UNIVERSIDAD INTERNACIONAL SEK

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Plan de Investigación de fin de carrera titulado:

"DESARROLLO DE UNA GUÍA METODOLÓGICA PARA EL ANÁLISIS FORENSE DIGITAL EN EQUIPOS DE CÓMPUTO CON SISTEMA OPERATIVO Mac OS X EN EL ECUADOR"

Realizado por:

LOARTE CAJAMARCA BYRON GUSTAVO

Director de Proyecto:

MSc. JUAN SEBASTIÁN GRIJALVA LIMA

Como requisito para la obtención del título de:

MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

Quito, ENERO de 2018

DECLARACION JURAMENTADA

Yo, BYRON GUSTAVO LOARTE CAJARMARCA, con cédula de identidad #171765322-2, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Byron Gustavo Loarte Cajamarca

C.C.: 171765322-2

DECLARATORIA

El presente trabajo de investigación titulado:

"DESARROLLO DE UNA GUÍA METODOLÓGICA PARA EL ANÁLISIS FORENSE DIGITAL EN EQUIPOS DE CÓMPUTO CON SISTEMA OPERATIVO Mac OS X EN EL ECUADOR"

Realizado por:

BYRON GUSTAVO LOARTE CAJAMARCA

Como requisito para la Obtención del Título de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA

Ha sido dirigido por el profesor

ING. JUAN SEBASTIÁN GRIJALVA LIMA, MSc.

Quien considera que constituye un trabajo original de su autor

Ing. Juan Sebastián Grijalva Lima, MSc.
DIRECTOR

DEDICATORIA

Dedico este trabajo a mi madre, hermana y mi familia por confiar siempre en mí y enseñarme que los sueños son posibles de alcanzar.

A la memoria de mi Padre que desde el cielo me cuida.

A Janneth P., Diana T. y Cristian A. por estar conmigo en los buenos y malos momentos, apoyándome con sus consejos y buenos deseos. Gracias por todo.

Finalmente, a todos mis compañeros de la carrera ya que juntos logramos formar una amistad tanto personal como profesional.

AGRADECIMIENTO

Al Ing. Sebastián Grijalva por su acertada dirección del proyecto de investigación. Su apoyo, profesionalismo y entrega fueron determinantes a la hora de conformar este documento.

A la Ing. Verónica Rodríguez, Ing. Mónica Romero y el Ing. Edison Estrella, quienes supieron impartir todos sus conocimientos durante la carrera, lo cual aportó una visión diferente e integradora para mi investigación.

A la Universidad Internacional SEK, por su esfuerzo en formar profesionales legítimos.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS Y FIGURAS

RESUMEN

La tecnología avanza cada día más rápido, y parte de ello se evidencia en el aumento del uso de las TIC (Tecnologías de la Información y Comunicación), como lo son correos electrónicos, video conferencias, redes sociales, internet, etc. en la vida cotidiana.

A medida que estas nuevas tecnologías se han desarrollado buscan satisfacer las necesidades de la sociedad mediante facilitar la realización de las tareas cotidianas de sus usuarios, quiénes masivamente consumen productos y servicios tecnológicos que los expone a nuevas amenazas de seguridad. Amenazas que se engloban en un sin número de delitos informáticos cometidos por diversos medios, entre los cuales 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 el Ecuador, el proceso judicial requiere de un proceso formal y avalado de judicialización de la evidencia, en este caso, evidencia proveniente de equipos de cómputo. Para lo cuál, el país requiere peritos informáticos o personas capacitadas en el uso de tecnologías específicas.

En nuestra investigación, evidenciamos que el sistema operativo Mac OS X no es ampliamente conocido por los expertos que ejercen su función como peritos informáticos. Además en el país, no existen metodologías que permitan a un perito informático recabar evidencia forense proveniente de estos equipos de cómputo. Ante esta problemática este trabajo plantea dotar una guía metodológica para el análisis forense en un equipo de cómputo con sistema operativo Mac OS X. Esta guía es un manual para el proceso judicial y busca ser usado por peritos informáticos. Esta guía toma como referencia herramientas, estándares, normas, buenas prácticas y guías propuestas por las principales organizaciones internacionales especializadas en el entorno de la informática forense, apegada al cien por ciento, a la actual normativa legal en el Ecuador. Esta guía pretende facilitar a los peritos informáticos en el país judicializar la evidencia proveniente de estos equipos de cómputo.

Palabras claves: Análisis forense, Sistema Operativo Mac OS X, informática forense, Perito Informático, TIC, Normativa legal en el Ecuador, Evidencia digital, Metodología de Análisis Forense.

ABSTRACT

Technology grows faster each day, and this is noticeable through the growth in ICT (Information and Communication Technologies) such as e-mail, video chat, social media, the internet, etc. in each day activities.

These technologies try to satisfy consumer needs through easing each day activities, which has led to mass consumption of technology products and services. Unfortunately, consumers are exposed to new security threads which are compiled in a variety of cybercrimes such as: data theft, digital bank account fraud, digital system hacking, grooming, child pornography, among others.

Ecuador's legal system requires a formal judiciary process to properly handle digital evidence. Hence, the country requires digital forensic analysts or people qualified in specific technologies to carry out this process.

In this research, we first show that the operating system: Mac OS X is not well known by the experts in digital forensic analysis in the country. Furthermore, we realize that there is not a methodology nor a guide that help a digital forensic analyst to analyze a computer with Mac OS X. Therefore, we propose this guide as a manual that takes tools, standards, norms, good practices and specialized international guides a hundred percent within the Ecuadorian law. This guide is meant to guide digital forensic analysts in the country to technically and within the law handle digital evidence of Mac OS X machines.

Keywords: Forensic analysis, Mac OS X, forensics, digital forensics analyst, ICT, Ecuadorian digital regulations, digital evidence, forensic analysis methodology.

CAPÍTULO I

INTRODUCCIÓN

1.1 EL PROBLEMA DE INVESTIGACIÓN

1.1.1 Planteamiento del Problema

En la actualidad es impresionante observar como el mundo se ha digitalizado, y la vez se ha incrementado la tecnología para actividades delictivas informáticas. El escaso conocimiento por parte de las víctimas de cómo protegerse de los delitos informáticos a través de las nuevas tecnologías, otorga a los delincuentes las llaves a las puertas de un inmenso campo fértil de potenciales víctimas de ataques.

En una publicación de El Comercio se menciona que "En el caso del Ecuador, la Fiscalía concluyó que en el 2014 este tipo de robos sumaron más de dos millones de dólares. Las bandas siempre se inventan modos para actuar.
QUITO.- Cinco áreas son vulnerables a los delitos cibernéticos, que en el Ecuador se han incrementado en un 16%." (AGN, 2015)

Es por eso que en el país estos delitos ya pueden ser sancionados como lo menciona la Fiscalía General del Estado en su página web "La Dirección de Política Criminal de la Fiscalía General del Estado registró 626 denuncias por delitos informáticos desde el 10 de agosto del 2014 -cuando entró en vigencia el Código Orgánico Integral Penal (COIP)- hasta el 31 de mayo del 2015. A partir del COIP se tipifica este tipo de delitos." (Fiscalia.gob.ec, 2015)

Pero 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 también que han sido procesados electrónicamente en algún medio computacional, como por ejemplo programas, mensajes y datos transmitidos en formato digital.

El hecho de que la información haya dejado de estar en papel para almacenarse digitalmente en cualquier medio tecnológico, toma mayor relevancia en un procedimiento de tipo penal o civil, esto a su vez, genera Pericias Informáticas muy específicas en obtener la evidencia, provocando una serie de incidentes:

- La 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.

- Actualmente la 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 se acepte legalmente en un tribunal.

- Desconocimiento acerca de los 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.

Finalmente se establece la causa principal causa, mediante los incidentes citados anteriormente que no permite judicializar la evidencia digital proveniente de equipos de cómputo con sistema operativo Mac OS X.

Lo mencionado anteriormente da como resultado la incidencia de este tipo de delitos 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.

1.1.1.1 Diagnóstico

En la actualidad el rápido avance y crecimiento exponencial de las Tecnologías de la Información, ha dado paso a que la información que se maneja en medios informáticos tenga un valor muy alto para las empresas. Esto motiva a la búsqueda de información de manera ilícita quebrantando la intimidad; provocando la eliminación, alteración o daño en la información, provocados en ocasiones por las mismas organizaciones o grupos delincuenciales, además de los comúnmente crackers y hackers que buscan otros fines. (Arroyo Jácome, 2016)

De la misma manera es impresionante ver como el desarrollo de la tecnología informática se ha convertido en una herramienta más para el cometimiento de los actos mencionados anteriormente, los cuales son dirigidos principalmente contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Estos actos suelen ser denominados en la actualidad como delitos informáticos.

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

El uso cada vez más progresivo de las Tecnologías de Información y Comunicación ha cambiado la forma en que realizamos nuestras actividades, y de la misma manera ha generado nuevas formas de ataque por parte de los criminales que usan las redes y computadoras, por ejemplo: fraudes, estafas, negación de servicios, cibercrimen, ciberterrorismo, pornografía

infantil, falsificación de tarjetas, spam, pishing, etc. Todos estos tipos de delitos reconocidos por la Organización de las Naciones Unidas (ONU).

De la misma manera, se realizó una fundamentación teórica de los síntomas mencionados, en el que se puede evidenciar el nivel de estudios que ostentan los peritos acreditados mediante el Sistema Pericial de la página web de la función judicial y de la página web de la Senescyt.

Para dicho estudio se seleccionó a peritos que cumplían los siguientes parámetros:

- **Provincia:** Pichincha
- **Área o Profesión:** Ingeniería
- **Especialidad:** Ingeniería Informática o de Sistemas

Para lo cual de 20 peritos informáticos se obtuvieron los siguientes resultados:

- **19** tienen título de tercer nivel
- **10** tienen título de cuarto nivel
- **1** tiene título de nivel Técnico o Tecnológico Superior.

Lo que conlleva a realizar otro estudio sobre las mallas curriculares de las principales universidades donde obtuvieron su título de tercer nivel.

Dando los siguientes resultados:

En la Escuela Politécnica Nacional se tomó como ejemplo a la carrera de Ingeniería en Sistemas Informáticos y de Computación en donde se evidenció que dentro de su malla curricular pensum 2009B existen materias de Arquitectura de Computadores y Sistemas Operativos de tercero y cuarto nivel respectivamente, que luego de un análisis más detallado de sus programas de estudio se puede concluir que si bien se da un enfoque general a las características de los sistemas operativos no se toma en cuenta al sistema operativo MAC como tal sino más bien se enfocan en los sistemas de software libre y por su parte en la materia de Arquitectura de Computadores es una visión general de los componentes de un computador tipo más no de uno en particular.

De la misma manera, se puede evidenciar que existen metodologías de análisis forenses tradicionales, que a su vez son muy específicas. Como lo mencionan Pous et al. (2009), va a depender mucho del punto de vista de lo que se va a analizar, por ello se tienen los siguientes tipos de análisis forense:

- Análisis forense de sistemas.
- Análisis forense de redes.

- Análisis forense de sistemas embebidos.

Sin embargo, actualmente existen trabajos relacionados sobre análisis forense tanto en dispositivos embebidos y de sistemas, un ejemplo claro es lo que proponen Sánchez et al. (2016) en su "Análisis forense a sistemas operativos mediante la utilización de herramientas Open Source, caso estudio Windows 8", otro ejemplo es lo que propone Pérez, J., (2017) en su "Elaboración de una metodología para la realización del análisis forense en dispositivos móviles basados en Android.". Pero actualmente no existe una metodología enfocada principalmente en equipos de cómputo con sistema operativo Mac OS X.

Con el objetivo de modernizar la investigación científica penal en el Ecuador, la Fiscalía General del Estado cuenta con 8 Centros de Investigación de Ciencias Forenses (CICF).
Cabe mencionar que estos centros que se encuentran distribuidos por todo el país, constan de seis plantas que alberga a 21 secciones. Policías y civiles altamente especializados en técnicas modernas se distribuyen en Criminalística (186); Sistemas de Investigación de Accidentes de Tránsito, (25); y, Medicina Legal (22) que comprende ADN, Psicología, Psiquiatría, Antropología Forense y Odontología. (Ministerio del Interior, 2014).

Pero se evidencia que no existe una Unidad Especializada, como el caso de Estados Unidos donde el FBI cuenta con el "COMPUTER CRIME UNIT", o en España la Guardia Civil que cuenta con un departamento especializado en esta clase de delitos informáticos, por mencionar algunos de ellos.

Según Azas, M., (2015) menciona que actualmente en el Ecuador no existe un modelo a seguir por parte de los Peritos Informáticos que están debidamente acreditados; por ende no toman las medidas necesarias para la realización del trabajo encomendado por Jueces y Fiscales, llevando esto a que no existan controles que evidencien que el equipo tecnológico o las pruebas donde se realizó la investigación no hayan sido alteradas por terceras personas para manipular el resultado de la investigación informática forense.

También se pudo evidenciar mediante una publicación realizada por el diario El Telégrafo, menciona que, desde enero a agosto del 2015 en el ecuador, se presentaron un total de 1026 denuncias relacionadas únicamente a delitos informáticos. Actualmente si bien se redujeron las audiencias fallidas en el Ecuador, aún siguen existiendo un porcentaje significativo del 26% en lo que respecta a daños materiales, violación de la propiedad privada, receptación, apropiación fraudulenta por medios electrónicos, etc. Como lo menciona el diario El Telégrafo en otra de sus publicaciones. De la misma manera según Camana, R. (2016) menciona que el uso de internet en el hogar, da paso para la adquisición de al menos una computadora de escritorio, hecho que en el 2015 a nivel nacional llega al 50,1%, demuestra una tendencia al alza para los siguientes 5 años. Sin embargo, el (Observatorio TIC, 2017), menciona que en el 2016 el porcentaje de hogares que tienen computador escritorio/laptop es del 42,3%. Con estas estadísticas se llega a la conclusión que, si se incrementa el número de equipos de cómputo en el Ecuador, también se incrementaran los delitos cometidos a través de estos medios, lo que ocasiona que no se pueda judicializar la evidencia digital y que las audiencias fallidas aumenten con el pasar de los días.

1.1.1.2 Pronóstico

Los antecedentes citados en el diagnóstico nos permiten concluir que el mundo se ha digitalizado cada vez más y esto ha provocado que se genere un incremento de la tecnología disponible para actividades delictivas informáticas, que combinado con el escaso conocimiento por parte de las víctimas de cómo protegerse de estos delitos a los que pueden ser expuestos, otorga a los delincuentes las llaves a las puertas de un inmenso campo fértil de potenciales víctimas de ataques.

Por este motivo de no tomarse medidas respecto a los delitos que se comenten en estos equipos de cómputo, dichos delitos se desarrollarán cada vez más, y por ende la judicialización de la evidencia proveniente de estos equipos de cómputo no podrá ser procesada legalmente en el Ecuador.

1.1.1.3 Control de Pronóstico

El dotar a los Peritos Informáticos de algún mecanismo que incluya técnicas y herramientas que permitan brindar el conocimiento necesario cuando lo requieran, podría convertirse en una solución donde los Peritos Informáticos contarán con una guía de procedimientos que les ayude a realizar las pericias adecuadas en búsqueda de la evidencia digital, lo que ayudaría a solucionar parte de la problemática, así como hacer campañas preventivas sobre los delitos informáticos y cómo esto está afectando a la sociedad.

1.1.2 Formulación del Problema

Si ocurre un delito en el cuál participe un equipo de cómputo con sistema operativo Mac OSX, la judicialización de la evidencia digital proveniente de los mismos, no se puede procesar debido a la falta de conocimientos técnicos por parte de los peritos informáticos sobre el funcionamiento de estos equipos.

1.1.3 Sistematización del Problema

- ¿Qué método permite al investigador, adquirir el conocimiento necesario para determinar las fuentes de evidencia digital?
- ¿Qué técnicas permite al investigador, adquirir el conocimiento sobre normas, estándares o buenas prácticas para el manejo adecuado de la evidencia digital proveniente de equipos de cómputo con sistema operativo Mac OS X?
- ¿De qué forma permite al investigador, adquirir el conocimiento sobre las metodologías y fases que debe seguir para judicializar la evidencia digital proveniente de equipos de cómputo con sistema operativo Mac OS X?

- ¿Cómo puede adquirir el investigador conocimiento sobre las herramientas que existen para obtener la evidencia digital proveniente de equipos de cómputo con sistema operativo Mac OS X?
- ¿Cómo poder judicializar la evidencia digital de manera adecuada proveniente de equipos de cómputo con sistema operativo Mac OS X?

1.1.4 Objetivo General

Desarrollar una guía metodológica para el análisis forense digital en equipos de cómputo con sistema operativo Mac OS X, tomando como referencia normas, estándares, guías y buenas prácticas internacionales para la judicialización de la evidencia digital proveniente de los mismos en procesos judiciales de Ecuador.

1.1.5 Objetivos Específicos

- Realizar un estudio del funcionamiento, arquitectura y sistema de archivos del sistema operativo Mac OS X, que permita adquirir el conocimiento necesario para identificar las fuentes de evidencia digital.
- Realizar un estudio sobre normas, estándares, guías y buenas prácticas internacionales para el buen manejo de toda la evidencia digital, en el análisis forense.
- Realizar un estudio y evaluación de las metodologías más aceptadas en la actualidad en cuanto se refiere a análisis forense, permitiendo determinar e identificar los procesos y fases a seguir.
- Realizar un estudio de las herramientas comerciales y de open source más adecuadas que ayuden al proceso de búsqueda de evidencia y adecuada interpretación de resultados en el análisis forense.
- Desarrollar una guía metodológica para el análisis forense digital en equipos de cómputo con sistema operativo Mac OS X en el Ecuador, tomando como referencia la normativa legal, las buenas prácticas internacionales, metodología y herramientas seleccionadas.

1.1.6 Justificación

En la actualidad existen escenarios donde se ha comprometido de alguna manera la información de una persona, su equipo de cómputo se convierte en una herramienta que ayudará a los Peritos Informáticos en la búsqueda de vestigios ocurridos en el mismo, sin embargo se evidencia que para equipos de cómputo con sistema operativo Mac OS X en el Ecuador no existe suficiente información; en consecuencia, el conocer y recuperar los datos

perdidos, robados y/o borrados dificulta a los profesionales en la búsqueda de vestigios dejados por el autor del delito.

La creación de una guía metodológica para el análisis forense en un equipo de cómputo con sistema operativo Mac OS X, en la cual se tome como referencia estándares, normas, buenas prácticas y guías propuestas por organizaciones internacionales principalmente especializadas en el área de informática forense, apegada 100% a la actual normativa legal, 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 que en la actualidad se presentan.

Por ello es de vital importancia realizar una investigación en este nuevo campo de la informática forense que es poco explorado, permitiendo de esta manera ampliar el conocimiento y contribuir con el entendimiento de los incidentes.

Es importante mencionar que la investigación a desarrollar es de tipo documental y experimental, debido a que, a través de la observación, consulta de fuentes bibliográficas y la experimentación controlada se recabará datos e información existente para sustentar toda la investigación y la solución a la problemática planteada.

Además, con la realización de este proyecto de investigación se pretende beneficiar a tres ejes importantes:

- A los profesionales que se dediquen al análisis forense en el Ecuador para que tengan un conocimiento técnico y científico que les permita conocer hasta donde pueden llegar con su investigación y de las repercusiones legales que pueden tener para no realizar una mala práctica, y que de esta manera no sea acusado ante una investigación penal.

- A los fiscales y jueces para que de esta manera puedan tener una base científica de los hechos que sucedieron con el delito cometido a través del trabajo realizado por parte de los Peritos Informáticos y que de esta manera no exista una ambigüedad en el momento de dictar la sentencia y no quede en la impunidad.

- A la sociedad para que sea una instancia de justicia en que se pueda judicializar la evidencia obtenida en estos equipos de cómputo. Siendo un aporte más de prueba para poder defenderse.

1.2 MARCO TEÓRICO

Delitos Informáticos en el Ecuador

En el 2012 comenzó a operar la Unidad de Investigación de Cibercrimen de la policía judicial en el Ecuador, la cual mencionó que en el 2013 se contabilizaron 433 denuncias y en los primeros 5 meses de 2014 existían 167 registradas lo que preocupaba a los profesionales en el tema. Este es solo un ejemplo de cómo los delitos en nuestro país han aumentado.

De la misma manera se puede constatar que no todos los incidentes son judicializados como lo menciona el diario La Hora en una publicación de mayo del 2016 "En los primeros cuatro meses del año, la sección contra el Cibercrimen de la Policía Nacional Civil (PNC) recibió 50 denuncias por delitos informáticos, sin embargo, investigadores consultados refieren que este número es solo una referencia porque no todos los ilícitos han sido revelados por parte de los afectados." (Diario la Hora, 2016)

Como se pudo observar los delitos informáticos están en pleno auge y aunque los ecuatorianos creen que por estar en vías de desarrollo no son vulnerables ante este tipo de nueva delincuencia y no se tomen conciencia, las estadísticas seguirán creciendo a medida que pase el tiempo.

Clasificación de los Delitos Informáticos

Debido al auge de las tecnologías de la información y de individuos cada vez más capaces de efectuar el crimen y borrar toda huella de los hechos, en ocasiones, imposible de deducir como se realizó dicho incidente ha generado la necesidad de una regulación jurídica.

En el Ecuador con el Código Orgánico Integral Penal existe la tipificación de algunos delitos informáticos, con penas de entre tres y cinco años, una de las limitaciones para el cumplimiento de la normativa y que se sigan tipificando más delitos en esta temática es la falta de conocimiento que existe no solo a nivel personal sino a nivel empresarial, la falta de denuncias, y en algunos casos la falta de evidencias encontradas al momento de realizar las respectivas pericias.

Muchos autores y de la misma manera organizaciones han clasificado a los delitos informáticos de diferentes maneras, sin embargo, a criterio personal y una vez investigadas algunas clasificaciones se considera que La Organización de las Naciones Unidas (ONU) engloba algunas clasificaciones de forma sintetizada clasificando a los delitos informáticos de la siguiente manera:

Tabla No 1

Clasificación de los delitos informáticos

<table>
<tr><th>DELITOS</th><th colspan="2">CLASIFICACIÓN</th></tr>
<tr><td>Fraudes cometidos mediante manipulación de computadoras</td><td colspan="2">a) Manipulación de los datos de entrada
b) Manipulación de programas
c) Manipulación de datos de salida
d) Fraude efectuado por manipulación informática</td></tr>
<tr><td>Falsificaciones informáticas</td><td colspan="2">a) Utilizando sistemas informáticos como objetos
b) Utilizando sistemas informáticos como instrumentos</td></tr>
<tr><td rowspan="4">Daños o modificaciones de programas o datos computarizados</td><td>Sabotaje informático</td><td>Acceso no autorizado a sistemas o servicios</td></tr>
<tr><td>Virus</td><td>Piratas informáticos o hackers</td></tr>
<tr><td>Gusanos</td><td>Bomba lógica o cronológica</td></tr>
<tr><td colspan="2">Reproducción no autorizada de programas informáticos con protección legal</td></tr>
</table>

Nota. Fuente: Byron Loarte

Ante el complicado panorama que actualmente existe por la lucha contra la falta de tipificación de los diferentes delitos la tabla anterior proporcionará un razonamiento adecuado tanto para jueces y fiscales con el fin de propiciar una reforma en el Código Penal en donde se incluya a todos los delitos informáticos en todas sus modalidades que en años atrás no tenían sentencia o procedimiento a seguir, para que de esta manera todos los incidentes que se presenten se puedan judicializar de una forma adecuada.

Sistema Operativo

En la actualidad una computadora se compone de 2 elementos principales:

- **Software. -** son un conjunto de programas, instrucciones y reglas informáticas para la realización de una tarea o función, siendo esta la parte blanda del computador y que es intangible.

- **Hardware. -** son un conjunto de componentes físicos y tangibles, por ejemplo: discos duros, procesadores, cables, etc., sino también a los periféricos (pendrives, cámaras, impresoras, etc.).

Es así que un Sistema Operativo (SO), es un grupo de programas de proceso que se encarga de explotar los recursos de hardware de uno o más procesadores para poder de esta manera ofrecer un conjunto de servicios a los usuarios del sistema.

En la actualidad existen muchos sistemas operativos, aunque mucha gente piensa que solo existen los famosos sistemas operativos Windows y GNU/Linux.

Según Prieto et al. (2002), muestran una clasificación y ejemplos de sistemas operativos, de los cuales vamos a citar algunos de ellos.

- Multitarea
    - ✓ Windows 95/98/Me
    - ✓ Windows NT/2000
    - ✓ Mac OS
    - ✓ Unix
    - ✓ OS/2
- Monotarea
    - ✓ MS-DOS
    - ✓ CP/M

Sin embargo, existe una parte crucial en un sistema operativo que es el Kernel o núcleo, siendo la capa interna el cual se encarga de agregar nuevas instrucciones especiales a la computadora y facilita a las aplicaciones el acceso seguro al hardware. Puesto que existen diversas aplicaciones y es muy limitado el acceso al hardware, el Kernel también decide, cuáles aplicaciones podrán usar un dispositivo de hardware y el período de tiempo a usarlo.

Normativa Legal en el Ecuador

La creación de las siguientes normativas legales en el Ecuador es para existan fundamentos jurídicos en caso de que cualquier individuo sea víctima de un delito informático, y que de esta manera controlar los delitos que en años atrás no tenían sentencia o procedimiento a seguir.

- **Código Orgánico Integral Penal**

Que fue publicado el lunes 10 de febrero de 2014 Registro Oficial Nº 180 El Código Integral Penal (COIP) "Este Código tiene como finalidad normar el poder punitivo del

Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas." (Ministerio de Justicia, 2014).

- **Ley de Comercio electrónico, firma electrónicas y mensajes de datos**

  Esta ley publicada en el Registro oficial N° 557 del 17 de abril del 2002, estipula "Art. 1.- Objeto de la Ley. - Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas" (Congreso Nacional, 2012)

- **Normativa 040-2014**

  Esta normativa es parte de la Función Judicial denominado Reglamento del Sistema Pericial Integral, el Pleno del Consejo de la Judicatura, aprobó esta resolución el 10 de marzo de 2014.

  El siguiente reglamento ha sido modificado por el Consejo de la Judicatura, el cual resolvió: "EXPEDIR EL REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL" (Consejo de la Judicatura, 2014)

  Este reglamento permite regular la administración y el funcionamiento del Sistema Pericial, tomando como prioridad todos los aspectos que los Peritos deben tener en cuenta al momento de participar en los procesos pre procesal, judicial, o de otra naturaleza que normalmente se ejecuten en la Función Judicial.

Usos del Análisis Forense

Según Gutiérrez et al. (2006) mencionan que "Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense" Como se puede apreciar en la Figura No 2, se evidencia claramente sus principales usos.

Tipos de Análisis Forense

Según Pous et al. (2009), va a depender mucho del punto de vista de lo que se va a analizar, es por eso que entre los cuales se tienen los siguientes tipos de análisis forense, como se puede apreciar en la Figura No 1.

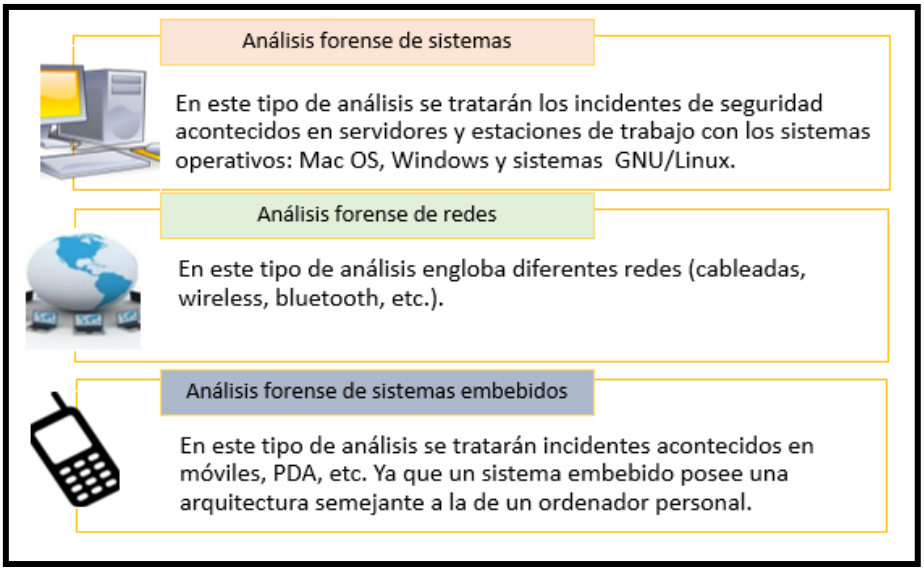


Figura No 1. Tipos de análisis forense

Fuente: Byron Loarte

Normas y Estándares relativos al Análisis Forense

En la actualidad en el ámbito internacional existen diversos organismos, los cuales han desarrollado estándares, normas y guías de mejores prácticas para el manejo de la evidencia digital de cara a la presentación de dichas evidencias en un proceso judicial de un análisis netamente científico.

Metodologías de Análisis Forense

El contar con una metodología clara, confiable y veraz proporcionará a los profesionales en el área los procedimientos, técnicas, actividades y demás estrategias metodológicas requeridas para un adecuado peritaje informático, puesto que ésta será la que avale la investigación desarrollada y la presente como prueba con gran relevancia en un proceso judicial.

Herramientas para el Análisis Forense

Actualmente existen herramientas tanto de software como de hardware convirtiéndose en un estándar prioritario de referencia en el ámbito de la informática forense, los cuales permitirán aportar en la investigación en donde la evidencia fuese digital. Cabe recalcar que las herramientas y los procedimientos que se utilicen deben garantizar en todo momento la integridad de la evidencia, para que de esta manera no pueda ser descartada como medio probatorio en el tribunal.

1.3 ESTADO DEL ARTE

Actualmente existen trabajos relacionados y ponencias sobre análisis forense tanto en dispositivos embebidos y de sistemas que se realizan en otros países. A continuación, se citan los más relevantes acordes al proyecto de investigación.

Existe una ponencia sobre Forense a bajo nivel en Mac OS X, impartida por (Joaquín Moreno, 2014)

De la misma manera existe un artículo propuesto por los autores (Pérez Laguna & Ríos Oruña, MAC OS X: PANTHER, 2003) en el cual dan un enfoque global sobre la arquitectura del sistema operativo Mac OS X, y de cómo ha ido evolucionando cada una de las versiones a lo largo de los años.

Otro ejemplo es lo que propone (Gervilla Rivas, C., 2014) en su trabajo "Metodología para un análisis forense" en donde da a conocer una visión global sobre la metodología de análisis forense para que este sea válido en el mayor espectro posible de situaciones que se pueden dar en este campo.

También es importante mencionar lo que proponen los autores Pous et al.(2009) en su libro "Análisis forense de sistemas informáticos" en el cual dan un enfoque general de los tipos, metodologías, fases y los problemas que existen en un análisis forense.

Mientras que en el ámbito local también existen trabajos relacionados al tema de investigación un ejemplo claro es lo que proponen Sánchez (2016) en su "Análisis forense a sistemas operativos mediante la utilización de herramientas Open Source, caso estudio Windows 8"

El autor Azas Manzano (2015) en su tema de tesis "DISEÑO DE UN MODELO PARA LA CADENA DE CUSTODIA Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE DE EQUIPOS TECNOLÓGICOS EN PROCESOS JUDICIALES EN EL ECUADOR" en el cual menciona los aspectos más importantes que se deben tener en cuenta para la cadena de custodia en equipos tecnológicos, que entran en investigaciones por ser pruebas en casos judiciales.

Por otro lado, el tema propuesto por (Grijalva, J. S. L., & Loarte, B. L.C., 2017) en su "Modelo para el análisis forense y la legalización de evidencia digital atípica en procesos judiciales en Ecuador."

Otro artículo relevante es el propuesto por (Loarte, B. G. C., & Grijalva, J. S. L., 2017) en su "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".

Con esta visión específica de los temas relacionados a la investigación se puede evidenciar que no existen trabajos relacionados sobre un equipo de cómputo con sistema operativo Mac OS X, lo que dificulta que en el país exista documentación y herramientas necesarias para realizar este tipo de análisis forense.

1.4 ADOPCIÓN DE UNA PERSPECTIVA TEÓRICA

El presente proyecto de investigación se fundamentará en ponencias que están enmarcadas principalmente en análisis forenses de Mac OS X a bajo nivel, de la misma manera se tomará como base otros trabajos relacionados ya que cada uno de ellos brinda una perspectiva general sobre el análisis forense y son las bases teórico-prácticas que sustentan la elaboración de la guía metodológica; un ejemplo de lo mencionado es lo que proponen los autores Pous et al. (2009). De igual manera se considerará como base el modelo propuesto por (Loarte, B. G. C., & Grijalva, J. S. L., 2017) ya que es un marco de trabajo adaptado a la normativa legal y está estandarizado para los análisis forenses de la evidencia digital en procesos penales y civiles en el Ecuador.

Además, se tomará como referencia el modelo propuesto por el autor Azas, Marlon (2015) ya que es un modelo que brinda aspectos relevantes en lo que respecta a la cadena de custodia de equipos tecnológicos.

Finalmente, el trabajo experimental que resulte de la investigación propuesta será desarrollar una guía metodológica para el análisis forense digital en equipos de cómputo con sistema operativo Mac OS X, el cual permitirá socializar en el país las ventajas de tener una instancia de justicia más que permitiría judicializar la evidencia obtenida en estos equipos de cómputo. El modelo propuesto será dirigido a organizaciones, profesionales, estudiantes que deseen involucrase en el análisis forense.

1.5 MARCO CONCEPTUAL

El punto de partida para el desarrollo de la investigación propuesta es la sustentación teórica, las mimas que se encuentran tanto en fuentes primarias como en secundarias permitiendo obtener todo el conocimiento adecuado para luego introducir al desarrollo de la guía metodológica para el análisis forense.

Sistema Operativo Mac OS X

OS X es la versión 10 del sistema operativo Apple Macintosh. OS X fue descrito por Apple como su primera "revisión completa" del sistema operativo ya que la versión anterior era la OS 9, y dicha versión tenía un enfoque en la modularidad para que los cambios futuros sean más fáciles de incorporar. OS X incorpora soporte para aplicaciones basadas en UNIX, así como para aquellas escritas solo para Macintosh.

Desde la primera versión de OS X, el sistema operativo ha pasado por una serie de actualizaciones, cada una con un nombre de código felino. (Rouse, M., 2006)

Análisis Forense

Conjunto de principios y técnicas comprendidas en el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial.

Evidencia Digital

Una evidencia digital es "Es la información que se obtiene a través de sistema informático, esta información puede ser: datos, programas almacenados y mensajes transmitidos. Que posteriormente realizado un análisis exhaustivo puedan ser presentadas como evidencias en un proceso judicial" (Loarte, B. G. C., & Lima, J. S. G., 2017)

Perito informático

Es una persona capacitada en el ámbito de la informática para emitir un criterio confiable en base a la investigación y la experiencia que posee. (Consejo de la Judicatura, 2014)

1.6 HIPÓTESIS

Una guía metodológica para el análisis forense en equipos de cómputo con sistema operativo Mac OS X, permitirá que los peritos informáticos tengan conocimientos sobre el funcionamiento de estos equipos de cómputo para el posterior desarrollo de pericias informáticas con el fin de judicializar la evidencia digital.

CAPÍTULO II.

MÉTODO

2.1TIPO DE ESTUDIO

Para la investigación se ha seleccionado el método exploratorio y correlacional como se detalla a continuación:

- **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 desarrollar una guía metodológica para el respectivo análisis forense de un equipo de cómputo con sistema operativo Mac OS X.

- **Correlacional**

  Mediante este tipo de estudio, se medirá la relación que existe entre el nivel de satisfacción que tengan los peritos informáticos y su incidencia en desarrollar una guía metodológica para el respectivo análisis forense de un equipo de cómputo con sistema operativo Mac OS X.

2.2 MODALIDAD DE INVESTIGACIÓN

Para la presente investigación se procede a identificar cual será la modalidad a seguir; para lo cual se considera lo siguiente:

- **De Campo**

  Esta modalidad va a permitir estar más en contacto con el objeto de estudio a fin de recolectar información esencial y relevante que será posteriormente analizada con la finalidad de tener varias conjeturas y tratar de llegar a una conclusión general.

- **Documental**

  Esta modalidad va a permitir obtener información de organismos internacionales y con la ayuda de diferentes fuentes bibliográficas permitirán profundizar y ampliar el conocimiento global de la investigación para el desarrollo de la guía metodológica.

2.3 MÉTODO

- **Método Hipotético-Deductivo**

  Este método se basará en la 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.

2.4 SELECCIÓN DE INSTRUMENTOS DE INVESTIGACIÓN

Los instrumentos que se utilizarán para esta investigación tienen como función esencial obtener información que se convertirá luego en resultados relevantes según (Abril, Víctor Hugo, 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.

  Es importante mencionar que las observaciones deben ser registradas en forma cuidadosa y experta, por tal motivo se realizará una ficha de observación, la cual permitirá obtener todos los datos del objetivo específico en el cual se facilite sistematizar, cuantificar y conservar los resultados de las observaciones

- **Experimentación**

  Ya que la investigación se basa en metodologías existentes se utiliza el estudio experimental debido a que 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.

2.5 VALIDEZ Y CONFIABILIDAD DE LOS INSTRUMENTOS

La validez determina la exactitud con que pueden hacerse mediciones significativas con los instrumentos de investigación seleccionados, para que de esta manera se pueda medir la característica o rasgo a evaluar.

Para la valoración del análisis documental se realizará en base al comité de pares quienes determinarán si la información y los resultados obtenidos presentados podrán ser relevantes para el desarrollo del proyecto de investigación.

De la misma manera para la valoración de la experimentación se realizará en base al juicio experto de un perito informático quien evaluará los resultados obtenidos y determinará si la información presentada podrá ser utilizada como evidencia judicializable, ya que esta deberá contener ciertos requisitos para ser catalogada como tal.

Finalmente, la valoración del documento de tesis será realizada en base a los miembros del tribunal quienes determinarán si los resultados obtenidos del proyecto de investigación son relevantes al problema de investigación planteado.

2.6 PROCESAMIENTO DE DATOS

En este apartado se procederá a realizar la toma de datos obtenidos durante la investigación y procesarlos con la finalidad de generar resultados, los mismos que permitirán evaluar el cumplimiento de objetivos e hipótesis propuestas.

Para lo cual uno de los primeros resultados es la fundamentación teórica que se realizó a cada uno de los síntomas mencionados en el apartado del diagnóstico, de la misma manera otro de los resultados obtenidos es la información que se encuentra en el marco teórico del presente documento de tesis. Finalmente, los resultados obtenidos de 2 publicaciones referentes a metodologías de análisis forense en el Ecuador, mismos que se encuentran en el apartado de la adopción de la perspectiva teórica.

CAPÍTULO III.

RESULTADOS

3.1 LEVANTAMIENTO DE DATOS / INFORMACIÓN

3.1.1 Sistema Operativo Mac OS X

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, consiste en un sistema operativo UNIX, fundamentado en los kernels Mach y BSB.

3.1.2 Arquitectura

Las arquitecturas internas de los sistemas operativos pueden ser 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. Sin embargo, para un mejor entendimiento de esta arquitectura se lo ha separado en capas, como se observa en la Figura No 4, de la cual vamos a describir cada una.

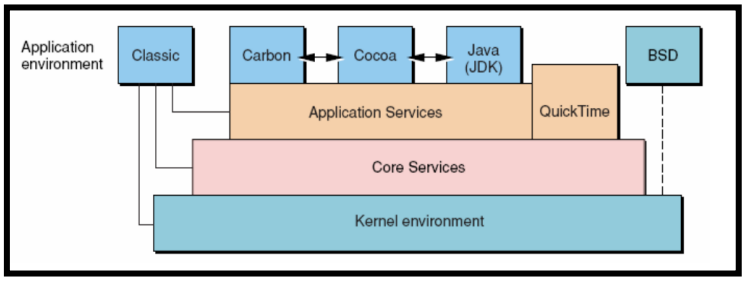


Figura No 2. Arquitectura en capas de MAC OS X

Fuente: (Pérez Laguna & Ríos Oruña, 2003)

3.1.2.1 Application Enviroment

Aquí se presentan cinco diferentes entornos de aplicación (o ejecución) de MAC OS X, estos entornos tienen dependencia con las demás capas inferiores.

Un entorno de aplicación no es más que los "frameworks", librerías y servicios (junto con su API) necesarios para la ejecución de programas desarrollados con esa API.

- **BSD**

  El entorno de comandos BSD, proporciona un shell (interprete de comandos), para poder de esta manera ejecutar programas por líneas de comandos.

  De la misma manera se observa que al estar conectado directamente con la capa de kernel environment, este entorno de kernel exporta servicios BSD, a las capas superiores por medio de las bibliotecas del sistema en /usr/lib.

- **CLASSIC**

  Mediante este entorno, también llamado compatibilidad sin ningún problema se pueden ejecutar aplicaciones de MAC OS 8.x y MAC OS 9.x. Aun así, la ejecución de programas antiguos está sujeta a ciertas limitaciones sin poder aprovechar las ventajas que ofrece el kernel.

- **CARBON**

  Consiste en un conjunto de interfaces de programación (APIs) derivado de los sistemas operativos anteriores, permitiendo de esta manera poder trabajar principalmente con el kernel environment de MAC OS X, y permitir a los desarrolladores enriquecer su código existente para las características de OS X, evitando el costo de re-programar para el entorno Cocoa.

- **COCOA**

  Este entorno permite desplegar aplicaciones escritas en Java y Objective-C, basado en dos frameworks orientados a objetos: Foundation (ofrece un conjunto de objeto y funcionalidades sin ningún impacto sobre la interfaz de usuario) y el Application Kit (básicamente el control y creación de objetos que aparecen en la interfaz del usuario) ambos ofreciendo APIs para las aplicaciones mencionadas anteriormente.

- **JAVA**

  Este último entorno no solo permite desarrollar sino ejecutar programas Java en MAC OS X, incluyendo la Java VM, por este motivo cualquier aplicación creada en Java es totalmente portable gracias a este entorno.

3.1.2.2 Application Services

Esta primera capa contiene principalmente el entorno gráfico y ventanas del MAC OS X, implementadas por Quartz y QuickDraw. Este entorno permite el renderizado de la pantalla, controlar eventos y la administración a bajo nivel de las ventanas y el cursor.

- **Quartz**

  Es un potente sistema grafico permitiendo renderizar 2D en tiempo real con una profundidad y claridad de imagen foto-realista. Permitiendo a los usuarios crear y manipular información en formato PDF usando cualquier aplicación en OS X sin necesidad de algún software adicional.

De la misma manera dentro de esta capa integra lo que es el OpenGl. Esta API proporciona componentes más avanzados para cuestiones de: renderizado 3D, mapeado de texturas, aplicaciones desarrolladas en 2D y 3D, etc.

3.1.2.3 QuickTime

Incorpora funciones de entorno gráfico y aplicaciones las mismas que van a proporcionar un entorno interactivo y multimedia a todos los formatos de imagen, audio, video y sonido disponibles a través de Internet.

3.1.2.4 Core Services

En esta segunda capa residen principalmente los servicios comunes que no forman parte de la interfaz gráfica de usuario (GUI). Se encuentran abstracciones básicas de programación para el manejo de strings, colecciones y run loops. Integra también varias APIs para lo que es el manejo en cuanto a procesos, threads, recursos, memoria e interacción con el sistema de archivos.

3.1.2.5 Kernel Enviroment

Esta última capa es el corazón del MAC OS X, este kernel está basado principalmente en UNIX conocido con el nombre de DARWIN, es una tecnología de Open Source diseñado para proporcionar estabilidad, fiabilidad y rendimiento.

El diseño de Darwin es prácticamente modular proporcionando la facilidad de añadir dinámicamente drivers, extensiones al sistema de red y nuevos sistemas de archivos.

Cabe destacar que el kernel enviroment proporciona funcionalidades a las capas superiores del sistema operativo que son:

- Sistema de memoria virtual avanzado con protección de memoria y asignación dinámica
- Acceso multiusuario
- Drivers de dispositivos
- Networking

Los componentes internos que integra la capa kernel enviroment son los siguientes:

- **MACH**

  Realiza funciones más críticas como son: controla recursos como el porcentaje de uso de la CPU y la memoria, controla el planificador de procesos, protección de memoria para evitar de que una aplicación no pueda escribir en el área de memoria de otra o en el área del sistema operativo, preemptive multitasking asegurará de que toda tarea obtenga los recursos que necesita manteniendo el nivel de actividad al máximo, advanced virtual memory proporcionará entornos de ejecución separado en un mismo sistema y real-time support garantizará un acceso de latencia bajo a los recursos del procesador en aplicaciones de tiempo real.

- **BSD**

  Fundamenta las bases para el sistema de archivos y facilidades de red. Adicional a ello proporciona distintos entornos de programación, modelo de procesos, políticas básicas de protección y seguridad como UserIDs y permisos.

- **XQUARTZ**

  En la actualidad las últimas versiones a partir de MAC OS X v10.5. Creó el proyecto XQuartz, el cual incorporan un nuevo y mejorado sistema de ventanas de su antecesor X11. Usado principalmente para dibujar controles, ventanas y otros elementos de la interface de usuario.

- **DEVICE-DRIVER SUPPORT**

  Para el desarrollo de controladores de dispositivos, Drawin ofrece un framework orientado a objetos llamado I/O Kit. Siendo modular y extensible lo cual facilita la creación de nuevos drivers y de la infraestructura que estos necesitan.

- **NETWORKING EXTENSIONS**

  Darwin permite a los desarrolladores del kernel una nueva funcionalidad para ampliar funcionalidades del sistema de red, permitiendo crear módulos de red, o incluso pilas de protocolos totalmente nuevas, monitorizar y modificar el tráfico de red.

- **FILE SYSTEM**

  El sistema de archivos Darwin está basado en extensiones del BSD y una versión mejorada del virtual file system mediante la cual introduce la posibilidad de asignar protección y permisos a los medios extraíbles, sistema de montaje de volúmenes basado en direcciones URL, nombre de ficheros largos basado en UTF-8, sistema de ficheros "journaling" que permite recuperarse después de un error. El cual se detallará de mejor manera en los siguientes apartados.

3.1.2.6 Umbrella Framework

La finalidad de Umbrella es independizar el desarrollo de aplicaciones del desarrollo del propio sistema operativo, para lo cual empaqueta las capas de Kernel Enviroment, Core Services, Application Services, Carbon y Cocoa.

3.1.3 Sistema de Archivos

Una parte importante en la mayoría de los sistemas operativos son los sistemas de archivos que están principalmente compuestos por particiones, archivos y directorios, y opcionalmente también de archivos de enlace (comúnmente los accesos directos en Windows). Los cuales son usados para almacenar datos de manera segura.

Para un mejor entendimiento plantearemos el siguiente escenario cuando se instala un nuevo sistema operativo en cualquier ordenador, este crea algunas [1]particiones de manera automática. Con lo cual, cada una de las particiones puede usar diferentes sistemas de archivos. Los sistemas de archivos son el formato donde la información es almacenada, y que el computador usa para controlar cómo almacenar e identificar los datos para su respectivo uso.

En conclusión, se puede afirmar que el particionado divide el disco de su totalidad en varios fragmentos y el sistema de archivos respectivamente va identificando cada una de las partes, para que de esta manera el acceso a la información sea mucho más rápido y de fácil acceso. Por tanto, un sistema de archivos es el modo en que el sistema operativo organiza los archivos en el disco duro, gestionándolo de manera que los datos estén de forma estructurada y sin errores.

El sistema de archivos, es la forma en la que la unidad de almacenamiento (disco duro, pendrive, disco duro externo...) ordena el contenido, las particiones y también cómo el sistema operativo va acceder a ella. Teniendo como responsabilidad primordial la recuperación de los datos proporcionando un nombre de archivo y su ruta de acceso, para lo cual lo hace usando tablas o punteros.

FAT, NTFS, EXT, HFS+… tras estas siglas se esconden diferentes formatos con atributos y especificaciones únicas que cada sistema operativo maneja, para nuestro caso nos enfocaremos en el sistema de archivos que usa MAC OS X.

3.1.4 Sistema de Archivos en MAC OS X

En septiembre de 1985, Apple introdujo el sistema de archivos HFS (Sistema de archivos por jerarquía), con lo cual reemplazaría al Macintosh File System (Sistema de Archivos Macintosh o MFS), el sistema de archivos original.

[1] Partición. - Es una unidad lógica de almacenamiento usada principalmente para dividir un disco duro físico en varios fragmentos, como si fuera múltiples discos independientes.

Conforme pasaron los años, más precisamente en el año de 1998 apareció el nuevo sistema de archivos HFS+ (Sistema de archivos por jerarquía extendido) siendo el sistema de archivos primario para los sistemas operativos MAC OS X.

A continuación, se mencionan aspectos importantes sobre el nuevo sistema de archivos:

Representa una optimización más eficiente del espacio del disco duro del antiguo sistema de archivos HFS. Por otra parte, con el nuevo sistema de archivos ya no existen límites para el tamaño de los bloques, lo que no pasaba con HFS que el número de bloques máximo permitido era de 65.536 a 4.290 millones. De la misma manera admite nombres de archivo más descriptivos, con una longitud máxima de 255 caracteres y codificación de texto Unicode, ofrece también un formato opcional de sistema de archivos con distinción entre mayúsculas y minúsculas para HFS+ lo que permite al administrador alojar sin problemas archivos utilizados por aplicaciones UNIX que requieren esta función. Además tienen la posibilidad de almacenar datos extra junto con cada archivo ([2]metadata) de una forma flexible. Otro aspecto importante es la integración del explorador de archivo, permitiendo acceder a cualquier parte del disco duro a través del sistema de archivos comúnmente estructurado de carpetas. Finalmente, el sistema operativo MAC OS X ejecuta una aplicación llamada Finder (búsqueda rápida) localizada en la esquina superior derecha, su función principal es la gestión total de los archivos de usuario, generando un uso más eficiente del sistema de archivos, discos, red y otras aplicaciones.

En la Figura No 5, se observa como es la estructura de un sistema de archivo HFS+. Posterior a ello se procede a describir cada componente en el mismo orden que aparecen en la figura para un mejor entendimiento.

[2] Metadata. - Se refiere a aquellos datos que hablan de los datos, es decir, se caracterizan por ser datos altamente estructurados que describen ciertas características como el contenido, calidad, información y otros atributos.

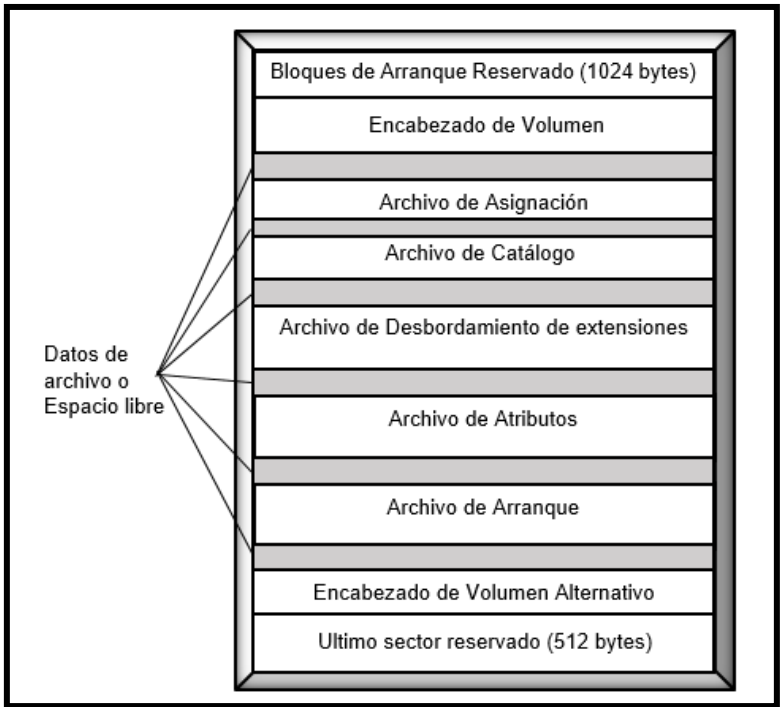


Figura No 3. Estructura de un sistema de archivos HFS+

Fuente: Byron Loarte

Como se puede apreciar en el gráfico, existen ciertas partes que son reservadas en, las cuales contienen meta información sobre el sistema de archivos, y el resto de bloques para la información en sí.

3.1.4.1 Bloques de Arranque Reservado

Los primeros 1024 bytes están reservados para usar como bloques de arranque, principalmente son bloques lógicos que ocupa los sectores 0 y 1, y es una parte fundamental para el arranque del sistema.

3.1.4.2 Encabezado de Volumen

Un aspecto importante a mencionar es que siempre un volumen HFS+ debe tener un encabezado de volumen, y este siempre está en una ubicación fija (1024 bytes desde el inicio del volumen). Contienen información sobre la fecha y hora de creación del volumen, cantidad de archivos en el volumen, así como la ubicación de las otras estructuras clave en el volumen. Pero su función principal es la de almacenar toda la información necesaria para que el sistema operativo pueda manejar y administrar el volumen.

Finalmente, los archivos especiales que están entre el bloque de encabezado de volumen y el bloque de encabezado de volumen alternativo pueden aparecer en cualquier orden y no son necesariamente contiguos.

3.1.4.3 Archivo de Asignación

Este archivo de asignación, es un archivo especial, el cual lleva el control de los bloques que están libres y en asignación. Esta misma función la realiza el mapa de bits del volumen HFS, aunque convertirlo en un archivo agrega flexibilidad al formato de volumen.

De la misma manera HFS+ utiliza un archivo de asignación para poder realizar un seguimiento minucioso sobre cada bloque que ha sido asignación o no en un volumen dentro del sistema de archivos; básicamente el contenido de este archivo especial es un mapa de bits. Dicho mapa de bits contiene un bit que significa que el bloque ha sido asignado en el volumen y está actualmente en uso por alguna estructura del sistema de archivos, caso contrario si el bit no está asignado el bloque de asignación no está actualmente en uso, y está disponible para su respectiva asignación.

Finalmente hay que recalcar que todo el volumen está compuesto por bloques de asignación como lo son el encabezado de volumen, el encabezado de volumen alternativo y las áreas reservadas (los primeros 1024 bytes y los últimos 512 bytes) deben ser marcado como asignado en el archivo de asignación.

3.1.4.4 Archivo de Catálogo

El siguiente archivo especial mantiene algunos metadatos sobre la ubicación y describe la jerarquía de carpetas y archivos en un volumen. Este archivo está organizado como un árbol B-tree (o "árbol equilibrado"), el cual permite búsquedas rápidas y eficientes a través de una gran jerarquía de carpetas; de la misma manera este archivo de catálogo almacena los nombres de archivos y carpetas que constan de hasta 255 caracteres Unicode.

Es importante mencionar que a cada archivo o carpeta del archivo de catálogo se asigna un identificador de nodo de catálogo único (CNID). Para las carpetas, el CNID es el identificador de carpeta, a veces llamado ID de directorio; para los archivos, es el ID de archivo. Para cualquier archivo o carpeta dado, el identificador principal es el CNID de la carpeta que contiene el archivo o carpeta, conocido como la carpeta principal.

Almacena cuatro tipos de registros que son:

- Un registro de carpeta contiene información sobre una única carpeta.
- Un registro de archivo contiene información sobre un único archivo.
- Un registro del nombre de carpeta y el CNID de su directorio padre
- Un registro del nombre de archivo y el CNID de su directorio padre

3.1.4.5 Archivo de Desbordamiento de Extensiones

Este archivo especial alberga información para ubicar el contenido extendido de archivos demasiado fragmentados o el contenido del archivo de bloques dañados. Sin embargo, la estructura del archivo de desbordamiento de extensiones es relativamente simple en comparación con la de un archivo de catálogo debido a que el archivo de desbordamiento de extensiones tiene una clave simple de longitud fija y un solo tipo de registro de datos.

Por ejemplo, para un archivo de un usuario, las primeras ocho extensiones de cada bifurcación se almacenan en el archivo del catálogo del volumen. Cualquier extensión adicional se almacena en el archivo de desbordamiento de extensiones, que también está organizado como un árbol B-tree.

3.1.4.6 Archivo de Atributos

El siguiente archivo especial que contiene datos adicionales (por ejemplo, permisos de lectura y escritura) para un archivo o carpeta, al igual que el archivo de catálogo, el archivo de atributos está organizado como un árbol B-tree. Es importante mencionar que un volumen no tenga ningún archivo de atributos. Si la primera extensión del archivo de atributos (almacenada en el encabezado del volumen) tiene cero bloques de asignación, entonces el archivo de atributos no existe.

3.1.4.7 Archivo de Arranque

Este archivo especial fue creado para facilitar el arranque de ordenadores que no ofrezcan soporte nativo para HFS+.

3.1.4.8 Encabezado de Volumen Alternativo

Finalmente, el penúltimo sector del disco reside una copia del encabezado de volumen, el encabezado de volumen alternativo, se almacena antes del final del volumen.

3.1.5 Versiones

En la actualidad Mac OS X incluye nuevas funciones para proveer una plataforma más estable y viable que sus predecesoras. Como se observa en Tabla No 2 las últimas versiones del MAC OS X junto con el tipo de procesador que operaria.

Tabla No 2

Versiones del sistema operativo MAC OS X

Versión	Nombre	Procesador		Versión	Nombre	Procesador
10.0	Cheetah	PowerPC		10.7	Lion	Intel
10.1	Puma	PowerPC		10.8	Mountain Lion	Intel
10.2	Jaguar	PowerPC		10.9	Mavericks	Intel
10.3	Panther	PowerPC		10.10	Yosemite	Intel
10.4	Tiger	PowerPC		10.11	El Capitan	Intel
10.5	Leopard	PowerPC		10.12	Sierra	Intel
10.6	Snow Leopard	Intel		10.13	High Sierra	Intel

Nota. Fuente: Byron Loarte

3.1.6 Seguridad

Actualmente si bien ningún sistema operativo está exento de ser atacado o infectado por un virus, MAC OS X incluye de fábrica utilidades y herramientas de seguridad como cortafuegos, cifrado de archivos y antispyware, incorporando mayores mecanismos de seguridad que las versiones anteriores.

Existen cada día más virus que afectan a este sistema operativo y el mito de que no existían virus para las plataformas de Apple ya solo es cuento del pasado, según los datos que recaba en Panda Security "se han cuadruplicado desde 2012 hasta hoy. Si hace cuatro años había alrededor de 500 programas maliciosos para estos sistemas operativos, en 2015 ya eran más de 2.200" (Security, s.f.)

Según (López Miguel, 2010) tuvo la oportunidad de hablar mediante una videoconferencia con Eugene Kaspersky, CEO de la compañía que lleva su nombre afirmando que "durante años, los usuarios de OS X han creído que estaban seguros. Pero OS X no es un sistema seguro, ya que es posible que se infecte del mismo modo con el que se infectan los sistemas Windows".

En conclusión, la fama de que existe un bajo número de vulnerabilidades en este sistema no es porque existan menos fallos sino porque es un sistema poco usado en el país y esto genera que se den menos ataques específicamente orientados.

3.1.7 Hardware

Las MACBooks son las computadoras portátiles que Apple ha comercializado en los últimos años y que forman parte de la familia Macintosh. Después, Apple lanzó la MacBook Air y la MacBook Pro, y una serie de actualizaciones de esos modelos, que llevan el mismo nombre.

Se tomó como referencia para la descripción del hardware el modelo MacBook Pro (13 pulgadas, principios del 2011), que será usada para la parte experimental de este proyecto de investigación sus especificaciones técnicas se ilustran en la Tabla No 3.

Tabla No 3

Especificaciones técnicas de la MacBook Pro

Procesador	Core i5 de Intel de doble núcleo a 2,3 GHz
Memoria	4 GB de SDRAM DDR3 a 1.333 MHz (dos módulos de 2 GB)
Disco Duro	Es de tipo Serial ATA de 250 GB a una velocidad de 5.400 rpm
Unidad óptica	SuperDrive a 8x (DVD±R principalmente de doble capa)
Tarjeta Grafica	Es una HD Graphics 3000 de Intel con 384 MB de SDRAM DDR3, que es compartida con la memoria principal

Nota. Fuente: Byron Loarte

A continuación, en la Figura No 6, se observa todos los componentes internos de una Macbook Pro.

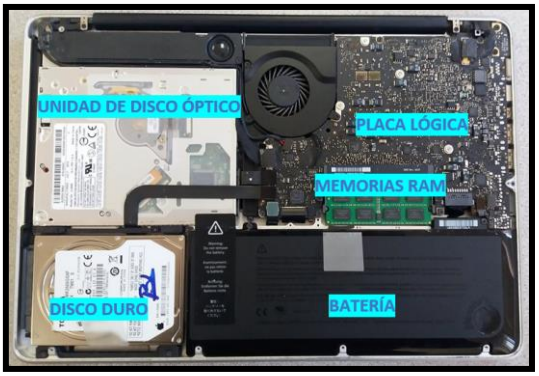


Figura No 4. Componentes internos de una Macbook Pro

Fuente: Byron Loarte

3.1.8 Normas y Estándares Relativos al Análisis Forense

3.1.8.1 Introducción

En la actualidad en el ámbito internacional existen diversos organismos, los cuales han desarrollado estándares, normas y guías de mejores prácticas para el manejo de la evidencia digital de cara a la presentación de dichas evidencias en un proceso judicial de un análisis netamente científico.

A continuación, se presenta algunas de las guías y buenas prácticas que permitirá tomar como referencia para desarrollar 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.

3.1.8.2 RFC 3227

El RFC 3227 es un documento guía para la recolección y almacenamiento de la evidencia digital, publicado en el 2002 por Dominique Brezinski y Tom Killalea, documento que es de libre distribución.

Este documento presenta una serie de pasos de alto nivel a seguir en actividades específicas para una correcta identificación y extracción de la evidencia digital en caso de existir un incidente de seguridad, definiendo este último en el [3]RFC-2888

Es importante mencionar que es una guía que hace hincapié en el orden de volatilidad de los datos en un orden determinado, además que es totalmente flexible y la estructura que presenta esta guía toma temáticas de gran relevancia dentro de una investigación forense.

El esquema que presenta dentro del RFC-3227 es la siguiente:

- **Introducción**
  - ✓ Convenciones utilizadas
- **Guía de principios durante la recolección de la evidencia**
  - ✓ Orden de volatilidad
  - ✓ Cosas que evitar
  - ✓ Consideraciones de privacidad
  - ✓ Consideraciones legales
- **Procedimiento de recolección**

[3] Shirey, R. W. (2007). Internet security glossary, version 2.

- ✓ Transparencia
- ✓ Pasos para la recolección

- **Procedimientos de almacenamiento**
  - ✓ Cambio de custodio
  - ✓ Almacenamiento
- **Herramientas**

3.1.8.3 ISO/IEC 27037

La ISO/IEC 27037 principalmente como la guía para la identificación, recolección, adquisición y preservación de la evidencia digital, teniendo en cuenta que no entra en el proceso de análisis de la evidencia.

Otro punto a favor de esta norma es que es de alcance global proveniente de la normativa de Seguridad Informática ISO 27000, definiendo los dispositivos y las funcionalidades usados en la misma por ejemplo (dispositivos de almacenamiento masivo, smartphone, GPS, ordenadores conectadas en red, sistemas de video vigilancia, etc.)

El objetivo de la citada norma es siempre mantener la integridad de la evidencia y con una metodología aceptable contribuir a su admisibilidad en cualquier proceso legal.

En la Figura No 7. Se observa como la norma se centra en 3 pilares fundamentales que es gobernada la evidencia digital que son:

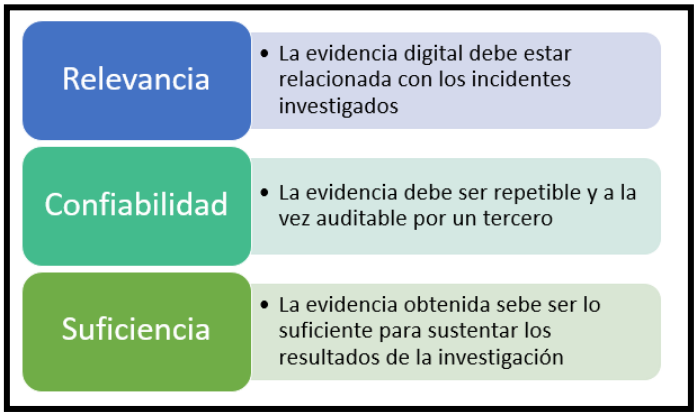


Figura No 5. Pilares fundamentales de la evidencia digital según ISOC/IEC 27037

Fuente: Byron Loarte

3.1.8.4 UNE 71505:2013

Estas normas son publicadas por la [4]AENOR, esta norma tiene por objetivo definir el proceso de análisis forense dentro del ciclo de gestión de las evidencias electrónicas, aplicable a cualquier organización con independencia de su actividad o tamaño.

De la misma manera dentro de esta norma, resalta la confiabilidad, es decir maximizar la veracidad de las evidencias electrónicas, fundamentando el cumplimiento de la siguiente manera:

- **Autenticación e integridad. -** Garantizando que la información no ha sido modificada.
- **Disponibilidad y completitud.** - La evidencia electrónica pueda ser localizada, recuperada, interpretada y presentada completamente.
- **Cumplimiento y gestión.** - La evidencia electrónica se ha obtenido después de haberse gestionado y conforme a lo planificado previamente.

3.1.8.5 Guía de buenas prácticas para evidencias basada en computadores

Esta guía fue desarrollada por la Asociación de Jefes de Policía del reino Unido (ACPO), publicando "Good Practice Guide For Computer-Based Electronic Evidence" (Wilkinson, S., & Haagman, D., 2010)

La policía creó este documento con el objetivo de ser usado por sus miembros como una guía de buenas prácticas, basándose en computadores y otros dispositivos electrónicos que puedan ser usados como evidencia.

El esquema que presenta dentro de esta norma es la siguiente:

1) Los principios de la evidencia basada en computadores.

2) Oficiales atendiendo a la escena.

3) Oficiales investigadores.

4) Personal para la recuperación de evidencia basada en computadores.

5) Testigos de consulta externos.

6) Anexos (legislación relevante)

[4] AENOR: Asociación Española de Normalización y Certificación.

3.1.8.6 Guía para la Aplicación de la Ley (Forensic examination of Digital Evidence: A Guide for Law Enforcement - NIJ)

Una de las guías que presenta el Departamento de Justicia de los estados Unidos (NIJ), en un reporte especial del 04 de Abril titulado "Forensic Examination of Digital Evidence: A Guide for Law Enforcement" (Hart, S. V., Ashcroft, J., & Daniels, D. J., 2004)

Diseñada para los agentes y otros miembros de la comunidad de las fuerzas del orden responsable para el examen de la evidencia digital.

La tecnología avanza a un ritmo tan rápido que las sugerencias de esta guía se examinan de mejor manera en el contexto de la tecnología y las prácticas actuales. De la misma forma es una guía que pueda ser utilizada en la ayuda del desarrollo de sus propias políticas y procedimientos para el análisis de la evidencia digital.

El esquema que presenta dentro de esta guía es la siguiente:

- Desarrollo de políticas y procedimientos.
- Valoración de la evidencia.
- Adquisición de la evidencia.
- Análisis de la evidencia.
- Documentación y reportes.

3.1.9 Metodologías para el Análisis Forense

En la actualidad el contar con una metodología clara, confiable y veraz proporcionará a los profesionales en el área los procedimientos, técnicas, actividades y demás estrategias metodológicas requeridas para un adecuado peritaje informático, puesto que ésta será la que avale la investigación desarrollada y la presente como prueba con gran relevancia en un proceso judicial.

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."

3.1.9.1 Forensic Control

La empresa [5]Forensic Control propone un modelo dirigido a un público no técnico, aplicado a cualquier dispositivo capaz de almacenar y/o transmitir información digital. Es importante mencionar que este modelo no se centra en ninguna legislación particular ni tiene por objeto impulsar un producto o empresa en particular.

Dividido en seis fases cronológicas las cuales se pueden observar en la Figura No 8.

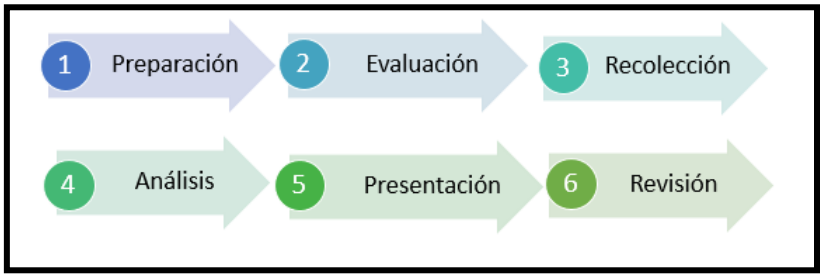


Figura No 6. Fases según Forensic Control

Fuente: Byron Loarte

3.1.9.2 UNE 71506:2013

La norma UNE 71506:2013 ha sido elaborada con el principal objetivo de definir el proceso de análisis forense dentro del ciclo de gestión de las evidencias electrónicas, publicada en julio 23 del 2013, complementa todos aquellos procesos que conforman la gestión de las evidencias electrónicas, según se describe en la UNE 71505.

Dividido en cinco fases cronológicas las cuales se pueden observar en la Figura No 9.

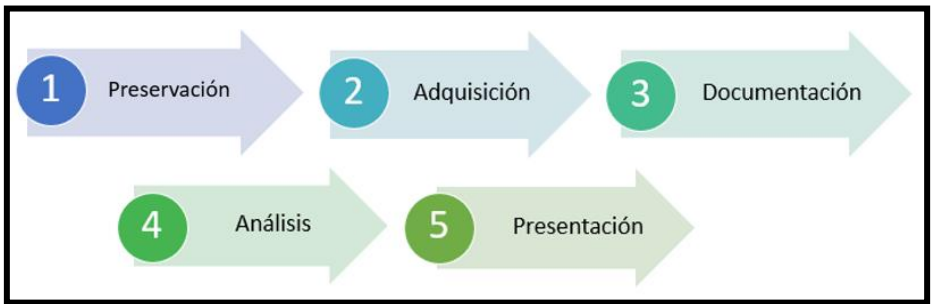


Figura No 7. Fases según la norma UNE 71506:2013

Fuente: Byron Loarte

[5] Forensic Control. - Es una empresa de gestión de riesgos y amenazas internas con oficinas en el centro de Londres. https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

3.1.9.3 Francisco Lázaro Domínguez

Según este autor en el libro "Introducción a la Informática Forense" el cual fue publicado en el año 2013 divide la investigación forense en cuatro fases como se puede observar en la Figura No 10, siendo una de estas la línea de tiempo la cual ayuda a comprender la evolución de los hechos.

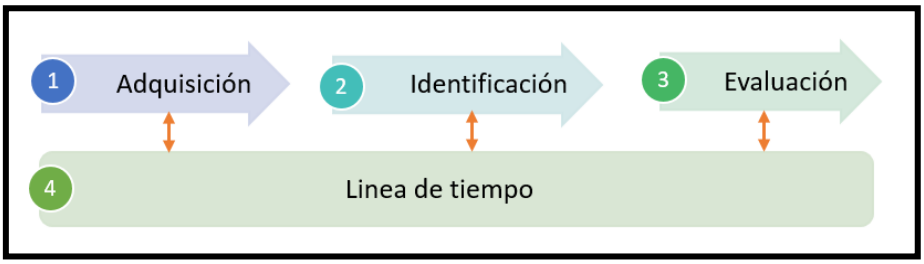


Figura No 8. Fases según la norma UNE 71506:2013

Fuente: Byron Loarte

3.1.9.4 Fase de investigación de la escena digital del crimen, del modelo IDIP (2003)

En este modelo propuesto por (Carrier, B., & Spafford, E. H., 2003), es mejorado de su antecesor IDIP, el cual introduce el concepto de escena digital, creado por el entorno virtual tanto en hardware y software conteniendo evidencias digitales.

Es importante mencionar que cuando termina la fase de la escena del crimen digital, los resultados obtenidos proporcionan una retroalimentación para la subfase posterior que es la reconstrucción de la escena física del crimen.

Dividido en cinco fases cronológicas y en algunas abarcando subfases, las cuales se pueden observar en la Figura No 11.

- **Fase de preparación**
  - ✓ Preparación de la operación
  - ✓ Preparación de la infraestructura
- **Fase de despliegue**
  - ✓ Detección y notificación
  - ✓ Conformación y autorización
- **Fase de investigación de la escena física del crimen**
  - ✓ Preservación
  - ✓ Sondeo
  - ✓ Documentación

- ✓ Búsqueda y recolección
- ✓ Reconstrucción
- ✓ Presentación

- **Fase de investigación de la escena digital del crimen**
  - ✓ Mismas súbase que la fase anterior
- **Fase de revisión**

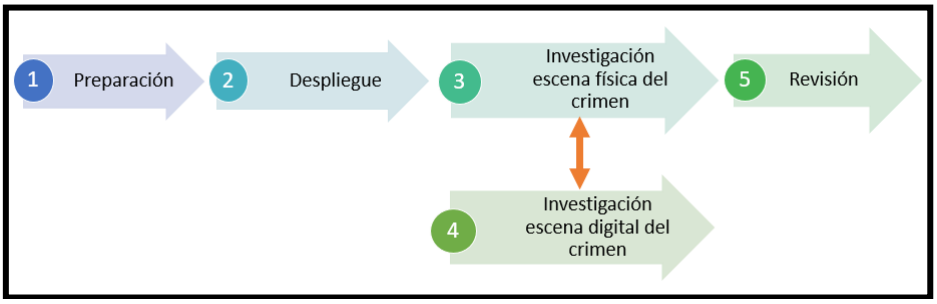


Figura No 9. Fases según modelo IDIP (2003)

Fuente: Byron Loarte

3.1.9.5 NIST

El Instituto de Instituto Nacional de Estándares y Tecnología (NIST), en su publicación de agosto del 2006 "Special Publication 800-86" propone un modelo de 4 fases para el proceso forense. Este modelo puede ser adaptado según a las necesidades y en función a las políticas a seguir.

Dividido en cuatro fases cronológicas, las cuales se pueden observar en la Figura No 12.

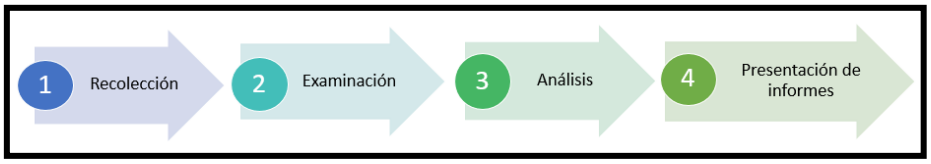


Figura No 10. Fases según el NIST

Fuente: Byron Loarte

3.1.9.6 DFRWS

Este modelo se presenta en el informe técnico "A Road Map for Digital Forensic Research" el cual propone un modelo de investigación de propósito general con 6 fases, las cuales se pueden observar en la Figura No 13.

El Digital Forensic Research Workshop (DFRWS), se dedica a compartir el conocimiento y las ideas sobre la investigación forense digital. Sin embargo, continúa reuniendo académicos y profesionales en un ambiente informal desde que organizó el primer taller abierto dedicado al forense digital en el 2001.

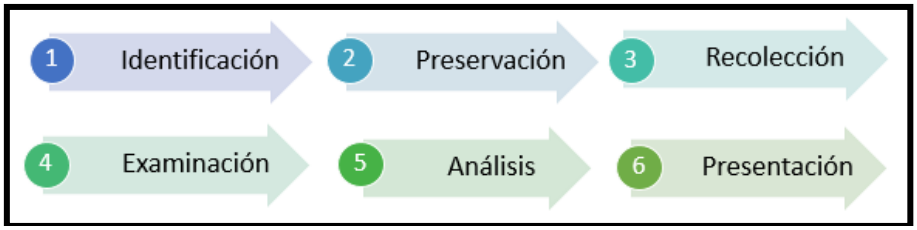


Figura No 11. Fases según DFRWS

Fuente: Byron Loarte

3.1.9.7 CASEY

Este modelo de Casey, es uno de los modelos menos abstracto y más extendido, el cual ha ido evolucionando desde su primera aparición en el 2002 hasta el modelo publicado en el 2004 en la segunda edición de su libro.

Dividido en cinco fases cronológicas y en algunas abarcando subfases, las cuales se pueden observar en la Figura No 14.

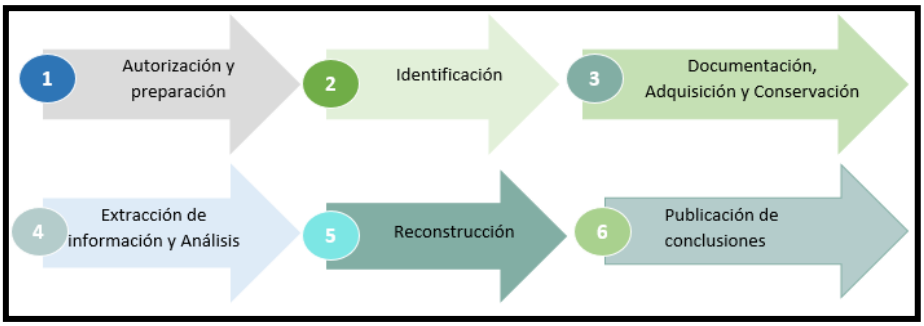


Figura No 12. Fases según Casey

Fuente: Byron Loarte

3.1.9.8 Evaluación de las Metodologías

Una vez realizado un análisis de cada una de las metodologías para el análisis forense propuesta por varios organismos y autores.

Se pudo observar que existen varios modelos que en gran parte de ellos reflejan los mismos principios básicos, pero lo que realmente diferencia uno de otro es las fases que poseen. Ya que algunos modelos tienden a ser demasiado detallados otros en cambio son muy generales, sin embargo, se debería seleccionar el modelo que más se ajuste a las necesidades requeridas.

Dicho esto, se evaluará cada una de los modelos citados tomando en cuenta varios aspectos como se presenta en la Tabla No 4, que son:

- Disponibilidad de documentación
- Adaptabilidad a normas y estándares relativos al análisis forense
- Adaptabilidad en la implementación experimental
- Fases claramente detalladas

Para lo cual el criterio de evaluación es entre 1 y 5

Tabla No 4

Evaluación de metodologías

Numero	Metodología	Fases	Ítems de evaluación				Resultados
			a	b	c	d	
01	Forensic Control	1. Preparación 2. Evaluación 3. Recolección 4. Análisis 5. Presentación 6. Revisión	3	3	3	4	13
02	UNE 71506:2013	1. Preservación 2. Adquisición 3. Documentación 4. Análisis 5. Presentación	4	5	5	5	19
03	Francisco Lázaro Domínguez	1. Adquisición 2. Identificación 3. Evaluación 4. Línea de tiempo	3	4	4	3	14

04	Fase de investigación de la escena digital del crimen, del modelo IDIP (2003)	1. Preparación 2. Despliegue 3. Investigación escena física del crimen 4. Investigación escena digital del crimen 5. Revisión	4	3	5	4	16
05	NIST	1. Recolección 2. Examinación 3. Análisis 4. Presentación de informes	4	5	4	4	17
06	DFRWS	1. Identificación 2. Preservación 3. Recolección 4. Examinación 5. Análisis 6. Presentación	3	4	4	5	16
07	CASEY	1. Autorización y preparación 2. Identificación 3. Documentación, Adquisición y Conservación 4. Extracción de Información y Análisis 5. Reconstrucción 6. Publicación de conclusiones	3	4	5	5	17

Nota. Fuente: Byron Loarte

3.1.9.9 Selección de la metodología UNE 71506:2013

Una vez realizado la evaluación respectiva se determinó que la metodología UNE 71506:2013 es la más adecuada para la realización de este proyecto de investigación. No obstante, será complementada con la actual normativa legal que existe en el Ecuador.

A continuación, se comenzará a profundizar a detalle sobre aspectos importantes y relevantes que tiene esta metodología seleccionada.

Es aplicable a cualquier tipo de organización con independencia de su actividad o tamaño, así como a cualquier profesional competente en este ámbito, enfocando también al personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas.

Cuenta con una estructura que es de la siguiente manera:

- Primeramente, proporciona una serie de términos, definiciones y abreviaturas serán de utilidad dentro de este documento, junto con los proporcionados en la norma UNE 71505-1.

- A continuación, se detalla claramente las principales fases de un análisis forense que son: Preservación, Adquisición, Documentación, Análisis y Presentación.

- Finalmente presenta una serie de anexos, el primero consiste en un modelo de informe pericial propuesto por la norma UNE 197001, el segundo trata acerca de las competencias que debe contar el personal, separadas en varias categorías: competencias técnicas, profesionales y personales, y el tercer anexo trata sobre el equipamiento para el análisis forense, las herramientas tanto de hardware como de software reconocidas por la comunidad forense internacional.

3.1.10 Herramientas para el Análisis Forense

En este capítulo se comienza a profundizar a detalle 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 Correa Delgado emitió el 10 abril 2008 en el cual adopta el Software Libre como política de estado, en el cual el Artículo 1 del presente Decreto Ejecutivo 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 así garantizar la admisibilidad en los tribunales y no se pueda vulnerar a una impugnación de descalificación.

Otro aspecto a tener en cuenta para las herramientas seleccionadas es seguir las recomendaciones del fabricante para su correcto uso o máximo aprovechamiento.

3.1.10.1 Selección de la Herramientas

En la actualidad no es necesario enfocarse en herramientas con licencias ya que existen herramientas libres en el mercado que cumplen con el objetivo de un análisis forense y a continuación se listan aquellas que nos permitirán cumplir con el proyecto de investigación.

De la misma manera 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 las investigaciones forenses.

Tabla No 5

Evaluación de metodologías

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 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	Libre

	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 descubrimientos y los	Libre

	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

Nota. Fuente: Byron Loarte

3.1.11 Desarrollo de la Guía Metodológica para el Análisis Forense

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

Esta guía metodológica utiliza como base para su desarrollo las guías y buenas prácticas “FRC-3227” y “Examinación Forense de la Evidencia Digital (NIJ)” 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 concluyó implementar el modelo a continuación presentando, propuesto por la UNE 71506:2013, porque es bastante completa para la administración de evidencias digitales, sin dejar de lado que será perfeccionado 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. 15, para englobar todos los aspectos a considerar en un análisis forense relacionado principalmente en el proceso de adquisición y análisis de la evidencia digital. 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 completamente la admisibilidad en los tribunales y no se pueda vulnerar a una impugnación de descalificación.

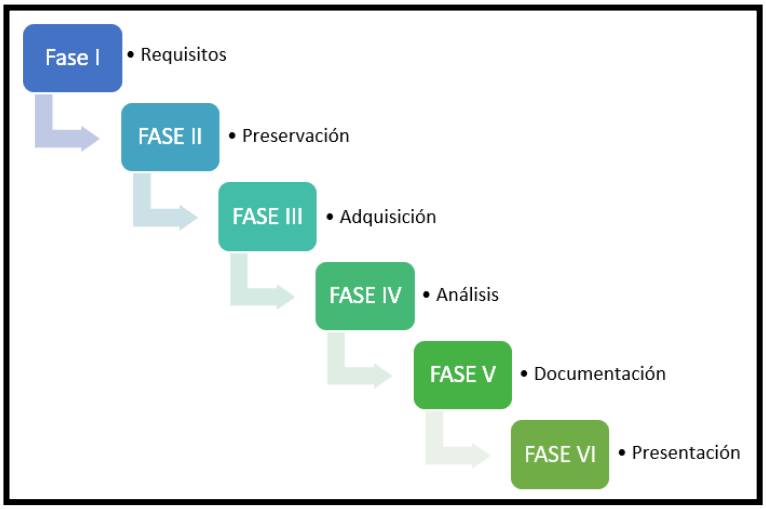


Figura No 13. Metodología propuesta

Fuente: Byron Loarte

3.1.11.1 Fase I

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.

Es primordial que tenga en cuenta cuales son los principales requisitos para poder calificarse como Perito Informático. El cual está plenamente reglamentado en el Artículo 18 de la Resolución 040-2014 (Consejo de la Judicatura, 2014), permitiendo regular de esta manera ciertos aspectos (calificación, evaluación y obligaciones) al momento de que participen en procesos judiciales, pre procesales o de cualquier otra índole que se lleven a cabo en la Función Judicial.

El Perito Informático que es acreditado deberá conocer cuáles son las fases de un proceso pericial y cuál es su ámbito de acción (Consejo de la Judicatura, 2016).

De la misma manera estos Peritos deberán tener el perfil que el artículo 511 del [6]COIP proporciona, para poder realizar una investigación forense.

La autoridad competente es la encargada de ordenar la designación de un Perito calificado con conocimiento y determinada experticia, en un proceso para la investigación de un delito informático determinado, sin olvidar especificar la necesidad de la experticia, considerando principalmente:

Siendo un proceso civil, se debe seguir el procedimiento que se indica en la Fig. 16.

Figura No 14. Fases de un procedimiento pericial para procesos civiles

Fuente: Byron Loarte

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)

[6] Código Orgánico Integral Penal (http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf)

Sin embargo, si es un proceso penal, en cambio se debe seguir otro tipo de procedimiento como se ilustra la Fig. 17.

Figura No 15. Fases de un procedimiento pericial para proceso penal

Fuente: Byron Loarte

Teniendo en cuenta que si es un proceso penal 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**

El Artículo 12 de la Resolución 040-2014 establece que la elección de Peritos ya sea para procesos de tipo penal o civil, será realizado respectivamente por un juez a través del sistema [7]SATJE. Respetando en todo momento aquellos principios de transparencia, profesionalidad, alternabilidad e igualdad.

No obstante, para procesos que no sean de tipo penales las partes procesales pueden fácilmente gestionar de forma directa la designación de un Perito, siempre y cuando tengan acceso al objeto de la pericia y teniendo en cuenta que los Peritos seleccionados de esta forma tienen que estar previamente calificados, y deberán cumplir con todas las obligaciones y deberes. 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.

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 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.

[7] SATJE. – Es un Sistema de catálogo de Peritos acreditados por el Consejo de la Judicatura, ubicándolos en un catálogo de Especialidades.

- **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, los resultados del peritaje deberán ser sustentador oralmente por el Perito, siendo una de sus obligaciones tanto en procesos Civiles como Penales, respondiendo al contrainterrogatorio y al interrogatorio de los sujetos procesales.

La defensa oral tiene por objetivo la aclaración, ampliación o ratificación de una pericia realizada. Ya que sin esta defensa oral las respectivas conclusiones del examen pericial, carecerán de valor como lo establece el Artículo 222 del COGEP (Código Orgánico General de Procesos, 2015).

De la misma manera es importante recalcar que si un Perito no va a defender su informe puede perder fácilmente su acreditación en ocasiones pudiendo ser llevado a la audiencia por medio del 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.

Aquí se listan toda la documentación que el Perito Informático va a requerir:

- Solicitud por escrito a una autoridad competente, porque en ciertos casos será necesario romper claves de seguridad e investigar sobre archivos concretamente personales en equipos informáticos o incluso para quebrantar los acuerdos de confidencialidad que tienen las empresas.
- **Formulario N° 1,** 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.
- **Formulario N° 2,** el cual contendrá información acerca de la escena del delito.
- **Formulario N° 3,** el cual contendrá información referente a la recopilación de la evidencia original de los diferentes dispositivos de almacenamientos.
- **Formulario N° 4,** 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.

Antes de comenzar con la Fase de Preservación el Perito Informático deberá llenar adecuadamente el **Formulario N° 1.**

3.1.11.2 Fase II

En esta fase se da prioridad en asegurar la integridad de la evidencia original tomada en la escena del delito, dicho de otro modo, no se debe modificar, alterar o destruir 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 de hardware y software 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 se menciona en el Artículo 178 del COIP.

Por lo tanto, se elaboró sub-fases enmarcadas concretamente en la escena del delito como se muestra en la Fig. 18.

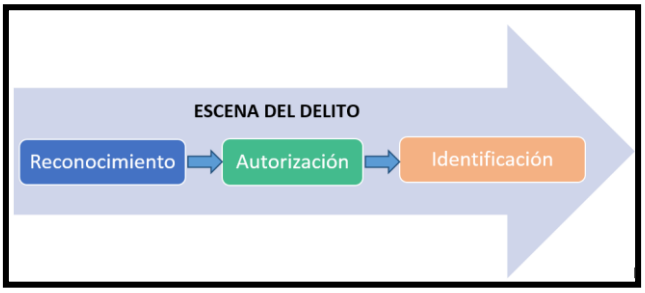


Figura No 16. Sub-fases de la Fase de II (Preservación)

Fuente: Byron Loarte

- **Sub-fase de reconocimiento**

Los Peritos pueden realizar sin problema actividades de reconocimiento del lugar de los hechos en territorio digital, medios o equipos tecnológicos teniendo en cuenta la preservación de la escena del delito, a fin de evitar la alteración y destrucción de la evidencia digital. Como lo establece el Artículo 460 del COIP.

- **Sub-fase de autorización**

Antes de empezar su experticia y hallar información relacionada expresamente con el incidente, el Perito deberá solicitar la respectiva autorización por escrito de parte de la autoridad competente, o las partes procesales, dado que en determinados casos se deberá romper claves de seguridad e investigar en archivos personales o incluso para quebrantar los acuerdos de confidencialidad que tienen las empresas.

Sin la autorización mencionada, el análisis no tendría validez legal y se estaría cometiendo un grave delito, según lo mencionado en el Artículo 178 del COIP, sobre la violación a la intimidad. El Artículo 292 del COIP, establece una pena privativa de libertad de uno a tres años, por alteración y destrucción de evidencias u otros elementos que sean catalogados como prueba.

- **Sub-fase de identificación**

En esta fase se realizará la identificación y el tipo de evidencia, determinando principalmente el tipo de información disponible y que forma parte esencial 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.

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, 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

Lo primordial es verificar el estado en el que se encuentra el equipo, si este está encendido o apagado, porque los procedimientos de recopilación de información tendrán un tratamiento

diferente para salvaguardar la integridad de la evidencia original. Por lo general, 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

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 acordonada y aislada, todas las actividades deben ser claramente documentadas. Se debe realizar una investigación eficaz en la búsqueda de materia, elementos de prueba o también 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

Es necesario realizar actividades que contribuyan con la descripción a detalle del lugar de los hechos y la focalizada localización de materia, los elementos de prueba o evidencias, usando técnicas establecidas siendo videos, fotografías, embalaje, imágenes y rotulado, entre otros. Todo lo antes mencionado, puede ser aplicado; como se establece en el Artículo 500, inciso cuatro del COIP.

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

9) Componentes relacionados al incidente

Los peritos informáticos verificarán la identificación, sobre 2 tipos de evidencia:

- **Evidencia electrónica. –** Generalmente, concurrirá todos los elementos materiales de hardware o de un sistema informático, en el caso de hardware, refiriéndose a todos los componentes físicos que lo componen.

- **Evidencia digital. -** Es toda la información conseguida en un sistema informático, como por ejemplo programas almacenados, datos y mensajes que hayan sido transmitidos, para posteriormente analizarlos y se puedan presentar como evidencias.

Es completamente crucial realizar este análisis, porque influirá en los procedimientos que se realicen a futuro de manera adecuada para cada tipo de evidencia, con el fin de encaminar lo más correcto posible 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 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 **Formulario N° 2**, el cual contendrá información sobre la escena del delito.

3.1.11.3 Fase III

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 porque 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 tomará en consideración algunas recomendaciones según (Rivas, C. G., 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, M. F., 2015).

Por lo indicado anteriormente, se elaboraron sub-fases englobadas principalmente en la evidencia original, como se muestra en la Fig. 19.

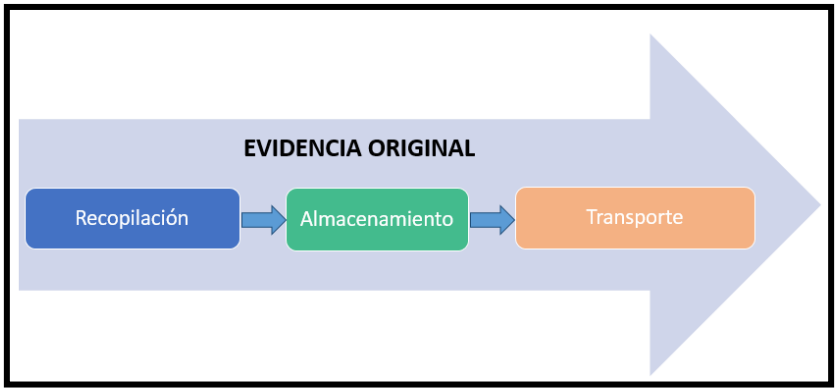


Figura No 17. Sub-fases de la Fase III (Adquisición)

Fuente: Byron Loarte

- **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 en el que se encentra el equipo, si este está encendido o apagado, porque los procedimientos de recopilación obviamente serán distintos para conservar la integridad de la evidencia original.

Es sumamente importante establecer el escenario del equipo ya que en esta sub-fase se deben aplicar técnicas y/o métodos para la correcta recopilación de la evidencia original, priorizando el orden de la 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 encender el equipo, siempre debe estar apagado, porque si se lo enciende se altera la evidencia, considerando que el atacante haya modificado el proceso de inicio/apagado con algún Script (es un código que se ejecuta cuando se enciende o apaga la maquina).

- No trabajar directamente con la evidencia original del soporte de almacenamiento de datos, se debe trabajar con una copia a bajo nivel usualmente llamado imagen forense. Para efectuar la copia, se debe usar medios forenses estériles, para ello se debe

emplear herramientas ya sea de hardware o software, que asegure perfectamente, que la evidencia no sea contaminada.

- Cuando se efectúa una imagen 100% completa del soporte de almacenamiento de datos, esta incluye las particiones totales, el sector de arranque, los espacios de disco duro sin usar, entre otros, etc., toda la información recopilada será útil para el análisis del contenido de estos y otras tareas de investigación; detallando lo citado 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 previamente obtenida, es necesario proceder a calcular el [8]Hash (huella digital única para un conjunto de datos que están debidamente cifrados), primeramente, del soporte de datos donde se encuentra la evidencia original, posterior a ello de la respectiva imagen forense extraída. Es importante indicar que los dos Hashes obligatoriamente deben ser iguales.

- Es fundamental el acompañamiento de otra persona en el proceso de recopilación, aparte del perito Informático; para que actué como testigo en las acciones realizadas, siendo preferente 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.

- Es importante que toda la información quede documentada sobre el soporte de datos original, si en el caso de que este soporte se encuentre alojado en un equipo informático, en cambio se debe documentar los respectivos números de serie. Es recomendable por si acaso acompañar con una fotografía de los procedimientos realizados anteriormente.

- Si se realizaron de manera adecuada los procedimientos mencionados, se garantizará completamente la integridad de la evidencia y no podrá ser eliminada como medio probatorio. Respetando el Artículo 500, inciso tres del COIP.

[8] Hash. – Básicamente son algoritmos de cifrado que por medio de algoritmos matemáticos sobre el conjunto de datos de cualquier longitud, genera un número hexadecimal de 32 dígitos

2) Equipo está encendido

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

- No se deberá apagar el equipo, porque se podría perder información sensible como por ejemplo: memoria RAM, usuarios conectados remotamente y localmente, procesos en ejecución, etc., resultando muy difícil volver a recopilar toda esta información, al decidir apagar el equipo.

- Es importante mencionar que la recopilación de la evidencia se ejecute en el orden de mayor a menor volatilidad de la información. Este orden descrito, enmarca el período de tiempo donde parte de la información es accesible, por esta razón se debe ejecutar la recopilación de la información en un tiempo menor, en otras palabras, cuya volatilidad sea mayor.

- El orden de la volatilidad, de acuerdo a lo establecido en el RFC 3227, es de lo más volátil a lo menos volátil siendo esto:

  - ✓ Contenidos de la caché y registros.
  - ✓ Contenido en la memoria RAM.
  - ✓ Estado de las diferentes conexiones de red, las tablas de ruteo.
  - ✓ Estado de los procesos encontrados en ejecución.
  - ✓ Contenido de los discos duros y del sistema de archivos.
  - ✓ Contenido de terceros dispositivos de almacenamiento.

  Como prioridad se tomará los 4 primeros puntos, porque si por algún error que puede ser involuntario se reinicia o apaga el equipo, podría perder toda la información o modificarse.

- Documentar toda la información recopilada del sistema en tiempo real, como:

  - ✓ La respectiva hora y fecha actual del sistema.
  - ✓ Procesos que pueden estar activos.
  - ✓ Todas las respectivas conexiones de red que pueden tener.
  - ✓ Todos y cada uno de los puertos TCP/UDP que pueden estar abiertos.
  - ✓ Todos y cada uno de los respectivos usuarios que pueden estar conectados de forma remota y también localmente.
  - ✓ Directorios abiertos.

- ✓ Archivos abiertos.

- En ocasiones puede ser que el atacante dejé instalando scripts o herramientas que pueden modificar, suplir y eliminar archivos; no obstante, en el peor de los escenarios el atacante puede seguir on-line detectando nuestra presencia y así trate de evadir las acciones o, aún peor, trate de eliminar todo tipo de información.

  En este caso, siendo que la información sea gravemente comprometida por la severidad del ataque, el equipo deberá ser apagado sin ninguna duda. Se perderá la información más volátil, pero principalmente se conservará información que será útil sobre el ataque.

- Posterior a ello, se debe inmediatamente recopilar toda la información volátil del sistema; para ello, se puede emplear un script para uso de sistemas UNIX/Linux o un archivo de proceso por lotes para uso exclusivo de sistemas Windows para que ejecute el proceso de copiado en forma automatizada. También sería de gran ayuda utilizar herramientas de que transmitan datos por la red, exportando la información a una portátil conectada en 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 seguidamente a calcular el Hash de la información previamente extraída.

- Realizados los procedimientos anteriormente mencionados de forma correcta, se garantizará completamente que la recolección de la evidencia se generó de manera transparente e completa respetando el Artículo 500, inciso uno y dos del COIP.

El perito informático documentará a detalle los procedimientos realizados anteriormente y toda la información obtenida registrando en el **Formulario N° 3**.

- **Sub-fase de almacenamiento**

Una vez culminado de recopilar toda la información requerida para la investigación y almacenándola cuidadosamente, es primordial definir métodos apropiados para el etiquetado y almacenamiento de las evidencias. Este proceso es usualmente llamado "cadena de custodia".

El Perito Informático debe aplicar la pertinente cadena de custodia a contenido digital materia de prueba o elementos físicos, garantizando la legitimidad, estado original y acreditando su identidad, como lo indica el Artículo 456 del COIP.

No obstante, 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 indica el Artículo 457 del COIP.

Para la elaboración de estos métodos, se tomará como referencia la guía para el almacenamiento y manejo de la evidencia digital como se describe: el RFC 3227, Modelo Extendido de Séamus Ó Ciardhuain. No obstante, se debe tener claro que la cadena de custodia, inicia en el sitio donde se obtiene o halla el elemento de prueba.

Para iniciar con el proceso de cadena de custodia, es importante contar con la presencia de la autoridad competente. Es importante mencionar que este proceso puede ser aplicado, como se indica en el Artículo 482, inciso uno y tres del COIP.

La cadena de custodia, debe efectuarse como se indica a continuación:

1) **Fijación del lugar de los hechos**
   Realizar actividades, las cuales permitan una descripción detallada del lugar donde sucedieron los hechos y la localización de evidencias o los elementos materia de prueba, usando técnicas previamente establecidas que pueden ser videos, fotografías, planos, entre otros. Se podrá aplicar cadena de custodia, de acuerdo a lo que establece el Artículo 500, inciso cuatro del COIP.

2) **Recolección de la evidencia**
   Una vez analizado el estado en el que se encuentra el equipo y aplicando las herramientas tanto de hardware como software, se conseguirá la imagen forense de acuerdo a 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 puede aplicar cadena de custodia; como lo indica el Artículo 500, inciso dos y tres del COIP.

3) **Embalaje y rotulado de la evidencia**
   Se debe registrar fotográficamente los equipos y las distintas conexiones antes de su embalaje, mientras dure el embalaje y al finalizar el embalaje y conjuntamente el rotulado.

   Revisar los dispositivos de almacenamiento removibles. (Algunos de los equipos en su interior contienen dispositivos de almacenamiento removibles, como por ejemplo tarjetas SD, [9]Memory Stick, etc.).

   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 hacer con una cinta previamente que se identificada como adecuada, que ofrezca seguridad y la correcta preservación del mismo.

[9] Memory Stick. - Familia de memorias flash que son fácilmente removibles, lanzadas por Sony.

Para el manejo de los soportes de almacenamiento de los datos y de la respectiva imagen forense obtenida, se deberán introducir en una bolsa antiestática y posteriormente colocar en una caja de cartón o sobre manila, en cuyo interior se consiga rellenar de plásticos con burbujas u otros materiales protectores. Sin embargo, si se desea más información se puede considerar algunas otras recomendaciones en la ISO 17799:2005 en el apartado 10.7.

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

Se debe rotular de manera consecutiva, a cada uno de los elementos a serán 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 **Formulario N° 4**, que garanticen 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 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 recopilada, así como los elementos que hayan sido incautados deben ser transportadas al respectivo laboratorio forense, el cual quedara registrado en el **Formulario N° 4**, 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 menciona el Artículo 500, inciso cuatro del COIP.

Durante el transporte, la cadena de custodia se debe mantener meticulosamente; tomando las precauciones que sean necesarias para minimizar la posibilidad de causar contaminación accidental a la evidencia. Si se realizó y documentó correctamente todos los procedimientos anteriormente mencionados, se garantiza la integridad; preservación e inalterabilidad de la evidencia. Como menciona el Artículo 457, del COIP.

3.1.11.4 Fase IV

Esta fase es transcendental y de vital importancia, porque por medio de la evidencia digital obtenida y si hubiera equipos incautados, el perito informático mediante un examen detallado aplicará procedimientos, herramientas y técnicas poniendo todos los conocimientos adquiridos en la búsqueda de vestigios de lo requerido a encontrar para llegar a responder una serie de interrogantes de dónde, cómo, quién y cuándo 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 (Rivas, C. G., 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 exclusivamente se lo debe efectuar 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 únicamente por el perito informático, para su análisis o estudio.

   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 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.**
   Efectuar la reconstrucción de la línea de tiempo, esto quiere decir, establecer la evolución de los hechos, desde el instante anterior al inicio del ataque detectado, hasta el momento de ser descubierto.

   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.

5) **Realizar su experticia únicamente en lo que ha sido designado**
Pueden ser severos los castigos, cuando el Perito Informático no efectúa una adecuada investigación forense. Puesto que en el momento de la audiencia se pueden escuchar una seria de argumentos como por ejemplo: ¿quién le dio autoridad para espiar la información personal de mi cliente? Con el fin de anular los Informes Periciales, dando paso a que se inicie nuevamente el proceso de indagación e incluso con una pena privativa de libertad como le establece el Artículo 178 del COIP, que trata sobre la violación a la intimidad. Y el Artículo 511, inciso 8 del COIP, 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.

3.1.11.5 Fase V

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 se menciona en el Artículo 511, inciso cinco y seis del COIP. De la misma manera y de forma obligatoria el informe debe ser presentado y cargado al Sistema Informático Pericial, en formato PDF; el mismo que posterior pueda ser descargado y estudiado por las partes y los interesados. Las respectivas aclaraciones o explicaciones, deberán ser presentadas de forma verbal y en algunos casos de forma escrita, conforme con la normativa procesal correspondiente, como se indica en el Artículo 19 y 20 de la Resolución 040- 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 la presentación, como lo instaura el Artículo 19 y 20 de la Resolución 040- 2014, siendo muy 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 que son obligatorios de todo informe pericial; son los siguientes:

1) **Datos generales del juicio, o proceso de indagación previa**
   En este punto deben contener la identificación del perito y los datos del juicio como principal requisito, que tiene por objeto determinar la responsabilidad en el caso de incumplimiento de obligaciones.

2) **Parte de antecedentes**
   Claramente se debe delimitar el encargo realizado, esto refiere a que se tiene que especificar el tema sobre el que informará, basado 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**
   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, en lo posible no debe ser extenso y en lo posible del caso ser redactado con un lenguaje muy compresible para un público no técnico, exponiendo cada una de las razones por las cuales se ha determinado 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.

3.1.11.6 Fase VI

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.

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.

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 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. 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.
- Realizar preguntas y presentar pruebas no notificadas oportunamente orientadas a determinar su parcialidad y no idoneidad, a desvirtuar el rigor técnico de cada una de sus conclusiones, así como también impugnar su credibilidad, como lo establece el Artículo 511, inciso seis y siete del COIP.
- El Perito podrá estar en la capacidad de responder a cada una de las preguntas del interrogatorio de las partes, valiéndose con ilustraciones gráficas, como lo indica el Artículo 511, inciso seis y siete del COIP.
- De existir informes periciales divergentes, el juez tendrán la potestad de establecer en ese momento un debate entre los peritos, para posterior a ello iniciar un interrogatorio y contrainterrogatorio, con el objetivo de aclarar aquellos puntos de controversia, como lo indica el Artículo 222 del COGEP.

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.

3.2 PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

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 señala que la pena privativa de libertad contra personas que publiciten, transmita, 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.

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, se detalla el procedimiento realizado, adjuntando imágenes y documentos utilizados en el caso expuesto como se ilustra en la Fig. 20.

Figura No 18. Herramientas utilizadas para la investigación forense

Fuente: Byron Loarte

El Perito Informático utilizando los guantes de nitrilo procede con suma cautela a la destrucción de los sellos de seguridad del Equipo Tecnológico con el fin de no contaminar la evidencia original como se ilustra en la Fig. 21.

Figura No 19. Destrucción de sellos en el Equipo Tecnológico

Fuente: Byron Loarte

El Perito Informático procede con la verificación el estado del Equipo Tecnológico y de cada uno de los puertos de entrada del mismo como se ilustra en la Fig. 22.

Figura No 20. Verificar el estado del Equipo Tecnológico

Fuente: Byron Loarte

Siguiendo con el procedimiento el Perito Informático procede con suma cautela a la obtención del disco duro del Equipo Tecnológico únicamente herramientas adecuadas, posterior a ello procede a almacenar el disco duro en una bolsa antiestática para su protección como se ilustra en la Fig. 23.

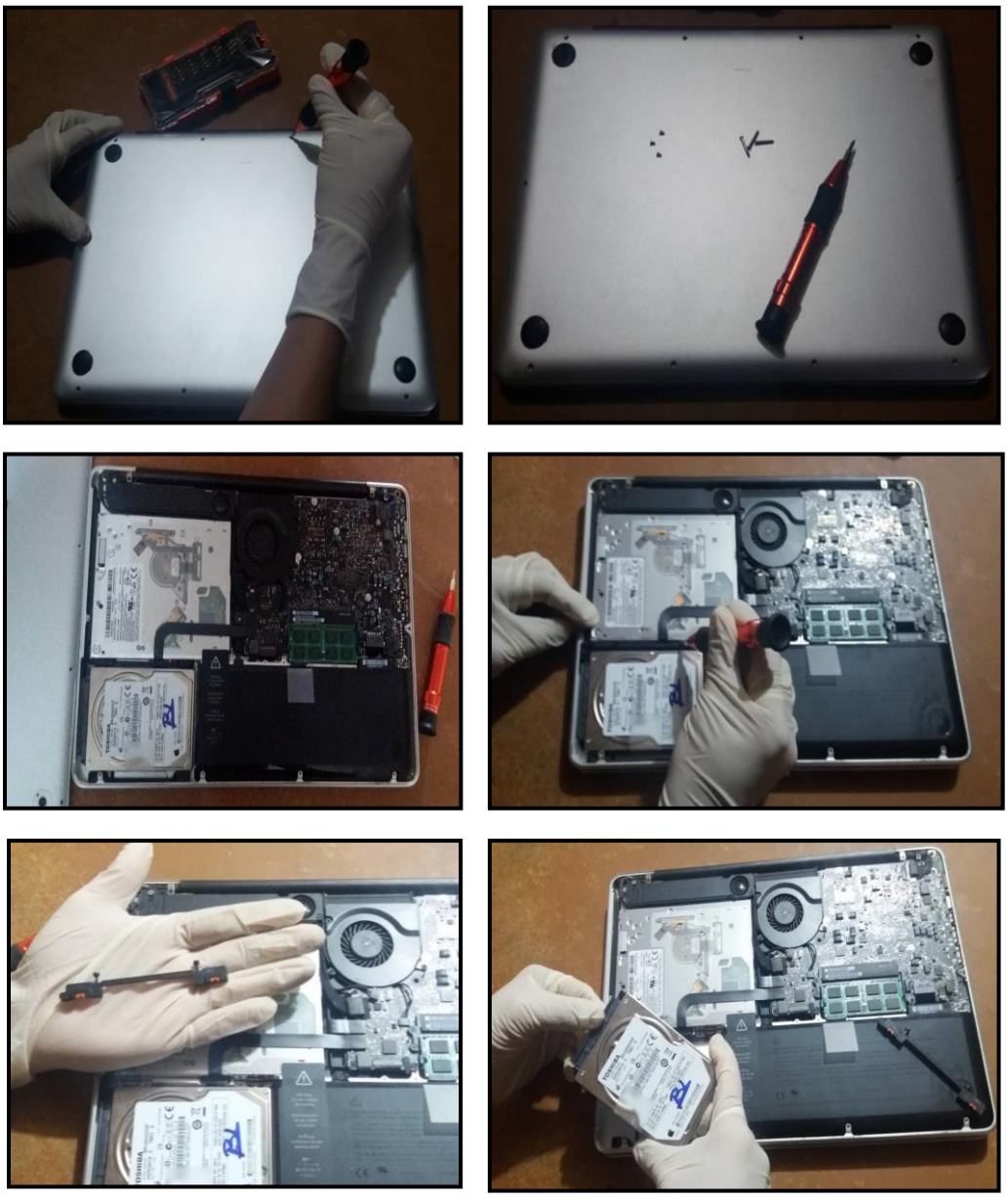


Figura No 21. Obtención del disco duro del Equipo Tecnológico

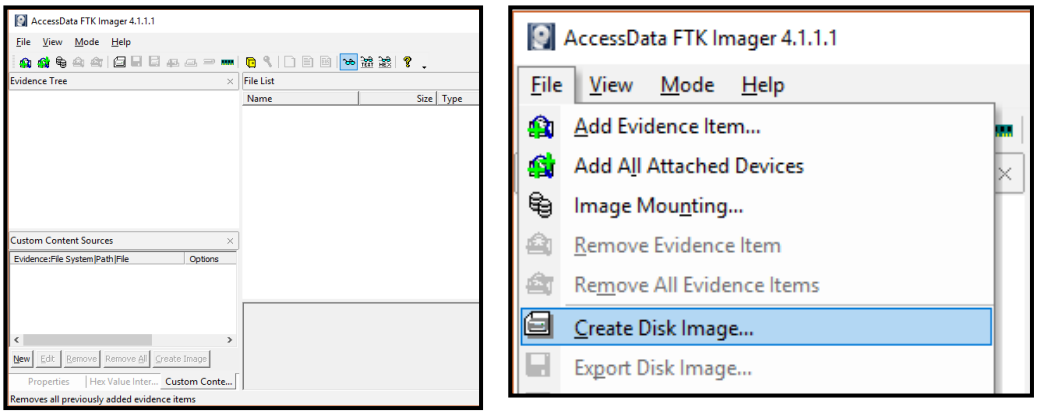
Fuente: Byron Loarte

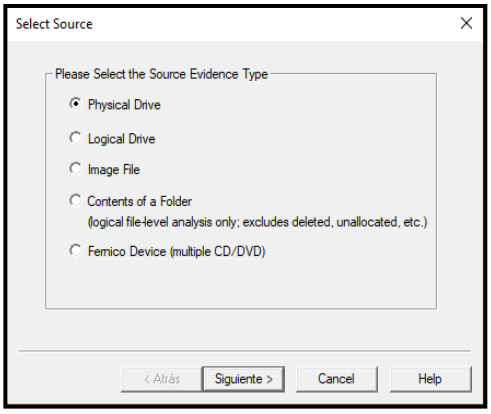
En la Fig. 24, se observa como el Perito Informático procede con suma cautela a preparar el ambiente para la creación de la imagen forense del disco duro obtenido.

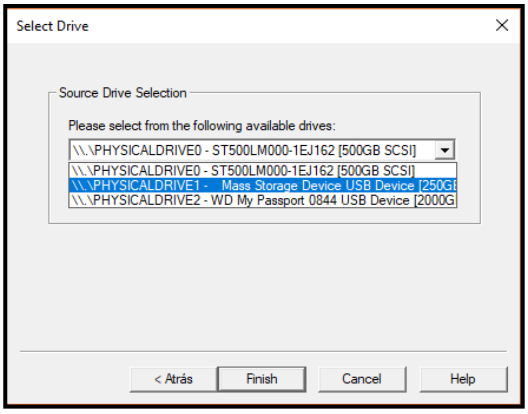
Figura No 22. Preparación para la creación de la imagen forense del disco duro

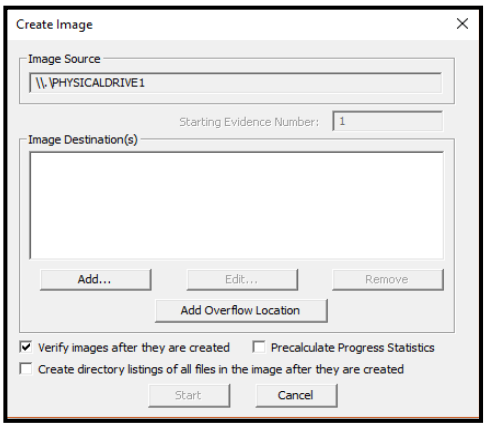
Fuente: Byron Loarte

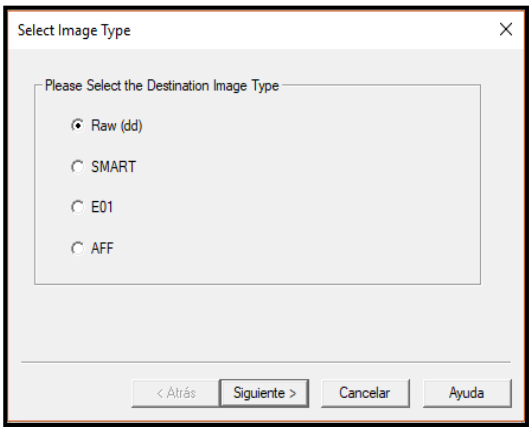
A continuación, el Perito Informático procede a la creación de la imagen forense con la herramienta FTK Imager 4.1.1.1 cómo se ilustra en la Fig. 25.

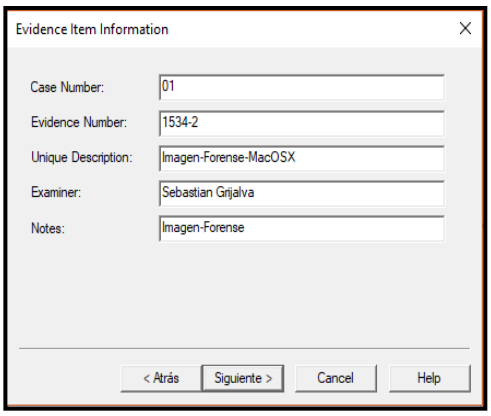


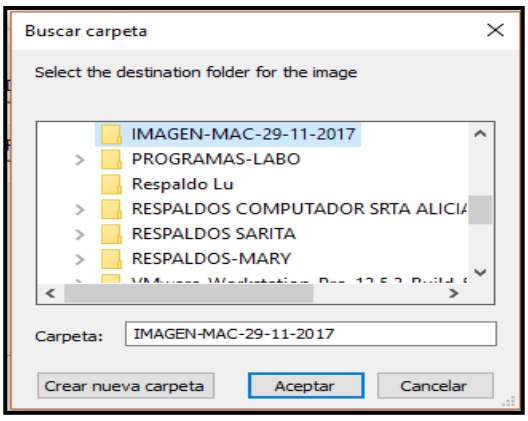

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Fernico Device (multiple CD/DVD)
< Atrás
Siguiente >
Cancel
Help


Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE0 - ST500LM000-1EJ162 [500GB SCSI]
\\.\PHYSICALDRIVE0 - ST500LM000-1EJ162 [500GB SCSI]
\\.\PHYSICALDRIVE1 - Mass Storage Device USB Device [250GB
\\.\PHYSICALDRIVE2 - WD My Passport 0844 USB Device [2000G
< Atrás
Finish
Cancel
Help


Create Image
Image Source
\\.\PHYSICALDRIVE1
Starting Evidence Number:
1
Image Destination(s)
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel


Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Atrás
Siguiente >
Cancelar
Ayuda


Evidence Item Information
Case Number:
01
Evidence Number:
1534-2
Unique Description:
Imagen-Forense-MacOSX
Examiner:
Sebastian Grijalva
Notes:
Imagen-Forense
< Atrás
Siguiente >
Cancel
Help


Buscar carpeta
Select the destination folder for the image
IMAGEN-MAC-29-11-2017
PROGRAMAS-LABO
Respaldo Lu
RESPALDOS COMPUTADOR SRTA ALICIA
RESPALDOS SARITA
RESPALDOS-MARY
Carpeta:
IMAGEN-MAC-29-11-2017
Crear nueva carpeta
Aceptar
Cancelar

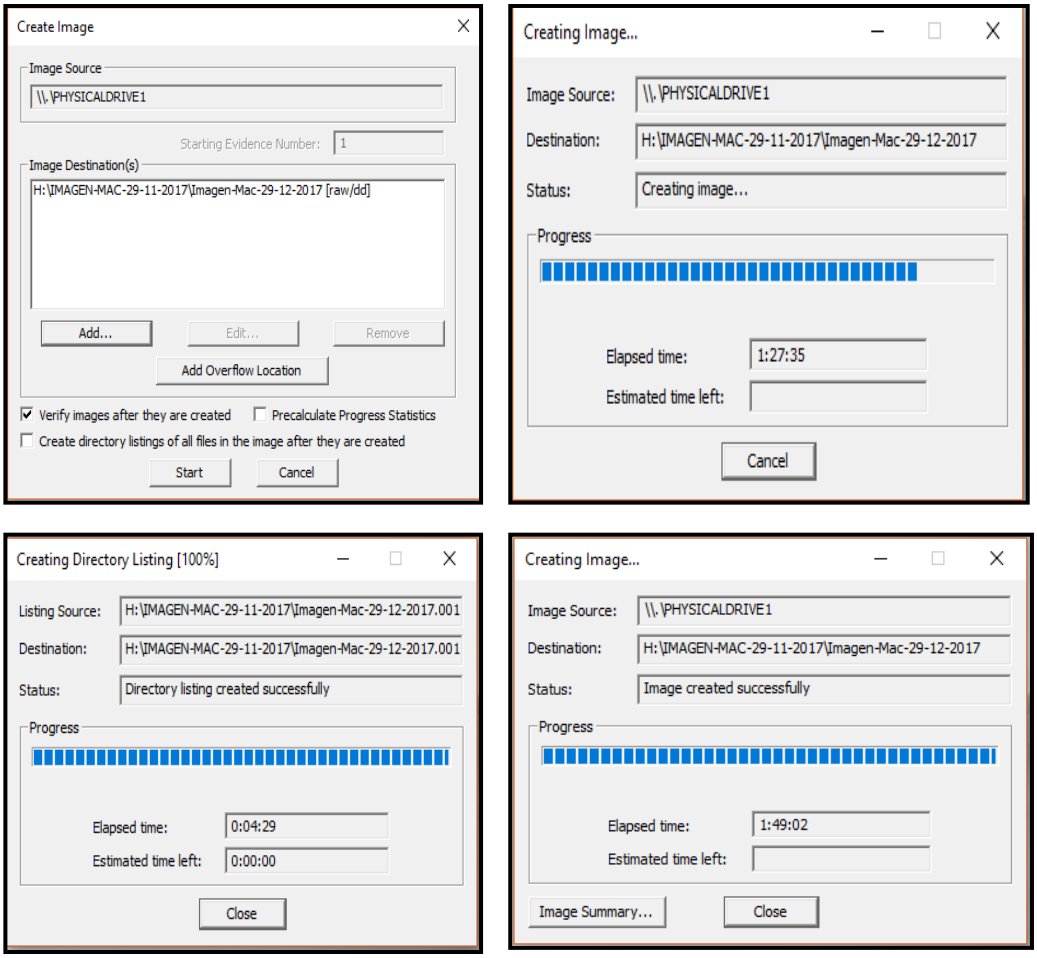
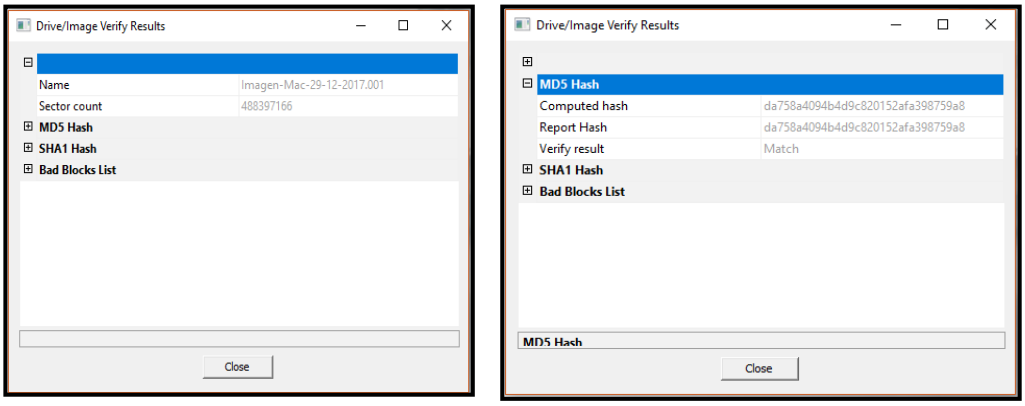


Figura No 23. Creación de la imagen forense del disco duro
Fuente: Byron Loarte

En la Fig. 26, 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.



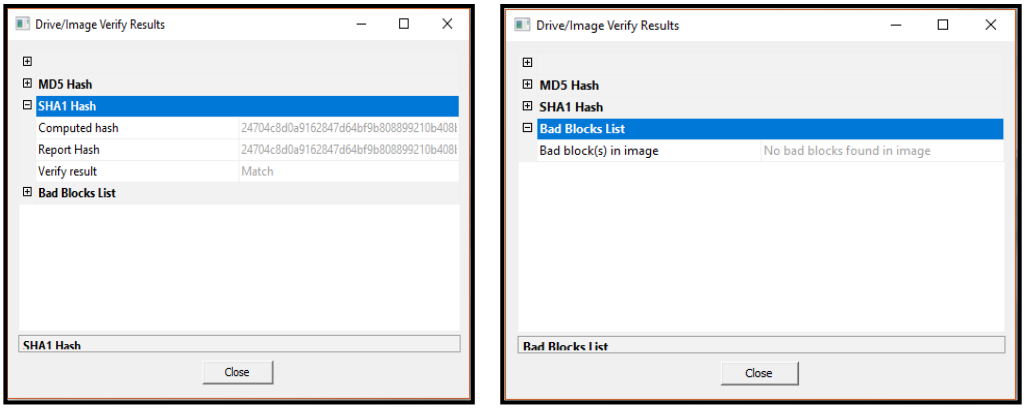
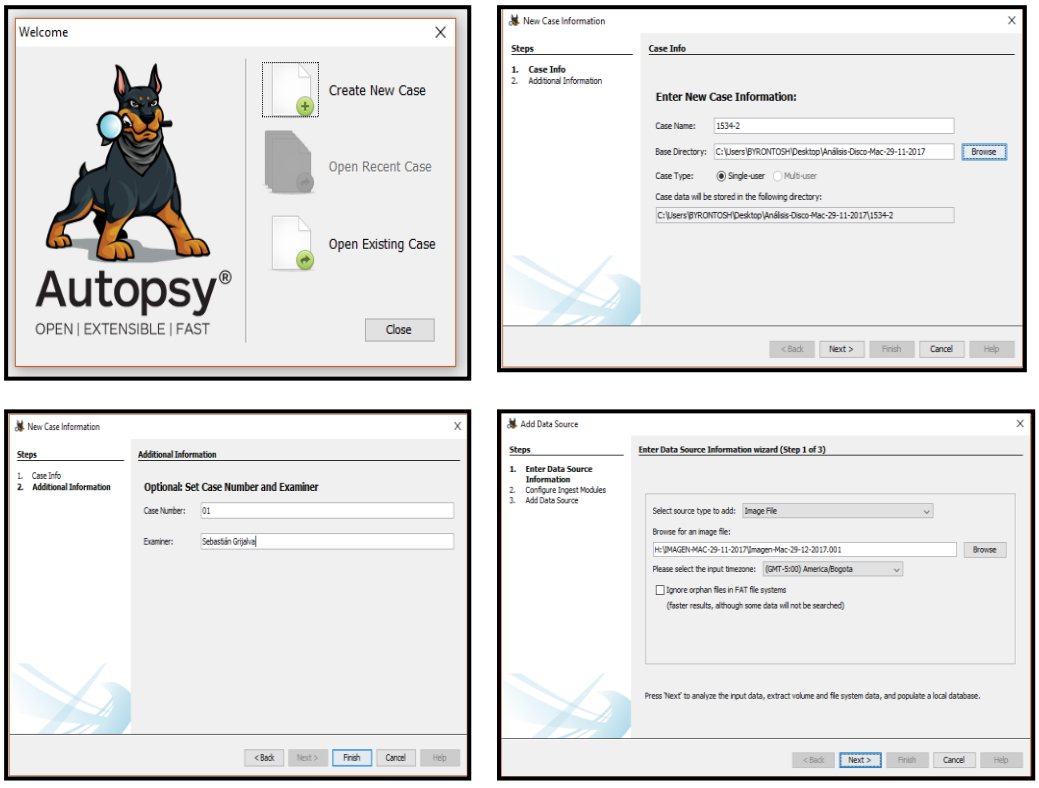


Figura No 24. Comprobación de la imagen forense creada
Fuente: Byron Loarte

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. 27.



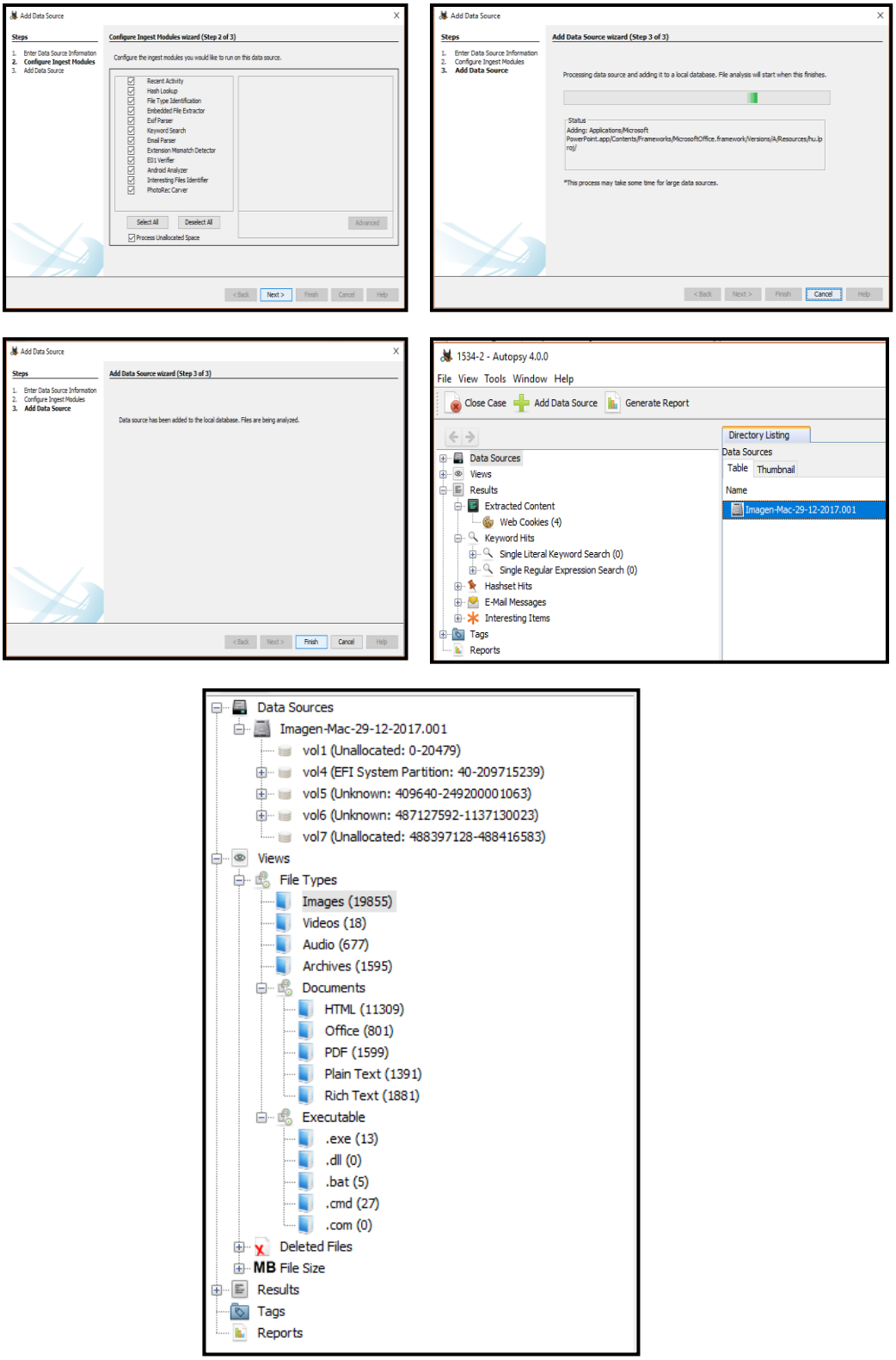
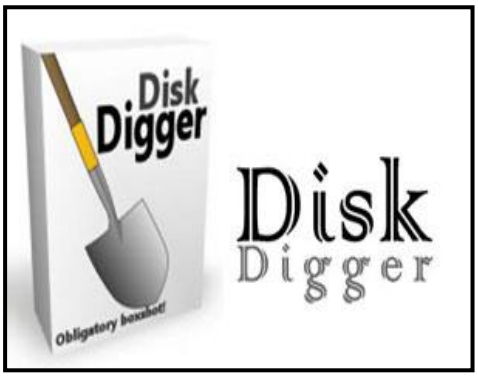
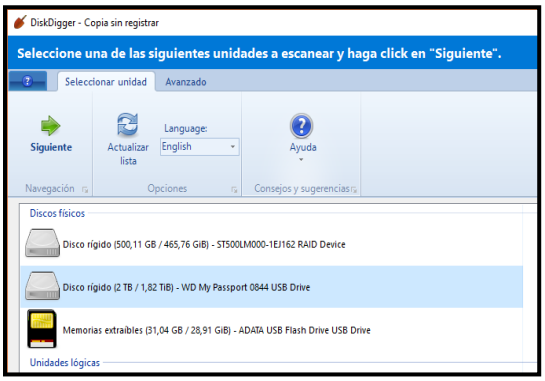


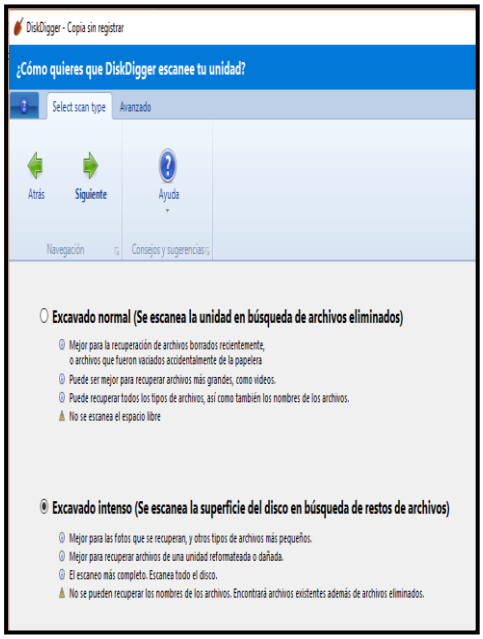
Figura No 25. Análisis de la imagen forense creada

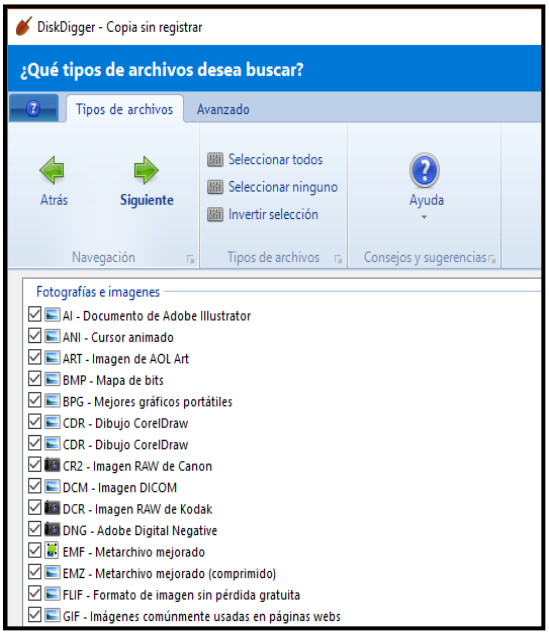
Fuente: Byron Loarte

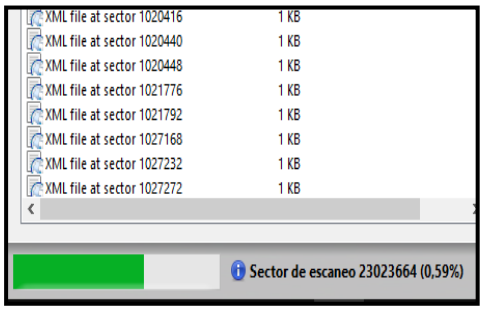
De la misma manera el Perito Informático realiza otro análisis con la herramienta DiskDigger 1.17 para poder encontrar más fuentes de evidencia, como se ilustra en la Fig. 28.

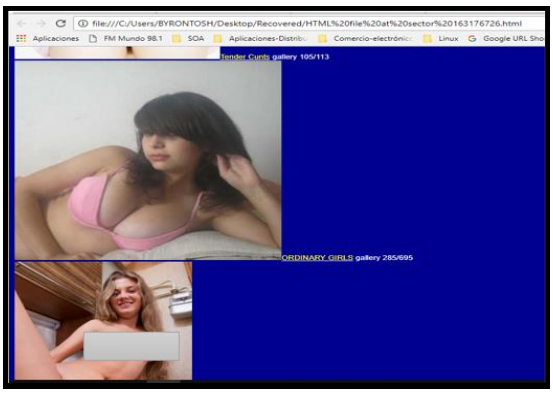


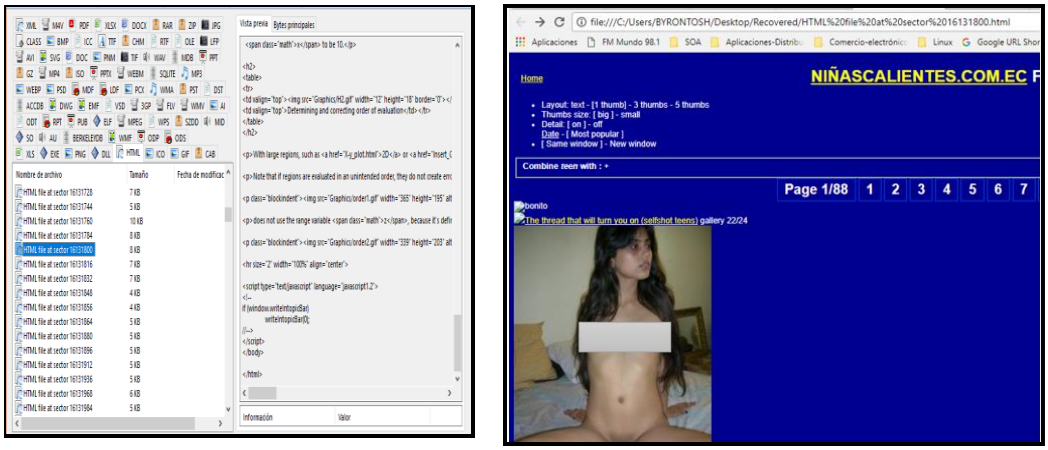












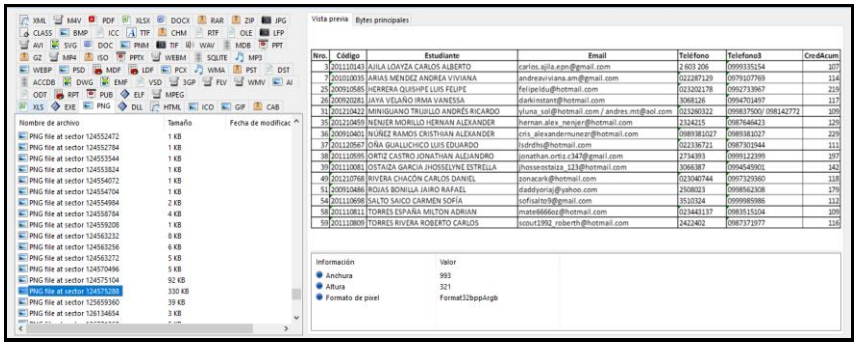


Figura No 26. Análisis de la imagen forense creada

Fuente: Byron Loarte

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. 17. Con lo cual el Perito Informático evidencia que existen imágenes sobre:

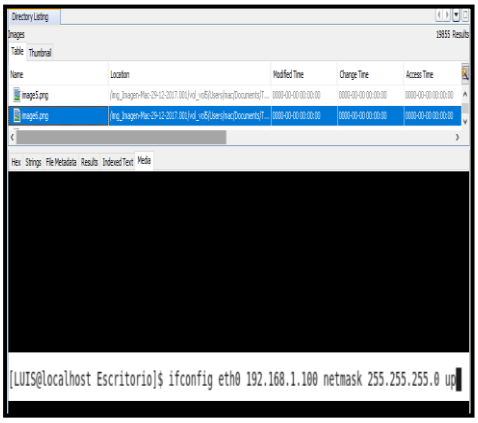
- Direcciones IP
- Nombre de usuario del Equipo Tecnológico
- Fondo de pantalla del Equipo Tecnológico
- Diversas imágenes de adolescentes

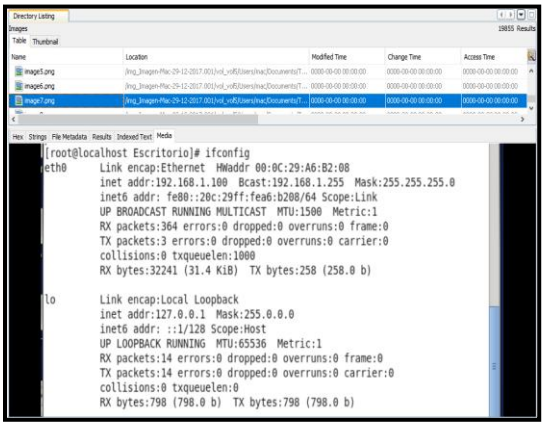
De la misma manera se determinó páginas web con más imágenes de adolescentes y archivos ofimáticos que en cada uno contenía:

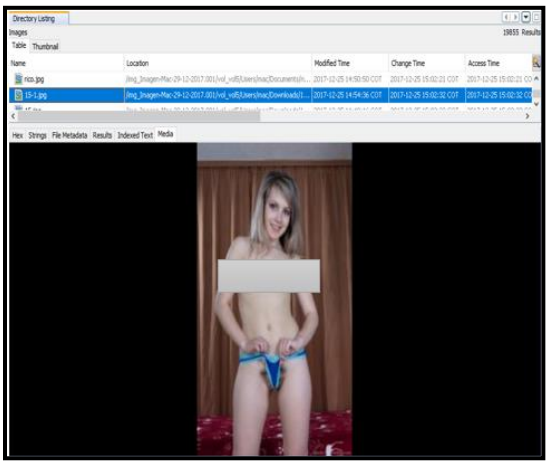
- Conversaciones
- Transferencias bancarias

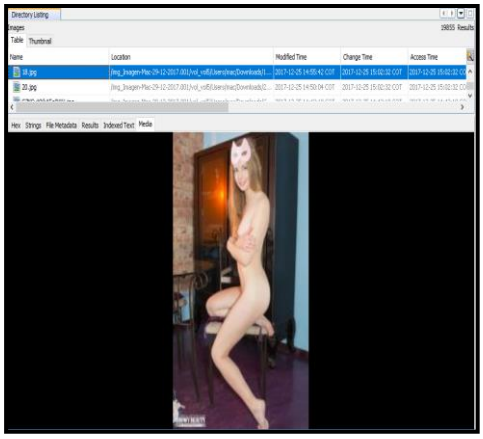
- Listado de personas con números telefónicos y correos electrónicos

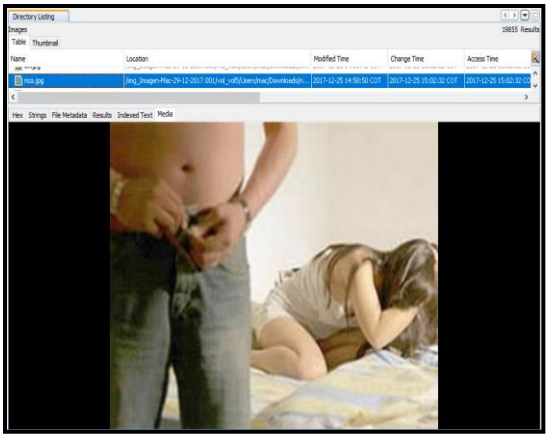
Cada evidencia fue conservada en un archivo adicional, para ser presentada en el informe final como parte de los Anexos











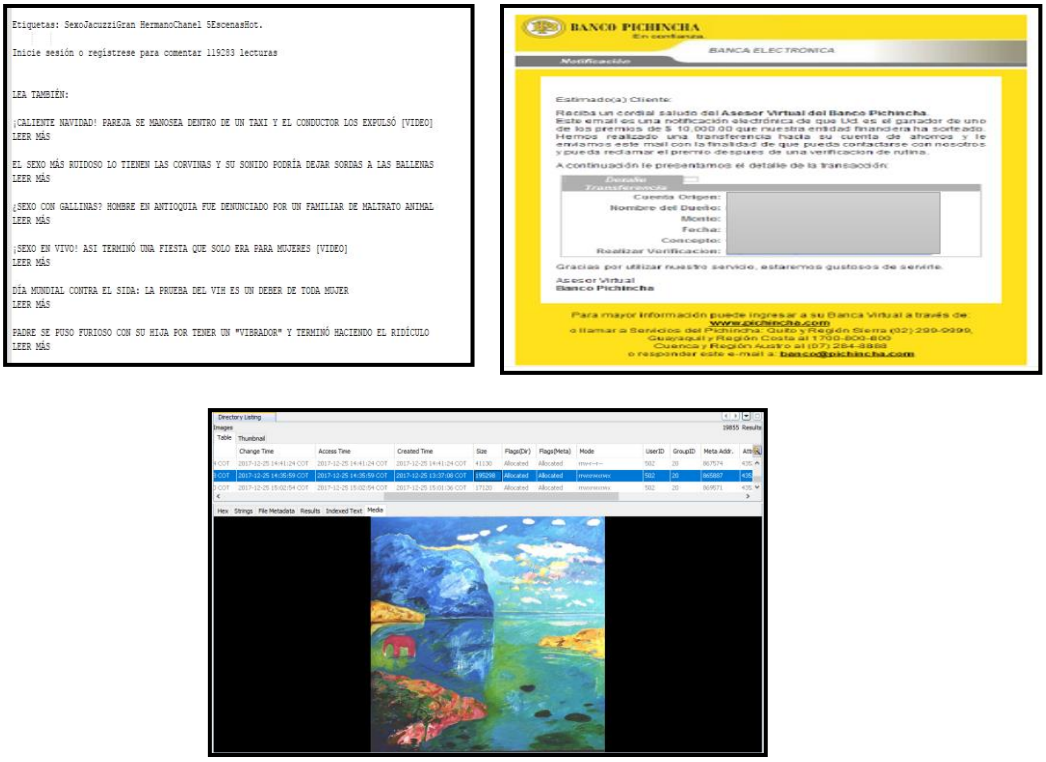
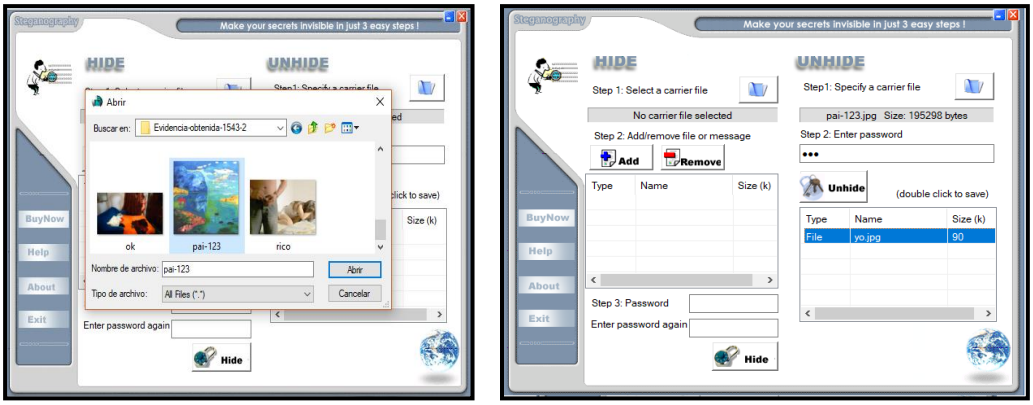


Figura No 27. Análisis de la imagen forense creada

Fuente: Byron Loarte

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. 30.



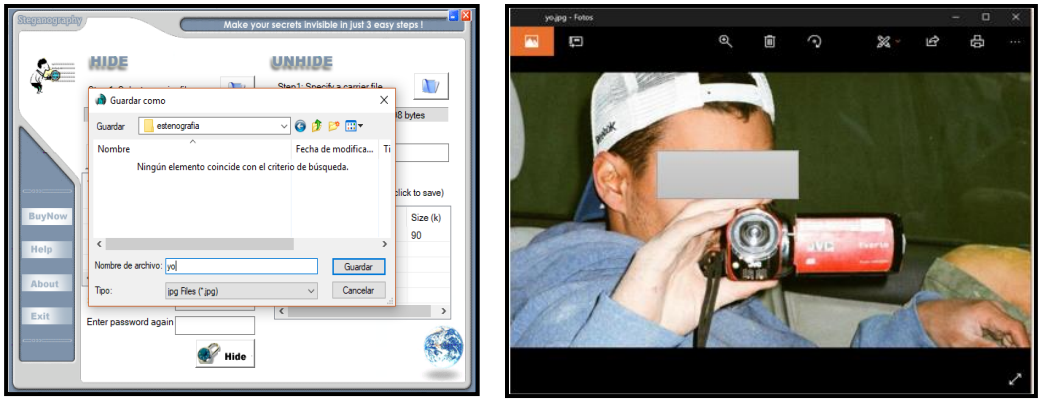


Figura No 28. Análisis de una imagen

Fuente: Byron Loarte

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 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.

CAPÍTULO IV.

DISCUSIÓN

4.1 CONCLUSIONES Y RECOMENDACIONES

- 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 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.

BIBLIOGRAFÍA

Abril, Víctor Hugo. (2008). *Técnicas 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. UNE 71506. (2013). *Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas.* Recuperado de http://www.aenor.es/aenor/inicio/home/home.asp

AGN. (01 de 02 de 2015). *En Ecuador, aumentan los delitos cibernéticos*. Recuperado el 23 de 08 de 2017, de Diario El Mercurio - Cuenca Ecuador: http://www.elmercurio.com.ec/462067-en-ecuador-aumentan-los-delitos-ciberneticos/

Arroyo Jácome, R. P. (2016). *Análisis de los delitos informáticos por ataque y acceso no autorizado a sistemas electrónicos, tipificados en los artículos 232 y 234 del Código Orgánico Integral Penal en el Ecuador.* Bachelor's thesis, Quito: UCE.

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.* (No. RFC 3227). Recuperado de http://www.rfc-editor.org/info/rfc3227

Carrier, B., & Spafford, E. H. (2001). *A Road Map for Digital Forensic Research.* Utica, New York: In Digital forensic research workshop.

Carrier, B., & Spafford, E. H. (2003). *Getting physical with the digital investigation process. International Journal of digital evidence* (Vol. 2).

Casey, E. (2004). *Digital Evidence and Computer Crime* (2 ed.). Academic Press.

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

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

Congreso Nacional. (2012). *ley de comercio electrónico firmas y mensajes de datos* (Registro Oficial Suplemento 557 ed.). Quito. Recuperado de http://www.justicia.gob.ec/

Consejo de la Judicatura. (2014). *Reglamento del sistema pericial integral de la función judicial.* Quito. Recuperado de http://www.funcionjudicial.gob.ec/

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

Constitución De La Republica Del Ecuador. (2008). Recuperado de http://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Diario la Hora. (29 de 05 de 2016). Sección contra el Cibercrimen recibió 50 denuncias por delitos informáticos. *Diario La Hora*. Recuperado de http://lahora.gt/seccion-cibercrimen-recibio-50-denuncias-delitos-informaticos/

Ernesto Martínez de Carvajal Hedrich. (2012). *Informática forense: 44 casos reales* (1ª Edición ed.). ISBN13:9788461581214 .

Estrada, G. M. (2008). *Delitos informáticos*. Recuperado de https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf

Europa, C. D. (2001). *Coe.int*. Recuperado de Convenio sobre la ciberdelincuencia: http://www.coe.int/en/web/portal/home

Fiscalia.gob.ec. (2015). *Los delitos informáticos van desde el fraude hasta el espionaje*. Recuperado el 23 de 08 de 2017, de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/boletines/151-2015/junio-2015/4208-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.

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

Gutiérrez J. D.& Zuccardi G. (2006). *Informática Forense.*

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

Huerta Miranda, M., & Líbano Manzur, C. (1996). Los Delitos. Editorial Jurídica Cono Sur.

ISO/IEC 27037. (2012). *Guidelines for identification, collection, acquisition and preservation of digital evidence* (1 ed.).

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response.* NIST Special Publication, 10, 800-86.

Lázaro Domínguez, F. (2013). *Introducción a la Informática Forense.* RA-MA EDITORIAL.

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 (1))*, 42-78. Obtenido de http://www.rmlconsultores.com/revista/index.php/crv/article/view/463

López Delgado, M. (2007). *Análisis Forense Digital* (2da Edición ed.).

López, M. (18 de 05 de 2010). *Applesfera.com*. Obtenido de La seguridad actual en OS X: datos, argumentos y razones para considerarla: https://www.applesfera.com/os-x/la-seguridad-actual-en-os-x-datos-argumentos-y-razones-para-considerarla

McKemmish, R. (1999). *What is forensic computing?* Canberra: Australian Institute of Criminology.

Ministerio de Justicia, D. H. (2014). *Código Orgánico Integral Penal.* Quito: Ministerio de Justicia, Derechos Humanos y Cultos. Recuperado de http://www.justicia.gob.ec/

Ministerio del Interior. (2014). *Ministerio del Interior*. Recuperado el 28 de 08 de 2017, de Laboratorio de Criminalística y Ciencias Forenses: Punto de encuentro técnico – científico: http://www.ministeriointerior.gob.ec/laboratorio-de-criminalistica-y-ciencias-forenses-punto-de-encuentro-tecnico-cientifico/

Pérez Laguna, C., & Ríos Oruña, A. (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

Pous, H. R., Ruiz, J. S., & López, J. L. R. (2009). *Análisis forense de sistemas informáticos.* Barcelona: Eureca Media, SL.

Prieto, A., Lloris, A., & Torres, J. (2002). Introducción a la Informática. McGraw-Hill.

Ramírez, G. A. (2003). Delitos cibernéticos. *Enter@te*(23). Recuperado el 23 de 08 de 2017, de http://www.enterate.unam.mx/Articulos/2003/octubre/delitos.htm

Rivas, C. G. (2014). *Metodologías para un análisis forense.*

Sánchez Herrera, K. E., & Basantes Salazar, C. A. (2016). *Análisis forense a sistemas operativos mediante la utilización de herramientas Open Source, caso estudio Windows 8.* Quito: Bachelor's thesis, Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería de Sistemas e Informática.

Security, P. (s.f.). *Así te infectan los 10 virus más peligrosos para Mac*. Recuperado el 23 de 08 de 2017, de Panda Security Mediacenter: http://www.pandasecurity.com/spain/mediacenter/malware/los-10-virus-mas-peligrosos-mac/

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

Tellez Valdez, J. (1996). Los delitos informáticos: situación en México. *revista iberoamericana de derecho informático, 1*(12-13-14-15), 461-473.

Wilkinson, S., & Haagman, D. (2010). *Good practice guide for computer-based electronic evidence.* Association of Chief Police Officers.

ANEXOS

ANEXO A - FORMULARIO N° 1

Información personal del perito a cargo de la investigación.

FORMULARIO N° 1 DATOS PERSONALES			
LUGAR Y FECHA			
NOMBRES COMPLETOS			
CEDULA DE CIUDADANÍA			
CORREO ELECTRÓNICO			
ESPECIALIZACIÓN			
CÓDIGO DE PERITO			
SERVIDOR/A PUBLICO		INSTITUCIÓN	
FIRMA PERITO INFORMÁTICO		_____	

ANEXO B -FORMULARIO N° 2

Información referente a la escena del delito

FORMULARIO N° 2 DESCRIPCIÓN DE LA ESCENA DEL DELITO				
CASO				
LUGAR				
FECHA Y HORA				
NÚMERO DE PERSONAS EN EL LUGAR				
NOMBRES COMPLETOS DE LAS PERSONAS EN EL LUGAR				
PERSONAS QUE TIENE ACCESO AL EQUIPO A SER INVESTIGADO				
FOTOGRAFÍA DEL LUGAR		DESCRIPCIÓN		
TESTIMONIOS DE LAS PERSONAS QUE ESTABAN EN EL LUGAR	SI			
	NO			
DESCRIPCIÓN DE LOS EQUIPOS A SER INVESTIGADOS				
NÚMERO DE ETIQUETA				
TIPO DE DISPOSITIVO		CARACTERÍSTICA		
DESCRIPCIÓN FÍSICA				
ESTADO	ENCENDIDO		APAGADO	
UBICACIÓN				
PERIFÉRICOS CONECTADOS				
CONEXIÓN A INTERNET				
FOTOGRAFÍA				

OBSERVACIÓN	
OBSERVACIONES GENERALES	
---------- **FIRMA PERITO INFORMÁTICO**	---------- **FIRMA NOTARIO / FISCAL**

ANEXO C -FORMULARIO N° 3

Información referente a la recopilación de la evidencia original de los diferentes dispositivos de almacenamiento que serán utilizados para la investigación.

FORMULARIO N° 3 RECOPILACIÓN DE LA EVIDENCIA ORIGINAL						
CASO						
NOMBRE DEL PERITO INFORMÁTICO						
LUGAR						
FECHA Y HORA						
NÚMERO DE ETIQUETA						
TIPO DE EQUIPO IMPLICADO						
ESTADO			ENCENDIDO		APAGADO	
FECHA Y HORA DE APAGADO DEL EQUIPO						
OBSERVACIÓN						
MARCA	SERIE	MEMORIA RAM	SISTEMA OPERATIVO		PROCESADOR	DISCO DURO
DESCRIPCIÓN DE LA RECOPILACIÓN DE LA EVIDENCIA						
NÚMERO DE ETIQUETA						
DISPOSITIVO DE ALMACENAMIENTO						
MÉTODO / APLICACIÓN UTILIZADO						
CREADO POR (NOMBRE Y CARGO)						
FECHA		HORA		CÓDIGO HASH		

---------- **FIRMA PERITO INFORMÁTICO**	---------- **FIRMA NOTARIO / FISCAL**

ANEXO D -FORMULARIO N° 4

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.

<table>
<tr><th colspan="6">FORMULARIO N° 3 ALMACENAMIENTO Y TRANSPORTE DE ELEMENTOS FÍSICOS O CONTENIDO DIGITAL</th></tr>
<tr><td colspan="3">CASO</td><td colspan="3"></td></tr>
<tr><td colspan="3">NOMBRE DEL PERITO INFORMÁTICO</td><td colspan="3"></td></tr>
<tr><td colspan="3">LUGAR</td><td colspan="3"></td></tr>
<tr><td colspan="6">DESCRIPCIÓN DEL ALMACENAMIENTO</td></tr>
<tr><td colspan="3">NÚMERO DE ETIQUETA</td><td colspan="3"></td></tr>
<tr><td colspan="3">TIPO DE EQUIPO IMPLICADO</td><td colspan="3"></td></tr>
<tr><td colspan="3">OBSERVACIÓN</td><td colspan="3"></td></tr>
<tr><td>MARCA</td><td>SERIE</td><td>MEMORIA RAM</td><td>SISTEMA OPERATIVO</td><td>PROCESADOR</td><td>DISCO DURO</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">REMITENTE</td><td colspan="3">DESTINATARIO</td></tr>
<tr><td>NOMBRE</td><td></td><td>FIRMA</td><td>NOMBRE</td><td></td><td>FRIMA</td></tr>
<tr><td colspan="3">MOTIVO</td><td>LUGAR</td><td colspan="2"></td></tr>
<tr><td colspan="3"></td><td>CÓDIGO HASH</td><td colspan="2"></td></tr>
<tr><td>FECHA</td><td></td><td>HORA</td><td colspan="3"></td></tr>
<tr><td colspan="3">FOTOGRAFÍA</td><td colspan="3"></td></tr>
<tr><td colspan="6">DESCRIPCIÓN DEL TRANSPORTE</td></tr>
<tr><td colspan="3">NOMBRE DE LA PERSONA A CARGO DEL TRANSPORTE</td><td colspan="3"></td></tr>
<tr><td colspan="2">MEDIO DE</td><td></td><td>PLACAS DEL TRANSPORTE</td><td colspan="2"></td></tr>
</table>

TRANSPORTE			
---------- FIRMA PERITO INFORMÁTICO	**---------- FIRMA NOTARIO / FISCAL**		**---------- FIRMA DEL TRANSPORTISTA**