Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

Desarrollo de una Guía Metodológica para el Análisis Forense en Equipos de Cómputo con Sistema Operativo Mac OS X

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

1 Escuela Politécnica Nacional-Ecuador, byron.loarteb@epn.edu.ec

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

RESUMEN

La tecnología cada día avanza más rápido, y parte de ello es el aumento del uso de las TIC (Tecnologías de la Información y Comunicación), como correos electrónicos, videoconferencias, redes sociales, etc., lo que a su vez refleja un mayor incremento en el manejo de internet en la vida cotidiana. Sin embargo, la utilización de internet, ofrece aparente anonimato para realizar gran cantidad de actividades ilícitas, de la misma manera pone al alcance de los usuarios herramientas para utilizarlos en forma indebida, fraudulenta o con fines no convencionales. Entre los delitos cometidos por medios informáticos se encuentran el robo de información, fraude a cuentas bancarias, interferencia en el funcionamiento de un sistema informático, grooming, pornografía infantil, tanto en su producción y como en su distribución, etc. En conclusión, el uso cada vez más de las TIC, ha provocado que se genere un incremento de la tecnología disponible para actividades delictivas informáticas, es por ello que, si ocurre un delito en el Ecuador en el cuál esté involucrado un equipo de cómputo con sistema operativo Mac OSX, la judicialización de la evidencia digital proveniente del mismo, no va a ser procesada correctamente debido a la falta de conocimientos técnicos por parte de los Peritos Informáticos sobre el funcionamiento de estos equipos y en la búsqueda de vestigios dejados por el autor del delito. Ante esta problemática se plantea dotar a los Peritos Informáticos con una guía metodológica para el análisis forense en un equipo de cómputo con sistema operativo Mac OS X, tomando como referencia normas, estándares, herramientas, guías y buenas prácticas propuestas por organizaciones internacionales especializadas principalmente en el área de informática forense apegada 100% a la actual normativa legal en el Ecuador permitiendo judicializar la evidencia proveniente de estos equipos de cómputo.

Palabras claves: Análisis forense, Sistema Operativo Mac OSX, Evidencia digital

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

Development of a Methodological Guide for Forensic Analysis in Computer Equipment with Mac OS X Operating System

ABSTRACT

Technology is advancing faster every day, and part of it is the increase in the use of ICT (Information and Communication Technologies), such as emails, videoconferences, social networks, etc., which in turn reflects a greater increase in the use of the internet in everyday life. However, the use of the internet offers apparent anonymity to carry out a large number of illicit activities, in the same way it makes tools available to users to use them in an improper, fraudulent or non-conventional way. Among the crimes committed by computer means are the data theft, bank account fraud, interference in the operation of a computer system, grooming, child pornography, both in its production and its distribution, etc. In conclusion, the increasing use of ICTs has led to an increase in available technology for computing criminal activities, which is why, if a crime occurs in Ecuador involving computer equipment with Mac OSX operating system, the judicialization of digital evidence from it, will not be processed correctly due to the lack of technical knowledge from Computer Experts about the operation of these devices and in the search for traces left by the perpetrator of the crime. In view of this problem, it is proposed to provide computer experts with a methodological guide for forensic analysis in a computer with Mac OS X operating system, taking as a reference standards, tools, guides and best practices proposed by international organizations specialized in the forensic computer area. The methodological guide is 100% adhered to the current legal regulations in Ecuador and allows the evidence coming from these computer equipment to be judicialized.

Keywords: Forensic Analysis, Mac OSX Operating System, forensic computing, Computer Expert, ICT, Legal Regulation in Ecuador, Digital Evidence, Forensic Analysis Methodology.

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

1. INTRODUCCIÓN

En la actualidad es impresionante observar como el mundo se ha digitalizado en gran parte y gracias a ello también se genera un incremento de la tecnología disponible para actividades delictivas informáticas combinado con el escaso conocimiento por parte de las víctimas de cómo protegerse de los delitos informáticos que pueden sufrir a través de las nuevas tecnologías, otorga a los delincuentes informáticos un inmenso campo fértil de potenciales víctimas de ataques.

Dichos ataques son dirigidos contra un objetivo comprometiendo la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, denominados en la actualidad como delitos informáticos.

Uno de los tipos de delito informático es la apropiación de la información de manera ilícita haciendo uso de la tecnología electrónica ya sea como método, medio o fin con el objetivo de realizar manipulación fraudulenta de los ordenadores, robo de información, la destrucción de programas o datos y el acceso no autorizado a la información afectando a los sujetos pasivos obteniendo grandes beneficios económicos o causar importantes daños materiales o morales.

En el Ecuador para que los delitos informáticos sean juzgados en un tribunal se necesita de la comúnmente llamada evidencia digital que no es más que la información almacenada en cualquier dispositivo de almacenamiento electrónico digital o que a su vez estos han sido procesados electrónicamente en un medio computacional como puede ser datos, programas y mensajes transmitidos en formato digital.

El hecho de que la información haya dejado de estar en papel para almacenarse digitalmente en cualquier medio tecnológico pasa a tener mayor relevancia en un procedimiento ya sea penal o civil derivando en Pericias Informáticas que son muy específicas y a la vez complicadas en la obtención de la evidencia provocando que conlleve a una serie de problemas:

- Falta de conocimientos técnicos por parte de los Peritos Informáticos sobre el funcionamiento de equipos de cómputo con sistema operativo Mac OS X, ocasionan la pérdida y negligencia en búsqueda de la evidencia digital.
- Falta de un método para el análisis forense en equipos de cómputo con sistema operativo Mac OS X, ocasionan que la evidencia digital obtenida no sea aceptada legalmente en un tribunal con elementos claros, contundentes y útiles.

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

- Falta de controles que evidencien que el equipo de cómputo o el análisis donde se realizó la investigación no hayan sido alterados por terceras personas para manipular el resultado de la investigación forense, ocasionan que los informes periciales no sean concisos y pierdan credibilidad.

Todos los problemas citados dan como resultado la incidencia de los delitos informáticos a escala nacional e internacional sin que se encuentre al culpable, quedando en la impunidad y no sean juzgados o peor aún exista negligencia en la búsqueda de vestigios y pérdida de juicios en tribunales.

Finalmente si no se toman medidas al respecto, dichos delitos informáticos se desarrollarán cada vez más, ocasionando que la evidencia digital proveniente de equipos de cómputo con sistema operativo Mac OS X no pueda ser judicializada.

Es por eso que el presente trabajo de investigación tiene como fin dotar a los Peritos Informáticos una guía metodológica para el análisis forense en un equipo de cómputo con sistema operativo Mac OS X, tomando como referencia normas, estándares, guías y buenas prácticas propuestas por organizaciones internacionales especializadas principalmente en el área de informática forense apegada 100% a la actual normativa legal, con lo cual ayudaría en el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales obtenidas en estos equipos de cómputo, permitiendo judicializar correctamente los delitos informáticos que en la actualidad se presentan.

2. METODO

En este apartado se procede a enunciar los respectivos métodos que van a ser utilizados para el presente proyecto de investigación.

2.1. TIPO DE PROYECTO

Este presente proyecto de investigación es de tipo tecnológica, ya que tiene como objetivo el solucionar una problemática de la comunidad de investigadores forenses quienes se ven en la necesidad de aplicar su criterio durante el proceso de análisis de evidencia digital en equipos de cómputo con sistema operativo Mac OSX, generando una confrontación respecto a la validez de la evidencia obtenida, así como del proceso de adquisición y preservación de la misma.

2.2. TIPO DE ESTUDIO

Según el análisis y alcance de los resultados serán de tipo descriptivo, exploratorio.

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

- **Descriptivo:** Con este tipo de estudio lo que se plantea es aplicar y describir los componentes de la metodología propuesta en un caso práctico.
- **Exploratorio:** Mediante este tipo de estudio lo que se busca es esclarecer un problema poco estudiado o analizado en base a revisiones bibliográficas, la experiencia y opinión de expertos en el tema o investigaciones de campo y de ello reconocer los beneficios que otorgará el desarrollo de una guía metodológica para el análisis forense en un equipo de cómputo con sistema operativo Mac OS X.

2.3. UNIVERSO Y MUESTRA

En este punto se realizará una segmentación del universo de acuerdo a las líneas de estudio forense. Para lo cual, el punto de partida es definir el tamaño de población, básicamente el tamaño de la población va a ser 29 Peritos Informáticos que están debidamente acreditados en el Consejo de la Judicatura de Ecuador, Sin embargo en el proceso de experimentación se plantea que se realicen estudios de aplicación en dos peritos acreditados por el Consejo de la Judicatura de Ecuador en el ámbito de la Informática para la validez de los resultados obtenidos.

2.4. MÉTODOS TEÓRICOS

- **Hipotético-Deductivo:** Este método se basará en una hipótesis, el mismo que permitirá obtener una deducción lógica cuantitativa en la aplicación de la guía metodológica para el análisis forense en equipos de cómputo con sistema operativo Mac OS X.

2.5. SELECCIÓN INSTRUMENTOS INVESTIGACIÓN

Los instrumentos que se utilizarán para esta investigación tienen como función esencial obtener información que se convertirá luego en resultados relevantes según (Abril, 2008), a continuación, se describe cada uno de los que se van a utilizar en el proyecto de investigación:

- **Análisis Documental**: Se realizará un estudio de fuentes bibliográficas primarias y secundarias, principalmente en base a otros estudios realizados anteriormente, toda esta documentación albergada en archivos, publicaciones, libros, etc. Referentes al proyecto de investigación.
- **Observación**: Principalmente se realizará una observación científica ya que nos va a permitir la percepción sistemática y dirigida a captar los aspectos más significativos del objeto de estudio.

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

- **Experimentación**: Finalmente se evaluará el comportamiento de la aplicación de la metodología de análisis forense bajo las condiciones particulares en un equipo de cómputo con sistema operativo Mac OS X.

2.6. RECURSOS DEL PROYECTO

- **Recursos humanos**: Tesistas del programa de Maestría en Tecnologías de la Información, Miembros del tribunal de tesis, Director de tesis y Perito Informático del Consejo de la Judicatura de Ecuador.
- **Bienes y equipos**: Laboratorio de Investigación Forense, MacBook Pro, Disco duro externo, External case 2.5" HDD, destornilladores, Laptop y Guantes de nitrilo.
- **Servicios**: Digitado, fotocopiado e inter-net
- Fuentes de financiamiento personal.

2.7. SISTEMA OPERATIVO Mac OSX

Mac OS, Sistema Operativo de Macintosh es el nombre del sistema operativo creado por Apple en 1984, para su línea de computadoras Macintosh (Mac). Es conocido por haber sido el primer sistema dirigido al público en contar con una GUI (Interfaz Gráfica de Usuario), compuesta por la interacción del mouse con ventanas, Icono y menús.

Para el año de 1999 Apple Computer, lanza la versión del Mac OS X Server, siendo una nueva generación de Sistemas Operativos y a la vez precursora y definitiva del Mac OS X, que hoy se conocen en la actualidad y que está virtualmente en todas las Mac´s, se trata de un sistema operativo UNIX, basado en los kernels Mach y BSB.

El objetivo del desarrollo del OS X es lanzar al mercado una nueva generación de sistemas operativos que puedan ser:

- Estables
- Seguros
- Extensibles
- Fáciles de usar

2.8. ARQUITECTURA

Las arquitecturas internas de los sistemas operativos son muy diferentes, debido a que los usuarios tienen metas distintas como: fácil de usar, seguro, rápido, estable y las propias que el sistema las requiera.

Para un mejor entendimiento de esta arquitectura se lo ha separado en capas, como se ilustra

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

en la Figura No 1, de la cual vamos a describir cada una.

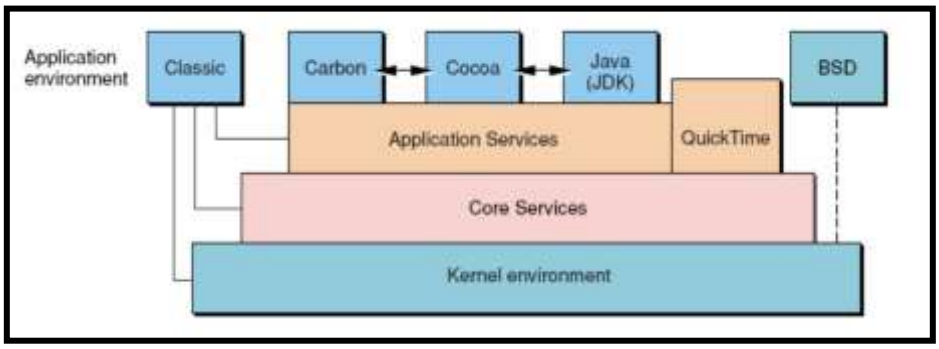


Figura No 1. Arquitectura en capas de Mac OS X

Fuente: Laguna, C. P., & Oruña, A. R. (2003). MAC OS X: PANTHER. En LA EVOLUCIÓN DE LAS ESPECIES. Barcelona. Recuperado de http://docencia.ac.upc.es/FIB/CASO/seminaris/1q0304/M11_Informe.pdf

2.9.METODOLOGÍAS PARA EL ANÁLISIS FORENSE

En este apartado se evaluarán las principales metodologías que existen para el análisis forense, propuestos por algunos organismos y autores que luego de un exhaustivo trabajo de investigación y tomando en cuenta algunas de las normas y estándares mencionadas anteriormente, proponiéndose así la "Guía metodológica para el análisis forense digital en equipos de cómputo con sistema operativo Mac OS X para la judicialización de la evidencia digital en procesos legales en Ecuador."

Las metodologías tomadas en cuenta para la evaluación son las siguientes:

- ✓ Forensic Control
- ✓ UNE 71506:2013
- ✓ Francisco Lázaro Domínguez
- ✓ Fase de investigación de la escena digital del crimen, del modelo IDIP (2003)
- ✓ NIST
- ✓ DFRWS
- ✓ CASEY

2.10. HERRAMIENTAS PARA EL ANÁLISIS FORENSE

En este apartado se detallara los aspectos importantes y relevantes sobre la elección de las herramientas que van a ser utilizadas para el análisis forense. Sin embargo, es importante recalcar que esta metodología iba ser desarrollada 100% apegada a la normativa legal vigente en el Ecuador, y es por ello que únicamente las herramientas de análisis forense van a ser de Software Libre.

Esta elección se la considero en base al Decreto Ejecutivo 1014, que el Pdte. Rafael

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

Correa Delgado emitió el 10 abril 2008 en el cual adopta el Software Libre como política de estado, en el cual el Artículo 1 menciona "Establecer como política pública para las Entidades de la Administración Pública Central la utilización de Software Libre en sus sistemas y equipamientos informáticos." (softwarelibre.conocimiento.gob.ec, 2008)

Por medio de este Decreto Presidencial, el Ecuador pasa a ser el tercer país latinoamericano después de Brasil y Venezuela que adopta el Software Libre como política nacional. Cabe recalcar que las herramientas y los procedimientos que se utilicen deben garantizar en todo momento la integridad de la evidencia y poder garantizar la admisibilidad en los tribunales y no ser vulnerable a una objeción de descalificación.

De la misma manera otro aspecto a tener en cuenta para las herramientas seleccionadas es seguir las recomendaciones del fabricante para su correcto uso y máximo aprovechamiento.

Mediante la investigación se determinó que al igual que existen herramientas específicas para el análisis forense, también existen suites o sistemas operativos que contienen diversos programas de acceso rápido, lo que disminuye el tiempo en el análisis de las respectivas investigaciones forenses. A continuación, en la Tabla No 2, se presentan las principales herramientas en base a los criterios ya mencionados.

Tabla 1 Selección de las herramientas.

Herramientas	Descripción	Distribución
Forensic Toolkit (FTK)	FTK Imager de AccessData es un paquete gratuito que permite generar imágenes de dispositivos de almacenamiento en varios formatos. Está orientado principalmente a la adquisición y tratamiento de imágenes de dispositivos de almacenamiento, para ser posteriormente usadas como de evidencias forenses. De la misma manera proporciona una poderosa navegación, búsqueda y filtrados de ficheros. Recupera automáticamente ficheros y particiones borradas, permitiendo realizar análisis de emails y ficheros Zip.	Libre
Autopsy	Es un programa fácil de usar, basado en GUI (Interfaz gráfica de usuario) con lo cual permite analizar de manera eficiente discos duros y teléfonos inteligentes. Siendo una	Libre

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

	herramienta muy intuitiva y accesible para que pueda ser utilizada de manera efectiva por investigadores no técnicos, cuenta con una línea de tiempo para identificar la actividad. Es importante mencionar que todos los resultados del análisis forense son presentados en una estructura de árbol. Sin embargo para facilitar la búsqueda de evidencia esta herramienta permite integrar módulos o complementos gracias a su arquitectura plu-gin.	
CAINE (Computer Aided Investigate Environment)	CAINE ofrece un pack de herramientas especializadas para realizar un análisis forense de algún equipo informático, es de fácil uso ya que proporcionar una interfaz gráfica homogénea que guía a los investigadores digitales durante la adquisición y el análisis de las pruebas electrónicas, ofreciendo de la misma manera un proceso semi-automático durante la documentación y generación de informes.	Libre
DEFT (Digital Evidence & Forensic Toolkit)	DEFT es un Live CD incorporado en la parte superior de Xubuntu con herramientas para la informática forense y respuesta a incidentes. Su principal característica es que permite ejecutar sistemas en vivo sin alterar o dañar dispositivos (discos duros, pendrives, etc...) conectados a la PC donde se lleva a cabo el proceso de arranque. Es un sistema fácil de usar que incluye una excelente detección de hardware y de las mejores aplicaciones de código libre y abierto dedicado a la respuesta a incidentes y análisis informático forense.	Libre
ForLEx	ForLEx es un Live CD basado en Debian Linux. El objetivo principal de la distribución es proporcionar varias utilidades útiles para el análisis forense.	Libre
EnCase	Es una poderosa plataforma líder en el mercado de investigación que recolecta datos digitales, realiza análisis, informa sobre	Libre

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

	descubrimientos y los preserva en un formato válido a efectos legales. Permite un copiado comprimido de discos fuente, realiza la búsqueda y análisis de múltiples partes de archivos adquiridos, permite la búsqueda y análisis en archivos tipo ZIP, soporte de múltiples sistemas de archivos, integración de reportes.	
Safeback	Es un conjunto de herramientas forenses, que permite crear copias de respaldo de discos duros. Permite la conservación de evidencia, de la misma manera puede extraer imágenes de un disco por medio del puerto de la impresora. SafeBack en sus últimas versiones comprime únicamente las secciones no usadas o no formateadas del disco duro, lo que permite incrementar la velocidad del proceso y ahorrar espacio de almacenamiento en el archivo imagen SafeBack.	Libre
Kali Linux	Kali está basada en Debian, y fue diseñada principalmente para la auditoria y seguridad informática en general. Sin embargo cuenta con una serie de herramientas preinstaladas para análisis forense	Libre
DiskDigger	Es una herramienta que permite recuperar archivos directamente desde los sectores del disco duro o de una tarjeta de memoria en busca de restos reconocibles. Gracias a esta lectura de bajo nivel, DiskDigger es capaz de recuperar fragmentos de ficheros en donde otros programas no encuentran nada.	Libre

3. RESULTADOS

Una vez culminada la fase de investigación se procede al desarrollo de la guía metodológica propuesta.

Esta guía metodológica utiliza como base para su desarrollo las guías y buenas prácticas “RFC-3227” (Brezinski & Killalea, 2002) y “Examinación Forense de la Evidencia Digital (NIJ)” (Hart, Ashcroft, & Daniels, 2004), debido a que estas implementan de mejor manera el proceso para un correcto análisis forense, ajustándose a la perfección las recomendaciones y directrices que sugieren las guías mencionadas. De la misma manera se decidió implementar el siguiente modelo propuesto por la “UNE 71506:2013” (AENOR), debido a que es bastante completa para el manejo de evidencias digitales, no

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

obstante, será complementado con la normativa legal vigente.

El objetivo de esta guía metodológica es el de proporcionar diferentes fases y sub-fases como se ilustra en la Fig. 3, para englobar todos los aspectos a considerar en un análisis forense relacionado principalmente en el proceso de adquisición y análisis de la evidencia digital proveniente de estos equipos de cómputo.

Dichos aspectos serán de carácter técnico y de jurídico para que de esta manera se mantenga la integridad de la evidencia digital en todo momento y poder garantizar la admisibilidad en los tribunales y no ser vulnerable a una objeción de descalificación.

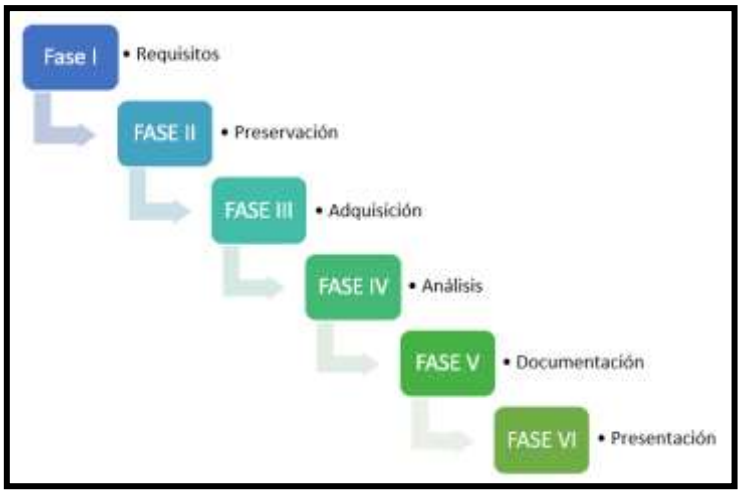


Figura No 3. Metodología propuesta

3.1.Fase I (Requisitos)

Esta fase tiene como propósito determinar los requisitos iniciales y el perfil que un investigador forense debe tener al momento de comenzar una investigación forense.

Los requisitos que deben cumplir las personas para calificarse como Perito Informático están reglamentados en el Artículo 18 de la Resolución 040-2014 (Consejo de la Judicatura, 2014), del Reglamento del Sistema Pericial Integral de la Función Judicial, 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.

El Perito Informático debidamente 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 (Consejo de la Judicatura, 2016).

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

De la misma manera estos Peritos deberán tener el perfil que el artículo 511 del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014) proporciona, para poder realizar una investigación forense.

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 proceso civil se debe seguir el procedimiento que se ilustra en la Fig. 4.

Figura No 3. Procedimiento pericial para procesos civiles

Teniendo en cuenta que en la Fase de Designación, mediante la última resolución del pleno del Consejo de la Judicatura en la Resolución 068-2017 en el Artículo 1 establece que "En procesos no penales, las partes procesales podrán elegir a los Peritos del Registro de Peritos del Consejo de la Judicatura, según lo que establece el Código Orgánico General de Procesos" (Consejo de la Judicatura, 2017)

Sin embargo, si es un proceso penal, en cambio se debe este procedimiento como se ilustra la Fig. 4.

Figura No 4. Procedimiento pericial para procesos penales

Teniendo en cuenta la Fase de Posesión se suprime, mediante la Resolución 067-2016 en su Artículo 11 y 12 (Consejo de la Judicatura, 2016).

- **Fase de Designación**

En el Artículo 12 de la Resolución 040-2014 (Consejo de la Judicatura, 2014), 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 [1]SATJE. Respetando siempre los principios de profesionalidad, especialidad, transparencia,

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

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

alternabilidad e igualdad.

Sin embargo, independientemente de la forma en la que el Perito haya sido designado será registrado en el sistema SATJE dejando constancia del código de calificación, como lo establece el Artículo 13 de la Resolución 040- 2014 (Consejo de la Judicatura, 2014).

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

El Perito Informático designado recibirá una notificación vía correo electrónico, de su asignación a un caso en particular, de la misma manera en la providencia se especifica el nombre del Perito que ha sido asignado, mediante un sorteo e indica fecha y hora en la que el Perito deberá posesionar el caso y tiempo para la presentación del informe pericial.

- **Fase de Investigación**

En esta fase el Perito Informático utilizará su experticia para realizar el análisis forense y encontrar información relacionada con el cometimiento del delito informático.

- **Fase Final**

Finalmente, 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 (Consejo de la Judicatura, 2015).

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.

Sin embargo, antes de iniciar una investigación forense, es necesario que el Perito Informático este un paso adelante y sepa la documentación necesaria que va a requerir en toda la investigación. Es por ello que como parte de esta guía metodológica es establecer cierta documentación como formularios y solicitudes indispensables que el Perito Informático va a requerir:

- Solicitud por escrito a una autoridad competente ya que ciertos casos se debe

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

romper claves de seguridad, investigar sobre archivos personales en equipos informáticos o incluso para quebrantar los acuerdos de confidencialidad que tienen las empresas.

- Un formulario, el cual contendrá información personal del Perito a cargo de la investigación, para corroborar que no se tenga ningún tipo de nexo con las personas procesadas.
- Un formulario, el cual contendrá información acerca de la escena del delito.
- Un formulario, el cual contendrá información referente a la recopilación de la evidencia original de los diferentes dispositivos de almacenamientos.
- Un formulario, el cual contendrá información referente a los diferentes elementos físicos o contenido digital, principalmente los que formaran parte de la investigación y de la cadena de custodia para ser transportados al laboratorio forense.

Es importante tener en cuenta que antes de comenzar con la Fase de Preservación el Perito Informático deberá llenar adecuadamente el primero formulario.

3.2. Fase II (Preservación)

La prioridad en esta fase 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.

El Perito Informático, antes de llegar a la escena del delito, debe conocer la mayor cantidad de detalles, tanto del área, equipos, personal, sistemas, dispositivos, etc., para saber ante que se encontrará y acudir con las herramientas necesarias para la investigación. Sin embargo, es importante mencionar que la o el servidor público o persona natural que intervenga o tome contacto con la escena del incidente será la responsable de su preservación, hasta contar con la presencia del personal especializado según lo menciona el Artículo 178 del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).

Para lo cual se elaboraron sub-fases enmarcadas en la escena del delito como se ilustra en la Fig. 5.

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

Figura No 5. Sub-fases de la Fase de Preservación

- **Sub-fase de Reconocimiento**

Los Peritos 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. Como lo establece el Artículo 460 del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).

- **Sub-fase de Autorización**

Antes de iniciar su experticia y encontrar información relacionada con el incidente, el Perito deberá solicitar 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, investigar sobre archivos personales o incluso para quebrantar los acuerdos de confidencialidad que tienen las empresas.

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 (Ministerio de Justicia, Derechos Humanos y Cultos, 2014), sobre la violación a la intimidad. El Artículo 292 del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014), 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.

- **Sub-fase de Identificación**

En esta fase se realizará la identificación y el tipo de evidencia, determinando entre otras cosas el tipo de información que está disponible y que forma parte de la evidencia a ser investigada.

Una vez que todo el personal especializado llega a la escena del incidente, estos deben actuar en forma ordenada y no de forma indiscriminada, permitiendo su actuación ponderable y eficaz para lograr el mejor de los resultados.

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

El orden que se debe seguir en un caso hipotético que esté involucrado un medio informático es el siguiente:

- Perito Fotógrafo
- Perito Criminalista
- Perito en Dactiloscopia

Una vez culminado las intervenciones de los expertos entra en escena el Perito en Informática Forense, el cual determinará una serie de procedimientos a realizar para la identificación de los elementos que necesita para su caso (elemento de estudio).

Saber con exactitud qué clase de evidencia es la que requiere es de vital importancia para una exitosa investigación, desafortunadamente un error común es tomar todo lo que este a su vista, pero debido cuestiones legales debe ser muy cauteloso en el ejercicio de sus funciones y de su encargo pericial. Es por eso que en este punto se enumeran algunas consideraciones a tener en cuenta.

1. **Orden de allanamiento**

Existen incidentes en los cuales es necesario realizar una orden de allanamiento para lo cual los artículos 478, 480, 481 y 482 del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014), determinan los parámetros, reglas y pautas que se deben tener en cuenta para el registro o incautación de los elementos a ser investigados.

2. **Verificar el estado de los equipos**

Es primordial verificar el estado del equipo, si este se encuentra encendido o apagado, debido a que los procedimientos de recopilación de información serán diferentes para mantener la integridad de la evidencia original. Por lo general es que si se encuentra el equipo apagado no encenderlo y caso contrario si se encuentra encendido no apagarlo.

Como recomendación si el equipo se encuentra encendido se debe realizar periódicamente movimientos del mouse, ya que algunos equipos cuentan con contraseñas a fin de evitar que el equipo se bloquee, permitiendo que el equipo se encuentre activo, así como programas ejecutados o archivos abiertos, en la fase de adquisición se detallara de manera clara el orden para la obtención de la información volátil.

3. **Etiquetado de dispositivos**

Es importante etiquetar con una numeración única cada uno de los dispositivos incautados de la misma manera acompañar con una fotografía.

4. **Cambio de custodia**

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

Es importante documentar los procedimientos realizados en un cambio de custodia, los responsables que estarán a cargo, los dispositivos incautados, si existió o no algún escrito y la nueva ubicación donde serán transportados.

5. 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, por lo cual se deberá mirar todo meticulosamente. Establecer un perímetro de protección de los equipos afectados garantizará que la evidencia original no sea alterada por personas ajenas a esta.

6. 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 (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).

Las actividades mencionadas se deben realizar con la utilización de guantes de látex, de esta manera estará en condiciones de tomar algún objeto con el fin de recabar algún dato relevante como el número de serie, conexiones de red, conexiones con los periféricos de entrada/salida, etc.

Es importante el uso de brazaletes antiestáticos con el fin de no alterar la evidencia producida por cargas electrostáticas en el momento de la manipulación de los equipos o dispositivos.

7. Recreación de la escena del delito

Realizar dibujos de la ubicación, bocetos de conexiones, y pequeñas descripciones de los dispositivos almacenamiento encontrados en la escena del delito, así como algunas notas al lado del teclado o cercano al equipo de cómputo donde puede existir información relacionada con la investigación. Sera de gran ayuda ya que conforme avance la investigación esta información recabada nos dará más pistas sobre donde poder buscar más evidencias.

8. Arquitectura de lo que se va a investigar

Identificar el tipo de arquitectura de lo que se va a investigar (servidores, estaciones de trabajo, sistemas operativos, router, switches, etc.). Es primordial ya que de esto

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

dependerán los procedimientos a seguir en la investigación para la obtención de la evidencia.

9. Componentes relacionados al incidente

Los peritos informáticos efectuarán la identificación sobre 2 tipos de evidencia

- **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 esto influirá en los procedimientos que se realicen de manera adecuada para cada tipo de evidencia, a fin de encaminar correctamente el análisis forense y de la misma manera esto proporcionará más evidencia durante el incidente a investigar.

10. Identificar los posibles implicados

En este punto es recomendable realizar entrevistas a todos los implicados o que tengan relación con la investigación ya sea con administradores o usuarios responsables de los sistemas, esto con el fin de recabar más información relacionada con el incidente.

11. Fotografiar y rotular las evidencias

Registrar fotográficamente (de preferencia con una cámara réflex si es digital entonces se deberá obtener su hash del archivo o archivos obtenidos por esta cámara digital) y acompañado con grabaciones de la escena del delito, si el equipo se encuentra apagado o encendido, los periféricos de entrada como de salida, y de las conexiones físicas del equipo, que se encuentran en la escena del delito. Esto servirá para demostrar cómo se encontró el equipo a ser investigado y mantener una correlación de los eventos, lo que proporcionara mayor oportunidad de encontrar evidencia.

12. Reconocer el Sistema Operativo

Es importante saber el sistema de archivos del equipo del cual se obtendrá la información, esto permitirá determinar cómo es su estructura del sistema de archivos y definir las herramientas de hardware como de software a utilizar.

13. Interrumpir las conexiones de red

Es importante que, si el equipo de cómputo está conectado mediante un cable de red, lo

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

recomendable es desconectar dicho cable ya que el atacante puede estar de manera remota y puede alterar la evidencia original.

14. Corroborar con el diseño de la investigación

Es primordial verificar si los procedimientos realizados son los correctos, están acordes y justificados con la situación del incidente, ya que cada caso es diferente.

15. Documentar todas las acciones

Finalmente, en esta esta sub-fase es importante documentar de manera estructurada todas las acciones, acontecimientos y decisiones que se adoptarán antes, durante y después de la escena del delito.

Documentar lo observado desde el inicio de la investigación, ayudará a determinar las acciones a seguir en la investigación, sirviendo de ayuda en la Fase de Documentación y en el Informe Pericial a ser emitido, para lo cual se utilizará el segundo formulario, el cual contendrá información sobre la escena del delito.

3.3. Fase III (Adquisición)

Según la metodología propuesta una vez ya identificados los equipos a ser investigados se debe realizar la extracción de la evidencia original contenida en los dispositivos de almacenamiento de los mimos. De la misma manera se deberá seguir con el proceso de almacenamiento y transporte de la evidencia digital obtenida sin olvidar la cadena de custodia.

Esta fase es de vital importancia ya que los procedimientos a seguir y la selección de las herramientas permitirán corroborar que la evidencia sea autentica a la original y la integridad de la misma.

Se tomara en consideración algunas recomendaciones según (Gervilla Rivas, 2014), en su trabajo “Metodología para un Análisis Forense”. Y el modelo de cadena de custodia para el análisis forense de equipos tecnológicos según (Azas Manzano, 2015).

Por lo mencionado anteriormente se elaboraron sub-fases englobadas en la evidencia original como se ilustra en la Fig. 6.

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

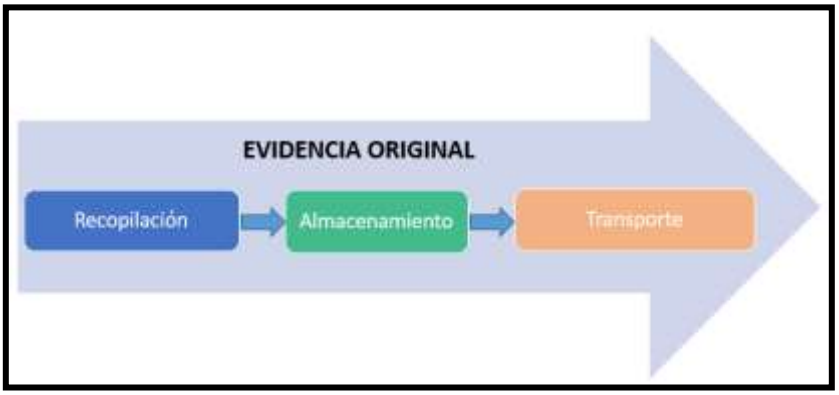


Figura No 6. Sub-fases de la Fase de Adquisición

- **Sub-fase de Recopilación**

La primera instancia de esta sub-fase es tener en cuenta que van a existir equipos que pueden ser trasladados al laboratorio forense y en ocasiones no, y estos pueden ser dispositivos y equipos irremplazables en el funcionamiento de la empresa.

Es por eso que siempre hay que 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 ya que en esta sub-fase se deben aplicar técnicas y/o métodos para la recopilación de la evidencia original priorizando el orden de volatilidad de los datos y de igual manera identificando que es lo más conveniente de acuerdo a las características del incidente, por lo mencionado los escenarios son:

1. **Equipo está apagado**

A continuación, se detallan una serie de procedimientos a realizar en lo que respecta a la obtención de la evidencia:

No prender el equipo, siempre debe estar apagado, ya que si se lo prende se puede alterar la evidencia, considerando que el atacante halla modificado el proceso de inicio/apagado con algún Script (es un código que se ejecuta cuando se enciende o apaga la maquina).

No 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 ya sea de software o hardware 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

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

sector de arranque, entre otros, etc., 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.

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

Sin embargo para corroborar la integridad de la evidencia original con la imagen forense obtenida se debe proceder a calcular el [2]Hash (es una huella digital única para cada conjunto de datos cifrados), primeramente del soporte de almacenamiento de datos original donde se encuentra la evidencia original y luego de la imagen forense extraída. Es importante mencionar que los dos Hashes deben ser iguales.

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

Documentar información de otros equipos que necesitan ser transportados para su respectiva investigación que pueden ser monitores, teclados, CDS/DVDS, memorias USB, impresoras, tarjetas de red, módems, etc.

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 acompañar con una fotografía de lo mencionado anteriormente.

Si los procedimientos mencionados anteriormente se realizaron de manera adecuada se garantizará la integridad de la evidencia y no podrá ser descartada como medio probatorio. Respetando el Artículo 500, inciso tres del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).

2. Equipo está encendido

A continuación, se detallan una serie de procedimientos a realizar en lo que respecta a la obtención de la evidencia:

[2] Hash son algoritmos de cifrado que realiza una operación matemática sobre el conjunto de datos de cualquier longitud, su salida es un número hexadecimal de 32 dígitos

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

No se debe apagar el equipo, ya que se puede perder información sensible como: memoria [3]RAM, usuarios conectados de forma remota y localmente, procesos en ejecución, etc., siendo muy difícil de volver a reunir toda esta información, si se decide apagar el equipo. Es importante que la recopilación de la evidencia se realice siguiendo el orden de mayor a menor volatilidad de la información. Este orden 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. El orden de volatilidad según lo establecido en el "RFC-3227" (Brezinski & Killalea, 2002), es de lo más volátil a lo menos volátil siendo esto:

- Registros y contenidos de la caché.
- Contenido de la memoria RAM.
- Estado de las conexiones de red, tablas de ruteo.
- 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.

Documentar toda la información del sistema en tiempo real como:

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

En ocasiones puede ser que el atacante dejé 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 detectando nuestra presencia y actué con una acción evasiva

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

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

o, peor aún, destructiva eliminando todo tipo de información.

En este caso si la información es gravemente comprometida por la severidad del ataque el equipo debe ser apagado sin dudarlo. Se puede perder información más volátil, pero se conservará información útil sobre el ataque.

Posterior a ello se debe proceder a recopilar toda la información volátil del sistema para lo cual se podría emplear un script para sistemas UNIX/Linux o un archivo de proceso por lotes para sistemas Windows para que realice el proceso de copiado de forma automatizada. También sería de gran ayuda emplear herramientas de trasmisión de datos por la red, enviando la información a una portátil conectada a la misma red.

Es recomendable que las herramientas que se utilicen para la obtención de la información vengan instaladas en un medio solo de lectura como puede ser un CD-ROM, y de igual manera para realizar el almacenamiento de la información extraída se debe utilizar medios forenses estériles.

De la misma manera se deberá proceder a calcular el Hash de la información extraída.

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 respetando el Artículo 500, inciso uno y dos del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014)

El perito informático documentará a detalle los procedimientos realizados anteriormente y toda la información obtenida en el tercer formulario.

- **Sub-fase de Almacenamiento**

Una vez culminado de recopilar toda la información requerida para la investigación y almacenándola cuidadosamente, es fundamental definir métodos adecuados para el almacenamiento y etiquetado de las evidencias. Este proceso es comúnmente llamado “cadena de custodia”.

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 (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).

Sin embargo, la demostración de la autenticidad de los elementos probatorios y evidencia física no sometidos a cadena de custodia, estará a cargo de la parte que los presente como lo menciona el Artículo 457 del COIP (Ministerio de Justicia, Derechos Humanos y

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

Cultos, 2014).

Para la elaboración de estos métodos se tomará de guía estándares para el manejo y almacenamiento de la evidencia digital como son: el "RFC-3227" (Brezinski & Killalea, 2002), Modelo Extendido de Séamus Ó Ciardhuain (Ciardhuáin, 2004). 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 (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).

La cadena de custodia debe realizarse de la siguiente manera:

1. **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, planos, entre otros. Se podrá aplicar cadena de custodia según lo establece el Artículo 500, inciso cuatro del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).

2. **Recolección de la evidencia**

Una vez analizado el estado del equipo y aplicando las herramientas tanto de software como hardware se obtendrá la imagen forense según un orden de volatilidad. De la misma manera se deberá documentar las características de los equipos a ser transportados para el laboratorio forense para su respectivo análisis. En este caso se podrá aplicar cadena de custodia como lo menciona el Artículo 500, inciso dos y tres del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).

3. **Embalaje y rotulado de la evidencia**

Registrar fotográficamente los equipos y sus conexiones antes de su embalaje, durante el embalaje y al finalizar el embalaje y rotulado.

Revisar los dispositivos de almacenamiento removibles. (Algunos equipos contienen en su interior dispositivos de almacenamiento removibles tales como tarjetas SD, [4]Memory Stick, etc.).

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

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

Sellar todas las entradas y salidas del equipo, así como puntos de conexión o de admisión de tarjetas o dispositivos de memoria.

Sellar todos los tornillos del equipo para evitar que se puedan reemplazar o retirar piezas internas.

Para el sellado de los equipos se debe realizar con una cinta adecuada que brinden seguridad y preservación del mismo.

Para el manejo de soportes de almacenamiento de datos y de la respectiva imagen forense obtenida se deben introducir en una bolsa antiestática 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. Sin embargo, si se desea más información se puede considerar algunas otras recomendaciones en la "ISO 27037:2012" (ISO/IEC 27037, 2012).

Escribir alguna firma y número único de identificación en cada sellado que se haya realizado y sobre esta adhiera cinta masking transparente.

Rotular de manera consecutiva cada uno de los elementos a ser incautados relacionados con la evidencia.

4. Documentar la cadena de custodia

El perito informático documentará a detalle los procedimientos realizados anteriormente y toda la información obtenida registrando en el cuarto formulario para que de estar manera garantice la seguridad y preservación de los elementos físicos que almacene, procese o transmita contenido digital y de las evidencias obtenidas (en este caso evidencia digital).

Respetando lo que menciona el Artículo 457, del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014), sobre la valoración de la prueba que se hará teniendo en cuenta su legalidad, autenticidad, sometimiento a cadena de custodia y grado actual de aceptación científica y técnica de los principios en que se fundamenten los informes periciales.

- **Sub-fase de Transporte**

Finalmente, toda evidencia así como los elementos incautados deben ser transportadas al laboratorio forense respectivo, el cual quedara registrado en el cuarto formulario, es importante el uso de brazaletes antiestáticos con el fin de no alterar la evidencia producida por cargas electrostáticas en el momento de la manipulación de los equipos o dispositivos.

Como lo menciona el Artículo 500, inciso cuatro del COIP (Ministerio de Justicia,

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

Derechos Humanos y Cultos, 2014).

La cadena de custodia se debe mantener meticulosamente durante el transporte tomando todas las precauciones necesarias para minimizar la posibilidad de contaminar la evidencia accidentalmente. 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 (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).

3.4. Fase IV (Análisis)

Esta fase es de vital importancia, ya que por medio de la evidencia digital obtenida y si hubieran equipos incautados, el perito informático mediante un examen detallado aplicará procedimientos, herramientas y técnicas poniendo todos sus conocimientos en la búsqueda de vestigios de lo que se quiere encontrar para llegar a responder las interrogantes de quién, cómo, cuándo, y donde sucedieron los hechos.

Es decir, esta fase es en sí el porqué de la investigación, brindando el máximo de información clara para poder documentar todo adecuadamente y realizar el Informe Pericial pertinente al caso.

Según lo que menciona (Gervilla Rivas, 2014) “Cabe recordar que no existe ningún proceso estándar que ayude a la investigación y habrá que estudiar cada caso por separado teniendo en cuentas las diversas particularidades que nos podamos encontrar”.

Por lo mencionado anteriormente, se pueden destacar varios procedimientos que habrá que adaptar en cada caso y recordar que el análisis únicamente se lo debe realizar en el Laboratorio Forense.

1. **Preparar un entorno de trabajo adaptado a las necesidades del incidente**

Retirar el embalaje de las evidencias transportadas al laboratorio forense, las cuales sólo podrán ser quitadas por el perito informático para su estudio o análisis.

Realizar un fuerte resguardo del material motivo de estudio, ya que esta es sensible a cambios de temperatura y en algunos casos a los campos electromagnéticos.

Se deberá definir las herramientas tanto de hardware como software determinadas para llevar a cabo la investigación y el análisis.

No se debe trabajar con la evidencia original sino con una copia del mismo, y del ser el caso y por precaución se deberá realizar una tercera copia, comprobar su integridad y trabajar sobre ella, de tal modo que en caso de cualquier alteración de los datos siempre

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

se tenga la segunda copia exacta al original de donde poder volver a realizar otra copia para realizar el análisis.

2. Reconstruir una línea temporal con los hechos sucedidos

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.

Registrar las fechas de modificación, acceso, cambio y borrado de archivos.

Registrar el huso horario de lugar del incidente con el lugar del análisis.

Realizar un estudio de los metadatos.

Acudir a los registros del sistema operativo el cual brindará información relativa a programas instalados, creación de usuarios, instalación del sistema operativo, archivos ocultos y eliminados.

Con los datos obtenidos se podrá crear un esbozo que permitirán afianzar la evolución de los hechos.

3. Determinar qué procedimiento se llevó a cabo por parte del atacante

Es importante determinar que procesos se ejecutaron por el atacante, con programas específicos y con un volcado de la memoria principal del equipo se determinaran estos procesos.

Llevar a cabo un examen detallado de la información concerniente al caso por ejemplo documentos, fotografías, grabaciones de audio, correos electrónicos, etc.

Identificar archivos fuera de común por ejemplo archivos con extensiones irregulares o posiblemente cambiados de nombre y ubicación de manera intencional con el fin de esconder información.

4. Identificar el autor o autores de los hechos

El volcado de la memoria proporciona información sobre las conexiones de red, ayudando a relacionar el posible origen del ataque buscando como datos como la dirección IP.

El perfil de usuario es otra fuente de información sobre las configuraciones en el entorno de trabajo de cada usuario. Incluyendo configuración de pantalla, programas instalados, conexiones de red, recursos a los que tiene acceso, etc.

Acudir a las cookies e historiales de internet suele ser de gran ayuda cuando se requiere obtener mayor información en la identificación del autor o autores que se investigan.

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

5. Realizar su experticia únicamente en lo que ha sido designado

Los castigos pueden ser severos cuando el Perito Informático no realiza una adecuada investigación forense. 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, lo que conlleva a que se inicie nuevamente el proceso de indagación e incluso con privación de libertad como le establece el Artículo 178 del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014), sobre la violación a la intimidad. Y el Artículo 511, inciso 8 del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014), sobre la pericia.

6. Documentar todo lo realizado

Documentar los procedimientos seguidos durante toda la fase de análisis, esto debido a que los resultados obtenidos deben ser completamente verificables y reproducibles por otro investigador forense con el fin de reconstruir lo realizado durante la investigación o en el caso de existir un recurso de revisión como lo menciona el Artículo 658, inciso tres del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).

3.5. Fase V (Documentación)

En esta Fase el Perito Informático debe tener todas las consideraciones mínimas para redactar el Informe Pericial, de tal manera que todas las actividades realizadas desde la Fase de Requisitos hasta la Fase de Análisis queden plasmadas en el documento y presentado dentro del plazo establecido, como lo establece el Artículo 511, inciso cinco y seis del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014). De la misma manera y de forma obligatoria el informe debe ser presentado y subido al Sistema Informático Pericial, en archivo PDF; el mismo que pueda ser descargado, conocido, estudiado por las y los interesados.

Las 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 (Consejo de la Judicatura, 2014).

El objetivo principal del Informe Pericial se centra en plasmar el conocimiento experto al proceso judicial, la claridad con que se presenten los resultados de la investigación marcará la diferencia si es aceptado la evidencia o no en un proceso legal, evitando al máximo los tecnicismos en su redacción siendo consistente con los hechos y resultados obtenidos. Estableciendo para ello un formato general de uso obligatorio que estandarice

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

la presentación, como lo establece el Artículo 19 y 20 de la Resolución 040- 2014 (Consejo de la Judicatura, 2014), siendo claro y entendible para las autoridades competentes.

El formato puede ser descargado desde la página web de la función judicial en la sección Peritos, los requisitos obligatorios de todo informe pericial son los siguientes:

1. **Datos generales del juicio, o proceso de indagación previa**

En este punto deben 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.

2. **Parte de antecedentes**

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.

3. **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.

4. **Parte de conclusiones**

Es el fruto del conocimiento del Perito, es lo que idealmente servirá de fundamento para el dictamen 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.

5. **Documentos de respaldo, anexos, o explicación de criterio técnico**

Se 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 deberá exponer y justificar claramente desde todo punto de vista las razones especializadas para llegar a la conclusión correspondiente incluidas en el informe pericial.

6. **Otros requisitos**

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

7. **Información adicional**

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

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.

8. 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.

9. Firma y rúbrica

Finalmente, 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.

Como recomendación final en la elaboración del informe pericial no debe ser extenso y redactado con un lenguaje compresible para un público no técnico explicando las razones por las cuales se ha llegado a tal o cual conclusión. Adjuntando todos los formularios que avalen el resultado de la investigación realizada, para que de esta manera se pueda judicializar la evidencia obtenida con elementos claros, contundentes y útiles.

3.6. Fase VI (Presentación)

Finalmente, con esta Fase culmina la metodología propuesta, ya que una vez culminado el informe pericial resultante de todo el procedimiento llevado en cada una de las Fases anteriores y remitiéndolo al solicitante de la pericial. 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, como lo establece el Artículo 505 del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).

Esta defensa oral tiene por objeto la aclaración, ratificación o ampliación de la pericia realizada ya que sin ella las conclusiones del examen pericial, carecerán de valor y no formará parte de la prueba que deba ser valorada por el juez, como lo establece el Artículo 222 del COGEP (Consejo de la Judicatura, 2015).

De la misma manera 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. Cabe mencionar que la inasistencia injustificada

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

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.

Sin embargo, los peritos volverán a declarar cuantas veces lo ordene la o el juzgador en la audiencia de juicio, como lo establece el Artículo 503, inciso tres del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014). Por lo mencionado anteriormente existen algunas habilidades y destrezas que todo perito debe tener en cuenta al momento de exponer en audiencias que son:

- Vestir adecuada al contexto lo cual denotara respeto a los sujetos procesales y la profesión de quien expone.
- Mantener una actitud respetuosa y cordial al otro profesional que puede discrepar el informe pericial, es señal de madurez psicológica y solvencia profesional.
- Responder a las preguntas con un lenguaje claro y comprensible, manteniendo la calma y 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 indiqué si debe responder o no.
- El interrogatorio directo es el que realiza la parte que introdujo al perito al proceso. Por lo cual el perito deberá acreditar su experiencia y exponer los fundamentos de los resultados de su pericia.
- Se pueden realizar preguntas y presentar pruebas no anunciadas oportunamente orientadas a determinar su parcialidad y no idoneidad, a desvirtuar el rigor técnico de sus conclusiones, así como impugnar su credibilidad, como lo establece el Artículo 511, inciso seis y siete del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).
- Los peritos podrán responder las preguntas del interrogatorio de las partes por cualquier medio y acompañar sus informes mediante ilustraciones gráficas, como lo establece el Artículo 511, inciso seis y siete del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014).
- Si existen informes periciales divergentes, el juez dispondrá un debate entre los peritos, para luego iniciar un interrogatorio y contrainterrogatorio de las partes hacia el perito para aclarar los puntos en controversia, como lo establece el

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

Artículo 222 del COGEP (Consejo de la Judicatura, 2015).

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.

3.7. Caso práctico

A continuación, se demuestra el uso de las herramientas en un proceso penal, donde el Ing. Juan Grijalva pone en práctica su experticia como Perito Informático.

El Artículo 104 del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014) señala que la pena privativa de libertad contra personas que publiciten, transmitan, descarguen, almacenen, compren, posean para uso personal o intercambio de material pornográfico de niños, niñas y adolescentes, es de 10 a 13 años.

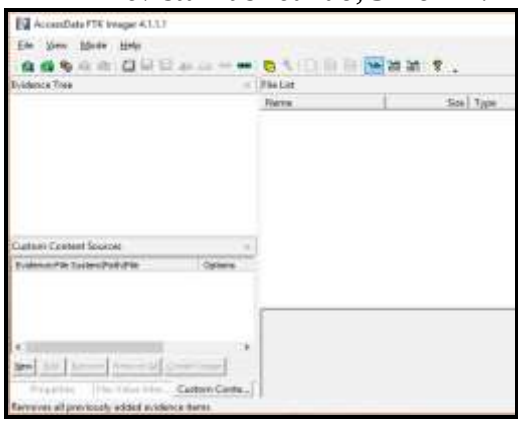
Ante este delito en Quito – Ecuador 2017, la Fiscalía provincial de Pichincha presentó este 27 de noviembre cargos en contra del ciudadano José Ignacio C., de 33 años, en la Unidad Judicial de Garantías Penales, Contravenciones y Menores Infractores. Al finalizar la audiencia, el juez acogió los elementos presentados por el fiscal de Pichincha, dictando prisión preventiva contra el acusado. Mientras se realizan las respectivas investigaciones pertinentes, el Juez solicita que se realicen la respectiva investigación forense al equipo tecnológico en donde se presume que existe material pornográfico. El Perito al cumplir con su deber accede a la posesión del caso donde se le es entregado el equipo con los sellos de seguridad. Finalmente la instrucción fiscal durará 30 días, para determinar responsables.

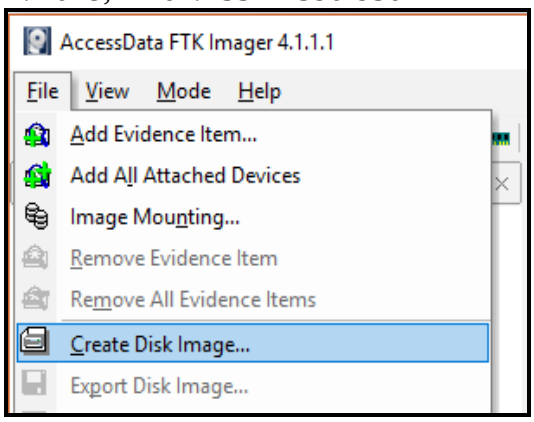
El equipo tecnológico es entregado al Perito Informático, y posterior a ello con las medidas de seguridad respectivas es transportado con el propósito de iniciar la investigación forense en su laboratorio forense.

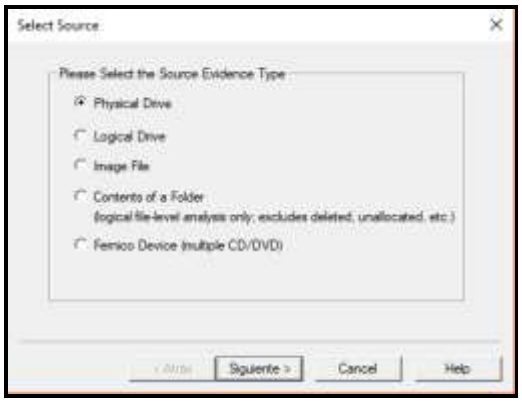
Hay que resaltar que el Perito Informático debe trabajar bajo un estándar o norma para evitar errores y retrasos en cada uno de los procesos judiciales inmersos, con el fin de evitar el desprestigio público sobre un trabajo mal realizado.

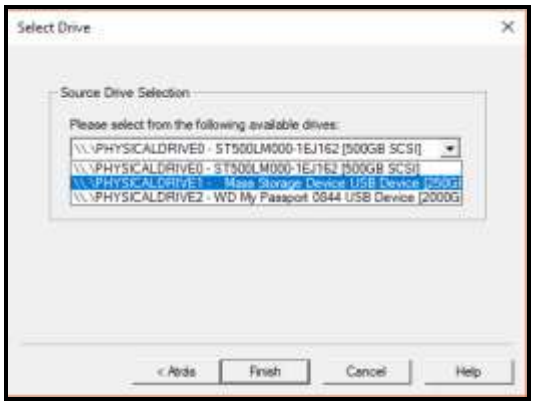
A continuación, el Perito Informático procede a la creación de la imagen forense con la herramienta FTK Imager 4.1.1.1 cómo se ilustra en la Fig. 7.

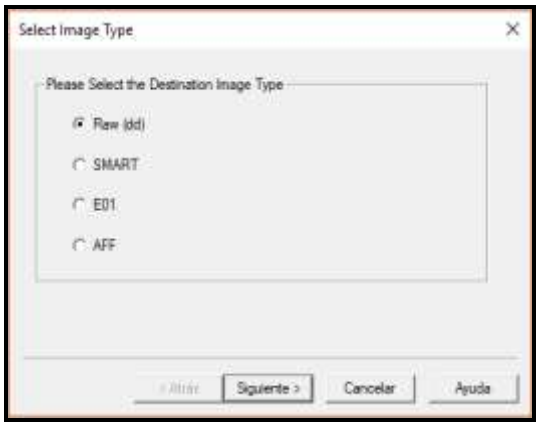
Received: 20-01-2018
Approved: 03-03-2018

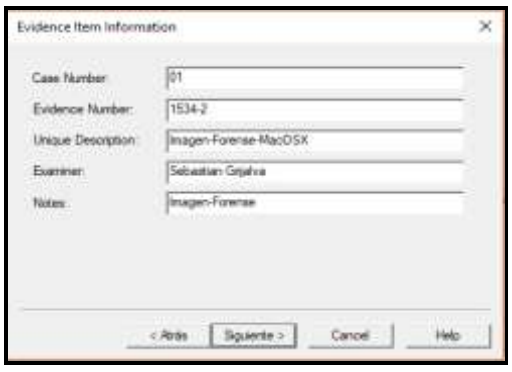


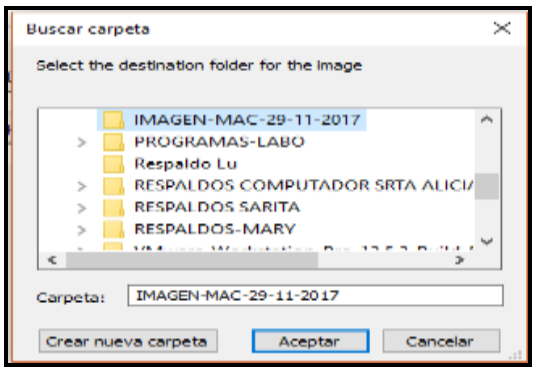












Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

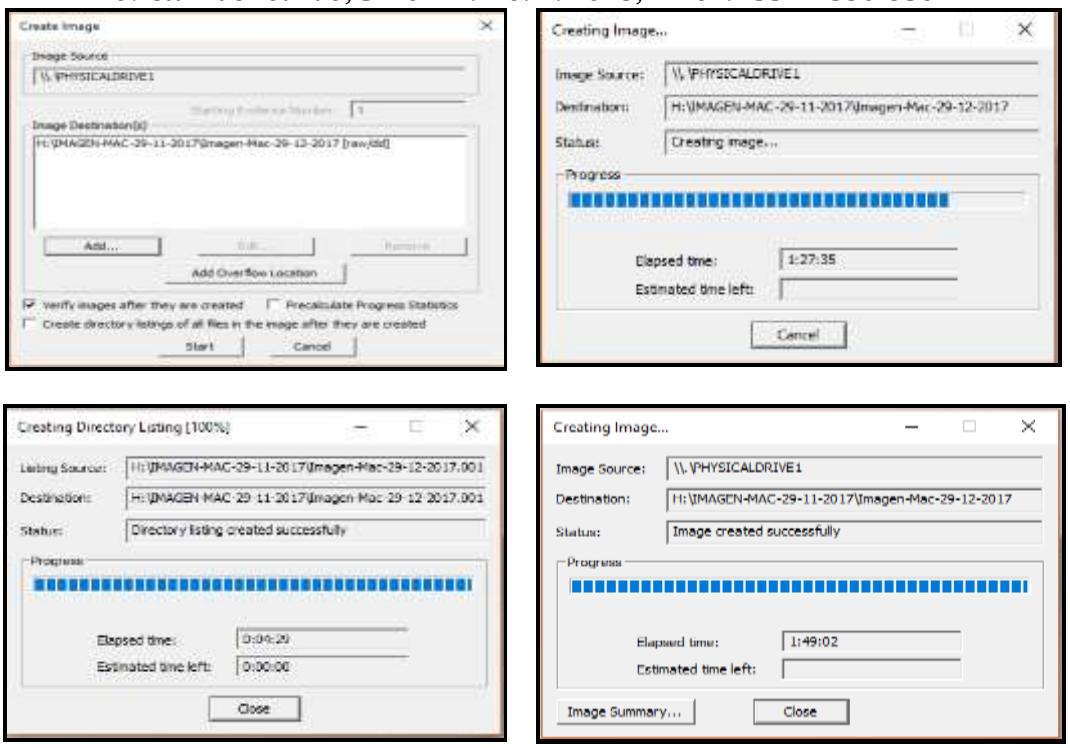
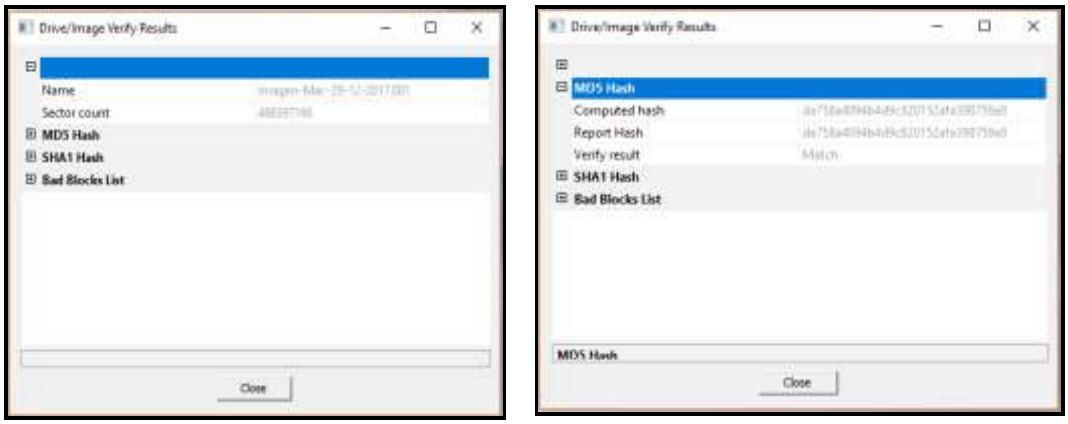


Figura No 7. Creación de la imagen forense del disco duro

En la Fig. 14, se ilustra los resultados obtenidos de la imagen forense, la comprobación de los hash (MD5, SHA1) obtenidos y también de que no existió ningún bloque defectuoso.



Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

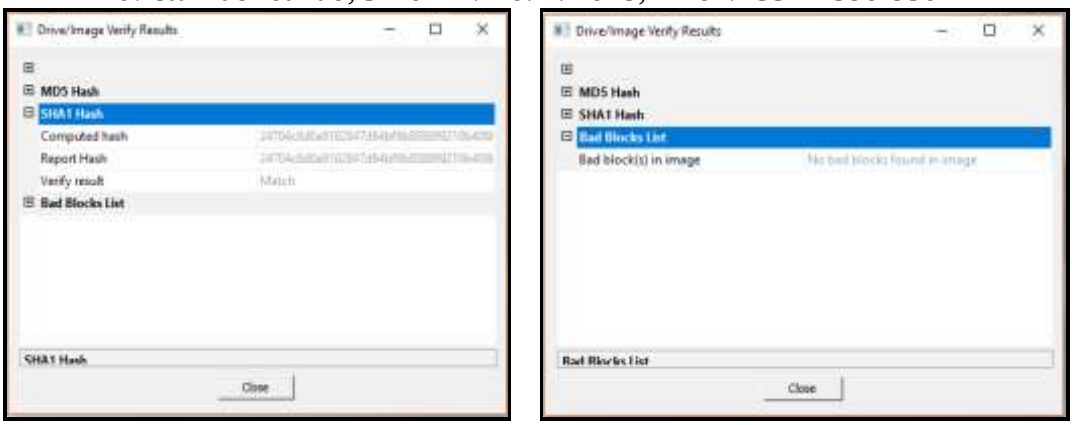
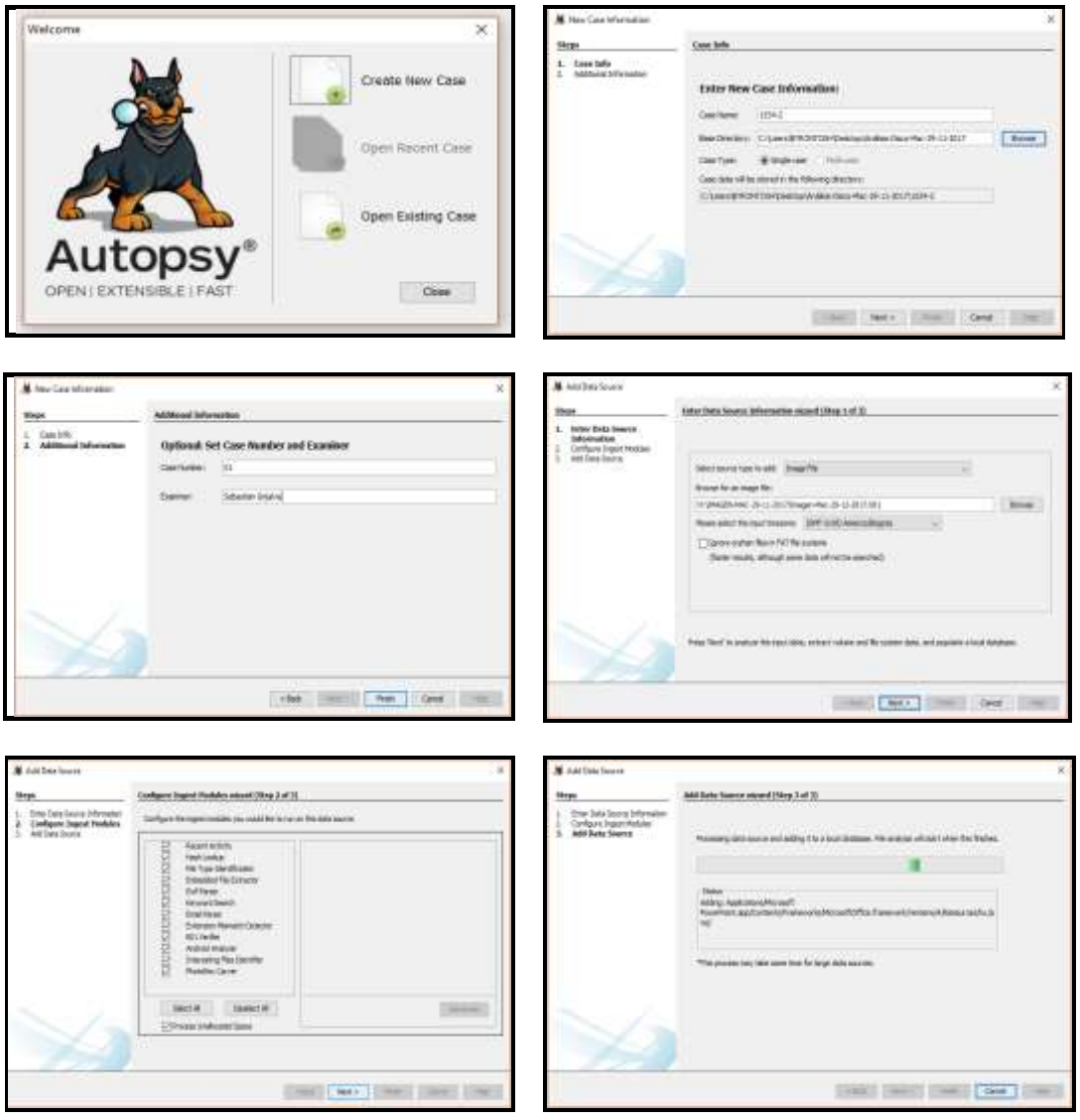


Figura No 8. Comprobación de la imagen forense creada

Una vez obtenida la respectiva imagen forense, el Perito Informático procede a realizar el análisis de la imagen forense con la herramienta Autopsy 4.0.0. Como se ilustra en la Fig. 8.



Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

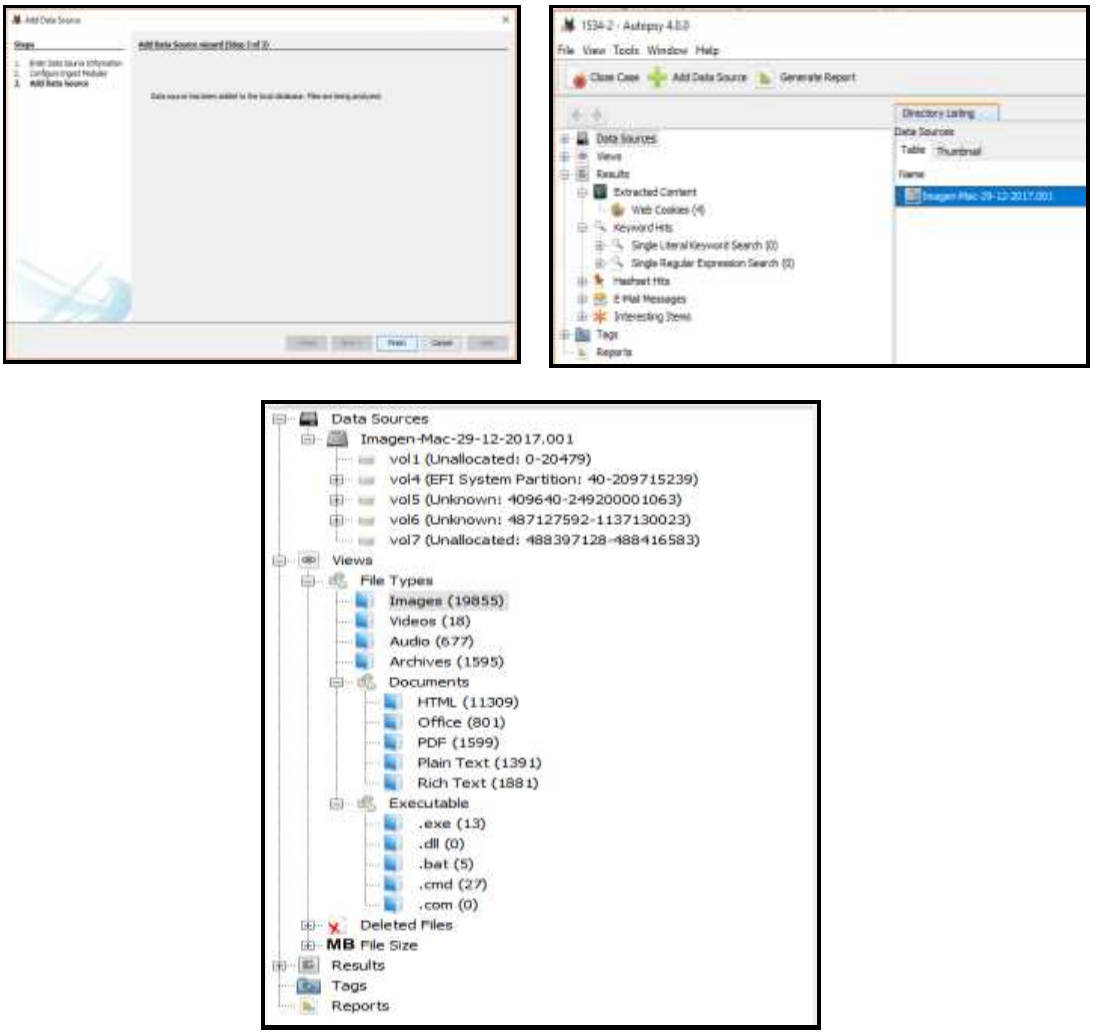
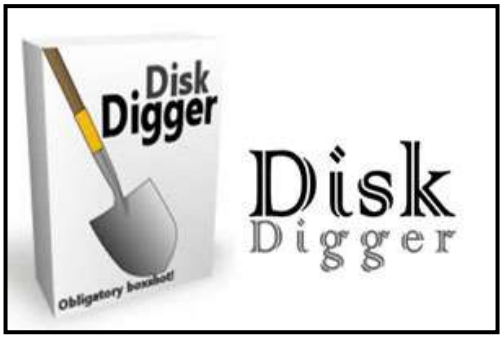
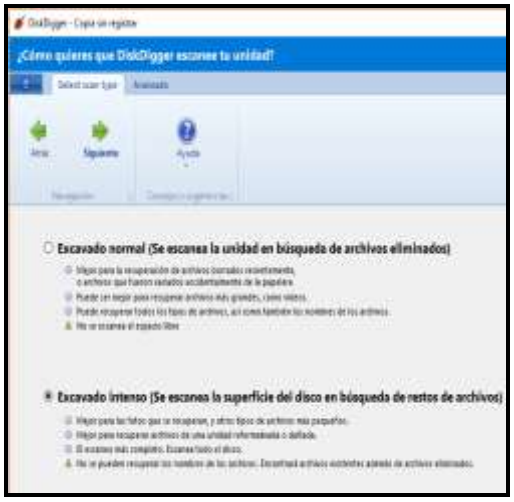


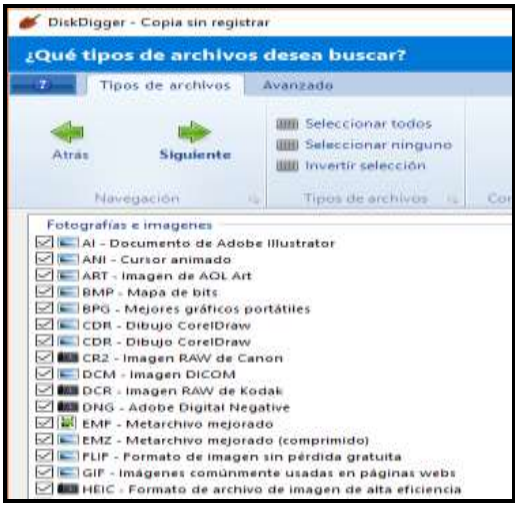
Figura No 8. Análisis de la imagen forense con la herramienta Autopsy 4.0.0

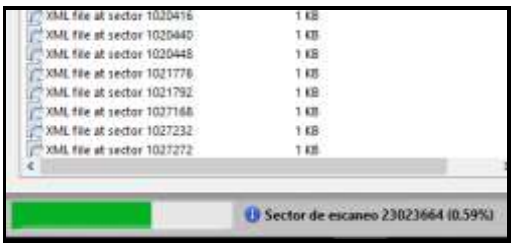
De la misma manera el Perito Informático realiza otro análisis con la herramienta DiskDigger 1.17 para poder encontrar más fuentes de evidencia, como se ilustra en la Fig. 9.

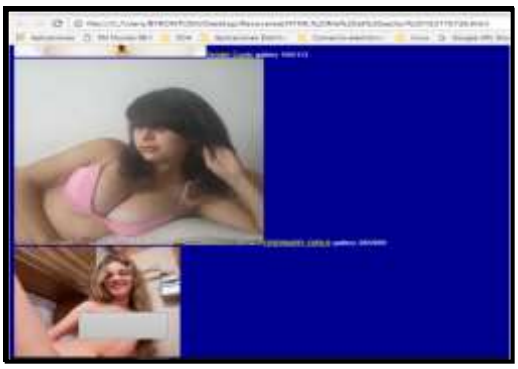
Received: 20-01-2018
Approved: 03-03-2018











Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

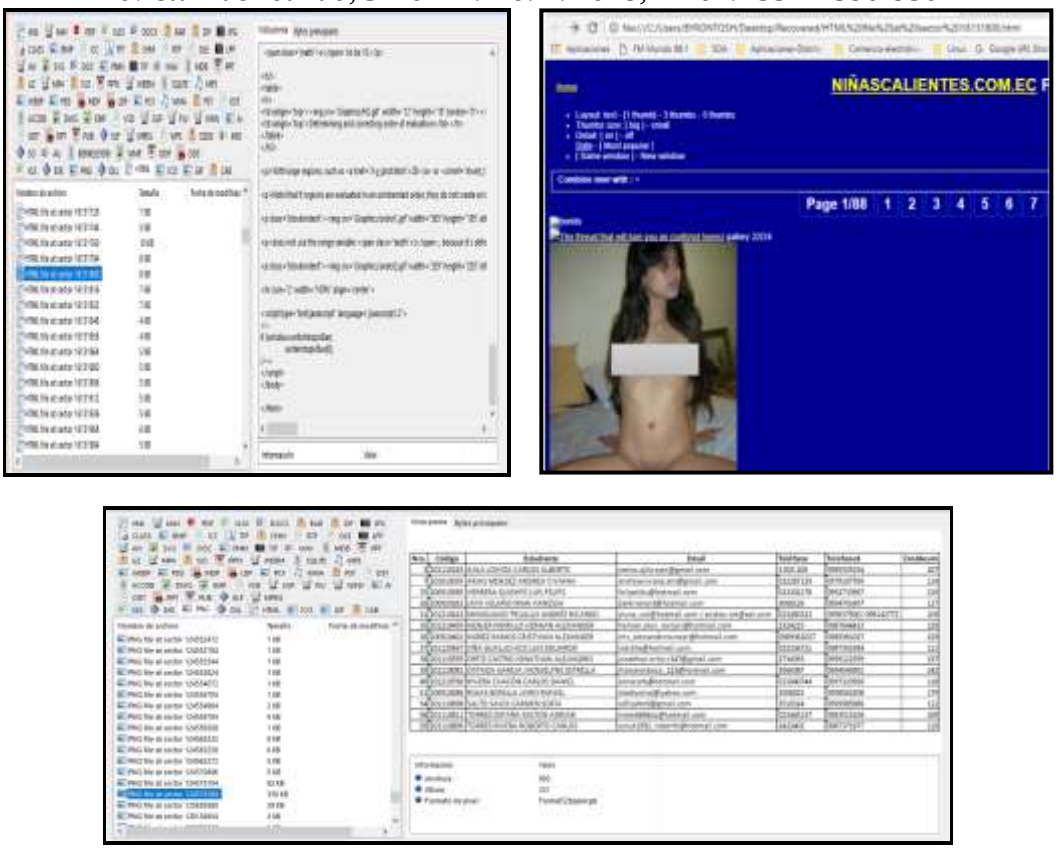


Figura No 9. Análisis de la imagen forense con la herramienta DiskDigger 1.17.

Este punto es de vital importancia ya que mediante los resultados obtenidos por parte de las 2 herramientas se procede a realizar un análisis más detallado, como se ilustra en la Fig. 10. Con lo cual el Perito Informático evidencia que existen imágenes sobre:

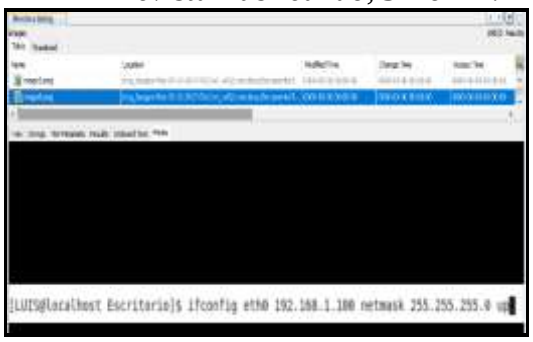
- Direcciones IP
- Nombre de usuario del Equipo Tecnológico
- Fondo de pantalla del Equipo Tecnológico
- Diversas imágenes de adolescentes

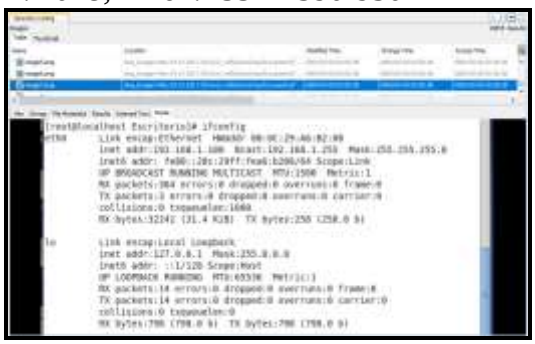
De la misma manera se determinó páginas web con más imágenes de adolescentes y archivos ofimáticos que en cada uno contenía:

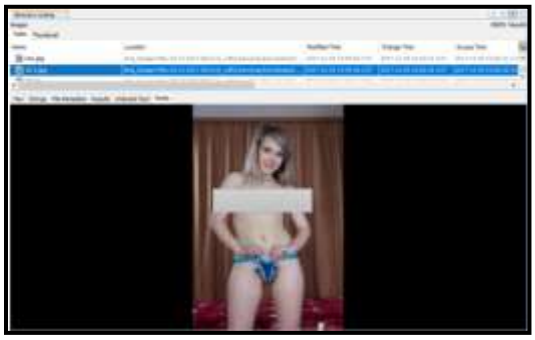
- Conversaciones
- Transferencias bancarias
- Listado de personas con números telefónicos y correos electrónicos

Cada evidencia fue conservada en un archivo adicional, para ser presentada en el informe final como parte de los Anexos.

Received: 20-01-2018
Approved: 03-03-2018







Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

Figura No 10. Análisis de la imagen forense con la herramienta DiskDigger 1.17.

Pero de todo el análisis existió una imagen en particular, el tamaño que tenía era demasiado para una imagen normal y corriente. Con lo cual se presume que puede contener algún metadato.

Por consiguiente se utiliza otra herramienta adicional para comprobar si existe información contenida sobre dicha imagen, como se ilustra en la Fig. 11.

Figura No 11. Análisis de una imagen con la herramienta Steganography 1.8

Finalmente se determinó que la imagen original contenía otra imagen adicional, como se mencionó todos los resultados obtenidos serán incluidos en el informe pericial.

Una vez culminado el análisis forense respectivo se procede a elaborar el respectivo

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

informe pericial, establecido en la fase V de la presente metodología. En esta Fase el Perito Informático debe tener todas las consideraciones mínimas para redactar el Informe Pericial, de tal manera que todas las actividades realizadas desde la Fase de Requisitos hasta la Fase de Análisis queden plasmadas en el documento y presentado dentro del plazo establecido

El formato puede ser descargado desde la página web de la función judicial en la sección Peritos, los requisitos obligatorios de todo informe pericial son los siguientes:

1. **Datos generales del juicio, o proceso de indagación previa**
2. **Parte de antecedentes**
3. **Parte de consideraciones técnicas o metodología a aplicarse**
4. **Parte de conclusiones**
5. **Documentos de respaldo, anexos, o explicación de criterio técnico**
6. **Otros requisitos**
7. **Información adicional**
8. **Declaración juramentada**
9. **Firma y rúbrica**

Como recomendación final en la elaboración del informe pericial no debe ser extenso y redactado con un lenguaje compresible para un público no técnico explicando las razones por las cuales se ha llegado a tal o cual conclusión. Adjuntando todos los formularios que avalen el resultado de la investigación realizada, para que de esta manera se pueda judicializar la evidencia obtenida con elementos claros, contundentes y útiles.

Para finalizar en la fase VI de la presente metodóloga propuesta el Perito Informático deberá sustentar oralmente los resultados del peritaje como una de sus obligaciones tanto en procesos Penales y Civiles.

4. CONCLUSIONES

- Al finalizar el presente proyecto de investigación se concluye que se ha creado una guía metodológica eficiente para el análisis forense en equipos de cómputo con sistema operativo Mac OSX, beneficiando a los Peritos Informáticos en su labor diaria y a los jueces para que puedan dictar una sentencia justa en un proceso judicial, por medio de un correcto informe pericial.
- El desarrolló de la guía metodología se fundamentó en aspectos relevantes de cada uno de los estándares, normas, herramientas y buenas prácticas emitidas por

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

organizaciones internacionales especializadas en el tema, para que los Peritos Informáticos tomen en cuenta en el momento de realizar una investigación informática forense y no exista confrontación respecto a la validez de la evidencia, así como del proceso de adquisición y preservación de la misma.

- El uso y difusión de esta guía metodológica, permitirá que siga adquiriendo relevancia y fortaleciéndose, debido a los nuevos y diversos delitos informáticos que existen en el Ecuador.
- Los procedimientos a seguir y herramientas utilizadas avalaron que la integridad de la evidencia original no sea alterada, con lo cual se garantiza la admisibilidad en los tribunales y no ser vulnerable a una objeción de descalificación.
- La fase de análisis es de vital importancia en toda investigación forense, ya que permite aclarecer el delito cometido, por lo cual se debe trabajar con las herramientas adecuadas y en todo momento tener calma y paciencia para obtener los resultados esperados.

5. REFERENCIAS BIBLIOGRÁFICAS

Abril, V. H. (2008). *écnicas e Instrumentos de la Investigación.* Recuperado de http://s3. amazonaws. com/academia. edu. documents/41375407/Tecnicas_e_Instru mentos_Material_de_clases_1. pdf

AENOR. [EN LINEA]. *UNE 71505-1:2013.* Obtenido de http://www.aenor.es/aenor/inicio/home/home.asp

Azas Manzano, M. F. (2015). *DISEÑO DE UN MODELO PARA LA CADENA DE CUSTODIA Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE DE EQUIPOS TECNOLÓGICOS EN PROCESOS JUDICIALES EN EL ECUADOR.* (Tesis Ingeniería). Universidad Internacional SEK. Ecuador.

Brezinski, D., & Killalea, T. (2002). *Guidelines for evidence collection and archiving*. Recuperado de http://www.rfc-editor.org/info/rfc3227

Ciardhuáin, S. Ó. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence*, 22.

Consejo de la Judicatura. (2014). *Reglamento del sistema pericial integral de la función judicial.* Recuperado de http://www.funcionjudicial.gob.ec/index.php/es/component/content/article/25-

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

consejo-judicatura/380-peritos.html

Consejo de la Judicatura. (2015). *Código Orgánico General de Procesos.* Recuperado de http://www.funcionjudicial.gob.ec/index.php/es/normativa/codigo-organico-general-de-procesos.html

Consejo de la Judicatura. (2016). *RESOLUCIONES DEL PLENO DEL CONSEJO DE LA JUDICATURA 2016.* Recuperado de http://www.funcionjudicial.gob.ec/index.php/es/component/content/article/25-consejo-judicatura/510-resoluciones-2016.html

Consejo de la Judicatura. (2017). *RESOLUCIONES DEL PLENO DEL CONSEJO DE LA JUDICATURA 2017.* Recuperado de http://www.funcionjudicial.gob.ec/www/pdf/resoluciones/2017/068-2017.pdf

Gervilla Rivas, C. (2014). *Metodología para un análisis forense.* (Tesis de Maestría). Universitat Oberta de Catalunya.

Grijalva Lima, Juan Sebastián; Loarte Cajamarca , Byron Gustavo;. (2017). Modelo para el análisis forense y la legalización de evidencia digital atípica en procesos judiciales en Ecuador. CienciAmérica: Revista de divulgación científica de la Universidad Tecnológica Indoamérica. Recuperado de https://dialnet.unirioja.es/descarga/articulo/6163708.pdf

Hart, S., Ashcroft, J., & Daniels, D. (2004). *Forensic examination of digital evidence: a guide for law enforcement.* Washington DC, USA, Tech. Rep. NCJ, 199408.

ISO/IEC 27037. (2012). Guidelines for identification, collection,acquisition and preservation of digital evidence. 38. Recuperado de https://www.iso.org/standard/44381.html

Laguna, C. P., & Oruña, A. R. (2003). *MAC OS X: PANTHER. En LA EVOLUCIÓN DE LAS ESPECIES.* Barcelona. Recuperado de http://docencia.ac.upc.es/FIB/CASO/seminaris/1q0304/M11_Informe.pdf

Received: 20-01-2018
Approved: 03-03-2018

Revista Publicando, 5 No 14 . No. 1. 2018, 24-67. ISSN 1390-9304

Loarte Cajamarca, B. G., & Grijalva Lima, J. S. (2017). Elaboración de un marco de trabajo estandarizado para el análisis forense de la evidencia digital en procesos civiles y penales en el Ecuador para ser utilizado por los Peritos acreditados en Informática por el Consejo de la Judicatura del Ecuador. *Revista Publicando, 4*(11), 42-78. Recuperado de http://www.rmlconsultores.com/revista/index.php/crv/article/view/463/pdf_341

Ministerio de Justicia, Derechos Humanos y Cultos. (2014). *Código Orgánico Integral Penal* (1ra. ed.). Quito: Ediciones Legales.

softwarelibre.conocimiento.gob.ec. (2008). Recuperado de Decreto Ejecutivo 1014: https://softwarelibre.conocimiento.gob.ec/wp-content/uploads/2016/04/Decreto_1014_software_libre_Ecuador_c2d0b.pdf

Received: 20-01-2018
Approved: 03-03-2018