Análisis forense en Android

Metodología

Jorge Coronado

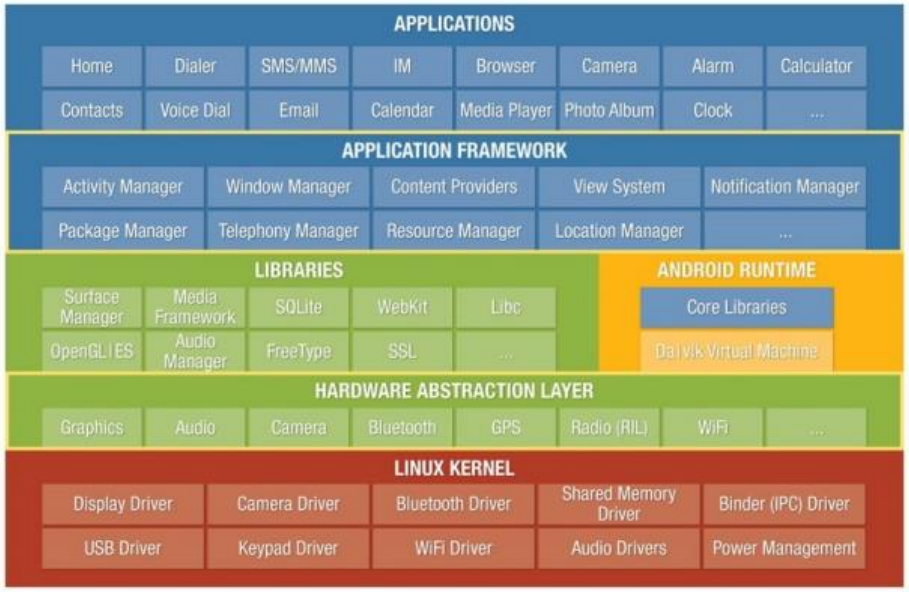
QUANTIKA 14

¿Qué vamos a ver?

1. Las entrañas de Android
2. Metodología sobre análisis forense en Android

ANTES DE SABER LA METODOLOGÍA TENEMOS QUE SABER CÓMO FUNCIONA ANDROID

La arquitectura de Android



El Entorno de ejecución Android está compuesto por un capa de librerías en java con funcionalidades de específicas de Android como pueden ser
las siguientes

- **android.app** Da acceso al modelo de la aplicación.
- **android.content** Facilita el acceso a contenido y comunicación entre aplicaciones y componentes.
- **android.database** Da acceso a datos con un sistema de interfaz con bases de datos sqlite.
- **android.opengl** Una interfaz para el API de OpenGL ES.
- **android.osAcceso** a servicios de el sistema operativo.
- **android.text** Para manipular texto en el dispositivo.
- **android.view** Servicios para creación de la interfaz gráfica.
- **android.widget** Componentes para la interfaz gráfica como botones labels listas etc.
- **android.webkit** Clases para interacción con la web

La parte más importante de esta es la llamada Dalvik Virtual Machine. Esta es una máquina virtual java optimizada para Android en la que se encarga de que cada aplicación Android este encerrada y funcione en su propia instancia virtual Dalvik por lo tanto haciendo que el sistema operativo sea muy seguro.

Cómo se inicializa

Es importante conocer cómo Android se inicializa para poder empezar a hacer un análisis forense de el dispositivo:

• **Boot ROM:** hay una dirección predefinida que al iniciar el microprocesador busca y encontrarás el bootloader por la cual procederá a cargar en memoria.

• **Bootloader:** este es el primer programa que se inicia al encender el dispositivo y es el encargado de encender los componentes hardware y manejar su funcionamiento y empezar la carga del arranque de el sistema.

• **Kernel:** el kernel es inicializado en la que montará el sistema de archivos memoria drivers y al terminar buscará el programa INIT que será el que inicie el sistema operativo Android

• **El proceso Init:** una vez montado el sistema de archivos se ejecutara el proceso de init encargado de comenzar el sistema operativo Android cargando las librerías a el sistema para el funcionamiento correcto de esta.

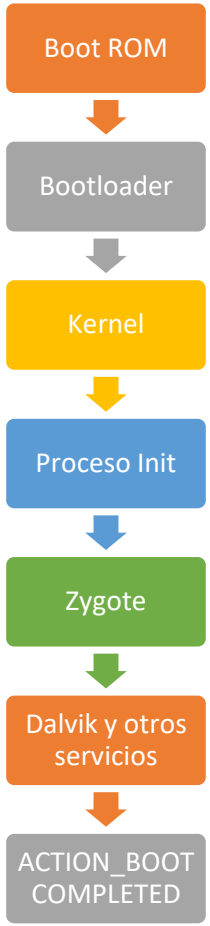
• **Zygote y Dalvik:** Init inicializa el servicio de Zygote que es el encargado de inicializar las librerías de clases de Android el encargado de que se inicialice las máquinas virtuales Dalvik que es la máquina virtual donde se ejecutarán los procesos.

• **Servicios del Sistema o Servicios:** Zygote también inicializará los servicios de sistema como son los sensores el módem, teclado, batería.

• **Boot completado: u**na vez completado el inicio, se mandara una acción de tipo BROADCAST al sistema con el mensaje "ACTION_BOOT_COMPLETED" que indicará el fin de la carga del proceso y debería de ver ya por pantalla nuestro escritorio Android

Las apps de Android pueden enviar o recibir mensajes de emisión desde el sistema de Android y otras apps para Android. Estas emisiones se envían cuando ocurre un evento de interés. Por ejemplo, el sistema Android envía emisiones cuando ocurren diferentes eventos del sistema, como cuando este se inicia o cuando el dispositivo comienza a cargarse. Las apps también pueden enviar emisiones personalizadas.

Más info:
https://developer.android.com/guide/components/broadcasts?hl=es-419



Los analistas de virus de la empresa Doctor Web detectaron un programa nocivo incrustado en el firmware de varios dispositivos móviles bajo la administración del SO Android. El troyano llamado Android.Triada.231 fue incrustado en una biblioteca del sistema. Penetra en los procesos de todas las aplicaciones activas y es capaz de descargar e iniciar los módulos extra sin autorización.

Particionamiento de la memoria

```
#cat /proc/mtd
dev:    size   erasesize  name
mtd0: 00040000 00020000 "misc"
mtd1: 00500000 00020000 "recovery"
mtd2: 00280000 00020000 "boot"
mtd3: 04380000 00020000 "system"
mtd4: 04380000 00020000 "cache"
mtd5: 04ac0000 00020000 "userdata"
```

- **Bootloader:** es donde encontramos el bootloader del teléfono y será lo primero que nuestro dispositivo iniciará.
- **Recovery:** desde el bootloader podemos elegir bootear desde esta partición y aquí tendremos herramientas de mantenimiento para el móvil. Al igual que la partición boot tiene su propio kernel y ramdisk.
- **Boot:** esta partición contiene el kernel y ramdisk de Android y es la que se inicia en un booteo normal.
- **System:** aquí encontramos el framework de Android.
- **Cache:** aquí se almacena los datos que el usuario utiliza con más frecuencia para agilizar la carga de ellos.

METODOLOGÍA

1. Evaluar la situación / asesoramiento
2. Confiscación y aislamiento
3. Adquisición
4. Análisis
5. Creación de un informe
6. Ratificación

¿Cómo evaluar la situación?

1. Finalidad de la investigación
2. ¿Cuál es el objetivo del cliente?
3. El estado físico del dispositivo
    1. Pantalla rota
    2. Entrada USB
    3. Micro SD
4. Versión de Android
5. Versiones de las aplicaciones
6. Anteriores formateos o modo fábrica
7. El móvil está rooteado
8. Está habilitada la depuración USB
9. ¿Está bloqueado? PIN, contraseña de desbloqueo, otras contraseñas, etc

¿Es necesario hacer la adquisición ante notario?

https://www.notariofranciscorosales.com/acta-notarial-de-una-web-2/

https://www.notariofranciscorosales.com/hash-y-actas-notariales/

9F5137476

D. JUAN PEREZ HEREZA
NOTARIO
Avda. Menéndez Pelayo, 5 - 2ºD
28009 MADRID
Tel.: 91 432 18 64 - Fax: 91 432 18 66

ACTA DE MANIFESTACIONES.-

NÚMERO NOVECIENTOS UNO. ----------

EN MADRID, mi residencia, a cuatro de Junio de dos mil nueve.----------

Ante mí, JUAN PÉREZ HEREZA, Notario del Ilustre Colegio de esta Capital, ----------

----------COMPARECEN ----------

DON [redacted], mayor de edad, casado, [redacted] DE FRANCISCO, mayor de edad, soltera, vecina de Getafe [redacted] D.N.I. número

¿Es necesario ser root?

https://www.notariofranciscorosales.com/acta-notarial-de-una-web-2/

https://www.notariofranciscorosales.com/hash-y-actas-notariales/