ANÁLISIS DE LA EVIDENCIA DIGITAL EN COLOMBIA COMO SOPORTE JUDICIAL DE DELITOS INFORMÁTICOS MEDIANTE CADENA DE CUSTODIA

DIEGO ARMANDO RAMÍREZ RIVEROS
ELMER FRANCISCO CASTRO SERRATO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VILLAVICENCIO
2018

ANÁLISIS DE LA EVIDENCIA DIGITAL EN COLOMBIA COMO SOPORTE JUDICIAL DE DELITOS INFORMÁTICOS MEDIANTE CADENA DE CUSTODIA

DIEGO ARMANDO RAMÍREZ RIVEROS
ELMER FRANCISCO CASTRO SERRATO

Informe final de proyecto aplicado para optar el título de
Especialista en Seguridad Informática

Director
ING. FRANCISCO JAVIER HILARIÓN NOVOA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VILLAVICENCIO
2018

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Villavicencio, diciembre de 2017

A Dios primero que todo, ya que gracias a él que nos guía es que todos nuestros proyectos y sueños se hacen realidad.

A nuestras excelentes madre Mercedes Riveros y María Hilda Serrato quienes siempre han sido siempre incondicionales y siempre apoyándonos en todas nuestras etapas de vida.

A nuestras bellas esposas Alejandra y Maricela y nuestros hermosos hijos Alejandro y Santiago ya que ellos son el motor que nos impulsa día a día a ser no solo mejores personas sino mejores profesional…Gracias.

AGRADECIMIENTOS

A todos y cada uno de los ingenieros y tutores que han hecho parte de este proceso de formación y que han contribuido de cierta manera para la culminación exitosa de este ciclo de aprendizaje.

De igual forma quiero dar un agradecimiento muy especial a la Universidad UNAD ya que como centro educativo y de formación siempre inculca los mejores valores para que como estudiantes y profesionales siempre aportemos nuestro grano de arena a nuestras regiones y al país.

A la corporación de alta tecnología para la defensa CODALTEC y a la Secretaría de TIC/CTeI de la Gobernación del Meta, que son los lugares donde trabajamos y nos han brindado los espacios necesarios para culminar este proceso educativo.

A nuestras familias que es la fuente que nos motiva siempre a hacer las cosas de la mejor manera posible.

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

INTRODUCCIÓN

Con la llegada de las nuevas tecnologías de la información, el fácil acceso a las mismas y al internet, se hace necesario resguardar uno de los activos más importantes hoy en día, dicho activo es la información; la seguridad informática busca proteger los diversos recursos tecnológicos inherentes a la operación de la empresa o entidad, estamos hablando de hardware y software, y a su vez se busca que estos sean utilizados de manera adecuada. La seguridad de la información se basa en tres principios: confidencialidad, integridad y disponibilidad[1].

La informática forense surge por la necesidad de investigar incidentes o delitos informáticos, es decir, se aplican una serie de métodos con el fin de obtener Información, datos o evidencias que puedan estar en un equipo de cómputo o sistema de información, que se haya visto involucrado en algún acto delictivo.

La cadena de custodia busca dar el tratamiento adecuado a las pruebas digitales que se puedan presentar en alguna investigación de delitos informáticos, debido a esto se deben establecer los procesos o métodos necesarios para la correcta recolección de dichas pruebas, evitando perdidas, daños o destrucción de las mismas[2].

Teniendo en cuenta lo mencionado anteriormente, se realizará un estudio del proceso de cadena de custodia y su aplicación en investigaciones de delitos

[1]Seguridad informática en Colombia. [en línea]. [citado en Febrero de 2016]. Disponible en Internet: http://seguridadinformacioncolombia.blogspot.com.co/2010/02/seguridad-de-la-informacion-y-seguridad.html

[2]La cadena de custodia aplicada a la informática, [en línea]. [citado en Febrero de 2016]. Disponible en Internet:http://www.informaticoforense.eu/la-cadena-de-custodia-aplicada-a-la-informatica-i/

informáticos en Colombia, se identificarán las posibles falencias y mejoras de este proceso.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

Falta de un estudio del proceso de cadena de custodia en la investigación de delitos informáticos para contribuir a identificar las falencias en el tratamiento de pruebas digitales que puedan ocasionar pérdidas, daños o destrucción de las mismas en procesos judiciales.

1.2 DESCRIPCIÓN DEL PROBLEMA

La cadena de custodia es un proceso o protocolo el cual debe seguirse para el tratamiento de una prueba por cierto tiempo que puede ser hasta que la prueba deje de ser válida o sea innecesaria. Según este proceso, se debe controlar la trazabilidad y la historia de la prueba, se debe conocer y referenciar quien, cuando, donde, ha tenido acceso a ella, entre otros ítems.

La creciente ola de delitos informáticos en el país, ha generado que las investigaciones y el proceso de cadena de custodia también aumenten, adoptando siempre las mejores prácticas respecto al manejo de las diferentes evidencias encontradas en equipos de cómputo, sistemas de información y demás elementos que se vean involucrados en los incidentes.

Teniendo en cuenta que la informática forense y el proceso de cadena de custodia aplicado a investigaciones de delitos informáticos en el país son relativamente nuevos, se pueden presentar diversos eventos que hagan que las evidencias digitales sean tratadas de manera incorrecta, ocasionando pérdidas de información, entre otras; lo anterior puede generar que los casos de investigación de delitos informáticos no lleguen a buen término para los directamente afectados.

1.3 FORMULACIÓN DE INVESTIGACIÓN

¿Cómo el estudio del proceso de cadena de custodia en la investigación de delitos informáticos puede contribuir a identificar las falencias en el tratamiento de pruebas digitales que puedan ocasionar pérdidas, daños o destrucción de las mismas en procesos judiciales?

2. JUSTIFICACIÓN

Dado el incremento en el uso de la tecnología, y el manejo de información de toda índole, la cual es tratada por los diferentes canales y medios tecnológicos, también es de conocer que existe gran cantidad de interesados en sacar provecho de sus conocimientos y aplicarlos para vulnerar la seguridad de dichos canales, logrando obtener algún tipo de beneficio.

La presente investigación tiene como propósitos, inicialmente revisar la documentación pertinente a la seguridad informática enfocada a la informática forense y más específicamente al manejo que se le da a las evidencias que se obtienen como resultado de investigaciones de delitos informáticos en nuestro país; de igual forma se pretende analizar este proceso con el fin de identificar las falencias que puedan existir y finalmente se busca documentar las mejoras y contribuir a las buenas prácticas del proceso de cadena de custodia y su aplicación en la investigación de delitos informáticos en Colombia.

Se busca por medio del presente proyecto aplicado, beneficiar de algún modo a peritos e investigadores informáticos, así como también a los responsables del proceso de cadena de custodia ya que al identificar las falencias y posibles mejoras para este proceso, se tendrá un punto de referencia respecto a como se viene llevando a cabo dicho proceso con el fin de obtener mejores resultados y de manera más eficiente.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Identificar las falencias en el tratamiento de pruebas digitales que puedan ocasionar pérdidas, daños o destrucción de las mismas en procesos judiciales por medio del estudio del proceso de cadena de custodia en la investigación de delitos informáticos en Colombia

3.2 OBJETIVOS ESPECÍFICOS

- ✓ Realizar el reconocimiento del proceso de custodia y su aplicación en la investigación de delitos informáticos en Colombia.

- ✓ Identificar las posibles falencias existentes en el proceso de custodia y su aplicación en la investigación de delitos informáticos en nuestro país.

- ✓ Realizar un informe de identificación con las posibles mejoras sobre el proceso de custodia de pruebas digitales para evitar pérdidas, daños o destrucción de las mismas y su aplicación en la investigación de delitos informáticos en Colombia.

4. MARCO REFERENCIAL

4.1 ANTECEDENTES

La seguridad informática y lo relacionado con delitos informáticos en Colombia, es un tema relativamente nuevo; la informática forense se introduce como una serie estructurada de pasos que permiten la recolección, análisis y tratamiento de evidencia digital con el fin de dar solución a algún incidente de seguridad informática.

Como referencia se toma algunos trabajos o monografías relacionadas con la informática forense y con la cadena de custodia.

El trabajo de grado propuesta de un modelo de procedimiento para el tratamiento de la evidencia digital, acorde a la normatividad colombiana sobre delitos informáticos, presentado por el Ingeniero Pablo Andrés Gaviria, para optar el título de especialista en seguridad informática en la Universidad Nacional Abierta y a Distancia, por medio del cual se formula un procedimiento y una guía para mejorar el tratamiento y procesamiento de la evidencia digital como medio técnico en el soporte judicial, por medio de herramientas y procedimientos forenses, el cual es orientado al personal encargado de las investigaciones desde el punto de vista técnico-científico[3].

El trabajo antes mencionado aporta al presente, conocimientos y conceptos relacionados con la informática forense, lo relacionado con el tratamiento de la información digital y cadena de custodia.

[3] PABLO ANDRES GAVIRIA. propuesta de un modelo de procedimiento para el tratamiento de la evidencia digital, acorde a la normatividad colombiana sobre delitos informáticos. Monografía. [en línea]. [Ingeniero de Sistemas]. Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas e Ingenierías

El anteproyecto de grado, manejo de evidencia digital en dispositivos de almacenamiento pendrive usb aplicando la norma iso/iec 27037:2012, presentado por el Ing. José Bernardo Cortes de la Rosa en el año 2014 en la Universidad Nacional Abierta y a Distancia, por medio del cual se establece aplicar la norma antes mencionada al momento de tratar la evidencia digital en medios de almacenamiento pendrive usb[4].

Este trabajo aporta a la presente investigación conocimientos sobre normas y procedimientos aplicados al manejo de evidencia digital.
El trabajo de grado, Diseño e implementación de un centro de informática forense en la Universidad autónoma de occidente, presentado por Guillermo Umaña Ramírez e Isabel Cristina Mosquera Navarrete en el año 2014 en dicha institución de educación superior, por medio del cual se establece los lineamientos y requerimientos necesarios para el montaje de un laboratorio forense[5].

Por medio de este trabajo, se logra tener una visión más amplia sobre las herramientas de software y hardware que se deben usar a la hora de llevar a cabo la evidencia digital.

El trabajo de grado, estado del análisis forense digital en Colombia presentado por Diego Alejandro Jaramillo y Martha Liliana Torres en la Universidad militar Nueva Granada en el año 2016, el cual platea la verificación y recolección de documentación referente a este tema con el fin de tener una visión sobre la historia y estado actual del análisis digital forense en nuestro país[6].

[4]JOSE BERNARDO CORTES DE LA ROSA. Manejo de Evidencia Digital en Dispositivos de Almacenamiento Pendrive Usb Aplicando la Norma Iso/Iec 27037:2012. Monografía.[en línea]. [Ingeniero de Sistemas].Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas e Ingenierías

[5] https://red.uao.edu.co/bitstream/10614/6473/1/T04529.pdf
[6] http://repository.unimilitar.edu.co/bitstream/10654/14401/1/TorresMoncadaMarthaLiliana2016.pdf Jaramillo, D. 2016

El anterior trabajo aporta a nuestro proyecto una referencia sobre cómo ha sido el avance del investigación y tratamiento de evidencias digitales en nuestro país desde su llegada hasta la actualidad, de igual forma permite conocer un poco más sobre la normatividad que rige este tema en Colombia.

4.2 MARCO TEÓRICO

4.2.1 Seguridad informática y de la información

Pueden sonar dos términos muy parecidos, pero en la realidad son diferentes, aunque se debe tener en cuenta que por medio de ambas se busca el mismo fin.

La seguridad informática busca proteger los diversos recursos tecnológicos inherentes a la operación de la empresa o entidad, estamos hablando de hardware y software, y a su vez se busca que estos sean utilizados de manera adecuada.

Por su parte la seguridad de la información, busca proteger la información de la empresa u organización independiente del medio en el que se encuentre almacenada. La seguridad de la información se basa en tres principios: confidencialidad, integridad y disponibilidad[7].

Al explicar en qué consiste cada una, se empieza a notar las diferencias existentes entre ambos términos; sin embargo una diferencia relevante es el manejo y tolerancia del riesgo. La seguridad informática basa su gestión de riesgos en las vulnerabilidades o posibles falencias tanto del hardware como del software tratando de disminuir el riesgo a un nivel que sea aceptado o tolerado por la empresa, entidad o institución; mientras que la seguridad de la información

[7]Seguridad informática en Colombia. [en línea]. [citado en Marzo de 2016]. Disponible en Internet: http://seguridadinformacioncolombia.blogspot.com.co/2010/02/seguridad-de-la-informacion-y-seguridad.html

busca gestionar y mitigar el riesgo a un nivel más bajo del que pueda asumir la empresa o la organización.

4.2.2 Informática forense

Surge y se divide de la seguridad informática con el fin de recolectar, analizar y validar todo tipo de evidencia digital, de igual forma se dice que es la ciencia de recopilar, almacenar y mostrar datos o información que de algún modo han sido procesados de manera electrónica y guardados en un medio informático.

Se puede decir que la informática forense es una disciplina que ayuda a la justicia hoy en día con el fin de enfrentar los diferentes delitos informáticos que se pueden cometer, de igual forma se encarga de la custodia de la evidencia digital recolectada en la escena del crimen y esta es aportada en procesos judiciales.

La informática forense se basa en una metodología estructurada que comprende varias fases y estas a su vez se dividen en etapas que buscan dar cumplimiento a las medidas de control necesarias para evitar imprecisiones a la hora del tratamiento de la información ya que el proceso bien sea legal o no se puede ver comprometido.

4.2.2.1 Fase de Identificación

Esta se lleva a cabo en el sitio específico donde sucedió el ataque informático, y se debe hacer el rotulado identificando las características físicas del elemento al cual se le hará el análisis forense; estos pueden ser desde discos duros hasta una serie de equipos de cómputo.

La etapa 1 de esta fase corresponde al levantamiento de información inicial para el análisis forense, para dar inicio debe haber una solicitud forense, que no es más que un documento suministrado por el administrador del equipo o sistema afectado donde se especifique toda la información suficiente para dar inicio al

análisis forense; dentro de la información que debe ser suministrada se encuentra la descripción del delito informático con fecha, duración y detalles del mismo.

También se debe anexar información general como el área donde se dio el ataque, nombre de la dependencia, responsable del sistema afectado, nombres y apellidos, cargo, etc. Se debe relacionar la mayor información sobre el equipo afectado, como por ejemplo dirección IP, nombre del equipo, marca y modelo, RAM, capacidad del disco duro, nombre y versión del sistema operativo, entre otras.

La etapa 2 corresponde a asegurar la escena, con el fin de cumplir con este requerimiento se necesita que el personal encargado del proceso forense esté muy bien capacitado tanto en los procesos como en las herramientas a utilizar y comprender la metodología que se debe seguir.

Se deben identificar las evidencias encontradas en la escena del crimen, esta evidencia se puede clasificar según el tipo de dispositivo como por ejemplo redes, dispositivos móviles, redes inalámbricas y otros; según el modo de almacenamiento puede ser volátiles que son aquellas que se pierden al apagar el equipo o no volátiles como los discos duros y memorias flash.

Se puede concluir que en este primer paso se identifican y buscan posibles evidencias al igual que su medio de almacenamiento y el sistema operativo utilizado, seguido a esto se procede a seleccionar las herramientas y procedimientos más adecuados para la recuperación de evidencias.

4.2.2.2 Fase de Validación y Preservación de los Datos Adquiridos

Una vez se tiene hecha la identificación, se hace una copia o imagen que sea igual al contenido de la evidencia, además se debe asignar un código único el cual corresponde a una serie de bytes que se convierten en el total del medio que se

está analizando; dicho código debe ser suficientemente seguro y complejo como para evitar que pueda ser verificado por personal no autorizado, desde este punto se empieza a tener una cadena de custodia eficiente. A partir de este punto se pueden hacer copias de la imagen para que el personal que corresponda pueda acceder a la información.

La etapa 1 de esta fase corresponde a hacer copias de la evidencia obtenida, esto se hace por medio de diversos métodos y se emplean funciones como MD5 o SHA1, esta firmas se deben incluir en la etiqueta de cada copia que se haga, debe incluir fecha y hora en que se ha creado la copia y se deben distinguir como copia 1 y copia 2 por ejemplo. Se debe tener especial cuidado con los discos duros por temas de temperatura y condiciones climáticas con el fin de preservarlos.

La etapa 2 hace referencia a la cadena de custodia donde se establecen responsables y controles sobre la evidencia. El acceso a la evidencia debe ser muy restrictivo con el fin de evitar manipulaciones incorrectas.

4.2.2.3 Fase de Análisis y Descubrimiento de la Evidencia

Se hace una serie de pruebas en el laboratorio basadas en la copia de seguridad que ha sido validada anteriormente, se puede hacer análisis y búsqueda de la información necesaria. El análisis forense se da inicio de acuerdo a la sospecha de algún tipo de ataque informático o acceso a información por personal no autorizado; cada caso o tipo de investigación se encamina de acuerdo a los sucesos y a la información suministrada por la persona u organización que hace la solicitud de la investigación forense.

Con base al análisis realizado se puede determinar el tipo de ataque y los patrones de comportamiento del atacante, entre otros. Este análisis finaliza cuando se determine la forma en que se hizo el ataque, las personas involucradas, por qué se realizó, objeto del ataque y los daños causados.

La etapa 1 consiste en la preparación para el análisis, se debe contar con un espacio o laboratorio adecuado, se debe trabajar preferiblemente con las copias de la evidencia, preferiblemente tener 2 estaciones para trabajar, instalar sistemas operativos que faciliten el manejo de las imágenes, de igual forma instalar un sistema operativo igual al del equipo afectado y hacer las simulaciones necesarias; otra alternativa es trabajar con programas de virtualización.

En la etapa 2 se hace la reconstrucción del ataque, para esto se debe crear una línea de tiempo de acuerdo a los sucesos que marquen los ficheros, como marcas de tiempo, ruta completa, tamaño y tipo de ficheros, permisos, si se borró o no.

La etapa 3 corresponde a la determinación del ataque y se hace por medio de la identificación de las vulnerabilidades que dieron pie a la realización del ataque, se valida los servicios y procesos abiertos, los puertos y las conexiones que estaban abiertas; una vez identificadas las vulnerabilidades se procede a buscar exploits anterior a la fecha del ataque que hayan hecho uso de esas vulnerabilidades, probar con las maquinas donde se tengan las imágenes de las evidencias con el fin de generar los mismos sucesos que se encuentran en las mismas.

Durante la etapa 4 se hace la identificación del atacante, para esto se puede recurrir a evidencia recolectada en las fases anteriores con el fin de validar, conexiones, servicios y puertos entre otros al igual que direcciones IP; se debe verificar los datos borrados con el fin de buscar huellas que pudieron ser borradas por el o los atacantes.

Una vez se tenga una dirección IP sospecho, se procede a validarla en el registro Ripe Ncc (www.ripe.net) para determinar a quién pertenece, se recomienda hacer uso de hacking ético para verificar si se dejó un troyano, se puede hacer uso de herramientas como Nmap para recopilar este tipo de información.

La etapa 5 consiste en identificar el perfil del atacante, entre los cuales se pueden encontrar Hackers, ScriptKiddies y Profesionales.

Por último en la etapa 6 de esta fase se lleva a cabo la evaluación del impacto causado en el sistema, se puede encontrar dos clases de ataques, los pasivos y los activos. Los ataques pasivos son aquellos donde el atacante no altera ni daña la información de la organización, solo visualiza; los ataques activos son aquellos donde la información es manipulada y se llega a causar inestabilidad en el sistema.

4.2.2.4 Informe

En esta fase corresponde la presentación de un informe escrito el cual debe ser comprensible para un usuario no especializado, se presenta un Cd que contenga la información ordenada y con la evidencia que ha sido recuperada junto con su interpretación. Es importante documentar y fechar todas las actividades que se lleven a cabo desde el inicio hasta la finalización del análisis forense con el fin de minimizar errores a la hora de gestionar los incidentes.

Durante la etapa 1 se utilizan formularios de registro del incidente que deben ser diligenciados por las áreas afectadas o por el administrador de equipos, dentro de los formularios se puede encontrar el documento de custodia de la evidencia, el de identificación de equipos y componentes, de incidencias tipificadas, publicación del incidente, recogida de evidencias, formulario de discos duros.

En la etapa 2 se procede con la elaboración del informe técnico por medio del cual se presenta de manera detallada el análisis forense realizado, este debe contener la metodología utilizada, los procedimientos y las evidencias encontradas; algunos de los ítems que debe contener el informe son la introducción, antecedentes del incidente, recolección de datos, descripción de la evidencia, entorno del análisis,

descripción de las herramientas, análisis de la evidencia, descripción del sistema operativo, aplicaciones, servicios, vulnerabilidades, metodología, hallazgos, huellas del intruso, alcance del ataque, origen del ataque, línea de tiempo, conclusiones, recomendaciones, referencias y anexos.

La etapa 3 comprende la elaboración del informe ejecutivo el cual es un documento escrito en un lenguaje poco técnico y de fácil comprensión para personal no especializado donde se describa lo sucedido y la forma en que se realizó el análisis; consta de introducción, análisis, sumario del incidente, conclusiones, solución al ataque y recomendaciones[8].

4.2.2.5 Proceso del Sistema de Cadena de Custodia

La cadena de custodia debe estar siempre ligada a un marco normativo según la ley, esta normativa a nivel mundial es igual ya que son los mismos principios, dado que la presunción de inocencia prevalece, por ende la cadena de custodia debe ser un aporte preciso y técnicamente comprobable.

En Colombia la fiscalía general de la nación entrego el manual de procedimientos para cadena de custodia, en el cual se brindan las pautas del buen proceder para su ejecución, planteando que ese documento está dirigido *"a los servidores públicos y particulares que tengan contacto con los elementos materia de prueba o evidencias físicas, involucrados en el aseguramiento y conservación de las características originales y registro de las modificaciones que sufran dichos elementos, desde su recolección hasta su disposición final*"[9]

[8] UNAD. Fases de la informática forense. [en línea]. [citado en Abril de 2016]. Disponible en Internet: http://datateca.unad.edu.co/contenidos/233012/unidad_1/u1_fases_de_la_informatica_forense.pdf

[9] FISCALIA GENERAL DE LA NACION. Sistema Penal Acusatorio Proceso penal [en línea]. [citado el 5 enero de 2012]. Disponible en Internet: http://www.fiscalia.gov.co/en/wp-content/uploads/2012/01/manualcadena2.pdf

Partiendo de este método generalizado donde se destacan sus diagramas de procesos, se puede evidencia que en primera instancia se inicia la fase de verificación y confirmación de la noticia criminal, este proceso siempre lo realiza la policía jurídica, donde nos muestra si existe material de prueba o evidencia que requiera su recolección o si solo es un bien a incautar.

Si la primera fase es positiva, se debe identificar si el elemento requiere de almacenamiento transitorio, si la prueba requiere un análisis se envía al laboratorio forense, sino simplemente se debe enviar al almacén de evidencias. Si requiere de análisis forense y el resultado de las pruebas es positivo este queda almacenado como EMP (Elementos Materiales Probatorio) o evidencia en bodega del laboratorio, partiendo del tipo del material de la evidencia encontrada. Para el caso de TIC este debería quedar bajo custodia en un almacén de evidencias. Cuando ya se tiene la evidencia resguardada en el almacén de evidencias, esta puede ser requerida judicial mente y entregada al juez que lleve el caso.

Este sería el procedimiento del sistema de cadena de custodia generalizado, dado que el caso fuese un delito informático y de ser así el juez que lo lleve y/o la fiscalía deben ordenar un peritaje informático a los equipos resguardados.

Donde la cadena de custodia no debe haber presentado ninguna falencia por parte de cuerpo policial quien decomiso los equipos ya que siempre debe estar asegurada para que la contraparte no tengan argumentos para invalidar o pronunciar que la cadena de custodia ha sido interrumpida, rota, contaminada o alterada ante el tribunal.

El método que se implemente para la cadena de custodia es fundamental para su sustentación ante el ámbito judicial y las herramientas a implementar para tal fin deben ser precisas ya que el resultado puede ser validado por otros peritos y este no debe cambiar.

En el ámbito judicial se pronuncian dos fases de la cadena de custodia una es la fase de extracción y preservación como la inicial y más vulnerable para cometer errores ya que cuando se inicia el proceso no es claro que evidencias van a encontrar el cuerpo policial y la segunda que está compuesta por su individualización, transporte apropiado y entrega controlada, la cual también está sujeta a posibles errores de procesos pero de menor vulnerabilidad.

Para no dejar cabida a pronunciamientos de la contraparte en el momento de recepcionar la evidencia tecnológica se debe realizar mediante notario que describa paso a paso los procedimientos de recolección, descripción y demás procesos que certifiquen la idoneidad y protección de la información en los equipos así como también el proceso de copia de los discos duros y memorias de los mismos, también realizando entrega oficial de la llaves publica de encriptación de la información mediante el algoritmo hash MD5 u otro si se requiere dado la cantidad de archivos almacenados en el computador.

4.2.2.6 Herramientas utilizadas en la informática forense.

Las herramientas más utilizadas por los expertos en seguridad informática e investigación forense, según Chandan Kumar son[10].

Autopsy, Programa forense digital de código abierto basado en GUI para analizar de forma eficiente los discos duros y teléfonos inteligentes, con ello un informático forense puede evidenciar y recopilar la información de lo que realmente paso en un caso de delito informático.

Sus características son:

[10] CHANDAN KUMAR. Herramientas de investigación forense. [en línea]. [citado en Septiembre 4 de 2016]. Disponible en Internet: https://geekflare.com/forensic-investigation-tools/

- Análisis de correo electrónico
- Detección de tipo de archivo
- Reproducción multimedia
- Análisis del registro
- Recuperación de fotos de la tarjeta de memoria
- Extraiga la geolocalización y la información de la cámara de archivos JPEG
- Extraer la actividad web del navegador
- Mostrar eventos del sistema en la interfaz gráfica
- Análisis de la línea de tiempo
- Extraer datos de Android: SMS, registros de llamadas, contactos, etc.

Tiene informes extensos para generar en formato de archivo HTML, XLS.

Detector de disco cifrado, es una herramienta de línea de comandos que puede comprobar de forma rápida y no intrusiva volúmenes cifrados en un sistema informático durante la respuesta a incidentes.

Investigador Forense, su diseño es un conjunto de herramientas Splunk donde la mayoría de las herramientas no necesitan acceso a internet con excepción de un par que utilizan llamadas API, sus herramientas combinadas son:

- Búsqueda WHOIS / GeoIP
- Silbido
- Escáner de puertos
- Banner grabber
- Descodificador / analizador de URL
- Convertidor XOR / HEX / Base64
- Visor SMB Share / NetBIOS
- Búsqueda total de virus

HashMyFiles, Es una herramienta que permite a los usuarios poder encriptar todo tipo de archivo recibiendo también todo tipo de extensión, donde el programa nos entrega los valores HASH en, MD5, SHA1, CRC32, donde estos valores permiten verificar la autenticidad e identidad de un archivo, lo cual permite validar si dicho documento sufrió alguna alteración, tienen algún error o modificación en su contenido, a lo cual podemos referir que el código hash es como el ADN de los documentos o archivos.

Esta herramienta también permite ver los procesos de encriptación y copiar los valores como HTML u otro tipo de documento de texto para ser publicados y con ello poder notificar del código HASH a usuarios o remitentes que requieran de la información contenida en algún documento u archivo y que esta sea verdadera la cual es respaldada por este código único.

Nmap, conocido como mapeador de red, esta herramienta permite escanear computadoras y redes enteras para validar puertos abiertos e información de modo discreto, con esta herramienta se logra evidenciar que servicios se ejecutan en un ordenador y hasta identificar el sistema operativo. Con Nmap los informáticos forenses logran evidenciar las debilidades de los firewall de red, Identificar los servicios que se ejecutan en cada equipo de una red, Determinar si una computadora revela más información sobre sí misma de lo que debería etc.

Wireshark, esta aplicación detecta todo el tráfico de una red informática, esta aplicación la usan los informáticos forenses para localizar si se envía información confidencial a través de la red en texto claro, también de forma maliciosa suplantar a otros equipos de la red para ubicar puntos vulnerables en la arquitectura de la red. También detecta un comportamiento extraño en la red que podría significar una interrupción.

Nessus, es un software que contiene una base de datos de todos los hack más actualizados con ello logramos escanear equipos y redes para detectar vulnerabilidades potenciales, se pueden aplicar parches de seguridad que pueden solucionar cualquier fallo de seguridad en una red.

Montaje de Discos, son utilidades para montar imágenes de disco o virtualizar unidades de forma que se tenga acceso al sistema de ficheros para posteriormente analizarla[11].

ImDisk, Controlador de disco virtual. Esta herramienta son alternativas de open source para la creación de discos RAM, de código abierto y por ende gratuito, donde la finalidad de esta herramienta es crear discos virtuales basados en imágenes tantos como los requiera el usuario para Windows y son administrados desde el panel de control, con una interfaz espartana pero al momento de la creación de un disco virtual se pueden evidenciar más parámetros como lo son el ajustar su letra de disco el tamaño de la unidad, el tipo de dispositivo y los privilegios de escritura.

La información que captura los discos RAM es almacenada en discos duros y son de gran importancia ya que el controlador admite el reenvió de solicitudes de E/S a manejadores de formatos de archivo de imagen de terceros como estaciones o equipos de una red, permitiendo iniciar maquinas con particiones NTFS con un Live-CD, también permite el uso de la herramienta devio para montar una partición NTFS dentro de una dañada o defectuosa.

Con todas estas características el ImDisk es un gran aliado a la hora de recuperar información de discos e incluso lograr arrancar maquinas donde Windows no lo logra mediante chkdsk.

[11] Forensics Power Tools. [en línea]. [citado en Septiembre de 2013]. Disponible en Internet: http://conexioninversa.blogspot.com.co/2013/09/forensics-powertools-listado-de.html

OSFMount, permite montar imágenes de discos locales en Windows asignando una letra de unidad. Esta herramienta nos permite montar también una imagen forense en Windows nos crea la unidad con una letra en modo de solo lectura lo cual garantiza que no se alteren los archivos de imágenes originales.

La herramienta también soporta el montaje de disco RAM permitiendo mayor velocidad al acceder a aplicaciones de bases de datos, juegos y navegadores, también bridan seguridad ya que los contenidos no son almacenados en un disco duro físico sino en la RAM y si se apaga la maquina estos no persisten.

Raw2vmdk, utilidad en java que permite convertir raw/dd a .vmdk, es una utilidad de java independiente del sistema operativo que permite montar imágenes de disco sin formato, como imágenes creadas por “dd”, utilizando VMware, VirtualBox o cual otra plataforma de Virtualización que admita el formato de disco VMDK.

Su interfaz de línea de comando es muy simple, solo debe ejecutar y montar cualquier imagen sin formato y cuenta con sistema operativo independiente.

También se cuenta con un listado de herramientas de Análisis de Memoria como los programas.

PD Proccess Dumper. Es una herramienta de ingeniería inversa de Windows para volcar los componentes de memoria o malware en el disco para su análisis. Utilizando un direccionamiento agresivo de reconstrucción de importaciones para facilitar el análisis, admite módulos de 32 y 64 bits.

Permite el volcado de regiones sin encabezados PE y en estos casos se generarán automáticamente encabezados PE y tablas de importación, permite la creación y el uso de una base de datos limpia-hash, por lo que se puede omitir el

volcado de archivos limpios como kernel32.dll. También nos permite encontrar y volcar módulos ocultos, así como fragmentos de código ejecutables.

FTK Imager, es un herramienta especializada principalmente en la adquisición de memoria RAM, permitiendo realizar replicas y visualización previa de datos, generando una evaluación rápida de invidencia electrónica y con ello determinar si se requiere realizar un análisis posterior con una herramienta forense.

Esta herramienta también crea copias perfectas pero es muy importante el uso de un bloqueador de escritura para que el sistema operativo no altere la unidad fuente original a la hora de crear la imagen forense desde un disco duro u otro dispositivo y a la hora de adjuntarlo a la computadora.

Es válido resaltar que FTK Imager al realizar una imagen duplica bit por bit de la unidad a analizar esto con el fin de evitar la manipulación accidental o intencional de la evidencia original

DumpIt; Realiza volcados de memoria a fichero de una forma muy simple ya que este software solo se debe de ejecutar y nos pregunta por medio de consola si realizamos o no un volcado de la memoria y si es positivo este se guarda en donde se encuentre el programa, Dumplt esta fusionada para win32 y win 64 en un solo ejecutable.

Una vez generado un volcado de memoria se puede verificar los archivos mediante un editor Hexadecimal, como WinHex

Herramientas de Análisis de Malware

PDF Tools, de Didier Stevens.

PDFStreamDumper, esta es una herramienta gratuita para el análisis PDFs maliciosos. Es un programa independiente que se ejecuta en Windows y contiene una interfaz gráfica muy eficiente con funcionalidades como varias firmas de Exploits PDF conocidas para escanear los documentos e identifica donde está el objeto sospechoso ejemplo un JavaScrip incrustado.

Otro parámetro es examinar Shellcode incrustado en un archivo PDF. Se utiliza generalmente para almacenar la carga de exploit o le código malicioso que se ejecuta en el sistema de la víctima, el PDFStreamDumper cuenta con la opción de "Shellcode_Analysis" la cual permite emular la ejecución de secuencias partiendo de algunas variables incorporadas como scLog, scDbg, scSig o Xor BruteForcer

SWF Mastah; Programa en Python que extrae stream SWF de ficheros PDF de e Brandon Dixon, su enfoque es poder evidenciar archivos SWF maliciosos dentro de un documento PDF con un proceso muy sencillo y automático.

Proccess Explorer, Muestra información de los procesos de forma avanzada en Windows y su gestión es rápida y fácil, se aplica desde Windows XP y en servidores desde Windows server 2003 incluyendo IA64

El explorador de proceso es una potente herramienta gráfica que no requiere instalación, permitiendo realizar una gestión avanzada de los procesos que se ejecutan en Windows. Con el explorador de procesos puede ver información detallada de los procesos, incluyendo el nombre del proceso, la línea de comandos, la ruta de la imagen completa, PID, la CPU, la descripción, la firma, nombre de la empresa, y otros valores para un completo análisis.

Captura BAT, es una herramienta de análisis que permite la monitorización de la actividad del sistema o de un ejecutable dado para la familia de sistemas

operativos de Win32, permitiendo validar como está el funcionamiento de un software e incluso si no contiene ningún código fuente disponible, el programa Captura BAT supervisa los cambios de estado a nivel de kernel bajo y se puede implementar en distintas versiones y configuraciones de SO Win32. CaptureBAT es desarrollado y mantenido por Christian Seifert del NZ Chapter.

Regshot, Crea snapshots del registro pudiendo comparar los cambios entre ellos, esto con el fin de validar alteraciones en el registro de una maquina ya sea por la instalación de algún software o programa, Regshot nos permite comparar entre un Snapshot1 y un Snapshot2 tomados rápidamente al registro mediante un archivo de texto o de formato HTML que contiene una lista de todas las modificaciones realizadas entre los dos estados de Snapshot.

FRAMEWORKS es un conjunto estandarizado de conceptos, prácticas y criterios en base al análisis forense de un caso. Los frameworks son estructuras conceptuales de soporte definido con módulos y aplicaciones concretas en el cual otro proyecto de software puede ser organizado y desarrollado como en un desarrollo web lograr evidenciar las vulnerabilidades de su código y así poder mitigar las falencias encontradas en un proyecto tecnológico

Log2timeline, Es un marco para la creación automática de una súper línea de tiempo. Su finalidad de diseño fue para extraer marcas de tiempo de varios archivos encontrados en un sistema informático típico y agregarlo.

Plaso, Evolución de Log2timeline. Framework para la creación automática de una súper línea de tiempo, convertido en un marco que admite agregar nuevos analizadores o analizar los plus-ins; agregar nuevos plug-ins de análisis y escribir guiones para automatizar tareas repetitivas en análisis forense de computadores o equivalentes. Plaso está en evolución para brindar nuevos parámetros y/o complementos de uso general que puedan no tener marcas de tiempo asociadas

a ellos, también agregando más contexto de análisis y permitiendo un enfoque más específico para la recopilación y análisis de las maquinas.

OSForensics, es una herramienta que nos permite realizar un diagnóstico forense a nuestros ordenadores trae una versión gratuita y de pago, con múltiples aplicaciones como lo es el algoritmo hash para obtener huellas digitales de cada archivo que poseemos en el ordenador y esta vienen también en la versión gratuita, con ello podemos evidenciar si un archivo fue borrado, modificado o alterado de algún modo, implementando diferentes algoritmos como MD5, SHA-1,SHA-256 entre otros, dispone de rainbow tables. Analiza datos de un disco ya montado.

Como estas herramientas existen muchas más que nos permite obtener un resultado exitoso al momento de requerir un análisis forense a un dispositivo de cómputo un teléfono inteligente. Estas también las encontramos en sistemas operativos expertos para tal fin como lo es Kali Linux.

También existen herramientas expertas y de pago para el análisis forense, como UFED Standard, XRY, Mobilyze, SecureView2, MobilEdit, Oxygen Forensic, CellDEK, Mobile Phone Examiner, Lantern, Device Seizure y Neutrino las cuales son bastante eficientes y con una larga trayectoria en el ámbito forense informático.

4.2.3 Cadena de custodia

El proceso de cadena de custodia es uno de los pasos más relevantes en la informática forense, ya que se debe establecer las diferentes responsabilidades y medidas de control respecto al personal que tiene contacto con las evidencias.[12]

[12] ARELLANO, Luis Enrique y CASTAÑEDA, Carlos Mario. La cadena de custodia informático-forense. Revista ACTIVA, Núm 3, enero-junio 2012, pp. 67-81.

Debe llevarse a cabo un documento en el que se registren los datos personales completos de todos involucrados en la manipulación de las copias, desde que hayan sido creadas a partir de la evidencia, hasta el momento de almacenamiento. Dicho documento debe contener información cómo, cuándo, dónde y quién tuvo contacto con la evidencia, también sus nombres completos, su cargo, las fechas y horas exactas; adicional a esto también se debe registrar los datos de la persona que tuvo bajo custodia la evidencia, el tiempo que esta estuvo bajo su poder y dónde fue guardada; también es importante que al momento de cambiar de custodio se debe registrar cuándo y cómo se produjo el intercambio, así como los datos de la persona que transportó la evidencia.[13]

Cada detalle es importante y por eso debe existir registro completo de toda la actividad.

La finalidad de la cadena de custodia no es más que mantener y preservar la integridad tanto física como lógica de una posible prueba o evidencia. Esta preservación se debe llevar a cabo desde el mismo instante de la recopilación o registro, su almacenamiento, transporte y análisis de la misma hasta culminar con su entrega a las entidades judiciales o a quien corresponda.

Cabe resaltar que en la mayoría de los casos, para que la cadena de custodia sea tomada como válida es necesario que un perito o alguna entidad judicial o del estado certifique que el proceso de custodia se ha llevado de manera correcta, evitando que la evidencia haya sido contaminada.

Las pruebas o evidencias documentales informáticas presentan una serie de características que necesitan de un tratamiento especial desde su recolección, conservación y transporte. Dichas características son[14]:

[13] Ibíd.
[14] Ibíd.

1. Se basa en indicios digitales, generalmente se encuentran cifrados y almacenados en un espacio digital específico, lo cual quiere decir que todo tipo de información se encuentra guardada.

2. Hay claras diferencias entre el elemento que contiene la información y su contenido, es decir, la misma información. Para esto se considera lo siguiente:

    - La información hace referencia al conocimiento que puede ser referido a un hecho u objeto y que puede ser cifrado y almacenado.
    - El objeto se refiere a un conjunto que se pueda determinar físicamente o que se pueda definir lógicamente.

3. La presentación de la información puede estar establecida por alguno de los estados que se indi can a continuación:

- Almacenada: indica que se encuentra guardada en un almacenamiento que puede ser primario, secundario o terciario y que se encuentra lista para ser accedida. Este es un estado estático y se puede tener acceso a la información bien sea por medios locales o remotos.

- En desplazamiento: indica que se encuentra transportándose por algún medio físico y su recolección se puede dar por la interceptación de dicho medio, teniendo en cuenta las leyes que cobijan la interceptación de comunicaciones o la violación de correspondencia.

- En proceso: es el estado más complejo y hace parte de la primera decisión que se debe tomar por parte de la persona encargada de la recolección. Al estar en uso un equipo de cómputo, la información se encuentra en proceso, es decir, se modifica, se actualiza y vuelve a ser almacenada, entonces se

debe decidir si se apaga o no el equipo de cómputo. Esta es una decisión vital ya que de ella depende la posible pérdida de la información y la alteración o daño de la posible evidencia que se quiere recolectar.

Se dice que es una decisión vital ya que si se decide dejar el equipo encendido se corre el riesgo de ser detectado y que se activen métodos que generen el borrado o destrucción de la información contenida en el equipo y que esta sea irrecuperable, es decir, entre más tiempo se deje encendido, mayor será el daño generado.

Si por el contrario, se decide apagar el equipo, de igual forma puede haber métodos que eliminen la información contenida no solo en los equipos locales sino en los reservorios de la misma red o las externas; frecuentemente la información se guarda en reservorios externos con el fin de mantenerla bajo el menor riesgo posible.

La mejor forma de dar solución a este tipo de inconvenientes es por medio de la inteligencia, haciendo ataques pasivos, escuchando y analizando el tráfico haciendo uso de herramientas remotas. Para lograr lo anterior se debe contar con recursos tanto tecnológicos como humanos que sean lo suficientemente eficientes para lograr el objetivo. Otro punto a tener en cuenta si se quiere implementar esta opción es que se debe contar con autorización por parte de las entidades judiciales, quienes no son tan flexibles en lo que a este campo se refiere. [15]

Cabe resaltar que esta solución del acceso remoto e indetectable por parte del accedido, es una temática que no se encuentra en discusión en Colombia.

El valor que adquiere la prueba depende de cómo esta sea introducida dentro del proceso con el fin de ser considerada con el suficiente peso jurídico dentro del

[15] Ibíd.

debido proceso. A diferencia de los documentos probatorios comunes, en el caso de las evidencias digitales, se tiene que un bit es exactamente igual a otro y que la copia de bit a bit del archivo original facilita el proceso de cadena de custodia debido a que se pueden conservar las copias manteniendo el valor probatorio del archivo original y de esta manera evitando riesgos para el mismo. [16]

Lo anterior significa que se puede entregar a un perito la copia del archivo que ha sido tomado del original y entregar en un tribunal otra copia en su reservorio original teniendo en cuenta los niveles de seguridad que se puedan ofrecer como una caja fuerte por ejemplo. La diferencia entre una prueba común como un documento, es que si a este se le van a realizar diferentes tipos de pruebas como la caligráfica, significa que el documento debe ser trasladado desde su lugar de almacenamiento y durante este proceso tanto de transporte como de pruebas, el documento puede ser destruido, dañado o modificado y de esta manera la prueba se perdería; mientras que con una evidencia digital que ha sido resguardada en un juzgado por ejemplo, y al requerirse su traslado y pruebas, se puede entregar una copia y de esta manera el original va a estar almacenado a salvo de cualquier riesgo.

En la recolección de documentación informática de pruebas, es suficiente con copiar bit a bit la prueba y luego proceder a hacer el traslado de la misma. La recolección de pruebas llevando a cabo procesos certificados de copiado, sustituyen la prueba original debido a que en ocasiones, la información está contenida en reservorios que son indispensables para el funcionamiento y operación de las diferentes entidades o empresas bien sean públicas o privadas.
Las diferentes herramientas o métodos existentes de certificación digital como las funciones hash, firma electrónica, firma digital, entre otros, son mucho más confiables y difíciles de falsificar que los métodos convencionales. Sin embargo la falta de conocimiento sobre todas estas nuevas herramientas tecnológicas por

[16] Ibíd.

parte del personal de las diferentes instituciones o entidades judiciales dificulta un poco su utilización ya que se genera cierto ambiente de desconfianza sobre el uso de estas. La tarea de aceptar, analizar y comprender el uso de este tipo de tecnología muy seguramente llevará algo de tiempo a medida que avancen los desarrollos informáticos en este campo.

Como ya se ha mencionado anteriormente, el proceso de cadena de custodia en la investigación de delitos informáticos, tiene como objetivo fundamental, generar la certeza de que la prueba cumple con los requisitos que se exigen procesalmente y por esto se debe garantizar[17]:

a) Trazabilidad: respecto a la humana, se refiere a que se deben establecer responsabilidades en lo concerniente a la manipulación de la prueba desde su recolección, almacenamiento, transporte y presentación final ante las entidades que corresponda.

   La trazabilidad física, incluye todos los equipos tanto locales como remotos e independiente de la función que desempeñen bien sea de almacenamiento, procesamiento o comunicación.
   La trazabilidad lógica hace referencia a la descripción y modelado de las diferentes estructuras de distribución de la información a la que se ha accedido y que ha sido almacenada.

b) Confiabilidad: se refiere a las demás características de la seguridad en cuanto a integridad, autenticidad, confidencialidad y no repudio.

[17] Ibíd.

4.2.3.1 Cadena de custodia y privacidad

Un tema importante que se debe tener en cuenta a la hora de llevar a cabo la cadena de custodia, es la privacidad; si bien es cierto que por medio de la cadena de custodia se asegura la confiabilidad de la evidencia digital recolectada y que esta a su vez implica la trazabilidad de la misma, no necesariamente se protege el derecho a la privacidad.

Esto se menciona ya que se puede contar con una evidencia digital que ha sido tratada de acuerdo a los procedimientos establecidos para la cadena de custodia, la cual presente una trazabilidad y preservación adecuada criminalística, informática y procesalmente hablando pero que se pudo haber generado a partir de algún tipo de acción ilegal; el tipo de ilegalidad a que se hace referencia es cuando se accede a la información o a los reservorios donde se encuentra dicha información, sin los debidos permisos u órdenes de allanamiento y de igual forma se habla de ilegitimidad cuando durante el proceso de recolección de pruebas se accede a más información de la que se tiene los permisos correspondientes con el fin de justificar la recolección de evidencias[18].

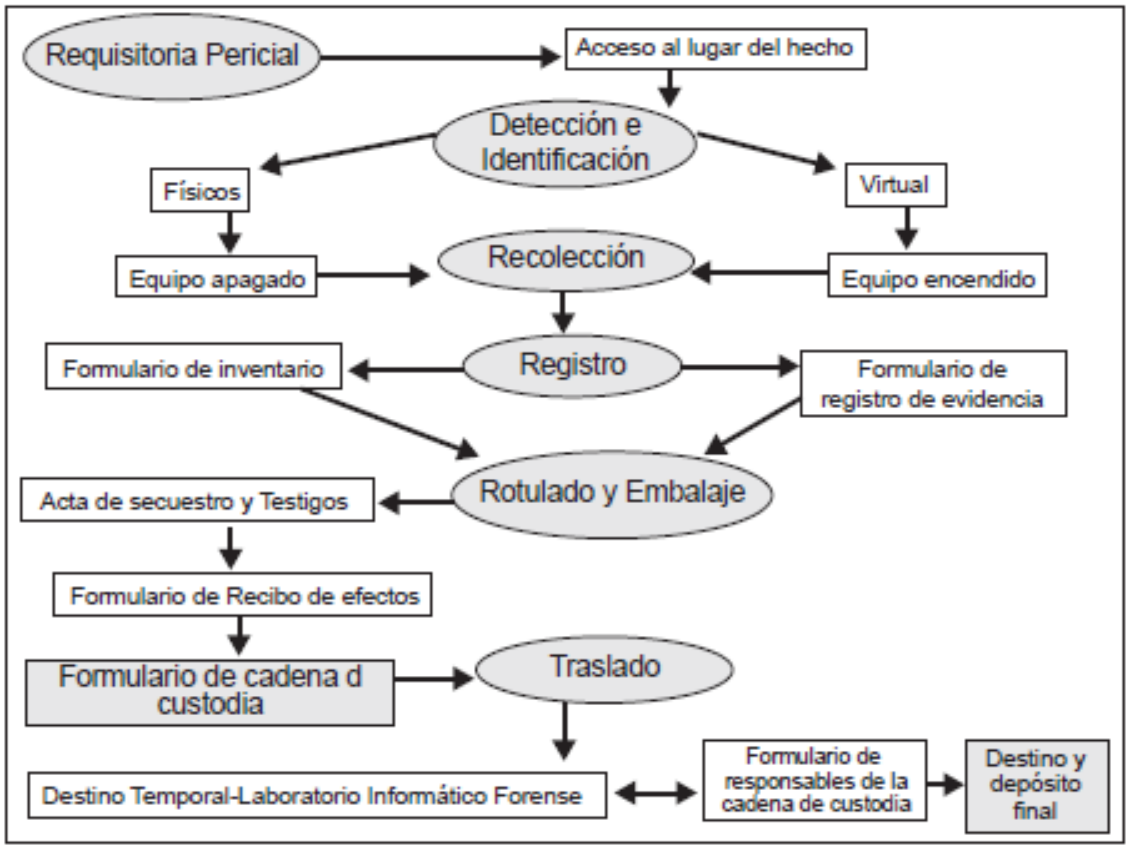
4.2.3.2 Cadena de custodia de evidencias digitales

Gracias a los lineamientos establecidos por la informática forense se cumplen los principales requisitos establecidos en la inspección judicial de la criminalística. En esta especialidad, los elementos que hacen parte de las pruebas o evidencias pueden ser físicos o digitales. Cuando se trabajan evidencias digitales, todo el proceso de manipulación desde la detección, identificación y recolección, debe hacerse con los equipos encendidos; dado que la información es un elemento no tangible que puede estar almacenada en diferentes medios tanto volátiles como no volátiles, requiere de cuidados especiales. Para determinar la validez de la información contenida en estos medios, se hace necesaria su certificación haciendo uso de hash; este tipo de funciones permiten la comprobación de la

[18] Ibíd.

integridad de las evidencias digitales recolectadas y verificar que corresponda a la original. [19]

Figura 1 Protocolo para la cadena de custodia en informática forense



Fuente: Arévalo y Castañeda.

En general se puede decir que el principal objetivo es conservar la evidencia; la validez de las pruebas depende en gran parte de mantener la seguridad, de generar que su almacenamiento sea legal y de seguir una metodología estructurada y documentada.

Teniendo en cuenta lo anterior, en el lugar de los hechos se deben llevar a cabo algunos pasos en una fase preliminar a la elaboración del documento de cadena

[19] Ibíd.

de custodia el cual se considera como información de tipo confidencial, clasificada y almacenada en un lugar seguro. [20]

4.2.3.3 Detección, identificación y registro

Debe tratar de identificarse la mayor cantidad de dispositivos y redes de equipos que harán parte del registro; seguido a esto se procede a hacer el inventario del hardware y se hace el reconocimiento judicial, estos quedarán dentro del documento del registro de la evidencia. Se debe tener en cuenta que la persona encargada de esta labor debe: [21]

- Usar guantes.

- Tomar fotografías o filmar todos los elementos encontrados en el sitio desde la parte periférica hasta el área donde se encuentren los equipos.

- Tomar fotografías de todos los elementos informáticos encontrados e indicar sobre cuales se deben tomar fotografías macro:

  - ✓ Pantallas de los monitores de los equipos examinados.
  - ✓ Vista de lado, de frente y posterior.
  - ✓ Etiquetas con seriales.
  - ✓ Periféricos.
  - ✓ Documentos impresos en el dispositivo o cerca a este.
  - ✓ Cables.
  - ✓ Equipos de conexión inalámbrica y alámbrica.
  - ✓ Diagramas de red y topologías.

- Hacer el inventario de todos los dispositivos encontrados a examinar, detallando la mayor cantidad de información sobre estos elementos en la

[20] Ibíd.
[21] Ibíd.

planilla de registro. También es muy importante generar un plano o croquis del lugar, identificando el lugar de acceso y la ubicación de los diferentes elementos informáticos encontrados, esto con el fin de generar de manera digital el diseño del sitio.

4.2.3.4 Recolección de elementos informáticos físicos o virtuales

La recolección y tratamiento de la evidencia por parte del perito informático debe llevarse a cabo de acuerdo a los procedimientos establecidos según la finalidad o el requerimiento de este proceso.

- Por orden judicial, cuyo proceso debe ser[22]:

  - ✓ Obtener la evidencia para posteriormente ser analizada en el laboratorio, el perito debe proceder de la siguiente manera:
    - ➢ Certificar por medio de alguna herramienta (hash por ejemplo) la evidencia.
    - ➢ Hacer la identificación y registro de la evidencia.
    - ➢ Elaborar un acta en presencia de testigos.
    - ➢ Dar inicio al proceso de cadena de custodia.
    - ➢ Movilizar la evidencia hasta el laboratorio forense.

  - ✓ Llevar a cabo la copia de la evidencia digital con el fin de que esta sea analizada en el laboratorio, para lo cual se debe proceder de la siguiente manera:
    - ➢ Certificar por medio de alguna herramienta (hash por ejemplo) la evidencia.
    - ➢ Hacer duplicado de la evidencia.
    - ➢ Hacer la identificación y el debido registro de la evidencia y de su copia.
    - ➢ Elaborar un acta en presencia de testigos.

[22] Ibíd.

- Movilizar la evidencia o su duplicado hasta el laboratorio forense.

- Por solicitud de una persona particular, empresa, organización, entidad o por otro profesional, en este caso se debe proceder:

  - ✓ Asistir al lugar de los hechos con un funcionario o escribano público.

  - ✓ Certificar por medio de alguna herramienta (hash por ejemplo) la evidencia ante el funcionario o escribano público.

  - ✓ Hacer el duplicado de la evidencia en presencia del funcionario o escribano público.

  - ✓ Hacer la solicitud al funcionario o escribano público que se deje por escrito en el acta el motivo del presente proceso, como también los datos de la o las personas que solicitan dicho proceso y la razón para llevar a cabo el mismo.

  - ✓ Solicitar una copia del acta.

  - ✓ Movilizar la copia de la evidencia hasta el laboratorio donde se llevara a cabo su análisis.

En algunos casos no es posible trasladar los equipos que contienen la información a ser recolectada como evidencia, para tal fin el perito o investigador informático debe trasladarse al lugar de los hechos y proceder a hacer la copia o duplicidad de la evidencia, este proceso se debe llevar a cabo de tal forma que la copia conserve la validez del contenido original.

La persona encargada de la recolección de la evidencia debe llevar elementos de almacenamiento limpios y desinfectados, dispositivos de arranque en vivo con protección contra escritura, el cual contenga el software base y el software para la autenticación y elaboración de la copia de las evidencias digitales.

Las imágenes de los discos se deben hacer bit a bit con el fin de obtener toda la información tal cual está en el disco, archivos eliminados, ocultos, etc. Esto de acuerdo a los procedimientos establecidos por el National Institute of Standard and Technology y adicionalmente el software seleccionado para tal fin debe cumplir con unas características especiales[23]:

- El software debe hacer la copia bit a bit de un disco duro o una partición en un elemento fijo o que sea removible.
- El software no debe alterar el disco original.
- El software debe tener acceso a discos de tipo SCSI e IDE.
- El software debe validar la integridad de la imagen que ha sido generada.
- El software debe registrar errores de entrada y de salida, de igual forma debe notificar si el dispositivo de origen es de mayor tamaño que el de destino.
- Se debe hacer uso de elementos de hardware que bloqueen la escritura para asegurar que el dispositivo accedido no sea alterado.

  El software debe tener la documentación acorde a los diferentes procesos a realizar. Se debe tener en cuenta que la imagen obtenida es la que se llevara al laboratorio para ser analizada.
- Se procede a apagar el equipo desconectando el cable de la toma de corriente.
- Se retira la unidad o unidades extraíbles.
- Se debe descargar la propia electricidad tocando alguna parte metálica y se abre la caja del equipo.
- Se desconecta el bus o cable de datos del disco.

[23] Ibíd.

- Desconectar la corriente del disco.
- Acceder al CMOS o a la BIOS del sistema.
- Encender el equipo.
- Acceder al CMOS o BIOS.
- Verificar la fecha y hora arrojada por el sistema y documentarla en el formato de recolección de evidencia; adjuntar cualquier dato que se considere importante para el proceso.
- Modificar la unidad de arranque para que sea la unidad extraíble con la que se inicie el sistema.
- Guardar cambios al salir.
- Verificar si hay discos en el equipo.
- Abrir la unidad y sacar el disco.
- Insertar la unidad extraíble donde corresponda para el arranque del sistema.
- Verificar el inicio desde la unidad correspondiente.
- Apagar el equipo.
- Asegurar contra escritura el disco o unidad de almacenamiento secundario original, esto se hace de acuerdo a la configuración del jumper según el fabricante o con el hardware que se considere necesario para tal fin.
- Conectar el cable que corresponda al disco.
- Conectar la corriente al disco master.
- Conectar el dispositivo que se vaya a utilizar para almacenar la copia como esclavo, este debe ser de tamaño mayor al disco o dispositivo original.
- Cerciorarse de que en el dispositivo de arranque se encuentren contenidos los controladores del hardware necesarios para hacer la copia de la información.
- Encender el computador iniciando desde el dispositivo configurado anteriormente.
- Hacer la certificación matemática del disco examinado o copiado.
- Almacenar el resultado en otro dispositivo.

- Hacer la imagen o la copia con los elementos de software y hardware seleccionados para tal fin.
- Hacer una o dos copias de la evidencia, esto con el fin de dejar una en el lugar de los hechos y con la otra se trabaja en el laboratorio; el original se deja en el repositorio judicial o se procede dependiendo si este proceso es solicitado por un particular (con un empleado o escribano público).
- Hacer la certificación matemática de las copias.
- Almacenar el resultado en otro dispositivo.
- Registrar el resultado obtenido por las copias en el correspondiente formulario de recolección de evidencia.
- Apagar el equipo.
- Quitar los tornillos que ajustan el disco duro
- Sacar el disco duro, teniendo precaución de no averiar los circuitos electrónicos.

4.2.3.5 Recolección y registro de evidencia digital

Cuando un equipo se encuentra encendido, se debe tener en cuenta la obtención de la información en tiempo real, es decir, en vivo; de igual forma otro aspecto a tener presente son los dispositivos de almacenamiento volátiles, ya que como se sabe, estos pierden información al apagarse el equipo[24].

La información que se encuentra en almacenamiento volátil muestra el comportamiento actual de los sistemas operativos y de las diferentes aplicaciones, procesos en ejecución, bloqueados, estado de la impresora y la cola de impresión, así como también las conexiones de red activas y los puertos que se encuentren abiertos.

[24] MAGRANER GIMENO, Jordi. Pruebas y evidencias telemáticas. Trabajo de grado. Universidad Politécnica de Valencia. Valencia, 2015.

Los datos volátiles se encuentran registrados en la CPU del microprocesador, en la memoria caché, en la RAM o en la memoria virtual también.

Para acceder a dispositivos de almacenamiento volátil se debe tener en cuenta lo siguiente[25]:

- ✓ Llevar a cabo la ejecución de un intérprete de comando que sea confiable o que esté debidamente certificado.
- ✓ Hacer el registro de hora, fecha y zona horaria del sistema.
- ✓ Identificar los usuarios que tengan sesión abierta, bien sean locales o remotos.
- ✓ Hacer el registro de los tiempos en que se crean, acceden y modifican todos los archivos.
- ✓ Identificar y registrar los puertos que se encuentren abiertos.
- ✓ Hacer el debido registro de las diferentes aplicaciones que se relacionen con los puertos mencionados en el anterior ítem.
- ✓ Hacer el registro de los procesos que se encuentren en ejecución.
- ✓ Validar y hacer el registro de todas las conexiones de red activasen el momento o recientemente.
- ✓ Verificar y registrar la fecha y hora actual del sistema.
- ✓ Validar la integridad de la información.
- ✓ Hacer la debida documentación de todas las tareas y los comandos que se llevaron a cabo durante este proceso de recolección.

Después de esto, lo ideal es hacer una recolección más específica y estricta sobre la información contenida en el almacenamiento volátil, para lo cual se debe hacer lo siguiente[26]:

- ✓ Revisar y obtener los registros de eventos del sistema.

[25] Ibíd.
[26] Ibíd.

- ✓ Hacer una revisión sobre la base de datos o los módulos del núcleo del sistema operativo.
- ✓ Hacer la verificación de la legitimidad de los comandos del sistema operativo.
- ✓ Validar y obtener los archivos con las claves del sistema operativo.
- ✓ Identificar y extraer los archivos de configuración más importantes del sistema operativo.
- ✓ Identificar y extraer la información que se encuentre en la memoria RAM.

El proceso como tal que se debe seguir con el fin de ejecutar las tareas mencionadas anteriormente, teniendo el equipo encendido y haciendo uso de las herramientas informáticas forenses que se encuentran en dispositivos extraíbles y de solo lectura, consiste en[27]:

- Hacer la ejecución de un intérprete de comando que sea confiable o que esté debidamente certificado.
- Hacer la identificación y obtención del listado de todos los comandos usados en el equipo, antes del proceso de recolección.
- Hacer el registro de hora y fecha actuales del sistema.
- Hacer la recolección y transferencia al medio forense seleccionado y hacer la correspondiente documentación del proceso.

    - ✓ Bitácora de fecha y hora del sistema
    - ✓ Imagen de memoria principal.
    - ✓ Usuarios que se encuentren conectados actualmente al sistema.
    - ✓ Registro de modificación, creación y tiempos de ingreso de los archivos.
    - ✓ Lista con los puertos abiertos y las aplicaciones que escuchan dichos puertos.
    - ✓ Listado de aplicaciones que se relacionan con los puertos abiertos.
    - ✓ Listado de procesos activos o en ejecución.

[27] Ibíd.

- ✓ Conexiones de red actual o reciente.
- ✓ Recursos compartidos.
- ✓ Tablas de ruteo.
- ✓ Tabla de ARP.
- ✓ Registro con los eventos de seguridad, del sistema, de aplicaciones y servicios en ejecución.
- ✓ Parametrización de las políticas de auditoría del sistema operativo.
- ✓ Estadísticas del núcleo del sistema operativo.
- ✓ Archivos que contengan usuarios y contraseñas del sistema operativo.
- ✓ Archivos de configuración más importantes del sistema operativo.
- ✓ Archivos temporales.
- ✓ Enlaces rotos.
- ✓ Archivos de e-mail.
- ✓ Archivos de navegación en internet.
- ✓ Integridad de datos debidamente certificada.
- ✓ Listado con los comandos usados en el equipo durante el proceso de recolección.
- ✓ Obtener la topología de red.

En caso de ser necesario hacer el proceso de recolección de evidencia con el equipo apagado, se debe tener la certeza de no hacer el arranque desde el disco que contiene la información a recolectar y hacer uso de dispositivos para el arranque de solo lectura y con herramientas de informática forense certificadas para tal fin[28].

- Se procede a apagar el equipo desconectando el cable de la toma de corriente.
- Se retira la unidad o unidades extraíbles.
- Se debe descargar la propia electricidad tocando alguna parte metálica y se abre la caja del equipo.

[28] Ibíd.

- Se desconecta el bus o cable de datos del disco.
- Desconectar la corriente del disco.
- Ingreso al CMOS o a la BIOS del sistema.
- Encender el equipo.
- Acceder al CMOS o BIOS.
- Verificar la fecha y hora arrojada por el sistema y documentarla en el formato de recolección de evidencia; adjuntar cualquier dato que se considere importante para el proceso.
- Modificar la unidad de arranque para que sea la unidad extraíble con la que se inicie el sistema.
- Guardar cambios al salir.
- Insertar la unidad extraíble donde corresponda para el arranque del sistema.
- Verificar el inicio desde la unidad correspondiente.
- Apagar el equipo.
- Asegurar contra escritura el disco o unidad de almacenamiento secundario original, esto se hace de acuerdo a la configuración del jumper según el fabricante o con el hardware que se considere necesario para tal fin.
- Conectar el cable que corresponda al disco.
- Conectar la corriente al disco master.
- Conectar el dispositivo que se vaya a utilizar para almacenar la copia como esclavo, este debe ser de tamaño mayor al disco o dispositivo original.
- Cerciorarse de que en el dispositivo de arranque se encuentren contenidos los controladores del hardware necesarios para hacer la copia de la información.
- Encender el computador iniciando desde el dispositivo configurado anteriormente.
- Hacer la certificación matemática del disco examinado o copiado.
- Almacenar el resultado en otro dispositivo
- Hacer el registro del resultado obtenido en el formulario de recolección de la evidencia.

Haciendo uso de las herramientas de informática forense, se procede a hacer la recolección y almacenamiento en medios forenses para luego proceder a hacer el análisis correspondiente que puede ser en el mismo sitio de los hechos o en el laboratorio forense, cabe recordar que todo este proceso se debe documentar; para esto se debe conocer lo siguiente[29]:

- ✓ Tipo de sistema operativo.
- ✓ Fecha, hora y zona horaria configurada en el sistema operativo.
- ✓ Versión de los sistemas operativos.
- ✓ Registrar el numero de particiones de los discos.
- ✓ Los Tipos de particiones encontrados.
- ✓ Estructura de la tabla de particiones.
- ✓ Lista con todos los nombres de los archivos, con fecha y hora.
- ✓ Detalle del espacio desperdiciado.
- ✓ Incluir el MBR.
- ✓ Incluir la tabla de particiones.
- ✓ Incluir la partición de inicio del sistema y los archivos de comandos.
- ✓ Registro de los espacios no asignados.
- ✓ Registro de los espacios de intercambio.
- ✓ Recuperar archivos que han sido eliminados.
- ✓ Hacer la búsqueda de archivos ocultos con palabras clave en el espacio desperdiciado, en el no asignado, en el de intercambio, en el MBR y en la tabla de particiones.
- ✓ Listado con las aplicaciones instaladas en el sistema.
- ✓ Software ejecutable sospechoso.
- ✓ Reconocimiento de extensiones de archivos sospechosos.
- ✓ Lista de archivos protegidos con claves.

[29] Ibíd.

- ✓ Listado con el contenido de los archivos de cada usuario que este en el directorio raíz y en los subdirectorios.
- ✓ Validación del comportamiento del sistema operativo, rendimiento e integridad de los sectores y comandos de los módulos y captura de pantallas.
- ✓ Hacer la certificación de los datos mediante algoritmos hash al finalizar el proceso.
- ✓ Almacenar las copias del software utilizado.
- ✓ Se puede apagar o dejar encendido el equipo, dependiendo de los requerimientos judiciales.

Una vez se ha realizado el proceso de detección, validación y recolección de la evidencia, esta debe ser almacenada y alistada para ser trasladada; para tal fin, se debe proceder de la siguiente manera[30]:

- Contar con un lugar amplio, limpio y despejado para proceder a rotular y registrar la evidencia.
- Ingresar en el correspondiente formulario destinado para el registro de la evidencia, todos los elementos inspeccionados durante el proceso de recolección y registrando la información que se considere pertinente.
- En bolsas antiestáticas se deben almacenar los diferentes dispositivos de almacenamiento secundario, quedando registrada la fecha, hora, tipo de elemento, números de serie, capacidad, nombres, apellidos y documento de identidad del perito informático forense al igual que su firma.
- De igual forma, en bolsas fabricadas con filamentos de cobre y níquel para evitar la interferencia de señales inalámbricas se deben almacenar teléfonos móviles, GPS, entre otros.
- En bolsas de plástico o estériles se deben almacenar otro tipo de elementos que se consideren importantes para el caso, teniendo la precaución de

[30] Ibíd.

rotularlos con la información del elemento y adicional los nombres, apellidos y firma del perito informático forense.

- Hacer el acta del secuestro de acuerdo al formulario del recibo de efectos.
- Colocar todos los elementos encontrados y registrados en una caja para ser trasladados, dicha caja debe asegurar y proteger contra cualquier daño los elementos durante el proceso de movilización.
- Hacer el traslado de todos los elementos en conjunto, en una sola caja, esto con el fin de evitar confusión o pérdida de alguno de los elementos al momento de almacenarlos posteriormente.

4.2.3.6 Traslado de la evidencia digital

La movilización de la evidencia digital recolectada se hace con destino al laboratorio forense del organismo que se haya establecido en el requisitorio pericial. El tiempo que la evidencia dure en el laboratorio puede ser temporal, sin embargo se debe asegurar mantener la estricta cadena de custodia durante su estadía en el laboratorio. De acuerdo al avance del caso judicial, se dispondrá que la evidencia sea entregada y almacenada en un lugar específico final[31].

4.2.4 Delito informático

Con el auge de la tecnología y a medida que el uso de internet se ha venido masificando cada día, de igual forma los riesgos y vulnerabilidades a las que se exponen los usuarios se hacen más frecuentes. Los métodos de atacar o de delinquir por medios informáticos han venido evolucionando con el desarrollo de la tecnología, el uso de los medios de comunicación y herramientas de información[32].

[31] ARELLANO, Luis Enrique y CASTAÑEDA, Carlos Mario, op. cit.
[32] MANJARRÉS BOLAÑO, Iván y JIMÉNEZ TARRIBA, Farid. Caracterización de los delitos informáticos en Colombia. Pensamiento Americano, Vol. 8, Num. 9, 2012, p. 71-82.

Inicialmente los ciberdelincuentes transportaban los virus en disquetes, luego empezaron a utilizar las redes de datos e internet, para luego hacer uso de las memorias usb para sus fines e iniciar contagios de malware. De igual forma el correo electrónico y los diferentes chats empezaron a ser utilizados para buscar posibles víctimas[33].

Toda clase de actos delictivos se han venido cometiendo por medio del uso de medios tecnológicos, desde pedófilos, traficantes, estafadores, secuestradores, sicarios y hasta terroristas hacen uso de la tecnología con el fin de incrementar sus negocios y ganancias[34].

Inicialmente las diferentes instituciones que trabajaban en la informática empezaron a desarrollar e implementar mecanismos de control y métodos para sancionar a quienes usaran de manera ilegal las diferentes herramientas tecnológicas o informáticas, sin embargo el problema de fondo es que no había como juzgar o judicializar a estas personas por la inexistencia de leyes específicas para proteger las violaciones hechas sobre la información.

Un delito informático es todo aquel acto antijurídico y de carácter culpable que se da por medios informáticos o que pretende manipular o dañar computadores, redes de internet o medios electrónicos.

Los delitos informáticos se pueden cometer mediante el uso de computadores, sistemas de información y otras clases de equipos de comunicaciones; también tienen por finalidad averiar, manipular, acceder o interrumpir la utilización de sistemas informáticos[35].

[33] Ibíd.
[34] Ibíd.
[35] Ibíd.

4.2.4.1 Clases de delito informático

Dentro de los delitos informáticos más comunes y que son castigados por la normatividad colombiana, se puede encontrar en cuanto a la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos[36]:

- Acceso abusivo a uno o más sistema informático.
-Obstaculización ilegitima de un sistema informático o una red de telecomunicación.
-captura e interceptación de datos informáticos.
-Daño informático.
-implementación de software malicioso.
-Violación y usurpación de datos personales.
-Suplantación de sitios web para capturar u hurtar datos personales.

Y en cuanto a los atentados informáticos y otro tipo de infracciones, se tiene:

-Hurto por medios informáticos y semejantes.
-Transferencia no consentida de activos.

4.3 MARCO CONCEPTUAL

4.3.1 Confidencialidad

Se define como la capacidad que tiene un sistema para evitar que la información contenida en él sea accesible por personas, entidades o procesos no autorizados para esto. La confidencialidad es de gran importancia debido a que las consecuencias en caso de que personal no autorizado acceda a la información, pueden ser muy graves para la organización. Dentro de los mecanismos más utilizados para proteger la confidencialidad se encuentran el control de acceso a los sistemas y el cifrado de la información y las comunicaciones.

[36] Ibíd.

4.3.2 Integridad

Dentro de la seguridad informática, se puede ver como un servicio que permite que la información sea creada, modificada o eliminada sólo por las personas autorizadas para tal fin. El sistema no debe permitir dañar o modificar la información contenida dentro del mismo ni permitir que personas que no estén autorizadas lo hagan; se debe tener en cuenta que la integridad incluye no solo modificaciones planeadas sino también las accidentales.

4.3.3 Disponibilidad

Hace referencia a que se debe garantizar el acceso del personal autorizado a la información en cualquier momento. En un sistema seguro se debe garantizar que la información siempre esté disponible para los usuarios y adicional a esto el sistema debe mantenerse siempre funcional y con la capacidad de recuperarse rápidamente en caso de alguna falla.

4.3.4 Custodia

La custodia y más específicamente la cadena de custodia es un procedimiento que se lleva a cabo de manera controlada y estructurada por medio del cual se busca aporta material probatorio que esté relacionado a hechos que pueden llegar a ser delictivos o no y asegurar ante los organismos de justicia la validez de dicho material evitando su contaminación hasta la disposición final según las órdenes judiciales.

4.3.5 Delito Informático

Se define como delito informático, todo acto delictivo que se relaciona con los sistemas, redes y datos. Los delitos informáticos son difíciles de ser comprobados debido a que muchas veces es difícil encontrar las pruebas; también son actos que pueden ejecutarse de manera rápida y sencilla, en ocasiones en segundos, solo basta con tener un equipo de cómputo y no se necesita estar en el lugar de

los hechos; de igual forma estos tienden a expandirse y así se complica un poco más identificarlos y perseguirlos.

4.3.6 Análisis forense

Es el conjunto de técnicas y procedimientos cuyo fin es adquirir información importante de diferentes medios de almacenamiento sin llegar a modificar el estado de los mismos, esto con el fin de encontrar información oculta, patrones o comportamientos y que pueden ser usados o no en una investigación.

4.3.7 Evidencia digital

También conocida como prueba electrónica, es aquel valor probatorio de la información que ha sido almacenada o transmitida de manera digital de modo que pueda ser utilizada en un juicio. Antes de ser aceptada por el juez u organismo encargado de impartir justicia, se debe validar la autenticidad de la prueba y si se acepta una copia o se requiere la original.

4.3.8 Trazabilidad

Hace referencia al historial que debe estar muy bien documentado sobre los diferentes procesos a los que se vea sometida la evidencia digital, así como la información precisa con nombres, cargos, fechas y horas exactas del personal que tenga acceso a las evidencias, bien sea en obtención, análisis, almacenado y transporte de las mismas.

4.3.9 Autenticidad

Se refiera a que la evidencia se ha generado y obtenido directamente en el lugar relacionado con el caso, más específicamente en el sitio del posible delito; por medio de esta característica se valora la no alteración de los medios originales.

4.3.10 Confiabilidad

Se establece si las diferentes evidencias digitales que son aportadas efectivamente proceden de medios verificables y creíbles. Esta característica gira en torno a que se sincronice el registro de las tareas realizadas por los usuarios y el registro íntegro de los mismos.

4.3.11 Suficiencia

Se refiere a que se aporte toda la evidencia necesaria para proceder con el caso. Es una de gran importancia ya que contribuye al éxito de las investigaciones en procesos judiciales.

4.3.12 Objetividad

Hace referencia a la capacidad que debe tener el perito o la persona encargada de la manipulación de la evidencia digital de acuerdo a los códigos de ética profesional.

4.4 MARCO LEGAL

Como eje principal se debe tener en cuenta que la normatividad colombiana así como la legislación en nuestro país se rige por la Constitución Política de Colombia de 1991.

Ley 1273 de 2009[37]

“Teniendo en cuenta que anteriormente los delitos clásicos y los delitos informáticos eran juzgados y penalizados bajo las mismas normas o leyes, surgió la necesidad de tipificar lo delitos informáticos como tal, es así como el 5 de enero

[37] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 de 2009. Diario Oficial. Bogotá, 2009.

de 2009 se da origen a tan importante ley, la 1273 de este año mediante la cual se modifica el código penal, de igual forma se establece un nuevo bien jurídico tutelado el cual es denominado “de la protección de la información y de los datos”, y se busca preservar de manera íntegra los diferentes sistemas que hagan uso de las tecnologías de información y las comunicaciones, entre otras disposiciones.

A continuación se describen los artículos que componen el Capitulo I. de la ley y que hacen referencia de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos:

Artículo 269A: *Acceso abusivo a un sistema informático*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: *Interceptación de datos informáticos*. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un

sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: *Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: *Uso de software malicioso*. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: *Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: *Circunstancias de agravación punitiva*: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Y del capítulo II que hace referencia de los atentados informáticos y otras infracciones:

Artículo 269I: *Hurto por medios informáticos y semejantes*. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: *Transferencia no consentida de activos*. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. *Circunstancias de mayor punibilidad*. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

Artículo 3°. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. *De los Jueces Municipales*. Los jueces penales municipales conocen:

6. De los delitos contenidos en el título VII Bis.

Artículo 4°. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal"[38].

- **Ley 527 de 1999**

Por medio de la cual se da validez a las evidencias digitales como material probatorio dentro de procesos de investigación judicial.

- Constitución Política de Colombia Artículos: 15, 29, 209, 228, 249, 250, 251 y 253 (con las modificaciones introducidas por el Acto Legislativo 03 de diciembre de 2002).
- Ley 600 de 2000 (Código de Procedimiento Penal), artículos 27, 232, 233, 241, 244, 245, 249, 251, 254, 255, 256, 257, 288, 289, 290, 314, 315, 317, 318, 319, 320, 321, 329, 345 y demás concordantes.
- Ley 906 de 2004 (Código de Procedimiento Penal), artículos 67, 114, 208, 213, 214, 215, 216, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 268, 276, 277, 278, 279, 280, 281, 484, 485.
- Resolución 0-0646, del 31 de mayo de 2001, de la Fiscalía General de la Nación, por medio de la cual se fijan las directrices para la ejecución de programas de mejoramiento institucional, oficialización de manuales de procesos y procedimientos administrativos, operativos y de funciones y en

[38] MINTIC. Ley 1273 de 2009. [en línea]. [citado en Marzo de 2016]. Disponible en internet:http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

general sobre todo lo relacionado con el desarrollo organizacional de la Fiscalía General de la Nación.

- Resolución 1890, de noviembre 5 de 2002, de la Fiscalía General de la Nación, por medio de la cual se reglamenta el artículo 288 de la Ley 600 de 2001.
- Resolución 0-2869 de diciembre 29 de 2003, de la Fiscalía General de la Nación, por medio de la cual se adoptó el manual de procedimientos de cadena de custodia.
- Resolución 0-6394 de diciembre 22 de 2004, de la Fiscalía General de la Nación, por medio de la cual se adopta el manual de procedimientos de cadena de custodia para el sistema penal acusatorio[39].

En Colombia las leyes para salvaguardar y penalizar una infracción del ámbito informático o de comunicaciones están bien estructuras, como la ponencia de la ley 1273 la cual vincula todas las series de delitos que se pueden presentar mediante la tecnología y sus aplicaciones.

[39] RESOLUCIÓN 0-6394 DE 2004, Fiscalía General de la Nación [en línea]. [Citado en diciembre de 2014]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=15634

5. DISEÑO METODOLÓGICO

5.1 METODOLOGÍA DE LA INVESTIGACIÓN

El desarrollo de la investigación se llevará a cabo de manera exploratoria y descriptiva, debido a que la ley sobre delitos informáticos es relativamente nueva así como lo es la informática forense, se tienen como antecedentes algunos trabajos que se han relacionado anteriormente y los cuales de algún modo hacen referencia en parte al tema en el que se pretende enfocar este estudio. Dada la naturaleza de la investigación, se puede decir que también es de tipo bibliográfica ya que como se refiere más adelante, de acuerdo a la recolección, selección y clasificación de la información que se haga, así mismo se irá fortaleciendo y consolidando la base teórica de la investigación abordada.

5.2 METODOLOGÍA DE DESARROLLO

Se hace necesario tener en cuenta las actividades principales a llevar a cabo dentro de la presente investigación y de esta manera hacer los subprocesos que conlleven al desarrollo exitoso de las mismas, por lo tanto establecer una metodología permite garantizar un buen desarrollo obteniendo ciertas ventajas, como lo son la estandarización de procesos y procedimientos, permitiendo su revisión constante y evidenciando los errores y oportunidades de mejora.

Las metodologías de investigación son herramientas que precisan el análisis de varios problemas que pertenecen a un mismo entorno, pero a su vez son independientes, dado que no importa en problema que se plantee, su método de estudio siempre va a ser el mismos.[40]

[40] VELÁZQUEZ, DEMIAN ROBERTO GARCÍA. METODOLOGÍA BASADA EN EL CÓMPUTO [en línea]. [Citado en México. Abril de 2014]. Disponible en internet:

Con el fin de identificar el proceso de custodia y su aplicación en la investigación de delitos informáticos en Colombia, inicialmente se debe recurrir a las principales fuentes de consulta de esta información, conocer las diferentes metodologías, tareas a seguir, estándares y como se viene desarrollando este proceso.

La metodología del análisis forense debe contener las siguientes fases para su óptimo desempeño, identificación, adquisición, análisis y presentación, donde la identificación es el estudio del entono objetivo de la situación que se allá presentado, donde en **primera fase** se debe notificar y obtener la autorización por la entidad que requiera el servicio de análisis, revisar las políticas y la legislación, identificar los miembros del equipo, realizar una evaluación y valoración para con ello iniciar la adquisición de pruebas, donde dicha evaluación mide y parametriza los recursos, alcance y objetivos de la investigación que permitan determinar el estado actual del sistema, que partes están afectadas, la sensibilidad de la información y la gravedad de los hechos, permitiendo obtener un informe analítico de la situación fijando el curso de la investigación de la forma acertada.

En este punto se inicia la cadena de custodia, diligenciando el formato correspondiente y la bitácora de los procesos que se lleven a cabo y el embalaje de la evidencia[41].

La adquisición como **fase dos** se debe tener bastante experiencia y cuidado para no ir a contaminar los sistemas o equipos que sean tomados como evidencia a los cuales se les debe sacar una imagen exacta como copia teniendo en cuenta todos los datos volátiles, los cuales son los registros de la cache del sistema, los

---

http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/3581/tesis.pdf?sequence=1

[41] DragonJAR. Metodología Básica de Análisis Forense – Parte 1 de 4 [en línea]. [Citado en marzo de 2017].Disponible en internet: https://www.dragonjar.org/metodologia-basica-de-analisis-forense-parte-1-de-4.xhtml

archivos temporales, también se encuentran los registros de sucesos y acontecimientos, referente a los dispositivos de la red se pueden evidenciar los registros internos y externos, los cuales son firewalls, routers, servidores proxy, los logs del sistema, aplicaciones, etc. Y de la cual se realizara otra imagen para su investigación y tratamiento.[42]

En la **fase tres se analizan y manipulan** los datos de una red, de un host u equipo de cómputo o se realiza análisis a los medios de almacenamiento.

El análisis de una red es para validar la seguridad perimetral, servidores web, firewalls, proxy y de más complementos de red con el fin de obtener los ficheros y registros que se hayan generado por los mismos y encontrar anomalías o rastros de vulnerabilidad y/o violación de su seguridad.

Referente al análisis de datos de una máquina de computo o host, se realiza para obtener información de los sistemas vivos mediante la lectura de la información de las aplicaciones y los sistemas operativos, se realizara búsqueda de aquella información que sea útil y se fijara criterios de búsqueda dependiendo de nuestros objetivos para poder filtrar la información que se requiera según el hallazgo de la incidencia.

En el análisis de los medios de almacenamiento también se definen criterios de búsqueda para identificar los posibles hallazgos e información relevante según los objetivos.

Preparación de **informe** como **fase cuatro o fase final** y la más delicada e importante ya que en él se plasmara y sustentara las pruebas para un proceso legal, donde la información debe estar bien organizada en todas sus fases con

[42] DragonJAR. Metodología Básica de Análisis Forense – Parte 2 de 4 [en línea]. [Citado en marzo de 2017].Disponible en internet: https://www.dragonjar.org/metodologia-basica-de-analisis-forense-parte-1-de-4.xhtml

soportes adjuntos como notas, antecedentes o información policial, siempre plasmando lo más relevante entregando conclusiones concisas teniendo en cuenta los hechos y presentando una lista de las pruebas, toda esta información debe escribirse en un lenguaje entendible para gente del común y no muy técnico, explicando claramente el propósito del informe, el objetivo del informe, el público objetivo y por qué se preparo

Una vez hecho lo anterior, se debe proceder a validar y revisar la información correspondiente a los delitos informáticos y cómo se llevan a cabo las investigaciones de este tipo de delitos en nuestro país; se hace importante conocer las fases de la informática forense y cómo se conjuga ésta con la investigación de los delitos informáticos en la actualidad.

Para identificar las posibles falencias existentes en el proceso de custodia y su aplicación en la investigación de delitos informáticos en nuestro país, es necesario realizar el análisis sobre la Información consultada, haciendo una selección sobre la más relevante y que contribuya a la identificación de las posibles actividades o subprocesos que probablemente se puedan mejorar o en las que se pueda incurrir en errores con el fin de ser mejorados.

Teniendo identificadas las falencias se debe validar la mejor forma de presentar los resultados obtenidos, pare este caso será un informe de identificación con las posibles mejoras sobre el proceso de custodia de pruebas digitales para evitar pérdidas, daños o destrucción de las mismas y su aplicación en la investigación de delitos informáticos en Colombia.

La base de la presente investigación es la consulta de toda la documentación posible sobre los diferentes temas contenidos en ella, como lo son la seguridad informática, la informática forense, las fases de la informática forense y el proceso

de cadena de custodia; de igual forma se buscara documentación sobre los delitos informáticos en nuestro país y como se llevan a cabo los procesos e investigaciones judiciales sobre delitos informáticos.

Es importante obtener la mayor cantidad de información con el fin de tener la documentación suficiente que permita hacer el análisis de cómo se está llevando a cabo el proceso de cadena de custodia en investigaciones de delitos informáticos en Colombia. Las fuentes de información serán internet y la biblioteca de la UNAD.

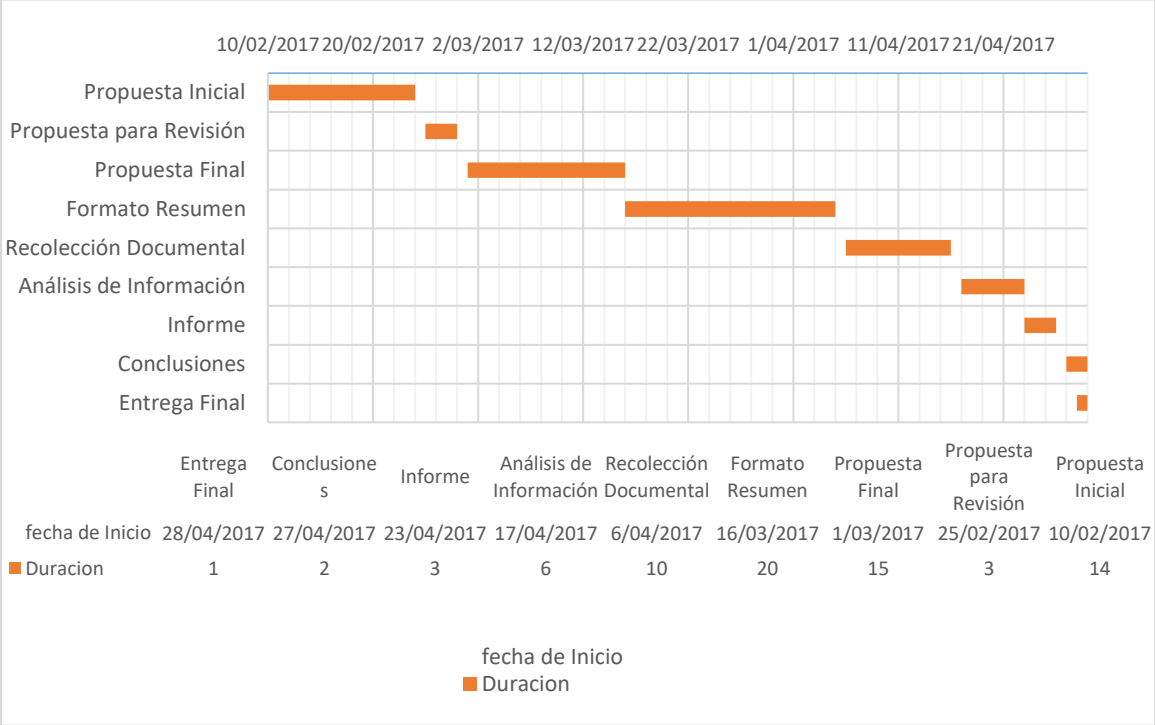
Una vez recopilada la información y hecho el análisis del proceso, se procede a documentar las falencias que se puedan presentar durante este proceso para luego identificar las posibles soluciones.

Finalmente se presentará un informe general sobre las mejoras que se puedan presentar al proceso de cadena de custodia y su aplicación en la investigación de delitos informáticos en Colombia.

En general para el desarrollo de la investigación, las fuentes de recolección de información serán secundarias debido a que se hará por medio de consultas bibliográficas y la técnica principal de dicha recolección será por medio de internet.

Para adelantar el estudio se consideró el siguiente cronograma, el cual se hace basado en una metodología de mejores prácticas para la gestión de proyectos y se ha tenido en cuenta el ciclo de vida del proyecto desde su inicio, planeación, ejecución, seguimiento – control y cierre. Lo anterior permite llevar un mejor control sobre las actividades que se deben llevar a cabo para lograr el éxito del proyecto.

Figura 2. Cronograma de Desarrollo



Fuente: Autor.

6. RESULTADOS Y DIVULGACIÓN

6.1 INVESTIGACIÓN DE DELITOS INFORMÁTICOS EN COLOMBIA

En este punto ya se puede hablar sobre el reconocimiento que hacen las diferentes entidades judiciales donde aceptan que se puede obtener evidencia a partir de equipos de cómputo para hacer parte de las investigaciones en casos judiciales; de hecho las autoridades Colombianas se vienen preparando cada vez más en estos temas con el fin de combatir de manera eficiente los delitos informáticos; es así como se observa que en el CTI de la Fiscalía o en la policía judicial, entre otras, se encuentran grupos especializados en el manejo de cibernética e informática forense.

De igual forma se vienen apoyando en empresas con la capacidad, experiencia y que cuentan con la infraestructura tecnológica y el recurso humano lo suficientemente capacitado con el fin de dar el mejor tratamiento a las evidencias digitales en investigaciones judiciales donde hagan parte elementos o equipos que funciones digitalmente.

A pesar de contar con el reconocimiento internacional en cuanto a normatividad sobre delitos informáticos, en Colombia, uno de los principales inconvenientes es la falta de preparación y conocimiento sobre este tema por parte de los jueces y fiscales, lo que genera retrasos ya que al no poder documentar de manera correcta estos casos, no se logra tipificar si estas conductas delictivas entran o no dentro de la clasificación de delitos informáticos, y es precisamente con el

tratamiento de la evidencia digital donde se presentan los mayores inconvenientes a la hora de procesar estos delitos[43].

Según el código penal colombiano contempla la mayoría de delitos informáticos ya inscritos como lo son: el acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño Informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, hurto por medios informáticos y semejantes y transferencia no consentida de activos, delitos amparados por la Ley 1273 de 2009.[44]

En Colombia ya se presentan diversos ataques a entidades de gobierno y privadas donde la fiscalía general de la nación cuenta con un espacio dentro de la página de fiscalía con un espacio donde plasman los delitos informáticos [45]

En Colombia lo más reciente ha venido siendo el malware ransomware ya que como experiencia en una unidad descentralizada de la gobernación del Meta fueron atacados por este malware encriptándo la información y cobrando en bitcoin

6.2 POSIBLES FALENCIAS EXISTENTES EN EL PROCESO DE CUSTODIA Y SU APLICACIÓN EN LA INVESTIGACIÓN DE DELITOS INFORMÁTICOS

Durante el proceso de recolección y análisis de la información concerniente a las investigaciones de delitos informáticos en Colombia, donde uno de los principales

[43] PÉREZ GARCÍA, Camilo. En Colombia se investigan delitos informáticos? [en línea]. [Citado en Septiembre de 2016]. Disponible en internet: https://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html
[44] Ley 1273 de 2009 [en línea]. [Citado en Enero de 2009].Colombia. Disponible en internet: http://www.mintic.gov.co/portal/604/w3-article-3705.html
[45] Tag: Delitos informáticos [en línea].[Citado en Diciembre de 2016]. Disponible en internet: http://www.fiscalia.gov.co/colombia/tag/delitos-informaticos/

elementos está directamente relacionado con la cadena de custodia y todo el tratamiento que se debe hacer sobre el material probatorio con que se cuente; desde la obtención hasta su procesamiento, se ha podido evidenciar la existencia de falencias en este proceso lo cual puede llevar a que las pruebas sean dañadas, manipuladas indebidamente o que pierdan su valor probatorio para los procesos judiciales.

A continuación se mencionan las principales falencias encontradas en el presente estudio del proceso de cadena de custodia y su aplicación en investigaciones de delitos informáticos en Colombia:

6.2.1 Desconocimiento de la metodología

Este es uno de los factores más relevantes ya que todo el proceso de cadena de custodia está muy bien estructurado y documentado, por eso, desconocer uno o algunos de los pasos y fases en los que se basa puede llegar a ocasionar no solo perdidas de la información sino también puede generar la anulación de la evidencia como material probatorio.

El hecho de no tener el conocimiento o experiencia en este tipo de procesos, pueden llevar a cometer errores durante alguno de los pasos a seguir, de igual forma se puede llegar a omitir el diligenciamiento de algún formato o validar más a fondo la información que se está recolectando.

"La legislación colombiana de delitos informáticos es suficiente, el problema es de conocimiento en la materia de parte de jueces, fiscales y organismos de policía judicial", comenta Andrés Guzmán, CEO de la firma Adalid Corp.

"En Colombia no existen fiscales ni jueces especializados en delitos informáticos. Si a un ciudadano le roban el carro puede dirigirse a una Fiscalía especializada en Automotores, pero si a esa misma persona la roban en Internet debe dirigirse a un

fiscal que en la mañana, por ejemplo, llevó un caso por inasistencia alimentaria", dice Guzmán.

"El reto más grande es que a pesar de que existe la Ley pocos jueces la entienden y a veces los fiscales no logran documentar los casos e identificar si realmente las conductas entran dentro de la tipificación de los delitos o no", señala el fundador de Mattica.

Resaltando estos aportes citados anteriormente se puede evidenciar que no es falta de reformar la legislación ni el debido proceso para el resguardo de la evidencia en una escena del crimen digital, si no es el fortalecimiento a jueces, magistrados y fiscalía, en el entendimiento de cómo lograr evidenciar la importancia del peritaje y de los resultados de la cadena de custodia en la informática forense, mediante capacitaciones constantes y entregando certificaciones que los avalen como expertos del tema y así poder contar con una línea de profesionales expertos en el área para brindar mayor respaldo y seguridad a la ciudadanía en el resguardo de la información y la vinculación de la tecnología en todos los procesos de gestión personal, laboral y social.

6.2.2 Falta de herramientas adecuadas

Como se evidencio durante la elaboración del presente documento, a la hora de llevar a cabo la cadena de custodia de evidencias digitales, es muy importante contar con las herramientas necesarias tanto de software como de hardware con el fin de hacer un manejo adecuado de la información.

Por lo anterior se debe tener en cuenta a la hora de seleccionar las herramientas de software por ejemplo, que deben ser las más adecuadas y que cumplan con los requerimientos que aseguren que la evidencia adquirida no pierda valor probatorio.

Para Iván Darío Marrugo, abogado especialista en Derecho de Telecomunicaciones, el proceso de investigación y el de prueba pericial e informática es la principal dificultad para procesar este tipo de delitos. "Solo desde hace unos años tenemos una Ley de procedimiento administrativo (Ley 1437 de 2011) y el Código General del Proceso (Ley 1564) que abrió la posibilidad de admitir pruebas electrónicas en este tipo de juicios", agrega.

De igual forma se debe contar con los equipos necesarios y con las características que el proceso de cadena de custodia ameritan, ya que en ocasiones puede llegar a hacerse uso de equipos obsoletos y sin la suficiente capacidad para lo que se requiere en estos casos; los espacios o laboratorios deben estar adecuados para la recepción y tratamiento de la información o evidencia que se recibe en los diferentes medios físicos.

A nivel internacional se ha venido dando mayor importancia a la informática forense en los años recientes. Para Adrián Rodríguez, consultor de seguridad informática de la empresa Digiware en Colombia, a raíz de los atentados del 11 de Septiembre de 2001 en los Estados Unidos, se hizo evidente la necesidad de mejorar la seguridad en los sistemas de información y en los mecanismos para recuperar datos después de un “ataque”.

Pero en la actualidad, sostuvo Rodríguez, “se han agregado nuevas cualidades de monitoreo que permiten recobrar más información y utilizando los protocolos adecuados, presentar y preservar la evidencia hallada como una prueba válida en un caso legal”.

Según Igor León, especialista en seguridad de Etek Internacional “solo hasta la década de los noventa se desarrollaron herramientas de software como SafeBack

y DIBS que permitieron recolectar los datos en discos, sin alterar la información original".[46]

6.2.3 Manejo inadecuado

En ocasiones la manipulación no adecuada de la evidencia digital bien sea al momento de su obtención, verificación o transporte, también puede convertirse en un factor determinante para la pérdida del valor probatorio de la evidencia digital. Vale la pena recordar que una de los principales objetivos de la cadena de custodia es velar para que la integridad de la evidencia digital o prueba se conserve hasta que ésta sea entregada a quien corresponda bien sea una persona o entidad judicial para que sea tenida en cuenta en el proceso a que tenga lugar y que no quede la menor duda de contaminación o daño para que esta conserve su valides dentro de la investigación o proceso judicial[47].

Para dar un claro ejemplo sobre este punto, se toma como referencia uno de los casos más reconocidos internacionalmente como lo es el del computador incautado tras la muerte de Raúl Reyes en un operativo militar, donde el fiscal Ecuatoriano Washington Pasántez recibió por parte del Gobierno Colombiano una copia del disco duro de dicho computador para su análisis y dependiendo de los resultados, estos se anexarían a la investigación tras el bombardeo a un campamento de las FARC el 1 de marzo de 2008 en territorio Ecuatoriano.

"Al margen de las formalidades, esta evidencia digital es un material que tiene calidad de evidencia (...) y debe recibir el tratamiento técnico y profesional que el

[46] PIÑEROS, Gonzalo. Los detectives de la era digital. [En línea]. [Citado en Noviembre de 2016]. Disponible en internet: http://www.enter.co/archivo/los-detectives-de-la-era-digital/

[47] Análisis forense. Cadena de custodia de la evidencia digital. [en línea]. [citado en Octubre de 2016]. Disponible en internet: http://www.securityartwork.es/2016/02/10/analisis-forense-cadena-de-custodia-de-la-evidencia-digital/

caso amerita", señaló Pesántez y agregó que, de comprobarse su autenticidad, "puede ser introducido como una prueba y ser valorada por la Justicia".[48]

En su momento además agregó que los peritos verificarían el contenido y analizarían si la información digital fue manipulada después de su incautación en 2008 pues, a criterio de Pesántez, "no se respetó la cadena de custodia".

Por consiguiente la cadena de custodia en informática forense tiene la muy compleja misión de asegurar que las pruebas o resultados encontrados según los procesos realizados en una escena de crimen, deben constatar ante un juez que son verídicas, confiables que puede ser demostrable por cualquier perito del mundo así realicen pruebas con herramientas diferentes ya que el resultado siempre será el mismo. Llegado este momento es donde la contraparte solicita realizar los estudios para poder desmentir dicha prueba con otros análisis.
La poca capacitación y actualización de procesos a los jueces e investigadores de la fiscalía referente a los procesos peritales en informática forense permiten vacíos y nublar las pruebas con pregustas tales como ¿Cómo sabemos, en el momento en que realizamos nuestra práctica forense, que estamos ante lo mismo que se recolectó en su día? Ya que se puede presumir que por ejemplo en un disco duro con fotos estas pueden ser alteradas o modificadas sin mayor dificultad, sin perder la fecha, hora y el tamaño de bytes, esto claro sin que se abran los ficheros. Marcaciones como estas ha permitido que una prueba forense sea descartada como evidencia judicial.

6.3 INFORME DE POSIBLES MEJORAS PARA EL PROCESO DE CADENA DE CUSTODIA DE EVIDENCIAS DIGITALES

[48] El Tiempo. La Fiscalía de Ecuador entregó a expertos copia del disco duro del computador de 'Raúl Reyes'. [en línea]. [citado en Noviembre de 2016]. Disponible en internet: http://www.eltiempo.com/archivo/documento/CMS-7859929

A continuación se describen las principales mejoras a tener en cuenta con el fin de ser aplicadas al proceso de cadena de custodia en la investigación de delitos informáticos en Colombia una vez evidenciadas las principales falencias que se pueden presentar en este proceso.

El presente informe está dirigido a todo el personal con formación en Informática forense, seguridad informática y demás áreas que se relacionen con los temas tratados en este documento, al personal que hace parte de las diferentes unidades de investigación criminal de delitos informáticos de las instituciones del Estado y en general al personal que está vinculado directamente a este tipo de investigaciones bien sea para impartir justicia o llevar a cabo procedimientos técnicos y que lo quieran tomar como referencia con el fin de documentarse sobre el proceso de cadena de custodia en investigaciones de delitos informáticos en Colombia.

6.3.1 Mejoras a tener en cuenta

Se debe dar gran importancia a la formación y especialización de los investigadores de policía judicial y de las diferentes entidades investigativas ya que a pesar de contar con tecnología relativamente y buena, el personal debe ser profesional en ingeniería de sistemas.

La capacitación necesaria para desarrollar este tipo de actividad debe ser permanente, de igual forma se estima que la formación de un perito o investigador forense tiene un costo aproximado de 50 millones de pesos; por este motivo es importante la continuidad del personal ya que si se capacita no debe ser cambiado de área.

Se requiere fortalecer la especialización policial que le permita al personal de investigadores forenses, desarrollar una carrera en esta área y mejorar sus conocimientos en hacking.

Para mitigar el desconociendo de los fiscales y jueces de la nación, en el ámbito de los delitos informáticos se deben plantear el fortalecimiento de expertos que brinden asesoramiento y capacitaciones constantes en seguridad de la información, resaltando temas como las vulnerabilidades de los sistemas de información, en la arquitectura de almacenamiento físico, en conocer la importancia e historial a nivel mundial de los crímenes y/o delitos resueltos por expertos del peritaje informático, las herramientas de análisis, los procesos y procedimientos los cuales son de naturaleza universal pero se van actualizando y modernizando por el crecimiento constante de la tecnología. Esto con el fin de ampliar las fronteras del conocimiento de fiscales y jueces y con ello poder contar con expertos que permitan brindar mayor credibilidad y objetividad para el sistema acusatorio y de justica.

En el sector público y privado se debe brindar cursos resaltando la importancia de la seguridad de la información, con un enfoque en la norma ISO 27001 la cual permite documentar los procesos de la información tangible e intangible de una entidad. Con ello se puede implementar cursos, talleres y seminarios con temas como.

- ✓ Delitos Informáticos y Ciberseguridad.
- ✓ Privacidad y Protección de Datos en Internet.
- ✓ Propiedad Intelectual en Internet.
- ✓ Responsabilidad Legal de Sitios y Buscadores.
- ✓ Uso Responsable de Internet
- ✓ Aspectos Legales de la Seguridad Informática.
- ✓ Resguardo de la seguridad de la información.
- ✓ Cuidado de la privacidad y la reputación online.
- ✓ Consecuencias de la publicación de contenidos.
- ✓ Prevención de engaños y estafas informáticas.

- ✓ Respuestas al hostigamiento online (cyberbullying).
- ✓ Detección de extorsiones sexuales (grooming).
- ✓ Denuncia e investigación de los delitos informáticos.

También se debe evaluar e implementar la norma ISO 27034 la cual habla de la seguridad de aplicaciones ya que proporciona una guía de seguridad de la información dirigida a los agentes de negocios y de TI, auditores, desarrolladores y todos los usuarios finales de TIC.[49]

El objetivo principal de la norma ISO 27034 es asegurar que todas las aplicaciones informáticas desarrolladas para un fin comercial, social, financiero o de cualquier otro orden, contenga un nivel adecuado de la seguridad con apoyo del tratamiento del sistema de gestión de seguridad de la información SGSI

La ISO 27034 permite enfocar aplicar, seleccionar y orientar los controles de seguridad de la información mediante un conjunto de procesos ya integrados a través del desarrollo del sistema de ciclo de una organización, estos son software internos los cuales se han adquirido de forma externa con enfoques híbridos.

El alcance de la norma ISO 27034 es entregar lineamientos para el tratamiento de la evidencia digital y establece las siguientes actividades: identificación, recolección, adquisición y preservación de almacenamiento digital como dispositivos móviles, GPS, circuito cerrado de televisión, dispositivos en red TCP/IP o similar.

En general la norma ISO 27034 es muy apropiada y compleja ya que fuera de entregar definiciones, conceptos y procesos que se ejecutan en la seguridad de un sistema, también pude aplicar gestión y control a dichas aplicaciones

[49] ISO 27034 Seguridad de aplicaciones [en línea].[Citado en abril de 2014]. Disponible en internet: http://www.pmg-ssi.com/2014/04/iso-27034-seguridad-de-aplicaciones/

desarrolladas internamente, las adquiridas a terceros y donde el funcionamiento es subcontratado con el fin de mitigar vulnerabilidades a los sistemas.

Todas estas recomendaciones son generalizadas para contar con profesionales del ámbito judicial y penal más especializados para entender que los delitos informáticos son cada día más constates y que se deben contrarrestar con personal más idóneo y conocedores del tema, como los profesionales del ámbito acusatorio, jueces y magistrados

Validando las cuatro etapas de la cadena de custodia. Identificación, adquisición, análisis y presentación se exponen las siguientes mejoras.

Cuando se realiza un hallazgo de un delito digital la identificación como parte inicial para el proceso de cadena de custodia se recomienda que se inicie las medidas de seguridad como lo debe ser la identificación si el delito está todavía en progreso también validar el estudio del entorno de la escena del crimen y la situación generada, se debe realizar valoración de las políticas de la empresa o entidad afectada si la tiene, evaluación de los recursos, parametrizar el alcance y los objetivos de la investigación y generar investigaciones que permitan determinar el estado actual del sistema, que partes fueron afectadas, la sensibilidad de la información y la gravedad de los hechos la cual permita obtener un informe analítico de la situación, con ellos fijar la ruta precisa de la investigación.

Luego en la adquisición de las evidencias como primera medida se debe identificar el grupo de especialistas para dicha recopilación de inventario y pruebas digitales para ello los profesionales deben contar con los trajes adecuados para no contaminar la escena del crimen ya que la estática puede alterar o contaminar los elementos electrónicos, se recomienda que usen zapatos y guantes apropiados.

Se debe sacar una imagen de los disco a intervenir con código hash para conservar el original y a este se le genera una nueva imagen para analizar. La recolección de la evidencia digital siempre se deben trabajar en pareja para no dejar pasar cualquier evidencia y su fijación, para ello debe ser bien rotulado y firmado por los dos. "investigador de campo"

Ya evidenciado todo el suceso, custodiado y rotulado se embala y se envía a laboratorio, para la fase de análisis, en el laboratorio se implementaran las herramientas necesarias para el fin específico planteado por los investigadores según el suceso.

También es muy importante seguir los lineamientos que entrega el Ministerio de TIC, el cual parametriza una serie de procesos según documento “Seguridad y privacidad de la Información”[50]

Donde el documento expone una serie de proceso para el levantamiento de la cadena de custodia resaltando las buenas prácticas de recolección y análisis de la información. En esta fase se recomienda que los investigadores y/o peritos forenses realicen los siguientes procesos.

- ✓ Creación del archivo / bitácora de hallazgos (cadena de custodia)
- ✓ Imagen de datos
- ✓ Verificación de integridad de la imagen - (sha1/md5).
- ✓ Creación de una copia de la imagen suministrada
- ✓ .aseguramiento de la imagen original suministrada
- ✓ Revisión antivirus y verificación de la integridad de la copia de la imagen
- ✓ Identificación de las particiones actuales y anteriores
- ✓ Detección de información en los espacios entre las particiones
- ✓ Detección de un HPA (host protected área)

[50] Seguridad y Privacidad de la Información [en línea]. [Citado en mayo de 2016].MinTIC. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

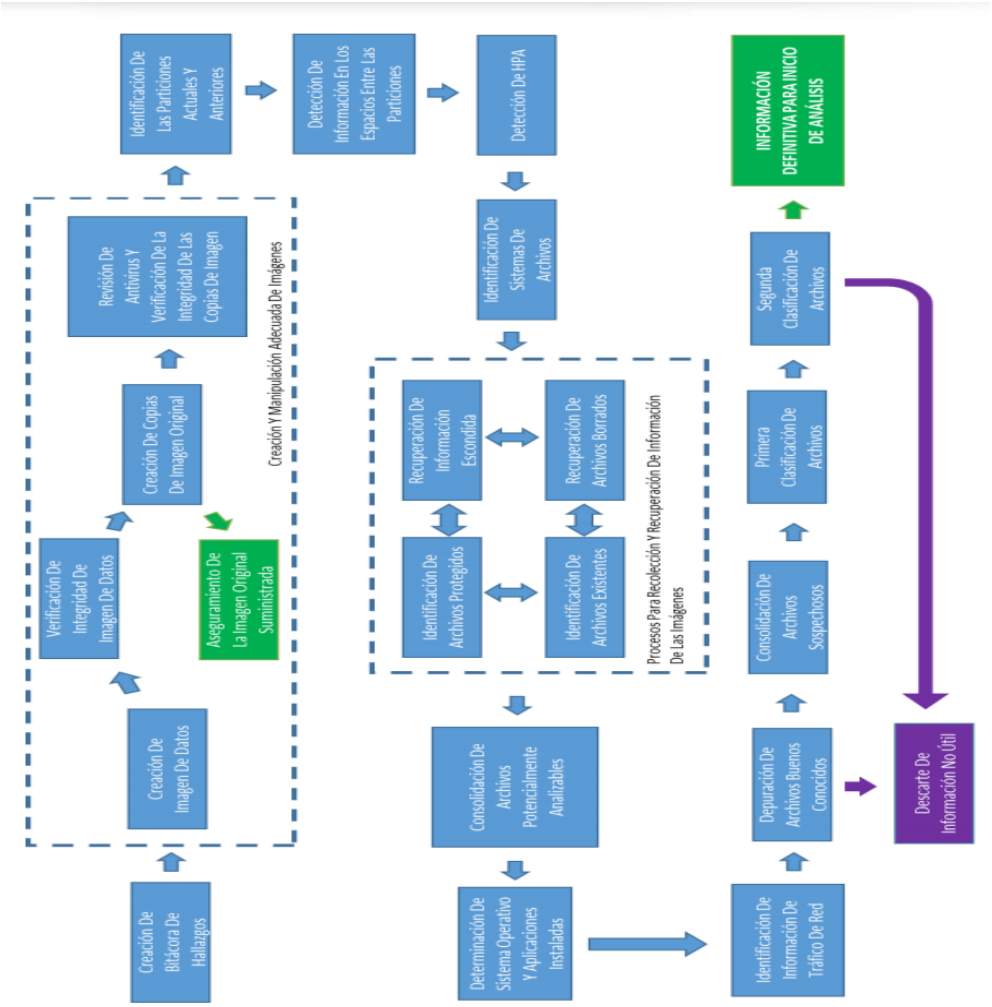
- ✓ Identificación del sistema de archivos
- ✓ Recuperación de los archivos borrados
- ✓ Recuperación de información escondida
- ✓ Identificación de archivos existentes
- ✓ Identificación de archivos protegidos
- ✓ Consolidación de archivos potencialmente analizables
- ✓ Determinación del sistema operativo y las aplicaciones instaladas
- ✓ Identificación de información de tráfico de red
- ✓ Depuración de archivos buenos conocidos
- ✓ Consolidación de archivos sospechosos
- ✓ Primera clasificación de archivos
- ✓ Segunda clasificación de archivos

Es válido resaltar que para lograr el objetivo de encontrar las causales de algún delito o anomalía presentado en un sistema de información o herramienta tecnológica no está de más contar con algunas recomendaciones para examinar y recolectar la información.

- ✓ Como lo es poder contar siempre con el equipo de incidentes para formular la manera adecuada de recolectar la información y así extraer la mayor cantidad posible para el análisis.
- ✓ Aislar cuando se requiera los equipos afectados del entorno o red para mitigar la incidencia de algún error o para preservar la evidencia.
- ✓ Controlar el impacto y la consecuencia de sacar un sistema de línea para generar una imagen la cual pude tomar mucho tiempo para la investigación.
- ✓ Utilización de herramientas forenses expertas tanto software y de hardware como una estación forense, que asegure la integridad de la información.
- ✓ Es muy importante poder recolectar y recibir la información con las estampas de tiempo precisas es decir, que todas las plataformas de

información se encuentren sincronizadas con un mismo reloj o servicio NTP. Esto garantizará mayor precisión en los estudios posteriores.

Figura 3. Diagrama de Examen y Recolección de Información



Fuente: MinTic https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf pag. 24

En el análisis la evidencia digital entrega cualquier tipo de información como datos, registros, formatos, archivos y extensiones los cuales están inmersos en los discos duros, memorias RAM, redes, temporales y demás plataformas de

almacenamiento electrónico y sistemas operativos, lo cual conlleva un reto poder generar de forma acertada un análisis forense.

La recomendación respecto a las herramientas utilizadas para la informática forense es la siguiente:

6.3.2 Hardware

- Procesador de cuatro núcleos.
- Entre 4 y 8 GB de memoria RAM.
- Capacidad de almacenamiento en el disco duro de al menos 1 terabyte (TB), es decir, 1.000 GB.
- Sistemas operativos que trabajan a 32 y 64 bits.
- Varias unidades ópticas, algunas con ‘quemador’ de CD y DVD, y otras solo para lectura de discos.
- Lo anterior con un costo aproximado de $ 31.880.000.

6.3.3 Software

Existe gran variedad de herramientas que permiten evidenciar procesos o indicios del flujo de la información en un ordenador, Tablet, celular, servidores o redes locales, las cuales sirven como evidencia para un tribunal.

Para el análisis forense existen herramientas específicas según la línea de investigación y/o la arquitectura de la red a analizar, de las cuales se proponen las más eficientes a la hora de realizar un análisis forense.

Para el análisis de las Redes tenemos dos sistemas muy relevantes por su eficiencia en el rastreo y captura del tráfico de datos en una red local.

HIDS (HosttlDS): un IDS para Host permite identificar rastros de intrusos en los equipos de una red.

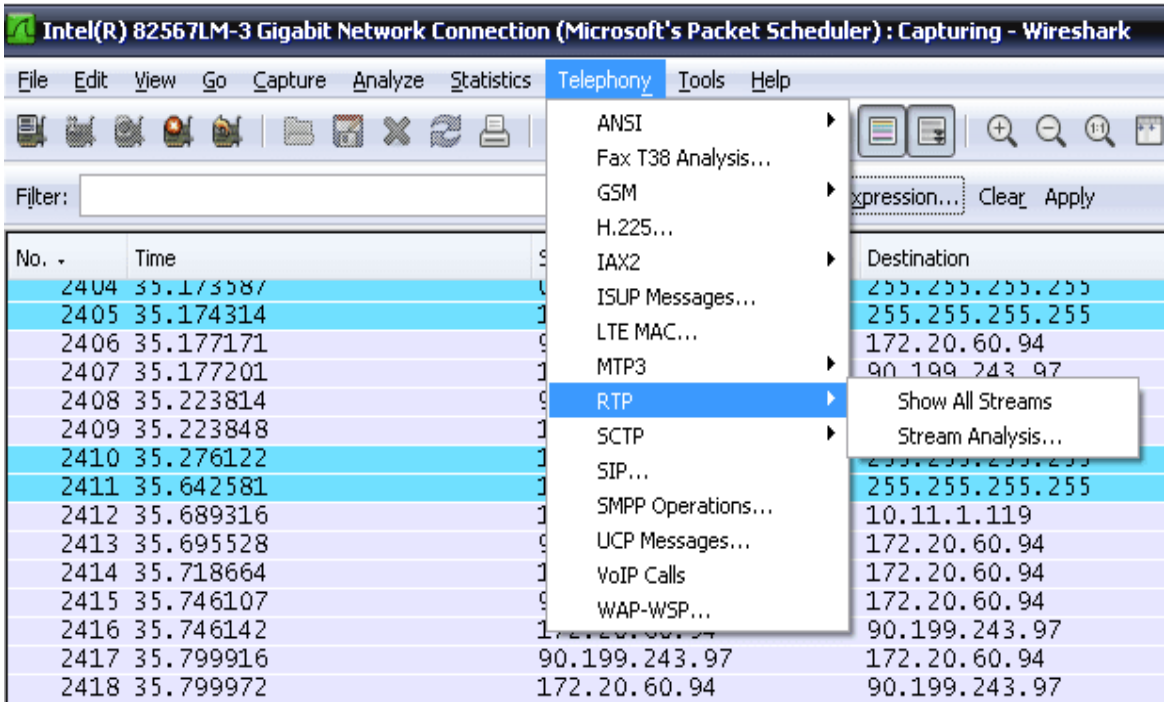
NIDS (NetwordkIDS: Permite detectar en todo el segmento de la red el rastro dejado por un intruso, por ende debe trabajar en modo promiscuo para capturar la totalidad de la red.

Otros programas recomendados son TCPDump el cual permite analizar el tráfico de la red mediante línea de comando y permite identificar problemas en la red como capturar datos que se trasmiten en la red sin ningún proceso de encriptación.

Para acceder a esta herramienta esta la versión 4.9.2 la cual fue lanzada el 3 de septiembre de 2017 en el sitio oficial url. http://www.tcpdump.org/
También es muy utilizado la herramienta WireShark: la cual permite capturar tramas y paquetes que viajan en una red local por medio de una interfaz de red, esta herramienta posee todas las características necesarias de un analizador de protocolos.

Para poder acceder a esta herramienta, ingresar al sitio oficial url. https://www.wireshark.org/

Figura 4. Pantallazo de wireshark

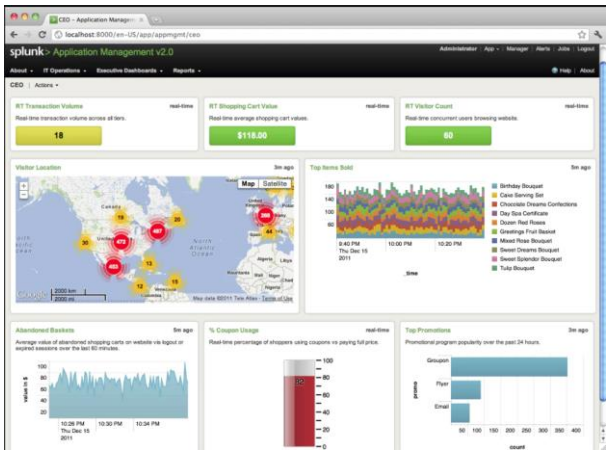


Fuente: Wireshark.

Splunk es un software muy utilizado en los sistemas de operación y gestión más importantes del mercado, permitiendo el monitoreo y análisis del tráfico de la red, detectando transacciones, registro de llamadas y sitios de navegación de los usuarios, adicional a ello el sistema cuenta con un módulo de firmado de datos, el cual permite entregar unas pruebas de autenticación en cualquier proceso de análisis forense o auditoria.

Existe diversidad de herramientas que realizan funciones similares en el análisis de datos en la red como Network Appliance Forensic Toolkit desarrollado en Python, NetworkMiner analiza la red utilizando filtros, Xplico extrae datos de la red utilizando el protocolo HTTP y los mensajes que tienen implementado el protocolo POP y SMTP, entre otros.

Figura 5. Aplicativo Splunk



Fuente: Imgix.

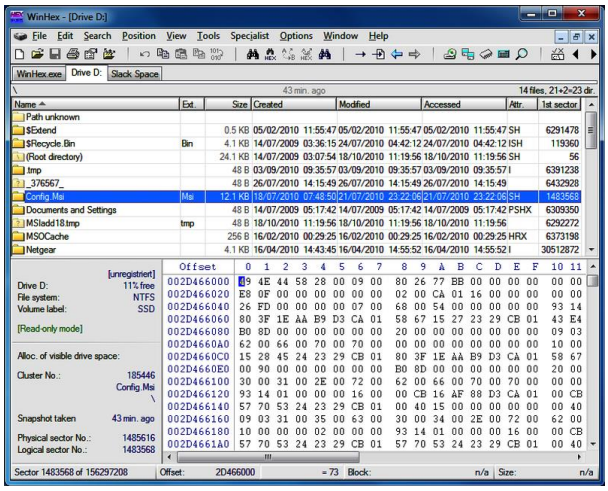
Para poder acceder a esta herramienta, ingresar al sitio https://www.splunk.com/en_us/download/splunk-enterprise.html

Así como están estas herramientas para validar y analizar el tráfico de una red también existen herramientas para otros aspectos dentro del análisis forense, como lo son:

Editores Hexadecimales (WinHEX). Permite editar todos los tipos de archivos, memorias RAM y dispositivos de almacenamiento, también permite recuperar archivos borrados en dispositivos con sistemas de archivos corruptos. GHEX este editor es solo para el ambiente o suite de Linux.

Para poder acceder a esta herramienta, ingresar al sitio http://www.winhex.com/winhex/index-m.html

Figura 6. Editores Hexadecimales (WinHEX)



Fuente: Techworld.

Recuperación de Archivos o proceso “Carving” el cual se define como extracción de un conjunto de datos que se encuentran inmersos en otro conjunto de datos.

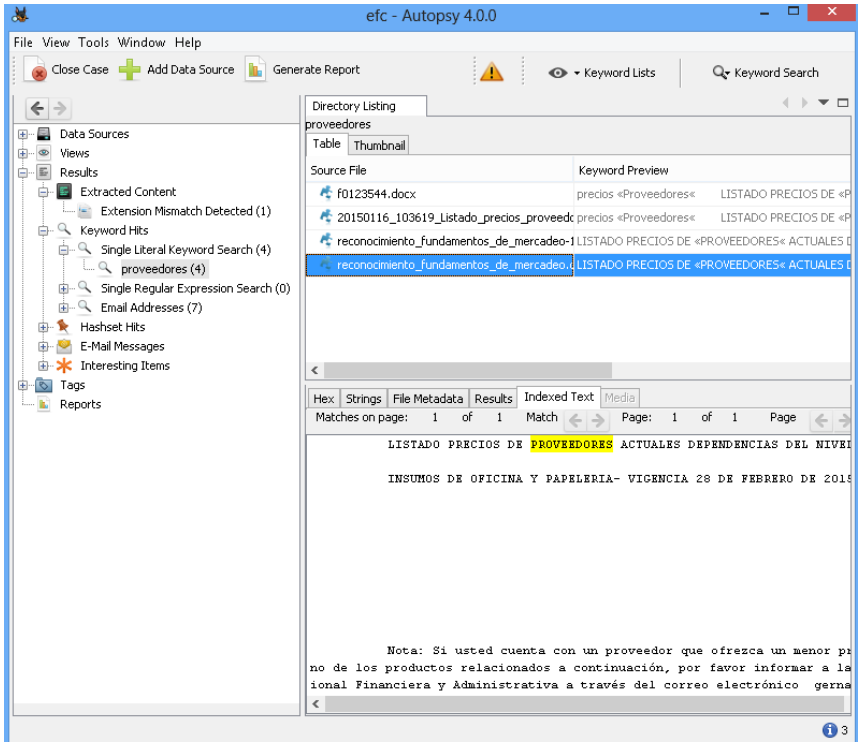
Entre ellos tenemos a Raid Recovery, Raid Reconstructor, NTFS Recovery, Linux Recovery, Recuva, CNW Recovery, Rstudio entre otros los cuales permiten recuperar archivos de múltiples sistemas de archivos

6.3.4 Suit estandarizada para el análisis forense

Autopsy y Sleuth Kit, son las herramientas más importantes en el análisis forense de grandes volúmenes de sistemas y archivos.

Este software se encuentra incorporado en las herramientas del sistema operativo de Kali Linux o también lo pueden descargar del sitio oficial https://www.autopsy.com/download/

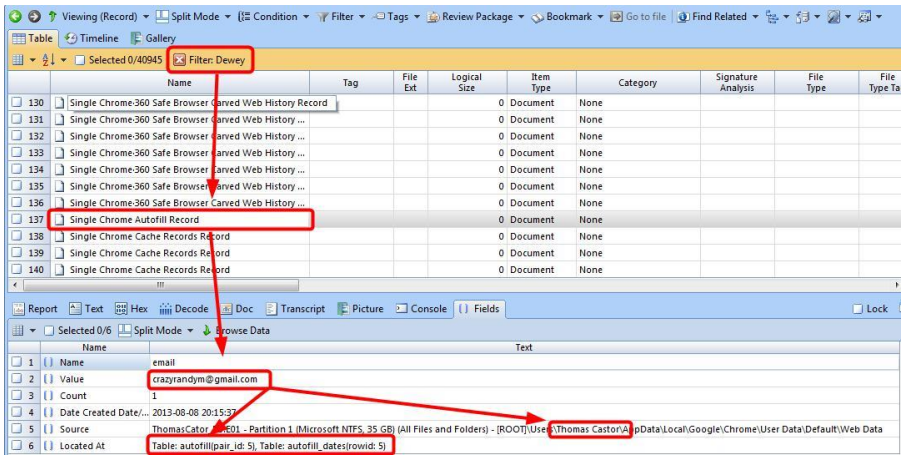
Figura 7. Autopsy



Fuente: Autor.

El software **ENCASE Forensic** es el líder mundial para el análisis forense informático por su eficiencia en el tratamiento de la información y su capacidad de realizar copias comprimidas sin pérdida alguna de la información y realizar comparaciones con otras copias en paralelo sin perder capacidad, también permite ser trabajado de forma local o en red, este software es ideal para realizar investigaciones donde se deba identificar hallazgos o alteraciones de la información en algún ordenador.

Figura 8. ENCASE Forensic



Fuente: 2.bp.blogspot.com.

El software se encuentra en la url. https://www.guidancesoftware.com

Otros sistemas especializados en el análisis forense más usados son:

OSForensics. Esta cuenta con un amplio conjunto de herramientas y entre ellas está la capacidad de analizar sobre copias de discos montados en el sistema, búsqueda de archivos y generación de código Hash.

Figura 9. OSForensics

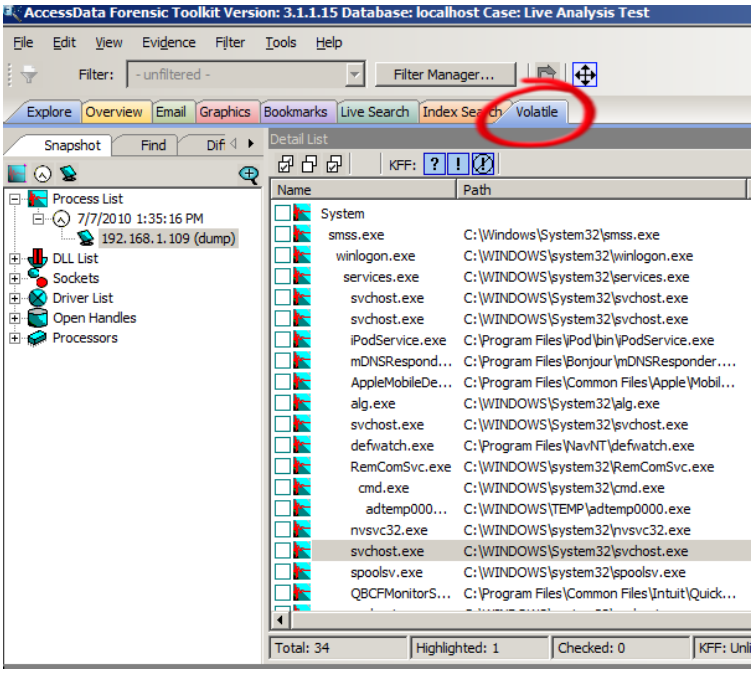
Fuente: Dottech.

El software se encuentra en la url. https://www.osforensics.com/download.html

ForensicsToolkit. Esta herramienta permite gestionar cientos de ficheros con parámetros definidos permitiendo al investigador encontrar evidencia más rápidamente, tiene la capacidad de ubicar archivos por tipo analizando sus cabeceras, evidenciando extensiones y archivos modificados intencionalmente, también entrega informes detallados de los análisis.

El software se encuentra en la url. https://forensic-toolkit.soft32.com/

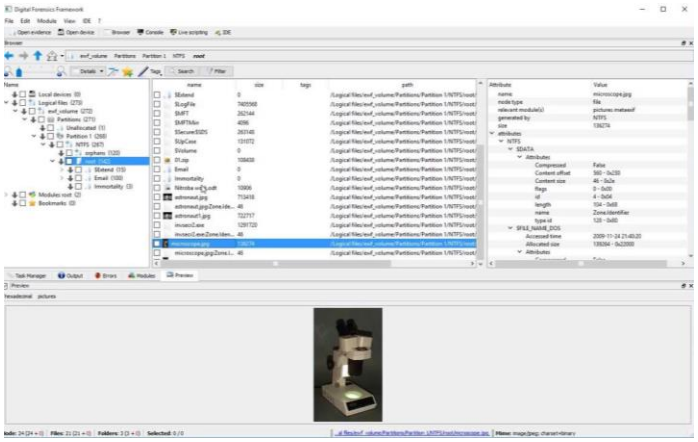
Figura 10. Forensic Toolkit



Fuente: blogs.sans.org

Digital Forensic Framework (DFF). Este contiene una interfaz gráfica amigable para ser usado por personas no tan expertas, sus ventajas son la capacidad de preservación de la evidencia digital (cadena de custodia) cuenta con funcionalidad de bloqueo de escritura de software y cálculo de hash criptográfico, lee formatos de archivos forenses digitales como Ewf, AFF 3, formatos de archivo RAW, reconstruye discos de máquinas virtuales, análisis de archivos en Windows y Linux, recupera archivos ocultos y eliminados entre otras funcionalidades que hacen de este framework un herramienta muy importante y además cuenta con licenciamiento libre y código abierto.

Figura 11. Digital Forensic Framework (DFF)



Fuente: i.ytimg.com

El software se encuentra en la url. http://www.digital-forensic.org/downloads

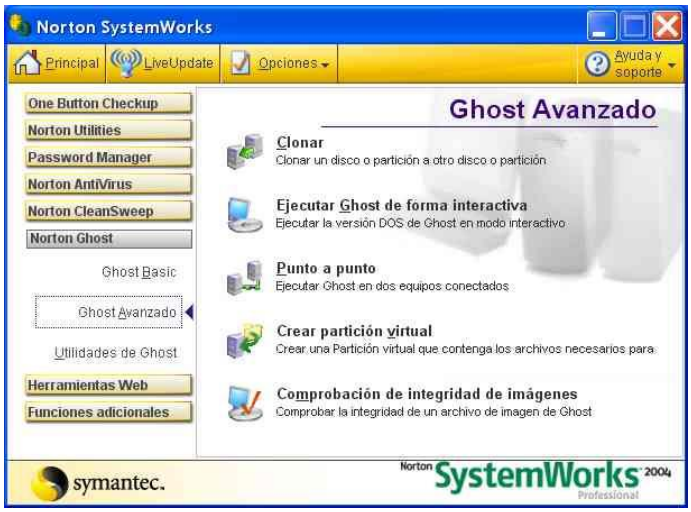
Herramientas de Clonación.

Este tipo de herramientas permiten generar una imagen o copia exacta de un disco o una partición del mismo, entre el software más eficientes se tienen:

Ghost: este software permite realizar imágenes copiando también su contenido o una partición, también es capaz de copiar discos más grandes y en formato de restauración para ser instalado en otro equipo.

El software se encuentra en la url. http://www.portalprogramas.com/norton-ghost/

Figura 12. Ghost

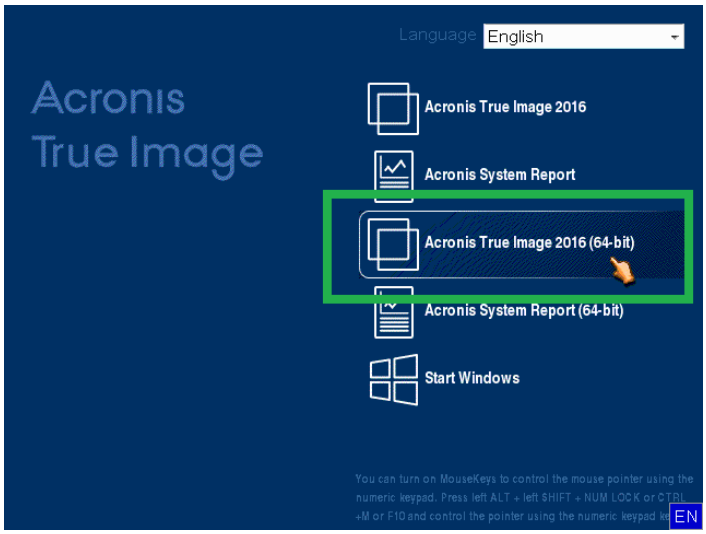


Fuente: ugc.kn3.net/i/origin/http://www2.configurarequipos.com

Acronis: este software es tan potente que puede clonar de forma exacta servidores Windows y Linux con todos sus componentes como la BD, SO y sus aplicaciones instaladas, de igual manera dicha clonación se pueden migrar a servidores virtuales o locales.

El software se encuentra en la url. https://www.acronis.com/es-mx/

Figura 13. Acronis

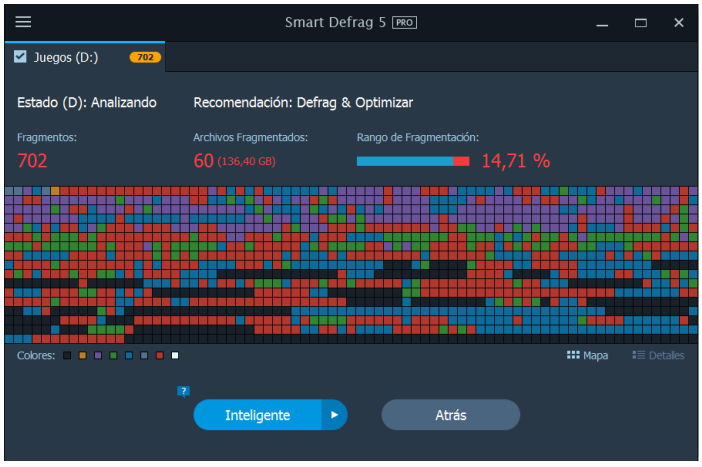


Fuente: dl2.acronis.com

Referente al **análisis de discos** tenemos **Smark**, cuya finalidad es el apoyo en el análisis forense identificando todos los dispositivos de almacenamente conectados y evidenciando la marca, modelo, capacidad y serial de los equipos.

El software se encuentra en la url. https://www.iobit.com/es/iobitsmartdefrag.php?a

Figura 14. Smark análisis de discos



Fuente: softzone.es

El programa **ILook** su principal característica es extraer y analizar imágenes digitales como cabeceras de archivos para verificar si pertenece los archivos a su tipo. También se pude garantizar la usabilidad de otros programas como ImDisk, Daemon Tools y **PassMarks OSFMount**.

Referente al **análisis de memoria RAM** podemos resaltar las funcionalidades de los siguientes Software.

FTK Imager. Software especializado en la recuperación y análisis de memoria RAM. **Proccess Dumper (DP)** este nos permite exportar un proceso de la memoria RAM en un archivo, **Volatility** permitiendo evidenciar los procesos que se están ejecutando en la memoria RAM y extrae información relevante y puntual de procesos.

Sistema de archivos: software para el tratamiento de la tabla maestra de archivos (MFT: Master File Table) y el (Directorio Prefetch) para darle tratamiento directo a la tabla maestra de archivos tenemos los programas “AnalyzeMFT, MFT Extractor, MFT Tools y MFT_Parser para darle tratamiento directo sobre el Directorio Prefetch usamos: Prefetch Parser y WinPrefectchview

Para los análisis de registros de Windows se debe realizar gestión sobre la shellbags que hacen referencia a los espacios donde el sistema operativo Windows guarda la información de las interacciones visuales de su interfaz gráfica de cada usuario.

Los programas más utilizados para tal fin son:

RegRipper muestra, extrae y correlaciona la información del registro. **WRR** este software permite obtener de forma gráfica datos del sistema, usuarios y

aplicaciones desde el registro de Windows. **Shellbag Forensics:** permite analizar de forma detallada la Shellbag de Windows.

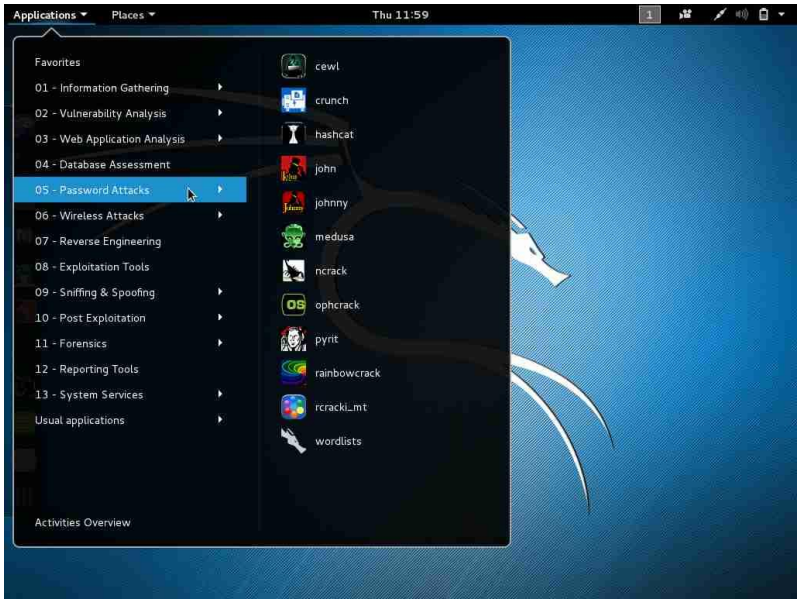
Las distribuciones de Linux en el ámbito de la seguridad informática y análisis forense que más tienen relevancia son:

KALI: Distribución de Linux especializada en Seguridad Informática, basada en SO Debian, está dirigida a la gestión de auditorías de seguridad enfocada al sector profesional.

Este sistema operativo es muy potente para la realización de control y gestión de vulnerabilidades de las redes y sistemas de integración de datos como base de datos, páginas web y demás sistemas de información, todas sus herramientas están enfocados a realizar tareas en el ámbito de la seguridad informática.

El software se encuentra en la url. https://www.kali.org/

Figura 15. Sistema Operativo Kali Linux

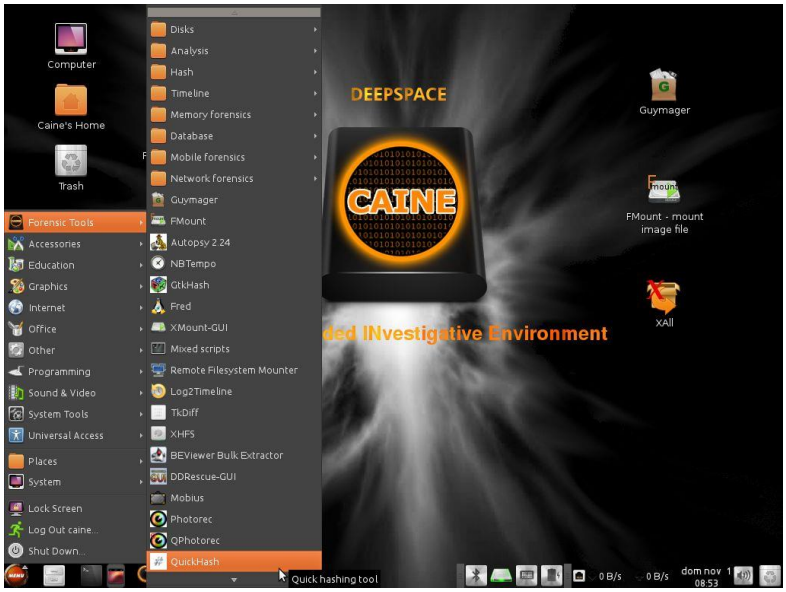


Fuente: techxstar.com

CAINE: Distribución de Linux, origen italiano enfocado al análisis forense, basada en SO Ubuntu, entregando un entorno interoperable que respalda al investigador digital durante las cuatro fases de la investigación digital.

El software se encuentra en la url. http://www.caine-live.net

Figura 16. Sistema Operativo CAINE

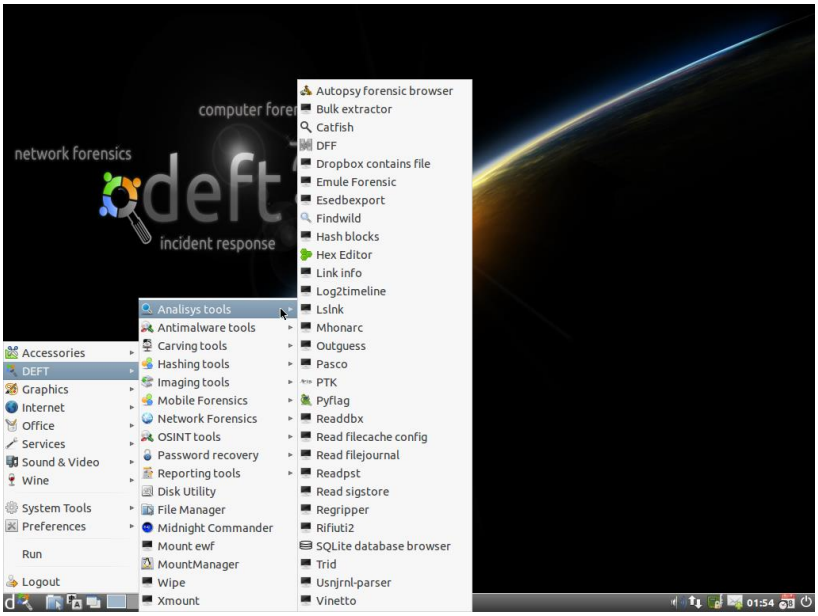


Fuente: uaeinfosec.com

DEFT: Distribución de Linux, enfocada al análisis forense, tanto en discos duros como en red y dispositivos Móviles, basado en Ubuntu.

El software se encuentra en la url. http://www.deftlinux.net/

Figura 17. Sistema Operativo DEFT



Fuente: Linuxbsdos.

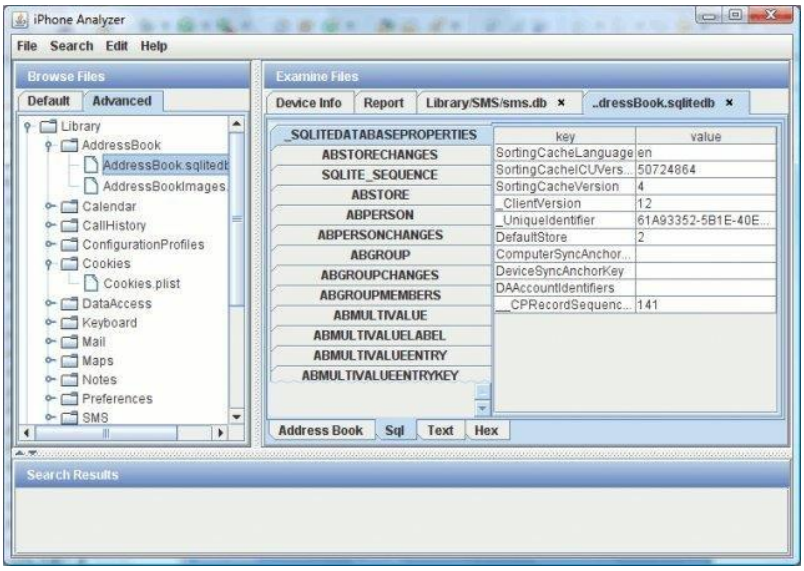
6.3.5 Programas y herramientas para dispositivos Móviles[51]

IPhone Analyzer. Es una aplicación de IOS que cuenta con las siguientes características. Permite Explorar iPhone y generar Backup, visualización de archivo nativo, con visualización (plist, SQLite, etc), incluye expresiones regulares, acceso ssh para los teléfonos con jailbreak (beta), Informes, Restaurar archivos, recuperar copias de seguridad, Ver todas las fotos del iPhone, examinar la libreta de direcciones, SMS y las cargas de los demás, encontrar y recuperar las contraseñas, entre otras.

El software se encuentra en la url.
https://sourceforge.net/projects/iphoneanalyzer/files/

[51] PEDREROS MARTÍNEZ, Wilson Leonardo y SUÁREZ URRUTIA, Jennifer Catherine. Herramientas aplicadas en el desarrollo del análisis forense informático en Colombia. Universidad Militar Nueva Granada. Bogotá, 2016.

Figura 18. IPhone Analyzer



Fuente: a.fsdn.com

Androguard: permite guardar, analizar, visualizar y modificar sus aplicaciones y de forma estática ya que mediante la ejecución de su mismo software o API, o también mediante la herramienta (androlyze) ejecutada en la línea de comando, este software es utilizado para hacer ingeniería inversa en aplicaciones específicas como el malware.

El software se encuentra en la url. https://n0where.net/android-application-analysis-androguard/

AFLogical OSE - Open source Android Forensics app and framework. Aplicación en formato APK que debe ser previamente instalada en el Android, permite extraer información de la tarjeta SD (registro de llamadas, listado de contactos y de aplicaciones instaladas, mensajes de texto y multimedia) y posteriormente ésta debe ser recuperada o bien conectando la tarjeta a un dispositivo externo o mediante el ADB.

El software se encuentra en la url. https://github.com/nowsecure/android-forensics/downloads

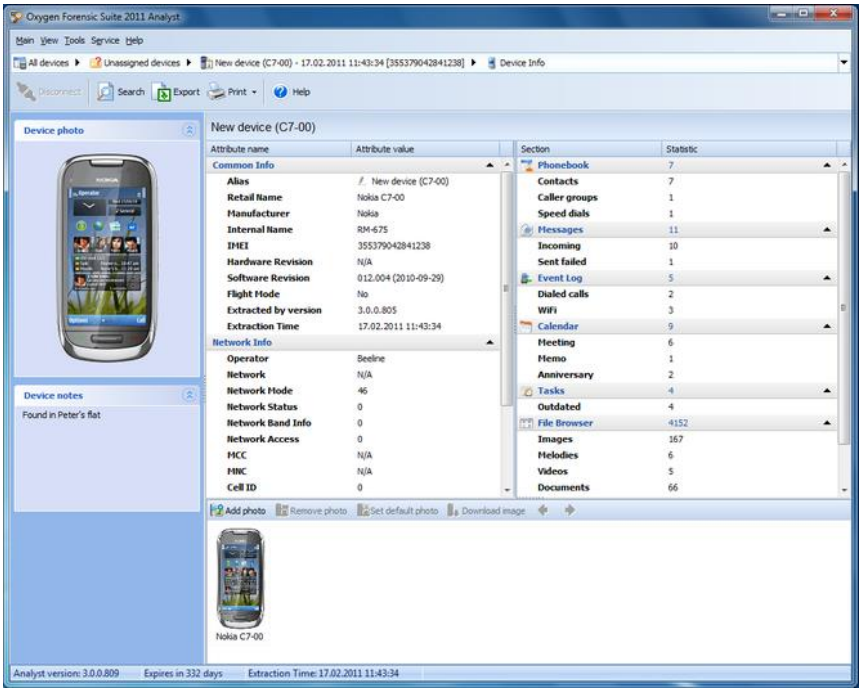
FTK Imager Lite se gestiona mediante volcados de memoria de dispositivos móviles para poder analizarlos y obtener evidencias.

El software se encuentra en la url. http://accessdata.com/product-download/ftk-imager-version-3.4.3

Oxygen Forensic Suite manifiestan que logran obtener información de más de 10.000 modelos diferentes de dispositivos móviles e incluso obtener información de servicios en la nube e importar backups o imágenes, lo cual sería adecuado para el análisis a algún equipo confiscado.

Es importante ampliar la infraestructura tecnológica y la cobertura en las diferentes entidades del Estado Colombiano para que los diferentes organismos cuenten con laboratorios adecuados y con tecnología de punta; en la actualidad se cuenta con centros de investigación forense en Barranquilla, Medellín, Bucaramanga, Bogotá, Cundinamarca, Pereira y Cali.

Figura 19. Oxygen Forensic Suite



Fuente: Qpdownload.

El software se encuentra en la url. https://www.oxygen-forensic.com/es/

Partiendo del análisis con el uso de las herramientas necesarias requeridas y habiendo extraído datos de diferentes fuentes se clasifica con una calificación de relevancia para un análisis más profundo, donde se debe validar la vinculación de las siguientes etapas.

- ✓ Análisis de la información prioritaria.
- ✓ Generación de listado de archivos comprometidos con el caso
- ✓ Obtención de la línea de tiempo de la evidencia.

El profesional debe gestionar un informe conciso no muy técnico y entendible para personas del común el cual se recomienda que deba contener la relación de hallazgos encontrados, donde el informe o reporte contenga.

- ✓ Resultados de análisis
- ✓ El por qué se utilizó algunas herramientas para la recolección y análisis de la información.
- ✓ Sustentación de la falencia encontrada, el proceso de ataque o infección, como optimizar y mitigar las vulnerabilidades.
- ✓ Determinar si el alcance dado es suficiente para la conclusión definitiva o si debe realizarse otro análisis más avanzado,
- ✓ Recomendaciones de mejora y proceso de control para la mitigación de vulnerabilidades.

Por lo tanto, como resultado del trabajo elaborado y gracias a la documentación que se consultó para la realización del mismo, se obtuvo los siguientes resultados:

Se consiguió tener una visión amplia sobre la seguridad informática comprendiendo los conceptos y bases fundamentales para garantizar la disponibilidad, confiabilidad e integridad de la información ya que esta representa el activo más importante hoy en día en las organizaciones.

Por medio de la anterior recopilación bibliográfica se hizo un análisis sobre los principales aspectos de la informática forense, se identificaron las fases y procesos que se deben llevar a cabo para el tratamiento de evidencias digitales y de esta manera conocer las mejores prácticas para el proceso de cadena de custodia de evidencias digitales.

Se evidencia que en Colombia, la normatividad vigente, más específicamente la ley 1273 de 2009 es una de las mejor estructuradas, donde se tipifican los diferentes delitos informáticos estableciendo las penas correspondientes; por otro lado en Colombia se combaten los delitos informáticos gracias a la existencia de esta ley, sin embargo se debe mejorar en cuanto a la capacitación del personal y entidades involucradas en las investigaciones de delitos informáticos.

La cadena de custodia en investigación de delitos informáticos es uno de los procesos más completos y por ende de mayor importancia a la hora del tratamiento de evidencias digitales, debido a que de la correcta manipulación de las evidencias, depende que estas conserven su valor probatorio dentro de los diferentes procesos judiciales.

Se hace necesario contar con personal capacitado constantemente, se debe conocer la metodología para la cadena de custodia, de igual forma se debe contar con las herramientas necesarias y que estas estén a la vanguardia en cuanto a innovación y desarrollo tecnológico; también se debe contar con equipos e instalaciones adecuadas con el fin de aplicar las mejores prácticas para el tratamiento de evidencias digitales y cadena de custodia.

El impacto del trabajo e investigación desarrollada se espera que sea un aporte importante en la medida en que llegue al personal involucrado en el proceso de cadena de custodia en la investigación de delitos informáticos en Colombia y que sea tenido en cuenta como recomendación para llevar a cabo este proceso.

7. DIVULGACIÓN Y RECOMENDACIONES

7.1 DIVULGACIÓN

Para la divulgación del presente trabajo se pretende hacer uso de los canales de comunicación directos que existen hoy en día como lo son las redes sociales y el correo electrónico, entre otros. Haciendo uso de las redes sociales como Facebook, Instagram, Twitter y otros como YouTube y plataformas académicas en donde se pretende dar a conocer el desarrollo del mismo, ya que son medios masivos y de fácil acceso para la comunicación.

En el Anexo A que corresponde al formato RAE se hace un resumen sobre el presente trabajo.

7.2 RECOMENDACIONES

Se debe profundizar mucho más en los temas tratados, de igual forma se recomienda que las personas y entidades involucradas en el proceso de cadena de custodia en la investigación de delitos informáticos en Colombia tomen las sugerencias dadas en el presente documento con el fin de contribuir a mejorar los procesos relacionados.

También se recomienda que los funcionarios de la fiscalía como los jueces que estén ligados a este tipo de procesos, sean capacitados en como la informática forense y la cadena de custodia permite plasmar o mostrar como sucedió un hecho intangible en un delito tecnológico, lo cual permitirá a la toma de decisiones y el entendimiento más claro y preciso a la hora de escuchar la explicación de perito en el tribunal “dictamen pericial”

Las diferentes personas involucradas en el proceso de cadena de custodia y tratamiento de evidencia digital deben contar con las herramientas tecnológicas tanto de software como de hardware, estas deben estar actualizadas y siempre estar a la vanguardia de los adelantos tecnológicos.

Se debe tener conocimiento sobre la normatividad vigente de delitos informáticos, así como las leyes que regulan la evidencia digital en investigación de delitos informáticos; también es importante estar actualizado en lo referente a la evolución de los ataques informáticos ya que cada vez estos se hacen de manera más sofisticada.

Es importante recopilar la infografía adecuada que permita adquirir los conocimientos necesarios sobre la metodología para el tratamiento de videncia digital en la cadena de custodia y de esta manera asegurar la correcta aplicación de dichos procesos.

9. CONCLUSIONES

La tecnología como herramienta fundamental para el crecimiento y desarrollo personal, social, económico y académico de las personas dentro de una sociedad de consumo, nos ha llevado a ser dependientes en gran escala de los equipos electrónicos ya sean celulares, tablets, computadores, sistemas de cámaras de video vigilancia, software a la medida, equipos de automatización y control de acceso, redes LAN, WAN y MAN como medio masivo de interacción de información más las redes sociales, han logrado que todo este sistema nos facilite las cosas y lograr mantener un control sobre lo que hacemos, pensamos y realizamos ya sea en el ámbito personal o laboral, pero también se volvió en uno de los medios más atacados de forma inapropiada con intereses oscuros por personas que reciben el nombre de ciberdelincuentes los cuales en los últimos años han incrementado sus ataques y también las personas que no tiene un alto grado de conocimiento de las tecnologías se han comprometido con algún acto inapropiado y vandálico por medio de alguna herramienta tecnológica. Por tal efecto Colombia mediante el Ministerio de Telecomunicaciones adopto una ley llamada "de la protección de la información y de los datos" Ley 1273 de 2009.

De este modo surge el peritaje digital los cuales son investigadores o ingenieros que se capacitan en buscar evidencias digitales para ayudar a resolver casos judiciales, pero para que dichas pruebas sean validadas deben cumplir con unos procesos y procedimientos que garantice la veracidad de la evidencia y es ahí donde la cadena de custodia es de vital importancia ya que este proceso garantiza su validez ante un juez o tribunal.

Es en este proceso donde la investigación nos indica que la implementación y forma de realizar el levantamiento del material probatorio tecnológico no es optimo ya que cuanta con falencias en sus procesos, por no contar con manuales,

dotaciones y personal certificado y en constante actualización para no contaminar las evidencias a la hora de su recolección, embalaje, rotulado y análisis.

Habiendo realizado el reconocimiento del proceso de cadena de custodia y su aplicación en la investigación de delitos informáticos en Colombia se logro identificar las falencias y sus factores más relevantes que inciden en el proceso de cadena de custodia de evidencias digitales, las cuales son:

Falta de capacitación o conocimiento de las metodologías. Dado que son muchas las formas y procedimientos para realizar procesos de custodia se debe contar con personal debidamente capacitado y que estén en constante retroalimentación ya que las tecnologías están en continuo desarrollo y esto permite el nacimiento de nuevas herramientas y formas de hackear o vulnerar la seguridad de la información.

Uso de herramientas inadecuadas, se debe contar con tecnología de punta, la cual permite al perito y/o investigador forense realizar validación y rastreo a los procesos que hayan dado lugar a una posible vulnerabilidad en la información de un usuario, equipo o entidad.

El manejo inadecuado, que en ocasiones por un mal procedimiento no cumple el marco normativo que dicta la ley, permite que este sea calificado por la contra parte como una prueba contaminada y que pierda su valides.

Como parte del reconocimiento del proceso de cadena de custodia y tratamiento de evidencias digitales que se llevó a cabo durante el desarrollo del presente trabajo, se pudo verificar las diferentes fases que lo componen, así como la importancia de seguir de manera estructurada y bien definida cada uno de los pasos que aseguran las mejores prácticas para este proceso

Una vez identificadas las falencias y posibles mejoras para el proceso de cadena de custodia de evidencias digitales, se puede contribuir para que el personal de las diferentes instituciones involucradas en este proceso, evalúen la manera en que lo vienen ejecutando y validen si cuentan con las herramientas tecnológicas necesarias para asegurar la validez de la evidencia digital como material probatorio en investigaciones de delitos informáticos.

En las mejoras a tener en cuenta se propone mantener en constante actualización al personal de investigación y vincular activamente a los jueces y miembros de las salas penales con el fin de ampliar sus conocimientos y entendimiento en el ámbito de las tecnologías y de cómo estas también son piezas claves en proceso delictivos y como esas herramientas pueden manifestar mediante procesos especiales con software expertos un aporte vital para resolver un caso.

BIBLIOGRAFÍA

ARELLANO, Luis Enrique y CASTAÑEDA, Carlos Mario. La cadena de custodia informático-forense. Revista ACTIVA, Núm 3, enero-junio 2012, pp. 67-81. [en línea]. <http://ojs.tdea.edu.co/index.php/cuadernoactiva/article/download/45/42> [citado en Septiembre de 2016]

CAMELO, Leonardo. Seguridad informática en Colombia [en línea]. <http://seguridadinformacioncolombia.blogspot.com.co/2010/02/seguridad-de-la-informacion-y-seguridad.html> [citado en febrero de 2016].

CORTES DE LA ROSA, José Bernardo. Manejo de Evidencia Digital en Dispositivos de Almacenamiento Pendrive USB Aplicando la Norma Iso/Iec 27037:2012. Monografía. [en línea]. < http://repository.unad.edu.co/handle/10596/2660> [Ingeniero de Sistemas]. Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas e Ingenierías

GARCÍA, José Aurelio. La cadena de custodia aplicada a la informática [en línea]. <http://www.informaticoforense.eu/la-cadena-de-custodia-aplicada-a-la-informatica-i> [citado en febrero de 2016]

GAVIRIA, Pablo Andrés. Propuesta de un modelo de procedimiento para el tratamiento de la evidencia digital, acorde a la normatividad colombiana sobre delitos informáticos. Monografía. [en línea]. < http://repository.unad.edu.co/handle/10596/4008> [Ingeniero de Sistemas] Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas e Ingenierías [citado en Octubre de 2016]

EL TIEMPO. La Fiscalía de Ecuador entregó a expertos copia del disco duro del computador de 'Raúl Reyes'. En: El Tiempo [en línea]. (12 de agosto de 2010). Disponible en: <http://www.eltiempo.com/archivo/documento/CMS-7859929> [citado en noviembre de 2016]

MAGRANER GIMENO, Jordi. Pruebas y evidencias telemáticas. Trabajo de grado. Universidad Politécnica de Valencia. Valencia, 2015.

MANJARRÉS BOLAÑO, Iván y JIMÉNEZ TARRIBA, Farid. Caracterización de los delitos informáticos en Colombia. Pensamiento Americano, Vol. 8, Num. 9, 2012, p. 71-82.

MINTIC. Ley 1273 de 2009 [en línea]. < http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf> [citado en marzo de 2016]

PÉREZ GARCÍA, Camilo. ¿En Colombia se investigan delitos informáticos? [en línea]. <https://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html> [citado en Septiembre de 2016]

PEDREROS MARTÍNEZ, Wilson Leonardo y SUÁREZ URRUTIA, Jennifer Catherine. Herramientas aplicadas en el desarrollo del análisis forense informático en Colombia. Universidad Militar Nueva Granada. Bogotá, 2016.

PERONA, Enrique. Análisis forense. Cadena de custodia de la evidencia digital [en línea]. <https://www.securityartwork.es/2016/02/10/analisis-forense-cadena-de-custodia-de-la-evidencia-digital/> [citado en octubre de 2016].

RESOLUCIÓN 0-6394 DE 2004, Fiscalía General de la Nación [en línea]. [Citado en diciembre de 2014]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=15634

PIÑEROS, Gonzálo. Los detectives de la era digital [En línea]. <http://www.enter.co/archivo/los-detectives-de-la-era-digital/> [citado en noviembre de 2016]

UNIVERSIDAD NACIONAL A DISTANCIA. Fases de la informática forense [en línea]. <http://seguridadinformacioncolombia.blogspot.com.co/2010/02/seguridad-de-la-informacion-y-seguridad.html> [citado en abril de 2016]

ANEXOS

Anexo A. Resumen Analítico Especializado RAE

Título de Documento.	ESTUDIO DEL PROCESO DE CADENA DE CUSTODIA EN INVESTIGACIONES DE DELITOS INFORMATICOS EN COLOMBIA
Autor	RAMIREZ, Diego Armando CASTRO, Elmer Francisco
Palabras Claves	Seguridad informática, Informática forense, Delitos informáticos, Evidencia digital, Cadena de custodia.
Descripción El presente trabajo corresponde a una monografía por medio de la cual se busca beneficiar de algún modo a peritos e investigadores informáticos, así como también a los responsables del proceso de cadena de custodia ya que al identificar las falencias y posibles mejoras para este proceso, se tendrá un punto de referencia respecto a como se viene llevando a cabo dicho proceso con el fin de obtener mejores resultados y de manera más eficiente.	
Fuentes Bibliográficas	PERONA, Enrique. Análisis forense. Cadena de custodia de la evidencia digital [en línea]. <https://www.securityartwork.es/2016/02/10/analisis-forense-cadena-de-custodia-de-la-evidencia-digital/> [citado en octubre de 2016].

ARELLANO, Luis Enrique y CASTAÑEDA, Carlos Mario. La cadena de custodia informático-forense [en línea]. <http://ojs.tdea.edu.co/index.php/cuadernoactiva/article/download/45/42> [citado en Septiembre de 2016]

El Tiempo. La Fiscalía de Ecuador entregó a expertos copia del disco duro del computador de 'Raúl Reyes'. En: El Tiempo [en línea]. (12 de agosto de 2010). Disponible en: <http://www.eltiempo.com/archivo/documento/CMS-7859929> [citado en noviembre de 2016]

CORTES DE LA ROSA, José Bernardo. Manejo de Evidencia Digital en Dispositivos de Almacenamiento Pendrive USB Aplicando la Norma Iso/Iec 27037:2012. Monografía. [en línea]. < http://repository.unad.edu.co/handle/10596/2660> [Ingeniero de Sistemas]. Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas e Ingenierías

GARCÍA, José Aurelio. La cadena de custodia aplicada a la informática [en línea]. <http://www.informaticoforense.eu/la-cadena-de-custodia-aplicada-a-la-informatica-i> [citado en febrero de 2016]

MINTIC. Ley 1273 de 2009 [en línea]. < http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf> [citado en marzo de 2016]

GAVIRIA, Pablo Andrés. Propuesta de un modelo de procedimiento para el tratamiento de la evidencia digital, acorde a la normatividad colombiana sobre delitos informáticos. Monografía. [en línea]. < http://repository.unad.edu.co/handle/10596/4008> [Ingeniero de Sistemas] Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas e Ingenierías [citado en Octubre de 2016]

	PÉREZ GARCÍA, Camilo. ¿En Colombia se investigan delitos informáticos? [en línea]. <https://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html> [citado en Septiembre de 2016] RESOLUCIÓN 0-6394 DE 2004, Fiscalía General de la Nación [en línea]. [Citado en diciembre de 2014]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=15634 PIÑEROS, Gonzálo. Los detectives de la era digital [En línea]. <http://www.enter.co/archivo/los-detectives-de-la-era-digital/> [citado en noviembre de 2016] CAMELO, Leonardo. Seguridad informática en Colombia [en línea]. <http://seguridadinformacioncolombia.blogspot.com.co/2010/02/seguridad-de-la-informacion-y-seguridad.html> [citado en febrero de 2016]. UNIVERSIDAD NACIONAL A DISTANCIA. Fases de la informática forense [en línea]. <http://seguridadinformacioncolombia.blogspot.com.co/2010/02/seguridad-de-la-informacion-y-seguridad.html> [citado en abril de 2016]
Contenido: el trabajo desarrollado consiste en hacer inicialmente una recopilación de la información pertinente a los temas abordados como son la seguridad informática, la informática forense, los delitos informáticos y el tratamiento de evidencias digitales, haciendo énfasis en el proceso de cadena de custodia en la investigación de delitos informáticos en Colombia. Una vez se tiene la documentación, se hace el análisis correspondiente con el fin de identificar las posibles falencias de dicho proceso y de esta manera generar las posibles mejoras las cuales se plasman en un informe final.	

Descripción del problema: La cadena de custodia es un proceso o protocolo el cual debe seguirse para el tratamiento de una prueba por cierto tiempo que puede ser hasta que la prueba deje de ser válida o sea innecesaria. Según este proceso, se debe controlar la trazabilidad y la historia de la prueba, se debe conocer y referenciar quien, cuando, donde, ha tenido acceso a ella, entre otros ítems.

La creciente ola de delitos informáticos en el país, ha generado que las investigaciones y el proceso de cadena de custodia también aumenten, adoptando siempre las mejores prácticas respecto al manejo de las diferentes evidencias encontradas en equipos de cómputo, sistemas de información y demás elementos que se vean involucrados en los incidentes.

Teniendo en cuenta que la informática forense y el proceso de cadena de custodia aplicado a investigaciones de delitos informáticos en el país son relativamente nuevos, se pueden presentar diversos eventos que hagan que las evidencias digitales sean tratadas de manera incorrecta, ocasionando pérdidas de información, entre otras; lo anterior puede generar que los casos de investigación de delitos informáticos no lleguen a buen término para los directamente afectados.

Objetivo General. Identificar las falencias en el tratamiento de pruebas digitales que puedan ocasionar pérdidas, daños o destrucción de las mismas en procesos judiciales por medio del estudio del proceso de cadena de custodia en la investigación de delitos informáticos en Colombia

Objetivos Específicos.

- ✓ Realizar el reconocimiento del proceso de custodia y su aplicación en la investigación de delitos informáticos en Colombia.
- ✓ Identificar las posibles falencias existentes en el proceso de custodia y su aplicación en la investigación de delitos informáticos en nuestro país.
- ✓ Realizar un informe de identificación con las posibles mejoras sobre el proceso de custodia de pruebas digitales para evitar pérdidas, daños o destrucción de las mismas y su aplicación en la investigación de delitos informáticos en Colombia.

Resumen de lo desarrollado en el proyecto.

Metodología

El desarrollo de la monografía se lleva a cabo de manera exploratoria y descriptiva, debido a que la ley sobre delitos informáticos es relativamente nueva así como lo es la informática forense, se tienen como antecedentes algunos trabajos que se han relacionado anteriormente y los cuales de algún modo hacen referencia en parte al tema en el que se pretende enfocar este estudio. Dada la naturaleza de la investigación, se puede decir que también es de tipo bibliográfica ya que como se refiere más adelante, de acuerdo a la recolección, selección y clasificación de la información que se haga, así mismo se irá fortaleciendo y consolidando la base teórica de la investigación abordada.

Conclusiones

Los factores más relevantes encontrados que inciden en el proceso de cadena de custodia de evidencias digitales son:
Falta de capacitación o conocimiento de las metodologías.
Uso de herramientas inadecuadas, se debe contar con tecnología de punta.
Manejo inadecuado, que en ocasiones es por alguna de las causas anteriores.

Recomendaciones.

Se debe profundizar mucho más en los temas tratados, de igual forma se recomienda que las personas y entidades involucradas en el proceso de cadena de custodia en la investigación de delitos informáticos en Colombia tomen las sugerencias dadas en el presente documento con el fin de contribuir a mejorar los procesos relacionados.

También se recomienda que los funcionarios de la fiscalía como los jueces que estén ligados a este tipo de procesos, sean capacitados en como la informática forense y la cadena de custodia permite plasmar o mostrar como sucedió un hecho intangible en un delito tecnológico, lo cual permitirá a la toma de decisiones y el entendimiento más claro y preciso a la hora de escuchar la explicación de perito en el tribunal “dictamen pericial”