Defining of a Practical Model for Digital Dorensic Analysis on Android Device Using a Methodology Post-Mortem

Johan Smith Rueda R.
Grupo de investigación INGAP
Universidad Francisco de Paula Santander Ocaña
Ocaña, Colombia
+57 317 349 5750
jsruedar@ufpso.edu.co

Dewar Wilmer Rico B.
Grupo de investigación INGAP
Universidad Francisco de Paula Santander Ocaña
2nd line of address
+57 312 397 3390
dwricob@ufpso.edu.co

ABSTRACT
The technologies are changing at a rapid pace and computer forensics must keep pace with events. The guidelines proposed by institutions concerning the digital forensics and incident response are not progressing at the pace required technology. In addition, there are relevant guidelines on specific issues of forensic process that are not taken into account by people who start this process. From the academy, a practical model, which consists of eight phases is proposed, and integrates the forensic process and best practices in the management of digital evidence and chain of custody in order to provide guidance in learning and study forensic digital analysis using a post-mortem methodology and directing it towards a mobile device with the Android operating system. Through the guide will detail all the knowledge you must have the forensic investigator before, during and after forensic investigation.

CCS Concepts
• **Applied computing**➞Computing Forensics ➞Evidence collection, storage and Analysis

Keywords
Android Forensics; Digital Mobile Forensics; Methodology post-mortem; Practical Model.

1. INTRODUCTION
El desarrollo tecnológico de los dispositivos móviles ha permitido que las actividades cotidianas a nivel personal y profesional se trasladen a dichas terminales, convirtiéndose en una herramienta de uso masivo [1]. Como consecuencia, los ataques que tradicionalmente eran dirigidos hacia los equipos de cómputo tradicionales han migrado a las plataformas móviles [2].

El sistema operativo Android es la plataforma más utilizada en la actualidad. Según un informe de IDC, en el periodo Q2 del 2015 tiene un 82.8 % de la cuota de mercado [3]. Esta popularidad lo ha convertido en el sistema operativo móvil más atacado, así lo muestra un informe presentado por Kaspersky Lab. & Interpol. En un periodo de 12 meses, entre junio de 2013 y junio de 2014, el malware detectado por los productos de este laboratorio de seguridad tuvo un total de 3.408.112, siendo marzo de 2014 el mes que mayor actividad reportó con 64.000 ataques. El tipo de malware más popular es el financiero, con un 59.06 % [4].

Una de las falencias que presenta esta plataforma es la gestión de los permisos que se le conceden a las aplicaciones [5]. Esta responsabilidad es otorgada a los usuarios, son ellos quién deciden sí los aceptan o no.

A nivel empresarial, tendencias como BYOD (*Bring Your Own Device*), en el cual los empleados usan sus dispositivos personales como una extensión de la infraestructura tecnológica corporativa para acceder desde ellos a los recursos de la organización, están siendo implementadas por las organizaciones para permitir una mayor movilidad, aumento de la productividad y satisfacción laboral [6] [7].

Pero este tipo de prácticas, si no son bien gestionadas por las organizaciones y, estas no manejan una políticas claras para la gestión de los dispositivos [8], implementando controles para su incorporación dentro de su red, su actualización y su uso en general puede traer consecuencias negativas, ya que estos dispositivos mal gestionados por sus dueños y no supervisados por las entidades se convierten en un agujero de seguridad para la infraestructura corporativa [9] [10] [11].

La información de los usuarios y de las organizaciones está siendo confiada a los dispositivos móviles y los cibercriminales están ideando mejores ataques hacia estas plataformas con el objetivo de conseguir dicha información para su beneficio propio.

Cuando un incidente de seguridad pasa o se sospecha que ha pasado es donde entra la informática forense, que puede ser definida como el proceso de aplicar métodos científicos para recopilar y analizar datos e información que puede ser utilizada como evidencia [12].

Instituciones como el *National Institute of Standards and Technology* – NIST y el *National Institute of Justice* (NIJ) – *U.S. Department of Justice* reconocidas a nivel internacional por ser referentes en el análisis forense digital y en la respuesta a incidentes han propuesto guías para ayudar a abordar este proceso.

Las guías de las NIST [13] [14] y el NIJ [15] [16] tienen más de siete años de antigüedad y han quedado cortas en su actualización en comparación a la rápida evolución que han tenido los dispositivitos móviles.

Por esta razón se vio la necesidad de definir una guía práctica que integre el proceso forense, las buenas prácticas que se debe tener en cuenta para realizarlo de una forma adecuada y las características de los dispositivos móviles Android más recientes.

En esta investigación se propuso resolver el siguiente interrogante: ¿Son las metodologías de análisis digital forense tradicional una guía idónea para realizar un análisis forense en un dispositivo móvil, teniendo en cuenta las características de dichas terminales?

Para ello, se propuso tres ejes de trabajo: El primero, caracterizar herramientas utilizadas en el análisis digital forense con licencia GPL para elegir las herramientas a usar durante las siguientes fases del proyecto. El segundo, realizar un análisis de las metodologías

978-1-5090-2435-3/16/$31.00 ©2016 IEEE

propuestas en años anteriores para el análisis digital forense tradicional. Y el tercer eje, definir una guía práctica que sirva como soporte para el análisis digital forense en un dispositivo móvil.

La guía que se propone en este documento se enfoca en el análisis forense a los medios de almacenamiento permanente de un dispositivo móvil bajo la plataforma Android. Otra de las consideraciones que se tuvieron presente fue la realización del procedimiento forense utilizando herramientas con licencia GPL, esto por el alto costo de las herramientas comerciales para el análisis forense y la restricción del uso de las mismas. Así también, no se realizó herramientas forenses de tipo hardware, por cuestiones económicas y restricciones para el uso de estas herramientas por cualquier persona ajena a las fuerzas del orden de una nación o una empresa que realice esta actividad de forma profesional y acorde con la legislación nacional. Su uso debe ser justificado.

El propósito de esta guía es servir como apoyo a los estudiantes e integrantes de los semilleros y grupos de investigación de las instituciones de educación superior, así también a todas las personas que quieran iniciarse en el estudio de la informática forense orientada a los dispositivos móviles.

2. METODOLOGÍA

Esta investigación fue cuantitativa de tipo descriptivo. Para la recolección de información se usó la técnica de observación estructurada. Técnica usada para probar una hipótesis o una descripción sistemática de un fenómeno donde el investigador sabe de antemano qué aspectos son relevantes y cuales no para el propósito de su investigación.

Se estudió las características del proceso forense, identificando las variables que intervienen en dicho proceso. Dichas características se tuvieron en cuenta a la hora de definir este modelo propuesto. Las variables fueron de utilidad para el modelo y para la evaluación de las herramientas y metodologías post-mortem estudiadas.

Para evaluar las herramientas forenses, luego de identificar las variables que intervienen en el proceso, se caracterizó dichas herramientas y se relacionó con las variables obtenidas. Se estudió los modelos propuestos por autores y organizaciones y que son aceptadas a nivel internacional como guías para el análisis forense.

3. DEFINICIÓN DEL MODELO

3.1 Revisión de literatura y herramientas

Antes de proponer la guía práctica, se estudiaron algunas herramientas forenses con el fin de seleccionar aquellas que pueden ser utilizadas para realizar un análisis forense digital en un dispositivo móvil con Android y las metodologías propuestas para tal fin.

Para seleccionar el software a utilizar se plantearon dos situaciones: La primera fue estudiarlas de forma individuales, en caso de que caso en que hubiese varias herramientas con un mismo propósito se procedió compararlas para elegir la más óptima. La segunda situación fue estudiar las suites forenses disponibles. Estas dos situaciones se plantearon para dar más libertad a la hora de elegir las herramientas y no limitarla a las consideraciones hechas por el autor.

Para seleccionar las herramientas individuales, luego de hacer la revisión de la literatura y descartar aquellas que no sirvan para los dispositivos móviles o estuvieses orientadas a una plataforma específica que no sea Android, se procedió a elegir las herramientas a usar y clasificarlas en tres grupos: 1. Herramientas para la adquisición, 2. Herramientas para el examen y 3. Herramientas para el análisis.

Las herramientas para la adquisición que se tuvieron cuenta son: dd, dc3dd y dcfldd para la adquisición de las imágenes forenses en las tarjeas MircoSD de los dispositivos. Al tener estas tres herramientas el mismo fin se procedió a compararlas (Ver Tabla 1). Y para la adquisición de la información del teléfono se usó la herramienta AFLogial OSE.

Tabla 1. Comparación de herramientas para la adquisición de imágenes forenses Fuente. Autor.

Herramienta	Implementación de Hash	Información al usuario	Segmentación de imágenes	Tiempo de ejecución	Total
dd	1	1	1	1	4
dc3dd	3	3	3	3	12
dcfldd	2	3	3	2	10

De los valores asignados como calificación en cada variable estudiada, el no cumplir con el requerimiento tiene el puntaje mínimo de 1. En caso de cumplir, la máxima calificación es 3. El puntaje de 2 se dio a aquellas herramientas que cumplían con el requerimiento pero no de forma óptima.

Las herramientas para el examen se seleccionaron: Foremost, Photorec, Testdisk y Myrescue. Estas herramientas tiene la finalidad de recuperación de archivos, el *Datacarving* y el *Filecarving*.

Para el análisis se tuvieron en cuenta las siguientes herramientas: Autopsy, Digital Forensic Framework y log2timeline. Seleccionándose Autopsy por sus características y por ser una herramienta aceptada por profesionales forenses. También fue seleccionada log2timeline para realizar la línea del tiempo de los hechos ocurridos, lo cual es relevante a la hora de analizar la información y determinar qué hecho pasó en que instante de tiempo.

Para seleccionar la suite de herramientas se estudiaron las distribuciones GNU/Linux orientadas al análisis forense y respuesta de incidentes en dispositivos móviles. Estas distribuciones son: CAINE Linux, Santoku, DEFT y SIFT Workstation (Ver Tabla 2).

Tabla 2. Comparación de suites forenses. Fuente. Autor.

Suite de herramientas	Soporta móviles	Soporte Android	Soporte técnico	Documentación	Soporte profesional	Total
CAINE	5	1	5	3.5	3.5	18
Santoku	5	5	4.5	4.2	4	22.7
DEFT	5	5	4.5	5	4	23.5
SIFT Workstation	3	1	5	5	5	20

Las distribuciones se evaluaron con los criterios establecidos por el autor. Que dichas distribuciones soportaran dispositivos móviles, que tuvieran soporte para la plataforma Android. El soporte técnico hace referencia al equipo desarrollador que mantiene y da soporte a la distribución, en brindar las respectivas actualizaciones y corrección de errores.

La documentación es la ayuda ofrecida por el proyecto que soporta dichas distribuciones, las guías brindadas a los usuarios para facilitar la apropiación de dichas distribuciones por parte de estos. El soporte profesional hace referencia al equipo forense que está dando soporte en la parte técnica y todo lo relacionado con el análisis forense, herramientas y procedimientos. La calificación es de 1-5, siendo 5 la máxima nota y representa el mayor grado de satisfacción de los criterios establecidos.

En cuanto a los modelos forenses, luego de hacer una revisión de la literatura se eligieron los más representativos. Esto con el fin de identificar los puntos fuertes y las falencias que presenta cada modelo. Se hizo un comparativo de las fases propuestas por los autores en cada modelo (Ver Figura 1).

Los modelos que se estudiaron son: El modelo del Modelo del *National Institute of Justice*, 2001; el modelo DFRWS, 2001; el modelo de Reith, Carr y Gunsch, 2002; el modelo Casey, 2004; el modelo del *National Institute of Justice*, 2004; el modelo extendido para las investigaciones de cibercrimen, 2004; y el modelo Cohen, 2009.

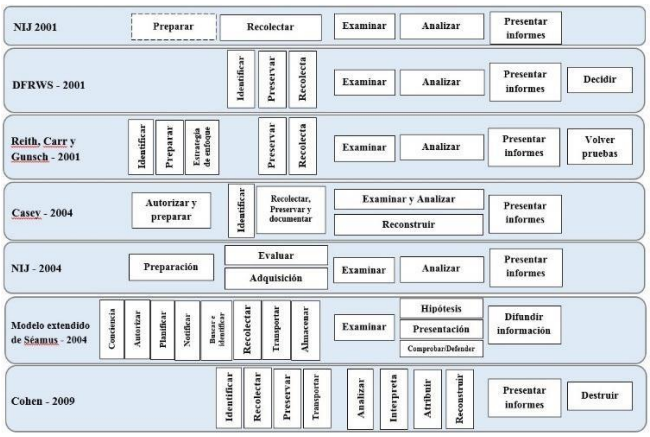


Figura 1. Fases de los modelos estudiados. Fuente: Autor.

Teniendo en cuenta estas consideraciones previas, y los resultados obtenidos se procedió a definir un modelo que sirva como guía práctica en el análisis digital forense utilizando una metodología post-mortem en los dispositivos móviles con sistema operativo Android.

3.2 Modelo propuesto

El modelo propuesto consta de ochos fases (ver Figura 2). Dicho modelo integra las cuatro fases tradicionales del procedimiento forense: Adquisición, examen y análisis de las pruebas y el presentar los respectivos informes. Pero también se propuso tres fases previas de carácter preparatorias y una fase final de revisión de todo el proceso forense realizado.

Las fases comprendidas en el modelo propuesto se describen a continuación:

Figura 2. Modelo propuesto. Fuente: Autor.

Identificación y evaluación. En esta fase, el equipo forense tiene el acercamiento con el caso a investigar solicitado por la víctima o una autoridad. Se debe procurar obtener la mayor parte de la información posible sobre el incidente. Se debe evaluar el alcance del procedimiento forense –esto reduce los costos en tiempo y dinero en búsquedas innecesarias–, la escena del crimen, el entorno donde se realizará la extracción de las pruebas de los dispositivos móviles –si el dispositivo se puede trasladar al laboratorio forense o no–; se identifica la potencial información que pueda servir como prueba y se tienen en cuenta las consideraciones legales como son las autorizaciones para realizar el procedimiento forense o la normatividad de la organización donde ocurrió el incidente informático, entre otras consideraciones.

Preparación. En esta fase el equipo o investigador forense se provee y prepara los elementos necesarios para la realización del procedimiento forense. Los elementos que se deben preparar son de tipo *hardware*, *software* y los suministros para el manejo de la evidencia y los profesionales que integran el equipo forense.

El *hardware* que se debe preparar están las interfaces para conectar el dispositivo móvil con la estación forense, los cargadores, fuentes de energía suplementaria para garantizar que el dispositivo se mantenga encendido el tiempo necesario para la extracción de las imágenes forenses, medios de almacenamiento esterilizados para almacenar dichas imágenes, cajas o bolsas de Faraday, bolsas antiestáticas y guantes de látex en caso que se requiera extraer las huellas dactilares del dispositivo.

En cuando al *software* se prepara la estación forense, utilizada para la adquisición, examen y análisis de la información recolectada en el terminal. Entre los suministros para el manejo de la prueba están formatos para en manejo de la prueba o evidencia, la cámara fotográfica y grabadora, etiquetas adhesivas, marcadores indelebles, libreta para notas rápidas y crear el croquis de la escena del crimen y todo aquello que sea útil para registrar y transportar la evidencia.

Preservación. En esta fase se asegura, evalúa y documenta la escena del crimen. Una vez hecho esto, se procede al embalaje, transporte y almacenamiento de las pruebas o evidencia encontrada en la escena. También se aisla es dispositivo móvil, se tiene las consideraciones necesarias para no contaminar las pruebas. Se tiene en cuenta el estado en que se encuentra el dispositivo, si esta encendido o apagado, y se procese con su embalaje, transporte y almacenamiento. En esta fase es donde se inicia la cadena de custodia.

Adquisición. Esta fase se busca, se identifica, recolecta y documenta las pruebas electrónicas. Se identifica la fuente de los datos, se desarrolla el plan para adquirir los datos. Luego los datos se adquieren y se verifica la integridad de los mismos.

Examen. Una vez los datos se han adquirido, en esta fase se procede a la reparación de archivos borrados, archivos escondidos, identificación los archivos existentes, consolidando los archivos potencialmente analizables con el fin de reducir la búsqueda y centrarse en ciertos archivos. Una vez esto, estos archivos se organizan.

Análisis. Con los archivos identificados y clasificados se procede el análisis de esa información. El objeto de esta fase es establecer un enlace creíble entre el atacante, la víctima y la escena del crimen. Se busca resolver las siguientes preguntas: ¿Quién lo hizo?, ¿qué hizo?, ¿cuándo lo hizo?, ¿por qué lo hizo?, y ¿cómo lo hizo?

Presentación de informes. En esta fase es donde se recopila todas las notas y apuntes tomadas en todas las fases y se prepara un resumen detallado de todas las medidas adoptadas y las conclusiones que se alcanzaron en la investigación. El informe debe ser soportado con el mayor número de evidencias, ya sean fotografiáis, capturas de video y acompañado de CD o DVD para presentar archivos cuyo formato no permite ser impreso como un video o audio.

Revisión. Esta fase busca la mejora continua. La revisión a conciencia de las actividades realizadas en cada fase durante la investigación permitirá refinar estas acciones para una futura investigación. Se busca en enriquecer la pericia del investigador o del equipo forense.

3.3 Formatos para el manejo de la prueba o evidencia

Se construyeron unos formatos donde se pueda registrar la evidencia física y digital y manejar la cadena de custodia, ver Figuras 3 a la Figura 8..

La construcción de dichos formatos es el resultado de la revisión de la literatura y el Manual de procedimientos para la cadena de custodia de la Fiscalía General de la Nación [17]. Estos formatos se muestran a continuación.

ROTULO DE EVIDENCIA FÍSICA O MATERIAL DE PRUEBA
Versión 1.0

Código del caso	Fecha y hora de la recolección
	D D M M A A - H H M M

Nombre del caso

Lugar del hallazgo

Descripción: _____

Evidencia fisica o material de prueba

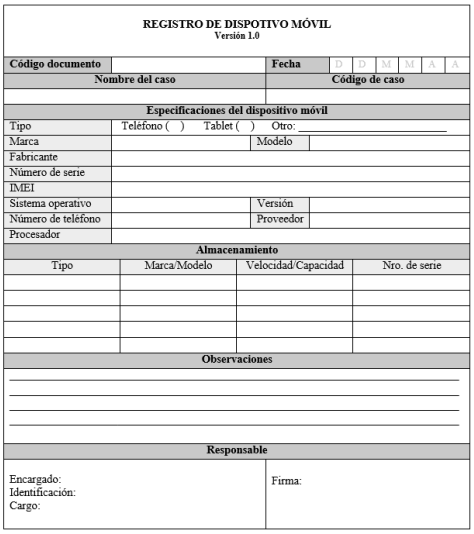
Descripción: _____

Observaciones

Responsable

Encargado: Identificación: Cargo:	Firma:

Figura 3. Formato de rotulado de evidencia física o materail de prueva. Fuente: Autor.



REGISTRO DE DISPOTIVO MÓVIL
Versión 1.0

Código documento		Fecha	D D M M A A
Nombre del caso		Código de caso	

Especificaciones del dispositivo móvil

Tipo	Teléfono ( ) Tablet ( ) Otro: _____		
Marca		Modelo	
Fabricante			
Número de serie			
IMEI			
Sistema operativo		Versión	
Número de teléfono		Proveedor	
Procesador			

Almacenamiento

Tipo	Marca/Modelo	Velocidad/Capacidad	Nro. de serie

Observaciones

Responsable

Encargado: Identificación: Cargo:	Firma:

Figura 4. Registro del dispostivo móvil. Fuente: Autor.

REGISTRO DE EVIDENCIA DIGITAL
Versión 1.0

Código documento		Fecha	D D M M A A
Nombre del caso		Código de caso	

Dispositivo de origen

Tipo	Teléfono ( ) Tablet ( ) Otro: _____		
Marca		Modelo	
Sistema operativo		Versión	
Tipo de memoria		Capacidad	

Medio de almacenamiento de la prueba

Nro. de serie	Tipo	Capacidad	Ubicación del medio de almacenamiento

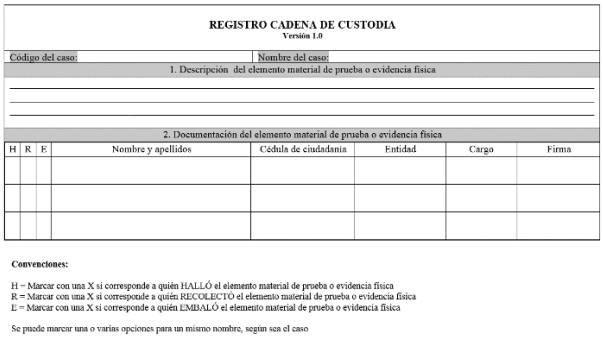
Observaciones

_____
_____
_____
_____

Responsable

Encargado: Identificación: Cargo:	Firma:

Figura 5. Registro de evidencia digital. Fuente: Autor.



REGISTRO CADENA DE CUSTODIA
Versión 1.0

Código del caso: Nombre del caso:

1. Descripción del elemento material de prueba o evidencia física

_____
_____
_____

2. Documentación del elemento material de prueba o evidencia física

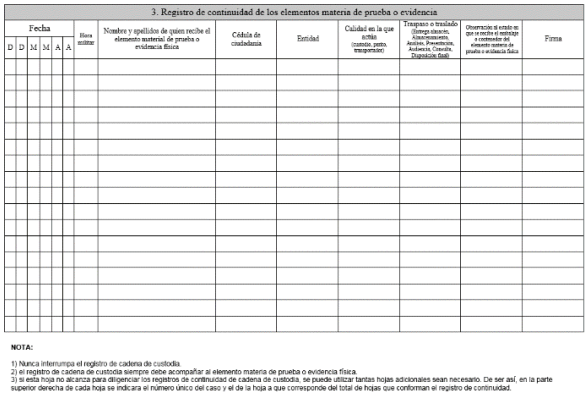
H	R	E	Nombre y apellidos	Cédula de ciudadanía	Entidad	Cargo	Firma

Convenciones:

H = Marcar con una X si corresponde a quién HALLÓ el elemento material de prueba o evidencia física
R = Marcar con una X si corresponde a quién RECOLECTÓ el elemento material de prueba o evidencia física
E = Marcar con una X si corresponde a quién EMBALÓ el elemento material de prueba o evidencia física

Se puede marcar una o varias opciones para un mismo nombre, según sea el caso

Figura 6-a. Registro de la cadena de custodia. Fuente: Autor.



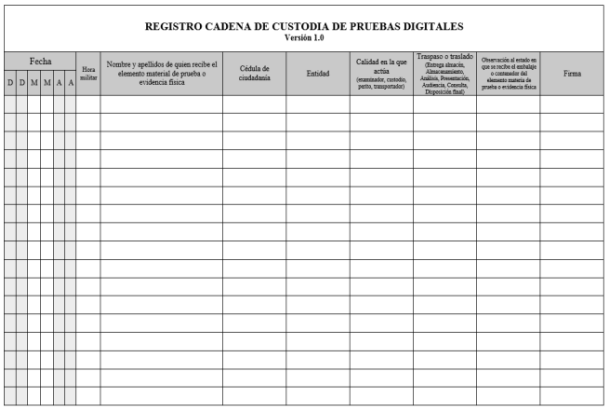
3. Registro de continuidad de los elementos materia de prueba o evidencia

Fecha	Hora militar	Nombre y apellidos de quien recibe el elemento material de prueba o evidencia física	Cédula de ciudadanía	Entidad	Calidad en la que actúa (cuestor, perito, transportador)	Traspaso o traslado (Entrega cliente, Almacenamiento, Análisis, Presentación, Audiencia, Custodia, Disposición final)	Observación si estado en que se recibe el embalaje o contenedor del elemento materia de prueba o evidencia física	Firma
D D M M A A								

NOTA:

1) Nunca interrumpa el registro de cadena de custodia.
2) el registro de cadena de custodia siempre debe acompañar al elemento materia de prueba o evidencia física.
3) si esta hoja no alcanza para diligenciar los registros de continuidad de cadena de custodia, se puede utilizar tantas hojas adicionales sean necesario. De ser así, en la parte superior derecha de cada hoja se indicara el número único del caso y el de la hoja a que corresponde del total de hojas que conforman el registro de continuidad.

Figura 6-b. Registro de la cadena de custodia. Fuente: Autor.



REGISTRO CADENA DE CUSTODIA DE PRUEBAS DIGITALES
Versión 1.0

Fecha	Hora militar	Nombre y apellidos de quien recibe el elemento material de prueba o evidencia física	Cédula de ciudadanía	Entidad	Calidad en la que actúa (examinador, custodio, perito, transportador)	Traspaso o traslado (Entrega cliente, Almacenamiento, Análisis, Presentación, Audiencia, Custodia, Disposición final)	Observación si estado en que se recibe el embalaje o contenedor del elemento materia de prueba o evidencia física	Firma
D D M M A A								

Figura 7. Registro de la cadena de custodia ditigal. Fuente: Autor.

REGISTRO RESPONSABLES DE CADENA DE CUSTODIA
Versión 1.0

Código del caso		**Evidencia**	Física ( ) Digital ( )
		Código documento	
Nombre del caso			
Responsable		**Fecha y hora**	
Entregado por	Firma	D D M M A A - H H M M	
Recibido por	Firma	D D M M A A - H H M M	
Responsable		**Fecha y hora**	
Entregado por	Firma	D D M M A A - H H M M	
Recibido por	Firma	D D M M A A - H H M M	
Responsable		**Fecha y hora**	
Entregado por	Firma	D D M M A A - H H M M	
Recibido por	Firma	D D M M A A - H H M M	
Responsable		**Fecha y hora**	
Entregado por	Firma	D D M M A A - H H M M	
Recibido por	Firma	D D M M A A - H H M M	
Responsable		**Fecha y hora**	
Entregado por	Firma	D D M M A A - H H M M	
Recibido por	Firma	D D M M A A - H H M M	

Figura 7. Registro responsables de la cadena de custodia. Fuente: Autor.

4. CONCLUSIONES

Dentro de las herramientas que manejan la filosofía del software libre encontramos una gama de posibilidades que nos posibilitan realizar un análisis forense en un entorno académico. Estás herramientas de fácil adquisición por su disponibilidad para su descarga y uso, su bajo costo son fundamentales en un entorno académico donde los recursos son limitados, donde el proceso se centra en la investigación y aprendizaje.

Las guías con las que se dispone a nivel internacional se están quedando cortas debido al ritmo de avance que tienen los dispositivos móviles y la falta de actualización de las mismas por parte de las instituciones que las soportan.

Los modelos forenses estudiados están más orientados al proceso forense en general, a los equipos de cómputo tradicionales y a las redes de comunicación. No se encuentra muchos modelos que estén orientados a los dispositivos móviles. Muchas de estos modelos hacen suposiciones, como por ejemplo, que el lector conoce el proceso de la cadena de custodia. Lo que dificulta la apropiación de estos criterios por parte de aquellas personas que quieren iniciar en el aprendizaje de esta rama del conocimiento.

5. REFERENCES

[1] IAB Spain Research, «VI Estudio Anual IAB Spain Mobile Marketing,» Madrid, 2014.

[2] A. Armando y A. Merlo, «Security considerations related to the use of mobile devices in the operation of critical infrastructures,» *International Journal of Critical Infrastructure Protection,* vol. 7, nº 4, pp. 247-256, 2014.

[3] IDC, «Smartphone OS Market Share, 2015 Q2,» 2015.

[4] Interpol & Kaspersky Lab., «Mobile Cyber Threats,» 2014.

[5] J. Crampton y J. Sellwood, «Sleeping Android: The Danger of Dormant Permissions,» de *Proceedings of the Third ACM workshop on Security and privacy in smartphones & mobile devices*, 2013.

[6] N. Altirriba Claramunt, «Universitat Oberta de Catalunya,» 15 Enero 2015. [En línea]. Available: http://hdl.handle.net/10609/39541. [Último acceso: Noviembre 2015].

[7] D. Bien, A. Negahban y J. Windsor, «BYOW in Practice: A comparison of Four BYOD Programs,» 2015.

[8] C. Kleiner, «Ensuring Mobile Device Security and Compliance at the Workplace,» *Procedia Computer Science,* pp. 274-281, 2015.

[9] S. Siwamogsatham, C. Polprasert y C. Vorakulpipat , «Managing Mobile Device Security in Critical Infrastructure Sectors,» de *Proceedings of the 7th International Conference on Security of Information and Networks*, 2014.

[10] Y.-S. Kang , J.-B. Kim, Y. Kim y Y. Shin, «A Study on Mobile Device Control Model for Critical Data Leakage Prevention in the Enterprise Business Service,» *International Journal of Security and Its Applications,* vol. 9, nº 10, pp. 373-380, 2015.

[11] E. F. Lanfranco, N. Macía, A. J. Sabolansky y P. Venosa, «Uso de dispositivos mobiles y BYOD: Su impacto en la seguridad,» de *XVII Workshop de Investigadores en Ciencias de la Computación (Salta, 2015)*, 2015.

[12] B. Nelson, A. Phillips y C. Steuart, Guide to Computer Forensics and Investigations, Fourth ed., Information Security Professionals, 2010.

[13] S. Chevalier, H. Dang, T. Grance y K. Kent, «Guide to Integrating Forensic Techniques into Incident Response – SP 800-86,» NIST, Gaithersburg, MD 20899-8930, 2006.

[14] R. Ayers y W. Jansen, «Guidelines on Cell Phone Forensics - SP 800-101,» NIST, Gaithersburg, MD 20899-8930 , 2007.

[15] National Institute of Justice, «Forensic Examination of Digital Evidence: A Guide for Law Enforcement.,» Washington, DC 20531, 2004.

[16] National Institute of Justice , «Electronic Crime Scene Investigation: A Guide for First Responders. Second edition.,» Washington, DC 20531 , 2008.

[17] Fiscalia General de la Nación, «Manual de procedimientos para la cadena de custodia de la Fiscalía General de la Nación».