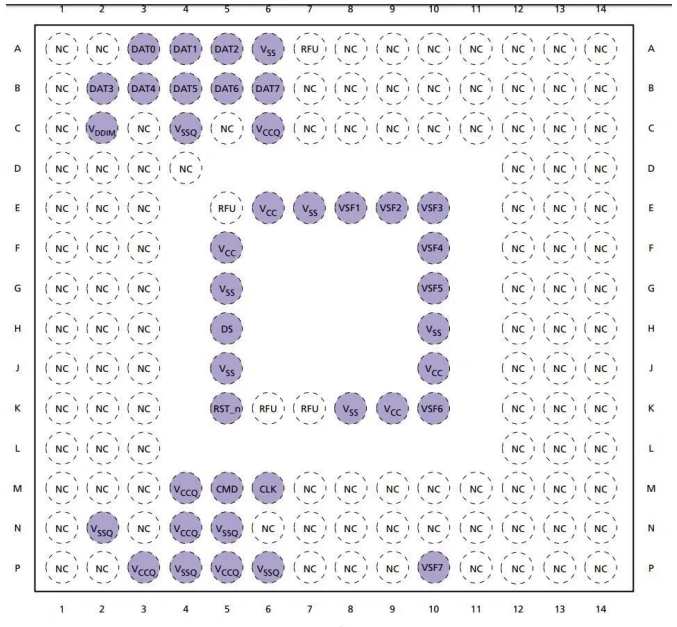
BGA 221

BGA 153 (this is us)

BGA 254

BGA 169 (another common one)

Remember - top down, mirror if you are looking at it.



SD and EMMC Pin Descriptions

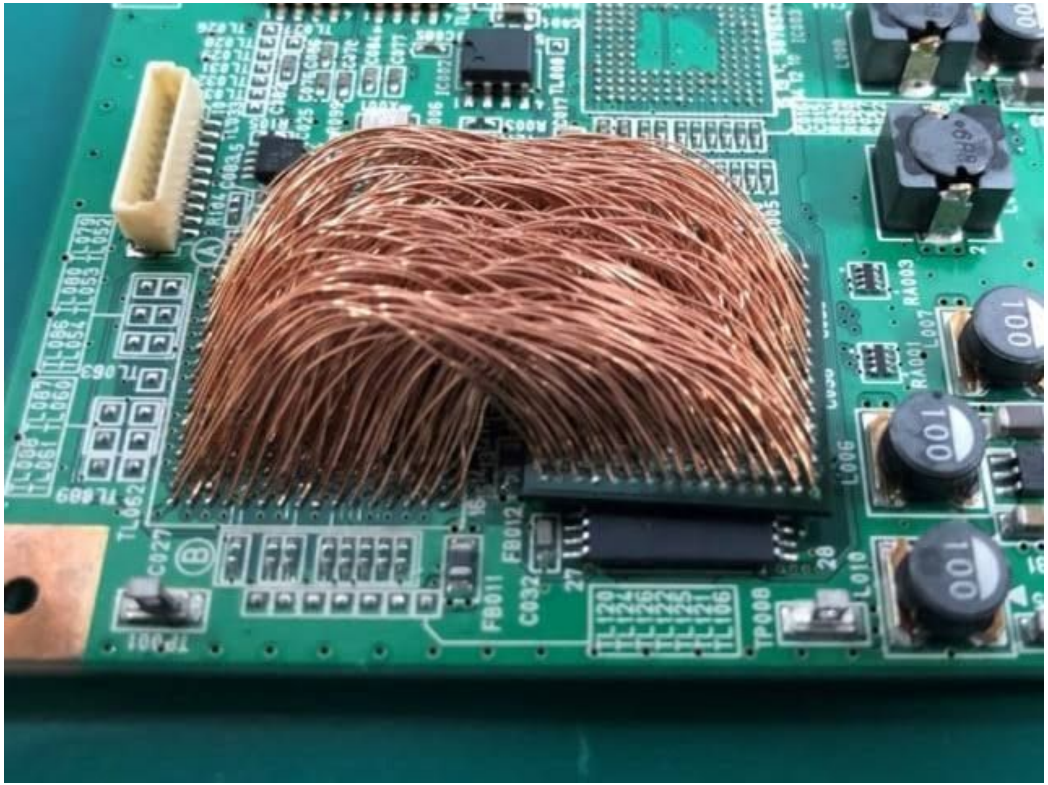
- VCC 1.8v and 3.3v
  - 1.8v controller
  - 3.3 flash
- GND
- CMD (command)
- CLK (clock)
- Data 0-7
  - SD uses 0-3
  - EMMC doubles, 0-7
  - Just need 1 (0 if you think that way)

Deadbugging

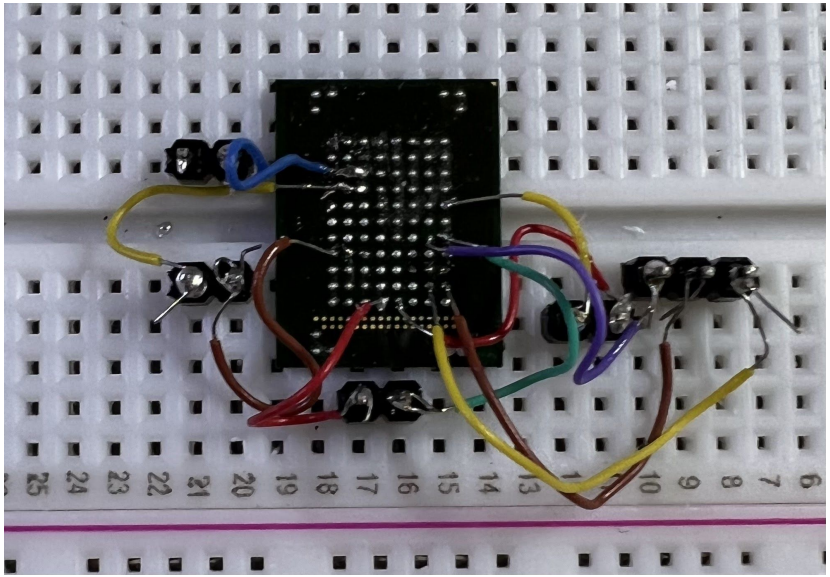
Connect from removed BGA (or traces) to chip

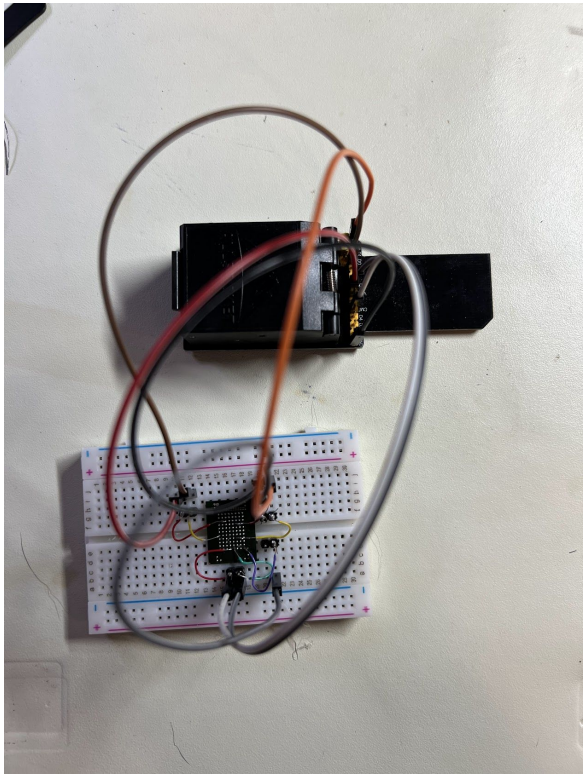
Did this once when I did not have an adapter

(Not my image)



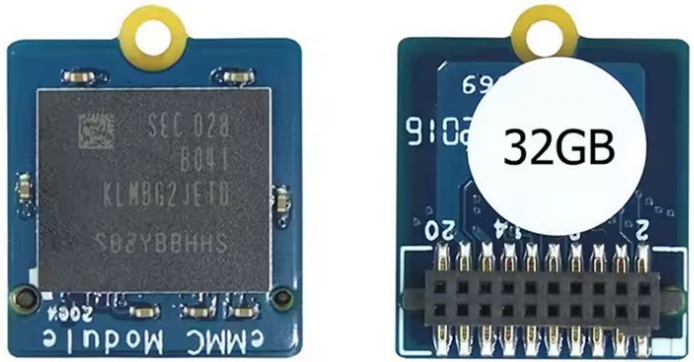
Deadbugging





Equipment

- Raspberry Pi
  - Pi 5 with SD card adapter
- SD to EMMC adapter (8GB)
  - Has SD card shaped PCB
  - Connects to EMMC
  - Caps are on power rails only
- Future versions
  - Combine boards
  - Use higher Tg
  - Move caps away from work area



eMMC module 32GB × 1

Micro SD to eMMC Module Adapter ×1

Lab 1

- Assemble EMMC adapter
- Carefully plug in on underside
- Power up
- Wifi SSID and Password
- Try to connect
  - Should be able to ping only

Lab 1

- Assemble EMMC adapter 192.168.55.1xx
- Carefully plug in on underside
- Power up
- Wifi SSID and Password
- Try to connect
  - Should be able to ping only

02
BGA Removal

Flux is your friend here

Flux

- Flux is your friend
  - Eliminates oxidation
  - Promotes heat transfer
  - Smells like hacking!
- Use a high quality rework flux
  - Single 10cc tube lasts long time
  - Stirri personal favorite
  - STIRRI-V3-TF
  - Be careful about counterfeits

Rework Heater

- Helpful but not necessary
  - Prevents heat shock on dense boards

Hot Air - Really HOT air

- Quick 861DW clone
- Be careful, it’s a soldering iron, but airborne
- Use setting 2, 375 temp and 40 airflow
- Do not turn off when done, return to holster and air will go to max and will cool down elements.
- Do not point at table, yourself, anyone else or FFS nothing flammable

Safety Third

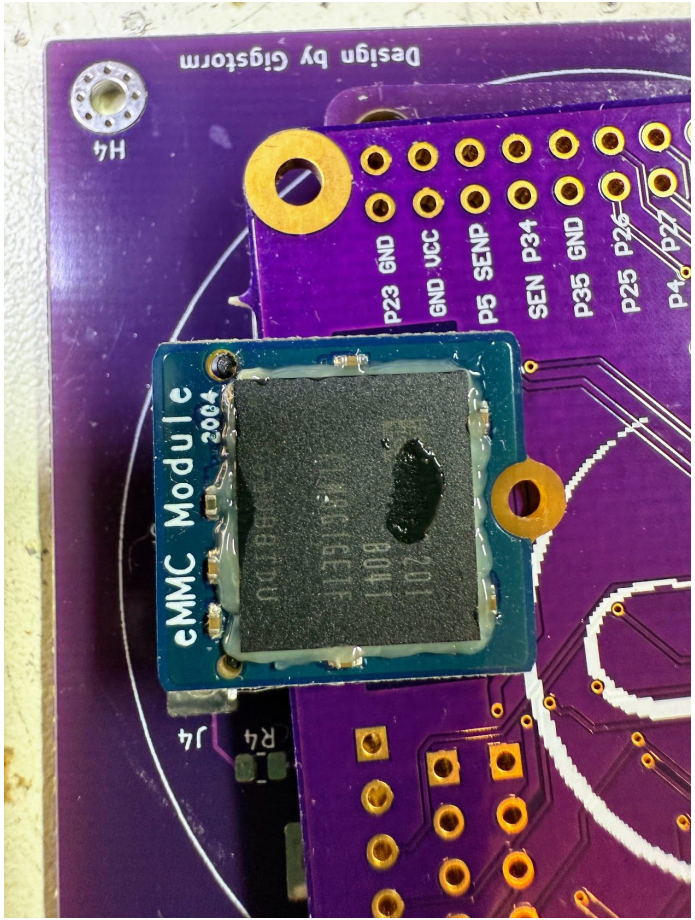
- Seriously though, wear eye protection
- Hot ceramic shards in the eye is bad

Kapton Tape

- Not necessary here
- I have some if you want to try it

Process

- Make a stack using scrap PCBs
- Put PCBS on silicon mat
- Apply liberal bead of flux along edge
  - Flux will wick underneath when heated
- Heat chip with low airflow and 375-400 temp
- Do not force or pry
- Remove quickly from board and remove heat
  - Let hot air cooldown

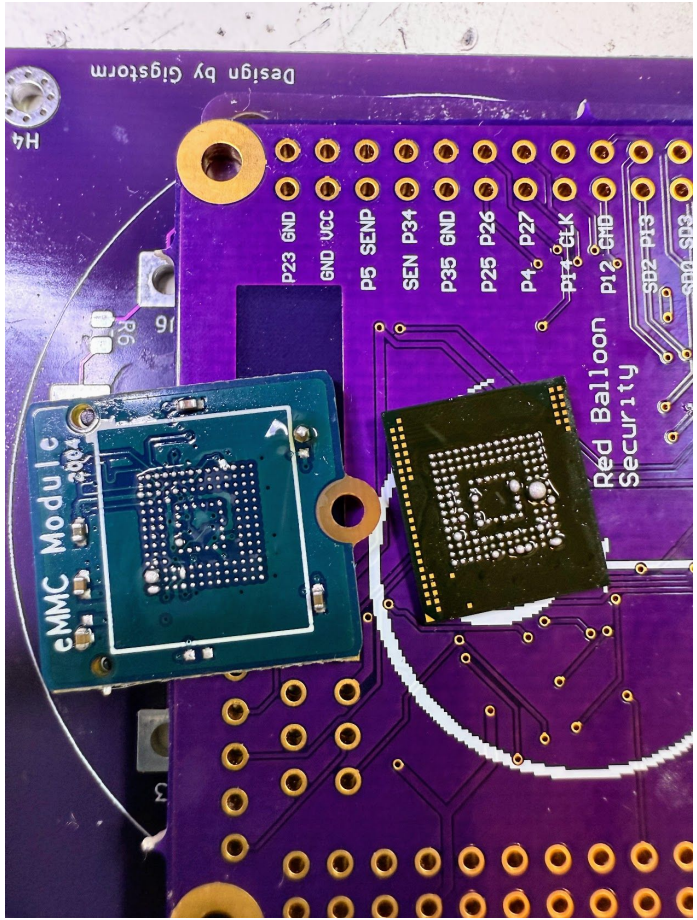


Cartridge based iron

- JBC clone FNIRSI and Sugon A9
  - Based on JBC CD-1SQF
  - C210 and C245 irons
  - C245 used in class
  - C210 smaller, used for rework
- Heater and thermocouple in cartridge
  - Adjusts power dynamically to maintain temperature

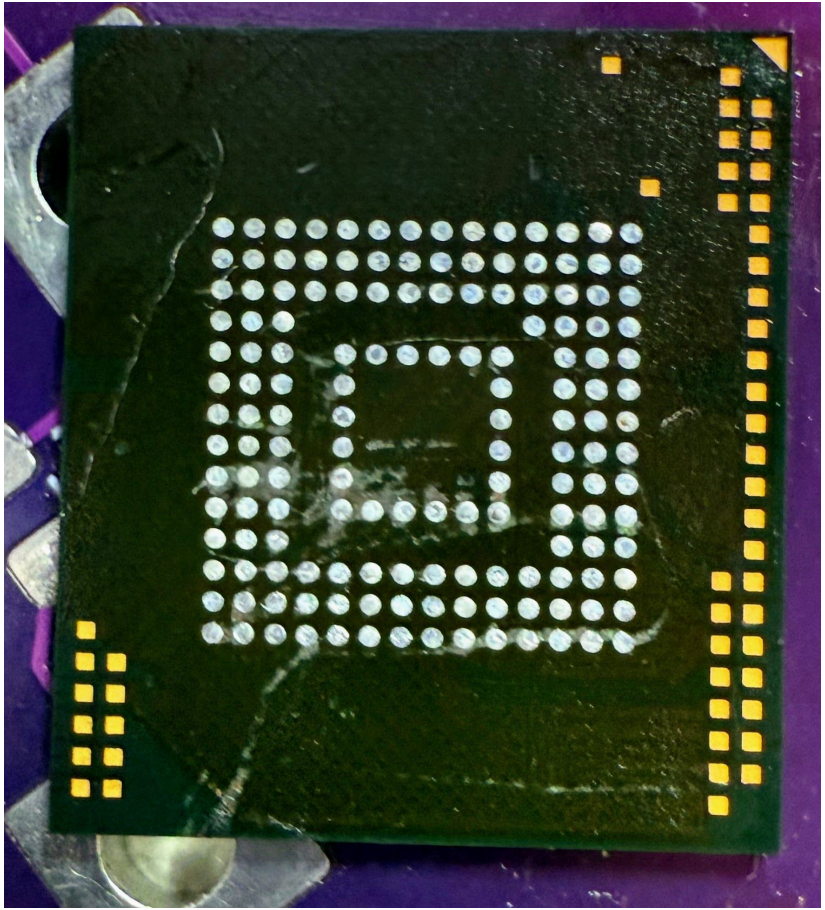
Cleanup

- Remove excess solder
  - From board
  - From bga
- Use iron and solder braid
- Use more flux
- Re-alloy if necessary
- Goal is a flat set of pads with minimal solder



Cleanup Results

- Remove excess flux
  - Use flux remover and swab
- Should have flat pads with minimal solder
- Remaining solder can prevent connection and imaging
- If you removed a cap, you can reattach if you want, not mandatory

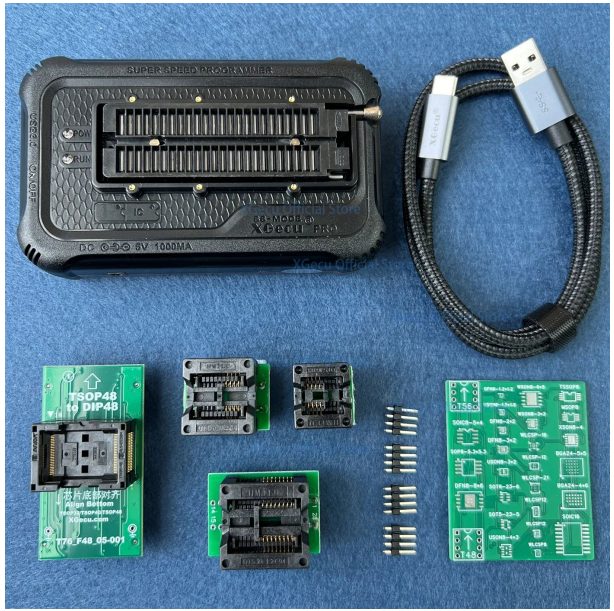


03
EMMC Imaging

Odin of Flash - The AllSocket

EMMC Imaging

- Devices
  - Flash reader
    - Read only
  - Allsocket
    - Can mount, make changes
    - Just a SD to EMMC clamshell
    - Few passives to stabilize connection
    - Can use to deadbug



EMMC Imaging

- Ensure EMMC is clean
- No raised solder pads
- Ensure pin 1 is lined up with arrow
- Try 1.8v first, 3.3 next
- Connect to VM, see if /dev/sd$ is recognized
- Should have 2 partitions look at messages
  - Sd? Attached SCSI removable disk
  - sd?: sd?1 sd?2

```
Device     Boot   Start      End  Sectors  Size Id
/dev/sdb1          16384  1064959  1048576  512M  c
/dev/sdb2        1064960 15269887 14204928  6.8G 83
```

EMMC Imaging Lab

- http://192.168.55.205:8000
- If you cannot get a connection, ask for help
- Could have bad connection, try re-alloying, removing solder again
- 2 options to copy (first is recommended)
  - dd if=/dev/sd(b,c...) of=$filename.img bs=1M status=progress oflag=sync
- Or dd if=/dev/sda1 and /dev/sda2 then manually partition target

04
Image Rooting

Choose your own backdoor

Image rooting

- If everything fails and you are unable to image
- I have a copy of the image on USB

Rooting is choose your own method

- Simple to elaborate
  - Change firewall,
  - Add user/ssh key
  - Change user password
  - Add Cron for reverse connection
  - Modify startup script

Hacking in movies:

Behind the scenes:

```
import secrets

bruh = secrets.token_hex(10000000)

print(bruh)
```

Rooting Lab 1

- Again, we are here to help
- Mounting hint
  - losetup -P -f
- Then may or may not have to manually mount partitions

Rooting Lab 3

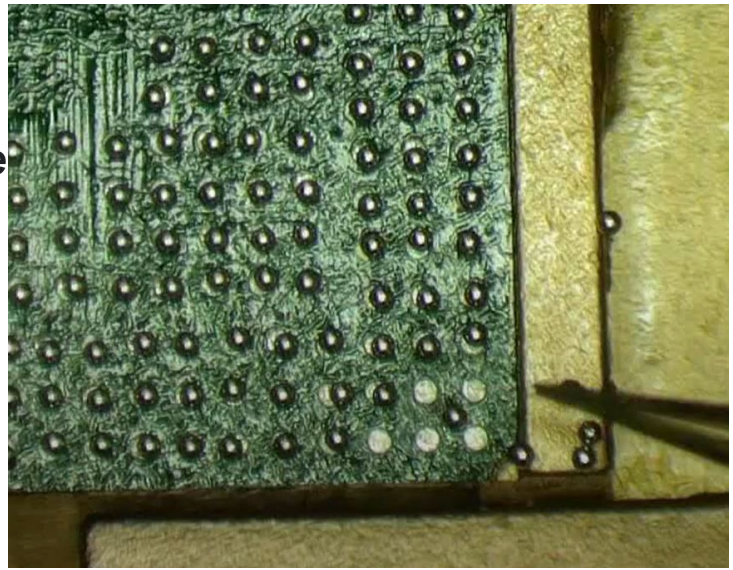
- Modifying hint
- chroot makes it much easier
  - bit.ly/41aerH9
- If you are completely stuck, I have a pre-rooted image you can use to copy over to new emmc

05
Reballing

And why it is a waste of time, most of the time

Reballing process

- Purchase appropriate size solder balls
  - Sub mm size .25mm for example
- Purchase appropriate size stencil
  - freeball it if you really want a challenge
- Apply thin layer of tacky flux
- Carefully put stencil in position
- Put a ball over each pad
- Remove stencil and reflow (don't use air)



OR

06
The no ball reball

Just replace the EMMC, most of the time its dirt cheap.

EMMC replacement cost vs your time

Reballing is fine if

- **The chip is difficult to replace**
- **Your time is not valuable**
- **You are a masochist**

The cost of the materials, time and effort is usually not worth the cost of buying a new EMMC

EMMC have a finite number of read/write cycles

Plus if you are resurrecting old hardware, you can replace with a more robust one

07
BGA Reattachment

The hardest part of the process

BGA Reattachment

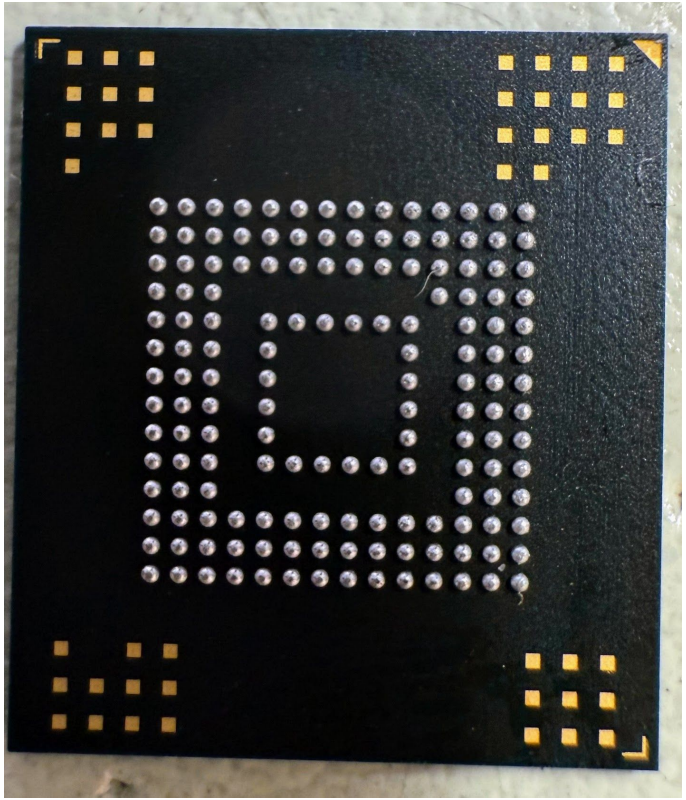
Apply flux to EMMC or board

Align pin 1 with markings

Can use kapton with loop to make alignment easier

Place board on scrap pcb rack and mat

Double, triple check before applying heat



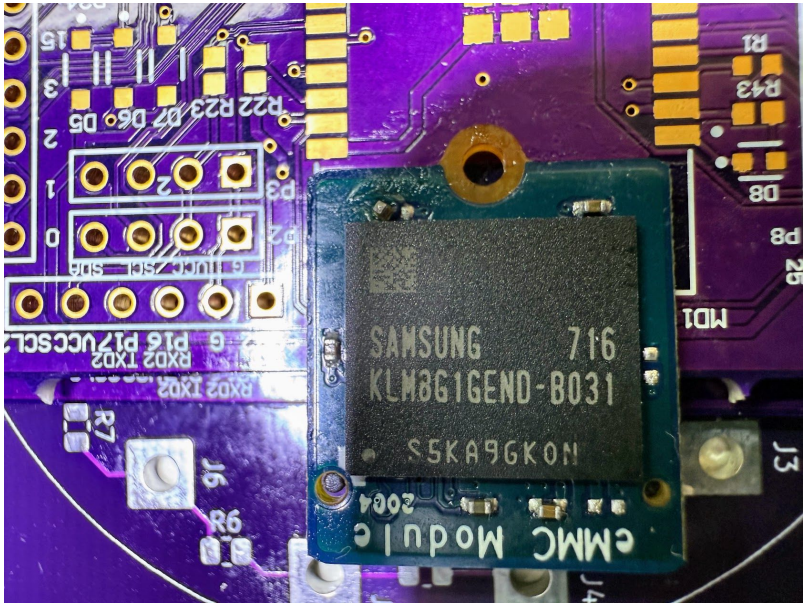
BGA Reattachment

Turn on hot air, setting 2

Move air in slow even movement, do not keep in same position

Watch carefully, wait for solder to melt and you should see the smallest movement as the chip aligns with pads.

Remove heat and do not touch until cool

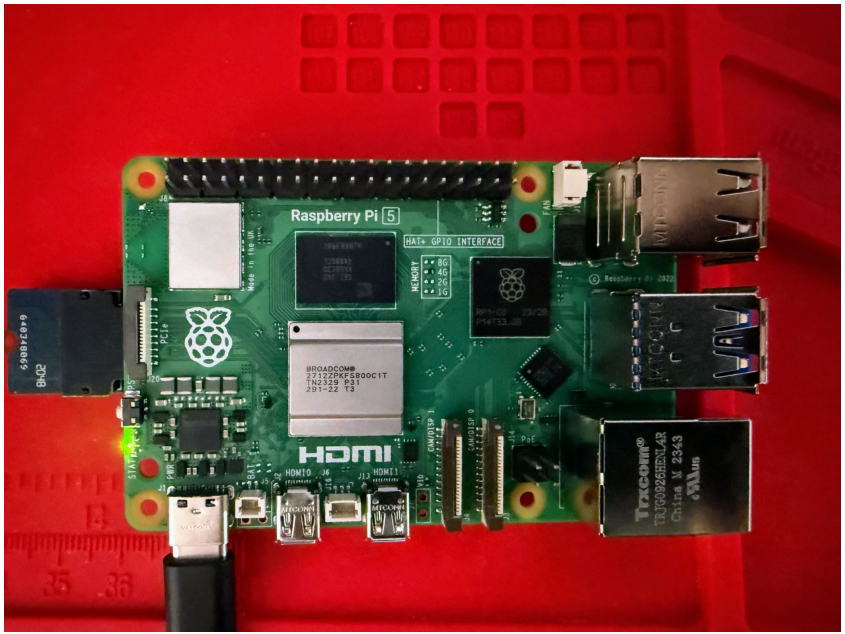


BGA Reattachment

After board has cooled, plug in and see if pi boots

Check for connectivity

Congratulations!



08
Additional Resources

Resources

Repo - https://github.com/pk-mdt/emmc_noball

Equipment

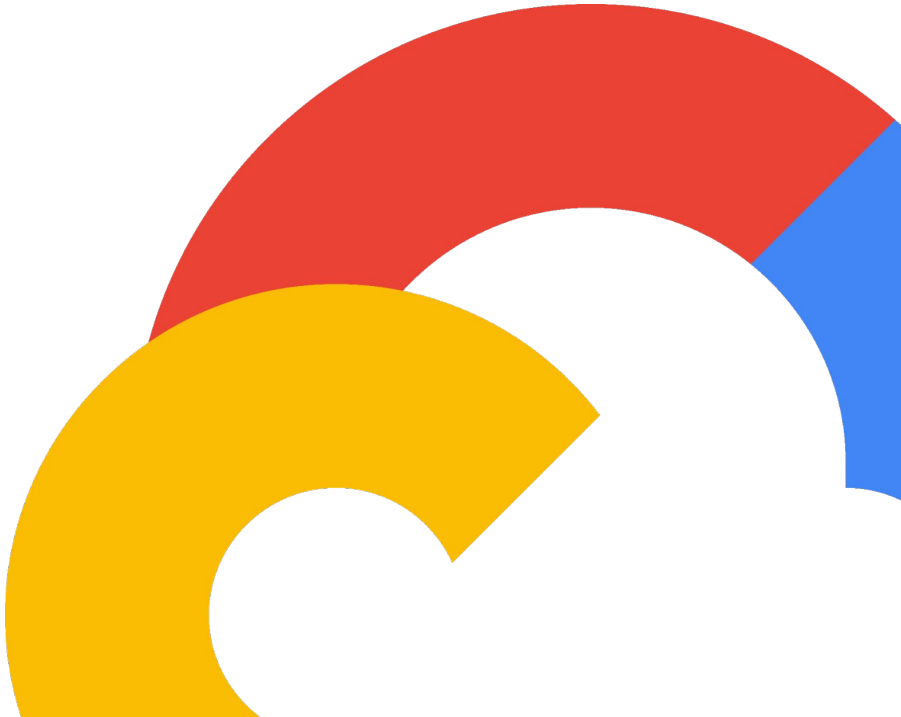
- **JBC - https://www.jbctools.com/**
- **Flux - https://stirri.com/products/stirri-v3-tf**
- **https://github.com/pk-mdt/emmc_noball**

Techniques

- **https://www.youtube.com/@rossmanngroup**
- **https://www.ipadrehab.com/**

Thank you

Safe Travels home



Google Cloud