



RECOPILACIÓN DE INFORMACIÓN DE DISPOSITIVO MÓVIL

SANTIAGO PEÑARANDA MEJIA

2025

BUENO LO PRIMERO QUE VAMOS HACER ES RECABAR INFORMACIÓN DE UN DISPOSITIVO MÓVIL, EXACTAMENTE UN ANDROID, VAMOS HACERLO DE UNA FORMA UN POCO CONVENCIONAL, ALGO POCO COMÚN PERO QUE SIRVE PARA RECABAR MUCHÍSIMA INFORMACIÓN MUY VALIOSA SI ESTAMOS HACIENDO UNA AUDITORÍA A UN MÓVIL.

*PARA ELLO VAMOS A USAR LA HERRAMIENTA DE LA PROPIA ANDROID QUE ES PARA DESARROLLADORES, SE LLAMA **ADB** (ANDROID **D**EBUG **B**RIDGE) ES UNA HERRAMIENTA DE LÍNEA DE COMANDOS QUE TE PERMITE COMUNICARTE CON UN DISPOSITIVO MÓVIL.*

PARA SU DESCARGA VAMOS HACERLA DE LA SIGUIENTE MANERA, LO PRIMERO ES IR A SU PÁGINA OFICIAL Y DESCARGARNOS LA ÚLTIMA VERSIÓN DE ESTA HERRAMIENTA (ES GRATIS).

[HTTPS://DEVELOPER.ANDROID.COM/TOOLS/RELEASES/PLATFORM-TOOLS?HL=ES-419](https://developer.android.com/tools/releases/platform-tools?hl=es-419)

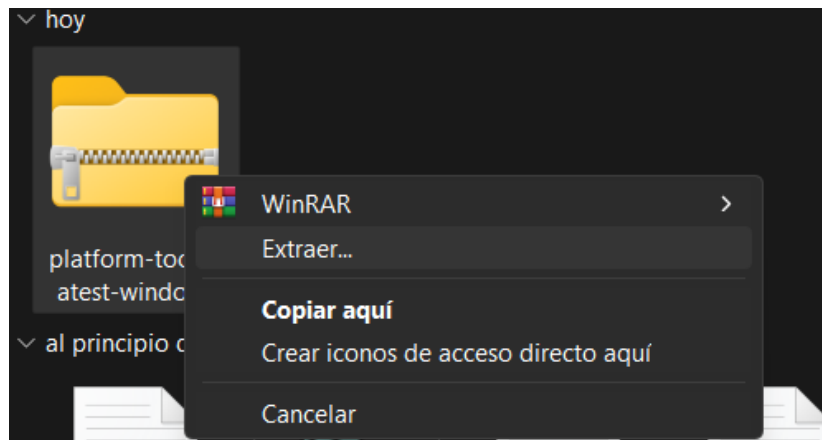


Leí y acepto los Términos y Condiciones anteriores

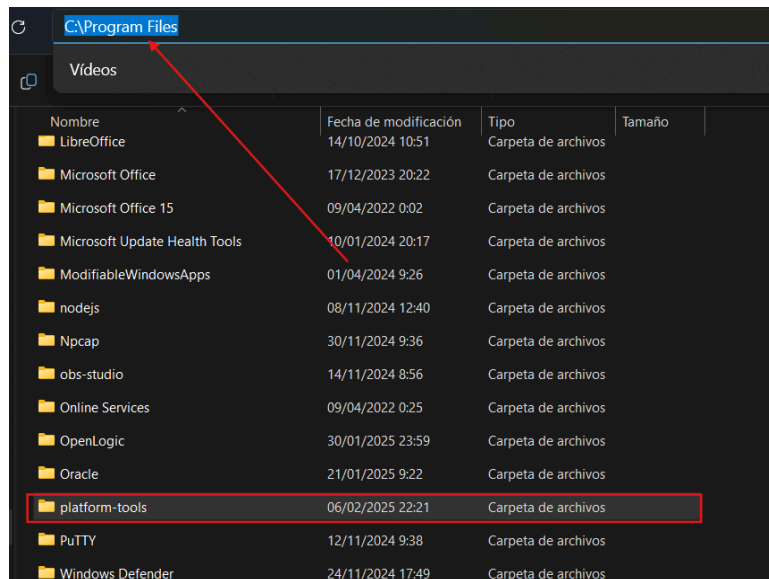
Descargar Android SDK Platform-Tools para Windows

[platform-tools-latest-windows.zip](#)

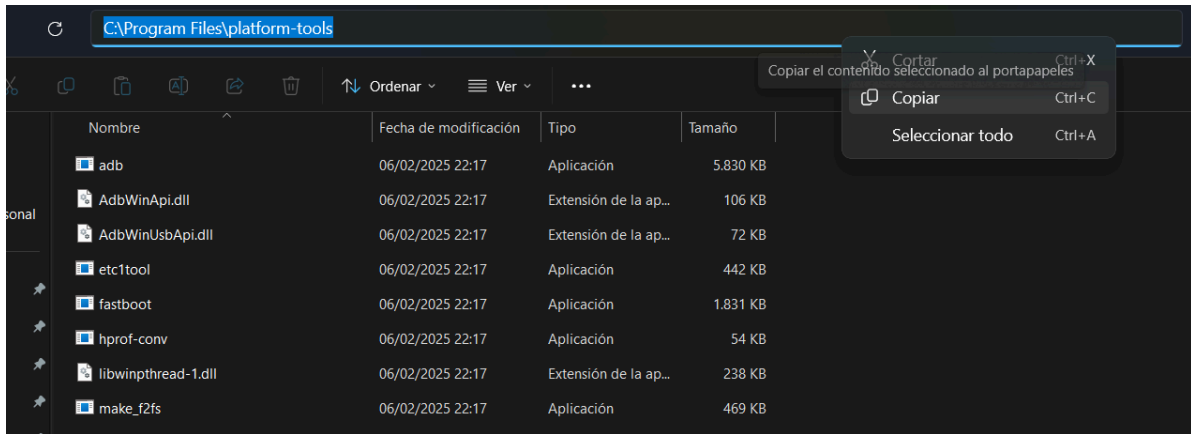
ESTO NOS DESCARGARA UN ZIP (ARCHIVO COMPRIMIDO) EL CUAL VAMOS A EXTRAER.



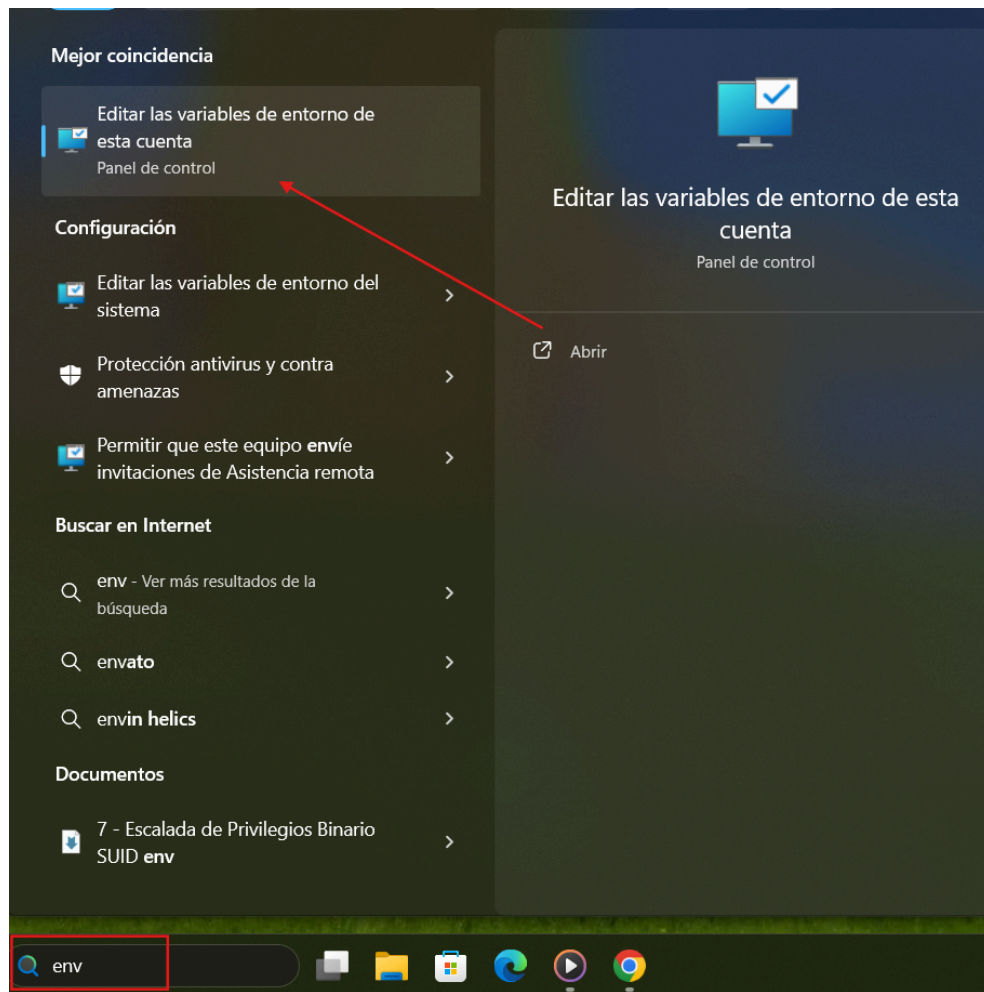
UNA VEZ YA TENGAMOS EXTRAÍDO LOS ARCHIVOS EN UNA CARPETA, VAMOS A MOVERLOS A LA SIGUIENTE UBICACIÓN: (C:\PROGRAM FILES) YA QUE ESTA CARPETA CONTIENE TODOS LOS FICHEROS DE TODAS LAS APLICACIONES DEL ORDENADOR



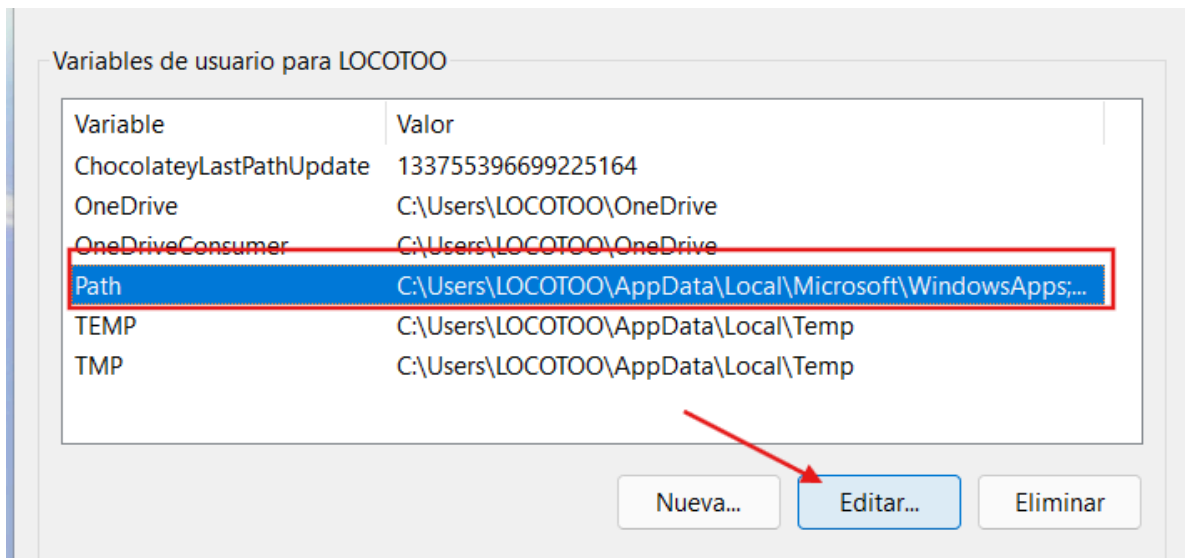
UNA VEZ YA LO TENGAMOS DESCARGADO VAMOS A ENTRAR A LA CARPETA Y COPIAR LA UBICACIÓN DEL FICHERO.



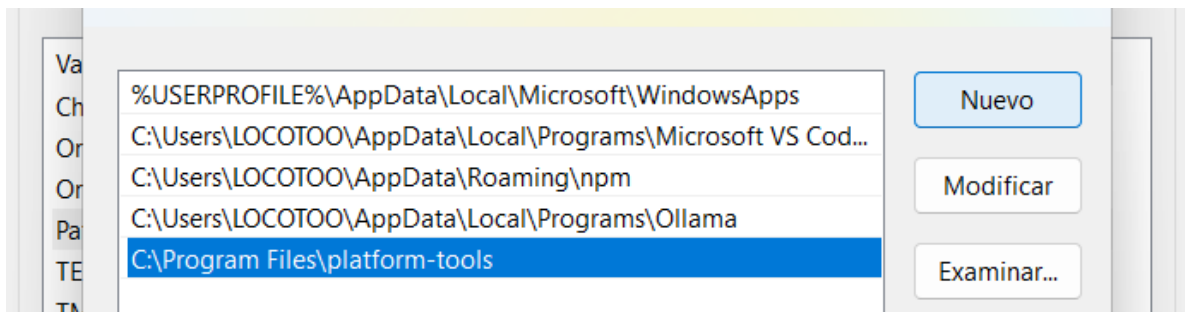
UNA VEZ YA TENGAMOS COPIADO LA UBICACIÓN DEL FICHERO, EN LA BARRA DE BÚSQUEDA DE WINDOWS ESCRIBIMOS (ENV) Y ENTRAMOS A LO PRIMERO QUE APAREZCA COMO SE VE EN LA IMAGEN Y ENTRAMOS AL EDITOR DE VARIABLES



SE NOS ABRIRÁ UNA VENTANA LA CUAL NOS PERMITIRÁ EDITAR LAS VARIABLES DE LAS APLICACIONES, EN VARIABLES DE USUARIO NOS DIRIGIREMOS A ESTA (PATH) Y PULSAMOS EN EL BOTÓN PARA EDITAR



SE NOS ABRIRÁ ESTA VENTANA, AQUÍ LE DAMOS A NUEVO Y PEGAMOS LA UBICACIÓN DE LA CARPETA QUE COPIAMOS ANTERIORMENTE



AHORA GUARDAMOS Y YA ESTARÍA.

PARA PROBAR SI QUEDO DESCARGADA CORRECTAMENTE VAMOS A ESCRIBIR EN LA TERMINAL DE WINDOWS (CMD) EL SIGUIENTE COMANDO (ADB) COMO SE VE EN LA IMAGEN

```
C:\Users\LOCOT00>adb
Android Debug Bridge version 1.0.41
Version 35.0.2-12147458
Installed as C:\Program Files\platform-tools\adb.exe
Running on Windows 10.0.26100

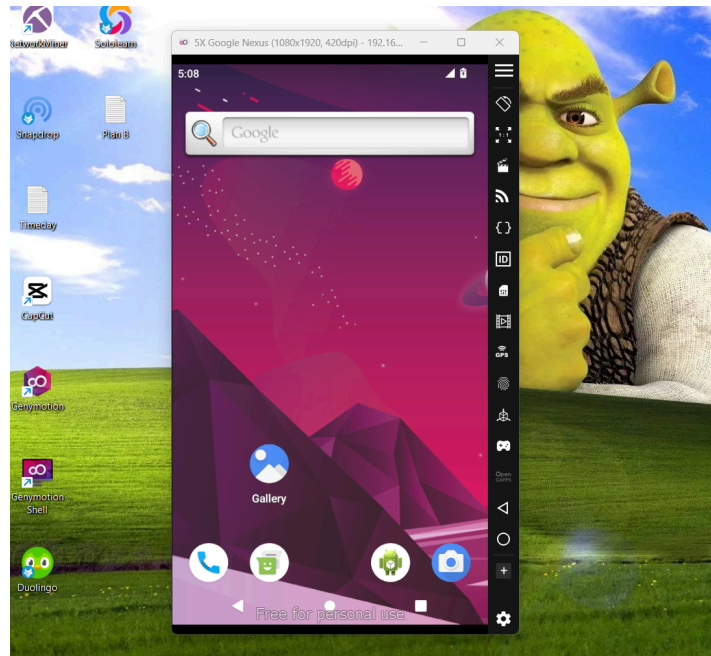
global options:
-a          listen on all network interfaces, not just localhost
-d          use USB device (error if multiple devices connected)
-e          use TCP/IP device (error if multiple TCP/IP devices available)
-s SERIAL   use device with given serial (overrides $ANDROID_SERIAL)
-t ID       use device with given transport id
-H          name of adb server host [default=localhost]
-P          port of adb server [default=5037]
-L SOCKET   listen on given socket for adb server [default=tcp:localhost:5037]
--one-device SERIAL|USB only allowed with 'start-server' or 'server nodaemon', server will only connect to one USB device, specified by a serial number or USB device address.
--exit-on-write-error exit if stdout is closed

general commands:
devices [-l] list connected devices (-l for long output)
help        show this help message
version     show version num

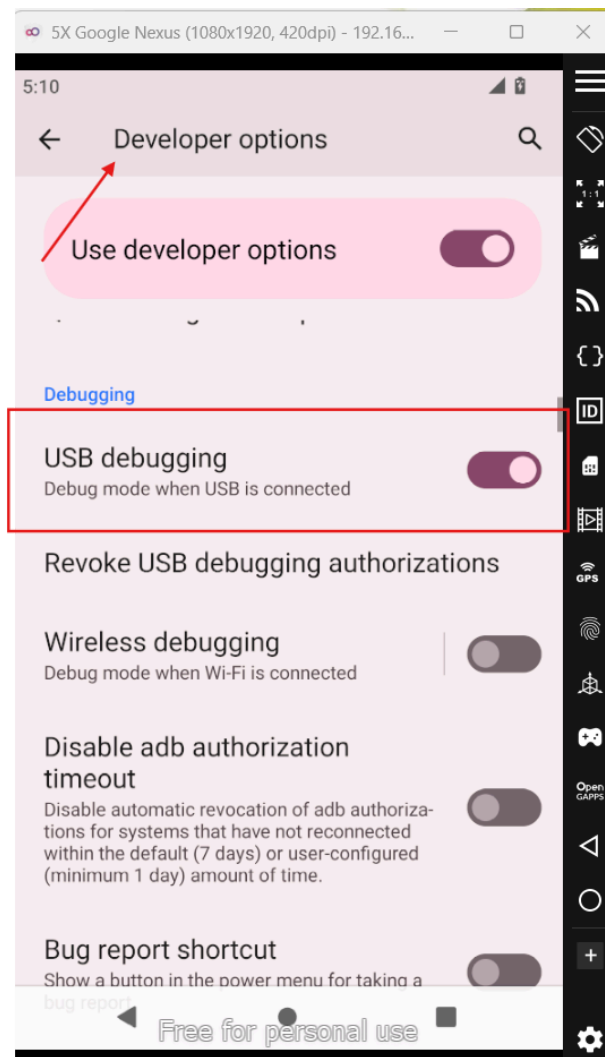
networking:
connect HOST[:PORT] connect to a device via TCP/IP [default port=5555]
disconnect [HOST[:PORT]]
```

Y SI SE NOS EJECUTA QUIERE DECIR QUE LA HERRAMIENTA QUEDÓ DESCARGADA EXITOSAMENTE.

PARA HACER ESTA PRUEBA VAMOS HACER USO DE UN EMULADOR PARA EMULAR NUESTRO DISPOSITIVO ANDROID, ESTO ES BÁSICAMENTE ES COMO SI LO TUVIÉRAMOS EN FÍSICO, NO CAMBIA NADA “BUENO ESO ENTRE COMILLAS”. EN MI CASO VAMOS HACER USO DEL PROGRAMA GANYMOTION QUE NOS PERMITE TENER VARIAS MÁQUINAS A LA VEZ, ASÍ QUE VAMOS A PRENDER NUESTRO ANDROID.



UNA VEZ YA TENGAMOS EL DISPOSITIVO ENCENDIDO, VAMOS A DIRIGIRNOS A LAS CONFIGURACIONES DEL MÓVIL Y ACTIVAR EL MODO (DEPURACIÓN USB), CABE RECORDAR QUE PARA ESTO TENEMOS QUE ESTAR EN MODO DESARROLLADOR.



*AHORA DESDE LA CMD ESCRIBIMOS ESTE COMANDO PARA VER SI TENEMOS CONECTIVIDAD CON EL DISPOSITIVO, ESTO FÍSICAMENTE LO HARÍAMOS MEDIANTE UNA CONEXIÓN **USB** CON EL DISPOSITIVO OBJETIVO.*

```
C:\Users\LOCOT00>adb devices
List of devices attached
192.168.1.149:5555    device

C:\Users\LOCOT00>
```

*Y COMO PODEMOS VER TENEMOS CONECTIVIDAD CON EL DISPOSITIVO, E INCLUSO NOS APARECE SU DIRECCIÓN **IP** Y POR EL PUERTO QUE ESTÁ CORRIENDO.*

AHORA VAMOS A INICIAR CON LA INSTRUCCIÓN, LO PRIMERO QUE VAMOS A RECABAR ES LA INFORMACIÓN GENERAL DEL DISPOSITIVO, PARA VER CON QUE NOS ESTAMOS ENFRENTANDO, Y A POSTERIOR VER QUE OTROS VECTORES DE ATAQUES TENEMOS.

PARA OBTENER LA VERSIÓN DEL **ANDROID ESCRIBIMOS EL SIGUIENTE COMANDO**

ADB SHELL GETPROP RO.BUILD.VERSION.RELEASE

```
C:\Users\LOCOT00>adb shell getprop ro.build.version.release
13
```

PARA OBTENER EL MODELO DEL DISPOSITIVO

ADB SHELL GETPROP RO.PRODUCT.MODEL

```
C:\Users\LOCOT00>adb shell getprop ro.product.model  
Nexus 5X
```

PARA OBTENER INFORMACIÓN BÁSICA DEL DISPOSITIVO EN GENERAL, ESCRIBIREMOS EL SIGUIENTE COMANDO, ESTO NOS DA MUCHÍSIMA INFORMACIÓN HASTA CON QUE VERSIONES CORREN ALGUNAS APLICACIÓN, ESTO NOS SIRVE PARA BUSCAR Y VER SI HAY ALGUNA VULNERABILIDAD EN DICHA VERSIÓN.

ADB SHELL GETPROP

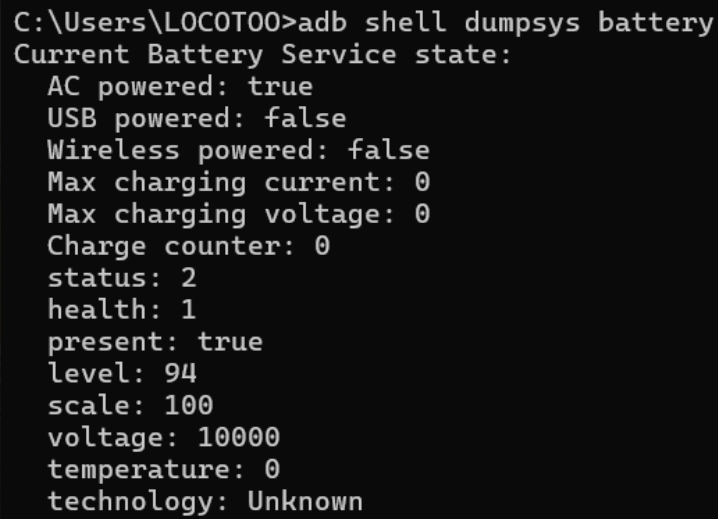
```
C:\Users\LOCOT00>adb shell getprop  
[androVM.initd]: [1]  
[androVM.vbox_dpi]: [420]  
[androVM.vbox_graph_mode]: [1080x1920-16]  
[apexd.status]: [ready]  
[bootreceiver.enable]: [1]  
[bpf.progs_loaded]: [1]  
[build.version.extensions.r]: [3]  
[build.version.extensions.s]: [3]  
[build.version.extensions.t]: [3]  
[cache_key.bluetooth.bluetooth_adapter_get_connection_state]: [-5143648363720310134]  
[cache_key.bluetooth.bluetooth_adapter_get_profile_connection_state]: [-5143648363720310133]  
[cache_key.bluetooth.bluetooth_adapter_get_state]: [-5143648363720310132]  
[cache_key.bluetooth.bluetooth_adapter_is_offloaded_filtering_supported]: [-5143648363720310141]  
[cache_key.bluetooth.bluetooth_device_get_bond_state]: [-5143648363720310139]  
[cache_key.bluetooth.bluetooth_map_get_connection_state]: [-5143648363720310138]  
[cache_key.bluetooth.bluetooth_sap_get_connection_state]: [-5143648363720310137]  
[cache_key.display_info]: [6809302335406972473]  
[cache_key.get_packages_for_uid]: [6809302335406972474]  
[cache_key.has_system_feature]: [6809302335406972381]  
[cache_key.is_compat_change_enabled]: [6809302335406972398]  
[cache_key.is_interactive]: [6809302335406972368]  
[cache_key.is_power_save_mode]: [6809302335406972394]  
[cache_key.is_user_unlocked]: [6809302335406972435]  
[cache_key.location_enabled]: [6809302335406972393]  
[cache_key.package_info]: [6809302335406972463]  
[cache_key.system_server.accounts_data]: [6809302335406972462]
```

Y ASÍ SUCESIVAMENTE PODRÍAMOS IR SACANDO INFORMACIÓN YA CON ESTA HERRAMIENTA DE ANDROID ADB Y EL MÓVIL QUE LO PUSIMOS EN MODO DESARROLLADOR, TENEMOS ACCESO A TODA LA INFORMACION DEL MOVIL SIN LIMITACIONES, Y LO MEJOR, SIN NINGUNA

INSTRUCCIÓN AGRESIVA NI NADA, SIMPLEMENTE POR SABER QUÉ USAR Y DE QUÉ MODO USARLO. VAMOS A SEGUIR RECABANDO INFORMACIÓN.

PARA OBTENER INFORMACIÓN DE LA BATERÍA

ADB SHELL DUMPSYS BATTERY



```
C:\Users\LOCOT00>adb shell dumsys battery
Current Battery Service state:
  AC powered: true
  USB powered: false
  Wireless powered: false
  Max charging current: 0
  Max charging voltage: 0
  Charge counter: 0
  status: 2
  health: 1
  present: true
  level: 94
  scale: 100
  voltage: 10000
  temperature: 0
  technology: Unknown
```

PARA LISTAR LAS APLICACIONES INSTALADAS

ADB SHELL PM LIST PACKAGES

```
C:\Users\LOCOT00>adb shell pm list packages
package:com.android.providers.media.module
package:com.android.modulemetadata
package:com.android.connectivity.resources
package:com.android.music
package:com.android.calllogbackup
package:com.android.internal.display.cutout.emulation.hole
package:com.android.settings
package:com.android.bips
package:com.android.internal.systemui.navbar.gestural_narrow_back
package:com.android.internal.display.cutout.emulation.tall
package:com.android.cameraextensions
package:com.android.dreams.phototable
package:com.android.providers.contacts
package:com.android.carrierconfig
package:com.android.internal.systemui.navbar.gestural_wide_back
package:com.android.inputmethod.latin
package:com.genymotion.settings
package:com.android.dreams.basic
package:com.android.companiondevicemanager
package:com.android.cts.priv.ctsshim
package:com.android.mms.service
package:com.android.providers.downloads
```

PARA OBTENER INFORMACIÓN DETALLADA DE UNA APLICACIÓN ESPECÍFICA, INCLUSO LO PERMISOS QUE TIENE OTORGADOS

ADB SHELL DUMPSYS PACKAGE (NOMBRE_DEL_PAQUETE)

YO LO HICE CON ESTA -> WALLPAPERBACKUP

```

/system/framework/android.hidl.base-V1.0-java.jar
/system/framework/org.apache.http.legacy.jar
timeStamp=2009-01-01 00:00:00
lastUpdateTime=2009-01-01 00:00:00
packageSource=0
signatures=PackageSignatures{d6e72f version:3, signatures:[cd3e7f05], past signatures:[]}
installPermissionsFixed=true
pkgFlags=[ SYSTEM HAS_CODE ALLOW_CLEAR_USER_DATA ]
declared permissions:
  com.android.messaging.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION: prot=signature, INSTALLED
install permissions:
  android.permission.DOWNLOAD_WITHOUT_NOTIFICATION: granted=true
  android.permission.CHANGE_NETWORK_STATE: granted=true
  android.permission.RECEIVE_BOOT_COMPLETED: granted=true
  android.permission.READ_PROFILE: granted=true
  android.permission.INTERNET: granted=true
  android.permission.WRITE_SMS: granted=true
  android.permission.ACCESS_NETWORK_STATE: granted=true
  com.android.messaging.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION: granted=true
  android.permission.VIBRATE: granted=true
  android.permission.WAKE_LOCK: granted=true
User 0: ceDataInode=447539 installed=true hidden=false suspended=false distractionFlags=0 stopp
false enabled=0 instant=false virtual=false
installReason=0
firstInstallTime=2009-01-01 00:00:00
uninstallReason=0
overlay paths:
  /data/resource-cache/com.android.systemui-neutral-n1QJ.frro
  /data/resource-cache/com.android.systemui-accent-WAjh.frro
oids=[3003]

```

BIEN UNA VEZ YA TENGAMOS RECABADA TODA LA INFORMACIÓN DEL DISPOSITIVO AHORA PODEMOS HACER OTRO TIPO DE COSAS COMO PUEDEN SER, TOMAR CAPTURAS DE PANTALLA, GRABAR LA PANTALLA DEL DISPOSITIVO, OBTENER LOGS DEL SISTEMA, OBTENER INFORMACIÓN DE LA RED Y MUCHO MÁS. ASÍ QUE VAMOS A HACER ALGUNAS DE ESTAS QUE YA SON DE OTRO NIVEL Y UN POQUITO MÁS INTERESANTES.

PARA HACER UNA CAPTURA DE PANTALLA: EL PRIMER COMANDO NOS TOMA LA CAPTURA Y EL SEGUNDO LO QUE HACE ES QUE TOMA ESA CAPTURA Y NOS LA DESCARGA EN EL DIRECTORIO DONDE ESTEMOS ACTUALMENTE

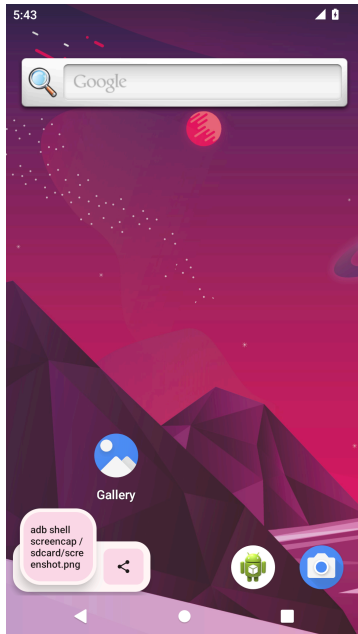
ADB SHELL SCREENCAP /SDCARD/SCREENSHOT.PNG

ADB PULL /SDCARD/SCREENSHOT.PNG

```
C:\Users\LOCOT00>adb shell screencap /sdcard/screenshot.png

C:\Users\LOCOT00>adb pull /sdcard/screenshot.png
/sdcard/screenshot.png: 1 file pulled, 0 skipped. 7.6 MB/s (523264 bytes in 0.065s)
```

Y SI HACEMOS UN DIR PODEMOS VER QUE TENEMOS LA CAPTURA EN NUESTRA PROPIA MAQUINA



```
08/02/2025 05:38 <DIR> Downloads
24/11/2024 20:16 <DIR> Favorites
24/11/2024 20:16 <DIR> Links
03/02/2025 22:15 <DIR> Music
08/02/2025 05:15 <DIR> OneDrive
05/02/2025 16:16 <DIR> Pictures
24/11/2024 20:16 <DIR> Saved Games
08/02/2025 06:44 523.264 screenshot.png
24/11/2024 20:16 <DIR> Searches
08/02/2025 05:21 <DIR> Videos
21/01/2025 08:49 <DIR> VirtualBox VMs
4 archivos 680.248 bytes
25 dirs 237.680.754.688 bytes libres

C:\Users\LOCOT00>
```

PARA OBTENER LOS LOGS DEL SISTEMA: LOS LOGS SON ARCHIVOS QUE DOCUMENTAN ACTIVIDADES QUE OCURREN EN UN SISTEMA, POR ESO SON TAN IMPORTANTES LOS LOGS YA QUE CON ESTOS PODEMOS SACAR INFORMACIÓN COMO ***ACCESO DE USUARIOS,*** TRANSACCIONES, CAMBIOS EN EL SISTEMA Y ACTIVIDADES RELEVANTES QUE OCURREN EN LA MÁQUINA.

ADB LOGCAT

```
02-08 06:07:56.701 494 494 I wificond: 5Ghz DFS frequencies: 5180 5200 5220 5240 5260 5280 5300 5320 5500 5520 5540
5560 5580 5600 5620 5640 5660 5680 5700 5745 5765 5785 5805 5825
02-08 06:07:56.701 494 494 I wificond: 6Ghz frequencies:
02-08 06:07:56.701 494 494 I wificond: 60Ghz frequencies:
02-08 06:07:56.707 657 783 W BestClock: java.time.DateTimeException: Missing NTP fix
02-08 06:07:56.713 657 783 D ConnectivityService: NetReassign [no changes]
02-08 06:08:00.020 2241 2286 D EGL_emulation: app_time_stats: avg=59960.33ms min=59960.33ms max=59960.33ms count=1
02-08 06:08:00.552 657 2231 D WifiNl80211Manager: Scan result ready event
02-08 06:08:00.552 657 2231 D WifiNative: Scan result ready event
02-08 06:08:14.132 657 774 D WifiConfigStore: Writing to stores completed in 35 ms.
02-08 06:08:16.699 657 774 E WifiScoringParams: Invalid frequency(-1), using 5G as default rssi array
02-08 06:08:20.564 657 2231 D WifiNl80211Manager: Scan result ready event
02-08 06:08:20.564 657 2231 D WifiNative: Scan result ready event
02-08 06:08:45.851 396 E android.hardware.power.stats@1.0-service-mock: Failed to getEnergyData
02-08 06:08:56.726 657 774 E WifiScoringParams: Invalid frequency(-1), using 5G as default rssi array
02-08 06:09:00.062 2241 2286 D EGL_emulation: app_time_stats: avg=60031.25ms min=60031.25ms max=60031.25ms count=1
02-08 06:09:00.589 657 2231 D WifiNl80211Manager: Scan result ready event
02-08 06:09:00.590 657 2231 D WifiNative: Scan result ready event
02-08 06:10:00.036 2241 2286 D EGL_emulation: app_time_stats: avg=59972.16ms min=59972.16ms max=59972.16ms count=1
02-08 06:10:16.779 657 774 E WifiScoringParams: Invalid frequency(-1), using 5G as default rssi array
02-08 06:10:20.638 657 2231 D WifiNl80211Manager: Scan result ready event
02-08 06:10:20.638 657 2231 D WifiNative: Scan result ready event
02-08 06:10:45.852 396 E android.hardware.power.stats@1.0-service-mock: Failed to getEnergyData
02-08 06:11:00.062 2241 2286 D EGL_emulation: app_time_stats: avg=60023.48ms min=60023.48ms max=60023.48ms count=1
02-08 06:11:32.310 657 2231 W BatteryExternalStatsWorker: error reading Bluetooth stats: 11
02-08 06:11:32.349 657 1272 W TelephonyManager: requestModemActivityInfo: Received an invalid ModemActivityInfo
02-08 06:11:32.350 657 1272 W BatteryExternalStatsWorker: error reading modem stats:ERROR_INVALID_INFO_RECEIVED
02-08 06:11:32.363 657 690 E KernelCpuSpeedReader: Failed to read cpu-freq: /sys/devices/system/cpu/cpu0/cpufreq/sta
ts/time_in_state: open failed: ENOENT (No such file or directory)
02-08 06:11:32.366 142 142 I binder:142_2: type=1400 audit(0.0:708): avc: denied { read } for name="wakeup2" dev="sy
```

PARA OBTENER INFORMACIÓN DE RED, ESCRIBIMOS EL SIGUIENTE COMANDO:

ADB SHELL IFCONFIG

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:da:ac:a6  Driver virtio_net
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feda:aca6/64 Scope: Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:191652 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122522 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:37704900 TX bytes:213087086

wlan0     Link encap:Ethernet  HWaddr 08:00:27:84:cb:06  Driver mac80211_hwsim
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14042 TX bytes:23154

radio0    Link encap:Ethernet  HWaddr d2:c8:8d:45:4c:f4
          inet6 addr: fe80::d0c8:8dff:fe45:4cf4/64 Scope: Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:767 errors:0 dropped:0 overruns:0 frame:0
          TX packets:156 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:120422 TX bytes:22561
```


*Y ASI ES COMO PODRÍAMOS RECABAR MUCHISIMA INFORMACION MUY UTIL QUE NOS SERVIRÁ EN CASO DE UNA AUDITORÍA MÓVIL GRACIAS A ESTA HERRAMIENTA DE DESARROLLADOR DE ANDROID **ANDROID DEBUG BRIDGE** (ADB) Y ESTO NO SON TODOS LOS COMANDOS, HAY MUCHÍSIMOS COMANDOS MÁS LOS CUALES NOS PUEDEN SERVIR PARA RECABAR INFORMACIÓN DE UN DISPOSITIVO MÓVIL.*

*CABE RECALAR QUE ESTE NO ES EL ÚNICO MÉTODO PARA RECOPILAR INFORMACIÓN, YA QUE DESDE EL MISMO MÓVIL PODEMOS DESCARGAR APLICACIONES COMO FIND O **MyPermissions** QUE TAMBIÉN NOS SERVIRÁN PARA RECABAR INFORMACIÓN O INCLUSO HAY MAS METODOS PARA SACAR DATA DEL UN MÓVIL, SINO QUE QUISE TRAER ESTE YA QUE ES UN POCO DIFERENTE E INTERESANTE.*

CHAO Y GRACIAS...

ATT... SANTIAGO PEÑARANDA.