COMPDES 2014
UNAN-Managua

Benchmarking de Herramientas Forenses para Móviles

Autores
Elmer Arturo Carballo Ruiz
Pedro Eliseo Peñate.

Tabla de Contenido

INTRODUCCIÓN

Actualmente, y cada día con más importancia, los dispositivos móviles (Smartphones y tablets) se han convertido en una herramienta indispensable en las labores diarias tanto a nivel corporativo y personal. Estos dispositivos no solo son capaces de almacenar información referente a la agenda de contactos o reproductor de música y vídeo, sino que son capaces de almacenar una gran cantidad de información que puede resultar ser muy útil en un caso de la informática forense. Nos enfrentamos a grades desafíos como es BYOD (Bring of your device) está política está haciendo grandes cambios en el mundo de los negocios ya que alrededor de un 90% de los empleados (en los países desarrollados) utilizan sus equipos de algún modo para acceder a la información de la empresa. En la mayoría de los casos las empresas no pueden cambiar esta tendencia. Algunos creen que BYOD ayuda a los empleados a ser más productivos otros creen que eleva la moral de los empleados ya que se permite la flexibilidad dentro de la empresa, pero otro punto de vista es que esto vuelve frágil la Seguridad de la Información y puede vulnerarse la seguridad a través de estos dispositivos.

En este proyecto se ha realizado la evaluación de dos suites que poseen diferentes herramientas forenses para dispositivos móviles y una herramienta especializada en extracción de datos, para ello se presenta una breve descripción de la arquitectura de los móviles Android, una breve descripción de las herramientas evaluadas, metodología utilizada para la realización del benchmarking, exponiendo los criterios utilizados para posteriormente presentar el análisis de los resultados obtenidos y algunas recomendaciones que son de mucha importancia para este estudio.

OBJETIVOS

Objetivo General

Comparar tres herramientas para el uso de un análisis forense informático en tecnologías móviles

Objetivos Específicos

Investigar herramientas a nivel de open source para el análisis forense de dispositivos móviles.

Establecer una comparación en base a criterios técnicos sobre las herramientas forenses para móviles.

ALCANCE Y LIMITACIONES

Alcance

Este estudio estaría basado sólo en el uso de herramientas forenses open source para dispositivos móviles sobre plataforma Android, y lo que se pretende es brindar una comparación de las ventajas y desventajas entre ellas y su aplicabilidad en el análisis forense.

Limitaciones

El proyecto se ha delimitado a la extracción de datos de dispositivos Android con herramientas Open Source de Adquisición Lógica.

Una herramienta de adquisición requiere que la versión de Android sea desde la 1.5 hasta la 4.1 en el caso de la otra herramienta evaluada la versión de Android requerida es 2.x.

La efectividad de las extracciones depende mucho de la versión de Android que el dispositivo analizado tenga instalado.

MARCO TEORICO

Dispositivos Móviles

El primer dispositivo móvil celular, reconocido como “celular” en nuestro medio; fue demostrado por Motorola en 1973. Comercialmente la red de Telefonía Celular fue lanzada en Japón por NTT desde 1979 y ha venido evolucionando desde esta fecha hasta ahora, comenzando por la primera generación donde se utilizaba tecnología análoga, pasando por una segunda generación con tecnología

digital hasta ahora donde ya se encuentra la tercera y cuarta generación con la que se puede contar con velocidades de transmisión de hasta 100Mbps para usuarios móviles en algunas tecnología como LTE.

La cosumerización en conjunto con la evolución de las tecnologías de telefonía celular ha permitido que el uso de los teléfonos celulares y dispositivos móviles no sea limitado a llamadas y mensajes de texto. Ahora se pueden realizar descargas de contenido web, envío de correos, descargas de video o contenido de media streaming e incluso transacciones bancarias.

Esto ha expandido una demanda de consumo de dispositivos móviles en los que muchos fabricantes han posicionado sus marcas tomando buena parte de este mercado. Entre las 5 marcas mayormente comercializadas a finales del 2012 se encuentran: Samsung, Nokia y Apple. Aun así aproximadamente el 40% de los fabricantes son variados y generalmente utilizan sistemas operativos de código abierto para poder administrar dichos dispositivos.

Top Five Worldwide Total Mobile Phone Vendors, Q4 2012			
Rank	**Manufacturer**	**Gartner**[22]	**IDC**[23]
1	Samsung	22.7%	23.0%
2	Nokia	18.0%	17.9%
3	Apple	9.2%	9.9%
4	ZTE	3.4%	3.6%
5	LG	3.2%	-
5	Huawei	-	3.3%
	Others	43.5%	42.3%

Tabla 1. Top Five Worldwide Total Mobile Phone Vendors (Wikipedia The Free Encyclopedia, 2014)

En base a esto se considera que uno de los sistemas operativos mayormente utilizados para los dispositivos móviles es el Sistema Operativo Android, tomando el mejor posicionamiento en este mercado.

Herramientas Forenses

SANTOKU

El nombre de Santoku, se traduce libremente como “tres virtudes” o “tres usos” (Santoku) y es un homenaje a un cuchillo japonés multiuso. Santoku está dedicado a los forenses móviles, análisis y seguridad empaquetados en un formato fácil de usar en una plataforma de código abierto.

Santoku es una distribución Linux basada en OWASP’s MobiSec especializada en pruebas de seguridad, análisis de malware y análisis forenses para teléfonos móviles, válida para dispositivos con Android, BlackBerry, iOS y Windows Phone (Motos, 2012).

Este kit de herramientas tiene muchas utilidades, entre las cuales podemos encontrar (Santoku): Herramientas de desarrollo, Analizadores Wireless, Ingeniería inversa, Herramientas Forenses, Pruebas de Penetración.

De todas estas características las que nos interesan son las herramientas orientadas a análisis forense para adquirir y analizar datos de los móviles, la herramienta es llamada AFLogical.

ADEL

ADEL que se entiende como una abreviatura de “ **Android Data Extractor Lite** ” (Blogtecnico.net, 2014). ADEL fue desarrollado para las versiones 2.x de Android y es capaz de volcar automáticamente los archivos de bases de datos SQLite seleccionados de

dispositivos Android y extraer los contenidos almacenados en los archivos objeto de dumping. El programa está desarrollado en Python (Lakhoua, 2013). ADEL interactúa con los dispositivos utilizando el Android Software Development Kit (SDK de Android) y especialmente el demonio adb para volcar los archivos de base de datos en el equipo del investigador.

Un diagrama de flujo que muestra la estructura de ADEL se muestra en la siguiente figura:

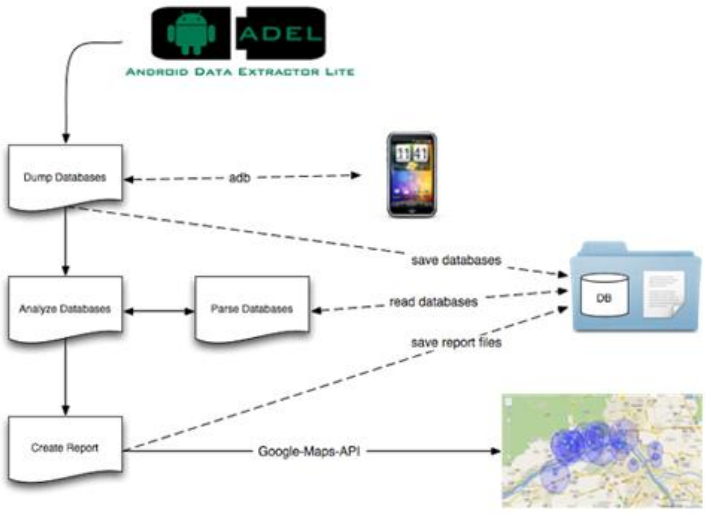


Figura 3. Estructura de ADEL (Forensic Blog)

Dentro de las características principales de esta herramienta se encuentran:

Principios forenses: ADEL está destinado a tratar los datos de manera correcta forense. Este objetivo se alcanza por el hecho de que las actividades no se realizan directamente en el teléfono, pero en una copia de las bases de datos. Este procedimiento asegura que los datos no se convierta en cambió, ni por los usuarios de ADEL ni por un sistema operativo no comprometido. Para la prueba de la exactitud forense de ADEL, valores hash se calcula antes y después de cada análisis, para garantizar que los datos sean objeto de dumping no se hicieron cambiar durante el análisis.

Facilidad de uso: El uso de la ADEL pretende ser lo más simple posible para permitir su uso tanto por personas calificadas y no expertos. En el mejor, el

análisis del teléfono móvil se lleva a cabo de forma autónoma de modo que el usuario no recibe ninguna notificación de los procesos internos. Por otra parte, el módulo de informes crea un informe detallado en un formato legible, incluyendo todos los datos decodificados. Durante la ejecución, ADEL escribe opcionalmente un archivo de registro amplio, donde se trazan todos los pasos importantes que se han ejecutado.

La herramienta consiste en dos módulos separados: un módulo para análisis y un módulo de informes y sus funcionalidades. La herramienta le permite al investigador la siguiente información:

- información telefónica y la tarjeta SIM (por ejemplo, IMSI y el número de serie)
- directorio telefónico y las listas de llamadas,
- entradas del calendario,
- Mensajes SMS,
- Ubicaciones GPS de diferentes fuentes en el smartphone.

Los datos recuperados de esta manera se escriben en un archivo XML mediante el módulo de informes con el fin de facilitar aún más el uso y la representación de los datos. A medida que el módulo de análisis, que puede ser fácilmente actualizado con respecto a posibles cambios en futuras versiones de Android o en los esquemas de bases de datos subyacentes.

OSAF

OSAF (Open Source Android Forensics) (OSAF Community, 2012) Es un proyecto de software libre para Análisis Forense de Androids, su objetivo fue crear un marco unificado para análisis forense de Androids centrándose principalmente en el malware dentro de las aplicaciones de Android. Su enfoque en primer lugar, la creación de una compilación fuente totalmente abierta de la ciencia forense y análisis de malware de software en la forma de Toolkit OSAF. En segundo lugar,

el objetivo era crear un proceso estandarizado para el uso del kit de herramientas y un conjunto de mejores prácticas para el análisis de las aplicaciones de Android.

OSAF-Toolkit fue desarrollado como un proyecto de diseño de alto nivel, por un grupo de estudiantes de TI de la Universidad de Cincinnati, con ganas de ser pioneros y allanar el camino para la normalización de los análisis de malware Android. La OSAF-Toolkit se construye a partir de Ubuntu 11.10 (skygear, 2012) y pre-compilado con todas las herramientas necesarias para destrozar las solicitudes de revisión de código y análisis de malware. El objetivo principal del kit de herramientas es para ser capaz de hacer análisis de aplicaciones lo más fácil posible.

En las suit Santoku y Osaf se tienen algunas herramientas en común, a continuación se presenta un listado de algunas herramientas que se tienen disponibles en estos kits.

Categoría	Herramientas en Santoku	Herramientas en OSAF
Herramientas de Desarrollo	Android SDK Manager	Android SDK incluye Android 2.3.3 API, Anroid SDK Tools, Android SDK Platform-tools, Extras package
	AXMLPrinter2	AndroGuard
	Fastboot	
	Heimdall (src | howto)	
	Heimdall (GUI) (src | howto)	
	SBF Flash	
Análisis Forense de Dispositivos	AFLogical Open Source Edition (src | howto)	AFlogical
	Android Brute Force Encryption (src | howto)	Sleuthkit
	ExifTool	Scalpel
	iPhone Backup Analyzer (GUI) (src | howto)	Exiftool
	libimobiledevice (src | howto)	
	scalpel	
	Sleuth Kit	

Pruebas de Penetración	Burp Suite	Firefox
	Ettercap	SQLite DB Browser
	Mercury	
	nmap	
	OWASP ZAP	
	SSL Strip	
	w3af (Console)	
	w3af (GUI)	
	Zenmap (As Root)	
Analisis de Wireless	Chaosreader	
	dnschef	
	DSniff	
	TCPDUMP	
	Wireshark	
	Wireshark (As Root)	
Ingeneria en Reversa	Androguard	
	Antilvl	
	APK Tool	
	Baksmali	
	Dex2Jar	
	Jasmin	
	JD-GUI	
	Mercury	
	Radare2	
	Smali	

Tabla 2. Algunas herramientas incluidas en cada Suite de Herramientas Open Source para informática forense en dispositivos móviles con sistema Android

AF Logica

AFLogical es una herramienta de extracción lógica para el análisis forense de Androids, fue lanzado en diciembre de 2011, desarrollado por viaForensics y ahora está alojado en GitHub.

AFLogical realiza una adquisición lógica de cualquier dispositivo Android con Android 1.5 o posterior. (ViaForensics, 2014) Los datos extraídos se guardan en la tarjeta SD del examinador en formato csv (valores separados por comas), que se puede importar fácilmente en un software de hoja de cálculo, por lo que es fácil de extraer y analizar los datos de Android. La aplicación proporciona un

marco básico para la extracción de datos de los dispositivos Android mediante proveedores de contenido, incluyendo (kswartz):

- Contactos
- Registro de llamadas
- SMS (Servicio de Mensajes Cortos)
- MMS (Mensajes Multimedia)
- MMS Parts
- Información del dispositivo

Esta herramienta puede encontrarse dentro de la suite de OSAF y SANTOKU.

Android Debug Bridge (ADB)

ADB es una herramienta de línea de comando muy versátil que permite la comunicación con una instancia de emulación o la conexión con un dispositivo soportado por el sistema operativo Android. (Android Developers) Se trata de un programa cliente-servidor que incluye tres componentes:

Cliente: Que se ejecuta en un equipo de desarrollo. Esta invoca un cliente desde un Shell ingresando un comando ADB. ADT plugin y DDMS también crean clientes ADB.

Servidor: Que se ejecuta como un proceso de segundo plano en el equipo de desarrollo. El servidor administra la comunicación entre el cliente y el "Daemon ADB" corriendo en el emulador o el dispositivo.

"Daemon": Que se ejecuta como un proceso de segundo plano la instancia de cada emulador o dispositivo.

Análisis forense en dispositivos móviles

El análisis forense en dispositivos móviles es relativamente una nueva área, y las herramientas que se pueden utilizar para dicho análisis todavía se encuentran en una etapa de inicio en su desarrollo. Las herramientas pueden ser

basadas en software o hardware, dependiendo de cómo la data se extrae del dispositivo. Adicionalmente la forma de extracción puede ser dividida cinco tipos, como lo explica Brother (Mobile Forensics World, 2012) Los primeros métodos de extracción son los métodos físicos que incluyen “Micro Read”, “Chip-off” y “Hex-Dump”. Los métodos de extracción físicos requieren mayor nivel de competencia técnica, pero tienen a favor que tienen mayor validez en términos forenses. Luego existe el método de extracción “lógica” y finalmente el método de extracción “manual”. En este caso, estos dos últimos, requieren de menor competencia técnica, pero pueden de una u otra manera perder validez en términos forenses.

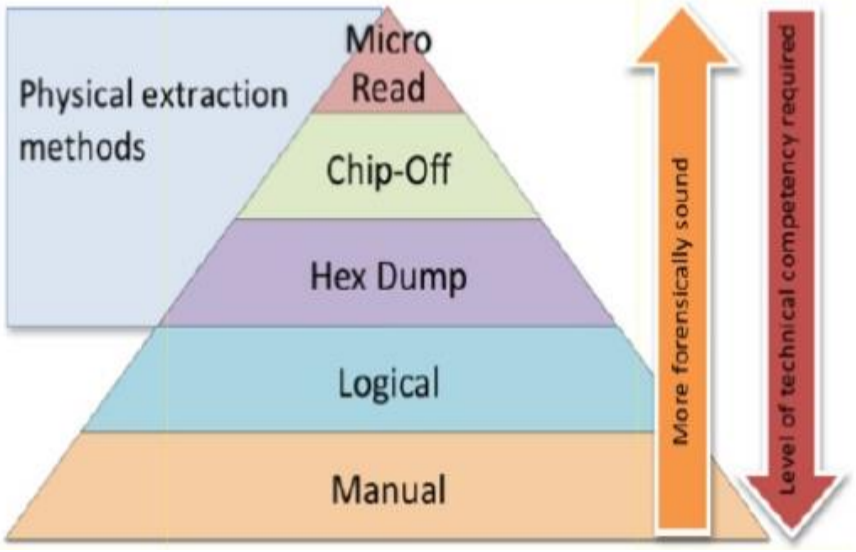


Figura 4. Pirámide de Herramienta de Análisis Forense (Mobile Forensics World, 2012).

Manual

El método de extracción manual, no es realmente muy utilizado en casos de análisis forenses, ya que por su simplicidad, puede fallar en la recuperación de data que puede resultar crítica en este tipo de análisis. Por ejemplo, en este caso, se podría omitir evidencia potencial tal como los archivos eliminados. Estos métodos son normalmente utilizados cuando el tiempo de adquisición es corto y la integridad de la data no es requerida.

Lógica

Por otro lado, el método de extracción “lógica” es ampliamente recomendado para la extracción de la data. En la mayoría de casos, esta técnica

requiere la copia de una pequeña aplicación de análisis forense de Android que luego puede ser removida sin impactar la integridad del dispositivo y su información. Este tipo de extracción es generalmente rápida, y no requiere de un alto nivel de experticia técnica. Aun así, en muchas ocasiones pierde validez forense para los analistas ya que se considera que pueden realizarse cambios en la data del dispositivo mientras se realiza el proceso de copiado de la herramienta.

Métodos de extracción física

Para estos caso, el método de extracción física, es el que se considera con mayor validez forense; ya que es en la práctica no existe ninguna alteración en los espacio de almacenamiento de la data.

HEX DUMP: requiere la carga de un bootloader para inicializar el dispositivo, lo que permite crear prácticamente una copia intacta del dispositivo. (Esto es similar a cargar una máquina desde un live boot CD).

“Chip-off”: es un técnica donde se remueven físicamente los dispositivos de almacenamiento (Chip NAND Flash) que son posteriormente analizados externamente. Esta técnica es normalmente utilizada cuando existe un daño físico en el dispositivo.

“Micro-Read”: es el que requiere de mayor experticia técnica, y utiliza un microscopio electrónico para ver el estado de la memoria del dispositivo. Este involucra un costo muy elevado y no es considerar un método estándar.

METODOLOGÍA DE EVALUACIÓN DE LAS HERRAMIENTAS SANTOKU, ADEL Y OSAF

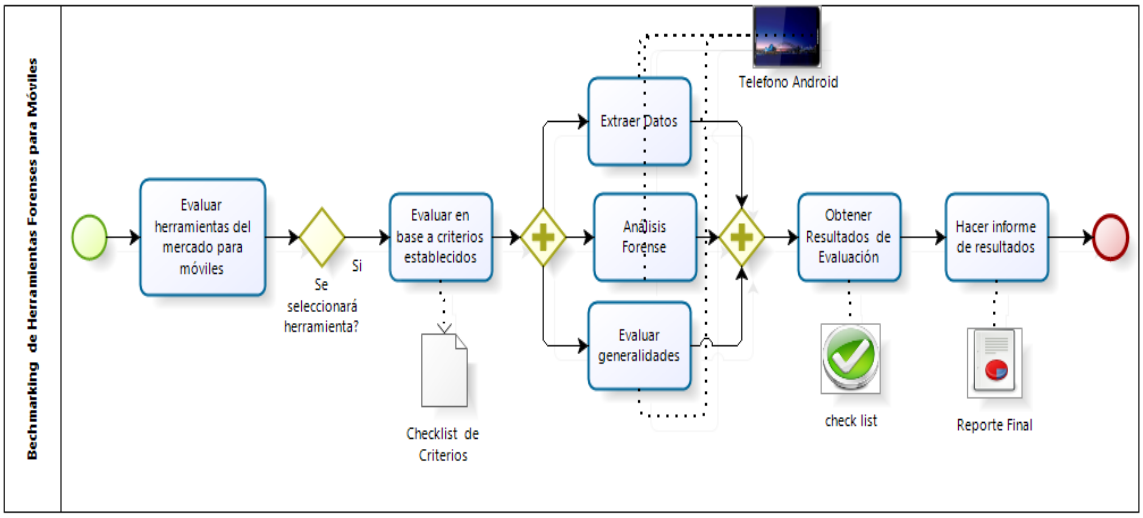
Metodología

El proceso de evaluación consiste en determinar a partir de una suite de herramientas que estén dedicadas al análisis forense sobre dispositivos móviles, el análisis y la seguridad, y se envasa en un formato fácil de usar, en una plataforma de código abierto. A partir de una investigación en internet, se seleccionará dos suites que poseen una diversidad de herramientas forenses para dispositivos móviles y una herramienta especializada en extracción de datos.

Posteriormente de la selección de tres herramientas para análisis forense se haga una evaluación en base a criterios de evaluación sobre ciertos procesos importantes como es la extracción de datos, la capacidad de análisis forense de los datos extraídos y la calidad de software en cuanto a la facilidad de uso, mantenimiento y operatividad entre otros. Los criterios serán evaluados en cada una de las categorías seleccionadas y se establecerá en un formato de tabla, un proceso de chequeo que si cumple cada uno de esos criterios, en algunos casos la evaluación es si cumple o no, y otros en qué nivel se logra realizar ese criterio, hemos ponderado en este último la forma de evaluación en tres niveles: Alta, Moderada y Baja.

Cada criterio será evaluado bajo un escenario con un dispositivo real Android, donde se demostrará en base a evidencias de imágenes cuando se esté ejecutando la herramienta si cumple el criterio. Adicionalmente se analizará los resultados de cada evidencia para verificar los resultados de las pruebas. Para una mejor comprensión del proceso ver figura 5.

Figura 5. Benchmarking de Herramientas Forenses para Móviles



Escenario

Para realizar el benchmarking se tomaran diferentes teléfonos celulares reales con sistema Android debido a que una de las herramientas es necesario que este en modo recovery y dentro del modo se puedan montar algunas carpetas principales del sistema de archivos de Android, para el caso OSAF y Santoku no es necesario que el dispositivo ingrese en modo recovery debido a que AFLogical se instala en sistema Android del dispositivo.

Especificación	Datos de Dispositivo 1	Datos de Dispositivo 2
Marca	Samsung	Samsung
Numero de Modelo	GT-I9190	GT-I9300
IMEI	357961052691724	354245057850151
Versión de android	4.2.2	4.1.2
Versión de banda base	I9190UBUAMG1	I9300UBELL1
Versión de kernel	3.4.0-1045871 se.infra@S0210-11 #1 Tue Jul 917:26:32 KST 2013	3.0.31-767276se.infra@SEI-75 #1 SMP PREEMPT Mon Dec 31 13:32:27 KST 2012
Numero de compilación	JDQ39.I9190UBUAMG1	JZO54K.I9300UBELL6
Modo Recovery	Soportado	Soportado
Montaje de Carpetas en Modo Recovery	No Soportado	Soportado
Depuración de USB	Habilitado	Habilitado
Evaluado en Herramienta	Santoku y OSAF	ADEL
Imagen de Dispositivo		

Tabla 3. Dispositivos Evaluados

Nombre de Herramienta	Versión	Función Principal	Android Soportado	Lenguaje de Desarrollo	Disponible en	Fabricante
AFLogical en Santoku	1.5.2_OSE	Extracción Lógica y Análisis	1.5 o superior	Java	Distribución de Linux Santoku y https://github.com/viaforensics/android-forensics	VIAFORENSICS
AFLogical en OSAF	1.5.2_OSE	Extracción Lógica y Análisis	1.5 o superior	Java	Distribución de Linux OSAF y https://github.com/viaforensics/android-forensics	VIAFORENSICS
ADEL	2	Extracción	2.X	Python	https://github.com/mspreitz/ADEL	Spreitzenbarth

		Lógica y Análisis				

Tabla 4. Herramientas para extracción y análisis

Nombre de Herramienta	Versión	Función Principal	Distribución Base	Características	Disponible en	Fabricante
Santoku	0.4	Suite de herramientas preinstaladas para informática móvil forense, análisis de malware y pruebas de seguridad	Ubuntu Linux ¿?	Herramientas de Desarrollo Pruebas de Penetración DeviceForensics Analizadores de WireLess Ingenieria en Reversa	https://santoku-linux.com	VIAFORENSICS
OSAF	RC2	Enfoque principal análisis de malware en Android y provisión de herramientas forenses para móviles	Lubuntu Linux ¿?	MobielForensics Análisis de Malware	http://osaf-community.org/home.html	Comunidad OSAF y Universidad de Cincinnati

Tabla 5. Suite de herramientas open source para informática forense en dispositivos móviles con sistema Android

Categorías de evaluación

Para este estudio los criterios de evaluación se han divido en diferentes categorías tales como:

- **Extracción de Datos**: Esta categoría se debe entender como la capacidad de extraer evidencia de datos o archivos digitales para que posteriormente sean analizados para el objetivo forense sobre el dispositivo móvil.
- **Análisis Forense**: Esta categoría se evalúa si el material adquirido sobre la herramienta tiene relevancia, que los procesos aplicables de las herramientas puedan ser auditadas, se posea bitácoras y que se pueda obtener información suficiente para ser analizada.
- **Generalidades**: Esta categoría contiene los criterios de calidad en cuento al software de las herramientas posean características que faciliten su uso, instalación, mantenibilidad, interoperable entre otros.

RESULTADOS

Para este estudio los criterios de evaluación se han divido en diferentes categorías tales como:

- Extracción de Datos: Evaluación de herramientas de extracción de Datos
- Análisis Forense: Evaluación de Suites de Herramientas basado en ISO / IEC 27037
- Generalidades: Evaluación de Suites de Herramientas basado en ISO/IEC 2500.

(Ver resultados en presentación de power point).

CONCLUSIONES

- Para poder elegir una herramienta de análisis forense es necesario tener bien definidas las necesidades para las que se va utilizar y los criterios que se busca evaluar, la mayoría de veces se utilizan dos o tres herramientas de análisis forense ya que de acuerdo a las necesidades de los casos que se presentan es necesario combinarlas.
- El análisis de forense de dispositivos móviles basado en sistema Android puede facilitarse o complicarse dependiendo de las características del dispositivo como si esta rooteado, si se pueda tener acceso a modos especiales como recovery, fastboot (carga de imagen de SO en RAM, las versiones del sistema Android, si el dispositivo está cifrado, si tiene seguridad de bloqueo de pantalla por PIN o patrón, etc. Para cada caso se debe de tener conocimiento de alguna herramienta que pueda apoyar al propósito de adquirir la información del sistema. Para el caso de las suites evaluadas existen varias herramientas que pueden servir al analista para lograr el objetivo de extraer, analizar y reportar la información de interés. Sobre esto la pericia, experiencia, comprensión del sistema Android del analista puede simplificar o complicar el análisis.

- Una herramienta fundamental que es utilizada por las herramientas de adquisición de información evaluadas, es el Android Debug Bridge (ADB) que es una herramienta para desarrolladores para el sistema Android y que es parte SDK de Android. ADB sirve de puente de conexión entre el equipo del analista y el dispositivo Android analizado y así como también puede realizar volcados de información e instalación o cargar de programas o información en el dispositivo Android
- Consideramos que el análisis forense a dispositivos móviles hoy día es un tema de gran importancia que tanto las empresas, así como las instituciones que persiguen el delito deberían capacitar a su personal de seguridad o TI para poder realizar este tipo de análisis, ya que en los dispositivos móviles se encuentra mucha información que puede involucrar a una persona en un delito, relacionarlo con personas delictivas o en un procedimiento no adecuado.

REFERENCIAS

25000, I. (n.d.). *Criterios de Calidad.*

Android Developers. (n.d.). *Android Debug Bridge*. Retrieved from Developers: http://developer.android.com/tools/help/adb.html

Blogtecnico.net. (2014). *Blogtecnico- Adele Extractor de Base de Datos SQL Lite*. Retrieved from Blog Tecnico Hacking Tecnología Sistemas: http://www.blogtecnico.net/adel-extractor-de-base-de-datos-sqlite/

Forensic Blog. (n.d.). *Forensic Blog ADEL*. Retrieved from Forensic Blog mobile phone forensics and mobile malware: http://forensics.spreitzenbarth.de/adel/

Hidalgo, E. (2012, Octubre 15). *Santoku, una distro de seguridad para dispositivos móviles y mucho más*. Retrieved from Linux Zone: http://linuxzone.es/2012/10/15/santoku-una-distro-de-seguridad-para-dispositivos-moviles-y-mucho-mas/

kswartz. (n.d.). *HOWTO forensically examine an Android device with AFLogical OSE on Santoku Linux*. Retrieved from SANTOKU: https://santoku-linux.com/howto/mobile-forensics/howto-forensically-examine-android-aflogical-santoku

Lakhoua, M. B. (2013, Julio 28). *ADEL- Android Forensics Tool*. Retrieved from SecTechno Information Security Blog: http://www.sectechno.com/2013/07/28/adel-android-data-forensics-tool/

Mejia, O. A. (n.d.). *Android.* Retrieved from UAM: http://www.izt.uam.mx/newpage/contactos/revista/83/pdfs/android.pdf

Mobile Forensics World. (2012, Abril 18). Cell Phone and GPS Forensic Tool Classification System Retrieved. Retrieved from www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_CellPhoneandGPSForensicToolClassificationSystem.pdf

Motos, V. (2012, Agosto 17). *Santoku: distribución de seguridad para dispositivos móviles*. Retrieved from Hack Players: http://www.hackplayers.com/2012/08/santoku-distribucion-de-seguridad-moviles.html

OSAF Community. (2012). *OSAF Community Site*. Retrieved from OSAF Open Source Android Forensics: http://osaf-community.org/

Santoku. (n.d.). *Santoku- Linux*. Retrieved from Santoku: https://santoku-linux.com/features

skygear. (2012, Febrero 22). *OSAF TK Open Source Android Forensics Toolkit*. Retrieved from Security List Network : http://seclist.us/2012/02/osaf-tk-open-source-android-forensics-toolkit.html

ViaForensics. (2014). *AFLogical viaforensics*. Retrieved from ViaForensics free tool: https://viaforensics.com/resources/tools/android-forensics-tool/

Wikipedia The Free Encyclopedia. (2014, Abril 1). *Mobile Phone*. Retrieved from Wikipedia The Free Encyclopedia: http://en.wikipedia.org/wiki/Mobile_phone