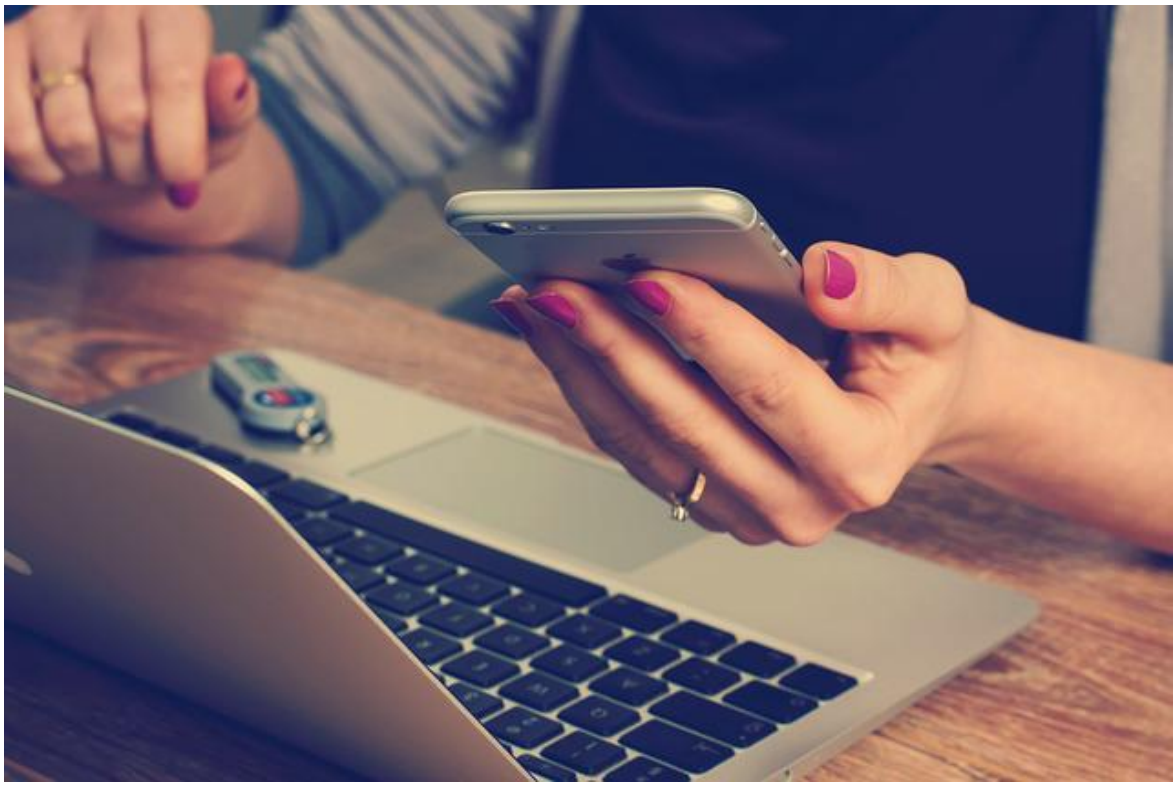
1.- Análisis Forense en Dispositivos Móviles.

Caso práctico



Pixabay (Dominio público)

María ha sido asignada a la investigación de un caso donde se sospecha que un usuario interno podría haber enviado información sensible de la empresa a la competencia a cambio de una compensación económica.

María es consciente que su portátil y el registro de sus comunicaciones corporativas es una fuente fundamental a revisar pero también es consciente que puede que el usuario no haya enviado la información a través de su equipo corporativo sino a través de su teléfono móvil donde es posible que no haya las mismas medidas de protección que podría tener el portátil corporativo.

Por eso nada más llegar al puesto del usuario en la empresa, solicita saber que dispositivos móviles tiene (personales y corporativos) para identificarlos como posible evidencias.

Uno de los principales objetivos dentro del análisis forense es entender que ha sucedido en un entorno digital donde uno o varios usuarios han ejecutado distintas acciones. Debido a ésta situación, investigación de la actividad de los usuarios, los dispositivos móviles son uno de los focos principales ya que casi todos los usuarios tendrán uno y el usuario suele almacenar mucha información en ellos. Esta información será una fuente rica a nivel forense.

La cantidad y tipos de herramientas de forense para dispositivos móviles es considerablemente diferente a la de las computadoras personales. Si bien las computadoras personales pueden diferir de los dispositivos móviles desde la perspectiva del hardware y el software, su funcionalidad se ha vuelto cada vez más similar.

Aunque la mayoría de los sistemas operativos de los dispositivos móviles son de código abierto (es decir, Android), algunos sistemas operativos como IOS de Apple suelen estar cerrados. Esto dificulta la interpretación de su estructura y sistema de ficheros internos. Muchos dispositivos móviles con el mismo sistema operativo también pueden variar ampliamente en su implementación, lo que resulta en una gran variedad de tipos y sistemas de ficheros. Estas permutaciones crean desafíos significativos para los fabricantes y examinadores de herramientas forenses para móviles.

Pixabay (Dominio público)

En esta unidad el alumno aprenderá:

- Entender la importancia de los dispositivos móviles en el análisis forense.
- Diferenciar distintos componentes dentro de un dispositivo móvil a nivel forense.
- Conocer los distintos modos de extracción de evidencias en un dispositivo móvil.
- Conocer las principales herramientas para el análisis forense en dispositivos móviles.

1.1.- Elementos de un dispositivo móvil.

Ideados y pensados para la portabilidad, un dispositivo móvil genera y almacena una gran cantidad de datos convirtiéndose en la mayoría de los casos en la base del usuario digital. De forma genérica y a efectos forenses podríamos identificar los los siguientes componentes:

Pixabay (Dominio público)

- Microprocesador
- Memoria ROM (*Read Only memory)*
- Memoria RAM *(Read Access memory)*
- Memoria interna (normalmente tipo *NAND -Not AND-)*
- Opcional: Memoria externa (tipo *Secure Digital* -SD- ó micro SDXC *Secure Digital Extended Capacity)*

La memoria RAM del móvil contiene mucha información pero es muy volátil por los que muchas veces cuando el investigador acude a la escena o empieza a trabajar con el móvil lo encuentra apagado y por tanto el contenido de esta memoria se encuentra vacío. En cambio la memoria interna sigue manteniéndose aunque el dispositivo esté encendido por lo que resulta la mayoría de veces de más utilidad para el analista forense.

Para saber más

Los dispositivos móviles modernos son auténticos ordenadores, donde podemos identificar los mismos componentes que un ordenador de escritorio tradicional (CPU, memoria, almacenamiento). Si bien para un analista forense el escenario no debería de ser muy distinto hay varios ítems que se deben tener en cuenta:

- Algunos fabricantes emplean sistemas operativos cerrados y funciones no documentadas por lo que dificulta la investigación forense
- El bloqueo de los terminales en algunos casos puede llegar a impedir el análisis forense del dispositivo

1.2.- Métodos de extracción.

Una vez que tenemos acceso al dispositivo móvil tendremos de forma general las siguientes opciones, tanto a nivel físico como lógico, para extraer las evidencias:

- Extracción manual
- Extracción lógica
- Extracción mediante JTAG y Hex Dump
- Chip-Off (extracción del chip)
- Extracción a nivel Micro

Pixabay (Dominio público)

La extracción manual sucede cuando visualizamos el contenido del móvil directamente sobre el propio dispositivo, por ejemplo cuando revisamos la lista de llamadas realizadas o los mensajes recibidos desde el propio dispositivo.

La extracción lógica implica la conexión con el dispositivo móvil mediante una interfaz (a través de cable con distintos conectores o de manera inalámbrica) para poder descargar y visualizar los datos. Hay que tener cuidado con este método ya que podría alterar la evidencia al ser manipulada.

La extracción mediante JTAF y Hex dump funciona a más bajo nivel y accede directamente

contra el propio dato almacenado en el dispositivo. La conexión se hace a través de un software especifico que en muchos casos carga distintos módulos dentro de la memoria o el sector de arranque del dispositivo haciendo de interfaz entre el software usado por el analista y el dispositivo.

El método *Chip-Off* consiste en la extracción física del chipset de memoria para transformarlo en una imagen binaria para ser analizada por el analista forense en el laboratorio.

La extracción micro rara vez es usada, sólo en casos muy puntuales o críticos, ya que requiere un gran nivel de conocimiento y herramientas avanzadas para ejecutar el análisis. A nivel técnico se usa un microscopio especial para ver cómo se comporta a nivel eléctrico los distintos componentes físicos. Existen pocas empresas en el mundo que puedan realizar este tipo de análisis.

Autoevaluación

Si tenemos que extraer el chip de memoria de una tablet, ¿Qué tipo de extracción sería?

- Extracción HexDump
- Extracción física
- Extracción lógica
- Extracción NAND

Al ser un acceso físico (chip) requerirá de una extracción física.

Opción correcta

Al ser un acceso físico (chip) requerirá de una extracción física.

Al ser un acceso físico (chip) requerirá de una extracción física.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

Si un investigador llega a la escena de un posible delito informático y se encuentra con una tablet encendida, ¿La información de qué componente deberá tener en cuenta para no perderla debido a su volatilidad?

- Registro aritmético
- Memoria RAM
- Tarjeta SIM
- Módulo memoria NAND

Siempre deberemos de conservar la memoria RAM en dispositivos encendidos.

Opción correcta

Siempre deberemos de conservar la memoria RAM en dispositivos encendidos.

Siempre deberemos de conservar la memoria RAM en dispositivos encendidos.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

Como investigador forense qué tipo de consideraciones tengo que tener en cuenta cuando trabaje con un dispositivo móvil?

- Ninguna
- Tipos distintos de almacenamiento que encontraré (RAM, Memoria interna, tarjetas SD...)
- Si el dispositivo tiene algún tipo de funda o protector
- Volumen de contactos o mensajes que pueda tener

Los dispositivos móviles condicionan mucho el análisis forense y las particularidades.

Opción correcta

Es irrelevante para el análisis.

No es relevante desde un punto de vista del procedimiento del análisis forense.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

Para saber más

Hace unos años, el FBI durante una invitación necesitó hacer un análisis sobre un dispositivo móvil de la marca Apple que estaba bloqueado y apagado. Después de intentar muchos opciones y contactar con muchos laboratorios forenses finalmente una empresa israelí llamada Cellebrite fue la única capaz de acceder a los datos contenidos en el teléfono mediante su propio software. Este hecho fue un autentico hito, ya que hasta entonces los analistas forenses eran incapaces de acceder a los datos de dispositivos de Apple cuando estaban bloqueados. Si te interesa la noticia puedes ver mas info aquí.

1.3.- Herramientas.

Cuando hablamos de herramientas forenses para análisis de dispositivos móviles tenemos que distinguir entre las herramientas de tipo hardware y de tipo software. A nivel de hardware necesitaremos tanto herramientas para poder desmontar y acceder a los componentes de un dispositivo móvil como cables y conectores específicos para poder acceder al dispositivo mediante software.

A nivel de software es donde encontramos mas tipos de herramientas, normalmente en forma ***suite*** de herramientas, es decir un conjunto de herramientas que no solamente acceden a los datos del dispositivo sino que además interpretan la información y la presentan de forma clara, facilitando el trabajo del analista forense.

El listado de herramientas mas comunes, según el tipo de extracción actualmente es:

- Extracción manual
  - Project-A-Phone
  - EDEC Eclipse
- Extracción lógica
  - Belkasoft (suite)
  - Access Data's FTK
  - Autopsy
  - Celebrate Physical Analyzer
- Hex Dump / JTAG
  - Cellebrite UFED Physical Analyzer
  - XACT
- Chip-Off
  - iSeasamo Phone Opening Tool
  - FEITA Digital inspection station

Pixabay (Dominio público)

Citas Para Pensar

"Es imposible que un delincuente actúe, sobre todo teniendo en cuenta la intensidad de un delito, sin dejar rastros de esta presencia". Edmon Locard

Para saber más

Uno de los mayores retos que nos podemos encontrar cuando trabajamos con dispositivos móviles es encontrar el dispositivo encendido pero bloqueado con la contraseña del usuario y desconocer la contraseña. En algunos sistemas operativos como IOS de Apple, el sistema entero está cifrado con contraseña y

sin ella hay muchos datos que no son recuperables. En el siguiente video puedes ver un tutoría de cómo se puede recuperar información muy interesante a nivel forense en estas situaciones, para ello hacen uso del software Cellebrite.

Puedes ver el video aquí.