UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ESTUDIO E IMPLEMENTACIÓN DE METODOLOGÍAS DE ANÁLISIS FORENSE DIGITAL APLICABLES EN UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

PROYECTO DE TITULACIÓN

Previa a la obtención del Título de:

INGENIERO EN NETWORKING Y TELECOMUNICACIONES

AUTOR:

JOHN STEVEN LARREA RONQUILLO

TUTOR:

ING. JORGE CHICALA ARROYAVE, M.SC.

GUAYAQUIL – ECUADOR
2016

Presidencia de la República del Ecuador — Plan Nacional de Ciencia, Tecnología, Innovación y Saberes — SENESCYT Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación		
REPOSITORIO NACIONAL EN CIENCIAS Y TECNOLOGÍA		
FICHA DE REGISTRO DE TESIS		
TÍTULO "ESTUDIO E IMPLEMENTACIÓN DE METODOLOGÍAS DE ANÁLISIS FORENSE DIGITAL APLICABLES EN UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES"		
	REVISORES:	
INSTITUCIÓN: Universidad de Guayaquil	**FACULTAD:** Ciencias Matemáticas y Físicas	
CARRERA: Ingeniería en Networking y Telecomunicaciones		
FECHA DE PUBLICACIÓN:	**N° DE PÁGS.:** 81	
ÁREA TEMÁTICA: Investigación Científica		
PALABRAS CLAVES: Metodologías, Análisis Forense, laboratorio, Informática Forense.		
RESUMEN: Este proyecto tiene como objetivo definir metodologías de trabajo en una propuesta de Laboratorio de Informática Forense que tendrá lugar en las instalaciones de la Carrera de Ingeniería en Networking y Telecomunicaciones.		
N° DE REGISTRO(en base de datos):	**N° DE CLASIFICACIÓN:** **Nº**	
DIRECCIÓN URL (tesis en la web):		
ADJUNTO PDF	[X] **SI**	[ ] **NO**
CONTACTO CON AUTOR: John Steven Larrea Ronquillo	**Teléfono:** 0982769494	**E-mail:** john.larrear@ug.edu.ec
CONTACTO DE LA INSTITUCIÓN: Universidad de Guayaquil, Facultad de Ciencias Matemáticas y Físicas, Carrera de Ingeniería en Networking y Telecomunicaciones Victor Manuel Rendón 434 entre Baquerizo Moreno y Córdova www.ug.edu.ec	**Nombre:** Ing. Harry Luna, M.Sc.	

CARTA DE APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, "ESTUDIO E IMPLEMENTACIÓN DE METODOLOGÍAS DE ANÁLISIS FORENSE DIGITAL APLICABLES EN UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES" elaborado por el Sr. LARREA RONQUILLO JOHN STEVEN alumno no titulado de la Carrera de Ingeniería en Networking y Telecomunicaciones de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Networking y Telecomunicaciones, me permito declarar que luego de haber orientado, estudiado y revisado, la Apruebo en todas sus partes.

Atentamente

Ing. JORGE CHICALA ARROYAVE, M.SC.

TUTOR

DEDICATORIA

Dedico este proyecto a mi madre Brenda Ronquillo Vélez, a mi hermana Dámaris Larrea y a mi novia Madeline Antón quienes han sido parte fundamental de mi vida y por quienes siento un profundo afecto; ellas me han enseñado valores, me han ayudado a ser una mejor persona y a tomar las mejores decisiones.

AGRADECIMIENTO

Agradezco a Dios por darme la vida, por darme fuerzas para salir adelante y por guiarme en cada paso que doy.

A mi familia por apoyarme en toda decisión y proyecto que emprendo, dándome ánimos para mejorar continuamente y superar cualquier desafío que se presente.

A la Universidad de Guayaquil, los docentes que forman parte de ella y en especial a mi tutor, el Ing. Jorge Chicala, quien confió en mí para ser parte de su proyecto.

TRIBUNAL PROYECTO DE TITULACIÓN

Ing. Eduardo Santos Baquerizo, M.Sc.
DECANO DE LA FACULTAD
CIENCIAS MATEMÁTICAS Y
FÍSICAS

Ing. Harry Luna Aveiga, M.Sc.
DIRECTOR
CINT

LSi. Óscar Apolinario Arzube, M.Sc.
PROFESOR REVISOR DEL ÁREA -
TRIBUNAL

Lcda. Viviana Pinos Medrano, M.Sc.
PROFESOR REVISOR DEL ÁREA -
TRIBUNAL

Ing. Jorge Chicala Arroyave, M.Sc.
PROFESOR DIRECTOR DEL PROYECTO
DE TITULACIÓN

Ab. Juan Chávez A.
SECRETARIO

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Proyecto de Titulación, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la UNIVERSIDAD DE GUAYAQUIL"

JOHN STEVEN LARREA RONQUILLO

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

"ESTUDIO E IMPLEMENTACIÓN DE METODOLOGÍAS DE ANÁLISIS FORENSE DIGITAL APLICABLES EN UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES"

Proyecto de Titulación que se presenta como requisito para optar por el título de

INGENIERO EN NETWORKING Y TELECOMUNICACIONES

Autor: LARREA RONQUILLO JOHN STEVEN
C.I. 0930626700

Tutor: ING. JORGE CHICALA ARROYAVE, M.SC.

Guayaquil, diciembre del 2016

CERTIFICADO DE ACEPTACIÓN DEL TUTOR

En mi calidad de Tutor del proyecto de titulación, nombrado por el Consejo Directivo de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil.

CERTIFICO:

Que he analizado el Proyecto de Titulación presentado por el estudiante LARREA RONQUILLO JOHN STEVEN, como requisito previo para optar por el título de Ingeniero en Networking y Telecomunicaciones cuyo tema es:

"ESTUDIO E IMPLEMENTACIÓN DE METODOLOGÍAS DE ANÁLISIS FORENSE DIGITAL APLICABLES EN UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES"

Considero aprobado el trabajo en su totalidad.

Presentado por:

Larrea Ronquillo John Steven	093062670-0
Apellidos y Nombres Completos	**Cédula de ciudadanía N°**

Tutor: Ing. Jorge Chicala Arroyave, M.Sc.

Guayaquil, diciembre del 2016

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES
Autorización para Publicación de Proyecto de Titulación en Formato Digital

1. Identificación del Proyecto de Titulación

Nombre del Alumno: Larrea Ronquillo John Steven	
Dirección: Bolivia 3328 y la 15ava	
Teléfono:0982769494	**E-mail:** john.larrear@ug.edu.ec

Facultad: Ciencias Matemáticas y Físicas
Carrera: Ingeniería en Networking y Telecomunicaciones
Título al que opta: Ingeniero en Networking y Telecomunicaciones
Profesor guía: Ing. Jorge Chicala Arroyave, M.Sc.

Título del Proyecto de Titulación: Estudio e implementación de metodologías de Análisis Forense Digital aplicables en un Laboratorio de Informática Forense en la Carrera de Ingeniería en Networking y Telecomunicaciones.

Tema del Proyecto de Titulación: Metodologías, Análisis Forense, laboratorio, Informática Forense.

2. Autorización de Publicación de Versión Electrónica del Proyecto de Titulación.

A través de este medio autorizo a la Biblioteca de la Universidad de Guayaquil y a la Facultad de Ciencias Matemáticas y Físicas a publicar la versión electrónica de este Proyecto de titulación.

Publicación electrónica:

Inmediata	**X**	Después de 1 año	

Firma Alumno:

3. Forma de envío:

El texto del proyecto de titulación debe ser enviado en formato Word, como archivo .Doc. O .RTF y .Puf para PC. Las imágenes que la acompañen pueden ser: .gif, .jpg o .TIFF.

DVDROM [**X**] CDROM [ ]

ÍNDICE GENERAL

ABREVIATURAS

Ab.	Abogado
ADN	Ácido desoxirribonucleico
BIOS	Basic Input Output System
CNUDMI	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
DD	Dataset Definition
DoS	Denial of Service
FBI	Federal Bureau of Investigation
GPS	Global Positioning System
IEPI	Instituto Ecuatoriano de la Propiedad Intelectual
Ing.	Ingeniero
IOSE	Instituto de Obra Social del Ejercito
IT	Information Technology
Lcda.	Licenciada
LSi.	Licenciado en Sistemas de Información
MD5	Message-Digest Algorithm 5
MSc.	Master
PDA	Personal Digital Assistant
RAM	Random Access Memory, RAM
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

ESTUDIO E IMPLEMENTACIÓN DE METODOLOGÍAS DE ANÁLISIS FORENSE DIGITAL APLICABLES EN UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

Autor: John Steven Larrea Ronquillo
Tutor: Ing. Jorge Chicala Arroyave

RESUMEN

A través de la presente investigación se estudiarán las diferentes metodologías existentes para el Análisis Forense Digital. El principal objetivo que se persigue con este trabajo es aplicar las mejores prácticas, procedimientos técnicos y normas operativas para la propuesta de implementación de un nuevo laboratorio en la Universidad de Guayaquil, específicamente en la Facultad de Ciencias Matemáticas y Físicas, Carrera de Ingeniería en Networking y Telecomunicaciones. Se define el concepto de evidencia digital y su clasificación, se mencionan manuales internacionales relacionados con la recolección, manipulación, preservación y análisis de la misma, así como las leyes relacionadas a delitos y fraudes informáticos que rigen en la legislación ecuatoriana. Se realiza una investigación tanto exploratoria como descriptiva por medio de encuestas a los alumnos para determinar la necesidad de implementación de un laboratorio de informática forense con las normas y procedimientos apropiados para efectuar el análisis de evidencia digital y para desarrollar el aprendizaje en esta ciencia. Se resalta la importancia que tienen los resultados obtenidos a partir de los objetos examinados ya que se pueden constituir como prueba fehaciente de la existencia de un delito, por ende se propone aplicar los métodos adecuados al momento de tratar la evidencia en todos sus aspectos, garantizando de esta manera que esta mantenga su integridad y que los resultados sean confiables.

Palabras claves: Metodologías, Análisis Forense, laboratorio, Informática Forense

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

STUDY AND IMPLEMENTATION OF DIGITAL FORENSIC ANALYSIS METHODOLOGIES APPLICABLE IN A LAB COMPUTER FORENSIC AT THE NETWORKING AND TELECOMMUNICATIONS ENGINEERING DEPARTMENT

Autor: John Larrea Ronquillo
Tutor: Ing. Jorge Chicala Arroyave

ABSTRACT

Through this research the different existing methodologies for digital forensics are studied. The main objective pursued with this study is to apply best practices, technical procedures and operational rules for the proposed implementation of a new laboratory at the University of Guayaquil, specifically in the Faculty of Mathematics and Physical Sciences, Networking and Telecommunications Engineering Department. The concept of digital evidence and its classification is defined, international manuals related to the collection, manipulation, preservation and analysis of it are mentioned, as well as the laws related to computer crime and fraud that govern Ecuadorian legislation. Both exploratory and descriptive research is conducted through student surveys to determine the need for implementation of a forensic computer lab with the appropriate rules and procedures to conduct digital evidence analysis and to develop learning in this science. It highlights the importance of the results obtained from the objects examined since they can be established as evidence of the existence of a crime, therefore it is proposed to apply the appropriate methods when dealing with the evidence in all its aspects, ensuring so that it maintains its integrity and that the results are reliable.

Keywords: Methodologies, Forensics, laboratory, I.T. Forensics

INTRODUCCIÓN

El presente proyecto servirá para establecer todas las normas, procedimientos y metodología de trabajo a usar en una propuesta de implementación de Laboratorio de Informática Forense que tendrá lugar en la Carrera de Ingeniería en Networking y Telecomunicaciones de la Universidad de Guayaquil. Dichos procedimientos ayudarán al correcto desempeño del personal tanto profesional como estudiantil que hará uso de las instalaciones del Laboratorio, al óptimo aprovechamiento de herramientas de análisis digital y a dar un trato apropiado a la evidencia digital que será investigada.

En (Zuccardi, 2006) dice que: "La informática o computación forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional". Es una ciencia que sirve como apoyo a la justicia en la actualidad, para hacer frente a los ciberdelincuentes, quienes aplican métodos sofisticados para cometer ataques y fraudes informáticos; esta rama es utilizada para evidenciar información sobre medios computacionales, que puede esclarecer un tema legal en proceso de investigación.

Actualmente, la informática forense ha ganado campo e importancia dentro de la informática electrónica. Esto se debe a que el valor y el uso de la información han ido en ascenso a nivel mundial y al uso de los ordenadores por disímiles entidades entre otros aspectos. Por esta razón, cuando ocurre un crimen informático, es difícil reunir la información o utilizarla a modo de prueba utilizando los mecanismos más conocidos. Debido a esto surge el estudio de la informática forense, la cual permite resolver crímenes de gran envergadura aplicando procedimientos estrictos y rigurosos.

Se conoce que los delitos informáticos ocurren con frecuencia, aunque los usuarios no los tomen en cuenta o no le den la importancia requerida. Actualmente un atacante o delincuente informático no solo realiza su crimen violando la seguridad de un sistema o un dispositivo, sino que también se ha

confirmado que este usa los datos que encuentra en los sistemas para su uso personal, pudiendo causar daños severos donde se logra concretar el hecho.

Los últimos avances tecnológicos han permitido entre otros logros el uso de diferentes herramientas forenses, que ayudan a realizar los Análisis Forenses, de tal modo que contribuyan y faciliten el proceso investigativo para obtener los resultados deseados por los analistas. Dichas herramientas forenses se aplican en diferentes áreas como Análisis Forense de redes, sistemas de archivos entre otros.

Existen diversas instituciones que se dedican a la ciencia de la investigación mediante la Computación Forense que cuentan con instalaciones, personal calificado y herramientas especializadas para este campo, pero para que funcionen adecuadamente es necesario usar una metodología apropiada y respetar todas las normas, reglas, pautas, políticas y procedimientos establecidos.

La evidencia digital es el componente principal en un análisis digital forense y debe ser tratada con las precauciones del caso, ya que si no se toman las debidas precauciones, esta puede ser alterada voluntariamente o no por este motivo es de fundamental importancia acatar los procedimientos implantados con el fin de evitar pérdida de información que puede incidir en la toma de decisiones sobre un proceso judicial. Por este motivo se propone implementar una metodología de trabajo adecuada para la propuesta de laboratorio a implementar en la Carrera de Ingeniería en Networking y Telecomunicaciones.

En el capítulo 1 de la investigación se abordará el problema; dónde está ubicado el mismo, las causas y consecuencias que han conllevado a la existencia de la situación existente, encontrándose entre ellos la clonación de tarjetas y los ataques informáticos a ordenadores, entre otros aspectos importantes. También se delimita y formula el problema. Los objetivos trazados para la realización de la investigación se definen de igual modo en este capítulo, lo cual es fundamental para el correcto desarrollo del trabajo investigativo. Finalmente se justifica la investigación de forma teórica, metodológica y práctica.

El capítulo 2 de la tesis, cuenta con varios temas que son cruciales para el presente trabajo. En este capítulo se hace un estudio de los antecedentes de la informática forense, así como de las principales herramientas y metodologías que han sido estudiadas y puestas en práctica, lo que servirá como base sólida para la propuesta que se realizará en capítulos posteriores. Unido a esto, se realiza un análisis de las legislaciones que se han establecido en Ecuador para proteger fundamentalmente la información. También se definen conceptos básicos para el estudio que se realiza como derecho y delito informático, evidencia digital, técnicas para recolectar la evidencia digital y su preservación entre otros temas de notoria importancia. Finalmente se define la idea a defender como la explicación al problema fundamental de esta investigación, la cual contribuye a la formulación de predicciones fundamentadas que servirán como sustentación para el desarrollo del presente trabajo.

En el capítulo 3 se podrá contar con el estudio metodológico del trabajo. En él se describe la modalidad y el tipo de la investigación. Así como los métodos a utilizar para la investigación, dentro de los cuales se encuentra el inductivo-deductivo. También se selecciona la población y muestra que servirá de soporte para el estudio, pues dicha muestra constituirá la cantidad de individuos a encuestar. En este capítulo se detalla, además, cómo se realiza el procesamiento y el análisis añadido a la recolección de datos. Por último, se realiza la validación de la hipótesis.

En el último capítulo de este trabajo se realizará la propuesta a llevar a cabo en el laboratorio forense que se implementará en la Universidad. La factibilidad de la propuesta será valorada, desde el punto de vista operacional, técnico y legal, lo que permitirá realizar una validación de la misma. De igual modo se propondrán las herramientas a utilizar en el laboratorio, por los especialistas que laborarán en él y las metodologías adecuadas a utilizar por los mismos para el procesamiento de la evidencia digital, de forma tal que constituya esto una guía sólida, concisa y robusta para lograr la realización del trabajo con la calidad requerida.

CAPÍTULO I

EL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

1.1 Ubicación del problema en un contexto

Actualmente, uno de los activos más importante que la sociedad posee es la información, la misma a la que se puede acceder mediante sistemas de datos, redes de cómputo, dispositivos de almacenamiento, dispositivos móviles, etc. Se debe contar con medidas para proteger dicha información e identificar el acceso no autorizada a la misma ya que los delitos informáticos son cada vez más frecuentes y representan grandes pérdidas para los afectados. Durante el procesamiento de una escena del crimen se pueden encontrar evidencias comunes, pero también se pueden hallar evidencias digitales las cuales deben ser manipuladas de manera correcta siguiendo los procedimientos adecuados basándonos en una metodología establecida, con el fin de que la evidencia no sea alterada, duplicada, modificada o eliminada ya que según el tipo de evidencia se requiere un tratamiento más específico debido a las características que posee cada elemento.

En esta entidad educativa no existe un laboratorio en el que se analicen los tipos de ataques informáticos y sus consecuencias. La investigación basa su fundamento en las características, la importancia y ventajas que tendrá la creación y apertura del laboratorio forense para la custodia, almacenamiento, preservación y análisis de evidencia real para los casos reales, que a su vez será utilizado como laboratorio común para los estudiantes de la carrera, permitiéndoles realizar el análisis digital forense, a través de los métodos y herramientas propuestos. En dicho laboratorio ubicado en la provincia del Guayas, cantón Guayaquil, Facultad de Ciencias Matemáticas y Físicas, Carrera de Ingeniería en Networking de la Universidad de Guayaquil se realizarán todos los estudios para lograr especializar y capacitar al personal necesario y de esta manera poder atender y hacer frente a los ataques informáticos.

1.2 Situación conflictos. Nudos críticos

Hace 14 años, en el 2002 se decretó la ley de comercio electrónico, firmas electrónicas y mensajes de datos. Con esta ley se aspira brindar protección a los usuarios de sistemas electrónicos regulando el uso de las tecnologías por parte de dichos usuarios. No obstante, en este país se dificulta el cumplimiento de esta ley, ya que son pocas las instituciones que se dedican a la ciencia de la informática forense como los profesionales que están capacitados en esta rama.

Se conoce que en la Fiscalía de Guayas se ideó crear una institución con este objetivo, y a nivel general tuvo gran aceptación. A partir fue creada la Unidad de Delitos Informáticos y Telecomunicaciones en el 2010, a través de la cual se investiga y persigue los crímenes informáticos que son cometidos.

En esta Unidad se realizan las investigaciones pertinentes para encontrar a los promotores de delitos, partiendo de la denuncia que previamente se ha realizado por el damnificado. Para realizar la investigación se ponen en práctica los métodos y herramientas que se deben aplicar para recolectar las evidencias necesarias y poder presentarlas legalmente.

1.3 Causas y consecuencias del problema

La era digital en la que se encuentra la sociedad ha revolucionado la forma de comunicarse y transmitir información de manera casi instantánea y de forma remota, pero no todas las veces esa información es bien utilizada, es decir no existe un control para que no se pueda enviar contenido ofensivo o dañino, y es por eso que cualquier persona puede intentar hacer uso de la tecnología para afectar a otros.

Al llevarse a cabo un delito informático, inevitablemente se ven involucrados los medios tecnológicos y la información digital. En la actualidad la correlación de evidencias, los rastros dejados por el autor entre otros aspectos se manejan de manera diferente al trabajo que frecuentemente era llevado a cabo.

En el siguiente cuadro se muestran las causas que afectan la seguridad de los usuarios.

CAUSAS Y CONSECUENCIAS

CUADRO N° 1

Causas	Consecuencias
Clonación de tarjetas magnéticas	Usuarios que pueden perder dinero de sus cuentas bancarias
Sustracción de cuentas	Usuarios que son víctimas de suplantación de identidad
Extorción a través de redes sociales	Los usuarios pueden ser víctimas de personas oportunistas que usando las redes sociales los presionan para conseguir información
Manipulación de programas contables	Hurto de los datos del correo de los usuarios afectados
Ciberacoso	Generalmente el usuario es acosado o es víctima de bullying a través de las tecnologías (teléfonos celulares, internet)
Delitos informáticos de ordenadores	Usuarios víctimas de un intruso que intenta robar información o robar su identidad.
Ataques con Malware	Programas que molestan y dañan los ordenadores.
Ataques de Bluesnarfing	Los intrusos a través de bluetooth acceden a la información de otros y la pueden manipular.

Elaborado por: John Larrea
Fuente: John Larrea

1.4 Delimitación del problema

Es necesario crear un laboratorio forense, en el cual se pongan en práctica metodologías de Análisis Forense digital para combatir las amenazas informáticas que atenten contra los usuarios dentro y fuera de la Universidad. Al mismo tiempo facilitarles a los estudiantes de la Universidad de Guayaquil, específicamente de la carrera de Ingeniería en Networking y Telecomunicaciones las herramientas necesarias para que comprendan en qué consiste el Análisis Forense y como llevarlo a cabo de la manera más óptima. Se conoce que la evidencia digital es muy delicada y cualquier acción que se realice sobre un archivo puede modificarlo, es importante tener definido un procedimiento para analizar estas pruebas, y de esta manera determinar quién o quiénes son los implicados en fomentar estas irregularidades y poder tomar acciones correctivas. Las normas, manuales y procedimientos que forman parte de ese estudio junto a una herramienta tecnológica, permitirán conservar, analizar y mostrar información de cualquier ataque informático.

1.5 Formulación del Problema

Como se conoce, inexplicablemente los criminales que realizan este tipo de actos delictivos, poco a poco se las han agenciado para utilizar la tecnología para cometer las infracciones con mayor facilidad y evadir la ley. Esta situación ha conllevado a que se tengan en cuenta el análisis digital de la información, como elemento fundamental para preservar la seguridad de la información. Debido al eminente y mencionado flujo de información y a que las amenazas son comunes hoy en día surge la necesidad de crear un Laboratorio de Informática Forense, en el cual se pueda velar por la seguridad de los usuarios dentro y fuera de la Universidad, evidenciando ataques de intrusos, suplantación de identidad, infecciones de virus provocadas, entre otros. Por esta razón se plantea el siguiente problema a resolver: ¨ **¿Cómo implementar metodologías para el Análisis Forense en el Laboratorio de Informática Forense en la Carrera de Ingeniería en Networking y Telecomunicaciones para su correcto uso en normas y procedimientos dentro del Laboratorio?** ¨, las cuales contribuirán a que el manejo de evidencia y el trabajo en general se realicen de una forma óptima.

1.6 Evaluación del Problema

Se ha realizado le evaluación del problema donde se pueden determinar los siguientes aspectos:

Claro: El procedimiento a seguir será conciso, entendible, ordenado y preciso con el fin de que los usuarios del laboratorio puedan cumplir las normas establecidas**.**

Evidente: Es evidente que el cumplimiento de las formalidades propuestas facilitará las tareas del personal calificado en técnicas de informática forense para llevarlas a cabo.

Relevante: La correcta aplicación de la metodología apropiada dará como resultado un dictamen irrefutable sobre una evidencia analizada.

Original: El análisis digital forense es un campo muy poco avanzado en el ámbito Nacional, por lo cual el estudio de normas y procedimientos enfocados a la investigación informática forense resulta novedoso.

Contextual: El uso del laboratorio involucra a estudiantes, docentes y contribuirá a la sociedad (peritos informáticos) para el análisis de casos reales demostrando las pruebas obtenidas en base a la evidencia.

Factible: La metodología elegida permitirá el uso adecuado de las instalaciones del laboratorio, la recolección, custodia, transporte y almacenamiento de la evidencia dando un resultado óptimo al momento de analizarla.

Evitar que existan delitos informáticos es muy difícil, pero se puede llegar a determinar quién ha sido el encargado de cometer la violación. Para poder dar seguimiento a estas irregularidades existen diversas metodologías y herramientas de Análisis Forense digital que es necesario estudiarlas para entender cuál es el procedimiento que se debe tomar para tener resultados acertados. Este tipo de análisis es bastante completo porque con la ayuda de herramientas informáticas se puede llegar a un resultado, pero siempre depende

de la intuición, ingenio y procesos que tiene que cumplir el investigador forense para llegar a una conclusión.

1.7 Alcances del problema

Los ecuatorianos pueden pensar que, debido a que Ecuador se encuentra en vías de desarrollo no es propenso o vulnerable a recibir ataques informáticos, pero no es así, ya que no existen sistemas completamente seguros y toda persona que acceda a medios computacionales está expuesta a ser víctima de este tipo de ataque.

Para contrarrestar esta situación, se realiza a través de este trabajo el estudio y profundización de las diversas metodologías y buenas prácticas que existen para realizar un adecuado Análisis Forense e implementar las metodologías especificas en la propuesta de laboratorio en la Carrera de Ingeniería de Networking y Telecomunicaciones. Además de proponer, a partir de las metodologías estudiadas, una que contenga las actividades y prácticas necesarias que sean eficaces para realizar la actividad de análisis con la calidad requerida en esta institución. Todo el estudio y la implementación de metodologías tendrán lugar en el Laboratorio de Informática Forense de la entidad mencionada. Este es el lugar destinado para montar todo el equipamiento necesario, donde al unísono se irá estudiando las diferentes opciones y metodologías para conseguir la propuesta adecuada a implementar en dicho laboratorio.

Se trabajará teniendo en cuenta uno de los elementos fundamentales dentro de la Informática Forense que es la evidencia digital. Para la cual según (Herrera, 2009) es necesario preservar:

- **Mantenimiento de la Cadena de Custodia:**
  Registro de todas las operaciones que se realizan sobre la evidencia digital.
  Resguardo de los elementos secuestrados utilizando etiquetas de seguridad.

- **Preservación de los elementos secuestrados de las altas temperaturas, campos magnéticos y golpes:**
  Los elementos de prueba originales deben ser conservados hasta la finalización del proceso judicial.

- **Obtención de imágenes forenses de los elementos secuestrados**
  Por cuestiones de tiempo y otros aspectos técnicos, esta tarea se realiza una vez que ha sido secuestrado el elemento probatorio original.
  En caso de que la creación de una imagen forense no sea posible, el acceso a los dispositivos originales se realiza mediante mecanismos de protección contra escritura.

- **Autenticación de la evidencia original**
  Generación de valores hash –MD5 o SHA-1- a partir de los datos contenidos en los diferentes dispositivos secuestrados.

También se tienen en cuenta planteamientos donde se menciona que la sustentación de la evidencia digital gravita en la redacción de un informe pericial en base a los resultados obtenidos. Para ello juegan un papel fundamental:

- La fuerza probatoria de los juicios informáticos la cual incide principalmente en la segura manipulación de la evidencia desde el instante de su recolección.
- El dictamen el cual debe ser neutral y exacto, debe contener los componentes necesarios para volver a ejecutar el proceso si así se lo requiere.

En esta investigación se destaca que la informática forense contribuye a la prevención y procesamiento de los crímenes computacionales. La misma tiene entre sus objetivos compensar a los damnificados por los daños que sufren a causa de los criminales, perseguir y procesar judicialmente a dichos criminales y aplicar las medidas necesarias para la prevención de casos de esta índole. El análisis que se realizará en el Laboratorio de Informática Forense permitirá sancionar a individuos que accedan a sistemas sin tener el permiso requerido o

cometiendo violaciones que atenten contra la seguridad de la información de entidades y personas en general.

1.8 Objetivos

Objetivo general

Realizar un estudio de las distintas metodologías de análisis digital forense para proponer un manual con los procedimientos adecuados a seguir en el Laboratorio de Informática Forense que se pueda implementar en la Carrera de Ingeniería en Networking y Telecomunicaciones.

Objetivos específicos

Seguidamente se muestran los objetivos específicos definidos para la presente investigación.

- Analizar diferentes metodologías existentes de Análisis Digital Forense para aplicar en un Laboratorio.
- Conocer las mejores prácticas para el Análisis Forense de evidencia digital.
- Establecer procedimientos técnicos y operativos para el análisis de medios informáticos.
- Definir una cadena de custodia para el respectivo control del material de prueba.
- Elaborar un diseño de metodología de trabajo aplicable a un Laboratorio de Informática Forense para evidenciar casos de delitos informáticos.

1.9 Justificación e importancia de la investigación

La informática forense surgió para investigar ataques a sistemas informáticos. Las investigaciones computacionales actuales se centran en descubrir los incidentes ocurridos en Sistemas Operativos, redes de datos y dispositivos de almacenamiento. La implementación de un Laboratorio de Informática Forense

beneficiará a la sociedad puesto que en él se formarán profesionales con conocimientos y habilidades en el área de la computación forense, además en este lugar se podrán analizar casos de delitos así como fraudes informáticos reales, proporcionando pruebas relevantes que pueden ser consideradas durante una investigación y presentadas ante un tribunal.

La aplicación de buenas prácticas además del cumplimiento de procedimientos de análisis forense son de suma importancia para lograr buenos resultados durante un proceso de investigación ya que el uso debido de las herramientas, el correcto tratamiento de los dispositivos secuestrados y el acatamiento de las normas establecidas permitirá que el estudio que se realice sobre la evidencia cumpla con todos los estándares en el ámbito forense.

La guía que se propone ayudará a entender los disímiles puntos que están relacionados la actividad de Análisis Forense, por lo que se obtendrá un proceso investigativo organizado y fiable. Para el adecuado desarrollo de la guía que se propondrá, se estudiaran precisamente los modelos de Análisis Forense que existen en la actualidad, además de las herramientas y procedimientos que facilitan que la investigación forense se lleve a cabo exitosamente y manteniendo el estado de la evidencia.

La falta de conocimiento de los estudiantes en esta rama y la necesidad de que los resultados de análisis de evidencia sean precisos son motivos suficientes para proponer la presente investigación, la cual beneficiará tanto a estudiantes en su preparación académica, a la institución que formará mejores profesionales y a la sociedad, ya que las autoridades podrán acudir al laboratorio para que se realice el estudio de evidencia real.

La investigación es factible puesto que en toda área o departamento son necesarios los procedimientos y deben llevarse a cabo con rigurosidad; la guía metodológica que se presenta garantizará que la evidencia digital mantenga su autenticidad y que los resultados obtenidos sean confiables.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes del Estudio

Según Serna (2012), en Colombia se ha estudiado la Informática Forense y dentro de ella, marcos de trabajo que contribuyan a esta rama. En esta investigación se indaga también en los repositorios de evidencia, donde se orienta dar prioridad a los repositorios más comunes como, los sistemas de archivos, archivos temporales, los registros de los Sistemas Operativos, etc. También se le otorga importancia al conocimiento que debe tener el investigador sobre el sistema para poder manejar la evidencia de la mejor manera sin dañar la información. Se brinda un resumen sobre cómo presentar un reporte que permita detallar los hallazgos encontrados durante un análisis.

En México también se ha tenido en cuenta los estudios y avances sobre la Informática Forense. Según Beltrán (2012), el volumen de datos que cruza hoy por cualquier organización, ha crecido de forma exponencial. En esta investigación se hace un análisis sobre un estudio previo, realizado por el FBI, el cual arrojó que 40% de usuarios detectaron penetraciones de delincuentes informáticos externos, 32% reportó ataques masivos de negación de servicios (DoS). Por otro lado, un 85% de usuarios tuvo incidentes de contaminación por virus, 80% reportó pérdidas financieras debido a los ataques de violaciones de seguridad informática y un 69% reportó pérdida y robo de computadoras portátiles.

Costa Rica ha sido un país, en el cual también se han realizado investigaciones sobre este tema. El investigador León (2013), realizó una investigación en la cual profundiza sobre las respuestas a incidentes de seguridad, análisis de conexiones, los tipos de ataques que pueden existir, así como analizar los paquetes de datos, cómo se lleva a cabo el trabajo realizado por los analizadores de datos. También analiza cómo se puede realizar la captura y el análisis de datos y de los ficheros transmitidos, además de las herramientas

utilizadas para el apoyo de investigaciones forenses y se define y estudia el Fingerprint, el cual no es más que una tecnología para identificar el contenido, basándose en una firma obtenida de una grabación de audio. A través de ella se utilizan algoritmos especiales para convertir las energías de una pieza en un sónico único, tal como la huella dactilar de cada individuo.

El licenciado Pagés (2013), ha sido uno de los especialistas españoles que se ha dedicado a estudiar esta rama en dicho país. El investigador, a través de su trabajo define la informática forense, sus principios, normas y objetivos fundamentales. Menciona en su estudio brevemente que en 1986, el teniente Oliver North escribió unos correos comprometedores, los cuales borró de su ordenador, pero las copias de respaldo fueron revisadas y los mensajes fueron recuperados, con lo cual el señor North fue declarado culpable. Con este ejemplo se demuestra cómo la evidencia puede determinar la culpabilidad o librar de ella a un individuo.

En Argentina se han hecho estudios similares que permiten conocer un poco mas sobre la evidencia digital, como preservarla y como recabar la información. Según Di Lorio (2013), La Informática Forense nace como una rama de las ciencias forenses, una disciplina auxiliar a la justicia, que consiste en la aplicación de técnicas que permiten adquirir, validar, analizar y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. A través de esta investigación se hace un destudio sobre cómo recuperar archivos eliminados, extraer la informacion a examinar dependiendo del tipo de archivo, asi como extraer archivos protegidos con contraseñas, entre otros aspectos fundamentales.

El estudio de bibliografías anteriores, facilita la realizacion de esta investigacion, ya que ha permitido conocer las violaciones más comunes y afectaciones que han traido para los usuarios los distintos ataques. Así como herramientas y metodologías para realizar el Análisis Forense. Esto contribuirá a que la propuesta que se ralizará como parte de la presente investigación, permita la recuperación de información a partir de las tareas previamente estructuradas y organizadas, respetando las buenas prácticas definidas por los organismos

internacionales, para guiar a los profesionales de la institucion en la realización de esta actividad y facilitarle a los estudiantes una metodología amplia y detallada del procedimiento a llevar a cabo, lo que será de gran ayuda para que ellos puedan comprender con facilidad los detalles del proceso.

2.2 Fundamentación teórica

La informática forense según (Giovanni, 2006) sirve como apoyo para investigaciones y procesos judiciales haciendo frente y buscando desenmascarar a delincuentes informáticos quienes disponen de técnicas avanzadas mediante el uso de la tecnología para sacar provecho de información perteneciente a terceros. Desde 1984, el Laboratorio del FBI y varias organizaciones que buscan hacer cumplir la ley comenzaron a elaborar programas para analizar evidencia digital.

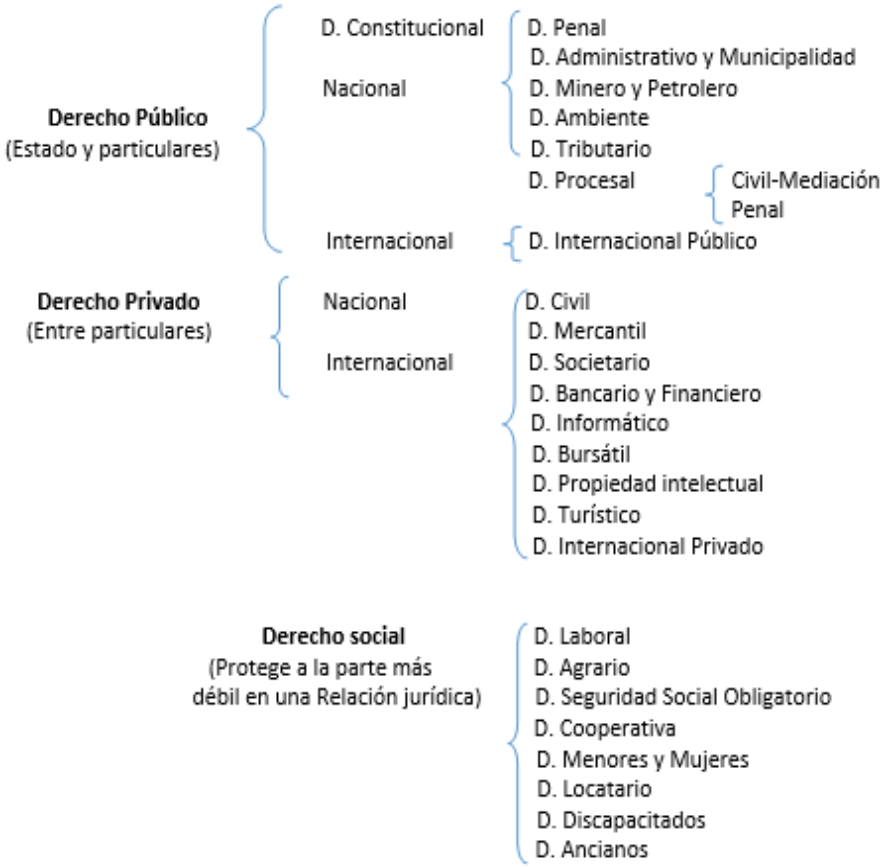
Es importante conocer, cómo se comportan los hechos de seguridad, las vulnerabilidades y los crímenes informáticos que ocurren. Se conoce que en los últimos años han aumentado este tipo de delitos, por esta razón es necesario analizar su comportamiento.

> **El informe de Evolución de Incidentes de Seguridad que corresponde al año 2007, elaborado anualmente desde 1999 por Red IRIS, determina que el incremento de incidentes que ha habido entre el año 2006 y 2007 es el 63.32% en el que se involucran escaneo de puertos en busca de equipos vulnerables, vulnerabilidades de sistemas web, errores de programación, vulnerabilidades de navegadores más utilizados, ataques de phishing, máquinas zombies, malware y otro tipo de ataques para el cometimiento de fraudes u inhabilitación de servicios, este mismo informe indica que el patrón de ataque continua siendo más dirigido, inteligente y silencioso con algún tipo de trasfondo que puede ser económico, religiosos, político o de ansias de poder.** (Ureta, 2009, pág. 4)

2.2.1 Derecho informático

El derecho informático es la combinación de palabras " derecho" e "informática" da consecuencia una materia jurídica que regula las tecnología y la información; por eso a la época se le ha denominado "la sociedad de información" o revolución electrónica" esto se debe a la transmisión de información que hay gracias a los aparatos electrónicos y de avanzada tecnología y a la facilidad que ofrecen, pero que también obligan a pensar en los problemas que esto puede repercutir, la tecnología no solo permite progreso si no también problemas que el Derecho debe adoptar y estar a la par, y desde la perspectiva jurídica se deben crear nuevos ordenamientos jurídicos que regulen las acciones de los hombres en cuanto tenga que ver con la tecnología, con el objetivo de que no se convierta en peligroso si no en un servicio. Dentro del derecho, el delito informático se clasifica en:

Gráfico 1: Clasificación de los delitos informáticos



Elaborado por: John Larrea
Fuente: (Cabrera, 2014)

2.2.2 Delito informático

Según Cabrera (2014), a finales del siglo XX nace la expresión delito informático justo cuando el internet comenzó a tomar fuerza en Norteamérica y la vida de sus habitantes. Durante una sesión en Francia varios países formaron un grupo denominado G8 el cual priorizó analizar los conflictos generados por la delincuencia que ya no eran únicamente ataques físicos, sino también a través de redes de datos por medio del internet, era en esos casos cuando se utilizaba el término "delito informático" para referirse a crímenes ejecutados desde el internet.

2.2.3 Evidencia Digital

La evidencia digital es: “cualquier dato que puede establecer que un crimen se ha ejecutado, o puede proporcionar un enlace entre un crimen y su víctima o un crimen y su autor” (Giovanni, 2006, pág. 8). La evidencia que se recoge en un papel es diferente a la evidencia computacional, pues esta última se puede hacer copiar idénticas. Otro aspecto que constituye un inconveniente es que la evidencia digital puede aparecer en varias copias de archivos sin ser autorizadas, y esto impide ubicar cuándo o quién las realizaron. Por estas razones entre otras se hace difícil en ocasiones investigar acerca de los delitos que se puedan llevar a cabo. Los especialistas verifican que sus copias sean idénticas a las de los sospechosos a través de tecnologías como Checksums o Hash.

Cuando ocurre alguna alteración o delito en la información, las personas responsables del crimen generalmente tratan de alterar la información o manipularla de tal modo que resulte engorroso encontrarlas, tratando de borrar los rastros que los puedan involucrar. Para mitigar esto, los especialistas trabajan haciendo uso de las características de la evidencia para determinar si esta ha sido alterada. La evidencia digital puede ser duplicada exactamente igual al archivo o documento original y esa copia puede ser estudiada y obtener de ella resultados positivos. Esto trabajo se realiza para proteger los archivos originales. Otra característica es que es muy difícil de eliminar, incluso si la

información es borrada del disco duro del computador o este haya sido formateada, se puede recuperar la información.

2.2.4 Clasificación de la evidencia digital

Zuccardi (2006) refiere que la evidencia digital tiene tres clasificaciones:

Registros generados por ordenador: Son llamados así porque se generan a causa de la programación de un ordenador. Estos no pueden ser modificados por un individuo, también se los conoce como logs o registros de eventos y se los utiliza para verificar si un dispositivo o programa está funcionando correctamente.

Registros simplemente almacenados por o en ordenadores: Son los que un individuo guarda en un ordenador, como lo son documentos de texto, hojas de cálculo, fotos, músicas, etc. En este tipo de registro es fundamental descubrir la identidad de su autor con el fin de comprobar un suceso a través de la evidencia adquirida.

Registros híbridos: Son la combinación de los registros mencionados anteriormente, como ejemplo se puede señalar una transferencia bacaria, ya que es un registro generado por un sistema pero es un usuario quien emite ese evento.

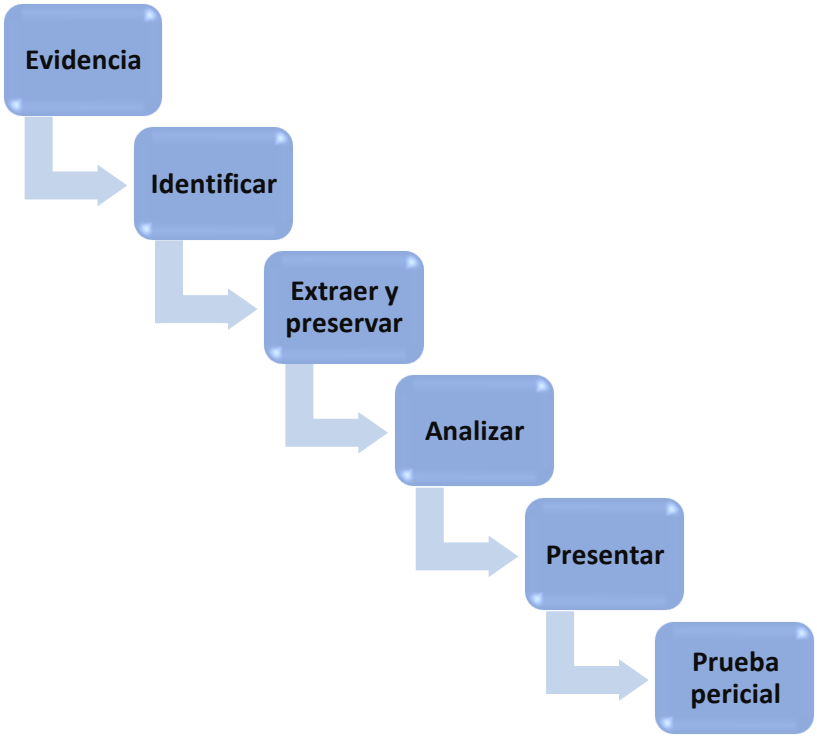
2.2.5 Manipulación de la evidencia digital:

Los especialistas que manipulan información deben conocer cómo hacer este trabajo. Para ello tendrán que hacer uso de los medios forense estériles para realizar los medios de información. Mantener la integridad del dispositivo inicial. En el instante en el que se recoge la evidencia, deberá protegerse y preservarla. La persona que acceda a una evidencia debe ser un especialista que maneje el tema. Las copias de los datos obtenidas deberán ser controladas y preservadas, además los resultados de la investigación tendrán que estar disponibles para ser verificados y estudiados, por lo que el proceso será reproducible, de forma tal que se pueda tener acceso a la información obtenida siempre que se estime. El especialista encargado de la evidencia digital, tendrá que ser responsable de las

acciones y decisiones que se tomen respecto a esta. Las agencias o entidades responsables de recolectar y analizar la evidencia digital, deberán garantizar que se realice lo antes mencionado.

2.2.6 Procedimientos para el análisis de datos

Gráfico 2: Análisis de datos



Elaborado por: John Larrea

Fuente: (Lucas, 2010)

2.2.7 Obtención de la evidencia digital

Luego de conocer que el sistema informático ha sido atacado, se debe realizar una investigación sobre la información existente de manera minuciosa.

Se comienza a realizar una descripción de los hechos, tomando notas de las operaciones realizadas sobre los sistemas. Se recopila la fecha, la hora de inicio y fin del análisis, los números de serie de cada equipo, número de código de identificación del activo informático. Se toman fotos del equipo y el entorno, en

caso de ser necesario. Guardar las garantías procesales adecuadamente, contribuirá a garantizar que el análisis realizado sea aceptado en un juicio.

Para recopilar evidencias, se debe seguir el siguiente orden: (Delgado, 2007)

- Registros y contenidos de la caché.
- Contenidos de la memoria.
- Estado de las conexiones de red, tablas de rutas.
- Estado de los procesos en ejecución.
- Contenido del sistema de archivos y de los discos duros.
- Contenido de otros dispositivos de almacenamiento.

La evidencia volátil es la evidencia que se puede perder con mayor rapidez. Dentro de este tipo de evidencias se les otorga prioridad a:

- Fecha y hora.
- Procesos activos.
- Conexiones de red.
- Puertos TCP/UDP abiertos y aplicaciones asociadas “a la escucha”.
- Usuarios conectados remota y localmente. (Delgado, 2007)

La información según el orden de volatilidad se clasifica en:

EVIDENCIA DIGITAL ALTAMENTE VOLÁTIL

CUADRO N° 2

Tipo de almacenamiento	Importancia forense
CPU (Registros, cache), Memoria de Video	Por lo general la información en estos dispositivos es de mínima utilidad, pero debe ser capturada como parte de la imagen de la memoria del sistema.

Elaborado por: John Larrea

Fuente: (Romo & Omar, 2011)

EVIDENCIA DIGITAL MEDIANAMENTE VOLÁTIL

CUADRO N° 3

Tipo de almacenamiento	Importancia forense
RAM	Incluye información sobre los procesos en ejecución. El hecho de capturarla hace que cambie, requiere de conocimiento especializado para poder reconstruirla, pero no se requiere de mucho conocimiento para buscar palabras clave.
Tablas del Kernel (Estado de la red y procesos en ejecución)	Permite analizar la actividad de red y los procesos que pueden ser evidencia de actividades no autorizadas.

Elaborado por: John Larrea

Fuente: (Romo & Omar, 2011)

EVIDENCIA DIGITAL POCO VOLÁTIL

CUADRO N° 4

Tipo de almacenamiento	Importancia forense
Medios fijos (discos duros)	Incluye área de swap7, colas, directorios temporales, directorios de registro, logs y otros directorios. La información recolectada en el área de swap y en las colas permite analizar los procesos y la información de los mismos, en un tiempo en particular. Los directorios permiten recuperar eventos.

Medio removible (cintas y CD-Rom)	Usualmente son dispositivos para almacenamiento de contenidos históricos del sistema. Si existen previamente a un incidente pueden ser usados para acotar e periodo de tiempo en el cual sucedió.
Medio Impreso (papel)	Difíciles de analizar cuando hay muchos, ya que no se pueden realizar búsquedas automáticas sobre ellos.

Elaborado por: John Larrea
Fuente: (Romo & Omar, 2011)

Para recopilar las evidencias volátiles se debe disponer de un lugar seguro para el almacenamiento de la información. En algunas ocasiones esta información puede requerir espacios considerables. Utilizar discos duros extraíbles es una opción muy acertada, ya que estos permiten recopilar grandes cantidades de información y el acceso a esta de forma rápida y sencilla.Emplear herramientas de transmisión de datos a través de la red como Netcat, la misma facilita el envío de la información que se ha recabado hacia un sistema seguro, definido previamente.

La información volátil no debe mantenerse nunca en el equipo que se está analizando, pues ese equipo está comprometido y pudiera hacerse difícil la posterior recuperación de dicha documentación. Los discos que se utilizan para el resguardo de la información contienen tipos de datos adicionales que son los metadatos, los cuales son de gran ayuda para la investigación. Generalmente se obtienen imágenes de disco utilizado sobre medios de solo lectura, para su análisis futuro.

Dentro de entornos UNIX/Linux, la herramienta (DD) Dataset Definition, es muy utilizada. Ella permite producir imágenes bit a bit, facilita la opción como el hash MD5 de la copia entre otras ventajas. Esta herramienta unida a la mencionada Netcat permite el envío de imágenes a través de la red.

2.2.8 Técnicas para recolectar evidencia

La recolección de la evidencia es importante para la obtención de resultados satisfactorios luego de una investigación. Para recabar la evidencia, es necesario ser cauteloso, y realizar los exámenes requeridos con minuciosidad para garantizar la integridad de la muestra.

Cuando un examinador, realiza su trabajo, la aplicación o sistema sobre la cual se trabaja, siempre se ve alterada o modificada, a pesar del cuidado que se tenga con esta. Se conoce que, para las investigaciones, algunas evidencias son mejores que otras, o sea pueden contribuir más que otras y se acepta que la evidencia se modifique, teniendo en cuenta que la misma es conocida.

2.2.9 Preservar evidencia digital

"Con planificación previa y procedimientos claros en la recolección de evidencia se pueden disminuir los tiempos sin afectar el restablecimiento operativo y manteniendo el mejor escenario para una eventual judicialización" (Presman, 2011, pág. 5).

Existen buenas prácticas para recolectar evidencia, algunas de ellas son:

- Realizar inventarios a los dispositivos de almacenamiento (Pendrives, Discos Duros, etc.)
- Uso de bolsas antiestáticas que protejan el magnetismo de los dispositivos.
- Registrar los elementos que se deben detallar en el documento de allanamiento (Modelo, Número de Serie y Fabricante), mencionar la ubicación de estos y la persona responsable de estos activos.

Estas prácticas se relacionan con los métodos que se han utilizado para la obtención de la evidencia digital. Sobre dichos métodos se muestra el siguiente cuadro, en el cual se definen sus ventajas y desventajas:

MÉTODOS DE OBTENCIÓN DE EVIDENCIA DIGITAL

CUADRO N° 5

Método	Ventajas	Desventajas
Secuestrar hardware	Requiere poca experticia técnica. Simple, sin críticas. El hardware puede ser examinado en un entorno controlado. El hardware está disponible para varios peritajes o aplicación de distintas técnicas forenses	Riesgo de dañar el equipamiento en el traslado. Riesgo ante evidencia encriptada. Riesgo de pérdida de evidencia digital (ej. RAM). Genera cuestionamientos por interrumpir la normal operatoria de un negocio. Riesgo de no ser capaces de poder encender el equipo (ej. password a nivel de BIOS)
Adquirir toda la evidencia digital on-site	La evidencia digital puede ser examinada a posteriori. El trabajo con una imagen forense evita daños sobre la evidencia original. Minimiza el impacto en la operatoria del negocio y evita daños al hardware.	Requiere entrenamiento y recursos tecnológicos forenses. Riesgo de imposibilidad de acceso a la evidencia encriptada. Riesgo de pérdida de evidencia digital (ej. RAM). Requiere tiempo (a veces es prohibitivo). Los métodos pueden ser cuestionados mucho más que al secuestrar el hardware, y pueden surgir impedimentos técnicos.

Adquirir selectivamente la evidencia digital on-site	Se puede aprovechar alguna asistencia local (ej. administrador de sistemas, si no está sospechado). Rápida y sin consumir demasiados recursos tecnológicos	Requiere experticia, entrenamiento y recursos tecnológicos forenses. Riesgo de perder o destruir evidencia. Los métodos pueden ser cuestionados mucho más que al secuestrar hardware y pueden surgir impedimentos técnicos

Elaborado por: John Larrea
Fuente: (Romo & Omar, 2011)

2.2.10 Herramientas utilizadas en la informática forense

Para realizar un examen forense, es necesario conocer las herramientas que son útiles para esta actividad. Con solo conocer la información que se extrae y los informes que esta permite generar, no basta. Conocer la relación de la herramienta son la aplicación sobre la que se ejecuta, qué afectaciones puede traer a la memoria, los archivos que se ven modificados y los recursos del sistema a los que puede acceder, son elementos fundamentales que se pueden obtener mediante las herramientas propicias.

Algunas de las herramientas más utilizadas para realizar los procederes informáticos forenses se mencionan seguidamente:

HERRAMIENTAS PARA PROCEDIMIENTOS FORENSES

CUADRO N° 6

Herramientas	Licencia	Imagen	Control de Integridad	Análisis
Encase	Si	Si	Si	Si
Forensic Toolkit	Si	Si	Si	Si
Winhex	Si	Si	Si	Si
Deft	No	Si	Si	Si

Elaborado por: John Larrea
Fuente: (Romo & Omar, 2011)

Unidas a esta, existen otras herramientas como Coroner´s Toolkit, la cual es de código abierto y no necesita licencia.

Para que una herramienta forense, sea confiable, debe tener características que se mencionan seguidamente: (Romo & Omar, 2011)

- Emplear disímiles categorías de abstracción: Debe manejar información tanto en alto como en bajo nivel ya que esta última es mucho más complicada de percibir.

- Deben ser capaces de obtener una imagen bit a bit de la evidencia digital. Se debe copiar desde el primer hasta el último bit de información incluyendo los espacios vacíos de memoria.

- Debe manejar un proceso de error de lectura muy sólido, ya que si falla algún sector del dispositivo, al momento de realizar la copia tendrá que señalar en el dispositivo de destino la misma ubicación y dimensión del sector que no fue legible en el origen, se deben detallar en el informe los inconvenientes de este tipo.

- La herramienta debe poder efectuar exámenes de forma científica con el objetivo de estos se puedan repetir por otros individuos obteniendo los mismos resultados.

2.2.11 Admisibilidad

La admisibilidad es un aspecto que está vinculado a las leyes. Basadas en esas leyes, existen, se han definido cuatro criterios que se necesitan para analizar si la evidencia es admisible o no. Según Romo & Omar (2011) los criterios son:

Autenticidad: Para autenticar la evidencia digital, deben cumplirse dos aspectos fundamentales: Probar que la evidencia se ha generado y ha sido registrada en el lugar de los hechos y que dicha evidencia debe demostrar que no se han modificado los medios iniciales de la información.

La evidencia digital puede ser manipulada fácilmente y es muy volátil a diferencia de los medios de prueba físicos por lo cual es necesario y fundamental validar la autenticidad de la evidencia digital presentada contrariamente a lo que sucede con los medios de prueba físicos en los cuales no se objeta su autenticidad.

Se necesita que una arquitectura exponga métodos los cuales aseveren que los archivos no han sido modificados ni alterados y mantienen su integridad. Estos métodos permiten reducir la desconfianza sobre la integridad de la evidencia ya que precisan mediante algoritmos la autenticidad de los archivos otorgando así credibilidad sobre la evidencia aportada.

Confiabilidad: Para que los registros generados por el computador sean confiables se debe comprobar que la estructura del software funcione correctamente, comprobando que todos los eventos que se generan son registrados y almacenados. La confiabilidad de una evidencia digital también depende de que el sistema que la generó funcionó correctamente y no fue alterado ni vulnerado al momento de almacenarla.

Completitud o suficiencia: Es un criterio muy importante para la resolución de un caso igual a los antes mencionados, ya que muchas veces la falta de material probatorio durante un proceso ocasiona la terminación del mismo el cual pudo haber sido resuelto.

La correlación de eventos es de gran ayuda para cumplir con este criterio ya que permite dar forma a la investigación uniendo diversas partes que conforman una prueba completa y consolidada. Esta correlación puede ser llevada a cabo manualmente o a través de sistemas automatizados. En la actualidad uno de los fundamentos en que se basa el sistema de gestión de seguridad informática es en las herramientas que generan y almacenan eventos y correlacionan los mismos como lo son las SIEM (Security Information and Event Management).

De acuerdo con Zuccardi (2006), existen muchos usos de la Computación Forense, son utilizados cotidianamente y no poseen necesariamente una vinculación directa con esta ciencia:

1) Persecución Criminal: Se puede utilizar la evidencia digital para aportar en la ejecución de procesos de disímiles delitos como por ejemplo lavado de dinero, narcotráfico, estafas o pornografía infantil.
2) Litigación Civil: La Computación Forense puede aportar en el procesamiento de casos como acoso, amenazas, discriminación, etc.
3) Investigación de Seguros: A través del análisis de ordenadores puede ser hallada evidencia que permita reducir los costos de entidades aseguradoras correspondientes a indemnizaciones por siniestros.
4) Temas corporativos: Se puede recolectar información que aporten a casos como fuga de información, espionaje empresarial o atentado contra la propiedad intelectual de terceros.
5) Mantenimiento de la ley: La Computación Forense puede ser aplicada en la exploración de órdenes judiciales.

Los preceptos científicos que existen durante dl procesamiento de una evidencia son utilizados en prácticas como:

- Recolección y análisis de ADN y huellas digitales.
- Recuperación de archivos o dispositivo averiados.
- Extracción de copias bit a bit de evidencias digitales.
- Generación de huellas digitales con algoritmos hash MD5 o SHA1 de documentos de texto asegurando la integridad de los mismos.
- Certificación de documentos informáticos mediante el uso de firmas digitales.

2.2.12 Buenas Prácticas Para un Laboratorio Forense

Todo departamento que se dedica a alguna actividad específica debe contar con normas estandarizadas para hacer un trabajo efectivo, de manera que pueda ser realizado de la misma forma por otra persona obteniendo resultados similares. "Es necesario contar con técnicas y procedimientos científicos, manuales

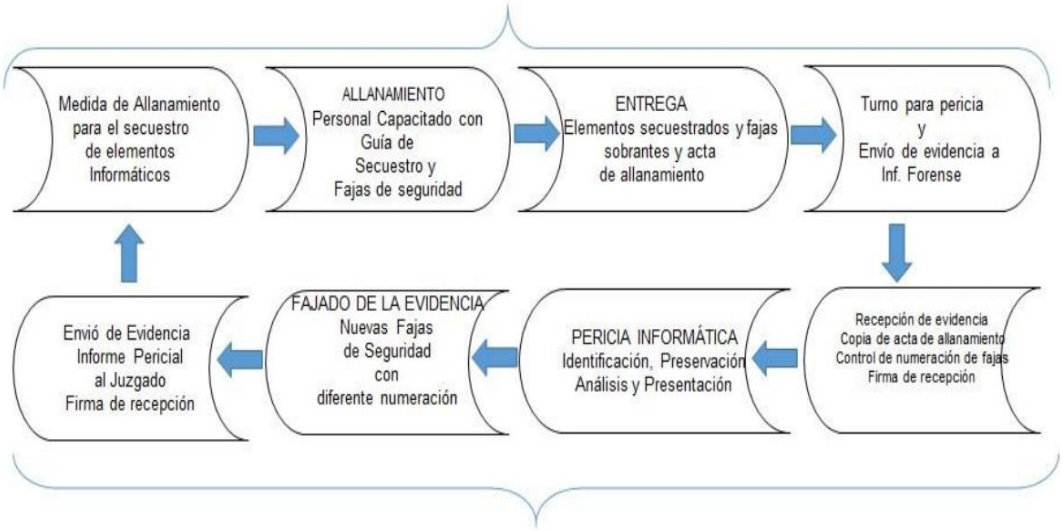
operativos y protocolos que permitan trabajar de forma ordenada, metodológica y sistematizada" (Semprini, 2015, pág. 28).

2.2.13 Cadena de custodia

La cadena de custodia es la serie de reglas que buscan garantizar la integridad de material probatorio, evidencia física o en este caso digital, mediante una serie de controles y formalidades al momento de recolectar, recibir, trasladar y entregar dicho material con el fin de evitar la alteración, sustracción o destrucción del mismo.

Es necesario contar con técnicas y procedimientos científicos, manuales. La cadena de custodia constituye un elemento fundamental de este protocolo, la cual describe la utilización de fajas de seguridad y se muestra a continuación:

Gráfico 3: Cadena de Custodia



Elaborado por: John Larrea
Fuente: (Semprini, 2015)

Manuales y metodologías internacionales utilizadas en los laboratorios forenses

Actualmente existen diversos manuales para trabajar con la evidencia digital, que son de gran ayuda. Uno de ellos es el Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0, creado por el doctor Santiago Acurio del Pino. Dicho manual propone como objetivo principal facilitar el

procedimiento para la obtencion de pruebas, a lo que se le otorga especial importancia, ya que esta ultima es necesaria para confirmar hipótesis y llegar a resultados verdaderos.

La propuesta también constituye una guía sobre cómo actuar para los miembros de la Policía Judicial y también para los funcionarios fiscales, al encontrarse e una escena del delito equipos informaticos que se relacionen con hechos inescrupulosos.

En este manual se describen los principios básicos, los principios del peritaje, asi como el reconocimiento de la evidencia digital, las clases de equipos informaticos y electrónicos. Tambien se detallan los pasos a realizar en la escena del delito y como reconstruir dicha escena. Acurio (2012) brinda ejemplos de buenas practicas que se muestran a continuación:

- Se debe recolectar el manual de usuario de los dispositivos secuestrados.
- Documentar cada acción realizada al recolectar y analizar los medios de almacenamiento
- Proteger los medios de almacenamiento alejándolos de otros dispositivos que pueden averiarlos mediante la emisión de ondas electromagnéticas potentes.

También se caracterizan las fuentes de evidencia digital, las cuales se muestran seguidamente:

- **Sistemas informáticos abiertos:** Son los cuales están constituidos por las denomindas PC, sus dispositivos de entrada/salida, laptops y servidores. En la actualidad estos equipos cuentan con gran capacidad de almacenamiento lo que los transforma en el origen de una cantidad considerable de evidencia computacional.
- **Sistemas de comunicación:** Se componen de redes de datos, dispositivos de comunicación y el Internet. También originan numerosa evidencia digital.

- **Sistemas convergentes de computación:** Se componen de dispositivos como smartphones, tablets, asistentes personales digitales PDAs, tarjetas de acceso magnéticas y disímiles dispositivos que posea afinidad digital.

2.3 Fundamentación social

Dentro de los principios de ciencia y tecnología se conoce:

La ciencia y la tecnología deben estar al servicio del desarrollo humano, ya que no puede entenderse el desarrollo, sino cuando la sociedad tenga acceso al bienestar, entendido como calidad de vida y oportunidades. (Mauricio, 2012)

El resultado de esta investigación, será positivamente aceptado en la sociedad, ya que al quedar definidas las metodologías adecuadas para el análisis en el Laboratorio Forense de la Universidad, los estudiantes tendrán una pauta de cómo proceder durante el análisis de evidencia digital, tomando todas las precauciones del caso y colaborando con la ciudadanía a que diversos delitos informáticos sean esclarecidos a través de los informes realizados en base al análisis de las pruebas recibidas, lo cual puede determinar la responsabilidad o no de uno o varios individuos en un delito o fraude informático.

2.3.1 Inclusión social

Se conoce que algunas formas de privaciones, pueden llevar a la exclusión social, y esta exclusión puede conllevar a otras privaciones. Precisamente a través de esta investigación se evitará que el individuo se vea limitado y excluido, por miedo a ser atacado, de las actividades que realiza cotidianamente a través del uso de las tecnologías.

En este sentido se puede afirmar que se mejorará la calidad de vida de la población, pues se pretende garantizar su seguridad y tranquilidad desde el punto de vista tecnológico.

Según Seguinfo (2005) debe ser primordial para los gobiernos, entidades y personas en general la aplicación de políticas de seguridad informática, pues la sociedad en la que vivimos cotidianamente emplea los medios informáticos, redes de datos y sistemas de comunicación con el objetivo de efectuar sus actividades diarias. A medida que incrementa la utilización de sistemas informáticos, aumentan también las probabilidades de ser víctimas de ataques de esta índole poniendo en riesgo la información que circula a través de los mismos. Por este motivo es de suma importancia aplicar medidas para contrarrestar las amenazas informáticas.

Cada día se hace más frecuente los reportes sobre vulnerabilidades que se detectan. Dichas vulnerabilidades son el escenario perfecto para que los intrusos intervengan en los sistemas informáticos con facilidad. Los intrusos se sienten motivados a realizar los delitos por diversos impulsos, que en la actualidad no han logrado descifrarse con claridad, debido a que los métodos que utilizan para atacar, son diferentes.

Pero, aunque pueda parecer difícil, la criminalística, permite el análisis y estudio de los escenarios cuando son atacados. De esta forma la informática forense se realza para conseguir la justicia, enfrentando los mecanismos y las técnicas que llevan a cabo los atacantes y para descifrar la verdad sobre la evidencia digital recabada.

2.4 Fundamentación legal

En el ámbito internacional, se ha tratado recurrentemente el tema de evidencia digital pues los crímenes por medios digitales han tenido tanto auge como la revolución tecnológica en sí. En consecuencia, los procedimientos que les permitan a los investigadores recuperar datos de computadores involucrados en actividades delictivas, para ser usados como evidencia en investigaciones criminales se han convertido en un tema fundamental para las agencias de policía internas de cada país.

Así, el tema se traslada del ámbito interno al ámbito internacional por su naturaleza misma. A manera de ejemplo, se puede presentar un caso en el que

el delito se origine en Colombia, pero se materialice en Estados Unidos, Islas Caimán y Rusia. En un caso como este, la evidencia digital necesaria, debe recolectarse de acuerdo a ciertos parámetros establecidos ¿Por quién? Y ¿Quién debe recolectarla? Esta clase de interrogantes se presentan a diario en casos que pueden aparentar ser sencillos.

De esta forma, se hace evidente la necesidad de adoptar procedimientos y estándares, científicamente evaluados, para conducir investigaciones forenses en sistemas de computación. Teniendo en cuenta este objetivo, se han realizado distintos estudios y el tema ha sido desarrollado eficazmente por distintas organizaciones internacionales y a nivel interno en unos países más que en otros. En esta ocasión, se verificará el trabajo que ha realizado, la Comunidad Europea, la regulación interna de Estados Unidos y el Instituto de Obra Social del Ejercito (IOSE). (Bogota & Claudia, 2016)

Hace más de veinte años, las Naciones Unidas se han proyectado por promover, a través de la Uncitral (CNUDMI: Comisión de Naciones Unidas para el Derecho Mercantil Internacional) la adaptación de las legislaciones mundiales a las leyes y modelos con las que estos cuentan. Por esta comisión se han aprobado diversas leyes dentro de las cuales se encuentra: la Ley Modelo sobre Comercio Electrónico y la Ley Modelo sobre Firmas electrónicas.

El país que mayores avances ha tenido en estos temas dentro de Sur América es Colombia. En 1999, este país público su ley 527, la cual regula el comercio electrónico, las firmas digitales y las entidades de certificación. Un año después, Perú anuncia y publica la Ley 27269, sobre Firmas y Certificados Digitales. Le siguieron en el 2001 Argentina y Venezuela y en 2002 Chile y Ecuador.

2.4.1 Legislaciones establecidas en Ecuador

Previo a la descripción de las legislaciones establecidas en Ecuador, se muestra a continuación, la estructura que comprenden dichas regulaciones:

Gráfico 4: Jerarquía de leyes. Pirámide de Kelsen

Elaborado por: John Larrea

Fuente: (Ureta, 2009)

En la legislación del Ecuador bajo el contexto de que la información es un bien jurídico a proteger, se mantienen leyes y decretos que establecen apartados y especificaciones acordes con la importancia de las tecnologías, tales como: (Ureta, 2009)

1) Ley Orgánica de Transparencia y Acceso a la Información Pública.
2) Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
3) Ley de Propiedad Intelectual.
4) Ley Especial de Telecomunicaciones.
5) Ley de Control Constitucional (Reglamento Habeas Data).

Gerberth Adín Ramírez Rivera, expresa “para que todo lo realizado en la informática forense sea exitoso, es necesario que se tengan regulaciones jurídicas que penalicen a los atacantes y que pueda sentenciárseles por los crímenes cometidos. Cada país necesita reconocer el valor de la información de

sus habitantes y poder protegerlos mediante leyes. De manera que los crímenes informáticos no queden impunes". (Ureta, 2009)

La legislación ecuatoriana se propone proteger la información como bien jurídico, a través de leyes y decretos en los cuales constan especificaciones sobre la relevancia que tienen las tecnologías:

2.4.1.1 Ley Orgánica de Transparencia y Acceso a la Información Pública:

La ley establece que todas las instituciones del sector público pongan a disposición de la ciudadanía, el libre acceso a la información institucional (estructura orgánica, bases legales, regulaciones, metas, objetivos, presupuestos, resultados de auditorías, etc.), a través de sus sitios web, bajo este mismo contexto las disposiciones contenidas en la Constitución Política del Ecuador vigente, en su capítulo tercero de las Garantías Jurisdiccionales de sus secciones cuarta y quinta de los Art. 91 y 92 sobre la acción de acceso a la información pública y acción de Habeas Data, también se establece dichas garantías. (Ureta, 2009)

2.4.1.2 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos:

La Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos está conformada por cinco títulos conteniendo cada uno varios capítulos y artículos 1) Título Preliminar. (Ureta, 2009)

- De las Firmas electrónicas, certificados de firmas electrónicas, entidades de certificación de información, organismos de promoción de los servicios electrónicos, y de regulación y control de las entidades de certificación acreditadas.
- De los servicios electrónicos, la contratación electrónica y telemática, los derechos de los usuarios, e instrumentos públicos.
- De la prueba y notificaciones electrónicas.
- De las infracciones informáticas.

A través de esta ley se rigen las transmisiones de mensajes de datos, haciendo uso de los principios jurídicos. La información y el contenido que incluyen los mensajes de datos son realmente importantes. Para interpretar la ley y la Propiedad Intelectual es necesario regirse por la legislación de Ecuador y los tratados extranjeros que han sido añadidos a las leyes ecuatorianas. Estas leyes permiten proteger la integridad de los datos y confidencialidad de los mensajes, y se define qué se entenderá por la violación de estos.

2.4.1.3 Ley de Propiedad Intelectual:

La Ley de Propiedad Intelectual (LPInt.), publicada en el Registro Oficial N° 320 del 19 de Mayo de 1998, nace con el objetivo de brindar por parte del Estado una adecuada protección de los derechos intelectuales y asumir la defensa de los mismos, como un elemento imprescindible para el desarrollo tecnológico y económico del país. El organismo nacional responsable por la difusión, y aplicación de las leyes de la Propiedad Intelectual en el Ecuador es el INSTITUTO ECUATORIANO DE PROPIEDAD INTELECTUAL (IEPI), el mismo que cuenta con oficinas en Quito, Guayaquil y Cuenca. Es una persona jurídica de derecho público, con patrimonio propio, autonomía administrativa, económica, financiera, y operativa, con sede en la ciudad de Quito. (Ureta, 2009)

2.4.1.4 Ley Especial de Telecomunicaciones:

La Ley Especial de Telecomunicaciones fue publicada en el Registro Oficial N° 996 del 10 de Agosto de 1992, en el que se declara que es indispensable proveer a los servicios de telecomunicaciones de un marco legal acorde con la importancia, complejidad, magnitud tecnología y especialidad de dichos servicios, así como también asegurar una adecuada regulación y expansión de los sistemas radioeléctricos, y servicios de telecomunicaciones a la comunidad que mejore de forma permanente la prestación de los servicios existentes. La Ley Especial de Telecomunicaciones tiene por objeto normar en el territorio nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos e información de cualquier naturaleza por hilo radioelectricidad, medios ópticos y otros sistemas electromagnéticos. (Ureta, 2009)

2.5 Idea a Defender

Para la investigación se plantea la siguiente idea a defender como una posible solución al problema plateado:

Si se implementan metodologías adecuadas para el Análisis Digital en el Laboratorio de Informática Forense de la Universidad de Guayaquil, específicamente en la Facultad de Ciencias Matemáticas y Físicas se podrá hacer uso correcto de las instalaciones, analizar evidencia digital apropiadamente como método de aprendizaje para los estudiantes así como en casos de delitos informáticos que ocurran en el país y por consiguiente obtener evidencias que constituyan pruebas sólidas ante la ley.

2.6 Definiciones Conceptuales

logs: Son registros que se generan por medio de sistemas informáticos, generalmente almacenados para determinar acciones realizadas por dichos sistemas.

Phishing: Según Moya (2013) se basa en la interferencia en el proceso de búsqueda de un nombre de dominio, es decir modifica fraudulentamente la resolución del nombre de dominio enviando al usuario a una dirección IP distinta. En este tipo de fraude, los usuarios inescrupulosos envían disímiles mensajes falsos que se originan en sitios web reconocidos o para los usuarios, como bancos o la empresa de las tarjetas de crédito de dicho usuario. De esta forma, logran que los mensajes que se envían parezcan oficiales, y así consiguen engañar a muchos usuarios. Las personas se confían, al notar seguridad en el envío y responden incluyendo sus números de tarjetas de crédito, las contraseñas, así como información referente a sus cuentas y datos personales.

Smartphone: es un teléfono celular inteligente que cuenta con utilidades avanzadas y aplicaciones similares a las de un computador.

Bluesnarfing: Es posible, en dispositivos de ciertas marcas, conectar con dicho dispositivo sin alertar al propietario, consiguiendo acceso a partes restringidas de los datos almacenados, incluyendo la agenda en su totalidad (y cualquier imagen u otros datos que vayan asociados con las entradas de la misma), calendario, reloj, propiedades, registro de cambio, IMEI. (Macho, 2006)

Función hash: es una función algorítmica que recibe parámetros de entrada que dan como resultado una cadena de números enteros. Este resultado cambia según los parámetros que recibió. Es frecuentemente usado para validar integridad y autenticación de datos.

Checksum: es una función hash que detecta la integridad de datos realizando una verificación al inicio y otra al final del envío de los mismos.

Malware: El término malware (también conocido como software malicioso o software malintencionado) hace referencia a todo tipo de programas diseñados específicamente para dañar un ordenador o una red o para obtener algún tipo de beneficio o hacer mal uso del mismo. El malware en muchos casos se instala en nuestro ordenador sin nuestro conocimiento, generalmente a través de descargas o enlaces de carácter engañoso que simulan ser contenido en el que podríamos estar interesados. (Jaen, 2012 , pág. 3)

Ciberacoso: Para algunos autores, como Bill Belsey el término hace referencia a la utilización de cualquiera de los medios propios de las nuevas tecnologías para transmitir información difamatoria y una comunicación hostil por parte de un individuo o grupo, con la finalidad de dañar a otro ya sea a través de E-mail, teléfono móvil, sitio Web personal, foros y mensaje de texto inmediato (msm). En cambio, para otros autores, como Inda Klein el término se circunscribe a la población de los menores de edad y al uso de medios tecnológicos más personales, como emails anónimos, mensajería instantánea (Messenger) o mensajes de texto a través del móvil, quedando fuera del concepto el uso de sitios web o foros para difamar. (Parés, 2007)

CAPÍTULO III

METODOLOGÍA

3.1 Diseño de la Investigación

3.1.1 Modalidad de la investigación

Una investigación es un proceso sistemático, organizado y objetivo, cuyo propósito es responder a una pregunta o hipótesis y así aumentar el conocimiento y la información sobre algo desconocido. Asimismo, la investigación es una actividad sistemática dirigida a obtener, mediante observación, la experimentación, nuevas informaciones y conocimientos que necesitan para ampliar los diversos pos de la ciencia y la tecnología.

Se define investigación al acto de ejecutar tareas experimentales y científicas de manera sistemática con el fin de incrementar el entendimiento sobre una ciencia específica y de esta manera aumentar el conocimiento científico, sin pretender en un comienzo alguna aplicación práctica (Cheesman, 2012).

Una parte considerable de la investigación, para este trabajo es bibliográfica, ya que el tema se desarrolla buscando, recopilando y realizando síntesis bibliográficas sobre la información teórica existente, lo cual permite obtener una visión panorámica sobre la rama estudiada. Una parte de la investigación se basa en los estudios y documentos literarios sobre Informática Forense, el cual constituye el tema fundamental de este trabajo.

La clasificación de la investigación en cuanto al grado de atracción, se considera es aplicada, debido a que los conocimientos teóricos adquiridos, como parte del análisis metodológico serán aplicados para la puesta en práctica del Laboratorio Forense en la Universidad de Guayaquil, específicamente en la Facultad de Ciencias Matemáticas y Físicas de la Carrera de Ingeniería en Networking y Telecomunicaciones.

Específicamente, la investigación aplicada, también denominada práctica o empírica, procura aplicar conocimientos obtenidos al mismo tiempo que se consiguen otros luego de efectuar la experiencia fundada en investigación (Cordero, 2009).

Este concepto resume claramente que el tipo de investigación permite generar conocimientos mejorados y más eficientes. Con lo que se puede afirmar que el desarrollo de la tesis facilitará conocimientos sobre la Informática Forense y contribuirá a difundir esta ciencia en el país.

La teoría sobre la cual se indaga, sirve como fundamento para la tesis, la misma incluye un porcentaje que está constituido por el estudio de campo que complementa todo el estudio llevado durante la realización de la investigación.
Se basa y está fundamentada en la ciencia del crecimiento de la actividad forense en la informática. La definición de la informática forense, sus fundamentos, análisis, y las herramientas que se usan en todo el mundo para complementar esa ciencia constituyen parte del desarrollo de la presente investigación.

Según la naturaleza de la información la investigación es cuantitativa, ya que se obtienen datos cuantitativos. Según el lugar, la investigación es de laboratorio, pues se crea el ambiente para la misma, buscando que sea limitado y que se relacionen con dicho estudio solamente las personas involucradas.

3.1.2 Tipo de investigación

El tipo de investigación que se realiza mediante este trabajo es exploratorio, debido a que el tema investigado no es ampliamente conocido por el autor del trabajo; por lo tanto, es necesario buscar, indagar e investigar lo mejor posible para obtener los conocimientos teóricos necesarios, los cuales puedan servir de fundamento para la posterior propuesta.

También se define la investigación como descriptiva, ya que se mencionan conceptos y características de la rama que se estudia teniendo en cuenta el criterio ofrecido por algunos especialistas. Dentro del análisis realizado se

describe la Informática Forense, se definen las normativas legales que la rigen dentro del país, entre otros aspectos importantes.

De igual modo, se describen las herramientas que son utilizadas para el análisis de la evidencia digital, de las cuales se resumen algunas características que fundamentan el estudio y servirán para constituir la propuesta de la investigación. El diseño del trabajo es cuasi-experimental, el cual se utiliza para realizar la investigación con el apoyo de un grupo de estudiantes, perteneciente a la Universidad de Guayaquil.

3.1.3 Métodos

Los métodos utilizados para la realización de la investigación son:

El método inductivo, el cual alcanza desenlaces generales a partir de indicios particulares. Se trata de un método común, en el cual se distinguen cuatro pasos principales: la observación de las situaciones para su exploración; la clasificación y el estudio de estas; la derivación inductiva partiendo de los hechos para lograr obtener una generalización; y la contrastación (Hernández Sampieri R. , 2010).

El método deductivo según Pagot (2010) puntualiza “un fenómeno o problema desde el todo hacia las partes, o sea examina la concepción para llegar a las especificaciones de las partes del todo”.

Se puede afirmar el estudio es **inductivo-deductivo** porque se realizó una exploración previa para conocer la situación actual sobre los ataques informáticos más relevantes que han ocurrido dentro del país y partiendo de estos hechos ocurridos, se realiza un análisis para obtener una propuesta que servirá como resultado general a la situación existente. Además, se realiza un estudio de las falencias que se refieren a este tema, teniendo en cuenta los estudios, datos y valoraciones realizados fuera del país, llegando más adelante a la ocurrencia de delitos informáticos dentro de Ecuador.

La naturaleza de la investigación es de acción pues, su resultado permitirá brindar soluciones a los problemas que existen en esta área, beneficiando a los

usuarios que están vinculados a la Universidad y a los externos. Además, se define la realización del análisis y síntesis como el método que permite determinar y describir los elementos que conforman una realidad y además organizar la información más importante, clasificada a partir de criterios ajustados a un propósito (Sánchez, 2009).

Estos procesos dependen de tres elementos fundamentales: 1) La información previa con que cuenta el investigador que desarrollará la tarea, 2) su destreza en la perspicacia del detalle y de relaciones novedosas entre elementos de la realidad objeto de estudio y 3) los objetivos de la investigación, que permitirán el establecimiento de criterios para identificar la información principal y organizarla en la elaboración de la síntesis. (Novak, 1998)

El uso de estos métodos se ve evidenciado dentro de la investigación, justo cuando se lleva a cabo un análisis documental de la información existente sobre la informática forense y luego se sintetiza todo el contenido para extraer conceptos, definiciones y características más importantes que complementen esta investigación.

3.1.4 Población y Muestra

Población:

"La población constituye el conjunto de elementos que forma parte del grupo de estudio, por tanto, se refiere a todos los elementos que en forma individual podrían ser cobijados en la investigación" (Guachichullca, 2015, pág. 29). Quienes serán beneficiados principalmente con este proyecto serán los estudiantes de Ingeniería en Networking y Telecomunicaciones, los cuales son un total de 1522 y definirán la población.

Muestra: La muestra se utiliza en todas las ocasiones en que no es posible o conveniente realizar un censo. La muestra constituye una parte de la población. Para que una muestra sea representativa, y por lo tanto útil, debe representar las similitudes y diferencias encontradas en la población y ejemplificar las características de la misma. Cuando se dice que una muestra es significativa, se

indica que reúne aproximadamente las características de población que son importantes para la investigación. (Cuesta, 2012)

El estudio que se lleva a cabo, está enfocado hacia los estudiantes y profesores que se desempeñan o que de alguna manera tienen relación con el área tecnológica. Se necesita trabajar con aquellos que estudian carreras tecnológicas, así como profesores especializados en esta rama, pues son estos los que pueden apoyar la investigación con total claridad y dominio.

Para delimitar la muestra es necesario remitirse a la Universidad de Guayaquil, Carrera de Ingeniería en Networking y Telecomunicaciones la cual está compuesta por 1522 estudiantes. Por lo tanto, la población de esta investigación está constituida por los alumnos que estudian telecomunicaciones.

CUADRO DISTRIBUTIVO DE LA POBLACIÓN

CUADRO N° 7

Población	Cantidad
Estudiantes	1522
Total	1522

Elaborado por: John Larrea

Fuente: Universidad de Guayaquil

Para el calcular el tamaño de la muestra se utilizó la siguiente fórmula:
Por lo que se tomó la siguiente fórmula, para el cálculo de su muestra según (Torres J. C., 2012).

$$\mathrm{n} = \frac{Z^2 * p * q * N}{d^2(N-1) + Z^2 * p * q}$$

Dónde:

N = Total de la población = 1522 individuos.

Z= 2.576 al cuadrado (si la seguridad es del 99%)

p = proporción esperada (en este caso 5% = 0.05)

q = 1 – p (en este caso 1-0.05 = 0.95)

d = precisión (en su investigación use un 5%).

n = tamaño de la muestra

Luego de realizar los cálculos pertinentes la muestra queda conformada por:

CUADRO DISTRIBUTIVO DE LA MUESTRA

CUADRO N° 8

Estrato	Población	Muestra
Alto	1522	235
Total		235

Elaborado por: John Larrea

Fuente: Universidad de Guayaquil

3.1.5 Técnicas e instrumentos de recolección de datos

Para realizar el presente estudio y obtener los datos necesarios se utilizará una técnica de campo, de tipo documentales, las cual es esencial, en la recolección de información: la encuesta.

Encuesta

Como parte de la investigación, es necesario aplicar una encuesta a los alumnos seleccionados que formaran parte de la muestra. La opinión de ellos será un puntal fundamental en la realización de la propuesta para conformar el laboratorio forense en la Universidad de Guayaquil, con el cual se solucionarán los problemas de ataques informáticos existentes en el país a partir de las importantes actividades a desarrollar sobre la evidencia digital.

La encuesta es una herramienta de la investigación en la cual se realiza una lista de preguntas conocida como cuestionario con el objetivo de conseguir información. La encuestación es el procedimiento que se usa para la recolección de información cuantitativa a través de preguntas bien estructuradas a los integrantes de una muestra (Alelú, 2008).

Para realizar la encuesta, se tendrán en cuentas otras referencias importantes como la que ofrece Hernández Sampieri, Collado Fernández y Batista Lucio (2011) los cuales definen que los cuestionarios aplicados, deben presentar preguntas cerradas, abiertas y mixtas. Los instrumentos que se utilizarán para llevar a cabo la entrevista y la encuesta, son:

Guión de entrevista: Es el instrumento que se utiliza para definir, las preguntas de la entrevista a aplicar. A través de él se definen todas las preguntas que reciben los entrevistados, y permite la fácil recolección de datos y respuestas sobre un tema en particular.

Cuestionario: Se define como un mecanismo que se utiliza con el fin de recopilar información para realizar investigaciones cuantitativas, principalmente las que usan el método de encuestas. Dicho de otro modo es un instrumento que le permite al investigador establecer una serie de preguntas para recopilar información organizada sobre una agrupación de personas definida como muestra, para obtener los resultados se cuantifican los datos de las respuestas para determinar el comportamiento de la población o deducir ciertas variables sobre el tema a tratarse (Meneses, 2011).

Se define entonces que el cuestionario es la técnica que se utilizará como parte de la metodología de la encuesta a aplicar. Los pasos que conforman el diseño del cuestionario ayudarán a recoger los datos deseados. Los instrumentos serán elaborados de forma detallada, y a estos solo tendrá acceso, el autor de la investigación, que será quien hará uso de los mismos en la búsqueda de información para apoyar y justificar la investigación. De tal modo que se garantiza la confiabilidad y la validez de los instrumentos.

3.1.6 Recolección de la información

Los instrumentos de navegación son los más utilizados en la actualidad. Una de las técnicas más utilizadas es la lectura comprensiva, investigativa, informativa y/o analítica. Este instrumento abarca notables recursos para la investigación,

pues la tesis está estructurada a partir de un estudio previo, por lo que la lectura es esencial para la investigación.

A través de la lectura se obtuvieron datos de ataques informáticos, sobre la evidencia, así como la utilización de herramientas forenses para la captura de evidencias. También se conocieron las leyes y tratados fundamentales sobre la informática forense. A través de la lectura e investigación previas, se publicaron conceptos fundamentales ofrecidos por autores conocidos, que permiten sustentar este estudio. Las técnicas y herramientas para la recolección de datos, fueron aplicadas y utilizadas el día 16 de Agosto de 2016 a las 6:pm en la Universidad de Guayaquil, en algunas de las aulas pertenecientes a la carrera de Ingeniería en Networking y Telecomunicaciones. Se tuvo en cuenta la cantidad de estudiantes antes mencionados, que constituyen la muestra de la investigación.

3.1.7 Procesamiento y análisis

Para analizar y procesar los datos, la técnica utilizada, fue la revisión minuciosa de los datos obtenidos, procesando la información ordenada, que constituyera un suplemento para el desarrollo del trabajo.

Luego de esta etapa, se procede a concluir, ofreciendo un criterio sobre los resultados alcanzados. Los criterios definidos ayudarán a sustentar el por qué, de la propuesta de esta investigación, justificarán con creces la necesidad existente o no de la creación del Laboratorio de Informática Forense con sus respectivas metodologías de trabajo en la entidad mencionada.

Análisis de la encuesta aplicada

La encuesta aplicada a los estudiantes, arrojó diversas respuestas dependiendo de las preguntas realizadas. La misma cuenta con 9 preguntas que ayudarán a corroborar según las respuestas ofrecidas, la necesidad de llevar a cabo los procedimientos para el laboratorio forense en la Universidad.
Luego de aplicar la encuesta, llega el momento de analizar los datos arrojados. Seguidamente se muestran las respuestas por preguntas realizadas.

Pregunta N° 1: ¿Conoce usted qué es un Laboratorio de Informática Forense?

El 32% de los encuestados contestaron que si conocen qué es un Laboratorio de Informática mientras que el 68% restante dijo que no. Este resultado da a entender que la ciencia de la informática forense no es muy conocida en nuestro entorno.

RESPUESTA PRIMERA PREGUNTA DE LA ENCUESTA

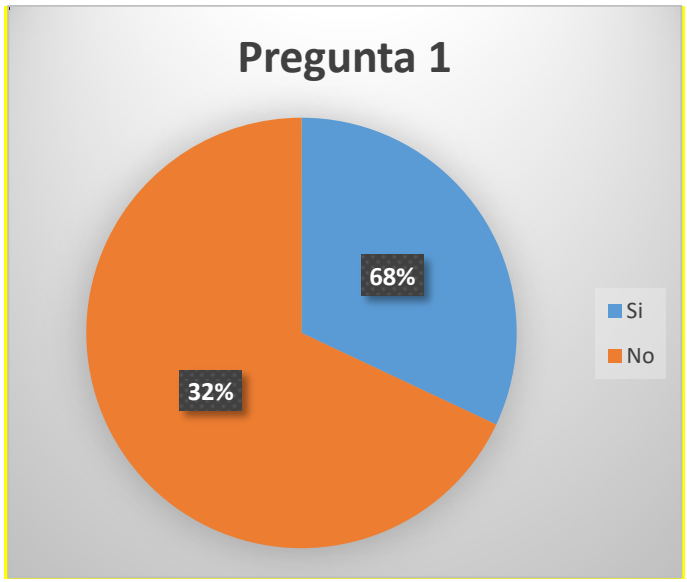
CUADRO N° 9

Alternativas	Frecuencia	Porcentaje
Si	75	32%
No	160	68%
Total	235	100%

Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Gráfico 5: Pregunta N° 1



Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Pregunta N° 2: ¿Ha recibido temas prácticos sobre Análisis Digital Forense?

Un grupo que representa el 12% respondió que han recibido temas prácticos sobre el análisis digital forense y el 88% dijo que no. Se muestra que son muy pocos los estudiantes que recibido algún tema práctico sobre esta rama.

RESPUESTA SEGUNDA PREGUNTA DE LA ENCUESTA

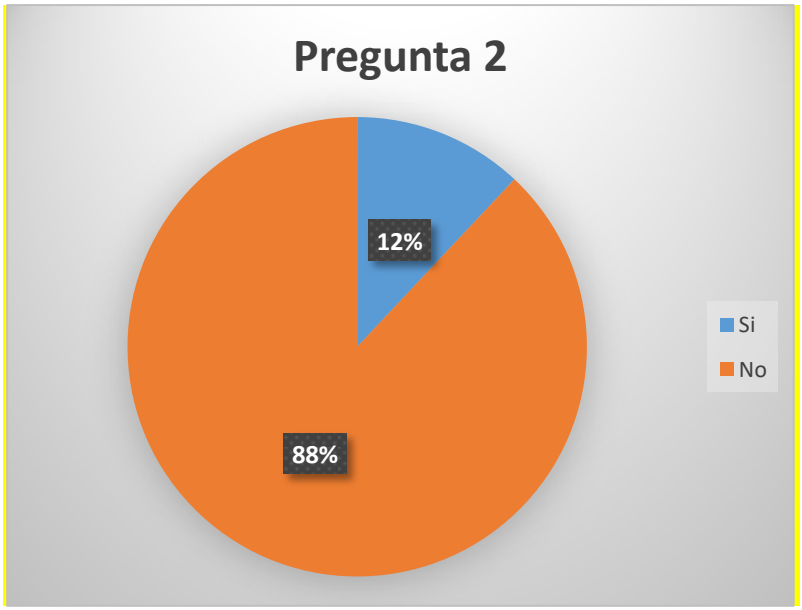
CUADRO N° 10

Alternativas	Frecuencia	Porcentaje
Si	28	12%
No	207	88%
Total	235	100%

Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Gráfico 6: Pregunta N° 2



Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Pregunta N° 3: ¿Cree usted que aprendería más sobre la Informática Forense haciendo actividades prácticas?

El 92% de los encuestados considera que aprenderían más sobre la informática forense a través de las actividades prácticas, y solo el 8% opina que no. La gran mayoría de estudiantes consideran que el tema mencionado requiere actividades prácticas.

RESPUESTA TERCERA PREGUNTA DE LA ENCUESTA

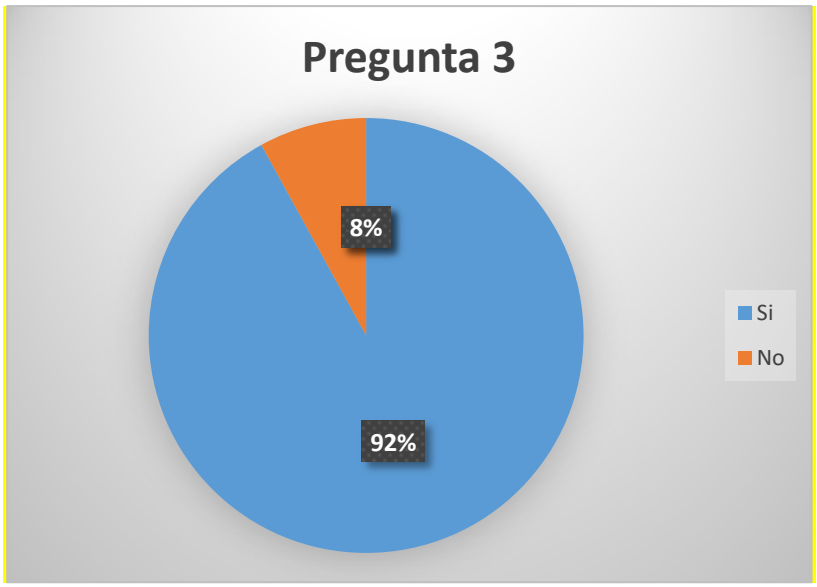
CUADRO N° 11

Alternativas	Frecuencia	Porcentaje
Si	216	92%
No	19	8%
Total	235	100%

Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Gráfico 7: Pregunta N° 3



Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Pregunta N° 4: ¿Cree usted que la Carrera de Ingeniería en Networking y Telecomunicaciones debería contar con un Laboratorio de Informática Forense?

El 90% de los alumnos respondió que sí, y solo el 10% no otorga importancia a la implementación de un Laboratorio de Informática Forense para la carrera.

RESPUESTA CUARTA PREGUNTA DE LA ENCUESTA

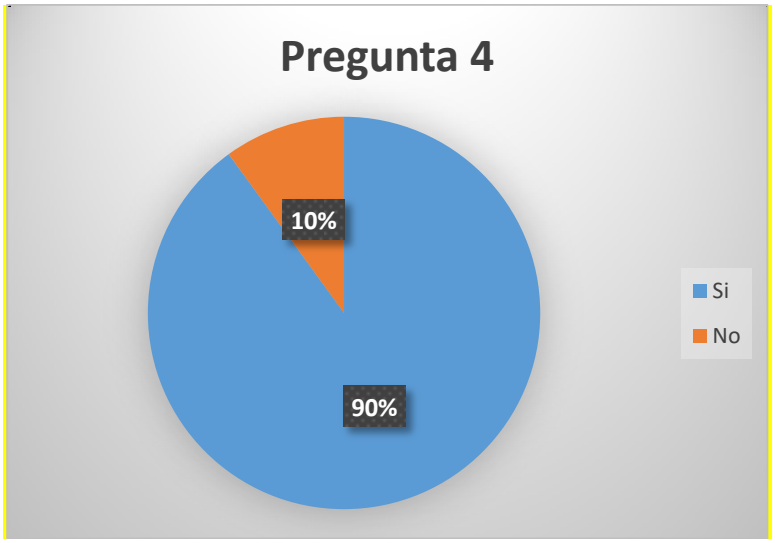
CUADRO N° 12

Alternativas	Frecuencia	Porcentaje
Si	212	90%
No	23	10%
Total	235	100%

Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Gráfico 8: Pregunta N° 4



Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Pregunta N° 5: ¿Usted conoce qué es la evidencia digital?

El 46% de los encuestados respondió que si conocen sobre la evidencia digital y el 54% dijo que no. poco menos de la mitad de los alumnos tienen conocimientos sobre evidencia digital, la otra parte desconoce del tema.

RESPUESTA QUINTA PREGUNTA DE LA ENCUESTA

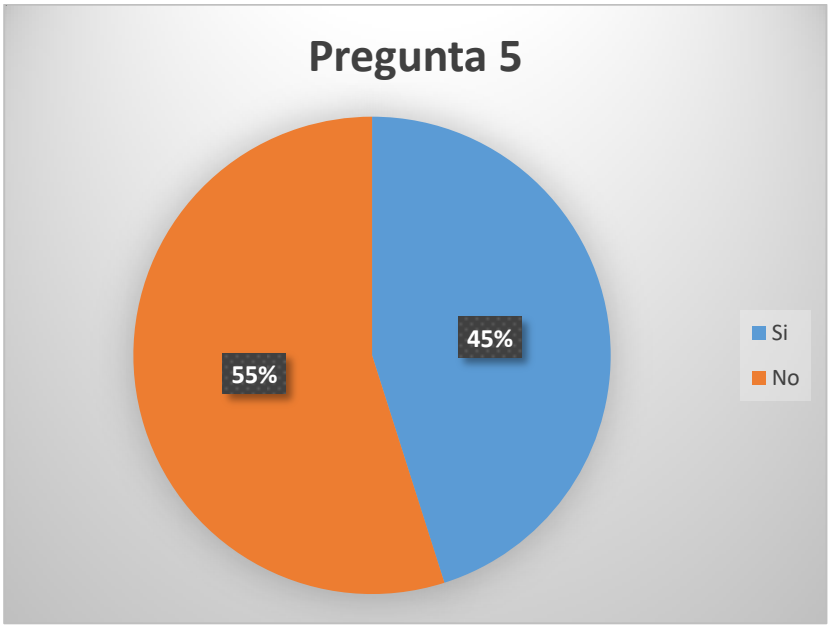
CUADRO N° 13

Alternativas	Frecuencia	Porcentaje
Si	108	46%
No	127	54%
Total	235	100%

Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Gráfico 9: Pregunta N° 5



Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Pregunta N° 6: ¿Conoce usted de la existencia de normas y procedimientos utilizados en la manipulación de evidencia digital?

A esta pregunta, el 22% de los encuestados respondió que sí conocen sobre las normas y procedimientos que se utilizan para manipular la evidencia digital, y el 78% dijo que no conoce al respecto.

RESPUESTA SEXTA PREGUNTA DE LA ENCUESTA

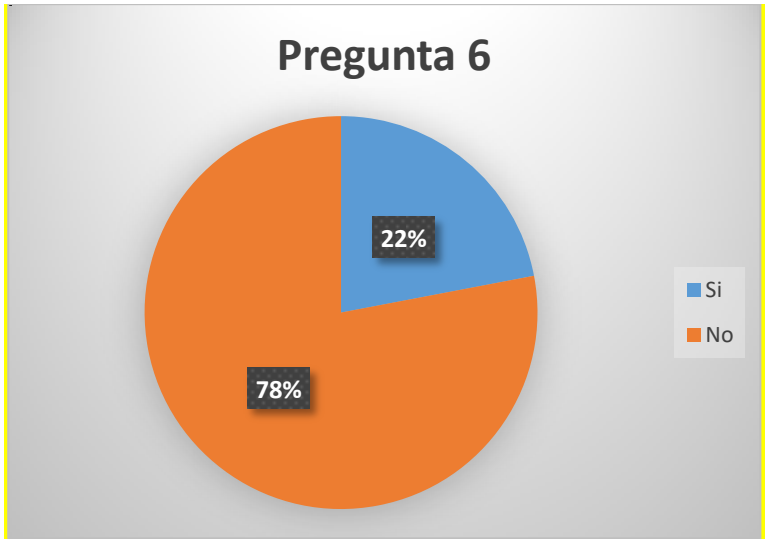
CUADRO N° 14

Alternativas	Frecuencia	Porcentaje
Si	52	22%
No	183	78%
Total	235	100%

Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Gráfico 10: Pregunta N° 6



Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Pregunta N° 7: ¿Deberían existir normas y procedimientos para el uso adecuado de las instalaciones en un Laboratorio de Informática Forense?

El 96% de los alumnos encuestados consideran que deberían existir procedimientos para utilizar adecuadamente los medios dentro de un Laboratorio de Informática Forense. La gran mayoría considera que si se debe contar con normas y procedimientos para el uso de las instalaciones del Laboratorio.

RESPUESTA SÉPTIMA PREGUNTA DE LA ENCUESTA

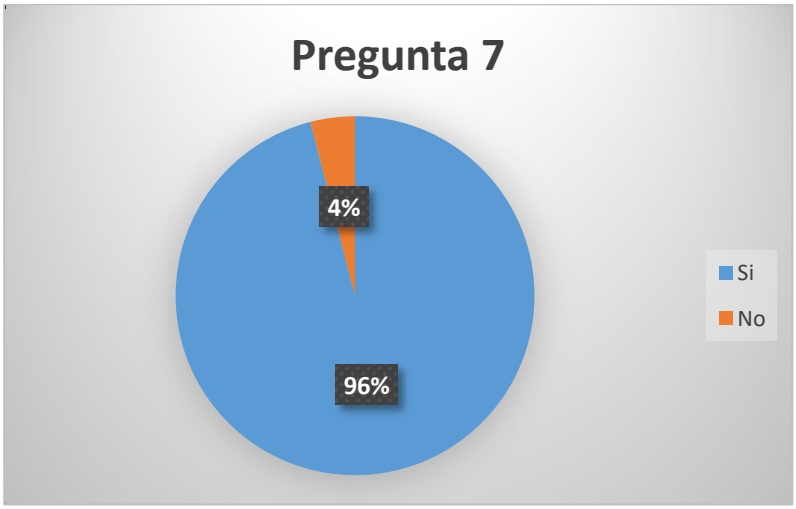
CUADRO N° 15

Alternativas	Frecuencia	Porcentaje
Si	226	96%
No	9	4%
Total	235	100%

Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Gráfico 11: Pregunta N° 7



Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Pregunta N° 8: ¿Considera usted necesario el uso de documentos y registros correspondientes a custodia, almacenamiento y análisis de la evidencia digital?

El 92% de los encuestados piensan que es importante el uso de documentos y registros para custodiar, almacenar y analizar la evidencia digital y solo el 8% considera que no es necesario.

RESPUESTA OCTAVA PREGUNTA DE LA ENCUESTA

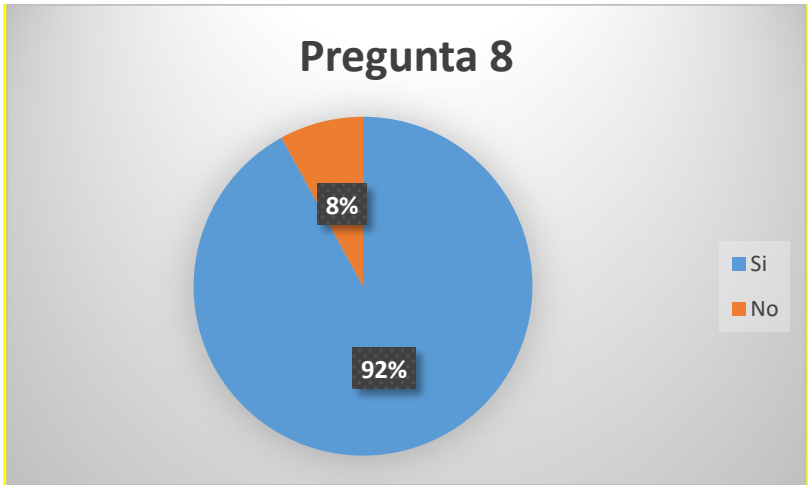
CUADRO N° 16

Alternativas	Frecuencia	Porcentaje
Si	216	92%
No	19	8%
Total	235	100%

Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Gráfico 12: Pregunta N° 8



Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Pregunta N° 9: ¿Se deberían aplicar procedimientos para evitar la incorrecta manipulación de la evidencia digital durante la recolección de la misma en la escena del delito?

El 96% de los alumnos dijo que si se debe recolectar la evidencia siguiendo un procedimiento y solo el 4% piensa que un procedimiento no es necesario.

RESPUESTA NOVENA PREGUNTA DE LA ENCUESTA

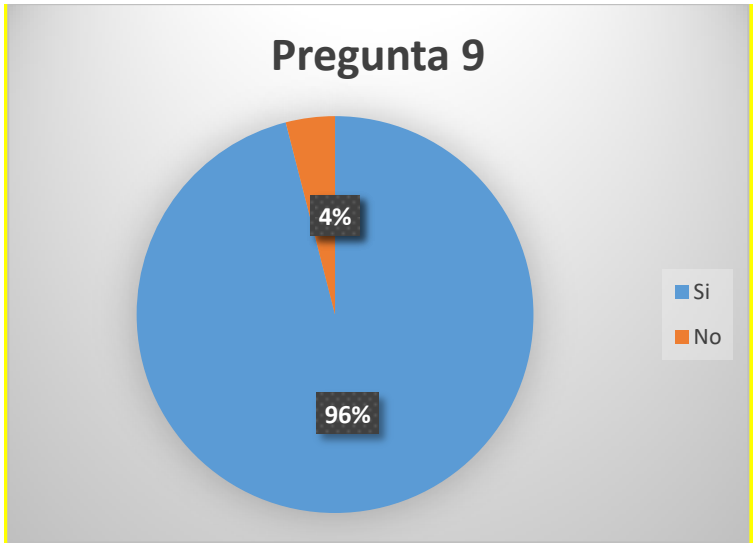
CUADRO N° 17

Alternativas	Frecuencia	Porcentaje
Si	226	96%
No	9	4%
Total	235	100%

Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

Gráfico 13: Pregunta N° 9



Elaborado por: John Larrea

Fuente: Encuesta a estudiantes de Ingeniería en Networking

3.1.8 Validación Idea a Defender

Los resultados obtenidos, luego de aplicar la encuesta, a los estudiantes corroboran la necesidad de la puesta en práctica del Laboratorio de Informática Forense en la Universidad de Guayaquil con sus respectivas normas políticas y procedimientos, para adquirir los conocimientos tanto teóricos como prácticos relacionados con la rama de la Computación Forense y que desde este lugar se trabaje en pos de evitar los delitos informáticos en el país, haciendo uso de la metodología y herramientas propuestas.

Gran parte de los encuestados afirmaron desconocer qué es un Laboratorio de Análisis Forense lo cual confirma que en nuestro medio a pesar de estar en una carrera tecnológica no se ha prestado la importancia del caso a este tema que va muy ligado con la seguridad de la información.

La mayoría de los entrevistados asintió que no han recibido nunca prácticas sobre el análisis de la evidencia digital forense, lo cual se debe a que no se cuenta con un Laboratorio con las características adecuadas para llevarlas a cabo en las instalaciones de la carrera.

Un porcentaje elevado piensa que si realizan actividades prácticas obtendrían mayores conocimientos sobre esta materia y mejoraría su aprendizaje; esto se debe a que es una ciencia muy aplicativa y de campo, por lo cual se requiere de actividades prácticas para obtener experiencia .

La mayoría de los encuestados afirma que es importante implementar un Laboratorio de Análisis Forense Digital para la carrera de Ingeniería en Networking y Telecomunicaciones, lo que contribuye un soporte para la propuesta a realizar.

Por otro lado, aproximadamente la mitad de los alumnos no conoce que es la evidencia digital, algo que deben conocer cada uno de ellos al pertenecer a esta carrera, ya que la seguridad de la información es un aspecto fundamental de la

tecnología. Este y otros temas quedarían claros con la puesta en práctica de la solución propuesta.

Acerca de las normas y procedimientos utilizados en la manipulación de evidencia digital solo un pequeño grupo de estudiantes tiene conocimiento, por otro lado gran parte de los encuestados afirma desconocer su existencia y su aplicación.

Sobre las normas y procedimientos a llevar a cabo dentro de un Laboratorio de Análisis Digital Forense, la gran mayoría asintió estar de acuerdo en que se las aplique para el uso adecuado de las instalaciones, lo que hace evidente que se debe implementar una metodología apropiada para el uso del Laboratorio.

La mayoría de los encuestados afirma la necesidad de documentación para todos los procesos involucrados con la evidencia digital como lo son la custodia, almacenamiento y análisis, de los cuales se llevará un registro detallado que servirá para garantizar la integridad de la evidencia.

Acerca de aplicar procedimientos para la debida recolección de evidencia en la escena del delito, solo un pequeño grupo indicó que no era necesario, mientras que en su mayoría afirmaron la necesidad de los mismos para su correcta manipulación.

Con los datos recopilados, se puede afirmar que es inminente la necesidad de crear un Laboratorio de Informática Forense que cuente tanto con normas así como procedimientos adecuados para la recolección, traslado, almacenamiento y análisis de evidencia digital, para poder obtener pruebas que constituyan un sustento legal, que se puedan servir de apoyo para sancionar a todo atacante que incurra en estos delitos.

Así como facilitar a los estudiantes de la carrera las herramientas necesarias para que puedan aprender todo lo necesario de la Informática Forense, lo cual contribuirá además a que estos se gradúen con los contenidos sólidos y adecuadamente impartidos.

CAPÍTULO IV

PROPUESTA TECNOLÓGICA

4.1 Análisis de factibilidad

Las organizaciones realizan estudios de factibilidad para comprobar si el negocio o producto propuesto tendrá resultados positivos o negativos y cuáles son los parámetros que se deberían cumplir para obtener éxito, además de los efectos que causará sobre el medio ambiente (Ramírez, 2013).

El principal objetivo primordial de un análisis de factibilidad se fundamenta en la exigencia de que se documente y justifique todas las inversiones a realizar demostrando que el país se vea beneficiado de las soluciones propuestas tanto en la parte técnica, económica como ambiental (Ramírez, 2013).

Según Luna (1999) **el estudio de factibilidad permite:**

- Saber si podemos producir algo.
- Conocer si la gente lo comprará.
- Saber si lo podremos vender.
- Definir si tendremos ganancias o pérdidas.
- Definir en qué medida y cómo, se integrará a la mujer en condiciones de equidad.
- Definir si contribuirá con la conservación, protección y/o restauración de los recursos naturales y el ambiente.
- Decidir si lo hacemos o buscamos otro negocio.
- Hacer un plan de producción y comercialización.
- Aprovechar al máximo los recursos propios.
- Reconocer cuáles son los puntos débiles de la empresa y reforzarlos.
- Aprovechar las oportunidades de financiamiento, asesoría y mercado.
- Tomar en cuenta las amenazas del contexto o entorno y soslayarlas.
- Iniciar un negocio con el máximo de seguridad y el mínimo de riesgos posibles.
- Obtener el máximo de beneficios o ganancias. (pág. 9)

En la opinión del autor la factibilidad es el nivel con el que se puede alcanzar algo o las posibilidades que existen de lograrlo. Se basa en el estudio que realiza una empresa o entidad para corroborar si es factible o no el estudio que se está proponiendo y las circunstancias sobre las cuales se debe llevar a cabo el proyecto para que tenga éxito.

Con la puesta en práctica del laboratorio forense en la Universidad, se obtendrán disímiles beneficios sociales, científicos, humanos y técnicos.

4.1.1 Factibilidad Operacional

Mediante la factibilidad operacional es posible determinar la probabilidad de que la funcionalidad de un nuevo sistema sea la correcta. Se debe considerar que el sistema propuesto no debe ser de un manejo complejo para que el usuario no tenga inconvenientes y cada función del mismo debe ser detallado para facilitar la comprensión del mismo (Sojo, 2008).

Para garantizar la obtención de resultados positivos se requiere que el personal que va a hacer uso de las instalaciones del Laboratorio Forense estén debidamente capacitados y altamente calificados en técnicas de análisis digital forense.

Los especialistas que formarán parte del laboratorio contribuirán al desarrollo de estrategias, las cuales tienen como fin explotar y utilizar al máximo la tecnología para la investigación dentro de la Informática Forense. El desarrollo de las metodologías se realiza en aras de lograr una infraestructura computacional óptima.

Para cumplir los objetivos planteados se definen políticas y metodologías organizacionales que permitan obtener el soporte técnico necesario dentro del laboratorio. De este modo lograr la realización de cada procedimiento con la calidad requerida.

Dentro de las políticas definidas se encuentran la estructuración del equipo de trabajo que formará parte del laboratorio, la cual se conforma por los profesores,

que son especialistas en esta rama y se encargarán de llevar a cabo el Análisis Forense y de impartir las prácticas necesarias a los estudiantes, así como:

- Vincular la tecnología informática a la administración, investigación, planificación y enseñanza.
- Clasificar la evidencia digital obtenida.
- Manipular la evidencia digital.
- Fomentar el uso de las metodologías definidas, para asegurar el correcto desarrollo de las actividades dentro del laboratorio.

Para lograr el cumplimiento de dichas actividades, se requiere tener en cuenta dos aspectos importantes como el nivel de capacitación con el que cuenta el personal para asumir y llevar a cabo la actividad en el Laboratorio de Informática Forense y las opciones existentes para garantizar dicha capacitación.

Por esta razón se define que el personal que formará parte de este trabajo estará integrado por: Un Jefe de Laboratorio, un Especialista en Hackeo Ético, un Especialista en Seguridad Informática, Especialista en Delitos Informáticos y un Especialista en Computo Forense.

Cada trabajador del laboratorio se encuentra debidamente capacitado, según las funciones que les corresponde desarrollar. Seguidamente se muestra un cuadro por cada trabajador, en las que se definen las actividades a llevar a cabo por estos.

NIVEL DE COMPETENCIA DEL JEFE DE LABORATORIO

CUADRO N° 18

<table>
<tr><th colspan="3">Entidad: Laboratorio Forense</th></tr>
<tr><td>Manual de Puestos y Funciones</td><td>Fecha:</td><td>23/8/2016</td></tr>
<tr><td colspan="3">Nivel Administrativo: Jefe de Laboratorio</td></tr>
<tr><td>Perfil de Competencias:</td><td colspan="2">Descripción:</td></tr>
<tr><td rowspan="2">Educación: Título de 3er Nivel
Experiencia: 3 años en puestos similares
Habilidades:
Ser emprendedor.
Dotes de psicología.
Capacidad de comunicación.
Liderazgo con motivación para dirigir.
Integridad moral y ética.
Capacidad de asumir responsabilidades.
Saber motivar al personal
Gran capacidad para delegar.
Creatividad.
Toma de decisiones.</td><td colspan="2">El Jefe de Laboratorio es el responsable de la representación legal, judicial y extrajudicial del proyecto, así como de la dirección del mismo. Desarrolla y define los objetivos de la organización. Planifica el crecimiento de la entidad por plazos.</td></tr>
<tr><td colspan="2">Funciones:
Conocimientos sólidos de informática forense.
Es el encargado de la vigilancia, de la organización, y el funcionamiento de la entidad.
Califica la calidad de los servicios.
Controla y evalúa al personal.
Mantiene el control de los procesos.
Claridad en la comunicación.</td></tr>
<tr><td>Relación Funcional</td><td colspan="2">Responsabilidades</td></tr>
<tr><td>Depende de:
Supervisa a:
Trabajadores de la Entidad</td><td colspan="2">Es el responsable de todas las actividades que se realizan en el laboratorio forense.</td></tr>
<tr><td>Elaboró</td><td>Revisó</td><td>Autorizó</td></tr>
</table>

Elaborado por: John Larrea
Fuente: John Larrea

NIVEL DE COMPETENCIA DEL ESP. HACKEO ÉTICO

CUADRO N° 19

<table>
<tr><th colspan="3">Entidad: Laboratorio Forense</th></tr>
<tr><td>Manual de Puestos y Funciones</td><td>Fecha:</td><td>23/8/2016</td></tr>
<tr><td colspan="3">Nivel Administrativo: Especialista en Hackeo Ético</td></tr>
<tr><td>Perfil de Competencias:</td><td colspan="2">Descripción:</td></tr>
<tr><td rowspan="2">Educación: Título de 3er Nivel
Experiencia: 1 año en puestos similares
Habilidades:
Integridad moral y ética.
Ser emprendedor.
Capacidad de comunicación.
Creatividad.
Toma de decisiones.</td><td colspan="2">Dominar conceptos y tareas sobre el hackeo ético.
Conocimientos solidos sobre criptografía y los sistemas criptográficos existentes.
Dominio de la ingeniería social.</td></tr>
<tr><td colspan="2">Funciones:
Aplicar bajo la ética profesional, los test de penetración y análisis de vulnerabilidades.</td></tr>
<tr><td>Relación Funcional</td><td colspan="2">Responsabilidades</td></tr>
<tr><td>Depende de:
Jefe de Proyecto
Supervisa a:</td><td colspan="2">El especialista en Hackeo Ético es el responsable de implementar los sistemas de seguridad.</td></tr>
<tr><td>Elaboró</td><td>Revisó</td><td>Autorizó</td></tr>
</table>

Elaborado por: John Larrea
Fuente: John Larrea

NIVEL DE COMPETENCIA DEL ESP. SEGURIDAD INFORMÁTICA

CUADRO N° 20

<table>
<tr><th colspan="3">Entidad: Laboratorio Forense</th></tr>
<tr><td>Manual de Puestos y Funciones</td><td>Fecha:</td><td>23/8/2016</td></tr>
<tr><td colspan="3">Nivel Administrativo: Especialista en Seguridad Informática</td></tr>
<tr><td>Perfil de Competencias:</td><td colspan="2">Descripción:</td></tr>
<tr><td rowspan="2">Educación: Título de 3er Nivel
Experiencia: 2 años en puestos similares
Habilidades:
Integridad moral y ética.
Ser emprendedor.
Capacidad de comunicación.
Creatividad.
Toma de decisiones.</td><td colspan="2">Dominar los tipos de virus y su acción directa.
Conocer los conceptos y características de delincuente informáticos y crackers.
Saber incluir la seguridad en las contraseñas.
Dominar contenidos de software, bases de datos, metadatos y archivos.</td></tr>
<tr><td colspan="2">Funciones:
Administrar el presupuesto de seguridad informática.
Definir la estrategia de seguridad informática del proyecto.
Detección de necesidades y vulnerabilidades de seguridad.</td></tr>
<tr><td>Relación Funcional</td><td colspan="2">Responsabilidades</td></tr>
<tr><td>Depende de:
Jefe de Proyecto
Supervisa a:</td><td colspan="2">Debe encontrar la forma para prevenir y resolver los problemas de seguridad con el costo óptimo para la entidad.</td></tr>
<tr><td>Elaboró</td><td>Revisó</td><td>Autorizó</td></tr>
</table>

Elaborado por: John Larrea
Fuente: John Larrea

NIVEL DE COMPETENCIA DEL ESP. EN DELITOS INFORMÁTICOS

CUADRO N° 21

<table>
<tr><th colspan="3">Entidad: Laboratorio Forense</th></tr>
<tr><td>Manual de Puestos y Funciones</td><td>Fecha:</td><td>23/8/2016</td></tr>
<tr><td colspan="3">Nivel Administrativo: Especialista en Delitos Informáticos</td></tr>
<tr><td>Perfil de Competencias:</td><td colspan="2">Descripción:</td></tr>
<tr><td rowspan="2">Educación: Título de 3er Nivel
Experiencia: 2 años en puestos similares
Habilidades:
Integridad moral y ética.
Ser emprendedor.
Capacidad de comunicación.
Creatividad.
Toma de decisiones.</td><td colspan="2">Conocer los tipos de delitos informáticos.
Dominar los tipos de delitos penales que constituyen delitos informáticos.
Dominar el ámbito de la aplicación de ley para la protección de datos.</td></tr>
<tr><td colspan="2">Funciones:
Definir una normativa penal, actualizada para sancionar las infracciones que se cometan.
Definir un marco penal y promover una tipificación de delitos, para evitar el alto grado de impunidad que aún existe en el país.</td></tr>
<tr><td>Relación Funcional</td><td colspan="2">Responsabilidades</td></tr>
<tr><td>Depende de:
Jefe de Proyecto
Supervisa a:</td><td colspan="2">Encargado de identificar y corroborar la existencia de un delito informático.</td></tr>
<tr><td>Elaboró</td><td>Revisó</td><td>Autorizó</td></tr>
</table>

Elaborado por: John Larrea
Fuente: John Larrea

NIVEL DE COMPETENCIA DEL ESP. EN CÓMPUTO FORENSE

CUADRO N° 22

<table>
<tr><th colspan="3">Entidad: Laboratorio Forense</th></tr>
<tr><td>Manual de Puestos y Funciones</td><td>Fecha:</td><td>23/8/2016</td></tr>
<tr><td colspan="3">Nivel Administrativo: Especialista en Cómputo Forense</td></tr>
<tr><td>Perfil de Competencias:</td><td colspan="2">Descripción:</td></tr>
<tr><td rowspan="2">Educación: Título de 3er Nivel
Experiencia: 3 años en puestos similares
Habilidades:
Integridad moral y ética.
Ser emprendedor.
Capacidad de comunicación.
Creatividad.
Toma de decisiones.</td><td colspan="2">Dominio en trabajos con dispositivos y servicios como: disco Duro, logs de seguridad, agendas electrónicas, dispositivos de Gps, impresoras, memorias usb, teléfonos móviles o celulares, credenciales de autentificación etc.</td></tr>
<tr><td colspan="2">Funciones:
Definir los antecedentes, la situación actual y el proceso a realizar para tomar las decisiones correctas referentes a la búsqueda y estrategias a seguir.
Realizar y generar las imágenes forenses que forman parte de la evidencia para realizar el análisis posteriormente.
Aplicar las técnicas a los medios duplicados para encontrar las pruebas requeridas.
Recopilar toda la información obtenida y generar un reporte final.</td></tr>
<tr><td>Relación Funcional</td><td colspan="2">Responsabilidades</td></tr>
<tr><td>Depende de:
Jefe de Proyecto
Supervisa a:</td><td colspan="2">Encargado de llevar a cabo la examinación forense digital.</td></tr>
<tr><td>Elaboró</td><td>Revisó</td><td>Autorizó</td></tr>
</table>

Elaborado por: John Larrea
Fuente: John Larrea

Según Barrios (2012) cuanto mayor sea el grado de formación y preparación del personal de la compañía, mayor será su nivel de productividad, cualitativa y cuantitativamente. Los programas de formación profesional constituyen una de las inversiones más rentables, el progreso tecnológico influye directamente y con frecuencia en los procesos empresariales.

La información ofrecida en los cuadros anteriores permite afirmar que el colectivo de trabajadores que formará parte de la puesta en marcha del laboratorio forense se encuentra capacitado para llevar a cabo sus actividades y contribuir con sus conocimientos, capacidades y trabajo al desarrollo del Laboratorio Forense Digital de la Universidad de Guayaquil, específicamente en la Carrera de Ingeniería en Networking y Telecomunicaciones.

4.1.2 Factibilidad Técnica

Se considera que la factibilidad técnica o tecnológica es la que dispone los conocimientos y habilidades en el manejo de métodos, procedimientos y funciones para el desarrollo e implantación del proyecto. Es la que indica sí disponen de materias primas e insumos, de los equipos y herramientas y del proceso productivo para el proyecto.

Nos permite evaluar si el equipo y software están disponibles y tienen las capacidades técnicas requeridas por cada alternativa del diseño que se esté planificando, también se consideran las interfaces entre los sistemas actuales y los nuevos (Ramíez Almaguer, 2009, pág. 1).

El diseño técnico del laboratorio, fue realizado por: Boris López Maxi y David Varela Porro, autores del trabajo: “Diseño, especificaciones técnicas y seguridad para la Implementación de un Laboratorio de Informática Forense para la Carrera de Ingeniería en Networking y Telecomunicaciones”; para el cual se definió que se utilizaría un área de la Universidad de poco uso.

Para la realización de este proyecto se previó la existencia de los equipos a utilizar en la conformación del laboratorio, así como las diversas instalaciones a realizar para estos dispositivos. También se ha definido que el área ambientalmente cuente con las condiciones requeridas, teniendo en cuenta que

exista la climatización requerida y que el lugar cuente con diversas vías para hacer su acceso lo mejor posible. Esto garantiza que el laboratorio forense pueda ser llevado a cabo, con los menores riesgos posibles.

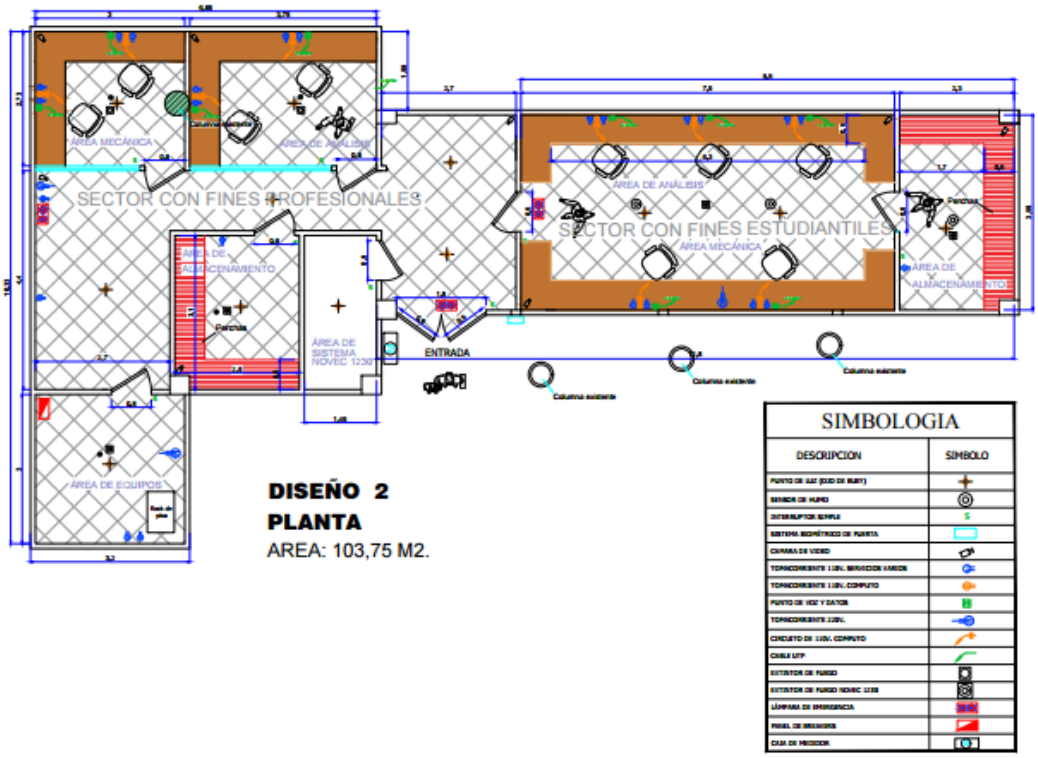
Específicamente, la entidad cuenta con una puerta de acceso, la cual facilitará a los asistentes asiduos del laboratorio acceder al él y sus respectivos dispositivos, un área de equipos de 3,2 m de ancho y 3 m de largo, donde se ubicará un rack de piso, tomacorrientes y un panel de breackers, un área de sistemas de 31,1m de ancho y 1,45m con un interruptor simple y un punto de luz, así como un área de almacenamiento, con 31,1m y 2,5 m, un tomacorriente, un extintor y un punto de luz.

El área mecánica se ubica al fondo de este laboratorio con 2,73 m y 3 m de ancho, la misma cuenta con una cámara, y varios tomacorrientes. Al lado de esta se encuentra el área de análisis, la cual cuenta con dos puntos de voz y datos y dos tomacorrientes de cómputo.

El área con fines estudiantiles, mide 3,95 m de ancho y 7,5 m de largo, esta cuenta con 5 puestos de trabajos, dos cámaras y dos puertas. En total se tienen 12 puntos de luz, 3 censores de humo, 9 interruptores simples, 1 sistema biométrico de puerta, 7 cámaras, 20 tomacorrientes de 110 V, para servicios varios, 1 tomacorriente de 220 V, 9 tomacorrientes de cómputo y circuitos de 110 V, 9 puntos de voz y datos, 2 extintores de fuego, 4 extintores de fuego Inergen, 2 paneles de breackers y una caja medidora.

Seguidamente se muestra una imagen con el diseño físico final y las especificaciones técnicas que se proponen para el laboratorio forense:

Gráfico 14: Diseño del laboratorio forense



Elaborado por: John Larrea
Fuente: (López, Varela, 2016)

4.1.3 Factibilidad Legal

Según (Lacayo, 2012) la factibilidad legal se refiere a los requerimientos legales del proyecto, para su operación y aprobación respectiva. La factibilidad legal se hace en este caso para determinar los requisitos que atenten contra el reglamento establecido en el laboratorio.

Las leyes por las cuales se regirá el laboratorio forense serán las establecidas por el gobierno ecuatoriano y mencionadas en el marco teórico, las cuales constituirán pautas y límites, para contrarrestar los hechos delictivos cometidos por intrusos y ayudarán a hacer de la evidencia digital obtenida un objeto que tenga validez legal.

Adicional a ello, se define que serán pagadas las licencias del software que se utilizarán en esta institución y que no se autoriza a ninguna entidad a hacer uso de estas en nombre de la Universidad. Tampoco se autoriza a los trabajadores del laboratorio a utilizar los activos y herramientas definidas para el laboratorio fuera del horario establecido o con objetivos no afines a las investigaciones. Además, cada trabajador deberá cumplir con las normas establecidas para el manejo de la información.

4.1.4 Factibilidad Económica

Se refiere a los recursos económicos y financieros necesarios para desarrollar o llevar a cabo las actividades o procesos y/o para obtener los recursos básicos que deben considerarse son el costo del tiempo, el costo de la realización y el costo de adquirir nuevos recursos (Cobarrubias, 2016).

4.1.4.1 Análisis costo/beneficio

En este epígrafe se define el costo aproximado de cada equipo o inversión realizada. La aplicación de la metodología que se propone contribuirá a disminuir los costos del seguimiento a los delitos. Se tuvieron en cuenta los siguientes:

Costo operativo: Para obtener el valor de este costo, se ha estimado el costo que requiere, la atención al personal para el desarrollo del proyecto. Seguidamente se muestra un cuadro de los costos por especialistas.

COSTO OPERATIVO

CUADRO N° 23

Recursos Humanos			
Cantidad de Esp.	Cargo	Costo Individual	Total
1	Jefe de laboratorio	$1200	$14.400
1	Esp. Hackeo Ético	$1000	$12.000
1	Esp. Seguridad Inf	$1000	$12.000
1	Esp. Delitos Inf	$800	$9.600
1	Esp. Cómputo Forense	$1100	$13.200
		Total	$61.200

Elaborado por: John Larrea
Fuente: John Larrea

Costo de inversión: Para conseguir el valor de este costo, se estimaron los valores del hardware y el software a utilizar en el proyecto, ya que estos representan los activos a utilizar para la puesta en práctica del laboratorio.

Durante la conformación del laboratorio forense se contará con dispositivos y computadores que permitan garantizar la velocidad de procesamiento de la información y la fiabilidad de los procesos. Dichos dispositivos y herramientas se listan a continuación.

COSTO DE INVERSIÓN

CUADRO N° 24

Recursos Tecnológicos			
Hardware			
Cantidad Rec.	Descripción	Costo/U	Total
7	Ordenadores Forenses	$2.295	$16.065
1	Celldek	$3.800	$3.800
1	Fred	$5.999	$600
1	Duplicadora RoadMasster-3	$12.995	$12.995
1	Ultrakit	$1.799	$1.799
12	Puntos de luz	$15	$180
3	Sensores de humo	$19	$57
9	Interruptores simples	$15	$135
1	Sistema Biométrico	$189	$189
7	Cámaras	$59	$413
20	Tomacorrientes 110V	$16	$320
1	Tomacorriente 220V	$16	$16
9	Puntos de Voz y Humo	$25	$225
2	Extintores de fuego	$14	$28
2	Paneles de breackers	$200	$400
1	Caja medidora	$260	$260
		Total	$37.482

Elaborado por: John Larrea
Fuente: John Larrea

Luego de haber definido los costos operativos y de inversión se procede a definir los costos de capacitación, los cuales suman $200 por cada especialista. También se especifican los costos por certificaciones de los especialistas, los que suman $350 por cada uno.

FLUJO DE PAGO
CUADRO N° 25

Recursos	Costos
Recursos Humanos	$61.200
Recursos Tecnológicos	$37.482
Capacitación	$1000.00
Certificación	$1.750
Total	$ 1099.932

Elaborado por: John Larrea
Fuente: John Larrea

COSTO DE OPERACIÓN
CUADRO N° 26

Descripción	Costo
Suministros y Gastos	$750
Costos de Impresión Manual	$50
Total	**$800**

Elaborado por: John Larrea
Fuente: John Larrea

Cabe recalcar que la propuesta presentada es sin fines de lucro, ya que representa muchos beneficios tanto para los estudiantes de la Universidad como para la sociedad.

4.2 Etapas de la Metodología del Proyecto

4.2.1 Product backlog

Es una lista detallada de las tareas a realizar durante la elaboración del proyecto donde se muestran los requerimientos y prioridades con respecto a los entregables del producto.

4.2.2 Sprint

Se menciona cada una de las acciones necesarias para completar el objetivo final.

SPRINT O HILOS DE LA METODOLOGÍA SCRUM

CUADRO N° 27

N°	SPRINT O HILOS
1	Estudio de evidencia digital
2	Clasificación de delitos informáticos
3	Análisis de Metodologías internacionales
4	Exploración de buenas prácticas recomendadas
5	Duplicado de Imágenes bit a bit
6	Extracción de código Hash
7	Análisis del diseño del Laboratorio
8	Comparación de Hardware y Software
9	Elección de cadena de custodia
10	Elaboración de registros

Elaborado por: John Larrea

Fuente: John Larrea

DESCRIPCIÓN DE LOS SPRINT DE LA METODOLOGÍA SCRUM

CUADRO N° 28

N°	HILOS	DESCRIPCIÓN	A CARGO DE:
SRPINT 1	Estudio de evidencia digital	Se realizó un estudio de normas y prácticas internacionales aplicadas en diversos Laboratorios de Análisis Forense.	John Larrea Ronquillo
	Clasificación de delitos informáticos		
	Análisis de Metodologías internacionales		
	Exploración de buenas prácticas recomendadas		
SPRINT 2	Duplicado de Imágenes bit a bit	Se definió el uso de copia bit a bit de los dispositivos y la obtención de código hash del dispositivo original y su copia.	John Larrea Ronquillo
	Extracción de código Hash		
SPRINT 3	Análisis del diseño del Laboratorio	Se ejecutó un análisis del diseño de laboratorio planteado y las herramientas a utilizar.	John Larrea Ronquillo
	Comparación de Hardware y Software		
SPRINT 4	Elección de cadena de custodia	Se estableció el cumplimiento de cadena de custodia y de formalidad de registros.	John Larrea Ronquillo
	Elaboración de registros		

Elaborado por: John Larrea

Fuente: John Larrea

4.3 Entregables del proyecto

En esta sección, se presenta la propuesta a llevar a cabo en el laboratorio forense. Esta constituye la parte más relevante de la investigación ya que es el resultado del estudio previo realizado y la contribución que se realiza a la entidad, para lograr un desarrollo adecuado de las actividades de informática forense a realizar en la institución.

- Propuesta práctica y metodológica para el Análisis Forense en el Laboratorio de Informática Forense. Ver **ANEXO 3**

4.4 Criterios de Validación de la Propuesta

Para validar la propuesta, se necesita implantar los indicadores que forman parte del proceso del laboratorio forense. Luego de implantar los indicadores se realiza un monitoreo durante los 25 o 30 días iniciales, lo que permitirá obtener los resultados sobre la monitorización de los procesos. Seguidamente se mostrará un cuadro con los resultados obtenidos:

MEDICIÓN DE LOS PROCESOS

CUADRO N° 29

Resultados del monitoreo de los procesos	
Indicador	**Resultado**
Recursos Humanos	
Herramientas de hardware	
Herramientas de sofware	

Elaborado por: John Larrea
Fuente: John Larrea

Adicionado a esto, la propuesta ha sido evaluada por los expertos de la Universidad en los temas de informática forense, los cuales constatan la validez de la propuesta, teniendo en cuenta su claridad y utilidad.

En cuanto a la claridad del contenido propuesto, se pretende constatar si este es claro para los que lo recibirán, si existen términos o palabras difíciles de comprender, si el contenido está bien relacionado con las características del trabajo y si existe la suficiente información.

Para verificar la utilidad del trabajo, es necesario constatar que el mismo sea útil para toda la sociedad y que ayude a los especialistas y estudiantes que asistan al laboratorio. Seguidamente se redactan las opiniones que forman parte de la valoración de la propuesta por parte de algunos especialistas de la Universidad.

4.4.1 Validación de la propuesta: ¨Estudio de implementación de metodologías de Análisis Forense digital aplicable en un Laboratorio de Informática Forense en la Carrera de Ingeniería en Networking y Telecomunicaciones ¨

La realización de una investigación previa, ha sido fundamental para la propuesta realizada. La misma está redactada con palabras fáciles de comprender pues, aunque se utilizan expresiones técnicas, no son difíciles de comprender, por su relación con el contenido.

El contenido cuenta con suficiente información, partiendo del problema planteado para la investigación. La metodología trazada no solo es de utilidad para los especialistas que laboraran en la entidad, sino también para la parte docente, ya que ayudará al crecimiento de los estudiantes en esta rama y que puedan elevar el bajo nivel que tienen en la informática forense.

Los especialistas que formarán parte del laboratorio, tendrán que comprometerse con la labor que realizarán y trabajar para lograr el beneficio de la sociedad. La investigación realizada puede ser de gran ayuda para el crecimiento exponencial de la informática forense y favorecer al desarrollo y conocimiento sobre esta rama. Lo cual representa una significativa ayuda para la sociedad y el ámbito tecnológico del país.

4.5 Criterios de Aceptación del Producto

La aceptación de un producto es la medida que ayuda a expresar la conformidad de un producto. O sea, el estar de acuerdo con el bien o servicio que se ofrece. Una alta aceptación significa que el resultado del producto ha sido el adecuado y esperado por todos sus interventores.

Detalle de cada especificación:

1-Nombre del Proyecto: Incluir el nombre especificado para el proyecto.

2-Identificador del Proyecto: Especificar el protocolo de aceptación. Incluir identificador del documento.

3- Identificador del Documento: Informe de verificación y validación realizado por el proveedor. Incluir identificador.

4-Aceptación Elaborada por: Informe de resultados. Incluir su identificador.

Seguidamente se muestran en un cuadro, los elementos que forman parte del proceso de aceptación del producto.

CRITERIO DE ACEPTACIÓN DEL PRODUCTO

CUADRO N° 30

Aceptación del Producto	
1-Nombre del Proyecto	
2-Identificador del Proyecto	
3-Identificador del Documento	
4-Aceptación elaborada por:	

Elaborado por: John Larrea
Fuente: John Larrea

Se da por aceptada la propuesta ¨**Estudio de implementación de metodologías de Análisis Forense digital aplicable en un Laboratorio de Informática Forense en la Carrera de Ingeniería en Networking y Telecomunicaciones** ¨

CONCLUSIONES

Como conclusiones finales de la presente investigación se puede decir que cada objetivo planteado fue cumplido exitosamente. Específicamente:

- Se analizaron diversas metodologías y procedimientos ya definidos y utilizados por instituciones internacionales para efectuar Análisis Digital Forense, lo cual permitió entender el modo de operación de dichas entidades para poder formular una propuesta detallada aplicable en el Laboratorio de Informática Forense a implementar en la Carrera de Ingeniería en Networking y Telecomunicaciones.

- A través del análisis de las metodologías estudiadas se pudieron conocer normas de buenas prácticas que optimizan el desempeño tanto del personal como de los recursos pertenecientes a un Laboratorio de Informática Forense permitiendo realizar el respaldo requerido de la evidencia encontrada, así como documentar las etapas de hallazgo, almacenamiento, análisis y entrega de dicha evidencia, partiendo de una base metodológica.

- Los procedimientos técnicos y operativos a tener en cuenta dentro del laboratorio se definieron en la propuesta de la investigación presentada en los anexos. Con los procedimientos propuestos, se garantiza la disminución del tiempo de realización de las pericias informáticas y las investigaciones previas. También se aspira obtener calidad en los procesos llevados a cabo. Se definió también como elemento fundamental, el uso de las herramientas tanto de software como hardware, además de los diferentes dispositivos que serán utilizados en el laboratorio para el procesamiento de la evidencia.

- Se estableció un control adecuado sobre la cadena de custodia con respecto a la evidencia digital con el soporte necesario en cuanto a documentación para el laboratorio. A través de la explicación sobre cómo debe llevarse a cabo el ciclo de custodia de la evidencia digital, se logra

que los especialistas del laboratorio desarrollen este proceso siguiendo métricas y obteniendo los resultados deseables y esperados para el Laboratorio.

- Se llevó a cabo una propuesta sólida, clara y detallada referente a las metodologías de trabajo dentro del Laboratorio Forense que cumplen con los estándares establecidos garantizando la integridad de la evidencia digital y facilitando la obtención de pruebas en base a ella. La metodología que se define, desde el punto de vista de la Informática Forense, especifica una estructura para guiar una investigación. Esta constituye un punto inicial para realizar el análisis de la evidencia digital dentro del Laboratorio Forense, ya que incluye el procedimiento y el tratamiento a llevar a cabo sobre la evidencia. También se puede afirmar que el trabajo realizado constituye una guía metodológica a tener en cuenta para enseñar el proceso de tratamiento de la evidencia digital a los estudiantes de la carrera de Ingeniería en Networking y Telecomunicaciones. Finalmente se puede afirmar que el desarrollo de este laboratorio permitirá favorecer a la sociedad ecuatoriana en general. Ya que a través de él se podrán revelar y dar a conocer posibles ataques, así como determinar a través de un estudio exhaustivo el infractor o perpetrador de un crimen.

.

RECOMENDACIONES

- Investigar y revisar periódicamente manuales internacionales con respecto al Computación Forense ya que de la misma manera que la tecnología presenta avances continuos, los delincuentes informáticos desarrollan nuevas técnicas para perjudicar a las personas o instituciones aprovechándose de las innovaciones tecnológicas, es por eso que se deben repasar frecuentemente metodologías existentes con el fin de poder hacer frente a nuevos tipos de delitos informáticos.

- Aplicar, utilizar en todo momento las buenas prácticas establecidas ya que fueron diseñadas con el fin de facilitar el trabajo además de permitir la obtención de resultados positivos durante el análisis de la evidencia.

- Como planes futuros del proyecto se pretende continuar perfeccionando el laboratorio con nuevas técnicas y procedimientos estandarizados. También se aspira a incorporar más profesionales para que apoyen el tratamiento de la evidencia digital dentro del área. Los especialistas que formen parte de la institución, deberán estar bien capacitados, y contar con conocimientos sólidos y experiencia en el área, ya que se requiere de un personal calificado capaz de realizar las actividades con la rigurosidad y la calidad requeridas.

- Llevar un control minucioso y respetar la documentación referida a la cadena de custodia, cumplir con las formalidades de entrega/recepción de evidencia y tener mucho cuidado durante el traslado, de la misma, es necesario que todo movimiento de la evidencia sea registrado cumpliendo las normas acerca de la custodia de la misma.

- Cumplir con la metodología de trabajo implementada para así garantizar el correcto análisis de la evidencia conservando su integridad en cualquier situación. Con ayuda de las experiencias en análisis de nuevos casos se podrá mejorar la metodología agregando o rediseñando procedimientos según la necesidad con el fin de que estos puedan ser

repetitivos y logren asegurar resultados positivos. También se deben mejorar con el transcurrir del tiempo los recursos con los que contará el laboratorio adquiriendo software licenciado, capacitando y certificando a los profesionales del área para así obtener un mayor prestigio y confiabilidad en la pericia informática.

BIBLIOGRAFÍA

Acurio, S. (2012). *Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0 .* Quito.

Aguilar, F. (2016). *Herramientas de análisis de hardware para la implementación de un laboratorio de informática forense en la Carrera de Ingeniería en Networking y Telecomunicaciones.* Guayaquil.

Alelú, M. (2008). *Estudio de Encuestas.* Madrid.

Barrios, Y. (31 de Julio de 2012). *Pymempresario*. Obtenido de Pymempresario: http://www.pymempresario.com/2012/07/la-importancia-de-la-capacitacion/

Beltrán, S. (2012). *Evidencia Digital e Informática Forense.* México.

Bogota, D., & Claudia, M. (2016). *Evidencia Digital en Colombia: Una reflexion en la práctica.* Colombia.

Bueno, E. (2003). *La investigacion cientifica: teoría y metodología. .* Zacatecas.

Cabrera, M. (2014). *La apropiación ilícita de redes sociales mediante la manipulación de claves de acceso personal como consecuencia de la falta de tipificación del delito informático en la legislación penal ecuatoriana.* Quito.

Castro, H. (2015). *TUTORIAL ANALIZADOR DE PROTOCOLOS "WIRESHARK".* Colombia.

Cheesman, S. (2012). *CONCEPTOS BÁSICOS EN INVESTIGACIÓN.* Guatemala.

Cobarrubias, C. (2016). *Desiciones sobre la factibilidad técnica económica de proyectos de inversión .* Venezuela.

Cordero, S. (2009). *LA INVESTIGACIÓN APLICADA: UNA FORMA DE CONOCER LAS REALIDADES CON EVIDENCIA CIENTÍFICA.* Costa Rica.

Cuesta, M. (2012). *Introducción al Muestreo.* Oviedo.

Delgado, L. (2007). *Análisis Forense Digital.*

Di Lorio, A. (2013). *La informatica forense y el proceso de recuperación de informática digital .* Mar de Plata.

García, M. (2015). *Análisis Forense con distribuciones Gnu/Linux.* Cataluña.

Giovanni, Z. (2006). *Informática Forense.* Bogotá: IF.

Granada, T. E. (2015). *Metodología para el análisis forense de datos e imágenes de acuerdo al Ecuador. .* Cuenca .

Guachichullca, C. (2015). *Diseño de la Metodología administrativa para el aseguramiento de calidad aplicada en las fases de Análisis, diseño y desarrollo para el prototipo del Sistema de Gestión académica de la Universidad de Guayaquil.* Ecuador.

Hernández Sampieri, Collado Fernández, & Batista Lucio. (2011). *Metodología de la investigación.* México: Editorial Mc Graw Hill.

Hernández Sampieri, R. (2010). *Metodología de la Investigación.* Ciudad México: McGraw Hill.

Herrera, H. (2009). *Informática Forense.* Argentina: Poder Judicial Provincial del Neuquen.

Jaen, U. (2012). *Software malicioso (malware) .* España.

Juarez, P. (2012). Tecnologías para inclusión social. *Fedaeps*, 1.

Lacayo, G. (27 de Julio de 2012). *SlideShare.* Obtenido de SlideShare: http://es.slideshare.net/tutor03770/factibilidad-administrativa-y-legal

León, J. (2013). *Curso informática forense redes.* Costa Rica.
López, Varela. (2016). *Diseño Especificaciones técnicas y seguridad para la Implementación de un Laboratorio de informática forense para la Carrera de Ingeniería en Networking y Telecomunicaciones.* Guayaquil.
Lucas, C. (2010). *Estudio de informática forense acerca de delitos ocurridos entre la interoperabilidad de sistemas operativos cliente de plataforma Windows y servidores con plataforma de software libre Linux dentro de redes hibridas .* Guayaquil.
Luna, R. (1999). *Manual para determinar la factibilidad economica de proyectos.* Nicaragua: PROARCA.
Macas Carrasco, N. P., & Juntamay Tenezaca, A. L. (2011). *Estudio y Aplicación de Procedimiento de Analisis Forense en Servidores de Bases de Datos SQL Server y MySQL. .* Ecuador: ESP.
Macho, A. (2006). *Vulnerabilidad en dispositivos Bluetooth .* Madrid.
Mauricio, C. (2012). *PLAN DE DESARROLLO DE LA CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA.* Ecuador.
Meneses, J. (2011). *El cuestionario y la entrevista.* Cataluña.
Moya, R. (2013). *Delitos Informáticos.* Colombia.
Novak, J. (1998). *Conocimiento y aprendizaje.Los mapas conceptuales como herramientas facilitadoras para escuelas y empresas.* Madrid: Alianza.
Pagés, J. (2013). *Temas avanzados en Seguridad y Sociedad de la Información.* Madrid.
Pagot, M. (2010). Metodologías inductivas y deductivas en técnicas de investigación. madrid, España: Prana.
Parés, M. (2007). *Ciber acoso. Un tema de reflexión.* España.
Presman, G. (2011). *Como preservar la evidencia digital en un incidente informático.* Argentina.
Ramíez Almaguer, D. (marzo de 2009). *Observatorio de la Economía Latinoamericana.* Obtenido de http://www.eumed.net/ce/2009a/
Ramírez, D. (30 de Mayo de 2013). *Eumed.net*. Obtenido de Eumed.net: http://www.eumed.net/ce/2009a/amr.htm
Rojas, P. E. (2013). *DEBIDO MANEJO DE LA CADENA DE CUSTODIA EN EL PROCESO ORAL PENAL ECUATORIANO.*
Romo, A., & Omar, R. (2011). *Metodología para la implementación de informática forense en sistemas operativos Windows y Linux.* Ecuador.
Sanchez, J. (2010). *Estudio de informática forense acerca de delitos ocurridos entre la interoperabilidad de sistemas operativos cliente de plataforma Windows y servidores con plataforma de software libre.* Guayaquil.
Sánchez, M. A. (2009). *Desarrollo de habilidades del pensamiento. Procesos básicosdel pensamiento.* México: Trillas.
Seguinfo. (2005). Informática forense, un camino hacia la investigación de crímenes informáticos . *Seguridad Inromática*, 1.
Semprini, G. (2015). *Estandarización de procedimientos y protocolos del laboratorio de Informática Forense.* Argentina: SID.
Serna, A. (2012). *Framework para la comutación forense en Colombia.* Colombia.
Sojo, E. (26 de Mayo de 2008). *Diseño de Sistemas II*. Obtenido de Diseño de Sistemas II: http://ersmsystem.blogspot.com/2008/05/definicin-de-factibilidad-tcnica.html
Torres, J. C. (2012). *Programa de Doctorado sobre la Sociedad de la Información y el conocimiento.* Cataluña .
Torres, P. (2014). *"EL CONTRATO VOLUNTARIO DE SEGUROS DE DAÑOS EN AUTOMOTORES EN EL ECUADOR.* Cuenca.
Ureta, A. (2009). *RETOS A SUPERAR EN LA ADMINISTRACIÓN DE JUSTICIA ANTE LOS DELITOS INFORMÁTICOS EN EL ECUADOR.* Guayaquil.
Zuccardi, G. (2006). *Informática forense.* Italia: IF.

ANEXOS

Anexo 1: Cronograma del Proyecto

UNIVERSIDAD DE GUAYAQUIL FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES	**CRONOGRAMA DEL PROYECTO**
Nombre del proyecto:	Estudio e implementación de metodologías de Análisis Forense Digital, aplicables en un Laboratorio de Informática Forense en la Carrera de Ingeniería en Networking y Telecomunicaciones
Nombre del tutor:	ING JORGE ARTURO CHICALA ARROYAVE
Duración de la ejecución del proyecto en meses:	4 meses

N°	ACTIVIDAD	SEMANAS	MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Estudio de evidencia digital	25/05/2016																				
2	Clasificación de delitos informáticos	13/06/2016																				
3	Análisis de Metodologías internacionales	16/06/2016																				
4	Exploración de buenas prácticas recomendadas	20/06/2016																				
5	Duplicado de Imágenes bit a bit	01/08/2016																				
6	Extracción de código Hash	05/08/2016																				
7	Análisis del diseño del Laboratorio	11/08/2016																				
8	Comparación de Hardware y Software	18/08/2016																				
9	Elección de cadena de custodia	19/08/2016																				
10	Elaboración de registros	22/08/2016																				

Elaborado por: John Larrea

Fuente: John Larrea

Anexo 2: Encuesta aplicada a los estudiantes de la Universidad de Guayaquil

UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERIA EN NETWORKING & TELECOMUNICACIONES

PROYECTO DE TITULACIÓN:

"ESTUDIO E IMPLEMENTACIÓN DE METODOLOGÍAS DE ANÁLISIS FORENSE DIGITAL APLICABLES EN UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES"

INSTRUCCIONES: Marque con una "X" la opción que usted elija, además tenga en cuenta que la veracidad de sus respuestas permitirá obtener la elaboración de una investigación real y efectiva.

1. **¿Conoce usted qué es un Laboratorio de Informática Forense?**

SI ☐ NO ☐

2. **¿Ha recibido temas prácticos sobre Análisis Digital Forense?**

SI ☐ NO ☐

3. **¿Cree usted que aprendería más sobre la informática forense haciendo actividades prácticas?**

SI ☐ NO ☐

4. **¿Cree usted que la Carrera de Ingeniería en Networking y Telecomunicaciones debería contar con un Laboratorio de Informática Forense?**

SI ☐ NO ☐

5. **¿Usted conoce qué es la evidencia digital?**

SI ☐ NO ☐

6. **¿Conoce usted de la existencia de normas y procedimientos utilizados en la manipulación de evidencia digital?**

SI ☐ NO ☐

7. **¿Deberían existir normas y procedimientos para el uso adecuado de las instalaciones en un Laboratorio de Informática Forense?**

SI ☐ NO ☐

8. **¿Considera usted necesario el uso de documentos y registros correspondientes a custodia, almacenamiento y análisis de la evidencia digital?**

SI ☐ NO ☐

9. **¿Se deberían aplicar procedimientos para evitar la incorrecta manipulación de la evidencia digital durante la recolección de la misma en la escena del delito?**

SI ☐ NO ☐

Elaborado por: John Larrea

Anexo 3: Entregable del Proyecto

Este anexo constituye la propuesta que se llevará a cabo en el laboratorio forense. Este es el punto más importante de la investigación ya que es el resultado del estudio previo realizado y con ello se contribuye a lograr el desarrollo adecuado de las actividades de Informática Forense en la entidad.

Propuesta práctica y metodológica para el Análisis Forense en el Laboratorio de Informática Forense.

Etapa inicial: Identificación del incidente

Inicial: En esta etapa se presentan las pautas globales de la investigación. La misión dentro de esta fase es encontrar, recabar y conservar la evidencia digital hallada. En esta etapa se genera una réplica idéntica del contenido digital que se encuentra en el dispositivo original.

Para realizar las actividades mencionadas se proponen las siguientes actividades:

- Asegurar la escena, con el objetivo de mantener la integridad física del área o campo donde se perpetró el crimen, desalojando el lugar y/o limitando su acceso.
- Observar y planificar, para definir una hipótesis sobre los hechos.
- Hacer uso de equipos de bioseguridad para garantizar la integridad de los especialistas que realizan la investigación, así como la evidencia hallada. Estos equipos deben ser guantes de látex, protectores naso bucales y oculares, además de trajes que eviten la contaminación de la escena.
- Documentar y registrar la evidencia a través de videos y fotografías.
- Evitar la contaminación y actuar metódicamente.
- Obtener una copia exacta de los datos para trabajarlos en un entorno adecuado.

Segunda etapa: Recopilación de evidencias

La recolección de evidencia debe ser llevada a cabo por personal calificado, que posea conocimientos de telemática, para la exitosa conservación y recuperación de información. A continuación, se listan las recomendaciones a tener en cuenta para el desarrollo de esta actividad:

- Hacer uso de dispositivos de protección para los equipos electrónicos, como los trajes de aislamiento antiestático o las manillas.
- Clasificar la evidencia, teniendo en cuenta si los datos que posee son volátiles o no volátiles.
- Definir si los equipos que forman parte de la investigación realizan actividades de centralización, o sea si son servidores o data centers, con los cuales se debe tener especial cuidado.
- Determinar en qué condiciones han sido encontrados los dispositivos y elementos. Para cada uno definir sus características de tipo físicas, fecha y hora del sistema, así como valorar las distintas opciones para desconectar o no un dispositivo usb, disco duro o Cd, DvD.
- Cuando los ordenadores están funcionando, debe establecerse un método para recuperar información estando el sistema en caliente.

La manipulación de información debe realizarse mediante el uso de herramientas que permitan:

- Obtener la información de sistemas que se encuentren activos, los que frecuentemente se guardan en la caché o memoria Ram.
- Realizar una imagen de los dispositivos fundamentales donde se ejecuta el sistema.
- Para manipular los equipos, se tratará de hacer lo mejor posible, mientras se documentarán las actividades realizadas según la fecha.

Cuando el ordenador no está encendido se debe:

- Registrar las características con las que fueron encontrados los dispositivos. Definir sus cualidades, físicas y sus datos específicos a través de series y códigos.
- Retirar los dispositivos conectados a los ordenadores.

- Guardar los dispositivos que contribuirán a la investigación como cámaras de video, impresoras, escáneres entre otros.
- Establecer los equipos que serán utilizados para proteger la información de los dispositivos encontrados.
- Llevar a cabo el procedimiento de cadena de custodia, para garantizar la autenticidad, continuidad, e integridad de la información haciendo uso de un rotulado conjuntamente con un expediente de continuidad, en el cual se especifique la fecha en la que los especialistas tuvieron contacto con los dispositivos.

Todos los aspectos mencionados anteriormente, deberán aplicarse cuando los escenarios se encuentran controlados. Donde el especialista que realiza la investigación tenga a su favor los diferentes factores. En caso de no ser así:

- El procedimiento estará enfocado a documentar mediante video o fotografías, los distintos dispositivos, de forma tal que se pueda guardar el estado en el que se encontraban los equipos.
- Definir que los dispositivos son importantes para realizar la investigación.
- Los dispositivos serán desconectados de sus fuentes de alimentación sin aplicar un apagado o suspensión sobre estos.
- Recabar y custodiar los dispositivos para su posterior embalaje, anotación del rotulo para ser trasladado luego hacia el laboratorio.

Para esta etapa uno de los documentos o fichas que se propone es el acta de recolección de pruebas. La misma permitirá listar y describir las incidencias encontradas inicialmente. Para llenar este documento, se tendrán en cuenta:

- El número de la prueba.
- La fecha de detección de la prueba.
- La hora.
- El lugar la cantidad o marca, en caso de trabajar con un dispositivo.
- Así como su modelo, fabricante, número de serie.
- Descripción de la prueba.
- También una descripción del de estado de la prueba.
- Los nombres y apellidos del encargado de la evidencia.
- Su cargo.
- Firma.

Acta de recolección de pruebas

Laboratorio forense, Universidad de Guayaquil.

Número de prueba: _____

Fecha: ____**/**_____**/**_____(dd/mm/aaaa)

Hora: _____:_____0-24 HORAS (hh:mm)

Lugar de recolección: _____ _____

Cantidad Marca: _____

Modelo: _____

Fabricante: _____

Número de serie: _____

Descripción de la prueba: _____ _____

Nota de estado de la prueba: _____ _____

Agente encargado de recolección ID: _____ _____

Nombres y apellidos: _____ _____

Cargo: _____

Firma: _____

Cadena de custodia para la evidencia digital

En la cadena de custodia digital, el flujo de trabajo, estará siempre enmarcado en el factor del tiempo, la evidencia y el especialista que tiene autorización sobre esta en un tiempo definido.

El tiempo: Es un factor fundamental en la cadena de custodia, y será el primero en registrarse dentro de ella teniendo en cuenta su seguimiento y control.

- Entregado(entregas)
- Inicio (fecha de inicio)
- Culminación (fecha de fin)
- Horas de trabajo (tiempo que demoró)

Identificación: Este factor también es importante, ya que junto al tiempo enfatizan la potestad de un especialista sobre la prueba digital dentro de la cadena de custodia.

- Especialista que solicita el análisis
- Identificador de la autorización
- Autoridad (quien realiza la solicitud)
- Nombre del caso
- Número del caso
- Prioridad
- Clasificación del caso (urgente, alto impacto, normal, reservado)

Descripción general: Facilita las características del especialista que verifica la evidencia, al igual que las especificaciones de la evidencia como tal.

- Analista/examinador propuesto
- Identificación del analista
- Número de la evidencia
- Sistema de archivos
- Datos que se analizan(tamaño)

Protección: Esta actividad es crucial dentro de la cadena de custodia digital, pues los métodos que se utilizan para la obtención de la información de la evidencia pueden conllevar a la perdida de la misma, por ello es importante garantizar la protección y la integridad de la información.

- Medios externos
- Respaldo

Detección: Esta etapa es parte del proceso de búsqueda de la evidencia digital, la misma necesita un cronograma detallado de acciones, pues esta actividad puede conllevar a un proceso de borrado u otros inconvenientes que afecten la evidencia parcial o totalmente.

- Registro especifico de las acciones realizadas respecto a la evidencia digital.
- Marcas de tiempo (creado, modificado, eliminado)
- Características (protegido, escondido)

Responder: Se encarga de registrar y notificar la información hallada a la entidad competente. Este documento para que sea efectivo debe contener la firma del jefe del laboratorio y el sello de la institución.

Recuperar: Se puede dar en cualquier instante, pues cada paso anteriormente mencionado puede comprometer la evidencia. A través de este proceso se pretende dejar a disposición la evidencia en el estado en que fue hallada y registrada inicialmente dentro de la cadena de custodia.

- Restaurar la evidencia comprometida
- Reconstruir la evidencia que ha sido destruida.

Para recopilar los datos de esta etapa se utilizará la ficha propuesta de entrada y salida de evidencia y la ficha de inventario.

La ficha de entrada y salida de evidencia está conformada por:

- Número de caso.
- Código de la evidencia.
- Ingreso y salida de la evidencia.
- Fecha.
- Hora.
- Justificación.
- Nombre del responsable.
- Firma del responsable.

Formato para registrar la entrada y salida de evidencia

Laboratorio forense, Universidad de Guayaquil.

ENTRADA Y SALIDA DE EVIDENCIA			
No Caso			
Código de evidencia			
Ingreso		Salida	
Fecha			
Hora			
Justificación			
Responsable			

X

Responsable

La ficha de inventario de evidencia propuesta comprende los datos de:

- Número de casos.
- Fecha de ingreso.
- Código de evidencia.
- Tipo de evidencia.
- Detalle adicional.

Formato para el inventario de evidencia

Laboratorio forense, Universidad de Guayaquil.

INVENTARIO DE EVIDENCIA				
N° Caso	Fecha de ingreso	Código de evidencia	Tipo de evidencia	Detalle

Tercera etapa: Preservación de la evidencia

En esta etapa se analizará el contenido recopilado para buscar vestigios e indicios de lo que se busca específicamente. El objetivo fundamental es encontrar la evidencia digital, o sea, aquello que relaciona al hecho con el actor del crimen y la víctima.

La etapa se conformará por tres etapas internas:

1. Extracción lógica.
2. Extracción física.
3. Análisis de relaciones.

En la primera etapa interna, se recuperará la información eliminada partiendo del sistema de archivos. Este sistema será utilizado para acceder a los bloques. Permitirá recuperar el archivo que se encuentra en un espacio disponible, ya que los sistemas no borran inmediatamente un archivo si no que permiten dar disponibilidad al espacio anteriormente ocupado.

A través de la extracción física se podrá buscar la información directamente en el espacio de datos, donde se puede omitir el tipo de estructura de sistema de archivo. Con ello se podrán aplicar diversas técnicas sobre lo que contiene el bloque en el dispositivo de almacenamiento.

En la próxima etapa se podrán identificar las relaciones entre los conjuntos de archivo para llegar a una conclusión. Ejemplo de ellos son los archivos de navegación por internet. También permitirá verificar las aplicaciones instaladas.

Esta metodología consta de dos etapas importantes, las cuales se listan y explican a continuación.

Actividades a realizar dentro del laboratorio

A través de las distintas actividades que se desarrollarán en el laboratorio, se podrá adquirir y preservar la información, así como presentar los resultados, luego de analizar los resultados obtenidos en los dispositivos estudiados.

Cuando los datos recabados se obtienen a partir del uso de procedimientos y métodos, las opciones de responder las interrogantes planteadas durante la investigación, serán mayores.

Dentro de las funciones a tener en cuenta se define que:

- Se tendrá en consideración los principios de la especialidad, así como sus protocolos, buenas prácticas, manuales operacionales y procedimientos operativos estandarizados (SOPs).
- Se tendrán en cuenta los objetivos y actividades a desarrollar por parte de los profesionales que forman parte del laboratorio.
- Se evaluarán las herramientas para el análisis forense, las técnicas forenses llevadas a cabo, también las metodologías puesta en práctica y se chequearán las herramientas y los manuales de calidad.
- En la jornada laboral se tendrán en cuenta las actividades operativas, el desarrollo de informes y capacitaciones, al igual que el control de la calidad.

Almacenamiento y etiquetado

- El almacén de evidencia debe estar en un lugar seguro y de acceso restringido.
- Las condiciones del almacén de evidencias deben ser las adecuadas teniendo en cuenta factores como temperatura, humedad, electricidad estática, etc.
- Se debe etiquetar con el código de evidencia cada dispositivo almacenado.
- Se deben registrar todos los detalles como: código, responsable de recolección, institución, descripción de dispositivo, día y hora de almacenamiento.
- Los dispositivos magnéticos u ópticos deben ser introducidos en bolsas antiestáticas y luego en una caja o cartón que los protejan de golpes.

El formato propuesto para la preservación de la evidencia recabada es el ingreso de evidencia, para el cual deben ingresarse los datos siguientes:

- Fecha de ingreso.
- Hora de ingreso.
- Número de caso.
- Fiscal asignado para el proceso.
- Responsable que entrega.
- Objetivo de la investigación.
- Descripción de la evidencia.
- Observaciones.
- Responsable que recibe.
- Firma de quien recibe.
- Firma de quien entrega.

Formato para ingreso de evidencia

Laboratorio forense, Universidad de Guayaquil.

INGRESO DE EVIDENCIA	
Fecha de ingreso	
Hora de ingreso	
Número de caso	
Fiscal asignado	
Entregado por	
Objeto de la investigación	
Descripción de la evidencia	
Observaciones	
Recibido por	

X ----------

Entregado por

X ----------

Recibido por

Cuarta etapa: Análisis de evidencia

Como parte fundamental del análisis forense, debe poderse recuperar la información eliminada, oculta o formateada. Para ello se proponen herramientas que no necesitan ser instaladas sobre el sistema operativo que se investiga.

La herramienta Photorec es muy utilizada para recuperar imágenes. La misma cumple los requisitos para mantener la integridad de la evidencia. El software es distribuido bajo licencia pública general GNU open source y multiplataforma.

Figura1: Uso de herramienta Photorec

Fuente: (Granada, 2015)

Los pasos que se proponen para la extracción de imágenes son los siguientes:

- Elaboración de un documento físico o digital en el que se describan por orden cronológico, todas las actividades a realizar, sirviendo el mismo como base histórica para la conformación del informe del laboratorio.
- Utilizar las herramientas requeridas para garantizar el bloqueo contra escritura y/o modificación de los dispositivos a analizar posteriormente.
- Crear un archivo para guardar la imagen forense.
- Constatar la integridad de la imagen forense.

Se tendrá en cuenta:

- Listar los usuarios conectados remotamente y local al sistema.
- Obtener fecha y hora del sistema.

- Enumerar los procesos que se mantienen activos, los usuarios y aplicaciones que los lanzan (ps y pslist) y los recursos que utilizan.
- Buscar ficheros ocultos o borrados.
- Visualizar registros y logs del sistema.
- Generar funciones hash de ficheros.
- Análisis de encabezados de correos electrónicos.

Para registrar la documentación de recopilada en esta etapa se propone utilizar la ficha de análisis de evidencia. La misma cuenta con datos que deben ser ingresados como:

- Numero de caso
- Código de evidencia.
- Tipo de análisis.
- Responsable de la evidencia.
- Hora de inicio de análisis de la evidencia.
- Fecha de comienzo de análisis de la evidencia.
- Duración del análisis de la evidencia.
- Detalles del análisis.
- Resultado obtenido.
- Firma del responsable.

Formato para Análisis de la evidencia

Laboratorio forense, Universidad de Guayaquil.

ANÁLISIS DE LA EVIDENCIA	
No Caso	
Código de evidencia	
Tipo de análisis	
Responsable	
Hora inicio	
Fecha	
Duración	
Detalle del análisis	
Resultado	

X

Responsable

Quinta etapa: Documentación y resultados

En esta etapa se recopilarán los datos para la redacción del informa forense, con el objetivo de detallar todas las actividades en este documento para que estas permitan, reanudar el camino del análisis y obtención de resultados en caso de ser necesario.

Para ello se proponen una serie de fichas, que permitirán recopilar información y darle seguimiento a la misma.

En esta etapa también se utilizará el informe técnico pericial. El cual está conformado por elementos esenciales, requerimientos y los archivos entregables.

Dentro del inicio de la presentación se debe entregar:

- La documentación del área y la documentación de la causa, las cuales estarán debidamente argumentadas.
- Se justificará qué juzgado, fiscalía, juez, o fiscal que recibe la evidencia. Igualmente se detallará la causa, el expediente y quien recibe el documento.
- Número de designación, tipo de designación y el número de designación.
- Definición y carácter de la misma junto al pedido.
- Preservación de los resultados y validación de estos.
- Técnicas utilizadas para el análisis.
- Documentación del resguardo de los resultados.
- Detallar el tipo de resguardo de la documentación.
- Presentar formulario con el registro de la evidencia.
- Explicación de las herramientas y procedimiento utilizado.
- Informe firmado por el jefe de laboratorio.

Laboratorio forense, Universidad de Guayaquil.

Fecha ……/……../…….

Documentación Pericial			
Elementos Esenciales del Informe	Requerimientos	Archivos para entregar	
Inicio de la presentación	Parte inicial de la presentación	Documentación del área Documentación de la causa	
	Receptor	Juzgado/Fiscalía Juez/Fiscal	
	Tipo de designación	Causa Quién recibe el documento Expediente	
Objetivo del informe	Solicitud del requerimiento	Nro. de designación Solicitud realizada Tipo de designación	
Puntos del informe	Definición	Definición Carácter de la definición Pedido	
	Conservación	Preservación de los resultados Validación de los resultados	
	Análisis	Técnicas utilizadas	
	Presentación	Obtener resultados Resguardar resultados	
Elementos que se	Objetos custodiados	Cantidad de	

facilitan		elementos Características	
	Objetos dubitados	Documentación Cd/DvD Imágenes	
Actividades que se realizan	Procedimientos	Génesis de la metodología Cuadro metodológico	
	Identificación	Explicación Fecha y hora de apertura Imágenes del procedimiento Formulario para registrar evidencia	
	Conservación	Explicación Imágenes del procedimiento Herramientas Resultados obtenidos	
	Análisis	Explicación Herramientas Técnicas Resultados	
	Revelar	Explicación Conservación y forma de entrega	
Entrega	Contenidos en dispositivos de respaldo	Informe y anexo en pdf Resultados obtenidos	
	Presentación impresa	Hojas del informe firmadas por el jefe de laboratorio	

Elaborado por: John Larrea
Fuente: John Larrea

Para esta etapa se elaboraron fichas a través de las cuales se definen las políticas que tendrá el laboratorio.
Para ello se elaboraron las fichas de control de ingreso:

- Salida al personal operativo:
- Fecha de entrada.
- Nombre.
- Hora de entrada.
- Hora de salida
- Firma.

Control de ingreso y salida al personal operativo

Laboratorio forense, Universidad de Guayaquil.

CONTROL DE INGRESO Y SALIDA DE PERSONAL

Fecha	Nombre	Hora de entrada	Hora de salida	Firma

_____X_____
Responsable

El control de ingreso de entrada y salida de visitantes:

- Fecha.
- Turno.
- Apellido y nombre del visitante.
- Hora de ingreso.
- Hora de salida.
- Firma del visitante.
- Detalles.
- Políticas del laboratorio.
- Firma del encargado o supervisor.

Control de ingreso de entrada y salida de visitantes

Laboratorio forense, Universidad de Guayaquil.

	REGISTRO DE INGRESO DE VISITANTES				
	Fecha				
	Turno				
	Apellido y Nombre	Hora de ingreso	Hora de salida	Firma	Asunto
1					
2					
3					
4					
5					
6					
7					
8					
	_____X_____ **Firma y sello del supervisor**				

Herramientas de software y hardware

Para aplicar esta metodología es necesaria la utilización de herramientas de hardware y software, las cuales garantizarán el cumplimiento de los pasos propuestos anteriormente.

Herramientas de hardware:

Figura 2: Herramienta Duplicadora RoadMasster-3

Elaborado por: John Larrea
Fuente: (Aguilar, 2016)

Esta herramienta es un laboratorio forense portátil, la cual posee un diseño para la adquisición de datos forenses de alta velocidad. La misma está reforzada, construida para su uso en carretera y está equipada con las herramientas necesarias para adquirir datos de los discos con las tecnologías de interfaz más actualizadas. Incluye una plataforma sólida y versátil para recabar datos forenses y analizarlos. Presenta una gama alta de procesamiento de energía. Está diseñado para ser compatible con unidades de alto rendimiento. Es compatible con disimiles interfaces de unidad, ofreciendo soporte para SAS, SATA, SCSI, USB 2 y USB 3. Incluye múltiples puertos como SAS, SATA, ESATA., dedicadas a pruebas y unidades sospechosas entre otros. Además, posee un diseño robusto, ya que cuenta con un estuche portátil de choque absorbente. No es una unidad muy pesada, y puede ser llevada como equipaje de mano. También cuenta con múltiples formas de funcionamiento como la captura individual, la captura Linuxdd, la captura E01, la copia IQ * entre otras.

Figura 2: Herramienta Ultrakit

Elaborado por: John Larrea
Fuente: (Aguilar, 2016)

Esta herramienta constituye un Kit portátil que cuenta con Ultrablocks, bloqueadores de escritura y hardware, así como adaptadores y conectores, para su uso luego de la adquisición de una imagen válida a efectos legales. Incluye fuentes de alimentación, cables de unidad de interfaz, cables de interfaz de una computadora y adaptadores.

Figura 3: Herramienta Fred

Elaborado por: John Larrea
Fuente: (Aguilar, 2016)

Esta herramienta está diseñada para el análisis, así como para conformar un laboratorio estacionario. Permite conectar a él, los discos duros sospechosos para adquirir la evidencia digital. Puede adquirir datos directos de discos IDE, EIDE, ATA, SATA, ATAPI, SAS, Firewire y USB. También facilita adquirir datos de Blu-ray, CD y DvD. Incluye conexiones del panel frontal, y bandejas de discos extraíbles, sin necesidad de abrir el sistema de procesamiento, de instalar unidades o rastreo alrededor de la parte posterior de la unidad para conectar dispositivos. Es rápido funcional y flexible. Cuenta con tres variadores de velocidad alta. Puede conectarse directamente a una red (10/100/1000 Mb ethernet) para su uso como una estación de trabajo o servidor de archivos estándar.

Figura 4: Herramienta Celldek

Elaborado por: John Larrea
Fuente: (Aguilar, 2016)

Es compatible con más de 950 de los teléfonos celulares más populares y PDA. Los investigadores pueden obtener de inmediato el acceso a información vital, el ahorro de días de espera de un informe de un laboratorio del crimen. Este teléfono celular, dispositivo de extracción avanzada de datos es un sistema autónomo que cuenta con una pantalla táctil que permite al usuario identificar rápidamente los dispositivos según la marca, número de modelo, dimensiones y fotografías.

Herramientas de software: Dispositivos móviles y memorias usb

Las herramientas de software también forman parte importante de presente propuesta. Seguidamente se mencionan, y se explica el proceso de instalación de cada una de ellas.
Las siguientes herramientas serán utilizadas para los dispositivos móviles. Estas disponen de una versión gratuita, por lo que no es necesario pagar sus licencias, lo cual constituye una de las ventajas por las que fueron escogidas.

MOBILedit Forensic

Es capaz de realizar extracciones simultáneas de múltiples dispositivos, exportaciones de datos a XML, HTML, PDF, MS Word y MS Excel. Consta de actualizaciones automáticas para mantener su instalación hasta a la fecha. Puede realizar copia de seguridad mejorada del sistema de archivos y la exportación Modo multimedia (MTP) de detección y resolución de la conexión, exportación de los datos de la Tarjeta SIM ampliado, es compatible con varios sistemas operativos móviles.

Especificaciones

- Conexión por cable y bluetooth
- Asistente de Extracción de Datos e información
- Compatible con Symbian, Windows Mobile, Apple IOS, Android, Blackberry, Media Tek MeeGO y Bada.
- Acceso al calendario, tareas y notas.
- Información de llamadas entrantes, salientes y perdidas,
- Log de envío y recepción de mensajes SMS, MMS, mensajes de correo electrónico.
- Acceso a los archivos del dispositivo móvil y memoria flash.
- Geo localización.
- Integridad de los datos de verificación.

Para la instalación de MOBILedit se utilizó un instalador que se puede obtener de la página oficial http://www.mobiledit.com, para pruebas que contiene la herramienta y los drivers necesarios para conectarse a diferentes dispositivos móviles. Para ver el proceso de instalación observe el Anexo 2.

Oxygen Forensic

Es considerado una de las más populares por ser una de las más completas en recuperación forense es desarrollado por Oxygen Sofware fundada en el año 2000 es especializada en el desarrollo de software para exámenes forenses avanzados para dispositivos móviles inteligentes. Para verificar como se realiza su instalación y configuración observe el anexo 3.
Consta de varias versiones de software:

Oxygen Forensics Suite Pro, es una de las más completas ya que puede extraer la información necesaria para la investigación forense, analizando información de fotografías, historiales de conexión, análisis de caché de navegadores.

Oxygen Forensics Suite Pro Analyst, tiene como principal objetivo procesos de recuperación de contraseñas

Oxygen Forensis Suite Pro, esta versión puede realizar un rooting, es decir realizar todas las extracciones como un usuario administrador la cual permite analizar más afondo la información.

Especificaciones

- Conexión por cable, bluetooth e infrarrojo.
- Asistente de Extracción de Datos e información
- Compatible con Symbian, Windows Mobile, Apple IOS, Android, Blackberry y Bada.
- Acceso al calendario, tareas y notas.
- Información de llamadas entrantes, salientes y perdidas,
- Log de envío y recepción de mensajes SMS, MMS, mensajes de correo electrónico.

- Acceso a los archivos del dispositivo móvil y memoria flash.
- Geo localización.
- Integridad de los datos de verificación.

Herramientas de software para analizar ordenadores

Las herramientas que se proponen para el análisis de ordenadores, al igual que las escogidas para los móviles también son hechas con software libre, por lo que tampoco es necesario pagar sus licencias. Seguidamente se muestran y se ofrecen algunas de sus características que permiten corroborar por que fueron elegidas.

Caine: Es una distribución Live CD para realizar Análisis Forense informático, creada por Giancarlo Giustini es una de las mejores opciones que tenemos a la mano cuando deseamos realizar un Análisis Forense de algún equipo informático.CAINE se diferencia de las demás distribuciones de su tipo (Forensic Boot CD, Helix, Deft, etc..) por su facilidad de uso y que proporcionar una interfaz gráfica homogénea que guía a los investigadores digitales durante la adquisición y el análisis de las pruebas electrónicas, y ofrece un proceso semi-automático durante la documentación y generación de informes. (García, 2015)

Autopsy: Tal vez la mejor herramienta libre que existe para el análisis de evidencia digital. Su interfaz gráfica es un browser que basado en las herramientas en línea de comandos del Sleuth Kit, permite un análisis de diversos tipos de evidencia mediante una la captura de una imagen de disco.

The SleuthKit: Es una colección de herramientas en línea de comandos para Análisis Forense de archivos y volúmenes de sistema. Las herramientas del sistema de archivos permiten examinar una computadora sospechosa sin comprometerla. Debido a que las herramientas no confían en el sistema operativo para procesar el Sistema de Archivos, se muestra contenido borrado u oculto. (García, 2015)

D.E.F.T: (Digital Evidence & Forensic Toolkit), es una distribución Linux basada en Xubuntu 9.10 con un kernel 2.6.31, escritorio LXDE además de una GUI con aplicaciones forenses (DEFT extra 2.0) pensada para policía, investigadores, administradores de sistemas o especialistas forenses. Entre sus opciones cabe destacar: Analysis: Herramientas de análisis de ficheros de diferentes tipos Antimalware: Búsqueda de rootkits, virus, malware, así como PDFs con código

malicioso. Data recovery:Software para recuperación de ficheros Hashing: Scripts que permiten la realización de cálculo de hashes de determinados procesos (SHA1, SHA256, MD5...) Imaging: Aplicaciones que podemos utilizar para realizar los clonados y adquisición de imágenes de discos duros u otras fuentes. Mobile Forensics: Análisis de Blackberry, Android, iPhone, así como información sobre las típicas bases de datos de dispositivos móviles en SQLite utilizadas por las aplicaciones. Network Forensics: Herramientas para procesamiento de información almacenada en capturas de red. (García, 2015)

Figura 5: Herramienta Deft

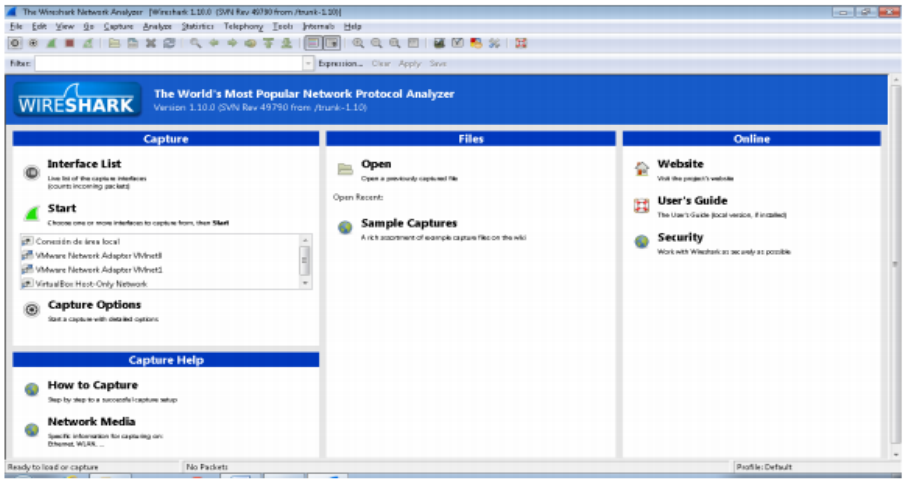
Elaborado por: John Larrea
Fuente: (García, 2015)

Herramientas de software para analizar redes

Wireshark: es un analizador de paquetes de red. Un analizador de paquetes de red intenta capturar los datos de esos paquetes tan detalladamente como sea posible. Se puede pensar en un analizador de paquetes de red como un dispositivo de medida usado para examinar que está pasando al interior de un cable de red. Universidad de los Andes – Ingeniería de Sistemas y Computación – Infraestructura de Comunicaciones.

Wireshark tiene todas las características estándares que se pueden esperar en un analizador de protocolos; su licencia es de código abierto y puede ser ejecutado sobre plataformas como Unix, Linux y Windows. (Castro, 2015)

Figura 6: Wireshark



Elaborado por: John Larrea

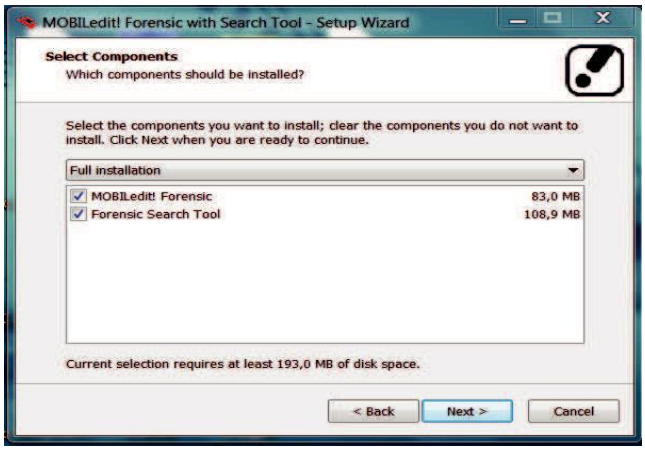
Fuente: (García, 2015)

Anexo 4: Proceso de instalación de la herramienta Mobiledit

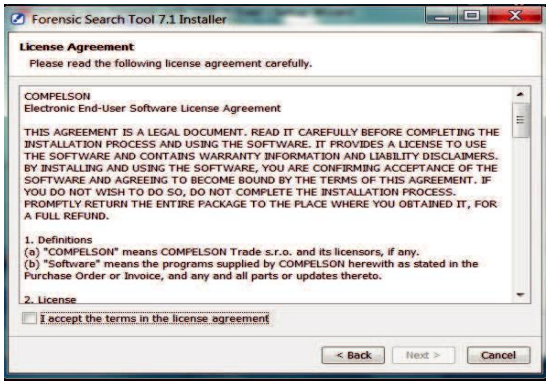
Inicio de Instalación (MOBILedit Forensic)

En la instalación completa nos permite seleccionar dos componentes, el MOBILedit Forensic y Forensic Search Tool.

Selección de Componentes (MOBILedit Forensic)

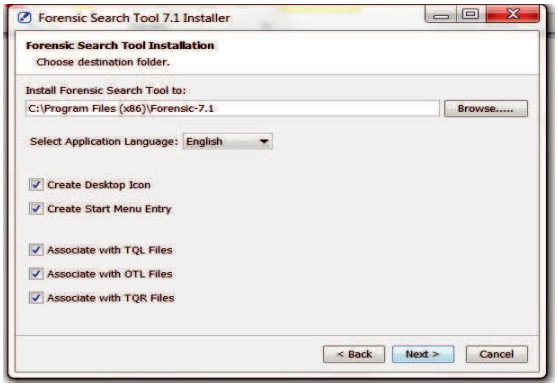


Términos de licencia (MOBILedit Forensic)

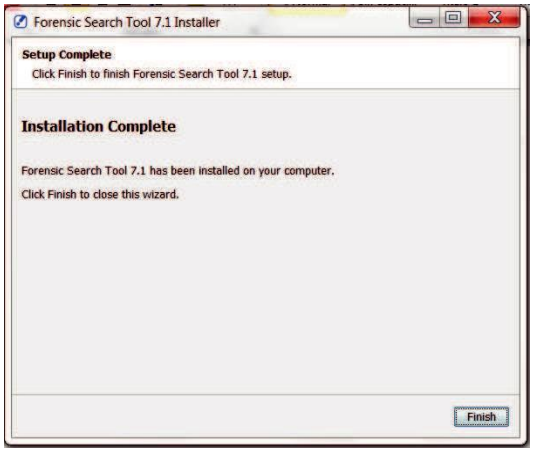


Se puede elegir el lugar donde se va a instalar el componente Forensic Searc Tool, y se desea crear accesos directos, y con qué tipos de archivos se desea asociar.

Lugar de Instalación (MOBILedit Forensic)



Final de Instalación de Componente (MOBILedit Forensic)

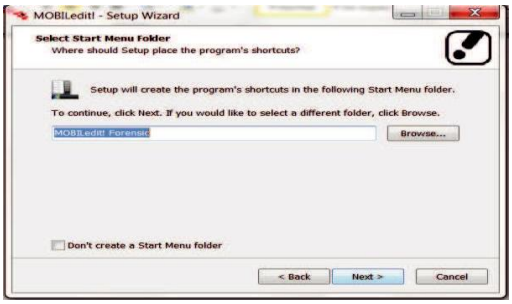


Al terminar de instalar el Forensic Search Tool, continua un procedimiento similar con el MOBILedit Forensic, con el primer paso de elegir el lugar donde se va a realizar la instalación.

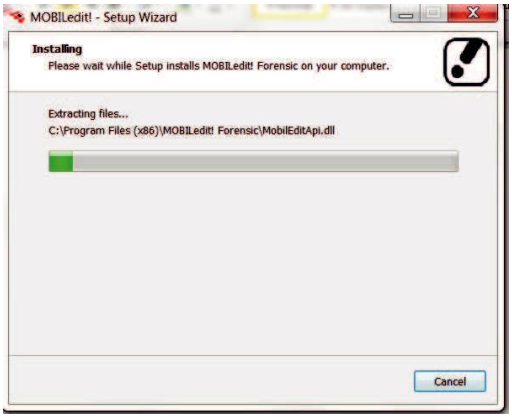
Ruta de Instalación del Software (MOBILedit Forensic)

Se puede escoger si se desea ubicar en la carpeta de menú, para facilitar al usuario ejecutar la aplicación, así como también acceso directo.

Ruta de Instalación en la carpeta Menú (MOBILedit Forensic)



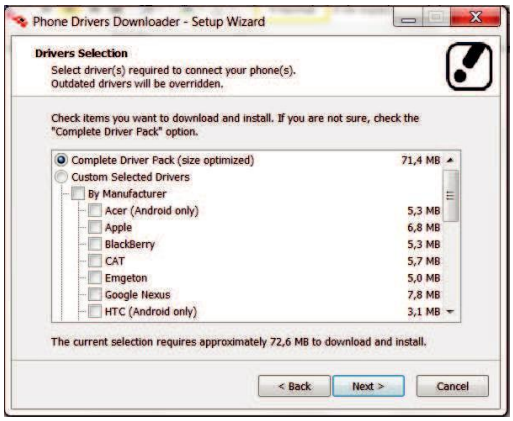
Proceso de Instalación (MOBILedit Forensic)



En el proceso de instalación de los drivers se lo realiza a través de un asistente de instalación.

Inicio de Instalación de Drivers (MOBILedit Forensic)

Opciones de Drivers (MOBILedit Forensic)



Según la selección de los drivers nos presenta un resumen de lo antes seleccionado, antes de proceder a descargar y a instalar.

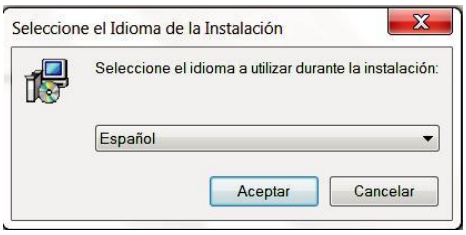
Referencia de Instalación de Drivers (MOBILedit Forensic)

Al finalizar nos muestra una ventana indicando más información acerca de algún dispositivo en especial

Finalización de Instalación (MOBILedit Forensic)

Anexo 5: Instalación y configuración de la herramienta Oxygen

Inicio de instalación (Oxygen Forensic Suite 2014)

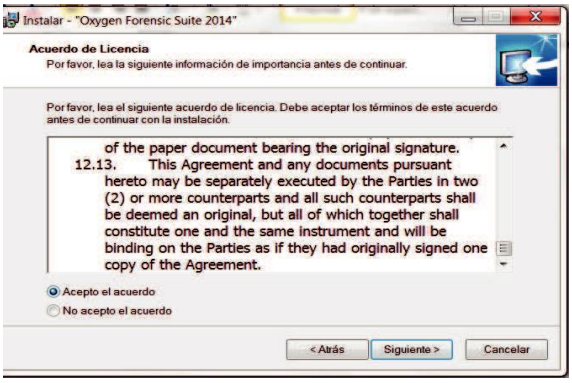


El asistente de instalación nos da la bienvenida y nos indica que se va a iniciar la instalación

Inicio de asistente de instalación (Oxygen Forensic Suite 2014)

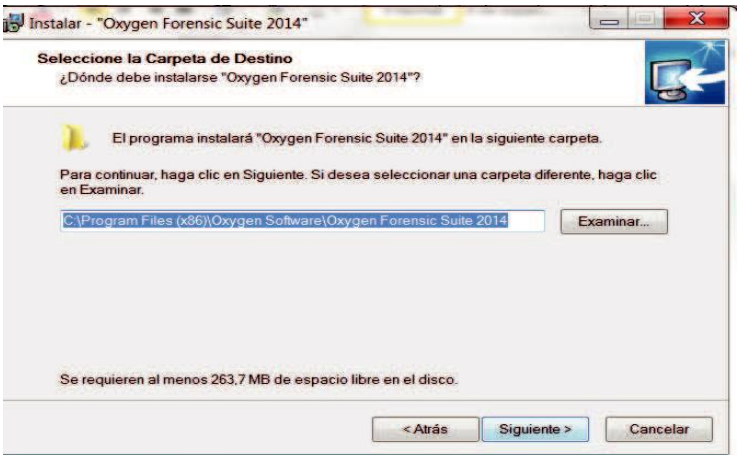
Se presenta un acuerdo con la licencia, que presenta términos de uso del software, en el cual se va a proceder aceptar.

Acuerdo de licencia (Oxygen Forensic Suite 2014)

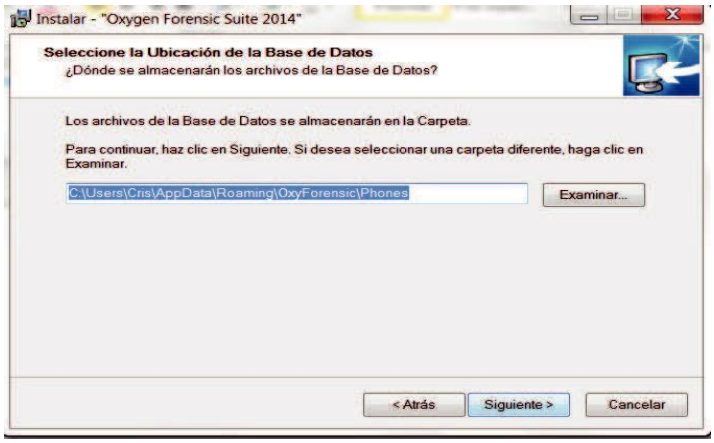


Se selecciona el lugar donde será el destino de instalación en el disco duro.

Selección de carpeta de destino (Oxygen Forensic Suite 2014)

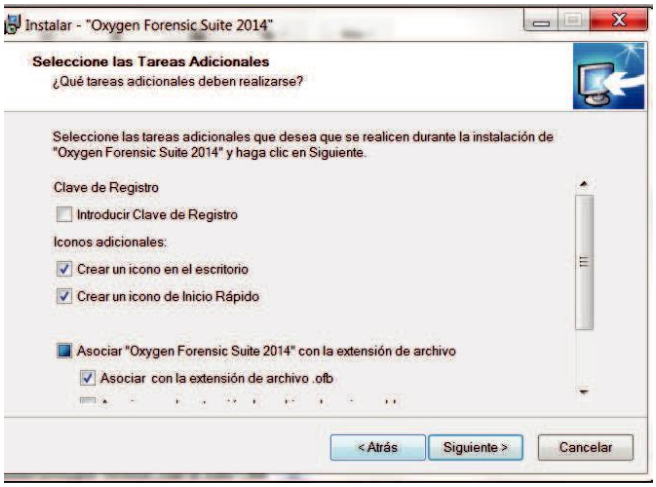


Selección de ubicación de la base de datos (Oxygen Forensic Suite 2014)



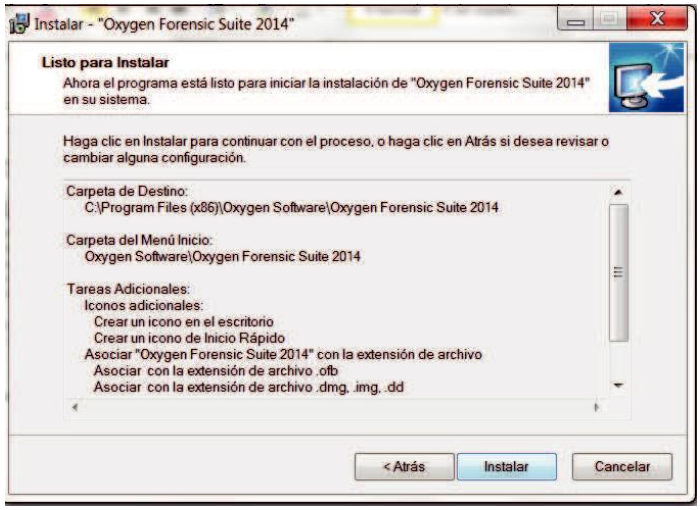
Si se desea se puede crear accesos directo al software

Creación de accesos directos (Oxygen Forensic Suite 2014)

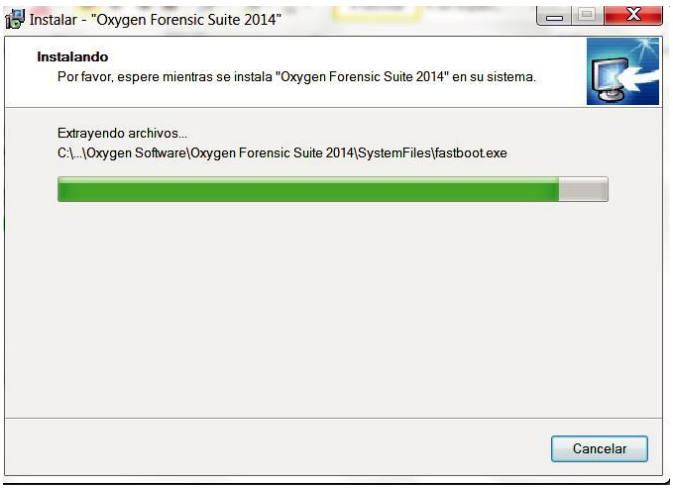


Después de seleccionar las diferentes opciones obtenemos un resumen de lo obtenido anteriormente y procedemos con la instalación

Resumen de opciones seleccionadas (Oxygen Forensic Suite 2014)



Proceso de instalación (Oxygen Forensic Suite 2014)



Al terminar la instalación nos permite ejecutar al finalizar.

Información de la instalación (Oxygen Forensic Suite 2014)