

Universidad Tecnológica de El Salvador

FACULTAD: INFORMÁTICA Y CIENCIAS APLICADAS

CARRERA: TÉCNICO EN INGENIERÍA DE HARDWARE



TEMA:

ELABORACIÓN DE UN KIT DE SOFTWARE DE INFORMÁTICA FORENSE
PARA SU USO EN LA ÁREA DE SEGURIDAD Y RECUPERACIÓN DE
INFORMACIÓN EN BENEFICIO DE LOS LABORATORIOS DE INFORMÁTICA
DE LA UNIVERSIDAD TECNOLÓGICA DEL SALVADOR

TRABAJO DE GRADUACIÓN PRESENTADO POR:

JOSE EDUARDO CALLEJAS LÓPEZ

DAVID ERNESTO VÁSQUEZ CARTAGENA

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERÍA DE HARDWARE.

SEPTIEMBRE, 2015

SAN SALVADOR, EL SALVADOR, CENTROAMERICA

PÁGINA DE AUTORIDADES ACADÉMICAS

ING. NELSON ZÁRATE SÁNCHEZ

RECTOR

LIC. JOSE MODESTO VENTURA

VICERRECTOR ACADEMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

LIC. LILIAN NOEMÍ ROMERO DE LEIVA

PRESIDENTE

ING. MARIO ALBERTO VALLE AGUIRRE

PRIMER VOCAL

ING. HUGO JOEL ORTIZ

SEGUNDO VOCAL

SEPTIEMBRE, 2015

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:

Ing. Mario Alberto Valle Aguirre, Ing. Hugo Joel Ortiz Saldaña, Licda. Lilian Noemí Romero de Leiva, a las 12:30m. del día Martes, 23 de junio de dos mil quince.

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

- | | |
|---|----------------------------|
| 1- <u>José Eduardo Callejas López</u> | <u>Carnet 28-1971-2013</u> |
| 2- <u>David Ernesto Vásquez Cartagena</u> | <u>Carnet 28-1973-2013</u> |

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:

"Elaboración de un kit de software de informática forense para el uso en el área de seguridad y recuperación de información en beneficio de los laboratorios de la Universidad Tecnológica de El Salvador"

PARA OPTAR AL GRADO DE:

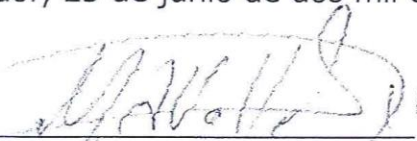
TÉCNICO EN INGENIERIA DE HARDWARE

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

Aprobado

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

San Salvador, 23 de junio de dos mil cinco.

F. 

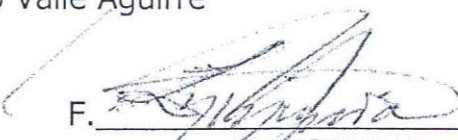
PRIMER VOCAL

Ing. Mario Alberto Valle Aguirre

F. 

SEGUNDO VOCAL

Ing. Hugo Joel Ortiz Saldaña

F. 

PRESIDENTE

Licda. Lilian Noemí Romero de Leiva

Agradecimiento

Le agradezco a Dios por darme la oportunidad de culminar mi carrera, por ser mi compañero en todo los momentos y por brindame una vida llena de aprendizajes, experiencias y sobre todo mucha felicidad.

Gracias a mis padres José Andrés Y Dora Yaneth por estar a mi lado en todo momento, por sus enseñanzas y consejos y por haberme dado la oportunidad de tener una excelente educación en mi vida.

A mis hermanos Iris Xiomara y Marvin Wilfredo por ser ejemplo de desarrollo profesional, gracias por apoyarme siempre y por ser parte de mi vida y por conformar la familia que somos.

Gracias Ingeniero Hugo Joel Ortiz por su conocimiento, confianza, apoyo y por habernos brindado su ayuda en la elaboración de nuestra tesis profesional y por aprender cosa nuevas que me ayudara en mi vida.

A mi compañero de tesis y amigos por su amistad y por creer en mi todo el tiempo y por haber hecho de mi etapa universitaria la mejor de mi vida. Gracias amigos.

Eduardo Callejas

Quiero agradecerle a Dios por darme la oportunidad de vivir y alcanzar todas mis metas propuestas, por ser mi guía y mi compañía en todo momento y darme felicidad cada día de mi vida.

A mis padres María Francisca y Israel Vásquez por tanto apoyo que me han brindado en cada etapa de mi vida, por guiarme y ayudarme a levantar y seguir en momentos difíciles y darme la oportunidad de estudiar y crecer en mi vida.

A nuestro asesor ing. Hugo Joel Ortiz por el apoyo, la ayuda y conocimiento que nos brindó en la elaboración de nuestro proyecto además de la paciencia.

A mi compañero de tesis que me brindó su apoyo y esfuerzo y a todos mis compañeros que hicieron de la universidad un sitio ameno de aprendizaje.

A todos los maestros de la universidad por esforzarse para que cada nuevo año surjan nuevos profesionales y personas de bien para la sociedad.

David Vásquez

Contenido

Introducción.....	i
Capítulo I Situación Actual.....	1
1.1 Situación Problemática	1
1.2 Enunciado Del Problema	2
1.3 Justificación	2
1.4 Objetivos	3
1.4.1 Objetivo General:.....	3
1.4.2 Objetivos Específicos:.....	4
1.5 Delimitaciones	4
1.5.1 Delimitación Geográfica	4
1.5.2 Delimitación Organizacional	4
1.5.3 Delimitación Temporal	5
1.6 Alcances	6
1.7 Estudio De La Factibilidad	8
1.7.1 Factibilidad Económica.....	8
1.7.2 Estudio De La Factibilidad Técnica	13
Capítulo II Documentación Técnica	18
2.1 Marco Teórico De Referencia.....	18
2.1.1 ¿Qué es la Informática Forense?	18
2.1.2 Objetivos de la Informática Forense	19
2.1.3 Pasos de la Informática Forense.....	20
2.1.4 Áreas de utilización de la Informática Forense	22
2.1.5 Ley Especial Contra Actos De Terrorismo	23
2.1.6 Ciencia Forense.....	24

2.1.7 Principio de Transferencia de Locard	25
2.1.8 Criptografia	26
2.1.9 Software de Informática Forense	28
2.2 Marco Teórico De La Solución.....	31
2.2.1 Ley Especial Contra Actos De Terrorismo	31
2.2.2 Instalación y uso de los programas	32
2.2.3 Lista de programas utilizados	130
2.2.4 Kit de herramienta en DVD y manual impreso.....	130
2.3 Marco Teórico Conceptual.....	131
2.4 Documentación Técnica.....	134
Capítulo III Desarrollo de la solución.....	149
3.1 Propuesta de la solución.....	149
3.2 Conclusiones	153
3.3 Recomendaciones	155
Referencias.....	156
Anexos	157
A1- Matriz De Congruencia.....	157

Introducción

En el presente trabajo se realizó una investigación sobre la Informática Forense, la utilización y formas de aplicaciones de Software Forense, en las diferentes áreas de la Informática.

En el primer capítulo denominado situación actual se plantea la situación problemática, cual es el motivo por el cual se realiza esta investigación, por ejemplo problemas relacionados con delitos informáticos, y cuál es la solución que se realizara así como los objetivos que se pretenden alcanzar con esta investigación.

También se realizó un estudio enfocado a la investigación y reconocimiento de problemas de los laboratorios de Informática de la Universidad Tecnológica de El Salvador, así como la resolución de dichos problemas utilizando Software de Informática Forense mejorando así el rendimiento en el Sistema Operativo y evitando problemas de pérdidas de información y datos importantes.

La Informática Forense está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y/o al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada (por Ej. El Internet), y al extenso uso de computadores por parte de las compañías de negocios tradicionales (por Ej. Financieras, Gobierno, Universidades). Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que los computadores guardan la información de

información forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación Forense como una ciencia relativamente nueva. Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada. La Informática Forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

En el tercer capítulo se muestra el resultado de toda la investigación, pruebas y desarrollo del manual impreso que sirve de apoyo para el Kit de Software de Informática Forense el cual se utilizaran en los laboratorios de Informática de la Universidad Tecnológica de El Salvador.

En el capítulo denominado propuesta de solución esta detallado como se desarrolló el Kit de Software de Informática Forense desde la selección de programas hasta el uso de cada uno; además de la creación del manual con todos los pasos de uso de dichos programas.

También en el tercer capítulo se encuentran las conclusiones y recomendaciones acerca del Kit de Software y manual impreso.

Capítulo I Situación Actual

1.1 Situación Problemática

Las nuevas tecnologías y el desarrollo del mercado relacionado con nuevos dispositivos que permiten el acceso a las nuevas comunicaciones están desarrollados, a través de una evolución tecnológica que es aprovechada por personas malintencionadas ya que utilizan la gama de herramientas tecnológicas para otros fines incorrectos, como lo que es la realización de un crimen de índole Informático, valiéndose muchas veces de que la información queda almacenada en forma digital, esto crea problemas logísticos ya que pueden sustraerla y manipularla de manera errónea. Cuando pasa una situación de este tipo se presentan algunos problemas, debido a que las computadoras guardan la información que pueden ocuparla como evidencia de forma tal que no puede ser recolectada por medios comunes, si no que se requiere la utilización de mecanismos diferentes a los tradicionales.

El Salvador experimenta una amplia variedad de delitos Informáticos, siendo este uno de los problemas que empieza a afectar a la ciudadanía. Este tipo de delitos no excluyen a nadie, afecta a todos los sectores que conforman nuestro país, como todo tipo de violencia afecta las posibilidades de desarrollo del país.

Los laboratorios de Informática de la Universidad Tecnológica de El Salvador presentan diferentes problemas relacionados con Hardware y Software, estos problemas afectan el funcionamiento de las computadoras y representan dificultades al momento de utilizarla.

Los problemas son los siguientes:

- Problemas de privacidad
- Pérdida de información
- Problemas de disco duro por sectores dañado
- Formateo de unidades de almacenamiento que hayan contenido información importante
- Robo de información confidencial

1.2 Enunciado Del Problema

¿De qué forma se pueden solucionar problemas Informáticos relacionados con la seguridad y pérdida de información para las computadoras de los laboratorios de Informática de la Universidad Tecnológica de El Salvador?

1.3 Justificación

El proyecto surge a partir de las necesidades de la Universidad Tecnológica de El Salvador, de implementar un método de solución para los problemas de Software y Hardware en las computadoras, y proporcionar una herramienta digital para solucionar los problemas antes mencionados.

El proyecto consta en la realización de un Kit de Software de Informática Forense y con esto se pretende solucionar problemas de recuperación de datos, escaneo y limpieza en los discos duros, recuperación de archivos perdidos en particiones borradas por los alumnos, pantalla de color azul al encender la computadoras (esto pasa con Windows XP, Windows 7 y pocas veces en Windows 8).

El kit de Software de Informática Forense se realizara con el objetivo principal de brindarle a la Universidad Tecnológica de El Salvador una herramienta para solucionar los problemas de mal funcionamiento del Software y Hardware, como por ejemplo cuando se pretende ofrecer a la venta un producto para el área de Informática el cual cumpla con las exigencia de los clientes, en la recuperación de información valiosa, limpieza de las computadoras y restauración del Sistema Operativo, entre otras necesidades del Software y Hardware .

Las ventajas que tiene la realización de este proyecto están:

- 1- Ayudará a los estudiantes a tener un aprendizaje más completo, en teoría de Informática Forense y práctica utilizando las herramientas digitales adecuadas.
- 2- Brindará una solución más rápida y eficiente a los responsables de los laboratorios de informática para resolver problemas Software y Hardware en las computadoras de los laboratorios de informática.
- 3- Mayor facilidad en el manejo de información y recolección y análisis de la misma.

1.4 Objetivos

1.4.1 Objetivo General:

Desarrollar un Kit de Software de Informática Forense para realizar el mantenimiento correctivo y preventivo a las computadoras de los laboratorios de Informática de la Universidad Tecnológica de El Salvador.

1.4.2 Objetivos Específicos:

- 1- Investigar diferentes herramientas de Software de Informática Forense su uso y aplicación en cuanto a mantenimiento correctivo y preventivo.
- 2- Desarrollar un Kit de Software de Informática Forense para mejorar y proteger las computadoras de los laboratorios.
- 3- Crear un manual que contenga los conocimientos teóricos sobre el uso de Software de Informática Forense.

1.5 Delimitaciones

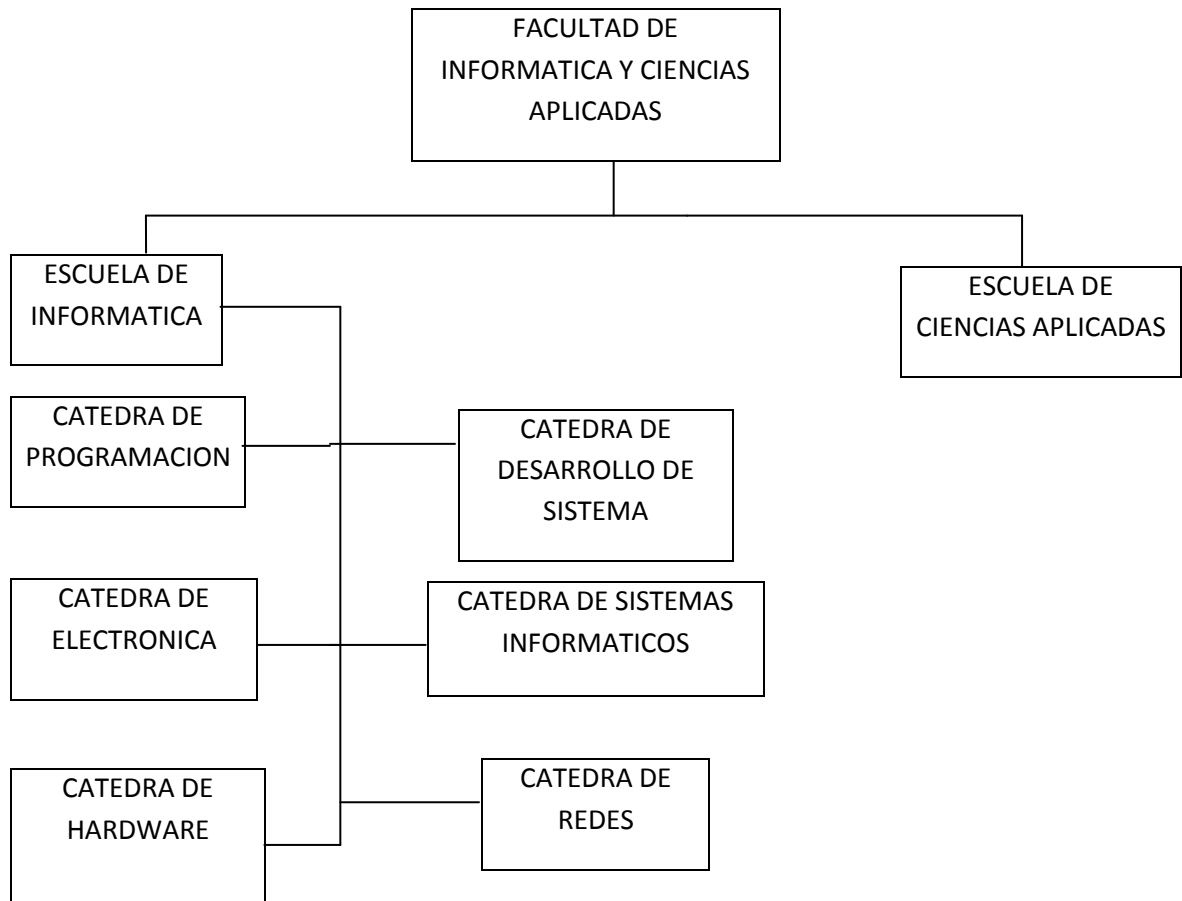
1.5.1 Delimitación Geográfica

Se realizara en el departamento de San Salvador usando como punto de referencia la Universidad Tecnológica de El Salvador, Calle Arce N.º 1020.

1.5.2 Delimitación Organizacional

El proyecto se llevara a cabo en la Universidad Tecnológica de El Salvador, en la Facultad de Informática y Ciencias Aplicadas.

La Escuela de Informática, se divide en las siguientes seis ramas: Hardware, Redes, Desarrollo de Sistemas, Programación y Sistemas Informáticos.



1.5.3 Delimitación Temporal

Del 16 de Febrero al 06 de Junio del 2015

1.6 Alcances

Al realizar este proyecto se ofrecerá un kit de Software de Informática Forense para la utilización en los laboratorios de Informática, además un material de apoyo y consulta que irá enfocado directamente al uso correcto de aplicaciones para resolver problemas de Software y Hardware, los cuales se identificaron haciendo uso de las computadoras. Entre los principales problemas a resolver están:

Problemas de Software

- Encriptar y Desencriptar archivos
- Daños en el sistema operativo por causa de malware
- Perdida de información
- Fallos a la hora de copiar, mover, borrar o crear ficheros

Problemas de Hardware

- Recuperación de información de sectores defectuosos
- Sectores defectuoso debido a una mala magnetización en discos duros
- Daños físicos en los discos duros

En el laboratorio de Hardware estará el manual para que los alumnos o encargados hagan el uso correcto de la utilización del Kit de Software de Informática Forense el cual brindará conocimientos teóricos y prácticos con imágenes de cómo utilizar el kit de herramientas.

PROMESA	PRODUCTO
Investigar las herramientas que se utilizan en la Informática Forense.	Herramientas de Software de Informática Forense.
Desarrollar un Kit de Software de Informática Forense.	Kit de Software para Informática Forense en formato “DVD”.
Conocer los pasos teóricos y prácticos de cómo utilizar el Kit de Software de Informática Forense.	Manual impreso.

1.7 Estudio De La Factibilidad

1.7.1 Factibilidad Económica

Cuadro de Evaluación económico de programas de diagnósticos de discos duros			
Estudio de Factibilidad económica			
Nombre del producto	Acronis Drive Monitor	Active Smart 2.9	HDDScan
Precios	\$0.0	\$33.00	\$0.0
Análisis	En el siguiente estudio económico se muestra que los programas Acronis Drive Monitor y HDDScan son los más factibles ya que son licencias gratuitas.		
Establecimiento consultado o URL	http://descargar.cnet.com/Acronis-Drive-Monitor/3000-2086_4-75212597.html	http://active-smart.waxoo.com/	http://www.gizmos.es/programas-y-aplicaciones/hddscan-30-una-herramienta-de-diagnostico-de-tu-disco-duro.html

Cuadro de Evaluación económico de reparadores de discos duros			
Estudio de Factibilidad económica			
Nombre del producto	TestDisk 7.0	Disk Heal	HDD Regenerator
Precios	\$0.0	\$0.0	\$99.99
Análisis	En el siguiente estudio económico se muestra que los programas TestDisk 7.0 y Disk Heal son los más factibles ya que son licencias gratuitas.		
Establecimiento consultado o URL	http://es.wikipedia.org/wiki/TestDisk	http://disk-heal.uptodown.com/	http://www.intercambiosvirtuales.org/software/hdd-regenerator-2011-repara-facilmente-sectores-defectuosos-de-tu-disco-duro

Cuadro de Evaluación económico de recuperación de información y archivos			
Estudio de Factibilidad económica			
Nombre del producto	Recovery my files v5	Handy Recovery	Easy Drive Data Recovery
Precios	\$0.0	\$49.99	\$15
Análisis	En el siguiente estudio económico se muestra que el programa Recovery my file es el más factible ya que su licencia es la de menor valor.		
Establecimiento consultado o URL	http://www.intercambiosvirtuales.org/software/filerecovery-2013-v5-professional-multilenguaje-espanol-herramienta-definitiva-para-la-recuperacion-de-archivos-y-datos	http://www.handyrecovery.es/	http://www.intercambiosvirtuales.org/software/ontrack-easyrecovery-professional-v10-0-2-3-espanol-recuperar-archivos-danados-o-borrados-aun-despues-de-formatear

Cuadro de Evaluación económico de programas de seguridad informática			
Estudio de Factibilidad económica			
Nombre del producto	Bit Defender Total Security 2015 V.18.11	Panda Internet Security 2015	Outpost Security Suite Pro V.9.1
Precios	\$89.95	\$ 37.00	\$29.95
Análisis	En el siguiente estudio económico se muestra que el programa Outpost Security Suite Pro es el más factible ya que es de menor valor.		
Establecimiento consultado o URL	http://www.fiuxy.com/programas-gratis/3660996-bitdefender-internet-security-2015-build-18-11-0-872-una-muy-buena-suite-de-seguridad.html	http://www.port.alprogramas.com/panda-antivirus/interne-t-security/	http://descargar.cnet.com/Agnitum-Outpost-Security-Suite-Pro-64-bit/3000-18510_4-75130122.html

Cuadro de Evaluación económico de programas de criptografía			
Estudio de Factibilidad económica			
Nombre del producto	TrueCrypt v7.2	Axcrypt V1.7.2850	CryptoForge v4.2.0
Precios	\$0.0	\$0.0	\$0.0
Análisis	En el siguiente estudio económico se muestra que los 3 programas: TrueCrypt V7.2; Axcrypt V1.7.2850 y CryptoForge V4.2.0 son factibles ya que son licencias gratuitas.		
Establecimiento consultado o URL	http://www.abcdatos.com/programa/truencrypt-linux.html	http://www.abcdatos.com/programa/prouter-documentos.html	http://www.abcdatos.com/programa/herramientas-encryptacion.html

1.7.2 Estudio De La Factibilidad Técnica

Evaluación programas de diagnóstico de discos duros se requiere un nivel de calificación del 75%

Característica técnica	ponderación	Acronis Drive Monitor		Active Smart 2.9		HDDScan	
		Valor	Total	Valor	Total	Valor	Total
Reconocimiento de, errores físicos	30%	2	60	1	30	2	60
Lector de temperatura	20%	2	40	2	40	2	40
Utilidades de reparación	20%	0	0	0	0	2	40
Prueba de rendimiento	20%	2	40	1	20	2	40
Interfaz grafica	10%	2	20	1	10	2	20
Totales	100%		160		100		200
Final		160/2	80	100/2	50	200/2	100

Análisis: en el cuadro anterior se hizo la comparación de 3 programas para diagnóstico de discos duros, y se escogió a Acronis Driver Monitor porque es el 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 programas de reparadores de discos duros se requiere un nivel de calificación del 70%

Característica técnica	Ponderación	TestDisk 7.0		Disk Heal		HDD Regenerator	
		Valor	Total	Valor	Total	Valor	Total
Reconoce sectores dañados	20%	2	40	1	20	2	40
Soporte de varios formatos	20%	1	20	2	40	2	40
Repara sectores defectuosos	30%	2	60	2	60	2	60
Almacenamiento de reportes	20%	0	0	0	0	0	0
Interfaz grafica	10%	1	10	1	20	2	20
Totales	100%		130		140		160
Final		130/2	65	140/2	70	160/2	80

Análisis: En el cuadro anterior se hizo 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 programas de recuperación de archivos se requiere un nivel de calificación del 85%

Característica técnica	Ponderación	TestDisk 7.0		Handy Recovery		EasyDrive Data Recovery	
		Valor	Total	Valor	Total	Valor	Total
Búsqueda profunda	20%	2	40	2	20	2	40
Visualizar un archivo antes de recuperarlo	20%	1	20	2	40	2	40
Recuperación de distintos tipos de archivos	30%	2	60	2	60	2	60
Archivos borrados en papelera de reciclaje	20%	1	20	2	20	2	40
Fácil uso	10%	1	10	2	20	1	10
Totales	100%		150		160		190
Final		150/2	75	160/2	80	190/2	95

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

Evaluación programas de seguridad informática se requiere un nivel de calificación del 90%

Característica técnica	Ponderación	Bit defender Security 2015 V.18.11		Panda Internet Security 2015		Outpost Security Suite Pro V.9	
		Valor	Total	Valor	Total	Valor	Total
Protección antivirus	20%	2	40	1	20	2	40
Optimización del sistema	20%	2	40	1	20	2	40
Protección de internet	30%	2	60	2	60	2	60
Análisis profundo	20%	2	40	1	20	1	20
Fácil uso	10%	1	10	2	20	2	20
Totales	100%		190		140		180
Final		190/2	95	140/2	70	180/2	90

Análisis: En el cuadro anterior se hizo la comparación de 3 programas que sirven para la seguridad informática y se ha escogido a Outpost Security Suite Pro V.9 porque es una protección para malware.

Evaluación programas de criptografía se requiere un nivel de calificación del 80%

Característica técnica	Ponderación	TrueCrypt v7.2		Axcrypt V1.7.2850		CryptoForge v4.2.0	
		Valor	Total	Valor	Total	Valor	Total
Protección de ficheros	30%	2	60	2	60	2	60
Utilización de clave de seguridad	30%	0	00	0	20	1	30
Codifica varios tipos de archivos	30%	2	60	2	60	2	60
Fácil uso	10%	1	10	2	20	2	20
Totales	100%		130		160		170
Final		130/2	65	160/2	80	170/2	85

Análisis: En el cuadro anterior se hizo la comparación de 3 programas que sirven para que la información se mantenga oculta y protegida, por ello se escogió a Axcrypt por que cumple con las características técnicas necesarias para brindar seguridad.

Capítulo II Documentación Técnica

2.1 Marco Teórico De Referencia

2.1.1 ¿Qué es la Informática Forense?

La Informática Forense se puede describir como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional para poder hacer uso de esos datos presentándolos como evidencia de algún delito (Zuccardi, 2006).

Debido a que la Informática Forense se utilizó para presentar pruebas contundentes se aplicó la Informática Forense como una disciplina auxiliar de la justicia moderna, desde entonces en el año 1984, el laboratorio del FBI y otras agencias que buscan el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional (Zuccardi, 2006).

La Informática Forense puede abarcar diferentes áreas: (Martinez, 2006).

Computación Forense (computer forensics): se puede entender como una disciplina dentro de las ciencias forenses, está enfocada a descubrir e interpretar la información en los medios informáticos para establecer hechos y formular hipótesis relacionadas con los casos o delitos; o como una disciplina científica y especializada que entiende los elementos propios de las tecnologías de los equipos de computación y ofrecer un análisis de la información residente en dichos equipos.

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

Esta conjunción de palabras establece a un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha utilizado para desarrollar y concluir su acción. (Lopez, 2001).

Forense Digital (digital forensic) (Mosquera, 2005): es la forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿por qué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

2.1.2 Objetivos de la Informática Forense (Zuccardi, 2006)

Los 3 objetivos principales de la Informática Forense son:

1. La compensación de los daños causados por criminales o intrusos.
2. La persecución y procesamiento judicial de los criminales.
3. La creación y aplicación de medidas para prevenir casos similares.

2.1.3 Pasos de la Informática Forense

Para que dichos objetivos sean logrados se debe de seguir una serie de pasos que en la Informática Forense son necesarios para la recolección de evidencias en casos de delitos informáticos

Identificación.

Es muy importante conocer los antecedentes a la investigación "HotFix"(Hotfix es una utilidad que se utiliza en la instalación de revisiones de Windows NT. Una revisión es una colección de uno o más archivos que se pueden aplicar a un sistema con el fin de corregir un problema.) , situación actual y el proceso que se quiere seguir para poder tomar la mejor decisión con respecto a las búsquedas y las estrategias (debes estar bien programado y sincronizado con las actividades a realizar, herramientas de extracción de los registros de información a localizar). Incluye muchas veces (en un momento específico Observar, Analizar Interpretar y Aplicar la certeza, esto se llama criterio profesional que origina la investigación) 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 (clonador de disco) para poder mantener la integridad de la evidencia y la cadena de custodia que se requiere (soportes). Al realizar una imagen forense, nos referimos al proceso que se requiere para generar una copia “bit-a-bit” (copia binaria) de todo el disco duro, 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, jueces o instancias que soliciten este informe, la generación (si es el caso) de una pericial y de su correcta interpretación sin hacer uso de tecnicismos; se deberá presentar de manera cauta, prudente y discreta al solicitante la documentación ya que siempre existirán puertas traseras dentro del sistema en observación y debe ser muy específica la investigación dentro del sistema que se documenta porque se compara y vincula una plataforma de telecomunicación y computo forense y que están muy estrechamente enlazadas no omitiendo los medios de almacenamiento magnéticos portables estos son basamentos sobre software libre y privativo. Deberá ser muy cuidadosa la información a entregar porque se maneja el prestigio técnico según las plataformas y sistemas. (Giovanni Zuccardi, 2006)

2.1.4 Áreas de utilización de la Informática Forense

Existen varias áreas de uso en las que se puede aplicar la Informática Forense, varios de estos usos provienen de la vida cotidiana y no están precisamente relacionados solo con la informática:

1. Persecución criminal. La evidencia recolectada es evidencia incriminatoria y puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.

2. Litigación civil. En casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser evidenciados con informática forense.
3. 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.
4. Temas corporativos. se puede recolectar información en casos que traten sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria e incluso espionaje industrial.
5. Mantenimiento de la ley. La Informática Forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

2.1.5 LEY ESPECIAL CONTRA ACTOS DE TERRORISMO

Delito informático

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

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

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

b)

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

La ley anterior se encarga de sancionar delitos a personas que utilicen las herramientas informáticas en la creación de actos delictivos.

2.1.6 Ciencia Forense

La Ciencia Forense proporciona los principios y técnicas que facilitan la investigación del delito criminal, en otras palabras: cualquier principio o técnica que puede ser aplicada para identificar, recuperar, reconstruir o analizar la evidencia durante una investigación criminal forma parte de la ciencia forense (Martinez, 2001).

Los principios científicos que hay detrás del procesamiento de una evidencia son reconocidos y usados en procedimientos como:

- Recoger y examinar huellas dactilares y ADN.
- Recuperar documentos de un dispositivo dañado.
- Hacer una copia exacta de una evidencia digital.
- Generar una huella digital con un algoritmo Hash MD5 o SHA1 de un texto para asegurar que este no se ha modificado.
- Firmar digitalmente un documento para poder afirmar que es auténtico y preservar la cadena de evidencias.

Un Forense aporta su entrenamiento para ayudar a los investigadores a reconstruir el crimen y encontrar pistas. Aplicando un método científico analiza las evidencias disponibles, crea hipótesis sobre lo ocurrido para crear la evidencia y realiza pruebas, controles para confirmar o contradecir esas hipótesis. Esto puede llevar a una gran cantidad de posibilidades sobre lo que pudo ocurrir, esto es debido a que un forense no puede conocer el pasado, no puede saber qué ocurrió ya que sólo dispone de una información limitada. Por esto, sólo puede presentar posibilidades basadas en la información limitada que posee. Un principio fundamental en la ciencia forense, que se usa continuamente para relacionar un criminal con el crimen que ha cometido, es el Principio de Intercambio o transferencia de Locard, (Edmond Locard) francés fundador del instituto de criminalística de la universidad de Lion.

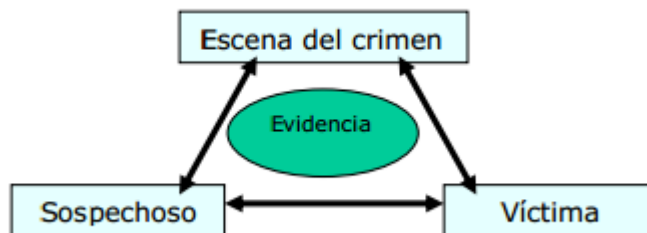


Figura 1 transferencia de Locard <http://e-informaticaforense.blogspot.com/>

2.1.7 Principio de Transferencia de Locard. (Zuccardi, 2006)

Este principio fundamental viene a decir que cualquiera o cualquier objeto que entra en la escena del crimen deja un rastro en la escena o en la víctima y vice-versa (se lleva consigo), en otras palabras: “cada contacto deja un rastro”. En el mundo real significa

que si piso la escena del crimen con toda seguridad dejaré algo mío ahí, pelo, sudor, huellas, etc. Pero también me llevaré algo conmigo cuando abandone la escena del crimen, ya sea barro, olor, una fibra, etc. Con algunas de estas evidencias, los forenses podrán demostrar que hay una posibilidad muy alta de que el criminal estuviera en la escena del crimen.

2.1.8 CRIPTOGRAFIA

La palabra criptografía es un término genérico que describe todas las técnicas que permiten cifrar mensajes o hacerlos ininteligibles sin recurrir a una acción específica. El verbo asociado es cifrar.

La criptografía se basa en la aritmética: En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números (en forma de bits ya que los equipos informáticos usan el sistema binario) y luego realizar cálculos con estos números para:

Modificarlos y hacerlos incomprensibles. El resultado de esta modificación (el mensaje cifrado) se llama texto cifrado, en contraste con el mensaje inicial, llamado texto simple.

Asegurarse de que el receptor pueda descifrarlos.

El hecho de codificar un mensaje para que sea secreto se llama cifrado. El método inverso, que consiste en recuperar el mensaje original, se llama descifrado.

El cifrado normalmente se realiza mediante una clave de cifrado y el descifrado requiere una clave de descifrado. Las claves generalmente se dividen en dos tipos:

Las claves simétricas: son las claves que se usan tanto para el cifrado como para el descifrado. En este caso hablamos de cifrado simétricos o cifrados con clave secreta.

Las claves asimétricas: son las claves que se usan en el caso del cifrado asimétrico (también llamado cifrado con clave pública). En este caso, se usa una clave para el cifrado y otra para el descifrado.

En inglés, el término decryption (descifrado) también se refiere al acto de intentar descifrar en forma ilegítima el mensaje (ya conozca o no el atacante la clave de descifrado).

Cuando el atacante no conoce la clave de descifrado, hablamos de criptoanálisis o criptoanálisis (también se usa el término decodificación).

La criptología es la ciencia que estudia los aspectos científicos de estas técnicas, es decir, combina la criptografía y el criptoanálisis.

El cifrado es la ciencia de la evolución de los datos de manera que sea irreconocible e inútil para una persona no autorizada, al descifrarlo está cambiando de nuevo a su forma original.

La mayoría de las técnicas de seguro utilizar un algoritmo matemático y un valor de la variable conocida como "clave".

La clave seleccionada (a menudo de cualquier serie de caracteres aleatorios) se introduce en la encriptación y es parte integrante de la evolución de los datos. Exactamente la misma clave debe ser la entrada para que el descifrado de los datos pueda darse.

2.1.9 Software de Informática Forense

A continuación se presenta una lista con programas de uso forense:

HERRAMIENTAS DE CÓMPUTO FORENSE

Sleuth Kit (Kit forense)

Py-Flag (navegador forense)

Dumpzilla (navegador forense)

Dcfldd (herramientas de imagen de disco)

Netcat (línea de comandos)

NTFS-Tools

Hetman software (Recuperador de datos borrados por los criminales)

Qtparted (particionador)

Regviewer (registro de Windows)

Viewer

X-Ways Win Trace

X-Ways Win Hex

X-Ways Forensics

R-Studio Emergency (recuperador bootable de multimedia)

R-Studio Network Edition

R-Studio RS Agent

Net resident

Faces

Encase

Snort

Helix

Net Flow

Hiren's boot

Canaima 3.1

Mini XP

HERRAMIENTAS PARA EL ANÁLISIS DE DISCOS DUROS

Access Data Forensic Toolkit (FTK)

Guidance Software Encase

Kit Electrónico de Transferencia de datos

Acronis Drive Monitor

HERRAMIENTAS PARA REPARACION DE DISCO DURO

HDD Regenerator

Disk Heal

HERRAMIENTAS DE RECUPERACIÓN DE INFORMACIÓN

Recover my files

Handy Recovery

Easy Drive Data Recovery

Pandora Recovery

HERRAMIENTAS DE SEGURIDAD INFORMÁTICA

Bit Defender Total Security 2015

Panda Internet Security

Outpost Security Suite Pro

AVG Antivirus

HERRAMIENTAS DE CRIPTOGRAFIA

TrueCrypt

Axcrypt

Cryptoforge

Secryptor

Folder Encripter

2.2 Marco Teórico De La Solución

2.2.1 LEY ESPECIAL CONTRA ACTOS DE TERRORISMO

Este manual debe ser utilizado según lo dicta la ley especial contra actos de terrorismo artículo 12 a y b, la cual dice lo siguiente:

Delito informático

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

- a) Utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, información, documentos electrónicos, soportes informáticos, programas o sistemas de información y de comunicaciones o telemáticos, de servicios públicos, sociales, administrativos, de emergencia o de seguridad nacional, de entidades nacionales, internacionales o de otro país;
- b) Creare, distribuyere, comerciare o tuviere en su poder programas capaces de producir los efectos a que se refiere el literal a, de este artículo.

Con esto se pretende que la utilización de este manual sea correcta y únicamente para fines educativos y resolución de problemas en la Universidad tecnológica de El Salvador, cualquier otro uso incorrecto dentro o fuera de la institución puede ser sancionado según lo estipula la ley.

2.2.2 Instalación y uso de los programas

Acronis Drive Monitor

Este programa se encarga específicamente en ayudar a identificar los problemas de discos duros con tiempo suficiente para proteger la computadora y además monitorea el estado del disco duro de servidores, PC y portátiles con la ventaja de advertirle a los usuarios de los problemas que puedan significar un fallo en el Sistema Operativo.

Instalación del programa Acronis Drive Monitor

Lo primero que se debe hacer es descargar el programa desde la página www.acronis.com una vez descargado se empieza la instalación y funcionamiento.

Paso 1:

Selecciona el programa Acronis Drive Monitor, y doble clic en él y aparece la siguiente imagen (Ver figura 1.1).



figura1

Paso 2:

En esta imagen aparecen 3 opciones se selecciona la opción “Install Acronis Drive Monitor” (Ver figura 1.2).

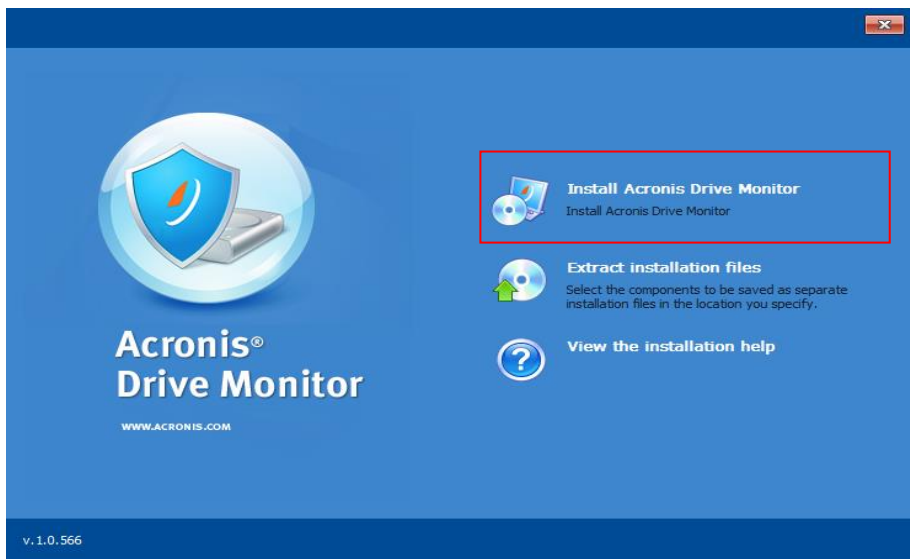


Figura 1.2

Paso 3:

En esta imagen da la bienvenida al programa Acronis Drive Monitor y explica que permite monitorear el disco, y le avisa si se detectan problemas. Luego clic en “siguiente” para continuar (Ver figura 1.3).

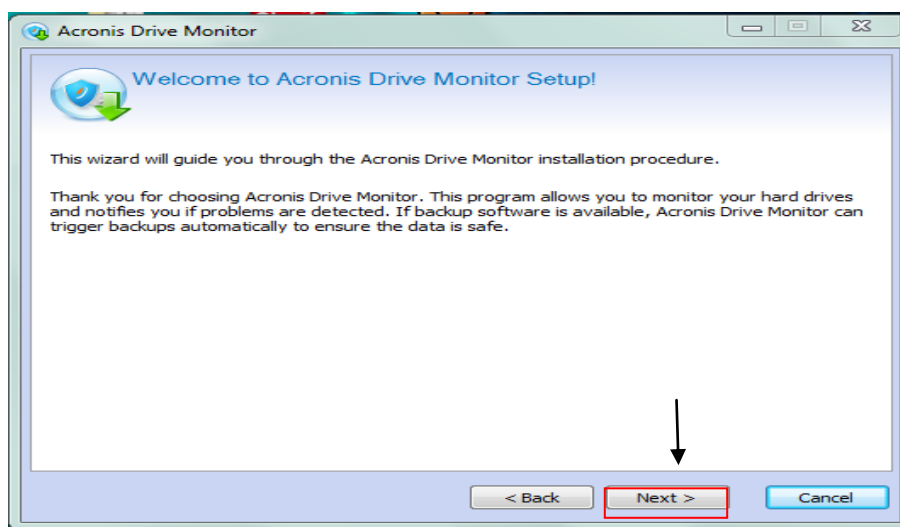


Figura 1.3

Paso 4:

En esta imagen explica los acuerdos de licencia de Acronis Drive Monitor, y se selecciona “I accept the terms of this agreement” y cli en siguiente (Ver figura 1.4).

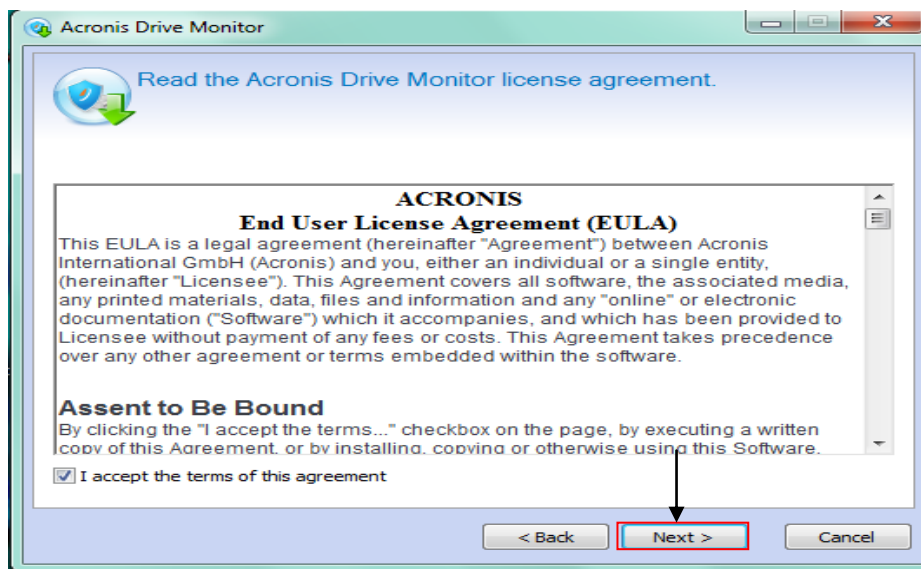


Figura 1.4

Paso 5:

En esta imagen se selecciona la forma en que desea que los componentes que se instalarán estén correctos, y clic en siguiente (Ver figura 1.5).

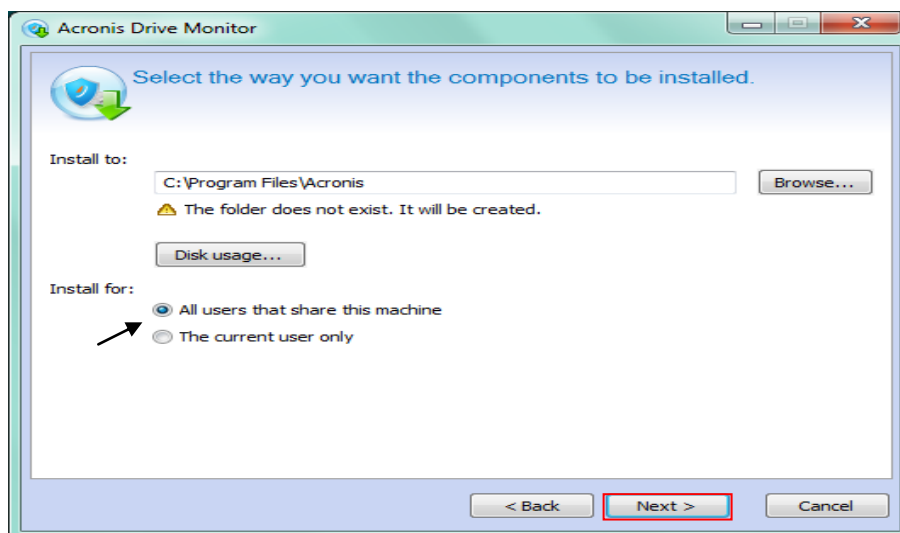


Figura 1.5

Paso 6:

En esta imagen muestra las operaciones que se van a realizar al instalar Acronis Drive Monitor y se hace clic en “Install” (Ver figura 1.6).

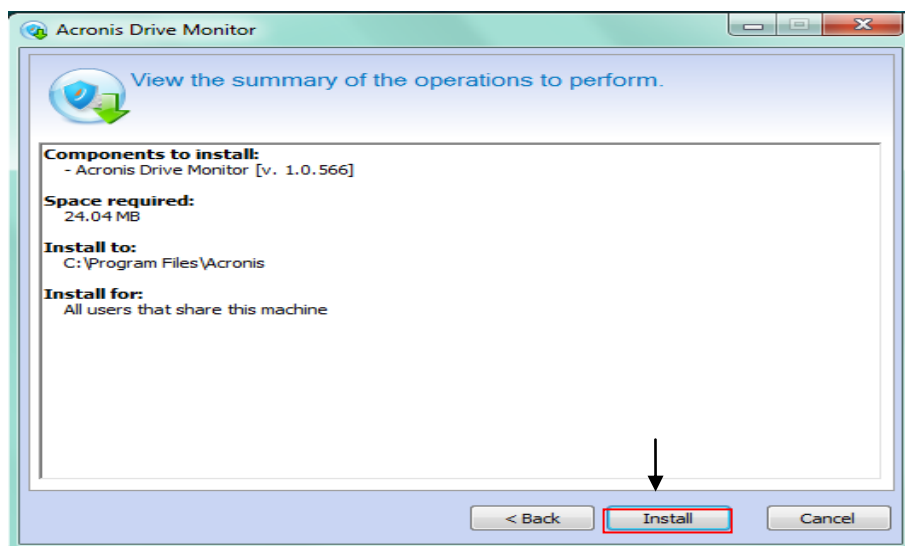


Figura 1.6

Paso 7:

En esta imagen es el proceso de instalación de Acronis Drive Monitor en la cual se tiene que esperar (Ver figura 1.7).

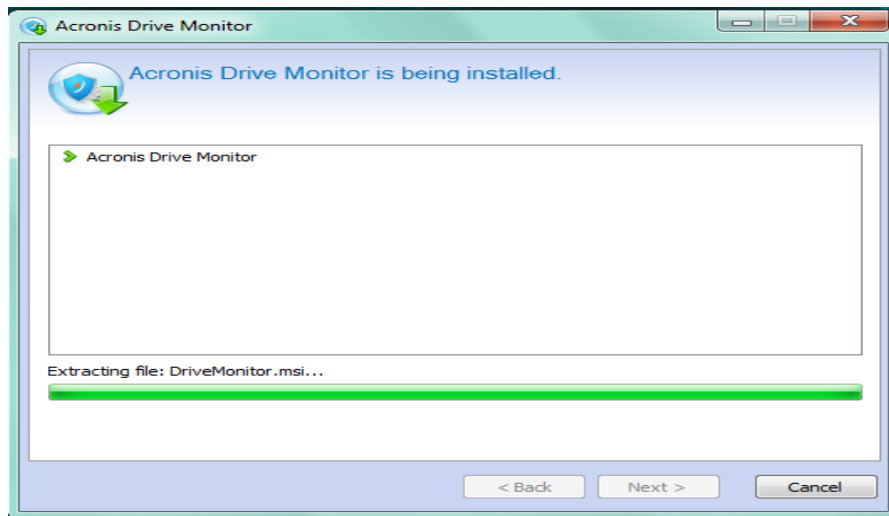


Figura 1.7

Paso 8:

En esta imagen muestra la finalización de la instalación de Acronis Drive Monitor, una vez terminado esto, muestra un acceso directo del programa (Ver figura 1.8).

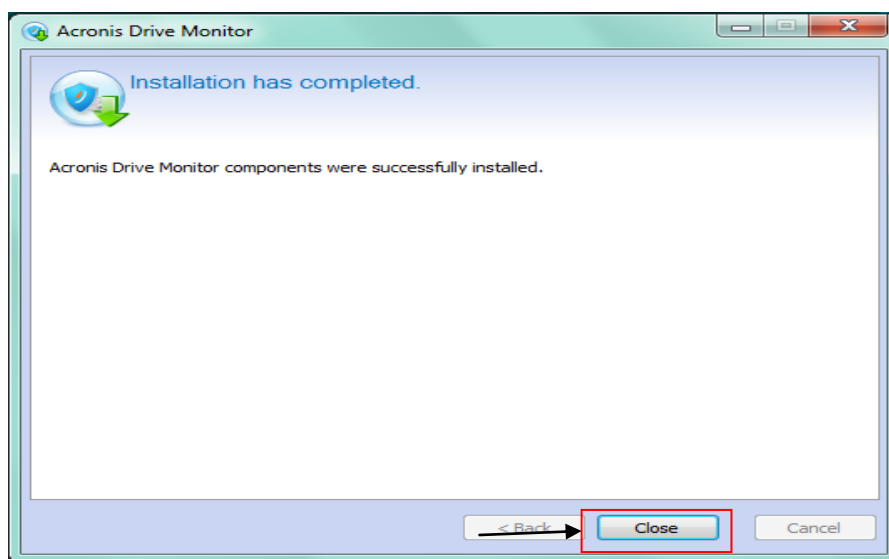


Figura 1.8

Paso 9:

En esta imagen muestra la pantalla de inicio de Acronis Drive Monitor, en la cual aparecen 3 opciones que se van a explicar más adelante (Ver figura 1.9).

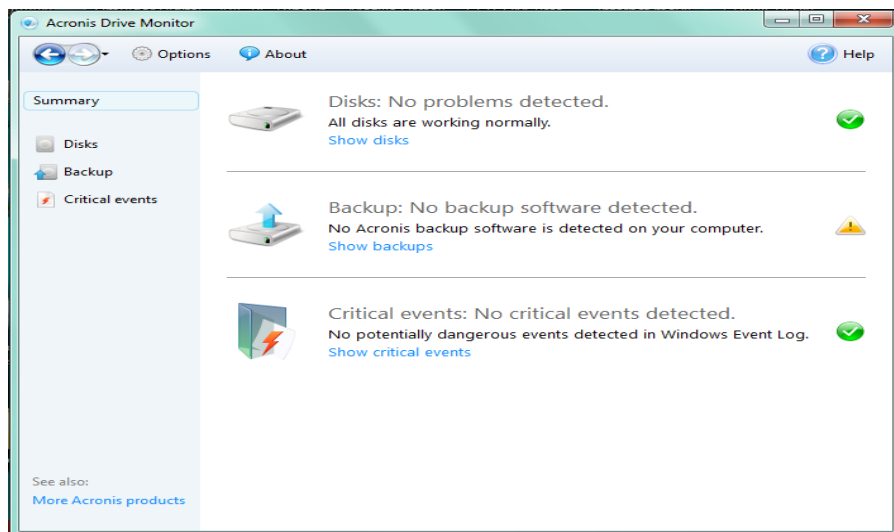


Figura 1.9

Paso 10:

En esta imagen se selecciona “Disk: No problems detected” para ver el contenido de esta opción (Ver figura 1.10).

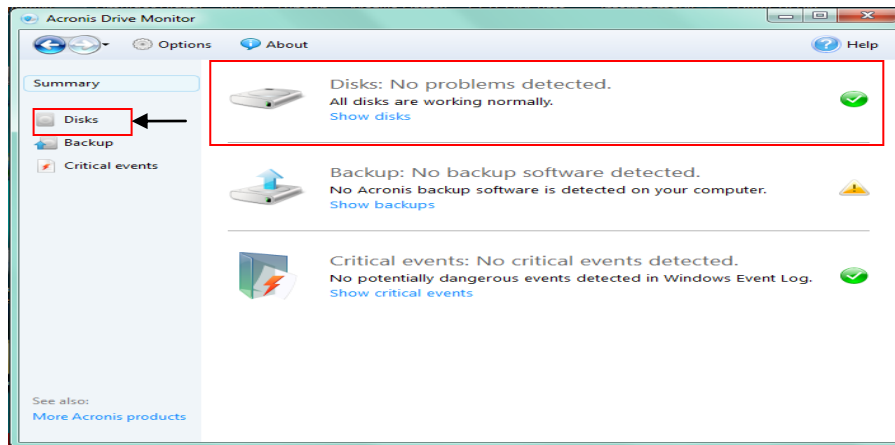


Figura 1.10

Paso 11:

Al seleccionar “disk” dice que el disco se controla a través de la interfaz de SMART, y muestra 3 pestañas con su contenido; la primera es “Disk over view” hace referencia a 4 pasos que son: monitoreo, tiempo de encendido, disco funcionando y la temperatura (Ver figura 1.11).

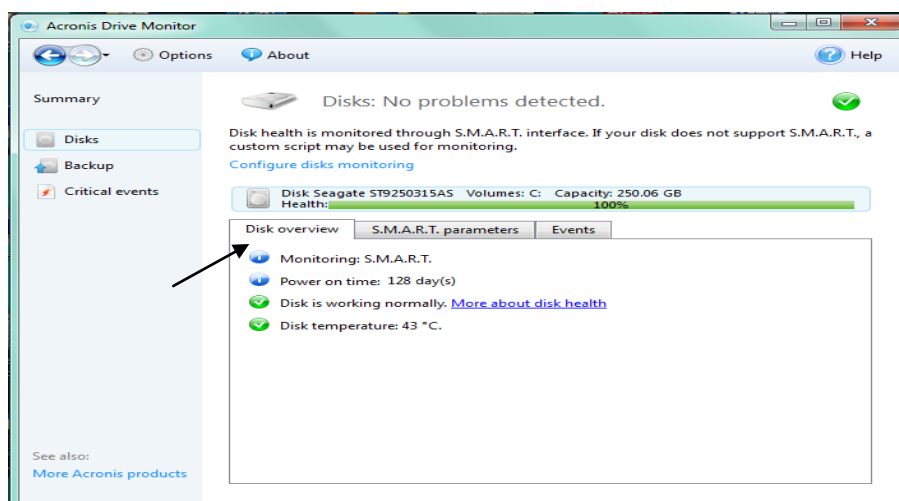


Figura 1.11

Paso: 12 y 13

La segunda es “S.M.A.R.T parámetros” esta contiene todos los parámetros como nombres, valor, estado, etc. Y la tercera que es “Eventos” esta es muy sencilla solo muestra los eventos que se han hecho (Ver figura 1.12 y 1.13).

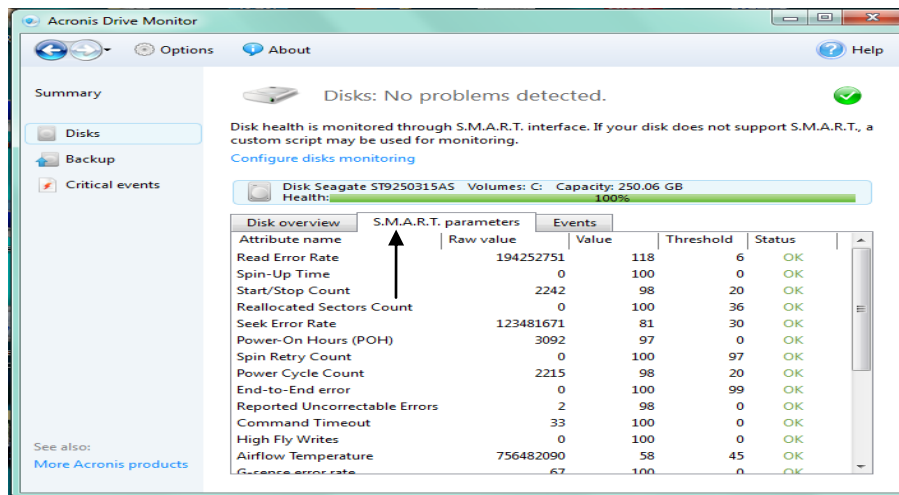


Figura 1.12

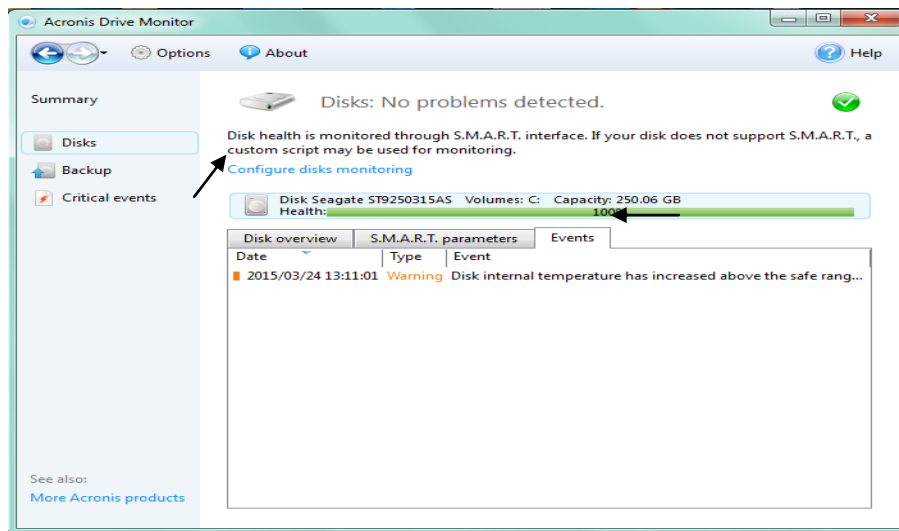


Figura 1.13

Paso: 14

Pero también al seleccionar “Configure disks monitoring” abre un cuadro con diferentes opciones al lado izquierdo (Ver figura 1.14).

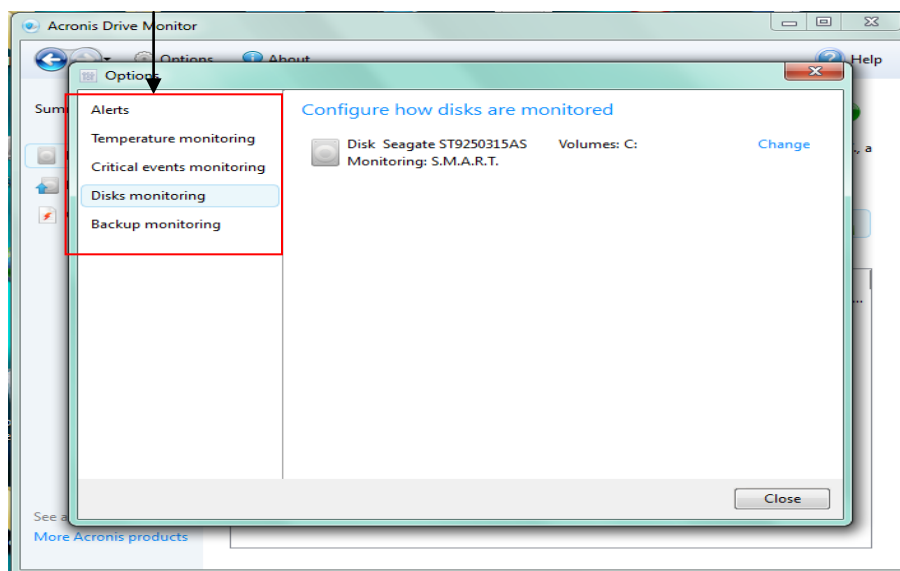


Figura 1.14

Paso: 15

En esta imagen se selecciona “Alerts” y mostrará como configurar las opciones de notificación, además explica que la notificación de e-mail no está configurado, también muestra un mensaje como advertencia (Ver figura 1.15).

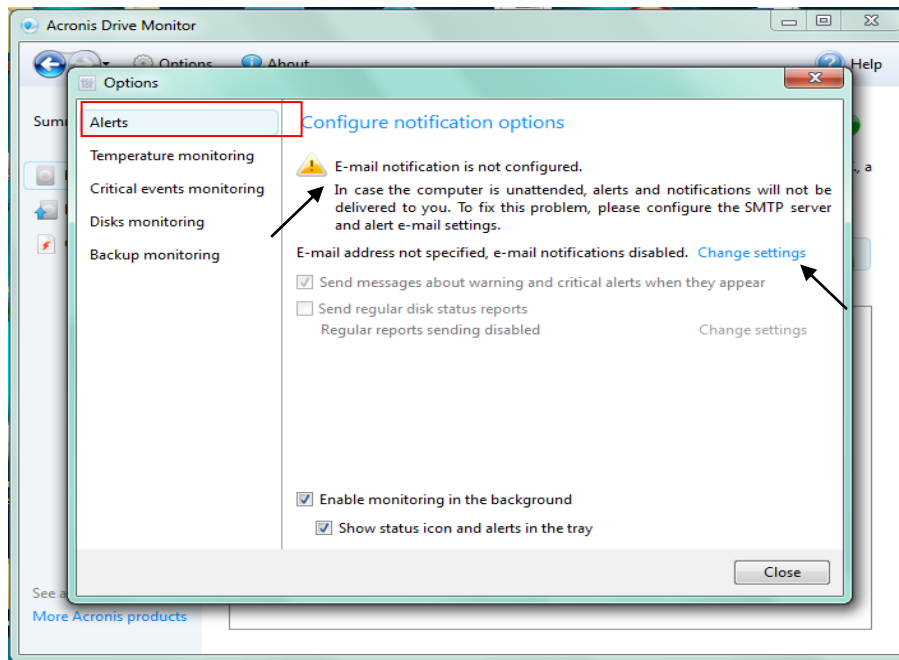


Figura 1.15

Paso: 16

En esta misma imagen aparece la opción de “Change settings” se selecciona y se abrirá la siguiente imagen que va mostrar los parámetros de configuración de E-mail (Ver figura 1.16).

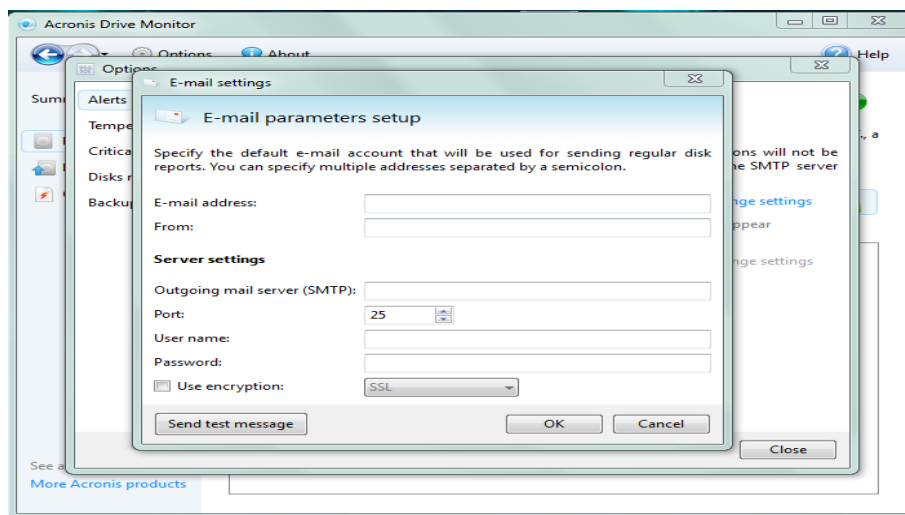


Figura 1.16

Paso: 17

En esta imagen se va a seleccionar “Temperature monitoring” la que muestra la unidad de temperatura y la temperatura normal y la crítica del disco (Ver figura 1.17).

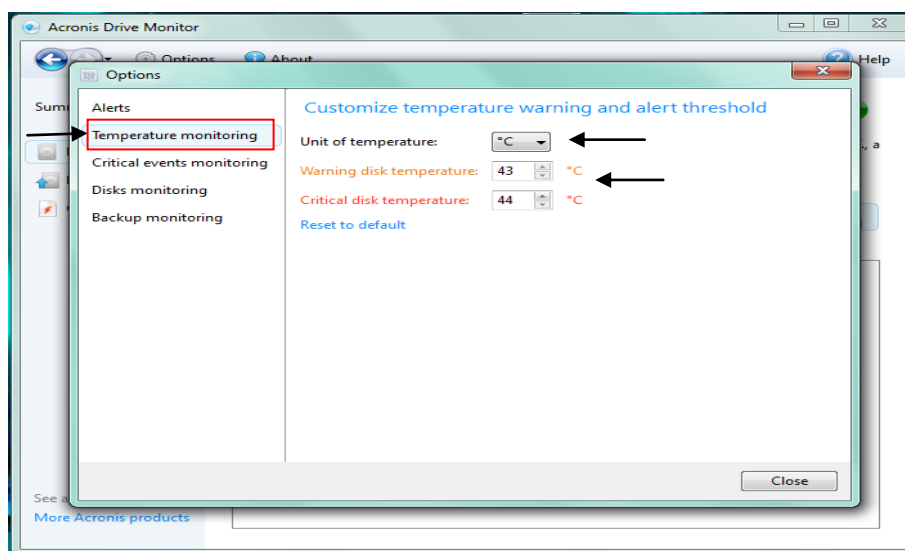


Figura 1.17

Paso: 18

En esta imagen se selecciona “Critical events monitoring” la cual se encarga de configurar Windows y de monitorización de registros de sucesos, también aparece la opción de “Reset to original settings” esto permite restaurar los valores originales (Ver figura 1.18).

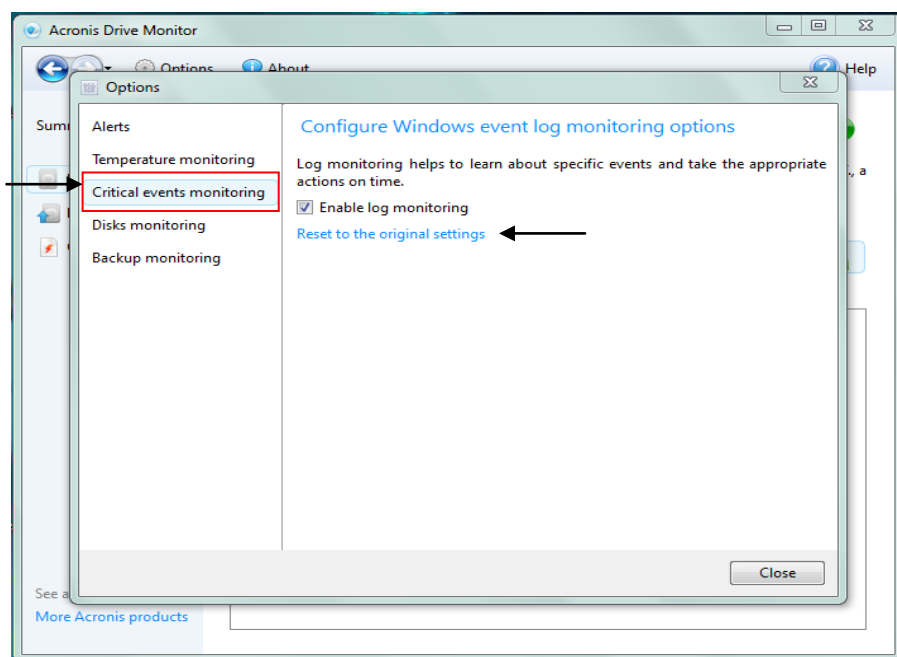


Figura 1.18

Paso: 19

En esta imagen se selecciona “Disks monitoring” esta se encarga de la supervisión y del control de discos (Ver figura 1.19)

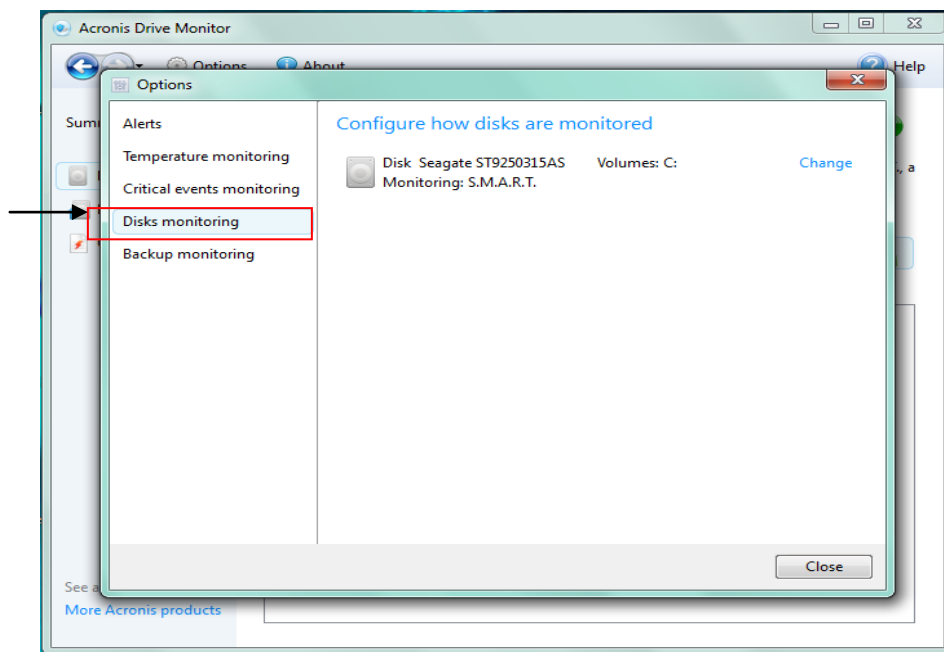


Figura 1.19

Paso: 20

También trae la opción de “Cambio” esta permite supervisar el uso de SMART, y también incluye “Monitor using custom script” esta opción se puede utilizar para supervisar las unidades de disco duro que no soportan SMART (Ver figura 1.20).

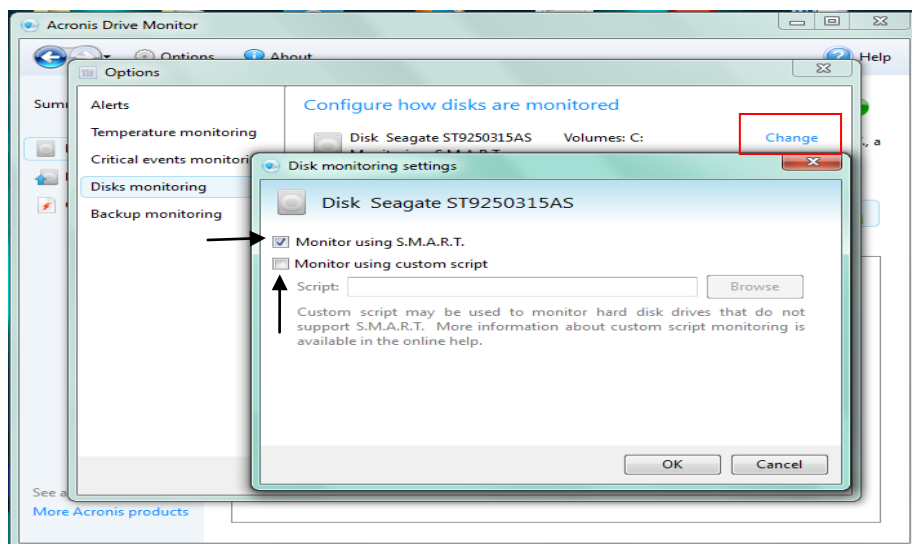


Figura 1.20

Paso: 21

En esta imagen se selecciona “Backup monitoring” esta permite configurar cómo se controlan las copias de seguridad (Ver figura 1.21).

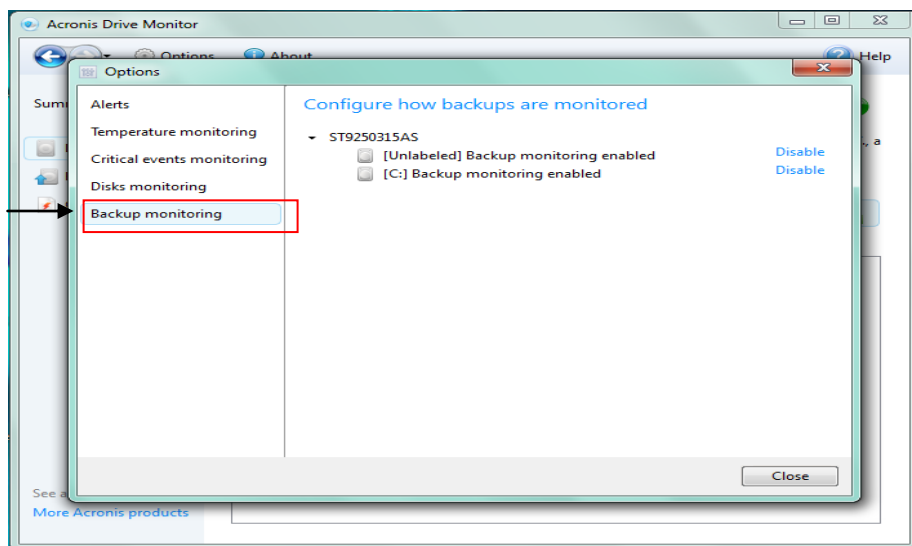


Figura 1.21

Paso: 22

En esta imagen se selecciona la segunda pestaña que es “Backup” ahí explica que no hay ningún software detectado en el programa (Ver figura 1.22).

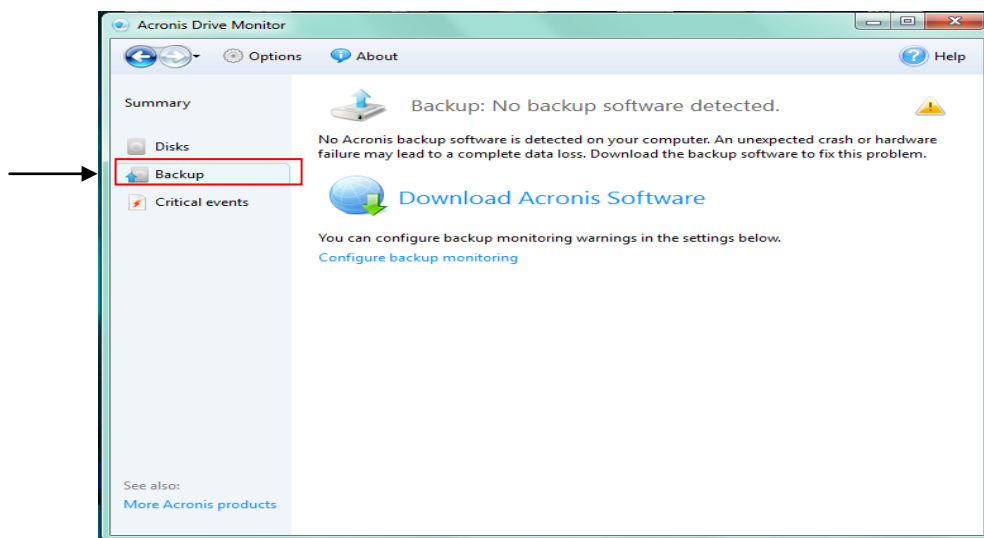


Figura 1.22

Paso: 23

En esta imagen se selecciona “Critical events” en esta pestaña se observa que no hay eventos que pueden indicar un mayor riesgo de los datos que se han detectado en Windows (Ver figura 1.23).

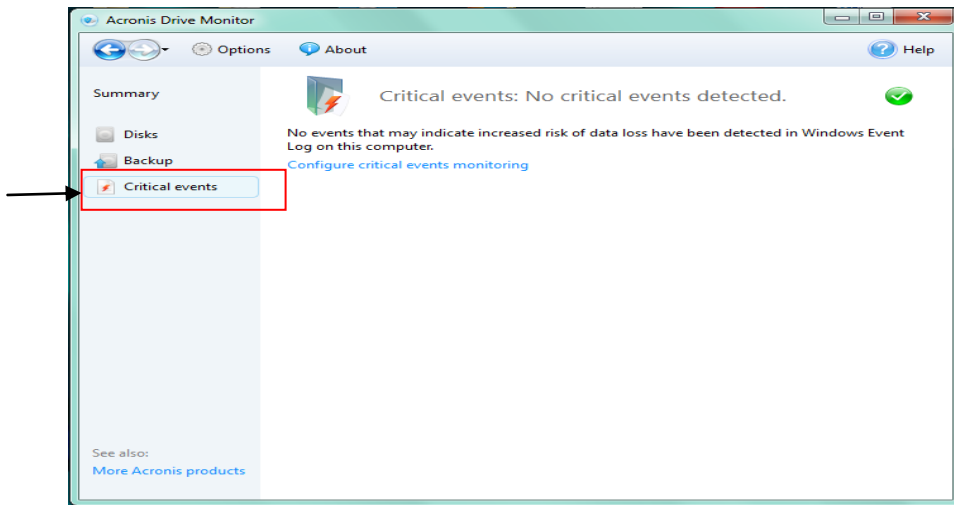


Figura 1.23

Paso: 24

En esta imagen se explica las opciones como por ejemplo: clic en “Opciones” aquí aparecerán las imágenes que se han explicado anteriormente, y al hacer en clic “About” explica todo lo referente del programa Acronis Drive Monitor, y por ultimo “Help” aquí muestra una página de resumen completo de todo Acronis Drive Monitor (Ver figura 1.24)

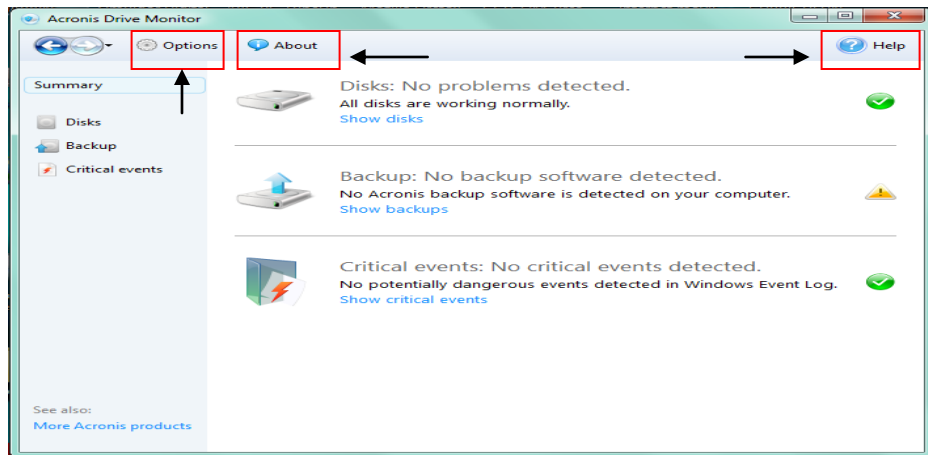


Figura 1.24

HHD Regenerador Full

Este programa se encarga de explorar y reparar sectores defectuosos que pueda tener el disco duro ya que con el paso de tiempo algunos discos duros tienen a magnetizarse o dañarse, lo que provoca que la computadora ande un tanto mal y con problemas.

Instalación del programa HHD Regenerator Full

Lo que se hace es descargar el programa HHD Regenerator Full desde la página <http://www.dposoft.net/hdd.html>, una vez descargado se empieza la instalación y su funcionamiento.

Paso: 1

Seleccionan el programa HHD Regenerator Full, y doble clic en él y aparecerá un cuadro que muestra la bienvenida de la instalación del programa y se selecciona “Next” para continuar (Ver figura 2.1).

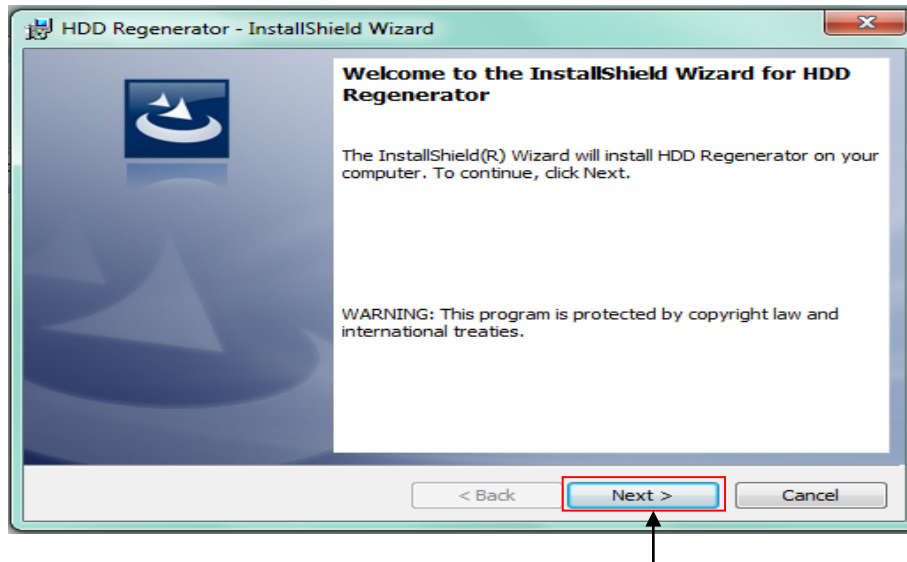


Figura 2.1

Paso: 2

En esta imagen explica los acuerdos de la licencia del programa ya que esto es muy importante en su instalación, se hace clic en “Aceptó los acuerdos de la licencia” y clic en “Next” para continuar (Ver figura 2.2).

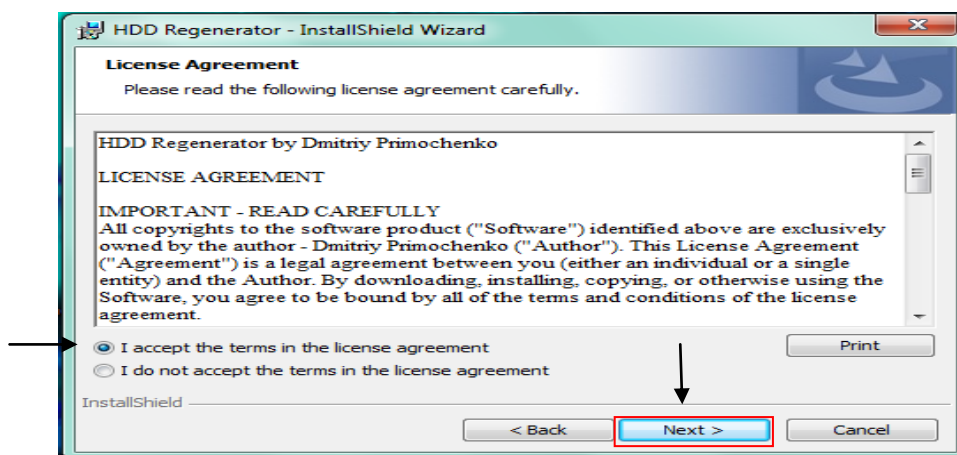


Figura 2.2

Paso: 3

En esta imagen muestra el proceso de instalación de HDD Regenerator Full en la cual tenemos que esperar unos minutos para finalizar su instalación (Ver figura 2.3).

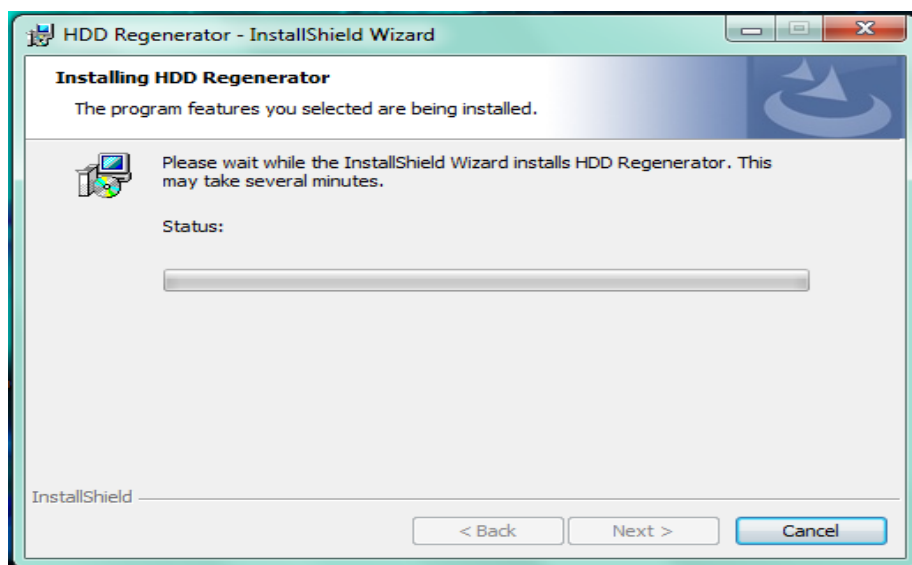


Figura 2.3

Paso: 4

En esta imagen ha finalizado la instalación del programa HDD Regenerator Full, y se hace clic en finalizar (Ver figura 2.4).

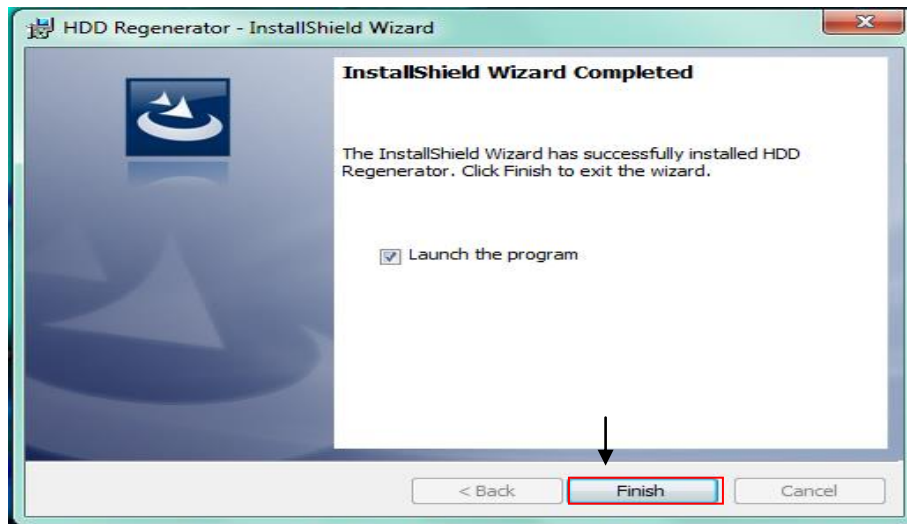


Figura 2.4

Pasos de activación del programa HDD Regenerator

Paso: 5

Una vez instalado el programa HDD Regenerator, hacer clic en el botón “Inicio” y buscar el programa (Ver figura 2.5).

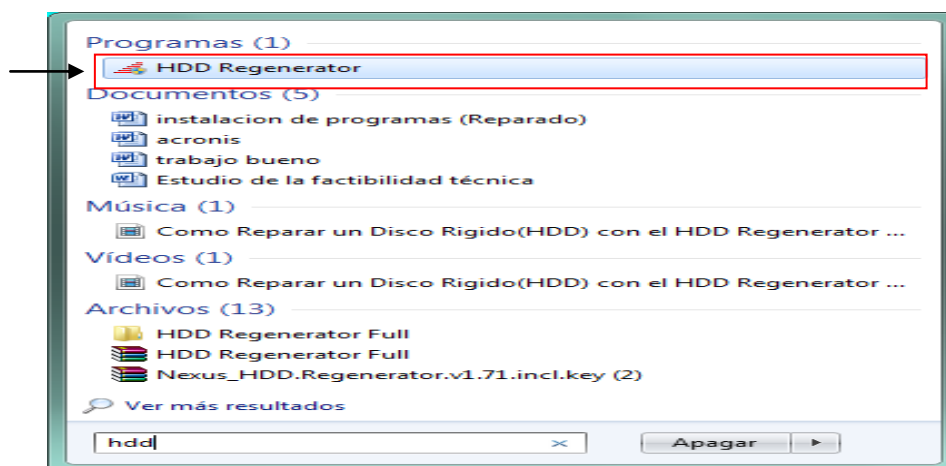


Figura 2.5

Paso: 6

Se selecciona el programa y clic derecho sobre él, y luego clic en propiedades para continuar (Ver figura 2.6).

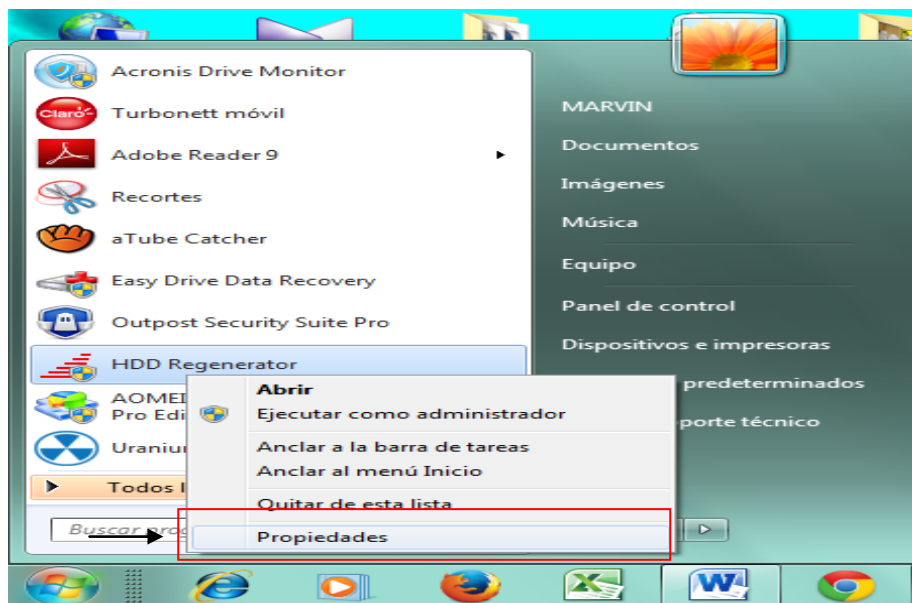


Figura 2.6

Paso: 7

Una vez seleccionado la opción “Propiedades” dar clic en la opción “Abrir ubicación” para continuar (Ver figura 2.7).

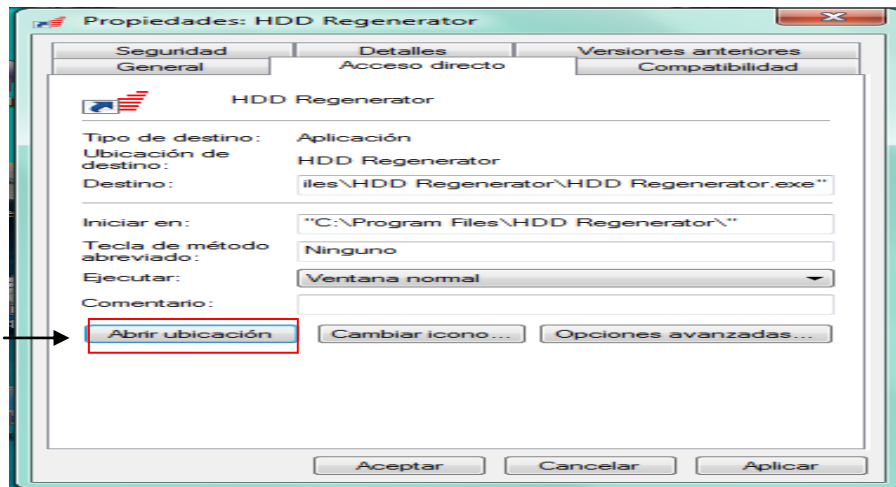


Figura 2.7

Paso: 8

Al abrir la ubicación, mostrara la siguiente carpeta con los siguientes archivos (Ver figura 2.8).

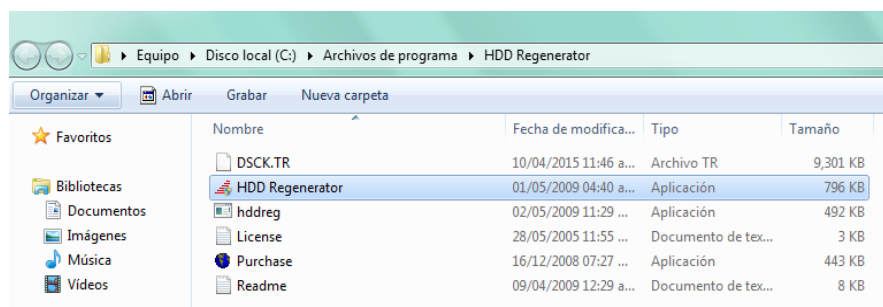


Figura 2.8

Paso: 9

Se minimiza esta carpeta, y se abre la carpeta que tiene como nombre “Activador” (Ver figura 2.9)

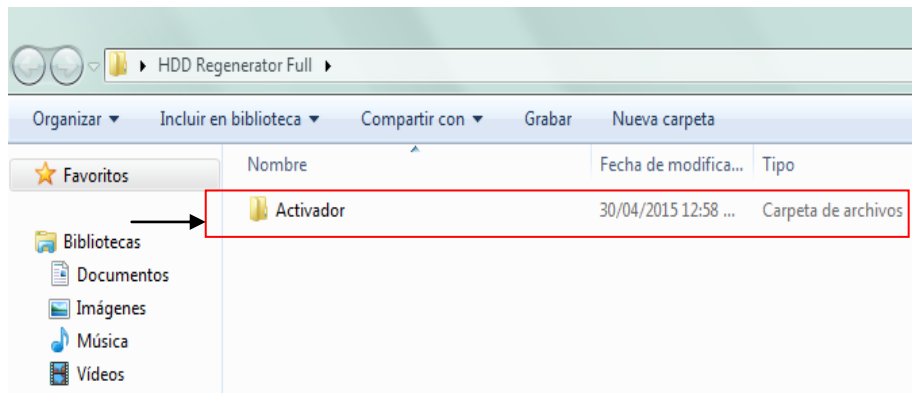


Figura 2.9

Paso: 10

Copiar todos los archivos que están en la carpeta “Activador” y se tienen que pegar en la carpeta en la ubicación del programa HDD Regenerator (Ver figura 2.10).

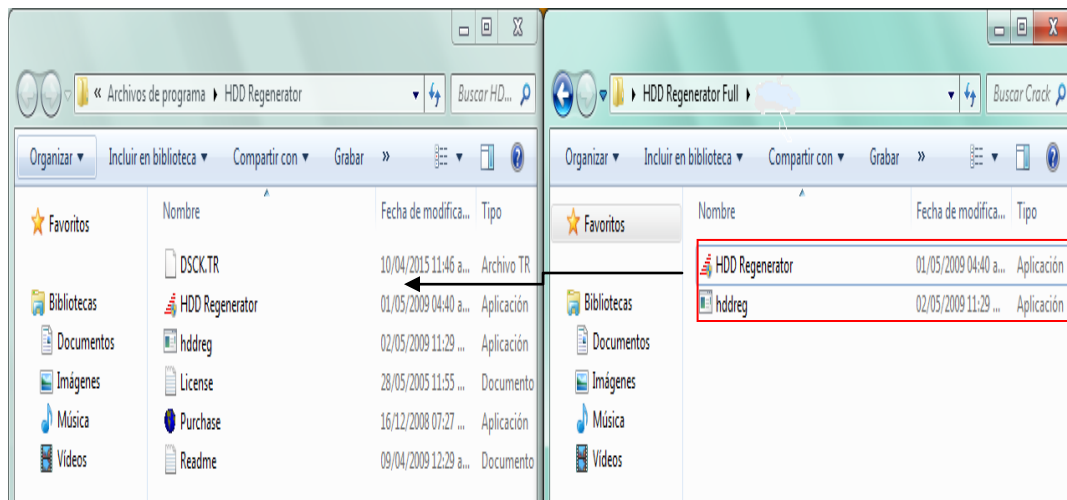


Figura 2.10

Paso: 11

Al copiar los archivos aparecen las siguientes advertencias en la cual se selecciona “Mover y reemplazar”, después el sistema pide permisos especiales en la cual se hace clic en “Continuar” (Ver figura 2.11).

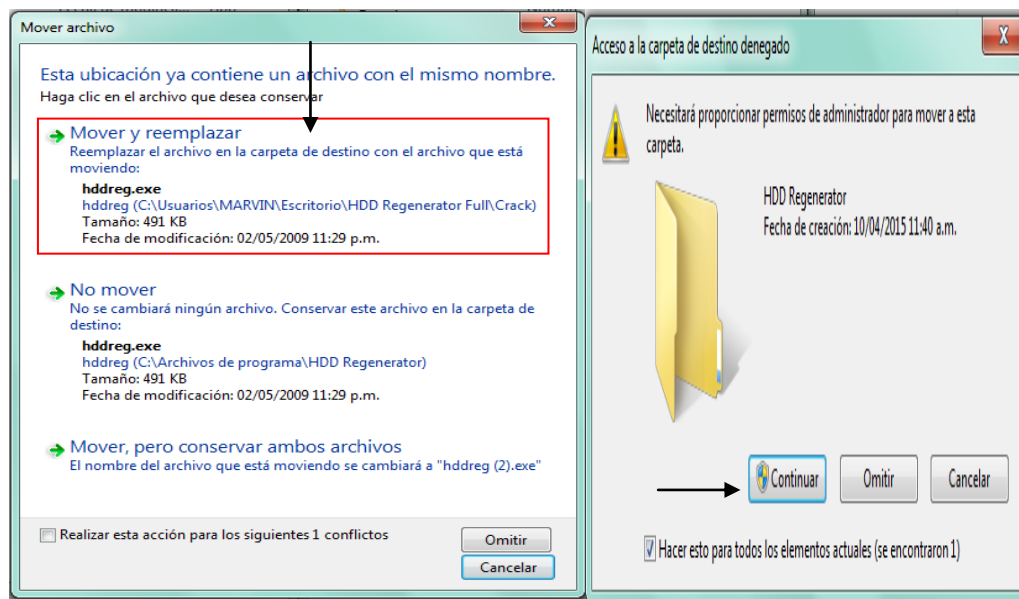


Figura 2.11

Paso: 12

Una vez copiados todos los archivos, volver a abrir el programa y se observara que está registrado (Ver figura 2.12).

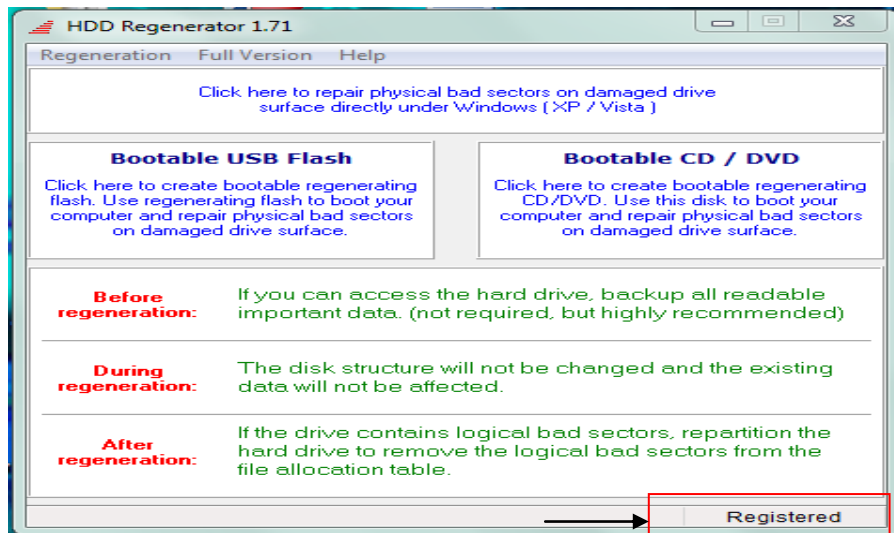


Figura 2.12

Pasos del funcionamiento de HDD Regenerator.

Paso 13: En esta imagen muestra la pantalla de inicio de HDD Regenerator, en la cual contiene dos opciones: la primera es de copiar el programa en una memoria USB y la segunda es de quemarlo en un CD o DVD, (Ver figura 2.13).

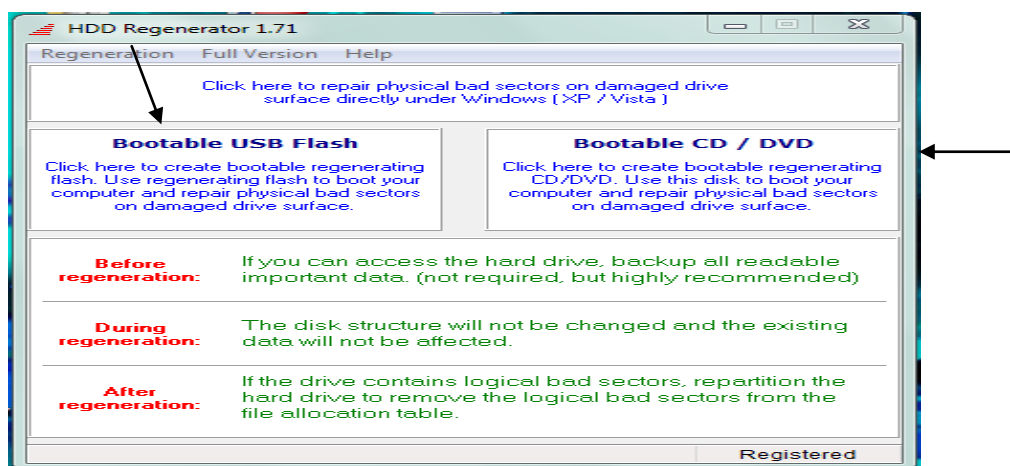


Figura 2.13

Paso: 14

Una vez seleccionada una de las dos opciones, en este caso se seleccionó “Bootable CD / DVD” mostrara esta imagen en la cual ha selecciona el dispositivo con el que se grabara el DVD y se hace clic en “OK” para continuar (Ver figura 2.14)

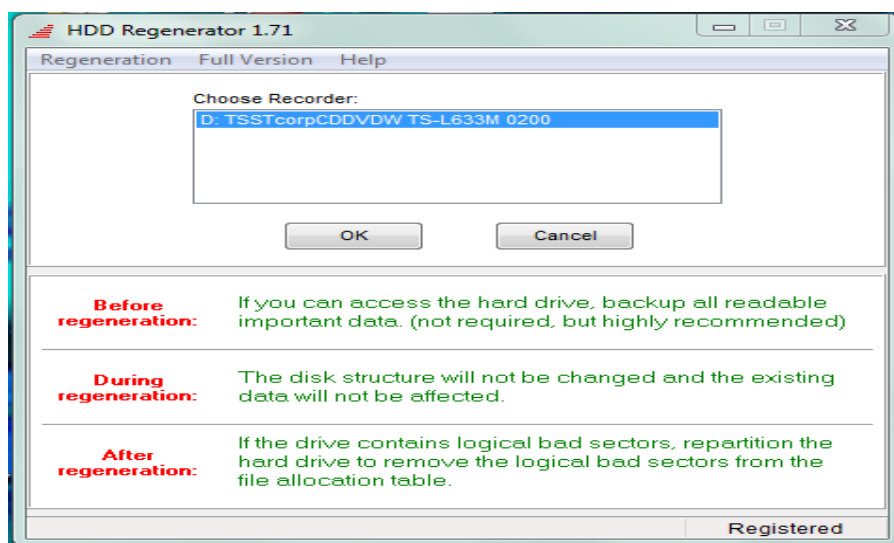


Figura 2.14

Paso: 15

En esta imagen se selecciona la velocidad de grabación de disco y en la cual se deja por lógica la opción “MAX” y se hace clic en “Burn CD” para continuar con el proceso (Ver figura 2.15).

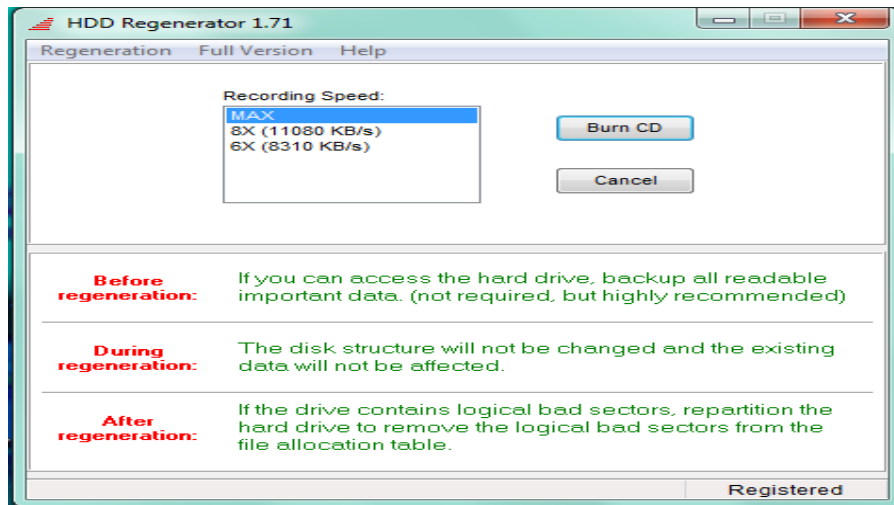


Figura 2.15

Paso: 16

En esta imagen está iniciando el proceso de copiado de archivos al DVD (Ver figura 2.16).

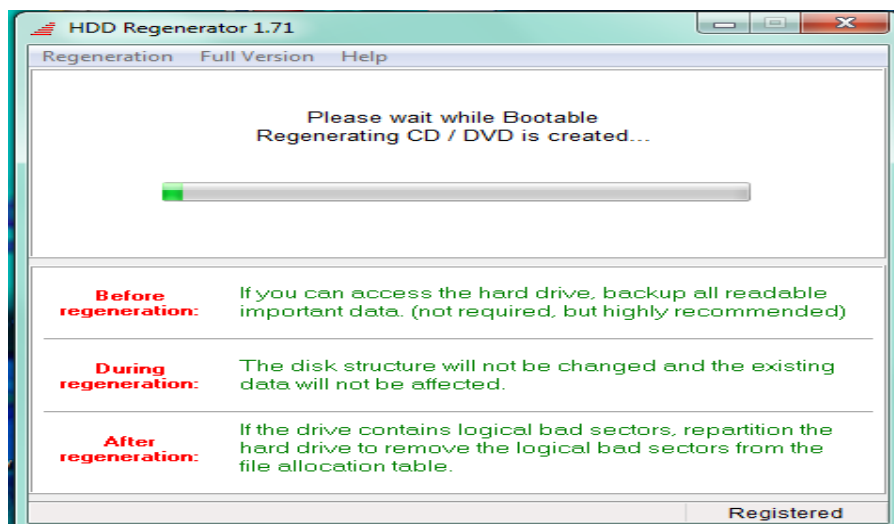


Figura 2.16

Paso: 17

En esta imagen muestra un mensaje donde explica que esta listo el DVD con los archivos copiados y pregunta que si se desea reiniciar el equipo y se hace clic en “Yes” para continuar (Ver figura 2.17).

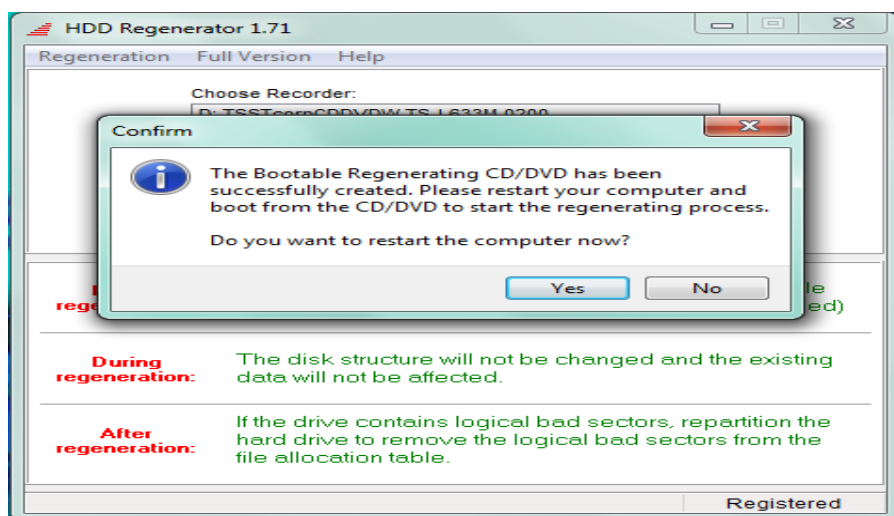


Figura 2.17

Paso: 18

Se procede apagar la computadora procurando dejar el DVD dentro del lector, y después encender la computadora y seleccionar la tecla que corresponde al menú booteo y luego aparecerá un menú donde se selecciona “Optical Disk Drive” para dar inicio a la revisión del disco (Ver figura 2.18).



Figura 2.18

Paso: 19

Ahí se espera que cargue el menú del programa HDD Regenerator, en el cual muestra los discos duros disponibles y se selecciona el disco que se quiera analizar (Ver figura 2.19).

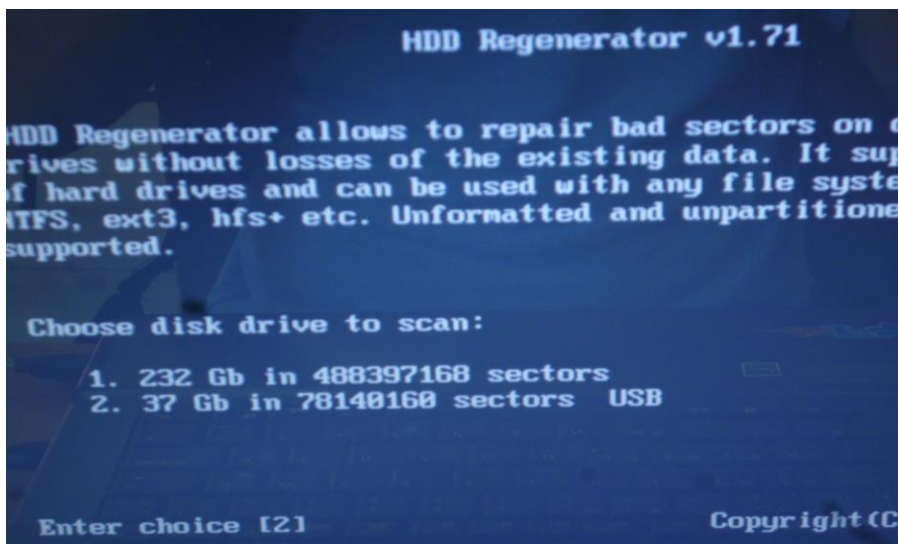


Figura 2.19

Paso: 20

En esta imagen muestra las 3 opciones del programa HDD Regenerator las cuales son la primera se encarga de escanear, la segunda se encarga de escanear pero no repara y la tercera es solo para que el usuario escoja el rango de donde hasta donde quiera reparar el disco duro, en este caso se selecciona la primera opción (Ver figura 2.20)

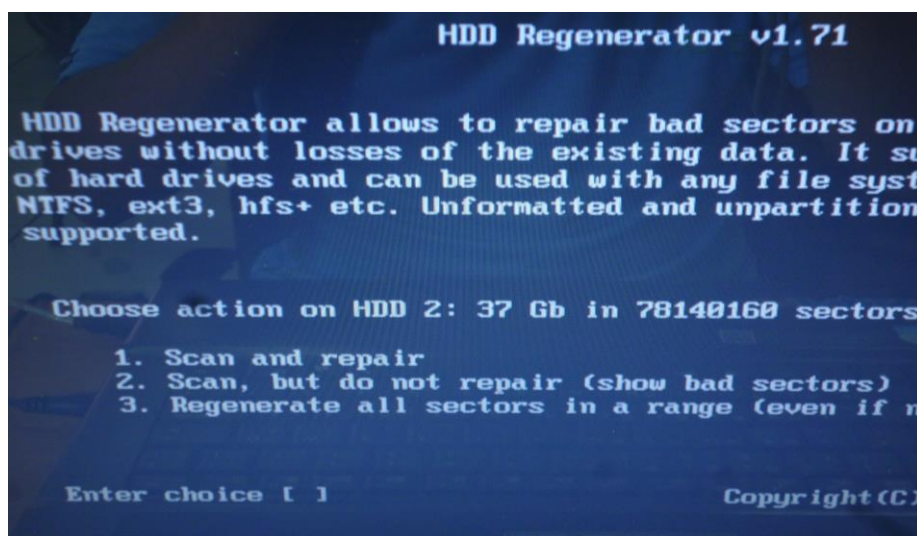


Figura 2.20

Paso: 21

En la siguiente imagen muestra los detalles del disco que se va a reparar y se hace clic en “Enter” para iniciar la reparación del disco duro (Ver figura 2.21)

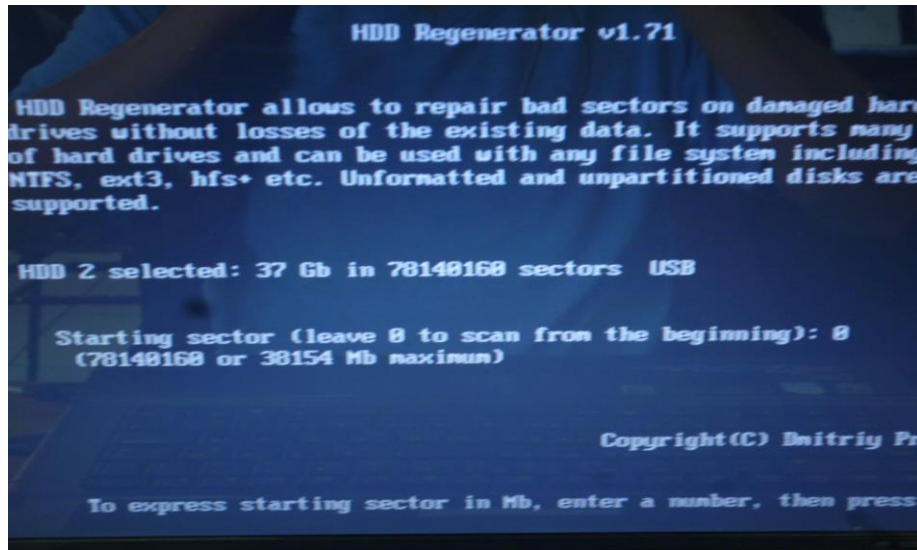


Figura 2.21

Paso 22: En esta imagen inicia el proceso de reparación y análisis y se debe esperar que termine el proceso en cual tendrá una duración dependiendo el tamaño del disco (Ver figura 22).

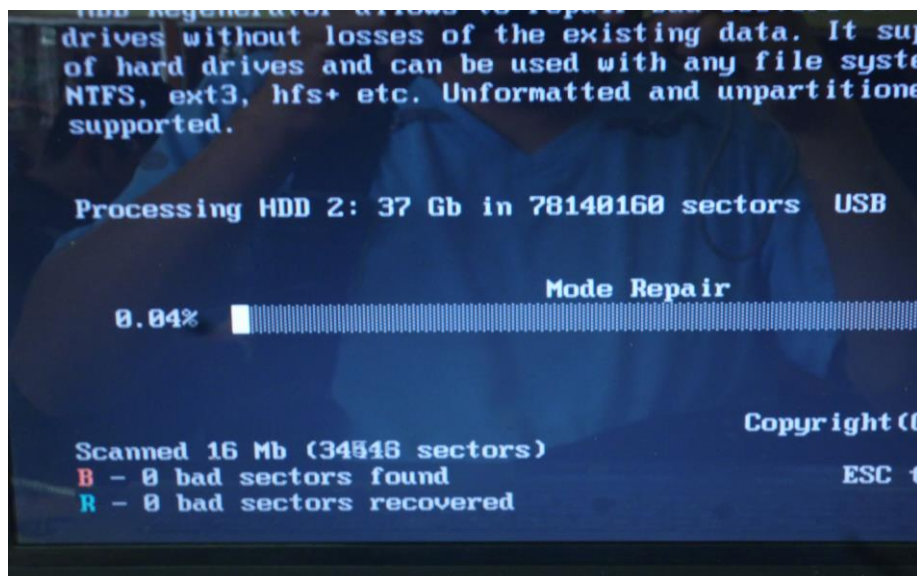


Figura 2.22

Easy Driver Data Recovery

Este programa se encarga de la recuperación de datos borrados, dañados o formateados y además permiten recuperar archivos que no están presentes en las entradas del sistema de archivos. Es posible recuperar fotos, imágenes, música, juegos y toda la información que estimas valiosa. Para recuperar archivos borrados de USB, Easy Drive Data Recovery funciona tanto con almacenamiento externo como interno y admite todo tipo de unidades Flash y USB.

Instalación del programa Easy Driver Recovery

Lo que se debe hacer es descargar el programa Easy Driver Recovery desde la página <http://www.munsoft.es/EasyDriveDataRecovery/>, una vez descargado se empieza la instalación y su funcionamiento.

Paso 1

Se selecciona el programa Easy Driver Recovery, y doble clic en él y aparecerá un cuadro que muestra la licencia del programa y se selecciona “Acepto” para continuar (Ver figura 3.1)



Figura 3.1

Paso: 2

En esta imagen hay que elegir el lugar de instalación de Easy Drive Recovery, una vez hecho esto, se hace clic en “Instalar” para empezar la instalación (Ver figura 3.2).

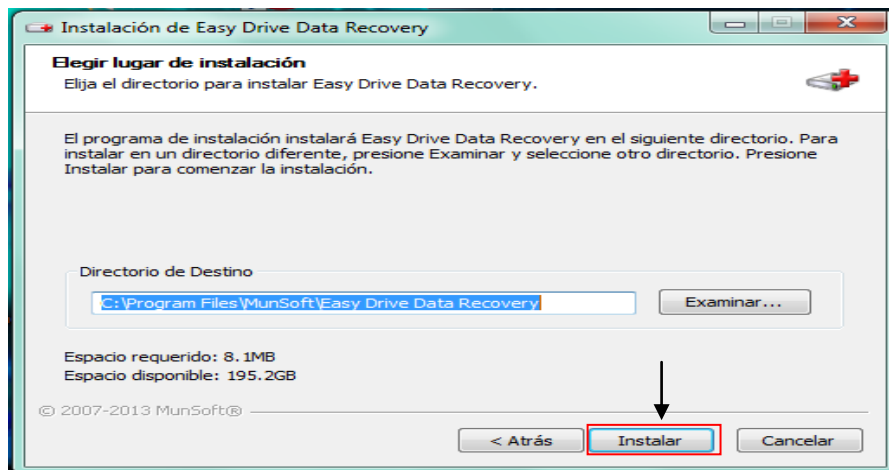


Figura 3.2

Paso: 3

En esta imagen ha completado la instalación del programa el cual ya está listo para funcionar (Ver figura 3.3)

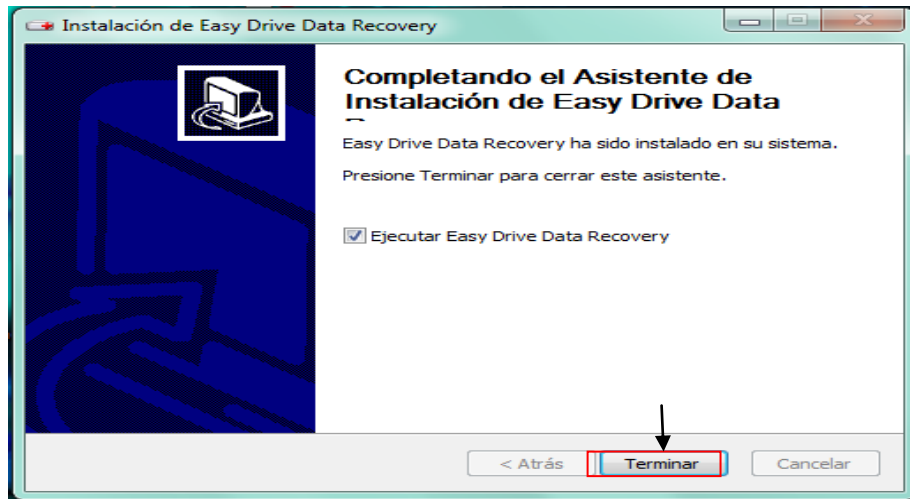


Figura 3.3

Cuando se ha terminado la instalación se empieza con los pasos para la activación del programa Easy Driver Data Recovery.

Pasos para la activación el programa Easy Drive Data Recovery.

Paso: 4

Una vez instalado el programa Easy Driver Data Recovery, hacer clic en el botón "Inicio" y buscar el programa (Ver figura 3.4).

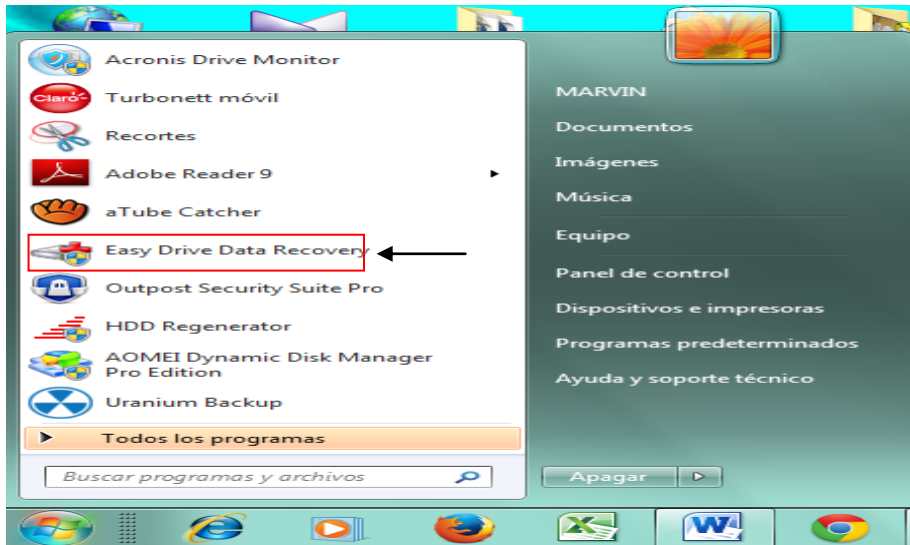


Figura 3.4

Paso: 5

Se selecciona el programa y clic derecho sobre él, y luego clic en propiedades para continuar (Ver figura 3.5).

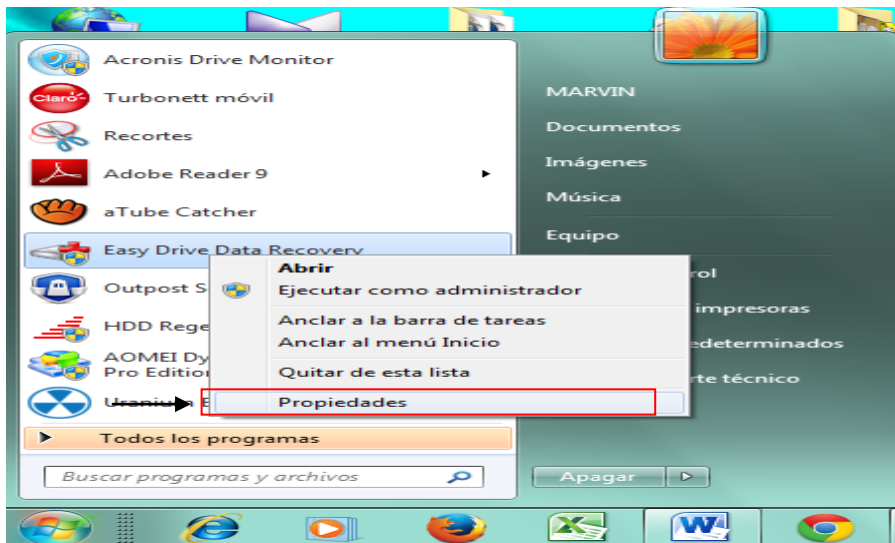


Figura 3.5

Paso: 6

Una vez seleccionada la opción “Propiedades” dar clic en la opción “Abrir ubicación” para continuar (Ver figura 3.6).

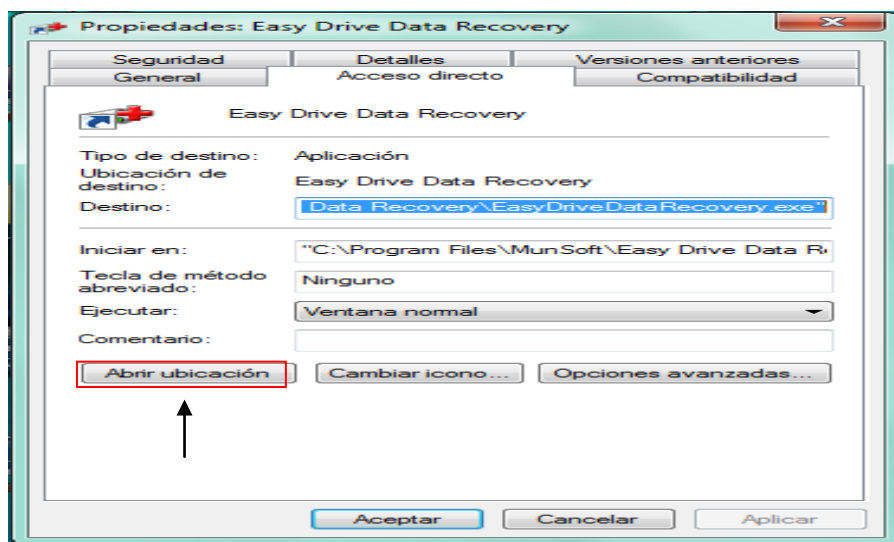


Figura 3.6

Paso: 7

Al abrir la ubicación, mostrara la siguiente carpeta con los siguientes archivos (Ver figura 3.7).

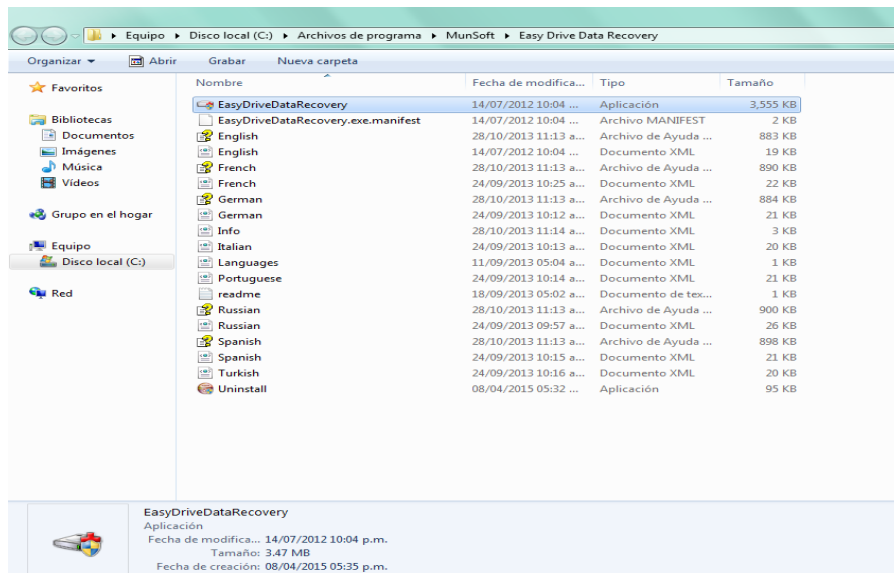


Figura 3.7

Paso 8:

Se minimiza esta carpeta, y se abre la carpeta que tiene como nombre “Activador” (Ver figura 3.8).

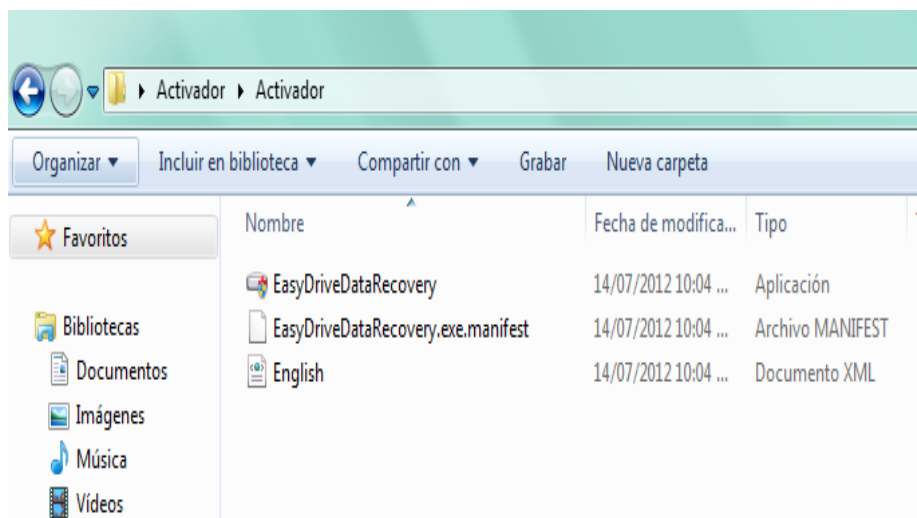


Figura 3.8

Paso: 9

Copiar todos los archivos que están en la carpeta “Activador” y se tienen que pegar en la carpeta en la ubicación del programa Easy Drive Data Recovery (Ver figura 3.9).

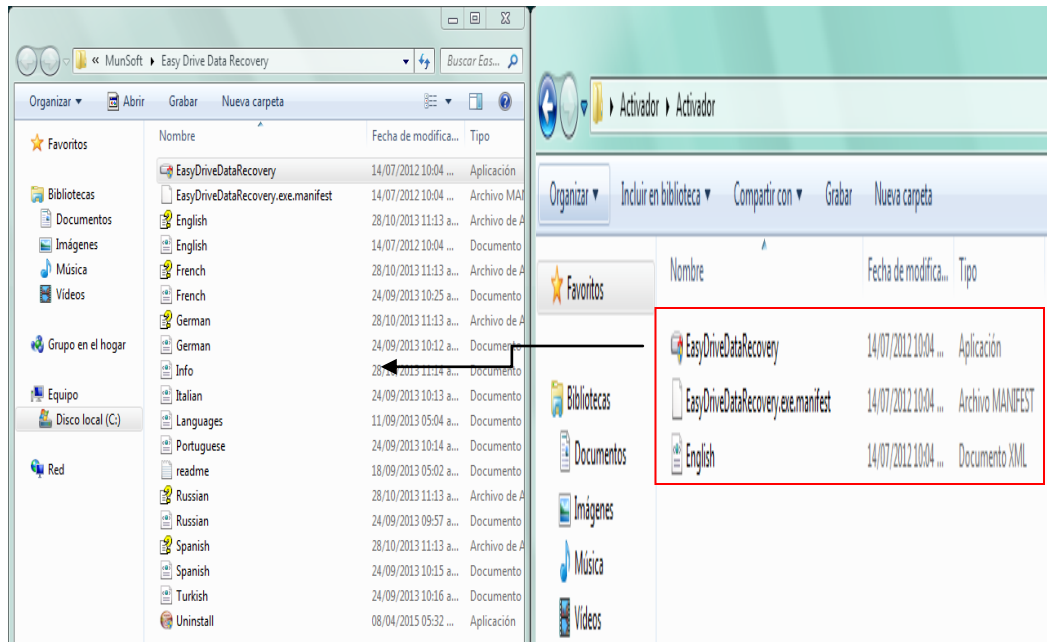


Figura 3.9

Paso: 10

Al copiar los archivos aparecen las siguientes advertencias en la cual se selecciona “Mover y reemplazar”, después el sistema pide permisos especiales en la cual se hace clic en “Continuar” (Ver figura 3.10).

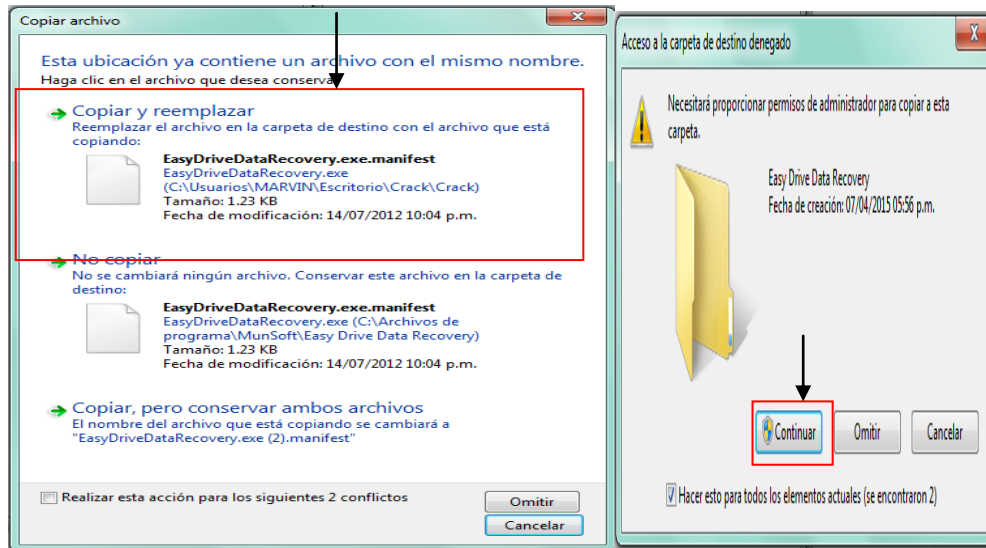


Figura 3.10

Paso: 11

Una vez copiados todos los archivos, volver a abrir el programa y se observara que está registrado (Ver figura 3.11).



Figura 3.11

Pasos del funcionamiento del programa Easy Drive Data Recovery.

Paso: 12

En esta imagen muestra la pantalla de inicio del programa, y muestra un cuadro donde se tiene que seleccionar el disco en el que se desea recuperar los archivos (Ver figura 3.12).

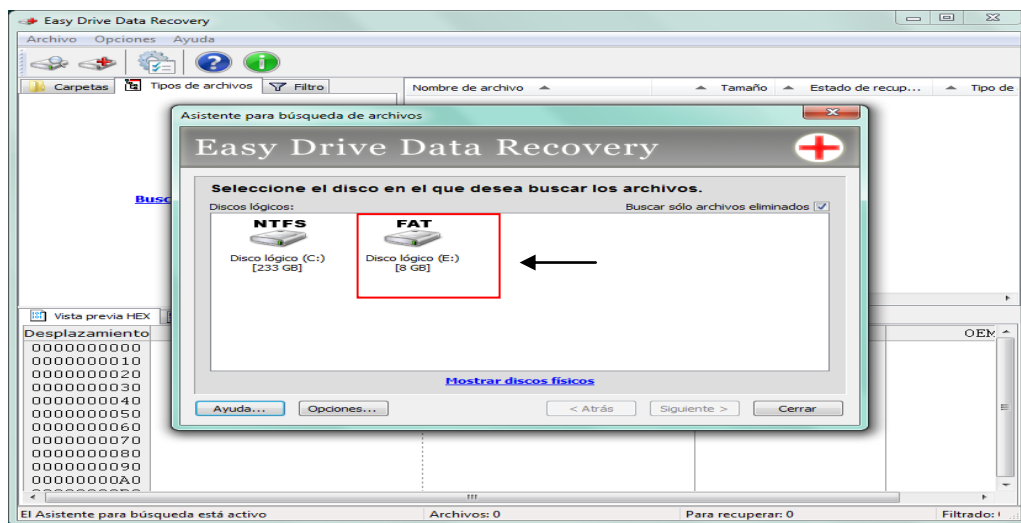


Figura 3.12

Paso: 13

Después de seleccionar el disco se hace clic en “siguiete” y empezara a explorar el disco para recuperar los archivos eliminados una vez terminado esto se selecciona la pestaña “carpeta” y aparecerán todos los archivos (Ver figura 3.13).

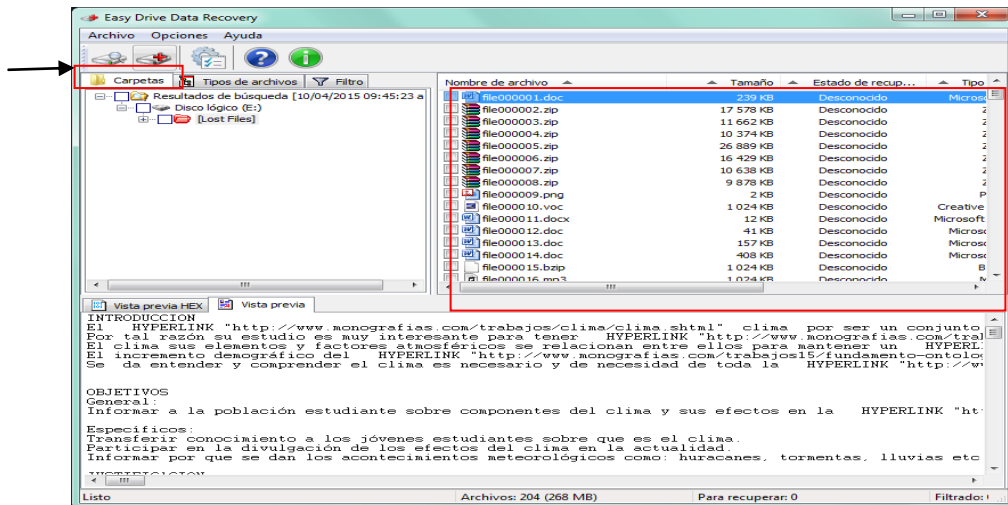


Figura 3.13

Paso: 14

En esta imagen se selecciona la pestaña “tipos de archivos” aquí aparecerán todos los archivos del disco portátil y también aparecerán los archivos eliminados con los nombres de “file 00001.doc, sucesivamente (Ver figura 3.14)

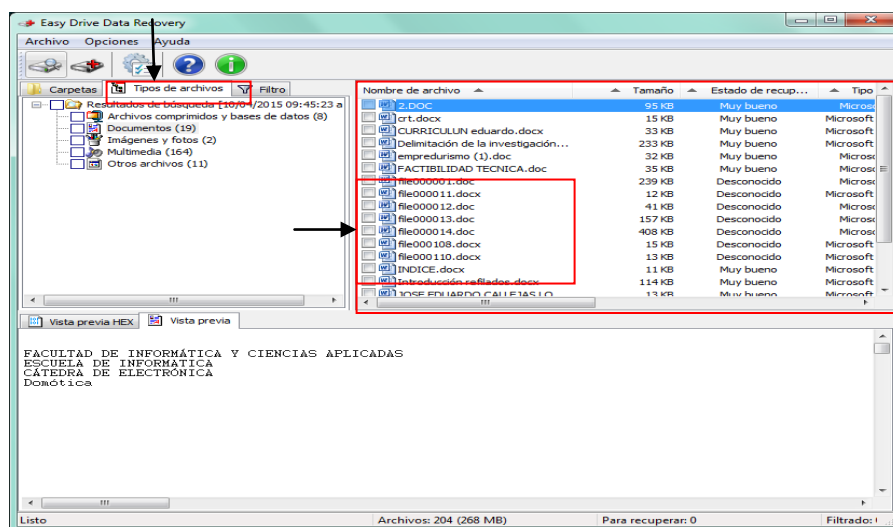


Figura 3.14

Pasos: 15 y 16

Para recuperar el o los archivos eliminados se seleccionan y luego se hace clic en “Recuperar archivos seleccionados” pero también se selecciona la carpeta donde se guardaran y clic en “Next” (Ver figura 3.15) y mostrara un cuadro donde dice que los archivos han sido recuperados (Ver figura 3.16).

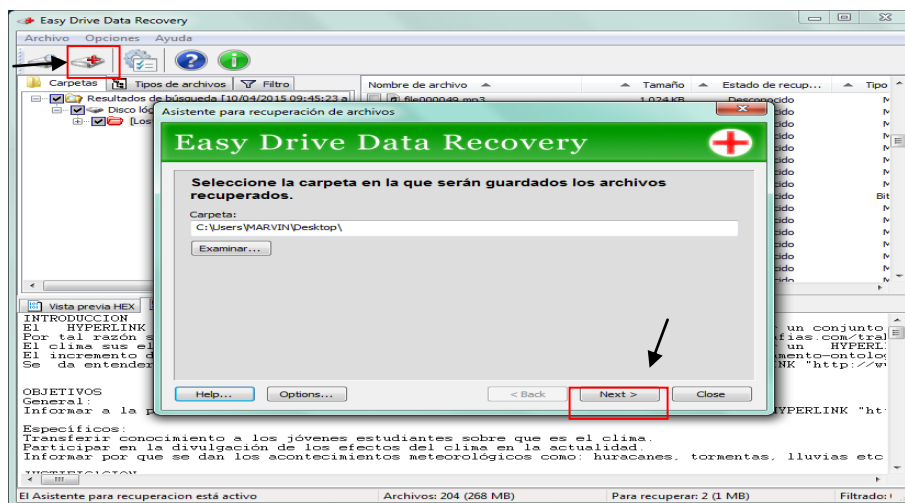


Figura 3.15



Figura 3.16

Paso: 17

Una vez terminado esto se busca la carpeta donde se han guardado los archivos que han sido recuperados en este caso la carpeta se llama “EDDR RECOVERED”, se abre y mostrara otras carpetas que se tienen que abrir para que muestren los archivos recuperados (Ver figura 3.17).

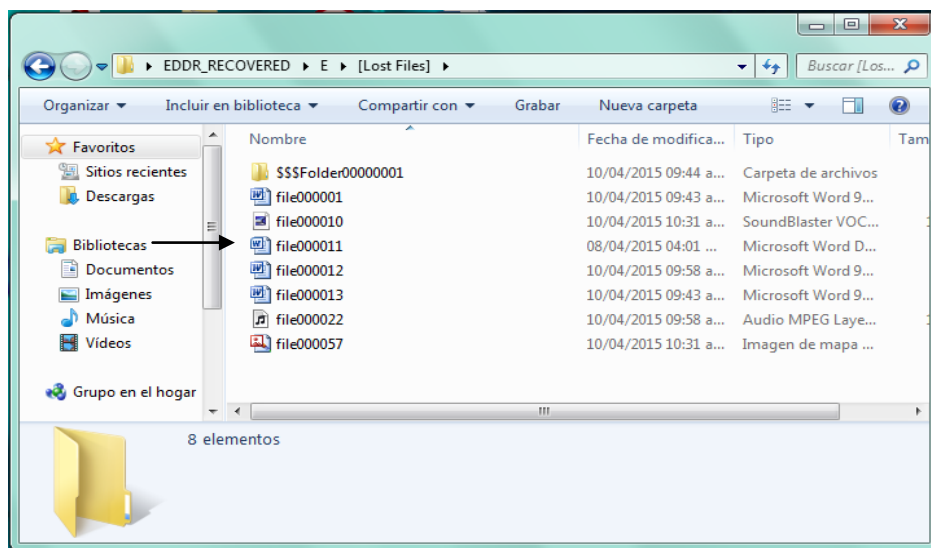


Figura 3.17

Outpost Security Suite Pro

Este programa se encarga de la seguridad del Sistema Operativo y proporciona un arsenal ampliamente superior de defensa contra amenazas actuales y futuras, que van desde malware hasta los piratas informáticos. Este programa cuenta con un cortafuego, antimalware rápido, protección de host y herramientas de seguridad web y un antispam de autoaprendizaje para una protección mas completa.

Instalación del programa Outpost Security Suite Pro 9.1

Lo primero que se hace es descargar el programa desde la página <http://www.dl2.agnitum.com>. Una vez descargado se empieza la instalación y funcionamiento.

Paso: 1

Seleccionan el programa Outpost Security Suite pro 9.1 doble clic en él y aparecerá la siguiente imagen donde se selecciona el idioma que se utilizara en el proceso de instalación (Ver figura 4.1).

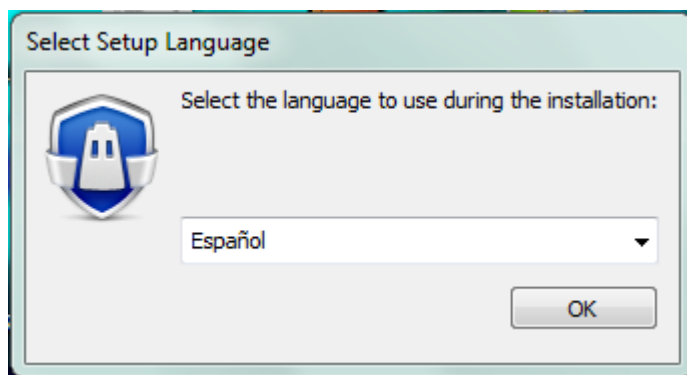


Figura 4.1

Paso: 2

En esta imagen el programa se está instalando en la computadora y en la cual está extrayendo los archivos (Ver figura 4.2).

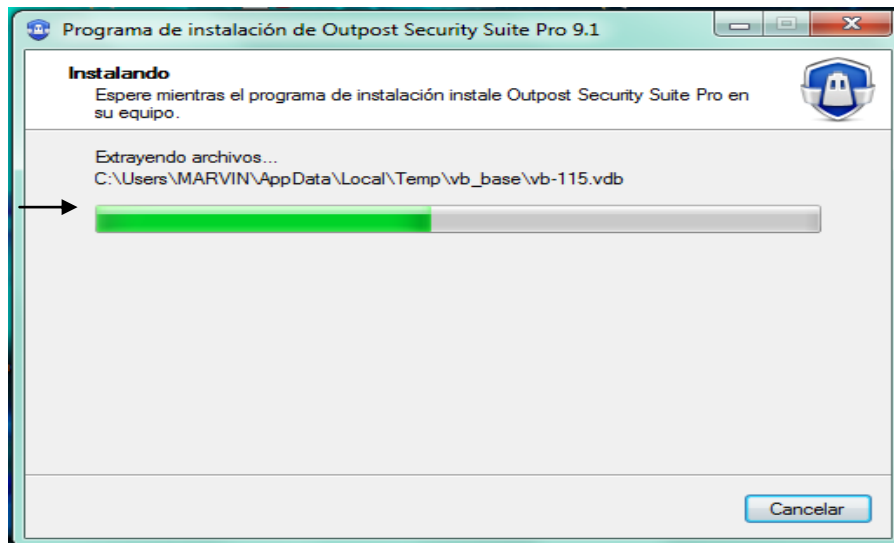


Figura 4.2

Paso: 3

En esta imagen da la bienvenida al asistente para la instalación de Outpost Security Suite Pro y además ofrece una protección integral en el equipo y se continua con el procesó (Ver figura 4.3).

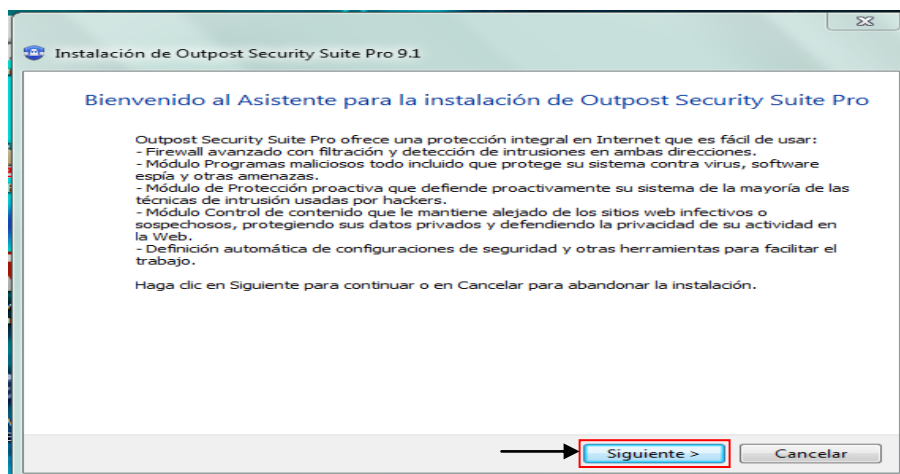


Figura 4.3

Paso: 4

Aquí en esta imagen aparece el contrato de licencia de Outpost Security Suite Pro donde muestra las condiciones antes de su instalación y se hace clic en “Aceptar” (Ver figura 4.4).

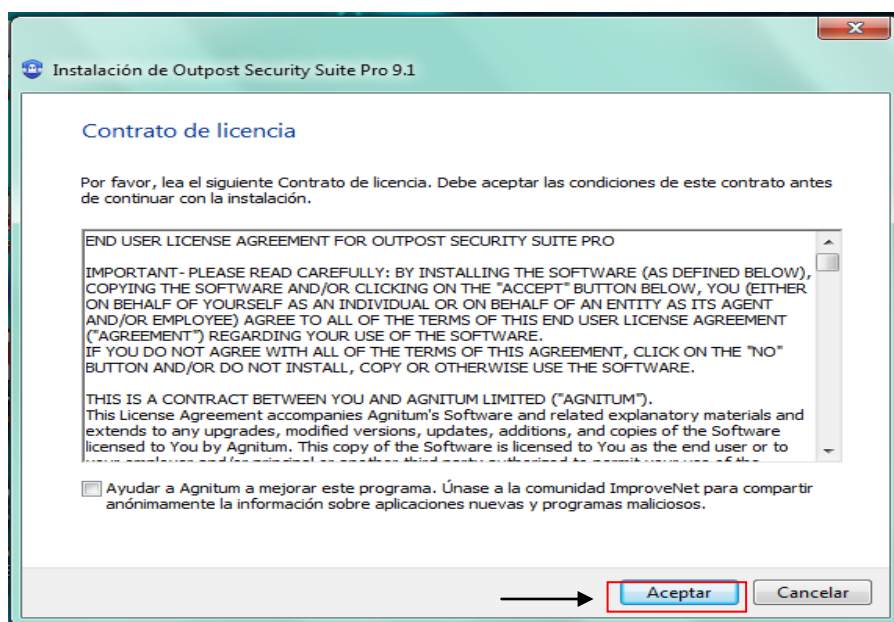


Figura 4.4

Paso: 5

En esta imagen el programa está buscando el posible software que esté malicioso ya que son amenazas en el sistema (Ver figura 4.5).

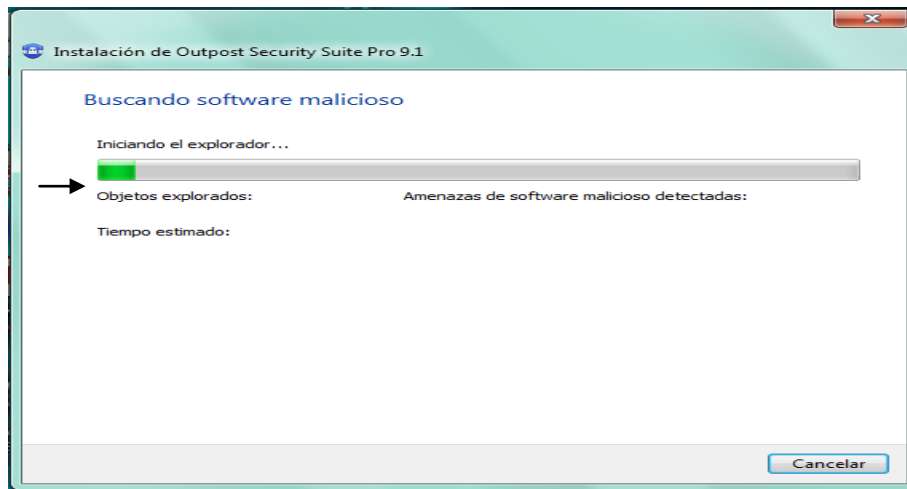


Figura 4.5

Paso: 6

Aquí muestra algunos componentes que pueden pertenecer a programas de seguridad de terceros en lo cual hay que confirmar la instalación de estos programas (Ver figura 4.6)

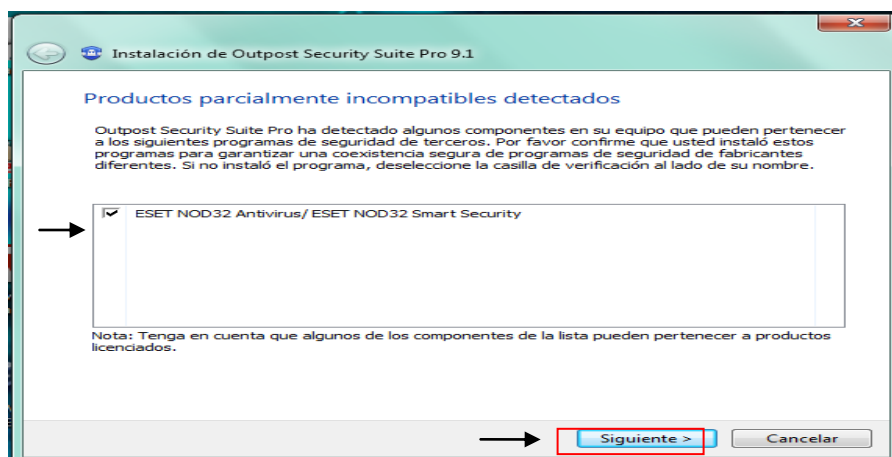


Figura 4.6

Paso: 7

En esta imagen el programa muestra dos tipos de instalación las cuales son la típica y la personalizada, en este caso se usara instalación típica (Ver figura 4.7).

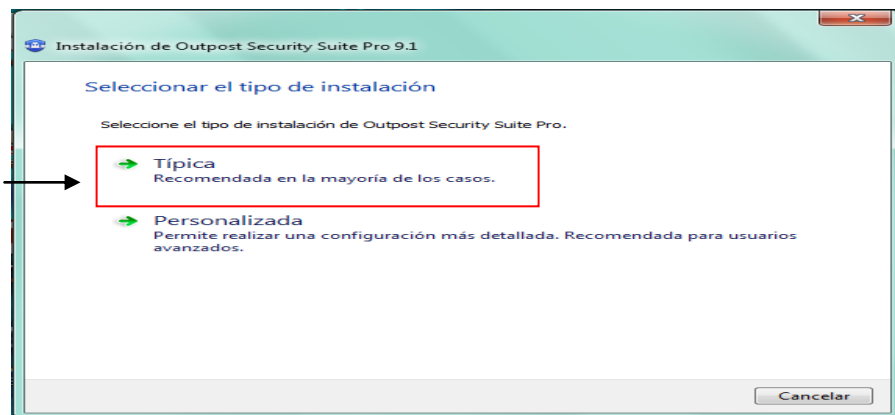


Figura 4.7

Paso: 8

En esta imagen muestra el programa de instalación instale Outpost Security Suite Pro en el equipo (Ver figura 4.8).

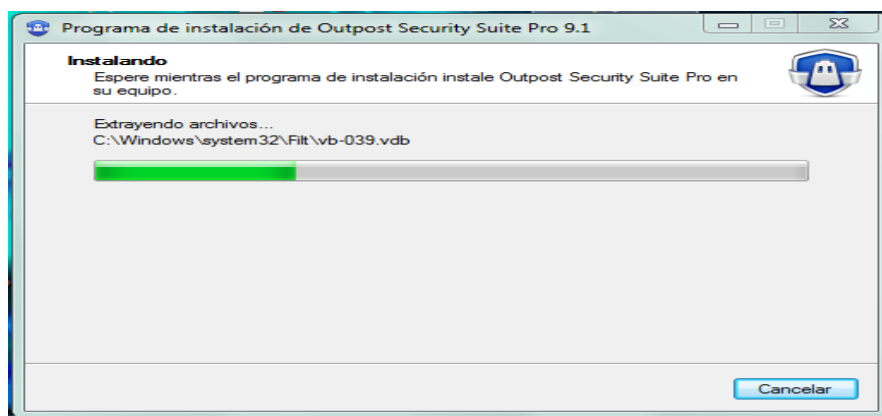


Figura 4.8

Paso: 9

En esta imagen el programa está realizando operaciones y a la vez la está buscando aplicaciones que estén protegidas este procedimiento tardara unos minutos (Ver figura 4.9).

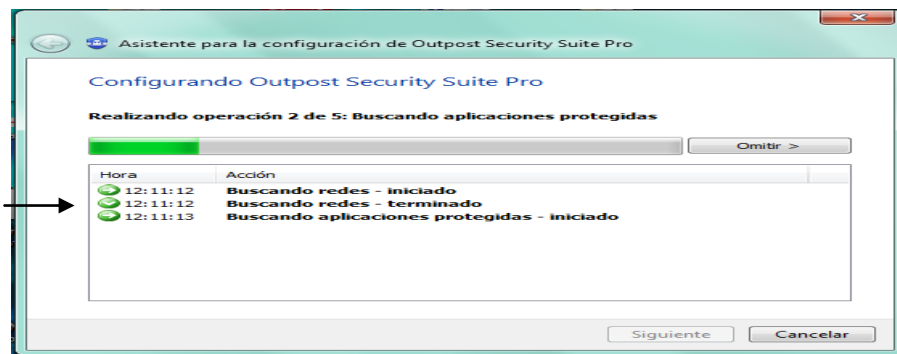


Figura 4.9

Paso: 10

En esta imagen explica que para finalizar la instalación se debe reiniciar el equipo y se hace clic en "Sí" para que se pueda ocupar el programa (Ver figura 4.10)

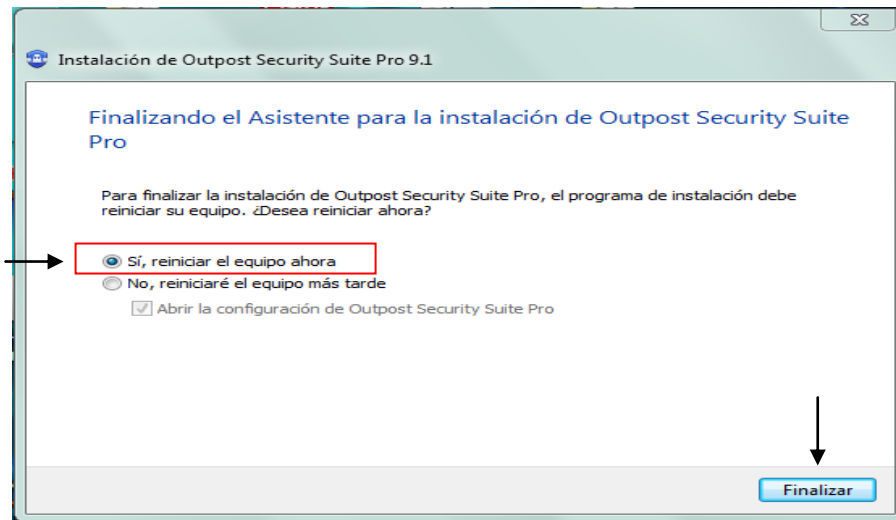


Figura 4.10

Paso: 11

En esta imagen muestra la pantalla de inicio de Outpost Security Suite Pro donde explica que el equipo está protegido (Ver figura 4.11).

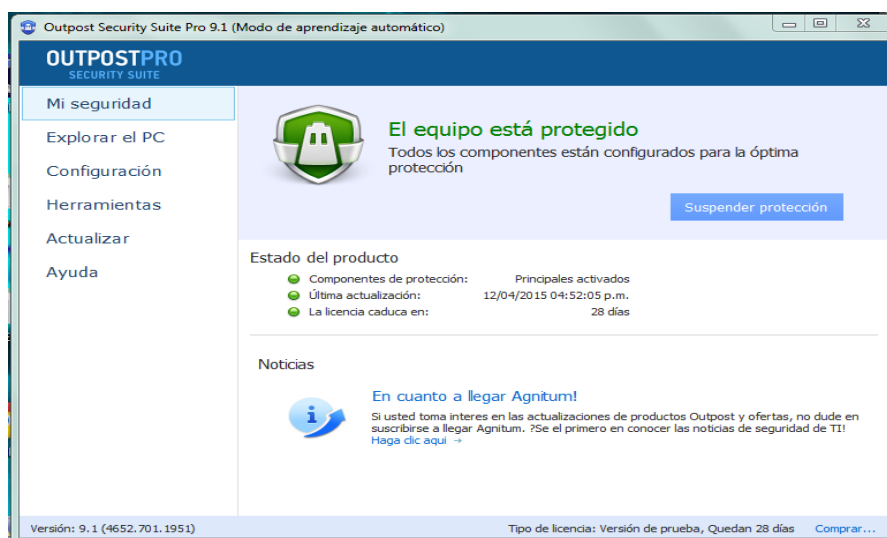


Figura 4.11

Paso: 12

En esta imagen se selecciona la opción “Explorar el PC” en la cual los muestra el tipo de exploración que se desea hacer en nuestro equipo (Ver figura 4.12).

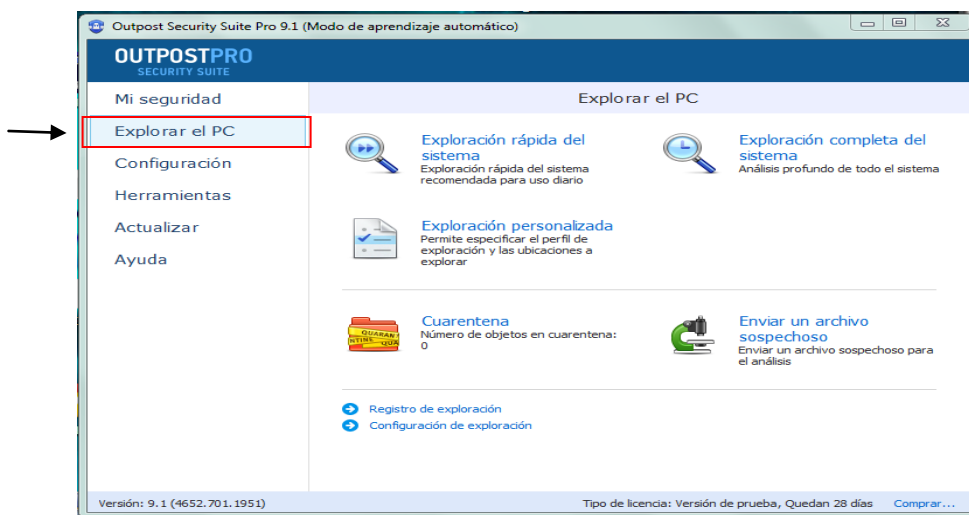


Figura 4.12

Paso: 13

En esta imagen se selecciona la opción de “Exploración rápida del sistema” aquí muestra que está analizando el equipo (Ver figura 4.13).

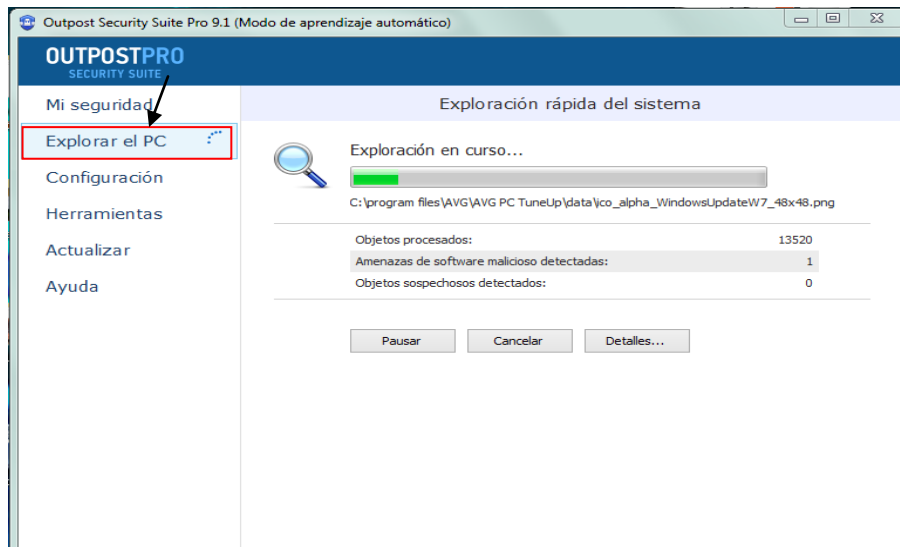


Figura 4.13

Paso: 14

En esta imagen se selecciona la opción de “configuración” aquí muestra todas las configuraciones establecidas del sistema (Ver figura 4.14).

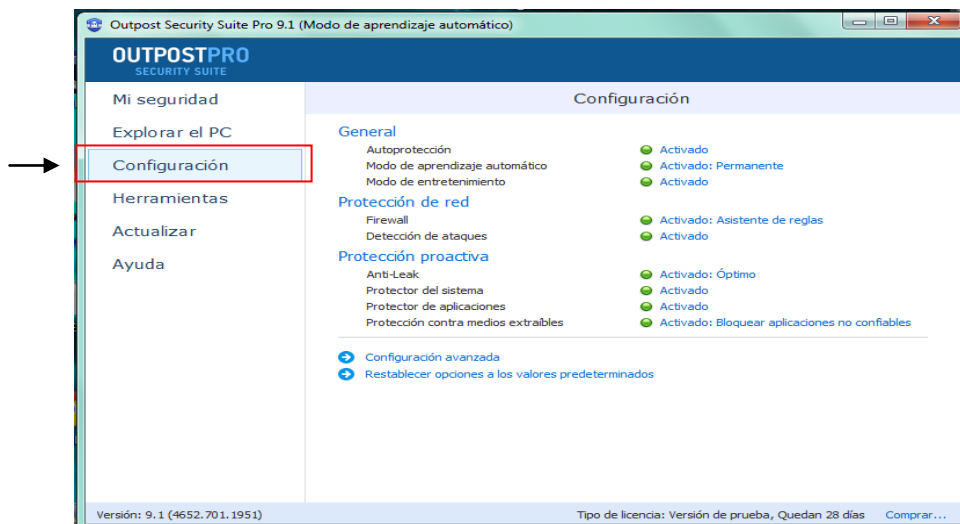


Figura 4.14

Paso: 15

En esta imagen se selecciona “Herramienta” dentro de esta aparecen todas las herramientas del programa (Ver figura 4.15)

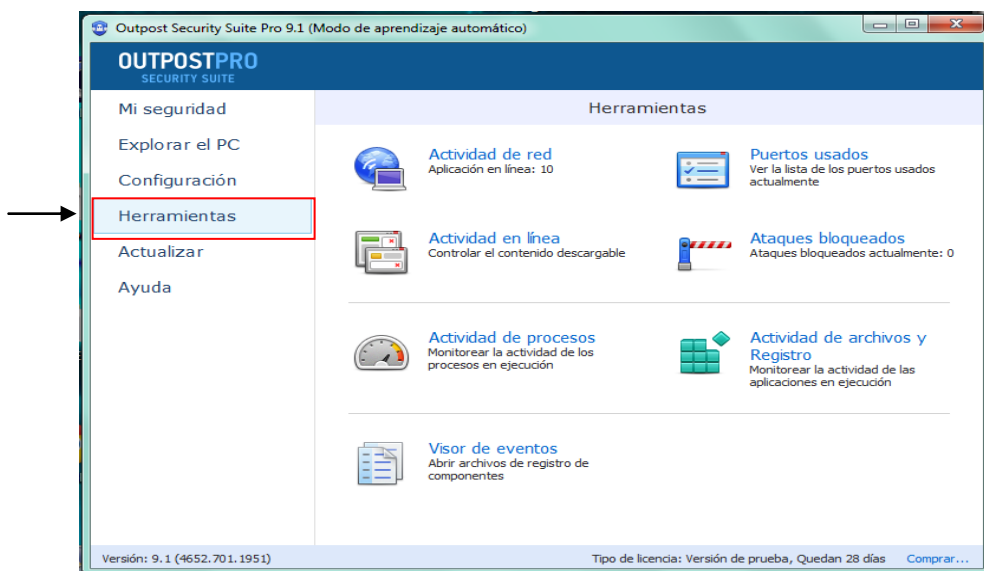


Figura 4.15

Paso: 16

En esta imagen se selecciona “Actualizar” aquí explica que la base de virus está completamente actualizada (Ver figura 4.16).

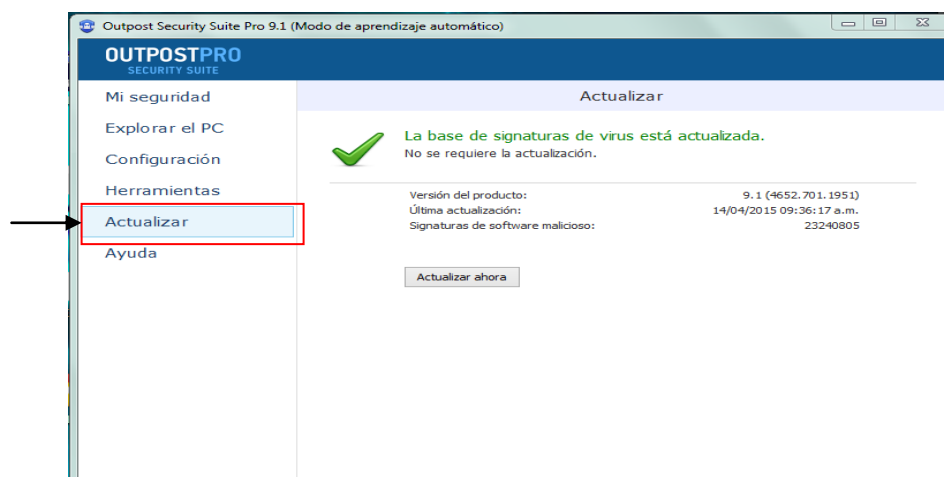


Figura 4.16

Paso: 17

En esta se selecciona la opción “Ayuda” aquí los brinda un conocimiento extra del programa tanto de cómo utilizar el programa, información de licencia (Ver figura 4.17).

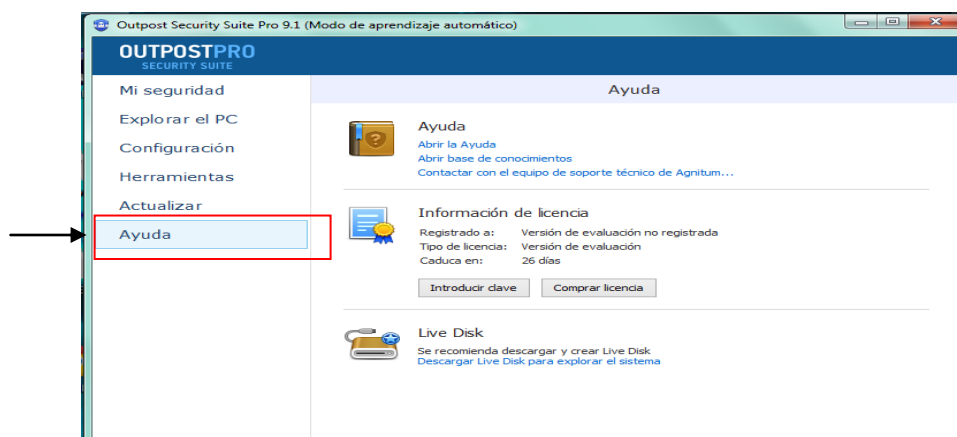


Figura 4.17

AxCrypt

Este programa permite cifrar archivos en el Sistema Operativo Windows, para poderlo así protegerlos y ocultarlos mediante una clave y además permite comprimir, descifrar, ver y editar archivos. Los archivos cifrados poseen la extensión *.axx y se muestran con un icono diferente.

Instalación del programa AxCrypt

Lo primero que debe hacer es descargar el programa desde la página <http://www.axantum.com/AxCrypt/> Una vez descargado se empieza la instalación y funcionamiento.

Paso 1

Selecciona el programa AxCrypt y doble clic en él y aparecerá la siguiente imagen que muestra los acuerdos de la licencia, y se hace clic en “I Agree” para continuar (Ver figura 5.1).

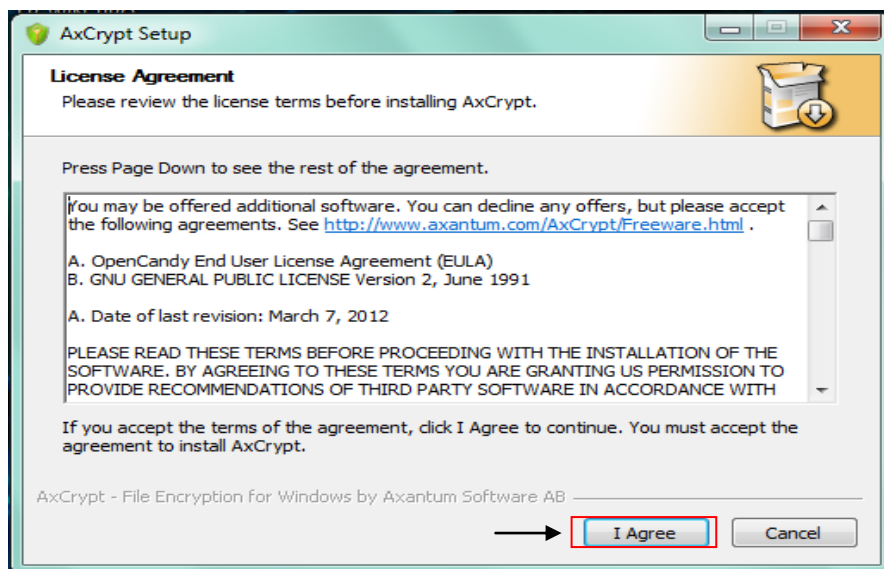


Figura 5.1

Paso: 2

En esta imagen muestra que ha completado el asistente de configuración de AxCrypt, se hace clic en "Finish" para continuar (Ver figura 5.2).

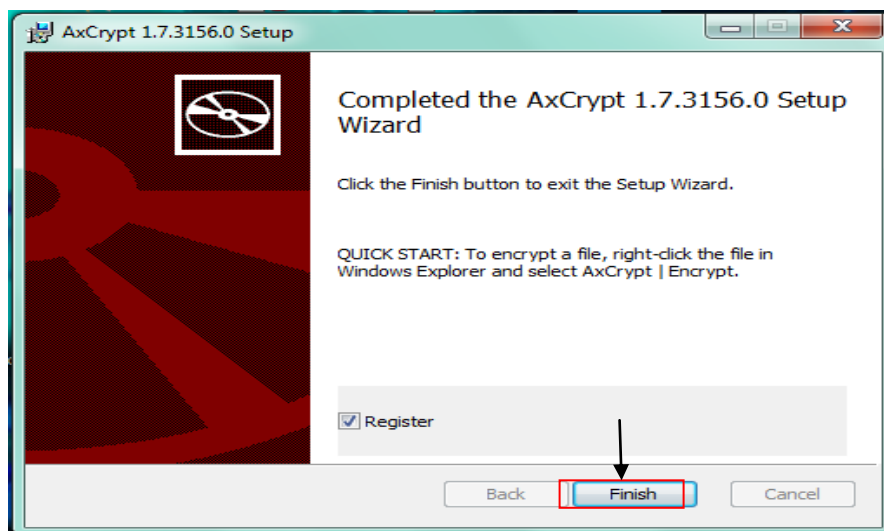


Figura 5.2

Paso: 3

En esta imagen da la bienvenida al programa, además el asistente de configuración permite cambiar la forma en que las características AxCrypt están instalados en su ordenador o para sacarlo de su ordenador, y se hace clic en “Next” para continuar (Ver figura 5.3)

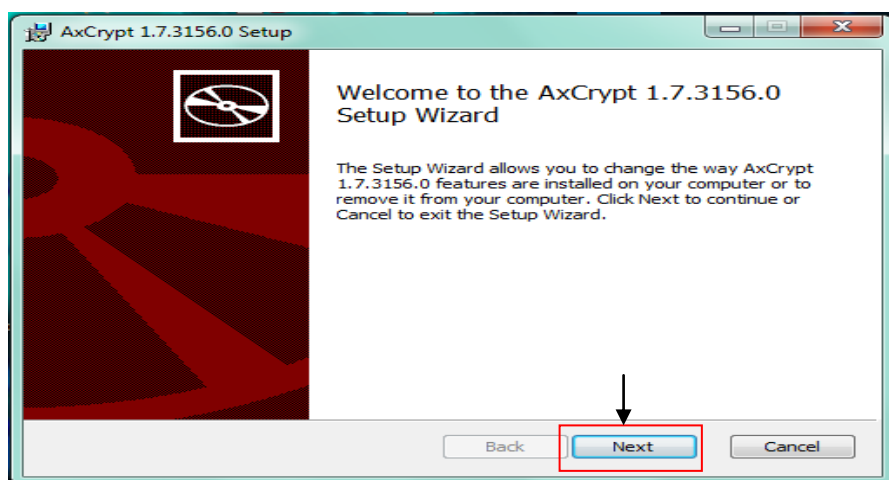


Figura 5.3

Paso: 4

En esta imagen aparecen 3 opciones las cuales son: “Change” esta permite cambiar la forma en que se instalan las características; “Repair” esta permite reparar los errores en la instalación; “Remove” retira el programa (Ver figura 5.4).

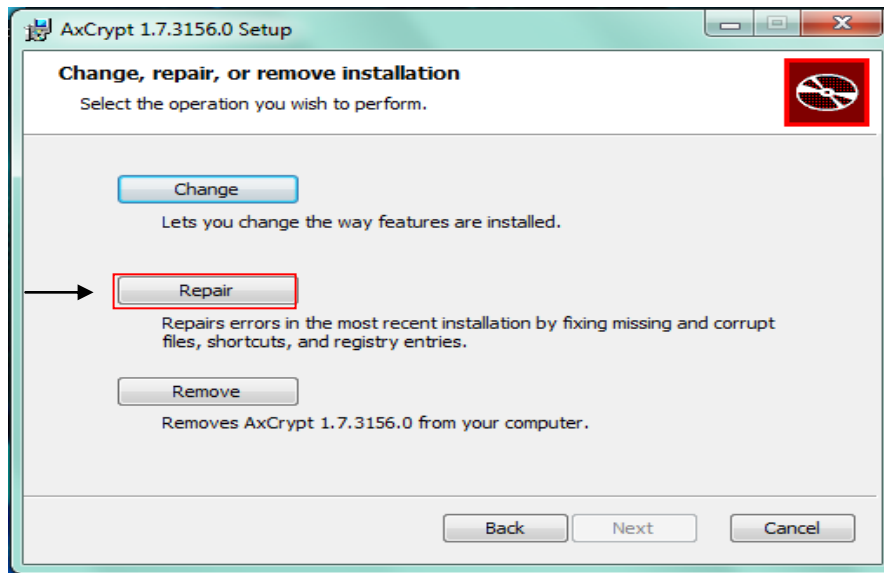


Figura 5.4

Paso: 5

En esta imagen ya se encuentra listo para reparar AxCrypt, se hace clic en “Repair” para continuar (Ver figura 5.5).

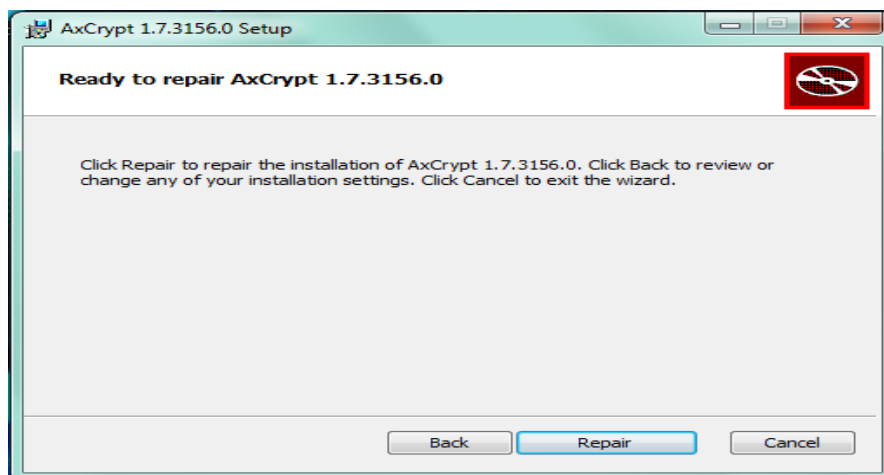


Figura 5.5

Paso: 6

La primera imagen muestra los archivos en uso y que algunos archivos que necesitan se actualizados están actualmente en uso, y se selecciona “Cerrar las aplicaciones”, y la segunda los muestra la reparación de AxCrypt (Ver figura 5.6).

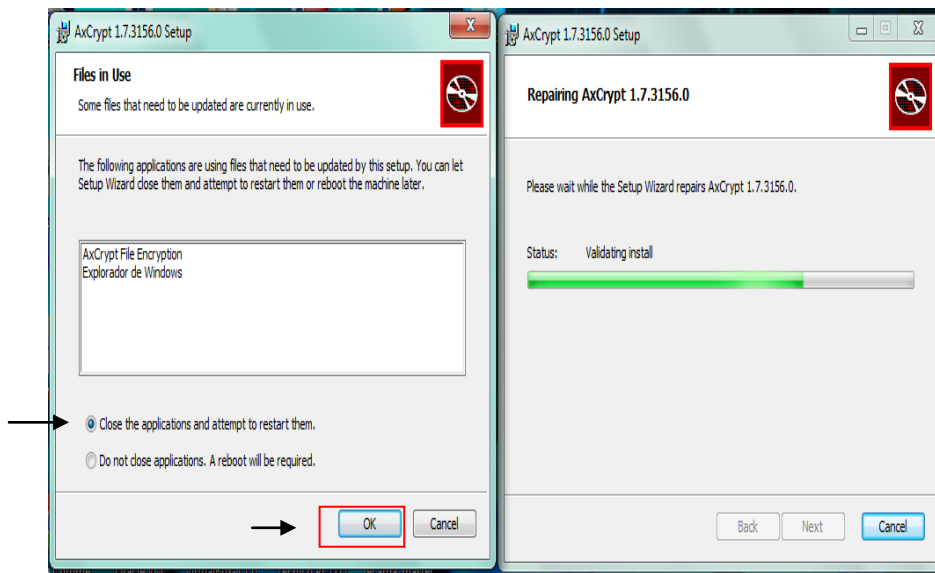


Figura 5.6

Paso: 7

Una vez finalizada la instalación se empieza con el funcionamiento del programa AxCrypt esta herramienta cuenta con dos formas de control de acceso de archivo. La primera es la que todo conocemos que se le asigna una clave al archivo.

En esta imagen se ha seleccionado la carpeta que tiene como nombre “Carpeta privada” donde hay documentos importantes para que nadie acceda a estos archivos (Ver figura 5.7)

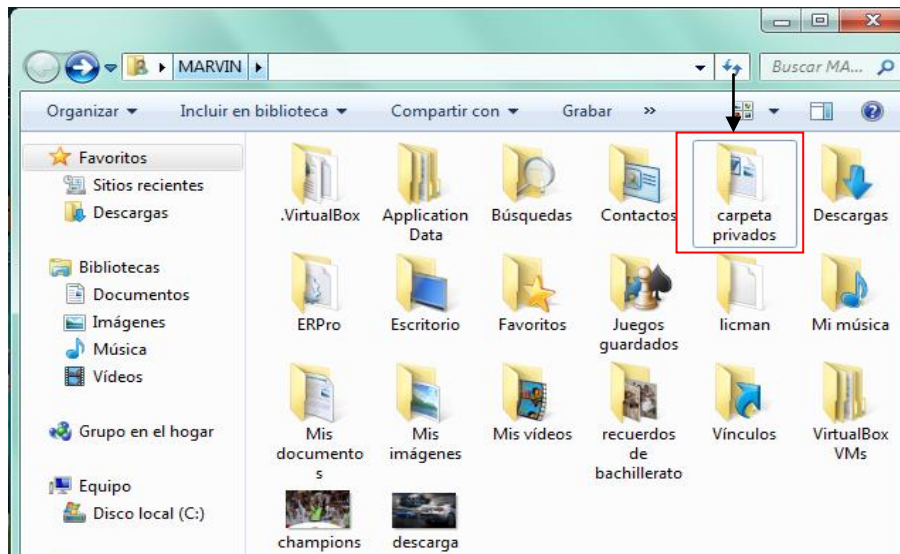


Figura 5.7

Paso: 8

En esta imagen se hace doble clic en la carpeta para que muestre los archivos que están, luego se selecciona el archivo, clic derecho y el programa ya instalado te muestra este submenú (Ver figura 5.8).

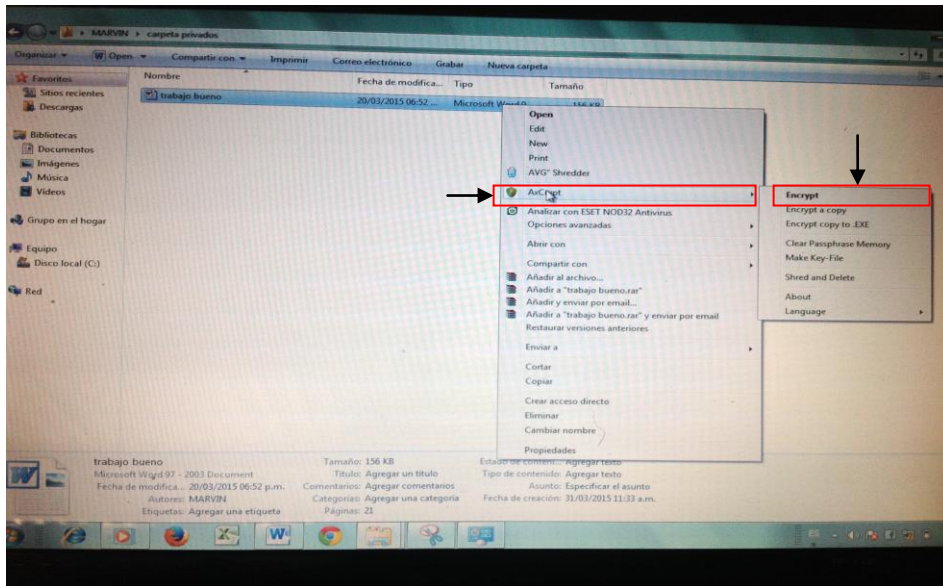


Figura 5.8

Paso: 9

Una vez seleccionado “Encrypt” muestra este cuadro donde se coloca una palabra como contraseña la verificamos y clic en “OK” para continuar (Ver figura 5.9).

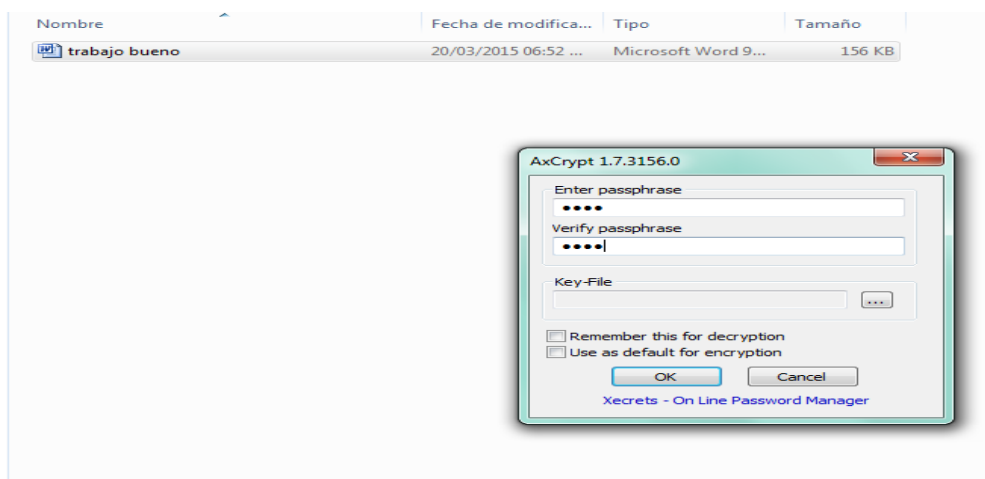


Figura 5.9

Paso: 10

En esta imagen muestra el archivo ya encriptado y a la vez lo comprime, ahora al abrir el archivo no lo va a dejar (Ver figura 5.10).

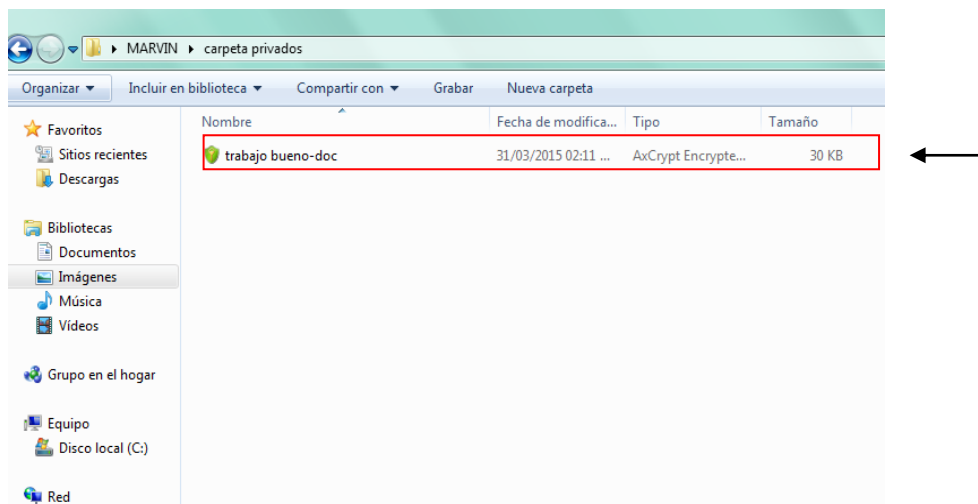


Figura 5.10

Paso: 11

En esta imagen se hace doble clic en el archivo y muestra el siguiente mensaje que tendrá de insertar la clave asignada, como solamente le dio abrir lo que hizo fue abrir el documento pero sigue encriptado (Ver figura 5.11).

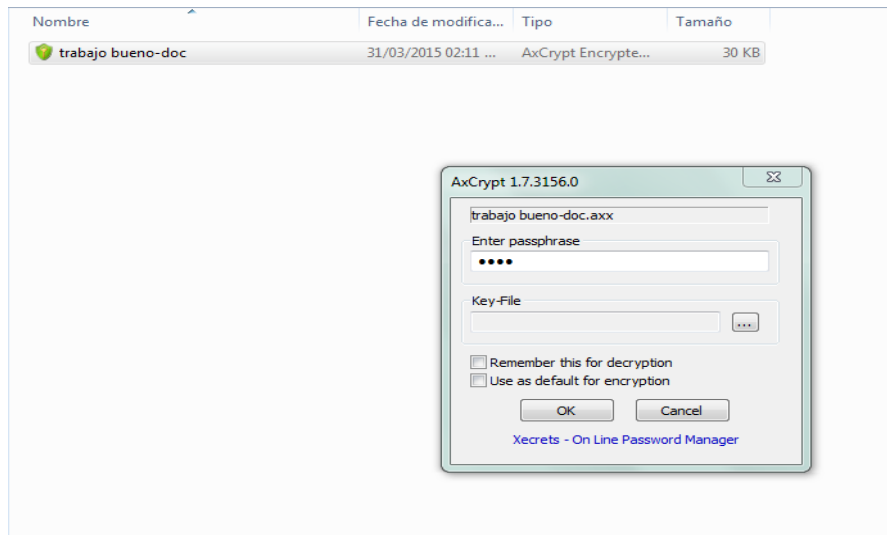


Figura 5.11

Paso: 12

Para quitarle la encriptación al archivo hacer clic derecho, en la opción AxCrypt muestra un cuadro donde se tendrá que darle en “Decrypt” (Ver figura 5.12).

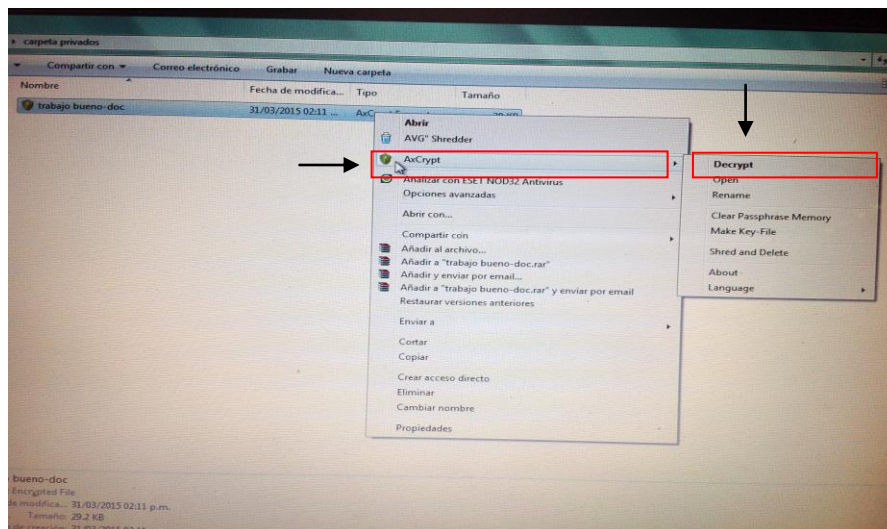


Figura 5.12

Paso: 13

En esta imagen muestra el cuadro donde se tiene que colocar la contraseña para desenscriptar el archivo (Ver figura 5.13).

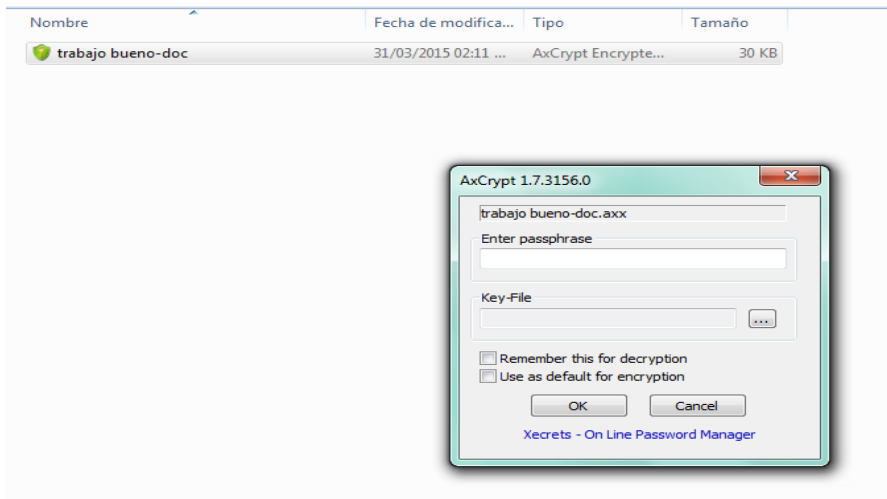


Figura 5.13

Paso: 14

En esta imagen muestra el archivo ya desenscriptado (Ver figura 5.14).

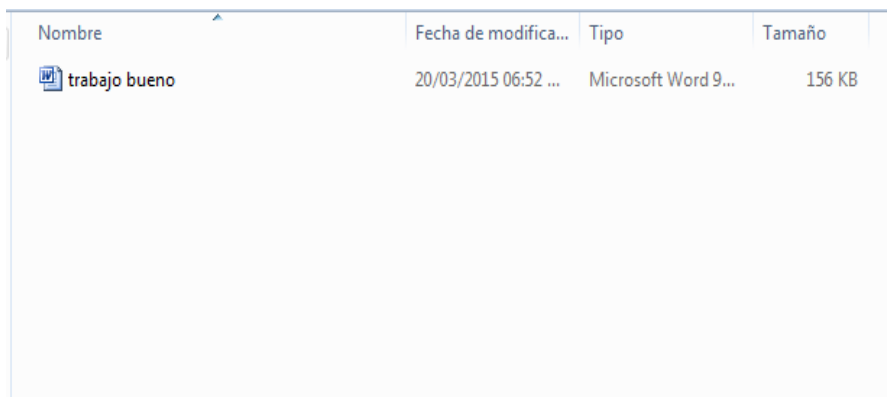


Figura 5.14

La segunda forma es crear un archivo que funcione como llave y acceder a la información así que cada vez que se quiera descriptar el archivo, se necesitaría ese archivo llave de otra forma no se puede.

Paso: 15

En esta imagen se selecciona el archivo, se hace doble clic en él y muestra submenú donde se selecciona la opción “Make Key-File” para crear la llave (Ver figura 5.15).

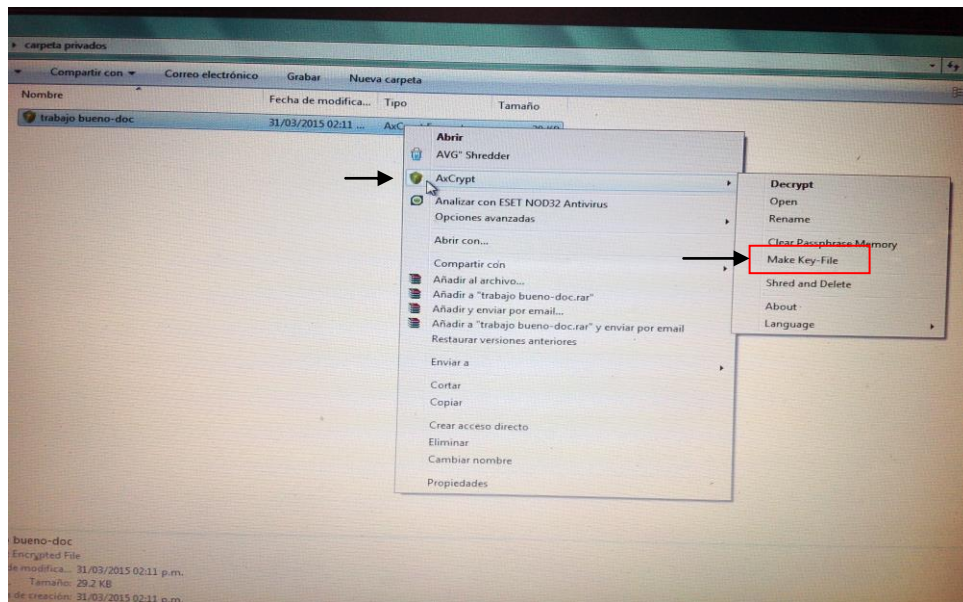


Figura 5.15

Paso: 16

Una vez seleccionada “Make Key-File, aparece un cuadro que explica que se va a crear una llave y que necesitara siempre que se quiera abrir ese archivo si está seguro (Ver figura 5.16).

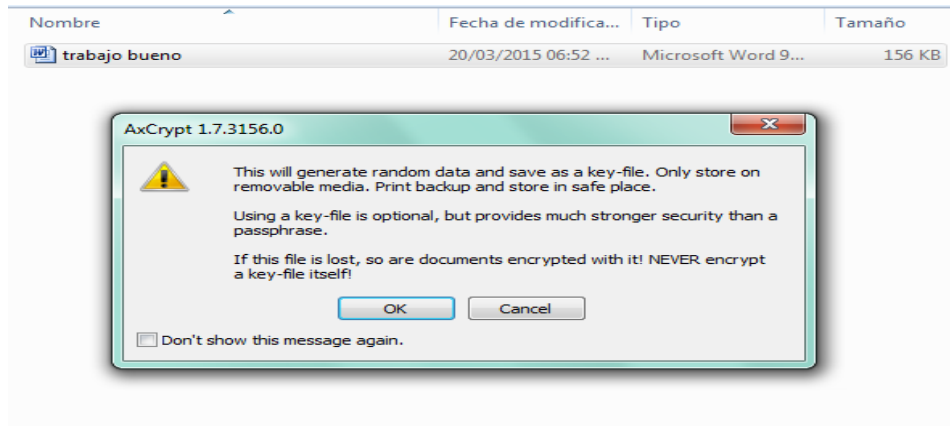


Figura 5.16

Paso: 17

Obviamente no se pone la llave en vista de todos, pero en este caso para cuestione didácticas se colocara en la misma carpeta que se llamara “Key” (Ver figura 5.17).

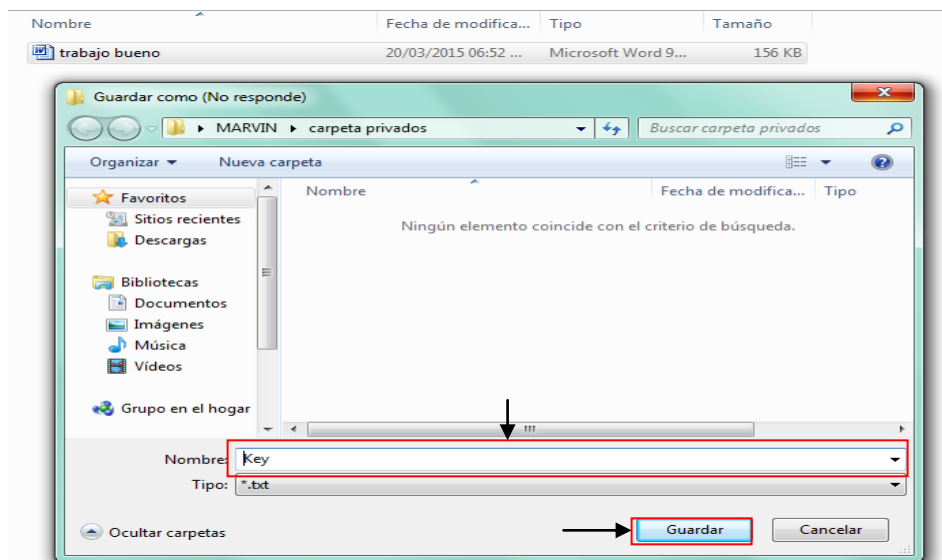


Figura 5.17

Paso: 18

En esta imagen se acepta la llave (Ver figura 5.18).

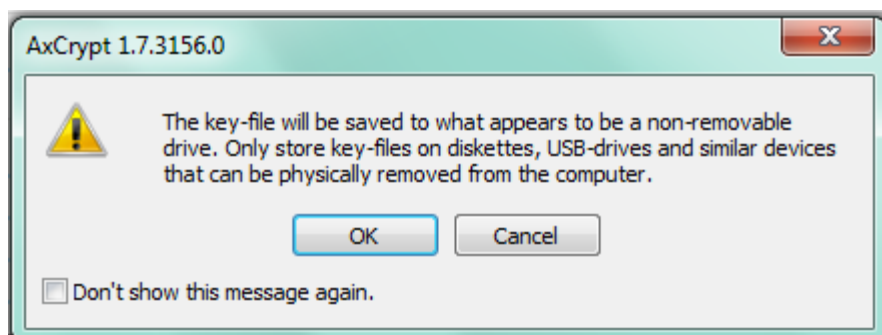


Figura 5.18

Paso: 19

En esta imagen muestra la llave ya creada que se ha guardado en la misma carpeta (Ver figura 5.19).

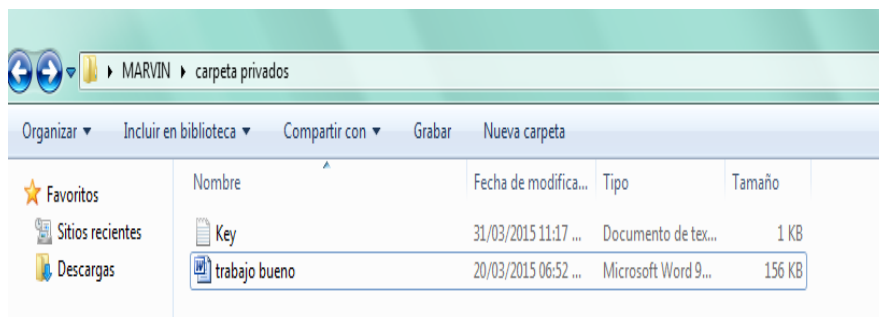


Figura 5.19

Paso: 20

En esta imagen todavía no se le asigna la llave a ningún archivo, pero ya está la llave ahora si se quiere encriptar este archivo que solamente se pueda abrir con una llave, se hace clic en “Encrypt” y en este caso se usara esta opción que sería usar un archivo llave (Ver figura 5.20).

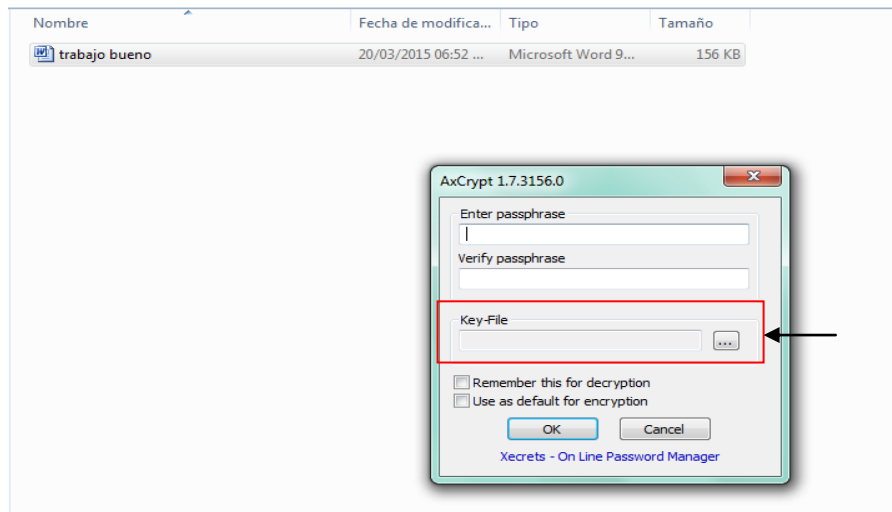


Figura 5.20

Paso: 21

En esta imagen muestra un mensaje de la llave que ya se tiene, se hace clic en “OK” para continuar (Ver figura 5.21).

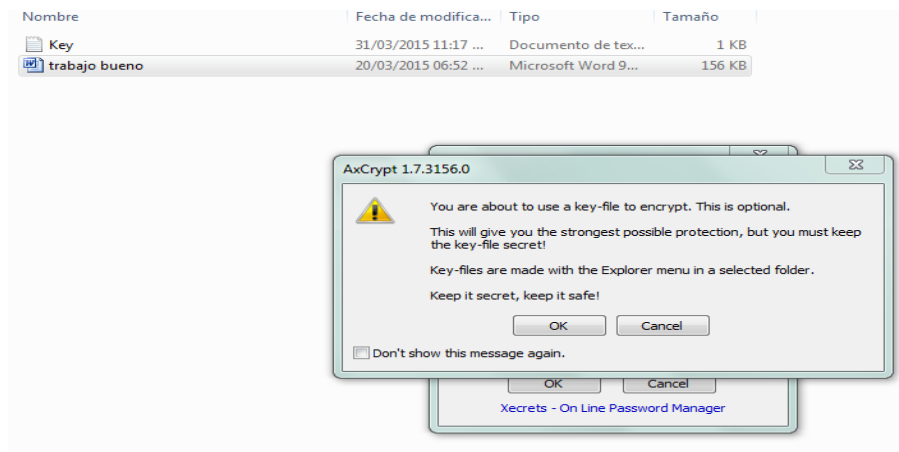


Figura 5.21

Paso: 22

Aquí en esta imagen se seleccionara la llave que se ha creado en la carpeta, simplemente se busca y se abrirá (Ver figura 5.22).

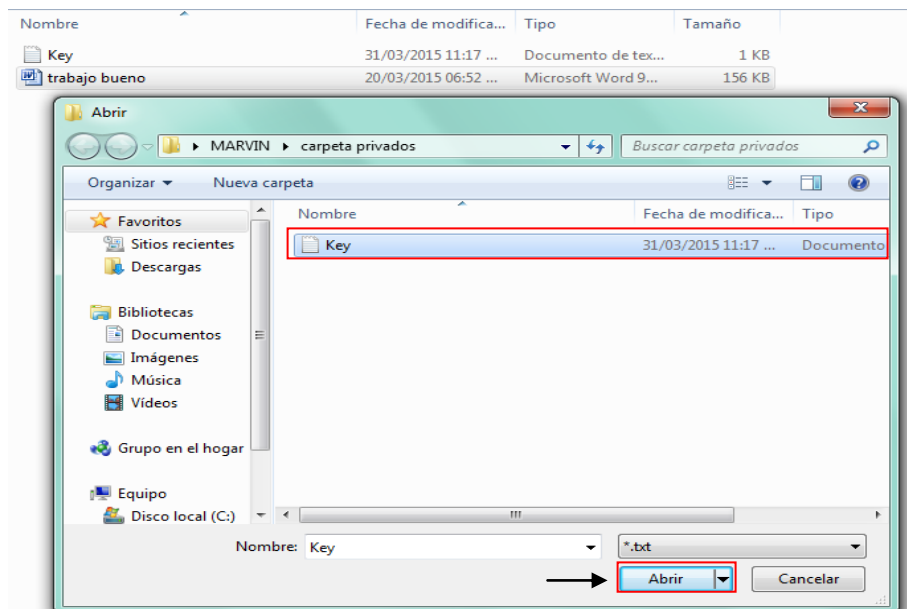


Figura 5.22

Paso: 23

En esta imagen ya está la llave, simplemente se selecciona “OK” y listo (Ver figura 5.23).

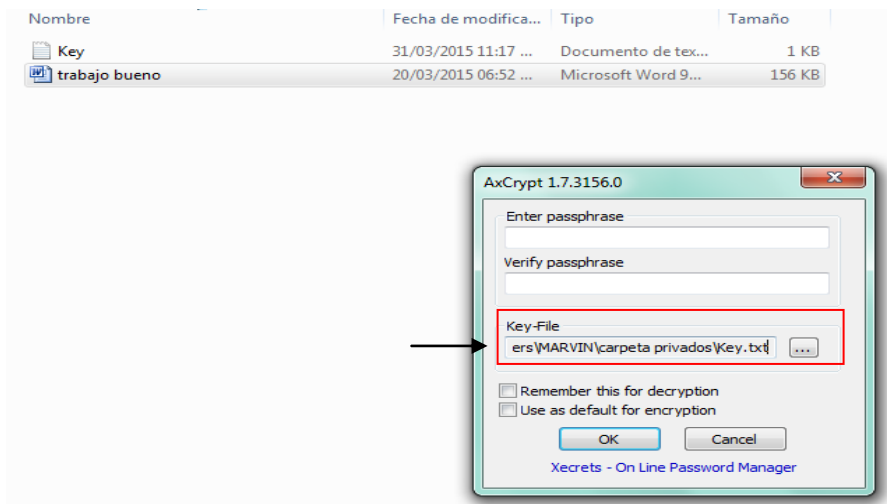


Figura 5.23

Paso: 24

En esta imagen ya está encriptado el archivo solamente que ahora no va a ser con una clave de acceso, si no que con un archivo de llave (Ver figura 5.24).

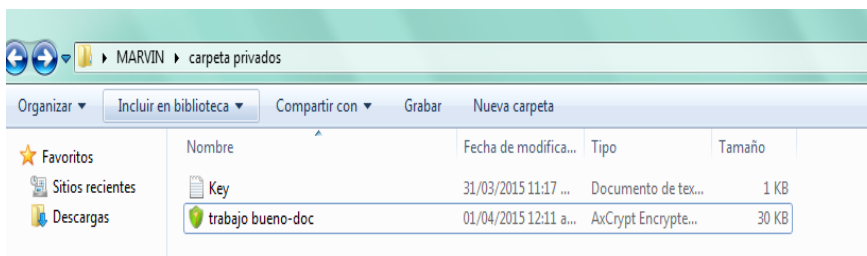


Figura 5.24

Paso: 25

En esta imagen cada vez que se quiera abrirlo o desenscriptar, no se necesitara una clave si no un archivo y se debe de tener bien guardado, se busca y se abre y se hace clic en “OK” para continuar (Ver figura 5.25).

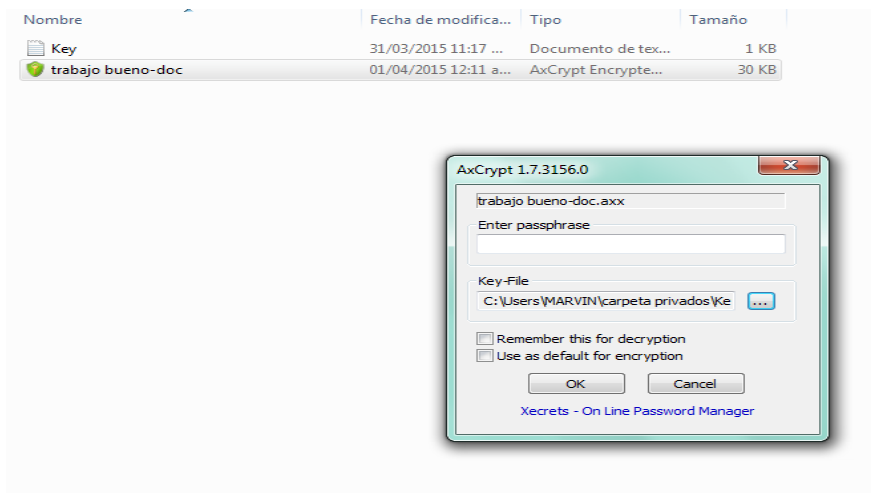


Figura 5.25

Paso: 26

En esta imagen muestra el archivo desenscriptado (Ver figura 5.26).

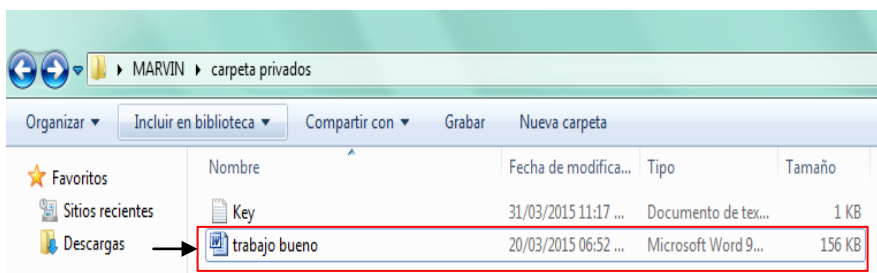


Figura 5.26

FTK Imager

FTK Imager es una herramienta para realizar réplicas y visualización previa de datos, la cual permite una evaluación rápida de evidencia electrónica para determinar si se garantiza un análisis posterior. FTK Imager puede crear copias perfectas (imágenes Forenses) de datos de computadora sin realizar cambios en la evidencia original.

Instalación del programa FTK Imager

Lo primero que se debe hacer es descargar el programa de la página oficial <http://accessdata.com/product-download> una vez descargado abrimos el instalador

Paso1: Abrir el instalador (Ver figura 6.1)



Figura6.1

Paso 2: En la siguiente imagen dar click en “next” para continuar con la instalación(Ver figura 6.2).

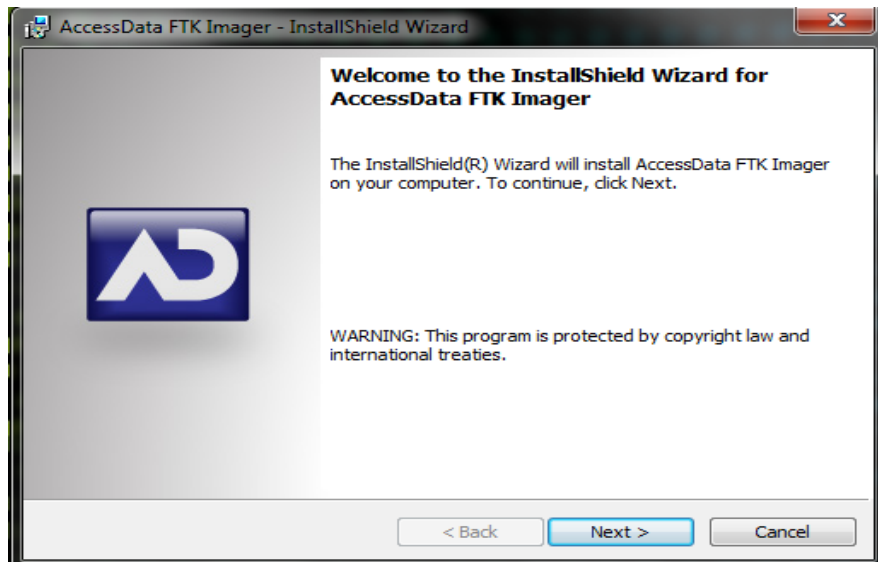


Figura 6.2

Paso 3: Seleccionar “aceptar en los términos de licencia” y click en next (Ver figura 6.3).

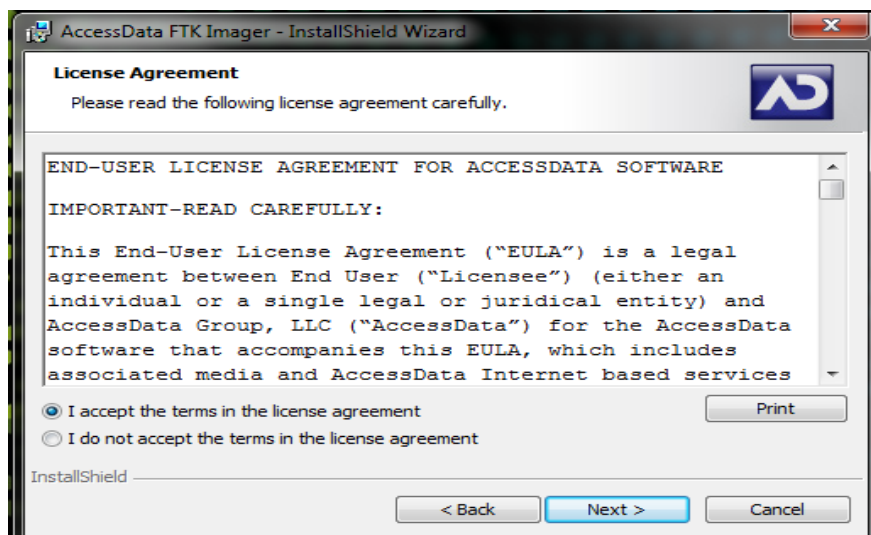


Figura6.3

Paso 4: Dar click en el botón “install” (Ver figura 6.4).

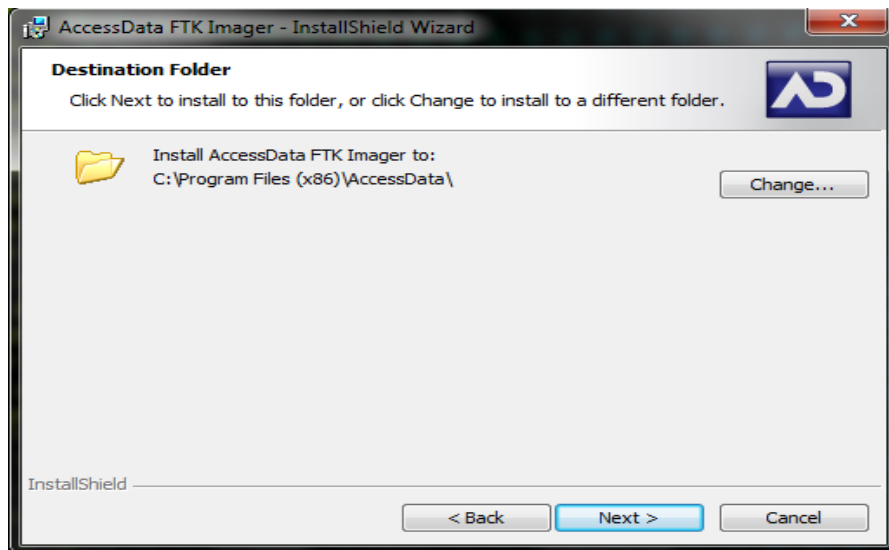


Figura 6.4

Paso 5: Esperar a que termine el proceso de instalación (Ver figura 6.5).

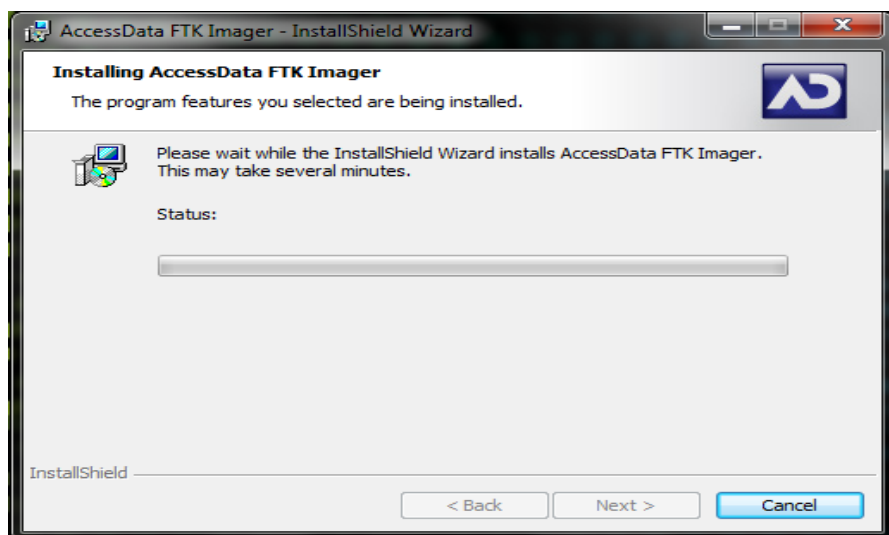


Figura 6.5

Paso 6: Una vez terminado el proceso se abre el programa y muestra la interfaz principal

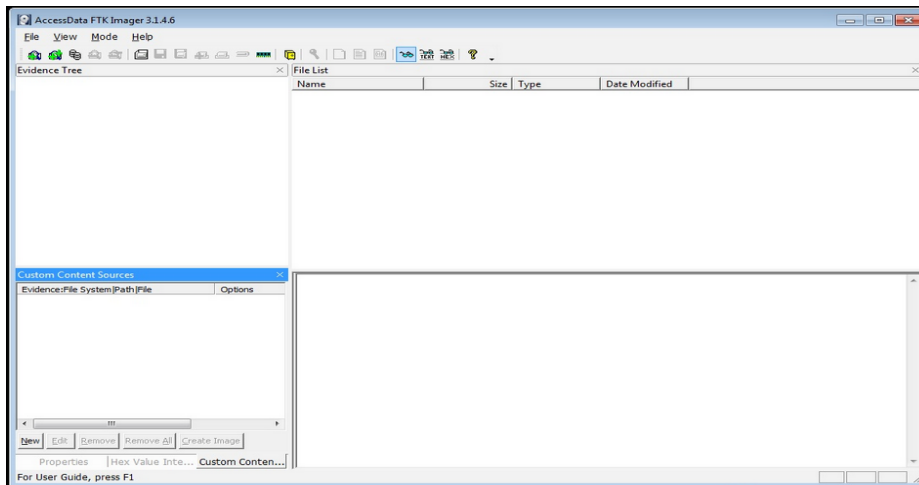


Figura 6.6

Paso 7: Hacer clic en la opción “File -> Create Disk Image” o Archivo -> Crear Imagen de Disco (Ver figura 6.7).

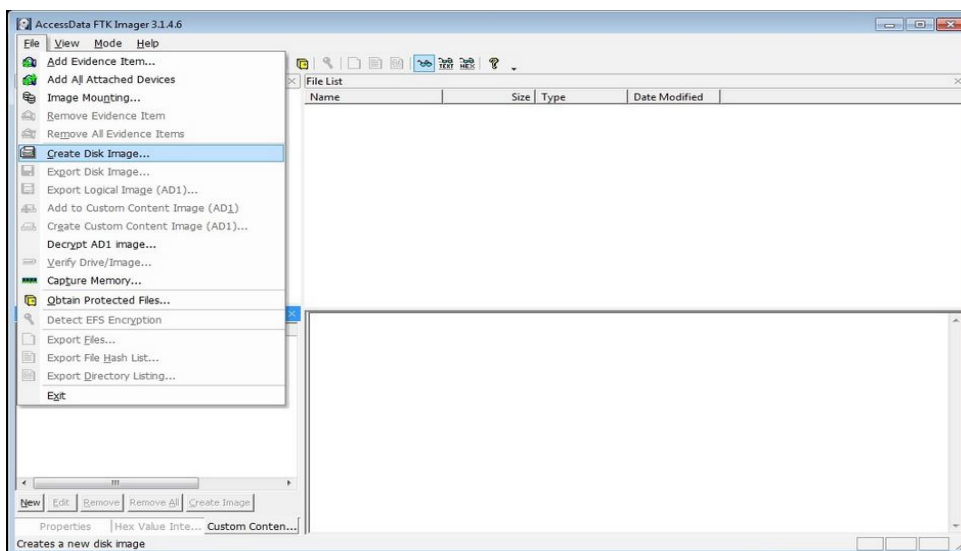


Figura 6.7

Paso 8: Se presentará una nueva ventana donde se requiere definir la Fuente. Para propósito de la presente práctica se creará una imagen Forense de toda una unidad USB o Memory Stick, por lo tanto se selecciona la opción “Physical Drive” o Unidad Física. Luego hacer clic en el botón “Siguiente” (Ver figura 6.8)..

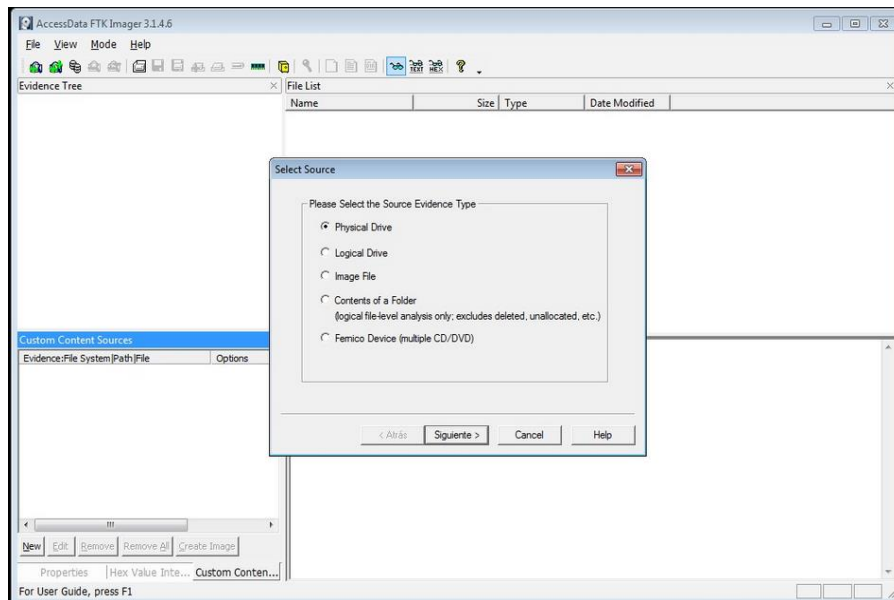


Figura 6.8

Paso 9:

En una nueva ventana se muestra un menú desplegable, en el cual se selecciona la Unidad Fuente correspondiente, para luego hacer clic en el botón “Finish” o Finalizar (Ver figura 6.9).

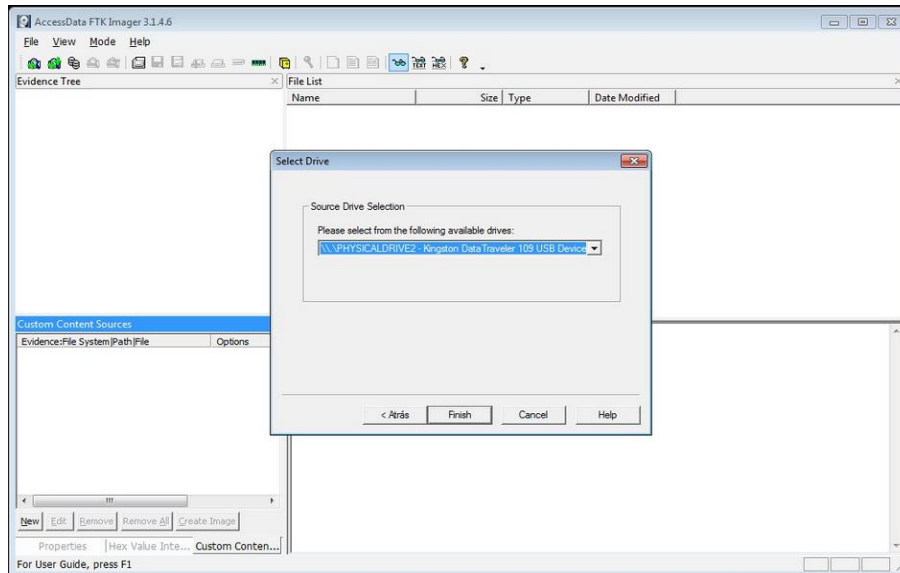


Figura 6.9

Paso 10: La siguiente ventana permite definir un Destino para la Imagen. Para esto es necesario hacer clic en el botón “Add.. (Ver figura 6.10).”

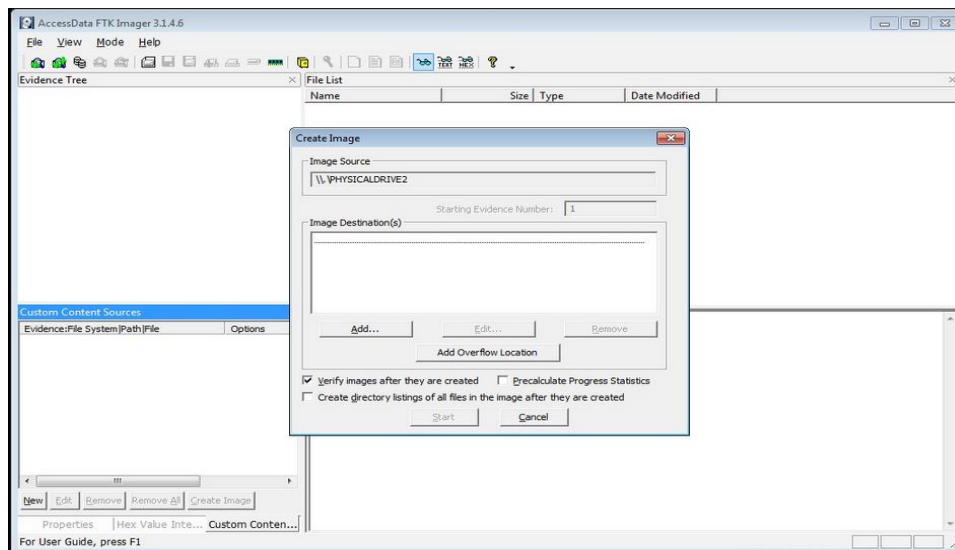


figura 6.10

Paso 11:

En esta ventana se define el tipo de la imagen de destino a crear. Para el caso de la presente práctica será una imagen “Raw” o en bruto, es decir tal y como sería creada utilizando una herramienta como dd o dcfldd. Revisar la publicación de título “Crear la Imagen Forense desde una Unidad utilizando dd” (Ver figura 6.11).

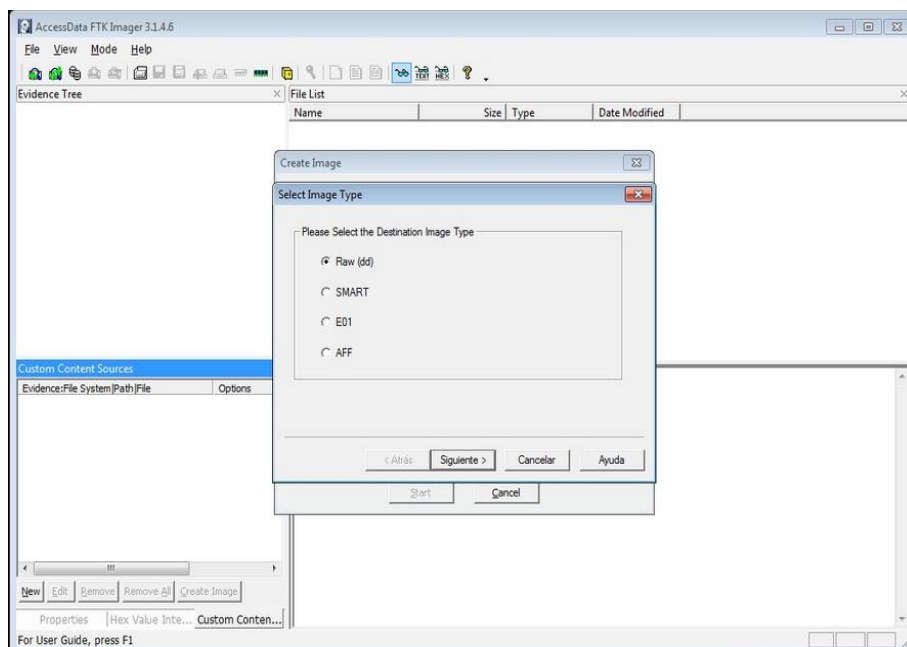


Figura 6.11

Paso 12:

La siguiente ventana solicita ingresar información sobre el ítem de evidencia. Al completar la información hacer clic en el botón “Siguiente” (Ver figura 6.12).

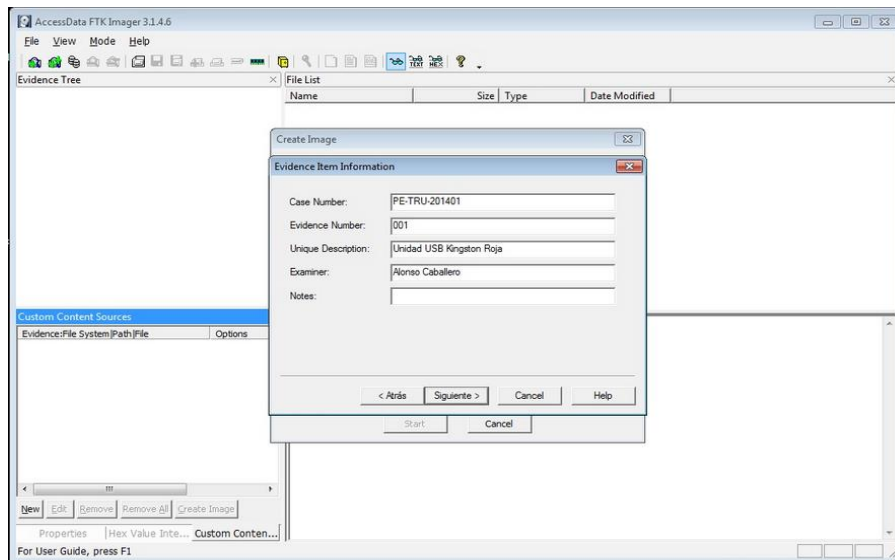


Figura 6.12

Paso 13:

Se requiere definir la carpeta donde se almacenará la imagen forense. La cual es seleccionada haciendo clic en el botón “Browse” o Navegar. A continuación se requiere nombrar la imagen forense (UnidadUSBKR). Y opcionalmente definir si la imagen resultante será dividida en varias partes o sino no será fragmentada. Para el caso de la presente práctica no será dividida, por lo tanto se define el valor “0” en el campo “Image Fragment Size (MB)” o Tamaño del Fragmento de la Imagen (Ver figura 6.13).

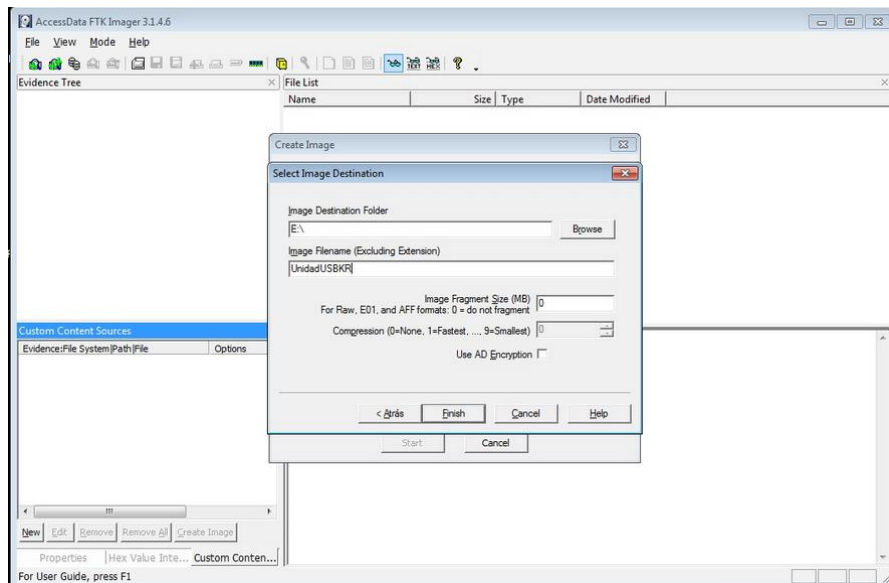


Figura 6.13

Paso 14: Al Hacer clic en el botón “Finish”. Se mostrará un resumen de las opciones seleccionadas (Ver figura 6.14).

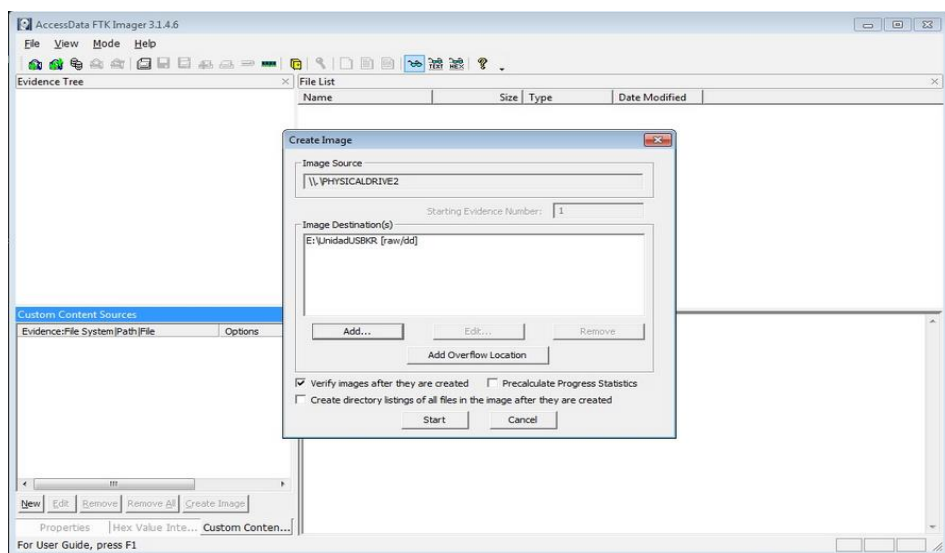


Figura 6.14

Paso 15:

El proceso de creación de la imagen forense desde la unidad USB o Memory Stick iniciará al hacer clic en el botón “Start” o Iniciar (Ver figura 6.15).

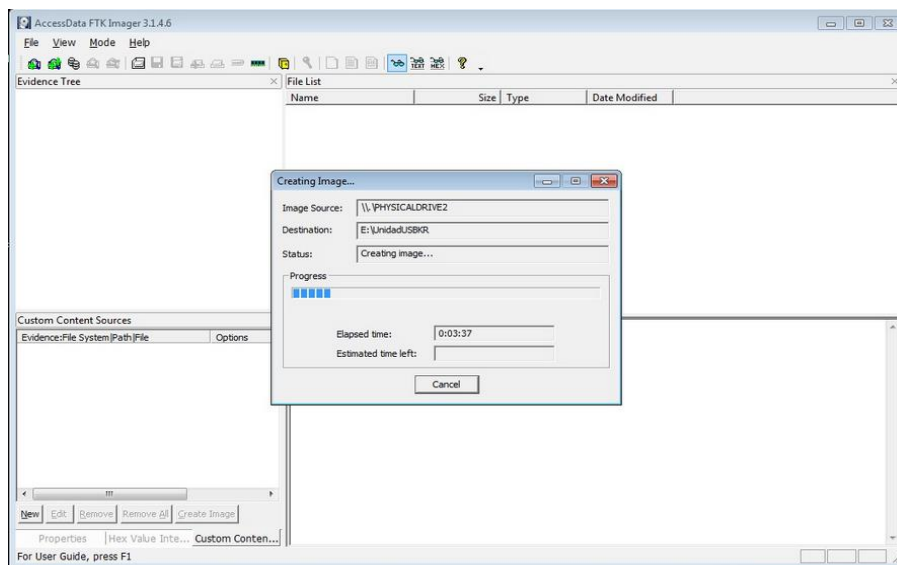


Figura 6.15

Paso 16:

Finalizada la creación de la imagen forense, inicia la verificación de la imagen creada (Ver figura 6.16).

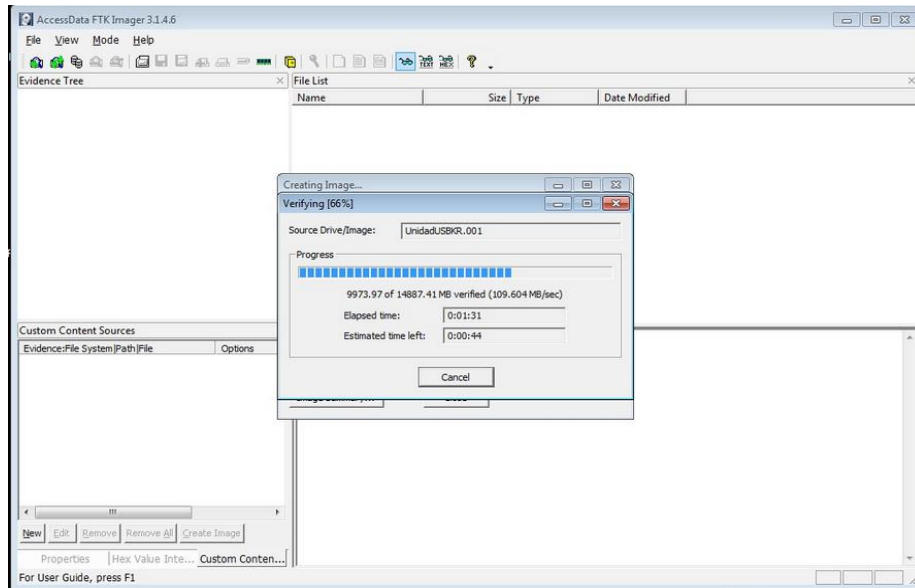


Figura 6.16

Paso 17:

Al finalizar todo este procedimiento se presentan algunos resultados finales. Los resultados muestran el número de sectores copiados. Anotar también que no se han detectado sectores Malos (Ver figura 6.17).

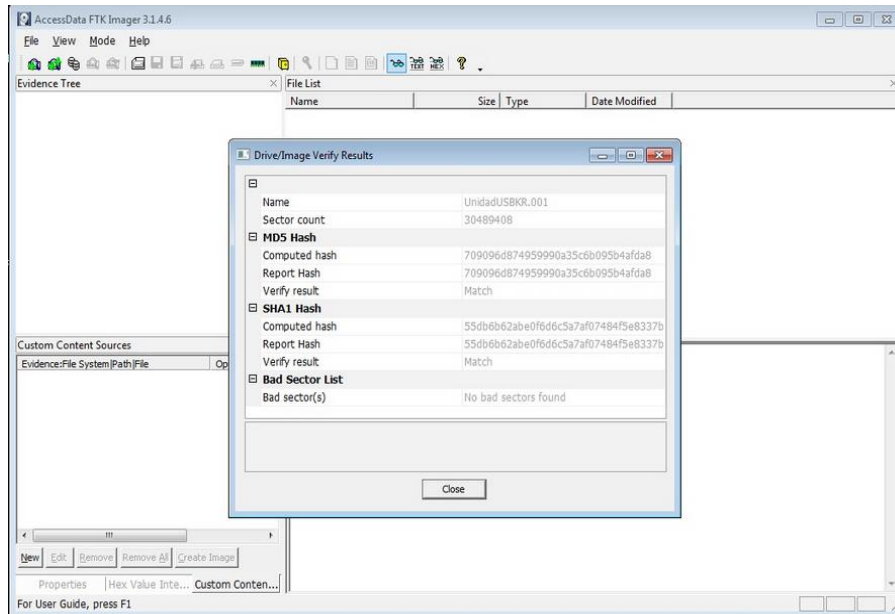


Figura 6.17

Paso 18:

En el mismo directorio o unidad donde se ha creado la imagen Forense, se encontrará un archivo de texto con el mismo nombre de la imagen Forense creada (UnidadUSBKR.txt), en el cual reside toda la información detallada del proceso realizado (Ver figura 6.18).

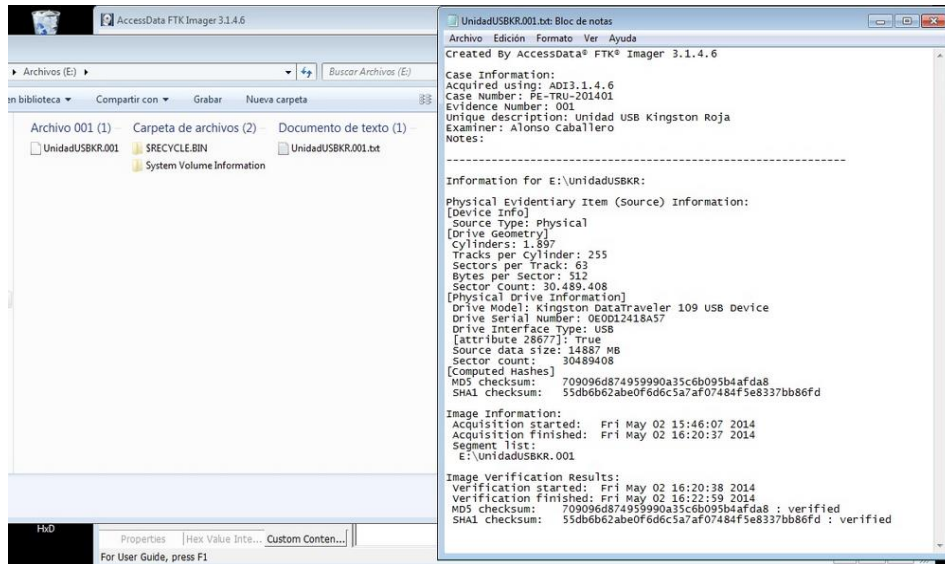


Figura 6.18

Clonezilla

Este programa se encarga de la clonación y copia de seguridad de disco permitiendo que los usuarios clonen una máquina individual, partición o disco para ser reproducido en otro medio. La clonación puede ser guardada como un archivo de imagen o como una copia exacta de datos.

Instalación del programa clonezilla

Para poder utilizar el programa es necesario insertar el disco y reiniciar la computadora en el modo BOOT para esto es necesario presionar la tecla correspondiente según el modelo de la computadora.

Paso: 1

Esperar que cargue el CD hasta que aparezca la siguiente imagen (Ver figura 7.1)

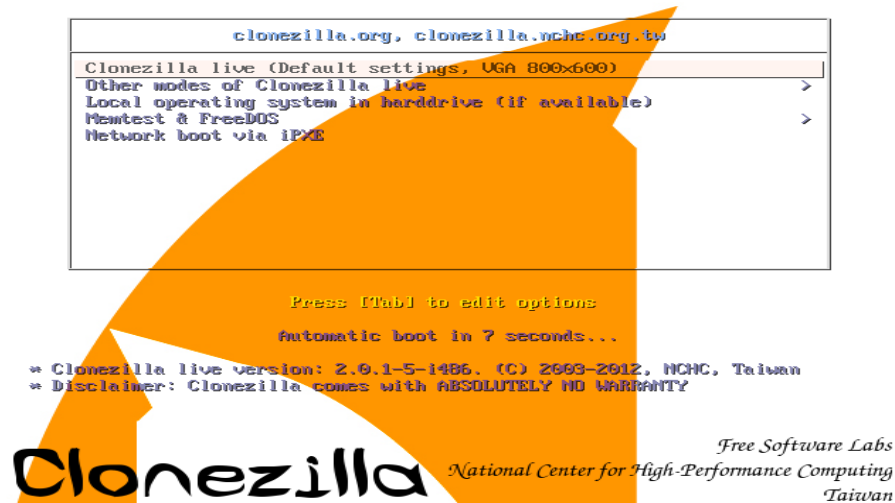


Figura 7.1

Paso: 2

En esta imagen muestra las opciones de idioma la cual se selecciona “es_ES.UTF-8 Spanish/Español” y presionamos “ENTER” (Ver figura 7.2).

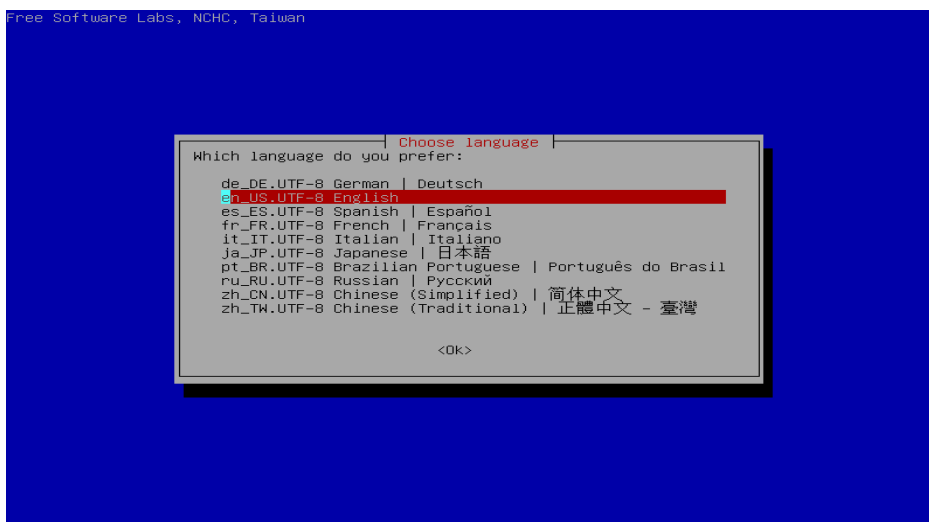


Figura 7.2

Paso: 3

En esta imagen mostrara los tipos de mapa de teclado según arquitectura la cual se selecciona “Elegir el mapa de teclado según arquitectura” y clic en “ENTER” (Ver figura 7.3).

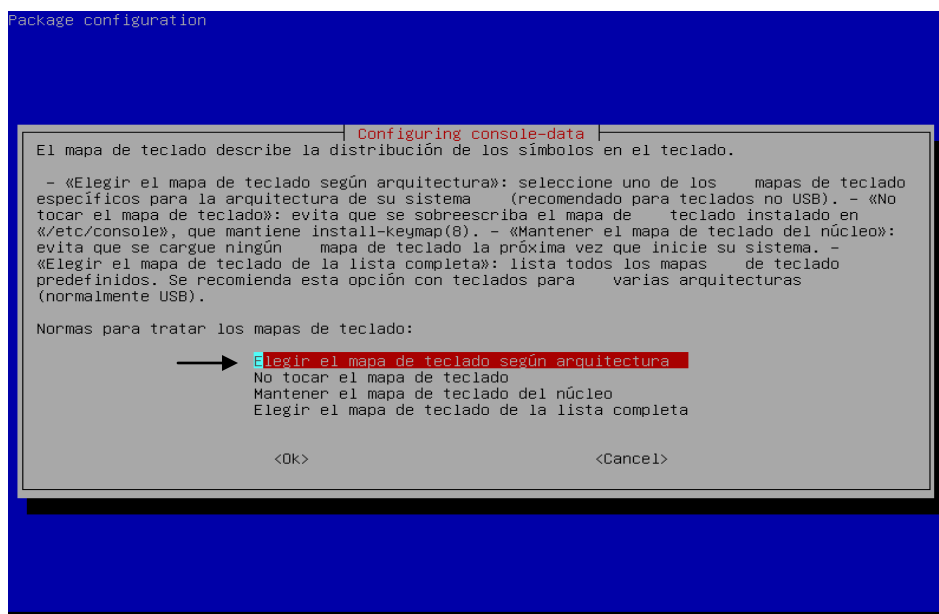


Figura 7.3

Paso: 4

En esta imagen muestra la distribución de teclado la cual se selecciona “qwerty” y clic en “ENTER” para continuar (Ver figura 7.4).

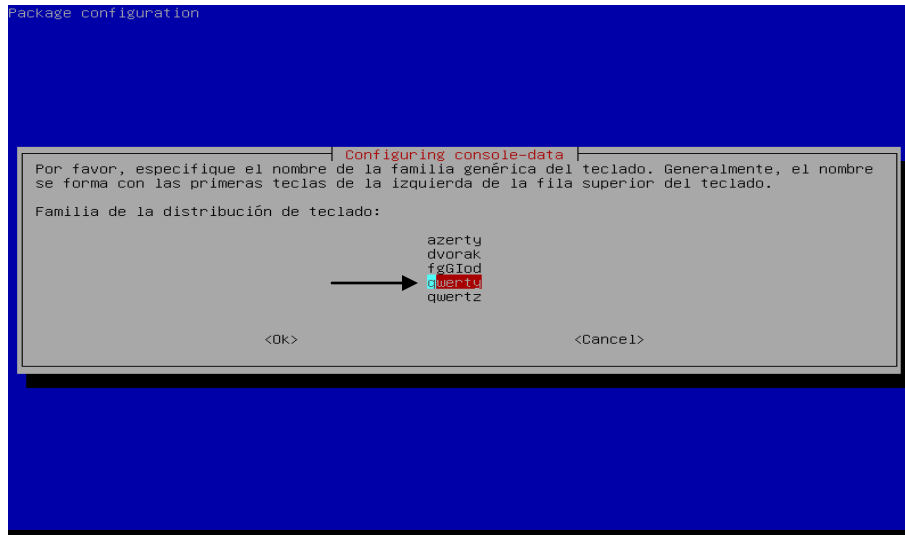


Figura 7.4

Paso: 5

En esta imagen muestra la distribución física del teclado y se selecciona la opción “Latin American” y clic en “ENTER” (Ver figura 7.5).

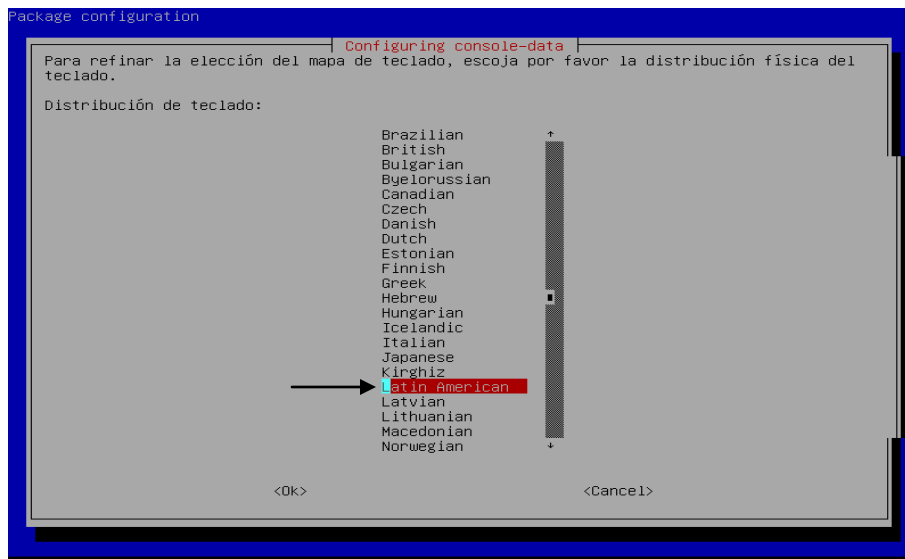


Figura 7.5

Paso: 6

En esta imagen se inicia clonezilla y se elige una línea de comando la cual se seleccionamos la primera opción (Ver figura 7.6).

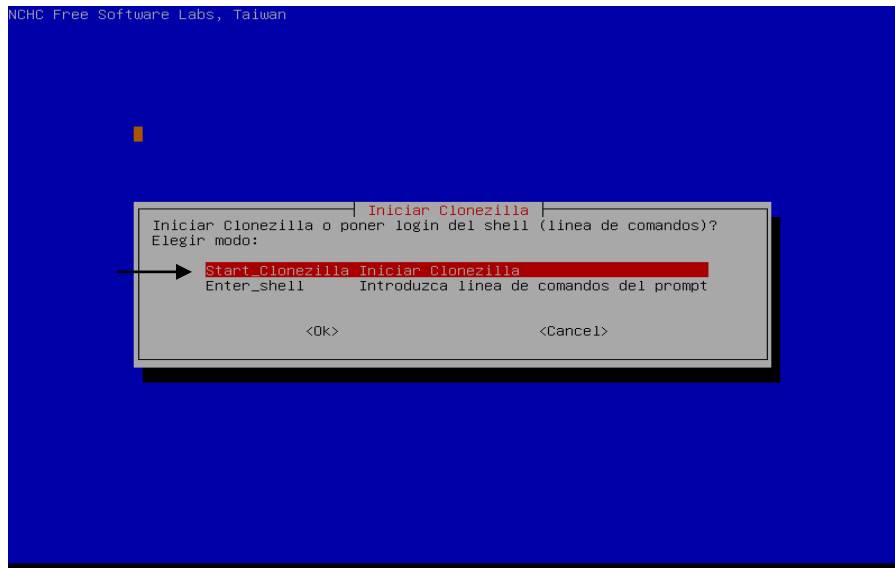


Figura 7.6

Paso: 7

En esta pantalla muestra dos opciones la cual se selecciona la segunda opción que es disco a disco o partición a partición clonada y clic en “ENTER” (Ver figura 7.7)

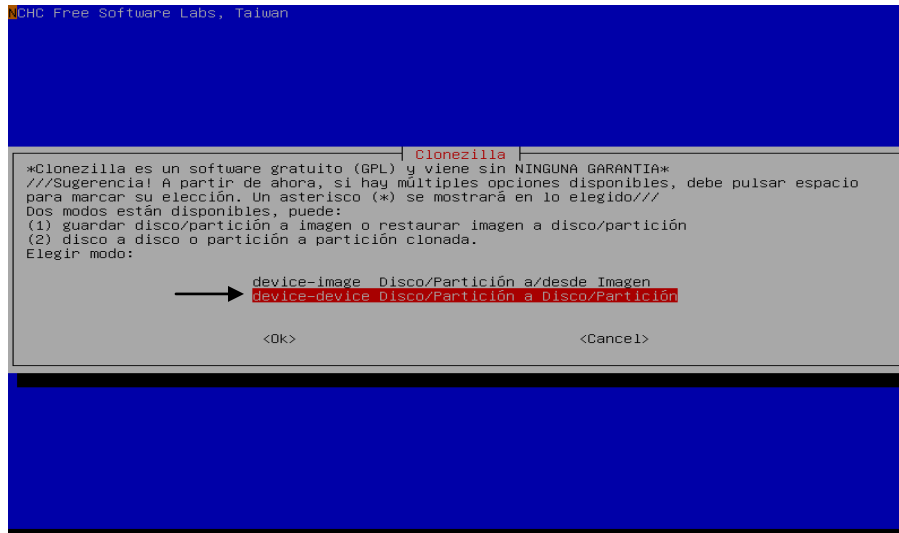


Figura 7.7

Paso: 8

En esta imagen se selecciona el modo de ejecución para el asistente, pero muestra dos opciones la cual se elige la primera y clic en "ENTER"(Ver figura 7.8).

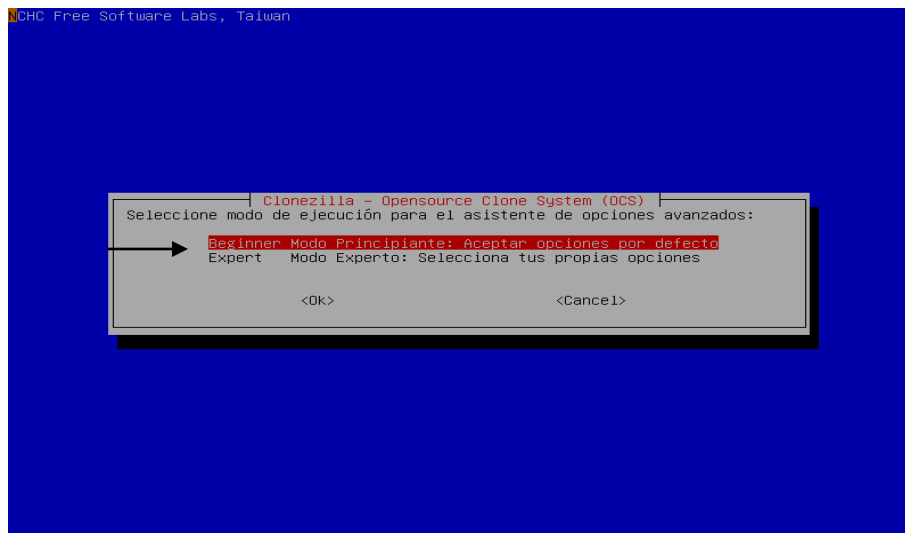


Figura 7.8

Paso: 9

En esta imagen muestra cuatro opciones, se selecciona la opción “disk to local disk” y clic en “ENTER” (Ver figura 7.9).

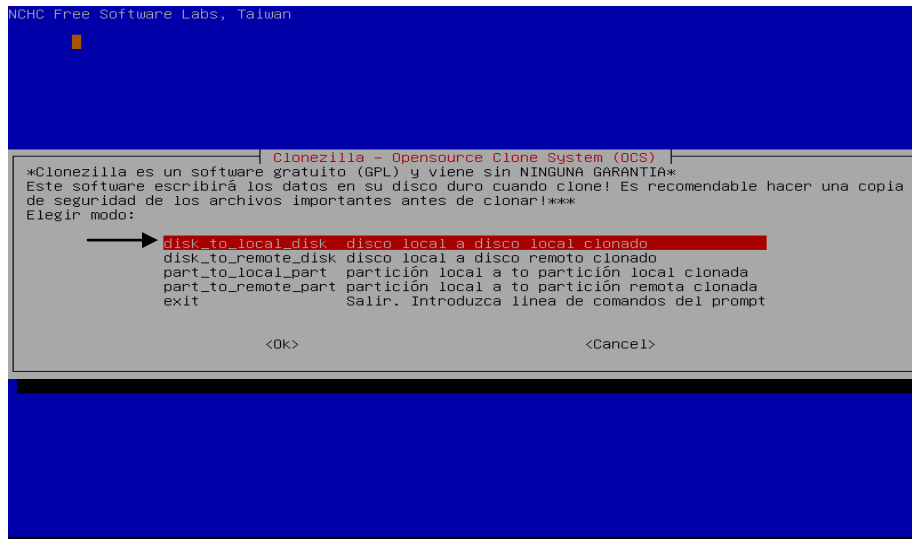


Figura 7.9

Paso: 10

En esta imagen se tiene que seleccionar el disco local como origen pero hay dos opciones la cual se elige la primera y clic en “ENTER” para continuar (Ver figura 7.10).

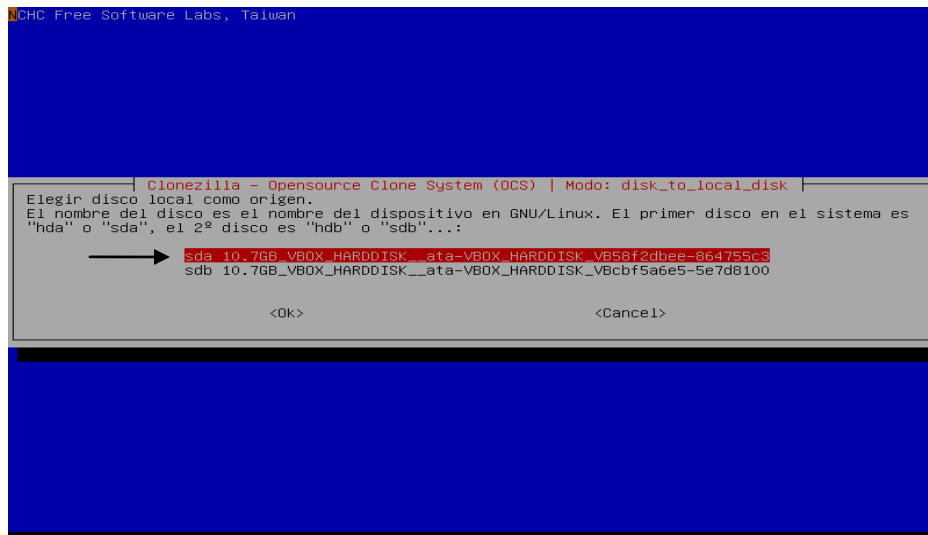


Figura 7.10

Paso: 11

En esta imagen se tiene que elegir el disco local como destino y clic en “ENTER” para continuar (Ver figura 7.11).

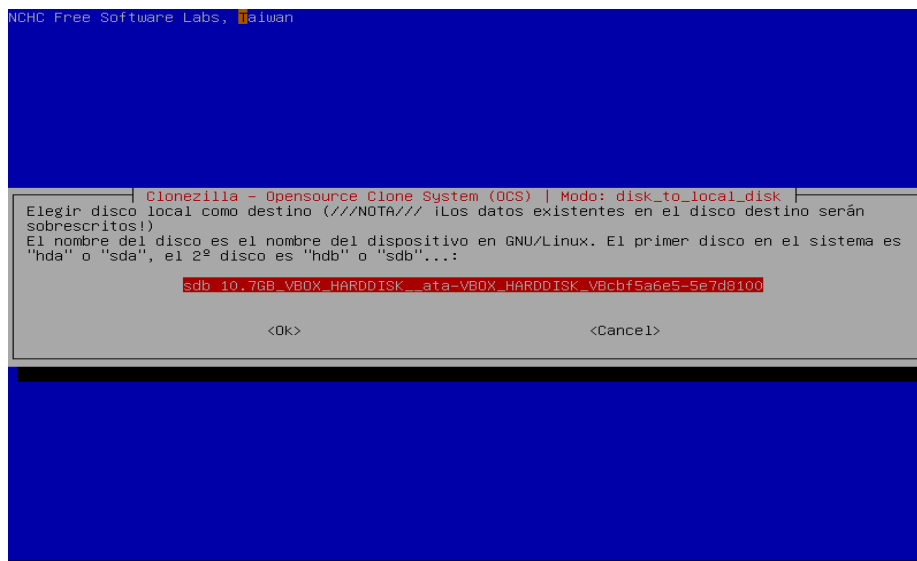


Figura 7.11

Paso: 12

En esta imagen muestra tres opciones, se selecciona la primera opción que es “Omitir la comprobación” y clic en “ENTER” (Ver figura 7.12).

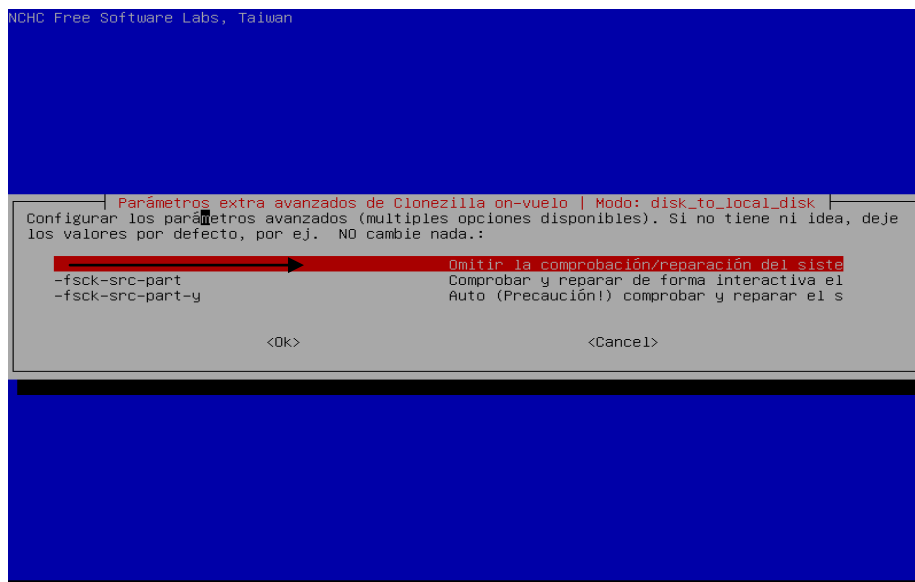


Figura 7.12

Paso: 13

En esta imagen muestra los comandos y se escribe “yes” para continuar (Ver figura 7.13)

```

dd if=/dev/sda of=/tmp/ocs_onthefly_local.104u01/src-hidden-data.img skip=1 bs=512 count=62
62+0 records in
62+0 records out
31744 bytes (32 kB) copied, 0.00100205 s, 31,7 MB/s
*****
Collecting partition /dev/sda1 info...
Non-grub boot loader found on /tmp/ocs_onthefly_local.104u01/sdb-mbr...
The CHS value of hard drive from EDD will be used for sfdisk.
[ 932.162933] BIOS EDD facility v0.16 2004-Jun-25, 2 devices found
Head and sector no. of /dev/sdb from EDD: 255, 63.
Searching for data partition(s)...
Excluding busy partition or disk...
Unmounted partitions (including extended or swap): sdb1
Collecting info.. done!
Getting /dev/sdb1 info...
*****
ATENCIÓN!!! ATENCIÓN!!! ATENCIÓN!!!
ATENCIÓN!! ¡LOS DATOS EXISTENTES EN ESTE/ESTOS DISCODOURO(S)/PARTICION(ES) SERÁN SOBRESCRITOS! TODOS L
OS DATOS SE PERDERÁN: sdb
*****
Machine: VirtualBox
sdb (10.7GB_VBOX_HARDDISK__ata-VBOX_HARDDISK_VBcbf5a6e5-5e7d8100)
sdb1 (10.7GB_ntfs(In_VBOX_HARDDISK_)_ata-VBOX_HARDDISK_VBcbf5a6e5-5e7d8100)
*****
¿Está seguro que quiere continuar? ? (y/n) yes
OK, ¡hagámoslo!!
*****
Se creará la partición en el destino...
Déje que le pregunte otra vez.
*****
Machine: VirtualBox
sdb (10.7GB_VBOX_HARDDISK__ata-VBOX_HARDDISK_VBcbf5a6e5-5e7d8100)
sdb1 (10.7GB_ntfs(In_VBOX_HARDDISK_)_ata-VBOX_HARDDISK_VBcbf5a6e5-5e7d8100)
*****
ATENCIÓN!!! ATENCIÓN!!! ATENCIÓN!!!
ATENCIÓN!! ¡LOS DATOS EXISTENTES EN ESTE/ESTOS DISCODOURO(S)/PARTICION(ES) SERÁN SOBRESCRITOS! TODOS L
OS DATOS SE PERDERÁN: sdb
*****
¿Está seguro que quiere continuar? ? (y/n)

```

Figura 7.13

Paso: 14

En esta imagen pregunta si se quiere clonar el boot se escribe “yes” para continuar (Ver figura 7.14).

```

/dev/sdb: unrecognized partition table type
Old situation:
No partitions found
New situation:
Units = sectors of 512 bytes, counting from 0

   Device Boot      Start         End      #sectors  Id System
/dev/sdb1   *          63       20948759       20948697    7 HPFS/NTFS/exFAT
/dev/sdb2                0           -             0    0 Empty
/dev/sdb3                0           -             0    0 Empty
/dev/sdb4                0           -             0    0 Empty
Successfully wrote the new partition table

Re-reading the partition table ...
[ 1052.288698] sdb: sdb1

If you created or changed a DOS partition, /dev/foo7, say, then use dd(1)
to zero the first 512 bytes: dd if=/dev/zero of=/dev/foo7 bs=512 count=1
(See fdisk(8).)
This is done by "sfdisk --force -C 1305 -H 255 -S 63 /dev/sdb < /tmp/ocs_onthefly_local.104u01/tgt_p
t.sf"
Informing the OS that partition table has changed...
[ 1052.374508] sdb: sdb1
Checking the integrity of partition table in the disk /dev/sdb...
done!
*****
The first partition of disk /dev/sdb starts at 63.
Restoring the hidden data between MBR (1st sector, i.e. 512 bytes) and 1st partition, which might be
useful for some recovery tool, by:
dd if=/tmp/ocs_onthefly_local.104u01/tgt-hidden-data.img of=/dev/sdb seek=1 bs=512 count=62
62+0 records in
62+0 records out
31744 bytes (32 kB) copied, 0.00649761 s, 4,9 MB/s
*****
*****
¿Quiere clonar el boot loader (área de código ejecutable, los primeros 446 bytes) a: sdb ?
[Y/n]

```

Figura 7.14

Paso: 15

En esta imagen comienza el clonado de datos a la máquina de destino, escribimos “yes” para continuar (Ver figura 7.15).

```
Units = sectors of 512 bytes, counting from 0

   Device Boot      Start         End      #sectors  Id System
/dev/sdb1 *            63      20948759      20948697   7  HPFS/NTFS/exFAT
/dev/sdb2                0           -             0   0  Empty
/dev/sdb3                0           -             0   0  Empty
/dev/sdb4                0           -             0   0  Empty
Successfully wrote the new partition table
Re-reading the partition table ...
[ 1052.288698]  sdb: sdb1

If you created or changed a DOS partition, /dev/foo7, say, then use dd(1)
to zero the first 512 bytes: dd if=/dev/zero of=/dev/foo7 bs=512 count=1
(See fdisk(8).)
This is done by "sfdisk --force -C 1305 -H 255 -S 63 /dev/sdb < /tmp/ocs_onthefly_local.104u01/tgt_p
t.sf"
Informing the OS that partition table has changed...
[ 1052.374508]  sdb: sdb1
Checking the integrity of partition table in the disk /dev/sdb...
done!
*****
The first partition of disk /dev/sdb starts at 63.
Restoring the hidden data between MBR (1st sector, i.e. 512 bytes) and 1st partition, which might be
useful for some recovery tool, by:
dd if=/tmp/ocs_onthefly_local.104u01/tgt-hidden-data.img of=/dev/sdb seek=1 bs=512 count=62
62+0 records in
62+0 records out
31744 bytes (32 kB) copied, 0.00649761 s, 4.9 MB/s
*****
*****
Quiere clonar el boot loader (área de código ejecutable, los primeros 446 bytes) a: sdb ?
[Y/n] yes
Cloning the boot loader (executable code area) from "sda" to "sdb"...
*****
Comienza el clonado de datos a la máquina destino...
¿Está seguro que quiere continuar? ? (y/n)
```

Figura 7.15

Paso: 16

En esta imagen muestra el porcentaje de proceso de clonación (Ver figura 7.16).

Lista de programas que formaran parte del Kit de Software de Informática Forense:

- Acronis Drive Monitor.
- HDD Regenerator Full.
- Easy Driver Recovery.
- Outpost Security Suite.
- Axcript.
- FTK Imager.
- Clonezilla.

Como se ha mostrado en la lista 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.

2.2.3 Kit de Software en DVD:

El DVD contendrá todos los programas que forman parte del Kit de Software de Informática Forense el cual va a mostrar la pantalla de inicio en la cual se selecciona el “Kit de Informática Forense” para continuar.



Figura 2.2.3.1: Página principal del Kit de Informática Forense



Figura 2.2.3.2: Menú del Kit de Informática Forense.

2.2.3 Lista de programas utilizados

Lista de programas que formaran parte del Kit de Software de Informática Forense:

- Acronis Drive Monitor.
- HHD Regenerator Full.
- Easy Driver Recovery.
- Outpost Security Suite.
- Axcrypt.
- FTK Imager.
- Clonezilla.

Como se ha mostrado en la lista 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.

2.2.4 Kit de herramienta en DVD y manual impreso

El DVD contendrá todos los programas que forman parte del Kit de Software de Informática Forense. Y el manual que contiene todos los pasos para el uso de cada programa, desde su instalación y su funcionamiento, se entregara en formato impreso.

2.3 MARCO TEÓRICO CONCEPTUAL

Archivos:

Un archivo o fichero informático es un conjunto de bits que son almacenados en un dispositivo. Un archivo es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene. A los archivos informáticos se les llama así porque son los equivalentes digitales de los archivos escritos en libros, tarjetas, libretas, papel o microfichas del entorno de oficina tradicional.

Criptografía:

La criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura.

Hacker:

Un hacker es alguien que descubre las debilidades de una computadora o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas. Los hackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta o por el desafío. La subcultura que se ha desarrollado en torno a los hackers a menudo se refiere a la cultura underground de computadoras, pero ahora es una comunidad abierta.

Imagen de disco:

Una imagen de disco es un archivo o unos dispositivos que contienen la estructura y contenidos completos de un dispositivo o medio de almacenamiento de datos, como un disco duro, un disquete o un disco óptico (CD, DVD). Una imagen de disco usualmente se produce creando una copia completa, sector por sector, del medio de origen y por lo tanto replicando perfectamente la estructura y contenidos de un dispositivo de almacenamiento.

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.

Investigación forense:

La investigación forense es la aplicación de prácticas científicas dentro del proceso legal. Esencialmente esto se traduce en investigadores altamente especializados o criminalistas, que localizan evidencias que sólo proporcionan prueba concluyente al ser sometidas a pruebas en laboratorios. Parte de la evidencia que hallan a menudo no puede ser vista a simple vista, a veces es hasta más pequeña.

Malware:

El malware (del inglés malicious software), 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.

Software

Se considera que el software es el equipamiento lógico e intangible de un ordenador. En otras palabras, el concepto de software abarca a todas las aplicaciones informáticas.

Recuperación de datos:

La recuperación de datos hace referencia a las técnicas empleadas para recuperar archivos que han sido perdidos o eliminados de algún medio de almacenamiento.

Unidad de disco duro:

Unidad de disco se refiere al dispositivo o aparato que realiza las operaciones de lectura y escritura de los medios o soportes de almacenamiento con forma de disco, más específicamente a las unidades de disco duro, unidades de discos flexibles (disquetes de 5¼" y de 3½"), unidades de discos ópticos (CD, DVD, HD DVD o Blu-ray) o unidades de discos magneto-ópticos (discos Zip, discos Jaz, SuperDisk).

2.4 DOCUMENTACIÓN TÉCNICA

Acronis Drive Monitor

Es una aplicación de Software diseñado específicamente para ayudar a identificar los problemas de disco duros con tiempo suficiente para proteger la PC y servidores frente a desastres.

Esta aplicación monitoriza el estado del disco duro de servidores, PC y portátiles y advierte a los usuarios de los problemas que puedan significar un fallo inminente en el sistema con el propósito de que se puedan guardar los datos almacenados en el disco duro y preparar su sustitución.

Una vez que Acronis Drive Monitor ha identificado un problema, se genera una notificación ya sea por correo electrónico o mediante una alerta en la pantalla, describiendo los detalles del síntoma descubierto. Adicionalmente, brinda una explicación del problema y aparte de ofrecerle al usuario una guía completa de los pasos que debe llevar a cabo para resolver la incidencia en cuestión. Un informe codificado por colores, proporciona una vista rápida del estado del disco y se genera un reporte semanal de los problemas identificados en nuestros discos duros.

Datos de Acronis Drive Monitor

- Autor: Acronis
- Licencia: Gratuita
- Tamaño: 18.0 MB
- Idioma: Ingles

Requisitos del Sistema.

- Sistemas operativos: Windows vista, Windows 7.
- Procesador: 2.4 GHz Pentium.
- Memoria: 1 GB de RAM.

Características principales de Acronis Drive Monitor.

- Monitorizar el disco duro.
- Avisará el estado de salud en tiempo real del disco duro.
- Informes sobre el estado de salud del disco duro.
- Interfaz simple e intuitiva.
- Soporte de instalación y desinstalación.
- Análisis: SMART.
- Monitorea la temperatura del disco.

HDD Regenerator:

Solamente HDDR puede verdaderamente recuperar tus datos perdidos y reparar sectores defectuosos. Aquí hay solo algunas de las prestaciones claves del HDD Regenerator: Explora los sectores defectuosos para darte una idea de la extensión del daño antes de reparar.

Intuitivo, interfaz amigable.

Configuraciones no complejas con las que no perder tiempo.

Puede ejecutarse como un proceso para automatizar operaciones de exploración y recuperación.

Bootable: puedes bootear el HDDR directamente, a fin de reparar discos que no puede realizar del todo su carga inicial.

Hardware independiente: puede reparar cualquier hardware de disco duro.

¿Cuándo debo usarlo?

No es necesario esperar por los sectores defectuosos o fallos del disco. Si trabajas con información sensible, debes ejecutar el HDDR periódicamente. Esto puede ahorrar mucho tiempo y el empeoramiento a largo plazo.

Detecta los sectores defectuosos: El HDDR analizará tu disco duro para encontrar los sectores defectuosos, dándote una idea de la extensión del problema antes de la reparación. Esto te ahorrará tiempo, si tienes una gran cantidad de sectores defectuosos y decides empezar con un nuevo disco.

Repara los sectores defectuosos: Si se encuentran sectores defectuosos, el HDDR recuperará tus datos importantes y hará los arreglos necesarios.

Interfaz Intuitiva: ¿De qué sirve cualquier pieza de software si es imposible usarla? El HDDR representa una interfaz gráfica amigable al usuario, que es un paseo para navegar. No necesitas ser un obseso informático para reparar tu propio disco duro en casa, usando el HDD Regenerator.

Ejecutar como un proceso: Si no quieres preocuparte por tener que recordar ejecutar las exploraciones del disco manualmente, el HDDR puede ser integrado para ejecutarse como un proceso startup, en Windows XP, Vista y Windows 7/8. Esto no es solo por

conveniencia, el ejecutarse como un proceso startup ofrece una cobertura de protección y seguridad adicional contra los problemas del disco duro.

Easy Drive Data Recovery

Easy Drive Data Recovery es un producto de Software destinado a la recuperación de datos de archivos eliminados o perdidos de otra manera que no han sido dañados. La pérdida de datos puede estar causada por el formateo de discos duros, la reinstalación del sistema o por daños en las unidades de memoria USB. En cualquiera de estos casos Easy Drive Data Recovery puede proporcionar una de las mejores soluciones de recuperación de datos del mercado. Incorpora un algoritmo especial, llamado Raw Search, que permite buscar casi 100 tipos de archivos y el programa funciona con todos los tipos de dispositivos de almacenamiento, siempre que se reconozcan.

Posee una interfaz intuitiva y comprensible, así como un Asistente de recuperación que guía al usuario a través de todo el proceso de recuperación. Incluso para alguien que no tenga demasiados conocimientos de informática y que tiene que preguntar: ¿Qué es la recuperación de datos?, no le resultará complicado utilizar el programa, ya que todo aparece escrito en la pantalla. Lo único que hay que hacer es elegir las unidades que desea analizar y luego especificar la ruta donde almacenar los archivos recuperados.

Si el disco duro ha sido formateado o se ha reinstalado el sistema operativo, no está todo perdido, como puede parecer. Incluso desde discos formateados, incluso en lugares donde no parece quedar nada que conseguir, la recuperación de datos es posible. Si la

información del archivo ya no está en el sistema de archivos, existe la posibilidad de que los datos se puedan recuperar. El programa recupera la máxima cantidad de datos posible y funciona con sistemas de archivos como FAT16, FAT32 y NTFS. Esto significa que también funciona con unidades de memoria USB y tarjetas de memoria. El programa es capaz de recuperar datos de dispositivo de almacenamiento dañados (siempre y cuando los reconozca) y la cantidad de datos recuperables se puede determinar consultando la vista previa que muestra los archivos y su contenido. El programa se puede descargar de forma gratuita, como versión de prueba, de modo que el usuario pueda comprobar con antelación si los archivos pueden recuperarse.

Datos de Easy Driver Recovery

- Autor: MunSoft
- Licencia de pago
- Tamaño: 7.8 MB
- Idioma: Español

Requisitos del Sistema.

- Sistemas operativos: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 o Windows 7.
- Memoria: 1 GB de RAM.
- 7 megabytes del espacio libre en el disco duro.

Características principales

- Es posible filtrar por nombre de archivo, fecha, tamaño o estado de recuperación.
- Los archivos y carpetas temporales se pueden excluir de la búsqueda.
- Compatible con flujos de datos nombrados y archivos comprimidos NTFS.
- Recuperación de archivos tras la reinstalación del sistema operativo.
- Motor de búsqueda optimizado, un 40% más rápido.
- Compatible con sistemas de archivos NTFS y FAT.
- Admite todos los tipos de unidades de disco duro.
- Es capaz de recuperar archivos de DOS eliminados.
- Sin restricciones de tamaño del disco duro.

Outpost Security Suite Pro

Outpost Security Suite Pro combina la mejor protección proactiva, en un producto integrado que incluye: antivirus + anti espía + cortafuegos + antispam, logrando la sólida protección que los usuarios de Internet necesitan actualmente, para una navegación sin riesgos.

Hoy en día, es necesario proteger la información contra las fallas de seguridad graves, que ocurren cuando un programa malicioso se transporta sobre una aplicación legítima, o utiliza sus permisos o credenciales para realizar actividades delictivas: robar claves o

datos personales, enviar correo no deseado, apoderarse del contenido de monederos electrónicos, aprovechar vulnerabilidades para implantar código malicioso, etcétera.

Outpost Security Suite incluye dos herramientas específicamente diseñadas para prevenir este tipo de comportamientos ilegítimos.

El Protector de aplicaciones aprende cuáles son los programas habilitados para Internet que se inician normalmente en el ordenador: navegadores, mensajeros instantáneos, juegos en línea, etcétera. Para llevar a cabo este aprendizaje, el Protector de aplicaciones se basa sobre los datos estadísticos recogidos por ImproveNet. Outpost protegerá automáticamente dichos programas, para que no compartan sus recursos inadvertidamente, o sean manipulados por código malicioso.

De esta forma, los elementos más importantes de estas aplicaciones, tales como cookies, historiales de navegación, contraseñas de acceso guardadas en la memoria, y otros datos personales que podrían ser utilizados ilegítimamente, estarán aseguradas contra el acceso inapropiado.

También es posible agregar exclusiones personalizadas para permitir que ciertos programas puedan leer los contenidos protegidos, y así realizar sus operaciones normales.

El Protector del sistema complementa el módulo de Protección proactiva. Este componente, permite definir una lista de programas y archivos de configuración que serán específicamente protegidos en el sistema. En la lista, se pueden incluir

configuraciones del registro, propiedades de la red, accesibilidad a los archivos del equipo, interacciones con los complementos de Flash y Acrobat Reader, entre otros objetos vulnerables a ataques cibernéticos. De esta forma, el Protector del sistema crea un blindaje especial para los archivos especificados, evitando que sean manipulados o utilizados de forma ilegítima.

Junto con el Protector de aplicaciones, estos dos componentes del módulo de Protección proactiva, refuerzan aún más la seguridad e integridad de los archivos de sistema y de los programas. Asimismo, proporcionan herramientas avanzadas para controlar la forma en que interaccionan las aplicaciones y los permisos para compartir sus recursos.

Requisitos de sistema para Outpost Security Suite Pro

Sistema operativo

- Windows 2000 SP3 o superior.
- Windows XP (32-bits y 64-bits).
- Windows Server 2003 (32-bits y 64-bits).
- Windows Server 2008 (32-bits y 64-bits).
- Windows Vista (32-bits y 64-bits).
- Windows 7 (32-bits y 64-bits).

Procesador

- Pentium 450 MHz o superior (x-86 / x-64 / multinúcleo).

Espacio libre en disco duro

- 400 MB.

Memoria RAM

- 256 MB.

Soporte antispam para los siguientes clientes de correo

- The Bat!
- Windows Mail.
- Microsoft Outlook Express.
- Microsoft Outlook 2000, 2002, 2003 y 2007.

AxCrypt 1.7

AxCrypt es un software de seguridad que permite proteger la confidencialidad de tus ficheros codificándolos fácil y cómodamente.

Para codificar un fichero sólo tienes que hacer clic con el botón derecho e introducir una contraseña. También podrás elegir un archivo llave, en este caso será necesario para poder decodificar el fichero original.

Descodificar un fichero es igual de fácil: simplemente haz doble clic sobre el archivo codificado e introduce la contraseña.

Gracias a AxCrypt, y a su codificación de 128 bits, puedes tener documentos totalmente protegidos en tu PC, incluso si lo compartes con otras personas. También es útil para enviar ficheros por correo electrónico con la seguridad de que sólo la persona receptora (si conoce la contraseña) podrá visualizarlos.

Esta aplicación podrás tener tus archivos encriptados, a los que solo tú solo podrás tener acceso, ya que estarás obligado a ingresar a través de una contraseña. Sin esta contraseña los datos que se encuentren en el interior no son accesibles de ninguna forma. Además, la carpeta encriptada no puede ser movida, renombrada, borrada o modificada de modo alguno.

Datos de AxCrypt.

- Autor: Axantum Software
- Licencia: Gratita
- Tamaño: 3.2 MB
- Idioma: Español

Requisitos del sistema.

- Sistemas operativos: Windows XP, Windows 7 y 8, Windows vista.
- Procesador: 1 GHz o mas.

- Mínimo 512 MB de RAM. A mayor memoria RAM disponible.

Características principales de AxCrypt.

- Protección de archivos sin límite de cantidad.
- Integración con el explorador de Windows.
- Posibilidad de abrir, editar y guardar archivos desde el explorar con doble clic.
- Sin necesidad de realizar configuración. Solo instalar y funcionar.
- Cifrado de todos los archivos enviados por Internet, por ejemplo, correo electrónico
- Multilenguaje.

FTK Imager

Es una herramienta para realizar réplicas y visualización previa de datos, la cual permite una evaluación rápida de evidencia electrónica para determinar si se garantiza un análisis posterior con una herramienta forense como Access Data Forensic Toolkit. FTK Imager también puede crear copias perfectas (imágenes forenses) de datos de computadora sin realizar cambios en la evidencia original.

Es importante mencionar el uso de un bloqueador de escritura al utilizar FTK Imager para crear la imagen forense desde un disco duro u otro dispositivo electrónico. Esto

asegura que el sistema operativo no alterará la unidad fuente original cuando se le adjunte a la computadora.

Para prevenir la manipulación accidental o intencional de la evidencia original, FTK Imager realizar una imagen duplicado bit a bit del medio. La imagen forense es idéntica en cualquier forma al original, incluyendo espacio de holgura o residual y espacio sin asignar o espacio libre de la unidad. Esto permite almacenar el medio original en un lugar seguro de daño mientras se procede con la investigación utilizando la imagen forense.

Datos de FTK Imager

- Autor: Access Data
- Licencia: Gratuita
- Tamaño: 30 MB
- Idioma: Ingles

Requisitos del sistema.

- Sistema operativos: Windows vista, Windows 7 y 8
- Procesador: 2.4 GHz Pentium
- Memoria: 1 GB de RAM

Características principales de FTK Imager

- Crea imágenes de discos duros, discos Zip, CD-ROM, DVD-ROM, carpetas o ficheros individuales.
- Vista previa de los ficheros y carpetas en discos duros, , discos Zip, CD-ROM y DVD-ROM.
- Monta la imagen para visualizar el contenido de la imagen exactamente como el usuario con la unidad original.
- Exportar ficheros y carpetas de imágenes de disco.
- Ver y recuperar ficheros que se han borrado desde la papelera de reciclaje, pero que aún no se han sobre escrito en la unidad.
- Crear hashes de ficheros mediante dos funciones: MD5 y SHA-1.
- Generar informes de hashes para fichero y para imágenes de disco para comprobar la integridad de los contenidos. El hash es la prueba de que los ficheros no se han alterado ni modificado en ningún caso.

Clonezilla

Es una aplicación de software que sirve para la clonación y copia de seguridad de disco duro. El CD de arranque puede ayudar a sus discos o particiones de seguridad y de fácil reubicación.

Hace una imagen ISO y la guarda en una partición en el disco o CD de arranque. La aplicación es compatible con formatos de archivos de sistema ext2, ext3, XFS, JFS y LVM2, y hace copias de los bloques de disco, que mejora la velocidad y el rendimiento de la clonación. Para los administradores de red, el modo de multidifusión puede ser muy útil para respaldar y restaurar un conjunto de equipos.

El programa en el momento de realizar la copia o clon, solo se basa en los bloques de datos utilizados, de esta manera aumenta el rendimiento, ya que ignorará los sectores o particiones de disco que se encuentren vacíos o sin datos.

Datos de Clonezilla

- Autor: NCHC Labs
- Licencia: Gratuita
- Tamaño:
- Idioma: Español

Requisitos del sistema.

- Sistemas operativos: Windows, Linux, Mac.
- Procesador: 2.4 GHz Pentium.
- Memoria: 1 GB de RAM.

Características principales de Clonezilla.

- Los sistemas de archivos de los discos a clonar pueden ser cualquiera de los siguientes : ext2, ext3, reiserfs, xfs, jfs de GNU/Linux, FAT, NTFS de Microsoft Windows, y HFS+ de Mac OS (actualmente en fase de pruebas)
- Soporte Multicast mediante Clonezilla SE, adecuado para clonar masivamente varios ordenadores.
- Mediante el uso de otro software libre Drbl-winroll, también desarrollado por el autor de Clonezilla, el nombre del host, del grupo y SID, puede ser cambiado automáticamente al clonar.

Capítulo III Desarrollo de la solución

3.1 Propuesta de la solución

El proyecto consiste en la elaboración de un Kit de Software de Informática Forense, el que tendrá los programas necesarios los cuales tienen funciones diferentes y se aplican a cada área básica de la Informática Forense, ya que estos programas juntos son un Kit de la Informática Forense los cuales ayudaran a resolver distintos problemas relacionados con la Informática Forense, y que se presentan muchas veces en las computadoras de los laboratorios de Informática de la Universidad Tecnológica de El Salvador.

El proyecto se hizo utilizando un conjunto de Software de Informática Forense, como herramienta de apoyo didáctico para los laboratorios de informática, los cuales se buscaron y se descargaron para hacer usos de ellos y sus funcionalidades, pero también una de las principales ventajas en la elaboración de este Kit de Software de Informática Forense, es que todos los programas puedan ser accesibles al usuario y de fácil utilización para dichos usuarios que deseen realizar prácticas.

Como primer punto se realizó la investigación de Software de Informática Forense; buscando las áreas donde se desarrolla de las cuales se escogieron las siguientes: diagnósticos de discos duros, reparación de disco duros, recuperación de información, seguridad informática y criptografía por cada área se seleccionó tres programas donde

Se comparó cada uno de ellos y se eligió uno de cada área por sus funciones y características, una vez elegido se descargaron los programas que sirven para la Informática Forense.

Los programas de Informática Forense se copian en un DVD, de manera que los usuarios puedan instalarlos desde aquí en cualquier computadora, pero algo importante todos los programas que se ocupan son específicamente para el sistema operativo Windows ya que este sistema es el que se utiliza en las computadoras del laboratorios de informática de la Universidad Tecnológica de El Salvador

El funcionamiento del proyecto se basa en resolver los problemas de cada área básica de la Informática Forense, es ahí donde se utilizará el Kit de Software de Informática Forense como un apoyo didáctico que contengan la teoría necesaria, este Kit estará disponible en los laboratorios de informática de la Universidad Tecnológica de El Salvador, así que cuando los estudiantes realicen prácticas sobre Informática Forense contarán con el equipo necesario proporcionado para poder utilizar cada programa que contiene el Kit de Software de Informática Forense.

La realización de este proyecto de Informática Forense, está dirigido a la Universidad Tecnológica de El Salvador, para que se tome en cuenta en la enseñanza en la Universidad y también para que los estudiantes practiquen para que obtengan un mejor conocimiento sobre la Informática Forense como su aplicación, su uso y utilización de

programas que ayuden prevenir problemas de Hardware y Software en las computadoras del laboratorio de Informática.

El proyecto se diseñó pensando en las aquellas necesidades que existen el laboratorios de Informática de la Universidad Tecnológica de El Salvador, por eso se determinó que para el problema antes mencionado se necesitara de un DVD en cual tendrá los programas necesarios para resolver los problemas antes mencionado.

Para el diseño del proyecto fue necesario realizar un proceso en el cual se debe tomar en cuenta muchos factores importantes como lo que es la situación problemática que se resolverá, crear la propuesta de solución en base al análisis, fijar los alcances y delimitaciones que llevara el proyecto, fijar los objetivos que se pretenden realizar, y desarrollar los productos que serán la solución del problema.

Además del producto principal que es el Kit de Software de Informática Forense, y también se cuenta con un manual impreso que se desarrolló primero investigando programas de cada área, esto lo llevo a comparar varios programas por ejemplo sus funciones, sus características, sus ventajas y desventajas, etc. El manual estará compuesto de los pasos de la instalación y del funcionamiento de cada uno de los programas informáticos que se van a ocupar para solucionar los problemas de Hardware y Software que se mencionan anteriormente en el documento, el manual se ha desarrollado de manera específica explicando paso a paso de cómo se instalara y de

cómo se utiliza cada programa, además se incluyen imágenes de los programas durante el proceso de instalación y su uso de cada uno de ellos.

El desarrollo del manual consistió en hacer uso de cada programa a la vez que se recopilaban todos los pasos con sus respectivas imágenes para luego insertarlos de forma ordenada en un documento en el cual se unieron de igual forma los demás programas y fue así como se elaboró el manual.

A cada uno de los programas que forman el Kit de Software de Informática Forense, se les realizó evaluaciones económicas y técnicas:

El proceso de evaluación económica se realiza de la misma manera para todos los programas 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 reflejado en un cuadro donde se colocó el nombre del producto, el precio y una comparación con otros programas similares que tienen la misma función y perteneciente a la misma área de la Informática Forense.

Después se realiza la evaluación técnica de cada uno de los programas, lo cual se desarrolla en investigar por lo menos las características técnicas básicas que debe tener cada uno de los programas y estas se asignan de acuerdo a su funcionamiento y porcentajes para que así se determine si es aprobado o reprobado.

Se debe tomar en cuenta que cada uno de los programas tienen sus ventajas y desventajas, pero todos han pasado en un proceso de evaluación tanto económicas y

técnicas en el cual fueron seleccionado para cubrir las áreas de la Informática Forense que se investigaron durante el desarrollo del marco teórico de referencia el cual contiene toda la teoría necesaria, esto ha sido la base del desarrollo e implementación de cada uno de los programas.

La propuesta de la solución se resume tomando en cuenta cada uno de los productos que se están ofreciendo como respuesta a la problemática planteada, los cuales ya fueron descritos detalladamente sabiendo la función de cada uno de ellos y de cómo sirven de complemento el uno con el otro para tener una mejor evaluación al momento que se quiera evaluar de cualquier manera tomando en cuenta que lo que se evalúa son los recursos que se utilizan en cada producto por ejemplo: recursos didácticos, tecnológicos, económico, técnicos, etc.

3.2 Conclusiones

En el desarrollo de este proyecto denominado: Elaboración de un Kit de Software de Informática Forense para resolver aquellos problemas de Hardware y Software como por ejemplo el daño de un sector en el disco duro, pérdida de información y daño en el sistema operativo debido a malware, en los laboratorios de Informática de la Universidad Tecnológica de El Salvador para beneficios de los estudiantes de la Facultad de Informática y Ciencias Aplicadas de la Universidad Tecnológica de El Salvador, el cual se ha podido incluir como material de apoyo didáctico este Kit de Software para demostrar que los programas contenidos aquí pueden resolver los posibles

problemas de Hardware y Software que muchas veces se presentan en la computadoras de los laboratorios de Informática.

Además de esto los estudiantes que realicen prácticas de Informática Forense por ejemplo: prácticas de reparar un sector en el disco duro, prácticas de recuperación de información entre otras, podrán fortalecer sus conocimientos, tanto teóricamente, como en la práctica conociendo programas útiles y fáciles de utilizar que ayuden a resolver problemas de Hardware y Software mencionados anteriormente que se presentan en las computadoras, además el estudiante podrá contar con el equipo informático necesario para facilitar el uso de cada uno de los programas que están presentados.

La experiencia adquirida en el desarrollo de este proyecto, durante la elaboración de los tres productos ha demostrado la importancia que tiene la Informática Forense en el campo de la misma Informática, como un área que se desarrolla utilizando el Software como una herramienta digital para poder resolver los problemas que puedan afectar los sistemas de información tanto de Hardware y Software que existen en las computadoras de los laboratorios de Informática.

En la actualidad la tecnología tiene un gran avance, así mismo los delitos informáticos aumentan, por lo que la Informática Forense es una disciplina que debe renovarse constantemente para estar a la vanguardia ante un nuevo delito informático.

3.3 Recomendaciones

- Los programas se deben usar correctamente como esta en el manual ya que su uso correcto ayudara a resolver errores de Hardware y Software en las computadoras de los laboratorios de Informática.
- Los programas contienen su serial solo para fines educativos esto quiere decir solo para su uso en los laboratorios de informática y no deben ser utilizados para fines incorrectos ya que su uso está contemplado según las leyes de delitos informáticos.
- Estudiar más a fondo la Informática Forense porque es un área muy extensa, y conocer más acerca de los delitos Informáticos e investigar el tratamiento que se le debe dar a cada uno de ellos.
- Evaluar las funciones de cada uno de los programas.
- Buscar software de otros sistemas operativos o para otras áreas de la informática forense tales como análisis de correos electrónicos y estenografía.

Referencias

- Zuccardi, G. & Gutierrez, J. D. (2006). *Informatica Forense*. Recuperado de <http://www.ninabook.com/freebook/reading/informatica-forense-giovanni-zuccardi-juan-david.html>V
- Mosquera, J. A.; Certain, A. F. & Cano, J. J. (2005). *Evidencia Digital: contexto, situacion e implicaciones*. (Trabajo de grado). Universidad de los Andes, Santiago, CL.
- Martinez, J. J. (2006). *Introduccion a la informatica forense*. ACIS.
- Haver Amaya, R. L. (2001). *Informatica Forense:generalidades, aspectos tecnicos y herramientas*. (Trabajo de grado). Universidad de Los Andes, Bogotá, CO.

Anexos

A1- Matriz De Congruencia

Matriz de congruencia		
Tema: Elaboración de un kit de software de informática forense para su uso en el área de seguridad y recuperación de informacion en beneficio de laboratorios de la Universidad Tecnológica de El Salvador.		
Enunciado del problema: ¿Sera necesario implementar un kit de software de informática forense para solucionar problemas de diferentes índole para las computadoras de la universidad		
Objetivo General: Desarrollar un kit de software de informática forense para realizar el mantenimiento correctivo y preventivo a las computadoras de los distintos laboratorios de la Universidad Tecnológica de El Salvador		
Objetivo Especifico 1: Investigar diferente software de informática forense su uso y aplicación en cuanto a mantenimiento correctivo y preventivo.	Objetivo Especifico 2: Desarrollar un kit de software de informática forense para mejorar y proteger las computadoras de los laboratorios	Objetivo Especifico 3: Crear un manual que contenga los conocimientos teóricos sobre el uso de software de informática forense

ALCANCE 1: Investigar las herramientas que se utilizan en la informática forense	ALCANCE 2: Desarrollar un kit de software de informática forense	ALCANCE 3: Conocer los pasos teóricos y prácticos de cómo utilizar el kit de herramientas digital de informática
PRODUCTO 1: Investigación de los mejores programas para aplicar en la informática forense.	PRODUCTO 2: Kit de software para informática forense en formato “DVD”	PRODUCTO 3: Manual impreso para la utilización del kit de herramientas digitales de informática forense

DOCUMENTACIÓN TÉCNICA: Acronis Drive Monitor • Autor: Acronis • Licencia: Gratuita • Tamaño: 18.0 MB • Idioma: Ingles Requisitos del Sistema. • Sistemas operativos: Windows vista, Windows 7. • Procesador: 2.4 GHz Pentium. • Memoria: 1 GB de RAM.	HDD Regenerator • Autor: Medicina Inc. • Licencia: De pago • Tamaño: 7.84 MB • Idioma: español Requisitos del sistema: • Sistemas operativos: Windows vista, Windows 7. • Procesador: 1 GHz • Memoria: 1GB de RAM
---	---

Easy Driver Data Recovery • Autor: MunSoft • Licencia de pago • Tamaño: 7.8 MB • Idioma: Español Requisitos del Sistema. • Sistemas operativos: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 o Windows 7. • Memoria: 1 GB de RAM. • 7 megabytes del espacio libre en el disco duro. AxCrypt. • Autor: Axantum Software • Licencia: Gratita • Tamaño: 3.2 MB • Idioma: Español Requisitos del sistema. • Sistemas operativos: Windows XP, Windows 7 y 8, Windows vista. • Procesador: 1 GHz o mas. • Mínimo 512 MB de RAM. A mayor memoria RAM disponible. Ftk imager • Autor: Accesdata • Licencia: Gratuita • Tamaño: 30 MB • Idioma: español Requisitos del Sistema. • Sistemas operativos: Windows vista, Windows 7. • Procesador: 2.4 GHz Pentium.	Outpost Security Suite Pro • Autor: Agnitum Ltd • Licencia de pago • Tamaño: 279 MB • Idioma: Español Requisitos del Sistema. • Sistemas operativos: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 o Windows 7. • Procesador: Pentium 450 MHz o superior • Memoria: 256 GB de RAM. • 400 megabytes del espacio libre en el disco duro. Soporte antispam para los siguientes clientes de correo • The Bat! • Windows Mail. • Microsoft Outlook Express. • Microsoft Outlook 2000, 2002, 2003 y 2007. Clonezilla • Autor: NCHC Labs • Licencia: Gratuita • Tamaño: • Idioma: Español Requisitos del sistema. • Sistemas operativos: Windows, Linux, Mac.
--	---

Memoria: 1 GB de RAM.	- Procesador: 2.4 GHz Pentium. - Memoria: 1 GB de RAM.
---	---

PROYECTO TEMÁTICO: Elaboración de un kit de software de informática forense para su uso en el área de seguridad y recuperación de información en beneficio de laboratorios de la Universidad Tecnológica de El Salvador.

DETALLE DEL PRESUPUESTO PROYECTADO:

Acronis Drive Monitor	HDD Regenerator	Easy Drive Data Recovery	Outpost Security Suite Pro	Axcrypt V1.7.2850	Ftk imager	clonezilla
\$ 0.0	\$99.99	\$15.00	\$29.95	\$0.0	\$0.0	\$0.0

OFERTA ECONOMICA:

Acronis Drive Monitor	HDD Regenerator	Easy Drive Data Recovery	Outpost Security Suite Pro	Axcrypt V1.7.2850	Ftk imager	Clonezilla
\$ 0.0	\$99.99	\$15.00	\$29.95	\$0.0	\$0.0	\$0.0