

Who am I

```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

- Graduado en Ingeniería Informática UNED
- Máster en Ciberseguridad UNED
- Consultor de seguridad S2 Grupo
- Desarrollo de herramientas forense móviles en S2 Grupo



nomed1



Agradecimientos

```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

Que luego pasa lo que pasa!!!!

- A la organización de Honey CON
- A los compañeros de S2 Grupo



Motivaciones

Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.



VS



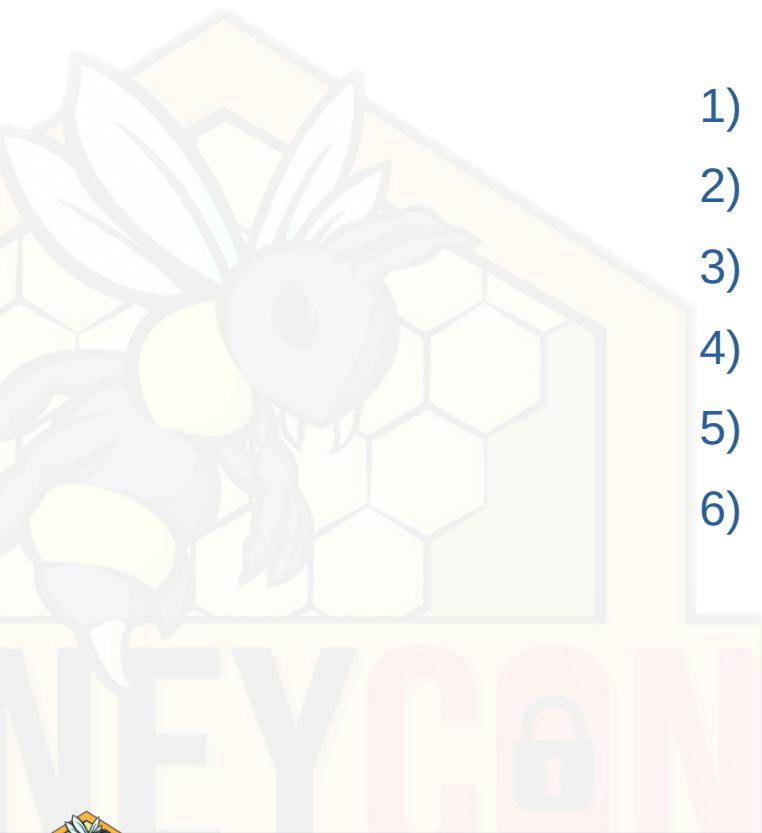
Análisis forense en dispositivos Android en casos extremos:
Entrando al laboratorio

Buenaventura Salcedo Santos-Olmo

[LinkedIn](#) [Twitter](#) nomed1



Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.

- 
- 1) Visión general
 - 2) Tipos de adquisiciones
 - 3) Caso de uso
 - 4) Explicación del proceso
 - 5) PoC con MSAB XRY
 - 6) Resultados



Problemática

- Fragmentación de modelos
- Fragmentación del firmware
- Fragmentación del hardware
- Fragmentación parches de seguridad
- Herramientas desfasadas
- Distintos estados de los dispositivos

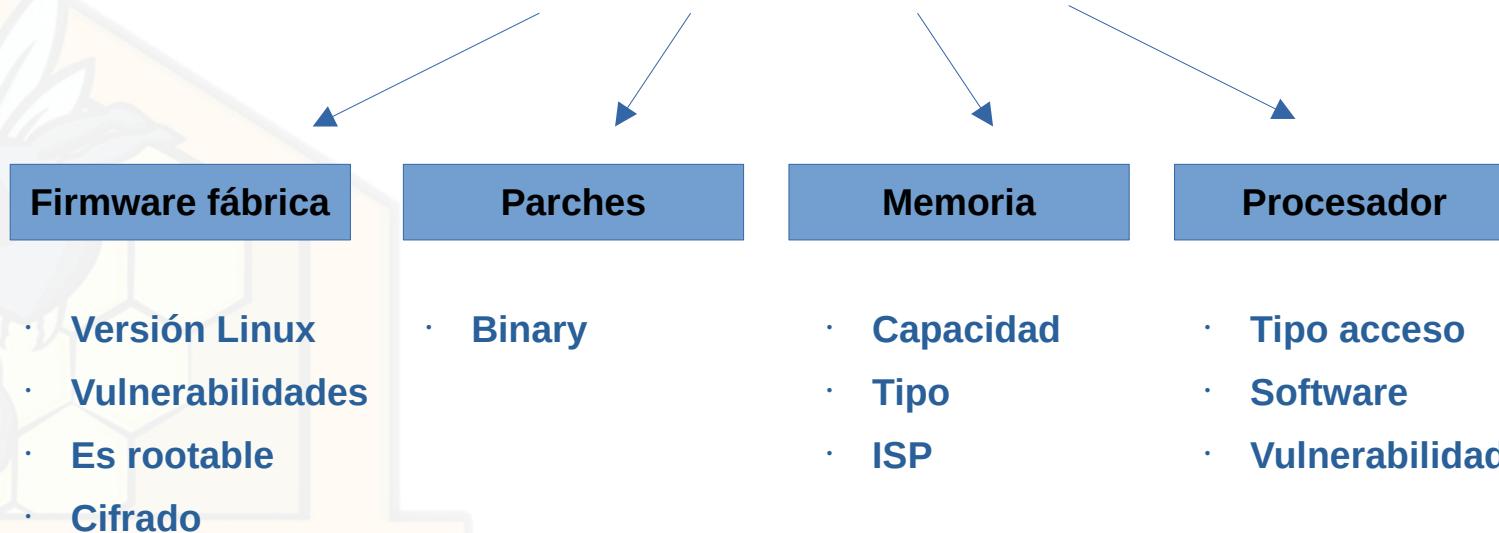


Para empezar

Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.

IDENTIFICACIÓN

Marca + Modelo



```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

Cifrado de datos “a partir” de Android 6.0



Lógica Manual

El terminal está **desbloqueado**

- Si no queda otro remedio
- Se grabaría el proceso con una **cámara**.
- Utilizaríamos copy/paste desde el propio **explorador del dispositivo**
- El destino sería por ejemplo una **tarjeta de memoria**.
- **.APK** que realizase el proceso teniendo en cuenta este **nivel de privilegios**.
 - Titanium backup
 - Migrate
 - Helium
 - OAndBackup



```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

Lógica adb backup + pull

El terminal está **desbloqueado**

- Se realiza el backup y se desempaquetá con **abe.jar**
- Las apps sin backup flag **no se obtienen**
- Se puede usar **apk downgrade**
- Sin root no hay acceso al área de usuario
- Hay info protegida accesible con **apks con privilegios**
- El pull captura también el área compartida visible con **MTP**
- Podríamos hacer uso de **My Phone Explorer**

```
$ adb backup -apk -shared -all -f backup.ab
$ java -jar abe.jar unpack backup.ab destino.tar
```



```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

Lógica para DFIR

El terminal está **desbloqueado**

- Dumpsys
- Logs
- Bugreports
- Logcat
- Algunos otros comandos adb shell

```
$ adb shell dumpsys -l
$ adb shell dumpsys <servicio>
$ adb shell dumpstate
$ adb bugreport salida.zip
```

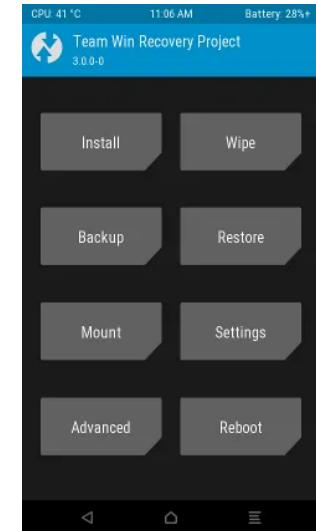


Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.

Física Custom Recovery

Modo recovery personalizado

- Hay que flashear la **partición recovery**
- Puede existir backup que lo activa el secure boot
- Solución: nada más flashear hacer **secuencia de botones**
- Recuperar **bricks y actualizar**
- Puede requerir **bootloader unlocked**
- Hay que montar las unidades con **Mount**
- Usar para **rootear** el dispositivo con **Install**
- Usar para hacer copia bit a bit, **si el dispositivo concede permisos con Backup**
- Hay menor riesgo que haciendo root
- Hay dos tipos de **TWRP**
 - Oficial en la web, funcionan 100%
 - No oficial: PORTS, pueden brickear el dispositivo



```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

Física ROOT

El terminal está **desbloqueado**

- Requiere **root**
- Se realiza con **dd**
 - A una sdcard
 - A través de netcat

TERMINAL DISPOSITIVO

```
$ adb forward tcp:7000 tcp:7000
$ adb shell
$ su
# dd if=particion | nc -l -p 7000
```

```
$ adb shell
$ su
# mount
# dd if=particion of=/sdcard/destino
```

EQUIPO FORENSE

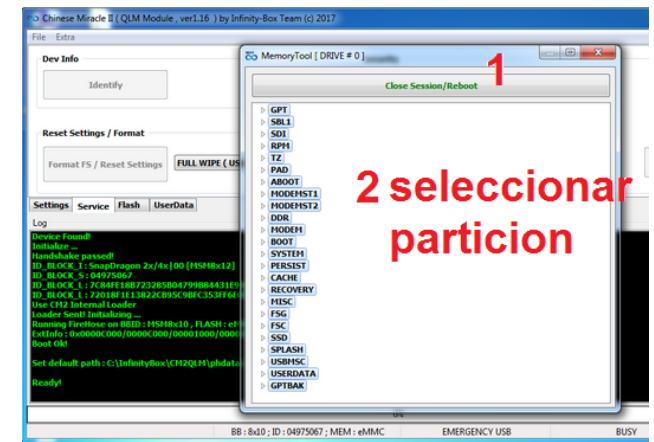
```
$ nc 127.0.0.1 7000 > dump.img
```

Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.

Física DUMP

El terminal **NO** está desbloqueado

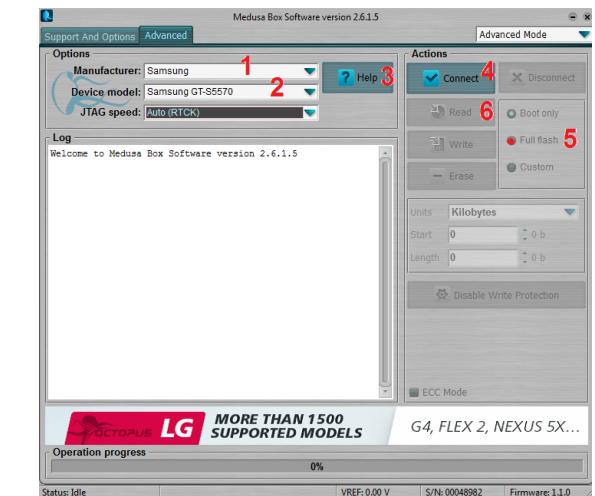
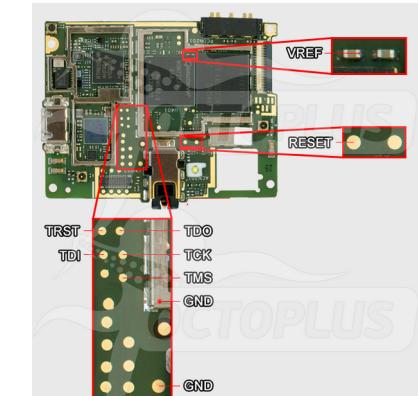
- Recordemos los modos de conexión
- Hay modos no invasivos que nos permitían adquirir las particiones
- Flashtools en MTK
- Firehose/Sahara en Qualcomm
- Download Mode (LG, Samsung)
- Boxes de servicio técnico
- **Herramientas de pago forenses**



```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

Física JTAG

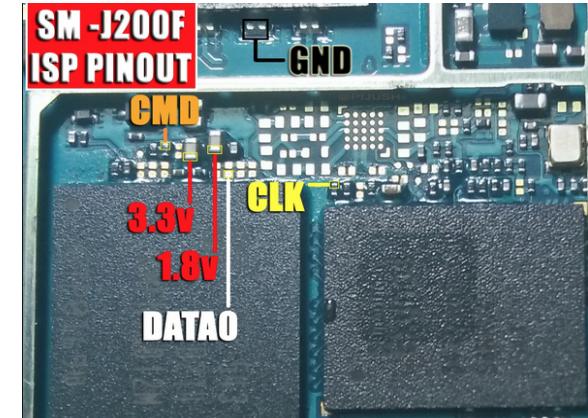
- **Join Test Action Group**, test hardware, debug
- Estándar desde 1985 en **sistemas embebidos**
- Son puntos para probar circuitos Test Access Ports (TAP)
- Atacamos al **procesador** para acceder a memoria
- Obtenemos los **datos brutos** de memoria
- Necesitamos un **loader**
- Necesitamos una **interfaz para los jtags**
- Soldar en placa, usar molex o agujas retráctiles (*)
- **No se destruye** el terminal



```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

Física ISP

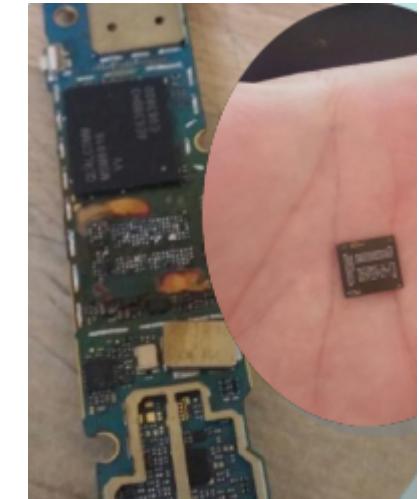
- In System Programming
- Presentes en la cercanía de la memoria
- Escritura/Lectura de memoria
- Válido también pendrives y mas placas
- Los pinouts se obtienen experimentalmente
- Tipos de memorias EMMC y UFS



```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

Física 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
- **DESTRUYE** el terminal
- Podríamos necesitar **procesador** y eeprom (casos de cifrado)
- Puede usarse para **traslado de componentes** a otra placa



```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

Física TP

- Aporte **adicional** a DUMP saltando protección
- Correr el software necesarios, se mantendrá a la espera
- **Puede o no necesitar** conectar la batería
- Esperar el fichero **dump resultante**
- También puede usarse con **modificaciones de firmware**
- **Escribir** custom firmware, exploits o parches



```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

más: Análisis forense casos extremos: <https://www.youtube.com/watch?v=fhWqLeQDA9o>



Análisis forense en dispositivos Android en casos extremos

Buenaventura Salcedo Santos-Olmo

```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

Huawei P9 lite

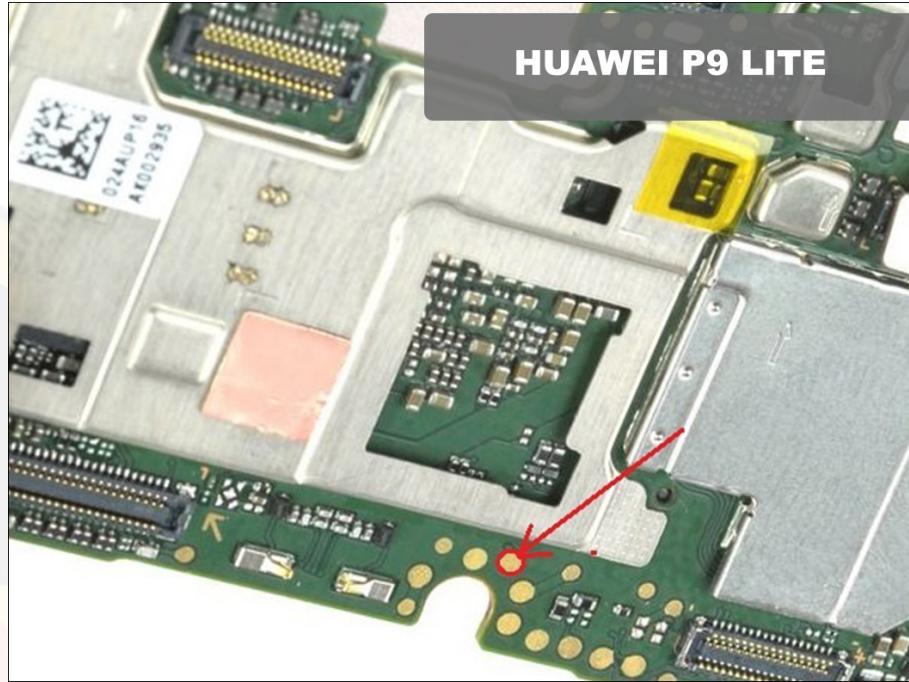
- Tiene código de seguridad
- El dispositivo esta mojado
- La placa ya ha sido tratada
- La pantalla no funciona aunque se cambie
- La tapa está sellada de serie
- Procesador KIRIN 650
- Utilizaremos MSAB XRY
- Método de adquisición: Física con TP



Explicación

```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

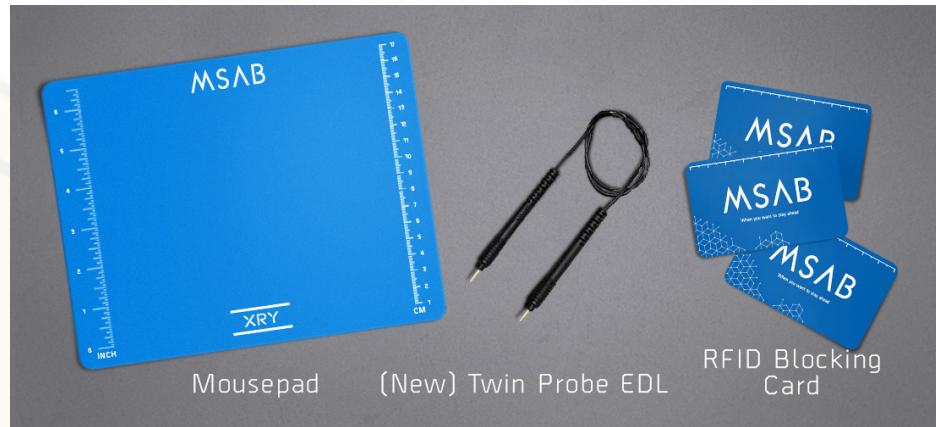
El proceso consiste ...



PoC

Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.

PoC



HoneyCON 2021

Buenaventura Salcedo - Ponencia: TP Venganza!

Resultados

Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.



Preguntas

```
Fixing /system/app permissions...
Fixing /data/app permissions...
Fixing /data/data/ permissions
Done fixing permissions.
```

