UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

"SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE 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 (ES):

MITE VILLÓN JIMMY ROLANDO

SÁNCHEZ MONTERO YURIS RAFAEL

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		
"SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES**"**		
	REVISORES: Lcda. Viviana Pinos Medrano, M.Sc, LSI. Oscar Apolinario Arzube, M.Sc**.**	
INSTITUCIÓN: Universidad de Guayaquil	**FACULTAD:** Ciencias Matemáticas y Físicas	
CARRERA: Ingeniería en Networking y Telecomunicaciones		
FECHA DE PUBLICACIÓN: 15 de diciembre del 2016	**N° DE PÁGS.:** 100	
ÁREA TEMÁTICA: Investigativa		
PALABRAS CLAVES: Investigación, Análisis Forense Digital		
RESUMEN: La propuesta del presente proyecto es realizar el análisis de la implementación de laboratorio forense digital dentro de la carrera de Ingeniería en Networking y Telecomunicaciones		
N° DE REGISTRO:	**N° DE CLASIFICACIÓN:**	
DIRECCIÓN URL:		
ADJUNTO PDF	[X] **SÍ**	[ ] **NO**
CONTACTO CON AUTOR: Mite Villón Jimmy Rolando	**TELÉFONO:** 0981041307	**E-MAIL:** Jimmy.mitev@ug.edu.ec
CONTACTO DE LA INSTITUCIÓN:	**NOMBRE:** Ing. Jorge Chicala Arroyave, M.Sc.	
	TELÉFONO: 2307729	

REPOSITORIO NACIONAL EN CIENCIAS Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS

"SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES**"**

	REVISORES: Lcda. Viviana Pinos Medrano, M.Sc, LSI. Oscar Apolinario Arzube, M.Sc**.**
INSTITUCIÓN: Universidad de Guayaquil	**FACULTAD:** Ciencias Matemáticas y Físicas
CARRERA: Ingeniería en Networking y Telecomunicaciones	
FECHA DE PUBLICACIÓN: 15 diciembre del 2016	**N° DE PÁGS.:** 100
ÁREA TEMÁTICA: Investigativa	
PALABRAS CLAVES: Investigación, Análisis Forense Digital	
RESUMEN: La propuesta del presente proyecto es realizar el análisis de la implementación de laboratorio forense digital dentro de la Carrera de Ingeniería en Networking y Telecomunicaciones	
N° DE REGISTRO:	**N° DE CLASIFICACIÓN:**
DIRECCIÓN URL:	
ADJUNTO PDF	[X] **SÍ** [ ] **NO**
CONTACTO CON AUTOR: Sánchez Montero Yuris Rafael	**TELÉFONO:** 0989658796 / **E-MAIL:** yuris.sanchez27@gmail.com
CONTACTO DE LA INSTITUCIÓN:	**NOMBRE:** Ing. Jorge Chicala Arroyave, M.Sc.
	TELÉFONO: 2307729

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, "**SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES.**" Elaborado por el **SR. MITE VILLÓN JIMMY ROLANDO,** Alumno no titulado de la Carrera de Ingeniería en Networking y Telecomunicaciones, Facultad de Ciencias Matemáticas y Físicas, 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

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, "**SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES.**" Elaborado por el **SR. SÁNCHEZ MONTERO YURIS RAFAEL,** Alumno no titulado de la Carrera de Ingeniería en Networking y Telecomunicaciones, Facultad de Ciencias Matemáticas y Físicas, 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

A Dios por ser quien siempre guía mi camino, a mis Padres que a pesar de ser pilares fundamentales siempre me apoyaron incansablemente a seguir adelante, mis hermanos, por ser una razón más para continuar y mirar siempre al frente pese a las grandes dificultades que pudieron vencernos, mis amigos y compañeros quienes sin importar nada a cambio compartieron su conocimiento y prestaron su ayuda.

DEDICATORIA

A mis Padres que siempre me brindan su apoyo incondicional, a mis hermanos que me motivaron a seguir mi Carrera Universitaria y no decaer ante cualquier adversidad.

AGRADECIMIENTO

Le agradezco a Dios por todas sus bendiciones, a mis padres, amigos y compañeros que siempre han estado presentes en todos mis proyectos.

AGRADECIMIENTO

Le agradezco a mi tía Sonnia Carrera por todo su apoyo ofrecido sin ningún interés y a mi padre el Sr. Yuris Sánchez Carrera por enseñarme a perseverar y trabajar.

TRIBUNAL DEL 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

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

LSI. Oscar Apolinario Arzube, M.Sc.
PROFESOR REVISOR DEL ÁREA -
TRIBUNAL

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

Ab. Juan Chávez Atocha, Esp.
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"

MITE VILLÓN JIMMY ROLANDO

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"

SÁNCHEZ MONTERO YURIS RAFAEL

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

"SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE 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: Mite Villón Jimmy Rolando

C.I.:0927371682

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

Guayaquil, 15 de diciembre del 2016

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

"SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE 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: Sánchez Montero Yuris Rafael

C.I.:0941218851

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

Guayaquil, 15 de 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 Mite Villón Jimmy Rolando, como requisito previo para optar por el título de Ingeniero en Networking y Telecomunicaciones cuyo problema es:

"SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES"

Considero aprobado el trabajo en su totalidad.

Presentado por:

Mite Villón Jimmy Rolando	0927371682
Apellidos y Nombres completos	**Cédula de ciudadanía N°**

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

Guayaquil, 15 de 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 Sánchez Montero Yuris Rafael, como requisito previo para optar por el título de Ingeniero en Networking y Telecomunicaciones cuyo problema es:

"SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES"

Considero aprobado el trabajo en su totalidad.

Presentado por:

Sánchez Montero Yuris Rafael	0941218851
Apellidos y Nombres completos	**Cédula de ciudadanía N°**

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

Guayaquil, 15 de diciembre del 2016

UNIVERSIDAD DE GUAYAQUIL

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

Autorización para Publicación de Tesis en Formato Digital

1. Identificación de la Tesis

Nombre del Alumno: Mite Villón Jimmy Rolando	
Dirección: Km 8 ½ Vía Daule, Sector Juan Montalvo, Coop. 8 de mayo Mz2192 Villa 27	
Teléfono: 0981041307	**E-mail:** Jimmy.mitev@ug.edu.ec
Facultad: Ciencias Matemáticas y Físicas	
Carrera: Ingeniería en Networking y Telecomunicaciones	
Título al que opta: Ingeniero en Networking y Telecomunicaciones	
Profesora guía: Ing. Jorge Chicala Arroyave, M.Sc.	
Título de la Tesis: SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES	
Temas Tesis: Implementación de laboratorio forense digital.	

2. Autorización de Publicación de Versión Electrónica de la Tesis

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 esta tesis.

Publicación electrónica:

Inmediata	**X**	Después de 1 año	

Firma Alumno: Mite Villón Jimmy Rolando

3. Forma de Envío:

El texto de la Tesis 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	

UNIVERSIDAD DE GUAYAQUIL

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

Autorización para Publicación de Tesis en Formato Digital

1. Identificación de la Tesis

Nombre del Alumno: Sánchez Montero Yuris Rafael	
Dirección: Durán "Cdla. Los Helechos" Mz c Sector 3 villa 30	
Teléfono: 0989658796	**E-mail:** yuris.sanchezm@ug.edu.ec
Facultad: Ciencias Matemáticas y Físicas	
Carrera: Ingeniería en Networking y Telecomunicaciones	
Título al que opta: Ingeniero en Networking y Telecomunicaciones	
Profesora guía: Ing. Jorge Chicala Arroyave, M.Sc.	
Título de la Tesis: SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES	
Temas Tesis: Implementación de laboratorio forense digital.	

2. Autorización de Publicación de Versión Electrónica de la Tesis

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 esta tesis.

Publicación electrónica:

Inmediata	**X**	Después de 1 año	

Firma Alumno: Sánchez Montero Yuris Rafael

3. Forma de Envío:

El texto de la Tesis 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

UG	Universidad de Guayaquil
DEFT	Digital Evidence & Forensic Toolkit
DAWF	DragonJAR Automatic Windows Forensic
RAM	Memoria de Acceso Aleatorio
HTML	Lenguaje de Marca de salida de Hyper Texto
Http	Protocolo de transferencia de Hyper Texto
Ing.	Ingeniero
M.Sc.	Master of Scienc
URL	Localizador de Fuente Uniforme
WWW	World Wide Web
TIC	Tecnología de Información de Comunicación
LXDE	Lightweight X11 Desktop Environment
S.O.	Sistema Operativo

ÍNDICE DE CUADROS

ÍNDICE DE IMÁGENES

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

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

SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

Autor: Mite Villón Jimmy Rolando – Sánchez Montero Yuris Rafael
Tutor: Ing. Jorge Chicala Arroyave, M.Sc.

RESUMEN

El presente proyecto de investigación tiene como objetivo presentar soluciones software Open Source demostrando su factibilidad para la implementación de un Laboratorio de Informática Forense, debido a que el número de incidentes en nuestra población aumenta conforme avanza la tecnología utilizando herramientas que ayudan al desarrollo de los delitos informáticos, generando actividades ilícitas que no tienen el adecuado seguimiento por no contar con un laboratorio especializado en Ciencias Forenses Digitales, el cual se encarga del análisis de los datos clasificados como evidencia digital basados en principios y lineamientos científicos con el propósito de encontrar a los posibles autores del acontecimiento ocurrido. Este estudio presenta las herramientas adecuadas con sus respectivos procedimientos para llevar a cabo un proceso forense, preservando la integridad y confidencialidad de los datos recolectados, tomando en cuenta que las pruebas encontradas pueden ser llevadas a un proceso legal con el fin de tener responsables estrictamente sancionados, además de conceptualizaciones destacadas, obtenidas de una metodología bibliográfica.

Palabras claves: Delitos Informáticos, Análisis Forense, Laboratorio Forense, Informática Forense.

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

FORENSIC SOFTWARE, ANALYSIS OF THE USE OF SOFTWARE TOOLS FOR IMPLEMENTATION OF A FORENSIC COMPUTER LABORATORY IN THE ENGINEERING CAREER IN NETWORKING AND TELECOMMUNICATIONS

Author: Mite Villón Jimmy Rolando – Sánchez Montero Yuris Rafael

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

ABSTRACT

The present research project aims to present Open Source software solutions demonstrating its feasibility for the implementation of a Computer Forensics Laboratory, because of the number of incidents in our population increases as the technology advances using tools that help the development of crime Generating illicit activities since they do not have an adequate follow-up because they do not have a specialized laboratory in Digital Forensic Sciences, which is the responsible for the analysis of the data classified as digital evidence based on scientific principles and guidelines in order to find the possible authors of the event occurred. This study presents the appropriate tools with their respective procedures to carry out a forensic process, preserving the integrity and confidentiality of the data collected, taking into account that the evidence found can be brought to a legal process in order to have strict sanction, in addition to outstanding conceptualizations, obtained from a bibliographical methodology.

Keywords: Cybercrime, Forensics, Forensic Laboratory, Computer Forensics.

INTRODUCCIÓN

La informática forense se ha convertido en una disciplina muy utilizada debido a su gran aporte para la sociedad, factor importante para la resolución de delitos donde su principal aliado es un computador, denominados entonces como ciberdelitos. La tecnología en la actualidad, cumple un papel muy importante dentro de cada estilo de vida, debido a su gran aporte para la ciencia lo que ha permitido el desarrollo de innovaciones tecnológicas revolucionando así, a la sociedad en general; por otra parte, y al ver que los progresos tecnológicos aumentan conforme pasan los días, existen personas que se aprovechan de estos desarrollos informáticos para realizar actos ilícitos que atentan contra la confidencialidad, integridad y disponibilidad de la información.

Un delito informático está atado a medios tecnológicos junto a evidencias digitales, donde información a recopilar no es la misma frente a otros análisis forenses. La evidencia digital es la parte más importante dentro de un proceso de análisis forense, esta es frágil y tiende a ser alterada o dañada con un movimiento indebido, por lo cual es necesario tener cuidado al momento del levantamiento de la misma, para esto Ecuador carece de un laboratorio de ciencias forenses digitales, permitiendo que los delitos informáticos no sean atendidos de la manera más adecuada y así poder combatir aquellos sucesos, donde lo conveniente es, seguir los procedimientos adecuados correspondiente al levantamiento de la evidencia digital, por lo tanto es indispensable contar con un laboratorio de informática forense digital el cual cuente con la incorporación de las herramientas software adecuadas para el proceso forense, haciendo énfasis a el análisis de los diferentes actos ilícitos con el fin de llegar a encontrar las personas responsables para luego seguir por un proceso legal.

Por otra parte, Latinoamérica cuenta limitadamente con Laboratorios de Informática Forense donde destaca Adalib Corp. uno de los más completo a nivel tecnológico para delitos informáticos, ubicado en Bogotá Colombia, quien, a pesar de brindar análisis forenses, adiciona a sus líneas de servicio: Seguridad de la Información y Servicio Legales. Cuenta con un personal amplio altamente

capacitado al igual que sus propios equipos, comandados por Encase Forencis, una solución comercial reconocida a nivel internacional por su capacidad de respuesta, complementado por un Hardware adecuado para el correcto funcionamiento de la herramienta, todos estos una vez unidos, son capaces de analizar múltiples evidencias digitales como: Tablets, Celulares Inteligentes y Unidades de disco (Londoño, s.f).

Tomando en cuenta que en la actualidad existe una lista muy competitiva de software comerciales y Open Source especializados en el tratamiento de la evidencia digital, donde se incluyen en este proyecto investigativo a DEFT y DAWF, describiendo a DEFT como una completa herramienta dedicada a la Informática Forense capaz de analizar cualquier dispositivo informático, con la finalidad de generar respuestas a los diferentes sucesos ocurridos dentro de un Sistema Operativo, cumple con un soporte completo para GNU/Linux y Windows, dando a conocer así, una desventaja hacia la familia Apple con su sistema operativo MacOs. A pesar de no contar con el soporte para S.O. Apple, DEFT se inclina completamente hacia la familia Windows, Sistema Operativo que cumple un porcentaje muy elevado en la población ecuatoriana, entre las principales herramientas que destacan a DEFT Linux, se encuentra Autopsy, aplicativo de ayuda capaz de realizar un análisis forense en tiempo real, haciendo prevalecer la integridad de la información, impidiendo una posible manipulación de los datos, adicional cuenta con la capacidad de buscar palabras claves que se relacionen con el delito planteado. Autopsy no deja atrás los navegadores web, donde puede extraer información sensible como los historiales, cookies y marcadores almacenados en un computador, siempre y cuando sea Google Chrome, Mozilla Firefox o Internet Explorer. A diferencia de DAWF, DEFT incluye en su paquete de soluciones donde se encuentran: recuperadores de archivos, recuperadores de contraseñas, analizadores de archivos, software para el análisis en dispositivos móviles, aplicaciones para el análisis de redes, entre otros.

Una de las principales ventajas de DEFT es, contar con la capacidad de ejecutar el Sistema Operativo sin la necesidad de ser instalado, solución que se denomina LIVE CD, donde solo se necesita de una computadora portátil con unidad de CD que cuente con la capacidad necesaria para agilitar los procesos a

realizar, esto permite la portabilidad del software forense para poderlo transportar hacia cualquier suceso ocurrido donde es imposible llevar todo el equipo forense, lo que convierte a DEFT en una herramienta necesaria para que un perito informático realice su respectivo proceso forense.

A pesar que DEFT es una herramienta muy completa, el actual proyecto presenta como ayuda o complemento a DAWF con el fin de corroborar que la información digital recolectada sea confiable y tenga validez en un proceso judicial. DAWF, es una herramienta orientada a trabajar en entornos Windows, la cual es muy sencilla al momento de ejecutar un análisis ya que cuenta con un solo botón, permitiendo al usuario iniciar o parar el análisis. A pesar de contar con una interfaz muy simple los resultados que muestra al culminar el proceso, son bastante útiles en un Análisis Forense, ya que puede mostrar la información completa del equipo analizado (configuraciones de red, software instalados, estado de los dispositivos, usuarios creados, procesos en ejecución, información de navegadores, contraseñas guardadas, información de clientes de mensajería instantánea, entre otros), como las activadas realizadas con hora y fecha, pese a trabajar netamente con Microsoft Windows, es compatible con todos sus Sistemas Operativos incluyendo Windows 10 como última actualización de Microsoft. Una de las principales funciones es el análisis de firmas de los archivos, lo que permite demostrar si un archivo ha sido modificado o no desde la creación del mismo.

El proyecto investigativo planteado, demuestra que tanto DEFT como DAWF son capaces de ayudar a generar un informe en cuanto a delito informático se refiere, las mismas que están a nivel de un software forense comercial pese a ser de código abierto, su popularidad y estadía en el mundo informático, hacen de las mismas un conjunto de soluciones óptimas para el desarrollo e implementación de un Laboratorio de Informática Forense, donde sus resultados en conjunto son favorables para un análisis forense, demostrando que la información recopilada sea eficiente ante los posibles procesos legales.

CAPÍTULO I

EL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

Ubicación del Problema en un Contexto

La tecnología informática ha evolucionado de tal manera que su influencia con la vida social abarca un gran número de áreas y es donde han surgido comportamientos ilícitos denominados generalmente como delitos informáticos. En relación a estos delitos varios son denunciados, pero la mayoría no son sentenciados ya que muchos de estos cargos son retirados por las mismas personas determinadas como víctimas, por el hecho, de no seguir el proceso de análisis de evidencias ya que esto implica tiempo y dinero.

Actualmente existe el Código Orgánico Integral Penal (COIP) quien se encarga de sancionar aquellos actos ilícitos, desde su aceptación el 10 de agosto del 2014 hasta el 31 de mayo del 2015 se registraron 626 denuncias por delitos informáticos, como lo indica la página web de la fiscalía (Fiscalía General del Estado, 2015). Entre los delitos que generan gran número de incidentes y que por ende presentan múltiples denuncias tenemos: apropiación indebida de valores económicos en cuentas bancarias, clonación de tarjetas de crédito, violación de datos personales, claves o sistemas de seguridad.

La implementación de un Laboratorio Forense en la Universidad de Guayaquil, siendo esta una de las instituciones más grandes y destacadas del País debido a sus logros y su alto nivel académico, razón por la cual la incorporación de un centro de estudio dedicado a la informática forense en una de sus entidades de mejor ubicación como lo es la Facultad de Ciencias Matemáticas y Físicas, Carrera de Ingeniería en Networking y Telecomunicaciones, ayudará a investigar y corroborar aquellos delitos que utilizan la tecnología para la ejecución de fraudes donde se encuentra involucrada la sociedad en general, en relación a dichos acontecimientos es importante centralizar la recolección de los datos y los

determinados análisis de evidencias en un lugar donde se lleve el adecuado tratamiento de la información como lo es un Laboratorio de Informática Forense Digital.

Situación Conflicto Nudos Críticos

El número de delitos informáticos en los últimos meses del 2016 registran aproximadamente 530 actos ilícitos donde la mayoría de estos son por obtención de datos utilizando medios electrónicos, lo que demuestra que hoy en día aquellos sucesos incrementan conforme avanza la tecnología la misma que está ligada a la implementación de nuevas plataformas que utilizan los datos importantes de las empresas, por lo cual dicha información se encuentra vulnerable ante cualquier actividad ilícita que gracias a los progresos tecnológicos aparecen nuevas herramientas y técnicas capaces de violar las seguridades de los diferentes sistemas que respaldan en su interior información confidencial (El Telegrafo, 2016).

Existen ciudades como Quito, Guayaquil, Cuenca, Machala entre otros, los cuales poseen un Laboratorio de Ciencias Forenses pero estos no se especializan en incidentes digitales, lo que indica, que aún no se cuenta con dicho laboratorio, por lo cual la Universidad de Guayaquil junto con estudiantes de la Carrera de Ingeniería en Networking y Telecomunicaciones, realizan un estudio de la implementación de un laboratorio el cual será capaz de analizar las evidencias digitales mediante lineamientos determinados que ayudarán a prevalecer la justicia en cuanto a delitos informáticos se refiere.

Contar con un laboratorio cuya función principal es el estudio de las evidencias digitales utilizando herramientas de software forense, involucra un personal altamente capacitado con los equipos adecuados para lograr identificar el suceso ocurrido, esto servirá de gran ayuda para aquellas personas, organizaciones públicas o privadas, donde su nivel de seguridad va por debajo de los conocimiento y destrezas de los diferentes tipos de “Hackers”.

Causas y Consecuencias del Problema

CAUSAS Y CONSECUENCIAS DEL PROBLEMA

CUADRO N° 1

CAUSAS	CONSECUENCIAS
No se cuenta con un laboratorio digital forense en la Carrera de Ingeniería en Networking y Telecomunicaciones de la Universidad de Guayaquil.	No poder demostrar ni sentenciar los diferentes actos ilícitos informáticos cometidos por los ciberdelincuentes, ya sean estos ocurridos tanto dentro como fuera de la Universidad de Guayaquil.
No poseer las herramientas necesarias para la ejecución de un análisis forense digital.	No se obtendrá suficiente evidencia digital para descubrir el acto ilícito realizado.
No contar con personal capacitado para la manipulación de las herramientas.	Mal manejo de las herramientas de software forense.
Recolección de evidencia digital sin procedimientos establecidos.	Información recopilada sin valor judicial.

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Investigación

Delimitaciones del Problema

El proyecto actual es desarrollado para un análisis de las posibles herramientas de software forense DEFT y DAWF que se utilizaran en el laboratorio con las siguientes consideraciones:

Campo: Empresarial

Área: Redes - Software .

Aspecto: Estudio de los diferentes tipos de software para el uso en un laboratorio forense.

Tema: “Software Forense, análisis del uso de las herramientas software para la implementación de un laboratorio de informática forense en la carrera de Ingeniería en Networking y Telecomunicaciones”.

Formulación del Problema

El problema planteado es ¿De qué forma herramientas de software Open Source como: DEFT y DAWF, contribuirán al desarrollo de un Laboratorio de Informática Forense en la Carrera de Ingeniería en Networking y Telecomunicaciones, Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil?

Evaluación del Problema

Los principales aspectos que se ajustan al actual proyecto de investigación son los siguientes:

Delimitado: La implementación del Laboratorio Digital Forense se realizará dentro de la Facultad de Ciencias Matemáticas y Físicas en la carrera de Ingeniería en Networking y Telecomunicaciones.

Claro: Mejorar el proceso de análisis forense mediante alineamientos que involucran el adecuado tratamiento de las evidencias digitales.

Relevante: La implementación de un Laboratorio Digital Forense conlleva un estudio científico exhaustivo, el cual una vez culminado ayudará a la comunidad educativa implementando los procesos adecuados de un Laboratorio Forense Digital, donde el compromiso es examinar minuciosamente las evidencias digitales, siguiendo políticas estandarizadas.

Contextual: El análisis que compromete la implementación de un Laboratorio Digital, servirá como guía para aquellas entidades donde su planeamiento apunta a un laboratorio especializado en ciencias forenses digitales.

Factible: Comprende el análisis de herramientas Open Source, las cuales no presentan valor monetario por tener licencia libre y que a pesar de ser no comerciales cuentan con las características adecuadas para levantar un proceso forense y así poder encontrar a la o las personas involucradas en un determinado delito informático.

Original: Actualmente no se cuenta con un laboratorio especializado en ciencias forenses, por lo cual se estudiará el software forense (DEFT, DAWF) para un Laboratorio Forense Digital dentro de la Universidad de Guayaquil, proyecto que

generará controversia por ser una de las primeras universidades en la implementación de un laboratorio especializado en delitos informáticos.

Alcance del Problema

Optimizar y consolidar el proceso de un análisis forense digital, donde existen diferentes fuentes de información pese al gran avance de la tecnología, además de evaluar las herramientas Open Source DEFT y DAWF con el propósito de cumplir el desempeño forense en sistemas operativos determinados como GNU/Linux y Windows de computadores portátiles o de sobremesa, lo que permitirá servir de guía para el correcto uso de las herramientas software que se utilizaran en la implementación de un laboratorio forense digital.

Es importante destacar las posibles soluciones donde las pequeña y medianas empresas son beneficiarias para la ejecución del antes mencionado laboratorio, así mismo enfatizar que el Laboratorio Forense Digital estará a disposición de la comunidad siempre y cuando la Universidad de Guayaquil decida prestar sus servicios, donde la práctica en casos reales es el mayor propósito para un buen desempeño del Laboratorio.

Objetivos de la Investigación

Objetivo General

Definir las ventajas y desventajas referente a las herramientas de software forense: DEFT y DAWF, para medir su factibilidad frente a los diferentes actos ilícitos que atentan contra la confidencialidad, integridad, y disponibilidad de los recursos informáticos.

Objetivos Específicos

- Desarrollar el estudio de la herramienta DEFT, para analizar e interpretar las funciones que nos permiten realizar un adecuado tratamiento de la evidencia digital en cuanto a un delito informático.

- Determinar el comportamiento del software forense DAWF, para complementar el desempeño de la herramienta Open Source en un Análisis Forense Digital.
- Establecer si el uso de software orientados al Análisis Forense: DEFT y DAWF es el adecuado para la Implementación de un Laboratorio Forense Digital en la Carrera de Ingeniería en Networking y Telecomunicaciones.

Justificación e Importancia de la investigación

El presente proyecto investigativo tiene el fin de servir como guía ante la implementación de un Laboratorio de Informática Forense, haciendo énfasis en las herramientas software a utilizar, las cuales serán el pilar para que un análisis sea lo suficientemente útil en la búsqueda de los presuntos responsables del delito.

Contar con un laboratorio especializado en informática forense ayudaría contundentemente a la sociedad que se encuentra involucrada con fraudes electrónicos, donde dejar el caso ocurrido en manos expertos es su mejor opción. Para de esta manera poder combatir con aquellas personas malintencionadas que buscan causar perjuicios.

Además, el presente proyecto consta con la fundamentación teórica correspondiente donde resaltan temas como: la ciencia forense, objetivos y usos de la informática forense, delitos informáticos y sus tipos de ataques, tipos de fases para el análisis, herramientas que se pueden en utilizar en un análisis forense, entre otros; con la finalidad de ayudar a los investigadores a entender esta disciplina y a desarrollar un correcto análisis forense digital.

El aumento de los ataques informáticos hacia personas, organizaciones o entidades financieras son las razones para que el actual proyecto de titulación se lleve a cabo, donde la Universidad de Guayaquil y los alumnos de la carrera de Ingeniería en Networking y Telecomunicaciones, argumentan que a través del uso de las herramientas de software forense, técnicas y procedimientos adecuados se

podrá recabar información la cual servirá de evidencia para demostrar un delito informático.

Debido a los informes de múltiples denuncias donde se asocian delitos informáticos y al ver que estos no son tratados como cualquier otro proceso forense por no contar con el personal o con las herramientas adecuadas, demuestra que la falta de un Laboratorio Informático especializado en Ciencias Forenses con todo el equipamiento software, es importante para llevar a cabo procesos legales dirigidos a personas que atentan contra la seguridad de la información.

Elaborar un centro forense con soluciones Open Source que se actualizan frecuentemente con el objetivo de corregir errores o realizar mejoras y que están al alcance de cualquier usuario debido a las condiciones de su licencia, lo cual basta con descargar el aplicativo desde la página web del proveedor y hacer uso del mismo para fines personales o profesionales; a pesar de no representar ningún valor monetario, las herramientas Open Source cumplen las expectativas necesarias para realizar un correcto análisis forense involucrando el correcto tratamiento de la evidencia digital.

CAPÍTULO II

MARCO TEÓRICO

Antecedentes del Estudio

En la actualidad no se cuenta con un laboratorio especializado en los delitos informáticos pese a la gran cantidad de sucesos ocurridos en los últimos años donde se ven envueltos equipos tecnológicos e información digital, lo que indica que Ecuador es vulnerable ante delitos informáticos por no contar con un sustento ante los sucesos ocurridos, por esta razón la Escuela Superior Politécnica del Litoral junto con un grupo de personas, estudiantes de dicha universidad, realizaron un estudio en el 2011 donde su objetivo era la implementación de un Laboratorio Forense Digital dentro del campus estudiantil, en ella se destaca la gran necesidad de un laboratorio especializado en el tratamiento de la información y recolección de las evidencias digitales para beneficio de las personas que resultaban ser víctimas de estos actos ilícitos y también de la universidad ya que era un progreso tecnológico para la institución (Calderón Valdiviezo, Guzmán Reyes, & Salinas González, 2011).

A pesar que Ecuador no cuenta con un sitio especializado para el análisis de casos de delitos informáticos, Latinoamérica tiene uno de los Laboratorios Forenses más completos, el cual lo posee Colombia, Adalib Corp. Quien tiene 10 años de investigación forense como lo indica su sitio web (www.adalib.com), su equipamiento está diseñado por ellos mismos, con software forense especializado para diferentes tipos de delitos, equipos que disminuyen el tiempo de investigación a tan solo semanas lo que antes tomaba meses, pese a ser una gran empresa presta sus servicios a clientes finales que requieren la recuperación de información de un dispositivo de almacenamiento determinado cuando ha sido borrada, así mismo sus servicios llegan a instituciones públicas y privadas que son afectadas por determinados actos ilícitos. De acuerdo a estas investigaciones y al ver que una de las empresas más desarrolladas y dedicada a los delitos informáticos se encuentra en Colombia, como principal objetivo es el estudio de las herramientas software DEFT y DAWF para la implementación de un

Laboratorio Forense Digital dentro de la Universidad de Guayaquil, lo que serviría de gran ayuda para combatir los múltiples delitos informáticos que se presentan de manera continua en Ecuador, un laboratorio especializado, equipado con las herramientas software adecuadas para centralizar la información digital, donde la eficiencia resalta en el tratamiento exhaustivo de los datos.

Fundamentación Teórica

Ciencias Forenses

Las ciencias forenses se pueden definir como un conjunto de disciplinas donde el objetivo fundamental es la recolección de pruebas para posteriormente vincularlo con un proceso judicial mediante métodos científicos; generalmente el término forense se lo familiariza con procedimientos como autopsias, cadáveres, pero la realidad es que, abarca un gran número de disciplinas, incluyendo la informática.

ANÁLISIS FORENSE DIGITAL

IMAGEN N° 1

Elaborado: Andrés Guzmán Caballero

Fuente:https://www.ambitojuridico.com/BancoConocimiento/Procesal-y-Disciplinario/la-valoracion-de-la-evidencia-digital-en-el-codigo-general-del-proceso.cshtml

Por lo tanto, el Análisis Forense Digital inclina a las ciencias forenses hacia el ambiente de los sistemas informáticos, sin embargo, es orientada para aquellos que están relacionados con las Tecnologías de la Información y las

Comunicaciones, donde se encuentra la piratería de software, piratería de comunicaciones, pornografía infantil, intrusiones y delitos informáticos en organizaciones, entre otros.

Objetivos de la informática forense

Entre los principales objetivos de la informática forense se encuentra la recolección de evidencias seguido de los siguientes puntos:

- La compensación de los daños realizados por la o las personas delictivas.
- El proceso legal correspondiente a las personas declaradas como criminales.
- implementación de medidas con el fin de evitar futuras acciones ilicitas.

Usos de la informática forense

Para la informática forense existen múltiples usos, donde muchos de ellos se originan de la vida diaria y no precisamente deben estar atados a la informática forense. Zuccardi & Gutiérrez (2006) destacan los siguientes usos:

- **Prosecución Criminal:** Los hechos incriminatorios suelen ser tomados para procesar múltiples crímenes como, homicidios, femicidios, fraudes financieros, distribución de sustancias psicotrópicas y estupefacientes.
- **Litigación Civil:** La informática forense puede aportar ayuda con temáticas que incluyan disoluciones conyugales, estupro, acosos sexuales entre otros.
- **Investigación de Seguros:** Los datos adquiridos de dispositivos informáticos facultarían una ayuda o soporte para las empresas aseguradoras con la finalidad de decrecer los costos por accidentes y retribuciones por la misma.
- **Temas corporativos:** La información referente a aspectos que incluyan espionaje a nivel industrial, divulgación u apropiación de información restringida, así como temáticas referentes a robos y acosos sexuales.
- **Mantenimiento de la ley:** La informática forense aportaría en la obtención o búsqueda en su parte primaria de órdenes judiciales y bajo la legalidad

que otorga la orden judicial la latente infiltración en la búsqueda de información (p.4).

Delito Informático

Un delito informático se lo puede considerar como cualquier actividad ilícita donde se encuentra asociado un computador y tiene la finalidad de obtener datos sensibles como contraseñas, número de celulares, identificación personal, cuentas bancarias, entre otras, las mismas que serán aprovechadas a favor del delincuente. Una de las entidades que sanciona este tipo de actos ilícitos es el COIP (Código Orgánico Integral Penal) sistema entró en vigencia el 10 de agosto del 2014 con el objetivo de disminuir el caso de delitos informáticos, entre los acontecimientos contemplados como delitos se encuentran: transferencia de dinero de forma ilegal, obtención y revelación de base de datos, acceso no autorizados a sistemas de información, pornografía infantil y acoso sexual.

Una de las empresas que se encarga de proteger los sistemas informáticos es GMS - Seguridad de la Información, la cual milita en el Ecuador sostiene que nuestro país debido al crecimiento económico puede tener más ataques ilícitos comparados a las cifras ya establecidas donde hasta el 2014 sumaban 60’090.173 ataques, un experto de Kaspersky afirma que 16% de los usuarios son víctimas de delitos informáticos (El Universo, 2014). La problemática de los delitos informáticos requiere un estudio especial en nuestro país con vistas a determinar la medida en que la legislación penal (códigos penales y leyes especiales) deba prever la incidencia en los citados ilícitos. Una de las peculiaridades de este tipo de delitos es que desafortunadamente no conllevan una problemática local; la existencia de redes internacionales como Internet, abren la posibilidad de transgresiones a nivel mundial y con gran impunidad. Entre las recomendaciones que se pueden tomar en cuenta para evitar un tipo de delito informático tenemos las siguientes:

- Evitar realizar cualquier tipo de transacciones cuando esté conectada a una red wifi pública.

- Procurar entrar a las páginas webs de manera segura, evitando ingresar por links sugeridos o cualquier tipo de enlace que no sea la principal dirección.
- Tener siempre actualizado el sistema operativo.
- Verificar que el sitio a navegar tenga certificado digital o sea reconocida como página segura.
- Tener password diferentes para cada una de las cuentas.
- Contar con un correcto antivirus instalado, el cual detecte las diferentes anomalías en el pc o en la navegación de páginas de internet.
- Actualizar las contraseñas frecuentemente.

Tipos de Delitos Informáticos

Los tipos de delitos reconocidos por La Organización de Naciones Unidas son los siguientes:

Fraudes cometidos mediante manipulación de computadoras

- **Manipulación de los datos de entrada:** Es uno de los delitos más utilizados en el ámbito informático ya que comprende la obtención de información para fines delictivos.
- **La manipulación de programas:** Tal como su nombre lo indica, consiste en la modificación de un software determinado alterando su funcionamiento para sacar provecho de los procesos ejecutados, se necesita de altos conocimientos técnicos ya que el objetivo de este delito es evitar que sea detectado, por lo cual el delincuente inserta códigos donde no se vea afectado el proceso principal.
- **Manipulación de los datos de salida:** Un ejemplo muy común es el caso de los cajeros automáticos donde dicha computadora se ve obligada a realizar procesos diferentes, como lo es: captar la información de la tarjeta electrónica o clonar la banda magnética, todo esto con el fin de acceder a su cuenta bancaria.
- **Fraude efectuado por manipulación informática:** Comprende la disminución monetaria en porciones muy pequeñas, suele pasar con las

cuentas bancarias donde el atacante se transfiere la mínima cantidad de dinero (0.01) para que la víctima no sospeche nada, tomando este ejemplo y multiplicándolo por todas las personas a quien el delincuente decide debitar da como resultado una excedida suma de efectivo.

Manipulación de los datos de entrada

- **Como objeto:** Sucede cuando la documentación almacenada en un determinado computador es alterada.
- **Como instrumento:** Involucra a las computadoras como parte de un delito informático, siendo estas utilizadas para realizar la modificación de información.

Daños o modificaciones de programas o datos computarizados

- **Sabotaje informático:** Corresponde a las conductas ilícitas que se ejecutan para evitar que el equipo o sistema atacado pueda realizar sus funciones normalmente.
- **Acceso no autorizado a servicios y sistemas informáticos:** En cuanto a estos accesos comprende aquellas acciones que saltan las seguridades para un fin determinado, ya se esté por curiosidad o algún tipo de delito informático.
- **Reproducción no autorizada de programas informáticos de protección legal:** Se puede considerar como pérdida económica para el o los propietarios del software comercial, esto ocurre cuando se hace uso de un programa de forma fraudulenta sin haber obtenido los derechos de ejecución, donde la forma habitual es adquiriendo la respectiva licencia (Carrion, 2001, p.1).

Metodología y fases de un análisis forense

En la ejecución de un análisis forense se necesita de 3 fases fundamentales el cual dependiendo del caso puede dividirse en más.

Adquisición de datos

La adquisición de datos es una etapa muy delicada en el ámbito forense, debido a que la recolección de información debe realizarse minuciosamente evitando ser manipulada por terceras personas, lo que no serviría de ayuda si la evidencia digital demuestra impurezas demostrando origines que no son reales. Para esto una vez que se ha detectado alguna anomalía de seguridad, la persona responsable debería decidir si el equipo designado como evidencia debería de apagarse o mantenerse encendido ya que existen registros que se almacenan en la memoria volátil y al apagarse se borrarían del sistema impidiendo ser recolectadas, por lo cual es importante que el analista tenga en cuenta el escenario donde va a trabajar.

Uno de los principales problemas dependiendo del caso, es obtener el nombre de la persona responsable del ordenador, teniendo presente que la mayoría de personas generalmente utilizan sobrenombres para la identificación de un usuario, siempre y cuando este no pertenezca a una organización, donde existen políticas que enrola al cliente con un determinado equipo, no obstante, es importante recolectar información como: número de series, características, modelos, sistema operativo, valor monetario, etc.

Una vez obtenida la información principal el siguiente paso es localizar los dispositivos de almacenamiento que están conectados o están siendo utilizados por el computador, como: memoria de almacenamiento masivo, memorias RAM, unidades de CD o DVD, discos duros, entre otros. Luego de la detección se debe registrar la marca, número de serie, modelo, donde estaba ubicado, extensiones de archivos, cantidad de espacio utilizada, esto con el fin de dar inicio al último paso, la clonación bit a bit, permitiendo una copia igual de las unidades a analizar con el objetivo de mantener la integridad de los datos y así poder llevarse una copia exacta de la evidencia digital, la ejecución de dicha clonación deberá hacerse mediante un LiveCD, evitando de esta manera alterar los datos originales. Es importante comprobar que la unidad clonada esa exactamente idéntica, permitiendo realizar modificaciones con el fin de extraer la mayor parte de huellas digitales, por consiguiente, se debe trasladar los dispositivos hallados hacia el laboratorio donde se realizará el respectivo Análisis Forense y la investigación.

Análisis e investigación

La etapa de análisis e investigación es una fase que requiere un alto conocimiento por parte del investigador ya que se consta con varias fuentes de obtención como lo son:

- Logs de los sistemas operativos analizados.
- Logs de sistemas detectores de intrusos.
- Logs de los firewalls
- Archivos del sistema operativo analizado.

En cuanto a las carpetas personales de los usuarios, no se encuentran dentro de esta categoría aquellas que son creadas por el mismo sistema operativo, por consiguiente, es recomendable contar con el asesoramiento adecuado para este tipo de recolección de los datos, ya que un mal tratamiento podría ocasionar graves problemas en la investigación, además de violar cualquier proceso legal sin tener conocimiento del mismo. Es esencial que la investigación esté orientada a encontrar todas las posibles evidencias en la información que no está catalogada como personal, ya que a estos datos solo se puede acceder mediante una orden judicial. Para realizar los respectivos análisis se debe tomar en cuenta los siguientes tipos:

- **Físico:** Datos que están fuera del alcance del sistema operativo.
- **Lógico:** Datos que se encuentran vinculados con el funcionamiento del sistema operativo donde se puede obtener registros de incidentes como: archivos que fueron eliminados, estructura de los archivos, tamaño, hora, fecha de creación y modificación de los archivos.

Una de las primeras acciones que se tienen que efectuar es validar o configurar la hora exacta en el sistema con el propósito de evitar que la información recolectada sea cuestionada durante el proceso forense a efectuar. Entre las principales herramientas por excelencia para esta fase de análisis e investigación tenemos; DEFT (Digital Evidence & Forensic Toolkit) y DAWF (DragonJAR

Automatic Windows Forensic), las cuales presentan un número de herramientas considerables para llevar a cabo el proceso dentro de un delito informático.

Redacción del informe

La redacción del informe puede ser muy compleja ya que en ella se encuentra toda la información recabada como evidencias, pruebas, e indicios del análisis realizado el cual debería estar redactado de forma clara y concisa ideal para que una persona ya sea o no experto pueda entender el informe a entregar. Todo informe deberá tener una fecha bien establecida indicado la finalización del proceso de igual manera con el número y nombre de personas involucradas en dicho proceso. Existen 2 tipos de informes: Ejecutivo y Técnico.

Informe ejecutivo

Está orientado hacia aquellas personas que no manejan un buen perfil técnico, pero se ubican en los altos rangos de una organización, por ejemplo: gerentes, sub gerentes, jefes departamentales, etc. Por tanto, el lenguaje del informe no debe ser muy técnico y, si se utiliza alguna modalidad, tiene que ser sustentada de forma clara y concisa. Este informe consta de los siguientes puntos:

- **Introducción:** objetivo del informe, detalles como el coste del incidente sucedido.
- **Descripción:** detalle de las acciones ocurridas durante el análisis por parte del sistema, tomando en cuenta ser aclaradas de una manera no muy técnica ya que dicho informe puede llegar a manos de personal con escasos conocimientos en la materia.
- **Recomendaciones:** acciones que pueden ser realizadas después de comprobar el incidente con el fin de evitar un suceso igual o peor.

Informe técnico

A diferencia del informe ejecutivo, este si incluye palabras técnicas ya que va dirigido hacia personas como: ingenieros, tecnólogos, expertos en el área, superiores, entre otros, el cual tiene como objetivo detallar los sucesos ocurridos

durante el Análisis Forense. Para la redacción del informe se debe tener en cuenta los siguientes puntos:

- **Introducción:** detalla el objetivo del informe como los puntos a seguir durante la redacción del mismo.
- **Preparación del entorno y recogida de datos:** procedimiento a seguir para la ejecución de análisis forense como la adquisición de los datos y el análisis e investigación.
- **Estudio forense de las evidencias:** describe las evidencias halladas y su definición en el ámbito forense.
- **Conclusiones:** sección donde se describen detalladamente las conclusiones como resultado final después del proceso forense realizado.

Software Forense

El campo software forense implica los distintos tipos de herramientas que ayudan a resolver sucesos ocurridos en un ambiente forense; existen soluciones comerciales y de código abierto, donde uno de los pioneros en el mercado es EnCase Forensic de sustentación monetaria por tener una mejor distribución y tiempo respuesta incomparable a los demás software, por otro lado se encuentran varias aplicación de código libre entre las que destacan: DEFT (Digital Evidence & Forensic Toolkit) y DAWF (DragonJAR Automatic Windows Forensic), que a pesar de ser Open Source cumplen con las funcionalidades que requiere un Análisis Forense Digital, debido a su gran trabajo en al ambiente forense. DEFT y DAWF son las adecuadas para la implementación de un Laboratorio Forense Digital con el fin de optimizar los recursos y la economía.

DEFT (Digital Evidence & Forensic Toolkit)

Es una distribución Live CD (booteable desde cualquier unidad de CD o DVD) basada en Lubuntu (Ubuntu con entorno LXDE), con una interfaz muy atractiva y fácil de usar, posee un amplio listado de las mejores soluciones forenses que realizan procesos como el análisis, recolección o recuperación de datos, con una excelente detección del hardware, sus inicios comienzan en el año 2005 donde se publicó su primera versión la cual fue desarrollada en Italia.

DEFT (DIGITAL EVIDENCE & FORENSIC TOOLKIT) LINUX

IMAGEN N° 2

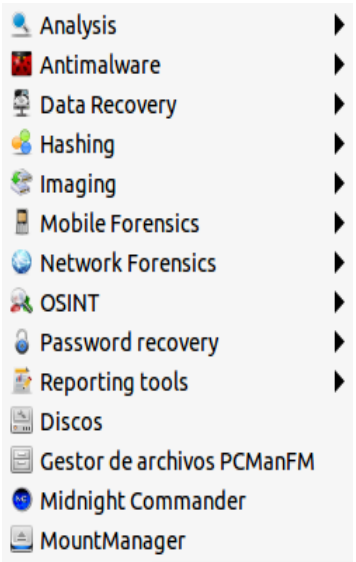
Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Investigación

Es un sistema fácil de usar con aplicaciones de código abierto dedicado a la respuesta de incidentes y análisis informático forense. El objetivo de DEFT es recolectar todas las herramientas posibles que permitan establecer un análisis forense digital y que estén a disposición para combatir los múltiples ciberdelitos.

HERRAMIENTAS DE DEFT LINUX

IMAGEN N° 3



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Investigación

Es una de las distribuciones de análisis forense que ha demostrado un progreso destacado en los últimos años, no solo han añadido una gran cantidad de herramientas forenses a su lista, sino que han sabido adaptarse a su entorno y emular las características de otras distribuciones similares. Entre las principales herramientas Open Source recogidas e incluidas por su funcionalidad ante un Análisis Forense tenemos las siguientes, las cuales se encapsulan dentro de un menú principal denominado DEFT:

- **Analysis** - Herramientas forenses destinadas al análisis de ficheros.
- **Antimalware** - Búsqueda de códigos maliciosos.
- **Data recovery** - Software para recuperación de ficheros
- **Hashing** – Soluciones para el cálculo de Hashes.
- **Imaging** – Clonación de discos bit a bit.
- **Mobile Forensics** – Herramientas para el análisis forense en dispositivos móviles.
- **Network Forensics** – Aplicativos para el análisis forense en redes.
- **OSINT Navegador Goole Chrome** – Aplicación de navegación web. personalizada con la finalidad de obtener información relacionada a un usuario y sus actividades realizadas.
- **Password recovery** – Software para la recuperación de contraseñas.
- **Reporting tools** – Herramientas para la generación de informes.

DEFT se encuentra actualmente en su versión 8.2, incluyendo en sus mejoras escritorio LXDE y gran variedad de aplicaciones utilitarias como gestores textos, archivos y ventanas, reproductores de música, entre otros. Adicionando también herramientas actualizadas dedicas al Análisis Forense. En las últimas versiones 8.1 y 82, se incluyeron unas cuantas novedades bastantes interesantes:

- Corrección del archivo /etc/resolv.conf
- Se ha corregido el error del sources.list apt-get
- Mejora el reconocimiento de dispositivos en modo directo
- Actualizado todos los paquetes a la última versión de Ubuntu disponible para cuánticos.

- Status de los discos en el gestor de archivos.
- Cifrado de unidades de almacenamiento mediante la herramienta Bitlocker.
- The Sleuthkit 4.1.3 permite la recuperación de archivos y analizar las imágenes ISO de los discos.
- Digital Forensics Framework 1.3 permite la generación de informes de los diferentes tipos de actividades generados en el sistema, una vez analizada la memoria volátil.
- Soporte para Smartphone imagen de las particiones incluyendo directorios y archivos en Android y iOS 7.1.
- JD GUI, es una utilidad grafica el cual permite descomprimir y examinar java 5, accediendo de manera instantánea a los métodos y campos.
- Inclusión de Skype Extractor 0.1.8.8
- Actualización de OSINT browser

DAWF (DragonJAR Automatic Windows Forensic)

Es una herramienta que anteriormente solo cumplía ciertas tareas específicas dentro de un análisis forense pero al ver que era útil para otras necesidades se optó por mejorarla, Restrepo (2016) fundador de DragonJAR comunidad dedicada al analisis forense quien a su vez DAWF (DragonJAR Automatic Windows Forensic) lleva su nombre por integrar herramientas que ayudaban su proceso, integró una interfaz sencilla orientada a las personas no profesionales pero con ganas de involucrarse en el mundo forense digital.

DAWF también es llamada ‘herramienta de botón gordo” debido a que dentro de su interfaz solo cuenta con un botón de ejecución. Esta herramienta cuenta 2 entornos:

- **Entorno Windows Vivo**: Permite la recolección de información cuando el equipo determinado como evidencia este encendido realizando una extracción de la memoria RAM mientras está corriendo y almacenando procesos que pueden ser vital para hallar al supuesto responsable.

- **Entorno Windows Revivido:** Es ideal cuando se ha realizado una clonación de las unidades de almacenamiento siguiendo los procedimientos adecuados, haciendo prevalecer la integridad de la información para luego sacar provecho de la imagen y así poder realizar los respectivos análisis sin realizar algún tipo de alteración en la evidencia original.

DAWF (DRAGONJAR AUTOMATIC WINDOWS FORENSIC)

IMAGEN N° 4

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Investigación

DAWF tiene una funcionalidad muy sencilla, basta con seleccionar el tipo de entorno antes mencionado y como paso siguiente dar clic en el botón “Inicio” el cual activa la ejecución de los procesos de análisis forense para la recolección de información, una vez culminado se crea una carpeta dentro del directorio del ejecutable con un nombre determinado proporcionado automáticamente por el sistema donde se encontrará la información extraída durante el proceso realizado.

En el interior de la carpeta herramientas se encuentran todas las aplicaciones que utiliza DAWF para lograr la mayor extracción de información, cuenta con dos archivos de texto entornoVivo.txt y entornoMuerto.txt, estos archivos son los que se encargan de enviar las instrucciones para que estas sean ejecutadas por DAWF. Hay que tener en cuenta que al ejecutar en un Entorno Vivo y no haber seleccionado la opción “Dumpear solo la RAM y SisInfo” se empezaran a realizar

procesos que podrían alterar la evidencia digital. DAWF como Software Forense cuenta con las siguientes funcionalidades:

- **Herramienta de BOTÓN GORDO:** Está diseñada para que cualquier usuario sin importar su perfil técnico lo pueda ejecutar para obtener un informe detallado de la auditoria del sistema. Es importante que se ejecute como administrador ya que necesita de permisos especiales para acceder a los procesos a analizar, posee un inicio automático el cual permite que DAWF se ejecute si por descuido se olvidó de presionar el botón.
- **Documenta Cada Acción Realizada:** Registra cada acción realizada con su respectiva fecha y hora exacta, además muestra las firmas de los archivos en diferentes formatos con el fin de corroborar que el o los ficheros no han sido modificados.
- **Funciona en Entornos Muertos y Vivos:** Cuenta con la opción de extraer la información de la memoria RAM cuando se trata de entornos vivos, para entornos muertos tiene el privilegio de ejecutar procesos donde se encuentra involucrada toda la información del dispositivo y así poder obtener resultados detallados de los sucesos ocurridos dentro de un sistema operativo determinado.
- **Portabilidad:** No necesita instalación, pese a ser solo un archivo ejecutable solo necesita permisos de administrador el cual se puede inicializar desde cualquier dispositivo de almacenamiento, además la generación de los informes los realiza dentro de la unidad ejecutada creando archivos nuevos sin comprometer a la evidencia digital.
- **Compatible con Windows XP-10:** Demuestra compactibilidad con la mayoría de Sistemas Operativos de la familia Microsoft, siendo el ultimo y con una cogida incomparable Windows 10, también cuenta con soporte para Windows XP ya que actualmente existen sistemas que aún se ejecutan bajo ese entorno, el cual pese a no tener soporte por parte del fabricante sigue siendo útil para varias compañías bancarias atentadas por delincuentes cibernéticos.
- **Parametrizable y Personalizable:** Puede ser ejecutada en sus dos modos antes mencionados, siempre y cuando sea con privilegios de

administrador, además cuenta con perfiles personalizables donde se puede omitir ciertos procesos que el investigador considere innecesarios.

- **Visual y Fácil de Entender:** Se puede tener un fichero con sentencias ya definidas, que realice instrucciones parecidas a DAWF, pero estos scripts no tienen determinado tiempo de respuesta, tampoco se puede visualizar que proceso está en ejecución, DAWF si muestra dichos detalles supervisando e indicando que procesos tiene ejecución incluyendo una barra de progreso donde se tiene en cuenta el tiempo que tardaría el análisis (Restrepo, 2016, p.1).

Comparación de Software Forenses

Es importante para el presente estudio demostrar las ventajas y desventajas de las herramientas incluidas en la implementación de un Laboratorio de informática Forense Digital, acotando las posibles soluciones que puede brindar cada software a estudiar, de tal manera que las funcionalidades incorporadas sirvan de gran ayuda cada proceso forense.

Por otra parte, y al ver que tanto DEFT como DAWF pueden trabajar en conjunto debido a que varias funciones de DAWF no se muestran en DEFT, esto demuestra que ambas herramientas sean imprescindibles para la ejecución de múltiples casos de Análisis Forenses.

Tomando en cuenta los aplicativos antes mencionadas, se ha realizado una tabla de comparación incluyendo EnCase Forencis, pionero en el mercado por sus destacadas funcionalidades, pero a diferencia de las demás herramientas, este, cuenta con un valor monetario para quienes lo desean utilizar. Presentando así, las diferentes características que posee DEFT, DAWF y EnCase, con el objetivo de mostrar lo favorable que resulta incorporar aplicativos Open Source en la implementación de un Laboratorio Forense Digital, demostrando que DEFT se asemeja en varias oportunidades a EnCase, pese a ser una solución Open Source.

COMPARATIVA DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO FORENSE DIGITAL

CUADRO N° 2

Características	DEFT	DAWF	ENCASE
Clonación de discos	X		X
Comprobación de integridad criptográfica	X		X
Información del sistema	X	X	X
Adquisición en vivo	X	X	X
Recuperación de contraseñas	X		X
Recuperación de archivos	X		X
Recuperación de correos			X
Análisis de navegadores	X		X
Análisis de firmas de archivos	X	X	X
Búsqueda de archivos	X		X
Reporte Automático / Manual	X	X	X
Volcado de memoria RAM		X	
Soporte sistema operativo Linux	X		X
Soporte sistema operativo Windows	X	X	X
Soporte sistema operativo Mac Os			X
Utilitarios extras	X		

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Investigación

Evidencia Digital

La evidencia digital es factor importante para el desarrollo de un proceso forense, donde se la puede definir como las pruebas que contiene información relevante a suceso ocurrido en formato digital y que puede ser usada en un juicio legal, donde la fiscalía y la sociedad en defensa presentan sus determinadas evidencias, las cuales pueden clasificarse en físicas y lógicas dependiendo del caso a tratar. Uno de los principales inconvenientes que enrola el tema de las evidencias es que muchas de estas pueden ser frágiles y necesitan cierto grado profesionalismo para una correcta recolección, lo que implica demostrar que dichas pruebas no han sido alteradas o modificadas durante el proceso forense. El procedimiento de una investigación por homicidio donde se vea comprometida la evidencia digital será totalmente distinto al que, se utilice en un suceso informático, por tanto, el tratamiento de los datos recolectados dependerá del tipo de fraude cibernético que se analizará.

Existen ciertas recomendaciones que se debe tener en cuenta al momento de la recolección de datos digitales, donde cualquier movimiento puede llegar a deteriorar la evidencia, impidiendo que los datos obtenidos sean capaces de cumplir con las expectativas del análisis forense.

- Evitar que el equipo utilizado en el crimen sea apagado ya que en la memoria volátil puede existir información importante para la resolución del caso.
- Desconectar los equipos de la red, previniendo que personas cómplices impidan el levantamiento de los datos mediante conexiones remotas al equipo en custodia.
- Mantener el sistema intacto sin realizar ninguna operación, evitando realizar cualquier proceso que puede llegar a sobrescribir los datos, complicando de esta manera llegar a detectar los verdaderos registros ocurridos.
- Impedir notablemente que los archivos del sistema sean abiertos, preservando de esta manera la fecha y hora exacta de los mismos.

Fuentes de Evidencia Digital

En cuanto a evidencias digitales, muchas veces se logra confundir con evidencia electrónica, ambos pueden ser usados como evidencia al igual que sinónimos, sim embargo dentro del campo de evidencia electrónica tenemos: PCs, CDs, DVDs, Memorias de todo tipo, mientras que en la evidencia digital la podemos definir en 3 grupos:

- **Sistemas de Computación Abiertos:** Comprende las computadoras personales incluyendo sus periféricos, como también las portátiles y los servidores, todos estos con ciertas características necesarias, capaz de cumplir infinidad de requerimientos.
- **Sistemas de Comunicación:** Involucra a las redes de telecomunicaciones ya sea esta cableada o inalámbrica, donde se puede encontrar parte de la evidencia digital.
- **Sistemas Convergentes de Computación:** Son los denominados Smartphone, PDAs, equipos inteligentes, etc., aquellos dispositivos que tienen características similares a un computador y que son capaces de generar y obtener evidencia digital.

Características de la Evidencia Digital

La evidencia digital es frágil frente a posibles modificaciones que pueden alterar el proceso forense, sin embargo, se puede prevalecer la integridad siguiendo ciertos lineamientos que ayudan a mantener los datos originales de un delito informático, para esto, hay tener en cuenta ciertas características que ayudan en el adecuado tratamiento de la misma:

- **Es Volátil:** Se puede perder la información con simple hecho de ejecutar cualquier acción indebida. Ej., al momento de apagar un equipo, de esta forma perderíamos la información que esta almacenada en la memoria RAM o CACHE del equipo.

- **Es Anónima:** Difícil de encontrar donde se encuentra la evidencia digital, ya que siempre se localiza en diferentes fuentes de información.
- **Es Duplicable:** Puede ser duplicada de manera exacta para luego ser analizada y evaluada en el proceso forense respectivo, sin manipular la evidencia original.
- **Es Alterable y Modificable:** Puede mostrarse alterada o modificada, no obstante, actualmente existen herramientas para comprobar dichas manipulaciones y poder así, mantener la integridad del caso.
- **Es Eliminable:** Se puede eliminar de manera fácil, tomando en cuenta las múltiples técnicas que implica el suprimir una información, pese a esto el registro u archivo puede ser recuperado en un proceso forense ya que existen sitios donde guardan copias y estas pueden ser encontradas con aplicativos de recuperación.

Categorías de la Evidencia Digital

Entre las categorías que comprende una evidencia digital tenemos:

- **Registros Almacenados en el Equipo de Tecnología Informática:** Son aquellos ficheros que son creados y almacenados por el usuario en una ubicación determinada del computador, registros que pueden llegar a demostrar la identidad de una persona con las acciones realizadas en el mismo archivo, estos pueden ser documentos en Word, Excel o de algún gestor que involucre interacción con el usuario.
- **Registros Generados por Equipos de Tecnología Informática:** Como su nombre lo indica son aquellos que se generan como parte de un sistema, presentan información relevante a sucesos ocurridos durante la ejecución de programa almacenando información de eventos que pueden servir para una posible auditoria del equipo.
- **Registros que Parcialmente ha sido Generados y Almacenados en Equipos de Tecnología Informática:** Son registros que necesitan de los dos antes mencionados ya que para corroborar ciertas actividades es importante la revisión de los logs (registros generado) y los ficheros sospechosos (registros almacenados) dentro de un Análisis Forense.

Incidente de Seguridad Informática

La definición de Incidente de Seguridad es amplia en el ámbito forense debido a la destacada evolución de la informática, pese a esto se puede considerar como, la infracción de las políticas de seguridad utilizando las buenas prácticas de los diferentes sistemas informáticos. En consecuencia, se detallan a continuación varios tipos de Incidentes que pueden llegar a causar cierto grado de afectación:

- **Incidentes de Denegación de Servicios (DoS):** Son aquellos cuya finalidad es consumir el rendimiento de sus recursos evitando de esta manera el correcto funcionamiento del servicio.
- **Incidentes de código malicioso:** Entre estos se considera todo tipo de virus, malware, gusanos, rootkit, etc., que se infiltre en el sistema y tenga objetivo alterar los procesos del mismo.
- **Incidentes de acceso no autorizado:** Ocurre cuando una persona determinada ingresa a cualquier sistema sin la autorización correspondiente.
- **Incidentes por uso inapropiado:** Se produce cuando usuarios evaden las seguridades con ayuda de aplicaciones para obtener acceso a sitios no autorizados, entre software más utilizados se encuentran: Tor y Ultrasurf
- **Incidente múltiple:** Cuando el acto ilícito comprende varios de los tipos antes mencionados.

Varios de los incidentes que se ejecutan hoy en día pueden entran en las categorías detalladas anteriormente, por lo cual es importante saberlas categorizar. Por ejemplo, un conjunto de instrucciones que se creó con la finalidad de alterar un sistema, y que logro insertarse, se lo puede encasillar dentro los Incidentes de código malicioso y no por Acceso no autorizado, por ser el virus la vía de infección.

Manipulación de la evidencia digital

Para conversar la evidencia digital y evitar algún tipo de manipulación es importante tener en algunos requisitos. Zuccardi & Gutiérrez (2006) destaca lo siguiente:

- Hacer uso de medios forenses estériles (para copias de información).
- Mantener y controlar la integridad del medio original. Esto significa, que, a la hora de recolectar la evidencia digital, las acciones realizadas no deben cambiar nunca esta evidencia.
- Cuando sea necesario que una persona tenga acceso a evidencia digital forense, esa persona debe ser un profesional forense.
- Las copias de los datos obtenidas, deben estar correctamente marcadas, controladas y preservadas. Y al igual que los resultados de la investigación, deben estar disponibles para su revisión.
- Siempre que la evidencia digital este en poder de algún individuo, éste será responsable de todas las acciones tomadas con respecto a ella, mientras esté en su poder.
- Las agencias responsables de llevar el proceso de recolección y análisis de la evidencia digital, serán quienes deben garantizar el cumplimiento de los principios anteriores. (p.11)

Peritos Informáticos

Anguas (2011) afirma. “Un perito debe tener formación y experiencia contrastable en el área objeto de pericia, de forma que pueda presentar un punto de vista sólido al respecto de las cuestiones que se le plantean” (p.8). Sin embargo, el desempeño de un perito reside en examinar los dispositivos informáticos, con el objetivo de encontrar información que sea relevante en el caso que se le ha otorgado para luego utilizarla como evidencia en el juicio jurídico. No existe diferencia entre el perito informático y los otros peritos ya que ambos deben reunir información acorde al tema del caso y a los requerimientos del magistrado.

Características

Para que un individuo pueda laborar a modo de perito informático se requiere cumplir con el perfil técnico adecuado donde es necesario conocer varias disciplinas y resolver los problemas generados con eficacia. Existen peritos especializados en hardware y otros en el software, ya que son dos escenarios totalmente distintos y requieren de conocimientos diferentes. Por lo cual es

indispensable e importante poder contar con estos profesionales y así poder lograr un exitoso proceso forense, logrando la compensación de los daños causados.

Es necesario que tenga la capacidad de analizar y presentar los acontecimientos necesarios para que el proceso forense efectuado tenga validez total frente al juzgado, para de esta manera favorecer a la víctima que busca sentenciar a la persona delictiva mediante gestiones legales. El perito recibe evidencias digitales para que emita un informe, realice determinadas acciones y sustente sobre la integridad de la misma.

Entorno de trabajo

El perito debe establecer un entorno de trabajo que le permita gestionar los casos en los que trabaja de forma ágil, rigurosa, fiable y segura. Ninguna técnica puede sustituir en ese sentido a la disciplina del propio perito a la hora de cumplir con aquellas restricciones y tareas necesarias para la debida gestión de los respectivos casos forenses.

Prueba Pericial

Es aquella que se genera del dictamen de un perito informático, el cual tiene la potestad de ser llamado por un juez e informar sobre los acontecimientos ocurridos, tomando en cuenta sus altos conocimientos en la informática forense, entre los aspectos más relevantes que conforma una prueba pericial tenemos:

1.- La Procedencia: Es importante contar con la información correspondiente al origen de las pruebas o evidencias encontradas para tener un enfoque correcto del caso a investigar.

2.- La Proposición: Comprende la o las evidencias digitales designadas a ser investigadas inclinando todo el proceso forense hacia aquellas pruebas, utilizando los múltiples procedimientos que se debe tener en cuenta para un ejecutar un Análisis Forense Digital.

3.- El Nombramiento: Todo perito debe ser llamado por el juez de la audiencia, con el objetivo de ser recusados por acontecimientos ocurridos antes o después de ser nombrado.

4.- El Diligenciamiento: Los defensores tienen el derecho de asistir al escenario donde el perito realizará el respectivo proceso forense, de igual manera están sujetos a escuchar sugerencias con el fin de despejar las posibles dudas generadas durante la prueba pericial.

5.- El Dictamen Pericial: Se puede definir como la documentación que presenta el perito informático en base al delito investigado, haciendo prevalecer las actividades llevadas a cabo durante el análisis forense, resaltando la hora y fecha exacta del suceso ocurrido en conjunto con las evidencias recolectadas. Es importante que la redacción resulte entendible para cualquier usuario sin utilizar términos técnicos que generen dudas al momento de la sustentación. Entre los términos que mantiene un dictamen pericial se encuentran los siguientes:

- Descripción de las evidencias involucradas en proceso forense, reseña del individuo, detalle del dispositivo a investigar.
- Detalle y resultados de todas las actividades realizadas en el Análisis Forense Digital.
- Hacer hincapié en las herramientas y/o metodologías utilizadas para la ejecución el respectivo dictamen pericial.
- Determinar las conclusiones del caso.

Fundamentación Social

Hasta la presente fecha en la provincia del Guayas ninguno de los centros de educación superior ha implementado un laboratorio digital forense que brinden servicios que permitan hallar actos ilícitos informáticos a la sociedad, entiéndase como manipulación de información, robo de información, intersección de datos, ataques de denegación de servicio (DoS), entre otros ataques.

El vigente proyecto será para orientar en la instalación de los programas forenses, uso adecuado de los aplicativos de software forense, incrementar la categoría académica a través del estudio de tal manera que catedráticos y alumnos contribuyan con los aprendizajes adquiridos de técnicas, procedimientos actuales considerando el proyecto como una gran referencia académica. Un Laboratorio de Informática Forense ayudará a buscar información para luego ser utilizada como evidencia mediante el estudio de los metadatos, tipos de archivos y las actividades realizadas por el computador; de esta manera poder determinar cuáles son incidentes.

Objetivos del Plan del Buen Vivir, Tomo I vigente en Ecuador desde 2013 hasta 2017

> **Objetivo 4. Fortalecer las capacidades y potencialidades de la ciudadanía.**
>
> 4.5. Potenciar el rol de docentes y otros profesionales de la educación como actores clave en la construcción del Buen Vivir
>
> 4.5 b. Fomentar la actualización continua de los conocimientos académicos de los docentes, así como fortalecer sus capacidades pedagógicas para el desarrollo integral del estudiante en el marco de una educación integral, inclusiva e intercultural. (Secretaría Nacional de Planificación y Desarrollo, s.f, p.47-p.49)
>
> **Objetivo 5. Construir espacios de encuentro común y fortalecer la identidad nacional, las identidades diversas, la plurinacionalidad y la interculturalidad**
>
> 5.2 Preservar, valorar, fomentar y resignificar las diversas memorias colectivas e individuales y democratizar su acceso y difusión
>
> 5.2b. Incentivar y difundir estudios y proyectos interdisciplinarios y transdisciplinarios sobre diversas culturas, identidades y patrimonios, con la finalidad de garantizar el legado a futuras generaciones. (Secretaría Nacional de Planificación y Desarrollo, s.f, p.52-p.53)

Objetivo 11. Asegurar la soberanía y eficiencia de los sectores estratégicos para la transformación industrial y tecnológica.

11.3. Democratizar la prestación de servicios públicos de telecomunicaciones y de tecnologías de información y comunicación (TIC), incluyendo radiodifusión, televisión y espectro radioeléctrico, y profundizar su uso y acceso universal.

11.3 n. Desarrollar redes y servicios de telecomunicaciones regionales para garantizar la soberanía y la seguridad en la gestión de la información. (Secretaría Nacional de Planificación y Desarrollo, s.f, p.68-p.69)

Fundamentación Legal

SECCIÓN TERCERA

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

Artículo 229.- **Revelación ilegal de base de datos. -** La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma

un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años. (Ministerio de Justicia, Derechos Humanos y Cultos, 2014, pp.93-95)

Idea a Defender

Mantener un sistema informático sin vulnerabilidades de seguridad es algo muy relativo ya que con los avances tecnológicos, explotarlas resulta menos complicado para el ciberdelincuente, de esta manera se entiende que un dispositivo informático hoy en día es el recurso más competente para cometer actos ilícitos, por ende, existen delitos que no se han logrado comprobar quién y cómo lo cometió, por lo cual el estudio de herramientas Open Source para la Implementación de un Laboratorio de Informática Forense tiene como principio

fundamental realizar el apropiado tratamiento de los datos, donde prevalecen las funcionalidades necesarias para la recolección de evidencia digital.

Es importante destacar que la idea a defender del presente proyecto está dada por la necesidad de la sociedad ecuatoriana tanto de los estudiantes, público en general y como las organizaciones de implementar un Laboratorio Forense en la Universidad de Guayaquil donde se utilicen herramientas de software que ayuden con el descubrimiento de información que pueda ser utilizada como evidencia en un caso judicial y no dejar impune el delito cometido.

Definiciones Conceptuales

Red: Podemos definir a una red, como un conjunto de equipos interconectados entre si bajo una estructura o medio de comunicación en común, donde se puede transmitir información y compartir recursos.

Wifi: Es una tecnología inalámbrica la cual no necesita de medios físicos para realizar una o varias conexiones hacia equipos portátiles, su comunicación se realiza mediante ondas electromagnéticas, la cual permite trasmitir internet a sus diferentes dispositivos, tablets, laptops, celulares, etc.

Sistema Operativo: Conjunto de programas que permite la interacción con el usuario al realizar una o varias tareas específicas, mediante la administración del hardware y sus diferentes aplicaciones.

Vulnerabilidad: se puede definir como debilidad o puntos bajos ante cualquier suceso, lo que puede ser aprovechado por terceras personas y causar daño al Sistema informático.

Certificado de Seguridad: es la encriptación de los datos entre el cliente y el servidor proporcionando seguridad en las diferentes transacciones, impidiendo que personas no esperadas puedan interceptar los datos.

Memoria Volátil: Es una memoria que mantiene la información mientras el computador este encendido, donde al apagarse y encenderse nuevamente, la memoria vuelve a tomar sus valores estándares sin guardar información.

Trivial: que es algo común.

Live CD: disco que contiene una imagen de sistema operativo, el cual permite la ejecución del mismo como si estuviera en una unidad física del equipo, contiene aplicaciones preinstaladas para agilitar las tareas de tal manera que no se vea la necesidad de instalar el sistema operativo.

Bootear: Modificar el orden de inicio de los dispositivos de un computador, se elige que unidad se prefiere que arranque como principal, uno de los ejemplos más cotidianos es cuando queremos instalar un sistema operativo donde escogemos como principal la unidad de cd, el cual tendrá un disco de instalación con su respectivo sistema operativo.

USB: Sus siglas significan Universal Serial Bus, son memorias de almacenamiento portátil capaz de guardar cualquier tipo de información y poder llevarla al lugar que se desee.

RAM: Random Access Memory, dicha memoria es utilizada por el computador en ella se guardan todos los procesos determinados por el microprocesador, para la ejecución de instrucciones las cuales puedes ser de lectura o escritura.

Cache: Es una memoria muy parecida a la principal la cual es utilizada por el microprocesador con fin de acceder a los datos de forma más rápida, acelerando de esta manera el procesamiento de los datos, pese a ser de menor tamaño esta solo guarda los datos temporalmente.

Jurista: Se determina jurista a una persona que está relacionada netamente con las leyes.

Inodo: Generalmente es utilizado en los sistemas Linux, donde representa la estructura de los datos con características como fecha, permisos y ubicación.

Control Parental: Permite la configuración de usuarios personalizados donde se ejecutan filtros para la navegación web, esto se utiliza principalmente cuando queremos que menores de edad no accedan hacia sitios indebidos.

Smartphone: Dispositivo táctil inteligente con la capacidad de ejecutar múltiples tareas, muy parecido a un pequeño computador.

PDA: También conocidos como asistentes personales digitales, al igual que un Smartphone se asemeja un computador con la mínima diferencia que estos cumplen una función más avanzada de una agenda electrónica.

LXDE: Es un entorno de escritorio que utiliza GNU/Linux en algunos de sus sistemas operativos como Debían, Fedora, Mint, entre otros, caracterizado por un bajo consumo de recursos y una simpática interfaz adaptada para el usuario final.

Logs: Son aquellos ficheros que registran las actividades realizadas en un determinado sistema operativo.

Recusado: Rechazar cualquier tipo de suceso que involucre procedimientos indebidos, donde se comprometida su imparcialidad.

Script: Conjunto de instrucciones procedentes de un lenguaje de programación definidas en un archivo determinado, para luego ser ejecutadas.

Ciberdelincuente: Es aquella persona que realiza actividades ilícitas con el apoyo de equipos de computación cuyo objetivo es robar información, acceder a sitios no autorizados, fraudes, y todo aquello que se encuentre comprometido con un delito informático.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

Diseño de la Investigación

Modalidad de la Investigación

El presente proyecto aplica la modalidad de investigación bibliográfica, la información fue obtenida de páginas web, artículos científicos y libros electrónicos al igual que propuestas similares al proyecto planteado. Por consiguiente, comprende un minucioso análisis durante la elección de los materiales a utilizar los mismos que deben estar bien documentados y ordenados para lograr un correcto proyecto investigativo.

Por otro lado, también consta de modalidad de campo, utilizada para realizar las diferentes demostraciones en entornos Microsoft Windows y Gnu/Linux sobre el uso de las herramientas software DEFT y DAWF en casos reales, actividad que será de vital ayuda en la implementación de Laboratorio de Informática Forense en la Carrera de Ingeniería en Networking y Telecomunicaciones, obteniendo de esta manera la experiencia necesaria para los futuros procesos forenses.

Tipos de Investigación

El tipo de investigación que se emplea en el presente proyecto de titulación es la investigación exploratoria, por la razón que, está orientada al estudio de un tema que no ha sido suficientemente tratado por los anteriores investigadores de la misma.

> De acuerdo con Kerlinger (1983) los estudios exploratorios buscan hechos sin el objetivo de predecir las relaciones existentes entre las variables. Se utilizan en situaciones en las que prácticamente no se dispone de información o el PON casi no se ha investigado. En este tipo de situaciones se inicia con un estudio exploratorio con el propósito de “preparar el

> terreno," (Dankhe, 1986), es decir, se desarrollan a fin de ir documentando el tema de investigación. (Perez, 2012, p.1)

Por otra parte, el actual proyecto consta de investigación descriptiva lo que comprende definiciones puntuales correspondientes a la informática forense, técnicas, procedimientos y herramientas que ayudan a la recolección de la evidencia digital. La investigación descriptiva en términos más precisos:

> Son el precedente de la investigación correlación y tienen como propósito la descripción de eventos, situaciones representativas de un fenómeno o unidad de análisis específica. Los censos económicos del Instituto Nacional de Estadística, Geografía e Informática (INEGI), los estudios por encuesta entre otros, son ejemplo de estudios descriptivos. (Perez, 2012, p.1)

Población y Muestra

Población

Se define a la población como el número global de personas que tienen en común habitar en un espacio o lugar determinado, lo cual permite el estudio de los mismos dando origen a la información de la investigación para luego ser recolectada y tabulada de acuerdo a los puntos relevantes del proyecto.

La población que participará en este estudio serán los estudiantes de la carrera de ingeniería en Networking y Telecomunicaciones de la Universidad de Guayaquil.

Muestra

Los investigadores conceptualizan muestra, a una cantidad específica de la población, la muestra de este estudio será los estudiantes que cursan el quinto semestre en adelante, se realizará el análisis para evaluar los distintos criterios obtenidos.

POBLACIÓN DE TESIS

CUADRO N° 3

INVOLUCRADOS	POBLACIÓN	PORCENTAJE
Estudiantes de la Carrera de Ingeniería en Networking y Telecomunicaciones.	1522	100%
Total	1522	100%

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris.

Fuente: Universidad de Guayaquil, Carrera de Ingeniería en Networking y Telecomunicaciones.

Tamaño de la Muestra

$$n = \frac{m}{e^2\,(m-1)+1}$$

m=tamaño de la población (1522)

E= error de estimación (6%)

n=Tamaño de la muestra (235)

$$n = \frac{1522}{0.06^2(1522-1)+1}$$

$$n = \frac{1522}{(0.0036)(1521)+1}$$

$$n = \frac{1522}{5.4756+1}$$

$$n = \frac{1522}{6.4756}$$

$$n = 235.03$$

$$n = 235$$

Instrumentos de Recolección de Datos

La Técnica

Para que una investigación resulte satisfactoria se necesita de técnicas que faciliten la integración de los datos, en cuanto a la estructura del proyecto, para lo cual es importante destacar los siguientes propósitos:

- Clasificar las fases de la investigación.
- Cooperar con herramientas para la administración de la información.
- Mantener una verificación de la información.
- Encaminar la adquisición de conocimientos.

La técnica aplicada en este proyecto es la de campo por lo tanto se efectuarán encuestas al alumnado de la Carrera de Ingeniería en Networking y Telecomunicaciones de la Universidad de Guayaquil; para saber si conocen o no sobre el uso de herramientas de software forense Digital.

Instrumentos De La Investigación

El presente proyecto está enfocado a la implementación de un laboratorio forense digital, el instrumento de la investigación a emplear serán los cuestionarios comandados por una encuesta la cual está diseñada para la obtención de datos reales acerca de los delitos informáticos tomando enfoque a los conocimientos sobre las herramientas software que se utilizan dentro de un análisis forense.

Podemos definir a la encuesta como un conjunto de preguntas específicas a realizar, lo que permitirá despejar las posibles dudas o inquietudes ante un tema relacionado, proporcionando las respuestas necesarias para comprobar la factibilidad de proyecto.

En cuanto a los cuestionarios, este presenta preguntas cerradas con una sola opción de respuesta, dicha encuesta se realizará a los estudiantes que forman parte de la universidad de Guayaquil carrera de ingeniería en Networking y telecomunicaciones, tomando en cuenta que en la actualidad los delitos

informáticos han incrementado de manera contundente lo cual no resultará desconocido para las personas que serán encuestadas.

Recolección de la Información

Las encuestas se realizaron a los estudiantes de la universidad de Guayaquil facultad de ciencias matemáticas y físicas de ambas carreras de ingeniería, se tomaron en cuenta estudiantes a partir de quinto semestre en adelante lo que generó respuestas favorables a nuestras preguntas planteadas con un grado de sinceridad muy elevado. Entre las actividades realizadas se detallan las siguientes:

1. Elaboración de los cuestionarios para la población elegida con el objetivo de obtener resultados estadísticos conforme a nuestra problemática.

2. Aprobación de la encuesta por parte de nuestro tutor guía, corroborando la correcta elaboración de las preguntas para un buen entendimiento hacia las personas a encuestar.

3. Ejecución de las encuestas a nuestra población escogida.

4. Tabulación de los datos obtenidos para realizar los respectivos análisis relevante nuestro estudio investigativo.

Procesamiento y Análisis

Una vez realizados los procedimientos correspondientes a la recolección de información se procede con la tabulación necesaria para evaluar los resultados obtenidos de las encuestas ejecutadas. En cuanto al análisis de los datos, esta se complementa con la ayuda de la herramienta Microsoft Excel, elaborando informes detallados en porcentaje y gráficos en forma de pastel, facilitando de esta manera la apreciación de los datos obtenidos.

1.- Considera usted ¿Qué cualquiera puede ser víctima de un delito informático?

ENCUESTA PARA ESTUDIO DE LA IMPLEMENTACIÓN DE UN LABORATORIO FORENSE DIGITAL – PREGUNTA N° 1

CUADRO N° 4

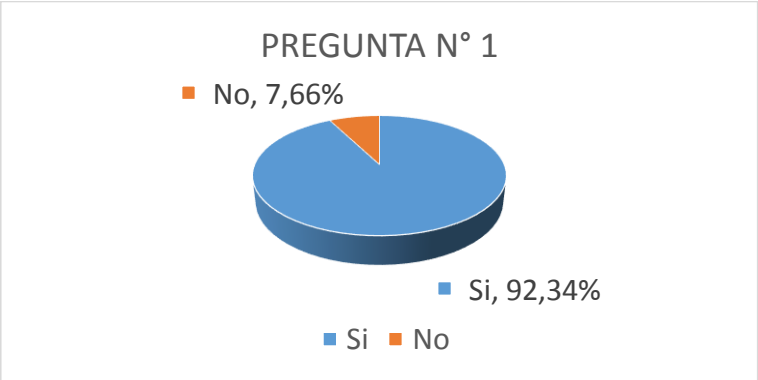
OPCIÓN	NUMERO DE RESPUESTAS POR MUESTRA	PORCENTAJE
Si	217	92.34%
No	18	7.66%
Total Muestra	235	100.00%

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

ESTADISCTICA DE LA ENCUESTA – PREGUNTA N° 1

GRÁFICO N° 1



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

Análisis: Del 100% de las encuestas tomadas (235) gran cantidad de alumnos (92.34%) afirman que cualquier persona puede ser víctima de un delito informático, mientras que el 7.66% indican lo contrario.

2.- ¿Conoce usted de alguna herramienta software que ayude a realizar el correcto análisis forense en un computador?

ENCUESTA PARA ESTUDIO DE LA IMPLEMENTACIÓN DE UN LABORATORIO FORENSE DIGITAL – PREGUNTA N° 2

CUADRO N° 5

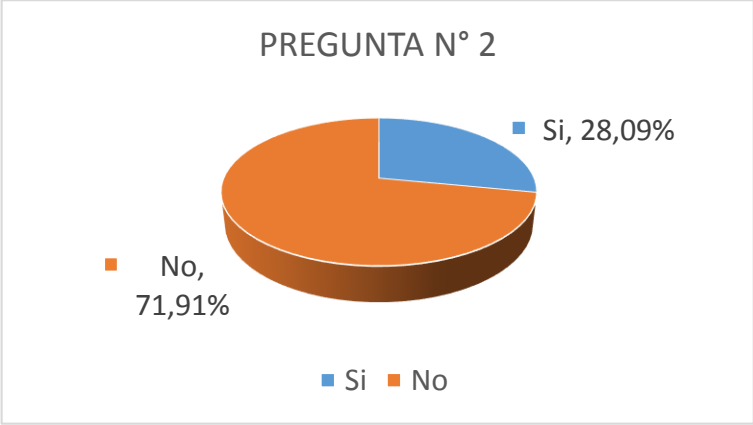
OPCIÓN	NUMERO DE RESPUESTAS POR MUESTRA	PORCENTAJE
Si	66	28.09%
No	169	71.91%
Total Muestra	235	100.00%

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

ESTADISCTICA DE LA ENCUESTA - PREGUNTA N° 2

GRÁFICO N° 2



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

Análisis: Dado el total de encuestas (235) en un 100% solo 28.09% (66) de alumnos indican conocer de herramientas software forense digital mientras que el otro 71.91% (169) afirman no saber de la existencia de dichas herramientas.

3.- ¿Cree usted que en la actualidad una herramienta software puede ayudar a descubrir responsables que han realizado algún tipo de acto ilícito utilizando equipos informáticos?

ENCUESTA PARA ESTUDIO DE LA IMPLEMENTACIÓN DE UN LABORATORIO FORENSE DIGITAL – PREGUNTA N° 3

CUADRO N° 6

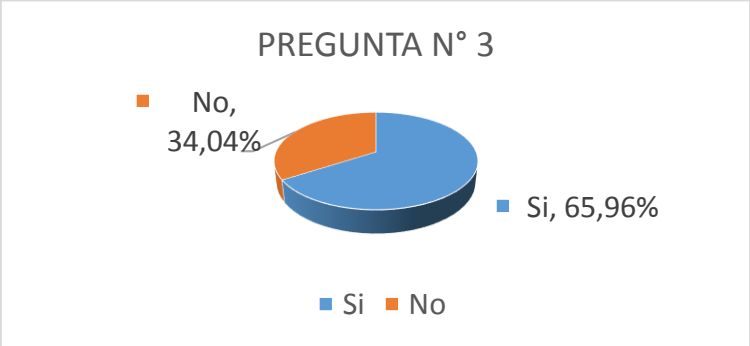
OPCIÓN	NUMERO DE RESPUESTAS POR MUESTRA	PORCENTAJE
Si	155	65.96%
No	80	34.04%
Total Muestra	235	100.00%

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

ESTADISCTICA DE LA ENCUESTA – PREGUNTA N° 3

GRÁFICO N° 3



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

Análisis: Del total de encuestas (235) en un equivalente al 100%, gran parte de los estudiantes (65.96%) asumen que un software puede ayudar en el proceso de análisis forense digital para encontrar involucrados de aquel acto ilícito y el 34.04% denotan lo contrario demostrando q la herramienta no ayudaría.

4.- ¿Cree usted que tanto el software como el hardware puede ser una evidencia digital dentro de un delito informático?

ENCUESTA PARA ESTUDIO DE LA IMPLEMENTACIÓN DE UN LABORATORIO FORENSE DIGITAL – PREGUNTA N° 4

CUADRO N° 7

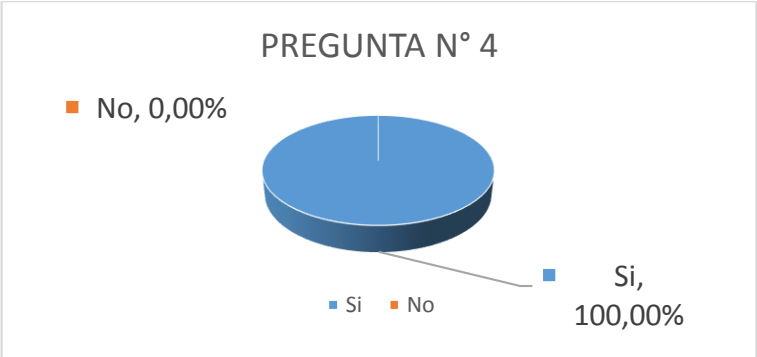
OPCIÓN	NUMERO DE RESPUESTAS POR MUESTRA	PORCENTAJE
Si	235	100.00%
No	0	0.00%
Total Muestra	235	100.00%

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

ESTADISCTICA DE LA ENCUESTA – PREGUNTA N° 4

GRÁFICO N° 4



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

Análisis: Tomado el 100% de encuestas (235), todos los alumnos indican que tanto el software como el hardware puede ser una evidencia digital.

5.- ¿Conoce usted que es un Laboratorio de Análisis Forense Digital?

ENCUESTA PARA ESTUDIO DE LA IMPLEMENTACIÓN DE UN LABORATORIO FORENSE DIGITAL – PREGUNTA N° 5

CUADRO N° 8

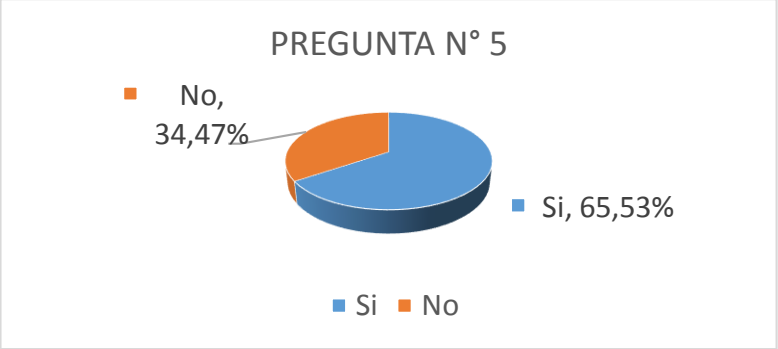
OPCIÓN	NUMERO DE RESPUESTAS POR MUESTRA	PORCENTAJE
Si	154	65.53%
No	81	34.47%
Total Muestra	235	100.00%

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

ESTADISCTICA DE LA ENCUESTA – PREGUNTA N° 5

GRÁFICO N° 5



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

Análisis: Tomada todas las encuestas (235) a pesar que gran número de estudiantes no conocían de una herramienta software forense digital en la pregunta #1, un porcentaje elevado (65.53%) conocían las funciones principales de un laboratorio de análisis forense digital, de igual manera existió un porcentaje (34.47%) que no tenían claro el objetivo del actual laboratorio a implementar.

6.- ¿Cree usted que la Carrera de Ingeniería en Networking y Telecomunicaciones debería tener un Laboratorio de Informática Forense?

ENCUESTA PARA ESTUDIO DE LA IMPLEMENTACIÓN DE UN LABORATORIO FORENSE DIGITAL – PREGUNTA N° 6

CUADRO N° 9

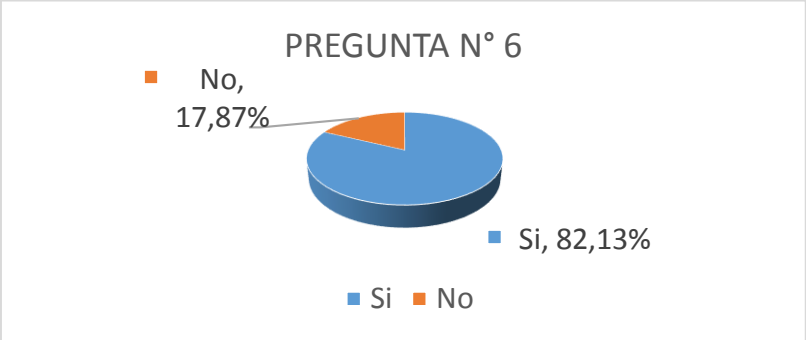
OPCIÓN	NUMERO DE RESPUESTAS POR MUESTRA	PORCENTAJE
Si	193	82.13%
No	42	17.87%
Total Muestra	235	100.00%

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

ESTADISCTICA DE LA ENCUESTA – PREGUNTA N° 6

GRÁFICO N° 6



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

Análisis: En la siguiente pregunta, pese a que un porcentaje de estudiantes (34.62%) no conocían la definición de un laboratorio forense digital en la pregunta #5 se procedió con dicha explicación lo que género que un 82.13% de alumnos afirmen que la carrera de ingeniería en Networking y telecomunicación debería tener un laboratorio de informática forense, aun así, hubo cierta población (17.87%) que no estaba de acuerdo con dicha implementación.

7.- ¿Cree usted que al contar con un Laboratorio de Informática Forense en la Carrera de Ingeniería en Networking y Telecomunicaciones ayudaría a la comunidad estudiantil en su formación profesional?

ENCUESTA PARA ESTUDIO DE LA IMPLEMENTACIÓN DE UN LABORATORIO FORENSE DIGITAL – PREGUNTA N° 7

CUADRO N° 10

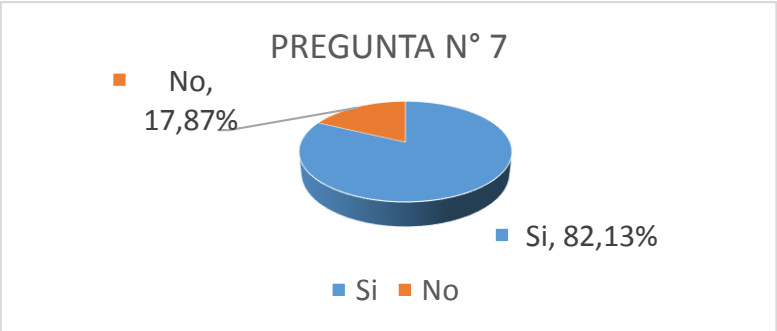
OPCIÓN	NUMERO DE RESPUESTAS POR MUESTRA	PORCENTAJE
Si	193	82.13%
No	42	17.87%
Total Muestra	235	100.00%

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

ESTADISCTICA DE LA ENCUESTA - PREGUNTA N° 7

GRÁFICO N° 7



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Encuesta

Análisis: Realizadas el total de encuestas (235), al igual que la pregunta anterior (#6) se pudo observar que la misma cantidad de encuestas (193) evaluadas en un 82.13 % están de acuerdo que la implementación de un laboratorio de informática forense ya que este ayudaría en la formación profesional de los estudiantes, a su vez personas con 17.87% no estaban de acuerdo.

Validación de la Idea a Defender

Una vez realizadas las encuestas a los estudiantes de la Carrera de Ingeniería en Networking y Telecomunicaciones, se obtuvo resultados favorables frente al actual proyecto investigativo, haciendo hincapié que cualquier persona puede ser víctima de un delito informático por ende consideran que la ayuda de herramientas de software forense y un personal capacitado como parte de un Laboratorio de Informática Forense Digital ayudaría de manera profesional a las personas que son víctimas de estos actos ilícitos, demostrando que herramientas especializadas software como DEFT y DAWF pueden brindar confiabilidad al momento de recoger la evidencia digital tomando en cuenta que aquel prueba puede ser física o lógica lo que implica cierto de grado de dificultad para el personal encargado en la recolección de los datos.

De acuerdo a los resultados obtenidos, los investigadores avalan el desarrollo del presente proyecto de titulación, pese a existir un sinnúmero de mecanismos utilizados en la violación de información esta guía presenta las herramientas software necesarias para realizar un análisis forense en los entornos de trabajos más utilizados: Microsoft Windows y GNU/Linux, lo que convierte a la actual guía en una documentación destacada para la implementación de un Laboratorio de Informática Forense Digital en la Carrera de Ingeniería en Networking y Telecomunicaciones.

CAPÍTULO IV

PROPUESTA TECNOLÓGICA

La informática forense en la actualidad es un campo muy poco explorado en Ecuador, pero en países vecinos como Colombia, esta siento utilizada de manera muy profesional debito a su funcionalidad principal que es descubrir sucesos ilícitos mediante procedimientos, técnicas, metodologías para obtener información íntegra la cual luego servirá de evidencia.

Por lo tanto se plantea el presente proyecto de titulación con el tema de **"Software Forense, Análisis del Uso de las Herramientas Software para la Implementación de un Laboratorio de Informática Forense en la Carrera de Ingeniería en Networking y Telecomunicaciones"**; el cual servirá de guía para realizar un correcto análisis forense digital mediante herramientas software como DEFT y DAWF, estas herramientas ofrecen varios tipos de soluciones que sirven de gran ayuda frente a un análisis forense digital lo que permite llevar una cadena de custodia siguiendo directrices determinadas, mediante informes detallados, como las actividades desarrolladas en un computador por ejemplo; instalación de un programa, utilización de un puerto USB, conexión a una red entre otros, con el fin de llevar la evidencia digital hacia un juicio penal.

Análisis de factibilidad

Es importante tener presente ciertos requisitos que involucra el estudio de las herramientas software para la Implementación de un Laboratorio Forense Digital, donde prevalece, el analizar las soluciones que presentan el software DEFT y DAWF en cuanto a un delito informático, no obstante en la actualidad se carece de centros especializados para ese tipo de actividades ilícitas que requieren de personal capacitado con conocimientos sólidos en informática forense; pese a existir dichas necesidades, estudiantes de la Carrera de Ingeniería en Networking y Telecomunicaciones plantean un estudio con la implementación de un laboratorio especializado en delitos informáticos donde según las encuestas ejecutadas a estudiantes de la misma carrera, afirman que un laboratorio forense

dentro de la carrera podría ayudar a su formación estudiantil y profesional, tomando en cuenta los escenarios de varios delitos efectuados a la población actual, los cuales siguen incrementando de manera indeterminada.

Para la investigación acorde a la Implementación de un Laboratorio Forense Digital en la Carrera de Ingeniería en Networking y Telecomunicaciones se realizaron las siguientes actividades:

- Estudio de campo relevante a los múltiples delitos informáticos.
- Levantamiento de Información correspondiente a software especializado para el Análisis Forense Digital.
- Selección de la herramienta software apropiada para elaborar el respectivo proceso forense.

Factibilidad Operacional

Es importante destacar que el presente estudio servirá como guía para que los usuarios encargados del análisis forense de un computador estén capacitados; manteniendo la integridad de los datos, encontrando hallazgos realizados por el o los ataques, obteniendo evidencia digital; y para que no cometan errores en la utilización de cada una de las herramientas, de esta manera se asegura brindar el mejor servicio de laboratorio de análisis forense digital para quien lo requiera.

Factibilidad Técnica

El actual proyecto consta de Factibilidad Técnica, ya que favorece al uso herramientas software Open Source (DEFT y DAWF) demostrando que no se necesita de un hardware con recursos potentes para realizar un correcto análisis donde se encuentran vinculados dispositivos informáticos; cabe recalcar que estos software se los puede instalar como también se los puede utilizar de forma LiveCD, además una de las ventajas es, que son parte de la familia Open Source que

gracias a las condiciones de su licencia estas se las puede encontrar de manera gratuita.

Generalmente las soluciones de código abierto presentan múltiples actualizaciones, brindando por ese medio las mejoras correspondientes a las brechas encontradas por los usuarios, o al contrario demostrando que los creadores de los software se encuentran a la par con los avances tecnológicos incluyendo nuevas características que se acoplan perfectamente al comportamiento de los recientes equipos, de esta manera es beneficioso contar con software forenses que se muestran actualizados constantemente.

Factibilidad Legal

El presente proyecto se realiza tomando en consideración el ciclo de vida que tiene un análisis forense digital, donde las actividades a realizar no influyen en ningún reglamento que impida la ejecución de dicho proceso. Por consiguiente, el analizar evidencias para fines legales y poder culminar con un delito informático de manera exitosa presentando responsables no genera infracciones ni violaciones contra la confidencialidad, disponibilidad e integridad de la información.

Factibilidad Económica

Los investigadores realizaron una analogía de software Open Source a utilizar, y como su nombre lo indica, las herramientas planteadas no tienen un valor monetario definido, por ser herramientas de código abierto; por lo cual se optó con dicha solución para la futura implementación del Laboratorio Forense Digital, los cuales cuentan con utilitarios extras que cumplen con los requerimientos necesarios para realizar un adecuado análisis de la información, permitiendo economizar el uso de las soluciones forenses en la Implementación del Laboratorio para la Carrera de Ingeniería en Networking y Telecomunicaciones de la Universidad de Guayaquil.

Etapas de la metodología del proyecto

Scrum es una metodología ágil que felicita el trabajo en equipo, considerando aspectos importantes dentro de un grupo de personas, muestra constante seguimiento a las actividades establecidas para cada integrante, permitiendo de esa manera avanzar notablemente con el proyecto investigativo. Entre las partes que intervienen en la metodología Scrum para el actual estudio tenemos:

Dueño de Producto: Carrera de Ingeniería en Networking y Telecomunicaciones de la Universidad de Guayaquil.
Scrum Master: Ing. Jorge Arturo Chicala Arroyave, M.Sc.

Equipo de trabajo Scrum: Mite Villón Jimmy, Sánchez Montero Yuris.

Para la elaboración de la metodología Scrum se definen los siguientes componentes los cuales van ligados al proyecto investigativo a realizar, cumpliendo de esta manera con los procedimientos adecuados para el análisis de herramientas software en un Laboratorio Forense Digital.

- Product backlog
- Sprint

Product backlog

Presenta una lista de actividades deseadas, relevante al proyecto investigativo donde se toman en cuenta los requerimientos junto con las prioridades que se asocian al proyecto, el cual puede mostrar modificaciones con forme avanza el proyecto.

Sprint

Muestra las acciones que se realizarán dentro de un ciclo de trabajo determinado, permitiendo detallar las actividades a ejecutar durante el tiempo establecido.

SPRINT O HILOS DE LA METODOLOGÍA SCRUM

CUADRO N° 4

N°	SPRINT O HILOS
1	Búsqueda de sistemas operativos forense
2	Comparación sistemas operativos forense
3	Elección del sistema operativo forense
4	Instalación del sistema operativo forense
5	Búsqueda de herramientas de software forense para la copia de información
6	Comparación y selección de la herramienta de software forense para la copia de información
7	Investigación de suites de herramientas para el análisis forense digital
8	Selección de la suite de análisis forense digital
9	Búsqueda de herramienta para el análisis hexadecimal de archivos.
10	Elección e instalación de la herramienta de análisis hexadecimal.

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Investigación

DESCRIPCIÓN DE LOS SPRINT DE LA METODOLOGÍA SCRUM

CUADRO N° 5

N°	HILOS	DESCRIPCIÓN	A CARGO DE:
SPRINT 1	Búsqueda de sistemas operativos forense	Se realizaron los hilos para obtener el mejor sistema operativo forense acorde a las necesidades.	Sánchez Montero Yuris, Mite Villón Jimmy
	Comparación sistemas operativos forense		
	Elección del sistema operativo forense		
	Instalación del sistema operativo forense		
SPRINT 2	Búsqueda de herramientas de software forense para la copia de información.	Se procedió a la instalación de la herramienta Guymager para las copias bit a bit de información.	Sánchez Montero Yuris, Mite Villón Jimmy
	Comparación y selección de la herramienta de software forense para la copia de información		
SPRINT 3	Investigación de suites de herramientas para el análisis forense digital	Utilización de la suite Autopsy para la creación del caso y análisis de la información.	Sánchez Montero Yuris, Mite Villón Jimmy
	Selección de la suite de análisis forense digital		
SPRINT 4	Búsqueda de herramienta para el análisis hexadecimal de archivos.	Se ejecutó la instalación de la herramienta GHex permitiendo el análisis hexadecimal de archivos.	Sánchez Montero Yuris, Mite Villón Jimmy
	Elección e instalación de la herramienta de análisis hexadecimal		

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Investigación

Entregables del Proyecto

Entre los entregables que avalan el presente proyecto de estudio se encuentran los siguientes:

- El desarrollo de todos los capítulos propuestos en la guía de elaboración brindada por la Universidad de Guayaquil; cumpliendo detalladamente con cada uno de los ítems, los mismos que servirán de soporte como resultado del proyecto investigativo realizado.
- Manual de instalación y operación de las herramientas software forense DEFT y DAWF con el fin de un adecuado uso para a los diferentes casos de delitos informáticos que se llevarán a cabo en el Laboratorio de informática Forense Digital.

Criterios de validación de la propuesta

Para la validación de la propuesta se procedió con una entrevista no dirigida hacia el Ing. Jorge Chicala Arroyave, M.Sc. docente de la Universidad de Guayaquil Carrera de Ingeniería en Networking y Telecomunicaciones, el cual está relacionado con el tema del presente proyecto donde prevalece la seguridad informática y sus derivados; el objetivo de esta entrevista es obtener juicios de expertos. Entre las preguntas realizadas se generó la siguiente respuesta por parte del docente:

Es muy importante para el desarrollo de la universidad y los estudiantes debido al gran enfoque con la seguridad informática, donde actualmente cierto porcentaje de la población no demuestra interés de resolución después de ser afectado por un delito informático, cuando la acción correcta es analizar y ver las posibles soluciones con respecto al problema que origino esa novedad. Por consiguiente, es indispensable contar con el software adecuado para la recolección de información, comprometiendo la integridad de los datos y la confidencialidad de los usuarios ante un proceso de Análisis Forense Digital.

Criterios de aceptación del Producto o Servicio

El análisis y uso de las herramientas software para la implementación de un Laboratorio de informática Forense en la carrera de Ingeniería en Networking y Telecomunicaciones, comprende una total aceptación de acuerdo a los siguientes argumentos:

- Tiene como propósito servir como base guía para la incorporación de soluciones software forense en la implementación de un Laboratorio de informática Forense Digital.
- Fines profesionales y académicos, beneficiando a la sociedad en general en cuanto a su prestación de servicios y a los estudiantes de la Carreta de ingeniería en Networking y Telecomunicaciones por su gran aporte estudiantil.
- No implica valor monetario ya que los aplicativos a utilizar son Open Source y se los puede obtener mediante la página del fabricante en la sección de descargas.
- Tanto DEFT como DAWF trabajan en entornos Microsoft Windows y GNU/Linux, siendo los sistemas operativos más utilizados para servidores empresariales y clientes finales, imprimiendo una acción favorable para el uso de las herramientas software si se presenta algún delito informático.
- Pruebas de concepto aceptables; cumpliendo con los objetivos y el alcance antes mencionado, satisfaciendo de esa manera con las necesidades que se requieren para desarrollar un análisis forense digital, recalcando su eficiencia a nivel de resultados, corroborando lo eficaz que son las herramientas software al momento de un delito informático.

Conclusiones y Recomendaciones

Conclusiones

Luego de realizar los respectivos análisis se presentan las siguientes conclusiones:

- DEFT como Software Forense presenta múltiples soluciones para la recolección de evidencia digital, pese a ser Open Source es completo donde su nivel de desempeño y respuesta son aceptables en comparación a otros Software Forenses, lo que permite que un Laboratorio Forense Digital sea eficiente al momento de presentar resultados.

- En la actualidad gran parte de los usuarios cuentan con sistema operativo Microsoft Windows instalado en su computador, ya sea este, portátil o de sobremesa; DAWF es una herramienta sencilla que presenta resultados positivos frente a un Análisis Forense Digital, mostrando las actividades ocurridas en un entorno Windows. De esta manera complementa los resultados obtenidos en cuanto a una recolección de evidencia digital, lo cual es esencial para la construcción de un Laboratorio especializado en Ciencias Forenses.

- Es importante destacar que las herramientas Open Source DEFT y DAWF, cumplen un papel fundamental en la implementación de un Laboratorio Digital, debido a los lineamientos que presentan al momento de ejecutar un Análisis Forense determinado, manteniendo la integridad de los datos durante todo el proceso forense, ya sea este en entorno Windows o GNU/Linux.

Recomendaciones

En cuanto a las recomendaciones establecidas para el actual proyecto investigativo tenemos:

- Realizar una revisión minuciosa de las múltiples soluciones que comprende el Software Forense DEFT, tomando en cuenta los tipos de evidencias digitales a analizar cómo pueden ser; discos duros, memorias, unidades USB, registros, etc., debido a que no todo software viene equipado de igual manera.

- Tener en presente el escenario al momento de ejecutar el respectivo Análisis Forense como lo es en “modo vivo” o “modo muerto”, donde se ve involucrada la evidencia digital ya que no comprende el mismo proceso cuando el equipo se encuentra encendido o apagado.

- Tener una capacitación continua de las herramientas software que forman parte del Laboratorio Forense Digital (DEFT, DAWF), debido a las múltiples actualizaciones que se presentan ya que pueden generar mejoras a nivel de rendimiento y desempeño, para de esta manera promover la implementación de futuros laboratorios forenses utilizando soluciones Open Source, no solo en la Universidad de Guayaquil sino en las diferentes localidades donde prevalecen los delitos informáticos.

BIBLIOGRAFÍA

Acurio Del Pino, S. (07 de Julio de 2009). *Manual de Manejo de Evidencias Digitales y Entornos Informáticos*. Obtenido de Organization of American States: https://www.oas.org/juridico/english/cyb_pan_manual.pdf

Anguas Balsera, J. (11 de Noviembre de 2011). *Peritaje en Informática.* Obtenido de INFORMÁTICA LEGAL: http://www.anguas.com/e1m6/Docs/01_Documentacion_Adicional_Curso_Peritaje_CPEIG.pdf

Bassini, A. E. (02 de Junio de 2013). *El Perito Informatico y La Prueba Pericial*. Obtenido de Derecho Penal Online: http://www.derechopenalonline.com/derecho.php?id=14,812,0,0,1,0

Bove, A. (16 de Junio de 2014). *Distribuciones con Herramientas para Análisis Forense*. Obtenido de El Hacker: http://blog.elhacker.net/2014/06/distribuciones-linux-herramientas-analisis-forense-digital-informatico.html

Caballero Quezada, A. E. (11 de Agosto de 2016). *Instalación De CAINE 7.0*. Obtenido de ReYDes: http://www.reydes.com/d/?q=Instalacion_de_CAINE_7

Calderón Valdiviezo, R. G., Guzmán Reyes, G. S., & Salinas González, J. M. (29 de 06 de 2011). *Diseño y Plan de Implementación de un Laboratorio de Ciencias Forenses Digitales.* Recuperado el 24 de 05 de 2016, de REPOSITORIO DE ESPOL: https://www.dspace.espol.edu.ec/bitstream/123456789/19927/3/Tesina%20Laboratorio%20Forense%20Digital.pdf

Carrion, H. D. (01 de Agosto de 2001). *Presupuestos para la Punibilidad del Hacking.* Obtenido de SEGURIDAD DE LA INFORMACION: http://delitosinformaticos.com/trabajos/hacking.pdf

Chiluiza Rodríguez, E. (10 de Enero de 2015). *LOS DELITOS INFORMÁTICOS EN EL COIP*. Obtenido de LA VERDAD: http://www.revista-laverdad.com/2015/01/10/los-delitos-informaticos-en-el-coip/

Delgado Granados, M. d. (28 de Octubre de 2003). *DELITOS INFORMÁTICOS DELITOS ELECTRÓNICOS*. Obtenido de Orden Jurídico Nacional: http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf

El Telegrafo. (16 de Agosto de 2016). *En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario*. Obtenido de El Telegrafo: http://www.eltelegrafo.com.ec/noticias/judicial/13/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

El Universo. (17 de Noviembre de 2014). *Delitos informáticos en la web podrían aumentar en Ecuador*. Obtenido de El Universo: http://www.eluniverso.com/noticias/2014/11/17/nota/4226966/ataques-web-podrian-aumentar

Ferrer Piera, M. (s.f. de s.f. de s.f.). *LOS 11 PASOS PARA IMPLEMENTAR METODOLOGÍA SCRUM*. Obtenido de MANAGEMENT PLAZA: http://managementplaza.es/blog/los-11-pasos-para-implementar-metodologia-scrum/

Fiscalía General del Estado. (13 de Junio de 2015). *Los delitos informáticos van desde el fraude hasta el espionaje*. Obtenido de Fiscalía General del Estado: http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

Guasch, J. (23 de Noviembre de 2013). *DEFT, DISTRIBUCIÓN LINUX PARA ANÁLISIS FORENSE*. Obtenido de Security By Default : http://www.securitybydefault.com/2013/11/deft-distribucion-linux-para-analisis.html

Guidance Software. (s.f.). *EnCase Enterprise*. Obtenido de GUIDANCE SOFTWARE: https://www2.guidancesoftware.com/Lang/Pages/es/EnCase-Enterprise.aspx

Hall, A. (s.f.). *Tipos de delitos informáticos*. Obtenido de Foro de Seguridad: http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

Legislación y Delitos Informáticos - Tipos de Delitos Informáticos. (s.f.). Obtenido de SEGURIDAD DE LA INFORMACION: http://www.segu-info.com.ar/delitos/tiposdelito.htm

Londoño, M. M. (s.f). *Historia*. Obtenido de ADALID: http://www.adalid.com/quienes-somos/historia/

López Delgado, M. (14 de Junio de 2007). *Analisis Forense Digital.* Obtenido de http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

MaTTica. (s.f.). *Laboratorio FORENSE*. Obtenido de MaTTica: http://mattica.com/laboratorio-forense/

Mesa Losada. (10 de Mayo de 2015). *KIT DE HERRAMIENTAS PARA INFORMÁTICA FORENSE*. Obtenido de HERRAMIENTAS PARA EL ANÁLISIS FORENSE: https://informaticaforenseunad.wordpress.com/

Metro Ecuador. (23 de Noviembre de 2015). *Fiscalía registra 1 026 denuncias por delitos informáticos en Ecuador*. Obtenido de Metro Ecuador: http://www.metroecuador.com.ec/noticias/fiscalia-registra-1-026-denuncias-por-delitos-informaticos-en-ecuador/rUrokw---SvYDq0dbtKlVM/

Ondata Internacional. (s.f.). *ENCASE FORENSIC SOFTWARE: CARACTERÍSTICAS Y FUNCIONES*. Obtenido de Ondata Internacional: http://www.ondata.es/recuperar/encase_forensic.htm

Ortega Sandoval, C. C. (17 de Octubre de 2012). *Informática Forense*. Obtenido de Prezi: https://prezi.com/-fev5qqvbvv8/informatica-forense/

Perez Garcia, L. (06 de Noviembre de 2012). *Estudios exploratorios descritivos, correcionales, explicativos*. Obtenido de Prezi: https://prezi.com/l6zhhvtr9eq3/estudios-exploratorios-descritivos-correcionales-explicativos/

Pimentel, E. (21 de Julio de 2013). *DEFT Linux*. Obtenido de Gustavo Pimentel's GNU/Linux Blog: http://gustavo.pimentel.eu/category/distribuciones-linux/deft-linux/

Policia Nacional del Ecuador. (02 de Septiembre de 2015). *Delitos Informáticos o Ciberdelitos*. Obtenido de Policia Nacional del Ecuador: http://www.policiaecuador.gob.ec/delitos-informaticos-o-ciberdelitos/

Restrepo, J. A. (28 de 10 de 2012). *DEFT (Digital Evidence & Forensic Toolkit)*. Obtenido de DragonJAR: http://www.dragonjar.org/deft-digital-evidence-forensic-toolkit.xhtml

Restrepo, J. A. (21 de 10 de 2014). *Los Foros de la Comunidad DragonJAR*. Obtenido de DragonJAR: http://comunidad.dragonjar.org/f157/llamado-beta-testers-nuevo-proyecto-dragonjar-dawf-15651/

Restrepo, J. A. (22 de Abril de 2016). *DAWF (DragonJAR Automatic Windows Forensic)*. Obtenido de DragonJAR: http://www.dragonjar.org/dawf-dragonjar-automatic-windows-forensic.xhtml

Rivas López, J. (08 de Julio de 2009). *Análisis forense de sistemas informáticos.* Obtenido de SEGURIDAD TELEMÁTICA : http://jlrivas.webs.uvigo.es/downloads/publicaciones/Analisis%20forense%20de%20sistemas%20informaticos.pdf

Romero Meza, H. (14 de Julio de 2015). *Población, Muestra y Muestreo*. Obtenido de METODOLÓGIA DE LA INVESTIGACIÓN: http://metodouba.blogspot.com/2015/07/poblacion-muestra-y-muestreo.html

Santillán, N. (12 de Mayo de 2014). *Técnicas de Investigación*. Obtenido de Prezi: https://prezi.com/9merilaz1brc/tecnicas-de-investigacion/

Secretaría Nacional de Planificación y Desarrollo. (s.f). *Responsabilidades del Plan Nacional para el Buen Vivir 2013-2017*. Obtenido de Buen Vivir: http://www.buenvivir.gob.ec/herramientas

Stefano, F. (10 de 08 de 2014). *DEFT 8.2 listo para descargar*. Obtenido de Deft: http://www.deftlinux.net/2014/08/10/deft-8-2-ready-for-download/

TANNHAUSSER. (18 de Enero de 2014). *DEFT Linux: una derivada de Lubuntu para la auditoría informática*. Obtenido de LA MIRADA DEL REPLICANTE:

http://lamiradadelreplicante.com/2014/06/18/deft-linux-una-derivada-de-lubuntu-para-la-auditoria-informatica

Trabajo de Investigación MANEJO DE LA EVIDENCIA DIGITAL EN EL DERECHO INFORMATICO Y APICACIONES DE SOFTWARE. (15 de Diciembre de 2008). Obtenido de Universidad Católica de Cuenca Repositorio Institucional: http://dspace.ucacue.edu.ec/bitstream/reducacue/4012/4/Trabajo%20Investigaci%C3%B3n%20MANEJO%20DE%20LA%20EVIDENCIA%20DIGITAL%20EN%20EL%20DERECHO%20INFORMATICO%20Y%20APICACIONES%20DE%20SOFTWARE.pdf

Zuccardi, G., & Gutiérrez, J. (Noviembre de 2006). *Informática Forense*. Obtenido de http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

ANEXOS

ANEXO N° 1: SOLICITUD PARA TOTAL DE ESTUDIANTES DE LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

UNIVERSIDAD DE GUAYAQUIL

ESPECIE UNIVERSITARIA– NIVEL PREGRADO

Guayaquil, 11 de Agosto del 2016

Rosa Procidel

Ing.
HARRY LUNA AVEIGA
Director de la Carrera de Ingeniería
EN NETWORKING Y TELECOMUNICACIONES

2681

En su despacho.-

De mis consideraciones:

Yo, BORYS ANDRÉS LÓPEZ MAXI con CI N° 093051111-8, estudiante de la carrera de **INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES** solicito a usted se me conceda el número de estudiantes actual desde primer hasta octavo semestre, dichos datos para aportación en mi tema de tesis ANALISIS, DISEÑO, ESPECIFICACIONES TECNICAS Y SEGURIDAD PARA LA IMPLEMENTACIÁN DE UN LABORATORIO DE INFORMÁTICA FORENSE PARA LA CARRERA DE INGENIERIA EN NETWORKING Y TELECOMUNICACIONES :

Por la atención favorable que dé al presente, quedo muy agradecido de usted.

Atentamente

Atendiendo la solicitud del Estudiante López Maxi Borys Andrés en lo que respecta a la cantidad de estudiantes matriculados de primero a octavo semestre en el periodo 2016 ciclo I, según reporte del Sistema JasperSoft existen 1522 estudiantes matriculados.

Carrera de Ingeniería en Networking y Telecomunicaciones.

Atendido: 18/08/2016 Rosa Cedeño

Recibido por:

BORYS ANDRÉS LÓPEZ MAXI
093051111-8
EMAIL: borys.lopezm@ug.edu.ec
CELULAR: 0981755621

11 AGO 2016
2432

UNIVERSIDAD DE GUAYAQUIL
TESORERIA

ANEXO N° 2: CRONOGRAMA DE ACTIVIDADES SCRUM

	UNIVERSIDAD DE GUAYAQUIL	**CRONOGRAMA DEL PROYECTO**
	FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS	
	CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES	
Nombre del proyecto:		SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES.
Nombre del tutor:		ING. JORGE ARTURO CHICALA ARROYAVE, M.Sc.
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	Búsqueda de sistemas operativos forense	25/05/16																				
2	Comparación sistemas operativos forense	15/06/16																				
3	Elección del sistema operativo forense	20/06/16																				
4	Instalación del sistema operativo forense	27/06/16																				
5	Búsqueda de herramientas de software forense para la copia de información	05/08/16																				
6	Comparación y selección de la herramienta de software forense para la copia de información	11/08/16																				
7	Investigación de suites de herramientas para el análisis forense digital	22/08/16																				
8	Selección de la suite de análisis forense digital	16/09/16																				
9	Búsqueda de herramienta para el análisis hexadecimal de archivos	22/09/16																				
10	Elección e instalación de la herramienta de análisis hexadecimal	26/09/16																				

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Datos de la Investigación

ANEXO N° 3: ENCUESTA PARA ESTUDIANTES DE LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

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

1.- Considera usted ¿Qué cualquiera puede ser víctima de un delito informático?

○ Si ○ No

2.- ¿Conoce usted de alguna herramienta software que ayude a realizar el correcto análisis forense en un computador?

○ Si ○ No

3- ¿Cree usted que en la actualidad una herramienta software puede ayudar a descubrir responsables que han realizado algún tipo de acto ilícito utilizando equipos informáticos?

○ Si ○ No

4.- ¿Cree usted que tanto el software como el hardware puede ser una evidencia digital dentro de un delito informático?

○ Si ○ No

5.- ¿Conoce usted que es un Laboratorio de Análisis Forense Digital?

○ Si ○ No

6.- ¿Cree usted que la Carrera de Ingeniería en Networking y Telecomunicaciones debería tener un Laboratorio de Informática Forense?

○ Si ○ No

7.- ¿Cree usted que al contar con un Laboratorio de Informática Forense en la Carrera de Ingeniería en Networking y Telecomunicaciones ayudaría a la comunidad estudiantil en su formación profesional?

○ Si ○ No

UNIVERSIDAD DE GUAYAQUIL

FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS

CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES

"SOFTWARE FORENSE, ANÁLISIS DEL USO DE LAS HERRAMIENTAS SOFTWARE PARA LA IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES"

MANUAL DE USUARIO

PROYECTO DE TITULACIÓN

Previa a la obtención del Título de:

INGENIERO EN NETWORKING Y TELECOMUNICACIONES

AUTOR (ES):

MITE VILLÓN JIMMY ROLANDO

SÁNCHEZ MONTERO YURIS RAFAEL

TUTOR: ING. JORGE CHICALA ARROYAVE, M.Sc.

GUAYAQUIL – ECUADOR

2016

ÍNDICE GENERAL

MANUAL DE USUARIO DE DEFT LINUX

Instalación de Deft Linux 8

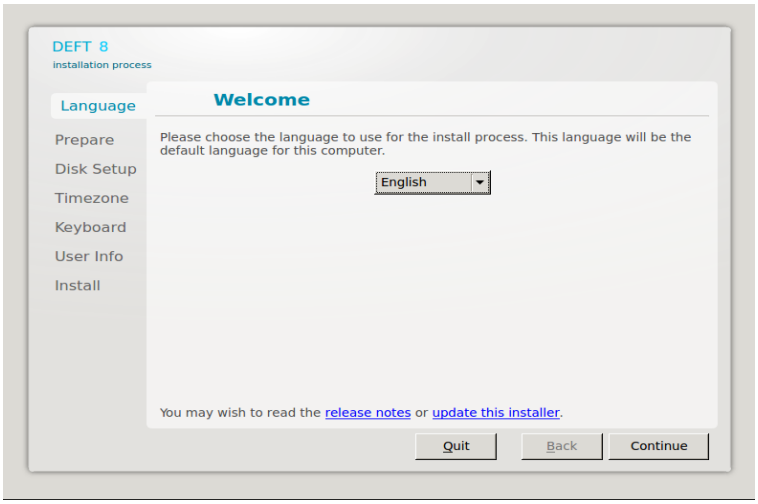
Para comenzar se debe escoger el idioma con el que vaya a trabajar en este caso English y luego seleccionar la opción Install DEFT Linux 8.

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Elección de Idioma

Pregunta en que idioma va a instalar el software, donde se escogerá English y clic en Continúe.

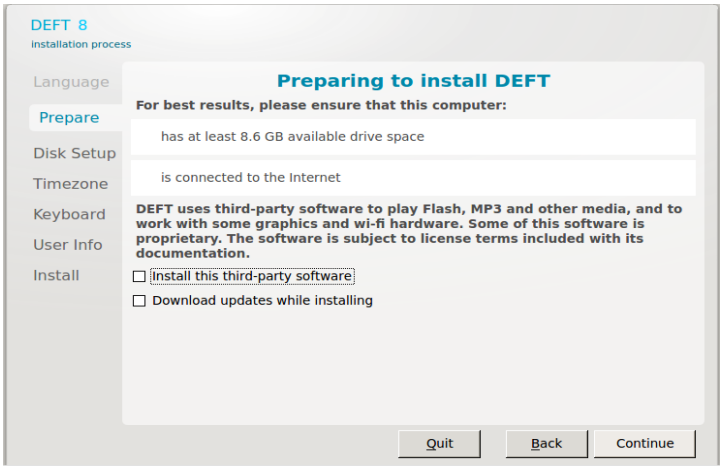


Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Preparación para la instalación de DEFT

En esta ventana de preparación indica que debe tener al menos 8.6 GB de espacio disponible en la partición o total del disco duro para seguir con la instalación, clic en Continue.

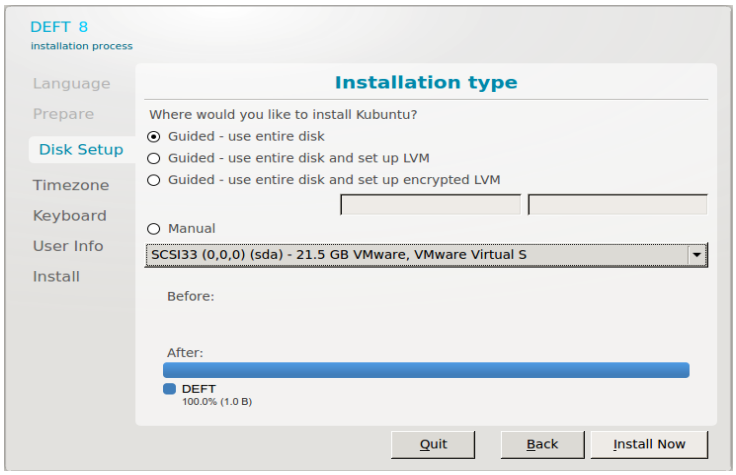


Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Tipo de instalación en el disco duro

Escoger la primera opción porque necesita usar todo el disco, también da la opción Manual en la cual puede realizar particiones; continua pulsando en Install Now.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Selección de la zona horaria

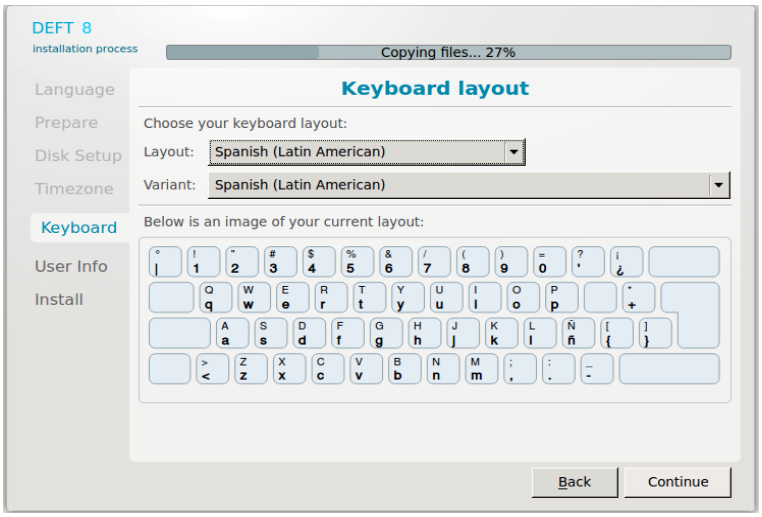
Escoger la zona Horaria y clic en continue.

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Verificación de diseño del teclado

El software automáticamente identifica el diseño de su teclado, comprueba que sea el correcto y pulsar sobre continue.

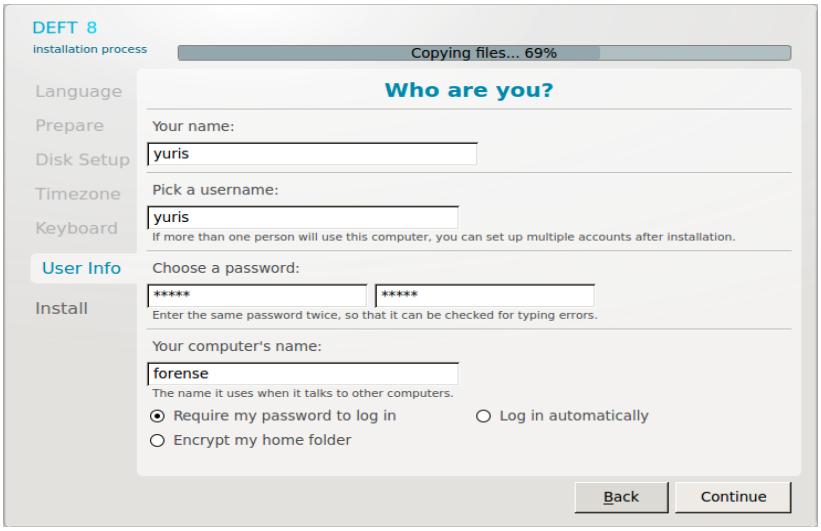


Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Configuración del usuario

Ingrese información para definir el nombre del computador, contraseña, nombre de usuario; mientras que los archivos de instalación se copian en segundo plano, clic en continúe.

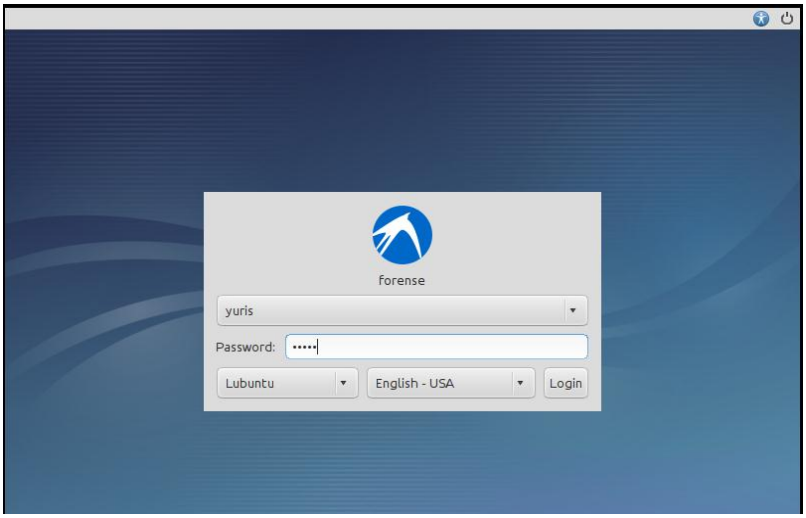


Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Ingreso con usuario creado

Espere a que termine la instalación, reinicie y a continuación el sistema operativo DEFT está listo para ser utilizado como lo muestra la imagen.

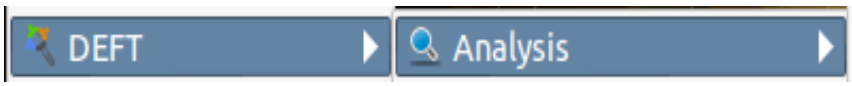


Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Analysis

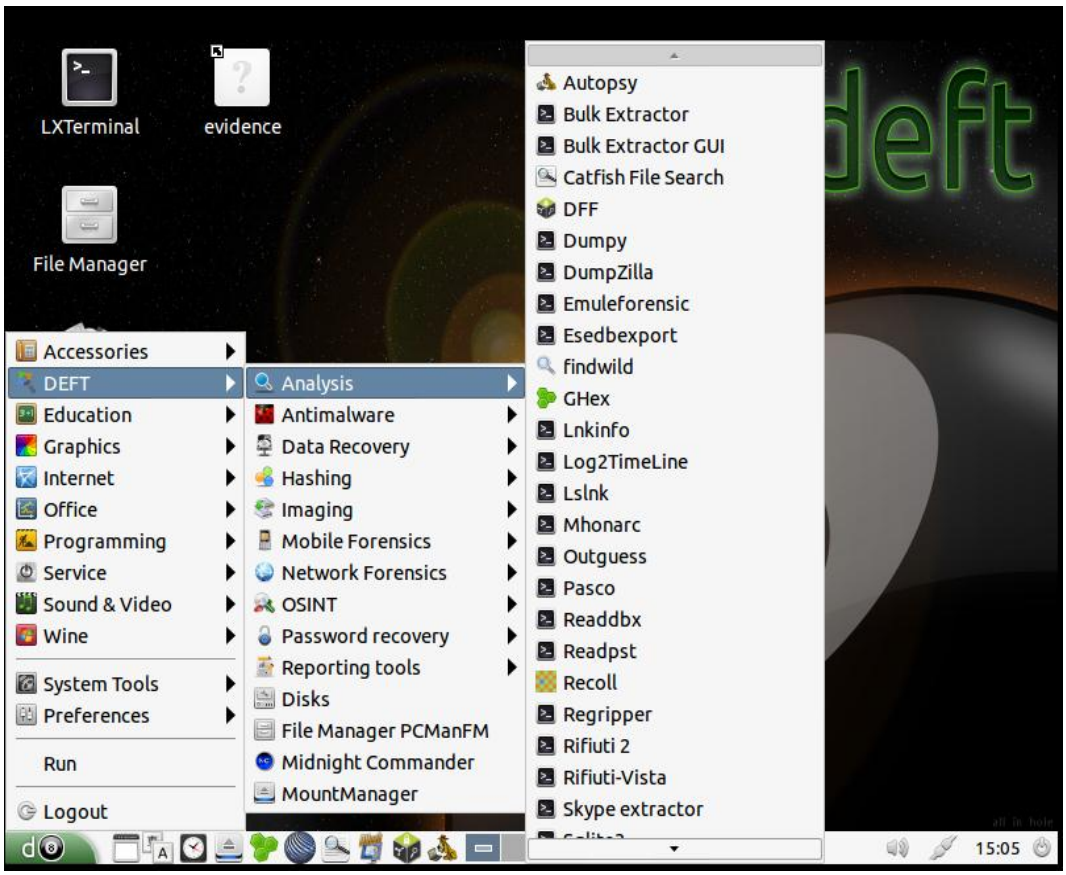
Para finalizar debe ubicar las herramientas forenses que contiene el software DEFT, ubicándose en la lista de menú DEFT y luego Analysis como lo muestra la siguiente imagen.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Colección de herramientas



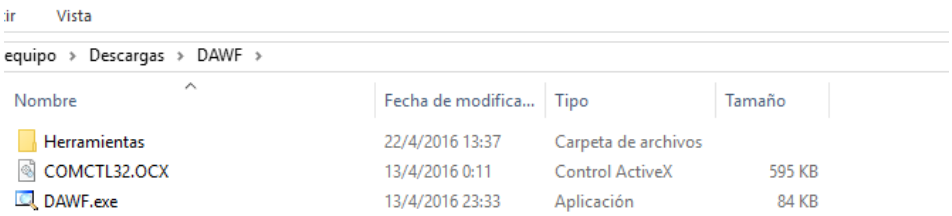
Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

MANUAL DE USUARIO DEL SOFTWARE DAWF

Descarga del software DAWF

El investigador descarga el programa del siguiente link https://mega.nz/#!Ho52SZwI!-5unLPQ0Ifx3jvG7nXyG3aBBdKWX3q_SZJbMM-ukbFA y a continuación descomprime el archivo, observa el ejecutable de DAWF.

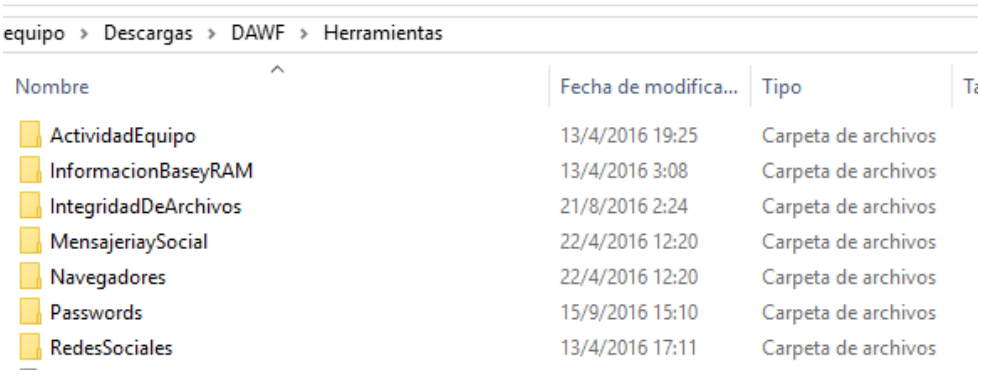


Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Colección de herramientas

Abre la carpeta Herramientas y se puede observar que existen otras carpetas las cuales sus nombres hacen referencia al propósito de las herramientas que contienen.

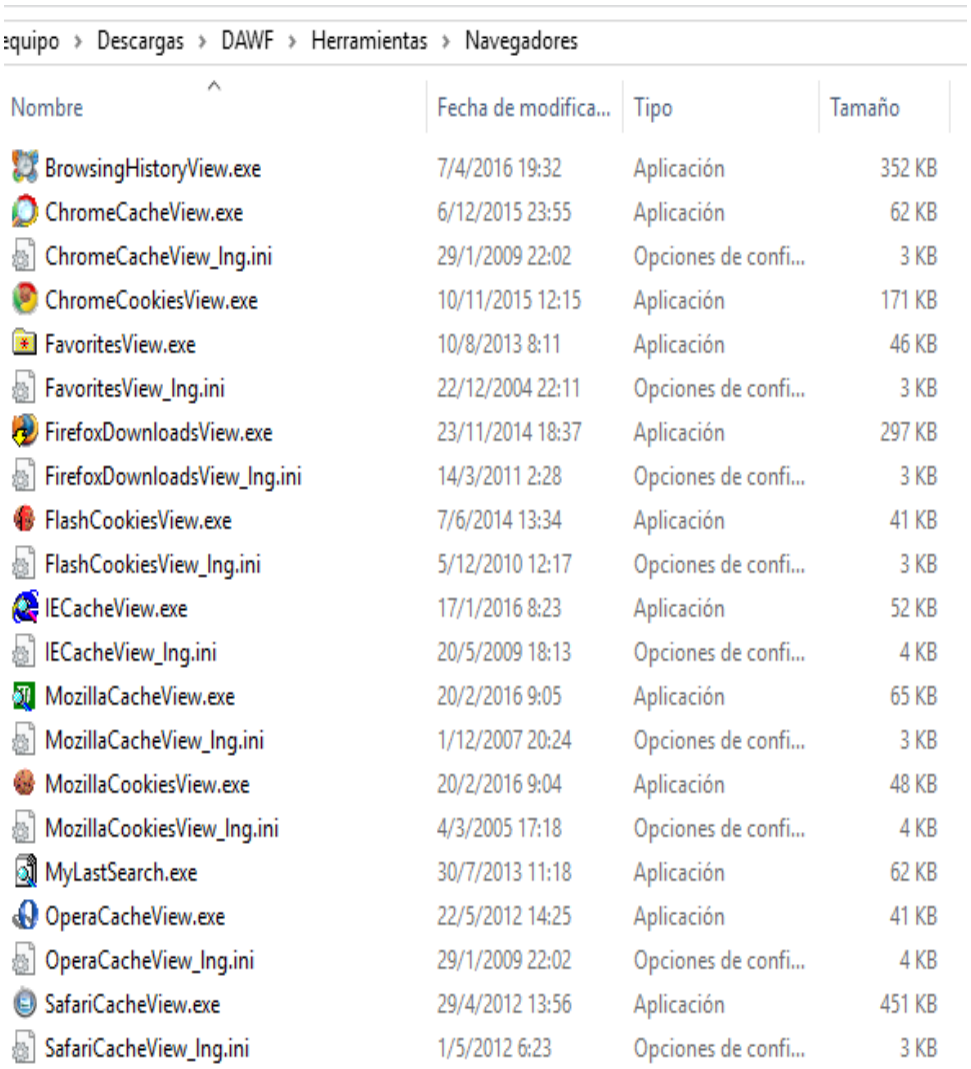


Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Herramientas para análisis de navegadores

Abre la carpeta Navegadores, visualiza que contiene herramientas para recabar información sobre las cookies, historiales, Cache de los navegadores instalados en el computador.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Ejecución del software DAWF

Una vez revisado todas las carpetas por el investigador sobre el contenido de las herramientas que tiene alojadas DAWF procede a ejecutar DAWF.exe en modo

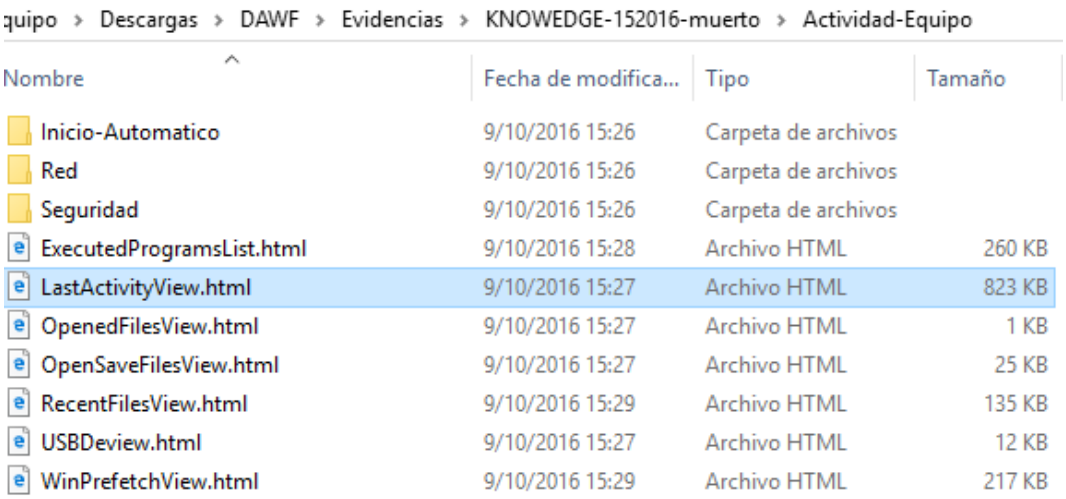
administrador, en este caso lo ejecuta sin marcar la pestaña inferior esto quiere decir en modo muerto lo cual ya ha sido tratado en el capítulo II.

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Recolección de evidencias

Se dirige a la ruta donde se creó la carpeta evidencias, abre la carpeta Actividad-Equipo y ve que se ha generado mucha evidencia en este caso solo abre el archivo LastActivityView.html.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Visualización de la información del archivo LastActivityView.html

El investigador abre archivo LastActivityView.html y muestra información como su nombre lo indica, las últimas actividades del computador**.**

Acciones de usuario y Lista de Eventos

Creado con LastActivityView

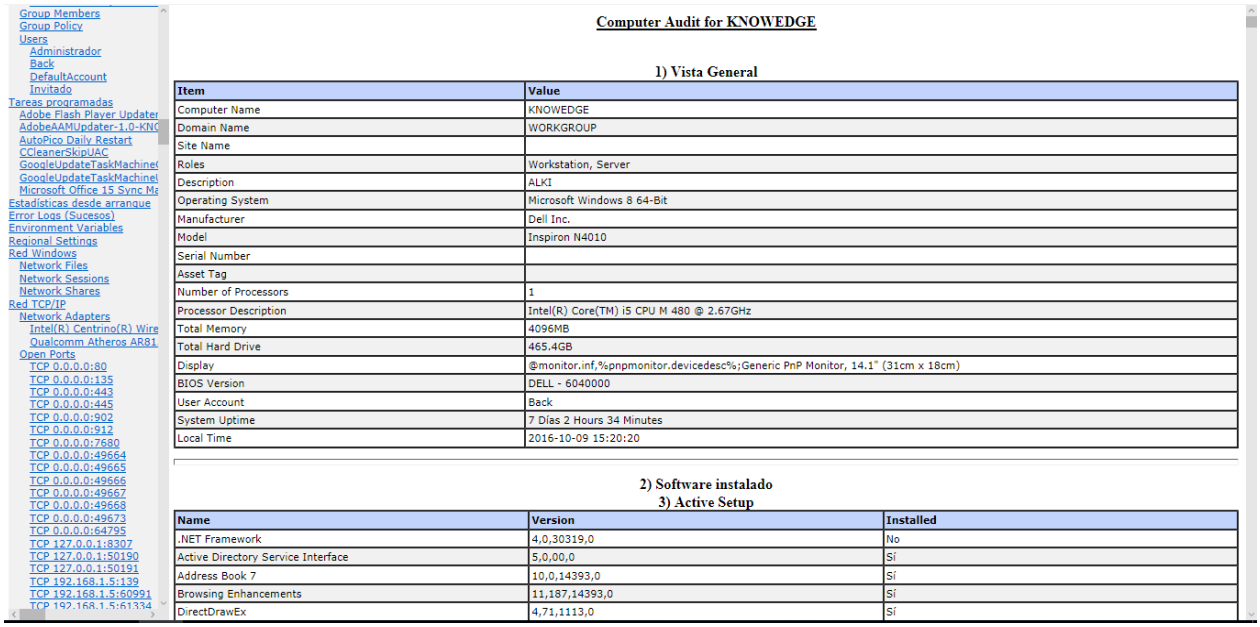
Hora de Acción	Descripción	Nombre de archivo	Directorio
9/10/2016 15:26:59	Ejecutar archivo .EXE	USBDEVIEW.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\ACTIVIDADEQUIPO\USBDEVIEW.EXE
9/10/2016 15:26:44	Ejecutar archivo .EXE	MYEVENTVIEWER.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\ACTIVIDADEQUIPO\MYEVENTVIEWER.EXE
9/10/2016 15:26:40	Ejecutar archivo .EXE	WINLOGONVIEW.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\ACTIVIDADEQUIPO\WINLOGONVIEW.EXE
9/10/2016 15:26:36	Ejecutar archivo .EXE	TURNEDONTIMESVIEW.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\ACTIVIDADEQUIPO\TURNEDONTIMESVIEW.EXE
9/10/2016 15:26:33	Ejecutar archivo .EXE	SECURITYSOFTVIEW.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\ACTIVIDADEQUIPO\SECURITYSOFTVIEW.EXE
9/10/2016 15:26:28	Ejecutar archivo .EXE	WHATINSTARTUP.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\ACTIVIDADEQUIPO\WHATINSTARTUP.EXE
9/10/2016 15:26:18	Ejecutar archivo .EXE	TASKSCHEDULERVIEW.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\ACTIVIDADEQUIPO\TASKSCHEDULERVIEW.EXE
9/10/2016 15:26:16	Abrir archivo o carpeta	CURSO DE TITULACION	D:\DISCO LOCAL\UNIVERSIDAD\CURSO DE TITULACION
9/10/2016 15:26:16	Abrir archivo o carpeta	manual de instalacion.docx	D:\DISCO LOCAL\UNIVERSIDAD\CURSO DE TITULACION\manual de instalacion.docx
9/10/2016 15:26:14	Ejecutar archivo .EXE	NETWORKOPENEDFILES.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\ACTIVIDADEQUIPO\NETWORKOPENEDFILES.EXE
9/10/2016 15:26:10	Ejecutar archivo .EXE	BLUETOOTHVIEW.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\ACTIVIDADEQUIPO\BLUETOOTHVIEW.EXE
9/10/2016 15:26:06	Ejecutar archivo .EXE	WIFIHISTORYVIEW.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\ACTIVIDADEQUIPO\WIFIHISTORYVIEW.EXE
9/10/2016 15:26:00	Ejecutar archivo .EXE	CURRPORTS.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\ACTIVIDADEQUIPO\CURRPORTS.EXE
9/10/2016 15:25:53	Ejecutar archivo .EXE	VNCPASSVIEW.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\PASSWORDS\VNCPASSVIEW.EXE
9/10/2016 15:25:44	Ejecutar archivo .EXE	SKYPELOGVIEW.EXE	C:\Users\Back\DOWNLOADS\DAWF\HERRAMIENTAS\MENSAJERIAYSOCIAL\SKYPELOGVIEW.EXE

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Visualización de la información de la herramienta WinAudit

Continua con el análisis en la carpeta InformacionBase-Sistema abre el fichero generado por la herramienta WinAudit llamado KNOWEDGE.html el cual muestra información sobre el modelo del computador, software instalados, entre otros.



Elaborado: Sánchez Montero Yuris, Mite Villón Jimmy

Fuente: Pruebas en el computador

Visualización del archivo de la herramienta BrowsingHistoryView

Ahora el investigador se ubica la carpeta Informacion-Navegadores y solo abre el fichero que ha sido creado por la herramienta BrowsingHistoryView, observa que le indica la fecha y hora, nombre de usuario y en que navegador se ha realizado una determinada búsqueda.

Browsing History Items

Created by using BrowsingHistoryView

	Title	Visit Time	Visit Count	Web Browser	User Profile	Browser Profile	URL Length	Typed Count
about:		30/9/2016 16:53:08	1	Internet Explorer 10/11 / Edge	Back		6	
about:blank		9/10/2016 14:09:01	21	Internet Explorer 10/11 / Edge	Back		11	
about:blank		30/9/2016 23:22:49	300	Internet Explorer 10/11 / Edge	Back		11	
file:///C:/Users/Back/AppData/Local/Temp/18T00478.pdf	18T00478 - 18T00478.pdf	4/10/2016 14:16:09	1	Firefox	Back	ekn0vr4n.default	53	
file:///C:/Users/Back/Desktop/14542798_1392174624129444_1277898885_n.jpg		4/10/2016 15:46:37	3	Internet Explorer 10/11 / Edge	Back		72	
file:///C:/Users/Back/Desktop/14542798_1392174624129444_1277898885_n.rar		4/10/2016 3:18:27	1	Internet Explorer 10/11 / Edge	Back		72	
file:///C:/Users/Back/Desktop/a.docx		2/10/2016 18:06:27	7	Internet Explorer 10/11 / Edge	Back		36	
file:///C:/Users/Back/Desktop/a.odt		2/10/2016 18:06:22	6	Internet Explorer 10/11 / Edge	Back		35	
file:///C:/Users/Back/Desktop/autofinal.jpg		2/10/2016 22:40:01	1	Internet Explorer 10/11 / Edge	Back		43	
file:///C:/Users/Back/Desktop/autofinal.zip		2/10/2016 22:40:31	1	Internet Explorer 10/11 / Edge	Back		43	
file:///C:/Users/Back/Desktop/Captu1.JPG		3/10/2016 0:13:01	1	Internet Explorer 10/11 / Edge	Back		40	
file:///C:/Users/Back/Desktop/Captu3.JPG		2/10/2016 17:10:16	1	Internet Explorer 10/11 / Edge	Back		40	
file:///C:/Users/Back/Desktop/Captura.JPG		4/10/2016 13:58:43	3	Internet Explorer 10/11 / Edge	Back		41	
file:///C:/Users/Back/Desktop/Captura.JPG.bak		3/10/2016 0:26:36	1	Internet Explorer 10/11 / Edge	Back		45	
file:///C:/Users/Back/Desktop/casoprac.docx		30/9/2016 23:24:17	1	Internet Explorer 10/11 / Edge	Back		43	
file:///C:/Users/Back/Desktop/dine.JPG		3/10/2016 0:25:42	1	Internet Explorer 10/11 / Edge	Back		38	
file:///C:/Users/Back/Desktop/Diseno%20de%20redes.vsdx		3/10/2016 23:24:22	1	Internet Explorer 10/11 / Edge	Back		54	
file:///C:/Users/Back/Desktop/Doc3.docx		4/10/2016 14:28:41	1	Internet Explorer 10/11 / Edge	Back		39	
file:///C:/Users/Back/Desktop/forencis.txt		30/9/2016 14:39:06	6	Internet Explorer 10/11 / Edge	Back		42	
file:///C:/Users/Back/Desktop/GUIA%20DE%20ELABORACION%20DE%20PROYECTO%20DE%20TITULACION.pdf	GUIA DE ELABORACION DE PROYECTO DE TITULACION.pdf	7/10/2016 17:50:02	1	Firefox	Back	ekn0vr4n.default	91	
file:///C:/Users/Back/Desktop/GUIA%20DE%20ELABORACION%20DE%20PROYECTO%20DE%20TITULACION.pdf		7/10/2016 17:50:01	1	Internet Explorer 10/11 / Edge	Back		91	

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Visualización de acciones realizadas en SKype

Regresa a la carpeta KNOWEDGE-152016-muerto, selecciona la carpeta Mensajeria-y-Social y da clic sobre el archivo nombrado igual a la herramienta que lo creó SkypeLogView; muestra información de las acciones realizadas en Skype.

Cuenta de Skype

Criado utilizando SkypeLogView

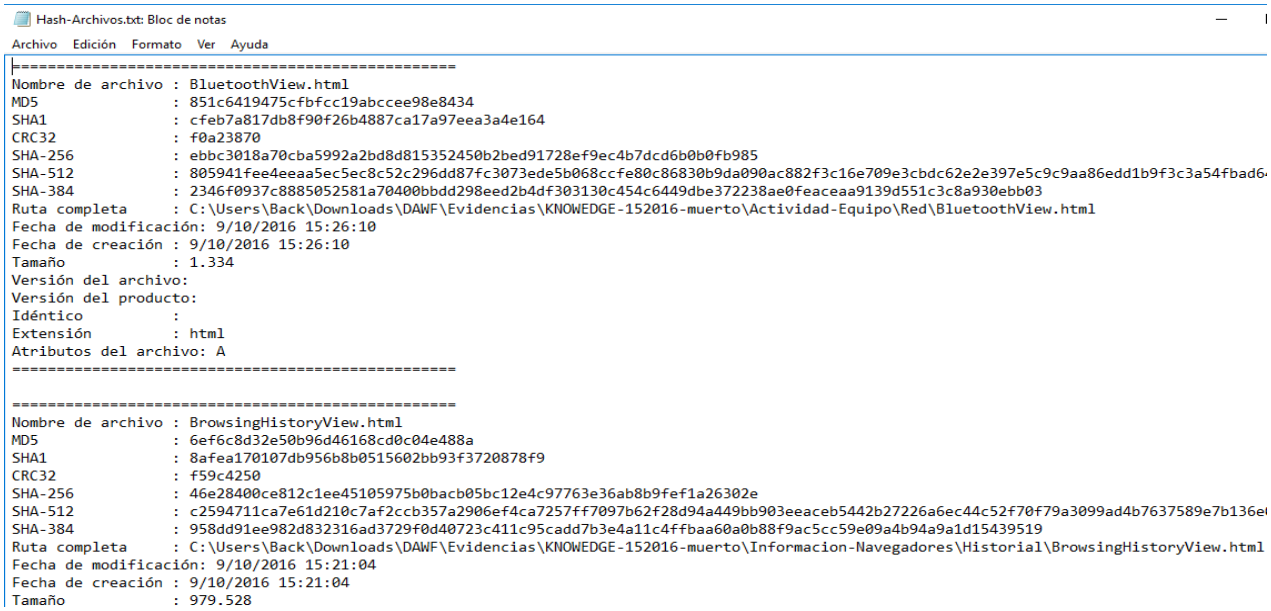
Número de registro	Tipo de acción	Día y hora	End Time	Usuario	Nombre mostrado	Duración	Mensaje	Identificación del chat	Nombre del archivo
1020	Llamada recibida			james.bastr	Jimmy M				
1022	Llamada recibida			alex.mendez08	Alexander Méndez				
1029	Llamada recibida			james.bastr	Jimmy M				
1033	Llamada recibida			alex.mendez08	Alexander Méndez				
1247	Llamada recibida			james.bastr	Jimmy M				
1252	Llamada recibida			james.bastr	Jimmy M				
1716	Llamada recibida			james.bastr	Jimmy M				
2328	Chat	29/8/2016 23:38:25		live:yuris-sata					
2372	Chat	14/9/2016 23:09:48		alex.mendez08 live:yuris-sata					
2547	Chat	29/9/2016 14:40:20		james.bastr live:yuris-sata					
2555	Chat	30/9/2016 14:44:38		james.bastr live:yuris-sata					
2571	Chat	4/10/2016 21:28:03		james.bastr live:yuris-sata					

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Visualización del archivo de Hash-Archivos

Para finalizar con el análisis el investigador abre el fichero Hash-Archivos y observa que la herramienta calculó hash para cada uno de los archivos generados al momento de ejecutar DAWF con el objetivo de mantener la integridad de los mismos.



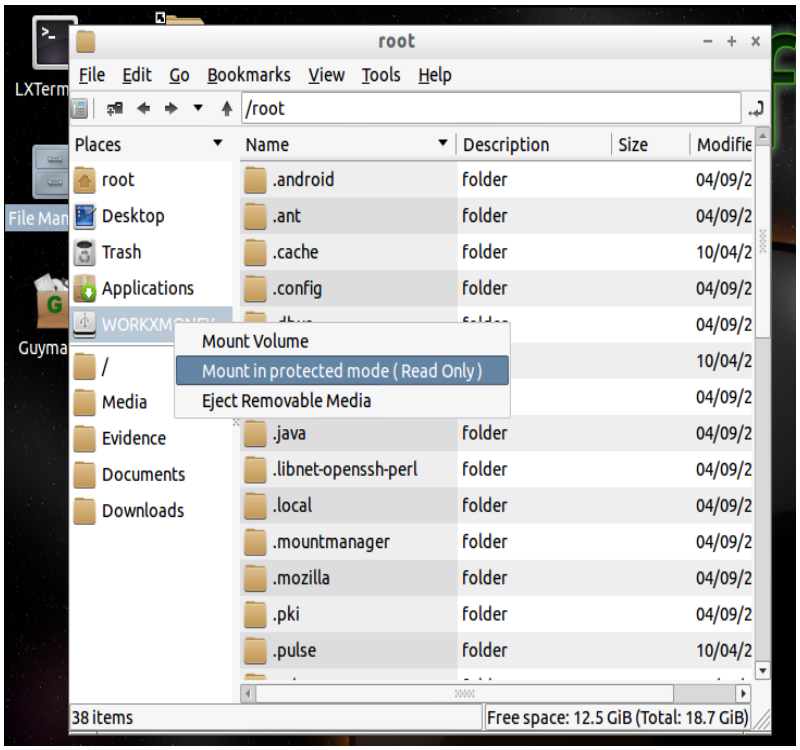
Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

MANUAL DE USUARIO DE ANÁLISIS FORENSE DIGITAL DE UN CASO DE ESTUDIO

Montaje del Dispositivo que será analizado

El investigador conecta el dispositivo en este caso utiliza un pendrive y lo monta en modo protegido (solo lectura), para que no sufra ningún cambio su información y pueda adquirir una imagen íntegra.

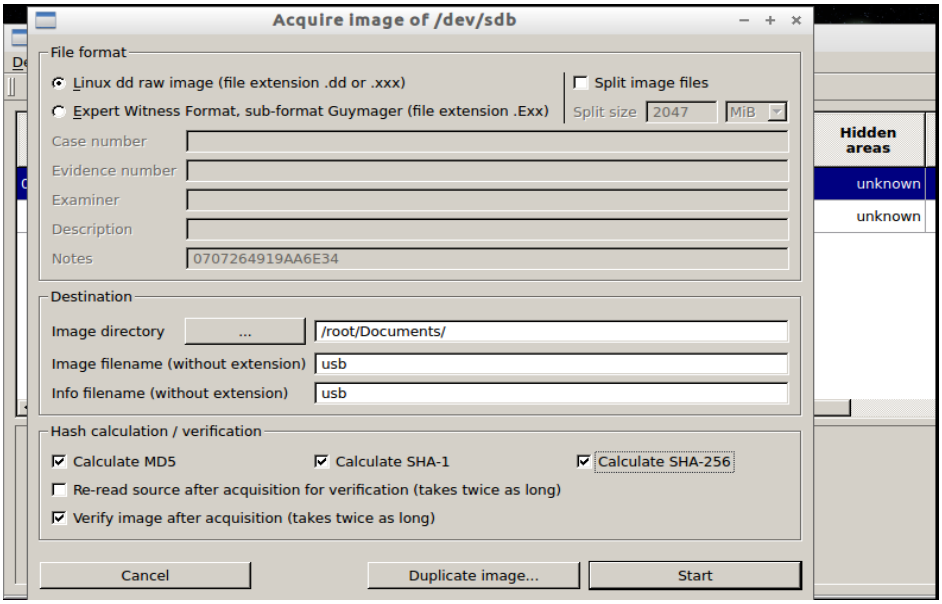


Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Clonación del Dispositivo que será analizado

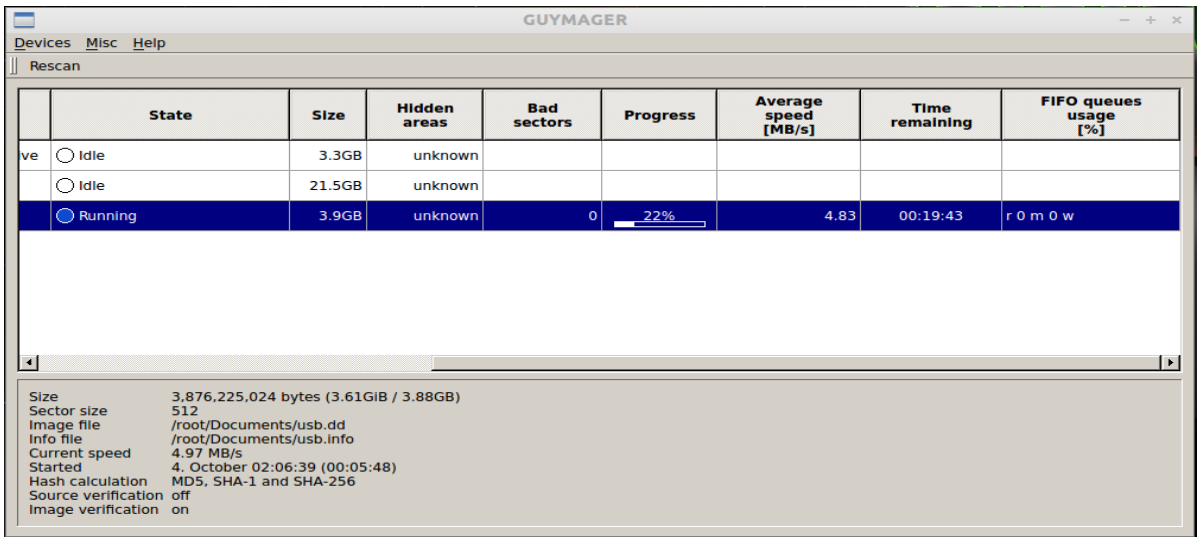
A continuación el investigador abre el programa GUYMAGER que permite realizar una copia bit a bit del dispositivo, da clic derecho sobre el dispositivo y escoge Acquire image luego deja ciertos parámetros como lo muestra la imagen, cambia como necesite que se llame la imagen del dispositivo y el directorio donde va hacer alojado.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

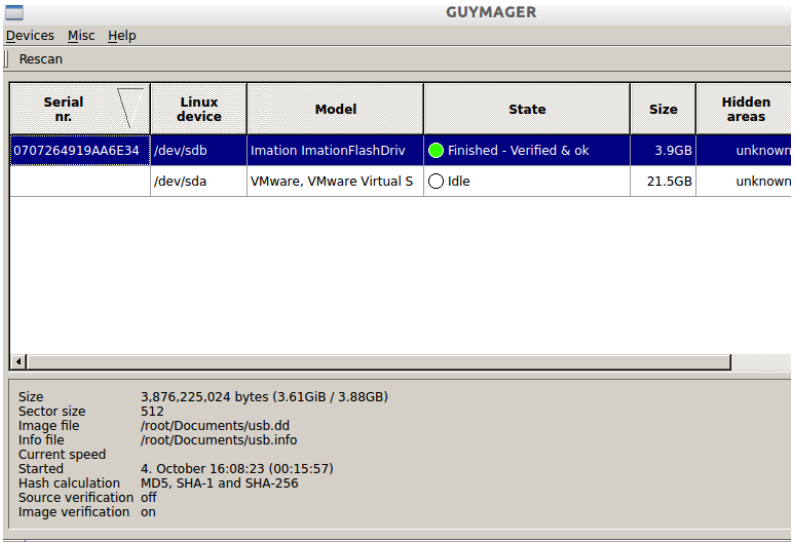
Espera a que termine de realizar la copia, en la parte inferior puede apreciar información muy importante como donde se guarda,el tamaño, el cálculo de los Hash de la imagen llamada usb.dd



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

El punto verde confirma que termino con éxito la creación de la imagen del dispositivo.

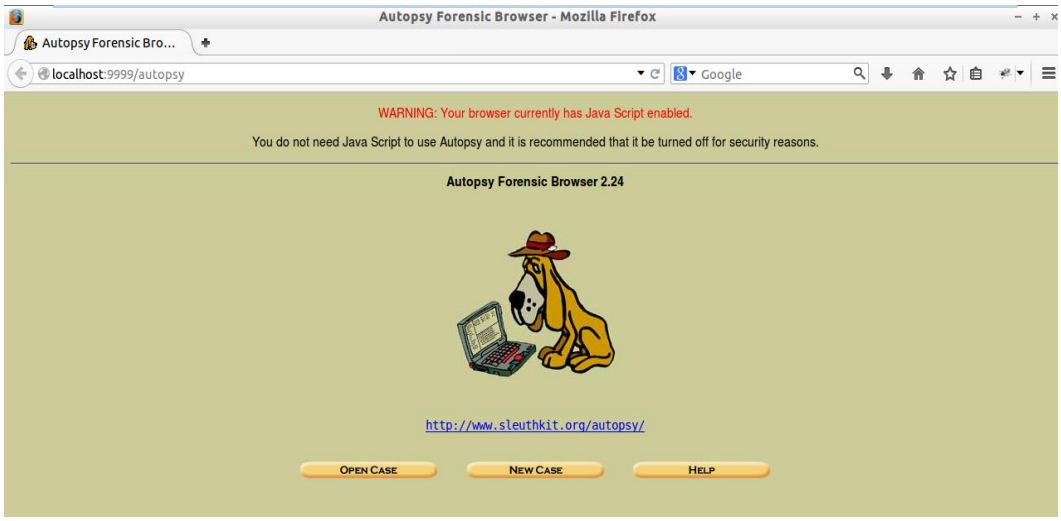


Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Análisis con Autopsy

Ahora para comenzar con el análisis abre el programa Autopsy mediante un navegador web digitando en la barra de direcciones http://localhost:9999/autopsy, luego pulsa en New Case.

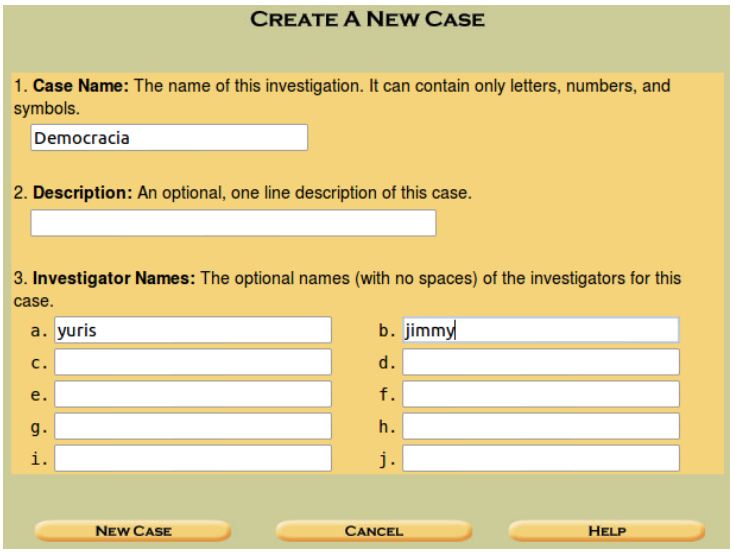


Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

El investigador sigue con la creación del caso y debe de ingresar información como:

a) Case Name: El nombre de esta investigación
b) Description: Descripción del caso
c) Investigator Names: Nombre de los investigadores del caso



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Se ha creado el caso Democracia, selección el nombre del investigador que va a abrir el caso, da clic en ADD Host para agregar el host (hace referencia al dispositivo que está siendo investigado).

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

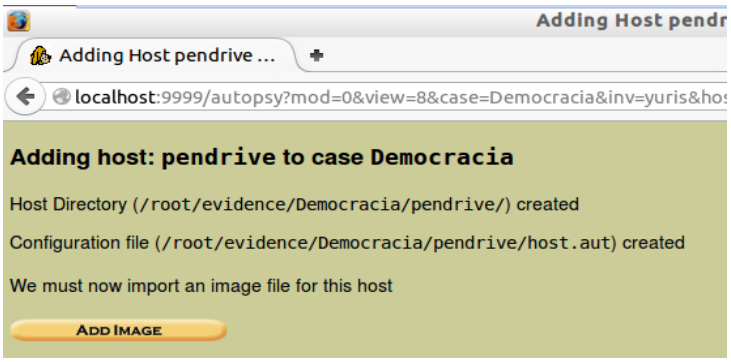
Fuente: Pruebas en el computador

Debe agregar el Host Name en este caso es pendrive y de clic en ADD Host.

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

El investigador visualiza que se creó un directorio para el Host y continúa dando clic en ADD IMAGE para importar una imagen al host.

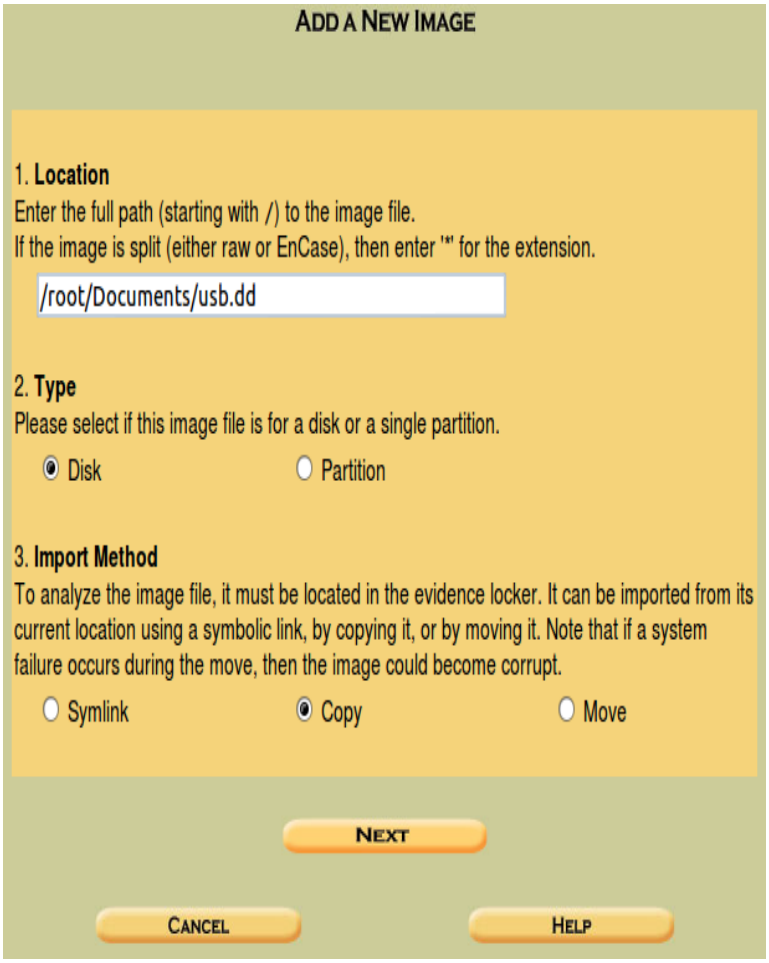


Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

En la ventana ADD A NEW IMAGE se debe ingresar la siguiente información:

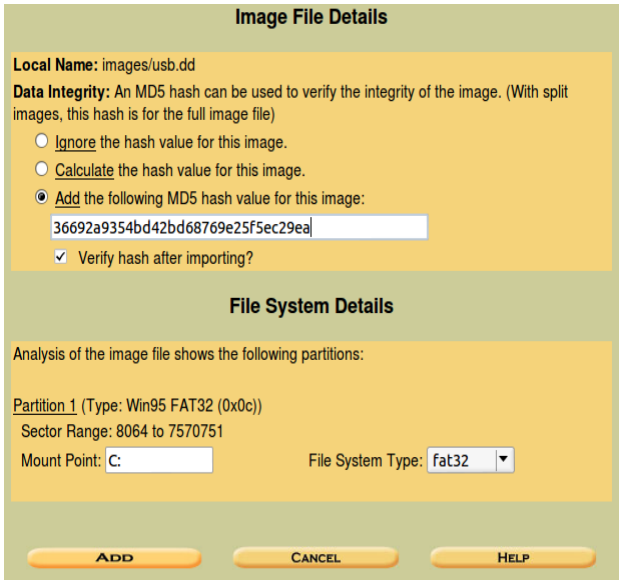
a) Location: Ingrese la ruta donde se encuentra la imagen dd
b) Type: Escoge el tipo de imagen si es de un disco completo o una partición
c) Import Method: Seleccione copy la cual va a permitir realizar una copia de la imagen y no trabajar la imagen original directamente evitando tentar con la integridad de la información.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

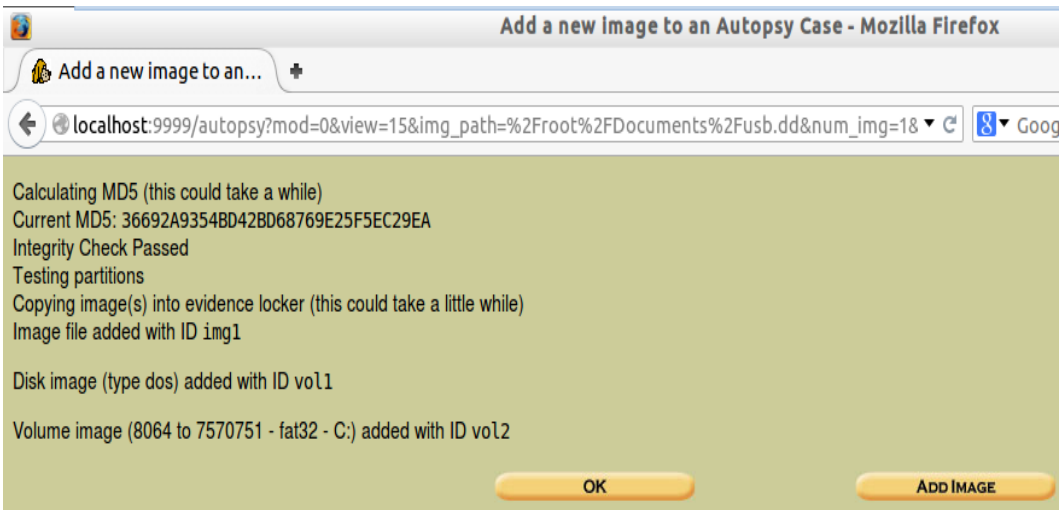
Seleccione ADD e ingrese el MD5 para comprobar que la copia sea exacta, en la parte inferior no cambie nada porque el tipo de sistema de archivo es fat32 y por ultimo de clic en ADD.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

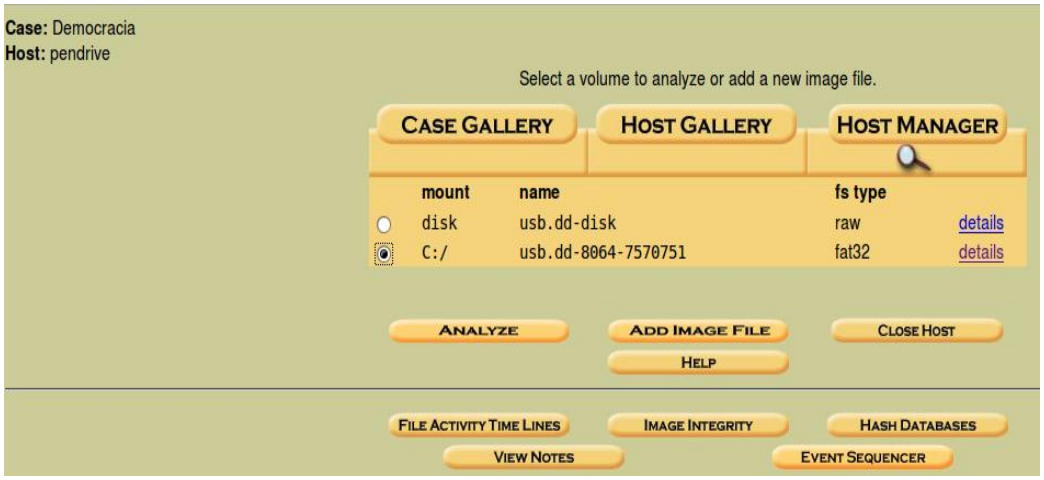
Observe que el cálculo del MD5 de la imagen usb.dd es igual a la agregada por el investigador eso quiere decir que la imagen esta íntegra y que puede seguir con su análisis, pulse el botón OK.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

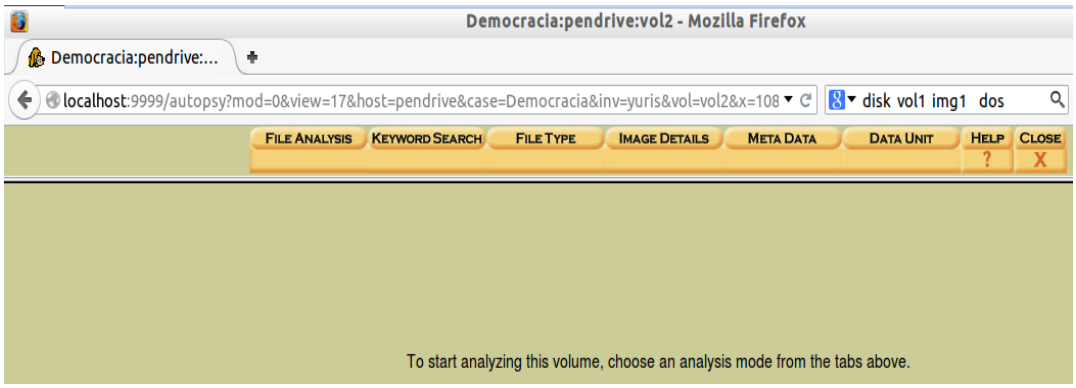
Escoja la c:/ y de clic sobre el botón ANALIZE



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

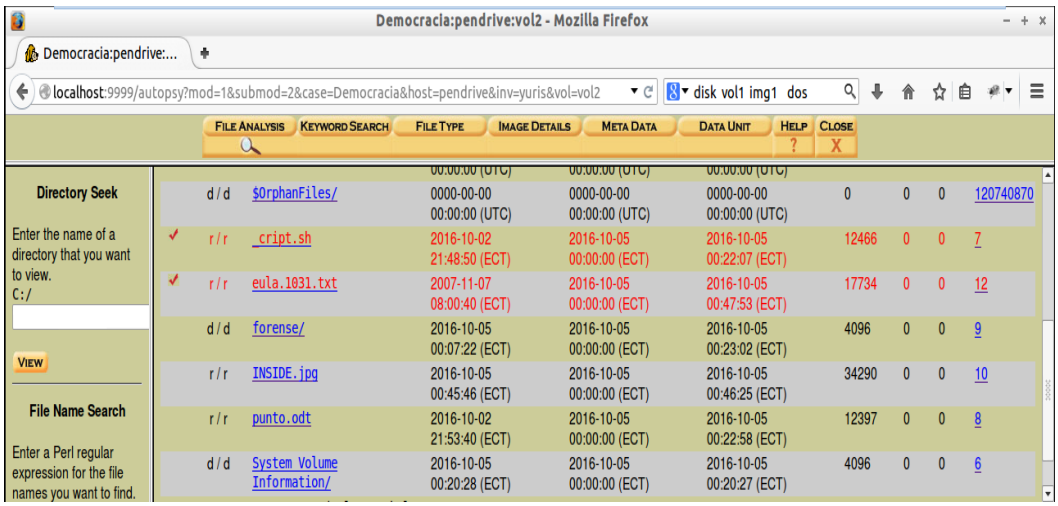
Le mostrará las diferentes opciones que tiene Autopsy para analizar la imagen, escoge la opción FILE ANALYSIS.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

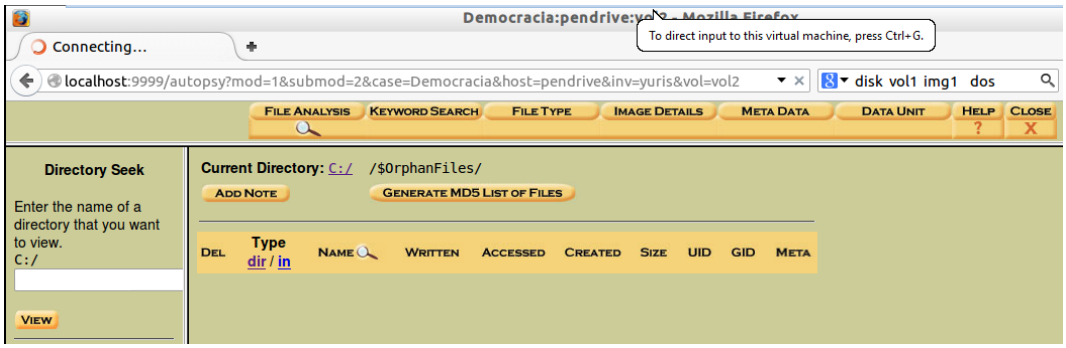
FILE ANALYSIS le presenta detalladamente todos los archivos que se encuentran en la imagen llamada usb.dd; observe que contiene dos archivos subrayados y con letras rojas eso quiere decir que han sido eliminados, puede recuperarlos siempre que el espacio o sector no haya sido cubierto por otro archivo.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

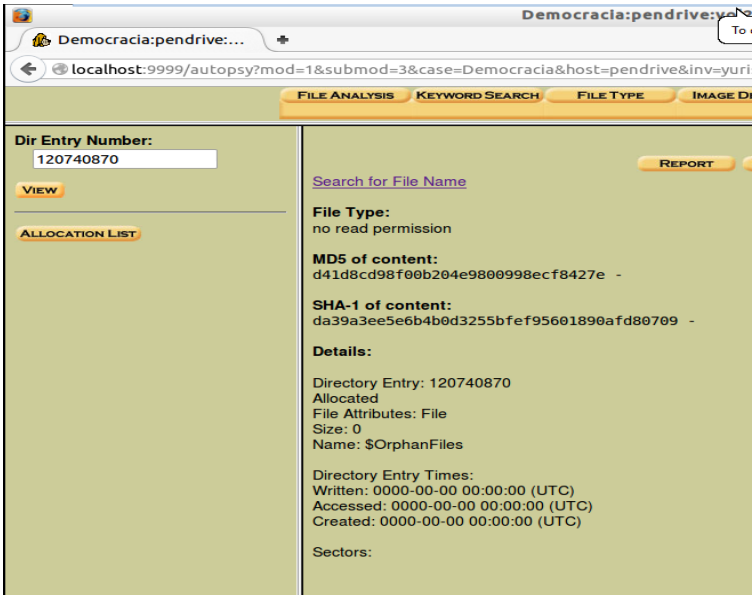
Analice la primera carpeta que aparece llamada $OrphanFiles dando clic sobre la misma, la cual por lo general contiene archivos eliminados, pero en este caso ha mostrado que está vacía.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

El investigador realiza otro análisis a la misma carpeta ahora dando clic sobre el valor de los Meta que es 120740870 y observa que está vacía porque no aparece ningún sector asignado, también muestra el size, el Md5 y otros parámetros.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Siguiendo con el análisis el investigador da clic sobre el archivo _cript.sh en la parte inferior se muestran caracteres entre ellos visualiza el texto opendocument.text el cual indica que el archivo no es .sh sino un .odt.

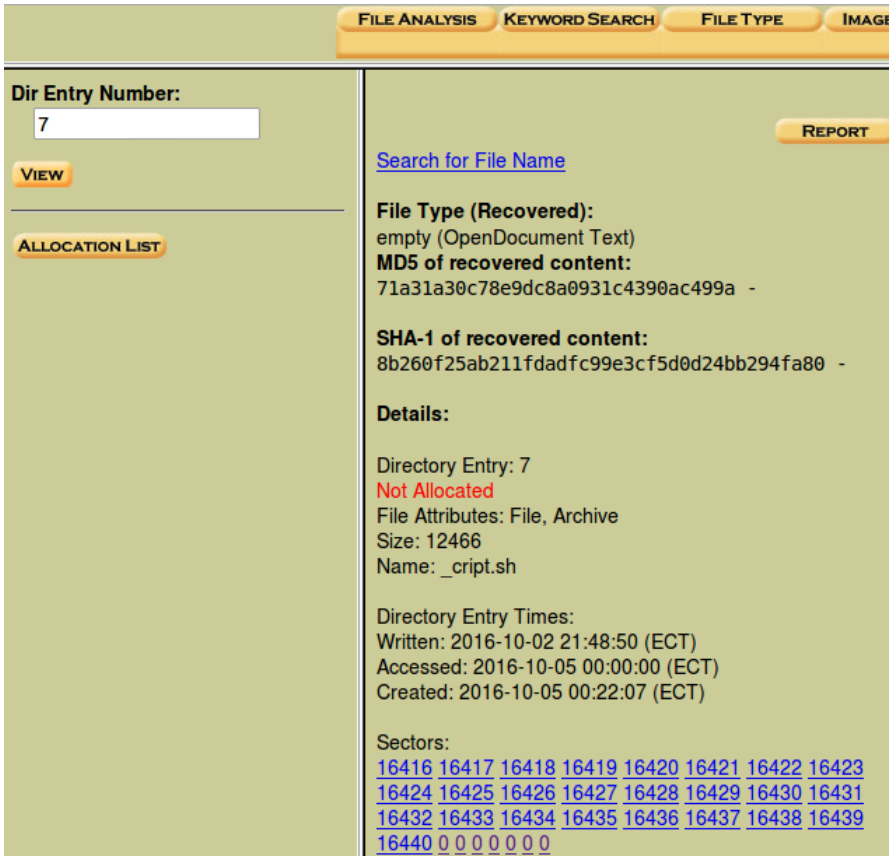
Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Para estar seguro de que al archivo _cript.sh se le ha cambiado la extensión da clic sobre el valor 7 que hace referencia al directorio en que se encuentra, aclara que el tipo de archivo es Opendocument text y observa que en la parte de sectores aparecen ceros esto puede significar dos cosas, la primera que el archivo ha sido manipulado o la segunda, que hay archivos eliminados en esos sectores sobrescritos con ceros para luego ser utilizados.

Para confirmar si el archivo ha sido manipulado calcula cuántos sectores debe ocupar entonces aplica la formula ((12466 + 511) / 512) = 25 sectores y ve que los sectores con ceros no pertenecen a este archivo.

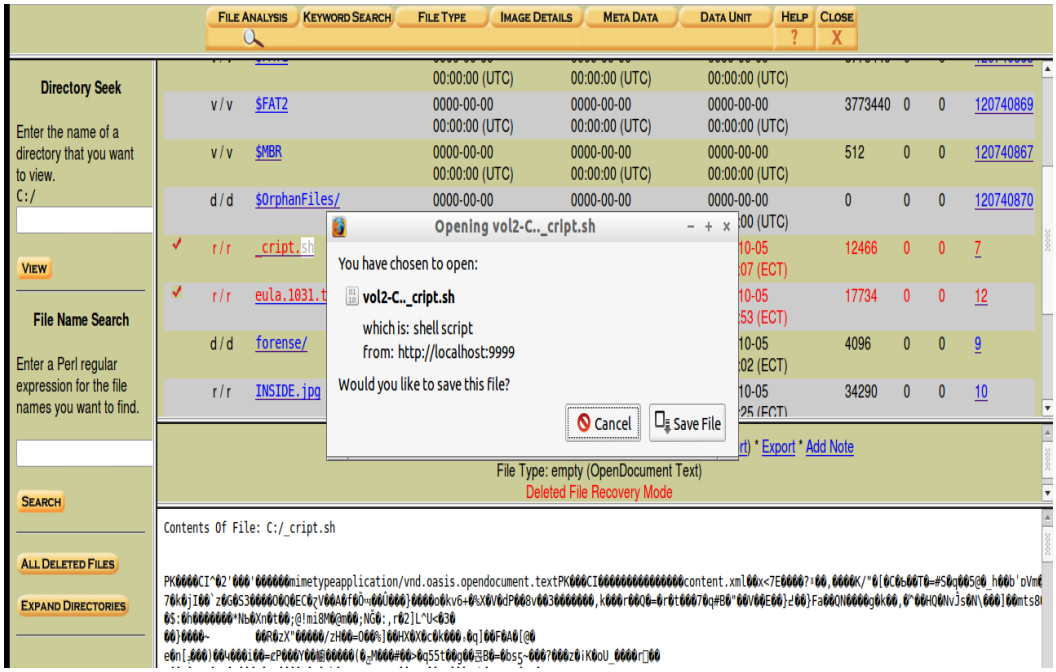
Nota: Un sector guarda 512 bytes de datos.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

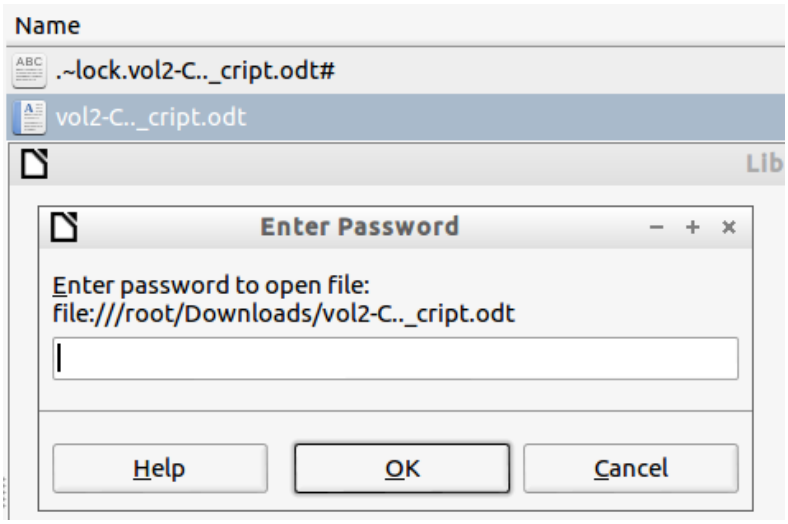
El investigador egresa a FILE ANALYSIS pulsa sobre _cript.sh, en la parte inferior selecciona Export y por ultimo Save file para descargar el archivo.



Elaborado: Sánchez Montero Yuris, Mite Villón Jimmy

Fuente: Pruebas en el computador

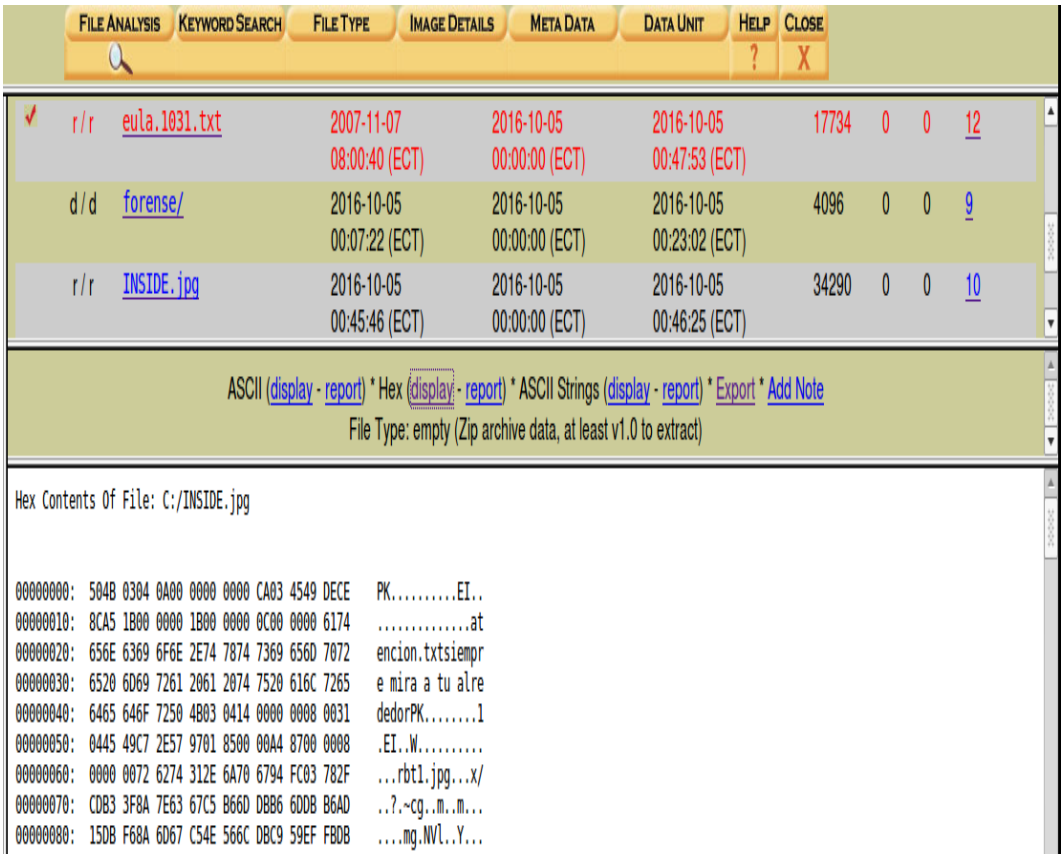
Ya descargado el archivo se procede a cambiarle la extensión a .odt que es la correcta y lo abre pero le pide una contraseña la cual todavía no la conoce.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

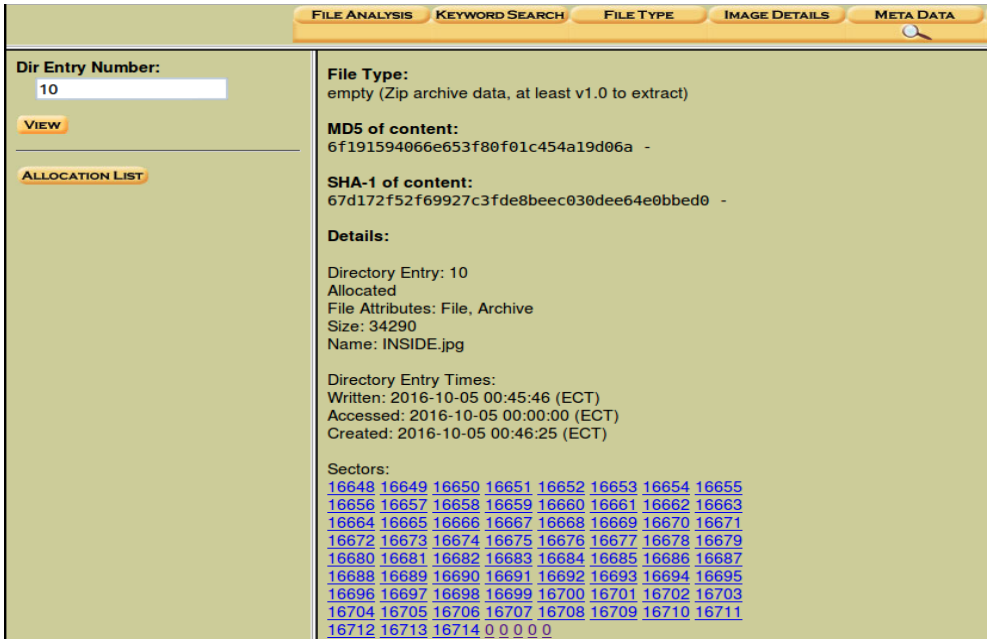
Se continua analizando los demás ficheros y no se encuentra nada relevante que se vincule con este documento hasta que hubo un fichero que llamó la atención que es el INSIDE.jpg vio sus caracteres en hexadecimal y su cabecera no concordaba con tipo de archivo jpg, la cabecera que posee este archivo es 50 4B 03 04 la cual pertenece a un archivo .zip.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

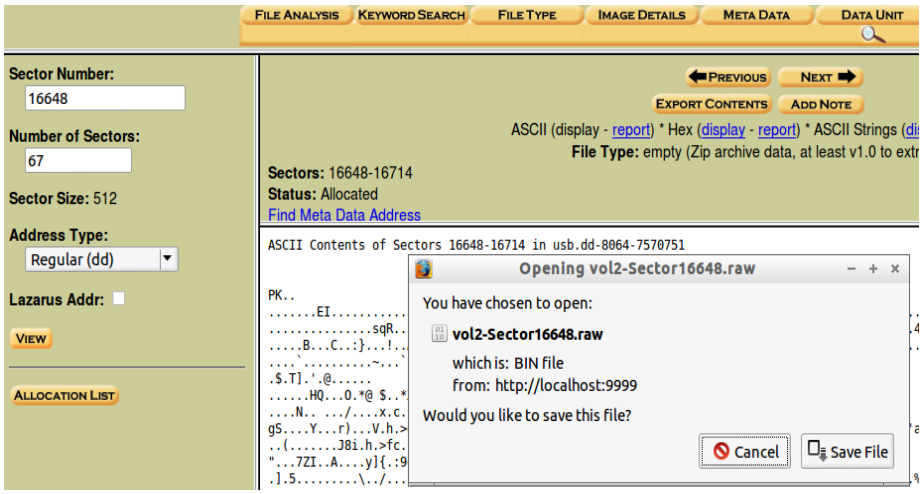
Seleccionar la opción META DATA e ingresar el valor 10 el cual pertenece al directorio del archivo INSIDE.jpg y confirma nuevamente que el archivo es de tipo zip, calcula la cantidad de sectores que se deben ocupar en 34290 bytes y como resultado es 67 lo cual está correcto.



Elaborado: Sánchez Montero Yuris, Mite Villón Jimmy

Fuente: Pruebas en el computador

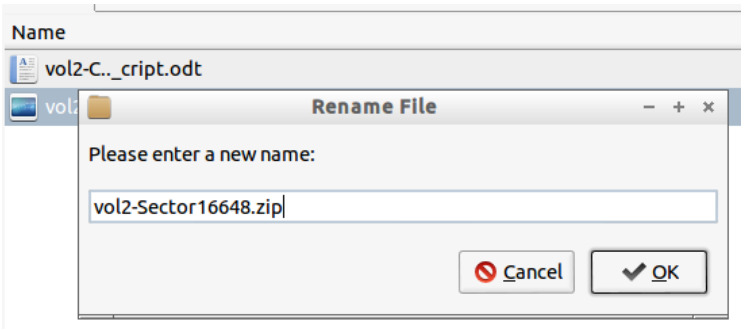
El investigador se dirige a la opción DATA UNIT ingresa el sector con el cual empieza, el número total de sectores del archivo INSIDE.jpg, escoge Export Contents y por ultimo clic Save File.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

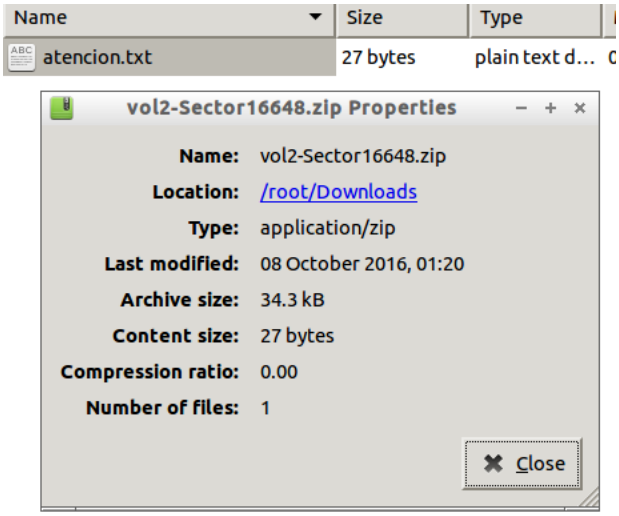
Descarga del archivo para cambiar la extensión a tipo zip y clic en ok.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Al abrir la carpeta solo se muestra un archivo llamado atencion.txt con un tamaño de 27 bytes pero en propiedades le indica que el tamaño del archivo es de 34.3 KB, esto le anuncia que hay un archivo oculto.

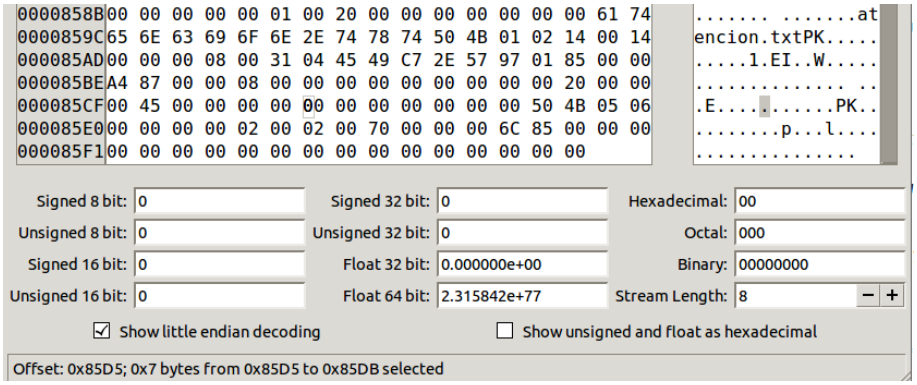


Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

El investigador procede con abrir el editor hexadecimal llamado GHex para analizar la carpeta y comienza a leer en la parte derecha que aparece el archivo llamado atención.txtPK y otro llamado rbt1.jpg, se dirige hasta la parte final y otra

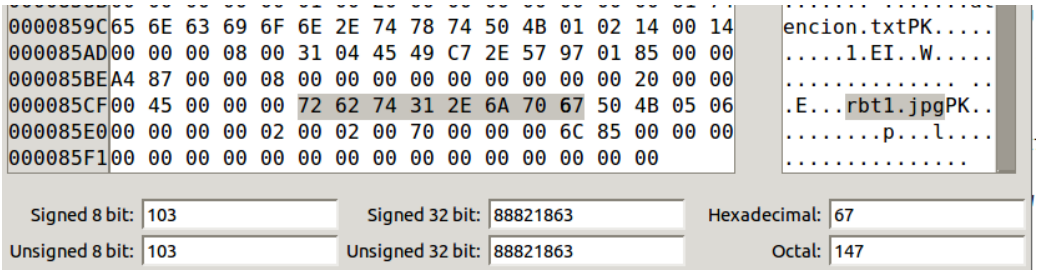
vez observa el archivo llamado atención.txtPK pero ahora ya no aparece el nombre del otro archivo solo puede ver unos puntos suspensivos seguidos de un PK.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

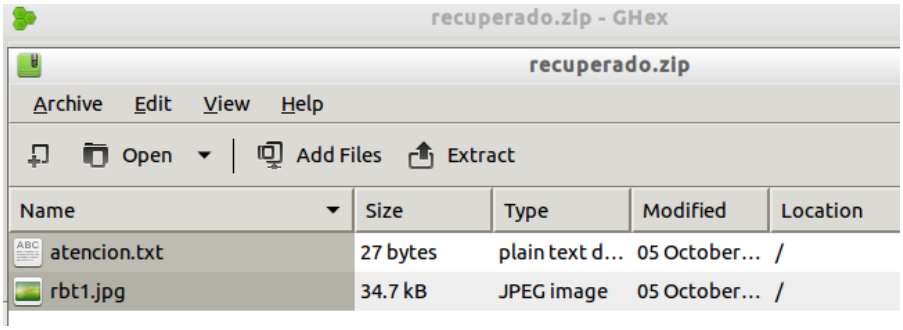
El investigador procede a agregar el nombre del archivo rbt1.jpg antes del último PK el cual ha sido remplazado por ceros para poder ocultarlo, guarda el archivo con nombre recuperado.zip.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

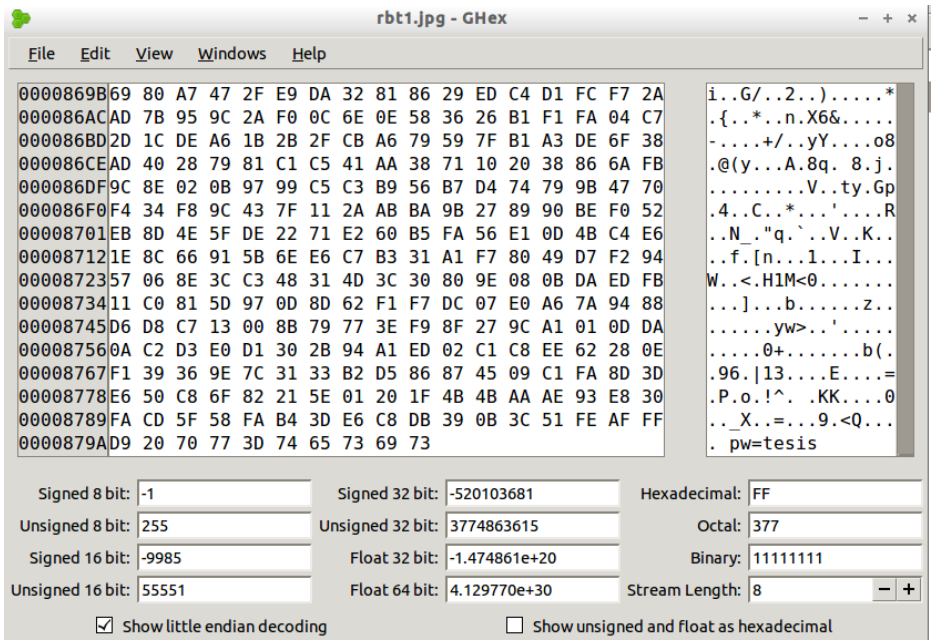
Al abrir el archivo recuperado.zip se puede observar que apareció el llamado rbt1.jpg.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

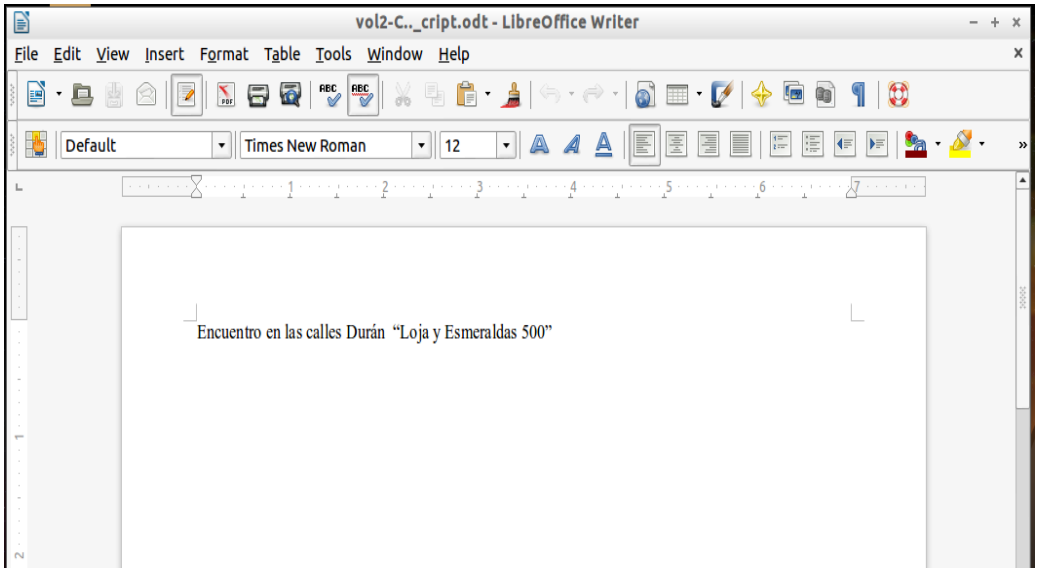
Analiza la imagen obtenida con el editor hexadecimal para saber cuál es el motivo de estar oculta, observa que al final se había agregado el texto pw=tesis. La cual prueba con el archivo .odt que pide una contraseña.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

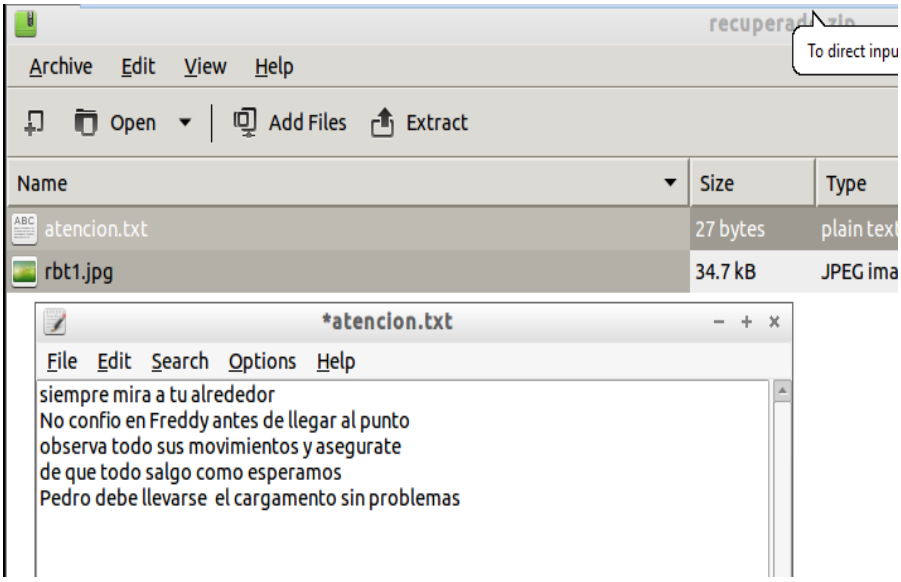
Ingresa por contraseña el texto “tesis” y el archivo .odt se abre dando la siguiente información.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Por último, el investigador abre el archivo atención.txt el cual presenta la siguiente información.



Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador

Mostrando de esta manera la siguiente información: “Siempre mira a tu alrededor, no confió en Freddy antes de llegar al punto observa todos sus movimientos y asegúrate de que todo salga como esperamos, Pedro debe llevarse el cargamento sin problemas “

Encuentro en las calles en las calles Durán “Loja y Esmeraldas 500”.

Elaborado: Mite Villón Jimmy, Sánchez Montero Yuris

Fuente: Pruebas en el computador