



VE&S

Engineering & Services



www.eysglobal.com



MÓDULO 1

TEMA 10: METODOLOGÍA DE TRABAJO PARTE 3 ENTORNO MOVIL

FASE DE ADQUISICIÓN - MAXIMIZANDO LA ADQUISICIÓN

La enorme cantidad de datos accesibles en un dispositivo móvil depende en gran medida del estado en que se encuentra:

- ✓ Desbloqueado: se puede acceder al dispositivo hasta que se bloquee por inactividad.
- ✓ Bloqueado por código u otro sistema de autenticación: es necesario introducir un código de acceso (o huella dactilar o similar), para acceder al dispositivo.
- ✓ Apagado: para poder acceder al dispositivo hay que pasar por el proceso de encendido.

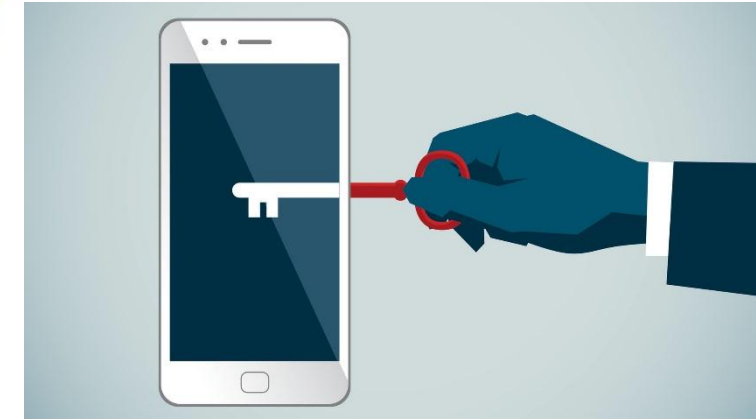
FASE DE ADQUISICIÓN - TIPOS DE ADQUISICIÓN



DISPOSITIVO DESBLOQUEADO

Si el dispositivo ha sido incautado, los pasos a realizar para desbloquearlo serán los siguientes:

- Aislar el dispositivo de la red. Es decir, habilitar el modo avión y extraer la tarjeta SIM. Aquí, es recomendable introducirlo en un recipiente que aisle el campo electro- magnético (por ejemplo, en una “Jaula de Faraday”). También hay que activar todas las opciones posibles, para permitir el acceso físico al dispositivo. Es decir:
- Eliminar el código de bloqueo (si es posible).
- Activar la depuración a través de USB.
- Desactivar el bloqueo por inactividad (activando la opción “siempre activo”).



FASE DE ADQUISICIÓN - TIPOS DE ADQUISICIÓN



DISPOSITIVO BLOQUEADO

Si el dispositivo se encuentra bloqueado solo podremos:

Aislar el dispositivo de la red, extraer la tarjeta SIM o introducirlo en una jaula de Faraday.

Comprobar si el dispositivo tiene activada la depuración a través de USB. En caso de que la conexión USB se encuentre activa, es posible que podamos cargar boot loaders, para modificar el sistema de arranque del dispositivo y permitir de este modo, el acceso físico al mismo.

Si el dispositivo no tiene activada la depuración USB, ejecutar un ataque para la extracción del código de bloqueo (smudge attack o fuerza bruta).



FASE DE ADQUISICIÓN - TIPOS DE ADQUISICIÓN



FASE DE ADQUISICIÓN - ANDROID:

El proceso de adquisición se debe realizar teniendo en cuenta la volatilidad de las evidencias, por lo que es necesario recoger primero las evidencias más volátiles.

A continuación, voy a describir un posible orden de adquisición según su volatilidad, aplicándose a dispositivos móviles los marcados en negrita

FASE DE ADQUISICIÓN - TIPOS DE ADQUISICIÓN

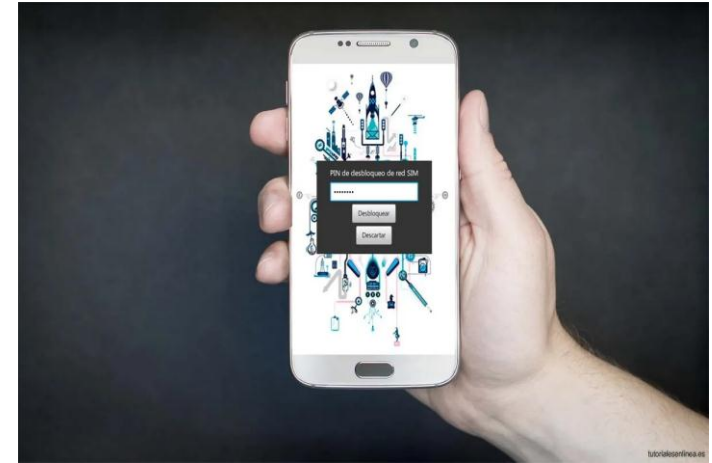


ADQUISICIÓN MANUAL

Solo es realizable si el teléfono se encuentra desbloqueado.

En la adquisición manual hay que listar todas las aplicaciones existentes y realizar capturas de pantalla de los elementos que se consideren pertinentes.

Es posible que para el acceso a los datos de algunas aplicaciones sea necesario conectar el dispositivo a Internet. Esto se debe realizar solo como ultimo recurso, ya que el dispositivo puede ser bloqueado remotamente.



FASE DE GESTIÓN DE EVIDENCIAS

La gestión de evidencias es un proceso fundamental para la validez de todo el proceso de análisis forense.

Una buena gestión de evidencias asegura que la cadena de custodia sea respetada y que, por lo tanto, las evidencias no han sido comprometidas.

Indicar que la cadena de custodia es el conjunto de procedimientos encaminados a la recogida, el traslado y la custodia de las evidencias relativas a una investigación.



FASE DE EXAMEN

El examen consiste en identificar las evidencias a partir de la información obtenida en la fase de adquisición.

En el análisis de un disco:

- ✓ Examinar las particiones y el sistema de archivos.
- ✓ Ficheros existentes y ficheros borrados.
- ✓ Espacio sin utilizar y bloques después de la marca de fin de fichero.
- ✓ Obtener metadatos, categorizar ficheros y descartar los no relevantes.

En el análisis de red:

- ✓ Descartar paquetes que no sean relevantes.
- ✓ En el análisis de la memoria:
- ✓ Descartar procesos que no sean relevantes.
- ✓ Extraer la información relevante de los procesos.

FASE DE ANÁLISIS

El análisis consiste en obtener conclusiones a partir de las evidencias obtenidas.

Es la fase más completa del proceso, y la que más libertad ofrece, por lo que suele variar en función del analista.

En ocasiones, el análisis de las evidencias puede originar una nueva fase de examen y extracción para hacer visibles nuevas evidencias.



FASE DE ANÁLISIS - FORMATO DE DATOS



Durante la etapa de análisis se revisan y estudian las evidencias adquiridas. Dada la ingente cantidad de información que almacenan los teléfonos móviles hoy en día, no se recomienda utilizar una estrategia en la que se extraiga toda la información posible del dispositivo sin orden ni justificación.

Dependiendo del origen de las evidencias y el caso concreto, se deberán formular una serie de hipótesis, donde se describan:

- ✓ Los principales tipos de datos que se pueden encontrar en un dispositivo.
- ✓ La forma de analizarlos dependiendo del tipo de evidencia adquirida.
- ✓ Los principales tipos de datos en las plataformas predominantes.

FASE DE PRESENTACIÓN

La presentación consiste en describir los diferentes sucesos probados y las evidencias que los corroboran.

Normalmente, esta fase consiste en la elaboración de un informe forense, el cual va a ser leído por personal que no es técnico (jueces, ejecutivos, etc.), por lo que debe ser claro y contener un lenguaje que se adapte al perfil adecuado.

En caso de que sea escrito para un proceso judicial, es posible que sea necesaria su defensa ante el juez.



EL INFORME FORENSE

El producto final de la actividad del perito es un informe con los resultados de su trabajo, que posiblemente tenga que ser expuesto y defendido ante un tribunal.

En general, el informe forense debe incluir las siguientes secciones:

- ✓ Sumario o resumen del caso (descripción detallada y exacta de los hechos).
- ✓ Herramientas utilizadas.
- ✓ Adquisición de evidencias (los elementos de evidencia hallados y cualquier otro ex- tremo que pudiera resultar de interés).
- ✓ Procesado de evidencias.
- ✓ Análisis de evidencias.
- ✓ Conclusiones.

INFORME EJECUTIVO E INFORME TÈCNICO

El informe ejecutivo debe ser claro, conciso y no debe contener lenguaje técnico, dado que por lo general va dirigido a gerentes, fiscales y/o jueces, que tienen poca relación con la informática.

El informe técnico debe detallar todos los procedimientos realizados, utilizar información técnica que permita a cualquier persona que siga esos pasos conseguir los mismos resultados que hemos conseguido.



SUMARIO O RESUMEN DEL CASO

Cada actuación debe ajustarse a derecho y a catálogos de buenas practicas, para que el informe no pueda ser impugnado por omisiones o defectos de forma. Aunque dependiendo del objetivo y ámbito del mismo, puede ser necesario ajustar la estructura del informe forense.

