

Práctica 1

Análisis forense en Android

Jose Almirón López

19 de Mayo del 2024

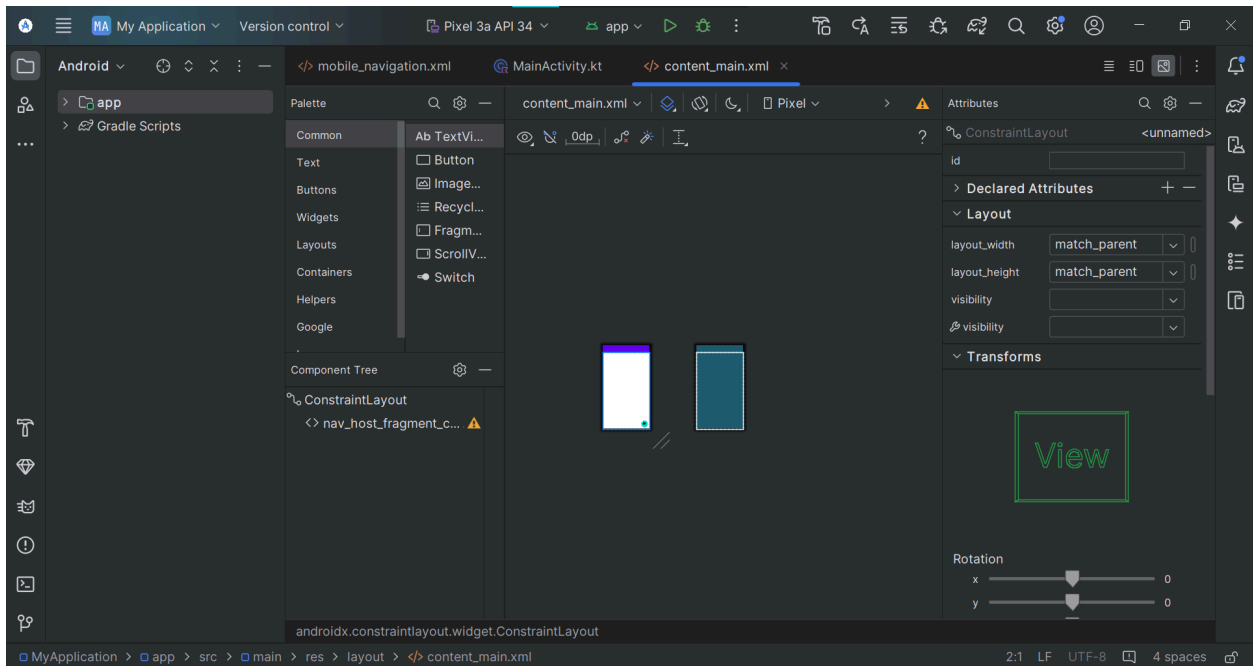


Tabla de contenidos

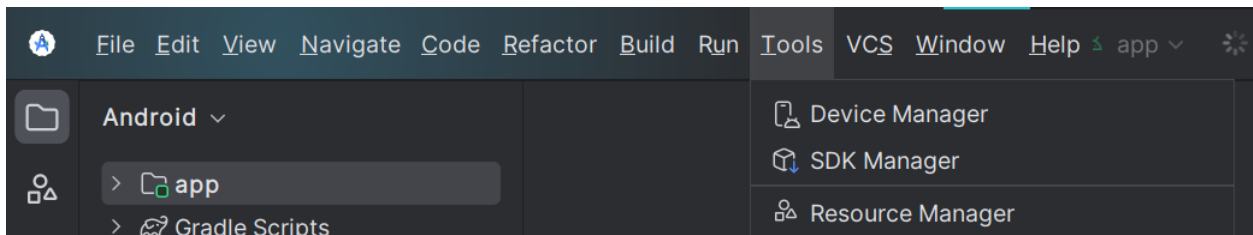
Familiarización con Android	3
Virtualización de Android en virtual box	8
Andriller	11

Familiarización con Android

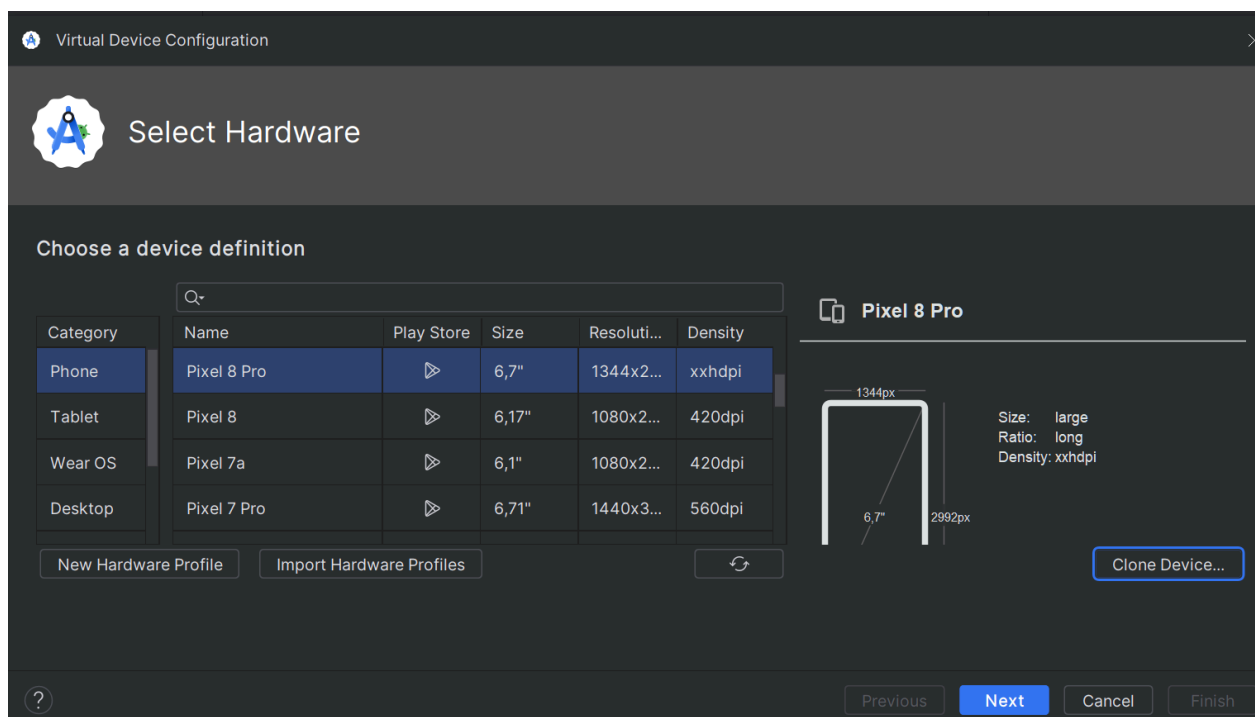
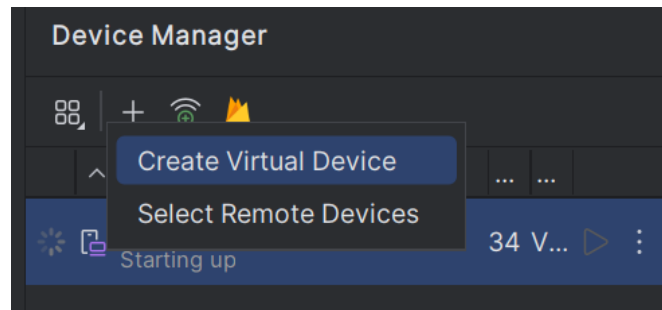
Para empezar a familiarizarnos con Android, lo primero que haremos será instalar Android Studio. Esta aplicación es utilizada por los desarrolladores para crear y programar aplicaciones Android, pero también nos permite ejecutar un dispositivo mediante emulación.



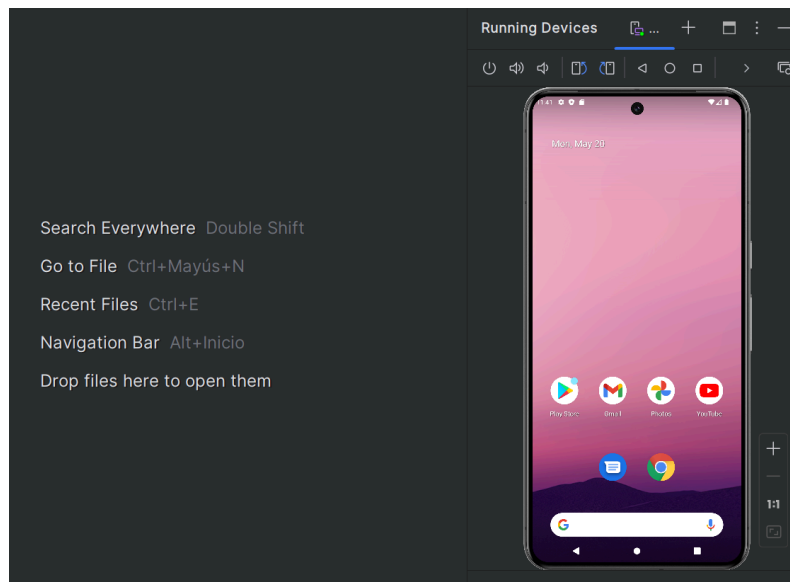
Para ejecutar una máquina virtual, seleccionaremos la opción Tools > Device Manager.



El proceso es sencillo: pulsaremos sobre el botón + y seleccionaremos Create Virtual Device, eligiendo el dispositivo que queramos emular.



Como podemos ver, ya tenemos un dispositivo emulado.



Para instalar el paquete Android Debug Bridge (ADB), descargaremos las herramientas desde la web oficial. Una vez descargadas, podremos utilizarlas de inmediato. Para trabajar de una forma más cómoda, podemos añadirlas al PATH del sistema.

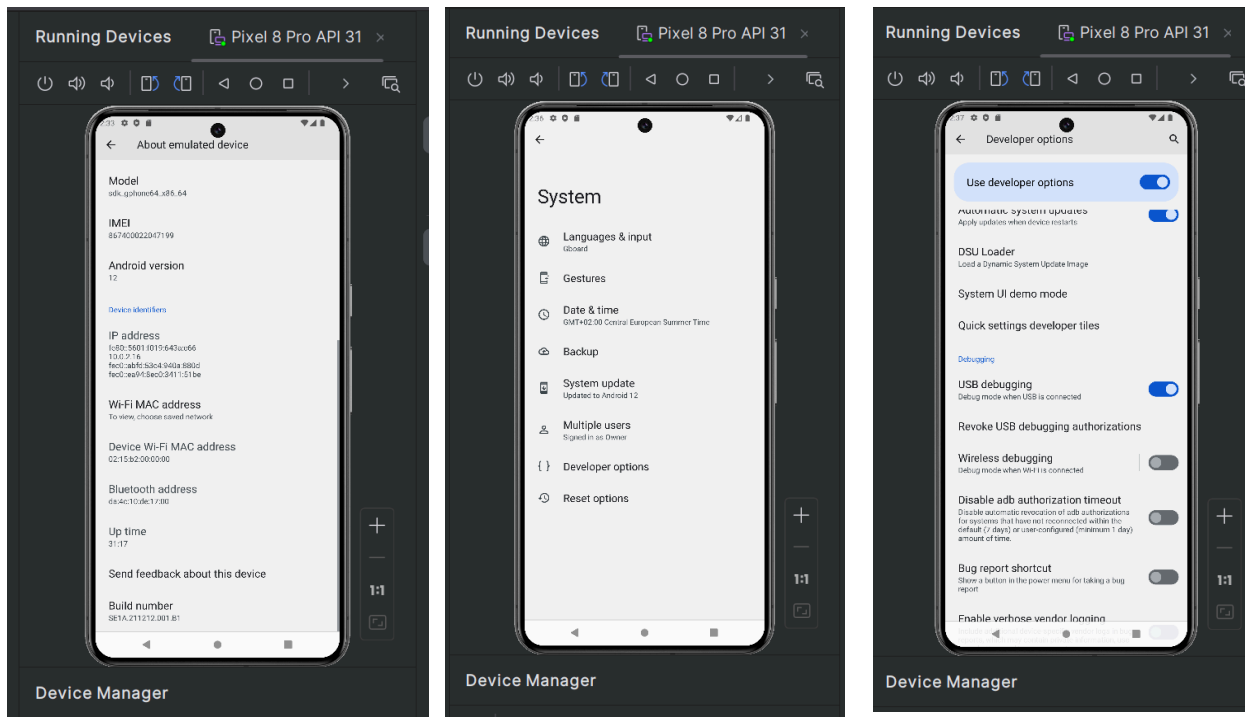
```
C:\Windows\System32\cmd.exe

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 2458-0222

Directorio de C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools

20/03/2024  17:42    <DIR>          .
20/03/2024  17:42    <DIR>          ..
20/03/2024  17:42           5.857.056 adb.exe
20/03/2024  17:42           108.320 AdbWinApi.dll
20/03/2024  17:42           73.504 AdbWinUsbApi.dll
20/03/2024  17:42           439.072 etc1tool.exe
20/03/2024  17:42           1.807.136 fastboot.exe
20/03/2024  17:42           54.560 hprof-conv.exe
20/03/2024  17:42           242.128 libwinpthread-1.dll
20/03/2024  17:42           477.472 make_f2fs.exe
20/03/2024  17:42           477.472 make_f2fs_casefold.exe
20/03/2024  17:42             1.157 mke2fs.conf
20/03/2024  17:42           754.464 mke2fs.exe
20/03/2024  17:42           1.110.529 NOTICE.txt
20/03/2024  17:42              38 source.properties
20/03/2024  17:42           2.838.304 sqlite3.exe
                14 archivos      14.241.212 bytes
                 2 dirs  68.523.556.864 bytes libres
```

Antes de poder usar las herramientas de ADB, necesitamos habilitar el modo desarrollador y la depuración USB. En nuestro caso, lo haremos en el emulador, pero el proceso es el mismo para un dispositivo real. Nos dirigimos a Configuración > Acerca del dispositivo y pulsamos sobre el Número de compilación varias veces.



Una vez que hayamos activado el modo desarrollador y la depuración USB, podremos empezar a usar ADB. Disponemos de varios comandos; por ejemplo, adb devices nos listará los dispositivos conectados.

```
C:\Windows\System32\cmd.exe

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>adb.exe devices
List of devices attached
emulator-5556    device

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>
```

Con adb shell podremos obtener una terminal para navegar por el dispositivo.

```
C:\Windows\System32\cmd.exe - adb.exe shell

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>adb.exe shell
emulator64_x86_64_arm64:/ $ ls
acct      bin        config     data_mirror  etc          linkerconfig  mnt          oem          product      storage      system_ext
adb_keys  bugreports d          debug_ramdisk  init         lost+found    odm          postinstall  sdcard       sys          vendor
apex      cache     data       dev           init.environ.rc  metadata      odm_dkrm     proc         second_stage_resources  system      vendor_dkrm
emulator64_x86_64_arm64:/ $
```

Con adb root, obtendremos permisos de administrador, siempre y cuando el dispositivo esté rooteado.

```
C:\Windows\System32\cmd.exe - adb shell

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>adb root
restarting adbd as root

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>adb shell
emulator64_x86_64_arm64:/ # whoami
root
emulator64_x86_64_arm64:/ #
```

Podemos subir archivos al dispositivo con el comando adb push.

```
C:\Windows\System32\cmd.exe - adb shell

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>adb.exe push C:\Users\jose_\Downloads\Magisk-v27.0.apk /storage/emulated/0/Download/
C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>adb.exe push C:\Users\jose_\Downloads\Magisk-v27.0.apk: 1 file pushed, 0 skipped. 45.0 MB/s (12498796 bytes in 0.265s)

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>adb shell
emulator64_x86_64_arm64:/ # ls /storage/emulated/0/Download/
Magisk-v27.0.apk
emulator64_x86_64_arm64:/ #
```

Con el comando adb pull, podremos descargar archivos del dispositivo a nuestro sistema.

```
C:\Windows\System32\cmd.exe

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>adb.exe pull /storage/emulated/0/Download/Magisk-v27.0.apk
/storage/emulated/0/Download/Magisk-v27.0.apk: 1 file pulled, 0 skipped. 41.2 MB/s (12498796 bytes in 0.289s)

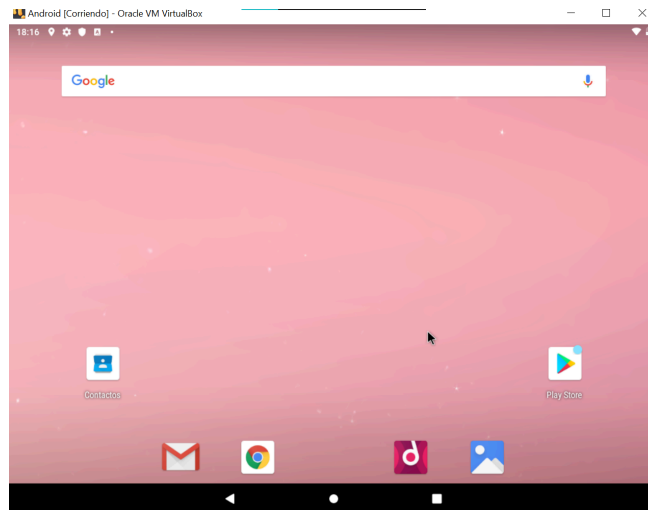
C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 2458-0222

Directorio de C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools

20/05/2024  15:07    <DIR>          .
20/05/2024  15:07    <DIR>          ..
20/03/2024  17:42             5.857.056 adb.exe
20/03/2024  17:42             108.320 AdbWinApi.dll
20/03/2024  17:42             73.504 AdbWinUsbApi.dll
20/03/2024  17:42             439.072 etc1tool.exe
20/03/2024  17:42             1.807.136 fastboot.exe
20/03/2024  17:42             54.560 hprof-conv.exe
20/03/2024  17:42             242.128 libwinpthread-1.dll
20/05/2024  15:07            12.498.796 Magisk-v27.0.apk
20/03/2024  17:42             477.472 make_f2fs.exe
20/03/2024  17:42             477.472 make_f2fs_casefold.exe
20/03/2024  17:42              1.157 mke2fs.conf
20/03/2024  17:42             754.464 mke2fs.exe
20/03/2024  17:42            1.110.529 NOTICE.txt
20/03/2024  17:42              38 source.properties
20/03/2024  17:42            2.838.304 sqlite3.exe
                15 archivos          26.740.008 bytes
                2 dirs 73.545.543.680 bytes libres
```

Virtualización de Android en virtual box

Instalamos una máquina virtual utilizando la imagen ISO de Android proporcionada, para poder trabajar con ella."



Una vez que hayamos instalado la máquina virtual, podemos acceder a la configuración de Wi-Fi y verificar la dirección IP que se nos proporciona, ya que ADB permite la conexión a través de la red.



Se nos solicita instalar la aplicación AFLogical OSE. Para ello, podemos usar la conexión por red con adb connect <ip>, y una vez tengamos acceso, ejecutar un adb install con el archivo APK.

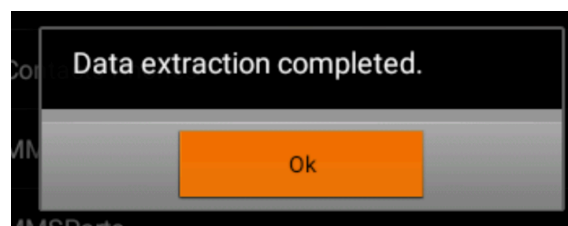
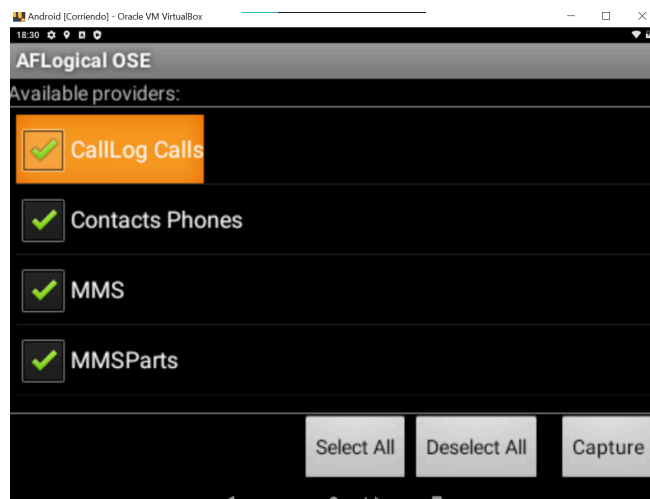
```
C:\Windows\System32\cmd.exe

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>adb connect 192.168.1.153
connected to 192.168.1.153:5555

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>adb install C:\Users\jose_\Downloads\AFLogical-OSE_1.5.2.apk
Performing Streamed Install
Success

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>
```

Esta herramienta permite realizar una extracción limitada de evidencias, ya que solo obtendremos SMS, registros de llamadas, contactos, entre otros.



Si obtenemos un shell, veremos que se ha generado un archivo, el cual podemos transferir a nuestro sistema local utilizando el comando adb pull, como vimos anteriormente.

```
C:\Windows\System32\cmd.exe - adb shell

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>adb shell
x86:/ $ ls sdcard/forensics/
20240520.1831
x86:/ $
```

```
C:\Windows\System32\cmd.exe

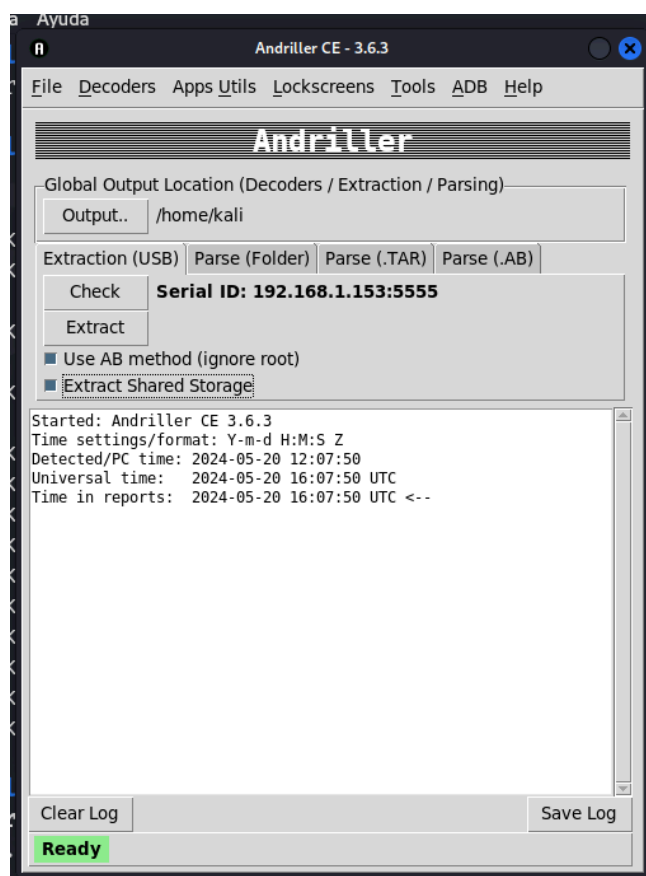
C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>adb.exe pull /sdcard/forensics/20240520.1831
/sdcard/forensics/20240520.1831/: 6 files pulled, 0 skipped. 1.9 MB/s (91615 bytes in 0.045s)

C:\Users\jose_\Downloads\platform-tools-latest-windows\platform-tools>
```

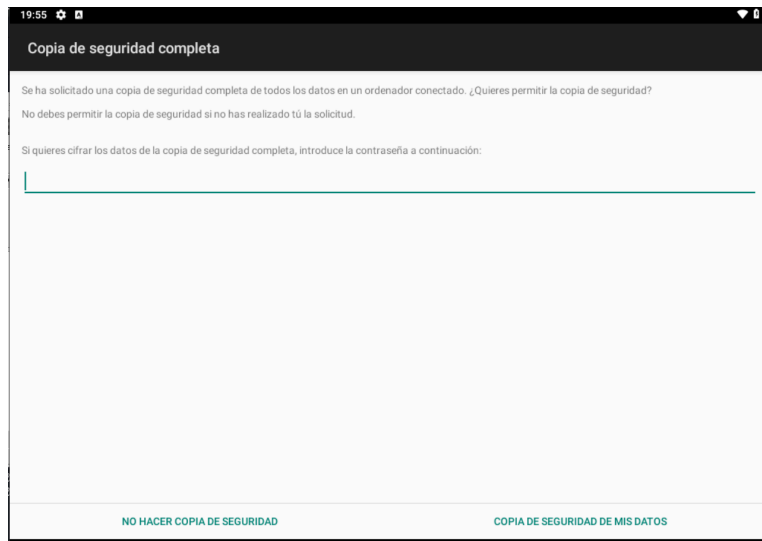
« platform-tools-latest-windows > platform-tools > 20240520.1831					Buscar en 20240520.1831	
	Nombre	Fecha de modificación	Tipo	Tamaño		
✦	CallLog Calls.csv	20/05/2024 16:37	Archivo de origen Co...	1 KB		
✦	Contacts Phones.csv	20/05/2024 16:37	Archivo de origen Co...	5 KB		
✦	info.xml	20/05/2024 16:37	Archivo de origen XML	85 KB		
✦	MMS.csv	20/05/2024 16:37	Archivo de origen Co...	1 KB		
✦	MMSParts.csv	20/05/2024 16:37	Archivo de origen Co...	1 KB		
✦	SMS.csv	20/05/2024 16:37	Archivo de origen Co...	1 KB		

Andriller

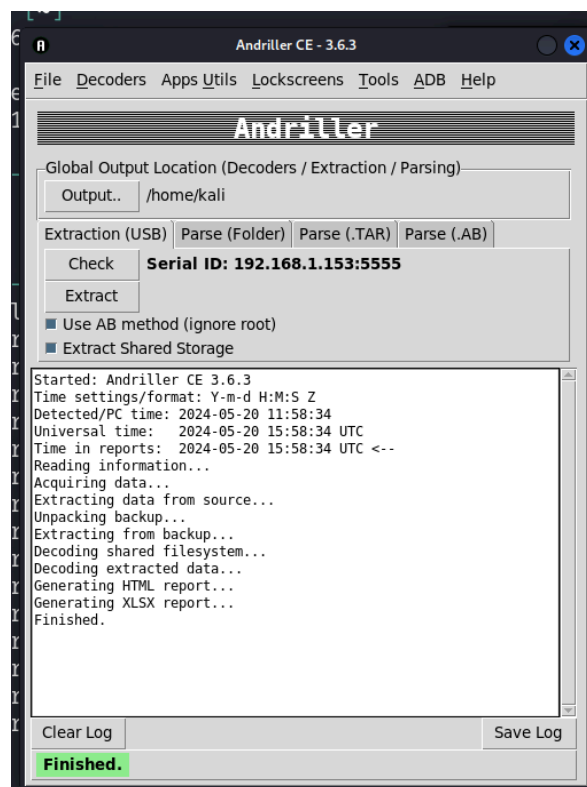
Procedemos a utilizar Andriller, una herramienta muy completa para obtener evidencias. En el repositorio oficial de GitHub de la herramienta, encontraremos la guía de instalación, y luego procedemos a realizar una extracción de evidencias con esta herramienta



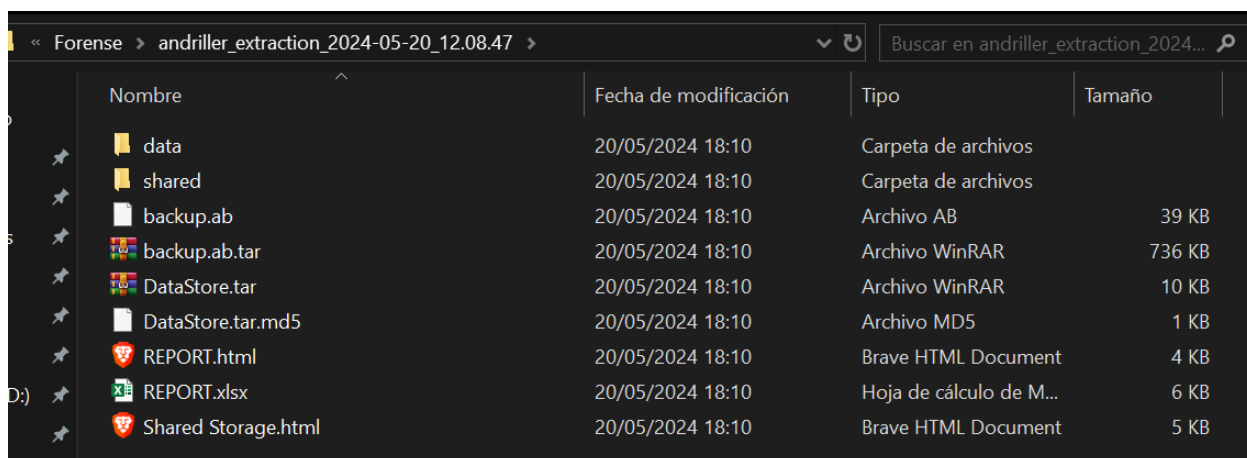
Desde la máquina virtual de Android, se nos solicitará si deseamos realizar una copia de seguridad, y también se nos ofrecerá la opción de cifrar la copia con una contraseña



Una vez que confirmemos la realización de la copia, el proceso en Andriller continuará.



Estos son los datos obtenidos por la copia



Nombre	Fecha de modificación	Tipo	Tamaño
data	20/05/2024 18:10	Carpeta de archivos	
shared	20/05/2024 18:10	Carpeta de archivos	
backup.ab	20/05/2024 18:10	Archivo AB	39 KB
backup.ab.tar	20/05/2024 18:10	Archivo WinRAR	736 KB
DataStore.tar	20/05/2024 18:10	Archivo WinRAR	10 KB
DataStore.tar.md5	20/05/2024 18:10	Archivo MD5	1 KB
REPORT.html	20/05/2024 18:10	Brave HTML Document	4 KB
REPORT.xlsx	20/05/2024 18:10	Hoja de cálculo de M...	6 KB
Shared Storage.html	20/05/2024 18:10	Brave HTML Document	5 KB

ANÁLISIS DEL MODELO DE DATOS DE LA RED SOCIAL WHATSAPP Y SUS APLICACIONES AL PERITAJE

¿En qué consisten los análisis forenses consensuados y no consensuados?

Los análisis forenses consensuados implican que la persona cuya información se va a analizar da su consentimiento explícito para que se realice la investigación forense. Esto puede incluir la entrega voluntaria de dispositivos o datos digitales para su análisis. Por otro lado, los análisis forenses no consensuados se llevan a cabo sin el consentimiento de la persona, generalmente mediante órdenes judiciales o autorización legal para acceder a dispositivos o datos digitales.

¿Qué técnicas se pueden utilizar para peritar una conversación de whatsapp?

Para peritar una conversación de WhatsApp, se pueden utilizar varias técnicas forenses digitales, como:

- Extracción de datos: Utilizando herramientas forenses especializadas para extraer la información de los dispositivos móviles, incluidos los archivos de bases de datos donde se almacenan las conversaciones de WhatsApp.
- Análisis de archivos de bases de datos: Examinando directamente los archivos de bases de datos de WhatsApp en busca de conversaciones y metadatos relevantes.

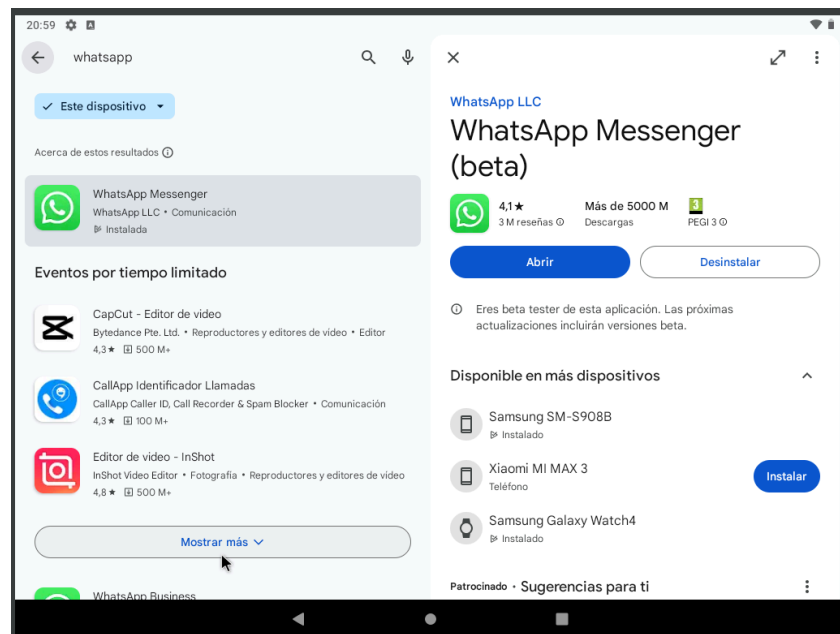
- Recuperación de datos eliminados: Empleando técnicas para recuperar mensajes eliminados o archivos adjuntos que aún pueden estar presentes en el dispositivo o en sus copias de seguridad.

¿Dónde guarda Whatsapp la clave de cifrado y sus BBDD? Cómo podemos extraer estos directorios.

WhatsApp guarda la clave de cifrado y sus bases de datos en la carpeta de datos de la aplicación en el dispositivo móvil. Estos archivos generalmente están almacenados en un formato encriptado para proteger la privacidad de los usuarios. Para extraer estos directorios y acceder a la información, se necesitaría acceso al dispositivo físico y el uso de herramientas forenses especializadas que puedan sortear las medidas de seguridad y encriptación implementadas por WhatsApp. Sin embargo, es importante tener en cuenta que acceder a estos datos sin el consentimiento adecuado puede estar sujeto a restricciones legales y éticas.

Obtención de base de datos de Whatsapp

Al final, se nos solicita instalar WhatsApp y obtener la base de datos de las conversaciones.



En la máquina virtual, no logro instalar WhatsApp; no estoy seguro si se debe a que forma parte del programa beta o a otro fallo. Sin embargo, dado que solo estamos practicando, decidí rootear un móvil antiguo, como detallaré en la práctica avanzada, e instalar WhatsApp en él para luego realizar la extracción de datos.

Dado que el dispositivo está rooteado y tenemos acceso root, podemos acceder al directorio /data/data donde se encuentra la base de datos de WhatsApp. Esto nos permite usar el comando adb pull para extraer el archivo que almacena la base de datos de WhatsApp y abrirlo con SQLite Studio.

The image shows two screenshots. The top one is a Windows command prompt window titled 'C:\Windows\System32\cmd.exe' showing the execution of the 'adb pull' command to extract the WhatsApp database from an Android device. The command is: `C:\Users\jose_\Downloads\ADB>adb pull /data/data/com.whatsapp/databases/msgstore.db`. The output is: `/data/data/com.whatsapp/databases/msgstore.db: 1 file pulled, 0 skipped. 33.1 MB/s (157831168 bytes in 4.545s)`. The bottom screenshot is the SQLite Studio (3.4.4) interface. The 'Databases' pane on the left shows the 'chat' database selected. The 'Data' tab is active, displaying a table with columns: _id, jid_row_id, hidden, subject, created_timestamp, display_name, last_message_timestamp, last_read_timestamp, last_read_jid, last_read_jid, last_import_timestamp, archived, sort_timestamp, mod_tag, and gen. The table contains 1606 rows, with the first row showing data for a contact named 'Family'.

```
C:\Windows\System32\cmd.exe

C:\Users\jose_\Downloads\ADB>adb pull /data/data/com.whatsapp/databases/msgstore.db
/data/data/com.whatsapp/databases/msgstore.db: 1 file pulled, 0 skipped. 33.1 MB/s (157831168 bytes in 4.545s)

C:\Users\jose_\Downloads\ADB>
```

SQLiteStudio (3.4.4) - [chat (msgstore)]

Base de datos Estructura Ver Herramientas Ayuda

Databases

Filter by name

Structure Data Restricciones Indexes Triggers DDL

Vista de rejilla Vista de formulario

Filterar datos Total rows loaded: 1606

_id	jid_row_id	hidden	subject	created_timestamp	display_name	last_message_timestamp	last_read_timestamp	last_read_jid	last_read_jid	last_import_timestamp	archived	sort_timestamp	mod_tag	gen
1	1	23	0 Family	1456489052000	1377276	1377276	1377276	1377276	1377276	1	0	1716237660000	233833	0
2	2	41	0 Los López	1379023135000	1376621	1376621	1376621	1376621	1376621	1	0	1716199812000	337389	0
3	3	40	0 NULL	0	1369452	1369452	1369452	1369452	1369452	1	0	1715186163000	874012	0
4	12	28	0 NULL	0	1272843	1272843	1272843	1272843	1272843	1	1	1681505969000	294319	0
5	22	52	0 NULL	0	1341751	1341751	1341743	1336847	1336847	1	1	1706896585000	870563	0
6	59	27	1 NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	0
7	60	36	1 NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	0