Revista de I+D TECNOLÓGICO

Portal de revistas: http://revistas.utp.ac.pa

Revisión sobre la forensía digital en dispositivos móvil con sistemas operativos Android

Review on digital forensics on mobile devices with Android operating systems

José Moreno[1], Isabel Leguias[2], Miguel Vargas Lombardo[2*]

[1]*Facultad de Ingeniería en Sistemas Computacionales, Universidad Tecnológica de Panamá, Panamá*

[2]*Grupo de Investigación en Salud Electrónica y Supercomputación, Universidad Tecnológica de Panamá, Panamá*

***Autor de correspondencia:** miguel.vargas@utp.ac.pa

RESUMEN- Esta investigación está enfocada en los procedimientos, mecanismos y metodologías de análisis forense digital en dispositivos móviles, con la intención de contar con un manual o metodología para el manejo de evidencias digitales en estos dispositivos. Por otra parte, trataremos las herramientas de *software* libre y privativas utilizadas para el análisis forense de *smartphones* con sistemas operativos Android. Como resultado se detectaron métodos de antiforensía que impiden la adquisición de los artefactos en los teléfonos inteligentes. En consecuencia, identificados técnicas antiforensía como técnicas criptográficas empleadas por los cibercriminales para esconder sus huellas o evidencias.

Palabras clave– *Adquisición, análisis, android, artefactos, antiforensía, datos, forensía, forensía para dispositivos vestibles, herramientas, protección de datos, teléfonos inteligentes.*

ABSTRACT– This research is focused on the procedures, mechanisms and methodologies of digital forensic analysis in mobile with the intention of having a manual or methodology for handling digital evidence in these devices. On the other hand, we will discuss the free and proprietary *software* tools used for the forensic analysis of *smartphones* with android operating systems. As a result, antiforestry methods were detected that prevent the acquisition of devices in *smartphones*. Consequently, identified antiforensic techniques as cryptographic techniques used by cybercriminals to hide their traces or evidence.

Keywords– *Acquisition, analysis, android, artifacts, antiforensy, data, forensics, forensics for wearable devices, tools, data protection, smartphone.*

1. Introducción

Forensía es la ciencia de examinar y descubrir ideas para la evidencia digital en la corte de acuerdo con la ley [1].

En el año de 1984 el FBI y diversas agencias que se dedican al cumplimiento de la ley inician el desarrollo de programas que examinan las evidencias computacionales. La primera persona procesada por un delito informático se da en 1989. El primer equipo conformado por el FBI es establecido en el año de 1991. Y en el año 1996 es utilizada la primera evidencia digital en un caso de delito informático en una corte [2].

Forensía digital es la disciplina o rama de la criminología y de la seguridad informática que consiste en obtener pruebas de un sistema.

En síntesis, el Principio de intercambio de Locard indica que cualquiera o cualquier objeto que ingrese en la escena del crimen transfiere un rastro en la escena o en la víctima y recíprocamente (se lleva consigo). En consecuencia, cada contacto deja un rastro o evidencia que lo asocia a la escena del crimen.

Igualmente, la informática forense incluye la preservación, identificación, extracción y documentación de la evidencia digital en forma de medios de almacenamiento magnético, óptico o electrónico. En consecuencia, dicha ciencia es sumamente importante a medida que los criminales expanden el uso de tecnología en actividades ilegales [3].

2. Sobre el alcance de la informática Forense

La informática forense es el proceso de investigación de los sistemas de información para detectar toda evidencia que pueda ser presentada como medio de prueba fehaciente para la resolución de un litigio dentro de un procedimiento digital [4]. Por otro lado, la evidencia digital se desarrolla sobre los elementos que pueda almacenar información en formato electrónico, de forma física o lógica y que permita constatar un hecho

Citación: J. Moreno y M. Vargas, “Revisión sobre la forensía digital en dispositivos móvil con sistemas operativos Android”, *Revista de I+D Tecnológico*, vol. 14, no. 2, pp. (74-83), 2018.

Tipo de artículo: Revisión. **Recibido:** 5 de junio de 2018. **Recibido con correcciones:** 21 de agosto de 2018. **Aceptado:** 16 de octubre de 2018.

investigado o el esclarecimiento del mismo. Son pruebas encontradas en algún componente de un sistema, pueden ser (memoria de un equipo, medio de almacenamiento, equipo de comunicación, periférico, etc.). Con referencia a la evidencia digital se explica cómo los materiales de la computadora y sus derivados pueden ser usados como evidencia contra actividades ilícitas [5].

2.1 Tipos de evidencia digital

Podemos clasificar las evidencias digitales en los siguientes tipos:

2.1.1 Evidencia volátil

Toda aquella evidencia que puede ser alterada con relativa facilidad.

Algunos ejemplos de evidencias volátiles son:

- Memoria caché
- Tablas de Enrutamiento
- Proceso en ejecución
- Memoria Ram.

2.1.2 Evidencia no volátil

Evidencia que no cambia con facilidad, sin embargo, igualmente cambia, pero no de manera constante.

Evidencias No volátiles:

- Discos duros
- CD/DVD
- Unidad *Flash*

2.1.3 Gestión de la evidencia digital

En este sentido se pretende evitar la invalidación de la evidencia digital, para ello el SANS define nueve elementos del proceso de forensía móvil [6] que explicaremos a continuación y podemos apreciar en la figura 1.

- Adquisición: recibe el dispositivo como prueba y se admite la solicitud de evaluación.
- Identificación: identifica las especificaciones y capacidades del dispositivo. Identifica las metas de la examinación e identifica la autoridad legal para realizar la evaluación.
- Preparación: se preparan los métodos y herramientas a utilizar. Prepara los medios de comunicación y la estación de trabajo forense para la evaluación, además prepara las herramientas a la versión más reciente.
- Aislamiento: se protege la evidencia y se evita la destrucción remota de datos, aislando el dispositivo de la red celular, *bluetooth* y *Wi-Fi*.
- Procesamiento: conduce a la adquisición forense y realiza el análisis forense, así como la búsqueda de *software* malicioso.
- Verificación: valida la adquisición, hallazgos forenses.
- Documentación/Informes: se toman notas sobre sus hallazgos y proceso para elaborar los informes forenses.
- Presentación: prepara las exposiciones y se presentan sus hallazgos.
- Archivar: mantiene una copia de los datos en un lugar seguro y de preferencia; mantenga los datos en formatos comunes para futuro.

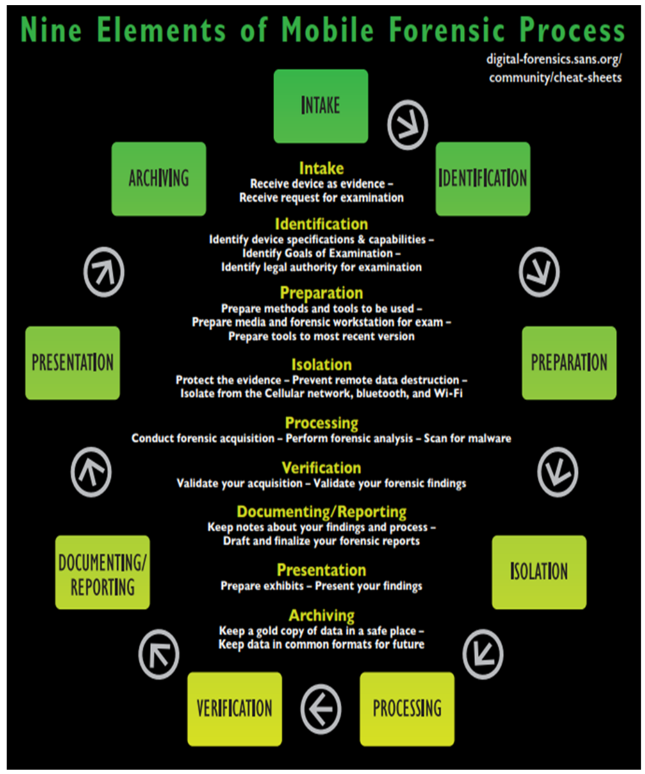

Figura 1. Diagrama de los nueve Elementos del Proceso de Forensía Móvil según el SANS [6].

3. Metodología Digital de Análisis Forense

Como Complemento del punto anterior en la siguiente sección identificamos los elementos o el esquema general para la Metodología Digital de Análisis Forense, según los autores [7] y que podemos observar el diagrama de la figura 2.

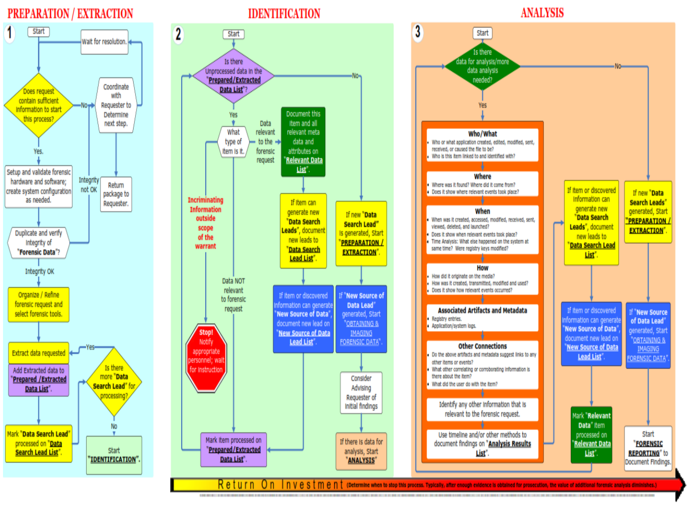

Figura 2. Mapa de la Metodología Digital de Análisis Forense según el departamento de justifica de los Estados Unidos [7].

3.1.1 Preparación y extracción de la información Forense

En esta fase los investigadores inician cuestionando si hay suficiente información para proceder, asegurando que hay una solicitud clara y que haya suficientes datos; si existe algún faltante coordinan con el solicitante, para luego establecer si continúan el proceso del análisis forense.

El primer paso de un proceso forense es la validación tanto del *hardware* y *software*, para asegurar que funcionen correctamente. Cuando el escenario forense está preparado para la investigación, el investigador duplica los datos forenses proporcionados en la solicitud y verifica su integridad. Se asume que los datos han sido obtenidos por un proceso legal apropiado y se ha creado una imagen forense de los mismos.

Los examinadores se aseguran de que la copia en su posesión esté intacta e inalterada. Por lo general, hacen esto verificando un *hash*, o huella dactilar digital, de la evidencia. En un examen posterior verifica la integridad de los datos a analizar y se desarrolla un plan para extraer datos. Luego se seleccionan las herramientas forenses que permitan responder las preguntas necesarias para resolver el caso. Los investigadores generalmente tienen ideas preliminares sobre las pistas (qué buscar), basándose en la solicitud. Estas pistas se agregan a una "Lista de pistas de búsqueda", que es una lista de ejecución de los elementos solicitados. Por ejemplo, la solicitud podría proporcionar pistas sobre "búsqueda de pornografía infantil".

Para cada pista de la búsqueda, los examinadores extraen los datos relevantes y marcan dicha pista de la búsqueda como procesado. Además, agregan cualquier cosa extraída a una segunda lista llamada "Lista de Datos Extraídos". Los examinadores persiguen todas las pistas de búsqueda, añadiendo resultados a esta segunda lista. Luego pasan a la siguiente fase de la metodología, la identificación.

3.1.2 Identificación de los parámetros

Durante el proceso de identificación, los investigadores repiten el proceso de identificación de cada artículo en la lista de datos extraídos. Primero determinan el tipo de artículo y si es o no relevante para la solicitud forense, donde es marcada como procesada y se mueve a la siguiente evidencia. Si un examen comprueba que el artículo es incriminante, pero está fuera del alcance del mandato de búsqueda original, se recomienda detener la actividad de manera inmediata y proceder a notificar a las personas apropiadas. Un ejemplo en esta situación la policía podría tomar una computadora por evidencia de fraude fiscal, pero el investigador encuentra pistas de pornografía infantil. En esta situación lo más prudente es detener la búsqueda y obtener una segunda orden que permita ampliar la búsqueda.

Si un artículo es relevante para la solicitud forense, los investigadores proceden a documentar en una tercera lista denominada Lista de Datos Relevantes. Esta lista es una colección de datos relevantes para responder a la solicitud forense original. Por ejemplo, en un caso de robo de identidad, los datos pertinentes pueden incluir números de seguridad social, imágenes de falsa identificación, *emails* sobre el robo de identidad, etc. También es posible que un elemento genere otra pista de búsqueda. Un *mail* podría revelar que un objetivo estaba usando otro apodo. Eso conduciría a una nueva búsqueda de palabras clave para el nuevo apodo. Los investigadores deberían añadir la pista a la Lista de pistas de Búsqueda para que pudieran remitir e investigarlo completamente.

Si los datos simples extraídos e identificados no son suficientes, los examinadores pasan a la siguiente fase, el análisis.

3.1.2 Análisis de los datos a investigar

Para lograr que los investigadores unan los puntos y obtengan una imagen completa para el solicitante. Por cada elemento de la lista de datos relevantes los investigadores deben responder preguntas como: ¿Quién?, ¿Qué?, ¿Cuándo?, ¿Dónde? y ¿Cómo? Tratando de explicar qué usuario o aplicación creó, editó, recibió o envió cada elemento y cómo se originó la existencia.

Los investigadores producen el análisis más valioso al observar cuándo sucedieron las cosas y producir una línea temporal que cuenta una historia coherente.

El análisis es documentado y cualquier información pertinente a la solicitud forense en la última lista “Lista de resultados de análisis”. Esta es una lista de todos los datos significativos que responde: quién, qué, cuándo, dónde, cómo y otras preguntas. La información en esta lista satisface la solicitud forense. Incluso en esta última etapa del proceso, cualquier cosa podría generar nuevos datos de búsqueda o una fuente de datos.

Fase de presentación de informes. En esta fase los investigadores documentan los resultados para que el solicitante pueda entenderlos y utilizarlos en el caso.

Los informes forenses son importantes porque todo el proceso forense vale tanto como la información que transmiten los investigadores al solicitante. Después de la presentación de informes, el solicitante realiza un análisis en el que interpreta los hallazgos en el contexto de todo el caso.

4. Forensía móvil

Es un nuevo tipo de recopilación de pruebas digital, basado en la extracción de pruebas desde el interior de la memoria de un teléfono móvil, cuando existe la capacidad de acceder a los datos [8].

En forensía de dispositivos móviles, nos ocupamos de al menos tres principales sistemas operativos *standard*, así como varios otros propietarios, que no necesariamente son "Imagen" de un dispositivo móvil como lo hacemos a un disco duro.

Los dispositivos de destino son "encendido" en lugar de "apagado". Es común, sin embargo, al oír a un investigador de informática forense, decir que forensía de dispositivos móviles no son, "real forensía" porque no hacemos una imagen en el teléfono de la misma manera que una imagen de disco duro.

4.1 Realidad móvil

- Los teléfonos inteligentes se han convertido en parte esencial para nuestra vida diaria.
- Se utilizan como una oficina móvil o centro de entretenimiento.
- Se han hecho susceptibles a las mismas y mayores vulnerabilidades que las PC.
- Los datos en los teléfonos inteligentes, tales como imágenes, documentos, correos electrónicos, videos y mensajes cortos (SMS) se puede acceder de forma remota si el dispositivo está conectado a Internet.
- Hay muchas aplicaciones que pueden ejecutarse en un teléfono inteligente y más se desarrollan todos los días.
- Teniendo en cuenta la variedad de vendedores, aplicaciones móviles y protocolos de red, la tarea de análisis forense en los teléfonos móviles es cada vez un reto.

4.2 Adquisición

En forensía digital la adquisición consiste en crear un archivo que contenga toda la información contenida en la evidencia original. En la tabla 1, se muestra la evidencia más relevante en *smartphones* según el SANS.

Tabla 1. Evidencias relevantes según el SANS [6]

Lógica	Archivos del Sistema	Física	Manual
Incluye información activa a partir de datos almacenados.	Incluye archivos, activos y carpetas de sistema de archivos.	Incluye data activa y borrada.	El examinador se desplaza a través de los archivos contenidos en el dispositivo.
Cuenta con el apoyo de la mayor parte dispositivos de casi todas las herramientas.	Puede contener restos de objetos eliminados.	Absoluto vs. Registros.	Las fotografías o video de datos mostrados.
Reporte sencillo.	Cuenta con el apoyo de la mayor parte dispositivos de casi todas las herramientas.	No es compatible con todos los dispositivos.	Soporte para todos los dispositivos a no ser que este dañado físicamente.
	Generación de informes puede ser más complejo	Los informes son generalmente más complejos.	Generación de informes simple.

4.3 Medios de almacenamiento

En relación con las implicaciones de las evidencias relevantes podemos mencionar los medios de almacenamiento de información en los sistemas operativos Android [9]:

- **SIM:** Significa (Suscriber Identity Module) y es componente esencial de un celular GSM (Global System Mobile Comunications) que contiene información particular al usuario. Contiene típicamente entre 16 y 64 KB de memoria, un procesador, y un sistema operativo. Un SIM identifica de forma exclusiva el abonado, determina el número de teléfono, y contiene los algoritmos necesarios para autenticar un abonado a una red.
  El sistema de archivos se utiliza para almacenar los nombres y números de teléfono, recibe y envía mensajes de textos e información de configuración de red.
- **Memoria del dispositivo:** Contiene la data creada y almacenada por el usuario, MMS, mensajes de textos, fotografías, media, además del sistema operativo del *smartphone*.
- **Tarjeta micro SD:** Permite extender la capacidad de almacenamiento de un teléfono celular. También proporcionan otra vía para el intercambio de información entre los usuarios que tienen *hardware* compatible.
  Los medios extraíbles son de almacenamiento no volátil, capaz de retener datos grabados cuando se extraen de un dispositivo.

4.4 Tipo de información

Los diversos tipos de información que encontramos dependiendo del cuadro de evidencias relevantes en sistemas operativos Androids, se presentan a continuación en la tabla 2.

Tabla 2. Evidencias Relevantes [8]

Evidencias	
Text messages (SMS/MMS)	*Search history*
Contacts	*Driving directions*
Call logs	*Facebook, Twitter, and other social media clients*
E-mail messages (Gmail, Yahoo, Exchange)	*Files stored on the device*
Instant Messenger/Chat	*Music collections*
GPS coordinates	*Calendar appointments*
Photos/Videos	*Financial information*
Web history	*Financial information*
Shopping history	*File sharing*

4.5 Artefactos en dispositivos móviles

El término artefacto es ampliamente utilizado en la informática forense, aunque no existe una definición oficial de este término.

En situaciones cuando se efectúa un análisis forense y no encuentra evidencias tienen que buscar rastros que dejan las aplicaciones o el propio sistema operativo. Los mecanismos que dejan rastro de la actividad de los usuarios, de los programas que se utilizan, los accesos, conexiones y aplicaciones, si han navegado, descargado o ejecutado algún programa, son los comúnmente denominados como artefactos [10].

Algunos de los artefactos de más relevancia en sistemas operativos Androids, podemos observarlo en la tabla 3, son los siguientes:

Tabla 3. Artefactos relevantes según el SANS [6]

Partición	**Archivos**	**Tablas**	**Descripción**
Data	*Root/Property/persist.sys.timezone*	*	Timezone
Data	*Root/Property/netpolicy.xml*	*	Timezone
Data	com.android.providers.contacts/contacts2.db	llamadas	Llamadas Logs
Data	com.android.providers.contacts/contacts2.db	Cuentas	Login info
Data	com.android.providers.contacts/contacts2.db	contactos & raw contacts	Contactos
Data	com.android.providers.telephony/mmssms.db	sms & part	SMS/MMS
Data	com.google .android.apps.maps/da_destination_history	Historial de destino	Mapas
Data	com.google.android.apps.maps/search_history.db	Historial y sugerencias	Mapas
Data	com.android.email/webviewCache.db	*0	Historial de Internet

Data	com.android.browser/databases/Browser.db	*	Historial de Internet
Data	com.android.browser/databases/webview.db	*	Historial de Internet
Data	com.android.browser/databases/webviewCache.db	*	Historial de Internet
Data	com.android.browser/app_databases/http_www.google.com_0.localstorage	*	Historial de Internet
Data	com.android.browser/app_geolocation/GeolocationPermissions.db	*	Historial de Internet
Data	/data/com.google.android.gm/databases/<mail-name>.db	conversations & messages	Gmail

4.6 Herramientas *software* para Forensía Digital Móvil

En relación con las herramientas para la adquisición de evidencia digital, mencionaremos algunas de las herramientas más utilizadas para realizar la extracción de dicha evidencia:

- **UFED Cellebrite:** es una extensa y reconocida herramienta forense utilizada en más de 60 países. El mecanismo de autodetección del *software* proporciona una guía paso a paso para el proceso de extracción, los dispositivos que se encuentran dentro del listado de soporte. Para los dispositivos móviles no listados, UFED ha desarrollado un perfil genérico para proporcionar soporte [11] y podemos ver la interfaz de la herramienta en la figura 3.

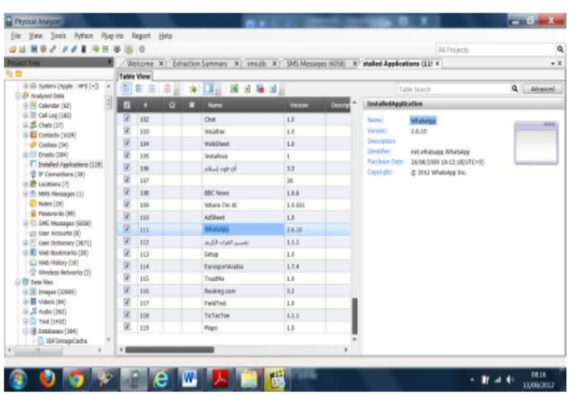

Figura 3. Análisis de aplicación instalada con UFED Cellebrite [8].

- **Oxygen Forensic Suite:** Oxygen Forensic es un *software* forense para la extracción y análisis de datos de teléfonos celulares, teléfonos inteligentes y *tablets*. Usando protocolos propietarios que permiten la extracción de artefactos, datos relevantes y garantiza un funcionamiento de *footprint* cero, sin dejar rastros y sin hacer modificaciones en el contenido del dispositivo. El *software* se distribuye a la policía, los organismos gubernamentales, militares, investigadores privados y otros especialistas forenses [1], la interfaz de la herramienta se puede observar en la figura 4.

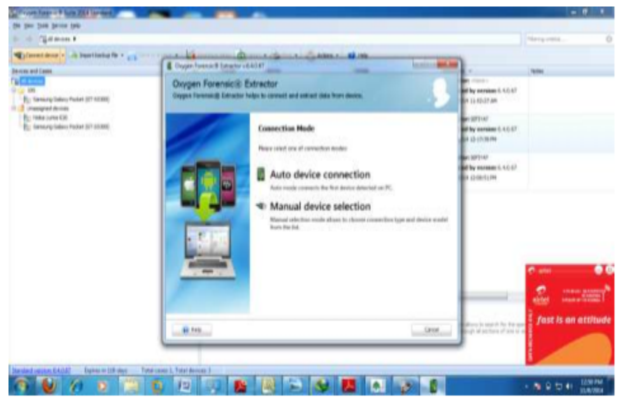

Figura 4. *Oxygen forensic display* [1].

- **MOBILedit:** es una herramienta para extracción y análisis de datos en dispositivos móviles, además es un generador de informes en una sola solución. Utiliza tanto los métodos de adquisición de datos físicos como lógicos, recuperación de datos eliminados, procesamiento simultáneo de teléfonos. Permite acceder a las copias de seguridad bloqueadas de ADB o iTunes con aceleración de GPU y operaciones multihilo para la máxima velocidad, para ello necesita de la contraseña y el código PIN [1]. En la figura 5 vemos la interfaz para el análisis, dependiendo del tipo de sistema operativo móvil.

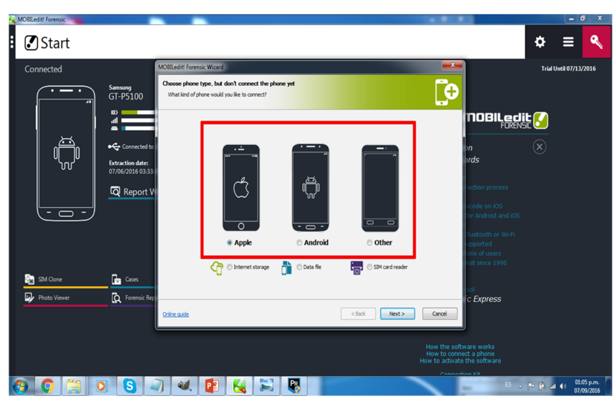

Figura 5. MOBILedit selección del dispositivo: Fuente propia.

- **Santoku:** Sistema operativo Linux basado en Debian, especializado en análisis forense móvil. Podemos observar la interfaz del sistema operativo en la figura 6.

Figura 6. Santoku instalado en una máquina virtual: Fuente propia.

Dentro de esta distribución encontramos una herramienta llamada “aflogical-ose”, que abre el *shell* de Santoku con opciones de ejecución de AFLogical, para ellos debemos tener el dispositivo móvil por analizar, conectado al PC por USB y habilitar el modo programador y transferencia por USB en el dispositivo móvil, ver figura 7.

El comando ejecutado crea una aplicación y la manda al dispositivo móvil para que esta sea ejecutada y pueda colectar la información del dispositivo como apreciamos en la figura 7.

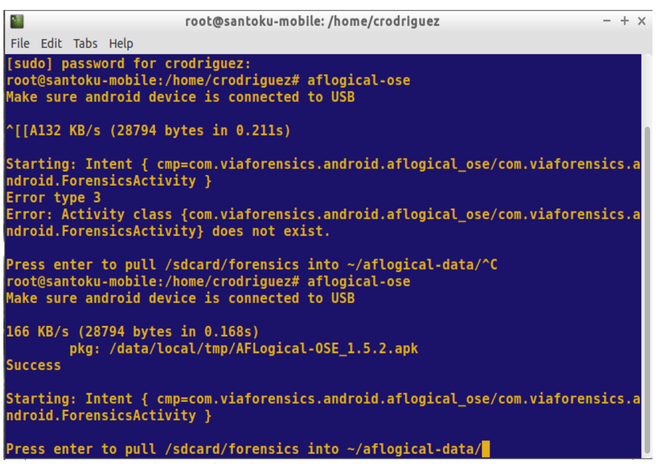

Figura 7. Aflogical generando la aplicación: Fuente propia.

Luego, la herramienta recolecta la evidencia y crea el folder y los archivos de la data colectada por el AFLogical, observamos este procedimiento en la figura 8.

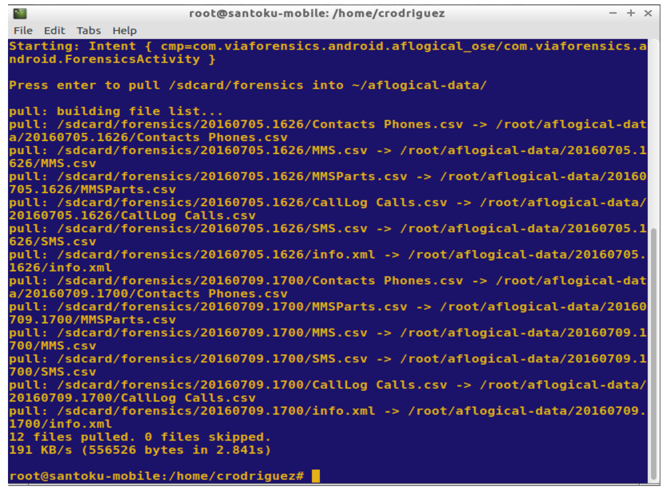

Figura 8. Aflogical recolectando información: Fuente propia.

5. Técnicas antiforensía

Definimos antiforensía como un método iniciado con la finalidad de impedir el proceso de investigación digital llevado por los investigadores forenses [12].

5.1 Clasificación de técnicas antiforensía

De lo anteriormente expuesto podemos clasificar la antiforensía entre métodos y técnicas que se agrupa en las siguientes categorías:

- **Ocultar datos:** una de las maneras de ocultar datos más habituales en las técnicas antiforensía es la esteganografía [13].

  La esteganografía (del griego *στεγανος* (*steganos*): cubierto u oculto, y *γραφος* (*graphos*): escritura), trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia [14].

  Existen programas de esteganografía desde la década de los 90, además de dichas herramientas la podemos encontrar para todos los sistemas operativos.

  Podemos encubrir información digital y almacenarla dentro de diversos tipos de archivos que incluyen audio, video, imágenes y ejecutables.

  En consecuencia, podemos encontrar métodos de esteganografía de baja tecnología que dificultan la informática forense. Un ejemplo de esto viene siendo ocultar texto blanco sobre un documento con fondo blanco con un mensaje oculto. Mensajes de código morse transpuestos sobre una imagen.

  Sin duda este tipo de tecnologías de esteganografía de bajo nivel son improbables que sean detectadas por alguna herramienta automatizada. Existen un sin número de técnicas para ocultar, por ejemplo, datos almacenados en espacios no asignados por el disco y metadatos de varios tipos de archivos.

- **Limpieza de artefactos:** con referencia a las herramientas para limpiar artefactos han existido por muchos años. Los programas de limpieza de artefactos eliminan archivos de datos y usan múltiples sobre escrituras, evitando que pueda realizarse la recuperación o sea prácticamente imposible. Estas herramientas son usadas comúnmente para la recuperación de espacio de almacenamiento eliminando archivos temporales innecesarios que fragmentan el disco duro. Otras herramientas de *software* más avanzadas no solo eliminan el historial de navegación, además borran archivos de caché, archivos del sistema operativo [15]. Tales como las siguientes:
    1. *BC Wipe*
    2. *Erarser*
    3. *PGP Wipe*
    4. *Evidence Eliminator*
    5. *Secure Clean*
    6. *Windowd Washer*
- **Ofuscación de registros:** la ofuscación se refiere a encubrir el significado de una comunicación haciéndola más confusa y complicada de interpretar.

    La ofuscación de los rastros ha sido un problema desde la década de los 70 con programas maliciosos enmascarado como el inicio de sesión denominado *Logon Spoofing (suplantación de inició de sesión)*. La propagación de ataques de denegación de servicios y denegación de servicios distribuidos da inicio a partir del año 96, han hecho la intrusión a redes más difícil de investigar a pesar de que existen métodos para el rastreo de los *ip* a la fuente que inicia el ataque. El programa conocido como *Onion Rounting*, que permite sistemas de comunicaciones anónimas, usa técnicas donde los mensajes son encapsulados en capas de cifrado, por eso la analogía de una cebolla (*onion*). Los datos cifrados son transmitidos a través de una serie de nodos de red llamados *onion routers*, cada nodo despoja una sola capa, descubriendo el siguiente destino. Cuando la capa final es descifrada, el mensaje llega a su destino. El remitente permanece anónimo debido a que cada intermediario conoce únicamente la ubicación del nodo siguiente. Está tecnología ha hecho casi imposible que se pueda hacer un análisis de trafico de red.
- **Ataques contra herramientas de forensía digital:** los procedimientos anti forenses se enfocan en atacar la confiabilidad de la evidencia digital, si cabe alguna duda en la confiabilidad que pueda ser cuestionada, el valor en la corte se vuelve nulo.

    Según los autores G. C. Kessler and G. C. Kessler,[12] la admisibilidad de la evidencia científica consta de cuatro factores:

    1. **Pruebas:** puede y ha sido probado el procedimiento.
    2. **Taza de error:** existe una taza de error conocida del procedimiento.
    3. **Publicaciones:** ¿se ha publicado el procedimiento y está sujeto a revisión por pares?
    4. **Aceptación:** ¿se acepta generalmente el procedimiento en la comunidad científica pertinente?

6. Hardware antiforensía

Existen herramientas como el USB Killer que explota la vulnerabilidad de sobretensión de alimentación en un USB, falla común en los dispositivos con conexiones USB. Muchos fabricantes para ahorrar gastos no protegen la energía o las líneas de datos de los dispositivos, lo que los deja abiertos a dicho ataque.

Cuando se conecta a un dispositivo, el USB Killer carga rápidamente sus condensadores desde las líneas de alimentación USB. Cuando se carga, -200VDC se descarga sobre las líneas de datos del dispositivo *host*. Este ciclo de carga y descarga se repite muchas veces por segundo, hasta que el USB Killer es removido.

6.1 *Software* antiForensía

Estas herramientas utilizan un mecanismo denominado *kill switch*, el cual apaga el dispositivo de manera abrupta, también puede ser una función de un host que deshabilita una aplicación o dispositivo de manera remota. Algunas de las herramientas más utilizadas según[12]:

- ***USBkill*:** herramienta antiforensía que espera un cambio en los puertos USB para entonces apagar de manera inmediata la computadora.
- ***Silk-gurdian*:** de igual manera que la herramienta anterior, esta espera un cambio en los puertos USB para limpiar la *ram*, borrar archivos y apagar la computadora.

6.2 MAFIA (Metasploit Anti-Forensics Project)

Cuya principal finalidad es desarrollar herramientas y técnicas para remover evidencia forense de las computadoras. Está compuesto de diversas herramientas como:

Timestomp: que permite remover o modificar las fechas de acceso, modificación, creación de los archivos. Podemos observar la ayuda del *framework* en consola en la figura 12.

```
C:\>timestomp.exe

TimeStomp Usage Information:
---------------------------------------------------------
If you mix a lot of options, the behavior is unpredictable. All times
should be entered in local time because the utility automatically
converts to UTC time.

TimeStomp <filename> [options]

        <filename>      the name of the file you wish to modify
                        you may need to surround the full path in ""
options:

        -m <date>       M, set the "last written" time of the file
        -a <date>       A, set the "last accessed" time of the file
        -c <date>       C, set the "created" time of the file
        -e <date>       E, set the "mft entry modified" time of the file
        -z <date>       set all four attributes (MACE) of the file

        <date>          "DayofWeek Month\Day\Year HH:MM:SS [AM|PM]"

        -f <src file>   set MACE of <filename> equal to MACE of <src file>
                        time stamps change, but file attributes are unchanged
        -b              set the MACE timestamps so that EnCase shows blanks
        -r              same as -b except it works recursively on a directory
                        (aka the Craig option)
        -v              show the UTC (non-local time) MACE values for <filename>

        -h              show this menu, help

examples:

1) sets the "last written" attribute of targetfile.txt

       TimeStomp targetfile.txt -m "Monday 7/25/2005 5:15:55 AM"

2) sets all four MACE attributes of targetfile.txt

       TimeStomp targetfile.txt -z "Saturday 10/08/2005 2:34:56 PM"

3) set the MACE attributes of targetfile.txt equal to srcfile.exe

       TimeStomp targetfiletxt -f srcfile.exe

4) set the MACE attributes of targetfile.txt equal to values that EnCase
   doesn't know how to display

       TimeStomp targetfile.txt -b

5) show the MACE attributes of targetfile.txt

       TimeStomp targetfile.txt -v
```

Figura 9. Herramienta *Timestomp*. Fuente Propia

- ***Slacker*****:** permite ocultar datos en el espacio desperdiciado, creado cuando un sistema de archivos define el espacio útil para la escritura de un fichero, normalmente se define más espacio de almacenamiento del necesario. La figura 13 muestra la ayuda de la herramienta slacker.

```
C:\>slacker.exe

Hiding a file in slack space:
------------------------------
slacker.exe -s <file> <path> <levels> <metadata> [password] [-dxi] [-n|-k|-f <xorfile>]
-s                      store a file in slack space
<file>                  file to be hidden
<path>                  root directory in which to search for slack space
<levels>                depth of subdirectories to search for slack space
<metadata>              file containing slack space tracking information
[password]              passphrase used to encrypt the metadata file
-dxi                    dumb, random, or intelligent slack space selection
-nkf                    none, random key, or file based data obfusaction
<xorfile>               the file whose contents will be used as the xor key


Restoring a file from slack space:
-----------------------------------
slacker.exe -r <metadata> [password] [-o outfile]

-r                      restore a file from slack space
<metadata>              file containing slack space tracking information
[password]              passphrase used to decrypt the metadata file
[-o outfile]            output file, else original location is used, no clobber
```

Figura 10. Herramienta Slacker. Fuente Propia

- ***Sam juicer*****:** un programa que adquiere los *hashes* del Security Access Manager sin manipular el disco duro.

7. Conclusiones

En nuestra sociedad utilizamos varios dispositivos electrónicos como celulares, dispositivos vestibles, dispositivos móviles en múltiples aspectos de nuestras vidas. Pero no somos los únicos que utilizamos dispositivos electrónicos también los cibercriminales que los utilizan con fines delictivos. La tecnología actual permite a los cibercriminales cometer actos delictivos de manera local e internacional y remota, obtener inteligencia y realizar contra espionaje con anonimidad. Como tal estos dispositivos almacenan datos que funcionan como evidencia de sus crímenes y pueden proveer informaciones en los sospechosos o víctimas.

En síntesis, el artículo presentado responde a la necesidad en Panamá de contar con un apoyo para el manejo de evidencias digitales con las mejores prácticas de parte de organismos internacionales como la OEA, el departamento de justicia de los Estados Unidos e instituciones de seguridad reconocidas a nivel mundial como el SANS.

Los procedimientos, herramientas y metodologías para las investigaciones de incidentes de seguridad informática o dispositivos con sistemas operativos embebidos son los mismos empleados en ambos casos, en el caso de los dispositivos de embebidos dado las limitantes en sus tecnología al ser dispositivos que son usados para una única función en la mayoría de los casos, por lo que el desarrollo de sus especificaciones técnicas y diseño de los mismos, son usados como nodos sensores que envían datos a otros nodos con mayor capacidad de computación, que analizan la data enviadas por los nodos sensores y, son estos equipos con mayor capacidad donde podemos realizar un análisis forense digital al sistema operativo que estén utilizando.

9. Referencias

[1] O. Osho and S. O. Ohida, “Comparative Evaluation of Mobile Forensic Tools,” I.J. Inf. Technol. Comput. Sci. Inf. Technol. Comput. Sci., vol. 1, no. 1, pp. 74–83, 2016.

[2] D. A. J. ARCINIEGAS and M. L. T. MONCADA, “Estado Del Analisis Forense Digital En Colombia,” 2016.

[3] J. P. Craiger and D. Ph, “DRAFT : NOT FOR DISTRIBUTION Computer Forensics Procedures and Methods DRAFT : NOT FOR DISTRIBUTION,” pp. 1–65.

[4] J. CANO, “Admisibilidad de la evidencia digital: de los conceptos legales a las características técnicas,” Boletín los Sist. Nac. Estadístico y …, pp. 93–108, 2003.

[5] D. Yadav, M. Mishra, and S. Prakash, “Mobile forensics challenges and admissibility of electronic evidences in India,” Proc. - 5th Int. Conf. Comput. Intell. Commun. Networks, CICN 2013, pp. 237–242, 2013.

[6] C. Murphy, “Advanced Smartphone Forensics Most Relevant Evidence Per GIGABYTE!,” POSTER SANS DFIR, vol. 30th Editi.

[7] B. O. L. Carroll, S. K. Brannon, and T. Song, “Computer Forensics : Digital Forensic Analysis Methodology,” Computer (Long. Beach. Calif)., vol. 56, no. 1, pp. 1–8, 2008.
[8] M. Al-hadadi and A. AlShidhani, “Smartphone Forensics Analysis: A Case Study,” Int. J. Comput. Electr. Eng., vol. 5, no. 6, pp. 576–580, 2013.
[9] W. Jansen and R. Ayers, “Forensic Tools for Mobile Phone Subscriber Identity Modules,” J. Digit. Forensics, Secur. Law, vol. 1, no. 2, pp. 75–94, 2006.
[10] C. Altheide and H. a Carvey, Digital forensics with open source tools using open source platform tools for performing computer forensics on target systems: Windows, Mac, Linux, UNIX, etc. 2011.
[11] J. Kong, “Data Extraction on Mtk-Based Android Mobile Phone Forensics,” vol. 10N4, no. 4, pp. 31–42, 2015.
[12] G. C. Kessler and G. C. Kessler, “Anti-Forensics and the Digital Investigator,” 2007.
[13] S. Azadegan, W. Yu, H. Liu, M. Sistani, and S. Acharya, “Novel anti-forensics approaches for smart phones,” Proc. Annu. Hawaii Int. Conf. Syst. Sci., pp. 5424–5431, 2011.
[14] G. C. Kessler, “An Overview of Steganography for the Computer Forensics Examiner,” pp. 1–29, 2016.
[15] S. M. A. Asbeh and S. M. Hammoudeh, “AES Inspired Hex Symbols Steganography for Anti- Forensic Artifacts on Android Devices,” vol. 7, no. 5, pp. 319–327, 2016.
[16] Y. Bai, L. Dai, and J. Li, “Issues and Challenges in Securing eHealth Systems,” Int. J. E-Health Med. Commun., vol. 5, no. 1, pp. 1–19, 2014.
[17] X. Li, M. H. Ibrahim, S. Kumari, and R. Kumar, “Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors,” Telecommun. Syst., pp. 1–26, 2017.
[18] M. Ahmed and M. Ahamad, “Combating abuse of health data in the age of eHealth Exchange,” Proc. - 2014 IEEE Int. Conf. Healthc. Informatics, ICHI 2014, pp. 109–118, 2014.