www.eysglobal.com

LABORATORIO DE ADQUISICIÒN DE DATOS

Técnicas de extracción y análisis de información en dispositivos móviles Android.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

El objetivo del laboratorio es mostrar las diferentes técnicas de extracción y análisis de información en dispositivos móviles Android.

En concreto, se van a realizar las siguientes actividades:

- Adquisición de una imagen forense de un dispositivo Android.
- Adquisición de una imagen de una tarjeta SD.
- Adquisición lógica de un dispositivo Android.
- Adquisición de la memoria de un dispositivo Android.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

IMAGEN FORENSE DE UN DISPOSITIVO ANDROID

CONEXION DEL DISPOSITIVO

Para la realización de este laboratorio es necesario disponer de un dispositivo rooteado.

La adquisición de la imagen del dispositivo se realizará mediante la conexión USB, por lo que procedemos a conectarlo al equipo de análisis.

Vamos a proceder a realizar la imagen desde Santoku, por lo que en VirtualBox, conectamos el dispositivo a la maquina virtual.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

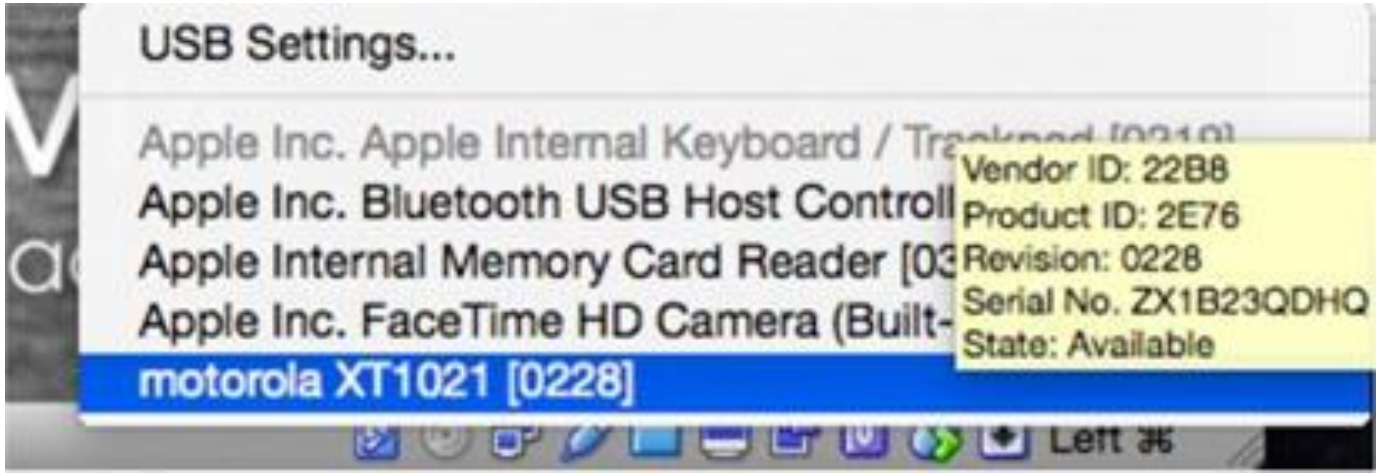


Figura : Conexión del dispositivo

En la opción de Settings, activamos la opción de USB 2.0 ´o 3.0, dependiendo de nuestro dispositivo. Para esto, debemos descargar una extensión de VirtualBox:

http://www.virtualbox.org/wiki/Downloads

Técnicas de extracción y análisis de información en dispositivos móviles Android.

PREPARACIÒN DE LA ADQUISICIÒN

Una vez conectado en Santoku, abrimos una shell en el dispositivo y cambiamos al usuario root:

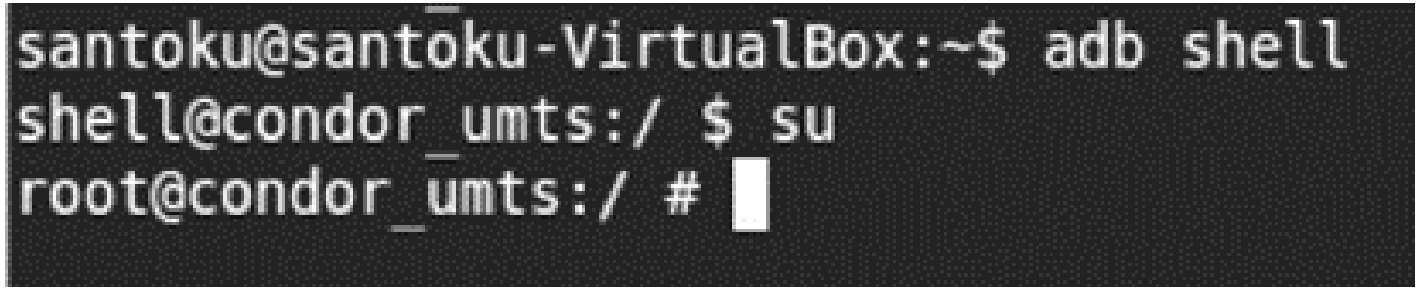


Figura : Preparación de la adquisición 1.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

Dado que la única partición que puede modificarse por el usuario es aquella que esta montada en data, utilizamos mount, para averiguar el dispositivo que le corresponde:

```
root@condor_umts:/ # mount | grep data
/dev/block/platform/msm_sdcc.1/by-name/system /system ext4 ro,seclabel,relatime,data=ordered 0 0
/dev/block/platform/msm_sdcc.1/by-name/userdata /data ext4 rw,seclabel,nosuid,nodev,noatime,nodiratime,discar
d,nobarrier,noauto_da_alloc,data=ordered 0 0
```

Figura : Preparación de la adquisición 2

Técnicas de extracción y análisis de información en dispositivos móviles Android.

```
root@condor_umts:/ # df /data
Filesystem               Size     Used     Free   Blksize
/data                    2.2G     1.2G   941.7M   4096
```

Figura : Preparación de la adquisición 3.

ADQUISICIÒN DE LA IMAGEN

La adquisición necesita de una tarjeta SD vacía en el dispositivo.

Dependiendo de la versión de Android y del dispositivo, la tarjeta se montara en un directorio.

```
root@condor_umts:/ # mount | grep sdcard
/dev/block/vold/179:65 /mnt/media_rw/sdcard1 vfat rw,dirsync,nosuid,nodev,r
mask=0007,dmask=0007,allow_utime=0020,codepage=cp437,iocharset=iso8859-1,sh
ro 0 0
/dev/fuse /storage/sdcard1 fuse rw,nosuid,nodev,relatime,user_id=1023,group
_other 0 0
root@condor_umts:/ #
```

Figura : Adquisición de la imagen 1.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

Para realizar la adquisición, ejecutamos dd con los parámetros correspondientes.

```
> dd if=/dev/block/platform/msm_sdcc.1/by-name/userdata
of=/storage/sdcard1/user.img bs=4096
```

Figura: Adquisición de la imagen 2.

Una vez se haya realizado la imagen desde la consola de la máquina de análisis escribimos:

```
> adb pull /storage/sdcard1/user.img
```

Figura : Adquisición de la imagen 3.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

IMAGEN DE UNA TARJETA SD

INSTALACIÒN DE BUSYBOX

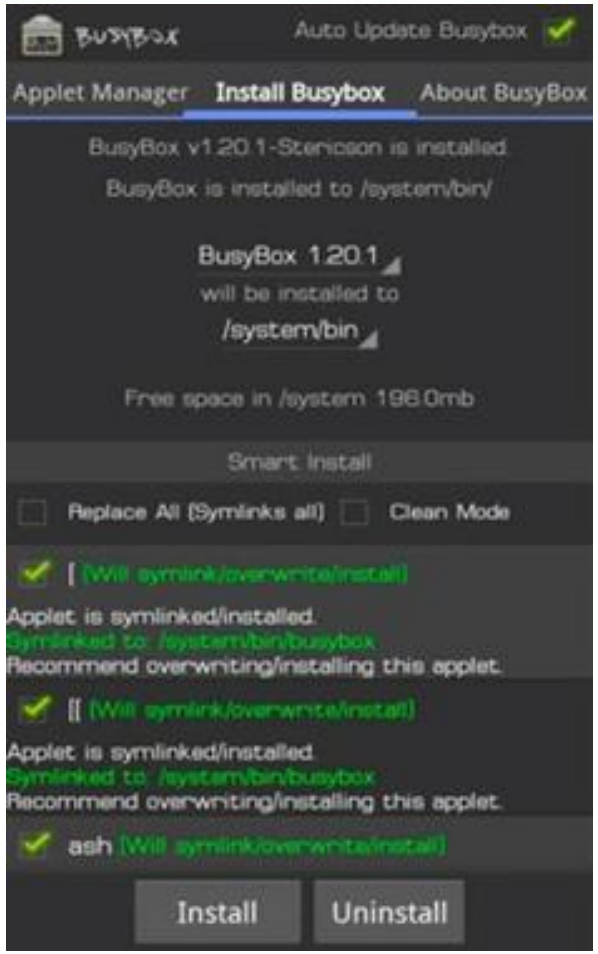
Para la adquisición de imágenes de tarjetas SD necesitamos otro dispositivo en el que almacenar la imagen capturada.

Mediante la utilidad BusyBox podemos redirigir los datos generados por dd directamente a un puerto donde los reciba la maquina de análisis.

Se puede instalar BusyBox a través de Google Play :

https://play.google.com/store/apps/details?id=stericson.busybox

Técnicas de extracción y análisis de información en dispositivos móviles Android.



Una vez instalado, lo ejecutamos y procedemos a la instalación sin aceptar los mensajes publicitarios.

Figura : Instalación de BusyBox.

OBTENCIÒN DE LA IMAGEN

Averiguamos el dispositivo correspondiente a la tarjeta de memoria:

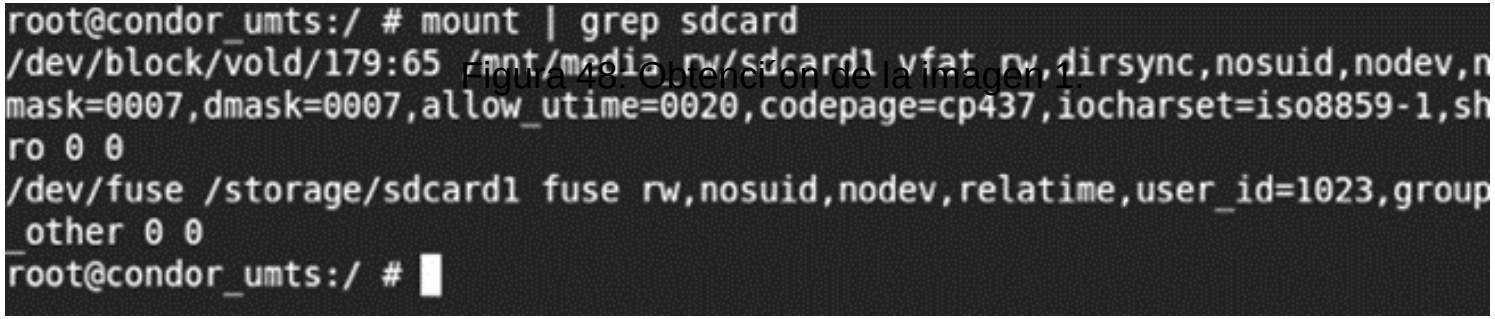


Figura 48: Obtenci´on de la imagen 1.

Figura : Obtención de la imagen 1.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

Dado que no podemos guardar la imagen en la tarjeta SD, la vamos a transmitir a la máquina de análisis a través de un socket. Para ello, abrimos una nueva ventana del terminal en la máquina de análisis y escribimos:

Figura : Obtención de la imagen 2.

De esta manera, nos aseguramos de que todo lo que le llega a a db por el puerto 8888, es transmitido a la máquina de análisis por el mismo puerto.

Ejecutamos:

```
> dd if=/dev/block/vold/179:65 | busybox nc -l -p 8888
```

Figura : Obtención de la imagen 4.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

Y en la máquina de análisis empezamos a recibir la información mediante el siguiente comando:

```
santoku@santoku-VirtualBox:~$ nc 127.0.0.1 8888 > sd_image.dd
santoku@santoku-VirtualBox:~$
```

Figura : Obtención de la imagen 4.

ADQUISICIÒN LÒGICA DE UN DISPOSITIVO ANDROID

INSTALACIÒN DE AFLOGICAL

En este laboratorio vamos a utilizar la herramienta Aflogical, para la adquisición lógica de evidencias.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

```
> aflogical-ose
```

Figura : Instalaciòn de Aflogical.

De este modo, se instalaría y ejecutaría la aplicación.

EJECUCIÒN DE AFLOGICAL

Una vez ejecutada la aplicación, en el dispositivo deberemos marcar la información que queremos extraer en el dispositivo.

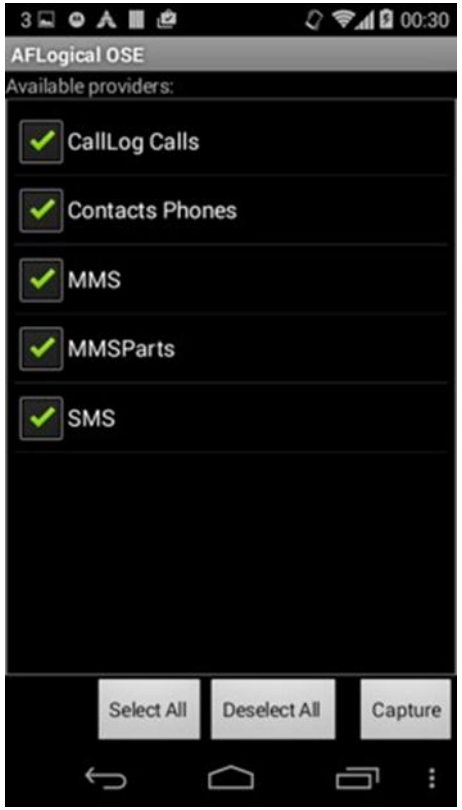


Figura : Ejecución de Aflogical 1.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

Una vez obtenida la información en el dispositivo, continuamos en la consola para transferir los datos a nuestro dispositivo.

```
santoku@santoku-VirtualBox:~$ aflogical-ose
Make sure android device is connected to USB
[sudo] password for santoku:

697 KB/s (28794 bytes in 0.040s)
        pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk
Success

Starting: Intent { cmp=com.viaforensics.android.aflogical_ose/com.viaforensics.a
ndroid.ForensicsActivity }

Press enter to pull /sdcard/forensics into ~/aflogical-data/

pull: building file list...
pull: /sdcard/forensics/20160215.2430/SMS.csv -> /home/santoku/aflogical-data/20
160215.2430/SMS.csv
pull: /sdcard/forensics/20160215.2430/MMS.csv -> /home/santoku/aflogical-data/20
160215.2430/MMS.csv
```

Figura : Ejecución de Aflogical 2.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

RESULTADOS

Los resultados pueden ser inspeccionados utilizando el navegador de archivos de Santoku Linux.

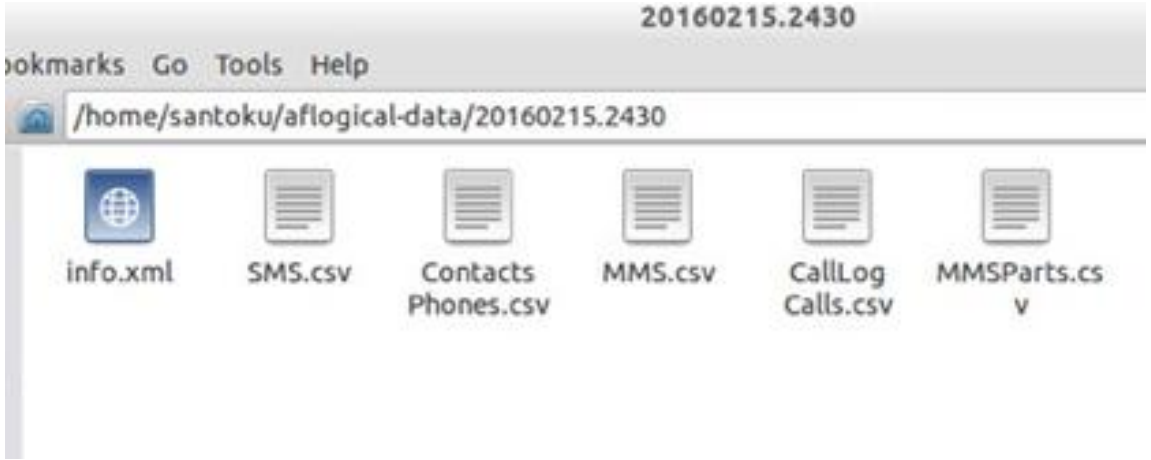


Figura : Resultado obtenido.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

ADQUISICIÒN DE MEMORIA EN ANDROID

INSTALACIÒN Y EJECUCIÒN DE LIME

Al igual que en el laboratorio anterior, en esta ocasión será necesario contar con un dispositivo rooteado.

En primer lugar, debemos descargar y compilar LiME. La guía de instalación se encuentra en:
https://github.com/504ensicsLabs/LiME/tree/master/doc

Una vez compilado, es necesario copiar el módulo al dispositivo del que se va a realizar el proceso de adquisición de la memoria:

Técnicas de extracción y análisis de información en dispositivos móviles Android.

```
> adb push lime.ko /storage/sdcard1/lime.ko
```

Figura : Instalación y ejecución de LiME 1.

Modificamos los puertos para redirigir la salida de LiME:

```
> adb forward tcp:4444 tcp:4444
```

Figura : Instalación y ejecución de LiME 2.

Abrimos una shell:

```
> adb shell
```

Figura : Instalación y ejecución de LiME 3.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

Accedemos a root y ejecutamos el mòdulo de kernel:

```
> su
> insmod /sdcard/lime.ko "path=/storage/sdcard1/ram.lime
format=lime"
```

Figura : Instalación y ejecución de LiME 4.

TRANSMISIÒN DE LA IMAGEN

La imagen se crea en formato lime en la sdcard del sistema.
Para obtenerla en la máquina de análisis utilizamos adb:

```
> adb pull /storage/sdcard1/ram.lime
```

Figura : Transmisión de la imagen 1.

Técnicas de extracción y análisis de información en dispositivos móviles Android.

La imagen obtenida puede ser analizada con volatility. Requiere de su instalación en Santoku:

```
> sudo apt-get install volatility
```

Figura : Transmisión de la imagen 2.