Universidad Tecnológica de El Salvador

FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS

TÉCNICO EN INGENIERÍA DE HARDWARE

TEMA:

"KIT DE HERRAMIENTAS DE SOFTWARE EN INFORMÁTICA FORENSE PARA SER UTILIZADO EN SEMINARIOS EN EL LABORATORIO DE HARDWARE DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR"

TRABAJO DE GRADUACIÓN PRESENTADO POR:

SAMUEL DOLORES ANTONIOLÓPEZ ALFARO

DOLORES WILFREDOROSALES

JONATHAN VLADIMIR SIBRIAN IRAHETA

PARA OPTAR POR EL GRADO DE:

TÉCNICO EN INGENIERÍA DE HARDWARE

SEPTIEMBRE, 2014

SANSALVADOR, EL SALVADOR, CENTRO AMERICA

AUTORIDADES UNIVERSITARIAS.

ING. NELSON ZÁRATE SÁNCHEZ

RECTOR

LIC. JOSE MODESTO VENTURA

VICERRECTOR ACADEMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

ING. CLAUDIA LISSETH RODRÍGUEZ DE DIMAS

PRESIDENTA

ING. MARIO ALBERTO VALLE AGUIRRE.

PRIMER VOCAL

LIC. MARVIN ELENILSON HERNÁNDEZ

SEGUNDO VOCAL

SEPTIEMBRE, 2014

SAN SALVADOR, EL SALVADOR, CENTRO AMERICA.

Universidad Tecnológica de El Salvador

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:

Ing. Mario Alberto Valle Aguirre, Lic. Marvin Elenilson Hernández Montoya, Ing. Claudia Lissette Rodríguez de Dimas, a las 12:30m. del día Viernes, 27 de junio de dos mil catorce.

Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

1-Samuel Dolores Antonio López Alfaro	Carnet 28-2573-2006
2-Dolores Wilfredo Rosales	Carnet 28-3516-2010
3-Jonathan Vladimir Sibrian Iraheta	Carnet 28-4463-2011

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:
"Kit de herramientas de Software en informática Forense, para ser utilizada en seminarios en el laboratorio de Hardware de la Universidad Tecnológica de El Salvador"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE HARDWARE

Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

APROBADO

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 27 de junio de 2014.

F. _____
PRIMER VOCAL
Ing.Mario Alberto Valle Aguirre

F. _____
SEGUNDO VOCAL
Lic.Marvin Elenilson Hernández Montoya

F. _____
PRESIDENTE
Ing.Claudia Lissette Rodríguez de Dimas

AGRADECIMIENTOS

Agradezco a Dios Nuestro Señor por haberme guiado en el desarrollo y culminación de mi carrera, a mi familia especialmente a María Julia Rosales (QEPD) por el apoyo incondicional brindado, a todos mis amigos que siempre estuvieron animando e impulsando a seguir adelante, agradezco de manera especial a Carolina González M. quien me dio la motivación para emprender mis estudios superiores. A Ing. Raúl Ramírez por su comprensión y apoyo, A Jorge Antonio Iraheta por sus consejos y asesoría técnica.

Agradezco a la Comisión de becas de la Alcaldía Municipal de Sensuntepeque por medio del Ing. Edgar Bonilla,por haber sido el motor económicoatravésde la beca otorgada a mi persona, que me permitiera realizar mis estudios.

Agradecido con todos los catedráticos de los que tuve el privilegio de ser alumno en las diferentes materias de mi plan de estudio por todos los conocimientos que compartieron conmigo. Al Lic. Marvin Hernández por su apoyo, paciencia y dedicación como asesor, a los miembros del jurado Ing. Claudia Lisseth Rodríguez de Dimas yIng. Mario Alberto Valle Aguirre.

A Samuel Dolores Antonio López Alfaro y Jonathan VladimirSibrianIraheta, con quienes tuve el honor de trabajar para poder culminar nuestro proyecto de grado.

¡¡¡Gracias y Que Dios dador de todo bien, les provea de múltiplesbendiciones!!!

Dolores Wilfredo Rosales.

Agradezco:

A mi familia y amigos por el apoyo brindado durante el desarrollo de esta tesis, a mis compañeros Dolores Wilfredo Rosales y Jonathan VladimirSibrianIraheta, por ser un excelente grupo de trabajo sin los cuales este proyecto no hubiese sido posible, al Lic. Marvin Elenilson Hernández Montoya por su gran aporte como asesor metodológico y técnico, por las observaciones y correcciones realizadas al presente trabajo, a los todos los catedráticos de las materias de las cuales consta el Técnico en Ingeniería de Hardware de la Universidad Tecnológica de El Salvador por los conocimientos transmitidos y finalmente a los miembros de jurado calificador Ing. Claudia Lisseth Rodríguez de Dimas y Ing. Mario Alberto Valle Aguirre.

Gracias a todos.

Samuel Dolores Antonio López Alfaro.

Agradecimientos

En primer lugar, quiero expresar mis agradecimientos a Dios por permitirme dar cumplir uno de mis grandes sueños. Y por supuesto a cada uno de aquellos que estuvieron siempre a mi lado brindándome apoyo.

También tengo que decirle gracias a mis padres fieles compañeros en los momentos más difíciles y que me presionaron muchas veces a seguir adelante.

A mis compañeros de estudio que aun en medio de la adversidad me bridaron aliento y me apoyaron.

Compañeros de tesis por los consejos y las observaciones, fueron muy valiosas gracias por su apoyo

Doy mis más profundos agradecimientos a los profesores que con amor y sabiduría nos guiaban por el camino.

No puedo pasar por alto a un buen amigo y asesor Lic. Marvin por su apoyo sin reservas gracias por ayudarme y seguir instruyendo a futuras generacionesdel bien.

Gracias por su apoyo.

Jonathan Vladimir SibrianIraheta,

Índice

Capítulo III Desarrollo de solución

INTRODUCCIÓN.

El presente trabajo de investigación muestra una visión muy clara sobre el efecto de las tecnologías de información como medio de violación a la privacidad. Es por eso que nace la política de seguridad denominada "Informática Forense".

Por ello se hace un planteamiento de la situación actual, sobre los conocimientos de informática forense que se adquieren en la Universidad Tecnológica de El Salvador, por lo que se busca reforzar dichos conocimientos. Haciendo una selección y evaluación de herramientas de software que muestran la factibilidad de estas, para desarrollar un kit de herramientas y material extra curricular, para los estudiantes.

Justificando así la elaboración de un kit de herramientas de software, que permita al estudiante adquirir y practicar conocimientos sobre la revelación de evidencias sobre actos ilícitos dentro de la informática.

Teniendo como objetivos, seleccionar y evaluar las herramientas de software que más se apeguen a las necesidades de los estudiantes. A la vez crear manuales de uso que permitan conocer el funcionamiento de cada uno de los programas y diseñar un material de apoyo para que sea utilizado en seminarios.

Dando a conocer los alcances que se desarrollaran con la elaboración de este proyecto, como lo son: ficha técnica y manual de uso de los programas, material de apoyo para seminario, y la elaboración de un DVD con las herramientas seleccionadas.

La Documentación Técnica presentada a continuación contiene la investigación realizada para poder desarrollar el kit de herramientas, dando a conocer una amplia información sobre la informática forense, su historia, objetivos, los estudios que permite y todo lo relacionado con los delitos informáticos, como lo es la aplicación de la informática forense, la evidencia digital, los orígenes de la evidencia, y una descripción de cada uno de las áreas retomadas en esta investigación todo esto contenido dentro del Marco Teórico de Referencia.

Que permite el desarrollo del Marco Teórico de la Solución, donde se enmarca la elaboración de los productos expuestos en los alcances a lograr dentro del proyecto tales como:

- Ficha técnica de cada uno de los programas seleccionados, que contiene los requisitos necesarios para poder hacer uso de los programas.
- Manuales de los programas seleccionados en los estudios de factibilidad económica y técnica, realizados de una manera clara y objetiva para que se le facilite al usuario la implementación.
- Material de Apoyo, con conceptos básicos sobre informática forense.
- Diseño de Portada e interfaz del DVD que contendrá el kit. Programa con un interfaz amigable al usuario.

La investigación también nos lleva a un Marco Teórico Conceptual, que se refiere a conceptos básicos sobre la informática forense, de los cual serán así llamados

específicamente durante todo el desarrollo del kit de herramientas y en su implementación.

Es de suma importancia conocer como estamos en nuestro país en leyes con lo que a informática forense se refiere por lo que se hace un estudio de un Marco Legal en el cual se mencionan algunos de los artículos relacionados con la criminalidad donde se ve involucrada la informática, y que deja en claro que no hay una ley especifica como en otros países que regule la criminalidad informática.

También es importante conocer los programas a utilizar por lo que en la Documentación Técnica se hace una descripción básica de los programas que permiten conocer sus características, requisitos, funcionamiento y área de aplicación, de esta manera se le facilita al usuario saber cuál es la mejor opción a la hora de elegir un software.

El desarrollo de la solución es la respuesta a la problemática sobre la informática forense, expuesta en las generalidades de esta investigación; donde se muestra información detalladamente de cada uno de los productos o soluciones contenidos dentro del kit de herramientas.

Brindando así un análisis detallado de lo que el kit contiene como los es:

- Software
- Fichas técnica
- Manuales de uso
- Material de apoyo

Para que se tenga una comprensión más fácil sobre los productos, y a la vez que sean de fácil implementación para poder llevar acabo nuestras investigaciones digitales sobre posibles delitos o vulnerabilidades de nuestra computadora.

Dentro de los detalles brindados en el desarrollo de la solución, se muestra la elaboración de un DVD que contendrá los software de herramientas y a la vez se da a conocer de una manera clara la función del producto denominado ficha técnicacontenido en el kit, haciendo referencia a la manera en la cual tiene que estar diseñada y que es lo que debe contener la ficha estipulada para cada software. De la misma manera se detalla el Manual de Uso que tiene que estar realizado de una manera clara y objetiva para que se le facilite al usuario la implementación de dicho manual.

También se hace una reseña del contenido del Material de Apoyo que permitirá al docente o instructor tener conceptos referentes a la informática forense para el desarrollo de los seminarios.

Cada uno de ellos basados en el desarrollo con claridad,y verificando el funcionamiento correcto de cada herramienta incluida en el kit, de igual manera los archivos de fichas técnicas, manual de uso y material de apoyo.

Capítulo I Situación actual

1.1 Situación problemática.

Los entornos tecnológicos y el posicionamiento de internet como herramienta vital para el cumplimiento de metas de individuos y organizaciones, plantean multitud de problemas jurídicos relacionados con el derecho a la privacidad de las personas, los derechos de autor, los derechos del consumidor, las operaciones financieras electrónicas, la adquisición de bienes y servicios , los delitos informáticos como:

- ✓ Pornografía en todas sus formas, inclusive Pornografía infantil.
- ✓ Delitos relativos a la propiedad intelectual e industrial.
- ✓ Delitos relativos al mercado y a los consumidores.
- ✓ Estafas.
- ✓ Descubrimiento y revelación secretos.
- ✓ Delitos contra el patrimonio y el orden socioeconómico.
- ✓ Delitos contra la intimidad y el derecho a la propia imagen.
- ✓ Competencia desleal.
- ✓ Espionaje industrial.
- ✓ Robo de información.
- ✓ Intrusión en sistemas informáticos.
- ✓ Uso fraudulento de recursos corporativos
- ✓ Suplantación de identidad.

La criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de fondos públicos y privados, en los cuales ordenadores y redes han sido utilizados como medio para llevarlos acabo.

Y en el medioestudiantil de técnico en hardware es mínimo el conocimiento teórico y prácticoespecíficoque se obtiene sobre el uso de herramientas, que permitan encontrar la vulnerabilidad o los responsables de dichos delitos informáticos. Esto representa un problema el cual genera un obstáculo en el desarrollo laboral, debido a que el desarrollo de la tecnología y el acelerado crecimiento de los sistemas informáticos van impactando sobre las actividades cotidianas.

Los problemas anteriormente mencionados, dejan como resultado la falta de desarrollo y competitividad laboral en los estudiantes que se especializan en la carrera de técnico en ingeniería en hardware, ya que actualmente las empresas exigen técnicos que brinden confianza, honestidad, y sobre todo conocimientos, habilidades y destrezas en el ámbito de especialidad informática.

1.2 Enunciado del problema.

¿Cómo se pueden complementar los conocimientos adquiridos sobre informática forense en la cátedra de informática de la Universidad Tecnológica de El Salvador?

1.3 Justificación del proyecto.

Con la elaboración de un kit de herramientas de software en informática forense se pretende reforzar las competencias de los estudiantes y además que tengan material extracurricular de apoyo y así proporcionarles herramientas practicas y teóricas que permitan inducir a mejorar la experiencia, desarrollo y competitividad, que los estudiantes necesitan para poder llegar a dominar aspectos importantes como:

- Adquisición y análisis de la memoria
- Herramientas de disco
- Criptografía
- Esteganografía
- Análisis del registro de Windows
- Herramientas de red.

Que son aspectos de mucha utilidad dentro del área de informática forense, ya que estos procesos relacionados con la investigación, hallazgos, y presentación de evidencias digitales, ante sucesos imprevistos relacionados con las Tecnologías de Información y comunicación, tales como: Actos digitales ilícitos, robo de información o vulnerabilidad de algún tipo de ataque informático.

Es por esto que es importante reforzar los conocimientos en esta área de la informática, para que los estudiantes del técnico en ingeniería de hardware de la Universidad Tecnológica de El Salvador, estén a la vanguardia de la informática forense para la

recuperación, verificación, y seguridad de archivos (fotos, video, música, documentos, red, y cuentas electrónicas) importantes.

Con el kit de herramientas de software de informática forense se facilitará manuales de uso, orientados al desarrollo seminarios en el laboratorio de hardware, para mejorar la experiencia, desarrollo y la competitividad que los estudiantes puedan tener en el aspecto laboral.

1.4 Objetivos.

1.4.1 Objetivo general.

Desarrollar un kit de herramientas de software en informática forense para ser utilizado en seminarios en el laboratorio de hardware de la Universidad Tecnológica de El Salvador.

1.4.2 Objetivos específicos.

- ✓ Seleccionar y Evaluar las herramientas de software a incluir en el kit de informática forense.
- ✓ Crear un manual de uso para cada una de las herramientas de software evaluadas y seleccionadas.
- ✓ Diseñar material de apoyo (conceptos básicos) para los alumnos, el cual será utilizado en seminarios sobre informática forense, en el laboratorio de Hardware de la Universidad Tecnológica de El Salvador.

- ✓ Elaborar un DVD con las herramientas de software que contendrá el kit en informática forense.

1.5 Delimitaciones

1.5.1 Temporal:

Nuestro trabajo tendrá una duración de 4 meses que comprende desde el 14 de Marzo al 6 de junio de 2014.

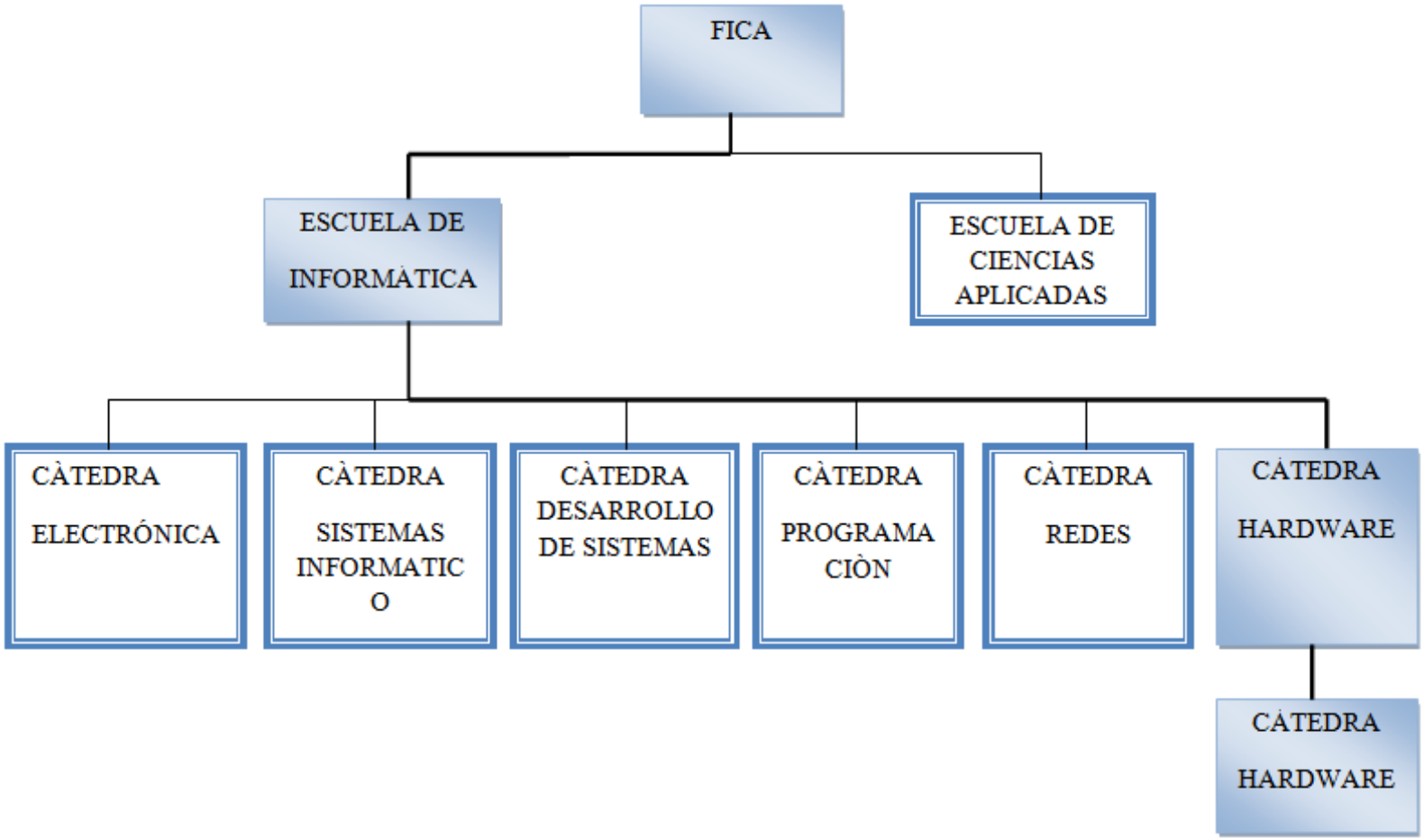
1.5.2 Espacial:

Se realizará en la Universidad Tecnológica de El Salvadorubicada en Calle Arce Nº 1020 San Salvador, El Salvador, Centro América.

1.5.3 Organizacional:

Universidad Tecnológica de El Salvador, a través de la Facultad de Informática y Ciencias Aplicadas, Escuela de Informática; Cátedra de Hardware, Laboratorio de Hardware.

A continuación se muestra el organigrama, en el que se explica el área en que será utilizado el proyecto



1.6 Alcances

El proyecto está orientadoa procesos relacionados con la investigación, hallazgos, y presentación de evidencias digitales, ante sucesos imprevistos relacionados con las Tecnologías de Información, tales como: Actos digitales ilícitos, robo de información o sufrimiento de algún tipo ataque informático.

Promesa		Producto	
1	Mostrar la información básica y requisitos de sistema para cada una de las herramientas de software en informática forense seleccionadas.	1	Ficha Técnica. Se dará una copia impresa para el laboratorio de hardware de la Universidad Tecnológica de El Salvador y un archivo pdf para ser reproducido en las maquinas del laboratorio de harware.
2	Servirá para orientar a los usuarios del kit como utilizar cada una de las herramientas.	2	Manual de Uso. Se dará una copia impresa para el laboratorio de hardware de la Universidad Tecnológica de El Salvador y un archivo pdf para ser reproducido en las maquinas del laboratorio de harware.

3	Será utilizado en los seminarios sobre informática forense en el laboratorio de hardware de la Universidad Tecnológica de El Salvador.	3	Material de Apoyo. Se dará una copia impresa para el laboratorio de hardware de la Universidad Tecnológica de El Salvador y un archivo pdf para ser reproducido en las maquinas del laboratorio de harware.
4	Incluirá todas las herramientas de software en informática forense seleccionadas, en las Áreas de: ➢ Adquisición y análisis de la memoria ➢ Herramientas de disco ➢ Criptografía ➢ Esteganografía ➢ Análisis del registro de Windows ➢ Herramientas de red.	4	DVD (Kit de herramientas en informática forense.). Se proporcionara una copia para el laboratorio de hardware de la Universidad Tecnológica de El Salvador, para reproducirse en las maquinas del laboratorio.

1.7 Estudio de factibilidad.

1.7.1 Factibilidad Económica.

ESTUDIO DE FACTIBILIDAD ECONÓMICA			
HERRAMIENTAS DE DISCO			
Nombre del programa	Recuva	DMDE	NTFS Recovery
Precio	Licencia libre	$ 95.00	$ 99.95
Análisis	Ya que es licencia libre, ecónomicamente Recuva es factible, ya que no genera ningun costo.		
Establecimiento domiciliado o URL	http://www.piriform.com/recuva/download	http://dmde.com/buy.html	http://www.diskinternals.com/order/ntfs/

ESTUDIO DE FACTIBILIDAD ECONÓMICA			
HERRAMIENTAS DE RED			
Nombre del programa	NetworkMiner	Wireshark	RSA NetWitness Investigator
Precio	$ 700.00	GPL	Precio enviado por solicitud
Análisis	Ya que es licencia libre, ecónomicamente Wireshark es factible porque no genera ningun costo.		
Establecimiento domiciliado o URL	http://www.netresec.com/?page=NetworkMiner	http://www.wireshark.org/download.html	https://www.emc.com/products/how-to-buy/index.htm

*GPL = General Public License.

ESTUDIO DE FACTIBILIDAD ECONÓMICA			
ADQUISICIÓN Y ANÁLISIS DE LA MEMORIA			
Nombre del programa	Proccess Dumper	Redline	Forensic Toolkitor (FTK Imager Lite Version)
Precio	Licencia libre	Licencia libre	Licencia libre
Análisis	Económicamente todas las herramientas son factibles, pero se seleccionará Forensic Toolkitor (FTK Imager Lite Version) por obtener uno de los mayores porcentajes de aceptación en la factibilidad técnica.		
Establecimiento domiciliado o URL	http://www.trapkit.de/research/forensic/pd/	http://www.mandiant.com/resources/download/redline/	http://www.accessdata.com/support/product-downloads#FTKImager

ESTUDIO DE FACTIBILIDAD ECONÓMICA			
ANÁLISIS DEL REGISTRO DE WINDOWS			
Nombre del programa	RegRipper	Windows Registry Recovery	Registry Decoder
Precio	Licencia libre	Licencia libre	Licencia libre
Análisis	Debido a que todos los programas son licencias libres, todos son economicamente factibles. Pero, se seleccionará RegRipper por obtener un mayor porcentaje de aceptación en la factibilidad técnica.		
Establecimiento domiciliado o URL	http://regripper.wordpress.com/	http://www.mitec.cz/wrr.html	http://www.digitalforensicssolutions.com/registrydecoder/

ESTUDIO DE FACTIBILIDAD ECONÓMICA			
CRIPTOGRAFÍA			
Nombre del programa	**CriptoClásicos v1_1b**	**AxCrypt v1_7_2850**	**Cryptic Disk Home v3_2_51_710**
Precio	**Licencia libre**	**Licencia libre**	**$ 34.95**
Análisis	**Ya que es licencia libre, lo cual no causará costos a los usuarios y su calificación en la factibilidad técnica fue mayor 75% AxCrypt v1_7_2850 fue seleccionado_**		
Establecimiento domiciliado o URL	**http://www.criptored.upm.es/software/sw_m001c.htm**	**http://www.axantum.com/AxCrypt/Default.html**	**http://www.exlade.com/cryptic-disk/**

ESTUDIO DE FACTIBILIDAD ECONÓMICA			
ESTEGANOGRAFÍA.			
Nombre del programa	OpenPuff 4.00	Steghide	My Lockbox
Precio	Licencia libre	Licencia libre	Licencia libre
Análisis	Debido a que todos los programas son licencias libres, todos son economicamente factibles. Pero, se seleccionará OpenPuff 4.00 por obtener un mayor porcentaje de aceptación en la factibilidad técnica.		
Establecimiento domiciliado o URL	http://embeddedsw.net/OpenPuff_Steganography_Home.html	http://steghide.sourceforge.net/index.php	http://fspro.net/my-lockbox/

1.7.2 Factibilidad Técnica.

ESTUDIO DE FACTIBILIDAD TÉCNICA.								
HERRAMIENTAS DE DISCO.								
Cuadro de evaluación. Se requiere un nivel de calificación del 75%								
Características Técnicas	Ponderación	Recuva		DMDE		NTFS Recovery	
		Valor	Total	Valor	Total	Valor	Total
Sistema Operativos: Windows OS, Linux	25%	1	25.00%	2	50.00%	1	25.00%
Recuperación de discos duros dañados o formateados	20%	2	40.00%	1	20.00%	2	40.00%
Recuperar archivos de una computadora	20%	2	40.00%	2	40.00%	2	40.00%
Recover deleted emails	5%	2	10.00%	0	0.00%	0	0.00%
Análisis en Profundidad	10%	2	20.00%	2	20.00%	2	20.00%
Restauración de discos después de accidente	10%	0	0.00%	0	0.00%	2	20.00%
Admite FAT12/16, FAT32, NTFS	10%	2	20.00%	2	20.00%	1	10.00%
Total	100.00%		155.00%		150.00%		155.00%
	% Final		77.50%		75.00%		77.50%
Análisis	Se utilizará el programa recuva ya que ha obtenido la calificación requerida.						
Calificación: (0) Si no cumple con la característica; (1) Si cumple a medias pero sigue siendo funcional; (2) Cumple con las características.							

ESTUDIO DE FACTIBILIDAD TÉCNICA.							
HERRAMIENTAS DE RED .							
Cuadro de evaluación. Se requiere un nivel de calificación del 75%							
Caracteristicas Técnicas	Ponderación	NetworkMiner		Wireshark		RSA NetWitness Investigator	
		Valor	Total	Valor	Total	Valor	Total
Sistema Operativos: Windows OS, Linux	25%	2	50.00%	2	50.00%	1	25.00%
Analizar archivos PCAP	20%	2	40.00%	2	40.00%	2	40.00%
Parse PcapNG files	20%	2	40.00%	2	40.00%	2	40.00%
Exportación de resultados a CSV / Excel	5%	2	10.00%	0	0.00%	0	0.00%
Velocidad de análisis PCAP	10%	2	20.00%	2	20.00%	2	20.00%
Directorio de salida de archivos configurable	10%	1	10.00%	2	20.00%	1	10.00%
Localización Geo IP	10%	2	20.00%	0	0.00%	2	20.00%
Total	100.00%		190.00%		170.00%		155.00%
	% Final		95.00%		85.00%		77.50%
Análisis	NetworkMiner ha obtenido el mayor nivel de calificación, pero se seleccionará Wireshark, por ser softwareGLP (General Public License).						
Calificación: (0) Si nocumple con la característica; (1) Si cumple a medias pero sigue siendo funcional; (2) Cumple con las característica.							

ESTUDIO DE FACTIBILIDAD TÉCNICA.							
ADQUISICIÓN Y ANÁLISIS DE LA MEMORIA.							
Cuadro de evaluación. Se requiere un nivel de calificación del 75%							
Caracteristicas Técnicas	Ponderación	Proccess Dumper		Redline		Forensic Toolkit (FTK Imager Lite Version)	
		Valor	Total	Valor	Total	Valor	Total
Version para linux y windows	10%	2	20.00%	2	20.00%	1	10.00%
Genera registro de auditoría e informes	20%	1	20.00%	1	20.00%	2	40.00%
Captura la memoria y permite analizarla	10%	1	10.00%	2	20.00%	2	20.00%
Dispone de entrono gráfico	30%	2	60.00%	2	60.00%	2	60.00%
Convierte un proceso de la memoria a fichero	20%	2	40.00%	1	20.00%	1	20.00%
Incluyen: NTFS, CDFS, UDF, HFS, FAT 12/16/32 y Linux EXT2 & EXT3.	10%	2	20.00%	2	20.00%	2	20.00%
Total	100.00%		170.00%		160.00%		170.00%
	% Final		85.00%		80.00%		85.00%
Análisis	Forensic Toolkit (FTK Imager Lite Version) ha obtenido una de las mayores calificación y como es licencia libre ha sido seleccionado para incluirse en el kit.						
Calificación: (0) Si nocumple con la característica; (1) Si cumple a medias pero sigue siendo funcional; (2) Cumple con las característica.							

ESTUDIO DE FACTIBILIDAD TÉCNICA.							
ANÁLISIS DEL REGISTRO DE WINDOWS.							
Cuadro de evaluación. Se requiere un nivel de calificación del 75%							
Caracteristicas Técnicas	Ponderación	RegRipper		Windows Registry Recovery		Registry Decoder	
		Valor	Total	Valor	Total	Valor	Total
Permite obtener de forma gráfica datos del sistema	10%	1	10.00%	1	10.00%	2	20.00%
Explorador del registro de seguridad	20%	2	40.00%	2	40.00%	0	0.00%
Muestra todos los clientes instalados, protocolos y servicios de la red	10%	0	0.00%	2	20.00%	1	10.00%
Abrir secciones de registro y analizarlas	30%	2	60.00%	2	60.00%	2	60.00%
Realizar la navegación, búsqueda, análisis y presentación de informes	20%	2	40.00%	1	20.00%	1	20.00%
Muestra todos los dispositivos configurados que funcionan en el equipo host	10%	2	20.00%	2	20.00%	2	20.00%
Total	100.00%		170.00%		170.00%		130.00%
	% Final		85.00%		85.00%		65.00%
Análisis	Por obtener la calificación mas alta y ser licencia libre se selecciono a RegRipper para incluirlo en el kit.						
Calificación: (0) Si nocumple con la característica; (1) Si cumple a medias pero sigue siendo funcional; (2) Cumple con las característica.							

ESTUDIO DE FACTIBILIDAD TÉCNICA.							
CRIPTOGRAFÍA.							
Cuadro de evaluación. Se requiere un nivel de calificación del 75%							
Características Técnicas	Ponderación	CriptoClásicos v1.1b		AxCrypt v1.7.2850		Cryptic Disk Home v3.2.51.710	
		Valor	Total	Valor	Total	Valor	Total
Sistema Operativo: Windows	20%	1	20.00%	1	20.00%	2	40.00%
Encriptación de documentos.	30%	2	60.00%	2	60.00%	2	60.00%
No requiere ninguna configuración de usuario necesario antes de su uso.	10%	0	0.00%	2	20.00%	0	0.00%
Cifrado AES con claves de 128 bits.	10%	0	0.00%	2	20.00%	2	20.00%
Opciones de modo de servidor.	10%	0	0.00%	2	20.00%		0.00%
Soporte para archivos de más de 4GB (a excepción de los archivos libre descifrar).	10%	0	0.00%	2	20.00%	2	20.00%
Se integra bien con los servicios de intercambio de archivos basado en web.	10%	0	0.00%	2	20.00%	0	0.00%
Total	100.00%		80.00%		180.00%		140.00%
	% Final		40.00%		90.00%		70.00%
Análisis	AxCrypt v1.7.2850 fue seleccionado ya que es licencia libre y por su alta calificación el la factibilidad técnica.						
Calificación: (0) Si no cumple con la característica; (1) Si cumple a medias pero sigue siendo funcional; (2) Cumple con las característica.							

ESTUDIO DE FACTIBILIDAD TÉCNICA.							
ESTEGANOGRAFÍA.							
Cuadro de evaluación. Se requiere un nivel de calificación del 75%							
Características Técnicas	Ponderación	OpenPuff 4.00		Steghide		My Lockbox	
		Valor	Total	Valor	Total	Valor	Total
Sistema Operativo: Windows, Linux.	20%	2	40.00%	2	40.00%	1	20.00%
Seguridad y la ofuscación.	20%	2	40.00%	2	40.00%	2	40.00%
Protección de carpetas.	10%	0	0.00%	0	0.00%	2	
Soporta imágenes (BMP, JPG, PCX, PNG, TGA).	10%	2	20.00%	2	20.00%	0	0.00%
Soporta audio (AIFF, MP3, NEXT / dom, WAV).	10%	2	20.00%	2	20.00%	0	0.00%
Soporta video (3GP, MP4, MPG, VOB).	10%	2	20.00%	0	0.00%	0	0.00%
Soporta Flash de Adobe (FLV, SWF, PDF).	10%	2	20.00%	0	0.00%	0	0.00%
Es portable.	10%	2	20.00%	0	0.00%	0	0.00%
Total	100.00%		180.00%		120.00%		60.00%
	% Final		90.00%		60.00%		30.00%
Análisis	Debido a que no genera costo y por la calificación obtenida en su evaluación tecnica se ha seleccionado el programa OpenPuff 4.00 para incluirse en el kit.						
Calificación: (0) Si no cumple con la característica; (1) Si cumple a medias pero sigue siendo funcional; (2) Cumple con las característica.							

1.7.3 Análisis General de Factibilidad.

Se detallarán los programas con sus características, precio (si no es licencia libre) y el porcentaje de aceptación por los cuales fueron seleccionados para formar parte del kit en informática forense.

Herramientas de disco.

Recuva: En la factibilidad económica fue seleccionado por no ocasionar ningún costo y en la factibilidad técnica cumplió con el porcentaje requerido para ser utilizado en el kit, por ese motivo fue seleccionado.

Características:

- Sistema Operativos: Windows OS.
- Recuperación de discos duros dañados o formateados.
- Recuperar archivos de una computadora.
- Recupera correos eliminados.
- Análisis en Profundidad.

Admite FAT12/16, FAT32, NTFS.

Porcentaje de aceptación: 77.50 %

Nota: Licencia libre.

Herramientas de red.

Wireshark: En el análisis de factibilidad económica fue seleccionado ya que no generá costo y en el análisis de factibilidad técnica cumplió con el porcentaje de aceptación. Fue seleccionado con base en el análisis de factibilidad técnica para formar parte del kit.

Características:

- Sistema Operativos: Windows OS.
- Analizar archivos PCAP.
- Velocidad de análisis PCAP.
- Directorio de salida de archivos configurable.

Porcentaje de aceptación: 85 %

Nota: Licencia libre.

Adquisición y análisis de memoria.

ForensicToolkitor (FTK Imager Lite Versión): Se incluirá en el kit por ser factible económicamente ya que no genera ningún costo y por obtener uno de los mayores porcentajes de aceptación en la factibilidad técnica.

Características:

- Versión para Windows.
- Genera registro de auditoría e informes.
- Captura la memoria y permite analizarla.
- Convierte un proceso de la memoria a fichero.
- Incluyen: NTFS, CDFS, UDF, HFS, FAT 12/16/32 y Linux EXT2 & EXT3.

Porcentaje de aceptación: 85 %

Nota: Licencia libre.

Análisis de registro de Windows.

RegRipper: Se incluirá en el kit por ser factible económicamente ya que no genera ningún costo y por obtener el mayor porcentaje de aceptación en la factibilidad técnica.

Características:

- Permite obtener de forma gráfica datos del sistema.
- Explorador del registro de seguridad.
- Abrir secciones de registro y analizarlas.
- Realizar la navegación, búsqueda, análisis y presentación de informes.
- Muestra todos los dispositivos configurados que funcionan en el equipo host.

Porcentaje de aceptación: 85 %

Nota: Licencia libre.

Criptografía.

AxCrypt v1.7.2850: seleccionado por características técnicas y su factibilidad económica ya que no genera ningún costo.

Características:

- Sistema Operativo: Windows.
- Encriptación de documentos.
- No requiere ninguna configuración de usuario necesario antes de su uso.
- Cifrado AES con claves de 128 bits.
- Opciones de modo de servidor.
- Soporte para archivos de más de 4GB (a excepción de los archivos libre descifrar).
- Se integra bien con los servicios de intercambio de archivos basado en web.

Porcentaje de aceptación: 90 %

Nota: Licencia libre.

Esteganografía.

OpenPuff 4.00: Seleccionado por su calificación en la factibilidad técnica y porque no genera ningún costo ya que es software de licencia libre.

Características:

- Sistema Operativo: Windows, Linux.
- Seguridad y la ofuscación.
- Soporta imágenes (BMP, JPG, PCX, PNG, TGA).
- Soporta audio (AIFF, MP3, NEXT / dom, WAV).
- Soporta video (3GP, MP4, MPG, VOB).
- Soporta Flash de Adobe (FLV, SWF, PDF). Es portable.

Porcentaje de aceptación: 90 %

Nota: Licencia libre.

1.8 Carta de Aprobación.

UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR

San Salvador, 30 de Marzo de 2014

Lic. Marvin Elenilson Hernández Montoya

UTEC

Presente.

Reciba un cordial saludo deseando muchos éxitos en sus labores cotidianos

El motivo de la presente es para solicitarle la aprobación para realizar nuestro proyecto de graduación con el tema: kit de herramientas de software en informática forense para ser utilizado en seminarios en el Laboratorio de Hardware de la Universidad Tecnológica de El Salvador, para realizarlo en el ciclo 01-2014

Confiando en obtener una respuesta positiva y sin otro particular, le expresamos nuestros más sinceros agradecimientos.

Firma y sello de aprobación:

Universidad Tecnológica
CÁTEDRA DE HARDWARE

F._____

Lic. Marvin Elenilson Hernández Montoya.

Capítulo II Documentación Técnica

2.1 Marco Teórico de Referencia.

2.1.1 Informática Forense.

La informática forense, también llamada cómputo forense, computación forense, análisis forense digital o exanimación forense digital es un campo dedicado a la investigación de delitos informáticos.

En 1978 Florida reconoce los crímenes de sistemas informáticos en el "ComputerCrimesAct", en casos de sabotaje, copyright, modificación de datos y ataques similares.(SYkRAYO, 2014)

Nace Copy II PC de Central Point Software en 1981. También es conocida como copy2pc, se usa para la copia exacta de disquetes, que generalmente están protegidos para evitar copias piratas. El producto será posteriormente integrado en las "Pc Tools". La compañía es un éxito y es comprada por Symantec en 1994. (SYkRAYO, 2014)

En 1982 Peter Norton publica UnErase: Norton Utilities 1.0, la primera versión del conjunto de herramientas "Norton Utilities", entre las que destacan UnErase, una aplicación que permite recuperar archivos borrados accidentalmente. Otras aplicaciones también serán útiles desde la perspectiva forense, como FileFix o TimeMark. Con el éxito de la suite de aplicaciones Peter publica varios libros técnicos, como Insidethe I. B. M. Personal Computer: Access toAdvancedFeatures and Programming, del que su

octava edición se publicó en 1999, 11 años después de la primera edición.. La compañía será vendida a Symantec en 1990. (SYkRAYO, 2014)

Objetivos de La Informática Forense.

La informática forense tiene 3 objetivos fundamentales que son:

- La persecución y procesamiento judicial de los delincuentes.
- La compensación de los daños causados por los criminales informáticos.
- La creación y aplicación de medidas para prevenir casos similares. (Hedrich, 2012)

Estudios que permite la Informática Forense.

Entre los estudios más conocidos que permite la informática forense están:

- Recuperación de evidencias en discos.
- Reconstrucción de eventos (Web-Internet).
- Acceso a archivos temporales y de caché.
- Recuperación de contraseñas y archivos encriptados.
- Detección y recuperación de Virus, Troyanos y Spyware.
- Detección de mensajes de esteganografía.
- Anonimato.
- Recuperación del Registro de Windows.

- Investigación de información. (Hedrich, 2012)

Usos de la Informática Forense.

Los usos en los cuales es requerida la informática forense se detallan a continuación:

- **Prosecución Criminal:** Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
- **Litigación Civil:** Casos que tratan con fraude, discriminación, acoso, proceso de divorcio, pueden ser ayudados por la informática forense.
- **Investigación de Seguros:** La evidencia encontrada en las computadoras, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
- **Temas corporativos:** Puede recolectarse la información en casos que tratan sobre acoso sexual, robo, apropiación de información confidencial o propietaria, de espionaje industrial.
- **Mantenimiento de la ley:** La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información.
- **Seguridad lógica:** virus, ataques de denegación de servicio, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidades, sustracción de cuentas de correo electrónico.

  (Estrada, 2009)

2.1.2 Evidencia Digital

El término evidencia ha sido en un principio asociado al de física dando como resultado el concepto de evidencia física, lo cual parece ser contrastante con el término evidencia digital, por cuanto, todo aquello relacionado con el término “digital” se ha asimilado al término “virtual”, es decir, que tiene existencia en el contexto de una simulación. Es importante aclarar que los datos o evidencia digital, siempre estarán almacenados en un soporte real, como lo son los medios de almacenamiento magnéticos o magneto ópticos u otros que se encuentran en fase de desarrollo, siendo todos estos de tipo físicos por lo que este tipo de evidencia es igualmente física.(informaticaforense, 2014)

Como prueba legal. Con el fin de garantizar su validez probatoria, los documentos deben cumplir con algunos requerimientos, estos son:

Autenticidad: satisfacer a una corte en que: los contenidos de la evidencia no han sido modificados; la información proviene de la fuente identificada; la información externa es precisa.

Precisión: debe ser posible relacionarla positivamente con el incidente. No debe haber ninguna duda sobre los procedimientos seguidos y las herramientas utilizadas para su recolección, manejo, análisis y posterior presentación en una corte. Adicionalmente, los procedimientos deben ser seguidos por alguien que pueda explicar, en términos “entendibles”, cómo fueron realizados y con qué tipo de herramientas se llevaron a cabo.

Características de la Evidencia Digital.

La evidencia digital es un tipo de la evidencia física, es menos tangible que otro tipo de evidencias, pero a diferencia de todas las demás evidencias físicas, ésta presenta ciertas ventajas, debido a que puede ser duplicada de una forma exacta, por lo que es posible peritar sobre copias, tal cual como si se tratará de la evidencia original, lo cual permite realizar diversos tipos de análisis y pruebas sin correr el riesgo de alterar o dañar la evidencia original.

En contraposición a lo que se piensa, es relativamente fácil determinar si una evidencia digital ha sido modificada o alterada a través de la comparación con su original o bien con el análisis de sus metadatos.

La evidencia digital no puede ser destruida fácilmente, tal como piensan los usuarios de computadoras, que creen que con ejecutar un comando de borrado (delete), ya ha desaparecido un documento o archivo objeto del mismo de la máquina. El disco duro de un sistema informático, guarda los datos en sectores creados en el momento del formateo del mismo, lo cual equivale a cuadricular una hoja de papel para insertar números y hacer operaciones matemáticas. Es posible que al guardar un archivo se necesiten varios sectores del disco. (González, Noviembre 2012)

Los sistemas operativos y hardware o parte física de la computadora, trabajan en conjunto en la ubicación de los archivos y programas para su visualización o ejecución, siendo los responsables específicos del acceso a los archivos, otros archivos denominados Meta.

Archivos con funciones de índice, contienen la información necesaria para abrir o visualizar rápidamente datos específicos en el disco duro. Lo que hace la ejecución del comando de borrado en la mayoría de los sistemas operativos es una eliminación de datos ubicado en el archivo índice del disco duro sin borrar real y físicamente el archivo en si, por lo que el archivo objeto de la instrucción de borrado queda en el disco duro sin que el usuario este consciente de ello. (Hedrich, 2012)

Fuentes de la Evidencia Digital.

A fin de que los investigadores forenses tengan una idea de dónde buscar evidencia digital, éstos deben identificar las fuentes más comunes de evidencia. Situación que brindará al investigador el método más adecuado para su posterior recolección y preservación.

Las fuentes de evidencia digital pueden ser clasificadas en tres grandes grupos:

Sistemas de computación abiertos, son aquellos que están compuestos de las llamadas computadoras personales y todos sus periféricos como teclados, mouse y monitores, las computadoras portátiles, y los servidores. Actualmente estas computadoras tiene la capacidad de guardar grandes cantidades de información dentro de sus discos duros.

Sistemas de comunicación, estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet.

Sistemas convergentes de computación, son los que están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, los asistentes personales digitales PDAs, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

Dada la ubicación de la evidencia digital es raro el delito que no esté asociado a un mensaje de datos guardado y trasmitido por medios informáticos. Un investigador entrenado puede usar el contenido de ese mensaje de datos para descubrir la conducta de un infractor, puede también hacer un perfil de su actuación, de sus actividades individuales y relacionarlas con sus víctimas.
(informaticaforense, 2014)

2.1.3 Delitos Informáticos

El delito informático implica cualquier actividad ilegal que se pueden enmarcar dentro de las figuras tradicionales ya conocidas como robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad.

Toda conducta típica, antijurídica y culpable que se vea facilitada o convertida en más daños o más lucrativa a causa de vulnerabilidades creadas o magnificadas por el uso creciente de los sistemas informáticos. En la delincuencia informática, la computadora puede fungir como objetivo de la acción dañosa, por ejemplo, en el sabotaje informático,

o bien como mero instrumento para la realización del hecho, por ejemplo, un fraude informático. (Hedrich, 2012)

Naturaleza del Delito Informático.

La naturaleza de los delitos informáticos se refiere específicamente a las actividades dirigidas a las computadoras con el fin hacer mal uso de ellas, a perturbar los sistemas de apoyo para robar, falsificar o destruir la información que almacenan.

Sin embargo, no es raro que la delincuencia informática, para referirse a un espectro más amplio de los actos que no sólo están destinados a las computadoras, muchas veces no se imaginan que puedan ocurrir situaciones como las siguientes:

El delincuente puede ser un empleado destituido que antes de salir de la empresa instala un código o bomba de tiempo, que más tarde desactiva las computadoras o envía un e - mail amenazando a los jefes de la empresa.

- Un empleado en una firma de abogados roba un juicio, con el fin de venderlo a otra firma de abogados.
- Los empleados de una agencia de hardware/software venden productos sin el consentimiento de la empresa quedando con la ganancia.
- Un estudiante descontento envía un e-mail amenazante, dando lugar a la clausura de su escuela.
- Alguien estafando sitios de subastas.
- Un sitio Web muestra documentos de identificación falsos.

- Numerosas personas venden tarjetas descodificadoras de televisión satelital provocando el tener servicio de cable en las casas sin pagar ningún costo a las empresas que proporcionan este servicio.
- Piratas de software utilizan un sitio en la Web para la distribución de software pirateado.
- Alguien vende software a través de sitios de subastas, alegando que es una copia legal, pero, de hecho, proporciona una copia pirata.
- Un hacker accede a los registros bancarios, roba datos personales, y utiliza estos para obtener el titular de la cuenta.
- El robo de espacio a servidores no protegidos, para intercambio de información o almacenar información considerada ilegal.

La naturaleza del crimen informático va desde la venganza, codicia, corrupción hasta la curiosidad de simple conveniencia pragmática, otros criminales se dirigen a la información almacenada en las computadoras, en otros casos, el delito no tiene persona en particular como un objetivo, los autores no hacen más daño del cual podrían hacer, solo el de almacenar archivos innecesarios o ciclos de procesamiento falsos. (Martínez, 2001)

La informática forense se utiliza para investigar casos como los crímenes que se perpetran, ahora se necesita que la evolución de las técnicas de la informática forense brinden respuestas de los hechos cometidos, la necesidad de enfoques han evolucionado

en respuesta para servir de evidencia y condenar acciones que atentan con los derechos de las personas.

Tipos de Delitos Informáticos.

Los delitos informáticos se definen dentro de tres categorías:

- La computadora puede ser el objetivo de un crimen como robarla, destruirla o utilizarla sin acceso autorizado. (Equipo informático usado como fin).
- La computadora puede ser la herramienta del crimen como en el caso del uso de Internet para enviar pornografía infantil, fraudes informáticos, amenazas y hostigamiento. (Equipo informático usado como medio).
- La computadora puede ser utilizada para almacenar evidencia de un delito como transacciones por lavado de dinero, narcotráfico o registros sensibles apropiados ilícitamente. (Equipo informático usado como método).

  (Hedrich, 2012)

Informática forense en dispositivos móviles.

Debido a su portabilidad los dispositivos móviles se han convertido en el medio de comunicación por excelencia, por la gran variedad de modelos, aplicaciones y características con las que estos cuentan, pero, la tecnología no es buena ni mala, sino que depende del uso que se le dé, por eso los mismos avances de estos dispositivos móviles pueden ser utilizados para cometer delitos informáticos tales como: intercepción

de mensajes en transacciones bancarias, la clonación de las simcard, narcotráfico, intercambio de imágenes de pedofilia, extorsiones y robos de información personal.

2.1.4 Perito Informático

Es la persona que tiene conocimientos en informática, cuyos servicios son utilizados por el juez para que lo ilustre en el esclarecimiento de un hecho que requiere los conocimientos especiales, científicos y técnicos relacionados a la informática.

Es el que posee conocimientos teóricos y prácticos en informática, informa bajo juramento al juez sobre puntos litigiosos en cuanto se relacionan con su especial saber o experiencia en el campo de la informática. (Estrada, 2009)

Peritaje

Es el examen y estudio que realiza el perito informático sobre el problema encomendado para luego entregar su informe o dictamen pericial a las autoridades que lo solicitan.

Este será la definición que se manejará y entenderá por peritaje a lo largo del presente estudio.

Pruebas Periciales

La prueba pericial es la que surge del dictamen de los peritos, que son personas llamadas a informar ante el juez, debido a sus conocimientos especiales y siempre que sea

necesario tal dictamen científico, técnico o práctico sobre hechos litigiosos.(Estrada, 2009)

2.1.5 Esteganografía.

La esteganografía (del griego στεγανος (steganos): cubierto u oculto, y γραφος (graphos): escritura), (wikipedia) está enmarcada en el área de seguridad informática, trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es decir, se trata de ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal.

Para que pueda hablarse de esteganografía debe haber voluntad de comunicación encubierta entre el emisor y el receptor.

Funcionamiento y terminología

La idea que sigue la esteganografía es enviar el mensaje oculto (E) "escondido" en un mensaje de apariencia inocua (C) que servirá de "camuflaje". Esto es, se aplica una función de esteganografía \ f(E). El resultado de aplicar la función (O), se envía por un canal inseguro y puede ser visto sin problemas por el guardián. Finalmente, el otro prisionero recibe el objeto O y, aplicando la función inversa f^{-1}(O), puede recupera el mensaje oculto.

Una descripción de la terminología típica usada en la esteganografía:

- Se define como **esquema esteganográfico** como el conjunto de componentes que permite llevar a cabo la comunicación esteganográfica.
- El portador es todo aquel conjunto de datos que es susceptible de ser alterado para incorporarle el mensaje que se va mantener en secreto. Puede ser de muchos tipos o formatos. Ejemplos: imagen (en sus distintos formatos), audio (en sus distintos formatos), texto plano, archivos binarios, un mensaje de protocolo de comunicación.
- Se llama mensaje-legítimo para referirse al mensaje transportado por el portador.
- Se llama mensaje esteganográfico al mensaje que se quiere mantener en secreto y queremos esconder dentro del portador. Puede ser de distintos tipos o formatos. Ejemplos: imagen (en sus distintos formatos), audio (en sus distintos formatos), texto plano, archivos binarios.
- Estego-algoritmo es el algoritmo esteganográfico que indica cómo realizar el procedimiento de incorporación del mensaje que se va a mantener en secreto en el portador.
- La acción de ocultar el mensaje dentro del portador se denomina embeber.
- Se llama estego-mensaje al resultado de embeber el mensaje esteganográfico dentro del portador.
- La acción de la recuperación, a partir del estego-mensaje, del mensaje oculto esteganográfico se denomina extraer.

La capacidad de alterar el portador de manera imperceptible es posible gracias a la existencia de redundancia en el mismo. Las alteraciones pueden realizarse tanto en el contenido como en otros parámetros como por ejemplo el tiempo de respuesta en la emisión del portador.(Zone-H, 2006)

Técnicas más utilizadas según el tipo de medio.

En documentos

El uso de esteganografía en los documentos puede funcionar con sólo añadir un espacio en blanco y las fichas a los extremos de las líneas de un documento. Este tipo de esteganografía es extremadamente eficaz, ya que el uso de los espacios en blanco y tabs no es visible para el ojo humano, al menos en la mayoría de los editores de texto, y se producen de forma natural en los documentos, por lo que en general es muy difícil que levante sospechas.(Zone-H, 2006)

En imágenes

El método más utilizado es el LSB, puesto que para un computador un archivo de imagen es simplemente un archivo que muestra diferentes colores e intensidades de luz en diferentes áreas (pixels). El formato de imagen más apropiado para ocultar información es el BMP color de 24 bit Bitmap), debido a que es el de mayor proporción (imagen no comprimida) y normalmente es de la más alta calidad. Eventualmente se prefiere optar por formatos BMP de 8 bits o bien otros tales como el GIF, por ser de

menor tamaño. Se debe tener en cuenta que el transporte de imágenes grandes por Internet puede despertar sospechas.

Cuando una imagen es de alta calidad y resolución, es más fácil y eficiente ocultar y enmascarar la información dentro de ella.

La desventaja del método LSB es que el el más conocido y popular, por tanto el más estudiado. Deja marcas similares a ruido blanco en el portador (imagen contenedora), lo cual la convierte en altamente detectable o vulnerable a ataques de estegoanálisis, para evitarlo se recurre a dispersar el mensaje, en general usando secuencias aleatorias.

Es importante notar que si se oculta información dentro de un archivo de imagen y este es convertido a otro formato, lo más probable es que la información oculta dentro sea dañada y, consecuentemente, resulte irrecuperable.

En audio

Cuando se oculta información dentro de archivos de audio, por lo general la técnica usada es low bit encoding (baja bit de codificación), que es similar a la LSB que suele emplearse en las imágenes. El problema con el low bit encoding es que en general es perceptible para el oído humano, por lo que es más bien un método arriesgado que alguien lo use si están tratando de ocultar información dentro de un archivo de audio.

Spread Spectrum también sirve para ocultar información dentro de un archivo de audio. Funciona mediante la adición de ruidos al azar a la señal de que la información se oculta dentro de una compañía aérea y la propagación en todo el espectro de frecuencias.

Otro método es Echo data hiding, que usa los ecos en archivos de sonido con el fin de tratar de ocultar la información. Simplemente añadiendo extra de sonido a un eco dentro de un archivo de audio, la información puede ser ocultada. Lo que este método consigue mejor que otros, es que puede mejorar realmente el sonido del audio dentro de un archivo de audio.

En vídeo

En vídeo, suele utilizarse el método DCT (DiscreteCosineTransform). DCT funciona cambiando ligeramente cada una de las imágenes en el vídeo, sólo de manera que no sea perceptible por el ojo humano. Para ser más precisos acerca de cómo funciona DCT, DCT altera los valores de ciertas partes de las imágenes, por lo general las redondea. Por ejemplo, si parte de una imagen tiene un valor de 6,667, lo aproxima hasta 7.

Esteganografía en vídeo es similar a la aplicada en las imágenes, además de que la información está oculta en cada fotograma de vídeo. Cuando sólo una pequeña cantidad de información que está oculta dentro del código fuente por lo general no es perceptible a todos. Sin embargo, cuanta mayor información se oculte, más perceptible será.

En archivos de cualquier tipo

Uno de los métodos más fáciles de implementar es el de inyección o agregado de bytes al final del archivo. Esta técnica consiste, esencialmente, en agregar o adosar al final de un archivo, de cualquier tipo, otro archivo que será el contenedor del "mensaje a

ocultar", también de cualquier tipo. Esta metodología es la más versátil, pues permite usar cualquier tipo de archivo como portador (documentos, imágenes, audio, vídeos, ejecutables, etc) y añadir al final del archivo contenedor el "paquete enviado", que es otro archivo, también de cualquier tipo.

Esta es una técnica que no se vale de las limitaciones humanas (vista y oído) para implementar la estrategia esteganográfica, sino que se vale de la forma de funcionamiento de las aplicaciones software que utilizan el portador. No degradan el contenido del portador de ninguna forma, por ejemplo, si es una imagen, permanecerá intacta; ya que el "mensaje" se le inyecta o adosa al final de la misma y la aplicación usada para visualizarla la mostrará normalmente hasta donde ella finalice. Esto es debido que todo tipo de archivo, en su cabecera, entre otros, contiene ciertos bytes fijos (en cantidad y ubicación) usados exclusivamente para indicar el tamaño del archivo. La aplicación que utilice un archivo, de cualquier tipo, siempre lee su cabecera primero, adquiere ese valor como su tamaño (en cantidad de bytes) y seguidamente lee el resto del archivo hasta el final indicado por dicho valor. De modo que si se coloca algo (mensaje) más allá del valor de ese parámetro, no será leído por la aplicación normal, por tanto no detectado, y el archivo portador funcionará normalmente.

Si bien es la técnica más sencilla de implementar, y de uso muy difundido, tiene la gran desventaja que provoca crecimiento del portador, tanto como el tamaño de su mensaje, siendo por tanto una estrategia fácilmente detectable. Un sencillo programa de estegoanálisis lo detecta por la sola lectura de su cabecera y la comprobación del tamaño

real de archivo portador; incluso cualquier usuario desconfiado puede muchas veces sospechar del portador por su tamaño ocupado en disco en relación a su contenido. Otra desventaja, aunque muy relativa y eventual, es que el crecimiento del portador podría ser limitante a la hora de trasferirlo por las redes, particularmente por Internet.

Los programas o software que utilizan esta técnica son llamados joiners, básicamente unen dos archivos, el portador y el de mensaje, manteniendo el valor inicial del tamaño en bytes indicado en la cabecera del primero. Esta es una técnica no utilizada si se pretende obtener características de indetectabilidad.

Si no se requiere reunir requisitos de indetectabilidad, es uno de los métodos preferidos por su sencillez, flexibilidad y escasas limitaciones. Prácticamente cualquier tipo de portador es admitido, con o sin compresión, incluso módulos ejecutables. En algunos casos provoca corrupción del portador, lo cual no es gran problema: practicada la técnica e inyectado el mensaje se prueba el portador con su aplicación correspondiente, si se ha degradado y/o no funciona bien, sencillamente toma otro, del mismo u otro tipo y se repite la operación.

Otros

Una nueva técnica esteganográfica implica el inyectar retardos (conocidos por su traducción al inglés como "delays") imperceptibles a los paquetes enviados sobre la red

desde el teclado. Los retardos en el tecleo de los comandos en algunos usos (telnet o software de escritorio remoto) pueden significar un retardo en paquetes, y los retardos en los paquetes se pueden utilizar para codificar datos.(Zone-H, 2006)

2.1.6 Criptografía

Criptografía (del griego κρύπτω krypto, «oculto», y γράφωςgraphos, «escribir», literalmente «escritura oculta») (wikipedia) tradicionalmente se ha definido como la parte de la criptología que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes. Por tanto el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes. Para ello se diseñaban sistemas de cifrado y códigos. En esos tiempos la única criptografía que había era la llamada criptografía clásica.

La aparición de la Informática y el uso masivo de las comunicaciones digitales han producido un número creciente de problemas de seguridad. Las transacciones que se realizan a través de la red pueden ser interceptadas. La seguridad de esta información debe garantizarse. Este desafío ha generalizado los objetivos de la criptografía para ser la parte de la criptología que se encarga del estudio de los algoritmos, protocolos (se les llama protocolos criptográficos) y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

Para ello los criptógrafos investigan, desarrollan y aprovechan técnicas matemáticas que les sirven como herramientas para conseguir sus objetivos. Los grandes avances que se

han producido en el mundo de la criptografía han sido posibles gracias a los grandes avances que se han producido en el campo de las matemáticas y la informática.(Franco, López, & Riaño, 2001)

Objetivos de la criptografía.

La criptografía actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican. El objetivo de la criptografía es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad. Por tanto el tipo de propiedades de las que se ocupa la criptografía son por ejemplo:

- Confidencialidad. Es decir garantiza que la información está accesible únicamente a personal autorizado. Para conseguirlo utiliza códigos y técnicas de cifrado.
- Integridad. Es decir garantiza la corrección y completitud de la información. Para conseguirlo puede usar por ejemplo funciones hash criptográficas MDC, protocolos de compromiso de bit, o protocolos de notarización electrónica.
- Vinculación. Permite vincular un documento o transacción a una persona o un sistema de gestión criptográfico automatizado. Cuando se trata de una persona, se trata de asegurar su conformidad respecto a esta vinculación (contentcommitment) de forma que pueda entenderse que la vinculación gestionada incluye el entendimiento de sus implicaciones por la persona.

Antiguamente se utilizaba el término "No repudio" que está abandonándose, ya que implica conceptos jurídicos que la tecnología por sí sola no puede resolver. En relación con dicho término se entendía que se proporcionaba protección frente a que alguna de las entidades implicadas en la comunicación, para que no pudiera negar haber participado en toda o parte de la comunicación. Para conseguirlo se puede usar por ejemplo firma digital. En algunos contextos lo que se intenta es justo lo contrario: Poder negar que se ha intervenido en la comunicación. Por ejemplo cuando se usa un servicio de mensajería instantánea y no se quiere que se pueda demostrar esa comunicación. Para ello se usan técnicas como el cifrado negable.

- Autenticación. Es decir proporciona mecanismos que permiten verificar la identidad del comunicador. Para conseguirlo puede usar por ejemplo función hash criptográfica MAC o protocolo de conocimiento cero.
- Soluciones a problemas de la falta de simultaneidad en la telefirma digital de contratos. Para conseguirlo puede usar por ejemplo protocolos de transferencia inconsciente.

Un sistema criptográfico es seguro respecto a una tarea si un adversario con capacidades especiales no puede romper esa seguridad, es decir, el atacante no puede realizar esa tarea específica.(Franco, López, & Riaño, 2001)

La criptografía simétrica

Es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.(Simmons, (1992))

La criptografía asimétrica

Es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.(Simmons, (1992))

2.1.7 Herramientas Utilizadas En Informática Forense.

En lo referente a las herramientas para la informática forense, existe una gran variedad y dependen del objetivo para la cual van a ser utilizadas. Existen para la recolección de evidencia, para el monitoreo o control de computadoras, para el marcado de documentos y de hardware (dispositivos físicos para la recolección de evidencia). A continuación se muestran algunas por áreas.

ADQUISICIÓN Y ANÁLISIS DE LA MEMORIA

pdProccessDumper - Convierte un proceso de la memoria a fichero.

FTK Imager - Permite entre otras cosas adquirir la memoria.

DumpIt - Realiza volcados de memoria a fichero.

Responder CE - Captura la memoria y permite analizarla.

Volatility - Analiza procesos y extrae información util para el analista.

RedLine - Captura la memoria y permite analizarla. Dispone de entrono gráfico.

MONTAJE DE DISCOS

ImDisk - Controlador de disco virtual.

raw2vmdk - Utilidad en java que permite convertir raw/dd a .vmdk

FTK Imager - Comentada anteriormente, permite realizar montaje de discos.

LiveView - Utilidad en java que crea una máquina virtual de VMware partiendo de una imagen de disco.

MountImagePro- Permite montar imágenes de discos locales en Windows asignando una letra de unidad

CARVING Y HERRAMIENTAS DE DISCO

RecoverRS - Recupera urls de acceso a sitios web y ficheros. Realiza carving directamente desde una imágen de disco.

NTFS Recovery - Permite recuperar datos y discos aún habiendo formateado el disco.

Recuva - Utilidad para la recuperación de ficheros borrados.

Raid Reconstructor - Recuperar datos de un RAID roto, tanto en raid 5 o raid 0. Incluso si no conocemos los parámetros RAID.

CNWrecovery- Recupera sectores corruptos e incorpora utilidades de carving.

Restoration - Utilidad para la recuperación de ficheros borrados.

UTILIDADES PARA EL SISTEMA DE FICHEROS

analyzeMFT- David Kovar's utilidad en python que permite extraer la MFT

MFT Extractor- Otra utilidad para la extracción de la MFT

INDXParse - Herramienta para los indices y fichero $I30.

MFT Tools (mft2csv, LogFileParser, etc.)Conjunto de utilidades para el acceso a la MFT

ANÁLISIS DE MALWARE

PDF Tools de Didier Stevens.

PDFStreamDumper - Esta es una herramienta gratuita para el análisis PDFs maliciosos.

SWF Mastah - Programa en Python que extrae stream SWF de ficheros PDF.

Proccessexplorer - Muestra información de los procesos.

Captura BAT - Permite la monitorización de la actividad del sistema o de un ejecutable.

Regshot - Crea snapshots del registro pudiendo comparar los cambios entre ellos

Bintext - Extrae el formato ASCII de un ejecutable o fichero.

LordPE- Herramienta para editar ciertas partes de los ejecutables y volcado de memoria

FRAMEWORKS

PTK - Busca ficheros, genera hash, dispone de rainbowtables. Analiza datos de un disco ya montado.

Log2timeline - Es un marco para la creación automática de un super línea de tiempo.

Plaso- Evolución de Log2timeline. Framework para la creación automática de unsuper línea de tiempo.

OSForensics - Busca ficheros, genera hash, dispone de rainbowtables. Analiza datos de un disco ya montado.

DFF - Framework con entorno gráfico para el análisis.

SANS SIFT Workstation - Magnifico Appliance de SANS. Lo utilizo muy a menudo.

Autopsy - Muy completo. Reescrito en java totalmente para Windows. Muy útil.

ANÁLISIS DEL REGISTRO DE WINDOWS

RegRipper - Es una aplicación para la extracción, la correlación, y mostrar la información del registro.

WRR - Permite obtener de forma gráfica datos del sistema, usuarios y aplicaciones partiendo del registro.

ShellbagForensics Análisis de los shellbag de windows.

RegistryDecoder - Extrae y realiza correlación aun estando encendida la máquina datos del registro.

HERRAMIENTAS DE RED

WireShark- Herramienta para la captura y análisis de paquetes de red.

NetworkMiner- Herramienta forense para el descubrimiento de información de red.

Network ApplianceForensicToolkit - Conjunto de utilidades para la adquisición y análisis de la red.

Snort- Detector de intrusos. Permite la captura de paquetes y su análisis.

Splunk- Es el motor para los datos y logs que generan los dispositivos, puestos y servidores. Indexa y aprovecha los datos de las generados por todos los sistemas e infraestructura de IT: ya sea física, virtual o en la nube.

RECUPERACIÓN DE CONTRASEÑAS

Ntpwedit- Es un editor de contraseña para los sistemas basados en Windows NT (como Windows 2000, XP, Vista, 7 y 8), se puede cambiar o eliminar las contraseñas de cuentas de sistema local. No valido para Active Directory.

Ntpasswd - Es un editor de contraseña para los sistemas basados en Windows, permite iniciar la utilidad desde un CD-LIVE

pwdump7 - Vuelca los hash. Se ejecuta mediante la extracción de los binarios SAM.

SAMInside/ OphCrack / L0phtcrack- Hacen un volcado de los hash. Incluyen diccionarios para ataques por fuerza bruta.(Sánchez, 2011)

2.1.8 Network Forensics

Forensia en redes, es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los

protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Es la captura, almacenamiento y análisis de los eventos de una red, para descubrir el origen de un ataque o un posible incidente.(Martínez, 2001)

2.1.9 Ethical Hacking

Las computadoras en todo el mundo son susceptibles de ser atacadas por crackers o hackers capaces de comprometer los sistemas informáticos y robar información valiosa, o bien borrar una gran parte de ella. Esta situación hace imprescindible conocer si estos sistemas y redes de datos están protegidos de cualquier tipo de intrusiones.

Por tanto el objetivo fundamental del Ethical Hacking (hackeo ético) es explotar las vulnerabilidades existentes en el sistema de "interés" valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc. Con la intención de ganar acceso y "demostrar" que un sistema es vulnerable, esta información es de gran ayuda a las organizaciones al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados.

Dicho lo anterior, el servicio de Ethical Hacking consiste en la simulación de posibles escenarios donde se reproducen ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que:

"Para atrapar a un intruso, primero debes pensar como intruso"

Para garantizar la seguridad informática se requiere de un conjunto de sistemas, métodos y herramientas destinados a proteger la información, es aquí donde entran los servicios del Ethical Hacking, la cual es una disciplina de la seguridad informática que echa mano de una gran variedad de métodos para realizar sus pruebas, estos métodos incluyen tácticas de ingeniería social, uso de herramientas de hacking, uso de Metasploits que explotan vulnerabilidades conocidas, en fin son válidas todas las tácticas que conlleven a vulnerar la seguridad y entrar a las áreas críticas de las organizaciones.(Plata, 2010)

Ethical Hackers.

Los hackers éticos también conocidos como Pen-Tester, como su nombre lo dice, realizan "Pruebas de Penetración". Un hacker ético es un experto en computadoras y redes de datos, su función es atacar los sistemas de seguridad en nombre de sus dueños, con la intención de buscar y encontrar vulnerabilidades que un hacker malicioso podría explotar. Para probar los sistemas de seguridad, los Ethical Hackers (hackerséticos) utilizan los mismos métodos que sus homólogos, pero se limitan únicamente a reportarlos en lugar de sacar ventaja de ellos.

El Ethical Hacking también es conocido como penetrationtesting (pruebas de penetración) o intrusión testing (pruebas de intrusión). Los individuos que realizan estas actividades a veces son denominados "hackers de sombrero blanco", este término proviene de las antiguas películas del Oeste, en donde el "bueno" siempre llevaba un sombrero blanco y el "malo" un sombrero negro.

(Plata, 2010)

Tipos de Ethical Hacking

Las pruebas de penetración se enfocan principalmente en las siguientes perspectivas:

- **Pruebas de penetración con objetivo**: se buscan las vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización.
- **Pruebas de penetración sin objetivo**: consisten en examinar la totalidad de los componentes de los sistemas informáticos pertenecientes a la organización. Este tipo de pruebas suelen ser las más laboriosas.
- **Pruebas de penetración a ciegas**: en estas pruebas sólo se emplea la información pública disponible sobre la organización.
- **Pruebas de penetración informadas**: aquí se utiliza la información privada, otorgada por la organización acerca de sus sistemas informáticos. En este tipo de pruebas se trata de simular ataques realizados por individuos internos de la organización que tienen determinado acceso a información privilegiada.

- **Pruebas de penetración externas**: son realizas desde lugares externos a las instalaciones de la organización. Su objetivo es evaluar los mecanismos perimetrales de seguridad informática de la organización.
- **Pruebas de penetración internas**: son realizadas dentro de las instalaciones de la organización con el objetivo de evaluar las políticas y mecanismos internos de seguridad de la organización.

A su vez, cada tipo de pruebas descrito anteriormente se puede ubicar en dos modalidades dependiendo si el desarrollo de las pruebas es de conocimiento del personal informático o no.

Red Teaming: Es una prueba encubierta, es decir que sólo un grupo selecto de ejecutivos sabe de ella. En esta modalidad son válidas las técnicas de "Ingeniería Social" para obtener información que permita realizar ataque. Ésta obviamente es más real y evita se realicen cambios de última hora que hagan pensar que hay un mayor nivel de seguridad en la organización.

Blue Teaming: El personal de informática conoce sobre las pruebas. Esta modalidad se aplica cuando las medidas tomadas por el personal de seguridad de las organizaciones ante un evento considerado como incidente, repercuten en la continuidad de las operaciones críticas de la organización, por ello es conveniente alertar al personal para evitar situaciones de pánico y fallas en la continuidad del negocio. (Plata, 2010)

2.2 Marco Teórico de la Solución.

En este apartado se presentan los productos que se entregaran en el proyecto:

- Ficha técnica de cada uno de los programas seleccionados.
- Manuales de los programas seleccionados en los estudios de factibilidad económica y técnica.
- Material de Apoyo, con conceptos básicos sobre informática forense.
- Diseño de Portada, interfaz del DVD que contendrá el kit.

2.2.1 Ficha Técnica.

Ficha técnica herramientas de disco: Recuva.

- Tamaño de fichero: 4.02MB.
- Requisitos: Windows 2000 / XP / Vista / Windows7 / XP64 / Vista64 / Windows7 64 / Windows8 / Windows8 64.
- Freeware (Licencia libre).

Ficha técnica herramientas de red: Wireshark.

Microsoft Windows

- Windows XP Home, XP Pro, XP Tablet PC, XP Media Center, Server 2003, Vista, 2008, 7, or 2008 R2 .
- Cualquier modern 32-bit x86 or 64-bit, procesador AMD64/x86-64.

- 128 MB de RAM disponible. Archivos de captura más grandes requieren más memoria RAM.
- 75 MB de espacio disponible en disco. Captura de archivos requieren espacio adicional en disco.
- 800*600 (1280*1024 o mayor) resolución con al menos 65.536 colores (16 bits) (256 colores deben funcionar si Wireshark se instala con la selección "GTK1 legado" de los lanzamientos 1.0.x Wireshark)..
- Una tarjeta de red con soporte para captura:

  - Ethernet:Cualquier tarjeta compatible con Windows debería funcionar. Vea las páginas wiki en la captura de Ethernet y la descarga de las cuestiones que puedan afectar a su entorno.
  - 802.11: Consulte la página wiki Wireshark. La captura de información raw 802.11 puede ser difícil sin equipo especial.
  - Otros: See http://wiki.wireshark.org/CaptureSetup/NetworkMedia

Observaciones:

- Muchas versiones más antiguas de Windows ya no se admiten por tres razones: Ninguno de los desarrolladores utilizan los sistemas antiguos porque se hace difícil dar soporte. Las bibliotecas Wireshark depende de (GTK, WinPcap) han abandonado el soporte para versiones anteriores. Microsoft también ha abandonado el soporte para estos sistemas.

- Windows 95, 98 y ME ya no se admiten. La "tecnología antigua" versiones de Windows no tienen protección de memoria (en concreto VirtualProtect) que utilizamos para mejorar la seguridad y la seguridad del programa. La última versión conocida de trabajo era 0.10.14 Ethereal (que incluye WinPcap 3.1). Usted lo puede obtener de http://ethereal.com/download.html. De acuerdo con este informe de error, es posible que tenga que instalar 0.10.0 Ethereal en algunos sistemas.
- Microsoft retiró el soporte para Windows 98 y ME en 2006.
- Windows NT 4.0 ya no funciona con Wireshark. La última versión conocida de trabajo fue Wireshark 0.99.4 (que incluye WinPcap 3.1). Usted todavía puede obtener de http://www.wireshark.org/download/win32/all-versions/wireshark-setup-0.99.4.exe.
- Microsoft retiró el soporte para Windows NT 4.0 en 2004.
- Windows 2000 ya no funciona con Wireshark. La última versión conocida de trabajo fue Wireshark 1.2.x (que incluye WinPcap 4.1.2). Usted todavía puede obtener de http://www.wireshark.org/download/win32/all-versions/.
- Microsoft retiró el soporte para Windows 2000 en 2010.
- Windows CE y las versiones incrustadas de Windows ya no son tienen soporte.
- Múltiples configuraciones de monitores están soportados, pero pueden tener un comportamiento un poco extraño.

Unix / Linux

- Wireshark actualmente se ejecuta en la mayoría de las plataformas UNIX. Los requisitos del sistema deben ser comparables a los valores de Windows mencionadas anteriormente.
- Los paquetes binarios están disponibles para, al menos, las siguientes plataformas:
    - Apple Mac OS X
    - Debian GNU/Linux
    - FreeBSD
    - Gentoo Linux
    - HP-UX
    - Mandriva Linux
    - NetBSD
    - OpenPKG
    - Red Hat Enterprise/Fedora Linux
    - rPath Linux
    - Sun Solaris/i386
    - Sun Solaris/Sparc
    - Canonical Ubuntu

Si un paquete binario no está disponible para su plataforma, usted debe descargar el código fuente y tratar de construirlo. Por favor, informe a sus experiencias para Wireshark-dev [AT] wireshark.org.

Ficha técnica criptografía: FTK Imager Lite Version

- Sistema operativo: Windows.
- Ejecutable desde disco local o extraíbles.
- No necesita instalarse.
- Peso: 24.10 MB

Ficha técnica criptografía: RegRipper

- Sistema operativo: Windows.
- Spyware / adware-libre.
- Completamente redistribuible.
- Portatil.
- Peso: 4.06 MB

Ficha técnica criptografía: AxCrypt v1.7.2850

- Está diseñado para funcionar en Windows 2003/XP/Vista/2008/7/8.
- Las versiones más antiguas funcionaban con Windows 95, 98 y ME, NT y 2000, pero desde que Microsoft ha caído todo el apoyo para él y AxCrypt requiere características de Windows XP y superior, AxCrypt también abandonado el soporte para estas versiones para el año 2008.
- Versión 1.7.2126 es la última versión compatible con Windows 2000.Versión 1.6.3 es la última versión compatible con 98/ME/NT.

Ficha técnica esteganografía: OpenPuffv4.00

- Sistema operativo: Windows, Linux.
- Spyware / adware-libre.
- Completamente redistribuible.
- OpenSource núcleo cripto-biblioteca (libObfuscate).
- Portatil.
- Peso: 8.75 MB

2.2.2 Manual de Uso.

Manual de uso herramientas de disco: Recuva.

Para la instalación del programa, el asistente del mismo proporciona al usuario una guía simple de instalación, por tal motivo el proceso de instalación no se detallará.

1. Para ejecutar el programa debe darse doble click sobre el icono creado en el escritorio, aparecerá la ventana de asistente de Recuva, click en siguiente.
2. En la siguiente ventana debe seleccionarse el tipo de archivo que se desea recuperar (en caso que sea un tipo de archivo en específico) o seleccionamos recuperar todos los archivos, una vez seleccionado el tipo de archivo se debe dar click en siguiente.

Imagen 2.2.2.1

3. Ahora se debe seleccionar la ubicación donde estaban los archivos, como se puede observar en la imagen 2.2.2.2.Recuva puede recuperar de distintas ubicaciones, en caso que se desconozca la ubicación de los archivos, se debe seleccionar no estoy seguro, luego dar click en siguiente.

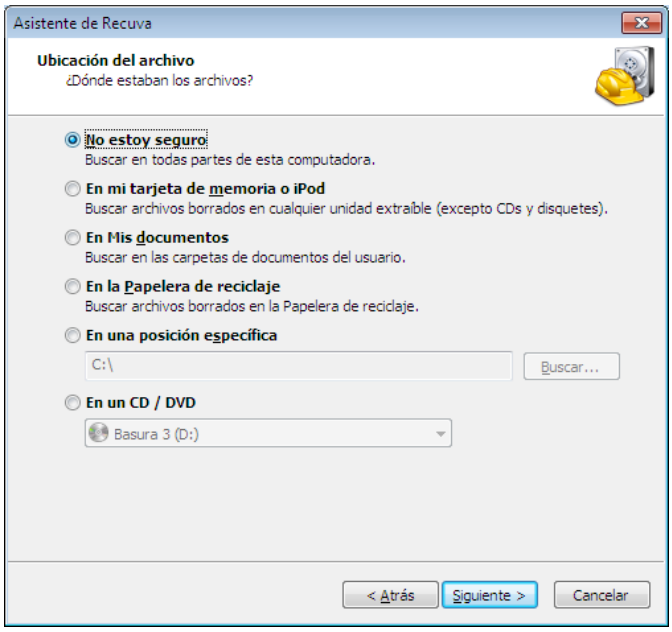


Imagen 2.2.2.2

4. En la siguiente ventana debe darse click en Iniciar, para iniciar el proceso de análisis para buscar archivos eliminados.
5. Una vez terminado el proceso, mostrara los resultados en una ventana, todos los archivos con un circulo de color verde son recuperables, los anaranjados son poco recuperables y los rojos irrecuperables (Imagen 2.2.2.3). Una vez seleccionado el o los archivos se debe dar click en recuperar, se debe indicar la ubicación de destino y dar clik en aceptar (2.2.2.4). Recordar que para una recuperación exitosa el archivo debe ser enviado a una unidad diferente de la que se realizo el proceso de recuperación.

Imagen 2.2.2.3

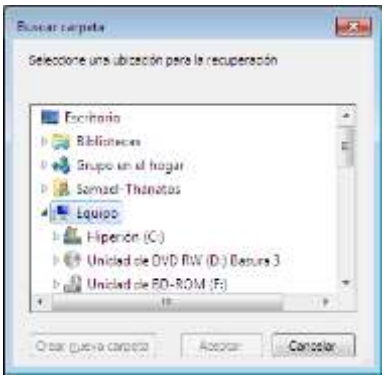


Imagen 2.2.2.4

6. Al finalizar el proceso deberá mostrar el mensaje en la imagen 2.2.2.5, luego se debe dar click en aceptar.

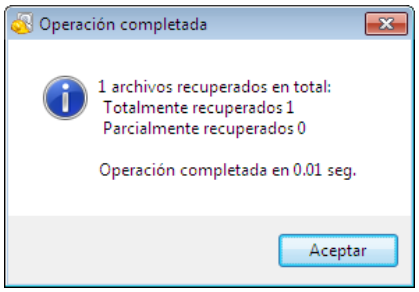


Imagen 2.2.2.5

Manual de uso herramientas de red: Wireshark

Para la instalación del programa, el asistente del mismo proporciona al usuario una guía simple de instalación, por tal motivo el proceso de instalación no se detallará.

1. Al iniciar Wireshark se mostrará su interfaz principal en la cual se debe seleccionar **Capture Options**.

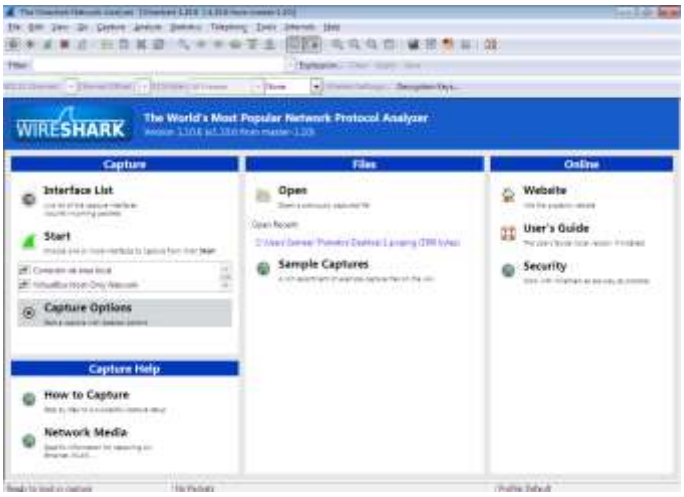


Imagen 2.2.2.6

2. En la venta siguiente se debe asegurar que la opción “Use promiscuousmodeonall interfaces”esta activa. En esta venta también se deben seleccionar las interfaces de la cuales de desea capturar paquetes. Una vez realizado lo anterior se procede a dar click en Star.

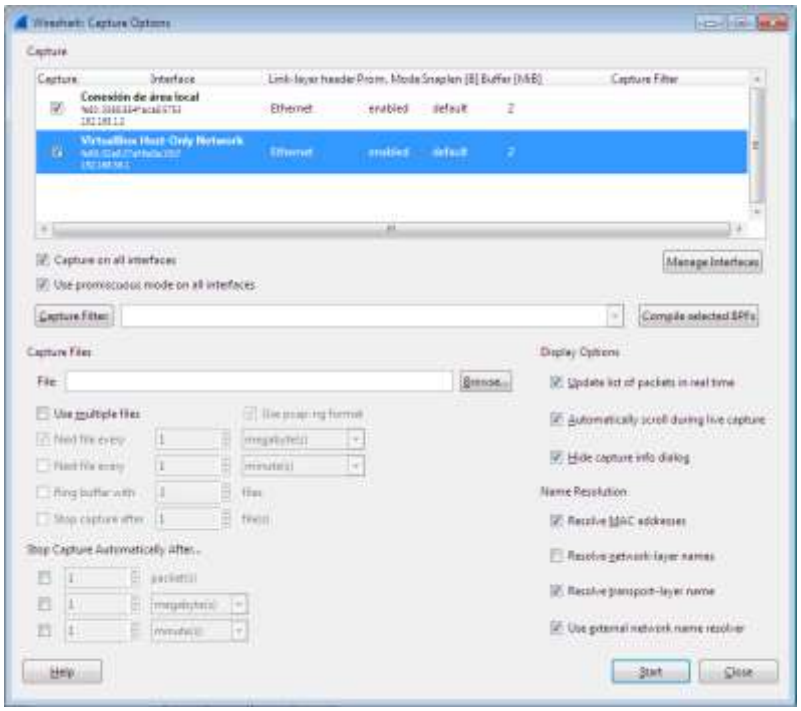


Imagen 2.2.2.7

3. En la siguiente venta se mostraran los paquetes capturados, con la información básica de estos paquetes como, número de paquete, tiempo entre paquetes, ip de origen, ip de destino, protocolo e información del paquete.

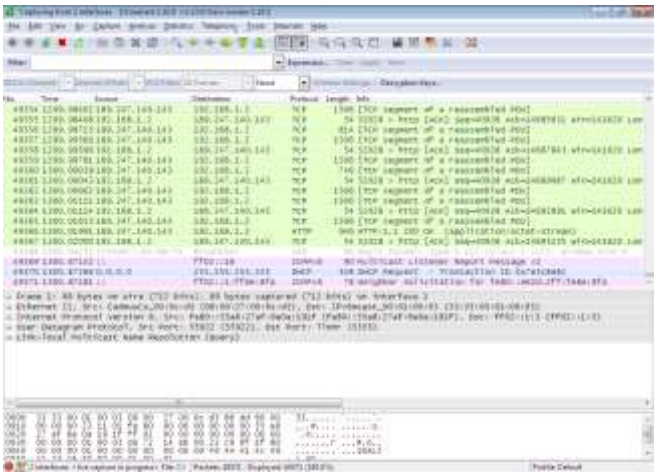


Imagen 2.2.2.8

4. Ahora se procede al análisis, se debe seleccionar el paquete a analizar y se podrá ver su información como se muestra en la imagen 2.2.2.9.

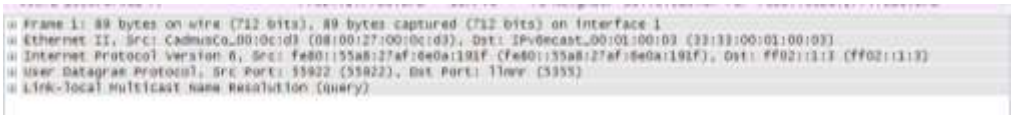


Imagen 2.2.2.9

Manual de uso análisis de memoria: FTK Imager Lite Version

Esta herramienta no necesita de instalación, solo se debe dar doble click izquierdo sobre el ejecutable.

Nota:FTK Imager Lite Versión, tiene otras funciones además de capturar y analizar la memoria ram, pero en este apartado solo se enfatizará en la captura y análisis de memoria.

1. Al iniciar FTK Imager se debe primero realizar la captura de la memoria RAM, para esto se debe ir al menú “File” opción “Capture Memory…”

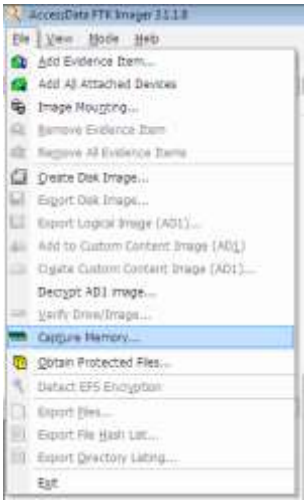


Imagen 2.2.2.10

2. En la siguiente ventana se debe seleccionar el directorio de destino de la imagen de captura de memoria, a continuación se debe dar click en “Capture Memory”.

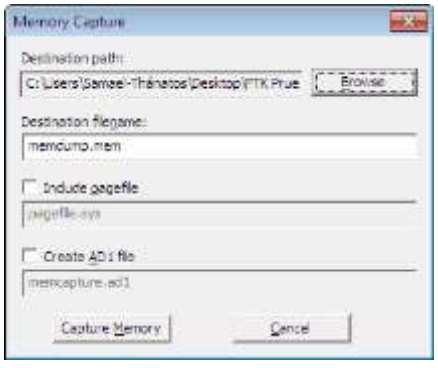


Imagen 2.2.2.11

3. Al completar la captura se debe dar click en “Close”.

Imagen 2.2.2.12

4. A continuación se procede a realizar el análisis de la captura, para ello se debe dar click en el menú “File” opción “ AddEvidenceItem…”

Imagen 2.2.2.13

5. En el siguiente recuadro se debe seleccionar “Image File” y dar click en “Siguiente”.

Imagen 2.2.2.14

6. En la siguiente ventana se debe seleccionar el archivo de imagen creado en el paso 2,a continuacion dar click en “Finish”

Imagen 2.2.2.15

7. Para el análisis se debe tener idea de lo que se está buscado para lo cual hacerclick derecho en los resultados mostrados y seleccionamos “Show Text Only”

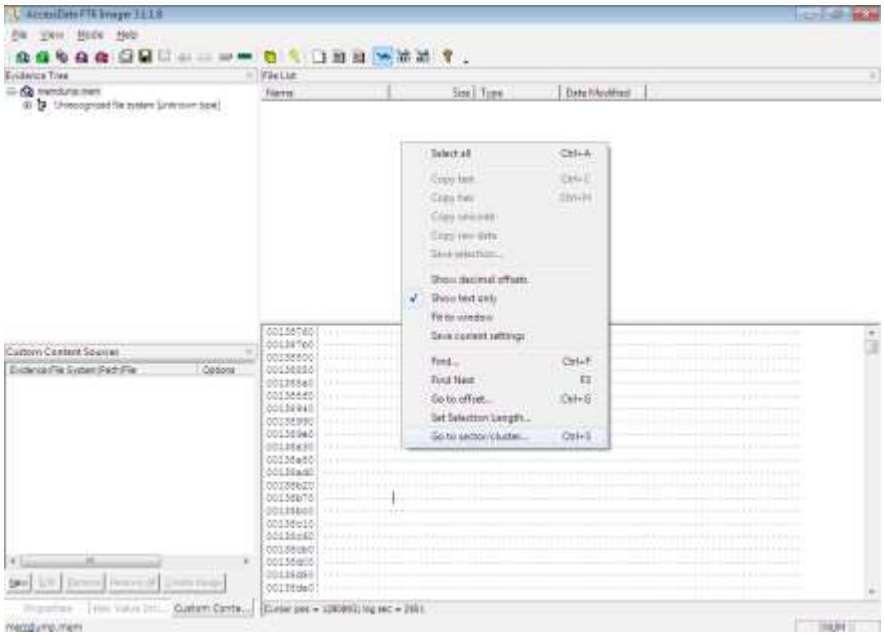


Imagen 2.2.2.16

8. Si se tiene el nombre de un archivo que desea encontrar que se ha utilizado o visto en la maquina a examinar, se procede a buscarlo presionando las teclas Ctrl + F y escribimos parte del nombre del archivo, para este ejemplo se escribirá parte del nombre del archivo en uso “Manual de uso, FTK Imager Lite Version”,.

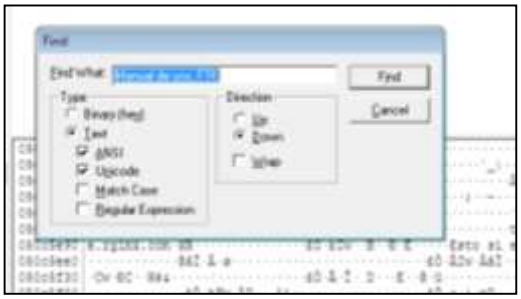


Imagen 2.2.2.17

9. Al dar click en “Find” buscara registros con ese nombre y los marcara en azul. De esta manera se puede analizar la memoria RAM en busca de evidencia.

Imagen 2.2.2.18

Manual de uso registro de Windows: RegRipper

Esta herramienta no necesita instalarse, solo se descarga el archivo de la pagina del fabricante se descomprime, y se ejecuta.

Este software puede analizar los registros NTUSER.DAT, SAM, SECURITY Y SOFTWARE. El proceso es el mismo para todos.

1. Se deben realizar copias de los registros ya mencionados.

2. Se ejecuta RegRipper. Al ejecutarlo se mostrará una venta donde se debe seleccionar la ruta donde se encuentra el registro a ser analizado (Hive File).

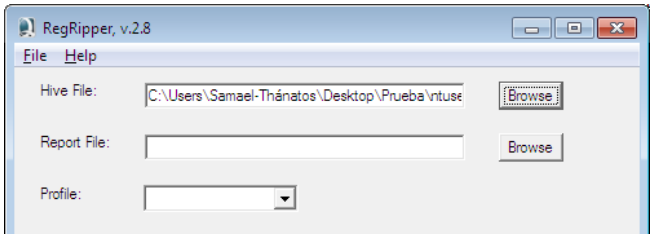


Imagen 2.2.2.19

3. A continuación se debe seleccionar el directorio donde se desea generar los reportes.

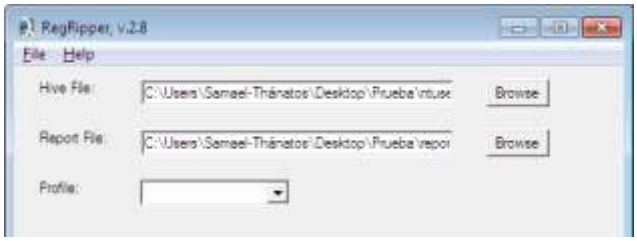


Imagen 2.2.2.20

4. En Profile, se debe seleccionar el tipo de registro a ser analizado; una vez realizado esto se debe dar click en Ripit.

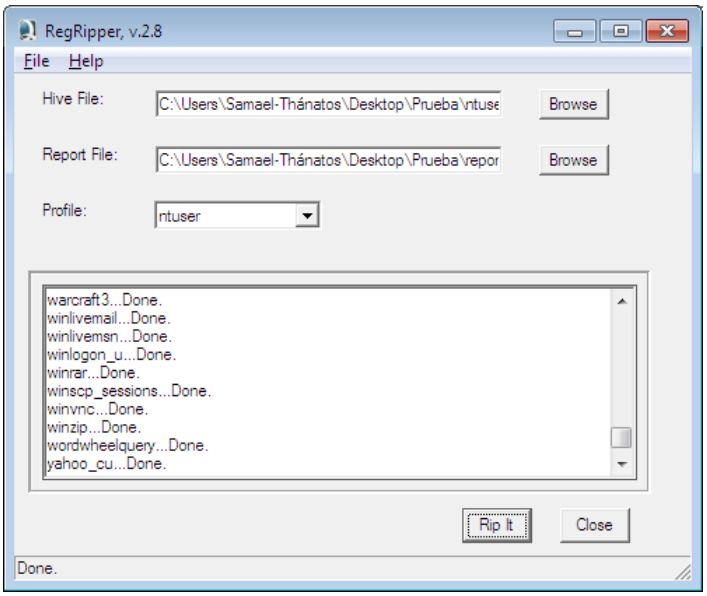


Imagen 2.2.2.21

5. Ahora solo de sebe revisar el directorio donde se enviaron los informes y se podrá visualizar la información obtenida.

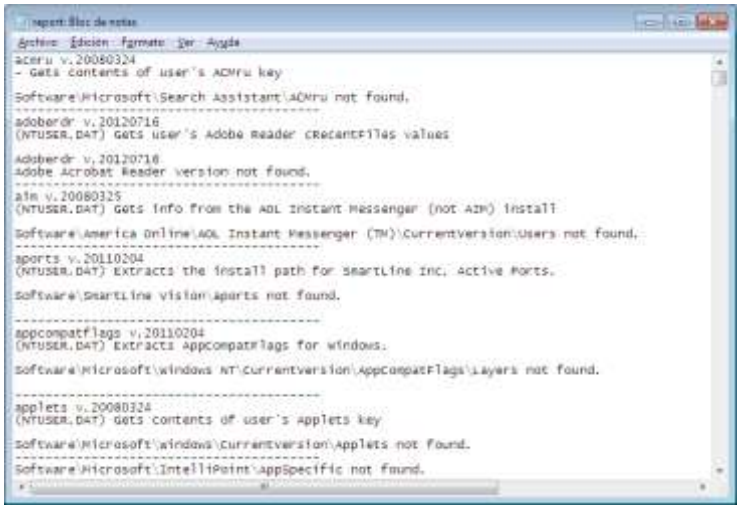


Imagen 2.2.2.22

Manual de uso criptografía: AxCrypt v1.7.2850

Para la instalación del programa, el asistente del mismo proporciona al usuario una guía simple de instalación, por tal motivo el proceso de instalación no se detallará.

Para encriptar o cifrar un archivo con contraseña:

1. Seleccionar el archivo a encriptar o cifrar, luego dar click derecho sobre el, en las opciones desplegadas seleccionar AxCryp y dar click en cifrar.

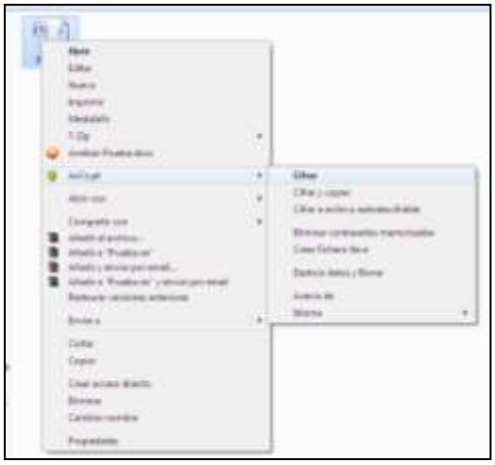


Imagen 2.2.2.23

2. En la ventana que aparece se debe digitar la contraseña, para la encriptación del archivo, a continuación dar click en aceptar, (se recomienda no seleccionar la casillas de “Recordar esta contraseña” y “Recordar y usar como contraseña por defecto”, esto para una mayor seguridad en el cifrado).

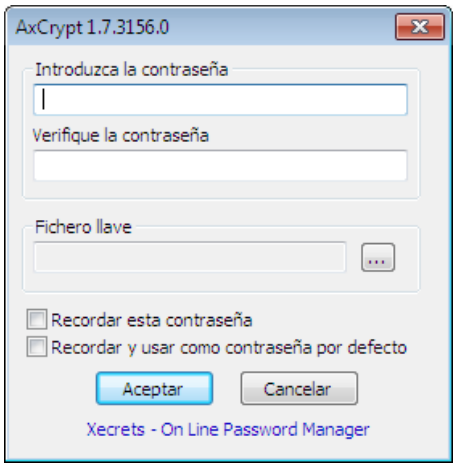


Imagen 2.2.2.24

3. Al finalizar el archivo deberá aparecer como se muestra en la imagen 2.2.2.25.

Imagen 2.2.2.25

4. Para descifrar el archivo, se debe repetir lo explicado en el numeral 1 de **encriptar o cifrar un archivo con contraseña**, luego digitar la contraseña y dar click en aceptar.

Para encriptar o cifrar un archivo con contraseña y fichero llave:

1. Seleccionar el archivo a encriptar o cifrar, luego dar click derecho sobre él, en las opciones desplegadas seleccionar AxCryp y dar click en crear fichero llave.

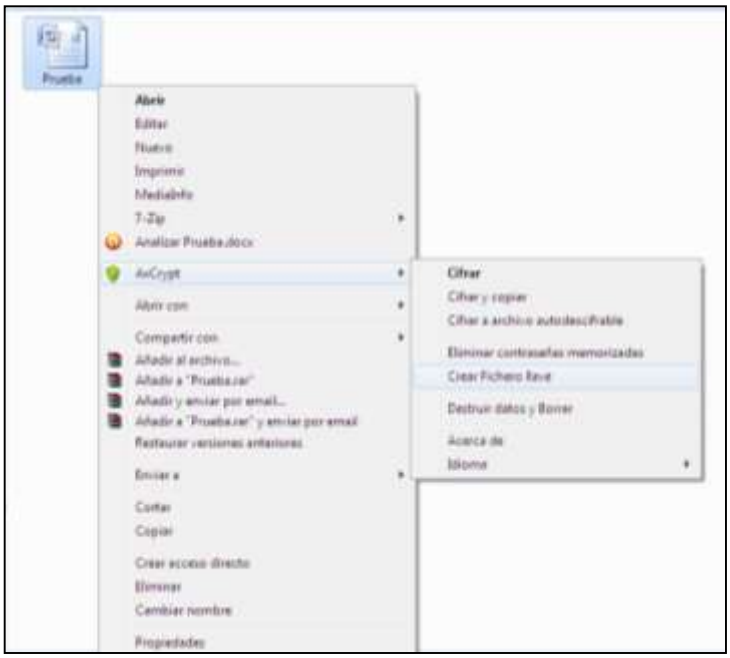


Imagen 2.2.2.26

2. A continuación se mostrará una ventana de advertencia en la cual se explicará que con el fichero llave la seguridad en los archivos protegidos será a un mayor, así como también el de guardar el fichero llave en una unidad extraíble USB, y tener el cuidado de no perderlo porque al perderlo no se podrá abrir el archivo protegido, al estar consiente de esto se debe proceder a dar click en aceptar.
3. Se pedirá una ubicación para crear el fichero llave, se debe seleccionar la ubicación deseada (Recordar guardarlo en una dispositivo extraíble USB).
4. Una vez creado el fichero llave, se procede a cifrar el archivo, para lo cual se debe dar click sobre el archivo, click en AxCryp y luego click en cifrar (ver Imagen 2.2.2.23).

5. En la ventana que aparecerá se debe escribir la contraseña y seleccionar la ruta donde se encuentra el fichero llave, luego proceder a dar click en aceptar, y click nuevamente en aceptar.

Imagen 2.2.2.27

6. Para descifrar el archivo, se debe repetir lo explicado en el numeral 1 de **encriptar o cifrar un archivo con contraseña y fichero llave**, luego digitar la contraseña, seleccionar el fichero llave y dar click en aceptar.

Manual de uso esteganografía: OpenPuffv4.00

Esta herramienta no necesita instalarse, solo se descarga el archivo de la pagina del fabricante se descomprime, y se ejecuta.

1. Una vez ejecutado el programa se realiza el proceso de ocultado de archivos, para eso se debe dar click sobre el botón Hide.

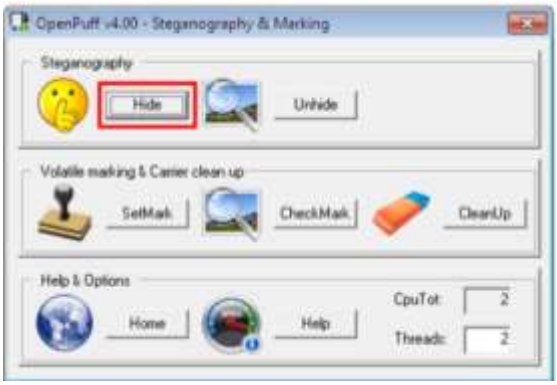


Imagen 2.2.2.28

1. Luego se deben digitar tres passwords diferentes uno de otros. Si no se desea digitar pueden deshabilitarse los password (B) y (C).

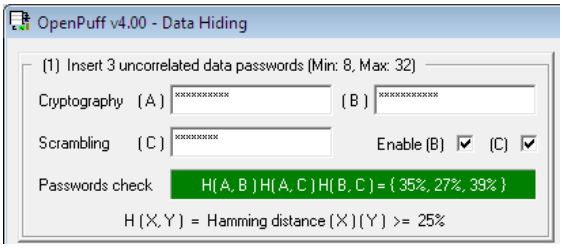


Imagen 2.2.2.29

2. A continuación se debe seleccionar el archivo a ocultar. El archivo no debe pesar más de 256 megabytes y se recomienda utilizar archivos zip o rar para ocultar más archivos.

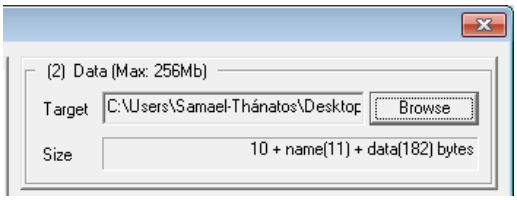


Imagen 2.2.2.30

3. En la siguiente parte se deben seleccionar los archivos transportadores donde se ocultaran los archivos seleccionados en el numeral 2. Debe tenerse en cuenta que el peso de los archivos transportadores debe superar al del archivo que se ocultará, como se puede observar en el recuadro verde de la imagen 2.2.2.31 (a la izquierda peso de archivos transportadores, a la derecha peso de archivo a ocultar).

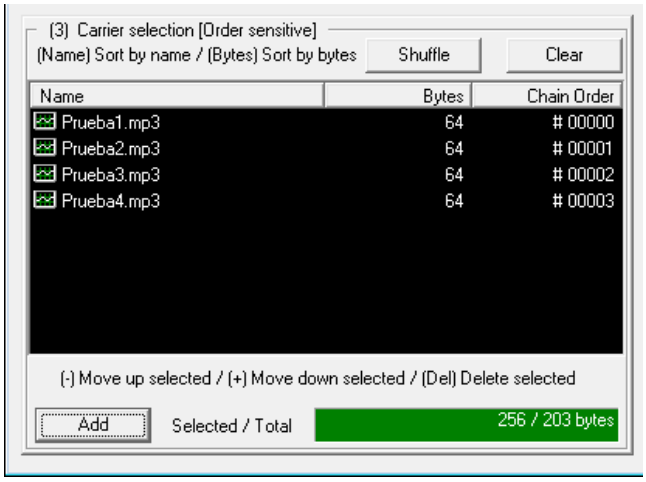


Imagen 2.2.2.31

4. En el siguiente recuadro se deberán seleccionar los tipos de bit, en este ejemplo se han utilizado archivos mp3, por lo tanto se debe seleccionar las opciones para Mp3 (audio), es recomendado dejar las opciones por defecto. Luego se presiona

Hide, seleccionar carpeta destino para archivos transportadores y dar click en aceptar.

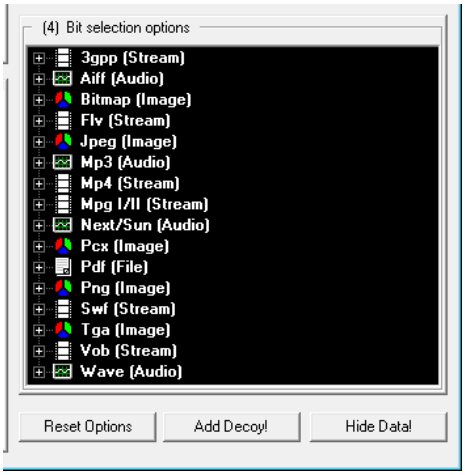


Imagen 2.2.2.32

5. Al final deberá mostrar el siguiente recuadro.

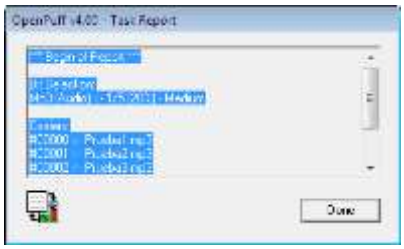


Imagen 2.2.2.33

6. Para mostrar los archivos ocultos se debe ejecutar la herramienta y presionar el botón Unhide.

Imagen 2.2.2.34

7. A continuación se deben digitar los passwords utilizados en el proceso de ocultado; también se deben seleccionar los archivos que se utilizaron como transporte en el orden que colocaron en el proceso de ocultado, así como el mismo tipo de selección de bit, (si esto no se realiza de esta forma no se podrá recuperar el archivo), se debe dar click en Unhide. (ver Imagen 2.2.2.35)

Imagen 2.2.2.35

2.2.3 Material de apoyo para los seminarios.

INFORMÁTICA FORENSE

Informática forense

Es el proceso de investigar dispositivos electrónicos o computadoras con el fin de descubrir, analizar y presentar información disponible, suprimida u ocultada que puede servir como evidencia en un asunto legal.

Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

Desde 1984, el Laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional.

Objetivos de La Informática Forense.

La informática forense tiene 3 objetivos fundamentales que son:

- La persecución y procesamiento judicial de los delincuentes.

- La compensación de los daños causados por los criminales informáticos.
- La creación y aplicación de medidas para prevenir casos similares.

Delitos informáticos.

1. El delito informático implica cualquier actividad ilegal que se pueden enmarcar dentro de las figuras tradicionales ya conocidas como robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad.

2. Toda conducta típica, antijurídica y culpable que se vea facilitada o convertida en más daños o más lucrativa a causa de vulnerabilidades creadas o magnificadas por el uso creciente de los sistemas informáticos. En la delincuencia informática, la computadora puede fungir como objetivo de la acción dañosa, por ejemplo, en el sabotaje informático, o bien como mero instrumento para la realización del hecho, por ejemplo, un fraude informático.

De acuerdo al avance de la tecnología han empezado a crearse junto con ella conductas ilícitas, a esto nos referimos con delitos informáticos. Desde un punto de vista legal un delito es un hecho antijurídico realizado por una persona, tipificado, culpable y sancionado por una pena. Existen diversos tipos de delitos y los siguientes están tipificados en el código penal Peruano:

•Delitos de Violación a la Intimidad, Pornografía infantil.

• Delito de Hurto agravado por Transferencia Electrónica de Fondos, telemática en general y empleo de claves secretas.

•Delito de Falsificación de Documentos Informáticos.

•Delito de suplantación de bienes informáticos (IP).

•Delito contra los derechos de autor de software, etc.

•Delito de Fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos.

Delincuente informático.

Es la persona o grupo de personas que en forma asociada realizan actividades ilegales haciendo uso de las computadoras y en agravio de terceros, en forma local o a través de Internet. Una de las prácticas más conocidas es la de interceptar compras "en línea" a través de Internet, para que haciendo uso del nombre, número de tarjeta de crédito y fecha de expiración, realizan compras de cualquier bien, mayormente software, o hasta hardware y para lo cual proporcionan una dirección de envío, diferente a la del titular del número de la tarjeta de crédito que usan en forma ilegal.

También es un delincuente informático el "pirata" que distribuye software sin contar con las licencias de uso proporcionadas por su autor o representantes, pues no solo atenta contra la propiedad intelectual, provocando la fuga de talentos informáticos, se enriquece ilícitamente y es un evasor de impuestos.

Legislación aplicada a los delitos informáticos en El Salvador.

En el salvador se reconoce los delitos informáticos solo en forma general:

- Ley anti terrorismoDELITO INFORMATICO Art. 12.
- CAPITULO III. Otros Ataques a La Libertad Sexual. Art. 172.- Art. 173
- CAPITULO II. De los delitos relativos a la intimidad violación de comunicaciones privadas. Art. 184.
- Violación agravada de Comunicaciones. Art. 185.
- CAPITULO V De Los Daños, Daños Agravados. Art. 222.- Art. 226
- Violación agravada a derecho de autor y derechos conexos (26). Art. 227.
- Violación a medidas tecnológicas efectivas (26) Art. 227-a.- Art. 227-b.-
- CAPITULO I. De los delitos relativos a la propiedad industrial, Infidelidad comercial. Art. 230.- Art. 231.-

Hacking ético.

Las computadoras en todo el mundo son susceptibles de ser atacadas por crackers o hackers capaces de comprometer los sistemas informáticos y robar información valiosa, o bien borrar una gran parte de ella. Esta situación hace imprescindible conocer si estos sistemas y redes de datos están protegidos de cualquier tipo de intrusiones.

Por tanto el objetivo fundamental del Ethical Hacking (hackeo ético) es explotar las vulnerabilidades existentes en el sistema de "interés" valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de

computadoras, aplicaciones web, bases de datos, servidores, etc. Con la intención de ganar acceso y "demostrar" que un sistema es vulnerable, esta información es de gran ayuda a las organizaciones al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados.

Evidencia Digital.

El término evidencia ha sido en un principio asociado al de física dando como resultado el concepto de evidencia física, lo cual parece ser contrastante con el término evidencia digital, por cuanto, todo aquello relacionado con el término “digital” se ha asimilado al término “virtual”, es decir, que tiene existencia en el contexto de una simulación. Es importante aclarar que los datos o evidencia digital, siempre estarán almacenados en un soporte real, como lo son los medios de almacenamiento magnéticos o magneto ópticos u otros que se encuentran en fase de desarrollo, siendo todos estos de tipo físicos por lo que este tipo de evidencia es igualmente física. (informaticaforense, 2014)

Como prueba legal. Con el fin de garantizar su validez probatoria, los documentos deben cumplir con algunos requerimientos, estos son:

Autenticidad: satisfacer a una corte en que: los contenidos de la evidencia no han sido modificados; la información proviene de la fuente identificada; la información externa es precisa.

Precisión: debe ser posible relacionarla positivamente con el incidente. No debe haber ninguna duda sobre los procedimientos seguidos y las herramientas utilizadas para su recolección, manejo, análisis y posterior presentación en una corte. Adicionalmente, los procedimientos deben ser seguidos por alguien que pueda explicar, en términos "entendibles", cómo fueron realizados y con qué tipo de herramientas se llevaron a cabo.

Características de la Evidencia Digital.

La evidencia digital es un tipo de la evidencia física, es menos tangible que otro tipo de evidencias, pero a diferencia de todas las demás evidencias físicas, ésta presenta ciertas

ventajas, debido a que puede ser duplicada de una forma exacta, por lo que es posible peritar sobre copias, tal cual como si se tratará de la evidencia original, lo cual permite realizar diversos tipos de análisis y pruebas sin correr el riesgo de alterar o dañar la evidencia original.

En contraposición a lo que se piensa, es relativamente fácil determinar si una evidencia digital ha sido modificada o alterada a través de la comparación con su original o bien con el análisis de sus metadatos.

La evidencia digital no puede ser destruida fácilmente, tal como piensan los usuarios de computadoras, que creen que con ejecutar un comando de borrado (delete), ya ha desaparecido un documento o archivo objeto del mismo de la máquina. El disco duro de un sistema informático, guarda los datos en sectores creados en el momento del

formateo del mismo, lo cual equivale a cuadricular una hoja de papel para insertar números y hacer operaciones matemáticas. Es posible que al guardar un archivo se necesiten varios sectores del disco.

Los sistemas operativos y hardware o parte física de la computadora, trabajan en conjunto en la ubicación de los archivos y programas para su visualización o ejecución, siendo los responsables específicos del acceso a los archivos, otros archivos denominados Meta.

Archivos con funciones de índice, contienen la información necesaria para abrir o visualizar rápidamente datos específicos en el disco duro. Lo que hace la ejecución del comando de borrado en la mayoría de los sistemas operativos es una eliminación de datos ubicado en el archivo índice del disco duro sin borrar real y físicamente el archivo en si, por lo que el archivo objeto de la instrucción de borrado queda en el disco duro sin que el usuario este consciente de ello.

Informática forense en dispositivos móviles.

Debido a su portabilidad los dispositivos móviles se han convertido en el medio de comunicación por excelencia, por la gran variedad de modelos, aplicaciones y características con las que estos cuentan, pero, la tecnología no es buena ni mala, sino que depende del uso que se le dé, por eso los mismos avances de estos dispositivos móviles pueden ser utilizados para cometer delitos informáticos tales como: intercepción de mensajes en transacciones bancarias, la clonación de las simcard, narcotráfico, intercambio de imágenes de pedofilia, extorsiones y robos de información personal.

Para el análisis de estos delitos existen herramientas de recuperación forense en telefonía móvil, de las cuales se presentan a continuación las principales:

- Bitpim
- Secureview ®
- DeviceSeizure ®
- Gsm .Xry ®
- Forensicsim ®
- Simcon ®
- Usimdetective ®
- Tulp2g
- Celldek ®
- Pilot-Link
- Simis2 ®
- ForensicCard Reader ®
- Phonebase2 ®
- OxygenPhone Manager ®, versión lite disponible.
- Mobiledit! (C), versión lite disponible.

Herramientas forenses.

- ADQUISICIÓN Y ANÁLISIS DE LA MEMORIA
- pdProccessDumper - Convierte un proceso de la memoria a fichero.
- FTK Imager - Permite entre otras cosas adquirir la memoria.
- DumpIt - Realiza volcados de memoria a fichero.
- Responder CE - Captura la memoria y permite analizarla.
- Volatility - Analiza procesos y extrae información util para el analista.
- RedLine - Captura la memoria y permite analizarla. Dispone de entrono gráfico.

MONTAJE DE DISCOS

ImDisk - Controlador de disco virtual.

raw2vmdk - Utilidad en java que permite convertir raw/dd a .vmdk

FTK Imager - Comentada anteriormente, permite realizar montaje de discos.

LiveView - Utilidad en java que crea una máquina virtual de VMware partiendo de una imagen de disco.

MountImagePro - Permite montar imágenes de discos locales en Windows asignando una letra de unidad

CARVING Y HERRAMIENTAS DE DISCO

RecoverRS - Recupera urls de acceso a sitios web y ficheros. Realiza carving directamente desde una imágen de disco.

NTFS Recovery - Permite recuperar datos y discos aún habiendo formateado el disco.

Recuva - Utilidad para la recuperación de ficheros borrados.

Raid Reconstructor - Recuperar datos de un RAID roto, tanto en raid 5 o raid 0. Incluso si no conocemos los parámetros RAID.

CNWrecovery - Recupera sectores corruptos e incorpora utilidades de carving.

Restoration - Utilidad para la recuperación de ficheros borrados.

UTILIDADES PARA EL SISTEMA DE FICHEROS

analyzeMFT - David Kovar's utilidad en python que permite extraer la MFT

MFT Extractor- Otra utilidad para la extracción de la MFT

INDXParse - Herramienta para los indices y fichero $I30.

MFT Tools (mft2csv, LogFileParser, etc.)Conjunto de utilidades para el acceso a la MFT

ANÁLISIS DE MALWARE

PDF Tools de Didier Stevens.

PDFStreamDumper - Esta es una herramienta gratuita para el análisis PDFs maliciosos.

SWF Mastah - Programa en Python que extrae stream SWF de ficheros PDF.

Proccessexplorer - Muestra información de los procesos.

Captura BAT - Permite la monitorización de la actividad del sistema o de un ejecutable.

Regshot - Crea snapshots del registro pudiendo comparar los cambios entre ellos

Bintext - Extrae el formato ASCII de un ejecutable o fichero.

LordPE - Herramienta para editar ciertas partes de los ejecutables y volcado de memoria

FRAMEWORKS

PTK - Busca ficheros, genera hash, dispone de rainbowtables. Analiza datos de un disco ya montado.

Log2timeline - Es un marco para la creación automática de un super línea de tiempo.

Plaso - Evolución de Log2timeline. Framework para la creación automática de unsuper línea de tiempo.

OSForensics - Busca ficheros, genera hash, dispone de rainbowtables. Analiza datos de un disco ya montado.

DFF - Framework con entorno gráfico para el análisis.

SANS SIFT Workstation - Magnifico Appliance de SANS. Lo utilizo muy a menudo.

Autopsy - Muy completo. Reescrito en java totalmente para Windows. Muy útil.

ANÁLISIS DEL REGISTRO DE WINDOWS

RegRipper - Es una aplicación para la extracción, la correlación, y mostrar la información del registro.

WRR - Permite obtener de forma gráfica datos del sistema, usuarios y aplicaciones partiendo del registro.

ShellbagForensics Análisis de los shellbag de windows.

RegistryDecoder - Extrae y realiza correlación aun estando encendida la máquina datos del registro.

HERRAMIENTAS DE RED

WireShark - Herramienta para la captura y análisis de paquetes de red.

NetworkMiner - Herramienta forense para el descubrimiento de información de red.

Network ApplianceForensicToolkit - Conjunto de utilidades para la adquisición y análisis de la red.

Snort - Detector de intrusos. Permite la captura de paquetes y su análisis.

Splunk - Es el motor para los datos y logs que generan los dispositivos, puestos y servidores. Indexa y aprovecha los datos de las generados por todos los sistemas e infraestructura de IT: ya sea física, virtual o en la nube.

RECUPERACIÓN DE CONTRASEÑAS

Ntpwedit - Es un editor de contraseña para los sistemas basados en Windows NT (como Windows 2000, XP, Vista, 7 y 8), se puede cambiar o eliminar las contraseñas de cuentas de sistema local. No valido para Active Directory.

Ntpasswd - Es un editor de contraseña para los sistemas basados en Windows, permite iniciar la utilidad desde un CD-LIVE

pwdump7 - Vuelca los hash. Se ejecuta mediante la extracción de los binarios SAM.

SAMInside / OphCrack / L0phtcrack- Hacen un volcado de los hash. Incluyen diccionarios para ataques por fuerza bruta.

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

¿Qué es la Seguridad Informática?

La seguridad informática es el área que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

El concepto de seguridad de la información no debe ser confundido con el de «seguridad informática», ya que este último solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad informática es también una disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

- La infraestructura computacional: Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas, robos, incendios,

boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

- Los usuarios: Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.

- La información: es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

¿Qué es una red informática?

Una red informática es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos. Básicamente, la comunicación dentro de una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, emisor y receptor, que se van asumiendo y alternando en distintos instantes de tiempo.

También hay mensajes, que es lo que estos roles intercambian. La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más extendido de todos el modelo TCP/IP, basado en el modelo de referencia o teórico OSI.

De la definición anterior podemos identificar los actores principales en toda red informática, que veremos a continuación.

Los dispositivos conectados a una red informática pueden clasificarse en dos tipos: los que gestionan el acceso y las comunicaciones en una red (dispositivos de red), como módem, router, switch, accesspoint, bridge, etc.; y los que se conectan para utilizarla (dispositivos de usuario final), como computadora, notebook, tablet, teléfono celular, impresora, televisor inteligente, consola de videojuegos, etc.

Los que utilizan una red, a su vez, pueden cumplir dos roles (clasificación de redes por relación funcional): servidor, en donde el dispositivo brinda un servicio para todo aquel que quiera consumirlo; o cliente, en donde el dispositivo consume uno o varios servicios de uno o varios servidores. Este tipo de arquitectura de red se denomina cliente/ servidor.

¿Qué es criptografía?

Criptografía (del griego κρύπτω krypto, «oculto», y γράφωςgraphos, «escribir», literalmente «escritura oculta») tradicionalmente se ha definido como la parte de la criptología que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes. Por tanto el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes. Para ello se diseñaban sistemas de cifrado y códigos. En esos tiempos la única criptografía que había era la llamada criptografía clásica.

La aparición de la Informática y el uso masivo de las comunicaciones digitales han producido un número creciente de problemas de seguridad. Las transacciones que se

realizan a través de la red pueden ser interceptadas. La seguridad de esta información debe garantizarse. Este desafío ha generalizado los objetivos de la criptografía para ser la parte de la criptología que se encarga del estudio de los algoritmos, protocolos (se les llama protocolos criptográficos) y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

¿Esteganografía?

La esteganografía (del griego στεγανος (steganos): cubierto u oculto, y γραφος (graphos): escritura), está enmarcada en el área de seguridad informática, trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es decir, se trata de ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal.

Para que pueda hablarse de esteganografía debe haber voluntad de comunicación encubierta entre el emisor y el receptor.

¿Qué es un ataque informático?

Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera).

Hay diversos tipos de ataques informáticos. Algunos son:

Ataque de denegación de servicio, también llamado ataque DoS (Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, normalmente provocando la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Man in themiddle, a veces abreviado MitM, es una situación donde un atacante supervisa (generalmente mediante un rastreador de puertos) una comunicación entre dos partes y falsifica los intercambios para hacerse pasar por una de ellas.

Ataques de REPLAY, una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida o retardada. Es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado.

Ataque de día cero, ataque realizado contra un ordenador, a partir del cual se explotan ciertas vulnerabilidades, o agujeros de seguridad de algún programa o programas antes de que se conozcan las mismas, o que, una vez publicada la existencia de la vulnerabilidad, se realice el ataque antes de la publicación del parche que la solvente.

Clases de ataques informáticos

A nivel mundial los ataques más populares son:

Phishing: Este fraude se basa en la obtención de tus datos personales así como la obtención de códigos de tarjetas de crédito, de cuentas bancarias, contraseñas u otros

datos. Este tipo de delito se ejecuta mediante elenvió de correos electrónicos, suplantando a alguna entidad de confianza para el usuario y solicitar sus cuentas bancarias. A la vez este tiene diversas ramificaciones; que en general engloban la misma idea. Ejemplos: Scam o Phishing Laboral, SMiShing, SpearPhishing, Vishing.

Spoofing: Es un ataque de suplantación de identidad; las cuáles son comúnmente utilizadas en malversaciones y/o investigación. Existen diversos tipos de suplantación: IP Spoofing(Sustituye direcciones IP de algún paquete por otro al que se desea suplantar), ARP Spoofing (Se infiltrar en una red Ethernet con el cual puede intervenir a los datos en la LAN, modificando el trafico en ella), DNS Spoofing(suplantación de indentidad por nombre de dominio), Mail Spoofing(suplantación en correo electrónico de la direcciones de email de usuarios).

Man-in-the-middle: Este ataque tiene la facilidad de interceptar comunicación entre dos usuarios sin que estos puedan detectarlo. Y consiguiendo manipular la información transmitida a su antojo.

AMENAZAS INFORMÁTICAS

¿Qué es Amenazas Informática?

Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información.

Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales.

¿Qué es un hacker?

Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos.

"algunos hackers diseñan virus informáticos muy perjudiciales"

Los términos hacker y hack pueden tener connotaciones positivas y negativas. Los programadores informáticos suelen usar las palabras hacking y hacker para expresar admiración por el trabajo de un desarrollador cualificado de soporte lógico, pero también se puede utilizar en un sentido negativo para describir una solución rápida pero poco elegante a un problema. Algunos desaprueban el uso del hacking como un sinónimo de cracker, en marcado contraste con el resto del mundo, en el que la palabra hacker se utiliza normalmente para describir a alguien que se infiltra en un sistema informático con el fin de eludir o desactivar las medidas de seguridad.

¿Qué es un Virus informático?

Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Tipos de virus informáticos.

Existen diversos tipos de virus, varían según su función o la manera en que este se ejecuta en nuestra computadora alterando la actividad de la misma, entre los más comunes están:

- Troyano: Consiste en robar información o alterar el sistema del hardware o en un caso extremo permite que un usuario externo pueda controlar el equipo.

- Gusano: Tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

- Bombas lógicas o de tiempo: Son programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una

combinación de teclas, o ciertas condiciones técnicas (Bombas Lógicas). Si no se produce la condición permanece oculto al usuario.

- Hoax: Los hoax no son virus ni tienen capacidad de reproducirse por si solos. Son mensajes de contenido falso que incitan al usuario a hacer copias y enviarla a sus contactos. Suelen apelar a los sentimientos morales ("Ayuda a un niño enfermo de cáncer") o al espíritu de solidaridad ("Aviso de un nuevo virus peligrosísimo") y, en cualquier caso, tratan de aprovecharse de la falta de experiencia de los internautas novatos.

- Joke: Al igual que los hoax, no son virus, pero son molestos, un ejemplo: una página pornográfica que se mueve de un lado a otro, y si se le llega a dar a cerrar es posible que salga una ventana que diga: OMFG!! ¡No se puede cerrar!.

NOTA: Existen otros tipos de virus que no son mencionados aquí.

REDES Y CONTROL DE ACCESO

Network Forensics

Forensia en redes, es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular. Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y

acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Es la captura, almacenamiento y análisis de los eventos de una red, para descubrir el origen de un ataque o un posible incidente.

Parámetros de seguridad en redes wifi

Las redes WiFi pueden ser abiertas o cerradas. En una red abierta, cualquier ordenador cercano al punto de acceso puede conectarse a Internet a través de él, siempre que tenga una tarjeta WiFi incorporada, claro. En la red cerrada el ordenador detectará una red inalámbrica cercana disponible, pero para acceder habrá que introducir la contraseña. Es lo que suele ocurrir en los aeropuertos y algunos hoteles, donde la contraseña se obtiene previo pago.

Hasta hace poco se empleaba un sistema de cifrado llamado WEP (WiredEquivalentPrivacy) para proteger las redes WiFi. Las transmisiones se cifran con una clave de 128 bits, y sólo los usuarios con contraseña pueden conectarse al punto de acceso. La mayoría de las tarjetas y puntos de acceso WiFi son compatibles con WEP, pero este sistema está desconectado por defecto. Los usuarios por lo general no se molestan en activarlo, y la red queda abierta. Si el vecino de al lado utiliza de vez en cuando la conexión de Internet quizá no sea demasiado grave, pero cuando accede a

información confidencial de la empresa o a fotos comprometidas de las vacaciones la cosa es más seria.

Hoy se utiliza un sistema de seguridad llamado WPA, que son las siglas de WiFiProtected Access. Este sistema está incluido en Windows XP con Service Pack 1, es más seguro que WEP y mucho más fácil de utilizar.

Medidores de seguridad en passwords

Si tu sitio web tiene la opción para registrarse como miembros, es importante que no pierdas de vista la primera impresión que los usuarios van a percibir desde que llenen el formulario de registro. Para que tus visitantes reconozcan que le das especial importancia a la seguridad del sitio y todos los datos que ellos están a punto de almacenar, es recomendable utilizar un medidor de seguridad en las contraseñas. Incluso si tú te preocupas por la seguridad de la data almacenada en la página web, las contraseñas poco seguras pueden tener serias consecuencias.

Es importante conocer algunas reglas básicas para la creación de passwords, que todos deberíamos saber, pero a las que realmente no hacemos caso y podríamos estar poniendo en riesgo nuestra identidad virtual.

- Mientras más caracteres, mejor. Usualmente nos conformamos con los 6 u 8 que nos exigen los sitios web, pero si empleáramos entre 13 y 15 podemos dormir más tranquilos.

• Intercala mayúsculas y minúsculas y tanto letras como números. Es más difícil ser vulnerable si no utilizas palabras comunes en el lenguaje y que puedes encontrar en un diccionario.

• Utiliza el lenguaje leet y símbolos especiales. Ojo que por símbolos especiales entendemos todos los símbolos, no necesariamente aquellos que están en la parte superior del teclado (#, $, %, &, /).

. A continuación ponemos a tu disposición unos scripts que serán útiles para crear una mejor interfaz de registro

- Password Meter: Password Meter nos explica fácilmente cuáles son los defectos que tienen las contraseñas que ingresamos y nos devuelve un porcentaje que indica qué tan segura es. Su algoritmo está basado en una función en lenguaje JavaScript bastante exacto.

-GeekWisdom: GeekWisdom nos ofrece un algoritmo JavaScript y nos devuelve un resultado numérico, además de darnos tips para la creación de contraseñas.

-YetAnotherPassword Mete: YetAnotherPassword Meter también nos detalla los aspectos evaluados y nos da un veredicto sobre la vulnerabilidad de la contraseña ingresada.

-jQuery: jQuery nos ofrece un código simple de entre su librería para diseñar un medidor de seguridad que podemos aplicar a nuestro sitio web.

-Dave’sWeblog: Dave’sWeblog nos ofrece un tutorial detallado para que podamos crear nuestros propios medidores de seguridad PHP, paso a paso.

El uso de estos medidores es útil para demostrar que todo miembro que se registre puede dejar de preocuparse acerca de qué va a pasar con su información, además de ser un proceso bastante sencillo para implementar en cualquier sitio. Muchas veces los usuarios no tienen conocimiento suficiente para crear una contraseña que verdaderamente sea segura en su afán de no olvidarla.

Tunneling

Se conoce como túnel o tunneling a la técnica que consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel de información dentro de una red de computadoras. El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc. La técnica de tunelizar se suele utilizar para trasportar un protocolo determinado a través de una red que, en condiciones normales, no lo aceptaría. Otro uso de la tunelización de protocolos es la creación de diversos tipos de redes privadas virtuales.

El establecimiento de dicho túnel se implementa incluyendo una PDU (unidad de datos de protocolo) determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel

queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH. Así, el protocolo A es encapsulado dentro del protocolo B, de forma que el primero considera al segundo como si estuviera en el nivel de enlace de datos.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

Sniffer de red

Un sniffer es un programa que absorbe o captura datos de la red. Todo lo que pasa por delante de sus narices lo absorbe y lo almacena para su análisis posterior. De esta forma, sin poseer acceso a ningún sistema de la red, se puede obtener información, claves de acceso o incluso mensajes de correo electrónico en el que se envían estas claves.

La forma más habitual de sniffing, probablemente porque está al alcance de cualquiera, es la que se puede llamar sniffing por software, utilizando un programa que captura la información de la red.

También es posible hacer lo llamar sniffing hardware, que pasaría por conectar en un cable de red un dispositivo que permita capturar el tráfico.

Con relación a este último tipo, la expresión "conectar el cable de red" es una expresión general que incluye el propio hecho de conectar un dispositivo a un cable de la red pero también incluye, por ejemplo, un receptor de radio que se sitúa en medio de un radio enlace. Como puedes imaginar, este tipo de técnicas requiere de unos conocimientos de electrónica adicionales muy importantes.

2.2.4 Un kit de herramientas en informática forense DVD.

El DVD contendrá lossoftwares contemplados dentro de las siguientes áreas:

- Adquisición y análisis de la memoria
- Herramientas de disco
- Criptografía
- Esteganografía
- Análisis del registro de Windows
- Herramientas de red.

El cual estará desarrollado con una interfaz amigable al usuario, para mayor facilidad de uso. A continuación se muestra el diseño del DVD:

Imagen 2.2.4.1

Pantalla de Inicio: en la pantalla de inicio o menú principal se encuentran las siguientes opciones: Software, Manual, Ficha Técnica, Software Extra.

Imagen 2.2.4.2

Botón de material de apoyo, contiene el documento de apoyo para los seminarios.

Software: Al ingresar a Software se encontrará el menú de los programas del kit

Imagen 2.2.4.3

Manual: accede al menú donde están los manuales de uso de cada software.

Imagen 2.2.4.4

Ficha técnica: accede al menú donde están los archivos con la información principal de los programas.

Imagen 2.2.4.5

Software Extra: accede al menú de los programa que van como un agregado.

Imagen 2.2.4.6

2.3 Marco Teórico Conceptual.

Informática Forense

Es el proceso de investigar dispositivos electrónicos o computadoras con el fin de descubrir, analizar y presentar información disponible, suprimida u ocultada que puede servir como evidencia en un asunto legal.

Ciencia Forense.

La ciencia forense nos proporciona los principios y técnicas que facilitan la investigación del delito criminal, en otras palabras: cualquier principio o técnica que puede ser aplicada para identificar, recuperar, reconstruir oanalizar la evidencia durante una investigación criminal forma parte de la ciencia forense.

Delitos Informáticos

El delito informático, o crimen electrónico, o bien ilícito digital es el término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Evidencia Digital.

Se puede decir que el término "Evidencia Digital" abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor.

Network Forensics

Forense en redes, es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular.

Perito Informático

Es la persona que tiene conocimientos en informática, cuyos servicios son utilizados por el juez para que lo ilustre en el esclarecimiento de un hecho que requiere los conocimientos especiales, científicos y técnicos relacionados a la informática y hace un análisis exhaustivo de los equipos informáticos, y sobre todo de las unidades de almacenamiento de datos en busca de todos aquellos elementos que puedan constituir prueba o indicio en el caso en cuestión de cómo se cometió un delito informático.

Ethical Hacking

Ethical Hacking es una disciplina de la seguridad informática que se sustenta en que la mejor forma de evaluar las amenazas que representan los llamados “hackers” o piratas de la información es conocer cómo actúan y operan.

Criptografía

Se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes.

Esteganografía.

Trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.

2.4 Marco Legal.

En El Salvador existe una base legal para algunos delitos informáticos, aunque es una base prematura; ya que no se ha reformado conforme al avance tecnológico y los códigos que rigen nuestra ley muestran de una forma generalizada, los delitos que se puede cometer dentro del medio informático.

El marco legal está basado en del Código penal y el código procesal civil y mercantil de El Salvador, de los cuales han sido retomados artículos que están vinculados con los delititos en nuestro país y el peritaje.

LEY ESPECIAL CONTRA ACTOS DE TERRORISMO

DELITO INFORMATICO

Art. 12.- Será sancionado con pena de prisión de diez a quince años, el que para facilitar la comisión de cualquiera de los delitos previstos en esta Ley:

a) Utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, información, documentos electrónicos, soportes informáticos, programas o sistemas de

información y de comunicaciones o telemáticos, de servicios públicos, sociales, administrativos, de emergencia de seguridad nacional, de entidades nacionales, internacionales o de otro país;

b) Creare, distribuyere, comerciare o tuviere en su poder programas capaces de producir los efectos a que se refiere el literal a), de este artículo.

CÓDIGO PROCESAL CIVIL Y MERCANTIL.

SECCIÓN CUARTA

PRUEBA PERICIAL

Nombramiento y aceptación del perito. Recusación

Art. 385.- El perito que hubiera sido designado por el juez será nombrado por éste para larealización del peritaje. En el plazo de tres días, dicho nombramiento le será comunicado al perito, quedeberá aceptar el encargo y prestará juramento o hará promesa de cumplir bien y fielmente el encargo.

El perito designado, podrá excusarse si concurre en él alguna de las causas de abstención. El tribunalprocederá a nombrar otro en los tres días siguientes a la recepción de la abstención.

El perito designado judicialmente podrá ser recusado a mas tardar dentro de los tres días siguientesa su designación, cuando por sus relaciones con las partes o con el objeto del proceso o, por cualquier otracausa razonable, hubiera dudas sobre su imparcialidad; debiéndose proceder en este caso a la designaciónde otro perito, conforme al inciso anterior.

Dictamen pericial

Art. 386.- El perito deberá presentar el dictamen por escrito y remitirlo al juez y a las partes dentrodel plazo otorgado, que deberá finalizar cuando menos diez días antes de la celebración de la audiencia probatoria.

CODIGO PENAL

CAPITULO III

Otros Ataques a La Libertad Sexual

Pornografía

Art. 172.- El que por cualquier medio directo, inclusive a través de medios electrónicos, fabricare, transfiriere, difundiere, distribuyere, alquilare, vendiere, ofreciere, produjere, ejecutare, exhibiere o mostrare, películas, revistas, pasquines o cualquier otro material pornográfico entre menores de dieciocho años de edad o deficientes mentales, será sancionado con prisión de tres a cinco años.

En la misma sanción incurrirá el que no advirtiere, de forma visible, sobreel contenido de las películas, revistas, pasquines o cualquier otro material,inclusive el que se pueda transmitir a través de medios electrónicos, cuando éstefuere inadecuado para menores de dieciocho años de edad o deficientes mentales.(18)

Utilización de personas menores de dieciocho años e incapaces o deficientes mentales en pornografía (18)

Art. 173.- el que produzca, reproduzca, distribuya, publique, importe,exporte, ofrezca, financie, venda, comercie o difunda de cualquier forma,imágenes, utilice la voz de una persona menor de dieciocho años, incapaz odeficiente mental, sea en forma directa, informática, audiovisual, virtual o porcualquier otro medio en el que se exhiban, en actividades sexuales, eróticas oinequívocas de naturaleza sexual, explícitas o no, reales o simuladas, serásancionado con prisión de seis a doce años.

CAPITULO II

De los delitos relativos a la intimidadviolación de comunicaciones privadas.

Art. 184.- El que con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido o se apodere de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivo o registro público o privado, será sancionado con multa de cincuenta a cien días multa.

Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos,a que se refiere el inciso anterior, la sanción será de cien a doscientos días multa.

El tercero a quien se revelare el secreto y lo divulgare a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa.

Violación agravada de Comunicaciones

Art. 185.- Si los hechos descritos en el artículo anterior se realizaren por las personasencargadas o responsables de los ficheros, soportes informáticos, archivos o registros, se impondrá, además de la pena de multa, inhabilitación del respectivo cargo o empleo público de seis meses a dos años.

CAPITULO V

De Los Daños

Daños Agravados

Art. 222.- Se impondrá prisión de dos a cuatro años: (8)

En el inciso "2"

2) Si el daño se realizare mediante manipulación informática.

Art. 226.- el que a escala comercial reprodujere, plagiare, distribuyere al mayoreo o comunicare públicamente, en todo o en parte, una obra literaria o artística o su transformación o una interpretación o ejecución artística fijada en cualquier tipo de soporte o fuere comunicada a través de cualquier medio,sin la autorización de los

titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios, será sancionado con prisión de dos a cuatro años.

En la misma sanción incurrirá, el que a escala comercial importare,exportare o almacenare ejemplares de dichas obras o producciones o ejecucionessin la referida autorización.

Escala comercial incluye la infracción dolosa significativa de derechode autor y derechos conexos, con el fin de obtener una ventaja comercial oganancia económica privada, así como la infracción dolosa que no tenga unamotivación directa o indirecta de ganancia económica, siempre que se cause undaño económico mayor a una infracción de poco valor. (26)

Violación agravada a derecho de autor y derechos conexos (26)

Art. 227.- será sancionado con prisión de cuatro a seis años, quienrealizare cualquiera de las conductas descritas en el artículo anterior,concurriendo alguna de las circunstancias siguientes:

1) usurpando la condición de autor sobre una obra o parte de ella o el nombre de un artista en una interpretación o ejecución;

2) modificando sustancialmente la integridad de la obra sinautorización del autor; y,

3) si la cantidad o el valor de la copia ilícita fuere de especial

Trascendencia económica. (26)

Violación a medidas tecnológicas efectivas (26)

Art. 227-a.- será sancionado con prisión de dos a cuatro años, el que confines de lograr una ventaja comercial o ganancia financiera privada:

a) evadiere, sin autorización del titular del derecho, cualquiermedida tecnológica efectiva que controle el acceso a una obra,interpretación, ejecución o fonograma protegido u otra materiaobjeto de protección;

b) Fabricare, importare, distribuyere, ofreciere al público,proporcionare o traficare dispositivos, productos o componentes;u ofreciere al público o proporcionare servicios al público, siempreque los dispositivos, productos o componentes, o los servicios:

1) Sean promocionados, publicitados o comercializados con el propósito de evadir una medida tecnológica efectiva;
2) Tengan únicamente un propósito limitado o uso de importancia comercial diferente al de evadir una medida tecnológica efectiva; o
3) Sean diseñados, producidos o ejecutados principalmente con el fin de permitir o facilitar la evasión de cualquier medida tecnológica efectiva.

Se excluye de responsabilidad penal, al que ejecute las actividadesexceptuadas conforme se establece en el artículo 85-d de la ley de propiedadintelectual. (26)

Violación a la información sobre gestión de derechos (26)

Art. 227-b.- será sancionado con prisión de dos a cuatro años, el que confines de lograr una ventaja comercial o ganancia financiera privada y a sabiendasque este acto podría inducir, permitir, facilitar o encubrir una infracción deun derecho de autor o derecho conexo:

a) A sabiendas suprimiere o alterare cualquier información sobre gestión de derechos;

b) Distribuyere o importare para su distribución la información sobre gestión de derechos, teniendo conocimiento que dicha información ha sido suprimida o alterada sin autorización del titular del derecho; o

c) Distribuyere, importare para su distribución, transmisión, comunicación o puesta a disposición del público copias de obras, interpretaciones o ejecuciones o fonogramas, teniendo conocimiento que la información sobre gestión de derechos ha sido suprimida o alterada sin autorización del titular del derecho.

Se excluye de responsabilidad penal, al que ejecute las actividadesexceptuadas conforme se establece en el artículo 85-e de la ley de propiedadintelectual. (26)

CAPITULO I

De los delitos relativos a la propiedad industrial

Infidelidad comercial

Art. 230.- El que se apoderare de documentos, soporte informático u otros objetos, paradescubrir o revelar un secreto evaluable económicamente, perteneciente a una empresa y queimplique ventajas económicas, será castigado con prisión de seis meses a dos años.

Revelación o divulgación de secreto industrial

Art. 231.- El que revelare o divulgare la invención objeto de una solicitud de patente o un secreto industrial o comercial, estando legal o contractualmente obligado a guardar reserva, será sancionado con prisión de seis meses a dos años.

Si el secreto se utilizare en provecho propio, la sanción se aumentará hasta en una tercera parte de su máximo.

Cuando el autor fuere funcionario o empleado público y el hecho se ejecutare en razón de sus funciones.

2.5 Documentación Técnica.

Documentación técnica: Recuva.

Recuva (pronunciado "recuperar") es una utilidad gratuita de Windows para recuperar archivos que han sido borrados accidentalmente de tu computadora. Esto incluye los archivos vaciados de la Papelera de reciclaje, así como imágenes y otros archivos que han sido eliminados por error del usuario de tarjetas de memoria de cámaras digitales o reproductores de MP3. Incluso va a traer de vuelta los archivos que han sido eliminados de su iPod, o por errores, accidentes y virus.

- Fácil de usar interfaz - simplemente haga clic en 'Scan' y seleccione los archivos que desea recuperar.
- Fácil de usar filtro de resultados basados en el nombre del archivo / tipo
- Ventanas simples como interfaz con la lista y la vista de árbol.

- Se puede ejecutar desde una unidad flash USB.
- Restaura todo tipo de archivos, documentos de Office, imágenes, vídeo, música, correo electrónico, cualquier cosa.
- Soporta FAT12, FAT16, FAT32, exFAT, NTFS, NTFS5, NTFS + EFS sistemas de archives.
- Restaura archivos de medios extraíbles (SmartMedia, Secure Digital, MemoryStick, cámaras digitales, discos flexibles, discos Jaz, Sony MemorySticks, tarjetas Compact Flash, Tarjetas Smart Media, Tarjetas Secure Digital, etc).
- Restaura archivos desde dispositivos ZIP externos, Firewire y discos duros USB.
- Es rápido, pequeño y toma segundos para correr.

Documentación técnica: Wireshark

Las siguientes son algunas de las muchas características Wireshark ofrece:

- Disponible para UNIX y Windows.
- Captura de paquetes de datos en vivo de una interfaz de red.
- Abrir archivos que contienen datos de paquetes capturados con tcpdump / WinDump, Wireshark, y una serie de otros programas de captura de paquetes.
- Los paquetes de importación de archivos de texto que contienen códigos hexadecimales de datos de paquetes.
- Visualice los paquetes con información muy detallada de protocolo.

- Guarde los datos de paquetes capturados.
- Exportación de algunos o todos los paquetes en una serie de formatos de archivo de captura.
- Filtre los paquetes en muchos criterios.
- Búsqueda de paquetes en muchos criterios.
- Colorear muestra de los paquetes en base a filtros.
- Crear varias estadísticas.

... Y mucho más!

Sin embargo, para apreciar realmente su poder, usted tiene que empezar a usarlo.

Documentación técnica FTK Imager Lite Version

FTK Imager ® es una herramienta de vista previa de datos y de imágenes que le permite evaluar rápidamente las pruebas electrónicas para determinar si un análisis más profundo con una herramienta forense como AccessData ® está garantizado ForensicToolkit ® (FTK). FTK Imager puede también crear copias perfectas (imágenes forenses) de datos de la computadora sin realizar cambios a la evidencia original.

Con FTK Imager, puede:

- Crear imágenes forenses de discos duros locales, disquetes, discos Zip , CD y DVD, carpetas enteras , o archivos individuales de diversos lugares dentro de los medios de comunicación.
- Archivos de previsualización y carpetas en los discos duros locales, unidades de red, disquetes, discos Zip, CD y DVD.
- Previsualizar el contenido de las imágenes forenses almacenados en el equipo local o en una unidad de red.
- Monte una imagen para una vista de sólo lectura que aprovecha el explorador de Windows para ver el contenido de la imagen exactamente como el usuario lo vio en la unidad original.
- Exportar archivos y carpetas de imágenes forenses.
- Ver y recuperar archivos que han sido borrados de la papelera de reciclaje, pero que aún no han sido sobrescritos.
- Crear hashes de archivos a través de cualquiera de las dos funciones hash disponible en FTK Imager: MessageDigest.(MD5) y el Secure Hash Algorithm (SHA- 1).

Generar informes de hash de los ficheros regulares e imágenes de disco (incluyendo los archivos dentro de imágenes de disco) que pueda después utilizar como punto de referencia para probar la integridad de la evidencia del caso.

Documentación técnica: RegRipper

Es una herramienta de código abierto, escrito en Perl, para extraer / analizar la información (claves, valores, datos) en el Registro y presentarlo para su análisis.

No necesita instalación.

Documentación técnica: AxCrypt v1.7.2850

Las siguientes son las características que realmente lo diferencian de todas las demás herramientas de cifrado de archivos, comercial, así como conexión:

- Haga doble clic para editar / ver con cualquier aplicación.
- Re-encriptación automática después de la modificación.
- Absolutamente ninguna configuración de usuario necesario o posible antes de su uso.
- El código abierto bajo licencia GNU GPL.12 idiomas en una distribución ejecutable.
- Amplia interfaz de línea de comandos para secuencias de comandos y programación.

Otras Características:

- Ventanas 2003/XP/Vista/2008/7/8 32 - y 64-bit compatible.
- Cifrado AES con claves de 128 bits.
- Editar un documento cifrado directamente con un doble clic.
- Caché frase de paso opcional - frases de paso de tipo una vez al inicio de sesión y / o reiniciar el sistema.

- Validación automática frase de acceso antes de descifrado o la edición.
- La generación de claves-File y apoyo.
- No hay opciones o interfaz de usuario - fácil de instalar y de usar.
- Relativamente ligero, menos de descargar 1Mb
- Amplia interfaz de línea de comandos.
- Opciones de modo de servidor.
- Soporte para archivos de más de 4GB (a excepción de los archivos libre descifrar).
- Dinámica de la fuerza bruta contra medida - envoltura clave iterativo.
- Se integra bien con los servicios de intercambio de archivos basado en web.
- Compresión selectiva antes del cifrado - rápidas descargas / subidas.
- Conserva el nombre de archivo original y la información de un archivo cifrado.
- Trituradora integrada.
- Trituración de todos los archivos de texto plano temporal y cifrados.
- Manejo de memoria Secure - no hay claves o datos en el archivo de paginación.
- Algoritmos estándar de la industria.
- Verificación de la integridad de datos - sin modificación no detectada.
- Únicas claves de cifrado de datos utilizados para cada archivo y el cifrado de (re-).
- Fácil de añadir más idiomas - en contacto conmigo (estoy especialmente en busca de idiomas nórdicos)!
- El código abierto - no hay puertas traseras.

- Apoyo de marca privada para las versiones comerciales o corporativos.
- Es GRATIS!

Documentación técnica: OpenPuffv4.00

Características:

- Generador de números aleatorios (CSPRNG).
- EsteganografíaDeniable.
- Cadenas superiores (hasta 256 MB de datos ocultos).
- Nivel de selección de bits de Carrier.
- Modern multi-criptografía (16 algoritmos).
- Varias capas de ofuscación datos (3 contraseñas).
- X-cuadrado resistencia steganalysis.

Capas únicas de la seguridad y la ofuscación:

- De 256 256 bit de criptografía de clave simétrica (con extensión contraseña KDF4).
- Datos de clave simétrica de cifrado 256 bits (barajar basado en CSPRNG).
- 256bit de clave simétrica para blanquear los datos (ruido basado en CSPRNG .mezcla).
- Codificación de bits de soporte no lineal adaptativo.

OpenPuff soporta muchos formatos:

- Las imágenes (BMP, JPG, PCX, PNG, TGA).
- El soporte de audio (AIFF, MP3, NEXT / dom, WAV).
- El soporte de video (3GP, MP4, MPG, VOB).
- Soporte Flash de Adobe (FLV, SWF, PDF).

Capítulo III Desarrollo de solución.

3.1 Propuesta de la solución.

Para complementar los conocimientos adquiridos sobre informática forense por los estudiantes de la cátedra de informática de la Universidad Tecnológica de El Salvador se ha desarrollado un kit de herramientas de software en informática forense para ser utilizado en seminarios en el laboratorio de hardware.

Con el kit los estudiantes que asistan a los seminarios podrán conocer y utilizar herramientas para adquisición y análisis de la memoria, herramientas de disco, criptografía, esteganografía, análisis del registro de Windows y herramientas de red, así como conceptos básicos relacionados a la informática forense.

Este kit está compuesto por:

- Ficha técnica de cada herramienta.
- Manual de uso de cada herramienta.
- Material de apoyo para seminarios.

- Instaladores o ejecutables de cada herramienta de software.

3.1.1 Ficha Técnica.

La ficha técnica dará a conocer la información de cada herramienta del kit relacionada a la compatibilidad con sistemas operativos, memoria RAM requerida, espacio requerido en disco duro, actualizaciones, plugings y programas adjuntos para complementar funcionamiento, de esta forma el usuario final del kit podrá analizar si herramienta que desea utilizar es compatible o no con la maquina en la que desea instalar o ejecutar dicha herramienta.

La ficha técnica se realizó considerando la importancia de conocer los requisitos que las herramientas en el kit necesitan para un óptimo funcionamiento y evitar que el usuario pierda el tiempo tratando de instalar una herramienta en una máquina que no cumple con los requisitos mínimos o que no es compatible con la herramienta. La ficha técnica se creó en un documento de texto y posteriormente convertido a PDF que está identificado con el nombre de cada herramienta del kit y mostrará la información de dicha herramienta, el archivo es liviano y de rápida ejecución en cualquier equipo del laboratorio de hardware de la Universidad Tecnológica de El Salvador.

Al momento de necesitar la información de una herramienta se deberá ejecutar el DVD con el kit de herramientas en informática forense, en el menú principal se deberá dar click sobre el botón “Fichas Técnicas”; en el siguiente menú se deberá seleccionar la

herramienta de la que se desea revisar la ficha técnica, de esta manera se podrá verificar los requisitos mínimos de cada herramienta.

La ficha técnica contendrá información clara y precisa de cada herramienta y de fácil comprensión para el usuario del kit.

Al laboratorio de hardware de la Universidad Tecnológica de El Salvador se le entregará una copia impresa y digital de las fichas técnicas de cada herramienta de software incluida en el kit.

3.1.2 Manual de Uso.

El manual de uso explicará a los estudiantes que asistan al seminario sobre informática forense como utilizar cada una de las herramientas incluidas en el kit de forma clara, precisa y detallada.

Para la creación del manual se tomó el tipo "paso a paso" ya que tiene un orden en su elaboración que permitió una explicación detallada, clara, ordenada y precisa, lo que generará una mejor comprensión para el uso de cada herramienta en el "kit de herramientas de software en informática forense para ser utilizado en seminarios en el laboratorio de hardware de la Universidad Tecnológica de El Salvador".

Se tomó en consideración para la creación del manual, realizarlo en un documento de texto y posteriormente convertido a PDF ya que este tipo de archivo es liviano y de

rápida ejecución; el manual explicará paso a paso la forma de utilizar cada herramienta del kit, para esto se incluirán imágenes para facilitar a los asistentes al seminario el uso de cada herramienta incluida en el kit.

Para visualizar el manual el usuario deberá buscar en el menú principal del kit de herramientas en informática forense DVD, el botón “Manuales de uso” en el siguiente menú deberá seleccionar dando click izquierdo sobre el botón del manual de uso que corresponde a la herramienta que se desea utilizar y a continuación se mostrará el manual de uso de dicha herramienta.

Al laboratorio de hardware de la Universidad Tecnológica de El Salvador se le entregará una copia impresa y digital del manual de uso de cada herramienta de software incluida en el kit.

3.1.3 Material de apoyo para los seminarios.

El material de apoyo para los seminarios proporcionará a los estudiantes conceptos básicos sobre informática forense, definiciones, clases de ataques informáticos, amenazas informáticas, información sobre tipos de delitos informáticos y las leyes aplicadas a estos delitos, así como dar a conocer herramientas utilizadas en la informática forense. Para el material de apoyo se tomó en consideración la investigación realizada en el marco de referencia, de ahí se pudo extraer información para que formará parte del material de apoyo, también se hizo uso de otras fuentes de

información tales como bibliotecas e internet, para proporcionar una variedad de información ordenada y de fácil comprensión para el lector.

Para facilitar la distribución del material de apoyo a los asistentes de los seminarios sobre informática forense que serán impartidos en el laboratorio de hardware de la Universidad Tecnológica de El Salvador, el material de apoyo se creó en un documento de texto y posteriormente convertido a PDF para incluirse en el kit de herramientas en informática forense DVD, para poder visualizarlo el usuario deberá ejecutar el DVD que contiene el kit, en el menú principal del DVD deberá dar click izquierdo en el botón "Material de apoyo" para ejecutar el archivo PDF que contiene la información del material de apoyo.

Al laboratorio de hardware de la Universidad Tecnológica de El Salvador se le entregará una copia impresa y digital del material de apoyo.

3.1.4 Kit de herramientas en informática forense DVD.

El DVD será utilizado para complementar los conocimientos de los estudiantes de técnico en ingeniería de hardware de la Universidad Tecnológica de El Salvador por medio de seminarios sobre informática forense que serán impartidos en el laboratorio de hardware.

El Kit de herramientas en informática forense DVD contiene los instaladores y/o ejecutables de cada herramienta seleccionada en el estudio de factibilidad, el material de

apoyo para los seminarios, la ficha técnica y el manual de uso de cada herramienta de software seleccionada previamente en el estudio de factibilidad del presente trabajo.

El DVD se creó con la finalidad de proporcionar al usuario una interfaz gráfica amigable y de fácil compresión para facilitar la identificación y aplicación de cada parte de su contenido antes mencionado.

Se realizaron pruebas para garantizar que cada herramienta de software el kit funciona correctamente, así mismo con los archivos de fichas técnicas, manuales de uso y material de apoyo.

Al laboratorio de hardware de la Universidad Tecnológica de El Salvador se le proporcionará una copia del Kit de herramientas en informática forense DVD, para que sea reproducida en las maquinas del laboratorio para los seminarios sobre informática forense.

Imagen 3.1.4.1: En la imagen se puede observar a los integrantes del grupo en la realización del menú del DVD que contiene el kit.

3.2 Conclusiones.

- Este trabajo tiene como una de sus metas primordiales el orientar a las generaciones futuras, sobre los aspectos importantes que se deben considerar en la Informática Forense de las empresas del sector informático.
- En el presente trabajo se pretende contribuir con la difusión y uso de las herramientas de Informática Forense en nuestro país y su aplicación en distintos tipos y gravedad de delitos.
- El desarrollo de esta tesis, ha permitido adquirir una mejor y mayor percepción de los problemas típicos por la falta de herramientas y técnicas para evitar los siniestros dentro de las empresas e instituciones.
- La Auditoría Forense en los siniestros informáticos es importante porque permite encontrar las evidencias necesarias y suficientes de un fraude o siniestro, así mismo actúa como un enfoque correctivo.
- Las metodologías y herramientas que se aplican en la Informática Forense son comunes en muchos delitos, pero así mismo utilizan las herramientas particulares en su enfoque que ayudan a dilucidar hechos ocurridos.

Para la universidad.

- La Informática Forense, en esta tesis, tuvo entre sus alcances incluir recomendaciones a la Universidad Tecnológica de El Salvador, lo cual permite establecer los principales controles y seguridades que deben implementarse en la Universidad.

- La Universidad Tecnológica de El Salvador se enfrentan hoy a una dura batalla, pues la proliferación de fraudes, robos y siniestros provocados por empleados o estudiante de la Universidad es muy frecuente en nuestro medio dada la grave crisis que afecta a nuestro país y es en la Informática Forense que los Directivos pueden encontrar una alternativa para llegar a tomar las medidas de seguridad informática dado a hechos pasados que les ayude a tomar una adecuada decisión.
- Esta tesis ayudará a conocer la importancia de la Informática forense, especialmente a los estudiantes de La Universidad Tecnológica de El Salvador debido a que la ciencia forense integra conceptos de temas de auditoría, contabilidad, informática, así como aspectos legales que se enmarcan en el perfil profesional integral.
- La informática forense es una disciplina que debe desarrollarse en forma integral y considerando que debe delinearse en forma concreta y por consenso, el entorno completo de operación con metodologías comunes, procedimientos, herramientas y técnicas en la Universidad Tecnológica de El Salvador.

3.3 Recomendaciones.

- Difundir el uso de las herramientas, técnicas y mecanismos necesarios para evitar los posibles fraudes, robos y siniestros que se pueden cometer dentro de un sistema de información.

- Se deben desarrollar prácticas y procedimientos de programación y control que busquen disminuir los problemas de seguridad en los productos de software y hardware.
- Revisiones periódicas constituyen una buena práctica de control interno y deben aplicarse en las organizaciones incluso para el entorno informático.

Para la universidad

- La mejor forma de evitar situaciones engorrosas de fraudes, robo y siniestros informáticos es estableciendo controles, pero por sobre todo, promover una cultura de seguridad Informática en las Universidades
- Adecuar a la Universidad con seguridad físicas y lógicas básicas para evitar que intrusos puedan obtener información.
- Los cambios tecnológicos y procesos globalizados demandan mayor rapidez, eficacia, efectividad y un mayor control, por lo cual los profesores y estudiantes vinculados a la investigación, así como los directivos de la Universidad deben profundizar en estos temas de actualidad.
- Ante los continuos cambios tecnológicos se recomienda que los profesores y estudiantes estén constantemente actualizándose en el uso de herramientas y técnicas hasta ganar la experiencia requerida para resolver casos con mayor facilidad.

3.4 Referencias

Cruz, J. A. (2006). *Herramienta de Apoyo para el Análisis Forenses de Computadoras*. Recuperado de http://www.etnassoft.com/biblioteca/herramienta-de-apoyo-para-el-analisis-forenses-de-computadoras/

Cummings, T. *La historia de la informática forense.* Recuperado de http://www.ehowenespanol.com/historia-informatica-forense-sobre_102525/

Estrada, L. E. (2009). *Informática Forense e Investigaciones en Cybercrime*. Recuperado de http://www.asobancaria.com/portal/pls/portal/docs/1/988056.PDF

Forense, H. D. *Historia de la informática forense*. Recuperado de Historia de la informática forense

Franco, J. P.; López, M. Á., & Riaño, J. L. (2001). *Criptografía digital. Fundamentos y aplicaciones.* España: Universidad de Cantabria.

Hedrich, E. M. (2012). *Informática Forense 44 casos reales.*

Informática forense. (2014). *Evidencia Digital*. Recuperado de http://informaticaforenseyevidenciadigital.wikispaces.com/Evidencia+Digital

Martínez, A. J. (2001). *La Formación de un IRT (Incident Response Team) Forense.*

Plata, P. A. (2010). *Seguridad.* Recuperado de http://www.seguridad.unam.mx/descarga.dsc?arch=2776

Sánchez, P. (2011). *Forensics Power Tools*. Recuperado de http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html

SYkRAYO. (2014). *Historia de la informática forense*. Recuperado de https://sites.google.com/site/sykrayolab/historia-de-la-informatica-forense

Zone-H. (2006). *Steganography A Mangarae*. Recuperado de http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf

3.5 Anexos.

3.5.1 Matriz de congruencia.

<table>
<tr><th colspan="4">MATRIZ DE CONGRUENCIA</th></tr>
<tr><td colspan="4">TEMA: KIT DE HERRAMIENTAS DE SOFTWARE EN INFORMÁTICA FORENSE PARA SER UTILIZADO EN SEMINARIOS EN EL LABORATORIO DE HARDWARE DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR.</td></tr>
<tr><td colspan="4">ENUNCIADO DEL PROBLEMA: ¿CÓMO SE PUEDEN COMPLEMENTAR LOS CONOCIMIENTOS ADQUIRIDOS SOBRE INFORMÁTICA FORENSE EN LA CÁTEDRA DE INFORMÁTICA DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR?</td></tr>
<tr><td colspan="4">OBJETIVO GENERAL: DESARROLLAR UN KIT DE HERRAMIENTAS DE SOFTWARE EN INFORMÁTICA FORENSE PARA SER UTILIZADO EN SEMINARIOS EN EL LABORATORIO DE HARDWARE DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR.</td></tr>
<tr><td>OBJETIVO ESPECÍFICO 1: SELECCIONAR Y EVALUAR LAS HERRAMIENTAS DE SOFTWARE A INCLUIR EN EL KIT DE INFORMÁTICA FORENSE.</td><td>OBJETIVO ESPECÍFICO 2: CREAR UN MANUAL DE USO PARA CADA UNA DE LAS HERRAMIENTAS DE SOFTWARE EVALUADAS Y SELECCIONADAS.</td><td>OBJETIVO ESPECÍFICO 3: DISEÑAR MATERIAL DE APOYO (CONCEPTOS BÁSICOS) PARA LOS ALUMNOS, EL CUAL SERÁ UTILIZADO EN SEMINARIOS SOBRE INFORMÁTICA FORENSE, EN EL LABORATORIO DE HARDWARE DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR.</td><td>OBJETIVO ESPECÍFICO 4: ELABORAR UN DVD CON LAS HERRAMIENTAS DE SOFTWARE QUE CONTENDRÁ EL KIT EN INFORMÁTICA FORENSE.</td></tr>
<tr><td>PROMESA 1: MOSTRAR LA INFORMACIÓN BÁSICA Y REQUISITOS DE SISTEMA PARA CADA UNA DE LAS HERRAMIENTAS DE SOFTWARE EN INFORMÁTICA FORENSE SELECCIONADAS.</td><td>PROMESA 2: SERVIRÁ PARA ORIENTAR A LOS USUARIOS DEL KIT COMO UTILIZAR CADA UNA DE LAS HERRAMIENTAS.</td><td>PROMESA 3: SERÁ UTILIZADO EN LOS SEMINARIOS SOBRE INFORMÁTICA FORENSE EN EL LABORATORIO DE HARDWARE DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR.</td><td>PROMESA 4: INCLUIRÁ TODAS LAS HERRAMIENTAS DE SOFTWARE EN INFORMÁTICA FORENSE SELECCIONADAS, EN LAS AREAS:
- ADQUISICIÓN Y ANÁLISIS DE MEMORIA.
- HERRAMIENTAS DE DISCO.
- CRIPTOGRAFÍA.
- ESTEGANOGRAFÍA.
- ANÁLISIS DEL REGISTRO DE WINDOWS.
- HERRAMIENTAS DE RED.</td></tr>
<tr><td>PRODUCTO 1: FICHA TÉCNICA.
SE DARÁ UNA COPIA IMPRESA PARA EL LABORATORIO DE HARDWARE DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR Y UN ARCHIVO PDF PARA SER REPRODUCIDO EN LAS MAQUINAS DEL LABORATORIO DE HARWARE.</td><td>PRODUCTO 2: MANUAL DE USO. SE DARÁ UNA COPIA IMPRESA PARA EL LABORATORIO DE HARDWARE DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR Y UN ARCHIVO PDF PARA SER REPRODUCIDO EN LAS MAQUINAS DEL LABORATORIO DE HARWARE.</td><td>PRODUCTO 3: MATERIAL DE APOYO. SE DARÁ UNA COPIA IMPRESA PARA EL LABORATORIO DE HARDWARE DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR Y UN ARCHIVO PDF PARA SER REPRODUCIDO EN LAS MAQUINAS DEL LABORATORIO DE HARWARE.</td><td>PRODUCTO 4: DVD (KIT DE HERRAMIENTAS EN INFORMÁTICA FORENSE.) SE PROPORCIONARÁ UNA COPIA PARA EL LABORATORIO DE HARDWARE DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR.</td></tr>
</table>

UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR

San Salvador, 11 de Julio de 2014

Reciban un cordial saludo deseando muchos éxitos en sus labores cotidianos

El motivo de la presente es para informar la finalización del proyecto kit de herramientas de software en informática forense para ser utilizado en seminarios en el Laboratorio de Hardware de la Universidad Tecnológica de El Salvador, presentado por:

López Alfaro, Samuel Dolores Antonio.

Rosales, Dolores Wilfredo.

Sibrian Iraheta, Jonathan Vladimir.

En el cual se entrega

1 Documento impreso del manual de uso de cada uno del software del kit en las áreas mencionadas. + Copia Digital

1 Documento impreso de la ficha técnica de los programas + Copia Digital

1 Documento impreso del material de apoyo + Copia Digital

2 Dvd con todo el contenido del Kit

2 ejemplares Empastados del trabajo.

F._____

Universidad Tecnológica
CÁTEDRA DE HARDWARE

Lic. Marvin Elenilson Hernández Montoya.