APUNTES 02

REALIZACIÓN DE ANÁLISIS FORENSES EN DISPOSITIVOS MÓVILES

ANÁLISIS FORENSE INFORMÁTICO

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

En esta unidad se 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. ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Uno de los principales objetivos dentro del análisis forense es entender qué ha sucedido en un entorno digital donde los usuarios han ejecutado distintas acciones. Debido a la investigación de la actividad de los usuarios, uno de los focos principales son los dispositivos móviles, ya que casi todos los usuarios tienen uno y suelen almacenar mucha información en ellos, que 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.

La mayoría de los sistemas operativos de los dispositivos móviles son de código abierto (Android), pero 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.

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:

- 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 lo 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.

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

La extracción manual sucede cuando visualizamos el contenido del móvil directamente sobre el propio dispositivo, por ejemplo, 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 (con cable de 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 específico 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, 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 comportan a nivel eléctrico los distintos componentes físicos. Existen pocas empresas que puedan realizar este tipo de análisis.

1.3.- HERRAMIENTAS

Las herramientas forenses para análisis de dispositivos móviles deben distinguirse 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 más 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 más 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

AUTOEVALUACIÓN

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

a) Extracción HexDump
b) Extracción física
c) Extracción lógica
d) Extracción NAND

2- 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?

a) Registro aritmético
b) Memoria RAM
c) Tarjeta SIM
d) Módulo memoria NAND

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

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

TEST I

1- En el ámbito del forense móvil se considera un método de extracción…:

a) Extracción lógica
b) JTAG
c) Extracción micro
d) Todas las anteriores

2- La extracción lógica podría alterar la evidencia al ser manipulada. ¿Verdadero o falso?

a) Verdadero
b) Falso

3- La extracción micro es uno de los métodos de extracción más comunes. ¿Verdadero o falso?

a) Verdadero
b) Falso

4- Los sistemas operativos de los dispositivos móviles a veces son:

a) Mono hilo
b) Cerrados
c) Mono núcleo.
d) Mono usuario.

5- Cuando nuestro código fuente necesita ser leído en tiempo real por un programa que lo traduce a código máquina, estamos hablando de lenguaje:

a) Depurado
b) Interpretado
c) Modular

6- Cuando visualizamos los mensajes o llamadas realizadas desde la pantalla del móvil estamos haciendo:

a) Consulta lógica
b) Extracción micro
c) Extracción física.
d) Extracción lógica.

7- Una de las complicaciones del análisis forense móviles:
a) Escenario heterogéneo
b) Poca documentación.
c) Dificultad para extraer memorias
d) Gran número de conectores.

8- En muchos casos la investigación del dispositivo móvil tiene como objetivo:
a) Tener resultados más precisos
b) Disponer de conclusiones de forma más rapida que en el análisis de un ordenador personal
c) Tener disponible las evidencias antes de tiempo.
d) Investigar la actividad del usuario.

9-La cantidad y tipos de herramientas de forense para dispositivos móviles es considerablemente diferente a la de las computadoras personales. ¿Verdadero o falso?
a) Verdadero
b) Falso

10- ¿Qué metodología se sigue a nivel forense?:
a) UNE UNI 2001.
b) La metodología es la misma si bien las herramientas cambian
c) La ISO 27001
d) No hay una metodologia clara.

TEST II

1- El método Chip-off consiste en la extracción lógica del chipset de memoria. ¿Verdadero o falso?
a) Verdadero
b) Falso

2- Los sistemas operativos móviles no condicionan el análisis forense
a) Verdadero
b) Falso

3- ¿Qué significa NAND?:
a) Nano Nato Technology
b) Nor AND
c) Not AND
d) Nano AND

4- ¿Por qué los dispositivos móviles son objetivos de análisis forense?:
a) Son evidencias que se procesan más rápido
b) Contienen gran cantidad de información sensible
c) Por que son más sencillos de analizar.
d) Requieren de menos procesos para ser analizados. Quitar mi elección

5- Los métodos de extracción de evidencias mediante Chip-off manipulan el sistema operativo del dispositivo. ¿Verdadero o fals
a) Verdadero
b) Falso

6- La extracción mediante JTAG y Hex dump funciona a bajo nivel.
¿Verdadero o falso?
a) Verdadero
b) Falso

7- La metodología del análisis forense móvil varía mucho de la de un ordenador. ¿Verdadero o falso?
Seleccione una:

a) Verdadero
b) Falso

8- iOS de Apple es un sistema cerrado. ¿Verdadero o falso?

a) Verdadero
b) Falso

9- Un ejemplo de sistema operativo abierto de dispositivos móviles es:

a) Nokia.
b) Android
c) iOS
d) Widows Vista.

10- Los dispositivos móviles requieren de conectores y cables específicos para ser analizados. ¿Verdadero o falso?

a) Verdadero
b) Falso

Respuestas autoevaluación:
1. b), Al ser un acceso físico (chip) requerirá de una extracción física.
2) b, Siempre deberemos de conservar la memoria RAM en dispositivos encendidos.
3. b), a- Los dispositivos móviles condicionan mucho el análisis forense y las particularidades. b- Opción correcta. c- Es irrelevante para el análisis. d- No es relevante desde un punto de vista del procedimiento del análisis forense.
Respuestas Test I
1. d), 2. a), 3. b), 4. b), 5. b), 6. a), 7. a), 8. d), c), d), 9. a), 10. b)
Respuestas Test II
1. b), 2. b), 3. c), 4. b), 5. b), 6. a), 7. b), 8. b), c), d), 9. a), 10. c)

Apartado 1 - Extracción de la evidencia

Para hacer esta tarea necesitaremos tener acceso a un dispositivo Iphone.
En caso de que no tengamos proporcionamos una imagen de un de un dispositivo Iphone creada con fines de formación. Si es tu caso puedes bajar la imagen, descomprimirla y saltar hasta el procesado.
http://downloads.digitalcorpora.org/corpora/mobile/ios_13_4_1/ios_13_4_1.zip
Empezaremos identificando físicamente nuestro dispositivo. Debemos tener en cuenta dos factores, si está encendido y si está bloqueado con código.
Si está apagado poco podremos hacer más que análisis a bajo nivel o con herramientas muy específicas.
Si está bloqueado con código y no lo conocemos nos encontraremos con el sistema de ficheros cifrado y además será difícil de hacer análisis forense. Aunque veremos alternativas en estos casos.
En este caso vamos a hacer una extracción lógica. Para ello probamos a conectar el dispositivo Iphone (conector lightning-USB) mediante cable a nuestro ordenador.
Lo primero que hará el ordenador y el teléfono móvil será pedirnos confiar en el ordenador y tendremos que "firmar" nuestro consentimiento de esta relación de confianza (móvil-ordenador) mediante el código de desbloqueo o sistema biométrico. (Esto sucede desde la versión 11.4 del sistema operativo de Iphone iOS)
Para realizar la extracción podremos hacerlo de dos maneras, bien con una herramienta forense específica para dispositivos móviles o mediante el software de Itunes de Apple a través de un backup.
Al ser una extracción lógica corremos el riesgo de cambiar el estado del dispositivo al realizar la extracción. Es uno de los riesgos que corremos con este tipo de procedimientos.
Para hacer la extracción de forma directa usaremos la herramienta de magnet acquire. Se puede descargar el software rellenando formulario en este enlace, al cabo de unas horas recibiremos el link de descarga. (*https://www.magnetforensics.com/resources/magnet-acquire/).*
Para la extracción mediante backup de itunes puedes ver una guía
https://www.youtube.com/watch?v=Gt8kxLVY1a0

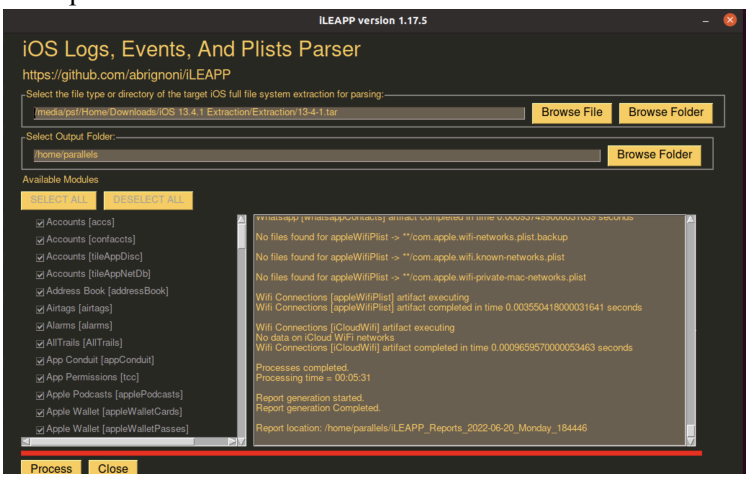
Apartado 2 – Análisis y Preguntas

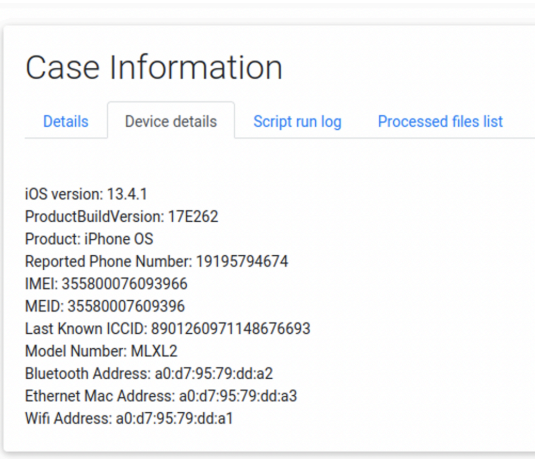
Para el procesado vamos a trabajar una herramienta open source para aportarnos visibilidad.
Funcionará tanto en Windows como en Linux, para este caso vamos a trabajar con una máquina virtual de Linux con Ubuntu.
La podremos descargar desde la web de github https://github.com/abrignoni/iLEAPP
Clonamos el repositorio mediante el comando:
git clone https://github.com/abrignoni/iLEAPP

```
parallels@ubuntu-linux-20-04-desktop:~$ git clone https://github.com/abrignoni/iLEAPP
Clonando en 'iLEAPP'...
remote: Enumerating objects: 4994, done.
remote: Counting objects: 100% (955/955), done.
remote: Compressing objects: 100% (376/376), done.
remote: Total 4994 (delta 615), reused 829 (delta 576), pack-reused 4039
Recibiendo objetos: 100% (4994/4994), 3.86 MiB | 5.58 MiB/s, listo.
Resolviendo deltas: 100% (3411/3411), listo.
parallels@ubuntu-linux-20-04-desktop:~$ cd iLEAPP/
parallels@ubuntu-linux-20-04-desktop:~/iLEAPP$ pip install -r requirements.txt
Ignoring python-magic-bin: markers 'platform_system == "Windows"' don't match your environment
Ignoring python-magic-bin: markers 'platform_system == "Darwin"' don't match your environment
Collecting numpy==1.21.4
  Downloading numpy-1.21.4-cp38-cp38-manylinux_2_17_aarch64.manylinux2014_aarch64.whl (13.0 MB)
     |████████████████████████████████| 13.0 MB 6.4 MB/s
Collecting astc_decomp
  Downloading astc_decomp-1.0.3.tar.gz (58 kB)
     |████████████████████████████████| 58 kB 8.7 MB/s
Collecting biplist
  Downloading biplist-1.0.3.tar.gz (21 kB)
Collecting bs4
  Downloading bs4-0.0.1.tar.gz (1.1 kB)
Collecting pyliblzfse
  Downloading pyliblzfse-0.4.1.tar.gz (47 kB)
     |████████████████████████████████| 47 kB 9.9 MB/s
Collecting packaging==20.1
  Downloading packaging-20.1-py2.py3-none-any.whl (36 kB)
Collecting pathlib2==2.3.5
  Downloading pathlib2-2.3.5-py2.py3-none-any.whl (18 kB)
```

Deberemos también instalar la lista de dependencias necesarias, mediante los comandos:
cd iLEAPP
Y luego:
pip install -r requirements
Una vez que tengamos instalado el software, lo arrancaremos, esta vez lo haremos mediante la interfaz gráfica (si estamos usando Linux tendremos que instalar la librería tkinter mediante sudo apt-get install tkinter)

pyhton3 ileappGUI.py
Para ello seleccionaremos el fichero .tar que nos ha creado la herramienta forense o directamente el directorio del backup de itunes.





Una vez que acabe de procesar se nos abrirá una página web donde veremos los detalles de la muestra. 1

Podremos ver el detalle del dispositivo (Importante anotar estos detalles)

PREGUNTAS

1. ¿Qué sucede cuando conectamos el dispositivo móvil al ordenador?
    a. Está respondido en el apartado 1, pero nos pedirá si confiamos en esta relación de confianza con el ordenador. Deberemos firmar este consentimiento mediante código de desbloqueo.
2. ¿Qué tipo de extracción es?
    a. Es una extracción de tipo lógica.
3. ¿Qué riesgo tenemos? ¿Qué cambios se han producido al hacer este tipo de extracción?
    a. Tenemos el riesgo de manipular la información, de hecho veremos que hemos provocado cambios como la lista de dipositivos conocidos, certifidados de confianza, permisos, etc
4. ¿Qué diferencias tenemos entre este tipo de extracción y una física?
    a. En la física requeriría de manipular el terminal. Para que una extracción física tuviera validez de cara a juicio deberíamos de tener un notario y un representante del dueño del móvil.
5. ¿Qué alternativas tenemos si no conocemos el código de desbloqueo pero tenemos o podemos conseguir el usuario y contraseña de la cuenta de apple?
    a. Podemos usar un backup hecho previamente y alojado en la nube de apple.
6. ¿Eres capaz de identificar el número de móvil?
    a. Podemos ver esta información en las propiedades del dispositivo
7. ¿Eres capaz de identificar que apps tienen concedidos permisos a qué recursos? ¿El usuario ha sido consciente de forma explícita de este consentimiento?
    a. Podemos ver los tipos de permiso y sus apps en el menú TCC