

Universidad Tecnológica de El Salvador

FACULTAD DE INFORMÁTICA Y CIENCIAS APLICADAS

TÉCNICO EN INGENIERÍA EN HARDWARE



TEMA: Elaboración de un kit de informática forense para material de apoyo en actividades de diplomados realizados en la Universidad Tecnológica de El Salvador.

TRABAJO DE GRADUACIÓN PRESENTADO POR:

David Emanuel Aguilar Vásquez

Marcos Rafael Constancia Perla.

Carlos Sigfredo López Hernández

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERÍA DE HARDWARE.

ABRIL, 2016

SAN SALVADOR, EL SALVADOR, CENTROAMERICA

PAGINA DE AUTORIDADES

ING. NELSON ZÁRATE SANCHEZ

RECTOR

LIC. JOSE MODESTO VENTURA

VICERRECTOR ACADEMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

ING. ERNESTO ALONSO EMESTICA AVALOS

PRESIDENTE

ING. MARIO ALBERTO VALLE

PRIMER VOCAL

LIC. MARVIN ELENILSON MONTOYA HERNANDEZ

SEGUNDO VOCAL

ABRIL, 2016

SAN SALVADOR, EL SALVADOR, CENTROAMERICA



ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:

Ing. Mario Alberto Valle Aguirre, Lic. Marvin Elenilson Hernández Montoya,
Ing. Ernesto Alonso Eméstica Avalos, a las 12:30m. Del día Miércoles 2 de
diciembre de dos mil quince.

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

- | | |
|---|----------------------------|
| 1- <u>Marcos Rafael Constanza Perla</u> | <u>Carnet 28-4878-2012</u> |
| 2- <u>David Emanuel Aguilar Vásquez</u> | <u>Carnet 28-4961-2010</u> |
| 3- <u>Carlos Sigfredo López Hernández</u> | <u>Carnet 28-3100-2013</u> |

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:

"Elaboración de un kit de Informática Forense para Material de apoyo en
actividades de diplomados realizadas en la Universidad Tecnológica de El
Salvador"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE HARDWARE

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

APROBADO

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

San Salvador, 2 de diciembre de dos mil quince.

F. 
PRIMER VOCAL
Ing. Mario Alberto Valle Aguirre

F. 
SEGUNDO VOCAL
Lic. Marvin Elenilson Hernández Montoya

F. 
PRESIDENTE
Ing. Ernesto Alonso Eméstica Avalos

Agradecimiento

Le agradezco primeramente a Dios por haberme acompañado y guiado a lo largo de mi carrera, y por ser mi fortaleza en los momentos de debilidad.

Le doy gracias a mis padres Sonia de Aguilar y Julio Aguilar por apoyarme en todo momento, por los valores que me han inculcado y por haberme dado la oportunidad de tener una excelente educación en el transcurso de mi vida.

Le agradezco el apoyo, dedicación y confianza a nuestro asesor Lic. Marvin Hernández por aceptarnos como grupo de trabajo a Carlos, Rafael y mi persona, por su apoyo moral en los momentos difíciles, así como también a nuestros jurados Ing. Ernesto Emestica e Ing. Mario Valle, por su apoyo brindado durante la defensa.

A mis amigas, Valeria Rivas, Michelle Romero, Nahomy Quintanilla, Karla Galdámez, Lily Cristales, Xiomara Zepeda, Clarissa Callejas, Karla Reyes, Claudia y Adaly Colon, Ana María Cortez, Jacqueline Portillo y Claudia Mendoza, por su apoyo moral y ayuda brindada.

Y en especial a Myrka Escalante, una persona muy significativa en mi vida, que gracias a su apoyo constante permitió que no me rindiera en los momentos de desesperación y poder seguir sacando adelante este trabajo y poder finalizarlo con éxito, por haberme apoyado en las buenas y en las malas y sobre todo por su paciencia y su cariño incondicional.

A mis amigos, Mario Narváez, Jonathan Deras, Edward Sifontes, por confiar y creer en mí, y por su apoyo moral durante el trayecto de este proyecto.

David Emanuel Aguilar Vásquez

Agradecimiento

Doy gracias a Dios por un año más y por dejarme cumplir mi sueño de ser un técnico en Ingeniería de Hardware, en la Universidad Tecnológica de El Salvador, y gracias a mi familia por el apoyo brindado desde el inicio de mis estudios y especialmente a mi tía. Rosa Deisy perla de Sorto y también a Hilda Isabel Perla de Blanco. Y Edith Feliziana Blanco de Perla.

Y especialmente a mi papa Marco Antonio Constancia Perla y a mi madre María Dolores Perla de Constancia Perla y a mi hermana María Inés Constancia Perla y a toda mi familia por su apoyo incondicional y también un agradecimiento especial a los catedráticos por su apoyo incondicional por sus enseñanzas y consejos especialmente a Ernesto Alonso Emestica Avalos, y también a Omar Otoniel Flores Cortez muchas gracias y también a mis compañeros por su apoyo y por darme ánimos en los momentos difíciles y por sus consejos y especialmente a mis amigos, Samuel Eduardo García García por su amistad y apoyo y también, Denis Edgardo Aguilar Hernández y a todos mis amigos gracias y estoy agradecido por mis amigos que integran este grupo de trabajo por su apoyo y amistad a Carlos Hernández y a David Aguilar por su apoyo y amistad primero Dios todas nuestras metas se cumplan en este año.

Marcos Rafael Constancia Perla

Agradecimiento

Primeramente estoy agradecido por la bendición de poder haber terminado mi carrera en Técnico en Ingeniería de Hardware gracias a Dios y por haberme cuidado a pesar de la delincuencia que se vive día con día, y porque a pesar de la situación económica mis padres estuvieron siempre echándome la mano para poder seguir estudiando.

Así mismo contento por todo lo que aprendí durante estos años en la universidad, gracias a los Ingenieros y Licenciados que siempre están dando lo mejor de ellos para los estudiantes .

Carlos Sigfredo López Hernández

Índice

Introducción.	i
--------------------	---

Capítulo I

Situación Actual

1.1. Situación Problemática.	1
1.2. Enunciado del Problema.	4
1.3. Justificación.	4
1.4. Objetivos.	5
1.4.1. Objetivo General.	5
1.4.2. Objetivos Específicos.	5
1.5. Delimitaciones.	6
1.6. Alcances.	8
1.7. Estudio de Factibilidad.	9
1.7.1. Estudio de Factibilidad Económica.	9
1.7.2. Estudio de Factibilidad Técnica.	12

Capítulo II

Documentación Técnica

2.1. Marco Teórico de Referencia.	21
2.1.1. Informática Forense.	21
2.1.2. Principios de la Informática Forense.	22
2.1.3. Informática Forense Normas Fundamentales.	22
2.1.4. Informática Forense Objetivos.	23
2.1.5. Evidencia Digitales.	24
2.1.6. Procedimiento utilizado para llevar a cabo un análisis forense.	24
2.1.7. Tipos de Análisis Forenses.	29
2.1.8. Marco legal.	32
2.2. Marco Teórico de la Solución.	38
2.2.1. Manual de instalación y uso de Filerecovery Professional.	39
2.2.2. Manual de instalación y uso de Recuva.	59

2.2.3. Manual de Instalación y uso de TweakNowRegCleaner.	69
2.2.4. Manual de uso de RegSeeker	76
2.2.5. Manual de instalación y uso de Malwarebytes.....	80
2.2.6. Manual de uso de NTPWEDIT	92
2.2.7. Manual de uso de Browser Password Decryptor	99
2.2.8. Manual de uso de WebBrowserPassView.....	106
2.2.9. Manual de uso de Ardamax Keylogger.....	109
2.2.10. Manual de uso de Revealer Keylogger	123
2.3. Marco Teórico Conceptual.....	128
2.4. Documentación Técnica.....	135
2.4.1 Documentación técnica de RegSeeker	135
2.4.2. Documentación técnica de RegCleaner.....	136
2.4.3. Documentación técnica de Malware Bytes Anti-Malware.....	137
2.4.4. Documentación técnica de NTPWEDIT	138
2.4.5. Documentación Técnica de Ardamax Keylogger	138
2.4.6. Documentación Técnica de Revealer Keylogger	139
2.4.7. Documentación Técnica de FILERECOVERYProfessional.....	140
2.4.8. Documentación Técnica de Recuva	141
2.4.9. Documentación Técnica de Browser Password Decryptor	142
2.4.10. Documentación Técnica de WebBrowserPassView	142

Capítulo III

Desarrollo de la Solución

3.1. Propuesta de solución.....	144
3.2. Conclusiones	159
3.3. Recomendaciones.....	160
3.4. Referencias.....	161
Anexos.....	162

Introducción.

El desarrollo de cada país se demuestra por el constante progreso tecnológico en los cuales existen aspectos notorios a tomar en cuenta, entre ellos destacan la situación problemática que experimenta la sociedad salvadoreña, por ende supone una evolución en el accionar de la delincuencia cibernética. Dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos cibernéticos ilícitos.

Es aquí donde surge el enunciado del problema ¿Con que tipos de herramientas debe contar el kit de informática forense que ayude como material de apoyo en actividades de diplomados realizadas en la Universidad Tecnológica de El Salvador?

Dando como justificación a dicho problema la elaboración de un kit de herramientas de informática forense con el cual se pretende ayudar y reforzar las competencias de los estudiantes sirviendo este como material de apoyo en los diplomados que la universidad realice.

Como objetivo general se ostenta el desarrollar un kit de herramientas de software básicas sobre informática forense para que pueda ser utilizado como material de apoyo en diplomados realizados por la Universidad Tecnológica de El Salvador.

Mientras que los objetivos específicos son. Evaluar las herramientas más adecuadas que se incluirán en el kit, como también desarrollar un manual de uso para cada una de ellas y por ultimo desarrollar un CD el cual contenga dichas herramientas con su respectivo manual de uso.

La Informática Forense es una disciplina criminalística que tiene como objeto la investigación en sistemas informáticos de hechos con relevancia jurídica o para la simple investigación privada. Para conseguir sus objetivos, la Informática Forense desarrolla técnicas idóneas para ubicar, reproducir, analizar y recuperar evidencias digitales o archivos con fines legales. Todo acto en el que un sistema informático digital esté involucrado puede convertirse en causa de estudio y de análisis y mediante este proceso puede llevarse a juicio según la información recopilada. Es a partir de ahí que se utilizan herramientas diseñadas para dicha causa por ejemplo:

- **Recuperación de archivos eliminados:** Se utilizará cuando se quiera recuperar información que ya ha sido eliminada ya sea por error o por el solo hecho de querer recuperarla.
- **Keyloggers:** La cual se utilizará para la captura de información de cuentas de correo electrónico, contraseñas e información que pueda ser útil para la investigación.
- **Recuperadores de contraseñas guardadas en navegadores:** Su utilización será para la recuperación de correos y contraseñas de cualquier sitio web.
- **Análisis de Malware:** Se utilizará para verificar que no existan archivos malintencionados dentro de la computadora.
- **Análisis del Registro De Windows:** Permitirá obtener datos del registro como usuarios, permisos, ficheros ejecutados, información del sistema, e información de aplicaciones.

- **Modificación de contraseñas de usuarios de Windows:** Permitirá acceder a un sistema operativo protegido por contraseña.

En el marco teórico de referencia se desarrolla la metodología forense así como la recolección y la identificación de evidencias digitales cuando se ha producido un ataque informático. Además se describen los usos que se le pueden dar a la informática forense. A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original, también posee un marco legal en el cual están descritos las acciones que están penadas como delito informático y la pena que se podría enfrentar el acusado de encontrársele culpable. Por otra parte se cuenta con un marco teórico conceptual en el cual se definen los términos utilizados en este documento, además cuenta con la documentación técnica, el cual describe las características de los programas que se incluyen el CD interactivo.

Capítulo I

Situación Actual.

1.1. Situación Problemática.

El constante progreso tecnológico que experimenta la sociedad salvadoreña, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos. Esta realidad ha originado un debate en torno a la necesidad de distinguir o no los delitos informáticos del resto.

Diversos autores y organismos han propuesto definiciones de los delitos informáticos, aportando distintas perspectivas y matices al concepto. Algunos consideran que es innecesario diferenciar los delitos informáticos de los tradicionales, ya que, según éstos se trata de los mismos delitos, cometidos a través de otros medios.

Partiendo de esta compleja realidad y tomando como referencia el “Convenio de Ciberdelincuencia del Consejo de Europa”, se puede definir los delitos informáticos como: “los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos”.

En la Universidad Tecnológica de El Salvador se necesita contar con más material de apoyo para que los alumnos posean conocimientos ante diversos factores que se pueden dar como delitos informáticos tradicionales hacker, trolls, cracker.

Características principales de delitos informáticos.

Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos.

La criminalidad informática tiene un alcance mayor y puede incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados como medio. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

La Organización de Naciones Unidas reconoce los siguientes tipos de delitos informáticos:

Fraudes cometidos mediante manipulación de computadoras.

Manipulación de datos de entrada.

Daños o modificaciones de programas o datos computarizados.

Existen leyes que tienen por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos en las variedades existentes contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías.

Violación de comunicaciones privadas, violación agravada de comunicaciones, captación de comunicaciones, revelación del secreto profesional.

Una misma acción dirigida contra un sistema informático puede incurrir a la violación de varias leyes penales, algunos autores expresan que el "uso de la informática no supone más que un *modus operandi* nuevo que no plantea particularidad alguna respecto de las formas tradicionales de comisión".

Una clara dificultad para la persecución de estos ilícitos, ha sido que el ciudadano no considera delincuente al autor de estos delitos, entre los propios victimarios algunas veces existe una reivindicación que subyace a toda su actividad, como es el caso de los hackers, quienes cuentan con toda una "filosofía" preparada para respaldar su actividad afirmando que esperan un mundo más libre, que disponga de acceso a todas las obras de la inteligencia, y basándose en ese argumento divulgan las claves que tienen en su actividad.

los Trolls describen a personas que publican mensajes provocadores, irrelevantes o fuera de tema en una comunidad en línea, como ser un foro de discusión, sala de chat, comentarios de blog, o similar, con la principal intención de molestar o provocar una respuesta emocional negativa en los usuarios y lectores, con fines diversos (incluso por diversión)² o, de otra manera, alterar la conversación normal en un tema de discusión, logrando que los mismos usuarios se enfaden y se enfrenten entre sí.

1.2. Enunciado del Problema.

¿Con que tipos de herramientas debe contar el kit de informática forense que ayude como material de apoyo en actividades de diplomados realizadas en la Universidad Tecnológica de El Salvador?

1.3. Justificación.

Con la elaboración de un kit de herramientas en informática forense se pretende ayudar y reforzar las competencias de los estudiantes siendo un material de apoyo en actividades de diplomados, proporcionando temas prácticos y teóricos que permitan mejorar el desarrollo y la competitividad que los estudiantes necesitan dominar en aspectos como:

Eliminación y modificación de contraseñas de usuarios de Windows

Recuperación de archivos borrados

Análisis y protección anti malware

Keyloggers

Análisis y limpieza del registro de Windows

Recuperación de contraseñas guardadas en navegadores Web, redes sociales y nube.

Se pretende reforzar los conocimientos en esta área de informática para que los estudiantes del técnico en ingeniería de hardware de la Universidad Tecnológica de El Salvador, estén a un nivel aceptable sobre el uso de la informática forense.

1.4. Objetivos.

1.4.1. Objetivo General.

Desarrollar un kit de herramientas de software básicas sobre informática forense para que pueda ser utilizado como material de apoyo en diplomados realizados por la Universidad Tecnológica de El Salvador.

1.4.2. Objetivos Específicos.

Identificar, y seleccionar las características de cada herramienta que se incluirá en el kit de informática forense.

Diseñar un manual para el uso correcto de las herramientas de software seleccionado.

Desarrollar un CD interactivo que contenga el manual de uso y las herramientas de software básicas de informática forense.

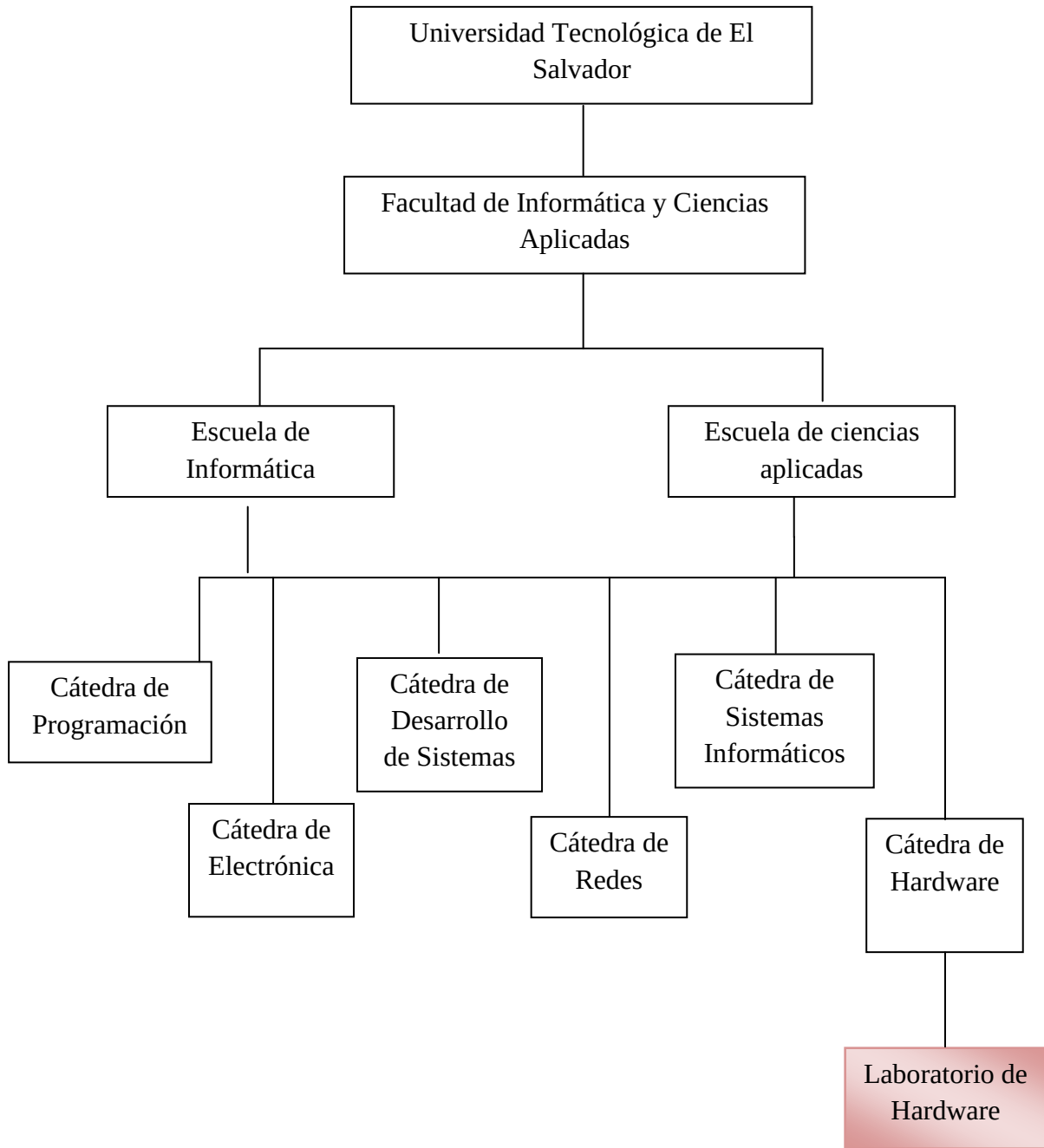
1.5. Delimitaciones.

Geográfica: Se realizará en la Universidad Tecnológica de El Salvador "Calle Arce #1020, San Salvador, El Salvador, Centro América.

Temporal: El proyecto de desarrollo de los productos se llevará a cabo en un lapso de tiempo comprendido desde Octubre 10 a Noviembre 5 del 2015.

Organizacional: Universidad Tecnológica de El Salvador, a través de su Facultad de Informática y Ciencias Aplicadas, Escuela de Informática, Cátedra de Hardware, Laboratorio de Hardware.

Organigrama.



1.6. Alcances.

El proyecto está enfocado en realizar un kit de herramientas básicas de informática forense el cual contará con su respectivo manual de uso de cada programa este se utilizará ante acciones relacionadas con la investigación, recuperación de archivos, recuperación de contraseñas almacenadas en los navegadores Web, análisis de malware, eliminación o modificación de contraseñas de usuarios de Windows, herramientas de captura de datos por medio del teclado, análisis y limpieza del registro de Windows, hallazgos y presentación de evidencias informáticas y de protección ante acciones tales como hurto de información personal, acciones digitales ilegales, ataques informáticos, y vulnerabilidades de sistemas, así como también resolver problemas de Software y Hardware, también contara con una ficha técnica de cada programa incluido.

Promesa	Producto
Identificar, y seleccionar las características de cada herramienta que se incluirá en el kit.	Fichas con características técnicas y requerimientos del sistema para cada programa.
Orientar a los usuarios sobre el uso correcto de algunas herramientas básicas de informática forense.	Manual impreso de uso de las herramientas básicas de informática forense.
Proporcionar a la institución un CD con un kit de herramientas básicas de informática forense.	Elaboración de un CD con herramientas básicas de software sobre informática forense y uso.

1.7. Estudio de Factibilidad.

1.7.1. Estudio de Factibilidad Económica.

Cuadro de Evaluación económico. Eliminación y modificación de contraseñas de usuarios de Windows.			
Estudio de Factibilidad Económica			
Nombre del Producto	NTPWEDIT	OPHCRACK	RESET WINDOWS PASSWORD
Precio	Free Software	Free software	Free software
Análisis	Económicamente los 3 software evaluados son factible para el usuario por ser de licencia free.		
Establecimiento consultado o URL	http://theoven.org/index.php?topic=1103.0	http://ophcrack.sourceforge.net/	http://tussoftwaresiemprefull.com/software/reset-windows-password-full-passcape-recupera-tu-contrasena-de-windows-vista-xp-y-7/

Cuadro de Evaluación económico. Análisis y limpieza del registro de Windows			
Estudio de Factibilidad Económica			
Nombre del Producto	RegDecoder	RegSeeker	RegCleaner
Precio	Free	Free	Free
Análisis	Económicamente los 3 software evaluados son factible para el usuario por ser de licencia free.		
Establecimiento consultado o URL	http://www.toolwar.com/2014/01/registrydecoder-windows-registry.html	http://regseeker.uptodown.com/	http://es.ccm.net/download/descargar-44-tweaknow-regcleaner

Cuadro de Evaluación económico. Recuperación de archivos borrados.			
Estudio de Factibilidad Económica			
Nombre del Producto	Recuva	Filerecovery Professional	DiskDigger
Precio	Free Software	Free software	Free software
Análisis	Económicamente los 3 software evaluados son factible para el usuario por ser de licencia free.		
Establecimiento consultado o URL	https://www.piriform.com/recuva	http://www.intercambiosvirtuales.org/software/filerecovery-2013-v5-professional-multilenguaje-espanol-herramienta-definitiva-para-la-recuperacion-de-archivos-y-datos	http://diskdigger.softonic.com/

Cuadro de Evaluación económico. Análisis y protección Anti Malware.			
Estudio de Factibilidad Económica			
Nombre del Producto	Malware bytes	Bit defender total security 2015	Emsisoft Anti Malware
Precio	Free Software	Free software	Free software
Análisis	Económicamente los 3 software evaluados son factible para el usuario por ser de licencia free.		
Establecimiento consultado o URL	https://es.malwarebytes.org/	http://www.fiuxy.com/programas-gratis/3799750-descargar-bitdefender-total-security-2015-espanol-mega-crack-1-ano-32-y-64-bits.html	http://a-squared-anti-malware.uptodown.com/

Cuadro de Evaluación económico. Keyloggers			
Estudio de Factibilidad Económica			
Nombre del Producto	Ardamax Keylogger	Revealer Keylogger	DanuSoft Free Keylogger
Precio	Free	Free	Free
Análisis	Económicamente los 3 software evaluados son factible para el usuario por ser de licencia free.		
Establecimiento consultado o URL	http://ardamax-keylogger.uptodown.com/	http://revealer-free-edition.uptodown.com/	http://www.updownload.es/danusoftware-free-keylogger/

Cuadro de Evaluación económico. Recuperación de contraseñas guardadas en navegadores Web.			
Estudio de Factibilidad Económica			
Nombre del Producto	Browser Password Decryptor	Web Browser Password View	Password RecoveryBundle
Precio	Free	Free	Free
Análisis	Económicamente los 3 software evaluados son factible para el usuario por ser de licencia free.		
Establecimiento consultado o URL	http://browser-password-decryptor.malavida.com/	http://descargar.info/webbrowserpasswordview/	http://www.intercambiovirtuales.org/software/elcomsoft-password-recovery-bundle-forensic-edition-v2013-recuperacion-completa-de-todos-los-tipos-de-contrasenas-rar-office-pdf-wireless-etc

1.7.2. Estudio de Factibilidad Técnica.

Cuadro de evaluación de productos. Eliminación y modificación de contraseñas de usuarios de Windows. Se requiere un nivel de calificación del 80%							
Característica Técnica	Ponderación	NTPWEDIT		OPHCRACK		RESET WINDOWS PASSWORD	
Elimina o modifica contraseñas de usuarios de usuarios Windows, colocando el disco duro en modo de unidad extraíble.	20%	2	40	0	0	0	0
Carga hashes desde SAM cifradas recuperadas desde una partición de disco duro.	20%	2	40	1	20	1	20
Restablece y modifica las contraseñas de los usuarios locales y administradores.	30%	2	60	2	60	2	60
Permite la instalación en el mismo sistema operativo del cual se quiere averiguar la contraseña.	10%	0	0	2	20	0	0
Módulo de fuerza bruta para contraseñas simples	10%	2	20	2	20	2	20
Gráficos en tiempo real para analizar las contraseñas.	10%	0	0	2	20	0	0
Total	100%		160		140		100
Ponderación Final			160/2 =80 %		140/2 =70%		100/ 2=50%
Resultado Obtenido		Aprobado		Reprobado		Reprobado	

Análisis: En la tabla anterior se hizo un análisis técnico de 3 programas que sirven para la eliminación y modificación de contraseñas a nivel de usuarios administradores en sistemas operativos Windows y se seleccionó el programa NTPWEDIT ya que elimina o modifica contraseñas de usuarios de usuarios Windows, colocando el disco duro en modo de unidad extraíble, módulo de fuerza bruta para contraseñas simples y carga hashes desde SAM cifradas recuperadas desde una partición del disco duro.

Cuadro de evaluación de productos. Recuperación de archivos borrados. Se requiere un nivel de calificación del 80%							
Característica Técnica	Ponderación	Recuva		Filerecovery Professional		DiskDigger	
Recupera Archivos borrados del disco duro.	20%	2	40	2	20	2	40
Capacidad de analizar todos los volúmenes en un ordenador local.	15%	0	0	1	15	0	0
Crea un árbol de directorios de archivos perdidos y eliminados.	20%	0	0	2	40	0	0
Recupera archivos de memorias USB y Micro SD.	15%	2	30	2	30	2	30
Motor de escaneo rápido que permite crear rápidamente la lista de archivos.	5%	1	5	1	5	2	10
Recupera en un 90% Imágenes borrados de cualquier medio.	25%	1	25	2	50	1	25
Total	100%		100		160		105
Ponderación Final			100/2=50%		160/2=80%		105/2=52.50%
Resultado Obtenido		Reprobado		Aprobado		Reprobado	

Análisis: En la tabla anterior se hizo un análisis técnico de 3 programas que sirven para la recuperación de archivos borrados y se seleccionó el software Filerecovery Professional ya que tiene la capacidad de crear un árbol de directorios de archivos eliminados, además recupera en un 90% imágenes y permite recuperar ya sea de discos duros o medios extraíbles como memorias USB, Micro SD. Y Mp3.

Cuadro de evaluación de productos. Análisis y protección Anti malware. Se requiere un nivel de calificación del 85%							
Característica Técnica	Ponderación	Malwarebytes		Bit defender total security 2015		Emsisoft Anti Malware	
Localiza y destruye toda clase de malware, como gusanos, troyanos, rootkits, rogues (falsos antivirus), spyware y otros.	20%	1	20	2	40	2	40
Evita el acceso de entrada y salida a las páginas web maliciosas conocidas.	15%	1	15	2	30	1	15
Eliminar cualquier aplicación con un comportamiento susceptible de constituir una amenaza.	20%	2	40	2	40	2	40
Lista de elementos ignorados para el escáner y la protección del módulo.	10%	2	20	1	10	1	10
Tres tipos de escaneo: análisis rápido, análisis personalizado y análisis completo.	15%	2	30	1	15	1	15
Tecnología de exploración y detección heurística avanzada.	20%	2	40	1	20	1	20
Total	100%		165		155		140
Ponderación Final			165/2 =82.50%		155/2 =77.50 %		140/2 =70%
Resultado Obtenido		Aprobado		Reprobado		Reprobado	

Análisis: En la tabla anterior se hizo un análisis técnico de 3 programas que sirven para el análisis, la detección y eliminación de malware y se seleccionó el programa Malwarebytes ya que localiza y destruye toda clase de malware, a la vez evita el acceso de entrada y salida a las páginas web maliciosas conocidas, posee tres tipos de escaneo: análisis rápido, análisis personalizado y análisis completo, consta de tecnología de exploración y detección heurística avanzada.

Cuadro de evaluación de Keylogger. Se requiere un nivel de calificación del 80%							
Característica Técnica	Ponderación	Revealer Keylogger		Ardamax Keylogger		DanuSoft Free Keylogger	
Envío al correo electrónico de registros capturados.	20%	2	40	2	40	2	40
Modo invisible hace absolutamente invisible a cualquier persona.	20%	2	40	2	40	2	40
Permite proteger la configuración del programa, de modo oculto y archivo de registro.	20%	2	40	2	40	0	0
Registra cada golpe de teclado. Captura las contraseñas y todo el texto.	15%	2	30	2	30	1	15
Configura una combinación de teclas para hacer visible la interfaz cuando está en modo oculto.	10%	2	20	2	20	1	10
Actúa en segundo plano de forma discreta.	15%	2	30	2	30	0	0
Total	100%		200		200		105
Ponderación Final			200/2 =100%		200/2 =100%		105/2 =52.50%
Resultado Obtenido			Aprobado		Aprobado		Reprobado

Análisis: En la tabla anterior se hizo un análisis técnico de 3 programas que sirven para la captura de datos en forma oculta y se seleccionó el programa Ardamax Keylogger ya que posee la capacidad de enviar al correo electrónico los registros capturados, además actúa en segundo plano de forma discreta y registra cada golpe de teclado, captura las contraseñas y todo el texto.

Cuadro de evaluación de Recuperadores de Contraseñas guardadas en navegadores Web. Se requiere un nivel de calificación del 80%							
Característica Técnica	Ponderación	Browser Password Decryptor		Web Browser Pass View		<u>Password RecoveryBundle</u>	
Descripta las contraseñas directamente desde el registro de Google Chrome.	20	1	20	1	20	2	40
Recupera contraseñas almacenadas de todos los navegadores.	30	2	60	2	60	0	0
Recuperación instantánea de contraseñas.	20	2	40	2	40	2	40
Muestra en una tabla, con el navegador, la URL, el usuario y la contraseña en otras columnas.	30	2	60	2	60	0	0
Total	100%		180		180		80
Ponderación Final			180/2 =90%		180/2 =90%		80/2 =40%
Resultado Obtenido		Aprobado		Aprobado		Reprobado	

Análisis: En la tabla anterior se hizo la comparación de 3 programas que sirven para la recuperación de contraseñas guardadas en los navegadores Web, se escogió el programa Browser Password Decryptor debido a que recupera contraseñas almacenadas de todos los navegadores y las muestra en una tabla con la URL de la página visitada.

Cuadro de evaluación de Análisis y Registro de Windows. Se requiere un nivel de calificación del 70%							
Característica Técnica	Ponderación	RegGripper		RegSeeker		RegCleaner	
Aplicación para la extracción, la correlación, y muestra la información del registro.	20%	1	20	1	20	1	20
Permite obtener de forma gráfica datos del sistema, usuarios y aplicaciones partiendo del registro.	20%	2	40	2	40	1	20
Extrae diversa información útil sobre la configuración y ajustes de la máquina.	15%	0	0	1	15	1	15
Explorador del Registro de Seguridad.	20%	2	40	2	40	2	40
Muestra el nombre del sistema Windows, ID y clave, fechas de instalación e información sobre el registro del usuario.	15%	0	0	2	30	1	15
Muestra una rápida visión general (CPU, Monitores, Tarjeta de Red y Sonido, además de tarjetas de Red), y mapeo completo de dispositivo de los dispositivos configurados que funcionan sobre la máquina.	10%	0	0	2	20	1	10
Total	100%		100		165		120
Ponderación Final			100/2 =50%		165/2 =82.50%		120/2 =60%
Resultado Obtenido		Reprobado		Aprobado		Reprobado	

Análisis: En la tabla anterior se hizo la comparación de 3 programas que sirven para el análisis y limpieza del registro de Windows y se eligió el programa RegSeeker, el cual permite obtener de forma gráfica datos del sistema, usuarios y aplicaciones partiendo del registro. Posee una aplicación para la extracción, la correlación, y muestra la información del registro, además muestra el nombre del sistema Windows, ID y clave, fechas de instalación e información sobre el registro del usuario, y libera espacio en el disco duro.

Análisis General de Factibilidad.

Según el registro anterior y las comparaciones económicas y técnicas de las áreas presentadas se ha escogido un software y los programas a utilizar son los siguientes:

- NTPWEDIT
- FileRecovery Professional
- MalwareBytes
- Ardamax Keylogger
- Browser Password Decryptor
- RegSeeker

Dispositivos móviles

Esta sección dispone de un set de utilidades y herramientas para la recuperación de datos y análisis forense de dispositivos móviles. He incluido herramientas comerciales dado que utilizo algunas de ellas y considero que son muy interesantes e importantes.

iPhone

- iPhoneBrowser - Accede al sistema de ficheros del iphone desde entorno gráfico.
- iPhone Analyzer - Explora la estructura de archivos interna del iphone.
- iPhoneBackupExtractor - Extrae ficheros de una copia de seguridad realizada anteriormente.
- iPhone Backup Browser - Extrae ficheros de una copia de seguridad realizada anteriormente.

- iPhone-Dataprotection - Contiene herramientas para crear un disco RAM forense, realizar fuerza bruta con contraseñas simples (4 dígitos) y descifrar copias de seguridad.
- iPBA2 - Accede al sistema de ficheros del iphone desde entorno gráfico.
- sPyphone - Explora la estructura de archivos interna.

BlackBerry

- Blackberry Desktop Manager - Software de gestión de datos y backups.
- Phoneminer - Permite extraer, visualizar y exportar los datos de los archivos de copia de seguridad.
- Blackberry Backup Extractor - Permite extraer, visualizar y exportar los datos de los archivos de copia de seguridad.
- MagicBerry - Puede leer, convertir y extraer la base de datos IPD.

Android

- android-locdump. - Permite obtener la geolocalización.
- androguard - Permite obtener, modificar y desensamblar formatos DEX/ODEX/APK/AXML/ARSC
- viaforensics - Framework de utilidades para el análisis forense.

La lista de software anteriores se ha elegido por ser de licencia free y técnicamente los más efectivos, beneficiando al usuario.

Análisis para evidencias digitales de fotografías

Amped FIVE

Software para el Análisis Forense de Imágenes y Videos

- Carga imágenes y videos en cualquier formato
- Distingue placas de licencias, caras y cualquier otra cosa mejorando notablemente la imagen
- Generación automática de reportes detallados con la metodología científica usada

Stegsecret

Stegsecret es un proyecto de código abierto steganalysis (GNU / GPL) que hace posible la detección de información oculta en diferentes medios digitales. StegSecret es una herramienta steganalysis multiplataforma basada en Java que permite la detección de información oculta mediante el uso de los métodos más conocidos esteganográficos. Detecta EOF, LSB, DCT y otras técnicas.

Capítulo II

Documentación Técnica.

2.1. Marco Teórico de Referencia.

2.1.1. Informática Forense

La Informática Forense es una disciplina criminalística que tiene como objeto la investigación en sistemas informáticos de hechos con relevancia jurídica o para la simple investigación privada. (Javier Pages Lopez, 2013)

Para conseguir sus objetivos, la Informática Forense desarrolla técnicas idóneas para ubicar, reproducir y analizar evidencias digitales con fines legales. (Javier Pages Lopez, 2013)

Todo hecho en el que un sistema informático esté involucrado, tanto si es el fin o un medio, puede ser objeto de estudio y análisis, y por ello, puede llevarse a juicio como medio probatorio. (Javier Pages Lopez, 2013)

Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. (Oscar López, 2002)

La informática forense nace en vista de la necesidad del personal del derecho en poder afrontar nuevas tareas probatorias. Esta necesidad crea el nacimiento de los llamados detectives digitales o peritos informáticos. Los Informáticos forenses tienen la ardua labor de realizar investigaciones en busca de evidencia digital. (Lilia Quituisaca Samaniego, 2015)

2.1.2. Principios de la Informática Forense

- Adherirse a estándares legales
- Formación específica en técnicas forenses
- Obtener Permisos:
 - investigación/ recolección evidencias
 - monitorizar uso de ordenadores
- Control de Evidencias Digitales. (Javier Pages Lopez, 2013)

2.1.3. Informática Forense Normas Fundamentales.

1. Preservar la evidencia original
2. Establecer y mantener la Cadena de Custodia
3. Documentar todo hecho
4. No extralimitarse
 - Conocimientos personales
 - Leyes, Normas , Procedimientos
5. Riesgos:
 - Corromper evidencias. (Sebastián Gómez Hernán Herrera , 2009)

2.1.4. Informática Forense Objetivos.

- Recoger rastros probatorios para averiguar información
- Recoger diferentes tipos de evidencias
- Analizar las evidencias encontradas
- Confirmar por pruebas cruzadas

Así se establecen las bases para probar que se han cometido actos deshonestos o ilegales.

(Sebastián Gómez Hernán Herrera , 2009)

Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto. (Javier Pages Lopez, 2013)

En el momento en que un criminal cruza una escena del crimen, o entra en contacto con una víctima, la víctima se queda con algo del criminal, pero este a su vez se lleva algo a cambio. (Javier Pages Lopez, 2013)

El Principio de Locard tiene plena validez en el ámbito informático y las evidencias electrónicas. Hay que determinar el ¿Cómo? el ¿Dónde? podemos encontrar las evidencias. (Javier Pages Lopez, 2013)

2.1.5. Evidencia Digitales.

- Cualquier documento, fichero, registro, dato, etc. contenido en un soporte informático.
- Susceptible de tratamiento digital
 - Documentos de Ofimática.
 - Comunicaciones digitales.
 - Imágenes digitales.
 - Bases de Datos.
 - Ficheros de Registro de Actividad. (Javier Pages Lopez, 2013)
 - Internet
 - Redes Sociales
 - Dispositivos Móviles
 - Sistemas en la Nube

2.1.6. Procedimiento utilizado para llevar a cabo un análisis forense.

Estudio preliminar.

En esta fase se realiza un estudio inicial mediante entrevistas y documentación entregada por el cliente con el objetivo de tener una idea inicial del problema que nos vamos a encontrar. (Jose Luis Rivas Lopez, 2009)

Adquisición de datos.

Se realiza una obtención de los datos e informaciones esenciales para la investigación. Se duplican o clonan los dispositivos implicados para un posterior análisis. En esta fase habrá que tener mucho cuidado en la adquisición de los datos puesto que cabe la posibilidad de incumplir los derechos fundamentales del atacante. (Jose Luis Rivas Lopez, 2009)

Análisis e investigación.

Se realiza un estudio con los datos adquiridos en la fase anterior. En esta fase también habrá que tener mucho cuidado puesto que cabe la posibilidad de incumplir los derechos fundamentales del atacante. (Jose Luis Rivas Lopez, 2009)

Realización del informe.

En esta fase se elabora el informe que será remitido a la dirección de la organización o empresa. Posteriormente, se podrá usar para acompañar la denuncia que realicemos a la autoridad competente. (Jose Luis Rivas Lopez, 2009)

Metodología en un incidente de seguridad.

Los incidentes de seguridad normalmente son muy complejos y su resolución presenta muchos problemas. A continuación se muestran las siguientes fases en la prevención, gestión y detección de incidentes: (Jose Luis Rivas Lopez, 2009)

Preparación y prevención.

En esta fase se toman acciones para preparar la organización antes de que ocurra un incidente. Por tanto, se deberá empezar por tratar de analizar qué debe ser protegido y qué medidas técnicas y organizativas tienen que implementarse. Una vez hechos los diversos análisis se podrá considerar que la organización ya tiene identificadas las situaciones que pueden provocar un incidente de seguridad y ha seleccionado los controles necesarios para reducirlas.

Pero aun hecho dicho análisis, siempre hay situaciones que no van a poder ser protegidas, por lo que se tendrá que elaborar un plan de continuidad de negocio. Dicho plan está formado por un conjunto de planes de contingencia para cada una de las situaciones que no están controladas. (Jose Luis Rivas Lopez, 2009)

Detección del incidente.

La detección de un incidente de seguridad es una de las fases más importante en la intervención de los sistemas. Hay que tener en cuenta que la seguridad absoluta es muy difícil y es esta fase la que nos sirve para clasificar y priorizar los incidentes acaecidos en nuestra organización.

La clasificación es la siguiente:

- Accesos no autorizados: un usuario no autorizado accede al sistema.
- Código malicioso: ha habido una infección de programas maliciosos (virus, gusano spyware, troyano, etc.) en un sistema

- Denegación de servicio: incidente que deja sin dar servicio (DNS, web, correo electrónico, etc.) a un sistema.
- Phishing: consiste en suplantar la identidad de una persona o empresa para estafar. Dicha estafa se realiza mediante el uso de ingeniería social consiguiendo que un usuario revele información confidencial (contraseñas, cuentas bancarias, etc.). El atacante suplanta la imagen de una empresa u organización y captura ilícitamente la información personal que los usuarios introducen en el sistema. (Jose Luis Rivas Lopez, 2009)

Respuesta inicial.

En esta fase se trata de obtener la máxima información posible para determinar qué tipo de incidente de seguridad ha ocurrido y así poder analizar el impacto que ha tenido en la organización. La información obtenida en esta fase será utilizada en la siguiente para poder formular la estrategia a utilizar. Dicha información será fruto como mínimo de:

- Entrevistas con los administradores de los sistemas.
- Revisión de la topología de la red y de los sistemas.
- Entrevistas con el personal de la empresa que hayan tenido algo que ver con el incidente con el objetivo de contextualizarlo.
- Revisar los logs de la detección de la intrusión. (Jose Luis Rivas Lopez, 2009)

Formulación de una estrategia de respuesta ante el incidente.

Una vez recabada la información de la fase anterior, hay que analizarla para después tomar una decisión sobre cómo actuar. Las estrategias a utilizar dependerán de varios factores: criticidad de los sistemas afectados, si el incidente ha salido a la luz pública, la habilidad del atacante, cómo de sensible es la información a la que se ha tenido acceso, si el sistema de información está caído y la repercusión que esto tiene, etc. (Jose Luis Rivas Lopez, 2009)

Investigación del incidente.

En esta fase se determina quién, cuándo, dónde, qué, cómo y por qué ha ocurrido el incidente. Para investigar dicho incidente se divide el proceso en dos fases:

- Adquisición de los datos. La obtención de los datos es la acumulación de pistas y hechos que podrían ser usados durante el análisis forense de los ordenadores para la obtención de evidencias.
- Análisis forense. En esta fase se revisan todos los datos adquiridos en la fase anterior. Esta fase será descrita detalladamente más adelante. (Jose Luis Rivas Lopez, 2009)

Redacción del informe.

En esta última fase se redacta un informe que será entregado a la dirección de la organización o empresa así como a los cuerpos de policía del Estado o al juzgado si el incidente se denuncia. Dicho informe puede ser de dos clases: ejecutivo y técnico. El informe ejecutivo es un informe enfocado a personas sin conocimientos técnicos, mientras que el informe técnico explica de una manera técnicamente detallada el procedimiento del análisis. Se describirá más adelante, en el apartado relativo a la redacción del informe. (Jose Luis Rivas Lopez, 2009)

2.1.7. Tipos de Análisis Forenses.

Dependiendo del punto de vista diferentes tipos de análisis forense. Si lo vemos desde el punto de vista de lo que se va a analizar, nos encontraremos los siguientes tipos:

Análisis forense de sistemas:

En este análisis se tratarán los incidentes de seguridad acaecidos en servidores y estaciones de trabajo con los sistemas operativos: Mac OS, sistemas operativos de Microsoft (Windows 9X/Me, Windows 2000 server/workstation, Windows 2003 Server, Windows XP, Windows Vista, Windows 2008 Server, etc.), sistemas Unix (Sun OS, SCO Unix, etc.) y sistemas GNU/Linux (Debian, RedHat, Suse, etc.). (Jose Luis Rivas Lopez, 2009)

Análisis forense de redes:

En este tipo se engloba el análisis de diferentes redes (cableadas, Wireless, Bluetooth, etc.). (Jose Luis Rivas Lopez, 2009)

Análisis forense de sistemas embebidos:

En dicho tipo se analizan incidentes acaecidos en móviles, PDA, etc. Un sistema embebido posee una arquitectura semejante a la de un ordenador personal (Jose Luis Rivas Lopez, 2009)

Metodología y fases de un análisis forense

En el análisis forense con 3 fases bien diferenciadas a pesar de que, dependiendo del enfoque y del tipo que sea, dicho análisis se podrá dividir en más fases. (Jose Luis Rivas Lopez, 2009)

Adquisición de datos.

La adquisición de datos es una de las actividades más críticas en el análisis forense. Dicha criticidad es debida a que, si se realizase mal, todo el análisis e investigación posterior no sería válido debido a que la información saldría con impurezas, es decir, la información que creemos que es del origen no lo es realmente.

Una vez que se ha detectado un incidente de seguridad, uno de los primeros problemas del analista en la recogida de datos se resume en decir si el equipo hay que apagarlo o no. (Jose Luis Rivas Lopez, 2009)

Otro de los problemas y dependiendo del tipo de organización es la obtención de los siguientes datos: nombre y apellidos del responsable del equipo y usuario del sistema. Otros datos que se deben obtener como mínimo serían: modelo y descripción del sistema, número de serie, sistema operativo que está corriendo, así como el coste económico aproximado que tiene dicho incidente (por ejemplo, si ha sido atacado el sistema de gestión de un láser y para su equilibrado se precisa de técnicos que tienen que desplazarse, sería un coste axial como el tiempo de estar parado). (Jose Luis Rivas Lopez, 2009)

Análisis e investigación

La fase de análisis e investigación de las evidencias digitales es un proceso que requiere obviamente un gran conocimiento de los sistemas a estudiar. Las fuentes de recogida de información en esta fase son varias:

- registros de los sistemas analizados
- registro de los detectores de intrusión
- registro de los cortafuegos
- ficheros del sistema analizado. (Jose Luis Rivas Lopez, 2009)

Redacción del informe

La redacción del informe es una tarea ardua a la par que compleja, porque no sólo hay que recoger todas las evidencias, indicios y pruebas recabados sino que, además, hay que explicarlos de una manera clara y sencilla. Hay que tener en cuenta que muchas veces dichos informes van a ser leídos por personas sin conocimientos técnicos y obviamente tiene que ser igual de riguroso y debe ser entendido, con lo que habrá que explicar minuciosamente cada punto. Todo informe deberá tener perfectamente identificada la fecha de finalización de éste, así como a las personas involucradas en su desarrollo. (Jose Luis Rivas Lopez, 2009)

2.1.8. Marco legal

Delitos informáticos contra la privacidad en El Salvador.

Los delitos informáticos contra la privacidad se pueden definir como un grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos.

Esta tipificación se refiere a quien, sin estar autorizado, se apodere, utilice o modifique en perjuicio de un tercero, datos reservados de carácter personal o familiar, que se hallen registrados en ficheros o soportes informáticos, electrónicos, o cualquier otro tipo de archivo o registro, ya sea público o privado. Existen algunas circunstancias agravantes de la divulgación, las cuales se dan en función de:

El carácter de los datos: Ideología, creencias, salud, origen racial y preferencia sexuales.

Las circunstancias de la víctima: Menor de edad o incapaz.

Se comprende también la interceptación de las comunicaciones utilizando los medios técnicos para escuchar, transmitir, grabar o reproducir el sonido o la imagen. El ejemplo más común de interceptación lo constituye el correo electrónico. Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el lavado de dinero y para la coordinación de entregas y recogidas.

Piratería: El plagio de propiedad intelectual, mejor conocido como piratería ha crecido significativamente gracias a Internet.

Tipos de piratería:

Copia y distribución de software entre amigos.

Reinstalación de software empresarial en más máquinas de las autorizadas por la licencia.

Copia y distribución de programas a gran escala para venta en el mercado negro.

Distribución gratuita de software pirata por Internet.

Como consecuencia de la piratería se puede mencionar que existe una inhibición de la innovación y del desarrollo de nuevos productos, evasión de impuestos; en suma, amenazan al ritmo de crecimiento de economía global de la información.

Legislación sobre delitos informáticos en El Salvador.

La proliferación de la informática ha llegado a todos los ámbitos de la actividad del hombre. La reglamentación que tiene como objetivo la búsqueda de una forma de convivencia más armónica de la sociedad, no está exenta de los efectos de este nuevo medio.

Algunos países han venido legislando sobre temas relativos a la comisión de delitos vinculados a la informática, ya sea porque utilizan herramientas informáticas para realizarlos o porque el blanco de la infracción es de índole informático.

En El Salvador no existe una ley especial que regule lo concerniente a este tipo de ilícitos, sin embargo, existen artículos del actual código penal que contienen elementos de tipificación de delitos informáticos.

Estos son:

Amenazas que atentaren contra la seguridad de la persona y su familia a través de medios electrónicos y /o que pudiesen ser anónimos. Por ejemplo, amenazas de muerte a un funcionario a través de un correo electrónico.

Los artículos del código procesal penal que se emplean son:

Amenazas

Art. 154.- El que amenazare a otro en producirle a él o a su familia, un daño que constituyere delito en su persona, libertad, libertad sexual, honor o en su patrimonio, será sancionado con prisión de uno a tres años.

Agravación Especial

Art. 155.- En el caso del artículo anterior se considerarán agravantes especiales que el hecho fuere cometido con arma o por dos o más personas reunidas o si las amenazas fueren anónimas o condicionales. En estos casos la sanción se aumentara hasta en una tercera parte de su máximo.

Promoción de Pornografía Infantil, exhibiciones obscenas a través de Internet y correo electrónico. Por ejemplo, promoción de pornografía a través de páginas Web así como el envío de imágenes pornográfica por medio de correo electrónico.

Inducción, promoción, favorecimiento y determinación de la prostitución a través de Internet y correo electrónico.

Los artículos del código penal que se emplean son:

Inducción, Promoción y Favorecimiento de la Prostitución.

Art. 169.- El que indujere, facilitare promoviere o favoreciere la prostitución de persona menor de dieciocho años será sancionado con prisión de dos a cuatro años.

Pornografía.

Art. 172.- El que por cualquier medio directo difundiere, vendiere, o exhibiere material pornográfico entre menores de 18 años de edad o deficientes mentales será sancionado con prisión de 6 meses a dos años.

Utilización de menores con fines pornográficos y exhibicionistas.

Art. 173.- El que utilizaré a un menor de 18 años, con fines o espectáculos o exhibicionistas o pornográficos, será sancionado con prisión de 6 meses a un año.

La interceptación de mensajes electrónicos y otra información. Por ejemplo, a través de la red se puede interceptar correos electrónicos.

Obtención de claves de acceso y/o información electrónica. Por ejemplo, el uso de programas para monitorear el uso de computadoras a través de los cuales se pueden obtener las claves o información.

Divulgación de secretos profesionales. Por ejemplo, la publicación a través de Internet y correo electrónico sobre los secretos administrativos de una empresa.

Violación de Comunicaciones Privadas.

Art. 184.- El que con 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 cualquier otro tipo de archivos o registro público o privado, será sancionado con multa de 50 a 100 días.

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 6 meses a 2 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 artículos 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.

Revelación del 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 6 meses a 2 años, e inhabilitación especial de profesión u oficio de uno a dos años. (Código Penal de El Salvador. 1998)

Ley Especial Contra Actos de Terrorismo

Delito informático

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

a) Utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, información, documentos electrónicos, soportes informáticos, programas o sistemas de información y de comunicaciones, de servicios públicos, sociales, administrativos, de emergencia o de seguridad nacional, de entidades nacionales.

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.

2.2. Marco Teórico de la Solución.

Es un instructivo para el usuario que se desarrollará con el único objetivo de apoyar a los estudiantes para que puedan hacer un uso correcto de las herramientas que posee el CD interactivo, que estarán al servicio del laboratorio de Hardware de la Universidad Tecnológica de El Salvador cuando se realicen diplomados de informática forense.

El manual cuenta con la información teórica y práctica acerca de los programas que se incluyen en el kit, según las necesidades que el usuario tenga, se cubren áreas como lo son: La recuperación de archivos eliminados, Análisis y limpieza de registro de Windows, Cambio o modificación de contraseñas de usuarios en Windows, Análisis y protección Anti-Malware, Keyloggers, Recuperación de contraseñas guardadas en navegadores Web.

2.2.1. Manual de instalación y uso de Filerecovery Professional

Nota: Para el uso de este programa se debe estar en una cuenta de administrador, este programa es compatible desde Windows 2000 hasta Windows 8. En esta ocasión se realizará en sistema operativo Windows 7.

1. Una vez abierto el CD de herramientas, se da click en programas, luego en recuperación de archivos, y se selecciona el Filerecovery Professional. (Como lo muestra la imagen 1).

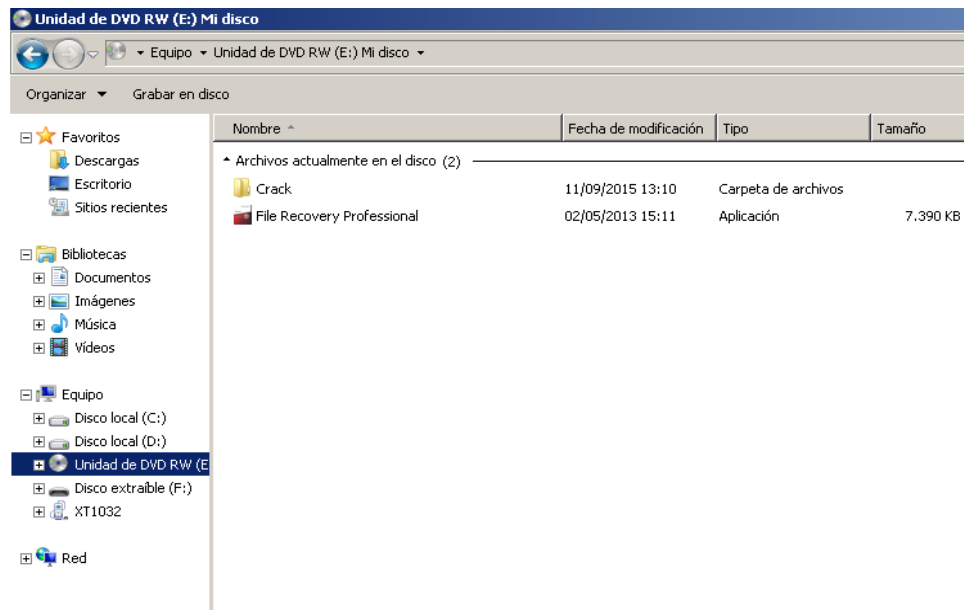


Imagen 1

2. Se presentará la siguiente ventana y se da click en “Next”. (Como se muestra en la imagen 2).



Imagen 2 (Welcome to the FILERECOVERY Professional Setup Wizard)

3. Seguidamente aparecerá el contrato de aceptación de términos, luego se selecciona la casilla de aceptación de términos y condiciones, seguidamente se da click en “Next”. (Como lo muestra la imagen 3).

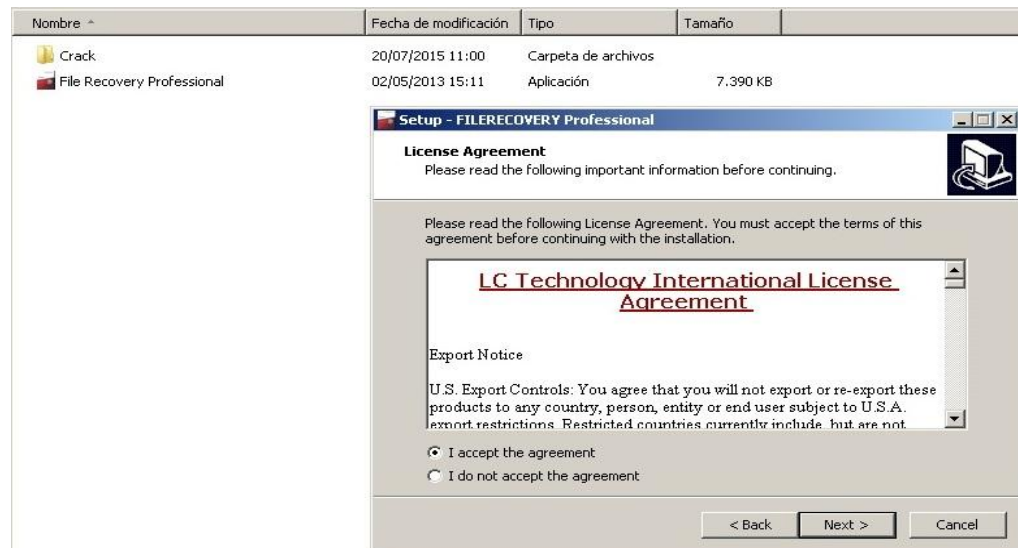


Imagen 3 (License Agreement)

4. En esta sección se elige la selección de ubicación de destino de la instalación, en este caso se elige la ruta predeterminada que indica el programa, se da click en "Next". (Como lo muestra la imagen 4).

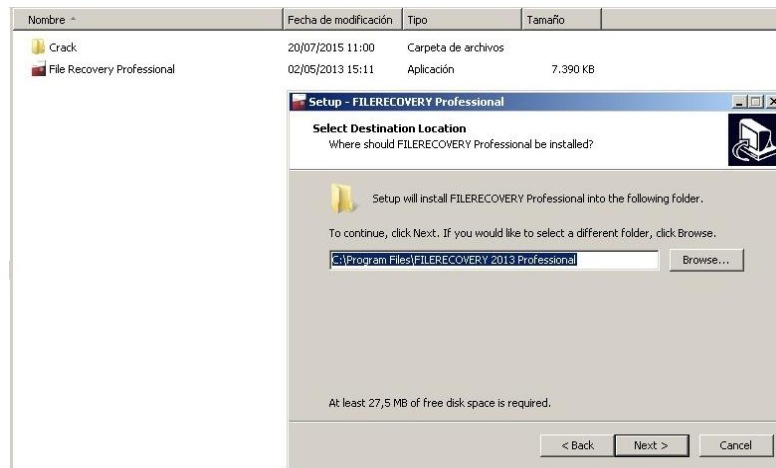


Imagen 4 (Select Destination Location)

5. En la siguiente ventana se muestra la carpeta del menú de selección de inicio, en esta sección la instalación creará los programas de accesos directos en la siguiente carpeta del menú inicio, en este caso se selecciona la ruta especificada del programa, click en "Next". (Como lo muestra la imagen 5).

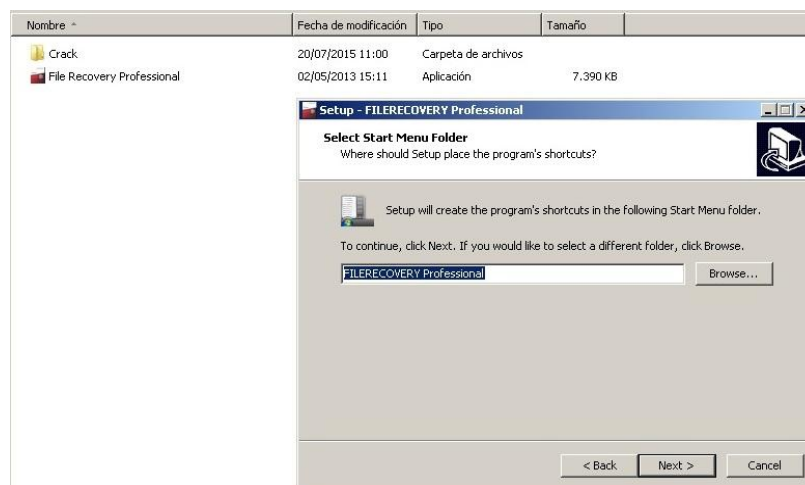


Imagen 5 (Select Start Menu Folder)

6. En esta ventana se seleccionan las tareas adicionales, la cual indica si se desea crear un acceso directo en el escritorio, de ser así se marca la casilla y luego se da click en "Next". (como lo muestra la imagen 6).

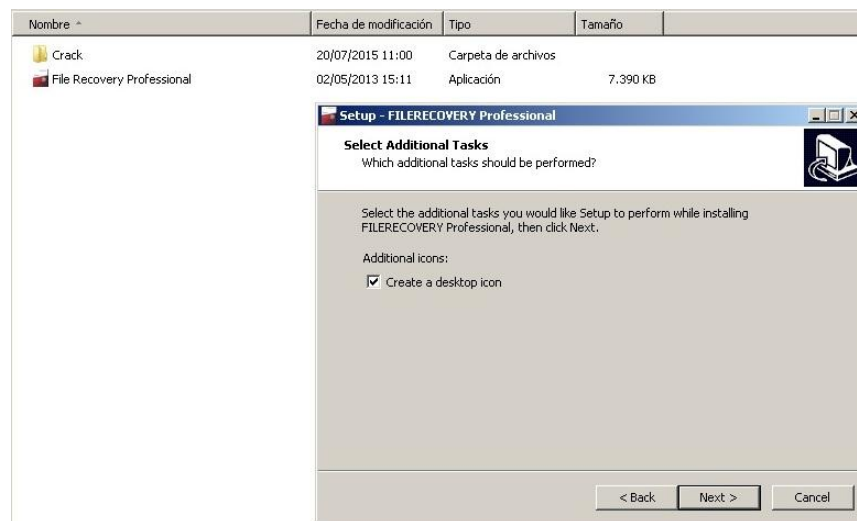


Imagen 6 (Select Additional Tasks)

7. En esta ventana se muestra la información de las opciones que anteriormente se seleccionaron como la selección de la locación del destino de la instalación, la carpeta del menú de selección de inicio, y las tareas adicionales, si todo esta correcto se continua con la instalación dando click en "Install" (Como se muestra en la imagen 7)



Imagen 7 (Ready to Install)

8. A continuación empezará con el proceso de instalación siguiendo los parámetros anteriormente seleccionados, este proceso durara pocos segundos. (Como se muestra en la imagen 8)

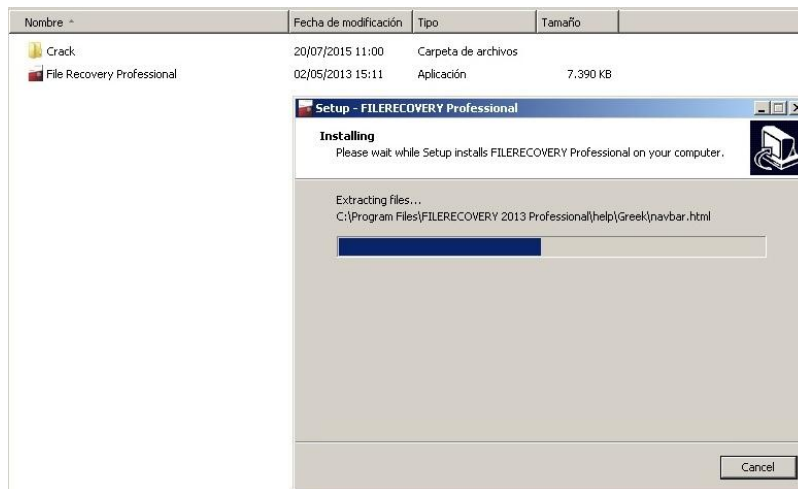


Imagen 8 (Installing)

9. Seguidamente mostrará la ventana donde indica que la instalación fue completada correctamente, seguidamente se desmarca la casilla "Launch FILERECOVERY Professional", para que no se ejecute el programa de inmediato ya que se procederá a ser activado, se da click en "Finish". (Como lo muestra la imagen 9).



Imagen 9 (Completing the FILERECOVERY Professional Setup Wizard)

Ahora se procederá a activar el programa (Solo para fines académicos)

1. Se ingresa a la unidad de CD, luego a la carpeta programas, después a la carpeta recuperadores, luego a la carpeta FILERECOVERY Professional y luego a la carpeta llamada Crack. (Como se muestra en la imagen 10).

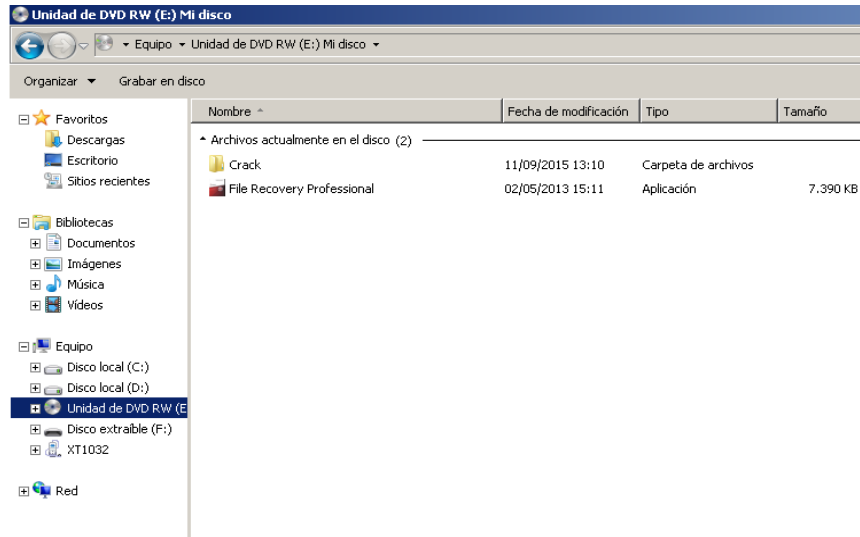


Imagen 10

2. Se seleccionan los 2 archivos llamados “frc” y “frc64”, luego click derecho sobre los archivos y luego click en copiar. (Como se muestra en la imagen 11).

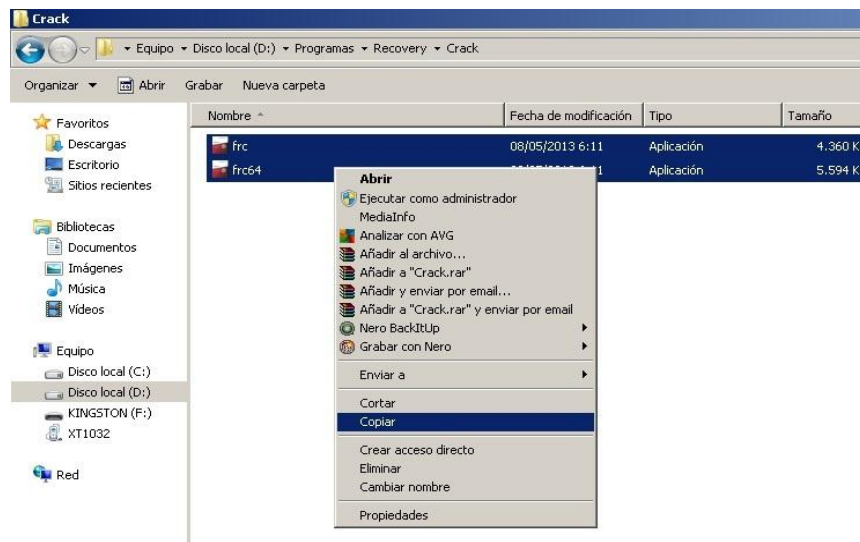


Imagen 11

3. Se da click en el menú inicio, luego click en equipo. (Como se muestra en la imagen 12).



Imagen 12

4. Se da click en Disco Local (C). Ya que en esa ubicación se encuentra instalado el programa. (Como se muestra en la imagen 13).

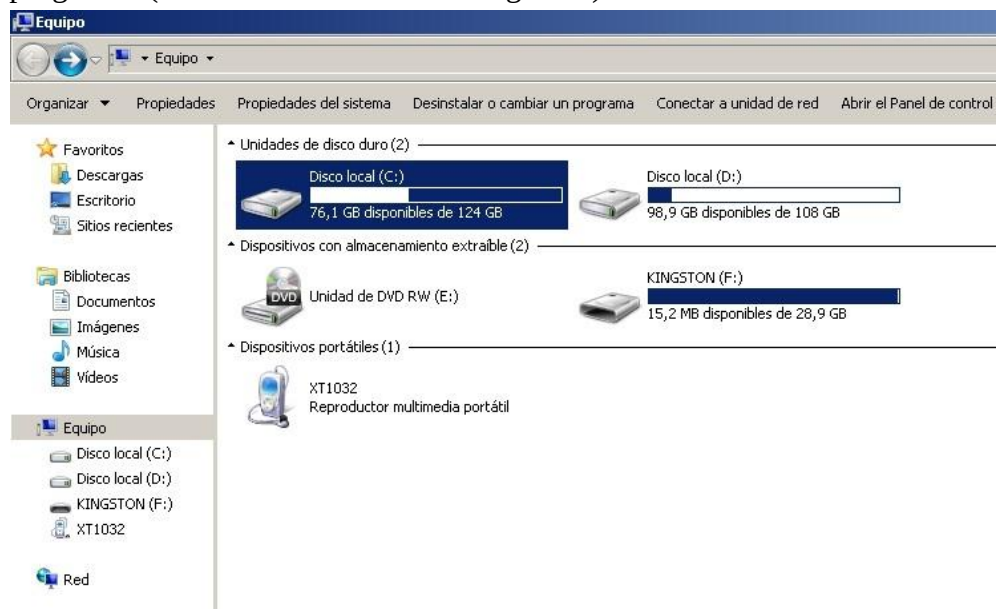


Imagen 13

5. Se localiza la carpeta “Archivos de programa y se da click. (Como se muestra en la imagen 14).

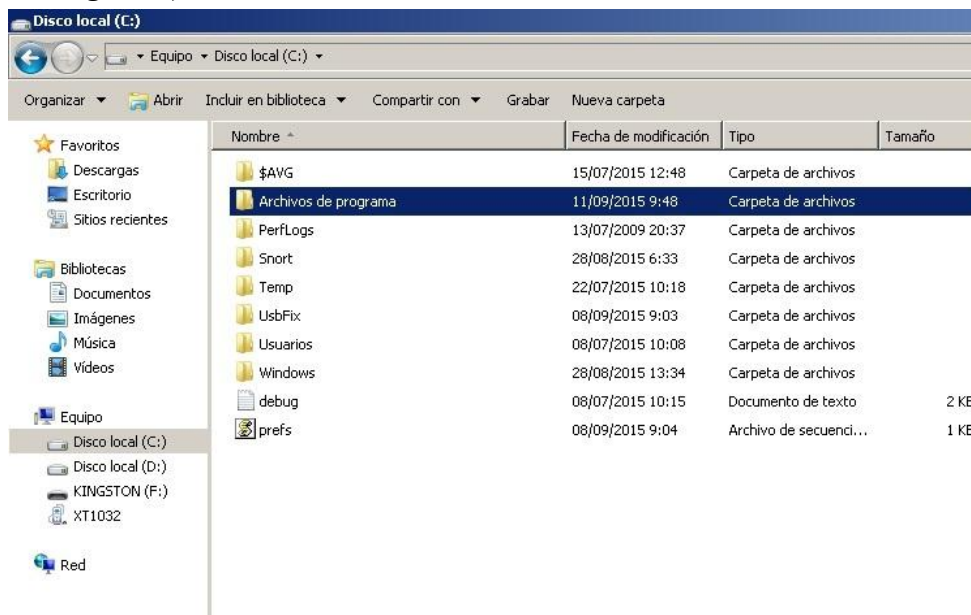


Imagen 14

6. Se localiza la carpeta con el nombre “FILERECOVERY 2013 Professional y se da click para poder ingresar. (Como se muestra en la imagen 15).

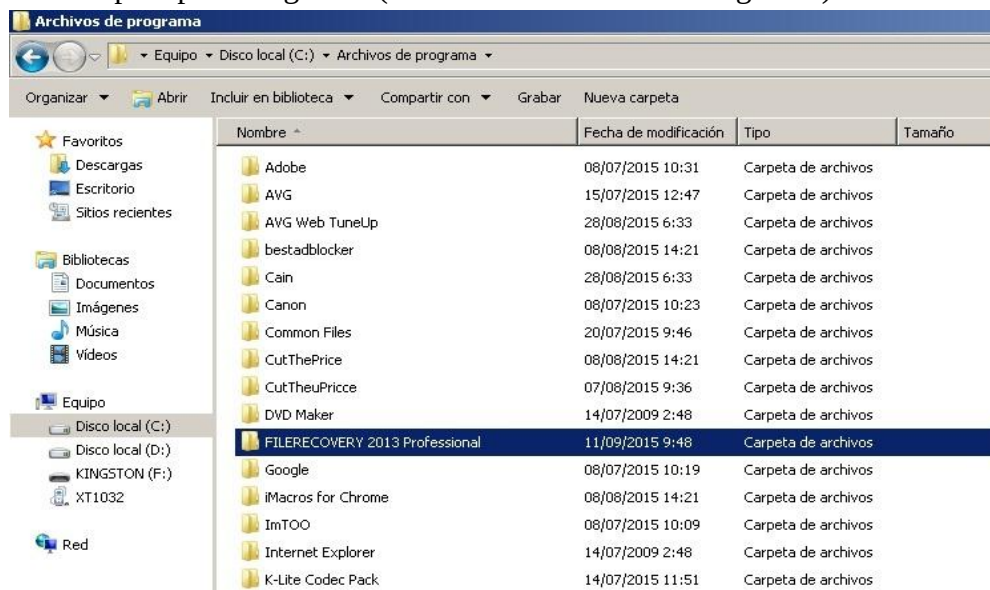


Imagen 15

7. Una vez dentro de la carpeta se hace el procedimiento de pegar los archivos que anteriormente se habían copiado, click derecho en el área vacía o en blanco, al aparecer el menú contextual seleccionar la opción pegar, los archivos serán copiados en esta carpeta. (Como se muestra en la imagen 16).

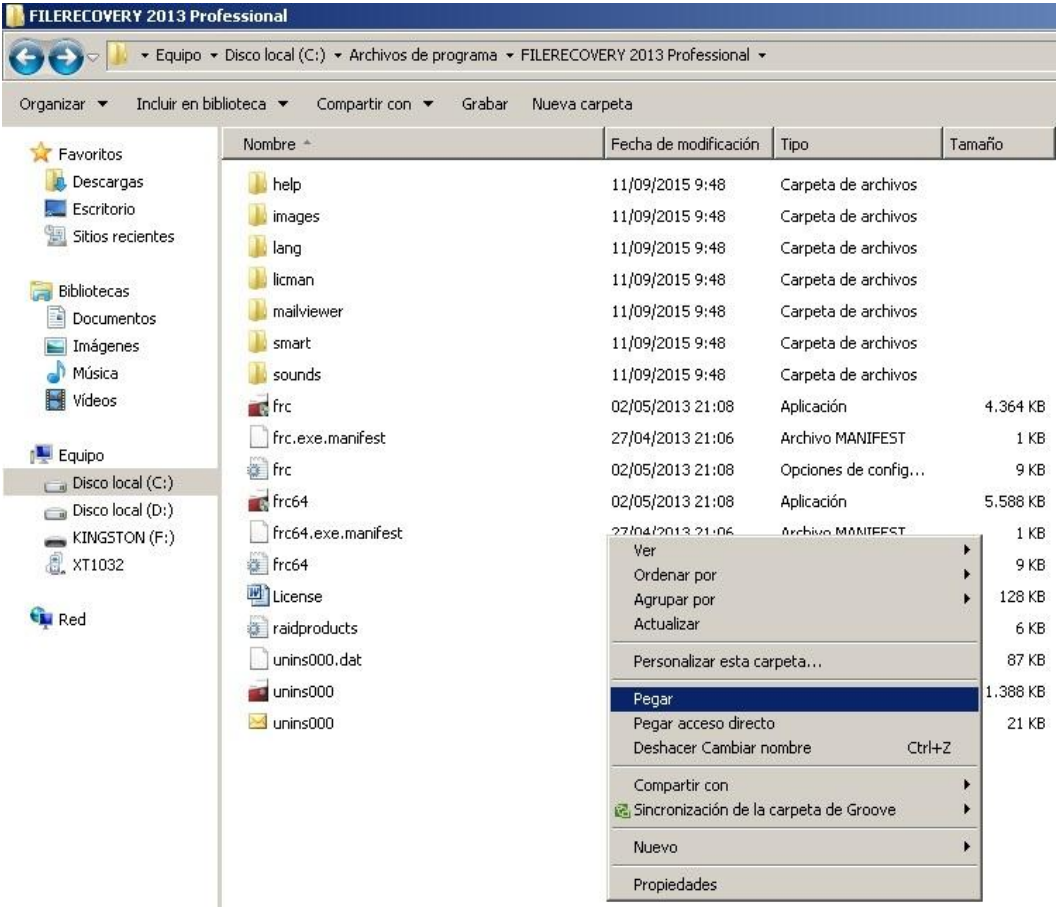


Imagen 16

8. A continuación saldrá una ventana donde dice que el archivo que se intenta copiar ya existe en la carpeta de destino, se marca la casilla de abajo que dice “Realizar esta acción para los siguientes 1 conflictos” y se da click en “copiar y reemplazar”. (Como se muestra en la imagen 17)

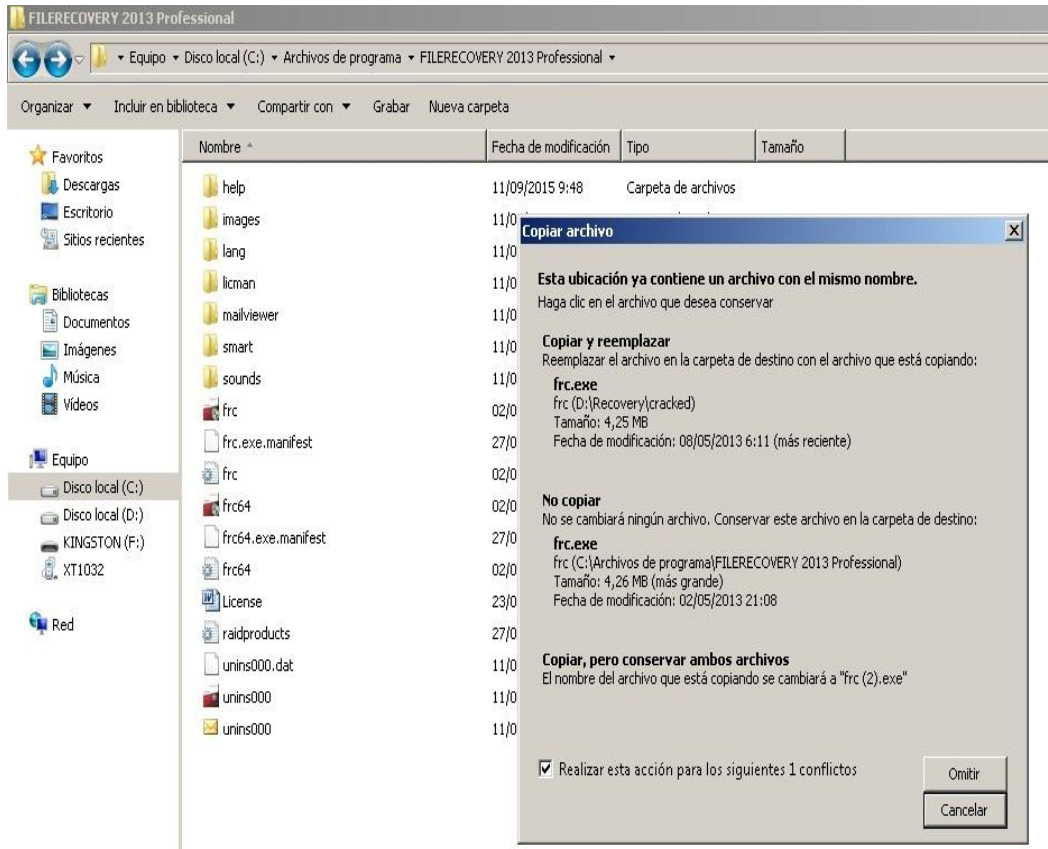


Imagen 17

9. En esta ventana solicita permisos de administrador para poder seguir con el copiado se da click en continuar. (Como se muestra en la imagen 18)

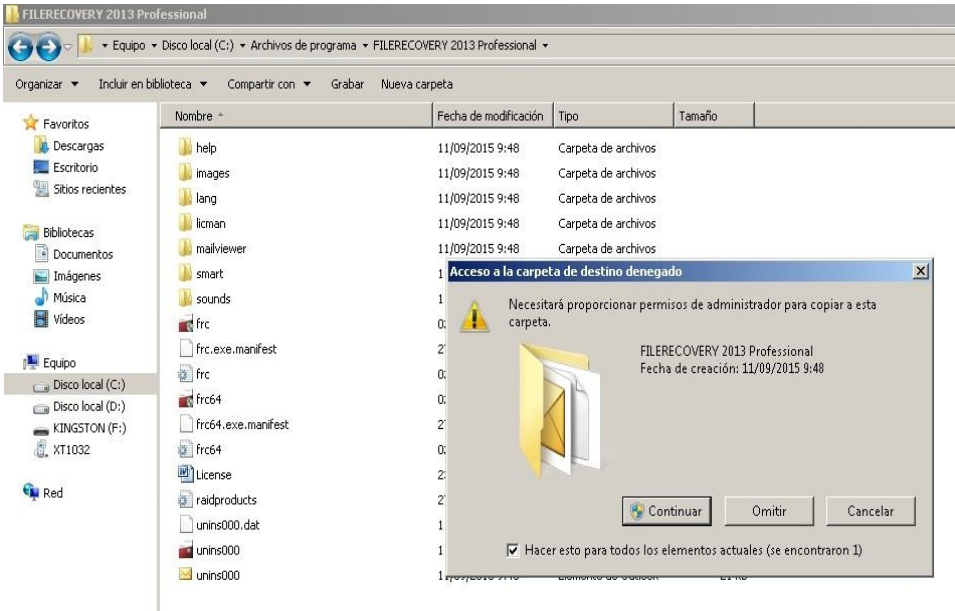


Imagen 18

10. Se espera a que finalice el copiado de archivos y ya estará el programa listo para ser utilizado. (Como se muestra en la imagen 19)

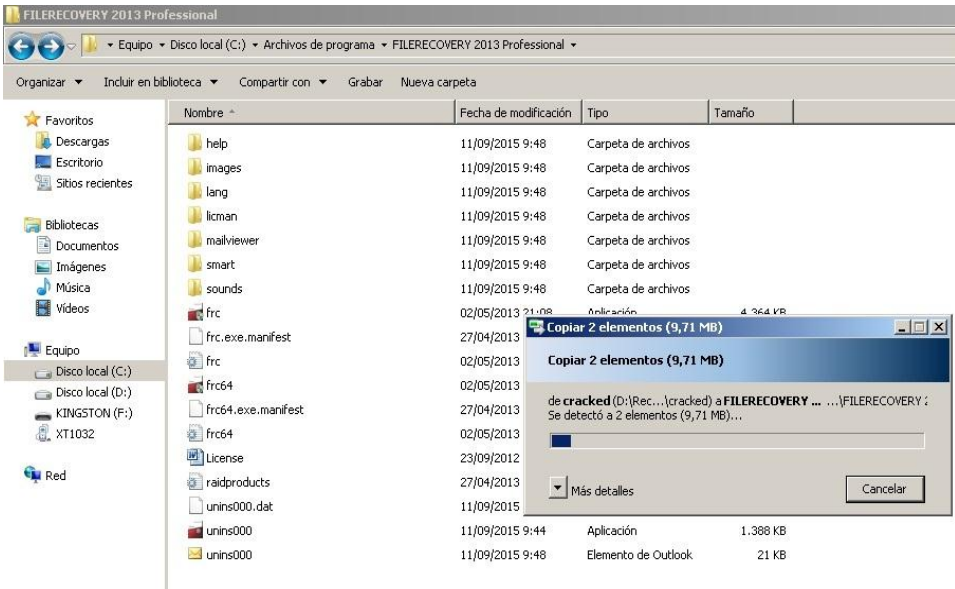


Imagen 19

Pasos para recuperar una o varias imágenes

1. Primero se eliminaran las imágenes de la memoria USB, para posteriormente recuperarlas. (Como se muestra en la imagen 20)

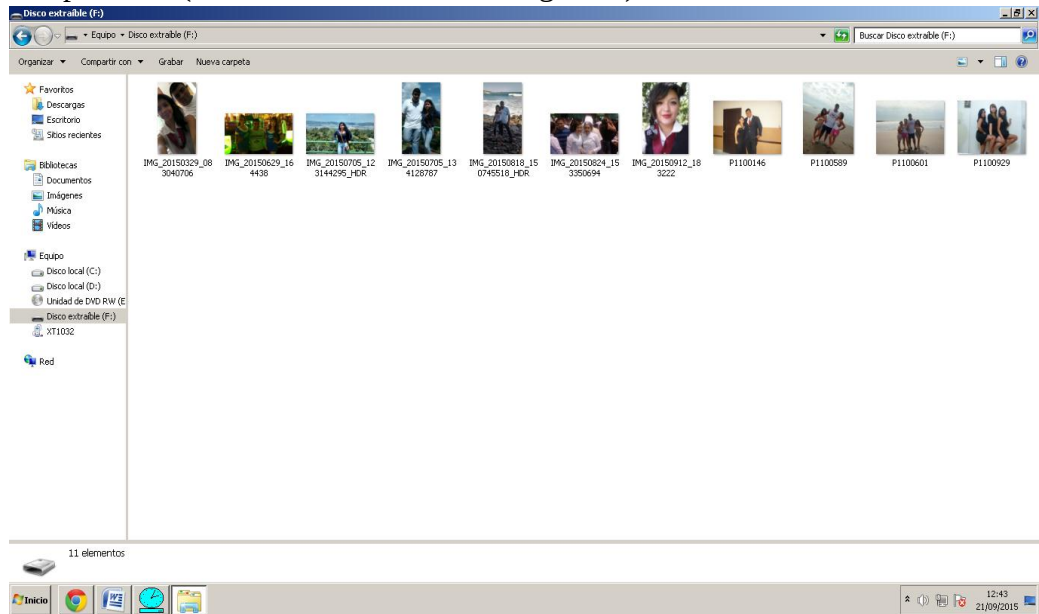


Imagen 20

2. Como se puede observar las imágenes ya están eliminadas, ahora se procederá a su recuperación. (Como lo muestra la imagen 21).

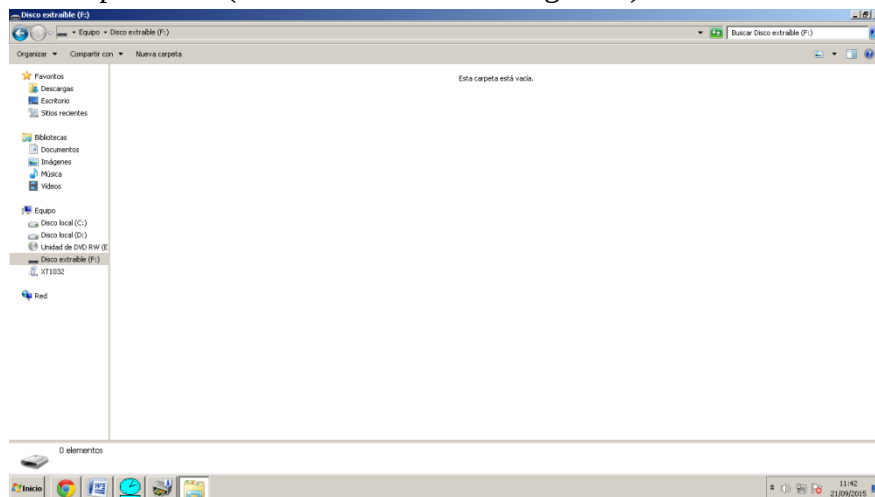


Imagen 21

3. Una vez instalado y activado se busca el acceso directo de FILERECOVERY Professional en el escritorio y se le da click. (Como lo muestra la imagen 22).

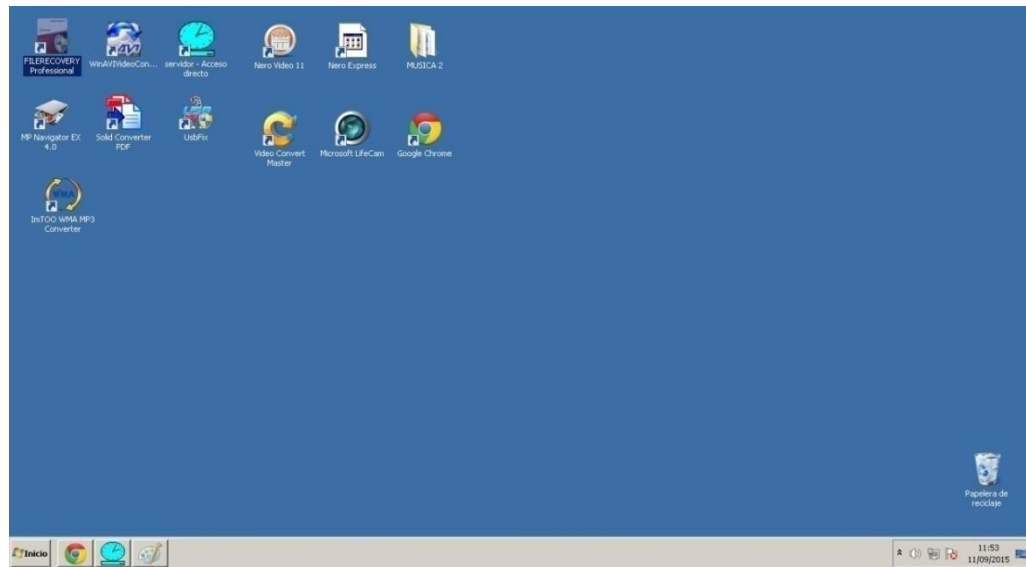


Imagen22

4. Por ser la primera vez que se instala aparecerá un cuadro en donde se elegirá el idioma del programa, se selecciona el idioma español y luego click en “ok” (Como lo muestra la imagen 23).

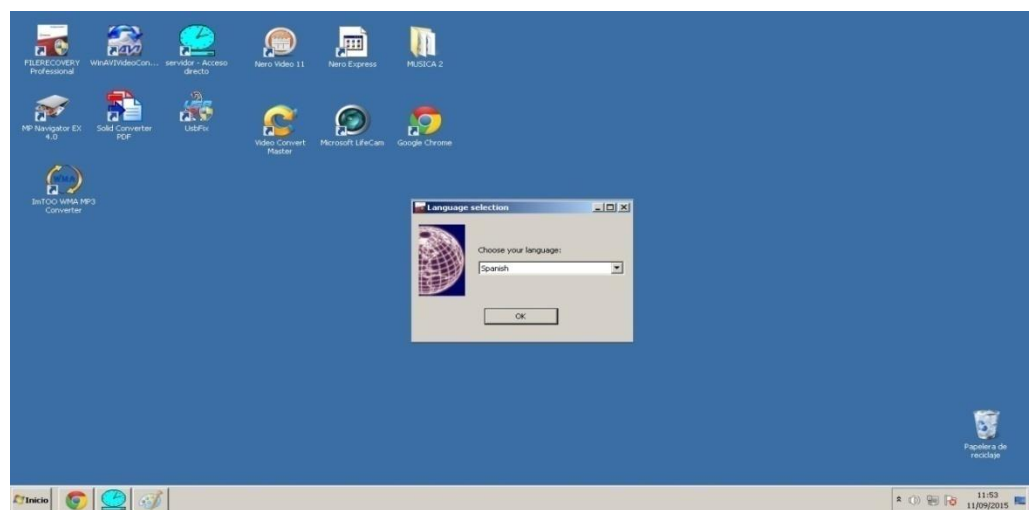


Imagen 23 (Choose your language)

5. A continuación se muestra el asistente de ayuda, se da click en continuar. (Como lo muestra la imagen 24).



Imagen 24 (FILERECOVERY 2013 Professional)

6. En esta parte se elige el dispositivo que se va a examinar, en este caso se selecciona "Dispositivo de memoria". (Como lo muestra la imagen 25).



Imagen 25 (Elija el tipo de memoria)

7. En esta sección se selecciona la unidad que se analizará. (Como lo muestra la imagen 26).

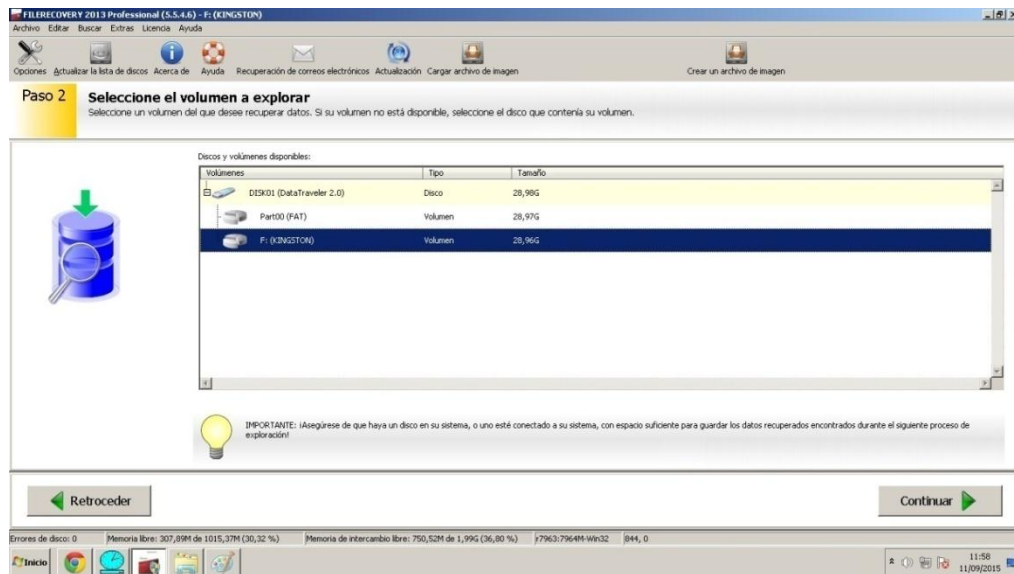


Imagen 26 (Seleccione el volumen a explorar)

8. Luego saldrá la siguiente ventana se seleccionará la opción recuperación de un archivo. (Como lo muestra la imagen 27).



Imagen 27 (Seleccione escenario de recuperación)

9. En esta parte muestra las opciones seleccionadas si todo está en orden se da click en "Continuar". (Como lo muestra la imagen 28).

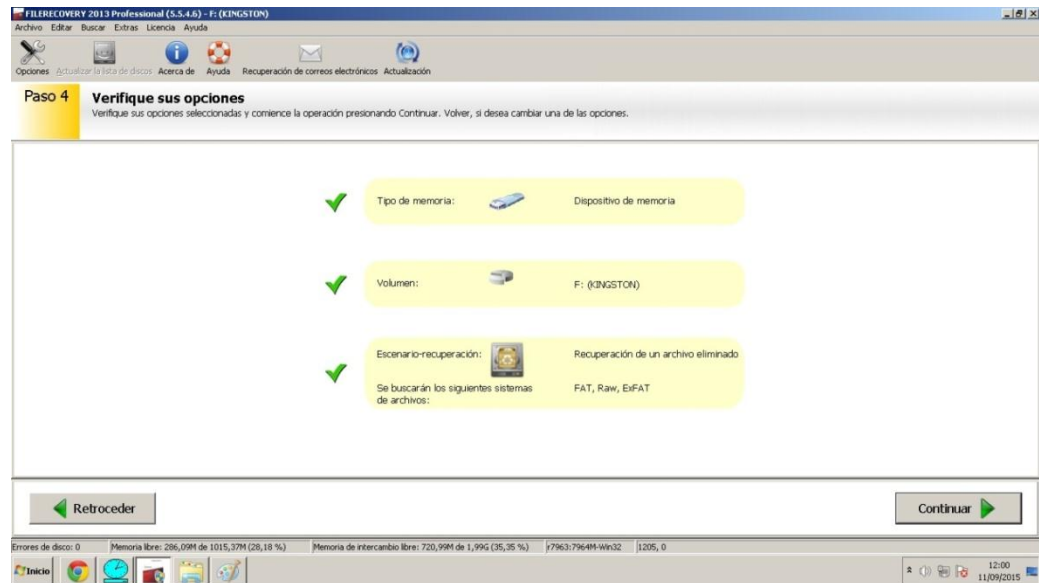


Imagen 28 (Verifique sus opciones)

10. A continuación empezará el asistente de exploración, tomará varios minutos dependiendo el tamaño de la unidad analizada. (Como lo muestra la imagen 29).

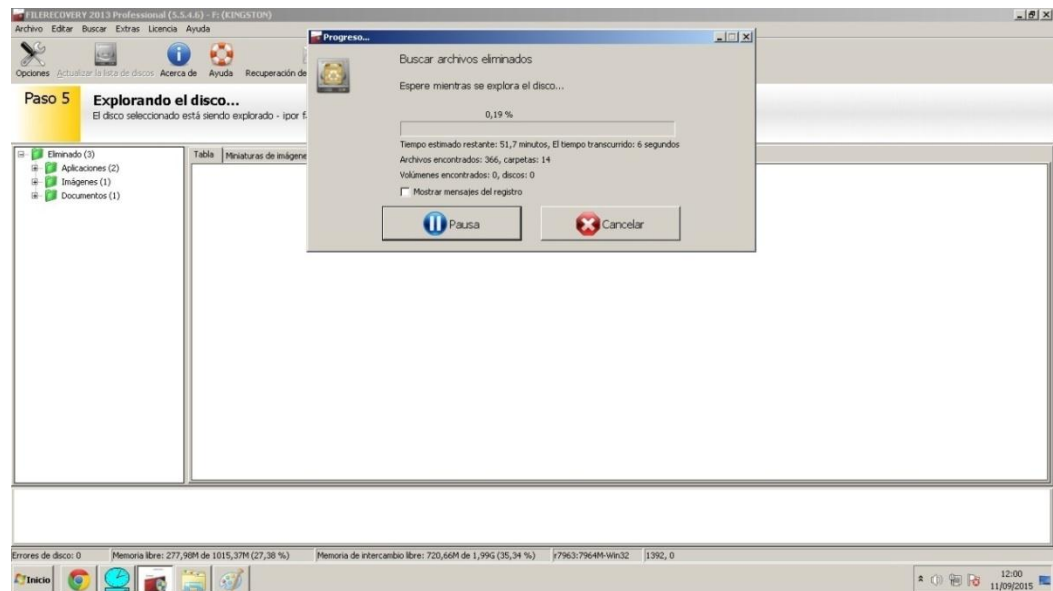


Imagen 29 (Buscar archivos eliminados)

11. Una vez finalizada la exploración mostrará el siguiente cuadro de información, se da click en "ok". (Como lo muestra la imagen 30).

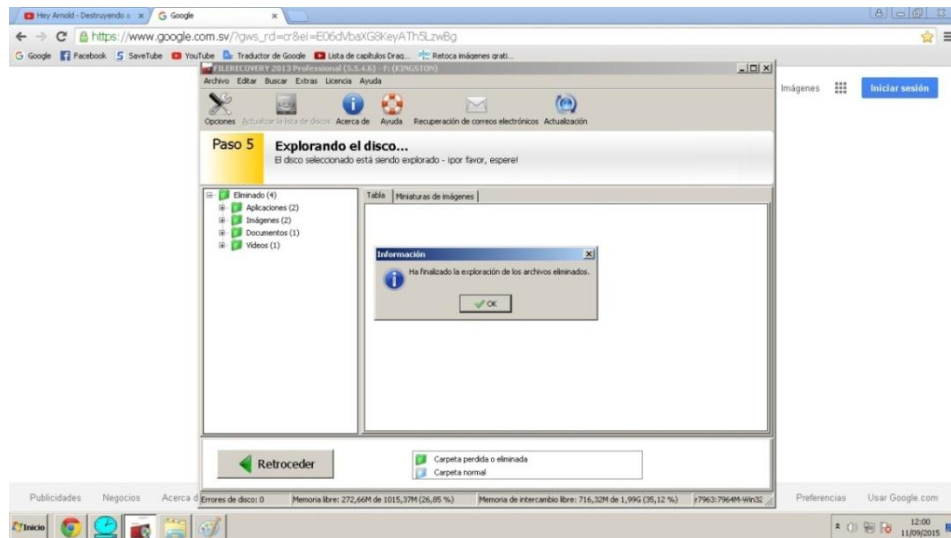


Imagen 30 (Información)

12. En esta pantalla se selecciona y se da click en la carpeta "Imágenes" (Como lo muestra la imagen 31).

Estas carpetas

Son creadas por el

Programa, ahí se

Almacenan los

Archivos

Recuperados.

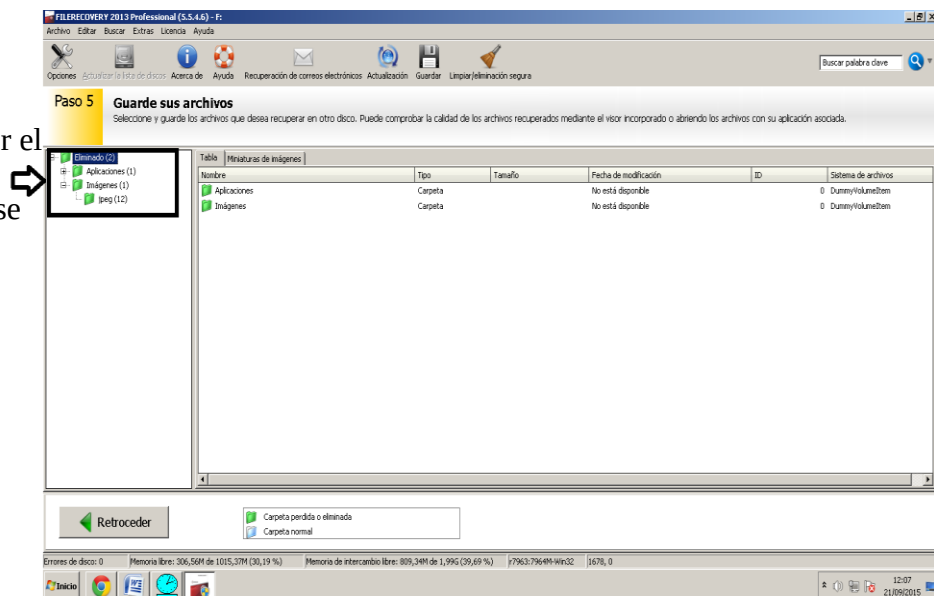


Imagen 31 (Guarde sus archivos)

13. En esta sección se da click a la carpeta llamada "JPEG" ya que lo que se ha recuperado son archivos de imagen. (Como lo muestra la imagen 32).

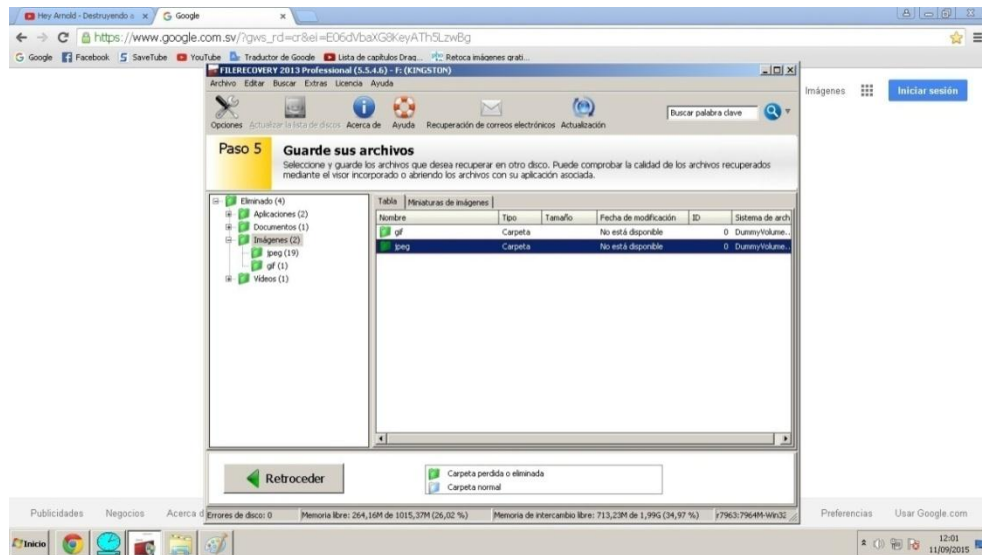


Imagen 32

14. A continuación mostraré la tabla donde se muestra el listado de los archivos recuperados. (Como lo muestra la imagen 33).

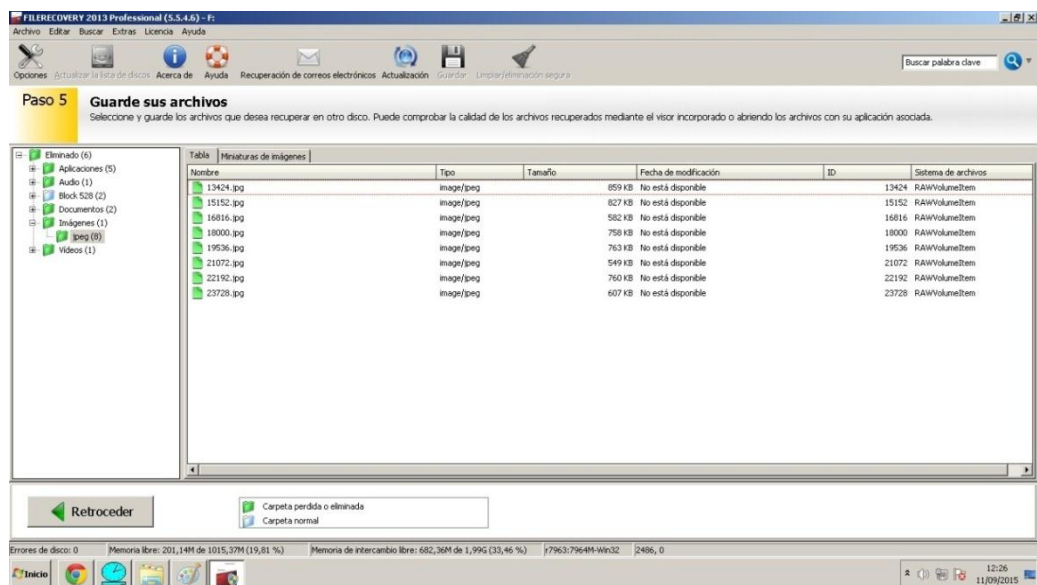


Imagen 33

15. Para poder observar las imágenes recuperadas se da click en la ficha "Miniaturas de imágenes" que se encuentra al costado derecho de la ficha "Tabla". (Como lo muestra la imagen 34).

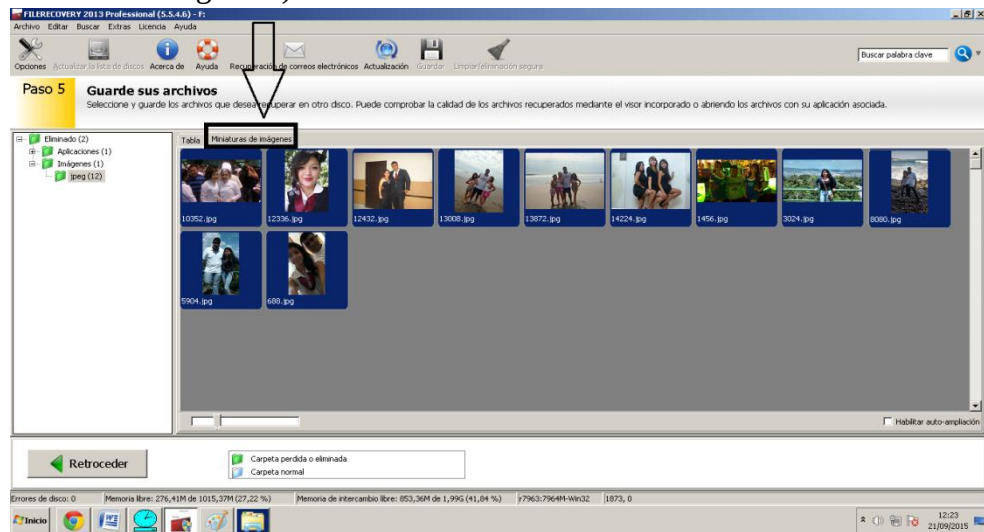


Imagen34

16. Se selecciona el archivo o archivos que se quieran recuperar, una vez seleccionados se da click derecho sobre un archivo y seguidamente se da click en "Guardar como". (Como lo muestra la imagen 35).

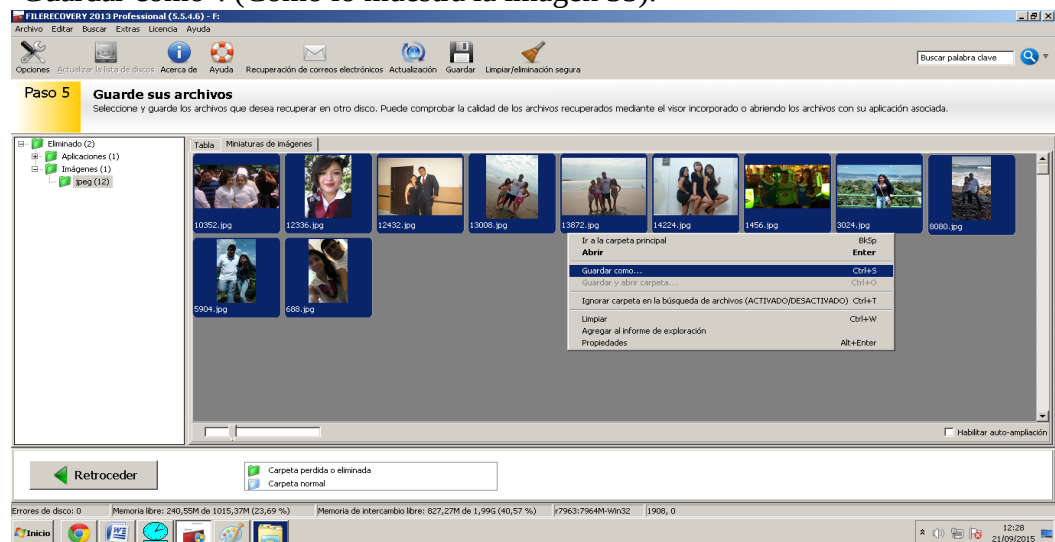


Imagen 35

17. En esta ventana se elige el lugar de destino para que sean guardadas las imágenes recuperadas, en este caso se seleccionará el "Escritorio de Windows". (Como lo muestra la imagen 36).

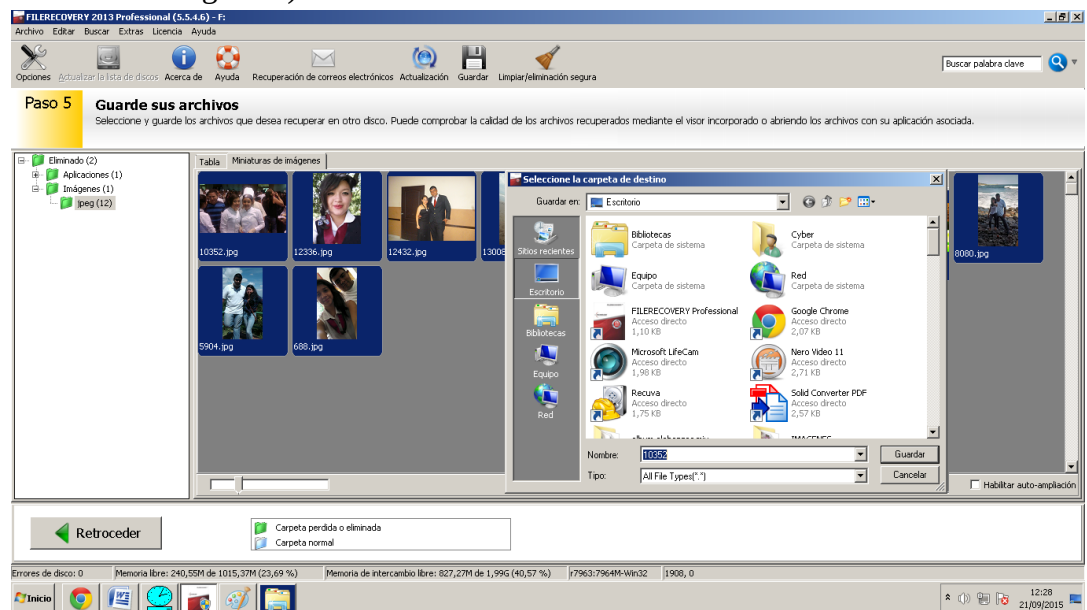


Imagen 36

18. Una vez finalice el proceso de guardado saldrá el siguiente mensaje, se da click en "Aceptar". (Como lo muestra la imagen 37).

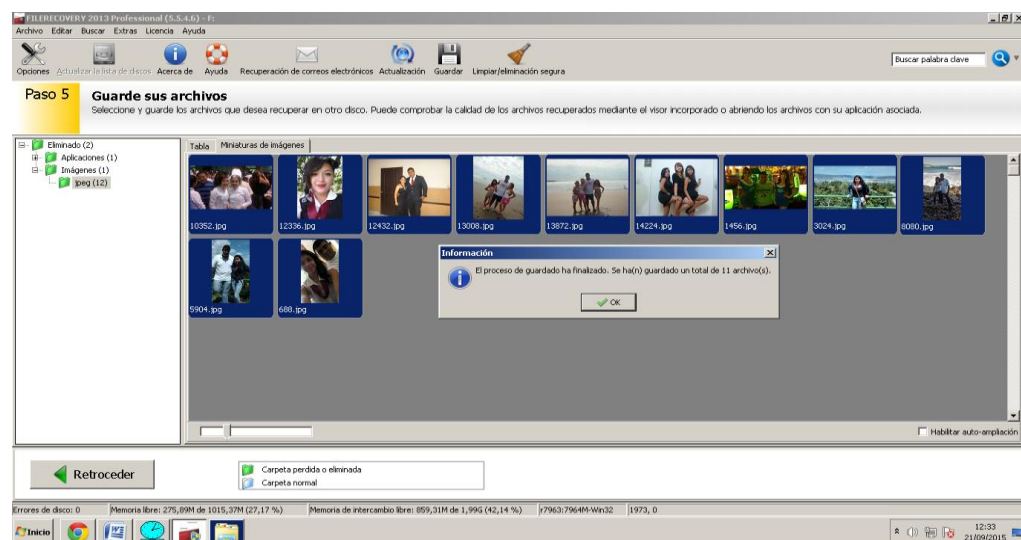


Imagen 37 (Información)

19. Con eso finaliza el proceso de recuperación de archivos, ahora se verificaran en el lugar destinado donde fueron guardados. (Como lo muestra la imagen 38).

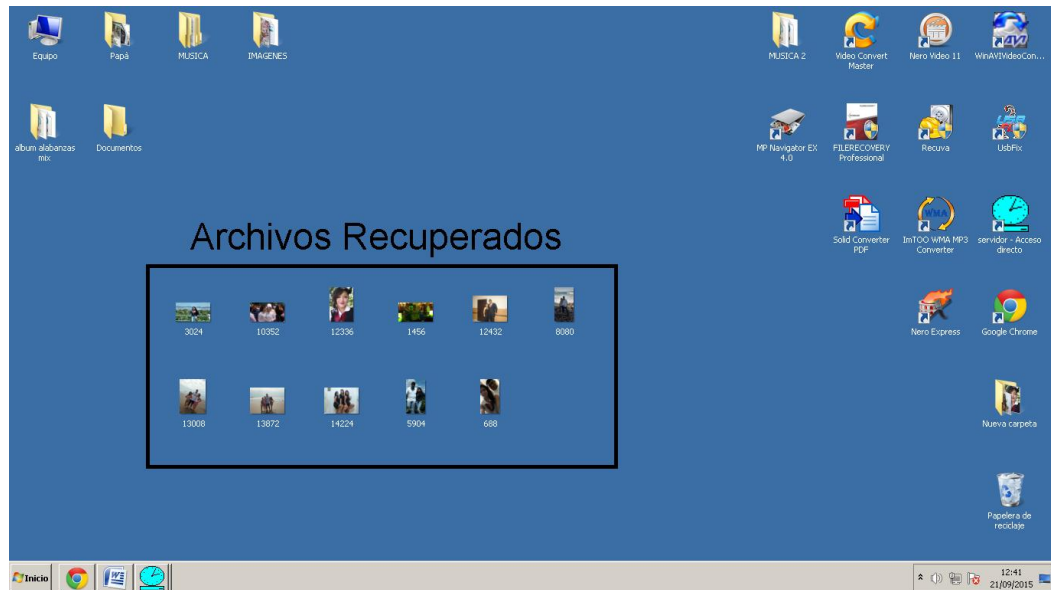


Imagen 38

2.2.2. Manual de instalación y uso de Recuva

Nota: Para el uso de este programa se debe estar en una cuenta de administrador, este programa es compatible desde Windows XP hasta Windows 8. En esta ocasión se realizará en sistema operativo Windows 7.

1. Una vez abierto el CD de herramientas, se da click en programas, luego en recuperación de archivos, y se selecciona Recuva. (Como se muestra en la imagen 39).

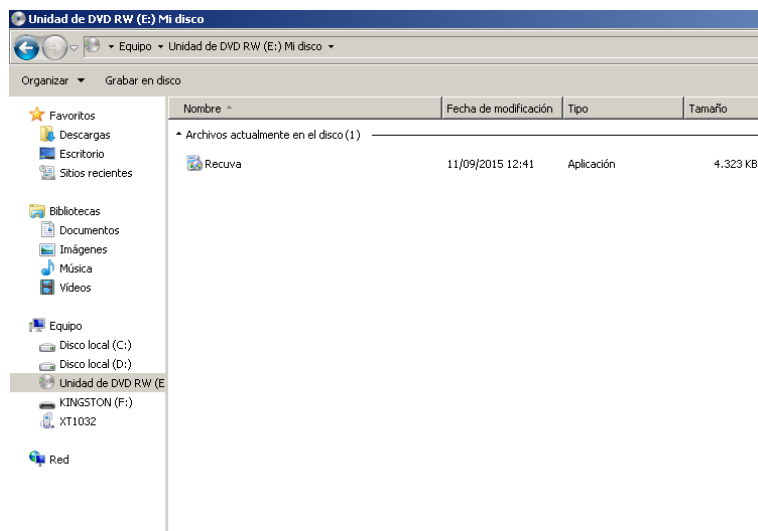


Imagen 39

2. Se presentará la siguiente ventana donde se seleccionará el idioma español y se da click en “Next”. (Como se muestra en la imagen 40).

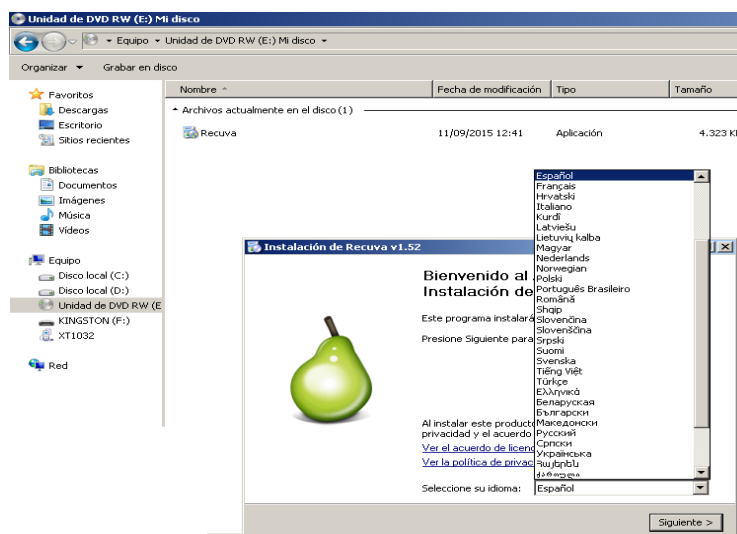


Imagen 40 (Bienvenidos al asistente de instalación de Recuva)

3. Luego saldrá la ventana de opciones de instalación, se seleccionan las opciones que se crean convenientes, y luego se da click en "Siguiente". (Como se muestra en la imagen 41).

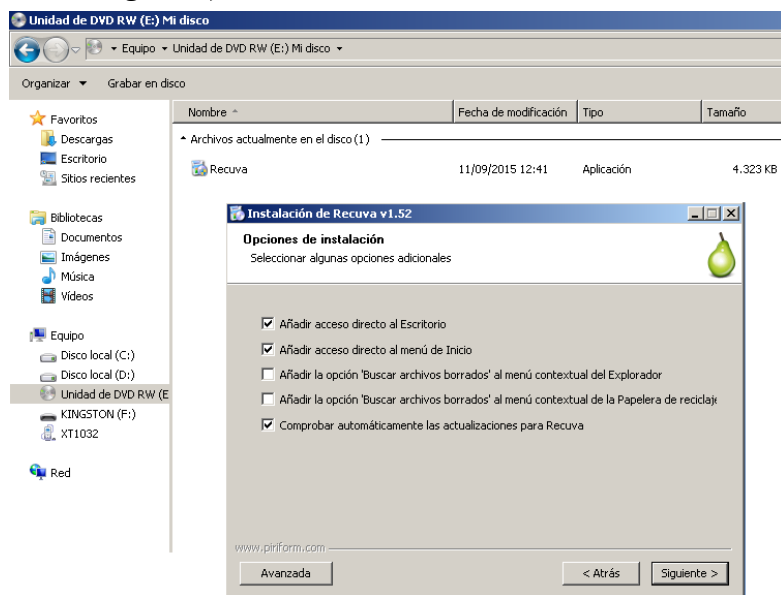


Imagen 41 (Opciones de instalación)

4. Seguidamente saldrá una aplicación extra si no se desea instalar se marca la casilla "No thanks" y se da click en siguiente. (Como se muestra en la imagen 42).

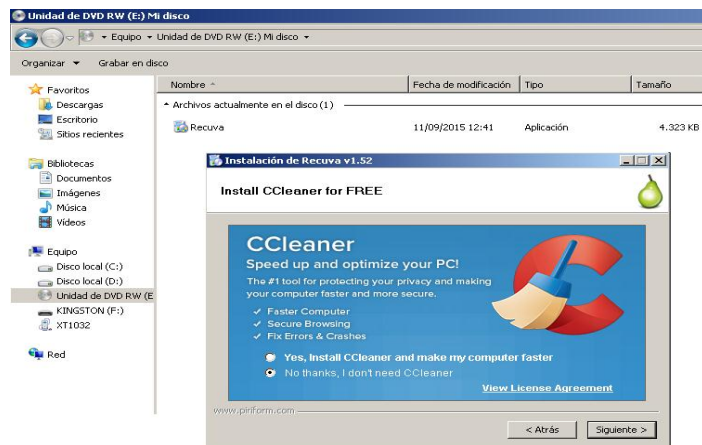


Imagen 42 (Install CCleaner for FREE)

5. Se espera a que se complete la instalación. (Como se muestra en la imagen 43)

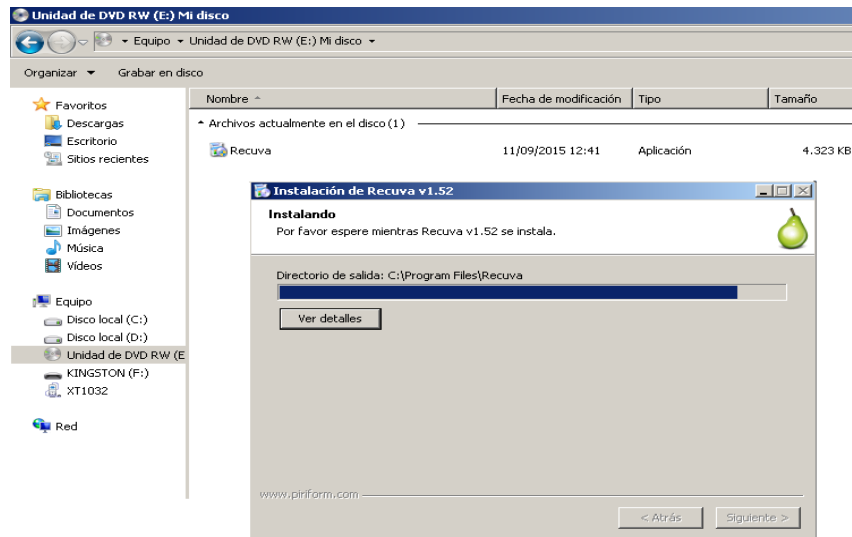


Imagen 43 (Instalando)

6. Una vez finalizada la instalación, se marca la casilla "Ejecutar Recuva" y se da click en "Terminar". (Como se muestra en la imagen 44)

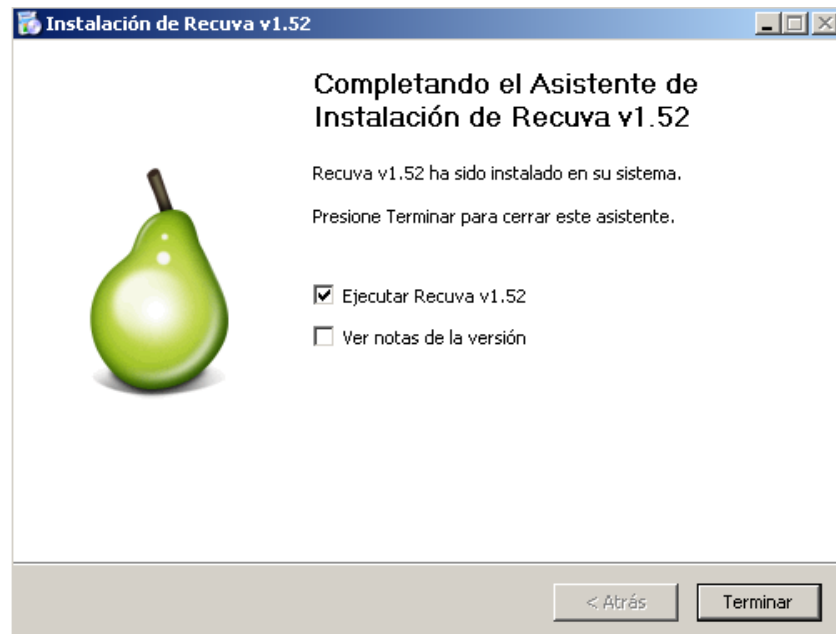


Imagen 44 (Completando el asistente de instalación de Recuva v1. 52)

Pasos para recuperar una o varias imágenes

1. Primero se eliminaran las imágenes de la memoria USB, para posteriormente recuperarlas. (Como se muestra en la imagen 45).

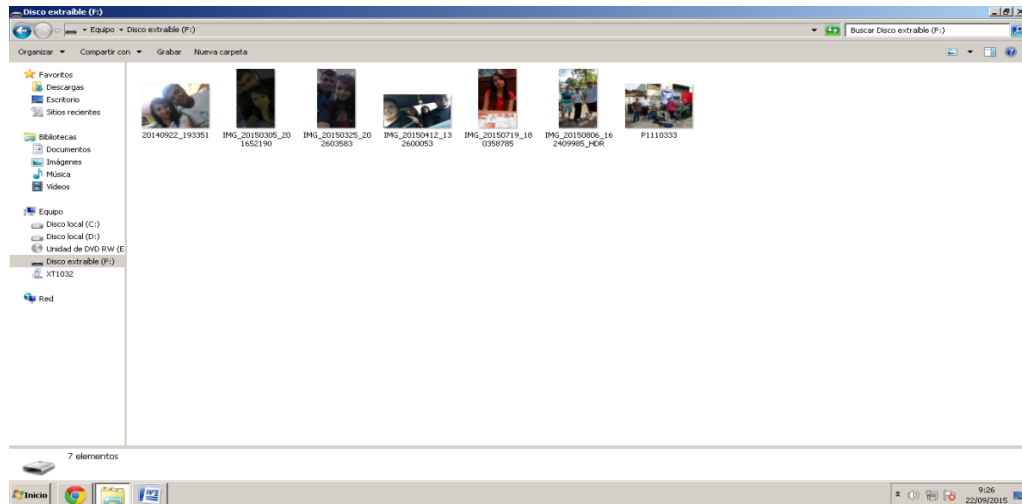


Imagen 45

2. Como se puede observar las imágenes ya están eliminadas, ahora se procederá a su recuperación. (Como lo muestra la imagen 46).

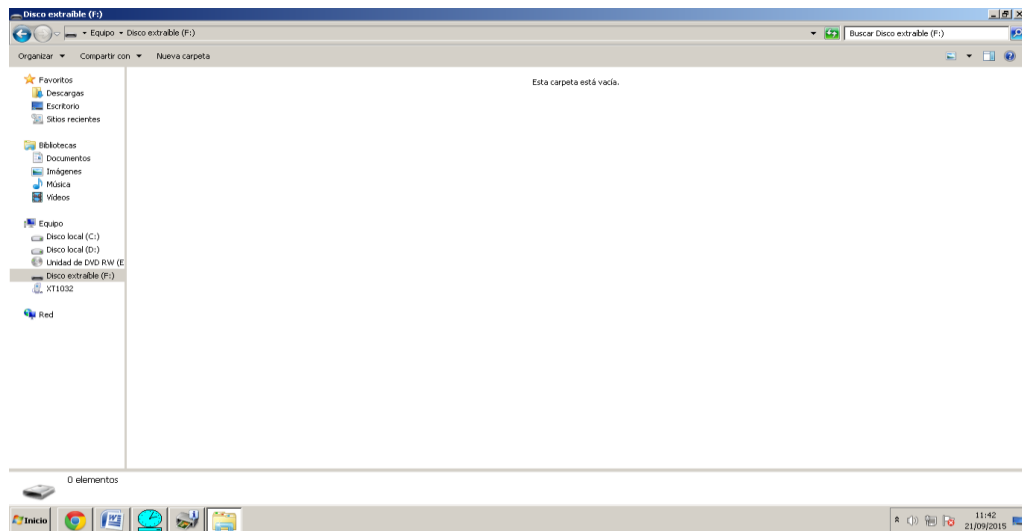


Imagen 46

3. Seguidamente aparecerá el Asistente de Recuva, se da click en "Siguiente".

(Como lo muestra la imagen 47).



Imagen 47 (Bienvenido al Asistente de Recuva)

4. En esta sección se elegirá el tipo de archivo a recuperar, en este caso se seleccionará imágenes, luego click en "siguiente". (Como lo muestra la imagen 48).



Imagen 48 (Tipo de archivo)

5. Aquí se seleccionará la ubicación en la que se realizará la exploración, se selecciona "En una unidad específica" luego click en "Buscar". (Como lo muestra la imagen 49).

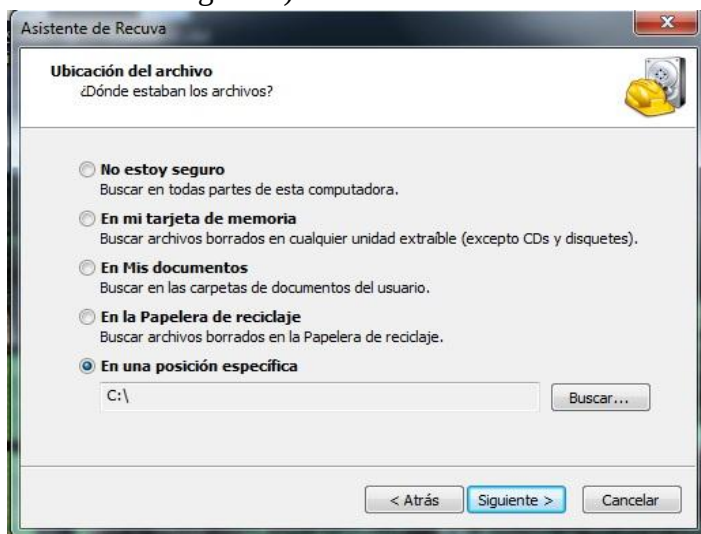


Imagen 49 (Ubicación de archivo)

6. Aparecerá la siguiente venta en la cual se elegirá la ubicación en la cual se realizará la exploración, en este caso será "Disco extraíble (M:)". (Como lo muestra la imagen 50).

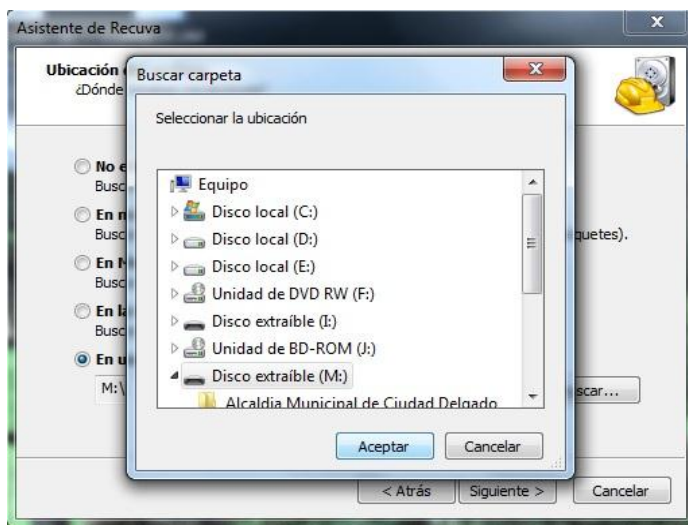


Imagen 50 (Buscar carpeta)

7. En esta ventana aparecerá un pequeño agradecimiento y un pequeño mensaje informativo, si se desea un análisis profundo se marcará la casilla "Activar escaneo profundo", este análisis llevará un poco más de tiempo dependiendo del tamaño de la unidad, luego se da click en "Iniciar". (Como lo muestra la imagen 51).



Imagen 51 (Gracias, Recuva está ahora listo para buscar sus archivos)

8. Se espera a que finalice la exploración de la unidad, esta acción puede durar unos minutos dependiendo del tamaño de la unidad. (Como lo muestra la imagen 52).

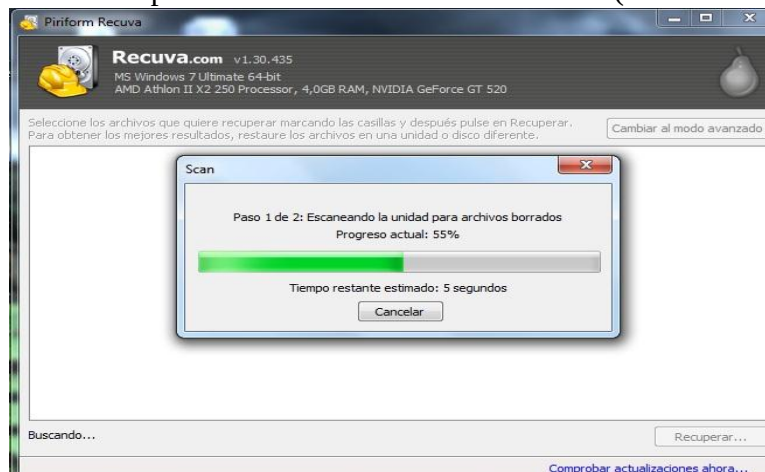


Imagen 52 (Scan)

9. Una vez finalizada la exploración mostrará las imágenes recuperadas, se selecciona la imagen o imágenes que se desean recuperar y luego se da click en "Recuperar". (Como lo muestra la imagen 53).



Imagen 53

10. Luego se elegirá el lugar de destino de las imágenes, en este caso se seleccionará el escritorio de Windows, seguidamente se da click en "Aceptar". (Como lo muestra la imagen 54).

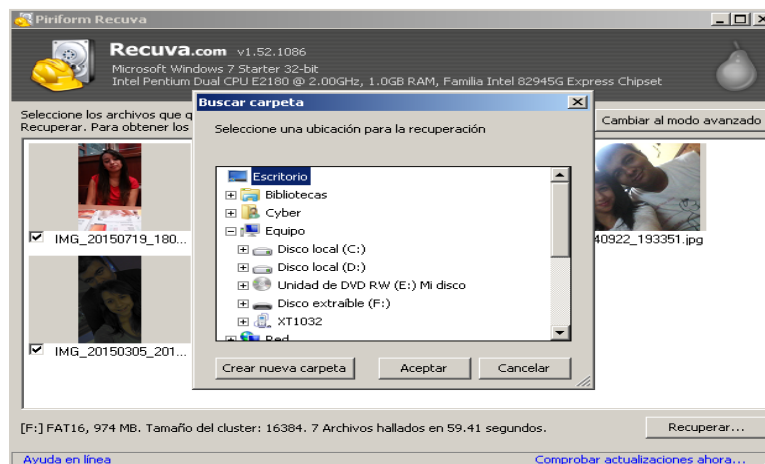


Imagen 54 (Buscar carpeta)

11. Se espera a que se realice el guardado de los archivos y aparecerá el siguiente cuadro de mensaje donde indica que se realizó la operación con éxito, se da click en aceptar. (Como lo muestra la imagen 55).

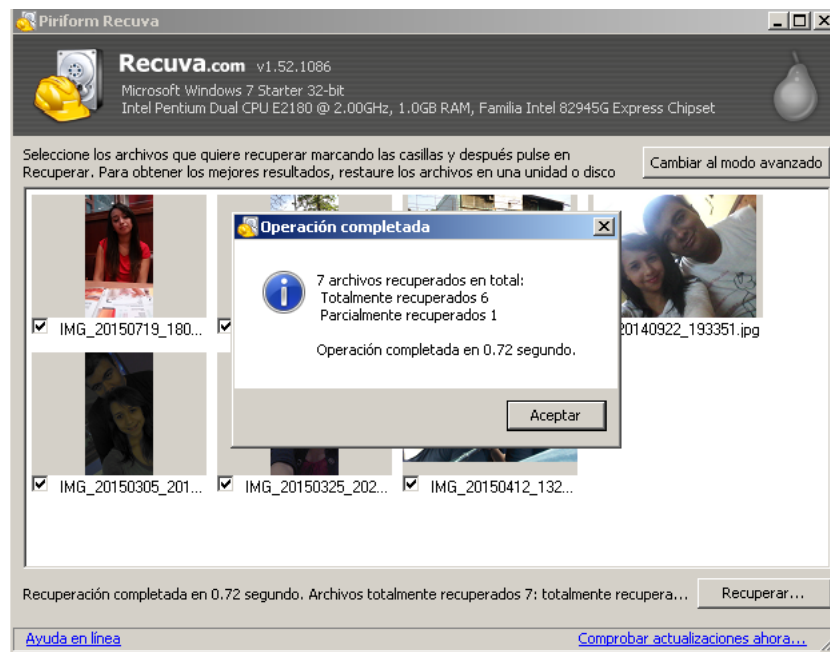


Imagen 55 (Operación completada)

12. Finalmente se comprueban los archivos recuperados en el lugar de destino seleccionado anteriormente. (Como se muestra en la imagen 56).



Imagen 56

2.2.3. Manual de Instalación y uso de TweakNowRegCleaner.

1. Una vez abierto el CD de herramientas, se da click en programas, luego en análisis y registro de Windows, y luego click en RegCleaner. (Ver imagen 57).

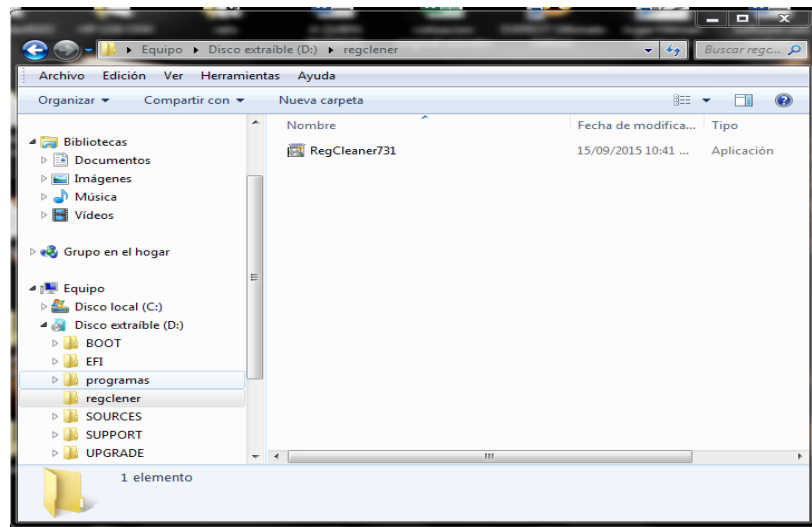


Imagen 57

2. Se presentara la ventana de bienvenida y a continuación se da click en "Next".
(Ver imagen 58).

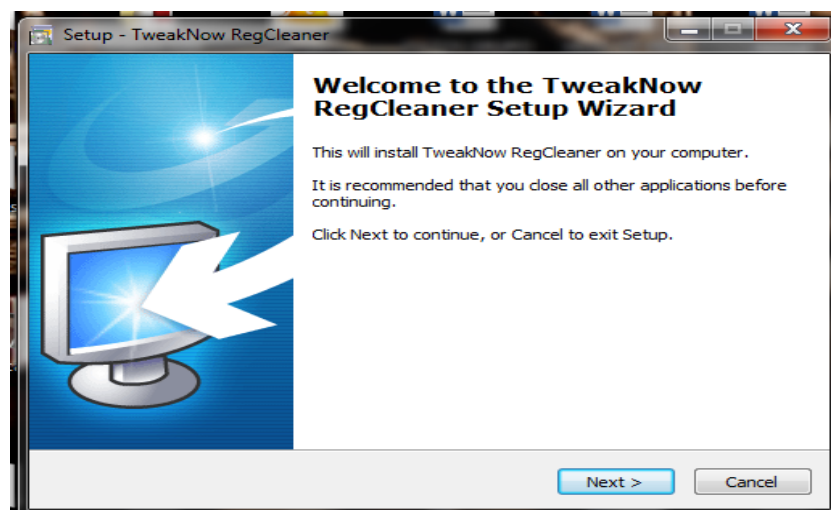


Imagen 58 (Welcome to the TweakNow RegCleaner Setup Wizard)

3. Seguidamente aparecerá el contrato de aceptación de términos, luego se marca la casilla de aceptación de términos y condiciones, seguidamente se da click en “Next”. (Ver imagen 59).

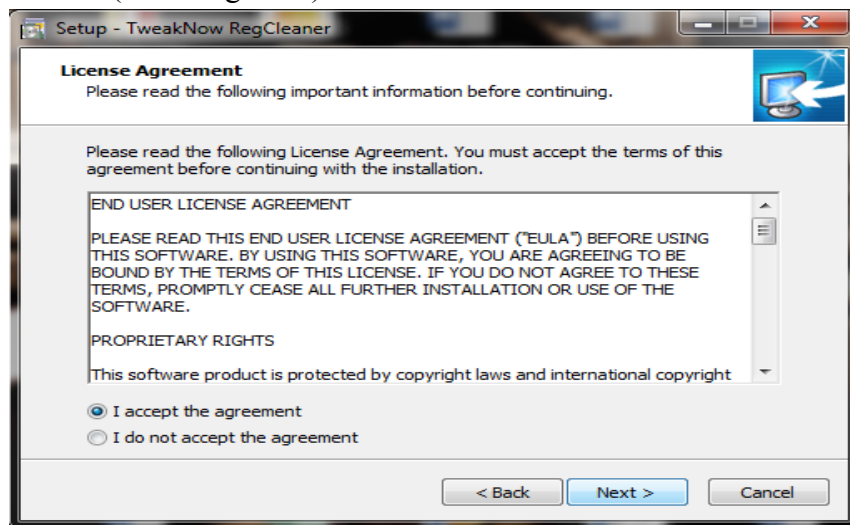


Imagen 59 (License Agreement)

4. En esta ventana se muestra la ruta de instalación del programa, en este caso se dejará la predeterminada por el programa, se da click en "Next". (Ver imagen 60).

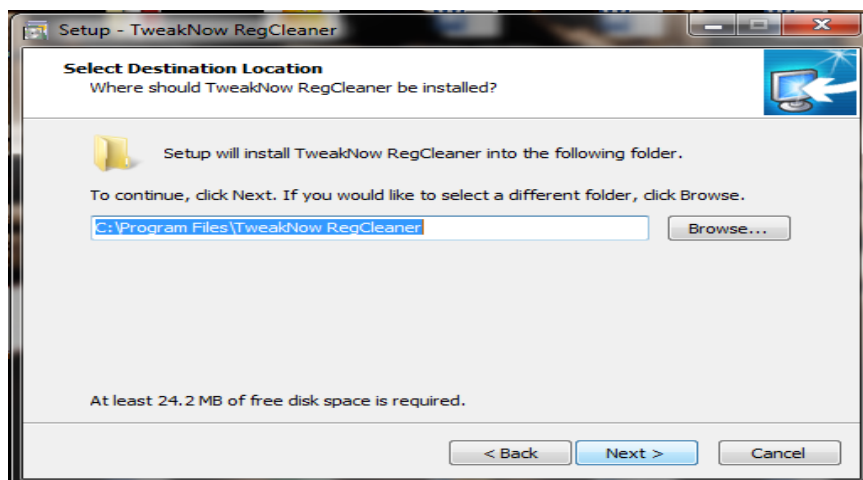


Imagen 60 (Select Destination Location)

5. Seguidamente saldrá la ventana donde indica que se seleccione el destino de los accesos directos en el menú inicio, se dejará la ruta indicada por el programa, se da click en "Next"(Ver imagen 61).

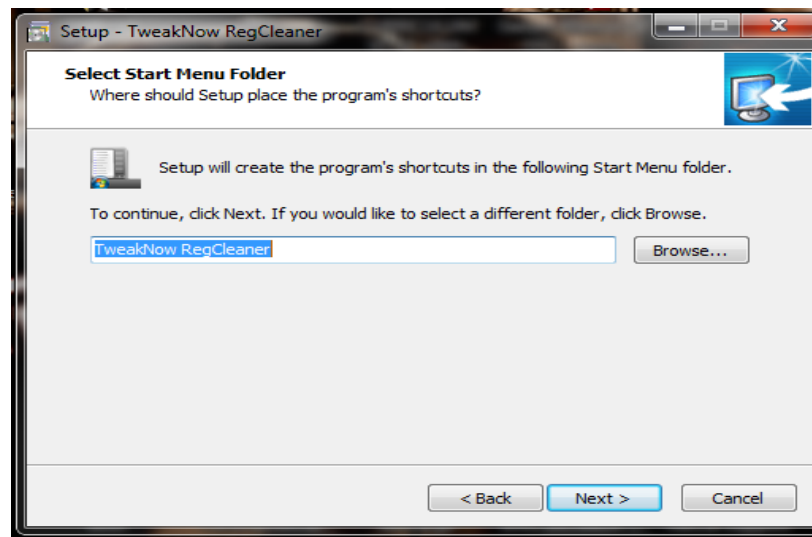


Imagen 61 (Select Start Menu Folder)

6. En este ventana indica si se desea crear un acceso directo en el escritorio, de ser así se marca la casilla y luego click en "Next". (Ver imagen 62).

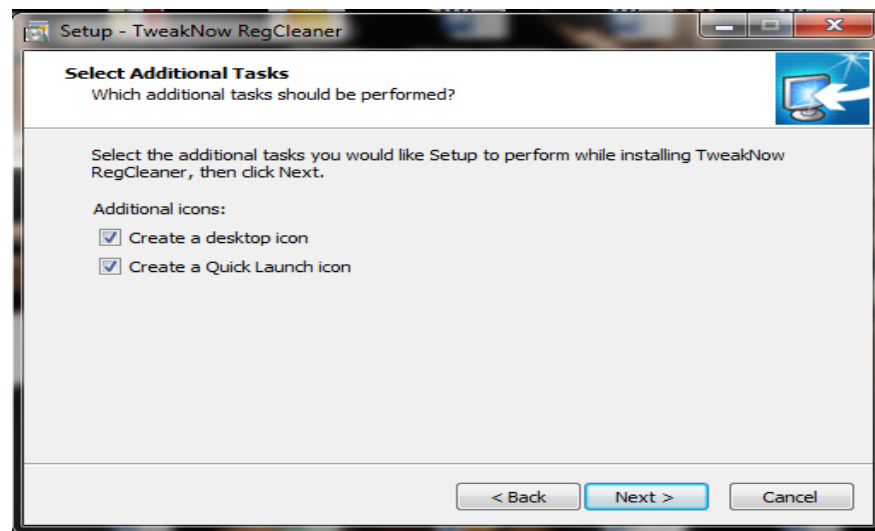


Imagen 62 (Select Additional Tasks)

7. En esta ventana se selecciona los componentes que se instalaran, en este caso se deja lo que el programa indica "Full installation", se da click en "Next" (Ver imagen 63).

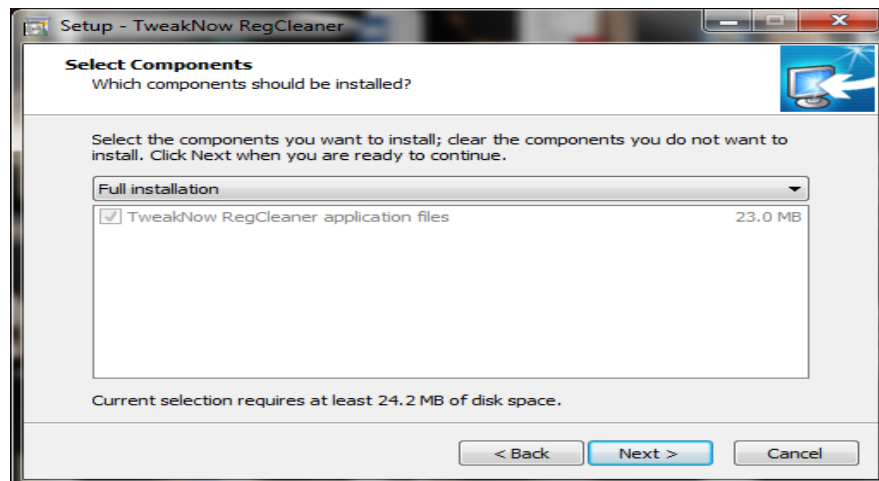


Imagen 63 (Select Components)

8. A continuación empezará la instalación del programa, este proceso puede durar varios minutos. (Ver imagen 64).

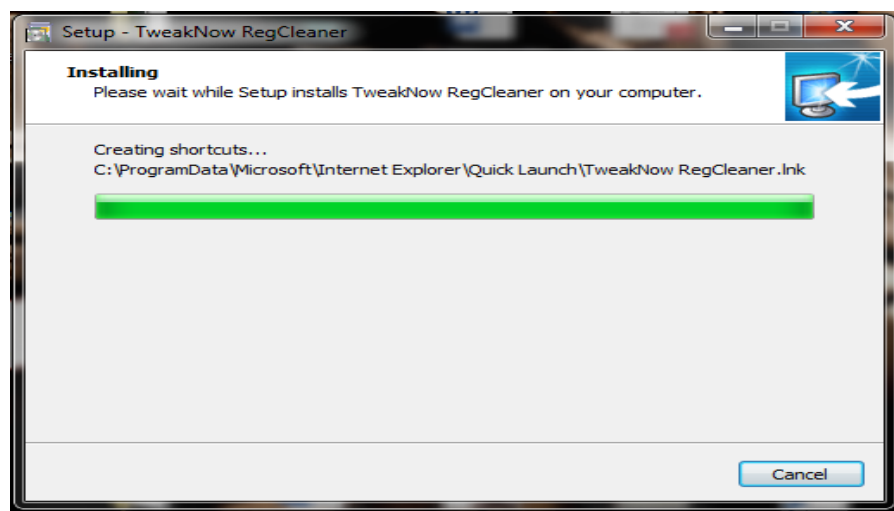


Imagen 64 (Installing)

9. En la siguiente ventana muestra que la instalación se realizó correctamente, se desmarca la casilla "VisitTweaknowRegCleanerWebsite" y se da click en "Finish". (Ver imagen 65).



Imagen 65 (Completing the TweakNowRegCleaner Setup Wizard)

Pasos para mantenimiento con RegCleaner

1. Seguidamente saldrá la pantalla principal del programa, en la barra de herramientas del programa se da click a la opción "Windows Cleaner". (Ver imagen 66).

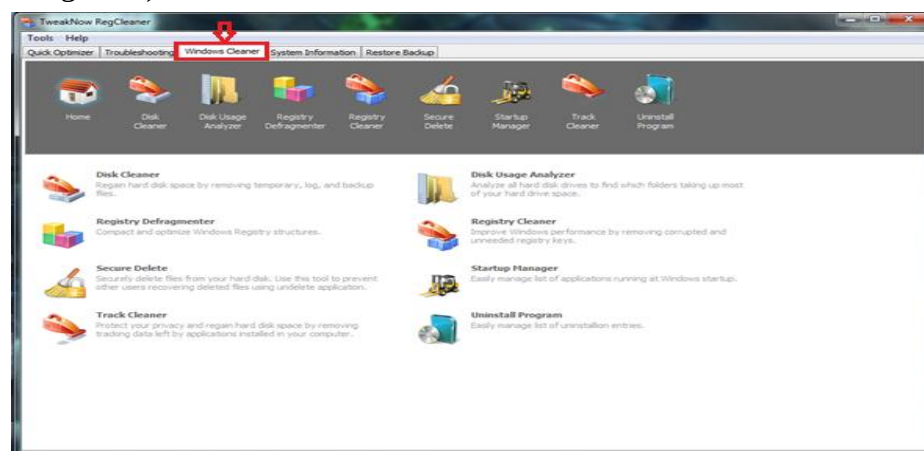


Imagen 66

2. Se selecciona la opción Disk Cleaner, y luego se selecciona el disco a analizar, en este caso se elige el disco local (C:/) seguidamente se da click en “ScanNow”.
- (Ver imagen 67).

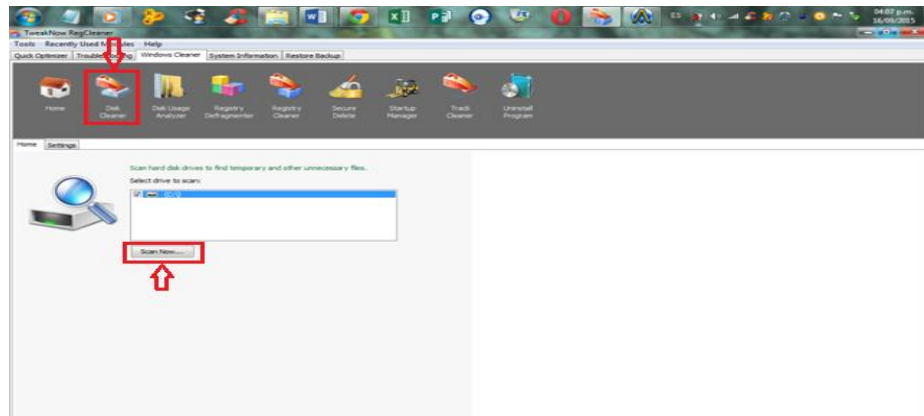


Imagen 67

3. A continuación empezará el análisis del disco duro, esta operación puede durar varios minutos. (Ver imagen 68).

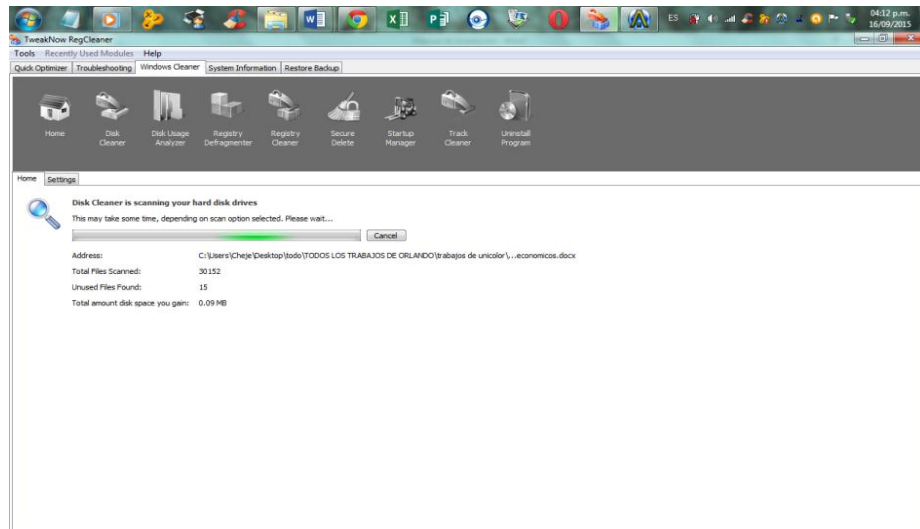


Imagen 68

4. Cuando finalice el proceso mostrará, en una lista el resultado del escaneo, para proceder a la eliminación, se da click en “Delete”. (Ver imagen 69).

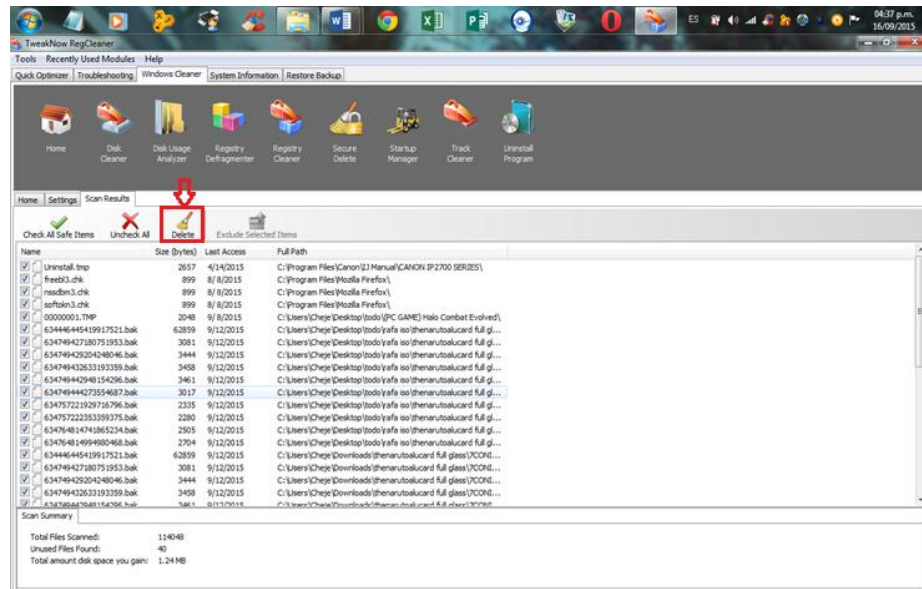


Imagen 69

5. Con eso finaliza el proceso de análisis de RegCleaner en el disco local C:/.

Los archivos están eliminados del disco local. (Ver imagen 70).

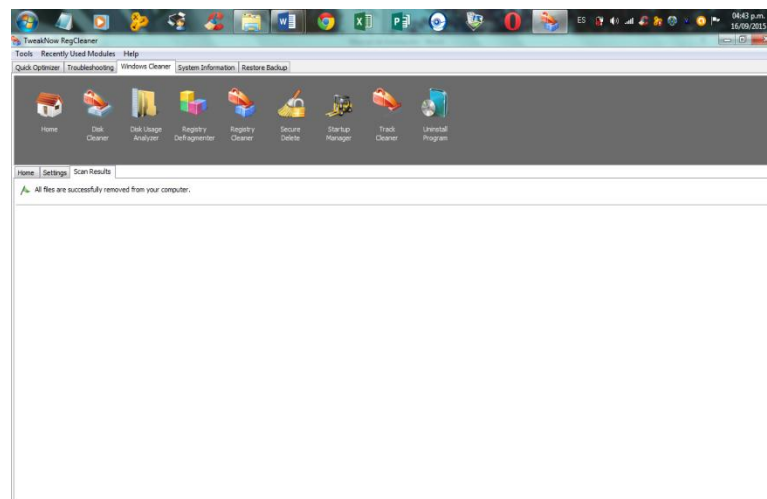


Imagen 70

2.2.4. Manual de uso de RegSeeker

(Este programa no necesita ser instalado)

1. Una vez abierto el CD de herramientas, se da clic en programas, se selecciona la opción de análisis y registro de Windows, seguidamente se da click en el programa “RegSeeker”. (Ver imagen 71).

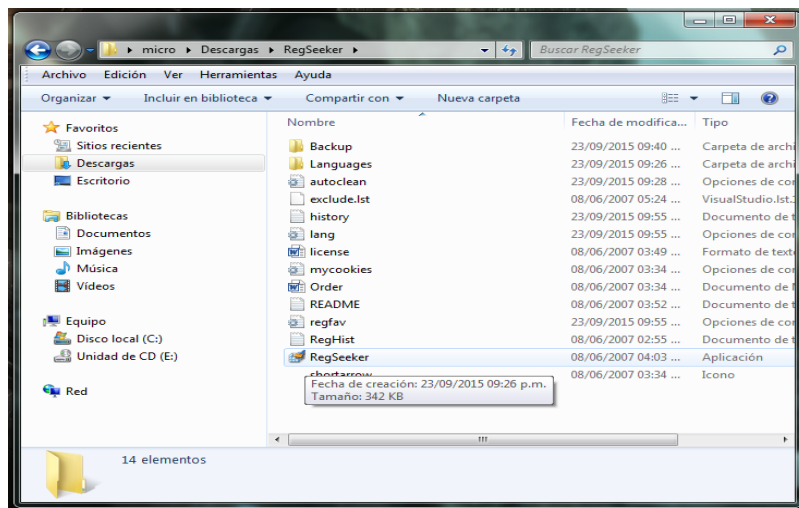


Imagen 71

2. Seguidamente saldrá la pantalla principal del programa, para cambiar el idioma se da click en la opción, “Languages” y se da click en el idioma deseado. (Ver imagen 72).



Imagen 72

1. Se procederá a limpiar el registro de Windows, se da click en “Limpiar el registro”. (Ver imagen 73).

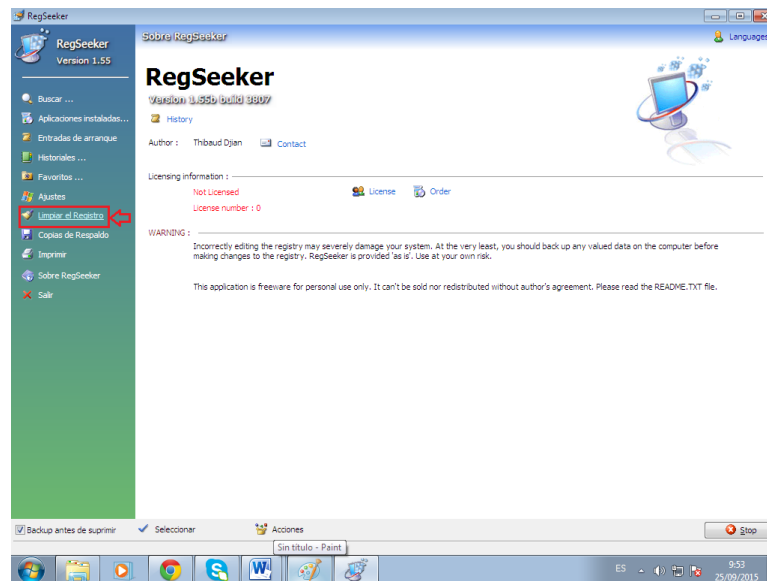


Imagen 73

2. Luego se da click en “Auto limpieza” lo que hace es que permite limpiar el registro del sistema automáticamente, lo que evita que se tenga que andar analizando, buscando y eliminando de forma manual todas las entradas y archivos inservibles. (Ver imagen 74).

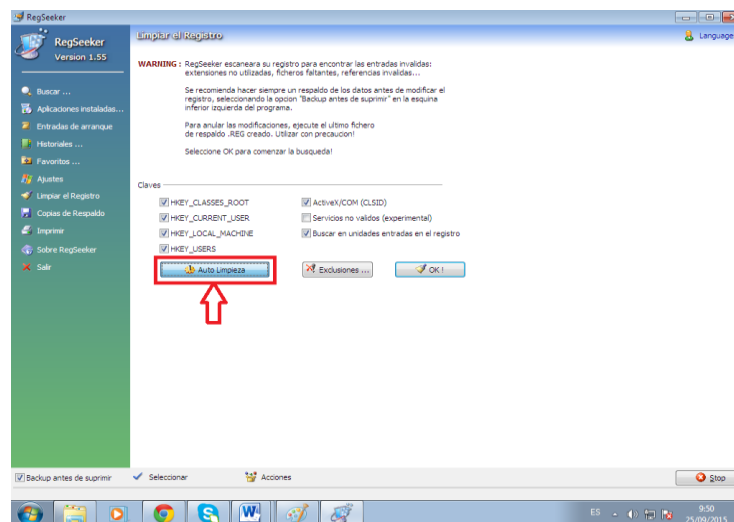


Imagen 74

3. Seguidamente saldrá una ventana con opciones, en este caso se dejaron los parámetros definidos por el programa, le damos click en “GO”. (Ver imagen 75).

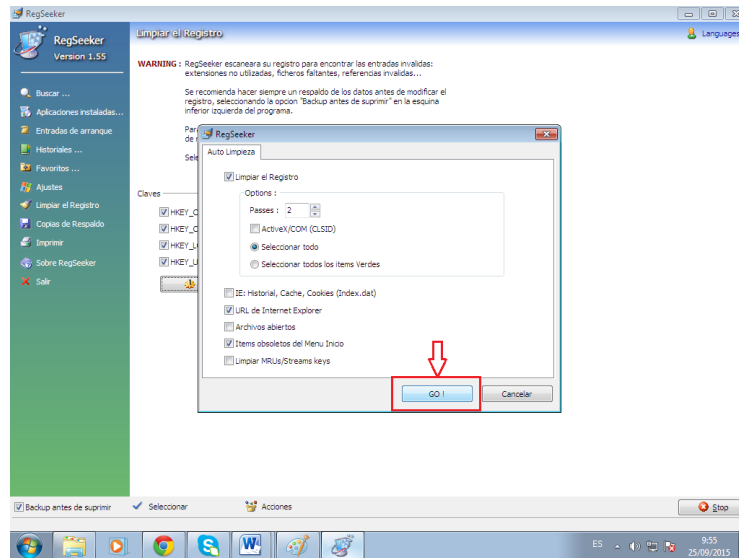


Imagen 75

4. A continuación empezará el análisis del registro. Esta operación puede durar varios minutos. (Ver imagen 76).

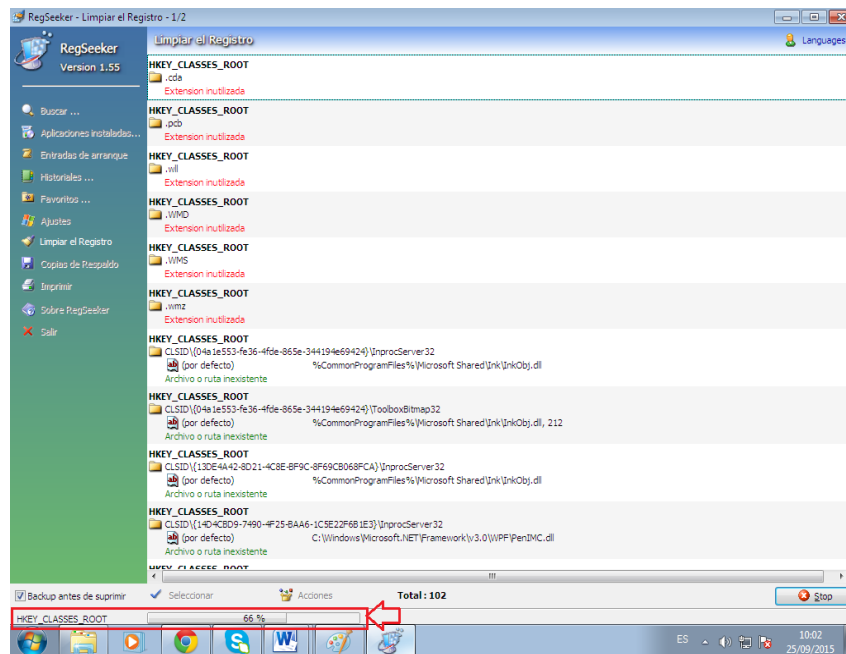


Imagen 76

5. Una vez completado el 100% del análisis se da click en “Stop”. (Ver imagen 77).

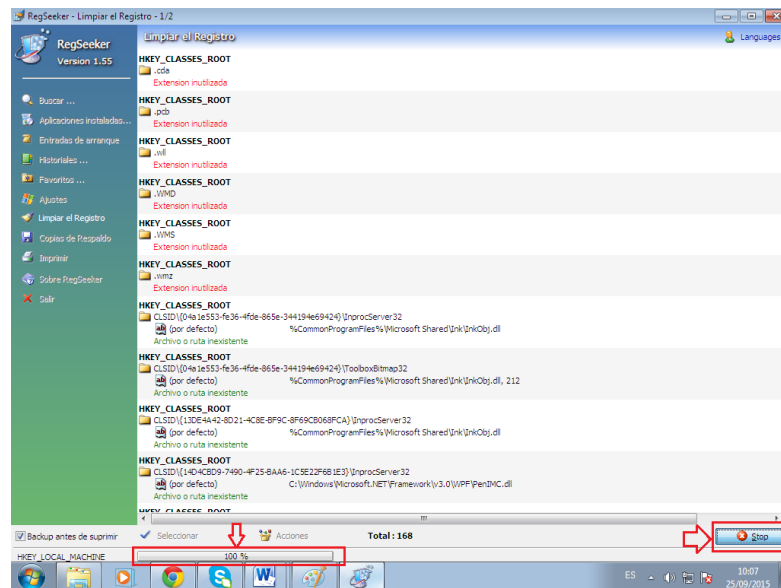


Imagen 77

6. Una vez finalizado el análisis saldrá una pequeña ventana diciendo que se ha completado la auto limpieza, se da click en “Ok” y con eso finaliza el proceso. (Ver imagen 78).

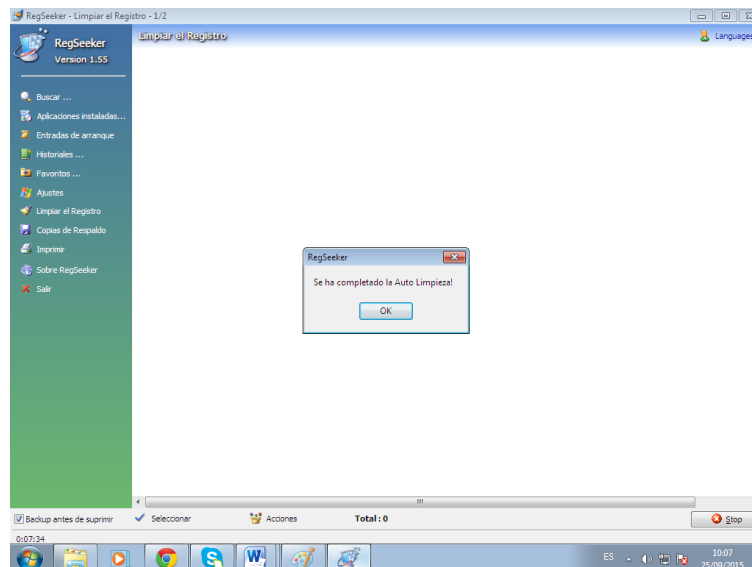


Imagen 78

2.2.5. Manual de instalación y uso de Malwarebytes

Nota: Para el uso de este programa se debe estar en una cuenta de administrador, este programa es compatible desde Windows XP hasta Windows 7. En esta ocasión se realizará en sistema operativo Windows 7.

1. Una vez abierto el CD de herramientas, se da click en programas, luego en Anti Malware, y se da click en el Malware Bytes. (Como lo muestra la imagen 79).

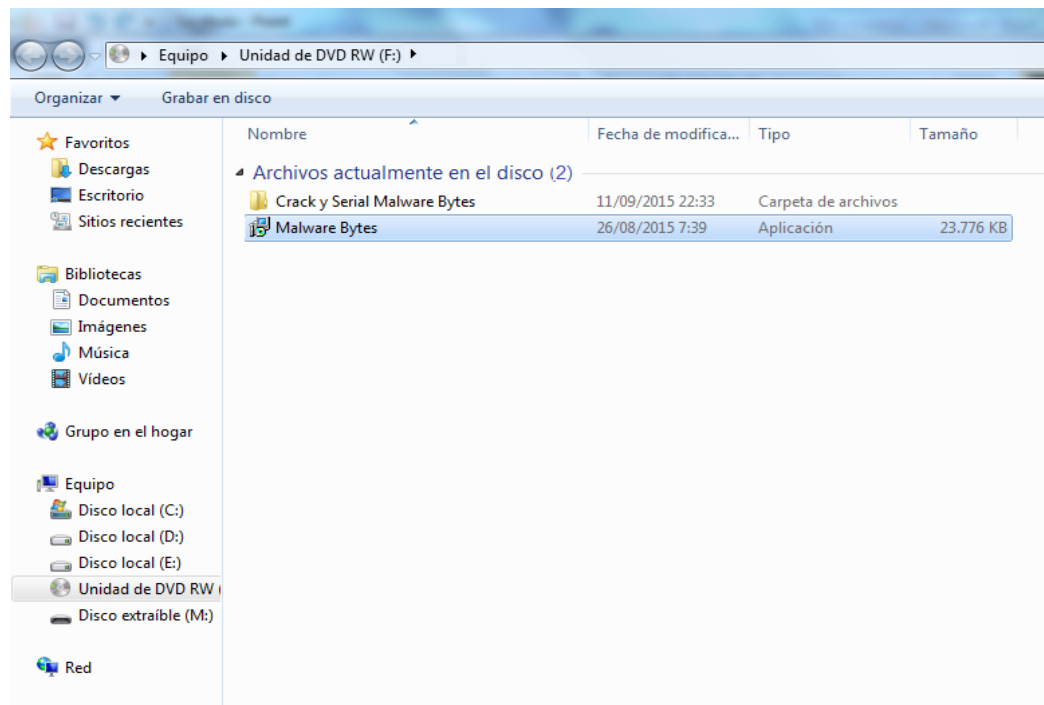


Imagen 79

2. A continuación saldrá una pequeña ventana en donde permite elegir el idioma que se utilizará, en este caso se deja el idioma español y se da click en aceptar. (como lo muestra la imagen 80).

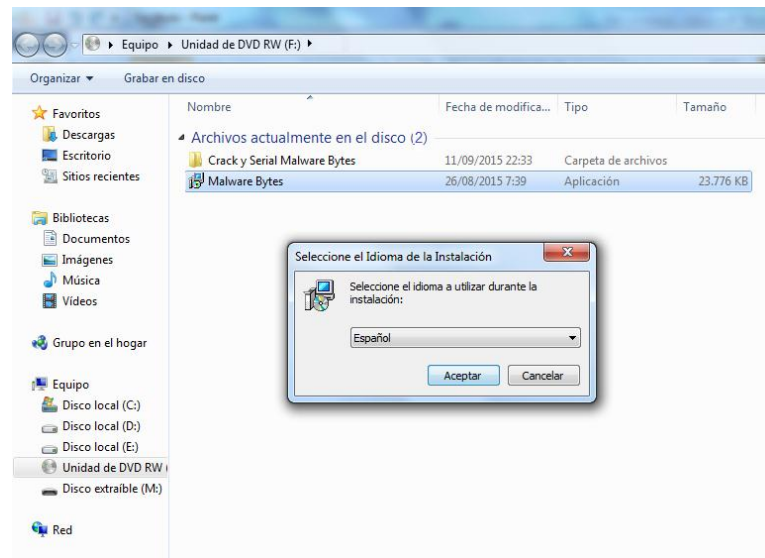


Imagen 80 (Seleccione el idioma de instalación)

3. Seguidamente saldrá la siguiente ventana en la cual se muestra una pequeña bienvenida y unas recomendaciones antes de proseguir con la instalación. (Como se muestra en la imagen 81).

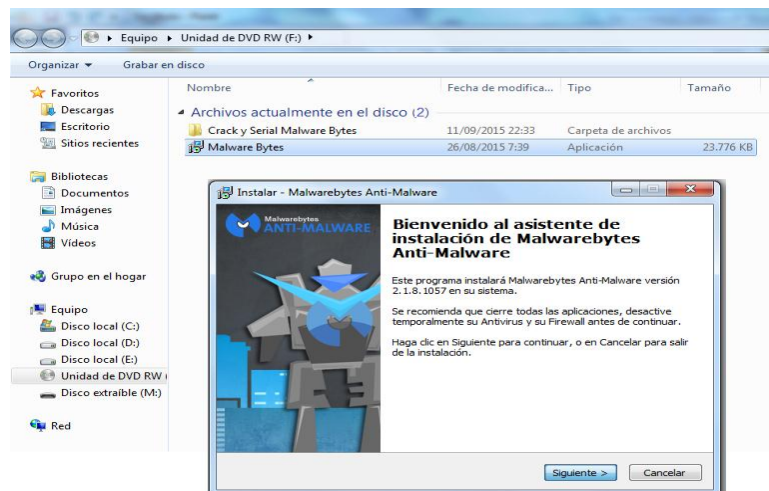


Imagen 81 (Bienvenido al asistente de instalación de Malwarebytes Anti-Malware)

4. Seguidamente aparecerá el acuerdo de licencia, una vez leído se marca la casilla de aceptación de acuerdos y se da click en "siguiente". (Como lo muestra la imagen 82).

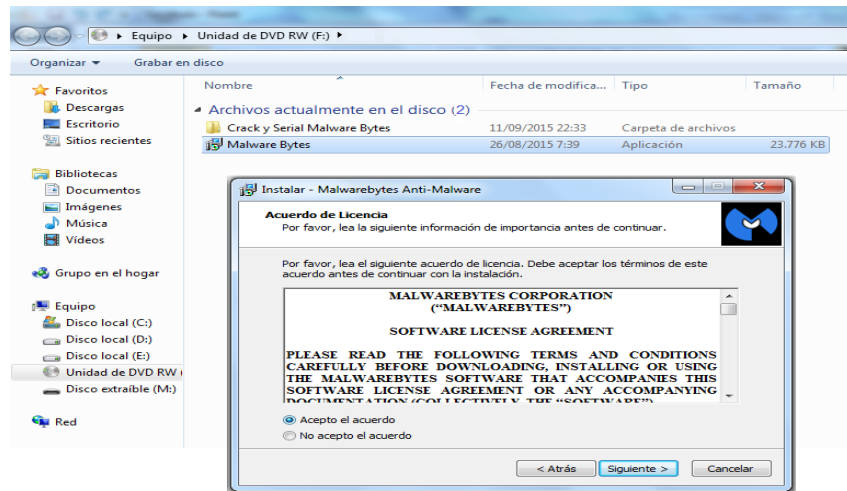


Imagen 82 (Acuerdo de licencia)

5. En esta ventana aparecerá información extra acerca del programa, una vez leída se prosigue con el proceso de instalación dando click en "siguiente". (Como lo muestra la imagen 83).

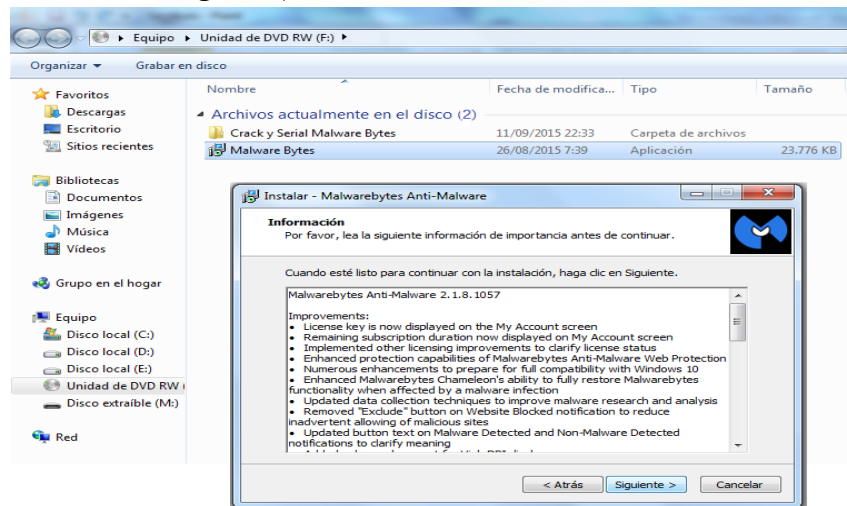


Imagen 83 (Información)

6. En esta ventana se seleccionará la carpeta de destino de la instalación, en este caso se dejará la ruta que el programa eligió, se da click en "siguiente". (Como se muestra en la imagen 84).

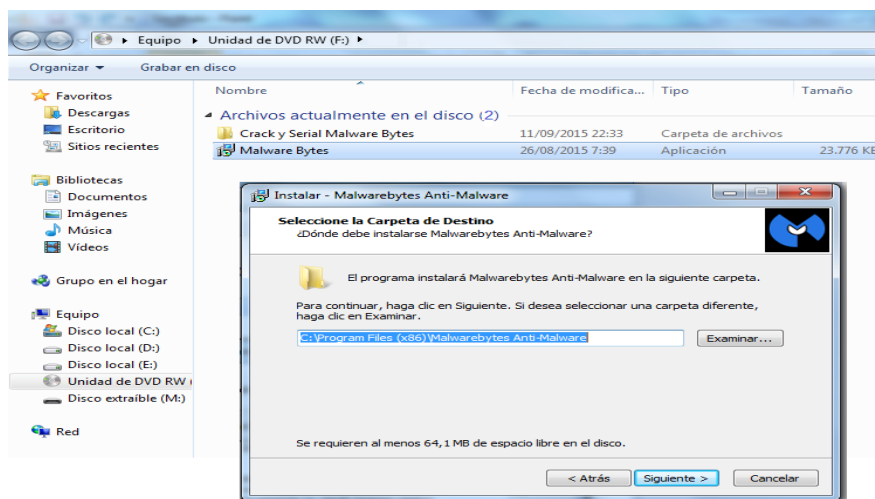


Imagen 84 (Seleccione la carpeta de destino)

7. En esta ventana se selecciona dónde deben colocarse los accesos directos del programa, en este caso se dejará los indicados por el mismo programa, se continua con el proceso de instalación dando click en "Siguiente" (Como se muestra en la imagen 85).

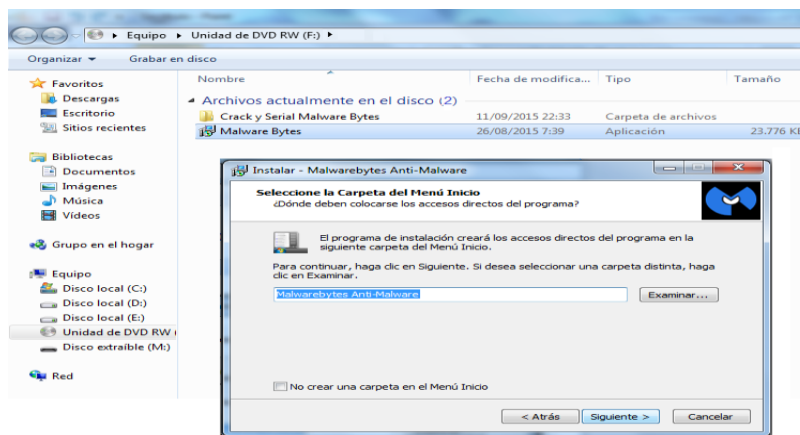


Imagen 85 (Seleccione la carpeta del menú inicio)

8. En esta ventana se muestran las tareas adicionales como por ejemplo crear un acceso directo del programa en el escritorio, se marca la casilla y se continúa dando click en "siguiente". (Como lo muestra la imagen 86).

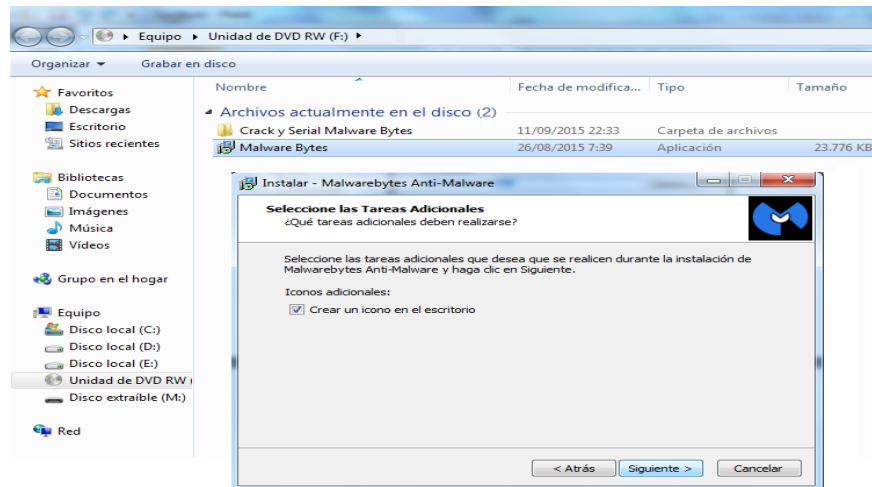


Imagen 86 (Seleccione las tareas adicionales)

9. Ahora ya está todo listo para iniciar con la instalación en esta ventana se muestran los parámetros anteriormente seleccionados, si todo esta correcto se continúa con el proceso de instalación dando click en "instalar". (Como se muestra en la imagen 87).

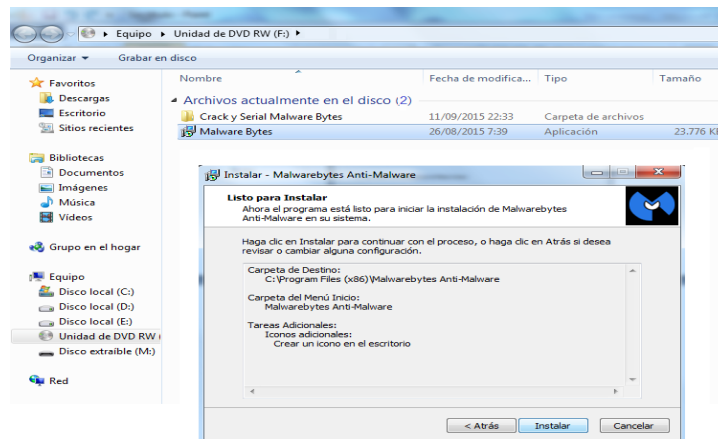


Imagen 87 (Listo para instalar)

10. A continuación iniciará con la instalación del programa, esta operación tardará varios minutos. (Como se muestra en la imagen 88).

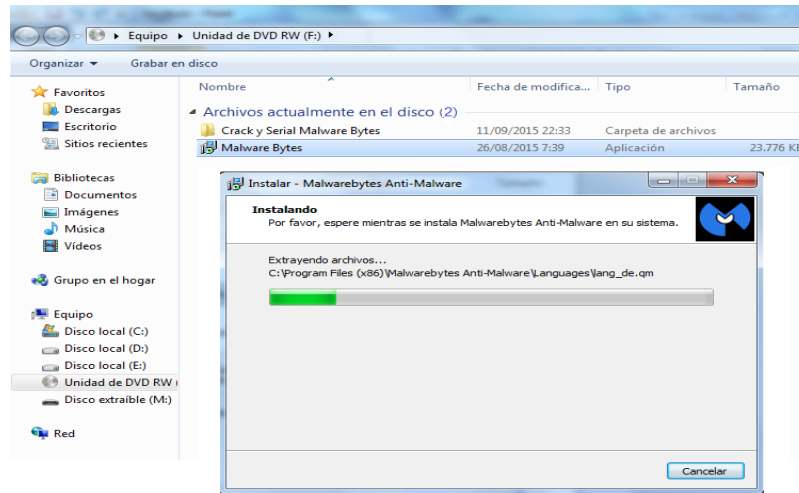


Imagen 88 (Instalando)

11. Una vez terminada la instalación saldrá la siguiente ventana de finalización, se marca la casilla "Ejecutar Malwarebytes Anti-Malware, y luego se da click en "finalizar". (Como se muestra en la imagen 89).

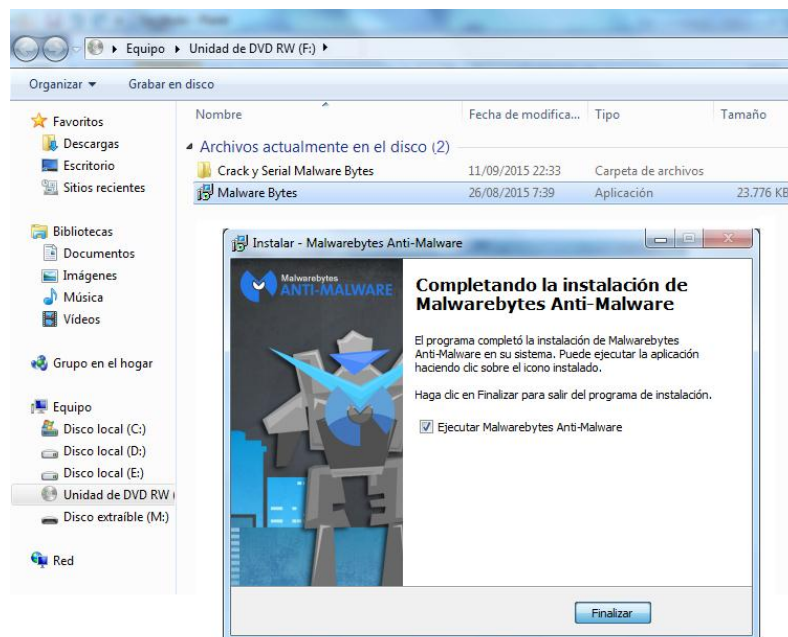


Imagen 89 (Completando la instalación de Malwarebytes Anti-Malware)

Ahora se procederá a activar el programa mediante una licencia. (Solo para fines educativos).

1. Se ingresa a la unidad de CD, luego a la carpeta programas, después a la carpeta Anti-Malware, luego a la carpeta Malwarebytes y luego a la carpeta llamada Serial Malware Bytes. (Como se muestra en la imagen 90).

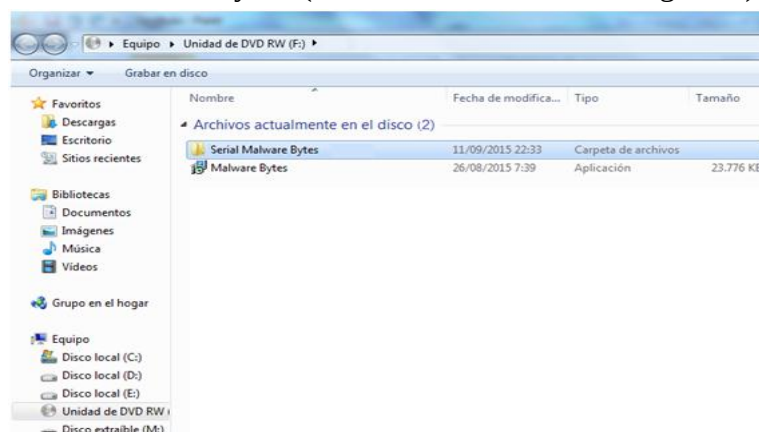


Imagen 90

2. Se da click sobre el documento ID Y KEY Malware Bytes para abrirlo ya que ahí se encuentra el ID y la licencia del programa. (Como se muestra en la imagen 91).

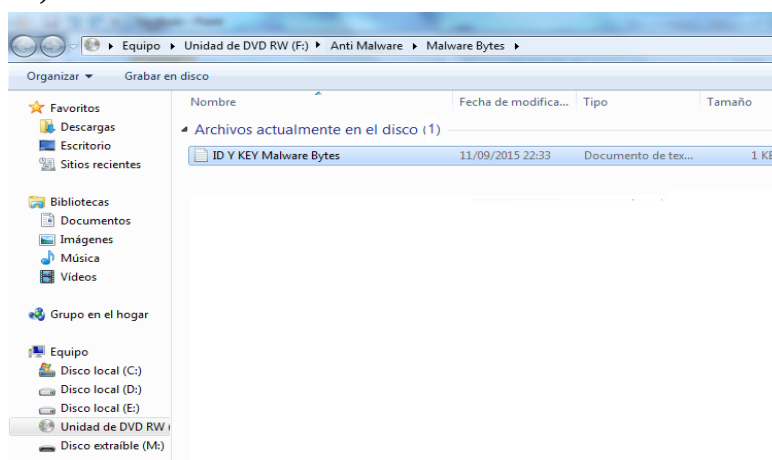


Imagen 91

- Una vez abierto el documento de texto mostrara el ID y el KEY de activación del programa, (Como se muestra en la imagen 92), luego se dirige al programa, para poder continuar con la activación.

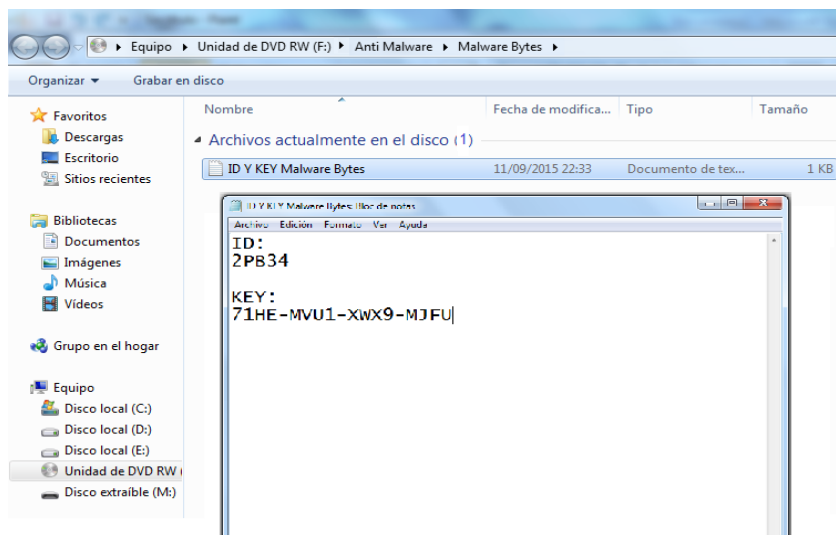


Imagen 92

- A continuación se presenta la ventana principal del programa, en el costado derecho se encuentra una opción llamada “Mi cuenta”, se da click para poder seguir con la activación. (Como se muestra en la imagen 93).

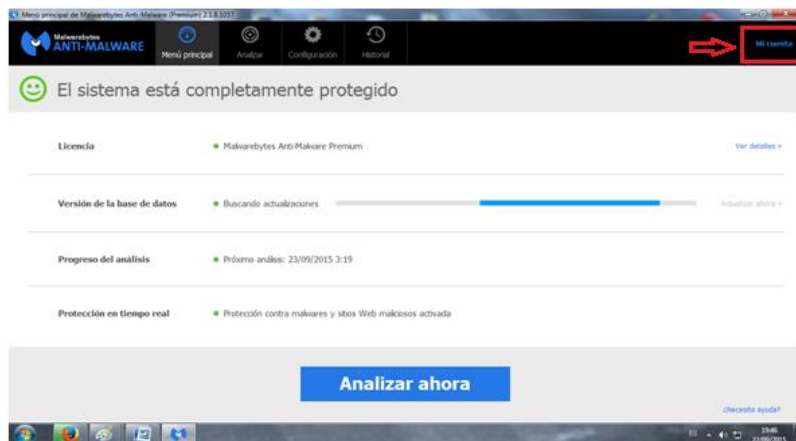


Imagen 93

5. Seguidamente saldrán los detalles de la cuenta, para poder ingresar una licencia válida, se da click en el costado derecho en la opción que se llama “Cambiar licencia”. (Como se muestra en la imagen 94).

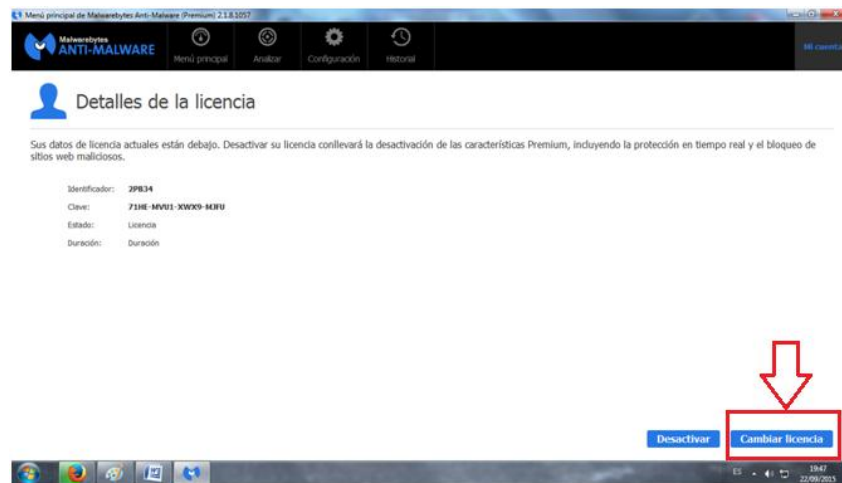


Imagen 94

6. Seguidamente saldrá una ventana, donde indica que se introducirán los datos de la nueva licencia, se da click donde dice “También tengo una identificación”. (Como se muestra en la imagen 95).

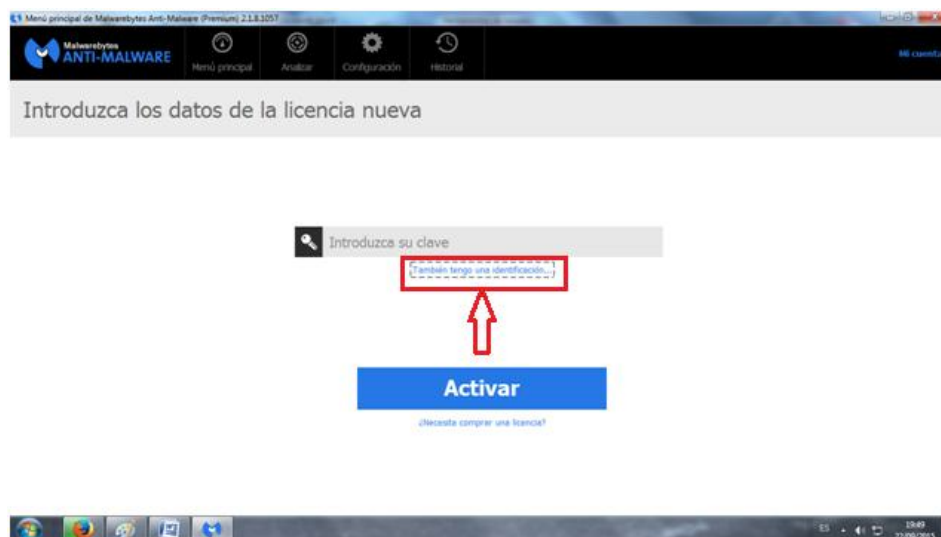


Imagen 95

7. A continuación aparecerán los campos para introducir los datos, en el campo llamado “ID” se pondrá: “2PB34” y en campo donde aparece un icono de llave se pondrá: “71HE-MVU1-XWX9-MJFU”, seguidamente se da click en “Activar” (Como se muestra en la imagen 96).

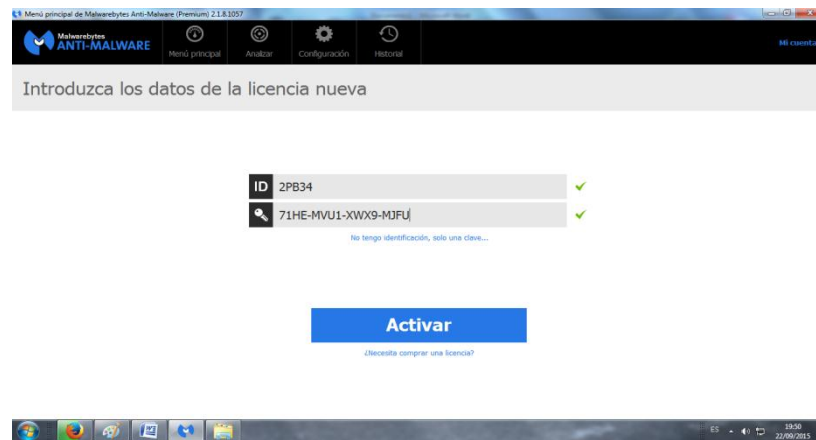


Imagen 96

Pasos para analizar el equipo en busca de infecciones

1. Una vez activado el programa, se procederá al análisis del equipo en busca de infecciones, para eso se da click en el botón “Analizar ahora”. (Como se muestra en la imagen 97).

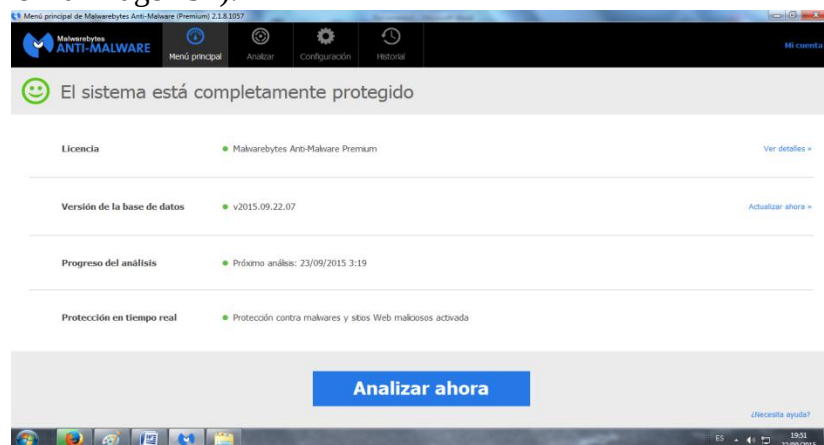


Imagen 97 (Menú principal)

2. A continuación comenzará el análisis de amenazas, este proceso puede durar varios minutos. (Como se muestra en la imagen 98).

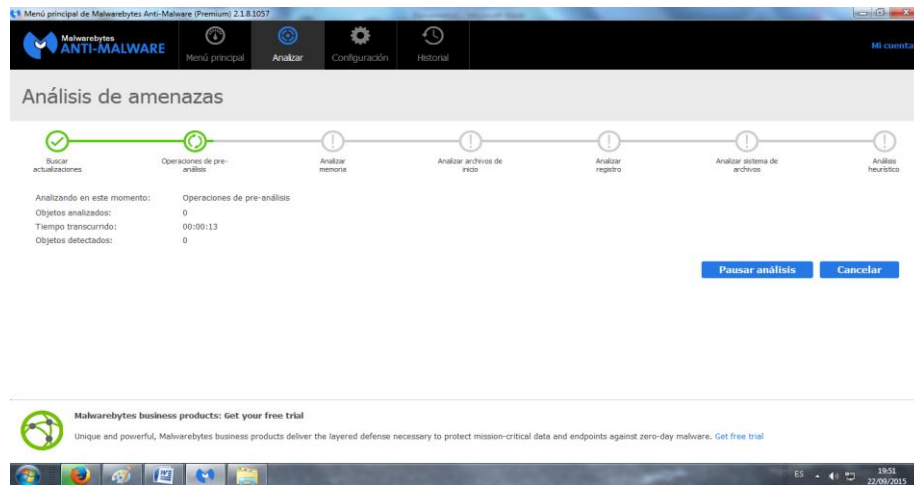


Imagen 98 (Análisis de amenazas)

3. Una vez finalizado el análisis muestra el resultado de las amenazas, en este caso se detectaron seis amenazas, ahora se procederá a su eliminación, dando click en “Eliminar amenazas”. (Como se muestra en la imagen 99).



Imagen 99 (Resultado de análisis de amenazas)

4. En esta ventana muestra que las amenazas han sido quitadas con éxitos, se finaliza dando click en “Terminar”. (Como lo muestra la imagen 100).

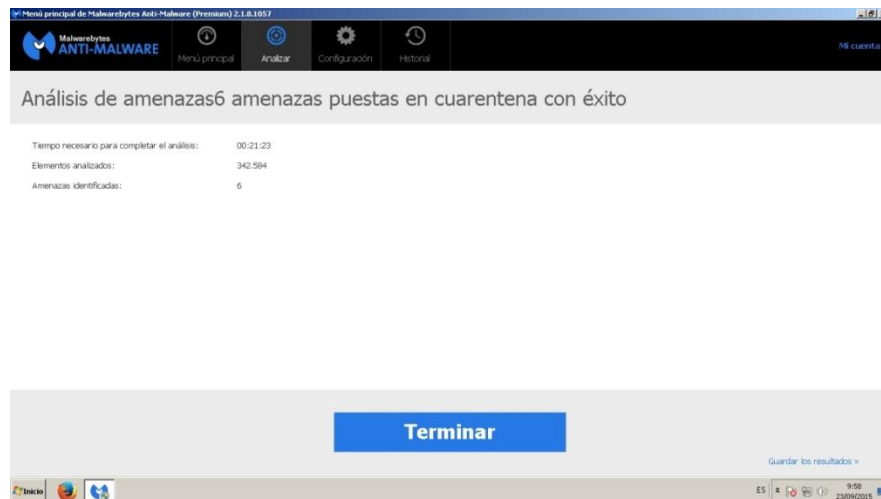


Imagen 100

5. Después de que se dio click en terminar aparecerá el siguiente cuadro donde pide que el equipo debe ser reiniciado para poder completar el proceso, se da click en “si” (Como se muestra en la imagen 101) y posteriormente el equipo será reiniciado, y con eso finaliza todo el proceso.

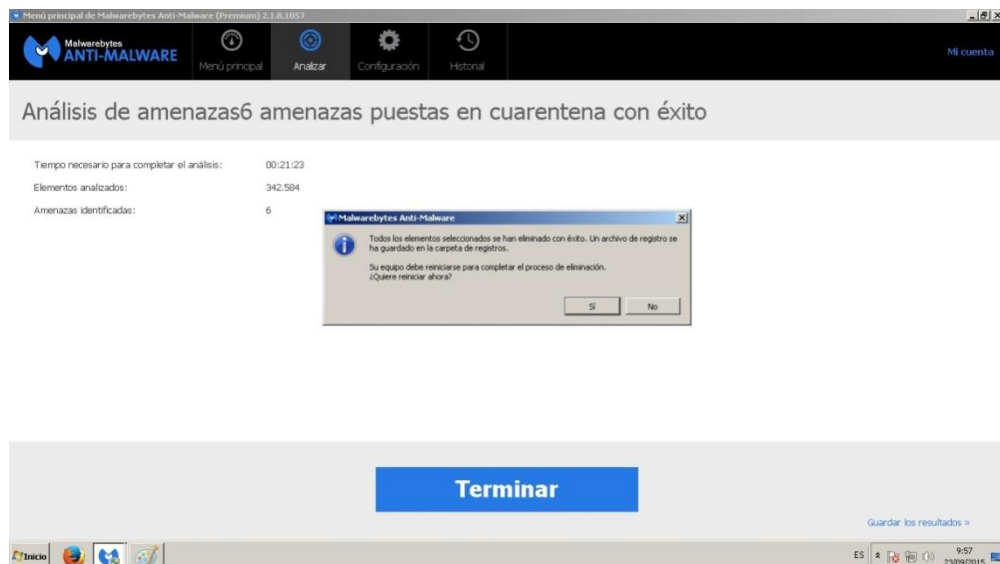


Imagen 101 (Malwarebytes Anti-Malware)

2.2.6. Manual de uso de NTPWEDIT

(Este programa no necesita ser instalado)

Nota: Para el uso de este programa no es necesario estar dentro de una cuenta de administrador, este programa es compatible desde Windows XP hasta Windows 7. En esta ocasión se realizará en sistema operativo Windows 7. En este caso se hará una modificación de contraseña.

1. Como se puede observar en (La imagen 102), la cuenta está protegida por contraseña.



Imagen 102

2. Para poder cambiar la contraseña se necesita desmontar el disco duro y colocarlo en un adaptador para conectarlo vía USB. (Como lo muestra la imagen 103).



Imagen103

3. Una vez abierto el CD de herramientas, se da click en programas, luego en eliminación o modificación de contraseñas de Windows, y se da click en el NTPWEDITI. (Como lo muestra la imagen 104). En este caso se utilizara el programa de 32 bits.

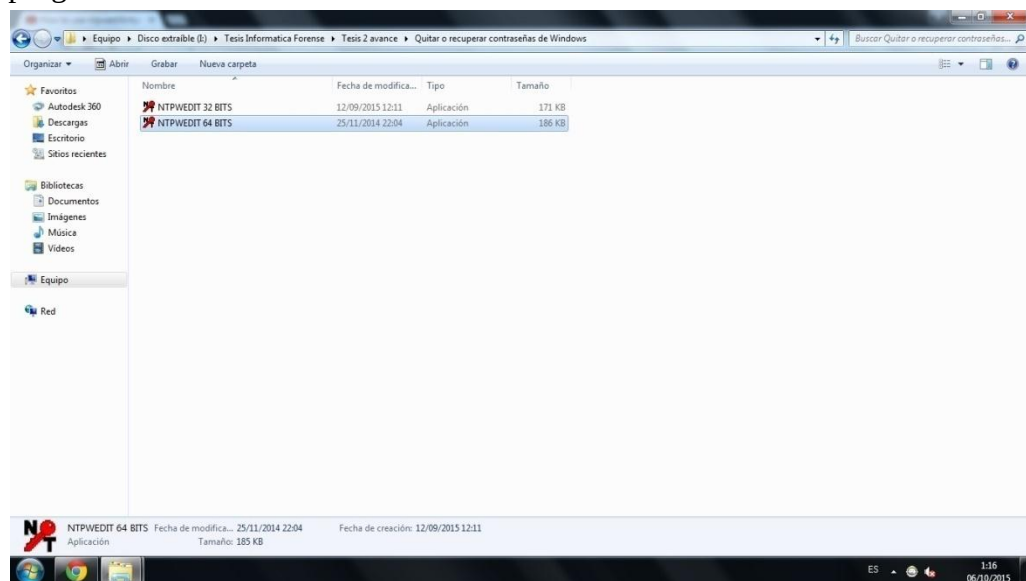


Imagen 104

4. Una vez abierto saldrá la pantalla principal del programa, para poder cambiar la contraseña se necesita acceder a un archivo protegido que se encuentra en esta ruta: C: \WINDOWS\SISTEM32\CONFIG\SAM, para eso se da click en open para avanzar a la ruta asignada. (Como lo muestra la imagen 105).

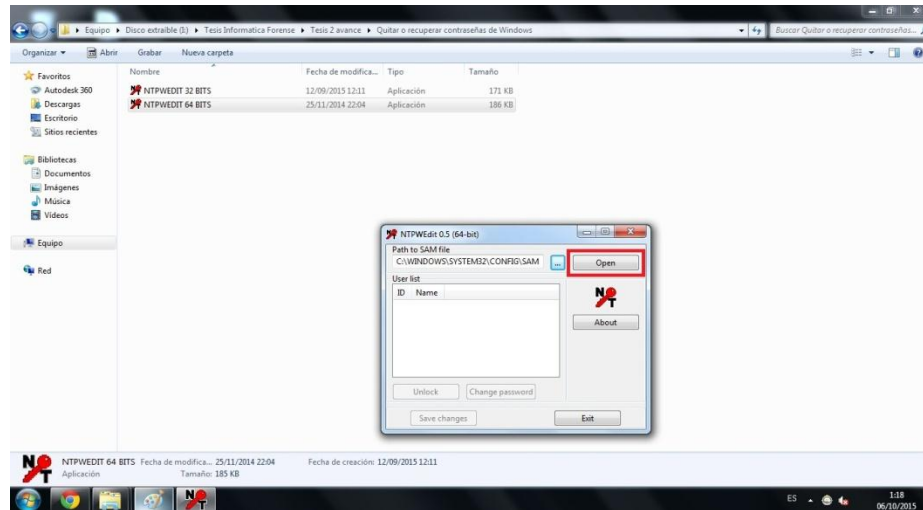


Imagen 105

5. Se da click en el disco duro externo en este caso es el Disco Local (H:) para poder llegar al archivo “SAM”, se da click para ingresar. (Como se muestra en la imagen 106).

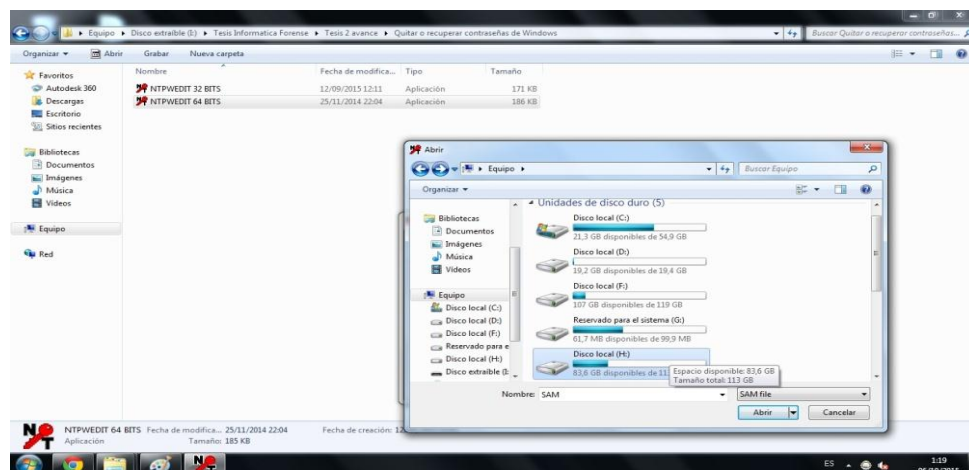


Imagen 106

6. Una vez dentro se da click en la carpeta llamada “Windows” (Como se muestra en la imagen 107).

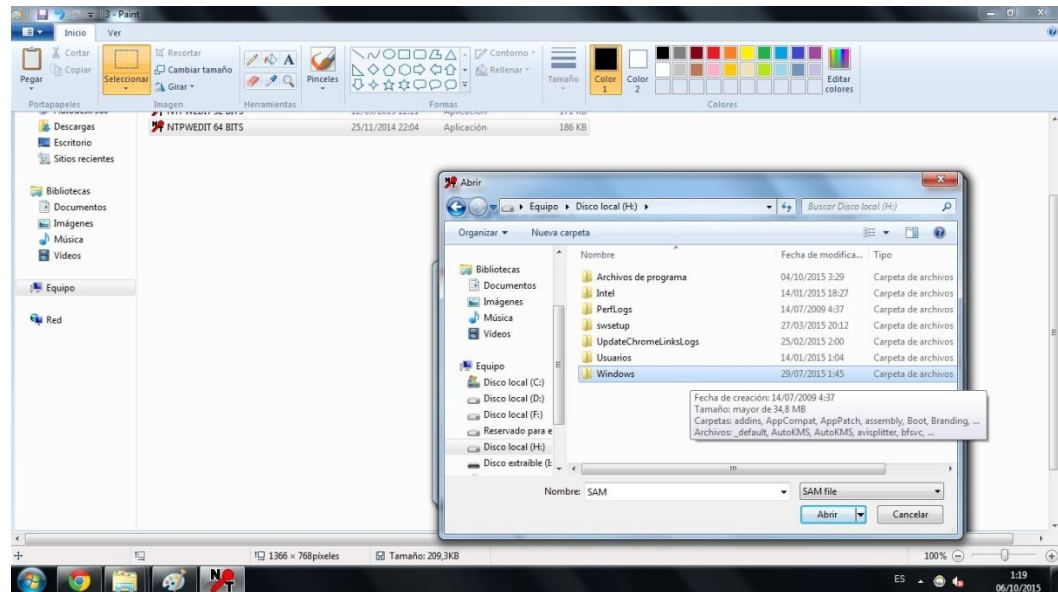


Imagen 107

7. Seguidamente se busca y se da click a la carpeta llamada “System 32” (Como se muestra en la imagen 108).

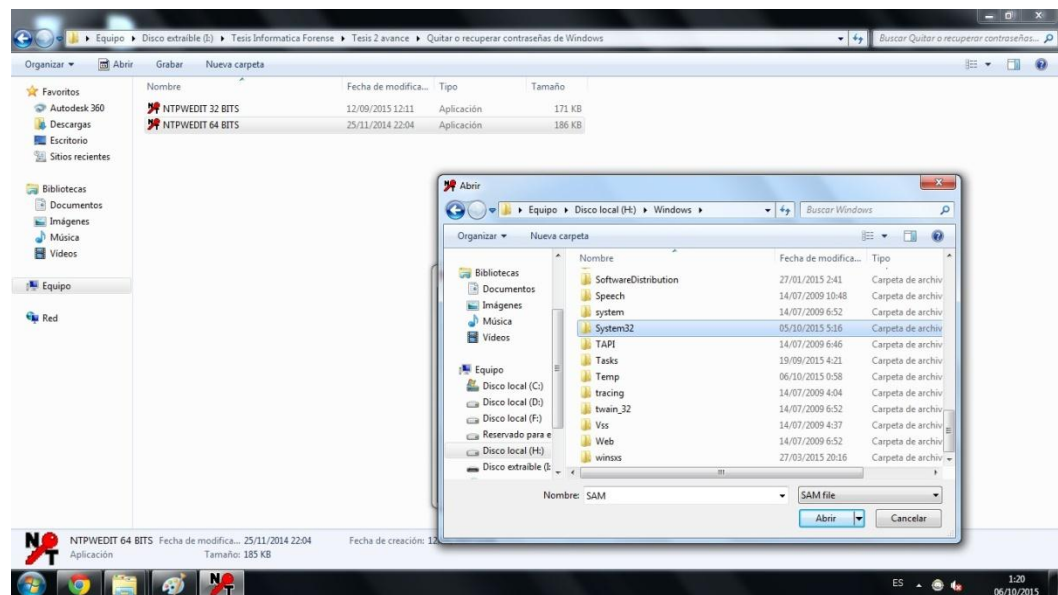


Imagen 108

8. Luego se busca y da click a la carpeta llamada “Config” (Como lo muestra la imagen 109).

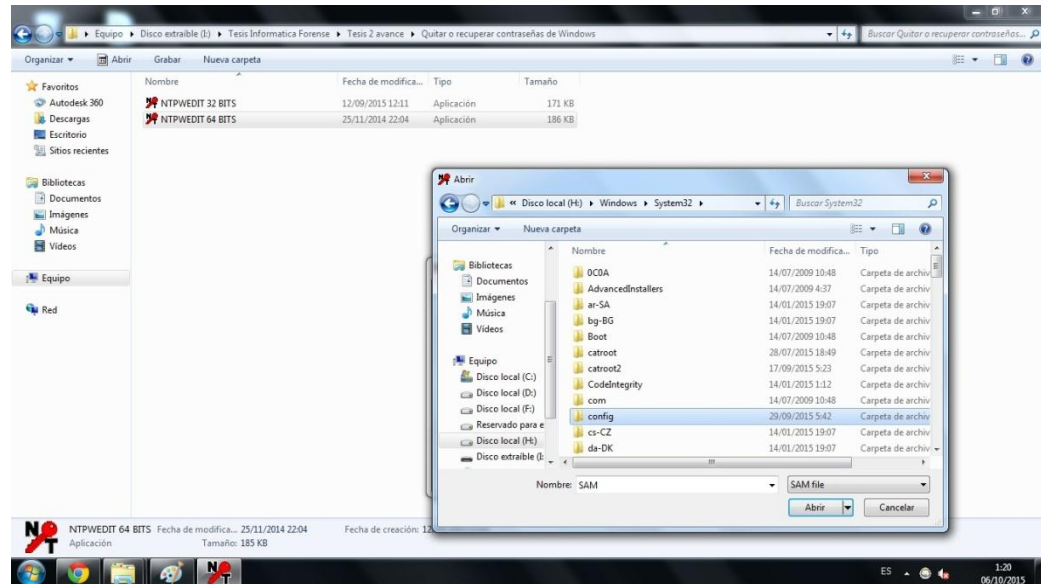


Imagen109

9. En esta ventana aparecerá el archivo llamado “SAM” se selecciona y da click en “abrir” (Como lo muestra la imagen 110).

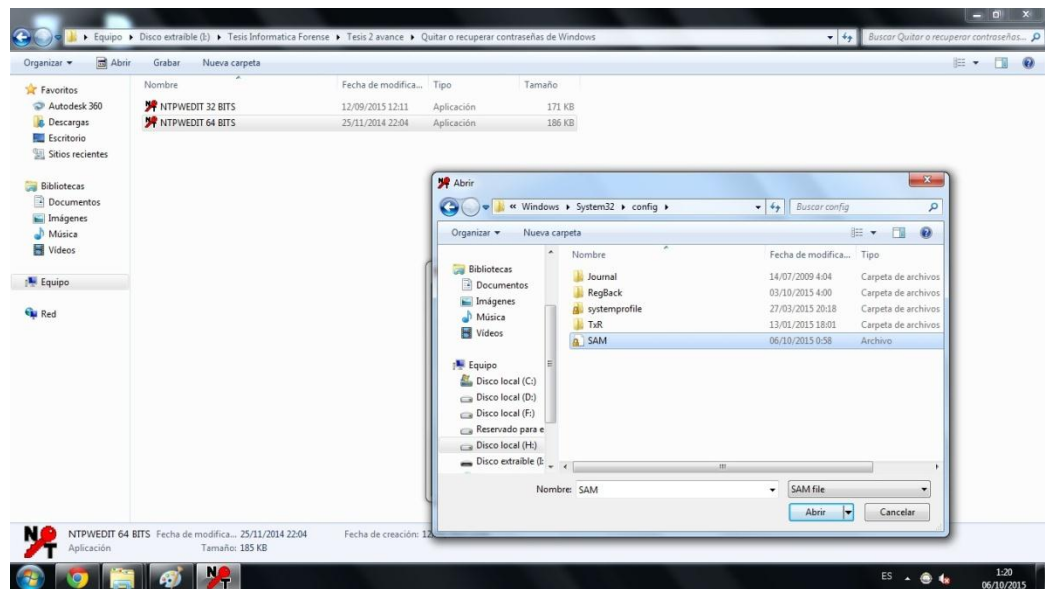


Imagen 110

10. Después saldrá una ventana donde muestra los usuarios que tiene ese disco duro, se selecciona el usuario “David” y luego se da click en “Change password”. (Como se muestra en la imagen 111).

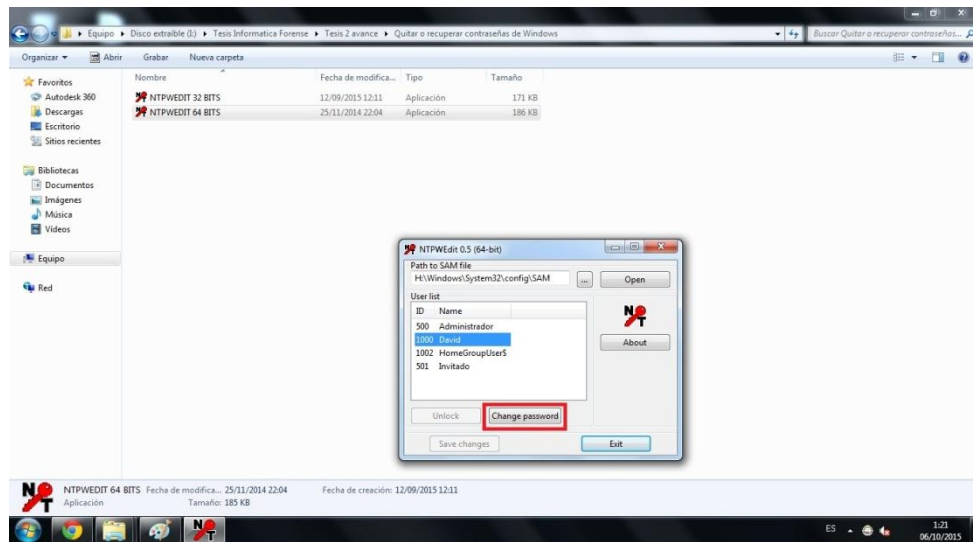


Imagen 111

11. A continuación en el cuadro que aparece, se escribe la contraseña que el usuario designe. (Ver Imagen 112).

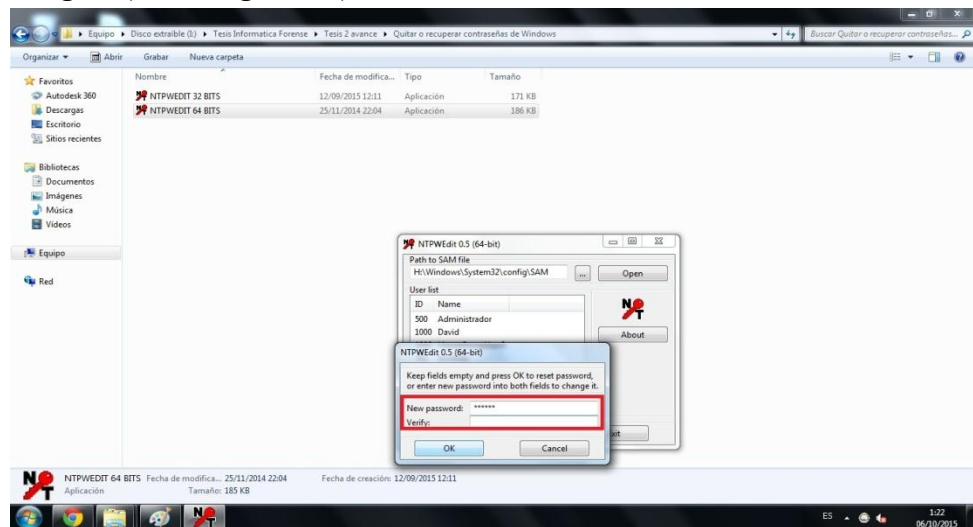


Imagen 112

12. Para guardar los cambios y que el disco duro quede con la contraseña que se eligió se da click en “Save Changes” y en “Exit” (Como se muestra en la imagen 113).

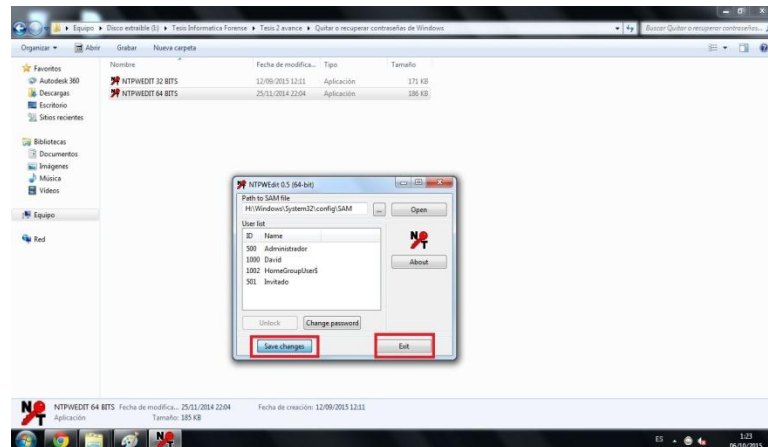


Imagen 113

13. Seguidamente se desmonta el disco duro del adaptador y se vuelve a colocar dentro de la laptop, se enciende y se espera que llegue a la pantalla de inicio de sesión una vez ahí se coloca la contraseña que se seleccionó en el proceso y se iniciara la sesión. (Como se muestra en la imagen 114).



Imagen 114

2.2.7. Manual de uso de Browser Password Decryptor

(Para la instalación del programa se debe desactivar el antivirus)

Nota: Para el uso de este programa no es necesario estar dentro de una cuenta de administrador, este programa es compatible desde Windows XP hasta Windows 7. En esta ocasión se realizará en sistema operativo Windows 7.

1. Se procederá a desactivar el antivirus, en la barra de tareas activas, se busca el icono del antivirus, en este caso se está utilizando el antivirus AVG, una vez localizado se da click derecho sobre el icono y se da click en “Deshabilitar la protección AVG temporalmente” (Como se muestra en la imagen 115).

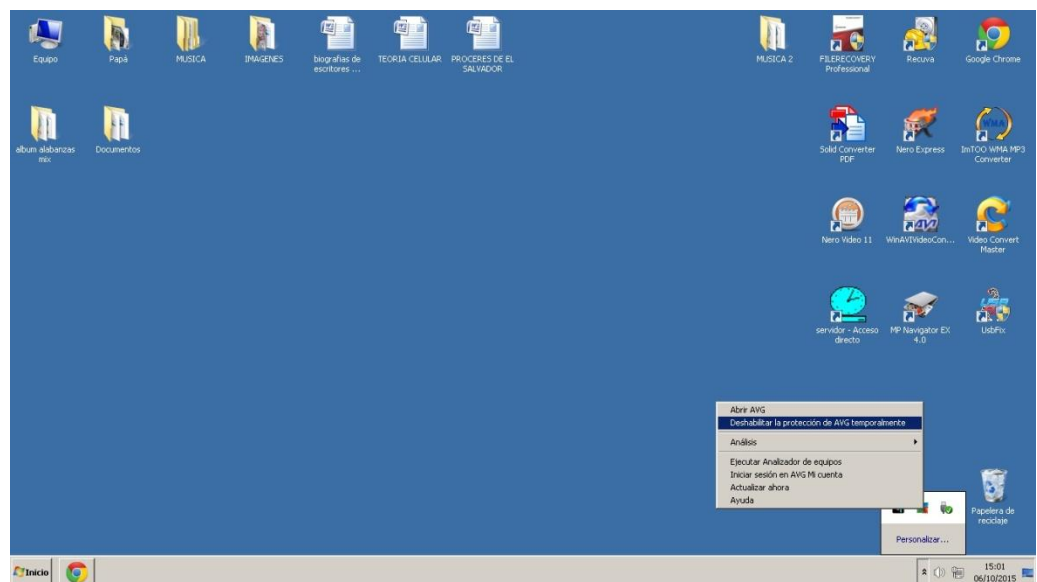


Imagen 115

2. Luego saldrá la ventana de deshabilitar protección de AVG temporalmente, se elige la opción de 15 minutos y se da click en aceptar. (Como se muestra en la imagen 116).

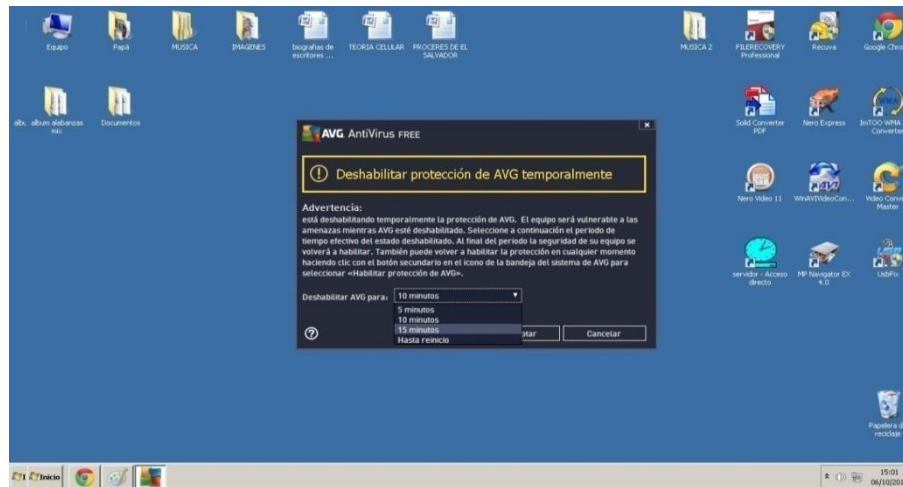


Imagen 116

3. Una vez abierto el CD de herramientas, se da click en programas, luego en Recuperación de contraseñas guardadas en navegadores, y se da click en el Browser Password Decryptor. (Como lo muestra la imagen 117).

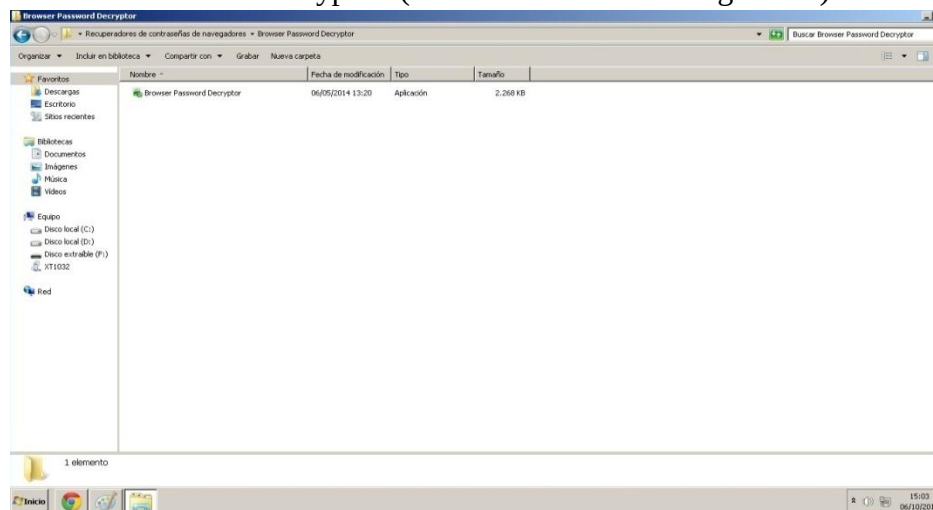


Imagen 117

4. Seguidamente saldrá la pantalla de bienvenida del programa, se da click en “Next” para seguir con la instalación. (Como se muestra en la imagen 118).



Imagen118 (Welcome)

5. En esta ventana muestra los términos del acuerdo, una vez leídos, se marca la casilla de aceptación de términos y condición y se da click en “Next” (Como lo muestra la imagen 119).



Imagen 119 (License Agreement)

6. En esta sección se elige la ruta del destino de la instalación, en este caso se deja la especificada por el programa y se da click en “Next”. (Ver imagen 120).



Imagen 120 (Choose Install Location)

7. En esta ventana muestra una confirmación de la instalación si no se realizaran cambios se da click en “Install”. (Ver Imagen 121).



Imagen 121 (Confirm Installation)

8. En esta ventana muestra el avance de la instalación. (Ver imagen 122)



Imagen 122 (Installing)

9. En esta sección saldrá una ventana con una oferta de software adicional, si no se desea instalar se da click en “Decline”. Ver imagen (123).



Imagen 123 (Installing)

10. Seguidamente aparecerá una nueva ventana ofreciendo software adicional, si no se desea instalar se da click en “Decline”. Ver imagen (124).



Imagen 124 (Installing)

11. Luego de eso finalizara la instalación y saldrá una ventana indicando los procesos realizados, se da click en “Next”. (Ver imagen 125).



Imagen125 (Installation Complete)

12. En esta ventana indica que la instalación fue realizada correctamente, para iniciar con el programa se marca la casilla “Run Browser Password DecryptorNow”.

(Ver imagen 126).



Imagen 126

Pasos para obtener las contraseñas guardadas en los navegadores

1. Una vez abierto el programa muestra su pantalla principal, al costado derecho se da click en “Star Recovery” (Ver imagen 127).



Imagen 127

2. El programa iniciara con la búsqueda de los sitios con contraseñas guardadas y luego las muestra el nombre del sitio y la contraseña. (Ver imagen 128)



Imagen 128

2.2.8. Manual de uso de WebBrowserPassView

(Para la instalación del programa se debe desactivar el antivirus, este programa no necesita instalación)

Nota: Para el uso de este programa no es necesario estar dentro de una cuenta de administrador, este programa es compatible desde Windows XP hasta Windows 7. En esta ocasión se realizará en sistema operativo Windows 7.

1. Se procederá a desactivar el antivirus, en la barra de tareas activas, se busca el icono del antivirus, en este caso se está utilizando el antivirus AVG, una vez localizado se da click derecho sobre el icono del antivirus y se da click en “Deshabilitar la protección AVG temporalmente” (Como se muestra en la imagen 129).

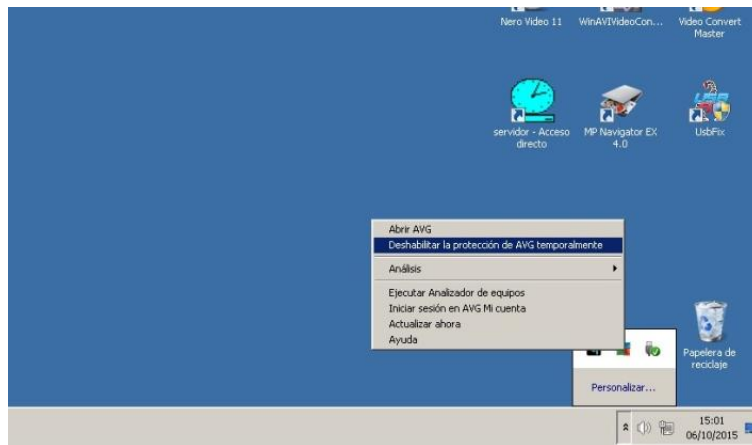


Imagen 129

2. Luego saldrá la ventana de deshabilitar protección de AVG temporalmente, se elige la opción de 15 minutos y se da click en aceptar. (Como se muestra en la imagen 130).



Imagen 130

3. Una vez abierto el CD de herramientas, se da click en programas, luego en Recuperación de contraseñas guardadas en navegadores, y se da click en el WebBrowserPassView. (Como lo muestra la imagen 131).

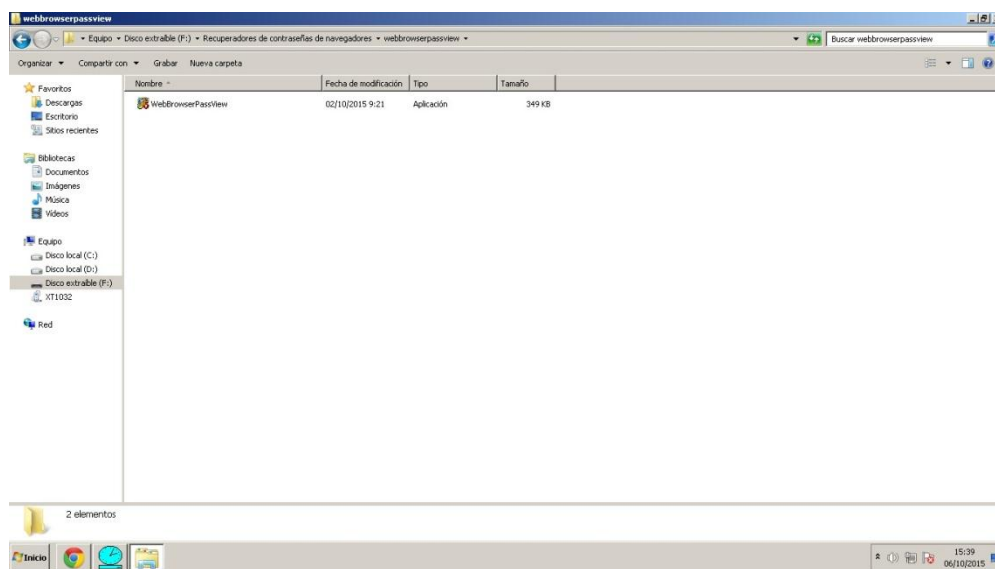


Imagen 131

4. Luego saldrá la ventana principal del programa y automáticamente mostrara las contraseñas guardadas en los navegadores. (Como se muestra en la imagen 132).

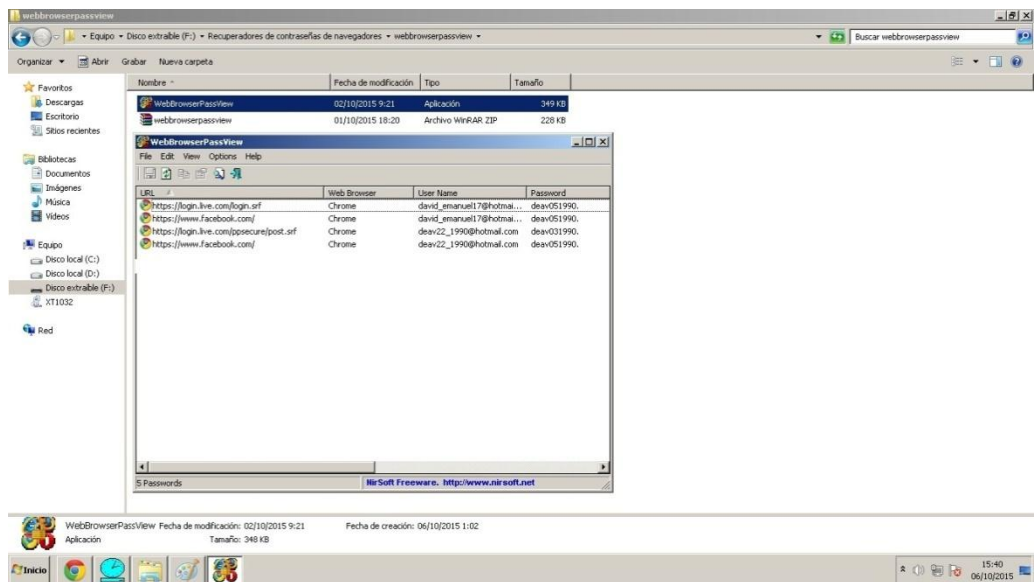


Imagen 132

2.2.9. Manual de uso de Ardamax Keylogger

(Para la instalación del programa se debe desactivar el antivirus)

Nota: Para el uso de este programa es necesario estar dentro de una cuenta de administrador, este programa es compatible desde Windows XP hasta Windows 7. En esta ocasión se realizará en sistema operativo Windows 7.

1. Se procederá a desactivar el antivirus, en la barra de tareas activas, se busca el icono del antivirus, en este caso se está utilizando el antivirus AVG, una vez localizado se da click derecho sobre el icono del antivirus y se da click en “Deshabilitar la protección AVG temporalmente” (Ver imagen 133).

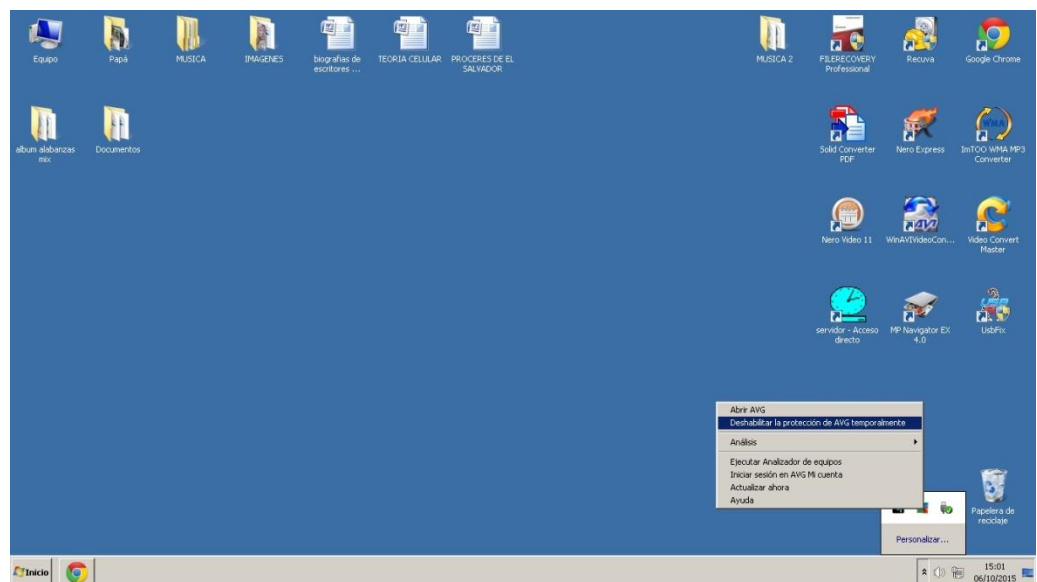


Imagen 133

2. Luego saldrá la ventana de deshabilitar protección de AVG temporalmente, se elige la opción de 15 minutos y se da click en aceptar. (Ver imagen 134).

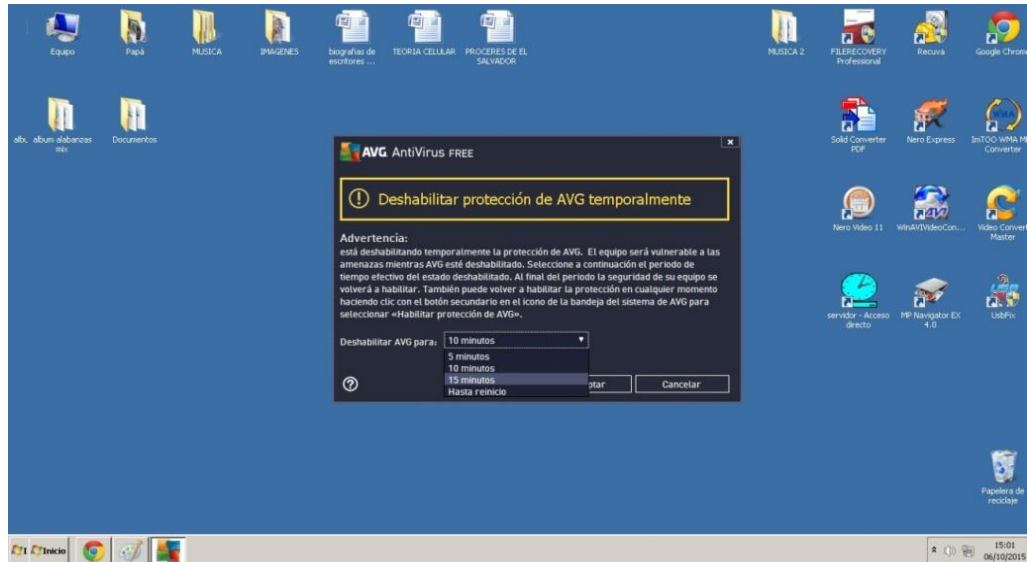


Imagen 134

3. Una vez abierto el CD de herramientas, se da click en programas, luego en Keyloggers, y se da click en el Ardamax Keylogger. (Ver imagen 135).

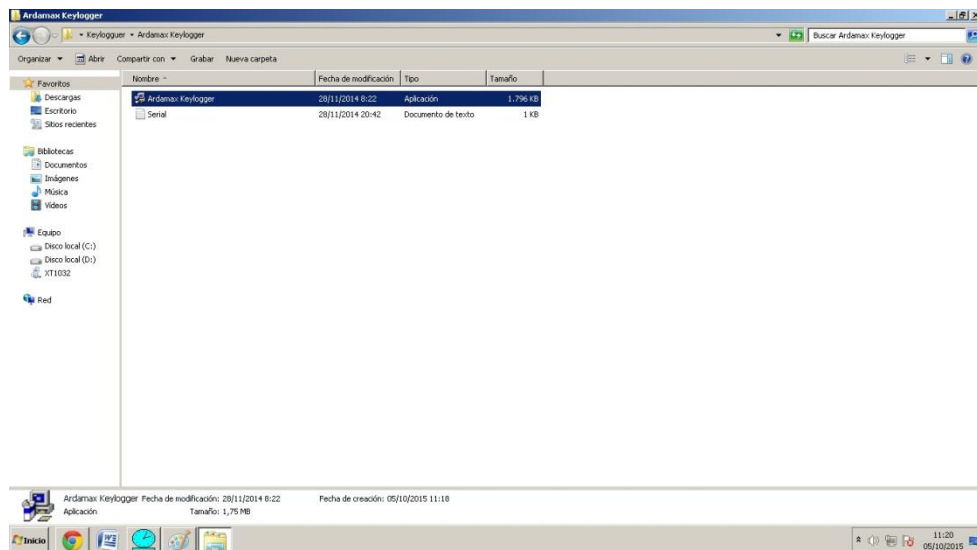


Imagen 135

4. Aparecerá la ventana de aceptación de términos y licencia, se da click en “I Agree” para aceptar y continuar. (Ver imagen 136).

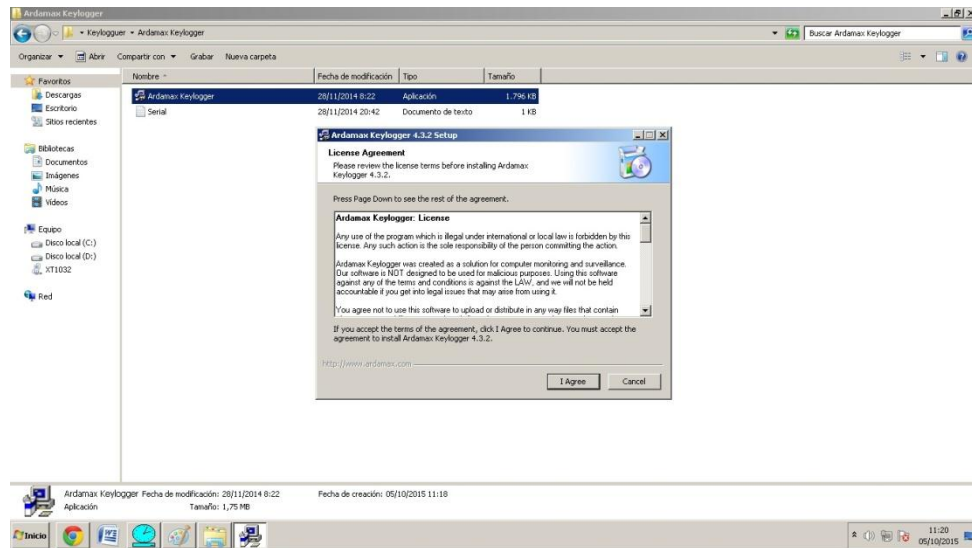


Imagen 136 (License Agreement)

5. En esta ventana muestra los componentes a instalar, el primero es el Keylogger y el segundo es el visualizador de las pulsaciones del teclado, por lo tanto no se desmarca ninguno, se procede dando click en “Next”. (Ver imagen 137).

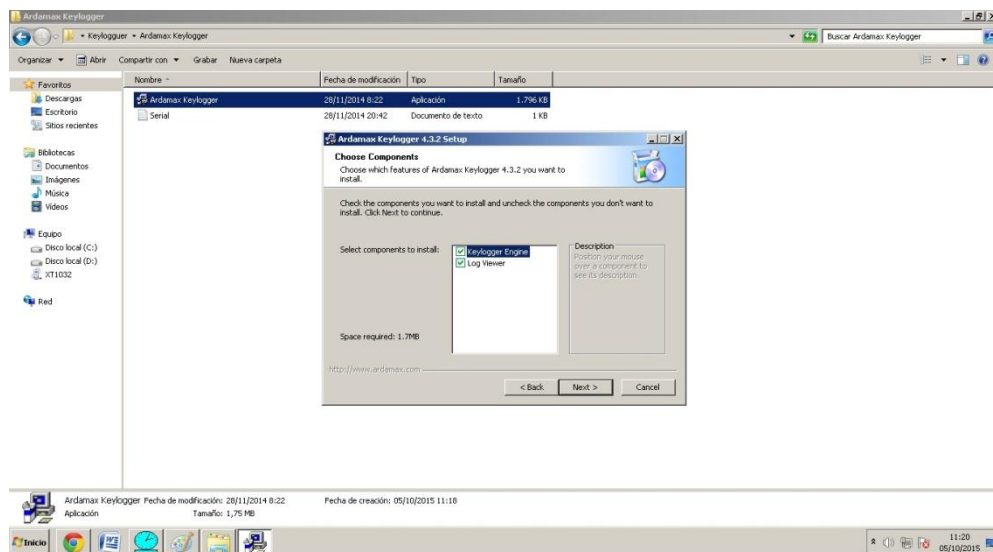


Imagen 137 (Choose Components)

6. Seguidamente saldrá la ventana donde se designa la localización de la instalación, se deja la predeterminada del programa y se da click en “Install”.
- (Ver imagen 138).

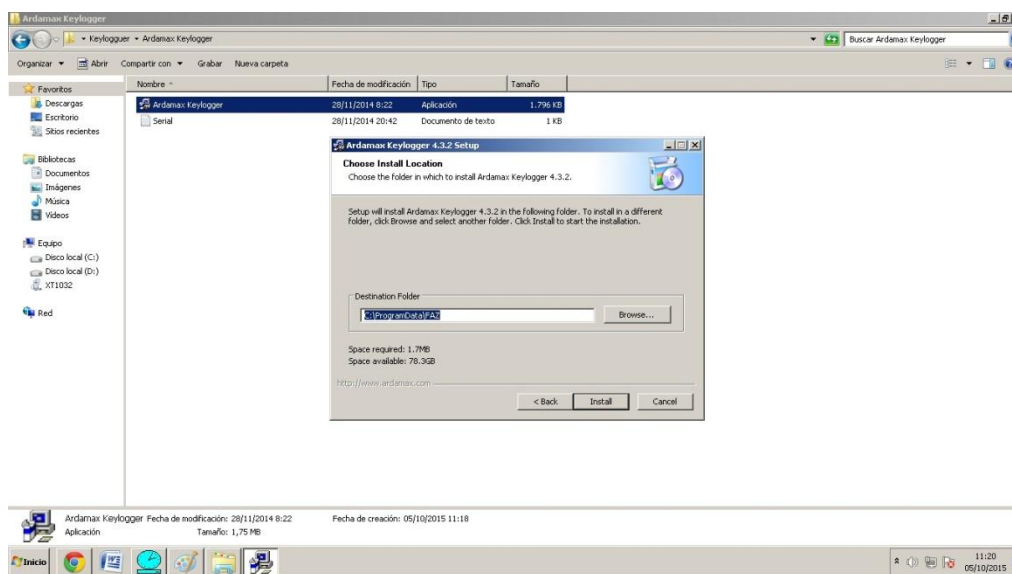


Imagen 138 (Choose Install Location)

7. A continuación empezará el proceso de instalación de los componentes. (Ver imagen 139).

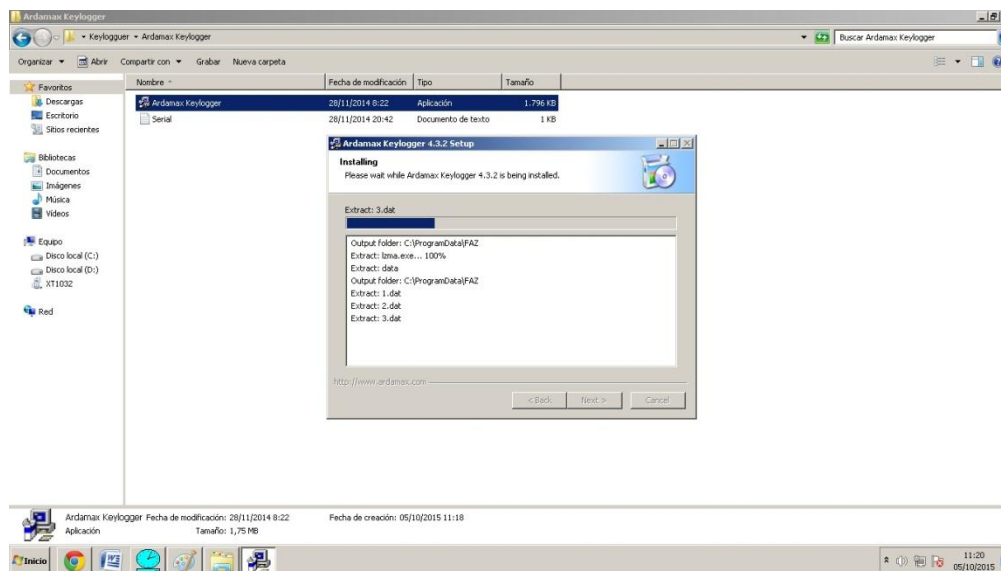


Imagen 139 (Install)

- Después de la instalación saldrá la ventana indicando que se completó correctamente el proceso, para finalizar se marca la casilla “Run Ardamax Keylogger” para que se abra el programa y luego se da click en “Finish” para salir del asistente de instalación. (Ver imagen 140).

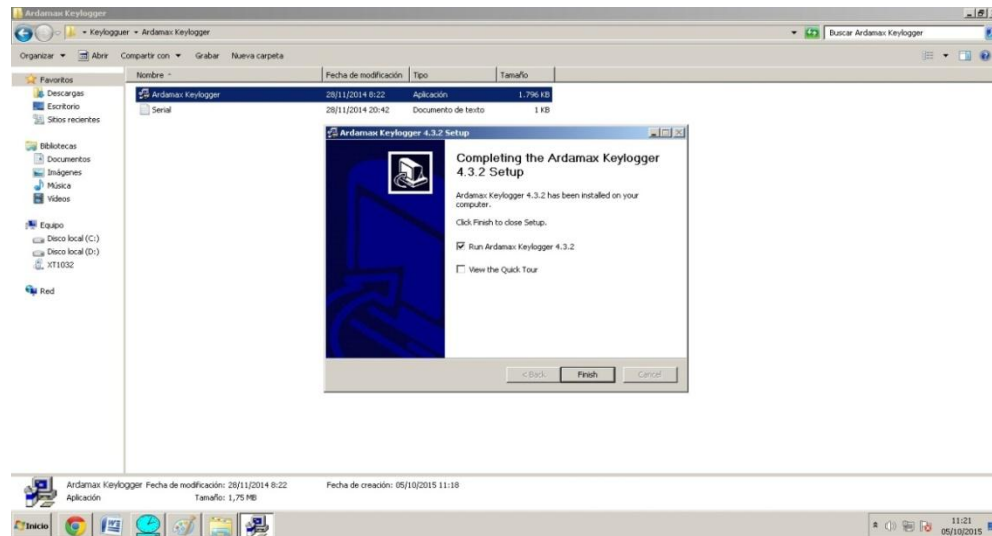


Imagen 140 (Completing the Ardamax Keylogger)

Ahora se procederá a activar el programa (Solo para fines académicos)

- En la barra de tareas activas se busca el icono del keylogger (Tiene forma de triángulo, color amarillo con un ojo en medio) se da click en “Enter registration key” (Ver imagen 141).

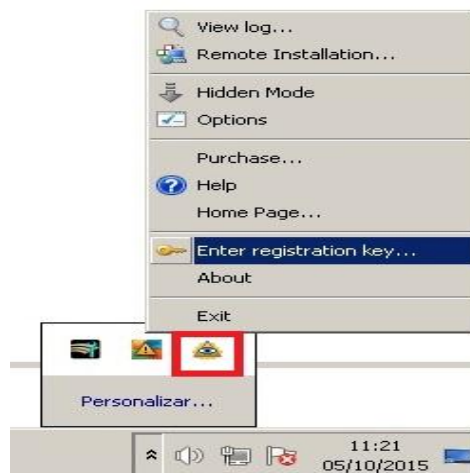


Imagen 141

2. Se ingresa a la unidad de CD, luego a la carpeta programas, después a la carpeta Keyloggers, luego a la carpeta Ardamax Keylogger y luego se abre el documento llamado “Serial” que guarda el nombre de registro y la licencia, se copia el nombre de registro y se pega en la ventana de activación del programa, el mismo proceso de copiado y pegado se repite con el Key del programa, cuando ya estén los campos completos se da click en “Ok” (Como se muestra en la imagen 142).

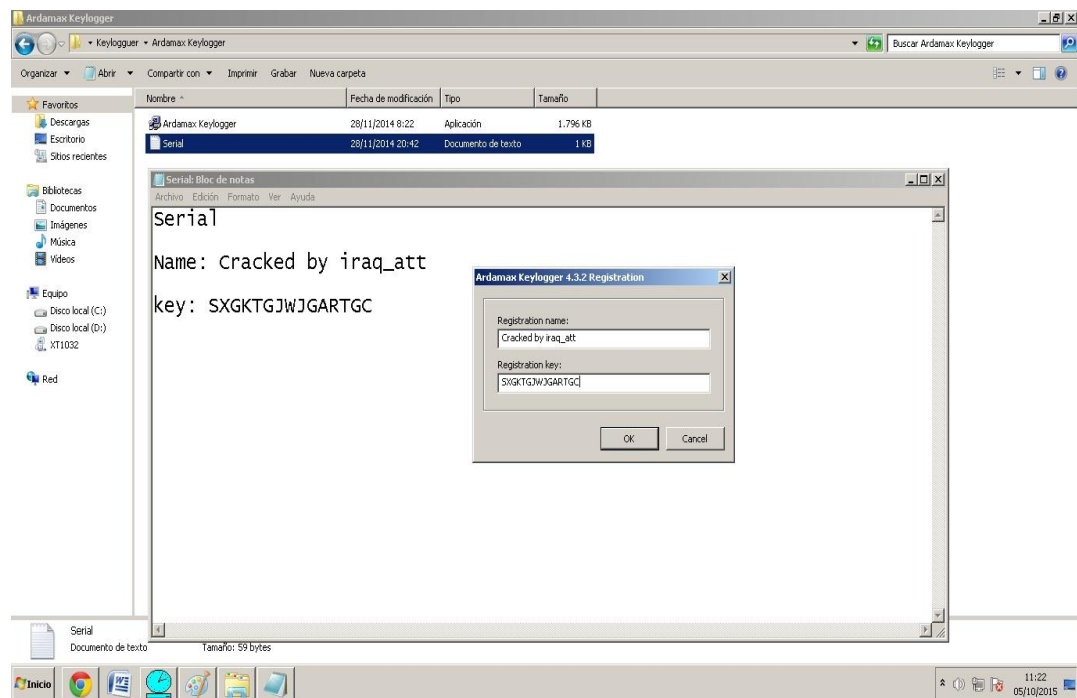


Imagen 142

3. Luego saldrá un cuadro confirmando que el programa quedo activado, se click en “Aceptar”. (Ver imagen 143).



Imagen 143

Configuración y uso de Ardamax Keylogger (Se realizara una prueba para que los datos introducidos en la PC. Del sospechoso se envíen por correo electrónico)

1. En la barra de tareas activas se busca el icono del keylogger (Tiene forma de triángulo, color amarillo con un ojo en medio) se da click en “Options” (Ver imagen 144).

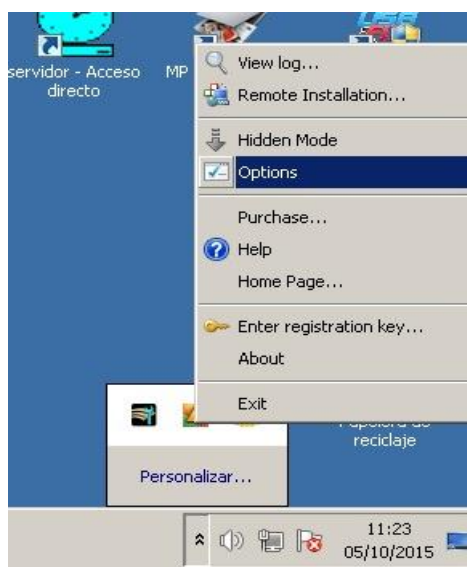


Imagen 144

2. Se procederá a cambiar el idioma del programa a español, una vez abierto se da click en “Options”, seguidamente se da click en “Interface Language” y se selecciona la opción “Español (Argentina)” y se da click en aceptar. (Ver imagen 145).

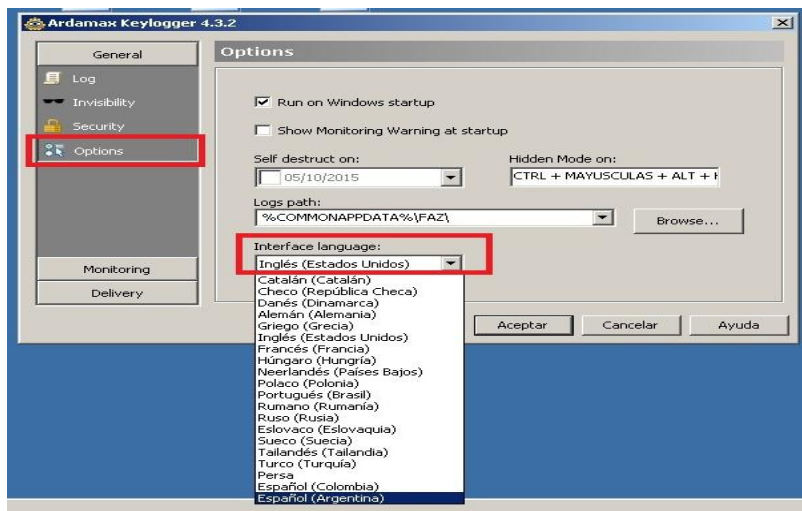


Imagen 145

3. Seguidamente saldrá un cuadro indicando que se debe reiniciar el programa para aplicar el nuevo idioma, se da click en aceptar. (Ver imagen 146).

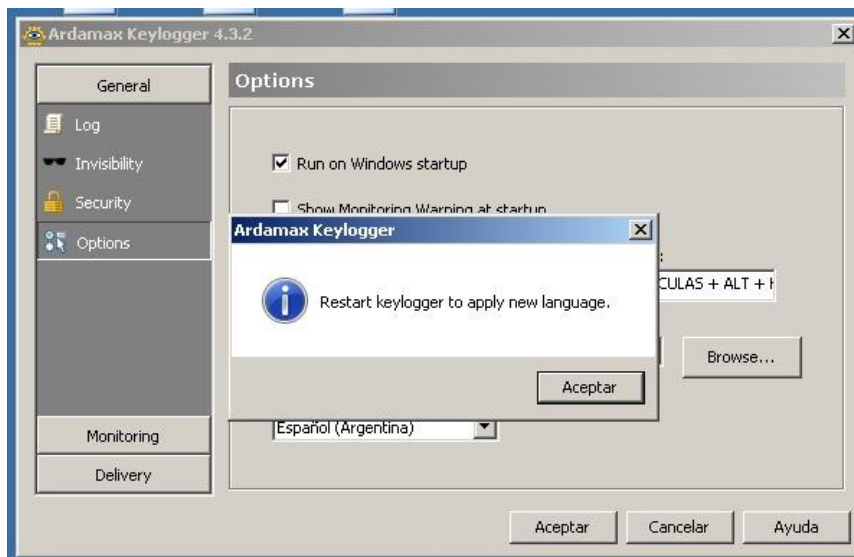


Imagen 146

4. Para reiniciar el programa se dirige a la barra de tareas activas, se busca el icono del programa y se da click derecho para que desplegué el menú, luego se da click en “Exit”. (Ver imagen 147).

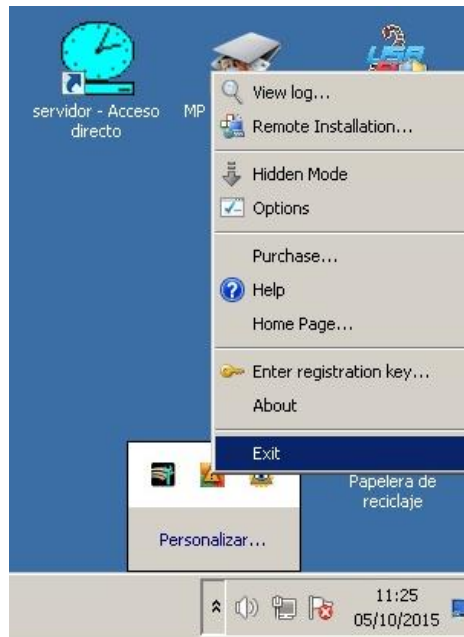


Imagen 147

5. Para abrir nuevamente el programa, se dirige y da click a la barra de inicio, luego se da click sobre el icono del programa. (Ver imagen 148).



Imagen 148

6. Nuevamente se dirige al panel de tareas activas y da click derecho sobre el icono del programa y luego click en “Opciones” como se puede observar el idioma ha cambiado a español. (Ver imagen 149).

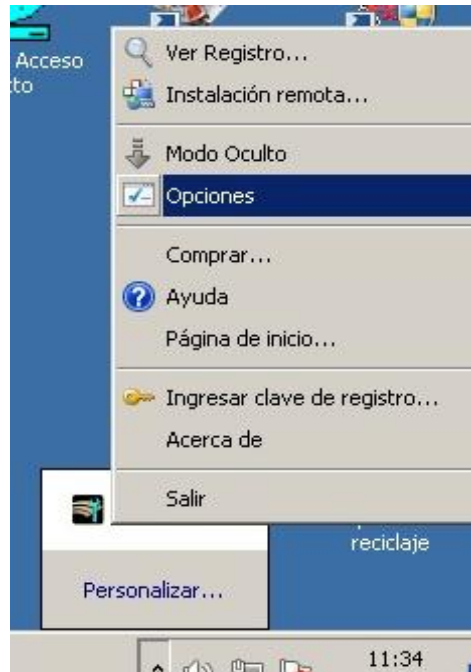


Imagen149

7. Para ocultar el programa del sospechoso, se dirige a la opción de invisibilidad y se marcan la mayoría de las casillas a excepción de la primera “Ocultar icono de la barra de tareas”. (Ver imagen 150).

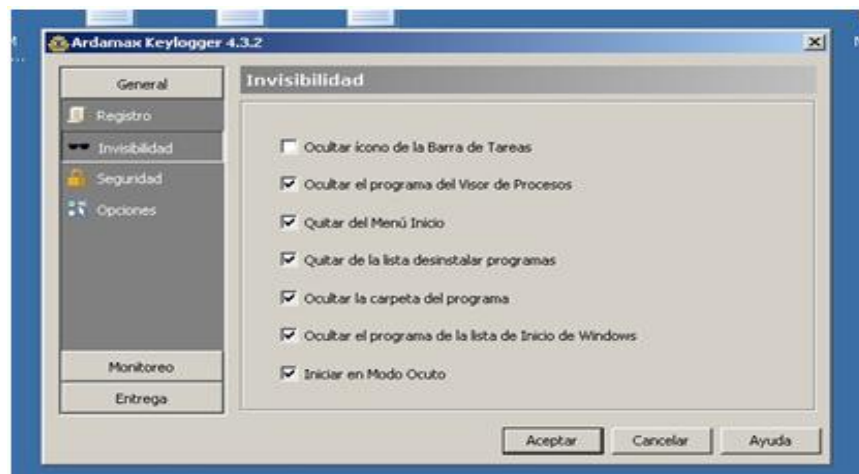


Imagen 150

8. Para configurar el programa para que envíe los registros por correo electrónico se da click en la opción de “Entrega” y luego click en la opción “Email”. En el campo de: “Enviar A:” se escribe la dirección de correo a la cual se quiere recibir el registro de datos, al igual que en el campo “Nombre de usuario” y en el campo de “Contraseña” se pone la contraseña del correo electrónico, por último se realiza una prueba de envío dando click en “Prueba” (Ver imagen 151).



Imagen 151

9. Seguidamente saldrá un cuadro indicando que la prueba fue realizada con éxito y pide revisar el correo electrónico. (Ver imagen 152).

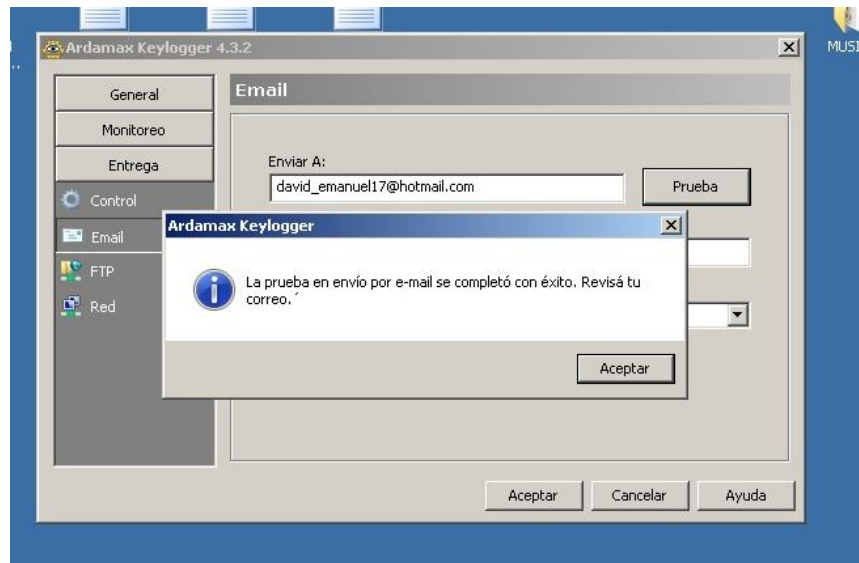


Imagen 152

10. Para verificar que el programa envía los registros se abre el navegador y se ingresa al correo electrónico. (Ver imagen 153).

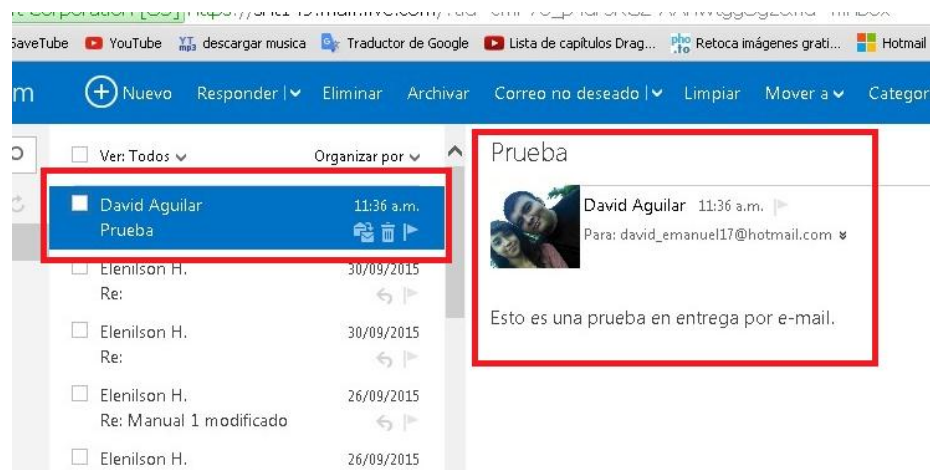


Imagen 153

11. Para configurar el tiempo de envío de los registros, se da click en la opción “Control” y se marca la casilla “Enviar registros cada” y al costado derecho se pone el tiempo de envío y luego se da click en “Aceptar”. (Ver imagen 154).

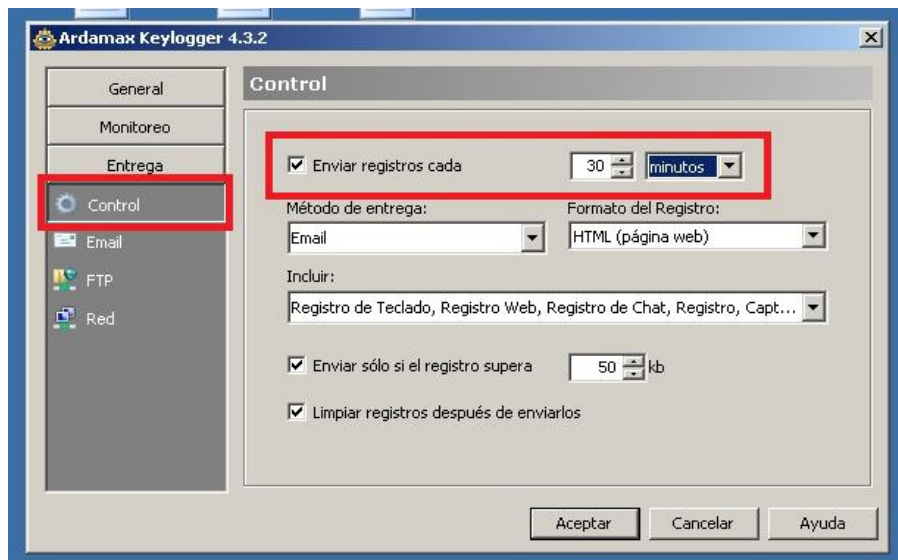


Imagen 154

12. Se realizara una segunda prueba para obtener la dirección de correo electrónico y contraseña del sospechoso. Se abre el navegador y se entra a la página de Facebook, ahí se pondrá el correo electrónico y la contraseña. (Ver imagen 155).



Imagen 155

13. Para verificar los datos se accede al correo electrónico, y efectivamente los datos son enviados ahora se tiene el acceso a la cuenta de Facebook del sospecho y se podrá obtener información de él. (Ver imagen 156).

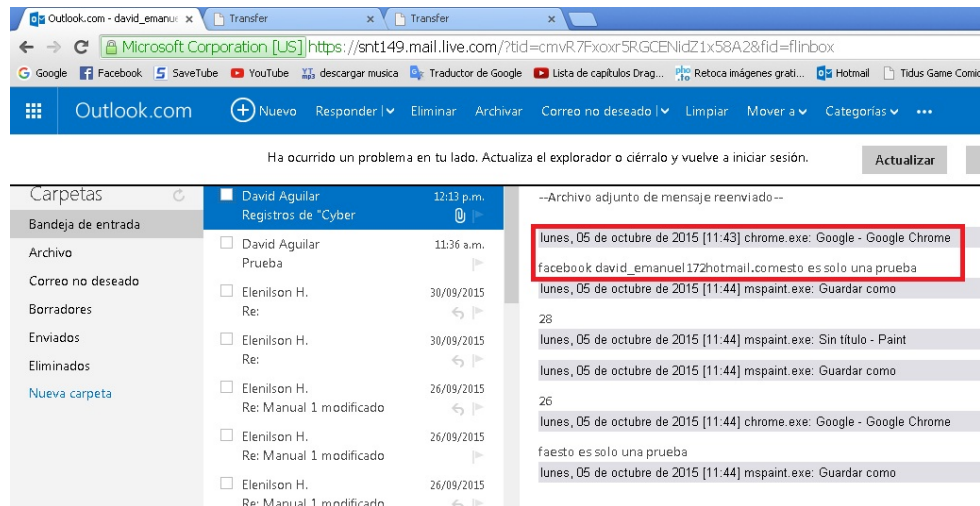


Imagen 156

14. Para verificar los registros ingresados desde la PC. En la cual está instalado el programa, se dirige a la barra de tareas activas y se da click derecho sobre el icono del programa, luego en la opción “Ver Registro”. (Ver imagen 157).



Imagen 157

15. Seguidamente saldrá una ventana mostrando los registros de la PC. (Ver imagen 158).

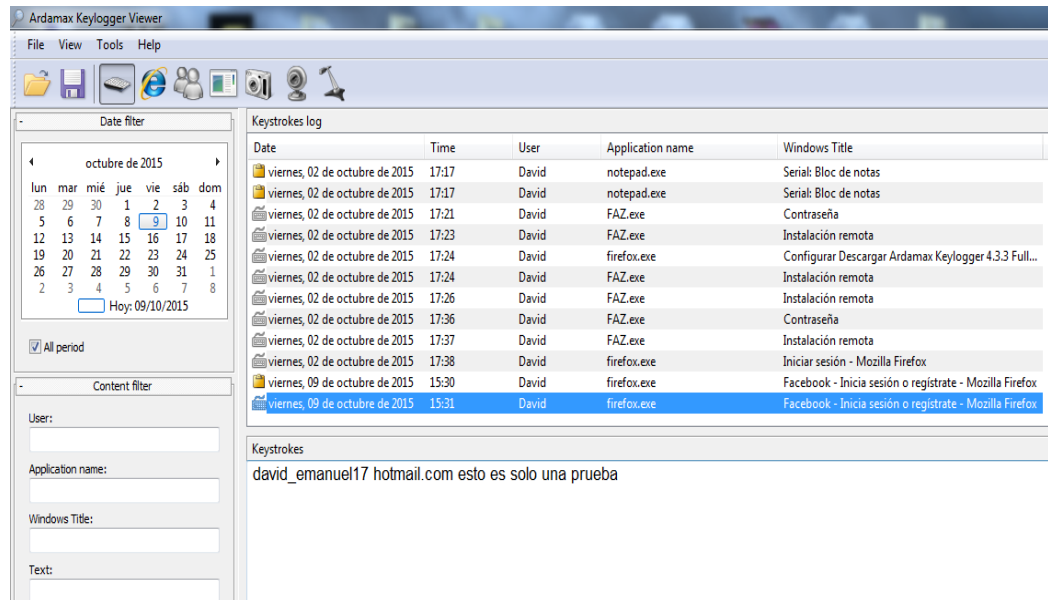


Imagen 158

2.2.10. Manual de uso de Revealer Keylogger

(Para la instalación del programa se debe desactivar el antivirus)

Nota: Para el uso de este programa es necesario estar dentro de una cuenta de administrador, este programa es compatible desde Windows XP hasta Windows 7. En esta ocasión se realizará en sistema operativo Windows 7.

1. Se procederá a desactivar el antivirus, en la barra de tareas activas, se busca el icono del antivirus, en este caso se está utilizando el antivirus AVG, una vez localizado se da click derecho sobre el icono del antivirus y se da click en “Deshabilitar la protección AVG temporalmente” (Ver imagen 159).

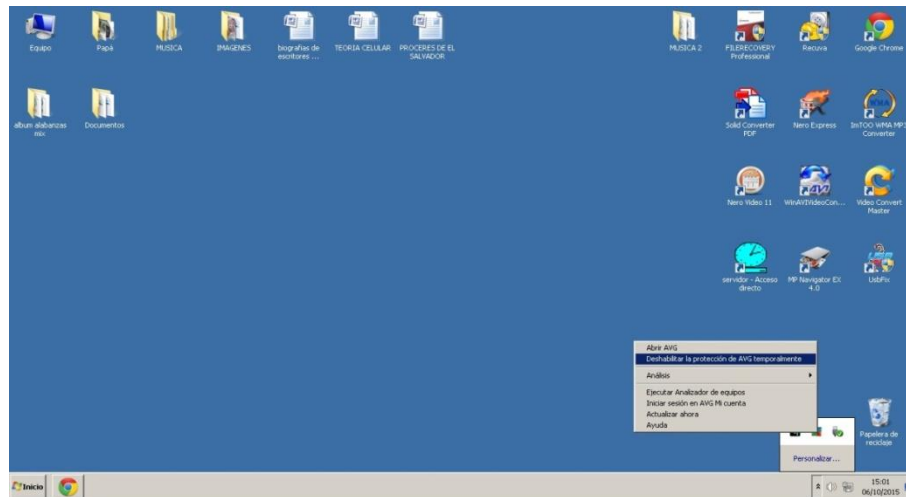


Imagen 159

2. Luego saldrá la ventana de deshabilitar protección de AVG temporalmente, se elige la opción de 15 minutos y se da click en aceptar. (Ver imagen 160).

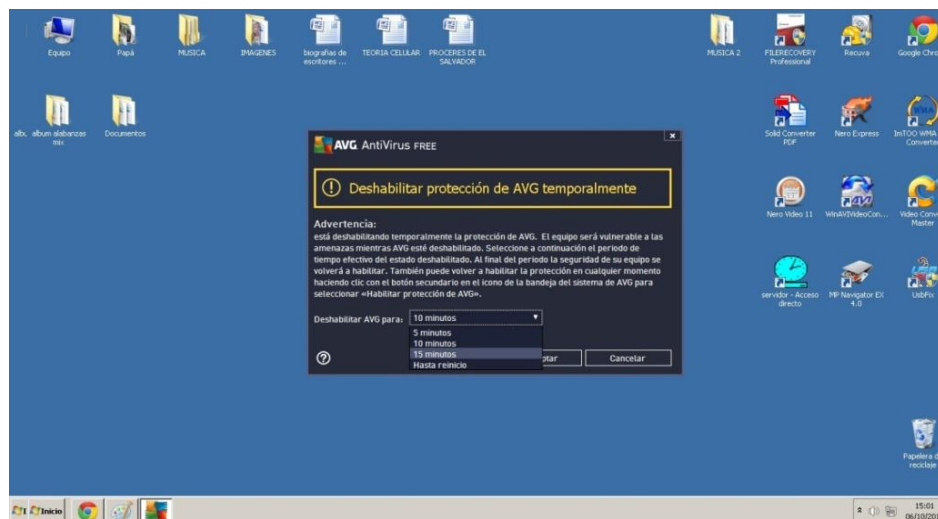


Imagen 160

3. Una vez abierto el CD de herramientas, se da click en programas, luego en Keyloggers, y se da click en el Revealer Keylogger. (Ver imagen 161).

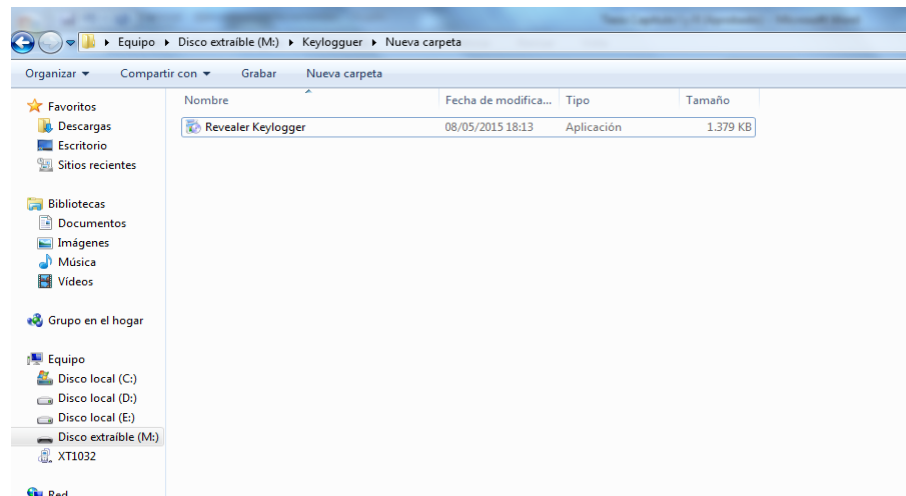


Imagen161

4. Seguidamente saldrá la ventana de instalación se da click en "Instalar ahora" (Ver imagen 162).

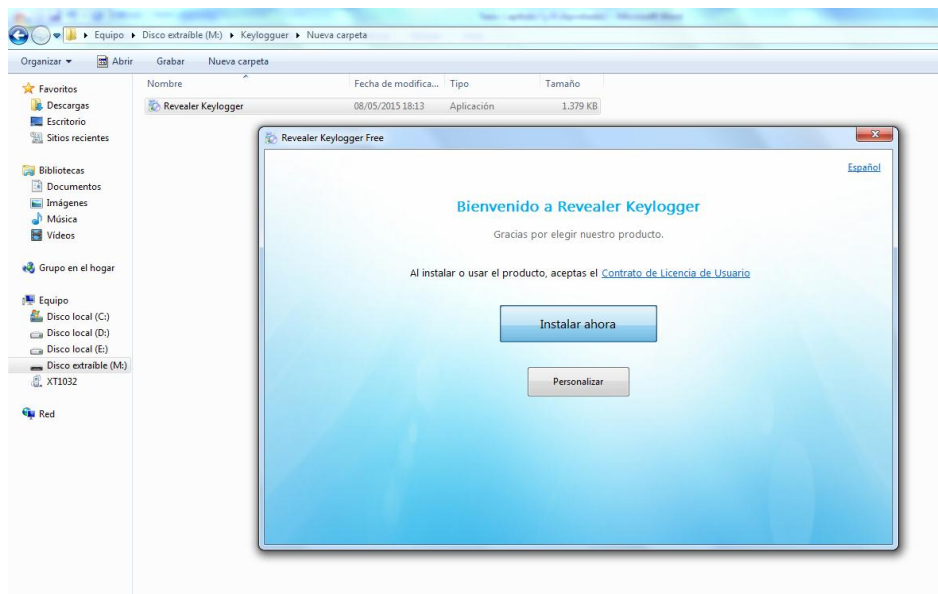


Imagen 162

5. Seguidamente empezara con el proceso de instalación. (Ver imagen 163)

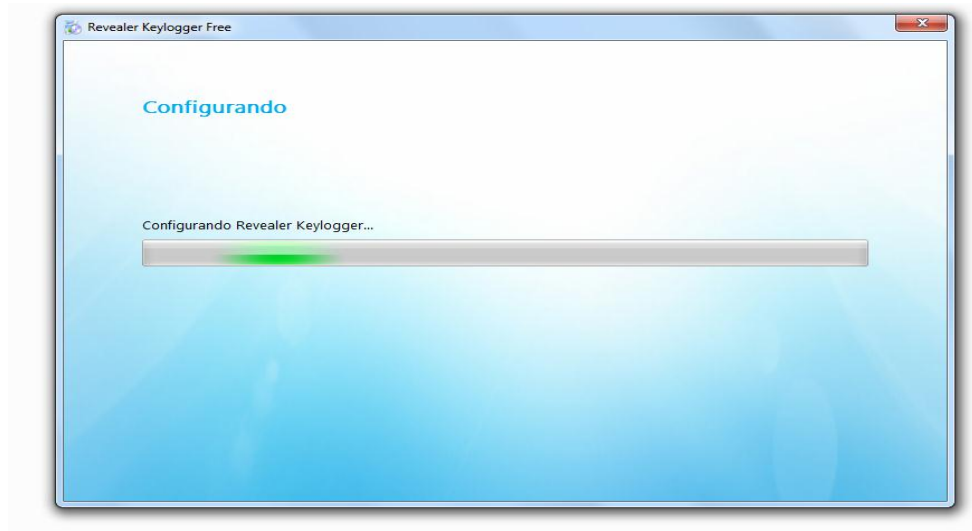


Imagen 163

6. Una vez finalizada la instalación el programa abrirá automáticamente su ventana principal, para que el programa empiece a capturar los datos se da click en la opción "Inicio". (Ver imagen 164).

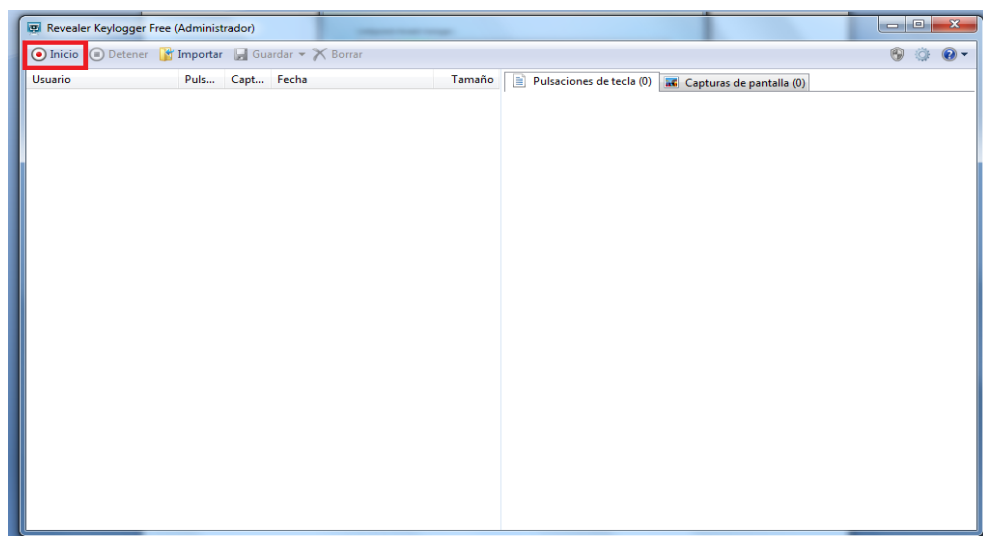


Imagen 164

7. Luego se cierra el programa y permanecerá oculto, antes de cerrarse por completo mostrara una ventana donde indica que se estará ejecutando en segundo plano y la combinación de teclas para volver a abrirlo las cuales son: "CTRL+ALT+F9" se da click en "aceptar" y empezara con la captura. Ver imagen 165).

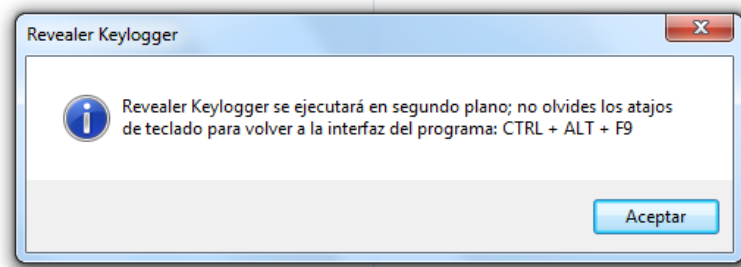


Imagen 165

8. Cuando se quiera revisar lo que el programa a capturado se presiona la combinación de teclas "CTRL+ALT+F9" enseguida abrirá la ventana principal mostrando los datos obtenidos, se da click en nombre de usuario y al costado derecho mostrara la información obtenida. (Ver imagen 166).

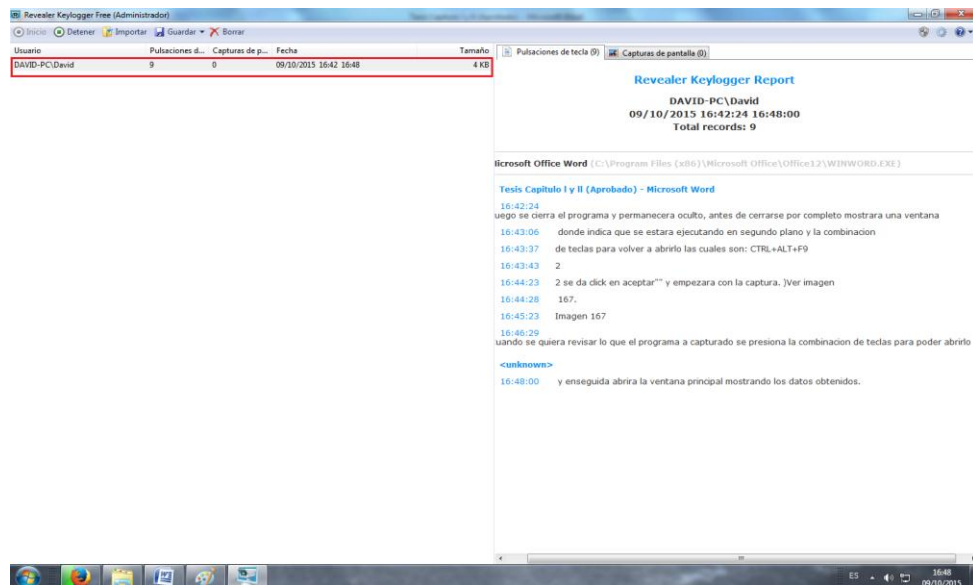


Imagen 166

2.3. Marco Teórico Conceptual

Archivos perdidos: Es la eliminación de archivos digitales.

Administradores: Es la persona que tiene la responsabilidad de implementar, configurar, mantener, monitorizar, documentar y asegurar el correcto funcionamiento de un sistema informático.

Ataques informáticos: Es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático ordenador, red privada.

Actos ilícitos: Son aquellos hechos humanos voluntarios, que son los que se efectúan con discernimiento intención y libertad, pero que son contrarios a lo dispuesto por las normas jurídicas.

Anómalos: Se usa para designar todo aquello que está fuera de lo que se considera como normal, ya sea en su aspecto o en su funcionamiento.

Árbol de directorios: Forma de mostrar todos los directorios de una unidad de almacenamiento (como un disco duro) en forma de estructura de árbol.

Backups: Es una copia o respaldo de archivos importantes, en caso de que se dañen los originales.

Contraseñas simples: Es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso.

CD interactivo: Se presente una pantalla que ofrece distintas rutas para explorar el Contenido del CD. El contenido se presenta a través de distintos lenguajes y formatos, se trabaja desde videos, audios hasta documentos de texto, fotografías y animaciones.

Ciber delincuencia: Se define con carácter general como cualquier tipo de actividad ilegal en la que se utilice Internet, una red privada o pública o un sistema informático doméstico.

Clonado de discos duros: Estaciones de acoplamiento y duplicadores independientes para proporcionar acceso externo a unidades de disco duro fácil y rápidamente, y clonar discos sin necesidad de software ni instalaciones en el ordenador.

Criminalidad informática: Es toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Chantaje: Es la amenaza de difamación pública o daño semejante para obtener algún provecho.

Crack: Un crack informático es un parche cuya finalidad es la de modificar el comportamiento del software original y creado sin autorización del desarrollador del programa.

Datos informáticos: Cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función.

Delitos informáticos: Un delito informático es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Delitos: Supone una conducta de infracción del derecho penal, es decir, una acción u omisión tipificada y penada por la ley.

Disco duro en modo de unidad extraíble: Es cuando se extrae el Disco duro del ordenador y por medio de hardware diseñado para ese fin, se puede tener como una memoria USB. Por medio de un adaptador ya sea IDE, o SATA.

Datos de una raíz: Generalmente representa la totalidad de un solo disco. No obstante, un directorio raíz puede representar sencillamente un sistema de archivos en particular; de varios que puede haber en un mismo dispositivo de almacenamiento.

Disco RAM: Es una unidad de disco que usa una zona de memoria RAM del sistema como almacenamiento secundario en lugar de un medio magnético.

Evidencias informáticas: Es una denominación usada de manera amplia para describir cualquier registro generado o almacenado en un sistema computacional que puede ser utilizado como prueba en un proceso legal.

Evidencias digitales: Es información almacenada o transmitida en formato electrónico.

Estructura de archivos: Es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene. A los archivos informáticos se les llama así porque son los equivalentes digitales de los archivos escritos en libros, tarjetas, libretas, papel o microfichas del entorno de oficina tradicional.

Fraude: Es una acción que resulta contraria a la verdad y a la rectitud. El fraude se comete en perjuicio contra otra persona o contra una organización.

Falsificación: Es un acto consistente en la creación o modificación de ciertos documentos, efectos, productos bienes servicios, con el fin de hacerlos parecer como verdaderos.

Fichero: Es un sistema real o virtual de organización de la información mediante una clasificación determinada.

Gráficos en tiempo real para analizar las contraseñas: Es una herramienta para modificar las contraseñas de Windows y posee una interfaz gráfica de usuario.

Gusano: Es un malware que tiene la propiedad de duplicarse a sí mismo.

Heurística avanzada: En los productos antivirus se conoce como heurística a las técnicas que emplean para reconocer códigos maliciosos (virus, gusanos, troyanos, etc.) que no se encuentren en su base de datos (ya sea porque son nuevos, o por no ser muy divulgados). El término general implica funcionalidades como detección a través de firmas genéricas, reconocimiento del código compilado, desensamblado, desempaquetamiento, entre otros.

Hurto de información personal: Es la apropiación de la identidad de una persona: hacerse pasar por esa persona, asumir su identidad ante otras personas en público o en privado, en general para acceder a ciertos recursos o la obtención de créditos y otros beneficios en nombre de esa persona.

Hashes: Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que *solo* puede volverse a crear con esos mismos datos).

Hackers: Es una persona o a una comunidad que posee conocimientos en el área de informática y se dedica a acceder a sistemas informáticos para realizar modificaciones en el mismo.

Interfaz: Se utiliza para nombrar a la conexión física y funcional entre dos sistemas o dispositivos.

Internet: Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP.

Informática forense: Es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

ID: Es un nombre o número de identificación de un usuario de un sistema.

Imagen de disco: Una imagen de disco es un archivo o unos dispositivos que contiene la estructura y contenidos completos de un dispositivo o medio de almacenamiento de datos, como un disco duro, un disquete o un disco óptico.

Identificación de ataques: Es cuando el atacante busca vulnerabilidades en el sistema operativo o una red inalámbrica o en una red social.

Licencia free: Es el software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Es decir, el software libre es una cuestión de libertad, no de precio.

Malversación de caudales públicos: Efectos públicos, también denominado el consentimiento para que ésta se verifique, o su aplicación a usos propios o ajenos por parte de quien los tenga a su cargo.

Litigios: Es un conflicto de intereses calificado y elevado a una autoridad jurisdiccional por un sujeto de derecho con una intención o pretensión contra otro que manifiesta una resistencia o que se opone al planteamiento del primero.

Logs: Es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué.

Módulo: Porción de un programa de ordenador tareas que debe realizar un programa para cumplir con su función u objetivos.

Mp3: Formato de compresión digital para la transmisión rápida de archivos de audio y vídeo a través de Internet.

Micro SD: Es un formato para tarjetas de memoria flash derivado del Trans Flash de SanDisk. Es especialmente usado en teléfonos móviles, dispositivos GPS portátiles, reproductores de MP3, consolas de videojuegos y unidades de memoria USB.

Memoria RAM: Es un tipo de memoria de ordenador a la que se puede acceder aleatoriamente; es decir, se puede acceder a cualquier byte de memoria sin acceder a los bytes precedentes. La memoria RAM es el tipo de memoria más común en ordenadores y otros dispositivos como impresoras.

Modus operandi: Es la forma en la que opera un delincuente

Manual digital: Es una versión digital de un libro de texto es accesible en soportes digitales, como un ordenador, una tableta, una pizarra digital interactiva

Módulo de fuerza bruta: Es la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso

Malware: Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario

Máquina virtual: Es un software que simula a una computadora y puede ejecutar programas como si fuese una computadora real.

Ordenadores: Es una máquina programable. Responde a un sistema específico de instrucciones de una manera bien definida. Puede ejecutar una lista de instrucciones pregrabadas.

Partición: Es el nombre genérico que recibe cada división presente en una sola unidad física de almacenamiento de datos. Toda partición tiene su propio sistema de archivos.

Programación: Es el proceso de diseñar, codificar, depurar y mantener el código fuente de programas.

Pruebas digitales: Son aquellas que se obtienen directamente desde un medio digital.

PDFS maliciosos: Es un archivo infectado por software malicioso.

Registro de Windows: Es una base de datos jerárquica que almacena los ajustes de configuración y opciones en los sistemas operativos.

Rootkits: Permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.

Rogue: Es un tipo de programa informático malintencionado cuya principal finalidad es hacer creer que una computadora está infectada por algún tipo de virus, induciendo a pagar una determinada suma de dinero para eliminarlo.

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Spyware: Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

USB: Es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información.

2.4. Documentación Técnica.

2.4.1 Documentación técnica de RegSeeker

Es una herramienta con la cual puedes hacer una excelente gestión o manejo del registro de Windows de una manera muy sencilla y con opciones bastante interesantes sin necesidad de realizar la instalación del programa ya que permite ser ejecutado como un programa portable.

- Permite editar fácilmente el registro con unos pocos clics.
- Se puede acceder a diferentes passwords guardados en el registro.
- Desinstalar programas de raíz para que no quede ningún rastro de ellos.
- Permite limpiar el registro de Windows con solo un clic.
- Aplicación para la extracción, la correlación, y muestra la información del registro.
- Permite obtener de forma gráfica datos del sistema, usuarios y aplicaciones partiendo del registro.

2.4.2. Documentación técnica de RegCleaner

Es un software que se especializa en una sola tarea: la eliminación de archivos basura del Registro de Windows. Su funcionamiento es automatizado, por lo que una vez instalado comenzará con sus labores inmediatamente. El usuario puede consultar los resultados, o los procesos en tiempo real, con solo unos cuantos clics.

- Analizar el registro de Windows para verificar si hay errores, daños o elementos obsoletos.
- Limpiar el registro de Windows de basura.
- Repara daños en el registro.
- Solucionar errores.
- Optimiza el registro

2.4.3. Documentación técnica de Malware Bytes Anti-Malware

El producto insignia de Malware bytes Corporación, empresa con base en estados unidos la cual se está posicionando muy fuertemente en el mercado de la seguridad informática; es una potente herramienta para detectar y remover todo rastro de malware no detectado por sistemas antivirus. Funciona en Windows y cuenta con un buen rango de detección, es muy sencillo de usar y no pesa mucho.

- Módulo de protección residente en tiempo real.
- Anti-Rootkit integrado en el escáner.
- Tecnología de exploración y detección heurística avanzada.
- Sistema de cuarentena, para enviar el borrado de falsos positivos.
- Lista de elementos ignorados para el escáner y la protección del módulo.
- Compatible totalmente con cualquier software Antivirus y Antispyware.
- Integración en el menú contextual para escanear archivos bajo demanda.
- Tres tipos de escaneo: análisis rápido, análisis personalizado y análisis Completo.

2.4.4. Documentación técnica de NTPWEDIT

Es una herramienta gratuita que le permite restablecer una contraseña de Windows sin saber la contraseña de administrador. Por supuesto, esto sólo funciona si tiene acceso a la instalación fuera de línea y de arranque de Windows a partir de un segundo sistema de Windows. 7.

- Permite cargar el fichero SAM que contiene los datos de usuario y contraseña de inicio de sesión en Windows.
- Es posible sobrescribir la contraseña de un usuario o administrador y poder así iniciar nuevamente sesión cuando se ha perdido la contraseña.
- Elimina o modifica contraseñas de usuarios de usuarios Windows, colocando el disco duro en modo de unidad extraíble.

2.4.5. Documentación Técnica de Ardamax Keylogger

Es un excelente y poderoso registrador del teclado que guarda cualquier actividad que realiza el propio usuario. Esta información queda archivada, por tanto, es por tanto, la herramienta ideal para conocer qué hace tu ordenador mientras estás ausente.

- Excelente y poderoso registrador de teclado que guarda cualquier actividad que realiza el propio usuario.
- Herramienta ideal para conocer qué hace tu ordenador mientras estás ausente.
- Mantiene una copia de seguridad de todos los datos mecanografiados de forma automática.
- Eficaz herramienta de supervisión a los hijos.

- Puede utilizarse como un dispositivo de vigilancia para detectar accesos no autorizados.
- Envía informes por correo electrónico.
- Genera todo tipo de informes sobre las direcciones de Internet que el usuario ha visitado en un momento determinado.
- Su acceso está protegido por contraseña.
- Trabaja en un modo oculto y seguro.
- Es absolutamente invisible y almacena la información y las aplicaciones por fechas.
- Interfaz muy amigable y muy fácil de utilizar.

2.4.6. Documentación Técnica de Revealer Keylogger

Es una utilidad que te permitirá controlar y grabar todos los textos que se introducen en un ordenador. Textos como páginas web, conversaciones e incluso usuarios y contraseñas.

Concretamente, Revealer Keylogger se encarga de registrar cualquier texto, ya sea un texto introducido en el navegador, en un e-mail, en un documento o en un programa de mensajería como MSN, GTalk, Skype o Facebook. Revealer Keylogger lo guarda todo

- Función de pantallazos automáticos
- Monitoreo remoto
- Modo invisible
- Captura las pulsaciones del teclado

- Puede utilizarse por cualquier usuario, independientemente del nivel de aprendizaje que éste tenga.
- Requiere de una conexión a Internet correctamente configurada para su instalación.
- No necesita de requisitos adicionales para su instalación y funcionamiento.
- Compatible con algunas versiones existentes de Windows.

2.4.7. Documentación Técnica de FILERECOVERY Professional

Recupera tus archivos, fotos, música y vídeos desde casi cualquier tipo de pérdida de datos. Recupera datos desde volúmenes dañados, borrados o corruptos, FILERECOVERY Professional ofrece una interfaz de asistente fácil de usar, permitiendo incluso a los usuarios principiantes recuperar datos.

Tiene la capacidad de analizar todos los volúmenes en un ordenador local y crea un árbol de directorios de archivos perdidos y eliminados. Puedes buscar archivos perdidos y eliminados que cumplen con los criterios del nombre de archivo.

El motor de análisis rápido permite crear rápidamente la lista de archivos con un administrador de tareas fácil de entender y el cuadro de diálogo típico de guardado de archivos.

- Capacidad de analizar todos los volúmenes en un ordenador local y crea un árbol de directorios de archivos perdidos y eliminados.
- Busca archivos perdidos y eliminados que cumplen con los criterios del nombre de archivo.

- Motor de escaneo rápido que permite crear rápidamente la lista de archivos.
- Administrador de tareas fácil de entender y diálogo típico de guardado de archivos.
- Es posible guardar los datos en cualquier unidad, incluyendo las unidades de red, medios extraíbles.

2.4.8. Documentación Técnica de Recuva

Recupera datos de discos corruptos, dañados, y cambiados formato; restaura documentos de Word; y suprime con seguridad archivos así que son irrecuperables, incluso por Recuva.

- Exploración profunda mejorada de NTFS.
- Exactitud mejorada de la estadística de la exploración.
- Cargamento mejorado de la imagen de VHD. (profesional de Recuva solamente).
- Ayuda mejorada de la localización y de la lengua.
- Mejoras menores en la interfaz de usuario.
- Ajustes menores y correcciones.

2.4.9. Documentación Técnica de Browser Password Decryptor

Recuperación de contraseñas de los navegadores. Todos los navegadores tienen una función para almacenar contraseñas, de modo que el usuario no necesita recordar y escribir la contraseña cada vez. Cada uno de ellos utiliza sus propias normas y su propio mecanismo de cifrado de almacenamiento para almacenar contraseñas. Browser Password Decryptor escanea automáticamente cada uno de estos navegadores y al instante recupera todas las contraseñas de inicio de sesión almacenados en el sitio web.

- Recupera de forma instantánea y descifra contraseñas almacenadas en forma cifrada en los navegadores web más populares.
- Recupera contraseñas de cualquier longitud y complejidad.
- Guardar los datos recuperados pueden ser en HTML / XML / TXT.

2.4.10. Documentación Técnica de Web Browser Pass View

Es una herramienta de recuperación de contraseña que revela las contraseñas almacenadas por los siguientes navegadores web: Internet Explorer (Versión 4.0 - 11.0), Mozilla Firefox (todas las versiones), Google Chrome, Safari y Opera. Esta herramienta se puede utilizar para recuperar su contraseña perdida olvidada de cualquier sitio web, incluyendo sitios web populares, como Facebook, Yahoo, Google y Gmail, siempre y cuando la contraseña es almacenada por su navegador Web.

- Esta utilidad funciona en cualquier versión de Windows, a partir de Windows 2000, y hasta Windows 10, incluidos los sistemas de 64 bits. Las versiones anteriores de Windows (Windows 98 / ME) no son compatibles, ya que esta utilidad es una aplicación Unicode.
- En Internet Explorer 7,0-9,0, las contraseñas se cifran con la URL del sitio Web, por lo Web Browser Pass View utiliza el archivo de historia de Internet Explorer para descifrar las contraseñas. Si borra la historia de Internet Explorer, Web Browser Pass View no será capaz de descifrar las contraseñas.

Capítulo III

Desarrollo de la solución

3.1. Propuesta de solución

Con la elaboración de este proyecto se pretende ayudar y reforzar las competencias de los estudiantes siendo un material de apoyo extra en actividades de diplomados, proporcionando temas prácticos y teóricos que permitan mejorar el desarrollo y la competitividad que los estudiantes necesitan dominar en aspectos de la informática forense como:

- ✓ Eliminación y modificación de contraseñas de usuarios de Windows
- ✓ Recuperación de archivos borrados
- ✓ Análisis y protección anti malware
- ✓ Keyloggers
- ✓ Análisis y limpieza del registro de Windows
- ✓ Recuperación de contraseñas guardadas en navegadores Web.

Se pretende reforzar los conocimientos en esta área de informática para que los estudiantes del técnico en ingeniería de hardware de la Universidad Tecnológica de El Salvador, estén a un nivel aceptable de la informática forense.

Para ello se ha diseñado un kit de herramientas de Informática Forense en un CD interactivo el cual, contendrá programas para cumplir con las necesidades de los aspectos antes mencionados, así como también contendrá para cada programa su

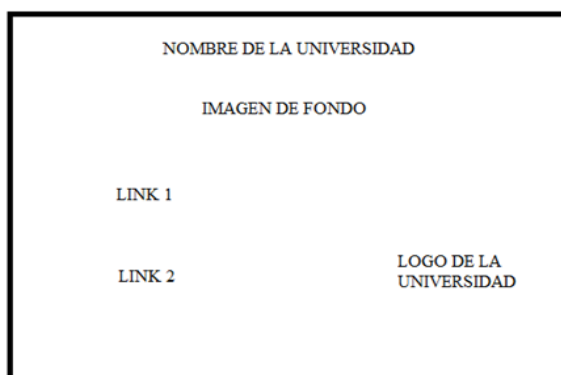
respectivo manual de instalación y uso, siendo este un material de apoyo extra para los estudiantes.

Para la selección de las herramientas de software que se incluyen en el CD se realizó un proceso de identificar cuáles eran las herramientas básicas y más accesibles para los usuarios, luego de identificar dichas herramientas se seleccionaron por medio de una evaluación económica las herramientas más factibles para los estudiantes, seguidamente se hace una evaluación técnica para seleccionar las herramientas que más cumplan con el propósito de los aspectos anteriormente seleccionados, para ser incluidas en el CD interactivo.

El presente CD Interactivo se realiza para los estudiantes que deseen participar en los diplomados de informática forense de la Universidad Tecnológica de El Salvador, ya que resulta imprescindible que los estudiantes fortalezcan sus conocimientos en dicha área de manera práctica y teórica ya que en el país no existen instituciones que brinden ese tipo de conocimiento tan profundamente, por otra parte el uso correcto de la informática forense permite conocer diferentes términos y aplicaciones para realizar, investigaciones y análisis críticos en cualquier equipo informático.

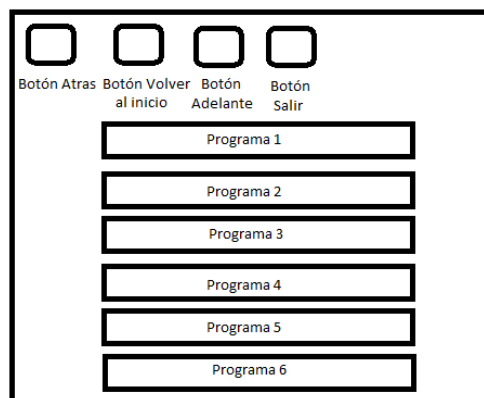
Este responde a la necesidad de mejorar en los estudiantes, las destrezas y habilidades en la informática forense específicamente en las áreas de: Recuperación de archivos borrados, recuperación de contraseñas guardadas en navegadores Web, Keyloggers, modificación o eliminación de contraseñas de usuarios de Windows, análisis y protección anti-malware, análisis y limpieza del registro de Windows.

El presente CD interactivo cuenta con una portada al inicio la cual contiene el nombre de la universidad centrado el cual es: Universidad Tecnológica de El Salvador, con un tipo de letra “Times New Román” tamaño N° 16, además incorpora el logo de la universidad al costado superior derecho, además contará con una imagen de fondo, también contará con 2 link el primero se llama Kit de Herramientas de Informática Forense con tipo de letra “Times New Román” tamaño N° 14, el cual redirigirá a la lista de aplicaciones y el segundo Manuales de Instalación y uso él, con tipo de letra “Times New Román” tamaño N° 14, el cual redirigirá a la lista de manuales incluidos para cada programa, en el apartado de los manuales se incluirá cada uno de los manuales en formato PDF, así como también el instalador de Adobe Acrobat Reader para que pueda ser instalado en dado caso la PC. No lo posea.

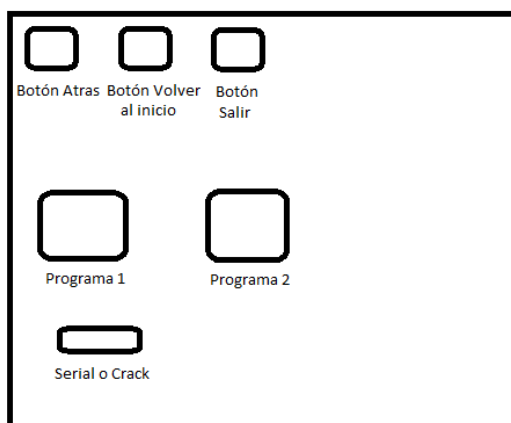


Cuando se de click en el primer link se redirigirá a la lista de los diferentes temas que se han elegido, el título de esa pantalla se llama Kit de Herramientas de Informática Forense estará centrado y el tipo de letra es “Times New Román” con tamaño N°16, los subtemas estarán formando una lista, esta estará con tipo de letra “Times New Román” tamaño N° 12, además contará con un botón con una flecha apuntando hacia la izquierda

que se utilizara para regresar a la pantalla anterior y se ubica al costado superior izquierdo, también contará con un botón en forma de casita cuya función será volver a la portada del CD, también contará con un botón con una flecha apuntando hacia la derecha que se utilizará para avanzar hacia adelante en los submenús del CD y tendrá un botón con la forma del icono apagar de Windows el cual su función será salir del CD.



Una vez se le de click a un determinado subtema redirigirá a los programas seleccionados para dicho subtema, saldrá el programa elegido mediante los cuadros de factibilidades y un programa extra de la misma categoría.



Cuando se seleccione el segundo link para revisar los manuales se redirigirá al listado de subtemas.

The screenshot shows a web interface with a navigation bar at the top containing four buttons: "Botón Atras", "Botón Volver al inicio", "Botón Adelante", and "Botón Salir". To the right of these buttons is a larger, empty rectangular box. Below the navigation bar is a list of six subtopics, each in a rectangular box: "Subtema 1", "Subtema 2", "Subtema 3", "Subtema 4", "Subtema 5", and "Subtema 6". To the right of this list is a larger rectangular box containing the text "Instalador Adobe Acrobat Reader".

Cuando se de click en el sub tema que se ha de elegir saldrán los manuales con el nombre del programa en formato PDF.

The screenshot shows a web interface with a navigation bar at the top containing four buttons: "Botón Atras", "Botón Volver al inicio", "Botón Adelante", and "Botón Salir". To the right of these buttons is a larger, empty rectangular box. Below the navigation bar is a list of two manuals, each in a rectangular box: "Manual 1" and "Manual 2". To the right of this list is a larger rectangular box containing the text "Instalador Adobe Acrobat Reader".

El CD interactivo está compuesto por su pantalla principal la cual contendrá la caratula con el logo de la Universidad Tecnológica de El Salvador, el nombre de la Universidad y dos botones uno el cual re direccionará a la lista de programas incluidos en el kit, y el segundo re direccionará a la lista de manuales por cada programa incluido, en el listado de programas se han incluido los siguientes cada uno para su respectiva área dentro de la informática forense

En el apartado de programas se incluirán los siguientes programas:

En el área de eliminación y modificación de contraseñas de usuarios de Windows, el cual servirá para ingresar a una computadora protegida por contraseña, permitiendo eliminar o modificar dicha contraseña sin necesidad de tenerla. El programa a utilizar en esta área es:

- ✓ NTPWEDIT

En el área de recuperación de archivos borrados, el cual permitirá recuperar archivos borrados ya sea que se han eliminado de la Papelera de reciclaje o que se han perdido por dar formato al disco duro o USB, por corrupción del mismo, por infección mediante un bloqueo inesperado del sistema o por un fallo de software. Los programas a utilizar en esta área son:

- ✓ FilerecoveryProfessional

- ✓ Recuva

En el área de análisis y protección antimalware, se utiliza para escaneos para identificar programas que son o pueden ser maliciosos. El programa a utilizar en esta área es:

- ✓ Malware Bytes

En el área de keyloggers se encargara de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet. Suele usarse como malware del tipo daemon, permitiendo que otros usuarios tengan acceso a contraseñas importantes, como los números de una tarjeta de crédito, u otro tipo de información privada que se quiera obtener. Los programas a utilizar en esta área son:

- Ardamax Keylogger
- Revealer Keylogger

En el área de análisis y limpieza del registro de Windows, Como el Registro es muy sensible a errores, no se puede hacer una limpieza manualmente. Es por eso que se necesita una herramienta para que realice este proceso. Los programas a utilizar en esta área son:

- ✓ RegCleaner
- ✓ RegSeeker

En el área de recuperación de contraseñas guardadas en navegadores Web, permite obtener las contraseñas y guardadas en todos los sitios en los que se ha registrado en los distintos navegadores. Los programas a utilizar en esta área son:

- ✓ Browser Password Decryptor
- ✓ Web Browser Pass View

En el apartado de Manuales se incluirán los siguientes:

Para el área de Keyloggers

- Manual de instalación y uso de Ardamax Keylogger
- Manual de uso de Revealer Keylogger

Para el área de recuperación de archivos borrados

- Manual de instalación y uso de Filerecovery Professional
- Manual de instalación y uso de Recuva

Para el área de recuperación de contraseñas guardadas en navegadores Web

- Manual de instalación y uso de Browser Password Decryptor
- Manual de uso de WebBrowserPassView

Para el área de eliminación o modificación de contraseñas de usuarios de Windows

- Manual de uso de NTPWEDIT

Para el área de análisis y protección anti-malware

- Manual de instalación y uso de Malwarebytes

Para el área de análisis y limpieza del registro de Windows

- Manual de Instalación y uso de Tweak Now Reg Cleaner
- Manual de uso de Reg Seeker

La implementación de este CD será cuando el alumno o encargado de la ponencia del diplomado necesite demostrar el funcionamiento de cada uno de los programas en lo que es el desarrollo del mismo, por ejemplo un uso que se le puede dar es cuando se necesite, iniciar sesión pero está este bloqueada con contraseña de usuario, en ese caso el alumno o docente desmontará el disco duro y lo pondrá de forma externa en otro computador y haciendo uso del CD interactivo se dirigirá al apartado de modificación o eliminación de contraseñas de Windows, otro ejemplo en el que se puede utilizar el CD interactivo es cuando se necesite obtener el correo y contraseña almacenada de un sitio web, para eso se seleccionará la opción de recuperación de contraseñas almacenadas en navegadores Web.

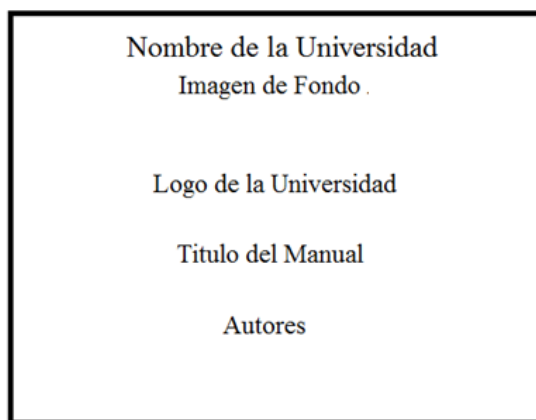
Posteriormente se diseñó un manual el cual se ha desarrollado de una manera específica explicando paso a paso como se utilizará cada programa desde su instalación, configuración y opciones de uso según sea su función específica.

El presente Manual de Instalación se realiza con el propósito de que los estudiantes que deseen participar en los diplomados de informática forense de la Universidad Tecnológica de El Salvador, los estudiantes reciban un apoyo teórico extra sobre la instalación correcta y uso de cada uno de los programas que se encuentran en el kit de

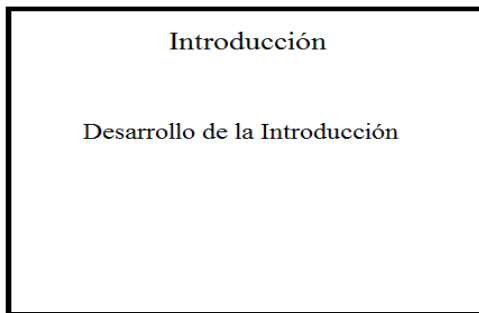
herramientas de informática forense y así fortalecer los conocimientos en dicha área de la informática.

El manual se realiza con el propósito de guiar a cada uno de los estudiantes en lo que es la correcta instalación y activación de cada programa, así como también de orientar en lo que es el uso correcto del mismo.

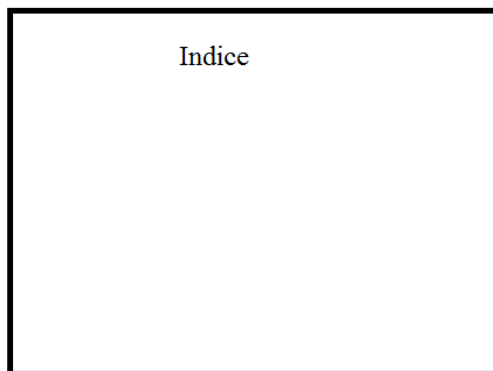
El presente manual de instalación y uso, es creado con Microsoft Office Word 2010, en página tamaño carta cada una numerada, con márgenes superior izquierdo de 4 CM. E inferior derecho de 2.5 CM. E interlineado de 2.0. Cuenta con una portada al inicio la cual contendrá el nombre de la Universidad de forma centrada el cual será: Universidad Tecnológica de El Salvador, con un tipo de letra “Times New Román” tamaño 24 en negrita, además debajo del título de la universidad contendrá el logo de la universidad, debajo del logo ira el título del manual con un tipo de letra “Times New Román” tamaño 20 en negrita, además contiene una imagen de fondo cuenta con una imagen, en el lado inferior centro contiene el nombre de los autores de dicho manual.



La siguiente página cuenta con una introducción al manual cuyo título va con un tipo de letra “Times New Román” tamaño 20 en negrita, y debajo ira el desarrollo de la introducción, con un tipo de letra “Times New Román” tamaño 12



La pagina siguiente cuenta con un indice automático para hacer mas fácil la búsqueda de cada subtema.



La siguiente página del manual contiene, el nombre del título del manual por programa centrado con un tipo de letra “Times New Román” tamaño 14 con negrita, debajo al lado izquierdo lleva una nota previa a la instalación dependiendo si el programa lo amerita, debajo de lo anterior mencionado contiene los pasos de instalación, al centro de la página se encuentra una imagen de referencia y en la parte inferior de la imagen de referencia se ubica el número de la imagen, este puede variar su ubicación estando al costado derecho de la imagen.

Titulo del Manual por Programa
Nota previa antes de la instalación
Pasos de la instalacion
Imagen de Referencia
Numero de la Imagen
Numero de Pagina

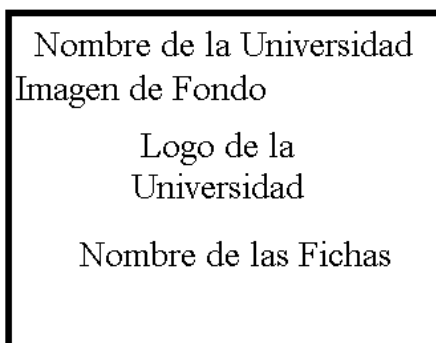
El Manual de Instalación y Uso está compuesto por 95 páginas el cual cada una está orientada al uso correcto de los programas que componen el kit de herramientas de informática forense, ordenada por número de páginas para facilitar la búsqueda al usuario, contara con imágenes demostrativas para una comprensión más fácil. Específicamente en las áreas de: Recuperación de archivos borrados, recuperación de contraseñas guardadas en navegadores Web, keyloggers, modificación o eliminación de contraseñas de usuarios de Windows, análisis y protección anti-malware, análisis y limpieza del registro de Windows.

La implementación de este manual de instalación y uso se lleva a cabo cuando el usuario necesita hacer uso de un programa específico del kit de herramientas de informática forense, por ejemplo el usuario necesita recuperar los archivos borrados de su ordenador para esto se tiene dirigir al manual y ubicarse en el área de recuperación de archivos borrados, el cual contara con dos opciones a elegir las cuales están detalladas por pasos para hacerlo más fácil al momento de usar dicho programa, por lo tanto el usuario podrá elegir cual es más factible para su uso.

Como tercer producto se diseñaron unas fichas técnicas las cuales contienen características de cada uno de los programas, así como también los requisitos mínimos de instalación

Las fichas técnicas se realizaron con el propósito de servir como un segundo material de apoyo extra, para los alumnos de La Universidad Tecnológica de El Salvador, ya que dentro de ellas se encuentran plasmadas cada una de las características propias de cada uno de los programas que conforman el kit de herramientas de informática forense, así como también cuentan con los requisitos mínimos del sistema para su correcta instalación y uso.

Las fichas técnicas contarán con una portada la cual al inicio cuenta con el nombre de la Universidad con un tipo de letra Times New Román tamaño 28 debajo del título lleva el logo de la Universidad en forma centrada y en la parte inferior centro llevara el título de las fichas, y como fondo posee una imagen color ocre con marco amarillo.



La siguiente página cuenta con una introducción al manual cuyo título va con un tipo de letra “Times New Román” tamaño 18 centrado, y debajo ira el desarrollo de la introducción, con un tipo de letra “Times New Román” tamaño 14

Introducción Desarrollo de la Introducción
--

La pagina siguiente cuenta con un indice automático para hacer mas fácil la búsqueda de cada ficha técnica.

Indice

Las fichas técnicas se elaboraron en páginas de papel bond tamaño carta con márgenes superior izquierdo de 4 CM. E inferior derecho de 2.5 CM. Con tipo de letra Times New Román N° 14 para los títulos, y para el resto del texto será con tipo de letra Times New Román N° 12, las características irán enumeradas dentro de una tabla, la cual cuenta con 2 columnas.

Titulo													
<table border="1"> <tr> <th colspan="2">Nombre del Programa</th> </tr> <tr> <td>Nº</td> <td>Características Técnicas</td> </tr> <tr> <td></td> <td></td> </tr> <tr> <td></td> <td></td> </tr> <tr> <td></td> <td></td> </tr> </table>		Nombre del Programa		Nº	Características Técnicas								
Nombre del Programa													
Nº	Características Técnicas												
<table border="1"> <tr> <th colspan="2">Requerimientos del Sistema</th> </tr> <tr> <td>Nº</td> <td></td> </tr> <tr> <td></td> <td></td> </tr> <tr> <td></td> <td></td> </tr> <tr> <td></td> <td></td> </tr> <tr> <td></td> <td></td> </tr> </table>		Requerimientos del Sistema		Nº									
Requerimientos del Sistema													
Nº													

El documento de las fichas técnicas está compuesto por un total de 13 páginas el cual se menciona cada una de las características principales de cada uno de los programas que se incluyen en el kit de herramientas de informática forense, así como también se incluyen los requisitos mínimos del sistema para su correcta instalación y funcionamiento, estas fichas tienen como objetivo orientar a los estudiantes a seleccionar adecuadamente los programas en base a las características que se necesitan y la capacidad de consumo que se necesitan a la hora de su debido uso. Las áreas que componen estas fichas son las áreas de: Recuperación de archivos borrados, recuperación de contraseñas guardadas en navegadores Web, keyloggers, modificación o eliminación de contraseñas de usuarios de Windows, análisis y protección anti-malware, análisis y limpieza del registro de Windows.

La implementación de estas fichas técnicas se lleva a cabo cuando el usuario necesita hacer uso de un programa específico del kit de herramientas de informática forense, por ejemplo el usuario necesita usar un programa recuperador de archivos borrados, pero necesita saber las características de ambos programas para ver cuál es el que más le conviene utilizar y también para poder ver cuáles son los requisitos mínimos del sistema para proceder con la instalación y su respectivo uso.

3.2. Conclusiones

1. Los productos elaborados para el desarrollo de este proyecto son de gran utilidad para los estudiantes de la Universidad Tecnológica de El Salvador, ya que con ello se pretende despertar el interés de los alumnos en esta área de la informática.
2. El desarrollo de este proyecto es de mucho beneficio académico para los alumnos de la Universidad Tecnológica de El Salvador, ya que obtendrán una mejor preparación en esta área, en comparación a otras universidades.
3. Con la investigación realizada 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.
4. Este trabajo pretende contribuir a mejorar la educación en el área de informática forense, en todos los alumnos de la Universidad Tecnológica de El Salvador.
5. El CD se creó con la finalidad de proporcionar al usuario una interfaz gráfica y fácil de uso para facilitar la identificación y aplicación de cada parte de su contenido antes mencionado, se realizaron pruebas para garantizar que cada herramienta de software del kit funciona correctamente, así mismo, con los documentos de las fichas técnicas y material de apoyo.

3.3. Recomendaciones

- Agregar más información relacionada al tema, por ejemplo kit móvil de información forense entre otros. Para que el documento sea más amplio en el tema que se ha tratado.
- Utilizar el manual para cada uno de los programas y realizar los pasos en el orden indicado.
- Al utilizar la informática forense se deben tomar en cuenta ciertos aspectos legales para no infringir la ley.
- Utilizar el kit de herramientas de informática forense a niveles educativos y utilizarla responsablemente.
- Para el buen desarrollo de este proyecto de informática forense, como grupo de trabajo se propone a la Universidad Tecnológica de El Salvador que para la realización de los diplomados de informática forense se tome en cuenta este producto ya que se creó con la finalidad de mejorar la calidad de enseñanza en la Universidad y también se pretende que los estudiantes que participen en estos diplomados puedan adquirir un mejor conocimiento acerca de la informática forense, su aplicación, su uso, y la utilización de programas que ayuden a resolver problemas de Hardware y Software en las computadoras, y promover el buen uso de este material.

3.4 Referencias

López Pages, Javier. (2013). *Informatica Forense*. Recuperado de <http://www.informatica-forense.es/>

López Rivas, José Luis. (2009). *Analisis Forenses de Sistemas Informaticos*. Recuperado de <http://www.gitsinformatica.com/Analisis%20forense%20de%20sistemas%20informaticos>.

Samaniego, Lilia. (2015). *Informática Forense Academia.edu*. Recuperado de https://www.academia.edu/1883410/Inform%C3%A1tica_Forense

López, Oscar. (2002). *Informática Forense: generalidades, aspectos técnicos y herramientas*. Recuperado de http://www.criptored.upm.es/guiateoria/gt_m180b.htm

Hernán Herrera, Sebastián. (2009). *Informática Forense Jornadas de Seguridad Informática*. Recuperado de <http://www.neuquen.gov.ar/seguridadinformatica/pdf/Informatica%20Forense%20-%20Hernan%20Herrera>.

Anexos

MATRIZ DE CONGRUENCIA		
TEMA: Elaboración de un kit de informática forense para material de apoyo en actividades de diplomados realizados en la Universidad Tecnológica de El Salvador.		
ENUNCIADO DEL PROBLEMA: ¿Con que tipos de herramientas debe contar el kit de informática forense que ayude como material de apoyo en actividades de diplomados realizadas en la Universidad Tecnológica de El Salvador?		
OBJETIVO GENERAL: Desarrollar un kit de herramientas de software básicas sobre informática forense para que pueda ser utilizado como material de apoyo en diplomados realizados por la Universidad Tecnológica de El Salvador.		
OBJ. ESPECÍFICO 1: Identificar, seleccionar y evaluar las herramientas de software que se han de incluir en el kit de informática forense.	OBJ. ESPECÍFICO 2: Diseñar un manual para el uso correcto de las herramientas de software seleccionado.	OBJ. ESPECÍFICO 3: Desarrollar un CD interactivo que contenga el manual de uso y las herramientas de software básicas de informática forense.
ALCANCE 1: Identificar, evaluar y seleccionar las herramientas que se incluirán en el kit.	ALCANCE 2: Orientar a los usuarios sobre el uso correcto de algunas herramientas básicas de informática forense.	ALCANCE 3: Proporcionar a la institución un CD con un kit de herramientas básicas de informática forense.
PRODUCTO 1: Fichas con características técnicas y requisitos mínimos de Instalación.	PRODUCTO 2: Se realizará un manual impreso de uso de las herramientas básicas de informática forense.	PRODUCTO 3: Elaboración de un CD interactivo con herramientas básicas de software sobre informática forense y uso.