UNIVERSIDAD MAYOR DE SAN ANDRÉS
POSTGRADO EN INFORMÁTICA
MAESTRÍA EN SOFTWARE LIBRE Y ESTÁNDARES ABIERTOS

TESIS DE MAESTRÍA

MODELO PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS EN FASES CARENTES DE TÉCNICAS Y HERRAMIENTAS: CASO TRATAMIENTO DE LA EVIDENCIA DIGITAL EN EL ENTORNO DEL SOFTWARE LIBRE UTILIZANDO PROCESOS UNIFICADOS

POSTULANTE: ING. ERIKA MARILYN CRUZ VELA
TUTOR: M.B.A. JUAN CARLOS LEA PLAZA

LA PAZ – BOLIVIA

2016

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

LA CARRERA DE INFORMÁTICA DE LA FACULTAD DE CIENCIAS PURAS Y NATURALES PERTENECIENTE A LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la referencia correspondiente respetando normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

ÍNDICE

Dedicatoria

Siempre me he sentido maravillada por la hermosa familia que tengo, ellos se han preocupado de forma incondicional desde el primer momento en que llegué a este mundo, me han formado para para saber cómo luchar y salir victoriosa antes las diversas adversidades de la vida.

Cada momento que paso junto a ellos es inolvidable y sus enseñanzas no cesan, quiero agradecerles por todo. Las palabras no me alcanzarían para expresarles el orgullo que siento por tener una familia tan maravillosa.

Agradecimientos

Agradezco a Dios ser maravilloso que me dio fuerza y fe para creer lo que parecía imposible terminar. A mi familia por ayudarme incondicionalmente en todo momento, siendo fuente de apoyo constante e incondicional en toda mi vida y más aún en mis duros años de carrera profesional.

Resumen

En el presente acápite ofrecemos un resumen de la tesis de postgrado, el presente trabajo de investigación ofrece, desarrolla y propone un modelo del análisis y gestión de riesgos en fases carentes de técnicas y herramientas, caso análisis forense en sistemas GNU / Linux, el cual utiliza un proceso unificado en la recuperación de información digital, trabajo que enfrenta la problemática de cómo realizar un análisis forense en un dispositivo de almacenamiento, siguiendo un modelo que asuma las recomendaciones de instituciones internacionales, contextualizadas en nuestro país. El presente trabajo se estructura en los bloques: marco del problema, marco teórico, marco del prototipo, marco de resultados; se plantearán la propuesta del modelo de análisis y las conclusiones respectivas. En este trabajo de investigación se describe someramente los instrumentos empleados como son los de recolección de datos y el análisis de los datos recolectados.

La relevancia es una condición técnicamente jurídica, que habla sobre aquellos elementos que son pertinentes a la situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos. Todo aquello que no cumpla con este requisito será irrelevante y excluido del material probatorio recabado para efectos del caso bajo estudio.

La confiabilidad es otra característica fundamental, que busca validar la repetitividad y auditabilidad de un proceso aplicado para obtener una evidencia digital, esto es, que la evidencia que se extrae u obtiene es lo que deber ser y que, si un tercero sigue el mismo proceso, deberá obtener resultados similares verificables y comprobables.

Los analistas forenses saben que la evidencia digital es frágil y que su

incorrecta manipulación puede producir contaminación de la misma, alterando su contenido

Mediante lo investigado se pretende validar la información extraída de un dispositivo de almacenamiento, para que la misma sea utilizada como evidencia digital en un juicio, en donde se determine la culpabilidad o no del acusado.

Abstract

In this paragraph is a summary of the graduate thesis, this research provides, develops and proposes a model of analysis and risk management phases lacking tools and techniques, forensics case in GNU / Linux systems, which It uses a unified digital information recovery process, work facing the problem of how to perform a forensic analysis on a storage device, based on a model that assumes the recommendations of international institutions, contextualized in our country. This paper is divided into blocks: frame the problem, theoretical frame, the prototype, results framework; the proposed analytical model and the respective findings will be raised. In this research the instruments used such as data collection and analysis of data collected are briefly described.

Relevance is a technically legal status, which talks about those elements that are relevant to the situation in analysis or research, in order to prove or disprove a hypothesis that has been raised about the facts. Anything that does not meet this requirement will be irrelevant and excluded from the evidentiary material collected for the purposes of the present case.

Reliability is another key feature, which seeks to validate the repeatability and auditability of a process used to obtain digital evidence, that is, that the evidence obtained is extracted or what should be, and that if a third party follows the same process you must obtain similar verifiable and demonstrable results.

Forensic analysts know that digital evidence is fragile and that their improper handling can cause contamination of it, altering its content

Through the investigation it is to validate the information from a storage device, so that it is used as digital evidence in a trial, where the guilt of the accused is.

Marco introductorio

Capítulo I

Marco del problema

1.1 Estado del Arte

La infraestructura tecnológica disponible y el entorno de globalización han transformado el concepto tradicional de información. El volumen de datos que cruza hoy en día por cualquier organización ha crecido en forma exponencial. La información es la principal mercancía que se intercambia cotidianamente alrededor del mundo. Lo anterior, implica necesariamente la circulación de mayor volumen de información en los intercambios intra e inter institucionales.

En este contexto se hace necesario analizar no sólo el origen y el destino de la información sino también la vulnerabilidad de los operadores y los medios de transmisión utilizados, el valor estratégico y la legalidad de los mensajes, las características e intereses de los destinatarios, y la capacidad de la organización para controlar la información que fluye desde y hacia ella. Al ser la informática forense una disciplina que no tiene muchos años siendo practicada en nuestro medio, se cometen errores al momento de manejar la evidencia digital parte fundamental en investigaciones de éste tipo, lo cual resta credibilidad al ser tratada de manera inadecuada y por ende es vulnerable a ser inadmisible en un proceso penal.

El presente trabajo de investigación desarrolla y propone un modelo del análisis y gestión de riesgos en fases carentes de técnicas y herramientas, caso análisis forense en sistemas GNU / Linux, el cual utiliza un proceso unificado en la recuperación de información digital.

Se plantea esta investigación porque es necesario tener un modelo que permita de manera confiable analizar y gestionar los riesgos en un proceso unificado para permitir la recopilación confiable de la evidencia digital, para así mantener elementos probatorios en la autenticidad, confiabilidad, conformidad y suficiencia de la información recuperada, para que esta pueda ser utilizada en la legislación vigente en el Estado Plurinacional de Bolivia y la misma sea admisible en un proceso judicial.

Es difícil precisar el inicio de la "informática forense" o el comienzo del campo para el caso, pero la mayoría de los expertos coinciden en que la informática forense comenzó a desarrollarse hace más de 30 años, en los Estados Unidos, cuando la policía y los investigadores militares comenzaron a ver que los delincuentes obtenían ayudas técnicas en la comisión de sus delitos.

Por el 1970, los crímenes electrónicos iban en aumento, sobre todo en el sector financiero. La mayoría de los ordenadores de esta época fueron los mainframes, utilizado por personas capacitadas con conocimientos especializados que trabajaban en las finanzas, la ingeniería, y la academia [30]. A principios del 1990, las herramientas especializadas para la informática forense estaban disponibles.

La asociación internacional de especialistas de investigación de computación (IACIS[1]) introdujo la capacitación en software para las investigaciones forenses, y el IRS[2] creó programas de búsqueda de órdenes. Sin embargo, ningún software GUI[3] comercial para la informática forense estaba disponible hasta que se creo un software en Macintosh para recuperar archivos borrados y

1 IACIS: international association of computer investigative specialists
2 IRS: *Internal Revenue* Service, es el Servicio de Impuestos Internos (Idioma inglés: *Internal Revenue* Service (*IRS*)) es la agencia federal del Gobierno de los Estados Unidos.
3 GUI: La interfaz gráfica de usuario, conocida también como GUI es un programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en una interfaz gráfica de usuario

fragmentos de archivos borrados. Luego se desarrollo el EnCase, el cual se había convertido en una popular herramienta de análisis informático forense.

Dado que las empresas de software se vuelven más conocedores de la informática forense y entienden la investigación, que están publicando más herramientas forenses para seguir el ritmo de la tecnología.

A comienzo de los años 90, el FBI (Federal Bureau of Investigation) observó que las pruebas o evidencias digitales tenían el potencial de convertirse en un elemento de prueba tan poderoso para la lucha contra la delincuencia, como lo era el de la identificación por ADN. Para ello, mantuvo reuniones en su ámbito, y a finales de los años 90 se creó la IOCE (International Organization of Computer Evidence) con la intención de compartir información sobre las prácticas de informática forense en todo el mundo.

En marzo del año 1998, el G8 –a través del subgrupo de trabajo denominado The High Tech Crime, conocido como el Grupo de Lyón– encargó a la IOCE el desarrollo de una serie de principios aplicables a los procedimientos para actuaciones sobre pruebas digitales, así como la armonización de métodos y procedimientos entre las naciones que garantizasen la fiabilidad en el uso de las pruebas digitales recogidas por un estado para ser utilizadas en tribunales de justicia de otro estado.

La Scientific Working Group on Digital Evidence (SWGDE), principal portavoz de la IOCE en Estados Unidos, y la Association of Chief Police Officers (ACPO) del Reino Unido, propusieron una serie de puntos que luego englobaron los principios generales que se presentaron en el año 2000 al Grupo de Lyón [30].

A continuación se realizará una relación de los hechos cronológicos suscitados en el campo de la informática forense y la recolección de evidencia digital, los

RELACIÓN CRONOLÓGICA DE LOS HECHO EN LA INFORMÁTICA FORENSE Y LA EVIDENCIA DIGITAL

AÑO	APLICACION	CARACTERISTICA	COMENTARIO
1980	CART	En 1984, fue creado un programa del FBI. Conocido por un tiempo como el Programa de Medios Magnéticos, que ahora se conoce como CART (CART, del inglés computer analysis and response team), o análisis de informática y equipo de respuesta	El campo de la informática forense se inició en la década de 1980, poco después de que las computadoras personales se convirtieran en una opción viable para los consumidores.
1988	Se forma la IACIS (IACIS, del inglés international association of computer investigative specialists).	Una reunión celebrada en 1988 en Oregon condujo a la formación de la IACIS o Asociación Internacional de Especialistas de Investigación.	Se celebraron las primeras clases en el SCERS (SCERS, del inglés seized computer evidence recovery specialists), o especialistas en recuperación de la evidencia informática incautada.
1990	Se fundó New Technologies, Inc.,	Michael Anderson fue considerado "padre de la informática forense".	Michael Anderson, y era un agente especial de la División de Investigación Criminal del IRS. Anderson trabajó para el gobierno en esta capacidad hasta mediados de 1990, tras lo cual fundó New Technologies, Inc., un equipo que lleva la firma forense.
1993,2	Se estableció la IOCE	Primera conferencia sobre la recopilación de pruebas de los equipos	IOCE (IOCE, del inglés international organization on computer evidence), u organización internacional de evidencia informática fue establecida.
1997	La INTERPOL celebra simposio.	INTERPOL celebró un simposio sobre informática forense.	Se reconoció ampliamente que los funcionarios encargados de hacer cumplir la ley en todo el mundo tenían que ser bien versados en la forma de adquirir la evidencia de las computadoras, un hecho puesto de manifiesto en un comunicado del G8 en 1997.
1999	Se estudian 2000 casos. CART del FBI continuó creciendo.	El programa CART del FBI abordó 2000 casos individuales.	Se analizó 17 terabytes de datos.
2003	Se examinaron 782 terabytes de datos en sólo un año.	Con el advenimiento de los teléfonos inteligentes y PDA, las formas en que la informática forense puede operar se ha vuelto aún más importante a medida que los delincuentes tienen muchas opciones para romper la ley mediante el uso de dispositivos de computación.	Con los avances en la informática y la proliferación del acceso a Internet en todo el mundo, la informática forense comenzó a desempeñar un papel más importante para los agentes del orden
2009	Surgen los RCFL, del inglés Regional Computer Forensics Laboratories.	el FBI cuenta con 14 laboratorios forenses Regional de Informática en los Estados Unidos	5.404 agentes de la ley recibieron formación en la ciencia forense digital.
2010	La formación en informática forense del FBI a través del programa RCFL ha dado lugar a procesamientos significativos.	Se encontró culpable a un hombre de Kansas City, con ayuda de procesos basados en la informática forense.	Formación en informática forense implica algo más que los discos duros y el crimen digital. También incluye los teléfonos celulares, cámaras digitales, unidades flash, sistemas de posicionamiento global y los medios de comunicación.

Tabla 2: Relación cronológica de los hechos.[31]

datos que se mostrarán a continuación son complementarios a los antecedentes descritos en anteriores líneas.

En la actualidad de acuerdo con la ISO/IEC 27037:2012 la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital, bien ésta sea utilizada para que sea admisible en corte o no.

La relevancia es una condición técnicamente jurídica, que habla sobre aquellos elementos que son pertinentes a la situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos. Todo aquello que no cumpla con este requisito será irrelevante y excluido del material probatorio recabado para efectos del caso bajo estudio.

La confiabilidad es otra característica fundamental, que busca validar la repetibilidad y auditabilidad de un proceso aplicado para obtener una evidencia digital, esto es, que la evidencia que se extrae u obtiene es lo que deber ser y que, si un tercero sigue el mismo proceso, deberá obtener resultados similares verificables y comprobables.

Finalmente y no menos importante la suficiencia, la cual está relacionada con completitud de pruebas informáticas, es decir que, con las evidencias recolectadas y analizadas tenemos elementos suficientes para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada. Este elemento está sujeto a la experiencia y formalidad del perito informático en el desarrollo de sus procedimientos y priorización de esfuerzos.

Si bien puede haber otros elementos que ayuden en el gobierno de la evidencia digital, ISO[4] ha determinado que estos tres, establecen las condiciones necesarias y suficientes para que los expertos en informática forense recaben, aseguren y preserven elementos materiales probatorios sobre medios digitales,

4 ISO: International Organization for Standardization

los cuales podrán ser revisados y analizados por terceros interesados y sometidos a contradicción según ordenamiento jurídico donde se encuentren.

Quienes se dedican al análisis forense y la investigación digital conocen bien las mejores prácticas basadas en documentos publicados por el NIST[5], el departamento de Justicia de los Estados Unidos y el FBI[6] entre otros pero hasta el momento no existía una norma de alcance global como la ISO/IEC 27037 Guía para la Identificación, recolección, adquisición y preservación de evidencia digital, proveniente del tronco de normativa de Seguridad Informática ISO 27000.

Los analistas forenses saben que la evidencia digital es frágil y que su incorrecta manipulación puede producir contaminación de la misma, alterando su contenido. La norma establece los principios de relevancia, confiabilidad y suficiencia así como también las siguientes etapas para el manejo de la evidencia digital: Identificación, Recolección, Adquisición y Preservación. Señala que DEFR[7] y DES[8] deberán documentar todas sus acciones, las que se regirán por los siguientes principios: Minimizar el manejo de la evidencia digital, Documentar cualquier acción que implique un cambio irreversible, Adherirse a las regulaciones y leyes locales, No extralimitarse en sus funciones [32]

La norma reconoce que en ocasiones se trabaja directamente con la evidencia original pudiéndose efectuar tareas que impliquen cambios irreversibles, pero a la vez establece con claridad que el analista forense debe supeditarse a las regulaciones vigentes en su territorio y al mandato de autoridad judicial.

Siguiendo los lineamientos de la serie de normas ISO 27000, el documentar las

5 NIST: National Institute of Standars and Technology
6 FBI: Federal Bureau of Investigation
7 DEFR:*Digital Evidence First Responder.* Perito que concurre a la escena del hecho.
8 DES:Digital Evidence Specialist. Es quien efectúa el análisis forense y produce el dictamen pericial.

acciones, decisiones y omisiones es fundamental, en especial cuando el incidente informático incluye evidencia digital que podría introducirse en ámbito judicial.

Por otra parte actualmente se han tenido nuevos estudios sobre el como tratar con la evidencia digital, una de las entidades reguladoras es la NIST, quien tiene la siguiente definición de evidencia digital:

Evidencia digital incluye información en las computadoras, archivos de audio, grabaciones de video, e imágenes digitales. Esta evidencia es esencial para los delitos informáticos y de Internet, sino que también es valiosa para el reconocimiento facial, fotos de la escena del crimen, y las cintas de vigilancia [33].

La NIST desarrollo diferentes proyectos, entre los cuales se encuentran:

Computer Forensic Reference Data Sets, Computer Forensics Tool Testing, National Software Reference Library, Real-Time Forensics Imaging for Analog and Digital Video Tapes.

La NIST desarrollo una adecuada documentación en la recolección de evidenicia digital, entre las recomendaciones que propone la NIST, analizamos las que se encuntran detalladas en el documento Investigative Uses of Technology: Devices, Tools, and Techniques, este documento esta destinado a establecer un procedimiento en la recolección de evidencia digital, ésta guía está destinada a los agentes de policía y otros miembros de la ley, comunidad de las fuerzas que son responsables para el examen de la evidencia digital. Esta guía esta basada en situaciones habituales desarrolladas en el examen de la evidencia digital. No es un mandato para la aplicación de la ley, se trata de una guía para desarrollar sus propias políticas y procedimientos.

La tecnología avanza a un ritmo tan rápido que las sugerencias de esta guía es la de examinar el contexto de la tecnología y las prácticas actuales. Cada caso es único y cuando se trata de la evidencia digital, el forense en general debe aplicar el siguiente procedimiento:

- Las medidas adoptadas para asegurar y reunir pruebas digitales no deben afectar a la integridad de esa evidencia.

- Las personas que realicen el examen de la evidencia digital deben ser capacitados para este propósito.

- Actividad relacionada con la incautación, el examen, el almacenamiento o la transferencia de la evidencia digital debe ser documentado, en conserva, y debe poder consultarse.

A través de todo esto, el examinador debe ser consciente de la necesidad de llevar a cabo una precisa y el examen imparcial de la evidencia digital [33].

En cuanto a los procesos unificados, estos quedan inmersos en la recolección de la evidencia digital, al construir un proceso unificado se debe construir un proceso unificado que sirva de base en la tarea de recuperación de la información digital en equipos de computación.

Ante la diversidad de soluciones existentes, surge la necesidad de un proceso formal unificado que valide la labor del profesional informático forense, que contemple la multiplicidad de dificultades y que permita tener una guía orientadora y rectora frente a cada problemática.

Existen procesos propuestos que constan de fases, etapas, tareas, técnicas y

herramientas disponibles recomendadas; existen entidades reguladoras que proponen guías de procedimiento para construir un buen proceso unificado, estas son:

- ACPO (Association of Chief Police Officers) – England, Wales and North Ireland. Good Practice Guide for Computer- Based Electronic Evidence. Oficial release version.

- NIJ (National Institute of Justice) Report – United States of America.

- Department of Justice. Forensic Examination of Digital Evidence: A guide for Law Enforcement.

- Law Enforcement Investigations - Active Army, Army National Guard, and US Army Reserve. FM 3-19.13. Chapter 11: Computer Crimes.

- Metodologías, Estrategias y Herramientas de la Informática Forense aplicables para la dirección nacional de comunicación y criminalística de la policía Nacional de Ecuador.

- RFC 3227: Guía Para Recolectar y Archivar Evidencia" (Guidelines for Evidence Collection and Archiving) , escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group.

- Guía de la IOCE (International Organization on Computer Evidence) "Guía para las mejores practicas en el examen forense de tecnología digital" (Guidelines for the best practices in the forensic examination of digital technology).

- Guía de Mejores prácticas de la ISFS (Sociedad de Seguridad Informatica y

Forense) Hong Kong.

- Guía Para El Manejo De Evidencia En IT - Estándares de Australia. APEC Telecommunications and Information Working Group [34].

La recuperación de la información en el ámbito de la informática forense puede ser considerada hoy en día un proceso crítico. Una de las mayores problemáticas es la falta de un proceso unificado que guíe a los expertos forenses en esta tarea tan compleja. Se presenta en éste trabajo los avances obtenidos hasta el momento en el proyecto de investigación denominado PURI "Proceso Unificado de Recuperación de la Información" cuyo objetivo es formalizar un proceso marco que abarque las fases, tareas, herramientas y actividades aplicables a diversos entornos y dispositivos [35].

A continuación se presenta el Proceso Unificado de Recuperación de la Información, en este proceso se plantea la fase de adquisición, fase de preparación, fase de análisis.

A partir de esta validación se detectaron áreas carentes, tanto de técnicas como de herramientas que apliquen técnicas que han sido propuestas por algunos autores.

Como ya se ha mencionado, las ciencias forenses deben cumplir con tres principios básicos: evitar la contaminación, actuar metódicamente y controlar la cadena de evidencia.

El modelo que se planteará en el presente trabajo de investigación deberá gestionar los riesgos en el tratamiento de la evidencia digital, riesgo que aparece en cada una de las fases de un proceso unificado.

1.2 Planteamiento del problema

El presente trabajo de investigación enfoca la problemática que existe en la informática forense durante el proceso de la obtención de evidencias. En principio se plantea un contexto forense en el que se ejecutará el modelo propuesto en el documento de investigación.

Muchos investigadores han planteado procesos formales que permitan guiar y validar la actividad del informático forense en la obtención de evidencias digitales, gran parte de estos procesos tienen como base un proceso unificado de la recuperación de la información; pero en la mayoría de los casos no se toman los riesgos que se tienen al momento de utilizar un proceso formal que tenga un proceso unificado no estandarizado.

El caso de aplicación enfocará el análisis forense de un sistema GNU / Linux, en donde se planteará un modelo que determine los aspectos carentes en un proceso unificado de recuperación de información digital, esto con el propósito de gestionar el riesgo asociado en la recolección de evidencias digitales. Se plantea el presente trabajo de investigación porque en un proceso unificado de recuperación de información digital se presenta el caso de tener dificultades en la diversidad de tecnologías y herramientas en la recolección de la evidencia digital y es en este punto que el riesgo de vulnerar la integridad de la información es mayor.

Por lo tanto debemos plantear un modelo que nos ayude a gestionar el riesgo en la recolección de evidencias en un sistema en primera instancia GNU / Linux. Pero a medida que se avance en la investigación se observará que a diversidad de tecnologías, métodos de ocultamiento de información, tiempos ajustados, falta de guías de operación, legislación vigente, intereses de

fabricantes, entre otras, dificulta y obstruye de gran medida la gestión de riesgos en la recolección de evidencia digital.

¿Cuáles son los riesgos en el tratamiento de evidencia digital en el entorno del software libre?

1.3 Formulación del problema

¿Cuáles son los riesgos en el tratamiento de evidencia digital cuando se utilizan procesos unificados de recuperación de información digital en software libre?

1.4 Planteamiento de objetivo

Proponer un modelo para el análisis y la gestión de riesgos en el proceso de recolección de evidencia digital en el entorno del software libre, de modo que exista una metodología en la recuperación de información digital.

1.4.1 Objetivo general

Considerando las recomendaciones de NIST (National Institute of Standars and Technology) y los trabajos realizados en el área de la informática forense, proponer un modelo para realizar el análisis en el proceso de recolección de la evidencia digital en software libre, de modo exista la gestión de riesgos en la recuperación de la información digital y de esta forma se puedan establecer informes claros en contra de acciones antijurídicas.

1.4.2 Objetivos específicos

- Proponer un caso de estudio en el análisis forense de un sistema GNU / Linux en donde se lleve a cabo el proceso unificado de recolección de información digital para el análisis y la gestión de riesgos en el tratamiento de la evidencia digital.

- Analizar las recomendaciones de la NIST en el caso de incidentes en la recuperación de información digital para el tratamiento de la evidencia digital en el entorno del software libre.

- Estudiar metodologías en la gestión de riesgos en la seguridad de la información para el análisis de riesgos en el tratamiento de la evidencia digital en el entorno del software libre.

- Estudiar paso a paso el análisis y la gestión de los riesgos del modelo propuesto, en el tratamiento de evidencia digital en el entorno del software libre.

1.5 Planteamiento de Hipótesis

En una investigación exploratoria no se establece una hipótesis, lo que se puede elaborar es una conjetura inicial; esta conjetura esta relacionada con el análisis y la gestión de riesgos en el tratamiento de la evidencia digital debe tratarse con un modelo razonable para que no fracture los procesos unificados en la recuperación de información digital, de modo que la evidencia digital es válida si se cumple con un modelo que cumpla con condiciones determinadas por recomendaciones internacionales; cumpliendo con este modelo la evidencia digital es considerada como un medio probatorio en un juicio.

1.6 Diseño Metodológico

El diseño de la investigación será de carácter transeccional descriptivo, preexperimental, con un enfoque cuantitativo.

1.6.1 Tipo de investigación

Cuando no existen investigaciones previas sobre el objeto de estudio o cuando nuestro conocimiento del tema es tan vago e impreciso que nos impide sacar las más provisorias conclusiones sobre qué aspectos son relevantes y cuáles no, se requiere en primer término explorar e indagar, para lo que se utiliza la investigación exploratoria.

Se desarrollará una investigación explorativa, porque la investigación exploratoria se utiliza cuando los problemas se encuentran en una etapa preliminar.

La investigación exploratoria se utiliza cuando el tema o asunto es nuevo y cuando los datos son difíciles de recopilar.

La investigación exploratoria terminará cuando, a partir de los datos recolectados, haya sido posible crear un marco teórico y epistemológico lo suficientemente fuerte como para determinar qué factores son relevantes al problema presentado en la presente investigación.

El estudio exploratorio se centra en descubrir.

1.6.2 Método de investigación

El método de investigación utilizado será el cuantitativo.

1.6.3 Fases metodológicas

1) Fase conceptual.

- Formulación y delimitación del problema.
- Revisión de la literatura.
- Construcción del marco teórico.
- Formulación de hipótesis.

2) Fase de planeación y diseño.

- Selección de un diseño de investigación.
- Identificación de la población que se va a estudiar.
- Selección de métodos e instrumentos.
- Diseño del plan de muestreo.
- Término y revisión del plan de investigación.
- Realización del estudio piloto y las revisiones.

3) Fase empírica.

- Recolección de datos.
- Preparación de los datos para análisis.

4) Fase analítica.

- Análisis de datos.
- Interpretación de resultados.

5) Fase de difusión.
- Comunicación de las observaciones.
- Aplicación de las observaciones [36].

1.6.4 Técnicas de investigación

Para explorar un tema relativamente desconocido se dispone de un amplio espectro de medios y técnicas para recolectar datos, por lo tanto las técnicas de investigación utilizadas en el presente trabajo de investigación serán: la revisión bibliográfica especializada, entrevistas y seguimiento de casos.

1.6.5 Universo o población de referencia

Se tomará una población de aproximadamente cien casos, por el teorema de límite central, el que se señala que una población de más de cien casos, será una población con una distribución normal en sus características, sin embargo la normalidad no debe asociarse con probabilidad. Esta población estará relacionada con la utilización del sistema operativo Linux.

1.6.6 Muestra o población de estudio

Se utilizará una muestra basada en sujetos voluntarios y expertos, quienes trabajan en diseños experimentales y en situaciones de laboratorio, relacionados con el sistema operativo Linux.

1.7 Delimitación

1.7.1 Delimitación geográfica

El trabajo de investigación se delimitará geográficamente en el Estado Plurinacional de Bolivia.

1.7.2 Delimitación temporal

El presente trabajo de investigación tendrá una delimitación temporal que comprenderá las gestiones: 2013, 2014.

Marco teórico

Capítulo II

Referencia Teórica

Caso de estudio: análisis forense de un sistema GNU /LINUX, aplicación de un proceso unificado para el tratamiento de la evidencia digital

La tecnología, en caso de análisis forense en sistemas informáticos, son aplicaciones que hacen un papel importante en reunir la información y pruebas necesarias. La ciencia forense es metódica y se basa en acciones premeditadas para reunir pruebas y analizarlas. La escena del crimen es el ordenador y la red a la cual éste está conectado.

En el presente documento se da una vista sobre el trabajo del análisis forense en el entorno GNU/LINUX, se presentan procedimientos pre-establecidos de tratamiento de información y un caso práctico, en el presente capítulo se mencionará cuales son las órdenes utilizadas en el entorno GNU/LINUX, órdenes utilizadas en un laboratorio forense, ordenes utilizadas para el análisis en un principio de la configuración del hardware de un dispositivo de almacenamiento de datos y terminar con el análisis interno de dicho dispositivo.

Se analizará un dispositivo de almacenamiento de estado sólido, para luego analizar un disco duro.

La problemática se da cuando se trata de preservar la escena en donde se desarrollo el supuesto delito, se dice supuesto porque hasta que no se

compruebe el mismo se mantiene el principio de inocencia; se dice que para mantener la escena del crimen intacta se la debe congelar, para que en un paso posterior utilizando herramientas apropiadas ya sea en hardware o en software se pueda extraer la información de forma que conserve el principio de integridad. En el presente trabajo se enfocará esta problemática desde el punto de vista de la utilización de herramientas en GNU/Linux, es decir desde el punto de vista del software.

Teniendo en cuenta que cada día los intrusos utilizan técnicas avanzadas de protección de sus herramientas, se cubrirá el tema de ocultación de información, a través de cifrado y ofuscación con Burneye y/o otras utilidades.

La tarea del análisis forense informático debe ser llevada acabo con máxima cautela, asegurándose que la información analizada se conserve intacta, en la mayor medida posible, la información contenida en el dispositivo de almacenamiento, tal es el caso de in dispositivo de almacenamiento sólido, en el que se encuentra un sistema comprometido, debe ser tratado con mucha cautela, de tal forma de no contaminar la escena del crimen, de forma similar que los investigadores policiales intentan mantener la escena del crimen intacta, hasta que se recogen todas las pruebas posibles.

El trabajo de un investigador forense es el equivalente al de un investigador policial, por lo tanto es necesario ofrecer un punto de partida fundamental para los investigadores policiales y los analistas forenses informáticos, pistas sólidas, que serán utilizadas como pruebas, evidencias, para su uso posterior.

Por lo tanto el objetivo de un análisis forense informático es realizar un proceso de búsqueda detallada para reconstruir a través de todos los medios el log de acontecimientos que tuvieron lugar desde el momento cuando el sistema estuvo en su estado integro hasta el momento de detección de un acceso no

autorizado.

Cada uno de los casos e incidentes es único, por lo tanto, el investigador forense externo es diferente en cada caso, ellos contribuyen según se de el contexto en cada uno de los casos, en nuestro país ellos trabajan con la policía nacional, pero se debe recalcar que nuestro país no tiene un departamento especializado en este tipo de incidentes.

Observado el caso de estudio a analizar, se debe contar con procedimiento apropiado para la confiscación del dispositivo de estado sólido y la preservación física del dispositivo, incluso muchos expertos de acuerdo a la experiencia que tienen mencionan que se debe apagar el dispositivo en donde este funcionando el dispositivo de almacenamiento. Tomando en cuenta todas estas sugerencias procederemos al análisis más crítico del caso, este se centra en la extracción lógica de los datos albergados en el dispositivo de almacenamiento.

En primera instancia se debe realizar una copia exacta de los datos del dispositivos de almacenamiento, este es un paso crucial; la clonación del dispositivo debe realizarse utilizando herramientas confiables, en el caso de la presente investigación se utilizarán herramientas lógicas pertenecientes al entorno GNU/LINUX.

Una vez que se tienen los datos clonados, pasaremos a analizar el objeto clonado, para ello será necesario previamente realizar una recolección de información del sistema informático: analizar ficheros log, estudiar el sistema de ficheros (FS) del equipo comprometido y reconstruir la secuencia de eventos para tener una imagen clara y global del incidente.

2.1 Equipo necesario

Existen distribuciones de Linux que incorporan directamente utilidades forenses en su instalación, pero se puede optar por utilizar una distro que no las incorpore ya que la instalación de estas herramientas por defecto a veces causa problemas. Mientras que si se utiliza cualquier distro como RedHat, Debian el analista puede configurar el software según sus preferencias.

En el presente caso de estudio se utilizará una distro, en la que se utilizarán órdenes que permitan el análisis de un dispositivo de almacenamiento, para ello necesitaremos:

- Un equipo con una placa compatible i386 con 2 tarjetas controladoras IDE.

- Tarjeta de interfaz SCSI (e.g., Adaptec 1542).

- Si el sistema está conectado a una red, deberá ser perfectamente parcheado y no tener ningún servicio de red funcionando salvo SSH (para acceso remoto y transferencia de ficheros). RedHat Linux 7.3 con Bastille Linux 2.0 BETA es muy buena opción (Combinación utilizada en el lab de Activa Link).

- Dispositivos de cinta DDS-3 ó DDS-4 4mm (se necesita bastante capacidad para almacenar información de las particiones grandes.).

- Por lo menos 2 discos duros > 8Gb. sobre el controlador IDE principal (para almacenar el sistema operativo y herramientas, más espacio para poder copiar las particiones salvadas desde la cinta, y espacio adicional para recuperar la información borrada desde discos duros).

- Un segundo controlador IDE sin utilizar. Eso significa que no deberá mezclarse

con modificación de configuraciones de hardware de los discos. Simplemente se los debe conectar y aparecerán como /dev/hdc (master) ó /dev/hdd (slave).

2.2 Hardware y software mínimo

Un equipo móvil de análisis, funcionando bajo GNU/Linux será suficiente para analizar sistemas de ficheros diferentes pero soportados como por ejemplo Sun UFS. Se podrá simplemente montar el sistema de fichero emitiendo el comando mount con la opción particular (ver página man del mount).

El equipo Móvil es un buen método de llevar el laboratorio hasta el sistema accidentado, este equipo debe contar con una tarjeta eth 10/100, disco duro de más de 18-20 Gb o espacio suficiente espacio, que permitirá almacenar toda la información de imágenes del sistema de ficheros (estas imágenes deberían luego almacenarse en cintas) para ser analizadas, visualizar los resultados, craquear las contraseñas scrypt() del intruso que puede posiblemente encontrar, y una mochila.

2.3 Congelación de la escena del crimen

Para prevenir esas modificaciones del sistema de ficheros es mejor sacar el cable de electricidad del enchufe. Hay que estar informados que puede ser que alguna información en la memoria o información del cache no guardada en el disco puede ser eliminada como estado de red, procesos ejecutándose en la memoria, accesos a memoria kernel, contenido de registros swap, etc.

Para ello antes de sacar el cable del enchufe puede hacer lo siguiente; ejecutar varios comandos antes de apagar el sistema. Si el administrador no está seguro

de lo que está haciendo, se debe simplemente desenchufar el sistema y ponerse en contacto con un investigador forense especializado, ya que las pruebas pueden ser dañadas con mucha facilidad.

Normalmente los sistemas Unix se cierran con el comando shutdown. Eso se hace para asegurarse que todos los servicios han finalizado de forma limpia, todos los ficheros cache y buffers de sistemas están flusheados y los usuarios están notificados. Este procedimiento es perfecto para sistemas intactos, pero en un sistema afectado, esa acción, lo más seguro que borre alguna información de interés. Hubo casos cuando los intrusos programaban sistemas para eliminar algunos ficheros en la máquina cuando el interfaz de red se deshabilitase (es decir, cuando el cable de conexión haya sido desconectado) o cuando el procedimiento de un shutdown normal haya sido activado.

En caso de que el administrador esté seguro de si mismo puede utilizar algunas de las herramientas que vienen a continuación, siempre con cuidado:

- find - Identificar todos ficheros corrientes, directorios modificados desde la fecha de último acceso no autorizado, o que pertenecen al usuario desde cuya cuenta se sospecha que fue originado el ataque.

Importante: La utilidad "find" modifica el i-node "last accessed" con el timestamp actual, entonces no debe utilizar esta utilidad para barrer el sistema de ficheros, si todavía quiere saber cuales son los ficheros accedidos por el atacante si el sistema de ficheros está montado en modo lectura y escritura.

- ls - Obtener el listado largo (ls -lat) de ficheros en lugares sospechosos, los home directories, directorio /dev, directorio /root, etc.

- ps - Obtener el listado largo de todos los procesos incluidos aquellos sin ttys

(e.g., ps auxwww y ps elfwww -- añadir más flags w si el listado se acorta).

- lsof - Obtener un listado completo de descriptores de ficheros, que puede mostrar algunos backdoors, sniffers, eggdrop IRC bots, redireccionadores de puertos para VNC, etc.(Ojo con cwd, cual es el directorio local en el cual el programa ha sido ejecutado.)

- last, w, who - Obtener el listado de usuarios actuales en el sistema, logins anteriores, etc.

- ltrace, strace, truss (SunOS 5) - Ver últimos accesos a ficheros de configuración de "rootkit", ejemplo: Examinar el fichero /bin/ls trucado.

2.4 Recolección de la información

Se debe también considerar montar el disco como noexec y nodev para asegurarse que no pueda ser ejecutada ninguna aplicación desde el disco duro comprometido y que se ignoren los ficheros de dispositivos en el directorio /dev. Es muy aconsejable estudiar bien la página man de la utilidad mount.

Ejemplo:

mount -o ro,noexec,nodev /dev/hda1 /t

Se debe cuestionar permanentemente la información que la máquina está proporcionando. Sería aconsejable y mucho más fácil y seguro si simplemente el disco duro fuese extraído de la máquina afectada y fuese montado en modo sólo lectura en una estación de análisis similar a la máquina atacada.

Si no hay seguridad de que las utilidades comunes estén mostrando la verdadera situación, se debe utilizar aplicaciones alternativas. Los módulos de kernel cargables o librerías dinámicas, pueden estar alteradas para proporcionar información falsa. En estos casos se debe utilizar binarios compilados de forma estática desde un toolkit descargados de la web de incident-responce.org.

Un sistema informático no sólo puede ser instruido para auto-destruirse una vez se produzcan las condiciones de riesgo consideradas por el intruso, sino también realizar tareas programadas de eliminación de archivos, sustitución de archivos y ejecuciones de aplicaciones determinadas.

2.5 Almacenamiento de pruebas

Es necesario tomar notas de lo que se hace con el disco duro, y a que hora, almacenándolo en una ubicación segura como por ejemplo una caja fuerte.

Es recomendable que siempre que se trabaje con el medio original esté acompañado por un colega, para que conste a los efectos legales y su testimonio pueda ser confirmado por alguien con un nivel de conocimientos similar.

Una vez el disco ha sido sacado de la máquina, debe ser almacenado de forma segura para poder ser utilizado como prueba a posteriori en un juicio. Si no se almacena de forma correcta, no será la primera vez que la investigación no pueda seguir o las pruebas se declaren nulas por parte de un juez o jurado por contaminación o tratamiento indebido.

Creación de imágenes es un método de hacer copias exactas de particiones de

disco duro.

Por supuesto, estas utilidades tienen su sitio merecido, pero a lo que se refiere al análisis forense, lo más importante es conservación de información.
Las copias deben ser hechas bit-por-bit, es decir será necesario hacer imágenes del disco. La investigación debe ser llevada sobre una copia y nunca sobre el disco original. Se debe hacer tres copias del disco duro original. Sobre todas las copias y original se debe llevar acabo una verificación criptográfica - un checksum MD5.

Todas las acciones realizadas durante el análisis deben ser documentadas detenidamente. Es fácil hacerlo, si se utiliza el programa script, el cual toma nota de toda la entrada y salida del shell. Script marca la hora de inicio/fin del log de eventos, y usa el comando date varias veces durante la sesión para guardar los tiempos intermedios.

Utilidades como tar y cpio están bien si la portabilidad es lo más importante, y dump y restore están perfectas para recuperar ficheros individuales en casos de que la consistencia de información es lo más importante.

Las utilidades descritas anteriormente no le permiten conservar el espacio "slack" al final de los ficheros, ni permiten conservar que es lo que exactamente contenían los bloques de los ficheros eliminados.

Ya que los intrusos frecuentemente almacenan ficheros en el espacio "slack" de los archivos y borran de forma segura los archivos logs una vez que hayan penetrado en el sistema para ocultar sus huellas.

2.6 Preparación para el análisis

Fotografiar el equipo afectado antes de mover cualquier detalle del mismo. Esto es necesario para que esto se convierta en una prueba y que la misma pueda acabar en una sala de juicio. Documentar los detalles de todos los dispositivos es también importante; es por esta razón que se tomo una fotografía del dispositivo de almacenamiento de estado sólido y se tomo en cuenta las características del mismo, estas características son:

Figura 1. Unidad SSD MU-PS1T0BEU de 250GB

En el caso del un disco duro se debe tomar en cuenta el valor del ID del dispositivo, se debe tomar en cuenta las características propias del mismo, características técnicas.

Documentar el trabajo realizado es otro de los factores que debe tomarse en cuenta, desde la fecha inicial en donde se comenzó a ejecutar el trabajo. Es importante que todos los hechos pertinentes al caso durante la preparación, recuperación y análisis de las pruebas sobre un ataque, estén perfectamente documentados, en el presente caso de estudio se tomó datos técnicos del dispositivo a analizar y se tomaron datos desde el primer momento en que se

analizó el dispositivo.

Se deben realizar por lo menos tres imágenes del disco duro entero y trabajar con copias, y no con el original. Este procedimiento se aplico al disco SSD.
Se deben realizar por lo menos tres imágenes del disco duro entero y trabajar con copias, y no con el original. Este procedimiento se aplico al disco SSD.

Las particiones del disco duro deben ser identificadas con el programa fdisk. Nunca se debe utilizar fdisk en modo interactivo, ya que se arriesga que la tabla de particiones existente o las etiquetas se modifiquen (fdisk es un programa i386 GNU/Linux, modelado a partir de su equivalente de DOS).

Por ejemplo:
fdisk -l /dev/hdd

```
# fdisk -l /dev/hdd


Disk /dev/hdd: 255 heads, 63 sectors, 1575 cylinders
Units = cylinders of 16065 * 512 bytes


   Device Boot      Start         End      Blocks   Id  System
/dev/hdd1   *           1         869     6980211    b  Win95 FAT32
/dev/hdd2             870        1022     1228972+  83  Linux
/dev/hdd3            1023        1035      104422+  82  Linux swap
/dev/hdd4            1036        1575     4337550   83  Linux
```

Figura 2. Ejecución de la orden fdisk

Este listado nos da un panorama de la partición /dev/hdd2 era partición root, y /dev/hdd4. Posteriormente se recurre al fichero salvado /etc/fstab, o alternativamente montarla partición y se puede examinar su contenido.

Posteriormente se generan los checksums de integridad de particiones con MD5 del disco original y sus imágenes para verificar si coinciden.

La orden mt se utiliza para saltar, volver atrás en un fichero para luego verificar su checksum MD5. Hay que estar seguro que se utiliza dispositivo "non-rewind" ya que a la hora de saltar de una imagen de fichero a otra podríamos sobrescribir información sobre la cinta y perder información. También hay que asegurarse que no hacemos ningún error con parámetros if= y of= - opciones del comando dd ya que podrá destruir información sobre el disco con facilidad.

```
# md5sum /dev/hdd2
7b8af7b2224f0497da808414272e7af4  /dev/hdd2
```

```
# mt status
SCSI 2 tape drive:
File number=0, block number=0, partition=0.
Tape block size 512 bytes. Density code 0x13 (DDS (61000 bpi)).
Soft error count since last status=0
General status bits on (41010000):
 BOT ONLINE IM_REP_EN
```

```
# dd if=/dev/hdd2 of=/dev/nst0
2457944+0 records in
2457944+0 records out
```

```
# mt bsf 1


# dd if=/dev/st0 | md5sum
2457944+0 records in
2457944+0 records out
7b8af7b2224f0497da808414272e7af4  -


# mt status
SCSI 2 tape drive:
File number=1, block number=0, partition=0.
Tape block size 512 bytes. Density code 0x13 (DDS (61000 bpi)).
Soft error count since last status=0
General status bits on (81010000):
EOF ONLINE IM_REP_EN
```

Figura 3. Ejecución de la orden mt

Montamos el sistema de ficheros root, pero no lo modificamos de ninguna manera. Para hacerlo bien la montamos en modo de solo lectura con opción "-r" o "-o ro". Tenemos que tener en cuenta que la pertenencia de archivos se contará basándose en el fichero /etc/group del sistema de análisis y no del fichero group del sistema comprometido.

```
# mount -r /dev/hdd2 /mnt


# ls -lat /mnt
total 73
drwxr-x---  17 root     root         1024 May  1 09:01 root
drwxrwxrwt   6 root     root         1024 May  1 04:03 tmp
drwxr-xr-x   8 root     root        34816 Apr 30 04:02 dev
drwxr-xr-x  34 root     root         3072 Apr 29 14:17 etc
drwxr-xr-x   2 root     root         2048 Apr 26 16:52 bin
```

```
drwxr-xr-x   2 root     root         1024 Apr 26 11:12 boot
drwxr-xr-x   3 root     root         3072 Apr 21 04:01 sbin
drwxr-xr-x   4 root     root         3072 Apr 21 03:56 lib
drwxrwxr-x   2 root     root         1024 Mar  3 13:27 cdrom
drwxr-xr-x   2 root     root         1024 Oct  9  1999 home
drwxr-xr-x   2 root     root        12288 Oct  9  1999 lost+found
drwxr-xr-x   4 root     root         1024 Oct  9  1998 mnt
drwxr-xr-x   2 root     root         1024 Oct  9  1999 proc
drwxr-xr-x  20 root     root         1024 Aug  2  1998 usr
drwxr-xr-x  18 root     root         1024 Aug  2  1998 var
```

Figura 4. Ejecución de mount

Observando este listado podemos notar que efectivamente no nos hemos equivocado ya que esa partición es de hecho la partición root ya que contiene directorios "usr", "var", "proc", "bin", "root", "etc", etc... Vemos que el directorio "home" tiene 2 enlaces, y el directorio "usr" tiene 20 enlaces (ya que por las entradas de directorios "." y ".." el número mínimo de enlaces que llevan a un directorio son 2). Todavía no sabemos que es lo que exactamente contiene la partición /dev/hdd4. Parece que posiblemente contiene el contenido del /home y no del /usr ni tampoco /var por las mismas razones.

Verificamos que es lo que contiene el fichero /etc/passwd para ver que UID/GIDs hay dentro. Este archivo debe ser copiado y utilizado con la aplicación mactime del suite de herramientas The Coroner's Toolkit [13]. La aplicación nos mostrará el mapeo correcto de UIDs y GIDs.

El archivo puede contener cuentas creadas por los intrusos como por ejemplo aquí:

```
# less /mnt/etc/passwd
 . . .
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
```

```
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
z:x:0:0::/:/bin/bash
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
r00t:x:598:500::/bin/bash
games:x:12:100:games:/usr/games:
y:x:900:100::/tmp:/bin/bash
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
gdm:x:42:42::/home/gdm:/bin/bash
xfs:x:100:233:X Font Server:/etc/X11/fs:/bin/false
user1:x:500:500:User 1:/home/user1:/bin/tcsh
user2:x:501:501:User 2:/home/user2:/bin/tcsh
user3:x:502:502:User 3:/home/user3:/bin/tcsh
named:x:25:25:Named:/var/named:/bin/false
```

Figura 5. Ejecución para observar si existen intrusos

En este momento nos encontramos en la fase de observación, ahora estamos tomando notas de lo que pasó, hemos verificado que tenemos el contenido de disco duro intacto, disponemos de tres copias del disco duro y las estamos estudiando en modo solo lectura.

Aparte de analizar el sistema de ficheros con detenimiento, se han recuperado todos los ficheros eliminados utilizando la utilidad "unrm" de TCT. Una examen de los ficheros recuperados mostró eliminación de algunos ficheros log y scripts. El siguiente es una parte del script de instalación/limpieza que está incluido con el rootkit.

```
cp /var/tmp/imap-d /var/tmp/XXXXX/programs/imapdis
rm -rf /var/tmp/imap-d
echo "6. cleaning logs"
```

```
cd /var/tmp/XXXXX
cp /var/tmp/clean /var/tmp/XXXXX/programs/clean
rm -rf /var/tmp/clean
/var/tmp/XXXXX/programs/clean XXXXXXX 1>/dev/null 2>/dev/null
/var/tmp/XXXXX/programs/clean XXX.XXX 1>/dev/null 2/dev/null
/var/tmp/XXXXX/programs/clean XXXX 1>/dev/null 2>/dev/null
echo "rootkit complete"
echo "rember to disable imapd"
echo "EOF"
```

Figura 6. Resultado de la orden ejecutada, para observar que archivos fueron eliminados

El siguiente ejemplo es un extracto de script "zapper" que elimina las huellas dejadas por el intruso, o restablece el tamaño de los ficheros log a 0 bytes. No se sabe si existe una copia de este script en el sistema de ficheros activo.

```
1. !/bin/bash

 . . .
WHAT=$(/bin/ls -F /var/log | grep -v "/" | grep -v "*" | grep -v ".tgz" | grep -v ".gz" | grep -v "

for file in $WHAT
   line=$(wc -l /var/log/$file | awk -F ' ' '{print $1}')
   echo -n "Cleaning $file ($line lines)..."
   grep -v $1 /var/log/$file > new
   mv -f new /var/log/$file
   newline=$(wc -l /var/log/$file | awk -F ' ' '{print $1}')
   let linedel=$(($line-$newline))
   echo "$linedel lines removed!"
done
echo " "
```

Figura 7. Ejecución de la orden

Los intrusos permanentemente mejoran sus técnicas, sean de acceso, ocultación de pruebas o de eliminación de huellas, siendo difícil, o en algunos casos imposibles de reconstruir el 100% de los eventos ocurridos.

Los forenses de hace varios años tienen dificultades adaptándose a las nuevas técnicas ya que no solo son necesarios los conocimientos de la materia sino experiencia en campos que tienen bastante poco que ver con la ciencia forense - ingeniería inversa, criptografía, programación en lenguajes de bajo nivel.

UNIVERSITAS MAJOR PACENSIS DIVI ANDREÆ

Capítulo III

Referencia Teórica

Modelos en la gestión de riesgos en la seguridad de la información, en el tratamiento de la evidencia digital

3.1 Modelos forenses

Existen diversos modelos de análisis forense para el manejo del proceso de investigación digital. El propósito de los modelos de investigación digital, es informar, formar y estandarizar las investigaciones digitales, algunos de los modelos forenses son [21]:

3.1.2 El modelo DFRWS (Digital Forensic Research Workshop)

El sistema DFRWS fue desarrollado entre 2001 y 2003 en el Digital Forensic Research Workshop. El sistema introduce “Clases de Acción en la Investigación Digital”, las cuales sirven para clasificar las actividades de una investigación en grupos. Este modelo no dicta que acciones en particular deben ser perseguidas, en cambio proporciona una lista de técnicas, algunas de las cuales son requeridas. Lo específico del sistema debe ser claramente redefinido para cada investigación particular.

El sistema está representado por una tabla, que incluye columnas para la clase de actividad y un renglón para la técnica a seguir. Estas técnicas pueden realizarse en persecución de las metas de la clase de acción asociada.

3.1.3 El modelo de Reith, Carr y Gunsch

El modelo presentado por Reith, Carr y Gunsch es muy similar al sistema DFRWS. El modelo incluye Preservación, Recolección, Análisis y Presentación, clases definidas en forma similar a las de DFRWS.

El modelo también agrega soporte para la preparación de herramientas y la formulación dinámica de acercamientos de investigación. Este modelo también soporta iteraciones libres de clases de actividad individuales.

3.1.4 El modelo de Ciardhuain

El modelo propuesto por Ciardhuain está basado en modelos previos, pero expone una arquitectura de cascada aumentada. Las clases de actividad del modelo están doblemente ligadas, de manera que la búsqueda de trabajo en una clase de actividad, puede causar una iteración de algunos o todos los trabajos en las clases de actividad anteriores. La inclusión de estructuras conocidas como flujo de información permite una comprensión más profunda de la fuente de evidencias y otros datos. Este flujo debe estar definido sobre una base organizacional, pero puede aplicarse a diferentes investigaciones dentro de la misma organización.

3.1.5 El modelo Beebe y Clark

El modelo de Beebe y Clark proporciona la estructura para las actividades mediante fases que consisten de múltiples sub fases, que van más allá que el agrupamiento por actividades. Las sub fases están basadas en objetivos, más

que estrictamente en actividades.

Las sub fases basadas en objetivos caen en una fase particular y consisten de una jerarquía de actividades particulares que están subordinadas al objetivo particular.

Además, el modelo Beebe y Clark, incluye los principios de la investigación digital sobre todas las fases y sub fases, lo cual afecta la forma en que éstas son llevadas a cabo. Las últimas metas para cada sub fase, están representadas como objetivos, más que como tareas específicas. Los objetivos son metas que espera alcanzar con actividades de naturaleza similar relacionadas con un caso específico. Las tareas están directamente ligadas a un caso específico, tipo de crimen, plataforma, etc.

Capítulo IV

Referencia Teórica

Análisis las recomendaciones de la NIST en el caso de incidentes en la recuperación de información digital y otras recomendaciones internacionales.

4.1 Metodología forense del instituto nacional de estándares de tecnología (nist)

El análisis forense es necesario en diferentes situaciones, tales como la recopilación de evidencia para los procedimientos judiciales y medidas disciplinarias internas, el manejo de incidentes relacionados con código malicioso y problemas operativos. Independientemente de las necesidades, el proceso de análisis forense debe realizarse de acuerdo al proceso de cuatro etapas, descritos en la Figura 1. Los detalles precisos de estas etapas, pueden variar de acuerdo al requerimiento del análisis forense.

El Instituto Nacional de Estándares de Tecnología (NIST) es una agencia federal no regulatoria dentro del Departamento de Comercio de los E.U. Y que tiene como misión promover la innovación y competitividad industrial mediante la medición avanzada de la ciencia, estándares y tecnología, de forma que se mejore la seguridad económica y la calidad de vida.

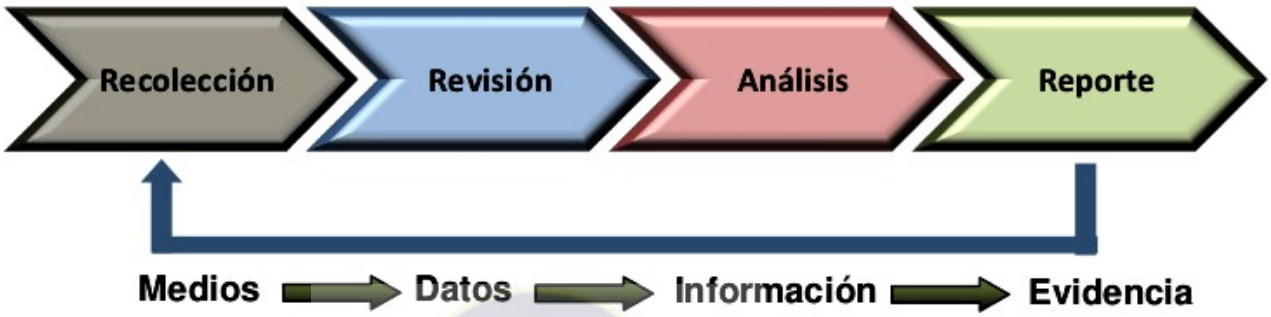

Figura 1. Proceso Forense del NIST

Como se observa en la Figura 1, el proceso forense transforma los medios en evidencia, donde la evidencia es necesaria para las autoridades o para uso interno de las organizaciones. La primera transformación ocurre cuando se examinan los datos recolectados y se convierten a un formato que sea compatible con las herramientas forenses. Segundo, los datos se transforman en información a través del análisis.

Finalmente la transformación de la información en evidencia se da en forma análoga a la acción de transferir el conocimiento – usando la información producida por el análisis en una o más formas durante la etapa de reporte.

4.1.1 Recolección de Datos

El primer paso en el proceso forense es identificar las fuentes potenciales de datos y la adquisición de éstos.

a. Identificar las posibles fuentes de datos

Los analistas deben tener en mente las fuentes de datos localizadas en otros lugares, por ejemplo, actividades en la red y el uso de aplicaciones. La

información también puede ser almacenada por otras organizaciones, por ejemplos los registros del proveedor del servicio de internet (ISP). Durante la recolección de datos, el analista debe tomar en cuenta al propietario de la fuente de datos. Por ejemplo, el obtener una copia de los registros del ISP requiere de una orden judicial.

El uso cada vez más generalizado de la tecnología digital tanto para fines profesionales como personales, da lugar a una abundante fuente de datos. Las fuentes de datos más comunes y evidentes son las computadoras de escritorio, servidores, dispositivos de almacenamiento en red, y laptops. Estos sistemas típicamente cuentan con unidades internas que aceptan medios digitales, como CD y DVD, también cuentan con varios tipos de puertos (USB, Firewire, PCMCIA) para conectar dispositivos de almacenamiento externo. Algunos ejemplos de dispositivos de almacenamiento externo que pueden ser fuentes de datos son las unidades extraíbles y tarjetas de memoria. Los sistemas de cómputo estándar también contienen datos volátiles que están disponibles temporalmente (antes de que el sistema de apague o reinicie). Además de estos dispositivos, muchos dispositivos digitales portátiles pueden contener datos (PDA's, celulares, cámaras digitales, videocámaras digitales, reproductores de audio). Los analistas deben ser capaces de localizar estos dispositivos durante la inspección en la escena del crimen y emplearlos como fuentes de datos.

Los analistas deben considerar además, las políticas de la organización y los aspectos legales, en relación a las propiedades externas a la organización, por ejemplo, la laptop de un empleado o de un contratista. La situación puede ser más complicada aún si se consideran controles fuera de la organización. A veces, simplemente no es posible obtener datos de una fuente primaria, por lo que se debe tomar en cuenta fuentes de datos alternas, que pueden contener algunos o la totalidad de los mismos datos y usar esas fuentes en lugar de la

original.

El registro centralizado evita que los usuarios manipulen la información y empleen técnicas anti-forenses para impedir su análisis. El realizar copias de seguridad con regularidad, permite a los analistas ver el estado del sistema en un momento predeterminado. Además, los controles de monitoreo de seguridad, como Sistemas Detector de Intrusos (IDS), Antivirus, Utilidades de Detección y Eliminación de Programas Espías, pueden generar registros de cuando y como se llevó a cabo un ataque o intrusión.

Las organizaciones por su parte, pueden tomar medidas proactivas para recopilar datos que puedan emplearse en un proceso forense, por ejemplo, configurar como parte del funcionamiento normal, el que los sistemas operativos auditen y registren ciertos tipos de eventos, como intentos de autenticación y cambios a las políticas de seguridad. Los registros de auditoría proporcionan información valiosa, incluyendo la hora en que se suscitó el evento y el origen de éste. Otra acción útil es implementar el registro centralizado, lo que implica que ciertos sistemas y aplicaciones envíen copia de sus registros a un servidor central.

Otra medida proactiva de recolección de datos es monitorear la actividad del usuario, por ejemplo que teclas presiona, cuales registros de un sistema en particular usa el teclado. Aunque esta medida proporciona un registro valioso de la actividad del usuario en el equipo de cómputo, también puede significar una violación a su intimidad, a menos que se le comunique por medio de las políticas de la organización que estas medidas pueden ser tomadas.

b. Adquisición de los Datos

Después de que se han identificado las fuentes de datos, el analista debe proceder ahora con la obtención de los datos de esas fuentes. La adquisición debe realizarse llevando a cabo el proceso de tres pasos: Desarrollar un plan de obtención de datos, Obtener los datos y Verificar su integridad.

i. Desarrollar un plan de adquisición de datos

Debido a la gran diversidad de fuentes de datos que se pueden localizar en una escena de crimen, es necesario que el analista elabore un plan en el cual se prioricen las fuentes, estableciendo el orden en el que van a obtenerse los datos.

ii. Obtención de datos

El proceso general para la obtención de datos, involucra el empleo de herramientas forenses para la recolección de datos volátiles, el duplicado de fuentes de datos no volátiles para obtener sus datos y el aseguramiento de las fuentes originales. El proceso de obtención de datos es posible realizarlo tanto de manera local, como en red.

iii. Verificar la integridad de los datos

Antes de que el analista inicie la recolección de los datos, él o el administrador, de acuerdo con las políticas de la organización y a las disposiciones legales, deben decidir sobre la necesidad de recolectar y preservar la evidencia, de manera que ésta se pueda emplear posteriormente en situaciones legales o en un procedimiento interno.

Una vez que se han obtenido los datos, se debe verificar su integridad. Es particularmente importante para un analista, probar que los datos no han sido

alterados, lo cual es necesario por razones legales.
En tales situaciones, se debe llevar de manera estricta un registro preciso, proceso conocido como cadena de custodia, el cual permitirá evitar acusaciones respecto a un mal manejo o manipulación de la evidencia.
Además, se deben seguir algunos otros pasos:

- A lo largo de todo el proceso, se debe llevar un registro de todas y cada una de las actividades realizadas para la recolección de datos, incluyendo información acerca de cada herramienta empleada.

- La documentación permite a otros analistas repetir el proceso en caso de ser necesario.

- Adicionalmente, es indispensable tomar fotografías de la evidencia para mantener presente la configuración del equipo de cómputo, así como de sus dispositivos periféricos.

- Antes de realizar cualquier acción sobre el equipo de cómputo, se debe tomar nota o fotografía de cualquier documento o programa que se muestre en el monitor en ese momento.

- Documentar si es que se encuentra activo algún protector de pantalla, el cual posiblemente cuente con contraseña.

- De ser posible, designar a una sola persona para que sea la encargada de custodiar la evidencia, fotografiar, documentar y etiquetar cada elemento encontrado, así como de registrar cada actividad que se realice durante el proceso.

- Para apoyar al analista con la recolección de evidencia, previamente deben

prepararse las estaciones de trabajo, los dispositivos de respaldo, medios en blanco, y accesorios de manipulación de evidencia (cuadernos, formatos de cadena de custodia, bolsas de almacenamiento de evidencia, cámaras digitales, cintas de evidencia).

- En algunos casos puede ser necesario que la escena del crimen esté asegurada físicamente para prevenir accesos no autorizados y alteración de la evidencia (guardia en la escena).

c. Consideraciones en la Respuesta a Incidentes

La organización también debe considerar el impacto que puede tener la contención del incidente, ya que un sistema fuera de actividad durante algún periodo de tiempo puede perjudicar sus operaciones y resultar en pérdidas.
Una de las medidas adoptadas con frecuencia para contener incidentes, es el de asegurar la periferia en torno al equipo comprometido y limitar el acceso a personal autorizado durante el proceso de recolección de datos y garantizar que la evidencia no sea alterada. Además, contar con una lista de las personas con acceso al equipo, ya que en un momento dado, podrían proporcionar información sobre contraseñas o donde se localiza algún dato en específico.

Cuando se realiza análisis forense durante la respuesta a un incidente, es importante considerar cuando y como se debe contener dicho incidente.

Si el equipo de cómputo forma parte de una red, desconectarlo puede evitar que algún usuario modifique la información de forma remota. Si el equipo utiliza una conexión inalámbrica, se pueden desactivar los adaptadores de red externo y/o interno o bien cortar la conexión de red a cualquier punto de acceso.

El aislamiento de algunos sistemas puede ser necesario para prevenir daños

mayores al sistema o sus datos y preservar la evidencia. En ocasiones, el analista debe trabajar en coordinación con el equipo de respuesta a incidentes para decidir, por ejemplo, que cables desconectar, aumentar las medidas de seguridad física, apagado de un host; esta decisión debe estar basada en las políticas y procedimientos relacionados con la contención del incidente, así como por la evaluación del riesgo del incidente, de modo que la estrategia de contención, mitiguen el riesgo mientras se mantiene la integridad de la evidencia, tanto como sea posible.

4.1.2 Revisión

Sin embargo, es posible utilizar diversas herramientas para reducir la cantidad de archivos de datos que deben ser analizados. Se pueden emplear búsqueda de documentos por un patrón en particular, un texto en el archivo, información relacionada con alguna persona o una dirección de correo electrónico.

Otra técnica, es emplear herramientas que pueden determinar el tipo de contenido de los archivos (texto, música, gráficos, archivos comprimidos), lo cual sirve para identificar archivos que merezcan un estudio más detallado, así como para excluir aquellos que no sean relevantes al caso en investigación.

Después de haber recolectado los datos, la siguiente fase consiste en examinar los datos, lo cual implica la evaluación y extracción de las partes de información relevantes de los datos recolectados. Esta fase también puede involucrar evitar o mitigar las características de Sistemas Operativos o aplicaciones que oculten datos y código (compresión de datos, cifrado y mecanismos de control de acceso).

El disco duro obtenido puede contener cientos o miles de archivos, la

identificación de los archivos que contienen información de interés puede ser una tarea desalentadora. Esta lista de archivos debe depurarse ya que por ejemplo un firewall puede tener millones de registros, pero solo cinco de ellos están relacionados con el incidente.

4.1.3 Análisis

Si la evidencia es necesaria en un juzgado, el analista debe documentar detalladamente todos los hallazgos y cada una de las actividades realizadas.

Una vez que ha sido extraída la información más relevante, el analista debe estudiarla y analizarla para generar las conclusiones del caso. La fundación de análisis forense emplea un enfoque metódico para obtener resultados con los datos disponibles o determinar que aún no es posible concebir una conclusión adecuada.

El análisis debe incluir la identificación de personas, lugares, objetos, eventos y la forma en que estos se relacionan, de modo que permita formar una conclusión preliminar.

4.1.4 Elaboración de Informes

La etapa final es la elaboración del informe de resultados del análisis forense, en la cual se prepara y se presenta la información resultante de la etapa de análisis. Existen algunos factores que influyen en la elaboración del informe, entre ellos:

a. Explicaciones alternas

Cuando la información relacionada con un evento no está completa, puede que no sea posible llegar a una explicación definitiva sobre lo ocurrido. Cuando un evento resulte con más de una explicación, cada una de ellas deben presentarse en el reporte. El analista debe emplear un enfoque metódico para probar o refutar cada explicación propuesta.

b. Considerar a la audiencia

El personal directivo puede querer simplemente un panorama general de lo sucedido, tal como una representación visual de cómo se produjo el ataque y que medidas deberían tomarse para prevenir situaciones similares.

Es importante conocer a quien se le presentará el informe. Un reporte para las autoridades judiciales, requiere un informe muy detallado de toda la información recopilada y es posible que se exija una copia de todas las evidencias obtenidas. Un administrador puede requerir ver todo el tráfico de la red y estadísticas con gran detalle.

c. Información procesable

El reporte también incluye la identificación de información procesable que puede permitir al analista recolectar nuevas fuentes de datos.

Una vez que se han aplicado los cambios propuestos, se informa a todos los miembros del equipo y recordar con frecuencia de los procedimientos a seguir. Los equipos suelen tener mecanismos de control de cambios e identificación de versiones de cada proceso y procedimiento. Además de esto, se puede contar con posters montados en puertas y paredes con los pasos a seguir.

Como parte del proceso de elaboración de reportes, el analista debe identificar problemas que deban ser solucionados, tales como deficiencias en las políticas o errores en los procedimientos. Muchos equipos de respuesta a incidentes y análisis forense se reúnen a discutir los resultados obtenidos, en la que se incluye un examen a conciencia de las posibles mejoras a las directivas y procedimientos y por lo general, se aprueban algunos cambios menores.

4.6 Recomendaciones del NIST

a. Las organizaciones deben ejecutar el proceso forense empleando métodos consistentes. Es recomendable que toda organización dedicada a actividades de investigación en materia de Informática Forense cuente con una metodología de análisis bien establecida, en el entendido que las etapas que conformen dicha metodología podrían variar, de acuerdo a las necesidades.

b. Los analistas deben conocer toda la gama de posibles fuentes de datos. Los analistas deben ser capaces de inspeccionar un área física y reconocer todas las posibles fuentes de datos, deben tener la capacidad de reconocer y considerar aquellas fuentes de datos ubicadas en otros lugares dentro y fuera de la organización.

c. Las organizaciones deben ser proactivas en la recolección de datos. Configurar características de auditoría de los Sistemas Operativos, implementado registros de eventos centralizados, realizando copias de seguridad del sistema de manera regular y usando mecanismos de monitoreo de la seguridad, pueden formar fuentes de datos que puedan emplearse en futuros esfuerzos de análisis forense.

d. Los analistas deben llevar a cabo la recolección de datos empleando un

proceso estandarizado. Las etapas de la metodología de análisis forense del DOJ, identifican fuentes de datos, desarrollan un plan para adquisición de los datos y verificación de la integridad de éstos.

e. Se debe seguir un enfoque metódico para analizar los datos. La Fundación de Análisis Forense, está utilizando un enfoque metódico en el análisis de los datos disponibles, de manera que el análisis pueda generar conclusiones apropiadas o determinar que el obtener una conclusión apropiada no es posible aún.

f. Se debe revisar el proceso y practicas forense con regularidad para identificar áreas de mejora. Mediante revisiones a las actuales y recientes acciones de análisis forense, puede ayudar a identificar deficiencias en las políticas de seguridad, errores en los procedimientos y otras cuestiones que necesiten de solución.

4.2 Otras recomendaciones

4.2.1 Metodologías de análisis forense

Una serie de modelos de análisis forense han sido desarrollados desde el año 2000 con el objetivo de ayudar al investigador a obtener una conclusión al término de su investigación. Algunos de los modelos de análisis forenses, incluyen – mas no están limitados a – los propuestos por Kruser, el Departamento de Justicia de los Estados Unidos (DoJ), Casey, Reith y Ciardhuain. En la Figura 2 se muestra un listado de diferentes modelos forenses y las etapas que los conforman [27].

En este capítulo, se abordarán más a detalle los modelos del Departamento de Justicia de E.U. (DoJ), el Instituto Nacional de Estándares de Tecnología (NIST), la Red Europea de Institutos de Ciencias Forenses (ENFSI) y el EC COUNCIL.

PROCESO	MODELO					
	ENFSI	DOJ	NIST	DFRWS	EC COUNCIL	Ciardhuain
Evaluación					*	
Analizar	*	*	*	*	*	
Recolectar		*	*	*	*	*
Examinar		*	*	*		*
Reporte	*	*	*		*	
Identificación				*	*	
Preservación	*			*		
Clasificación		*	*			
Presentación				*		*
Decisión				*		
Preparación	*				*	
Estrategia	*					
Sensibilización						*
Autorización						*
Planeación	*				*	*
Notificación						*
Transportación	*					*
Almacenamiento						*
Hipótesis	*					*
Prueba/Defensa						*
Difusión						*
Autoevaluación					*	

Figura 2. Modelos de Análisis Forense Digital

El análisis forense digital ha experimentado una rápida serie de avances desde su aparición hasta la fecha. Una investigación forense está compuesta de múltiples facetas, que incluyen aspectos tecnológicos, procedimientos y aspectos legales, por lo que se vislumbra la necesidad de un Modelo de Análisis Forense Integral.

Los modelos de análisis forense digital consisten de tres etapas básicas que Kruse y Heiser refieren como las tres A's. Estas son Adquirir la evidencia asegurándose que la integridad sea preservada; Autenticar la validez de los datos obtenidos y Analizar los datos manteniendo su integridad [23]. Algunos de los modelos forenses que se tratarán en este capítulo incluyen estas tres etapas.

4.2.2 Metodología forense del departamento de justicia de los estados unidos

El Laboratorio de Cibercrimen en la Sección de Propiedad Intelectual y Crimen Computacional (Computer Crime and Intellectually Property Section) desarrolló

un diagrama de flujo en el cual se describe la Metodología de Análisis Forense Digital, dicho trabajo se realizó después de consultar con numerosos analistas forenses de varias agencias federales. Los elementos clave del Cómputo Forense se listan a continuación:

- El empleo de métodos científicos.
- Recolección y Preservación.
- Validación.
- Identificación.
- Análisis e Interpretación.
- Documentación y Presentación.

El Departamento de Justicia de los Estados Unidos, establecido el 22 de junio de 1870 e inaugurado el 1o. de julio del mismo año, es un ministerio, parte del Gobierno de los Estados Unidos, diseñado para hacer cumplir las leyes, defender los intereses del país de acuerdo con la ley y para asegurar una administración de justicia imparcial y justa para todos los estadounidenses.

En la Figura 3 se ilustra una vista general del proceso, en el cual, las tres etapas, Preparación/Extracción, Identificación y Análisis están resaltadas debido a que conforman el núcleo del análisis forense para este organismo.

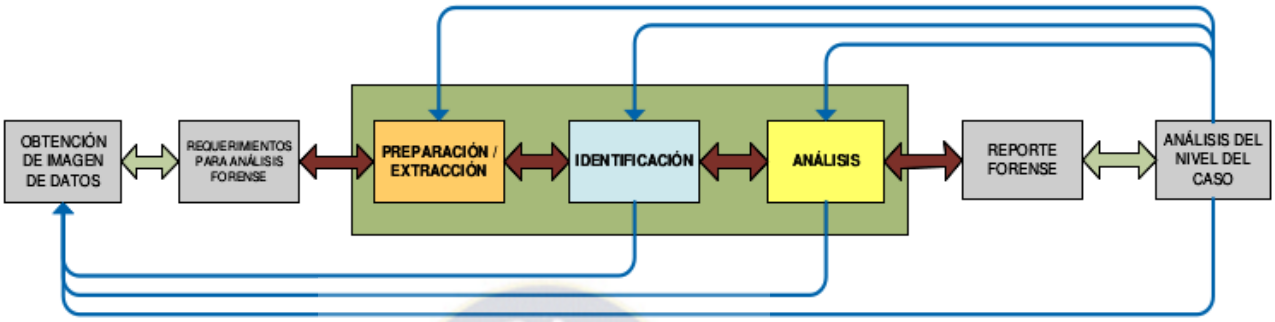

Figura 3. Proceso de Análisis Forense DoJ.

Las tres etapas del proceso forense, se explican partiendo de que los analistas ya han obtenido previamente la imagen de los datos, así como los recursos necesarios para el análisis, y hasta antes de que se elabore el reporte y el análisis del nivel del caso.

4.2.2.1 Preparación/Extracción

La primera etapa en cualquier proceso forense es la validación del hardware y software a emplear, para asegurarse de que éste funcione de forma adecuada. Existe todavía la controversia en la comunidad forense con respecto a la frecuencia con que se debe probar el software y el equipo. La mayoría de los analistas están de acuerdo que, como mínimo, las organizaciones deberían validar cada pieza de software después de adquirirlo y antes de que sea utilizado.

Cuando la plataforma de los analistas está lista, realizan un duplicado de los datos forenses proporcionados en la petición y verifican su integridad. Este proceso asume que las autoridades ya han obtenido los datos a través de un proceso legal y realizado la imagen forense de dichos datos. También se asume

que el analista ha recibido una copia de trabajo de los datos asegurados, en caso de que el analista cuente con la evidencia original, debe realizar una o varias copias de trabajo y guardar la cadena de custodia de la evidencia original.

Los analistas comienzan preguntándose si hay suficiente información para proceder. Se aseguran de que la petición es clara y de que cuentan con los datos suficientes para poder responder a dicha petición. Si algo hace falta, establecen coordinación con quien realizó la petición, de otra manera dan inicio al proceso.

Las pruebas también deben realizarse después de alguna actualización, parche o nueva configuración.

Después de que los analistas han verificado la integridad de los datos, se desarrolla un plan para la extracción de los datos, se organiza y detalla la petición forense en preguntas que ellos comprendan y puedan responder. Seleccionan las herramientas que permiten responder a estas preguntas. Generalmente, los analistas cuentan con ideas preliminares acerca de que es lo que se debe buscar, basándose en la petición o requerimiento, lo cual agregan a una “Lista de Búsqueda Principal”, que es una lista de recopilación de los elementos solicitados. Los analistas manejan esta lista para ayudar a enfocarse en el examen forense. Para cada búsqueda los analistas extraen los datos relevantes y marcan esa búsqueda como “procesada” y anexan cualquier dato extraído a otra lista llamada “Lista de Datos Extraídos”. Los analistas llevan el seguimiento de todas las búsquedas, agregando los resultados a esta segunda lista y continúan con la siguiente etapa de la metodología, la Identificación.

El analista se asegura de que la copia en su posesión está intacta y sin alteraciones, lo cual normalmente se lleva a cabo verificando el hash o huella

digital de la evidencia, si se encuentra algún problema, el analista consulta con el solicitante acerca de cómo proceder.

4.2.2.2 Identificación

Si un elemento es relevante para la investigación, el analista lo debe documentar en una tercera lista, la “Lista de Datos Relevantes”, la cual es una colección de datos que dan respuesta al requerimiento original. Por ejemplo, en un caso de robo de identidad, los datos relevantes pueden incluir números de seguro social, imágenes de identificaciones falsas o correos electrónicos donde se trate el robo de identidad, entre otras cosas. También es posible que un elemento genere una nueva búsqueda, por ejemplo que un correo electrónico revele un nuevo nombre de usuario, este nuevo nombre de usuario generará otra “Lista de Búsqueda Principal”, en particular para ese nombre.

Los analistas repiten el proceso de identificación para cada elemento de la “Lista de Datos Extraídos”. Primero se determina qué tipo de elemento es. Si el elemento no es relevante para la investigación, simplemente se marca como “procesado” y se mueve. Tal como en una búsqueda física, si el investigador se encuentra con un elemento incriminatorio, pero que está fuera del alcance de la orden de registro, se recomienda que detenga toda actividad inmediatamente y notifique el descubrimiento a las personas apropiadas, incluyendo al solicitante y espere nuevas instrucciones.

Un elemento puede apuntar a una nueva fuente de datos. Por ejemplo, es posible encontrar que el objetivo estaba empleando otra cuenta de correo electrónico y las autoridades pueden desear citar el contenido de esta nueva cuenta. Se puede encontrar también que el objetivo almacenaba información en un medio removible (USB) alguno no encontrado en la búsqueda inicial. Bajo

estas circunstancias, las autoridades considerarán obtener una nueva orden de registro para buscar el dispositivo USB. Un análisis forense puede apuntar a muchos tipos diferentes de evidencia, tales como log de firewall, registros de acceso a edificios, videos de seguridad, lo cual se documenta en una cuarta lista, la “Lista de Nuevas Fuentes de Datos”.

En este punto del proceso, es aconsejable que el investigador informe al solicitante de sus conclusiones iniciales.

Dependiendo de la etapa en la que se encuentre un caso, los datos obtenidos hasta ese momento pueden otorgar al solicitante la información suficiente para continuar con el caso y que los investigadores no tengan que seguir trabajando en la búsqueda de información.

Tras haber procesado la Lista de Datos Extraídos, los investigadores regresan a las nuevas pistas encontradas. Para cualquier nueva búsqueda de datos, se considera volver a la etapa de Extracción para procesarlos. De la misma manera, para cualquier nueva fuente de datos que conduzca a nueva evidencia, se considera regresar a la etapa de obtención y realización de imágenes de los nuevos datos para la investigación forense.

Si los datos obtenidos hasta esta etapa no son suficientes se procede a la siguiente etapa, el análisis.

4.2.2.3 Análisis

A menudo, es posible que los investigadores generen un análisis de mucho más valor, observando el momento en que ocurrieron las cosas, produciendo una línea de tiempo que haga más coherente las conclusiones obtenidas. Para cada

elemento relevante, se trata de explicar cuando fue creado, accedido, modificado, recibido, enviado, visto, borrado y ejecutado. Se observa y se obtiene una secuencia de los eventos y se anota cuales eventos ocurrieron al mismo tiempo.

En la etapa de análisis, los investigadores relacionan todos los datos encontrados y bosquejan una imagen completa del caso al solicitante. Para cada elemento de la "Lista de Datos Relevantes", los investigadores responden a las preguntas ¿Quién?, ¿Qué?,
¿Cuándo?, ¿Dónde? Y ¿Cómo? Tratan de explicar que usuarios o aplicaciones crearon, editaron, recibieron o enviaron cada elemento y la forma en que existía originalmente; explican también lo que han encontrado, pero principalmente explican y justifican el porqué toda esa información analizada es importante y qué relación tiene con el caso.

Los investigadores documentan todo su análisis y otra información relevante a la petición hecha, agregando todo lo anterior a una quinta lista, la "Lista de Resultados del Análisis", la cual es una lista de todos los datos significativos que responden al ¿Quién, cuando, como, donde, qué? entre otras preguntas.

Finalmente, después de que los investigadores han repetido este proceso varias veces, es posible que puedan responder satisfactoriamente las necesidades del solicitante del análisis forense y es hasta ese entonces, que proceden con la siguiente etapa, la etapa de Reporte de Resultados. La información contenida en esta lista satisface a la solicitud del cliente. Incluso en esta última etapa del proceso algún elemento podría generar nuevas búsquedas, si esto sucede, se agregan a las listas apropiadas y se analizan completamente los nuevos datos.

4.2.2.4 Reporte de Resultados

Esta es la etapa en la que los investigadores documentan y detallan todos sus hallazgos, de tal manera que el solicitante pueda entenderlos y emplearlos en su proceso judicial. El reporte final es la mejor manera que tienen los investigadores de comunicar los resultados del análisis forense a los interesados.

4.3 Metodología de análisis forense de europea de institutos forenses (enfsi)

El grupo de Proyectos de Aseguramiento de Competencia (CAP, Comptetence Assurance Project), el cual forma parte del Comité de Calidad y Competencia (QCC, Quality and Competence Comitee) en la ENFSI, desarrolló los "Estándares Basados en Desempeño para los Profesionales de las Ciencias Forenses (Performance Based Standards for Forensic Science Practicioners), los cuales son aplicados por todos los profesionales forense adscritos a la ENFSI.

El objetivo de la Red Europea de Institutos de Ciencias Forenses (ENFSI, European Network of Forensic Science Institutes) es garantizar que la calidad del desarrollo y presentación de la ciencia forense en toda Europa se halla a la vanguardia del mundo. Inicio en 1993 con 11 miembros y al 2005 eran ya 50 los miembros pertenecientes a esta red [36].

Estos estándares pueden ser aplicables en todos los Sistemas de Justicia Penal. Los Estándares cubren todo el proceso forense, desde la primera acción que el oficial realiza en la escena del incidente, pasando por la inspección de la escena, el análisis en un laboratorio, hasta la interpretación y presentación del informe de resultados para mostrar ante una corte, no son prescriptivos y

reconocen que existe más de una forma para llevar a cabo una tarea.

Figura 4. Metodología Forense de la ENFSI.

Los estándares describen lo que un profesional forense debe realizar, más no

como hacerlo. En su forma genérica son aplicables a todas las disciplinas forenses.

El proceso forense en general consta de nueve actividades y cada una de ellas se desglosa en uno o varios estándares o normas, este proceso se ve más claramente en la Figura 4 y se describen en los siguientes párrafos.

4.3.1 Actividades Iniciales en la Escena

En esta etapa, lo que se busca es obtener el control de la escena, de tal modo que el lugar se mantenga intacto para cuando arriben los peritos encargados de la investigación, además de realizar una evaluación inicial para verificar que se haya cometido un delito. En esta etapa se tiene solo un estándar o norma:

a. Preservación inicial y acciones de control en la escena.

- Verificar que en realidad se haya cometido un delito.
- Restringir el acceso a la escena del incidente.
- Realizar un análisis de riesgos de la escena.
- Recolectar la evidencia.
- Mantener la escena asegurada.
- Contar con la autorización correspondiente para llevar a cabo la búsqueda de evidencia en la escena.

4.3.2 Desarrollar Estrategia de Investigación

En esta actividad, se debe entender cuáles son los requisitos de la investigación y de los investigadores, además de realizar una evaluación de la escena y determinar las medidas necesarias para cumplir con dichos requisitos. La

estrategia de investigación se desarrolla con la finalidad de satisfacer las necesidades de la investigación, tomando en cuenta los principios y prácticas implicadas en el proceso de investigación.

a. Determinar los requisitos de la investigación

- Comprobar las anotaciones proporcionadas por el investigador acerca del incidente y de la escena, además de otras fuentes y asegurarse de que estén debidamente documentadas.
- Determinar el tipo de análisis que se llevará a cabo, de acuerdo a la información proporcionada.
- Considerar la posibilidad de que existan otros escenarios vinculados de forma que se asegure la línea de investigación.
- Determinar la logística de la investigación y resolver los problemas conocidos, haciendo énfasis en la eficacia, eficiencia y economía.
- Considerar la seguridad de todo el personal y verificar que todas las precauciones se lleven a cabo.
- Identificar los recursos y equipo necesario para la investigación y hacer los arreglos necesarios para llevarlos a la escena.

b. Evaluar la escena y determinar los requisitos

- Llevar un registro de todas las personas que estuvieron en la escena antes de que fuera restringida.
- Revisar los hallazgos iniciales en la escena, identificar y consultar otras fuentes de información.
- Identificar los recursos y equipo necesario para la investigación y hacer los arreglos necesarios para llevarlos a la escena.
- Registrar los datos relevantes, relacionados con la investigación, al momento del análisis.

4.3.2 Investigación en la escena

Esta actividad está directamente relacionada con la revisión de la escena, así como con la ubicación, identificación y recuperación de la posible evidencia, la cual será analizada con mayor detenimiento.

a. Establecer y preservar el control de la escena

- Establecer y comunicar las responsabilidades de la búsqueda en la escena.
- Confirmar si es necesario modificar los límites de la escena del crimen.
- Mantener el área debidamente acordonada.
- Restringir la entrada y salida de personal al área protegida.
- Mantener control de la escena para que la evidencia no sufra daño, contaminación o pérdida.

b. Preparativos para inspeccionar la escena

- Documentar y registrar la integridad de la escena antes de que sufra cualquier alteración.
- Establecer comunicación con el personal pertinente, a fin de gestionar la investigación científica.
- Evaluar, determinar y acordar el tipo y secuencia de análisis que serán necesarios.
- Asesorar a otros miembros respecto a los requisitos para recolección de evidencia y que se registren todas sus observaciones al momento del análisis.
- Preparar el equipo necesario verificando que éste funcione correctamente.

c. Inspeccionar la escena

- Asegurarse de que la inspección se lleve a cabo de conformidad con los requisitos legales y de la organización.
- Realizar la inspección en un orden lógico, de modo que se garantice la detección y recuperación óptima de todo tipo de evidencia.
- Seleccionar y usar métodos óptimos de recuperación de evidencia.
- Registrar toda la información relevante al momento de la inspección.

d. Recolección de evidencia

- Priorizar y recolectar, de manera secuencial la evidencia con apoyo de otro personal especializado.
- Preservar la evidencia recolectada, sin daños, degradados o contaminados.
- Establecer y mantener la seguridad del material recolectado.
- Documentar todas las actividades realizadas.

e. Empacar los elementos y muestras

- Empacar y manipular la evidencia de modo tal que se preserve su integridad y se evite la contaminación.
- Identificar claramente cada empaque.
- Sellar, etiquetar y registrar la evidencia de acuerdo a los lineamientos legales y de la organización.
- Mantener la continuidad e integridad de la evidencia.

4.3.3 Interpretar los hallazgos y ordenar nuevo análisis

Esta actividad se refiere a la interpretación de los hallazgos iniciales encontrados en la escena de forma que sea posible determinar la secuencia de

eventos acontecidos.

a. Analizar la probable secuencia de eventos

- Basar el análisis sobre los hallazgos encontrados y la información proporcionada acerca de la escena.
- Consultar fuentes de información que puedan ayudar a la reconstrucción de los hechos.
- Considerar más de una explicación de lo que pudo haber ocurrido.
- Documentar toda la información.

b. Decidir cuales elementos serán analizados a fondo

- Registrar y revisar todos los elementos de evidencia obtenidos.
- Estimar los elementos que puedan proporcionar más información en un análisis más detallado.
- En caso de ser necesario solicitar asesoría de otros especialistas en otros campos.
- Solicitar de ser necesario los análisis adicionales que pudieran ayudar a obtener más información.

c. Transferir los elementos a los lugares designados

- Seleccionar un método de transporte legal, seguro y sin riesgo de contaminación, destrucción o pérdida.
- Segregar en caso de que sea necesario los diferentes elementos cuidando mantener su integridad.
- Mantener la continuidad e integridad de la evidencia durante su transporte.
- Descontaminar los contenedores y los vehículos para transporte en caso de ser necesario haciéndolo de una manera segura o en su caso llegar hasta la

destrucción.
- Documentar todas las actividades.

d. Almacenar los elementos y muestras de evidencia

- Manipular la evidencia de tal manera que ésta sea preservada, manteniendo su continuidad, evitando la contaminación y que se ajuste a los requisitos de salud y seguridad.
- Conservar la evidencia en las mejores condiciones y que en caso de que se elimine algún elemento, esto se haga de manera segura.
- De ser necesario, descontaminar el área de almacenamiento, de acuerdo a los requerimientos de salud y seguridad.

4.3.4 Desarrollar estrategia de análisis en laboratorio

Actividad que se refiere a la elaboración de una estrategia para análisis forense, que responda a las necesidades del caso en investigación, dicha estrategia debe tomar en cuenta los principios y prácticas científicas.

a. Establecer los requerimientos del caso en investigación

- Confirmar que los elementos presentados son apropiados para la labor que se llevará a cabo.
- Determinar los requerimientos de almacenamiento para la evidencia y hacer los arreglos para que dichas instalaciones estén limpias y seguras.
- Registrar la información relevante de manera completa, precisa, y legible.
- Preparar el equipo y área en que se llevará a cabo el análisis.
- Identificar, documentar y corregir el equipo que no sea adecuado.

b. Determinar la estrategia de análisis

- Confrontar los detalles del caso contra las necesidades de la investigación.
- Determinar una estrategia de análisis tomando en cuenta las necesidades del caso.
- Revisar y hacer ajustes a la estrategia en acuerdo con el personal apropiado.

4.3.5 Preparación para análisis en laboratorio

Esta actividad busca garantizar que se lleven a cabo los preparativos adecuados antes de que se realice el análisis de los elementos de evidencia encontrados, esta preparación se realiza en todos los casos, independientemente del medio ambiente que se trate.

La preservación, integridad y continuidad de la evidencia son críticas y deben mantenerse en todo momento.

a. Determinar la integridad de los elementos y muestras

- Transportar la evidencia de manera segura a las instalaciones donde serán almacenadas.
- Confrontar los elementos contra los registros para identificar cualquier diferencia y hacer las correcciones que se consideren necesarias.
- Registrar los detalles de almacenamiento, manipulación, traslado y embalaje de los elementos para garantizar su continuidad.
- Identificar y documentar cualquier problema de empaquetado y tomar las medidas apropiadas.
- Almacenar y transportar el material de evidencia de una manera tal que se evite la contaminación.

- Almacenar y mover el material de evidencia dentro del laboratorio de manera que se evite la contaminación, daño o pérdida.

b. Inspeccionar el material de evidencia que se presentaron para su análisis

- Remover la evidencia de su paquete y manipularlo de forma segura para evitar que sufra cualquier tipo de daño o alteración.
- Confirmar la identidad del material de evidencia conforme a la documentación presentada.
- Identificar la posible evidencia y seleccionar el método de análisis más adecuado.
- Tomar las medidas adecuada en caso de identificar un problema o posibilidad de éste.
- Decidir la estrategia de muestreo a seguir para los elementos que se analizarán.
- Mantener la continuidad del material de evidencia en todo momento.
- Registrar la información que vaya resultando de manera, clara y precisa.

4.3.6 Analizar evidencia

En esta actividad se trata de localizar, identificar y recuperar la evidencia de todo el material recolectado. Esta función suele ser llevada a cabo, ya sea en la misma escena del incidente, en un laboratorio u otro lugar adecuado.

a. Vigilar y mantener la integridad del material

- Manipular el material de forma que se evite la contaminación, daño parcial o total del mismo.

- Etiquetar el material y mantener en todo momento su integridad y continuidad.
- Registrar la información de las actividades realizadas, de manera, clara y precisa, en todo momento.

b. Identificar y recuperar la evidencia potencial

- Realizar los análisis en un orden en el que se garantice la óptima detección y recuperación de evidencia.
- Localizar y recuperar evidencia física potencial y huellas.
- Identificar nuevas áreas de especialización.
- Mantener durante todo el proceso, la integridad y continuidad del material recuperado.
- Seleccionar y utilizar métodos que optimicen la recuperación.
- Registrar en todo momento, toda la información que se genere, de forma clara y precisa.

c. Determinar los análisis que se realizarán en el caso

- Seleccionar los análisis que se llevarán a cabo de acuerdo al contexto del caso.
- Planear y calendarizar los análisis, de manera que sean confiables y brinden resultados fiables.
- Solicitar la asesoría de expertos, en caso de que se requiera otro tipo de información especializada.
- Registrar en todo momento la información generada de la planeación, en forma clara y precisa.

d. Llevar a cabo el análisis

- Llevar a cabo los análisis al material con las medidas de seguridad

adecuadas.

- Adaptar los procedimientos y prácticas de trabajo, a las diferentes situaciones y condiciones y documentar dichas adaptaciones.
- Identificar resultados insuficientes y tomar las acciones correctivas que procedan.
- En caso de que se requiera información más especializada, solicitar asesoría de expertos.
- Asegurarse que los resultados sean registrados de forma clara y precisa durante todo el proceso de análisis.

e. Producción de notas y registros de laboratorio

- Generar notas y registros de laboratorio en el momento del análisis, claros, precisos y sin ambigüedades.
- Ordenar las notas y registrar la información de forma que sirva como apoyo al control por parte de terceros.
- Únicamente designar registros y archivos que ayuden a la fácil recuperación.
- Ordenar y combinar todas las anotaciones generadas durante el proceso de análisis acerca del caso.

4.3.7 Interpretar hallazgos

Esta actividad se refiere a resumir y evaluar los análisis forenses realizados, interpretar los resultados y sacar conclusiones antes de que el informe se prepare, dichas conclusiones, buscarán satisfacer los requerimientos del cliente o bien soportar una o más de las varias hipótesis que se han obtenido o simplemente desmentir una hipótesis dada.

a. Cotejar los resultados de los análisis

- Reunir y combinar los resultados en un formato claro y sin ambigüedades.
- Completar una evaluación de los resultados obtenidos.
- Presentar un resumen de los resultados en un formato perfectamente estructurado.
- Asegurar que la evaluación, comentarios e información de apoyo sea precisa y se presente de manera clara.

b. Interpretar los resultados del análisis

- Tener completos todos los datos de análisis.
- Basar la interpretación sobre los resultados obtenidos y documentados, así como en la información proporcionada acerca del caso.
- Consultar las fuentes de datos, en el momento adecuado de manera que contribuyan a interpretar más claramente los resultados.
- Confirmar los resultados y datos para precisar la validez y fiabilidad.
- Bosquejar las opiniones de los resultados, basados en criterios acordados y que dichas opiniones estén debidamente documentados.
- Registrar en todo momento, la información que se genere durante la interpretación de resultados.
- Considerar la posibilidad de dar explicaciones alternas y probar otras hipótesis, generando el dictamen pertinente.

4.3.8 Reporte de resultados

Esta activad es la presentación de informes acerca de los resultados de un análisis forense.

a. Generar el reporte

- Determinar el tipo, alcance y propósito de la información.
- Utilizar información actual en el reporte, precisa y sin ambigüedades.
- Informar todos los resultados expresando claramente las limitaciones de la evidencia utilizada.
- Presentar un informe lógico, imparcial, exacto y adecuado que responda a las necesidades del usuario final.
- Expresar dictámenes y conclusiones dentro del área de especialización del investigador, firmemente basadas en los resultados y la información disponible.
- Asegurar que el informe se ajusta a los requisitos legales y que se hacen las referencias apropiadas a las notas del caso y material relacionado.
- Considerar la posibilidad de más de una explicación a los hallazgos.

b. Participar en consultas previas al juicio

- Proporcionar asesoría basada en principios científicos establecidos y que sean equilibrados y realistas dentro del contexto del caso.
- Explicar claramente los resultados y su interpretación dentro del contexto de la investigación.
- Considerar la posibilidad de más de una explicación y probar más de una hipótesis, generando los dictámenes correspondientes.
- Identificar, aclarar y resumir los puntos de acuerdo y desacuerdo.
- Buscar la retroalimentación para verificar que los participantes comprenden los resultados.
- Registrar toda información relevante.
- Crear relaciones de trabajo eficaces con los clientes.

c. Presentar la evidencia oralmente ante los tribunales

- Entregar la evidencia en forma audible y comprensible.

- Dar pruebas de que es coherente con el informe escrito.
- Contestar las preguntas con imparcialidad, sinceridad y flexibilidad de manera inequívoca y admisible.
- Pedir se aclaren las preguntas confusas antes de responder.
- Explicar de manera específica las preguntas, de modo que faciliten el entendimiento de los presentes.
- Tomar en cuenta la información adicional, así como analizar las hipótesis alternas que sean presentadas, considerando las limitaciones de no contar con un análisis más detallado.
- Distinguir claramente entre hechos y dictámenes y asegurar que las opiniones emitidas están dentro del área de especialización.

4.3.9 Metodología de análisis forense del ec-council

El siguiente apartado del presente capítulo, está basado en el modelo empleado por el EC-COUNCIL, organización dedicada al desarrollo de cursos y al otorgamiento de certificaciones en el área de Seguridad Informática y Comercio electrónico, en dicha modelo se llevan a cabo pasos estándar mientras se realiza la preparación de un caso para solución de un problema forense, estas etapas o pasos se muestran en la Figura 5.

Figura 5. Metodología de Análisis Forense del EC-Council

4.3.10 Consideraciones previas

El permiso para llevar a cabo en el lugar del delito, se solicita a las autoridades locales de esa región. Las pruebas que pueden aportar información al caso en investigación deben ser buscadas en la escena del crimen. Una computadora puede ser una valiosa fuente de información que apoye al cumplimiento de la ley en la resolución de un caso. En ocasiones, la computadora y todos sus componentes pueden determinar la cadena de eventos que condujeron a un crimen y pueden proporcionar la evidencia necesaria para una condena.

Antes de comenzar una investigación, lo primero que se debe considerar es la ocurrencia de algún incidente y su impacto, en caso de que exista. Un Sistema de Detección de Intrusos (IDS) sólo puede indicar un intento, una intrusión fallida o bien una falsa alarma. Por lo tanto, es necesario medir las fortalezas, debilidades y otras características relacionadas con las fuentes, así mismo incluir otros factores, tales como los humanos y los digitales.

Se debe realizar una evaluación preliminar para la búsqueda de evidencia, después de dicha evaluación se debe recoger y asegurar los equipos que se emplearon en la comisión del delito, documentar todo lo relacionado con los equipos recolectados, tales como los CDs, DVDs, unidades de disco, etc. Antes de realizar la recolección de evidencia se debe tomar una imagen instantánea de la escena del crimen. Después de haber obtenido toda la información, el investigador puede listar los pasos que puede seguir durante la investigación y después dar inicio a ella.

4.3.11 Evaluación inicial del caso

El investigador debe realizar preguntas relacionadas con las personas y documentar las respuestas. Las preguntas pueden estar relacionadas con la incautación de los equipos informáticos, los componentes de seguridad y todo esto debe ser realizado por una compañía de seguridad.

Identificar los requerimientos del caso implica conocer el tipo de caso que se va a investigar. Se trata de esbozar los detalles del caso de manera sistemática, esto es, conocer la naturaleza del caso, las evidencias disponibles y su ubicación, así como el tipo de estas (disco duro, disquetes, etc.), los sistemas operativos empleados por el sospechoso, tipo de sistema de archivos (FAT, NTFS, etc.) el tipo de trabajo que desempeña el personal, y los motivos del sospechoso.

4.3.12 Determinar un diseño preliminar o la manera de abordar el caso

Durante esta etapa, se prepara un esquema general para la investigación. En esta etapa se determina si la computadora o el equipo puede ser incautado

durante las horas de trabajo o el investigador debe esperar hasta el término de la jornada laboral o incluso al fin de semana.

4.3.13 Preparación de un diseño detallado

Los lineamientos generales que se prepararon en las etapas anteriores se deben refinar y detallar, tomando en cuenta la estimación de tiempo y recursos necesarios para completar cada etapa. Esto ayuda al investigador forense a llevar el seguimiento del progreso de la investigación y tener un control adecuado de la misma, en caso de que se presente alguna desviación al plan inicial.

4.3.14 Determinar los recursos requeridos

El tipo de software que se utilizará para la investigación varía, de acuerdo al sistema operativo con que trabaja el equipo sospechoso.

Sin embargo, es recomendable contar con un kit de herramientas estándar ya preparado y conforme avance la investigación, emplear aquellas que se requieran.

4.3.15 Obtener la evidencia

Los diferentes tipos de equipos empleados por los sospechosos para cometer un crimen se incautan y se aseguran. Durante el proceso de recolección, el investigador debe observar el lugar en el que la evidencia se encuentra almacenada. Es aconsejable contar con una lista de verificación previamente preparada para marcar todos los hallazgos y listar todas las posibles cosas que

pudieron ser empleadas en la comisión del delito.

Es claro que no es posible obtener evidencia de todo el sistema, puesto que implica un gran consumo de tiempo, debido a esto, es necesario enfocarse en aquellas cosas realmente relevantes para el caso y evitar caer en una sobre recolección de evidencia.

Se debe tomar en cuenta que no toda la evidencia permanece por largo tiempo, es decir se considera volátil y depende principalmente del suministro de energía eléctrica, en este orden de ideas se debe asegurar de obtener la evidencia de acuerdo al orden de volatilidad de ésta, un ejemplo de esto puede ser:

- Registros y memoria cache.
- Tablas de ruteo.
- Memoria ARP.
- Tabla de procesos.
- Estadísticas del Kernel y módulos.
- Erradicar vías externas de alteración.

Se debe obtener la evidencia mediante el empleo de técnicas y procedimientos aceptados. Todo el proceso de obtención de evidencia debe documentarse plenamente, por lo que debe prepararse la cadena de custodia de toda la evidencia que se encuentre, anotando entre otros datos, las estampas de tiempo y firmas digitales.

4.3.16 Copiar la evidencia del disco

La siguiente etapa, después de recuperar la evidencia, es copiarla a disco y analizar los datos sobre la copia, de esta manera se evita que la evidencia

original sufra alteraciones en sus datos, ya que la primera regla en el análisis forense es “preservar la evidencia original”. La mejor manera de crear una imagen del disco es hacerlo bit a bit, para lo cual existen diferentes herramientas tanto comerciales como de uso libre, además de la funcionalidad que ofrece MS.DOS con el comando diskcopy.

4.3.17 Identificar el riesgo involucrado

A menudo, los investigadores se enfrentan a muchos problemas durante la conducción de la investigación y requieren documentar todos los problemas que se encuentren a lo largo de la investigación, a esta fase de documentación se le conoce como “Evaluación de Riesgos Estándar”. Por ejemplo, un usuario puede tener configurado su equipo de tal manera que este se apague o incluso se borre el disco duro si alguien quiere cambiar la contraseña, lo cual impide que el investigador manipule o intente acceder al equipo, este tipo de problemas debe documentarse para posteriormente analizar las acciones a seguir.

4.3.18 Minimizar el riesgo

Un analista forense debería distinguir diferentes formas de minimizar los riesgos, por ejemplo, si el sospechoso tiene protegido el disco duro con contraseña, el analista debería realizar múltiples copias de ese disco duro antes de iniciar la investigación, lo cual resultará de mucha utilidad en la etapa de recuperación de información, ya que se intentará acceder al disco duro de diferentes formas sin el riesgo de alterar la información del disco original y en caso de que el disco duro se dañe, se cuenta con copias adicionales para realizar el análisis.

4.3.19 Probar el diseño

Las decisiones que fueron tomadas y las etapas que se llevaron a cabo deberían ser revisadas. Esta revisión, la cual es ejecutada por un investigador, permite detectar cuales de los pasos realizados son correctos y justificados.

4.3.20 Analizar y recuperar la evidencia digital

La evidencia digital puede ser analizada y extraída empleando diferentes herramientas de software y otros recursos que han sido determinados en etapas anteriores.

4.3.21 Investigación de los datos recuperados

Una vez que se han extraído y analizado los datos, estos pueden organizarse de modo tal que ayuden a probar la inocencia o culpabilidad del sospechoso.

4.3.22 Completar el reporte del caso

Se prepara un reporte completo y detallado acerca de lo que el analista forense realizó y encontró en los datos que fueron recuperados del incidente y durante su investigación.

4.3.23 Criticar el caso

La metodología empleada por el EC-COUNCIL culmina con la autoevaluación por parte del investigador. Después de que la investigación ha concluido y se ha generado el reporte, éste debe ser revisado para identificar las acciones y

decisiones tomadas, con el fin de mejorar su procedimiento, lo cual le ayudará en sus investigaciones futuras.

4.4 Comparativa de actividades de las diferentes

4.4.1 Metodologías de análisis forense digital

En el presenta apartado se muestra un cuadro comparativo con el desglose de las diferentes actividades que se realizan en cada una de las metodologías analizadas en este trabajo, en el cual se puede observar, que a pesar de la diversidad de actividades, la mayoría de ellas son comunes a todas las metodologías que se estudiaron, con la diferencia de que algunas se aplican en etapas con diferente nombre.

ACTIVIDADES	METODOLOGÍA			
	DoJ	NIST	ENFSI	EC-COUNCIL
La investigación forense parte de una petición	*			*
Obtener orden judicial		*	*	*
Aseguramiento de la escena		*	*	
Verificar la ocurrencia del incidente			*	*
Tomar instantánea de la escena del crimen				*
Inspeccionar la escena del crimen		*	*	
Documentar y registrar la integridad de la escena antes de sufrir alguna alteración			*	
Determinar los requerimientos de la investigación			*	*
Considerar como y cuando contener el incidente		*		
Manejo de "Listas" para clasificación y seguimiento de evidencia	*			
Determinar manera de abordar el caso				*
Identificar fuentes potenciales de datos		*	*	
Desarrollar plan de obtención de datos		*	*	
Obtener la imagen de los datos	*	*		*
Determinar y obtener los recursos necesarios para el análisis	*		*	*
Verificar que la información disponible sea suficiente.	*			
Determinar el tipo de análisis que se llevará a cabo			*	
Verificar la posibilidad de que existan otros escenarios			*	
Validación de hardware y software.	*		*	
Preservar la evidencia recolectada.			*	

Figura 6. Cuadro comparativo entre las diferentes metodologías

ACTIVIDADES	METODOLOGÍA			
	DoJ	NIST	ENFSI	EC-COUNCIL
Documentar todas las actividades de recolección			*	
Duplicado de los datos forenses obtenidos	*			
Verificación de integridad de los datos	*	*		
Realizar copia de trabajo de los datos asegurados	*			*
Mantener cadena de custodia de la evidencia original	*	*		
Verificar que la copia de trabajo no tenga alteraciones (hash)	*			
Desarrollo de un plan para extracción de datos	*			
Creación de la "Lista de Búsqueda Principal" (elementos solicitados)	*			
Extracción de datos relevantes de la "Lista Principal".	*			
Creación de la "Lista de Datos Extraídos"	*			
Determinación del tipo elemento contenido en la "Lista de Datos Extraídos".	*			
Examinar los datos recolectados.		*		*
Clasificación de los elementos de la "Lista de Datos Extraídos" (relevante, no relevante)	*		*	
Evaluar y extraer información relevante		*		
Creación de la "Lista de Datos Relevantes".	*		*	
Reducir cantidad de datos que serán analizados		*	*	
Generación de nuevas búsquedas.	*			
Identificación de nuevas fuentes de datos (Lista de Nuevas Fuentes de Datos)	*			
Nuevas búsquedas retorno a etapa de Extracción.	*			
Nueva fuente de datos implica obtencion de imagen de datos.	*			
Informar al solicitante conclusiones iniciales.	*			
Transferir la evidencia a los lugares designados			*	
Almacenar la evidencia de manera que se conserve su integridad			*	
Determinar la estrategia de análisis			*	
Analizar la información relevante		*	*	*
Etiquetar la evidencia y mantener su integridad			*	
Relacionar todos los datos encontrados	*			
Bosquejar una imagen completa del caso al solicitante	*			
Identificar resultados ineficientes			*	

ACTIVIDADES	METODOLOGÍA			
	DoJ	NIST	ENFSI	EC-COUNCIL
Responder a las preguntas Que, Quien, Cuando, Donde, Como a cada elemento de Datos Relevantes	*			
Explicar que usuarios o aplicaciones crearon, editaron, recibieron o enviaron cada elemento de Datos Relevantes	*			
Justificar la relación que tiene la información con el caso.	*	*		
Producción de la línea de tiempo.	*			
Obtener secuencia de eventos	*		*	
Documentar hallazgos y actividades realizadas.	*	*	*	
Creación de "Lista de Resultados del Análisis".	*			
Reunir y combinar los resultados en un formato claro y sin ambigüedades.			*	
Interpretar los resultados del análisis			*	
Determinar tipo, alcance y propósito de la información			*	
Considerar explicaciones alternas.		*	*	
Considerar a la audiencia.		*		
Considerar información procesable.		*		
Elaborar reporte de resultados del análisis	*	*	*	*
Participar en consultas, previas al juicio			*	
Presentar evidencia oralmente ante tribunales			*	
Identificar problemas que deban solucionarse		*		
Discutir resultados obtenidos.		*		*
Analizar posibles mejoras al procedimiento.		*		*
Contempla recomendaciones para las organizaciones		*		

Figura 7. Cuadro Comparativo de Metodologías de Análisis Forense Digital

Se puede observar una serie de comparaciones entre las metodologías analizadas en líneas atrás y se puede determinar que estas metodologías tienen sus fortalezas y debilidades y que cada una de ellas trabaja en un área en que sobresale por sus fortalezas, pero se puede observar que ninguna de ellas esta adaptada a nuestro contexto de análisis.

Capítulo V

Desarrollo conceptual

5.1 Informática forense

La Informática forense se refiere al análisis y evaluación a fondo de la información que circula en los equipos, plataformas y sistemas de una

organización. Este trabajo no se circunscribe a recuperar información de un equipo de cómputo, sino también al trabajo de inteligencia para evaluar posibles delitos cibernéticos.

La informática forense es una disciplina auxiliar en la búsqueda de información estratégica y en el descubrimiento de evidencia en los sistemas y redes informáticas. El análisis de inteligencia, última fase de la informática forense, debe producir informes concretos y concluyentes. Una vez obtenida la información de la fuente cibernética se le debe dar la interpretación adecuada para obtener las pruebas necesarias para la solución del problema.

En casos judiciales, la información recuperada es inútil a menos que sea admitida en juicio. Es por ello que se requieren expertos forenses para asegurar que la información obtenida es la adecuada y certificar que no ha habido alteraciones en el proceso de recopilación correspondiente.

5.2 Evidencia

Certeza manifiesta y tan perceptible de una cosa que nadie puede racionalmente dudar de ella. Material sensible significativo que ha sido objeto de peritación.

5.3 Evidencia digital

Es un tipo de evidencia física, menos tangible que otras formas de evidencia (DNA, huellas digitales, componentes de computadores).

Es la certeza clara, manifiesta y tan perceptible que nadie puede dudar de ella. Asimismo, es cualquier mensaje de datos almacenados y trasmitidos por medio

de un Sistema de Información que tengan relación con el hecho indebido que comprometa gravemente el sistema y que posteriormente guíe a los investigadores al descubrimiento de los incriminados.

5.3.1 Características

- Puede ser duplicada de manera exacta y copiada tal como si fuese el original.
- Con herramientas adecuadas es relativamente fácil identificar si la evidencia ha sido alterada, comparada con la original.
- Aún si es borrada, es posible, en la mayoría de los casos, recuperar la información.

5.3.2 Fuentes de la evidencia digital

a. Sistemas de computación abiertos

Son aquellos que están compuestos de las llamadas computadoras personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles y los servidores.

b. Sistemas de comunicación

Están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet, grandes fuentes de información y evidencia digital.

c. Sistemas convergentes de computación

Aquellos formados por los teléfonos celulares llamados inteligentes, los sistemas inteligentes y de convergencia digital.

5.3.3 Clasificación de la evidencia digital

La evidencia digital se puede clasificar de la siguiente manera.

- Registros generadores por computador:

Generados como efecto de la programación de un computador, son inalterables por una persona, llamados registros de eventos de seguridad y sirven como prueba tras demostrar el correcto y adecuado funcionamiento del sistema o computador que genero el registro.

- Registros no generados sino simplemente almacenados por o en computadores:

Generados por una persona, y que son almacenados en el computador, por ejemplo, un documento realizado con un procesador de palabras. En estos registros es importante lograr demostrar la identidad del generador, y probar hechos o afirmaciones contenidas en la evidencia misma.

- Registro híbrido que incluyan tanto registros generados por computador como almacenados en los mismos:

Los registros híbridos son aquellos que combinan afirmaciones humanas y los registros llamados de evento de seguridad.

Por lo tanto una evidencia digital:

- Puede ser duplicada de forma exacta y se puede sacar una copia para ser examinada como si fuera la original.

- Mediante herramientas informáticas existentes se puede comparar la evidencia digital con su original, para determinar si ha sido alterada.

- Es muy fácil de eliminar. Aun cuando un registro es borrado del disco duro del computador, y éste ha sido formateado, es posible recuperarlo.

- Cuando los individuos involucrados en un crimen tratan de destruir la evidencia, existen copias que permanecen en otros sitios.

5.3.4 Manipulación de evidencia digital

- Hacer uso de medios forenses estériles (para copias de información)
- Mantener y controlar la integridad del medio original. Esto significa, que a la hora de recolectar la evidencia digital, las acciones realizadas no deben cambiar nunca esta evidencia.
- Cuando se necesario que una persona tenga acceso a evidencia digital forense, esa persona debe ser un profesional forense.
- Las copias de los datos obtenidos, deben estar correctamente marcadas, controladas y preservadas. Y al igual que los resultados de la investigación, deben estar disponibles para su revisión.
- Siempre que la evidencia digital este en poder de algún individuo, este será responsable de todas la acciones tomadas con respecto a ella, mientras este en su poder.
- Las agencias responsables de llevar el proceso de recolección y análisis de la videncia digital, serán quienes deben garantizar el cumplimiento de los principios de criminalística.

UNIVERSITAS MAJOR PACENSIS DIVI ANDREÆ

MARCO LEGAL O INSTITUCIONAL

Capítulo VI

Marco legal o institucional

6.1 Marco legal

No existe una figura jurídica que tipifique este tipo de delitos en nuestro código penal, la figura jurídica de la evidencia digital es una figura que surge gracias a los nuevos delitos informáticos.

En la Nueva Constitución Política del Estado Plurinacional de Bolivia en el artículo 130 perteneciente a la sección III denominada acción de privacidad, establece que toda persona tiene el derecho fundamental de la protección de sus datos así sea que sus datos estén almacenados en cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, así mismo toda persona tiene el derecho a la privacidad de sus datos, porque si cualquier persona alterare este tipo de información estaríamos flagrando el derecho a la intimidad y privacidad de esta persona atentando contra su propia imagen, honra y reputación; por lo tanto el Estado protege de esta manera el derecho fundamental de la protección de sus datos.

La ley 164 que tiene por nombre Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, en el artículo 7, parágrafo IV hace mención a la firma y documentos digitales, pero no se dice nada de la evidencia digital.

En el Código Penal Boliviano no se tiene tipificada la figura de la evidencia digital, esto porque cuando se consideró este tema nuestro código penal no

tomo este tipo de consideraciones que son actuales. Muchos de los delitos informáticos son relacionados con figuras tipificadas en el código Penal, pero ningún delito es propio de los delitos informáticos. Se puede observar que en el capítulo IX del Código Penal tenemos el tratamiento de los delitos informáticos, en donde observamos el Artículo 363 bis cuyo nomen iuris responde a la manipulación informática, también se menciona al Artículo 363 ter cuyo nomen iuris hace mención al tratamiento de la alteración, acceso y uso indebido de datos informáticos; pero en ningún lugar hace mención al tratamiento de la evidencia digital.

En la Ley de servicios financieros, Ley 393 en el artículo 491 cuyo nomen iuris responde al de los delitos financieros, se incorpora en el Título XII del Código Penal, el Capítulo XII relativo a delitos financieros, en el artículo 363 quater en el inciso , en donde se establece: “c) Apropiación Indebida de Fondos Financieros. El que sin autorización y mediante la utilización de medios tecnológicos u otras maniobras fraudulentas, se apoderare o procurare la transferencia de fondos, ya sea para beneficio suyo o de terceros incurrirá en privación de libertad de cinco (5) a diez (10) años y multa de cien (100) a quinientos (500) días”. Se puede observar que no existe una regulación exclusiva para el tratamiento de la evidencia digital.

Por lo tanto nuestra legislación no contempla en ninguna norma una figura normativa en el tema del tratamiento de la evidencia digital.

MARCO INGENIERÍA DE PROTOTIPO

Capítulo VII

Ingeniería de Prototipo

7.1 Descripción y procesamiento de datos recopilados

De acuerdo a los datos recopilados en el caso de estudio planteado en el entorno Linux se tiene lo siguiente:

Partiendo de caso de Kevin Mitnick, considerado el hacker más famoso del mundo es un ejemplo del empleo de la Informática Forense en la investigación digital.

Tras ser detenido en 1995 por el FBI, que lo acusaba de introducirse en los sistemas informáticos de empresas como Motorola Inc., Novell Inc., Nokia Corp. y Sun Microsystems fue condenado a 46 meses de prisión. Para conocer el caso completo, ver el Anexo A. este es un caso claro de la vulneración de la seguridad de los sistemas informáticos, este no es un caso aislado al análisis forense.
Una vez planteado el caso de estudio en el entorno Linux, se tienen los siguientes datos:

7.2 Diseño del prototipo

7.2.1 Modelo propuesto

Este punto presenta el modelo de análisis forense a dispositivos de

almacenamiento de estado sólido, el cual se ha construido con base a los procedimientos operativos estándar y siguiendo las recomendaciones y buenas prácticas emitidas por la NIST, IOCE, ACPO; principalmente de la NIST. Además de presentar las características y componentes que integran el modelo propuesta, se describen como un aspecto importante, los roles del equipo de investigación forense. Finalmente, se describen los riesgos en las diferentes fases del análisis forense, que deben ser administrados de forma adecuada.

El modelo propuesto se basa principalmente en la aplicación del método científico y de las mejores prácticas internacionales.

Mediante la aplicación del método científico se logra la obtención y el estudio de evidencia observable y medible, aplicando el razonamiento lógico y elaborando hipótesis, la cuales podrán ser corregidas y mejoradas según se obtiene más evidencia.

Al aplicar las mejores prácticas recomendadas internacionalmente por la NIST se desarrolla un proceso formal de investigación digital consecuente con las recomendaciones de instituciones internacionales, para el manejo de evidencia digital.

Específicamente, este modelo se ha desarrollado con base en la aplicación de los procedimientos operativos estándar, y considera cuatro de ellos, cada uno de los cuales corresponde a cada una de las etapas del proceso forense.

Características del modelo

Un modelo formal permite a un investigador abordar e investigar un delito

informático de manera racional y rápida, sin una pérdida de minuciosidad. Lo más importante es que a través de el se establece un protocolo mediante el cual la evidencia digital (física y lógica) es reunida y manejada, contribuyendo a minimizar los casos en que la evidencia se contamine o sea alterada a través de garantías de custodia.

Sin un modelo adecuado, será dificultosa la investigación y se dudará de ella, esto desembocara en una investigación poco confiable en un proceso legal.

Cualquier proceso o procedimiento de investigación usado para efectuar el análisis forense debe contemplar las características de una metodología científica.

Los pasos aplicados deben ser racionales, deben ayudar a evitar que se generen resultados inconsistentes o imparciales, mediante la aportación de un marco de trabajo racional dentro del cual las actividades de investigación puedan llevarse a cabo.

La evidencia que se reúne sin un modelo adecuado no será admitida como válida en las cortes. A continuación, se enumeran algunas de las características que presenta la propuesta de investigación:

i. Se basa en el método científico

La propuesta de investigación se basa en el método científico porque es un método de investigación usado principalmente en la producción de conocimiento en las ciencias. Para ser llamado científico, un método de investigación debe basarse en la empírica y en la medición, sujeto a los principios específicos de las pruebas de razonamiento. Método es el significado general de modelo lógico que se sigue en la investigación científica.

ii. Es congruente con lineamentos y metodologías internacionales

Los métodos definidos cumplen con los principios y objetivos, las cuales aseguran la validez, admisibilidad e integridad mientras la evidencia es manejada. De esta manera, el modelo estará construido con base en organizaciones internacionales, especializadas en el área de la ciencia forense digital.

iii. Es de aplicación limitada

Es complicado que un modelo pueda atender o resolver todas las posibles circunstancias que pudieran generarse en un momento determinado. Por lo tanto, el modelo propuesto presenta limitaciones al momento de su aplicación y debe analizarse cada caso de aplicación.

iv. Se define requisitos de las herramientas que deberán usarse

Las herramientas que se utilicen para hacer análisis forense en equipos con discos de estado sólido que sean capaces de recolectar la información contenida en estos dispositivos se deben cumplir con los requisitos señalados en el modelo propuesto. Adicionalmente, deberá existir un equipo de cómputo o computadora, la cual deberá de contar con la capacidad de interactuar entre el dispositivo a ser analizado herramientas forenses especializadas, las mismas deberán desarrollarse en software libre.

v. Se definen líneas de tiempo

Mediante la línea de tiempo es posible identificar la actividad del sistema. En el ámbito de la Informática Forense, existen herramientas que permiten la creación de una línea temporal que se vuelve útil cuando se intenta determinar qué archivos han sido modificados, creados o accedidos recientemente, la línea temporal puede mostrar los directorios donde el

investigador debería centrar su atención y no precisamente sobre cada uno de los cientos o miles de archivos que componen a tal sistema. De esta forma, las líneas de tiempo generadas le permiten al investigador forense obtener rápidamente una perspectiva de alto nivel acerca de la actividad del sistema o usuarios.

vi. Se define la cadena de custodia de los equipos

Esencialmente, este es un medio de justificar: ¿quién ha entrado en contacto con la evidencia?, ¿cuándo entró en contacto? y ¿qué fue lo que hizo con la evidencia? Es una manera de demostrar que la evidencia no ha sido dañada o alterada mientras estuvo al cuidado del investigador. Un fallo en demostrar la cadena de custodia de la evidencia puede conducir a serias cuestiones relativas a la autenticidad e integridad de la evidencia y los análisis que dependen de ella. Un mal manejo en la cadena de custodia puede arruinar el caso.

Un modelo debe incluir generación y ejecución de tareas, la aplicación de técnicas, documentos, informes, etc. Así como la aplicación de herramientas para realizar un análisis forense a equipos.

Alcance

Existen diversas propuestas de metodologías para guiar el proceso forense digital en muchas partes del mundo.

Sin embargo, no se ha llegado a ninguna conclusión sobre cuál es la más apropiada, ninguna de ellas se centra en la información específica que está involucrada en el análisis forense a equipos que tienen dispositivos de almacenamiento de estado sólido.

El modelo propuesto se ha desarrollado para ayudar a los practicantes

forenses y oficiales en la investigación de delitos o incidentes informáticos que involucren tales dispositivos.

Este modelo ha incorporado prácticas y técnicas estándar existentes en el mundode la investigación física y digital. Este modelo intenta superar los principales deficiencias de los modelos digitales forenses existentes discutidos en las secciones anteriores y enfatiza una estrategia sistemática y metódica para una investigación forense digital.

El modelo propuesto esta conformado por: Objetivo, Limitaciones, Requisitos y Etapas Propuestas.

Objetivo

El objetivo del modelo propuesto es establecer un marco de trabajo válido, estándar y aceptado. Se deberán establecer procedimientos que permitan realizar un manejo adecuado de la evidencia digital almacenada en equipos que tengan dispositivos de almacenamiento de estado sólido. Estos procedimientos estarán basados en recomendaciones de las mejores prácticas definidas por distintos organismos internacionales reconocidas en el área de la ciencia forense digital.

Limitaciones

La metodología presenta las siguientes limitaciones:

- El alcance de la metodología está limitada a dispositivos de almacenamiento de estado solido.

- Las condiciones y facilidades que se deben tener sobre los equipos que se deben analizar con este modelo. En general, para que las herramientas forenses puedan ser utilizadas, se requiere un dispositivo de

almacenamiento de estado solido.

Requisitos

Acerca del Personal

El modelo se ha diseñado para que pueda ser comprendida por cualquier profesional que tenga conocimientos fundamentales de la informática y comunicaciones. A continuación los actores y sus roles.

Los primeros actuantes

Es el personal entrenado, el cual es el primero en llegar y atender la escena, proporciona una evaluación inicial. Las responsabilidades son: asegurar la escena del incidente, solicitar el soporte apropiado requerido, y asistir en la tarea de recolección de evidencia.

Los investigadores

Entre sus roles se encuentran planear y administrar la preservación, adquisición, inspección, análisis y reporte de la evidencia digital. Es decir, se encargarán de diseñar estrategias concretas basadas en la metodología.

Los técnicos

Los técnicos son los responsables de identificar y recolectar la evidencia, además deben de documentar la escena del incidente. Ellos son personal entrenado especialmente para asegurar el equipo electrónico, otra de las tareas requeridas es la de adquirir los datos residentes en el dispositivo de estado sólido.

Los examinadores Forenses

Consiste en personal especialmente entrenado, el cual reproduce las imágenes adquiridas del equipo asegurado y recupera los datos digitales. Los Examinadores hacen visible la información almacenada en el dispositivo. Usando equipo altamente especializado, exhaustiva utilización de ingeniería inversa, u otro medio apropiado no disponible al alcance de los Técnicos Forenses.

El analista Forense

Evalúa el producto del Inspector Forense para determinar la significancia y valor probatorio relativo al caso.

Se puede decir que no son todos los actores y que además , los roles podrían se modificado de alguna manera, según se presente el caso de análisis.

Acerca de las Herramientas

Requisitos para la computadora. La cual indica aquellas características o especificaciones deseables para aquel equipo dedicado al análisis forense a equipos que contengan dispositivos de almacenamiento de estado sólido.

Un equipo portátil con puertos USB 2.0 para conectar los cables del teléfono. FireWire para conectar una DVR (Digital video Recorder) a la computadora y capturar datos que no sea de otra forma recuperable.

Etapas del modelo Propuesto

Cada investigación es distinta con su propio y único conjunto de circunstancias, un enfoque de procedimiento definitivo es complicado de

establecer. A pesar de todo, varias propuestas hacen referencia a las mismas áreas, aunque resaltan el grado de importancia en aspectos diferentes.

El modelo aquí propuesto está orientado a ser empleada en aquellos incidentes o delitos en los que se requiera obtener evidencia digital de un equipo con un dispositivo de almacenamiento de estado sólido. El modelo se construyo en base a fases, que permitan incluir la mayor cantidad de puntos a considerar para realizar el proceso de análisis forense a equipos con un dispositivo de almacenamiento de estado sólido y se explican a continuación.

Fase adquisición

Adquisición de medio de almacenamiento persistente

- Bloqueo del medio de almacenamiento (impedir escrituras en el mismo)

- Captura y resguardo de la imagen (copia exacta del contenido del medio de almacenamiento)

- Opcional: compresión y división de la imagen

- Validación de original y copia (verificación de que es copia fiel del original)

Adquisición de medio de almacenamiento volátil

- Captura y resguardo de la imagen (copia de la información volátil que el equipo encendido manipula)

La fase de adquisición comprende etapas que de acuerdo al entorno en el que se deba llevar a cabo la recuperación de la información, aplicará o no

involucrarlas en el proceso.

Esta fase comprende toda actividad vinculada con la generación de una réplica exacta de todo el contenido digital alojado en el dispositivo original.

Fase preparación

Restauración de la Imagen

- Ensamblado de las divisiones de la imagen

- Descompresión de la imagen

- Opcional: Validación de original y copia

Preparación de la Extracción

- Preparación para Extracción Lógica (configuración de lectores de sistemas de archivos)

- Preparación Extracción física (configuración de acceso al contenido en crudo del archivo de imagen)

Identificación

- Identificación de cantidad y tipos de Sistemas Operativos Presentes

- Identificación de cantidad de discos, particiones y tipos de sistemas de archivo presentes

- Identificación de Máquinas virtuales presentes

Preparación de ambiente de trabajo

- Preparación de ambiente de exanimación: de acuerdo a características de lo adquirido.

Como primera etapa, la fase de preparación contempla la restauración de la imagen. Esto significa que si la misma se encontrara dividida, encriptada o comprimida deberá realizarse el proceso contrario, a fin de lograr el original.

A continuación se deberá validar que la restauración ha sido exitosa mediante un algoritmo de hash, como se mencionó previamente.

Si la imagen que se obtuvo es de un sistema de archivos de un determinado sistema operativo, entonces será útil generar una máquina virtual que tome dicha imagen como su disco principal.

Al hacerlo se debería realizar una copia a fin de no alterar la imagen original.

Finalmente esta etapa contempla la identificación de tipos de sistemas de archivos y sistemas operativos contenidos en los medios de almacenamiento originales.

Esta fase involucra todos los procedimientos necesarios para generar el entorno de pruebas preciso para llevar a cabo en primer lugar la inspección, y eventualmente la recuperación de la información.

Fase de análisis

Extracción Lógica

- Recuperación de archivos eliminados

- Extracción de información a examinar por tipo de archivo (determinación de formatos de archivo ignorando la extensión)

- Extracción de metadatos de archivo presentes en el sistema de archivos

- Extracción de metadatos propios del archivo (Lectura de los atributos del archivo contenidos en la propia información del archivo)

- Extracción de archivos protegidos con contraseña

- Extracción de archivos comprimidos

- Extracción de archivos encriptados

- Búsqueda de determinado tipo de archivo oculto (determinar en todo el contenido aquellos tipos de archivos que no se corresponden con su extensión)

- Búsqueda de información en el área de paginado de la memoria virtual

- Búsqueda de Información de Configuración presente en el equipo

- Búsqueda de Información en Procesos en Memoria

Extracción Física

- Búsqueda de palabras en disco

- Extracción de archivos en espacio desalojado no fragmentado. Carving

- Primera Generación.

- Extracción de archivos en espacios desalojados, que puedan estar fragmentados. Carving Segunda generación.

Análisis de Relaciones

- Identificación de relaciones entre conjunto de archivos

- Verificación de aplicaciones instaladas

El objetivo de la fase de análisis en el caso de un proceso judicial o pre-judicial es encontrar la denominada Evidencia Digital, es decir, aquello que relaciona el hecho ocurrido con el "imputado" y la "víctima".

Entonces, se piensa en la evidencia digital como en un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.

La fase de análisis comprende las siguientes etapas:

a) Extracción lógica

b) Extracción física

c) Análisis de relaciones

La extracción lógica representa la recuperación de información eliminada a partir del sistema de archivos. Por esa razón se denomina "lógica", ya que no se accede en forma directa a los bloques, sino a través del Sistema de Archivos, y del Sistema Operativo como intermediario.

La extracción física, en cambio, va directo al dispositivo, eludiendo el Sistema Operativo. La mayoría de los sistemas operativos no eliminan la

información en el momento en el que un Usuario solicita el borrado de un archivo determinado, sino que, de alguna manera, dejan registrado el espacio que ocupaba dicho archivo ahora.

De esta manera, si fuese posible hallar tal espacio entonces sería posible reconstruir la información original.

La etapa de análisis de relaciones trata justamente de identificar relaciones entre conjuntos de archivos, con el fin de obtener una conclusión.

Esto involucra puntualmente la Identificación de relaciones entre conjunto de archivos vinculados a una actividad en particular. Esta fase comprende el fuerte del trabajo en donde se analiza el contenido adquirido en busca de vestigios de lo que se quiere hallar.

Fase de presentación

Armado del Informe detallando el modelo utilizado y asegurando trazabilidad y reproducción

Preparación de la información a presentar / entregar

Administración de los aspectos carentes detectados en el proceso planteado

En el proceso detallado en la sección anterior se detectaron áreas carentes de técnicas y/o herramientas que se detallarán a continuación, a fin de proponer la administración de los riesgos en las fases del modelo propuesto.

Carencias en Fase de Preparación

- Identificar máquinas virtuales presentes en el equipo

Hoy en día la utilización de máquinas virtuales es una actividad que no solo está ampliamente difundida sino que ya es una herramienta en muchas plataformas empresariales. Potencialmente cada maquina virtual simula un equipo real con toda su complejidad, lo que permite que la información pueda ocultarse o perderse aún dentro de ellas. Esto implica que, cada máquina virtual hallada dentro del equipo físico a analizar, debería tratarse como un equipo por separado.

Así, la problemática inicial que existe es verificar la existencia de maquinas virtuales en el equipo original.

Durante la investigación, no se halló una herramienta que permitiera efectuar tal operación [11].

Carencias en Fase de Extracción – Etapa Extracción Lógica

* Extracción de archivos encriptados

Otro de los aspectos es la extracción de archivos encriptados, el primer paso es la determinación del tipo de archivo que se encuentra encriptado, , esto es, si existe o no la posibilidad de existencia de una evidencia en dicho archivo, en base al objetivo buscado.

En un siguiente paso se debe requerir del software o algoritmo que nos permita acceder a la clave de seguridad para acceder a los datos buscados.

Por el momento no se ha encontrado la herramienta que nos permita llevar a cabo estas tareas.

Carencias en Fase de Extracción – Etapa Extracción Física

En la actualidad no existe una herramienta, ya sea comercial o libre, que implemente la técnica de Semantic Carving, solamente se encuentra disponible un prototipo experimental llamado S2, desarrollado por Simson Garfinkel para el DFRWS 2006 [13].

S2 es un Carver semántico escrito en C++ que utiliza una serie de estrategias para reducir el S2 es un Carver semántico escrito en C++ que utiliza una serie de estrategias para reducir el número de secuencias que se necesitan testear.

El Smart Carving es un nicho carente desde el punto de vista que lo poco que hay, está solo orientado a recuperación de fotos.

Uno de los aspectos carentes que vincula la extracción física de la información, es la validación de los archivos devueltos por las herramientas de recuperación de archivos eliminados en el dispositivo de almacenamiento de estado sólido.

Para llegar a administrar este riesgo analizaremos el algoritmo que hace posible la recuperación de datos en el dispositivo de almacenamiento.

En el año 2007 Garfinkel[12] propuso una nueva técnica de file Carving que incluía la utilización de validadores de archivos como parte integral del proceso de recuperación. Junto con la técnica de Carving, Garfinkel propuso también un framework de validación de archivos, y es ésta la propuesta la que se tomó como base para la realización del prototipo de herramienta.

Si un archivo no logra pasar una etapa de validación, se lo descarta como archivo inválido y no se prosigue con las siguientes etapas. Esto se realiza para maximizar la velocidad de procesamiento de los archivos, realizando primero las validaciones más básicas y rápidas de realizar, sus etapas son

[14]:

1. Validación por medio de header y footer.

2. Validación de consistencia de punteros internos del archivo.

3. Validación por medio de descompresión.

4. Validación semántica.

5. Validación humana.

Se busca reproducir la validación, permitiendo que se utilice como parte integral los algoritmos de Carving, o que se pueda utilizar en forma independiente para validar archivos ya recuperados.

Por lo tanto la fase más crítica es la etapa de análisis, en esta etapa se tiene la fragilidad en la extracción física de los datos; porque se debe realizar: la búsqueda de palabras en disco, la extracción de archivos en espacio desalojado no fragmentado. Carving Primera Generación, la extracción de archivos en espacios desalojados, que puedan estar fragmentados. Carving Segunda generación.

El File Carving es el proceso de extracción de archivos u objetos del disco en ausencia de metadatos del sistema de archivo, es decir, accediendo directamente al contenido de los bloques [1]. El proceso de file carving se basa en recuperar información que ha sido eliminada o es inaccesible debido a daños del dispositivo o del sistema de archivos. Su uso es vital en la Informática Forense, ya sea para recuperar archivos eliminados que puedan ser utilizados como prueba, como para recuperar información comercial o personal valiosa [2].

Existen varias técnicas de File Carving, algunas implementadas en herramientas, y otras ún no.

Estas técnicas varían desde las más básicas, basadas en la lectura del header y footer de un archivo, hasta otras mucho más complejas como Bifragment Gap (Garfinkel), Smart Carving (Pal, Memon etal) o Semantic Carving (Garfinkel). Incluso algunas tienen varios enfoques, como por ejemplo Header/Footer carving que puede aplicarse en una sola o en múltiples pasadas.

El proceso de File Carving ha ido evolucionando en los últimos años, sin embargo no cuenta áun con una definición flexible, adaptable e integradora, que permita describir y utilizar las técnicas que mejor se adapten a cada estructura de archivos [15].

Por otro lado, los File Carvers actuales (herramientas que implementan file carving) presentan varias limitaciones. Las herramientas más populares suelen presentar resultados incompletos, una tasa muy alta de falsos positivos y recuperar archivos dañados o no válidos. También ocurre que aquellas herramientas con muy buena performance recuperan grandes cantidades de archivos y muchos de ellos inválidos, lo que dificulta el acceso a los resultados de interés.

Como parte del desarrollo de soluciones que implementen file Carving, soluciones desarrolladas en el entorno libre implementan dos soluciones de preprocesamiento, cuatro algoritmos de file Carving, dos soluciones de postprocesamiento y un logger de extracción, junto con otros objetos asociados los mismos que son necesarios para mantener un equilibro entre el nivel de abstracción deseado en cada parte y el rendimiento del producto.

Es cierto que en el mercado se tienen soluciones comerciales como es el caso del Encase, las soluciones desarrolladas en software libre son las que

se utilizan con cierta frecuencia en el análisis y recuperación de datos en dispositivos de almacenamiento de estado sólido, tal es el caso de Kali, una herramienta desarrollada en software libre que ayuda de gran manera en el campo de la informática forense.

Es destacable que, si bien se mantuvo un alto grado de abstracción que permite la fácil implementación de algoritmos de Carving y componentes de pre y postprocesamiento, las herramientas mencionadas en líneas anteriores utilizan file Carving en la recuperación de datos e información de diferentes dispositivos de almacenamiento.

En la actualidad se viene desarrollando CIRA que es un framework que integra el preprocesamiento, Carving y el postprocesamiento; esta herramienta tiene la finalidad de recuperar datos de dispositivos de almacenamiento, pero no se ha concluido aún con el desarrollo de este framework.

CIRA en el preprocesamiento realiza la exclusión y extracción de bloques de análisis. Uno de los preprocesadores permite que se excluyan bloques arbitrarios, definidos como una cadena de texto y genera un archivo con los rangos que se desean excluir. El otro preprocesador realiza un análisis estadístico de los bloques disponibles y decide, en base a la media aritmética y la entropía, si los bloques deben excluirse del análisis. Esta técnica facilita, por ejemplo, la selección de bloques que contienen datos binarios, excluyendo los datos ASCII usualmente asociados con archivos de texto [16].

Este preprocesador se encuentra en una fase de experimentación y ajuste, que está planeado realizar como parte del trabajo futuro.

Con respecto a los algoritmos de Carving, se implementaron variantes de header/footer Carving y se realizó una implementación de Carving basado

en la estructura interna de archivos este desarrollo se lo puede observar en distintas herramientas utilizadas en informática forense.

Los algoritmos de header footer carving implementados fueron denominados Single Format Carve, Multiple Format Carve y Maximum Length Carve en el desarrollo del framework CIRA, quien poseía variantes de header footer carving, es decir que generaban los archivos desde la ocurrencia de un encabezado de archivo hasta la ocurrencia de una cadena, el footer, que delimita el fin de un archivo.

En el orden que fueron presentados, puede considerarse como la evolución de la variante más simple de la técnica de header footer carving hacia su versión más compleja.

Con respecto al algoritmo de Carving basado en la estructura interna de los archivos, durante el trabajo con los validadores de archivo se descubrió que al comenzar el análisis de validez de archivo de un determinado en posiciones arbitrarias de la imagen de disco, era posible encontrar y extraer archivos JPG que resultaban problemáticos para el algoritmo de Single Format Carve, sobre el que se estaba trabajando en ese momento. Esta experiencia se tomó como base para la implementación de un Carver que combina una parte del funcionamiento de Multiple Format Carve y utiliza el Framework de Validación para llevar a cabo la extracción de archivos válidos luego de analizar su estructura. Pese a que su funcionamiento presenta ventajas con respecto a las técnicas de header/footer, aún pueden implementarse mejoras, tanto los validadores como el Carver de estructura interna.

La etapa de postprocesamiento desarrollo dos postprocesadores, uno que realiza la verificación de los archivos extraídos por medio del framework de validación, y otro que calcula los hashes MD5 y SHA-1 de los archivos extraídos, que suelen utilizarse para verificar su integridad respecto a otras

versiones del mismo archivo disponible.

CIRA continúa en desarrollo y prevee implementar otros algoritmos de Carving, continuar la optimización de los módulos actuales y construir nuevos módulos de pre y posprocesamiento.

Como se puede observar File Carving es una de las técnicas más utilizadas en la recuperación de archivos, en la informática forense.

Por lo tanto para minimizar este riesgo se deben implementar los algoritmos de File Carving en la recuperación de datos e información, afortunadamente la mayoría de las herramientas desarrolladas en software libre utilizan los algoritmos de File Carving, uno de estas herramientas es Kali.

Es cierto que los aspectos carentes detectados constituyen un conjunto de necesidades con potencialidad de ser resueltas y que mediante una adecuada administración de los riesgos detectados se beneficiara a la sociedad en general, y a las ciencias forenses en particular.

3.3 Arquitectura tecnológica

Para el diseño del prototipo emplearemos herramientas basadas en software libre, estas se pueden observar en el Anexo B.

El diseño del prototipo cuenta con el apoyo en la extracción lógica de datos, de Kali Linux, esta es una plataforma robusta que contribuirá de forma eficiente en la extracción de datos de dispositivos de almacenamiento.

En el Anexo B se detalla el proceso de extracción lógica de datos utilizando Kali Linux.

La propuesta va conforme con los procedimientos descritos en líneas atrás, se debe recalcar que Kali Linux utiliza File Carving en la recolección de datos y el clonado de los dispositivos de almacenamiento.

3.4 Interpretación de Resultados

De acuerdo al modelo planteado en el presente trabajo de investigación se puede interpretar lo siguiente:

El modelo tendría un impacto transcendental en el tratamiento de la evidencia digital si es que el contexto jurídico del país sería consecuente con el tratamiento de la evidencia digital, pero es un modelo que tiende a flexibilizarse en la aplicación del mismo en el contexto.

El análisis crítico en la extracción lógica de los datos es un hecho que no debe pasar de largo y es en lo que la tesis puntualiza como un punto débil de muchas metodologías, es por esa razón que el trabajo de investigación analiza la herramienta que se va a a emplear en la extracción lógica de los datos del dispositivo de almacenamiento, se propone utilizar software libre, específicamente Kali como sistema operativo de análisis forense, debido a que de acuerdo a las pruebas realizadas sobre un dispositivo de estado sólido se pudo evidenciar su versatilidad, claro que se comparó este análisis con respecto al software privativo Autopsy y se detectó que Kali logró recuperar de forma íntegra y versátil la información almacenada en el dispositivo de estado sólido, las pruebas respectivas se las puede observar en el Apéndice B; esto se debe al algoritmo de recuperación de datos que emplea Kali, este es el Scalpel perteneciente o cooperante del modelo planteado por File Carving en el análisis del Header y el Footer; esto hace que la recuperación de Kali, en cuanto a archivos se refiere, es uno de los sistemas operativos más utilizados en el mundo de la informática forense, el algoritmo Scalpel se lo detalla en el Anexo C.

Por lo tanto de acuerdo al análisis de los resultados comparativos entre el software libre y el software privativo, encontramos que por la característica cooperativa en el enfoque de desarrollo, el software libre es el que le lleva la delantera al software privativo.

Otro de los aspectos que nos ayuda a tomar esta conclusión en el análisis de los resultados es el que nos brinda el análisis estadístico de los instrumentos de recopilación de datos, en ellos se puede observar que de acuerdo a las entrevistas y cuestionarios realizadas a: Ingenieros encargados de soporte técnico, usuarios especialistas del software forense, usuarios que tienen relación con la recogida de evidencia digital; entrevistas y cuestionarios detallados en el Anexo D, Anexo E se puede interpretar lo siguiente:

De la entrevista propuesta se puede establecer que en el Estado Plurinacional de Bolivia no tiene un modelo para realizar el análisis en el proceso de recolección de la evidencia digital en software libre. Los especialistas entrevistados recalcaron la importancia de adoptar recomendaciones internacionales y contextualizarlas en nuestro medio.

Se pudo evidenciar que de acuerdo a la experiencia de estos especialistas, el mayor problema se da en la copia de los datos del dispositivo en custodia a otro que los mismos le denominan clon, en la mayoría de los casos estos especialistas utilizan hardware para realizar esta tarea, pero encontramos que a medida que los dispositivos se actualizan, cambian y esto representa una mayor inversión y una pronta desactualización del hardware que utilizan los forenses.

Esta es una de las razones por las cuales se debe plantear un modelo que sea robusto en la extracción de datos, la consistencia se la debe dar en el algoritmo de extracción que se utilice, es por esta razón que se utiliza el

algoritmo de análisis denominado File Carving en el análisis del Header y el Footer [19], el mismo tiene como núcleo central el algoritmo Scalpel [20] y el de Boyer Moore [18] el mismo se lo detalla en el Anexo C

Capítulo IV

Marco de Resultados

4.1 Estado de los Objetivos

Objetivo general

Se logró alcanzar el objetivo general, considerando las recomendaciones de NIST (National Institute of Standars and Technology) y los trabajos realizados en el área de la informática forense, se propuso un modelo para realizar el análisis en el proceso de recolección de la evidencia digital en software libre, de modo que se realizó un análisis de la gestión de riesgos en la recuperación de la información digital y de esta forma se puedo establecer informes claros en contra de acciones antijurídicas, de tal forma que mediante el procedimiento planteado en el modelo propuesto se puede establecer que la información analizada no presente contaminación en el análisis lógico de los datos recopilados del dispositivo de almacenamiento en custodia.

Objetivos específicos

- Se propuso un caso de estudio en el análisis forense de un sistema GNU / Linux en donde se llevó a cabo el proceso unificado de recolección de información digital para el análisis y la gestión de riesgos en el tratamiento de la evidencia digital.

- Se analizó las recomendaciones de la NIST en el caso de incidentes en la

recuperación de información digital para el tratamiento de la evidencia digital en el entorno del software libre.

- Se estudiaron metodologías en la gestión de riesgos en la seguridad de la información para el análisis de riesgos en el tratamiento de la evidencia digital en el entorno del software libre.

- Se estudiar paso a paso el análisis y la gestión de los riesgos del modelo propuesto, en el tratamiento de evidencia digital en el entorno del software libre.

- Se realizó una estadística de metodologías que utilicen software libre en el tratamiento de evidencia digital para la gestión de riesgos en el tratamiento de la evidencia digital.

4.2 Estado de la Hipótesis

En una investigación exploratoria no se establece una hipótesis, lo que se puede elaborar es una conjetura inicial; esta conjetura esta relacionada con el análisis y la gestión de riesgos en el tratamiento de la evidencia digital debe tratarse con un modelo razonable para que no fracture los procesos unificados en la recuperación de información digital, de modo que la evidencia digital es válida si se cumple con un modelo que cumpla con condiciones determinadas por recomendaciones internacionales; cumpliendo con este modelo la evidencia digital es considerada como un medio probatorio en un juicio. Tomando estas consideraciones se puede establecer que el presente trabajo de investigación logro construir el modelo en base al análisis de los aspectos carentes de los procesos unificados en el tratamiento de la evidencia digital.

4.3 Conclusiones y Recomendaciones

La práctica de la Informática Forense difiere de otras disciplinas forenses en las metodologías y herramientas que utiliza, las mismas difieren con el tiempo, la evolución del hardware y el software que es abrumadoramente rápida, así como las técnicas que utilizan los delincuentes para ejecutar sus actividades delictivas. Para quien decide embarcarse en esta carrera es importante destacar el valor de estar preparado para el cambio.

Las herramientas que se utilizan en Informática Forense son muy variadas, tienen diferentes formas y tamaños, grandes, costosas, con varias características comerciales, gratuitas, tareas complicadas, sencillas. Pero al final un buen forense debe saber que herramienta necesita para el caso específico e interpretar adecuadamente los resultados que esta herramienta arroja.

Otra de las prioridades del informático forense es que debe familiarizarse con las herramientas cada vez que sea posible antes de que la investigación lo requiera, con esto gana tiempo valioso para la investigación.

Se presentó y describió una herramienta, que permitirá realizar el análisis de la evidencia digital, sobre el material objeto de estudio, la misma se desarrolla en el entorno del Software Libre, ella posee un algoritmo confiable en el análisis de datos de la evidencia digital.

Este trabajo desde un inicio pretendió ser un apoyo y guía para quienes en un futuro desarrollen actividades sobre la Informática Forense en un determinado siniestro informático.

La investigación exploratoria terminó cuando, a partir de los datos recolectados, ha sido posible crear un marco teórico y epistemológico lo suficientemente fuerte como para determinar qué factores son relevantes al

problema encontrado en la investigación y por lo tanto se cumplió con la construcción del marco teórico y epistemológico.

En ciertas ocasiones los diseños preexperimentales pueden servir como estudios exploratorios, pero sus resultados deben observarse con precaución.

Con respecto al objetivo general, se debe realizar un estudio más detallado en el análisis de los algoritmos de recuperación de datos, en el caso de los dispositivos de almacenamiento puestos en custodia.

El desarrollo de este trabajo sin duda me ha permitido adquirir una mejor percepción de la seguridad, no solo a nivel empresarial sino también personal, porque hoy en día nadie está exento de un crimen donde esté involucrado un ente informático.

Con respecto a los objetivos específicos, se debe prestar más atención en la proposición de modelos de análisis forense en nuestro medio y más que todo se debe acompañar el proceso con el diseño de procesos concretos en la extracción de datos lógicos; se debe concluir que se alcanzó cada uno de los objetivos específicos, desarrollándose como capítulos en la presente investigación.

Se concluye que la mejor forma de evitar situaciones o actos delictivos informáticos es estableciendo controles, pero la mejor forma de defenderse es promover una cultura de seguridad en los hogares y organizaciones, para ello es necesario aplicar un modelo adecuado para tratar de forma correcta estos incidentes informáticos.

Esto se consigue con una capacitación constante para fomentar y mejorar el uso de herramientas forenses, esto incluye traer expertos de otros países en donde estas técnicas son de uso general y su nivel de experiencia es mas

óptimo; a través de esta experiencia se plantea en la investigación un modelo que recopila estas experiencias, siguiendo recomendaciones internacionales.

La presente investigación se apoya en esta premisa, porque en las entrevistas formuladas a expertos internacionales, se pudo evidenciar que los problemas son similares y la manera de resolverlos es de la misma forma similar; los expertos sugieren atacar el problema siguiendo un modelo, esto nos permitiría seguir una forma ordenada en la resolución de los casos forenses; además como somos un país que está dispuesto a recoger experiencias internacionales y extraer de las mismas los aspectos positivos y aprender de los errores; los expertos recomiendan ser muy cautelosos con la extracción de la evidencia digital porque en cualquier momento esta puede ser contaminada, además de dominar la herramienta a utilizar para este propósito, así sea software o hardware.

Con las recomendaciones sugeridas en el modelo propuesto, se considera que los profesionales en la actualidad, tienen los conocimientos necesarios para enfrentarse ante un caso forense, además los mismos han desarrollado habilidades que permiten encontrar evidencia digital en un caso delictivo, empleando herramientas y técnicas básicas de ingeniería inversa.

En cuanto a las recomendaciones, que fueron recolectadas tanto de las entrevistas, en los cuestionarios y en la publicación de la investigación; las mismas puntualizan la importancia de tener un modelo de investigación forense, que asegure la integridad de la evidencia digital extraída y del acompañamiento, que este modelo debe tener, debe contar con la participación de las instituciones pertinentes en el tratamiento de incidentes informáticos, esto se centra en la capacitación de una entidad pertinente y que la misma cuente con el personal adecuado, el mismo debe aplicar el modelo propuesto, debiéndose conservar de forma segura la evidencia digital extraída de la escena en custodia.

Finalmente este trabajo pretende contribuir con la difusión y uso de la Informática Forense desde el enfoque del Software Libre en nuestro país y su aplicación en los distintos entes de justicia como apoyo en la resolución de casos, a través de un modelo que recolecte de forma adecuada la evidencia digital, utilizando Software Libre para este propósito. La investigación se apoya en el Software Libre porque los algoritmos desarrollados para la recolección de la evidencia digital son algoritmos robustos que mediante la aplicación correcta de un procedimiento establecido en el modelo propuesto pueden dar como resultado una evidencia confiable, la cual pueda utilizarse en un juicio, como medio probatorio de un hecho antijurídico.

Bibliografía

[1] CONSTANZO, Bruno; WAIMANN, Julián El estado actual de las Técnicas de File Carving y la necesidad de Nuevas Tecnologías que implementen Carving Inteligente. Journal CADI (2012)
[2] BREZINSKI, D. y KILLALEA, T. (2002) RFC 3227: Guidelines for Evidence Collection and Archiving. Network Working Group. February. Disponible: http://www.normes-internet.com, accedido el 4 de Julio de 2011
[3] ACPO (Association of Chief Police Officers) – England, Wales and North Ireland. Good Practice Guide for Computer-Based Electronic Evidence. Oficial release version. Disponible en www.acpo.police.uk, accedido el 3 de Abril de 2013
[4] A guide to basic computer forensics – TechNet Magazine, Marzo de 2008. Disponible en www.technet.microsoft.com/en-us/magazine/2007.12.forensics.aspx , accedido el 11 de Abril de 2013
[5] Law Enforcement Investigations - Active Army, Army National Guard, and US Army Reserve. FM 3- 19.13. Disponible en www.armystudyguide.com, accedido el 4 de Abril de 2013
[6] María Daniela Álvarez Galarza, "METODOLOGÍAS, ESTRATEGIAS Y HERRAMIENTAS DE LA INFORMÁTICA FORENSE APLICABLES PARA LA DIRECCIÓN NACIONAL DE COMUNICACIÓN Y CRIMINALÍSTICA DE LA POLICÍA NACIONAL". Ecuador. Disponible en www.dspace.ups.edu.ec/bitstream/123456789/546/5/CAPITULO4.pdf, accedido el 4 de Julio de 2011
[7] Forensic Examination of digital Evidence: A Guide for law enforcement, NIJ Report, US Department of Justice, Office of Justice Programs, disponible en http :// www. ojp. usdoj. gov / nij
[8] Survey of Disk Image Storage Formats Version 1.0, Common Digital Evidence Storage Format Working Group, Digital Forensic Research WorkShop, 2006. disponible en www. dfrws. org / CDESF / survey - dfrws - cdesf - diskimg -01. pdf
[9] Mesfer Al-Hajri et al, "An overview of mobile embedded memory and forensics methodology" , disponible en http://ro.ecu.edu.au/ecuworks/1223/ accedido el 10 de Abril de 2012
[10] Bolivia, Órgano Ejecutivo del nivel central del Estado, 2013, Ley de servicios financieros, 5 de agosto de 2013, página 143.
[11] http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/430/Trabajo, Determinación de aspectos carentes en un Proceso Unificado de Recuperación de Información digital, Ana Haydée Di Iorio, Rita Evelina Sansevero, Martín Castellote, Ariel Podestá, Fernando Greco, Bruno Constanzo, Julián Waimann, pg 6.
[12] "Carving contiguos and fragmented files with fast object validation", Garfinkel, S., DFRWS 2007, 2007 accedido el 1 de Septiembre de 2012

[13] http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/430/Trabajo, Determinación de aspectos carentes en un Proceso Unificado de Recuperación de Información digital, Ana Haydée Di Iorio, Rita Evelina Sansevero, Martín Castellote, Ariel Podestá, Fernando Greco, Bruno Constanzo, Julián Waimann, pg 6.
[14] http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/430/Trabajo, Determinación de aspectos carentes en un Proceso Unificado de Recuperación de Información digital, Ana Haydée Di Iorio, Rita Evelina Sansevero, Martín Castellote, Ariel Podestá, Fernando Greco, Bruno Constanzo, Julián Waimann, pg 6.
[15] http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/1,Un framework de file Carving como solución a una necesidad detectada en la generación de un PURI - Proceso Unificado de Recuperación de Información, Ana Haydée Di Iorio1, Martín Castellote2, Ariel Podestá3, Fernando Greco4, Bruno Constanzo5, Julián Waimann6, pg 6)
[16] http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/, Un framework de file Carving como solución a una necesidad detectada en la generación de un PURI – Proceso Unificado de Recuperación de Información, Ana Haydée Di Iorio1, Martín Castellote2, Ariel Podestá3, Fernando Greco4, Bruno Constanzo5, Julián Waimann6,pg 7
[18] R.S. Boyer, J.S. Moore: A Fast String Searching Algorithm. Communications of the ACM, 20, 10, 762-772 (1977)
[19] D.M. Sunday: A Very Fast Substring Search Algorithm. Communications of the ACM, 33, 8, 132-142 (1990)
[20] R.N. Horspool: Practical Fast Searching in Strings. Software - Practice and Experience 10, 501-506 (1980)
[21]. Ray, Daniel A. y Bradford, Phillip G. Models of Models: Digital Forensics and Domain-Specific Languages.
[23]. The Enhanced Digital Investigation Process Model; Venansius Baryamureeba and Florence Tushabe; Agosto 2004.
[24] MEROLA A.: Data Carving Concepts, SANS Institute (2008)
[25] http://digitalforensicssolutions.com/papers/android-memory-analysis-DI.pdf accedido el 12 de Septiembre de 2012
[26] http://digitalforensicssolutions.com/Android_Mind_Reading.pdf accedido el 1 de Septiembre de 2012
[27]. Köhn Michael, Eloff J.H.P., Olivier MS; UML Modelling of Digital Forensic Process Models; Information and Computer Security Architectures.
[28]. www.enfsi.org, consultada el 16 de Junio de 2009.
[29] “Carving contiguos and fragmented files with fast object validation”, Garfinkel, S., DFRWS 2007, 2007 accedido el 1 de Septiembre de 2012
[30] Bill, N.2009. Computer forensic investigations as a profession [en línea] Boston, United States, Cengage Learnig. <http://books.google.es/books?, [consulta: 19 julio 2014]
[31] Elaboración propia y Rodrigues M., Francisca. 2010. Historia de la informática forense [en línea]

<http://www.ehowenespanol.com/historia-informatica-forense-sobre_102525/>[consulta: 18 julio 2014]
[32] ISO/IEC 27037. 2012. Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence. [en linea]<http://www.iso.org/iso/catalogue_detail?csnumber=44381>[consulta: 27 julio 2014]
[33] NIST. 2012. Digital evidence. [en línea]<http://www.nist.gov/oles/forensics/digital_evidence.cfm>[consulta: 26 julio 2014]
[34] Congreso argentino de ingeniería forense. 2014. La necesidad de adopción de un Proceso Unificado de Recuperación de Información: "PURI - Una propuesta"[en línea]<http://www.copitec.org.ar/comunicados/CAIF2014/PURIUFASTA-DiIorio.pdf> [consulta: 9 julio 2014]
[35] Di Iorio, A. 2014. La recuperación de la información y la informática forense: Una propuesta de proceso unificado [en línea], http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/, [consulta: 4 julio 2014]
[36] Fuente: Monje A. Carlos. 2011. Metodología de la investigación cuantitativa cualitativa guía didáctica. [en línea]. http://carmonje.wikispaces.com/file/view/Monje

Anexos

Anexo A

Kevin Mitnick, el hacker más famoso del mundo

Anexo B

Herramientas de investigación forense basadas en Software Libre

Anexo C

Scalpel, Boyer Moore

Anexo D

Entrevistas

Anexo E

Cuestionario