Marco de trabajo estandarizado para el análisis forense de la evidencia digital

Byron Gustavo Loarte Cajamarca [1], Grijalva Lima Juan Sebastián [2]

1 Escuela Politécnica Nacional-Ecuador, by_tosh20@hotmail.com

2 Universidad Internacional SEK-Ecuador, sebastian.grijalva@uisek.edu.ec

RESUMEN

El crecimiento exponencial de las Tecnologías de la Información ha permitido ser una herramienta más para el cometimiento de diversos delitos informáticos.

La información almacenada digitalmente pasa a tener mayor relevancia como evidencia en un procedimiento penal o civil derivando en Pericias Informáticas muy específicas y complicadas en la obtención de la evidencia.

Una de las mayores problemáticas es la falta de un proceso que guie a los Peritos Informáticos en la aplicación de técnicas, métodos y buenas prácticas asegurando que realizaron todas las tareas encomendadas con los mecanismos adecuados enmarcados en la normativa legal vigente.

Ante este panorama tan complejo se propone elaborar un marco de trabajo estandarizado para el análisis forense, sustentado en normas, estándares, herramientas y buenas prácticas emitidas por organizaciones internacionales especializadas en el área de Informática Forense complementándola con la normativa legal vigente, para que de esta manera la evidencia sea aceptada legalmente en un tribunal con elementos claros, contundentes y útiles.

Palabras claves: análisis forense, informática forense, perito informát**ico**

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

Standardized framework for the forensic analysis of digital evidence

ABSTRACT

The exponential growth of Information Technology has allowed to be an additional tool for the commission of various computer crimes.

The digitally stored information becomes more relevant as evidence in a criminal or civil procedure deriving in highly specific and complicated computer skills in obtaining the evidence.

One of the major problems is the lack of a process that guides IT experts in the application of techniques, methods and good practices ensuring that they performed all the tasks entrusted with the appropriate mechanisms within the current legal framework.

Given this complex scenario, it is proposed to develop a standardized framework for forensic analysis, based on norms, standards, tools and good practices issued by international organizations specialized in Forensic Informatics, complementing it with the current legal regulations, so that this Evidence is legally accepted in a court with clear, compelling and useful elements.

Keywords: Forensic analysis, computer forensics, digital forensic expert

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

1. INTRODUCCIÓN

A Pericia Informática en dispositivos de almacenamiento electrónicos digitales o que a su vez estos han sido procesados electrónicamente en un medio computacional es uno de los servicios que habitualmente se ofrece en el ámbito de la actividad profesional de un Perito Informático.

El Perito Informático es el responsable de recoger y preservar la evidencia digital, aplicando normativa legal, técnicas, herramientas, entre otras, que el considere las más apropiadas sustentadas de manera técnica y científica, sin embargo en la actualidad muy pocos Peritos Informáticos acreditados por el Consejo de la Judicatura poseen los conocimientos legales y técnicos de lo que realmente se debe realizar en un Análisis Forense.

El objetivo de este proyecto fue establecer un marco de trabajo estandarizado para el correcto Análisis Forense de la evidencia digital en procesos penales y civiles en el Ecuador. El cual se desarrolló en base a una metodología seleccionada componiéndose con varias Fases y sub-fases, detallando los procedimientos, técnicas, mejores prácticas que se deben realizar en cada una de ellas como por ejemplo: recomendaciones que debe tener en cuenta en la preservación de la evidencia, herramientas y técnicas de software como de hardware válidas para la adquisición de la evidencia si el equipo esta encendido o apagado, métodos adecuados para el almacenamiento, etiquetado y transporte de la evidencia, consideraciones mínimas para redactar el informe pericial, el análisis de la evidencia en equipos informáticos como en dispositivos móviles, habilidades y destrezas para sustentar oralmente sus resultados obtenidos durante la investigación y finalmente las consecuencias legales que pueden tener sus actos u omisiones para evitar realizar una mala práctica, que lo pueda llevar a ser acusado con las implicaciones legales que esto conlleva.

Permitiendo de esta manera a las autoridades competentes confiar en las tareas desarrolladas por los Peritos Informáticos acreditados por el Consejo de la Judicatura, y así enriquecer la capacidad de juzgar en un delito que tenga elementos informáticos.

A. Las tecnologías de la información y la informática forense en la actualidad

En la actualidad con el uso de las Tecnologías de la Información pasamos de un modelo de economía donde la principal riqueza se encontraba en los bienes tangibles, a una

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

economía donde la riqueza está dada por el acceso a la información. Información que es de vital importancia en el desarrollo de la vida cotidiana y laboral.

Hoy en día, más y más personas utilizan computadoras y medios de comunicación por ejemplo (teléfonos móviles, correo electrónico e internet) que inadvertidamente colocan una gran cantidad de información y realizan transacciones en repositorios informáticos y sitios web que fácilmente podrían ser violentados y/o vulnerados con diferentes tipos de ataques como: fraudes financieros en la web, infección con malware, ataques de denegación de servicio (DoS), phishing, entre otros, debido a esto las computadoras y las redes de comunicación se han convertido en la principal herramienta para el cometimiento de un delito informático [1].

Cabe mencionar que las organizaciones sufren frecuentemente ataques de diversos tipos a sus sistemas de información por ejemplo: Kaspersky Lab, en su portal web Secuelist ofrece información actualizada y completa sobre aquellas amenazas de Internet que están activas, una de sus publicaciones “Desarrollo de las amenazas informáticas en el tercer trimestre de 2016” [2] expone los programas maliciosos en Internet y los principales ataques mediante la web.

Ofreciendo estadísticas trimestrales del año 2016 en base a los incidentes de seguridad de múltiples organizaciones alrededor del mundo. Pero no solo organizaciones como la banca, comercio y entidades del Estado, entre otros sectores, se ven afectados por este tipo de delitos informáticos, si no que un número considerable de ciudadanos comunes también se ven afectos por estos incidentes.

En el Ecuador el Código Orgánico Integral Penal (COIP) sancionan los delitos informáticos, cuyos actos se comenten con el uso de tecnología para violentar la integridad, confidencialidad y disponibilidad de los datos personales. Estos actos que se registran a través de la Internet pueden ser: fraude, chantaje, extorsión, robo, falsificaciones, suplantación de identidad, espionaje, clonación de tarjetas de crédito, pornografía infantil, entre otros, principalmente crímenes donde se ha utilizado la tecnología [3].

Sin embargo, para conocer qué fue lo que realmente sucedió, cómo pasó, quien lo realizó, desde donde lo realizó y que buscaba obtener; estos cuestionamientos únicamente los puede responder el Análisis Forense Informático.

B. La informática forense y su papel en el área civil y penal

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

La informática forense está adquiriendo una gran importancia dentro de procedimientos civiles y penales permitiendo el esclarecimiento de grandes crímenes, como también en el área de la información electrónica, debido al aumento del valor de la información y/o al uso que se le da a ésta a diario.

En el Ecuador una gran cantidad de casos necesitan ser investigados por las autoridades competentes, los cuales en su gran mayoría no pueden ser atendidos ya que necesitan ciertos conocimientos ajenos a su saber específico y requieren ser auxiliados por personas con conocimientos, procedimientos establecidos y reconocidos legalmente, conocimientos que únicamente especialista en informática forense posee, con el fin de enriquecer la capacidad de juzgar en un procedimiento Penal (COIP) o Civil (COGEP) este último regula la actividad procesal en todas las materias, excepto la constitucional, electoral y penal, con estricta observancia del debido proceso [4].

C. Estado del arte del perito informático forense

Un Perito Informático (especialista en informática forense) es aquel profesional con conocimientos legales y técnicos en el área de las Tecnologías de la Información, quien con sus conocimientos y basándose en el análisis profundo de los elementos informáticos proveerá información u opinión a los administradores de justicia; para que adquieran un grado de conocimiento y así determinar las circunstancias de cómo se cometió el delito informático.

El Artículo 178 de la Constitución de la República del Ecuador establece que “El Consejo de la Judicatura es el órgano de gobierno, administración, vigilancia y disciplina de la Función Judicial” [5].

1. Resolución 040-2014

Esta resolución es el Reglamento del Sistema Pericial Integral de la Función Judicial, aprobado por el Pleno del Consejo de la Judicatura, el pasado 10 de marzo de 2014. Este reglamento ha sido modificado mediante el Consejo de la Judicatura el cual resolvió: “EXPEDIR EL REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL” [6]. Permitiendo regular el funcionamiento y administración del Sistema Pericial, en relación a la calificación, designación, obligaciones, evaluación y cualquier otro aspecto que tenga relación con los peritos que participen en los procesos judiciales, pre procesales, o de cualquier otra naturaleza que se lleven a cabo en la Función Judicial.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

2. Sistema automático de trámite judicial ecuatoriano "SATJE"

"SATJE " es un sistema donde se encuentran registrados todos los peritos acreditados por el Consejo de la Judicatura, ubicándolos en un catálogo de Especialidades.

El proceso de selección del perito es un proceso aleatorio que garantiza una igual distribución o asignación de peritajes entre todos los profesionales registrados en la base de datos.

3. Requisitos de acreditación de Peritos Informáticos

Los requisitos que deben cumplir las personas para calificarse como Perito Informático están reglamentados en el Artículo 18 de la Resolución 040- 2014 [7] del Reglamento del Sistema Pericial Integral de la Función Judicial, según el cual estos son:

--Ser mayor de edad.

--Deben ser expertos en la profesión, arte, oficio, o actividad para cual soliciten calificarse.

--En caso de ser profesionales, deben tener al menos dos (2) años de graduadas o graduados. Para los demás expertos tener al menos dos (2) años de práctica y experiencia en el oficio arte o actividad.

--Finalmente, no encontrarse incursas o incursos en las inhabilidades o prohibiciones para ser calificada o calificado como Perito previstas en la ley y mencionadas en este reglamento.

4. Especialidades de Peritos Informáticos

Un Perito Informático puede calificarse en las siguientes especialidades:

--Criminalística Informática: Siempre y cuando se otorgué una capacitación por afinidad que será avalado por la Policía Nacional.

--Ingeniería Informática o de Sistemas: Requiriendo su título de profesión debidamente aprobado por la SENECYT.

5. Otorgamiento del certificado de Perito

Una vez que el profesional ha cumplido con todos los pasos y requisitos establecidos en el Reglamento del Sistema Pericial Integral de la Función Judicial, la Dirección Provincial del Consejo de la Judicatura correspondiente procederá:

1) Entregar el certificado o identificación de calificación de Perito del Consejo de la Judicatura con una validez de dos (2) años, con la siguiente información:

--Nombres y Apellidos completos;

--Numero de cedula de ciudadanía;

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

--Numero de código de calificación;

--Tiempo de vigencia; y,

--Área y especialidad a las que corresponde la calificación.

2) Asignar un código al Perito calificado, y abrir un expediente personal en el sistema informático pericial, para su evaluación y seguimientos de sus actuaciones posteriores en el ejercicio de actividad pericial.

6. Obligaciones y derechos de los Peritos Informáticos

A. Obligaciones

El Artículo 18 de la Resolución 040- 2014 [7] menciona como obligaciones generales que un perito debidamente calificado debe cumplir: desempeñar su función de auxiliar de la justicia con objetividad, imparcialidad, responsabilidad, oportunidad, puntualidad, rectitud, corrección, honestidad y que su trabajo deberá enmarcarse en todo momento en la ética, junto con la presentación de su criterio técnico y especializado, exento de juicios de valor de ningún tipo.

De igual manera el Artículo 19 de esta Resolución [7], establece las obligaciones específicas que el perito de cumplir, dentro de las que se mencionan:

--El perito debe asistir obligatoriamente cuando es convocado dentro de un proceso judicial.

--Posesionarse obligatoriamente una vez que han sido designados.

--Presentar el informe pericial correspondiente en la forma, plazos y términos previstos por la normativa o por la autoridad judicial correspondiente.

--Explicar y defender el informe presentado con sus respectivas conclusiones.

--Presentar conjuntamente con su informe en todos los procesos judiciales, una copia de la factura de honorarios.

--Aprobar todos los cursos de capacitación y cualquier otra obligación.

--El Perito está en la obligación de realizar y terminar las pericias a su cargo, en caso de que haya sido excluido en su calidad de tal.

--El perito debe exponer su informe en la audiencia convocada y contestar las preguntas realizadas por el juez, las partes o el fiscal, dependiendo de cada caso. Tanto la exposición como las preguntas deben referirse a aspectos técnicos contenidos en el informe.

--El perito mediante su informe no puede emitir juicios de valor, ni a favor ni en contra de ninguna de las partes, su alcance es exclusivamente técnico.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

B. Derechos

El Artículo 24 de la Resolución 040- 2014 [7] menciona que los Peritos tienen derecho de percibir honorarios por la actividad pericial que desarrollen tanto en los procesos judiciales y/o pre procesales, los cuales serán pagados por el Consejo de la Judicatura, o por las partes interesadas, según sea el caso.

D. Fases del proceso pericial

El Perito Informático acreditado, deberá estar al tanto de cuál es su ámbito de acción y cuáles son las fases del proceso pericial, las mismas que están establecidas en el Reglamento del Sistema Pericial Integral de la Función Judicial [7].

La autoridad competente ordenará la designación de un perito calificado con determinada experticia y conocimiento dentro de un proceso para la investigación de un determinado delito informático, especificando la necesidad de la experticia teniendo en cuenta que:

Si es un procedimiento Civil se debe seguir este proceso como se ilustra la Fig. 1.

Si es un procedimiento Civil se debe seguir este proceso como se ilustra la Fig. 1.

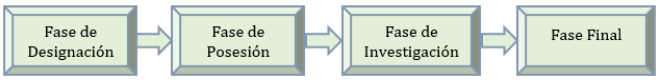

Fig. 1. Fases de un proceso pericial para procedimiento Civil

Sin embargo si es un procedimiento Penal se debe seguir este proceso:

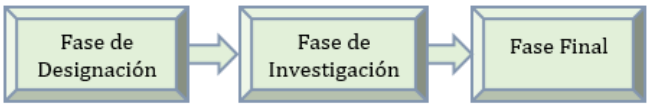

Fig. 2. Fases de un proceso pericial para procedimeito Penal.

Mediante la Resolución 067-2016 en su Artículo 12 [6] suprime la Fase de Posesión como se observa en la Fig. 2.

1. Fase de Designación

El Artículo 12 de la Resolución 040-2014 [7] señala que la designación de Peritos tanto en procesos judiciales o pre procesales de la Función Judicial, serán realizados por las y los jueces, mediante un sorteo en el SATJE. Respetando siempre los principios de profesionalidad, especialidad, transparencia, alternabilidad e igualdad.

Sin embargo, las partes procesales podrán solicitar la designación de Peritos de forma directa de una persona experta o experto específico, teniendo en cuenta que los Peritos seleccionados de esta forma tienen que estar previamente calificados, y deberán cumplir con todas las obligaciones y deberes.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

Independientemente de la forma en la que el Perito haya sido designado será registrado en el SATJE dejando constancia del código de calificación, como lo establece el Artículo 13 de la Resolución 040- 2014 [7].

Cabe mencionar además que el Artículo 13 de dicho reglamento [7] establece que en caso que un Perito no acepte su designación injustificadamente, el juez o el fiscal competente registrarán este inconveniente a través del SATJE, y designará inmediatamente un nuevo Perito.

2. Fase de Posesión

En el caso de que fuera un procedimiento Civil se debe realizar la respectiva posesión del Perito Informático designado para realizar su experticia [4].

3. Fase de Investigación

Con respecto a la fase de investigación, el Perito Informático debidamente acreditado utilizará su experticia para realizar el análisis forense y encontrar información relacionada con el cometimiento del delito informático.

2. METODOS

Se enuncian los métodos de investigación utilizados durante la investigación.

Este marco de trabajo se lo realizará utilizando la normativa legal vigente, metodología, estándares y guías de mejores prácticas para el análisis forense.

Existen varias metodologías para el análisis forense propuesto por algunos autores como:

--Modelo según la Norma UNE 71506:2013, de AENOR[1].[8]
--Modelo según Francisco Lázaro Domínguez en su libro introducción a la Informática Forense [9]
--Modelo según el NIST[2], en su Special Publication 800-86 [10]
--Modelo según DFRWS[3] (2001), en su informe técnico que lleva por título A Road Map for Digital Forensic Research [11]
--Modelo según IDIP[4] (2003), propuesto por Carrier y Spafford [12]

Todas estas metodologías tienen sus fases bien diferenciadas reflejando en cada una de ellas los mismos principios básicos. Por ello cualquiera de estas metodologías son aplicables a un análisis forense, sin embargo se podría escoger entre una de ellas dependiendo de las necesidades que se requiera, ya que algunas tienden a ser muy generales y otras más específicas.

[1] AENOR: Asociación Española de Normalización y Certificación
[2] NIST: Instituto Nacional de Normas y Tecnología
[3] DFRWS: Taller Digital de Investigación Forense
[4] IDIP: Proceso de Investigación Digital Integrado

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

Para el desarrollo del presente marco de trabajo, se decidió implementar la siguiente metodología propuesta por la UNE 71506:2013. Ya que es bastante completa para el manejo de evidencias digitales, no obstante será complementado con la normativa vigente para garantizar la admisibilidad en los tribunales y no ser vulnerable a una objeción de descalificación; La Fig. 3 ilustra la metodología propuesta.

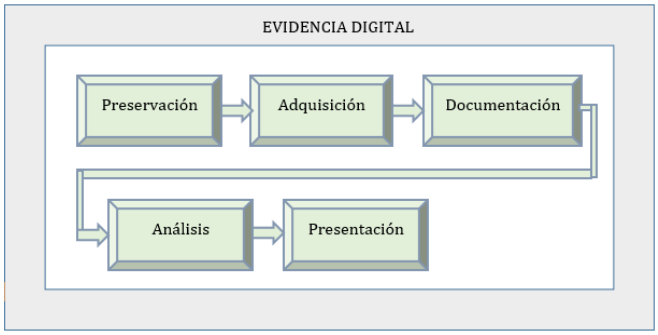

Fig. 3. Metodlogia UNE: 71505:2013.

3. RESULTADOS

A continuación se detallan las distintas fases.

1. Fase de Preservación

En esta fase la prioridad es asegurar la integridad de la evidencia original en la escena del delito, es decir, no se debe realizar modificaciones, alteraciones o destrucción sobre dicha evidencia.

Para lo cual se elaboraron sub-fases enmarcadas en la escena del delito como se ilustra en la Fig. 4.

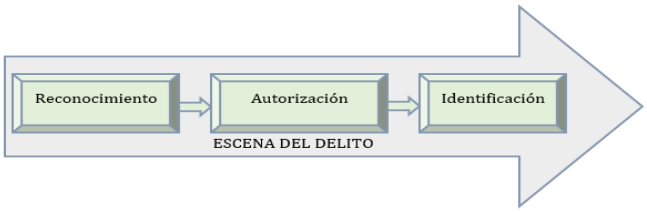

Fig. 4. Sub-fases de la Fase de Preservación.

a. Sub-fase de reconocimiento

Los Peritos Informáticos realizarán las respectivas diligencias de reconocimiento del lugar de los hechos en territorio digital, servicios digitales, medios o equipos tecnológicos, preservando en todo momento la escena del delito para evitar que se realicen modificaciones o destrucciones de la evidencia digital existente con lo mencionado en el Artículo 460 del COIP (Código Orgánico Integral Penal) sobre el reconocimiento de los hechos [3].

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

b. Sub-fase de autorización

Antes de iniciar su experticia y encontrar información relacionada con el caso, los Peritos Informáticos deberán obtener una autorización por escrito por parte de la autoridad competente o las partes procesales, ya que en ciertos casos se debe romper claves de seguridad o investigar sobre archivos personales.

Sin esta autorización el análisis no tendría una validez legal y de hecho, se estaría cometiendo un delito según lo menciona el Artículo 178 del COIP sobre la violación a la intimidad [3].

El Artículo 292 del COIP [3] menciona además que la alteración o destrucción de vestigios de evidencias materiales u otros elementos de prueba, serán sancionadas con pena privativa de libertad de uno a tres años.

c. Sub-fase de identificación

Los Peritos Informáticos efectuarán la identificación sobre 2 tipos de evidencia digital:

- Evidencia electrónica.- Comúnmente será todo elemento material de un sistema informático o hardware, este último refiriéndose a todos los componentes físicos que lo integra.

- Evidencia digital.- Es toda la información obtenida en un sistema informático como puede ser datos, programas almacenados y mensajes transmitidos para su posterior análisis y puedan ser presentadas como evidencias.

Es crucial efectuar este análisis, ya que de esto dependerá que los procedimientos se realicen de manera adecuada para cada tipo de evidencia, a fin de encaminar correctamente el análisis forense.

Es importante mencionar además que el marco de trabajo propuesto se enmarca en la evidencia digital proporcionando al Perito Informático los métodos más adecuados para su posterior recolección y almacenamiento.

En esta sub-fase de identificación es necesario mencionar algunas consideraciones o reglas para que la evidencia sea admisible.

1) Llevar indumentaria adecuada para evitar descargas electrostáticas.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

2) Evitar contaminarla con software que no garantice un proceso limpio.
3) Alejar a todas las personas no autorizadas de la escena.
4) Mantener el estado de los dispositivos si están encendidos, no apagarlo y viceversa.
5) Identificar los equipos afectados, que pueden ser equipos informáticos o a su vez dispositivos de almacenamiento.
6) Realizar una evaluación de las herramientas de software, hardware y procedimientos que se van a utilizar sobre el equipo afectado a analizar.
7) Asegurar que todo el proceso que se realice en esta sub-fase debe ser claramente documentado.

Como recomendación final se debe tomar todas las precauciones necesarias para minimizar la posibilidad de contaminar de la evidencia accidentalmente.

2. Fase de Adquisición

Según la metodología propuesta se debe realizar en esta fase de adquisición un clonado a bajo nivel de los datos originales del soporte de almacenamiento de datos, para lo cual se tomara de guía el RFC 3227 (Directrices para la recopilación de evidencias y su almacenamiento) [13], son directrices que contienen las mejores prácticas relacionado durante la recolección de evidencia y su almacenamiento.

Por lo mencionado anteriormente se elaboraron sub-fases enmarcadas en la evidencia original como se ilustra en la Fig. 5.

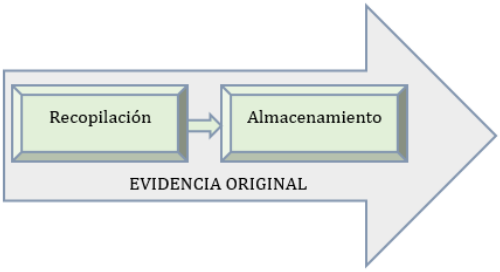

Fig. 5. Sub-fases de la Fase de Adquisición.

a. Sub-fase de recopilación

El primer paso es verificar el estado del equipo, si este se encuentra encendido o apagado, debido a que los procedimientos de recopilación serán diferentes para mantener la integridad de la evidencia original.

Es importante determinar el escenario del equipo:

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

- **Equipo apagado**

No prender el equipo, siempre debe estar apagado, ya que si se lo prense se puede alterar la evidencia.

Por norma, no se debe trabajar con la evidencia original del soporte de almacenamiento de datos sino con una copia a bajo nivel del mismo comúnmente llamado imagen forense; para realizar la copia se debe utilizar medios forenses estériles, empleando para ello herramientas de software especial que asegure que la evidencia no sea contaminada.

Cuando se realiza una imagen completa del soporte de almacenamiento de datos esta incluye todas las particiones, los espacios de disco duro sin utilizar entre las mismas, el sector de arranque e incluso zonas reservadas como HPA[5] y la DCO[6], toda esta información será útil para analizar el contenido de los mismos y otras tareas de investigación, detallando lo mencionado en la Fase de análisis.

Existen procedimientos tanto de software como de hardware que permiten la adquisición de una imagen forense.

- *Procedimiento por Software:* las herramientas que se muestran en la Tabla I se han convertido principalmente en un estándar de referencia en el campo de la Informática Forense.

TABLA I
HERRAMIENTAS DE SOFTWARE PARA ADQUISICIÓN DE LA IMAGEN FORENSE

	Herramienta	Distribución
Herramientas para Soporte de Almacenamiento de Datos	ENCASE	Propietario
	F-RESPONSE	Propietario
	FORENSICTOOLKIT(FTK)	Propietario
	HELIX	Libre
	DFF(DIGITAL FORENSIC FRAMEWORK)	Libre
	DEFT(DIGITAL EVIDENCE & FORENSIC TOOLKIT)	Libre
	DCDD3	Libre
	GUYMAGER	Libre
	LINRES	Libre
	(AIR)AUTOMATED IMAGE AND RESTORE	Libre

Independientemente del software que se utilice es recomendable es recomendable utilizar un bloqueador de escritura como por ejemplo Tableau Ultrablock FireWire Kit, forzando a que el soporte de almacenamiento de datos funcione solo en modo lectura y no en escritura.

[5] HPA: Área protegida del anfitrión.
[6] DCO: Superposición de la configuración de datos.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

- *Procedimiento por Hardware:* existen dispositivos dedicados a la copia completa del soporte de almacenamiento de datos, como los que se muestran en la Tabla II.

TABLA II
HERRAMIENTAS DE HARDWARE PARA ADQUISICIÓN DE LA IMAGEN FORENSE

	Herramienta	Descripción
Herramientas de Hardware	Tableau T8u USB 3.0 Forensic Bridge Kit	Ideal para prevenir la escritura sobre aquellos dispositivos de almacenamiento
	Forense UltraDock v5.	
	Wiebetech Media WriteBlocker	
	Wiebetech Forensic UltraDock	
	Wiebetech Ditto Forensic FieldStation	
	Paraben Mobile Field	

Una vez obtenida la imagen forense se debe proceder a calcular el Hash de la información extraída. El Hash son algoritmos de cifrado que realiza una operación matemática sobre el conjunto de datos de cualquier longitud y su salida es un número hexadecimal de 32 dígitos, básicamente la salida es una huella digital única para cada conjunto de datos cifrado.

NIST publicó la versión final del algoritmo de Hash SHA-3 siendo una herramienta de última generación para asegurar la integridad de la información.

El procedimiento habitual consiste en hacer en primer lugar un Hash del soporte de almacenamiento de datos original donde se encuentra la evidencia original. Acto seguido se obtiene otro Hash de la imagen forense extraída. Es importante mencionar que los dos Hashes deben ser iguales.

Es importante que acompañe al Perito en este proceso de recopilación otra persona, que actúe como testigo de las acciones realizadas, de preferencia una autoridad competente.

Una regla importante es documentar toda la información sobre el soporte de almacenamiento de datos o si este se encuentra alojado en un equipo, números de serie, hora de inicio y de fin de cada uno de los procedimientos que se realicen, etc., de preferencia siempre es recomendable tomar una fotografía de lo mencionado anteriormente.

Si se realizó los procedimientos mencionados anteriormente de manera adecuada se garantizará la integridad de la evidencia y no podrá ser descartada como medio probatorio.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

- **Equipo encendido**

Es importante que la recopilación de la evidencia se realice siguiendo el orden de mayor a menor volatilidad de la información.

El orden de volatilidad se enmarca al período de tiempo donde cierta información es accesible, es por eso que se debe hacer la recopilación de la información que va a estar durante un tiempo menor, es decir cuya volatilidad sea mayor.

Se establecerá el siguiente orden de volatilidad según lo establecido en el RFC 3227 [13] al momento de realizar la recolección de evidencias.

- Registros y contenidos de la caché.
- Contenidos de la memoria.
- Estado de las conexiones de red, tablas de rutas.
- Estado de los procesos en ejecución.
- Contenido del sistema de archivos y de los discos duros.
- Contenido de otros dispositivos de almacenamiento.

Se tomará como prioridad los 4 primeros puntos, ya que si por algún error involuntario se reinicia o se apaga el equipo podría modificarse o perder toda la información.

De igual manera es de vital importancia recuperar información del sistema en tiempo real como:

- Fecha y hora.
- Procesos activos.
- Conexiones de red.
- Puertos TCP/UDP abiertos.
- Usuarios conectados remota y localmente.

Por lo mencionado anteriormente se listan algunas recomendaciones que se podrían tomar en cuenta si el equipo se encuentra encendido:

- Si lo apaga, se puede bloquear el equipo por alguna contraseña.
- Sellar todas las entradas y salidas del equipo.
- Sellar todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

- Sellar todos los tornillos del equipo para evitar que se puedan reemplazar o retirar piezas internas.
- Revisar los dispositivos de almacenamiento removibles. (Algunos equipos contienen en su interior dispositivos de almacenamiento removibles tales como tarjetas SD, Compact flash, Tarjetas xD[7], Memory Stick[8], etc.)

Es importante mencionar que no se debe apagar el equipo, ya que se puede perder información oculta como: memoria RAM[9], conexiones de red activas, usuarios conectados remota y localmente, procesos que se estén ejecutando, sistema de archivo, etc., siendo muy difícil de volver a reunir toda esta información, si se decide apagar el equipo.

El atacante puede dejar instalando herramientas o scripts que podrían modificar, sustituir y eliminar archivos; sin embargo en el peor de los casos puede ser que el atacante siga on-line y detecte nuestra presencia y actué con una acción evasiva o, peor aún, destructiva eliminando todo tipo de información.

Si la información es gravemente comprometida por la severidad del ataque el equipo debe ser apagado sin dudarlo. Se puede perder información volátil de la memoria RAM, micro, etc. Pero se conservará información y útil sobre el ataque.

En este punto es donde se debe proceder a recopilar toda la información volátil del sistema para lo cual se podría emplear un script en Perl[10] para sistemas UNIX/Linux o un archivo de proceso por lotes para sistemas Windows para que realice el proceso de copiado de forma automatizada.

Otra opción es emplear herramientas de trasmisión de datos por la red tipo netcat[11] o dcfldd[12], enviando la información a una portátil conectado en la misma red o a su vez directamente a la portátil conectada directamente con el equipo afectado.

Una vez obtenida la imagen forense se debe proceder a calcular el Hash de la

[7] Tarjetas xD: Es un tipo de tarjeta de memoria creada por Fuji y Olympus, basada en los circuitos de memoria flash de tipo NAND

[8] Memory Stick: Son un tipo de familia memoria flash removible, lanzadas por Sony en octubre de 1998

[9] Memoria RAM: Memoria principal de la computadora, donde residen programas y datos.

[10] Perl: Es un lenguaje de programación que toma características del lenguaje C, del lenguaje interpretado bourne shell (sh).

[11] Netcat: Es un comando en los sistemas operativos Linux cuyo proposito principal es la adquisión de la imagen forense.

[12] Dcfldd: Herramienta para la adquisión de una imagen forense.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

información extraída.

Si estamos manipulando dispositivos móviles debemos tener precaución de que no entren en contacto con redes inalámbricas, evitando manipular los datos contenidos dentro de ellos. Por consiguiente se debe poner el dispositivo en modo avión, de esta forma se evita que se pueda conectar a las redes celulares e inalámbricas.

La imagen forense del dispositivo móvil puede obtenerse por medio de una herramienta de software con dd y netcat o a su vez se puede utilizar kits forenses como el Cellebrite UFED, un excelente kit especializado en el análisis de dispositivos móviles.

Si se realizó los procedimientos mencionados anteriormente de forma adecuada se garantizará que la recolección de la evidencia se efectuó de manera transparente e integra.

b. Sub-fase de almacenamiento

Una vez obtenida la imagen forense, es fundamental definir métodos adecuados para el almacenamiento y etiquetado de las evidencias. Este proceso es comúnmente llamado "cadena de custodia".

Para la elaboración de estos métodos se tomara de guía estándares para el manejo y almacenamiento de la evidencia digital como son: el RFC 3227[13], ISO 27370[14], Modelo Extendido de Séamus Ó Ciardhuain.

El Perito Informático deberá aplicar la respectiva cadena de custodia a elementos físicos o contenido digital materia de prueba, garantizando la autenticidad, acreditando su identidad y estado original como lo menciona el Artículo 456 del COIP [3].

Sin embargo hay que tener claro que la cadena de custodia inicia en el lugar donde se obtiene o encuentra el elemento de prueba.

Para poder iniciar con el proceso de cadena de custodia se debe contar con la presencia de la autoridad competente. Este proceso puede ser aplicado según lo mencionado en el Artículo 482, inciso uno y tres del COIP [3].

La cadena de custodia debe realizarse de la siguiente manera:

1) Manejo del lugar de los hechos

El área debe ser aislada y acordonada, toda actividad debe ser claramente documentada. Se debe realizar una eficaz investigación en la búsqueda de elementos materia de prueba o evidencias físicas.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

2) Fijación del lugar de los hechos

Se debe realizar actividades que permitan la descripción detallada del lugar de los hechos y la localización de los elementos materia de prueba o evidencias utilizando técnicas establecidas que pueden ser fotografías, videos, imágenes, embalaje y rotulado entre otros. Todo lo mencionado puede ser aplicado según lo establece el Artículo 500, inciso cuatro del COIP [3].

3) Recolección de la evidencia

Este punto es crucial ya que se debe analizar el estado del equipo, aplicando las herramientas tanto de software como hardware se obtendrá la imagen forense según el orden de volatilidad. Se podrá aplicar cadena de custodia como lo menciona el Artículo 500, inciso dos y tres del [3].

4) Embalaje y rotulado de la evidencias

Registrar fotográficamente los equipos y sus conexiones antes de su embalaje, durante el embalaje y al finalizar el embalaje y rotulado. Para el sellado de los equipos se debe realizar con la cinta adecuada que brinden seguridad y preservación del mismo, para soportes de almacenamiento de datos se deben introducir en bolsas antiestáticas y posterior a ello ponerla en una caja de cartón o sobre manila cuyo interior se pueda rellenar con plásticos con burbujas u otro material protector. Previamente se debe imprimir alguna firma y número de documento de identificación sobre el contenedor en la parte de su cierre y sobre esta adhiera cinta de sello. Rotular de manera consecutiva cada uno de los elementos a ser incautados relacionados con la evidencia.

5) Transporte de la evidencia

Toda evidencia así como los elementos incautados debe ser transportada al laboratorio forense respectivo. La cadena de custodia se debe mantener meticulosamente durante el transporte.

6) Abrir el embalaje de la evidencia

El embalaje sólo podrá ser abierto por el Perito Informático para su estudio o análisis.

Si se realizó y se documentó correctamente los procedimientos mencionados anteriormente se garantiza la integridad, conservación e inalterabilidad de la evidencia. Como lo menciona el Artículo 457, del COIP [3].

3. Fase de Documentación

En esta Fase el Perito Informático debe tener todas las consideraciones mínimas para

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

redactar el informe pericial, de tal manera que todas las actividades realizadas desde la Fase de Preservación hasta la Fase de Análisis queden plasmadas en el documento, como lo establece el Artículo 511, inciso seis del COIP [3].

El Informe Pericial obligatoriamente debe ser presentado y subido al Sistema Informático Pericial, en archivo tipo PDF; el mismo que pueda ser descargado, conocido, estudiado por las y los interesados. Sus explicaciones o aclaraciones, se presentarán de forma verbal y/o escrita, de conformidad con la normativa procesal correspondiente. Como lo establece el Artículo 19 y 20 de la Resolución 040- 2014 [7].

El Informe Pericial traslada el conocimiento experto al proceso judicial, estableciendo para ello requisitos mínimos que no solo estandaricen la presentación, sino que exista un formato general como lo establece el Artículo 19 y 20 de la Resolución 040- 2014 [7], siendo claro y entendible para las autoridades competentes.

Los requisitos obligatorios de todo informe pericial son los siguientes:

a) Datos generales del juicio, o proceso de indagación previa

El Informe Pericial deberá contener los datos del juicio y la identificación del perito como requisito que tiene por objeto la determinación de la responsabilidad en caso de incumplimiento de obligaciones.

b) Parte de antecedentes

En este punto se debe delimitar claramente el encargo realizado, esto significa, se tiene que especificar el tema sobre el que informará en base a lo ordenado por la autoridad competente y/o lo solicitado por las partes procesales. Cabe recalcar que es la guía que limita la intervención pericial, con la prohibición de efectuar juicios de valor.

c) Parte de consideraciones técnicas o metodología a aplicarse

Este punto es de suma relevancia ya que el Perito debe explicar claramente, cómo aplico sus conocimientos especializados de su profesión al caso. Deberá relacionar los contenidos de sus conocimientos y experticia con el objeto de la pericia encargada.

d) Parte de conclusiones

Es el fruto del conocimiento del Perito, es lo que idealmente servirá de fundamento para la decisión judicial. Después de las consideraciones técnicas las conclusiones que se redactarán en el informe serán claras, directas y solamente se referirán a los temas materia de la pericia debidamente delimitados y explicados en los antecedentes.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

e) Documentos de respaldo, anexos, o explicación de criterio técnico

El Perito deberá sustentar sus conclusiones ya sea con documentos y objetos de respaldo (fotos, láminas demostrativas, copias certificadas de documentos, grabaciones de audio y video, etc.).

El Perito claramente debe exponer y justificar desde todo punto de vista las razones especializadas para llegar a la conclusión correspondiente incluidas en el informe.

f) Otros requisitos

El Perito podrá incluir requisitos adicionales a los establecidos por el reglamento siempre y cuando la ley procesal correspondiente determine la inclusión de estos.

g) Información adicional

A más de las obligaciones mínimas mencionadas anteriormente el Perito podrá incluir también en el informe cualquier otro tipo de información adicional siempre y cuando se encuentren dentro de los límites del objeto de la pericia.

h) Declaración juramentada

El Perito deberá declarar bajo juramento que toda la información que ha proporcionado es auténtica, al igual que el informe es independiente y corresponde a su real convicción profesional.

i) Firma y rúbrica

Al finalizar el Informe Pericial deberá constar con la siguiente información: la firma y rúbrica del Perito, el número de cédula de ciudadanía, y el número de su calificación y acreditación pericial.

4. Fase de Análisis

Una vez que la imagen forense fue recopilada, almacenada y documentando correctamente todo el proceso. Comienza la fase de Análisis, en donde el Perito Informático mediante un examen detallado pondrá todos sus conocimientos en la búsqueda de vestigios de lo que se quiere encontrar.

El objetivo del análisis se enfoca principalmente en:

- Realizar la reconstrucción de la línea de tiempo, es decir, determinar la evolución de los hechos desde el instante anterior al inicio del ataque, hasta el momento de su descubrimiento.
- Llevar a cabo un examen detallado de los sistemas de archivos, detectar archivos sospechosos, realizar operaciones de búsqueda de caracteres, búsqueda de archivos

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

específicos, recuperación de información y ejecutar otras tareas de investigación.

Esta fase es de vital importancia y laboriosa, ya que por medio de la evidencia digital y del análisis que se realice aplicando procedimientos, herramientas y técnicas, se llegará a responder las interrogantes de quién, cómo, cuándo, y donde sucedieron los hechos.

Por lo mencionado anteriormente se elaboraron sub-fases. Teniendo en cuenta que el análisis únicamente lo debe realizar en el Laboratorio Forense como se ilustra en la Fig. 6.

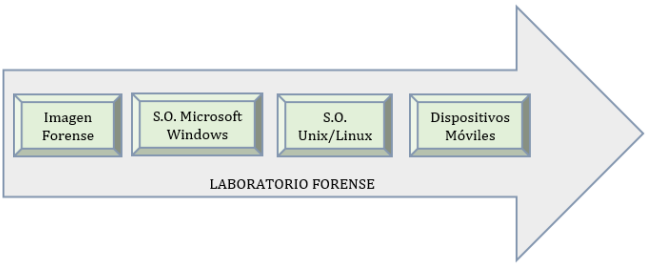

Fig. 6. Sub-fases de la Fase de Análisis.

a. Análisis de una imagen forense

Antes de realizar un análisis se debe seguir una metodología basada en niveles de funcionamiento, muy similar al modelo de capas OSI de redes de informática. Permitiendo recolectar información en cada nivel como se ilustra en la Fig. 7.

Este es un enfoque propuesto por Brian Carrier en su publicación “Investigación Forense de Sistemas de Archivos” [15], puede ser aplicado para cualquier sistema de archivos y tecnología de soporte de datos.

Para el análisis es importante la reconstrucción de la línea de tiempo y esto se logra recopilando información a través de la extracción lógica.

Este tipo de información es la que llevará más tiempo recopilar, pero actualmente existen muchas herramientas como por ejemplo The Sleuth Kit de distribución Libre, permitiendo que el análisis sea mucho más detallado y fácil de interpretar. La idea es encontrar información eliminada en rutas poco comunes y que es desapercibida por una persona común.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

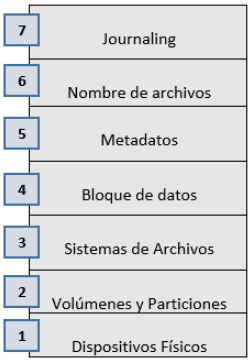

Fig. 7. Niveles de Análisis de una imagen forense.

1) Recuperación de archivos eliminados

La recuperación de archivos se puede realizar con una técnica denominada redireccionamiento, la cual permite introducir la salida de un comando como entrada de otro. Esta técnica está disponible en todos los Sistemas Operativos basados en línea de comando, como por ejemplo, Unix/Linux, MS-Windows y Mac OSX. Con lo cual garantizamos que el archivo generado contiene los mismos datos que el original.

2) Firmas características

¿Es posible saber de qué tipo es un archivo recuperado?

Sí, basta con examinar la firma característica del archivo mediante un editor hexadecimal, por ejemplo HxD[13], con lo cual se determinará el tipo de archivo y si en este no se utilizaron técnicas de ocultación.

3) Documentos

Los documentos de texto encontrados en el transcurso de una investigación pueden ser: Open Office (OOXML[14]), Open Document, Documentos RTF[15], Archivos MS-Office. Estos documentos tienen mucha importancia e interés no solo por su contenido sino porque alojan otro tipo de información en su interior. Toda esta información es llamada metadatos.

4) Archivos gráficos

Las imágenes encontradas en el transcurso de una investigación pueden ser: GIF[16], PNG[17], TIFF[18], Archivos JPEG[19], contienen metadatos que puede ser útiles al momento de recopilar información como: fecha y hora de cuando se tomó, modelo de la cámara y

[13] HxD: Potente y rápido editor Hexadecimal.
[14] OOXML: Es un formato de archivo abierto cuyas extensiones más comunes son .docx, .xlsx y .pptx.
[15] RTF: Es un formato de archivo informático para el intercambio de documentos multiplataforma
[16] GIF: Formato de Gráficos Intercambiable
[17] PNG: Gráficos de Red Portátiles
[18] TIFF: Formato de Etiquetado de Archivo de Imagen
[19] JPEG: Grupo Conjunto de Expertos en Fotografía

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

coordenadas geográficas (este último en dispositivos móviles equipados con cámara y GPS[20]), etc.

5) Multimedia

Los archivos multimedia encontrados en el transcurso de una investigación pueden ser: MPEG-1, WMV[21], MPEG-3 (MP3), ACC/M4A[22], contienen metadatos como: dimensiones de la imagen, caudal de datos en video y audio, etc.

6) Archivos ejecutables

Este tipo de archivos constituyen un caso especial, ya que al momento de analizar los metadatos se debe evitar que se ejecuten intencionalmente dañando con esto el sistema, para lo cual es recomendable trabajar en un entorno seguro que puede ser un sandbox[23], una máquina virtual o una plataforma aislada de hardware.

7) Data carving

La mayor parte de archivos antiguos se habrán perdido, debido a que el soporte de almacenamiento de datos se ha formateado o se sobrescribieron con nuevos archivos, pero gracias al datacarving se puede recuperar estos archivos antiguos.

b. Análisis de sistema operativo Microsoft Windows

Cuando el equipo a investigar contenga un Sistema Operativo Microsoft Windows es imprescindible recopilar toda la información posible en tiempo real (cuando el equipo esta encendido).

1) Fecha y hora del sistema

Es importante obtener la fecha y hora del sistema para poder comenzar a elaborar una buena línea de tiempo.

En una consola de comandos (cmd) de Windows se procede a teclear el siguiente comando:

- time
- date

2) Conexiones de red abiertas

En ocasiones suele suceder que los atacantes aún están conectados al equipo a investigar por medio de equipos remotos, esto se puede comprobar de la siguiente manera.

El siguiente comando:

[20] GPS: Sistema de posicionamiento global.
[21] WMV: Formato de Audio Digital
[22] ACC/M4A: Codificación de Audio Avanzada
[23] Sandbox: Es un mecanismo para ejecutar programas de seguridad y de manera separada.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

- netstat –n

Obteniendo información relacionada a conexiones que el sistema mantiene abiertas, indicando direcciones IP tanto locales como remotas, con lo cual se sabrá si alguien está accediendo al sistema desde una IP sospechosa.

3) Puertos TCP o UDP abiertos

El siguiente comando:

- netstat –n

Obtiene información de todos los puertos abiertos y si estos están en estado LISTENING (esperando por una conexión), ESTABLISH (conexión establecida) y CLOSE_WAIT / TIME WAIT (Cerrada).

4) Usuarios conectados al sistema

Se puede obtener información de si existen usuarios conectados al sistema, si están accediendo a recursos compartidos o realizando tareas de otro tipo.

Para ello se debe utilizar PSLoggedOn, perteneciente a la suite de herramientas PsTools.

5) Tabla de enrutamiento interna

El siguiente comando:

- netstat –rn

Obteniendo información de ruta sobre redes remotas y conectadas directamente, con se podría conocer si el atacante está desviando el tráfico de red para evadir cortafuegos o IDS[24].

6) Procesos en ejecución

Si además de los procesos normales del sistema y aplicaciones del usuario, existe algún otro proceso dejado por el atacante que pudiera ser sospechoso se debe utilizar Pslist, perteneciente a la suite de herramientas PsTools.

Pslist muestra un listado de procesos junto con sus números PID[25] correspondientes e incluso a detectar procesos que han sido creados con el mismo nombre de procesos legítimos del sistema.

7) Archivos abiertos

PsFile perteneciente a la suite de herramientas PsTools, muestra una lista de todos los archivos del sistema que han sido abiertos de forma remota.

[24] IDS: Sistema de Detección de Intrusos
[25] PID: Identificador del proceso.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

8) Papelera de reciclaje

Cuando alguien borra un archivo ya sea de forma accidental o intencionada estos se envían a la papelera de reciclaje y se genera un archivo llamado INFO2, el cual es invisible y no se muestra en un listado de directorio normal. Este archivo registra las rutas completas de los archivos que han sido eliminados.

El siguiente comando:

- dir/a

Se puede analizar directamente el contenido de este archivo.

Existen herramientas que permiten la visualización con una interfaz gráfica para el análisis y la interpretación, por ejemplo: Mount Image Pro y Rifiuti.

9) Historial de Internet

En la actualidad los ordenadores ya no se utilizan solo para tareas estáticas como: redactar informes, llevar contabilidad o solo como entornos de programación. Ahora con las telecomunicaciones, la Web, el acceso universal a Internet y conexiones de banda ancha, los usuarios emplean sus ordenadores para navegar por varias páginas en Internet y realizar diferentes tipos de actividad.

Los navegadores Web, como por ejemplo Internet Explorer, Firefox, Chrome, Opera o Safari conservan por defecto las páginas web que se visitan. Por consiguiente el lugar más aconsejable para iniciar una investigación es en el historial del navegador.

- Microsoft Internet Explorer: el archivo a analizar es index.dat, que contiene el historial de navegación con las páginas visitadas y otros elementos de interés. El archivo index.dat es de tipo binario pero su contenido puede ser examinado con la herramienta Pasco.
- Mozilla/Firefox: Es importante mencionar que este navegador guarda toda su información en bases de datos SQLite[26]. El archivo a analizar se llama profiles.ini el cual contiene archivos como: formhistory.sqlite, downloads.sqlite, cookies.sqlite y place.sqlite con toda la información sobre los historiales de navegación.
- Chrome: Al igual que Firefox, este navegador utiliza base de datos SQLite para poder organizar los datos que se generan por la actividad del usuario, siendo el archivo a analizar place.sqlite.

10) Correo electrónico

Otro de los objetivos del análisis forense es investigar el correo electrónico almacenado

[26] SQLite: Sistema de Gestión de Base de Datos.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

localmente en el equipo a través de un cliente de correo electrónico ya sea Outlook, Eudora, Opera Mail, Mozilla Thunderbird o cualquier otro tipo mediante protocolos POP3 o IMAP.

Los elementos de Outlook ya sean mensajes de correo electrónico, el calendario y demás elementos se conservan en un archivo de tipo .pst y .ost. Herramientas como PST-Viewer permiten analizar estos archivos.

Sin embargo, si es un cliente de correo basado en código libre el archivo a analizar es .mbx o .mbox que fácilmente pueden ser interpretados por un editor de texto.

11) Búsqueda de caracteres

El objetivo consiste en localizar texto revelador de las actividades delictivas llevadas a cabo por un sospechoso. Actualmente existen herramientas que emplean funciones para rastrear los sectores de un disco a bajo nivel en busca de cadena de caracteres. WinHex[27] permite realizar búsqueda por cadenas tanto de texto como de código hexadecimal.

12) Metadatos

Los metadatos de modo simplificado son datos que hacen referencia a otros datos constituyendo otra fuente de información de gran valor para el investigador forense. Cuando el usuario crea o edita documentos de cualquier tipo como: MS-Office[28], imágenes, Audio, etc., automáticamente está produciendo información sobre su actividad en el sistema.

FOCA es una herramienta útil ya que permite localizar metadatos en documentos de diversos formatos.

13) Registro de Windows

El análisis al Registro de Windows constituye un amplio campo para la investigación forense no solo por la gran cantidad de información almacenada, sino también por el tipo de información que se puede obtener analizando este Registro como: conocer si el sospechoso conecto un dispositivo USB, si se instaló algún tipo de aplicación, los últimos archivos abiertos, si el sistema está contaminado por algún tipo de malware[29]; constituyendo así esta información en elementos de evidencia el cual puede lograrse con el comando:

- regedit.exe

Sin embargo si el ordenador está apagado también puede obtener esta información con

[27] WinHex: Es un editor hexadecimal universal útil en el campo de la informática forense
[28] MS-Office: Es un paquete de programas informáticos desarrollado por Microsotf.
[29] Malware: Es todo tipo de programa malicioso.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

la herramienta Windows Registry Recovery de la empresa Mitec.

c. Análisis de sistema operativo Unix/Linux

En la actualidad un conocimiento sobre los sistemas Unix /Linux le va a permitir al investigador forense:

- Permitir montar su estación de trabajo sin las cuantiosas inversiones que requiere un software comercial.
- Beneficios a nivel operativo que puede ser: realización de imágenes in situ, técnicas de recuperación de archivos eliminados mediante técnicas de data carving, etc.
- Ofrecer nuevas oportunidades para el aprendizaje de la profesión por medio de: tecnología, herramientas, recursos y abundante documentación.
- Por lo mencionado anteriormente el conocimiento de Linux resulta imprescindible para moverse en números ámbitos de la investigación forense actual.

1) Montaje automático de particiones

Para comenzar el análisis forense, existen una amplia gama de distribuciones en la página web www.distrowatch.com y se puede elegir la más apropiada.

Es importante mencionar sobre el journaling, y lo que repercutiría en la integridad de la evidencia y la conservación de la cadena de custodia sino se toma las debidas precauciones al respecto.

Un sistema de journaling funciona a base de archivos auxiliares que registra de manera provisional el estado de una transacción ejecutada por el sistema de archivos (abrir, copiar, modificar o borrar un archivo). En otras palabras el montaje automático de una partición con journaling modifica datos, con lo cual el hash de un soporte de almacenamiento de datos montado con posterioridad a su adquisición forense no volverá a coincidir con el de la imagen realizada originalmente.

Para evitar este inconveniente del montaje automático de particiones con journaling (por ejemplo si se trata de sistemas de archivos NTFS[30], ext3[31], ReiserFS[32]) se sugiere:

- Al realizar una copia a bajo nivel deben realizarse a través de bloqueadores de escritura.

[30] NTFS: Sistema de archivos de Windows NT.
[31] Ext3: Sistema de archivos en distribuciones Linux
[32] ReiserFS: Sistema de archivos de propósito general diseñado por la empresa Namesys

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

- Desactivar udev[33], HAL[34] y d-messagebus [35]en los scripts de arranque de Linux

2) Marca de tiempo

Por medio de una marca de tiempo se puede determinar de qué manera un archivo ha sido manipulado en un ordenador a ser investigado.

La información que se puede obtener es: archivos escritos por última vez, si el archivo fue leído o ejecutado y si el archivo sufrió cambio en los metadatos de su inode [36]esto en Linux. Para el estudio de las marcas de tiempo debe hacerse desde una perspectiva crítica que no afecte a la integridad de la evidencia.

3) Información volátil

Para proceder con el análisis de un equipo en funcionamiento con sistema Linux se debe tener en cuenta:

- **Fecha y hora del sistema**

Esta información puede marcar un preciso límite para diferenciar entre manipulaciones realizadas por el sospechoso y de las que posteriormente se deriven en el análisis.

- **Puertos y conexiones abiertas**

Existe la posibilidad de que el sistema esté infectado por un rootkit cuando el sospechoso accedió al equipo de forma remota.

Posterior a ello se puede emplear una serie de comandos como se ilustra en la Tabla III para examinar las conexiones abiertas verificando si existe alguna dirección IP sospechosa. Para los cual se recomienda utilizar programas compilados estáticamente desde un CD[37] en lugar de herramientas locales del sistema.

TABLA III
HERRAMIENTAS PARA ADQUISICIÓN DE LA IMAGEN FORENSE

Comando	Descripción
ifconfig –a	Interfaces de red
netstat –anp	Conexiones de red activas
netstat –rn	Tabla de enrutamiento del kernel
Isof	Archivos abiertos por procesos en

- **Procesos en ejecución**

Al momento de obtener la lista de procesos es importante tener mucho cuidado con los

[33] Udev: Crear todo el sistema de nodos para la gestión de dispositivos
[34] HAL: Mantiene en memoria información sobre dispositivos conectados
[35] d-messagebus: Es un mecanismo que permite a las aplicaciones entran en comunicación e intercambiar datos unas con otras.
[36] Inode: Es una estructura de datos propia de los sistemas de archivo Unix/Linux.
[37] CD: Comunmente conocido como disco compacto, es un disco óptico para almacenar datos en formato digital.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

procesos parásitos ya que tienen la mala costumbre de camuflarse bajo los nombres de otros legítimos para confundir al investigador.

4) Adquisición forense

Una vez que ya se adquirió la información volátil, se procede a apagar el equipo pero no ejecutando el comando shutdown sino por el método tradicional en las investigaciones forenses cortando directamente la corriente del equipo.

Posterior a ello se puede emplear herramientas para realizar la adquisición de la imagen forense.

5) Línea de tiempo

TSK (The Sleuth Kit) está compuesto por un conjunto de herramientas que funcionan en línea de comando, en la actualidad TSK se encuentra incluido en todas las distribuciones Linux especializadas en seguridad informática, por ejemplo el comando fls permite la elaboración de una línea de tiempo a partir de la imagen forense mostrando un listado de archivos con sus marcas de tiempo.

6) Recuperación de archivos eliminados

Para obtener una lista de archivos eliminados en un directorio se puede recurrir a fls de TSK, posteriormente a ello se utiliza el comando icat para recuperar el archivo eliminado con el mismo grado de funcionalidad y las mismas características.

Con el comando file identifica el tipo de archivo y para examinar el contenido el comando strings.

7) Otras herramientas

Chrootkit y Rkhunter son scripts que utilizan comandos como strings o grep para localizar cadenas de texto sospechosas.

d. Análisis de dispositivos móviles

Es importante como en la actualidad y con el pasar de los años los dispositivos móviles se han convertido en el diario vivir de las personas.

El mercado de dispositivos parece estar en una etapa estandarizada de marcas reducidas como: Apple iOS, Android, Windows Mobile y BlackBerry. Todo apunta a un crecimiento exponencial con el pasar de los años ofreciendo ventajas significativas así como también muchos retos para la informática forense.

El análisis forense en dispositivos móviles no solo implica un examen detallado de la información que sea relevante y que pueda estar almacena, escondida y cifrada, sino también implica el uso de técnicas y procedimientos para la adquisición y análisis de la

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

información; con una base amplia de conocimientos sobre las plataformas y herramientas.

1) Información obtenible

El investigador forense sin problema puede rescatar información de la SIM[38], una lista de contactos, registro de llamadas, algunos SMS[39] y un poco más en un teléfono móvil antiguo. Con el pasar del tiempo el teléfono móvil amplió sus capacidades y una infinidad de posibilidades toda esta evolución de mejoras le facilitaron llegar a lo que es en la actualidad un smartphone.

Un smartphone almacena gran cantidad de información, por ejemplo: información referente a aplicaciones, historial de navegación web, Logs[40] y archivos de registro.

Esta información es el resultado de una exploración lógica por medio de un backup convencional del smartphone por medio del software de sincronización. Pero el investigador puede ir un poco más profundo en la exploración de información menos accesible con técnicas especiales.

2) Análisis de dispositivos apple iOS

Para mantener la integridad de la evidencia el análisis del dispositivo se realizará por medio de niveles algo similar al estudio de las redes informáticas

- Primer nivel: la extracción manual o visualización directa de los datos, para lo cual se debe tomar fotografías de toda la pantalla y de todas las operaciones realizadas.
- Segundo nivel: Se realizará lo siguiente poner el dispositivo en modo avión para evitar que se conecte a redes celulares e inalámbricas, luego proteger el dispositivo en una jaula de Faraday[41] que no permita un borrado remoto, finalmente se procede a la adquisición lógica con el software de sincronización o aplicaciones de transferencia de archivos desarrolladas por terceros.

Para la adquisición lógica este proceso suele ser automático pero se debe tener ciertas consideraciones para evitar la destrucción accidental de la evidencia si no se tiene en cuenta: el estado de las aplicaciones, mensajes de advertencia, descargar nuevas versiones del iTunes, sincronización de aplicaciones y otros parámetros de ajuste, caso contrario iTunes dejará intacto las copias de respaldo que hay en el dispositivo para realizar un nuevo backup.

[38] SIM: Es uan tarteja inteligente desmontable usada en teléfonos móviles para la identificación del abonado
[39] SMS: Servicio de mensajes cortos de texto
[40] Logs: Termino usado para la grabación secuencial de las actividades de un sistema en un archivo.
[41] Jaula de Faraday: Es una caja metálica que protege de los campos eléctricos estáticos.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

La adquisición física para un dispositivo iPhone u otras versiones del software iOS se utilizará herramientas de terceros que son: Oxygen Forensics, XRY, Lantern, Paraben Device Seizure o EnCase Neutrino.

Existe la posibilidad de utilizar dispositivos hardware como Cellebrite UFED (Universal Forensics Extraction Device).

- Tercer nivel: En este nivel de extracción física es mucho más exigente y sofisticado ya que consiste en la realización de una imagen forense del dispositivo. El procedimiento desarrollado por Jonathan Zdziarski, antiguo investigador de McAffee[42]. Requiere herramientas que deben ser descargadas de la página web de Zdziarski [16] permitiendo transferir al iPhone un agente de software capaz de crear y transferir la imagen forense al ordenador del investigador.
- Niveles superiores: Son niveles con procedimientos muy costosos en recursos económicos y tiempo en donde se deben aplicar técnicas que únicamente están al alcance de técnicos especializados, por ejemplo en microelectrónica[43].

3) Dispositivos android

El investigador forense primeramente deberá realizar una imagen forense a aquellos dispositivos móviles que disponen de un slot para tarjetas microSD o SD.

La extracción se lo realiza en base a procedimientos y herramientas mencionados anteriormente.

De igual manera se procede a la adquisición lógica con el ordenador del investigador, un cable y el software de sincronización que en este caso es Samsung Kies Pc, un software gratuito y descargable del Internet, dando comienzo con el proceso de adquisición de la información.

En la adquisición física para un dispositivo Android se debe tener en cuenta que el dispositivo móvil este en depuración usb para que funcione como un soporte de almacenamiento de datos.

El rooting en dispositivos móviles Android consiste en proporcionar privilegios al directorio raíz (/) de un dispositivo móvil.

Hay que tener en cuenta que el momento de lograr hacer rooting al dispositivo no implicará una sobreescritura de la partición del sistema y que variara del modelo y

[42] McAffee: Es una compañía de software espacializado en seguridad informática
[43] Microelectrónica: Aplicación de la ingeniería electrónica a componentes y circuitos de dimensiones muy pequeñas.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

versión del sistema operativo del dispositivo móvil. Una vez conseguido lo anterior se podrá realizar una imagen forense.

Posterior a ello se deben tener algunas consideraciones:

a) Realizar la imagen forense a cada uno de estos archivos mtd3 (archivos del sistema operativo) y mtd5 (datos del usuario).
b) Disponer en el slot del dispositivo una tarjeta completamente vacía y con espacio suficiente para realizar la extracción de la imagen forense.

Finalmente para el análisis de la tarjeta microSD o SD se puede utilizar las utilidades que proporciona la herramienta de TSK.

4) Otros dispositivos

En el caso de que algún dispositivo móvil antiguo llegue a las manos del investigador es posible aplicar un método general de trabajo con 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 NIST 800-101[17].

"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" [18].

De la misma manera el Perito Informático debe aplicar los conocimientos especializados y tener presente los aportes de otras guías de mejores prácticas y de procedimiento a nivel internacional, (ACPO & 7SAFE) [19], (SWGDE -1) [20].

5) Privacidad

Los castigos pueden ser severos cuando no se realiza una adecuada investigación forense en dispositivos móviles. Ya que en el momento de la audiencia se pueden oír argumentos de este tipo: ¿y quién le dio permiso para poder espiar la información personal de mi cliente? con el propósito de anular los informes periciales de que se inicie nuevamente el proceso de indagación e incluso con privación de libertad como le establece el Artículo 178 del COIP [3] sobre la violación a la intimidad.

5. Fase de Presentación

Con esta Fase culmina el marco de trabajo propuesto se obtendrá el informe final pericial resultante de todo el procedimiento llevado en cada una de las Fases anteriores. Se podría decir que es el desenlace de la investigación realizada remitiendo el informe al solicitante de la pericia.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

El informe final pericial debe ser redactado con un lenguaje compresible para un público no técnico explicando las razones por las cuales se ha llegado a tal o cual conclusión.

El Perito Informático no pondrá juicios de valor en el informe.

1. Fase Final

El Perito deberá sustentar oralmente los resultados del peritaje como una de sus obligaciones tanto en procesos Penales y Civiles, respondiendo al interrogatorio y al contrainterrogatorio de los sujetos procesales.

La defensa oral tiene por objeto la ratificación, aclaración o ampliación de la pericia ya que sin ella las conclusiones del examen pericial, carecerán de valor y no hará parte de la prueba que deba ser valorada por el juez como lo establece el Artículo 222 del COGEP [4].

La inasistencia injustificada del Perito a defender su informe, será considerada como falta gravísima perdiendo su acreditación e incluso pudiendo ser llevado a la audiencia mediante el uso de la fuerza pública.

El Perito tendrá la capacidad técnica y profesional de manejar y defender su informe presentado, sin desviarse de su especialidad y del objeto mismo de la pericia, para así no caer en contradicciones, falsedades o juicios de valor, explicando, detallando y defendiendo su experticia.

Existen algunas habilidades y destrezas que todo Perito debe exponer en audiencias que son:

- Forma de vestir adecuada al contexto lo cual denotara respeto a los sujetos procesales y la profesión de quien expone.
- Revisar otras experticias en el caso de haberlas.
- Mantener una actitud respetuosa y cordial al otro profesional que discrepa con nuestro criterio es señal de madurez psicológica y solvencia profesional.
- Utilizar un lenguaje claro y comprensible en la defensa de la audiencia.
- Responder las preguntas con calma y tranquilidad, siempre teniendo coherencia por lo escrito en el informe y lo expuesto oralmente.
- Recordar que cuando escuché la palabra Objeción por parte de uno de los abogados, deberá esperar a que únicamente el juez le indique si debe responder o no.
- El interrogatorio directo es el que realiza la parte que introdujo al perito al proceso. Para lo cual el Perito deberá acreditar su experiencia y exponer los fundamentos de los resultados de su pericia.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

- El Artículo 223 del COGEP [4] establece que se pueden realizar preguntas y presentar pruebas no anunciadas oportunamente orientadas a determinar su parcialidad y no idoneidad, a desvirtuar el rigor técnico o científico de sus conclusiones así como impugnar su credibilidad.
- No caer en la trampa con las estrategias de desacreditación de la contraparte en el contrainterrogatorio al Perito.
- El Artículo 511, inciso seis y siete del COIP [3] establece que los Peritos podrán responder las preguntas del interrogatorio de las partes por cualquier medio y acompañar sus informes mediante ilustraciones gráficas.
- El Artículo 222 del COGEP [4] establece que si hay informes periciales divergentes, el juez dispondrá un debate entre los peritos concluido este se abrirá un interrogatorio y contrainterrogatorio de las partes hacia el Perito para aclarar los puntos en controversia.

De la misma manera en esta fase serán devueltos todos los elementos que fueron incautados como parte de la investigación, dando por finalizado así el caso asignado al Perito Informático.

4. CONCLUSIONES

Se ha elaborado un marco de trabajo estandarizado para el análisis forense de la evidencia digital en equipos informáticos y dispositivos móviles tomando como puntos importantes las acciones más relevantes de las buenas prácticas, normas y estándares internacionales para que los Peritos Informáticos acreditados tomen en cuenta en el momento de realizar una investigación forense.

El contar con un marco de trabajo estandarizado garantizará la admisibilidad de la evidencia de manera contundente en un procedimiento Penal o Civil.

En el Ecuador los delitos informáticos son sancionados cuyos actos se comenten con el uso de tecnología para violentar la integridad, confidencialidad y disponibilidad de los datos personales, sin embargo, es preciso, desarrollar y establecer mecanismos para el análisis forense, permitiendo que estas se desarrollen dentro de marcos regulados y controlados.

Se espera que este modelo sirva de referencia debido a la creciente demanda de diversos delitos informáticos, el uso y difusión puede ser el punto de partida para que este marco de trabajo siga adquiriendo relevancia y fortaleciéndose.

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304

5. REFERENCIAS BIBLIOGRÁFICAS

[1] Mónica Uyana, Milton Escobar, "PROPUESTA DE DISEÑO DE UN ÁREA INFORMÁTICA FORENSE PARA UN EQUIPO DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD INFORMÁTICOS (CSIRT)". Disponible: http://repositorio.espe.edu.ec:8080/bitstream/21000/8123/1/AC-GSR-ESPE-047639.pdf

[2] SecureList, "Desarrollo de las amenazas informáticas en el tercer trimestre de 2016. Estadística" 2016. Disponible: https://securelist.lat/analysis/informes-trimestrales-sobre-malware/84164/it-threat-evolution-q3-2016-statistics/

[3] Ledy Zúñiga Rocha "Código Orgánico Integral Penal", Ministerio de Justicia, Derechos Humanos y Cultos, vol. 1, ISBN: 978-9942-07-592-5, 2014.

[4] Gustavo Jalkh R. "Código Orgánico General de Procesos" Ministerio de Judicatura, Disponible: http://www.funcionjudicial.gob.ec/ index.php/es/normativa/codigo-organico-general-de-procesos.html

[5] Fernando Cordero Cueva "CONSTITUCIÓN DEL ECUADOR" Asamblea Constituyente, 2008, Disponible: http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

[6] Gustavo Jalkl Roben "Resolución 067-2016" Ministerio de Judicatura, 2016, Disponible: http://www.funcionjudicial.gob.ec/www/pdf/ resoluciones/067-2016.pdf

[7] Gustavo Jalkl Roben "Resolución 040-2014" Ministerio de Judicatura, 2014, Disponible: http://www.funcionjudicial.gob.ec/www/pdf/ resoluciones/2014cj/040-2014.pdf

[8] AENOR "La Asociación Española de Normalización y Certificación", 2016, Disponible: http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051414#.WKHjgDvhAdV

[9] Francisco Lazaro Dominguez, "INTRODUCCION A LA INFORMÁTICA FORENSE", RA-MA, ISBN: 9788499642093, 2015.

[10] Karen Kent, "Guide to Integrating Forensic Techniques into Incident Response", 2006, Disponible: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50875

[11] Collective work of all DFRWS attendees, "A Road Map for Digital Forensic Research", 2001, Disponible: http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304
[12] Carrier y Spafford, "GETTING PHYSICAL WITH THE DIGITAL INVESTIGATION PROCESS", 2003, Disponible: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2003-29.pdf

[13] RFC 3227 "Guidelines for Evidence Collection and Archiving" RFC-Base.org, 2002, Disponible: http://www.rfc-base.org/rfc-3227.html

[14] Azas Marlon, ISO 27370 "Diseño de un Modelo para la cadena de custodia y herramientas para el análisis forense de quipos tecnológicos en procesos judiciales en el Ecuador", Universidad Internacional SEK, 2015.

[15] Brian Carrier "File System Forensic Analysys", Adisson Wesley Professional, ISBN: 0-32-126817-2, Disponible: http://www.campus64.com/digital_learning/data/cyber_forensics_essentials/info_file_system_forensic_analysis.pdf

[16] Jonathan Zdziarski "ZDZIARSKI'S BLOG OF THINGS", 2017, Disponible: https://www.zdziarski.com/blog/?cat=11

[17] Rick Ayers, "Guidelines on Mobile Device Forensics",2014, Disponible: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

[19] Dan Haagman, "Good Practice Guide for Computer-Based Electronic Evidence",1996, Disponible: https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf

[20] SWGDE Best Practices for Mobile Phone Forensics, "cientific Working Group on Digital Evidence", versión 2.0, 2013, Disponible: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Forensics

[21] Dan Haagman, "Good Practice Guide for Computer-Based Electronic Evidence",1996, Disponible: https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf

[22] Juan Miguel Tocados, "Metodologìa para el desarrollo de procedimientos periciales en el ambito de la informtica forense",Trabajo de Fin de Grado, 2015, Disponible: https://ruidera.uclm.es/xmlui/bitstream/handle/10578/6667/TFG_Juan_Miguel_Tocados.pdf?sequence=1&isAllowed=y

Revista Publicando, 4 No 11. (1). 2017, 42-78. ISSN 1390-9304
[23] Francisco Lazaro Dominguez, "INFORMÁTICA FORENSE", RA-MA, ISBN: 978-958-762-113-6, 2013.

[24] Pereyra, Damián; Eterovic, Jorge, "Desarrollo de una Guía de Asistencia para el Análisis Forense Informático en un Ambiente Piloto", Disponible: http://sedici.unlp.edu.ar/bitstream/handle/10915/43214/Documento_completo.pdf?sequence=1

[25] Leopoldo Sebastián Gómez, "Análisis forense de dispositivos de telefonía celular mediante procedimientos operativos estandarizados",2015, Disponible: http://sedici.unlp.edu.ar/bitstream/handle/10915/55345/Documento_completo.pdf-PDFA.pdf?sequence=1