Práctica 1. Análisis forense en Android.

Extracción de evidencias.

El Smartphone se ha convertido en una herramienta imprescindible en todos los sectores de la sociedad europea: desde consumidores normales hasta altos funcionarios gubernamentales y el sector empresarial.

Los teléfonos inteligentes son famosos por su versatilidad: en un solo día, un teléfono inteligente puede hacer de monedero (wallet), de lector de códigos de barras, de sistema de navegación por satélite, de cliente de correo electrónico o red social, de punto de acceso WiFi y obviamente se pueden utilizar para realizar una llamadas telefónicas. Destacar que últimamente se están utilizando como sensores de salud inteligente, lo que permite a los pacientes cardíacos permanecer en casa de manera segura, mientras el personal médico controla y supervisa sus problemas cardíacos.

El análisis forense móvil se refiere al análisis forense digital relacionado con la recuperación de datos o evidencia digital de un dispositivo móvil (es decir, teléfonos móviles, así como otros dispositivos digitales como tabletas y dispositivos GPS). Es importante que esta recuperación se realice en condiciones forenses. Hay una serie de elementos que deben tenerse en cuenta cuando se trata de análisis forense móvil:

- En cuanto a adquisición de datos, nos vemos obligados a adquirir datos de un sistema encendido, ya que es posible que no haya forma de tomar imágenes, ya que las interfaces (hardware / software) para acceder a la memoria interna del dispositivo pueden faltar a propósito. Hay que tener cuidado de adquirir datos de la memoria extensiones (como tarjetas SD), ya que pueden contener información valiosa para fines de investigación.

- Establecer y mantener la cadena de custodia (CoC) y mantener la integridad en el dispositivo móvil puede resultar bastante difícil cuando se trata de dispositivos móviles. La mayoría de las herramientas forenses disponibles requieren que el investigador instale una aplicación en el sistema que se analizará. Además, no hay forma de hacer que los sistemas de archivos sean de solo lectura. Investigar el dispositivo en un entorno de prueba puede resultar reconocido por malware y conducir a la pérdida de pruebas. Por lo tanto, la obtención de pruebas de dispositivos móviles puede dañar la integridad de las pruebas y hacerlas no admitidas para los juicios.

Objetivos:

- Tomar conciencia de las dificultades que presenta la obtención de evidencias forenses en Android.
- Aprender a extraer evidencias en dispositivos móviles con SO Android.

Materiales

- Android Studio
- Virtualbox
- SDK platform tools
- Andriller
- AFLogical OSE

Se pide:

1) Familiarización con Android.

    a) Instala Android Studio.
    b) Ejecuta una máquina virtual con Android (AVD)
    c) Instala el paquete Android Debug Bridge (ADB platform tools)
    d) Habilita la depuración en el emulador (Developer Options>USB debugging) y practica el comando ADB con los siguientes modificadores: DEVICES,, SHELL, ROOT, PULL y PUSH.

2) Virtualización de Android de la forma que más se aproxima a la realidad.

    a) Descarga la versión x86 de Android aquí.
    b) Crea una VM de linux de 32bits (2GB RAM, 8GB HD y 256MB de Video).
    c) Instala Android en la VM anterior. Registrate con tu cuenta habitual y sincroniza los contactos, correo, etc.
    d) Instala la aplicación "AFLogical OSE" (ADB CONNECT e INSTALL) y realiza una extracción de evidencias. Ten en cuenta las instrucciones que te ofrecen en el siguiente enlace.
    e) Instala en el PC la aplicación "Andriller" y realiza una extracción de evidencias de la VM Android.

3) Lee la **sección 2** del documento "ANÁLISIS DEL MODELO DE DATOS DE LA RED SOCIAL WHATSAPP Y SUS APLICACIONES AL PERITAJE" y contesta a las siguientes preguntas:

    a) ¿En qué consisten los análisis forenses consensuados y no consensuados?

    b) ¿Qué técnicas se pueden utilizar para peritar una conversación de whatsapp?

    c) ¿Dónde guarda Whatsapp la clave de cifrado y sus BBDD? Cómo podemos extraer estos directorios.

4) Instala “Whatsapp” en la VM del apartado anterior. Realiza una extracción de la clave de cifrado y las BBDD y utiliza alguna herramienta (Andriller) para visualizar las información (pide a alguien que te escriba).