



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

Buenaventura Salcedo Santos-Olmo

```
Co
Fi
Lo
Copied recover
Fixing /system/app permissions...
Fixing permissions
Fixing /data/app permissions...
Loading packages
Fixing /data/data/permissions
Permissions
Permissions
Permissions
Partition details...
Number of partitions to back
of all data: 1056MB
Updating partition details
* Available space: 7559MB
* Total number of partitions to back up: 5
* Total size of all data: 1056MB
[BACKUP STARTED]
* Available space: 7559MB
* Backup Folder: /sdcard/TWRP/BAC
Backing up System...
[BACKUP STARTED]
* Backup Folder: /sdcard/TWRP/BACKUPS/509F2
Backing up System...
```



Quien soy yo

Casi Graduado en Ingeniería Informática en la UNED

CEO Servicio Técnico de telefonía móvil e informática



nomed1



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

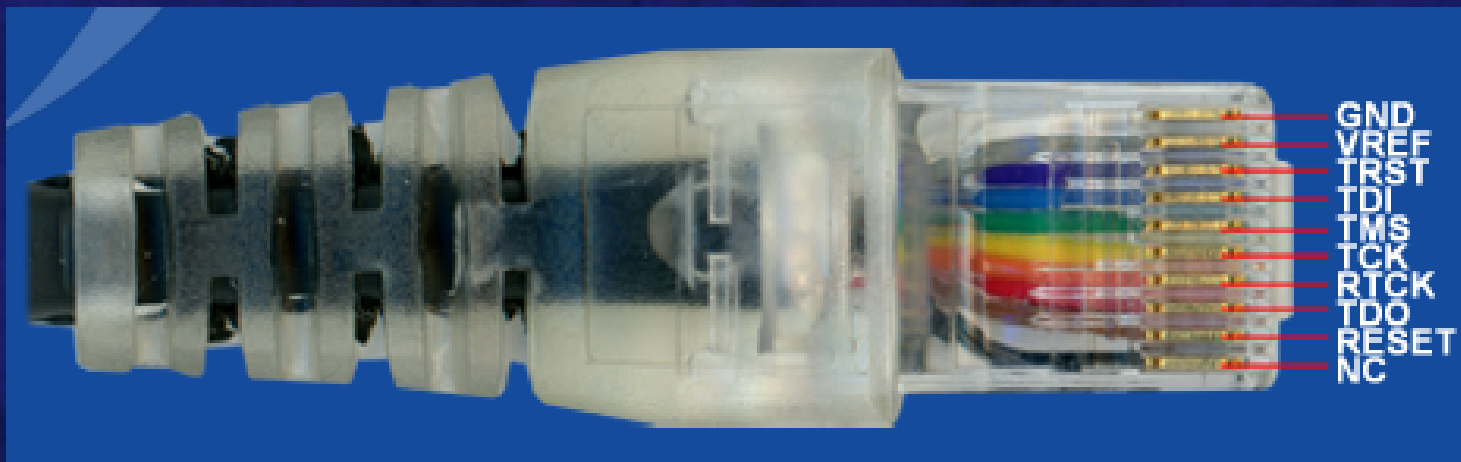
JTAG Interface



- 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



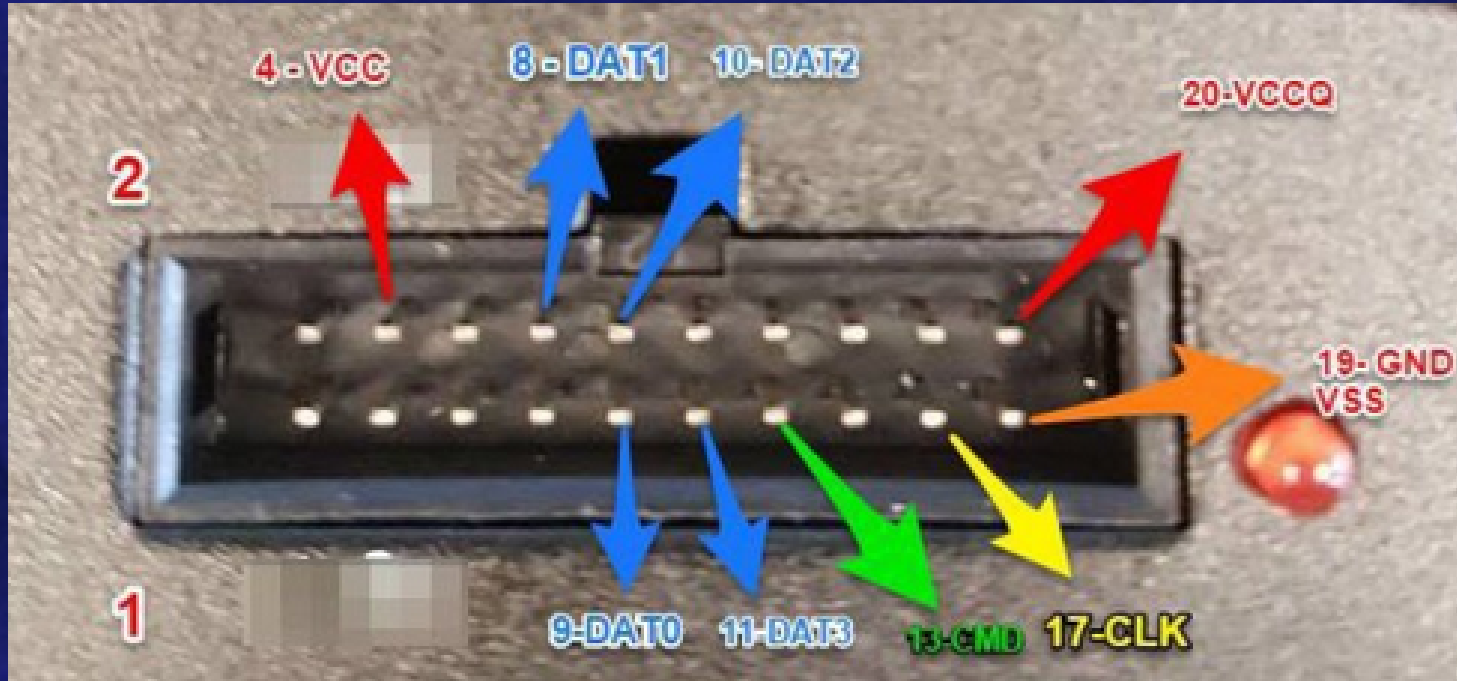


MEDUSA PRO PINOUT INFO

NC	NC	NC	NC	NC	NC	NC	NC	NC	NC
1.8V	2.9V	GND	CMD	CLK	D3	D2	D1	D0	GND



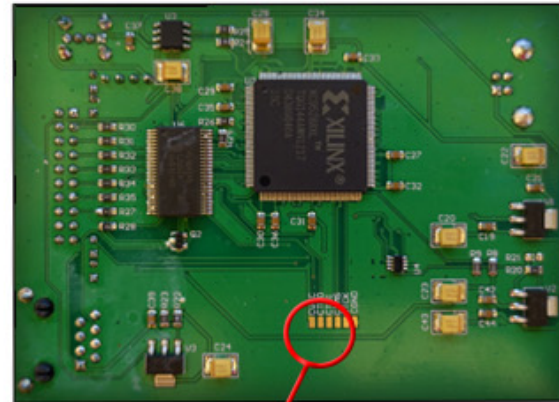
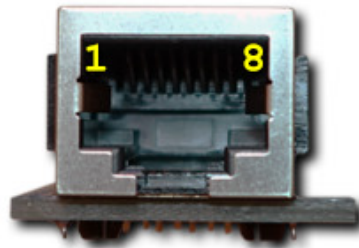
EMMC PRO PINOUT INFO



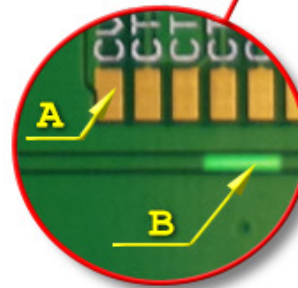


RIFF BOX PINOUT MODIFICATION

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

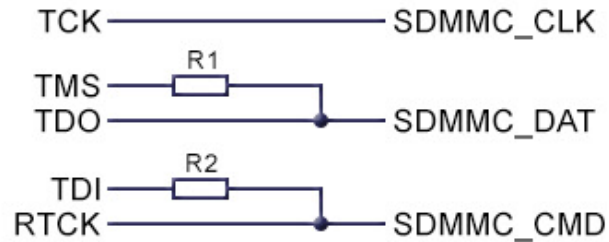


RIFF BOX PINOUT JTAG INFO

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

Chinese Miracle II (MTK Module , ver 1.58) by Infinity-Box Team (c) 2014-2016

File Settings Help

Log

Card found: F/W: 64528723, 6136
Chinese Miracle II [MTK module] v 1.58

Settings Service Security **Flash** Extra UserData / Forensic

CPU / Platform / WorkMode

FP : Auto [625A..6261] [6255..6276] NOR|NAND

FP : Auto [625A..6261] [6255..6276] NOR|NAND

SP : Auto [2601] [6571..6595] [6732..6797] [81|83|87xx] NAND|eMMC

SP : Auto [625A..6261] Nokia MTKx

SP : Select Model [6571..6797]

Interface

USB [AutoDetect] Scan

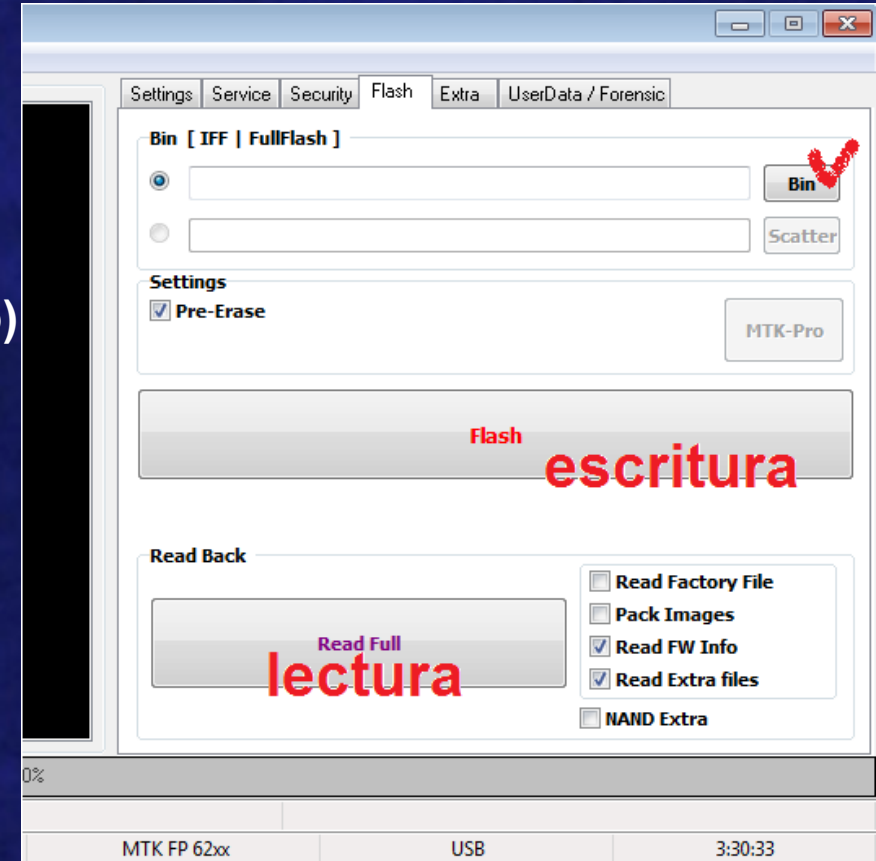
0%

READY MTK FP 62xx USB 3:23:54



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

Chinese Miracle II (MTK Module , ver 1.58) by Infinity-Box Team (c) 2014-2016

File Settings Help

Log

Card found : S/N : 045187E3 , v0136
Chinese Miracle II [MTK module] v 1.58

Settings Service Security Flash Extra UserData / Forensic

SP Platform [Android]

Read Pattern / DP Reset UserLocks Reset Privacy Lock

DataProtect UserData Safe

FP Platform [Phone]

Reset User Code Read

User Memory Repartition

Check / Report

Direct Data Recovery Module [FP/SP]

Read Data

Extract Settings

PhoneBook Calls Vcard v3

SMS

Photo / Video / VoiceRec

0%

READY MTK FP 62xx USB 3:44:09



B.- TP con Infinity box (CM2QLM)

Chinese Miracle II (QLM Module , ver1.16) by Infinity-Box Team (c) 2017

File **Extra** 1

- EDL Boot
- Open MemoryTool** 2
- Diag Enable

MemoryMode : AUTO

Connection Settings

Interface : QC HSUSB EMERGENCY [USB]

Settings Service Flash UserData

Log

Card found: 013107E3, v0136
Infinity-Box Chinese Miracle Qualcomm Module [QLM] v 1.16

0%

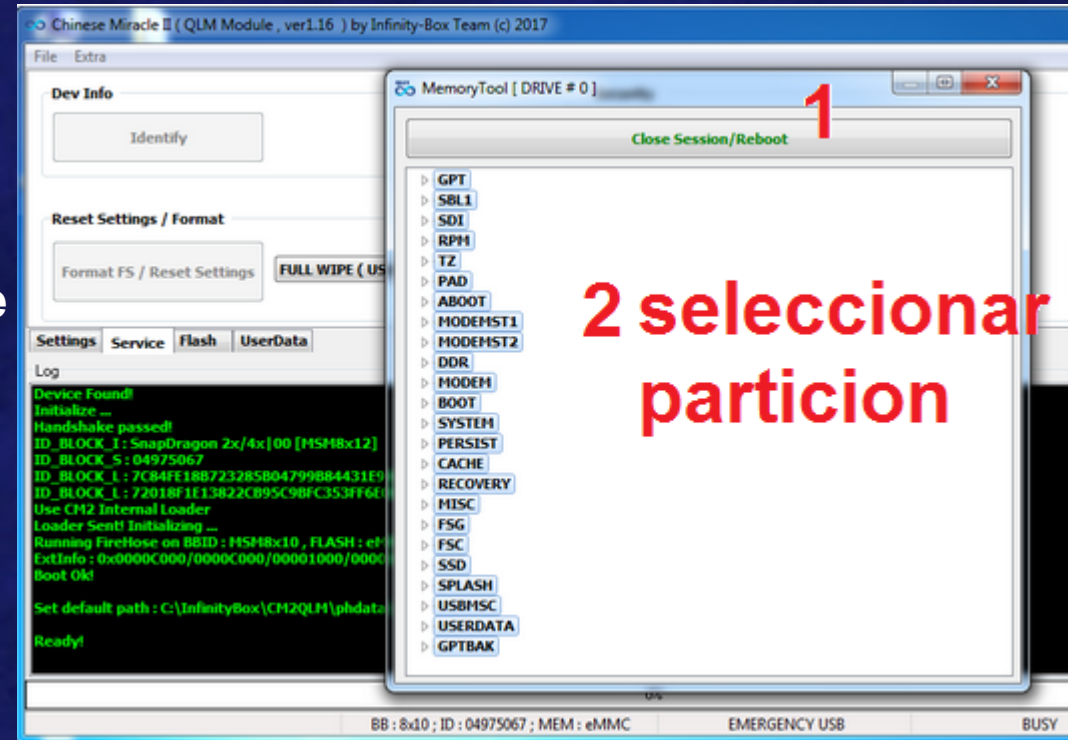
EMERGENCY USB READY 3:48:02



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



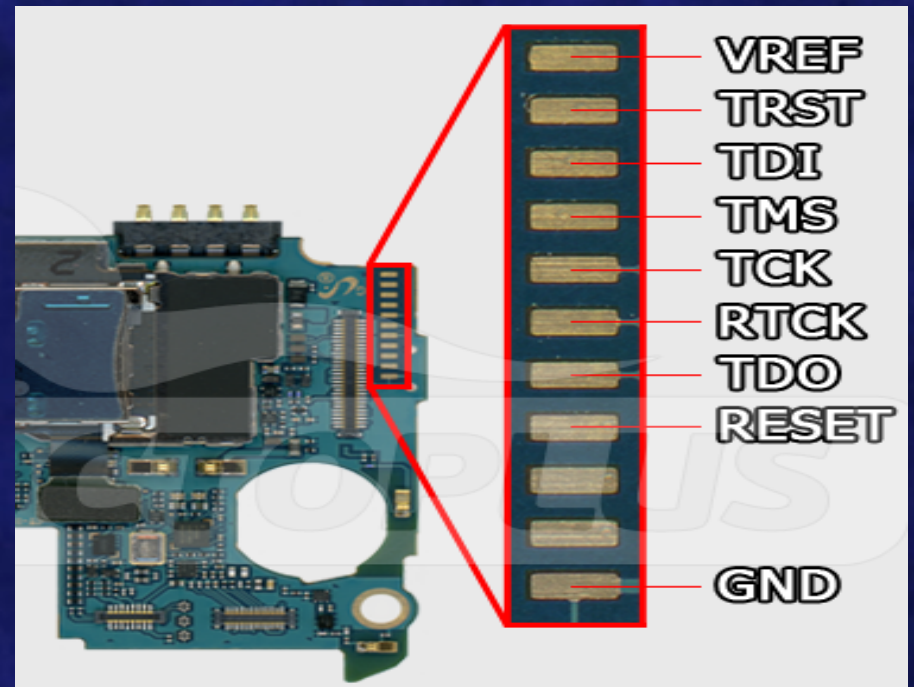
* No hace falta batería, antes de leer la partición asignar la ruta de almacenamiento



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

Medusa Box Software version 2.6.1.5

Support And Options | **Advanced** | Advanced Mode

Options

Manufacturer: Samsung **1**

Device model: Samsung GT-S5570 **2**

JTAG speed: Auto (RTCK)

? Help **3**

Actions

Connect **4** Disconnect

Read **6** Boot only

Write Full flash **5**

Erase Custom

Units: Kilobytes

Start: 0 0 b

Length: 0 0 b

Disable Write Protection

ECC Mode

Log

Welcome to Medusa Box Software version 2.6.1.5

OCTOPUS LG MORE THAN 1500 SUPPORTED MODELS G4, FLEX 2, NEXUS 5X...

Operation progress 0%

Status: Idle VREF: 0.00 V S/N: 00048982 Firmware: 1.1.0



D.- JTAG con RiffBOX a Samsung s5570



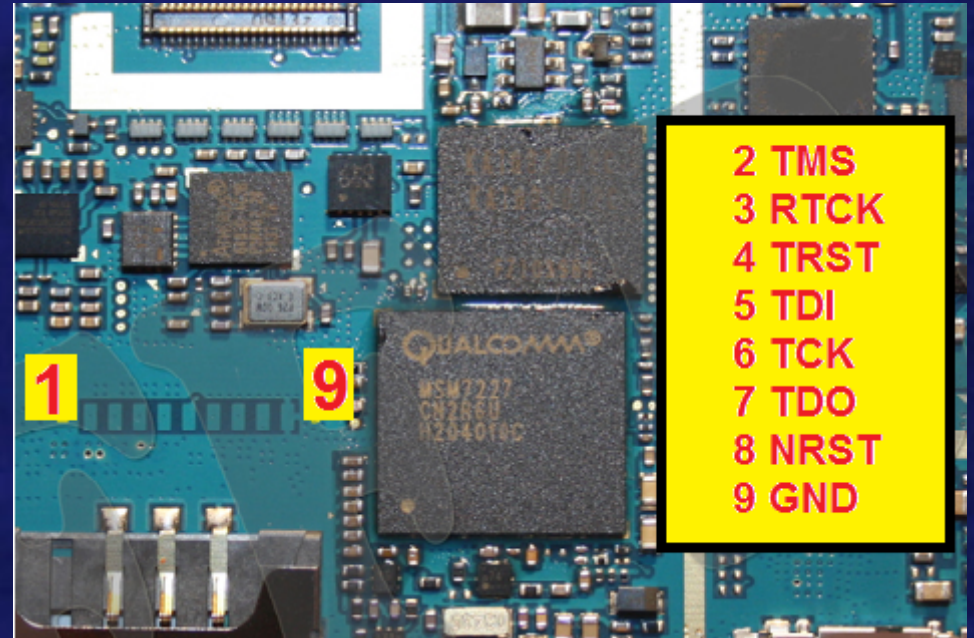
1 VCC	11 RTCK
3 TRST	13 TDO
5 TDI	15 NRST
7 TMS	2,17,19 GND
9 TDK	RESTO NO CONECTADOS

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

JTAG Manager for RIFF Box. Version: 1.82

Resurrection JTAG Read/Write DCC Read/Write eMMC Read/Write USB Read/Write Useful Plugins Box Service

Found and Initialized: 0 New and 20 Old External Repair Pack(s)

Automatic Parameters Show All Resurrectors

SAMSUNG Samsung S5570

JTAG TCK Speed: RTCK Sample at 40 kHz

DCC Loader USB Interface

Target (Core): ARM926EJ

Reset Method: RESET, Wait 0 ms, Special

JTAG I/O Voltage: 2.60V

TAP# (Multichain position): 0

AYUDA

Interface Pinout Resurrection Help RIFF BOX Pinout Search for DLL Resurrection

Ready Firmware 1.51 RIFFBOX1 Press CTRL+F for Fast Search 0 kB/s



D.- JTAG con RiffBOX a Samsung s5570

Equipo

JTAG Manager for RIFF Box, Version: 1.82

Resurrection JTAG Read/Write DCC Read/Write eMMC Read/Write USB Read/Write Useful Plugins Box Service

Connecting to the Updates Server...OK
Getting Updates Information from the Server...OK
Disconnecting from the Updates Server...OK

RIFF Updates Manager

- All Updates (1334)
 - JTAG Manager Root (7)
 - Resurrectors (1185)
 - HJAWEI (87)
 - LENOVO (15)
 - LG (171)
 - NOKIA (22)
 - SAMSUNG (450)
 - XIAOMI (11)
 - ZTE (53)
 - FLY (4)
 - HTC (167)
 - ONEPLUS (1)
 - ALCATEL (11)
 - MICROMAX (9)
 - MOTOROLA (19)
 - OPPO (5)
 - PRESTIGIO (1)
 - ACER (4)
 - ARCHOS (2)
 - ARTEL (2)
 - ASUS (14)
 - SONY (29)
 - INTEX (2)
 - TEXET (1)
 - PANTECH (25)
 - VOLKSWAGEN (1)
 - GENERAL MOBILE (1)
 - MEGAFON (1)

Position	Download	File Path	File Name
1	No	Resurrectors	Samsung_G355H_ISP.dll
2	No	Resurrectors	Samsung_G532G_ISP.dll
3	No	Resurrectors	Samsung_J200F_ISP.dll
4	No	Resurrectors	Samsung_J330F_ISP.dll
5	No	Resurrectors	Samsung_TS85_ISP.dll
6	No	Resurrectors	Samsung_G150NS_ISP.dll
7	No	Resurrectors	Samsung_G350E_ISP.dll
8	No	Resurrectors	Samsung_G361F_ISP.dll
9	No	Resurrectors	Samsung_I9060M_ISP.dll
10	No	Resurrectors	Samsung_E250K_ISP.dll
11	No	Resurrectors	Samsung_E250S_ISP.dll
12	No	Resurrectors	Samsung_I8200_ISP.dll
13	No	Resurrectors	Samsung_J105B_ISP.dll
14	No	Resurrectors	Samsung_J106H_ISP.dll
15	No	Resurrectors	Samsung_J111M_ISP.dll
16	No	Resurrectors	Samsung_J120AZ_ISP.dll
17	No	Resurrectors	Samsung_J120A_ISP.dll
18	No	Resurrectors	Samsung_J200M_ISP.dll
19	No	Resurrectors	Samsung_J3110_ISP.dll
20	No	Resurrectors	Samsung_J320AZ_ISP.dll
21	No	Resurrectors	Samsung_J320A_ISP.dll
22	No	Resurrectors	Samsung_J320F_ISP.dll
23	No	Resurrectors	Samsung_J320F_ISP.dll
24	No	Resurrectors	Samsung_J321AZ_ISP.dll

Account Manage

RIFF BOX News >>

User Manuals >>

Support Files >>

Support Forum >>

Advanced Settings

Edit Repair Package

Create Repair Package

Stop

Start Probing

Firmware Update

Get BOX Info

Automatic Parameters

Show All Resurrectors

SAMSUNG

Samsung S5570

JTAG TCK Speed:

RTCK

Sample at 40 kHz

DCC Loader USB Interface

Target (Core):

ARM926EJ

Reset Method:

RESET, Wait 0 ms, Special

JTAG I/O Voltage:

2.60V

TAP# (Multichain position):

0

Partitions to back up: 5
data: 1056MB
STARTED
7559MB
up Folder: /sdcard/TWRP/BACKUP
up System...





D.- JTAG con RiffBOX a Samsung s5570

- 4.- Pulsar en Connect & Get ID
- 4.1.- Corregir los errores
- 5.- Rango o usar emmc o plugin
- 6.- Read Memory y pulsar ON
- 7.- Hashear y ANÁLISIS

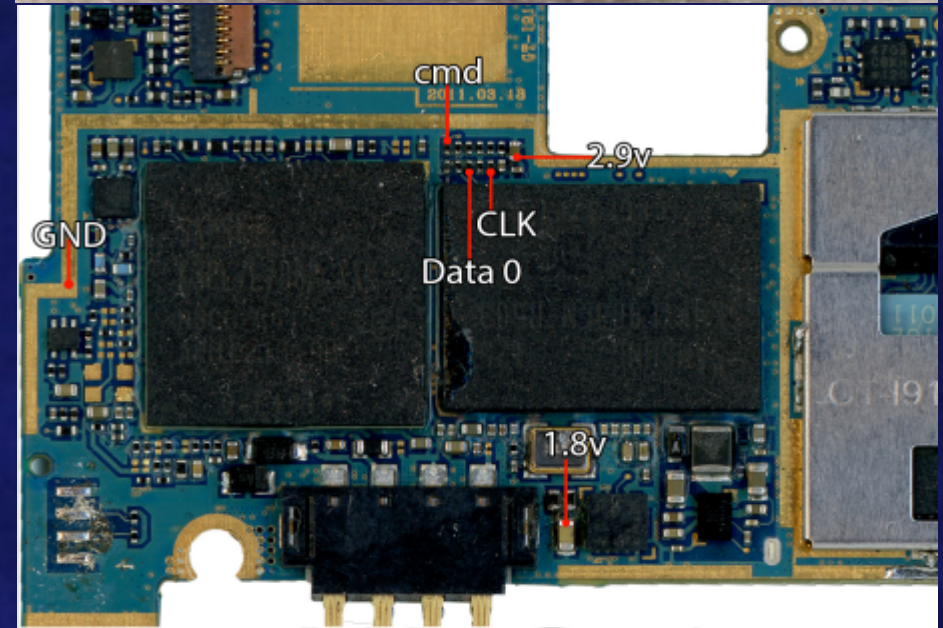
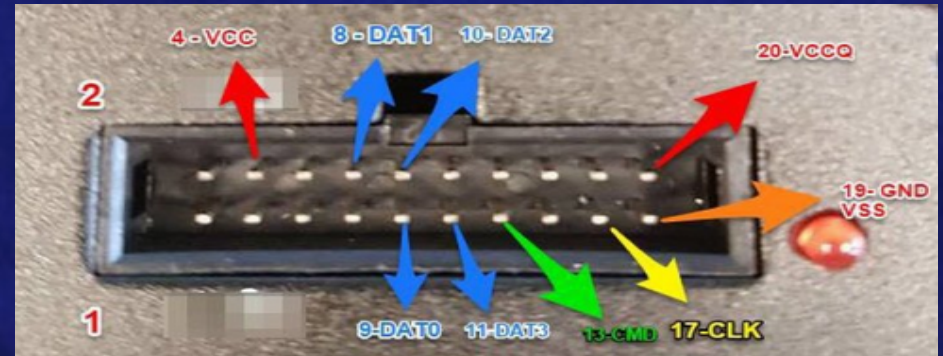


E.- ISP con emmcPRO BOX sam i9100

- 1.- Realizar las soldaduras ISP
- 2.- Abrir el software de emmcPRO
- 3.- Revisar las ayudas para los pinout

VCC = 1.8v

VCCQ = 2.8v





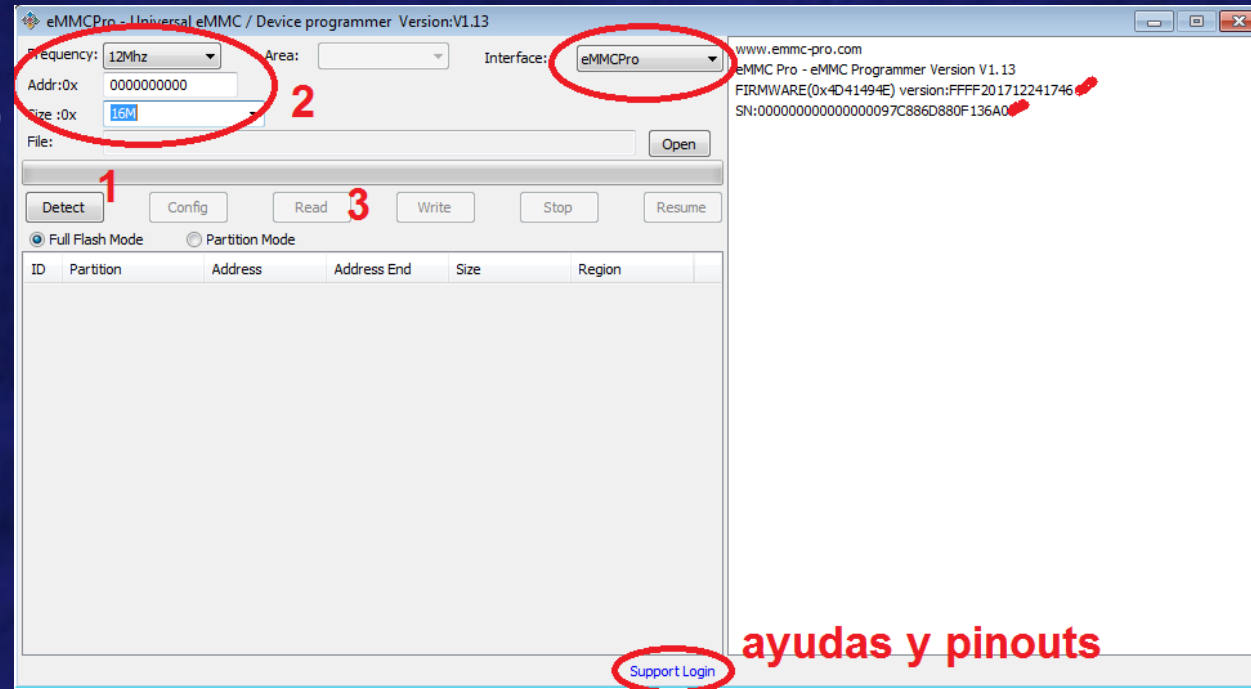
E.- ISP con emmcPRO BOX sam i9100

4.- Seleccionar Interface emmcPRO

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

6.- Read

7.- Hashear y ANÁLISIS





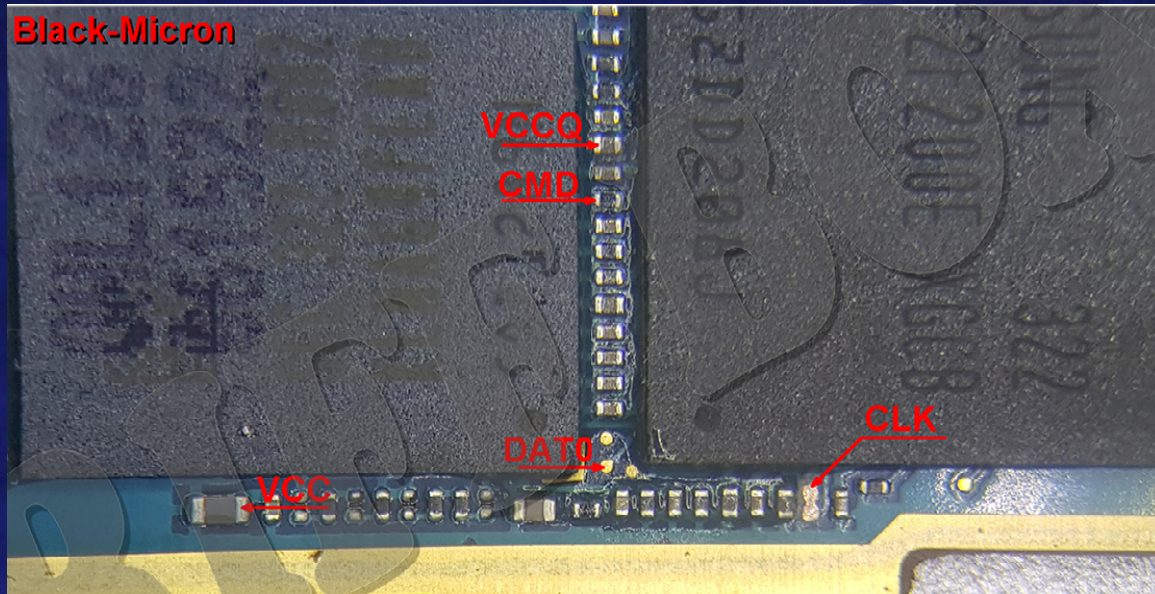
F.- ISP con Medusa PRO BOX i9505

- 1.- Realizar las soldaduras ISP
- 2.- Abrir el software de MedusaPRO
- 3.- Revisar las ayudas para los pinout

VCC = 1.8v

VCCQ = 2.8v

NC	NC	NC	NC	NC	NC	NC	NC	NC	NC
■	■	■	■	■	■	■	■	■	■
1.8V	2.9V	GND	CMD	CLK	D3	D2	D1	D0	GND
■	■	■	■	■	■	■	■	■	■





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

PRO Medusa Pro Software version 1.6.9

Model Settings Interface: JTAG USB eMMC ADB

Brand: Samsung **3** **2**
Model: GT-I9505
Voltage: Auto Bus Mode: Auto **ayudas**
Bus speed: Auto

Welcome eMMC Pin finder

Connect **4** Disconnect
 Read Android build info while connecting
 6
 Write data verification

Main Factory repair eMMC service

Boot Area Partition 1 Boot Area Partition 2
 GP1 GP2 GP3 GP4

User Data Area
Partitions Hex values
 Custom Start 0 0 b
 Full **5** Length 0 0 b

Exclusively in Octopus – Android 7.0 reset FRP!

Progress 0%

VREF: Box not connected Speed: Progress: ETA: Box status: Not connected Firmware version: S/N: 48982



G.- Chip Off y adaptador MOORC-SD

- 1.- usar indicaciones de uso y protección de la placa
- 2.- TERMOMETRO!!!!!!!!!!!!
- 3.- crear o cargar PROFILE

RE-7500 Control Room [Machine Offline]

File Profile Tools Help

seleccion de perfil

indicador calentador

control calentadores

ventilador

T/C Temperature vs. Time curve

T/C Reading: 0 C

Alarm = 205

Temperature (C)

Time (Sec)

Start Plotting Save Graph Reset Graph

Alarm Edit

UP UP

Dn Dn

FAN Fan

OFFLINE

Machine Status: N/A

JOVY SYSTEMS®
Technology Versus Future

RE-7500
BGA/SMD
REWORK
SYSTEM



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

RE-7500 Profile Editor

RE-7500 Profile Characteristic curve

□ T/C Reading: C ■ User Graph

Temperature (C)

Time (Sec)

fase 1

Preheat Phase

X1 Temperature Setpoint: 120 C

X1 Message: UH L6

Lower Heater State: FAST REFL

Upper Heater State: FAST REFL

FAN Normal Mode

fase 2

Soak Phase

X2 Temperature Setpoint: 170 C

X2 Message: UH L4

Lower Heater State: FAST REFL

Upper Heater State: FAST REFL

FAN Normal Mode

fase 3

Reflow Phase

X3 Temperature Setpoint: 225 C

X3 Message: keep to 225

Lower Heater State: FAST REFL

Upper Heater State: FAST REFL

FAN Normal Mode

General Parameters

Profile Name: Mobile LF1 File Name: C:\Users\nomed\Desktop\progs\ Save Graph FAN ON/OFF

Profiles on Computer Profiles on RE-7500

New Open Save Retrieve Save Profile 1 Profile 2 Profile 3 Run Exit Profiles



G.- Chip Off y adaptador MOORC-SD

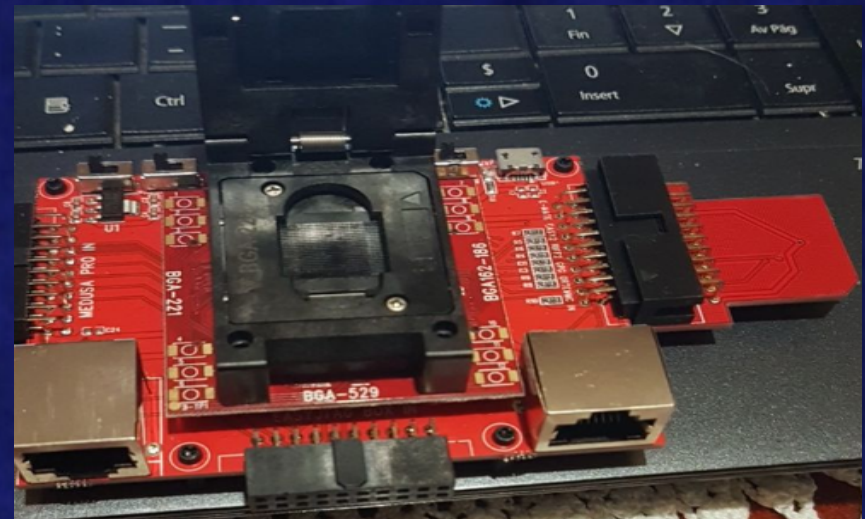
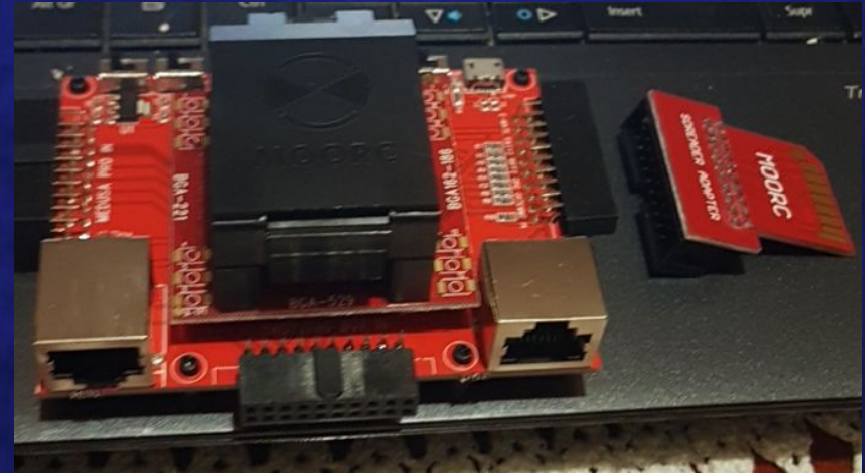
8.- Poner el chip en el MOORC con un SD MOORC adapter

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

RE-7500 Control Room [Machine Offline]

File Profile Tools Help

seleccion de perfil

indicador calentador

control calentadores

ventilador

T/C Temperature vs. Time curve

T/C Reading: 0 C

Alarm = 205

Temperature (C)

Time (Sec)

Start Plotting Save Graph Reset Graph

Alarm Edit

UP UP

Dn Dn

FAN Fan

OFFLINE

Machine Status: N/A

JOVY SYSTEMS®
Technology Versus Future

RE-7500
BGA/SMD
REWORK
SYSTEM



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

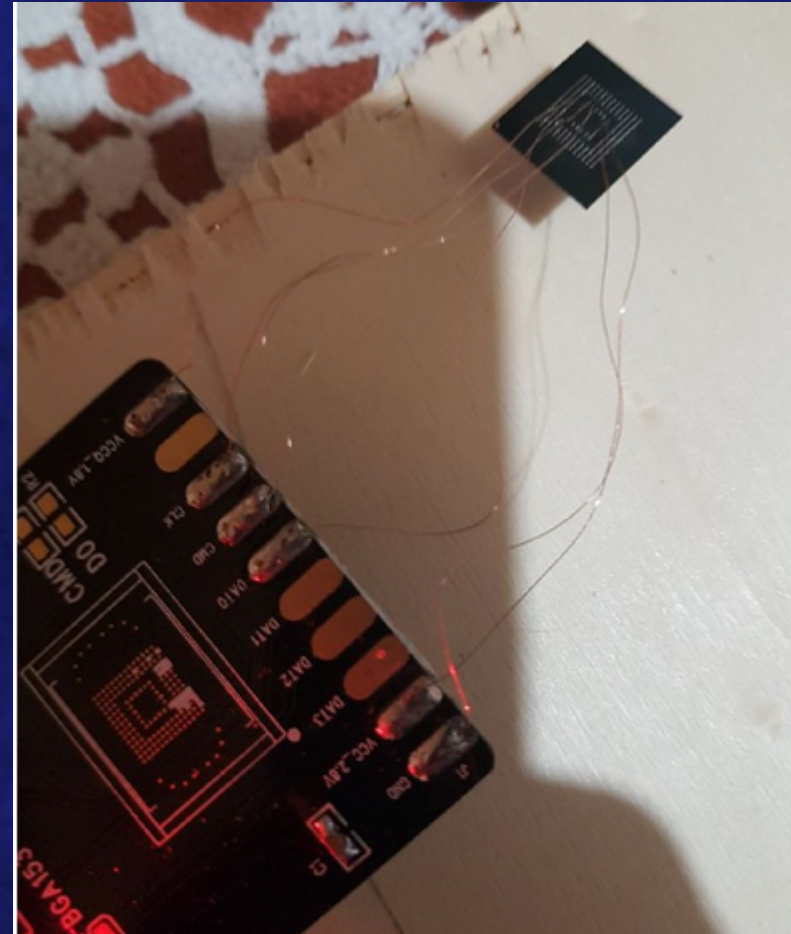
8.- Soldamos los 6 pinouts con hilo de cobre, mirar el dataset

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

10.- montar con:

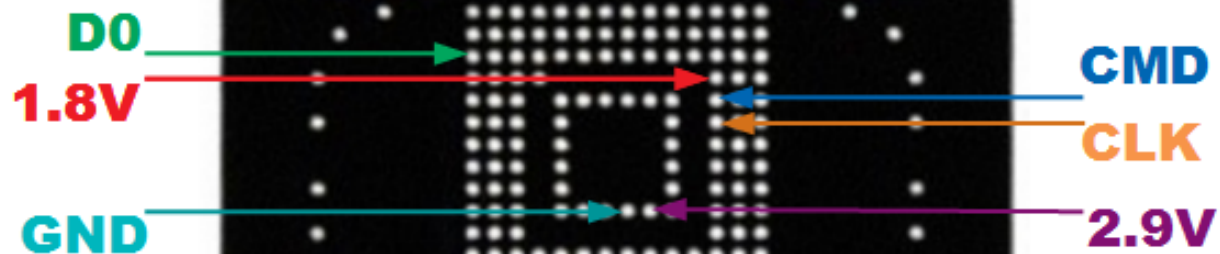
10.1. FTK imager

10.2. MV Kali linux (p.ej.)



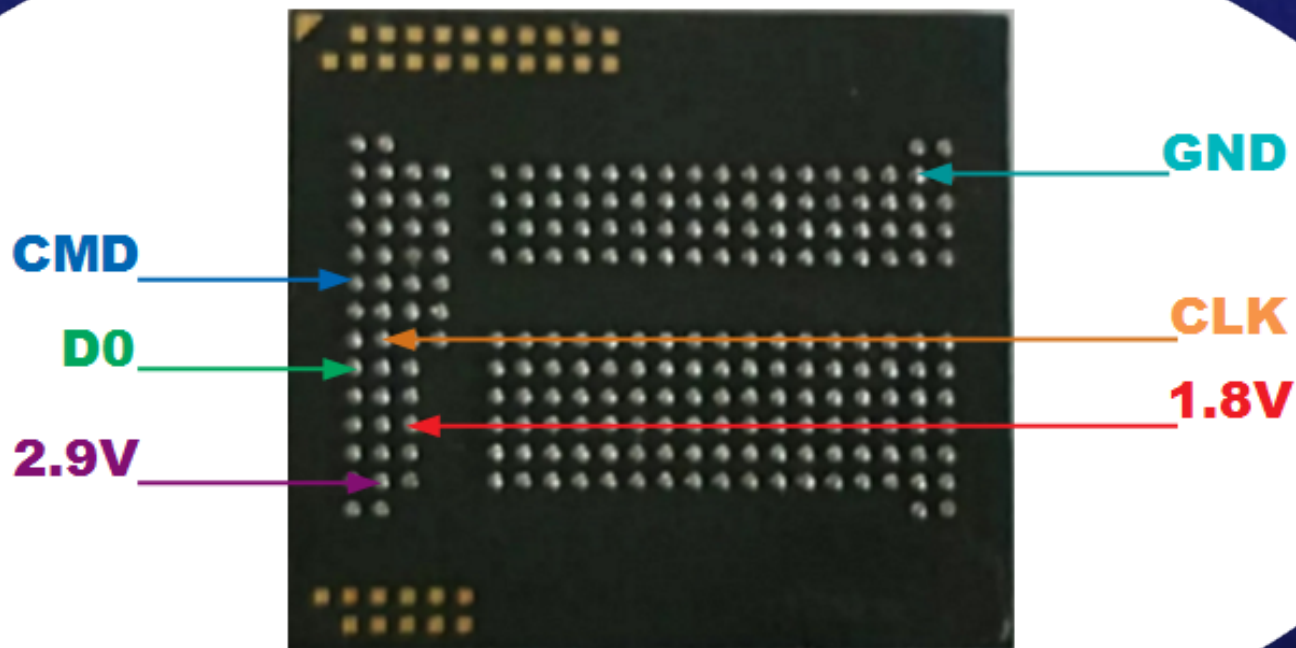


Info general: BGA 153/169



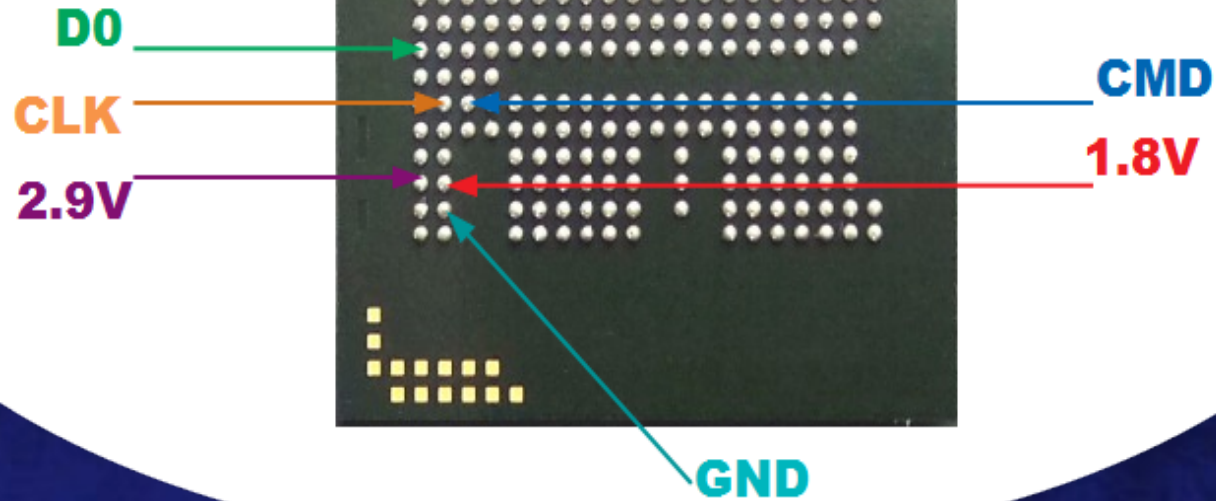


Info general: BGA 221



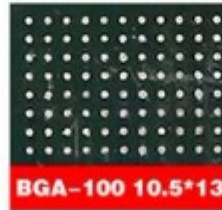


Info general: BGA 162/186





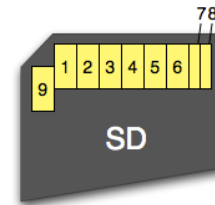
Info general: encapsulados



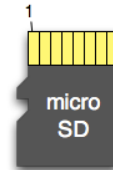


Info general: pinouts SD

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



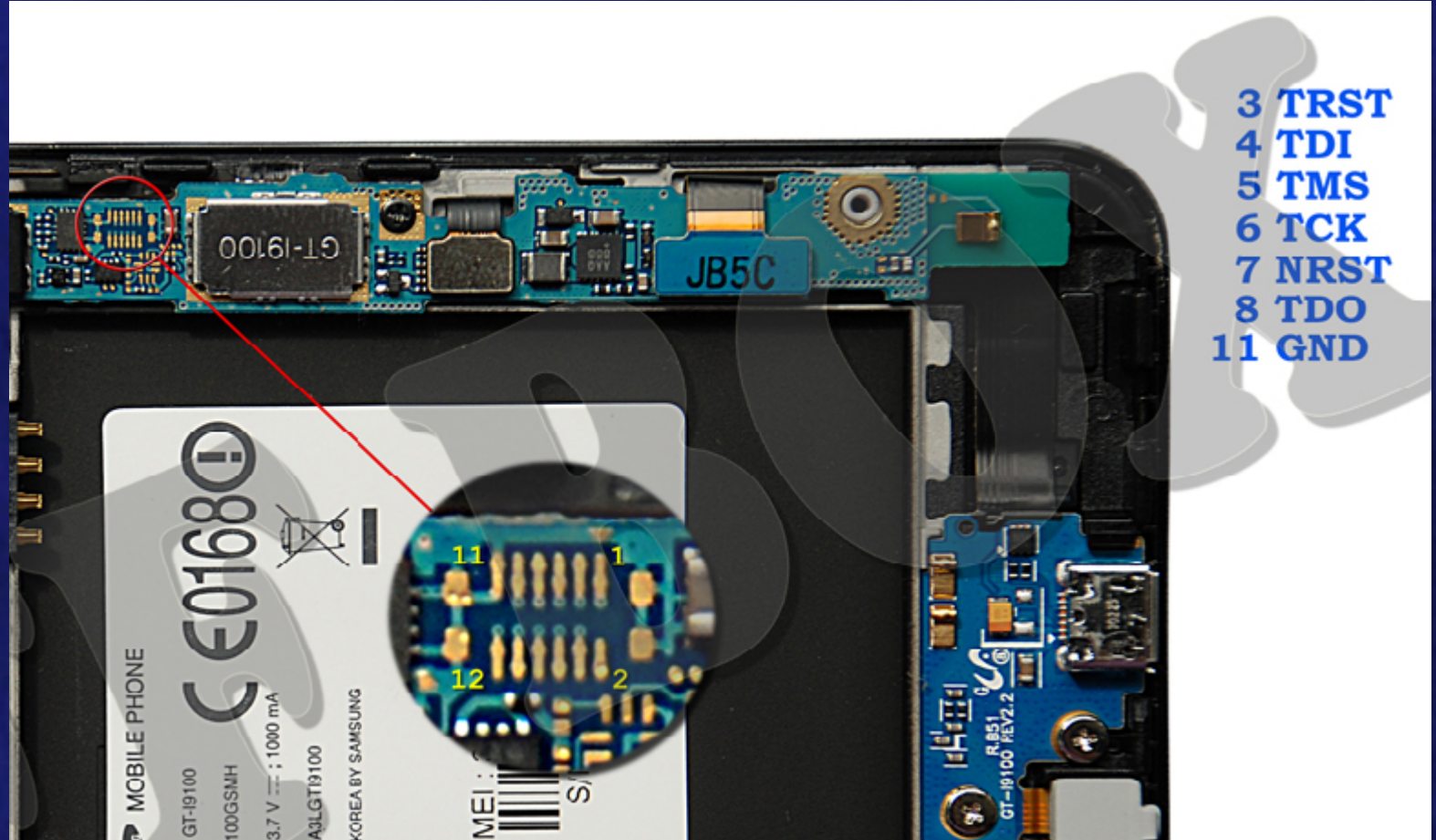
Pin	SD	SPI
1	CD/DAT3	CS
2	CMD	DI
3	VSS1	VSS1
4	VDD	VDD
5	CLK	SCLK
6	VSS2	VSS2
7	DAT0	DO
8	DAT1	X
9	DAT2	X



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

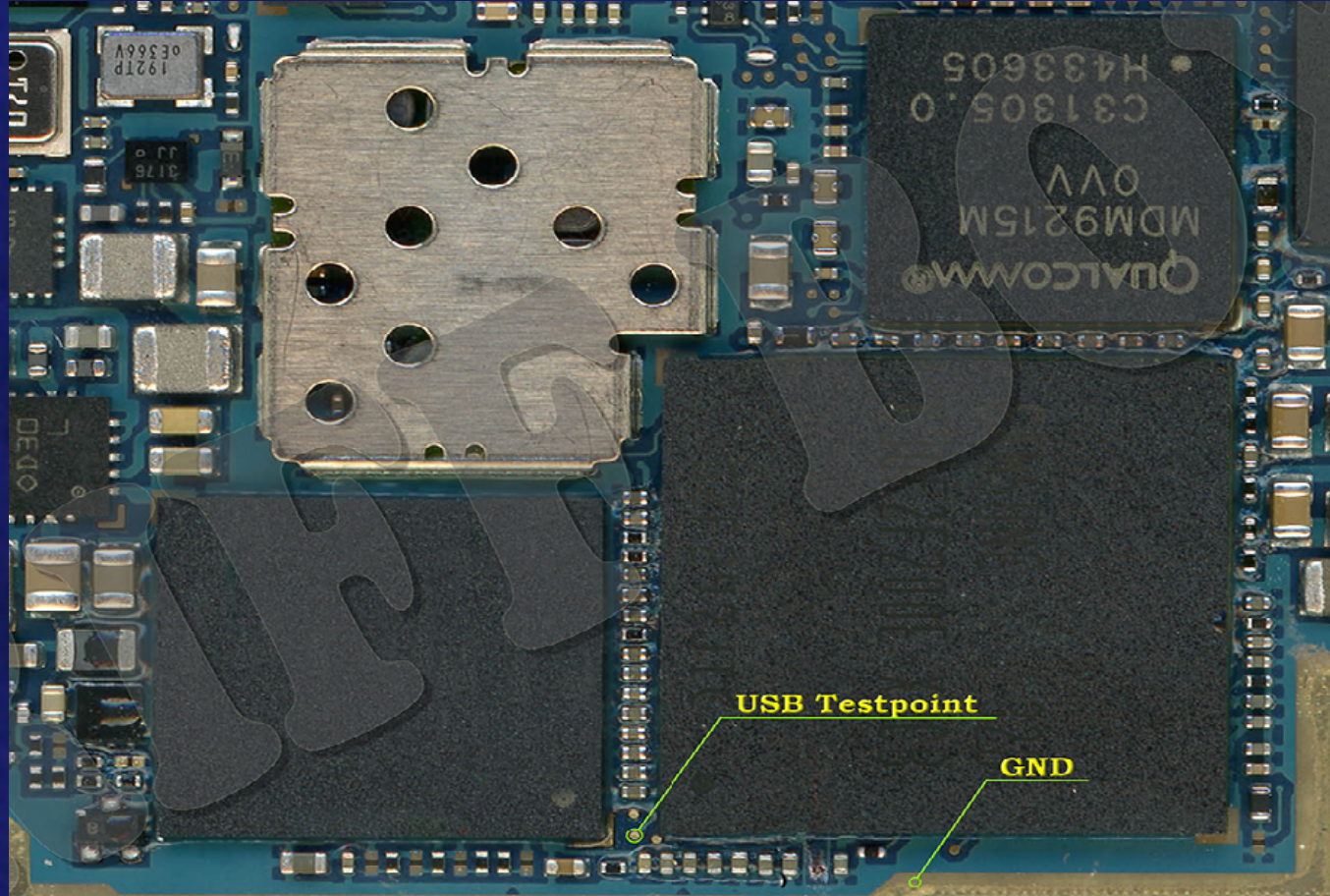


Info general: SAMSUNG i9100 S2 JTAG





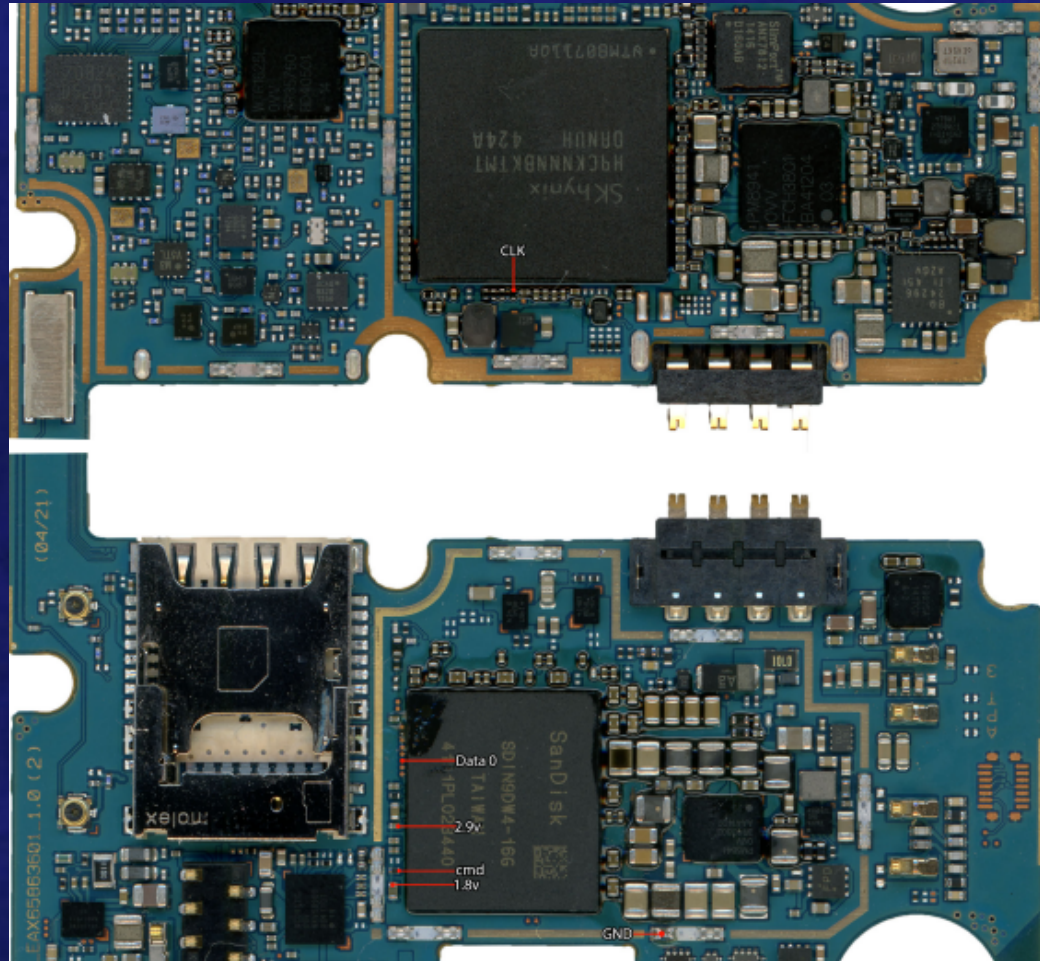
Info general: SAMSUNG i9505 S4 TP





Info general: LG D855 G3

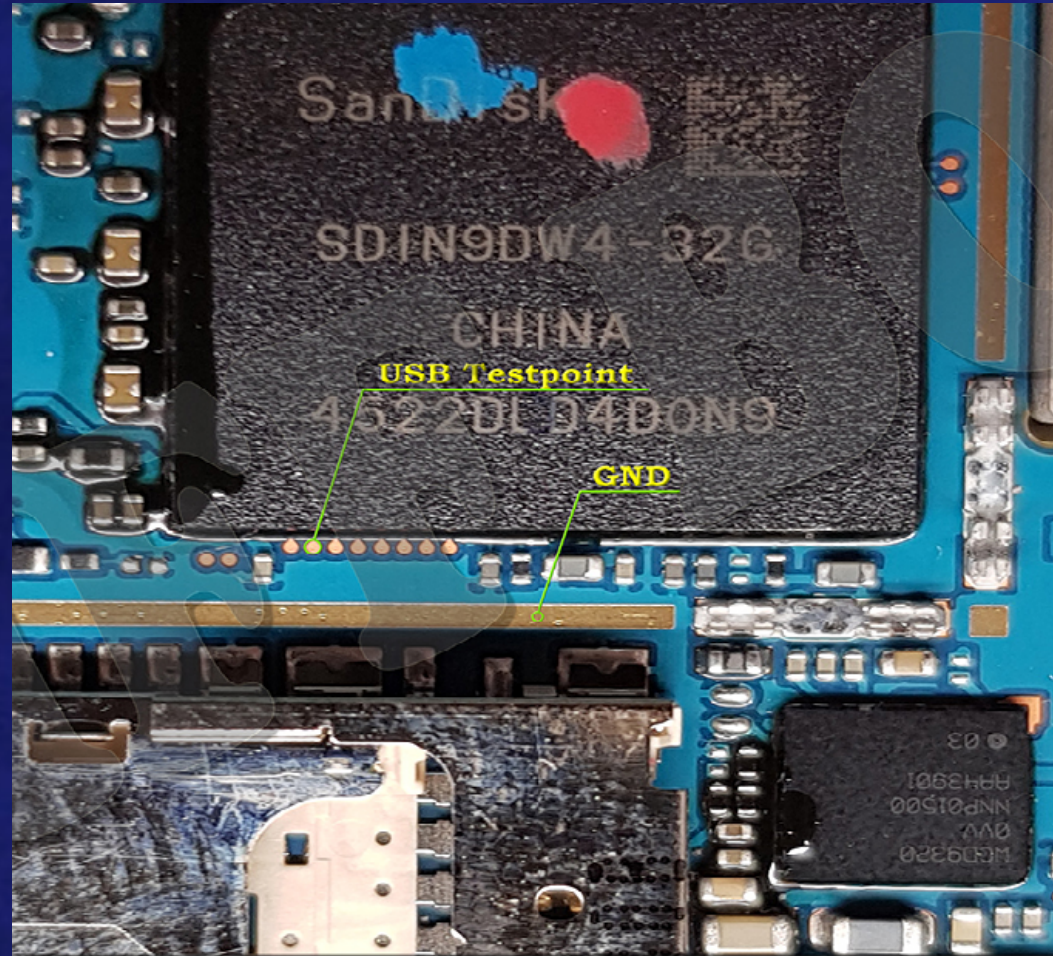
ISP





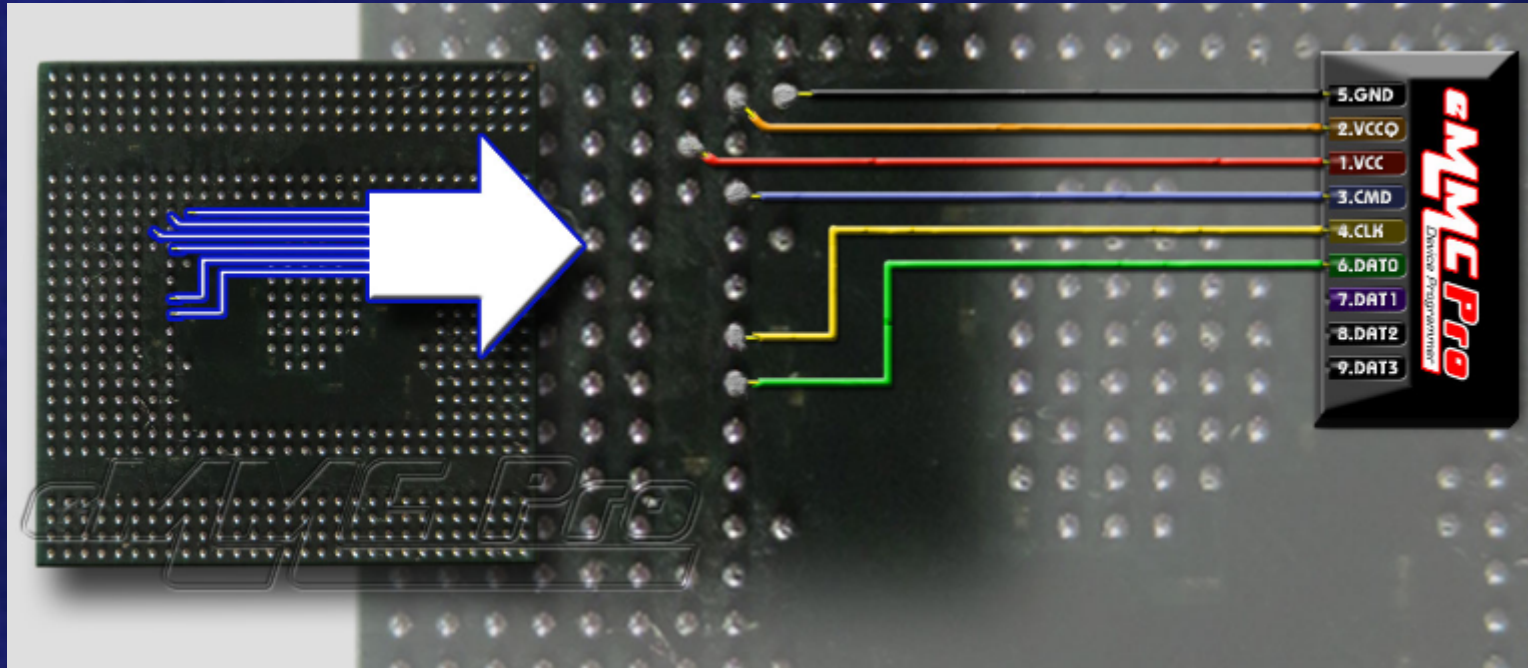
Info general: LG D855 G3

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

!!!!!!!!!!!!!!





Preguntas

