



Facultad de Informática y Ciencias Aplicadas

Carrera Técnico en Ingeniería de Hardware



Tema:

Desarrollo de un kit de herramientas digitales de informática forense para las soluciones a problemas de hardware y software en el laboratorio de hardware de la Universidad Tecnológica de El Salvador.

Trabajo de Graduación Presentado por:

Braulio Enrique Hernández Sosa

Oscar Alexander Valenzuela Cortez

Para optar al grado de:

Técnico en Ingeniería de Hardware

Marzo 2013

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

Página de autoridades

Ing. Nelson Zárate Sánchez

Rector

Ing. Francisco Armando Zepeda

Decano

Jurado Examinador

Ing. Claudia Lissette Rodríguez de Dimas

Presidenta

Ing. Mario Alberto Valle

Primer Vocal

Lic. Marvin Elenilson Hernández Montoya

Segundo Vocal

Marzo 2013

San Salvador, El Salvador, Centroamérica

HOJA DE REVISION DESPUES DE LA DEFENSA

Por este medio los miembros del Jurado evaluador del Trabajo de Graduación Titulado:

Desarrollo de un kit de herramientas digitales de informática forense para las soluciones a problemas de hardware y software en el laboratorio de Hardware de la Universidad Tecnológica de El Salvador.

Presentado por:

1 - Braulio Enrique Hernández Sosa

2 – Oscar Alexander Valenzuela Cortez

Después de la Defensa Oral, hemos revisado el Trabajo escrito y se han incluido en él las observaciones realizadas durante la misma.

Por lo que damos por APROBADO y finalizado el Trabajo:

F. _____

F. _____

Ing. Mario Valle

Lic. Marvin Elenilson Hernández Montoya

F. _____

Ing. Claudia Rodríguez de Dimas

San Salvador, 03 de enero de 2013

Agradecimientos.

A Dios Todopoderoso por permitirme iniciar y culminar mi carrera profesional, a mi madre por su apoyo en todo mi proceso de formación profesional, a mi tía Rosa Lidia Arriaga de Cortez por todo su apoyo espiritual, a mis primos y en especial a Baltazar Cortez Arriaga por su apoyo incondicional en todo el desarrollo de mi formación técnica como Técnico en la especialidad de Ingeniería de Hardware y a Baltazar Cortez Velásquez por su apoyo dado, también a todos mis amigos y compañeros de trabajo que me guiaron compartiendo sus conocimientos conmigo como lo fue Juan Paz Romero y a mi compañero de grupo Oscar Alexander Valenzuela Cortez por el trabajo realizado durante todo este proceso de graduación.

A la Alcaldía Municipal de Apopa por otorgarme la beca y así ayudarme en el transcurso de mi carrera Profesional.

Atte. Braulio Enrique Hernández Sosa.

Agradecimientos.

Primeramente a DIOS por permitirme el don de la vida por su gran bondad y saberme guiar en el camino del bien y protegerme siempre de todo mal.

Agradezco a mi familia en general por siempre brindar su apoyo sus consejos, su aliento a seguir hasta el final de mi carrera.

Mama: gracias por darme todo por siempre sacarme adelante por luchar siempre por que fuera un profesional, gracias por siempre estar a mi lado por siempre velar por mi salud, gracias mama eres la mejor del universo.

Tíos meme y Aracely: quiero darles las gracias por siempre estar ahí a pesar de no estar en el país jamás me abandonaron y estuvieron en los momentos que mas necesite de ustedes, mil gracias por su ayuda por su cariño incondicional.

A mi jefe Erick Alfredo Landaverde por permitirme estudiar en horas laborales por tenerme paciencia en todo, por enseñarme todo lo que hoy se en mi trabajo.

A mi Compañero de Tesis Braulio Enrique Hernández Sosa, que luchamos desde el primer ciclo hasta el final de nuestra carrera.

Agradezco a mis compañeros de trabajo por su ayuda por sus consejos especialmente a Edwin Eulises Estrada Hernández, a Anabel Palacios gracias por demostrarme su amistad y enseñarme a luchar por mis sueños.

Contenido

Introducción	i
1.1 Situación Problemática	1
1.2 Enunciado del Problema	2
1.3 Justificación	2
1.4 Objetivos	4
1.4.1 Objetivo General:	4
1.4.2 Objetivos Específicos:	5
1.5 Delimitaciones	5
1.6 Alcances	6
1.7 Estudio de factibilidad	8
1.7.1 Estudio de factibilidad Económica	8
1.7.2 Estudio de Factibilidad Técnica	12
1.8 Carta de Aceptación	19
1.9 Análisis General de todos los programas comparados	20
1.10 Anexos	21
1.10.1 A1 Matriz de congruencia	21
2.1 Marco Teórico de referencia	23
2.1.1 ¿Qué es la Informática Forense?	23
2.1.2 Pasos de la informática forense:	24
2.1.3 Herramientas de la informática forense:	26
2.1.4 Usos de la informática forense:	28
2.5 Áreas principales de la Informática Forense	32
2.5.1 Criptografía	32
2.5.2 Esteganografía	35
2.5.3 Recuperación de información	36
2.5.4 Hackeo de redes Wireless	37
2.2 Marco teórico de la solución	38
2.2.1 Manual de utilización del Kit de herramientas digitales de Informática Forense.	38

2.2.2 Kit de herramientas digitales de informática forense.....	122
2.2.3 CD Interactivo:.....	132
2.3 Marco Teórico Conceptual.....	134
2.4 Documentación Técnica.....	144
3.1 Propuesta de la solución.....	152
3.2 Conclusiones.....	157
3.3 Recomendaciones	159
3.4 Bibliografía	160

Introducción

El capítulo I establecido como Situación Actual del Proyecto, se realizará en la Universidad Tecnológica de El Salvador, en la cual se encuentra la situación problemática, en su Laboratorio de Hardware, donde están las Computadoras que por tener daños en su software, archivos que se han eliminado por error en los equipos, y que afectan el rendimiento de los mismos en su Hardware y Software.

En el laboratorio de hardware es donde se encuentra la situación problemática que describe las necesidades que tienen las computadoras de tener en ellas un kit de herramientas digitales de informática forense, para un mejor rendimiento en el sistema operativo, aplicaciones secundarias, y así servir de una forma más eficiente cuando sean utilizadas por los estudiantes que decidan realizar el seminario de informática forense.

En las computadoras del laboratorio de hardware se generan muchos problemas de hardware y software debido a que los hackers crean cada día diferentes tipos de malware para la red, los correos, redes sociales etc.

En el capítulo II establecido como Documentación Técnica del proyecto, describe claramente los tres marcos teóricos los cuales son: marco teórico de referencia, marco teórico de la solución y marco teórico conceptual.

En el marco teórico de referencia se describen las bases sobre las cuales está desarrollándose el proyecto, así como también teoría importante sobre el tema que se

está tratando en este documento, se explicará el concepto de informática forense, pasos que se utilizan en la informática forense, áreas principales de la informática forense etc.

En el marco teórico de la solución se mencionan los tres productos propuestos en el capítulo anterior y la manera en que ellos darán la solución a los problemas planteados anteriormente.

En el marco teórico conceptual se encontrará un glosario con todos los conceptos básicos sobre la informática forense usados en este documento, como por ejemplo: informática forense, criptografía, esteganografía, hacker, datos, entre otros.

En la parte de la Documentación Técnica se describen cada programa que contiene el kit de herramientas digitales de informática forense, explicando sus características técnicas.

En el capítulo III establecido como Desarrollo de la Solución, presenta la culminación del proyecto que se está desarrollando el cual se refiere a la informática forense, y se dará un producto principal para la solución de la situación problemática que se planteó anteriormente en este documento, además de este producto habrán otros dos que lo complementan para un funcionamiento mejor en el área de software, y también de hardware en computadoras de escritorio y laptops.

Además de la propuesta de la solución que como grupo se ofrece para resolver la situación problemática que existe en el Laboratorio de Hardware de la Universidad Tecnológica de El Salvador, también se realizó el diseño de un portafolio digital con

toda la información necesaria de los productos que se han evaluado utilizando el modelo ADDIE que es el que describe cada producto en diferentes etapas como lo son el análisis del producto seleccionado, el diseño con el que se realizó cada uno de los productos, el desarrollo del producto, la implementación del producto y la evaluación del mismo.

Al final del capítulo se presentan las conclusiones del documento general explicando detalladamente el desarrollo del kit de herramientas digitales de informática forense, el uso adecuado de cada uno de los programas que se usarán por medio del manual de utilización del kit de herramientas digitales de informática forense y el CD interactivo que tendrá los videos donde se verán los procesos para usar cada programa, imágenes de las ventanas que presentan cada uno de los programas.

CAPITULO I

Situación Actual

1.1 Situación Problemática

La Universidad Tecnológica de El Salvador, en su Facultad de Informática y Ciencias Aplicadas tiene a su disposición en la Escuela de Informática un Laboratorio de Hardware de computadoras para el uso de los estudiantes de la universidad.

En el Laboratorio de Hardware se imparten diferentes seminarios siendo uno de ellos el de informática forense, en el cual el desarrollo de este es insuficiente debido a que no se cuenta con un material didáctico de apoyo bien estructurado y enfocado en la informática forense, para que los estudiantes obtengan el conocimiento teórico y práctico en el área.

En los seminarios anteriores se ha observado que el desarrollo de los mismos no cumple con las necesidades de los estudiantes porque solamente son desarrollados teóricamente y no prácticamente para que puedan fortalecer las habilidades técnicas de los integrantes.

Según lo planteado anteriormente los problemas más comunes que se presentan en el laboratorio de hardware de la Universidad Tecnológica son:

- Pérdida de Información por el mal uso del usuario.
- Mala manipulación en los dispositivos haciendo así que generen conflictos entre el sistema.

- Mala memoria del usuario y olvido de contraseñas de usuarios de Windows.
- Problemas de discos duros por sectores defectuosos.
- Eliminación de particiones del sistema o formateo de unidades de almacenamiento que hayan contenido información valiosa.
- Problemas a nivel de redes informáticas como jaqueo de redes.
- Problemas en el correo electrónico por filtración de spyware.

El proyecto a desarrollarse en el laboratorio de hardware ofrece una implementación completa para un mejor desarrollo de los seminarios de informática.

1.2 Enunciado del Problema

¿Es necesaria la implementación de un kit de herramientas digitales de informática forense para la solución de problemas de hardware y software que tengan las computadoras del laboratorio de hardware?

1.3 Justificación

El siguiente proyecto surge a partir de las necesidades de la Universidad Tecnológica de El Salvador, de implementar un método de solución para problemas de software y hardware en computadoras de escritorio y laptop, y también proporcionar una herramienta digital para solucionar estos problemas antes mencionados, de los cuales se pueden mencionar los siguientes:

Problemas de Hardware:

- Sectores defectuosos debido a una mala magnetización en discos duros.

- Recuperación de información de sectores defectuosos.
- Fallos a la hora de copiar, mover, borrar o crear ficheros.

Problemas de software:

- Pérdida de información en discos duros.
- Daños en el sistema operativo por causa de malware.
- Daños lógicos en los discos duros.
- Pérdida de paquetes de datos informáticos.
- Inseguridad en correos electrónicos.
- Pérdida de información en pen drive.
- Desencriptar archivos encriptados.

El proyecto consta de la realización de un kit de herramientas digitales de informática forense y así proporcionar una herramienta de solución para problemas de recuperación de datos, escaneo y limpieza de malware en el disco duro, recuperación de archivos perdidos en particiones borradas accidentalmente por el usuario, conflictos entre direcciones IP, hacker de cuentas de correos electrónicos, pantalla de color azul al encender la computadora, congelamiento del sistema etc.

El kit de herramientas digitales de informática forense se realizará con el objetivo principal de darle a la Universidad Tecnológica de El Salvador una herramienta nueva para solucionar problemas de mal funcionamiento del hardware y software, así como también se realizará con el fin de ofrecer a la venta un producto para el área de

informática forense que cumpla con las demandas del cliente, en la recuperación de información, restauración del sistema operativo, limpieza de la computadora a nivel lógico en laptops y desktops, entre otras necesidades del hardware y software.

La Universidad Tecnológica de El Salvador, en su Laboratorio de Hardware se realizan seminarios enfocados hacia la informática forense desarrollados teóricamente, por lo que se pretende implementar un método de informática forense que pueda ser desarrollado en estos seminarios y sirva como una herramienta tanto teórica como práctica para fortalecer los conocimientos y habilidades de los estudiantes de estos seminarios.

Entre las ventajas que tiene la realización de este proyecto están:

1. Ayudará a solucionar de una forma más rápida y eficiente problemas de software y hardware en computadoras de escritorio y laptops.
2. Brindará un material de apoyo para el seminario de informática forense que se realiza en la Universidad Tecnológica de El Salvador.
3. Ayudará al estudiante a tener un aprendizaje más completo, en teoría de informática forense y práctica utilizando las herramientas digitales adecuadas al desarrollarse el seminario en la Universidad Tecnológica de El Salvador.

1.4 Objetivos

1.4.1 Objetivo General:

- Desarrollar un kit de herramientas digitales de informática forense, con el fin de dar solución a los problemas de hardware y software antes mencionados, que presentan las

computadoras del laboratorio de hardware que pertenece a la Universidad Tecnológica de El Salvador y también brindar un material de apoyo para la realización de seminarios de informática forense en la Universidad Tecnológica de El Salvador.

1.4.2 Objetivos Específicos:

- Investigar un método de solución a problemas de hardware y software, bajo la orientación de la informática forense.
- Desarrollar un manual para la utilización correcta de las herramientas digitales de informática forense.
- Mejorar el funcionamiento lógico y físico de las computadoras de escritorio y laptops, mediante la aplicación de herramientas digitales de informática forense.

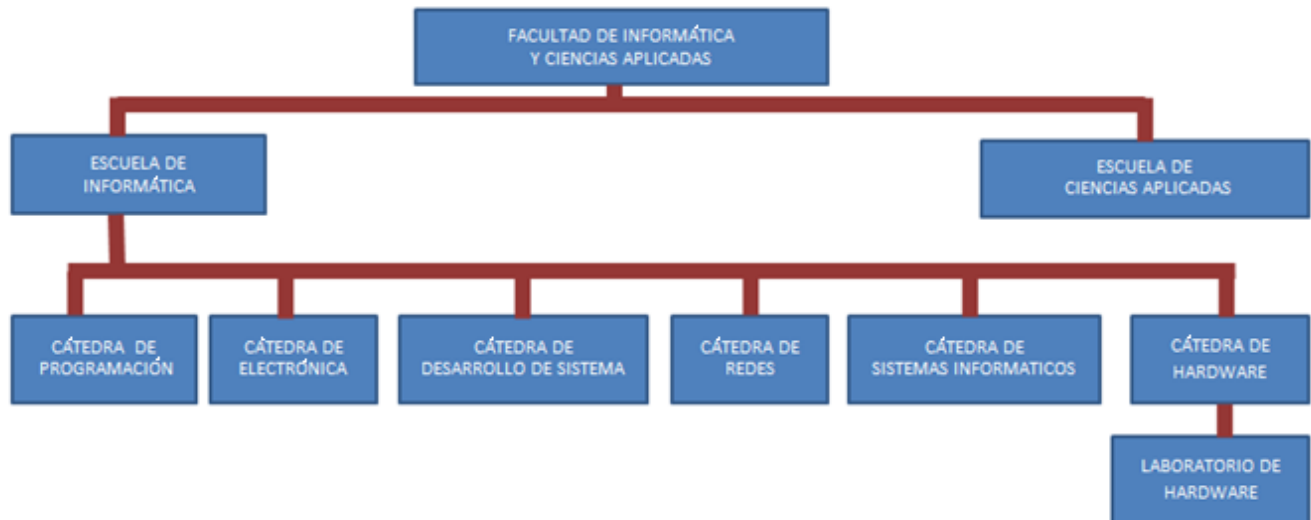
1.5 Delimitaciones

Geográfica: En la Universidad Tecnológica de El Salvador ubicada en Calle Arce, No. 1026 San Salvador.

Temporal: Del 23 de julio al 16 de noviembre de 2012.

Organizacional: Este proyecto será desarrollado en la Universidad Tecnológica de El Salvador en el laboratorio de hardware.

Organigrama



1.6 Alcances

Al realizar este proyecto se ofrecerá un kit de herramientas digitales de informática forense para la utilización en el laboratorio de hardware, utilizándose como un material didáctico de apoyo enfocado especialmente al uso correcto de aplicaciones que ayudan al usuario a resolver problemas de software y hardware, entre los cuales están:

Problemas de Hardware:

- Sectores defectuosos debido a una mala magnetización en discos duros.
- Recuperación de información de sectores defectuosos.
- Fallos a la hora de copiar, mover, borrar o crear ficheros.

Problemas de software:

- Pérdida de información en discos duros.
- Daños en el sistema operativo por causa de malware.
- Daños lógicos en los discos duros.
- Pérdida de paquetes de datos informáticos.
- Inseguridad en correos electrónicos.
- Pérdida de información en pen drive.
- Desencriptar archivos encriptados.

En el laboratorio de hardware estará disponible para los usuarios un manual impreso para la correcta utilización del kit de herramientas digitales de informática forense el cual brindará conocimientos teóricos y prácticos con imágenes y fotografías de cómo resolver problemas de hardware y software en computadoras de escritorio y laptops.

Se ofrecerá un CD interactivo que contenga en formato digital el manual teórico y práctico de cómo utilizar adecuadamente el kit de herramientas digitales de informática forense.

Promesa	Producto
Brindará a los usuarios conocimientos teóricos y prácticos sobre cómo utilizar el kit de herramientas digitales de informática	Manual impreso para utilización del kit de herramientas digitales de informática forense.

forense.	
Se utilizará un lenguaje comprensible para el usuario en el desarrollo de los videos para un mejor entendimiento sobre el proceso a seguir.	CD interactivo
Las computadoras del laboratorio de hardware tendrán un mejor rendimiento físico y durabilidad.	Kit de herramientas digitales de informática forense.

1.7 Estudio de factibilidad

1.7.1 Estudio de factibilidad Económica

Reparadores de discos duros

Producto	HDD Regenerator 1.51	Hard Disk Sentinel Free 3.60	Disk Heal
Precio C/U	Licencia \$84.99	Licencia EUR 16	Licencia Libre

En este cuadro comparativo se presentan tres reparadores de disco duros en el cual se ha elegido a HDD Regenerador debido a que es accesible en la red de internet para los usuarios y cumple con las características necesarias para su uso.

Recuperadores de Información

Producto	Ontrack Easy Recovery Profesional 6.22	Easy File Undelete 2.6	Disk Doctor Undelete 1.00
Precio C/U	Licencia Libre	Licencia EUR 33	Licencia \$49

En este cuadro comparativo se presentan tres recuperadores de información en el cual se ha elegido a Ontrack Easy Recovery Profesional 6.22 por ser un software que cumple con las características que se necesitan para su uso.

Diagnósticos de discos duros

Producto	HD Tune Pro 4.6	Tune Up Utilities 2012	Active Smart 2.9
Precio C/U	\$34.95	Licencia \$29	Licencia \$33

En este cuadro comparativo se presentan tres diagnósticos de disco duros en el cual se ha elegido a HD Tune por contar con las características necesarias para su uso.

Seguridad Informática

Producto	Bit Defender 2012 Total Security v15.0	PC Tools Internet Security	Defenx Internet Security
Precio C/U	Licencia \$79.95	Licencia \$33	Licencia \$69.95

En este cuadro comparativo se presentan tres aplicaciones de seguridad informática en el cual sea elegido a Bit Defender 2012 Total Security por ser un programa que utiliza varias configuraciones en un mismo software para dar seguridad a las computadoras de escritorio y laptop para evitar la intrusión de malware.

Criptografía

Producto	Axcrypt v1.7.2850	Asistente de prácticas de seguridad informática v4.0.0	Crypcolor v1.2
Precio C/U	Licencia Libre	Licencia Libre	Licencia Libre

En el cuadro comparativo anterior se presentan tres software que son para encriptar información de los cuales se eligió al programa Axcrypt por ser de fácil uso al usuario y poseer licencia libre siendo así más económico.

Esteganografía

Producto	My Lockbox	Password Folder	Free Hide Folder
Precio C/U	Licencia Libre	Licencia libre	Licencia Libre

En el cuadro comparativo anterior se presentan tres programas para poder ocultar las carpetas y archivos que el usuario desee que no se encuentren a la vista, de los cuales se eligió a My Lockbox ya que cumple con las características económicas para el usuario de ser de licencia libre y fácil de usar.

Hackeo de redes inalámbricas

Producto	Beini 1.2.2	Wiress Hark	Wireless Key View
Precio C/U	Licencia Libre	Licencia Libre	Licencia Libre

En el cuadro comparativo anterior se presentan tres programas para realizar el hackeo de redes inalámbricas, de los cuales se ha elegido a beini por ser un software eficiente en la decodificación de claves WEP y WPA y además posee licencia Libre para ayudar a la economía del usuario.

1.7.2 Estudio de Factibilidad Técnica

Evaluación del Bit Defender 2012 Total Security el cual será aprobado si es = 70%

Características	Peso%	Defenx Internet Security		PC Tools Internet Security		Bit Defender Total Security 2012	
		Clasificación	Puntaje	Clasificación	Puntaje	Clasificación	Puntaje
Sistema de adquisición	10%	1	10	1	10	2	20
Antivirus y antispysware.	30%	2	60	1	30	2	60
Protección Ethernet	30%	2	60	2	60	2	60
Optimización de las operativas	30%	2	60	1	30	2	60
Totales	100%		190		130		200
Ponderación Final			190/2=95%		130/2=65%		200/2=100%
Resultado Obtenido		Aprobado		Reprobado		Aprobado	

Análisis: En la tabla anterior se hizo la comparación de 3 programas que sirven para la seguridad informática y se escogió a Bit Defender 2012 Total Security por que posee una configuración de protección para malware y spyware, además de esto pose protección Para Ethernet y Host.

Evaluación Ontrack Easy Recovery Profesional 6.22 el cual será aprobado si es = 70%

Características	Peso %	Ontrack Easy Recovery Profesional		Easy File Undelete 2.6		Disk Doctors Undelete 1.00	
		Clasificación	Puntaje	Clasificación	Puntaje	Clasificación	Puntaje
Recupera cualquier dato de discos duros	40%	2	80	1	40	2	80
Visualizar un archivo antes de recuperarlo.	10%	1	10	1	10	2	20
Búsqueda muy potente.	20%	2	40	2	40	2	40
Búsqueda Rápida.	20%	2	40	2	40	1	20
Búsqueda de papel de reciclaje.	10%	2	20	1	10	1	10
Totales	100%		190		140		170
Ponderación Final		190/2= 95%		140/2= 70%		170/2= 85%	
Resultado Obtenido		Aprobado		Aprobado		Aprobado	

Análisis: En el cuadro anterior se ha hecho la comparación de 3 programas para recuperación de datos, de los cuales se ha escogido a Ontrack Easy Drive Data Recovery 2.5 por ser eficaz en la recuperación de archivos, además de esto ofrece al usuario visualizar el documento antes de recuperarlo.

Evaluación HD Tune el cual será aprobado si es = 70%

Características	Peso %	HD Tune		Tune Up Utilities		Active Smart 2.9	
		Clasificación	Puntaje	Clasificación	Puntaje	Clasificación	Puntaje
Prueba de rendimiento.	30%	2	60	1	30	2	60
Panel de datos Smart.	10%	2	20	1	10	1	10
Búsqueda de errores físicos.	20%	2	40	2	40	2	40
Indicador de temperatura.	20%	2	40	1	20	1	20
Mantenimiento lógico de	20%	2	40	2	40	2	40
Totales	100%		200		140		170
Ponderación Final		200/2= 100%		140/2= 70%		170/2= 85%	
Resultado Obtenido		Aprobado		Aprobado		Aprobado	

Análisis: En la tabla anterior se hizo la comparación de 3 programas de diagnósticos de discos duros, y se escogió a HD Tune por que cumple con las características técnicas necesarias para dar un buen diagnóstico en computadoras y tiene la capacidad de encontrar fallas lógicas y físicas.

Evaluación del HDD Regenerator 1.51 el cual será aprobado si es = 70%

Características	Peso %	HDD Regenerator 1.51		Disk heal		Salvation HDD scan	
		Clasificación	Puntaje	Clasificación	Puntaje	Clasificación	Puntaje
Escaneo de sectores defectuosos	40%	2	80	1	40	1	40
Reparación de sectores dañados	30%	1	30	1	30	1	30
formatos FAT y NTFS	10%	2	20	1	10	1	10
La regeneración se efectúa con un CD de arranque	20%	2	40	2	40	1	20
Totales	100%		170		120	1	100
Ponderación Final		170/2 = 85		120/2 = 60		100/2 = 50	
Resultado Obtenido		Aprobado		Reprobado		Reprobado	

Análisis: En la tabla anterior se ha hecho la comparación técnica de tres programas que sirven para la reparación de sectores dañados en discos duros, y se ha elegido a HDD Regenerator porque cumple con las características técnicas necesarias de funcionamiento.

Evaluación de Axcrypt el cual será aprobado si es = 70%

Características	Peso %	Axcrypt v1.7.2850		Asistente de prácticas de seguridad informática v4.0.0		Crypcolor v1.2	
		Clasificación	Puntaje	Clasificación	Puntaje	Clasificación	Puntaje
Proteger tus ficheros	40%	2	80	1	40	1	40
codificar un fichero	30%	1	30	1	30	1	30
codificado e introduce la contraseña	10%	2	20	1	10	1	10
totalmente protegidos en tu PC	20%	2	40	2	40	1	20
Totales	100%		170		120	1	100
Ponderación Final		170/2 = 85		120/2 = 60		100/2 = 50	
Resultado Obtenido		Aprobado		Reprobado		Reprobado	

Análisis: En la tabla anterior se hizo la comparación de 3 programas que sirven para que la información se mantenga oculta y segura, por ello se escogió a Axcrypt porque cumple con las características técnicas necesarias para dar seguridad y ocultar archivos en computadoras.

Evaluación de My Lockbox el cual será aprobado si es = 70%

Características	Peso %	My Lockbox		File lock		Universal Shield	
		Clasificación	Puntaje	Clasificación	Puntaje	Clasificación	Puntaje
Protege los archivos de usuarios extraños	40%	2	80	1	40	1	40
Utiliza una clave de seguridad para el archivo	30%	1	30	1	30	1	30
Su desinstalación requiere la clave del usuario	10%	2	20	1	10	1	10
	20%	2	40	2	40	1	20
Totales	100%		170		120	1	100
Ponderación Final		170/2 = 85		120/2 = 60		100/2 = 50	
Resultado Obtenido		Aprobado		Reprobado		Reprobado	

Análisis: En la tabla anterior se hizo la comparación de 3 programas que sirven para que la información se mantenga oculta y segura, por ello se escogió a My Lockbox porque cumple con las características técnicas necesarias para dar seguridad y ocultar archivos en computadoras.

Evaluación del software Beini el cual será aprobado si es = 70%

Características	Peso %	Beini 1.2.2		Wireshark		Wireless Key View	
		Clasificación	Puntaje	Clasificación	Puntaje	Clasificación	Puntaje
Más tarjetas y drivers soportados.	30%	2	60	2	60	2	60
Ataque de diccionario wep	20%	1	20	1	20	2	40
Mejor velocidad de crackeo	30%	2	60	1	30	1	30
Captura de múltiples tarjetas	20%	2	40	1	20	1	20
Totales	100%		180		130		150
Ponderación Final		180/2=90		130/2=65		150/2=75	
Resultado Obtenido		Aprobado		Reprobado		Aprobado	

Análisis: En la tabla anterior se presentan tres aplicaciones con función de detectar y crackear redes inalámbricas, de las cuales se ha elegido a Beini por tener las funciones básicas necesarias para la detección y captura de varias señales inalámbricas.

1.8 Carta de Aceptación

UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR

San Salvador, 30 de agosto de 2012



Lic. Marvin Elenilson Hernandez Montoya

UTEC

Presente.

El motivo de la presente es para solicitar la autorización para el desarrollo de nuestro proyecto de graduación llamado: Desarrollo de un kit de herramientas digitales de informática forense para las soluciones a problemas de hardware y software en el laboratorio de hardware de la Universidad Tecnológica de El Salvador.

Esperando su favorable respuesta.

Atentamente.

F. _____

Lic. Marvin Elenilson Hernandez Montoya.

1.9 Análisis General de todos los programas comparados

Según el registro anterior y las comparaciones económicas y técnicas de todas las aplicaciones presentadas se ha escogido un software por cada área presentada y los programas a utilizar son los siguientes:

- HDD Regenerator 1.51 (Reparador de discos duros)
- Bit Defender 2012 Total Security (Seguridad Informática)
- Ontrack Easy Recovery Profesional 6.22 (Recuperación de datos)
- HD Tune Pro 4.60 (Diagnósticos de discos duros)
- My Lockbox Pro 2.3 (Ocultar información)
- Axcript 1.7.2 (ocultar archivos)
- Beini 1.2.2 (hackeo de redes inalámbricas)

La lista de aplicaciones anteriores se ha elegido porque su licencia es fácil de encontrar en la red de internet.

1.10 Anexos

1.10.1 A1 Matriz de congruencia

Matriz de congruencia		
Tema: Desarrollo de un kit de herramientas digitales de informática forense para las soluciones a problemas de hardware y software en el laboratorio de hardware de la Universidad Tecnológica de El Salvador.		
Enunciado del problema: ¿Es necesaria la implementación de un kit de herramientas digitales de informática forense para la solución de problemas de hardware y software que tengan las computadoras del laboratorio de hardware?		
Objetivo General: Desarrollar un kit de herramientas digitales de informática forense, con el fin de dar solución a los problemas de hardware y software que presentan las computadoras del laboratorio de hardware que pertenece a la Universidad Tecnológica de El Salvador y también brindar un material de apoyo para la realización de seminarios de informática forense en la Universidad.		
Objetivo Especifico 1: Investigar un método de solución a problemas de hardware y software, utilizando un kit de herramientas digitales de	Objetivo Especifico 2: Desarrollar un manual para la utilización correcta de las herramientas digitales de informática forense.	Objetivo Especifico 3: Mejorar el funcionamiento lógico y físico de las computadoras de escritorio y laptops, mediante la aplicación de herramientas

informática forense.		digitales de informática forense.
Promesa 1: Desarrollar un método específico que sirva para solucionar problemas de hardware y software en computadoras de escritorio y laptop.	Promesa 2: Hacer un manual escrito que contenga los pasos para utilizar el kit de herramientas digitales de informática forense.	Promesa 3: Mejorar el funcionamiento lógico y físico de las computadoras de escritorio y laptop del laboratorio de hardware que pertenece a la Universidad Tecnológica de El Salvador usando el kit de herramientas digitales de informática forense.

Capítulo II

Documentación Técnica

2.1 Marco Teórico de referencia

2.1.1 ¿Qué es la Informática Forense?

Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal, dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Esta disciplina hace uso no solo de tecnología de punta para poder mantener la integridad de los datos y del procesamiento de los mismos, sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. El conocimiento del informático forense abarca no solamente del software sí o no también del hardware, redes, seguridad, hacking, cracking, recuperación de información etc.

La informática forense ayuda a detectar pistas sobre los ataques informáticos, robo de información, conversaciones o pistas de email, chats, la importancia de estos y el poder mantener su integridad se basa en que la evidencia digital o electrónica es sumamente frágil, por el simple hecho de dar doble clic a un archivo modificaría la última fecha del acceso del mismo, es muy importante mencionar que la informática forense no tiene

parte preventiva, es decir, que no se encarga de prevenir delitos informáticos, si no que para esto la encargada es la seguridad informática. (Wikipedia, 2001)

La infraestructura informática que puede ser analizada es toda aquella que posee una memoria informática, por lo que se pueden analizar los siguientes dispositivos:

- Disco duro de una computadora o servidor.
- Logs de seguridad.
- Firewalls,
- IP.
- Software de monitoreo y seguridad.

2.1.2 Pasos de la informática forense:

El proceso de análisis forense a una computadora se describe a continuación:

Identificación:

Es muy importante conocer los antecedentes, situación actual y el proceso que se quiere seguir para poder tomar la mejor decisión con respecto a las búsquedas y la estrategia de investigación. Incluye muchas veces la identificación del bien informático, su uso dentro de la red, el inicio de la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia), la revisión del entorno legal que protege el bien y del apoyo para la toma de decisión con respecto al siguiente paso una vez revisados los resultados.

Preservación:

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta para poder mantener la integridad de la evidencia y la cadena de custodia que se requiere. Al realizar una imagen forense, nos referimos al proceso que se requiere para generar una copia “bit-a-bit” de todo el disco, el cual permitirá recuperar en el siguiente paso, toda la información contenida y borrada del disco duro. Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios.

Análisis:

Proceso de aplicar técnicas científicas y analíticas a los medios duplicados por medio del proceso forense para poder encontrar pruebas de ciertas conductas. Se pueden realizar búsquedas de cadenas de caracteres, acciones específicas del o de los usuarios de la máquina como son el uso de dispositivos de USB (marca, modelo), búsqueda de archivos específicos, recuperación e identificación de correos electrónicos, recuperación de los últimos sitios visitados, recuperación del caché del navegador de Internet, etc.

Presentación:

Es el recopilar toda la información que se obtuvo a partir del análisis para realizar el reporte y la presentación a los abogados, la generación (si es el caso) de una pericial y de su correcta interpretación sin hacer uso de tecnicismos. (Martinez, 2012)

2.1.3 Herramientas de la informática forense:

Es aquel conjunto de programas o aplicaciones que se utilizan en diferentes sub áreas de la informática forense como lo es la esteganografía, la criptografía, recuperación de información, seguridad de correo electrónico, diagnóstico de discos duros, hackeo de redes etc.

Aquí se presenta una lista de aplicaciones de informática forense:

- Sleuth Kit (Forensics Kit).
- Py-Flag (Forensics Browser).
- Autopsy (Forensics Browser for Sleuth Kit).
- dcfldd (DD Imaging Tool command line tool and also works with AIR).
- foremost (Data Carver command line tool).
- Air (Forensics Imaging GUI).
- md5deep (MD5 Hashing Program).
- netcat (Command Line).
- cryptcat (Command Line).
- NTFS-Tools.

- Hetman software (Recuperador de datos borrados por los criminales).
- qtparted (GUI Partitioning Tool).
- regviewer (Windows Registry).
- Viewer.
- X-Ways Win Trace.
- X-Ways Win Hex.
- X-Ways Forensics.
- R-Studio Emergency (Bootable Recovery media Maker).
- R-Studio Network Edition.
- R-Studio RS Agent.
- Net resident.
- Faces.
- Encase.
- Snort.
- Helix.

Herramientas para el análisis de discos duros

- Access Data Forensic Tool Kit (FTK).
- Guidance Software EnCase.

Herramientas para el análisis de correos electrónicos

- Paraben.

Herramientas para el análisis de redes

- E-Detective-Decision Computer Group
- Silent Runner-Access data.
- Herramientas para filtrar y monitorear el tráfico de una red tanto interna como a internet.

Herramientas para el análisis de USB

- USBDeview (Forense, 2012)

2.1.4 Usos de la informática forense:

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense:

- **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, divorcio, pueden ser ayudados por la informática forense.
- **Investigación de Seguros:** La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.

- **. Temas corporativos:** Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial. (Giovanni Zuccardi, 2010)
- **Código Procesal Penal:** Es el conjunto de normas jurídicas correspondientes al derecho público interno que regulan cualquier proceso de carácter penal desde su inicio hasta su fin entre el estado y los particulares tienen un carácter primordial como un estudio de una justa e imparcial administración de justicia.
- **Ley Antiterrorismo en el Código Procesal Penal:** En el artículo número 12 literal A y B se hace constar que a la persona se le considerará víctima en caso de ser ofendida y en el caso de que la ofensa cause la muerte de la víctima.
- **Ley de comunicación Privada:** En los artículos 184,185,186,187 se hace constar que la persona que sea víctima de robo y logre recuperar el objeto que le ha sido robado deberá presentarlo delante del tribunal correspondiente si así lo requiere.

Herramientas de investigación forense:

En la actualidad existen cientos de herramientas las cuales se pueden clasificar en cuatro grupos principales.

Herramientas para la recolección de evidencia:

Existen una gran cantidad de herramientas para recuperar evidencia. El uso de herramientas sofisticadas se hace necesario debido a:

- La gran cantidad de datos que pueden estar almacenados en un computador.

- La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
- Limitaciones de tiempo para analizar toda la información.
- Facilidad para borrar archivos de computadores.
- Mecanismos de inscripción, o de contraseñas.

Encase: Es un ejemplo de herramientas de este tipo. Desarrollada GUI dance Software Inc permite asistir al especialista forense durante el análisis de un crimen digital.

Se escogió mostrar esta herramienta por tratarse del software líder en el mercado, el producto más ampliamente difundido y de mayor uso en el campo del análisis forense.

Herramientas para el monitoreo y control de computadoras

KeyLogger: Es una herramienta que pertenece a esta categoría. Puede ser útil cuando se quiere comprobar actividad sospechosa; guarda los eventos generados por el teclado, por ejemplo, cuando el usuario teclea la tecla de retroceder, esto es guardado en un archivo o enviado por email. Los datos generados son complementados con información relacionada con el programa que tiene el foco de atención, con anotaciones sobre las horas, y con los mensajes que generan algunas aplicaciones.

Herramientas de marcado de documentos

Un aspecto interesante es el de marcado de documentos; en los casos de robo de información, es posible, mediante el uso de herramientas, marcar software para poder detectarlo fácilmente.

El foco de la seguridad está centrado en la prevención de ataques. Algunos sitios que manejan información confidencial o sensitiva, tienen mecanismos para validar el ingreso, pero debido a que no existe nada como un sitio 100% seguro, se debe estar preparado para incidentes.

Herramientas de Hardware

Debido a que el proceso de recolección de evidencia debe ser preciso y no debe modificar la información se han diseñado varias herramientas como DIBS Portable Evidence Recovery Unit (Evidencia Portable Unidad de Recuperación).

DIBS Portable Evidence Recovery Unit el cual es un software utilizado como herramienta digital de informática forense para resolver problemas de hardware en computadoras de escritorio y laptops. (Oscar Lopez, 2012)

Las herramientas de hardware son muy populares en el mercado de la informática forense, ya que existen empresas de sólido prestigio que se dedican a la comercialización de estas herramientas, como por ejemplo Guidance Software que distribuye los siguientes productos principales:

- Encase Forensic.
- Encase FIM /Encase Forensic for consultants.
- Encase Enterprise /Encase ediscovery.
- Encase Portable.
- Fastbloc3 FE.
- Encase Neutrino.

Además de estas herramientas de hardware, también se puede mencionar el uso de un laboratorio de informática forense.

Este laboratorio de informática forense es móvil, que permite realizar labores de adquisición, investigación y análisis de evidencias digitales con equipos de última tecnología, como duplicadores forenses de alta velocidad, dispositivos de toma de imágenes forenses, bloqueadores de dispositivos, docking para discos duros, kit para recuperación de datos, estaciones forenses portátiles y de escritorio con software especializado de captura y análisis de evidencia, sistema de almacenamiento centralizado de evidencias digitales y una infraestructura virtual que soporta todas las labores del laboratorio.

2.5 Áreas principales de la Informática Forense

2.5.1 Criptografía

Es la parte 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 y codificado,

para hacerlos ininteligibles a intrusos que intercepten esos mensajes. Por tanto el único objetivo de la criptografía es 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.

Objetivos de la Criptografía

- Estudiar los algoritmos.
- Estudiar los Protocolos.
- Estudiar los sistemas de seguridad.

Características de la Criptografía

Confidencialidad

Es decir garantiza que la información esta 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 notaría electrónica.

La notarización electrónica es un registro de datos por una tercera parte fiable, quien da fe ulteriormente de la exactitud de los mismos y de algunos de sus atributos tales como contenido, origen, fecha, hora y emisor.

No repudio

Es decir proporciona protección frente a que algunas de las entidades implicadas en la comunicación, pueda negar haber participado en toda o parte de la comunicación. Para conseguirlo puede usar por ejemplo firma digital.

Autenticación

Es decir proporciona mecanismos que permiten verificar la identidad del comunicante. Para conseguirlo puede usar por ejemplo función hash criptográfica MAC o protocolo de conocimiento cero. (Talens, 2012)

Tipos de Criptografías

Criptografía simétrica

Agrupar aquellas funcionalidades criptográficas que se apoyan en el uso de una sola clave para encriptar y desencriptar de un mensaje, esta clave se debe intercambiar entre los equipos por medio de un canal seguro, ambos extremos deben tener la misma clave para cumplir con el proceso.

Criptografía de clave pública o criptografía asimétrica

Agrupar aquellas funcionalidades criptográficas que se apoyan en el uso de parejas de claves compuestas por una clave pública, que sirve para cifrar, y por una clave privada, que sirve para descifrar.

Criptografía con umbral

Agrupar aquellas funcionalidades criptográficas que se apoyan en el uso de un umbral de participantes a partir del cual se puede realizar la acción.

Criptografía basada en identidad

Es un tipo de criptografía asimétrica que se basa en el uso de identidades. (Jose Pastor Franco, 2001)

2.5.2 Esteganografía

Es la parte de la criptografía en la que se estudian y aplican técnicas que permiten el ocultamiento de 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 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.

Funcionamiento de la Esteganografía

La esteganografía tiene la función específica de enviar un mensaje oculto dentro de otro que servirá de camuflaje cuando se envíe por un canal inseguro y pueda ser visto por el guardián sin problemas aplicando la función inversa puede recuperar el mensaje oculto. (Molina, 2012)

2.5.3 Recuperación de información

Es la ciencia de la búsqueda de información en documentos electrónicos y cualquier tipo de colección documental digital, encargada de la búsqueda dentro de estos mismos, búsqueda de metadatos que describan documentos, o también la búsqueda en bases de datos relacionales, ya sea a través de internet, intranet, y como objetivo realiza la recuperación en textos, imágenes, sonido o datos de otras características, de manera pertinente y relevante.

La recuperación de información es considerada como un instrumento científico ya que tiene una característica en común con los demás instrumentos científicos y es que sirve para buscar, adquirir, medir, observar y almacenar datos reproducibles y verificables.

Aplicaciones de la recuperación de datos en informática forense

- Discos duros de desktop y laptop.
- Dispositivos USB.
- Dispositivos de almacenamiento extraíble o CD.

- Servidores.
- Bases de datos.
- Redes Sociales.
- Redes informáticas. (Journal, 2012)

2.5.4 Hackeo de redes Wireless

Se refiere a la acción de explorar y buscar las limitantes de un código o de una máquina. También significa acción de irrumpir o entrar de manera forzada a un sistema de cómputo o a una red.

Es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), esta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos.

Una de sus principales ventajas es notable en los costos, ya que se elimina todo el cable Ethernet y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe tener una seguridad mucho más exigente y robusta para evitar a los intrusos.

En la actualidad las redes inalámbricas son una de las tecnologías más prometedoras. (Hackeo, 2012)

2.2 Marco teórico de la solución

2.2.1 Manual de utilización del Kit de herramientas digitales de Informática Forense.

Es un instructivo o manual para el usuario que se desarrollará con el único objetivo de ayudar a los estudiantes a que puedan hacer un mejor uso de las herramientas digitales de Informática Forense que estarán al servicio del Laboratorio de Hardware cuando se realicen los seminarios de Informática Forense.

El manual tendrá información tanto teórica como práctica acerca de las herramientas digitales de Informática Forense y como utilizar cada una de las aplicaciones que contiene el kit según las necesidades del usuario en las diferentes áreas que se cubrirán como lo son la esteganografía, la criptografía, recuperación de información, diagnostico de discos duros, seguridad de redes, seguridad de correos electrónicos, diagnostico de USB etc.

Pasos para encriptar un archivo en Windows

buscar y seleccionar el archivo o carpeta a encriptar y dar clic derecho sobre él y seleccionar propiedades (ver imagen 1.1)

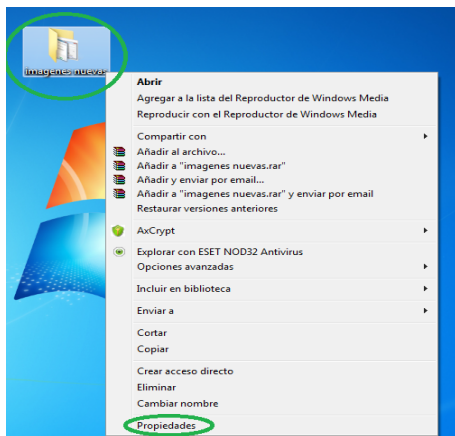


Imagen 1. 1

En la ficha general, haga clic en avanzadas. (ver imagen 1.2)

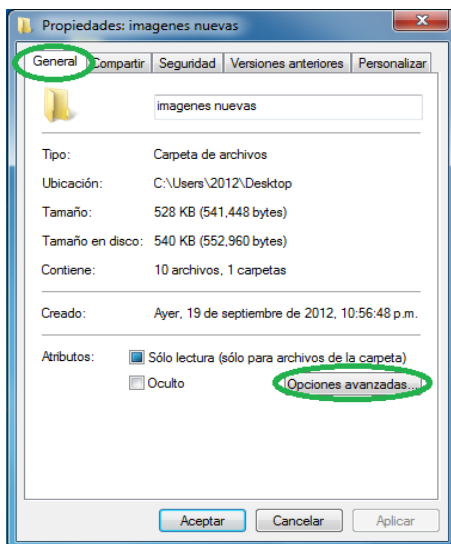


Imagen 1. 2

En atributos de compresión y cifrado active la casilla de verificación cifrar contenido para proteger datos y, a continuación, haga clic en aceptar. Con las siguientes configuraciones en los atributos de índice y archivo histórico se lograra que la búsqueda sea clasificada y ordenada y permita acelerar la búsqueda y en punto atributos de compresión esta opción permite de una sola vez proteger los archivos cifrándolos en el mismo paso (ver imagen 1.3)

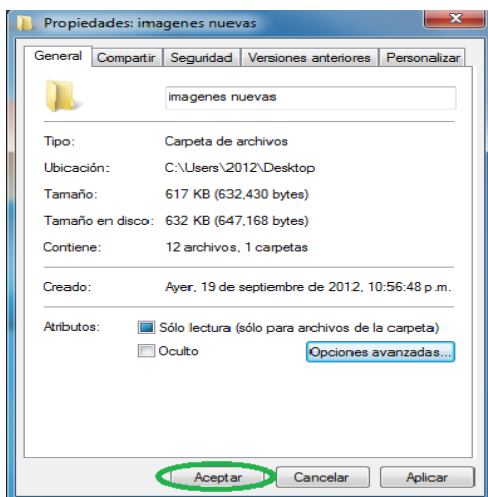


Imagen 1. 3

Haga clic en aceptar. Para continuar (ver imagen 1.4)

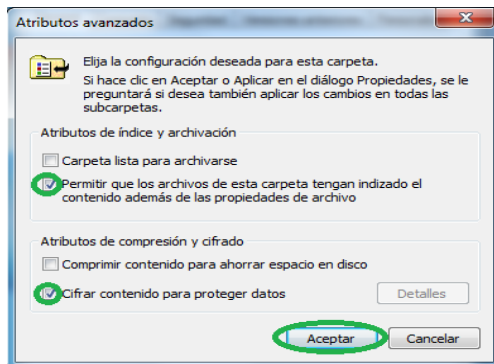


Imagen 1. 4

- Recibirás una advertencia la cual indicara que tipo de encriptación se ejecutara si deseas que solo se encripte la carpeta que seleccionaste con sus archivos o si deseas encriptar la carpeta y subcarpetas y los archivos en esta explicación elije la opción aplicar cambios a esta carpeta y a todas las subcarpetas y archivos y el proceso de encriptar lo ejecutara Windows (ver imagen 1.5)

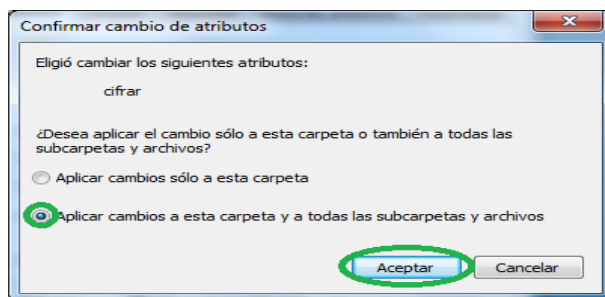


Imagen 1. 5

- Cuando ya sea ejecutado la encriptación de dicha carpeta y archivos se podrá visualizar que dicha carpeta y contenido sus nombres cambio a color verde esto indica que esta encriptado (ver imágenes 1.6 - 1.7)

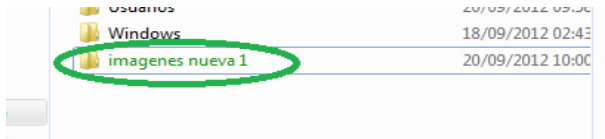


Imagen 1. 6

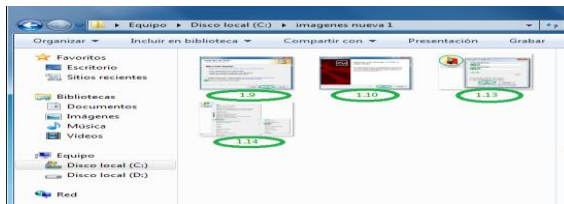


Imagen 1. 7

Los beneficios de encriptar un archivo en Windows se muestra a continuación:

- Encriptar en Windows permite que los demás usuarios no puedan visualizar los archivos (ver imágenes 1.8 – 1.9 – 1.10)

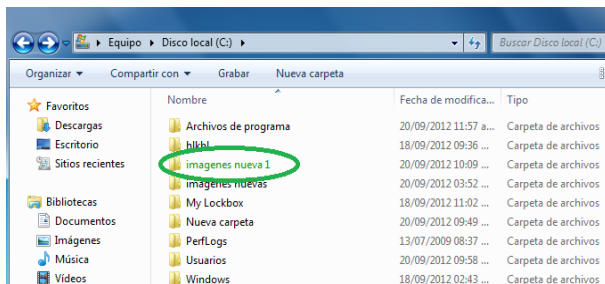


Imagen 1. 8

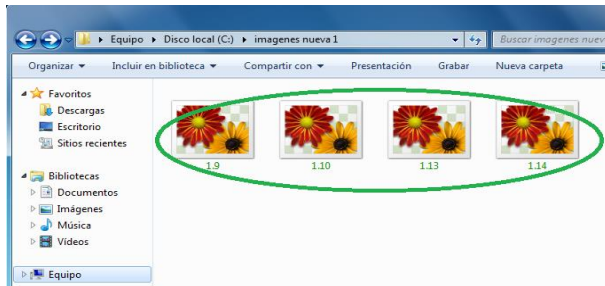


Imagen 1. 9

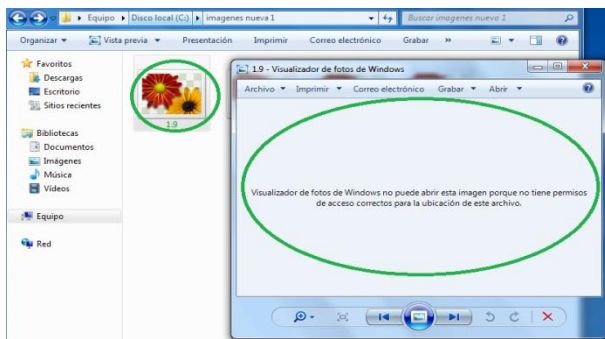


Imagen 1. 10

Pasos para descriptar archivos en Windows

- Seleccionar la carpeta o archivo encriptado y dar clic derecho sobre seleccionar propiedades (ver imagen 1.11)

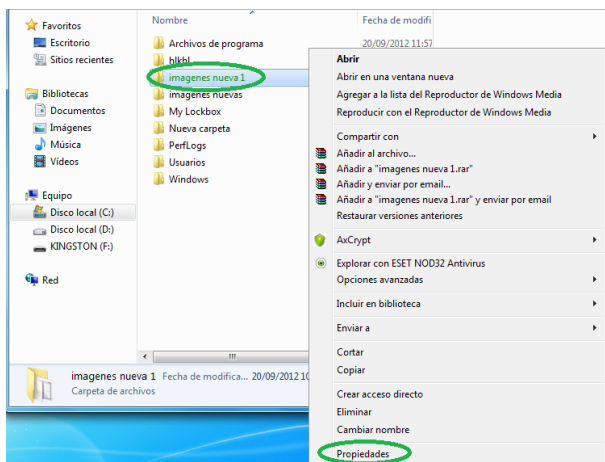


Imagen 1. 11

En la ficha general, haga clic en avanzadas. (ver imagen 1.12)

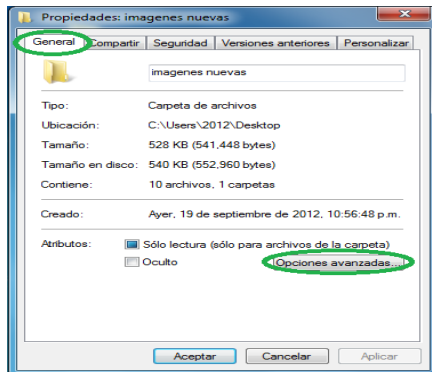


Imagen 1. 12

En los atributos avanzados deselecciona la opción cifrar contenido para proteger datos y dar clic en aceptar (ver imagen 1.13)

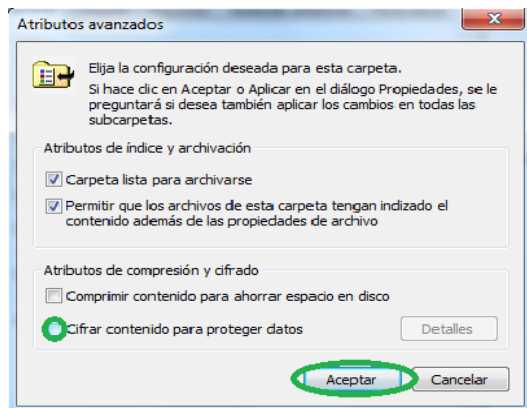


Imagen 1. 13

- Podrás visualizar que la carpeta y archivos el nombre regresa a su color original negro esto indica q la carpeta y archivos ya no están encriptados (ver imagen 1.14)

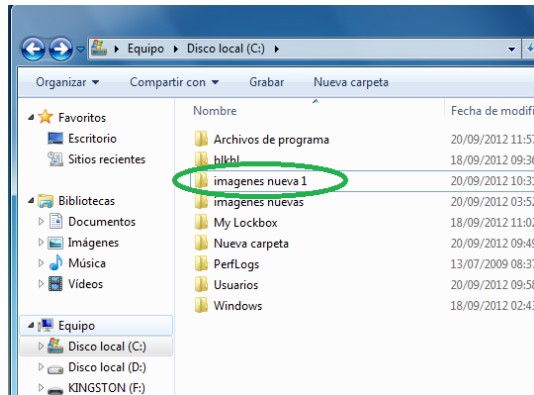


Imagen 1. 14

Pasos para encriptar un archivo usando el software Axcrypt

Encriptar:

Para saber que es la encriptación informática, primero se define lo que es la encriptación. Encriptar es una manera de codificar la información para protegerla frente a terceros.

Por lo tanto la encriptación informática sería la codificación de la información de archivos o de un correo electrónico para que no pueda ser descifrado en caso de ser interceptado por alguien mientras esta información viaja por la red.

Es por medio de la encriptación informática como se codifican los datos. Solamente a través de un software de decodificación que conoce el autor de estos documentos encriptados es como se puede volver a decodificar la información.

- Descarga la aplicación Axcrypt de internet en tu computadora. Desde este link <http://www.axantum.com/axcrypt/Downloads.html>
- En el menú que se le despliega al ingresar a la página de descarga Seleccionar 32 o 64bit y esperar a que se descargue por completo la aplicación en su computadora (ver imagen 1.15)

Main Downloads

If you are [logged on](#), you have access to more downloads!

OS Type	Download	Description	Type
32- or 64-bit	AxCrypt-1.7.2931.0-Setup.exe	AxCrypt Encryption	Setup w/OpenCandy
32- or 64-bit	AxDecrypt.exe	AxCrypt Decryption Only	Portable
Android 1.6+	XecretsDroidView-2678.apk	Xecrets Password Manager	App
32- or 64-bit	Xecrets2Go.exe	Xecrets Password Manager	Portable

Imagen 1. 15

Instala la aplicación en tu computadora siguiendo estos pasos:

- Ejecutar el programa dar clic en yo acepto, al aceptar estará firmando un contrato que el cual está sujeto a las políticas de uso del software a instalar para continuar con la instalación (ver imagen 1.16)

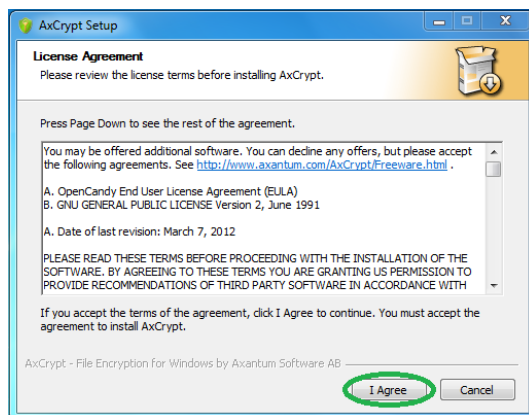


Imagen 1. 16

- Seleccionar no quiero instalar Nitro Pdf Reader porque ese programa no interesa por el momento debido a que es una aplicación adicional que el creador a agregado lo cual por el momento no está con fines de resolver el problema por el cual no se instalara dicho programa y dar clic en Instalar para continuar con la instalación (ver imagen 1.17)

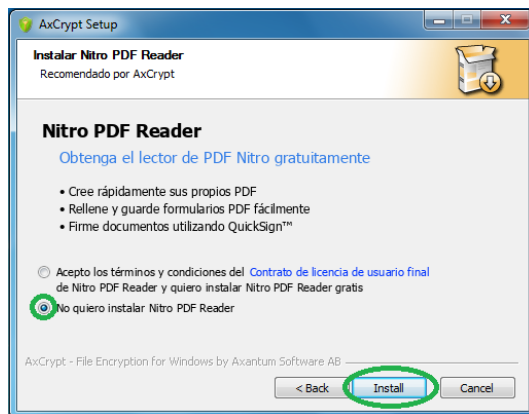


Imagen 1. 17

- Esperar que el programa instale todos los archivos y registros necesarios en la computadora para poder empezar a usarlo (ver imagen 1.18)

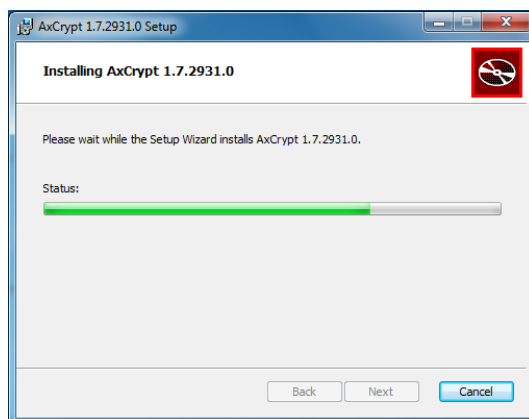


Imagen 1. 18

- Quitar el cheque de Registrar debido a que el software que se está instalando es versión libre y no requiere licencia y no es necesario registrarse. Luego dar clic en Finalizar para terminar con la instalación (ver imagen 1.19)

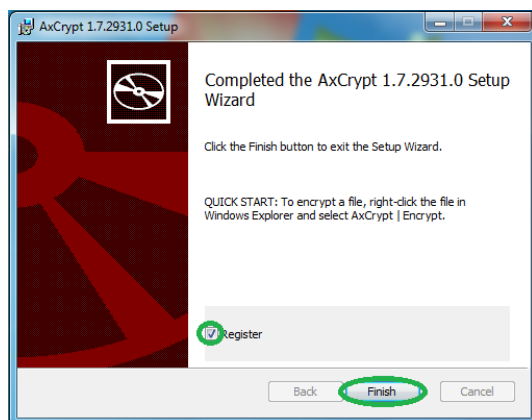


Imagen 1. 19

Pasos para Usar Axcrypt

- Haz clic derecho sobre el archivo a encriptar y seleccionas la opción Axcrypt. (ver imagen 1.20)

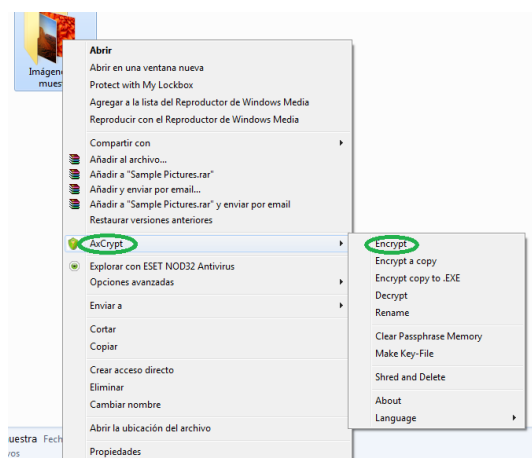


Imagen 1. 20

- Al estar dentro de la aplicación ingresa la contraseña que deseas utilizar pueden ser números o palabras para codificar el fichero y haz clic en aceptar para comenzar la encriptación de un fichero. (ver imagen 1.21)

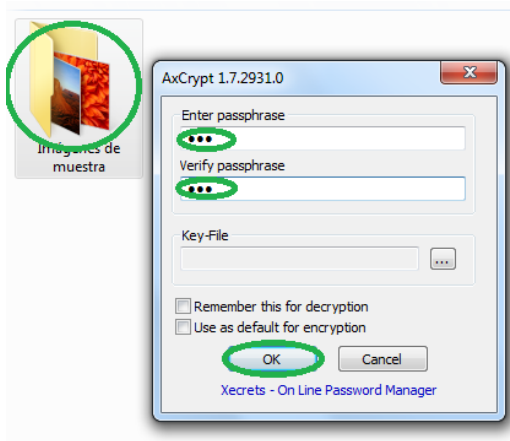


Imagen 1. 21

- Puedes visualizar como el programa empieza a codificar cada uno de los archivos (ver imagen 1.22)

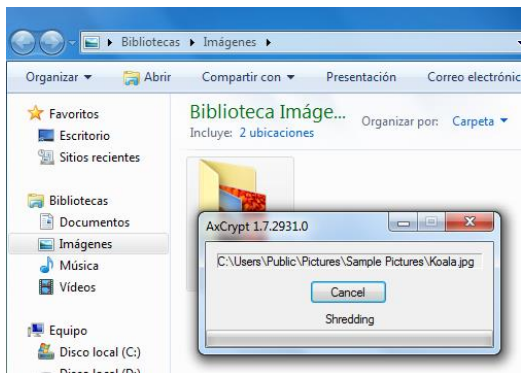


Imagen 1. 22

- Así quedara la carpeta y archivos ya encriptados (ver imágenes 1.23 – 1.24)



Imagen 1. 23

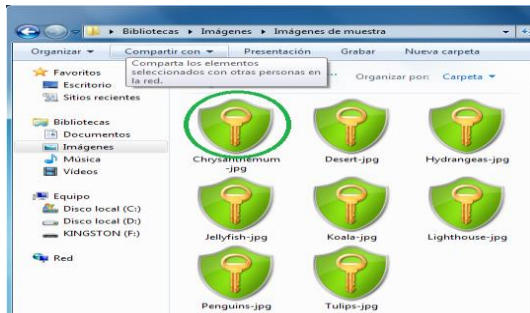


Imagen 1. 24

Los beneficios que el usuario obtiene al encriptar con Axcrypt se muestran a continuación:

- Al encriptar ya sea un archivo o una carpeta completa se puede visualizar que ningún usuario que no contenga la clave personal podrá visualizar los archivos ya que al intentar abrir el archivo pedirá la clave de encriptación (ver imagen 1.25)

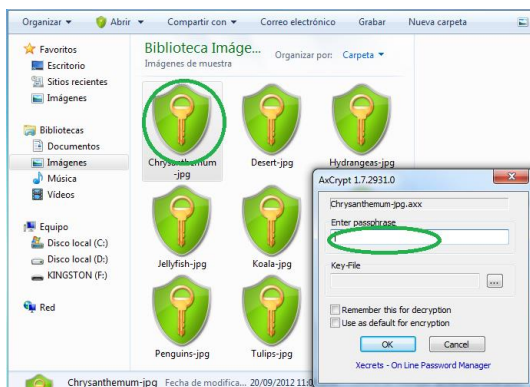


Imagen 1. 25

Pasos para decodificar un archivo

- Ir a la carpeta o archivo encriptados y dar clic derecho sobre él, dirigirse a la opción axcrypt y luego a la opción decrypt (ver imagen 1.26)

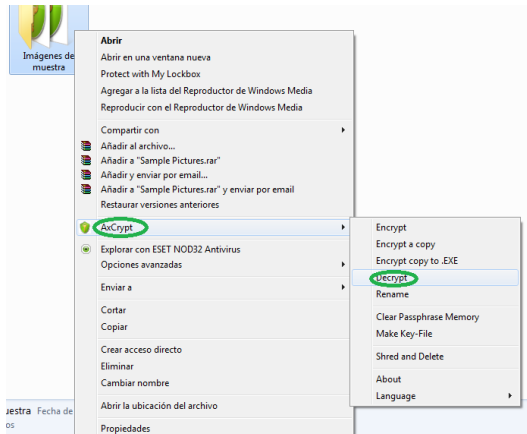


Imagen 1. 26

- Escribir dicha contraseña y dar clic en OK para desencriptar el archivo (ver imagen 1.27)

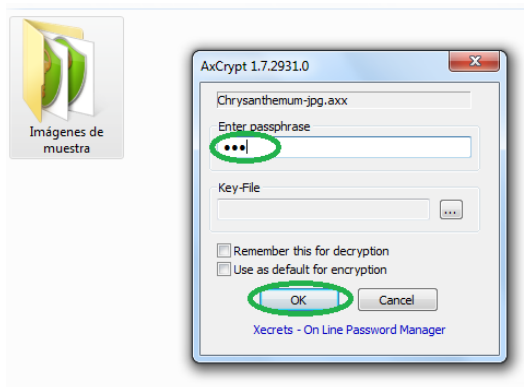


Imagen 1. 27

Pasos para ocultar mensajes usando esteganografía

Métodos de sustitución

El valor (11111111) es un número binario de 8 bits. Al bit ubicado más a la derecha se le llama bit menos significativo (LBS) porque es el de menor peso alterándolo cambia en la menor medida posible el valor total del número representado.

Un ejemplo de esteganografía: ocultamiento de la letra A. Si se tiene parte de una imagen con pixeles con formato RGB (3bytes), su representación original podría ser la siguiente (3pixeles, 9 bytes):

(11011010) (01001001) (01000011)

(00011110) (01011011) (11011111)

(00001110) (01000111) (00000111)

El mensaje a cifrar es A cuya representación ASCII es (10010111), entonces los nuevos pixeles alterados serian:

(1101101**1**) (0100100**0**) (0100001**0**)

(0001111**1**) (0101101**0**) (1101111**1**)

(0000111**1**) (0100011**1**) (0000011**1**)

Observar que se ha sustituido el bit del mensaje (letra A, marcados en negritas) en cada uno de los bits menos significativos de color de los 3 pixeles. Fueron necesarios 8 bytes para el cambio, uno por cada bit de la letra A, el noveno byte de color no se utilizó, pero es parte del tercer pixel (su tercera componente de color).

Pasos para ocultar archivos usando la aplicación My Lockbox

- Descarga la aplicación de internet desde este link <http://www.mediafire.com/?jltukhmmiaz> esperar que se descargue por completo el software en su computadora
- ejecute el programa desde el setup del instalador anteriormente descargado (ver imagen 1.28)

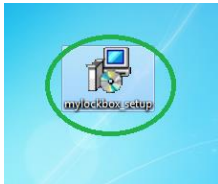


Imagen 1. 28

- dar clic en siguiente para continuar con la instalación (ver imagen 1.29)

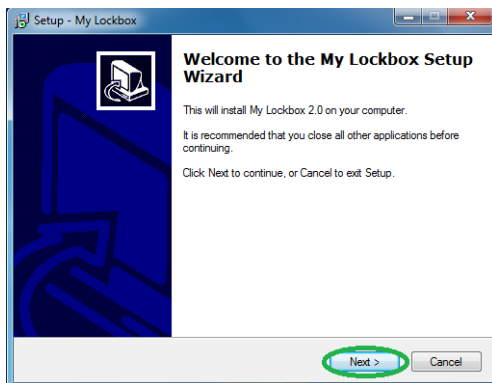


Imagen 1. 29

- Seleccionar acepto agregar en este paso esta aceptando los términos legales del uso apropiado de dicha aplicación para continuar con la instalación dar clic en siguiente (ver imagen 1.30)

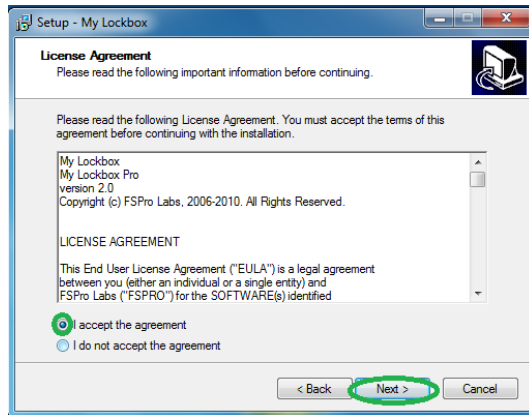


Imagen 1. 30

- Dar clic en siguiente no tocar la dirección de carpeta donde se instalara el programa para continuar con la instalación (ver imagen 1.31)

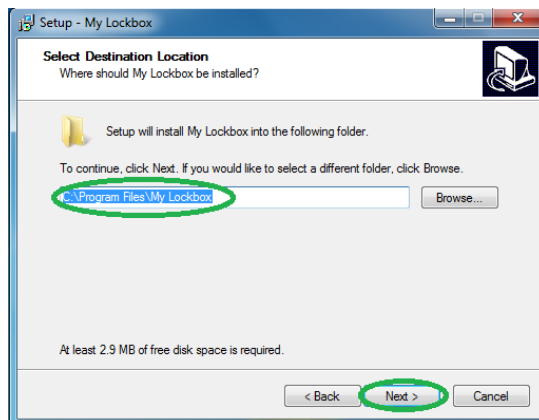


Imagen 1. 31

- Dar clic en siguiente para continuar con la instalación (ver imagen 1.32)

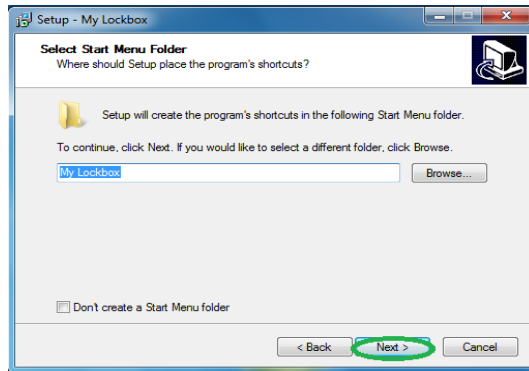


Imagen 1. 32

- Dar clic en instalar para continuar con la instalación (ver imagen 1.33)

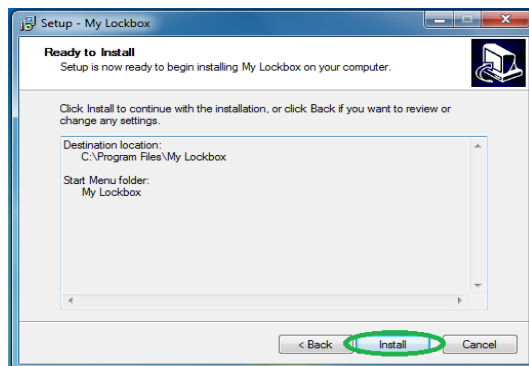


Imagen 1. 33

- Esperar q el programa instale los archivos necesarios en su computadora (ver imagen 1.34)

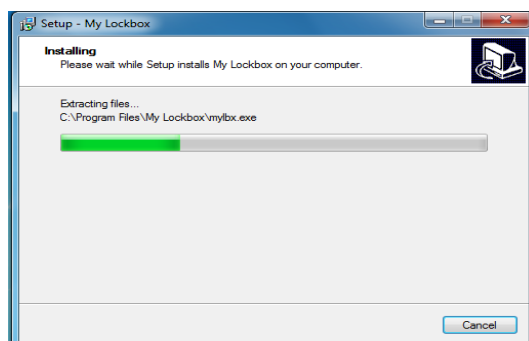


Imagen 1. 34

- Introducir la clave luego confirmar dicha clave y se podrá poner un indicio de dicha clave para futuros olvidos esto servirá para proteger el archivo o carpeta y al programa y que ningún usuario pueda desinstalar ni usar sin tener dicha contraseña, para continuar con la instalación dar clic en siguiente (ver imagen 1.35)

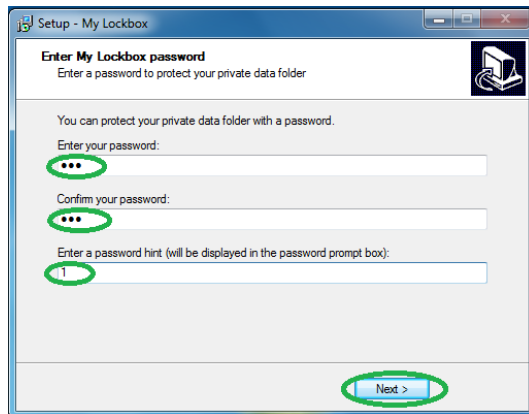


Imagen 1. 35

- Dar clic en siguiente para continuar con la instalación (ver imagen 1.36)

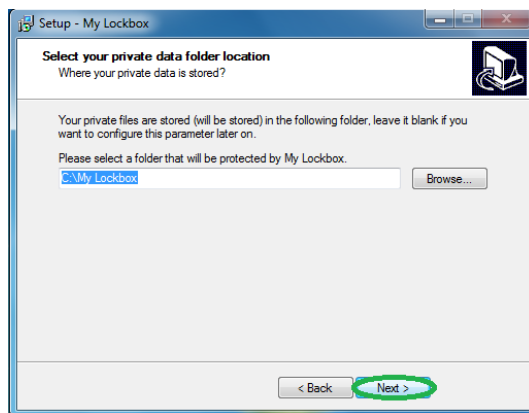


Imagen 1. 36

- Seleccionar la opción agregar protección a my Lockbox en menú de Windows dar clic en continuar para continuar con la instalación (ver imagen 1.37)

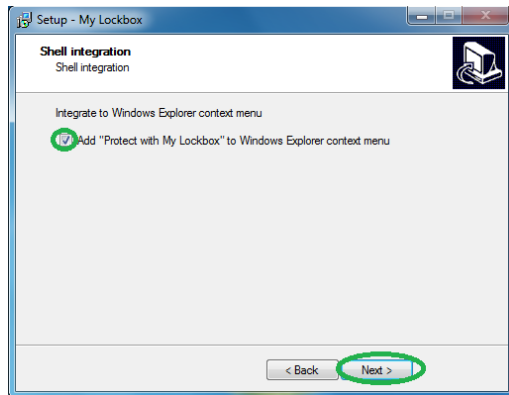


Imagen 1. 37

- Dejar seleccionada la opción permitir ver las notas del programa al ejecutarlo dar clic en siguiente para continuar (ver imagen 1.38)

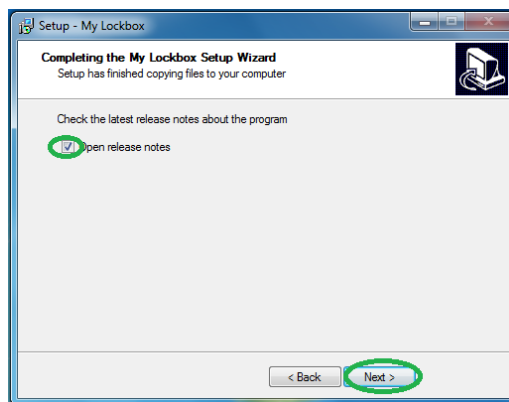


Imagen 1. 38

- Dar clic finalizar para terminar con el proceso de instalación (ver imagen 1.39)



Imagen 1. 39

Pasos para usar el programa

- Ejecuta el programa desde el icono, introduce la contraseña y dar clic en OK (ver imagen1.40)



Imagen 1. 40

- En el menú del programa selecciona la opción agregar luego selecciona el archivo o carpeta a ocultar y proteger de los demás usuario y clic en aceptar (ver imagen 1.41)



Imagen 1. 41

- Para poder ocultar y proteger el archivo o carpeta anteriormente seleccionar dar clic en proteger y automáticamente el archivo o imagen se ocultara de la vista normal (ver imagen 1.42)



Imagen 1. 42

- Al dar clic en proteger la imagen ya no aparece a la vista (ver imagen 1.43)



Imagen 1. 43

Beneficios al usar el programa My lockbox se muestran a continuación:

- Al usar este software permite poder proteger de cualquier usuario mal intencionado. Como pudieron visualizar en las imágenes anteriores este programa aparte de proteger los archivos con una contraseña también los oculta.

Pasos para decodificar y poder visualizar un archivo o carpeta con My lockbox:

- Ir al icono del programa y ejecutarlo introducir la contraseña y dar clic en ok y automáticamente el programa desprotege dicho archivo o carpeta (ver imagen 1.44)

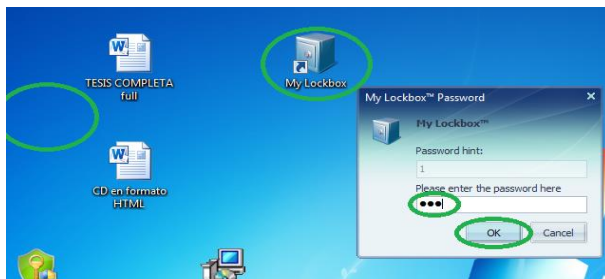


Imagen 1. 44

- Aquí la carpeta protegida ya es visible (ver imagen 1.45)

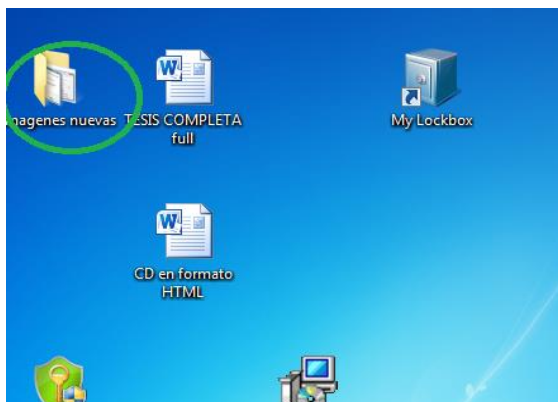


Imagen 1. 45

Pasos para recuperar archivos borrados con software Easy Drive Data Recovery 2.5

- Descarga la aplicación easy recovery profesional desde este link <http://depositfiles.com/files/pzjgtvsee> esperar a que descargue todo el software en tu computadora.
- Instalar el programa desde el setup y ejecutarlo para iniciar la instalación (ver imagen 1.46)



Imagen 1. 46

- Selecciona el idioma de tu conveniencia y dar clic en aceptar para continuar con la instalación (ver imagen 1.47)

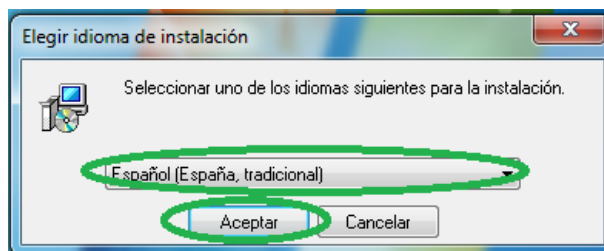


Imagen 1. 47

- Espera que el programa prepare la instalación este paso escanea el ordenador para comprobar que cumple con los requisitos mínimos para poder ser instalado (ver imagen 1.48)

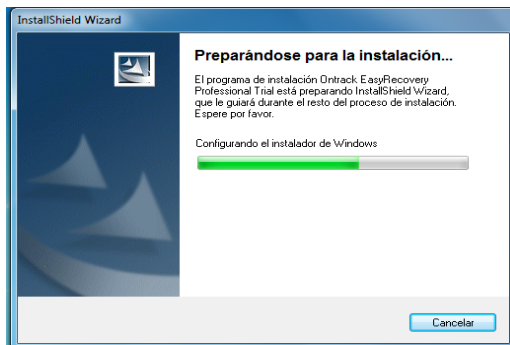


Imagen 1. 48

- Dar clic en siguiente para continuar con la instalación (ver imagen 1.49)

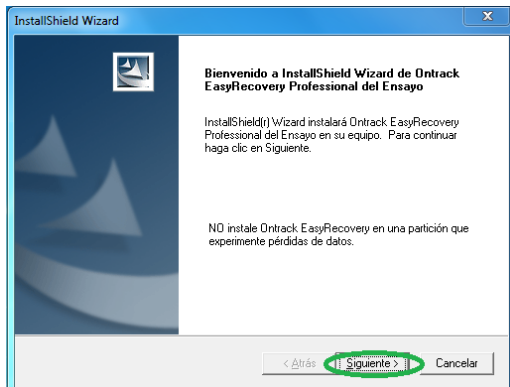


Imagen 1. 49

- Dar clic en acepto los términos legales de la licencia libre para poder usar dicho programa para continuar con la instalación (ver imagen 1.50)

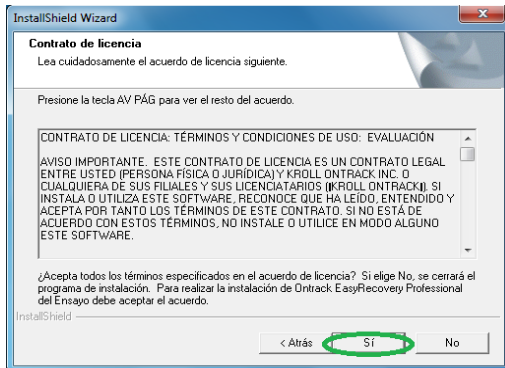


Imagen 1. 50

- Dar clic en siguiente para continuar con la instalación (ver imagen 1.51)

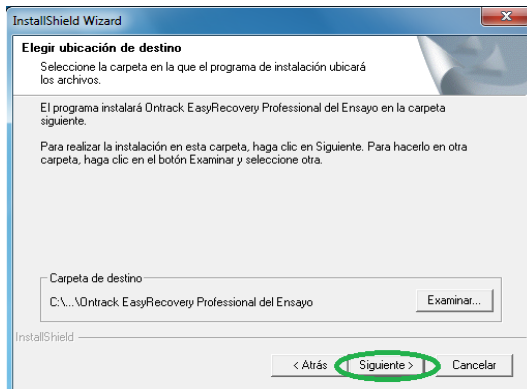


Imagen 1. 51

- No tocar la carpeta de destino de la instalación y Dar clic en siguiente para continuar con la instalación (ver imagen 1.52)

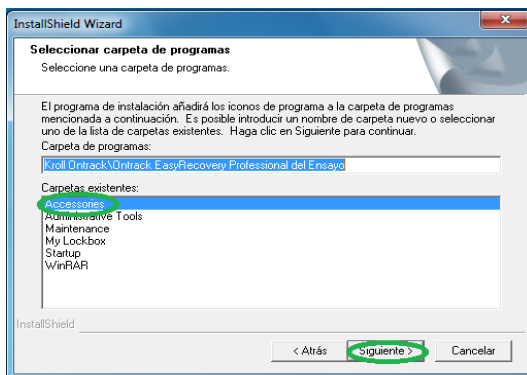


Imagen 1. 52

- Dar clic siguiente para continuar con la instalación (ver imagen 1.53)

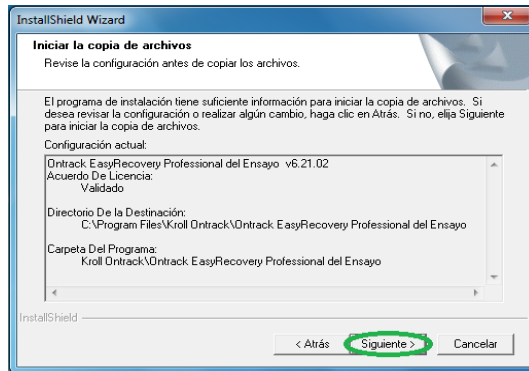


Imagen 1. 53

- Esperar que se ejecute la instalación ,instalara todos los archivos necesarios de dicho programa (ver imagen 1.54)

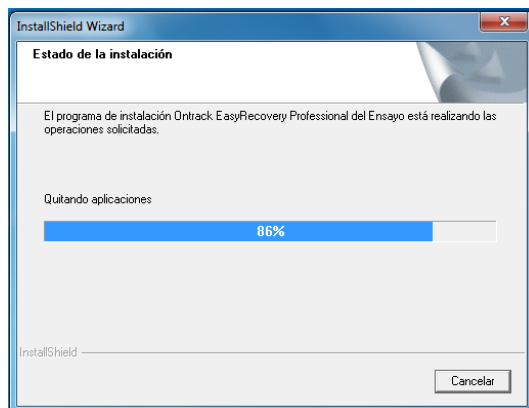


Imagen 1. 54

- Dar clic en finalizar para terminar con la instalación (ver imagen 1.55)

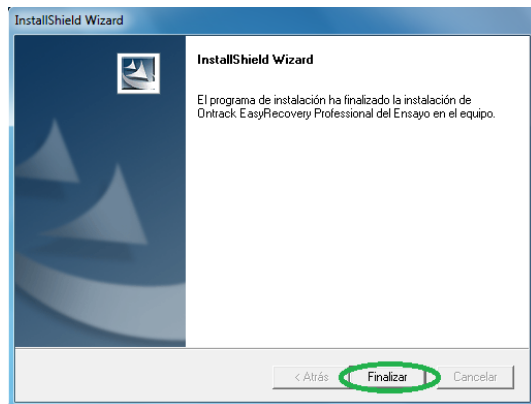


Imagen 1. 55

Pasos para utilizar el programa:

- Ejecutar el programa desde el icono para iniciar (ver imagen 1.56)



Imagen 1. 56

- Al abrir el programa seleccionar recuperación de datos y luego la opción recuperación avanzada. En este paso se explica en la opción recuperación de datos de un disco duro (ver imagen 1.57)



Imagen 1. 57

- Seleccionar la unidad de donde se quiere recuperar los datos, se seleccionara de la lista de la izquierda. (ver imagen 1.58)

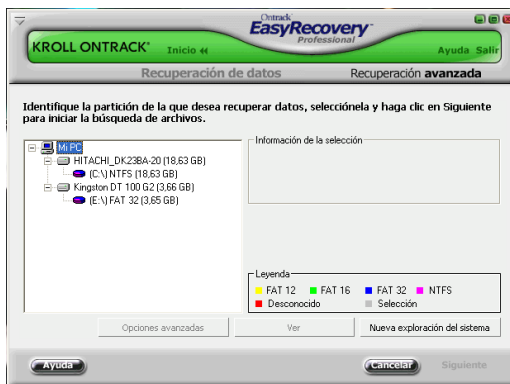


Imagen 1. 58

- Seleccionar opciones avanzadas y en la pestaña exploración de sistema de archivos elegir el sistema y luego seleccionar la opción exploración avanzada y elegir aceptar. (ver imagen 1.59)

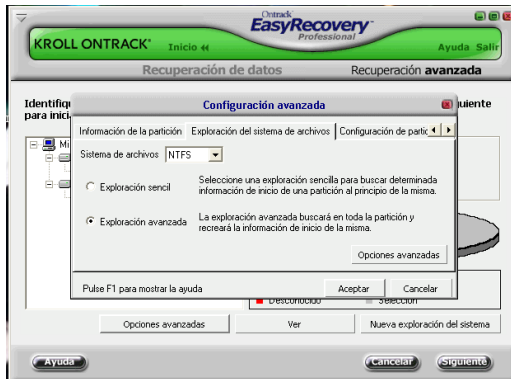


Imagen 1. 59

Ahora seleccionar la opción nueva exploración del sistema y presentara una advertencia donde dirá ¿desea explorar el sistema de nuevo? Y seleccionar sí. (ver imagen 1.60)

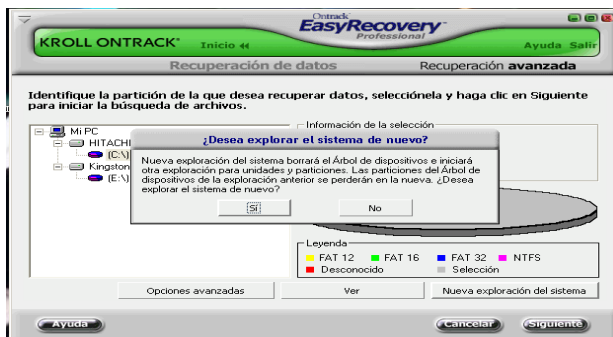


Imagen 1. 60

- Al finalizar el proceso mostrara una ventana con los archivos recuperados y pedirá una ubicación para copiarlos y con eso ya se han recuperado todos los archivos. (ver imagen 1.61)

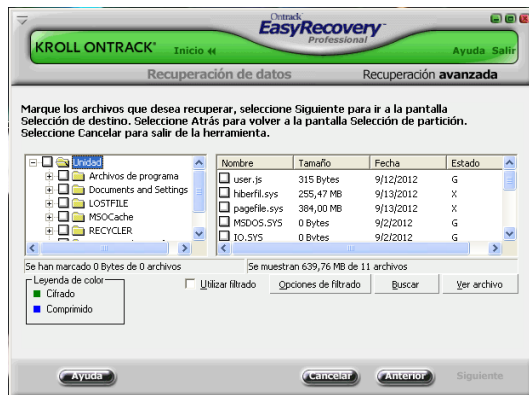


Imagen 1. 61

- Beneficio de usar easy recovery en la opción recuperar datos, opciones avanzadas, le permite al usuario en general poder recuperar en su totalidad información valiosa que fue eliminada o borrada accidentalmente por el usuario ya que permite recuperar información desde disco duros formateados, desde memorias extraíbles etc.

Pasos para diagnóstico de errores en partición de disco duros con Easy Recovery:

- Seleccione la opción diagnóstico de disco duro y luego la opción pruebas de particiones (ver imagen 1.62)



Imagen 1. 62

- Seleccione la partición a escáner error y dar clic en siguiente (ver imagen 1.63)

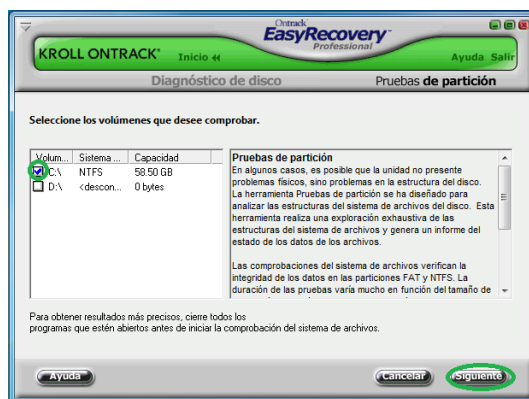


Imagen 1. 63

- En este momento el programa inicia el proceso de escaneo en el sistema y en la partición para detectar posibles problemas en la partición (ver imagen 1.64)

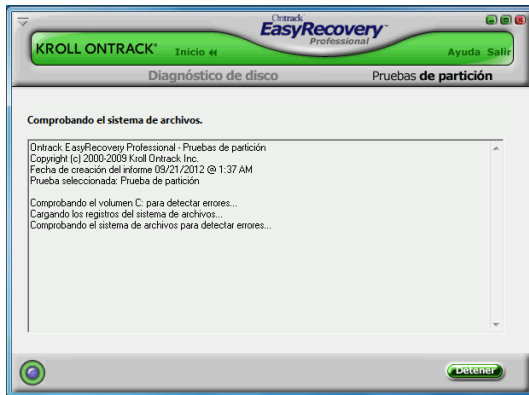


Imagen 1. 64

- Se ha terminado el proceso de escaneo de error en la partición lo cual ha dado un resultado negativo debido a que ha encontrado daños en los sectores de partición en esta opción permite guardar el diagnostico par futuras pruebas (ver imagen 1.65)

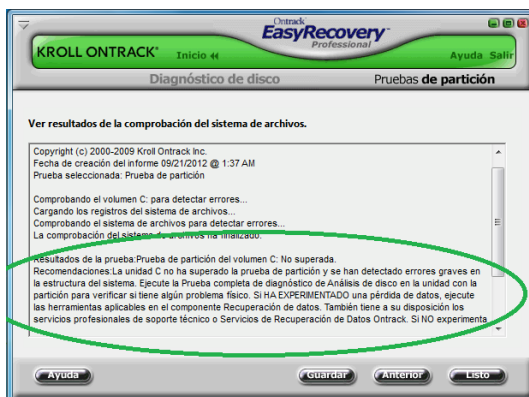


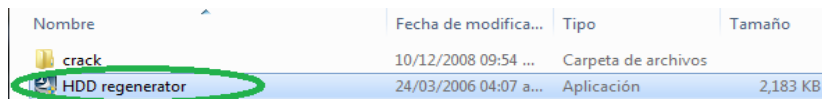
Imagen 1. 65

- Beneficio de usar la herramienta de escaneo de partición del easy recovery le permite al usuario ayudar a detectar posibles daños en los sectores de discos duros así poder hacer backup de información a tiempo y no perder los documentos.

Pasos para reparar sectores defectuosos de discos duros con software HDD Regenerator.

Pasos para descargar HDD Regenerator 1.51

- Descarga la aplicación HDD Regenerator 1.51 del link <http://www.gratisprogramas.org/descargar/hdd-regenerator-151-repara-hdd-danados-full/>
- Ejecutar el instalador de programa anteriormente descargado para iniciar la instalación (ver imagen 1.66)



Nombre	Fecha de modifica...	Tipo	Tamaño
crack	10/12/2008 09:54 ...	Carpeta de archivos	
HDD regenerator	24/03/2006 04:07 a...	Aplicación	2,183 KB

Imagen 1.66

- Dar clic en siguiente para continuar con la instalación (ver imagen 1.67)

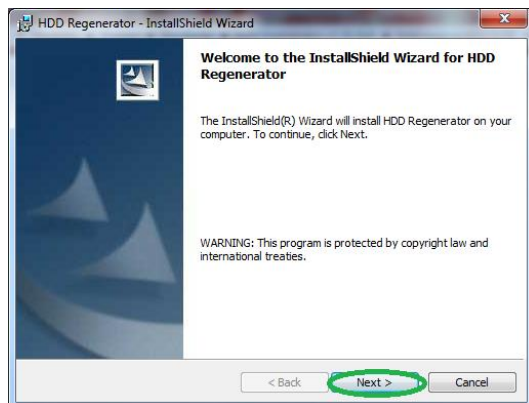


Imagen 1.67

- Clic en aceptar en este punto el usuario acepta los términos de la licencia y su uso respectivo del programa luego clic en siguiente para continuar con la instalación (ver imagen 1.68)

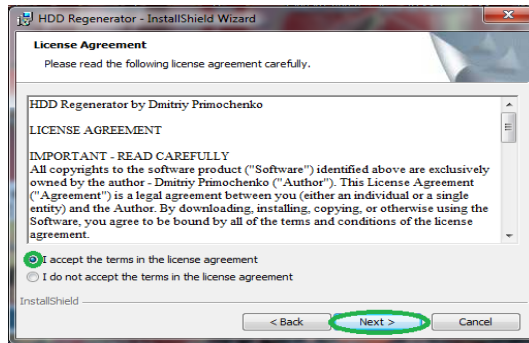


Imagen 1.68

- Dar clic en siguiente para que la aplicación ejecute todos sus archivos (ver imagen 1.69)

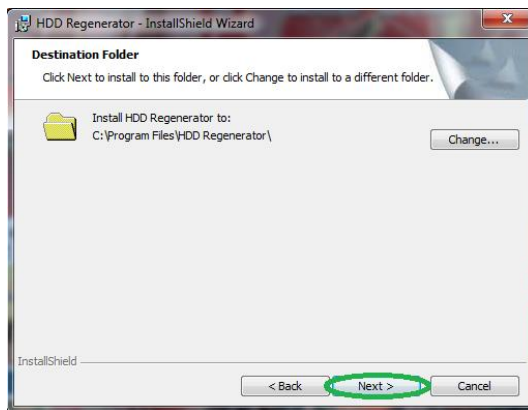


Imagen 1.69

- Esperar que el programa instale todos los archivos y registros en el ordenador y poder usar la aplicación (ver imagen1.70)

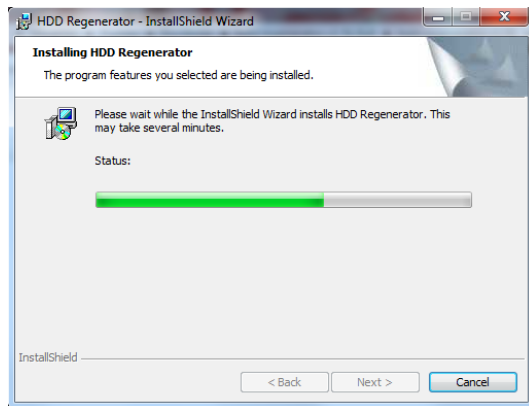


Imagen 1.70

- Dar clic en finalizar para terminar con la instalación del programa (ver imagen 1.71)

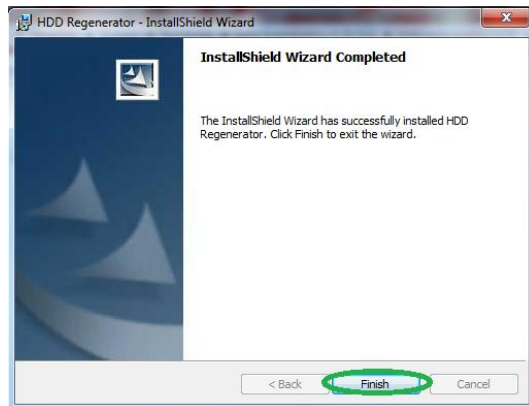


Imagen 1.71

Pasos para ejecutar crack

- Al terminar la instalación, ejecutar el crack para poder utilizar el programa full, dicho crack se encuentra en la carpeta de descarga del instalador de programa (ver imágenes 1.72 - 1.73)

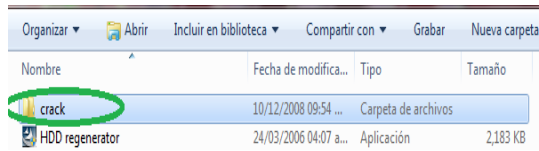


Imagen 1.72

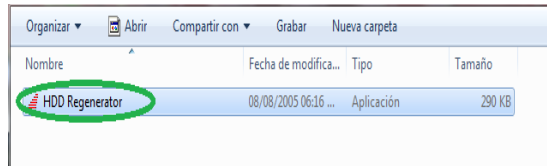


Imagen 1.73

- Copiar el crack al siguiente directorio: disco C: Archivos de Programa: HD Regenerator: dar pegar y luego saldrá un menú en el cual se copia y reemplaza el programa para estar completo (ver imagen 1.74)

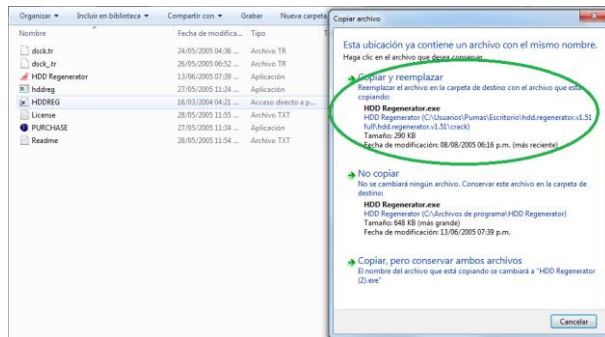


Imagen 1.74

- Ejecutar el crack para dejar el programa full el crack se encuentra en la carpeta del instalador del programa (ver imagen 1.75)

Nombre	Fecha de modifica...
 crack	10/12/2008 09:54 ...
 HDD regenerator	24/03/2006 04:07 a...
 link de descarga	13/10/2012 07:59 ...

Imagen 1.75

- Abrir la carpeta clic derecho y copiar (ver imagen 1.76)

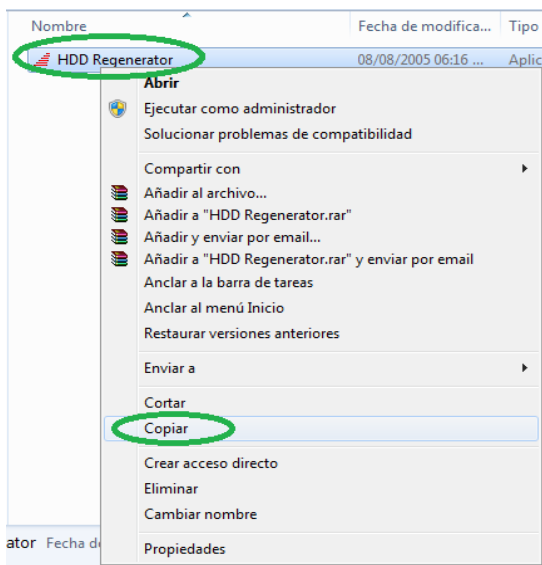


Imagen 1.76

- Buscar la carpeta donde se instalo anteriormente el programa en la siguiente dirección :
disco local C: archivos de programa: HDD Regenerator y copiar el archivo a la carpeta del instalador (ver imágenes 1.77 – 1.78 – 1.79)

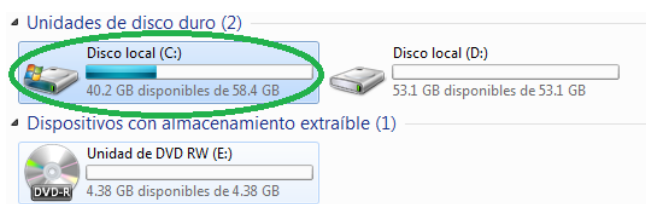


Imagen 1.77

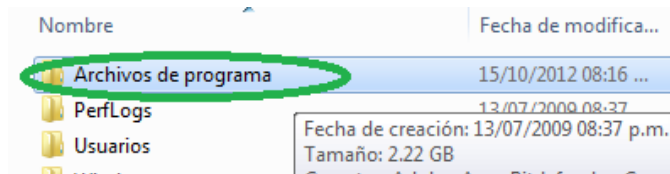


Imagen 1.78

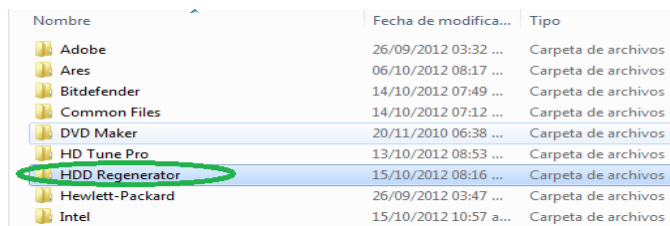


Imagen 1.79

- Al copiar el archivo en la carpeta de instalador saldrá una ventana con un menú en el cual elegir la opción copiar y reemplazar el archivo (ver imagen 1.80)

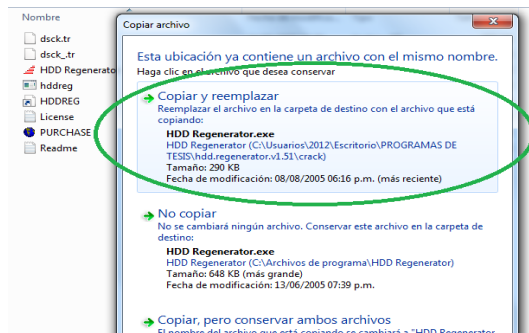


Imagen 1.80

- Al seleccionar la opción copiar y reemplazar el archivo ya existente saldrá una ventana con la advertencia de permisos de administrador dar clic en continuar para reemplazar el archivo y poder dejar full el programa (ver imagen 1.81)

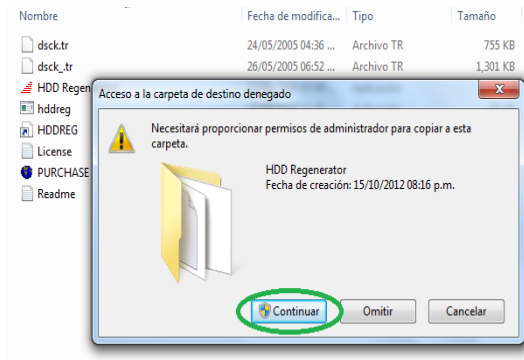


Imagen 1.81

Pasos para usar HDD Regenerator 1.51

Ejecutar el programa desde el icono que aparece en el escritorio (ver imagen 1.82)



Imagen 1.82

- En el menú del programa elije la opción crear un cd booteable. En este paso el programa quemará los archivos necesarios a un CD para poder utilizar HDD Regenerator. (Ver imagen 1.83)

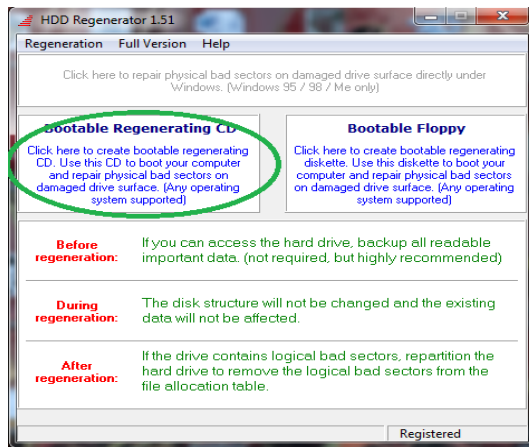


Imagen 1.83

- Seleccionar la unidad de DVD ROM donde insertar un CD en blanco donde se grabarán los archivos luego dar clic en ok para iniciar la copia de los archivos a CD.
(Ver imagen1.84)

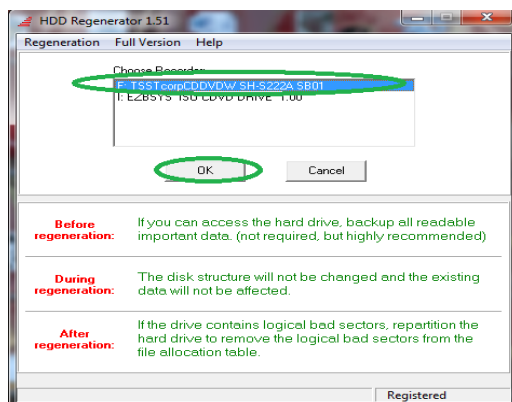


Imagen 1.84

- Para continuar seleccionar la velocidad de lectura a la cual será grabado en cd anteriormente seleccionado elegir la velocidad de 8x y dar clic en grabar cd (burn cd)
(ver imagen 1.85)

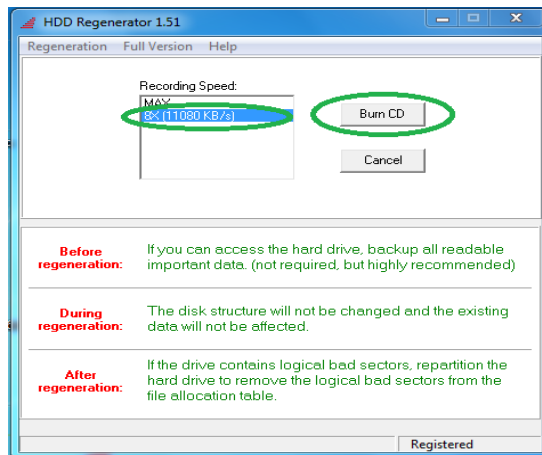


Imagen 1.85

- Teniendo ya grabado los archivos necesarios de programa hdd regenerator hizo el cd booteable ahora reiniciar la pc y botear con el cd, se desplegara el menú de hd regenerar (ver imagen 1.86)
1. Escanear (detecta zonas malas)
 2. Escañero norma mente (luego reparar)
 3. Información
 4. Ver estadísticas

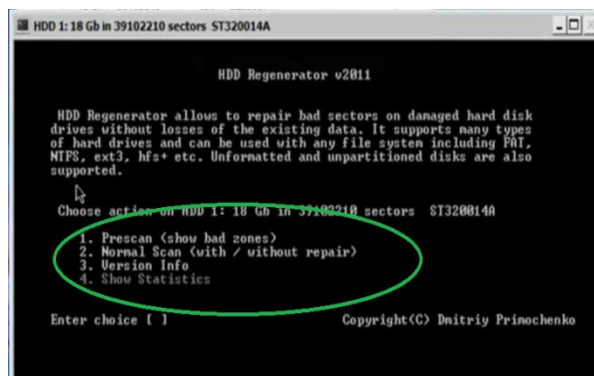


Imagen 1.86

- Elegir la opción mas adecuada a su necesidad, tecla el numero de menú y dar enter (1)
enter (ver imagen 1.87)

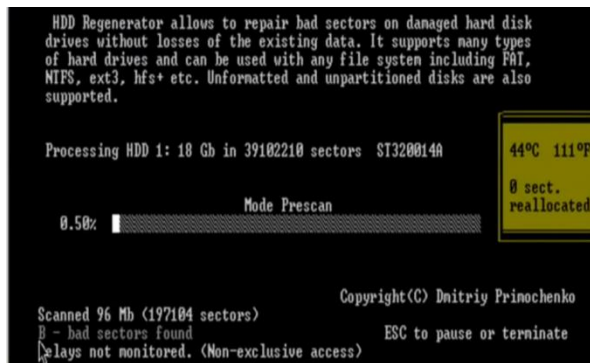


Imagen 1.87

- Al finalizar si detecta algún sectores dañados se desplegara otro menú y seleccionarme la opción 1 para que inicie el proceso de reparación (ver imagen 1.88)

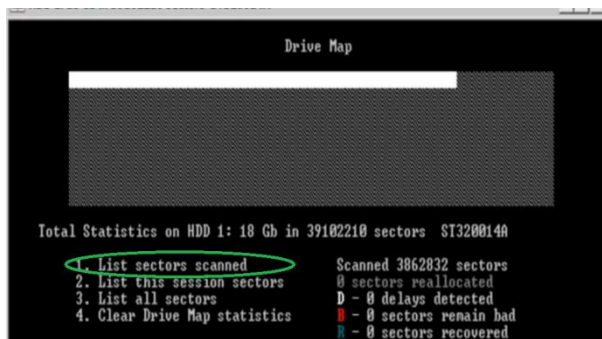


Imagen 1.88

Beneficios de usar el programa HDD Regenerator 1.5

- Usar la aplicación HDD Regenerator permite al usuario reparar los sectores dañados en su disco duro y además recupera la información guardada en el disco duro de sectores defectuosos

Pasos para instalar HD tune pro 4.6

- Descarga la aplicación HD Tune pro 4.6 desde el link

<http://depositfiles.com/files/r7070gx3o%20>

- Ejecutar el instalador de programa anteriormente descargado para iniciar la instalación (ver imagen 1.89)

Nombre	Fecha de modifica...	Tipo	Tamaño
HD Tune Pro 460	15/11/2010 12:28 a...	Carpeta de archivos	
HDtunepro_460_trial	30/08/2010 06:34 ...	Aplicación	1,408 KB
Patch	31/08/2010 10:47 a...	Aplicación	839 KB

Imagen 1.89

- Para iniciar la instalación hacer clic en continuar para seguir con la instalación (ver imagen 1.90)

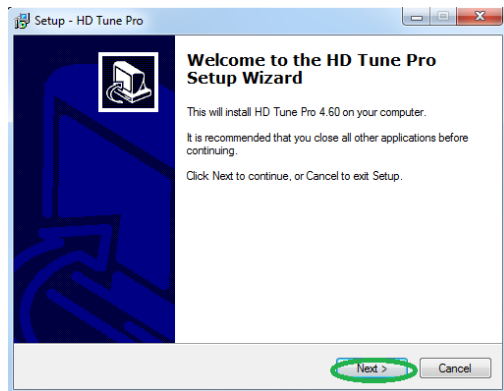


Imagen 1.90

- Seleccionar aceptar en este punto se acepta los términos de la licencia y su uso adecuado luego dar clic en siguiente para continuar con la instalación (ver imagen 1.91)

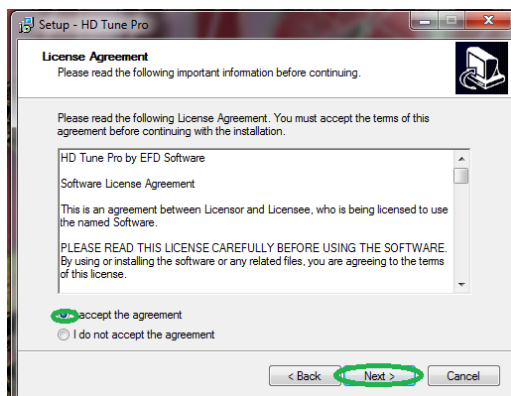


Imagen 1.91

- Dar clic en siguiente para continuar con la instalación en este paso se selecciona la carpeta de destino donde se ubicara el programa (ver imagen 1.92)

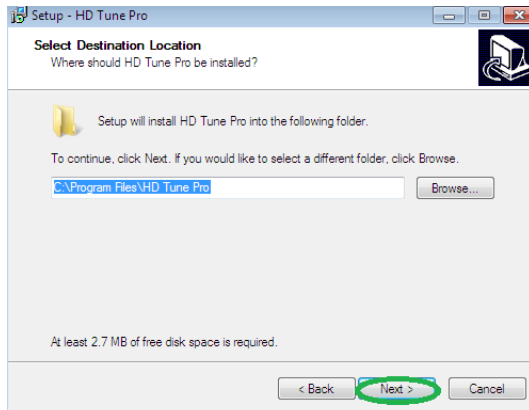


Imagen 1.92

- Dar clic en siguiente para continuar con la instalación (ver imagen 1.93)

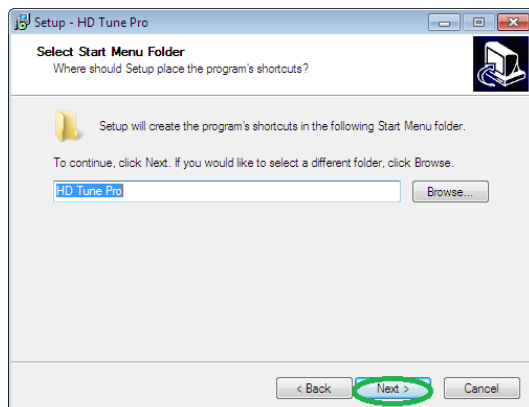


Imagen 1.93

- Dar clic en la opción para crear un icono en el escritorio, y luego dar clic en siguiente para continuar con la instalación del programa (ver imagen 1.94)

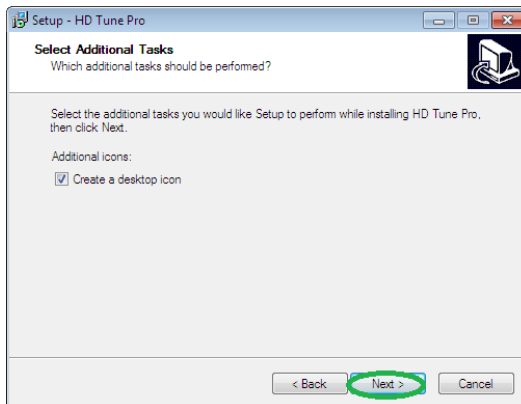


Imagen 1.94

- Dar clic en instalar para continuar con la instalación (ver imagen 1.95)

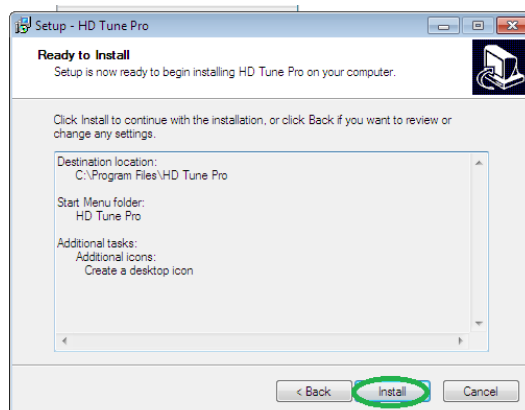


Imagen 1.95

- Esperar a que el programa instale todos los archivos y registros en el ordenador para poder utilizar la aplicación (ver imagen 1.96)

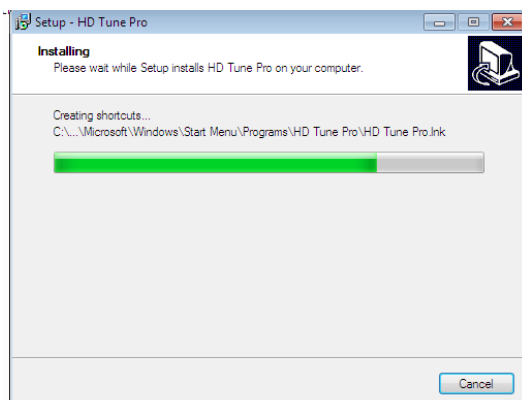


Imagen 1.97

- Al terminar la instalación del programa dar clic en finalizar (ver imagen 1.98)

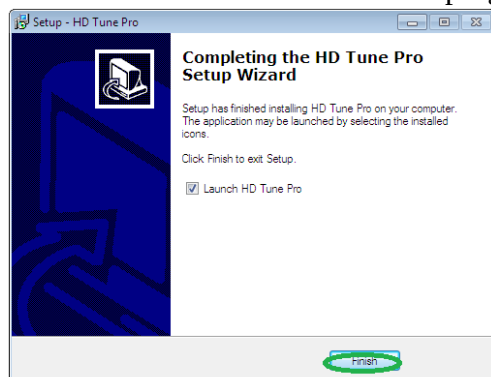


Imagen 1.98

Pasos para crackear el programa HD Tune Pro

- Ejecutar el crack para dejar el programa completo, dicho crack se encuentra en la carpeta de descarga del instalador (ver imagen 1.99)

Nombre	Fecha de modifica...	Tipo
 crack	13/10/2012 08:49 ...	Carpeta de archivo:
 HDtunepro_460_trial	30/08/2010 06:34 ...	Aplicación

Imagen 1.99

- Abrir la carpeta que dice crack dando clic derecho y seleccionar copiar (ver imagen 2)

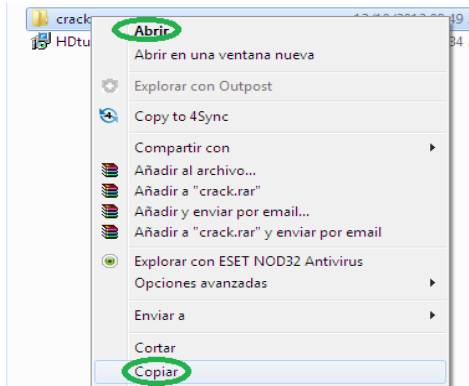


Imagen 2

- Buscar la carpeta donde se instaló anteriormente el programa en la siguiente dirección :
disco local C: archivos de programa: HD Tune y copiar el archivo a la carpeta del instalador (ver imágenes 2.1 - 2.2 – 2.3)



Imagen 2.1

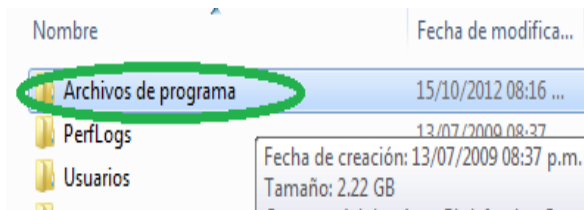


Imagen 2.2

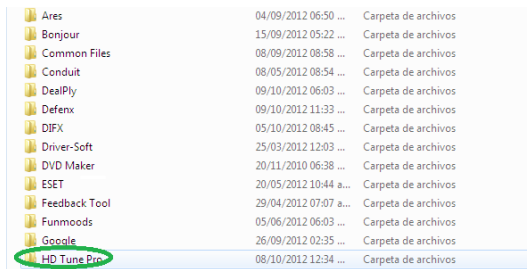


Imagen 2.3

- Al copiar el archivo en la carpeta de instalador saldrá una ventana con un menú en el cual elegir la opción copiar y reemplazar el archivo (ver imagen 2.4)

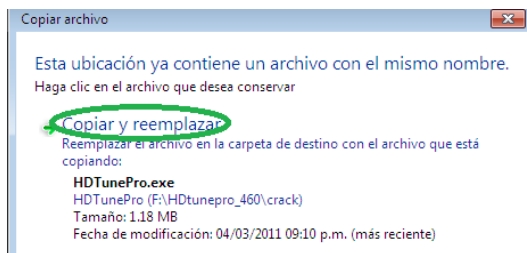


Imagen 2.4

- Al seleccionar la opción copiar y reemplazar el archivo ya existente saldrá una ventana con la advertencia de permisos de administrador dar clic en continuar para reemplazar el archivo y poder dejar full el programa (ver imagen 2.5)

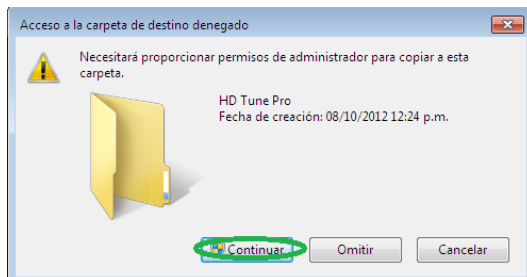


Imagen 2.5

Pasos para utilizar HD Tune Pro 4.6

- Ejecutar el software desde el icono que está en el escritorio dando doble clic en el (ver imagen 2.6)



Imagen 2.6

- Aparecerá la ventana abierta del programa (ver imagen 2.7)

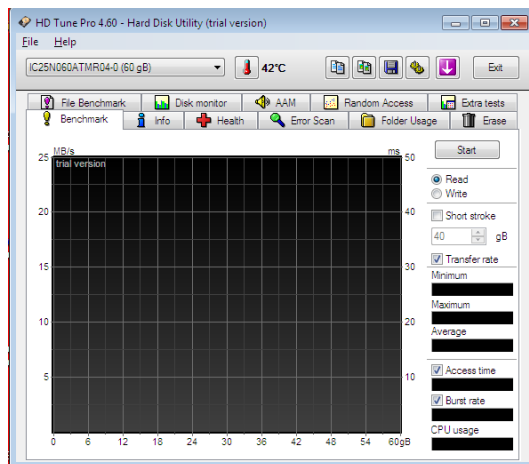


Imagen 2.7

- Seleccione el dispositivo a analizar, en esta ocasión se elegirá un disco duro desplegando el menú que se encuentra en la parte superior izquierda de la ventana del programa (ver imagen 2.8)

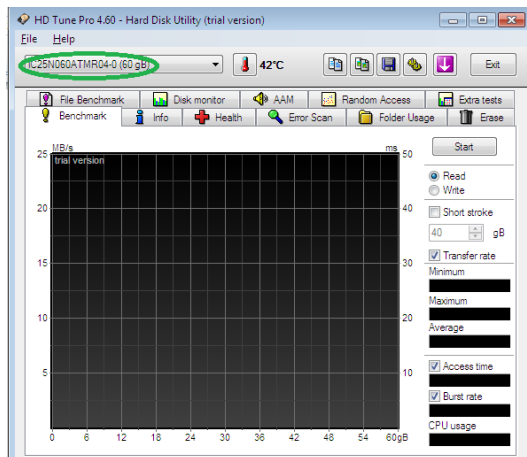


Imagen 2.8

- Seleccionar la opción escanear error y dar clic en start (ver imagen 2.9)

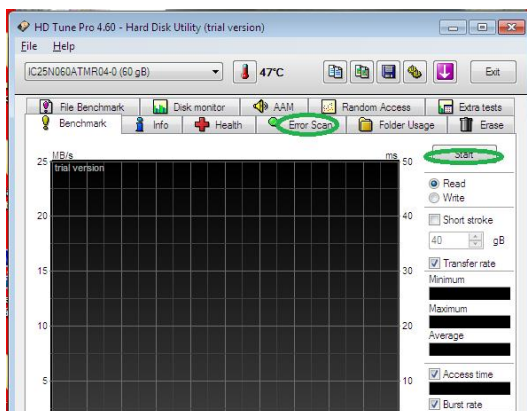


Imagen 2.9

- Al seleccionar estas opciones el programa empezara a realizar un escaneo en busca de errores en el disco duro seleccionado (ver imagen 2.10)

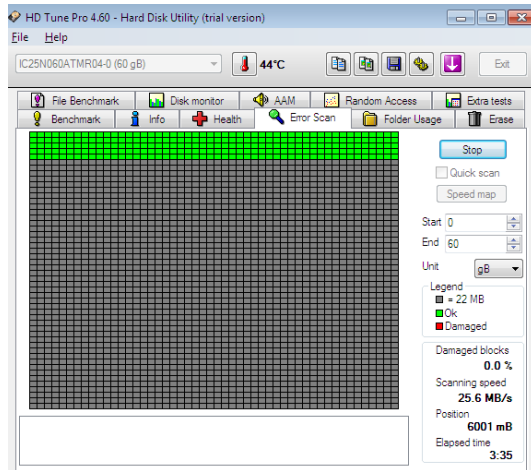


Imagen 2.10

- Al terminar el escaneo en busca de errores en el disco duro el programa mostrara la siguiente ventana, en este caso no muestra ningún error de disco porque el disco se encuentra en buenas condiciones (ver imagen 2.11)

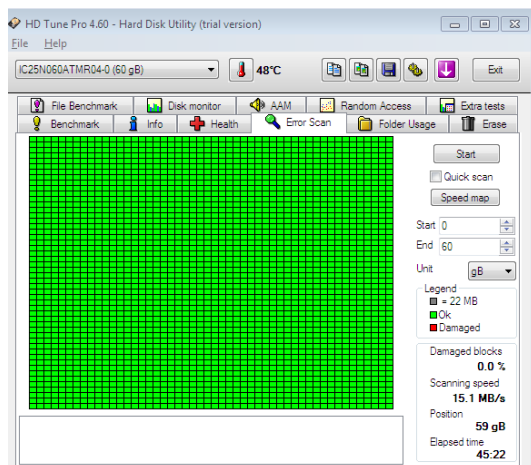


Imagen 2.11

- Al seleccionar la opción benchmark y luego start el programa realizara la prueba de rendimiento del disco duro y comprueba la velocidad de la tasa de transferencia de datos (ver imagen 2.12)

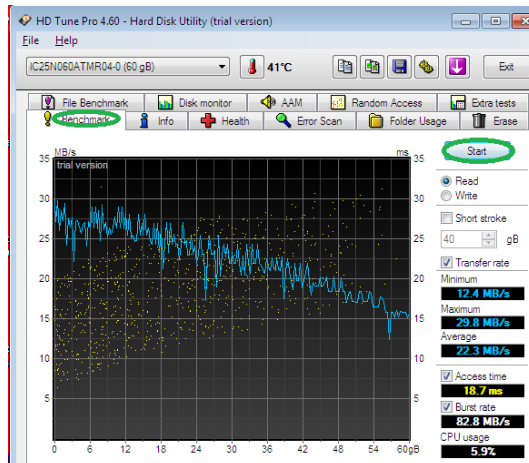


Imagen 2.12

- En la siguiente opción del programa que es file benchmark y luego start mostrara la prueba de rendimiento del disco duro pero mediante un gráfico de barras (ver imagen 2.13)

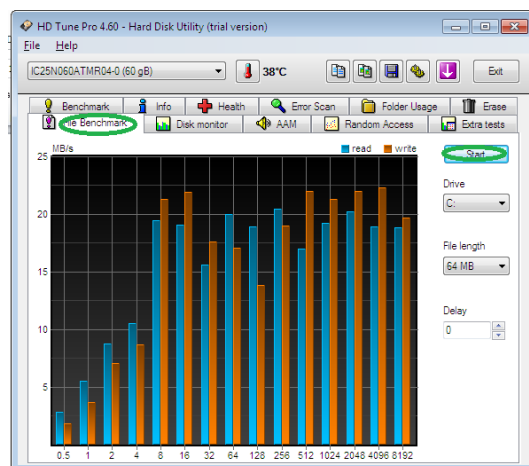


Imagen 2.13

- Al seleccionar la opción info el programa mostrara toda la información del disco duro y sus características técnicas (ver imagen 2.14)

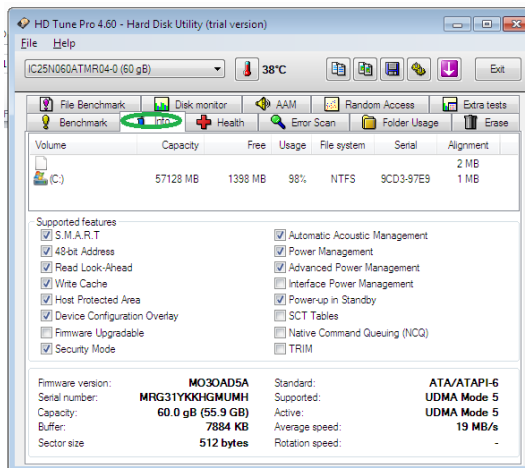


Imagen 2.14

- En la siguiente opción Health (corazón) muestra el estado del disco duro como sectores defectuosos, temperatura, etc. En el cual señalara con una franja amarilla si tiene algún error (ver imagen 2.15)

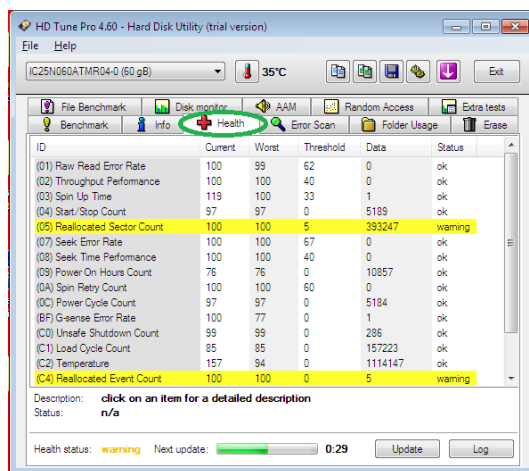


Imagen 2.15

Beneficios de usar la aplicación HD Tune Pro 4.6

- Usar la aplicación HD Tune Pro 4.6 permite al usuario realizar un escaneo completo en busca de errores en el disco duro, prueba de rendimiento, visualización de la información del disco duro, además de esto también muestra la temperatura a la que se encuentra el dispositivo (ver imágenes 2.16 – 2.17 – 2.18)

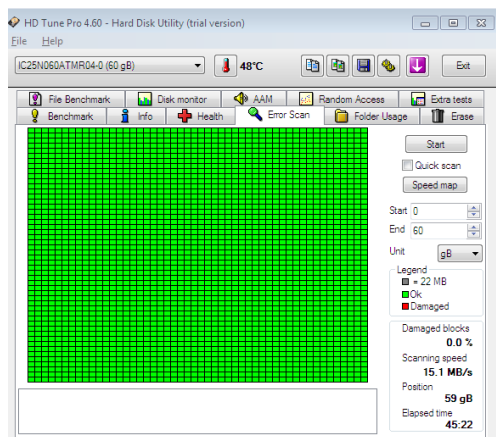


Imagen 2.16

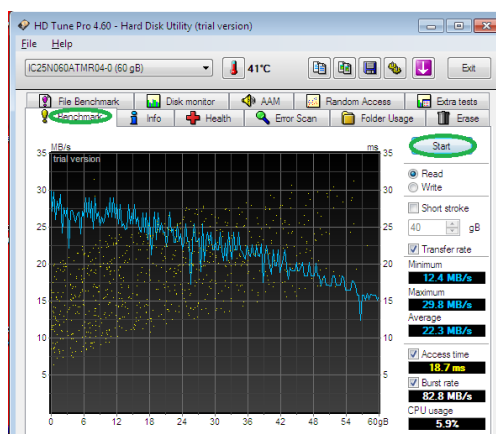


Imagen 2.17

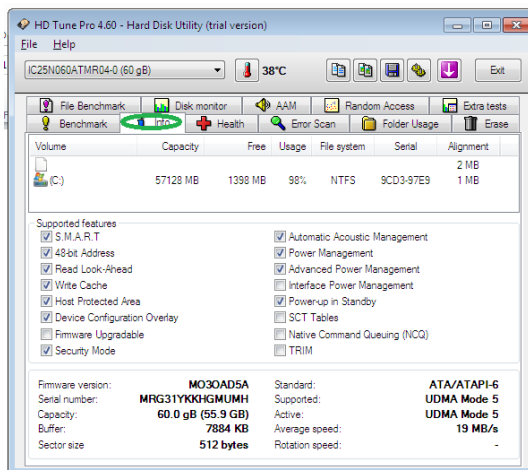


Imagen 2.18

Pasos para instalar Bit Defender 2012 Total Security v15.0.27.312

- Descarga la aplicación Bit Defender 2012 Total Security v15.0.27.312 del link <http://depositfiles.com/files/ykk0o1cqa>
- Ejecutar el programa desde el icono que se encuentra en el escritorio haciendo doble clic sobre el (ver imagen 2.19)

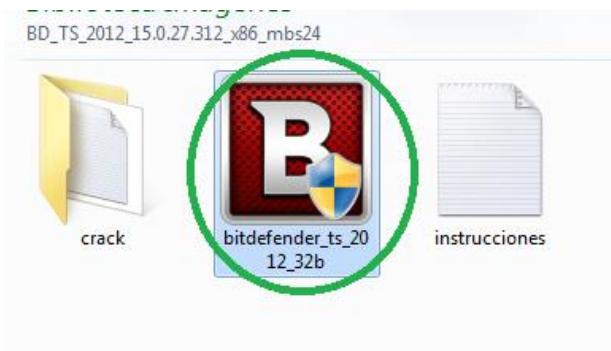


Imagen 2.19

- Ejecutar el instalador como administrador dar clic derecho sobre el icono del instalador y seleccionar ejecutar como administrador. En Windows 7 aparece una ventana de advertencia dar clic en si para continuar con la instalación (ver imagen 2.20)

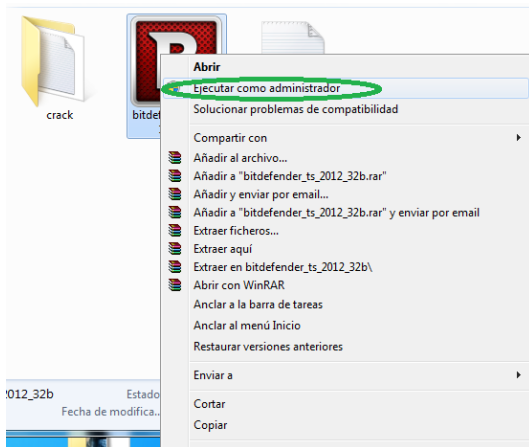


Imagen 2.20

- El programa descomprimirá todos los archivos necesarios para continuar con la instalación esperar a que se descomprima por completo (ver imagen 2.21)

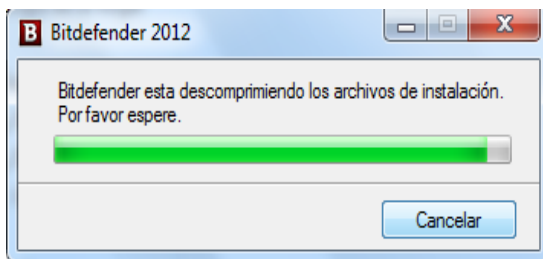


Imagen 2.21

- Para poder continuar con la instalación recuerde tener conectada su computadora a internet el ejecutador descargara los archivos necesarios para continuar con la instalación (ver imagen 2.22)

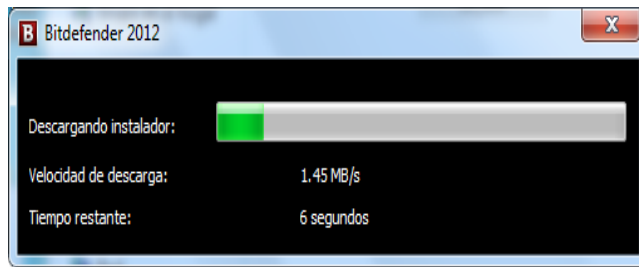


Imagen 2.22

- Para continuar con la instalación aceptar los términos de uso de licencia, aceptarás las condiciones y políticas de dicho software para el uso adecuado del mismo (ver imagen 2.23)

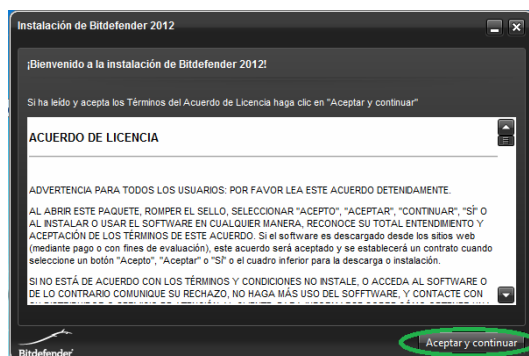


Imagen 2.23

- Registrar el producto, utilizando una cuenta de correo electrónico la cual se escribirá en el espacio en blanco que tiene a la par la indicación correo electrónico y al hacerlo el usuario recibirá en su cuenta lo necesario para completar el proceso de registro (ver imagen 2.24)

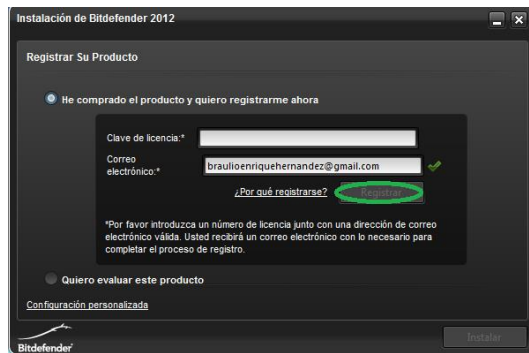


Imagen 2.24

- Dar clic en la opción quiero evaluar este producto y luego dar clic en instalar para continuar con la instalación del programa (ver imagen 2.25)

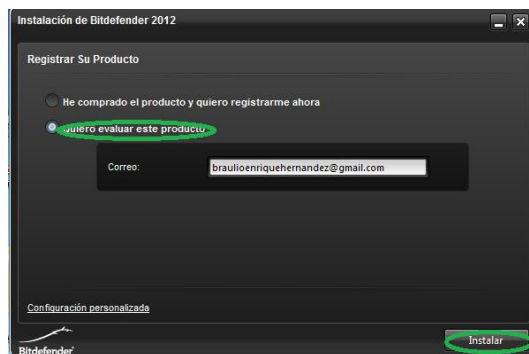


Imagen 2.25

- Esperar a que el programa termine de descargar todos los archivos al ordenador (ver imagen 2.26)

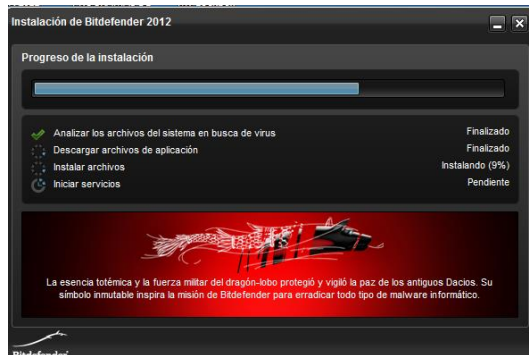


Imagen 2.26

- Dar clic en finalizar para terminar con la instalación del programa (ver imagen 2.27)



Imagen 2.27

Pasos para crackear el software Bit Defender 2012

- Al finalizar la instalación del programa, reinicie la computadora y entre en modo seguro utilizando f8 antes de que la pc pase de del post y muestre el menú de modo seguro seleccionar modo seguro y dar clic en enter (ver imagen 2.28)

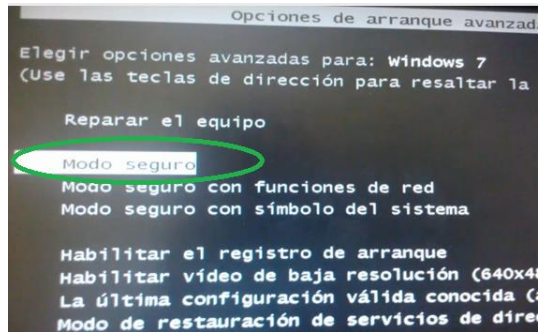


Imagen 2.28

- Cuando ya se allá iniciado la pc mostrar un mensaje de que se a entrado en modo seguro (ver imagen 2.29)

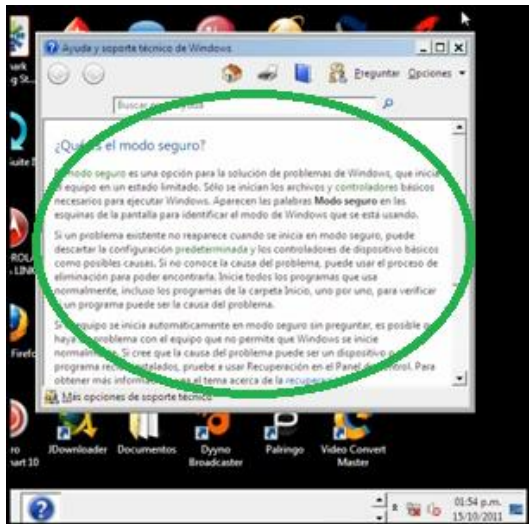


Imagen 2.29

- Dirigirse a la carpeta del instalador y en la carpeta llamada crack abrir y descomprimir el archivo rar (ver imagen 2.30)

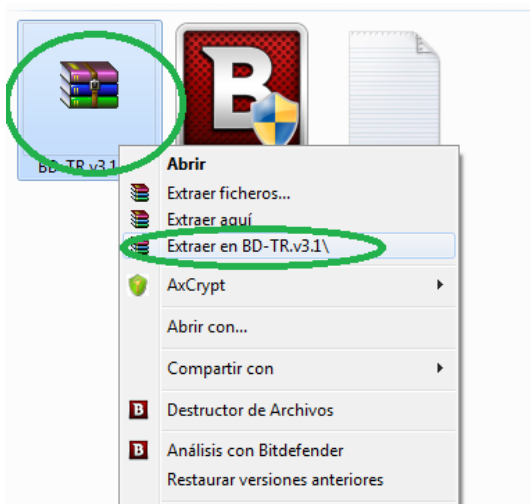


Imagen 2.30

- Ejecutar el archivo descomprimido llamado (BD2011-TR.v3.) luego dar clic en “Year 2045” saldrá un mensaje con la nota de q haciendo activador dar clic en aceptar y luego reiniciar la pc en modo normal (ver imágenes 2.31 - 2.32)



Imagen 2.31

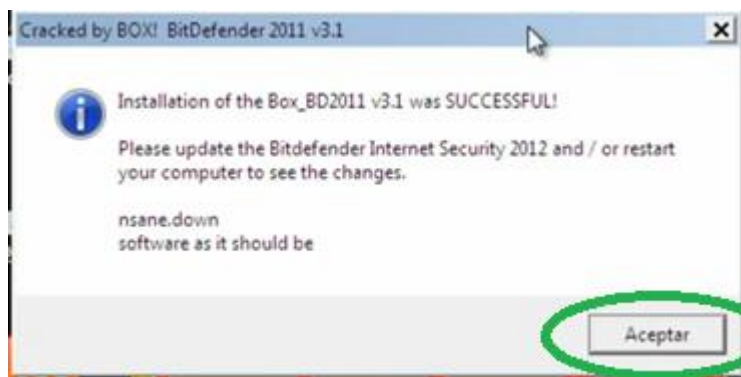


Imagen 2.32

Pasos para utilizar el software Bit Defender 2012 Total Security

- Ejecutar el programa desde el icono del escritorio (ver imagen 2.33)



Imagen 2.33

- Aparecerá la siguiente ventana del programa (ver imagen2.34)



Imagen 2.34

- Elegir la primera configuración del programa (ver imagen 2.35)



Imagen 2.35

- En esta configuración se debe dar clic en el icono que aparece en esta configuración ,
(ver imagen 2.36)



Imagen 2.36

- Esta opción muestra un menú de funciones que el programa puede realizar dentro de esta opción llamada Antivirus, además ofrece las opciones de realizar un análisis en tiempo real y Active virus control (ver imagen 2.37)



Imagen 2.37

- En la configuración de Antivirus dar clic en analizar y desplegar para ver las opciones de análisis, elegir análisis completo (ver imagen 2.38)



Imagen 2.38

- Al seleccionar la opción analizar y desplegar para elegir análisis completo se mostrara la siguiente ventana con el proceso de análisis del disco duro en busca de malware y otras actividades que podrían ser de dudosa procedencia para el ordenador (ver imagen 2.39)



Imagen 2.40

- Al terminar el análisis completo del disco duro, el programa mostrara la siguiente ventana dando el informe completo de los archivos escaneados y los infectados si los hay (ver 2.41)

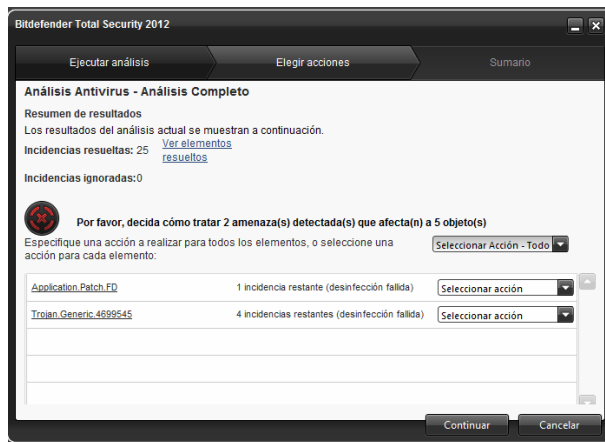


Imagen 2.41

- Elegir la segunda configuración del programa (ver imagen 2.42)

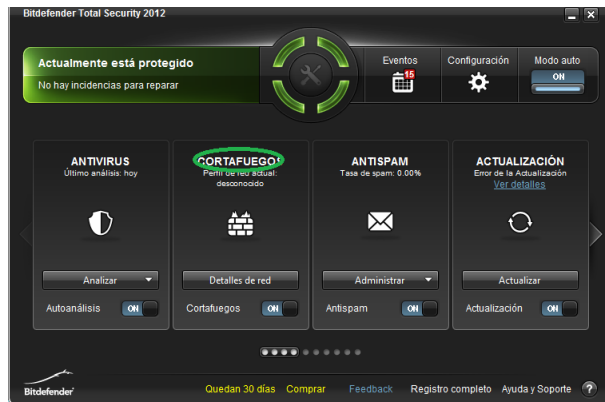


Imagen 2.42

- En la opción Cortafuegos dar clic en el icono de abajo (ver imagen 2.43)



Imagen 2.43

- Al seleccionar el icono anterior mostrara un menú de funciones que el programa puede realizar en esa configuración, como por ejemplo activar la detección de intrusos y monitorear el tráfico de internet inalámbrico y LAN (ver imagen 2.44)



Imagen 2.44

- Elegir la tercera configuración del programa (ver 2.45)

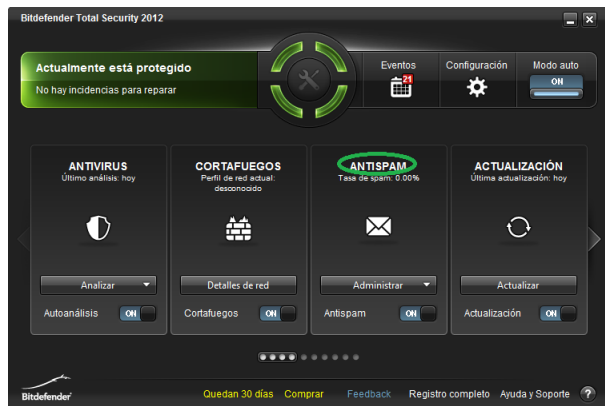


Imagen 2.45

- En la configuración del Antispam dar clic en el icono de abajo (ver imagen 2.46)



Imagen 2.46

- Al seleccionar el icono anterior mostrara un menú de funciones que el programa puede realizar en esa configuración, como por ejemplo medir el nivel de sensibilidad y el filtro para detectar spam (ver imagen 2.47)

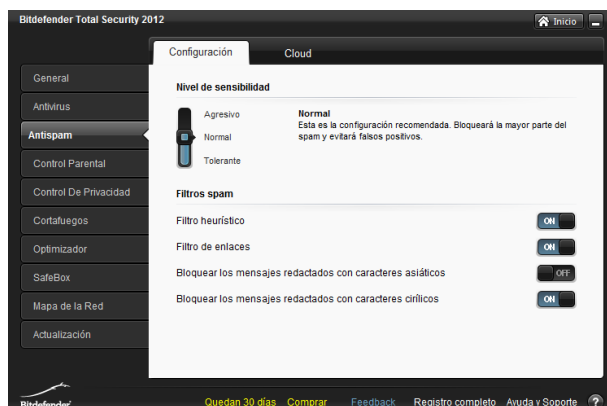


Imagen 2.47

- Elegir la cuarta configuración del programa (ver imagen 2.48)

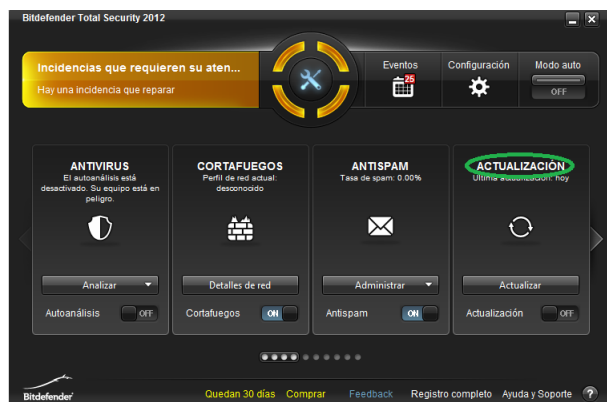


Imagen 2.48

- En la configuración de actualización dar clic en el icono de abajo (ver imagen 2.49)

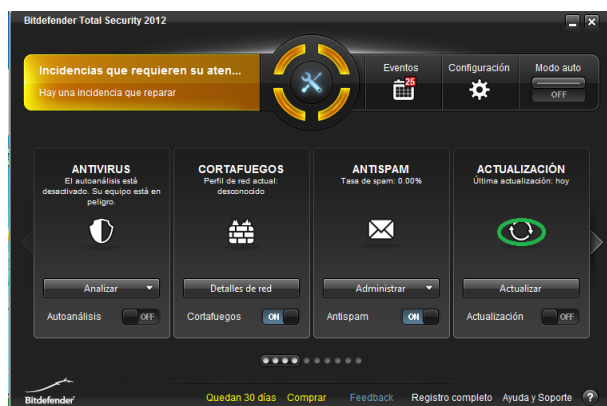


Imagen 2.49

- Al seleccionar el icono anterior mostrara un menú de funciones que el programa puede realizar en esa configuración, como por ejemplo actualizar la base de datos de firmas de virus utilizando la conexión a internet, y la actualización silenciosa (ver imagen 2.50)

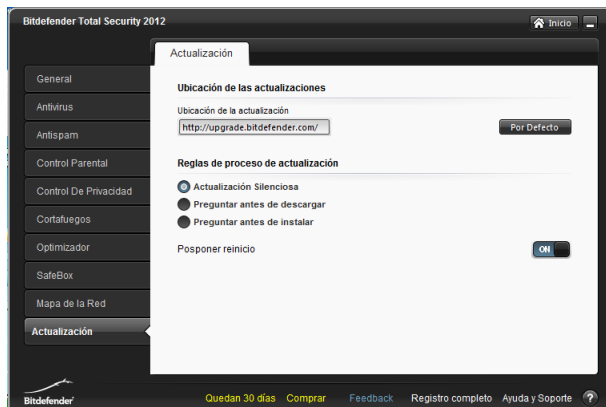


Imagen 2.50

- Al seleccionar la actualización por conexión a internet recordar estar conectados a esta conexión antes mencionada y dar clic en la opción por defecto para comenzar la actualización del programa (ver imagen 2.51)

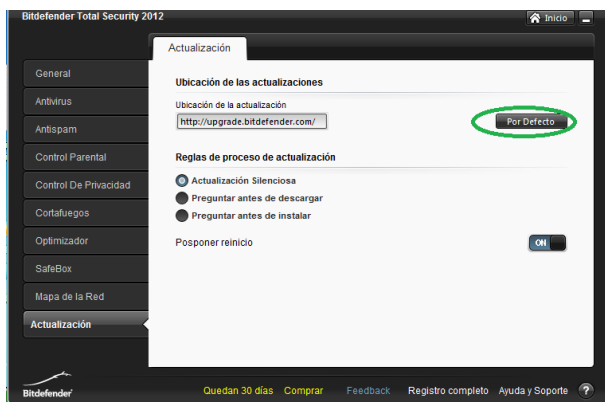


Imagen 2.51

Pasos para instalar y usar Beini 1.2.2

Que es una imagen ISO: Es un archivo donde se almacena una copia o imagen exacta de un sistema de ficheros, normalmente un disco óptico.

- Descarga la aplicación Beini 1.2.2 del link <http://www.mediafire.com/?ncnyaleq7d5zclj>
- Dirigirse a la carpeta de descarga y acceder a la carpeta contenedora del programa encontraran el archivo en forma de imagen ISO (ver imágenes 2.52 – 2.53)

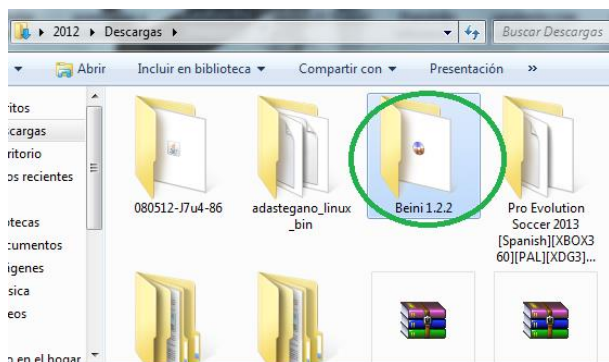


Imagen 2.52

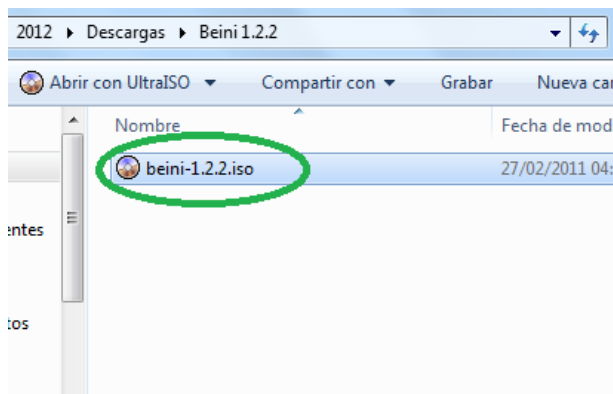


Imagen 2.53

- Grabar esta imagen ISO en CD con el Nero u otro programa para grabación de datos (ver imagen 2.54)

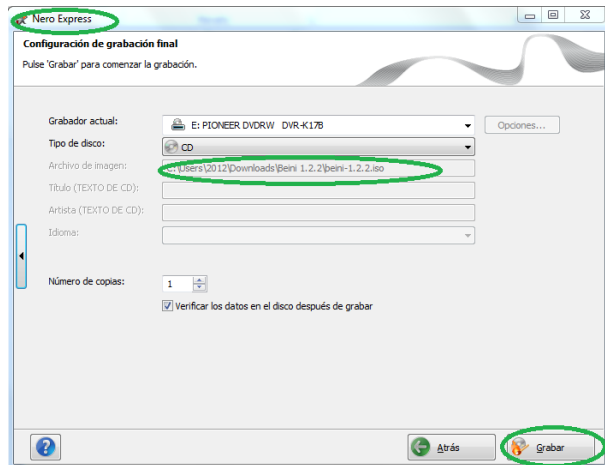


Imagen 2.54

- Ejecutar el programa desde un CD Booteable, iniciando el ordenador desde el CD Booteable entrando a la configuración de arranque en la BIOS y seleccionando el CD como arranque prioritario (ver imagen 2.55)

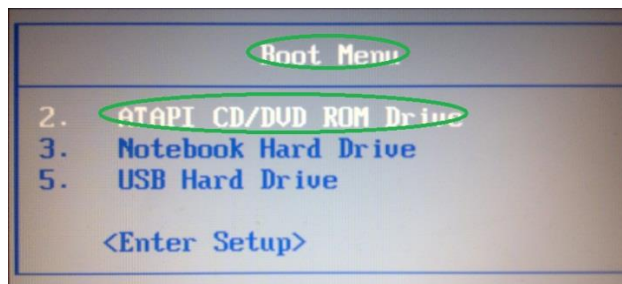


Imagen 2.55

- Aparecerá la siguiente ventana del programa Unetboot in en el cual seleccionar la opción que dice Start Beini 1.2.2 para iniciar este programa (ver imagen 2.56)

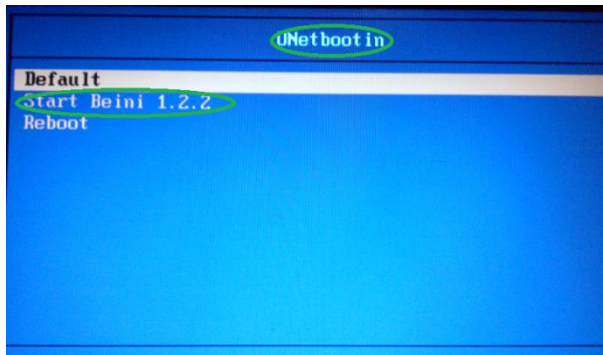


Imagen 2.56

- Esperar a que el programa cargue todos los archivos necesarios (ver imagen 2.57)

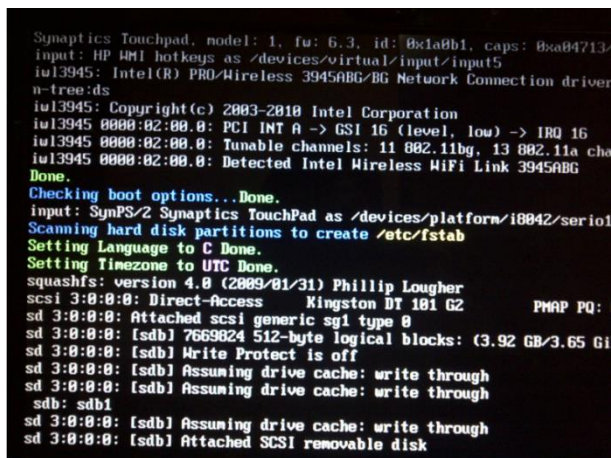


Imagen 2.57

- Aparecerá la siguiente ventana del programa (ver imagen 2.58)

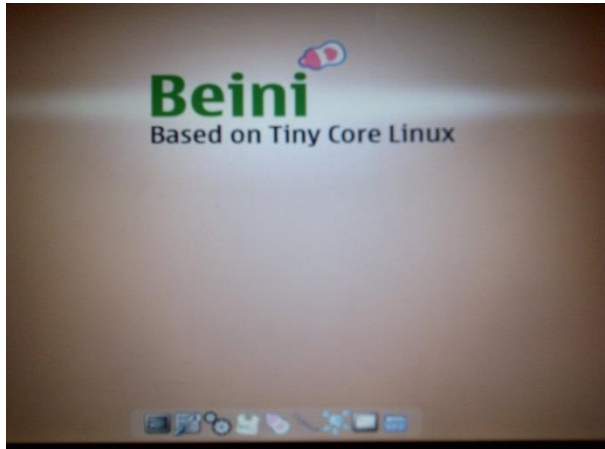


Imagen 2.58

- Seleccionar la opción Feeding Bottle para iniciar el proceso de hackeo de redes inalámbricas (ver imagen 2.59)

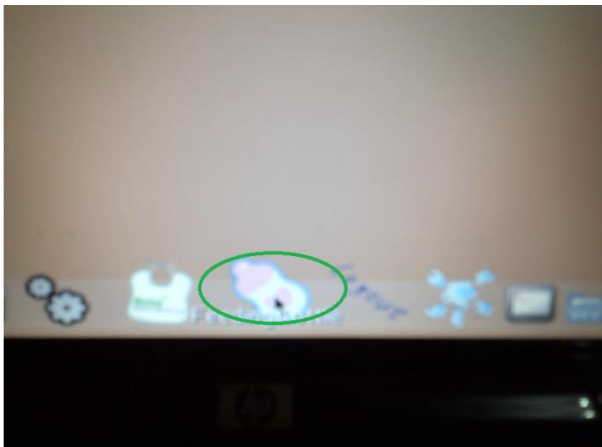


Imagen 2.59

- Aparecerá la siguiente ventana y dará el mensaje que pedirá que por favor no se realice el hackeo del punto de acceso, dar clic en Yes para continuar con el proceso de hackeo (ver imagen 2.60)

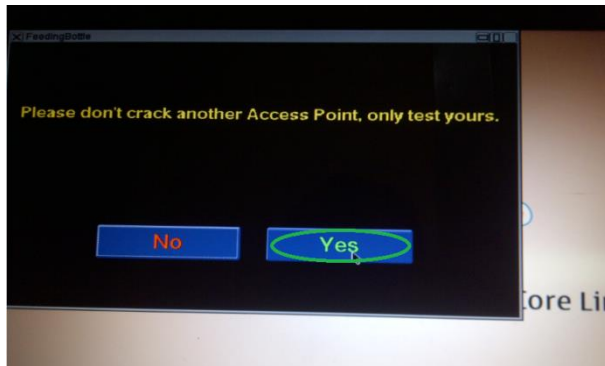


Imagen 2.60

- Seleccionar la tarjeta de red que tiene el ordenador dando clic en la primera opción y configurar para que se prepare a modo monitor (ver imagen 2.61)

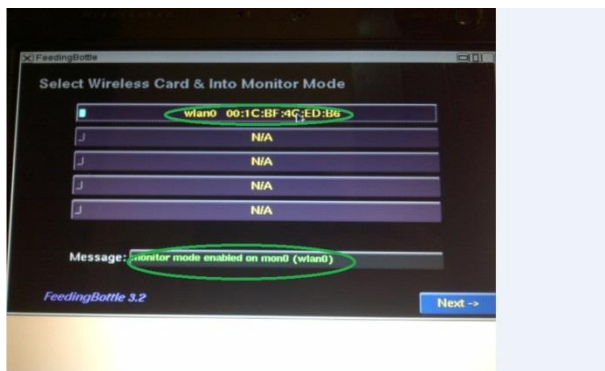


Imagen 2.61

- Dar clic en Scan para que el programa empiece a buscar las redes inalámbricas existentes mas cercanas (ver imagen 2.62)

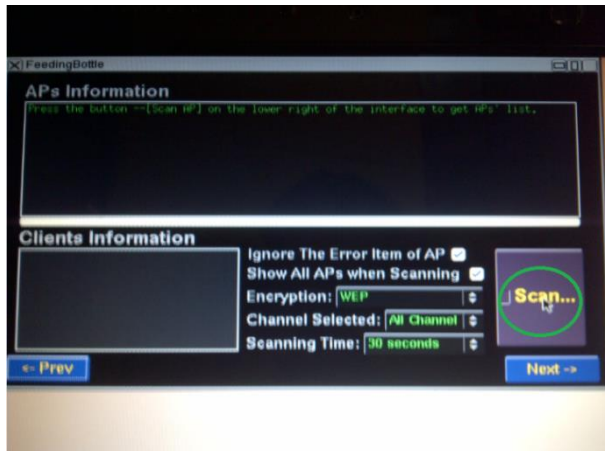


Imagen 2.62

- En este paso el programa empieza a mostrar la lista de conexiones inalámbricas disponibles a su alcance y empieza a mandar los paquetes a las redes disponibles (ver imagen 2.63)



Imagen 2.63

- Aparecerá la siguiente ventana mostrando las conexiones inalámbricas disponibles mas cercanas (ver imagen 2.64)

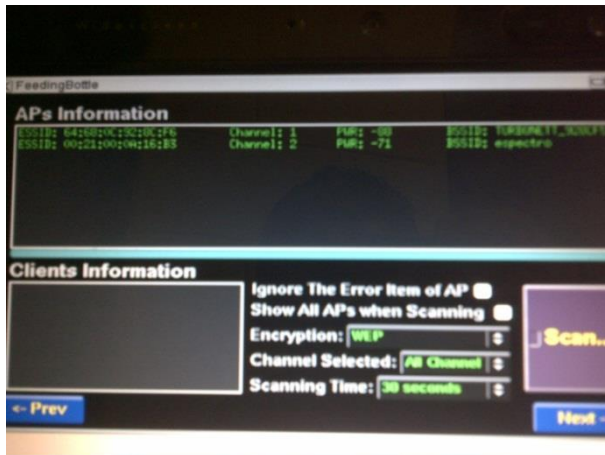


Imagen 2.64

- Seleccionar la conexión en la cual se desea realizar el hackeo de redes inalámbricas dando clic en ella (ver imagen 2.65)

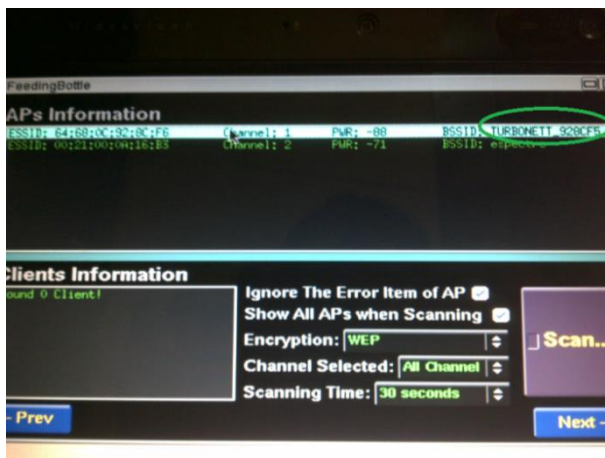


Imagen 2.65

- Seleccionar la cantidad de pps en este caso son 800pps (ver imagen 2.66)

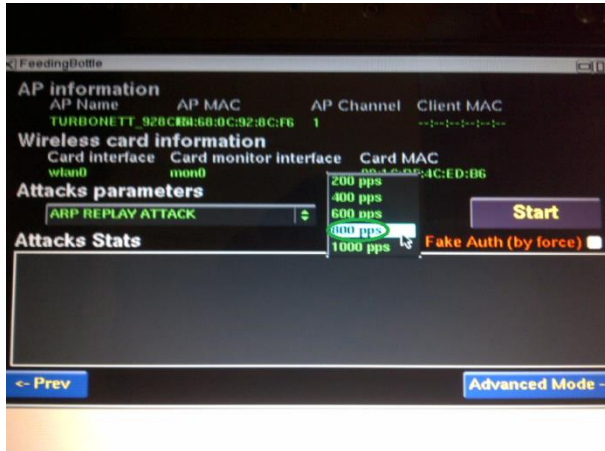


Imagen 2.66

- Dar clic en Start para iniciar el ataque a la red seleccionada (ver imagen 2.67)

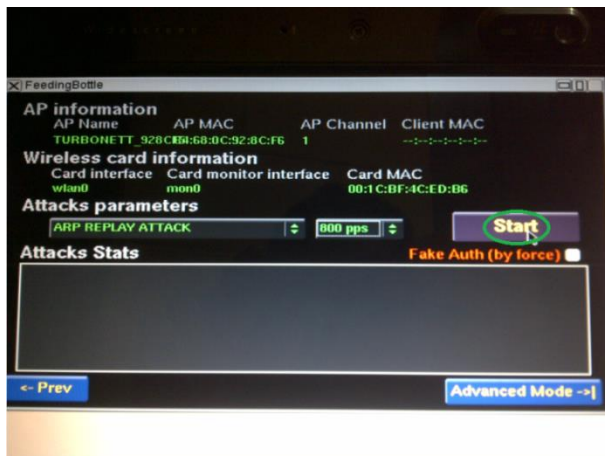


Imagen 2.67

- En este paso el programa realiza la captura de los paquetes de la red y muestra los datos probados y los perdidos (ver imagen 2.68)

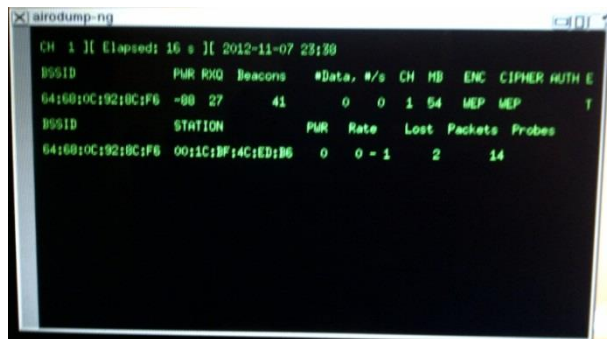


Imagen 2.68

Segunda configuración para realizar el hackeo de redes inalámbricas

- Dar clic en el icono que dice Minid wap gtk (ver imagen 2.69)

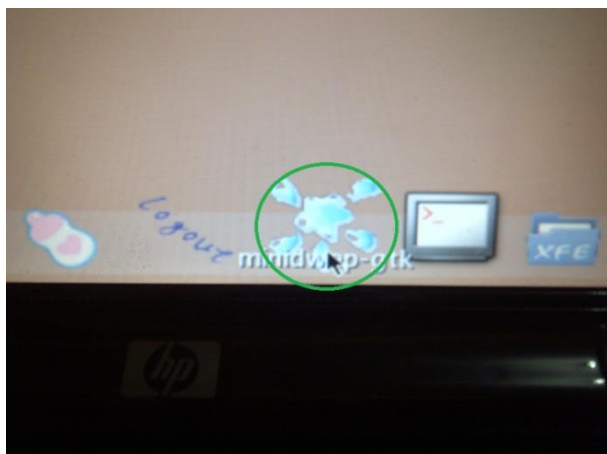


Imagen 2.69

- Dar clic en ok para continuar con el hackeo de la red (ver imagen 2.70)

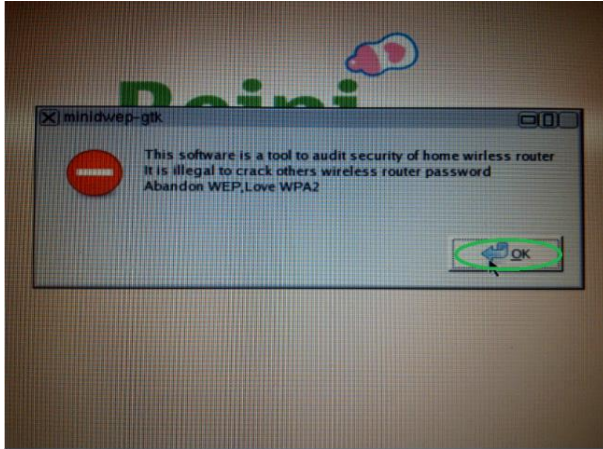


Imagen 2.70

- Aparecerá la siguiente ventana del programa mostrando la tarjeta de red ya seleccionada, la encriptación y el modo de selección, todas estas opciones en la parte izquierda de la ventana del programa, dar clic en la opción Scan para que el software empiece a buscar las redes inalámbricas existentes mas cercanas (ver imagen 2.71)

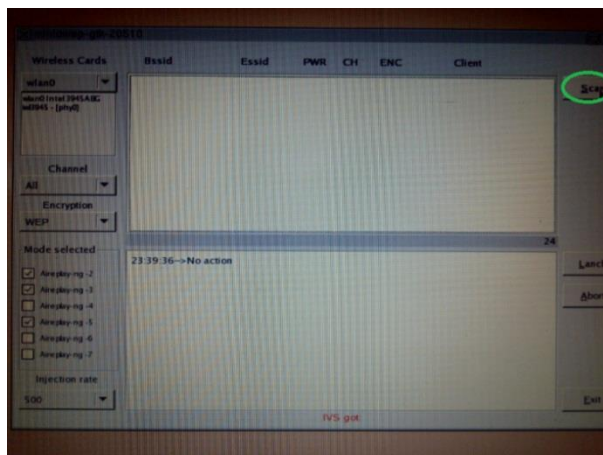


Imagen 2.71

- En este paso el programa buscara las redes inalámbricas mas cercanas que estén a su alcance (ver imagen 2.72)

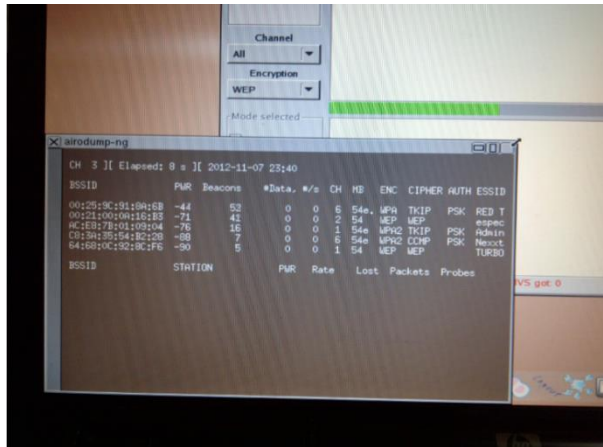


Imagen 2.72

- Elegir la conexión inalámbrica que se desea hackear (ver imagen 2.73)

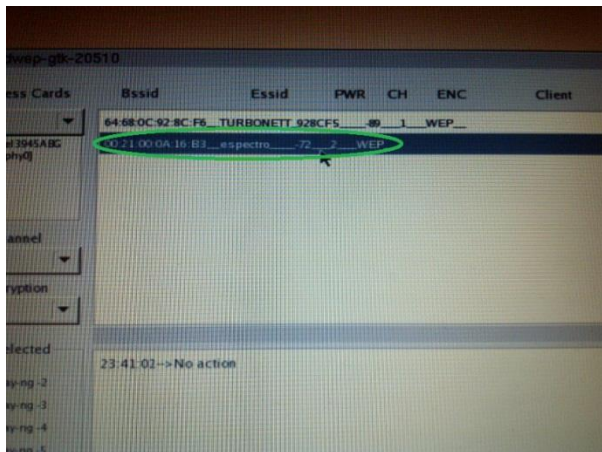


Imagen 2.73

- Dar clic en la opción Launch para iniciar el ataque a la red (ver imagen 2.74)

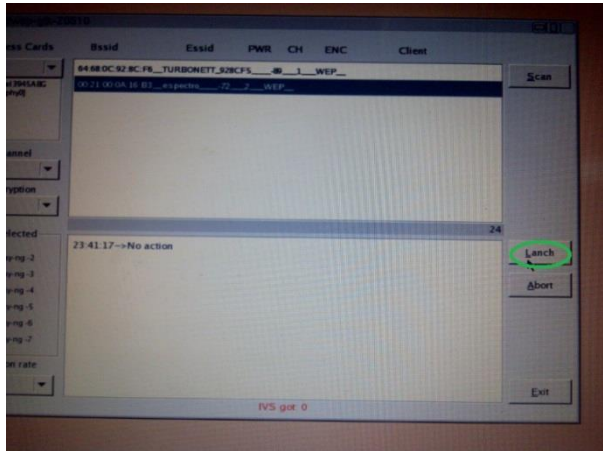


Imagen 2.74

- En este paso el programa mandara los paquetes de datos y mostrara los perdidos y los probados (ver imagen 2.75)



Imagen 2.75

- En este paso el programa hará la decodificación para encontrar la clave de la red inalámbrica seleccionada (ver imagen 2.76)

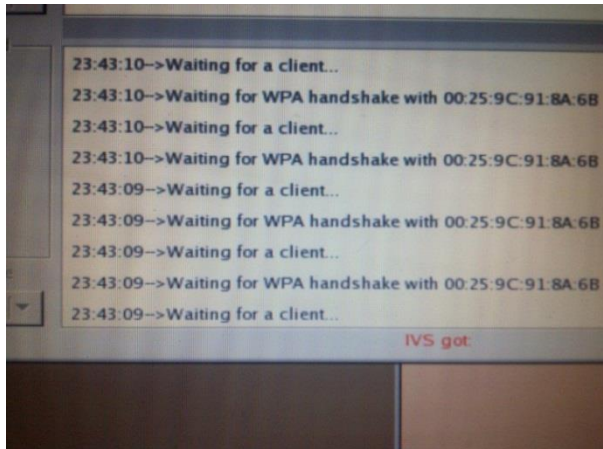


Imagen 2.76

2.2.2 Kit de herramientas digitales de informática forense

El kit de herramientas digitales de informática forense consiste específicamente en un conjunto de aplicaciones o programas informáticos que tienen funciones diferentes para cada área básica de la informática forense como lo son la criptografía, esteganografía, recuperación de datos, diagnostico de discos duros, reparación de discos duros, seguridad de correos electrónicos, hackeo de redes wireless. Además de estas funciones que tendrán cada uno de los programas según sea su área de trabajo, el kit de herramientas digitales de informática forense servirá como un respaldo y apoyo didáctico para cuando se desarrollen los seminarios de informática forense en el laboratorio de Hardware de la Universidad Tecnológica de El Salvador.

Lista de aplicaciones que formaran parte del kit de herramientas digitales de informática forense:

- HDD Regenerator
- Ontrack Easy Recovery Professional
- HD Tune
- Axcrypt
- My Lockbox
- Bit defender 2012
- Beini

Como se ha mostrado en la lista anterior se ha elegido solamente a un software por cada área básica de la informática forense ya que estos cumplen con las características técnicas y económicas para poder servir como herramienta útil y eficiente para solucionar diferentes problemas que a menudo tienen los usuarios.

Descripción de los programas a utilizar en el kit de herramientas digitales de informática forense:

Programa Axcrypt :

Este programa tiene la función única de codificar o encriptar una carpeta o un archivo para proteger la información de otros usuarios o intrusos que deseen ver la información, por medio de un código que es escrito por el usuario en el momento de decodificar el archivo y la carpeta tendrá la apariencia del icono del programa, así cuando un usuario

extraño quiera entrar en ese archivo el programa axcript le pedirá automáticamente la contraseña para poder ver la información que hay dentro.

La aplicación también cuenta con la opción de decodificar o desenscriptar las carpetas y los archivos si el usuario así lo desea.

Las características principales de este software son:

- Es un software con licencia libre y económica al usuario.
- Es fácil de usar para el usuario.
- Posee compatibilidad con Windows XP y 7.
- Ocupa poco espacio en el disco duro.
- Es fácil de instalar.
- Funciona para 32 y 64 bits.
- Posee configuración sencilla.

Ventajas de utilizar software Axcript

- Es fácil de descargar de una página libre en la web.
- Su instalación es rápida y sencilla para el usuario.
- Es casi automático su funcionamiento.
- Posee varias versiones.
- No necesita actualizaciones.
- No necesita crack.
- Posee versión portable para el usuario.

Desventajas de utilizar el software Axcrypt

- La contraseña no es 100% segura en sus caracteres.
- No posee configuraciones adicionales a la configuración de funcionamiento.

Programa My Lockbox

Es un software que tiene la función de ocultar una imagen, un archivo de texto o una carpeta cualquiera utilizando el método de la esteganografía, que es el método que oculta una imagen dentro de otra de modo que el usuario pase desapercibido de la información que hay en la imagen y los datos se mantengan seguros, aunque no en un 100%.

Características principales de este software son:

- Es fácil de descargar en internet.
- Su instalación es rápida y sencilla.
- Es de fácil uso para el usuario.
- Utiliza un código para mantener segura la información.
- Ocupa poco espacio en disco duro.
- Es compatible con Windows XP y 7.
- Se utiliza para 32 y 64 bits.

Ventajas de utilizar software My Lockbox

- Oculta archivos de forma que el usuario extraño que desea verlos pase desapercibido.
- Posee una licencia libre para el usuario.
- Su instalación es rápida en el sistema operativo.
- Ocupa poco espacio en disco duro.
- Utiliza un código para poder ver la información oculta.
- Es compatible con Windows XP y 7.
- Se usa para 32 y 64 bits.

Desventajas de utilizar My Lockbox

- La contraseña no es 100% segura en sus caracteres.
- No posee configuraciones adicionales a la configuración de funcionamiento.

Programa Ontrack Easy Recovery Profesional

Es un software que se utiliza para la recuperación de datos, como por ejemplo archivos de texto, archivos de audio, archivos de video, imágenes, etc. Este software se encarga de rescatar la información aunque se haya formateado el disco duro completamente y permite visualizar los archivos borrados antes de recuperarlos, para que el usuario pueda seleccionar manualmente los archivos que desea que el programa recupere del disco duro, USB, CD, u otro dispositivo de almacenamiento que haiga perdido datos.

Además este programa posee la opción para ubicar los datos ya recuperados, y el usuario decide en donde guardarlos.

Las características de este software son:

- Recupera todo tipo de archivo en dispositivos de almacenamiento.
- Posee varias versiones.
- Es compatible con Windows XP y 7.
- Posee licencia libre para el usuario.
- Es fácil de usar para el usuario.
- Ocupa poco espacio en disco duro.
- Instalación rápida y sencilla

Ventajas de utilizar software Ontrack Easy Recovery Profesional

- Su licencia es libre y accesible al usuario.
- Recupera cualquier tipo de archivo.
- Ocupa poco espacio en disco duro.
- Recupera archivos aunque el disco este formateado.
- Es fácil de usar para el usuario.
- Permite visualizar los archivos antes de recuperarlos.
- Realiza un escaneo profundo.
- Tiene un menú muy amplio que permite elegir la opción más adecuada para recuperar los archivos.
- Existe versión portables.

Desventajas del software Ontrack Easy Recovery Professional

- No recupera archivos en un 100%
- No recupera archivos en dispositivos de almacenamiento dañados.

Programa HDD Regenerator

Es un software que tiene la función de reparar los sectores dañados de los discos duros debido a una mala magnetización.

Características de este software:

- Repara defectos físicos del disco duro.
- Repara los sectores defectuosos debido a una mala magnetización.
- No afecta a los datos existentes en el disco duro.
- Seguro y eficaz en la mayoría de problemas de sectores defectuosos.
- Se utiliza desde un CD de arranque o una USB flash de arranque.
- Posee una interfaz simple e intuitiva.
- Fácil de usar para el usuario.

Ventajas de utilizar HDD Regenerator

- Fácil de usar.
- Interfaz sencilla.
- Repara sectores defectuosos de los discos duros.
- No ocupa demasiado espacio en el disco duro.
- Es compatible con Windows NT, 2000, XP y 7.
- No afecta a los datos existentes en el disco duro.

- Soporte para instalación y desinstalación.

Desventajas de utilizar HDD Regenerator

- No siempre se podrán reparar todos los sectores defectuosos de los discos duros.
- No repara daños físicos causados por el mal uso como golpes físicos en el disco duro.
- No funciona sin hacer un CD de arranque o en una USB flash.

Programa Bit defender 2012 Total Security

Es un programa informático del área de seguridad informática, que tiene la función de brindar seguridad al sistema operativo y a las demás aplicaciones que están dentro del sistema protegiéndolas de ataques de malware, spiware, phishing y otros.

Características de este programa

- Posee varias configuraciones para mejorar la seguridad en el ordenador.
- Tiene una interfaz sencilla para el usuario.
- Es compatible con Windows XP y 7.
- Su instalación requiere conexión a internet.
- Las actualizaciones se descargan automáticamente al instalar el software.
- Realiza un escaneo completo del disco duro.
- Controla el tráfico de la información en la red.

Ventajas de utilizar Bit defender 2012 Total Security

- Mantiene seguro el ordenador contra todo tipo de malware.
- Posee configuraciones para mejorar la seguridad en el ordenador.

- Monitorea el tráfico de información en la red.
- Es compatible con Windows XP y 7.
- Su descarga e instalación es gratis utilizando una cuenta de correo electrónico.
- Realiza un análisis del disco duro en tiempo real.
- Muestra un mapa de la red en su configuración.

Desventajas de utilizar Bit defender 2012 Total Security

- No se instala sin conexión a internet.
- Al estar instalado no se actualiza sin tener conexión a internet.

Programa HD Tune

Es un software que realiza la función de escanear completamente el disco duro y detectar errores en el mismo.

Características de este programa

- Realiza un escaneo completo en el disco duro del ordenador.
- Da un informe del estado en que se encuentra el disco duro que se ha escaneado.
- Utiliza gráficos de barras para mostrar la prueba de rendimiento del disco duro.
- Posee tres configuraciones para la revisión del disco duro.
- Es compatible con Windows XP y 7.
- Utiliza un crack para un óptimo funcionamiento.
- Funciona para discos duros de tipo IDE y SATA.

Ventajas de utilizar HD Tune

- Se conoce el estado funcional de los discos duros.
- Realiza un escaneo completo del disco duro seleccionado y muestra los errores que se han detectado.
- Posee varias versiones.
- Es compatible con Windows XP y 7.
- Escanea discos duros IDE, SATA y Encloser.
- Es de fácil utilización para el usuario.
- Posee una interfaz sencilla.

Desventajas de utilizar HD Tune

- Solamente escanea discos duros en funcionamiento.
- No funciona full sin instalar su crack.
- Solamente detecta los errores, pero no los repara automáticamente.

Programa Beini

Es un software que se usa para el hackeo de redes inalámbricas que poseen claves de tipo wep en su mayoría.

Características de este software

- Hackea redes inalámbricas.
- Decodifica las claves WEP.
- Captura los paquetes de las redes inalámbricas más cercanas a él.
- Se utiliza en Linux y Windows.

- Es compatible con Windows XP y 7.
- Posee una interfaz sencilla.
- Tiene dos formas para realizar el proceso de hackeo de una red inalámbrica.

Ventajas de utilizar beini

- Se puede usar en Linux y Windows.
- Decodifica claves WEP.
- Posee una interfaz grafica sencilla para el usuario.
- Es de fácil utilización.
- Identifica la tarjeta de red instalada en el ordenador.
- Identifica todas las redes inalámbricas que estén a su alcance.
- Se puede seleccionar manualmente la red que se desea hackear.

Desventajas de utilizar Beini

- Funciona mejor en Linux que es la plataforma en la que fue creado.
- No decodifica rápido las claves WEP.

2.2.3 CD Interactivo:

El CD interactivo es un dispositivo de almacenamiento extraíble que contendrá la descripción completa de cada uno de los programas que forman parte del kit de herramientas digitales de informática forense, y también las imágenes de cómo descargar las aplicaciones, los pasos específicos para instalar cada aplicación, pasos para configurar los programas y como utilizarlos según la función respectiva que tienen cada

uno de ellos, ya que estos programas cubren un área principal en específico de la informática forense, y se ha elegido un software por cada área tomando en cuenta que este cumple con las características económicas, técnicas y de funcionamiento óptimo, además de esto el CD tendrá tutoriales de cada programa sobre su uso correcto.

La creación de este CD se realizara con la ayuda de un software que creara el formato completo donde se pondrá todo el material de cada software que compone el kit de herramientas digitales de informática forense, los cuales son:

- Axcrypt.
- My Lockbox.
- Easy Recovery Profesional.
- HDD Regenerator.
- HD Tune.
- Bit defender 2012 Total Security.
- Beini.

¿En qué consiste el CD Interactivo?

El CD interactivo internamente consiste en un conjunto de imágenes, videos, tutoriales y material de apoyo necesario relacionado con el tema que se está tratando en el documento, es una recopilación de información adicional para el desarrollo del proyecto con el objetivo principal de presentar la solución mediante los productos ya anteriormente ofrecidos en el proyecto.

Este CD también servirá como producto principal de las promesas a cumplir en el proyecto, además de esto se hará un formato específico dentro del cómo puede ser la creación de una portada, un índice, información de forma textual y con imágenes que la respalden, videos, tutoriales, sonidos entre otros.

El CD puede ser muy interactivo ya que además de poseer la información del tema y las imágenes que respalden estas teorías de cada programa, se pueden agregar sonidos multimedia, videos, y otras animaciones para que pueda ser más útil y dinámico para todos los usuarios que deseen utilizarlo.

2.3 Marco Teórico Conceptual

Archivos

En informática, un archivo es un grupo de datos estructurados que son almacenados en algún medio y pueden ser usados por las aplicaciones. La forma en que una computadora organiza, da nombre, almacena y manipula los archivos se denomina sistema de archivos y suele depender del sistema operativo y del medio de almacenamiento (disco duro, disco óptico, etc).

Cadena de custodia

Un procedimiento controlado que se aplica a los indicios materiales (prueba indiciaria) relacionados con un hecho delictivo o no, desde su localización hasta su valoración por los encargados de administrar justicia y que tiene como fin asegurar la inocuidad y

esterilidad técnica en el manejo de los mismos, evitando alteraciones, sustituciones, contaminaciones o destrucciones, hasta su disposición definitiva por orden judicial.

Correo electrónico

Es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos. Principalmente se usa este nombre para denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías

Criptografía

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 y/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.

Datos

Del latín datum (“lo que se da”), un dato es un documento, una información o un testimonio que permite llegar al conocimiento de algo o deducir las consecuencias legítimas de un hecho. Por ejemplo: “Hemos descubierto al asesino gracias a los datos aportados por un testigo”.

Disco duro

Disco duro o disco rígido (en inglés Hard Disk Drive, HDD) es un dispositivo de almacenamiento de datos no volátil que emplea un sistema de grabación magnética para almacenar datos digitales. Se compone de uno o más platos o discos rígidos, unidos por un mismo eje que gira a gran velocidad dentro de una caja metálica sellada. Sobre cada plato, y en cada una de sus caras, se sitúa un cabezal de lectura/escritura que flota sobre una delgada lámina de aire generada por la rotación de los discos.

Esteganografía

Es la parte de la criptología en la que se estudian y aplican técnicas que permiten el ocultamiento de 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 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.

Hacker

Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el fin de obtener información secreta. En la actualidad, el término se identifica con el de delincuente informático, e incluye a los cibernautas que realizan operaciones delictivas a través de las redes de ordenadores existentes.

Hardware

Corresponde a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.¹ Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado; contrariamente, el soporte lógico es intangible y es llamado software.

Huella Digital

La intención de la tecnología de huella digital es identificar de manera precisa y única a una persona por medio de su huella digital. Certificando la autenticidad de las personas de manera única e inconfundible por medio de un dispositivo electrónico que captura la huella digital y de un programa que realiza la verificación.

Imagen forense

Llamada también “Espejo” (en inglés “Mirror”), la cual es una copia bit a bit de un medio electrónico de almacenamiento. En la imagen quedan grabados los espacios que ocupan los archivos y las áreas borradas incluyendo particiones escondidas.

Información

Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Informática forense

Permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos. Gracias a ella, las empresas obtienen una respuesta a problemas de privacidad, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial surgidos a través de uso indebido de las tecnologías de la información. Mediante sus procedimientos se identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal.

Infraestructura Tecnológica

Básicamente, la infraestructura tecnológica es el conjunto de todos los elementos tecnológicos que integran un proyecto o sustentan una operación.

Por ejemplo, las computadoras de un banco, sus redes de datos, los sistemas de energía que las alimentan, etc.

Investigación forense

Las técnicas de forense son la aplicación de una técnica de investigación metódica para reconstruir una secuencia de eventos. Las técnicas de forense digital son el arte de recrear que ha pasado en un dispositivo digital.

IP

es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP. Dicho número no se ha de confundir con la dirección MAC que es un identificador de 48bits para identificar de forma única a la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP, decida asignar otra IP (por ejemplo, con el protocolo DHCP), a esta forma de asignación de dirección IP se denomina dirección IP dinámica (normalmente abreviado como IP dinámica).

Malware

También llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.¹ El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.

Paquetes de red

Paquete de datos a cada uno de los bloques en que se divide, en el nivel de Red, la información a enviar. Por debajo del nivel de red se habla de trama de red, aunque el concepto es análogo.

En todo sistema de comunicaciones resulta interesante dividir la información a enviar en bloques de un tamaño máximo conocido. Esto simplifica el control de la comunicación, las comprobaciones de errores, la gestión de los equipos de encaminamiento (routers), etc.

Programa

Consiste en una clase de software que se diseña con el fin de que para el usuario sea más sencilla la concreción de un determinado trabajo. Esta particularidad lo distingue del resto de los programas, entre los cuales se pueden citar a los sistemas operativos (que son los que permiten el funcionamiento de la computadora), los lenguajes de programación (aquellos que dan las herramientas necesarias para desarrollar los programas informáticos en general) y las utilidades (pensadas para realizar acciones de mantenimiento y tareas generales).

Recuperación de archivos

Es el proceso de restablecer la información contenida en dispositivos de almacenamiento secundarios dañados, defectuosos, corruptos, inaccesibles o que no se pueden acceder de forma normal. A menudo la información es recuperada de dispositivos de almacenamiento tales como discos duros, cintas, CD, DVD, RAID y otros dispositivos electrónicos. La recuperación puede ser debido a un daño físico en el dispositivo de almacenamiento o por un daño lógico en el sistema de archivos que evita que el dispositivo sea accedido desde el sistema operativo.

Red Informática

Una red es un sistema donde los elementos que lo componen (por lo general ordenadores) son autónomos y están conectados entre sí por medios físicos y/o lógicos y

que pueden comunicarse para compartir recursos. Independientemente a esto, definir el concepto de red implica diferenciar entre el concepto de red física y red de comunicación.

Seguridad Informática

Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). 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, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

Servidor

Una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor.

Snifers de red

El sniffer es un software que permite capturar tramas de la red. Generalmente utilizado con fines maliciosos para capturar textos de emails, chats, datos personales, contraseñas, etc.

Por ejemplo: Podemos darle la instrucción a un Sniffer que me capture textos cuando entre estos aparezca una palabra específica, como por ejemplo "contraseña".

La cantidad de tramas que puede obtener un sniffer depende de la topología de red. Para poner en funcionamiento este tipo de software, la persona debe tener algunos conocimientos sobre las estructuras de la red.

Software

Se conoce como software al equipamiento lógico o soporte lógico de un sistema informático, comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos, que son llamados hardware.

2.4 Documentación Técnica

AxCrypt

encripta y protege archivos con un clic

Son muchos los datos, archivos y ficheros que tenemos en nuestra PC que desearíamos mantenerlos seguros, fuera del alcance de personas terceras indeseadas. Y métodos de protección son los que en la actualidad van creciendo de manera radical.

AxCrypt es un programa libre que te permitirá encriptar, codificar y cifrar tus datos, archivos y ficheros más importantes que consideres confidenciales, así de tal manera que sólo tú puedas tener acceso a los mismos mediante la protección con contraseña.

El programa se integra en el explorador de Windows. Cuando le das clic para desplegar el menú de opciones de cualquier fichero o carpeta, estará un nuevo menú llamado AxCrypt el cual te dará varias opciones para cifrar tus datos más importantes.

Algunas de las características más destacadas de AxCrypt son:

- Re-encriptación luego de modificar un archivo cifrado.
- Multilenguaje, más de 7 idiomas disponibles.
- Totalmente libre, con licencia pública general (GPL).
- Integración total en el explorador de Windows.
- De sencillo uso, casi automático.
- Edita cualquier archivo encriptado.

- Y muchas características más.

Es un programa creado para Windows que definitivamente ayudará en la tarea de proteger aquellos archivos que se consideren más importantes y que se desea que estén fuera del alcance de personas curiosas. A probarlo ahora mismo.

Hoja Técnica del software Axcript

Programa: AxCrypt 1.7.2687.

Editor: [Axantum.](#)

Licencia: Gratis.

Tamaño: 1.578 KB.

Idioma: Español / Inglés / Francés / Alemán.

Sistema Operativo: Windows 2003 / Windows XP / Windows Vista / Windows 7.

My Lockbox

My Lockbox es una aplicación gratuita para Windows que permitirá tener una carpeta oculta y protegida con contraseña de una manera fácil y rápida.

Durante la instalación del programa, pedirá que se le indique cual es la carpeta que se debe ocultar y proteger, la contraseña con la que se quiere ocultar, entonces la carpeta quedara lista.

El funcionamiento es muy sencillo, una vez que está instalado sólo se tiene que abrir a través de su icono y saltará una ventana pidiendo la contraseña. Se le introduce y automáticamente muestra en primer plano el contenido de la carpeta privada.

Para volver a ocultarla después de haber estado trabajando con ella sólo se debe ir al icono que deja en la barra de tareas con forma de candado, pulsarle con el botón derecho encima y decirle Lock and quit. Ya se tiene cerrada y completamente oculta ante otras personas.

La carpeta que se le indico al principio de la instalación, se podrá cambiar cuando se desee. Únicamente hay que volver a abrir My Lockbox y luego entrar en las opciones del programa a través del icono de la barra de tareas que se mencionó antes. Ahí, aparte de cambiar la carpeta oculta se podrá cambiar la contraseña que se le indica y otras opciones varias del programa.

Es una herramienta muy útil aunque su uso no es muy complicado teniendo en cuenta que sólo puede ocultar una carpeta. Pero es una aplicación gratuita y una alternativa bastante interesante.

Hoja Técnica del software My Lockbox

Programa: My Lockbox 2.2

Editor: [Espro.](#)

Licencia: Gratis.

Tamaño: 2.470 KB.

Idioma: Inglés.

Sistema Operativo: Windows 2003 / Windows XP / Windows Vista / Windows 7.

Ontrack Easy Drive Data Recovery

Ontrack Easy Drive Data Recovery puede ser usado para recuperar datos desde discos formateados por error. El programa usa los algoritmos potentes únicos que permiten recuperar los archivos que no están presentes en las entradas del sistema de archivos. Seleccione un disco con los datos que será analizado, obtenga la vista preliminar del contenido de archivos y seleccione los archivos a recuperar. No importa en qué circunstancia se hayan perdido los datos, el programa recuperará los archivos borrados accidentalmente por el usuario.

- Se puede obtener la vista preliminar del contenido de archivos antes de recuperarlos.
- El filtro por el nombre de archivo, fecha, tamaño o estado de recuperación está disponible.
- Es posible excluir de los resultados de búsqueda los archivos y carpetas temporales, así como archivos temporales de Internet.
- Es compatible con los nombres de archivos y carpetas en diferentes idiomas.
- Se admiten archivos comprimidos de NTFS y flujos de datos con nombre.

- Los archivos se recuperan aun cuando usted haya reinstalado el sistema operativo.
- Motor de búsqueda de velocidad optimizada.
- Es compatible con la base de datos de la Papelera de reciclaje.
- Es compatible con los sistemas de archivos NTFS, FAT16 y FAT32.
- Es compatible con los discos duros IDE, ATA y SCSI.
- La recuperación de archivos es posible aun cuando el archivo haya sido eliminado en la línea de comandos DOS.
- Es compatible con los discos duros de gran tamaño.
- Es compatible con los sistemas operativos Windows® 2000, XP, Server 2003, Vista, Server 2008 y 7.

Hoja Tecnica del software Ontrack Easy Drive Data Recovery

Programa: Easy Drive Data Recovery 7.1.

Editor: [Espro.](#)

Licencia: Gratis.

Tamaño: 44.5 MB.

Idioma: Español.

Sistema Operativo: Windows XP / Windows 7.

HDD Regenerator:

Es un software que se encarga de reparar los sectores dañados de los discos duros.

Programa: HDD Regenerator

Versión: 1.51.

Editor: Dposoft.

Licencia: \$ 84.99.

Tamaño: 8.386kb.

Idioma: Ingles.

Sistema Operativo: Windows XP, Vista y 7.

Programa HD Tune:

Es un software que realiza la función de escanear todo el disco duro, para dar un informe de la salud del mismo y detectar errores en los sectores.

Programa: HD Tune.

Version: Pro 4.6.

Licencia: \$ 34.95.

Tamaño: 1550kb.

Idioma: Ingles.

Sistema Operativo: Windows XP y 7.

Bit defender 2012 Total Security

Es un programa que da seguridad al sistema operativo y sus demás aplicaciones, detectando todo tipo de malware, spyware, phishing etc.

Programa: Bit defender 2012 Total Security.

Licencia: \$79.95.

Tamaño: 4.00 kb.

Idioma: Español.

Sistema Operativo: Windows 7, 8 y XP.

Beini

Es un software basado en Linux que tiene la función específica de hackear redes inalámbricas capturando sus paquetes y decodificando la clave WEP que tiene la red cercana elegida.

Programa: Beini.

Licencia: GPL.

Tamaño: 4.00kb.

Idioma: Español.

Sistema Operativo: Windows 7, XP y Linux.

Capítulo III

Desarrollo de la solución

3.1 Propuesta de la solución

El proyecto consiste en el desarrollo de un kit de herramientas digitales de informática forense, el cual contiene los programas o aplicaciones necesarias que tienen funciones distintas y se aplican a cada área básica de la informática forense, ya que estas aplicaciones juntas son un kit de la informática forense que ayudarán a resolver los problemas relacionados con la informática forense, y que se presentan en las computadoras que se encuentran en el Laboratorio de Hardware de la Universidad Tecnológica de El Salvador.

El proyecto se desarrollará utilizando un conjunto de programas o software de informática forense, como una herramienta de apoyo didáctico para el Laboratorio de Hardware, es decir se buscarán cada uno de estos programas en la red de internet y se descargarán para poder hacer uso de ellos y sus funcionalidades, cabe destacar que una de las principales ventajas de la creación de este kit de herramientas digitales de informática forense, es que todas las aplicaciones puedan ser accesibles al usuario, y de fácil utilización para dichos usuarios que deseen realizar el seminario de informática forense en el Laboratorio de Hardware de la Universidad Tecnológica de El Salvador.

Después de descargar y tener listas todas las aplicaciones que sirven para la informática forense, se grabarán en un CD o dispositivo de almacenamiento extraíble, de manera que

el usuario pueda ejecutarlas desde aquí e instalar en cualquier computadora de escritorio o laptop, cabe mencionar que todas las aplicaciones que se utilizarán son especialmente para uso en plataforma Windows ya que es el sistema operativo que se está utilizando y el que se tiene en las computadoras del Laboratorio de Hardware.

El funcionamiento de este proyecto estará disponible en el Laboratorio de Hardware de la Universidad Tecnológica de El Salvador, cuando se realicen los seminarios de informática forense se utilizará el kit de herramientas digitales de informática forense como un apoyo didáctico que contenga la teoría sobre el tema a impartir y en la práctica se darán los programas a utilizar en cada área del tema impartido, además de esto los estudiantes que deseen realizar este seminario contarán con el equipo informático necesario proporcionado para poder utilizar cada aplicación que contiene el kit de herramientas digitales de informática forense.

Este proyecto informático, se desarrollará con el objetivo principal de satisfacer las necesidades que tiene el Laboratorio de Hardware, en sus computadoras por los problemas de hardware que se presentan en las mismas como por ejemplo el daño de un sector en un disco duro, daños en el sistema operativo por una lesión física en el disco duro, problemas de software como por ejemplo daños en el sistema operativo por amenazas de malware, descryptar un archivo etc. Será enfocado para el uso de los estudiantes de la Universidad Tecnológica de El Salvador cuando realicen el seminario de informática forense y así puedan tener un mejor conocimiento tanto teórico como

práctico y que conozcan el uso de nuevas aplicaciones que se usan en la informática forense.

El diseño del proyecto, se realizó pensando en las necesidades que se tienen en la Universidad Tecnológica de El Salvador, en su Facultad de Informática y Ciencias Aplicadas en su escuela de Informática que es donde se encuentra el Laboratorio de Hardware, por esto se determinó que para el problema antes mencionado se necesita realizar el diseño de un CD el cual contenga las aplicaciones necesarias para solventar los problemas antes mencionados.

Para el desarrollo del proyecto, es necesario realizar un proceso en el cual se debe de tomar en cuenta varios factores principales como lo son la situación problemática que se resolverá, analizar y comprender la situación problemática, formular la propuesta de solución en base al análisis hecho de la situación problemática, fijar los alcances y delimitaciones que tendrá el proyecto, fijar el objetivo general y los objetivos específicos que se pretenden realizar, desarrollar los productos que serán la solución del problema, etc.

Además del producto principal que es el kit de herramientas digitales de informática forense, también se incluye un manual impreso que contiene la descripción completa de cada uno de los programas informáticos que se van a utilizar para la solución de los problemas de hardware y software que se mencionaron anteriormente en este documento, el manual se ha desarrollado de una manera específica explicando paso a

paso como se utilizará cada programa desde su descarga, instalación, configuración y opciones de uso según sea su función específica, además se incluyen imágenes de los programas durante el proceso de descarga, instalación, configuración y uso de cada uno de ellos.

También se incluye como producto de la solución, al CD interactivo el cual servirá de apoyo y respaldo para el proyecto, tendrá imágenes, fotos, videos etc. Que demostrarán el uso correcto y adecuado de cada aplicación del kit de herramientas digitales de informática forense, usadas para su respectiva situación ya sea problema de hardware o software que involucren informática forense.

A cada uno de los programas que se han elegido para ser parte del kit de herramientas digitales de informática forense, se les ha realizado una evaluación económica dando su precio que tiene directamente del fabricante de este producto y en base a esta cotización económica se ha considerado que puede utilizarse con usuarios comunes que deseen buscar las aplicaciones en la red de internet, cabe destacar que en el manual de utilización del kit de herramientas digitales de informática forense se ha puesto el link desde donde el usuario pueda descargar la aplicación de una manera rápida y segura sin riesgos de descargar un malware perjudicial para la computadora.

El proceso de evaluación económica se realiza de la misma manera para todas las aplicaciones que se han mencionado anteriormente en este documento y además de investigar sus precios en la red desde la página principal del fabricante estos se ven

reflejados en una tabla donde se pone el nombre del producto, su precio y se hace una comparación con otras dos aplicaciones similares ósea con la misma función y perteneciente a la misma área de informática forense para poder determinar cuál de estas aplicaciones es la más factible para el usuario.

Después de realizar esta evaluación económica se realizó la evaluación técnica de cada una de las aplicaciones la cual consiste en investigar por lo menos las características técnicas básicas que debe tener cada uno de los programas y estas se asignan en base a su funcionamiento y configuraciones que tenga el software y luego se asignan porcentajes que sean válidos a cada característica que será evaluada dentro del programa seleccionado y en base a la cantidad de puntos que el programa hace en cada una de sus características se determina si es aprobado o es reprobado.

La propuesta de la solución se puede resumir tomando en cuenta cada uno de los productos que se están ofreciendo como respuesta a la problemática planteada, los cuales ya han sido descritos detenidamente sabiendo la función de cada uno de ellos y como sirven de complemento el uno con el otro para poder tener una mejor valoración a la hora de que se quiera evaluar de cualquier manera tomando en cuenta que lo que se evalúa es cada uno de los recursos que se utilizan en cada producto, ya sean recursos didácticos, tecnológicos, metodológicos, económico, técnico, etc.

Con la realización de este proyecto de informática forense, como grupo de trabajo se propone a la Universidad Tecnológica de El Salvador que para la realización de los

seminarios de informática forense impartidos en el Laboratorio de Hardware, se tome en cuenta este producto que es un kit de herramientas digitales de informática forense que se ofrece con la finalidad de mejorar la calidad de enseñanza en la Universidad y también se pretende que los estudiantes que participen en estos seminarios puedan adquirir un mejor conocimiento acerca de la informática forense, su aplicación, su uso, y la utilización de programas que ayuden a resolver problemas de hardware y software en las computadoras del Laboratorio de Hardware.

Es de tomar en cuenta de que cada uno de los programas que se utilizarán tienen sus ventajas y desventajas, pero ya han aprobado un proceso de evaluación técnica y evaluación económica en el cual fueron seleccionados para cubrir las áreas de la informática forense que se han investigado durante el desarrollo del marco teórico de referencia el cual posee toda la teoría buscada y seleccionada de fuentes de información confiables, esta ha sido la base para el desarrollo e implementación de cada uno de los productos creados.

3.2 Conclusiones

Durante el desarrollo de este proyecto, titulado: Desarrollo de un kit de herramientas digitales de informática forense para las soluciones a problemas de hardware como por ejemplo el daño de un sector de un disco duro y software como por ejemplo el daño del sistema operativo debido a malware, en el laboratorio de hardware de la Universidad Tecnológica de El Salvador se pretende lograr el beneficio de los estudiantes de la facultad de Informática y Ciencias Aplicadas de la Universidad Tecnológica de El

Salvador, que deseen participar en los seminarios impartidos por la Cátedra de Hardware en el Laboratorio de Hardware, en el cual se ha podido incluir como material de apoyo didáctico un kit de herramientas digitales de informática forense, para poder demostrar que los programas contenidos aquí pueden resolver los problemas de hardware y software que muchas veces se presentan en las computadoras del Laboratorio de Hardware.

Además de esto los estudiantes de los seminarios de informática forense podrán fortalecer sus conocimientos, tanto teóricamente, como en la práctica conociendo programas útiles y fáciles de utilizar que ayudan a resolver problemas de hardware y software mencionados anteriormente que se presentan en las computadoras del Laboratorio de Hardware, también el estudiante podrá contar con el equipo informático necesario para facilitarle el uso de cada uno de los programas que se están presentando.

También se hizo un CD interactivo, que servirá de apoyo al desarrollo del seminario de informática forense además del kit de herramientas digitales de informática forense y el manual de utilización del kit de herramientas digitales de informática forense, tendrá imágenes, fotos, videos del tema que ha sido abordado en este documento.

La experiencia adquirida en el desarrollo de este proyecto, durante la creación de los tres productos ha demostrado la importancia que tiene la informática forense en el campo de la misma informática, como una área que se desarrolla utilizando el software como una herramienta digital para poder resolver los problemas de hardware y software que tienen

las computadoras del Laboratorio de Hardware de la Universidad Tecnológica de El Salvador.

3.3 Recomendaciones

- Agregar Software para detectar intrusos en redes inalámbricas, al kit de herramientas digitales de informática forense.
- Incorporar aplicaciones de plataforma Linux.
- Incluir programa para rastrear información a través de las redes sociales.
- Usar software o links para detectar información a través de los correos electrónicos.
- Agregar más información relacionada al tema como por ejemplo kit móvil de informática forense entre otros. Para que el documento sea más amplio en el tema que se ha tratado.
- Utilizar el manual para cada uno de los programas y realizar los pasos indicados en orden que están en el mismo.
- Utilizar el CD interactivo como un apoyo didáctico más.
- Evaluar cada uno de los programas según el criterio de usuario y comparar con otros que tengan las mismas funciones.
- Tomar en cuenta la bibliografía del documento a la hora de buscar mas información en internet.

3.4 Bibliografía

- Forense, G. (2012). *Herramientas de la informática forense*. Obtenido de <http://www.ondata.es/recuperar/forensics-guidance.htm>
- Giovanni Zuccardi, J. D. (2010). *Usos de la informática forense*. Obtenido de <http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf>
- Hackeo, w. m. (2012). *Hackeo de redes Wireless*. Obtenido de <http://www.seguridadwireless.net/hwagm/commview-for-wifi.html>
- Jose Pastor Franco, M. A. (2001). *Tipos de Criptografías*. Obtenido de <http://es.wikipedia.org/wiki/Criptograf%C3%ADa>
- Journal, A. o. (2012). *Recuperación de información*. Obtenido de <http://seri.org.es/pages/recursos/revistas>
- Martinez, E. (2012). *Pasos de la informática forense*. Obtenido de http://es.wikipedia.org/wiki/C%C3%B3mputo_forense
- Molina, B. (2012). *Esteganografía*. Obtenido de <http://sanmartinbaq.edu.co/revistas/index.php/gd/article/view/49>
- Oscar Lopez, H. A. (2012). *Herramientas de investigación forense*. Obtenido de http://www.criminalistaenred.com.ar/Informatica_F.html
- Talens, S. (2012). *Áreas principales de la Informática Forense*. Obtenido de <http://www.uv.es/~sto/articulos/BEI-2003-04/criptologia.html>
- Wikipedia. (2001). *Qué es la Informática Forense*. Obtenido de http://es.wikipedia.org/wiki/C%C3%B3mputo_forense