



NAVAJA NEGRA CONFERENCE

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

Buenaventura Salcedo Santos-Olmo



www.eltallerde losandoides.com/blog



QUIEN SOY YO

- ★ Cuasi Graduado en Ingeniería Informática en la UNED
- ★ Jefe Servicio Técnico de telefonía móvil e informática
- ★ Desarrollador de artifacts forenses para smartphones
- ★ Escritor en el blog de Comunix Group
- ★ Desarrollador del primer cluster español Linux de cálculo para sha1
- ★ Colaborador en el proyecto Easyunlocker Box
- ★ Desarrollador del primer gestor masivo de códigos online español



GRACIAS NAVAJA NEGRA, GRACIAS ALBACETE

TODO COMENZÓ AQUÍ





EN ESTA PRESENTACIÓN

Vamos a dar cobertura técnica

- 1.- Observaciones generales en smartphones**
- 2.- Comentarios de herramientas y consumibles de laboratorio**
- 3.- Como preparar y abordar las placas**
- 4.- Consideraciones físicas de las placas**
- 5.- Estudio de algunas interfaces de lectura**
- 6.- Puesta en escena chip-off (si todo sale bien!!!!!! :)**



BÁSICAMENTE ACERCAR UN LABORATORIO HARDWARE



CONSIDERACIONES GENERALES

- No vamos a hablar de leyes.
- La cobertura legal para los juristas
- Los experimentos deben repetibles
- Tenemos que mancharnos
 - Si la cagamos no hay marcha atrás



QUE CASOS SE NOS PLANTEAN

CONDICIONES EXTREMAS de los terminales





QUE CASOS SE NOS PLANTEAN

CONDICIONES EXTREMAS de los terminales

- **Conecadores rotos (SAT) (video 1)**
- **Interruptores rotos (SAT)**
- **Pantallas rotas (SAT)**
- **Golpeados, aplastados y sumamente deteriorados (p.e.1)**
- **No encienden sin motivo aparente**
- **Mojados y/o expuestos a largos periodos de humedad**

>> ADEMÁS DE LAS CONDICIONES NORMALES DE BLOQUEOS <<

***SAT = Labor trivial de Servicio Técnico**

DISTINTAS TÉCNICAS DE ADQUISICIÓN DE MEMORIA

- DUMP directo (aunque no encienda no se descarta)
- Test Point (TP)
- Joint Test Action Group (JTAG)
- In System Programming (ISP)
- Chip-OFF



CONDICIONES EXTREMAS – HERRAMIENTAS

HERRAMIENTAS DE MEDICIÓN

Multímetro, osciloscopio, capacímetro, termómetro tipo K y/o digital, ...

HERRAMIENTAS DE SOLDADURA

- **Herramientas de ayuda a la soldadura**

Lupas o microscopios, soportes, extractores de humo, ...

GADGETS Y CONSUMIBLES

Hilos, estaño, flux, pinzas, pegamentos, ...



HERRAMIENTAS

HERRAMIENTAS DE SOLDADURA

a) Estación de aire caliente



b) Estación de infrarrojos

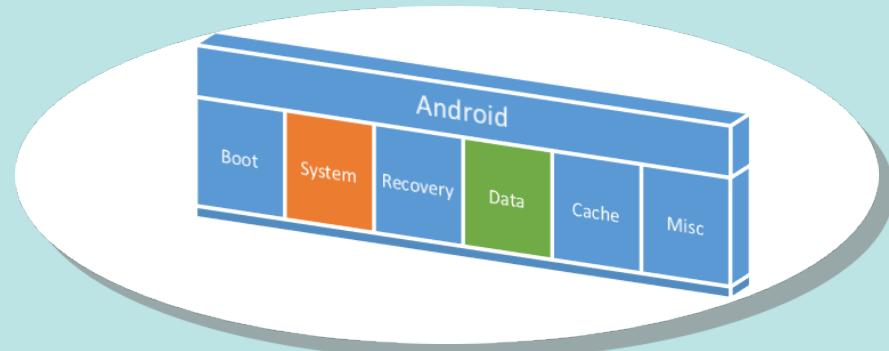


c) Estación robotizada



QUE BUSCAMOS Y QUE HAY DENTRO

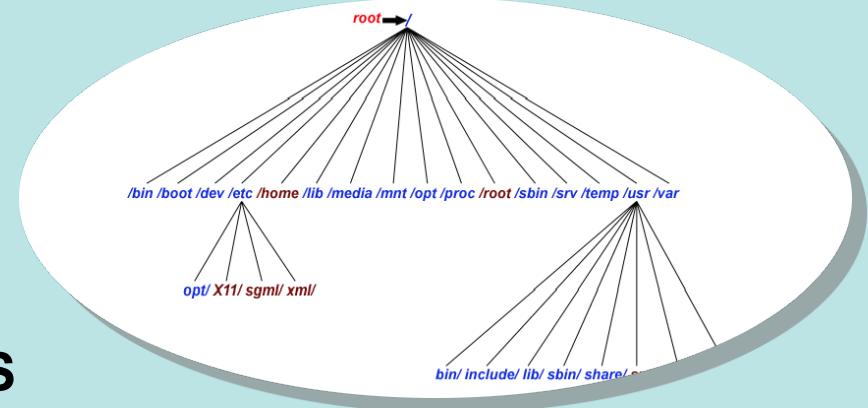
- **/USERDATA - /DATA - /STORAGE**
- **/SDCARD (si existe fuera)**
- **/CACHE**
- **/METADATA (*)**
- **/SYSTEM**
- **/RECOVERY**
- **/TEE**
- **/ABOOT**
- **/PROINFO**



*otra charla

QUE FORMATO PUEDE TENER LA INFORMACIÓN ADQUIRIDA

- EXT 2-3-4
- FAT – FAT32
- FICHEROS IMAGEN
- FICHEROS RAW (autopsy p.e)
- FICHEROS ORDINARIOS
- DATOS CIFRADOS

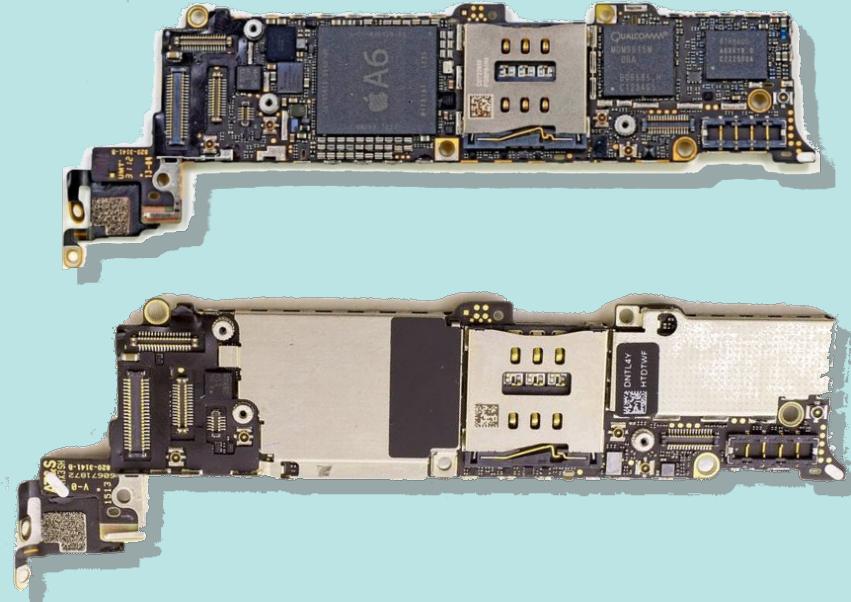


ExFAT

TÉCNICAS INVASIVAS ADQUISICIÓN – MAINBOARD

EL FABRICANTE PUEDE PROTEGER LA PLACA CON

A) BLINDAJES SOLDADOS A PLACA

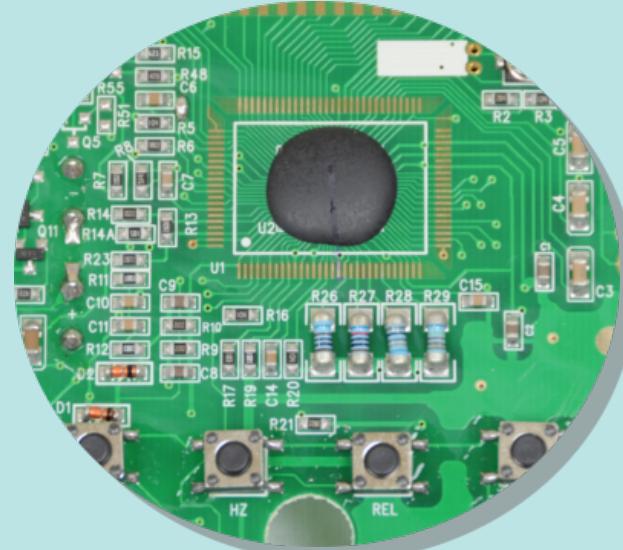
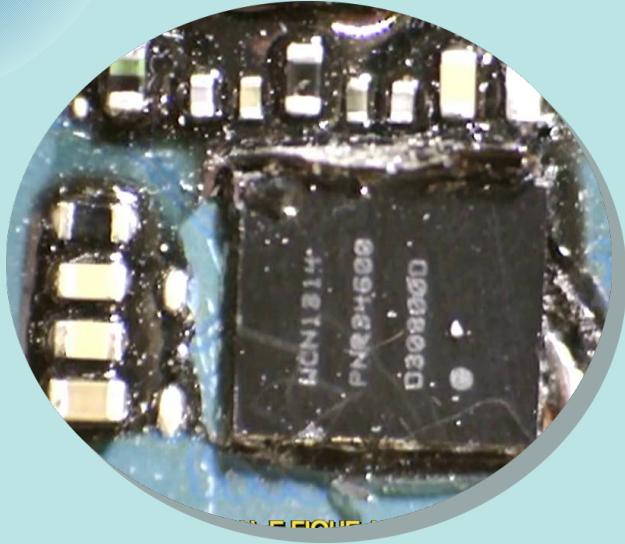


* Puede ser necesario quitarlas para acceder a TP, JTAG, ISP o CHIP-OFF

TÉCNICAS INVASIVAS ADQUISICIÓN – MAINBOARD



B) EPOXY EN LOS INTEGRADOS



**¡CUIDADO! EN CHIP-OFF PUEDE HABER EPOXY
TAMBIÉN DEBAJO DEL INTEGRADO**

TELÉFONOS MOJADOS Y OXIDADOS

LIMPIEZA CON LIMPIACONTACTOS

LIMPIEZA CON CEPILLOS

LOS RESTOS MUY AGARRADOS CON FIBRA DE VIDRIO Y

CUBETA DE ULTRASONIDOS CON:

- AGUA DESTILADA
- ALCOHOL ISOPROPÍLICO
- CÍTRICOS + AMONIACO (HAY QUE RETIRAR RESTOS) ???
- OTRAS SUSTANCIAS O QUÍMICOS DEL MERCADO



TÉCNICAS INVASIVAS ADQUISICIÓN – PROTEGER

PROTECCIÓN DE LA PLACA

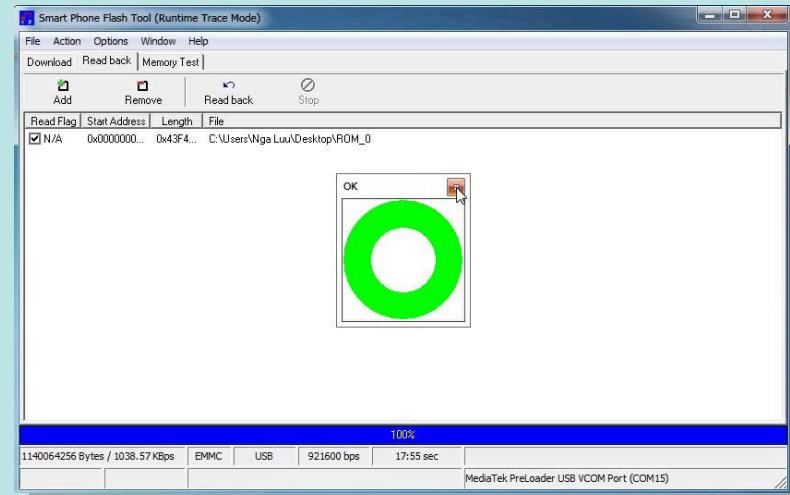
- **Eliminar la brujería electrónica**
- **Reducir la distribución de calor**
- **Eliminar el movimiento de componentes**
- **Reducir el estrés de los componentes**
- **Concentrar la atención**



1) TÉCNICAS INVASIVAS ADQUISICIÓN – DUMP

DUMP Lectura directa del terminal con USB

- Puede funcionar aunque no encienda
- Usado con procesadores Mediatek
- Podríamos necesitar mapa
- Mucho software disponible
- Conector debe estar OK
- Botón de subir/bajar volumen OK
- Usado con procesadores QLCM
- Modo EDL en muchos modelos
- EDL puede necesitar cable modificado (*)
- En Samsung (viejos) JIG para download mode



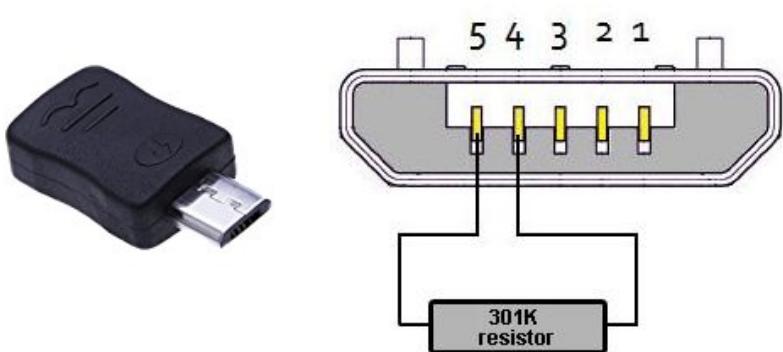
1) TÉCNICAS INVASIVAS ADQUISICIÓN – DUMP

Lectura directa del terminal con USB

PINOUT JIG SAMSUNG

RESISTENCIA 300K ENTRE GND Y NC

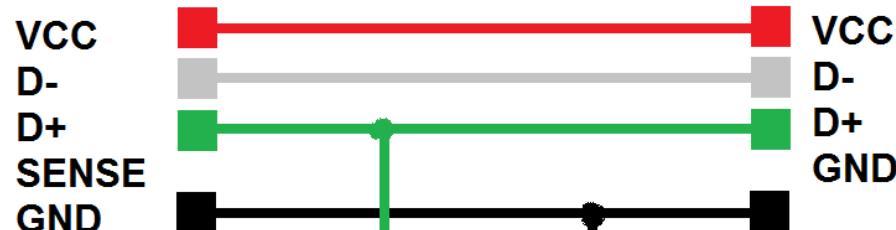
PONE EL TERMINAL EN DOWNLOAD MODE



1) TÉCNICAS INVASIVAS ADQUISICIÓN – DUMP

Lectura directa del terminal con USB

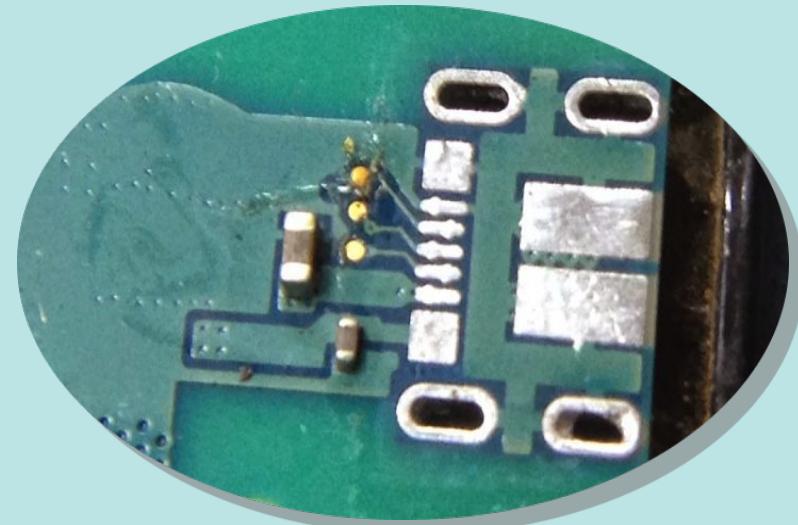
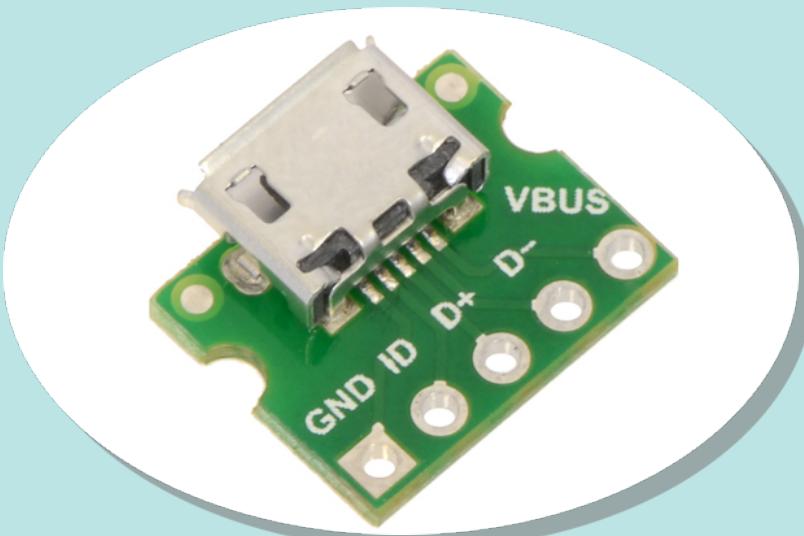
PINOUT CABLE EDL



1) TÉCNICAS INVASIVAS ADQUISICIÓN – DUMP

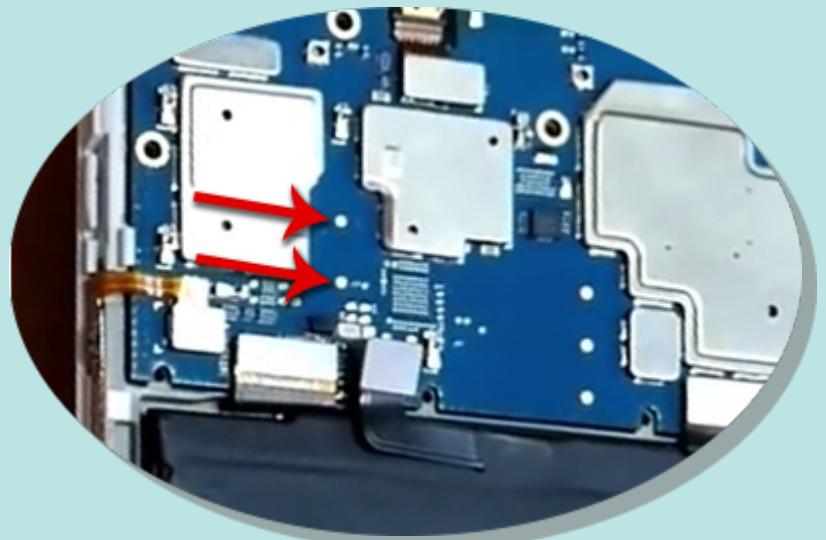
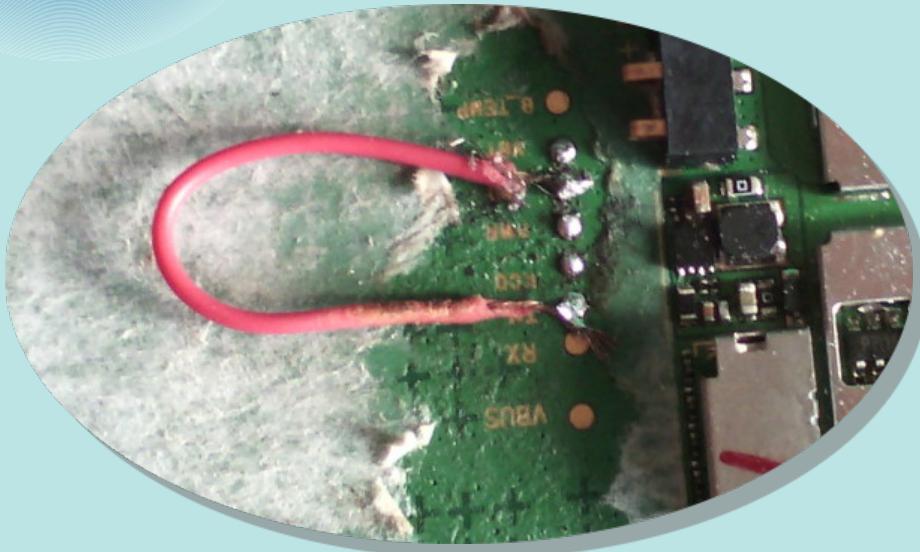
Lectura directa del terminal con USB

EN CASO DE PERDIDA DE PISTAS DE CONECTOR
RECOMPONER CON HILO DE COBRE



2) TÉCNICAS INVASIVAS ADQUISICIÓN – TESTPOINT

Realizar TP es hacer un corto(puente) entre dos puntos ESPECÍFICOS de la placa, **uno suele ser GND**



¿Cómo conocemos el TP?



2) TÉCNICAS INVASIVAS ADQUISICIÓN – TESTPOINT

Salta protección de arranque poniendo el terminal en EDL mode o 9008, que aprovecharemos para dump

- Puede funcionar aunque no encienda
- Usado con procesadores QLCM, Huawei, Xiaomi
- Podríamos necesitar mapa
- Posible montar directamente en Linux, sin port de lectura(*)
- Drivers HS-USB qualcomm.
- Conector debe estar OK
- Puede ser necesario desconectar la batería, ej XIAOMI.
- Posible necesario loaders y/o software específico.

*LG permite en muchos modelos sin TP, incluso write about



2) TÉCNICAS INVASIVAS ADQUISICIÓN – TESTPOINT

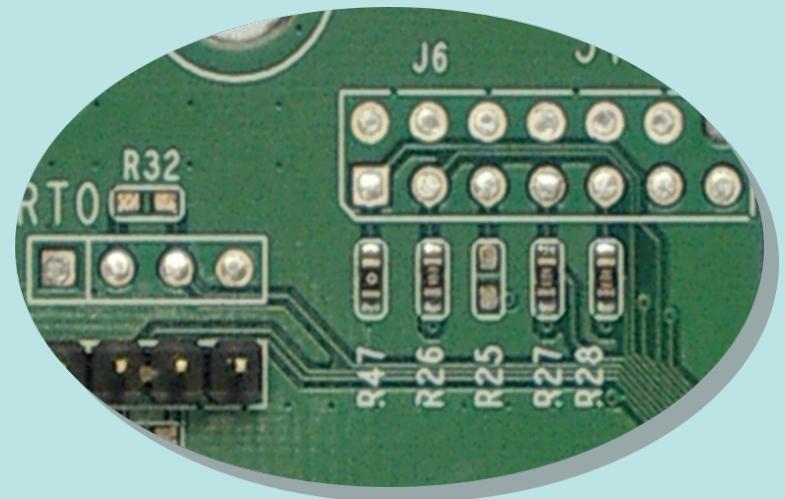
Procedimiento general:

- Correr el software necesarios, se mantendrá a la espera
- Puede o no necesitar conectar la batería
- Realizar el TP
- Conectar USB
- Mantener TP hasta que salte el boot e inicie el proceso de lectura
- Esperar el fichero dump resultante

3) TÉCNICAS INVASIVAS ADQUISICIÓN – JTAG

Join Test Action Group (JTAG)

- Estándar desde 1985
- Presentes en Sistemas Embebidos
- Son puntos para probar circuitos
- Esos puntos son Test Access Ports (TAP)
- Test hardware
- Escritura/Lectura de firmware
- Debug

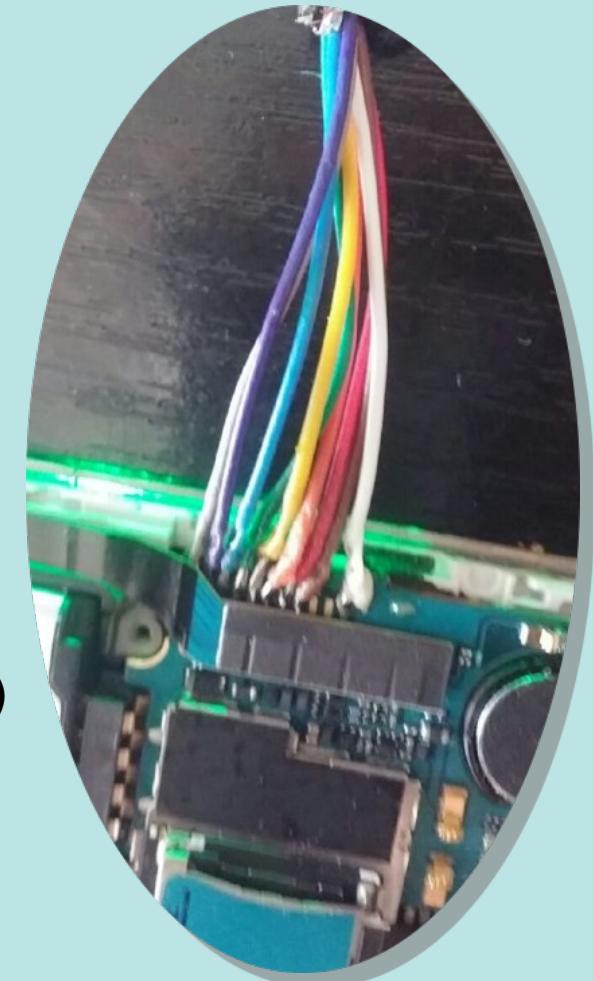


3) TÉCNICAS INVASIVAS ADQUISICIÓN – JTAG



JTAG Forensics

- Atacamos al procesador para acceder a memoria
- Obtenemos los datos brutos de memoria
- Necesitamos un loader
- Necesitamos una interfaz para los jtags
- Soldar en placa, usar molex o agujas retráctiles (*)
- No se destruye el terminal



*depende del terminal

3) TÉCNICAS INVASIVAS ADQUISICIÓN – JTAG

CONSIDERACIONES JTAG

- El soporte de la interfaz suministra JTAG schemes
- Hilos o cables cortos
- Cuidado con los pinouts en la placa
- Cuidado con los pinout en la interfaz
- La placa debe estar alimentada (3,7v o 5v)(*)
- Configurar la frecuencia en la interfaz
- Podríamos usar modo automático

*depende del terminal



3) TÉCNICAS INVASIVAS ADQUISICIÓN – JTAG

INTERFACES JTAG (BOX)

- RIFF – RIFF 2
- MEDUSA – MEDUSA PRO
- EASY JTAG Z3X
- OCTOPLUS BOX PRO
- ATF
- UFI
- GPG EMMC
- ORT (ahora es EMMC PRO y NAND PRO iphone)



* Validas también ISP y chip-off

3) TÉCNICAS INVASIVAS ADQUISICIÓN – JTAG

INTERFACES JTAG PINOUTS

- VCC
- TRST
- TDI
- TMS
- TCK
- RTCK
- TDO
- NRST



RJ45 Pinout	
1 - 4.2V	5 - MBUS
2 - UART TX	6 - PROBE
3 - UART RX	7 - BSI
4 - UART TX2	8 - GND

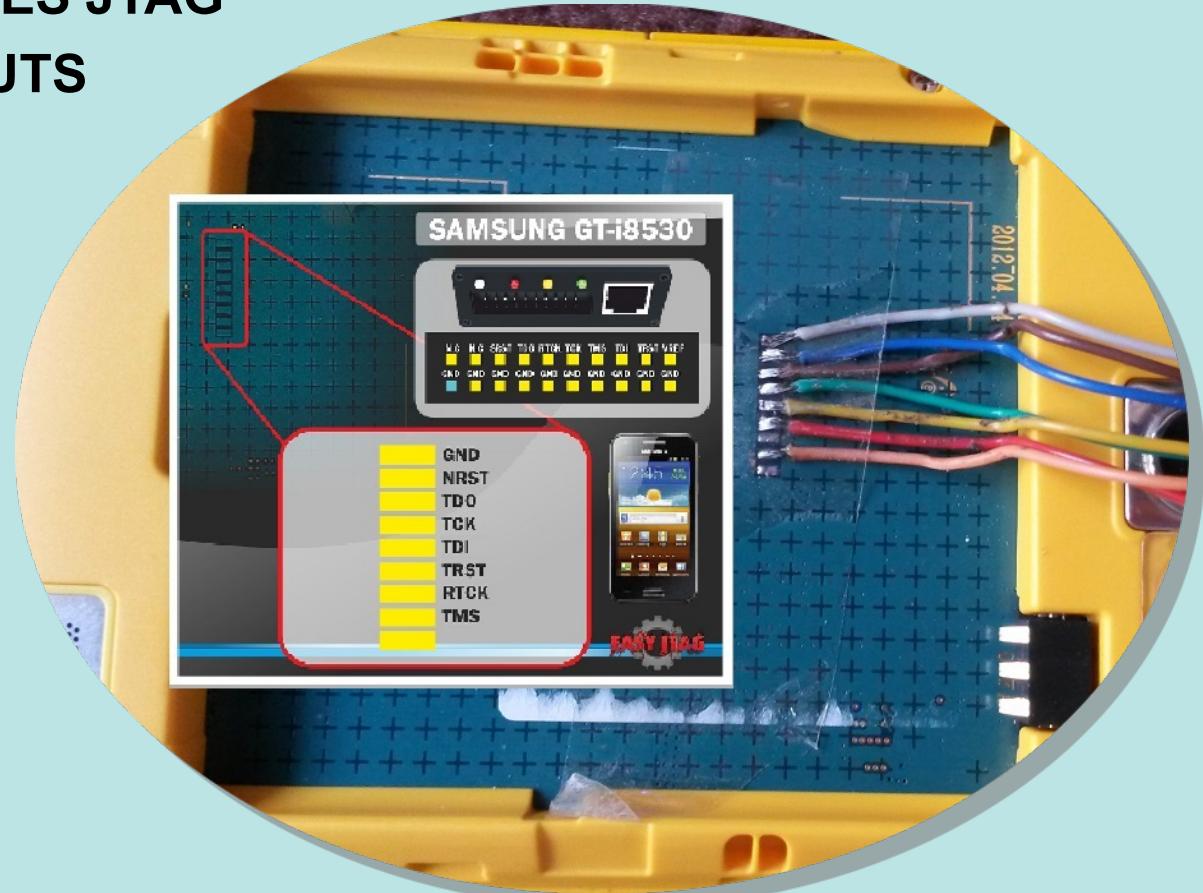
1 - VCC (black)
3 - TRST (red)
5 - TDI (yellow)
7 - TMS (orange)
9 - TCK (green)

11 - RTCK (purple)
13 - TDO (brown)
15 - NRST (blue)
20 - GND (white)

3) TÉCNICAS INVASIVAS ADQUISICIÓN – JTAG

INTERFACES JTAG PINOUTS

- VCC
- TRST
- TDI
- TMS
- TCK
- RTCK
- TDO
- NRST





3) TÉCNICAS INVASIVAS ADQUISICIÓN – JTAG

GADGETS JTAG

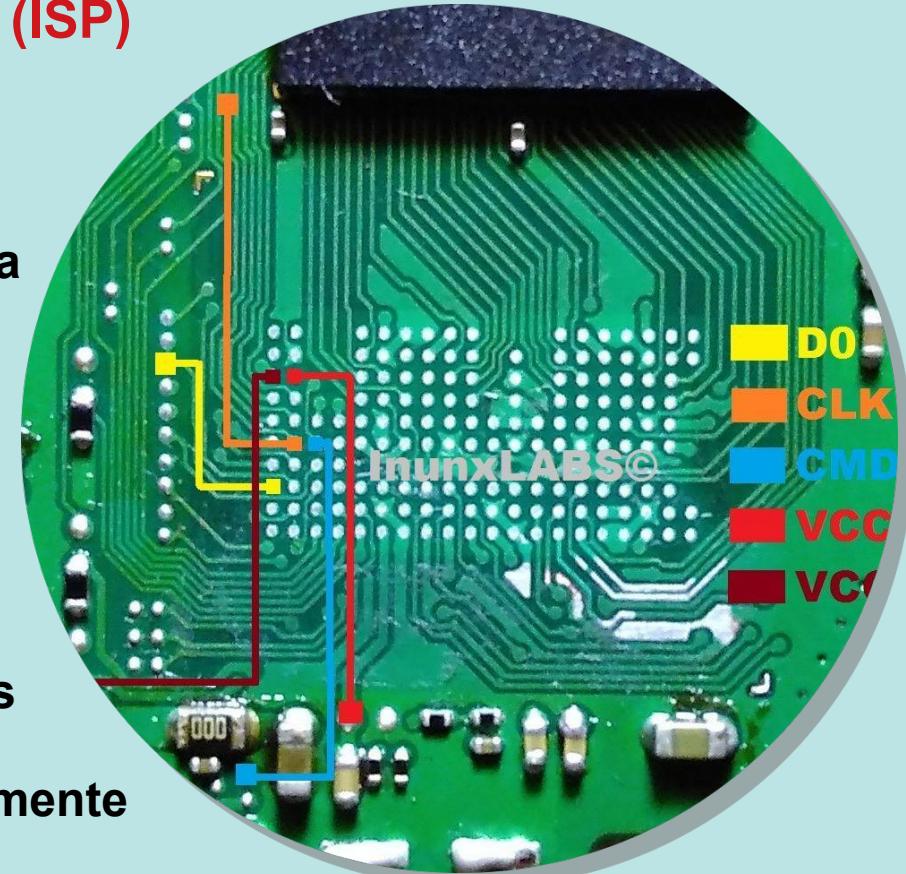
VR-TABLE



4) TÉCNICAS INVASIVAS ADQUISICIÓN – ISP

In System Programming (ISP)

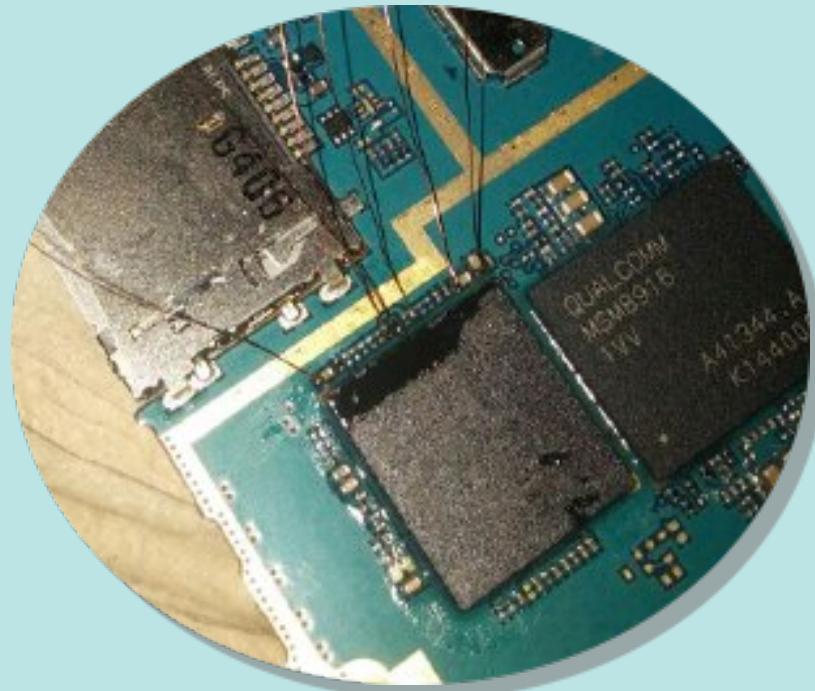
- Presentes en la cercanía de la memoria
- Son puntos para probar memorias
- Test hardware
- Escritura/Lectura en memoria
- Valido también pendrives y mas placas
- Los pinouts se obtienen experimentalmente



4) TÉCNICAS INVASIVAS ADQUISICIÓN – ISP

ISP Forensics

- Atacamos el chip de memoria
- Obtenemos los datos brutos de memoria
- Necesitamos un mapper
- Necesitamos una interfaz para la lectura
- Soldar en placa o agujas retráctiles (*)
- No se destruye el terminal



*depende del terminal

4) TÉCNICAS INVASIVAS ADQUISICIÓN – ISP

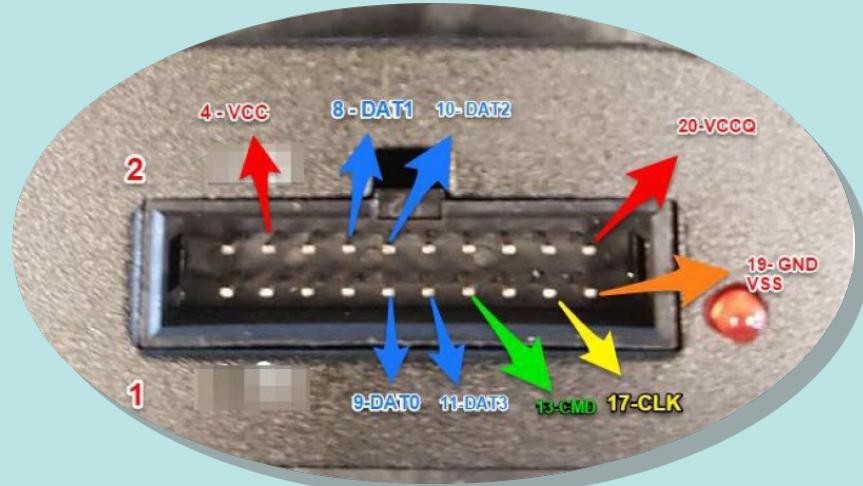


INTERFACES ISP PINOUTS

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

eMMC pinout

NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC
1.8V	2.8V	GND	CMD	CLK	D3	D2	D1	D0	GND		
Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Yellow		

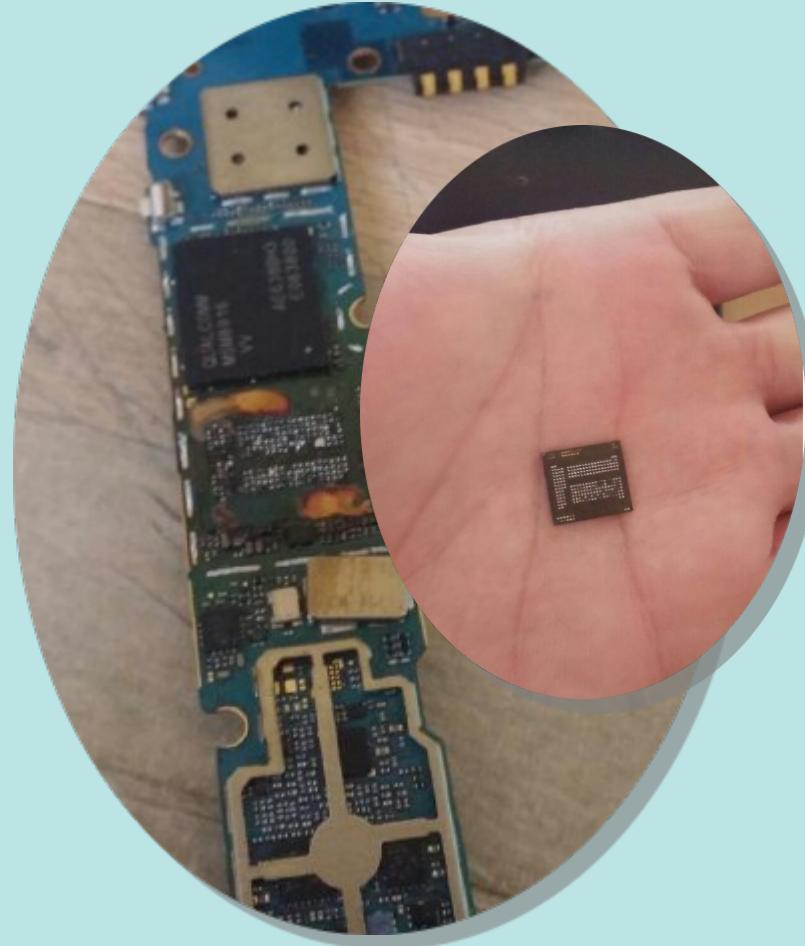


5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF



CHIP-OFF

- Atacamos el chip de memoria
- Obtenemos los datos brutos de memoria
- Necesitamos un mapper
- Necesitamos una interfaz para la lectura
- Extraemos el chip
- SI DESTRUYE el terminal(*)



*puede usarse para traslado de componentes a otra placa



5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

CONSIDERACIONES CHIP-OFF

- Distintos tipos de memoria
- Podemos hacer traslado de componentes
- Podríamos necesitar procesador y eprom (casos de cifrado)
- Limpieza y/o reboleado
- Podemos hacer lectura externa
- Podemos usar adaptadores SD
-
- Podemos soldar también a los puntos del chip

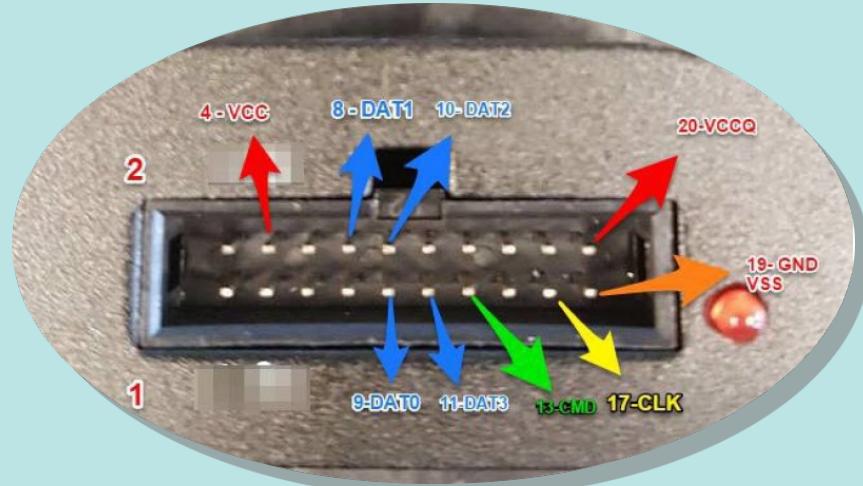
5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

INTERFACES CHIP-OFF PINOUTS

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

eMMC pinout

NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC
1.8V	2.8V	GND	CMD	CLK	D3	D2	D1	D0	GND		
Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Yellow		

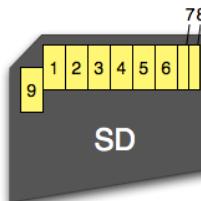




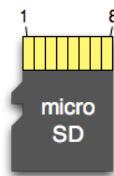
5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

INTERFACES CHIP-OFF PINOUTS

- **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

5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

INTERFACES CHIP-OFF MÓDES – FORMAT - ENCAPSULADO

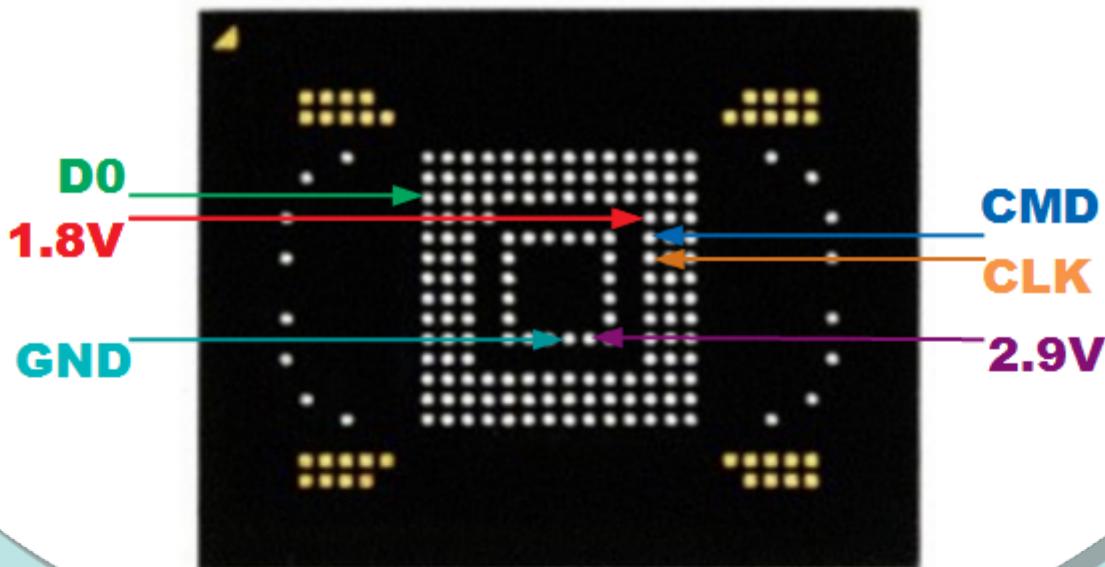


5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

INTERFACES CHIP-OFF PINOUTS

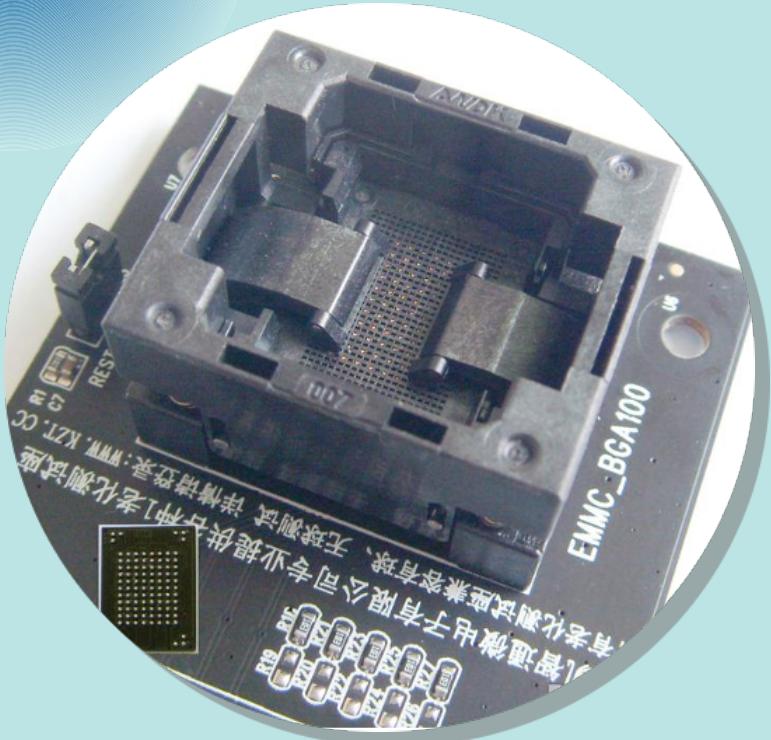
- VCCQ(1.8v)
- VCC(2.8v/3.7v)
- GND(vss)
- CMD
- CLK
- D0..Dx

BGA 153/169



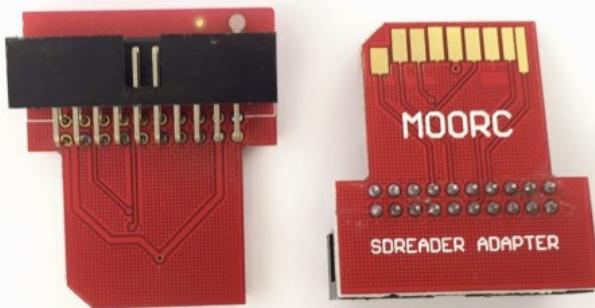
5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

ADAPTADORES



5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

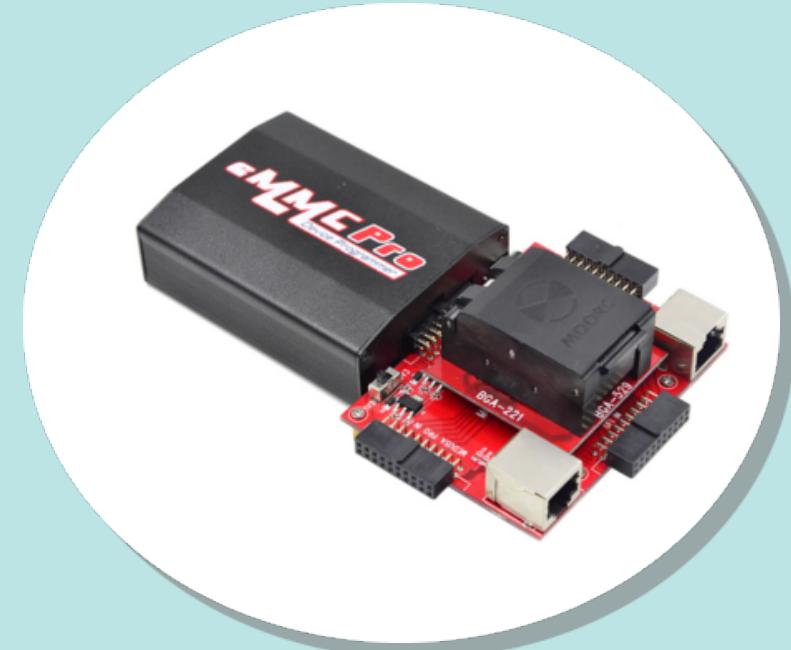
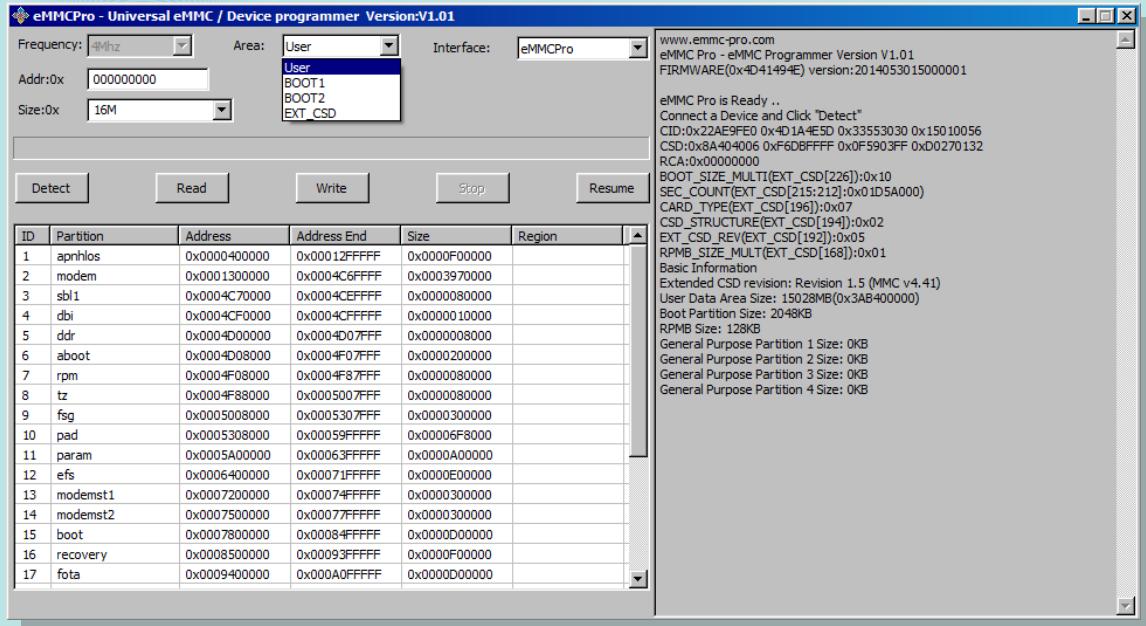
ADAPTADORES



5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

BOXES – CAJAS – INTERFACES WORKING

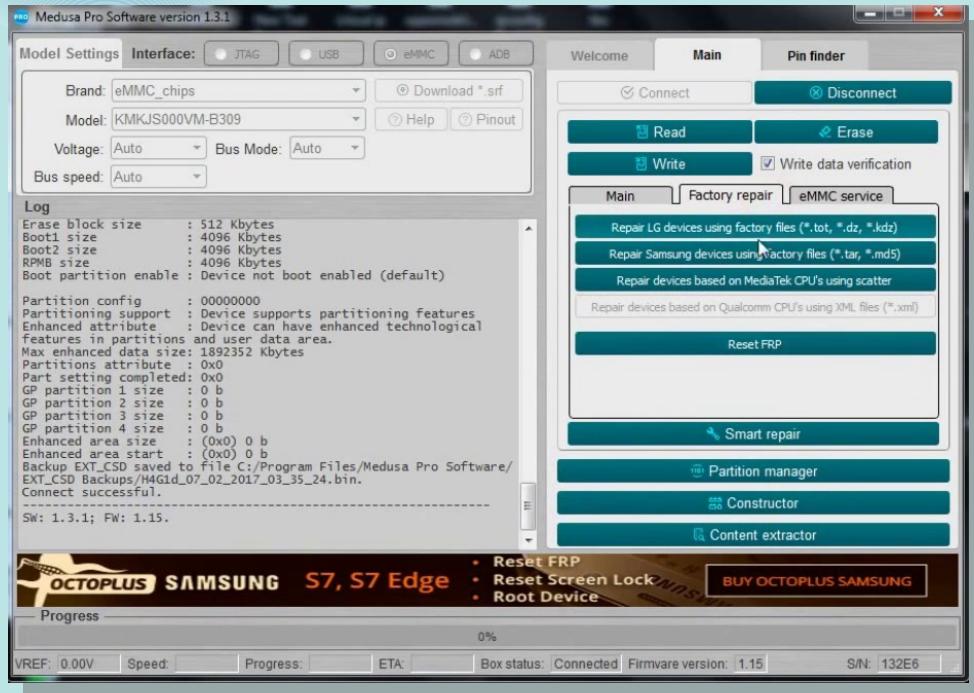
EMMCPRO- ORT



5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

BOXES – CAJAS – INTERFACES WORKING

MEDUSA PRO

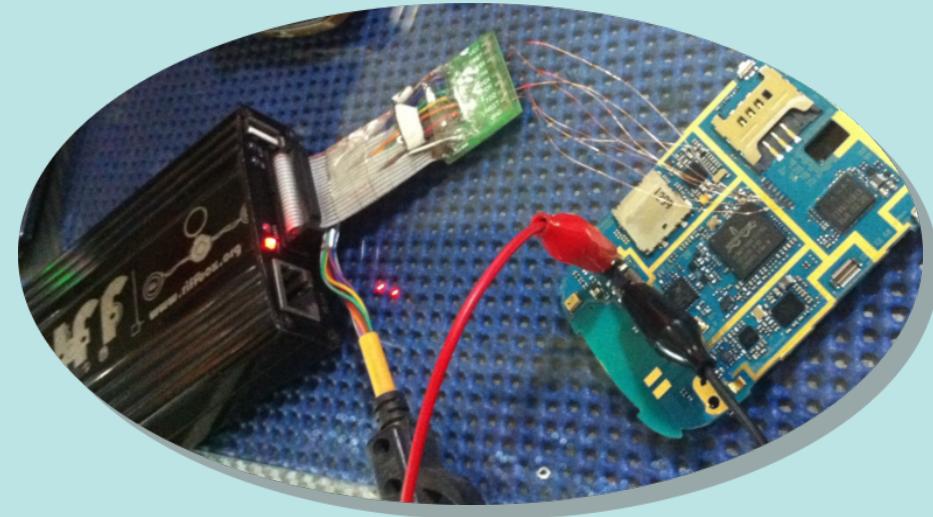
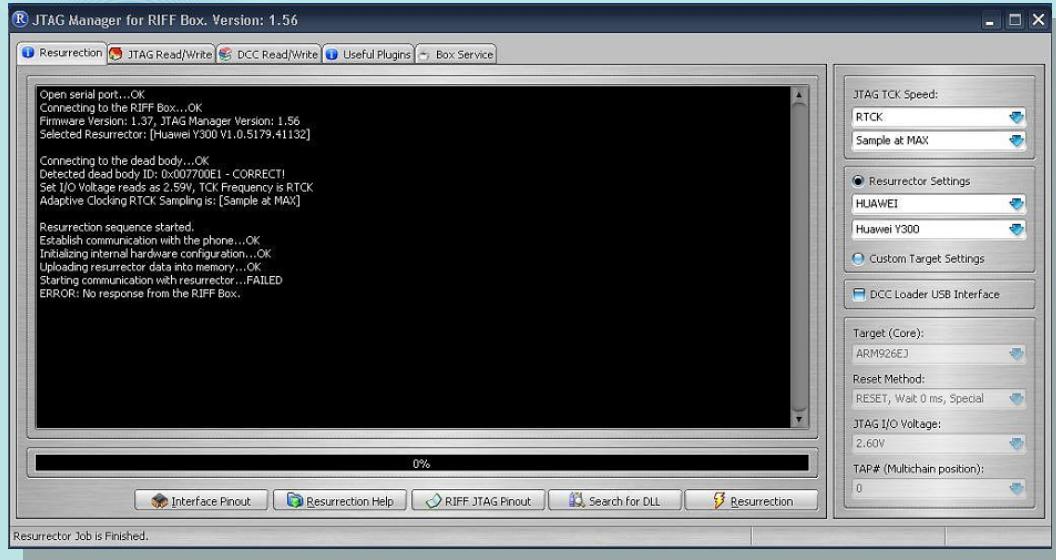


* ISP

5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

BOXES – CAJAS – INTERFACES WORKING

RIFF BOX



* **JTAG**

RIFF → RIFF 2

5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

BOXES – CAJAS – INTERFACES WORKING

NUPROG-E
(MEMORIA UFS)





5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

(offline)

PASOS PROCESO CHIP-OFF lectura online (p.e.)

- 1) Preparar la placa para disipar calor y retirar epoxy
- 2) Calentar y retirar el ic memoria, procesador y/o eprom
- 3) Limpiar y preparar los chip para reboleado
- 4) Colocar los componentes extraídos en placa destino
- 5) Calentar para ajustar y soldar
- 6) Preparar adquisición con operaciones necesarias



HERRAMIENTAS PARA ANÁLISIS

TOOLS DE PAGO RECONOCIDAS

- Cellebrite (la pepa para los amigos)
- XRY
- Oxygen
- X-ways
- Belkasoft
- y otras ...



* Válido también para condiciones extremas



HERRAMIENTAS PARA ANÁLISIS

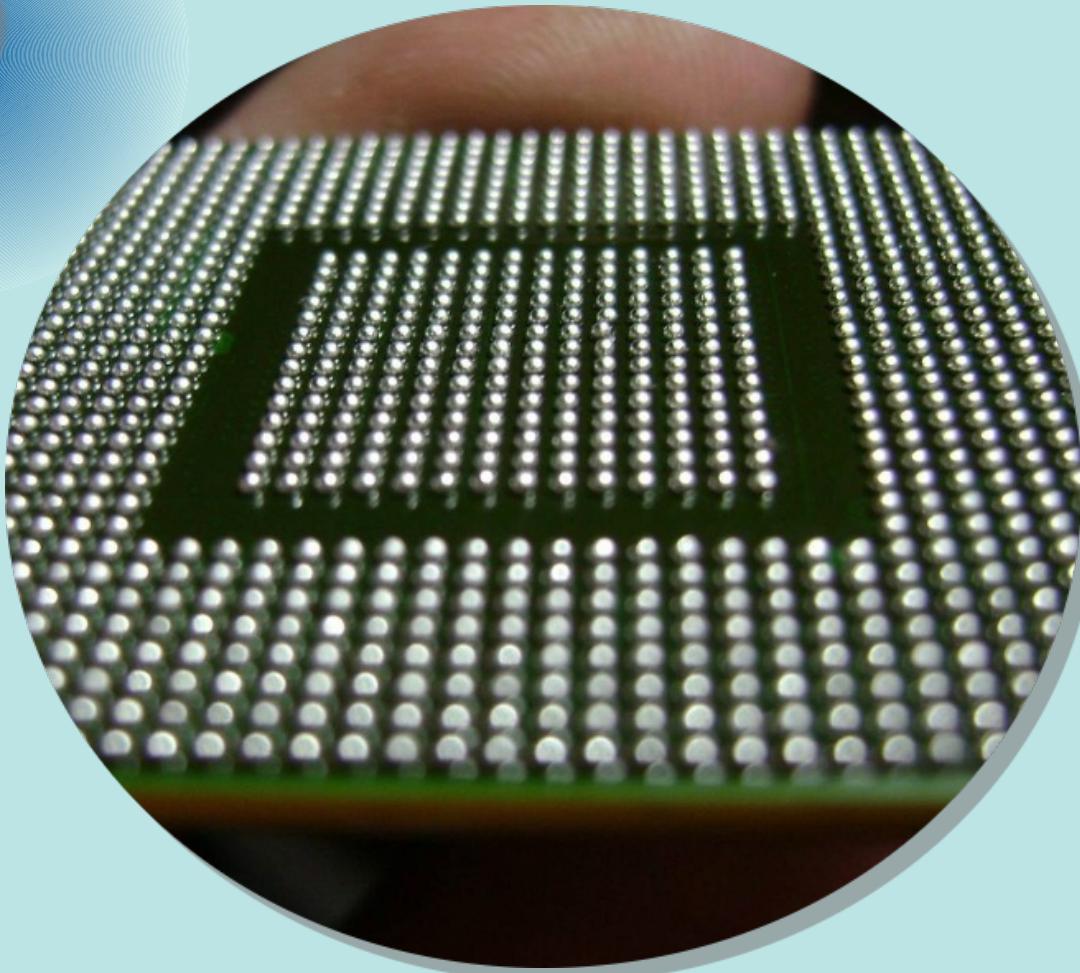
SOFTWARE PARA ANÁLISIS – Después de adquisición...

- **FTK imager lite**
- **Autopsy**
- **Repositorios GitHub y GitLab**
- **Nuestros Artifacts**
- **Y los ya mencionados de pago**





5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF



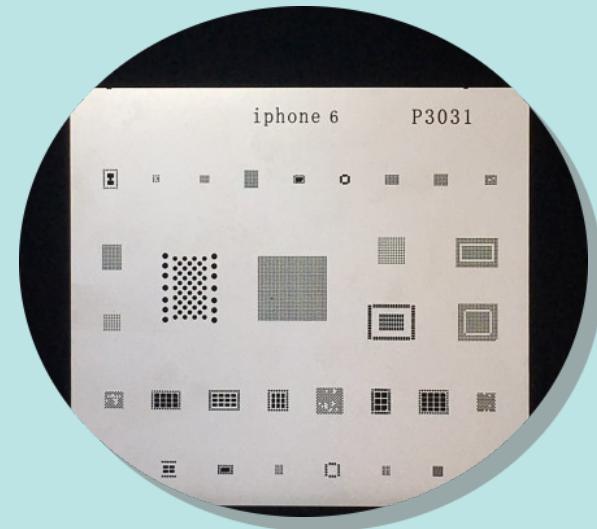
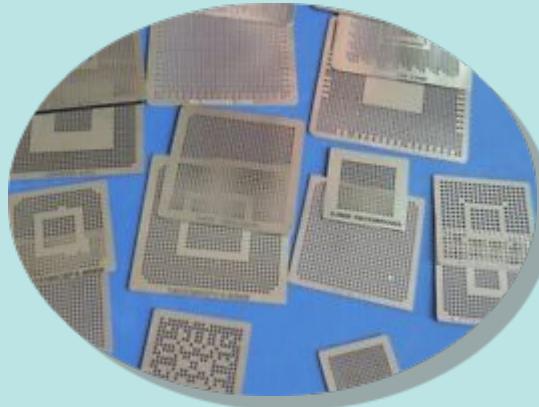
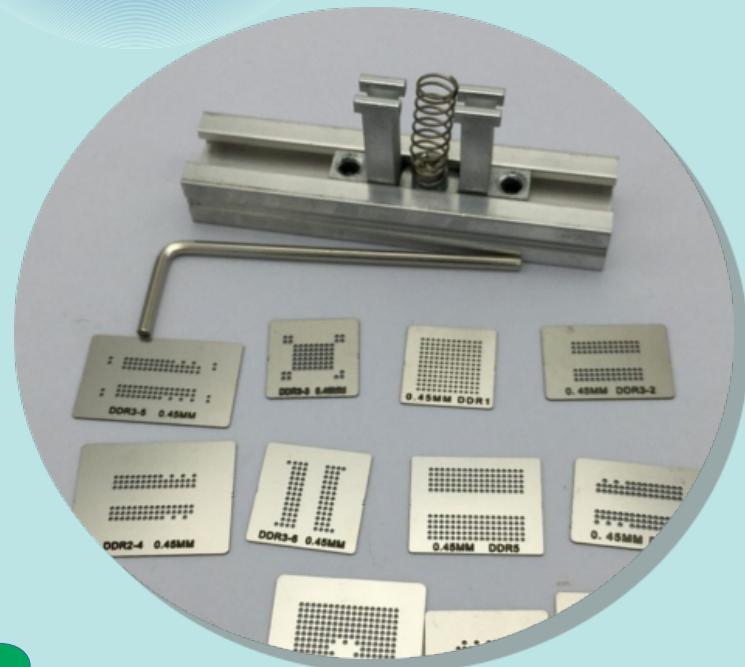
REBALLING

Volver a colocar bolas

- 1) limpiar ic
- 2) colocar ic en soporte
- 3) seleccionar plantilla
- 4) repartir bolas (*)
- 5) retirar plantilla
- 6) calentar para ajustar

5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

GADGETS DE REBALLING

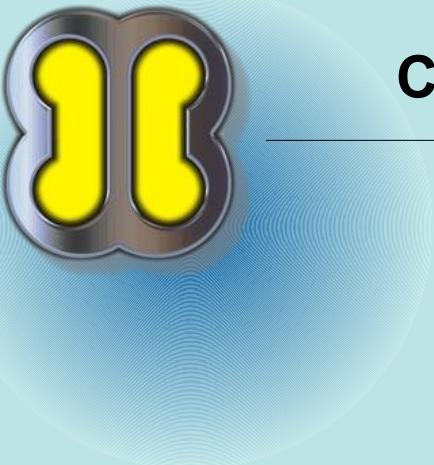




5) TÉCNICAS INVASIVAS ADQUISICIÓN – CHIP-OFF

GADGETS DE REBALLING



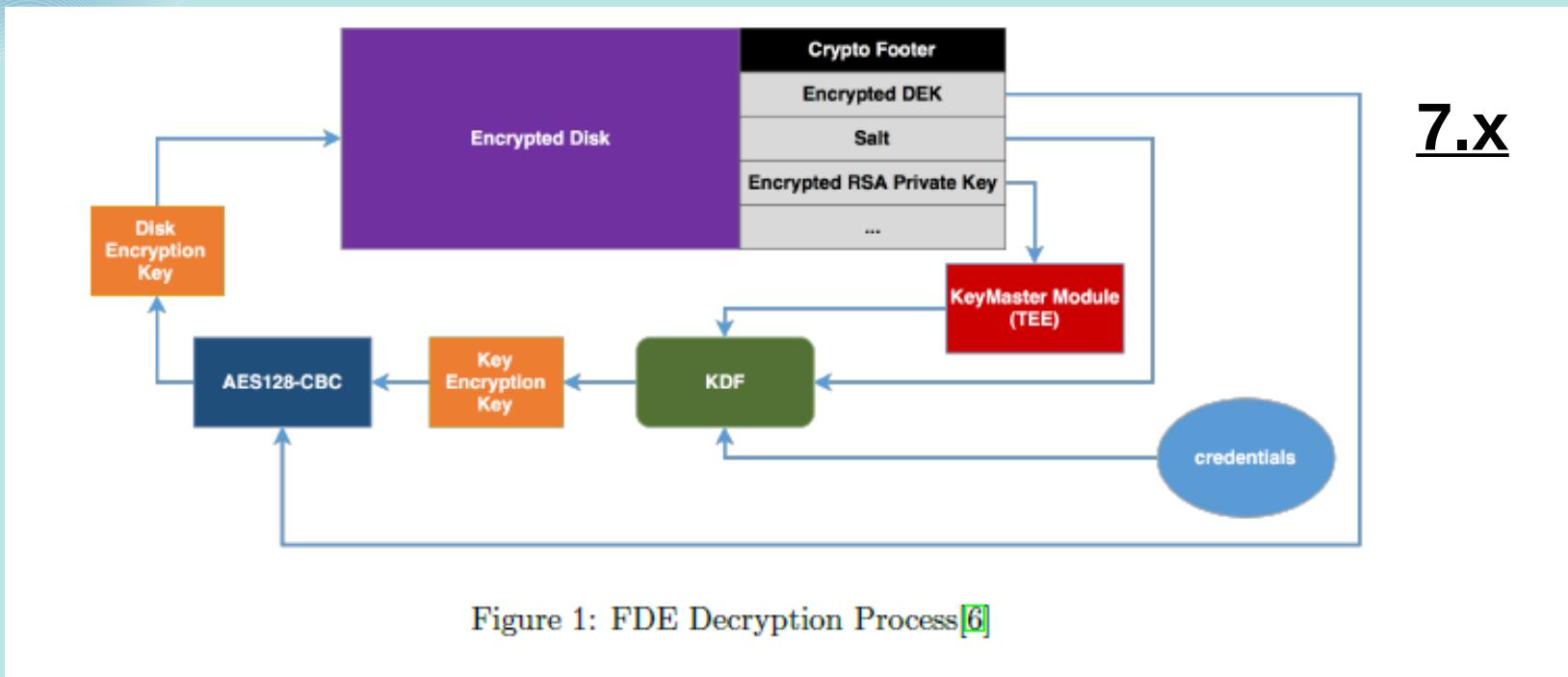


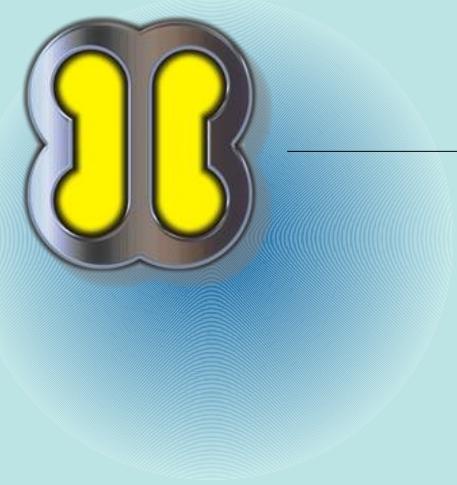
CONCLUSIONES

- **Conocer el ambiente del procesador del terminal**
- **Documentar gráficamente**
- **Limitar el estrés a los componentes**
- **Limitar la disipación de calor**
- **La química siempre es nuestra amiga**
- **Nuestro límite es el cifrado del terminal**
- **En casos normales cuidar la integridad del software**

LINEAS FUTURAS DE INVESTIGACIÓN

- Ampliación del estado del arte en memorias UFS
- El cifrado del área de datos





Puesta en escena chip-off



AGRADECIMIENTOS

- A TODOS LOS PRESENTES
- A LA ORGANIZACIÓN DE NAVAJA NEGRA
- A SARA POR SU COLABORACIÓN Y ASISTENCIA
- A WWW.PHONEPARTS.ES por ceder una estación nueva
- A LONGINOS RECUERO por animarme a venir
-
- A ANTONIO SANZ por su tiempo, revisiones y aportaciones

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



AGRADECIMIENTOS

¿PREGUNTAS?

