Práctica 3. Análisis forense en Android.

Viabilidad de realizar un peritaje forense en Android.

En general, es bien conocida la importancia del análisis forense de los volcados de memoria RAM así como el análisis de la memoria persistente. Después de los logros conseguidos al respecto en los sistemas operativos Windows, Linux y Mac OS X es hora de preguntarnos si las herramientas de análisis forense ampliamente consolidadas, como son DD, LiME y Volatility, pueden ser usadas para analizar dispositivos Android.

Existen multitud de trabajos de investigación sobre el análisis de RAM correspondiente para dispositivos Android basados en Linux. Estos artículos están dirigidos principalmente a dispositivos Android virtualizados.

Objetivos:

- Investigar las dificultades que aparecen cuando se realizan peritajes forenses en Android.
- Estudiar las posibilidades de realizar una pericial forense a un dispositivo dependiendo de las características del mismo.

Documentación:

- Practical Infeasibility of Android Smartphone Live Forensics
- MobilEdit! Forensic Express

Se pide ojear la documentación anterior y contestar a las siguientes preguntas:

1. ¿Cúal es la situación ideal que permitiría un perfecto análisis forense a un dispositivo Android? (Clonado de memoria interna y volcado de memoria volátil)

2. ¿Cúal es la situación real con la que nos encontramos en un dispositivo Android genérico tipo Samsung, Xiaomi o Asus? ¿Qué problemas presentan y cómo sería teóricamente posible solucionarlos?

3. Con respecto a la funcionalidad de adquisición física que presentan algunos dispositivos:

    a. Investiga en qué consiste la extracción física usando el hack EDL.

    b. Investiga en qué consiste la extracción física de dispositivos con chipset MTK.

    c. Investiga en qué consiste la extracción física usando el hack LG.

    d. Investiga la vulnerabilidad DIRTY COW para conseguir rootear un dispositivo Android.

4. Tenemos la necesidad imperiosa de rootear un dispositivo Android con el fin de hacer un clonado de su memoria persistente. Pide al profesor que te preste un dispositivo, investiga qué pasos tendría que dar para conseguirlo y rootea el dispositivo intentando no perder las información almacenada en el mismo.