



ANÁLISIS FORENSE

Unidad 1. Actividad 1



01 DE ABRIL DE 2023
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Análisis de dispositivos móviles	2
Ejercicio 1 (2 puntos) El número IMEI	2
Ejercicio 2 (2 puntos) La tarjeta SIM	5
Ejercicio 3 (2 puntos) Recogida de evidencias forenses de dispositivos móviles.	6
Ejercicio 4 (4 puntos) Copia de seguridad de un dispositivo móvil usando herramientas externas.	7

Análisis de dispositivos móviles

Ejercicio 1 (2 puntos) El número IMEI

¿Qué es?

El número IMEI (Identidad Internacional de Equipo Móvil, por sus siglas en inglés) es un código único de 15 dígitos que se utiliza para identificar de forma exclusiva a un dispositivo móvil, como un teléfono celular o una tableta. Cada dispositivo tiene su propio IMEI, que no se repite en ningún otro.

¿Para qué sirve?

El IMEI tiene varias funciones, entre ellas se encuentra:

- **Identificación del dispositivo:** El IMEI proporciona una identificación única para cada dispositivo móvil. Esta identificación es esencial para que los proveedores de servicios de telecomunicaciones puedan distinguir entre dispositivos y gestionar su uso en las redes.
- **Rastreo y recuperación de dispositivos:** En caso de robo o pérdida de un dispositivo, el IMEI se utiliza para rastrear y localizar el dispositivo. Las autoridades y los proveedores de servicios pueden utilizar esta información para ayudar en la recuperación del dispositivo y en la prevención del uso no autorizado.
- **Bloqueo y desbloqueo del dispositivo:** Los dispositivos móviles pueden ser bloqueados o desbloqueados utilizando su IMEI. En caso de robo o pérdida, los propietarios pueden solicitar el bloqueo del dispositivo para evitar que sea utilizado por personas no autorizadas. Además, el IMEI se puede utilizar para desbloquear un dispositivo móvil cuando se cambia de operador o se desea utilizar el dispositivo en otra red.
- **Autenticación y seguridad:** El IMEI se utiliza como una medida de seguridad para verificar la autenticidad de un dispositivo móvil. Los proveedores de servicios y las autoridades pueden verificar el IMEI de un dispositivo para garantizar que no esté asociado con actividades ilegales, como el robo o la falsificación de identidad.

¿Cuántas partes tiene y para que sirve cada una?

El IMEI se divide en 3 partes:

1. Tipo de Identificador (TAC): Los primeros seis dígitos del IMEI conforman el Tipo de Identificador (TAC). Este código identifica el tipo de dispositivo móvil, su modelo y su fabricante. Sirve para proporcionar información básica sobre el dispositivo, como la marca y el modelo.

2. Número de Serie (SNR): Los siguientes seis dígitos después del TAC forman el número de serie único del dispositivo. Este número de serie es exclusivo para cada dispositivo y se utiliza para distinguir un dispositivo específico dentro de una serie de producción o de dispositivos similares. Sirve para identificar de manera única cada dispositivo.

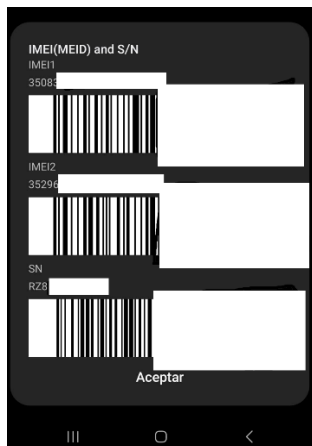
3. Código de Verificación (CD): Los últimos dos dígitos del IMEI son el Código de Verificación (CD). Estos dígitos se utilizan para verificar la validez del IMEI y detectar errores de transmisión o manipulación. El algoritmo utilizado para generar el código de verificación garantiza que el IMEI sea válido y esté libre de errores. Sirve para verificar la integridad del IMEI.

¿De que forma puedo localizar el número IMEI en un dispositivo un móvil?

He encontrado de 4 formas distintas:

1. Marcando un código en el teléfono:

- En la mayoría de los dispositivos, puedes encontrar el IMEI marcando ***#06#** en la aplicación del teléfono y luego pulsando el botón de llamada.

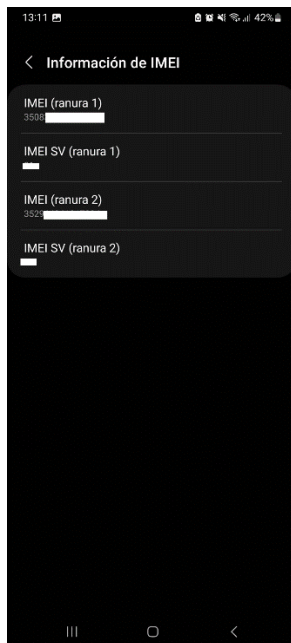


(En la foto esta recortado claramente)

2. Configuración del dispositivo:

En muchos dispositivos, puedes encontrar el número IMEI en la configuración del dispositivo.

- En dispositivos Android, por ejemplo, puedes ir a "Configuración" > "Acerca del teléfono" > "Estado" y allí encontrarás el número IMEI.



- En dispositivos iOS (iPhone), puedes ir a "Configuración" > "General" > "Información" y el IMEI estará listado junto con otra información del dispositivo.



(esta foto es de internet ya que no tengo iphone)

3. En la bandeja de la tarjeta SIM:

En algunos dispositivos, el número IMEI se puede encontrar impreso en la bandeja de la tarjeta SIM.



4. En la etiqueta del dispositivo:

En muchos dispositivos, especialmente aquellos que son nuevos, el número IMEI estará impreso en una etiqueta ubicada en la parte trasera del dispositivo o dentro de la bandeja de la tarjeta SIM.

Puedes buscar esta etiqueta y encontrar el número IMEI impreso en ella.



Este realmente no estoy seguro de si se sigue usando a día de hoy ya que en la caja de mi móvil actual no he encontrado el IMEI.

Ejercicio 2 (2 puntos) La tarjeta SIM

Define que es un número PIN y un número PUK.

El PIN y el PUK son códigos que vienen impresos en la tarjeta plástica que contiene el chip y que se te entrega al momento de la activación de la línea.

¿Qué ocurre si introducimos un número PIN no válido hasta superar el límite de intentos?, ¿y un número PUK?.

Si por alguna razón ingresaras mal 3 veces el código PIN, necesitarás el PUK para desbloquear el chip.

Si ingresas el PUK en forma errónea 10 veces consecutivas, deberás realizar cambio de chip.

Indica que datos guarda una tarjeta SIM y para que sirven.

A cada tarjeta SIM se le asigna un número de identificación único que almacena información sobre tu plan, como el tipo de plan, los datos disponibles, los minutos de voz y los mensajes de texto. Las compañías usan esta información para verificar el estado de tu cuenta y aplicar cargos.

Cada vez que envías un mensaje de texto o realizas una llamada, el dispositivo envía una señal a la red para solicitar acceso. La tarjeta SIM se usa para verificar que tu dispositivo esté autorizado a llamar o enviar mensajes de texto dentro de una red. Si la tarjeta SIM no está autorizada, se deniega la solicitud.

Además de los datos de la red, se almacena información personal en una tarjeta SIM. Datos como el número de teléfono, los contactos y el historial de mensajes de texto se almacenan en una tarjeta SIM, lo que facilita la transferencia de información de un dispositivo a otro.

Haz una lista de los pasos a seguir cuando debemos analizar un dispositivo móvil, describiéndolos.

1. Recopilación de información preliminar:

En esta etapa, es crucial recopilar toda la información relevante sobre el dispositivo y el caso en cuestión. Esto incluye detalles como el modelo del dispositivo, su sistema operativo, y cualquier información sobre el propietario del dispositivo que pueda estar disponible. Además, es importante identificar el motivo o incidente que justifique el análisis del dispositivo para orientar adecuadamente la investigación.

2. Preparación del entorno de análisis:

Antes de comenzar el análisis del dispositivo, se debe establecer un entorno controlado y seguro. Esto implica utilizar hardware y software especializado para garantizar la integridad de los datos durante el proceso de análisis. Además, es esencial disponer de suficiente espacio de almacenamiento para guardar los datos extraídos de manera segura.

3. Preservación de la evidencia:

Preservar la evidencia digital es una parte crítica del análisis forense de dispositivos móviles. Para evitar cualquier alteración de los datos, es recomendable apagar el dispositivo o ponerlo en modo de vuelo para evitar cualquier comunicación remota. Luego, se debe utilizar software especializado para capturar una imagen completa del dispositivo, manteniendo intacta la cadena de custodia para garantizar la validez de la evidencia.

4. Extracción de datos:

Utilizando herramientas forenses específicas, se extraen los datos del dispositivo. Esto puede incluir archivos, registros, metadatos y datos de aplicaciones. Es importante utilizar métodos forenses adecuados para recuperar datos eliminados o cifrados, si es necesario, garantizando siempre la integridad de los datos extraídos.

5. Análisis de datos:

Durante esta fase, se examinan detalladamente los datos extraídos en busca de información relevante para la investigación. Esto puede incluir revisar mensajes, historiales de llamadas, archivos multimedia y otros datos almacenados en el dispositivo. Se utilizan herramientas especializadas para identificar patrones, conexiones o actividades sospechosas que puedan ser importantes para el caso.

6. Documentación y elaboración de informes:

Todos los pasos realizados durante el análisis del dispositivo deben ser documentados cuidadosamente. Esto incluye registrar las acciones realizadas, los hallazgos relevantes y cualquier evidencia digital obtenida. Posteriormente, se elabora un informe detallado que resume los procedimientos seguidos, los resultados obtenidos y cualquier recomendación para acciones futuras.

7. Presentación de resultados:

Una vez completado el análisis y elaborado el informe, se presentan los resultados a las partes interesadas, como abogados, investigadores o autoridades legales. En esta etapa, el analista debe estar preparado para proporcionar testimonio experto en caso de que sea necesario.

8. Seguimiento y revisión:

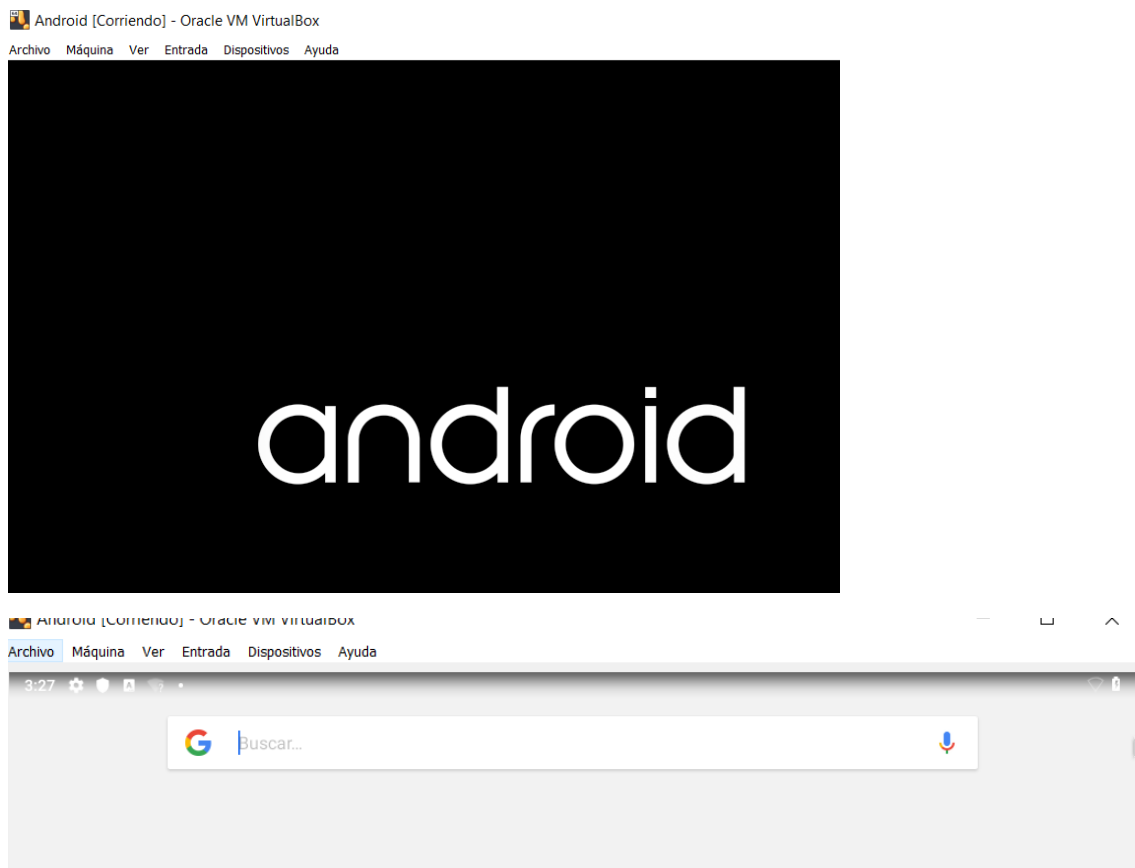
Por último, es importante realizar un seguimiento regular de los procedimientos y técnicas de análisis para mantenerse actualizado con las últimas tendencias y herramientas en el campo de la forense digital. Además, cualquier desarrollo adicional en la investigación que pueda requerir un análisis adicional del dispositivo móvil debe ser atendido diligentemente.

Ejercicio 4 (4 puntos) Copia de seguridad de un dispositivo móvil usando herramientas externas.

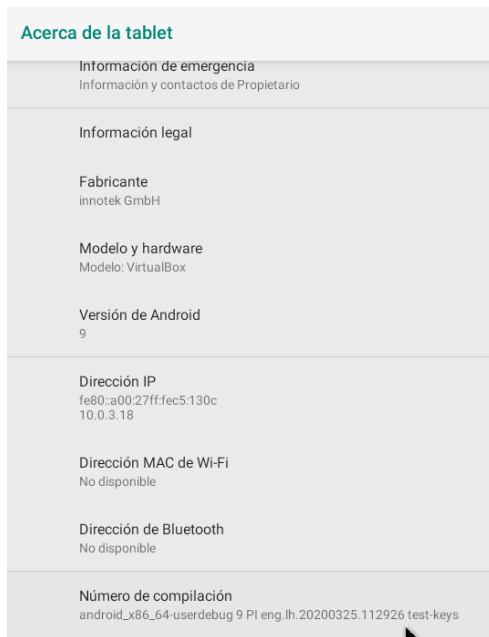
Usando un emulador de Android, ya sea para Virtualbox o de otro tipo, realiza una copia del contenido del teléfono del emulador Android mediante la herramienta ADB, describiendo todo el proceso que has realizado y los comandos que has usado.

Puedes ejecutar la herramienta ADB desde Linux o Windows.

Primero nos instalamos el Android:



Primero ponemos el Android como desarrollador. Pulsamos varias veces sobre Número de compilación:



Ahora ponemos la opción de permitir la depuración por usb:



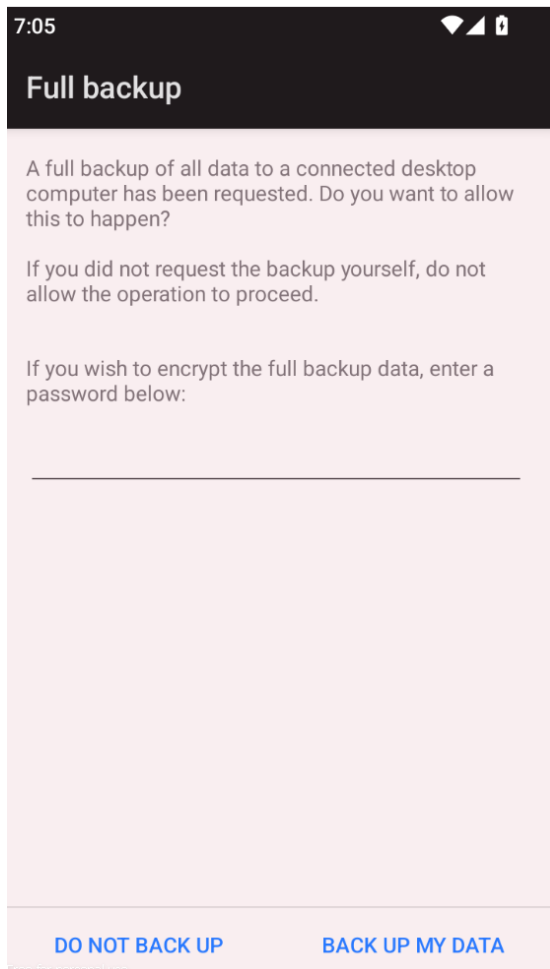
Nota: Con VirtualBox no me ha funcionado. Ahora voy a usar Genymotion.

En mi caso estoy usando mi propio Windows para hacer el uso del adb.







Como vemos me detecta el móvil:

```
C:\platform-tools>adb devices
List of devices attached
192.168.191.101:5555    device
```

Ahora podemos realizar la copia de seguridad con el comando `adb backup -all -f backup.ab`:



Como vemos ahora tenemos nuestro backup del Android realizado:

 adb.exe	08/04/2024 20:39	Aplicación
 AdbWinApi.dll	08/04/2024 20:39	Extensión de
 AdbWinUsbApi.dll	08/04/2024 20:39	Extensión de
 backup.ab	08/04/2024 21:07	Archivo AB
 etc1tool.exe	08/04/2024 20:39	Aplicación
 fastboot.exe	08/04/2024 20:39	Aplicación