Taller: Análisis forense en dispositivos Android en casos extremos: Entrando al laboratorio

Buenaventura Salcedo Santos-Olmo

Quien soy yo

Casi Graduado en Ingeniería Informática en la UNED

CEO Servicio Técnico de telefonía móvil e informática

Equipamientos y recursos

https://forensicswiki.org/wiki/JTAG_and_Chip-Off_Tools_and_Equipment

http://www.teeltech.com/mobile-device-forensic-software/teel-tech-jtag-box-sets/

http://winkgsm.blogspot.com/

https://ma.juii.net/blog/unbrick-jtag-smartphones

Equipamientos y recursos

TeelTech JTAG Box Set 2

JTAG Accessories, JIG Kit, and Jtag Boxes

Jtag Boxes

- RIFF Box V2
- OctoPlus
- GPG eMMC
- Z3X Easy JTAG
- ORT
- ATF Turbo

Also includes:

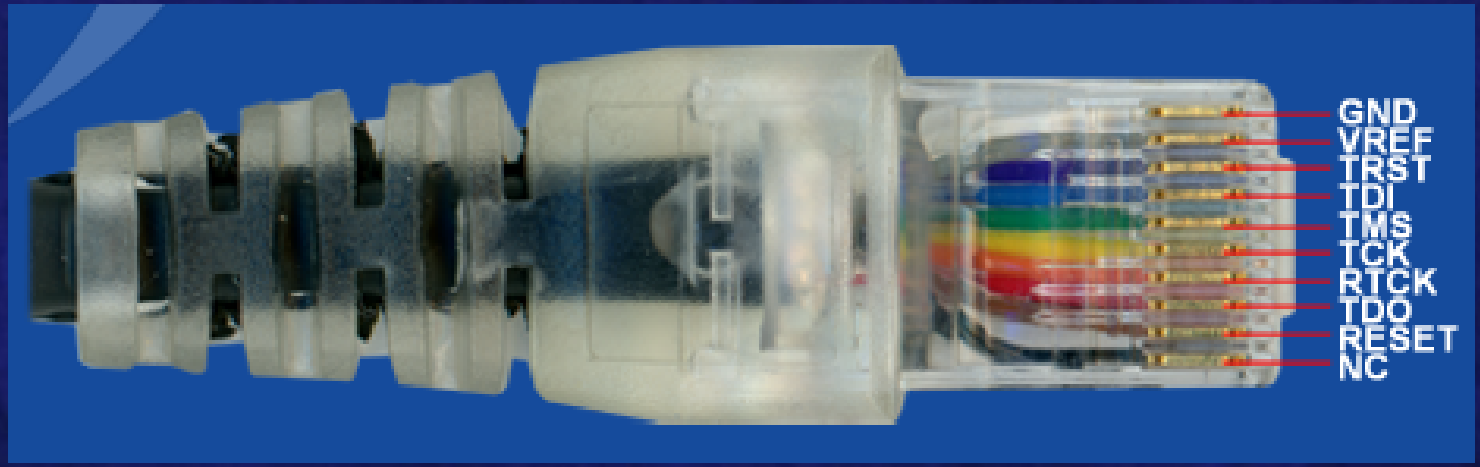
- Moorc Molex JPIN Adapters
- Total of +20 JIGS, Adapters and Tools.
- TeelTech Riff Color Coded Solder Guide

RIFF BOX PINOUT JTAG INFO

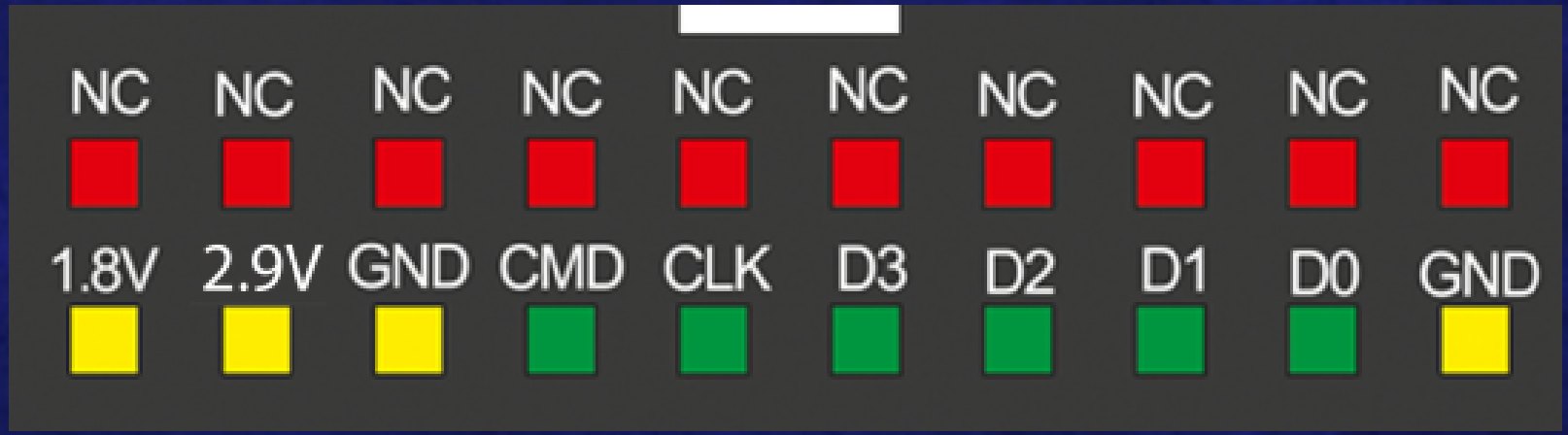
JTAG Interface

1 - VCC
3 - TRST
5 - TDI
7 - TMS
9 - TCK
11 - RTCK
13 - TDO
15 - NRST
4,6,8,10,12,14,16,18 - GND
2,17,19 - N.C.

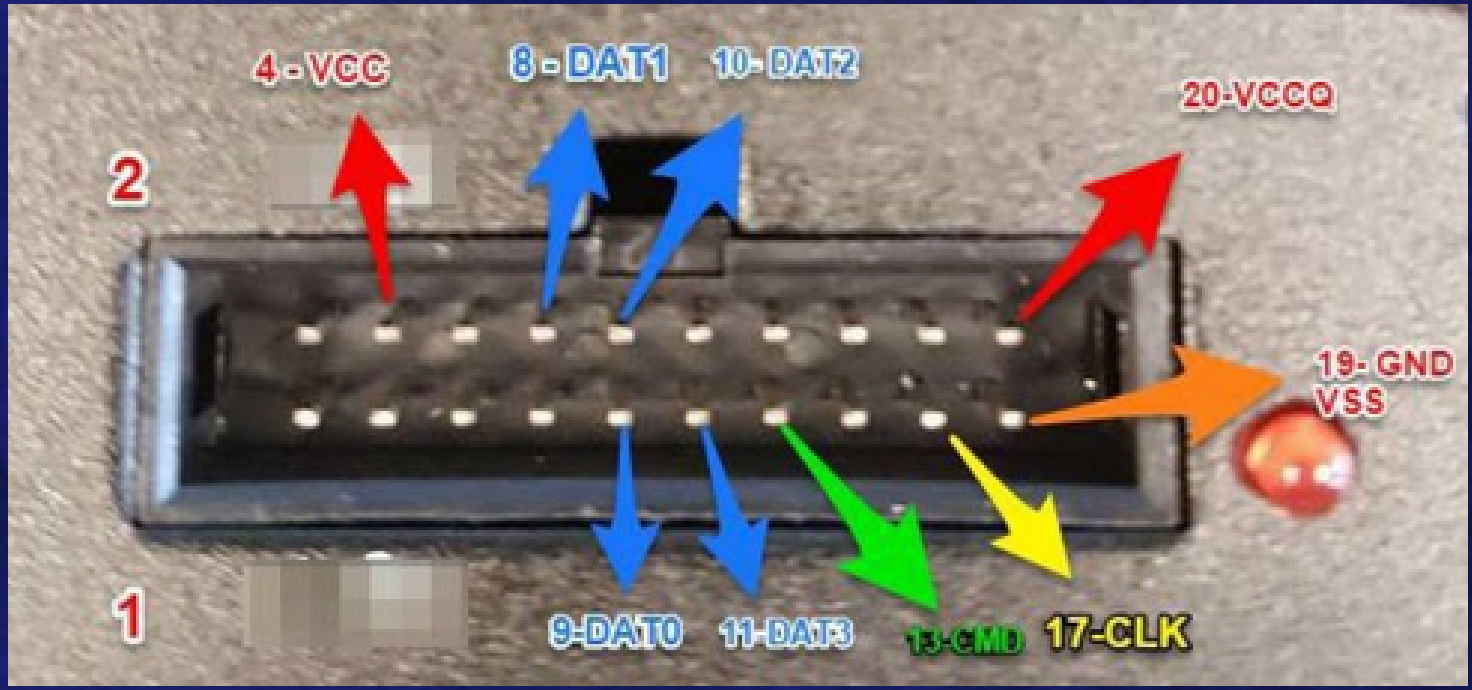
MEDUSA PINOUT INFO



MEDUSA PRO PINOUT INFO

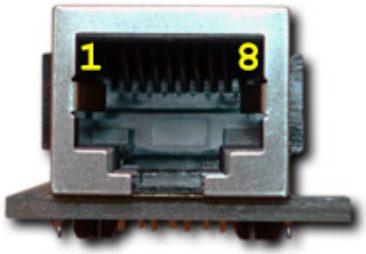


EMMC PRO PINOUT INFO



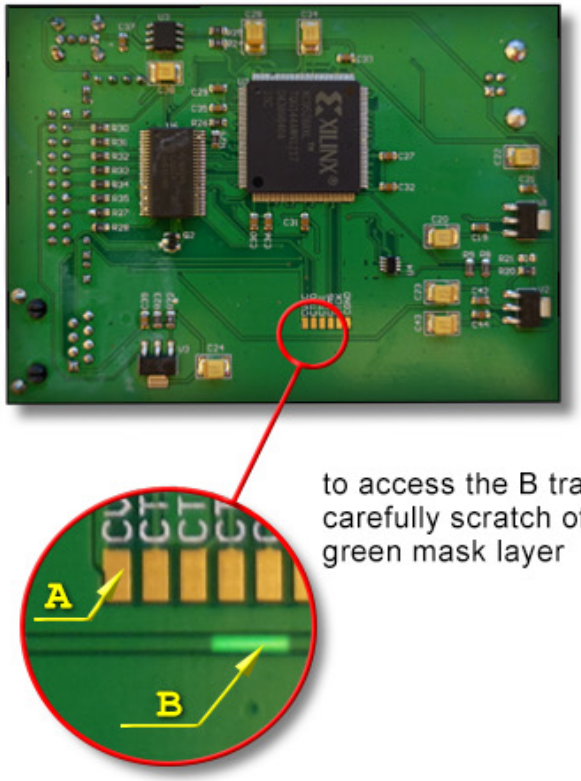
RIFF BOX PINOUT MODIFICATION

SD/MMC Interface on the RJ-45 Connector



1 - 4.2V
2 - SDMMC_CLK
3 - SDMMC_DAT0
4 - SDMMC_CMD
5 - GPIO1
6 - RIFFBOX_PROBE
8 - SDMMC_GND

A - SDMMC_VCC
B - SDMMC_VCCIO

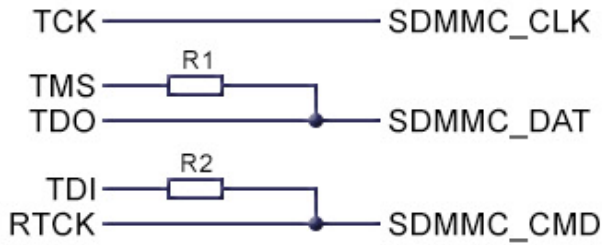


to access the B track carefully scratch off the green mask layer

RIFF BOX PINOUT JTAG INFO

SD/MMC Interface on the JTAG Connector

5 - TDI
7 - TMS
9 - TCK
11 - RTCK
13 - TDO



R1, R2 - adjust for best signal quality (0 Ohm ... 1 kOhm)
VCC, VCCIO - as A & B for RJ-45 pinout

EXPERIMENTOS propuestos

A.- Dump con Infinity BOX

B.- TP con Infinity BOX

C.- JTAG con MedusaBOX

D.- JTAG con RiffBOX

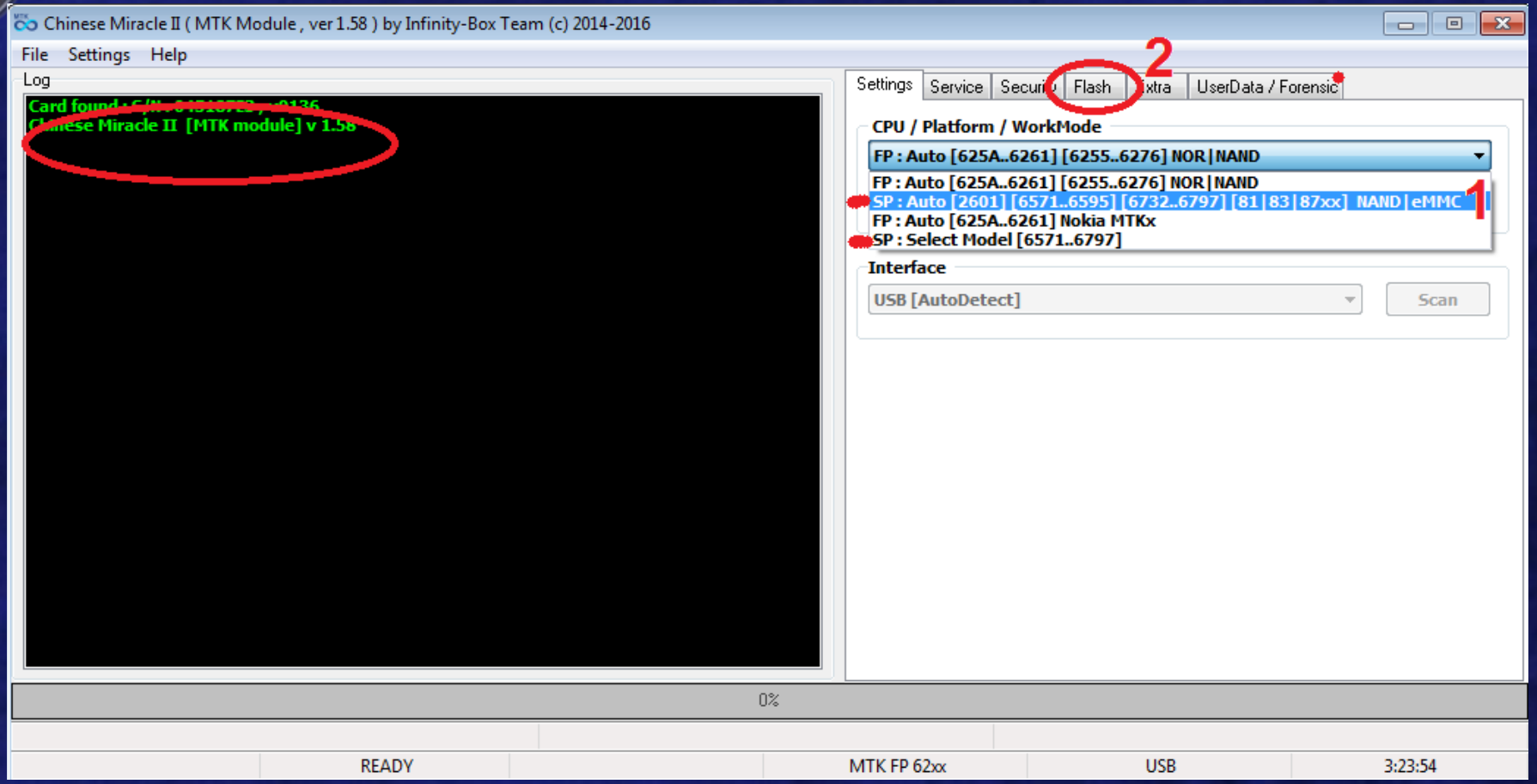
E.- ISP con emmcPRO BOX

F.- ISP con Medusa PRO BOX

G.- Chip Off con adaptador MOORC y SD

H.- Chip Off sin adaptador (directo a memoria) con emmcBOOSTER

A.- Dump con Infinity box



A.- Dump con Infinity box

1.- Abrir el software correspondiente (MTK)

2.- Seleccionar plataforma y modelo si procede

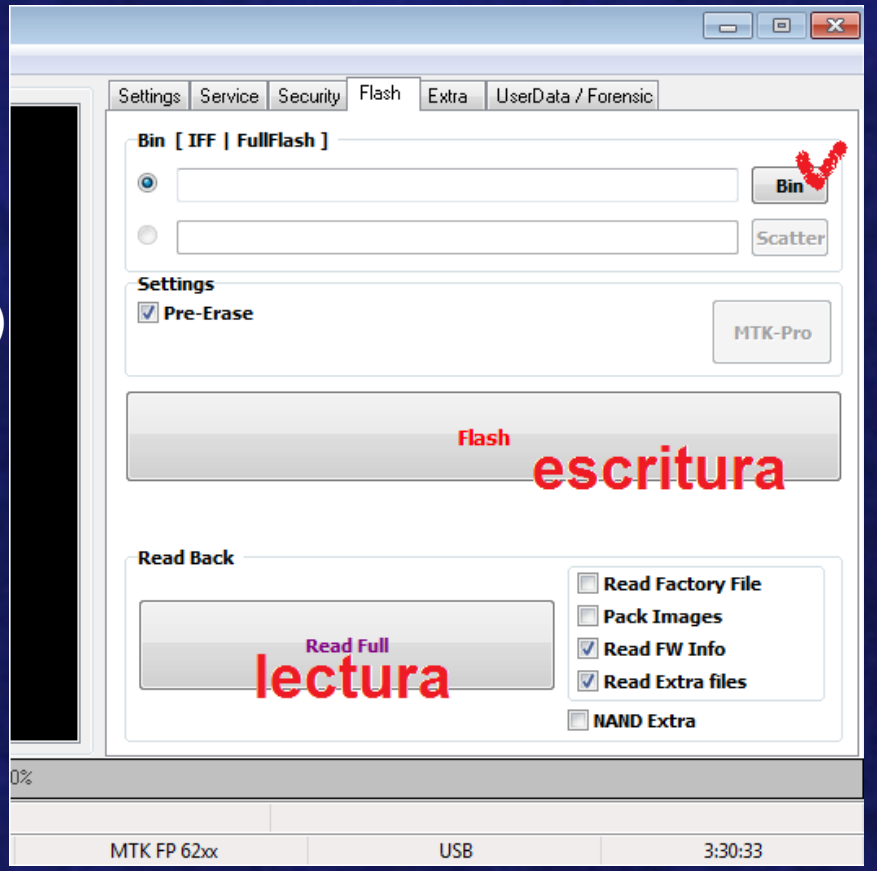
3.- Pestaña Flash y Read Full (nombre por defecto)

4.- Conectar USB para download mode

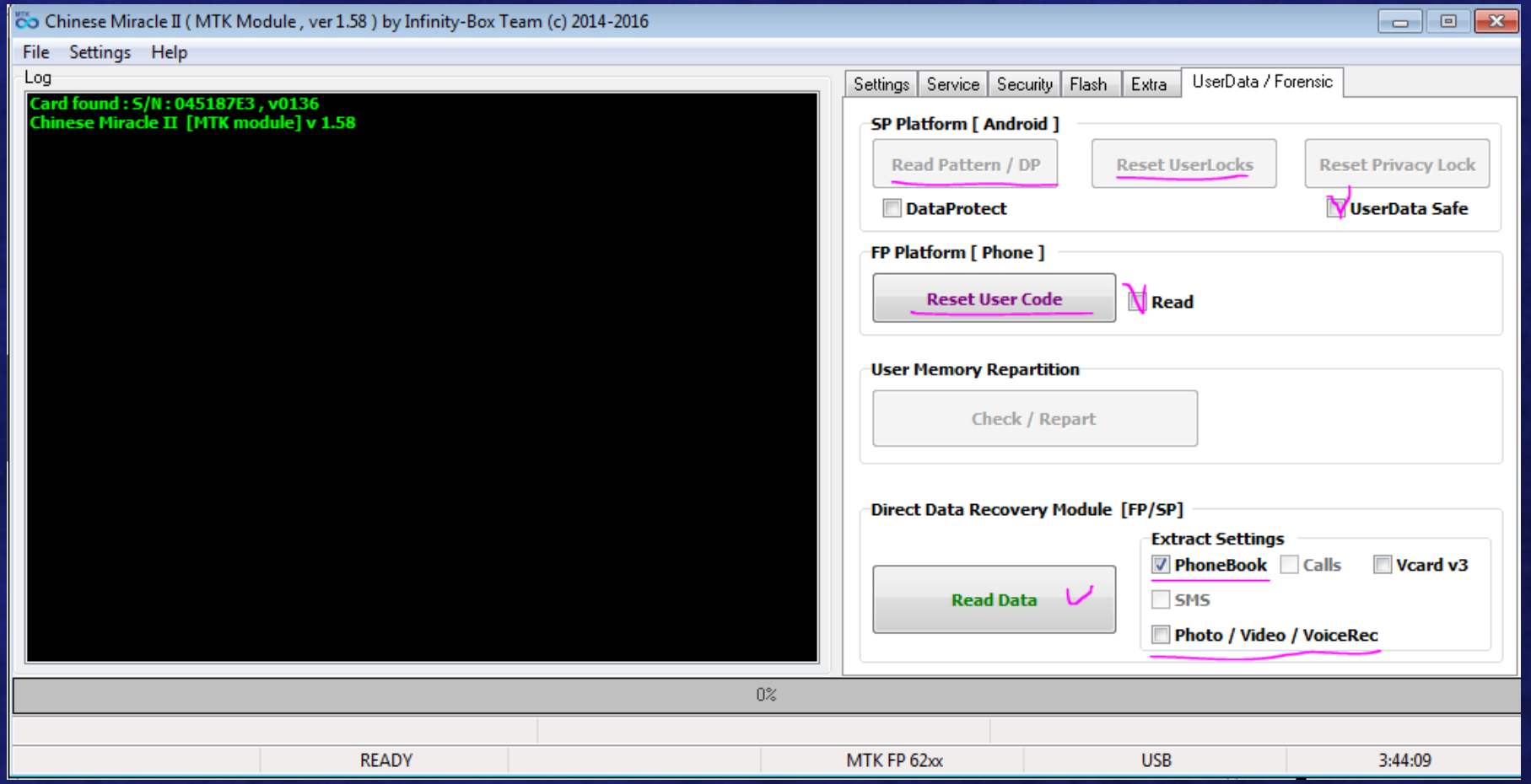
5.- Hashear y abrir dump con FTK (ANÁLISIS)

5.1.- Si no particiones entonces mapear

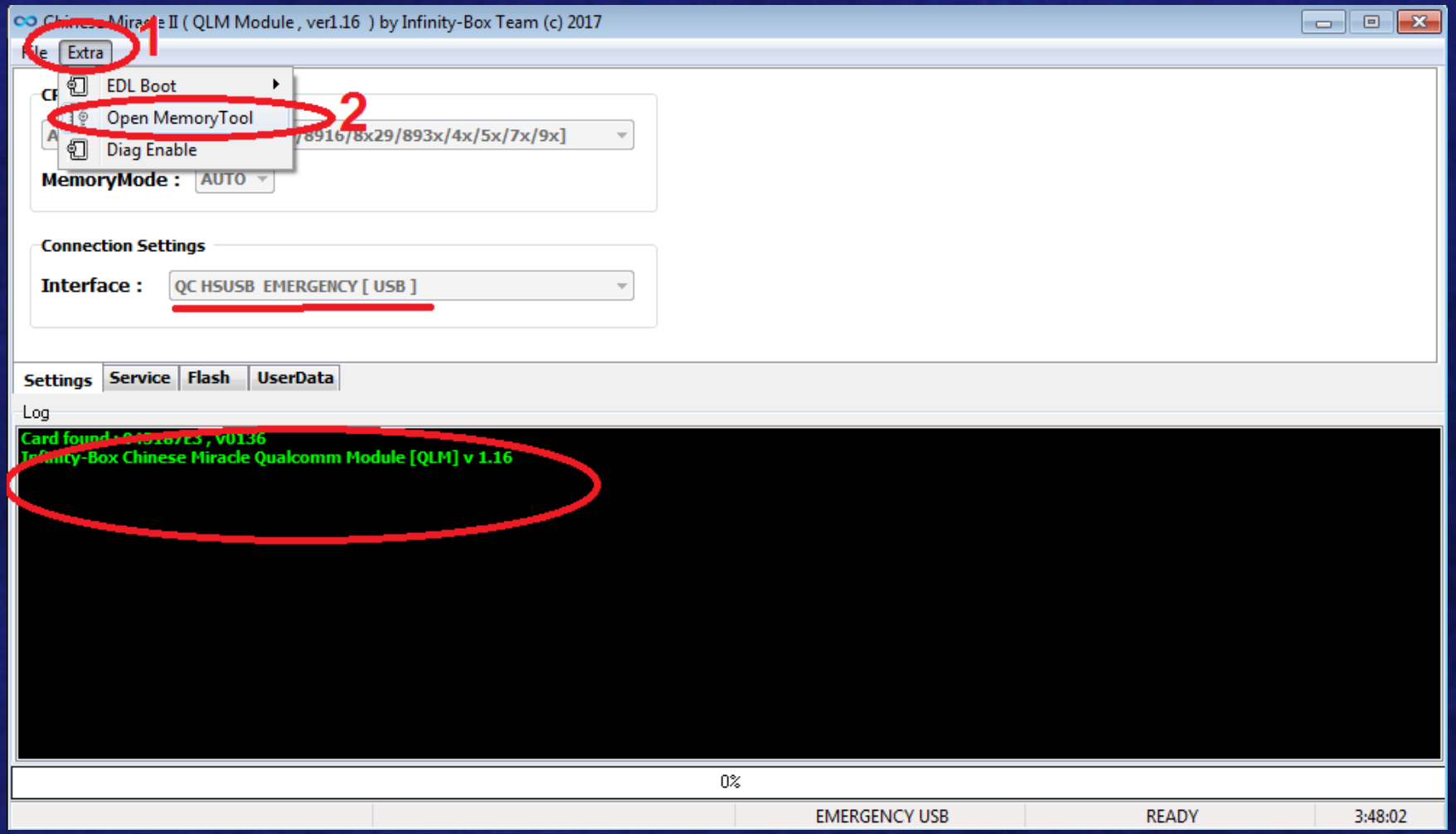
5.2.- Si no se puede mapear autopsy o pago



A.- Dump con Infinity box



B.- TP con Infinity box (CM2QLM)



B.- TP Infinity box (CM2QLM)

IMPORTANTE: Los drivers deben ser instalados en el mismo orden que aparecen en la carpeta c:\InfinityBox\CM2QLM\Drivers

1.- Abrir el software correspondiente

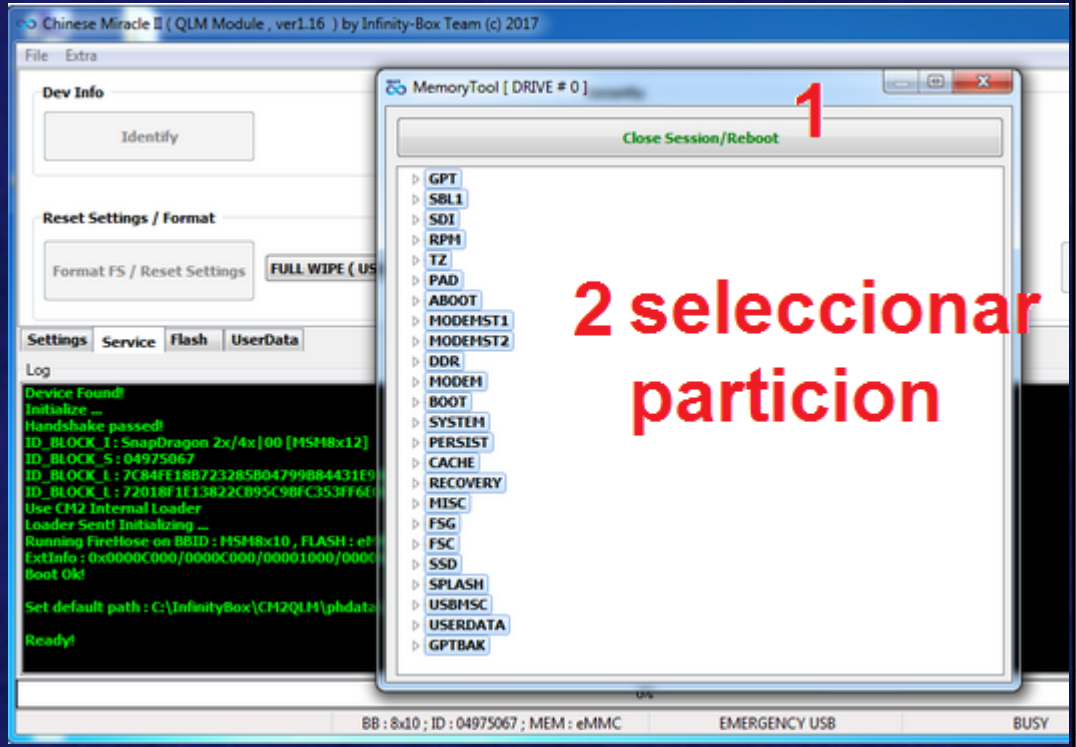
2.- Extra – Open Memory Tool – Init Device

3.- Realizar TP y conectar USB → EDL mode

4.- Después de boot desconectar TP

5.- Seleccionar partición y b.d. READ

6.- Hashear y ANÁLISIS

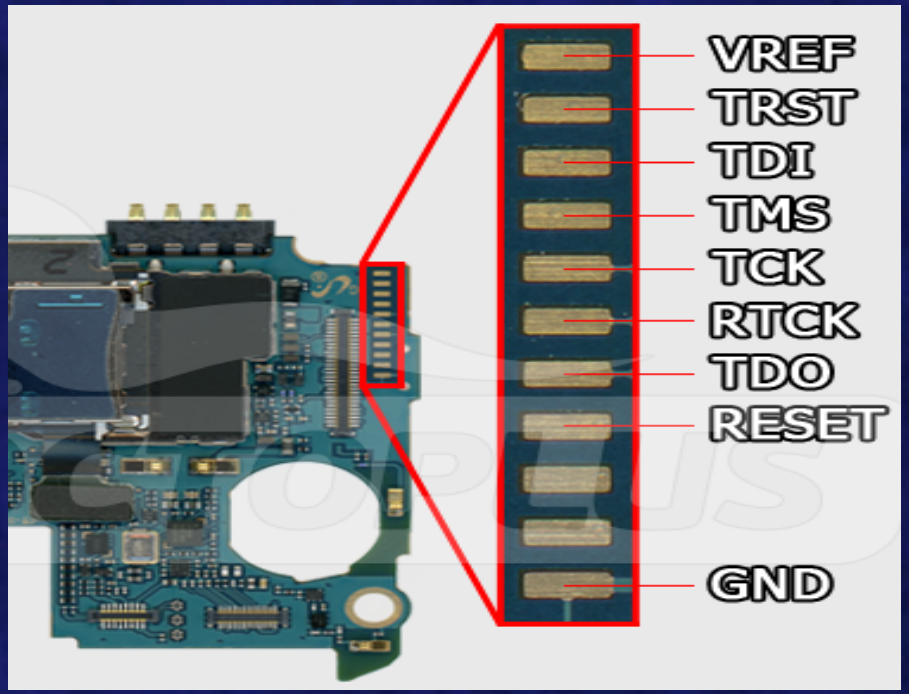


* No hace falta batería, antes de leer la partición asignar la ruta de almacenamiento

C.- JTAG con Medusa a Samsung i9505

1.- Realizar el JTAG

2.- Abrir el software de RiffBOX



C.- JTAG con Medusa a Samsung i9505

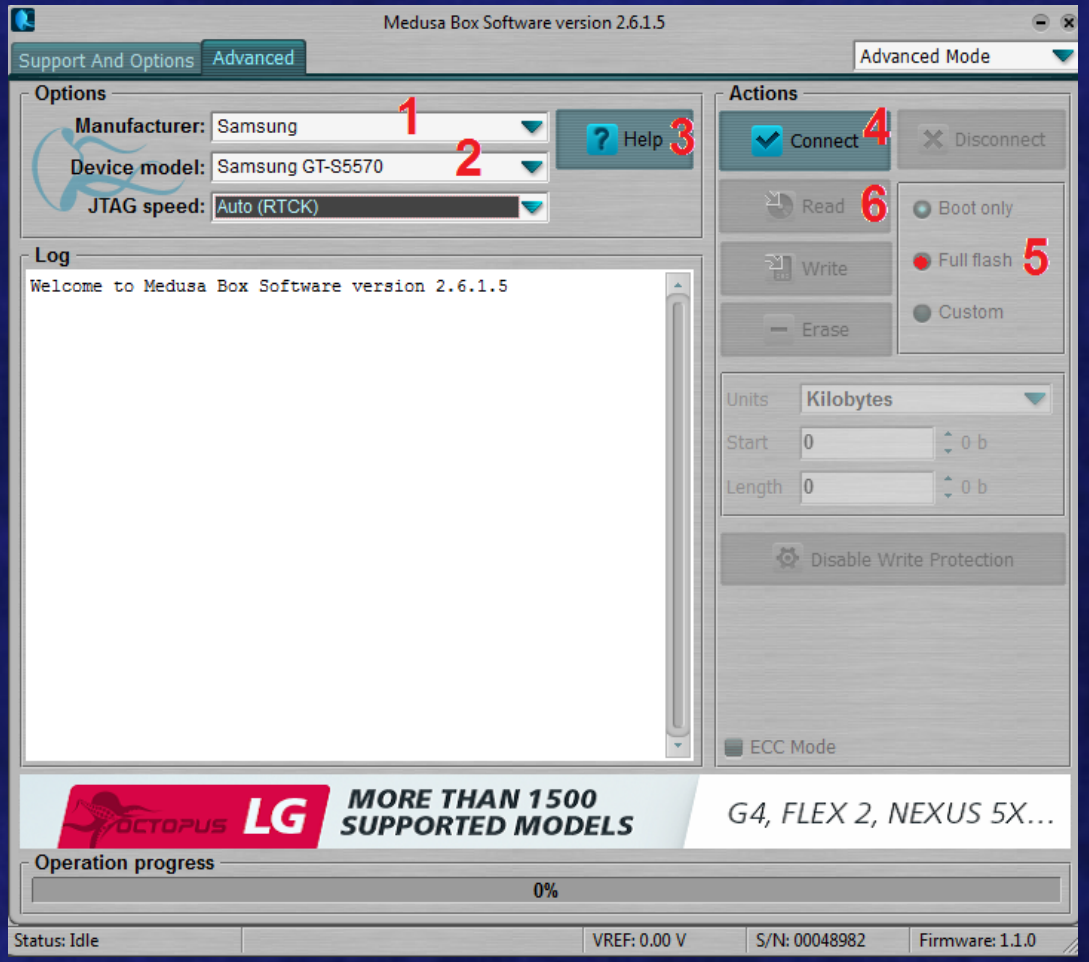
3.- Seleccionar marca - modelo

4.- Pulsar en Connect y pulsar ON

4.1.- Corregir los errores

5.- Full Flash y Read

6.- Hashear y ANÁLISIS



D.- JTAG con RiffBOX a Samsung s5570

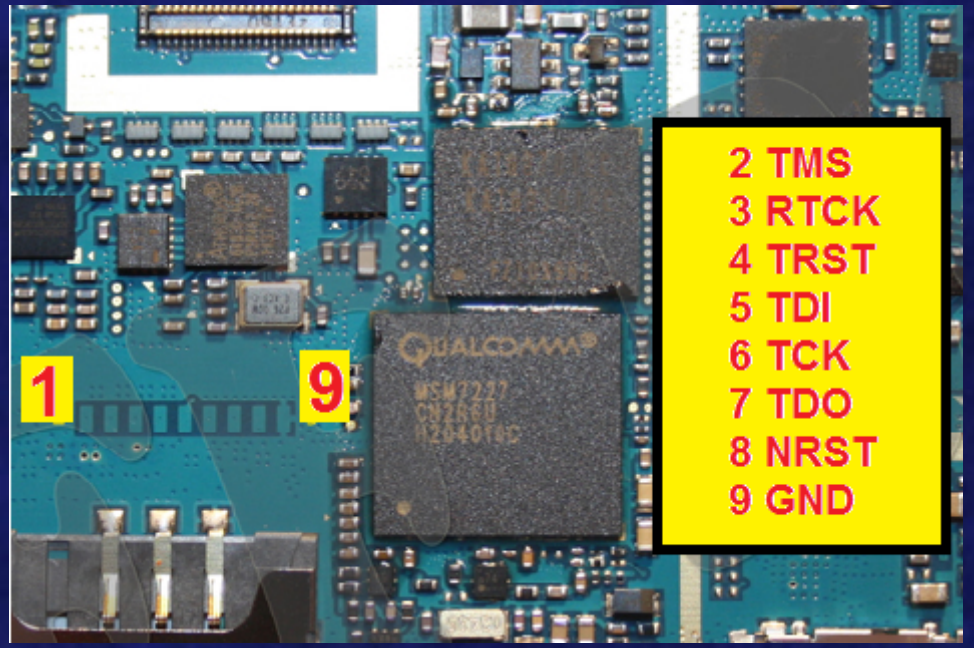
1 VCC	11 RTCK
3 TRST	13 TDO
5 TDI	15 NRST
7 TMS	2,17,19 GND
9 TDK	RESTO NO CONECTADOS

1.- Realizar el JTAG

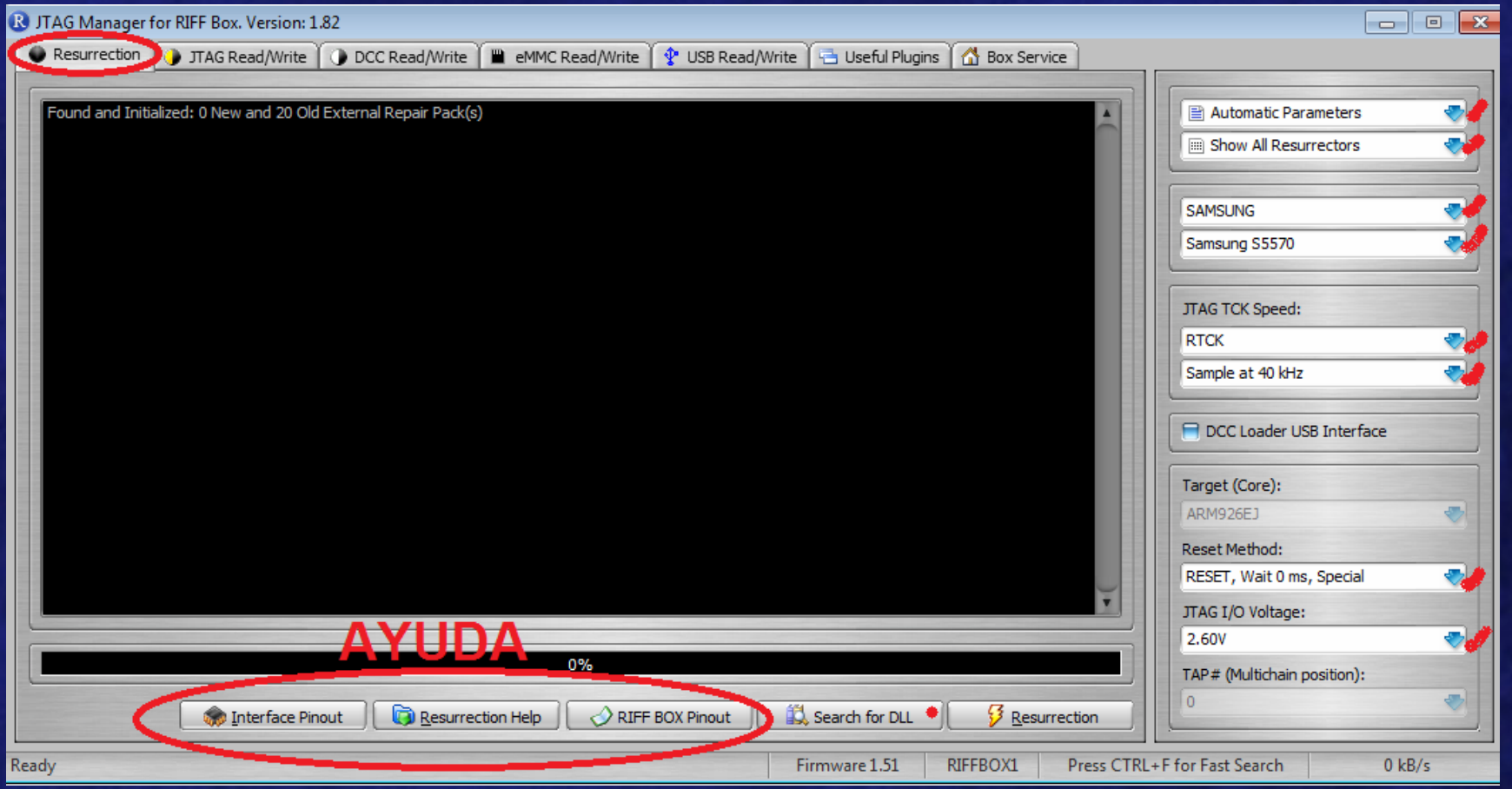
2.- Abrir el software de RiffBOX

3.- Revisar las ayudas para los pinout

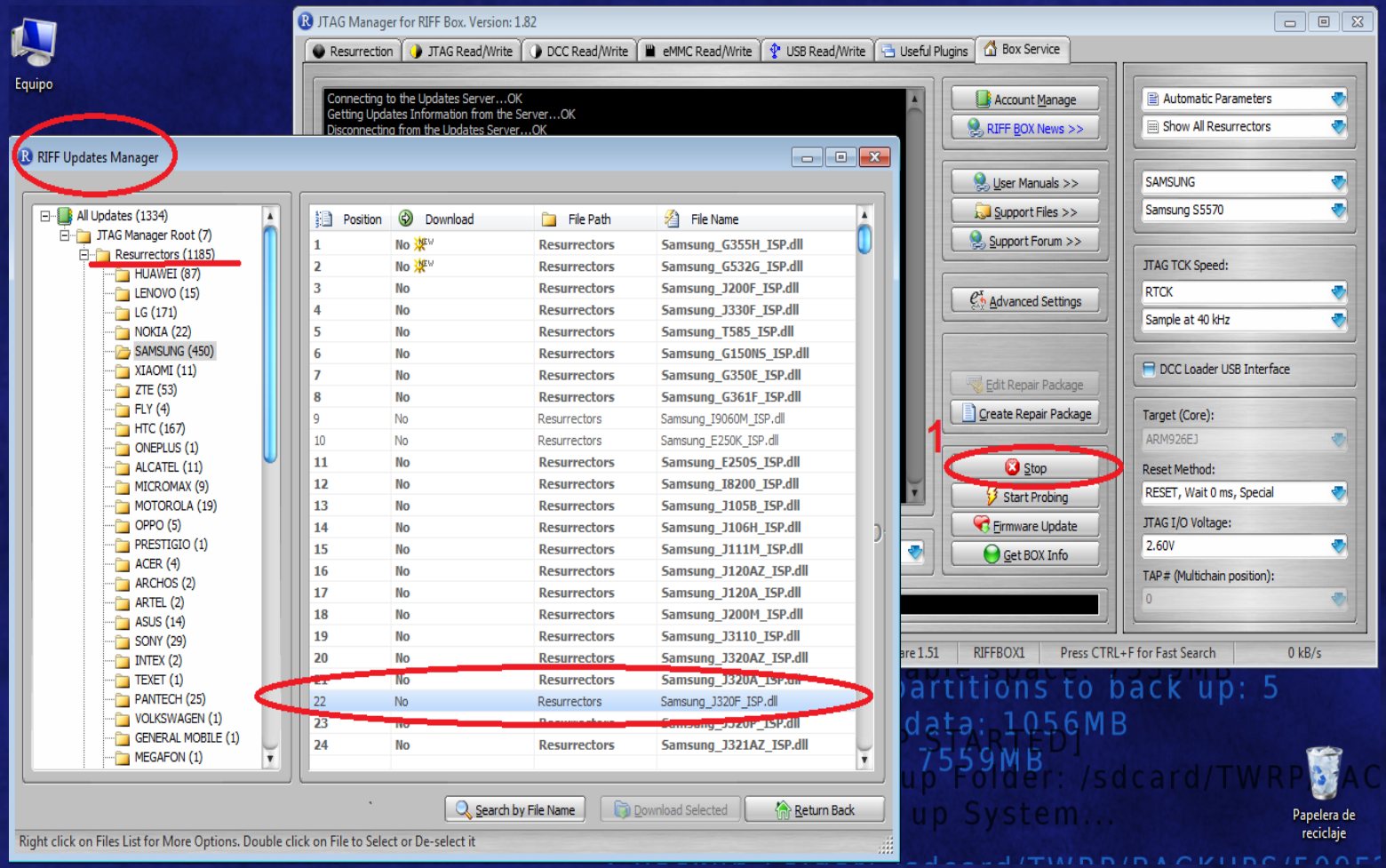
3.1.- Si no existe el pinout que necesitamos buscar el resurrector necesario



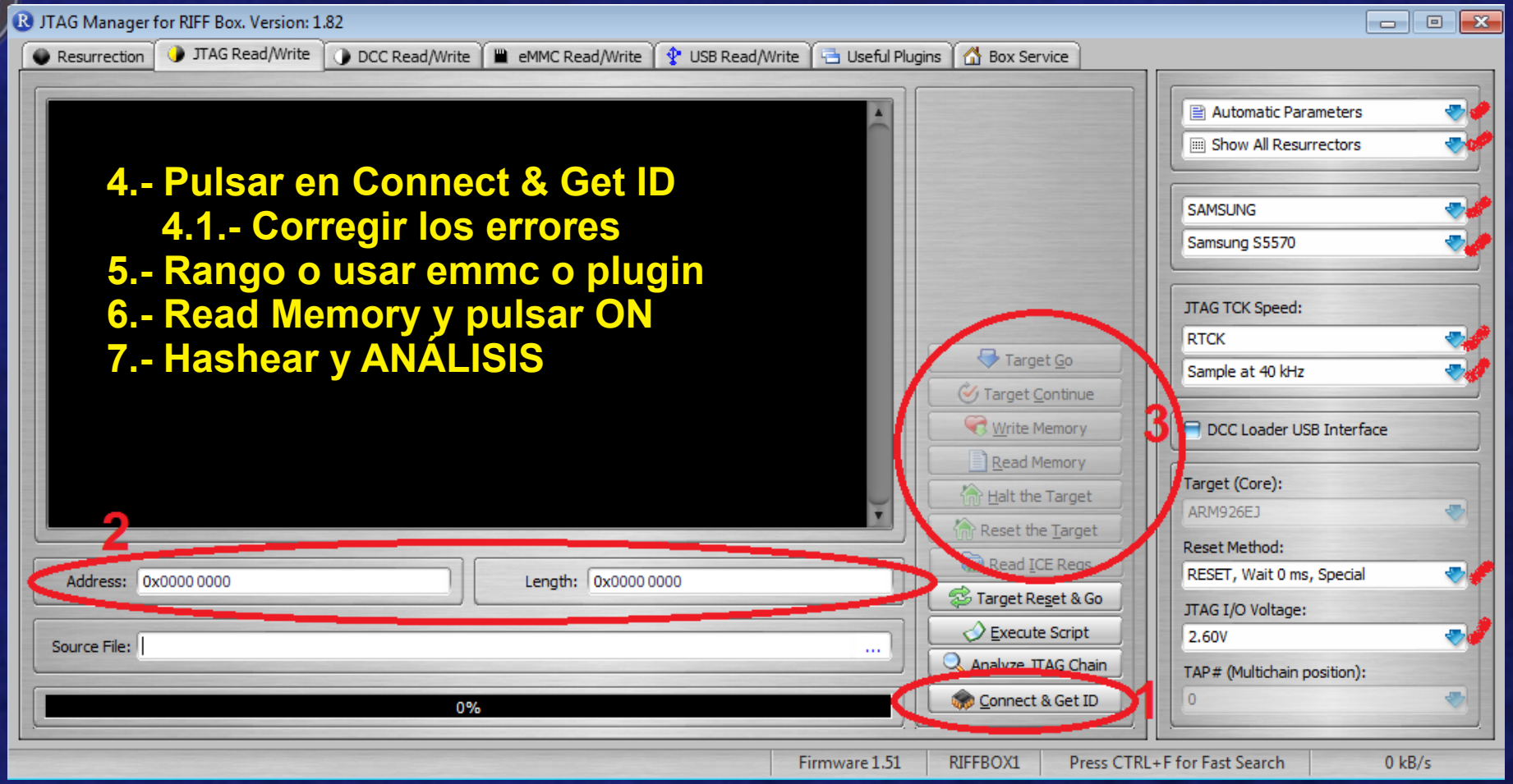
D.- JTAG con RiffBOX a Samsung s5570



D.- JTAG con RiffBOX a Samsung s5570



D.- JTAG con RiffBOX a Samsung s5570



E.- ISP con emmcPRO BOX sam i9100

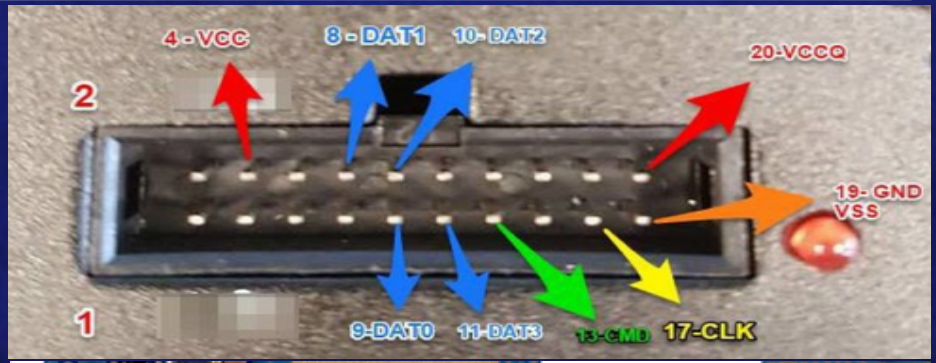
1.- Realizar las soldaduras ISP

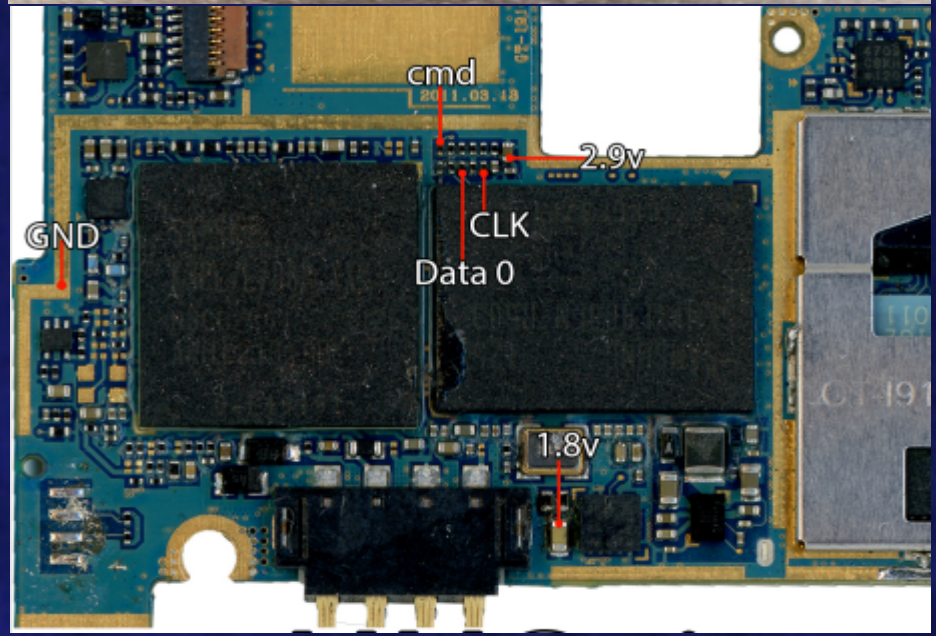
2.- Abrir el software de emmcPRO

3.- Revisar las ayudas para los pinout

VCC = 1.8v

VCCQ = 2.8v





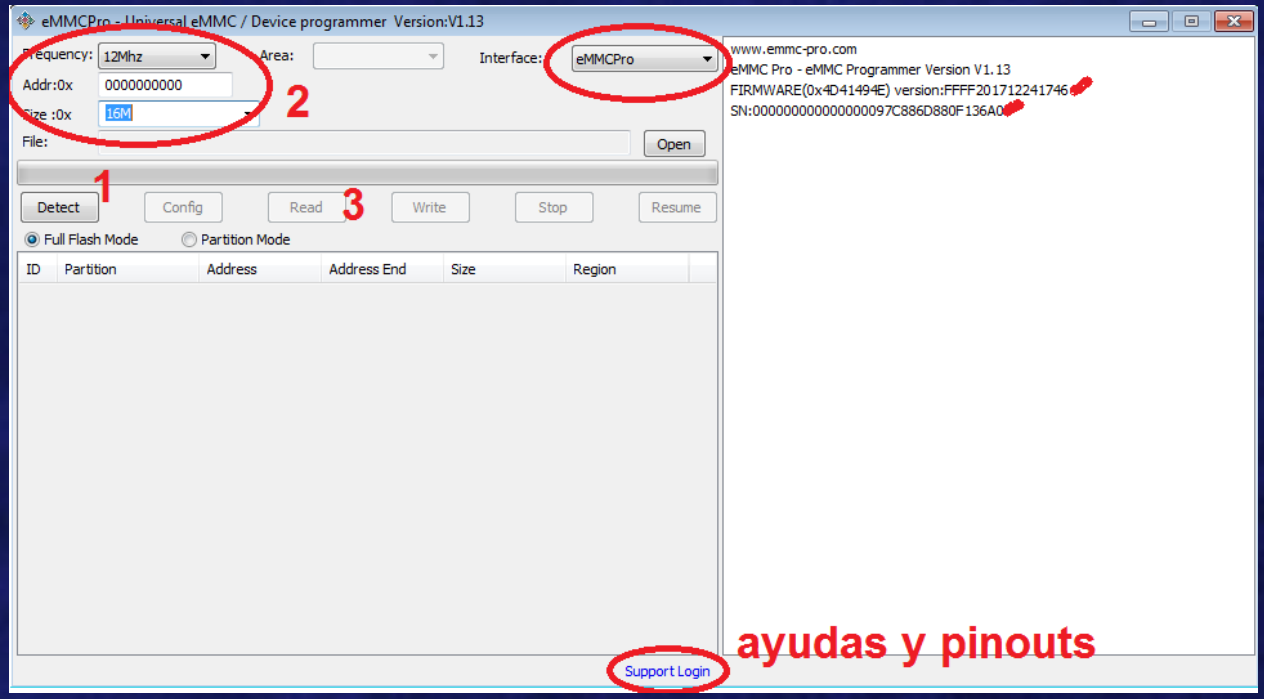
E.- ISP con emmcPRO BOX sam i9100

4.- Seleccionar Interface emmcPRO

5.- Detect y configurar (2 s.e.n.)

6.- Read

7.- Hashear y ANÁLISIS



F.- ISP con Medusa PRO BOX i9505

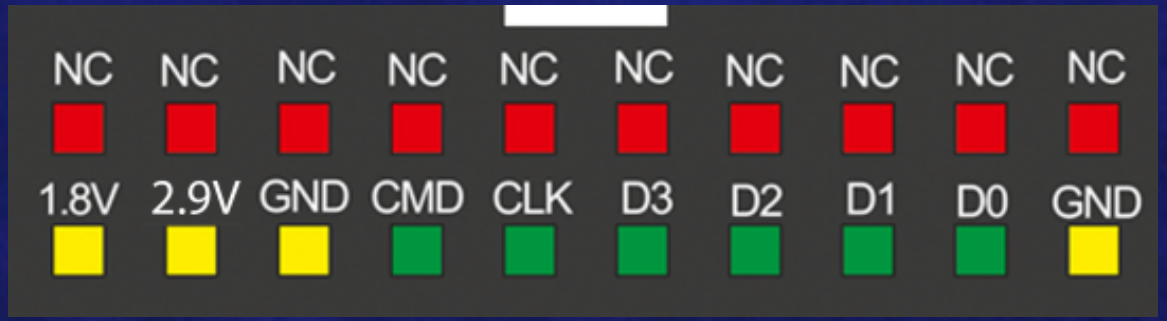
1.- Realizar las soldaduras ISP

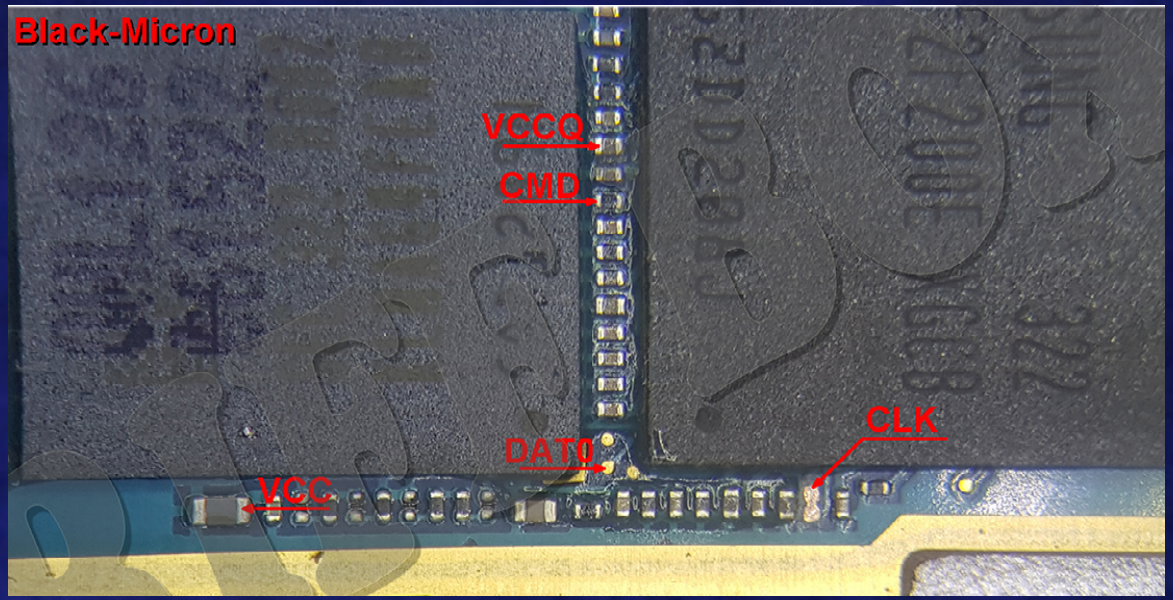
2.- Abrir el software de MedusaPRO

3.- Revisar las ayudas para los pinout

VCC = 1.8v

VCCQ = 2.8v





F.- ISP con Medusa PRO BOX i9505

4.- Seleccionar Interface (emmc)

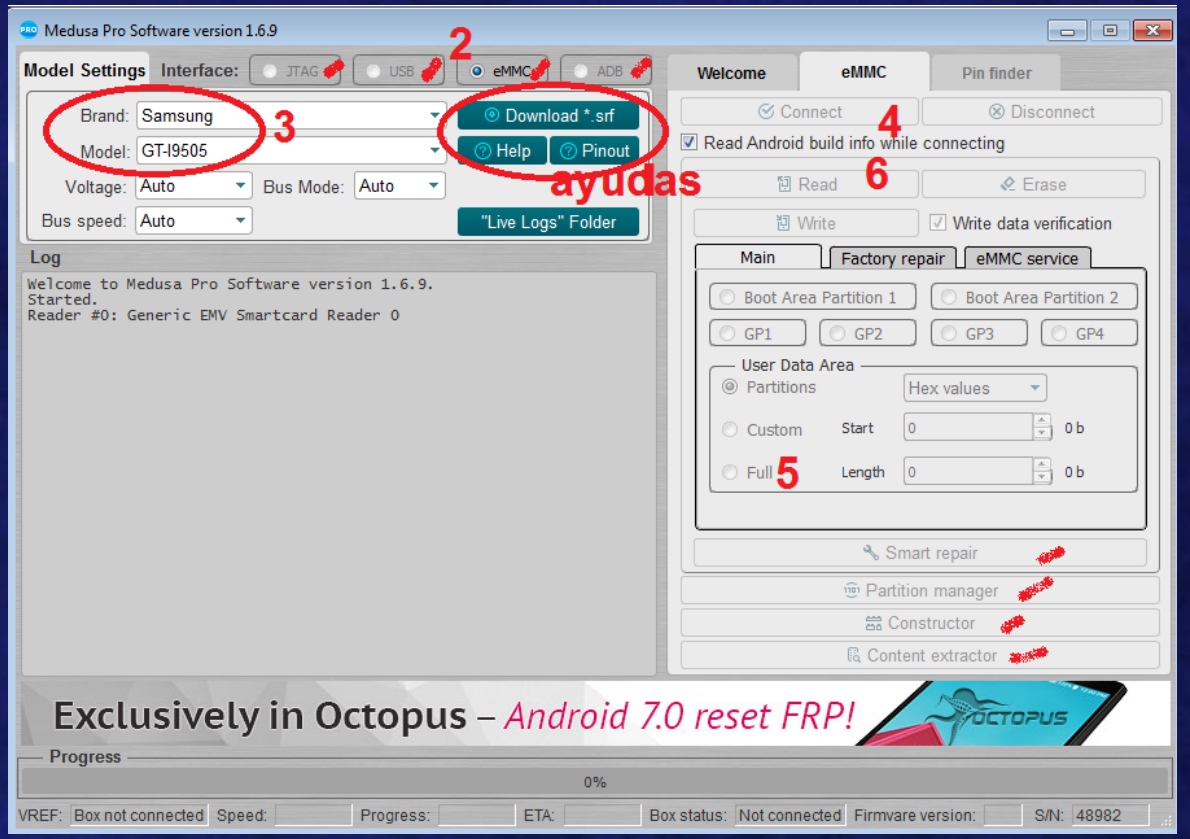
5.- Seleccionar marca - modelo

6.- Conect y corregir errores

7.- Seleccionar tamaño lectura (full)

8.- Read (elegir si queremos BUILD)

9.- Hashear y ANÁLISIS

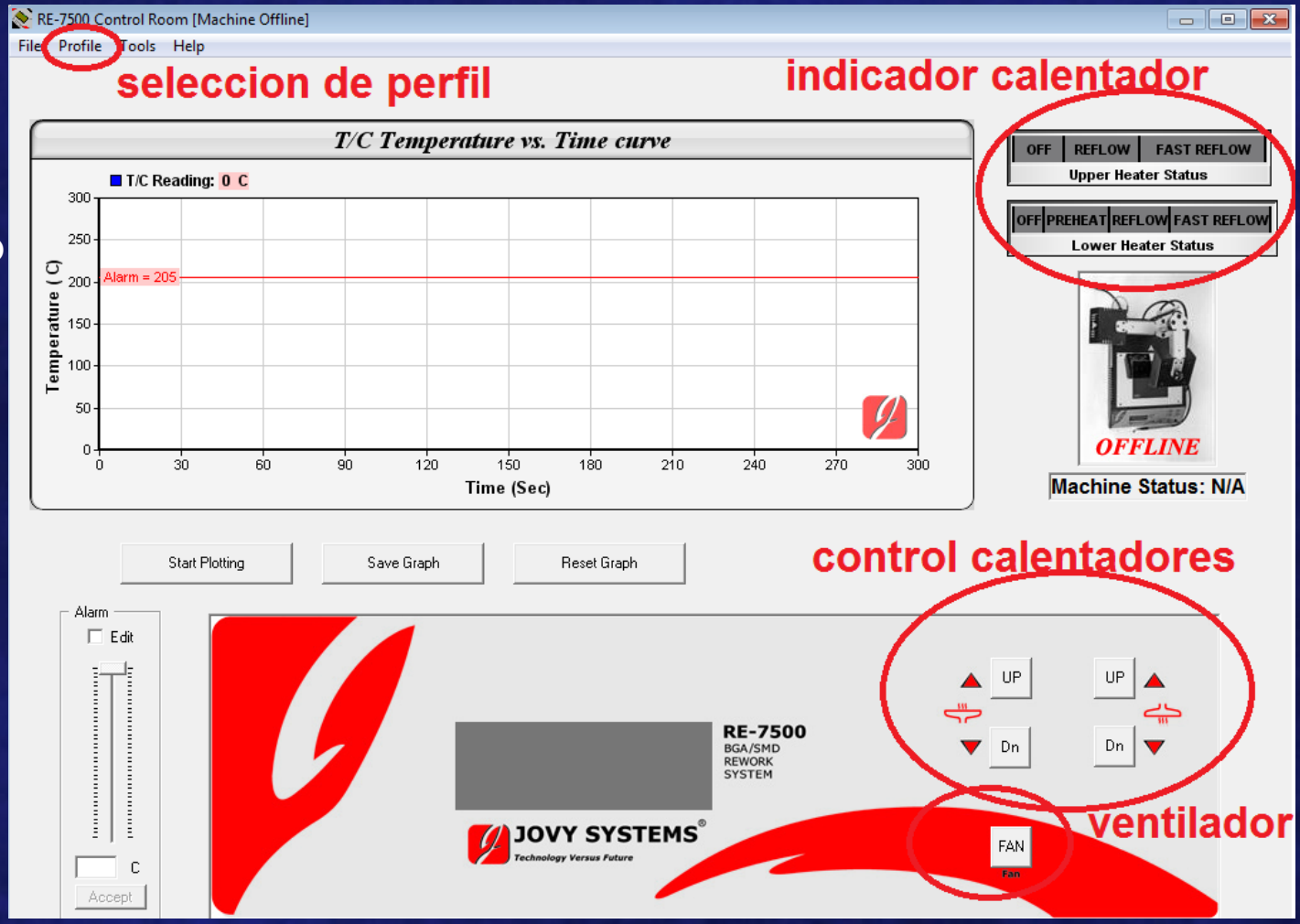


G.- Chip Off y adaptador MOORC-SD

1.- usar indicaciones de uso y protección de la placa

2.- TERMOMETRO!!!!!!!!!

3.- crear o cargar PROFILE



G.- Chip Off y adaptador MOORC-SD

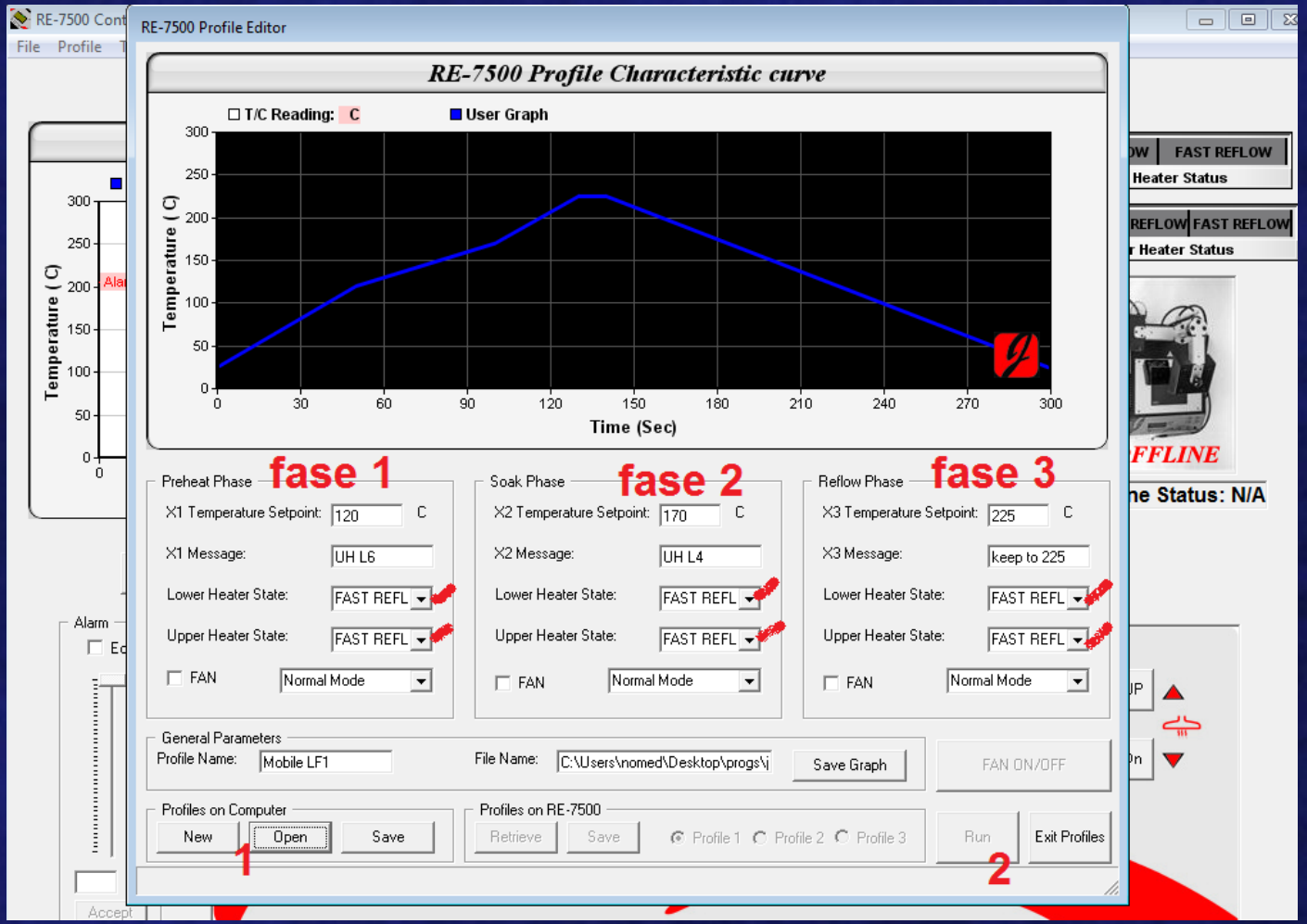
3.- configurar el perfil

4.- RUN

5.- NORMAL MODE
(girar brazos de máquina)

6.- quitar chip con PUMP

7.- limpiar el chip



G.- Chip Off y adaptador MOORC-SD

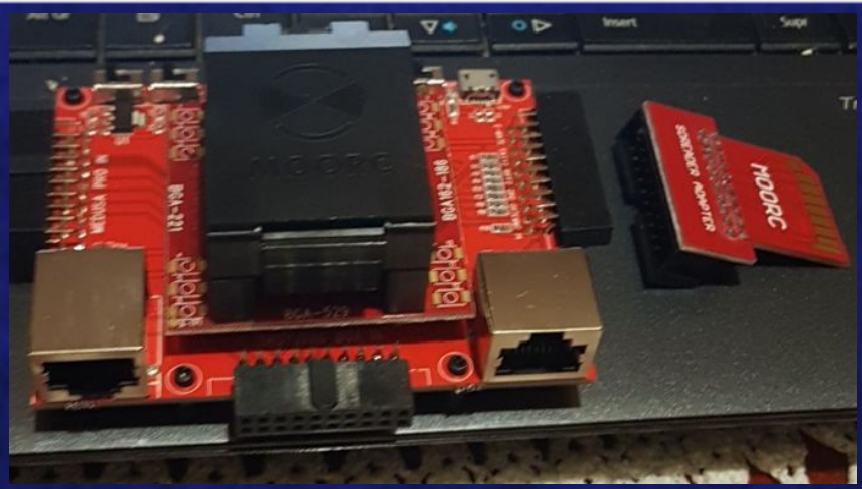
8.- Poner el chip en el MOORC con un SD MOORC adapter

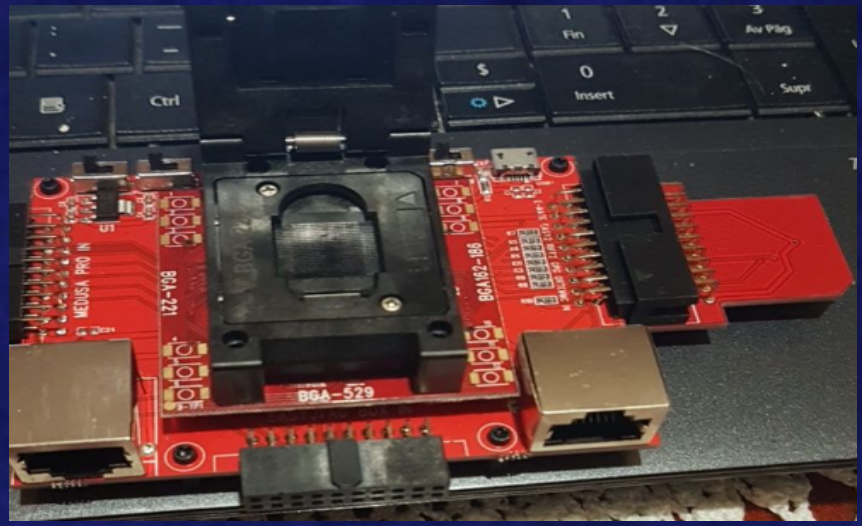
9.- Usar un lector de memorias

10.- montar con:

10.1. FTK imager

10.2. MV Kali linux (p.ej.)

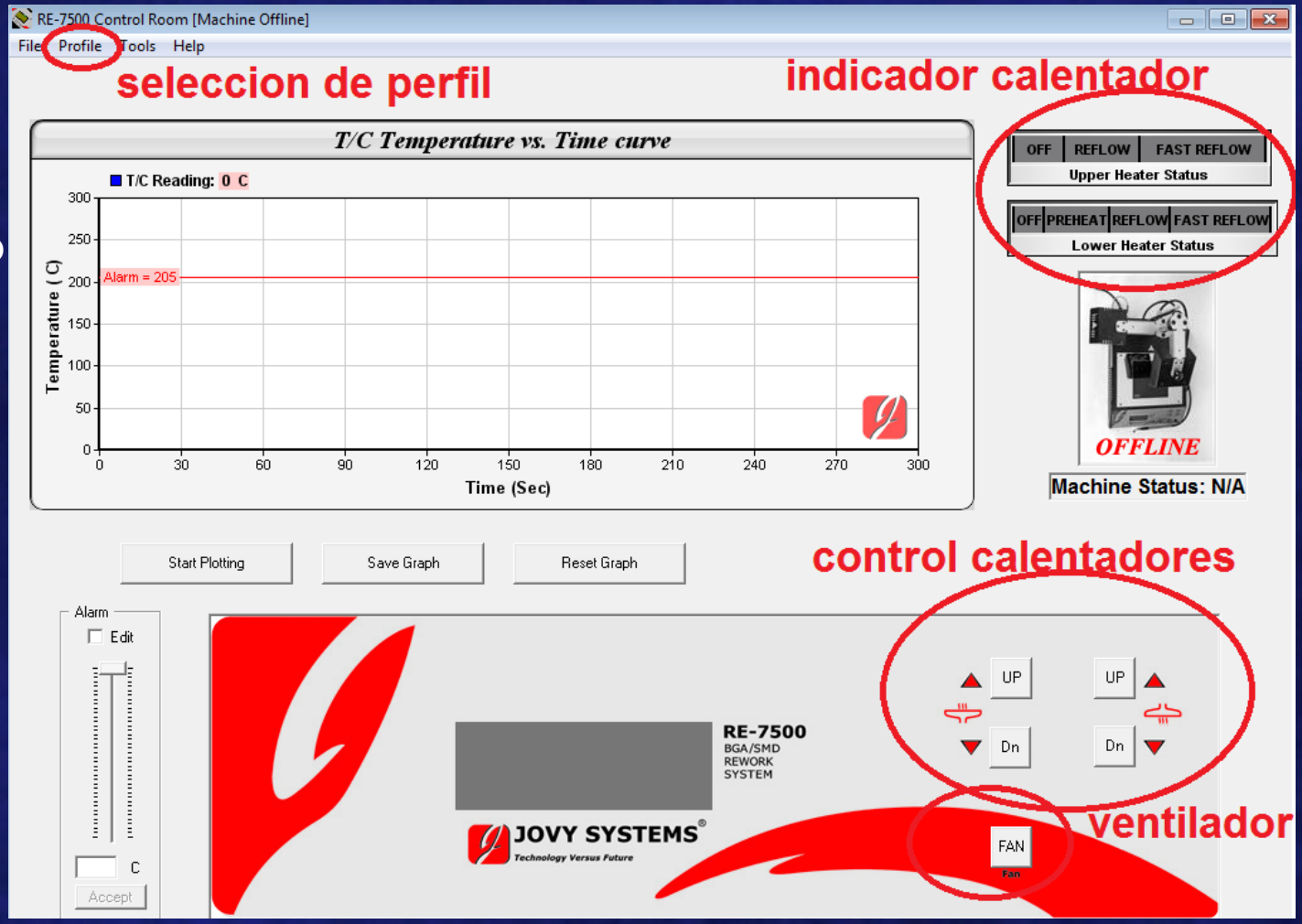




H.- Chip Off sin adaptador emmcBOOSTER

1.- usar indicaciones de uso

2.- crear o cargar PROFILE



H.- Chip Off sin adaptador emmcBOOSTER

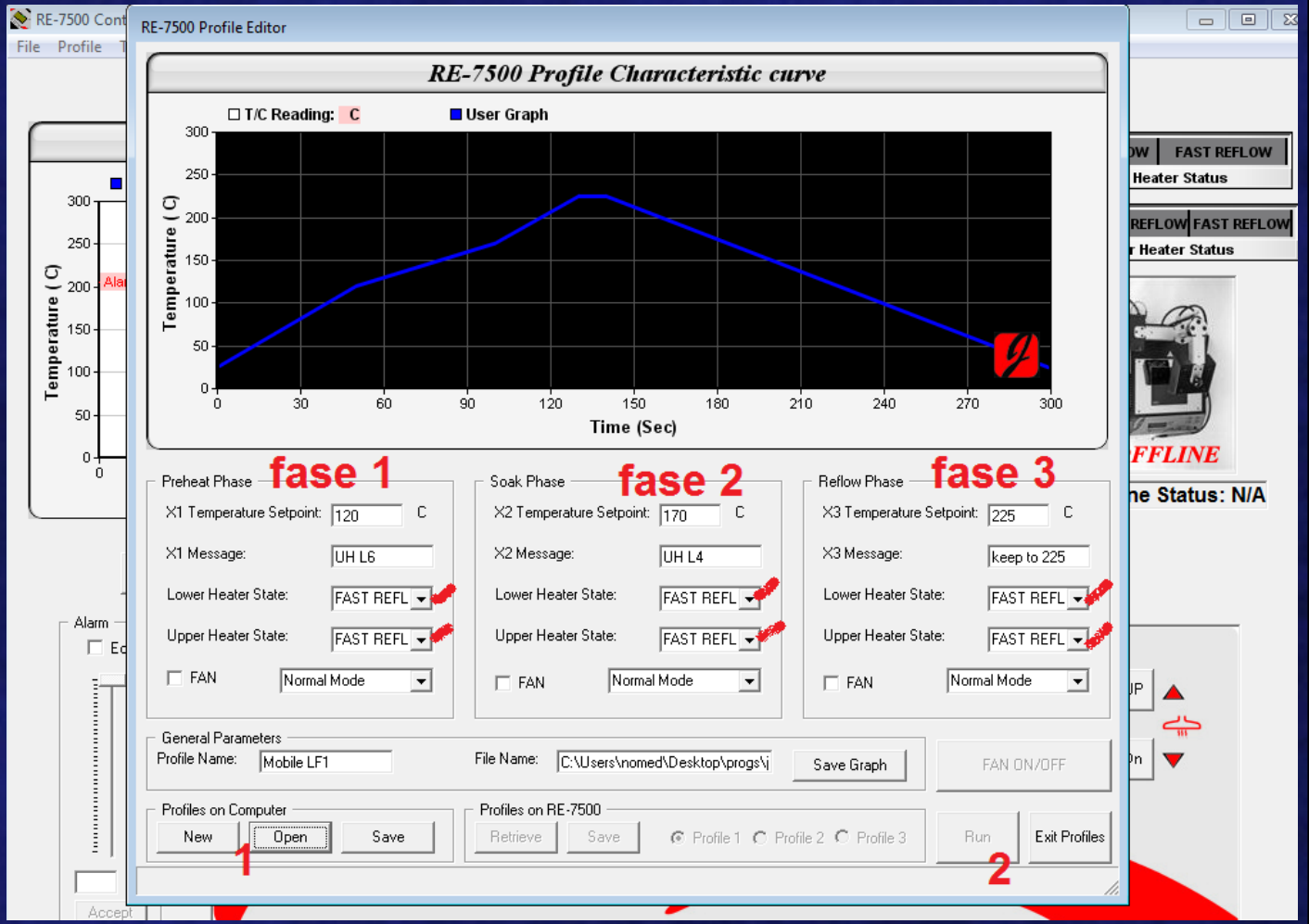
3.- configurar el perfil

4.- RUN

5.- NORMAL MODE
(girar brazos de máquina)

6.- quitar chip con PUMP

7.- limpiar el chip



H.- Chip Off sin adaptador emmcBOOSTER

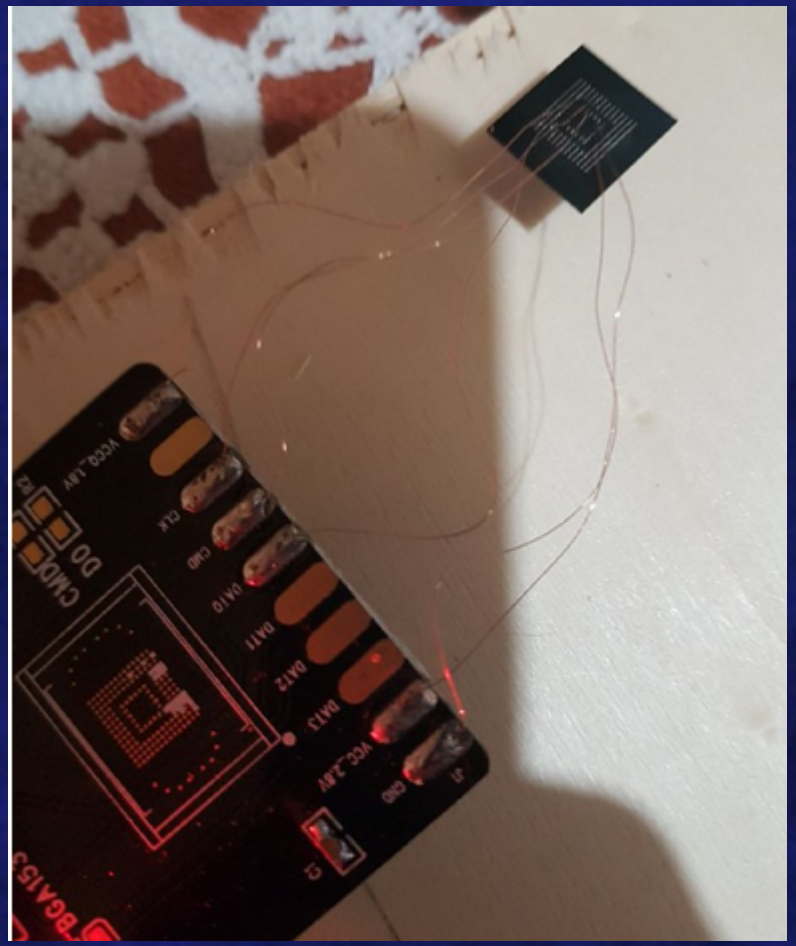
8.- Soldamos los 6 pinouts con hilo de cobre, mirar el dataset

9.- Enchufar a emmc BOOSTER (podemos usar un adaptador sd)

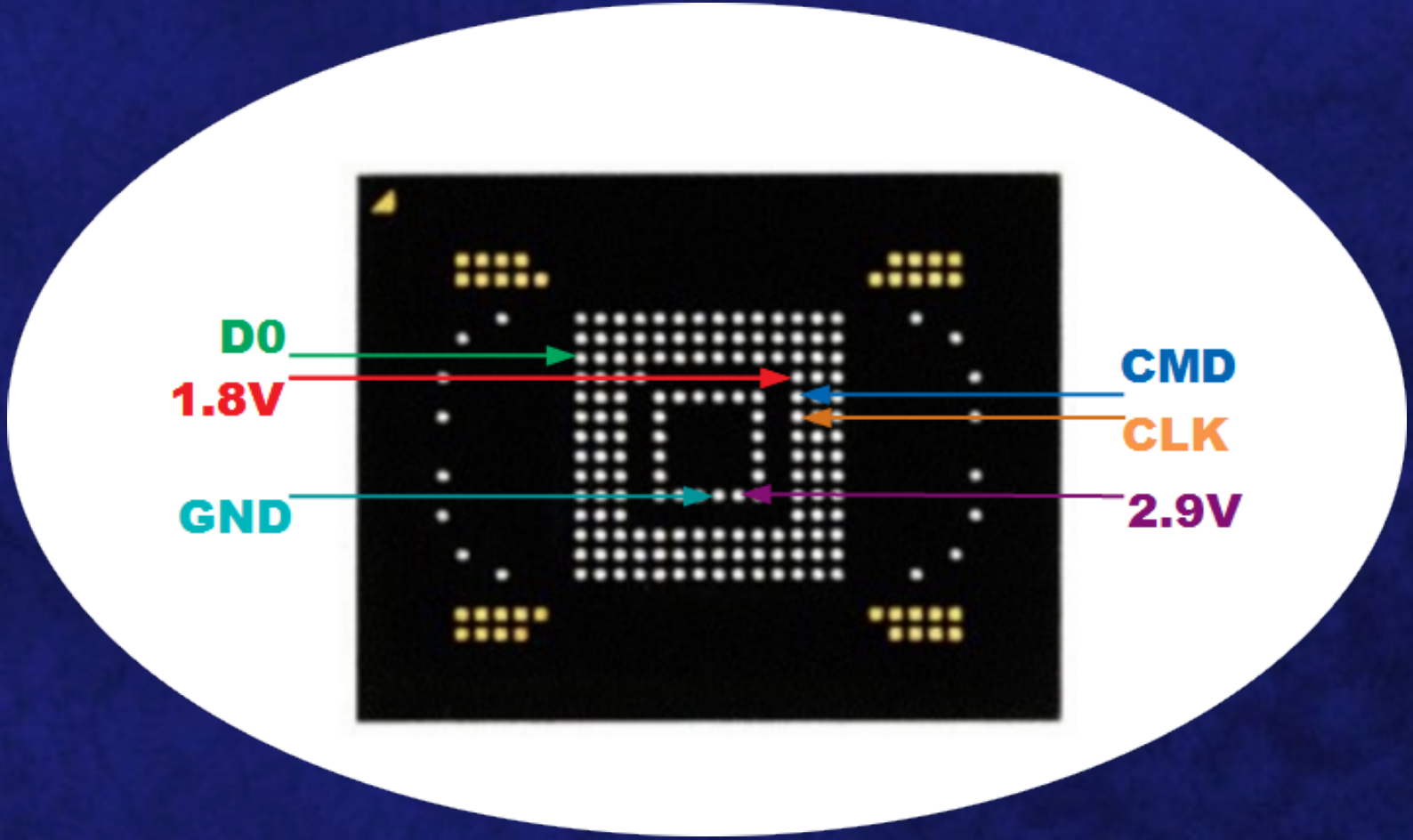
10.- montar con:

10.1. FTK imager

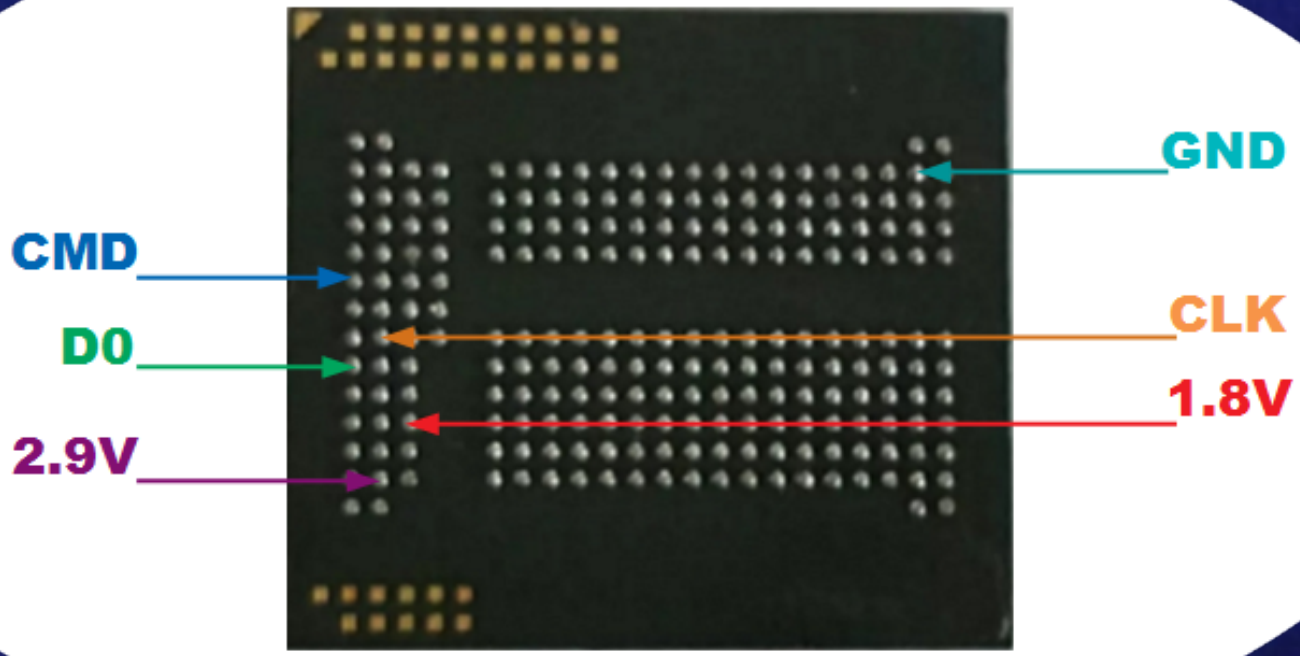
10.2. MV Kali linux (p.ej.)



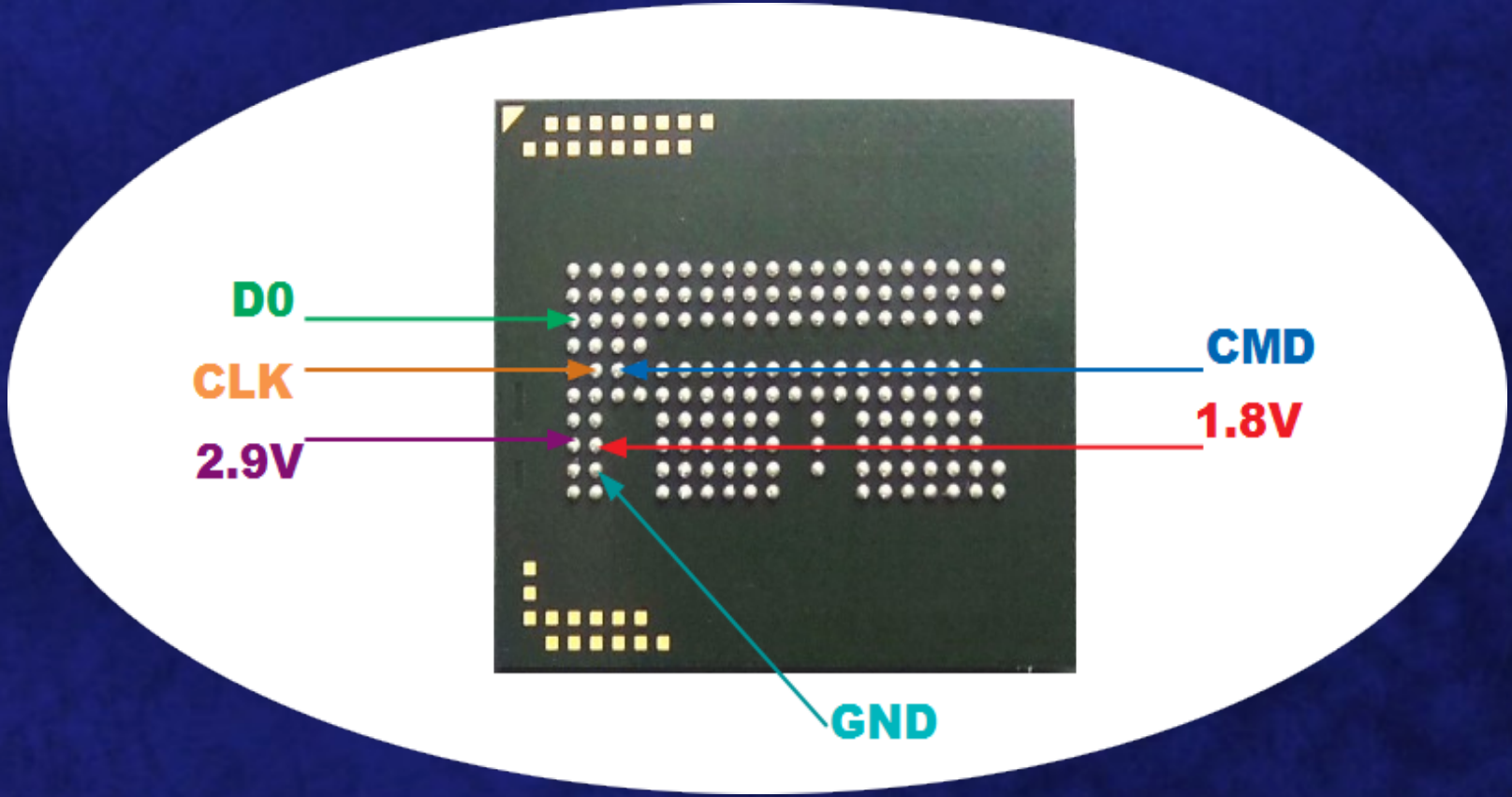
Info general: BGA 153/169



Info general: BGA 221



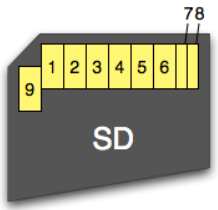
Info general: BGA 162/186



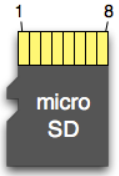
Info general: encapsulados

Info general: pinouts SD

- VCCQ(1.8v)
- VCC(2.8v/3.7v)
- GND(vss)
- CMD
- CLK
- D0..Dx

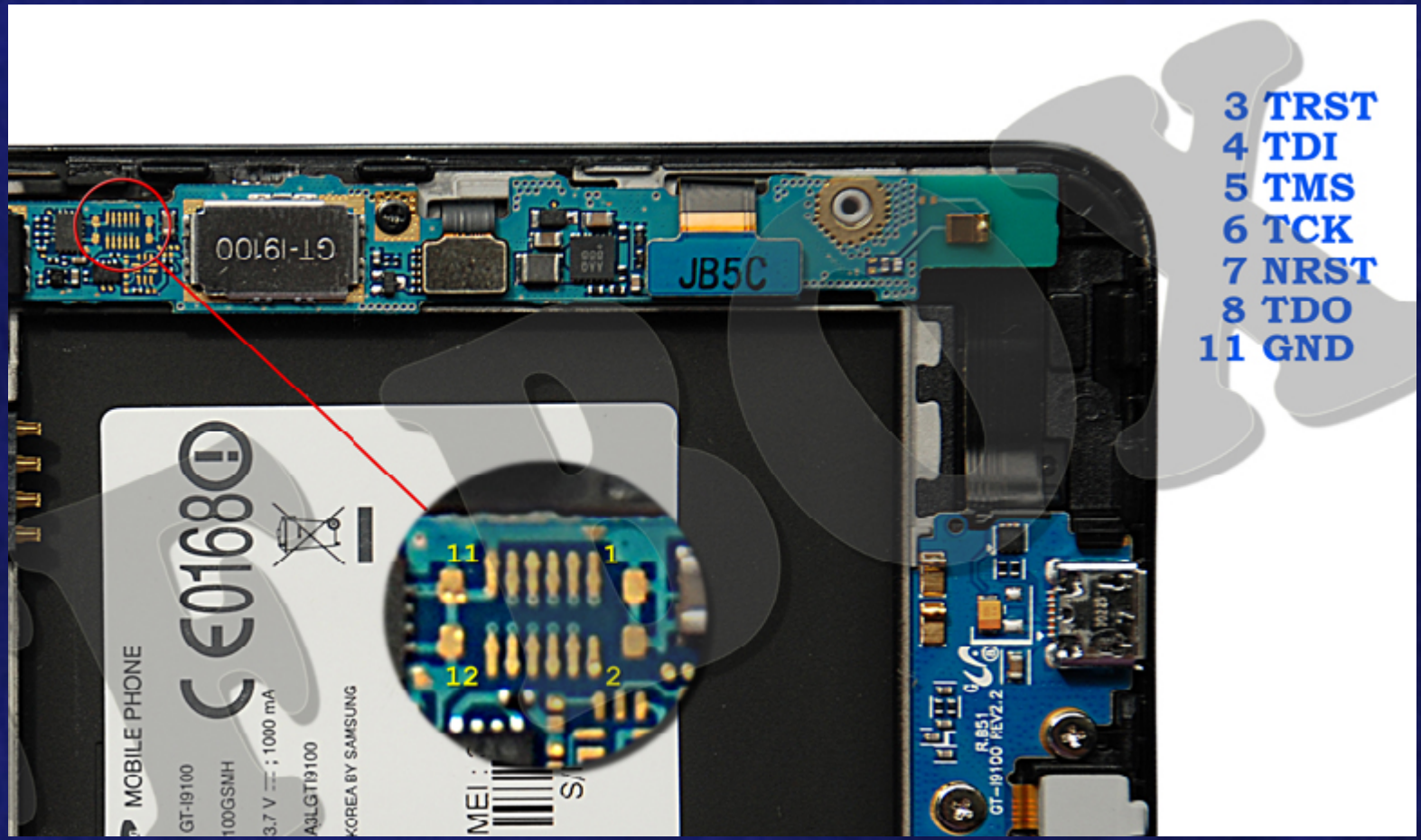


Pin	SD	SPI
1	CD/DAT3	CS
2	CMD	DI
3	VSS1	VSS1
4	VDD	VDD
5	CLK	SCLK
6	VSS2	VSS2
7	DAT0	DO
8	DAT1	X
9	DAT2	X

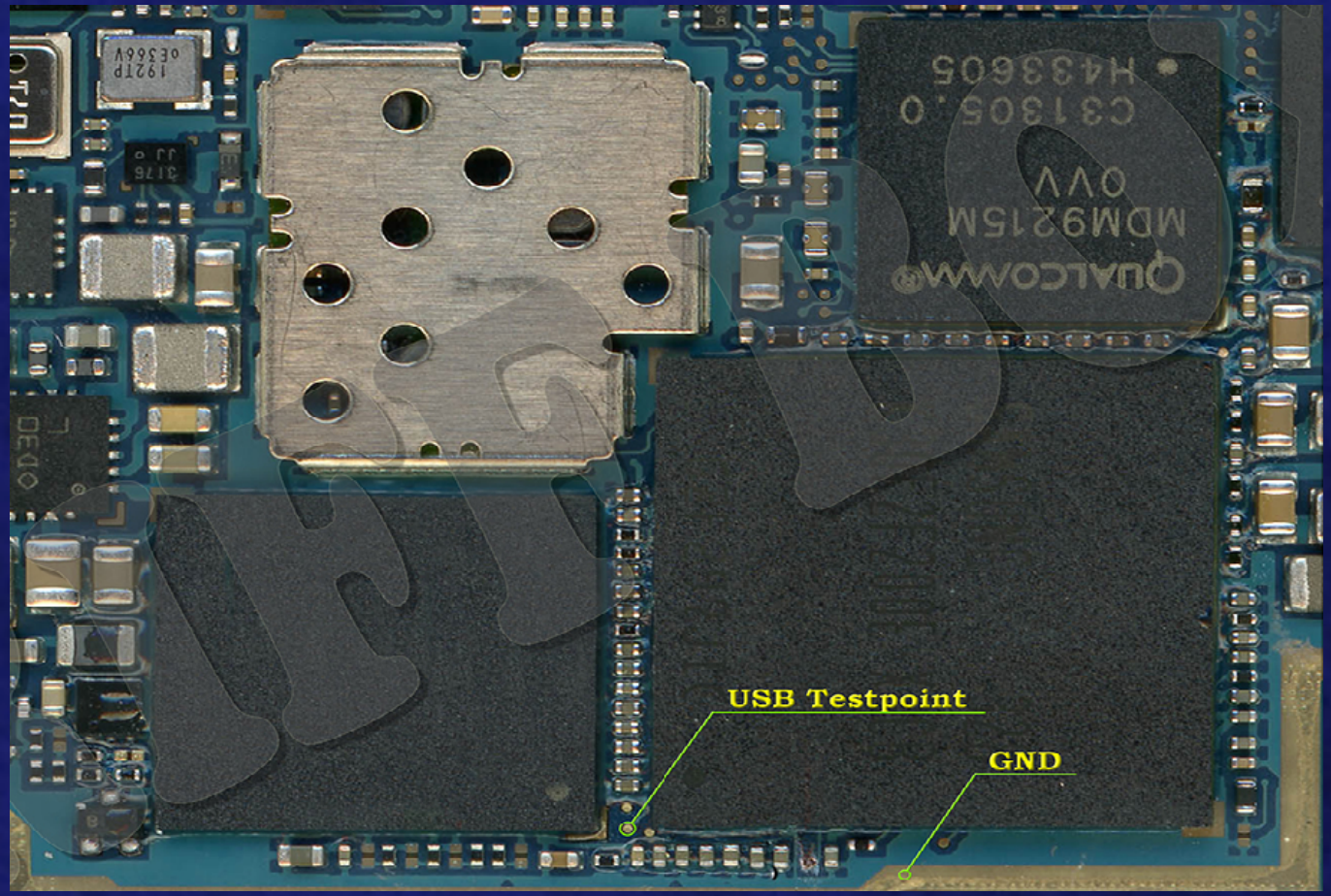


Pin	SD	SPI
1	DAT2	X
2	CD/DAT3	CS
3	CMD	DI
4	VDD	VDD
5	CLK	SCLK
6	VSS	VSS
7	DAT0	DO
8	DAT1	X

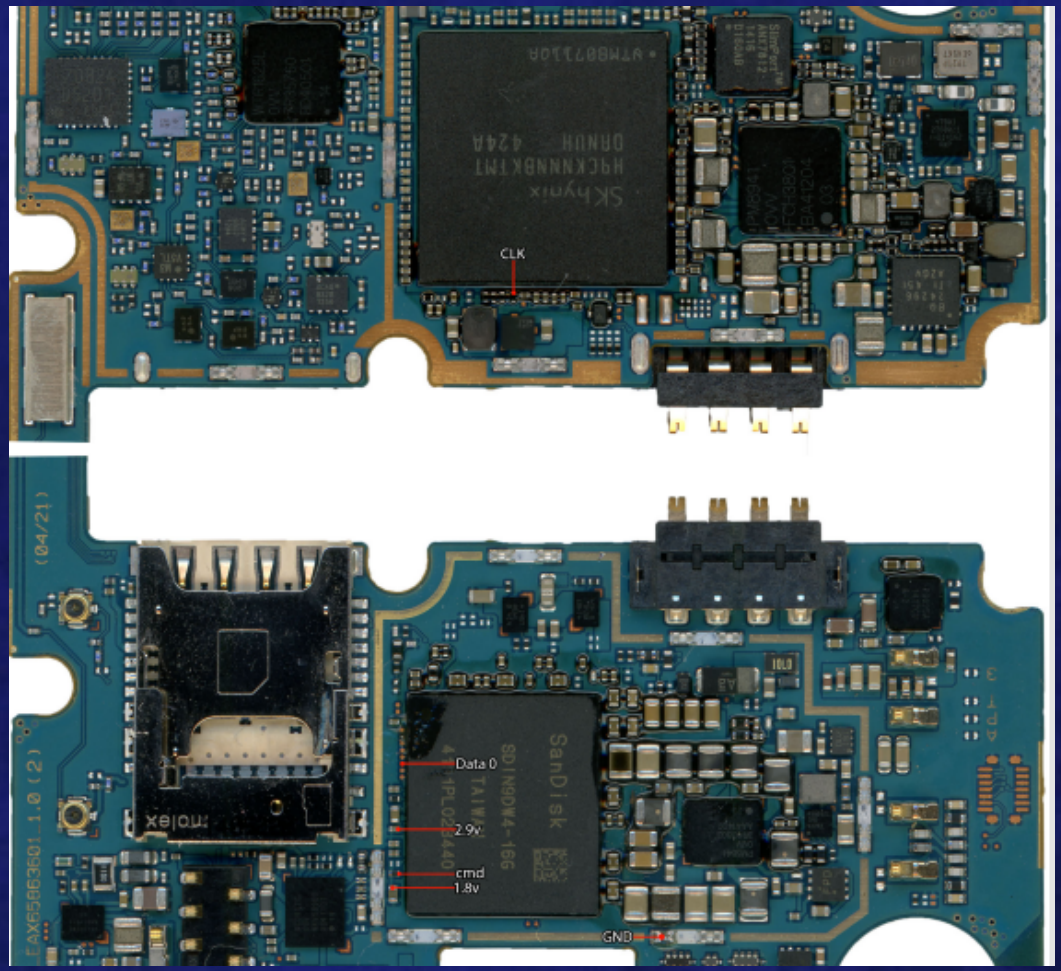
Info general: SAMSUNG i9100 S2 JTAG



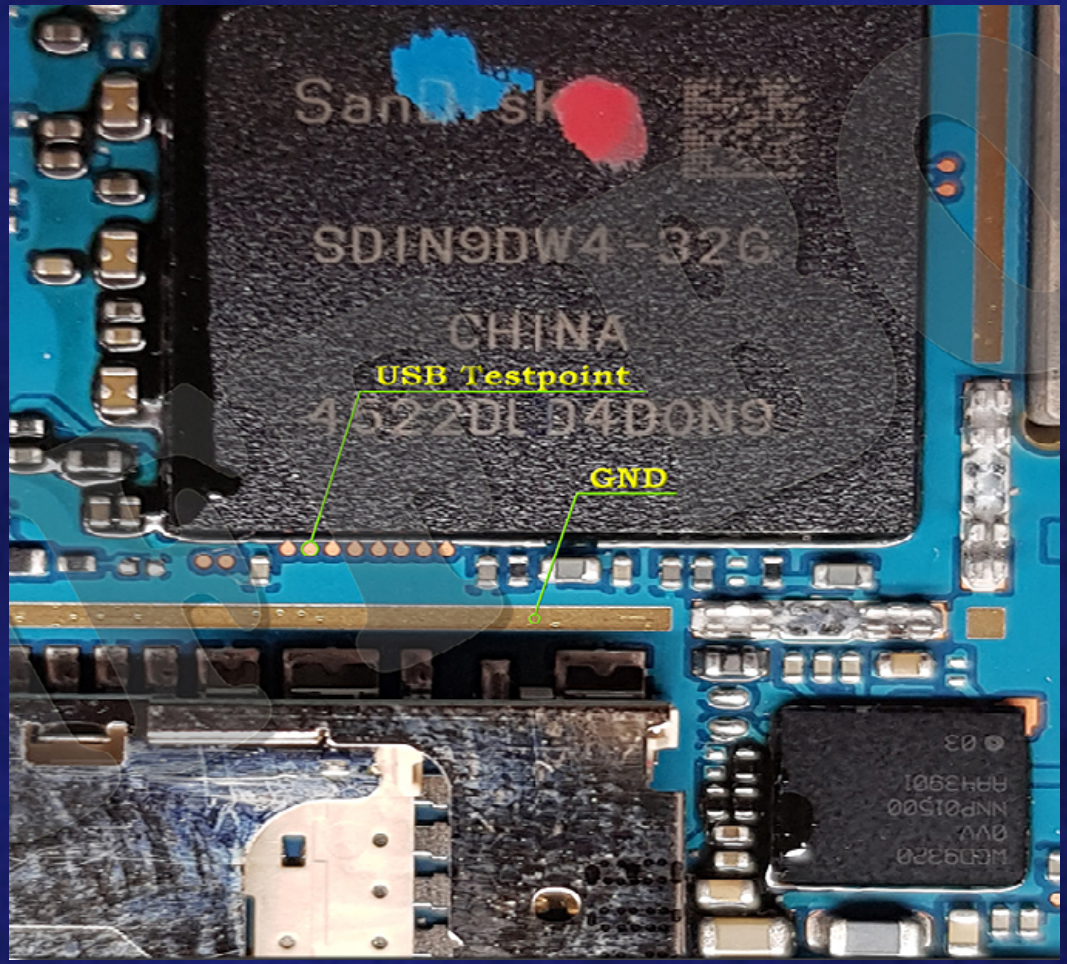
Info general: SAMSUNG i9505 S4 TP



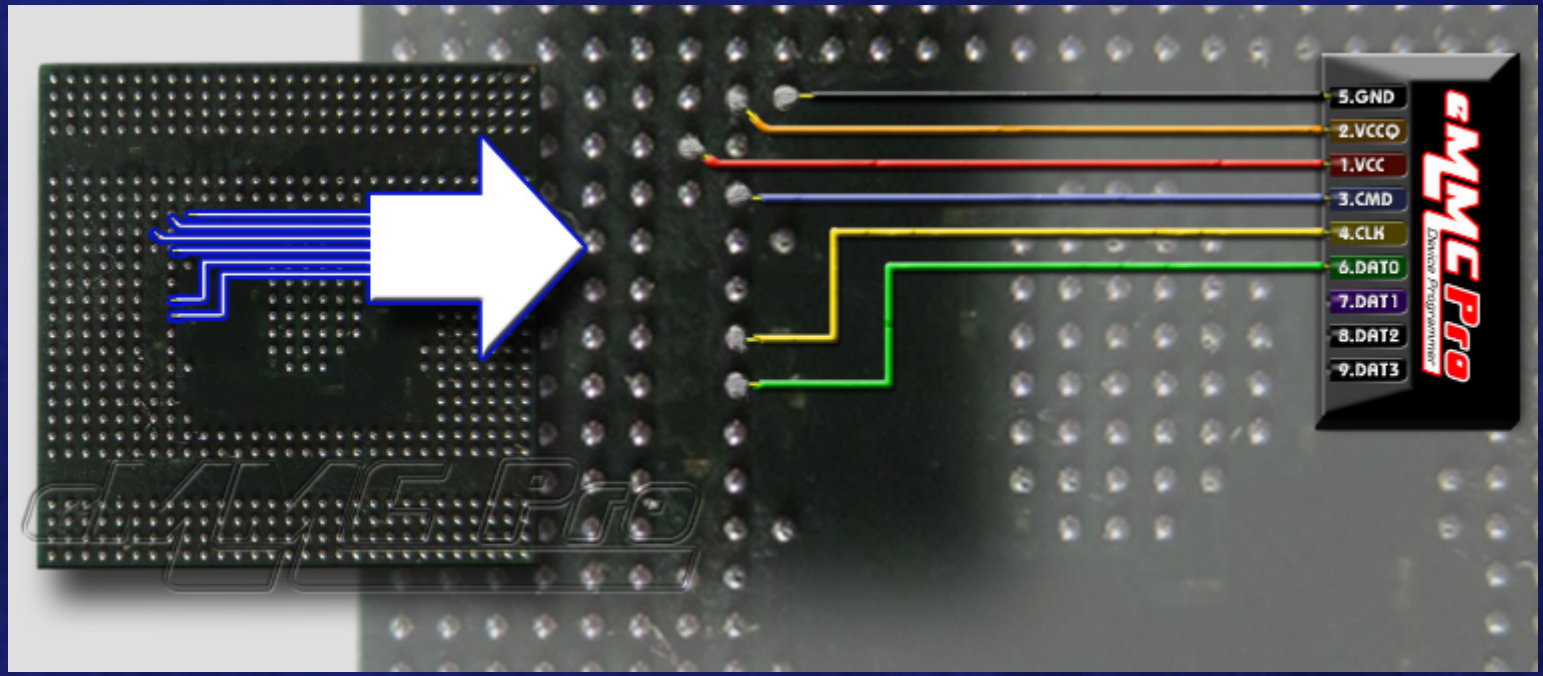
Info general: LG D855 G3 ISP



Info general: LG D855 G3 TP



Info general: SAM N910F NOTE4 CHIP-OFF



Agradecimientos

A TODOS LOS PRESENTES

A LA ORGANIZACIÓN DE HONEY CON 2018 y HONEYSEC

A COMUNIX GROUP Y SU BLOG

A ANTONIO SANZ y SARA siempre por su aportaciones y revisiones

!!!!!!!!!!!!! MUCHAS GRACIAS !!!!!!!!!!!!!!!!!!!

comunix

Preguntas