www.eysglobal.com

MÓDULO 1
TEMA 10:METODOLOGÌA DE TRABAJO PARTE 2 ENTORNO MOVIL

PARTICULARIDADES DEL ENTORNO MÒVIL

Uno de los principales problemas de la informática forense es que debe adaptarse a la constante aparición de nuevos dispositivos:

- ✓ Durante sus inicios, la informática forense trataba delitos que se cometían a través de medios informáticos. Por lo tanto, las investigaciones se centraban especialmente en estaciones de trabajo, servidores y redes.

- ✓ La aparición de teléfonos móviles ofreció nuevos datos (SMS y llamadas) y empezó a acercar la informática forense a delitos que se suceden fuera de los medios telemáticos.

PARTICULARIDADES DEL ENTORNO MÒVIL

- ✓ La aparición de los Smartphone amplio el abanico de información a recolectar de un dispositivo (mensajes, correos electrónicos, localización, etc.).
- ✓ Los nuevos dispositivos conectables (wearables, vehículos, domótica, etc.) ofrecen aun más información que puede ser de gran importancia durante una investigación judicial.

RAZONES:
Diferentes sistemas operativos

pese a que *Android* es el SO móvil de uso mayoritario, existen otros que también tienen una importante cuota de mercado y que, por tanto, deben ser conocidos en profundidad, para poder llevar a cabo el proceso de toma de evidencias. Algunos de ellos son: iOS, Windows Phone y BlackBerry OS, linux

CONSIDERACIONES LEGALES

durante el proceso es fundamental cumplir en todo momento con la normativa vigente, con el fin de mantener la validez legal de las pruebas en caso de que se requiera.

TÈCNICAS ANTI-FORENSE:

Al igual que sucede con otros dispositivos, como en el caso de los ordenadores, es posible realizar diferentes acciones para dificultar la identificación de pruebas en un proceso forense, como por ejemplo: la destrucción, ocultación o falsificación de las evidencias.

SISTEMAS DE PROTECCION Y CIFRADO

- ✓ El bloqueo por código de un terminal evita el acceso al dispositivo, incluso por cable en algunos sistemas.
- ✓ El borrado remoto permite eliminar todas las pruebas de un dispositivo sin tener acceso físico al mismo.
- ✓ El cifrado de disco imposibilita la lectura de las memorias a través del acceso físico al chip.

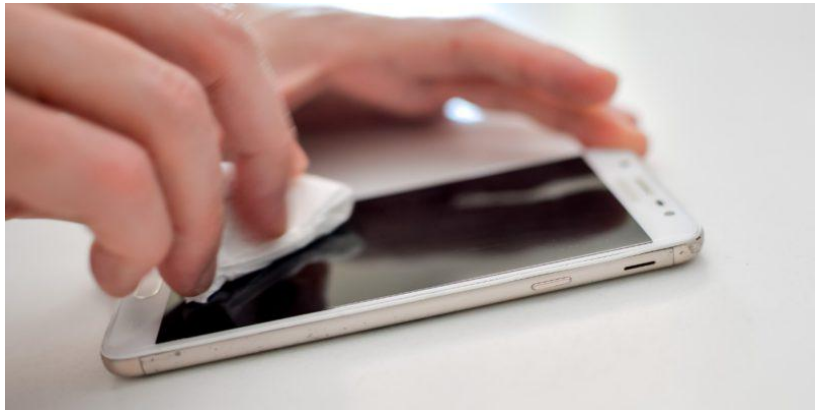
Por ultimo, podemos añadir que existen millones de aplicaciones disponibles para cada dispositivo, cada una con un mecanismo de almacenamiento de información diferente.

EVIDENCIAS RELEVANTES EN EL ENTORNO MÒVIL

Casi cualquier elemento digital se puede considerar una evidencia. Algunos ejemplos son:

ALMACENAMIENTO DE EVIDENCIAS

Es imprescindible definir los métodos adecuados para el almacenamiento y etiquetado de las evidencias. Una vez que se cuenta con todas las evidencias del incidente, es necesario conservarlas intactas. Para ello, se debe seguir el siguiente proceso:



ETAPAS DEL ANALISIS FORENSE PARA ESTA METODOLOGÌA

1 PREPARACIÒN

2 ADQUISICIÒN

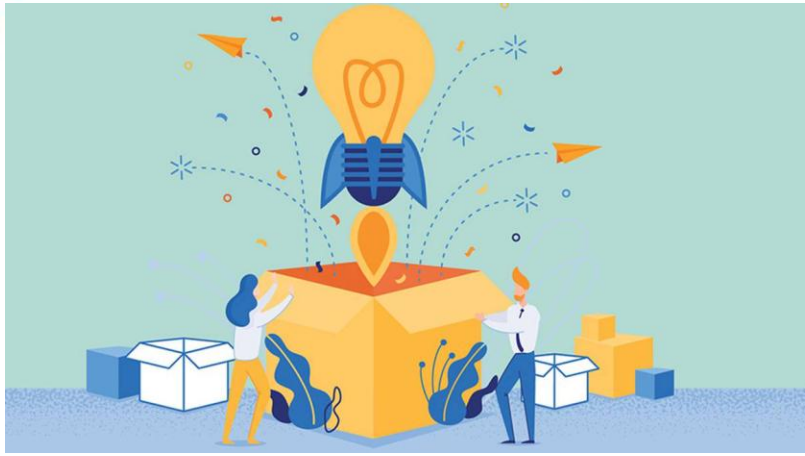
3 GESTIÓN DE EL PROCESO DE ANÁLISIS

4 EXAMEN

5 Análisis

6 PRESENTACIÓN

ETAPAS DEL ANALISIS FORENSE PARA ESTA METODOLOGÌA



Para tener en cuenta:

Las notas, cuanto más detalladas mejor, pueden incluir, por ejemplo:

- ✓ **Capturas de pantalla.**
- ✓ **Localización de evidencias encontradas.**
- ✓ **Notas manuscritas.**
- ✓ **Utilización de sistemas de anotación dentro de la propia aplicación forense.**

FASE DE PREPARACIÒN

Esta etapa se ejecuta de forma previa al proceso de análisis y consiste en identificar los elementos físicos que se van a analizar y las evidencias que se buscaran en cada uno de los elementos analizables.

Estás dependen del objetivo del análisis forense. Por ejemplo:

- ✓ El análisis de una intrusión a través de un dispositivo móvil requerirá, por ejemplo, el análisis del almacenamiento del dispositivo en busca de pruebas de acceso ilegitimo a los sistemas.
- ✓ El análisis de un dispositivo para la comprobación de una coartada requerir a, por ejemplo, el análisis del almacenamiento del dispositivo para comprobar las localizaciones en las que ha estado el dueño del dispositivo.

FASE DE PREPARACIÒN

- ✓ Bolsas especiales. Estas bolsas distan de ser perfectas, por lo que el perito debería tomar la precaución de envolver el dispositivo móvil en papel de plata – tres capas como mínimo – para apantallar por completo la señal.
- ✓ Papel de aluminio. Otro truco consiste en envolver el dispositivo móvil en papel de aluminio de buena calidad, cuanto más grueso sea el papel mejor. Si con una capa no basta, sería necesario envolver el dispositivo en dos vueltas de papel de aluminio.

Bolsa de Faraday.

FASE DE ADQUISICIÒN - CONSIDERACIONES

En un entorno ideal, la adquisición de datos del dispositivo no debería modificar el estado físico del dispositivo.

Por desgracia, esto no siempre es posible. Dependiendo de su estado, el tipo de adquisición y las herramientas utilizadas, el estado del dispositivo se vera afectado:

- ✓ Fecha y hora de acceso a ficheros.
- ✓ Borrado o creación de nuevos ficheros.
- ✓ Modificación de la memoria del dispositivo, para la carga de aplicaciones de volcado.

FASE DE ADQUISICIÒN - MÈTODOS DE ADQUISICIÒN

Una vez enumeradas las evidencias que se van a adquirir, hay que obtener los datos de los dispositivos que van a ser objeto del informe forense.
El método utilizado para adquirir los datos del dispositivo variará dependiendo de:

- ✓ La plataforma de la que se van a adquirir los datos (en este caso, Android).
- ✓ La versión especifica del hardware, software y configuración del dispositivo (versión del dispositivo, configuración de desbloqueo activa, etc.).
- ✓ El estado en el que se encontró el dispositivo (apagado o encendido, bloqueado o sin bloquear, etc.).
- ✓ El tipo de datos a adquirir y su volatilidad (capturar datos en almacenamiento persistente o en memoria).

FASE DE ADQUISICIÒN - TIPOS DE ADQUISICIÒN

Dependiendo de las variables anteriores (vistas en el apartado anterior) se pueden realizar tres tipos de adquisición: manual, lógica y física.

ADQUISICIÒN MANUAL

En la adquisición manual se interacciona con el propio dispositivo, para acceder a los datos del mismo. La adquisición de los datos se realiza mediante capturas de pantalla o directamente a través de fotografías de la pantalla del dispositivo.

FASE DE ADQUISICIÒN - TIPOS DE ADQUISICIÒN

LA ADQUISICIÓN LÓGICA, consiste en copiar los archivos y directorios del sistema de archivos del dispositivo. Este tipo de adquisición forense requiere inevitablemente la ayuda de la interfaz USB.

Para ello, se utilizan:

- ✓ Las propias API de acceso al sistema de ficheros del dispositivo objeto de análisis. El SO del dispositivo se encargara de copiar a otro dispositivo los ficheros y directorios solicitados.
- ✓ Las API del SO de la herramienta de adquisición. La unidad se conecta al dispositivo que hay que analizar. Los datos del sistema analizado seguirán siendo leídos por el firmware del dispositivo analizado.

FASE DE ADQUISICIÒN - TIPOS DE ADQUISICIÒN

ADQUISICIÒN FÌSICA

Consiste en el copiado *bit* a *bit* del dispositivo físico de almacenamiento (permite obtener una copia *bit* a *bit* del contenido de los *chips* de memoria del dispositivo analizado), por lo que requiere de acceso completo al dispositivo de almacenamiento.

En el dispositivo móvil, por lo general, el sistema de almacenamiento se encuentra soldado al resto de los componentes del teléfono y no es accesible de forma física.