20 DE MARZO DE 2024

INTRODUCCIÓN A LA DEPURACIÓN USB Y ADB

ANÁLISIS FORENSE INFORMÁTICO

ERIC SERRANO MARIN
CETI

Contenido

Muestre, de manera ordenada, el sistema de archivos de mayor a menor (los 10 primeros)

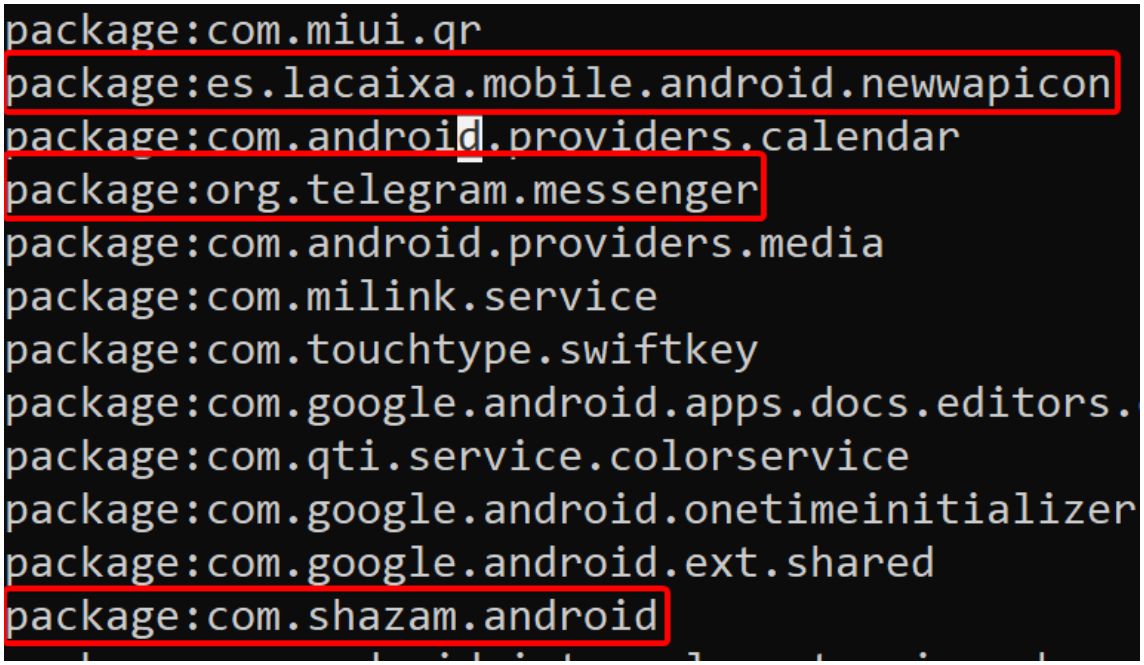
```
grus:/ $ df | sort -nrk4 | head -n 10
/dev/fuse         53417456 39615552  13654448  75% /storage/emulated
/dev/block/sda29  53417456 39615552  13654448  75% /data
tmpfs              2859036        0   2859036   0% /mnt
tmpfs              2859036        0   2859036   0% /apex
none               2859036        0   2859036   0% /sys/fs/cgroup
tmpfs              2859036     1328   2857708   1% /dev
/dev/block/sda28    999320   625764    346688  65% /cust
/dev/block/sda27    237536    10884    218792   5% /cache
/dev/root          3555292  3418116    120792  97% /
/dev/block/dm-1    1523628  1491968     15276  99% /vendor
```

Muestre los paquetes instalados en el dispositivo Android. ¿Cuántos tiene instalados? Muestre el nombre del package de 3 APP conocidas

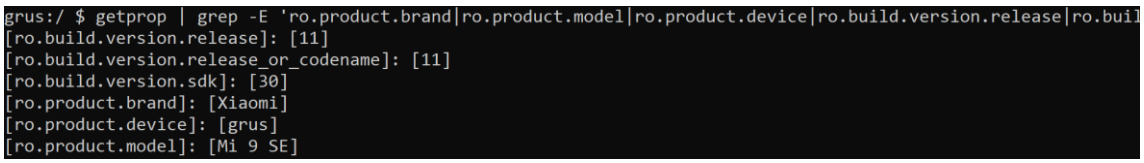
```
grus:/ $ pm list packages | wc -l
373
grus:/ $
```

```
grus:/ $ pm list packages
package:com.miui.screenrecorder
package:com.sofascore.results
package:com.android.cts.priv.ctsshim
package:com.google.android.youtube
package:com.mcdonalds.android
package:com.qualcomm.qti.qcolor
package:com.android.internal.display.cutout.emulation.corner
package:com.google.android.ext.services
package:com.qualcomm.qti.improvetouch.service
package:com.android.internal.display.cutout.emulation.double
package:com.android.providers.telephony
package:com.android.dynsystem
package:com.miui.powerkeeper
```

Conocidas: Caixa, Telegram y Shazam.



Muestre los valores de las diferentes propiedades del dispositivo Android. Muestre 5 características importantes de su dispositivo.



ro.product.brand: Marca del dispositivo.

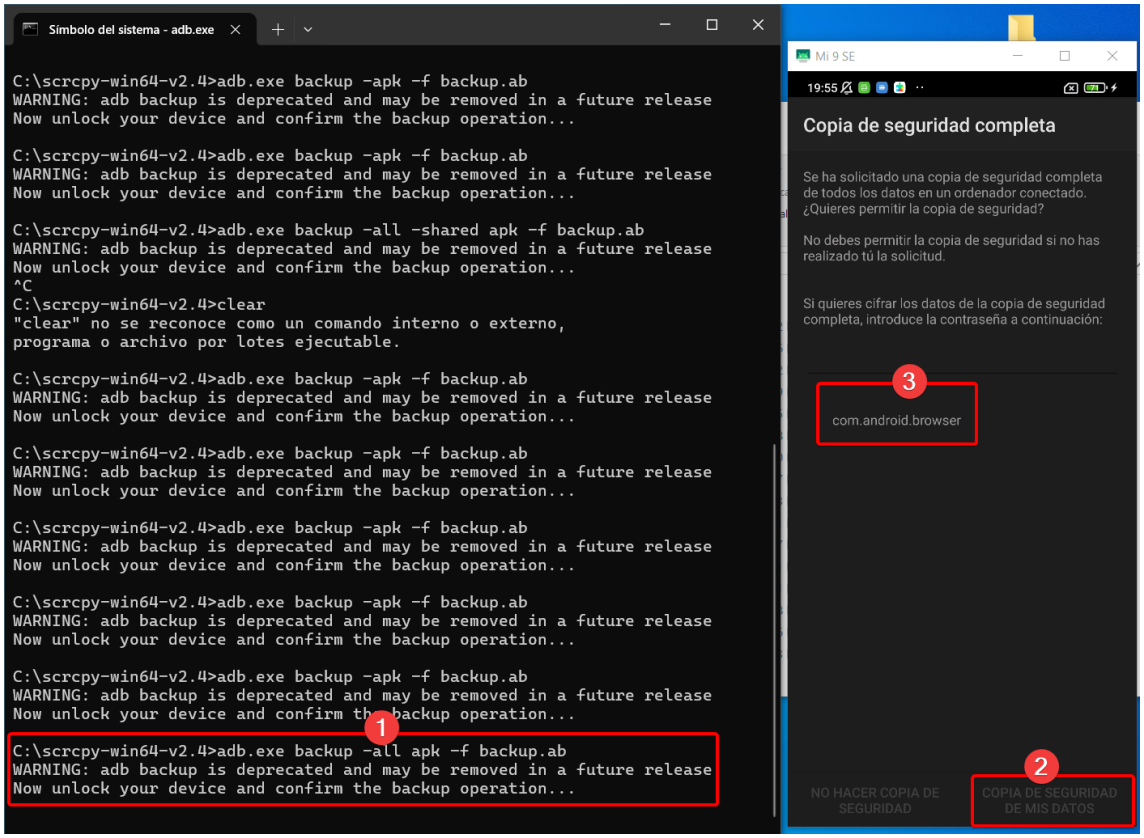
ro.product.model: Modelo del dispositivo.

ro.product.device: Nombre del dispositivo.

ro.build.version.release: Versión de Android.

ro.build.version.sdk: Número de SDK de Android.

Realice una copia de seguridad de todas las APP



```
C:\scrcpy-win64-v2.4>adb.exe backup -apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -all -shared apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...
^C
C:\scrcpy-win64-v2.4>clear
"clear" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\scrcpy-win64-v2.4>adb.exe backup -apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -all apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...
```

Copia de seguridad completa

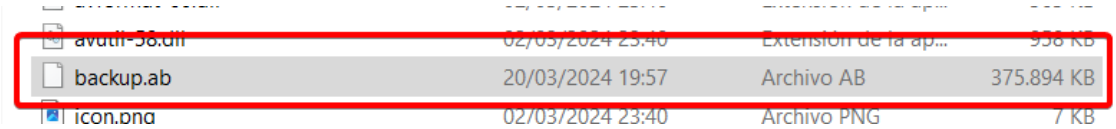
Se ha solicitado una copia de seguridad completa de todos los datos en un ordenador conectado. ¿Quieres permitir la copia de seguridad?

No debes permitir la copia de seguridad si no has realizado tú la solicitud.

Si quieres cifrar los datos de la copia de seguridad completa, introduce la contraseña a continuación:

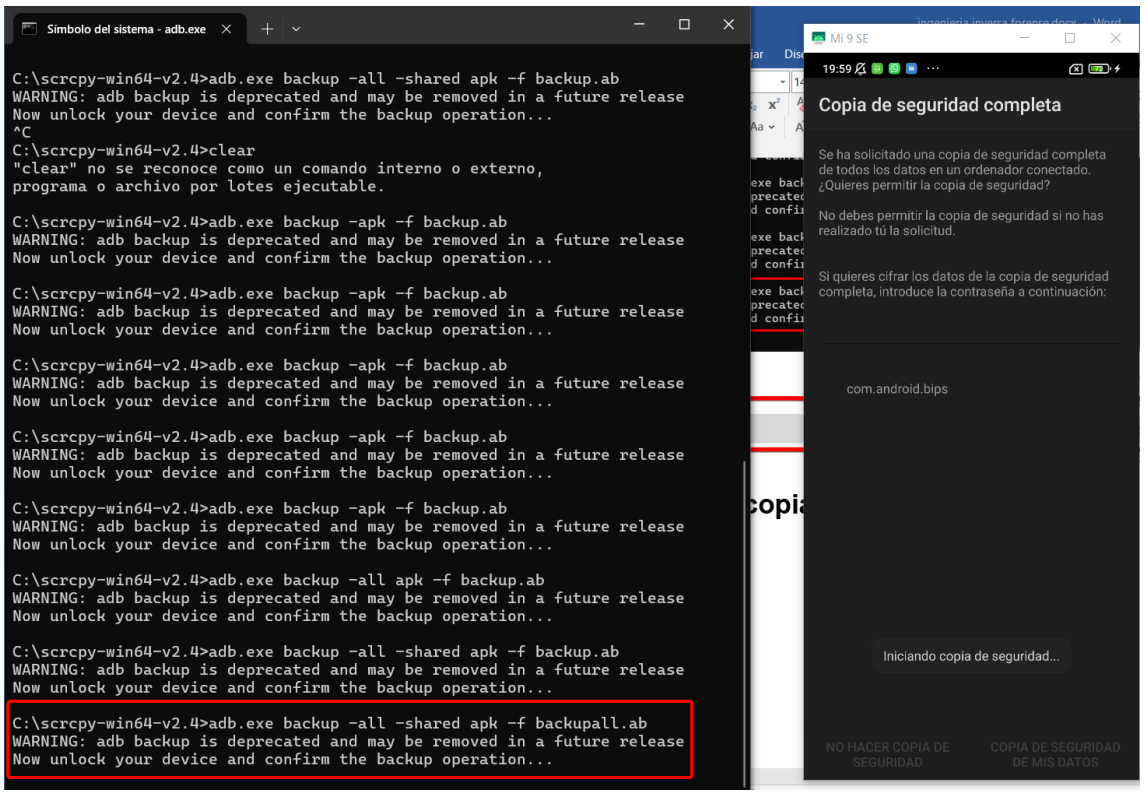
com.android.browser

NO HACER COPIA DE SEGURIDAD | COPIA DE SEGURIDAD DE MIS DATOS



avutil-58.dll	02/03/2024 23:40	Extensión de la ap...	958 KB
backup.ab	20/03/2024 19:57	Archivo AB	375.894 KB
icon.png	02/03/2024 23:40	Archivo PNG	7 KB

Realice una copia de seguridad de toda la información del sistema.



```
C:\scrcpy-win64-v2.4>adb.exe backup -all -shared apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...
^C
C:\scrcpy-win64-v2.4>clear
"clear" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\scrcpy-win64-v2.4>adb.exe backup -apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -all apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -all -shared apk -f backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...

C:\scrcpy-win64-v2.4>adb.exe backup -all -shared apk -f backupall.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...
```

Copia de seguridad completa

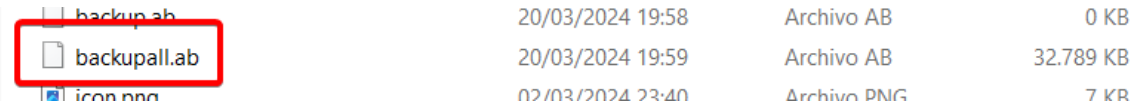
Se ha solicitado una copia de seguridad completa de todos los datos en un ordenador conectado. ¿Quieres permitir la copia de seguridad?

No debes permitir la copia de seguridad si no has realizado tú la solicitud.

Si quieres cifrar los datos de la copia de seguridad completa, introduce la contraseña a continuación:

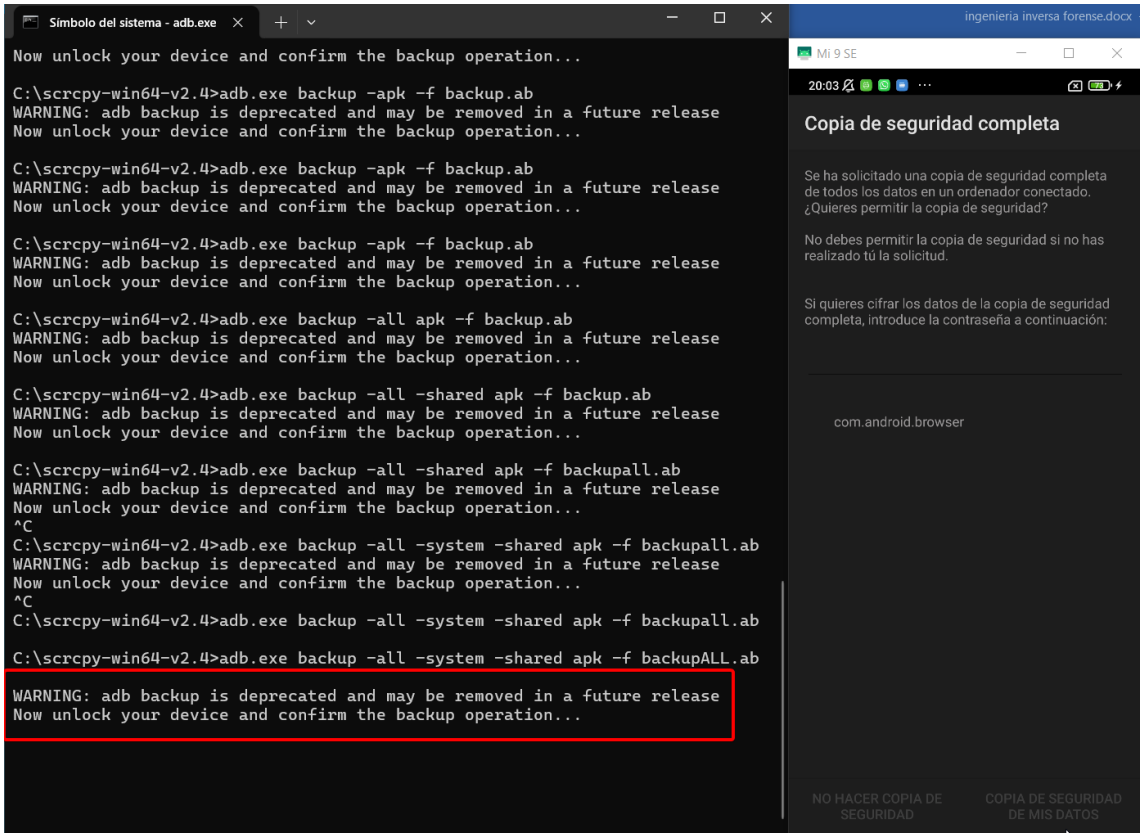
com.android.bips

Iniciando copia de seguridad...

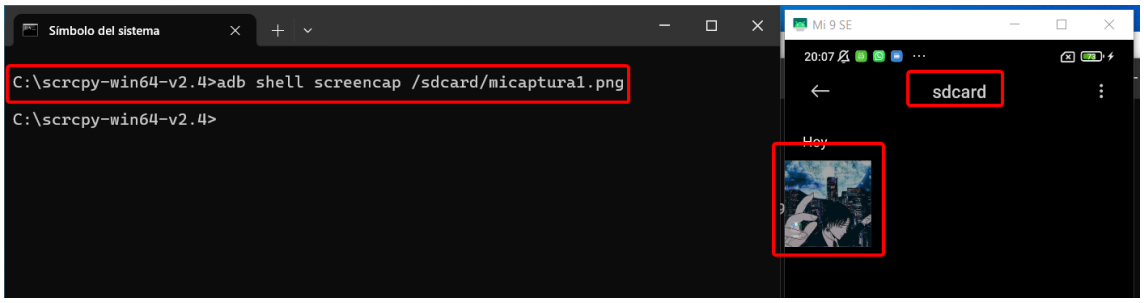


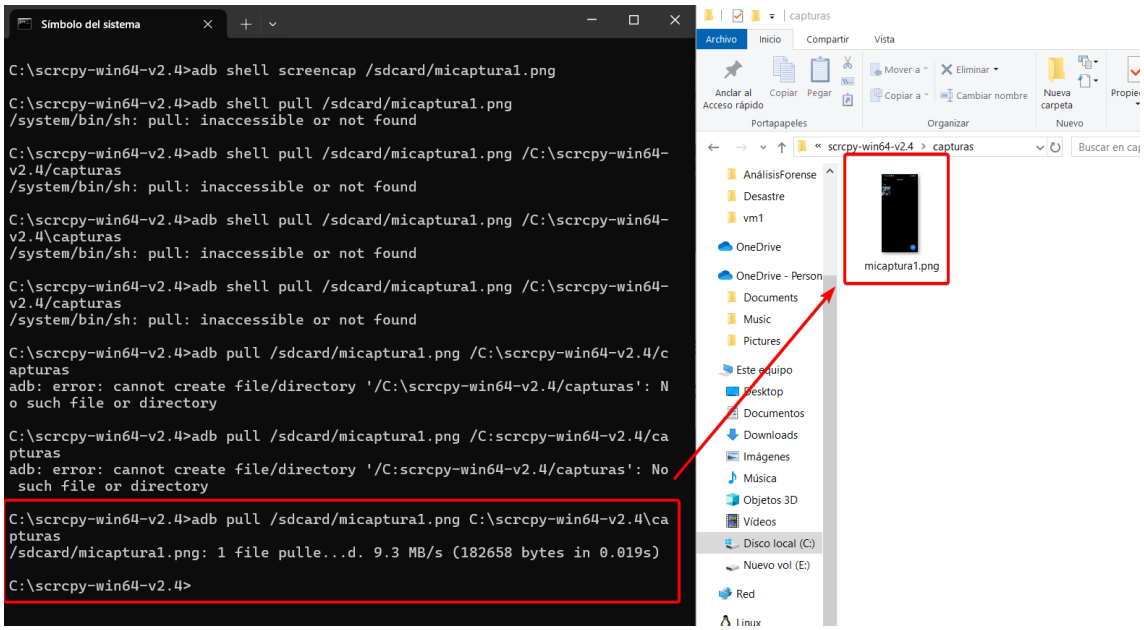
backup.ab	20/03/2024 19:58	Archivo AB	0 KB
backupall.ab	20/03/2024 19:59	Archivo AB	32.789 KB
icon.png	02/03/2024 23:40	Archivo PNG	7 KB

Realice una copia de seguridad

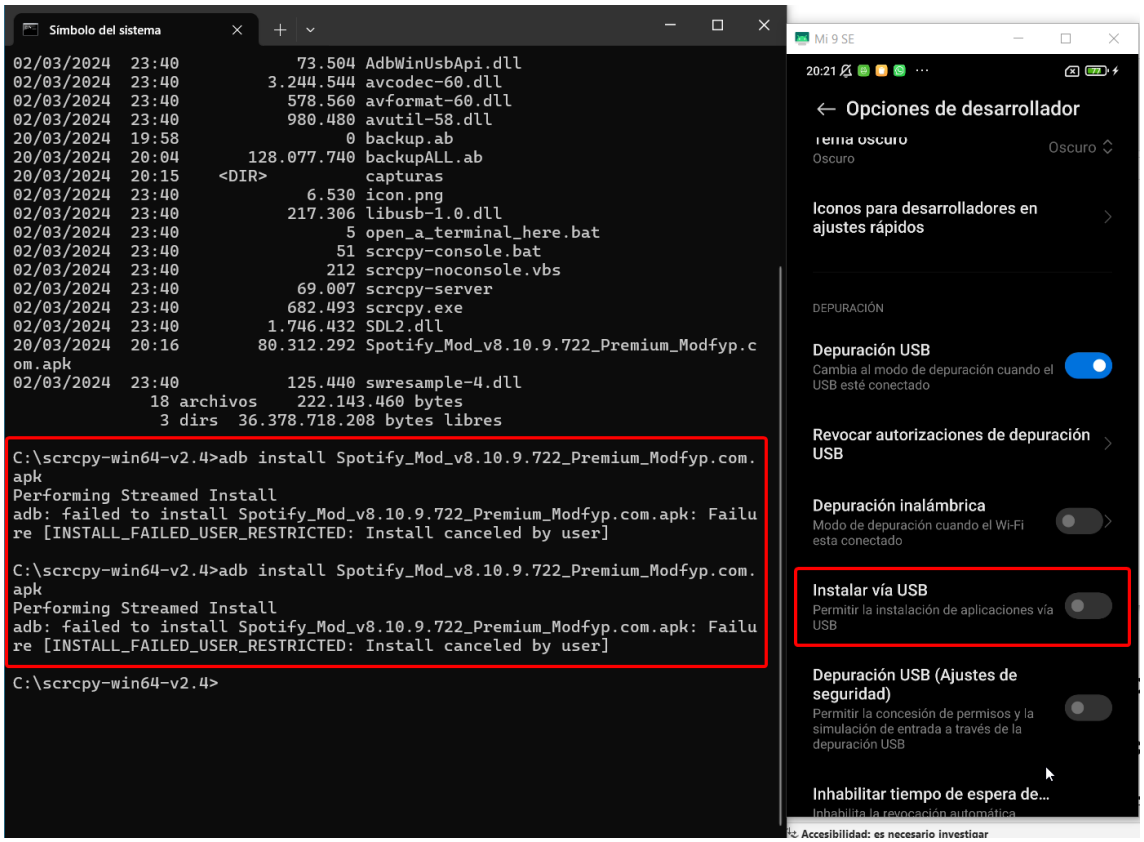


Realice una captura de pantalla con ADB y copie esa captura a su PC local (todo con comandos ADB)



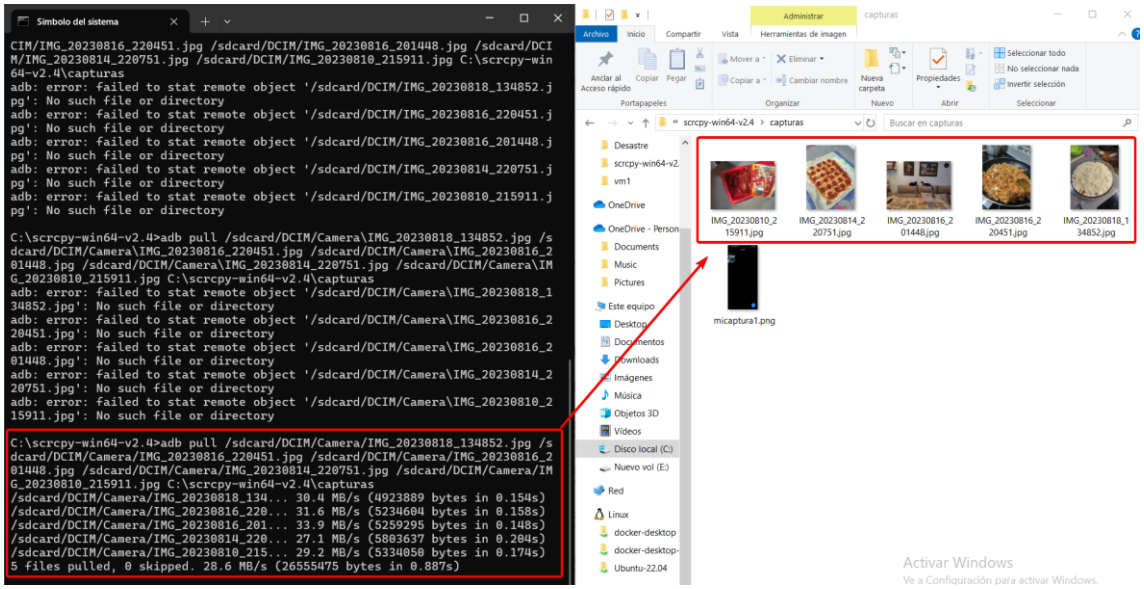


Descargue una APP de Internet "premium" o la que quiera e instálela en su dispositivo Android a través de ADB

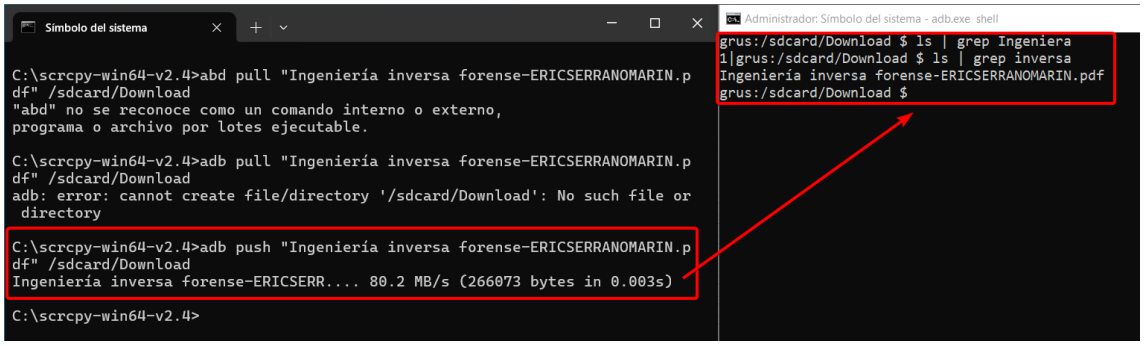


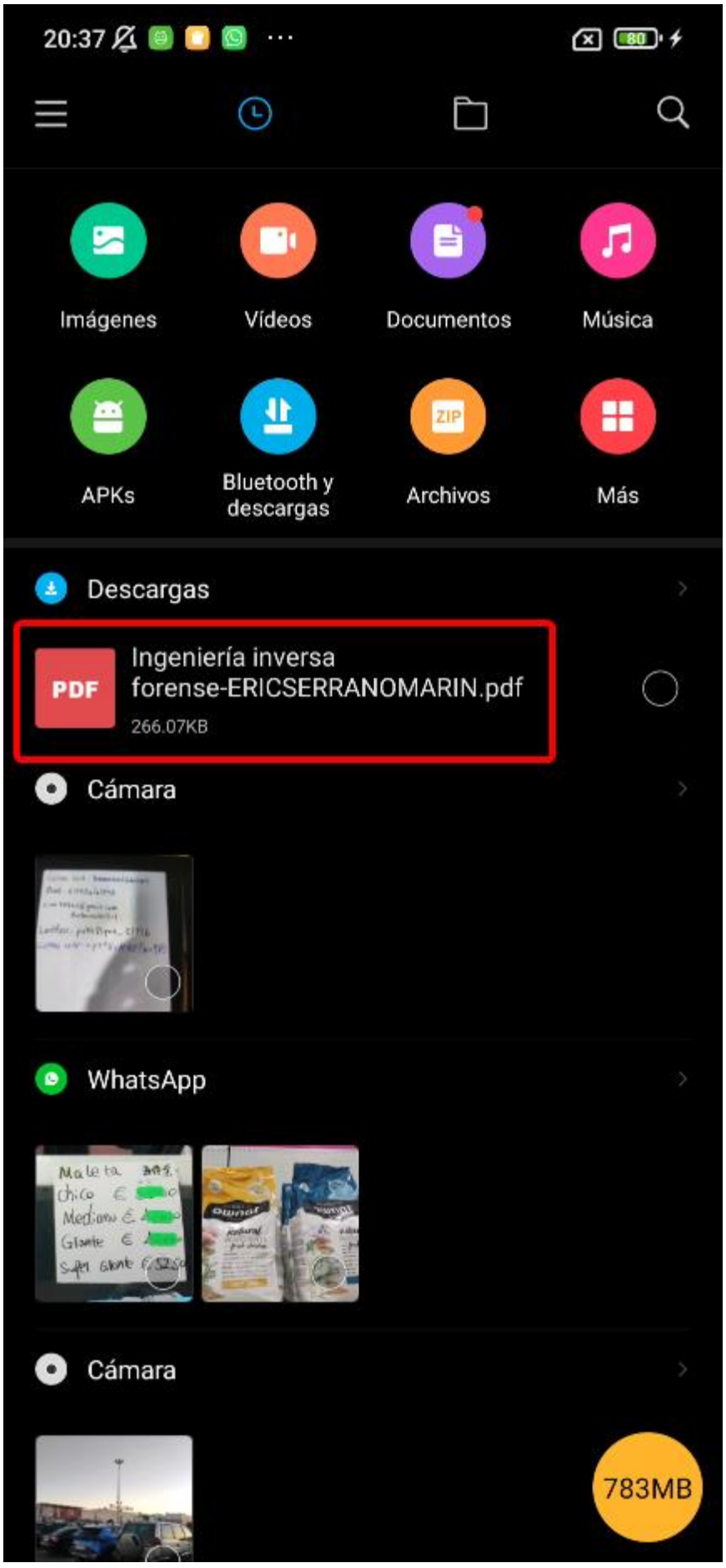
No me ha dejado instalar, ya que hace falta que tenga la SIM metida para poder iniciar sesión en Xiaomi.

Copie 5 fotografías de su dispositivo Android a su PC



Copie PDF de su PC a su dispositivo Android (carpeta de descargas). Compruebe que puede abrirlas con el móvil.




20:37
Imágenes
Vídeos
Documentos
Música
APKs
Bluetooth y descargas
Archivos
Más
Descargas
PDF
Ingeniería inversa forense-ERICSERRANOMARIN.pdf
266.07KB
Cámara
WhatsApp
Cámara
783MB

20 DE MARZO DE 2024

INGENIERIA INVERSA FORENSE

ANÁLISIS FORENSE INFORMÁTICO

ERIC SERRANO MARIN
CETI

Contenido

Reinicie su móvil con comandos ADB

```
C:\scrcpy-win64-v2.4>adb reboot

C:\scrcpy-win64-v2.4>
```

Reinicie su móvil en modo RECOVERY con ADB

```
C:\scrcpy-win64-v2.4>adb reboot recovery

C:\scrcpy-win64-v2.4>
```

Reinicie su móvil en modo FASTBOOT con ADB

Reinicie su móvil en modo BOOTLOADER con ADB

```
C:\scrcpy-win64-v2.4>adb reboot bootloader

C:\scrcpy-win64-v2.4>
```

Muestre los LOGS del sistema con ADB

```
C:\scrcpy-win64-v2.4>adb logcat
--------- beginning of crash
04-11 14:36:09.420   560   560 F libc    : Fatal signal 6 (SIGABRT), code -1 (SI_QUEUE) in tid 560 (init), pid 560 (init)
04-11 14:36:09.447   560   560 F libc    : crash_dump helper failed to exec
04-11 14:36:09.453   568   568 F libc    : Fatal signal 6 (SIGABRT), code -1 (SI_QUEUE) in tid 568 (init), pid 568 (init)
04-11 14:36:09.465   568   568 F libc    : crash_dump helper failed to exec
--------- beginning of system
04-11 14:36:09.606   592   592 I vold    : Vold 3.0 (the awakening) firing up
04-11 14:36:09.606   592   592 D vold    : Detected support for: ext4 ntfs vfat
04-11 14:36:09.609   592   592 D vold    : Found unmanaged dm device named vroot
04-11 14:36:09.609   592   592 D vold    : Found unmanaged dm device named vendor-verity
04-11 14:36:09.609   592   592 W vold    : Failed to LOOP_GET_STATUS64 /dev/block/loop6: No such device or address
04-11 14:36:09.609   592   592 W vold    : Failed to LOOP_GET_STATUS64 /dev/block/loop1: No such device or address
04-11 14:36:09.609   592   592 W vold    : Failed to LOOP_GET_STATUS64 /dev/block/loop3: No such device or address
04-11 14:36:09.609   592   592 W vold    : Failed to LOOP_GET_STATUS64 /dev/block/loop7: No such device or address
04-11 14:36:09.609   592   592 W vold    : Failed to LOOP_GET_STATUS64 /dev/block/loop2: No such device or address
04-11 14:36:09.609   592   592 W vold    : Failed to LOOP_GET_STATUS64 /dev/block/loop5: No such device or address
04-11 14:36:09.609   592   592 W vold    : Failed to LOOP_GET_STATUS64 /dev/block/loop0: No such device or address
04-11 14:36:09.609   592   592 W vold    : Failed to LOOP_GET_STATUS64 /dev/block/loop4: No such device or address
04-11 14:36:09.609   592   592 I vold    : [libfs_mgr]dt_fstab: Skip disabled entry for partition system
04-11 14:36:09.610   592   592 D vold    : VoldNativeService::start() completed OK
04-11 14:36:10.541   642   658 I QISL    : QSEE Interrupt Service Listener Thread is started
04-11 14:36:10.542   642   658 I QISL    : QSEE Interrupt Service Listener was activated successfully
04-11 14:36:10.557   592   592 I Checkpoint: cp_prepareCheckpoint called
```