Análisis forense de dispositivos de telefonía celular mediante procedimientos operativos estandarizados

Leopoldo Sebastián Gómez[1]

[1] Poder Judicial del Neuquén
sebastian.gomez@jusneuquen.gov.ar

Resumen. La aplicación de procedimientos operativos estandarizados junto a la segmentación de tareas operativas por roles profesionales son factores críticos dentro de las unidades periciales para garantizar la calidad en las labores forenses, a la vez que favorecen a mejorar la productividad y reducir las listas de espera de casos en trámite. La pericia informática sobre dispositivos de telefonía celular forma parte de los servicios que habitualmente se ofrecen en el marco de la actividad profesional del perito informático. Sustentado en las guías de buenas prácticas desarrolladas por la comunidad científica y otros documentos de referencia a nivel internacional se presenta un procedimiento operativo estandarizado para peritajes sobre este material probatorio. Estos lineamientos de trabajo tienen la virtud de estar articulados con un protocolo de actuación para pericias informáticas que ha sido aprobado institucionalmente y tiene carácter reglamentario en el ámbito judicial de la provincia de Neuquén.

1 Introducción

La informática forense es un área de especialización cuya popularidad va en aumento como producto de los avances de las tecnologías de la información y de la comunicación (TICs) y la estrecha y necesaria vinculación con el servicio de Justicia.

El panorama es desafiante ya que la evidencia digital comienza a hacerse presente en toda clase de actos ilícitos. En el nuevo sistema de justicia penal los peritajes han pasado a ser la reina de las pruebas y dentro de este ámbito las pericias informáticas tienen un pedestal asegurado.

Aquel profesional que se perfecciona en un área de especialidad, en este caso la informática forense, toma como desafío el acercamiento constante al estado del arte. No sólo desde el ámbito académico se brindan aportes que se integran al conocimiento científico para avanzar con el desarrollo de nuevas técnicas y herramientas. Actualmente se han logrado muchas contribuciones directas a la disciplina por parte de especialistas que detectan necesidades concretas que surgen del ejercicio de la actividad pericial.

El perfil profesional más adecuado para la actividad pericial involucra una sólida formación académica en ciencias informáticas junto al manejo de metodologías, técnicas y herramientas propias de esta nueva disciplina. La especialidad se completa con conocimientos jurídicos que provienen del Derecho, así como también adopta principios y métodos de investigación que tienen origen en la Criminalística. La

cantidad de especialistas es reducida si se la compara con otras áreas de ejercicio profesional dentro de las ciencias informáticas.

La masificación en el uso de tecnología digital actúa en correlación directa con el número creciente de fuentes de evidencia digital. Teniendo presente el crecimiento exponencial del universo digital y el fenómeno de big data junto a otros postulados como las leyes de Moore y Kryder, comienza a resultar anacrónica la aplicación del modelo de gestión basado en la asignación de pericias individuales. Se requiere evolucionar hacia la conformación de equipos especializados que actúen con una metodología de trabajo coordinada para la producción de un resultado final. Es así que comienza a plantearse la actuación profesional con roles y responsabilidades acordes a la experticia y área de competencia.

Sin perjuicio de los años de experiencia y las competencias técnicas individuales que posea un perito, cuando su actuación se desarrolla en el marco de un equipo profesional resulta imprescindible contar con procedimientos operativos estandarizados -en adelante SOPs- que establezcan los lineamientos sistemáticos mínimos de trabajo para garantizar la calidad en el servicio ofrecido, conformando así un modelo de trabajo pericial escalable para afrontar la creciente demanda de actividades forenses.

2 Procedimientos operativos estandarizados

Un SOP es un procedimiento interno desarrollado para realizar una rutina compleja con tiempo y recursos limitados. La importancia de un SOP adecuado a la estructura de un equipo profesional radica en el uso habitual de un procedimiento operativo escrito que está adaptado a un ambiente de trabajo y vinculado a la aplicación de técnicas y operación de herramientas, cuyo contenido está ordenado mediante texto, gráficos y otras especificaciones.

Si en lugar de aplicar o mejorar SOPs el profesional se concentra solamente en el uso de herramientas forenses, éste tiende a limitar su campo de acción y sólo actúa como si se tratase de un simple operario de aplicaciones y dispositivos. En el mejor de los casos, esta modalidad de trabajo sin pautas preestablecidas produce desvíos que atentan contra la productividad, pero también se corre el riesgo de realizar un análisis forense incompleto que indefectiblemente no conduce a obtener los mejores resultados en una pericia informática.

Los SOPs otorgan trazabilidad en la actividad pericial desarrollada, de forma tal que si los resultados de una pericia informática son cuestionados siempre es posible repetir la experticia. Los SOPs se establecen para demostrar que los pasos propios del trabajo metodológico siempre son más valiosos que el hardware o software que se utilice para una pericia informática.

Las herramientas forenses son siempre necesarias, pero ninguna de ellas debe ser considerada superior a las demás ya que todas ellas tienen fortalezas y debilidades. Por ello, siempre es importante que el perito informático posea una amplia variedad de hardware y software forense de forma tal que pueda utilizarlas para brindar el mejor resultado a los requerimientos periciales.

El conocimiento especializado juega un papel esencial a la hora de seleccionar técnicas y herramientas forenses, mientras que los pasos apropiados para el desarrollo de la actividad pericial pueden ser guiados mediante SOPs.

La experticia que debe tener el perito informático consiste en mantener el apego a los lineamientos de trabajo pautados para los casos ordinarios y a su vez tener la flexibilidad de poder aplicar los conocimientos avanzados que posee como especialista para encontrar la mejor solución al problema cuando la situación lo amerite.

3 Principios básicos para el manejo de evidencia digital

Desde 1984 a la fecha han surgido diversas propuestas metodológicas para informática forense, cada una con sus bondades y carencias, así como también se ha intentado conciliarlas en un modelo común que reúna y simplifique estos marcos de trabajo pericial [Yussof et al., 2011]. Sin tomar preferencia por alguna de ellas, queda claro que el proceso forense digital está conformado por actividades operativas orientadas a la identificación, preservación, análisis y presentación de evidencia digital.

La actividad pericial informática sobre telefonía celular debe mantener apego a los lineamientos procedimentales que resulten apropiados para esta fuente de evidencia digital. Han surgido otras propuestas [Murphy, 2010] en un nivel más detallado y orientado a los dispositivos de telefonía celular que desagregan estas etapas y cuya metodología queda comprendida por las siguientes fases: Ingreso, Identificación, Preparación, Aislamiento, Procesamiento, Verificación, Documentación, Presentación y Archivado. Aunque se encuentra en una etapa previa a la publicación del estándar internacional, el modelo de proceso armonizado para la investigación digital forense propuesto en la ISO/IEC 27043 ya comienza a ser estudiado en la comunidad académica para evaluar su adecuación al trabajo pericial con dispositivos de telefonía celular [Mumba and Venter, 2014].

En referencia al manejo de evidencia digital es menester tener presente los principios básicos establecidos en esta materia [ACPO & 7Safe, 2008], sin dejar de considerar que algunas reglas no pueden aplicarse a dispositivos de telefonía celular.

Principio 1: El personal policial no debe cambiar ningún dato almacenado en una computadora o dispositivo de almacenamiento que pueda ser presentado como prueba en un proceso judicial.

Principio 2: En aquellas circunstancias en las que una persona requiera acceder a los datos originales almacenados en una computadora o dispositivo de almacenamiento, dicha persona debe ser competente para hacerlo y ser capaz de presentar la evidencia explicando su relevancia y las consecuencias de las acciones que ha llevado a cabo sobre la misma.

Principio 3: Se debe crear y preservar un registro, reporte o bitácora de todos los procedimientos aplicados a la evidencia digital. Cualquier parte en el proceso judicial debería poder examinar dichos procedimientos y alcanzar el mismo resultado.

Principio 4: La persona que sea encargada de llevar adelante la investigación es responsable de asegurar el respeto a las normas y el cumplimiento de estos principios.

Como ya ha sido postulado en varios estudios sobre informática forense aplicada a dispositivos móviles [Zarouni, 2007] [Owen and Thomas, 2011] no es posible acatar estrictamente los principios 1) y 2) de la ACPO debido a la naturaleza dinámica de la información digital almacenada en este tipo de material probatorio. En virtud de lo expuesto, se han publicado documentos de buenas prácticas, guías de procedimiento y normas internacionales orientadas a la identificación, recolección, adquisición y preservación de evidencia digital con particulares referencias a dispositivos móviles, como la ISO/IEC 27037:2012. También habrán de tomarse en consideración los lineamientos de la ISO/IEC 27042, que tiene prevista su versión final para este año, en particular lo que concierne al análisis de evidencia digital sobre dispositivos de telefonía celular.

4 Pericias informáticas sobre dispositivos de telefonía celular

En el mercado existe una inmensa variedad de equipos de telefonía celular, con sistemas operativos propietarios, sistemas de archivos embebidos, así como también con disponibilidad de aplicaciones, servicios y periféricos. Ello demanda que un perito informático cuente con la mayor cantidad posible de técnicas y herramientas forenses y las aplique en función de su experticia.

Cuando se identifican las herramientas apropiadas para el análisis, un paradigma que resulta de mucha utilidad es el uso de un sistema por niveles sobre dispositivos de telefonía celular [Brothers, 2009]. Este sistema permite categorizar a las herramientas forenses para análisis de dispositivos de telefonía celular y GPS por el nivel de profundidad que tienen en el acceso a los datos, desde el simple acceso manual a los datos, pasando por la extracción lógica y física, hasta la lectura de memoria a nivel microscópico. A medida que se avanza en complejidad, los métodos son más puros a nivel forense pero como contraparte las herramientas son más costosas y se requiere mayor entrenamiento y tiempo para el análisis.

Los teléfonos celulares están diseñados para comunicarse con la red de telefonía celular y con otras redes de datos mediante networking vía Bluetooth, Infrarrojo y/o Wi-Fi. La mejor forma de preservar los datos del teléfono celular es aislarlo de las redes cercanas, pero en algunos casos esto podría no ser posible. Actualmente estos dispositivos de comunicación pueden contar con diversas funcionalidades de almacenamiento de información digital e incluso sincronizar información con repositorios de datos online. En praxis resulta necesario aplicar más de una herramienta forense para extraer datos de un teléfono celular y sus dispositivos de almacenamiento asociados.

Existen situaciones en las que las herramientas forenses utilizadas para extraer la información digital de dichos dispositivos podrían tener incompatibilidades o bien emitir reportes con información errónea. Es por ello que siempre que sea posible, resulta esencial verificar la precisión de los datos extraídos desde dichos dispositivos utilizando o complementando las técnicas con más de una herramienta forense. Algunos investigadores han reportado la existencia de casos donde el proceso de extracción ha modificado la información digital [Ayers et al., 2009].

Convenientemente se han desarrollado matrices que correlacionan aquellas herramientas forenses que son compatibles con una determinada tecnología de teléfonos celulares [Kessler, 2009] y también están disponibles otros recursos de consulta online en sitios especializados en pericias informáticas sobre telefonía celular.

Pese a que la cantidad de datos almacenados por los teléfonos celulares es pequeña si se la compara con la capacidad de almacenamiento de información digital que tienen las computadoras, el volumen de información digital contenido en estos dispositivos continúa en aumento.

Los tipos de datos contenidos en los teléfonos celulares y la forma en que ellos son utilizados están en evolución constante. La popularidad de los llamados teléfonos inteligentes hace que ya no sea suficiente la extracción de agendas de contactos, históricos de llamadas, mensajes de texto, fotografías digitales, entradas de agenda personal, notas y otros archivos multimedia. Muchas aplicaciones instaladas en dichos dispositivos deben ser analizadas, ya que pueden contener información sensible como contraseñas, datos de geolocalización o históricos de navegación en Internet.

Las formas de extraer datos desde los teléfonos celulares podrían variar dependiendo de las técnicas que se utilicen para ello. Dependiendo de la finalidad y profundidad con la que se requiera determinada información en el marco de una investigación judicial podrían requerirse solamente algunos datos del teléfono celular o bien una extracción completa del sistema de archivos embebido y/o de la memoria física del teléfono.

La verificación del requerimiento judicial es una condición necesaria para todo análisis forense. Muchos autores han resaltado la necesidad de consultar y obtener la autorización formal por parte de quien esté conduciendo la investigación penal como paso previo a cualquier intervención pericial [Mislan et al., 2010].

Habiendo resaltado algunos puntos críticos sobre la temática abordada, resulta oportuno exponer un procedimiento operativo estandarizado para pericias informáticas sobre telefonía celular que es perfectamente apto para ser documentado conforme las pautas actuales de elaboración científica de dichos documentos establecidas por el Scientific Working Group on Digital Evidence [SWGDE, 2004].

5 Especificación del procedimiento operativo estandarizado

Las pericias sobre telefonía celular forman parte de la actividad pericial informática en lo que refiere a extracción de evidencia digital, tal lo indicado en el apartado 2.a) “Descripción general de servicios de informática forense” del Protocolo de Actuación para Pericias Informáticas[1].

El teléfono celular es una fuente de evidencia digital sobre la que es viable aplicar procedimientos operativos estandarizados. Los buenos SOPs no deben contener o mencionar el nombre del hardware/software, ya que ello requiere de la experticia del

[1] Cfr. “Protocolo de Actuación para Pericias Informáticas”, Poder Judicial del Neuquén, aprobado por Acuerdo N°4908, protocolizado y publicado el Boletín Oficial, 2012. http://www.jusneuquen.gov.ar/images2/Biblioteca/ProtocoloActuacionPericiasInformaticas.pdf

perito informático a la hora de seleccionar la herramienta de informática forense que le ofrece los mejores resultados para el caso.

En consonancia con los aportes realizados por investigadores en la materia, el procedimiento operativo estandarizado para pericias informáticas sobre dispositivos de telefonía celular queda establecido mediante las siguientes actividades:

1. Verificar que el requerimiento judicial cumpla las pautas establecidas en el apartado d) del Protocolo de Actuación para Pericias Informáticas ("*Del requerimiento judicial*")

2. Priorizar el caso conforme los criterios detallados en el apartado e) del Protocolo de Actuación para Pericias Informáticas ("*De la priorización de casos urgentes*")

3. Dar ingreso al material probatorio siguiendo los lineamientos del apartado f) del Protocolo de Actuación para Pericias Informáticas ("*Del traslado y recepción del material secuestrado*")

4. Determinar si el teléfono celular está encendido o apagado

a. Si está apagado, debe quedar apagado

b. Si está encendido debe ser aislado de la red de telefonía celular lo antes posible con la opción que se estime apropiada:

i) Configurando el modo "Avión" en el teléfono celular, si lo permite

ii) Colocándolo en una caja de Faraday

iii) Encendiendo un inhibidor de señal en cercanía del teléfono celular

iv) Envolviéndolo con tres o más capas de papel de aluminio

v) Apagando el teléfono y retirando la batería

5. Obtener información sobre el modelo del teléfono celular y planificar la estrategia para la extracción de evidencia digital

a. Identificar la tecnología general del teléfono celular

b. Localizar cables, drivers y determinar el software o hardware forense a utilizar para la pericia informática. La selección de herramientas forenses para una pericia informática sobre telefonía celular depende de diversos factores, como el nivel de detalle requerido en los puntos de pericia, el modelo de teléfono celular en cuestión y la presencia de otras funcionalidades de almacenamiento externo del dispositivo

c. Determinar funcionalidades del teléfono celular y posibles datos almacenados en el mismo

d. Si el teléfono celular no tiene puerto de datos, no se cuenta con el cable de datos, o no existe software o hardware forense disponible para dicho modelo, se registra esta situación

6. Consultar las especificaciones técnicas del teléfono celular y sus capacidades de almacenamiento de datos

7. Preservar y analizar las fuentes de evidencia digital siguiendo las pautas prescriptas en el Protocolo de Actuación para Pericias Informáticas ("*Del análisis forense*")

a. Tarjeta de Memoria Externa

i. Realizar una imagen forense con la herramienta de informática forense apropiada

ii. Extraer la evidencia digital que resulte relevante conforme los puntos de pericia que hayan sido indicados

b. Tarjeta SIM

i. Generar una SIM clonada o leer la información digital de dicho dispositivo utilizando un lector de SIM protegido contra escritura

ii. Si el SIM está bloqueado por PIN y éste no es conocido, se deja constancia o se utiliza el PUK en caso de estar disponible

iii. Si el SIM no está bloqueado, se extrae la información digital relevante al caso

c. Equipo de telefonía celular

i. Aislar el dispositivo de la red de telefonía celular previamente a la extracción de información digital y si es posible, durante todo el proceso.

ii. Realizar una extracción física de la memoria del teléfono celular o bien una extracción lógica utilizando todas las herramientas forenses apropiadas, tanto de hardware como de software

iii. Verificar los resultados obtenidos

1. Que los datos de salida tengan el formato adecuado al tipo de dato asociado

2. Que las fechas y horas sean consistentes

3. Que todos los datos requeridos pudieron ser extraídos

a. Mediante comparación con datos obtenidos desde el teléfono celular

b. Utilizando más de una herramienta forense y comparando resultados

c. Validando mediante valores hash distintos artefactos digitales del teléfono celular

8. Documentar los resultados en un reporte informático forense

9. Elaborar el dictamen para dar respuesta a los puntos de pericia informática haciendo referencia a la evidencia digital detallada en el reporte informático forense, siguiendo las pautas establecidas en el apartado h) del Protocolo de Actuación para Pericias Informáticas ("*De la presentación del dictamen*")

10. Remitir el dictamen junto a los elementos probatorios siguiendo los lineamientos de apartado i) del Protocolo de Actuación para Pericias Informáticas ("*De la remisión del material secuestrado*")

En cuanto a la verificación de resultados, es posible realizar validaciones sobre el sistema de archivos de los dispositivos celulares generando valores hash de todos los elementos extraídos y haciendo una segunda extracción al concluir el análisis forense con el objeto de chequear la integridad de dichos archivos. Cualquier cambio debería ser analizado en profundidad para determinar si se trata de archivos del sistema operativo o bien son archivos de usuario con el objeto de intentar determinar la razón de dichos cambios [Murphy, 2009].

Sin perjuicio de los pasos indicados en el procedimiento operativo estandarizado para pericias informáticas sobre dispositivos de telefonía celular, el perito informático debe aplicar los conocimientos especializados sobre la materia y tener presente los aportes de otras guías de mejores prácticas y de procedimiento a nivel internacional [NIST, 2007], [ACPO & 7Safe, 2008], [SWGDE-1, 2013], [NIST-1,2014] .

6 Actuación profesional en laboratorios de informática forense

En toda actividad pericial a gran escala es necesario que existan roles y responsabilidades asociadas a la ejecución de procedimientos que armonicen con el nivel de experticia del equipo profesional. En algunas situaciones una sola persona puede cumplir más de un rol. Sin embargo, tener una clara distinción de roles profesionales es una forma muy útil para asignar responsabilidades y asegurar que el

alcance general de las actividades periciales es completo y suficiente. Las competencias referidas al personal que trabaje en pericias sobre telefonía celular han sido desarrolladas por el SWGDE [SWGDE-2, 2013].

Actualmente existen pocos laboratorios de informática forense que tienen acreditación internacional en el manejo de evidencia digital. A falta de una norma específica para la especialidad, la acreditación internacional comenzó a sustentarse en la estándar ISO/IEC 17025:2005 y otros requerimientos suplementarios determinados por la American Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD/LAB) para laboratorios de informática forense. Existen numerosas críticas referidas a la dificultad o imposibilidad de aplicación a la informática forense de las cláusulas establecidas en esta normativa, así como también la falta de especificidad en cuanto a los criterios de cumplimiento.

Los aspectos esenciales para el desarrollo de laboratorios de informática forense están centrados en la conformación de equipos de trabajo con recursos humanos calificados, la elaboración y seguimiento de procedimientos operativos formales, el uso de hardware y software forense de última generación, y la capacidad de gestión autónoma del área pericial informática para solucionar temas de personal, administrativos y financieros. La carencia de varios de estos tópicos forma parte de la realidad cotidiana de todas las áreas periciales o incipientes laboratorios de informática forense de la Justicia provincial y nacional.

El camino a seguir está estrictamente vinculado a los lineamientos ya establecidos en otras organizaciones pioneras en la materia. Las condiciones de suficiencia que requiere un laboratorio forense para alcanzar este nivel de madurez involucran el apego a procedimientos operativos estandarizados y el control de calidad en distintos aspectos que hacen al servicio pericial.

7 Conclusiones

Se ha presentado un procedimiento operativo estandarizado para pericias informáticas sobre dispositivos de telefonía celular que está alineado a las buenas prácticas, normas y estándares internacionales aplicables a la informática forense. La inclusión de este procedimiento operativo estandarizado en un protocolo[2] aprobado por el Poder Judicial del Neuquén ha posibilitado que dicha normativa tenga carácter reglamentario en el ámbito de la Justicia provincial.

La adopción de un método formal de trabajo para la praxis forense sobre dispositivos de telefonía celular coadyuva a sustentar la admisibilidad de la prueba digital y conforma un novedoso avance normativo que acompaña la introducción de la evidencia digital en las reformas más recientes de los códigos procesales[3].

La creciente demanda de actividades forenses sobre fuentes de evidencia digital obliga a avanzar hacia un modelo de trabajo pericial escalable, conformando equipos

[2] Cfr. Gómez, L., Pericias informáticas sobre dispositivos de telefonía celular, Protocolo, http://www.jusneuquen.gov.ar/images2/Biblioteca/ProtocoloPericiasTelefoniaCelular.pdf

[3] Cfr. Código Procesal Penal de la Provincia del Neuquén, art. 153, Información digital. http://www.jusneuquen.gov.ar/images2/Biblioteca/CPPenalNqn.pdf

profesionales que procedan en forma metodológica. La segmentación de tareas operativas por roles permite profesionalizar la labor del perito informático, mejora la productividad del equipo de trabajo y contribuye a reducir las listas de espera de casos en trámite.

La informática forense es una disciplina técnico-legal. Se trata de una especialidad con base en las ciencias informáticas que se nutre de otros conocimientos propios del derecho y la criminalística. Independientemente del carácter fungible del perito, éste debe tener mínimamente un título universitario habilitante en la materia pertinente respecto de la cual ha de expedirse. Sin perjuicio de la diversidad de dispositivos tecnológicos que existen en la actualidad y entre ellos los equipos de telefonía celular, cuando se trata de ejecutar peritajes en procura de evidencia digital se hace indispensable contar con conocimientos especializados.

Todo dictamen debe contener la relación detallada de las operaciones practicadas en la pericia y su resultado. El apego a procedimientos operativos estandarizados contribuye a garantizar que los resultados de la actividad pericial informática sean verificables y repetibles, es decir, científicos.

La correcta aplicación de los pasos prescritos permite que se desarrolle la actividad pericial sobre dispositivos de telefonía celular sin perder de vista el marco metodológico requerido para el manejo de evidencia digital, pudiendo hacer uso de las técnicas y herramientas de informática forense que estén disponibles.

Los procedimientos operativos estandarizados contribuyen a mantener la calidad del servicio y llevan al siguiente nivel a las guías básicas de buenas prácticas. Se espera que esta propuesta sea considerada como impulsora y sirva como modelo de referencia para el desarrollo de otros procedimientos operativos estandarizados que conformen los futuros manuales de operaciones de otras unidades periciales la Justicia nacional y provincial.

Referencias

1. ACPO & 7Safe (2008), Good Practice Guide for Computer-Based Electronic Evidence, Guide for Mobile phone seizure and examination, http://www.7safe.com/
2. Ayers, R., Dankar, A. and Mislan, R. (2009), Hashing Techniques for Mobile Device Forensics, *Small Scale Digital Device Forensics Journal* , pp.1-6.
3. Brothers, S. (2011), How Cell Phone "Forensic" Tools Actually Work - Cell Phone Tool Leveling System, *DoD Cybercrime Conference,* Atlanta.
4. Kessler, G. (2010), Cell Phone Analysis: Technology, Tools, and Processes. *Mobile Forensics World,* Chicago: Purdue University.
5. Mislan, R.P., Casey, E. and Kessler, G.C. (2010), The Growing Need for On-Scene Triage of Mobile Devices, *Digital Investigation*, Elsevier, *6*(3-4), pp.112-124
6. Mumba, E. and Venter, H. (2014), Mobile forensics using the harmonised digital forensic investigation process, *Information Security for South Africa (ISSA) Conference, Johanesburg.*
7. Murphy, C. (2009), The Fraternal Clone Method for CDMA Cell Phones. *Small Scale Digital Device Forensics Journal*, pp.4-5.

8. Murphy, C. (2010), Cell Phone Evidence Extraction, *Digital Forensics Magazine*, July 2010, http://digitalforensicsmagazine.com/blogs/?p=80
9. NIST (2007), Jansen, W. and Ayers, R., Guidelines on Cell Phone Forensics, SP 800-101, http://csrc.nist.gov/
10. NIST-1 (2014), Ayers, R., Brothers, S. and Wayne, J., Guidelines on Mobile Forensics, SP 800-101 Revision 1, http//dx.doi.org/10.6028/NIST.SP.800-101r1
11. Owen, P. and Thomas (2011), P., An analysis of digital forensic examination: Mobile devices versus hard disk drives utilising ACPO and NIST Guidelines, *Digital Investigation*, 8, Elsevier, pp.135-140, http://dex.doi.org/10.1016/j.diin.2011.03.002
12. SWGDE (2004), SWGDE Recommended Guidelines for Developing Standard Operating Procedures, https://www.swgde.org/
13. SWGDE-1 (2013), SWGDE Best Practices for Mobile Phone Forensics, https://www.swgde.org/
14. SWGDE-2 (2013), SWGDE Core Competencies for Mobile Phone Forensics, https://www.swgde.org/
15. Yusoff, Y., Ismail, R. and Hassan, Z. (2011), Common phases of computer forensics investigation models, *International Journal of Computer Science & Information Technology* (IJCSIT), Vol 3, No 3.
16. Zarouni, A. (2007), Introduction to Mobile Phone Flasher Devices and Considerations for their Use in Mobile Phone Forensics, *Australian Digital Forensics Conference*, http://ro.ecu.edu.au/adf/16/