UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE CUENCA

CARRERA DE INGENIERÍA DE SISTEMAS

Tesis previo a la obtención del

Título de Ingeniero de Sistemas

"METODOLOGÍA PARA EL ANÁLISIS FORENSE DE DATOS E IMÁGENES DE ACUERDO A LAS LEYES DEL ECUADOR"

Autor: Gabriela Estefanía Granda Tonato

Director: Ing. Pablo Gallegos

Cuenca, Marzo 2015

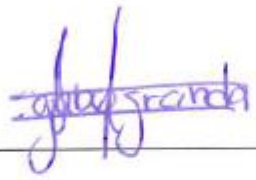
ECUADOR

DECLARACIÓN

Yo, GABRIELA ESTEFANIA GRANDA TONATO, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que incluyen en este documento.

A través de la presente declaración cedo el derecho de propiedad intelectual correspondiente a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad vigente.

Cuenca, Marzo del 2015



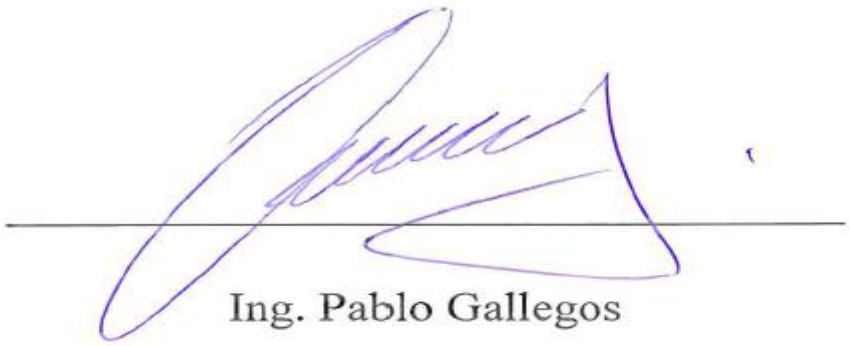
Gabriela Granda Tonato

CERTIFICACIÓN

Ing. Pablo Gallegos

Certifico:

Haber dirigido y revisado adecuadamente cada uno de los capítulos del proyecto de Tesis titulado **METODOLOGÍA PARA EL ANÁLISIS FORENSE DE DATOS E IMÁGENES DE ACUERDO A LAS LEYES DEL ECUADOR",** realizado por la Srta. Gabriela Estefanía Granda Tonato, y por Cumplir los requisitos autorizo su presentación.



Ing. Pablo Gallegos

Director de Tesina

DEDICATORIA

A mi familia, porque a pesar de los duros momentos que nos tocó vivir estuvieron a mi lado alentándome para seguir adelante, a mis amigos quienes con sus palabras y acciones me dieron la fortaleza para no decaer.

AGRADECIMIENTO

Agradezco a Dios por llenarme de bendiciones en cada momento de mi vida, mandándome ángeles como mi familia y amigos quienes a lo largo de esta tesis me dieron palabras de aliento haciéndome saber que cuento con personas que esperan verme triunfar.

De manera muy especial agradezco a mi tía Norma, pues fue un pilar muy importante en mi formación académica y personal, sé que estará muy orgullosa de verme culminar una meta más.

A mis padres, José y Verónica, ya que gracias a su esfuerzo y dedicación me han dado la oportunidad de formarme académicamente.

Al Ing. Pablo Gallegos por su paciencia y dedicación al acompañarme durante el desarrollo de este proyecto de tesis.

ÍNDICE DE CONTENIDOS

ILUSTRACIONES

ANTECEDENTES

De acuerdo al censo realizado en el Ecuador en el año 2010 y el estudio realizado en el 2013, la página Web del [1]Instituto Nacional de Estadísticas y Censos (INEC) informa que el 40 % de los ecuatorianos utiliza regularmente el servicio de internet. Realizando la comparación entre las estadísticas recogidas en el 2010 y el 2013 el aumento en el uso del internet es bastante grande pues en el 2010 solamente el 11.8% de la población lo utilizaba generando un crecimiento considerable ya que para el 2013 ya se registraban entre el 37% y 40% de uso, por lo que a largo plazo las estadísticas subirán y los índices de delitos que se desarrollan sobre este medio serán muy altos.

En base a las estadísticas presentadas por [2]Diario el Telégrafo en su artículo presentado de Junio del 2014 se realiza el siguiente diagrama.

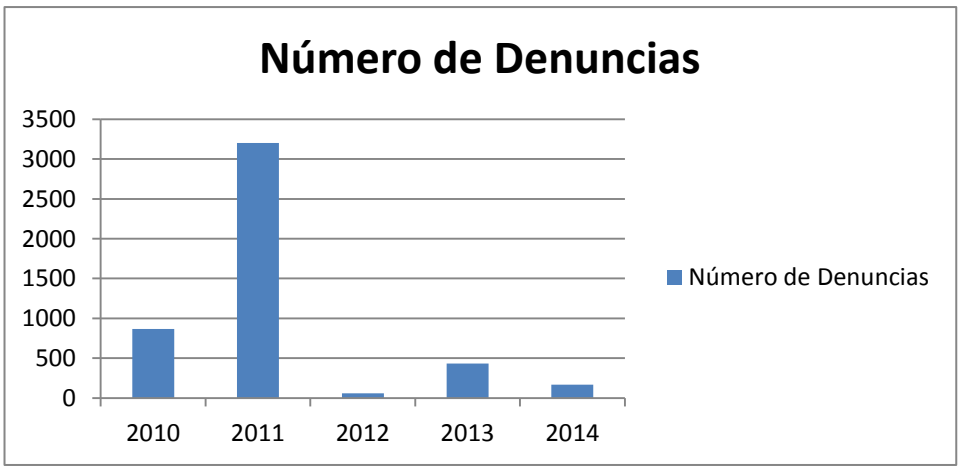


Ilustración 1 Número de Denuncias Años 2010-2014

Fuente: Diario El Telégrafo Junio 2014

Como se puede observar en el grafico el año 2011 fue donde más denuncias sobre delitos informáticos recibió la policía nacional y por esta razón se realizó un estudio

[1] Instituto Nacional de Estadísticas y Censos (Disponible en : http://www.ecuadorencifras.gob.ec/, Consultado: 07-10-2014)
[2]Diario el telégrafo, 25 de Junio del 2014 (Disponible en: http://www.telegrafo.com.ec/justicia/item/hay-600-casos-de-delitos-electronicos-en-17-meses.html, Consultado: 07-10-2014)

y se conformó la [3]Unidad de Investigación de Cibercrimen - Policía Judicial del Ecuador con bases en las unidades existentes en países como [4]Chile, esta unidad de la policía esta encarda de investigar y dar seguimiento a delitos donde se vean inmiscuidos medios informáticos y electrónicos.

Los delitos informáticos más comunes y por lo que existen varias denuncias se mueven bajo la técnica denominada Ingeniería Social, la cual abarca delitos como suplantación de identidad, robo de información, fraudes bancarios, acoso, estafa, entre otros. Se la denomina con este nombre ya que no hace falta de un amplio conocimiento informático, más bien se busca atrapar a la víctima de una manera casual, social es decir con el simple hecho de enviarle una foto, un video que le llame la atención el delincuente puede cometer uno de estos delitos.

La suplantación de identidad ha sido un caso que viene dándose desde el 2011 donde una cantidad considerable de personas denuncian haber sido víctimas de la clonación de sus perfiles en redes sociales causando malestar en la población ecuatoriana.

La falta de conocimiento y de penalidad ha hecho que este tipo de delitos crezca considerablemente, por lo que las autoridades han tomado cartas en el asunto ya que sea modificado el [5]Código Orgánico Integral Penal (COIP), tipificando algunos delitos informáticos por lo que el Ecuador comienza a ponerle frente a la delincuencia.

Otro factor que influye en el crecimiento de estos índices es el analfabetismo informático que sufre el Ecuador, si bien la población comienza a utilizar el internet, no lo hace a conciencia es decir no toma medidas de seguridad para evitar ser víctimas de delincuentes cibernéticos que se aprovechan del desconocimiento de la mayoría de las personas para enviarles programas maliciosos disfrazados en imágenes videos, correos, etc.

---

[3] Unidad de Investigación de Cibercrimen (Disponible en :https://www.facebook.com/CibercrimenPJ.EC, Consultado: 07-10-2014)

[4] Brigada Investigadora del Ciber Crimen, (Disponible en: http://www.policia.cl/paginas/brigadas/bg-bricib/bg-bricib.htm, Consultado: 07-10-2014)

[5]COIP.(Disponible en: http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf, Consultado: 10-10-2014)

JUSTIFICACIÓN

El Ecuador presenta un crecimiento en el uso del servicio de internet, ya que en ocasiones llega a ser tomado como uno de los servicios básicos de una familia, teniendo la misma prioridad como el servicio de agua y luz.
Es por esto que el gobierno ecuatoriano debe tomar cartas en el asunto y comenzar a dar soluciones legales sobre delitos que se pueden cometer mediante el uso de este servicio.

El Código Orgánico Integral Penal vigente presenta una sección de artículos donde se tipifican algunos de los delitos más comunes que en el Ecuador suceden, sin embargo estos artículos no son suficientes ya que existen otros delitos que no son cubiertos.

El nuevo proceso de firmas digitales, voto electrónico, factura electrónica, etc, que está viviendo el Ecuador nos llevan a tomar en consideración esta temática, pues la necesidad de saber que los datos e imágenes utilizadas en estos procesos son verdaderos, es de importancia pública.

El estudio del arte y la creación de una metodología para realizar un análisis informático con bases legales es decir una metodología que se apegue 100% a lo que dicta el ámbito judicial ecuatoriano, ayudaría para que se puedan juzgar y penalizar correctamente los delitos informáticos que en la actualidad se presentan.

Para garantizar la confianza de la comunidad en cuanto a la seguridad de su información ya sea en este caso “DATOS” e “IMAGENES”, se puede hacer uso de la ciencia forense, ya que se dedica a estudiar y definir las actividades que involucren la recuperación y el análisis de pruebas judiciales en caso de existir algún delito informático. Esta herramienta ayudaría para verificar, comprobar y publicar la validez de los procesos anteriormente mencionados, y así lograr que la comunidad crea en el cambio digital que presenta esta era.

OBJETIVOS

Objetivo General

- Desarrollar una metodología para el análisis forense de datos e imágenes de acuerdo a las leyes del Ecuador.

Objetivos Específicos

- Analizar y Entender las leyes ecuatorianas referentes a delitos informáticos.
- Investigar y Comprender términos referentes a la informática forense.
- Definir una cadena de custodia genérica para datos e imágenes.
- Desarrollar una metodología para el análisis de datos e imágenes.

INTRODUCCIÓN

Los delitos informáticos se encuentran en pleno auge, aunque la ciudadanía no comprenda o no lo tome enserio, las estadísticas son muy altas.

El manual de Prevención y Control de Crímenes informáticos de las Naciones Unidad clasifica como crimen cibernético al fraude, falsificación y acceso no autorizado.

Con esto quiero expresar que un hacker ya no solamente es la persona que violaba la seguridad de algún sistema o dispositivo solamente para demostrar sus conocimientos, sino que hace uso de los datos o información encontrados en estos sistemas para beneficio personal, por lo que puede incurrir en varios delitos típicos llevados al mundo digital.

Los ecuatorianos pensamos que por ser un país en vías de desarrollo no somos vulnerables ante este tipo de delincuencia, es por esto que la Asamblea Nacional del Ecuador ha tomado en consideración las estadísticas presentadas por la Unidad de Investigación de Cibercrimen y ha puesto en vigencia 6 artículos dentro de la sección Tercera denominada DELITOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN, así como el desarrollo de la ley de [6]Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, buscando controlar o tipificar los delitos que en años atrás no tenían sentencia o procedimiento a seguir.

De acuerdo a la Unidad de Investigación de Cibercrimen en el Ecuador se han presentado 452 denuncias en los primeros 6 meses del año 2014 de los cuales el 55% de estos corresponden a fraude electrónico superando las estadísticas del años 2013 que presentaban un 34% con respecto a este delito.

[6] Ley de Comercio Electrónico (Disponible en : http://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf , Consultado: 13-10-2014)

Los principales delitos presentados son por fraude electrónico, ingreso no autorizado y robos virtuales, es decir el sector bancario es el más afectado por los ciberdelincuentes, sin dejar atrás delitos como el acoso sexual, suplantación de identidad etc.

Es por esto de la presencia de la Unidad de Investigación de Cibercrimen, la cual vela por proveer de seguridad en el ámbito cibernético, digital a la población Ecuatoriana.

CAPITULO I. INTRODUCCIÓN

1.1 Definición de Delito Informático

En la actualidad no existe una definición aprobada o aceptada mundialmente sobre que es un delito informático, por lo que citare algunas definiciones como la de [1]JIJENA LEIVA quien considera que un delito informático es "toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento autorizado de la misma."[7]

Por otro lado el Departamento de Investigación de la Universidad de México considera que como delito informático a [8]"todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático".

Como definición personal considero como Delito Informático a todo aquel delito que pueda juzgarse bajo el Código Penal del Ecuador, y que haya hecho uso de dispositivos, datos, información, sistemas informáticos, como medio, o fin para el desarrollo de una actividad ilícita.

[7] Renato Javier Jijena Leiva, "la criminalidad informática: situación de lege data y lege ferenda en chile," informática y derecho, 1994

[8]Delitos Cibernéticos, Gustavo Gutiérrez, UNAM (Disponible en: http://www.enterate.unam.mx/Articulos/2003/octubre/delitos.htm Consultado: 13-10-2014)

1.2 Principio de Intercambio Locard

[2]El principio fue planteado en el año de 1910 por el [9]Dr. Edmond Locard, Profesor de la Universidad de Lyon en Francia.

El Dr. Locard baso su investigación en que en un delito siempre existirá evidencia entre el autor del crimen y la víctima es decir "Todo contacto deja un rastro". Por esta razón es llamado el principio de intercambio.

Principio de intercambio de Locard: **"Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto".**

Este principio da pie para entender que cuando sucede un delito informático siempre encontraremos algún rastro o huella de quien fue el autor de dicho delito, informáticamente hablando existen varios software y hardware de los que nos podemos ayudar para determinar el autor o la causa.

Por esta razón la validez de la evidencia informática encontrada depende de la perfecta identificación, aislamiento y almacenamiento, con el fin de no comprometer los rastros encontrados.

1.3 Estudio de la Legislación Ecuatoriana aplicada al código penal

1.3.1 Código Penal

De acuerdo a las Nomas Rectoras en el Articulo 1, El Código Orgánico Integral Penal "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".

[9] Dr. Edmond Locard, Biografía, (Disponible en: http://es.wikipedia.org/wiki/Edmond_Locard, Consultado: 14-10-2014)

El Código Orgánico Integral Penal aprobado en Agosto del 2014 permite sancionar delitos informáticos, que pueden tener condenas de cárcel por entre 3 y 5 años.

La sección Tercera del Capítulo 3 del Código Orgánico Integral Penal (COIP) presenta los **DELITOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN**.

Los delitos informáticos tratados en esta sección son los siguientes:

- **Artículo 229:** Revelación ilegal de base de datos.
- **Artículo 230:** Interceptación ilegal de datos.
- **Artículo 231:** Transferencia electrónica de activo patrimonial.
- **Artículo 232:** Ataque a la integridad de sistemas informáticos.
- **Artículo 233:** Delitos contra la información pública reservada legalmente.
- **Artículo 234:** Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

Es de importancia para el desarrollo de este tema de tesis mencionar artículos que se encuentran dentro del COIP, que están relacionados directamente con las ciencias forenses, debido a que estos artículos mencionan parte de una cadena de custodia en cuanto a evidencia, se los puede aplicar dentro de un juicio por delito informático.

- **Artículo 449:** Atribuciones: Atribuciones del personal del Sistema especializado integral de investigación, medicina legal y ciencias forenses.
- **Artículo 456:** Cadena de Custodia.
- **Artículo 457:** Criterios de valoración.
- **Medios de Prueba. Artículo 499:** Reglas Generales: El documento.
- **Artículo 500:** Contenido digital.

1.3.2 Delitos contra la seguridad de los activos de los sistemas de información y comunicación

- **Intercepción ilegal de datos**

Este artículo se refiere a las personas que de alguna forma intercepten, escuchen, graben, o alteren datos informáticos ya sean en el emisor o en el receptor. Por lo que podemos ser juzgados bajo este artículo si se llegara a comprobar la alteración de alguna imagen o dato informático.

- **Transferencia electrónica de activo patrimonial.**

La trasferencia electrónica de activo patrimonial sanciona a la o las personas que con ánimo de lucro altere sistemas o datos informático entre estos imágenes, audio, etc., con el fin de apropiare de un activo patrimonial no concedido.

- **Ataque a la integridad de sistemas informáticos**

Este artículo sanciona a la o las personas que atenten contra la integridad física y lógica de sistemas informáticos.

Dentro del daño lógico de los sistemas informáticos, encontramos el borrar, alterar, causar mal funcionamiento, etc.

Se puede acudir a este artículo para respaldar la investigación de imágenes y datos alterados con el fin de verificar la validez de los mismo para ser utilizados como evidencia en algún de delito.

- **Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.**

El acceso no concedido a un sistema informático, telemático o de telecomunicaciones sanciona a la o las personas que no tengan autorización para acceder a los diferentes sistemas anteriormente mencionados. Este artículo puede ser

de ayuda para la realizar un análisis forense de datos e imágenes ya que estos medios pueden contener virus backdoor, etc. para realizar el ingreso a los sistemas mencionados.

1.3.3 Sistema Especializado integral de investigación de Medicina legal y ciencias forenses.

Cito los siguientes artículos del COIP, con los que se puede trabajar en el campo de la informática forense, debido a que el Código Orgánico Integral Penal del Ecuador, no contiene artículos donde se explique las bases para realizar investigación informática forense, se toman como referencia estos artículos.

- **Atribuciones del personal del Sistema especializado integral de investigación, medicina legal y ciencias forenses.**

Este artículo contiene varios ítems de importancia entre ellos:

- "Vigilar, resguardar, proteger y preservar el lugar donde presuntamente se comente la infracción y recoger los resultados, huellas, señales, armas, objetos, instrumentos y demás vestigios". Haciendo uso de este ítem se puede decir que nos ayudaría como referencia para vigilar, resguardar, proteger y preservar, tanto el lugar de la infracción y los dispositivos informáticos que se encuentren en dicho lugar.
- "Proceder al levantamiento e identificación del cadáver".
- Como se explicó anteriormente estos ítems nos sirven como referencias para realizar la investigación pertinente en caso de un delito informático, por lo que este ítem se podría interpretar por "El levantamiento e identificación de dispositivos, sistemas informáticos y telemáticos".
- "Cumplir de acuerdo con los plazos señalados, las disposiciones para la práctica de diligencias investigativas de la o el fiscal."
- "Solicitar a la o al fiscal la autorización judicial para la práctica de diligencias investigativas."

- Este ítem se lo toma como referencia para iniciar y finalizar la investigación, de acuerdo a los plazos que el fiscal allá señalado.

Cadena de Custodia

Este artículo explica cuál será la cadena de custodia de los elementos físicos o contenido digital, que servirá como prueba.

Esta cadena de custodia garantía la integridad de los elementos y contenido recogido, llevando una bitácora de los cambios hechos por cada custodio.

La cadena de custodia comienza en el momento de la recolección de las evidencias y termina cuando existe una orden de la autoridad competente.

Es de gran importancia aplicar una cadena de custodia, pues los elementos de prueba no se verán comprometidos en caso de una mala práctica, ya que se llevara una bitácora de cambios, de esta forma no se alterar la evidencia. Los responsables de que se cumpla con la cadena de custodia según el COIP son el personal del Sistema especializado integral de investigación de medicina legal y ciencias forenses, así como cada custodio de la evidencia.

Criterios de valoración

Dentro de los criterios de valoración se toma en cuenta la cadena de custodia, para valorar la autenticidad y legalidad de las prueba presentadas, así también se las deberá fundamentar científicamente.

Medios de Prueba: Reglas Generales

En el artículo reglas generales, se establece que registros, archivos, ya sean estos físicos o digital sirven como material probatorio dentro de un juicio.

Medios de Prueba: Contenido Digital

Contenido Digital se refiere a cualquier dato digital almacenado, procesado o transmitido en dispositivos o siendo parte de un sistema informático.

El COIP presenta 4 reglas a seguir para realizar una investigación donde son parte fundamental los datos digitales.

- Análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizara a través de técnicas digitales forenses.
- Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizara su recolección, en el lugar y en el tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicara la cadena de custodia y se facilitara su posterior valoración y análisis de contenido.
- Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizara su recolección, con técnicas digitales forenses para preservar su integridad, se aplicara la cadena de custodia y se facilitara su posterior valoración y análisis de contenido.
- Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e investigar cada objeto individualmente, fijara su ubicación física con fotografías y un plano de lugar, se protegerá a través de técnicas digitales forenses y se trasladara mediante cadena de custodia a un centro de acopio especializado para este efecto.

Este último artículo engloba de alguna forma los pasos o reglas a seguir en una investigación donde las pruebas principales son datos digitales, dispositivos, sistemas informáticos o telemáticos.

1.3.4 [10]Ley de Comercio electrónico, firma electrónicas y mensajes de datos.

[3]La ley de comercio electrónico presenta artículos donde se especifica y reconoce como evidencia ante un juicio legal, documentos digitales y dispositivos informáticos y telemáticos.

Esta ley se pone en vigencia debido a que en la actualidad el INTERNET se ha vuelto un medio para el comercio y la producción de negocios grandes como pequeños. El gran auge del internet ha llevado el comercio común al mundo informático, es decir la mayor parte de negocios ahora se los puede realizar de manera electrónica, requiriendo así de una alta seguridad en sus transacciones.

Es por esto de la creación de esta ley, para que en el Ecuador existan fundamentos jurídicos en caso de ser víctimas de un delito dentro del medio electrónico.

Para aclarar el para que de esta ley cito el articulo uno de la misma.

"Artículo 1: Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluyendo el comercio electrónico y la protección a los usuarios de estos sistemas."

- **Mensaje de Datos, Artículo 2:** Este artículo reconocer que los mensajes de datos tienen igual valor jurídico que los documentos escritos.

- **Mensaje de Datos, Artículo 3:** Específica que se podrá presentar o referir como evidencia todo contenido que este dentro de un mensaje de datos, es decir si llegara a estar un enlace o link a una página o documentos electrónico, el contenido de estos también forma parte del mensaje de datos.

[10] Ley de Comercio Electrónico del Ecuador, (Disponible: http://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf Consultado: 17-10.2014)

- **Mensaje de Datos, Artículo 5:** Especifica el grado de confidencialidad y reserva del contenido de los mensajes de datos.

- **Mensaje de Datos, Artículo 6:** Información Escrita: los mensajes de datos podrán ser presentados como información escrita solamente si estos pueden ser accesibles para una posterior consulta.

- **Mensaje de Datos, Artículo 7:** Específica que el mensaje de datos debe ser presentado en su forma original, es decir conservar su integridad, manteniendo completo su contenido y sin ninguna alteración.
- Este mensaje deberá pasar por un proceso donde se comprobara que el mensaje no ha sido modificado.

- **Mensaje de Datos, Artículo 8:** Este artículo trata sobre la conservación de los mensajes de datos, presenta 4 reglas o requerimientos para la correcta conservación del mensaje de datos.

    - El contenido del mensaje de datos deberá ser accesible para una posterior consulta.
    - Se deberá conservar el formato original de envió o recepción del mensaje, o en su defecto por cuestiones de almacenamiento o preservación se deberá utilizar un formato donde se a demostrable el formato original.
    - En una posterior consulta el mensaje deberá contener sus datos originales, es decir fecha y hora de cuando fue creado, generado, procesado, enviado, recibido y almacena. Así como el origine y el destino de dicho mensaje.
    - Mantener la integridad del mensaje y su contenido, durante el tiempo de investigación y el que establezca la ley.

- **Mensaje de Datos, Artículo 10:** Establece las acciones a tomar con referencia a la procedencia e identidad de un mensaje de datos. Este artículo deduce que si el emisor no avisa previamente que los mensajes de datos que salen de su cuenta no son de su autoría, estos automáticamente son atribuidos

a él. En cuanto al receptor, este está autorizado para realizar cualquier acción con dicho mensaje.

- **Mensaje de Datos, Artículo 11**: Presenta reglas o ítems a seguir para establecer cuál es el lugar y momento de envió y recepción de un mensaje de datos

- **Mensaje de Datos, Artículo 12:** Un mensaje de datos es único, es decir cada mensaje de datos presentado ser considerado como diferente.

- **Firmas Electrónicas, Artículo 13:** Una firma electrónica son datos dentro de un mensaje de datos, el cual abala o identifica al titular de dicho mensaje. Al incorporar una forma electrónica dentro de un mensaje de datos el emisor aprueba y reconoce el contenido del mensaje de datos.

- **Firmas Electrónicas, Artículo 14:** Una firma electrónica tiene la misma valides y efectos jurídicos que una firma manuscrita. Esta forma podrá ser utilizada como prueba o evidencia dentro de un juicio.

- **Firmas Electrónicas, Artículo 15:** Este artículo presenta los requisitos para una firma electrónica valida:

    - Deberá ser única e individual
    - Deberá permitir identificar la identidad del dueño de la firma.
    - Método de Creación y verificación confiable
    - Los datos que será firmados deben estar bajo el conocimiento y control del dueño de la firma electrónica.

- **Firmas Electrónicas, Artículo 18**: La duración de la firma electrónica es indefinida, no obstante estas podrán ser anuladas o suspendida de acuerdo a la ley vigente.

- **Firmas Electrónicas, Artículo 19:** La eliminación o extinción de una firma electrónica solamente se dará en caso del fallecimiento o voluntad del titular de la firma, o por causa judicialmente declarada.

1.3.5 Unidad de Investigación de Cibercrimen – Policía Judicial del Ecuador

La [11]Unidad de Investigación de Cibercrimen del Ecuador ubicada en la ciudad de Quito fue creada en enero del 2012 con el fin de manejar estadísticas relacionadas a los diferentes delitos informáticos o cibernéticos del Ecuador, así como de investigar y detectar toda actividad que es declarada como delito bajo el código penal del Ecuador y que para realizar dicha acción utiliza medios informáticos, electrónicos, telemáticos.

Con el fin de utilizar los resultados de dicha investigación como evidencia y preservar la seguridad digital del Ecuador.

Esta unidad de investigación ya ha realizado importantes capturas de estafadores y acosadores que utilizaban las redes sociales para realizar este tipo de crímenes. Para realizar una denuncia debemos acercarnos a la fiscalía, y de esta forma la Policía Judicial asignara el proceso de investigación a esta unidad.

Es de gran importancia el apoyo de esta unidad, pues mediante redes sociales, publicidad, etc., dan a conocer nuevos virus, spam, malware, hackers, que están delinquiendo y causando malestar a la población Ecuatoriana, como también difunde información para que la población conozca cómo cuidarse de estos ciberdelincuentes.

La Unidad de Investigación de Cibercrimen posee una cuenta de Facebook con el nombre "CibercrimenPJ.EC", así también presenta su cuenta de correo dnpj.uidt@policiaecuador.gob.ec en la que se puede solicitar información.

[11] Unidad de Investigación de Cibercrimen, (Disponible en: https://www.facebook.com/CibercrimenPJ.EC, Consultado: 20-10-2014)

CAPITULO II. INFORMÁTICA FORENSE

2.1 Definición de Informática Forense

Informática forense es la ciencia que permite la recolección, procesamiento, investigación y preservación de datos que se encuentran en dispositivos informáticos, con el fin de ser presentados como pruebas legales.

La forensita digital es un concepto que abre el camino para entender la informática forense, ya que [4]"es la forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos."

[4]Según el FBI la informática forense es "la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional"[12]. Debido a que la informática forense es un campo nuevo de estudio, todavía no tiene establecidos estándares internacionales, por lo que no es conocida aun como una ciencia.

Una parte fundamental para la aplicación de la informática forense es el uso de herramientas (software), que ayudan a realizar este proceso de una forma más a fondo, ya que estos softwares pueden analizar en periodos largos y lograr buenos resultados. Estas herramientas pueden ser aplicadas en el proceso de identificación, prevención, análisis y presentación para seguir o desarrollar una metodología forense.

[12] Generalidades y Principios de la Informática Forense [online]. (Disponible en: https://docs.google.com/document/d/1_ucocecybf3sqmc_ape373xob9xyxlx2cwzfrzxbwoy/edit Consultado: 21-10-2014)

[5]Cabe destacar que la informática forense no [13]es un mecanismo de protección sino es un mecanismo post delito si se podría llamar así ya que esta es solamente aplicada una vez que exista sospecha o a ciencia cierta se conozca que ha sucedido un delito.

2.2 Definición de Cadena de Custodia

Se denomina Cadena de Custodia al proceso aplicado sobre material probatorio para realizar diferentes investigaciones, este proceso trata de mantener la integridad, etiquetado y control de la evidencia tanto digital como electrónica.

Dentro del proceso se deberá registrar una serie de reglas entre ellas el llevar una bitácora de cambios realizados sobre la evidencia y especificar el nombre del custodio.

La cadena de custodia comienza desde el momento mismo en que son reconocidos los objetos como evidencia, entendiéndose como objetos a datos digitales, sistemas, dispositivos tanto informáticos como telemáticos, hasta llegar a los científicos forenses o funcionarios judiciales quienes realizaran la investigación respectiva y harán un informe pericial donde se especifique las alteraciones realizadas en el estudio, durante este proceso debe implementarse un procedimiento con bases científicas, utilizando metrologías criminalística.

El objetivo principal de una cadena de custodia es el conservar la integridad tanto física como lógica de los objetos recolectados, haciendo uso de procedimientos controlados que en palabras cortas se transforma en 4 fases como son la identificación, preservación, análisis y presentación de la evidencia, con esto se busca brindar un soporte científico a la evidencia digital recolectada y se espera que sea aceptada por un juez en un caso judicial.

[13] Centro de Posgrados y Actualización Profesional en Informática (CPAP).(Disponible en : .http://www.fing.edu.uy/cpap/cursos/metodolog%C3%ADas-para-el-an%C3%A1lisis-forense-inform%C3%A1tico, Consultado: 22-10-2014)

Una cadena de custodia obliga a seguir lineamientos o procesos para asegurar la **confiabilidad** de los objetos recolectados, por este motivo la preservación de la integridad, autenticidad, confidencialidad y el no repudio de los objetos recolectados aseguran un proceso transparente en el que no se encuentran contaminados los objetos de investigación y los resultados obtenidos son confiables para ser presentados como elementos probatorios.

Dentro del Código Orgánico integral Penal del Ecuador encontramos el artículo 500 donde se presenta 4 reglas a seguir dentro de una cadena de custodia, este articulo podría servir como base para crear una cadena de custodia que se apegue a una investigación por delito informático.

El aplicar correctamente las reglas que propone una cadena de custodia ayuda a que la evidencia no sea alterada o contaminada y así ser tomada como elemento probatorio dentro de un proceso judicial de esta manera garantizar que los objetos recolectados son los mismo que están siendo presentados ante el juez.

2.3 Esteganografía

2.3.1 Definición de ESTEGANOGRAFÍA

La palabra esteganografía significa "escrito protegido", por lo que según [6]EC Council la esteganografía es "la práctica de la incorporación de mensajes ocultos dentro de bits muertos o sin uso de una imagen, así como en audio la alteración o inserción de frecuencias bajas que el oído humano no escucharía"[14], los usuarios normales que comúnmente son a quienes van dirigidos estos ataques son un blanco fácil debido a su falta de conocimiento ya que no pueden detectar la alteración que sufrió su audio, video o documento, pudiendo ser víctimas de un ciberdelincuente, cabe mencionar que esta técnica puede ser utilizada de forma legal como ilegal.

[14] EC-Council, "EC-Council," in Computer Forensics Investigating Data and Image Files. USA: EC-Council, 2010, p. 227.

La esteganografía se divide en tres grandes categorías como son la esteganografía técnica, esteganografía lingüística y la esteganografía digital.

Esteganografía técnica consta de métodos físicos o químicos, ya que utilizan tintas invisibles para ocultar mensajes, por ejemplo el uso de esferos que utilizan dicha tinta y que al iluminarlos con luz led revelan el mensaje escondido.

Esteganografía lingüística hace uso de símbolos, pinturas, dibujos, letras de música, etc. para ocultar un mensaje.

Esteganografía digital hace uso de medios digitales para ocultar un mensaje, un medio digital puede ser una imagen, documento, video o audio.

Los métodos de esteganografía digital se encuentran divididos en métodos clásicos y modernos.

Entre los métodos modernos constan el enmascaramiento y filtrado, uso de algoritmos, es decir utilizan fórmulas matemáticas para ocultar información, inserción de bits menos significativos, este último el más utilizado tanto en audio, video y datos ya que se vale de las limitaciones de la percepción humana para ingresar información y de esta forma los sentidos como la vista y el oído no detectan ningún cambio.

Técnicas de esteganografía digital:

- Inyección
- Bit menos significativo
- Técnicas de Transformación de Dominio
- Generación de archivos
- Técnicas de Distorsión
- Método Estadístico
- Codificación de espectro expandido

El modelo genérico para realizar esteganografía costa de cuatro pasos, el primero de estos es determinar cuál será el mensaje que se ocultara, segundo determinar el medio que se utilizara, tercero establecer la clave secreta con la que se cifrara y descifrara el mensaje y por último el mensaje dentro del medio utilizado.

Cabe recalcar que la esteganografía no es lo mismo que la criptografía de datos, pues cuándo utilizamos la criptografía, el interceptor o intruso solamente recibirá información o datos ilegibles (sin sentido) y que sin una llave no podrá leer el contenido, mientras que en la esteganografía, utiliza una imagen, audio, video o dato, como medio para enviar información oculta, es decir si alguna persona mira una imagen no se percatara que existe algún dato detrás.

La esteganografía es una técnica muy antigua, pero que en la actualidad se la sigue utilizando, con tan solo descargarse un imagen podemos estar siendo víctimas de un virus que vino dentro de esta.

El uso de la esteganografía puede ser el inicio de un delito informático, pues como se mencionó en el capítulo anterior, se tipifica como delito a el acceso no autoriza y la alteración de información, con lo que la esteganografía puede darnos el ingreso a sistemas, dispositivos, etc.

El conocer el procedimiento para analizar imágenes y datos que pueden estar alterados mediante esteganografía es de importancia pues si se investiga un delito informático, debemos poder detectar cual es el código, algoritmo, dato o información que contiene dicha imagen o documento y que está afectando al normal desenvolvimiento del sistema o dispositivo, este estudio o detección de la esteganografía se la denomina estegoanálisis.

El estegoanálisis es el estudio de técnicas o procedimientos para la detección de cambios o alteraciones que sufren las imágenes, documentos, audio y video, este estudio aprovecha las huellas que deja la esteganografía para poder desarrollar sus técnicas, cabe recalcar que el estegoanálisis proporciona resultados por medio de estadísticas.

La aplicación técnicas de estegoanálisis garantizan la integridad y autenticación de las imágenes, documentos, audio y video que pueden ser utilizados en un litigio, por ejemplo si se presenta un video como evidencia este deberá ser estudiando mediante técnicas para verificar que no haya sido alterado y de esta forma ser aceptado como una prueba legal.

2.4 Proceso de análisis forense genérico

El análisis forense de la evidencia digital presentada debe apegarse a un proceso denominado cadena de custodia, dicho proceso se resume en cuatro pasos o reglas a seguir al momento de recolectar, investigar y almacenar la evidencia.

En el punto 2.2 se dio a conocer la importancia de la utilización de una cadena de custodia, por lo que se presentara la definición de un proceso o cadena de custodia genérica, es decir que puede tener variantes mínimas apegadas siempre a mantener limpia la evidencia, en otras palabras procurar conservar la integridad y autenticidad de la evidencia.

Aunque las pruebas digitales pueden ser versátiles para la investigación, es decir se las puede clonar y de esta manera no contaminar la evidencia, este proceso debe ser tomado con responsabilidad pues depende de cómo se lo trabaje para que la evidencia pueda ser aceptada en un litigio.

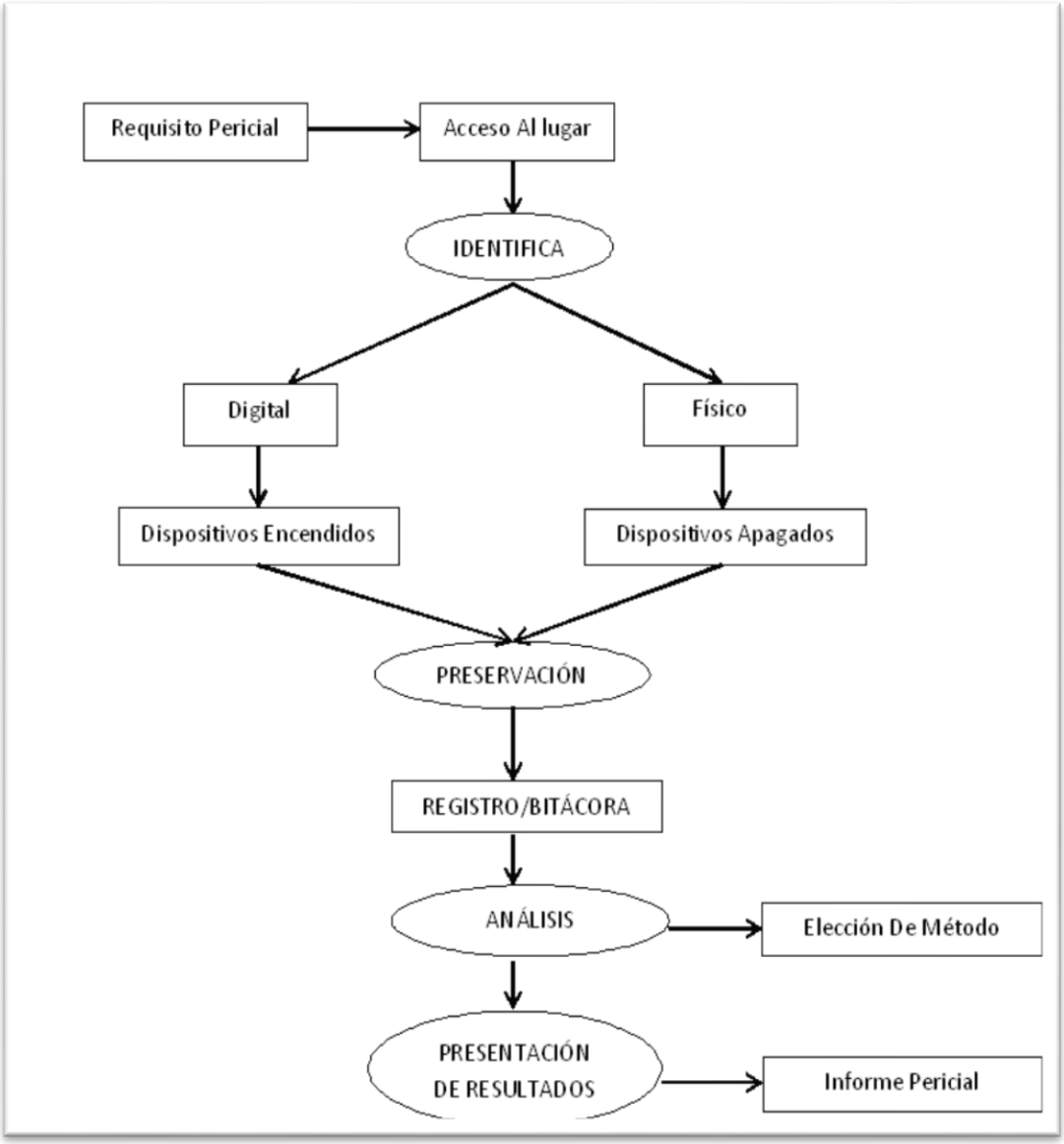


Ilustración 2 Fases de Cadena de Custodia Genérica

2.4.1 Identificación

El proceso de investigación debe ser realizado en el lugar original es decir donde se recauda o recoge el objeto de evidencia. La identificación consiste en recolectar información importante o relevante de los dispositivos que han sido utilizados para cometer un delito, por ejemplo si se trata de un [15]CPU, se debe de recolectar su número de serie, modelo, características y si es posible respaldar toda esta información con fotografías.

[15] Unidad Central de Procesamiento, (Disponible en: http://es.wikipedia.org/wiki/Unidad_central_de_procesamiento, Consultado: 25-10-2014)

Para esta fase se debe realizar un inventario del hardware que se encuentra en las instalaciones donde se ha cometido el delito, este inventario deberá ser realizado sobre un formulario de registro de evidencia.

En la identificación se deberá tener completo hermetismo en el lugar y cumplir con las normas de seguridad para no contaminar la evidencia.

[7]El uso de guantes especiales puede ser una de las normas de seguridad a seguir así como el fotografiar cada uno de los dispositivos incautados o filmar todo lo que se encuentra en el lugar[16].

Se deberá fotografiar pantallas de quipos, vistas frontales laterales, posteriores del mismo, con el fin de que no se llegara a dudar que el equipo incautado no sea el mismo al final del proceso.

De esta forma se deberá utilizar el mismo proceso para todos los dispositivos que se encuentren en el área, ya sea impresoras, tablets, teléfonos celular, cableado, dispositivos telemáticos, diagramas, etc.

Como parte de la identificación de los objetos de evidencia, es recomendable realizar un bosquejo del lugar donde se ubiquen cada uno de los objetos incautados para posteriormente representarlo en un software de diseño.

Parte de la identificación de los objetos que serán llevados como material probatorio es el de colocar una marca única, es decir se deberá colocar un número, un símbolo, un nombre etc., con el cual este objeto será reconocido dentro de la investigación.

Este proceso garantiza que los objetos recolectados en esta fase sean aceptados como evidencia y de igual forma da certeza de que no hayan sido reemplazados por otro.

[16] Luis Enrique Arellano, "La cadena de Custodia Informático Forense," *ACTIVA*, no. 3, pp. 67-81, 2012

Esta fase de la cadena de custodia es realizada por el personal especializado de la policía o el designado por la autoridad competente, estas personas deberán realizar un informe con los detalles mencionados o llenar un formulario de registro de evidencia con el fin de garantizar que la evidencia es la misma desde que se la recogió hasta su presentación el juicio.

2.4.2 Preservación

La preservación o conservación del objeto incautado es el punto más fuerte dentro de una cadena de custodia, pues este es el encargado de que la evidencia no se contamine y se mantenga intacta, su objetivo es el de asegurar que al final de la investigación el objeto incautado es el mismo.

Una vez identificados los objetos se los deberá clasificar de acuerdo a su forma de almacenamiento, es decir los equipos o dispositivos que tengan una memoria volátil deberán seguir un proceso diferente a los que solamente contengan una memoria de almacenamiento permanente o no volátil.

Esta clasificación se ejecuta ya que en los dispositivos con memoria volátil se debe realizar la preservación de la información en el momento que se recaudan estos objetos, se debe considerar que aquellos objetos que una vez desenchufados pierden información importante, por ejemplo un [17]router, se perdería información de los acceso, [18]logs, etc. que alberga en su memoria [19]RAM, con lo que perderíamos información comprometedora y valiosa.

[17] Router: enrutador o encaminador, (Disponible en: http://es.wikipedia.org/wiki/Router, Consultado: 26-10-2014)
[18] Logs: registro oficial de eventos durante un rango de tiempo en particular. (Disponible en: http://es.wikipedia.org/wiki/Log_%28registro%29, Consultado:26-10-2014)
[19] RAM: Memoria de Acceso Aleatorio.

Para este tipo de dispositivos con memoria volátil, lo primero que se debe realizar es el registro de la fecha, hora y zona horaria del sistema, determinar quién o quienes se encuentran con sesiones abiertas ya sean estas de usuarios locales o remostos.

Así también se debe registrar toda información sobre los archivos, puertos abiertos, aplicaciones con sus respectivos puertos, procesos activos, extraer archivos de configuración relevantes para el sistema operativo.

Examinar la base de datos, extraer registros de eventos, obtener y examinar la información que contiene la memoria RAM, etc.

Por otra parte en el caso de dispositivos que tengan su información en unidades de almacenamiento no volátiles como un disco duro, se podrá aplicar un proceso diferente, ya que estos podrán ser transportados a los laboratorios para poder ser investigados y aplicados diferentes métodos para recolectar evidencia dentro de estos, la clonación puede ser un proceso aplicado a estos dispositivos, sin olvidar las normas de clonación que el Instituto Nacional de Estandarización y Tecnología NIST propone.

[20]Que la herramienta que sea utilizada para la clonación debe crear una imagen bit a bit del disco original o una partición, dicha herramienta debe garantizar que no alterara al disco original, así como la integridad de la imagen creada, para esto se recomienda hacer uso de un bloqueador de escritura preferiblemente de tipo hardware.

Esta herramienta también deberá informar si el espacio será suficiente para la creación de la copia.

Como se puede apreciar la evidencia digital es mucho más versátil que la evidencia física, por lo que se presta para realizarse varios procesos investigativos. La clonación es uno de los procesos más aplicados sobre dispositivos informáticos y

[20] NIST, Instituto Nacional de Estandarización y Tecnología, (Disponible en: http://www.nist.gov/, Consultado: 01-11-2014)

telemáticos, sin embargo no se debe olvidar que estos objetos de prueba o clonados servirán como evidencia de un juicio, por lo que se debe realizar la cadena de custodia sobre estos, ya que los resultados de la investigación estarán vasados en estas copias o clonaciones y el juez no debe dudar de la veracidad de los resultados científicos arrojados por la investigación.

2.4.3 Análisis

El análisis dentro de la cadena de custodia debe ser realizado utilizando métodos y procedimientos científicos comprobados y que principalmente no comprometan al objeto recolectado.

Como recalco a lo largo de este capítulo el cumplimiento de la cadena de custodia es de gran importancia, es así que la correcta elección de los métodos a utilizar tienen el papel principal dentro del análisis, sin olvidar los documentos, formularios o bitácoras que se tendrán que realizar durante este proceso, con el fin de conocer que cambios sufrió o se realizaron en el objeto durante este estudio.

En esta fase se debe tener mucho cuidado al escoger el método de investigación a ser aplicado, buscando siempre que este no comprometa la integridad del objeto, haciendo que la cadena de custodia cumpla con su objetivo.

El análisis debe ser de tipo científico es decir, aplicar el método elegido y de este obtener resultados que posteriormente y si se lo requiere pudieran ser comprobados, con esto quiero decir que un resultado de un análisis no puede ser una sospecha o hipótesis ya que esto no serviría como una prueba o evidencia ante un juez.

Las herramientas a utilizar para el análisis de la evidencia deberán ofrecer el 100% de confiabilidad, y de la misma forma se deberá tener la certeza de que la seguridad implementada en los equipos que se utilizaran para la investigación funcionen

correctamente de esta forma no arriesgaremos la integridad de la evidencia así también no nos expondremos a posibles ataques.

Con el fin de no comprometer la evidencia, se debe tomar en consideración los niveles de volatilidad de las unidades de almacenamiento para decidir si el análisis se realizara en el lugar de la incautación como se expresa en la fase de preservación de la evidencia, esto con el fin de no borrar información comprometedora.

Unidades de Almacenamiento según su nivel de volatilidad.

- Registros y contenidos de la cache.
- Contenidos de Memoria RAM.
- Estado de Conexiones de la red, tablas de rutas.
- Estado de los procesos en ejecución.
- Contenido del sistema de archivos y discos duros.
- Contenido de otros dispositivos de almacenamiento.
- Como tarea inicial básica se recomienda:
- Enumeración de puertos [21]TCP y [22]UDP abiertos así como las aplicaciones que los están utilizando.
- Listar usuarios conectados local y remotamente al sistema.
- Obtener hora y fecha del sistema.
- Enumerar procesos activos, recursos utilizados, con sus respectivas aplicaciones y usuarios.
- Mapear las direcciones IP del sistema así como las direcciones físicas [23]MAC.
- Escanear el sistema con el fin de recolectar ficheros ocultos o borrados.
- Analizar el tráfico de la red.

[21] Puerto TCP, (Disponible en: http://es.wikipedia.org/wiki/Transmission_Control_Protocol, Consultado: 01-11-2014)
[22] Puerto UDP, (Disponible en: http://es.wikipedia.org/wiki/User_Datagram_Protocol, Consultado: 01-11-2014)
[23] Dirección Física MAC, Tras los Pasos de un Hacker, Néstor Marroquín, Pag, 556, (Disponible en: https://books.google.com/books?id=tSdGxtSrlU8C&printsec=frontcover&hl=es#v=onepage&q&f=false, Consultado: 01-11-2014)

Después de haber recolectado los datos preliminares, se debe comenzar a buscar indicios en todos los dispositivos incautados, la verificación de la integridad de los archivos es el primer paso a realizar.

2.4.4 Presentación

La última fase y se podría decir la más importante de la cadena de custodia y dentro de un juicio es la presentación del informe pericial, este informe debe ser conciso y claro, es decir el juez deberá poder entender lo que hemos concluido en base a las resultados obtenidos.

La estructura y la uniformidad de este documento tienen recomendaciones y normas internacionales que pueden servir como directrices para la realización de este documento.

El documento debe tener partes claramente identificables donde se exprese los resultados obtenidos del proceso científico aplicado sobre el objeto investigado, con el fin de que el juez no se pierda al leer el documento, cabe recalcar que la información descrita debe ser entendible para cualquier persona, es decir contener palabras sencillas fáciles de comprender, no utilizar un lenguaje técnico, ya que el juez no tiene por qué saber terminologías informáticas complicadas, si llegase el caso que necesariamente se deba redactar el documento con palabras técnicas, estas deberán ser explicadas en un apartado para que así cualquier persona pueda entenderlas.

La frase “Menos es Más” calza muy bien en esta fase ya que no es necesario realizar un informe extenso y con un lenguaje complicado para presentar los resultado, con un informe bien estructurado y claro es suficiente ya que el juez podrá valorarlo y entenderlo rápidamente agilizando así el proceso de juzgamiento.

Aunque este documento no tiene que ser técnico, si se deberán presentar los informes y bitácoras recolectadas a lo largo de la cadena de custodia, con el fin de que el resultado expuesto tenga un respaldo y la debida documentación técnica, para que en cualquier momento se pudiera comprobar los resultados.

2.5 Software para análisis forense

En la actualidad existe una variedad de software dedicados al estudio forense de imágenes, datos, audio y video, con el fin de aportar en la investigación donde la evidencia fuese digital.

Cabe recalcar que estos softwares deben cumplir con una serie de características para poder ser utilizados, esto debido a los requerimientos que la cadena de custodia obliga a seguir para que la evidencia no fuese contaminada.

La principal características es la preservación de la **confiabilidad** ya que en esta se inmiscuye la integridad, autenticidad y confidencialidad, características que por obligación se deben mantener en una evidencia con el fin de que esta no sea rechazada, o genere algún punto de refutación durante el juicio de la que forme parte.

Entre los softwares que cumplen con las características mencionadas encontramos los siguientes:

- [8]**AMPED FIVE**
  - [24]Amped Five es software privativo, pero que cumple con las características especificadas.
  - Este software es utilizado para el análisis forense de imágenes y videos, permitiendo el uso de varios formatos.
  - La filosofía aplicada en este software se base en filtros, es decir se ingresa el objeto original y de este es extraída una copia con la que se trabaja internamente con el fin de mantener la integridad del objeto original.

  - Entre los análisis que se pueden realizar con este software tenemos:

    - Importación y la conversión de las imágenes
    - Análisis del formato.
    - Aclarar el contenido.
    - Tomar medidas de la escena del crimen.
    - Generar el informe técnico que se llevará a la sala de audiencias.

[24] Software AmpedFive, (Disponible en: http://ampedsoftware.com/es/five, Consultado: 04-11-2014)

- [9]**Live Response**

  - [25]Live Response es un software propietario diseñado para recoger datos volátiles de cualquier dispositivo informático que sea parte de los objetos incautados para la investigación.
  - Este software es de fácil uso ya que se lo instala en una memoria USB por lo que se vuelve muy práctico en el momento de utilizarlo.
  - Al insertar la memoria USB en el dispositivo a ser investigado, presentara un menú de opciones donde se mostrara que tipo de datos se puede recoger.
  - Entre las opciones que ofrece este software encontramos:
    - Memoria física
    - Conexiones de red.
    - Cuentas de Usuario
    - Tareas Planificadas.
    - Capturas de Pantalla
    - Contraseñas
    - Cookies
    - Puertos Abiertos
    - Variables de entorno
    - Historial de Buscadores

- [10]**Steg Secret**

  - [26]Steg Secret es un software de código abierto distribuido bajo licencia GPL, que tiene como objetivo desarrollar y mantener un conjunto de herramientas que permitan realizar Estegoanálisis, con el fin de detectar información oculta en medios digitales como son audio, video y datos.

[25] Más Información, Live Response, (Disponible en: http://www.e-fense.com/live-response.php, Consultado: 05-11-2014)
[26] StegSecret. A simple steganalysis tool. (Disponible en: http://stegsecret.sourceforge.net, Consultado: 05-11-2014)

- Este software es de fácil uso ya que cuenta en su página oficial con un manual de usuario que nos puede servir de apoyo en el momento de su aplicación.
- Steg Secret es un software multiplataforma desarrollado en java, con el cual se puede realizar análisis para la detección de información oculta, estando a la vanguardia con los métodos tradicionales y nuevos de esteganografía, con los que de cierta forma garantizar un análisis profundo ya que se encuentra actualizado en cuanto a métodos de esteganografía.
- Los desarrolladores de este software trabajan "implementando algoritmos para la detección de información oculta con técnicas como son LSB es decir ocultar información en pixeles elegidos de forma secuencial o pseudoaleatoria, ya sea en archivos JPEG, GIF."[27]

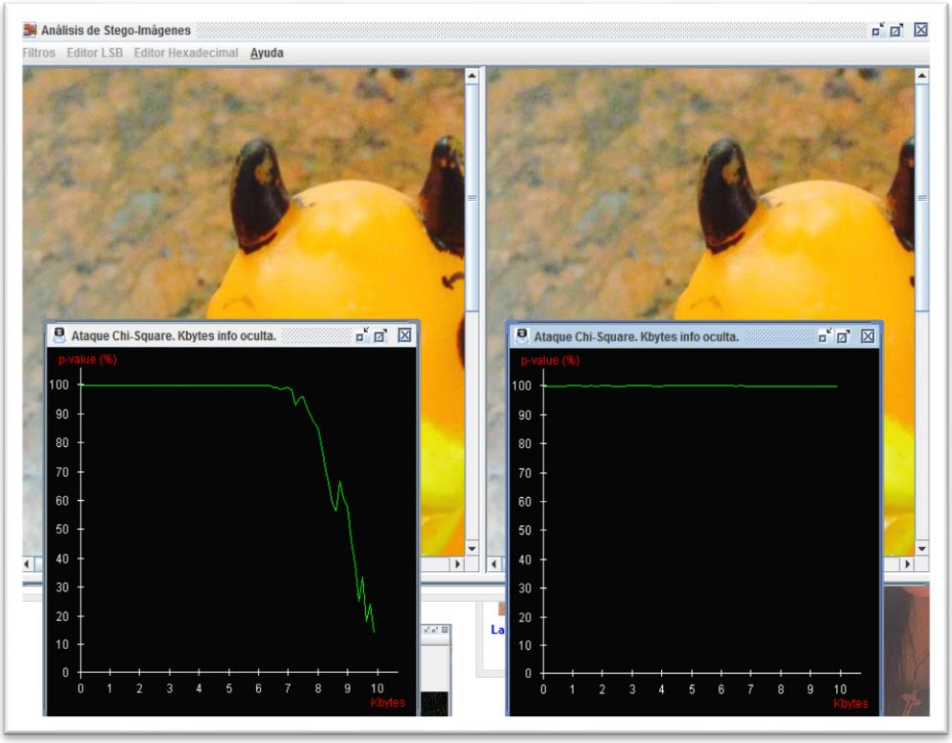


Ilustración 3Captura de Pantalla Software Steg Secret

[27]Alfonso Muñoz. (Disponible en :http://stegsecret.sourceforge.net/indexS.html, Consultado: 05-11-2014)

2.6 Guías y buenas prácticas para la gestión de evidencia digital

En la actualidad existen una gran cantidad de guías y buenas prácticas para la gestión de la evidencia, las mismas que nos ayudaran como referencia para la creación de la metodología.

Estas guías proporcionan directrices para la recopilación, almacenamiento y análisis de la evidencia digital, ya que presentan diferentes fases con las que se deben trabajar durante una investigación forense.

Aunque las guías están planteadas con un esquema legal referente a su país y a criterio de la organización o persona que las desarrolle, apuntan a un solo fin, que es el de presentar resultados ante una corte judicial producto de una análisis netamente científico.

A continuación presento algunas de las guías y buenas prácticas con las que me guiare para el desarrollo de la metodología planteada en esta tesis.

2.6.1 RFC-3227

[28]IOCE, [29]Guidelines for the best practices in the forensic examination of digital technology, 2002.

El RFC 3227 es un documento en el que se presentan directrices para la recolección y almacenamiento de evidencia digital, este documento es de distribución libre por lo que se lo puede descargar de la página oficial de RFC.

Este documento es una guía que presenta diferentes pasos a seguir para una correcta identificación y extracción de la evidencia digital en caso de existir un incidente de seguridad, definido este en el [30]RFC-2828. Cada paso se encuentra debidamente detallado, por lo que es una guía flexible ya que puede ser tomada como referencia para el desarrollo de metodologías ajustadas a los requerimientos de la organización que la necesite.

[28] IOCE, International Organization on Digital Evidence
[29] RFC-3227, (Disponible en: http://www.rfc-base.org/txt/rfc-3227.txt, Consultado: 10-11-2014)
[30] RFC-2828, (Disponible en: http://www.rfc-base.org/txt/rfc-2828.txt, Consultado: 10-11-2014)

El esquema que presenta RFC-3227 es el siguiente:

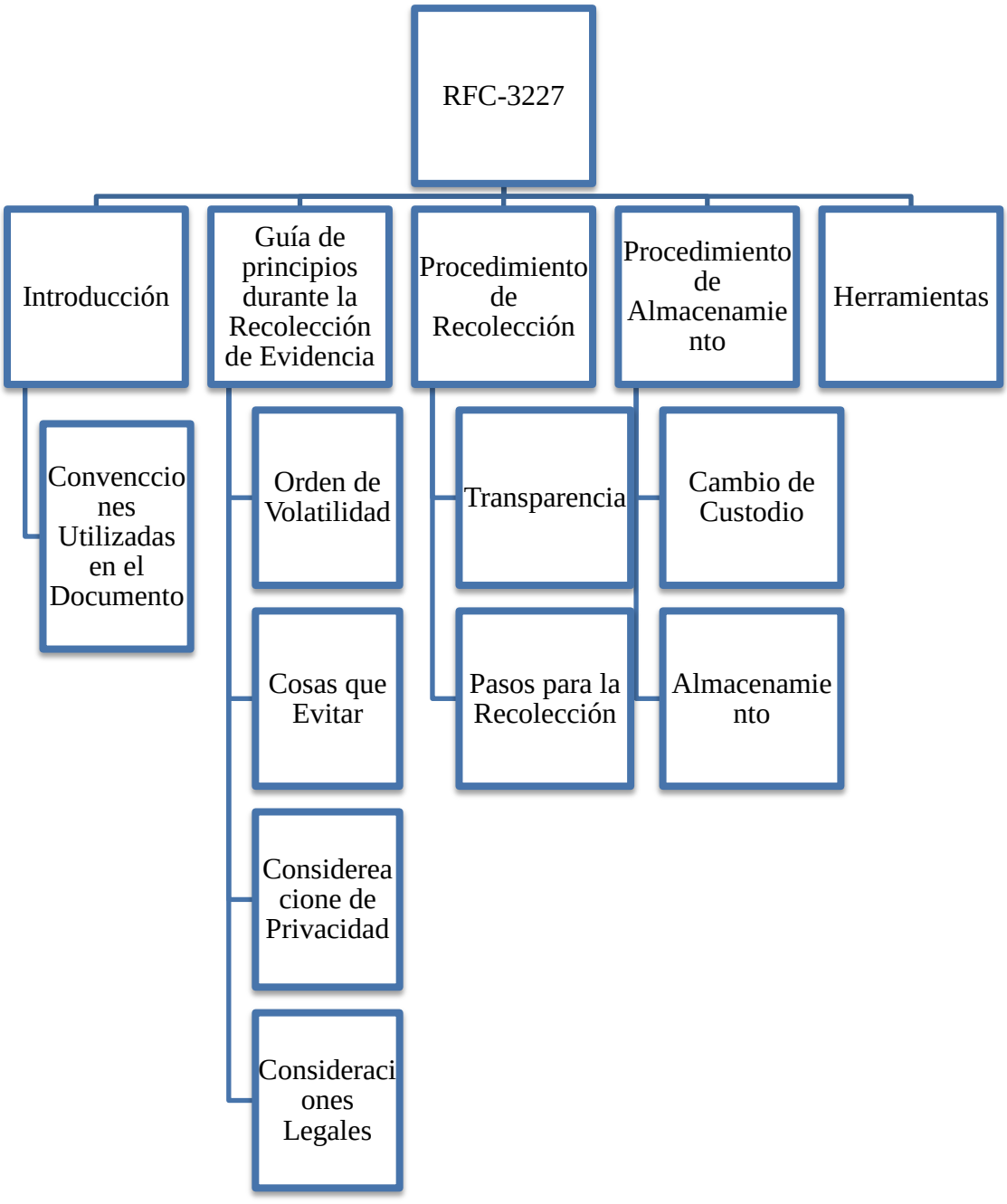


Ilustración 4 Estructura de RFC-3227

Como se puede apreciar en la Ilustración 4 la estructura que presenta esta guía toma temáticas de gran relevancia dentro de una investigación forense, ya que estas forman parte del proceso de análisis forense genérico donde se presentan 4 fases básicas como son Identificación, Preservación, Análisis y Presentación de la evidencia digital.

La correcta aplicación de esta estructura dentro de las fases ayudara para que se pueda recolectar la mayor cantidad posible de evidencia y así tener posibilidades bien altas de ser aceptadas en una corte judicial.

Desarrollo de la Estructura de RFC-3227

- Introducción

El RFC-3227 en su primer capítulo define el propósito para el cual ha sido creado y la temática que tratara a lo largo del documento siendo esta una respuesta a un incidente de seguridad el mismo que se encuentra definido en el RFC-2828.

El RFC-2828 define como **"Incidente de Seguridad"** a un evento relevante del sistema en el que las políticas de seguridad fueron omitidas o incumplidas.

Partiendo de esta definición el documento toma forma para definir cuáles serán las acciones a tomar en caso de que ocurra dicho incidente informático.

Cabe destacar que el documento es solamente una guía donde las diferentes expresiones como debe, puede, no debe, conviene entre otras deben ser interpretadas como se las define en el [31]RFC-2119.

- Guía de principios para la Recolección de Evidencia

Este capítulo detalla los pasos a seguir antes de la recolección de la evidencia digital, entre los más generales y los que en toda investigación forense se deberían realizar son:

- Cumplir con las políticas de seguridad de la organización o empresa.
- Realizar una copia bit a bit de unidades de almacenamiento

[31] RFC-2119, (Disponible en: http://www.rfc-es.org/rfc/rfc2119-es.txt, Consultado: 10-11-2014)

- Realizar notas detalladas, sobre información relevante para el caso, las mismas que deberán ser firmadas.
- Verificar el reloj.
- Procurar mantener la integridad de la evidencia recogida.
- Recolectar información de los dispositivos más volátiles hasta los menos volátiles.

Para realizar correctamente los pasos anteriores el documento sugiere crear o clasificar la información de acuerdo a su nivel de volatilidad, es decir realizar una lista de los medios de almacenamiento desde el más volátil al menos volátil.

De igual forma propone no realizar ninguna acción con la que podamos perder información valiosa, como por ejemplo apagar el equipo, modificar tiempos de acceso, utilizar softwares que se encuentren sobre el sistema operativo sospechoso.

Por otro lado la privacidad es otro tema que aborda este capítulo el mismo que sugiere, apegarse siempre a las normas y reglas que la empresa tiene para administrar la privacidad sobre sus dispositivos, información y personal. La recolección de la evidencia debe realizarse de una manera profesional es decir no se debe inmiscuir en la vida privada de las persona o tratar de recolectar información que no tiene por qué ser recogida.

Como último paso previo a la recolección de la información el documento presenta las consideraciones legales a ser atendidas como son la admisibilidad, autenticidad, fiabilidad, credibilidad y parcialidad.

- Procedimiento de Recolección de Evidencia

El procedimiento para la recolección de la evidencia digital, debe ser concreta, es decir debe tener las acciones a realizar bien definidas con el fin de minimizar las decisiones en el momento de la recolección.

Los métodos a utilizar para la extracción de la evidencia deben ser métodos probados por expertos.

Los pasos para la recolección de la evidencia son:

- Realizar una lista de los sistemas sospechosos y de los que se procederá a extraer la evidencia.
- Realizar una lista de volatilidad para cada sistema.
- Verificar y anotar el grado de sincronización del reloj del sistema.
- Documentar cada acción realizada
- Detallar por escrito la información de las personas inmiscuidas en el incidente.
- Utilizar medios para proteger la integridad y la seguridad de la evidencia recolectada, estas pueden ser la generación de sumas de comprobación y firmas criptográficas.

- Procedimiento de almacenamiento de evidencia

Para el almacenamiento de la evidencia el documento recalca el cumplimento de la cadena de custodia, estando está claramente documentada para que en un futuro no existan dudas.

Dentro de la documentación de la cadena de custodia se debe detallar con claridad cómo se encontró la evidencia, y que procedimientos se realizó sobre ella. Donde cuándo y por quien fue descubierta, recogida, manipulada o examinada.

Los nombres de los custodios y tiempo que permaneció con la evidencia también deberán constar en el documento de la cadena de custodia.

Una vez almacenada la evidencia esta deberá ser restringida es decir, crear niveles de acceso para que no exista una violación a la integridad.

- Herramientas

Las herramientas a utilizar para la recolección y almacenamiento de la información deben ser herramientas que no realicen cambios en los registros del sistema, no necesiten de librerías externas y que puedan ser ejecutadas desde medios de solo lectura como son CD, USB, Disco Duros externos.

2.6.2 Examinación Forense de la Evidencia Digital – Una guía Para la Aplicación de la Ley (Forensic Examination of Digital Evidence - A Guide for Law Enforcement - NIJ)

Otra de las Guías y buenas prácticas en la que presenta el Instituto Nacional de Justicia de EEUU ([32]NIJ) en su reporte especial de Abrir 04 titulado [33]**"Forensic Examination of Digital Evidence - A Guide for Law Enforcement"**.

Este documento fue desarrollado en conjunto por el Instituto Nacional de Justicia de EEUU, Instituto Nacional de Estándares y Tecnología ([34]NIST) y la Oficina de Normas y Aplicación de la Ley con el fin de proveer una guía para la elaboración de una propia metodología o procedimiento para el análisis de evidencia digital.

Las características principales que rescata este documento para la investigación forense son:

- Uso herramientas que no alteren la integridad de la evidencia digital recogida.
- Las personas que realizan la investigación forense deben tener un perfil profesional apegado a las acciones que se van a realizar es decir deberán estar debidamente capacitado para las labores que involucra una investigación forense.
- Las fases de incautación "identificación y extracción", almacenamiento "extracción y preservación", documentación y cambios de custodios, deben ser documentadas y preservada para una posterior revisión.

[32] National Institute of Justice, (Disponible en: http://www.nij.gov/Pages/welcome.aspx, Consultado: 10-11-2014)
[33] Forensic Examination of Digital Evidence, (Disponible en: www.ncjrs.gov/pdffiles1/nij/199408.pdf, Consultado: 10-11-2014)
[34]National Institute of Standards and Tecjnology,(Disponible en: www.nist.gov, Consultado: 10-11-2014)

Este documento se maneja mediante 5 temas o fases, las mismas que deberán seguir el orden sugerido para realizar una correcta investigación.

- Desarrollo de políticas y procedimientos
- Valoración de la evidencia
- Adquisición de la Evidencia
- Análisis de la Evidencia
- Documentación y Reportes

Estos son los 5 temas o fases con los que trabaja esta guía y los que nos servirán como directrices para la creación de la metodología en el siguiente capítulo.

Desarrollo de los temas expuestos en el reporte especial "Examinación Forense de la Evidencia Digital"

- Desarrollo de políticas y procedimientos

En esta fase el documento proporciona información de cómo deberá ser el proceso de investigación, que características debe cumplir, como por ejemplo sugiere que los procedimientos que se desarrollen deben ser probados con anterioridad.

De igual forma presenta un perfil para el personal forense con el que se trabajara durante una investigación, ya que estos deberán estar debidamente capacitados para realizar las actividades que se les asigne.

Otra de las características es el de utilizar herramientas (hardware y software) con su respectivas licencias si se habla de herramientas comerciales.

- Valoración de la evidencia

En esta fase se deberá realizar una búsqueda de todo aquello que pueda utilizarse como evidencia, analizar cada uno de los procesos a realizarse para la búsqueda de la evidencia, mantener presente la posibilidad de obtener evidencia digital adicional

como puede ser el de un proveedor de internet ([35]ISP), es decir evaluar si se necesita información de una entidad externa.

Entre la evidencia potencial en un caso informático pueden ser fotografías, videos, hojas de cálculo, bases de datos, cuentas de correo electrónico, configuración y usuarios de la red, etc.

Entre las actividades que recomienda realizar a primera instancia se encuentran:

- Identificación y Numero de Equipos
- Verificar si existe una red
- Entrevistas al personal
- Identificar y documentar medios de almacenamiento externos e internos.
- Identificar áreas de almacenamiento remotos.
- Identificar el software.

Para trabajar bajo el marco legal, los peritos deben asegurarse de que la solicitud para la investigación es la correcta es decir que tenga un sustento legal y científico.

- Adquisición de la Evidencia

Para la adquisición de la evidencia este documento presenta ciertos pasos a realizar para evitar contaminar o en el peor de los caso eliminar la evidencia.

- Utilizar hardware y software limpio por parte del perito forense.
- Protegerse físicamente es decir protegerse de la electricidad estática y campos magnéticos en el momento de analizar el hardware.
- Identificar dispositivos del almacenamiento.
- Capturar información e la BIOS mediante un arranque controlado.
- Registrar horas y fichas del sistema.

[35] ISP, Proveedor de Servicios de Internet, (Disponible en: http://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet, Consultado: 10-11-2014)

- Utilizar discos de análisis forense
- Utilizar dispositivos de protección para solo lectura
- Utilizar protección de escritura.
- Realizar copias bit a bit de medios de almacenamiento

- Análisis de la Evidencia

En esta fase se trabaja la extracción y el análisis de la evidencia digital recolectada en el paso anterior. Con **Extracción** quiere decir la recuperación de datos de los medios de almacenamiento no volátiles y que han sido transportados al laboratorio de investigación, mientras que el **Análisis** se refiere a la interpretación de los datos recuperados es decir responder a las preguntas como llego ahí, de donde viene, que significa, que propósito tenía.

Para el análisis de la evidencia el documento sugiere realizarlo sobre una copia de la evidencia ya que así preservaremos la integridad de la evidencia original.

Los pasos generales para el análisis son los siguientes:

- Preparación
- Extracción
- Análisis y Extracción de datos
- Conclusiones

- Documentación y Reportes

Para la documentación la guía propone realizarlo de una forma completa y precisa, es decir expresar los resultados deben ser completos, detallar todos los resultados obtenidos en cada fase. El investigador no debe olvidar que la documentación se la realiza durante toda la investigación.

Características generales para una correcta documentación:

- Mantener la solicitud inicial para la investigación.
- Tomar notas detalladas de cada acción realizada.
- Mantener una copia de la documentación de la cadena de custodia.
- Detallar las irregularidades encontradas en los documentos.
- Adjuntar topologías de red si existen.
- Documentación sobre las características de dispositivos y softwares.
- Detalle de resultados obtenidos en cada proceso.

CAPITULO III. METODOLOGÍA PARA EL ANÁLISIS FORENSE DE UNA IMAGEN Y DATOS

El presente capitulo desarrollara la metodología propuesta donde se presentaran diferentes herramientas a ser utilizadas para el correspondiente análisis estenográfico, y paralelamente se presenta diferentes formularios creados con el fin de mantener la cadena de custodia, la cual es el pilar fundamental en un análisis forense, ya que esta será la que avale la investigación y la presente como prueba con gran relevancia en una corte judicial.

Esta metodología utiliza como base para su desarrollo las guías y buenas prácticas **"RFC-3227"** y **"Examinación Forense de la Evidencia Digital (NIJ)"** debido a que estas implementan de mejor manera el proceso genero para un correcto análisis forense, es decir cada una de las fases presentadas en la metodología a desarrollar se ajusta a la perfección a las recomendaciones y directrices que sugieren las guías mencionadas.

El alcance de esta metodología es el de proporcionar diferentes fases para el análisis forense cada una con su respectivo objetivo y las herramientas con las que se pueden trabajar para alcanzar dicho objetivo.

A continuación se presenta un diagrama de procesos donde se expresa brevemente la metodología a ser desarrollada.

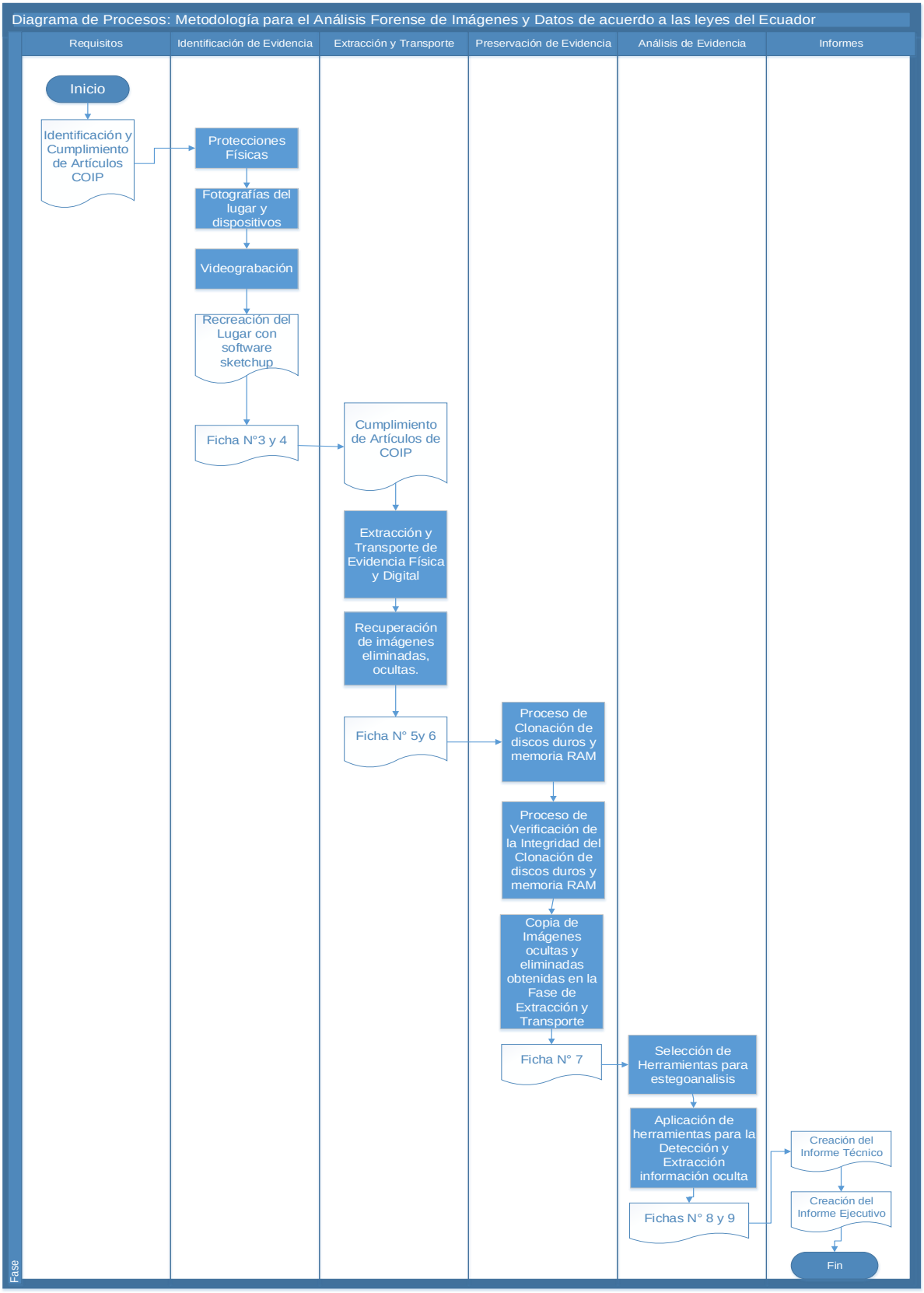


Ilustración 5 Metodología para el análisis forense de imágenes y datos de acuerdo a las leyes del Ecuador

La presentación de documentos que avalen el correcto cumplimiento de la cadena de custodia durante la investigación hace que los resultados científicos obtenidos sean pruebas altamente valiosas dentro de un caso en la corte judicial, es por esto que se ha desarrollado una serie de fichas para que al final de la investigación sean presentadas como una forma de demostrar que la cadena de custodia se ha cumplido a cabalidad ya que estas contendrán información de los custodios, así como horas y fechas de entrega, cambios realizados y herramientas por los que ha pasado la evidencia

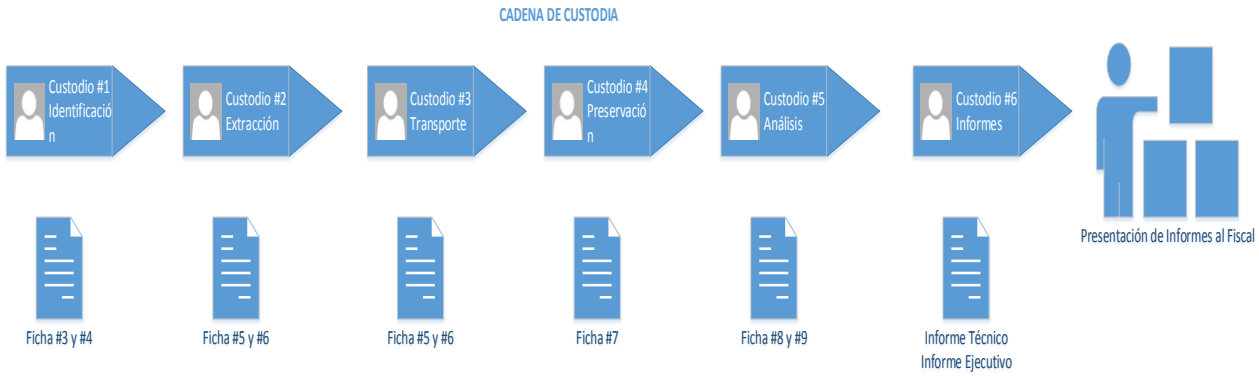


Ilustración 6 Cadena de Custodia (Fichas)

3.1 Definir los requisitos para comenzar un análisis forense.

Este es el punto de partida para realizar un análisis informático forense sobre datos e imágenes.

Los peritos forenses deberán recibir una solicitud de investigación y deberán realizar el estudio científico bajo la dirección de la Fiscalía y administrativamente bajo el mando del ministerio de telecomunicaciones.

Estos peritos forenses deberán tener el perfil que el artículo 511 del [36]COIP proporciona, para poder realizar una investigación forense.

[36] COIP.(Disponible en: http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf, Consultado: 12-11-2014)

El análisis forense debe ser realizado bajo el Código Orgánico Integral Judicial, por lo que los expertos forenses certificados por la fiscalía se deberán acoger a los diferentes artículos que se expresan en este código.

Como primer artículo a ser aplicado esta el 481 el cual se refiere a los parámetros que deberá tener una orden de allanamiento para que pueda comenzar la investigación.

El siguiente artículo es el 482 donde explica las reglas a seguir en un allanamiento.
El articulo 478 en su primer y segundo literal donde se expresan las pautas para el registro o incautación de los elementos a ser investigados.

De acuerdo a este articulo para comenzar con la identificación y siguientes pasos de esta metodología se deberá tener el consentimiento de la persona afectada o la investigada, de no ser el caso se deberá tener una orden judicial con la que podamos aplicar la metodología.

De esta misma forma se debe cumplir con el articulo 480 donde nos expresa en qué casos se debe realizar un allanamiento.

Para cumplir con el artículo 456 del [37]COIP referente a la importancia de cumplir con la cadena de custodia durante el análisis forense, procedemos a crear una ficha donde se expresen los nombres de cada uno de los peritos forenses en cada una de las etapas de investigación, y de la misma forma procedemos a llenar un formulario con su información personal, estas fichas o formularios son llenados con el fin de saber qué persona tubo en su custodia la evidencia, que acciones realizo sobre ella y que resultados obtuvo, de esta forma no tendremos discrepancias o dudas durante el proceso de investigación.

El formulario o ficha donde se detallaran los nombres de los peritos forenses a cargo de las diferentes etapas del análisis se encuentra en el **Anexo A Ficha N° 1,** este

[37] COIP.(Disponible en: http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf, Consultado: 12-11-2014)

formulario debe ser llenado con rigurosidad ya que no podrán variar las personas involucradas en la investigación, este proceder apoya a que los resultados obtenidos de la investigación tengan un gran peso como prueba en la corte.

De la misma forma la ficha de datos personales de los peritos forense se encuentra en el **Anexo A Ficha N° 2**, esta ficha contendrá toda la información de las personas inmiscuidas en el proceso de investigación, de esta forma se podrá corroborar que no tienen ningún tipo de nexo con las personas procesadas o las empresas que se encuentran dentro del caso.

La aplicación adecuada de cada uno de los artículos del COIP a lo largo de esta metodología apoyara para que no exista discrepancia cuando se juzgue el caso o dentro del proceso jurídico.

Una vez verificados que estos requisitos se hayan cumplido, procedemos a iniciar el análisis forense sobre la evidencia incautada, específicamente sobre imágenes y datos (texto plano).

3.2 Identificación de evidencia (imágenes, datos) a ser analizados.

En esta fase de la metodología para el análisis forense se debe trabajar bajo el articulo 478 con el cual tendremos el consentimiento de las partes para la identificación de los objetos o a su vez tendremos una orden judicial con la que legalmente podremos comenzar con la identificación de los objetos que serán investigados siendo estos dispositivos informáticos y telemáticos y a su vez toda la información contenida en los mismos.

Una vez lista la parte legal procedemos a la identificación de los objetos, manteniendo la cadena de custodia que hemos venido estudiando.

PASOS A REALIZAR PARA LA IDENTIFICACIÓN DE LA EVIDENCIA

- Tomar las debidas protecciones físicas.
- Fotografiar dispositivos, y escena del delito.
- Video grabar toda la escena del delito.
- Realizar una reconstrucción grafica de la escena del delito, incluyendo dispositivos, inmuebles existentes.
- Llenar la ficha para la identificación de la evidencia (Ficha N° 3,4).

3.2.1 Protecciones Físicas

Como primer paso para la identificación tendremos las protecciones físicas adecuadas, siendo estas:

- Preservar la escena del delito, esta paso se deba llevar acabo de acuerdo a lo que dicta el artículo 458 de COIP donde detalla quien tendrá la responsabilidad de preservar la escena del delito.
- La o el servidor público o persona natural deberá cerrar el paso a cualquier persona hasta que llegue el personal especializado y que conste en la nómina de peritos forense establecida anteriormente.
- [38]Manillas antiestáticas para evitar cualquier descarga y dañar la evidencia.
- Guantes quirúrgicos, en el caso de poder llevar el o los dispositivos al laboratorio y así no contaminarlo con nuestras huellas.
- Etiquetar con un número único a cada uno de los dispositivos incautados.

  Las etiquetas que se asignaran a cada dispositivo e imágenes deberán tener el siguiente formato.

  - **Etiqueta para Dispositivos:**

    (Numero)Dis(Tipo Dispositivo)

    Ejemplo: 01DisRouter

  - **Etiqueta para Imagines:**

    (Numero)Img(Extensión)

[38] Manilla Antiestática, (Disponible en: http://es.wikipedia.org/wiki/Brazalete_antiest%C3%A1tico, Consultado: 12-11-2014)

Ejemplo: 01ImgJPG

- **Etiqueta para Archivos (Texto Plano):**

  (Numero)Txt(Extensión)

  Ejemplo: 01TxtDocx

3.2.2 Fotografiar la Escena del Delito junto con los dispositivos físicos encontrados

El segundo paso de esta fase es el **tomar fotografías** de cada uno de los dispositivos encontrados donde se sospecha se cometió el delito.

Esto es de gran importancia pues es un respaldo visual del estado y lugar donde se encontraron los dispositivos incautados y que serán presentados como evidencia.

Este material apoya la investigación pues existen varios casos en donde no se puede retirar los dispositivos del lugar donde se encuentra y por este motivo las fotografías ayudan a confirmar diferentes indicios que arroje la investigación.

Dentro de las fichas que posteriormente se presentan, existe un campo donde se deberá adjuntar las fotografías tomadas.

3.2.3 Videograbación

Se deberá video grabar todo el lugar del delito pues esto nos ayudara para que posteriormente se pueda recrear gráficamente el lugar del delito, y de igual forma se puedan ubicar los dispositivos que se encontraron en dicho lugar.

3.2.4 Recreación grafica de la escena del delito junto con los dispositivos encontrados.

Ayudándonos del video que se realizó en el paso anterior, procedemos a recrear la escena del delito con el software [11]SketchUp.

[39]SketchUp es un programa de diseño gráfico en 3D que nos ayuda a realizar fácilmente estructuras físicas como oficinas, edificios, casas etc., y de igual forma nos ayuda con el diseño de interiores, que en este caso nos facilitara la ubicación de los dispositivos encontrados en la escena del delito.

[39] SketchUp, (Disponible en: http://www.sketchup.com/es, Consultado: 12-11-2014)

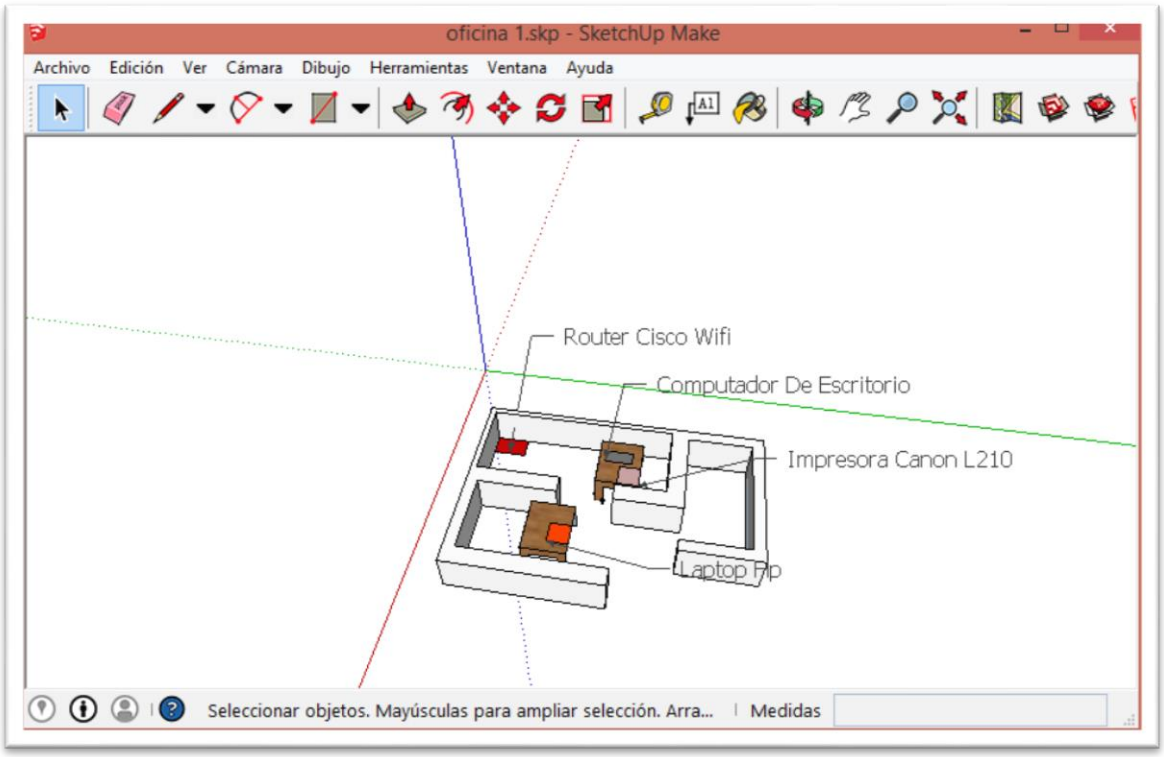


Ilustración 7 Captura de Programa SketchUp

3.2.5 Ficha de Registro de Evidencia

Se deberá llenara los formulario de registro de la evidencia, los cuales contendrá diferentes ítems con los que se identificara cada uno de los objetos que fueron utilizados para cometer un delito.

Cabe destacar que se dispondrá de diferentes formularios ya que como se explicó en el capítulo anterior, como parte de la evidencia se incautarán diferentes tipos de dispositivos y la información (datos, imágenes) que contengan estos que en adelante se la denominara **evidencia digital**.

El formulario para el registro de los objetos físicos ya sean estos dispositivos informáticos y telemáticos se encuentra en el **Anexo A Ficha N° 3,** donde se especifican características de los dispositivos y se deberán adjuntar las fotografías tomadas en el paso anterior. Se debe tener precaución con el número o etiqueta que se asigne a cada dispositivo pues este deberá ser único y es con el que se trabajara a lo largo de la investigación.

El formulario de registro para evidencia digital ya sean archivos, imágenes se encuentran en el **Anexo A Ficha N° 4** de igual forma q el anterior el número de registro deberá ser único**.**

La mayoría de las características que se requieren llenar en este formulario las encontraremos en la opción propiedades de cada archivo o imagen.

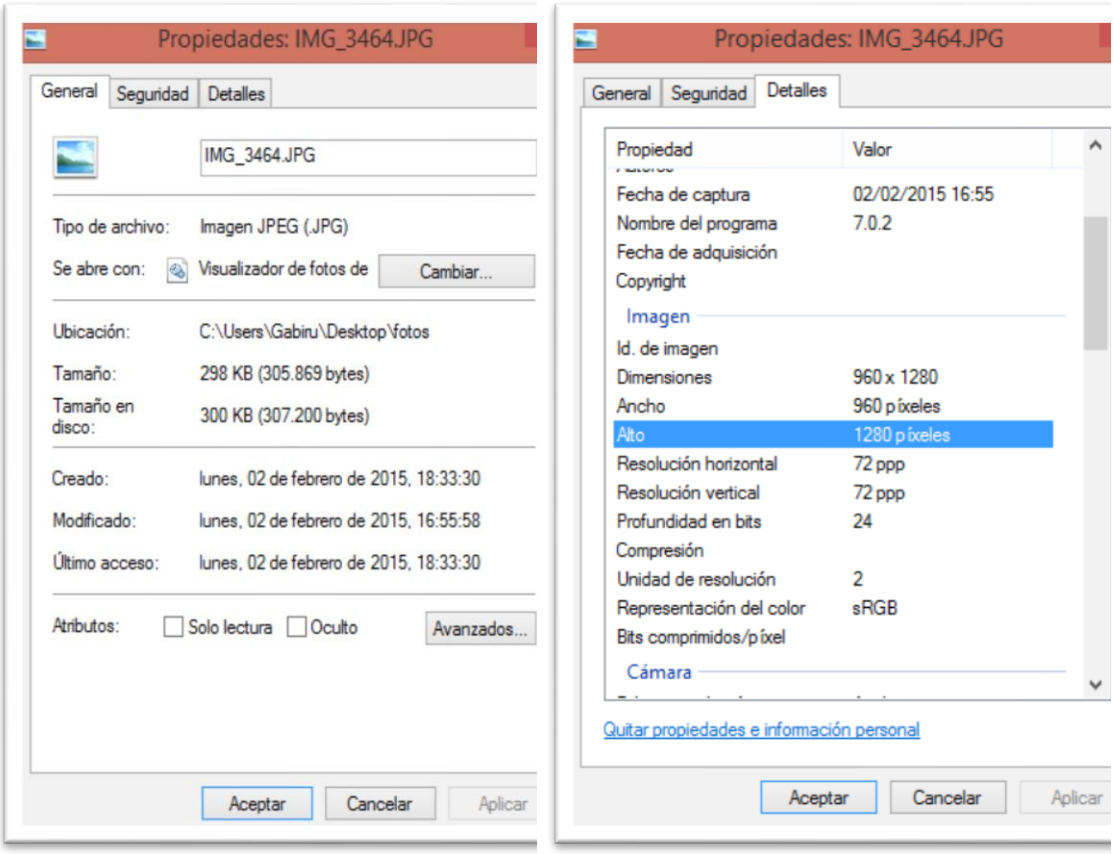


Ilustración 8 Características de Imágenes

La recolección de información sobre las evidencias es de gran importancia y debemos procurar mantener la integridad tanto de los dispositivos y evidencia digitar recolectada, no hay que olvidar mantener la cadena de custodia, es decir cumplir con los cuidados para que la evidencia no se contamine, conocer a la perfección las técnicas que se aplican para que estas no hagan cambios en la evidencia.

3.3 Extracción y transporte de la evidencia (imagen, datos) a ser analizados.

Ya habiendo sido registrados los objetos (dispositivos) y evidencia digital, se deberá seguir con el proceso de extracción y transporte de la evidencia sin olvidar mantener la cadena de custodia.

Para actuar dentro del Organismo Judicial se deberá aplicar nuevamente el artículo 478 y 482 en su 3 literal sin olvidar el referente a la cadena de custodia que se encuentra en el artículo 456.
En esta fase de la metodología se debe tomar mayor atención al artículo 500 que detalla cual es el procedimiento forense para la evidencia digital.

La elección de las herramientas a ser utilizadas en esta fase debe ser muy cuidadosa ya que debemos mantener la cadena de custodia intacta es decir que se debe asegurar la integridad de la evidencia cuando se está realizando la extracción y transporte de los dispositivos y evidencia digital.

La primera instancia en la fase de Extracción y Transporte de Dispositivos es la de diferenciar si los dispositivos físicos van a poder ser removidos y trasladados al laboratorio de investigación o de lo contrario no pueden ser reemplazados, con lo que podremos tomar las medidas necesarias para la extracción.

PASOS A REALIZAR EN LA FASE DE EXTRACCIÓN Y TRANSPORTE DE EVIDENCIA DIGITAL Y FÍSICA

- Diferenciar cuales son los dispositivos físicos que pueden ser trasladados al laboratorio de investigación y cuáles no.
- Para los dispositivos físicos que no pueden ser trasladados se realizan las siguientes tareas.
    - Volcado de Memoria RAM
    - Clonación bit a bit de disco duro
    - Extracción de Imágenes, Video y Datos ocultos y borrados
- Para los dispositivos que si pueden ser trasladados se realizan las siguientes tareas.

- Volcado de Memoria RAM
- Verificación del Volcado de Memoria RAM

- Llenar la ficha para la extracción y transporte de la evidencia, (Ficha N°5,6).

3.3.1 Extracción y Transporte de Dispositivos Físicos

Dispositivos Físicos que no pueden ser trasladados al laboratorio de investigación.

Para la extracción de dispositivos físicos como CPUs, [40]routers, [41]switch, etc., debemos tomar en cuenta si estos se los puede llevar al laboratorio de investigación ya que pueden ser dispositivos irremplazables en el funcionamiento de una empresa, de ser este el caso entonces debemos utilizar herramientas con las que podamos realizar una copia exacta de la información contenida hasta ese momento, sin alterar la evidencia para mantener los objetivos de la cadena de custodia.

Los pasos a realizar en este caso son los siguientes:

- Volcado de Memoria RAM
- [42]Clonación bit a bit del disco duro.
- Extracción de Imágenes, Video y Datos ocultos y borrados.

Dispositivos Físicos que pueden ser trasladados al laboratorio de investigación.

Por otro lado si es posible llevar los dispositivos al laboratorio entonces debemos recolectar la información volátil que contenga dichos dispositivos antes de apagarlos ya que si lo hacemos estaremos perdiendo información que podría ser clave para la investigación es decir realizar un volcado de memoria en vivo.

[40] Router, Enrutador o Encaminador, (Disponible en: http://es.wikipedia.org/wiki/Router, Consultado: 13-11-2014)

[41] Switch, Un conmutador o switch es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI, (Disponible en: http://es.wikipedia.org/wiki/Conmutador_(dispositivo_de_red), Consultado: 13-11-2014)

[42] Más Información de Clonación de Disco Duro, (Disponible en: http://es.wikipedia.org/wiki/Clonaci%C3%B3n_de_discos, Consultado: 13-11-2014)

Para la extracción de la información o datos volátiles no se debe utilizar herramientas que tengan que ser instaladas en el Sistema Operativo anfitrión ya que el atacante pudo haber dejado una secuencia de órdenes que nos podrían devolver respuestas erróneas, es por esto que se recomienda que las herramientas a ser utilizadas vengan instaladas en un medio de solo lectura como puede ser un CD-ROM, y de igual forma el almacenamiento de la información extraída deberá ser realizada sobre un medio que esté completamente vacío y formateado como puede ser un USB, disco duro externo o en su defecto una ordenador portátil que se encuentre en red, con esto cumplimos con los objetivos de la cadena de custodia ya que no estaríamos violando la integridad del dispositivo y su información.

Con este escenario los pasos a ser realizados son:

- Volcado de Memoria RAM
- Verificación del Volcado de Memoria RAM

Una vez realizados los pasos anteriores procedemos a pagar el dispositivo y se deberá llenar el formulario que se encuentra en el **Anexo A Ficha N° 5.**

3.3.2 Extracción de Evidencia Digital (Imágenes y Datos (Texto Plano))

Volcado de Memoria RAM

[12]Se conoce como volcado de memoria RAM al proceso de copiado de la Memoria Volátil (RAM), el cual nos devolverá información sobre procesos en ejecución, procesos en fase de terminación, conexiones activas ya sean estas TCP, UDP, Drivers, Ejecutables, Ficheros, Objetos en Cache como direcciones Web, password, comandos utilizados en consola, elementos ocultos, etc.

Se puede realizar un volcado de Memoria mediante diferentes softwares, entre los más comunes encontré:

- LiveKD
- **[43]EnCase Forensic**
- **[44]AccessData FTK Imager**

[43]EnCase Forensic, (Disponible en: https://www.guidancesoftware.com/, Consultado: 12-11-2014)

Para esta metodología recomiendo utilizar [13]**AccessData FTK Imager** desarrollado por la empresa AccessData en su versión 3.3.0.5, esta herramienta forense permite realizar un volcado de memoria RAM, con lo que podremos recuperar usuarios y contraseñas, sitios web, etc., para luego ser analizadas de una forma hexadecimal.

Este software debe ser instalado sobre un medio externo, evitando el uso del sistema operativo cuestionado. Como se podrá apreciar en la captura de pantalla de este software, cumple con el requisito del almacenamiento en un medio externo, limpio y con el espacio suficiente para realizar el volcado, ya que nos da la opción de elegir donde guardaremos el volcado realizado.

Como parte de la seguridad que provee este software, presenta un hash ya sea MD5 o has1, con el cual más adelante podremos comprobar la integridad del volcado de memoria RAM que hemos realizado.

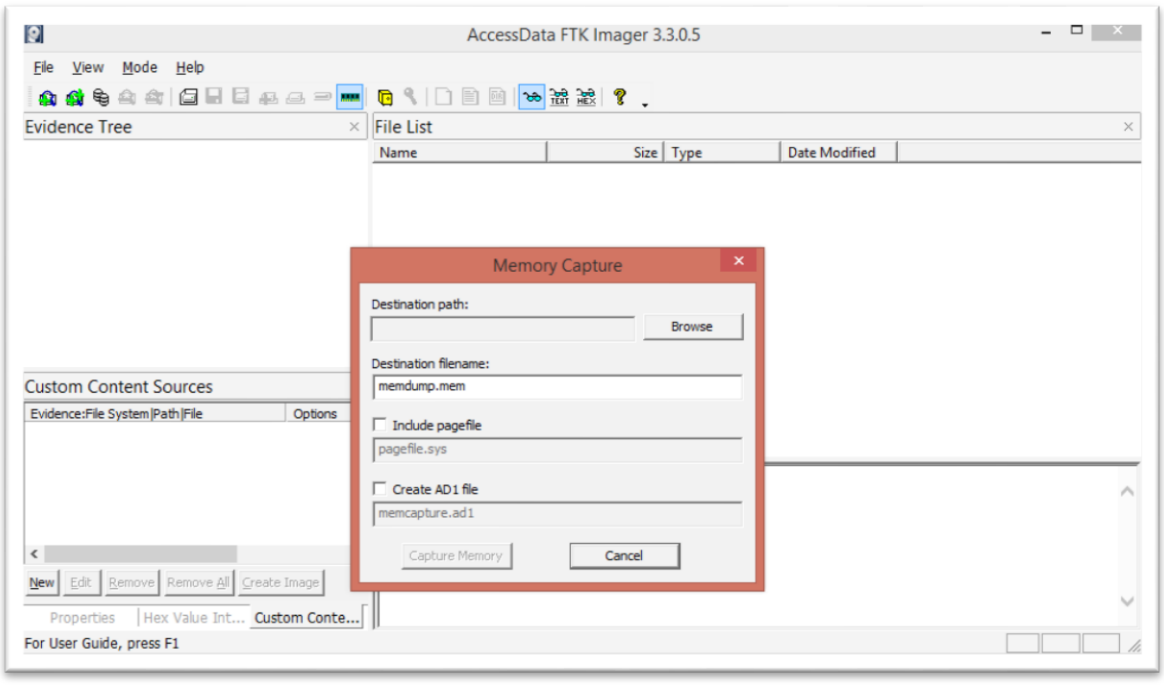


Ilustración 9 Captura de pantalla de Software Access Data FTK Image 3.3.0.5

[44]AccessDataFTKImager☹Disponible en:http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.3.0, Consultado: 14-11-2014)

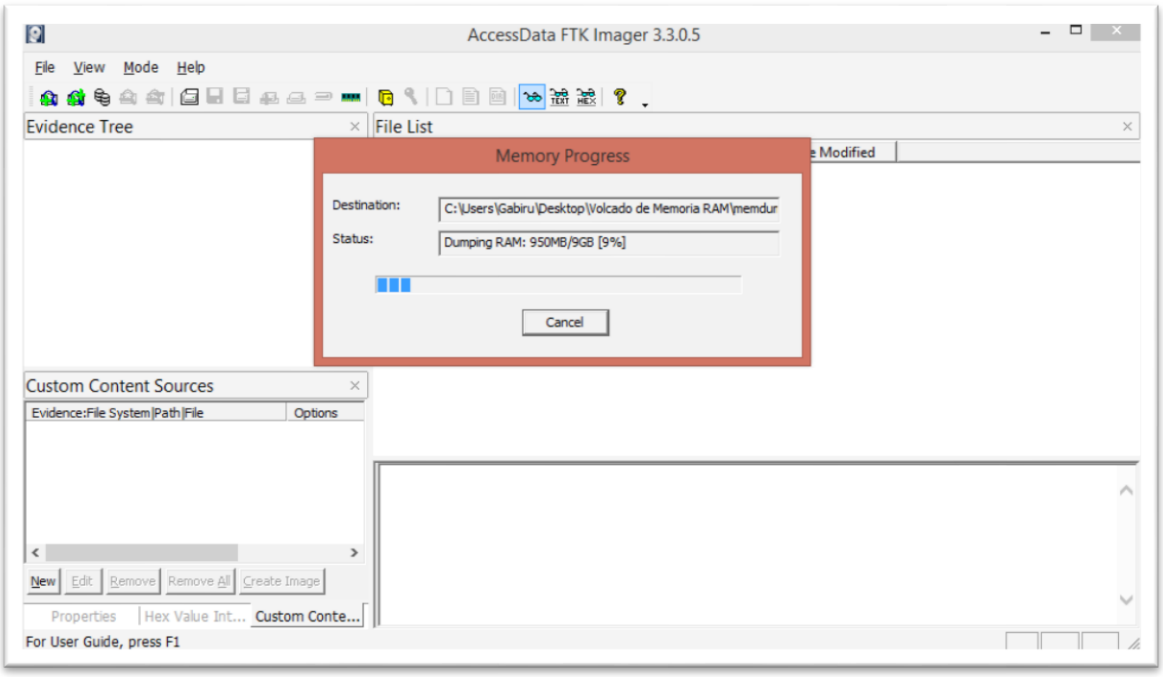


Ilustración 10 Captura de Pantalla del Proceso de Volcado de Memoria RAM

Verificación de la integridad del volcado de memoria

Este es uno de los pasos importantes luego de realizar una copia de los medios de almacenamiento de los dispositivos incautados, pues como se viene explicando a lo largo de esta tesis, la integridad es la característica principal de la cadena de custodia.

Existen varias herramientas con la que se puede realizar la verificación de la integridad, como es el software [45]**AccessData FTK Imager** que se utilizó en el paso anterior para el volcado de memoria RAM.

Md5Summer

[14]**Md5summer** es un software que nos permitirá realizar la verificación de la integridad del volcado de memoria realizado, este software tiene un ambiente gráfico, fácil de utilizar. [46]**Md5summer** es un software de código abierto y gratuito, distribuido bajo licencia GPL y desarrollado en Borland Delphi 7.

[45] AccessData. AccessData. (Disponible en: http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.3.0, Consultado: 14-11-2014)
[46] Luke Pascoe. MD5Summer. (Disponible en: http://www.md5summer.org/about.html, Consultado: 14-11-2014)

Md5summer devolverá un hash md5 o sha1 dependiendo de nuestra elección con el cual posteriormente se podrá realizar una verificación de la integridad.

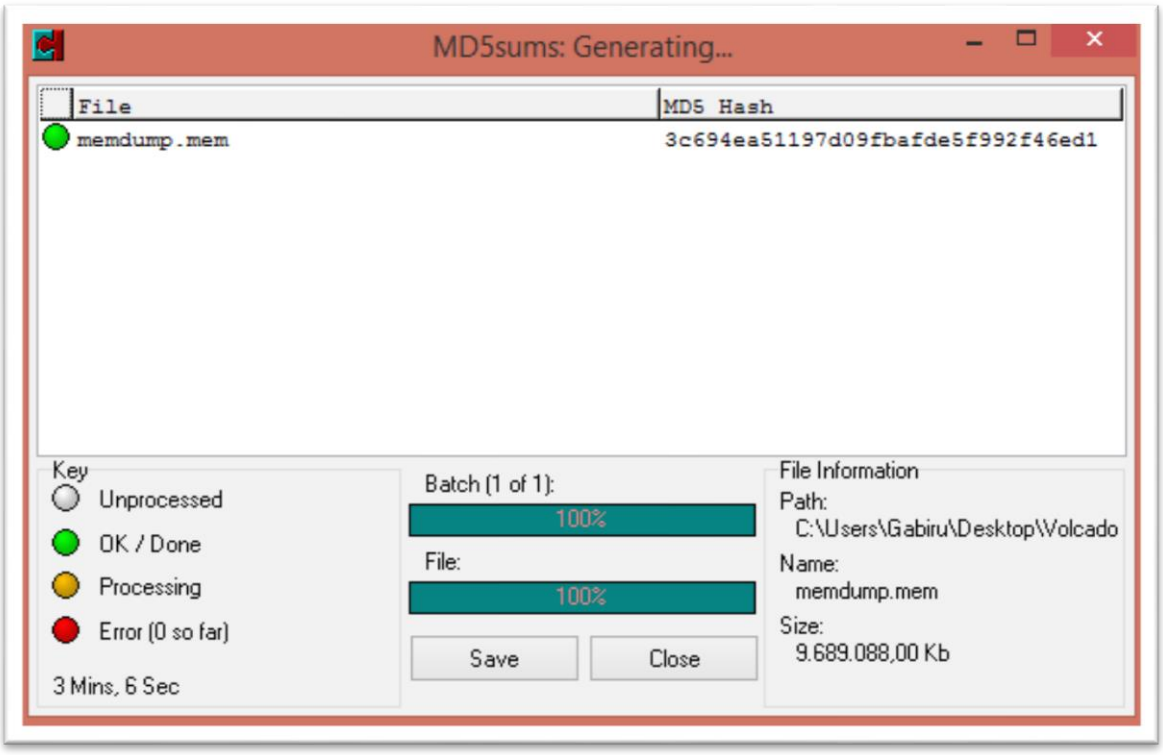


Ilustración 11 Captura de Pantalla de Software MD5sums

Como se puede apreciar en la Ilustración 7 el software MD5sums genera un hash en este caso de tipo md5 con el que posteriormente se podrá validad la integridad del volcado realizado.

3.3.3 Ficha de extracción y transporte de evidencia

Posteriormente se deberá llenar el formulario que se encuentra en el **Anexo A Ficha N° 5** donde se detallan fecha y hora de apagado del equipo, esta característica es muy importante pues forma parte de la cadena de custodia ya que se lleva un registro de hasta qué hora y fecha estuvo activo el dispositivos y se podrán hacer comparaciones de fechas.

Otro de los registros pedidos en el formulario es el medio de almacenamiento para los dispositivos físicos extraídos que por lo regular se deberá hacerse con cartón y el uso de envoltorio de plástico de burbujas o con otro material acolchado que cubra todos los lados, se debe tener excesivo cuidado al empacar para que luego no existan

discrepancias sobre la investigación, se deberá sellarlo y no ser abierto hasta que esté en manos del siguiente custodio en lista.

Luego del empaque el nuevo custodio es la persona que traslade la evidencia del lugar de delito al laboratorio forense, la información de esta persona también deberá constar en el la **ficha N° 5.**

De igual forma se deberá llenar la **ficha N° 6** que se encuentra en al **Anexo A** el mismo que contiene campos donde se deberá detallar datos sobre cuáles fueron las herramientas de extracción utilizadas, hora y fecha de extracción de la información, medios y formatos de almacenamiento, y al igual que en la ficha N°6 el nombre del nuevo custodio y los datos del medio en el que será transportada la información.

3.4 Preservación de la evidencia.

Una vez recibidos los dispositivos físicos incautaos y los dispositivos en donde fueron almacenados la información extraída, procedemos a preservar la información que estos contiene.

La preservación de la evidencia se vuelve un punto fundamental dentro de la metodología ya que existe varios casos donde la evidencia presentada no fue admitida dentro de la corte debido a que no tuvo un correcto respaldo documental y científico o existió negligencia durante el cumplimiento de los objetivos de la cadena de custodia, por este motivo la correcta aplicación de las herramientas para realizar la reservación de la evidencia es fundamental.

Como se explicó en el capítulo 2 existen varias formas para preservar la información por lo que recomiendo la clonación de todo medio de almacenamiento e información, para así poder trabajar sobre la copia y no alterar la confiabilidad de los dispositivos e información incautada.

PASOS A REALIZAR EN LA FASE DE PRESERVACIÓN DE LA EVIDENCIA

- Clonación bit a bit de disco duro.
- Verificación de la integridad del clonado de disco duro.
- Verificación de la integridad del volcado de memoria RAM.
- Recuperación de imágenes y datos eliminados y ocultos.
- Llenar la ficha para la extracción y transporte de la evidencia, (Ficha N° 7).

3.4.1 Clonación medios de almacenamiento

[47]Clonación de disco duro bit a bit.

Como explique anteriormente la clonación de la información toma gran importancia sobre la investigación, ya que nos permitirá realizar un análisis sobre las copias realizadas.

No debemos olvidar que estas copias o clones deberán llevar un etiquetado al igual que los originales, y de la misma forma se deberá cumplir con la cadena de custodia sobre estas ya que también serán presentadas ante la corte.

Para realizar la clonación bit a bit de un disco duro se podrá utilizar los mismos softwares utilizados para un volcado de memoria RAM, siendo estos.

- EnCase Forensic
- AccessData FTK Imager 3.3.0.5

Recomiendo utilizar el software AccessData FTK Imager en su versión 3.3.0.5, este software nos proporciona como parte de su seguridad un hash de tipo MD5 y sha1 con los cuales podremos verificar la integridad de la copia más adelante.

[47] Clonación de Disco Duro, (Disponible en: http://es.wikipedia.org/wiki/Clonaci%C3%B3n_de_discos, Consultado: 16-11-2014)

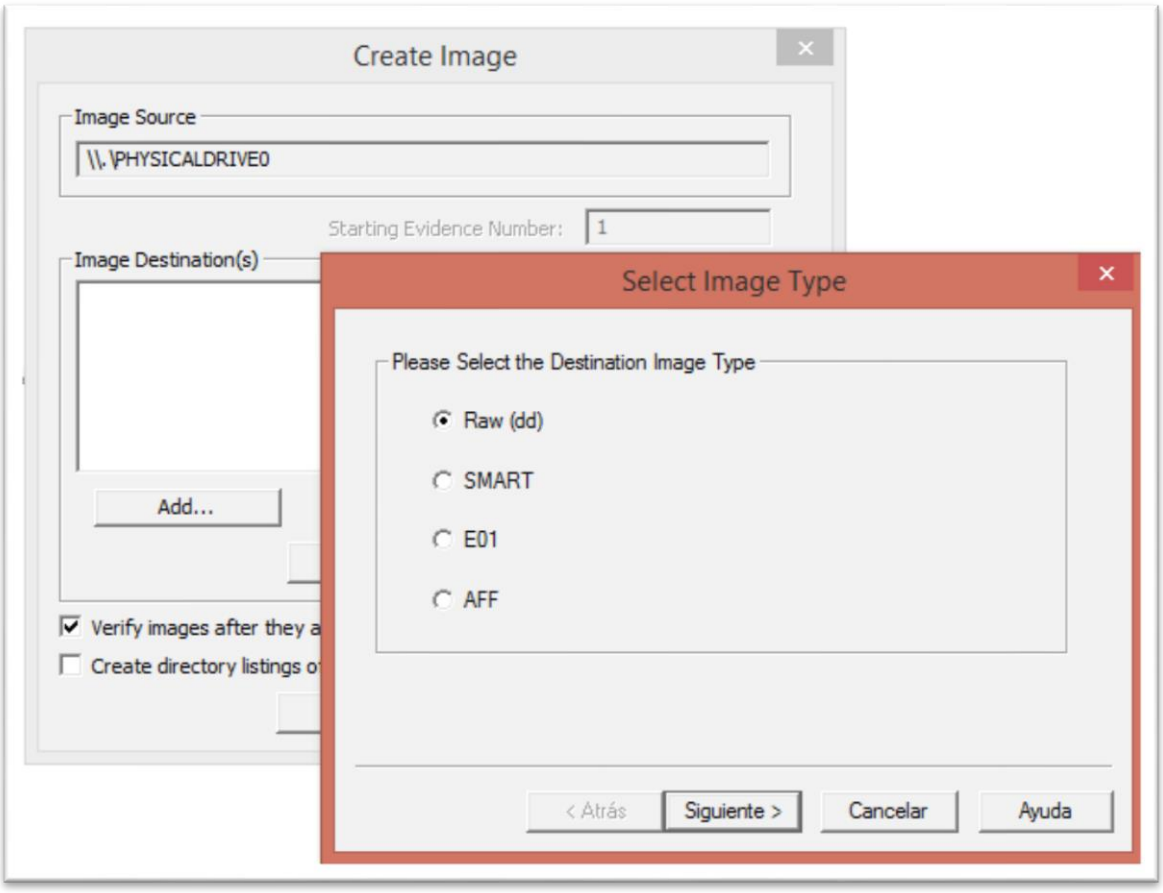


Ilustración 12 Captura de pantalla de Clonación de Disco Duro AccessData FTK Imager 3.3.0.5

AccessData FTK Imager 3.3.0.5 presenta varios formatos para realizar una imagen bit a bit del disco duro, el que sugiero elegir es RAW ya que es un formato de imagen sin particiones, y no es estándar de ninguna marca por lo que lo hace flexible y la mayoría de softwares de análisis forense lo reconoce.

Como característica a tener en cuenta es que necesita el mismo espacio de almacenamiento del origen en el destino.

Este software permite el etiquetado de la evidencia de acuerdo como se explicó en la fase de Identificación de la Evidencia, y nos proporciona varios datos con los que podremos llenar la ficha de preservación de la evidencia que más adelante se explicara.

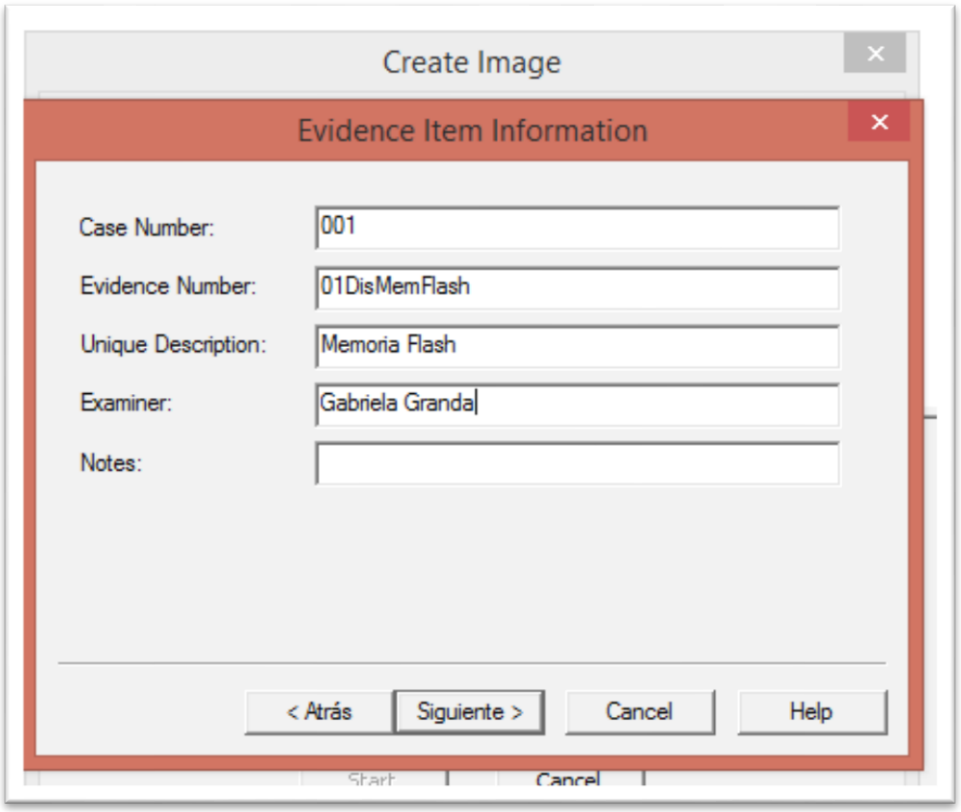


Ilustración 13 Información para el Etiquetado de la evidencia

3.4.2 Verificación de Integridad

Para la verificación de la integridad se utilizara el software que se realizó en la presento en la fase de extracción de evidencia.

Volcado de Memoria RAM

En el caso del volcado de Memoria RAM, la imagen resultante de dicho volcado fue sometida al software **Md5summer** con el cual obtuvimos un hash MD5, ahora en la fase de preservación volveremos a pasar la misma imagen resultante del volcado por el software **Md5summer** con el fin de verificar que el hash que devuelva el programa sea el mismo hash que se obtuvo en la fase de extracción.

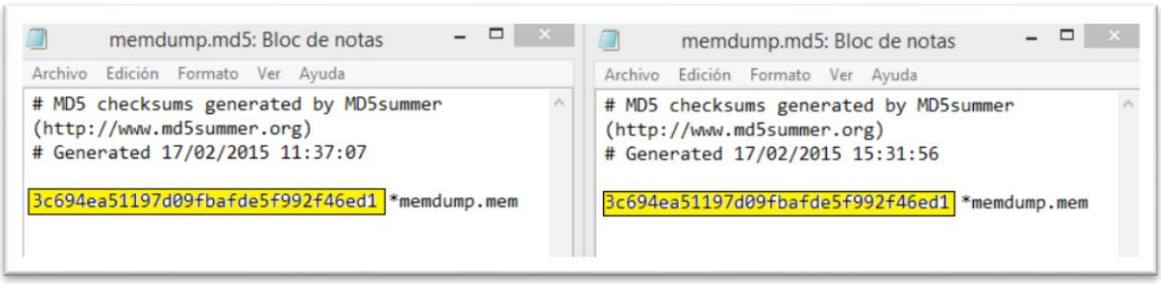


Ilustración 14 Verificación de Integridad con MD5summer

Copia bit a bit de Disco Duro

La verificación de la integridad del Disco Duro recomiendo se lo realice con el mismo software es decir con **Md5summer,** debido a que la copia bit a bit se lo realizo con el software **AccessData FTK Imager 3.3.0.5** el cual nos proporciona hash de tipo MD5 y sha1, podremos hacer la comparación con el hash resultante del software MD5sumer.

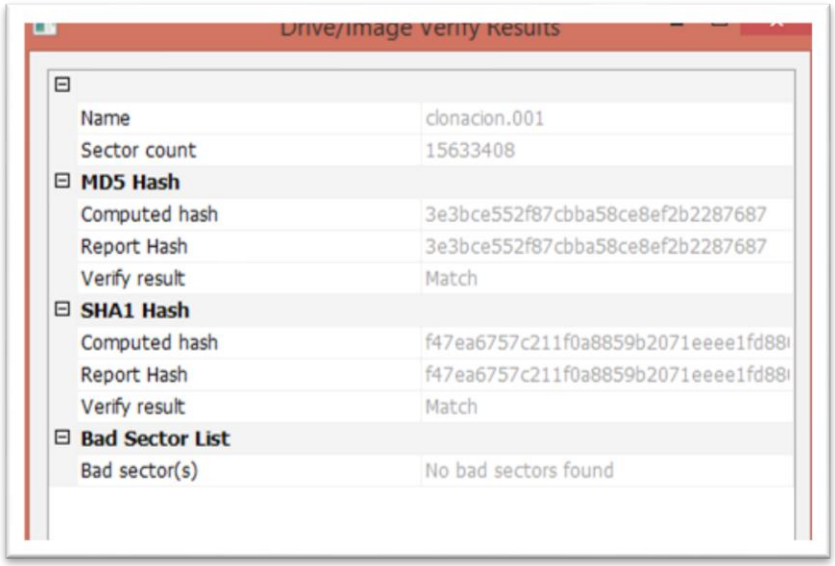


Ilustración 15Hash MD5 y SHA1 devueltas por software AccessData FTK

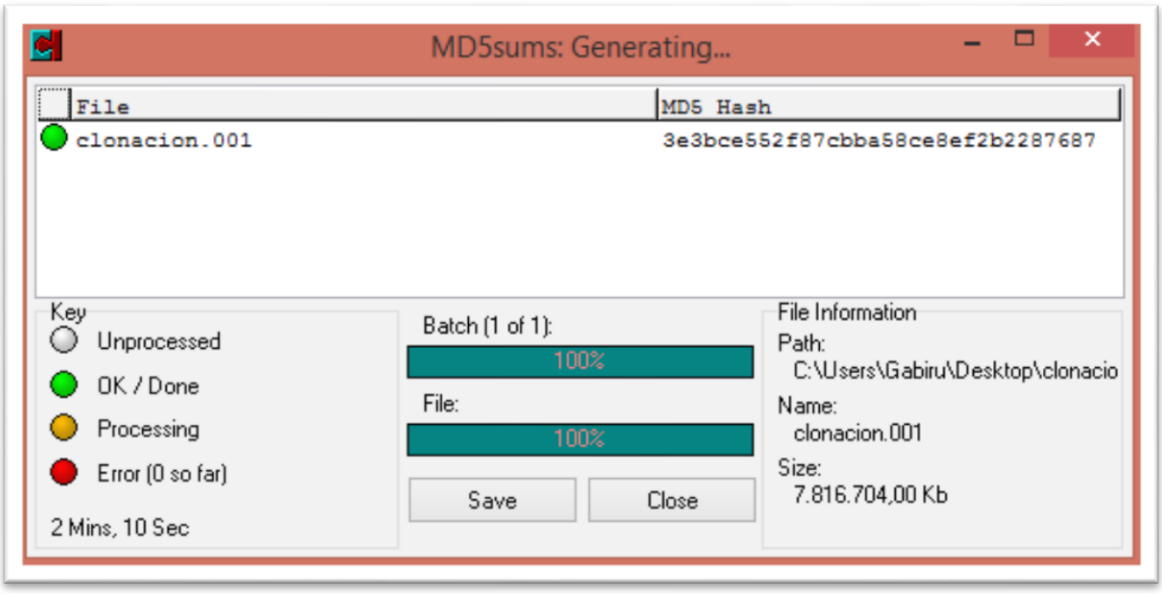


Ilustración 16 Verificación de Integridad de Clonación con software MD5sums

Como se aprecia en la ilustración anterior el software devuelve un hash MD5 que coincide exactamente con el hash que proporciona como medida de seguridad el software **AccessData FTK Imager 3.3.0.5** después de realizar una clonación de disco duro.

3.4.3 Recuperación de Imágenes

Como parte del análisis forense, se debe recuperar información eliminada, formateada u oculta, por lo que se deberá hacer uso de herramientas que al igual que en el volcado de memoria deben ser herramientas que no necesiten ser instaladas sobre el sistema operativo investigado y que el almacenamiento de la información extraída sea en un medio externo y limpio.

La herramienta que recomiendo utilizar para este análisis es [15]**Photorec**, ya que está diseñado para recuperar imágenes, videos y documentos que han sido eliminados, o perdidos y cumple con los requisitos para mantener la integridad de la evidencia haciendo que cumplamos con los objetivos de la cadena de custodia.

Esta herramienta permite recuperar información que se encuentre en diferentes sistemas de archivos, y también podremos escoger que tipo de archivos vamos a recuperar haciendo de esta herramienta muy flexible.

La recuperación se puede realizar en medios que fueron formateados o que sufrieron algún error en su ejecución.

Este software es distribuido bajo licencia pública general GNU, multiplataforma y es open source.

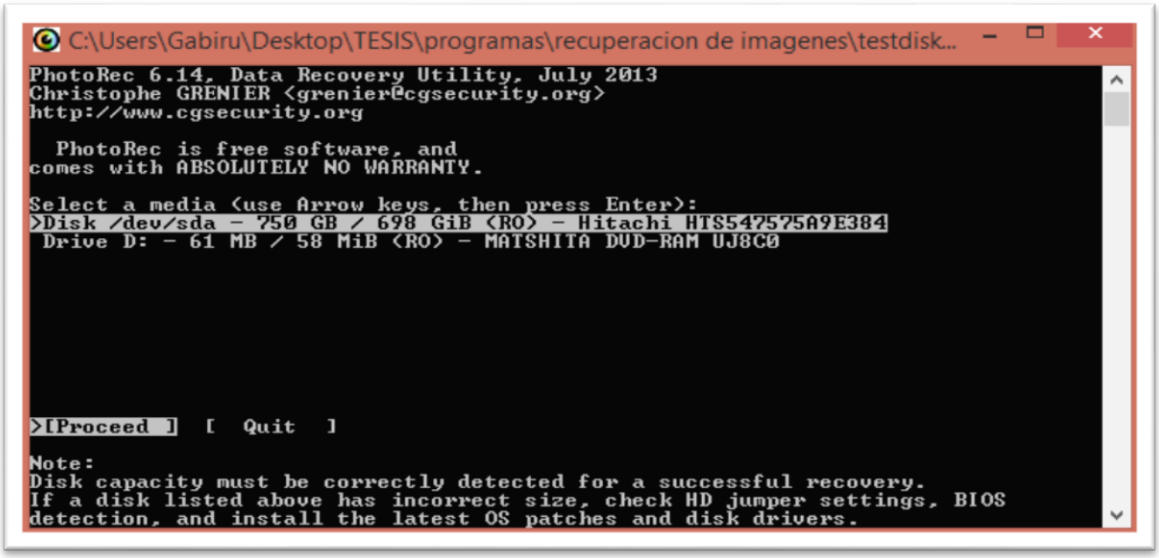


Ilustración 17 Captura de Herramienta PhotoRec 6.14

3.4.4 Ficha para la extracción y transporte de la Evidencia

Al igual que en las fases anteriores se deberá llenar la ficha que se encuentra en el **Anexo A Ficha N°7** la cual contiene campos donde se deberán especificar los nombres y características de las herramientas que se utilizaron para la clonación de los datos (disco duro bit a bit), hora y fecha de inicio y fin de la clonación, medios de almacenamiento de clon y la etiqueta que se le asignó a dicho clon.

3.5 Análisis: Aplicación de técnicas para detección de datos ocultos en imágenes y datos.

En la fase anterior realizamos la clonación bit a bit del disco duro cuestionado, por lo que en esta fase realizaremos un estegoanálisis sobre imágenes y texto plano que este contenga y que sean sospechosas.

La elección de una correcta herramienta es de gran importancia en esta fase pues debemos tener en mente la preservación de la confiabilidad, con lo que estaremos asegurando la correcta aplicación de la cadena de custodia.
Se deberá realizar una búsqueda minuciosa de herramientas especializadas en estegoanálisis ya que con sus cambios de versiones suelen tener mayores utilidades para un análisis.

Lo más recomendables es realizar el proceso de análisis con una herramienta y confirmarla con otra, ya que existen softwares que devuelven resultados por medio de porcentajes, entonces esta comprobación asegurar los resultados que obtengamos.

PASOS A REALIZAR EN LA FASE DE ANÁLISIS DE LA EVIDENCIA

- Seleccionar o definir el kit forense es decir elegir las herramientas con las que se realizara el análisis de las imágenes y texto plano.
- Analizar la cabecera de los archivos para verificar que su extensión corresponde.
- Aplicación de las Herramientas seleccionadas en busca de información oculta en la evidencia digital recolectada.
- Llenar las ficha para el análisis de la evidencia, (Ficha N°8,9).

3.5.1 Herramientas para estegoanálisis

El estegoanálisis es una técnica utilizada para el estudio, detección y extracción de datos o información oculta en medios como imágenes, audio, video y texto plano.

Como primer paso para realizar un estegoanálisis es el reconocimiento del formato del archivo, ya que este nos ayudara a elegir brevemente la herramienta estegoanalítica a ser utilizada.

En la actualidad existen varias herramientas dedicadas a este estudio, las más conocidas y por ser gratuitas son [10]StegSecret y [16]Stegdetect, las cuales están disponibles en la página oficial de su respectivo desarrollador.

Por otro lado tenemos a las herramientas comerciales como la [17]Stego Suite[48] desarrollada por WetStone A Division of Allen Corporation, quienes tienen dentro de su suite la herramienta [18]StegoHunter[49] la cual se utiliza para analizar imágenes sospechosas de haber sido procesadas por un programa de esteganografía.

Entre las herramientas gratuitas que recomiendo se encuentran:

- [10]StegSecret[50] es un conjunto de herramientas libres con las que podremos detectar y extraer la información oculta en diferentes medios informático.
- [16]Stegdetect[51], este es un comando Linux con el cual hace un análisis estadístico que verifica si una imagen ha sido tratada mediante una herramienta que realiza esteganografía, de igual forma busca el nombre de la herramienta utilizada para incrustar la información oculta.

[48] WetStone Technologies. WetStone Stego Suit.(Disponible en: https://www.wetstonetech.com/product/stego-suite/, Consultado: 20-11-2014)
[49] WetStone Technologies. WetStone StegoHunter. (Disponible en; https://www.wetstonetech.com/product/stegohunt/, Consultado: 20-11-2014)
[50] StegSecret. A simple steganalysis tool. (Disponible en:. http://stegsecret.sourceforge.net/, Consultado: 20-11-2014)
[51] Niels Provos. Ubuntu Manuals. (Disponible en: http://manpages.ubuntu.com/manpages/hardy/man1/stegdetect.1.html#contenttoc7, Consultado: 20-11-2014)

- [19]Bless Text Editor[52]: esta herramienta trabaja con imágenes y texto plano, nos permite ver el código hexadecimal y de esta manera podremos apreciar el texto oculto.

Estas herramientas nos ayudaran a extraer los datos ocultos que se encuentren en las imágenes y texto plano procesado.

3.5.2 Detección y Extracción de Información Esteganografía

Verificación de formatos de archivos

Propongo este procedimiento como primer paso ya que estaremos segregando la información obtenida para que posteriormente pueda ser analizada con herramientas de estegoanálisis en busca de información oculta.

La verificación del formato del archivo nos ayudara a saber si estamos tratando con un archivo verdadero, es decir que su extensión es correcta e idéntica a la que se presenta a primera vista. Este análisis del formato ayuda en primera instancia a verificar si existe algún contenido sospechoso ya que con la herramienta que posteriormente se presentaran podremos darnos cuenta muy superficialmente si existe algún tipo de contenido que no pertenece a la imagen o al texto.

Existen varios delitos informáticos que se pueden desencadenar debido a que la población ecuatoriana en su mayoría no conoce lo suficiente acerca de formatos y extensiones de archivos, por ejemplo una persona puede ser víctima de robo de información sensible ya que sin percatarse acepto e instalo un programa pensando que solamente era una imagen o un documento de texto, es por esto que los delitos cibernético o informáticos se vuelven comunes dentro del Ecuador y la verificación de la extensión del archivo que estamos por abrir toma gran importancia.

El software con el que podemos analizar el formato de un fichero es **AccessData FTK Imager 3.3.0.5** con su opción Add Evidence Item.

[52] Bless Hex Editor. (Disponible en: http://home.gna.org/bless/, Consultado: 20-11-2014)

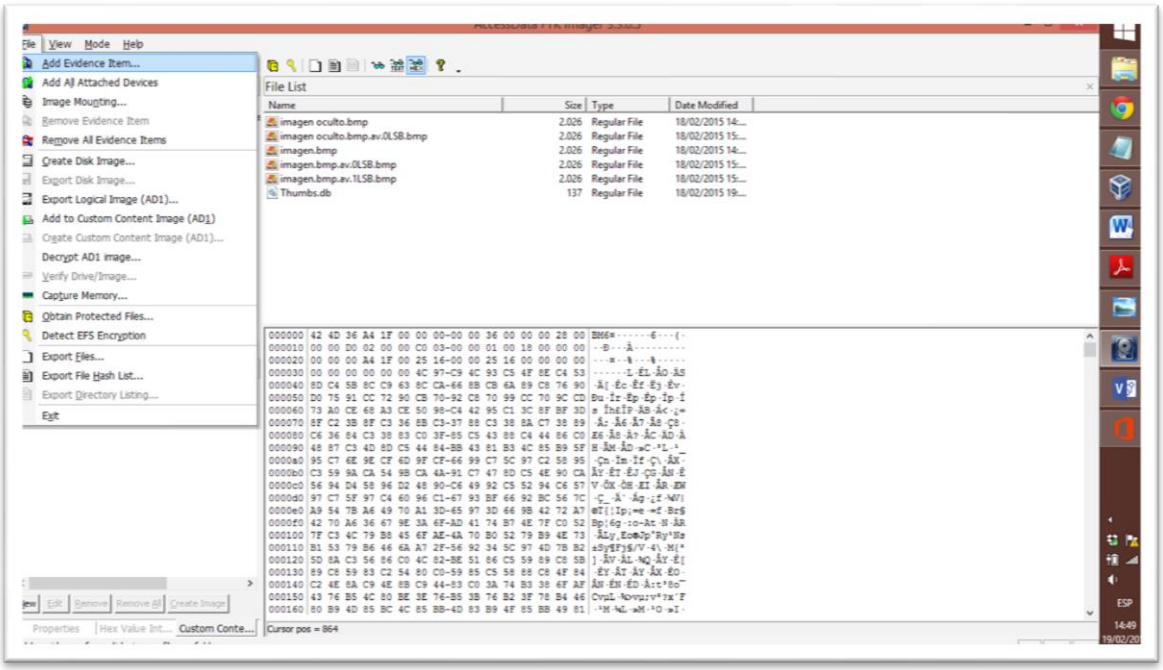


Ilustración 18 Análisis de Cabecera con Access Data FTK Imager

Una vez añadido como un ítem de evidencia, procedemos a elegir la carpeta en la que se encuentran las imágenes y texto plano a ser analizados.

En el siguiente grafico se puede apreciar el resultado de una imagen JPG que no tiene información oculta, cuando es analizado por este software solo presenta información sobre la cabecera o tipo de archivo, mientras que si se analiza un archivo con contenido oculto este presenta información de la cabecera más caracteres q indican información adicional que podría tratarse de información oculta.

De esta manera se pude ir segregando las imágenes y documentos a ser analizados.

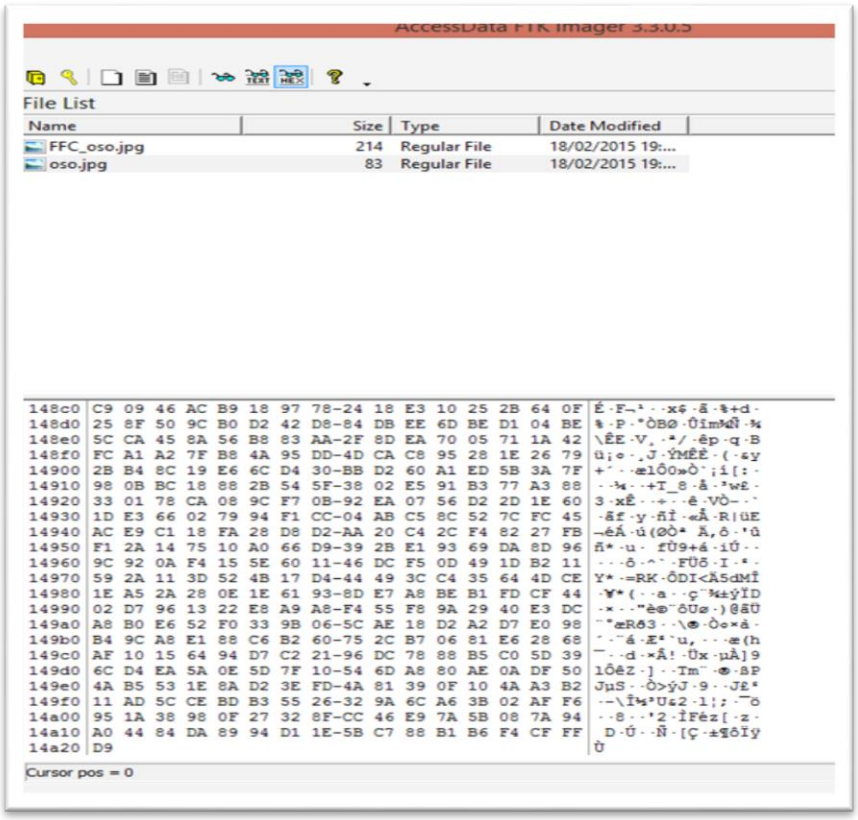


Ilustración 19 Cabecera de Imagen JPG sin información oculta

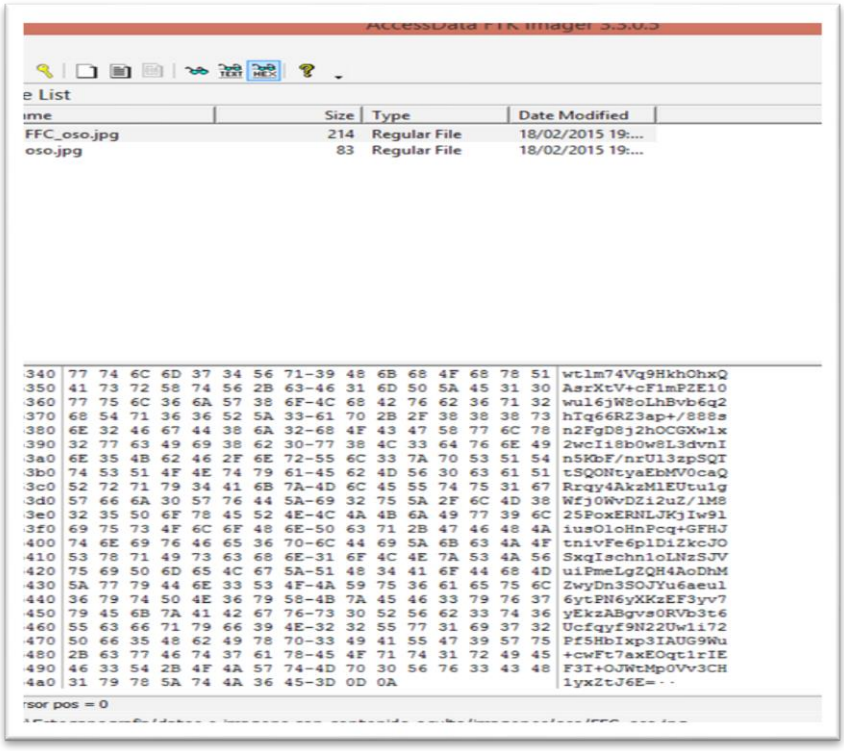


Ilustración 20 Cabecera de Imagen JPG con información oculta

- XStegSecret

En este paso de la metodología utilizaremos el software [53]**XStegSecret**, debido a que este software implementa diferentes algoritmos estegoanalíticos, realiza ataques Visuales, estadísticos y [54]RS.

El primer paso para la aplicación de esta herramienta es verificar que las imágenes a ser analizadas cumplan con los formatos que recibe este software como son BMP, GIF y JPEG, ya que estos son los formatos más utilizados, cabe recalcar que se deberá revisar el tamaño de las imágenes y del texto ya que este puede ser un indicador superficial que demuestra que una imagen pudo haber pasado por el proceso de esteganografía.

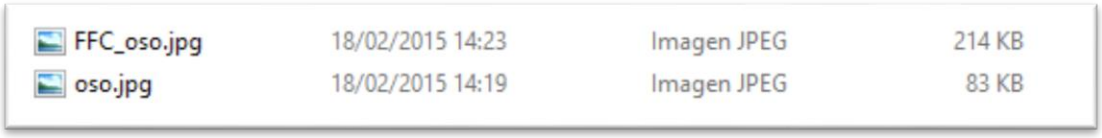


Ilustración 21Ilustración 11 Ejemplo de Cambio de Tamaño de Imagen Cuando tiene Contenido Oculto

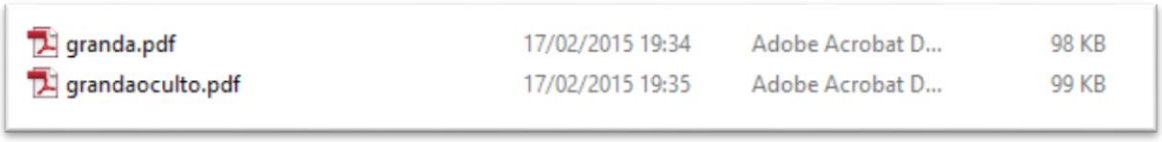


Ilustración 22 Ejemplo de Cambio de Tamaño de Texto Cuando tiene Contenido Oculto

[53] StegSecret. A simple steganalysis tool. (Disponible en: http://stegsecret.sourceforge.net/, Consultado: 21-11-2014)
[54] Manual stegsecret, pag.5, (Disponible en: stegsecret.sourceforge.net/SpanishManual.pdf, Consultado: 21-11-2014)

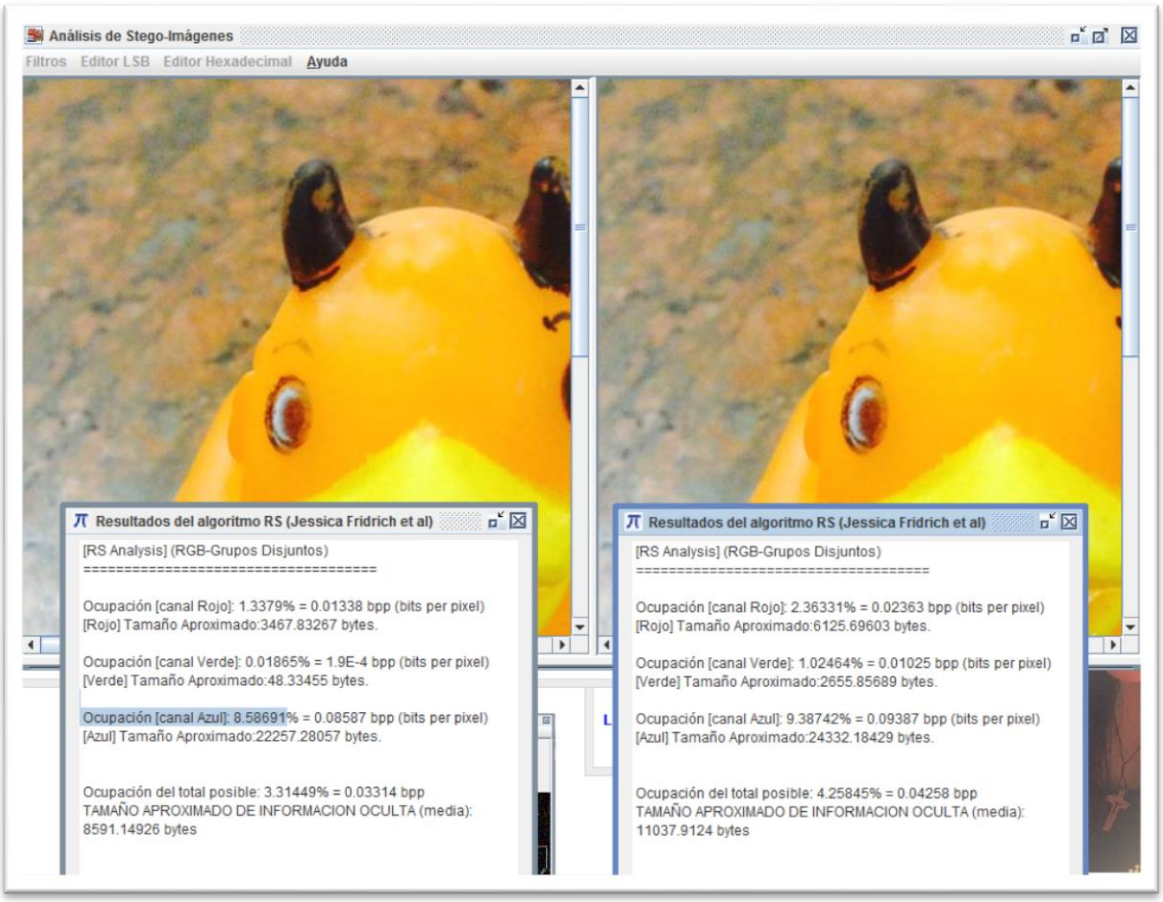


Ilustración 23Captura de Pantalla del Software StegSecret Ataque RS.

En la imagen anterior tenemos del lado izquierdo una imagen sin contenido oculto y del lado derecho tenemos la misma imagen con contenido oculto.

Estas imágenes fueron sometidas al ataque [55]RS-Atack del cual podemos deducir un estimado de la cantidad de datos ocultos que contiene la imagen ya que este ataque detecta modificaciones cuando se alteran los bits menos significativos aleatoriamente, es decir se realiza esteganografía LSB sin seguir ningún patrón, este ataque tiene mayor precisión sobre imágenes de formato BMP.

Este ataque detecta información oculta si el tamaño de esta es mayor a los 0.005 bits por pixel, como se aprecia en la captura de pantalla este software nos puede devolver valores con un margen de error o falso positivos, sin embargo estos no son muy altos.

[55] Manual stegsecret, pag.5, (Disponible en: stegsecret.sourceforge.net/SpanishManual.pdf, Consultado: 21-11-2014)

- **StegDetect**

[16]StegDetect permite la detección de las herramientas con las que se realizó esteganografía y trabaja solamente con imágenes de formato JPEG, este paquete es de distribución libre y corre solamente sobre Linux.

En la siguiente imagen se presenta un ejemplo del análisis de una imagen **JPEG** que utilizo la herramienta [56]JHPS Steganography Software para ocultar la información.

Mediante el comando "**stegdetect –s 4 imagen.jpg"** podremos recibir cual es el nombre del a aplicación que ha sido utilizada para ocultar información en dicha imagen.

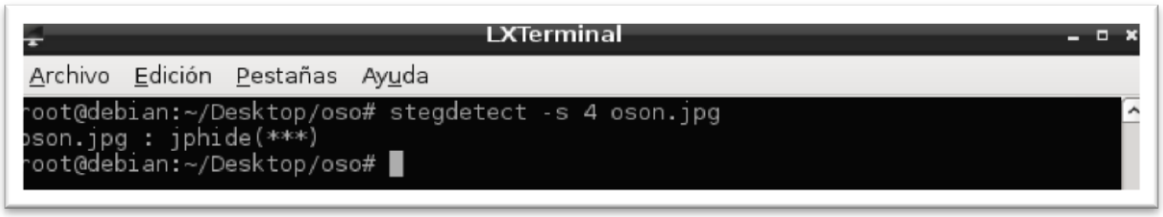


Ilustración 24 Captura de Pantalla software Stegdetect Identificación de Herramienta

3.5.3 Ficha para el Análisis de la Evidencia

De la misma manera que en las anteriores fases se deberá llenar un formulario para mantener la cadena de custodia intacta, es decir para saber si sufrió algún tipo de cambio durante el análisis, por otro lado constara el nombre del custodio, el mismo que realizara un informe detallando los resultados obtenidos.

Este formulario contendrá campos donde se detallara si se encontró información oculta, el nombre de la herramienta utilizada para el estegoanálisis, tamaños aproximados de información oculta, si es posible el nombre de la herramienta que se utilizó para ocultar la información y la información oculta encontrada, todos estos campos se encuentran en la **ficha N° 9** del **Anexo A,** de igual forma en la **ficha N°8** se pedirán los mismos datos con la única diferencia de que en esta deberá constar la imagen procesada donde se muestra el contenido oculto**..**

[56]JHPS Steganography: (Disponible en: http://bit599.netai.net/jphs.htm, Consultado: 22-11-2014)

3.6 Documentación y presentación de resultados.

Esta es la fase final de la metodología para un análisis forense sobre imágenes y datos, donde se realizara un documento donde se entreguen todas los formularios que se llenaron durante todo el proceso de análisis con esto respaldaremos el resultado científico que se logre obtener de la investigación.

Se deberá realizar un documento técnico (**Informe Técnico**) con el correspondiente apoyo científico, es decir explicar cuáles fueron las primeras instancias de recolección o identificación de la evidencia, que herramientas fueron utilizadas para tratada la evidencia a lo largo del proceso explicar de una forma muy detallada si sufrió cambios, cuales fueron estos y si fueron esperados o existió algún tipo de negligencia. Se deberá también detallar los resultados obtenidos en cada una de las fases de esta metodología y poniendo más énfasis en los resultados obtenidos después de procesar a la evidencia con la herramienta de detección y extracción de la información oculta.

De igual forma se deberá presentar los formularios que avalan el correcto cumplimento de la cadena de custodia por parte de los peritos forenses que formaron parte de la investigación.
La redacción de este documento debe ser de un carácter técnico, es decir que cualquier ingeniero de sistemas que lo lea deberá entenderlo.

Por otro lado se deberá redactar un documento denominado **"Informe Ejecutivo"** donde se explique con palabras no técnicas y de fácil entender para un abogado, el juez, etc, con esto se agilizará el proceso de juzgamiento y podremos de alguna forma tener cierta certeza de que los resultados obtenidos podrán servir como evidencia contundente o de gran importancia en el proceso judicial.
Este documento no debe ser extenso y como se dijo no tener un carácter técnico, se deberá enumerar las técnicas utilizadas, si ha existido algún problema, y por último los resultados obtenidos.

3.6.1 Informe Técnico

El informe técnico a presentar deberá contener los siguientes puntos:

- Nombre del Perito Forense
- Fecha
- Presentar Ficha N°1 y Ficha N°2
- Expresar cuales son los primeros indicios para la realización de la investigación.
- Expresar brevemente que artículos del COIP fueron cumplidos a cabalidad
- Adjuntar Imágenes del lugar.
- Recreación grafica del Lugar
- Herramientas utilizadas para la extracción de la evidencia y sus respectivos resultados es decir indicar la etiqueta que se ha asignado a cada uno de los dispositivos físicos y de almacenamiento utilizados e incautados.
- Herramientas utilizadas para la preservación de la evidencia y sus respectivos resultados es decir detallar la etiqueta asignada a los clones realizados, tamaños de cada clon, formatos.
- Herramientas utilizadas para el estegoanálisis de las imágenes y datos sustraídos en los pasos anteriores.
- Resultados del proceso de estegoanálisis.
  - Etiqueta de la imagen o texto plano
  - Detalles de las imagen o texto plano evaluado
  - Porcentaje de Contenido Oculto
  - Gráficos obtenidos de las herramientas.
- Conclusiones

3.6.2 Informe Ejecutivo

El informe Ejecutivo a presentar deberá contener los siguientes puntos:

- Nombre del Perito Forense
- Fecha
- Presentar Ficha N°1 y Ficha N°2
- Expresar cuales son los primeros indicios para la realización de la investigación.
- Expresar brevemente que artículos del COIP fueron cumplidos a cabalidad.
- Presentación de Resultados
- Conclusiones

CAPITULO IV. IMPLEMENTACIÓN DE LA METODOLOGÍA DESARROLLADA

4.1 Aplicación de Metodología

En el presente capitulo se realizara la aplicación de la metodología desarrollada en el capítulo tres haciendo uso de los diferentes herramientas que se han expuesto y de la misma forma se utilizaran diferentes formatos de imágenes.

Para la aplicación me basare en la Ilustración 3 en donde se encuentra un diagrama de los pasos que se deberán realizar a lo largo de la metodología y en la Ilustración 4 la cual nos indica el proceso para llenar las fichas que nos ayudaran a cumplir con la cadena de custodia.

CASO A SER INVESTIGADO

Uno de los casos comunes en el Ecuador es el robo de información de diferentes empresas o personas naturales, el cual está debidamente tipificado en el Código Orgánico Integral Penal en la Sección Tercera "Delitos Contra la Seguridad de los Activos de los Sistemas de Información" y detallado en sus respectivos artículos.

Este tipo de delito puede tener varios indicios pero uno en particular puede ser el haber abierto una imagen sin saber que dentro de esta contenía una serie de comandos que desencadena la instalación o ejecución de un software, ya sea este un virus, malware, keylogger, backdoors, etc, con el cual estaríamos dando acceso a la información y al control del equipo y de ser el caso de toda la red a la que estemos conectados.

Por lo que con la aplicación de la metodología propuesta, se buscara identificar la imagen que contiene dicho software malicioso, ya que presenta pasos a seguir para mantener una cadena de custodia y sugiere diferentes softwares para la extracción, preservación y análisis de las imágenes o texto plano.

4.2 Desarrollo

PASO 1: DEFINICIÓN DE LOS REQUISITOS PARA EL INICIO DE LA INVESTIGACIÓN.

- Definición de requisitos

Para comenzar con la investigación doy a conocer que trabajare bajo la dirección y petición del consejo de la judicatura, fiscalía y el ministerio de telecomunicaciones, declaro haber recibido los siguientes documentos:

- Orden de Allanamiento
- Consentimiento libre de la persona afectada para el registro y extracción de evidencia.

Los peritos forenses a trabajar en esta investigación están debidamente certificados y constan en la ficha N°1 y su respectiva información personal en la ficha N°2.
El desarrollo de estas fichas se encuentra en el **Anexo B Ficha N°1 y N°2**

PASO 2: IDENTIFICACIÓN DE DISPOSITIVOS Y EVIDENCIA DIGITAL, RECOLECCIÓN DE INFORMACIÓN VOLÁTIL.

- Identificación

Debido a que ya tenemos en nuestro poder el consentimiento de la persona afectada para realizar la identificación de los dispositivos y la información digital procedemos a realizar los siguientes pasos:

Cumpliendo con las **protecciones físicas** realizamos los siguientes pasos:

- Guantes

Ilustración 25 Uso de Guantes Quiturgicos

- Etiquetado de la evidencia

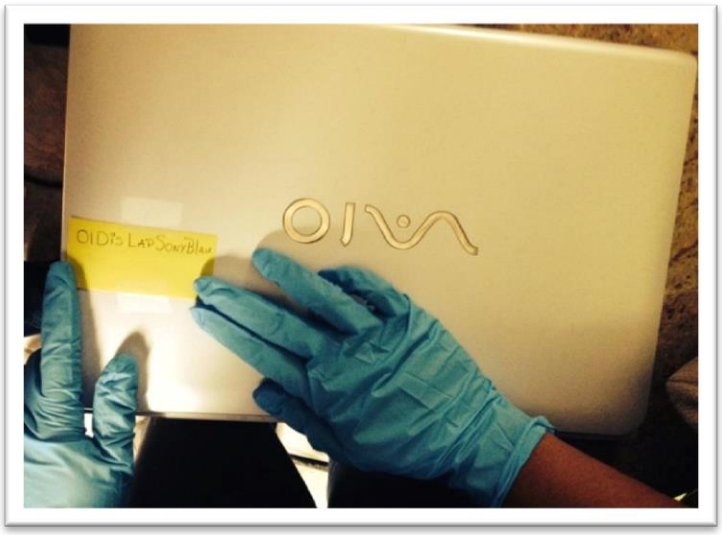


Ilustración 26 Etiquetado de Evidencia

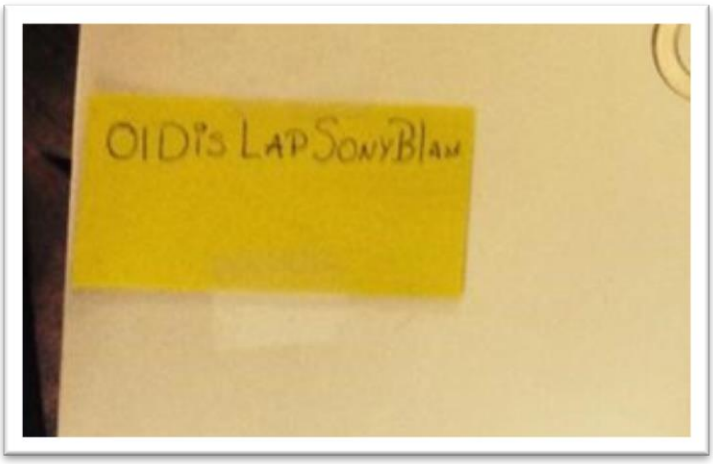


Ilustración 27 Número de Etiqueta

El segundo para para la identificación es el de **fotografiar la escena** donde se encuentra la el dispositivo donde se cometió el delito en este caso una Laptop Sony Vaio Blanca.

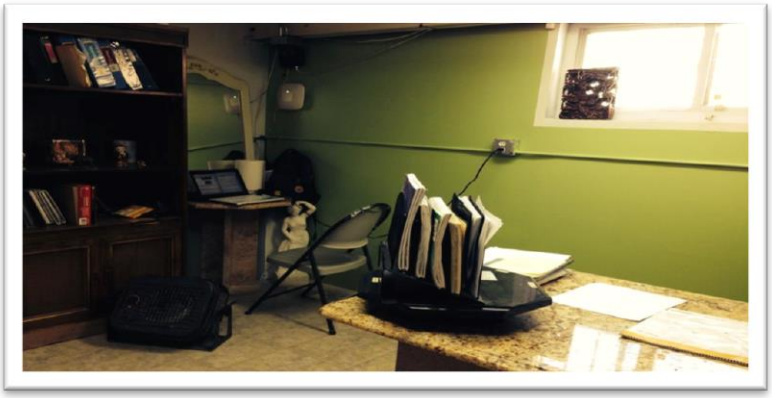


Ilustración 28 Imagen donde se encuentra Computadora a ser investigada

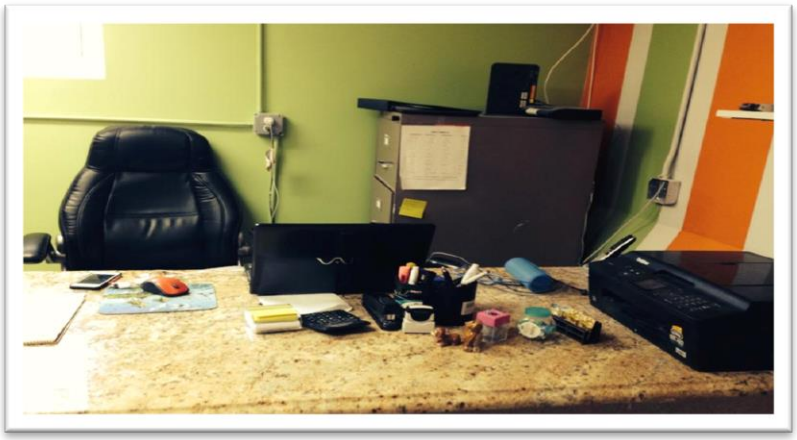


Ilustración 29 Imagen del lugar donde se encuentra la evidencia

El tercer paso dentro de la identificación de la evidencia es el de **video grabar** el lugar donde se encuentra la evidencia también deberá ser etiquetado.

01VidOfficEvidencia

El cuarto paso de la identificación de la evidencia es la **recreación del lugar** donde se encuentra la evidencia realizado con el software SketchUp.

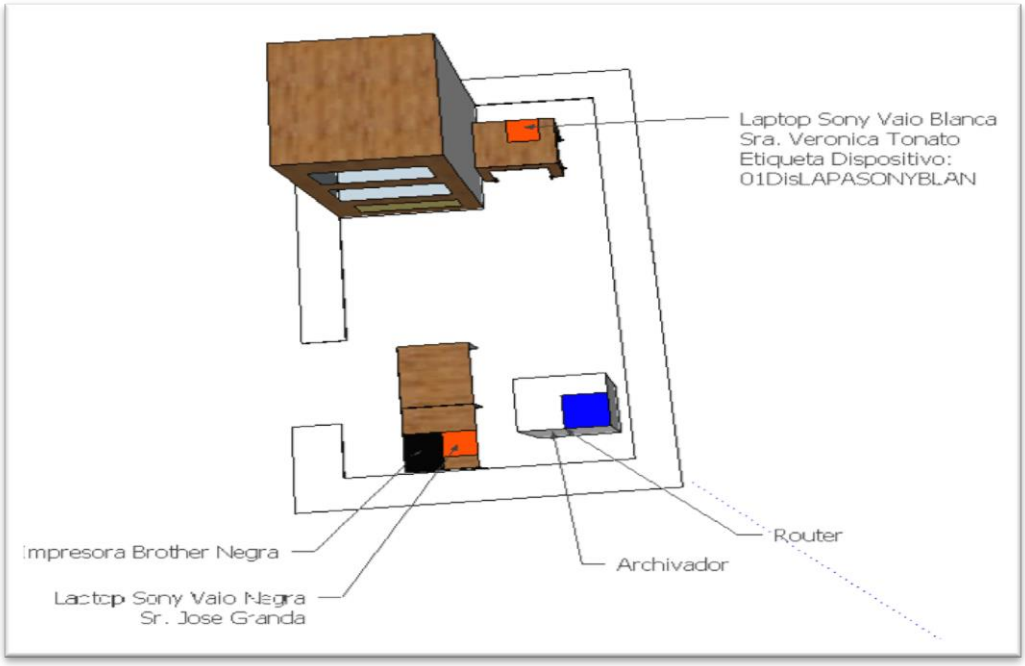


Ilustración 30 Reconstrucción grafica del lugar donde se encuentran los dispositivos a ser analizados

El quinto y último paso de esta fase de identificación es **el registro** de las características del dispositivo físico a ser incautado y el registro de la evidencia volátil recogida todo esto en las **fichas N°3 y N°4**.

El desarrollo de estas fichas se encuentra en el **Anexo B Ficha N°3 y N°4**

PASO 3: EXTRACCIÓN DE LA INFORMACIÓN VOLÁTIL, EMPAQUETADO Y TRANSPORTE DE DISPOSITIVOS E INFORMACIÓN EXTRAÍDA.

- Extracción y Transporte de la Evidencia

El dispositivo a ser investigado si puede ser extraído del lugar donde se lo encontró por lo que procedemos a realizar el primer paso de la fase de extracción y transporte por lo realizamos un **volcado de la memoria RAM**, la misma que será almacenada en un disco DVD-R, la etiqueta a ser colocada en este volcado es 01VolcRAM.

Como muestra la metodología se utiliza el software AccessData FTK Imager en su versión 3.3.0.5 con la opción Capture Memory  la misma que devolverá la Ilustración 28.

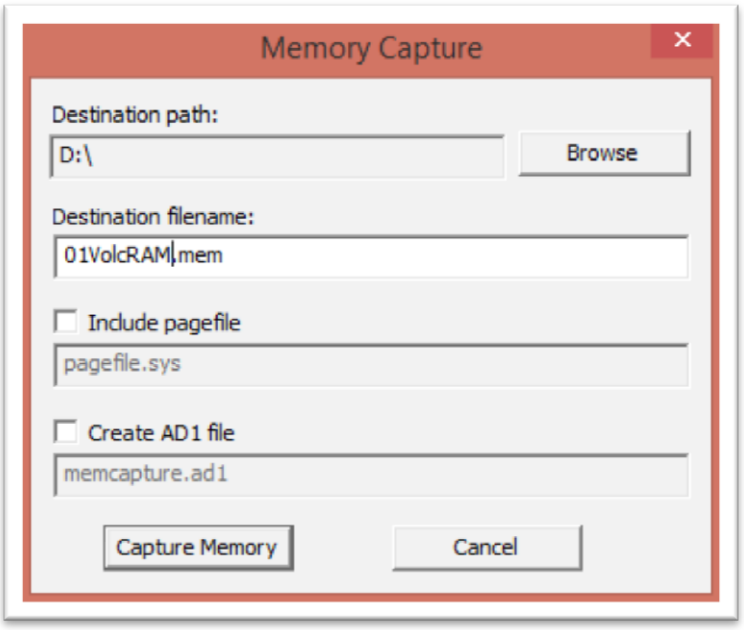


Ilustración 31 Imagen del etiquetado de volcado de memoria RAM

Después de estos pasos ya tendremos una imagen de la memoria RAM la misma que tiene extensión ".mem".

Esta imagen la utilizaremos más adelante para analizarla y conocer información sobre proceso, ejecutables, conexiones, etc., las cuales podrían ayudar con la investigación ya que podrán dar indicios de que software es el que se está comportando de manera extraña.

El segundo paso para de la fase de extracción es la generación de un hash MD5 para luego pasar por la verificación del mismo y de esta forma **comprobar la integridad** del volcado realizado.

El hash generado por el software md5 del volcado de memoria RAM realizado es "**7b574e4ff0768280bf46b1d743f76636".**

El tercer paso de esta fase es el **empaquetado de la evidencia** de acuerdo a los parámetros que establece la metodología

Ilustración 32 Empaquetado de Evidencia 01DisLAPSONBLAN

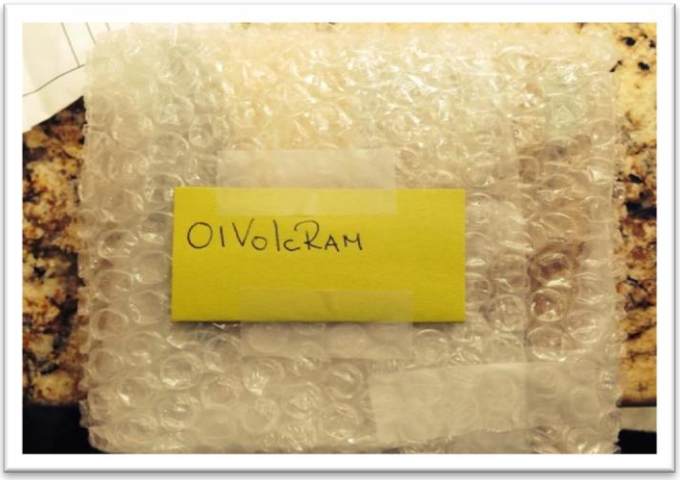


Ilustración 33 Empaquetado de DVD-R que contiene volcado de memoria RAM

El cuarto y último paso de esta fase es **llenar las fichas N° 5 y N°6 Anexo B.**

PASO 4: COPIAS BIT A BIT DE MEDIOS DE ALMACENAMIENTO, VERIFICACIÓN DE INTEGRIDAD Y RECUPERACIÓN DE IMÁGENES OCULTAS Y ELIMINADAS.

- Preservación de la Evidencia

El primer paso de esta fase es la **clonación bit a bit** del disco duro, el clonado tendrá la etiqueta **01DisHDHitachi**.

De igual forma se realizara una clonación del volcado de memoria RAM extraído en la fase de Extracción y Transporte.

El segundo paso es **la verificación de la integridad** tanto del volcado de memoria RAM y de la clonación bit a bit de disco duro.

	Hash obtenido en fase de extracción y transporte:	Hash obtenido en fase de preservación	
Memoria RAM	7b574e4ff0768280bf46b1d743f76636	7b574e4ff0768280bf46b1d743f76636	
Disco Duro	3e3bce552f87cbba58ce8ef2b2287687	3e3bce552f87cbba58ce8ef2b2287687	

Ilustración 34Verificación de Integridad

El tercer paso de esta metodología es la **recuperación de Imágenes** ocultas, borradas, etc., para esto hago uso del software **Photorec**.

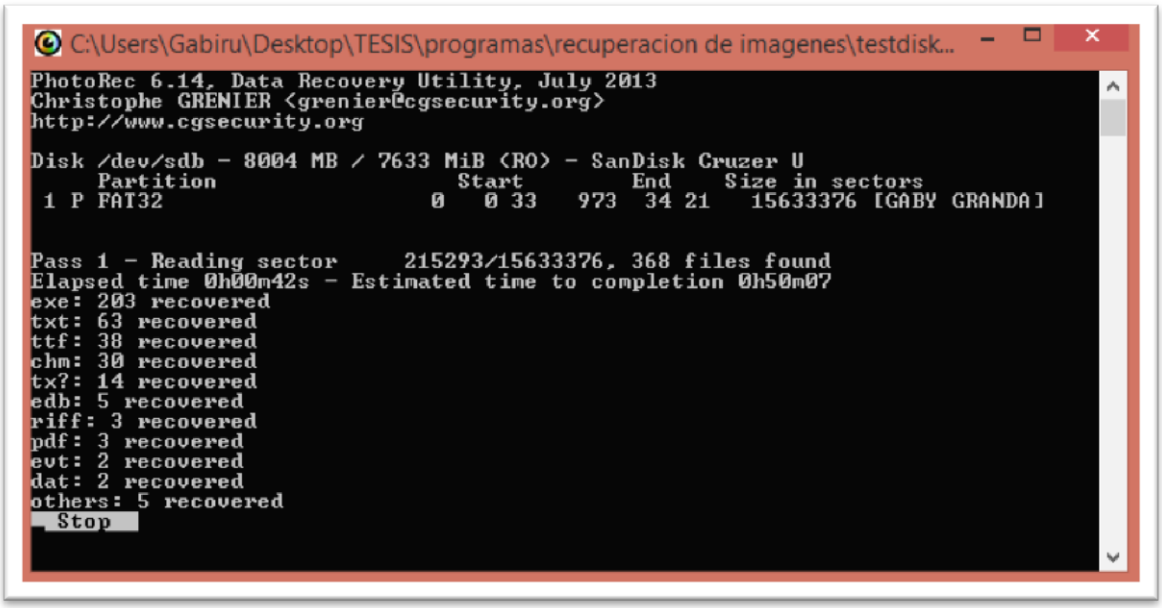


Ilustración 35 Recuperación de Imágenes Eliminadas de Disco Duro

Una vez finalizado el procedimiento de recuperación, procedemos a la identificación de imágenes o documentos que podrían ser las portadoras del software malicioso utilizad para cometer el delito.

El cuarto y último paso de esta fase es llenar la **Fichas N° 7** que se encuentra en el **Anexo B**.

PASO 5: IDENTIFICACIÓN, DETECCIÓN DE CONTENIDO OCULTO

- Análisis

En esta fase se analizaron los clones realizados ayudándonos de la herramienta AccessData FTK Imager.

De los resultados obtenidos del análisis de los clones y de las imágenes obtenidas con Photorec segregué las imágenes que podrían contener información oculta, por lo que realizare un análisis estenográfico sobre algunas imágenes utilizando los softwares que presenta las fases de análisis en la metodología.

El primer paso para el análisis es el de **verificar la cabecera del documento**, es decir verificar que una imagen JPG tenga en su cabecera solo contenido propio. Este

paso lo realice con el software AccessData FTK Imager sobre la imagen con nombre "imagen.jpg" y etiqueta pudiendo observar muy superficialmente que dentro de esta cabecera se aloja un archivo exe, por lo que procedo al siguiente paso del análisis.

El segundo paso es el de **detección y extracción de la información oculta**, para esto eh utilizado el paquete Stegdetect en Linux ya que estoy trabajando con una imagen de formato JPG.

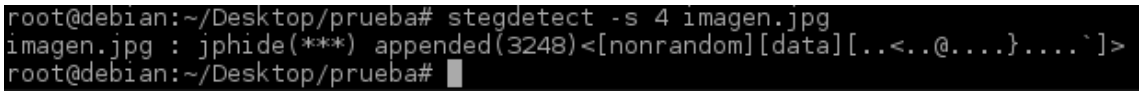


Ilustración 36Analisis con Stegdetect

En la Ilustración 33 se puede ver que con el paquete stegdetect se pudo verificar que si existe información oculta y que probablemente fue introducida con el software [57]jphide y que los datos no están introducidos de forma aleatoria.

El cuarto y último paso de la metodología es el llenar la ficha **N° 9 Anexo B**.

PASO 6: RECOLECCIÓN DE FICHAS PARA SUSTENTAR LA CADENA DE CUSTODIA Y CREACIÓN DE INFORMES TÉCNICO Y EJECUTIVO.

- Documentación: Informes

Este es el último paso de la metodología donde redactare el Informe Ejecutivo y Técnico de acuerdo a las directrices que la metodología propone.

[57] JPHide: (Disponible en: http://linux01.gwdg.de/~alatham/stego.html, Consultado: 05-01-2015)

INFORME TÉCNICO

Perito Forense: Gabriela Granda

Fecha: 24-02-2015

Adjunto: Fichas (1-9), Ilustración 25,26,27

Se recibió una solicitud del Consejo de la Judicatura y de la Fiscalía para realizar la investigación, sobre los delitos tipificados como “Interceptación ilegal de datos” y “Acceso no consentido a un sistema informático, telemático o de telecomunicaciones” que sufrió el Sr. José Granda, el mismo que ha dado la autorización para realizar los diferentes procesos que mantiene la metodología a seguir.

Como bien la metodología indica se han cumplido con los artículos 482, 456, 480, 478 del Código Integral Penal.

Se utilizó la herramienta AccessData FTK Imager versión 3.3.0.5 para la extracción de la evidencia con etiqueta “01VolcRAM”, teniendo un resultado positivo ya que esta herramienta devuelve un informe donde indica si ha existido algún fallo.

En esta fase también se realizó parte de la integridad del volcado de memoria RAM obteniendo un hash MD5, el mismo que fue verificado en la fase de preservación y coincidieron, por lo que la integridad se mantuvo.

El transporte de la información se realizó sin ningún percance llegando en buen estado los dispositivos incautados al laboratorio.

En la fase de preservación de la información se ha utilizado el mismo software AccessData FTK Imager versión 3.3.0.5 con el cual se realizó una clonación bit a bit del Disco Duro incautado con etiqueta “01DisHDHitachi” devolviendo una imagen con formato RAW sin particiones ni segmentaciones y con nueva etiqueta “01DisHDHitachiClon”, de igual forma este software devolvió un hash MD5 el cual fue verificado con el software md5summer y se obtuvo un resultado positivos.

De igual forma se realizó el clonado manual del volcado de memoria RAM con etiqueta “01VolcRAM” devolviendo una copia exacta con la

etiqueta “01VolcRAMClon”, la verificación de la integridad de esta copia se realizó sin ningún problema utilizando el hash 7b574e4ff0768280bf46b1d743f76636.

Por otro lado se realizó la búsqueda de imágenes ocultas y eliminadas en el dispositivo mediante el software PhotoRec.

Una vez preservada la información comenzamos a realizar un análisis de los clones realizados, sacando como resultado la imagen de formato JPG con nombre “Imagen.JPG” y con etiqueta “02ImgImagenJPG”, la misma fue sometida a un análisis superficial con el software AccessData FTK Imager verificando que en su cabecera existía información adicional correspondiente una aplicación .exe.

‘Luego de este análisis la imagen “02ImgImagenJPG” se sometió a una herramienta de estegoanálisis llamada Stegdetect, la cual nos confirmó la presencia de contenido oculto y nos proporcionó el nombre del software con el cual se ocultó la información siendo este JPHIDE, de igual forma nos avisa que no se ha utilizado un algoritmo que oculte la información de forma aleatoria.

Conclusiones:

Mediante el análisis realizado se ha logrado identificar la imagen con la que el atacante logro tomar el control y robar información sensible.

La Imagen con etiqueta “02ImgImagenJPG” contenía una un archivo.exe en su cabecera el cual se ejecutaba en paralelo cuando la imagen era abierta.

INFORME EJECUTIVO

Perito Forense: Gabriela Granda

Fecha: 24-02-2015

Adjunto: Fichas (1-9), Ilustración 25,26,27

Se recibió una solicitud del Consejo de la Judicatura y de la Fiscalía para realizar la investigación, sobre los delitos tipificados como “Interceptación ilegal de datos” y “Acceso no consentido a un sistema informático, telemático o de telecomunicaciones” que sufrió el Sr. José Granda, el mismo que ha dado la autorización para realizar los diferentes procesos que mantiene la metodología a seguir.

Como bien la metodología indica se han cumplido con los artículos 482, 456, 480, 478 del Código Integral Penal.

Mediante el análisis realizado se ha logrado identificar la imagen con la que el atacante logro tomar el control y robar información sensible.

La Imagen con etiqueta “02ImgImagenJPG” contenía una un archivo.exe en su cabecera el cual se ejecutaba en paralelo cuando la imagen era abierta.

CAPÍTULO V. ANÁLISIS DE RESULTADOS

Una vez terminada la aplicación de la metodología, los resultados son satisfactorios pues se logra alcanzar el objetivo de encontrar cual fue el causante o provocador del delito, en este caso la imagen con el software oculto.

Por otro lado los pasos de la metodología explican cada acción a realizar con el fin de no comprometer la integridad de la evidencia, por lo que en varias ocasiones se realiza la verificación de la integridad con lo que la investigación y los resultado de la misma tendrán mayor aceptación en el ámbito jurídico, pues una cadena de custodia bien llevada es sinónimo de una investigación limpia y sin negligencias.

Como se presenta en cada fase, las diferentes fichas también aportan mayor credibilidad pues con estas se puede saber qué cambios sufrió la evidencia, que software fue utilizado para analizarla y que resultados se obtuvieron de igual forma aporta en el fortalecimiento de la cadena de custodia pues es un documento donde constaran los nombres de cada uno de los custodios en cada fase acompañados de la firma de un notario o testigo quienes certifican la validez del proceso realizado.

Las directrices presentadas para la realización del Informe Técnico y Ejecutivo, ayudan para que se pueda realizar de una manera simplificada pero al mismo tiempo entendible por el público al que va dirigido y de esta manera agilizar la presentación en la corte.

La metodología presenta varias herramientas tanto comerciales como libres que nos ayudan durante el proceso de investigación, por lo que la hace versátil al momento de aplicarla.

Debido a que en el ejemplo presentado no se trabajó con otras extensiones de imágenes no se pudo encontrar un estimado de información oculta que devuelve el software xStegSecret, sin embargo se logró conocer la herramienta con la que se realizó la incrustación y ocultación de la información, y a breves rasgos se pudo conocer de qué tipo de información se trataba.

CONCLUSIONES Y RECOMENDACIONES

- La metodología presentada podrá ser utilizada para realizar investigaciones forenses ya que tiene una alta posibilidad de ser aceptada en una corte judicial pues fue desarrollada bajo directrices proporcionadas por guías y buenas prácticas como son el RFC-3227 y Examinación Forense de Evidencia Digital de [58]NIJ-EEUU.

- Esta metodología contiene referencias hacia artículos presentes en el Código Orgánico Integral Penal (COIP) vigente en el Ecuador, de esta forma se trabaja bajo el marco legal Ecuatoriano, haciendo que la metodología sea más funcional no solo en el ámbito técnico sino que ante una corte judicial este tendrá mayor valor jurídico.

- Mediante el análisis del COIP eh encontrado que este contiene artículos orientados hacia las ciencias forenses dando mayor detalle a la medicina, creando un vacío en las investigación referentes a la informática forense por lo que en esta metodología se han utilizado como referencias los artículos que aunque no han sido creados para uso en la informática, nos ayudan a crear un camino en la investigación y análisis en caso de existir un delito informático.

- De acuerdo a las directrices que proporcionan las guías y buenas prácticas mencionadas, la metodología creada contiene seis fases en las cuales se proporciona herramientas con las que se podrá trabajar durante la investigación, haciendo de esta una metodología práctica y flexible pues presenta herramientas comerciales como de uso libre.

- La cadena de custodia durante una investigación forense es vital, por lo que la metodología creada contiene diferentes fichas que deberán ser llenadas a lo largo de la investigación con el fin de que al culminar dicha investigación, se pueda presentar una documentación precisa y completa de cada una de las

[58]NIJ, Instituto Nacional de Justicia de EEUU

acciones realizadas sobre la evidencia recogida, haciendo que los resultados obtenidos de la investigación tengan mayor probabilidad de ser aceptados en una corte judicial.

- El mantenimiento de la integridad de la evidencia recolectada es uno de las características primordiales en una investigación forense, por lo que en la metodología creada se a echo énfasis en la verificación y preservación de la integridad, recomendando herramientas y procesos para esta tarea.

- Con la aplicación de esta metodología se podrá llegar a conocer cuál fue el desencadenante de un delito informático, es decir se evalúa tanto imágenes como textos sospechosos buscando softwares maliciosos o códigos incrustados en estos archivos.

- La aplicación de la metodología presentada busca dar soluciones a los delitos informáticos que se han venido presentando hasta la actualidad en el Ecuador, proporcionando directrices para una correcta investigación, teniendo como punto fuerte la aplicación de ciertos artículos del COIP los mismos que apoyaran los resultados obtenido.

REFERENCIAS BIBLIOGRÁFICAS

[1] RENATO JAVIER JIJENA LEIVA, "LA CRIMINALIDAD INFORMATICA: SITUACION DE LEGE DATA Y LEGE FERENDA EN CHILE," *Informática y Derecho*, 1994.

[2] Mercedes Salcedo Cifuentes, "La evidencia Fisica o Elementos Motivos de Prueba," in *Manejo de la evidencia física de posible fuente biológica*.: Universidad del Valle, 2007, p. 107 Páginas.

[3] Pleno del Congreso Nacional del Ecuador, "LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS," , Quito, 2002.

[4] GENERALIDADES Y PRINCIPIOS DE LA IF. GENERALIDADES Y PRINCIPIOS DE LA IF. [Online]. https://docs.google.com/document/d/1_uCOcecybF3sQMC_ApE373xob9xyXLx2CWZfrzxBwoY/edit

[5] Centro de Posgrados y Actualización Profesional en Informática (CPAP). Centro de Posgrados y Actualización Profesional en Informática (CPAP). [Online]. http://www.fing.edu.uy/cpap/cursos/metodolog%C3%ADas-para-el-an%C3%A1lisis-forense-inform%C3%A1tico

[6] EC-Council, "EC-Council," in *Computer Forensics Investigating Data and Image Files*. USA: EC-Council, 2010, p. 227.

[7] Luis Enrique Arellano, "La cadena de Custodia Informático Forense," *ACTIVA*, no. 3, pp. 67-81, 2012.

[8] Amped Software. Amped Software. [Online]. http://ampedsoftware.com/es/features

[9] E-fense. [Online]. http://www.e-fense.com/live-response.php

[10] StegSecret. A simple steganalysis tool. [Online]. http://stegsecret.sourceforge.net/

[11] SketchUp. SketchUp. [Online]. http://www.sketchup.com/es/download/sketchup-make/windows/thank-you

[12] Pablo Katcheroff Alexis Burgos, "Problemas de Funcionamiento," in *Tecnico en Windows*., 206, ch. 3, p. 115.

[13] AccessData. AccessData. [Online]. http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.3.0

[14] Luke Pascoe. MD5Summer. [Online]. http://www.md5summer.org/about.html

[15] Chirstopher Grenier. PhotoRec ES. [Online]. http://www.cgsecurity.org/wiki/PhotoRec_ES

[16] Niels Provos. Ubuntu Manuals. [Online]. http://manpages.ubuntu.com/manpages/hardy/man1/stegdetect.1.html#contenttoc7

[17] WetStone Technologies. WetStone Stego Suit. [Online]. https://www.wetstonetech.com/product/stego-suite/

[18] WetStone Technologies. WetStone StegoHunter. [Online]. https://www.wetstonetech.com/product/stegohunt/

[19] Bless Hex Editor. [Online]. http://home.gna.org/bless/

[20] Users Staff, "Hacking," in *Hacking desde Cero*.: USERSHOP, p. 37.

[21] Certificacion Electronica Banco Central del Ecuador. Certificacion Electronica Banco Central del Ecuador. [Online]. https://www.eci.bce.ec/

[22] Alejandro Reyes Plata, "Ethical Hacking," Mexico, 2010.

[23] José Vladimiro Rivera Ramos, "CICLO DE VIDA DE UNA PRUEBA DE PENETRACIÓN FÍSICA," Guatemala, 2011.

[24] A/S Rodrigp Guirado, CISA, and CGEIT, "Penetration Testing - Conceptos generales y situación actual," 2009.

[25] Victor H. Montero, "Técnicas del Penetration Testins," Buenos Aires, Argenina, 2005.

[26] Ronald L. Vines, Russell Dean Krutz, *CEH Prep Guide : The Comprehensive Guide to Certified Ethical Hacking*. Hoboken, NJ, USA : Wiley Publishing. INC, 2008.

[27] Kimberly Graves, *CEH : Certified Ethical Hacker Study Guide*. Hoboken, NJ, USA : Sybex , 2010.

[28] José Cegarra Sánchez, *Metodología de la investigación científica y técnológica*. Madrid: Dias Santos, 2011.

[29] Ecuador en Cifras. [Online]. http://www.ecuadorencifras.gob.ec/

[30] WetStone Technologies. WetStone. [Online]. https://www.wetstonetech.com/product/stegohunt/

[31] INEC. Instituto Nacionar de Esctadisticas y Censos. [Online]. http://www.ecuadorencifras.gob.ec/

ANEXOS

ANEXO A

- **Ficha 1**

Ficha de Peritos forense que se encargaran del análisis forense por etapas.

FICHA N°1 PERITOS FORENSES CADENA DE CUSTODIA		
Fecha		
Etapa de Investigación	**Nombre Perito Forense (Custodio)**	
Identificación de Evidencia	**HARDWARE**	
	SOFTWARE	
Extracción de Evidencia	**HARDWARE**	
	SOFTWARE	
Transporte de Evidencia	**HARDWARE**	
	SOFTWARE	
Preservación de la evidencia	**HARDWARE**	
	SOFTWARE	
Verificación y Extracción de datos ocultos	**IMÁGENES**	
	DATOS (TEXTO PLANO)	
Informes Final: Informe Técnico y Ejecutivo		
_____ **FIRMA NOTARIO – TESTIGO**		
Universidad Politécnica Salesiana **METODOLOGÍA PARA EL ANÁLISIS FORENSE DE DATOS E IMÁGENES DE ACUERDO A LAS LEYES DEL ECUADOR**		

- **Ficha 2**

Ficha de información personal de los peritos forenses a cargo de la investigación.

FICHA N° 2 FICHA PERSONAL PERITOS FORENSES	
Fecha	
Cedula de identidad	
Nombres	
Apellidos	
Dirección	
Teléfono	
Correo Electrónico	
Especialización	
Firma	
Universidad Politécnica Salesiana *METODOLOGÍA PARA EL ANÁLISIS FORENSE DE DATOS E IMÁGENES DE ACUERDO A LAS LEYES DEL ECUADOR*	

- **Ficha 3**

Ficha de Registro para objetos físicos (dispositivos informáticos y telemáticos).

FICHA N°3 FICHA DE REGISTRO HARDWARE		
Nombre del Perito Forense		
Fecha		
Hora		
Número de Registro / Etiqueta	**Tipo de Dispositivo**	**Número de Serie**
Modelo	**Características**	**Numero de Fotografías**
Sistema Operativo	**Estado**	**Ubicación**
	Prendido	
	Apagado	
Descripción General		
Observaciones		
FIRMA PERITO FORENSE	**FIRMA NOTARIO – TESTIGO**	

- **Ficha 4**

Ficha de Registro para evidencia digital (archivos, imágenes).

FICHA N° 4 FICHA DE REGISTRO EVIDENCIA DIGITAL	
Nombre Perito Forense	
Fecha	
Hora	
Número de Registro / Etiqueta	
Nombre del Archivo	**Hora de última modificación**
Tipo de Archivo (Formato)	**Fecha de última modificación**
Medio en el que se encuentra almacenado	**Fecha de creación**
Ubicación	**Fecha de ultimo acceso**
Tamaño en Disco	**Tamaño**
Permisos del sistema	**Usuarios o Grupos al que pertenece**
Dimensiones (píxeles)	
Resolución Horizontal	
Resolución Vertical	
Profundidad en Bits	
Compresión	
Unidad de Resolución	
Representación de Color	
Número de Hojas (Documento)	

Software utilizado para la extracción	Hora de última modificación
Medio en el que se almacena la evidencia	**Fecha de última modificación**
Formato de almacenamiento de la información	
Descripción General	
Observaciones	
FIRMA PERITO FORENSE	**FIRMA NOTARIO – TESTIGO**

- **Ficha 5**

Ficha de Extracción y Transporte de objetos físicos (dispositivos informáticos y telemáticos).

FICHA N°5 FICHA DE EXTRACCIÓN Y TRANSPORTE DE EVIDENCIA HARDWARE		
Nombre del Perito Forense		
Fecha		
Hora		
Número de Registro / Etiqueta		
Estado de Dispositivo	**Prendido**	
	Apagado	
Hora de Apagado de dispositivo	**Fecha de Apagado de dispositivo**	
Medio de Almacenamiento	**Medio de Transporte**	
Nombre de Persona que Transporta Dispositivo	**Placas del medio de Transporte**	
Observaciones		
_____ **FIRMA PERITO FORENSE** _____ _____ **FIRMA NOTARIO / TESTIGO** **FIRMA DE P. TRANSPORTE**		
Universidad Politécnica Salesiana ***METODOLOGÍA PARA EL ANÁLISIS FORENSE DE DATOS E IMÁGENES DE ACUERDO A LAS LEYES DEL ECUADOR***		

- **Ficha 6**

Ficha de adquisición de evidencia digital (archivos, imágenes).

FICHA N°6 FICHA DE EXTRACCIÓN Y TRANSPORTE DE EVIDENCIA DIGITAL	
Nombre del Perito Forense	
Fecha	
Hora	
Número de Registro / Etiqueta	
Nombre del Archivo	
Herramienta de extracción	
Hora de Extracción	**Fecha de Extracción**
Medio de Almacenamiento (Dispositivo)	**Formato de Almacenamiento**
Número de Registro / Etiqueta de Medio de Almacenamiento	**Nombre de Persona que Transporta Dispositivo**
Medio de Transporte	**Placas del medio de Transporte**
Método de seguridad aplicado	**Formato de Almacenamiento**
Perdida de confiabilidad :	
Integridad	
Autenticidad	
Confidencialidad	
Observaciones	

_____

FIRMA PERITO FORENSE

_____ _____

FIRMA NOTARIO / TESTIGO **FIRMA DE P. TRANSPORTE**

- **Ficha 7**

Ficha de Preservación de la Evidencia

FICHA N°7 FICHA DE PRESERVACIÓN DE LA EVIDENCIA	
Nombre del Perito Forense	
Fecha	
Hora	
Número de Registro / Etiqueta	
Nombre del Archivo	
Tipo de Dispositivo	
Tipo de Clonación	**Herramienta de Clonación**
Hora de Inicio de Clonación	**Hora de fin de clonación**
Fecha de clonación	
Medio de Almacenamiento del Clon	**Número de Registro o etiqueta del Clon**
Observaciones	
_____ FIRMA PERITO FORENSE	_____ FIRMA NOTARIO - TESTIGO
Universidad Politécnica Salesiana *METODOLOGÍA PARA EL ANÁLISIS FORENSE DE DATOS E IMÁGENES DE ACUERDO A LAS LEYES DEL ECUADOR*	

- **Ficha 8**

Ficha para el análisis y extracción de información oculta en imágenes

FICHA N° 8 FICHA DE VERIFICACIÓN Y EXTRACCIÓN DE INFORMACIÓN OCULTA EN IMÁGENES		
Nombre del Perito Forense		
Fecha		
Hora		
Número de Registro / Etiqueta		
Nombre del Archivo		
Información oculta	**SI**	
	NO	
Herramienta utilizada para estegoanálisis		
Tamaño aproximado de información oculta (bytes)		
Algoritmo utilizado en la herramienta de estegoanálisis		
Herramienta esteganografía utilizada		
Información oculta		
Imagen (Incautada)	**Imagen Procesada (Estegoanálisis)**	
Observaciones		
_____ **FIRMA PERITO FORENSE**	_____ **FIRMA NOTARIO – TESTIGO**	
Universidad Politécnica Salesiana **METODOLOGÍA PARA EL ANÁLISIS FORENSE DE DATOS E IMÁGENES DE ACUERDO A LAS LEYES DEL ECUADOR**		

- **Ficha 9**

Ficha para el análisis y extracción de información oculta en texto plano

FICHA N° 9 FICHA DE VERIFICACIÓN Y EXTRACCIÓN DE INFORMACIÓN OCULTA EN TEXTO PLANO		
Nombre del Perito Forense		
Fecha		
Hora		
Número de Registro / Etiqueta		
Nombre del Archivo		
Información oculta	**SI**	
	NO	
Herramienta utilizada para estegoanálisis		
Tamaño aproximado de información oculta (bytes)		
Algoritmo utilizado en la herramienta de estegoanálisis		
Herramienta esteganografía utilizada		
Información oculta		
Observaciones		
_____ **FIRMA PERITO FORENSE**	_____ **FIRMA NOTARIO – TESTIGO**	
Universidad Politécnica Salesiana ***METODOLOGÍA PARA EL ANÁLISIS FORENSE DE DATOS E IMÁGENES DE ACUERDO A LAS LEYES DEL ECUADOR***		

ANEXO B

- **Ficha N°1**

Ficha N°1 Peritos Forenses Cadena de Custodia		
Fecha	**24-02-2015**	
Etapa de Investigación	**Nombre Perito Forense (Custodio)**	
Identificación de Evidencia	**HARDWARE**	**Gabriela Granda**
	SOFTWARE	**Gabriela Granda**
Extracción de Evidencia	**HARDWARE**	**Gabriela Granda**
	SOFTWARE	**Gabriela Granda**
Transporte de Evidencia	**HARDWARE**	**Gabriela Granda**
	SOFTWARE	**Gabriela Granda**
Preservación de la evidencia	**HARDWARE**	**Gabriela Granda**
	SOFTWARE	**Gabriela Granda**
Verificación y Extracción de datos ocultos	**IMÁGENES**	**Gabriela Granda**
	DATOS (TEXTO PLANO)	**Gabriela Granda**
Informes Final: Informe Técnico y Ejecutivo	**Gabriela Granda**	
_____ **FIRMA NOTARIO - TESTIGO**		

- **Ficha N°2**

Ficha N°2 Ficha Personal Peritos Forenses	
Fecha	**24-02-2015**
Cedula de identidad	**0105140933**
Nombres	**Gabriela Estefanía**
Apellidos	**Granda Tonato**
Dirección	**Yhanaurco y Colta**
Teléfono	**0987180944**
Correo Electrónico	**ggrandat@est.ups.edu.ec**
Especialización	**Ingeniero de Sistemas**
Firma	

Universidad Politécnica Salesiana
METODOLOGÍA PARA EL ANÁLISIS FORENSE DE DATOS E IMÁGENES DE ACUERDO A LAS LEYES DEL ECUADOR

- **Ficha N°3**

FICHA N°3 FICHA DE REGISTRO HARDWARE			
Nombre del Perito Forense	Gabriela Granda		
Fecha	24-02-2015		
Hora	13:37		
Número de Registro / Etiqueta	Tipo de Dispositivo		Número de Serie
01DisLAPSONYBLAN	Laptop Computadora Portátil		SVE14118EXW
Modelo	Características		Numero de Fotografías
Sony Vaio	Memoria RAM: 8 GB Tipo de Sistema: 64 bits Procesador: Intel Core i5-2450		001
Sistema Operativo	Estado		Ubicación
Windows 8.1 Pro 64 bits	Prendido	x	Esquina Izquierda
	Apagado		
Descripción General			
Computadora Sony Vaio, elaborada en el año 2012 color blanca, rayones en su base, teclado desgastado.			
Observaciones			
El dispositivo se encontró prendido por lo que se procederá a la extracción de la memoria RAM, se encontró abierta un imagen de nombre imagen.bmp, la misma que será analizada.			
_____ **FIRMA perito forense**		_____ **FIRMA NOTARIO – TESTIGO**	

- **Ficha N°4**

FICHA N° 4 FORMULARIO DE REGISTRO EVIDENCIA DIGITAL	
Nombre Perito Forense	Gabriela Granda
Fecha	18-02-2015
Hora	9:44
Número de Registro / Etiqueta	01ImgImagenBMP
Nombre del Archivo	**Hora de última modificación**
Imagen.bmp	
Tipo de Archivo (Formato)	**Fecha de última modificación**
Imagen de mapas de bits	
Medio en el que se encuentra almacenado	**Fecha de creación**
Disco Duro	18 Febrero de 2015
Ubicación	**Fecha de ultimo acceso**
C:\Users\Gabiru\Desktop\TESIS\programas\ Esteganografia\datos e imagens con contenido oculto\imagenes\bmp	18 de Febrero de 2015 / 9:44
Tamaño en Disco	**Tamaño**
1.98 MB	1.97MB
Permisos del sistema	**Usuarios o Grupos al que pertenece**
Control Total **Modificar** **Lectura y Ejecución** **Lectura** **Escritura**	System Gabiru Granda Administradores
Dimensiones (píxeles)	720 x 960
Resolución Horizontal	720 píxeles
Resolución Vertical	960 píxeles
Profundidad en Bits	24

Compresión	
Unidad de Resolución	
Representación de Color	
Número de Hojas (Documento)	
Software utilizado para la extracción	**Hora de última modificación**
Medio en el que se almacena la evidencia	**Fecha de última modificación**
Disco Duro My Passport 1 TB	
Formato de almacenamiento de la información	Imagen Comprimida en Zip
Descripción General	
No tiene atributos de solo lectura Los permisos del sistema son los mismos que tienen todos los usuarios.	
Observaciones	
La Imagen Recogida es la se encontró abierta en el momento de la incautación	
_____ **FIRMA PERITO FORENSE**	_____ **FIRMA NOTARIO – TESTIGO**

- **Ficha N°5**

FICHA N°5 FICHA DE EXTRACCIÓN Y TRANSPORTE DE EVIDENCIA HARDWARE		
Nombre del Perito Forense	Gabriela Granda	
Fecha	24-02-2015	
Hora	16-12	
Número de Registro / Etiqueta	01DisLAPSONYBLAN	
Estado de Dispositivo	**Prendido**	X
	Apagado	
Hora de Apagado de dispositivo	**Fecha de Apagado de dispositivo**	
17:00	24-02-2015	
Medio de Almacenamiento	**Medio de Transporte**	
Envoltorio Plástico de Burbujas	Automóvil	
Nombre de Persona que Transporta Dispositivo (Nuevo Custodio)	**Placas del medio de Transporte**	
Gabriela Granda	ABC2211	
Observaciones		
La evidencia ha sido empacada tal como dicta la metodología.		
_____ **FIRMA PERITO FORENSE**		
_____ **FIRMA NOTARIO / TESTIGO**	_____ **FIRMA DE P. TRANSPORTE**	
Universidad Politécnica Salesiana ***METODOLOGÍA PARA EL ANÁLISIS FORENSE DE DATOS E IMÁGENES DE ACUERDO A LAS LEYES DEL ECUADOR***		

- **Ficha N°6**

FICHA N°6 FORMULARIO DE EXTRACCIÓN Y TRANSPORTE DE EVIDENCIA DIGITAL	
Nombre del Perito Forense	Gabriela Granda
Fecha	24-02-2015
Hora	16:21
Número de Registro / Etiqueta	01VolcRAM
Nombre del Archivo	01VolcRAM
Herramienta de extracción	
AccessData FTK Imager	
Hora de Extracción	**Fecha de Extracción**
15:26:14	15:36:33
Medio de Almacenamiento (Dispositivo)	**Formato de Almacenamiento**
Disco Duro My Passport	Men
Número de Registro / Etiqueta de Medio de Almacenamiento	**Nombre de Persona que Transporta Dispositivo**
01VolcRAM	Gabriela Granda
Medio de Transporte	**Placas del medio de Transporte**
Automóvil	ABC2211
Método de seguridad aplicado	**Formato de Almacenamiento**
Hash MD5	Mem
Perdida de confiabilidad :	
Integridad	no
Autenticidad	No
Confidencialidad	No
Observaciones	
EL volcado de memoria se realizó directamente en el DVD-R por lo que no se lo almaceno con otro formato. Hash MD5: 7b574e4ff0768280bf46b1d743f76636 *01VolcRAM.mem El tamaño del volcado es de 9.24 GB	

_____ FIRMA PERITO FORENSE
_____ _____ FIRMA NOTARIO / TESTIGO FIRMA DE P. TRANSPORTE

- **Ficha N°7**

FICHA N°7 FICHA DE PRESERVACIÓN DE LA EVIDENCIA	
Nombre del Perito Forense	Gabriela Granda
Fecha	24-02-2015
Hora	17:19
Número de Registro / Etiqueta	01DisHDHitachi
Nombre del Archivo	clonacion.001
Tipo de Dispositivo	Disco Duro
Tipo de Clonación	**Herramienta de Clonación**
Bit a Bit	AccessData FTK Imager
Hora de Inicio de Clonación	**Hora de fin de clonación**
17:04:43	18:09:20
Fecha de clonación	
Martes, 24 de Febrero del 2015	
Medio de Almacenamiento del Clon	**Número de Registro o etiqueta del Clon**
Disco Duro My Pasport	01DisHDHitachiClon
Observaciones	
EL hash de la clonación del Disco duro es 3e3bce552f87cbba58ce8ef2b2287687.	
_____ **FIRMA Perito forense**	_____ **FIRMA NOTARIO – TESTIGO**

FICHA N°7 FICHA DE PRESERVACIÓN DE LA EVIDENCIA	
Nombre del Perito Forense	Gabriela Granda
Fecha	24-02-2015
Hora	18:04
Número de Registro / Etiqueta	01VolcRAM
Nombre del Archivo	01VolcRAM
Tipo de Dispositivo	Memoria RAM
Tipo de Clonación	**Herramienta de Clonación**
Volcado de Memoria RAM	AccessData FTK Imager
Hora de Inicio de Clonación	**Hora de fin de clonación**
17:04:43	17:10:20
Fecha de clonación	
Martes 24 de Febrero del 2015	
Medio de Almacenamiento del Clon	**Número de Registro o etiqueta del Clon**
DVD-R	01VolcRAMCLON
Observaciones	
La clonación del Volcado de memoria realizado ha sido comprobada con el hash del volcado original teniendo una respuesta positiva pues si coincidieron. Siendo el hash 7b574e4ff0768280bf46b1d743f76636	
_____ **FIRMA Perito forense**	_____ **FIRMA NOTARIO – TESTIGO**

- **Ficha N°8**

FICHA N° 8 FORMULARIO DE VERIFICACIÓN Y EXTRACCIÓN DE INFORMACIÓN OCULTA EN IMÁGENES		
Nombre del Perito Forense	Gabriela Granda	
Fecha	24-02-2014	
Hora	18:46	
Número de Registro / Etiqueta	02ImgImagenJPG	
Nombre del Archivo	Image.jpg	
Información oculta	**SI**	**X**
	NO	
Herramienta utilizada para estegoanálisis	Paquete StegDetect	
Tamaño aproximado de información oculta (bytes)		
Algoritmo utilizado en la herramienta de estegoanálisis	Algoritmo de inserción no aleatorio, suma tamaños de los dos archivos.	
Herramienta esteganografía utilizada	JPHIDE	
Información oculta		
Imagen (Incautada)	**Imagen Procesada (Estegoanálisis)**	
		
Observaciones		
_____ FIRMA Perito forense	_____ **FIRMA NOTARIO – TESTIGO**	
Universidad Politécnica Salesiana **METODOLOGÍA PARA EL ANÁLISIS FORENSE DE DATOS E IMÁGENES DE ACUERDO A LAS LEYES DEL ECUADOR**		