Universidad Tecnológica de El Salvador

INFORMÁTICA Y CIENCIAS APLICADAS

TÉCNICO EN INGENIERÍA DE HARDWARE

TEMA:

DESARROLLO DE UN KIT DE HERRAMIENTAS BÁSICAS DE SOFTWARE SOBRE INFORMÁTICA FORENSE COMO MATERIAL DIDÁCTICO DE APOYO EN EL ÁREA DE INFORMÁTICA EN EL INSTITUTO NACIONAL SAN LUIS.

TRABAJO DE GRADUACION PRESENTADO POR:

SANDRA CRISTINA ROBERTO ALFEREZ

KEILA BIRZAVIT RUIZ NUILA

WENDY MARISOL RUIZ ROMERO

PARA OPTAR AL GRADO DE:

TECNICO EN INGENIERIA DE HARDWARE

SAN SALVADOR, EL SALVADOR, CENTRO AMERICA.

PÁGINA DE AUTORIDADES

ING. NELSON ZÁRATE SÁNCHEZ
RECTOR

LIC. JOSÉ MODESTO VENTURA
VICERRECTOR ACADÉMICO

ING. FRANCISCO ARMANDO ZEPEDA
DECANO

JURADO EXAMINADOR

TEC. WILLIAM ENRIQUE GARCÍA
PRESIDENTE

ING. MARIO VALLE
PRIMER VOCAL

LIC. EDSON ALIRIO CERÓN
SEGUNDO VOCAL

SEPTIEMBRE, 2013

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

Acta de aprobación

Universidad Tecnológica de El Salvador

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:

Ing. Mario Alberto Valle, Lic. Edson Ceron Martínez, Tec. William Enrique García

a las 12:30p.m. del día Jueves, 27 de junio de 2013.

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

1-Sandra Cristina Roberto Alferez Carnet 28-3699-2011

2-Keila Birzavit Ruíz Nuila Carnet 28-2302-2011

3-Wendy Marisol Ruíz Romero Carnet 28-0517-2011

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:
"Desarrollo de un Kit de herramientas básicas de software sobre informática forense como material didáctico de apoyo en el área de informática en el Instituto Nacional San Luis"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE HARDWARE

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

APROBADO

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

San Salvador, 27 de junio de 2013.

F. _____
PRIMER VOCAL
Ing. Mario Alberto Valle

F. _____
SEGUNDO VOCAL
Lic. Edson Ceron Martínez

F. _____
PRESIDENTE
Tec. William Enrique García

Calle Arce No. 1020, San Salvador, El Salvador, C.A. Apdo. 1770. Teléfono: (503) 2275-8888 • Fax: (503) 2271-4764 • e-mail: infoutec@utec.edu.sv

Agradecimientos

Primeramente agradezco a mi gran Dios por su gran bondad hacia mí, al permitirme finalizar una etapa importante de mi preparación académica, a una persona muy importante y especial que siempre pide a Dios por mí, agradezco a mis padres por su apoyo incondicional en todo aspecto, haciendo todo lo posible para ayudarme, agradezco a mis hermanos y hermanas que siempre han apoyado mis decisiones y me han aconsejado a seguir adelante y no desmallar, diciéndome que El éxito en la vida consiste en seguir siempre adelante.

Agradezco a nuestro asesor Lic. Edson Cerón quien siempre estuvo con nosotras ayudándonos, aconsejándonos, motivándonos a hacer las cosas mejor, teniendo fé en nosotras, recordándonos siempre que nosotras tenemos una gran capacidad, agradezco el tiempo que se tomó para ayudarnos, lo recordaré como un excelente asesor que fue para nosotras quien siempre creyó en nosotras dándonos así una gran motivación.

Agradezco al Lic. Marvin Hernández, por su apoyo en la revisión de nuestro proyecto y por la información brindada a lo largo de la carrera y por demostrar el espíritu de servicio siempre, por ser una guía y excelente catedrático, quien nos instruyó y enseño muchas cosas importantes que nos servirán para toda la vida.

A mis amigas con los cuales tuve la oportunidad y el privilegio de realizar esta tesis, porque gracias a ellas este proyecto es posible. Por su comprensión y paciencia que nos ayudó a superar esos momentos difíciles.

A mis amigas con los cuales tuve la oportunidad de comentar algunas dudas de esta tesis, porque gracias a sus observaciones pude lograr salir de muchos problemas y además mejorar este trabajo.

Keila Birzavit Ruiz Nuila

Agradecimientos

Hace dos años y medio inicie un camino, el cual ha concluido con la aprobación de esta tesis, camino que tuvo sus momentos de alegría y tristezas cosa que no hubiese logrado sin el apoyo y ayuda de mi Dios.

A mi esposo Rubén Acosta, a mi madre Reina Alférez, que me apoyaron económicamente, y mi hermana Julia Alférez quien me cuido a mis hijos y en muchas ocasiones los cuidaba por largas jornadas, a Diego y Sophia mis hijos. Y a toda mi familia en general que siempre estuvo pendiente de mi estudio.

Así mismo a Wendy Ruiz Y Keila Ruiz, compañeras con las cuales realice esta tesis, a todos los compañeros que he tenido a lo largo de esta carrera ya que para lograr este objetivo fue muy importante el establecer buenas relaciones sociales. También a los profesores que fueron facilitadores en los conocimientos que hoy poseo.

También animo a las personas que tienen el deseo de tener un grado académico más a que se esfuercen en hacerlo porque si bien es cierto que ya con una familia establecida no es tan sencillo estudiar, pero la recompensa que se tiene al final es grande.

Y finalizo esta carta de agradecimiento con la siguiente frase:

"Aquel quien la buena obra empezó fue fiel en completarla" (carta de pablo a los filipenses 1.6)

Sandra Cristina Roberto Alférez

Agradecimientos

Todo este esfuerzo no hubiese dado frutos sin la ayuda de Dios y de personas e instituciones que han facilitado las cosas para que este trabajo llegue a un buen final. Por ello, es para mí un verdadero placer utilizar este espacio para expresarles mis agradecimientos.

Agradezco primeramente a Dios por haberme guiado a lo largo de mi carrera, por haber sido mi fortaleza en momentos de debilidad y por darme la sabiduría para terminar uno de los muchos logros que Él tiene para mi vida.

De manera especial a mi abuela Carmen Fuentes, a mis padres César y Marisol y a toda mi familia por haberme dado sus consejos en momentos de necesidad y desesperación.

También quiero agradecer a dos personas muy especiales las cuales fueron de gran ayuda en esta etapa de mi vida las cuales son el Lic. Edson Cerón y el Lic. Marvin Hernández por aceptar realizar esta tesis bajo sus direcciones. Su apoyo y confianza en mi trabajo y sus capacidades para guiar mis ideas ha sido un aporte invaluable, no solamente en el desarrollo de esta tesis, sino también en mi formación como profesional, les agradezco también el haberme facilitado siempre los medios suficientes para llevar a cabo todas las actividades propuestas durante el desarrollo de esta tesis. ¡Muchas gracias!

Quiero expresar también mi más sincero agradecimiento a mis compañeras de tesis Keila y Sandra por su apoyo, paciencia y motivación en los momentos difíciles.

A todas mis amigas les agradezco por haber creído en mí y haber hecho de toda mi etapa universitaria una experiencia que jamás olvidare.

Wendy Marisol Ruiz Romero

INDICE

CAPITULO III

DESARROLLO DE LA SOLUCIÓN

Introducción

En el Instituto Nacional San Luis, es importante apoyar el material didáctico de la materia de informática ya que los estudiantes no poseen conocimientos sobre lo que es la informática forense y algunas de las utilidades que esta posee para investigar delitos informáticos.

Los más comunes son:

- Robo de información
- Violación de la privacidad
- Hackeo de redes
- Fraude
- Espionaje
- Acoso por medio de las redes sociales
- Robar conversaciones del chat, entre otros.

Es por esto que existe la necesidad de apoyar el material didáctico de la materia de informática, por medio de la informática forense para que los estudiantes aprendan a utilizar nuevas herramientas básicas para investigar los problemas antes mencionados posteriores a un delito informático.

Con la implementación de este proyecto los alumnos obtendrán conocimientos básicos sobre una de las grandes áreas de la informática, motivándolos a especializarse en informática forense ya que según investigaciones realizadas no hay muchas

instituciones en El Salvador en donde las personas interesadas en esta rama puedan especializarse, por lo que esto genera una deficiencia de especialistas en el país.

Además no hay suficientes leyes sobre delitos informáticos, las leyes que existen se encuentran en el código penal procesal y la ley antiterrorismo las cuales mencionan los delitos y las penalizaciones que se impondrán si éstos son llevados a cabo.

Para contribuir a la falta de interés que hay en cuanto a la informática forense se ha desarrollado este proyecto para el Instituto Nacional San Luís con el fin de despertar el interés de los alumnos a seguir estudiando y a especializarse en dicha área.

La institución recibirá un kit de herramientas básicas de software sobre informática forense y un manual impreso con imágenes sobre el uso de cada aplicación para un mejor entendimiento de los maestros y estudiantes, también se entregará un CD interactivo con video-tutoriales; a este CD se le incorporará el manual en digital, todos estos productos serán utilizados en beneficio de los estudiantes como apoyo para el aprendizaje de la materia de informática.

En la factibilidad económica y técnica se han realizado investigaciones y comparaciones sobre los programas que conformarán dicho kit y se han elegido porque son fáciles de utilizar ya que su interfaz es amigable para usuarios no expertos en el área, poseen licencia gratuita y aunque el proyecto posee herramientas gratuitas, éste tiene un costo económico aproximado de US$50 mensuales para la institución mientras se utilice.

Para desarrollar este proyecto es necesario conocer un poco sobre lo que es informática forense para lo cual se ha realizado una investigación acerca de la historia, concepto, usos y objetivos de la informática forense así como las áreas que corresponden a esta disciplina y el trato que se le da a la información cuando es recopilada para presentar los datos y que estos no pierdan su veracidad.

Para el kit de herramientas básicas, el manual y el CD interactivo fue necesario conocer la estructura de cada uno de los elementos, es decir, que pasos se seguirán para la creación de éstos. Por lo cual se investigó el concepto y los tipos de cada uno de ellos.

El desarrollo de éste proyecto tiene la finalidad de contribuir a la difusión de esta área para ayudar a los estudiantes por medio de este proyecto y la entrega de un kit de herramientas básicas sobre informática forense, con su respectivo manual de procedimientos y un CD interactivo, el cual contiene video-tutoriales sobre los programas del kit de herramientas para mayor comprensión de la instalación y uso de cada uno de ellos.

CAPITULO I
SITUACIÓN PROBLEMÁTICA

1.1 Situación problemática

La informática forense está adquiriendo gran relevancia dentro del área de la información digital, esto se debe a la importancia que tiene la información y/o al uso que se le da a ésta, con esto también se incrementan los delitos informáticos. Por ejemplo: robo de información, violación de la privacidad, Hackeo de redes, fraude electrónico, chantaje, pornografía infantil, ataques a sistemas.

Estas situaciones se han vuelto muy comunes en estos tiempos y muchas veces los usuarios no se dan cuenta de que están siendo víctimas de ataques informáticos que pueden causar serios problemas.

En nuestro país existe tan poca información sobre los delitos informáticos, lo que genera que éstos se incrementen, además en las instituciones educativas no se imparte la informática forense como una rama importante de la informática como es el caso del Instituto Nacional San Luis donde se imparte la materia de informática, la cual no abarca dicha área como contenido importante dentro de la materia de informática, para que los alumnos se interesen por esta técnicas de investigar los delitos informáticos y los pasos para proteger la evidencia de cualquier alteración.

Otro problema es la falta de difusión de la información acerca de las leyes que penalizan los delitos informáticos en nuestro país y la falta de más especialistas en el área de la informática forense.

1.2 Enunciado del Problema

¿Será necesario desarrollar un kit de herramientas básicas de software sobre informática forense, para apoyar el material didáctico del área de informática del Instituto Nacional san Luis?

1.3 Justificación

Este proyecto surge a partir de la necesidad de apoyar el material didáctico de la materia de informática del Instituto Nacional San Luis, por medio de la informática forense que permite la investigación de delitos informáticos relacionados con la inseguridad informática. Gracias a ella, los usuarios obtendrán conocimientos sobre como investigar y el trato que se le da a la evidencia digital de un delito informático surgido a través del uso indebido de las tecnologías de la informática ya que es necesario tratar con delicadeza esta información para que sea verídica y admisible ante un juicio judicial y extrajudicial.

Por otro lado, cuando la seguridad de los usuarios ya ha sido perjudicada, la informática forense permite recoger rastros probatorios para averiguar, el origen del ataque (si existe vulnerabilidad de la seguridad) o las posibles alteraciones, manipulaciones, fugas o destrucciones de datos a nivel interno para determinar las actividades realizadas desde uno o varios equipos.

Con este proyecto se pretende proporcionar un material didáctico que contendrá un kit de herramientas básicas de software sobre informática forense con su respectivo manual de uso el cual ayudará al estudiante a darle un uso apropiado a las herramientas recopiladas en este kit para un aprendizaje básico de la informática forense. De manera que con el desarrollo del kit de herramientas básicas de software se pretende que la utilización de la informática, sea un medio por el cual se den a conocer aplicaciones relacionadas a la informática forense.

Y ante la necesidad que se presenta de la falta de conocimientos de herramientas básicas de software, se hará este proyecto para que los alumnos del Instituto Nacional San Luis adquieran un nuevo conocimiento, y con la puesta en marcha y estudio del proyecto obtengan experiencia.

1.4 Objetivos

1.4.1 Objetivo general

Desarrollar un kit de herramientas básicas de software sobre informática forense para los alumnos del Instituto Nacional San Luis, con el fin de proporcionar un material didáctico de apoyo para la materia de informática.

1.4.2 Objetivos específicos

1. Identificar las herramientas que se utilizarán para el desarrollo del contenido del material de apoyo en el área de informática.

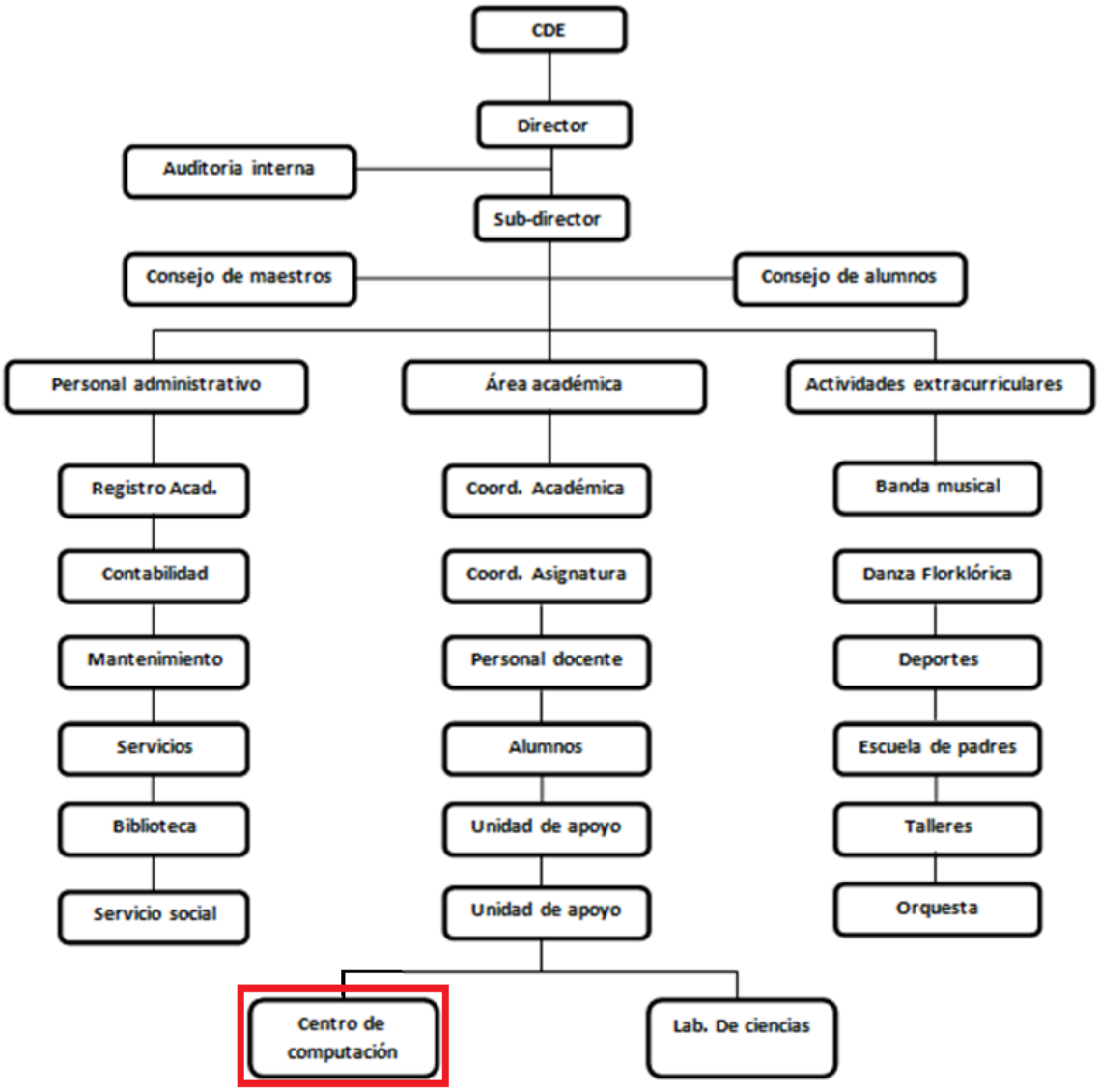
2. Crear un manual para el uso adecuado de las herramientas de software de informática forense.

3. Desarrollar un CD interactivo que contenga ayudas audio-visual para facilitar el uso de las herramientas básicas de la informática forense.

1.5 Delimitaciones

- **Geográfica:** Final Calle La Fuente Col. El Pepeto Cantón El tránsito Soyapango.
- **Temporal:** El proyecto se llevará a cabo en un período de tiempo comprendido del 15 Marzo al 31 Mayo de 2013.
- **Organizacional:** Este proyecto se realizará en el centro de cómputo del Instituto Nacional San Luis.

1.5.1 Organigrama



1.6 Alcances

Al realizar este proyecto se ofrecerá un kit de herramientas básicas de informática forense que servirá como material didáctico de apoyo para la materia de informática en el instituto Nacional San Luis.

Este kit estará conformado por un grupo de herramientas de software de informática forense, un manual impreso para la correcta utilización de las aplicaciones contenidas en el kit de herramientas, el cual brindará conocimientos teóricos y prácticos para que conozcan sobre la investigación y tratamiento de la información recopilada en un hecho delictivo referente a los delitos informáticos.

También se ofrecerá un CD interactivo que contenga en formato digital y comprensible ayudas audio-visuales para utilizar adecuadamente los programas que forman el kit de herramientas básicas y estará disponible para los alumnos del Instituto Nacional San Luis.

Debido a que la informática forense es muy extensa este proyecto se ha delimitado en las siguientes áreas de la informática forense: Esteganografía, Criptografía, Backdoors, Escala de privilegios, Ethical hacking, Recuperadores de información, Sniffer de red y Hackeo de redes.

Ya que son áreas que cumplen con las características de ser básicas y esenciales de la informática forense, además se encuentran software gratuitos.

Promesa	Producto
Proporcionar a la institución un kit de herramientas básicas de informática forense.	Kit de herramientas básicas de software sobre informática forense enfocado en las áreas de: Esteganografía, Criptografía, Backdoors, Escala de privilegios, Ethical hacking, Recuperadores de información, Sniffer de red y Hackeo de redes.
Elaborar un documento que ayude a utilizar de manera adecuada las herramientas de software.	Manual impreso para el uso adecuado de las herramientas de informática forense.
Se utilizará un medio audio-visual que ayude a facilitar el uso de las herramientas que poseerá el kit.	CD interactivo que contendrá, tutoriales y el manual en formato digital para comprender mejor el uso de los programas.

1.6.1 Tabla de Alcances

1.7 Estudio de factibilidad

1.7.1 Estudio de factibilidad económica

Cuadro de evaluación económico Grabador de CD y DVD			
Estudio de factibilidad económica			
Recuperadores de información	Alcohol 120%	Nero Burning ROM 7	Burn4Free
Precios	Licencia US$50.57	Licencia US$64.82	Licencia gratis
Establecimiento consultado ó URL	http://www.alcohol-soft.com/	http://www.nero.com/esp/downloads/	http://www.burn4free.com/
Análisis	En este cuadro comparativo se presentan tres Programas que son para grabar en CD y DVD dos de estos programas tienen licencias que no son gratis lo cual puede afectar a la economía por lo cual se elige el Burn4Free por ser gratuito.		

Tabla 1.7.1.1

Cuadro de evaluación económico procesadores de texto			
Estudio de factibilidad económica			
Recuperadores de información	Open office	Office Home and Student	AbiWord
Precios	Licencia Gratis (GPL)	Licencia US$120.00	Licencia Gratis (GPL)
Establecimiento consultado ó URL	http://openoffice.softonic.com/	http://www.siman.com/elsalvador/office-home-and-student.html	http://abiword.softonic.com/
Análisis	En este cuadro comparativo se presentan tres Programas que son para procesar texto dos de estos programas tienen licencias gratuita pero se eligió a Open Office porque posee herramientas para crear documentos básicos y puede archivar los documentos en una gran variedad de formatos.		

Tabla 1.7.1.2

Cuadro de evaluación económico Recuperadores de información			
Estudio de factibilidad económica			
Recuperadores de información	Recuva	UnDelete plus	Glary UnDelete
Precios	Licencia gratis	Licencia gratis	Licencia gratis
Establecimiento consultado o URL	http://recuva.softonic.com/descargar	http://descargar.portalprogramas.com /Undelete-Plus.html	http://www.glarysoft.com /glary-undelete/download/
Análisis	En este cuadro comparativo se presentan tres Programas que son de mucha utilidad para recuperar archivos y se ha elegido al programa Recuva porque es gratuito, posee un entorno sencillo y es el recuperador más utilizado.		

Tabla 1.7.1.3

Cuadro de evaluación económico Recuperadores de información			
Estudio de factibilidad económica			
Recuperadores de información	Avira UnErase	Wise Data Recovery	Pandora Recovery
Precios	Licencia gratis	Licencia gratis	Licencia gratis
Establecimiento consultado ó URL	http://avira-unerase.programas-gratis.net/descargar#estasviendo	http://api.downloadmr.com/installer/4fe0cf9f-1fe4-4abb-905a-57915bc06f2f/5836324/open	http://pandora-recovery.softonic.com /
Análisis	En este cuadro comparativo se presentan tres Programas que son de mucha utilidad para recuperar información por lo cual se ha elegido al programa Wise Data Recovery porque es gratuito, posee un entorno amigable y recupera archivos de correo electrónico.		

Tabla 1.7.1.4

Cuadro de evaluación económico Recuperadores de información			
Estudio de factibilidad económica			
Recuperadores de información	Acronis Backup & Recovery® 11.5 Server for Windows	Easy recovery	PC Inspector file recovery
Precios	Licencia US$75	Licencia gratis	Licencia gratis
Establecimiento consultado ó URL	http://www.acronis.com/backup-recovery/wizard/	http://www.softonic.com/s/easy-recovery-gratis-espa%C3%B1ol	http://pc-inspector-file-recovery.softonic.com/descargar
Análisis	En este cuadro comparativo se presentan tres Programas para recuperar información por lo cual se ha elegido Easy recovey porque no requiere instalación y es gratuito.		

Tabla 1.7.1.5

Cuadro de evaluación económico Esteganografía			
Estudio de factibilidad económica			
Esteganografía	Spimage 2.0	Steganography	Bon Kyu Bon
Precios	Licencia Gratis	Licencia US$24.95	Licencia Gratis
Establecimiento consultado ó URL	http://spimage.softonic.com/	http://stegstudio.sourceforge.net/	http://bon-kyu-bon.softonic.com/
Análisis	En este cuadro comparativo se presentan tres Programas para ocultar archivos dentro de imágenes por lo cual se ha elegido Spimage 2.0 porque posee un entorno gráfico sencillo, llamativo y es gratuito.		

Tabla 1.7.1.6

Cuadro de evaluación económico Esteganografía			
Estudio de factibilidad económica			
Esteganografía	Fileinyector	XiaoSteganography	Dound's Steganography
Precios	Licencia gratis	Licencia gratis	Licencia gratis
Establecimiento consultado ó URL	http://www.spotynow.es/fileinyector-esteganografa-en-windows/	http://www.spotynow.es/fileinyector-esteganografa-en-windows/	http://www.dound.com/Progs/Steg.Html
Análisis	En este cuadro comparativo se presentan tres Programas del cual se ha elegido File inyector por ser de licencia gratuita y no requiere instalación.		

Tabla 1.7.1.7

Cuadro de evaluación económico Esteganografía			
Estudio de factibilidad económica			
Esteganografía	PlainSight	Camouflage	Hide&Reveal
Precios	Licencia gratis	Licencia gratis	Licencia Gratis (GPL)
Establecimiento consultado ó URL	http://plain-sight.softonic.com/	http://camouflage.programas-gratis.net/	http://www.softpedia.com/get/Security/Security-Related/Hide-Reveal.shtml
Análisis	En este cuadro comparativo se presentan tres Programas que permite ocultar un mensaje o texto en una imagen, de estos se ha elegido el Camouflage por ser muy sencillo y con licencia gratuita.		

Tabla 1.7.1.8

Cuadro de evaluación económico Criptografía			
Estudio de factibilidad económica			
Criptografía	Cryptic disk 3 home edition	Paranoic encryption	Encrypt Easy
Precios	licencia US$34.95	Licencia gratis	Licencia de prueba
Establecimiento consultado ó URL	http://cryptic-disk.softonic.com/	http://paranoic-encryption.softonic.com/descargar#downloading	http://encrypt-easy.softonic.com/
Análisis	En el cuadro comparativo anterior se presentan tres software de los cuales se ha elegido paranoic encryption por ser un programa fácil de utilizar y poseer licencia gratis.		

Tabla 1.7.1.9

Cuadro de evaluación económico Criptografía			
Estudio de factibilidad económica			
Criptografía	File Secure Free	Axcrypt	FreeOTFE Explorer
Precios	Licencia gratis	Licencia GPL	Licencia gratis
Establecimiento consultado ó URL	http://es.download.cnet.com/File-Secure-Free/3000-2092_4-75729419.html	http://es.kioskea.net/download /descargar-2046-axcrypt	http://freeotfe-explorer.softonic.com/ descargar
Análisis	En el cuadro comparativo anterior se presentan tres software que son para ocultar información de los cuales se eligió al programa Axcrypt por ser de uso fácil y poseer licencia libre siendo así una ayuda económica para los usuarios.		

Tabla 1.7.1.10

Cuadro de evaluación económico Criptografía			
Estudio de factibilidad económica			
Criptografía	BCArchive	True Crypt	Encriptor
Precios	Licencia gratis	Licencia gratis	Licencia gratis
Establecimiento consultado ó URL	http://bcarchive.softonic.com/	http://www.truecrypt.org /downloads	http://encriptor.softonic.com /descargar#downloading
Análisis	En este cuadro comparativo se presentan tres Programas que permite encriptar y ocultar datos de estos se ha elegido el true Crypt porque es gratis y es fácil de utilizar.		

Tabla 1.7.1.11

Cuadro de evaluación económico Sniffer de Red			
Estudio de factibilidad económica			
Sniffer de Red	SmartSniff	Free IP tools	EffeTech HTTP Sniffer
Precios	Licencia gratis	Licencia gratis	US$29.95
Establecimiento consultado ó URL	Smartsniff.softonic.com	http://free-ip-tools.softonic.com/descargar #downloading	http://www.softpedia.com/ progDownload/EffeTech-HTTP-Sniffer-Download-593.html
Análisis	En este cuadro comparativo anterior se presentan tres software de los cuales se ha elegido Free IP tools por tener un entorno gráfico y amigable para trabajar además posee licencia gratis.		

Tabla 1.7.1.12

Cuadro de evaluación económico Hackeo de Redes			
Estudio de factibilidad económica			
Hackeo de Redes	Backtrack	Commview for wifi	Wifi auditor
Precios	Licencia gratis	Licencia de prueba	Licencia gratis
Establecimiento consultado ó URL	http://www.backtrack-linux.org/download/	http://commview-for-wifi.softonic.com/	Wifi-auditor.softonic.com
Análisis	En este cuadro comparativo anterior se presentan tres software de los cuales se ha elegido Backtrack por tener licencia gratis y es la herramienta más conocida para hackear redes.		

Tabla 1.7.1.13

Cuadro de evaluación económico Backdoors			
Estudio de factibilidad económica			
Backdoors	Back Orifice	RealVNC Enterprise Edition	TeamViewer 8
Precios	Licencia gratis	Licencia gratis	Licencia gratis
Establecimiento consultado ó URL	http://www.softonic.com/s/back-orifice	http://www.intercambiosvirtuales.org/software/realvnc-enterprise-edition-v5-0-5-winlinuxmac-administra-cualquier-pc-a-control-remoto#more-59872	http://teamviewer..com/en /download/ Windows.aspx
Análisis	En este cuadro comparativo anterior se presentan tres software de los cuales se ha elegido TeamViewer 8 por tener licencia gratis y poseer un entorno sencillo.		

Tabla 1.7.1.14

Cuadro de evaluación económico Escala de privilegios	
Estudio de factibilidad económica	
Escala de privilegios	Hiren′s boot CD
Precios	Licencia gratuita
Establecimiento consultado ó URL	http://ftp-mirror.internap.com/pub/hirensbootcd/Hirens.BootCD.15.2.zip
Análisis	En el siguiente cuadro se presenta un programa para evadir la escala de privilegios el cual es gratuito y fácil de utilizar.

Tabla 1.7.1.15

1.7.2 Estudio de factibilidad técnica

Cuadro de evaluación técnica de quemadores el cual será aprobado si su calificación es => 85 %							
Características	Ponderación%	Alcohol 120%		Nero Burning ROM 7		Burn4Free	
		Valor	Total	Valor	Total	Valor	Total
Ocupa poco en el disco duro	10%	2	20%	1	10%	2	20%
Graba todo tipo de discos ópticos	20%	1	20%	2	40%	1	20%
Graba y abre discos ISO	10%	2	20%	2	20%	2	20%
Grabador de discos CD y DVD	20%	2	40%	2	40%	2	40%
Compilaciones de datos o música	20%	2	40%	2	40%	1	20%
buscador para localizar archivos	10%	2	20%	1	10%	1	10%
Opciones avanzadas de grabación	10%	1	10%	2	20%	1	10%
Totales	100%		170%		180%		140%
Ponderación final		170%/2= 85%		180%/2= 90%		140%/2= 70%	
Resultado Obtenido		Aprobado		Aprobado		Reprobado	

Tabla 1.7.2.1

Análisis: En la tabla anterior se han comparado tres software para quemar Discos ópticos de los cuales se seleccionó al Nero Burning ROM 7 porque es una aplicación que tiene las características técnicas necesarias para quemar un disco óptico.

Cuadro de evaluación técnica de editor de texto el cual será aprobado si su calificación es => 85 %							
Características	Ponderación%	Open office		Microsoft Office Home and Students		AbiWord	
		Valor	Total	Valor	Total	Valor	Total
Compatible con muchos formatos	30%	2	60%	2	60%	2	60%
Guarda a PDF	10%	1	10%	2	20%	1	10%
Corrección y traducción	20%	2	40%	2	40%	1	20%
Macros para automatizar tareas	20%	1	20%	2	40%	1	20%
bajo consumo de recursos	20%	2	40%	1	20%	2	40%
Totales	100%		170%		180%		150%
Ponderación final		170%/2= 85%		180%/2= 90%		150%/2= 75%	
Resultado Obtenido		Aprobado		Aprobado		Reprobado	

Tabla 1.7.2.2

Análisis: En la tabla anterior se han comparado tres software editores de texto por lo cual se ha escogido a Microsoft Office Home and Students porque posee todos los elementos para realizar diversas funciones, automatizar tareas y es el editor de texto más conocido.

Cuadro de evaluación técnica de recuperadores de información el cual será aprobado si su calificación es => 85 %							
Características	Ponderación%	Recuva		Undelete plus		Glary UnDelete	
		Valor	Total	Valor	Total	Valor	Total
Recupera archivos que han sido borrados de discos duros	30%	2	60%	2	60%	2	60%
Recupera los datos después de un formateo.	30%	2	60%	2	60%	1	30%
Restaurar archivos borrados de memorias Flash/USB	20%	1	20%	2	40%	1	20%
Los análisis son rápidos	10%	2	20%	1	10%	2	20%
Recupera archivos vaciados de la Papelera de reciclaje	10%	1	10%	1	10%	2	20%
Totales	100%		170%		180%		150%
Ponderación final		170%/2= 85%		180%/2= 90%		150%/2= 75%	
Resultado Obtenido		Aprobado		Aprobado		Reprobado	

Tabla 1.7.2.3

Análisis: Del anterior cuadro se han comparado tres software para recuperar datos se seleccionó el Recuva porque sirve para recuperar archivos que se han borrado, los detecta permite seleccionarlos cómodamente, también es capaz de recuperar fotos, documentos, imágenes**.**

Cuadro de evaluación técnica de recuperadores de información el cual será aprobado si su calificación es => 85%							
Características	Ponderación%	AviraUnErase		Wise Data Recovery		Pandora recovery	
		Valor	Total	Valor	Total	Valor	Total
Recuperación de la información eliminada de un dispositivo	40%	2	80%	2	80%	2	80%
Entorno sencillo y práctico de utilizar	10%	1	10%	2	20%	1	10%
Recupera archivos de correo electrónico, tales como EML	20%	1	20%	1	20%	2	40%
Recupera datos después de un formateo.	10%	1	10%	2	20%	1	10%
Recupera la mayor cantidad de formatos de archivos	20%	1	20%	2	40%	1	20%
Totales	100%		140%		180%		160%
Ponderación final		140%/2= 70%		180%/2= 90%		160%/2= 80%	
Resultado Obtenido		Reprobado		Aprobado		Reprobado	

Tabla 1.7.2.4

Análisis: En el anterior cuadro se han comparado tres software para recuperar datos se seleccionó el Wise Data Recovery porque es un programa muy amigable y además es una herramienta que recupera múltiples formatos de imágenes, documentos, y también de cualquier dispositivo de almacenamiento.

Cuadro de evaluación técnica de recuperadores de información el cual será aprobado si su calificación es => 85%							
Características	Ponderación%	Acronis Backup & Recovery		Easy recovery		TestDisk	
		Valor	Total	Valor	Total	Valor	Total
Restaura los archivos eliminados.	30%	2	60%	2	60%	2	60%
Encuentra datos eliminados con facilidad	10%	2	20%	1	10%	2	20%
Funciona también con memorias USB y tarjetas de memoria.	10%	2	20%	2	20%	2	20%
Realiza un completo análisis para recuperar los archivos eliminados.	20%	2	40%	2	40%	2	40%
Posee entorno gráfico	30%	2	60%	2	60%	0	0%
Totales	100%		200%		190%		140%
Ponderación final			200%/2= 100%		190%/2= 85%		140%/2=70%
Resultado Obtenido		Aprobado		Aprobado		Aprobado	

Tabla 1.7.2.5

Análisis: De la tabla anterior se han comparado tres software para recuperar datos, se seleccionó al Easy recovery por tener herramientas de análisis de particiones, es una herramienta multiplataforma que utiliza un entorno gráfico, amigable para el usuario y cumple a las características que se buscan en el programa.

Cuadro de evaluación técnica de Esteganografía el cual será aprobado si su calificación es => 85%							
Características	Ponderación%	Spimage 2		Steganography		Bon Kyu Bon	
		Valor	Total	Valor	Total	Valor	Total
Puede ocultar programas	20%	1	20%	1	20%	1	20%
Oculta imágenes (JPEG, GIF y PNG)	10%	1	10%	2	20%	2	20%
Oculta archivos de sonido	10%	2	20%	1	10%	0	0%
Oculta archivos vídeos	10%	2	20%	1	10%	0	0%
Oculta archivos de texto	20%	2	40%	2	40%	2	40%
Oculta y codifica.	30%	2	60%	1	30%	1	30%
Totales	100%		170%		130%		110%
Ponderación final		170%/2= 85%		130%/2= 65%		110%/2= 55%	
Resultado Obtenido		Aprobado		Reprobado		Reprobado	

Tabla 1.7.2.6

Análisis: En la tabla anterior se hizo la comparación técnica de tres programas que sirven para ocultar información dentro de otro archivo y se escogió a Spimage 2.0 porque su interfaz gráfica es amigable y puede ocultar y codificar todo tipo de archivos dentro de cualquier archivo.

Cuadro de evaluación técnica de Esteganografía el cual será aprobado si su calificación es = 85%							
Características	Ponderación%	FileInyector		Xiao Steganography		Dound's Steganography	
		Valor	Total	Valor	Total	Valor	Total
Combina cifrado y Esteganografía	20%	1	20%	1	30%	1	30%
Es fácil de usar	20%	2	40%	2	40%	2	40%
Oculta en imágenes (JPEG, GIF y PNG)	20%	2	40%	0	0%	0	0%
Buena protección	20%	2	40%	2	40%	1	20%
Oculta un mensaje dentro de otro	20%	2	40%	1	10%	2	20%
Totales	100%		180%		120%		110%
Ponderación final		180%/2= 90%		120%/2= 60%		110%/2= 55%	
Resultado Obtenido		Aprobado		Reprobado		Reprobado	

Tabla 1.7.2.7

Análisis: En la tabla anterior se hizo la comparación técnica de tres programas que sirven para ocultar información dentro de otro archivo y se escogió FileInyector porque combina cifrado y Esteganografía además puede ocultar un mensaje dentro de otro, se instala en pocos segundos y es muy fácil de usar.

Cuadro de evaluación técnica de Esteganografía el cual será aprobado si su calificación es => 85%							
Características	Ponderación%	Camouflage		Plaing Sight		Hide&Reveal	
		Valor	Total	Valor	Total	Valor	Total
Interacción con el menú de Windows	10%	2	20%	2	20%	0	0%
Fácil de usar	20%	2	40%	1	20%	2	40%
Buena protección	20%	2	40%	2	40%	2	40%
Oculta en todo tipo de imagen	30%	2	60%	2	60%	1	30%
Oculta un archivo dentro de otro	20%	2	40%	2	40%	1	20%
Totales	100%		200%		180%		130%
Ponderación final		200%/2= 100%		180%/2= 90%		130%/2= 65%	
Resultado Obtenido		Aprobado		Aprobado		Reprobado	

Tabla 1.7.2.8

Análisis: En la tabla anterior se hizo la comparación técnica de tres programas que sirven para ocultar información importante de personas no deseadas se escogió Camouflage su funcionamiento es muy sencillo, tanto que no tiene ventana principal en sí sino que se activa desde el menú contextual, seleccionando los archivos a ocultar.

Cuadro de evaluación técnica de Criptografía el cual será aprobado si su calificación es => 85%							
Características	Ponderación%	File Secure Free		Axcrypt		Free OTFE	
		Valor	Total	Valor	Total	Valor	Total
Se incorpora con el menú de Windows	20%	1	20%	2	40%	1	20%
Cifrar, Descifrar, ver y editar archivos	20%	2	40%	2	40%	2	40%
Muestra un icono diferente para los archivos encriptados	10%	0	0%	2	20%	0	0%
Destruir o eliminar archivos de forma segura	10%	2	20%	1	10%	2	20%
Ofrece varios algoritmos de cifrado	20%	1	20%	2	40%	2	40%
Posibilidad de cifrar una unidad extraíble	20%	2	40%	2	40%	0	0%
Totales	100%		140%		190%		120%
Ponderación Final		140%/2= 70%		190%/2= 95%		120%/2=60%	
Resultado Obtenido		Reprobado		Aprobado		Reprobado	

Tabla 1.7.2.9

Análisis: En la tabla anterior se hizo la comparación técnica de tres programas que ayudan a proteger la información se escogió Axcrypt porque este programa encripta con una contraseña la información y además no tiene ventana principal en sí sino que se activa desde el menú contextual de Windows.

Cuadro de evaluación técnica de Criptografía el cual será aprobado si su calificación es => 85%							
Características	Ponderación%	Cryptic disk 3 home edition		Paranoic Encryption		Encrypt Easy	
		Valor	Total	Valor	Total	Valor	Total
Interfaz sencilla	10%	1	10%	2	20%	1	10%
Protección de cifrado por contraseña	20%	2	40%	1	20%	0	0%
Software gratuito	30%	0	0%	2	60%	0	30%
Cifrado de texto	20%	0	0%	2	40%	0	0%
No requiere instalación	20%	0	0%	2	40%	2	40%
Totales	100%		50%		180%		90%
Ponderación Final		50%/2= 25%		180%/2= 90%		90%/2= 45%	
Resultado Obtenido		Reprobado		Aprobado		Reprobado	

Tabla 1.7.2.10

Análisis: En el cuadro anterior se ha hecho la comparación de tres herramientas para el cifrado de información en el cual se escogió Paranoic Encryption por ser una herramienta práctica de cifrado de texto es rápido y fácil de usar y cumplea las características necesarias.

Cuadro de evaluación técnica de Criptografía el cual será aprobado si su calificación es => 85%							
Características	Ponderación%	BCArchive		Encriptor		True Crypt	
		Valor	Total	Valor	Total	Valor	Total
Posibilidad de cifrar una partición o un disco completo	20%	0	0%	0	0%	2	40%
Codifica y decodifica los datos	20%	2	40%	2	40%	2	40%
Seguridad de encriptación por contraseña	20%	2	40%	0	0%	2	40%
Encripta particiones	10%	2	20%	1	10%	1	10%
permite esconder el volumen para que no sea detectado	20%	0	0%	0	0%	1	20%
La encriptación es en tiempo real	10%	1	10%	2	20%	2	20%
Totales	100%		110%		70%		170%
Ponderación Final		110%/2=55%		70%/2=35%		170%/2=85%	
Resultado Obtenido		Reprobado		Reprobado		Aprobado	

Tabla 1.7.2.11

Análisis: En el cuadro anterior se evaluaron tres programas de los cuales se escogió a TrueCrypt porque ofrece la posibilidad de crear discos virtuales y aprovechar una partición ya existente para guardar ficheros cifrados es fácil de usar además tiene variedad de algoritmos de cifrado.

Cuadro de evaluación técnica de Sniffer de red el cual será aprobado si su calificación es => 85%							
Características	Ponderación%	Free IP Tools		Smartsniff		EffeTech HTTP Sniffer	
		Valor	Total	Valor	Total	Valor	Total
Capturar los paquetes de conexiones inalámbricas.	20%	2	40%	1	20%	1	20%
Escaneo de puertos de una dirección IP	30%	2	60%	1	30%	1	30%
Permite capturar los paquetes sin instalar ningún controlador	20%	1	20%	2	40%	2	40%
Controlar el tráfico de red	30%	2	60%	1	30%	1	30%
Totales	100%		170%		120%		120%
Ponderación final		170%/2=85%		120%/2=60%		120%/2=60%	
Resultado Obtenido		Aprobado		Reprobado		Reprobado	

Tabla 1.7.2.12

Análisis: En la tabla anterior se hizo la comparación de 3 programas para al software Free IP Tools qué cumple con las características técnicas necesarias para realizar una inspección de la red.

Cuadro de evaluación Backdoors se requiere un nivel de calificación = 〉 85 %							
Características	Ponderación%	Teamviewer 8		RealVNC		Back Orifice	
		Valor	Total	Valor	Total	Valor	Total
Capaz de establecer contraseña de acceso en el servidor	20%	1	20%	2	40%	1	20%
Leer y modificar ficheros	20%	2	40%	2	40%	1	20%
Gobernar cualquier función del ordenador remoto	30%	2	60%	2	60%	2	60%
Comunicarse a través de las. barreras de los firewalls sin necesidad de configuración especial	30%	2	60%	1	30%	2	60%
Totales	100%		180%		170%		160%
Ponderación final		180%/2= 90%		170%/2= 85%		160%/2= 80%	
Resultado Obtenido		Aprobado		Aprobado		Reprobado	

Tabla 1.7.2.13

Análisis: En la tabla anterior se hizo la comparación de 3 programas para al software Team viewer 8 por qué cumple con las características Técnicas para tomar el control de otra computadora por medio de control remoto.

Cuadro de evaluación técnica de Hackeo de redes el cual será aprobado si su calificación es => 85%							
Características	Ponderación%	Backtrack		Commview for WiFi		WiFi Auditor	
		Valor	Total	Valor	Total	Valor	Total
No requiere instalación	20%	2	40%	2	40%	1	20%
Herramientas para auditoría Inalámbrica	10%	2	20%	2	20%	2	20%
Capturar el nombre de la aplicación y de la ventana activa	10%	2	20%	2	20%	2	20%
Descifra claves WPA	20%	2	40%	1	20%	1	20%
Descifrar claves WEP	20%	1	20%	2	40%	1	20%
Scanner de puertos y vulnerabilidad	20%	2	40%	1	20%	2	40%
Totales	100%		180%		160%		140%
Ponderación final		180%/2= 90%		160%/2= 80%		140%/2= 70%	
Resultado Obtenido		Aprobado		Reprobado		Reprobado	

Tabla 1.7.2.14

Análisis: En la tabla anterior se hizo la comparación de 3 programas para al software Backtrack porque cumple con las características Técnicas y herramientas útiles que permiten extraer información.

Cuadro de evaluación técnica de Escala de privilegios el cual será aprobado si su calificación es = 85%			
Características	Ponderación%	Hiren's Boot CD	
		Valor	Total
No requiere instalación	20%	2	40%
Cambio o eliminación de contraseñas en el equipo	50%	2	100%
Live CD	10%	1	10%
secuencia de arranque múltiple	20%	1	20%
Totales	100%		170%
Ponderación final		170%/2= 85%	
Resultado Obtenido		Aprobado	

Tabla 1.7.2.15

Análisis: En la tabla anterior se presenta un programa que es para quitar la contraseña de administrador del equipo por lo cual es elegido para la Escala de privilegios y cumple con las necesidades requeridas para esta área.

Análisis general de todos los programas comparados técnica y económicamente

Según el registro anterior y las comparaciones realizadas de todas las aplicaciones presentadas se han escogido los siguientes software:

QUEMADORES DE DISCOS ÓPTICOS: Nero Burning ROM 7, se escogió este quemador de discos debido a que este programa ocupa poco espacio en el disco duro y tiene diversas opciones para quemar discos ópticos, aunque la licencia no es gratuita se escogió este quemador.

EDITOR DE TEXTO: Microsoft office, se escogió este editor de textos debido a que este editor de texto es compatible con muchos formatos y posee macros para automatizar tareas y aunque la licencia no es gratuita este programa cumple con las características necesarias para realizar el manual y el trabajo escrito.

RECUPERADORES DE INFORMACION: Recuva, Wise Data Recovery, Easy recovery, se han elegido porque cumplen con las características económicas y técnicas necesarias de un recuperador de información.

ESTEGANOGRAFIA: Spimage 2, FileInyector, Camouflage, se han seleccionado estos programas por tener licencia gratuita, son programas fáciles de utilizar y con las características técnicas adecuadas según la factibilidad técnica realizada.

CRIPTOGRAFIA: Axcrypt, Paranoic Encryption, True Crypt, estos programas para encriptar se escogieron en la factibilidad económica porque son gratuitos ayudando a la economía de los usuarios y en la factibilidad técnica también cumplieron con el porcentaje requerido para su aprobación por las características técnicas para encriptar información.

SNIFFER DE RED: Free IP Tools, se eligió porque según la factibilidad técnica es un programa que cumple con las principales características para inspeccionar en tráfico de las redes y además en la factibilidad económica se eligió porque es de licencia gratuita y posee una interfaz amigable para el usuario.

BACKDOORS: Team viewer 8, se escogió este programa porque cumple con las características técnicas para tomar el control completo de una computadora evadiendo la seguridad de los firewalls y es indetectable para los antivirus, además en la factibilidad económica se eligió porque es gratuito.

HACKEO DE REDES: En la factibilidad económica se eligió el programa Backtrack porque es gratuito y en la factibilidad técnica se escogió porque posee muchas herramientas que son de gran utilidad pero solamente se usará la herramienta que es solo para hackear redes.

ESCALA DE PRIVILEGIOS: Para esta área solo se tiene el programa Hiren's Boot CD este programa es gratuito y cumple con la funcionalidad necesaria para eliminar las contraseñas del administrador.

1.8 Carta de aceptación

INSTITUTO NACIONAL SAN LUIS
CIENCIA, CULTURA Y SUPERACIÓN

Soyapango, 08 de marzo de 2013

Sres.
Universidad Tecnológica de El Salvador
Presente.-

Reciba un cordial saludo de parte de la Comunidad Educativa del Instituto Nacional San Luis de Soyapango, deseando muchos éxitos en su importante labor.

Mediante la presente les comunicamos que damos por aceptado el proyecto **"Desarrollo de un kit de herramientas básicas de software sobre informática forense"** como material didáctico en el área de informática para esta institución, este proyecto fue presentado por tres alumnas de su institución cuyos nombres son:

1. Sandra Cristina Roberto Alférez
2. Keila Birzavit Ruiz Nuila
3. Wendy Marisol Ruiz Romero

Agradeciendo de antemano la atención a la presente, me suscribo.

Atentamente

Pedro Hernández Martínez
Coordinar Académico

CAPÍTULO II
DOCUMENTACIÓN TÉCNICA

2.1 Marco teórico de referencia

2.1.1 Informática forense

El mundo tecnológico evoluciona constantemente y así mismo la información digital, esto genera inseguridad en los sistemas informáticos ya que por fallas en el diseño de los mismos crea un excelente ambiente para los intrusos informáticos que se dedican a atacar a los usuarios por diversas motivaciones. Por ejemplo: Reto, ego, espionaje, ideología, dinero, venganza.

Estos intrusos informáticos encuentran la manera de penetrar en los equipos de una u otra forma es por esto que es de vital importancia conocer la mente y la forma de atacar de estos intrusos para protegerse de sus ataques, debido a esta necesidad aparece la informática forense como una rama auxiliar de la informática para ayudar a investigar y conocer diferentes técnicas de la misma y algunas de sus áreas respectivas: Esteganografía, Criptografía, Backdoors, Escala de privilegios, Ethical hacking, Recuperadores de información, Sniffer de red y Hackeo de redes para enfrentar los desafíos de los intrusos informáticos.

La informática forense es de gran ayuda para detectar pistas sobre ataques informáticos como: Robo de información, conversaciones de emails, chats, fraude electrónico, chantaje. Uno de los objetivos de la informática forense es recopilar información y protegerla luego de que se ha cometido un delito informático para proteger la integridad y veracidad de la misma.

La informática forense requiere conocimientos sobre software, hardware, redes, hacking, cracking, seguridad informática y recuperación de información. Estos conocimientos son un requisito para una persona especialista en esta área constituido como un informático forense.

Este proyecto se llevará cabo con fines educativos en el Instituto Nacional San Luis con el propósito de que los estudiantes puedan conocer las técnicas básicas sobre la investigación que realiza la informática forense para esclarecer un delito informático y así puedan interesarse en el área de la informática forense.

2.1.2 Historia de la informática forense

La informática forense surgió en la década de 1980, poco después de que las computadoras personales se convirtieran en una opción factible para los consumidores. En 1984, fue creado un programa del FBI(Federal Bureau of investigation). Conocido por un tiempo como el Programa de Medios Magnéticos, que ahora se conoce como CART del inglés computer analisys and response team. CART proporciona exámenes de las computadoras y sus discos como un apoyo a las investigaciones y en juicio. Poco después, el "padre de la informática forense", a quien se le atribuye este sobrenombre comenzó a trabajar en esta rama de la informática. Su nombre era Michael Anderson él era un agente especial de la División de Investigación Criminal del IRS del inglés Internal Revenue Service (Servicio de impuestos internos). Michael Anderson trabajó para el gobierno en esta área hasta mediados de 1990, y debido a esto fundó New Technologies, Inc., un equipo que lleva la firma forense.

En la actualidad las compañías dedicadas a la creación de software producen software más potentes y seguros y los agentes de la ley y militares entrenan a más personal para responder a los crímenes informáticos.

2.1.3 Concepto de la informática forense

La informática forense según (Cano, 2009) la manifestación natural del entorno digital y de la sociedad de la información para responder a la creciente ola de incidentes, fraudes y ofensas (en medios informáticos y a través de medios informáticos), con el fin de enviar un mensaje claro a los intrusos: Estamos preparados para responder a sus acciones, y continuamos aprendiendo para dar con la verdad de sus acciones.

Es decir, es una rama de la informática para investigar la información digital que pasa por una computadora, por medio de la red o en cualquier dispositivo electrónico de almacenamiento para ser analizada y posteriormente mostrada para su destino.

2.1.4 Tratamiento de la información

MANUAL DE MANEJO DE EVIDENCIAS DIGITALES Y ENTORNOS INFORMÁTICOS

Principios Básicos

1. El funcionario de la Fiscalía o de la Policía Judicial nunca debe acudir solo al lugar de los hechos, este tipo de actividad debe ser realizada como mínimo por dos funcionarios. Un segundo funcionario, por un lado, aporta seguridad personal y, por otro, ayuda a captar más detalles del lugar de los hechos. Los funcionarios deberían planear y coordinar sus acciones. Si surgen problemas inesperados, es más fácil resolverlos porque "dos cabezas piensan más que una.

2. Ninguna acción debe tomarse por parte de la Policía Judicial, la Fiscalía o por sus agentes y funcionarios que cambie o altere la información almacenada dentro de un sistema informático o medios magnéticos, a fin de que esta sea presentada fehacientemente ante un tribunal.

3. En circunstancias excepcionales una persona competente puede tener acceso a la información original almacenada en el sistema informático, objeto de la investigación siempre que después se explique detalladamente y de manera razonada cual fue la forma en la que se produjo dicho acceso, su justificación y las implicaciones de dichos actos.

4. Se debe llevar una bitácora de todos los procesos adelantados en relación a la evidencia digital. Cuando se hace una revisión de un caso por parte de una tercera parte ajena al mismo, todos los archivos y registros de dicho caso y el proceso aplicado a la evidencia que fue recolectada y preservada, deben permitir a esa parte recrear el resultado obtenido en el primer análisis.

5. El Fiscal del Caso y/o el oficial a cargo de la investigación son responsables de garantizar el cumplimiento de la ley y del apego a estos principios, los cuales se aplican a la posesión y el acceso a la información almacenada en el sistema informático. De igual forma debe asegurar que cualquier persona que acceda a o copie dicha información cumpla con la ley y estos principios. (escuela.fgr.gob.sv)

Principios del Peritaje

1. Objetividad: El perito debe ser objetivo, debe observar los códigos de ética profesional.

2. Autenticidad y conservación: Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios

3. Legalidad**:** El perito debe ser preciso en sus observaciones, opiniones y resultados, conocer la legislación respecto de sus actividad pericial y cumplir con los requisitos establecidos por ella

4. Idoneidad: Los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso.

5. Inalterabilidad**:** En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.

6. Documentación: Deberá establecerse por escrito los pasos dados en el procedimiento pericial.

Estos principios deben cumplirse en todas las pericias y por todos los peritos involucrados:

- **Reconocimiento de la evidencia.**

Es importante clarificar los conceptos y describir la terminología adecuada que nos señale el rol que tiene un sistema informático dentro del iter criminis o camino del delito. Esto a fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener nuestro caso. Es así que por ejemplo, el procedimiento de una investigación por homicidio que tenga relación con evidencia digital será totalmente distinto al que, se utilice en un fraude informático, por tanto el rol que cumpla el sistema informático determinara donde debe ser ubicada y como debe ser usada la evidencia.

Ahora bien para este propósito se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (*evidencia*

electrónica) y la información contenida en éste (*evidencia digital*). Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital. En este contexto el hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, programas almacenados y mensajes de datos trasmitidos usando el sistema informático. (Salvador, 2013)

- **Incautación de Equipos Informáticos o Electrónicos**

Si el investigador presume que existe algún tipo evidencia digital en algún aparato electrónico o en algún otro soporte material relacionado con el cometimiento de una infracción. Este debe pedir la correspondiente autorización judicial para incautar dichos elementos, de igual forma debe tener la autorización judicial para acceder al contenido guardado, almacenado y generado por dichos aparatos.

Antes de realizar un allanamiento e incautación de Equipos Informáticos o electrónicos se debe tomar en cuenta lo siguiente:

1. **¿A qué horas debe realizarse?**

- Para minimizar destrucción de equipos, datos
- El sospechoso tal vez estará en línea
- Seguridad de investigadores

2. **Entrar sin previo aviso**

- Utilizar seguridad
- Evitar destrucción y alteración de los equipos, o la evidencia contenida en esta.

3. **Materiales previamente preparados (Cadena de custodia)**

- Embalajes de papel
- Etiquetas
- Discos y disquetes vacíos
- Herramienta
- Cámara fotográfica

4. **Realizar simultáneamente los allanamientos e incautación en diferentes sitios**

- Datos pueden estar en más de un lugar, sistemas de red, conexiones remotas.

5. **Examen de equipos**
6. **Aparatos no especificados en la orden de allanamiento**
7. **Creación de Respaldos en el lugar, creación de imágenes de datos.**

Autorización para duplicar, reproducir datos encontrados (por ejemplo, un aparato contestador)

8. **Fijar/grabar la escena**

- Cámaras, videos, etiquetas

9. **Códigos/claves de acceso/contraseñas**
10. **Buscar documentos que contienen información de acceso, conexiones en redes.**
11. **Cualquier otro tipo de consideración especial (consideraciones de la persona involucrada: médicos, abogados, información privilegiada, etc.)**

La falta de una orden de allanamiento e incautación que ampare las actuaciones (sobre los equipos y sobre la información) de la Policía Judicial y la Fiscalía puede terminar con la exclusión de los elementos probatorios por violación de las Garantías Constitucionales.

EN LA ESCENA DEL DELITO

Los Investigadores que llegan primero a una escena del crimen tienen ciertas responsabilidades. (Pino, 2013)

- **Observe y establezca los parámetros de la escena del delito**

El primero en llegar a la escena, debe establecer si el delito está todavía en progreso, es decir, si todavía se está ejecutando el delito. Luego tiene que tomar nota de las características físicas del área circundante. Para los investigadores forenses esta etapa debe ser extendida a todo sistema de información y de red que se encuentre dentro de la escena. En estos casos dicho sistema o red pueden ser blancos de un inminente o actual ataque como por ejemplo uno de denegación de servicio (DoS).

- **Iniciar las medidas de seguridad**

El objetivo principal en toda investigación es la seguridad de los investigadores y de la escena. Si uno observa y establece en una condición insegura dentro de una escena del delito, debe tomar las medidas necesarias para mitigar dicha situación. Se deben tomar las acciones necesarias a fin de evitar riesgos eléctricos, químicos o biológicos, de igual forma cualquier actividad criminal.

- **Facilite los primeros auxilios**

Siempre se deben tomar las medidas adecuadas para precautelar la vida de las posibles víctimas del delito, el objetivo es brindar el cuidado médico adecuado por el personal de emergencias y el preservar las evidencias.

- **Asegure físicamente la escena**

Esta etapa es crucial durante una investigación, se debe retirar de la escena del delito a todas las personas extrañas a la misma, el objetivo principal es el prevenir el acceso no

autorizado de personal a la escena, evitando así la contaminación de la evidencia o su posible alteración.

- **Asegure físicamente las evidencias**

Este paso es muy importante a fin de mantener la cadena de custodia de las evidencias, se debe guardar etiquetar cada una de ellas. En este caso se aplican los principios y la metodología correspondiente a la recolección de evidencias de una forma práctica. Esta recolección debe ser realizada por personal entrenado en manejar, guardar y etiquetar evidencias.

- **Entregar la escena del delito**

Después de que se han cumplido todas las etapas anteriores, la escena puede ser entregada a las autoridades que se harán cargo de la misma. Esta situación será diferente en cada caso, ya que por ejemplo en un caso penal será a la Policía; en un caso corporativo a los Administradores del Sistema. Lo esencial de esta etapa es verificar que todas las evidencias del caso se hayan recogido y almacenado de forma correcta, y que los sistemas y redes comprometidos pueden volver a su normal operación.

- **Elaborar la documentación de la explotación de la escena**

Es indispensable para los investigadores documentar cada una de las etapas de este proceso, a fin de tener una completa bitácora de los hechos sucedidos durante la explotación de la escena del delito, las evidencias encontradas y su posible relación con los sospechosos. Un investigador puede encontrar buenas referencias sobre los hechos ocurridos en las notas recopiladas en la explotación de la escena del delito.

- **Reconstrucción de la Escena del Delito**

La reconstrucción del delito permite al investigador forense comprender todos los hechos

relacionados con el cometimiento de una infracción, usando para ello las evidencias disponibles. Los indicios que son utilizados en la reproducción del delito permiten al investigador realizar tres formas de reconstrucción a saber:

Reconstrucción relacional, se hace en base a indicios que muestran la correspondencia que tiene un objeto en la escena del delito y su relación con los otros objetos presentes. Se busca su interacción en conjunto o entre cada uno de ellos.

Reconstrucción funcional, se hace señalando la función de cada objeto dentro de la escena y la forma en que estos trabajan y como son usados

Reconstrucción Temporal, se hace con indicios que nos ubican en la línea temporal del cometimiento de la infracción y en relación con las evidencias encontradas.

QUÉ HACER AL ENCONTRAR UN DISPOSITIVO INFORMÁTICO O ELECTRÓNICO

1. No tome los objetos sin guantes de hule, podría alterar, encubrir o hacer desaparecer las huellas dactilares o adeníticas existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.

2. Asegure el lugar.

3. Asegure los equipos. De cualquier tipo de intervención física o electrónica hecha por extraños.

4. Si no está encendido, no lo encienda (para evitar el inicio de cualquier tipo de programa de autoprotección

5. Verifique si es posible el Sistema Operativo a fin de iniciar la secuencia de apagado a fin de evitar pérdida de información.

6. Si usted cree razonablemente que el equipo informático o electrónico está destruyendo la evidencia, debe desconectarlo inmediatamente.

7. Si está encendido, no lo apague inmediatamente (para evitar la pérdida de información "volátil")

8. Si es posible, llame un técnico.

Cuando no hay técnico:

1. No use el equipo informático que está siendo investigado, ni intente buscar evidencias sin el entrenamiento adecuado.

2. Si está encendido, no lo apague inmediatamente.

3. Si tiene un "Mouse", muévalo cada minuto para no permitir que la pantalla se cierre o se bloqueé.

4. Si una Computadora Portátil (Laptop) no se apaga

5. Cuando es removido el cable de alimentación, localice y remueva la batería, esta generalmente se encuentra debajo del equipo, y tiene un botón para liberar la bacteria del equipo. Una vez que está es removida debe guardarse en un lugar seguro y no dentro de la misma máquina, a fin de prevenir un encendido accidental.

6. Si el aparato está conectado a una red, anote los números de conexión, (números IP).

7. Fotografíe la pantalla, las conexiones y cables

8. Usar bolsas especiales antiestática para almacenar discos ópticos discos duros, y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos

9. Coloque etiquetas en los cables para facilitar reconexión posteriormente

10. Anote la información de los menús y los archivos activos (sin utilizar el teclado)

11. Cualquier movimiento del teclado puede borrar información importante.

12. Si hay un disco, una cinta, un CD u otro medio de grabación en alguna unidad de disco o grabación, retírelo, protéjalo y guárdelo en un contenedor de papel

13. Bloqueé toda unidad de grabación con una cinta, un disco o un disquete vacío aportado por el investigador (no del lugar de los hechos). Al utilizar algún elemento del lugar del allanamiento o de los hechos, se contamina un elemento materia de prueba con otro.

14. Selle cada entrada o puerto de información con cinta de evidencia

15. De igual manera deben selle los tornillos del sistema a fin de que no se puedan remover o reemplazar las piezas internas del mismo.

16. Desconecte la fuente de poder

17. Quite las baterías y almacénela de forma separada el equipo (si funciona a base de baterías o es una computadora portátil)

18. Mantenga el sistema y medios de grabación separados de cualquier tipo de imán, o campo magnético

19. Al llevar aparatos, anote todo número de identificación, mantenga siempre la cadena de custodia.

20. Lleve todo cable, accesorio, conexión

21. Lleve, si es posible, manuales, documentación, anotaciones

22. Tenga en cuenta que es posible que existen otros datos importantes en sistemas periféricos, si el aparato fue conectado a una red, por tanto desconecte el cable de poder de todo hardware de Red (Router, modem, Swich, Hub).

23. Si el equipo es una estación de trabajo o un Servidor (conectado en red) o está en un negocio, el desconectarla puede acarrear (siempre consulte a un técnico experto en redes) daño permanente al equipo y es responsabilidad Civil para la Policía Judicial y la Fiscalía General del Estado la interrupción ilegal del giro del negocio. (Pino, 2013)

Rastreo del Correo Electrónico

El Correo Electrónico permite enviar cartas escritas con el computador a otras personas que tengan acceso a la Red. El correo electrónico es casi instantáneo, a diferencia del correo normal. Se puede enviar correo a cualquier persona en el Mundo que disponga de conexión a Internet y tenga una cuenta de Correo Electrónico.

Al enviar un correo electrónico, la computadora se identifica con una serie de números al sistema del proveedor de servicios de Internet (ISP). Enseguida se le asigna una dirección IP y es dividido en paquetes pequeños de información a través del protocolo TCP/IP. Los

paquetes pasan por una computadora especial llamada servidor (server) que los fija con una identificación única (Message-ID) posteriormente los sellan con la fecha y hora de recepción (Sello de tiempo). Más tarde al momento del envió se examina su dirección de correo para ver si corresponde la dirección IP de alguna de las computadoras conectadas en una red local (dominio). Si no corresponde, envía los paquetes a otros servidores, hasta que encuentra al que reconoce la dirección como una computadora dentro de su dominio, y los dirigen a ella, es aquí donde los paquetes su unen otra vez en su forma original a través del protocolo TCP/IP. (Protocolo de Control de Transferencia y Protocolo de Internet). Siendo visible su contenido a través de la interface gráfica del programa de correo electrónico instalado en la máquina destinataria.

Hay que tomar en cuenta que los correos electrónicos se mantienen sobre un servidor de correo, y no en la computadora del emisor o del destinatario, a menos que el operador los guarde allí. Al redactarlos se transmiten al servidor de correo para ser enviados. Al recibirlas, nuestra computadora hace una petición al Servidor de correo, para los mensajes sean transmitidos luego a la computadora del destinatario, donde el operador la puede guardar o leer y cerrar.

Al cerrar sin guardar, la copia de la carta visualizada en la pantalla del destinatario desaparece, pero se mantiene en el servidor, hasta que el operador solicite que la información sea borrada. (Pino, 2013)

2.1.5 Kit de herramientas básicas de software

El proyecto propuesto al Instituto Nacional San Luis consiste en realizar un kit de herramientas básicas de software que ayuden a conocer las técnicas básicas de la informática forense así como algunas de las áreas contenidas en la informática forense las cuales son: Recuperadores de información, Criptografía, Esteganografía, Sniffer de red, Hackeo de redes, Backdoors, Escala de privilegios, Ethical hacking; por cada una de estas áreas se han investigado algunos software que se especializan en cada una de ellas.

ÁREAS QUE FORMAN EL KIT DE HERRAMIENTAS BÁSICAS

2.1.5.1 Recuperadores de información

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

Hay dos formas básicas de perder información de un medio: pérdida física de datos o pérdida lógica de datos.

La pérdida física de datos, que es la más complicada, implica un problema real sobre la superficie donde están almacenados los datos. Por ejemplo, un rayón en un CD. En general, la información que se altera físicamente es más difícil (sino imposible) de recuperar.

La pérdida lógica de datos es la eliminación de archivos utilizando la opción de "borrar archivo" de cualquier sistema operativo (también puede pasar por un virus).

En los discos duros y otros medios de almacenamiento, los archivos no son borrados realmente del disco, sino que son marcados como eliminados. El sistema operativo interpreta que estos lugares del disco marcado como eliminados son en realidad espacio libre y, por lo tanto, podrá escribir sobre ellos. Muchas veces la información así marcada no es sobre escrita rápidamente, y por esta razón se puede recuperar.

La información es muy valiosa para las personas por esta razón han adoptado medidas de almacenaje electrónico para proteger dicha información, pero al mantener almacenada la información se incrementan las causas de pérdida de información, estas pueden ser desde formateos involuntarios, ataques de virus, bloqueos del sistema, averías mecánicas, golpes, incendios, inundaciones. Por lo que un correcto diagnóstico en el primer momento determinará si se puede o no recuperar la información que se eliminó. Debido al valor que tiene la información se han creado aplicaciones para ayudar a resolver dichos problemas y a los estudiantes del Instituto Nacional San Luis le ayudará a conocer sobre los recuperadores de información, ya que muchas veces se piensan que los archivos que han sido "borrados" de un medio de almacenamiento son borrados o eliminados de inmediato; pero realmente no conocen que estos archivos no han sido borrados y eliminados de inmediato si no que las referencias a ellos en la estructura de directorios ha sido movida, y el espacio que ocupan se vuelve disponible para su posterior sobre-escritura. Mientras menos se sobre-escriba en la unidad de almacenamiento mejor será la recuperación de datos.

Sistemas de archivos

Archivos FAT

(File AllocationTable - Tabla de Ubicación de Ficheros). Sistema de archivos que utilizan las ediciones no empresariales de Microsoft Windows hasta Windows MileniumEdition. Además es un sistema admitido casi por todos los sistemas operativos.

El sistema de archivos FAT fue creado por Bill Gates y Marc McDonald en 1977. Existen las versiones FAT12 del año 1977, FAT16 del año 1988 y FAT32 del año 1996.

Las implementaciones más extendidas de FAT tienen algunas desventajas; por ejemplo, la fragmentación excesiva de los datos. Cuando se borran y escriben nuevos archivos, suele dejar fragmentos dispersos por todo el soporte de almacenamiento. Esto complica el proceso de lectura y escritura, haciéndose cada vez más lento. Para agilizar la lectura/escritura se usa una herramienta de desfragmentación, pero es un proceso demasiado largo. El sistema FAT tampoco fue diseñado para ser redundante ante fallos. También, a diferencia de otros sistemas, no posee permisos de seguridad para cada archivo, por lo tanto cualquier usuario puede acceder a cualquier fichero en el soporte.

Es un formato sencillo, muy popular para disquetes, tarjetas de memorias, almacenamiento USB y dispositivos similares. (Alegsa, 1998-2012)

El sistema de archivos FAT se compone de cuatro secciones:

- Sector de arranque.
- Región FAT: que contiene la tabla de asignación de archivos.
- La región del directorio raíz.
- La región de datos: donde se almacena el contenido de ficheros y carpetas.

Actualmente el sistema FAT es reemplazado en Windows XP y superiores por el sistema NTFS. (Alegsa, 1998-2012)

Archivos NTFS

(New Technology File System). Es un sistema de archivos diseñado específicamente para Windows NT, y utilizado por las versiones recientes del sistema operativo Windows. Ha reemplazado al sistema FAT utilizado en versiones antiguas de Windows y en DOS.

Fue creado para lograr un sistema de archivos eficiente y seguro y está basado en el sistema de archivos HPFS de IBM/Microsoft usado en el sistema operativo OS/2. También tiene características del file System HFS diseñado por Apple.

NTFS permite definir el tamaño del clúster de forma independiente al tamaño de la partición. El tamaño mínimo del bloque es de 512 bytes. Este sistema también admite compresión nativa de archivos y encriptación.

Es un sistema ideal para particiones de gran tamaño, pudiendo manejar discos de hasta 2 terabytes.

Windows NT, 2000, 2003, XP y Vista soportan el sistema NTFS.

Sus desventajas son:

- Utiliza gran cantidad de espacio en disco para sí mismo.
- No es compatible con sistemas operativos como DOS, Windows 95, 98 ni ME.
- No puede ser usado en disquetes.
- La conversión a NTFS es unidireccional, por lo tanto, no se puede volver a convertir en FAT al actualizar la unidad.

Sus ventajas y mejoras con respecto al FAT son:

- Compatibilidad mejorada con los metadatos.
- Uso de estructura de datos avanzadas (árboles-B), optimizando el rendimiento, estabilidad y aprovechando espacio en disco, pues acelera el acceso a los ficheros y reduce la fragmentación.
- Mejora de la seguridad
- Listas de control de acceso
- El registro de transacciones (journaling), que garantiza la integridad del sistema de ficheros. (Alegsa, 1998-2012)

Algunos de los programas utilizados en esta área de la informática forense son: Recuva, Hiren´s, PC inspector file recovery, Pandora recovery, Get data back for ntfs, Ontrack Easy Recovery, Restoration, UrgentRecovery.

2.1.5.2 Criptografía

La evolución de la informática y el uso exagerado de las comunicaciones digitales han causado un gran número de problemas de seguridad, la constante evolución de la tecnología ha generado comodidad en las personas ya que hoy en día es más fácil realizar una transacción bancaria desde una PC, comunicarse con otras personas a distancia, enviar contraseñas por correo electrónico o simplemente chatear enviando mensajes con información importante ó guardar información de vital importancia en sus ordenadores o en un dispositivos de almacenamiento de información sin darse cuenta que toda esta información puede ser interceptada por intrusos que utilizan dicha información para dañar la integridad o causar otros daños a las personas.

Es de aquí que surge la importancia de conocer el área de la criptografía esta técnica busca mantener la integridad de la información por medio del cifrado, esto se refiere a la codificación del texto plano de la información convirtiéndolo a un texto cifrado por medio de claves o símbolos que sean incomprensibles para probables intrusos y brindar seguridad a las comunicaciones y a la información.

La Criptografía es el arte de ocultar y cifrar mensajes con símbolos, números o caracteres que sean ininteligibles al leerlos.

La seguridad de una información debe basarse sobre el tamaño de las claves utilizadas a la hora de encriptar y no sobre los algoritmos de encriptación aunque los algoritmos deben de ser seguros.

Para conocer un poco esta técnica se investigaron una serie de programas en los cuales cada uno de ellos tiene características diferentes. Por ejemplo encriptan documentos, programas y texto además crean particiones encriptadas que se comportan como un disco duro donde se puede almacenar la información recopilada en una investigación para protegerla.

Algunos de los programas de esta área son: TrueCrypt**,** AxCrypt**,** Paranoic Encryption, Encryton click, VsEncryptor, Password decryptor, Paragon encrytor disk SE, Hideit! Pro.

FORMAS DE CIFRADO DE ENCRIPTACIÓN

SIMÉTRICO: Cuando utiliza la misma clave para cifrar y descifrar.

Utiliza una clave para la encriptación y desencriptación del mensaje. Esta clave se debe intercambiar entre los equipos por medio de un canal seguro. Ambos extremos deben tener la misma clave para cumplir con el proceso. (Pachuca, Criptografia Simétrica y asimétrica)

Algoritmos de cifrado de encriptación simétrica

- **DES:** Se trata de un sistema de cifrado simétrico por bloques de 64 bits, de los que 8 bits (un byte) se utilizan como control de paridad (para la verificación de la integridad de la clave). Cada uno de los bits de la clave de paridad (1 cada 8 bits) se utiliza para controlar uno de los bytes de la clave por paridad impar, es decir, que cada uno de los bits de paridad se ajusta para que tenga un número

impar de “1” dentro del byte al que pertenece. (Kioskea) Por lo tanto, la clave tiene una longitud “útil” de 56 bits, es decir, realmente sólo se utilizan 56 bits en el algoritmo.

El algoritmo se encarga de realizar combinaciones, sustituciones y permutaciones entre el texto a cifrar y la clave, asegurándose al mismo tiempo de que las operaciones puedan realizarse en ambas direcciones (para el descifrado).

- **Triple DES:**

  En criptografía el Triple DES se llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES, fue desarrollado por IBM en 1998.

  TDES (en castellano: Triple Estándar de Cifrado de Datos), una alternativa para DES. El Triple DES está desapareciendo (Sánchez, 2012) lentamente, siendo reemplazado por el algoritmo AES. Sin embargo, la mayoría de las tarjetas de crédito y otros medios de pago electrónicos tienen como estándar el algoritmo Triple DES (anteriormente usaban el DES). Por su diseño, el DES y por lo tanto el TDES son algoritmos lentos. AES puede llegar a ser hasta 6 veces más rápido y a la fecha no se ha encontrado ninguna vulnerabilidad.

- **AES:** (Advanced Encryption Standard - AES). También conocido como Rijndael. Esquema de cifrado por bloques, que fue adoptado como estándar de cifrado por el gobierno estadounidense. Reemplaza progresivamente a su

predecesor (DES y Triple DES). AES es uno de los algoritmos más utilizados en criptografía simétrica.

Fue anunciado el 26 de noviembre de 2001 por el NIST (Instituto Nacional de Estándares y Tecnología), luego de un proceso de estandarización que duró 5 años. Se transformó en estándar el 26 de mayo de 2002.

El cifrador fue desarrollado por Joan Daemen y Vincent Rijmen, dos criptólogos de Bélgica, estudiantes de la Universidad Católica de Leuven.

AES es una red de sustitución-permutación, no una red de Feistel (como DES). AES también es mucho más rápido que DES, tanto en hardware como en software y además, requiere poca memoria. (Alegsa, 1998-2012)

- **MD5:** Las siglas en ingles de este algoritmo significan Message-Digest algorithm 5 (algoritmo de resumen del mensaje 5) es un algoritmo de reducción criptográfico de 128 bits.
- **SHA1:** (Secure Hash Algorithm, Algoritmo de *Hash* Seguro). Es un algoritmo de encriptación de 160 bits (20 bytes), y se basa en principios parecidos a los usados por el profesor Ronald L. Rivest del MIT en el diseño de los algoritmos de resumen de mensaje MD4 y MD5.
- **BLOWFISH: S**egún (Technologies) (llave de 448 bits) es un algoritmo de encriptación rápido y fuerte. Su creador es Bruce Schneier, uno de los más prestigiosos criptógrafos.

- **RC5:** Es un sistema de cifrado el cual fue diseñado por Ronald Rivest en 1994, en sustitución del algoritmo RC4 y ofrece diversos tamaños de bloques de 32, 64 o 128 bits para la encriptación.

ASIMÉTRICO: También llamada asimétrica, se basa en el uso de dos claves diferentes, claves que poseen una propiedad fundamental: una clave puede desencriptar lo que la otra a encriptado. Una de las claves de la pareja, llamada clave privada, es usada por el propietario para encriptar los mensajes, mientras que la otra, llamada clave pública, es usada para desencriptar el mensaje. (Pachuca)

Algoritmos de cifrado de encriptación simétrica

- **RSA:** 1978 apareció el algoritmo de clave pública creado por Rivest, Shamir y Adelman es por esto que recibe el nombre de RSA. Este algoritmo se usaba en el año 2002 para proteger los códigos de las armas nucleares de Estados Unidos y Rusia.

2.1.5.3 Esteganografía

La Esteganografía proviene del griego que steganos significa, encubierto con el sentido de oculto y graphos significa escritura, del cual nace el término steganography (Esteganografía) que es el arte de escribir de forma oculta.

Esteganografía es la parte de la criptografía que se encarga de estudiar y aplicar ciertas técnicas que permiten ocultar mensajes o archivos sensibles (privado), dentro de otros, los cuales son llamados portadores. Portador es aquel conjunto de datos que son

alterados para incorporar la información que se quiere mantener en secreto, de este modo se consigue que la información sensible no sea percibida su presencia, es decir que la Esteganografía trata de ocultar un mensaje dentro de otro de esta forma se establece un canal que encubre la información la cual pasará inadvertida para las terceras personas que tengan el acceso a esta canal que en este caso será al portador de la información oculta la cual solo podrá ser recuperada por un usuario legítimo.

La Esteganografía en ocasiones suele confundirse con la criptografía debido a que ambas tratan los procesos de protección a la información pero son disciplinas diferentes, tanto en su forma de implementación como en el objetivo que poseen, sin embargo la Criptografía y la Esteganografía suelen complementarse dando un nivel de protección superior cuando el mensaje a Esteganografíar sea previamente encriptado, de este modo al haber un intruso no solo tendrá que advertir la presencia del mensaje, sino que al llegar a obtener la información esta estaría cifrada.

Las técnicas de la criptografía "revuelven" la información su objetivo es que al ser encontrada no sea posible comprenderla. Por otro lado la Esteganografía "camuflagea" la información para esconder la existencia y hacerla pasar como invisible, de esta manera oculta el hecho de que se está enviando un mensaje. Un mensaje encriptado levanta sospechas, pero un mensaje oculto o invisible no lo hace.

En la Esteganografía clásica se pretendía únicamente en que se desconociera el canal encubierto bajo uso.

La Criptografía se empezó a manifestar en la antigüedad, en la antigua Grecia. Donde se cuentan historias de cómo escribían mensajes en tablas que luego eran cubiertas con cera, de tal forma que no se percibían los mensajes de esta manera al ser interceptadas las tablas los enemigos no tenían percepción del mensaje oculto.

Otro de los métodos utilizados durante siglos consistía en tatuar al mensajero generalmente esclavo, en la cabeza rapada, con el tiempo el pelo crecería ocultando el mensaje dejándolo oculto y el esclavo estaba listo para ser mandado a su receptor con la instrucción que rasurara su cabeza.

Durante este periodo también se utilizaba otra sencilla y eficaz técnica, al enviarse textos con inocentes mensajes, pero al extraer una letra concreta de cada palabra se podía componer otra frase corta que era el verdadero significado del mensaje.

Tintas invisibles se han usado a lo largo de la historia y hasta en la actualidad, las más básicas son con alto contenido de carbono como la leche, orina, jugo de limón, jugo de naranja, jugo de manzana, jugo de cebolla, soluciones azucaradas, miel diluida, coca cola diluida, vino, vinagre, etc. Básica mente con cualquiera de las “tintas” que se mencionan anteriormente sean utilizadas, al calentar la superficie de donde se escribió el mensaje invisible, el carbono reaccionara haciendo aparecer el mensaje en un tono café. Las “tintas” más sofisticadas aparecen al aplicar una reacción química, o al ser expuestas a un cierto tipo de luz como luz infrarroja (IR), luz ultravioleta (UV).

Esta rama de la informática forense ha estado presente en nuestra civilización desde tiempos inmemorables y ha sido empleada por agencias militares y de inteligencia, la policía, organizaciones criminales y terroristas.

La Esteganografía volvió a tener un gran auge a partir de 1990 con la llegada de las computadoras. La tecnología digital proporciona nuevas formas de aplicar las técnicas esteganográficas. Lo más común y más utilizada es ocultar texto en imágenes, de manera que sea imposible siquiera detectar que en la imagen existe un mensaje oculto, a no ser que se tengan conocimientos en el proceso de inversión.
Para la computadora una imagen es una serie de números que representan la intensidad de los colores en pixeles.

Almacenar la información que va a ser escondida en una imagen requiere de dos archivos. El primero es la imagen "inocente" que será nuestra portador y alojará la información que queremos esconder. El segundo archivo es el mensaje (la información a esconder). Un mensaje puede ser texto plano, un texto encriptado, otra imagen o cualquier cosa que pueda ser llevado a bits, hoy en día, todo.

Dentro de los programas de la Esteganografía se tienen: Camouflaje, XioSteganography, FileInyector, Spimage 2, PlaingSight, PicCrypt, Hide&Reveal, HIP (Hide In Picture), PixelCryptor.

2.1.5.4 Sniffer de red

Es un programa que es utilizado para monitorear y canalizar el tráfico en una red, dando la posibilidad de observar los paquetes que fluyen de un lado a otro. En un segmento de red sin un switch o enrutador de paquetes, todo el tráfico destinado a una máquina es enviado a todos los integrantes del segmento, pero puesto a que las direcciones IP no coinciden con las del paquete transmitido, estas simplemente los rechazan. (Cano, 2009)

Para conseguir esto el Sniffer le dice a la computadora que deje de ignorar todo el tráfico no destinado al equipo y preste atención a este tráfico, esto es conocido como poner en estado "confuso" a la NIC (Network Interface Card).

En la actualidad la seguridad en las redes es de mucha importancia, porque toda la información que se transmite a través de éstas algunas veces puede ser utilizada para realizar delitos informáticos o para fines de lucro.

Una vez que la NIC está en este estado "confuso" se necesitarán los privilegios de administrador (ROOT), de ésta manera la computadora puede ver todos los datos transmitidos por la red es entonces cuando el programa comienza a hacer una lectura de toda la información entrante a la computadora por la tarjeta de red.

Con esto el Sniffer puede observar el equipo de origen, de destino y el número de puerto.

En otras palabras un programa para Sniffer de red puede ver la información intercambiada entre dos computadoras.

El uso que se le da a éste tipo de aplicaciones es importante ya que gracias a ellos podemos ayudar a que nuestra red sea más segura, hacer pruebas y así poder tener un muy buen resultado, el problema viene cuando otros usuarios lo utilizan para cometer delitos informáticos, ya que con éste tipo de programas se puede obtener información confidencial.

Algunas de las aplicaciones utilizadas en los Sniffer de red son: IP Sniffer, Free IP tools, SwitchSniffer, wireshark portable, Lycos WLAN Sniffer, ComViewforWifi, Wefi.

Los principales usos que se le pueden dar son:

- Captura de contraseñas enviadas sin cifrar y nombres de usuario de una la red. Esta capacidad es utilizada en muchas ocasiones por atacantes de sistemas.
- Análisis de fallos para detectar problemas en la red, tales como: Que un ordenador llamado M no puede establecer comunicación con el ordenador N
- Medición del tráfico, mediante el cual es posible descubrir cuellos de botella en la red.
- En aplicaciones cliente-servidor un Sniffer permite analizar la información en vivo que se transmite por la red.

Algunos Sniffer trabajan sólo con paquetes de TCP/IP, pero hay otros más sofisticados que son capaces de trabajar con un número más amplio de protocolos e incluso en niveles más bajos tal como el de las tramas del Ethernet.

Un Sniffer es de gran importancia en la administración de una red, con fines de seguridad y funcionalidad, pero hay que tomar en cuenta de que es una herramienta que puede ser de doble filo, ya que algún usuario puede utilizarla con un fin inadecuado y pueda tomar ventaja de este.

Es importante conocer el funcionamiento de estas aplicaciones para poder utilizarlas en una determinada circunstancia.

2.1.5.5 Backdoors

Una puerta trasera o Backdoors en inglés es en un sistema informático una secuencia exclusiva dentro de un código de programación ya existente, mediante el cual se pueden violar los escudos de seguridad para acceder libremente al sistema. Aunque estas puertas pueden ser utilizadas para fines maliciosos y espionaje no siempre son para usadas para ello, también pueden ser utilizadas para espionaje en casos de hechos delictivos para esclarecer el hecho.

Un Backdoor es un programa que se introduce en la computadora y establece una puerta trasera a través de la cual es posible controlar el sistema afectado, en algunos casos con conocimiento por parte del usuario o sin conocimiento del mismo. Una

puerta trasera (backdoors) en un sistema de inicio de sesión puede tomar la forma de un riguroso código de usuario y una contraseña que le da acceso al sistema.

Aunque el número de puertas traseras en los sistemas que utilizan software propietario (software cuyo código fuente no está disponible públicamente), no se le atribuye, no dejan expuestos con frecuencia. Los programadores han logrado incluso instalar secretamente grandes cantidades de código benigno en los programas; también es posible crear una puerta trasera sin modificar el código fuente de un programa, o incluso modificar después de la compilación.

Estos programas son diseñados para abrir una "puerta trasera" en nuestro sistema para darle acceso al creador del Backdoor al sistema y hacer lo que desee con él. Con este software se puede obtener contraseñas, archivos y todo lo que el atacante desea. El objetivo del Backdoor es lograr una gran cantidad de computadoras infectadas para disponer de ellos libremente hasta el punto de formar redes.

Dentro de los programas para Backdoors se tienen: TeamViewer 8

2.1.5.6 Hackeo de redes

Para lograr comprender lo básico de la estructura de un asalto a una sección TCP (protocolo de control de transmisión), se debe tener conocimiento de algunos conceptos básico como WEP (Wired Equivalent Privacy), WPA (Works Projects Administration), TCP (Protocolo de Control de Transmisión), host y router.

El proceso de hackeo consiste en dos fases, primero capturar el paquete con la clave correspondiente encriptado, para acceder a la red WLAN de otro usuario y utilizar su ancho de banda para conectarse a internet, y segundo paso desencriptar esta clave.

El objetivo de una sesión TCP es coordinar múltiples conexiones TCP concurrentes entre un par de host. Una aplicación típica de una sesión TCP es la coordinación entre conexiones TCP concurrentes entre un servidor web y un cliente, en donde las conexiones correspondientes se le atribuyen componentes de una página web. (Padmanabhan)

La monitorización de redes consiste en detectar las redes inalámbricas cuyas ondas ha podido detectar nuestro captador de señal wifi.

Existen dos tipos de cifrado de contraseña para protegerla, estos son WEP y WPA. Hay que decir que es más seguro el cifrado WPA, por lo tanto más difícil de desencriptar.

Dentro de los programas para Hackeo de redes se tienen: Backtrack, commviewforWifi, Wirelesssnif, Wifiway, SwifiKeygen, Aircrack.

2.1.5.7 Escala de privilegios

Esto se refiere a ejecutar comandos desde una capa nivel inferior con el fin de aumentar los privilegios de un usuario o apoderarse de otro para poder tener acceso a él sin necesidad de tener permisos de administrador o una contraseña.

Aparentemente cuando se encuentra con un ordenador al que no se puede acceder por una contraseña o por cambiar algo por lo permisos de administrador se cree que no se puede ingresar pero ningún sistema operativo es perfecto, agradable a la vista, funcional, que consuma pocos recurso y sobre todo seguro.

La seguridad es algo que no se ha podido contrarrestar ya que en el mundo de la informática siempre existirán personas que día con día crean y prueban todo tipo de software.

Cuando se intenta entrar a un sistema se busca algún hueco en la seguridad del mismo, esto sucede cuando el sistema no está actualizado por lo cual no es totalmente seguro y es más fácil explotar alguna vulnerabilidad no parcheada del sistema permitiendo el acceso al intruso con permisos de administrador.

Es por eso que es necesario mantener actualizado el sistema operativo para mantenerse seguro aunque no totalmente y evitar que sea fácil ingresar al equipo como administrador.

2.1.5.8 Ethical hacking

Cuando las organizaciones empezaban a incrementar sus procesos informatizados dentro de su sistema de información, sus administradores y analistas técnicos eran los responsables de buscar las brechas de seguridad para solucionarlas, por lo tanto no se tenía una idea concreta acerca de la seguridad de la información o de las intrusiones de terceros que se pudieran presentar en sus sistemas.

Con el paso del tiempo dichas organizaciones crecieron y se multiplicaron lo cual hizo que surgiera la necesidad de informatizar aún más, tomando a Internet como plataforma para sus movimientos informáticos, de este modo las comunicaciones interpersonales, transacciones y flujo digital de todo tipo y nivel de importancia, por lo tanto muchos más datos quedaron expuestos.

Por estas intrusiones se hizo necesario algún servicio profesional que minimizará estos ataques o capacitará al personal con las metodologías que usaban los intrusos, de esta manera las brechas, agujeros en el sistema podían ser descubiertas y buscar una forma de prevenir los accesos no autorizados y las vulnerabilidades. Muchos especialistas en la seguridad informática estudiaban y practicaban métodos de intrusión en sus trabajos, laboratorios o casas, empezando a brindar a las organizaciones sus servicios a modo de consultores externos y para darle un nombre formal, lo llamaron Ethical hacking lo cual incluye las denominaciones de escaneo de vulnerabilidades y test de penetración.

"Hacking" este término con el tiempo se ha ganado una reputación negativa y se asocia con actividades destructivas o indeseables, frecuentemente se ha debatido si la piratería puede ser ética dado el hecho de que cualquier acceso que no es autorizado constituye a un delito. Cuando en realidad Hacking es un término que se utiliza para describir el desarrollo rápido de nuevos programas o la ingeniería inversa de software que ya existen para mejorarlos y hacerlos más eficientes.

Ethical hacking prácticamente es el tipo de metodología que usan las hackers éticos para descubrir las vulnerabilidades que existen en algunos entornos operativos de sistemas informáticos, estos suelen emplear las mismas técnicas y herramientas que suelen utilizar los criminales, pero sus intenciones no son dañar los sistemas ni robar información manteniéndose así la integridad de su trabajo y la confidencialidad de sus sistemas. Su trabajo es evaluar la seguridad de los objetivos de la organización en respecto a su vulnerabilidad de las situaciones que se han descubierto y las recomendaciones que se dan para que se mitiguen dichas situaciones.

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

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

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

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

¿Quiénes son los Ethical Hackers?

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

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

Los piratas informáticos pueden ser clasificados en varias categorías según su perfil de actividades:

- **Los de Sombreros Blanco**: son las personas que profesan las habilidades de hackers y utilizarlas con fines defensivos. También conocido como "Los analistas de seguridad.
- **Los de Sombreros grises**: Son las personas que trabajan tanto ofensiva como defensivamente en varias ocasiones. Ellos creen que otras personas que se encuentran con la información revelada son capaces de hacer un uso juicioso de la información. Esto es discutible ya que no existe la moral universal de los valores o normas.
- **Los de sombreros negros**: se usa para describir a los individuos con habilidades extraordinarias computación, que utilizan sus conocimientos informáticos con malas intenciones, propósitos ilegales esta categoría a generalmente se asocia con actividades criminales, maliciosas y destructivas también conocidos como "Crackers".

Imagen 2.1.5.8.1

El sombrero blanco y sombrero negro
que se le atribuye al tipo de hacker

¿Por qué hacer un Ethical Hacking?

A través del Ethical Hacking (es posible detectar el nivel de seguridad interno y externo de los sistemas de información de una organización, esto se logra determinando el grado de acceso que tendría un atacante con intenciones maliciosas a los sistemas informáticos con información crítica.

Las pruebas de penetración son un paso previo a los análisis de fallas de seguridad o riesgos para una organización. La diferencia con un análisis de vulnerabilidades, es que las pruebas de penetración se enfocan en comprobar y clasificar vulnerabilidades y no tanto en el impacto que éstas tengan sobre la organización.

Estas pruebas dejan al descubierto las vulnerabilidades que pudieran ser vistas y explotadas por individuos no autorizados y ajenos a la información como: crackers, hackers, ladrones, ex-empleados, empleados actuales disgustados, competidores, etc. Las pruebas de penetración, están totalmente relacionadas con el tipo de información que cada organización maneja, por tanto según la información que se desee proteger, se determina la estructura y las herramientas de seguridad pero nunca a la inversa.

Estas pruebas de penetración permiten:

Evaluar vulnerabilidades a través de la identificación de debilidades provocadas por una mala configuración de las aplicaciones.

- Analizar y categorizar las debilidades explotables, con base al impacto potencial y la posibilidad de que la amenaza se convierta en realidad.
- Proveer recomendaciones en base a las prioridades de la organización para mitigar y eliminar las vulnerabilidades y así reducir el riesgo de ocurrencia de un evento desfavorable.

La realización de las pruebas de penetración está basada en las siguientes fases.

1. Recopilación de información
2. Descripción de la red
3. Exploración de los sistemas
4. Extracción de información
5. Acceso no autorizado a información sensible o crítica
6. Auditoría de las aplicaciones web
7. Elaboración de informes
8. Informe final (Reyes, 2010)

¿Por qué ético?

Para emular la metodología de ataque de un intruso informático y no serlo, tiene que haber ética de por medio, más allá de todas las condiciones, términos y activos que haya alrededor del caso. Imaginemos que las autoridades de un banco contratan a

alguien para que simule un robo (no a mano armada, claro está) y de ese modo se pruebe la eficiencia de su sistema de seguridad. Este supuesto ladrón profesional, luego de lograr su cometido, informa a sus dueños en detalle cómo pudo hacerlo y cómo ellos deberían mejorar su sistema de seguridad para que no volviera a pasar. Lógicamente, no se puede encargar de hacer esto una persona sin ética, alguien in moral.

La ética implica que el trabajo y la intervención del profesional en seguridad informática o de la información no comprometen de ningún modo los activos de la organización, que son los valiosos datos con los que ella cuenta.

Estos daños podrían ser hechos de varias maneras: alteración, modificando a conciencia registros o datos sensibles; borrado, destruyendo información, bases de datos o sobrescribiendo algún tipo de dato; dar a conocer información a terceros, incumpliendo las normas de confidencialidad; sustracción, robando o guardando datos en medios de almacenamiento externos. Todo esto, ya sea en la búsqueda de riesgos mediante un security assessment o comprobación de seguridad, como también en la divulgación de lo que se vió, habló, escuchó o manipuló en el transcurso, en la planificación o en el desarrollo de la tarea misma y en su análisis final. Más allá de la ética propia de cada profesional, existen conductas mínimas que éste debe cumplir:

- Hacer su trabajo de la mejor manera posible.
- Dar el mejor reporte.
- Acordar un precio justo.

- Respetar el secreto.
- No hablar mal ni inculpar a un administrador o equipo de programadores.
- No aceptar sobornos.
- No manipular o alterar resultados o análisis.
- Delegar tareas específicas en alguien más capacitado.
- No prometer algo imposible de cumplir.
- Ser responsable en su rol y función.
- Manejar los recursos de modo eficiente.

En nuestros tiempos, para la mayoría de la gente y de la prensa, la palabra hacking está ligada a delincuentes comunes, a personas de dudosa moralidad que utilizan conocimientos de informática o electrónica para delinquir. (Tori, 2008).

2.1.6 Manual

El proyecto también lo conforma un manual para el cual ha sido necesario recopilar información para la elaboración del mismo. Dicho producto se entregará en el Instituto Nacional San Luis en donde se describirá de manera detallada el uso de los software que se incorporarán en el kit de herramientas básicas.

2.1.6.1 Definición de manual

Son los documentos en los que se integra la información, instrucciones o procedimientos en forma ordenada y explicativa sobre los pasos para desarrollar tareas que se considera necesario para el buen manejo de estas.

2.1.6.2 Tipos de manuales

Según (Andres, 2013) los manuales se distinguen en:

- **Organización:** este tipo de manual resume el manejo de una empresa en forma general. Indican la estructura, las funciones y roles que se cumplen en cada área.
- **Departamental:** dichos manuales, en cierta forma, legislan el modo en que deben ser llevadas a cabo las actividades realizadas por el personal. Las normas están dirigidas al personal en forma diferencial según el departamento al que se pertenece y el rol que cumple.
- **Política:** sin ser formalmente reglas en este manual se determinan y regulan la actuación y dirección de una empresa en particular.
- **Procedimientos:** este manual determina cada uno de los pasos que deben realizarse para emprender alguna actividad de manera correcta.
- **Técnicas:** estos manuales explican minuciosamente como deben realizarse tareas particulares, tal como lo indica su nombre, da cuenta de las técnicas.
- **Bienvenida:** su función es introducir brevemente la historia de la empresa, desde su origen, hasta la actualidad. Incluyen sus objetivos y la visión particular de la empresa. Es costumbre adjuntar en estos manuales un duplicado del reglamento interno para poder acceder a los derechos y obligaciones en el ámbito laboral.
- **Puesto:** determinan específicamente cuales son las características y responsabilidades a las que se acceden en un puesto preciso.

- **Múltiple:** estos manuales están diseñados para exponer distintas cuestiones, como por ejemplo normas de la empresa, más bien generales o explicar la organización de la empresa, siempre expresándose en forma clara.
- **Finanzas:** tiene como finalidad verificar la administración de todos los bienes que pertenecen a la empresa. Esta responsabilidad está a cargo del tesorero y el controlador.
- **Sistema:** debe ser producido en el momento que se va desarrollando el sistema. Está conformado por otro grupo de manuales.
- **Calidad:** es entendido como una clase de manual que presenta las políticas de la empresa en cuanto a la calidad del sistema de operación de la empresa. Puede estar ligado a las actividades en forma sectorial o total de la organización.

Según la información anterior sobre los diferentes tipos de manuales que existen el que más se adapta a las necesidades para el manual que se le entregará a la institución es el manual de procedimientos por lo tanto se escogió este manual porque en él se especifican los pasos para realizar una actividad o tarea de manera adecuada sirviéndonos de guía para el uso correcto de las aplicaciones comprendidas en el kit de herramientas básicas de software.

2.1.6.3 Elaboración de un manual

- Visualizar que tipo de manual se realizará.
- Un editor de texto.

- Hacer un diagrama de flujo para verificar como ira estructurado el manual
- Realizar el procedimiento para crear el manual y describirlo en un texto siguiendo como base el diagrama que se ha hecho previamente.
- Agregar las versiones de los programas a utilizar ya que estos varían de una versión a otra.
- Añadir imágenes ilustrativas de los diversos pasos; entre menos alteradas estén la imágenes mejor.
- Escribir los pasos con el texto de explicación de las imágenes del manual.

2.1.7 CD interactivo

2.1.7.1 Definición de CD interactivo

Es una herramienta innovadora que puede estar conformado por imágenes, sonidos, texto, video, animaciones, gráficos, etc. Que muestra el contenido grabado en él de manera moderna e interesante para el usuario.

2.1.7.2 Funcionamiento de un CD interactivo

Es un CD que posee un archivo Autorun que hace que una vez insertado en el CD ROM se reproduzca automáticamente.

Este CD interactivo contendrá tutoriales y el manual en digital para mayor comprensión de los diferentes programas que poseerá el Kit de herramientas básicas de software.

Para llevar a cabo este proyecto se desarrollaron tres productos con los cuales se alcanzaron los objetivos propuestos en este proyecto.

2.2 Marco teórico de la solución

2.2.1 Productos que conforman el proyecto

2.2.1.1 Kit de herramientas básicas de software

El cual consta de 13 programas los cuales han sido distribuidos por las siguientes áreas: Esteganografía, Criptografía, Backdoors, Escala de privilegios, Ethical hacking, Recuperadores de información, Sniffer de red y Hackeo de redes.

Programas que conforman el kit de herramientas básicas de software			
Áreas	**Programa 1**	**Programa 2**	**Programa 3**
Recuperadores de información	Recuva	Wise Data Recovery	Easy Recovery
Esteganografía	Camouflage	Spimage 2	Fileinyector
Criptografía	AxCrypt	TrueCrypt	Paranoic encryption
Backdoors	Teamviewer 8		
Sniffer de red	free IP tools		
Escala de privilegios	Hiren´s boot CD		
Hackeo de redes	Backtrack		

2.2.1.2 manual de usuarios de instalación de programas de informatica forense

MANUAL DE PROGRAMAS SOBRE INFORMÁTICA FORENSE

CONTENIDO DEL MANUAL

1. RECUPERADORES DE INFORMACIÓN

1.1 CONCEPTO

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

1.2 PROGRAMAS

1.2.1 RECUVA

1.2.2 WISE DATA RECOVERY

1.2.3 EASY RECOVERY

Recuva Manual

- ✓ Instalación
- ✓ Recuperación de datos

INSTALACIÓN

Paso 1: Introducir el cd del kit de herramientas en el reproductor de CD ó DVD e insertar la bandeja. (Ver imagen 1)

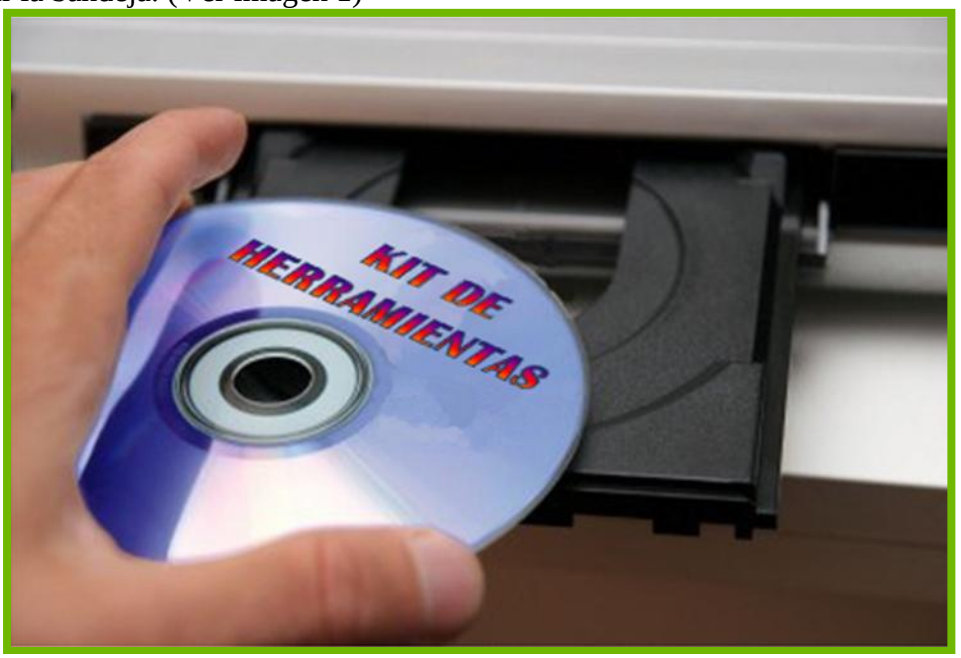


Imagen 1

Paso 2: Aparece la siguiente ventana, dar clic en el botón programas. (Ver imagen 2)

Imagen 2

Paso 3: Dar clic en el botón de esteganografía. (Ver imagen 3)

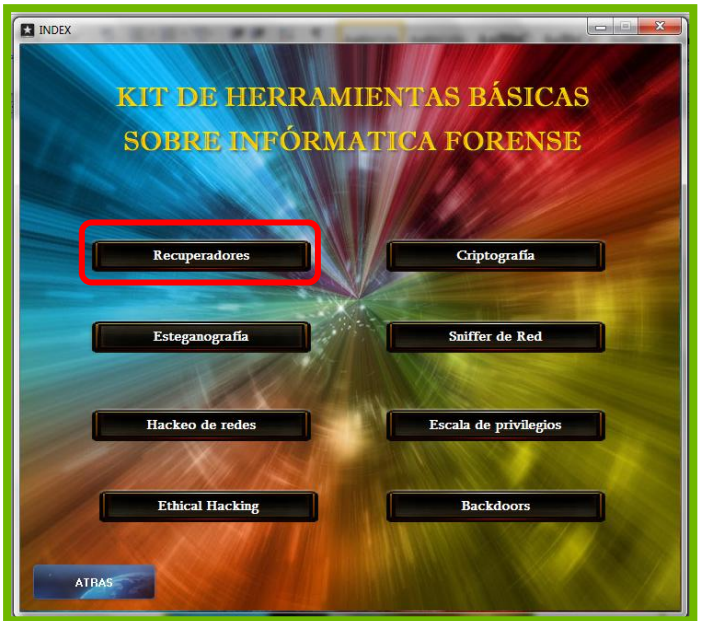


Imagen 3

Paso 4: Ubicar el instalador para comenzar la instalación del programa de recuperación de datos y dar clic. (Ver imagen 4)

Imagen 4

Paso 5: Seleccionar el idioma deseado para el programa, luego dar clic en Next y aparecera nuevamente la pantalla de instalacion y dar clic en siguiente. (Ver imagen 5)

Imagen 5

Paso 6: En esta ventana se puede configurar la instalación del programa Recuva para seleccionar algunas opciones adicionales. (Ver imagen 6)

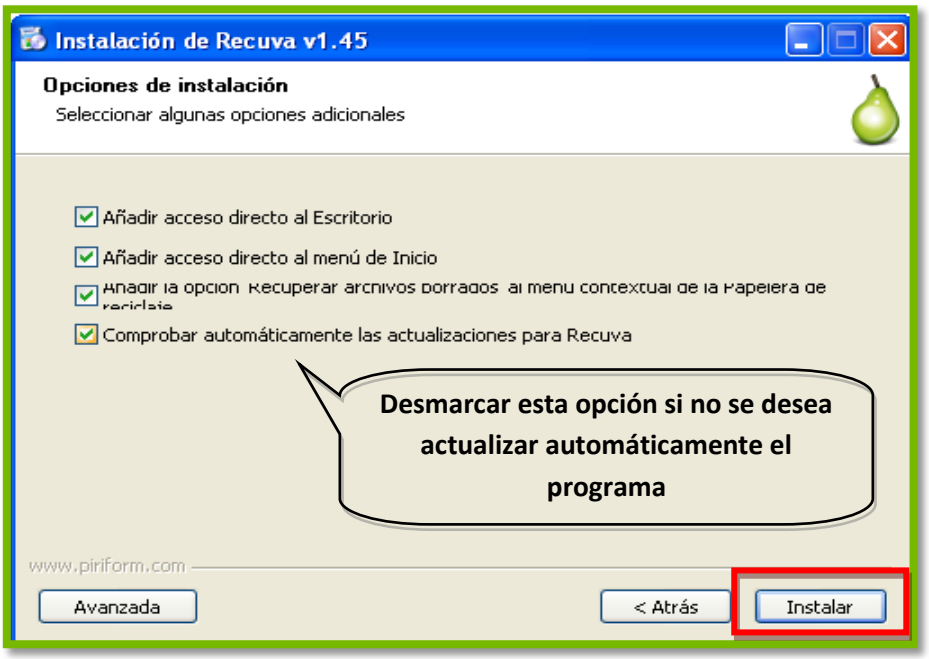


Imagen 6

Paso 7: Esperar mientras el programa se instala. (Ver imagen 7)

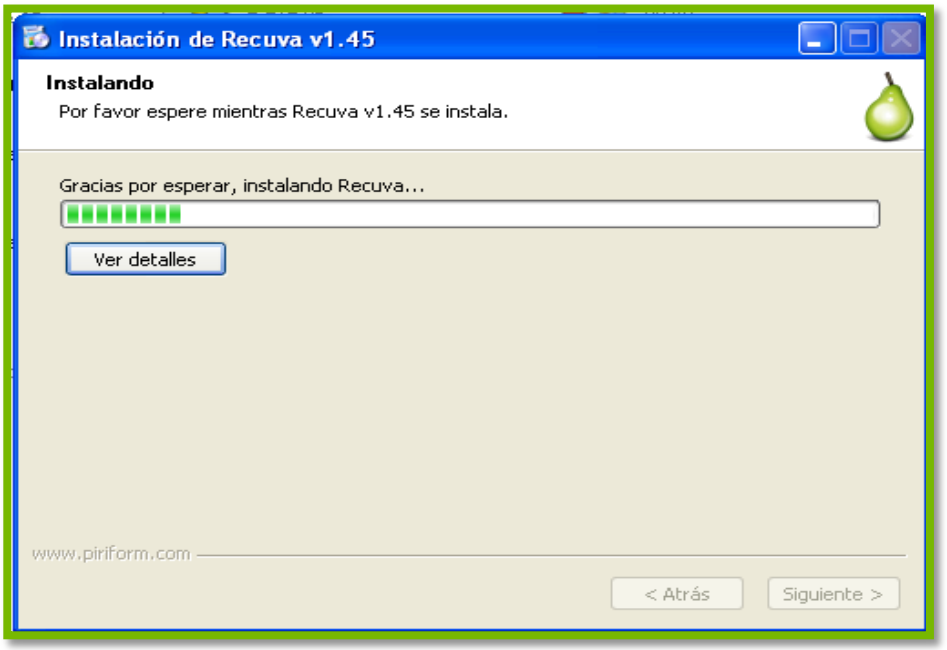


Imagen 7

Paso 8: Desmarcar la opción seleccionada y dar clic en la opción terminar para finalizar la instalación del programa Recuva (Ver imagen 8)

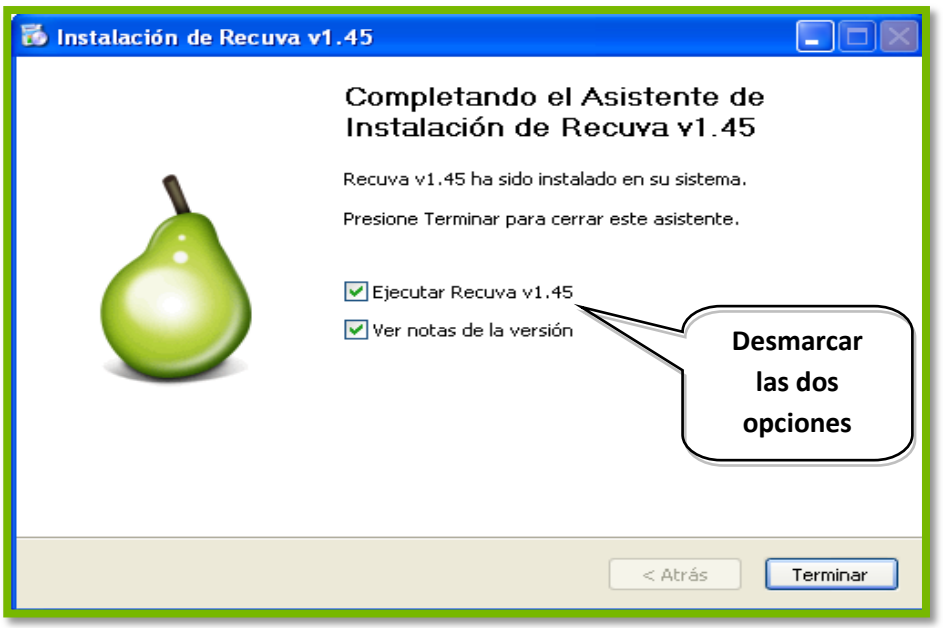


Imagen 8

RECUPERACIÓN DE DATOS

Paso 9: Esta es la ventana de opciones personalizadas de Recuva. (Ver imagen 9)

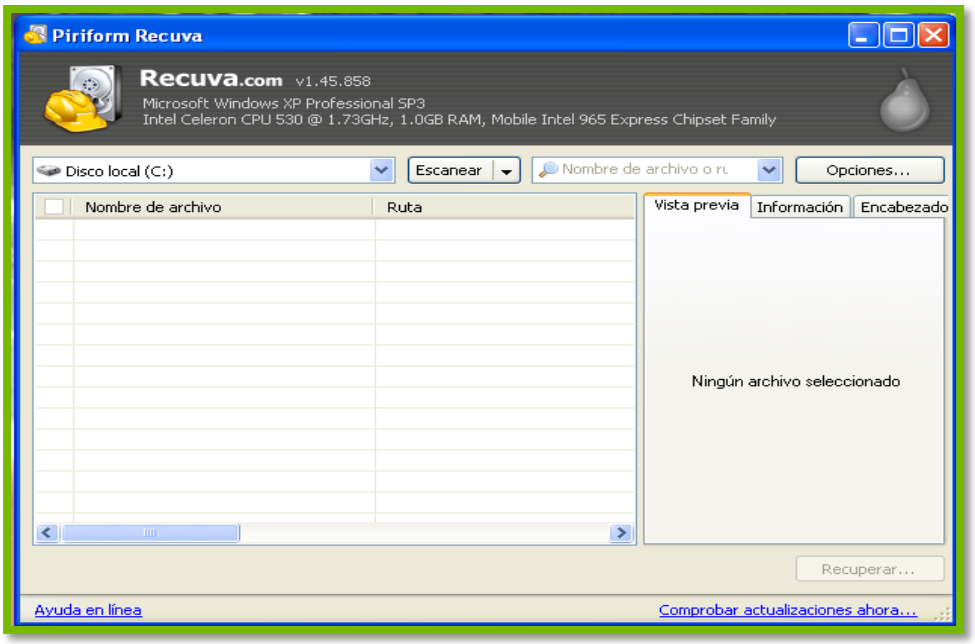


Imagen 9

Paso10: Seleccionar la unidad a escanear para la recuperación de datos y dar clic en escanear. (Ver imagen 10)

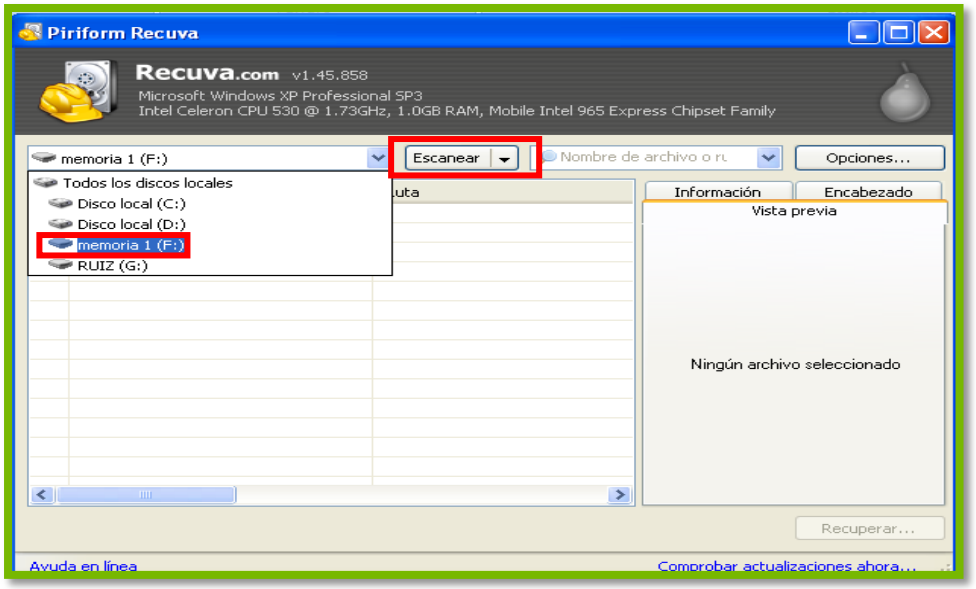


Imagen 10

Paso 11: A continuación aparecerán todos los datos recuperados en la unidad analizada. (Ver imagen 11)

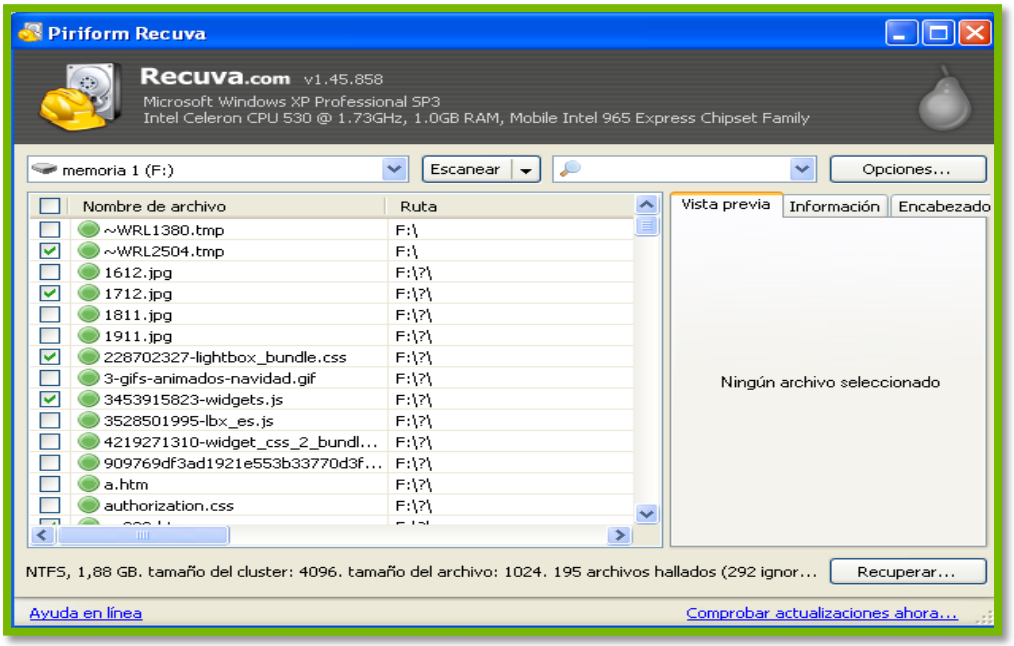


Imagen 11

Paso 12: Esta opción sirve para encontrar solo un tipo de archivo: fotos, videos, documentos, etc. Se selecciona y dar clic en escanear, cuando aparezcan los archivos recuperados se marcan y dar clic en recuperar. (Ver imagen 12)

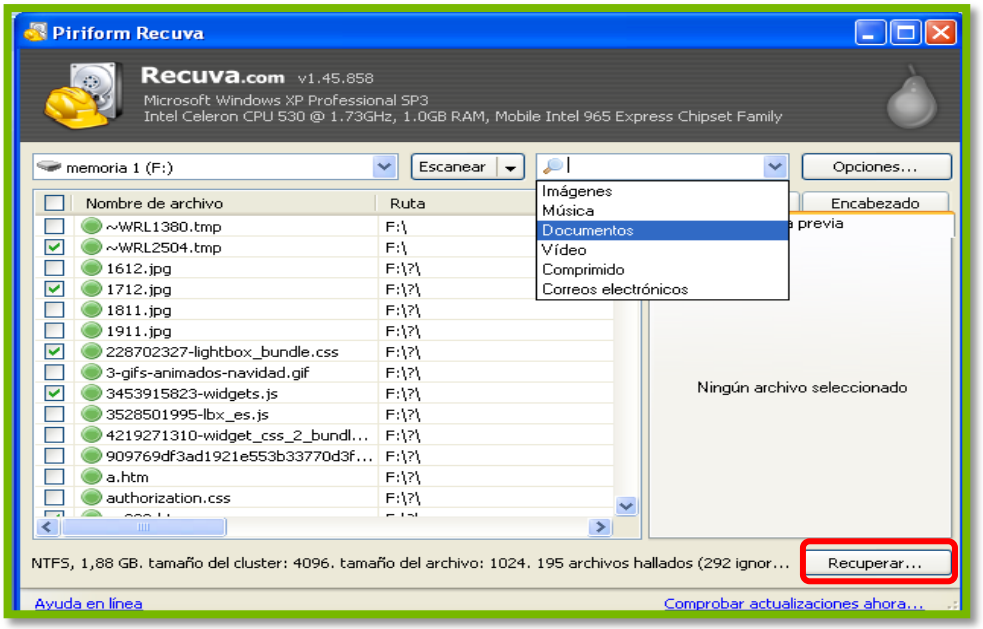


Imagen 12

Paso 13: Cuando aparecen los archivos encontrados se selecciona una unidad diferente de la que se está analizando y guardar los archivos recuperados. (Ver imagen 13)

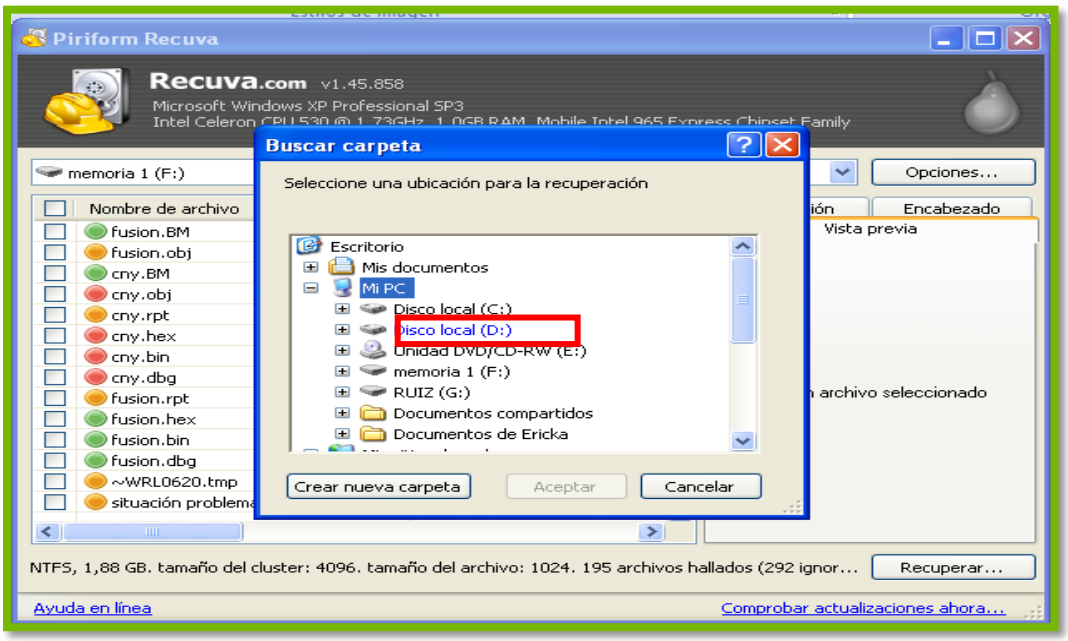


Imagen 13

Paso 14: Luego muestra la información de los archivos recuperados. (Ver imagen 14)

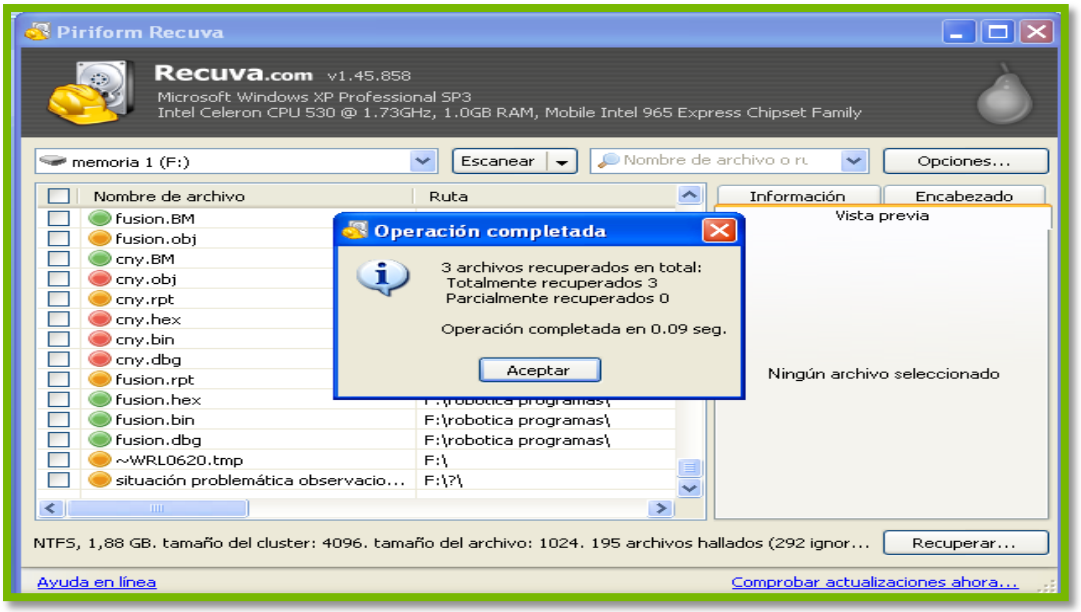


Imagen 14

Wise Data Recovery Manual

- ✓ **Instalación**
- ✓ **Recuperación de datos**

INSTALACIÓN

Paso 1: Introducir el cd del kit de herramientas en el reproductor de CD o DVD e introducir la bandeja. (Ver imagen 1)

Imagen 1

Paso 2: Aparece la siguiente ventana, dar clic en el botón programas. (Ver imagen 2)

Imagen 2

Paso 3: Dar clic en el boton de esteganografia. (Ver imagen 3)

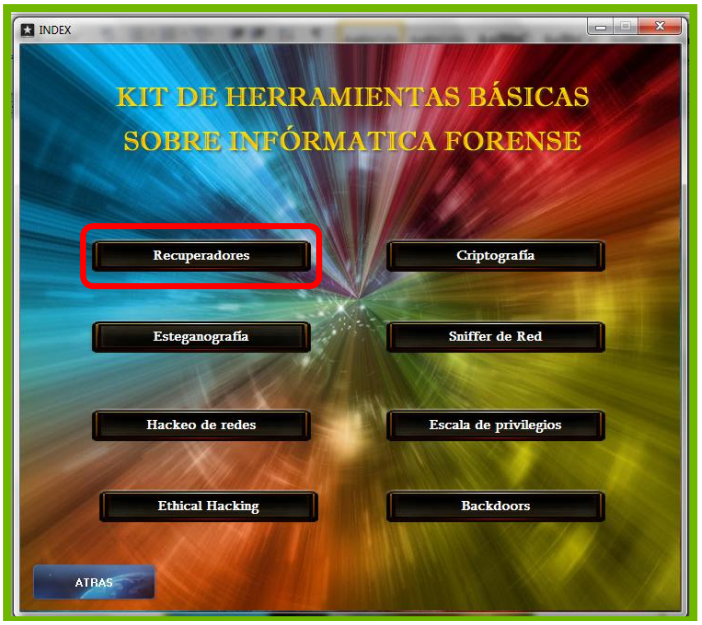


Imagen 3

Paso 4: Ubicar el instalador del Wise Data Recovery y dar doble clic para comenzar el proceso de instalación. (Ver imagen 4)

Imagen 4

Paso 5: Aparecerá una ventana de instalación y dar clic en la opción Next (Siguiente). (Ver imagen 5)

Imagen 5

Paso 6: Aparecerá el contrato de licencia y seleccionar la opción acepto los términos de licencia luego dar clic en Next (Siguiente). (Ver imagen 6)

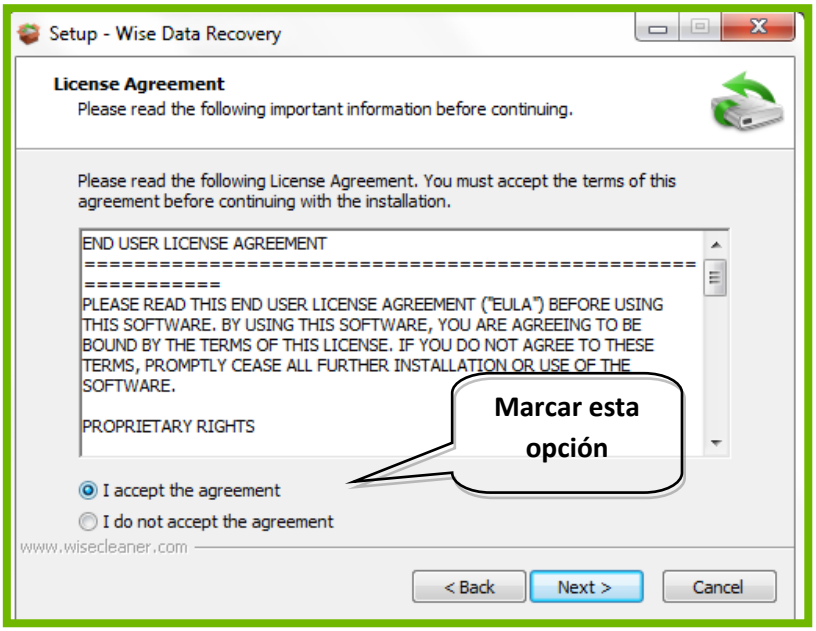


Imagen 6

Paso 7: Elegir la ubicación para la instalación del programa, con el icono Browse se puede visualizar las opciones de carpetas donde se puede instalar el programa. Dar clic en Next (Siguiente), para continuar con el proceso. (Ver imagen 7)

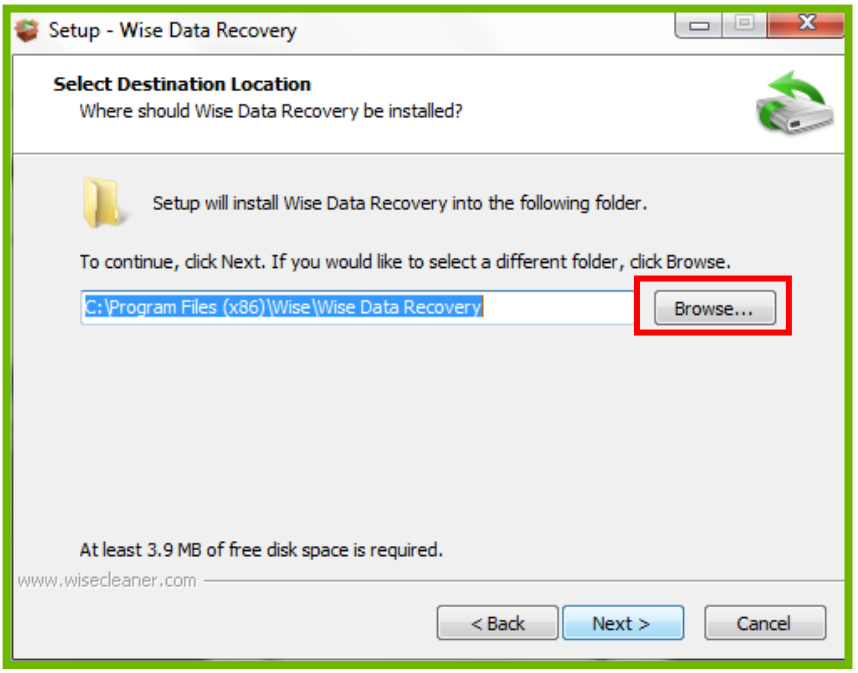


Imagen 7

Paso 8: Al igual que en la ventana anterior aquí se puede elegir la ubicación del programa, y para continuar darle clic en la opción Next (Siguiente). (Ver imagen 8)

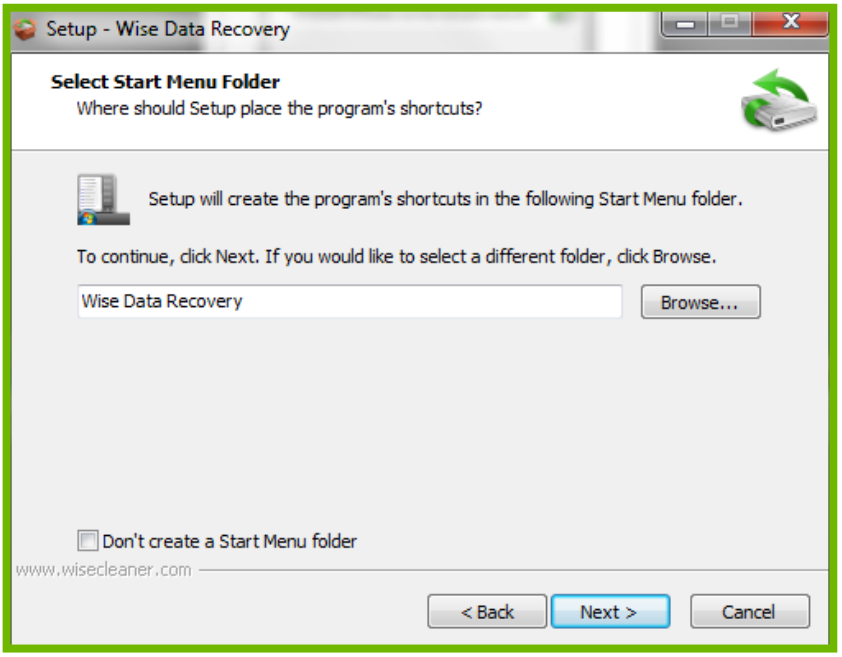


Imagen 8

Paso 9: En esta ventana se puede marcar o desmarcar la opción para crear un icono en el escritorio, luego dar clic en Next (Siguiente). (Ver imagen 9)

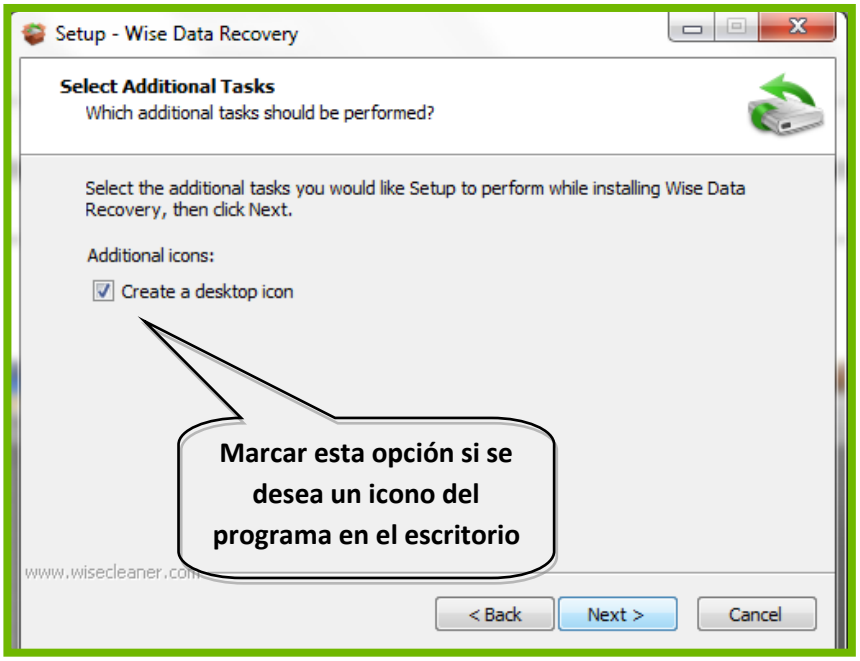


Imagen 9

Paso 10: Aquí se indica la dirección en donde se instalará el programa, luego dar clic en Install (Instalar). (Ver imagen 10)

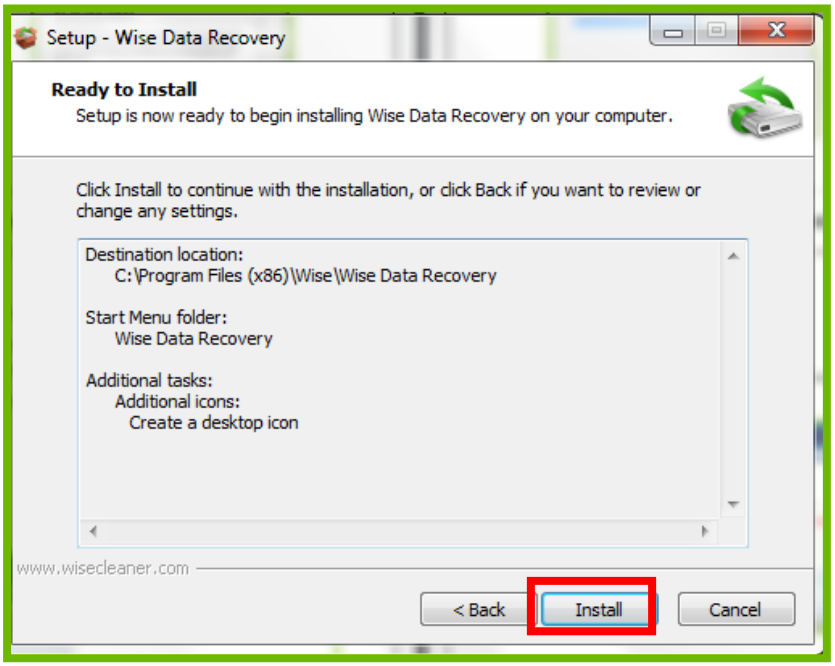


Imagen 10

Paso 11: Esperar unos segundos a que cargue la instalación (Ver imagen 11)

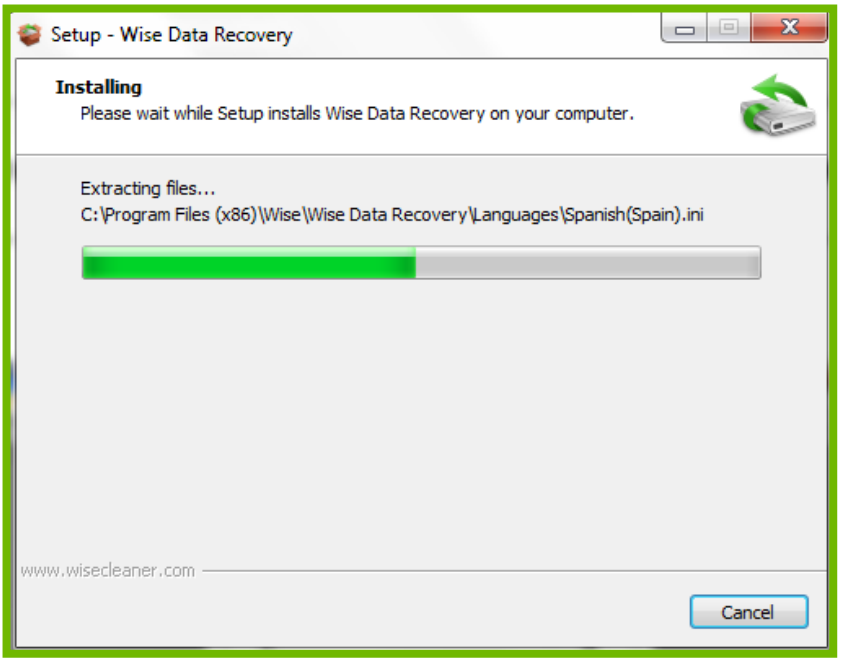


Imagen 11

Paso 12: Desmarcar la casilla de descarga y luego dar clic en Finish (Finalizar). (Ver imagen 12)

Imagen 12

RECUPERAR ARCHIVOS

Paso 13: Interfaz principal del Wise Data Recovery. (Ver imagen 13)

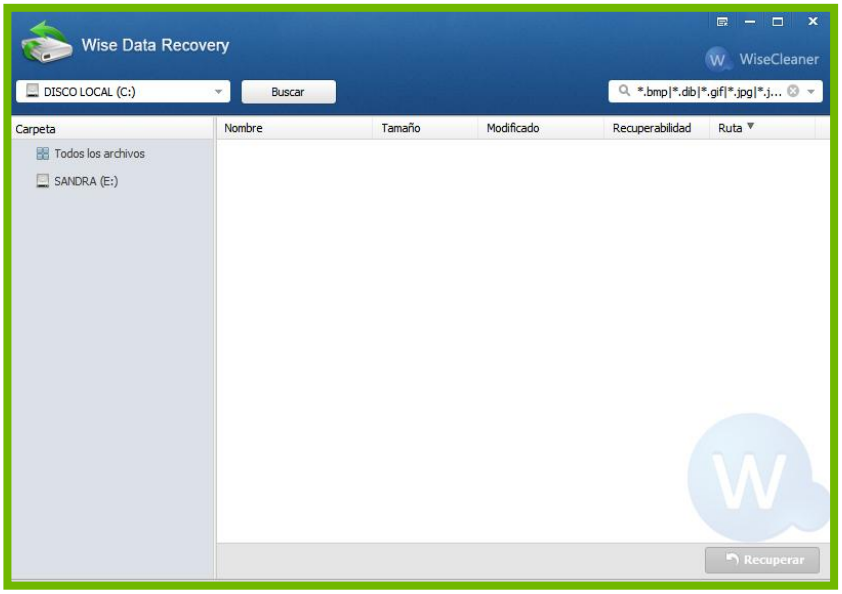


Imagen 13

Paso 14: Con esta herramienta podemos especificar el tipo de archivo que se desea recuperar o colocar una palabra clave para su búsqueda. (Ver imagen 14)

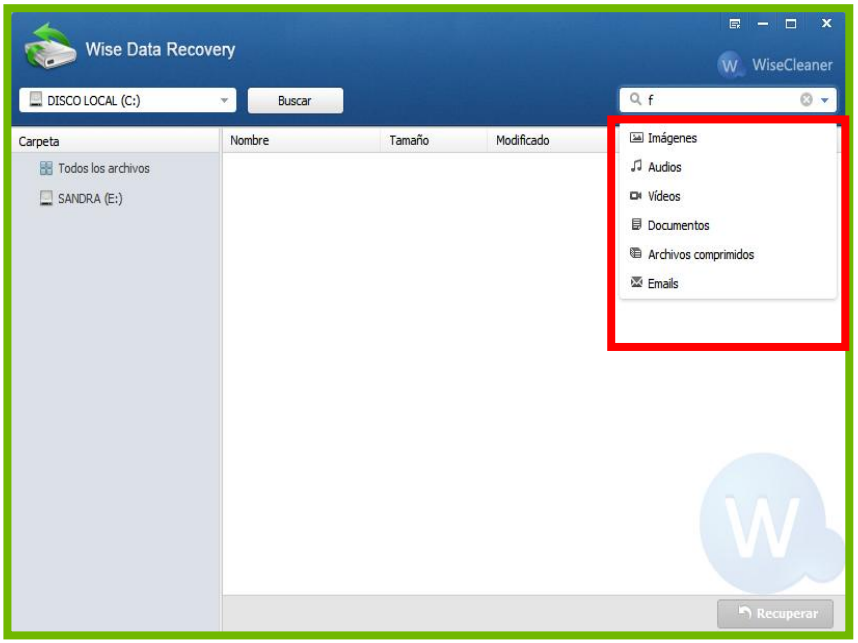


Imagen 14

Paso 15: Clic en buscar y a continuación se presentara el listado de archivos que han sido borrados. (Ver imagen 15)

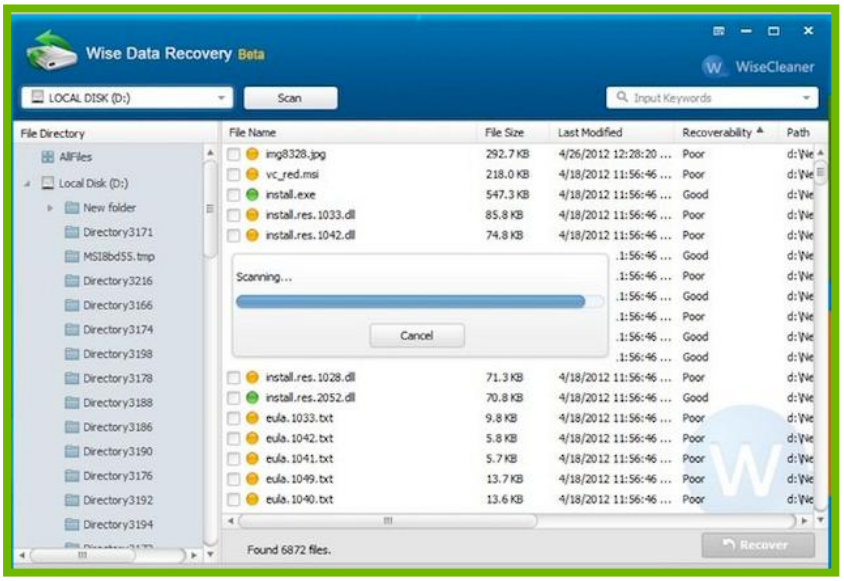


Imagen 15

Paso 16: En este listado de archivos muestra cuales son recuperables y los que son irrecuperables, se marca el archivo que se desea recuperar y luego clic en recuperar. (Ver imagen 16)

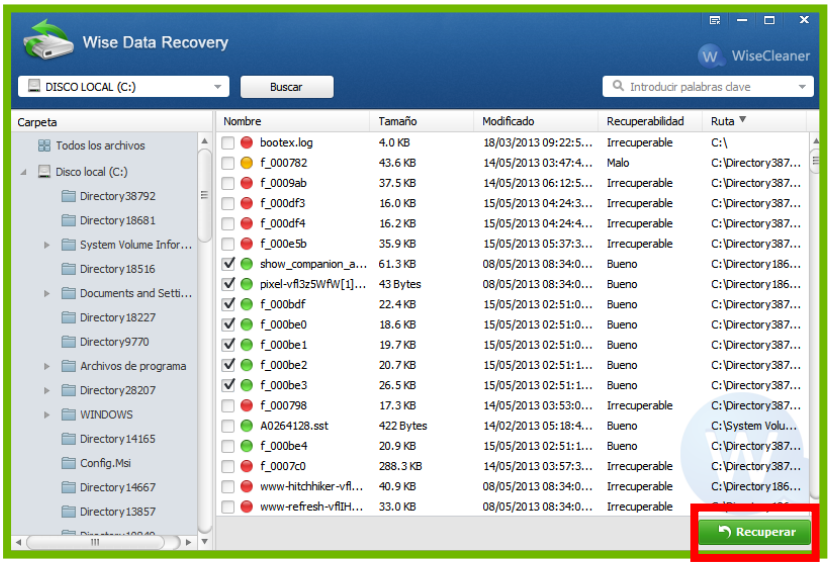


Imagen 16

Paso 17: En el siguiente cuadro se pide un destino para guardar el archivo recuperado.

(Ver imagen 17)

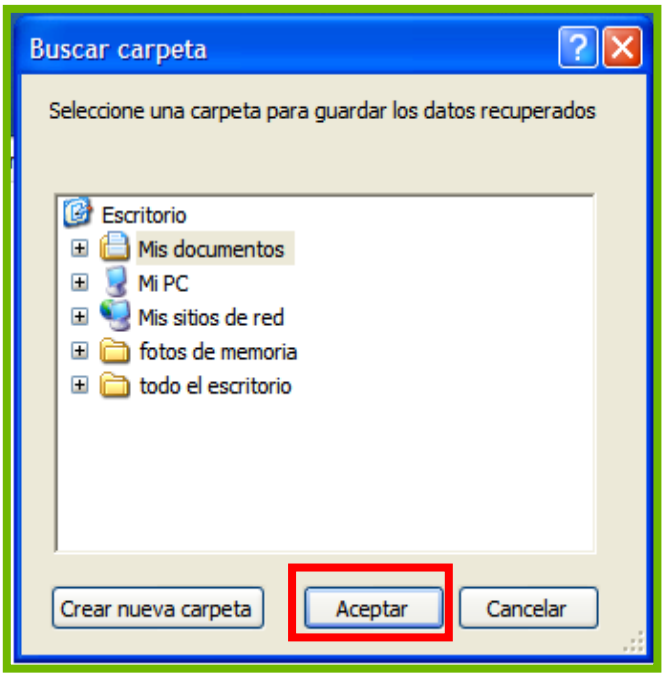


Imagen 17

Paso 18: Clic en aceptar para terminar la recuperación de datos. (Ver imagen 18)

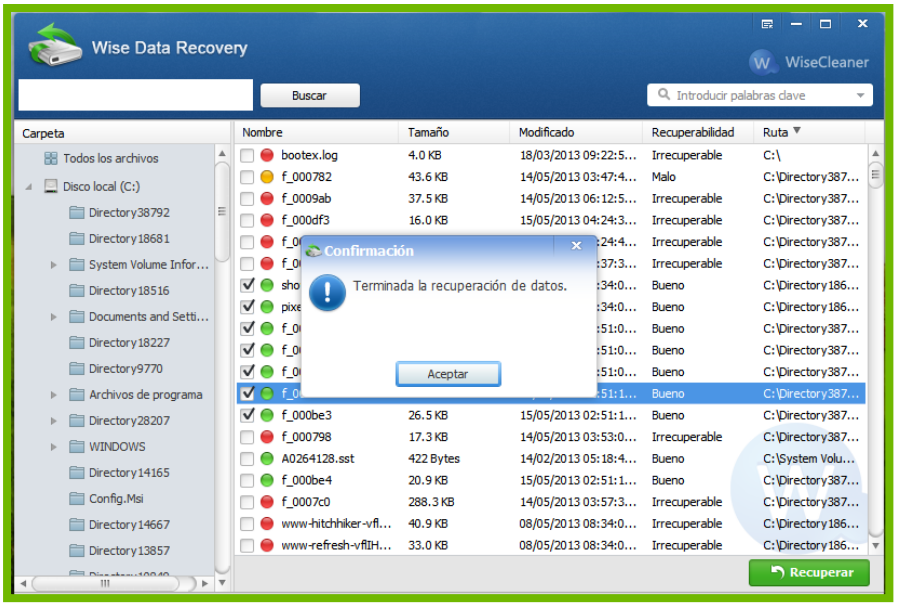


Imagen 18

EasyRecovery Manual

- ✓ Instalación
- ✓ Recuperación de datos

INSTALACIÓN

Paso 1: Introducir el cd del kit de herramientas en el reproductor de CD o DVD e introducir la bandeja. (Ver imagen 1)

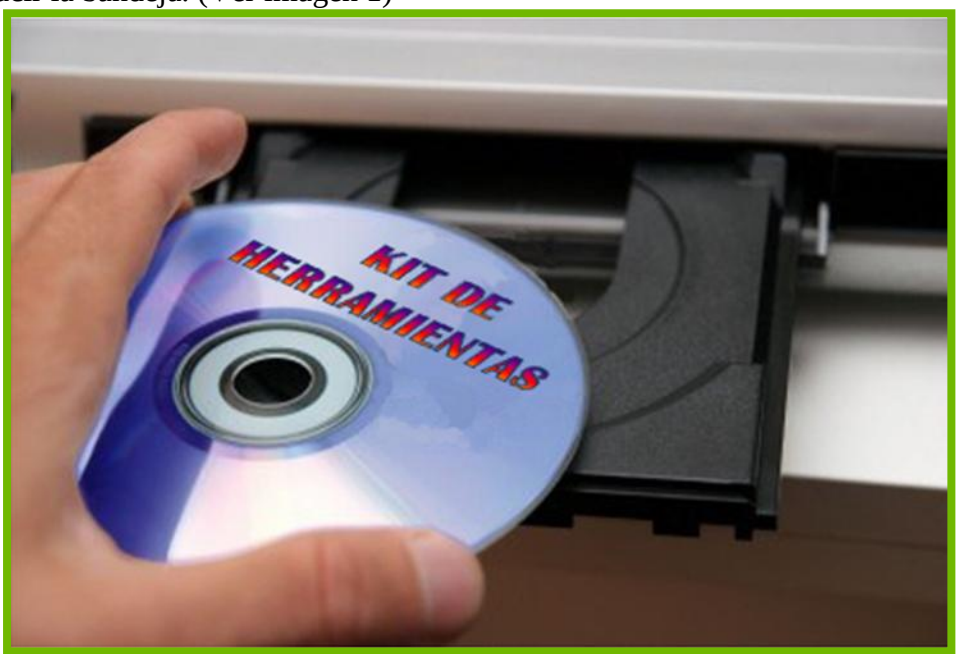


Imagen 1

Paso 2: Aparece la siguiente ventana, dar clic en el botón programas. (Ver imagen 2)

Imagen 2

Paso 3: Dar clic en el botón de esteganografia. (Ver imagen 3)

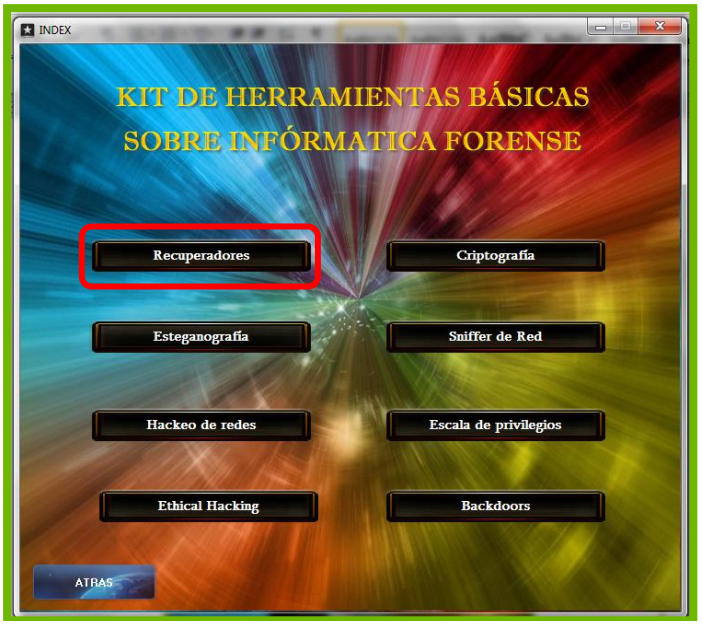


Imagen 3

Paso 4: Ubicar icono de instalación del EasyRecovery. (Ver imagen 4)

Imagen 4

Paso 5: Interfaz principal del EasyRecovery donde se le indica las acciones a realizar en este caso se eligen las opciones sobre recuperar datos. (Ver imagen 5)

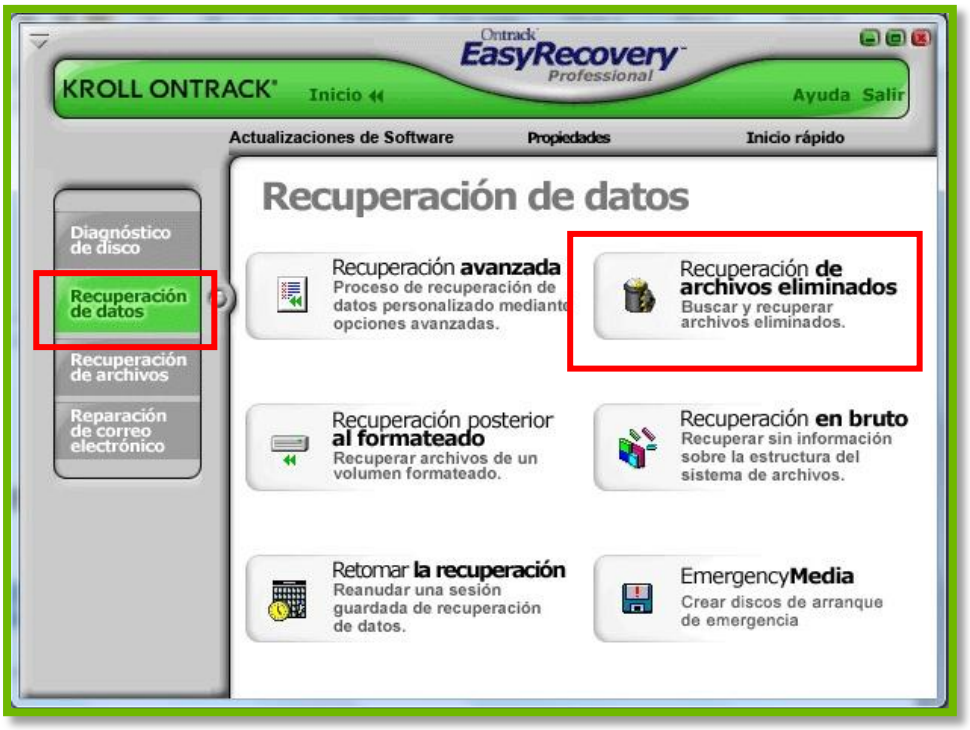


Imagen 5

A continuación se presenta el siguiente cuadro de dialogo dar clic en ok. (Ver imagen 6)

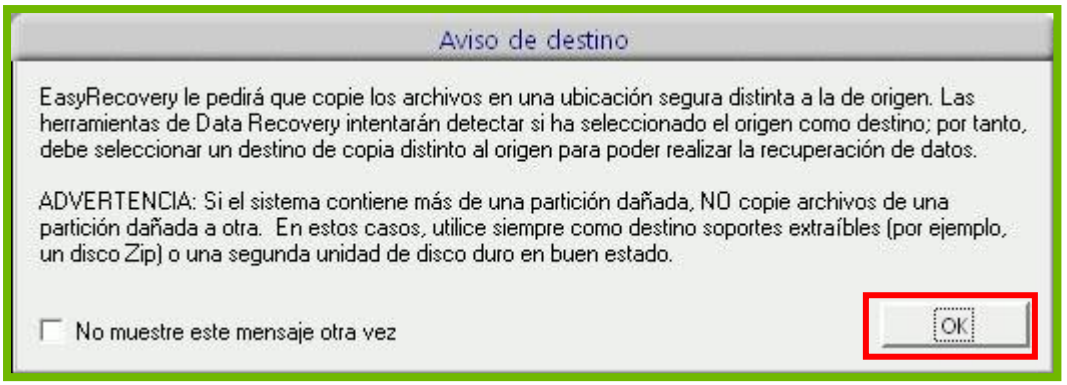


Imagen 6

Paso 6: Se elige la unidad donde estaban los archivos eliminados y opcionalmente la extensión (aunque no es necesario).Y clic en siguiente. (Ver imagen 7)

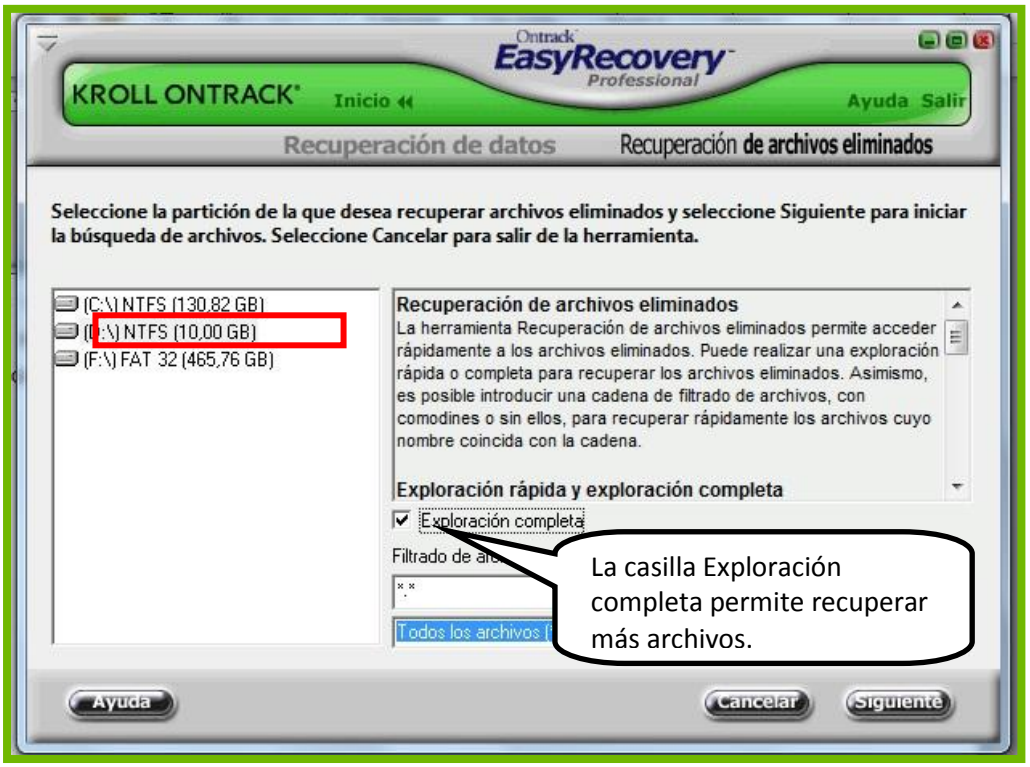


Imagen 7

Un aspecto importante es la limitación de la búsqueda. Se puede refinar la búsqueda introduciendo conceptos de búsqueda. Se recomienda cuando se recuerda el nombre del archivo o sólo cuando se recuerda una parte del nombre. Por ejemplo, para el uso de marcadores de posición:

Si se busca *.doc encontrará todos los archivos que inicien por cualquier nombre, con el tipo de extensión DOC. (Ver imagen 8)

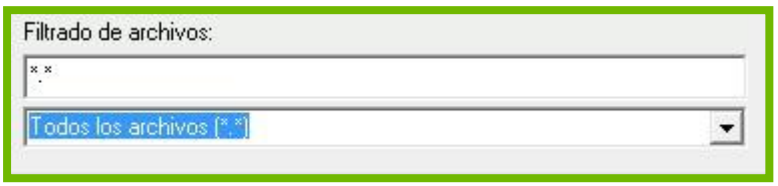


Imagen 8

Paso 7: Clic en Siguiente para iniciar la búsqueda. Esta herramienta analiza las unidades seleccionadas una detrás de la otra. Especialmente en el caso de unidades de disco duros de mayor capacidad, cuando no se introducen conceptos de búsqueda, es posible que el proceso tarde un poco más. (Ver imagen 9)

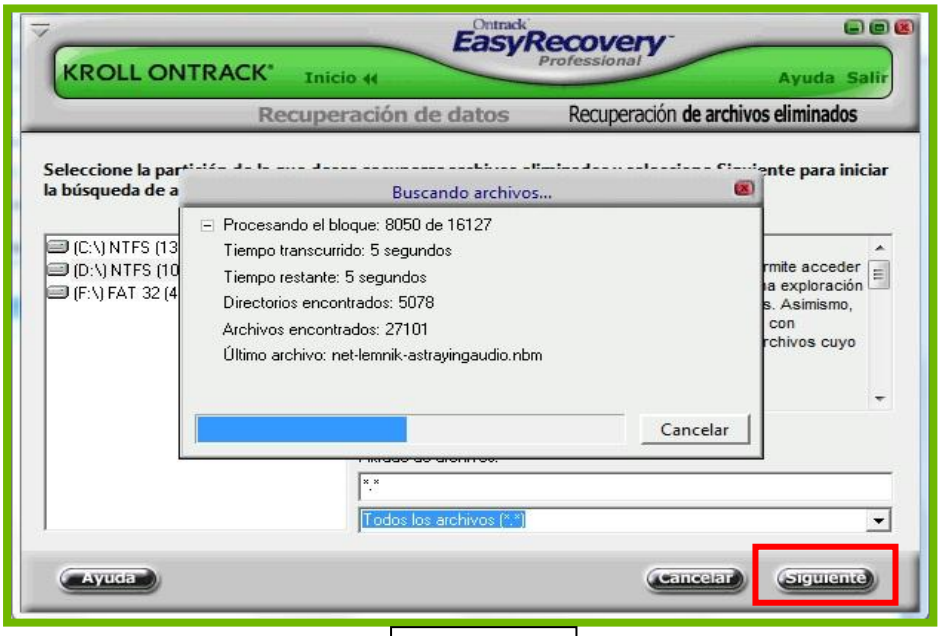


Imagen 9

Paso 8: Una vez terminado este proceso presenta el siguiene cuadro en el cual se debe elegir lo que se quiere recuperar.marcar la casilla de lo que se quiere recuperar. (Ver imagen 10)

Imagen 10

Paso 9: En este cuadro pide el destino de recuperación se debe colocar un destino diferente de donde se está recuperando y comienza la recuperación de datos. (Ver imagen 11)

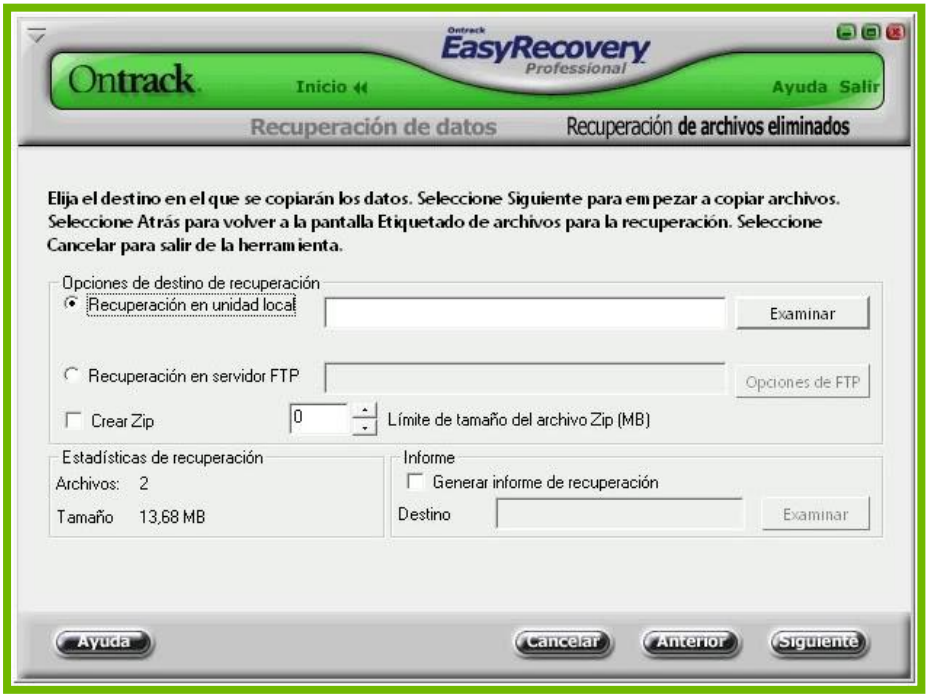


Imagen 11

Paso 10: Se elige un desino diferente a la unidad que se está analizando y dar clic en aceptar. (Ver imagen 12)

Imagen 12

Paso 11: Se debe esperar unos minutos para esperar el proceso de recopilación de datos. (Ver imagen 13)

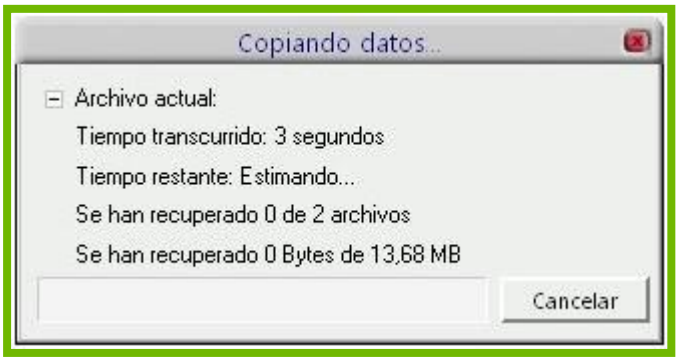


Imagen 13

Paso 12: El programa finaliza su tarea de recuperación de datos con un informe y se puede elegir lo que se desea hacer con el informe: guardar o imprimir. (Ver imagen 14)

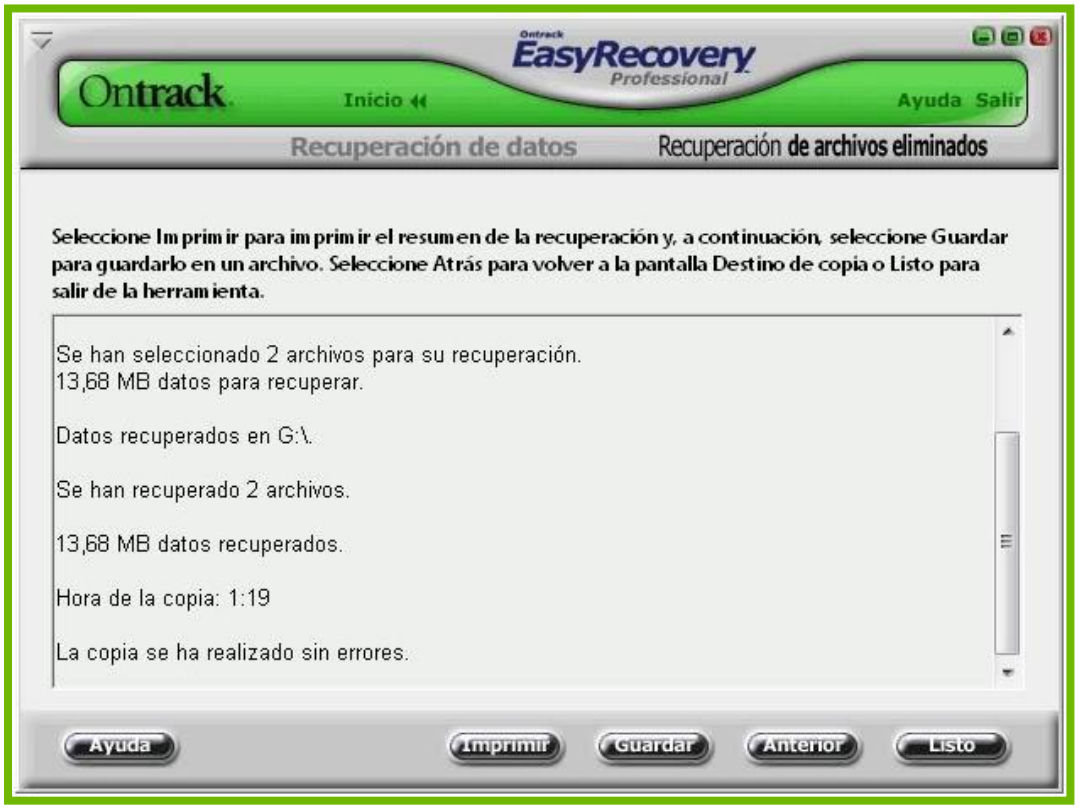


Imagen 14

2. ESTEGANOGRAFÍA

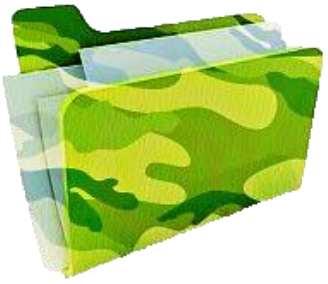
2.1 CONCEPTO

La palabra Esteganografía literalmente significa escritura encubierta. Esteganografía es el arte o ciencia de comunicar de manera oculta un mensaje.

2.2 PROGRAMAS

2.2.1 HIREN´S BOOT CD

2.2.2 CAMOUFLAGE



2.2.3 FILE INYECTOR

Spimage 2 Manual

- ✓ **Instalación**
- ✓ **Codificar**
- ✓ **Descodificar**

INSTALACIÓN

Paso 1: Introducir el cd del kit de herramientas en el reproductor de CD o DVD e introducir la bandeja. (Ver imagen 1)

Imagen 1

Paso 2: Aparece la siguiente ventana, dar clic en el botón programas. (Ver imagen 2)

Imagen 2

Paso 3: Dar clic en el boton de esteganografia. (Ver imagen 3)

Imagen 3

Paso 4: Ubicar el icono de instalación del programa Spimage y dar clic. (Ver imagen 4)

Imagen 4

Paso 5: Dar clic en Next (siguiente) para iniciar la instalación. (Ver imagen 5)

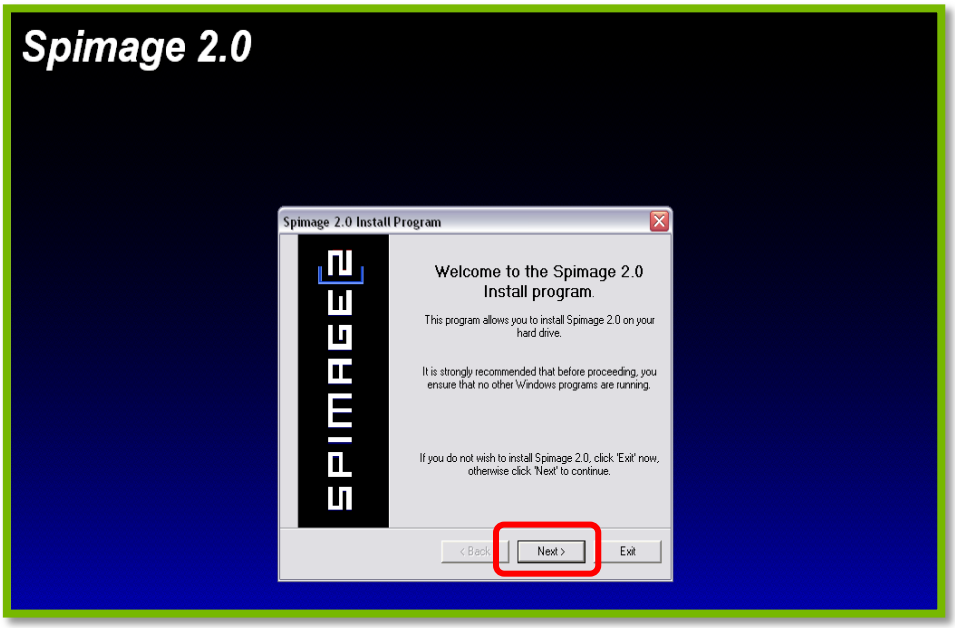


Imagen 5

Paso 6: Marcar la primera casilla para aceptar términos y condiciones, dar clic en Next, (Ver imagen 6)

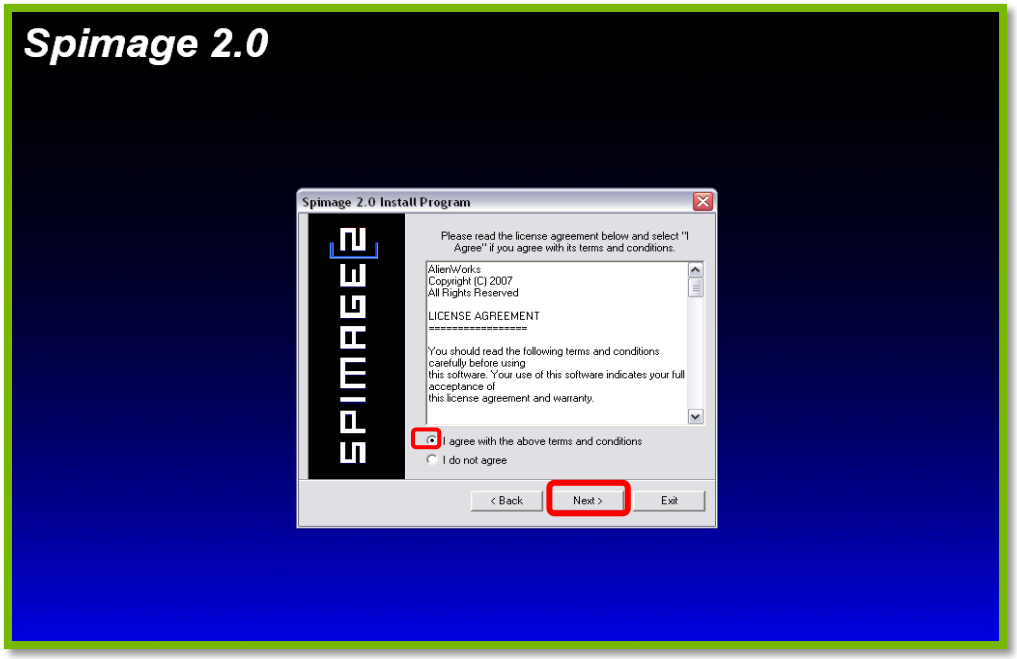


Imagen 6

Paso 7: Seleccionar la ubicación en donde se instalará el programa, clic en Next (siguiente). (Ver imagen 7)

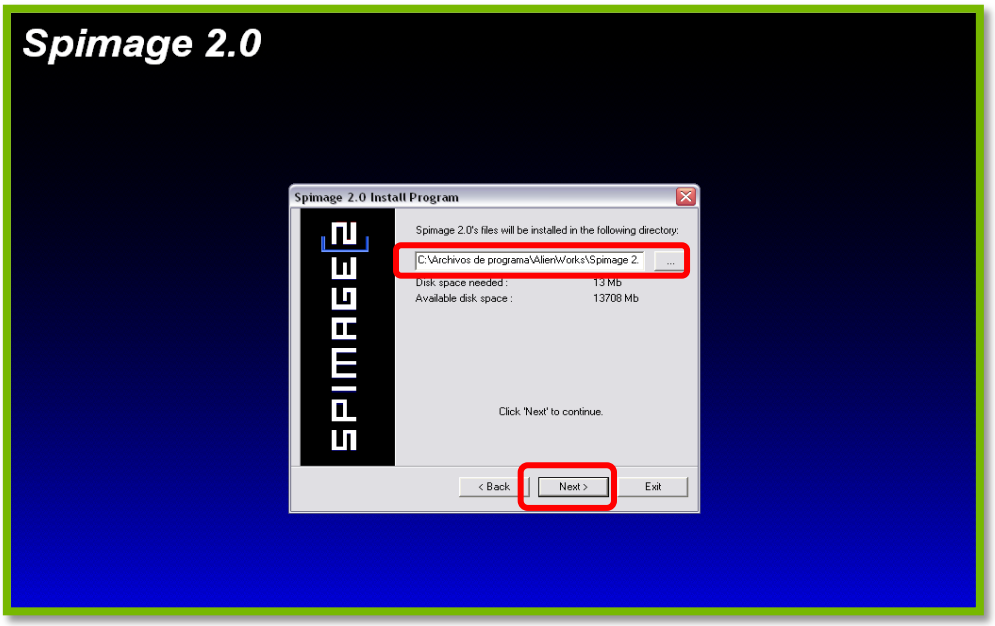


Imagen 7

Paso 8: Dar clic en si para crear un nuevo directorio. (Ver imagen 8)

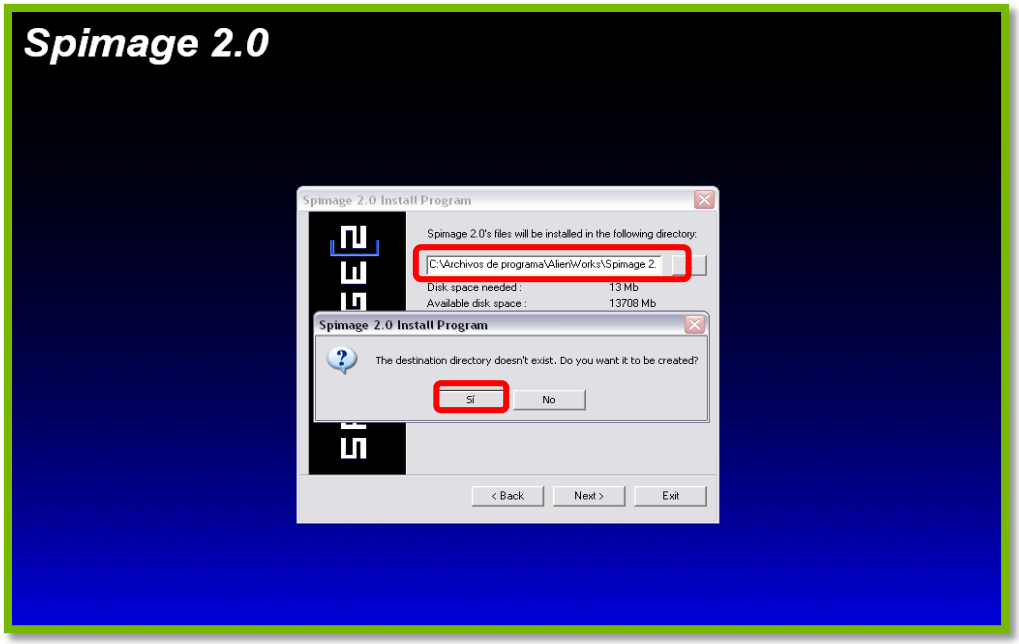


Imagen 8

Paso 9: Dar clic en Start para iniciar la instalación. (Ver imagen 9)

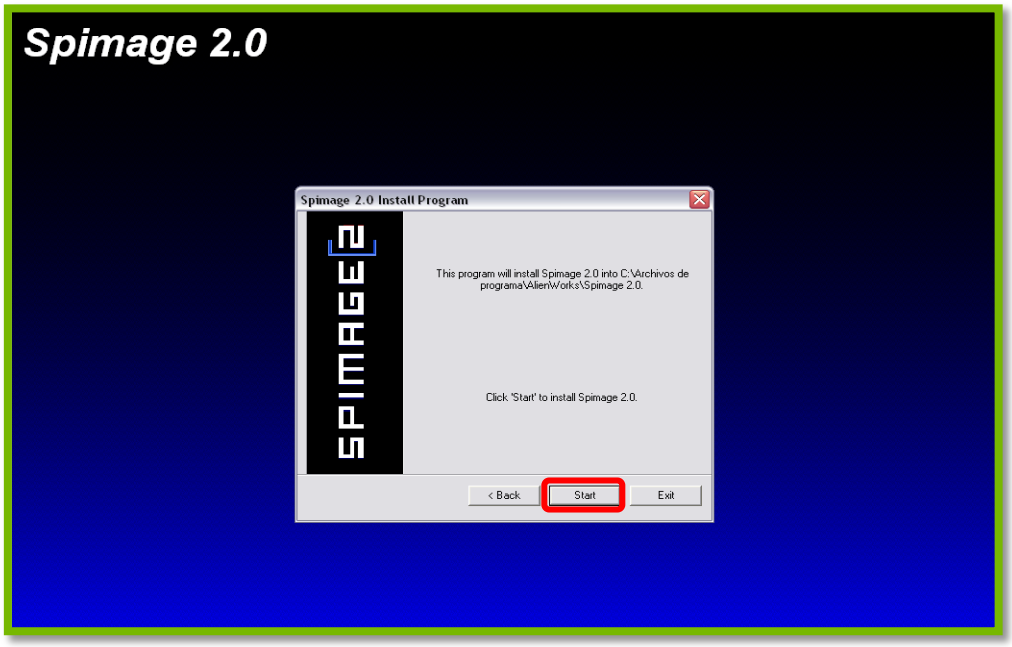


Imagen 9

Paso 10: Esperar unos segundos para que se complete la instalación. (Ver imagen 10)

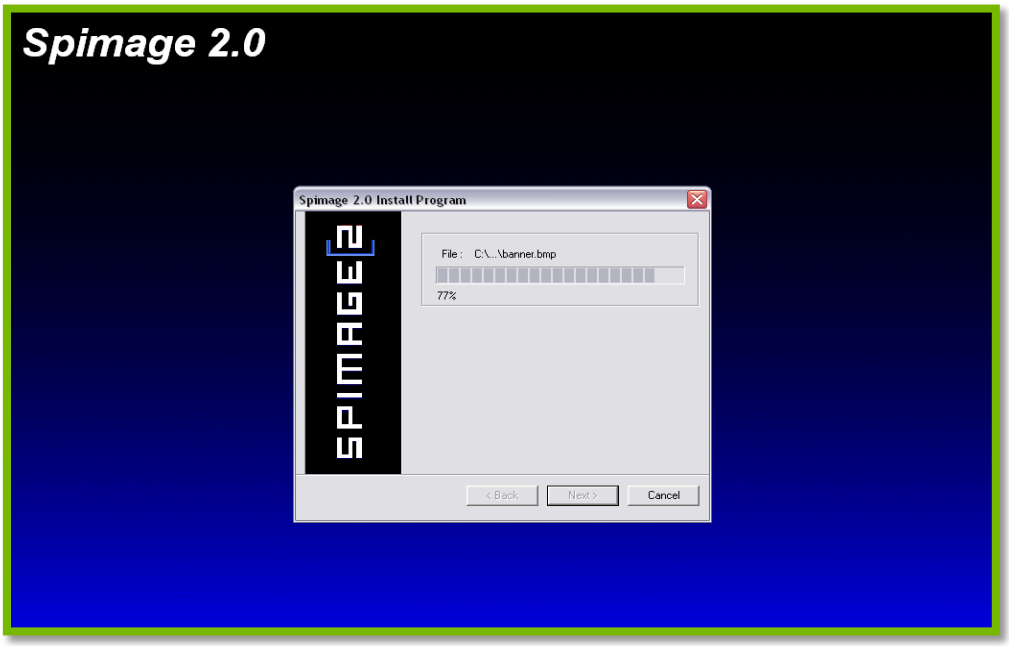


Imagen 10

Paso 11: Spimage se ha instalado, dar clic en Next (siguiente) para continuar. (Ver imagen 11)

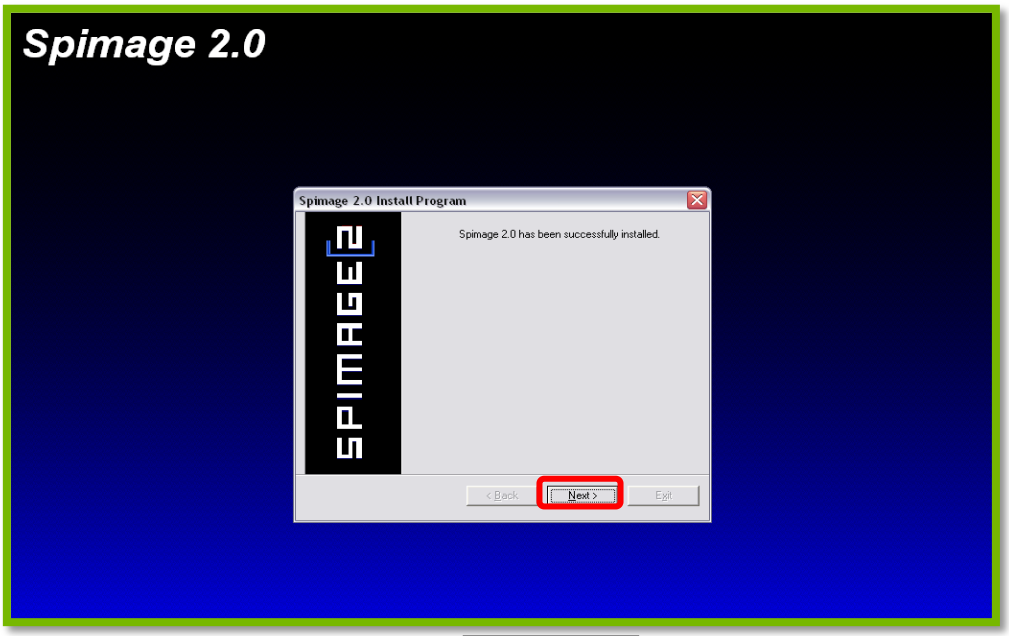


Imagen 11

Paso 12: Dar clic en Exit (Salir) para finalizar con la instalación. (Ver imagen 12)

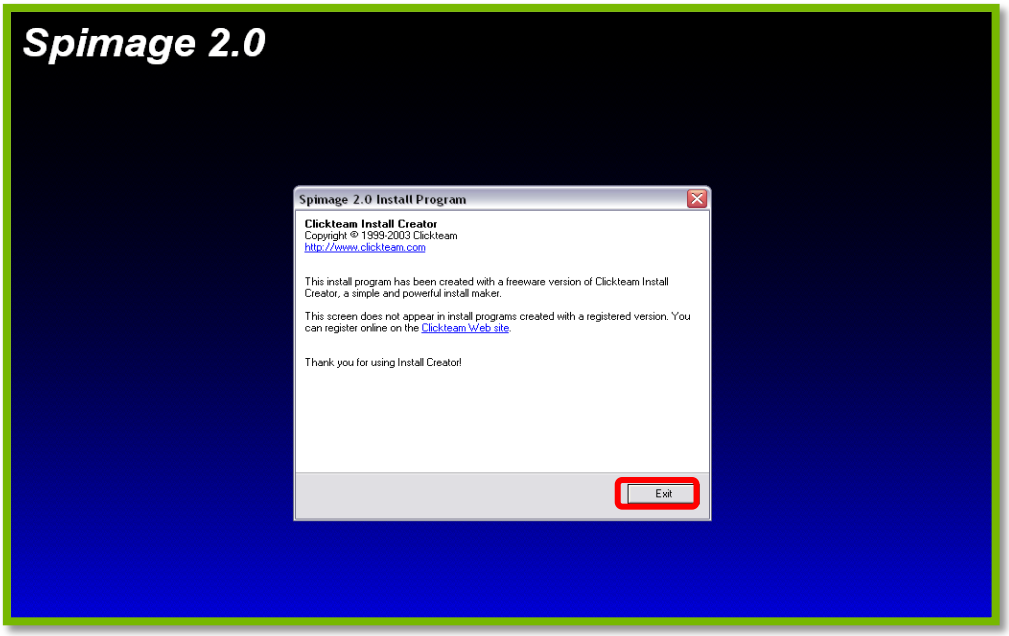


Imagen 12

CODIFICAR

Paso 13: Dar doble clic al icono que nos aparecerá en el escritorio. (Ver imagen 13)

Imagen 13

Paso 14: Dar clic en Encode para codificar. (Ver imagen 14)

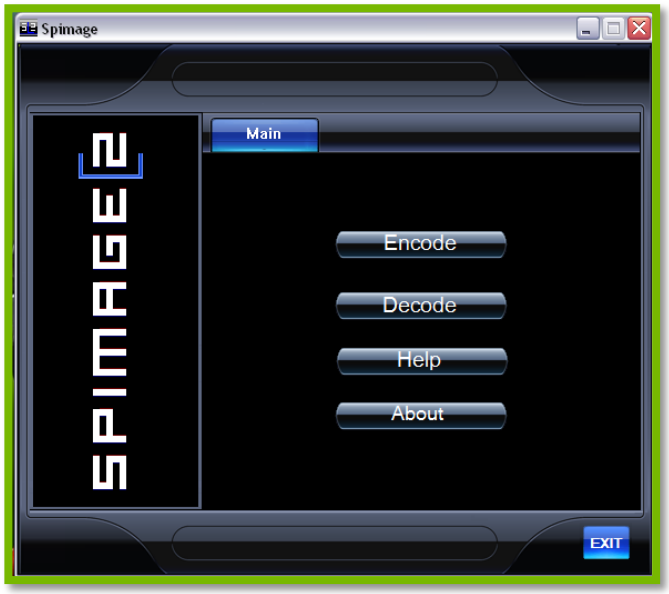


Imagen 14

Paso 15: Dar clic en las primeras flechitas cruzadas para buscar la imagen. (Ver imagen 15)

Imagen 15

Paso 16: Seleccionar la ubicación de la imagen. (Ver imagen 16)

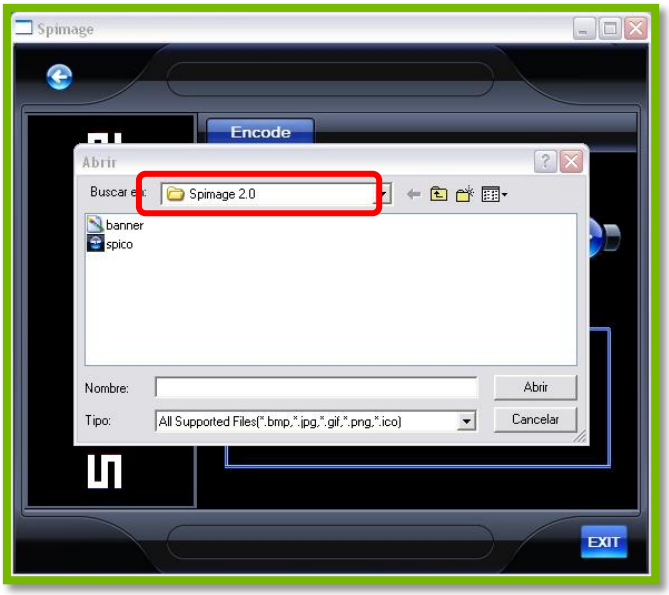


Imagen 16

Paso 17: Seleccionar la imagen y dar clic en abrir. (Ver imagen 17)

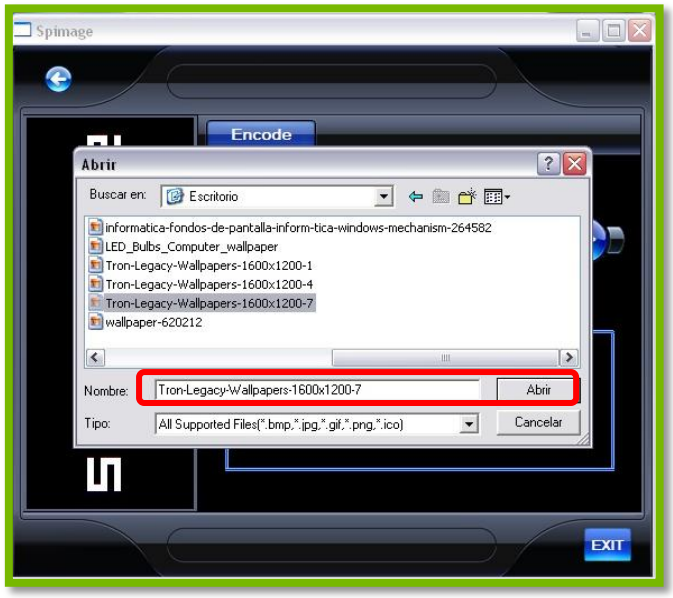


Imagen 17

Paso 18: Dar clic en las segundas flechitas cruzadas para seleccionar el archivo que se ocultará. (Ver imagen 18)

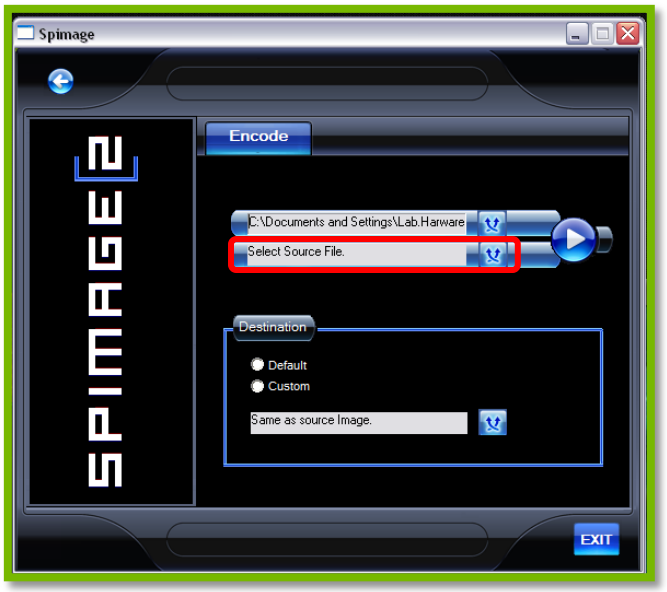


Imagen 18

Paso 19: Seleccionar el archivo que se ocultará y dar clic en abrir. (Ver imagen 19)

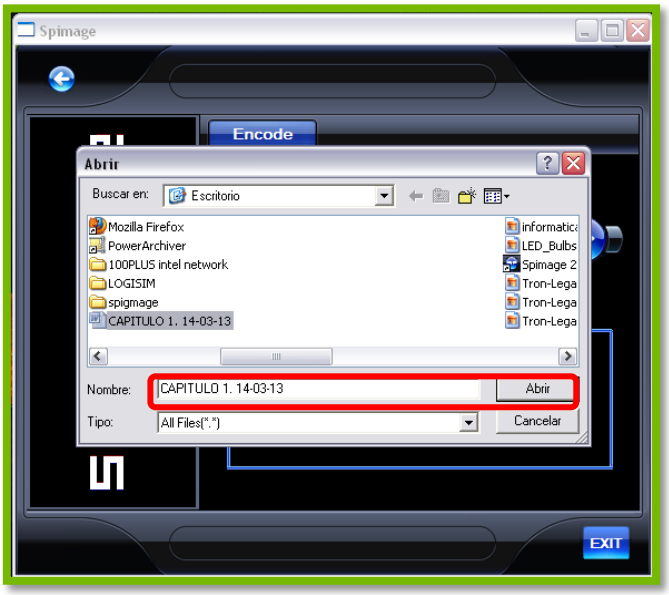


Imagen 19

Paso 20: Marcar la opción de Custom (personalizado) y seleccionar la ruta de destino. (Ver imagen 20)

Imagen 20

Paso 21: Dar nombre al archivo que se guardará en el escritorio y dar clic en guardar. (Ver imagen 21)

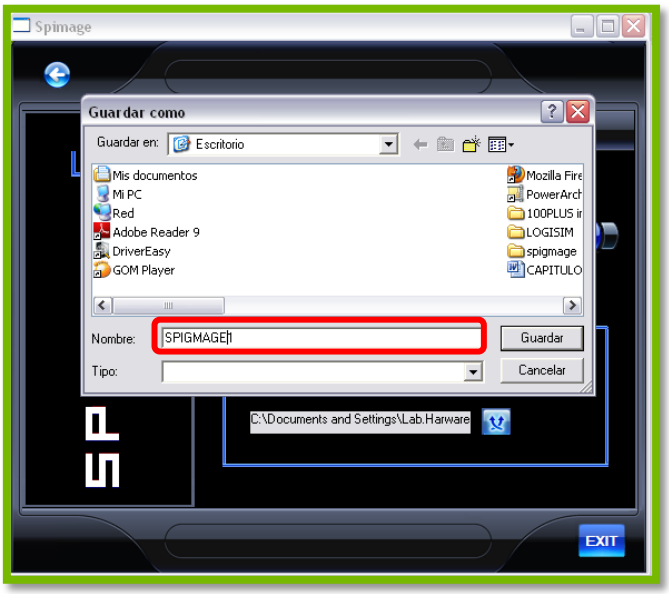


Imagen 21

Paso 22: Dar clic en el icono de Play. (Ver imagen 22)

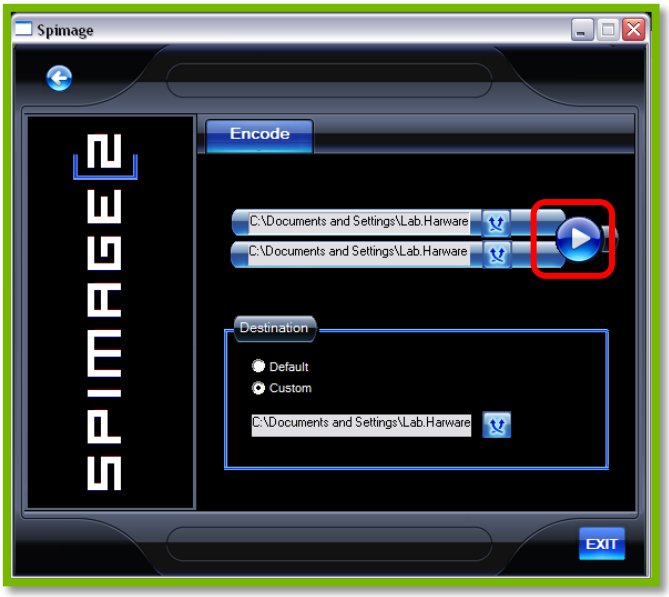


Imagen 22

Paso 23: Clic en aceptar, para aceptar la ruta de destino. (Ver imagen 23)

Imagen 23

Paso 24: Se asignará una clave que posterior mente descifrará el documento. (Ver imagen 24)

Imagen 24

DECODIFICAR

Paso 25: Seleccionar la imagen que contiene el archivo oculto. (Ver imagen 25)

Imagen 25

Paso 26: Seleccionada la imagen dar clic en abrir. (Ver imagen 26)

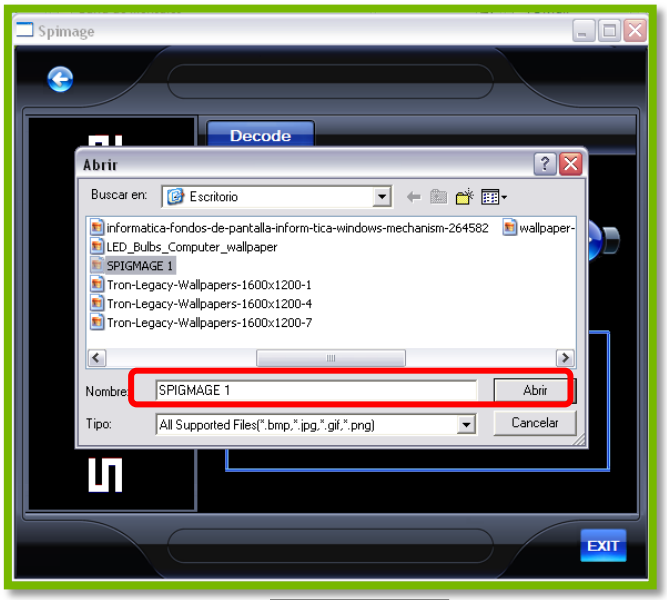


Imagen 26

Paso 27: Introducir la clave antes proporcionada. (Ver imagen 27)

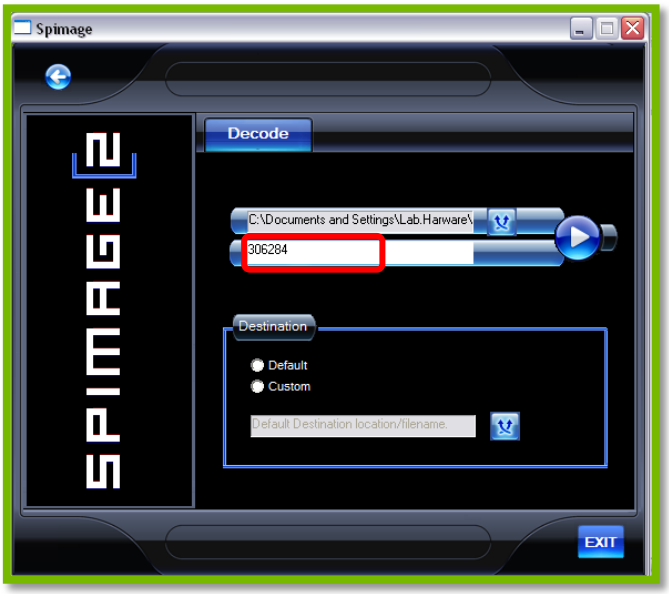


Imagen 27

Paso 28: Marcar Custom (personalizado) para elegir la ruta donde se guardara el archivo oculto. (Ver imagen 28)

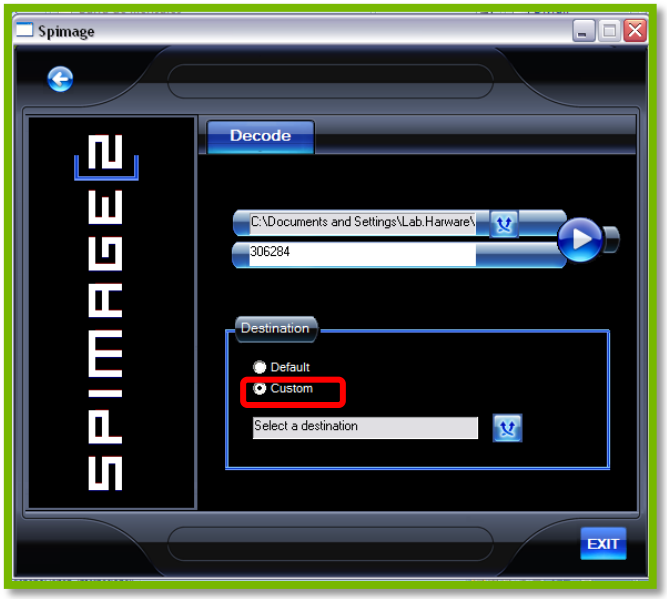


Imagen 28

Paso 29: Nombrar al archivo oculto para su extracción y clic en guardar. (Ver imagen 29)

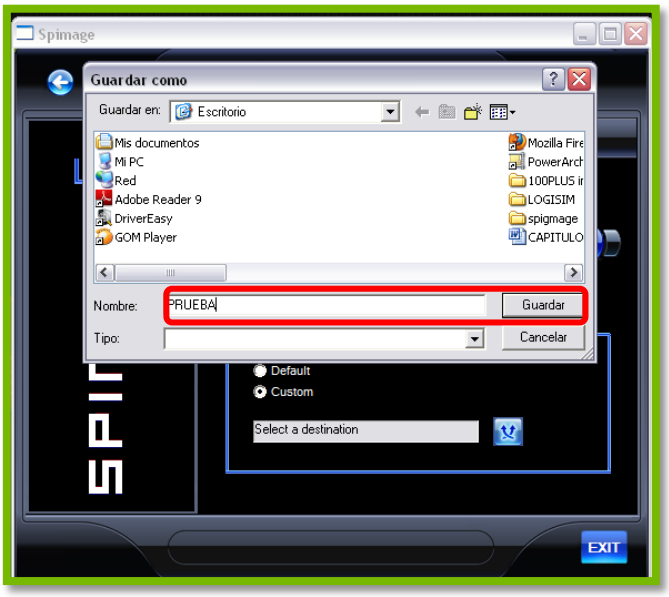


Imagen 29

Paso 30: Clic en aceptar. (Ver imagen 30)

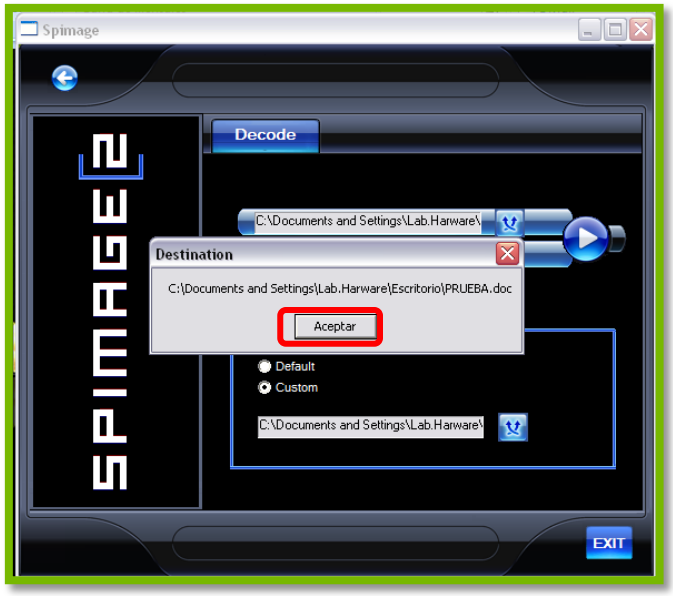


Imagen 30

Paso 31: Spimage a decodificado con éxito dar clic en Exit para Salir del programa. (Ver imagen 31

Imagen 31

Camouflage Manual

- ✓ **Instalación**
- ✓ **Camouflagear**
- ✓ **Descamouflagear**

INSTALACIÓN

Paso 1: Introducir el cd del kit de herramientas en el reproductor de CD o DVD e introducir la bandeja. (Ver imagen 1)

Imagen 1

Paso 2: Aparece la siguiente ventana, dar clic en el botón programas. (Ver imagen 2)

Imagen 2

Paso 3: Dar clic en el boton de esteganografia. (ver imagen 3)

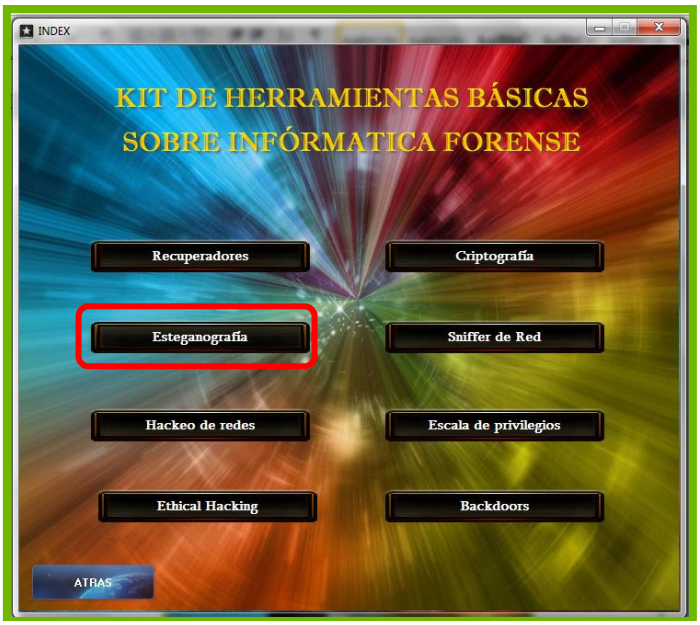


Imagen 3

Paso 4: Ubicar el icono de instalación del programa Camouflage y dar clic. (Ver imagen 4)

Imagen 4

Paso 5: Dar clic en Unzip para descomprimir los archivos de instalación. (Ver imagen 5)

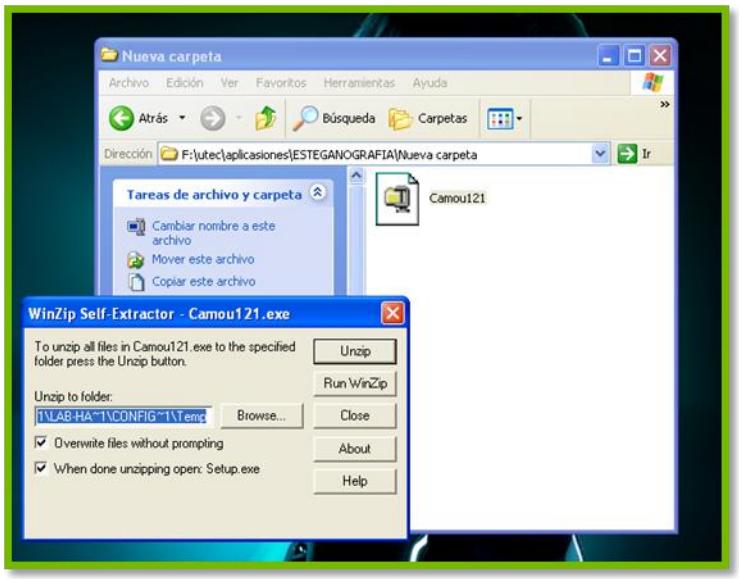


Imagen 5

Paso 6: Dar clic en aceptar para iniciar con la instalación. (Ver imagen 6)

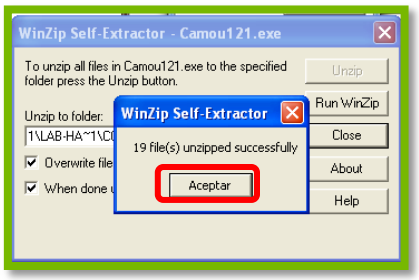


Imagen 6

Paso 7: Esperar unos según a que cargue la ventana de instalación. (Ver imagen 7)

Imagen 7

Paso 8: Clic en Next (siguiente) para iniciar la instalación. (Ver imagen 8)

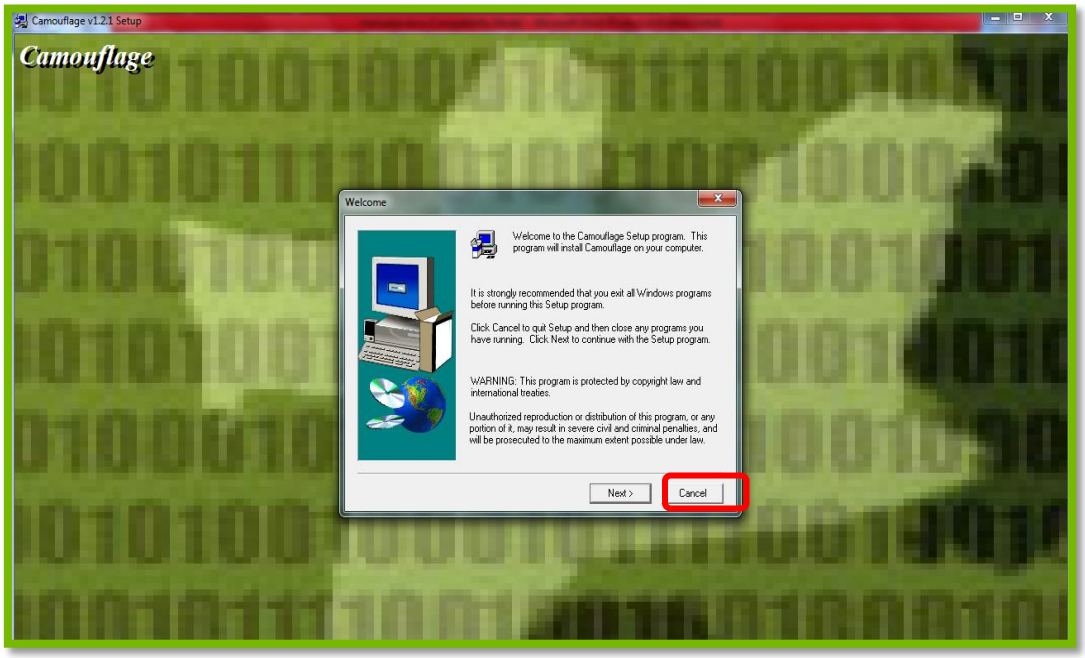


Imagen 8

Paso 9: Dar clic en la opción Yes para aceptar los términos de licencia (Ver imagen 9)

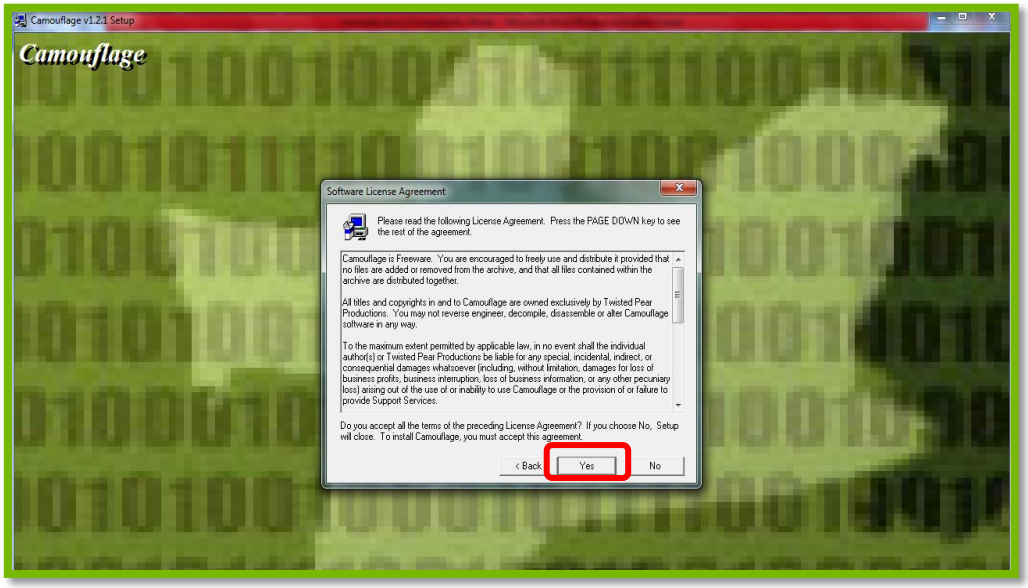


Imagen 9

Paso 10: Clic en Next (siguiente) para continuar con la instalación instalándose en un lugar predeterminado. (Ver imagen 10)

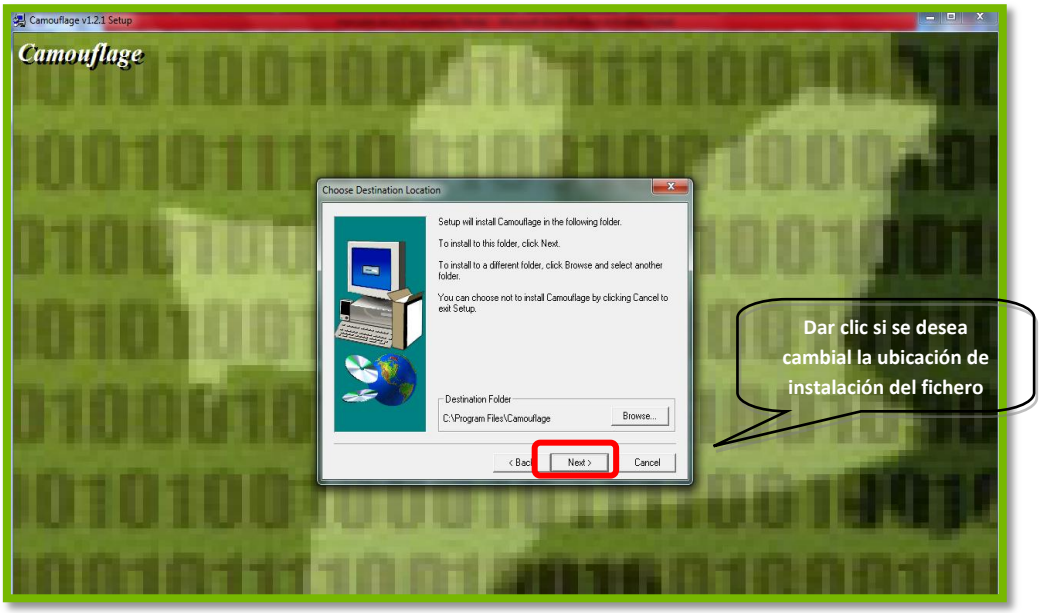


Imagen 10

Paso 11: Clic en Next (siguiente) para continuar con la instalación. (Ver imagen 11)

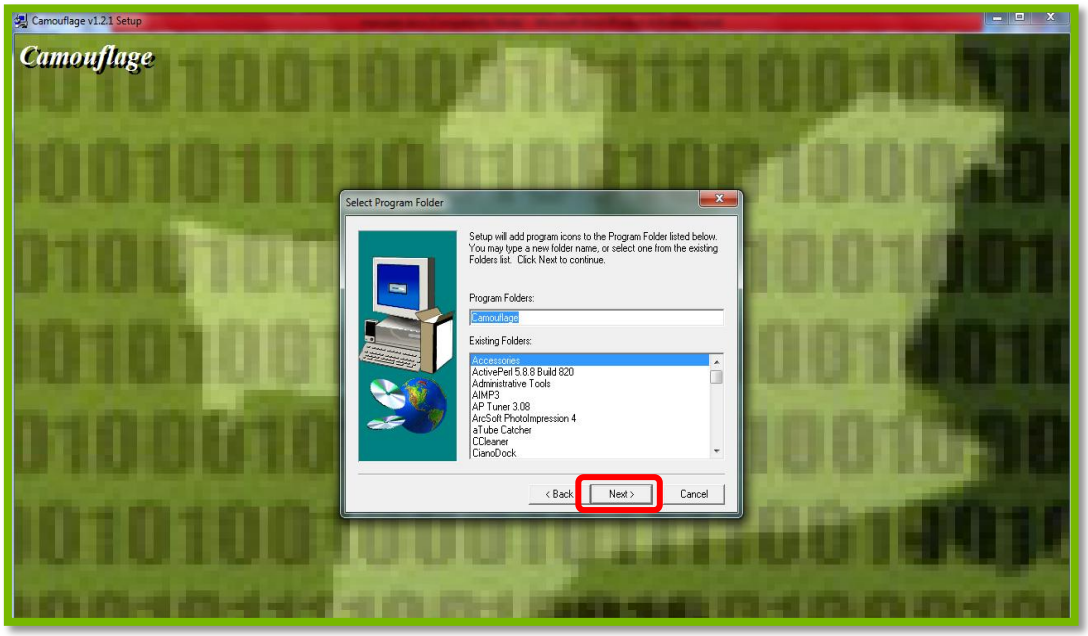


Imagen 11

Paso 12: Clic en Next (siguiente) para continuar con la instalación. (Ver imagen 12)

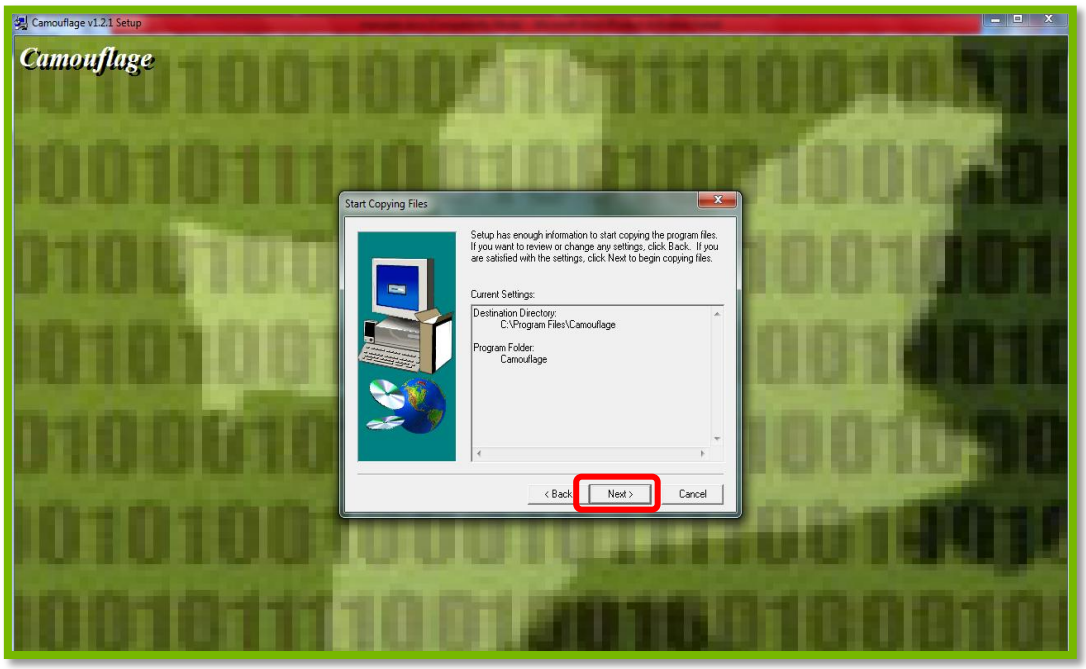


Imagen 12

Paso 13: Desmarcar las 2 casillas y dar clic en Finish (finalizar) para terminar la instalación. (Ver imagen 13)

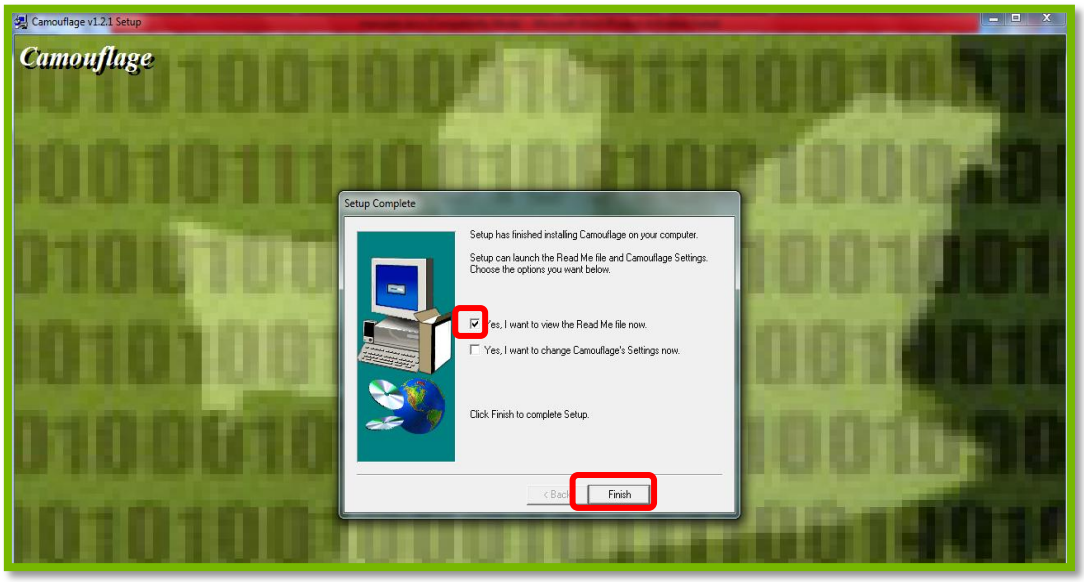


Imagen 13

AJUSTES

Paso 14: Ir a menú inicio dar clic en todos los programas, clic en la carpeta de camouflage clic en el icono camouflage settings. (Ver imagen 14)

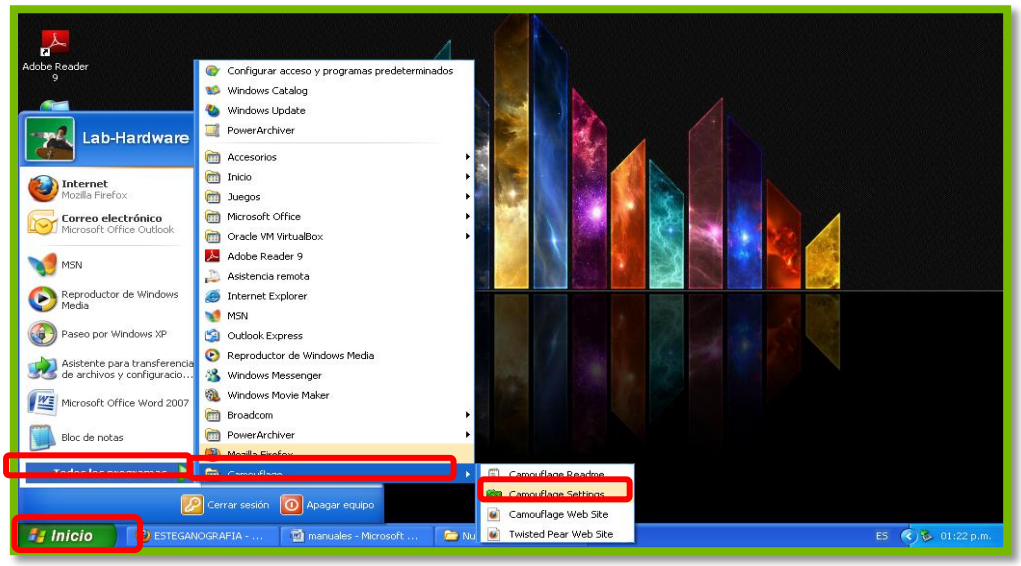


Imagen 14

Paso 15: En el menú de opciones se puede cambiar el nombre con el que se desea que las opciones para camuflajear y descamuflajear aparezcan en el menú contextual, clic en close para cerrar. (Ver imagen 15)

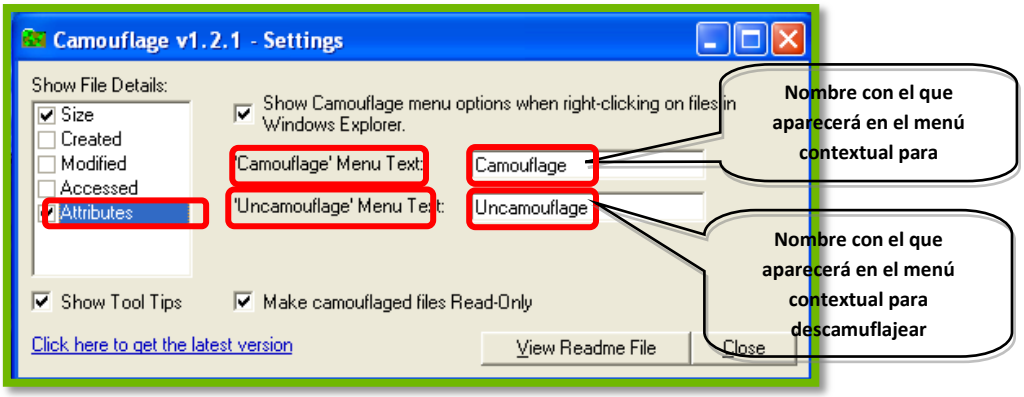


Imagen 15

CAMOUFLAGEAR UN ARCHIVO

Paso 16: Dar clic derecho sobre el archivo que se quiere ocultar y seleccionar la opción Camouflage. (Ver imagen 16)

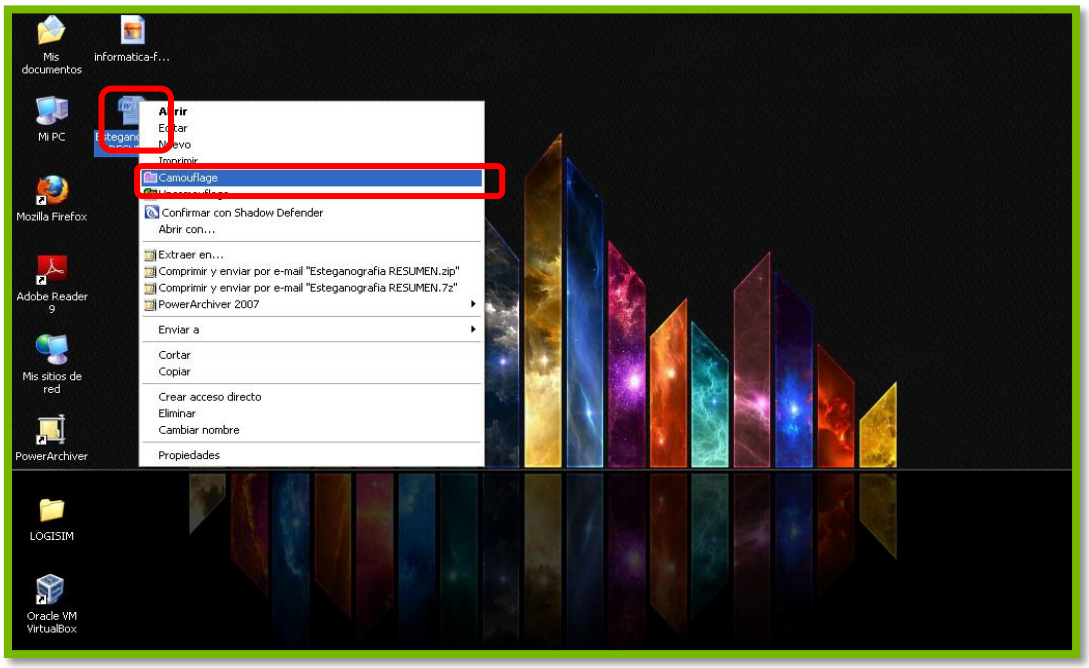


Imagen 16

Paso 17: Dar clic en Next (siguiente) para continuar. (Ver imagen 17)

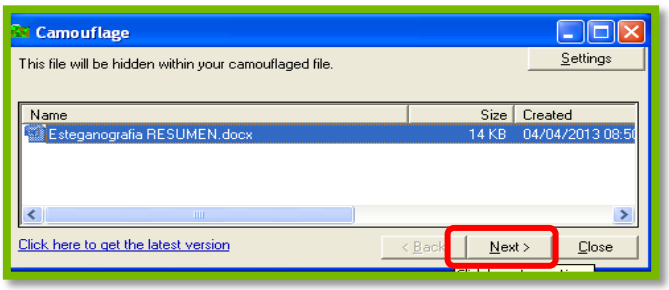


Imagen 17

Paso 18: Seleccionar el archivo portador del documento y dar clic en abrir. (Ver imagen 18)

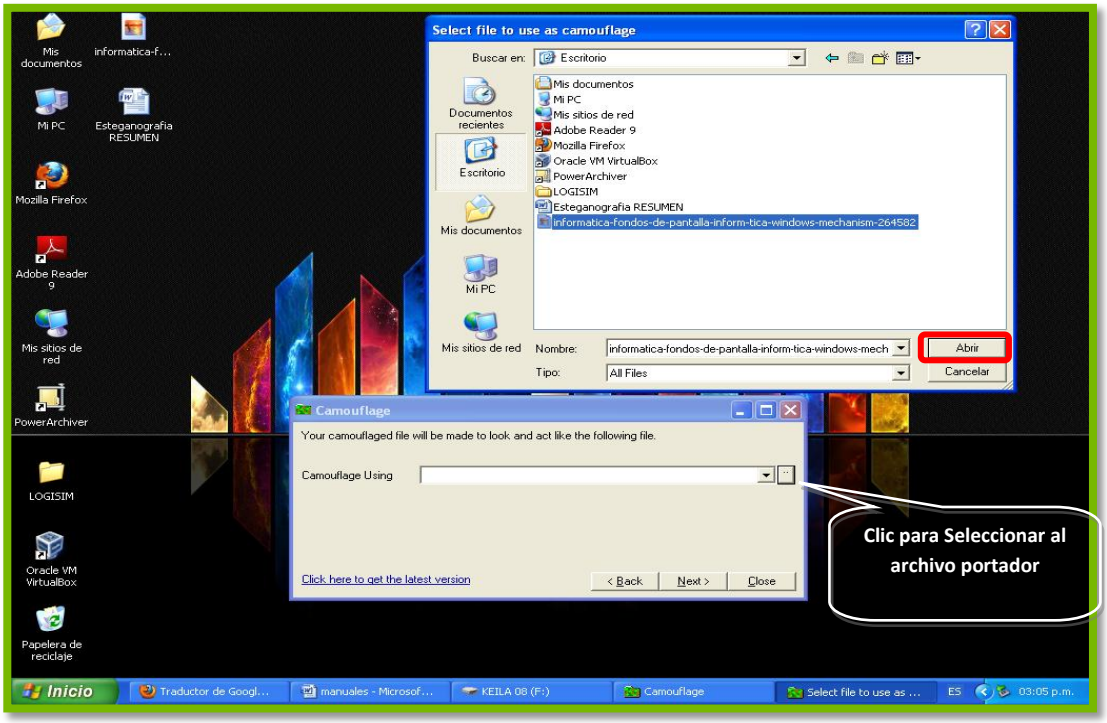


Imagen 18

Paso 19: Dar clic en Next (siguiente) para continuar. (Ver imagen 19)

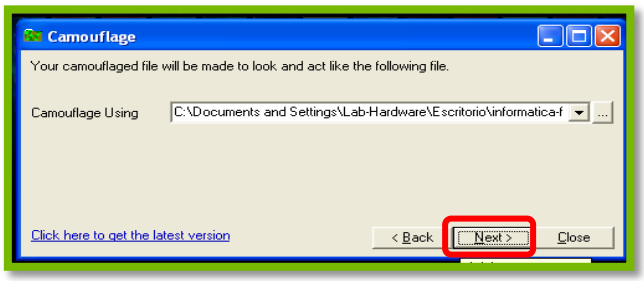


Imagen 19

Paso 20: En este paso se selecciona la ubicación en donde se guardará el portador y el nombre que poseera, dar clic en guardar. (Ver imagen 20)

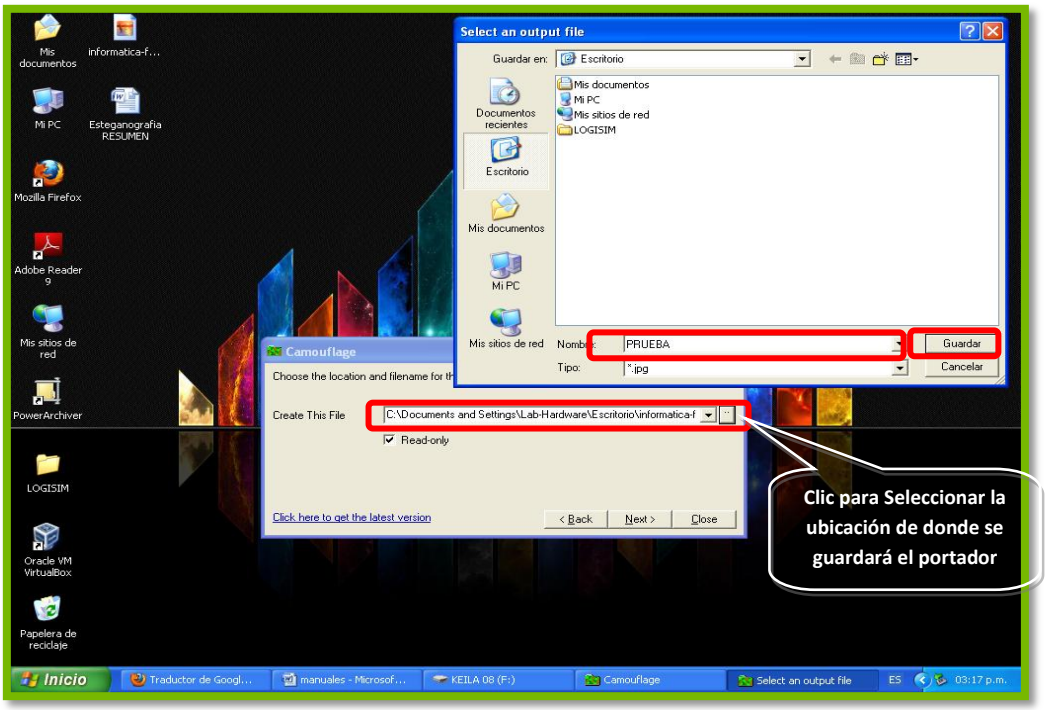


Imagen 20

Paso 21: Clic en Next (siguiente) para continuar. (Ver imagen 21)

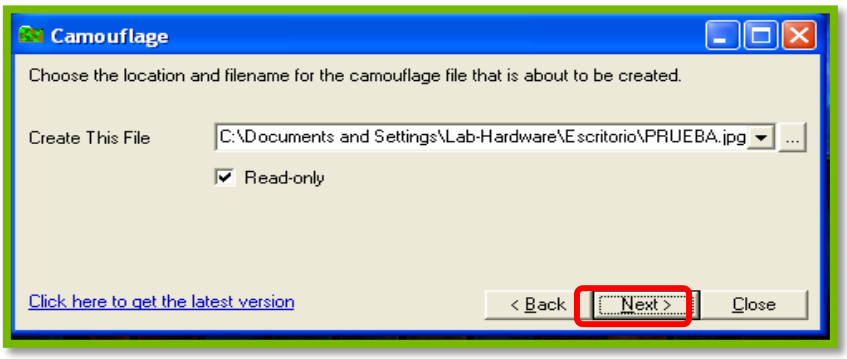


Imagen 21

Paso 22: Introducir la contraseña que tendrá el archivo y dar clic en Finish. (Finalizar). (Ver imagen 22)

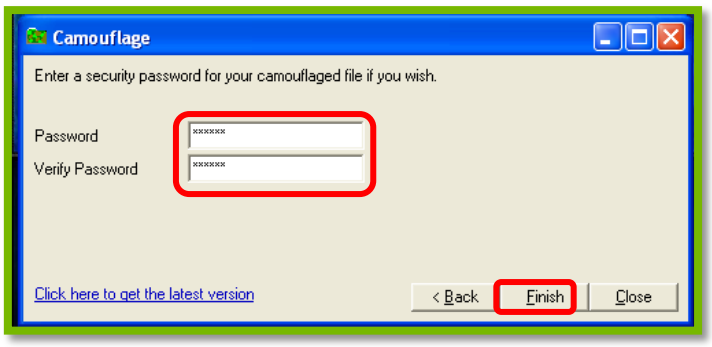


Imagen 22

Paso 23: En esta pantalla se muestra la imagen con el archivo oculto. (Ver imagen 23)

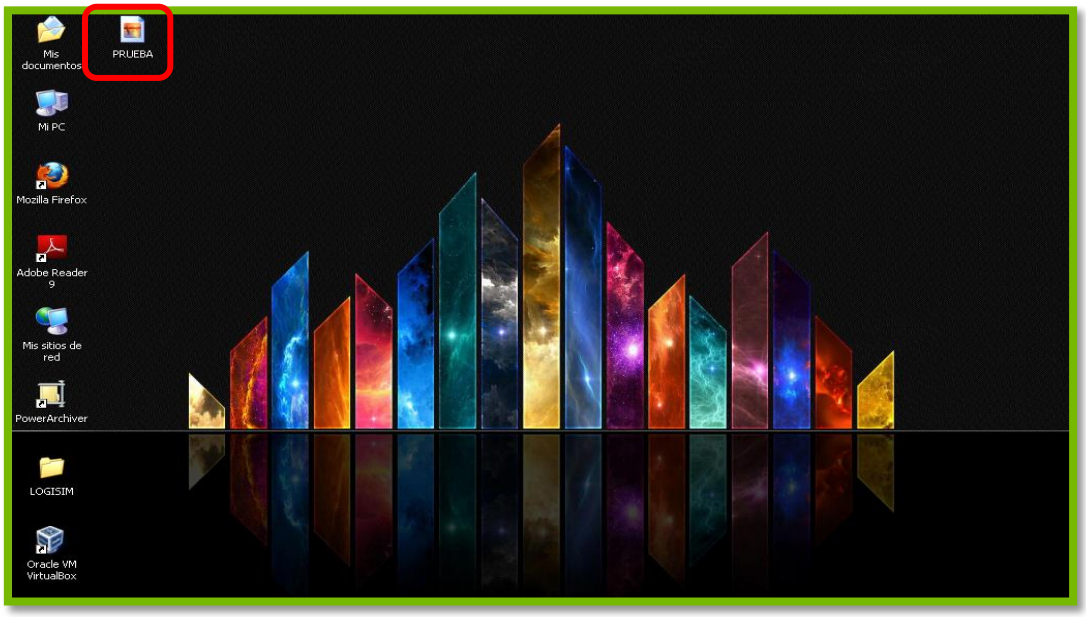


Imagen 23

DESCAMUFLAGEAR

Paso 24: dar clic derecho sobre el archivo portador, seleccionar la opción Uncamouflage. (Ver imagen 24)

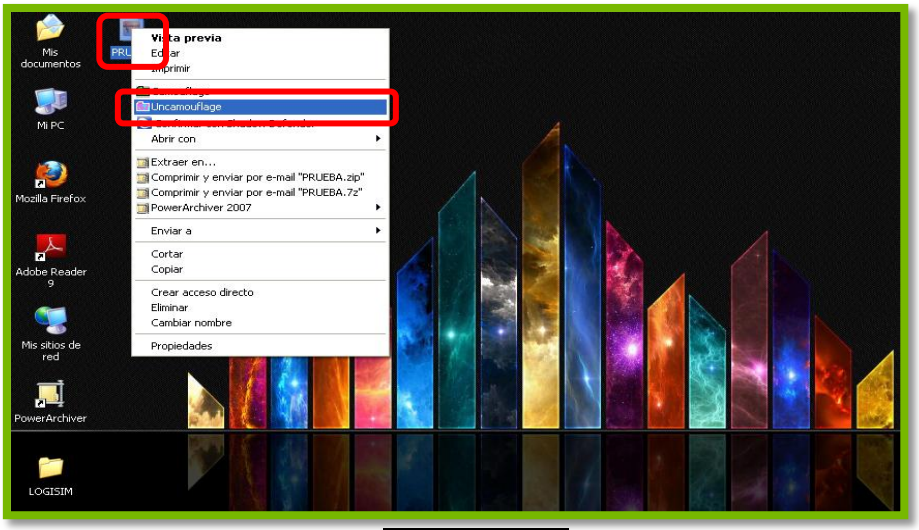


Imagen 24

Paso 25: Introducir la contraseña y dar clic en Next (siguiente). (Ver imagen 25)

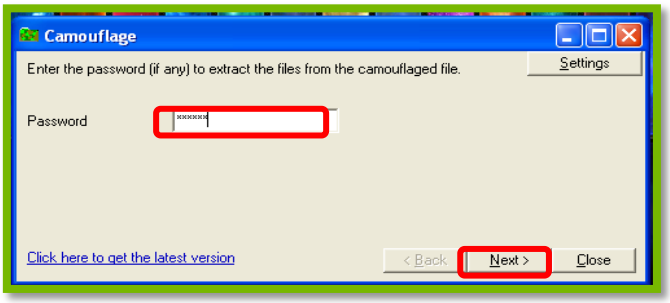


Imagen 25

Paso 26: Dar clic en Next (siguiente) para continuar con la extracción del archivo. (Ver imagen 26)

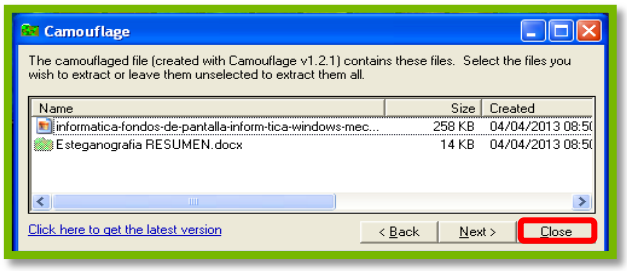


Imagen 26

Paso 27: En este paso seleccionar la ubicación en donde se extraerá el archivo y el nombre que tendrá el archivo a extraer. (Ver imagen 27)

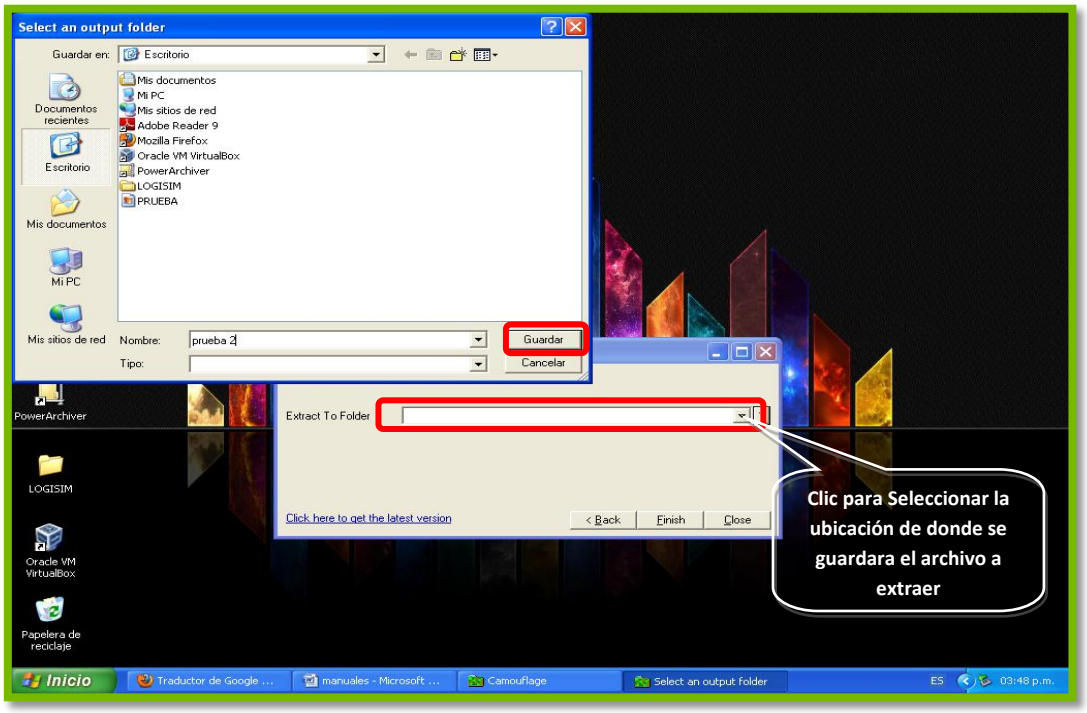


Imagen 27

Paso 28: Dar clic en Finish (finalizar) para continuar con la extracción. (Ver imagen 28)

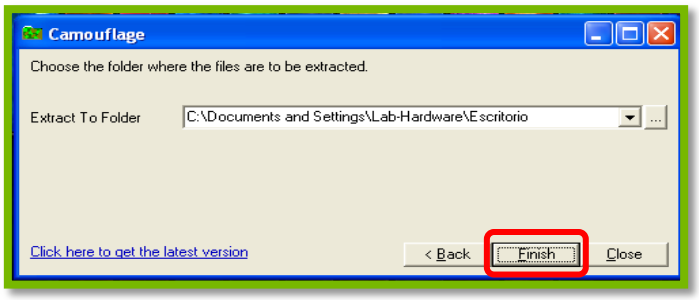


Imagen 28

Paso 29: En esta pantalla aparece el archivo portador y el archivo que se ocultó. (Ver imagen 29)

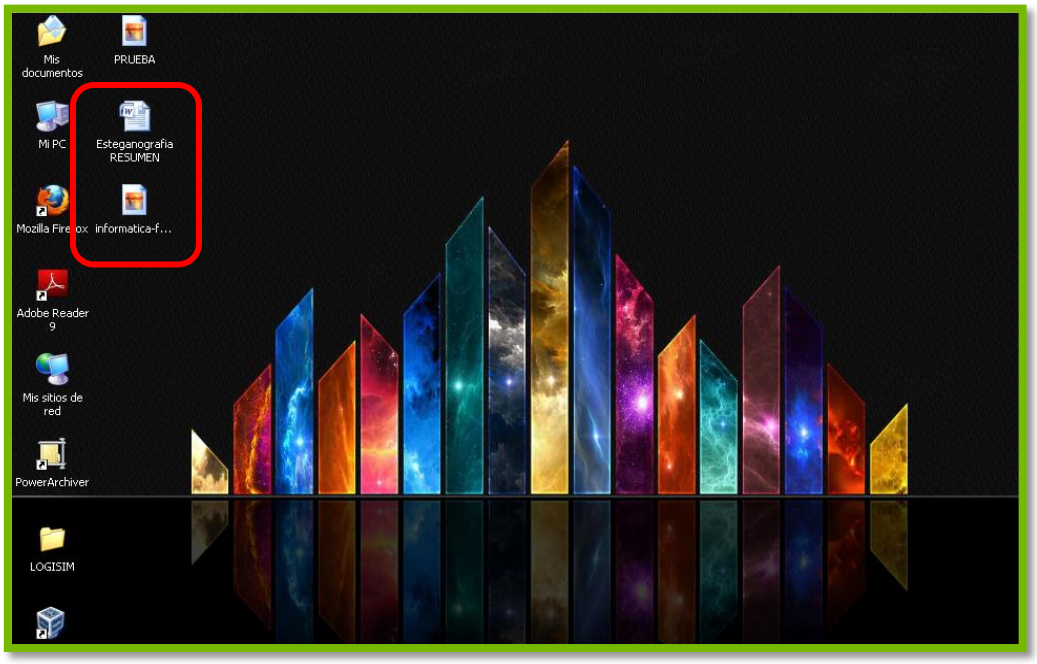


Imagen 29

FileInyector Manual

- ✓ **Instalación**
- ✓ **Codificar**
- ✓ **Descodificar**

EJECUCIÓN

Paso 1: Introducir el cd del kit de herramientas en el reproductor de CD ó DVD e introducir la bandeja. (Ver imagen 1)

Imagen 1

Paso 2: Aparece la siguiente ventana, dar clic en el botón programas. (Ver imagen 2)

Imagen 2

Paso 3: Dar clic en el boton de esteganografia. (ver imagen 3)

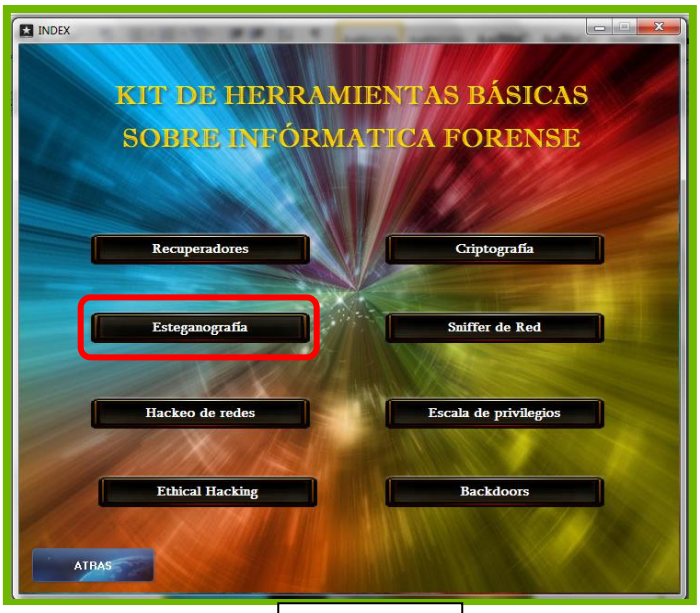


Imagen 3

Paso 4: Ubicar el icono del programa Camouflage y dar clic. Este programa no necesita instalación (Ver imagen 4)

Imagen 4

OCULTAR ARCHIVO

Paso 5: Para seleccionar la imagen dar clic en cargar imagen. (Ver imagen 5)

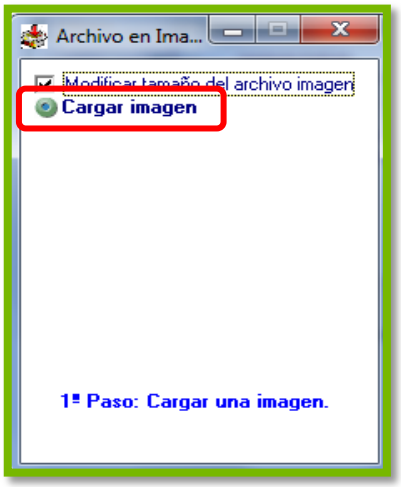


Imagen 5

Paso 6: Seleccionar la imagen y dar clic en abrir. (Ver imagen 6)

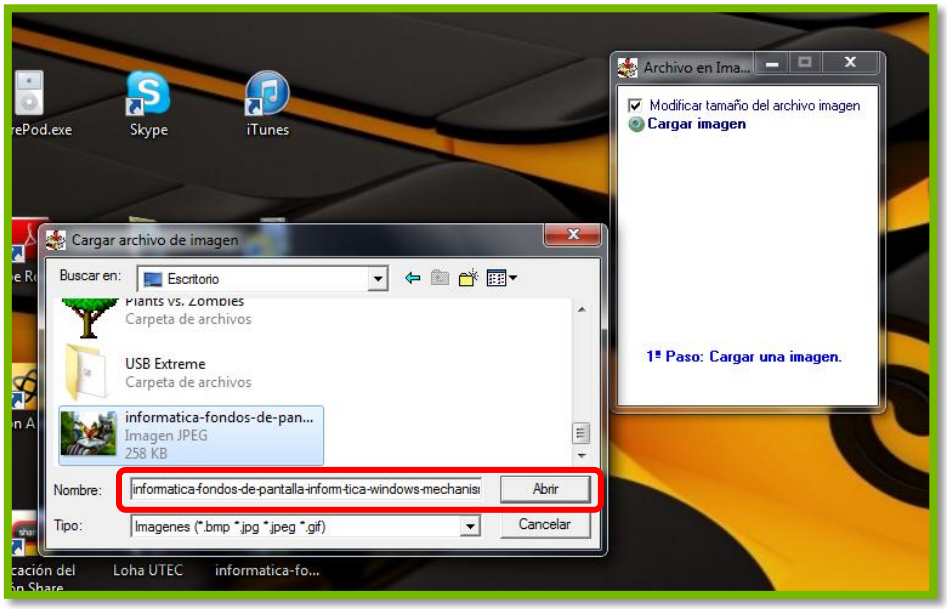


Imagen 6

Paso 7: Dar clic en la segunda opción en inyectar archivo en la imagen. (Ver imagen 7)

Imagen 7

Paso 8: Seleccionar el archivo que será inyectado y dar clic en abrir. (Ver imagen 8)

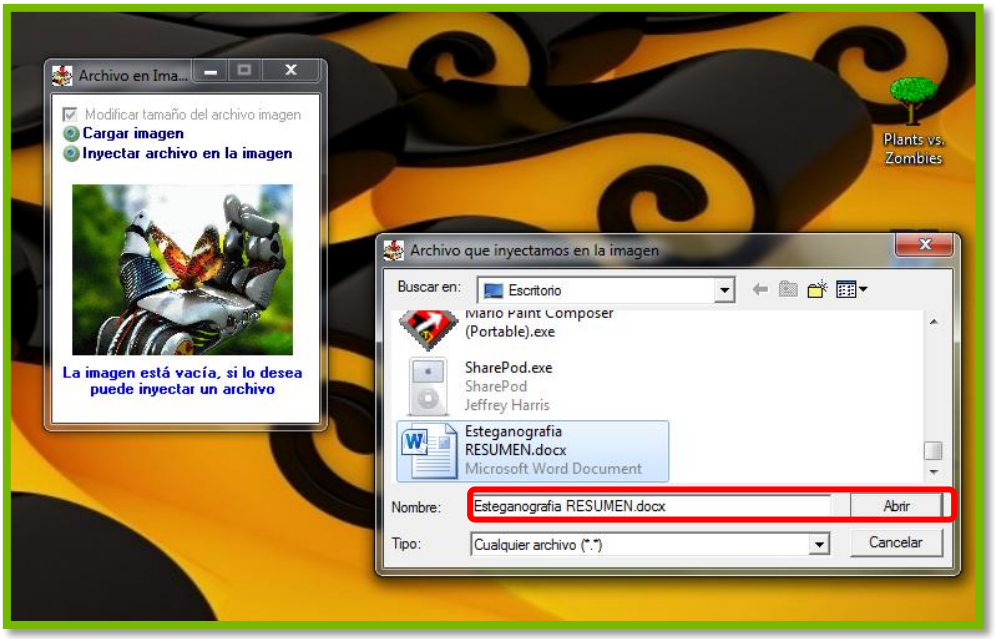


Imagen 8

Paso 9: Escribir la contraseña que se desea para la inyección y dar clic en ok. (Ver imagen 9)

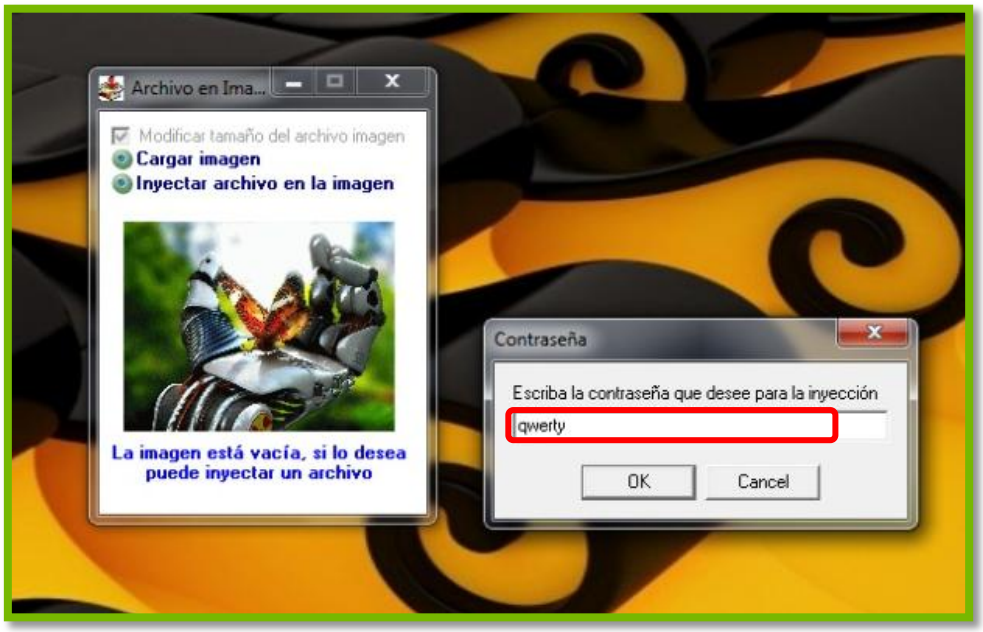


Imagen 9

Paso 10: La inyección fue realizada con éxito. (Ver imagen 10)

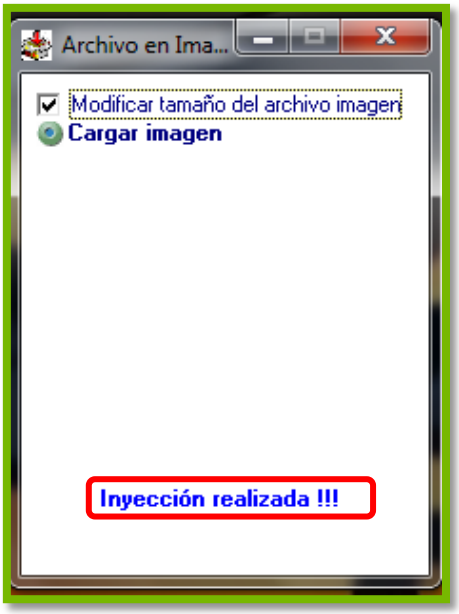


Imagen 10

EXTRAER ARCHIVO

Paso 11: Dar clic en cargar imagen para buscar la imagen que contienen el archivo. (Ver imagen 11)

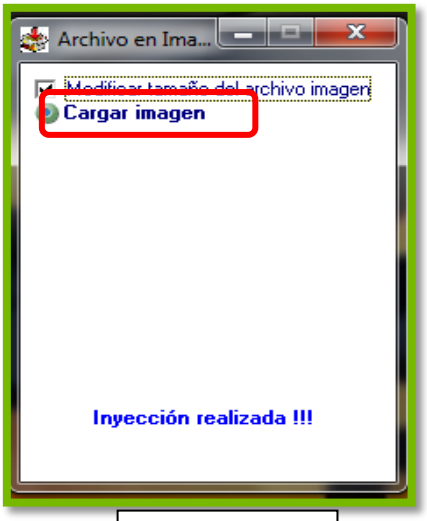


Imagen 11

Paso 12: Abrir la imagen con el archivo inyectado. (Ver imagen 12)

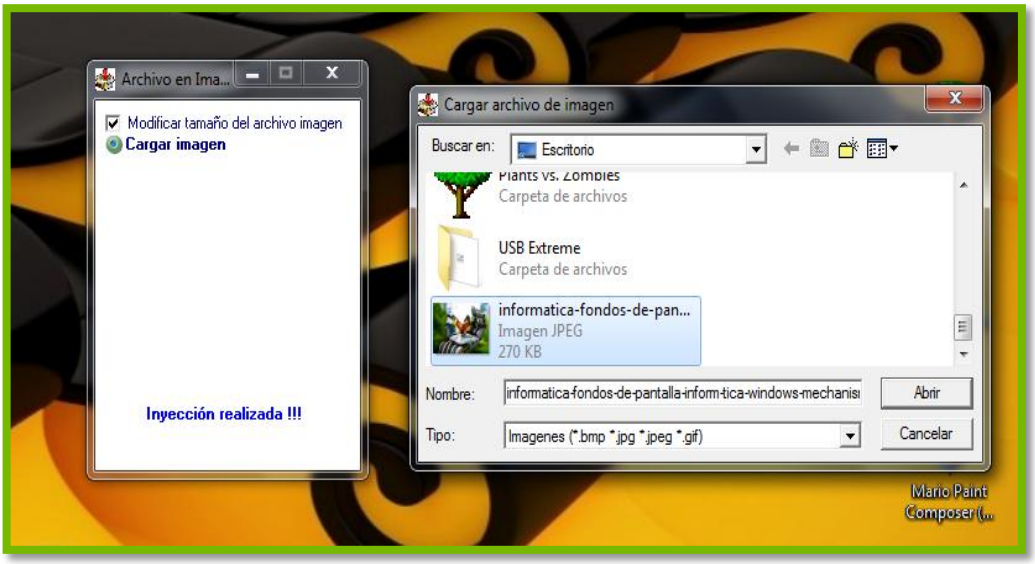


Imagen 12

Paso 13: Dar doble clic en la segunda opción extraer archivo de la imagen. (Ver imagen 13)

Imagen 13

Paso 14: Escribir la contraseña que se le dio y clic en ok. (Ver imagen 14)

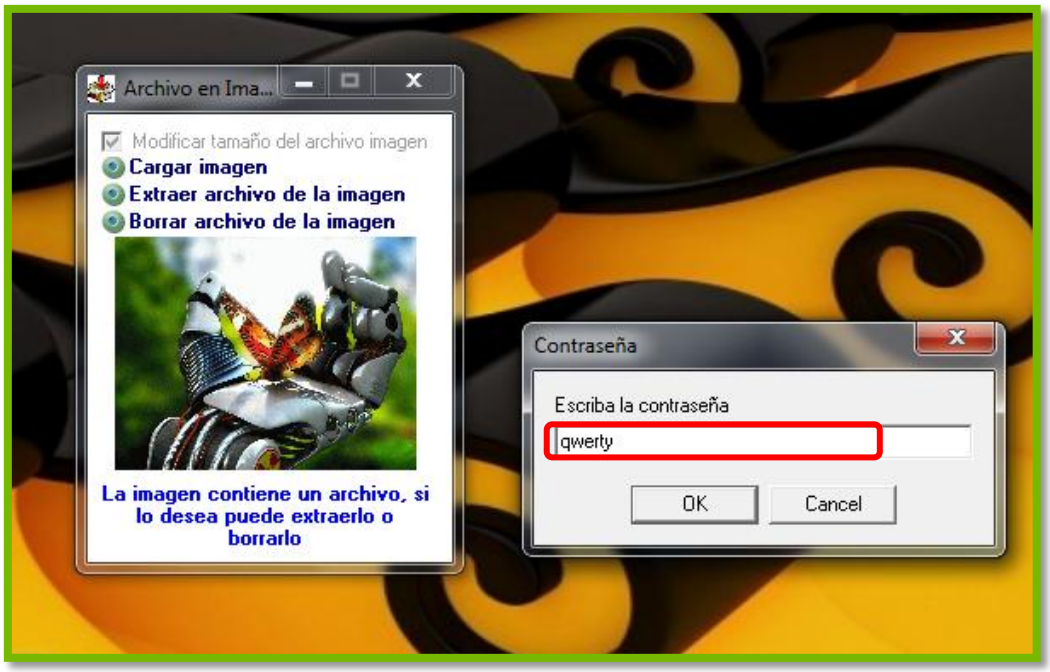


Imagen 14

Paso 15: Seleccionar la ubicación en donde se extraerá el archivo, el nombre y clic en abrir. (Ver imagen 15)

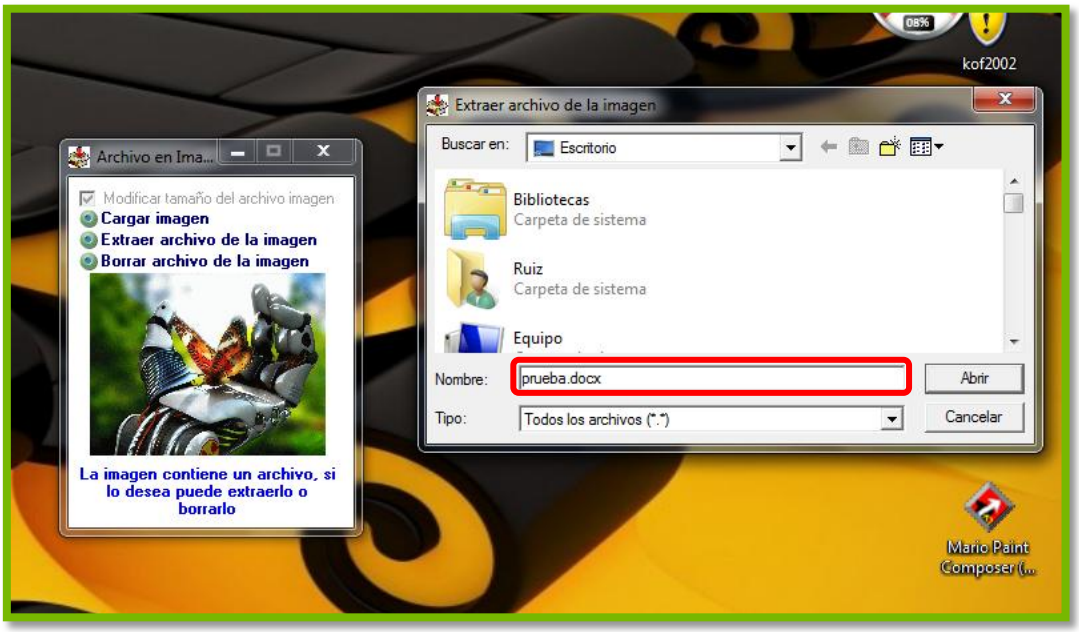


Imagen 15

Paso 16: La extracción ha sido realizada con éxito. (Ver imagen 16)

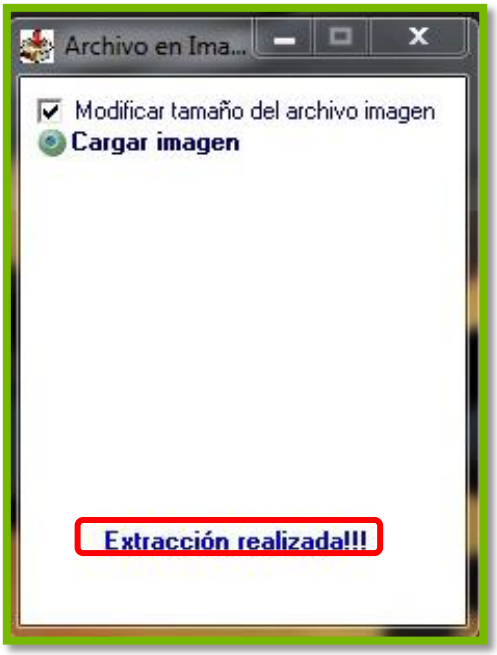


Imagen 16

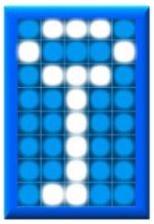
3. CRIPTOGRAFÍA

3.1 CONCEPTO

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.

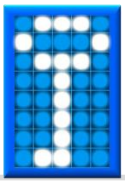
3.2 PROGRAMAS

3.2.1 TRUE CRYPT



3.2.2 AXCRYPT

3.2.3 PARANOIC ENCRYPTION



True Crypt Manual

- ✓ Instalación
- ✓ Cifrado de volumen

INSTALACIÓN

Paso 1: Introducir el cd del kit de herramientas en el reproductor de CD o DVD e introducir la bandeja. (Ver imagen 1)

Imagen 1

Paso 2: Aparece la siguiente ventana, dar clic en el botón programas. (Ver imagen 2)

Imagen 2

Paso 3: Dar clic en el boton de esteganografia. (ver imagen 3)

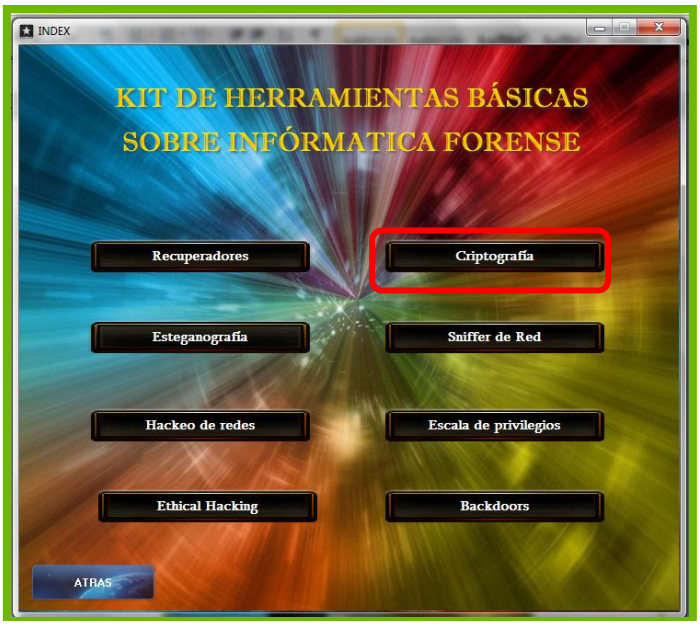
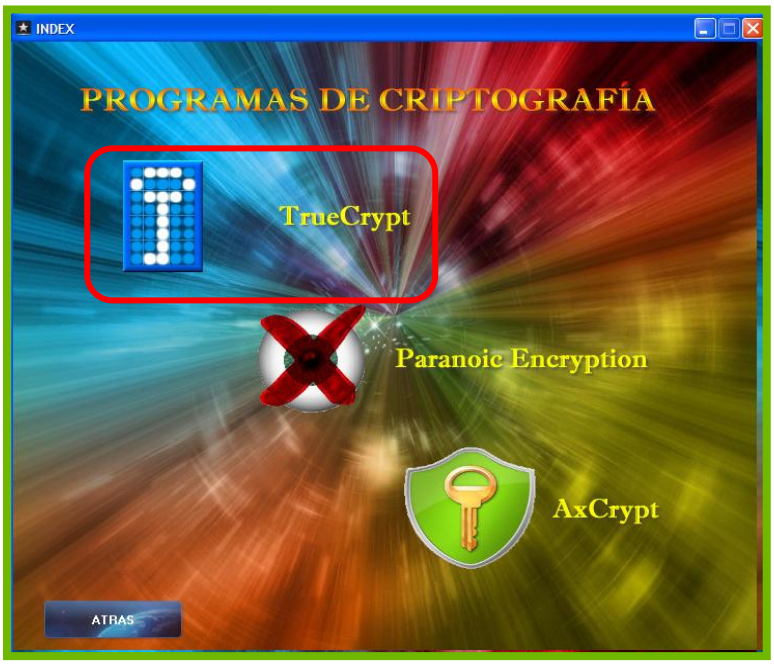
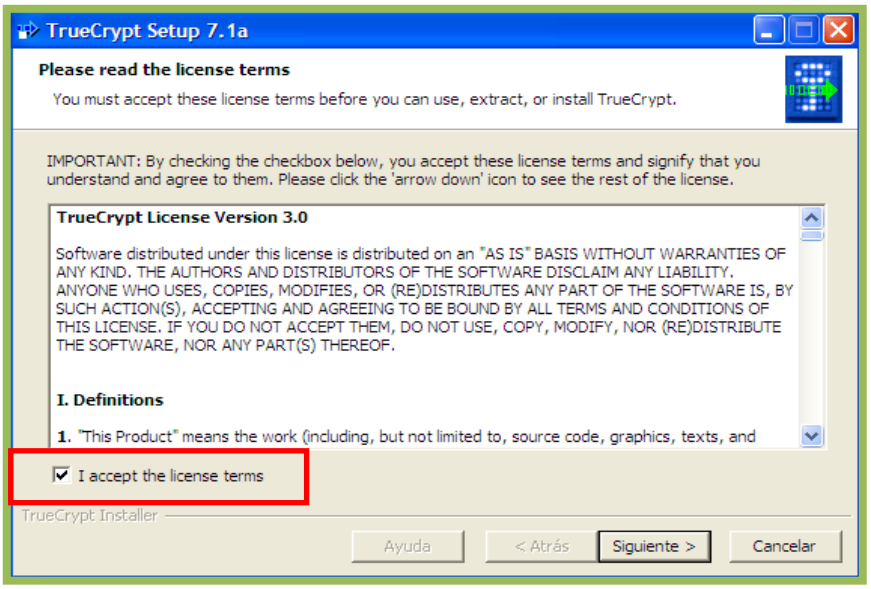


Imagen 3

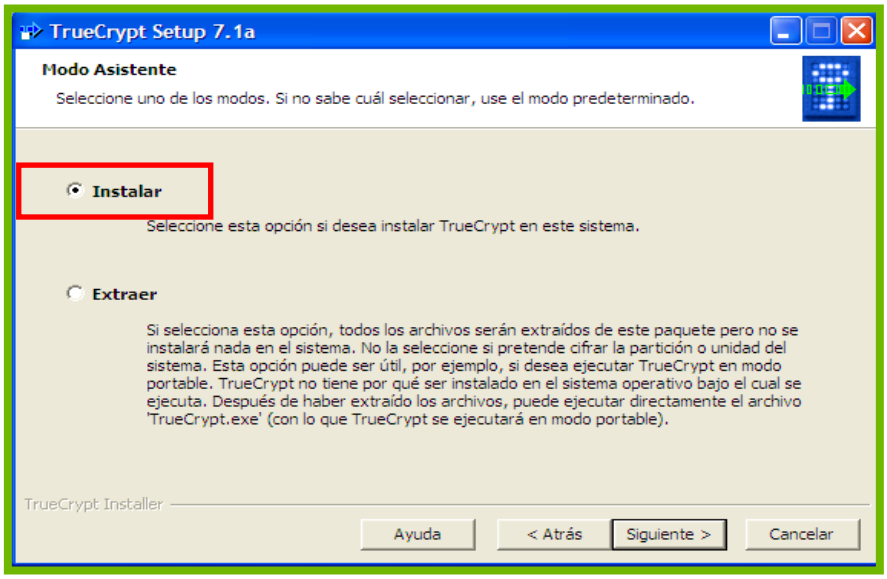
Paso 4: Ubicar el icono del programa TrueCrypt y dar clic para iniciar la instalación (Ver imagen 4)



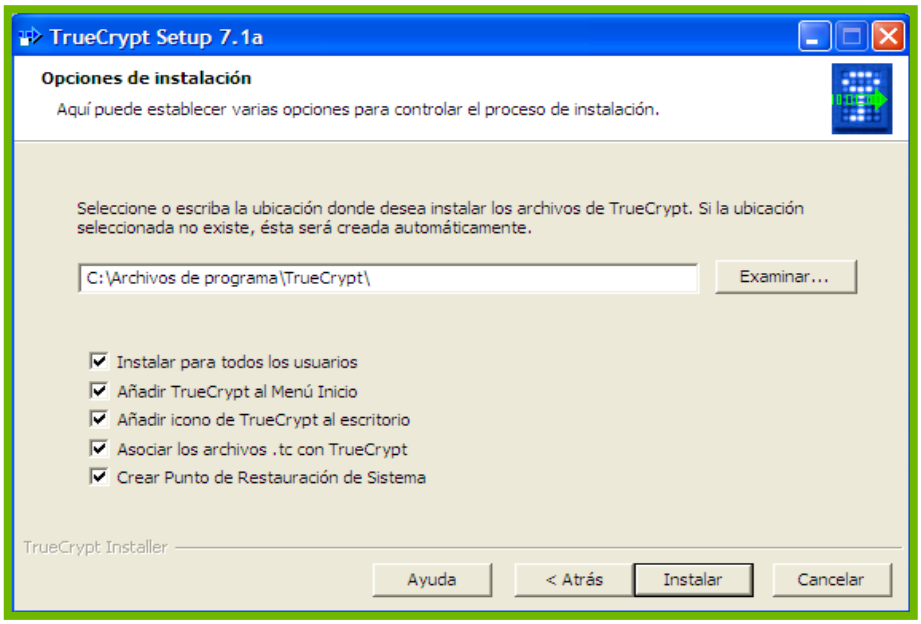
Paso 5: Aparece la ventana de acuerdo de licencia marcar la opción aceptar términos, y dar clic en siguiente. (Ver imagen 5)



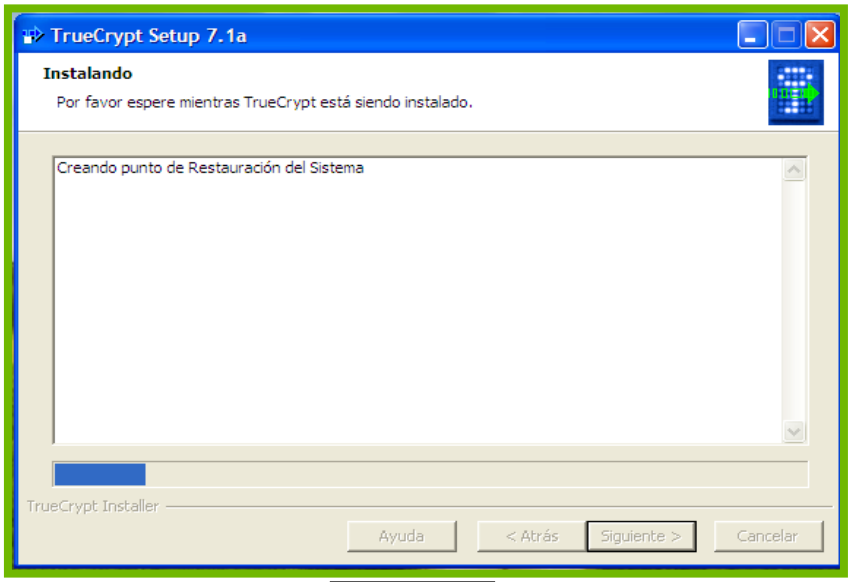
Paso 6: Marcar la opción Instalar el programa y dar clic en siguiente. (Ver imagen 6).



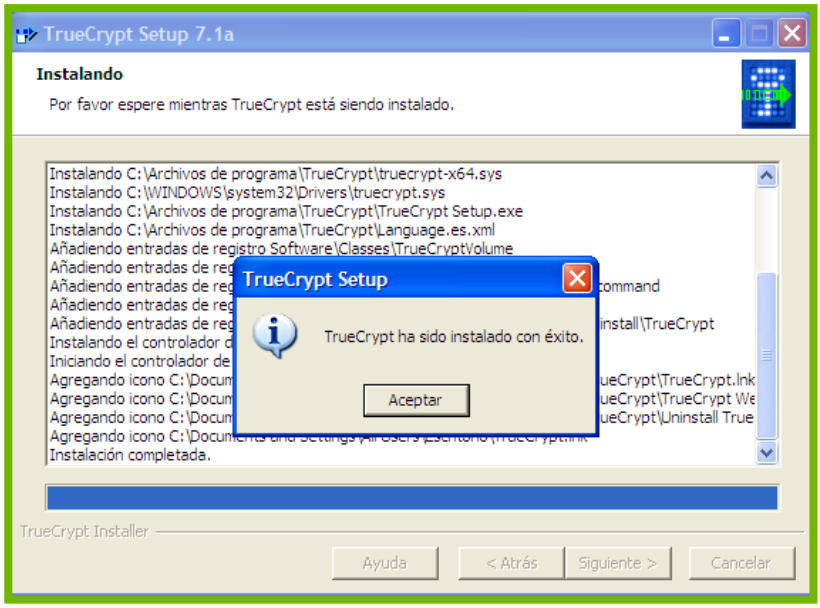
Paso 7: En esta ventana se puede cambiar la ruta de ubicación del programa, además de ofrecer las opciones de crear un icono en el escritorio, y que se añada al menú de inicio. Y dar clic en Instalar. (Ver imagen 7).



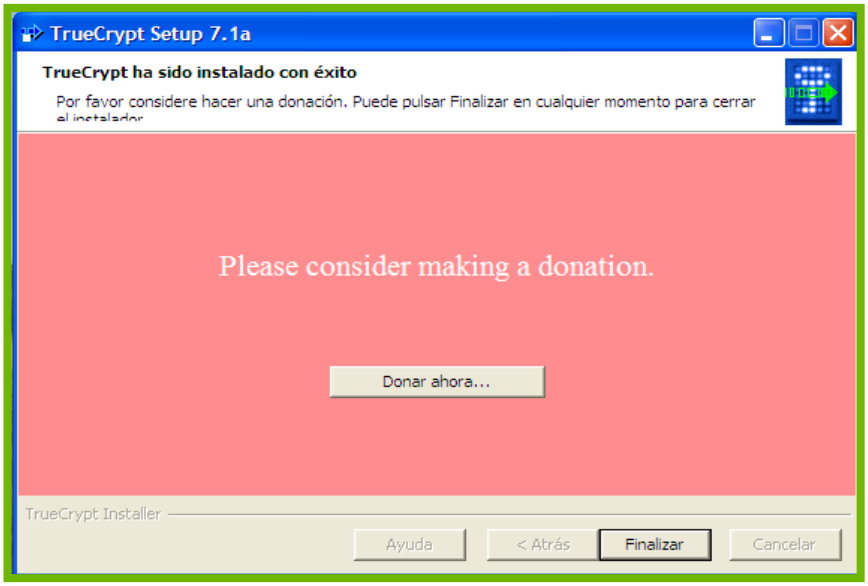
Paso 8: Esperara unos segundos mientras el programa se instala. (Ver imagen 8).



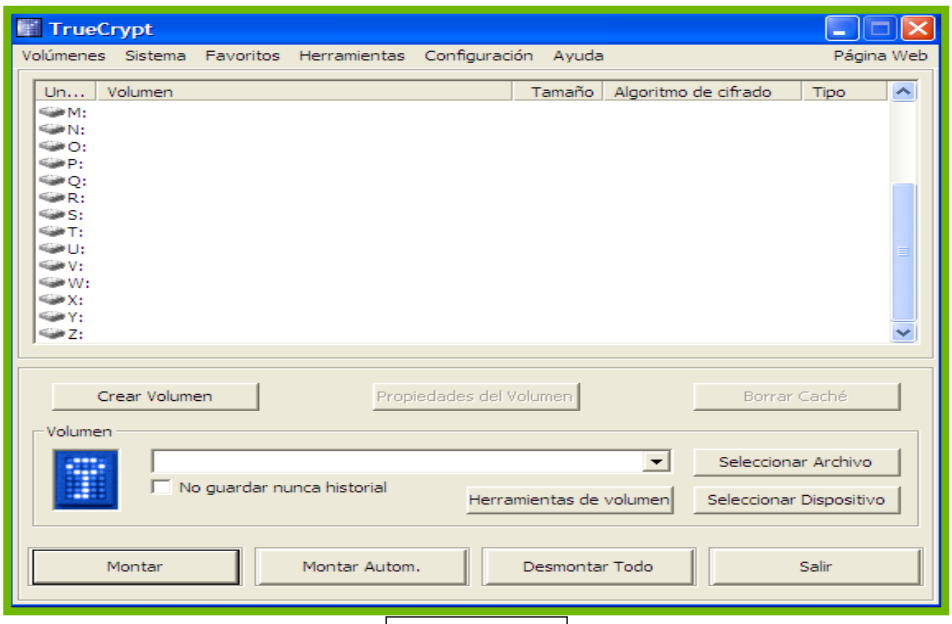
Paso 9: El programa se ha instalado, dar clic en aceptar. (Ver imagen 9).



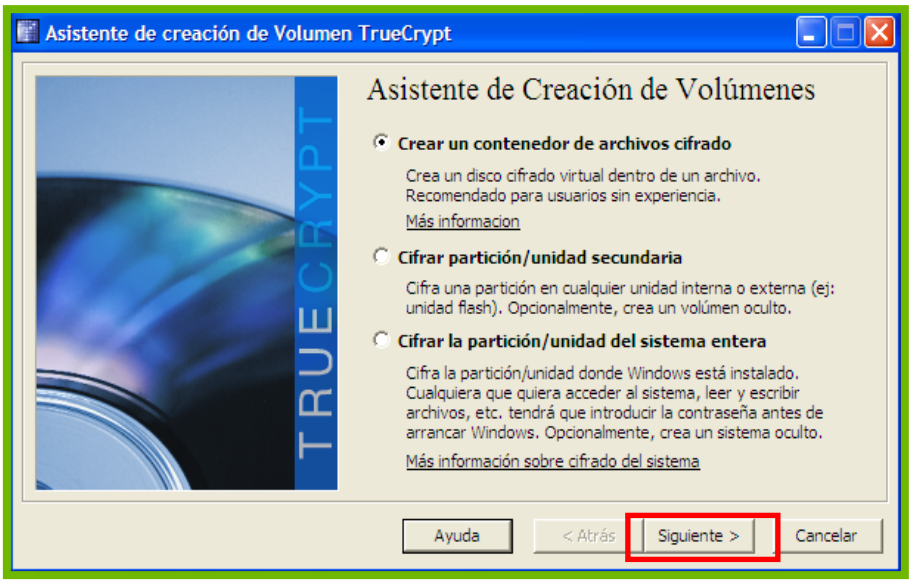
Paso 10: En esta pantalla dar clic en finalizar. (Ver imagen 10).



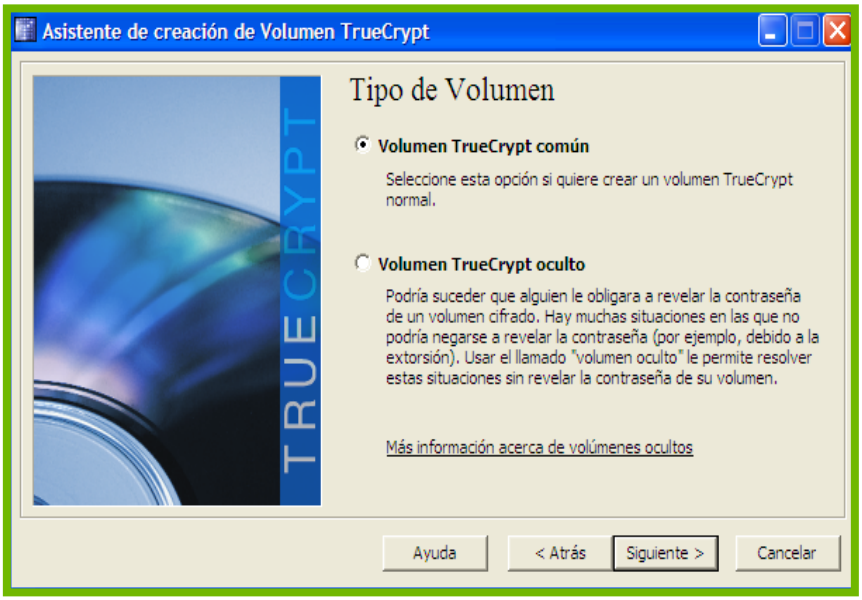
Paso 11: Esta es la primera ventana del programa en cual aparece un listado de unidades y se elige la unidad en la cual se desea crear el volumen de encriptación. Luego dar clic en Crear Volumen. (Ver imagen 11).



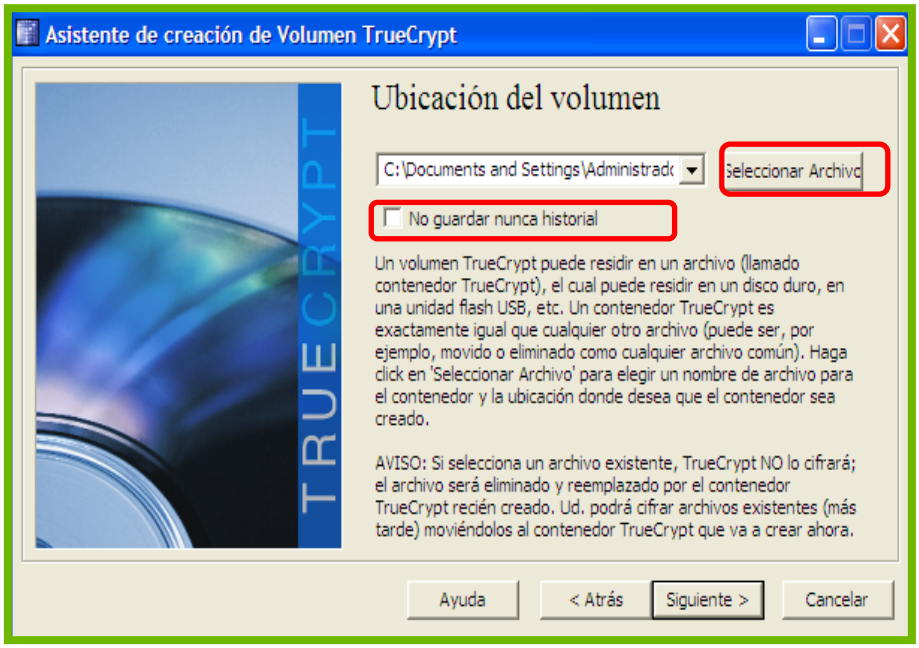
Paso 12: Aparece el Asistente de creación de Volumen, se deja mercada las opciones que ya tiene por defecto y dar clic en siguiente. (Ver imagen 12).



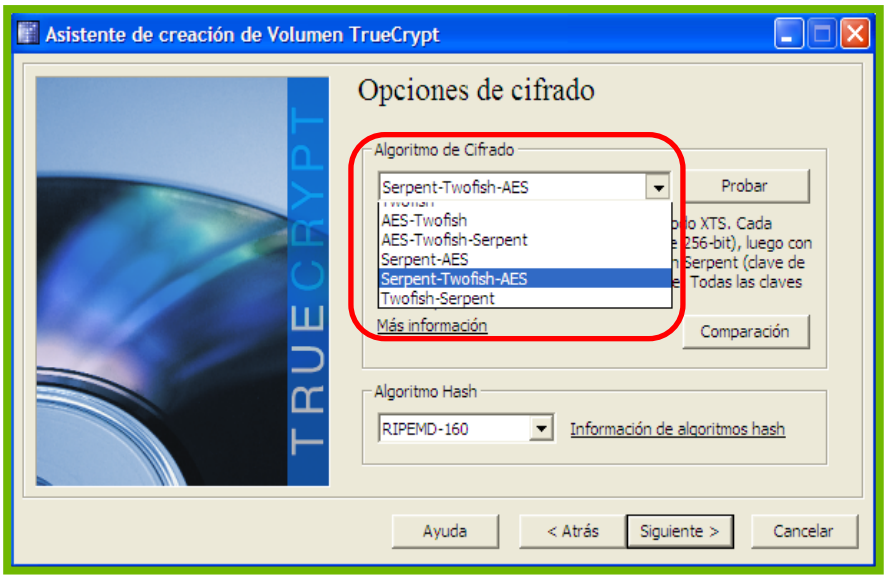
Paso 13: En esta ventana clic en siguiente (Ver imagen13).



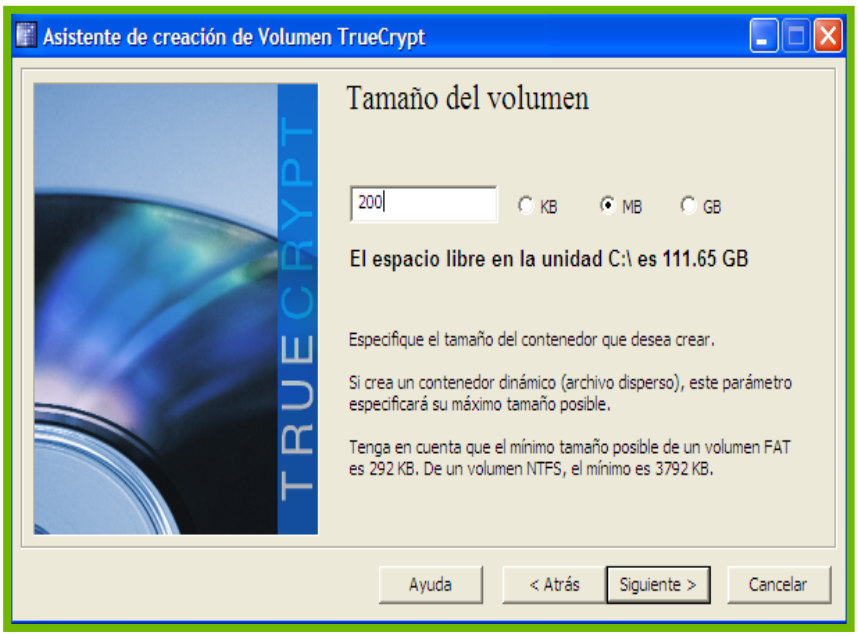
Paso 14: Seleccionar un archivo de la computadora, cuando ya se eligió dar clic en el botón guardar y desmarcar la opción No guardar nunca Historial y dar clic en siguiente (Ver imagen 14).



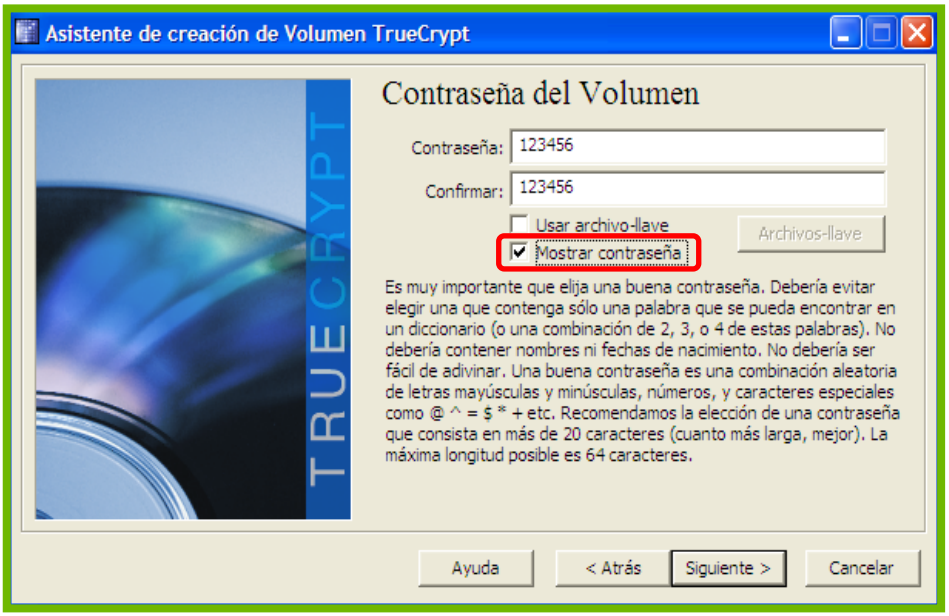
Paso 15: Seleccionar el tipo de algoritmo de encriptación y dar clic en siguiente (Ver imagen 15).



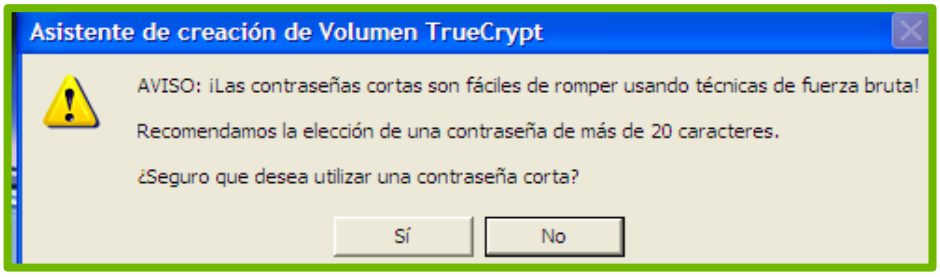
Paso 16: En esta ventana se le asigna el tamaño de volumen, dar clic en siguiente (Ver imagen 16).



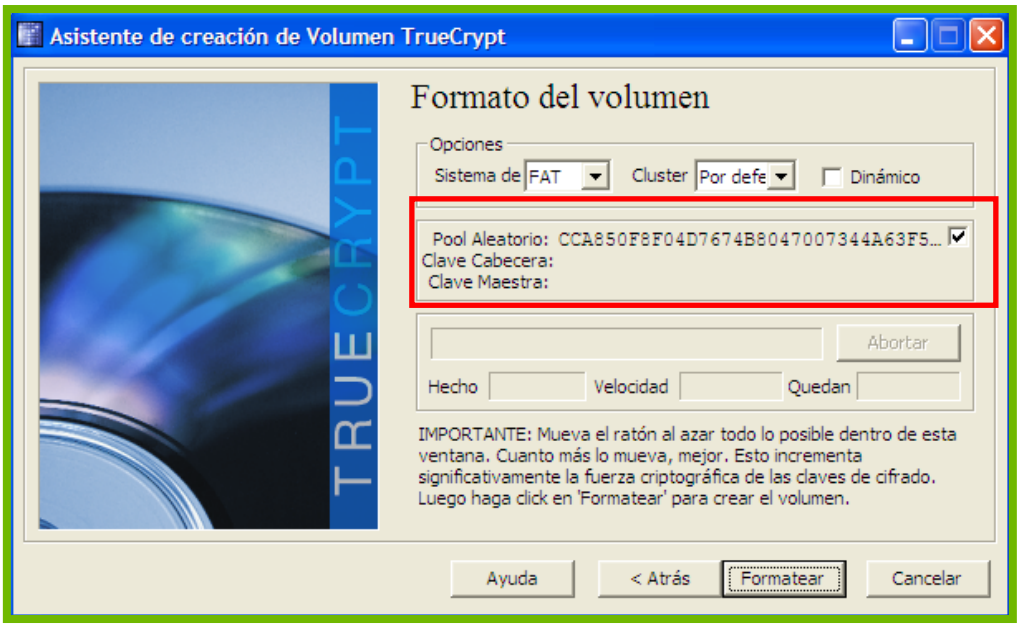
Paso 17: Crear una contraseña y marcar la opción Mostrar contraseña, clic en siguiente (Ver imagen 17).



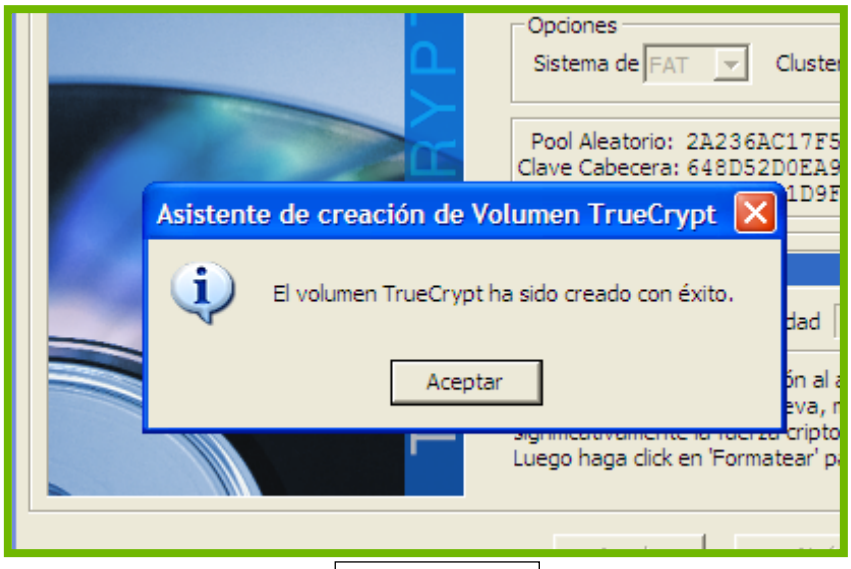
Paso 18: Clic en la opción si se desea usar una contraseña corta, es recomendable una contraseña de 20 caracteres para mayor seguridad de encriptación. (Ver imagen 18)



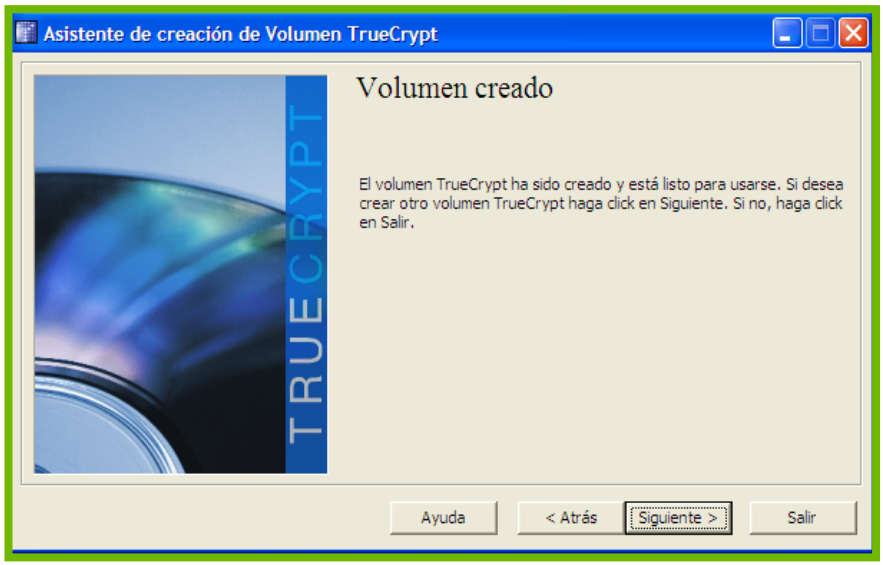
Paso 19: Una técnica para que el algoritmo sea más seguro es mover el mouse en la opción que dice Pool Aleatorio, después de unos segundos de realizar este movimiento, dar clic en Formatear (Ver imagen 19).



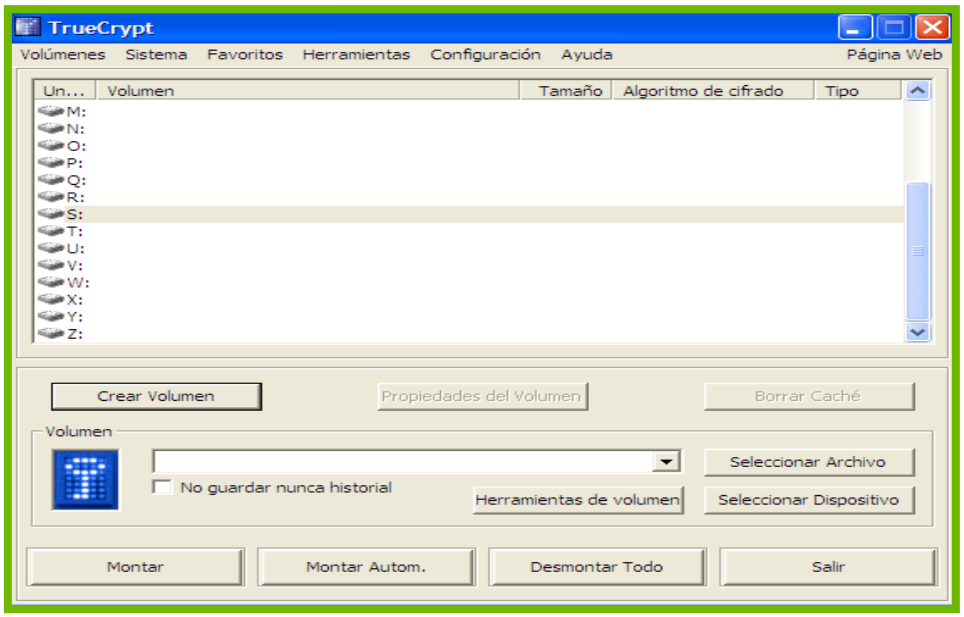
Paso 20: True Crypt ha creado el volumen, dar clic en aceptar. (Ver imagen 20).

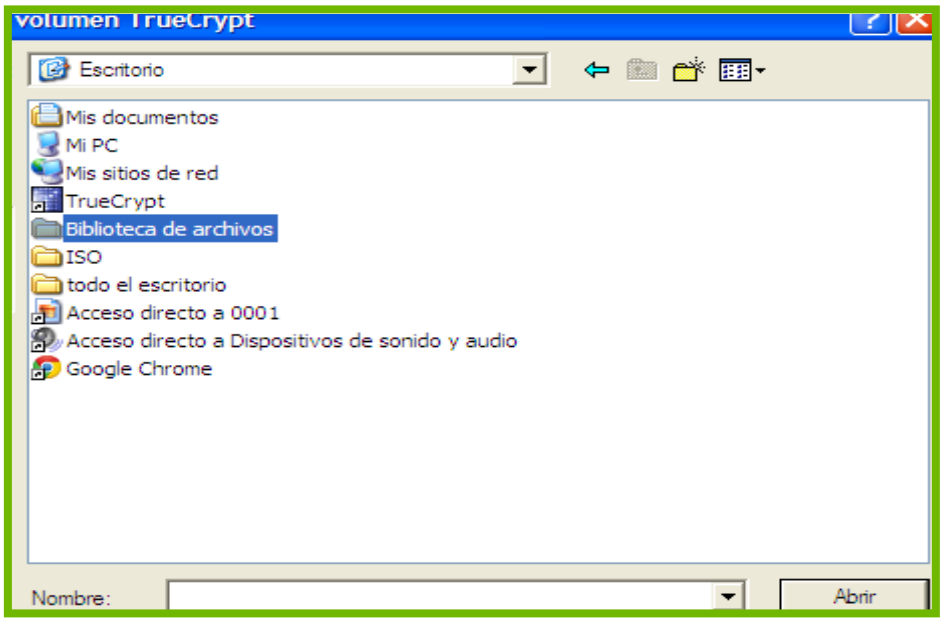


Paso 21: ahora ya está creado el volumen TrueCrypt dar clic en siguiente para continuar con el programa. (Ver imagen 21)

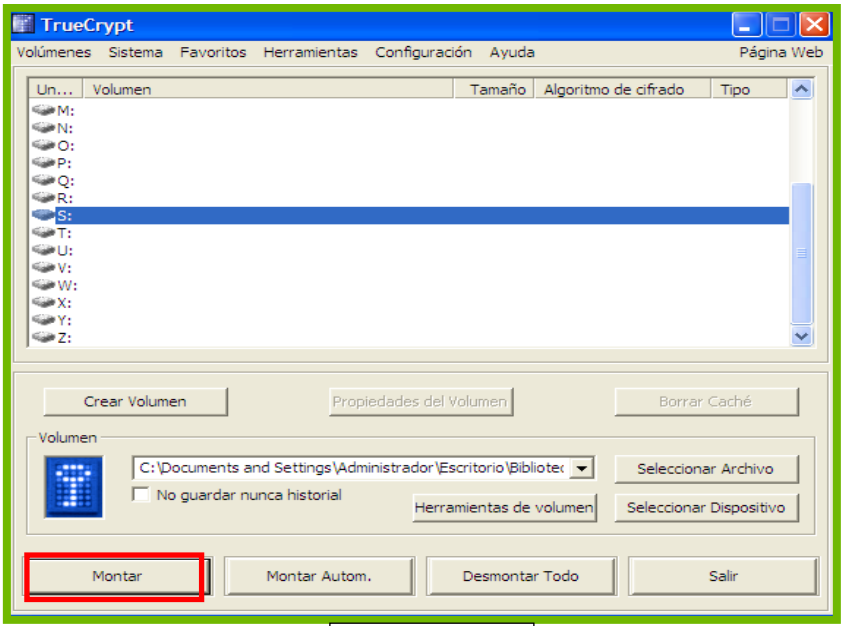


Paso 22: Ahora seleccionar la ubicación en la que se creó el volumen, aparece oculta; para hacerla ver dar clic al botón Seleccionar Archivo en el cual se ha basado para crear el cifrado, seleccionar el archivo y clic en abrir (Ver imagen 22 y 23).

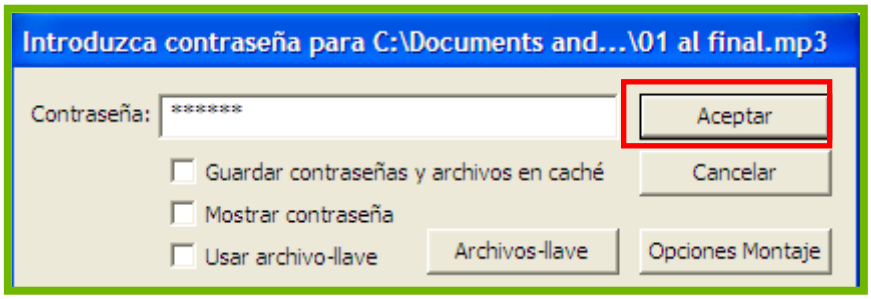




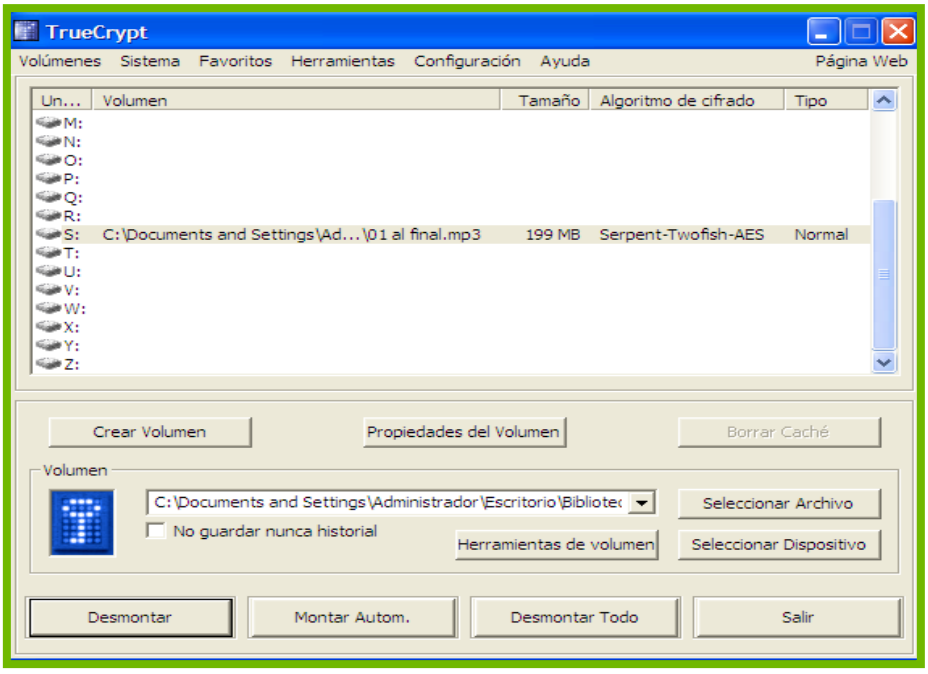
Paso 23: Dar clic sobre la opción Montar ya que la unidad no se puede utilizar si no se monta. (Ver imagen 24)

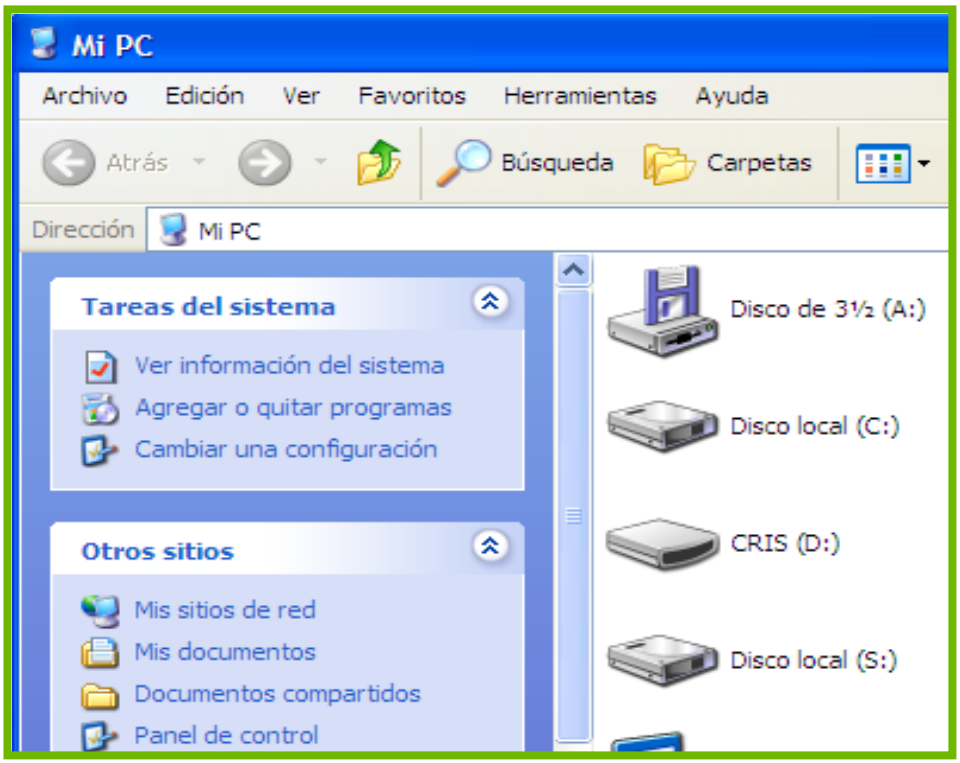


Paso 24: Introducir la clave que anteriormente se asignó y dar clic en aceptar (Ver imagen 25).

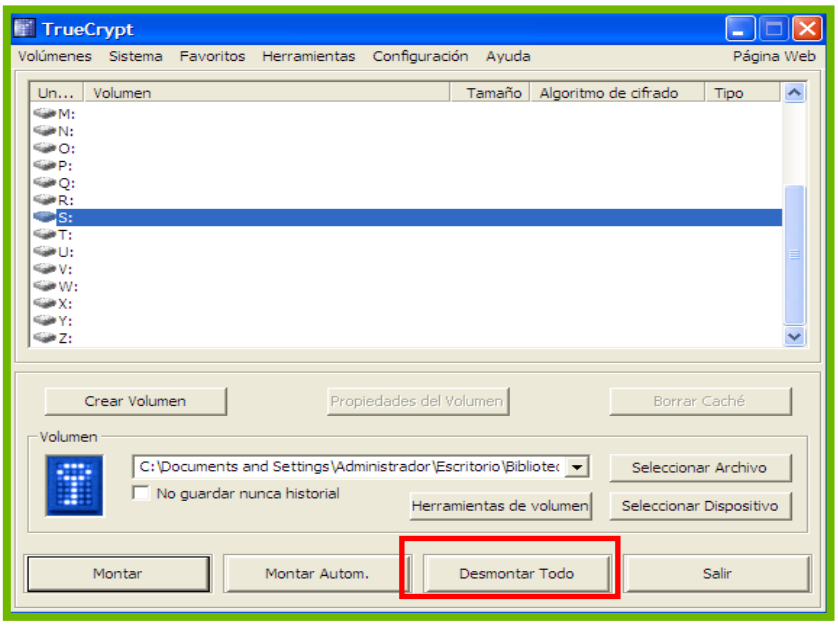


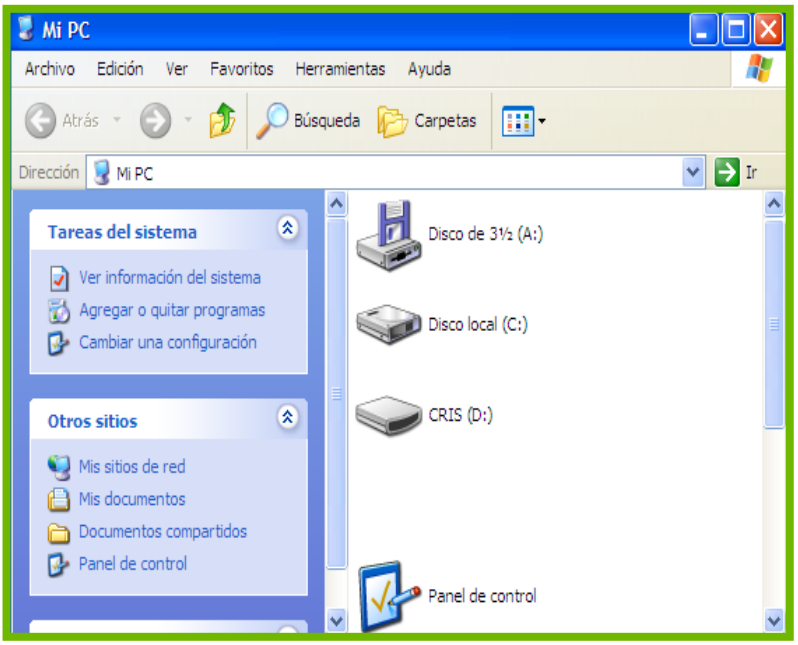
Paso 25: Ahora ya aparece la unidad en la que creo el volumen, y también aparece en la computadora. (Ver imagen 26 y 27)





Paso 26: Si no se desea que esta unidad este visible y los datos que esta contiene sigan ocultos se le debe dar clic en el botón Desmontar y los archivos que esta contengan serán ocultos aunque se busquen por nombre en la computadora (Ver imagen 28 y 29).


TrueCrypt
Volúmenes Sistema Favoritos Herramientas Configuración Ayuda Página Web
Un... Volumen Tamaño Algoritmo de cifrado Tipo
M:
N:
O:
P:
Q:
R:
S:
T:
U:
V:
W:
X:
Y:
Z:
Crear Volumen
Propiedades del Volumen
Borrar Caché
Volumen
C:\Documents and Settings\Administrador\Escritorio\Bibliotec
Seleccionar Archivo
No guardar nunca historial
Herramientas de volumen
Seleccionar Dispositivo
Montar
Montar Autom.
Desmontar Todo
Salir


Mi PC
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás
Búsqueda
Carpetas
Dirección
Mi PC
Ir
Tareas del sistema
Ver información del sistema
Agregar o quitar programas
Cambiar una configuración
Otros sitios
Mis sitios de red
Mis documentos
Documentos compartidos
Panel de control
Disco de 3½ (A:)
Disco local (C:)
CRIS (D:)
Panel de control

AxCrypt Manual

- ✓ **Instalación**
- ✓ **Encriptar**
- ✓ **Desencriptar**

INSTALACIÓN

Paso 1: Introducir el cd del kit de herramientas en el reproductor de CD ó DVD e introducir la bandeja. (Ver imagen 1)

Imagen 1

Paso 2: Aparece la siguiente ventana, dar clic en el botón programas. (Ver imagen 2)

Imagen 2

Paso 3: Dar clic en el boton de esteganografia. (ver imagen 3)

Imagen 3

Paso 4: Ubicar el icono del programa AxCrypt y dar clic para iniciar la instalación (Ver imagen 4)

Imagen 4

Paso 5: Dar clic en I Agree para aceptar los términos de licencia. (Ver imagen 5)

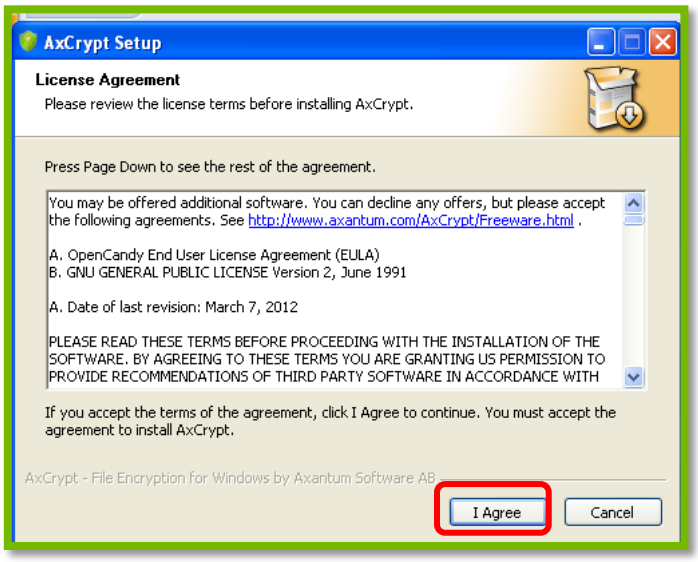


Imagen 5

Paso 6: Preparándose para la instalación. (Ver imagen 6)

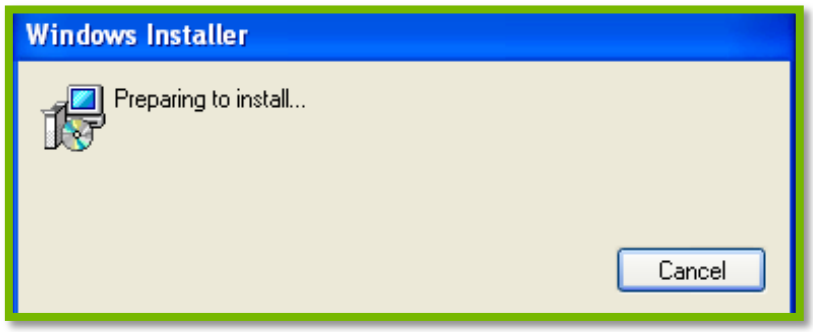


Imagen 6

Paso 7: Dar clic en Finish para finalizar la instalación. (Ver imagen 7)

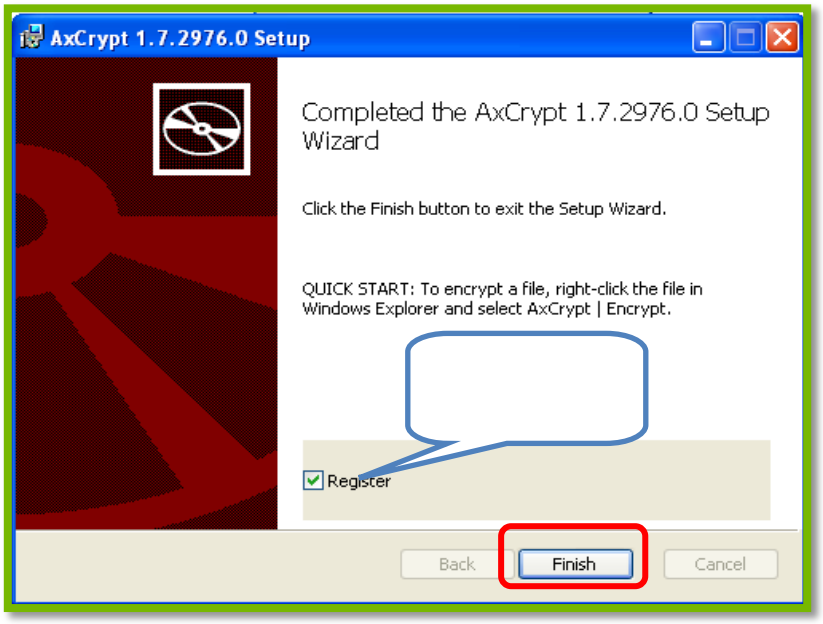


Imagen 7

ENCRIPTAR

Paso 8: Dar clic derecho al documento que se desea encriptar seleccionar AxCrypt y clic en Encrypt. (Ver imagen 8)

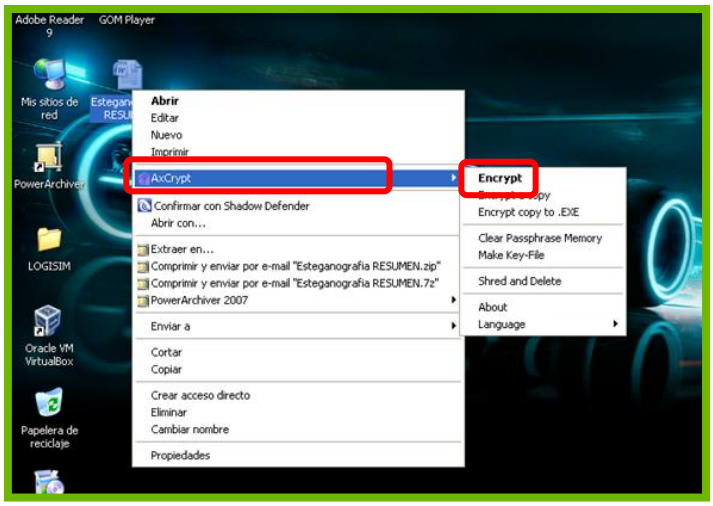


Imagen 8

Paso 9: Introducir la clave que se desee. (Ver imagen 9)

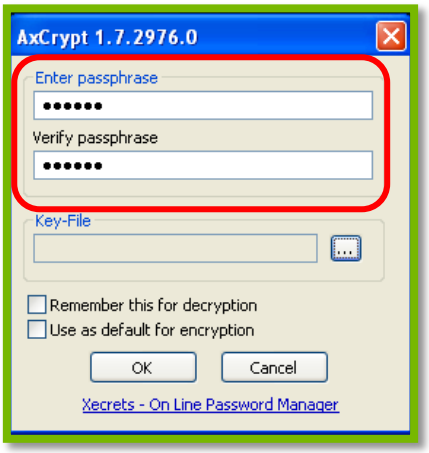


Imagen 9

Paso 10: El documento aparecerá encriptado. (Ver imagen 10)

Imagen 10

DESENCRIPTAR

Paso 11: Dar clic derecho sobre el documento encriptado seleccionar AxCrypt y dar clic sobre Decrypt. (Ver imagen 11)

Imagen 11

Paso 12: Introducir la clave y dar clic en ok. (Ver imagen 12)

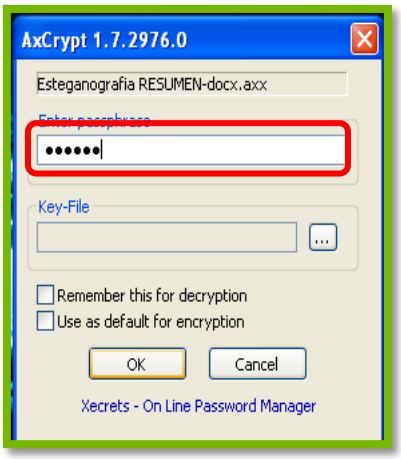


Imagen 12

Paso 13: El archivo aparecerá desencriptado. (Ver imagen 13)

Imagen 13

Paranoic Encryption Manual

- ✓ **Instalación**
- ✓ **Encriptar texto**
- ✓ **Desencriptar texto**

Ejecución

Paso 1: Introducir el cd del kit de herramientas en el reproductor de CD ó DVD e introducir la bandeja. (Ver imagen 1)

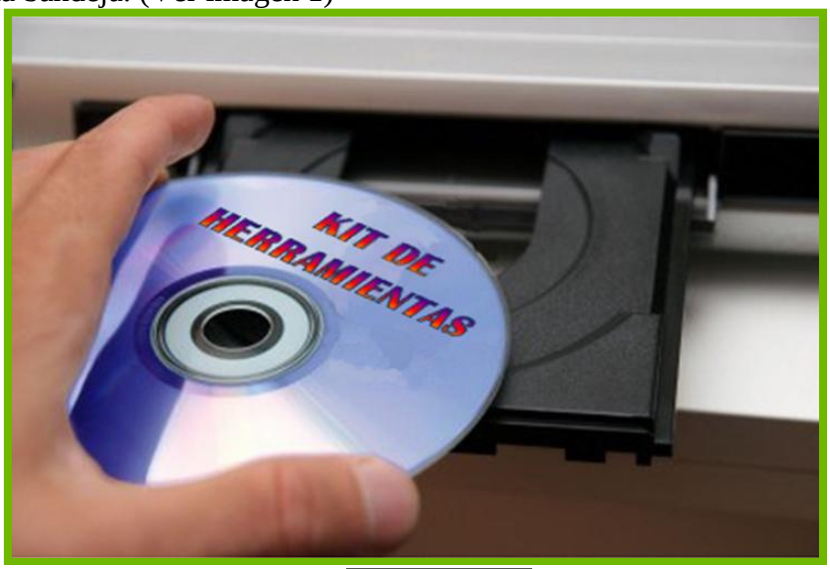


Imagen 1

Paso 2: Aparece la siguiente ventana, dar clic en el botón programas. (Ver imagen 2)

Imagen 2

Paso 3: Dar clic en el boton de esteganografia. (ver imagen 3)

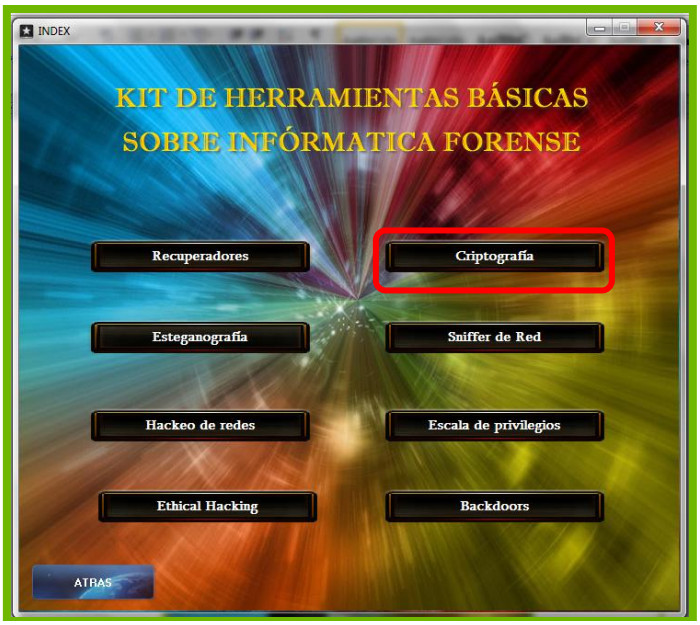


Imagen 3

Paso 4: Ubicar el icono del programa Paranoic Encryption, dar clic para ejecutar el programa (Ver imagen 4)

Imagen 4

ENCRIPTAR

Paso 5: Introducir la clave que se desee, entre más larga y segura sea será mucho mejor. (Ver imagen 5)

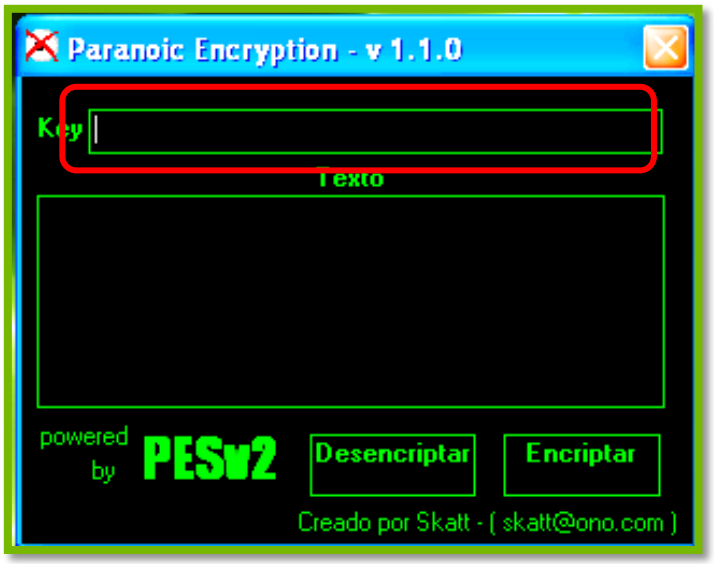


Imagen 5

Paso 6: Introducir el texto que se desea encriptar. (Ver imagen 6)

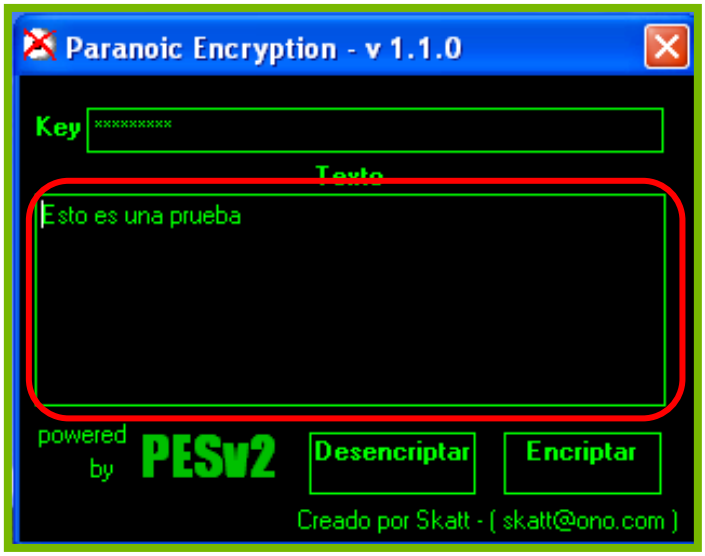


Imagen 6

Paso 7: Dar clic en el botón de encriptar para que el texto se encripte (Ver imagen 7)

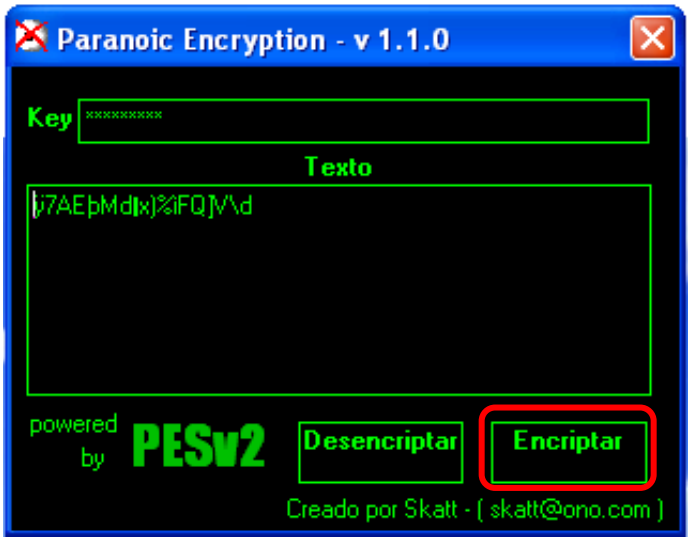


Imagen 7

DESENCRIPTAR

Paso 8: Introducir el texto y la clave que se le ha ingresado anteriormente. (Ver imagen 8)

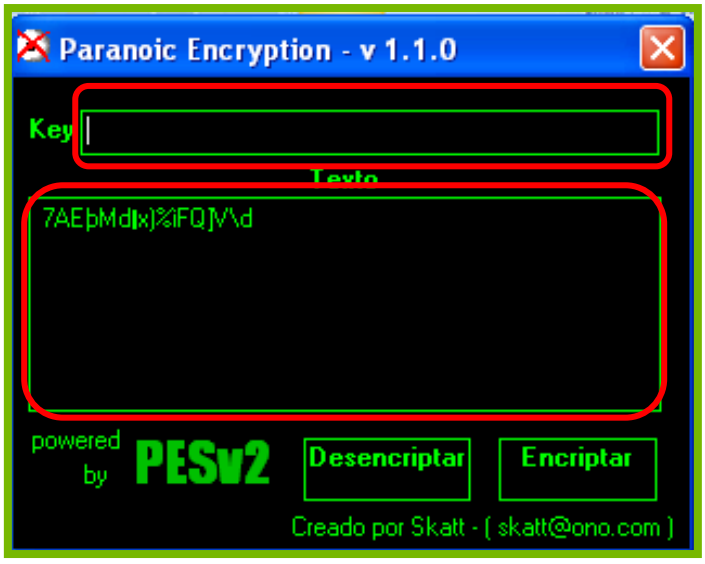


Imagen 8

Si la clave que se introduce no es correcta o no se introduce el texto no se podrá desencriptar. (Ver imagen 9)

Imagen 9

Paso 9: Dar clic en desencriptar. (Ver imagen 10)

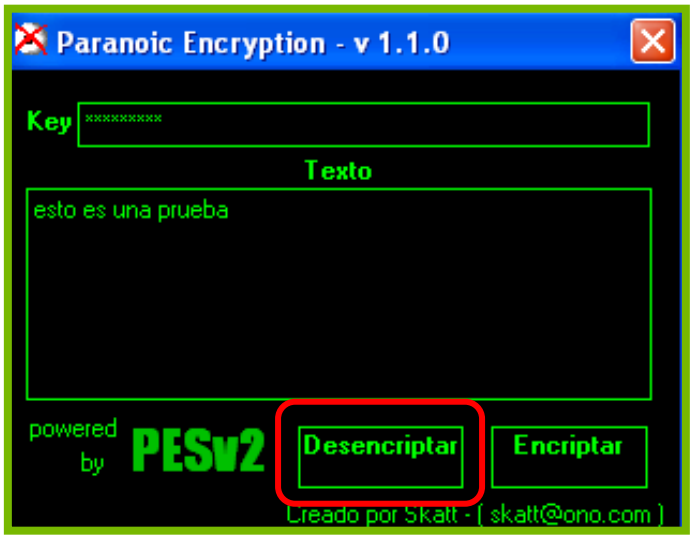


Imagen 10

4. SNIFFER DE RED

4.1 CONCEPTO

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

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

4.2 PROGRAMA

4.2.1 FREE IP TOOLS

Free IP Tools Manual

- ✓ **Instalación**
- ✓ **Auditoria de red**

INSTALACIÓN

Paso 1: Introducir el cd del kit de herramientas en el reproductor de CD o DVD e introducir la bandeja. (Ver imagen 1)

Imagen 1

Paso 2: Aparece la siguiente ventana, dar clic en el botón programas. (Ver imagen 2)

Imagen 2

Paso 3: Dar clic en el botón de esteganografia. (ver imagen 3)

Imagen 3

Paso 4: Ubicar el icono del programa Free IP Tools y dar clic para iniciar la instalación (Ver imagen 4)

Imagen 4

Paso 5: Esta es la ventana de bienvenida para la instalación del Free IP tools. Dar clic en Next (Siguiente) (Ver imagen 5)

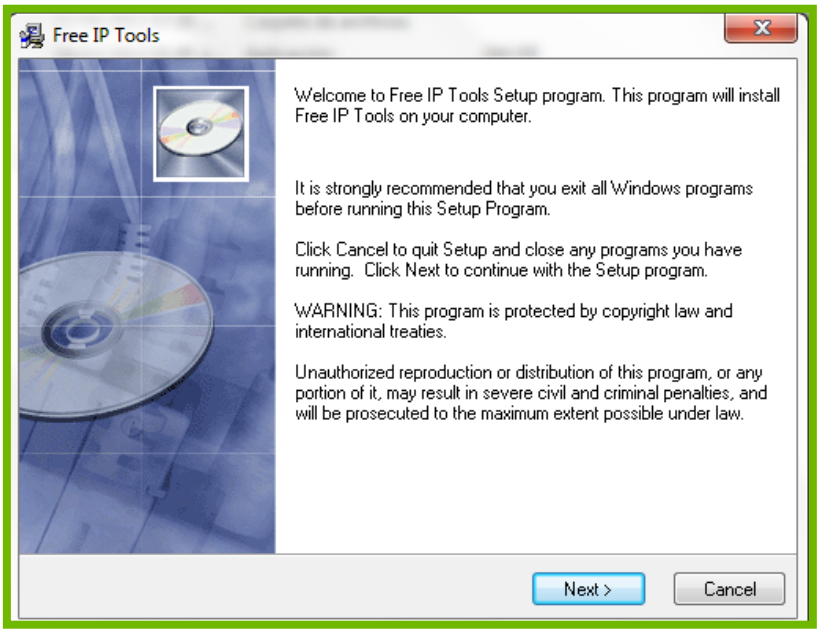


Imagen 5

Paso 6: Aceptar el contrato de licencia, dar clic en Yes para proceder a la instalación. (Ver imagen 6)

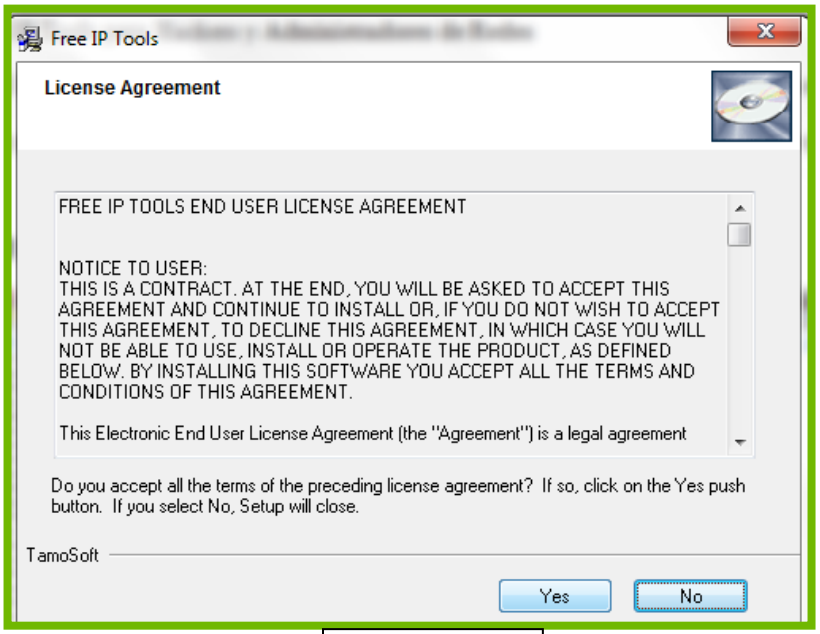


Imagen 6

Paso 7: En esta ventana se puede elegir la ubicación para el programa, dar clic en Browse si se desea instalas en una carpeta diferente a archivos de programas y luego dar clic en Next. (Ver imagen 7)

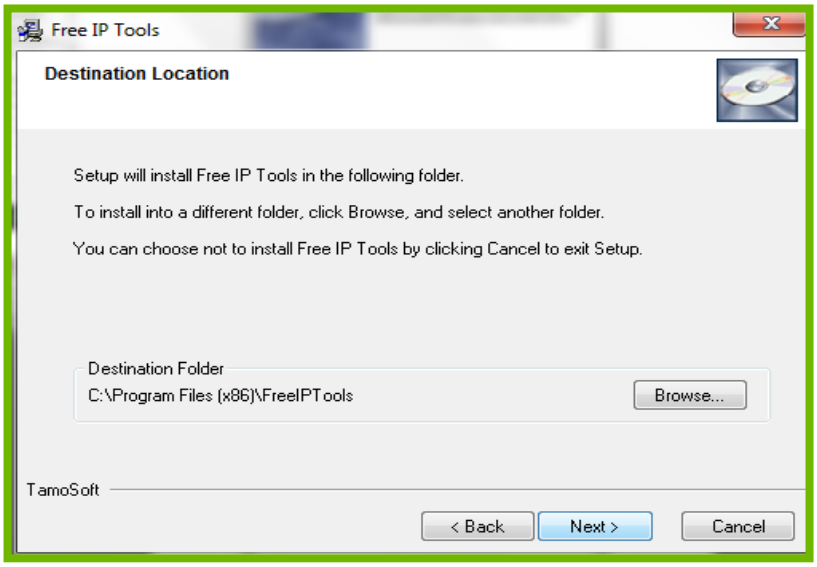


Imagen 7

Paso 8: Escoger el grupo donde se guardará el programa, y dar clic en Next. (Ver imagen 8)

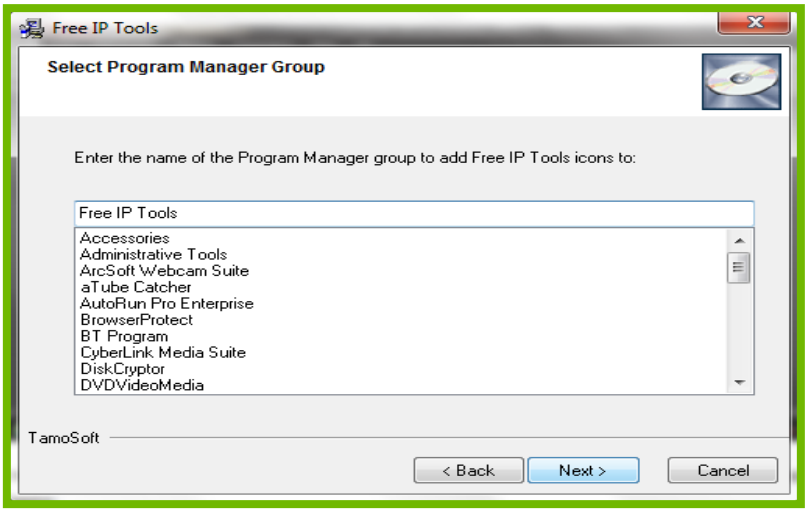


Imagen 8

Paso 9: Elegir idiomas adicionales y luego dar clic en Next. (Ver imagen 9)

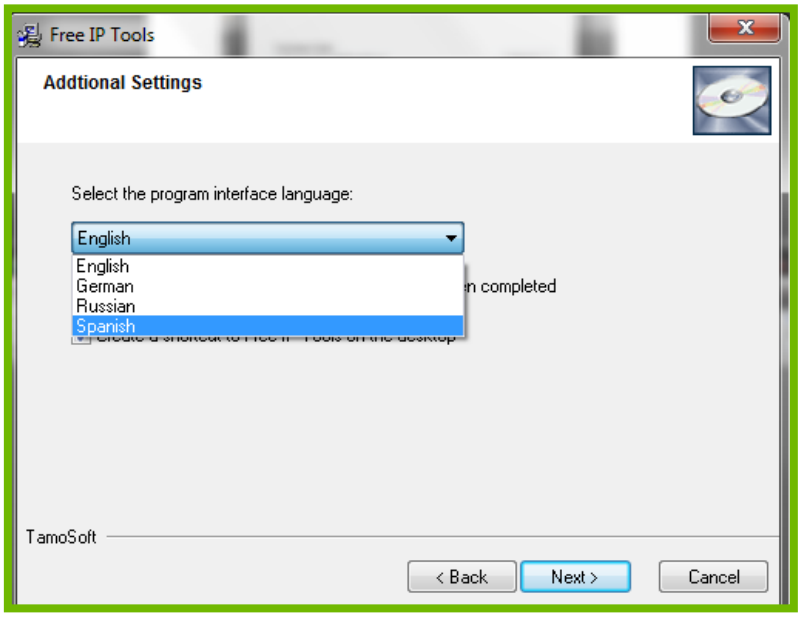


Imagen 9

Paso 10: Presione el botón Next para continuar con la instalación (Ver imagen 10)

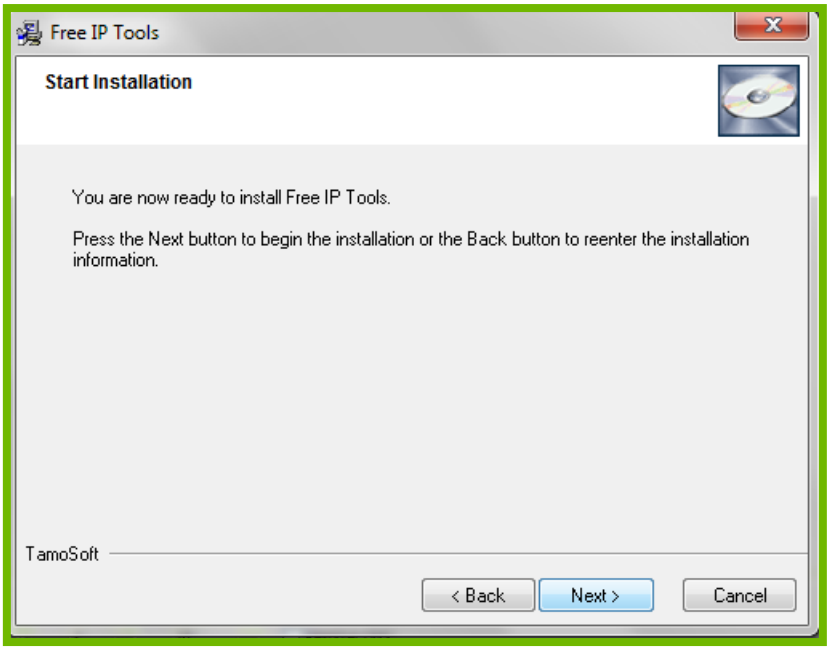


Imagen 10

Paso 11: Esperar unos segundos para que se complete la instalación (Ver imagen 11)

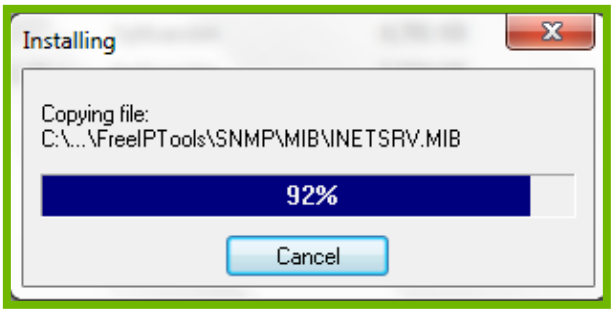


Imagen 11

Paso 12: Dar clic en Finish para terminar la instalación (Ver imagen 12)

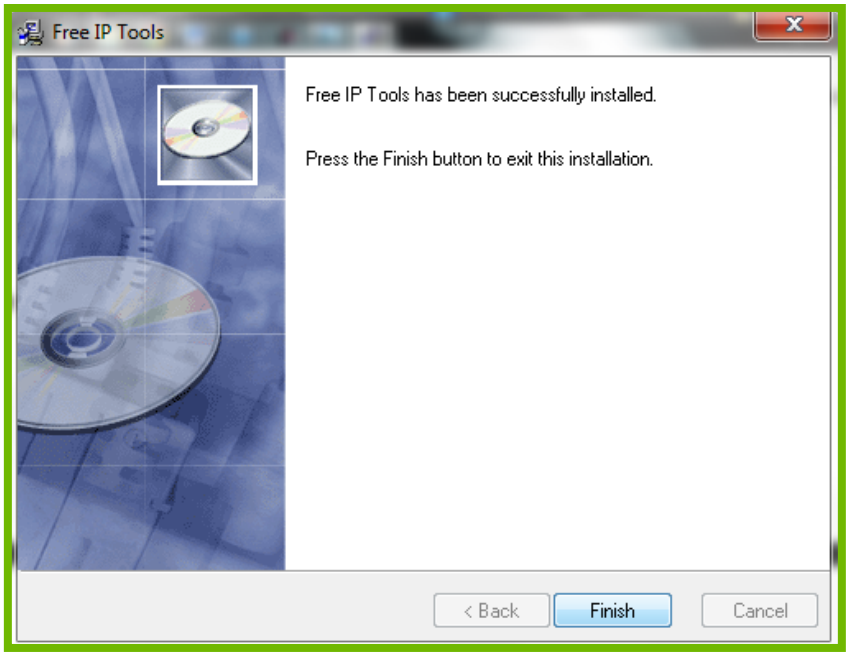


Imagen 12

Una vez instalado y ejecutado el programa, aparecerá una cómoda interfaz como la siguiente: (Ver imagen 13)

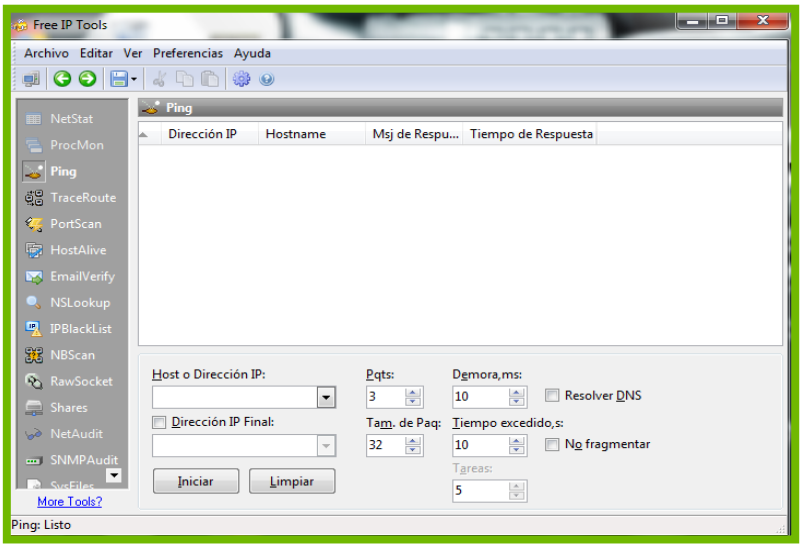


Imagen 13

AUDITAR LA RED

Paso 13: Si se selecciona **PortScan** se hará un escaneo de puertos de una dirección IP, o se puede escanear un rango de direcciones IP. Si se selecciona escanear un rango de direcciones IP, se puede observar los puertos abiertos de las IPs dentro del rango, el número de puertos cerrados y los puertos silenciosos. (Ver imagen 14)

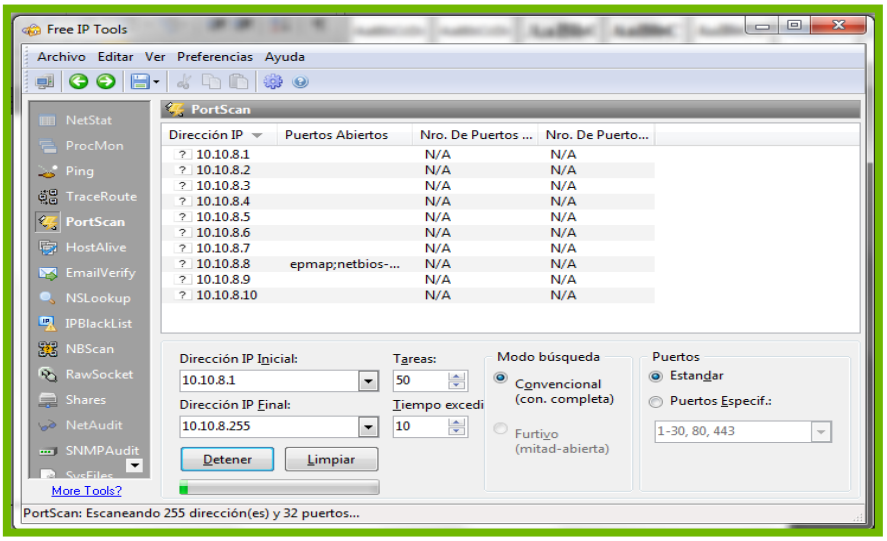


Imagen 14

Paso 14: Si se selecciona **Ping** estará usando el clásico ping para observar si 2 o más nodos se ven dentro de una red. Al igual que en el PortScan se puede hacer dentro de un rango (Ver imagen 15)

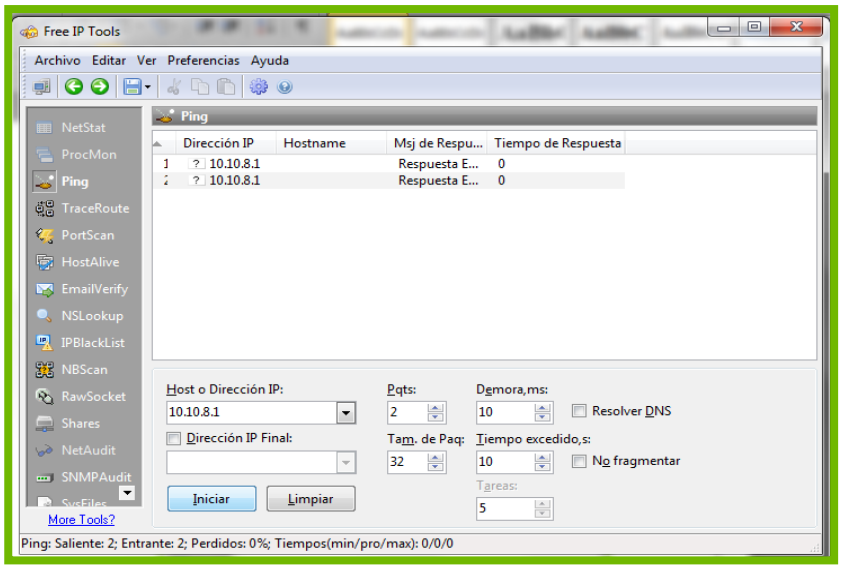


Imagen 15

Paso 15: La herramienta **Traceroute** es el clásico rastreador de paquetes que permite seguir y saber los lugares que pasa nuestros paquetes para ir de un nodo a otro. (Ver imagen 16)

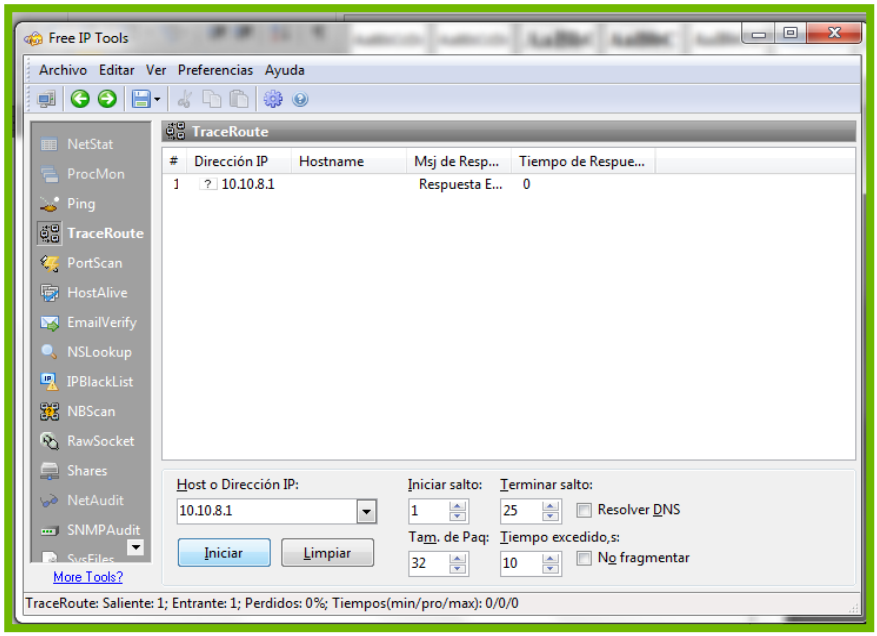


Imagen 16

Paso 16: IPBlackList es una utilidad que permite saber si una determinada dirección IP o un Host está incluida en la lista negra como emisor de Spam. (Ver imagen 17)

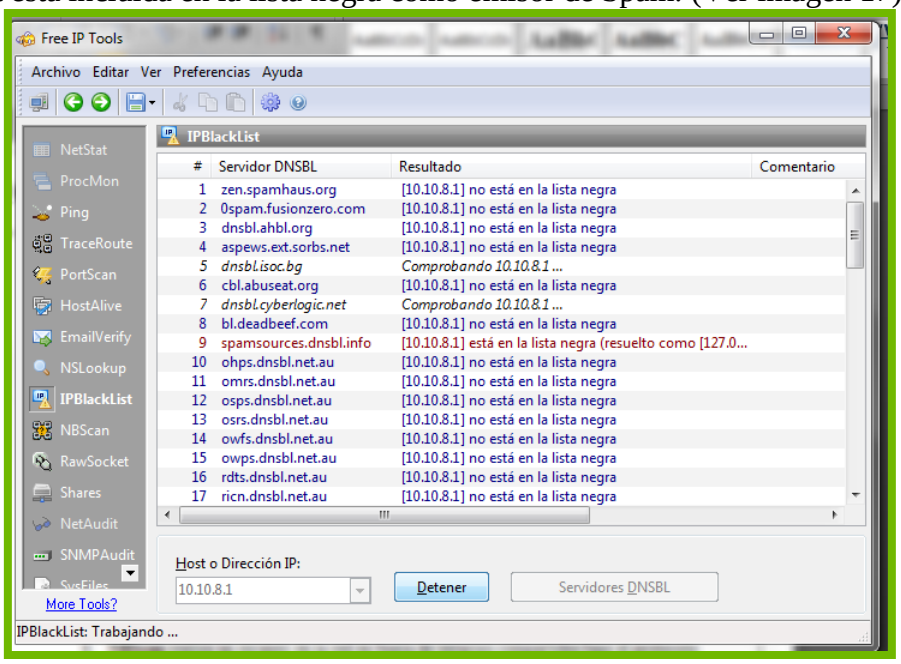


Imagen 17

Paso 17: EmailVerify: Esta herramienta sirve para verificar si las cuentas de correo electrónico se encuentran existentes. (Ver imagen 18)

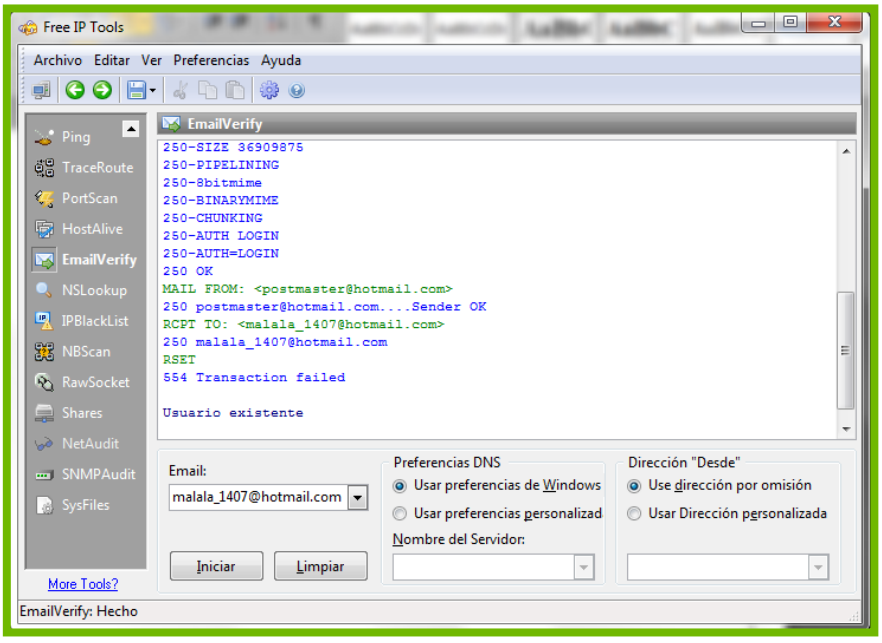


Imagen 18

Paso 18: NSLookup permite observar si la DNS está resolviendo de manera correcta los nombres y las direcciones IPs. (Ver imagen 19)

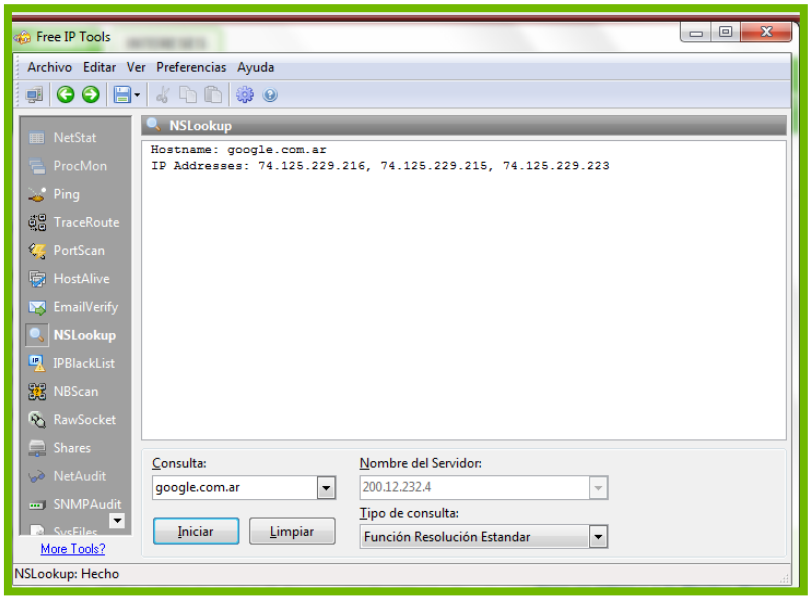


Imagen 19

Paso 19: La herramienta **Shares** permite la conexión de recursos compartidos y monitorizar el pc y sus recursos. Muy útil sobre todo para una red Lan. (Ver imagen 20)

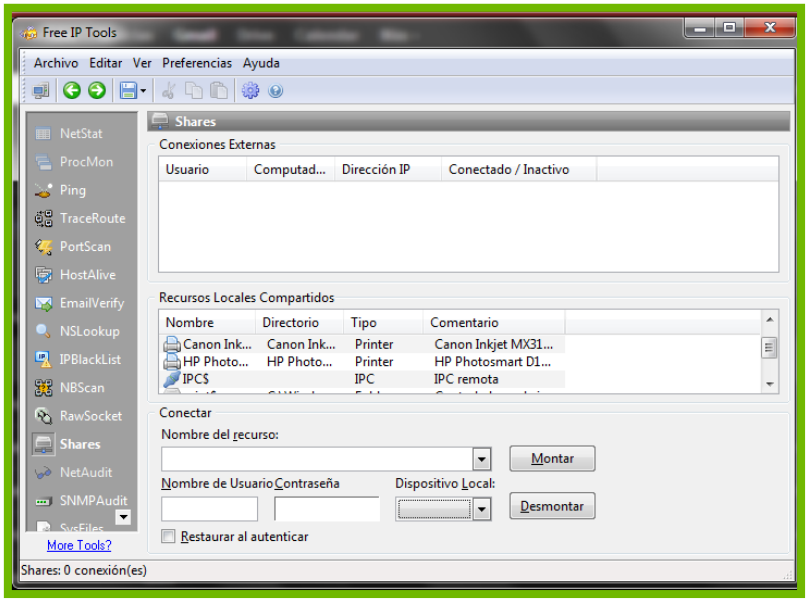


Imagen 20

5. HACKEO DE REDES

5.1 CONCEPTO

Empacar o hackear se refiere a la acción de explorar y buscar las limitantes de un código o de una máquina.

5.2 PROGRAMA

5.2.1 BACKTRACK

Backtrack Manual

- ✓ Instalación
- ✓ Hackeo de redes

UTILIZACIÓN PARA HACKEAR REDES

Paso 1: Introducir el live CD en la lectora de CD/DVD y reiniciar la computadora. (Ver imagen 1)

Imagen 1

Paso 2: Presionamos f12 para configurar la BIOS, seleccionando el CDROM como dispositivo de arranque primario, presionar f10 para reiniciar la pc. (Ver imagen 2)

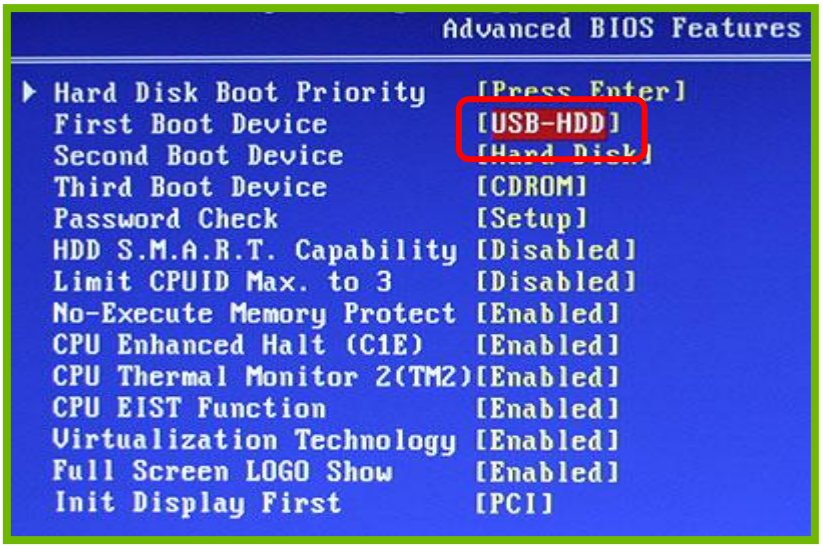


Imagen 2

Paso 3: Aparece esta ventana dar clic en la primera opción**.** (Ver imagen 3)

Imagen 3

Paso 4: cuando cargue todo el proceso aparece una ventana "root@root", Se introduce el comando "startx" sin las comillas y pulsar enter.

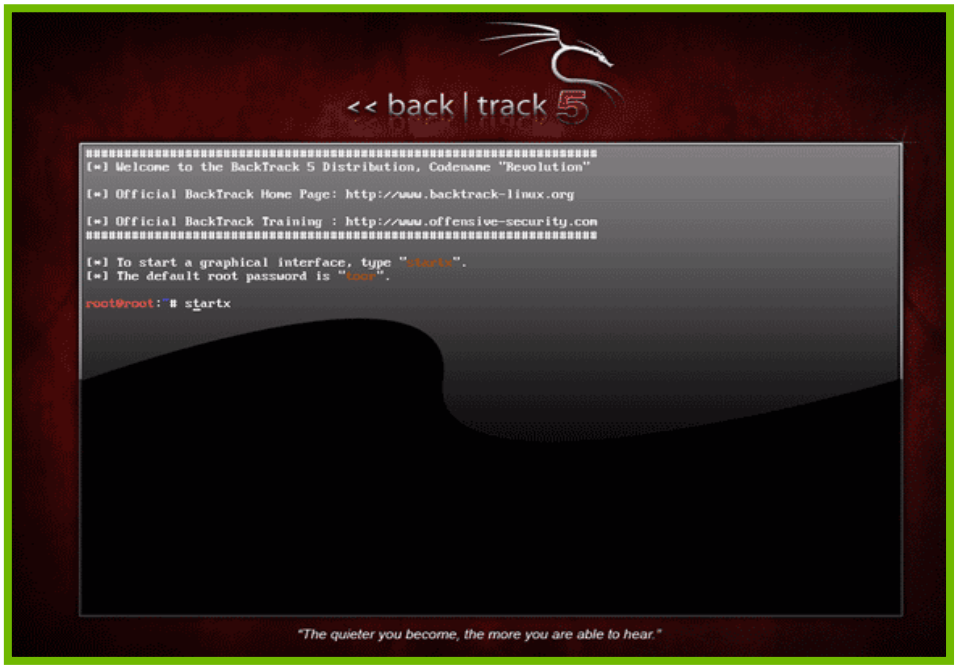


Imagen 4

Paso 5: En esta ventana abrir una terminal. (Ver imagen 5)

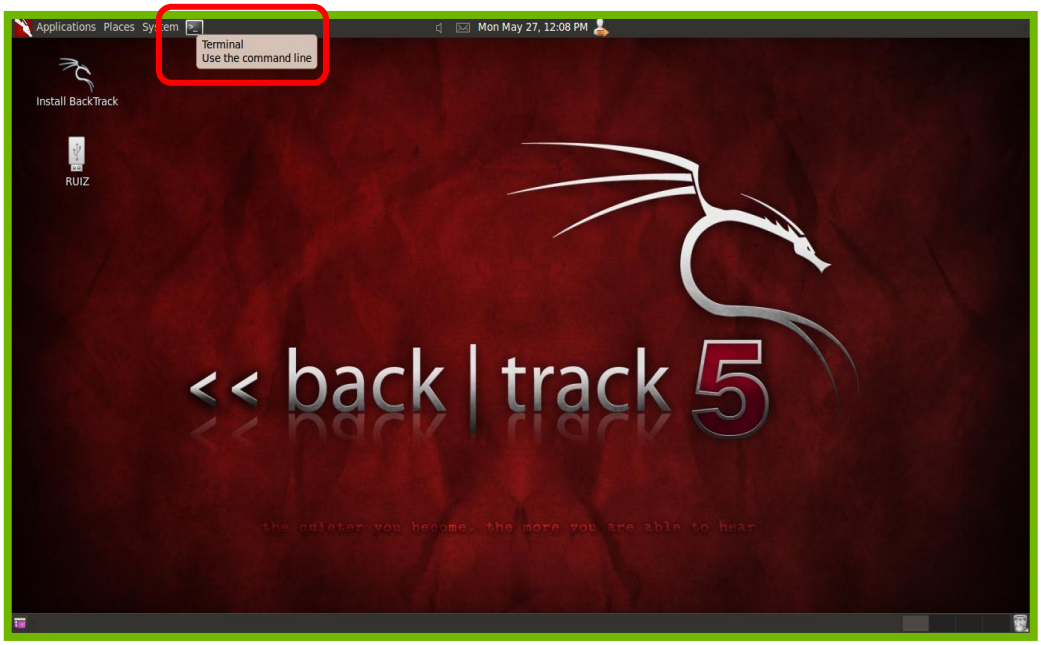


Imagen 5

Paso 6: El segundo paso es poner la tarjeta inalambrica en modo monitor, para esto digitamos el comando: **airmon-ng start wlan0.** (Ver imagen 6)

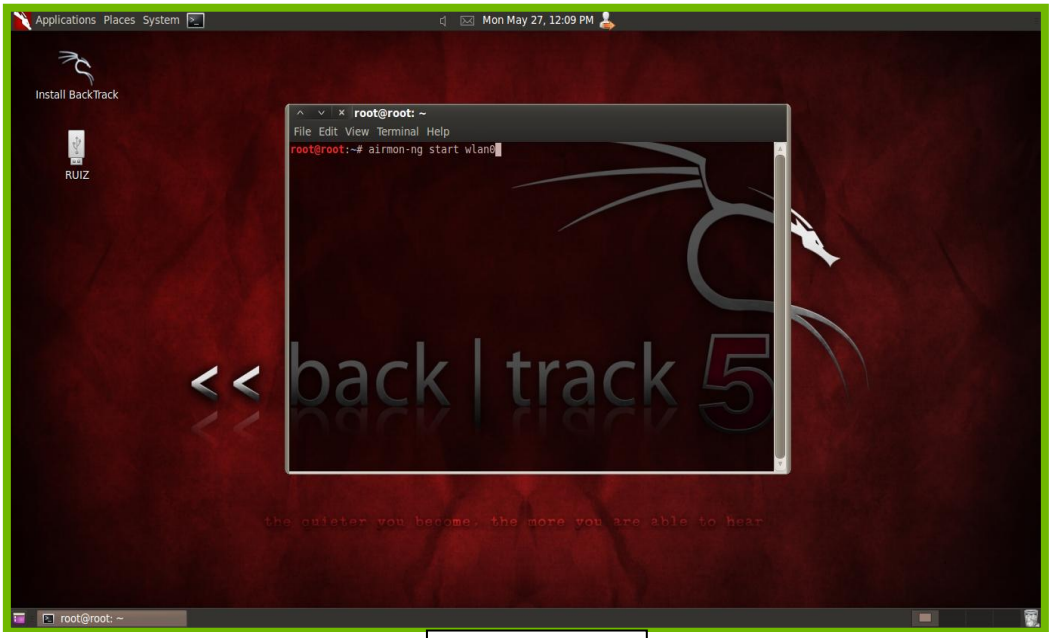


Imagen 6

Paso 7: Ahora se buscarán las redes disponibles, para esto ejecutar el siguiente comando: **airodump-ng mon0.** (Ver imagen 7)

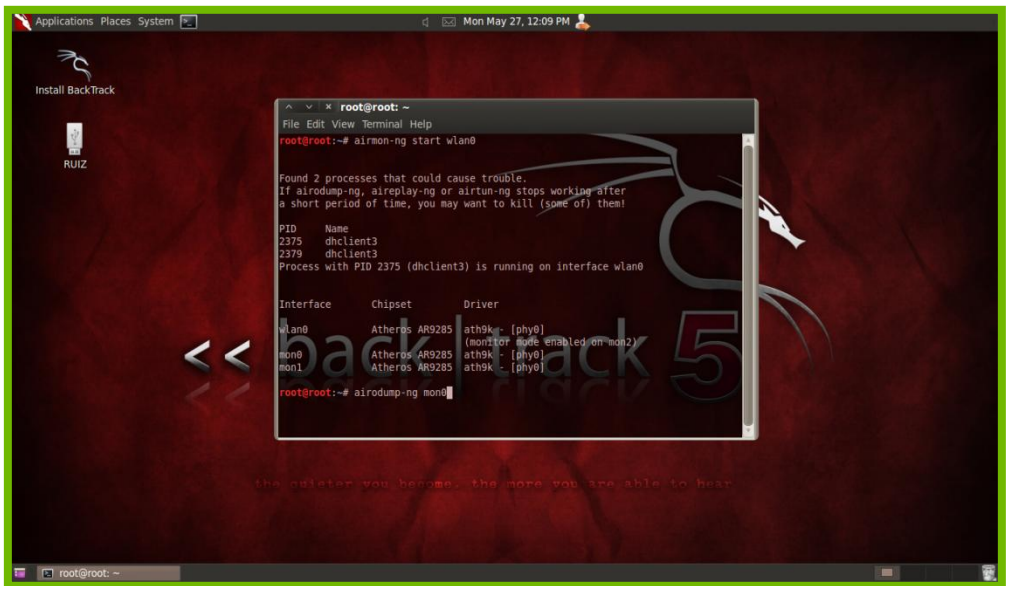


Imagen 7

Como se puede observar aquie se estan escaneando las redes disponibles. Para detener el escaneo presionar **ctrl+c.** (Ver imagen 8)

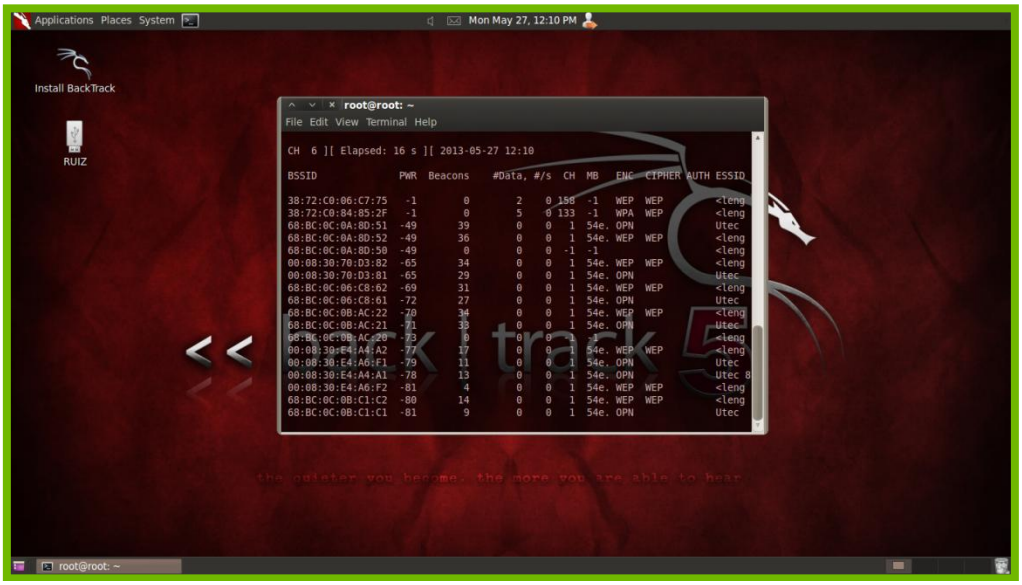


Imagen 8

Paso 8: Aquí se captura la red a hackear para despues obtener el "handshake", y ahora se introduce el siguiente comando: **airodump-ng -w redes -c (canal de la red) --bssid (numero de bssid) mon0.**

Donde: -w: Es el nombre del archivo donde se guardan la capturas de datos

-c: Especifica el canal de la red

-bssid: Especifica la mac (máscara de sub-red) de punto de acceso.

Mon0: Es la interfaz de la tarjeta de red en modo monitor. (Ver imagen 9)

Imagen 9

Aquí se puede observar que se esta escaneando la red y la estación de la red a Hackear (Ver imagen 10)

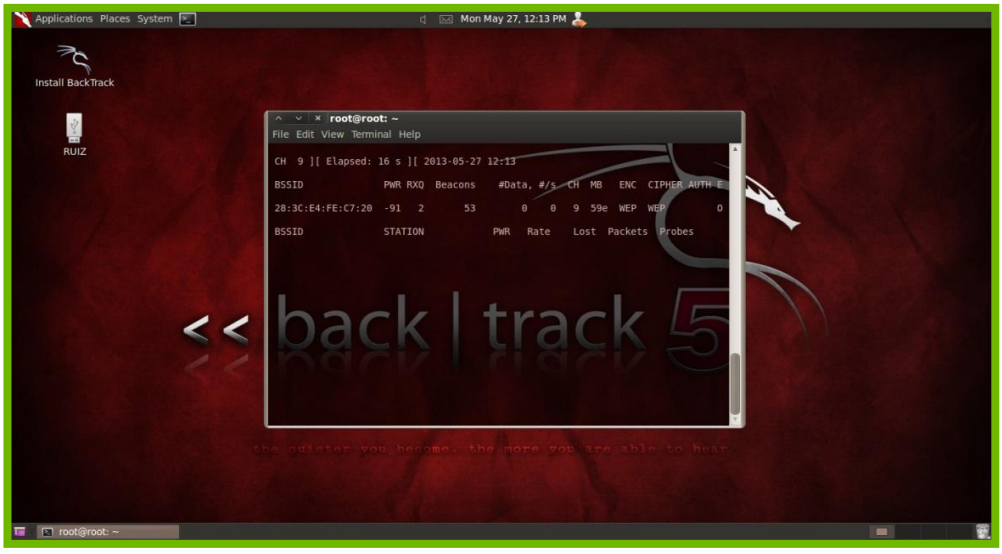


Imagen 10

Paso 9: Ahora abrir una segunda terminal (sin cerrar la primera) y escribir lo siguiente:

Aireplay-ng -deauth -a (bssid) mon0. (Ver imagen 11)

Deauth: (representa # de veces que se desconectará al dispositivo)

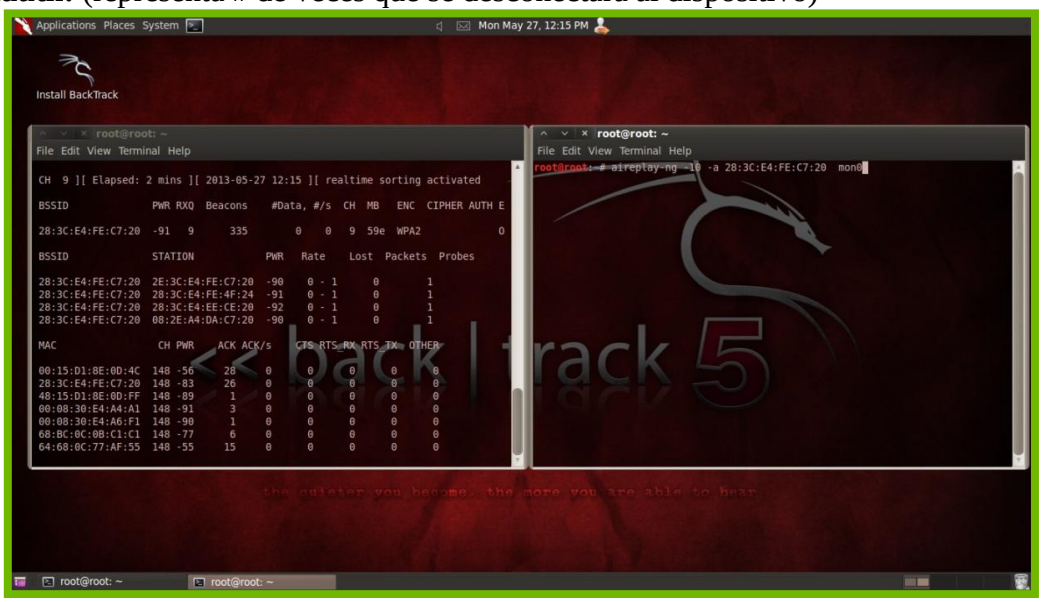


Imagen 11

Paso 10: Ahora la PC esta asociada con la red a hackear.(Ver imagen 12)

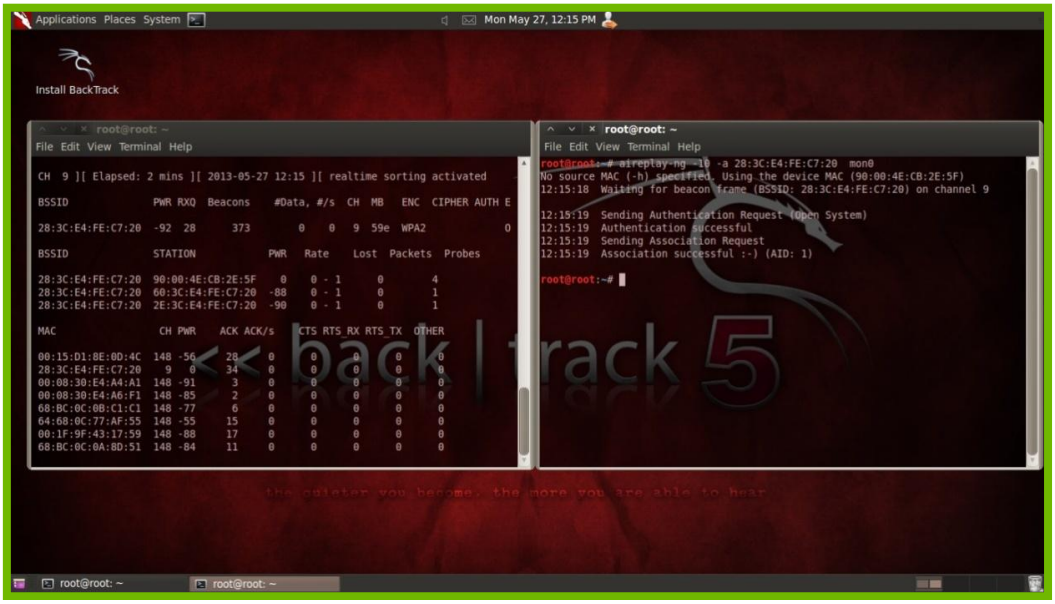


Imagen 12

Paso 11: Ahora hay que inyectar los paquetes a la red, para esto introducimos el siguiente comando: **aireplay-ng -3 –b (bssid) mon0** (Ver imagen 13)

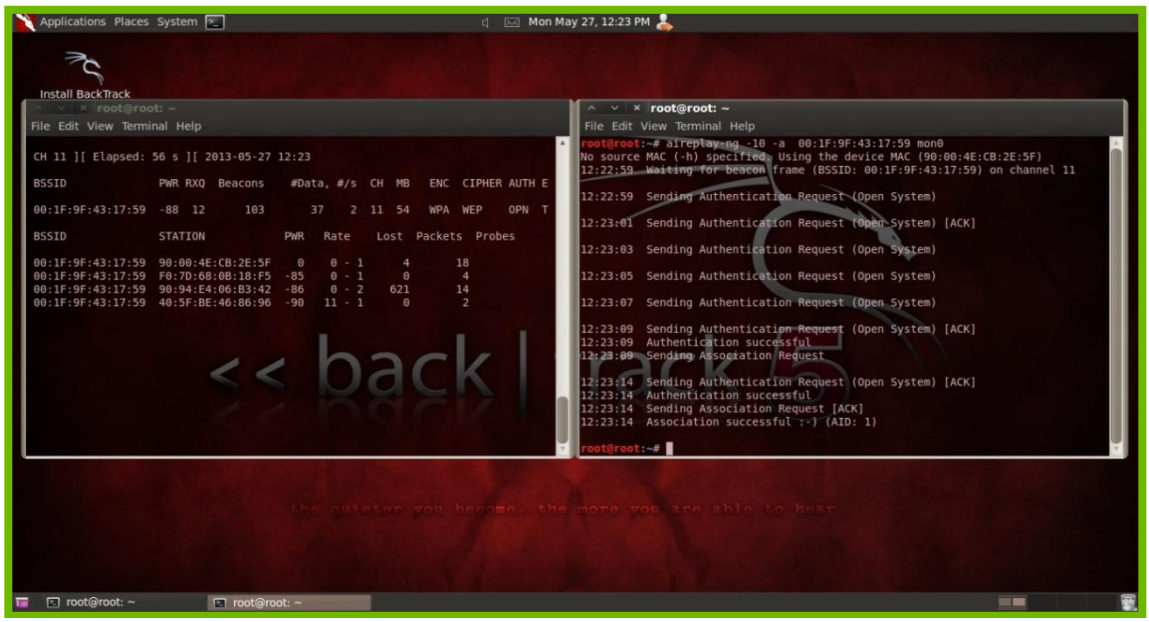


Imagen 13

Con esto se enviarán y recibirán paquetes. Regresar a la primera terminal y en la columna **#data** y se observará que se incrementará rápidamente y esperar a que llegue a los 30,000 datos para poder desencriptar la clave. (Ver imagen 14)

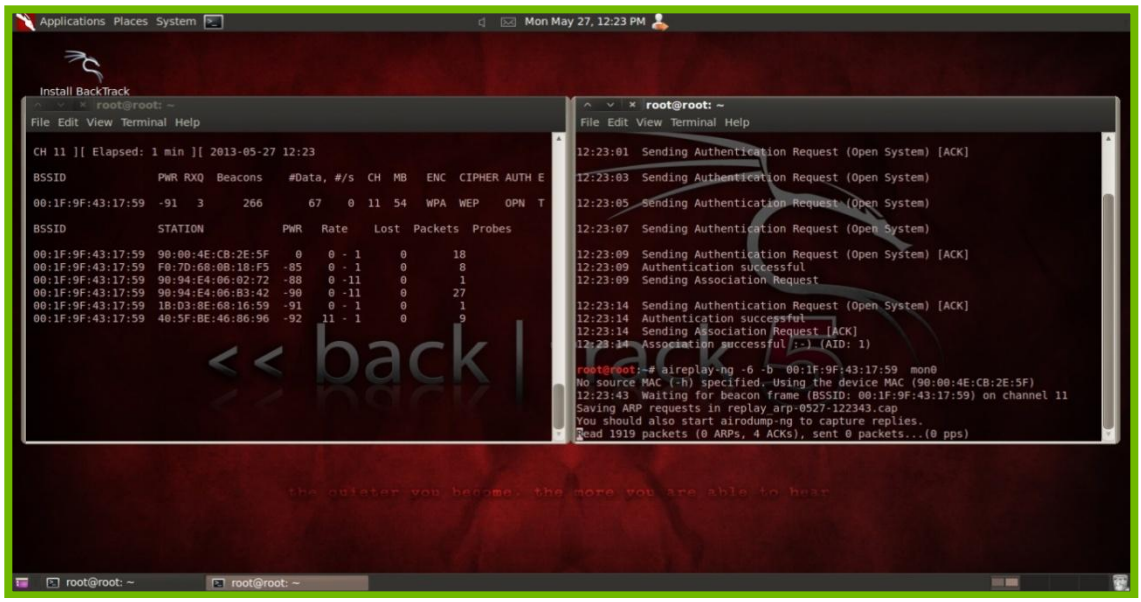


Imagen 14

Paso 12: Cuando llegue a los 30,000 datos abrir una tercera terminal y última terminaly escribir el comando: **aircrack-ng redes-01.cap** (Ver imagen 15)

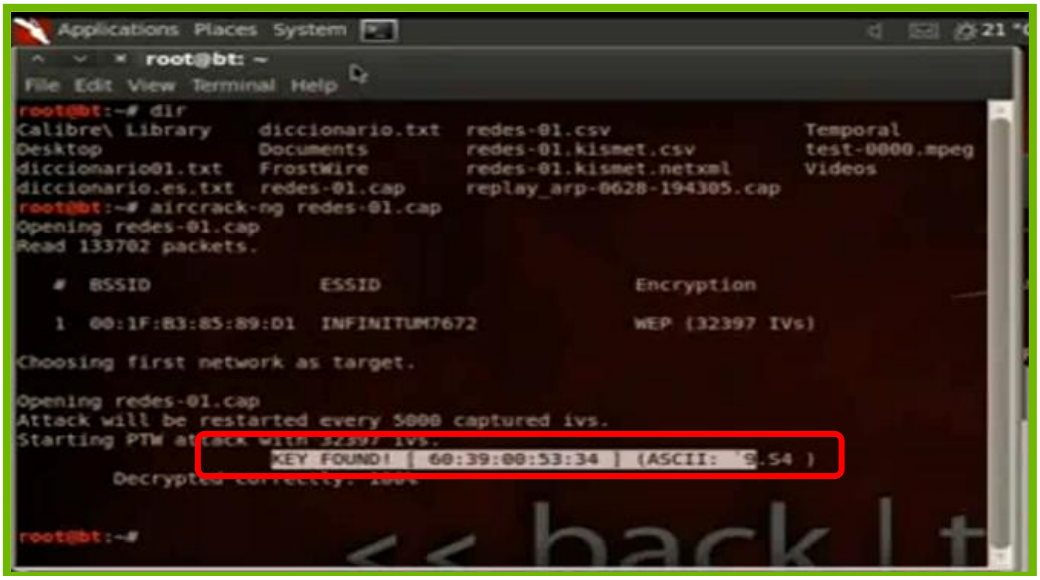


Imagen 15

Redes: archivo donde se guardará la captura (.cap) dar enter y se empezará a descifrar la clave y listo ya se desencripto la clave.

6. BACKDOORS

6.1 CONCEPTO

También conocido como Puerta trasera, programa que permite acceder de forma remota ignorando los procedimientos de autentificación y obtener el control de los mismos permitiendo el ingreso de gusanos o troyanos.

6.2 PROGRAMA

6.2.1 TEAM VIEWER 8

TeamViewer 8 Manual

- ✓ Instalación
- ✓ Control de acceso a PC

INSTALACIÓN

Paso 1: Introducir el cd del kit de herramientas en el reproductor de CD ó DVD e introducir la bandeja. (Ver imagen 1)

Imagen 1

Paso 2: Aparece la siguiente ventana, dar clic en el botón programas. (Ver imagen 2)

Imagen 2

Paso 3: Dar clic en el boton de esteganografia. (ver imagen 3)

Imagen 3

Paso 4: Ubicar el icono del programa Team Viewer 8 y dar clic para iniciar la instalación (Ver imagen 4)

Imagen 4

Paso 5: En esta ventana se muestra las opciones que tiene el Team Viewer de instalación. Si se desea instalarlo en el ordenador dar clic en instalar, si solo se desea ejecutar sin instalación dar clic en iniciar. (Ver imagen 5)

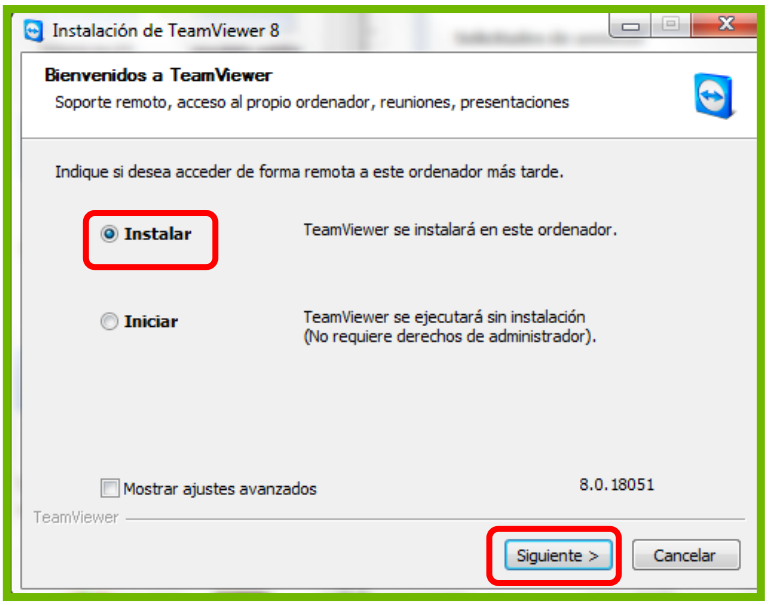


Imagen 5

Paso 6: Especificar de qué manera se va a utilizar el TeamViewer, en este caso lo utilizaremos como comercial t dar clic en Siguiente. (Ver imagen 6)

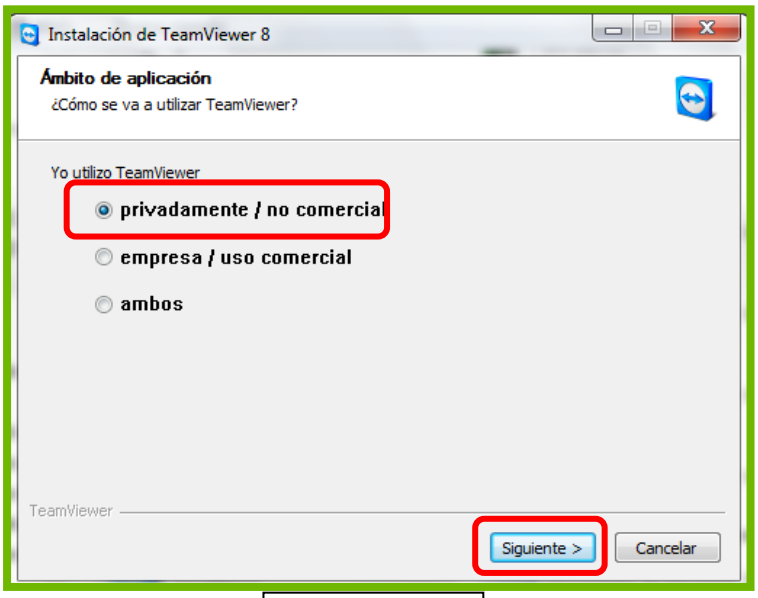


Imagen 6

Paso 7: Por seguridad elegir la opción **no (predeterminado)** para que cada vez que se desee accesar al equipo siempre se reinicie la contraseña para evitar que se accese al equipo sin autorización. Pero si es un equipo de confianza y desea acceder siempre al equipo seleccione la opción **sí.** (Ver imagen 7)

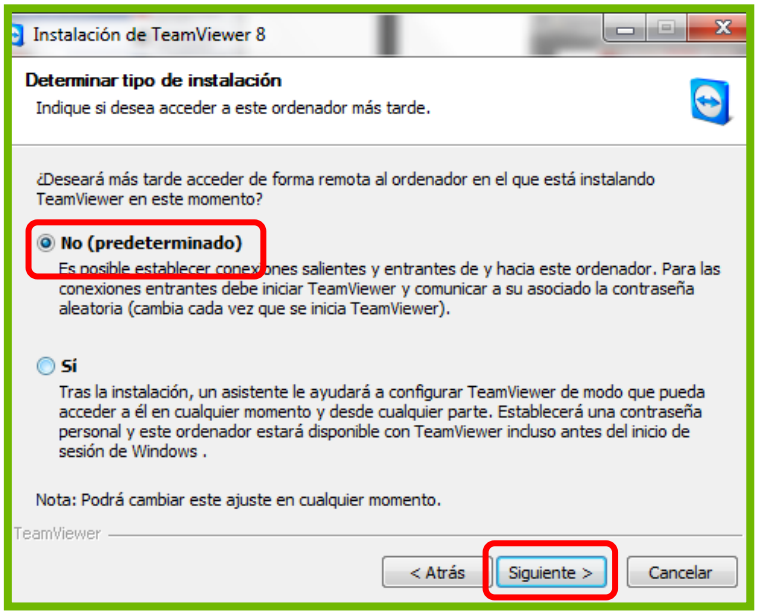


Imagen 7

Paso 8: Aceptar los términos de licencia y la confirmación del uso de TeamViewer, dar clic en siguiente (Ver imagen 8).

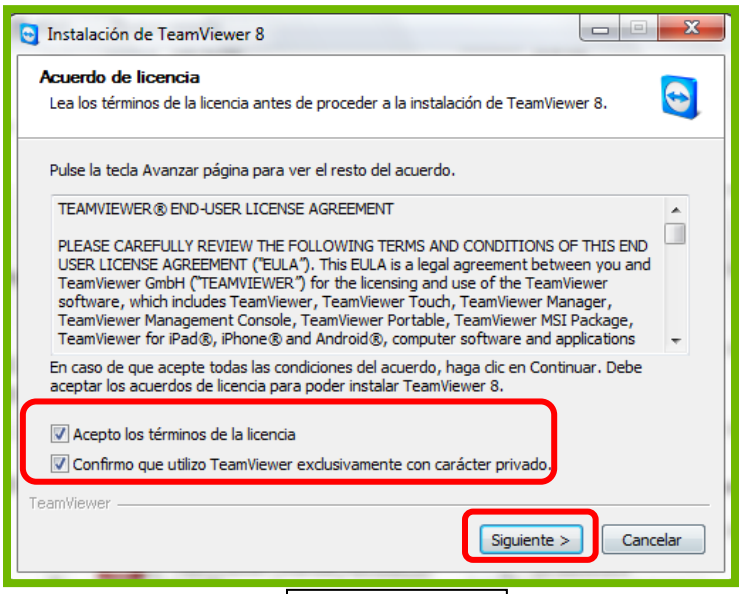


Imagen 8

Paso 9: Esperar unos momentos mientras se instala el programa (Ver imagen 9)

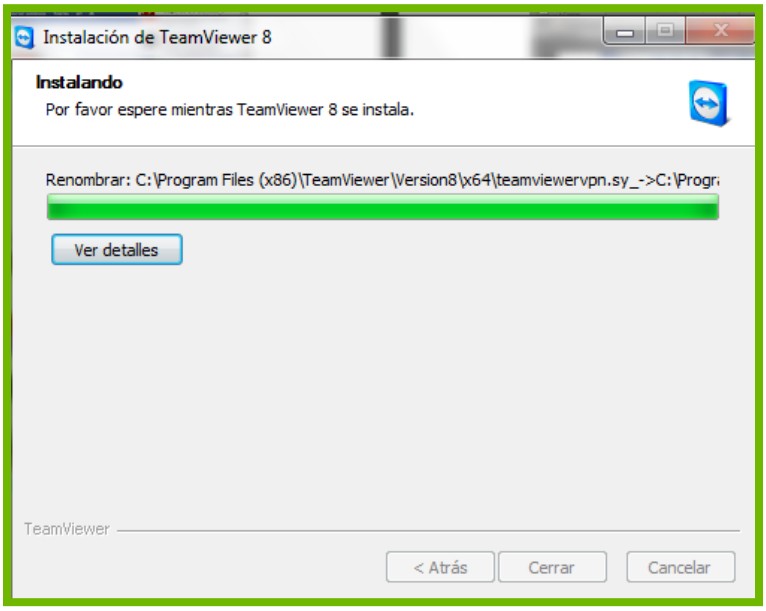


Imagen 9

ESTABLECER UNA CONEXIÓN

Este apartado describe cómo crear mediante sencillos pasos una sesión de control remoto. El proceso de establecer una conexión para una sesión VPN o de transferencia de archivos es el mismo.

Para conectarse con un asociado para una sesión de control remoto, siga estos pasos:

Paso 10: Inicie TeamViewer y dar clic en la pestaña **Control remoto** (Ver imagen 10)

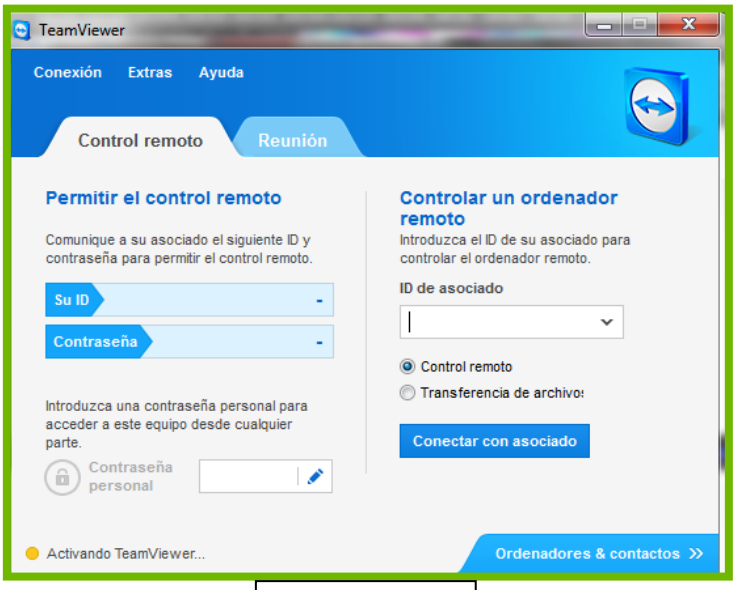


Imagen 10

Paso 11: Solicite a su asociado que inicie la versión completa TeamViewer Solicite a su asociado que le facilite su ID de TeamViewer y su contraseña. A continuación introduzca la ID de su asociado en el cuadro combinado **ID de asociado**. (Ver imagen 11)

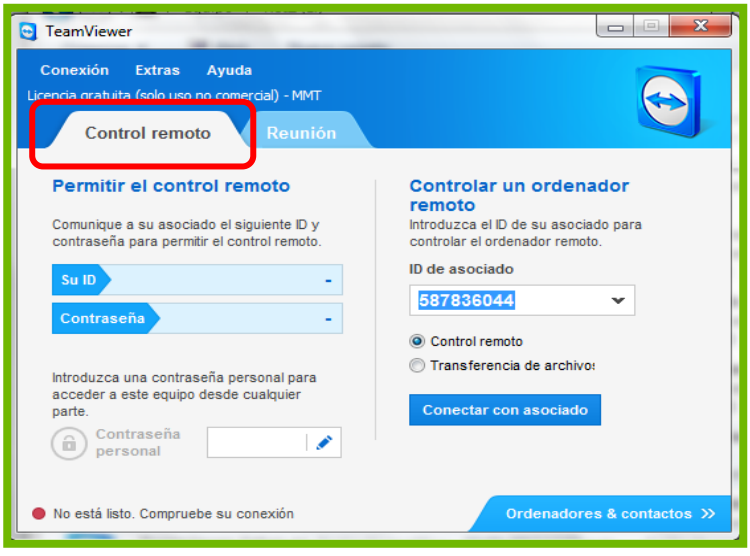


Imagen 11

Paso 12: Haga clic en el botón de opción **Control remoto**.

Paso 13: Haga clic en el botón **Conectar con asociado**. Se abrirá el cuadro de diálogo **Autenticación de TeamViewer**.

Paso 14: Introduzca la contraseña del asociado, Haga clic en **Iniciar sesión** (Ver imagen 12)

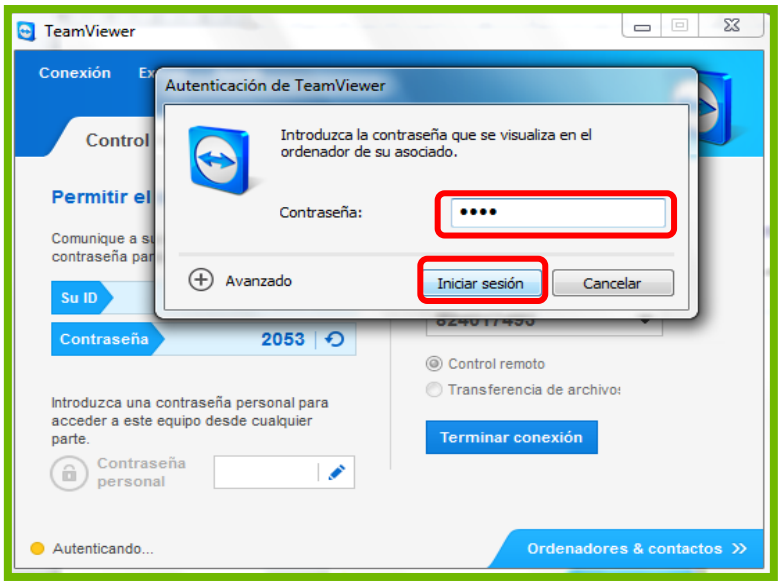


Imagen 12

Ya está conectado al ordenador de su asociado (Ver imagen 13)

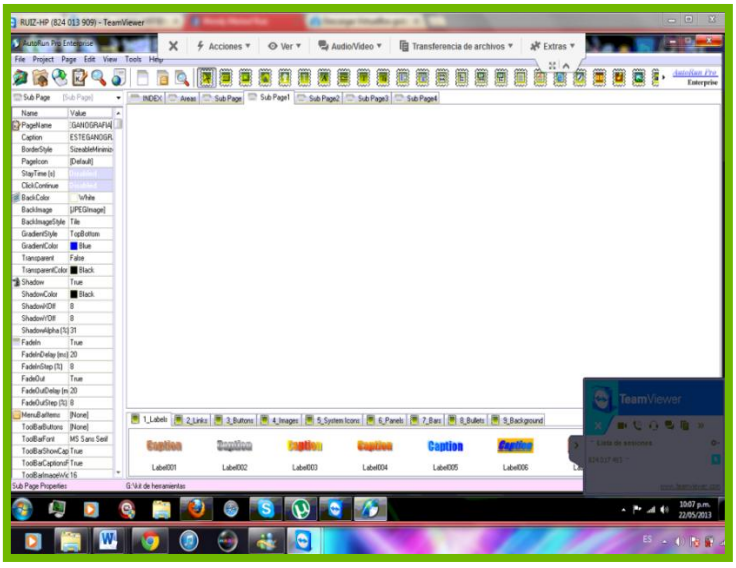


Imagen 13

7. ESCALA DE PRIVILEGIOS

7.1 CONCEPTO

La escalada de privilegios consiste en que un usuario gane acceso, a través de un error de programación, a otro nivel de privilegios en los recursos del sistema, que no le son permitidos para este usuario.

7.2 PROGRAMA

7.2.1 Hiren's boot cd

Escala de privilegios Manual

✓Utilización

En el área de la informática no existe un sistema operativo perfecto, es decir, que consuma pocos recursos, que sea agradable a la vista, funcional, sencillo, versátil, y sobre todo seguro.

La seguridad es una de las mayores preocupaciones de Microsoft y Cía, pero por más que lo intenten, Linux, Unix, Windows, Android, y Mac nunca llegarán a ser perfectos. En el mundo de la informática muchas personas se dedican día a día a probar todo tipo de software, en busca de bugs, y agujeros de seguridad, como el que vamos a examinar hoy.

¿QUE ES LA ESCALADA DE PRIVILEGIOS?

Escalar privilegios es "Ejecutar comandos desde una capa a nivel inferior con el fin de aumentar los privilegios de un usuario o apoderarse de otro"

La escalada de privilegios consiste en que un usuario gane acceso, a través de un error de programación, a otro nivel de privilegios en los recursos del sistema, que no le son permitidos para este usuario. La vulnerabilidad es errores que permiten realizar desde afuera actos sin permiso del administrador del equipo, incluso se puede suplantar al usuario, actualmente, ya hay muchas amenazas que tratan de tener acceso a las computadoras.

Vulnerabilidades comunes asociadas a la escalada de privilegio son buffer o verflow

o shell injection. En UNIX es común, además, explotar vulnerabilidades sobre comandos que tienen activado el bit SUID (Set UserID). El bit SUID permite, en la ejecución de un comando, que el usuario efectivo sea el dueño del archivo. En UNIX es común que ciertos programas que necesitan acceso como usuario administrador tengan este bit encendido.

Con las herramientas que nos ofrece el Hiren´s Boot Cd, se puede quitar contraseñas en los casos que sea necesario iniciar como administrador. Aprovechando la vulnerabilidad de los sistemas operativos.

La vulnerabilidad en sí es bastante simple. Cuando se arranca una computadora, nos encontraremos con la pantalla de selección de usuario de Windows XP.

En cualquiera de las dos, si pulsamos la tecla SHIFT cinco veces aparecerá una ventana en la que podemos configurar las opciones de accesibilidad de Windows XP:

Esto, en realidad, no es sino la ejecución del programa C:\WINDOWS\SYSTEM32\sethc.exe.

Paso 1: Insertar hiren´s boot cd en la lectora de CD/DVD e introducir la bandeja. Y reiniciar la máquina. (Ver imagen 1)

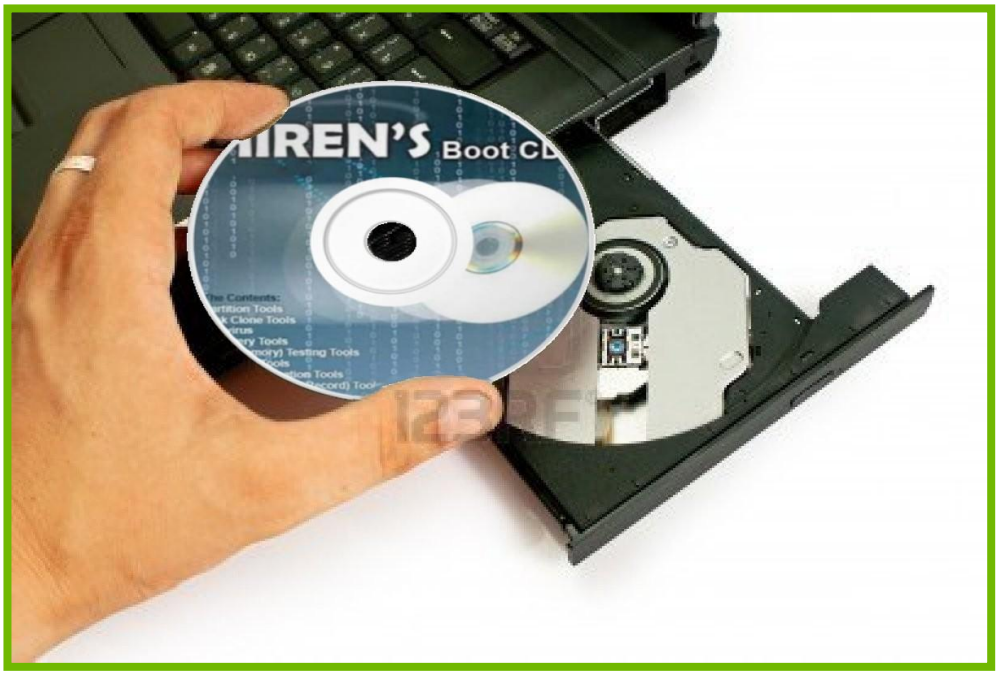


Imagen 1

Paso 2: seleccionar la primera opción mini Windows Xp (Ver imagen 2)

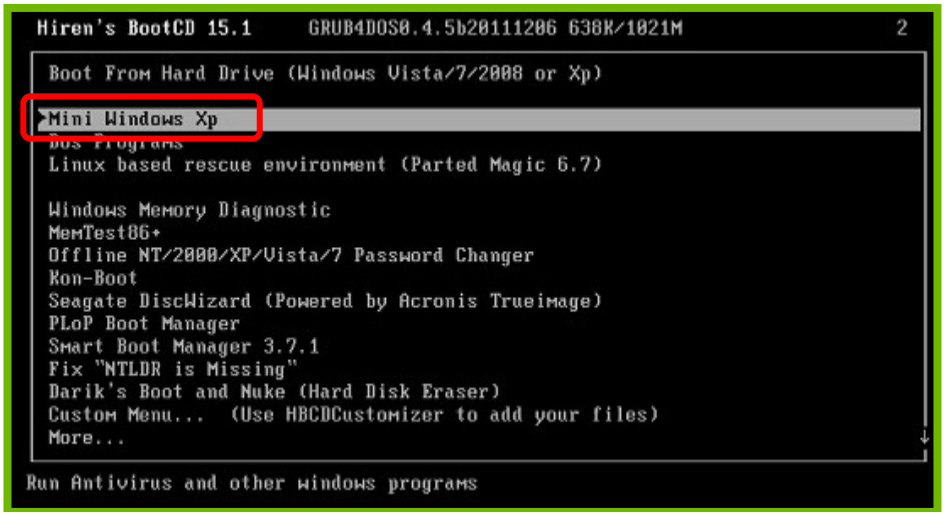


Imagen 2

Paso 3: Esperar que cargue la ventana de Mini Windows Xp (Ver imagen 3)

Imagen 3

Paso 4: Cuando se termina de cargar, se abrirá un escritorio como el siguiente, dar clic en “HBCD Menu” (Ver imagen 4)

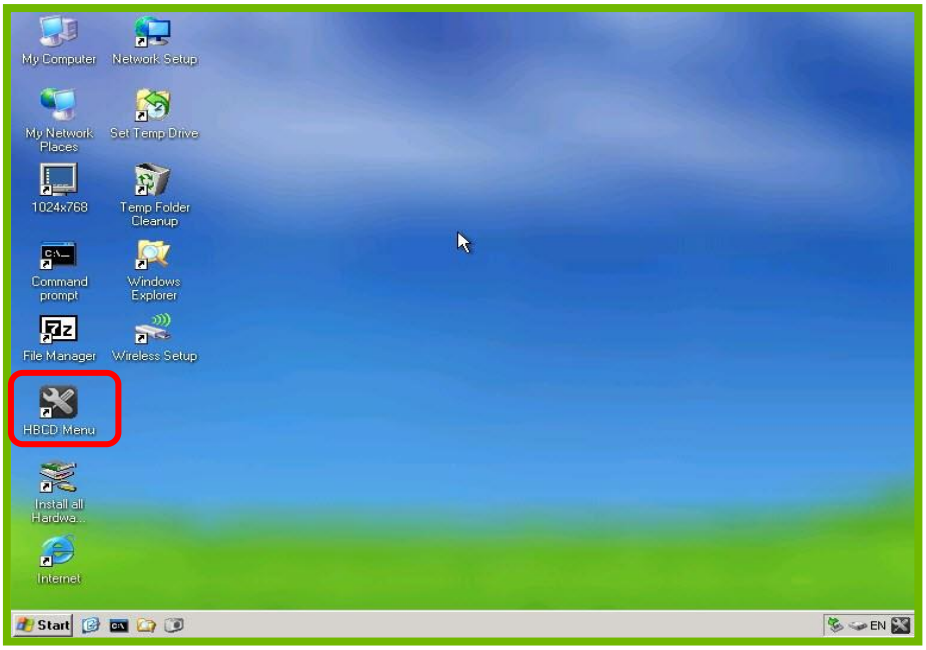


Imagen 4

Paso 5: En esta ventana se tiene el menu principal del programa,y hacer clic en Programs (Ver imagen 5)

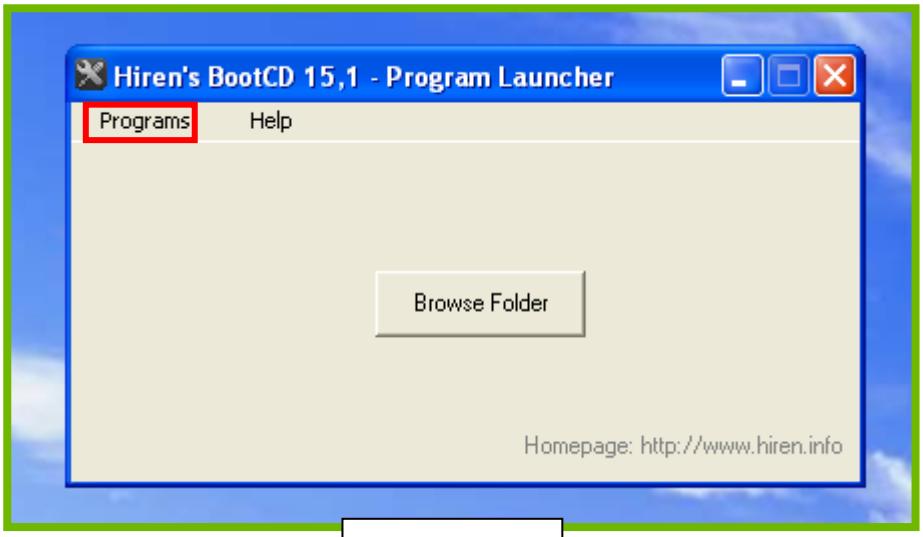


Imagen 5

Paso 6: Una vez ha cargado, se obtiene una pantalla similar a esta, dar clic en:

1. Password Keys
2. Windows Login
3. NTPWEdit(Reset Xp/Vista/7 User Password) (Ver imagen 6)

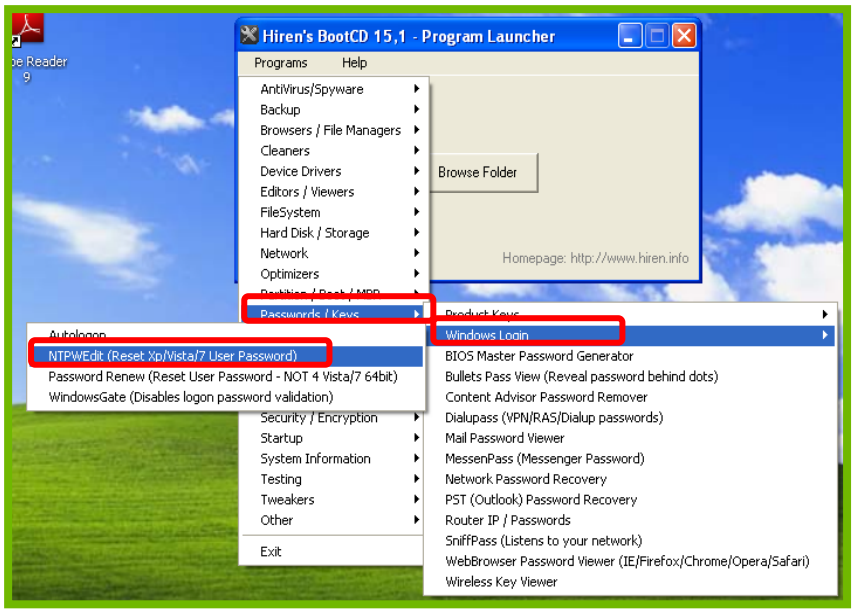


Imagen 6

Paso 7: Elegir (Re) open, para que el programa detecte automáticamente la ruta donde se encuentran las contraseñas de los usuarios. A continuación, seleccionar el usuario al que se quiere cambiarle la contraseña y le dar a "Change password": (Ver imagen 7)

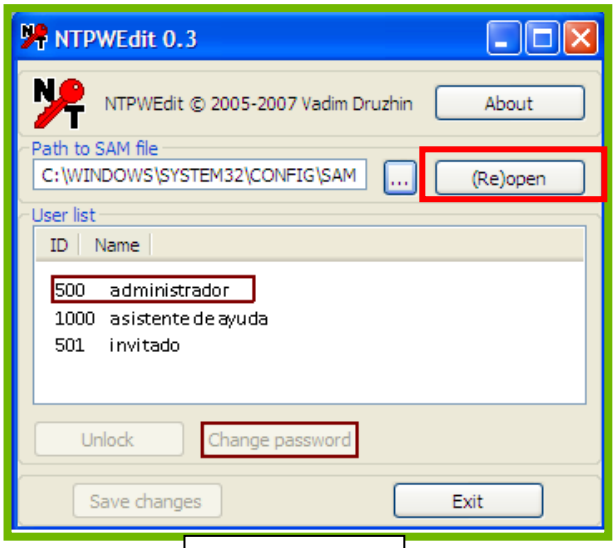


Imagen 7

Paso 8: En la siguiente ventana se escribe la nueva contraseña, en la casilla de abajo se escribe una vez más para su confirmación (Ver imagen 8)

Imagen 8

Ethical Hacking

8. ETHICAL HACKING

Las computadoras alrededor del mundo están siendo víctimas sistemáticamente de ataques de hackers (piratas informáticos), capaces de comprometer un sistema, robar todo lo valioso y borrar completamente la información en pocos minutos.

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

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

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

Para garantizar la seguridad informática se requiere de un conjunto de sistemas, métodos y herramientas destinados a proteger la información, es aquí donde entran los servicios del Ethical Hacking , la cual es una disciplina de la seguridad informática que echa mano de una gran variedad de métodos para realizar sus pruebas, estos métodos incluyen tácticas de ingeniería social, uso de herramientas de hacking , uso de Metasploits

que explotan vulnerabilidades conocidas, en fin son válidas todas las tácticas que conlleven a vulnerar la seguridad y entrar a las áreas críticas de las organizaciones.

¿Quiénes son los Ethical Hackers?

Ethical Hackers son redes de computadoras y expertos que atacan sistemas informáticos en nombre de sus propietarios, con los mismos métodos que sus homólogos, en busca de posibles fallas de seguridad con la finalidad de brindar un informe de todas las vulnerabilidades encontradas que podrían ser aprovechadas por los piratas informáticos.

Para tales fines los ethical hackers han desarrollado lo que se conoce como pruebas de penetración, (PEN-TEST por sus siglas en inglés).

Tests de intrusión

Una prueba de penetración es un paso previo natural a todo análisis de fallas de seguridad o riesgo para una organización. A diferencia de un análisis de vulnerabilidades, una prueba de penetración se enfoca en la comprobación y clasificación de las mismas; y no en el impacto que estas tienen sobre la organización. . Los individuos que realizan estas actividades a veces son denominados "hackers de sombrero blanco", este término proviene de las antiguas películas del Oeste, en donde el "bueno" siempre llevaba un sombrero blanco y el "malo" un sombrero negro.

Tipos de Tests de intrusión

Las empresas que se dedican a realizar pruebas de penetración, luego de analizar las necesidades del cliente, las enfocan en las siguientes perspectivas:

- ✓ Tests de intrusión con objetivo: se busca las vulnerabilidades en componentes específicos de los sistemas informáticos que son de mayor importancia para la empresa.
- ✓ Tests de intrusión sin objetivo: a diferencia de la prueba de penetración con objetivo esta prueba examina la totalidad de los componentes en los sistemas informáticos presentes en la empresa
- ✓ Tests de intrusión ciega: se utiliza únicamente la información pública disponible sobre la empresa. Esta prueba de penetración trata de simular los ataques de un ente externo a la empresa.
- ✓ Tests de intrusión informada: se utiliza información privada, otorgada por la empresa, sobre sus sistemas informáticos. Esta prueba de penetración trata de simular ataques hechos por un ente interno a la empresa y con cierto grado de información privilegiada.
- ✓ Tests de intrusión externa: se realiza de manera externa a las instalaciones de la empresa. La motivación de esta prueba es evaluar los mecanismos perimetrales de seguridad informática de la empresa.
- ✓ Tests de intrusión interna: es realizada dentro de las instalaciones de la empresa con el motivo de probar las políticas y los mecanismos internos de seguridad de la empresa.

El resultado de este servicio le brinda al cliente un documento con una lista detallada de las vulnerabilidades encontradas y certificadas (eliminación de falsos positivos). Adicionalmente el documento provee una lista de recomendaciones a aplicar, sobre la

cual los responsables de seguridad de la organización pueden apoyar su programa de control.

Este servicio está dirigido a empresas con infraestructura de red propia con servicios accesibles desde el exterior, como por ejemplo, Internet (compañías que alojen su propia página web, Proveedores de Servicios de Internet (ISP), empresas que permitan el acceso remoto a sus trabajadores (VPN, RAS), etc.).

Es importante realizar pruebas de penetración .La seguridad de una organización es un aspecto cambiante. Una empresa puede alcanzar un nivel de protección óptimo en un momento determinado y ser totalmente sensible poco después, tras cambios en la configuración de un servidor o tras la instalación de nuevos dispositivos de red. Al mismo tiempo, continuamente aparecen nuevos fallos de seguridad en software existentes, que previamente se creían seguros.

Una política de realización de pruebas de penetración periódicas mitiga, en gran medida, el riesgo asociado a un entorno en constante cambio, tal como lo representan los sistemas informáticos de cualquier compañía.

Descripción del servicio.

Las empresas dedicadas a realizar pruebas de penetración, generalmente, al comenzar realizan un reconocimiento de la visibilidad de los sistemas desde el exterior. Comenzando por recopilar información sobre el cliente (la organización a testear) y sobre los sistemas informáticos de los que este dispone. Para ello se emplean técnicas no intrusivas. Este análisis permite conocer qué tipo de información muestra la organización al exterior y puede ser accesible por cualquiera.

A continuación se detalla que sistemas entrarán dentro del alcance del test y se procede a iniciar el ataque. En este ataque se respetan los siguientes puntos, sujetos a cambios en función de las necesidades del cliente:

1. Se realiza desde una máquina remota, cuya dirección IP pública se pondrá en conocimiento del cliente antes de iniciar la intrusión.
2. Se tienen en cuenta las metodologías OSSTMM, ISSAF y OWASP durante todo el proceso, aunque el equipo auditor podrá hacer chequeos adicionales no contemplados en estas metodologías fruto de experiencias previas.
3. Durante el test no se realizarán pruebas de Denegación de Servicio o Ingeniería Social si no es solicitado expresamente por parte del cliente.

La realización del test está regida por las siguientes fases. Cada una brinda información útil para proteger en el futuro los sistemas del cliente y para continuar analizando la red en fases posteriores:

1. Recopilación de información
2. Enumeración de la red
3. Exploración de los sistemas
4. Extracción de información
5. Acceso no autorizado a información sensible
6. Auditoría de las aplicaciones web
7. Elaboración de informes
8. Comprobación del proceso de parcheado de los sistemas
9. Informe final

El resultado de la intrusión de los sistemas y redes informáticas en todo el mundo ha provocado la pérdida o modificación de los datos sensibles a las organizaciones, representando daños que se traducen en miles o millones de dólares.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.

Una alternativa viable, en aras de alcanzar una seguridad informática apropiada para cualquier red o sistema (aunque para la mayoría de los expertos el concepto de seguridad en la informática es ficticio porque no existe un sistema 100% seguro) lo representa, sin duda alguna, las empresas que se dedican a estos menesteres, teniendo un rol importante en esta tarea los servicios de Ethical Hacking.

Beneficios de un test de intrusión

1. Proporciona un conocimiento del grado de vulnerabilidad de los sistemas de información, imprescindible para aplicar medidas correctivas.
2. Descubre fallas de seguridad tras cambios de configuración.
3. Determina sistemas en peligros debido a su desactualización.

4. Identifica configuraciones erróneas que pudieran desembocar en fallos de seguridad en dispositivos de red (switches, routers, firewalls, etc.).
5. Reduce la probabilidad de materialización de aquellos riesgos que pueden representar grandes pérdidas de capital.
6. Se ahorra tiempo y dinero al afrontar y corregir situaciones negativas antes de que sucedan.

De este modo que un programa para que sea efectivo de testeo de aplicaciones web, debe incluir como elementos a testear: Personas, Procesos y Tecnologías.

Los Ethical Hacking tiene un reglamento que se le presenta a la empresas en la cual tiene conceptos claves a la vez que introduce un marco de trabajo específicamente diseñado para evaluar la seguridad de aplicaciones web para la empresa, compañía o institución.

Paso 1: Antes de comenzado el desarrollo

a) Revisión de Políticas y Estándares
b) Desarrollo de un Criterio de Medidas y Métricas (Aseguramiento de la Trazabilidad)

Paso 2: Durante la definición y el diseño

a) Revisión de los Requerimientos de Seguridad
b) Diseño de Revisión de Arquitectura
c) Creación y Revisión de modelos UML
d) Creación y Revisión de modelos de Amenaza

Paso 3: Durante el desarrollo

a) Code Walkthroughs (Tutoriales de Código)

b) Revisión de Código

Paso 4: Durante el deployment (despliegue)

a) Testeo de Penetración sobre la Aplicación

b) Testeo sobre la Administración y Configuración

Paso 5: Operación y mantenimiento

a) Revisión Operacional

b) Conducción de Chequeos Periódicos

c) Verificación del Control de Cambio.

También en el manual tendrá un apartado para lo que es la escala de privilegios ya que para esta área no existen programas especializados en ello, la escala de privilegios de Windows se trabaja por medio de consola y opciones de Windows.

Otro apartado que tendrá el manual es el área de Ethical hacking ya que es importante que se conozca sobre la ética que se debe tener cuando se utilizan estas herramientas para usarlas de manera responsable y no para dañar a otros.

2.2.1.3 CD interactivo

El cd interactivo se realizó con la ayuda de las herramientas que conforman el kit de informática forense ya que el cd interactivo consta de los videos tutoriales que muestran la utilización de los programas del kit.

También se incorporó el manual para que la Institución pueda contar con este material en digital.

2.3 Marco teórico conceptual

A continuación se presentan una serie de conceptos que pueden tener varios significados pero que se han definido según el uso que se requiere para entender el proyecto.

1. Aplicación: Es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos.

2. Autorun: Es una característica de un sistema operativo que permite ejecutar automáticamente ciertas instrucciones contenidas él en archivo autorun.inf contenida en la unidad insertada (CD, DVD, memoria flash, etc.).

3. Acceso remoto: En redes de computadoras, acceder desde una computadora a un recurso ubicado físicamente en otra computadora, a través de una red local o externa (como internet).

4. Automatizar: Es un conjunto de métodos que sirven para realizar tareas repetitivas en un ordenador.

5. Audio-visual: Es el concepto que aúna lo auditivo y lo visual (imagen y sonido).

6. Boot: Hacer que la computadora inicie la ejecución de instrucciones.

7. Backdoors: En un sistema informático es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema.

8. CD interactivo: Es aquel CD que presenta un contenido multimedia, como sonido, texto, imágenes, movimiento, video entre otros, destinado a ser visto especialmente en las PC.

9. Criptografía: Es una técnica que altera las representaciones lingüísticas de mensajes, mediante técnicas de cifrado y/o codificado, para hacerlos ininteligibles a intrusos que intercepten esos mensajes.

10. Cifrado: Es ocultar mediante un procedimiento criptográfico.

11. Coaxial: Es un tipo de cable que se utiliza para transmitir señales de electricidad de alta frecuencia. Estos cables cuentan con un par de conductores concéntricos: el conductor vivo o central (dedicado a transportar los datos) y el conductor exterior, blindaje o malla (que actúa como retorno de la corriente y referencia de tierra). Entre ambos se sitúa el dieléctrico, una capa aisladora.

12. Cracker: El término se refiere a una persona que usa sus habilidades de hacker con fines ofensivos.

13. CD Autónomo: Una distribución live o Live CD o Live DVD, más genéricamente Live Distro, (traducido en ocasiones como CD vivo o CD autónomo), es un sistema operativo (normalmente acompañado de un conjunto de aplicaciones) almacenado en un medio extraíble, tradicionalmente un CD o un DVD

14. Dispositivos de red: Es equipo de hardware para la interconexión de redes de las computadoras que opera en la capa tres (nivel de red).

15. Debug: Significa depurar (escrutar y eliminar fallos).

16. Desbordamiento de buffer: (del inglés buffer overflow o buffer overrun) es un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto (buffer), de forma que si dicha cantidad es superior a la capacidad pre-asignada los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original. Esto constituye un fallo de programación.

17. Escala de privilegios: Es ejecutar comandos desde una capa a nivel inferior con el fin de aumentar los privilegios de un usuario o apoderarse de otro

18. Ethical Hacking: Técnica utilizada en la evaluación del riesgo informático de una red, sistema o aplicación. Consiste en la simulación de acciones que realizaría un "cracker" para tener acceso no autorizado a un sistema, información o generar la perdida de prestación del servicio.

19. Esteganografía: Es la parte de la Criptología en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.

20. Ethernet: Es un estándar de transmisión de datos para redes de área local que se basa en el siguiente principio: Todos los equipos en una red Ethernet están conectados a la misma línea de comunicación compuesta por cables cilíndricos.

21. Ejecutables: Es un archivo binario cuyo contenido es interpretado por la computadora como un programa. Generalmente, contiene instrucciones en código máquina de un procesador, .Además suele contener llamadas a funciones específicas de un sistema operativo.

22. Freeware: ("software gratis", del inglés free software, aunque esta denominación también se confunde a veces con "libre" por la ambigüedad del término en el idioma inglés) define un tipo de software que se distribuye sin costo, disponible para su uso y por tiempo ilimitado.

23. FAT: File AllocationTable.Tabla de asignación de archivos. Parte del sistema de archivos, que lleva un seguimiento de la ubicación de los datos almacenados en un disco.

24. Fibra Óptica: Son filamentos de vidrio flexibles, del espesor de un cabello. Llevan mensajes en forma de haces de luz que realmente pasan a través de ellos de un extremo a otro, donde quiera que el filamento vaya (incluyendo curvas) sin interrupción.

25. Hackeo de redes: Acción de irrumpir o entrar de manera forzada a un sistema de cómputo o a una red.

26. Hacker: El nombre se refiere a una persona que disfruta aprendiendo los detalles de los sistemas informáticos y estirar sus capacidades.

27. Hacking: El verbo se describe el desarrollo rápido de nuevos programas o la ingeniería inversa de software ya existente para hacer mejor el código y eficiente.

28. Hacker ético: Un hacker ético es un experto en computadoras y redes de datos, su función es atacar los sistemas de seguridad en nombre de sus dueños, con la intención de buscar y encontrar vulnerabilidades que un hacker malicioso podría explotar.

29. Host o anfitrión: Es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Más comúnmente descrito como el lugar donde reside un sitio web. Un host de Internet tiene una dirección de Internet única (direcciónIP) y un nombre de dominio único o nombre de host.

El término host también se utiliza para referirse a una compañía que ofrece servicios de alojamiento para sitios web.

30. Intrusos: Persona que intenta acceder a un sistema informático sin autorización.

31. Interacción: Es la disciplina que estudia el intercambio de información mediante software entre las personas y las computadoras. El objetivo es que el intercambio sea más eficiente: minimizar errores, incrementar la satisfacción, disminuir la frustración y, en definitiva, hacer más productivas las tareas que rodean a las personas y los computadores.

32. Imágenes inyectadas: Permite subir imágenes inyectadas con código a una página web, burlándose los filtros de protección para después poder ejecutar código en el servidor remoto por medio de una inclusión a la imagen.

33. Ingeniería inversa: Es obtener información o un diseño a partir de un producto accesible al público, con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado

34. Interfaz: La superficie de un objeto (real o virtual) que nos habla por medio de sus formas, texturas, colores, etc.

35. Informática forense: La informática forense según la manifestación natural del entorno digital y de la sociedad de la información para responder a la creciente ola de incidentes, fraudes y ofensas en medios informáticos y a través de medios informáticos.

36. IP: Es parte de la capa de Internet del conjunto de protocolos TCP/IP. Es uno de los protocolos de Internet más importantes ya que permite el desarrollo y transporte de datagramas de IP (paquetes de datos).

37. Ininteligibles: Imposible de entender

38. Kit: Conjunto de objetos o productos que sirven para un mismo uso.

39. kB: Un kilobyte (pronunciado /kilobáit/ o en una jerga más popular /ká/) es una unidad de almacenamiento de información cuyo símbolo es el kB y equivale a 103 bytes.

40. Logs: Es un registro de la actividad de un programa, servidor, cliente, etc. Para el caso particular de las páginas web, es el registro de todas las acciones del servidor web y donde quedan registradas las visitas a las páginas.

41. Manual de usuario: Este tipo de manual brinda las instrucciones necesarias para que un usuario pueda utilizar un determinado producto o servicio.

42. Macros: Es una instrucción compleja, formada por otras instrucciones más sencillas.

43. Metasploits: Es un proyecto open Source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración y en el desarrollo de firmas para Sistemas de Detección de Intrusos.

44. NIC: Una tarjeta de red o adaptador de red es un periférico que permite la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más computadoras.

45. Pendrive: Es un dispositivo portátil de almacenamiento, compuesto por una memoria flash, accesible a través de un puerto USB.

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

47. Partición: Es el nombre que reciben las divisiones de una unidad física de almacenamiento de datos**.**

48. Plausible: Que merece encomio o aprobación; Que merece crédito por su verosimilitud o sensatez.

49. Ping: Herramienta que permite averiguar si existe un camino (comunicación) de TCP/IP entre dos computadoras de cualquier parte de Internet.

50. Pixel: Son los puntos que forman las imágenes digitales.

51. Quemar un archivo: Es grabar los archivos en el CD o el DVD.

52. Root: Es el nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos sobre una computadora.

53. Router: El término de origen inglés router puede ser traducido al español como enrutador o ruteador**,** aunque en ocasiones también se lo menciona como direccionador**.** Se trata de un producto de hardware que permite interconectar computadoras que funcionan en el marco de una red**.**

54. Sniffer de red: Es un software que permite capturar tramas de la red. Generalmente utilizado con fines maliciosos para capturar textos de emails, chats, datos personales, contraseñas.

55. TCP/IP: Es un conjunto de protocolos. La sigla TCP/IP significa "Protocolo de control de transmisión/Protocolo de Internet". Proviene de dos protocolos importantes, del protocolo TCP y del protocolo IP.

56. TCP: En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP).

57. Tráfico: En un sitio web el tráfico se refiere a la cantidad de datos enviados y recibidos por los usuarios del sitio web.

58. Traceroute: Programa de ejercicio y diagnostico que extiende a Ping para incluir los tiempos de ida y vuelta no sólo hasta el anfitrión de destino sino también hasta todos los en caminadores (routers) intermedios.

59. Texto plano: Son aquellos que están compuestos únicamente por texto sin formato, sólo caracteres. Estos caracteres se pueden codificar de distintos modos dependiendo de la lengua usada

60. Texto cifrado: Es aquel texto que ha sido Criptografíado con algún algoritmo determinado y clave de cifrado

61. UTP: Es un cable que no tiene revestimiento o blindaje entre la cubierta exterior y los cables. El UTP se utiliza comúnmente para aplicaciones de REDES Ethernet, el

término UTP generalmente se refiere a los cables categoría 3, 4 y 5 especificados por el estándar TIA/EIA 568-A estándar.

62. Virus: Son una combinación de gusanos, caballos de troya, jokeprograms, retros y bombas lógicas. suelen ser muy destructivos. pequeño segmento de código ejecutable escrito en ensamblador o lenguaje de macro, capaz de tomar el control de la maquina o aplicación en algún momento y auto replicarse, alojándose en un soporte diferente al que se encontraba originalmente.

63. WEP: Significa "Wired Equivalent Privacy" (Privacidad Equivalente a Cableado) Es un protocolo de seguridad para Wi-Fi de redes. Dado que las redes inalámbricas transmiten datos a través de ondas de radio, es fácil de interceptar los datos o "espiar" transmisiones de datos inalámbricos.

64. WPA: (en español «Acceso Wi-Fi protegido») es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, Wired Equivalent Privacy (WEP).

2.4 Documentación técnica

2.4.1 Recuva

Recuva es un programa gratuito para Windows que permite restaurar archivos que han sido borrados accidentalmente. Por ejemplo, se pueden restaurar archivos que han sido eliminados de la papelera de reciclaje así como imágenes y otros archivos que también han sido borrados por error. Es posible recuperar fotografías borradas de tarjetas de memoria de cámaras digitales o de reproductores MP3: incluso es posible recuperar

archivos y canciones que han sido eliminados del disco duro de dispositivos como iPod o iPhone.

Recuva es una aplicación que ha sido desarrollada por el mismo equipo de CClean, lo cual significa que es un programa ligero, fácil de usar y sobre todo gratuito, que funciona muy bien y no consume muchos recursos del sistema éstas son algunas características de Recuva:

- Filtros fáciles de usar que permiten seleccionar archivos, ya sea por nombre o por tipo.
- Interfaz usuario simple y fácil de utilizar parecida al explorador de Windows, con una organización jerárquica basada en una estructura de tipo árbol.
- Recuva se puede ejecutar desde una unidad de memoria USB.
- La aplicación puede restaurar una gran cantidad de archivos diferentes: documentos de Office, imágenes, video, música, correos, etc.
- Tiene soporte nativo para los siguientes sistemas de archivos: FAT12, FAT16, FAT32, ex FAT, NTFS, NTFS5, NTFS y EFS.
- Se pueden restaurar archivos desde unidades de almacenamiento removibles como tarjetas de memoria utilizadas en teléfonos celulares y cámaras digitales.
- Es posible recuperar archivos borrados desde discos flexibles (JAZ, diskettes, etc.,), así como dispositivos de almacenamiento más grandes como discos duros o unidades ZIP.

- Recuva es un programa completamente gratuito que no requiere de registro alguno y se puede utilizar en cualquier computadora que tenga el sistema operativo Windows.

El archivo de instalación tiene un tamaño aproximado de 2.3 MB y puede ser descargado desde varios servidores. Una vez que se ha descargado el archivo, sólo hay que hacer doble clic sobre él para que el asistente de instalación comience el proceso. Después de algunos segundos la aplicación quedará instalada completamente lista.

Recuva es compatible con muchas versiones de Windows: desde Windows 95 hasta Windows 7. Sin duda se trata de una excelente opción para recuperar archivos borrados y que se creían perdidos para siempre.

Conclusión: Recuva nos sirve para recuperar archivos perdidos, además de ser un programa fiable, gratis y eficiente.

2.4.3 Wise Data Recovery

Wise Data Recovery es una luz, rápida y gratuita herramienta de recuperación de archivos eliminados - fácilmente puede recuperar los datos perdidos de disco duro y unidad extraíble.

Recuperación de datos de dominio público, recuperación de datos perdidos, no importa que sean imágenes, documentos, audios, vídeos, archivos comprimidos o correos electrónicos. Se puede buscar en forma rápida y segura y recuperar el archivo que desee, siempre y cuando se especifique la unidad, el tipo de archivo o el nombre

del archivo. Wise Data Recovery también le mostrará el nivel de dificultad de la recuperación mediante la indicación de los datos como "Bueno", "Malo", "Insuficiente" o "Lost" en el resultado del escaneo.

Características:

- Totalmente gratis
- Recuperar documentos como word, excel, txt, etc
- Recuperar foto / imagen, como: Jpg, Gif, Gif, etc
- Recuperar archivos de correo electrónico, por ejemplo. Eml
- Recuperar otros datos como audio, video, archivo
- Recuperación de datos del disco extraíble, como ipod, reproductor de mp3, etc
- Mostrar estado explícito de los datos que deben recuperarse

2.4.4 Ontrack Easy Recovery

Con la Ontrack EasyRecovery podemos restaurar archivos eliminados de nuestro sistema siempre y cuando Windows no haya sobrescrito igualmente el espacio que ocupaban anteriormente. Esta herramienta nos permite:

- Restaura los archivos eliminados.
- Encuentra datos eliminados con sólo unos clics.
- Funciona también con memorias USB y tarjetas de memoria.
- Algunas de las características es que se pueden recuperar fácilmente los archivos eliminados de forma accidental.

- Por ello, no importa si los archivos perdidos estaban guardados en el disco duro, en la memoria USB o en otro soporte, como una tarjeta de memoria de una cámara.
- Permite seleccionar el disco duro o la partición que queremos recuperar archivos y también realiza un completo análisis para recuperar los archivos eliminados.

2.4.5 AxCrypt

Es una herramienta extremadamente fácil y súper apropiada para dar los primeros pasos en la encriptación de archivos. Mediante un algoritmo AES de 128 bits, permite proteger los archivos de forma eficaz, sin necesidad de mayores esfuerzos.

Características y funciones de AxCrypt

El principal aspecto a destacar de esta aplicación, es que se trata de un programa totalmente gratuito, de muy poco peso y con una interfaz extremadamente sencilla y de uso ágil.

Contrariamente a lo que cualquier usuario puede pensar de una aplicación que pesa poco menos de 1Mb, AxCrypt posee muchas funciones de seguridad, como por ejemplo la creación de un archivo llave, que puede alojarse en una memoria USB y sin el cual no puedes abrir los archivos, o bien la eliminación de todos los archivos temporales que puedan contener alguna clave de acceso a los archivos codificados.

Posee además soporte para archivos de hasta 4Gb en Windows 2000 y XP.

Algunas características importantes que categorizan esta herramienta como una de las 3 mejores aplicaciones de codificación, es que además de ser una aplicación extremadamente liviana y sencilla, tiene todas las medidas de seguridad necesarias para que nadie pueda conocer las contraseñas. Un ejemplo de esto es que no guarda archivos de acceso en la memoria RAM ni en otras partes del ordenador y el código es completamente abierto.

La conclusión es que si se desea descargar AxCrypt**y** probar así su funcionamiento el requisito es que el SO sea: Win 2000/XP/2003/Vista/7.

2.4.5 TrueCrypt

TrueCrypt este programa es gratuito de cifrado de archivos mediante los algoritmos de cifradoAES-256, Serpent y Twofish, que ofrece la posibilidad de encriptar archivos, encriptar un disco duro entero o encriptar USB. Truecryptes un programa multiplataforma que está disponible para Windows 2000, Windows XP, Windows Vista y Windows 7, además de Linux y Mac OS X.

Las principales características de TrueCrypt son las siguientes:

- Crea un disco virtual encriptado con un fichero y lo monta como un disco real
- Encriptación de particiones completas o dispositivos de almacenamiento como discos USB o discos duros
- Encriptación de la partición o disco donde está instalado Windows

- La encriptación es automática, en tiempo real y transparente al usuario Paralelización y pipelining.
- Los datos se pueden leer y escribir tan rápido como si el disco no estuviera encriptado
- La encriptación se puede acelerar por hardware en los procesadores modernos
- Se provee la opción de denegación plausible, en caso de que alguien nos forzase a revelar la contraseña

2.4.6 ParanoicEncryption

Es un sencillo y pequeño encriptador/desencriptador de textos que usa un algoritmo de encriptación llamado PESv2.

Sólo está destinado a textos, siendo su uso tremendamente sencillo, ofreciendo los resultados de manera instantánea. Simplemente se debe introducir una contraseña, tanto para la encriptación como la desencriptación, e introducir el texto quese quiere cifrar o descifrar. Así de sencillo.

Práctico, rápido y diminuto.

2.4.7 Camouflage

Es una utilidad que permite ocultar ficheros a ojos demasiado fisgones desordenando dicho fichero y eliminando el tag que adjudica a cada tipo de fichero el programa que lo ejecuta.

Los ficheros camuflados tienen funciones como de cualquier otro fichero normal, lo puede enviar por correo electrónico sin levantar ningún tipo de sospecha.

Para mayor seguridad puedes proteger mediante contraseña tus ficheros camuflados. Contraseña que será necesaria cuando se quiera realizar la extracción del fichero.

2.4.8 Spimage 2

Codifica diversos tipos de archivo en un fichero de imagen, ocultando los primeros y condicionando el acceso a la posesión de una contraseña.

El programa puede ocultar ejecutables (EXE), imágenes (JPEG, GIF y PNG), archivos de sonido (WMA y MP3) y vídeos (AVI, MPG, SVID, DIVX y SWF) en ficheros JPEG, BMP, PNG y GIF. De esta manera, se pueden enviar archivos a través de Internet sabiendo que sólo el receptor que comparte la contraseña podrá descodificar los archivos y leerlos.

La imagen resultante no difiere de cualquier otra por lo que sólo aquel que sepa que se trata de una spimage tratará de descodificarla. Así que en realidad la protección es doble: ocultación y codificación.

2.4.9 FileInyector

FileInyector oculta cualquier archivo que se desea dentro de una imagen (en formatos BMP, JPG, GIF). Aunque a ojos de cualquiera seguirá siendo simplemente eso, una imagen.

La sencillez envuelve FileInyector, con una interfaz simple pero francamente desfasada y poco usable. Eso sí, se agradece su poco tamaño (140kB) y que no requiera instalación.

Echamos de menos más formatos compatibles de imagen "inyectable". Tampoco permite convertir la imagen inyectada en un archivo ejecutable, con lo que es necesario el propio FileInyector para recuperar el archivo oculto dentro de la imagen.

Pros

Portable y ocupa apenas 140kB

Eficaz para ocultar archivos

Contras

Necesitas Fileinyector para recuperar el archivo insertado

No admite PNG, TIF y otros tantos formatos de imagen

Usabilidad mejorable y diseño obsoleto

2.4.10 Free IP Tools

Una excelente forma de mantener todas las herramientas de red importantes en un solo lugar.

Free IP Tools incluye 12 herramientas esenciales para resolver problemas de red y para hacer un debug de aplicaciones y servicios relacionados con la red. Estas

herramientas están claramente empaquetadas dentro de un solo programa con una interfaz de usuario gráfica y una configuración ajustable.

Detalle de las herramientas incluidas:

- Ping: esta utilidad presenta los resultados de ping y traceroute en un conveniente formulario.
- PortScan: escaneador de puertos que permite buscar puertos abiertos en tu red. Incluye dos modos de búsqueda: Convencional y Furtivo.
- HostAlive: es una herramienta para monitorear la disponibilidad de un host remoto y servicios de red ofrecidos por el host (servidor HTTP o FTP).
- EmailVerify: chequea si determinada dirección de e-mail es válida preguntando al servidor correspondiente.
- NSLookup: resuelve nombre de host a direcciones IP.
- IPBlackList: es una utilidad que comprueba si una dirección IP o host está en la lista negra de las bases de datos de spam, proxies abiertos y otros servicios populares. Esta herramienta permite comprender por qué ciertos servicios son denegados a un host.
- NBScan: escanea tu red en busca de compartidos en Windows disponibles, esto incluye archivos, carpetas, impresoras y otros dispositivos.
- RawSocket: puede crear sockets de bajo nivel TCP y UDP para probar y ajustar diferentes servicios de red.

- Shares: monitoriza recursos compartidos en el PC y monitoriza quién conecta a tus archivos y dispositivos compartidos.
- SNMPAudit: es un avanzado escáner SNMP que puede fácil y rápidamente localizar dispositivos SNMP.
- SysFiles: ofrece un modo fácil para editar los cinco archivos de sistema más importantes para la red: Servicios, Protocolos, Networks, Host y LMHosts

Free IP Tools ofrece sin dudas un interesante camino para mantener un control casi completo de todo lo que sucede en nuestra red.

SistemaOperativo:

WinXP, Windows2000, Windows2003, Windows Vista Starter, Windows Vista Home Basic, Windows Vista Home Premium, Windows Vista Business, Windows Vista Enterprise, Windows Vista Ultimate, Windows Vista Home Basic x64, Windows Vista Home Premium x64, Windows Vista Business x64, Windows Vista Enterprise x64, Windows Vista Ultimate x64

Requerimientos mínimos del sistema:

Pentium III orhigher, 128 RAM, 5 Mb HDD

2.4.11 TeamViewer

Es una aplicación de control remoto que pone el acento en la facilidad de uso. Cada PC que esté ejecutando TeamViewer, además de actuar como servidor, puede conectarse a otro y obtener una vista interactiva del Escritorio de otro PC.

TeamViewer 8 añade más opciones para el trabajo en equipo. La más destacada es sin duda la consola de gestión (TeamViewer Management Console), que permite administrar todo el equipo de soporte remoto a través del navegador.

Otras mejoras de TeamViewer 8 enfocadas al trabajo en grupo son la transferencia de sesión de control remoto, que permite pasar una sesión a otro miembro de un equipo de soporte, y el uso compartido de grupos, útil para mover clientes o amigos entre una cuenta y otra.

Por último, TeamViewer mejora todavía más la grabación de audio y vídeo de las sesiones remotas, y en conexiones lo bastante rápidas permite ver y oír lo mismo que ve y oye el usuario, ya sean sonidos de sistema o presentaciones con vídeos.

Cómo conectar a un PC remoto

Para conectar a un PC con TeamViewer solo tienes que introducir el número de sesión del ordenador al que quieres conectar -una especie de número de 'teléfono' de TeamViewer- y la contraseña que te proporcionará la otra persona. Incluso puedes grabar un vídeo de la sesión.

Las opciones de TeamViewer permiten definir una contraseña permanente (útil para el acceso a un terminal propio) y varios parámetros para una seguridad adicional.

La conexión, gracias al cifrado AES de 256 bits, es segura en la mayoría de situaciones. En cuanto a la calidad de la imagen de TeamViewer, ésta depende -sobre todo- de la velocidad de conexión entre los equipos.TeamViewer no requiere componentes adicionales y se ejecuta rápidamente incluso en equipos modestos.

Pros

- Increíblemente fácil de usar
- Chat de voz y vídeo simultáneo
- Conexión con cifrado de 256 bits
- Instalación rápida y sencilla
- Hasta 25 participantes virtuales
- Soporte para varios monitores

2.4.12BackTrack

Con BackTrack todo lo que se escriba desde el ordenador donde el programa ha sido instalado quedará capturado en los ficheros de log del equipo y se podrá recuperar más tarde perfectamente organizado.

BackTrack ofrece la posibilidad de saber, incluso, la aplicación y la ventana activa en la que se está escribiendo. Es muy útil para todas aquellas personas que deben controlar qué se hace desde sus ordenadores cuando ellos no están presentes.

Cada día se crea un nuevo fichero log, por lo que se conocerá exactamente qué se hizo, en qué día se hizo y qué se escribió, de manera que no habrá ninguna parte de la información que se pierda con este programa. Además, todos los logs se guardan por lo que pueden ser consultados cuando nosotros queramos sin miedo a perder la información.

BackTrack es la herramienta perfecta si se quiere controlar qué se hace en los ordenadores de la empresa, en el tuyo propio, etc.

2.4.2 Hiren's boot cd

Es un CD autónomo. Este contiene una secuencia de arranque, así puede ser útil incluso cuando el sistema operativo primario no pueda ser iniciado. Porque el sector cero o MBR no es escrito correctamente o carece de alguno. El Hiren'sBootCD tiene una lista extensa del software. Las utilidades con funcionalidad similar en el CD se agrupan juntas y parecen redundantes, sin embargo existen diferencias entre ellas o se complementan. El 18 de Marzo 2008 lanzaron la versión actual que es la 9.5, que contiene varias utilidades tales como:

- Pruebas del funcionamiento del sistema.
- Reproductores multimedia.

- Gestor del Master Boot Record.(MBR)
- Herramientas del BIOS.
- Cambio o eliminación de contraseñas en el equipo.
- Programas de recuperación de datos.

Y muchos otros que resuelven los problemas de la computadora como errores con particiones algunas veces cuando estamos instalando un sistema operativo podemos encontrar diversos errores, como es que la tabla de partición no funcione correctamente, o el espacio del disco duro no coincida y eso nos lleve a encontrar diversos errores.

CAPITULO III
DESARROLLO DE LA SOLUCIÓN

3.1 Propuesta de la solución

La informática forense es un tema no muy conocido por las personas hoy en día volviéndose un problema ya que abren paso para que se cometan delitos informáticos. Además en las instituciones educativas no se imparte la informática forense como una rama importante de la informática para que los estudiantes conozcan aplicaciones de la informática forense para investigar y protegerse de los delitos informáticos como por ejemplo: recuperación de información, robo de contraseñas, visitas a páginas de internet no autorizadas, Hackeo de redes, fraudes y muchos delitos que se pueden cometer por medio de los dispositivos electrónicos. Tal es el caso del Instituto Nacional San Luis donde se imparte la materia de informática, en la cual no se abarca la informática forense como contenido importante dentro de la materia, de manera que los estudiantes desconocen esta área de la informática, contribuyendo a la deficiencia que hay en el país sobre la informática forense.

Es por esto que surge este proyecto llamado: **Desarrollo de un kit de herramientas básicas de software sobre informática forense como material didáctico de apoyo en el área de informática en el Instituto Nacional San Luis.**

Debido a la necesidad de apoyar el material didáctico de la materia de informática del Instituto Nacional San Luis, por medio de la elaboración de un kit de informática

forense que permite la investigación de delitos tecnológicos relacionados con la seguridad informática.

Para que los estudiantes conozcan sobre estas aplicaciones, por medio de este proyecto, los alumnos obtendrán una respuesta favorable a problemas de: Privacidad, Hackeo de redes, Fraude, Pérdida de datos, Robo de información. Surgidos a través del uso indebido de las tecnologías de la informática ya que es necesario estar capacitado para la investigación de este tipo de delitos informáticos, con la ayuda de aplicaciones que nos brinda la informática forense.

Para desarrollar este proyecto se investigó primeramente el concepto de informática forense para obtener mayor conocimiento sobre el tema, además la informática forense está conformada por una serie de áreas las cuales son: Recuperadores de información, Esteganografía, Criptografía, Backdoors, Escala de privilegios, Ethical hacking, Sniffer de red y Hackeo de redes.

Para estas áreas de la informática forense se recopiló una serie de programas que conciernen a las áreas mencionadas anteriormente.

- Para el área de los recuperadores de información se recopilaron los siguientes software:

1. Recuva
2. Wise data recovery
3. Easy Recovery

- Para el área de Criptografía se recopilaron los siguientes software:
    1. Axcrypt
    2. TrueCrypt
    3. Paranoic Encryption

- Para el área de Esteganografía se recopilaron los siguientes software:
    1. Camouflage
    2. Spimage 2.0
    3. FileInyector
- Para el área de Backdoors se investigó el siguiente software:
    1. TeamViewer 8
- Para el área de Sniffer de red se investigó el siguiente software:
    1. Free IP Tools
- Para el área de Hackeo de redes se investigó el siguiente software:
    1. Backtrack
- Para el área de Escala de privilegios se investigó el siguiente software:
    1. Hiren's Boot CD

Para este proyecto se realizarón 3 productos los cuales conforman este proyecto el primer producto se denomina kit de herramientas básicas de software sobre informática forense, con la investigación realizada y los programas seleccionados se creará este kit que está conformado como se dijo anteriormente por 13 aplicaciones

perteneciente a cada una de las áreas de la informática forense el cual se diseñará con la ayuda de otra aplicación llamada AutoRun Pro Enterprise la cual es una herramienta que ayuda a diseñar de una manera amigable la interfaz del kit de herramientas para comodidad de los usuarios.

El producto antes mencionado se implementará en el Instituto Nacional San Luis, por medio de una demostración a nivel básico que se impartirá a una pequeña muestra de alumnos y los maestros encargados del área de informática de la Institución para que posteriormente pueda ser impartido por los maestros a todos los alumnos del Instituto Nacional San Luis, este kit se utilizará como un material de apoyo para la materia de informática que servirá para conocer algunas técnicas que ayudan a investigar y proteger los equipos simplemente porque muchos no conocen de la existencia de herramientas de software que ayudan a investigar y a esclarecer las faltas o intrusiones en los equipos informáticos por ejemplo, robo de información, ocultar información para que no pueda ser visible para terceros, recuperación de datos, visitar páginas prohibidas por la institución y el Hackeo de las redes.

El kit de herramientas básicas de software sobre informática forense se entregará en un CD el que se quemarán los programas seleccionados para el desarrollo de este proyecto.

El segundo producto es un manual de procedimientos en el cual se especificará el uso adecuado de cada aplicación, en él se describe detalladamente los pasos a seguir para la instalación, configuración y el uso de los programas del kit de herramientas.

Este producto se utilizará al momento en el que esté siendo utilizado el kit de herramientas básicas de software sobre informática forense ya que cuando sea utilizado por los beneficiarios del proyecto surgirán preguntas en cuanto al funcionamiento de cada programa para poder instalarlo, configurarlo y conocer otras funciones de los programas.

Además es necesario que los alumnos que van a utilizar este kit también cuenten con un manual para estudiar un poco acerca de los programas ya que una mala configuración podría dañar o hacer que el programa no funcione correctamente.

El manual de procedimientos se ha diseñado en el programa Microsoft Word 2010 ya que este programa permite estructurar el manual de una manera sencilla y comprensible para las personas que hagan uso del manual.

La estructura del manual se ha hecho procedimental ya que según la investigación realizada para escoger un manual de acuerdo a las necesidades requeridas para la utilización de los programas se eligió un manual de procedimientos ya que en él se describe paso a paso los procedimientos a seguir para la instalación, configuración y utilización de los programas.

Este manual además de realizarse impreso se hará también en formato digital el cual se incorporará en el CD interactivo para el uso de los alumnos o docentes que enseñen a utilizar los programas sobre las áreas de la informática forense y a utilizarlos de forma adecuada.

El manual ya terminado se entregará en formato digital e impreso para que los usuarios puedan tener varias alternativas para consultar este manual según como lo prefiera el usuario.

El tercer producto es el CD interactivo el cual es de mucha importancia ya que este es el complemento del manual de procedimientos y el kit de herramientas ya que muchas veces no se comprende al 100% leyendo un manual por lo que se ha tomado a bien crear un CD en el cual se incorporarán video-tutoriales en el cual se explicará de manera real el uso, configuración e instalación de los programas del kit de herramientas.

Para realizar este producto se investigó primeramente que es un CD interactivo para conocer cómo funciona dicho CD.

Se ha investigado la manera más sencilla y eficaz de realizar este CD y se escogió hacerlo en el AutoRun Pro Enterprise ya que esta herramienta se ha utilizado para realizar el portafolio digital y el kit de herramientas y se ha verificado que es una herramienta práctica para diseñar de una manera diferente y amigable el contenido de los CD.

Este CD interactivo tiene un fondo para su página principal y una serie de iconos de los video-tutoriales de cada programa que conforma el kit de herramientas básicas de software. Al darle clic a estos iconos se ejecutan los video-tutoriales para que sean vistos por los usuarios.

También en el CD interactivo se encuentra un icono que contiene el manual de procedimientos que se hizo en Microsoft Office Word 2010 para que se pueda tener de manera impresa y digital.

Para la creación de este CD fue necesario contar con algunos elementos los cuales son:

1. Plantillas para el fondo del CD interactivo
2. Botones
3. Video-tutoriales
4. Tipos y tamaños de letras
5. El manual

Todos estos elementos son importantes ya que con ellos se construirá el CD interactivo.

Luego de haber recolectado dicha información se procede a darle estilo al CD interactivo agregándole la plantilla para el fondo que se vea mejor, luego el tipo y tamaño de letra también se eligierón los botones que llevará el CD.

Cada uno de los botones se ha vinculado a los video-tutoriales para que al darle clic al botón correspondiente para cada video según el programa este pueda visualizarse. Y se le ha agregado un botón para ver el manual, como se dijo anteriormente que se incorporará a este CD.

Estos son los tres productos que conforman el proyecto a desarrollar en el Instituto Nacional San Luis para lo cual fue necesario visualizar primeramente la necesidad que hay de apoyar la materia de informática de esta institución ya que cada día la tecnología va en aumento y es necesario estudiar técnicas que ayuden a investigar y a proteger de intrusiones informáticas. Esto impulso a la creación de este proyecto para darle una solución a esta necesidad en el Instituto Nacional San Luis.

De manera que con este estudio se pretende la utilización de la informática, como un medio por el cual se den a conocer aplicaciones relacionados a la informática forense.

3.2 Conclusiones

1. Los productos elaborados para el desarrollo de este proyecto será de gran utilidad para el Instituto Nacional San Luis, ya que con ello se pretende despertar el interés de los estudiantes en el área de la Informática Forense.
2. El desarrollo de este proyecto beneficiará a los estudiantes del Instituto Nacional San Luis, ya que obtendrán una mejor preparación en el área de la Informática en comparación a otras Instituciones Educativas.
3. El proyecto presentado al Instituto Nacional San Luis posee un costo económico muy mínimo, aunque los programas sean gratuitos es necesario que se contrate o se capacite al personal que impartirá este estudio de la informática forense para seguir investigando y utilizando este proyecto.
4. Este trabajo pretende contribuir con la difusión y uso de la Informática Forense en nuestro país y su aplicación como recurso de enseñanza para el Instituto Nacional San Luis.
5. Con el estudio de este trabajo se comprobó que el área de la informática forense es muy extensa y por esta razón es necesario seguir adquiriendo conocimientos en dicha área.
6. En la actualidad la tecnología tiene un gran auge, así mismo los delitos informáticos, por lo que la Informática Forense es una disciplina que debe renovarse constantemente para estar a la vanguardia ante un nuevo delito Informático.

7. En este país casi no existen Instituciones Educativas que promuevan el estudio de la informática Forense.
8. En consecuencia la ignorancia sobre los delitos informáticos se debe al poco conocimiento de la legislatura sobre las leyes que penalizan esta clase de delitos.

3.3 Recomendaciones

1. Se recomienda al Instituto Nacional San Luis hacer uso de este kit de herramientas básicas sobre Informática Forense. por medio de charlas, seminarios, clases extras o incluirlo en el material didáctico de la materia de informática y de esta manera promover el interés de los estudiantes en el área de la Informática Forense.
2. Contratar a una persona capacitada en el área de Informática Forense para que imparta sus conocimientos con los estudiantes y de esta manera incrementar sus conocimientos, habilidades, destrezas y aptitudes académicas.
3. Se recomienda a la institución hacer buen uso del kit de herramientas de software, el manual y el cd- interactivo, ya que estos productos que forman el proyecto se ven limitados a los alcances de proyecto haciendo ver las áreas principales de la Informática forense.
4. Es recomendable agregar más información referente a las áreas de la Informática Forense que se refieren a las redes en el proyecto.

5. Estudiar más a fondo la Informática Forense ya que 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.
6. Al emplear la Informática Forense se deben de tener en cuenta algunos aspectos éticos para no infringir la ley.
7. Propagar información sobre las leyes que penalizan los delitos informáticos para que se puedan disminuir y castigar los delitos informáticos.

3.4 Carta de finalización del proyecto

INSTITUTO NACIONAL SAN LUIS
CIENCIA, CULTURA Y SUPERACIÓN

Soyapango, 31 de Mayo de 2013

Sres.

Universidad Tecnológica de El Salvador

Presente.-

Reciba un cordial saludo de parte de la Comunidad Educativa del Instituto Nacional San Luis de Soyapango, deseando muchos éxitos en su importante labor.

Mediante la presente les comunicamos que damos por finalizado el proyecto presentado el día 08 de Marzo del presente año denominado **"Desarrollo de un kit de herramientas básicas de software sobre informática forense como material didáctico de apoyo en el área de informática del Instituto Nacional San Luis"** Este proyecto fue desarrollado por tres alumnas de su institución cuyos nombres son:

1. Sandra Cristina Roberto Alférez
2. Keila Birzavit Ruiz Nuila
3. Wendy Marisol Ruiz Romero

Agradeciendo de antemano la atención a la presente, me suscribo.

Atentamente

Pedro Hernández Martínez
Coordinador Académico

Bibliografía

Alegsa. (1998-2012). Alegsa.com.ar. Recuperado de http://www.alegsa.com.ar/Dic/aes.php

Andres, Nicolas. (2013). *TiposDe.org*. Recuperado de http://www.tiposde.org/cotidianos/568-tipos-de-manuales/

Cano, Jeimy. (2009). *Computacion Forense.* México: Alfaomega.

Kioskea. *Kioskea*. Recuperado de

http://es.kioskea.net/contents/crypto/des.php3

Pino, D. S. *Manual de Manejo de Evidencias Digitales y Entornos* . Recuperado de http://www.oas.org/juridico/english/cyb_pan_manual.pdf

República, F. G. *Escuela.fgr.gob.sv*. Recuperado de http://escuela.fgr.gob.sv/?page_id=624

Reyes, Alfonso. (2010). *Hacking Etico*. Recuperado de http://www.portantier.com/biblioteca/seguridad/hacking-etico.pdf

Salvador, U. D. Recuperado de http://ri.ues.edu.sv/3190/1/Estudio%20y%20an%C3%A1lisis%20sobre%20la%20inform%C3%A1tica%20forense%20en%20El%20Salvador.pdf

Sánchez, N. G. (2012, Marzo 27). *Seguridad en redes*. [Registro web]. Recuperado de http://seguridad-en-redes-mimi.blogspot.com/2012/03/algoritmo-3des.html

Technologies, R. *Encriptacion crytoforge*. Recuperado de http://www.cryptoforge.com.ar/seguridad.html

Tori, Carlos. (2008). *HACKING ETICO*. Buenos Aires, Argentina: Mastroianni impresiones.

Universidad Politecnica de Pachuca. *Criptografia Simétrica y Asimétrica*. Recuperado de http://maytics.web44.net/web_documents/criptograf_a_sim_trica_y_asim_trica.pdf

Universidad Politecnica de Pachuca. *Criptografia Simétrica y Asimétrica*. Recuperado de http://maytics.web44.net/web_documents/criptograf_a_sim_trica_y_asim_trica.pdf

Anexos

A1 matriz de congruencia

MATRIZ DE CONGRUENCIA		
TEMA: Desarrollo de un kit de herramientas básicas de software sobre informática forense, como material didáctico de apoyo en el área de Informática en el Instituto San Luis.		
OBJETIVO GENERAL: Desarrollar un kit de herramientas básicas de software sobre Informática Forense para los alumnos del Instituto Nacional San Luis, con el fin de proporcionar un material didáctico de apoyo para la materia de informática.		
OBJETIVO ESPECIFICO 1: Identificar las herramientas que se utilizarán para el desarrollo del contenido del material de apoyo en el área de informática.	**OBJETIVO ESPECIFICO 2:** Crear un manual para el uso adecuado de las herramientas de software de informática forense.	**OBJETIVO ESPECIFICO 3:** Desarrollar un CD interactivo que contenga ayudas audio-visual para facilitar el uso de las herramientas básicas de la informática forense.
ALCANCE 1: Proporcionar a la institución un kit de herramientas básicas de informática forense.	**ALCANCE 2**: Elaborar un documento que ayude a utilizar de manera adecuada las herramientas de software.	**ALCANCE 3:** Se utilizará un medio audio-visual que ayude a facilitar el uso de las herramientas que poseerá el kit.

PRODUCTO 1: Kit de herramientas básicas de informática forense enfocado en las áreas de: Esteganografía, Criptografía, Etical hacking, Backdoors, Escala de privilegios, Recuperadores de datos, Sniffer de red y Hackeo de redes.	**PRODUCTO 2:** Manual impreso para el uso adecuado de las herramientas de informática forense.	**PRODUCTO3:** CD interactivo que contendrá, tutoriales y el manual en formato digital para comprender mejor el uso de los programas.

DOCUMENTACION TECNICA:

1. RECUVA:

Recuva es un programa gratuito para Windows que permite restaurar archivos que han sido borrados accidentalmente. Por ejemplo, se pueden restaurar archivos que han sido eliminados de la papelera de reciclaje así como imágenes y otros archivos que también han sido borrados por error.

- Interfaz usuario simple y fácil de utilizar parecida al explorador de Windows, con una organización jerárquica basada en una estructura de tipo árbol.
- Recuva se puede ejecutar desde una unidad de memoria USB.
- La aplicación puede restaurar una gran cantidad de archivos diferentes: documentos de Office, imágenes, video, música, correos, etc.
- Tiene soporte nativo para los siguientes sistemas de archivos: FAT12, FAT16, FAT32, ex FAT, NTFS, NTFS5, NTFS y EFS.
- Se pueden restaurar archivos desde unidades de almacenamiento removibles

como tarjetas de memoria utilizadas en teléfonos celulares y cámaras digitales.

- Es posible recuperar archivos borrados desde discos flexibles (JAZ, diskettes, etc.,), así como dispositivos de almacenamiento más grandes como discos duros o unidades ZIP.
- Recuva es un programa completamente gratuito que no requiere de registro alguno y se puede utilizar en cualquier computadora que tenga el sistema operativo Windows.

2. WISE DATA RECOVERY:

Wise Data Recovery es una luz, rápida y gratuita herramienta de recuperación de archivos eliminados - fácilmente puede recuperar los datos perdidos de disco duro y unidad extraíble.

Características:

- Totalmente gratis
- Recuperar documentos como Word, Excel, TXT, etc.
- Recuperar foto / imagen, como: JPG, GIF, etc.
- Recuperar archivos de correo electrónico, por ejemplo. Eml
- Recuperar otros datos como audio, video, archivo
- Recuperación de datos del disco extraíble, como iPod, reproductor de mp3, etc.
- Mostrar estado explícito de los datos que deben recuperarse.

3. EASY RECOVERY

Con la Ontrack EasyRecovery podemos restaurar archivos eliminados de nuestro

sistema siempre y cuando Windows no haya sobrescrito igualmente el espacio que ocupaban anteriormente. Esta herramienta nos permite:

- Restaura los archivos eliminados.
- Encuentra datos eliminados con sólo unos clics.
- Funciona también con memorias USB y tarjetas de memoria.
- Algunas de las características es que se pueden recuperar fácilmente los archivos eliminados de forma accidental.
- Por ello, no importa si los archivos perdidos estaban guardados en el disco duro, en la memoria USB o en otro soporte, como una tarjeta de memoria de una cámara.
- Permite seleccionar el disco duro o la partición que queremos recuperar archivos y también realiza un completo análisis para recuperar los archivos eliminados.

4. AXCRYPT

Es una herramienta extremadamente fácil y súper apropiada para dar los primeros pasos en la encriptación de archivos. Mediante un algoritmo AES de 128 bits, permite proteger los archivos de forma eficaz, sin necesidad de mayores esfuerzos.

5. TRUECRYPT

Este programa es gratuito de cifrado de archivos mediante los algoritmos de cifrado AES-256, Serpent y Twofish, que ofrece la posibilidad de encriptar archivos, encriptar un disco duro entero o encriptar USB. Truecrypt es un programa multiplataforma que está disponible para Windows 2000, Windows XP, Windows Vista y Windows 7, además de Linux y Mac OS X.

6. PARANOIC ENCRYPTION

Es un sencillo y pequeño encriptador/desencriptador de textos que usa un algoritmo de encriptación llamado PESv2.

Sólo está destinado a textos, siendo su uso tremendamente sencillo, ofreciendo los resultados de manera instantánea. Simplemente se debe introducir una contraseña, tanto para la encriptación como la desencriptación, e introducir el texto que se quiere cifrar o descifrar. Así de sencillo.

Práctico, rápido y diminuto.

7. CAMOUFLAGE

Es una utilidad que permite ocultar ficheros a ojos demasiado fisgones desordenando dicho fichero y eliminando el tag que adjudica a cada tipo de fichero el programa que lo ejecuta.

Los ficheros camuflados tienen funciones como de cualquier otro fichero normal, lo puede enviar por correo electrónico sin levantar ningún tipo de sospecha. Para mayor seguridad puedes proteger mediante contraseña tus ficheros camuflados. Contraseña que será necesaria cuando se quiera realizar la extracción del fichero.

8. SPIMAGE 2

Codifica diversos tipos de archivo en un fichero de imagen, ocultando los primeros y condicionando el acceso a la posesión de una contraseña.

El programa puede ocultar ejecutables (EXE), imágenes (JPEG, GIF y PNG), archivos de sonido (WMA y MP3) y vídeos (AVI, MPG, SVID, DIVX y SWF) en ficheros JPEG, BMP, PNG y GIF. De esta manera, se pueden enviar archivos a través de Internet sabiendo que sólo el receptor que comparte la contraseña podrá

descodificar los archivos y leerlos.

La imagen resultante no difiere de cualquier otra por lo que sólo aquel que sepa que se trata de una spimage tratará de descodificarla. Así que en realidad la protección es doble: ocultación y codificación.

9. FILEINYECTOR

FileInyector oculta cualquier archivo que se desea dentro de una imagen (en formatos BMP, JPG, GIF). Aunque a ojos de cualquiera seguirá siendo simplemente eso, una imagen.

La sencillez envuelve FileInyector, con una interfaz simple pero francamente desfasada y poco usable. Eso sí, se agradece su poco tamaño (140kB) y que no requiera instalación.

Echamos de menos más formatos compatibles de imagen "inyectable". Tampoco permite convertir la imagen inyectada en un archivo ejecutable, con lo que es necesario el propio FileInyector para recuperar el archivo oculto dentro de la imagen.

10. FREE IP TOOLS

Una excelente forma de mantener todas las herramientas de red importantes en un solo lugar.

Free IP Tools incluye 12 herramientas esenciales para resolver problemas de red y para hacer un debug de aplicaciones y servicios relacionados con la red. Estas herramientas están claramente empaquetadas dentro de un solo programa con una interfaz de usuario gráfica y una configuración ajustable.

11.TEAMVIEWER

Es una aplicación de control remoto que pone el acento en la facilidad de uso. Cada PC que esté ejecutando TeamViewer, además de actuar como servidor, puede conectarse a otro y obtener una vista interactiva del Escritorio de otro PC.

TeamViewer 8 añade más opciones para el trabajo en equipo. La más destacada es sin duda la consola de gestión (TeamViewer Management Console), que permite administrar todo el equipo de soporte remoto a través del navegador.

Pros

- Increíblemente fácil de usar
- Chat de voz y vídeo simultáneo
- Conexión con cifrado de 256 bit.
- Instalación rápida y sencilla
- Hasta 25 participantes virtuales
- Soporte para varios monitores

12. BACKTRACK

Con BackTrack todo lo que se escriba desde el ordenador donde el programa ha sido instalado quedará capturado en los ficheros de log del equipo y se podrá recuperar más tarde perfectamente organizado.

BackTrack ofrece la posibilidad de saber, incluso, la aplicación y la ventana activa en la que se está escribiendo. Es muy útil para todas aquellas personas que deben controlar qué se hace desde sus ordenadores cuando ellos no están presentes.

Cada día se crea un nuevo fichero log, por lo que se conocerá exactamente qué se

hizo, en qué día se hizo y qué se escribió, de manera que no habrá ninguna parte de la información que se pierda con este programa. Además, todos los logs se guardan por lo que pueden ser consultados cuando nosotros queramos sin miedo a perder la información.

A3 Leyes

LEY ANTITERRORISMO

DELITO INFORMATICO

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

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

CODIGO PENAL PROCESAL

DE LOS DELITOS RELATIVOS A LA INTIMIDAD

VIOLACIÓN DE COMUNICACIONES PRIVADAS

Art. 184.- El que con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido o se apodere de datos reservados de carácter

personal o familiar de otro, registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivo o registro público o privado, será sancionado con multa de cincuenta a cien días multa.

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

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

VIOLACIÓN AGRAVADA DE COMUNICACIONES

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

CAPTACIÓN DE COMUNICACIONES

Art. 186.- El que con el fin de vulnerar la intimidad de otro, interceptare, impidiere o interrumpiere una comunicación telegráfica o telefónica o utilizare instrumentos o artificios técnicos de escucha, transmisión o grabación del sonido, la imagen o de cualquier otra señal de comunicación, será sancionado con prisión de seis meses a un año y multa de cincuenta a cien días multa.

Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de prisión de seis meses a un año y multa de cien a ciento cincuenta días multa.

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

El que realizare los actos señalados en el primer inciso del presente artículo para preparar la comisión de un delito grave será sancionado con la pena de dos a seis años. (9)

REVELACIÓN DE SECRETO PROFESIONAL

Art. 187.- El que revelare un secreto del que se ha impuesto en razón de su profesión u oficio, será sancionado con prisión de seis meses a dos años e inhabilitación especial de profesión u oficio de uno a dos años.

A3 están en proceso las leyes de delitos cibernéticos

Analizan propuesta de ley contra delitos cibernéticos

El Ministro de Seguridad, David Munguía Payés, reveló a Transparencia Activa que se ha presentado una propuesta de ley contra el delito cibernético para su análisis y posterior envío a la Asamblea Legislativa. La normativa permitiría castigar

penalmente a quienes desde el anonimato, acosen, calumnien y cometan otro tipo de crímenes cibernéticos.

Escrito por: **Henry Flores** el 14/05/2013.

Categorias: **Seguridad**

Tags: **Delitos**, **El Salvador**, **Informática**, **Transparencia**

El ministro reveló la iniciativa a Transparencia Activa. (Foto: MJSP)

El ministro de Seguridad, David Munguía Payés, reveló a Transparencia Activa que presentaron a Casa Presidencial una propuesta de ley contra el delito cibernético para su análisis y posterior envío a la Asamblea Legislativa.

"Hay mucha gente que se aprovecha del anonimato. Esos delitos provocativos decantan en violaciones, agresiones o acosos; también desprestigian a personas con calumnias, desde el anonimato hacen fraudes a bancos, instituciones financieras, etc.", explicó el funcionario.

La ley contra delitos cibernéticos o informáticos daría herramientas legales para procesar a quienes sin escrúpulos usan internet y las redes sociales para dañar a terceros. De momento, dichos delitos en la mayoría de los casos quedan impunes por la falta de una legislación especial.

En México implementan campañas para la denuncia de los delitos informáticos.

En El Salvador, se reportan casos de mujeres que denuncian acoso a través de redes sociales como Facebook. Fátima Ortiz, directora ejecutiva del Consejo contra la Trata

de Personas, revela que “muchos crean cuentas exprés para buscar víctimas para prostitución infantil, por ejemplo”.

Consultados sobre el tema, la ciudadanía cibernauta y que usa herramientas informáticas ve positivo una ley que castigue fuertemente ese tipo de delitos.

“Es de mucha importancia que el país cuente con una ley para castigar delitos informáticos, ya que estos son muy comunes, porque estos ciber-delincuentes están enterados que no hay nada y nadie los castigue ni les prohíba sus acciones”, opina Erika Candray.

Países de Latinoamérica como México, Brasil, Venezuela, Colombia y más recientemente Costa Rica cuentan con una ley contra delitos cibernéticos que castiga hasta con seis años de prisión a quienes calumnien, difamen a través de correos electrónicos o usen sistemas informáticos para fraudes, robos de contraseñas o distribución de virus.