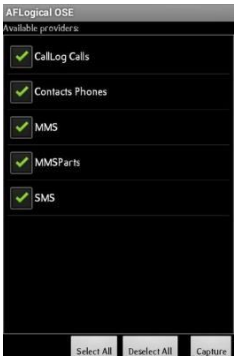
Asignatura: Application development for mobile devices.
Tarea 30: Análisis forense de un móvil.

La AFLogical OSE Open Source Edition, es una aplicación de código abierto de Android Forensics. La edición de código abierto ha sido lanzada para su uso por parte de personal ajeno a la aplicación de la ley, aficionados a Android y gurús forenses por igual. Le permite a un examinador extraer llamadas de CallLog, teléfonos de contactos, mensajes MMS, MMSParts y mensajes SMS de dispositivos Android.

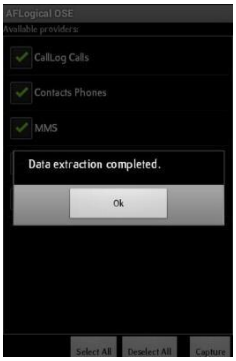
Para mayor información se puede consultar el siguiente sitio:
https://spijartech.wordpress.com/2016/03/13/aflogical-open-source-edition-ose-forensics-tool/

Paso 1. Instalar y ejecutar el archivo adjunto AFLogical OSE.

Paso 2. Cuando se ejecuta el archivo se muestran las opciones de búsqueda de información, habilitando o deshabilitando las opciones mostradas. Enseguida, digitar en Capture:



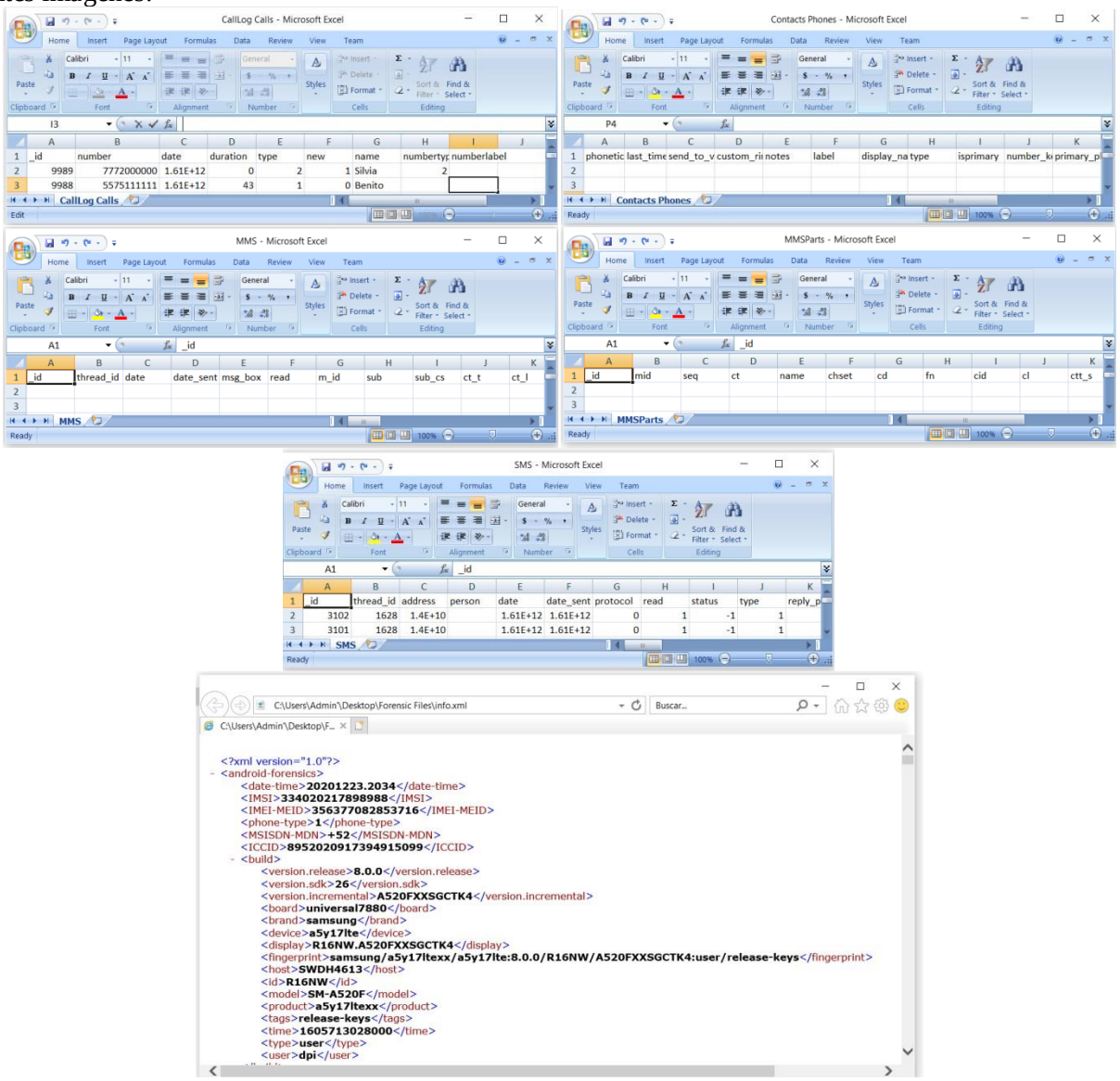
Paso 3. Al terminar, se indica el mensaje de terminación de la extracción de datos. Digitar en OK:



Paso 4. Abrir el Administrador de archivos y buscar una carpeta denominada Forensics. Cuando se abre la carpeta Forensics, se localiza una subcarpeta que al abrirla contiene los archivos con la información extraída. Esta carpeta se puede transferir después a cualquier otro dispositivo para analizar posteriormente estos contactos y registros de llamadas.

Paso 5. Abrir los archivos para leer los contactos en cualquier editor.

Paso 6. Si los archivos mostrados se abren bajo el sistema operativo Windows, la apariencia será similar a la mostrada en las siguientes imágenes:



EJERCICIO.
Diseñar una aplicación móvil que permita transferir la carpeta de archivos, con la información extraída, a cualquier otro dispositivo para analizar posteriormente estos contactos y registros de llamadas.

Nota: Generar un reporte con todos los pasos detallados con imágenes del desarrollo de la aplicación. Guardar la aplicación y todos los archivos obtenidos en una carpeta comprimida con la sintaxis AlumnoTarea28Grupo.zip. Enviar el reporte al sitio indicado por el profesor.

ANEXO.
Las siguientes herramientas son alternativas para el análisis forense.

- Oxygen Forensic Suite

Es una herramienta de análisis forense para dispositivos móviles, extracción de datos de múltiples fuentes, obtiene historial

de ubicaciones y archivos multimedia de drones, puede extraer datos de servicios como iCloud, Google, Microsoft, etc. Así como también puede obtener datos de IO y smartwatches, importación y análisis de registros de datos de llamadas.

- MSAB XRY

Es una herramienta de análisis forense que permite extraer y decodificar datos rápidamente de dispositivos más actuales y de otros dispositivos digitales, protege la integridad de la evidencia y soporta 28,150 dispositivos y apps.

- CellDEK

Compatible con más de 950 de los dispositivos más actuales y PDAs, está diseñado para utilizarse en laboratorios y en el campo pues permite obtener acceso a información de vital importancia. Es una suite muy completa.

- Paraben DDS

Está diseñado para el uso rápido en el campo con cualquier dispositivo móvil. Permite extracción de datos lógicos tales como registro de llamadas, mensajes de texto, imágenes, entre otros, y que pueden ser extraídos fácilmente usando DDS.

- Cellebrite UFED

Dispositivo que puede ser utilizado en campo y en laboratorios forenses. Puede extraer datos de vital importancia como imágenes, videos, mensajes de texto, registro de llamadas, información del dispositivo como el IMEI y ESN de más de 3200 dispositivos.

- The Sleuth Kit.

Es un conjunto de herramientas open source para el análisis de imágenes de discos. Cuenta con una interfaz gráfica conocida como Autopsy que agrupa todas sus herramientas y plugins.

- Bitpim

Programa open source que permite ver y manipular datos en muchos teléfonos CDMA de LG, Samsung, Sanyo y otras manufactureras. Incluye el directorio, calendario, imágenes, sonidos, sistema de archivos entre otras opciones.

- Mobiledit Lite

Puede transferir el contenido de su teléfono a otro dispositivo. Simplemente se selecciona el tipo de datos que se desea conservar, hacer clic y copiar. Copia contactos, mensajes, calendario, fotos, música, aplicaciones y documentos. Todo se colocará de forma inteligente en las carpetas correspondientes de un nuevo teléfono.