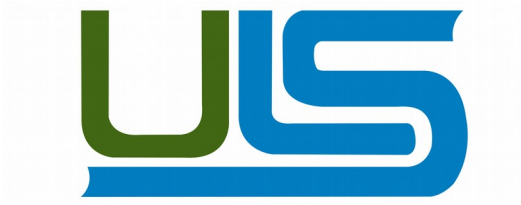
UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN



IMPLEMENTACION DE UN PROGRAMA PARA LA RECUPERACION DE EVIDENCIA FORENSE INFORMATICA

MATERIA:

ANALISIS DE SISTEMAS

INTEGRANTES:

N°	Apellidos	Nombres	Carnet	Participación
1	Rodriguez Rodriguez	Marbin Antonio	RR01132610	100%
2	Gonzales	Oscar Antonio	G01132991	100%
4	Mejia Barahona	Carlos Alberto	MB01132820	100%

DOCENTE:

LIC. JOSÉ LUIS ALVARADO AGUILAR

SAN SALVADOR 14 DE NOVIEMBRE DE 2017

PRESENTACIÓN

Este perfil del trabajo final, pretende mostrar todos los aspectos generales que contendrá el documento del proyecto final, como proyecto, se pretende mostrar los aspectos fundamentales que tiene el software “Autopsy”, así como también los pasos a seguir para su correcta instalación y manejo.

Autopsy es una plataforma de interfaz gráfica para las herramientas de análisis forense digital que en sistemas Unix trabajo bajo la linea de comandos, este software es utilizado para investigar lo que sucedió en una computadora, tratar la información de discos duros e incluso se puede utilizar para recuperar información de una memoria USB. Autopsy es una interfaz intuitiva fácil de usar, esta basado en HTML, se puede conectar al servidor de Autopsy usando un navegador y en el se crea una interfaz de tipo ”Administrador de Archivos” que muestra detalles de los datos eliminados y las estructuras del sistema de archivos.

La utilización de un software para el manejo de evidencia forense, como “Autopsy”, permitirá obtener el conocimiento necesario para la gestión de la información de nuestros equipos de computo, así como también profundizar en el conocimiento de nuevas herramientas que nos permitan mantenernos al día con las técnicas que se utilizan en casos reales de delitos informáticos, así como también en el manejo de las evidencias informáticas forenses.

JUSTIFICACIÓN

En nuestros días, es de vital importancia conocer herramientas informáticas que nos permitan estar al tanto de lo que pasa o pasó en nuestros equipos de computo, es de todos sabido que las computadoras son vulnerables a miles de ataques a través de la Internet, ataques que pueden venir desde cualquier parte del mundo sin saber quien los provocó o para que, también no solo,estos ataques pueden venir de la Red, sino que también pueden darse o provocarse en nuestros mismos computadores, simplemente con dejar nuestra computadora encendida estamos siendo vulnerables a que cualquier persona pueda entrar en nuestros sistemas y archivos, y cambiar o modificar nuestros datos.

La utilización de herramientas para tratar las evidencias informáticas forenses, vienen a contribuir al conocimientos de técnicas que podemos poner en practica a la hora de tratar nuestra información en casos en los que queramos comprobar la veracidad de dichos datos, la implementación de un software como “Autopsy” es de gran ayuda para dar seguimiento a una investigación de un delito informático, ya sea que se requiera analizar un disco duro, una memoria o todo el computador, este software cubre con estas necesidades.

En tal sentido, este proyecto permitirá afianzar los conocimientos necesarios para el buen trato de la información en casos de delitos informáticos y también viene a reforzar el uso de herramientas informáticas dedicadas para fines específicos, lo cual abona al conocimiento y desarrollo técnicas para nuestro aprendizaje.

OBJETIVOS

OBJETIVO GENERAL

- Conocer de manera general el funcionamiento del software autopsy y cuales son su aportes a la informática forense.

OBJETIVOS ESPECÍFICOS

- Mostrar como se realiza la instalación del software de informática forense autopsy
- Enumerar las ventajas y desventajas que ofrece autopsy a la informática forense.
- Realizar un análisis básico de informática forense utilizando autopsy

ANTECEDENTES

El campo de la informática forense se inició en la década de 1980, poco después de que las computadoras personales se convirtieran en una opción viable para los consumidores. En 1984, fue creado un programa del FBI. Conocido por un tiempo como el Programa de Medios Magnéticos, que ahora se conoce como CART (CART, del inglés computer analysis and response team), o análisis de informática y equipo de respuesta. Poco después, el hombre al que se le atribuye ser el "padre de la informática forense", comenzó a trabajar en este campo. Su nombre era Michael Anderson, y era un agente especial de la División de Investigación Criminal del IRS. Anderson trabajó para el gobierno en esta capacidad hasta mediados de 1990, tras lo cual fundó New Technologies, Inc., un equipo que lleva la firma forense.

Autopsy® es una de las principales plataformas forense digital e interfaz gráfica de extremo a extremo. Construido por Basis Technology con las características que se espera de las herramientas forenses comerciales, Autopsy es una solución de investigación de disco duro rápida, completa y eficiente que evoluciona según sus necesidades.

MATERIALES Y MÉTODOS

1. Área de estudio: La investigación se realizara en las instalaciones de la Universidad Luterana Salvadoreña y en el hogar de cada miembro del equipo de expertos involucrados en al caso.

2. Materiales y equipos:

Materiales y Equipos	Descripción
3 Equipos portátiles	
Sistema Operativos Debian 8	
Autopsy	Herramienta libre que existe para el análisis de evidencia digital.
fdisk	Es un comando para manipular las particiones lógicas de una unidad físicas de almacenamiento.
photorec	Es un software diseñado para recuperar archivos perdidos incluyendo videos, documentos y archivos de los discos duros y CDRoms así como imágenes perdidas (por eso el nombre PhotoRecovery) de las memorias de las cámaras fotográficas, MP3 players, PenDrives, etc. PhotoRec ignora el sistema de archivos y hace una búsqueda profunda de los datos, funcionando incluso si su sistema de archivos está muy dañado o ha sido re-formateado.
dd	Es un comando de la familia de los sistemas operativos Unix, que permite copiar y convertir datos de archivos a bajo nivel, se utiliza para crear copias de seguridad de la información en crudo.
Exiftool	Herramienta para la extracción y manipulación de meta-datos de un archivo.

3. Métodos y procedimientos: se describirán brevemente, los métodos y procedimientos que se planee usar dando, si fuera el caso, las citas bibliográficas correspondientes, si ya fueran conocidos, e indicando claramente si se trata de desarrollar nuevos métodos o procedimientos.

La metodología a utilizar para la investigación estará basada en las directrices para la recopilación de evidencias y su almacenamiento descritas en el RFC3227.

Que dicta los siguientes procedimientos:

- Capturar una imagen del sistema tan precisa como sea posible.
- Realizar notas detalladas, incluyendo fechas y horas indicando si se utiliza horario local o UTC.

- Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
- En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis.
- Recoger la información según el orden de volatilidad (de mayor a menor).
- Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera.

4. Duración: El tiempo que se tomará para realizar la investigación será un lapso de 16 días el cual inicia el día diez de noviembre de 2017 y finaliza el día 25 de noviembre dela año de 2017.

CRONOGRAMA DE ACTIVIDADES

ACTIVIDADES	SEMANAS					
	Sem 1			Sem 2		
Creación de imagen de dispositivos para el análisis	X					
Extracción y recopilación de datos a nivel de bits		X				
Análisis de los datos Extraídos			X			
Documentación de Resultados				X		
Entrega de los resultados obtenidos					X	

BIBLIOGRAFÍA

http://software-libre-if.blogspot.com/p/tutorial-de-autopsy.html