UNIVERSIDAD DE HUANUCO

FACULTAD DE INGENIERIA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

“PROPUESTA METODOLÓGICA PARA LA RECOLECCIÓN DE EVIDENCIAS DIGITALES BAJO LOS SISTEMAS OPERATIVOS WINDOWS EN EL ÁMBITO DEL PERITAJE INFORMÁTICO”

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR: Trujillo Del Alamo, Cesar Alberto

ASESOR: Lopez De La Cruz, Edgardo Cristiam Iván

HUÁNUCO – PERÚ

2021

U

D

H

TIPO DEL TRABAJO DE INVESTIGACIÓN:

- Tesis (X)
- Trabajo de Suficiencia Profesional( )
- Trabajo de Investigación ( )
- Trabajo Académico ( )

LÍNEAS DE INVESTIGACIÓN: Proceso de enseñanza aprendizaje

AÑO DE LA LÍNEA DE INVESTIGACIÓN (2018-2019)

CAMPO DE CONOCIMIENTO OCDE:

Área: Ingeniería, Tecnología

Sub área: Ingeniería eléctrica, Ingeniería electrónica

Disciplina: Ingeniería de sistemas y comunicaciones

DATOS DEL PROGRAMA:

Nombre del Grado/Título a recibir: Título Profesional de Ingeniero de sistemas e informática

Código del Programa: P06

Tipo de Financiamiento:

- Propio (X)
- UDH ( )
- Fondos Concursables ( )

DATOS DEL AUTOR:

Documento Nacional de Identidad (DNI): 45666120

DATOS DEL ASESOR:

Documento Nacional de Identidad (DNI): 40394603

Grado/Título: Magister en ciencias de la educación

Código ORCID: 0000-0001-9815-7708

DATOS DE LOS JURADOS:

N°	APELLIDOS Y NOMBRES	GRADO	DNI	Código ORCID
1	Sulca Correa, Omar Ivan	Título oficial de máster universitario en ingeniería informática	42230320	0000-0002-6442-588X
2	Rodriguez Melendez, Fabio	Maestro en ingeniería de sistemas, mención en tecnologías de información y comunicación	42883191	0000-0003-4533-5595
3	Solis Jara, Paolo Edver	INGENIERO DE SISTEMAS E INFORMATICA	41656218	0000-0002-6936-1985

UNIVERSIDAD DE HUANUCO

Facultad de Ingeniería

P. A. DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO(A) DE SISTEMAS E INFORMÁTICA

En la ciudad de Huánuco, siendo las 11:00 horas del día 03 del mes de febrero del año 2021, mediante la plataforma Google Meet, en cumplimiento de lo señalado en el Reglamento de Grados y Títulos de la Universidad de Huánuco, se reunieron los **Jurados Calificadores** integrado por los Docentes:

- Mg. Omar Iván Sulca Correa (Presidente)
- Mg. Fabio Rodríguez Meléndez (Secretario)
- Ing. Paolo Edver Solís Jara (Vocal)

Nombrados mediante la Resolución N° 038-2021-D-FI-UDH, para evaluar la **Tesis** intitulada: **"PROPUESTA METODOLÓGICA PARA LA RECOLECCIÓN DE EVIDENCIAS DIGITALES BAJO LOS SISTEMAS OPERATIVOS WINDOWS EN EL ÁMBITO DEL PERITAJE INFORMÁTICO".** Presentada por el (la) **Bach. TRUJILLO DEL ALAMO CÉSAR ALBERTO.** Para optar el Título Profesional de Ingeniero (a) de Sistemas e Informática

Dicho acto de sustentación se desarrolló en dos etapas: exposición y absolución de preguntas: procediéndose luego a la evaluación por parte de los miembros del Jurado.

Habiendo absuelto las objeciones que le fueron formuladas por los miembros del Jurado y de conformidad con las respectivas disposiciones reglamentarias, procedieron a deliberar y calificar, declarándolo(a) APROBADO por UNANIMIDAD con el calificativo cuantitativo de 12 y cualitativo de SUFICIENTE (Art. 47).

Siendo las 11:59 horas del día 03 del mes de febrero del año 2021, los miembros del Jurado Calificador firman la presente Acta en señal de conformidad.

Presidente

Secretario

Vocal

DEDICATORIA

A mis amados padres por haberme inculcado todas las enseñanzas y valores las cuales hacen de mí una persona de bien, así como a todas aquellas personas que me han apoyado durante todo el trayecto para que este trabajo por fin sea una realidad.

AGRADECIMIENTO

Quiero agradecer a mis padres por creer en mí siempre y por brindarme todo su apoyo incondicional en toda mi formación profesional y personal.

A su vez, a mi pareja por contar con su apoyo y sabiduría en los momentos más difíciles en los que necesitaba un sabio consejo.

Asimismo, a mi Universidad por ser mi segunda casa en la que me forjaban para ser un profesional honesto y correcto.

Y finalmente a mi asesor, por acompañarme en todo este complicado y largo camino guiándome con total dedicación.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La investigación fue planteada en base a la necesidad de la unidad de criminalística de la policía de la ciudad de Huánuco de contar con unas herramientas digitales para asistir en el proceso del peritaje informático y resolución de algunos delitos informáticos denunciados en la ciudad de Huánuco y así aminorar las derivaciones de dichos casos a la ciudad de Lima.

Se han utilizado herramientas digitales gratuitas bajo el sistema operativo Windows, ya que es un sistema predominante en el uso de equipos cliente de las diferentes instituciones de la localidad, en este caso la unidad de criminalística, se realizó la selección adecuada de las herramientas a usar, así como también las pruebas en un entorno virtualizado simulando casos reales de delitos informáticos para posteriormente realizar el peritaje informático.

En la fase de capacitación y uso de estas herramientas, se contó con el apoyo y aceptación por parte del personal de la unidad, realizando las tareas de peritaje informático en una prueba piloto, propiciando las gestiones posteriores para la creación de una unidad especializada en el tratamiento de delitos informáticos y la aplicación del peritaje informático.

Finalmente se entregó el manual de peritaje informático conjuntamente con las herramientas digitales para el uso correspondiente en las labores diarias la unidad criminalística de la ciudad de Huánuco.

Palabras clave: Peritaje informático, delito informático, hacking ético.

ABSTRACT

The investigation was based on the need of the criminal crime unit of the police of the city of Huánuco to have digital tools to assist in the process of computer expertise and resolution of some computer crimes reported in the city of Huánuco and thus reduce the referrals of these cases to the city of Lima. Free digital tools have been used under the Windows operating system, since it is a predominant system in the use of client computers of the different institutions of the locality, in this case the criminalistics unit, the appropriate selection of the tools to be used was made, as well as tests in a virtualized environment simulating real cases of computer crimes to later perform the computer expertise. In the phase of training and use of these tools, there was support and acceptance by the unit staff, performing the tasks of computer expertise in a pilot test, promoting subsequent efforts to create a specialized unit in the treatment of computer crimes and the application of computer expertise. Finally, the computer expert manual was delivered together with the digital tools for the corresponding use in the daily work of the criminal unit of the city of Huánuco.

Keywords: Computer expertise, cybercrime, ethical hacking.

INTRODUCCION

La investigación se desarrolló bajo el marco de trabajo de la investigación científica siguiendo la línea de investigación de la seguridad informática, se planteó el objetivo principal: de elaborar una guía propuesta del uso de herramientas digitales para la recolección de evidencias digitales en sistemas Windows en el ámbito del peritaje informático. La metodología que se empleo es basada en la consulta y selección de información, la aplicación y prueba piloto, la documentación, y la redacción de la guía. Esta investigación de tipo tecnológica, se basó en la aplicación y solo en la utilización de la guía para efecto de uso y soporte en las actividades diarias de la unidad de criminalística de la ciudad de Huánuco.

El desarrollo y la implementación se llevó a cabo primero desde un entorno virtualizado y simulando los delitos informáticos para luego aplicar dichas herramientas para el peritaje informático. En cuanto a los resultados fueron esperados según lo previsto ya que se contó con la participación y aceptación del personal de la unidad de criminalística, realizando y ejecutando las pruebas de peritaje informático usando las herramientas digitales.

Se hizo la entrega oficial del manual impreso y digital a la unidad para que sirva como soporte en el desarrollo de actividades diarias en relación a la solución de delitos informáticos y peritaje informático de los casos presentados y denunciados en la ciudad de Huánuco.

CAPÍTULO I

LINEA DE INVESTIGACIÓN

1.1 Formulación y justificación de investigación

1.1.1. Descripción de la línea de investigación

La investigación se desarrolla bajo la política: “Seguridad Informática”, en la línea de investigación: “Auditoria Forense”, cuya referencia es: “Buscar desarrollar técnicas, métodos para identificar las causas de los posibles incidentes de seguridad o ciber delitos”. Las políticas, líneas de investigación y referencias han sido propuestas por la escuela académico profesional de Ingeniería de Sistemas e Informática de la Universidad de Huánuco.

Está planteada la investigación bajo estos marcos de referencia, debido al objetivo primordial de la misma: el de elaborar una guía propuesta de herramientas digital para la recolección de evidencias en el ámbito del peritaje informático.

1.1.2. Descripción del Problema

La seguridad de la información es un problema fehaciente y constante en estos tiempos, la información se ha convertido en el principal activo de las organizaciones, siendo en algunos casos vulnerable a diferentes amenazas tanto internas como externas, que se traducen en el robo de información, alteración, intercepción entre otros. En el Perú existe una ley que regula los delitos informáticos, la ley 30096, dicha ley propone mediante títulos y artículos las diferentes sanciones y medidas a tomar contra el cometido de un delito informático. En la ciudad de Huánuco, la situación actual en cuanto a los delitos informáticos es incierta; a continuación, se detalla dicha incertidumbre mediante las

entrevistas realizadas a las autoridades de las diferentes instancias de justicia del Estado de la ciudad de Huánuco.

En Huánuco no existe un área especializada para tratar el tema de delitos informáticos, y si se comete algún delito informático y este es denunciado se deriva a la fiscalía de la nación en el departamento de lima, en algunos casos se envía a un perito especializado al lugar en el cual realiza el informe respectivo. (Salazar, 2018).

En el departamento de Investigación criminal, DEPINCRI de la ciudad de Huánuco, también se dio a conocer que solo en lima existe un área especializada llamada DIVINDAT (Dirección de Investigación de Delitos de Alta Tecnología). Si es que se presentase un delito informático y este es denunciado se procede de la siguiente forma, se realiza un documento dirigido a la DIVINDAT, posterior a ello, desde lima se envía a un personal especializado conocido como ciber policía que se encarga de la investigación, finalizando con un informe en el cual es entregado al a Fiscalía. (Lozano, 2018).

Así mismo en el Poder Judicial de Huánuco, también negaron la existencia de un área específica para el peritaje informático, que solo existe un área, una mesa de partes donde se deriva las denuncias a la capital para luego enviar personal capacitado en las investigaciones, se hace hincapié en el poco número de casos denunciados. (Domínguez, 2018).

Sin embargo, en la oficina de criminalística perteneciente al departamento de investigación criminal de Huánuco, ubicado en la Av. Marcos Duran Martel s/n Amarilis, se llegó a entrevistar con el comandante Erik Moreno Luna, la cual nos dio a conocer que en la unidad si se realizan en sus actividades diarias algunos procesos de peritaje informático en tareas básicas, como descargar videos de las cámaras de videovigilancia o rescatar algunos archivos eliminados de máquinas que han sido involucradas en un delito,

entre otros; también nos afirmó que algunas tareas no pueden realizarse debió a la carencia de herramientas y de conocimiento por tal motivo algunos casos se reenvían a lima, trayendo como consecuencia la demora y saturación de dichos casos para la capital.

1.1.3. Justificación del Problema

Justificación Práctica

El resultado de la investigación tiende a dar como resultado una guía práctica de uso de herramientas digitales para perito informático bajo el entorno Windows para poder ser usado en la oficina de criminalística de la ciudad de Huánuco.

Justificación Teórica

El beneficio teórico se refleja en contar con una guía propuesta de los procedimientos para aplicar la recolección de evidencias digitales bajo entornos Windows usando diferentes herramientas especializadas, esta guía contiene los pasos a seguir para utilizar dichas herramientas.

1.1.4. Propuesta y Solución de Alcance

La propuesta se basa en la elaboración de un documento guía donde se da a conocer los procedimientos técnicos teóricos y prácticas para la utilización de herramientas digitales en la recolección de evidencias digitales en entornos Windows. Dicho documento se hará llegar a la unidad de criminalística de la ciudad de Huánuco.

En cuanto al alcance de la investigación se centra en la proposición de una guía de uso de estas herramientas para apoyar a las actividades informáticas relacionadas al peritaje informático, cabe destacar que el ámbito del peritaje informático es muy amplio y por lo tanto requiere especialización, sin embargo se pueden realizar y ejecutar algunas tareas dentro del ámbito de peritaje informático

utilizando herramientas básicas para el soporte y desarrollo en este caso del personal de la oficina de criminalística de la ciudad de Huánuco, esta oficina es la más cercana a una oficina de delitos informáticos de la ciudad. Para la utilización de las herramientas solo se requerirá el dominio básico del sistema operativo Windows y las herramientas de ofimática. Se realizaran pruebas en el uso de estas herramientas en entornos virtualizados creando el delito o la situación a investigar (borrado de archivos, intrusión no autorizada, alteración, modificación de archivos) de tal forma que la recopilación de la información estará propuesta en este guía. Es así que se ha previsto analizar, personalizar, configurar, elaborar, algunas herramientas digitales para el proceso de peritaje informático para apoyar y dar soporte a las actividades diarias del departamento de criminalística de la ciudad de Huánuco, se opta por el entorno Windows por el hecho de que las maquinas que están instaladas en el departamento o área, funcionan bajo el sistema operativo Windows. En cuanto a las herramientas software utilizadas en esta investigación para la guía propuesta del peritaje informático cuenta con la licencia de software libre.

1.2. Objetivos

1.2.1. Objetivo Principal

Elaborar una propuesta metodológica para la recolección de evidencias digitales en sistemas Windows en el ámbito del peritaje informático.

1.2.2. Objetivos Secundarios

- Descargar, y recopilar las herramientas necesarias para la recolección de evidencias digitales.
- Realizar las pruebas necesarias en máquinas virtuales bajo el sistema operativo Windows.
- Redactar de la guía manual de herramientas digitales para la recolección de evidencias digitales.
- Publicar la metodologia para su acceso y uso por las correspondientes personas asignadas del departamento de criminalística de la ciudad de Huánuco.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de la investigación

A nivel Internacional

Arnedo, (2014), realizo la investigación: *Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos*. En la Universidad Internacional de la Rioja. La investigación llego a las siguientes principales conclusiones: Para resistir la creciente incidencia de incidentes de seguridad informática en todo el mundo y las formas cada vez más sutiles y avanzadas de ataques informáticos, la informática forense se ha reforzado continuamente. En este documento, todos los asuntos relacionados con el uso real de herramientas de análisis forense y los resultados de la evidencia efectiva obtenidos en la investigación y la efectividad real cuando se combinan con la aplicación se reflejan con profesionalismo integral e investigación de alto nivel. Varios métodos forenses estudiados en un mismo documento.

A nivel Nacional

Yopla y Yopla, (2014), realizo la investigación: *Metodología para la colecta de la Evidencia Digital*. En la Universidad Tecnológica del Perú. La investigación llego a las siguientes principales conclusiones: Este artículo presenta un método para capturar evidencia digital en análisis forense. Este problema se ha vuelto muy importante, principalmente por el desarrollo de la tecnología de la información y la globalización de las redes informáticas, que ha provocado un aumento de los delitos a través de dispositivos digitales.

A nivel Local

Ostos, (2016), realizo la investigación: *La Auditoría Forense como Metodología para Detectar los Delitos en la Administración de la*

Municipalidad Provincial de Lima Metropolitana Periodo 2012-2013. En la Universidad Nacional Hermilio Valdizan. La investigación llego a las siguientes principales conclusiones: El uso de procedimientos y técnicas de auditoría forense sobre la base de planes y programas de auditoría adecuados tendrá un impacto en los delitos de malversación ilegal de bienes, enriquecimiento ilegal y pago indebido propuestos en la investigación y administración. Ciudad Metropolitana de Lima.

2.2 Bases Teóricas

Peritaje Informático

Es una rama de la ingeniería informática que utiliza tecnología detallada y / o investigación científica, y utiliza la tecnología y los métodos de la disciplina para confirmar o refutar un hecho determinado, con determinados hechos o que ocurra directamente, Se puede inferir. Para ello, los informáticos deben buscar, capturar, guardar, investigar y registrar una serie de pruebas digitales y conservar sus características inalteradas para presentarlas a las autoridades judiciales.. (Torre, 2019).

El equipo de informáticos de Evidencias Informáticas también puede realizar contra-peritajes con contra-informes periciales, en este caso nuestros informáticos utilizarán argumentos técnicos consistentes y válidos para analizar y refutar los peritajes de la otra parte. Asimismo, cuando sea necesario, los expertos en informática que preparan el informe testificarán en el juicio para aportar la conclusión de la investigación forense como perito calificado. Este servicio especial no está incluido en la experiencia de TI, pero se presupuestará por separado.

Así mismo, el equipo de pruebas informáticas también brinda servicios profesionales para asesorar a la empresa en la implementación de estrategias y mecanismos de seguridad. (Informáticas, 2019)

El informe pericial será presentado al cliente en un lenguaje sencillo por el experto en tecnologías de la información, y al juez en su caso, para que

cualquier novato pueda comprender el propósito del conocimiento y la conclusión profesional. Los informes periciales informáticos deben alejarse lo más posible de las técnicas y vocabulario típicos de la asignatura, aunque siempre es inevitable incluir dichos términos, por tratarse de un informe técnico.. (Alamillo, 2013).

Evidencias digitales

La evidencia digital se define como cualquier tipo de información almacenada en una computadora que representa hechos o acciones. Toda la evidencia digital se encuentra en un área específica relacionada con ella, y los expertos en TI son responsables de documentar a fondo el área.

La evidencia digital debe obtenerse lo antes posible, porque la evidencia digital se degenerará con el tiempo y es difícil probar completamente una cadena de custodia efectiva. Por lo tanto, la cadena de custodia de la evidencia digital se define como un procedimiento técnico que se utiliza para confirmar evidencia sin ninguna duda. De expertos en TI El número sigue siendo el mismo desde el momento en que se observa en el entorno donde se constató que fue llevado ante la justicia. (Torre, 2019)

2.3 Definiciones conceptuales

DEPINCRI: División de Investigación Criminal y apoyo a la Justicia. Sede responsable de investigar denuncias específicas de diversas formas de delincuencia común y delincuencia organizada. (INEI, 2014).

DIVINDAT: División de Investigación de Delitos de Alta Tecnología. (INTERIOR, 2016).

FREEWARE: El software libre es cualquier programa o aplicación que se pueda distribuir a los consumidores sin pagar ninguna tarifa. (NeoAttack, s.f.).

GPL: El software publicado debe ser software gratuito. Para ser gratuito, debe ser lanzado bajo una licencia de software libre. (Sistema Operativo GNU, 2018).

ISO: Las normas ISO Son documentos que especifican los requisitos que se pueden utilizar en la organización para garantizar que los productos y / o servicios proporcionados por la organización cumplan con sus objetivos.. (ISOTOOLS, 2018).

OPEN SOURCE: Por lo general, el código abierto se refiere a cualquier programa que los usuarios u otros desarrolladores consideren apropiado y cuyo código fuente se pueda utilizar o modificar. (Rouse, 2016).

CAPÍTULO III

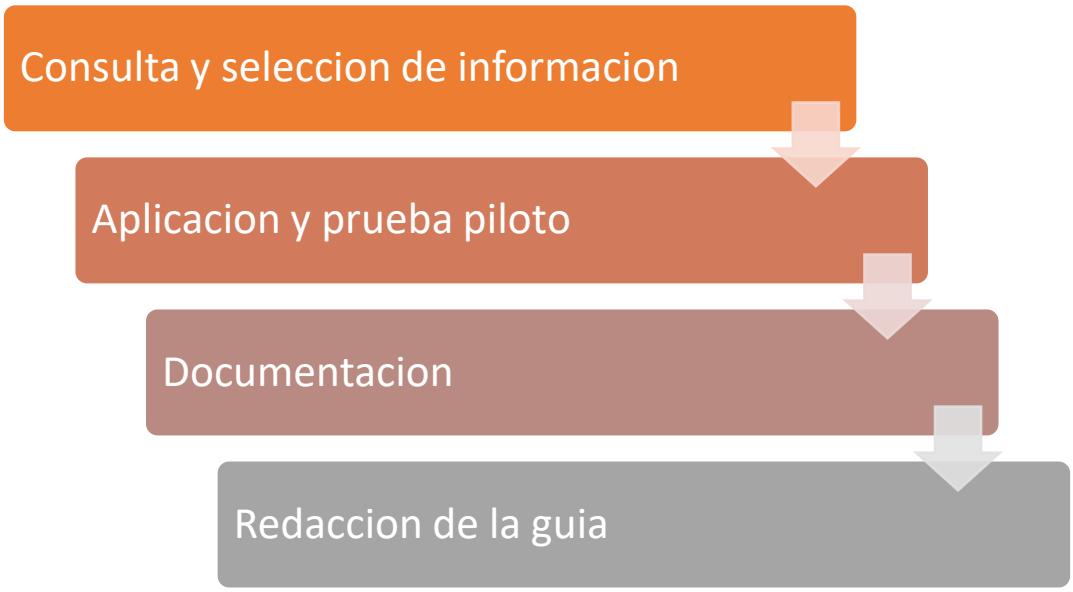
METODOLOGIA

3.1 Metodología

La metodología que se empleo fue propuesta por el propio investigador y adecuada a la naturaleza de los objetivos y en correlación con los mismos, se basó en fases relacionadas y secuenciales para la elaboración de la propuesta guía técnica:

Figura 1:

Fases de la metodología para el peritaje informático



Fuente: Propia

Fase01: Consulta y Selección de Información:

En esta fase se procedió con la búsqueda de información sobre las herramientas digitales que operan en el ámbito del peritaje informático en entornos Windows, se recurrió a las páginas web especializadas, para su posterior descarga y análisis de la herramienta a utilizar, se realizó la documentación previa donde se lista la versión del programa herramienta, requisitos, el nombre de la herramienta:

Tabla 1:

Ficha de recolección de evidencias digitales

Herramienta de recolección de evidencias digitales		
Nombre	Versión	requisitos

Fuente: Propia

En cuanto a las necesidades planteadas por la institución fueron:

- Herramientas para recuperación de información eliminada
- Herramientas para recuperación de información alterada
- Herramientas para realización de diagnóstico y estado actual del sistema
- Herramientas para la detección de intrusos.

Fase02: Aplicación y prueba piloto:

En esta fase se ejecutaron y se realizaron las pruebas necesarias en un entorno virtual bajo el sistema operativo Windows. La prueba piloto consistió en desencadenar situaciones ficticias donde se ha llevado a cabo un incidente dentro del computador ejecutándose el sistema operativo, posteriormente se realizó el test de la herramienta y se comprueba el nivel de efectividad en cuanto a logro del objetivo propuesto del uso de la herramienta. Se usa la siguiente ficha:

Tabla 2:

Ficha de pruebas y resultados

Nombre:			
Versión:		Fecha:	_____/_____/_____
Pasos:	Objetivo:	Resultados:	Supuesto incidente

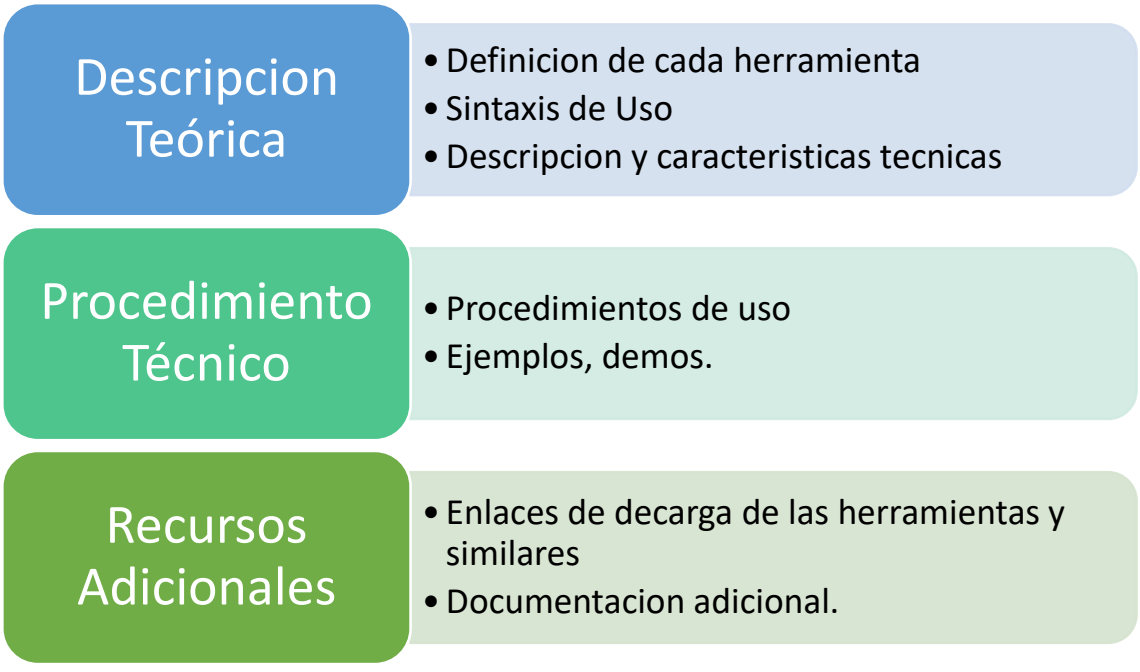
Fuente: Propia

Fase03: Documentación:

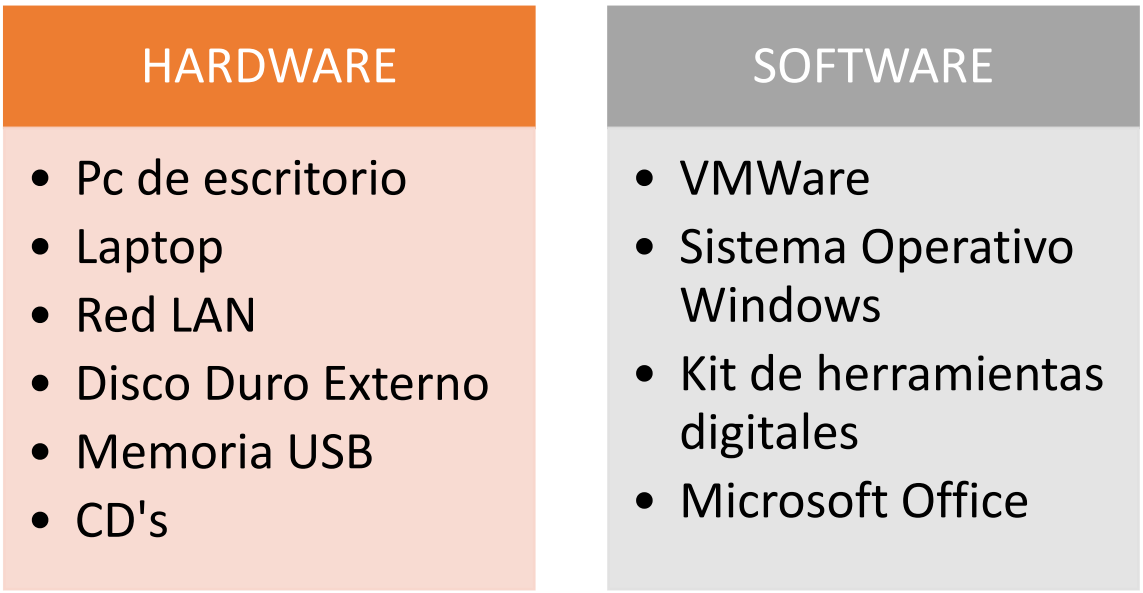
En esta fase se procedió con la elaboración de la documentación de la aplicación, se realizó la anotación del paso incluido en la ficha anterior, se detalló minuciosamente el procedimiento para utilizar la herramienta digital y las recogidas de evidencias digitales en el sistema operativo, se listaron las herramientas testeadas y funcionales con sus características, en el caso de incluir código, se documentó el programa, se incluyó las fuentes o repositorios de algunas dependencias y ejecutables.

Fase04: Redacción de la Guía:

Con la documentación terminada, se procedió a elaborar la guía que fue el entregable final o documento que sirvió como manual de aplicación de las herramientas digitales para la recolección de evidencias en entornos Windows. Esta guía contiene:



3.2 Herramientas



VMWARE: es un hipervisor alojado que se ejecuta en versiones x64 de los sistemas operativos Windows y Linux; permite a los usuarios configurar máquinas virtuales en una sola máquina física y usarlas simultáneamente con la máquina real.

Esta herramienta se usará como plataforma de virtualización para realizar la instalación y pruebas de cada una de las herramientas digitales que conformará el kit de herramientas digitales para el peritaje informático.

WINDOWS: es el nombre de una familia de distribuciones de software para PC, smartphone, servidores y sistemas empotrados, desarrollados y vendidos por Microsoft y disponibles para múltiples arquitecturas, tales como x86, x86-64 y ARM.

Es el sistema operativo, en este caso Windows 8 y 7 donde se pondrá a prueba las herramientas de peritaje informático, este sistema operativo está presente en todas las maquinas instaladas en el departamento de criminalística de la ciudad de Huánuco.

CAPÍTULO IV

DESARROLLO E IMPLEMENTACION

4.1 Desarrollo e implementación

El desarrollo de la investigación se basó en cuatro fases ordenadas y relacionadas, estas fases forman parte de la Metodología empleada.

Consulta y seleccion de informacion

En esta fase se procedió a recurrir a las oficinas del departamento de criminalística de la ciudad de Huánuco para obtener las necesidades en cuanto al peritaje básico de casos informáticos. Estas necesidades fueron listadas en base a las actividades usuales y comunes que se hacían en las oficinas del departamento de criminalística, a su vez se hizo un listado de todas las herramientas digitales que se utilizaron al momento de la redacción del manual. El proceso de recolección de datos se realizó conjuntamente con los trabajadores del área en previas entrevistas acordadas. El cuadro que se muestra a continuación es el resultado de las pruebas realizadas por el investigador y a la selección idónea de la herramienta para el sistema operativo. En cuanto a las tecnologías de información y comunicación provistas en la institución, se incluía computadoras I5, impresoras e Internet.

Tabla 3:

Ficha de herramientas digitales

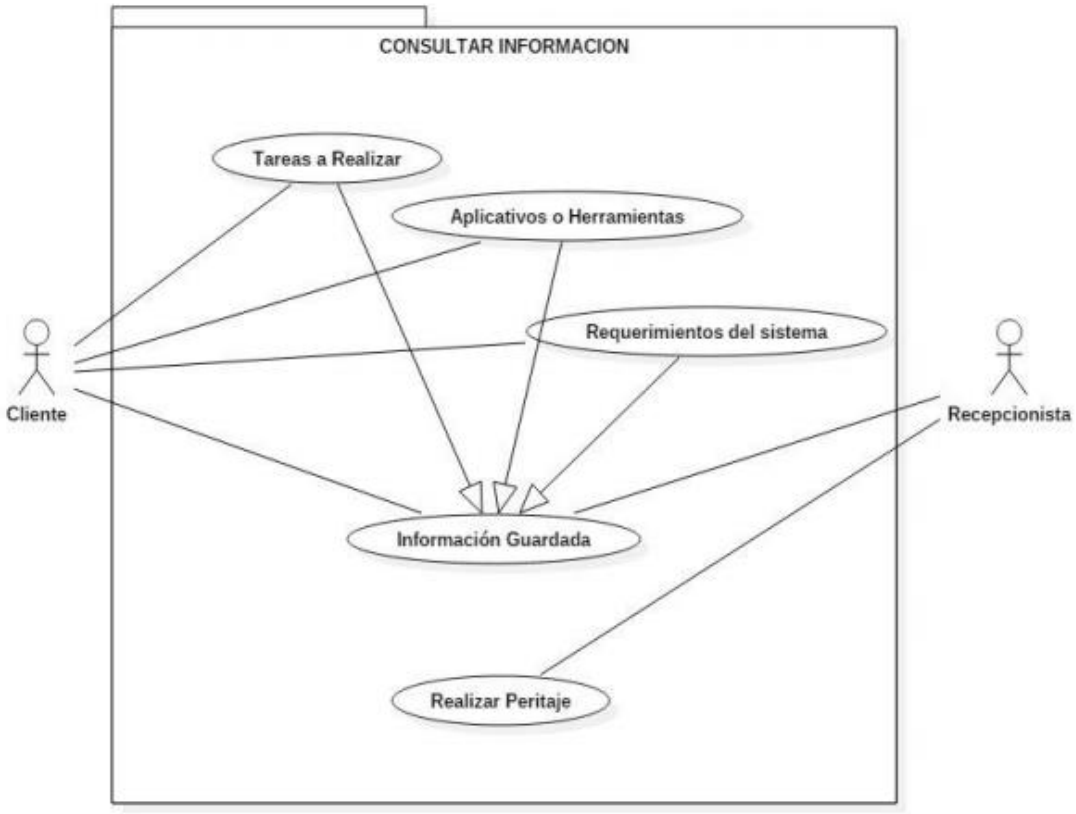
Herramienta de recolección de evidencias digitales		
Nombre	Versión	requisitos
AUTOPSY	4.13.0	Sistema operativo Linux o Windows de 32 o 64 bits

OSFORENSICS	7.0.1	Win7 x32, Windows 10, Windows 8, WinVista, Win7 x64
FOCAPRO	3.0.0	Sistema operativo Linux o Windows de 32 o 64 bits
TESTDISK	7.2	Sistema operativo Linux o Windows de 32 o 64 bits
DMDE	3.6.0	Win7 x32, Windows 10, Windows 8, WinVista, Win7 x64
PWDUMP7	7.1	Win7 x32, Windows 10, Windows 8, WinVista, Win7 x64

Fuente: Propia

Figura 2:

Caso de uso de consulta de información



Fuente: Propia

Tabla 4:

Ficha De Roles De Tareas Y Asignación De Maquinas

MAQUINA	PC01-UC	AREA	Unidad de Criminalística
		USUARIO	User01-PC01
IP	192.168.10.15	SISTEMA OPERATIVO	WINDOWS 8
		ESTADO	OPERATIVA
TAREA 01		Redactar informes y almacenar solicitudes y denuncias policiales.	
TAREA 02		Maquina conectada a Impresora, realiza impresión y escaneado de documentos, cuenta con un Scanner conectado.	
MAQUINA	PC02-UC	AREA	Unidad de Criminalística
		USUARIO	User02-PC02
IP	192.168.10.16	SISTEMA OPERATIVO	WINDOWS 8
		ESTADO	OPERATIVA
TAREA 01		Máquina para la evaluación de evidencias recolectadas.	
TAREA 02		Contiene el software para buscar expedientes y denuncias realizadas.	
MAQUINA	PC03-UC	AREA	Unidad de Criminalística
		USUARIO	User03-PC03

IP	192.168.10.17	SISTEMA OPERATIVO	WINDOWS 10
		ESTADO	OPERATIVA
TAREA 01		Maquina con software de virtualización para realizar las pruebas de las herramientas de peritaje.	
TAREA 02		Maquina también accede a impresora y escáner	
MAQUINA	PC04-UC	AREA	Unidad de Criminalística
		USUARIO	User04-PC04
IP	192.168.10.18	SISTEMA OPERATIVO	WINDOWS 10
		ESTADO	OPERATIVA
TAREA 01		Maquina con software de virtualización para realizar las pruebas de las herramientas de peritaje	
TAREA 02		Maquina también accede a impresora y escáner	

Fuente: Propia

ENCUESTA PARA DETERMINACION DE NECESIDADES Y TAREAS BASICAS RELACIONAS AL PERITAJE INFORMATICO.

1. Realiza operaciones de recuperación de data, su objetivo está más centrado en:
   - Celulares
   - Tablets
   - Laptos y CPUs
   - Memorias USB
   - Discos Externos

2. Cuando se realiza diagnóstico del equipo mayormente que parte del equipo a nivel de software se evalúa:
   - Memoria RAM
   - Papelera de reciclaje
   - Archivos Temporales
   - Historial de Navegación
   - Documentos accedidos

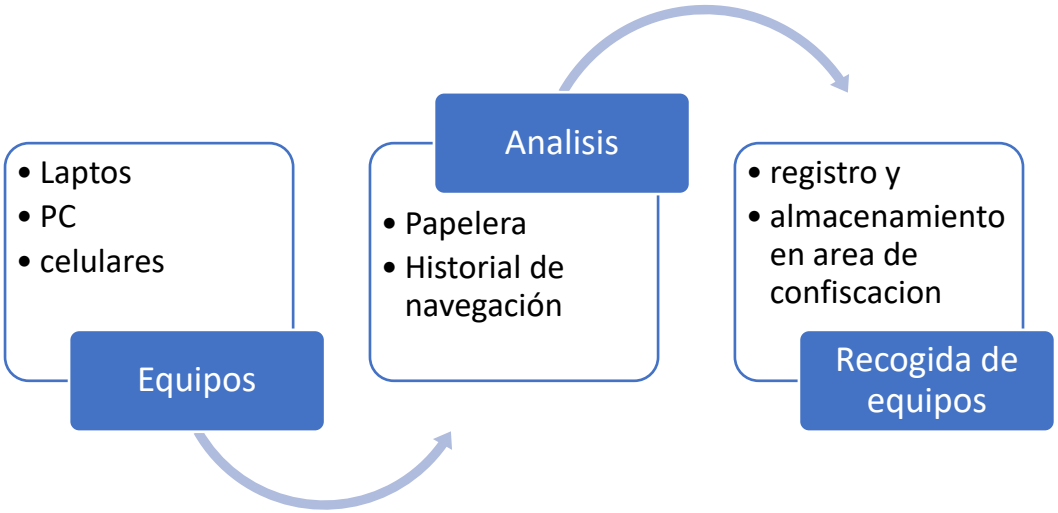
3. Pose sistemas de detección de intrusos:
   - Si
   - No

4. Cuando llega un equipo a analizar qué es lo primero que procede:
   - Registrar equipos
   - Analizar equipo
   - Derivar a otra área
   - Poner en lista de espera
   - Almacenar en área de equipos confiscados

En relación a las respuestas se muestra el diagrama donde se ilustra las necesidades básicas de peritaje informático:

Figura 3:

Necesidades de Peritaje Informático

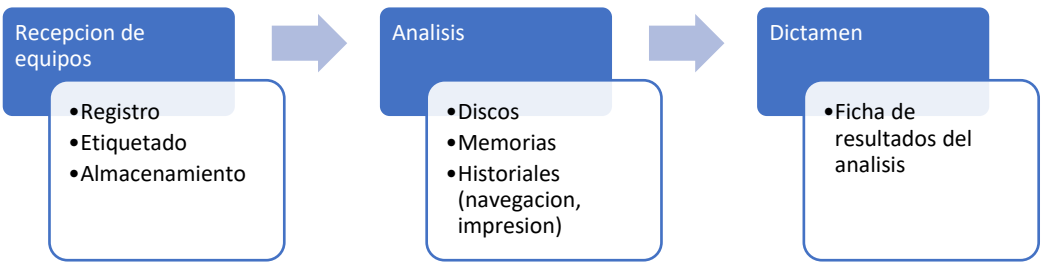


Fuente: Propia

Para ello la metodología propuso:

Figura 4:

Modelo propuesta de pasos para proceso de Peritaje



Fuente: Propia

Se cuenta con los siguientes formatos para los pasos:

Tabla 5:

Registro De Recepción De Equipos (Evidencias)

EQUIPO		FECHA	_____/_____/_____
ESTADO		PROCEDENCIA	
DECRIPCION DEL EQUIPO			
POSIBLE DELITO:			
ASIGNADO A:			

Fuente: Propia

Para su empleo, el formato fue impreso, y luego volcado a una hoja de cálculo para llevar el control del registro como se muestra a continuación:

Tabla 6:

Registro resumido de equipos para proceso de peritaje

EQUIPO	FECHA	ESTADO	PROCEDENCIA	DESCRIPCION	DELITO	ASIGNADO

Fuente: Propia

Tabla 7:

Registro De Recepción De Equipos (Caso Practico)

EQUIPO	Laptop	FECHA	___18_/_05__/_19__
ESTADO	Operativo sin cargador	PROCEDENCIA	Municipalidad de Huánuco
DECRIPCION DEL EQUIPO			
El equipo de marca Lenovo color negro no trae cargador y tenia conectado una memoria USB al momento de la intervención, además el equipo fue apagado al momento de su intervención. El equipo este operativo, pero en malas condiciones, la pantalla tiene un desperfecto en la parte superior izquierda.			
POSIBLE DELITO:	Alteración de la base de datos del sistema de Papeletas de Transito		
ASIGNADO A:	Área de Transportes		

Fuente: Propia

La metodología propuso:

Figura 5:

Volcado de registro a hoja de cálculo

Fuente: Propia

Tabla 8:

Ficha De Evaluación De Aplicativos Para El Peritaje Informático

TIPOLOGÍA					
Nombre					
Tipo de aplicación	☐ App Móvil ☐ De Escritorio ☐ En la Nube				
Modo de uso	☐ Local ☐ Offline ☐ En red				
Plataforma	☐ Windows ☐ Linux				
REQUISITOS TECNICOS					
Nombre					
A nivel de software					
A Nivel de Hardware					
A nivel de Red					
ASPECTOS DE USABILIDAD					
NIVELES	**Nada**	**Poco**	**Regular**	**Bastante**	**Mucho**

Facilidad de instalación					
Facilidad de uso					
Documentación y ayuda					
Portabilidad					
Sistema de Navegación					
Calidad de la interfaz					

Fuente: Propia

Tabla 9:

Ficha De Evaluación De Aplicativos Para El Peritaje Informático (Caso Practico)

TIPOLOGÍA					
Nombre	TESDISK				
Tipo de aplicación	□ App Móvil □ **De Escritorio** □ En la Nube				
Modo de uso	□ **Local** □ Offline □ En red				
Plataforma	□ **Windows** □ Linux				
REQUISITOS TECNICOS					
Nombre	TESTDISK				
A nivel de software	Windows NT 4/2000 / XP / 2003 / Vista / 2008/7/10				
A Nivel de Hardware	Mínimo de 1 GB de RAM 700 MB de espacio libre en disco				
A nivel de Red	Ninguno				
ASPECTOS DE USABILIDAD					
NIVELES	**Nada**	**Poco**	**Regular**	**Bastante**	**Mucho**
Facilidad de instalación				**X**	
Facilidad de uso				**X**	
Documentación y ayuda			**X**		
Portabilidad		**X**			
Sistema de Navegación				**X**	

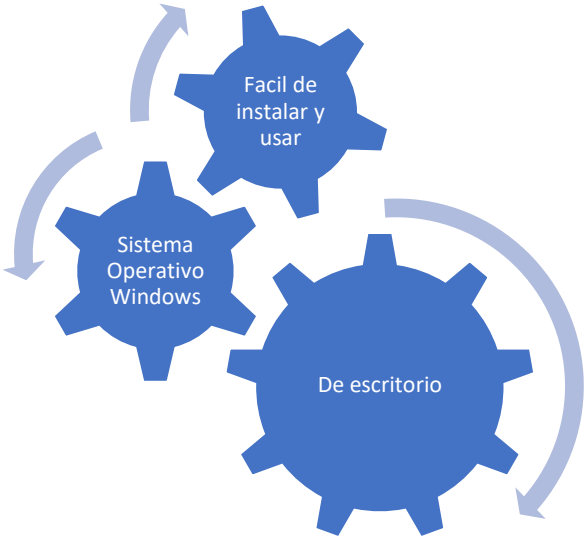
Calidad de la interfaz				X	

Fuente: Propia

Bajo la metodología se escogieron aquellos programas que cumpliesen lo siguiente:

Figura 6:

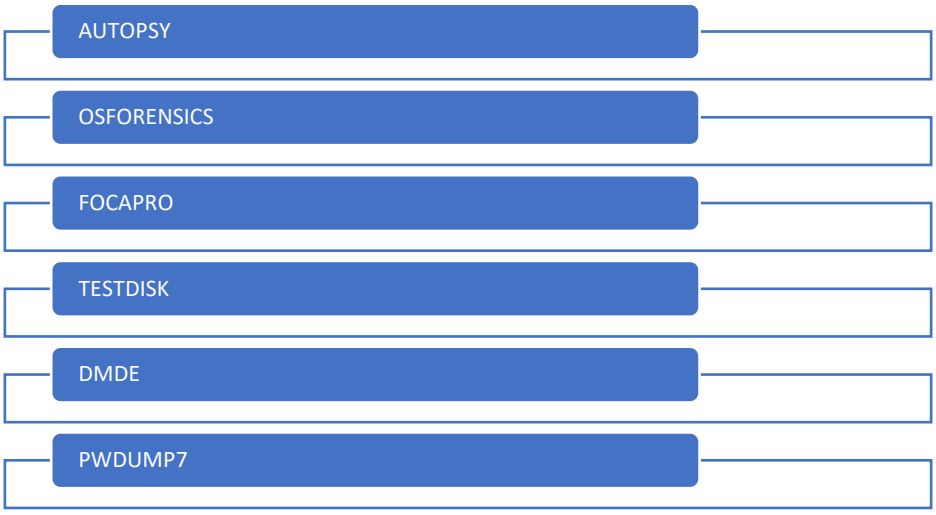
Requisitos para el uso de las herramientas para el peritaje



Fuente: Propia

Figura 7:

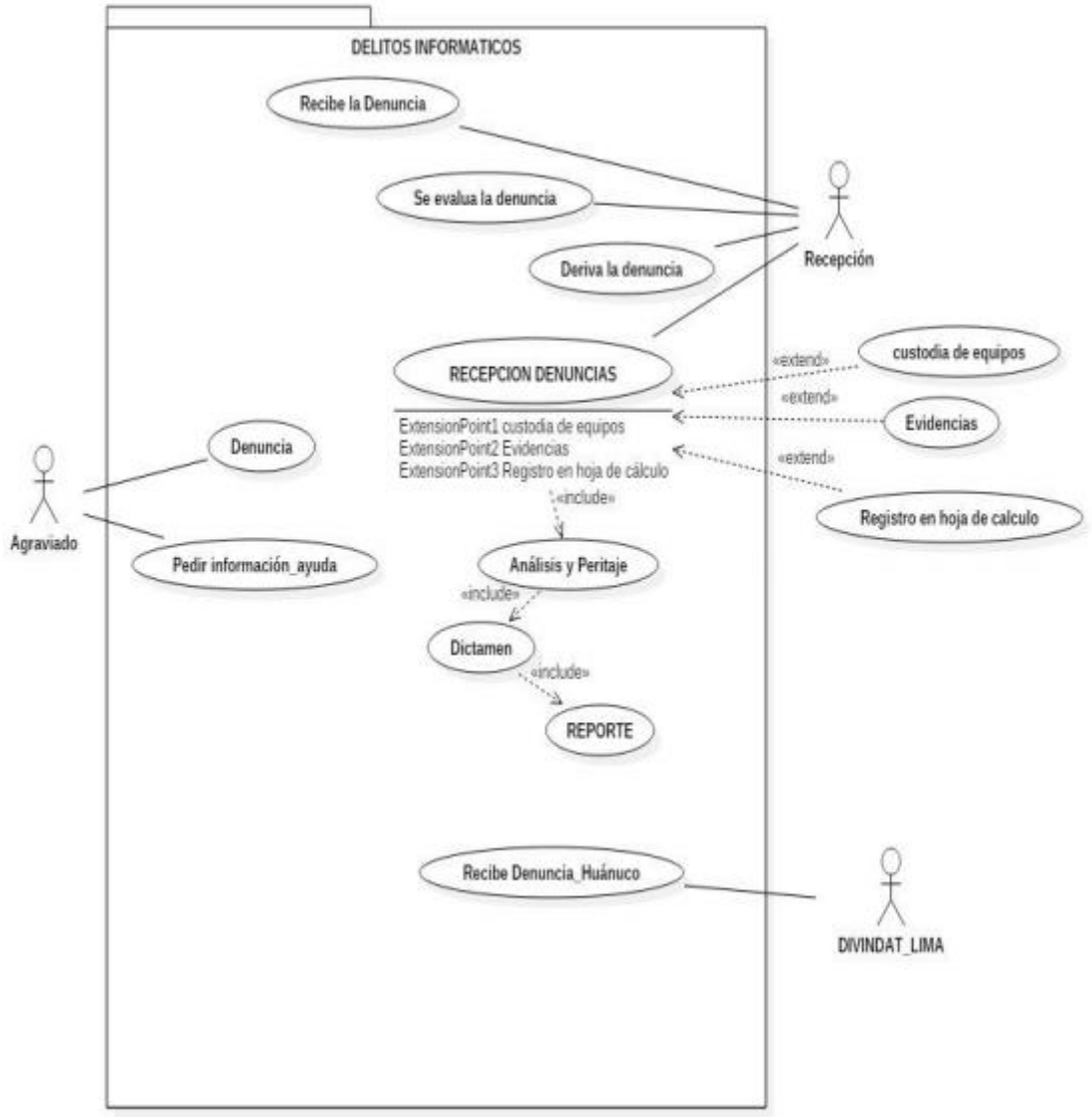
Herramientas seleccionadas para el Peritaje Informático



Fuente: Propia

Figura 8:

Caso de Uso de proceso de atención del peritaje informático



Fuente: Propia

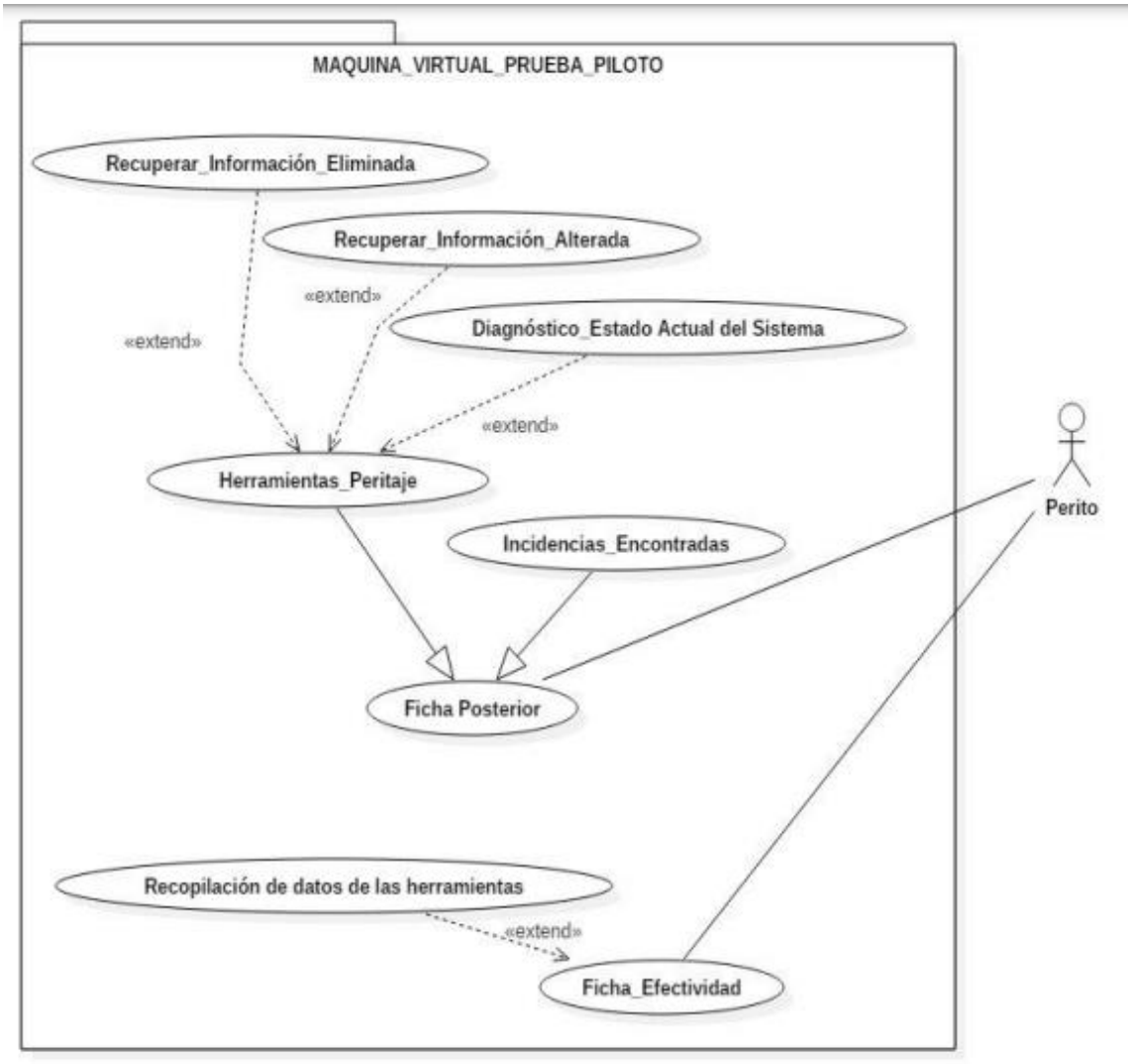
Aplicacion y prueba piloto

Los escenarios de prueba se realizaron primero en las máquinas virtuales creadas mediante el software de virtualización para realizar las pruebas

correspondientes y luego llevarlo a cabo en la computadora física real de las oficinas del departamento de criminalística. No se realizó una clasificación previa de cada herramienta, porque se basó en los casos obtenidos y según prioridad de resolución, además a nivel de pruebas se consideró los resultados más importantes y que hayan sido efectivos tanto en la máquina virtual como en la física.

Figura 9:

Caso de uso de prueba piloto



Fuente: Propia

En esta fase se realizaron las pruebas piloto utilizando los posibles y frecuentes delitos informáticos ocurridos y denunciados en el departamento policial, se llevó a cabo en un entorno virtualizado, a continuación de muestra las fichas prueba piloto realizada:

Tabla 10:

Ficha de prueba piloto Autopsy

Nombre:	AUTOPSY		
Versión:	4.13.0	Fecha:	10/06/2019
Pasos:	Objetivo:	Resultados:	Supuesto incidente
Ver página nº 03 del manual	Analizar lo ocurrido en el equipo	Información sobre Archivos, carpetas eliminados	Ingreso al sistema y borrado de carpetas y archivos.

Fuente: Propia

Con respecto a la efectividad de la herramienta AUTOPSY se logró obtener registros detallados de información eliminada de la máquina virtual como de la maquina real (intervenida) suponiendo o creando el ataque ficticio; cabe mencionar que, en algunos casos, se realizaron con eventos reales.

Tabla 11:

Ficha de prueba piloto Osforensics

Nombre:	OSFORENSICS		
Versión:	7.0.1	Fecha:	10/06/2019
Pasos:	Objetivo:	Resultados:	Supuesto incidente
Ver página nº 07 del manual	Comprobación de la integridad de	Información y comprobación sobre	Ingreso al sistema y modificación de algunos archivos y carpetas

	archivos y carpetas	archivos alterados	

Fuente: Propia

Con respecto a la efectividad de la herramienta OSFORENSICS se pudo comprobar aquellos archivos y carpetas modificas y/0 eliminadas del sistema operativo, dando a conocer la fecha, el usuario y los elementos eliminados.

Tabla 12:

Ficha de prueba piloto Focapro

Nombre:	FOCAPRO		
Versión:	3.0.0.	Fecha:	11/06/2019
Pasos:	Objetivo:	Resultados:	Supuesto incidente
Ver página nº 12 del manual	Detección de metadatos de la información almacenada	Extracción de datos relevantes de algunos archivos.	Archivos o adjuntos de correo enviados anonimamente.

Fuente: Propia

Con respecto a la efectividad de la herramienta FOCAPRO se pudo extraer los metadatos de algunos archivos como, por ejemplo: geolocalización, fecha de modificación, creación, autor, nombre del pc, dirección IP entre otras.

Tabla 13:

Ficha de prueba piloto TestDisk

Nombre:	TESTDISK		
Versión:	7.2	Fecha:	11/06/2019

Pasos:	Objetivo:	Resultados:	Supuesto incidente
Ver página nº 18 del manual	Recuperar imágenes eliminadas	Imágenes, fotografías recuperadas	Eliminación de fotografías, evidencias de un caso.

Fuente: Propia

En cuanto a la efectividad de la herramienta TESTDISK se pudo recuperar imágenes borradas tanto del disco duro como de los dispositivos de almacenamiento extraíbles, en algunos casos las imágenes se corrompieron y no podían visualizarse, pero en la mayoría de los casos se mostraba íntegramente las imágenes recuperadas.

Tabla 14:

Ficha de prueba piloto DMDE

Nombre:	DMDE		
Versión:	3.6.0	Fecha:	11/06/2019
Pasos:	Objetivo:	Resultados:	Supuesto incidente
Ver página nº 23 del manual	Recuperar de discos duros	Discos duros recuperados	Fallo intencional físico del disco duro.

Fuente: Propia

Con respecto a la efectividad de la herramienta DMDE se pudo recuperar discos duros fallados o formateados, o intencionalmente dañados, rescatando así la información almacenada.

Tabla 15:

Ficha de prueba piloto PWDUMP7

Nombre:	PWDUMP7		
Versión:	7.1	Fecha:	11/06/2019

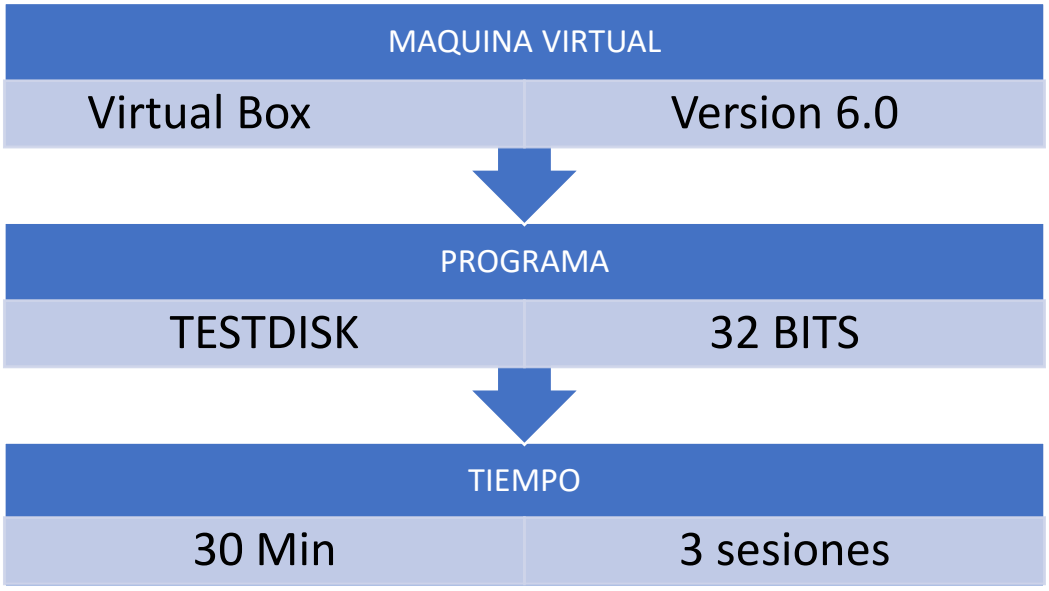
Pasos:	Objetivo:	Resultados:	Supuesto incidente
Ver página nº 25 del manual	Recuperar contraseñas del sistema operativo Windows	Contraseñas recuperadas	Cambio de contraseñas y olvido.

Fuente: Propia

Con respecto a la efectividad de la herramienta PWDUMP7 se pudo recuperar contraseñas de las computadoras con el sistema operativo Windows, en el caso que la evidencia o maquina comprometida este bajo contraseña.

Figura 10:

Ficha prueba piloto

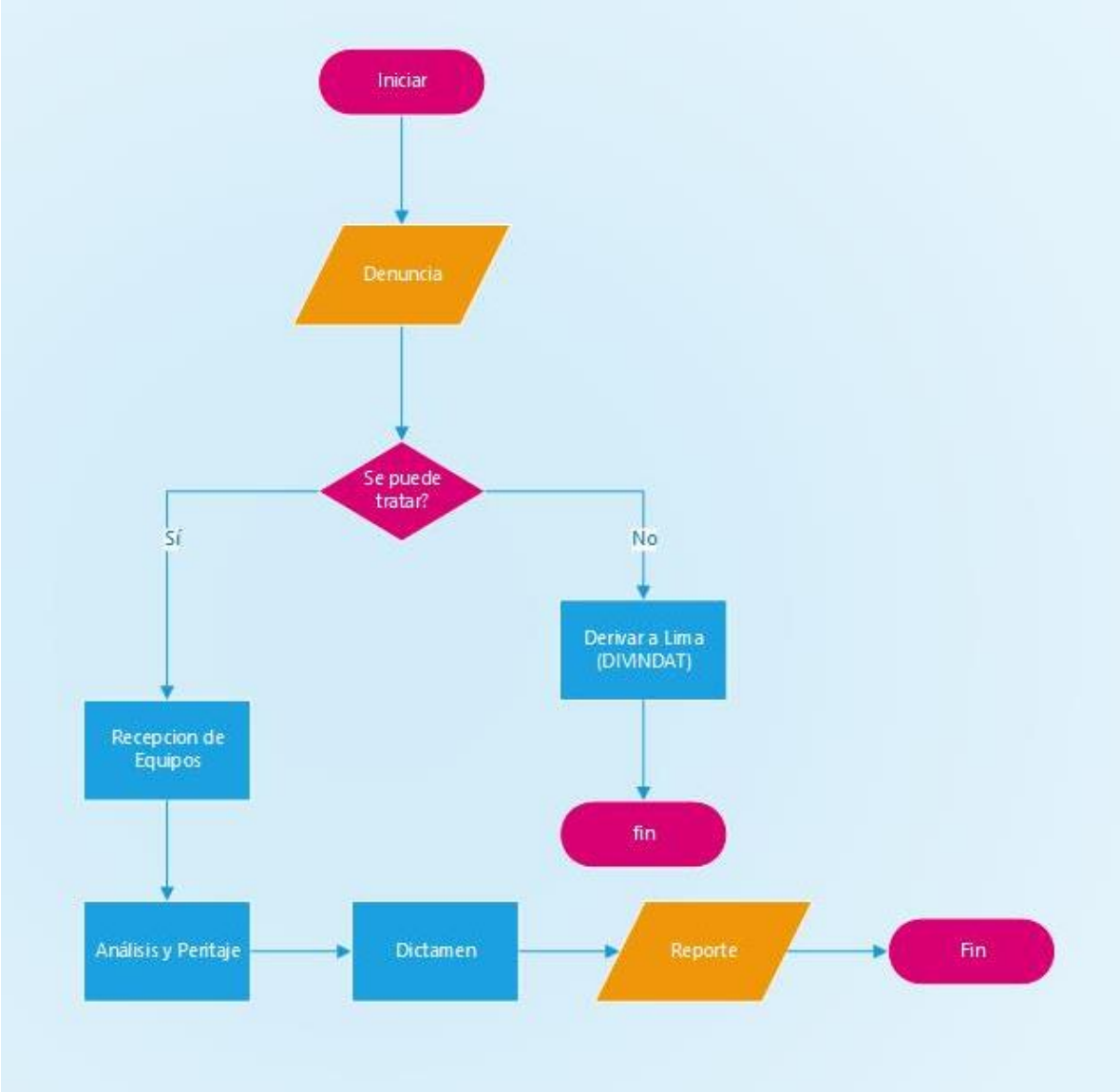


INCIDENCIA	Borrado de los logs accedidos a la base de datos.
RESULTADOS	Lista de archivos de textos eliminados de la papelera de reciclaje
VEREDICTO	Archivos recuperados

Fuente: Propia

Figura 11:

Diagrama de Flujo para el reporte de casos en el peritaje informático



Fuente: Propia

Tabla 16:

Ficha de registro de incidencias

Nro. de Incidencia:			
Fecha y hora:			
Lugar			
Descripción:			
Realizado por:		Firma:	

Fuente: Propia

Tabla 17:

Ficha de registro de incidencias (caso práctico)

Nro. de Incidencia:	001		
Fecha y hora:	05/04/2019		
Lugar	Huánuco – Municipalidad de Huánuco		
Descripción:			
Se encontró la base de datos del sistema de papeletas alterada mediante el registro o logs de los desencadenadores de la base de datos, esto hace suponer que se han estado modificando los registros de las tablas en forma no autorizada.			
Realizado por:		Firma:	

Fuente: Propia

Tabla 18:

Ficha De Evaluación De La Efectividad De La Herramienta

Responda con una "X" en el recuadro correspondiente	**SI**	**NO**
¿La herramienta fue fácil de instalar?		
¿La interfaz de la herramienta fue amigable?		
¿La interfaz de la herramienta fue fácil de usar?		
¿La herramienta cumplió con su objetivo?		
¿Cumplio las expectativas que tenia de la herramienta?		
¿Se encontró con algún error al momento de usar la herramienta?		
Se informa el resultado de la acción.		
Se presenta los mensajes de éxito de forma clara.		
Fácil acceso y retorno al o del sistema de ayuda.		
Se ofrece ayuda contextual en tareas complejas.		
Los iconos son entendibles		
El tamaño y color de la letra permite leer con facilidad.		
Las funcionalidades del sistema son fáciles de ubicar.		

Fuente: Propia

Documentación y redacción de la guia

Para el proceso de la documentación se tomó en cuenta los pantallazos y anotaciones echas en las pruebas realizadas en las máquinas virtuales, las fuentes consultadas fueron los manuales y páginas web de cada herramienta, consolidando los requisitos, instalación y forma de uso. La fuente o descarga de cada herramienta se da a conocer posteriormente en cada sección empleadas por la herramienta.

Las herramientas no necesitaron validarse ya que son herramientas estandarizadas y reconocidas en el ámbito del peritaje informático, además el objetivo de la investigación no se centró en la validación de estas solo en la selección, uso y efectividad de cada uno de ellas.

En la sección anexos se presenta la documentación y redacción de la guía de Peritaje Informático.

4.2 Resultados

Los hallazgos teóricos obtenidos en la investigación están en relación a la aplicación de las herramientas digitales para el peritaje informático y la documentación de la misma, en este caso se consolido los conocimientos adquiridos en el dominio del tratamiento de los delitos informáticos relacionados a: eliminaron y alteración de información.

En cuanto a los hallazgos técnicos, se consiguió la ejecución de las pruebas pilotos usando las herramientas digitales en sus diferentes versiones y escogiendo la más apta para la ejecución, también se pudo emplear otras técnicas no mencionadas usando dichas herramientas, por medio del uso de comandos en el sistema operativo.

La relevancia practica de la investigación reside en la recopilación y conocimiento y puesta a practica de estas herramientas por los trabajadores del área de criminalística, anteriormente a esta investigación dicho personal no tuvo una capacitación o interacción con estas tecnologías limitando su labor diaria, y derivando los casos a la ciudad de lima, en cuanto a la relevancia teoría es en si la metodología, el manual para ser consultado en cualquier momento al tratar de solucionar un caso donde se ponga a prueba las habilidades del peritaje informático.

Al concluir la investigación se hizo la capacitación correspondiente al personal de la unidad policial y se empezaron a utilizar las herramientas informáticas para soportar el proceso de peritaje informático básico asignado a la unidad, se pudieron solucionar algunos casos prácticos como obtención de datos borrados de laptops, recuperación de contraseñas, entre otros.

Se hizo entrega de forma oficial el manual de peritaje informático a la unidad policial instando que se use constantemente y también en la actualización y descarga de las aplicaciones recientes que se muestra en el manual.

Se realizaron las sesiones de capacitación y aplicación demostrando el uso de las herramientas y casos de uso, esto conllevo a que el personal, instale en cada computador las herramientas específicas, se tuvo que añadir como

excepciones al antivirus para que no las elimine, ya que algunas de estas herramientas son detectadas como malware.

La unidad policial conjuntamente con el coronel de la Policía Nacional del Perú: Héctor Bernal Alva, están interesados en la creación de una unidad especial para la gestión de los delitos informáticos, concluyeron afirmando que esta iniciativa es muy interesante ya que propiciaría las gestiones posteriores para la creación y funcionamiento de dicha Área.

Finalmente, se les hizo entrega del manual documentado en cuanto el uso de las herramientas informáticas para el peritaje informático en entornos Windows conjuntamente con el Cd de aplicaciones.

CONCLUSIONES

- Se realizó las coordinaciones previas y entrevistas con el personal encargado de la unidad de criminalística de la Policía de la ciudad de Huánuco, quedando en un acuerdo de capacitación y aplicación en el uso de las herramientas de peritaje informático, para la resolución de casos menores en el ámbito de los delitos informáticos.
- Se efectuó el proceso de selección y pruebas de las herramientas digitales de peritaje informático bajo el entorno Windows. Las pruebas se realizaron bajo un entorno virtual aplicando en casos simulados de delitos informáticos, de todas ellas se seleccionó las más pertinentes en relación a la facilidad de uso, de licencia gratuita y también por la funcionalidad para soportar el proceso de la gestión de delitos informáticos en la ciudad de Huánuco.
- Se elaboró la guía manual de herramientas digitales para la recolección de evidencias digitales, en base a las pruebas realizadas, este manual se utilizó en la capacitación del personal de la unidad personal, así mismo se hizo entrega en formato impreso y digital de dicho manual como herramienta de trabajo diario para la unidad.
- Se ha propiciado el interés por parte de la unidad de criminalística de la ciudad de Huánuco en la gestión para la creación de una unidad especialidad en el tratamiento de los delitos informáticos y uso de las herramientas digitales oficiales para el proceso de peritaje informático.

ANEXOS

GUIA MANUAL PARA LA INFORMÁTICA FORENSE

PARA LA PLATAFORMA

WINDOWS

AUTOPSY

DESCRIPCION

Es una herramienta de análisis forense digital gratuita desarrollada para investigar lo ocurrido en el equipo. Es rápida ya que ejecuta varias tareas en segundo plano, aprovechando los núcleos del procesador, para tener resultados lo antes posible.

REQUISITOS PARA INSTALAR

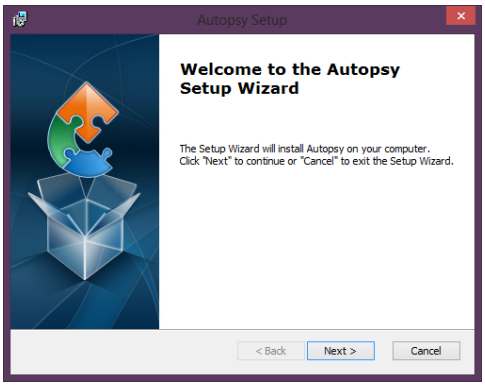
Es altamente recomendable remover o deshabilitar cualquier software antivirus desde las computadoras en las cuales se procesarán o revisarán los casos. Frecuentemente el software antivirus podría crear conflicto con el software forense y puede poner en cuarentena o incluso borrar algunos de los resultados antes de tener la oportunidad de analizarlos.

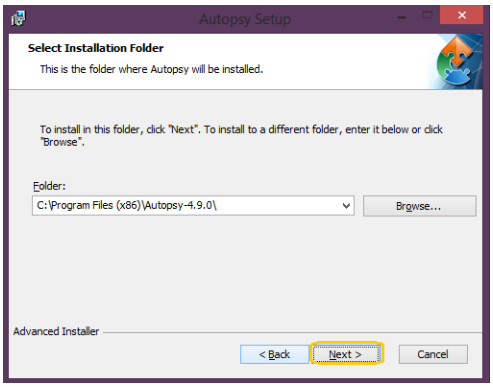
DESCARGA DE LA PÁGINA OFICIAL

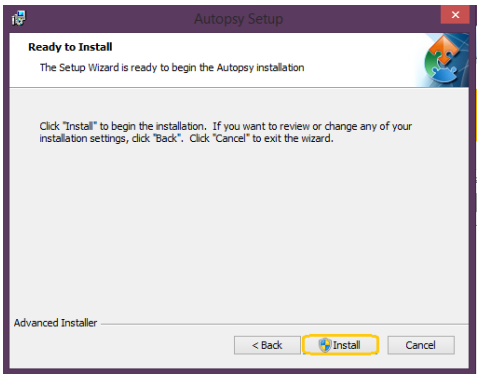
https://www.sleuthkit.org/autopsy/download.php

INSTALACIÓN

1. Ejecutar el archivo de extensión “msi” de Autopsy.
2. Si Windows presenta UAC (User Acccount Control), hacer clic en Yes.
3. Hacer clic a través de las cajas de diálogo hasta llegar al botón de nombre “Finish” y hacerle nuevamente clic.
4. Autopsy ahora está completamente instalado.

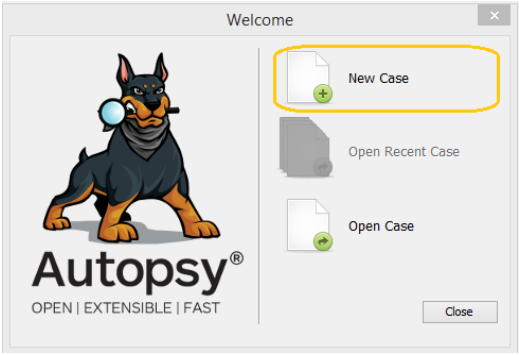




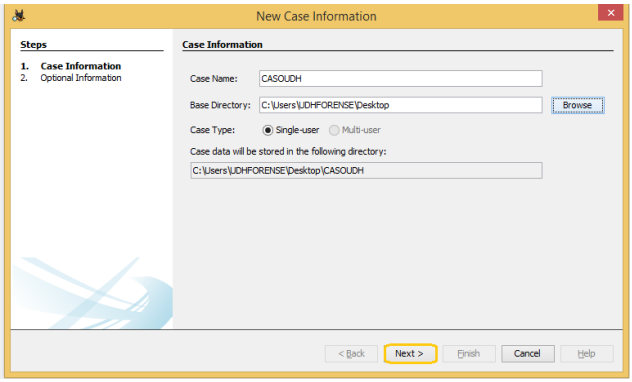


PRACTICA

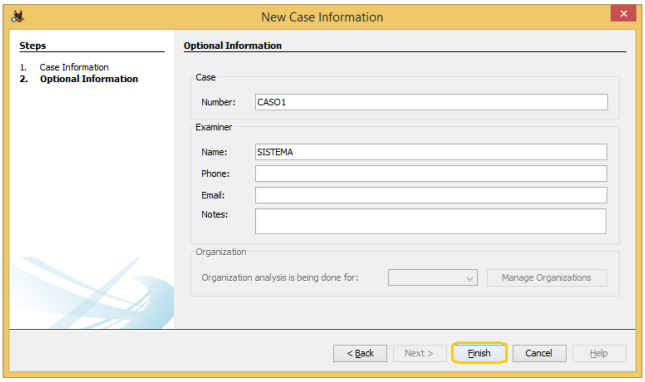
- Crear un caso nuevo.



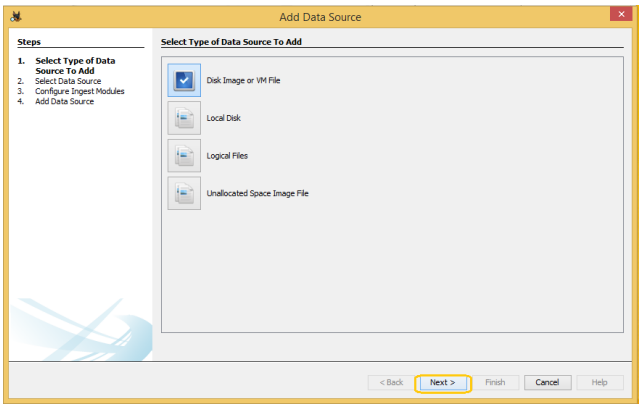
- Ingresamos el caso nombre (CASOUDH) y la dirección, por ejemplo en escritorio (Desktop) y next.



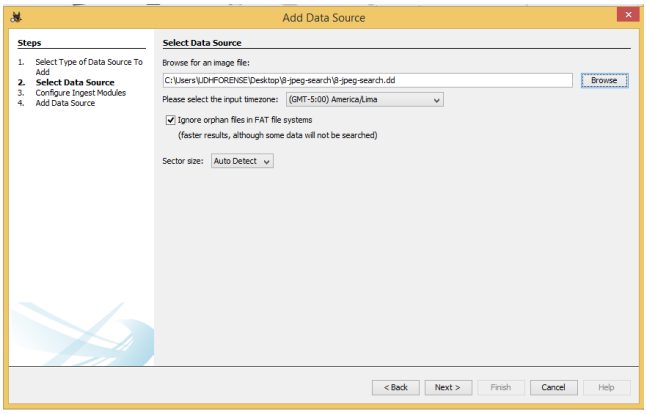
- Definimos el número de caso (CASO1) y el nombre examinador ejemplo (SISTEMA).



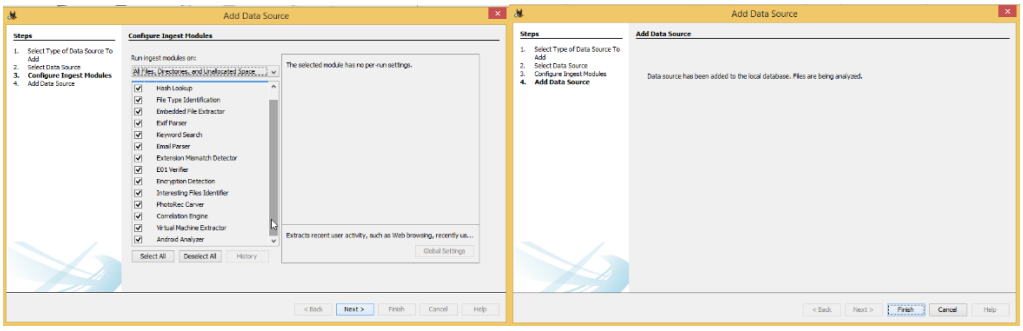
- Seleccionar con lo que vamos a trabajar por ejemplo (Disk Image or VM File) y next.



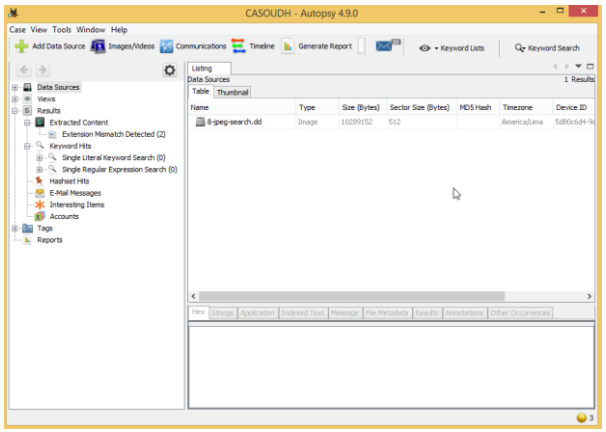
- Hacemos clic en browser, buscamos el fichero imagen del disco extraído un disco que fue descargado del repositorio de imágenes públicas su extensión es (.dd) y podemos escoger la zona de horario.



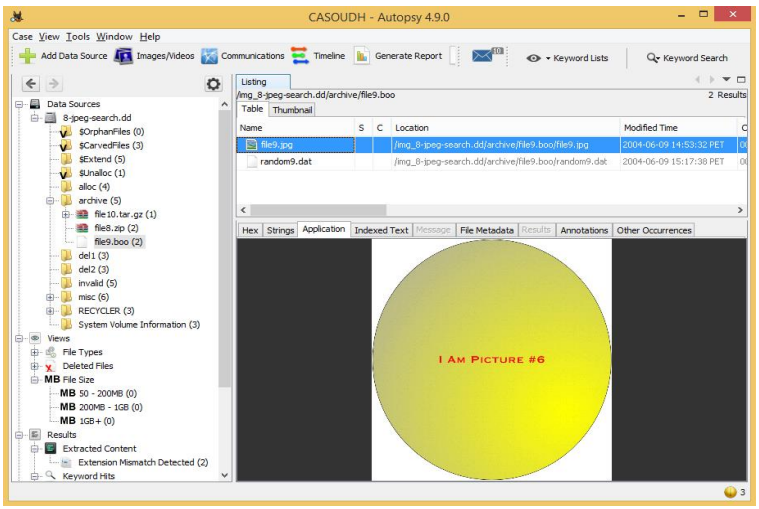
- seleccionar todos los módulos que se va a realizar, next y finish.



- Tenemos nuestro disco analizado.



- Tenemos archivos que podemos visualizar como por ejemplo imágenes, archivos eliminados, etc.



OSFORENSICS

DESCRIPCION

Es un software de análisis forense. Lo más interesante es que deja utilizar **algoritmos** *hash* **para obtener "huellas digitales" de cada archivo que poseemos en la PC**. De esta forma podemos comparar si un archivo fue borrado, modificado, o alterado de algún modo, podemos elegir entre varios tipos de algoritmos diferentes: **MD5, SHA-1, SHA-256**, etc.

REQUISITOS PARA INSTALAR

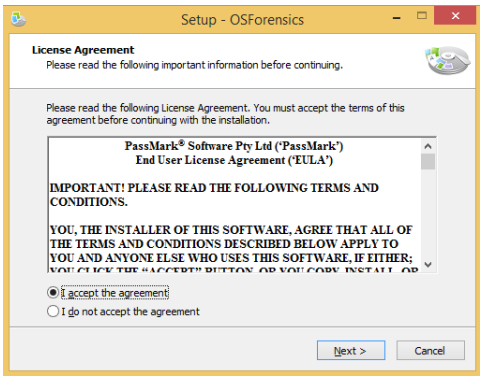
- Windows XP SP3, Vista, Win 7, Win 8, Win 10.
- Windows Server 2000, 2003, 2008, 2012.
- 32 bits y 64 bits compatibles (se recomiendan 64 bits).
- Mínimo de 1 GB de RAM. (Se recomienda 4GB +).
- 60 MB de espacio libre en disco, o se puede ejecutar desde una unidad USB.

DESCARGA DE LA PÁGINA OFICIAL

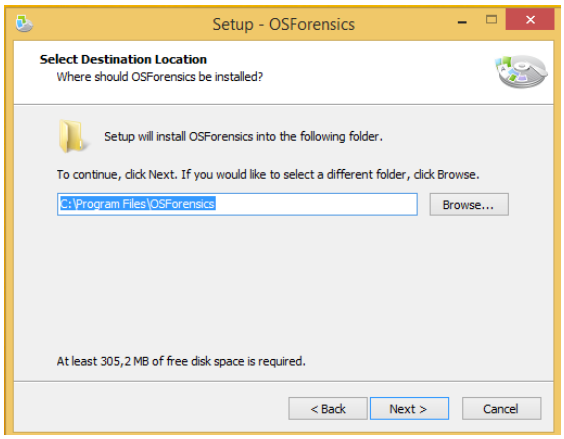
https://www.osforensics.com/download.html

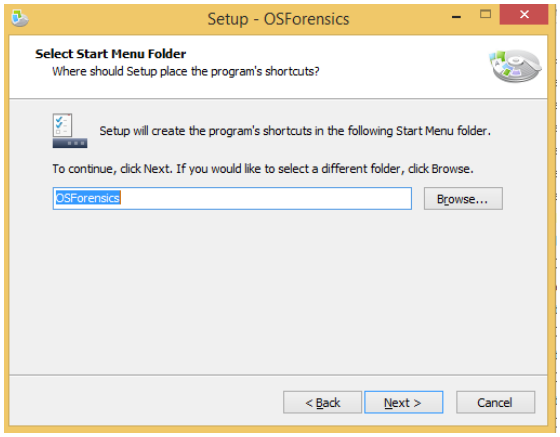
INSTALACIÓN

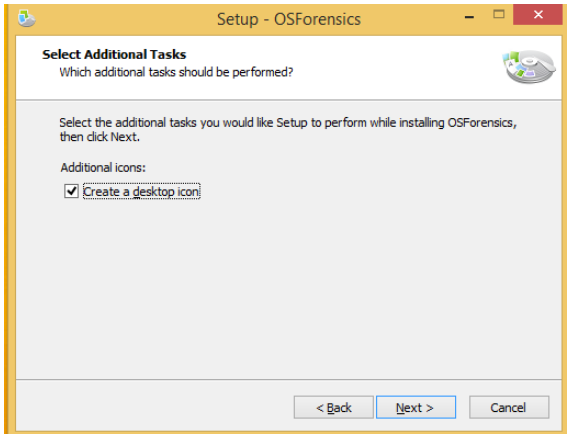
1. Ejecutamos el archivo, luego Aceptar las condiciones y next.

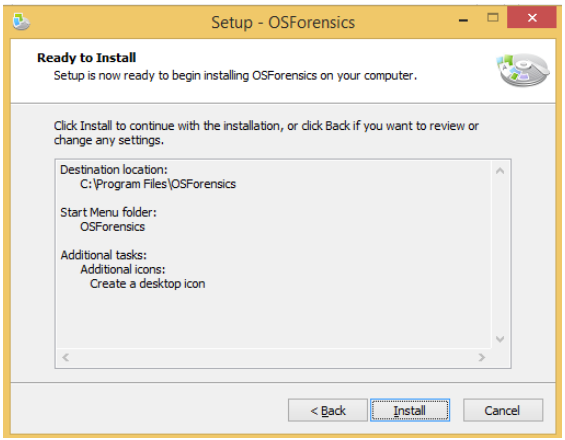


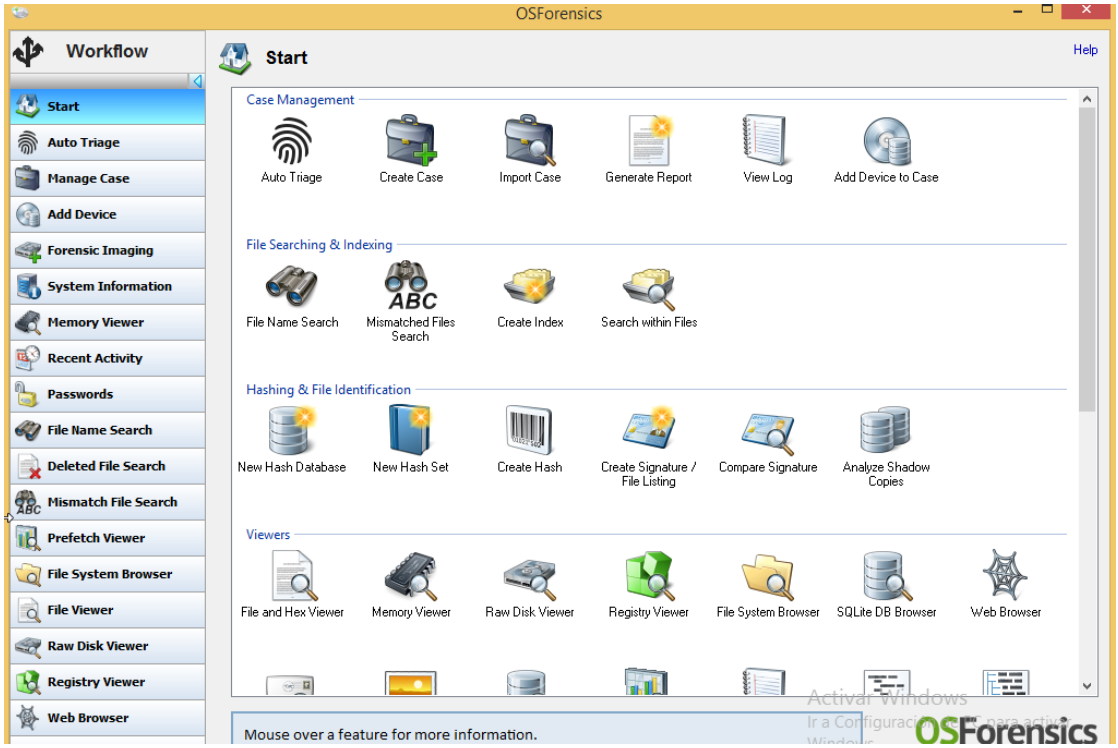
2. Seleccionamos la ruta donde se va instalar y todo next.


Setup - OSForensics
Select Destination Location
Where should OSForensics be installed?
Setup will install OSForensics into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\OSForensics
Browse...
At least 305,2 MB of free disk space is required.
< Back
Next >
Cancel


Setup - OSForensics
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
OSForensics
Browse...
< Back
Next >
Cancel

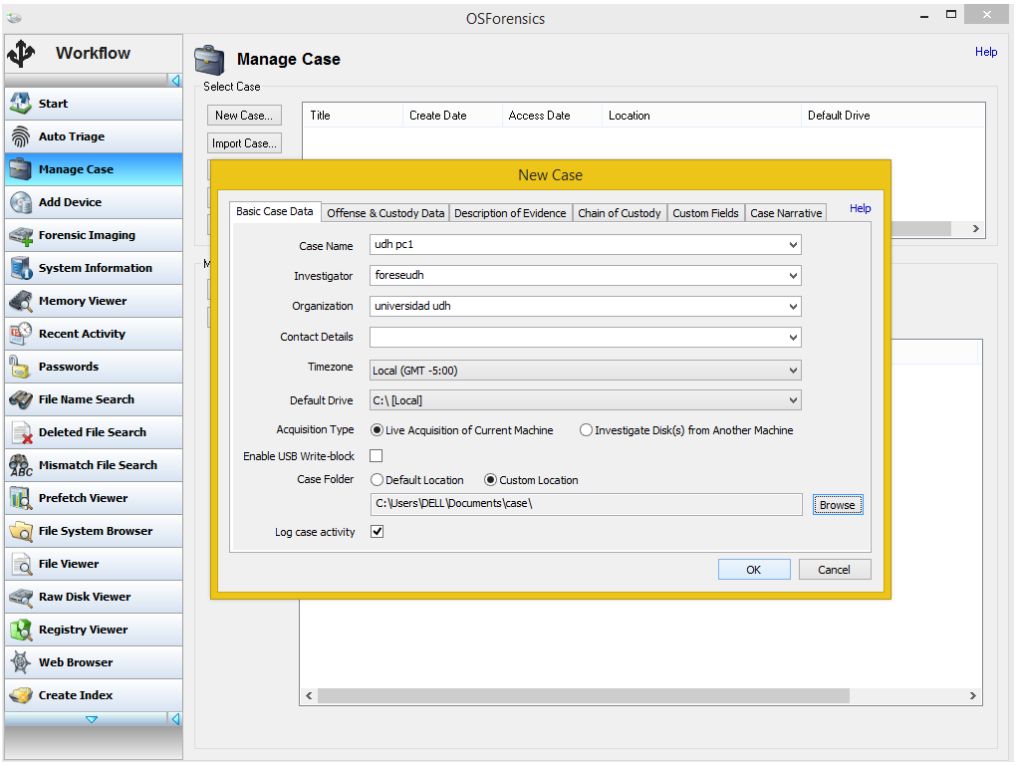

Setup - OSForensics
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing OSForensics, then click Next.
Additional icons:
Create a desktop icon
< Back
Next >
Cancel


Setup - OSForensics
Ready to Install
Setup is now ready to begin installing OSForensics on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\OSForensics
Start Menu folder:
OSForensics
Additional tasks:
Additional icons:
Create a desktop icon
< Back
Install
Cancel

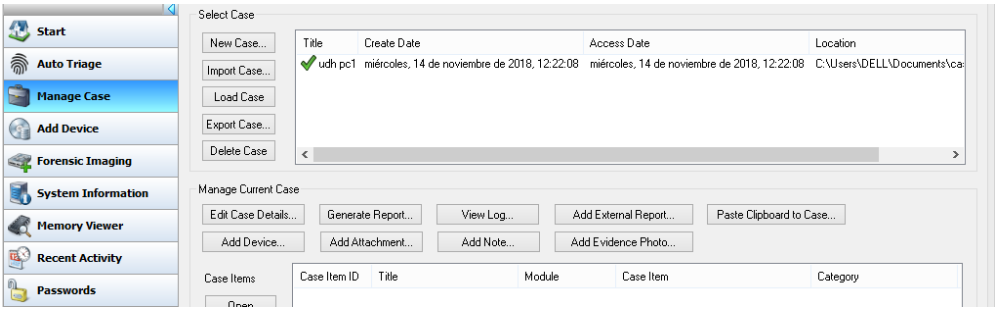

OSForensics
Workflow
Start
Auto Triage
Manage Case
Add Device
Forensic Imaging
System Information
Memory Viewer
Recent Activity
Passwords
File Name Search
Deleted File Search
Mismatch File Search
Prefetch Viewer
File System Browser
File Viewer
Raw Disk Viewer
Registry Viewer
Web Browser
Start
Help
Case Management
Auto Triage
Create Case
Import Case
Generate Report
View Log
Add Device to Case
File Searching & Indexing
File Name Search
Mismatched Files Search
Create Index
Search within Files
Hashing & File Identification
New Hash Database
New Hash Set
Create Hash
Create Signature / File Listing
Compare Signature
Analyze Shadow Copies
Viewers
File and Hex Viewer
Memory Viewer
Raw Disk Viewer
Registry Viewer
File System Browser
SQLite DB Browser
Web Browser
Mouse over a feature for more information.
OSForensics

PRACTICA

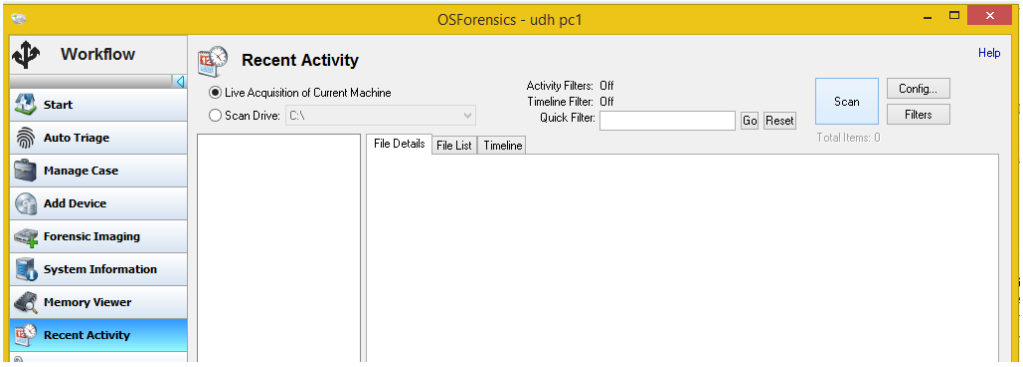
1. Vamos a crear un nuevo caso y clic en ok.



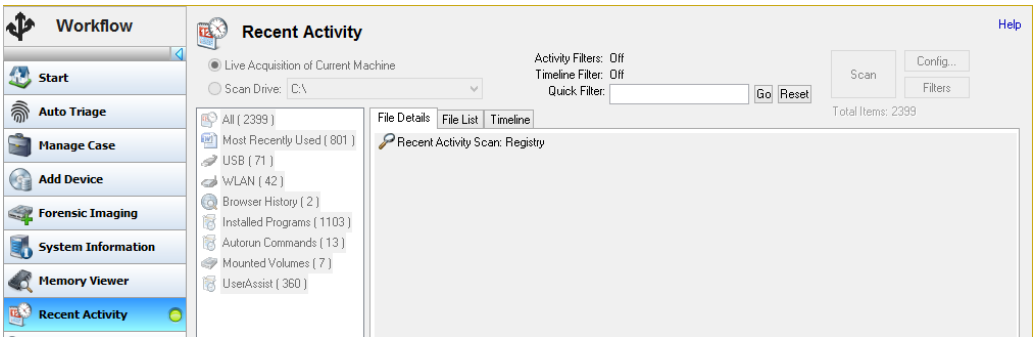
2. Cuando esta creado el nuevo caso.



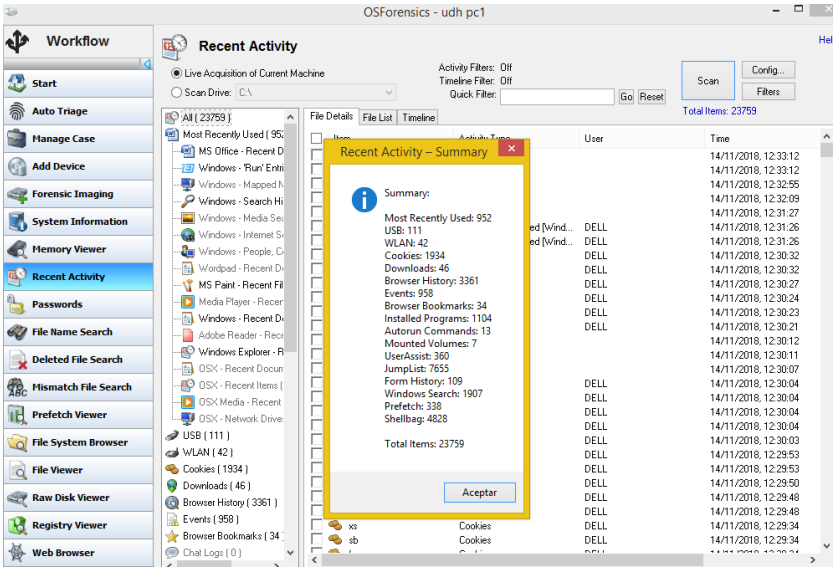
3. Hacemos un clic en Recent Activity (nos permite escanear todas las actividades recientes) y clic en "Scan" para realizar la búsqueda.



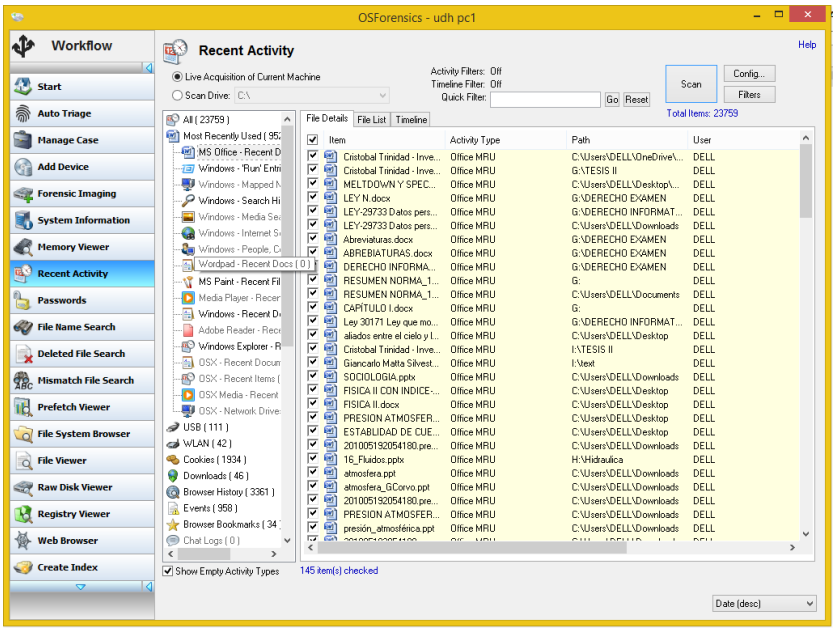
4. Como se puede apreciar, se está haciendo la búsqueda, todas las actividades.



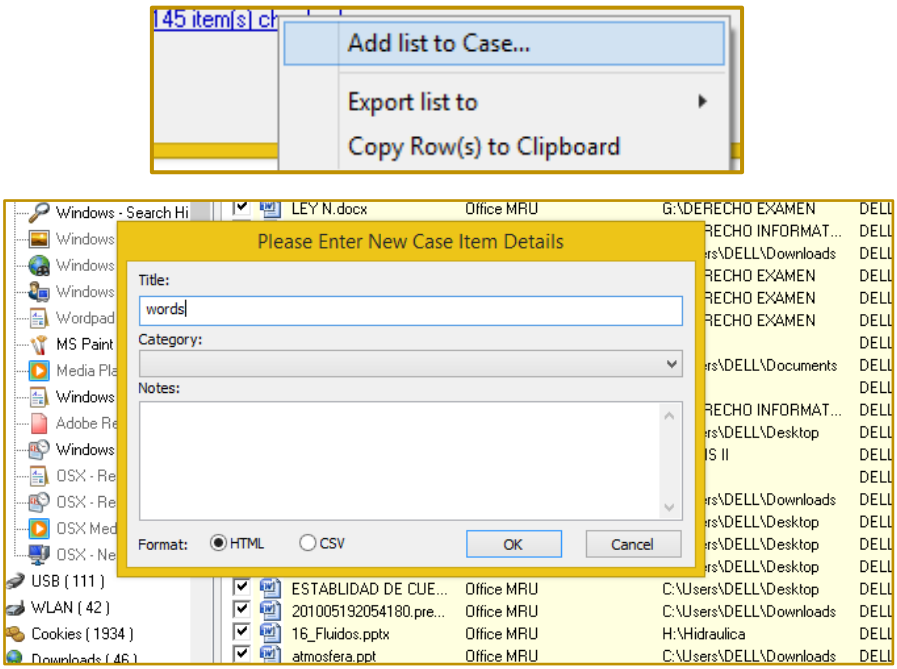
5. Clic en aceptar y se verá todas las configuraciones recientes.



6. Por ejemplo veremos todos los archivos de Ms Office 145 archivos y estos archivos podemos agregar al caso.



7. Para poder agregar al caso solo clic derecho en ítem(s) , clic en "add list to case...", le agregamos un nombre y clic en ok.



NOTA

En realidad el programa es mas optimo si se adquiere con la licencia completa, pero si el programa se instala en modo trial, el tiempo y algunas opciones serán limitadas, pero de todas maneras es muy útil para poder recuperar archivos cuando se encuentra en modo trial si se usara de forma provisional.

FOCAPRO

DESCRIPCION

FOCA (*Llamado así en honor a Francisco OCA, aunque luego buscaran las siglas "Fingerprinting Organizations with Collected Archives"*) es una herramienta para encontrar Metadatos e información oculta en documentos de Microsoft Office, Open Office y documentos PDF/PS/EPS, extraer todos los datos de ellos exprimiendo los ficheros al máximo y una vez extraídos cruzar toda esta información para obtener datos relevantes de cualquier entidad.

REQUISITOS PARA INSTALAR

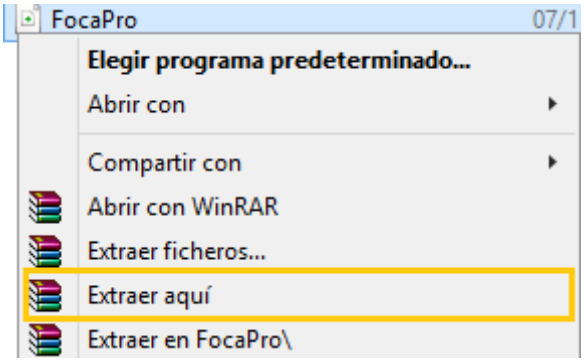
- Windows XP SP3, Vista, Win 7, Win 8, Win 10
- Windows Server 2000, 2003, 2008, 2012
- 32 bits y 64 bits compatibles
- Mínimo de 1 GB de RAM
- 800 MB de espacio libre en disco, o se puede ejecutar desde una unidad USB

DESCARGA DE LA PÁGINA OFICIAL

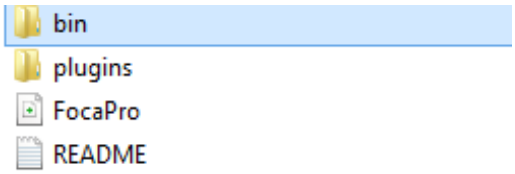
https://www.elevenpaths.com/es/labstools/foca-2/index.html

INSTALACIÓN

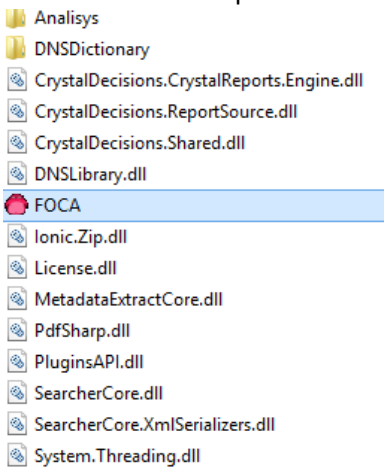
- Una vez descargado, extraer.



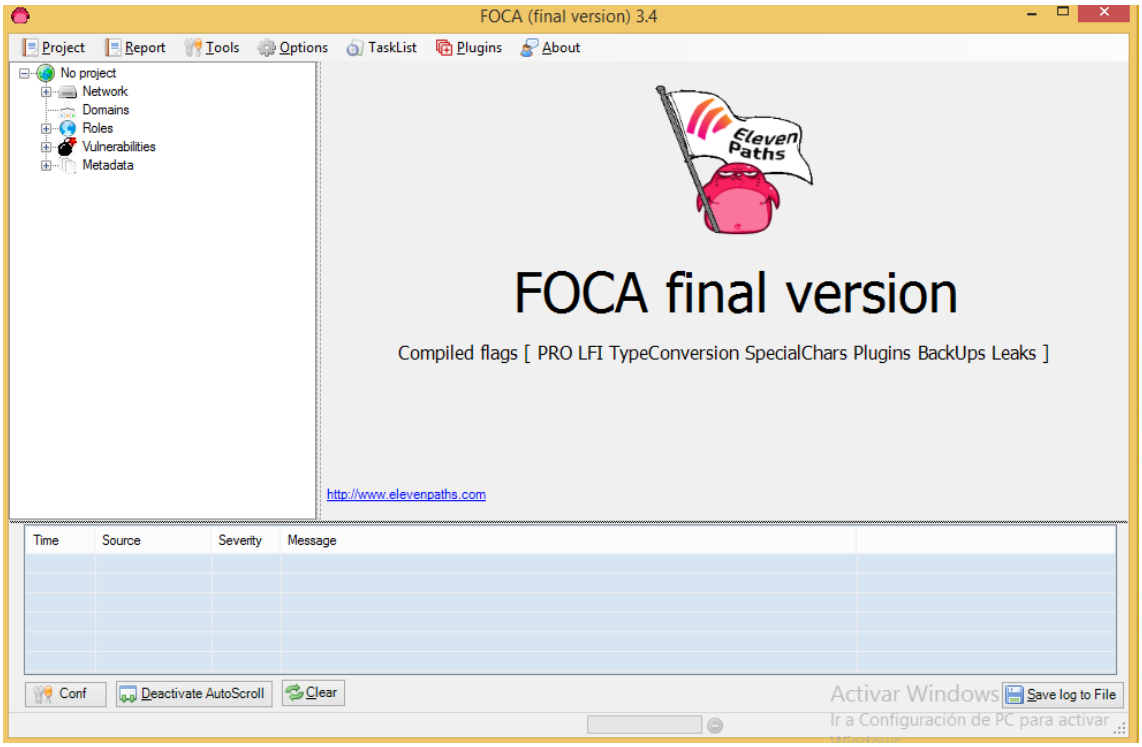
- Se extraerá todos los archivos y luego abrimos la carpeta **bin.**



- Doble clic en FOCA para abrir.

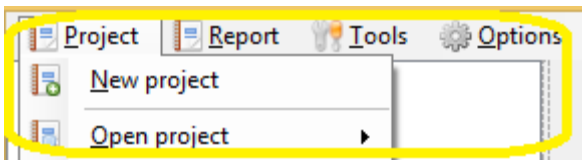


- El software foca.

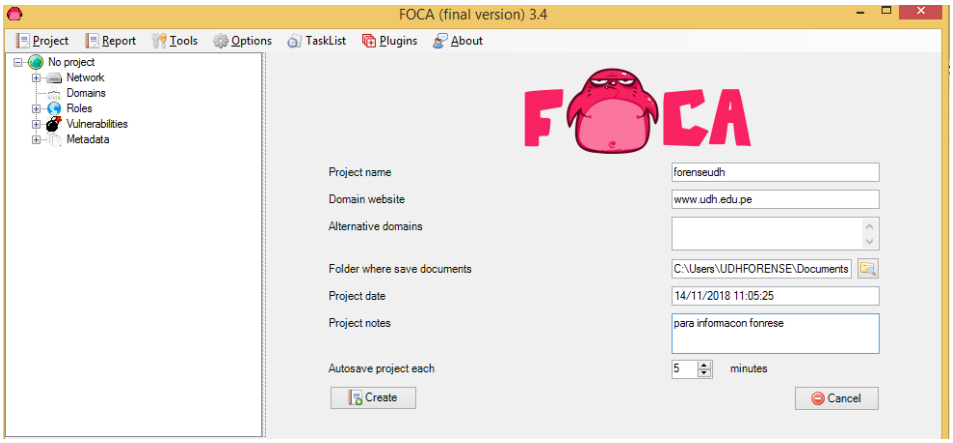


PRACTICA

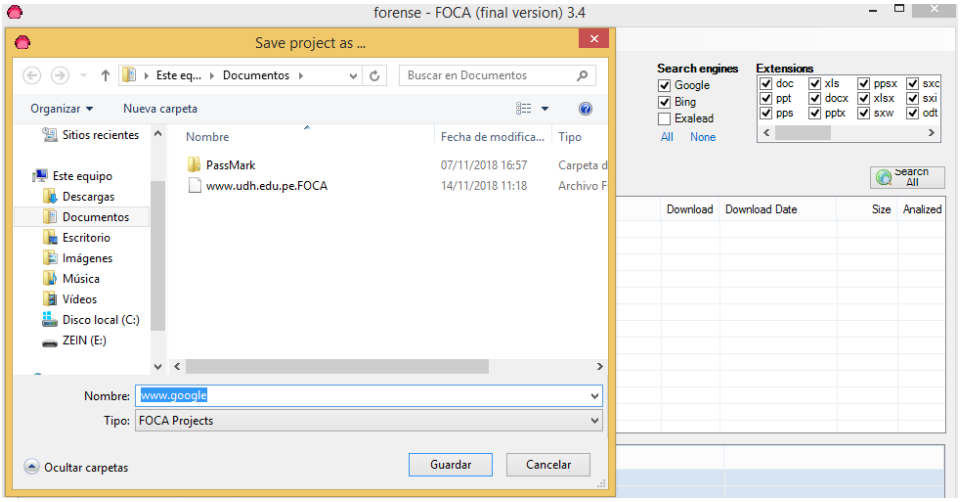
1. Clic en la pestaña Project -> clic en "new project"



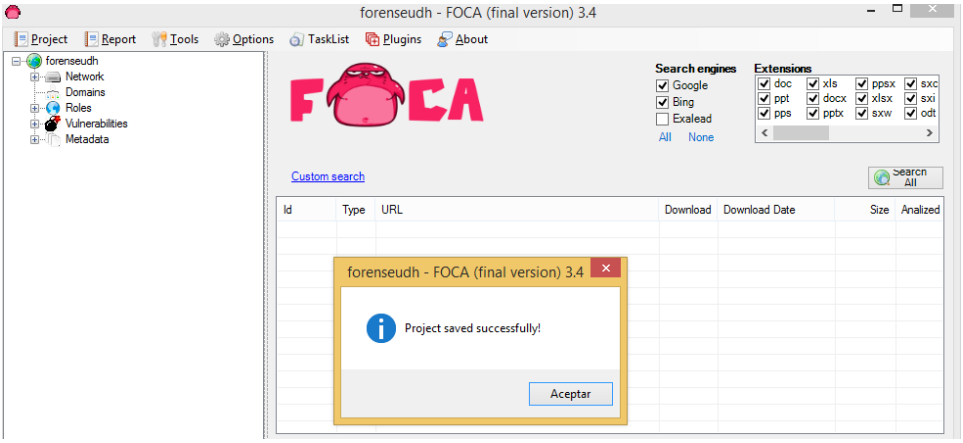
2. En la ventana siguiente rellenamos los campos (nombre, dominio, donde se va guardar, nota y fecha) el tiempo del proceso puede durar 5 minutos aproximadamente luego clic en Create.



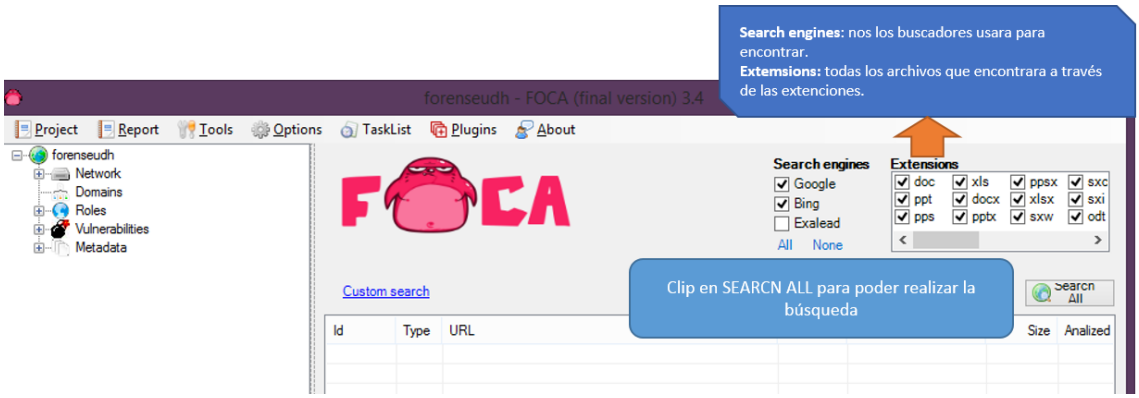
3. Clic guardar.



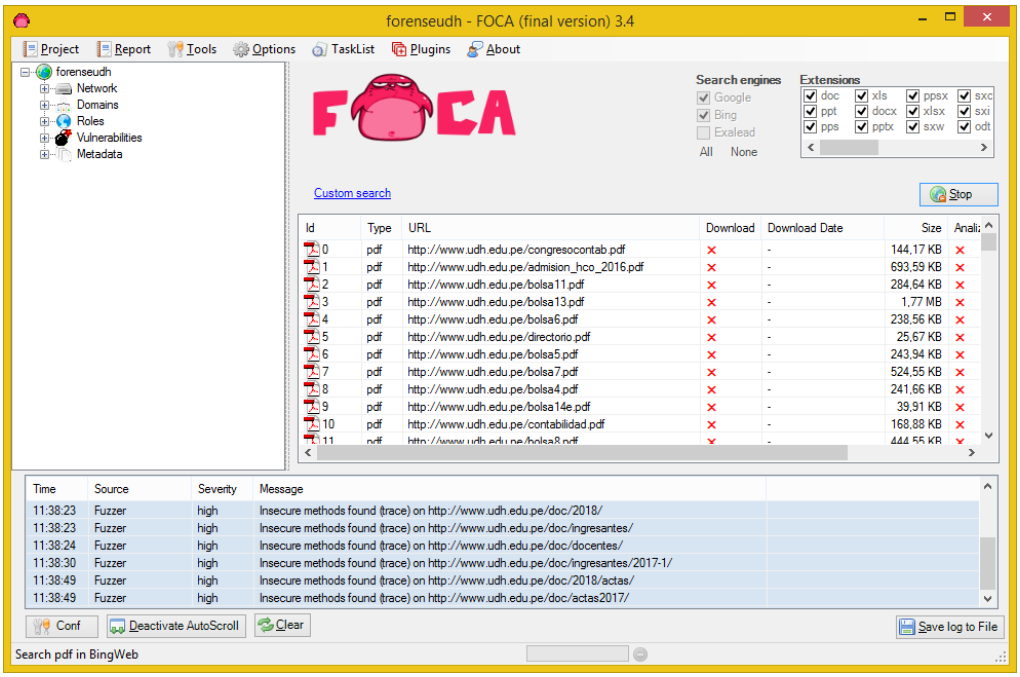
4. Clic en aceptar.



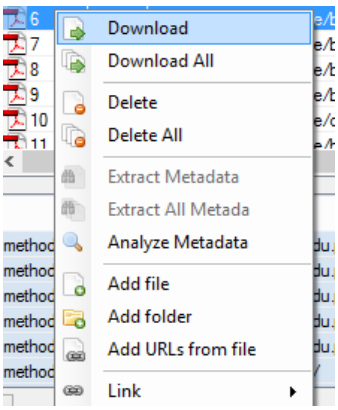
5. Realizaremos la búsqueda de todo el contenido de la dirección.

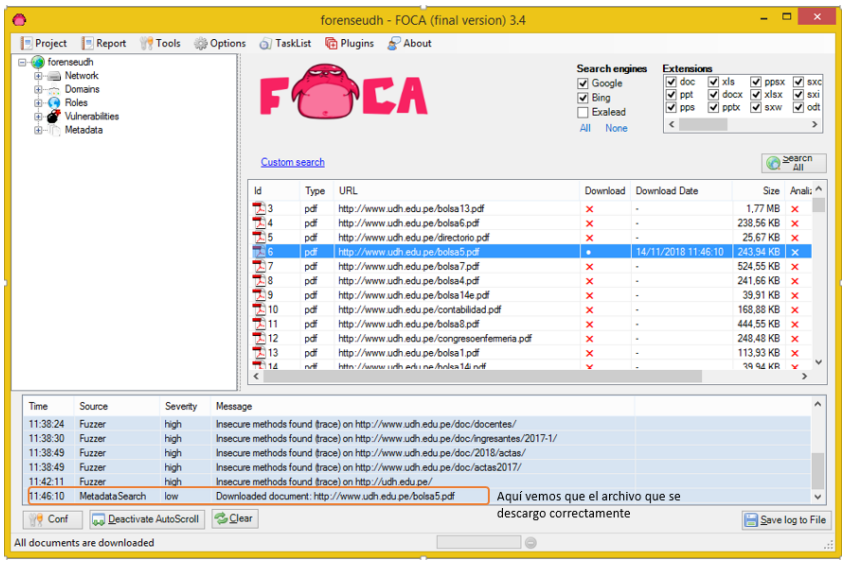


6. Como se puede apreciar tenemos varios resultados de la búsqueda.

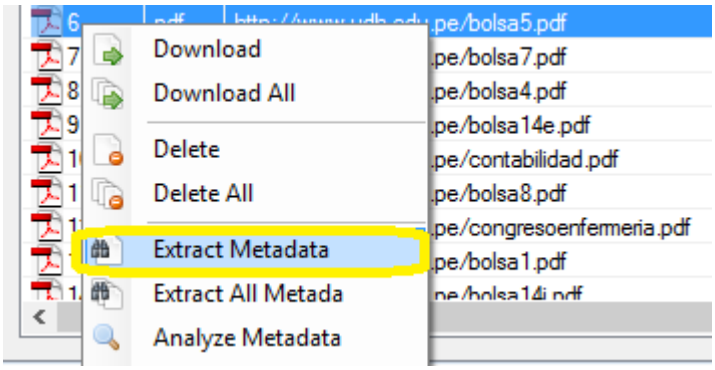


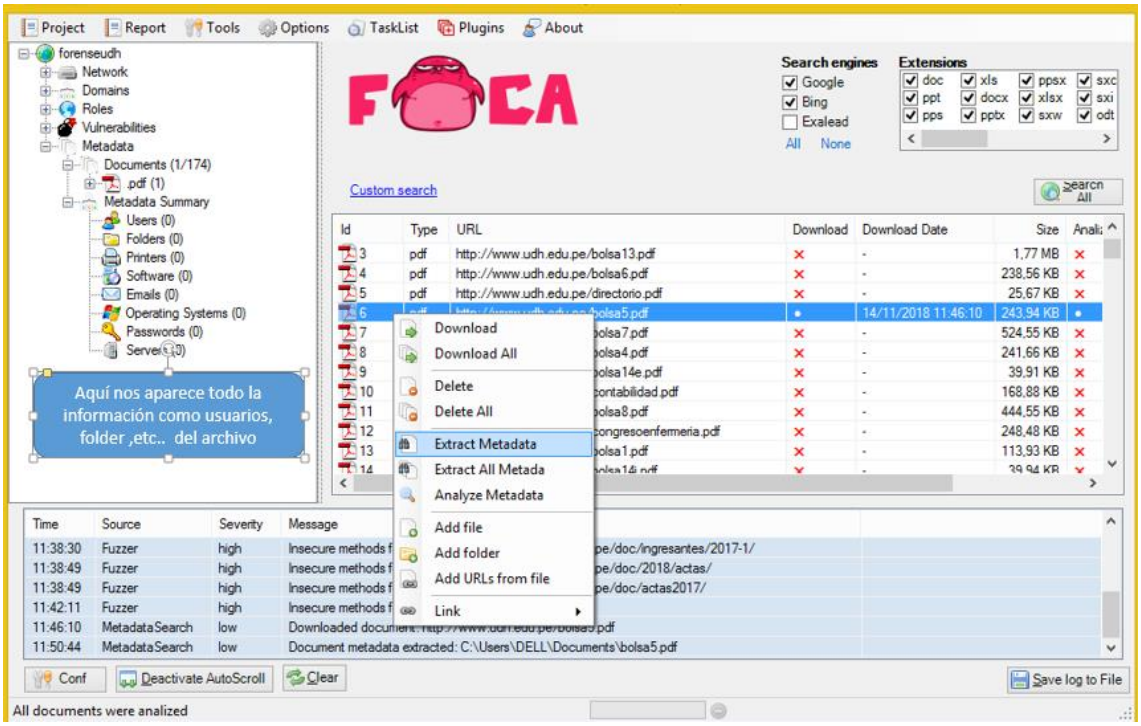
7. En esta parte podemos descargar el archivo para poder hacer el respectivo análisis.



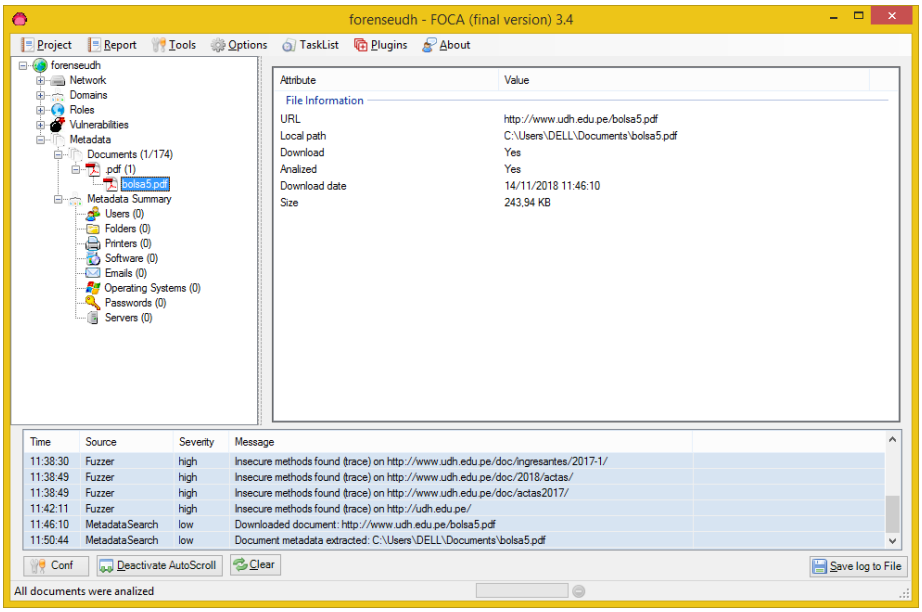


8. Luego extraeremos las metadatas.





9. Haremos clic en Archivo, para ver todo la información y también se puede consultar las demás opciones como usuarios, fólderes, imágenes, etc.



TESTDISK

DESCRIPCION

Es un software de recuperación de datos de archivos, diseñado para recuperar archivos perdidos incluidos videos, documentos, archivos de discos duros, CD-ROM e imágenes perdidas de la memoria de la cámara digital. PhotoRec ignora el sistema de archivos y persigue los datos subyacentes, por lo que seguirá funcionando incluso si el sistema de archivos de sus medios ha sido dañado o reformateado.

REQUISITOS PARA INSTALAR

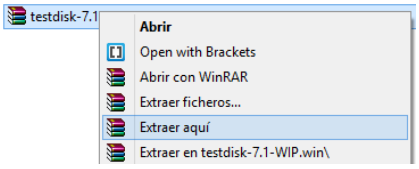
- DOS / Windows 9x
- Windows NT 4/2000 / XP / 2003 / Vista / 2008/7/10
- Linux
- FreeBSD, NetBSD, OpenBSD
- Sol solaris
- Mac OS X
- Mínimo de 1 GB de RAM
- 700 MB de espacio libre en disco

DESCARGA DE LA PÁGINA OFICIAL

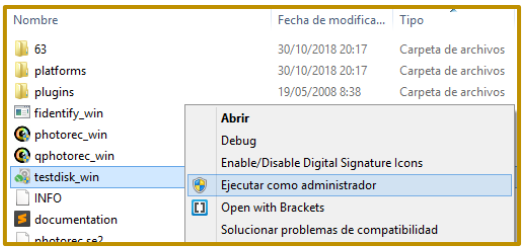
https://www.cgsecurity.org/wiki/TestDisk_Download

INSTALACIÓN

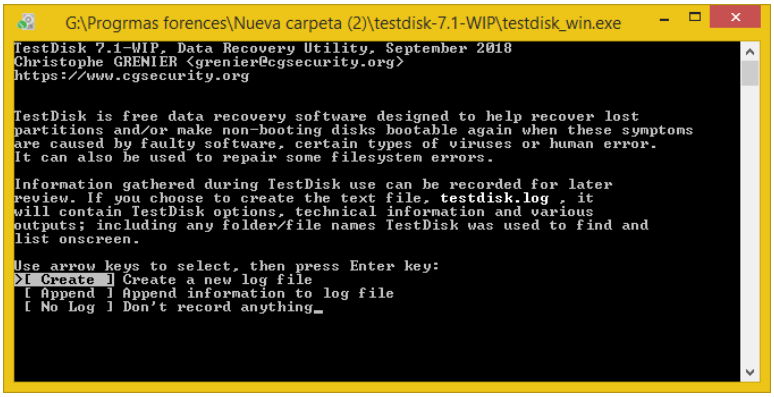
1. Extraemos los archivos.



2. Una vez extraído, ingresar a la carpeta y ejecutar al programa como administrador.

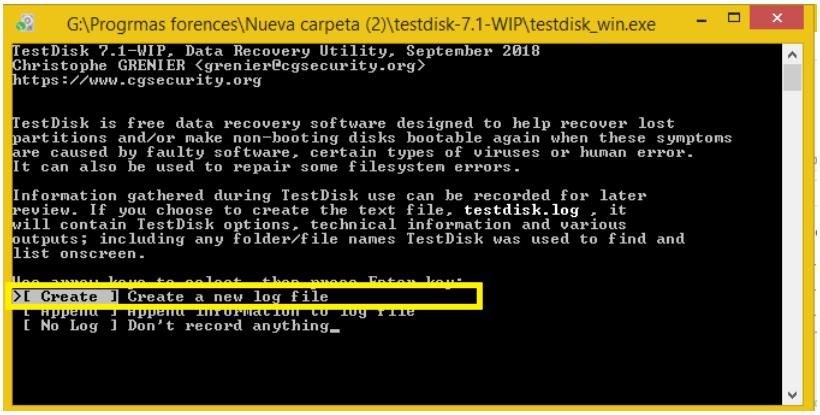


3. Se abrirá la siguiente ventana.

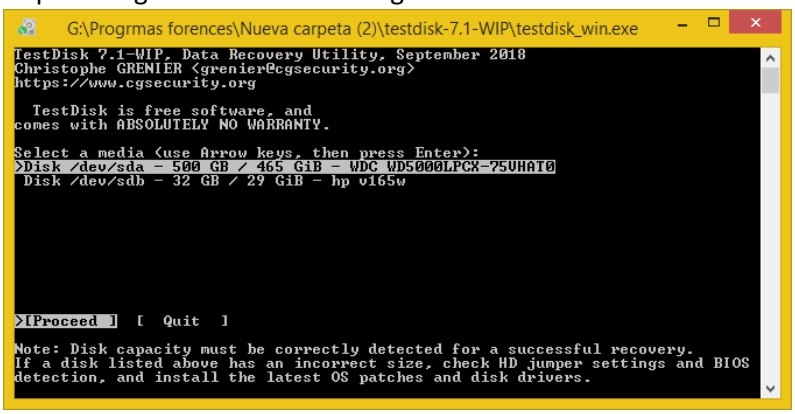


PRACTICA

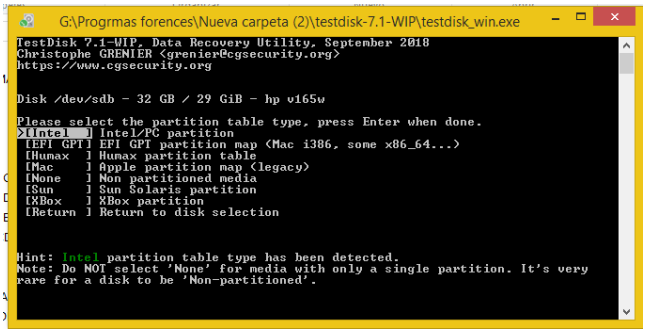
1. Una vez ejecutado, seleccionamos (Create a new log file) y presionamos Enter.



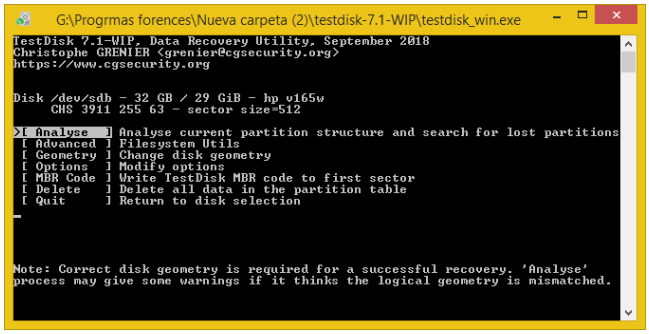
2. En esta venta elegimos la unidad vamos a recuperar datos borrados,
   Por ejemplo escogeremos la unidad 32gb



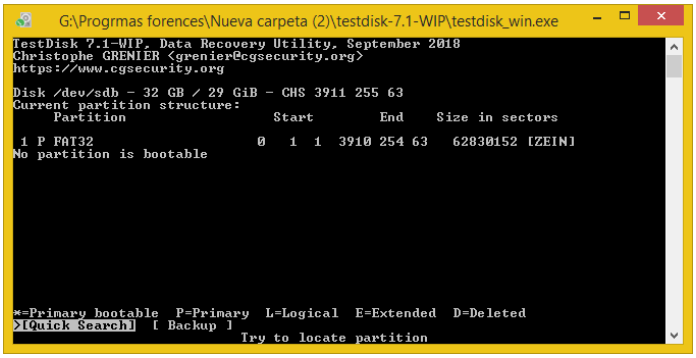
3. En esta parte seleccionamos la partición de la tabla o tipo y presionamos Enter, en este caso será (Intel)



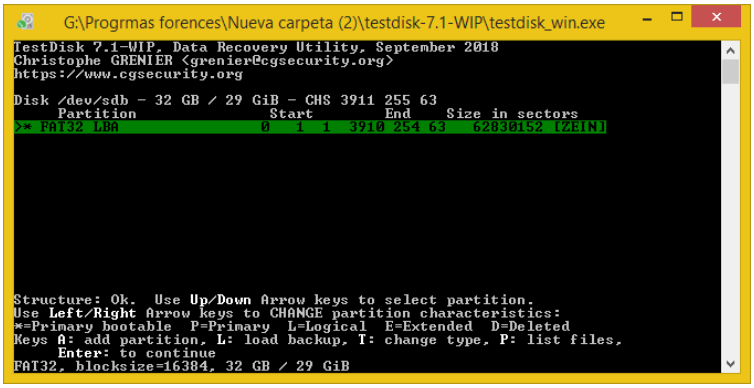
4. Aqui seleccionaremos Analyse y luego Enter.



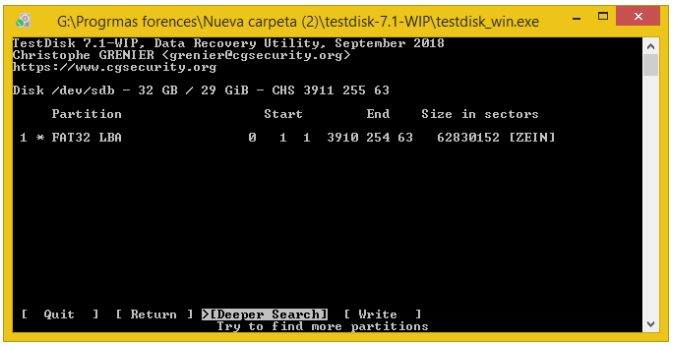
5. En esta parte seleccionaremos Quick Search y luego enter



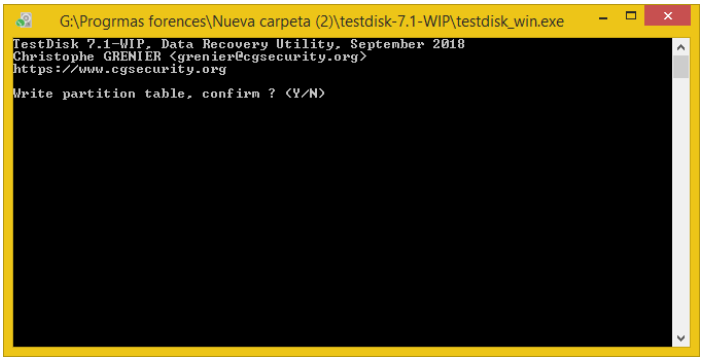
6. Aparecen todas las particiones existentes, en este caso elegiremos la partición que se hara la recuperación de datos y Enter.



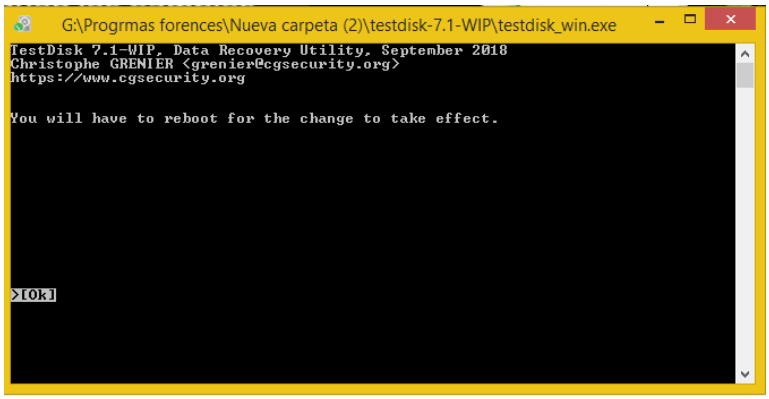
7. Seleccionamos la opción Write y Enter.



8. Presionamos la letra "Y" y Enter para seguir con el proceso.



9. Presionamos Enter, se deberá reiniciar la PC para que se aplique los cambios realizados y poder visualizar la partición recuperada.



Nota

Al reiniciar la PC se visualizara el disco eliminado por error con todos los datos obtenidos.

DMDE

DMDE

DESCRIPCION

DMDE es un potente software para la búsqueda, edición y recuperación de datos en discos. Puede recuperar la estructura del directorio y los archivos en algunos casos complicados mediante el uso de algoritmos especiales cuando otro software no puede ayudar. El software está listado, revisado y premiado en revistas y catálogos.

REQUISITOS PARA INSTALAR

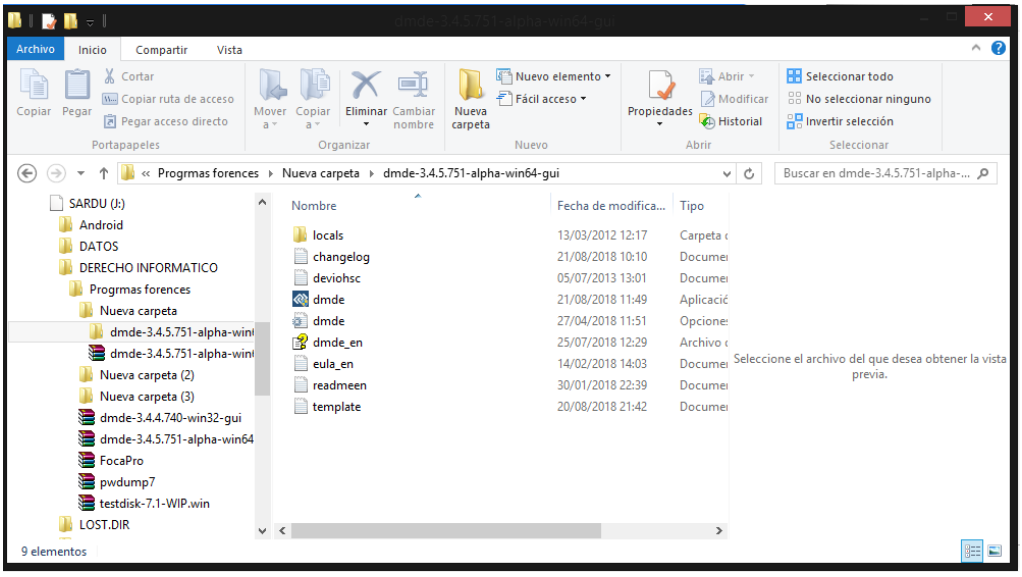
DMDE es compatible con NTFS, FAT12 / 16, FAT32, exFAT, Ext2 / 3/4, HFS + / HFSX y se ejecuta en Windows 98 / .. XP / .. 7 / .. 10, Linux, macOS, DOS (Consola).

DESCARGA DE LA PÁGINA OFICIAL

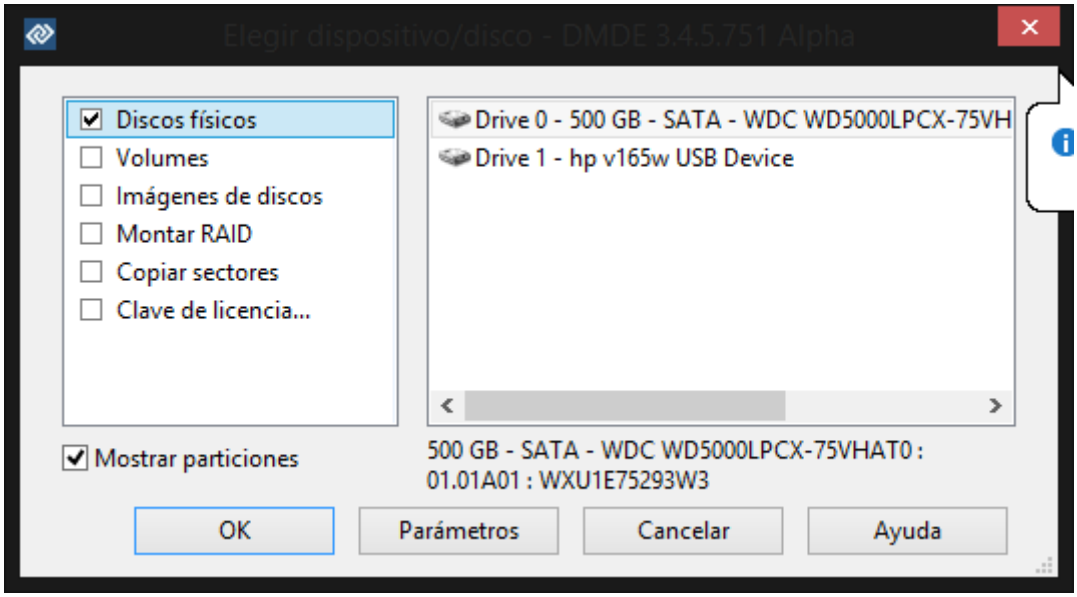
https://dmde.com/download.html

INSTALACIÓN

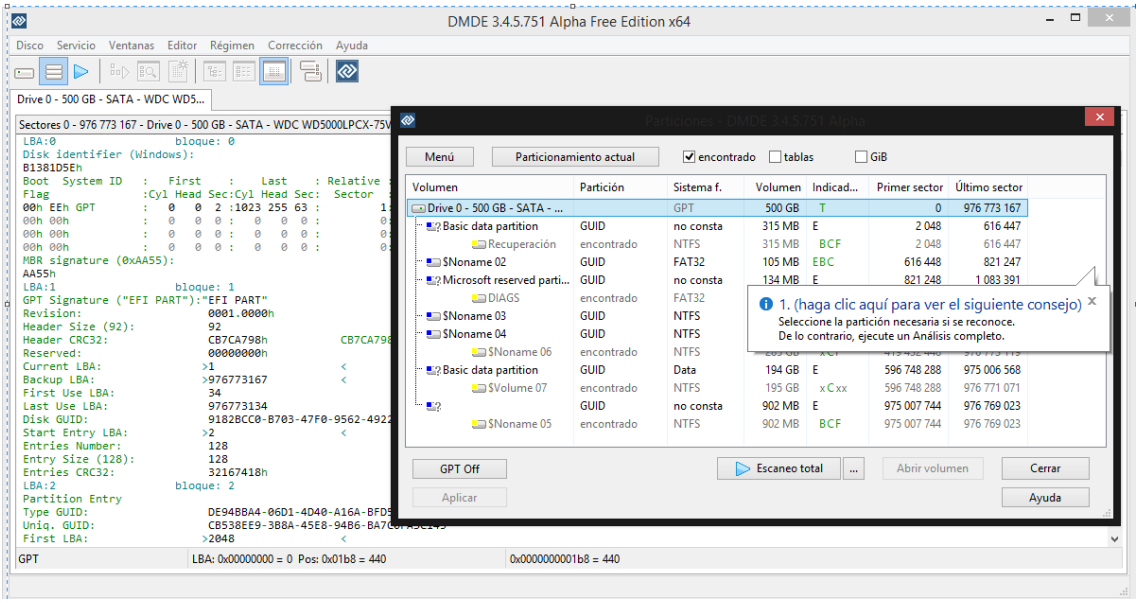
- Para la instalación solo hay que descomprimirlo y ejecutamos el programa como administrador.



- Escogemos el disco que vamos a examinar.



- Nos presentara todas las particiones que se encuentran en el disco, luego clic en escaneo total .

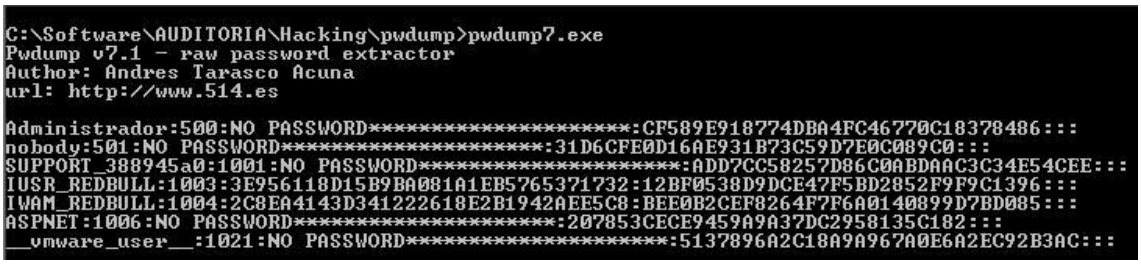


PWdump7

PWDUMP7

DESCRIPCION

Un nuevo dumper de contraseñas para Windows llamado PWDUMP7. La principal diferencia entre pwdump7 y otras herramientas de pwdump es que la herramienta se ejecuta al extraer el archivo SAM y SYSTEM binario del sistema de archivos y luego se extraen los hashes. Para esa tarea se utilizan los controladores del sistema de archivos NTFS y FAT32 de Rkdetector



USO:

- pwdump7.exe (contraseñas del sistema de volcado)
- pwdump7.exe -s <samfile> <systemfile> (Dump contraseñas de los archivos)
- pwdump7.exe -d <nombre_de_archivo> [destionation] (Copiar nombre de archivo a destionation)
- pwdump7.exe -h (Mostrar esta ayuda)

REQUISITOS PARA INSTALAR

- Disco espacio: 900mb
- Memoria: 1gb

DESCARGA DE LA PÁGINA OFICIAL

http://www.tarasco.org/security/pwdump_7/

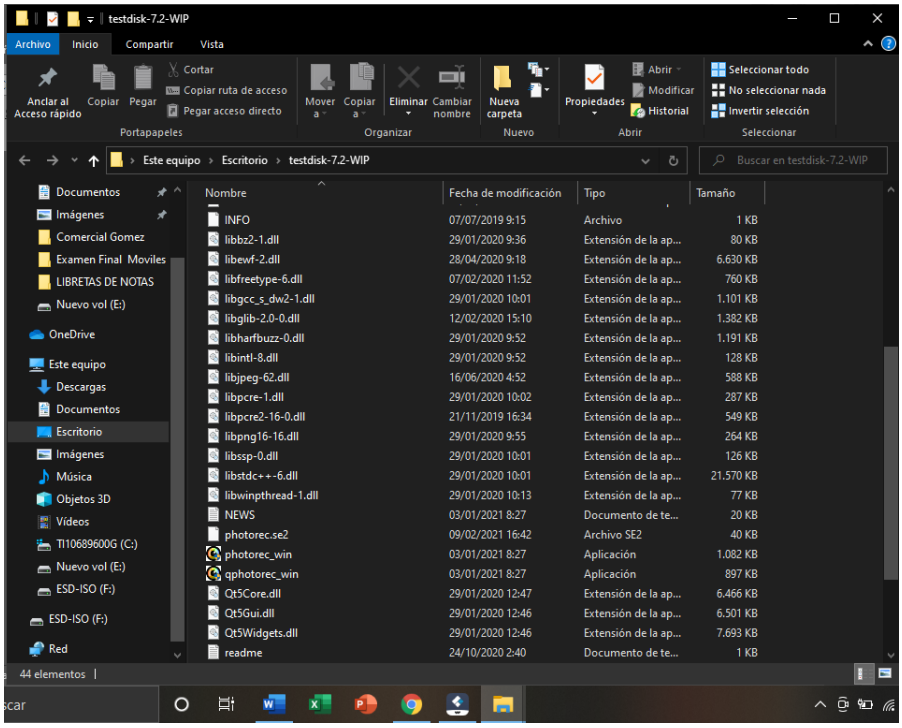
PRUEBAS PILOTO

HERRAMIENTA QUE SE PUEDE USAR PARA RECUPERAR UN ARCHIVO

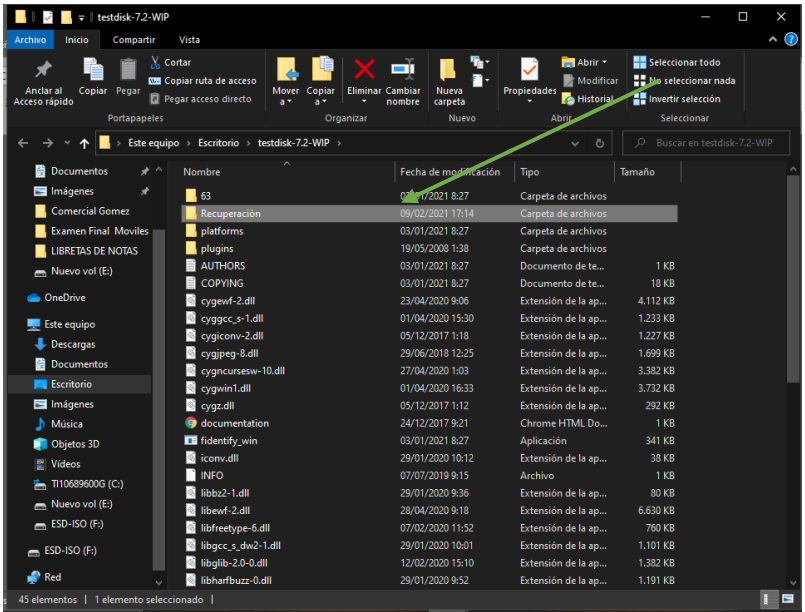
1.- Segunda herramienta para recuperar un archivo eliminado

Testdisk 7.2

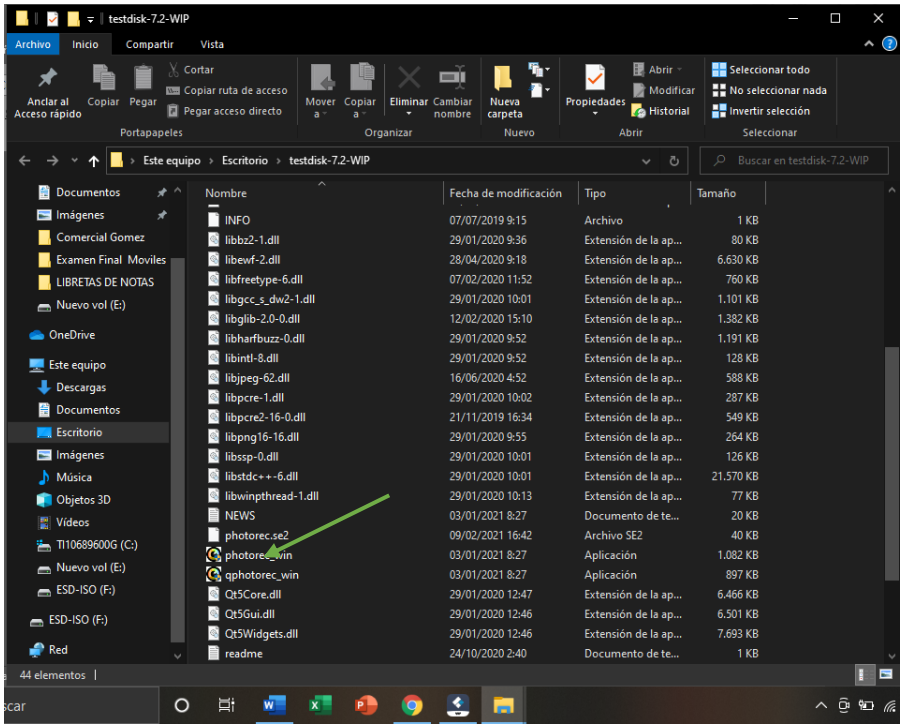
- Este es un archivo que se recupera mediante la consola



- Luego se crea una carpeta con un nombre cualquiera ya que ahí almacenara todos los archivos recuperados
- Para el ejemplo tomamos el nombre de **Recuperaciòn**

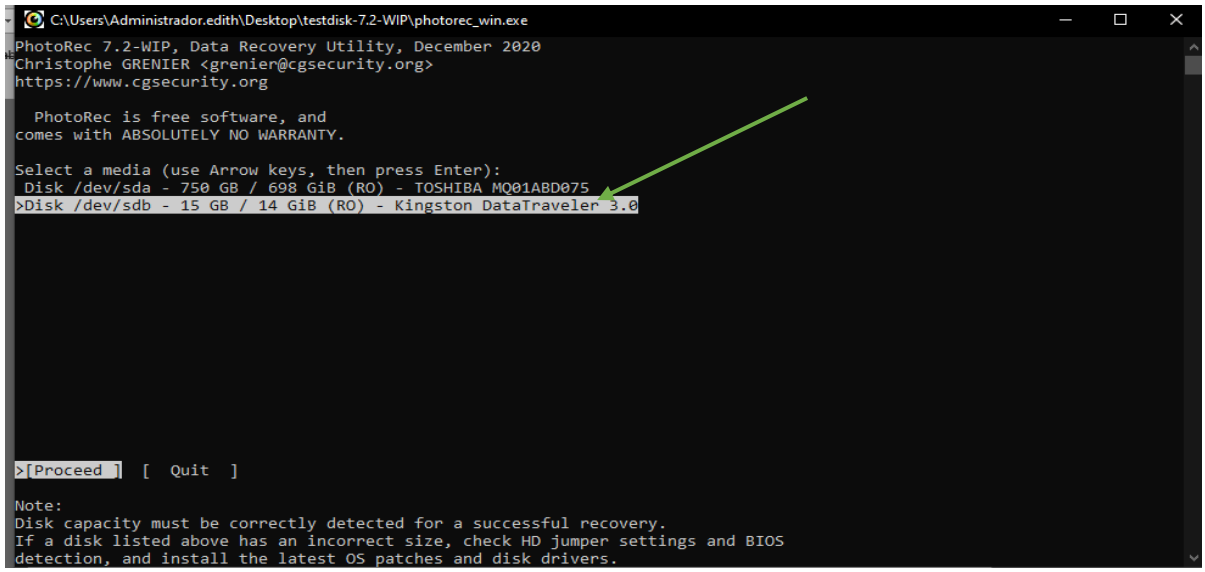


- Se usa la opción **photorec_win** y se instala como administrador

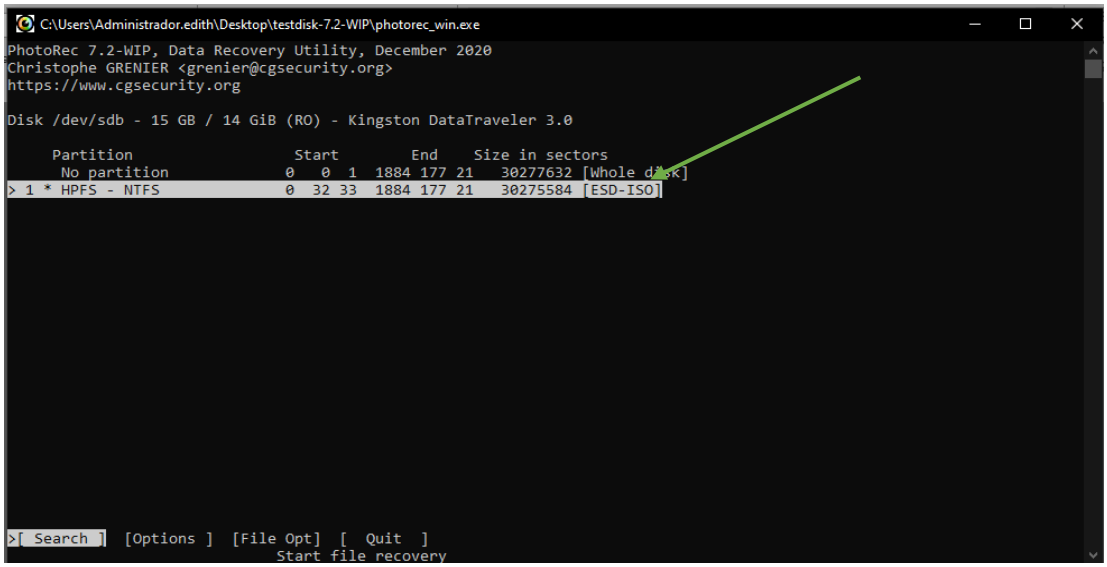


- Se abre la consola con instalas o abres el archivo **photorec_win**

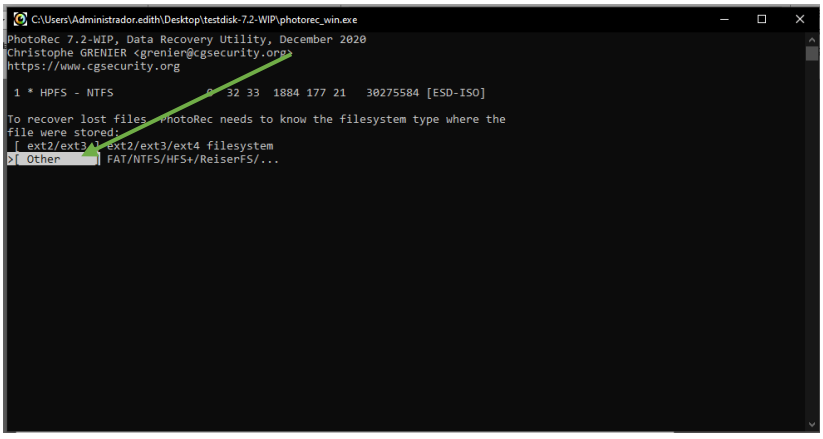
- Ahí muestra todos los discos que la pc reconoce y para el ejemplo usamos el disco USB
- Para la prueba escogemos el disco USB



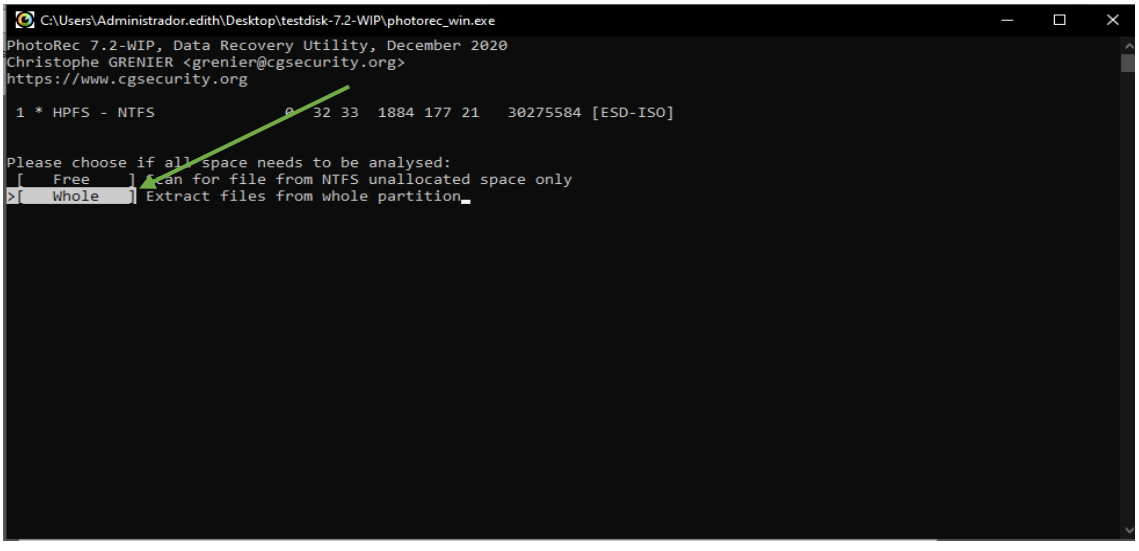
- Luego presionamos la tecla **INTRO**
- Se abre la siguiente ventana y seleccionamos la opción **HPFS - NTFS**



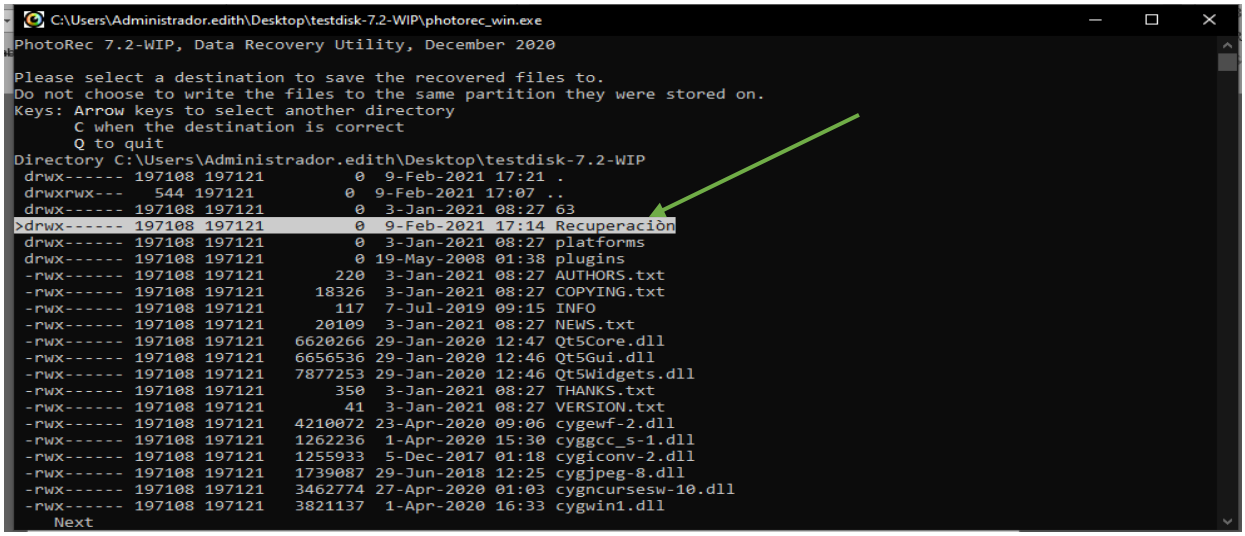
- Luego nuevamente presionamos el teclado **INTRO**
- Luego escogemos la opción **OTHER** y le damos con la tecla **INTRO**



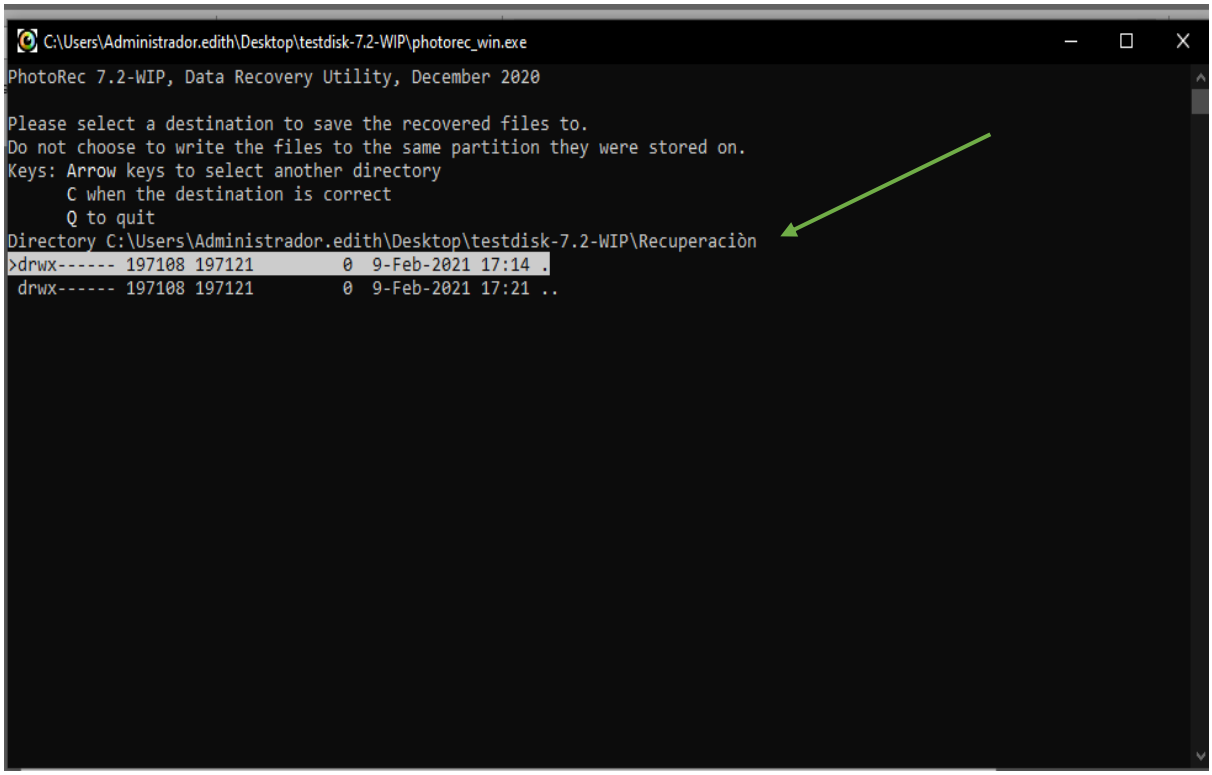
- A continuación escogemos la opción **WHOLE** ya que con esa opción es más rápido que con la opción **FREE**

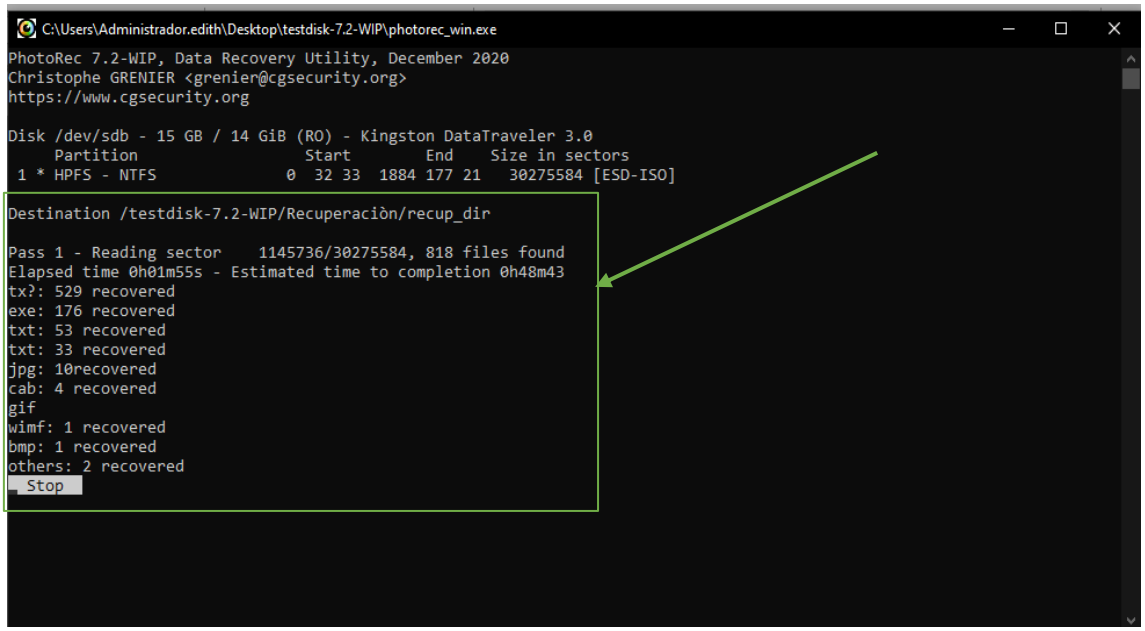


- Nuevamente le damos al teclado INTRO para ingresar a seleccionar la carpeta que creamos como ejemplo, ya que ahí es donde se va almacenar todo lo recuperado.
- Recordemos que para este ejemplo creamos una carpeta llamada **RECUPERACIÒN, seleccionamos** esa carpeta

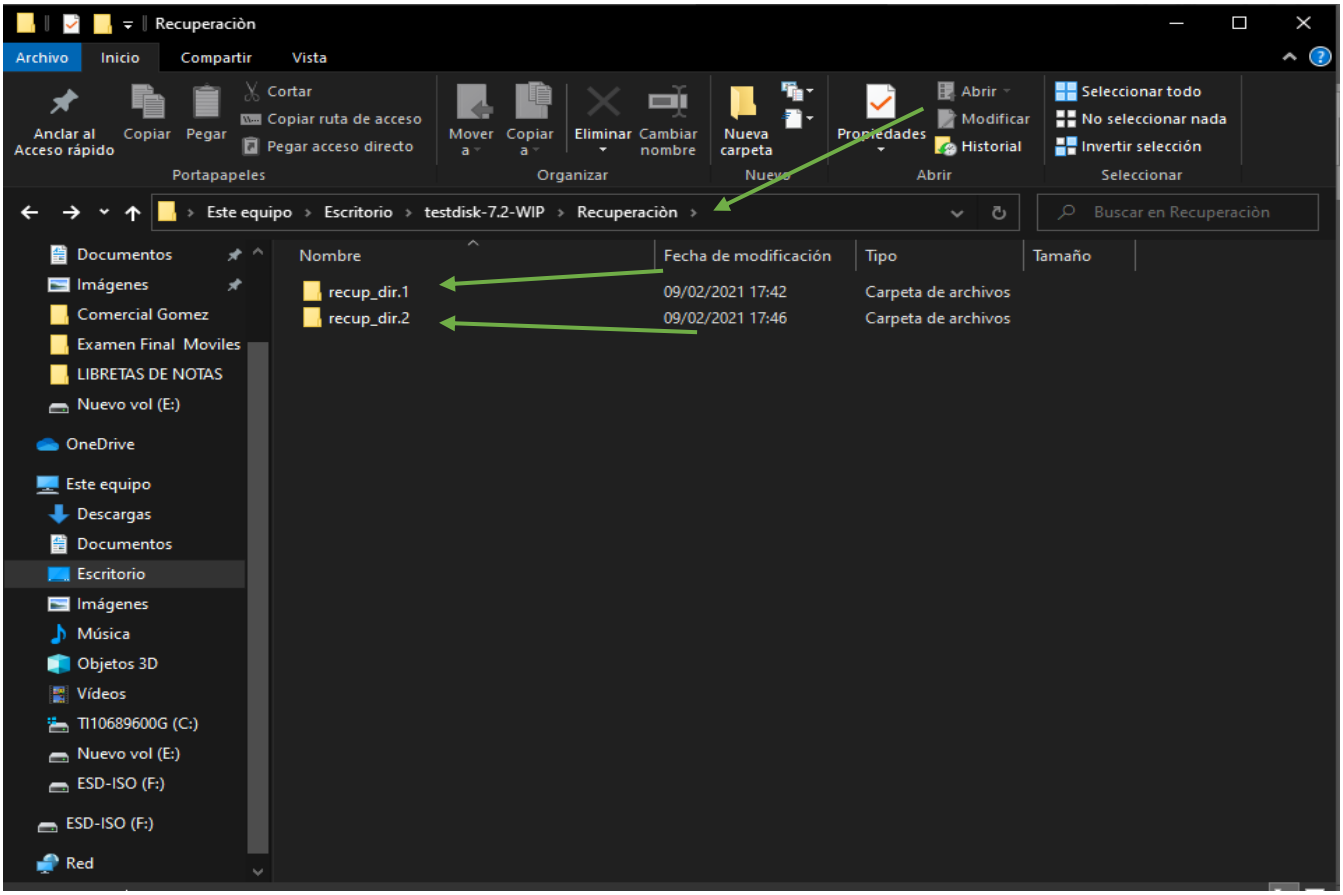


- Y luego le damos al teclado de **INTRO**
- Luego en la siguiente ventana digitamos la letra c mayúscula **“C”**





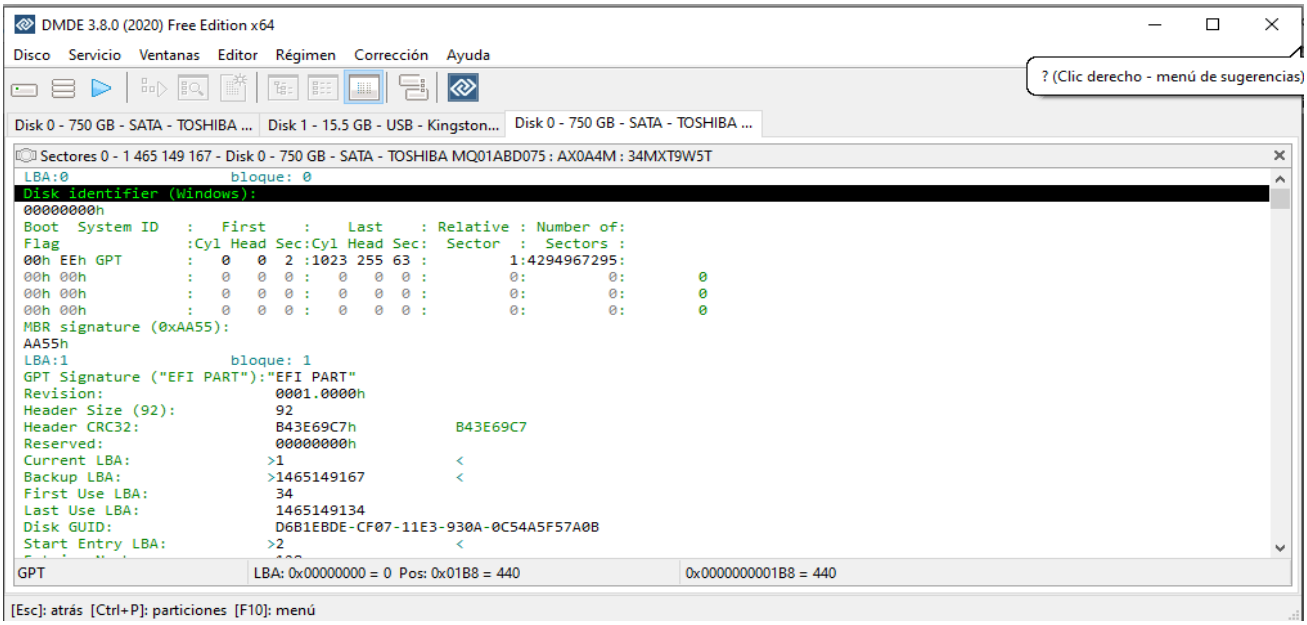
- Y por último nos dirigimos a donde está la carpeta de ejemplo que pusimos que es **recuperación**
- En este ejemplo podemos que si es la carpeta y que recupero 2 archivos



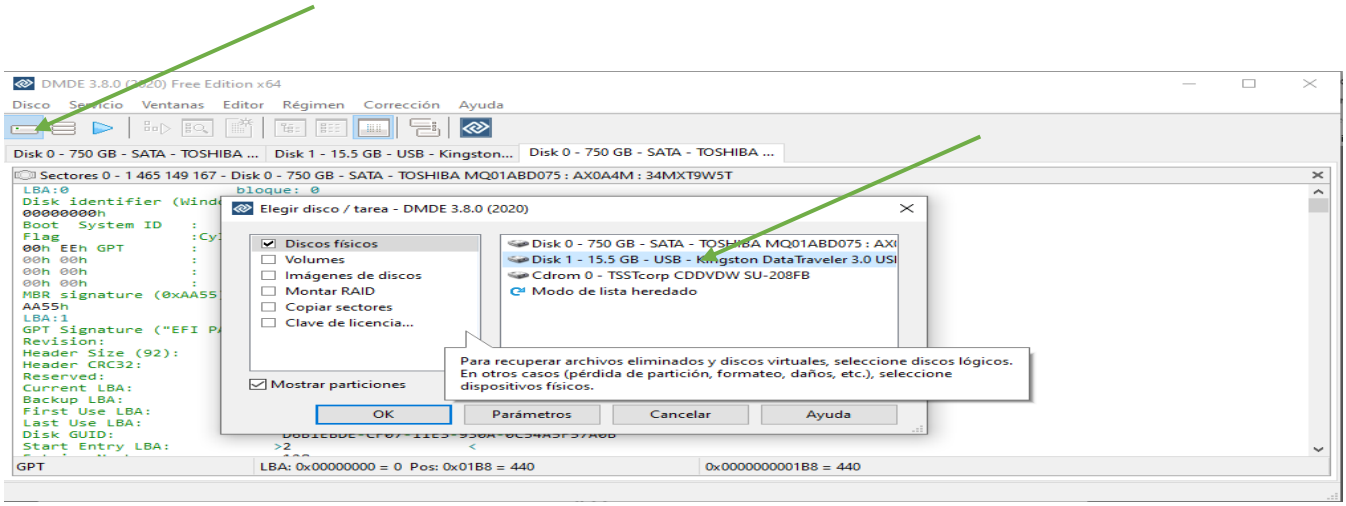
2.- Segunda herramienta para recuperar un archivo eliminado

Herramienta dmde

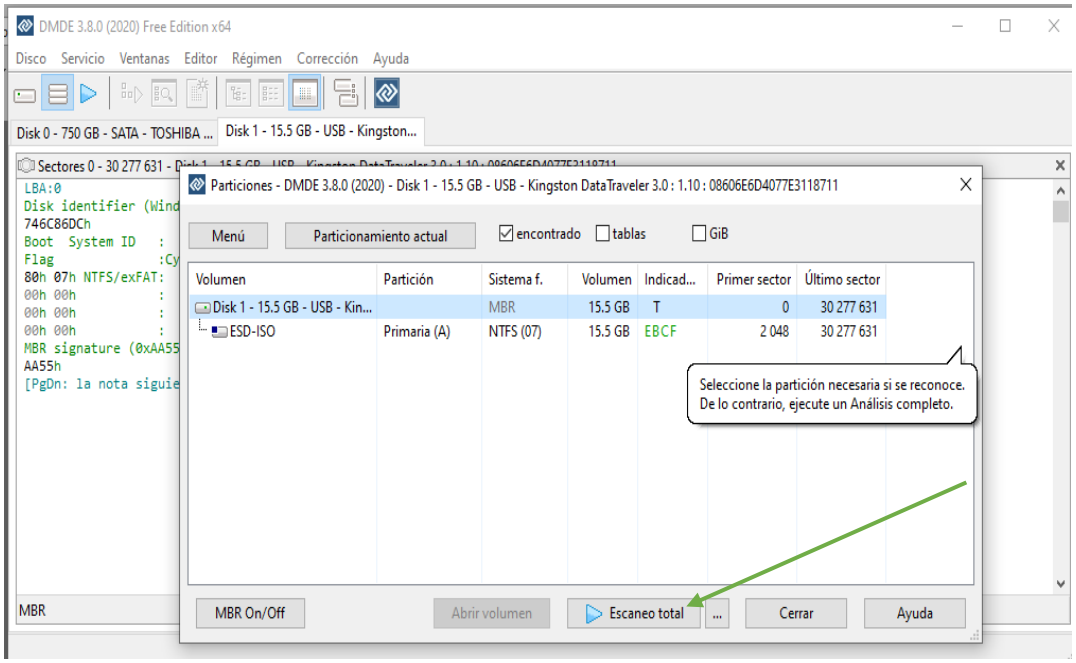
- Instalamos el aplicativo y cuando esté listo por defecto el sistema toma el disco duro de la PC



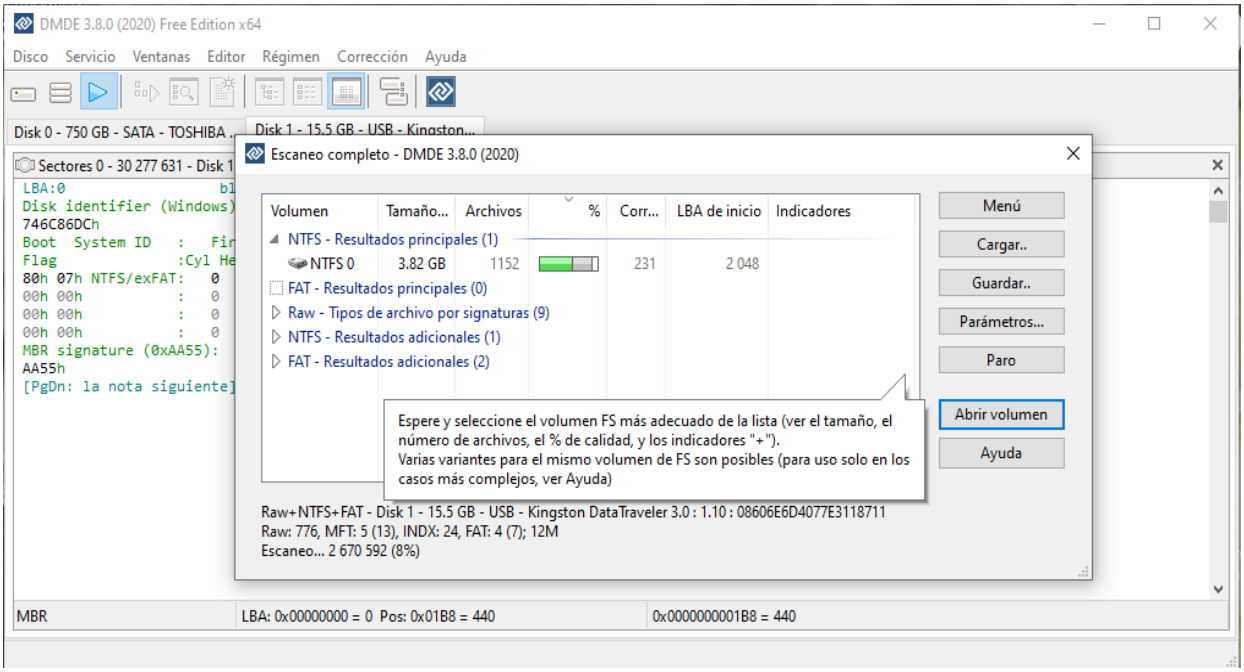
- Cambiamos al disco de ejemplo en este caso es un USB y para eso nos vamos al icono de un disco
- Hacemos click y se abre otra venta y ahí cambiamos el disco a trabajar y le damos a OK para cambie de disco



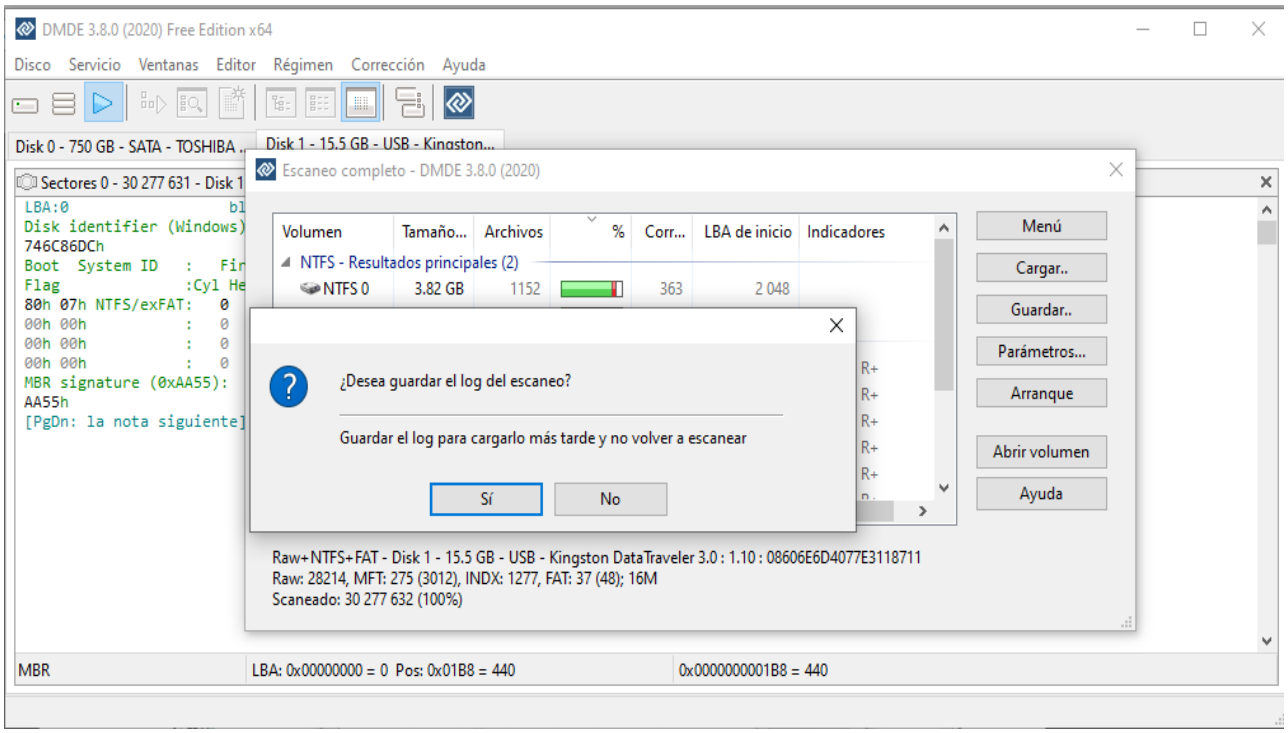
- El sistema escanea todos los archivos visibles y luego le das click en el botón ESCANEO TOTAL para que empiece a buscar todos los archivos eliminados y ocultos



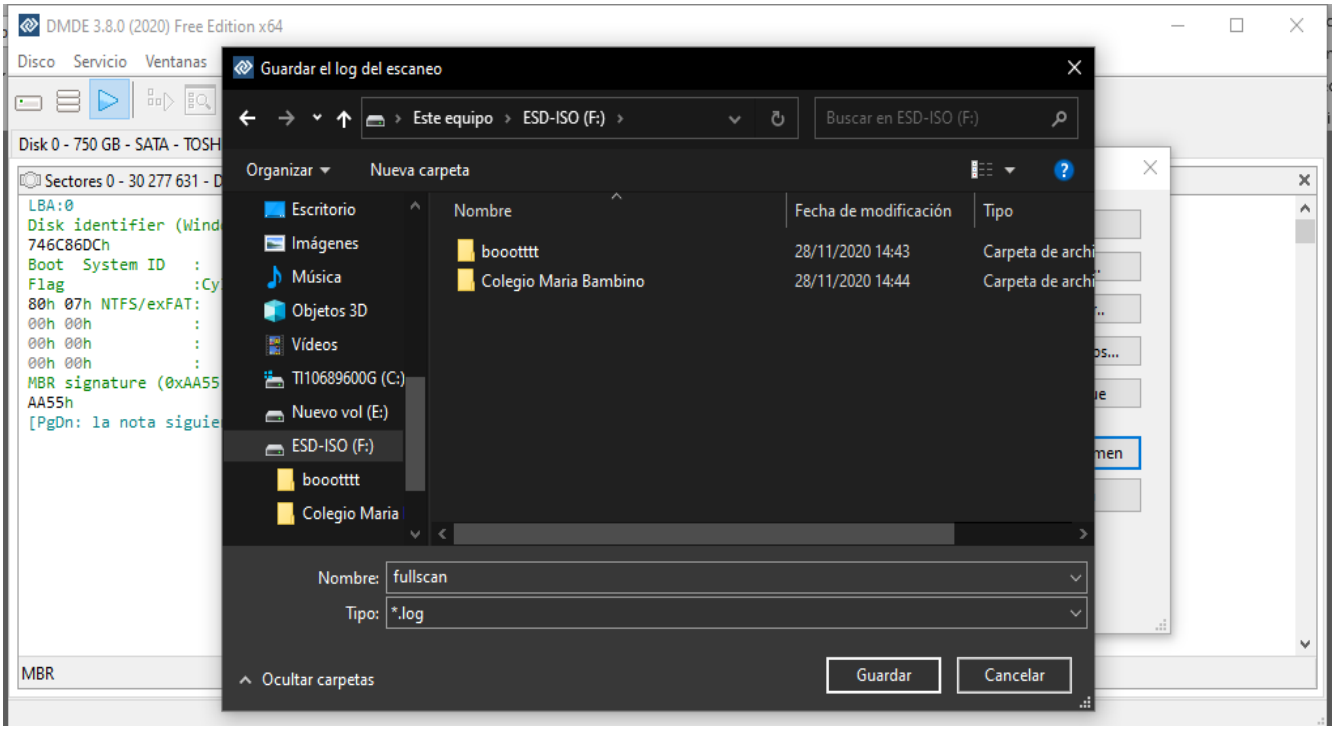
- A continuación empieza a escanear todo el disco USB



- Después cuando termine sale una ventana donde te da una opción a guardar todo lo recuperado y en ese caso le damos click a la al botón con la opción SI



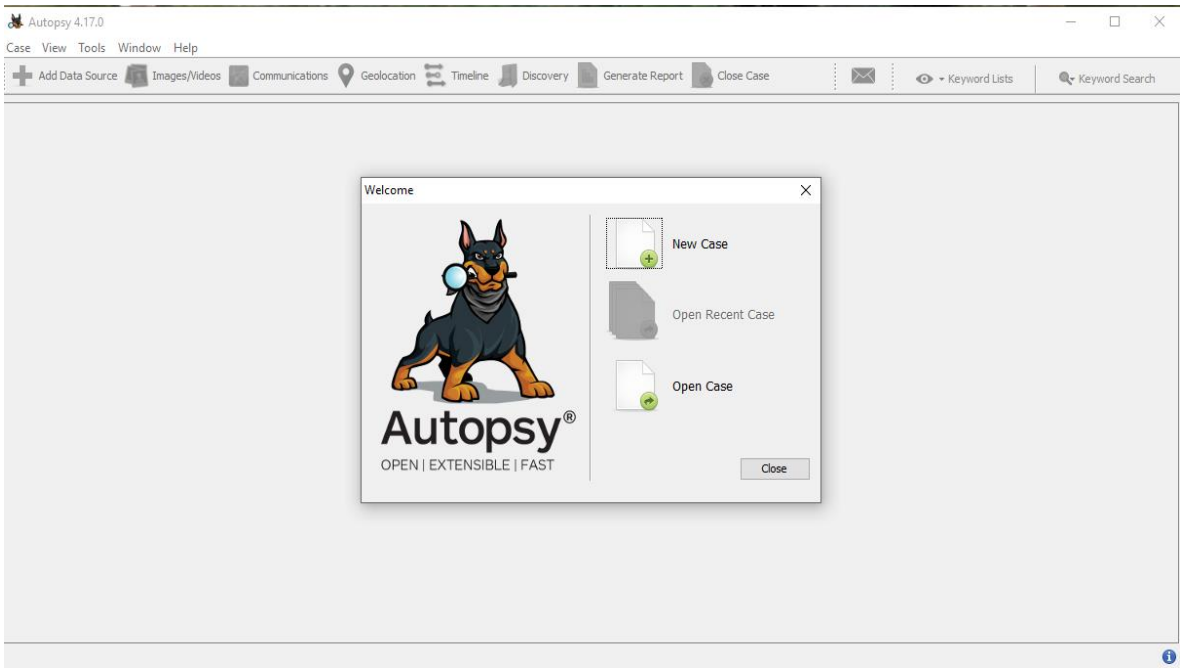
- Y se habre el explorador de archivos de windows donde podemos guardar los archivos en la carpeta que tenemos o escojamos en este caso lo guardamos en el mismo deico USB y ahí termina todo el proceso



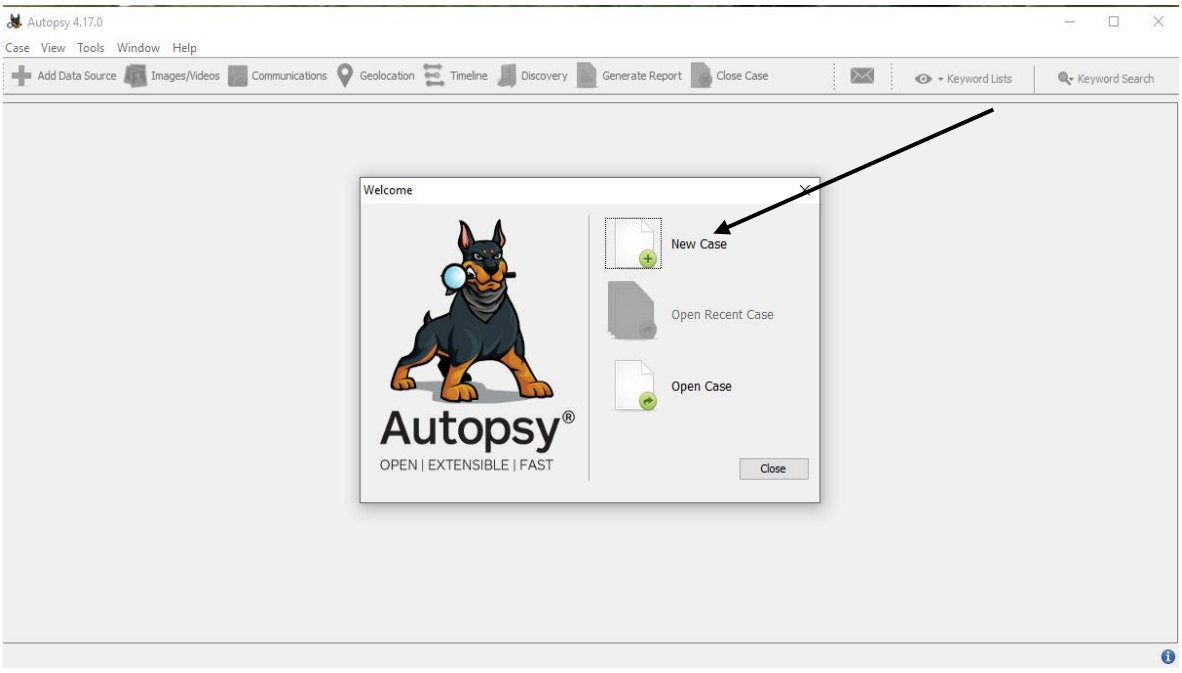
3.- Tercera herramienta para recuperar un archivo eliminado

Autopsy

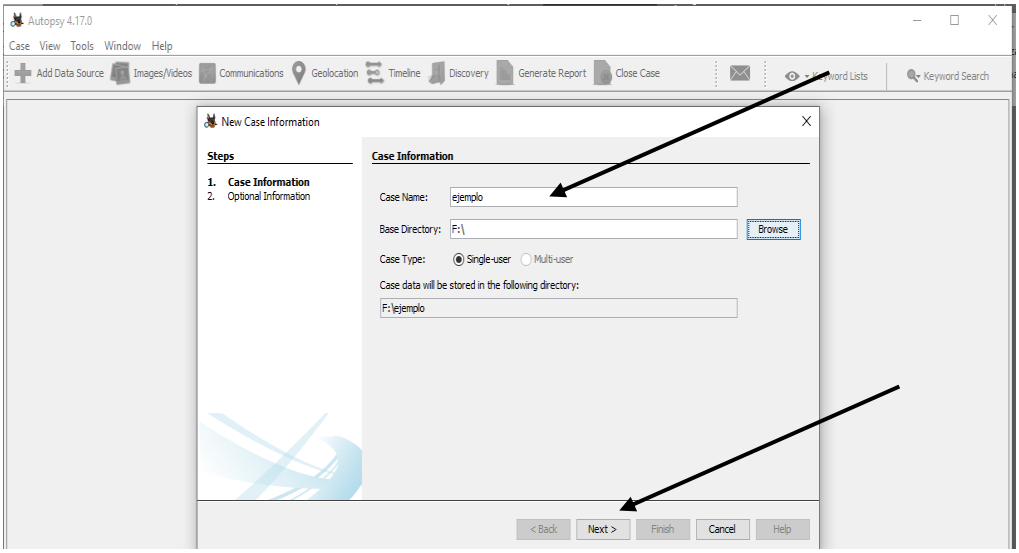
- ESTE sistema tiene 3 opciones al abrir el sistema y son:
- Nuevo caso
- Abrir caso reciente
- Abrir casos existentes



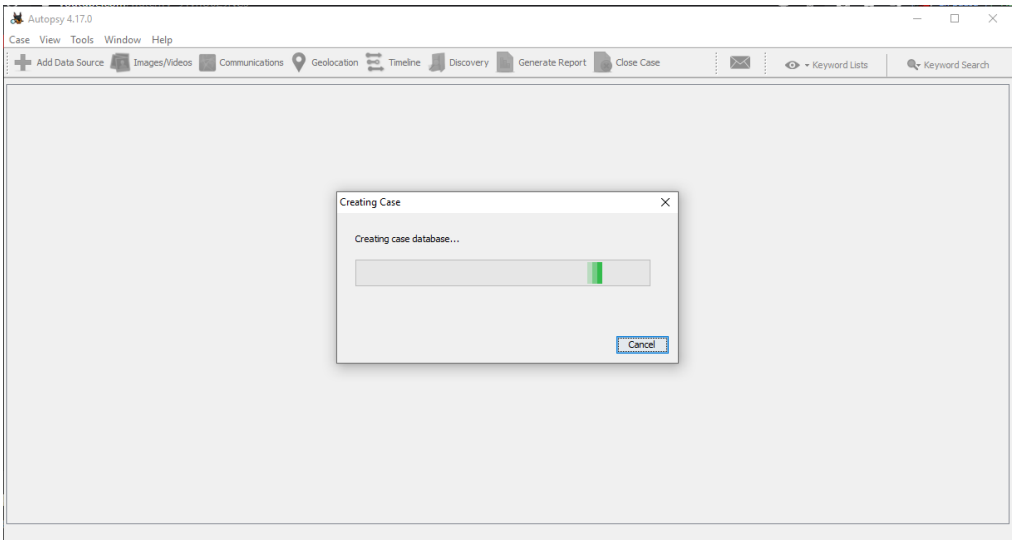
- Para el ejemplo vamos a tomar como ejemplo la primera opción y es NEW CASE



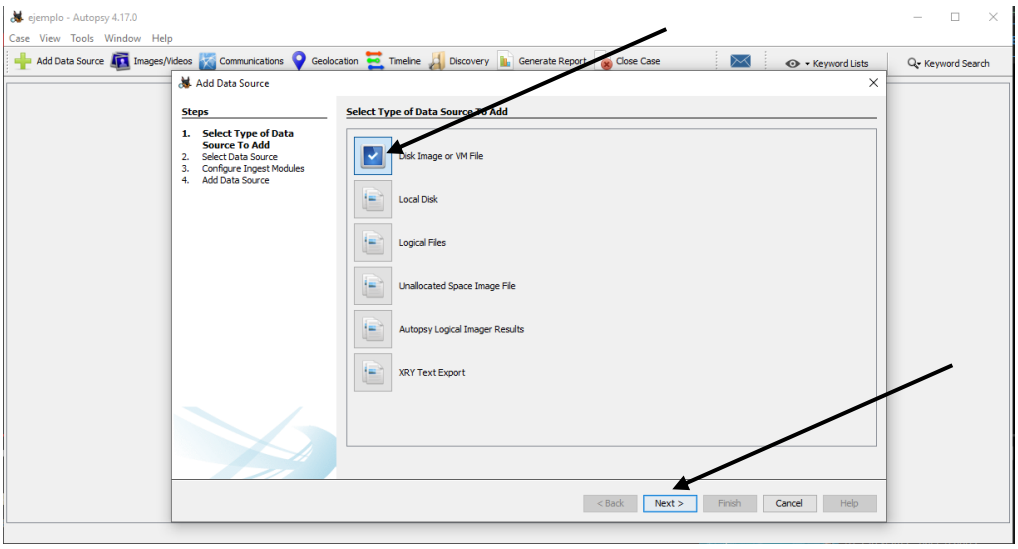
- Luego ingresamos un nombre y para este caso tomamos el nombre de EJEMPLO
- Luego le damos click al botón NEXT



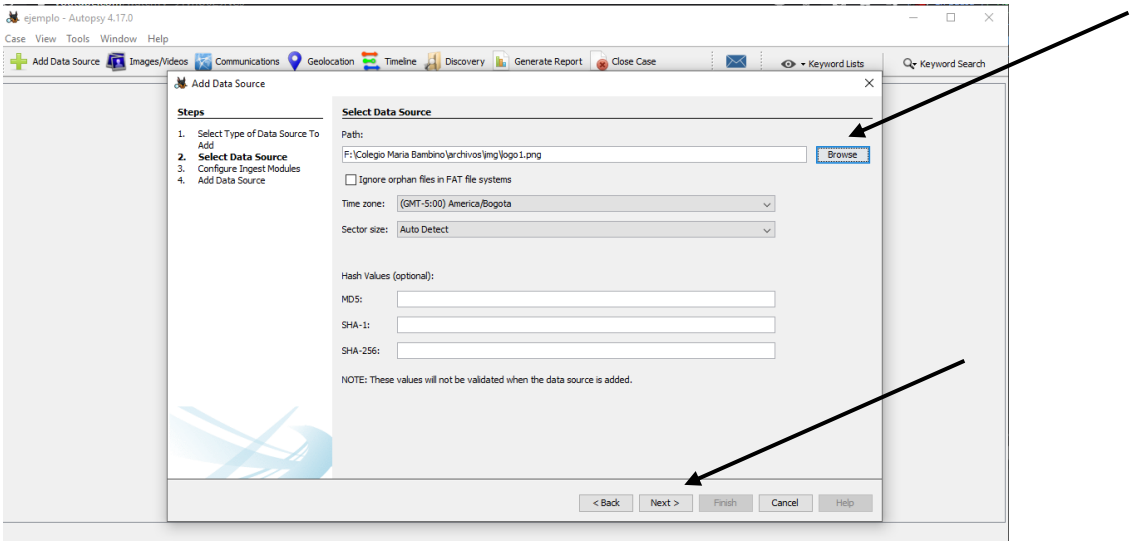
- El sistema empieza a cargar todos los datos ingresados



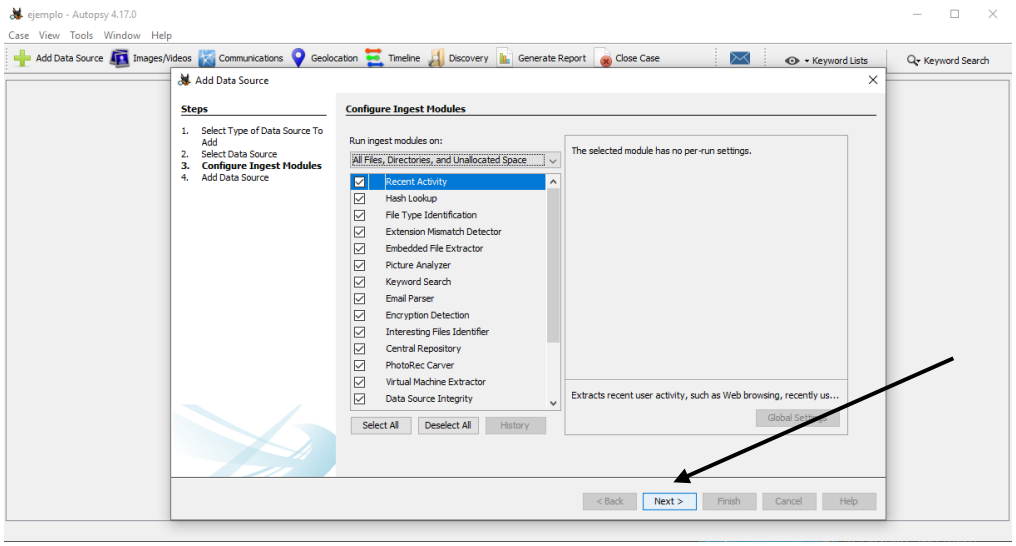
- En este caso vamos a darle en la opción de DISK IMAGE
- Luego en la opción NEXT



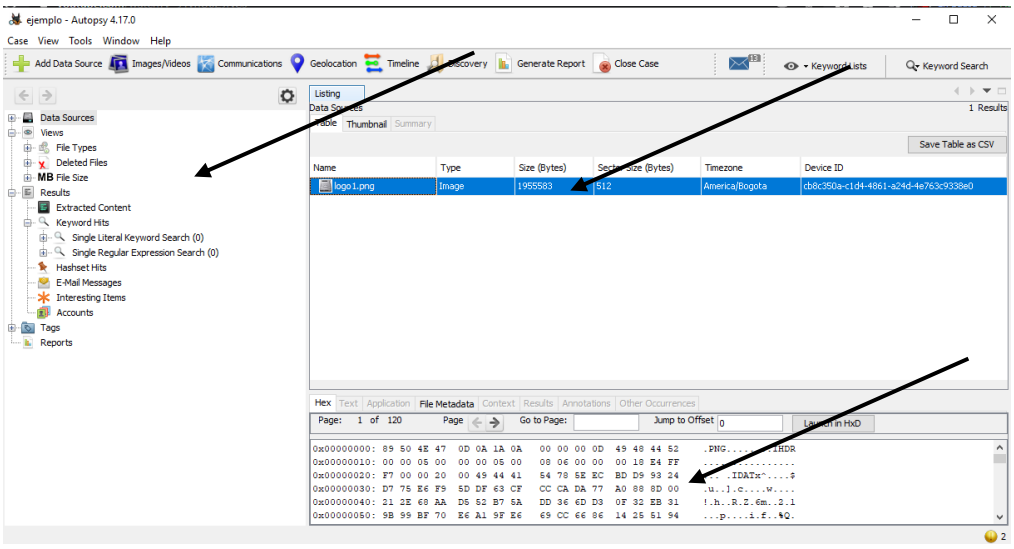
- Buscamos la opción BROWNS la carpeta donde esta ubicado el archivo a examinar en este caso tomamos el disco USB y cargamos la imagen
- Luego le damos en la opción NEXT



- Se cargan todas esas opciones por defecto y le damos NEXT



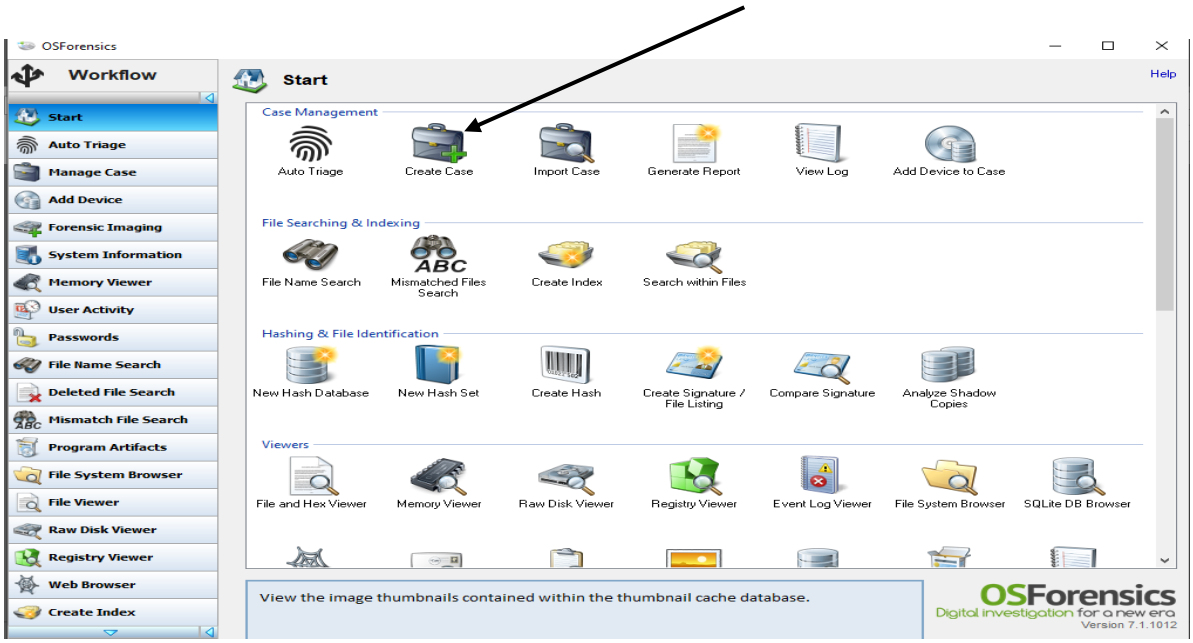
- LUEGO se cargan todo los archivos la imagen y al costado esta la barra de herramientas que se usaran paa saber l procedencia de esa imagen a examinar



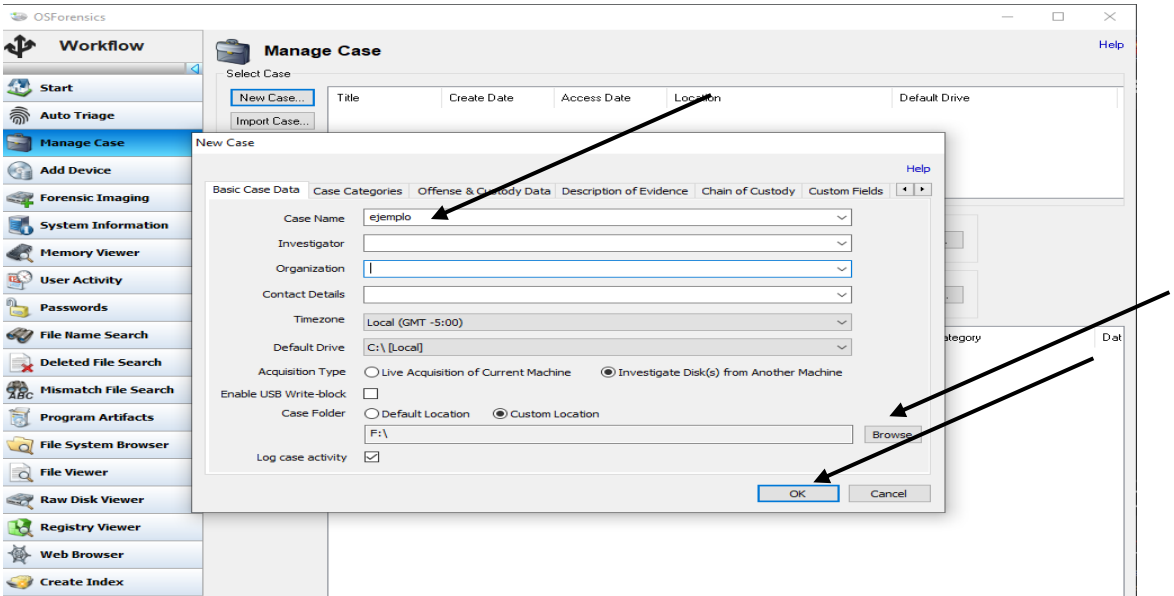
4.- Cuarta herramienta para recuperar un archivo eliminado

FORENSICS

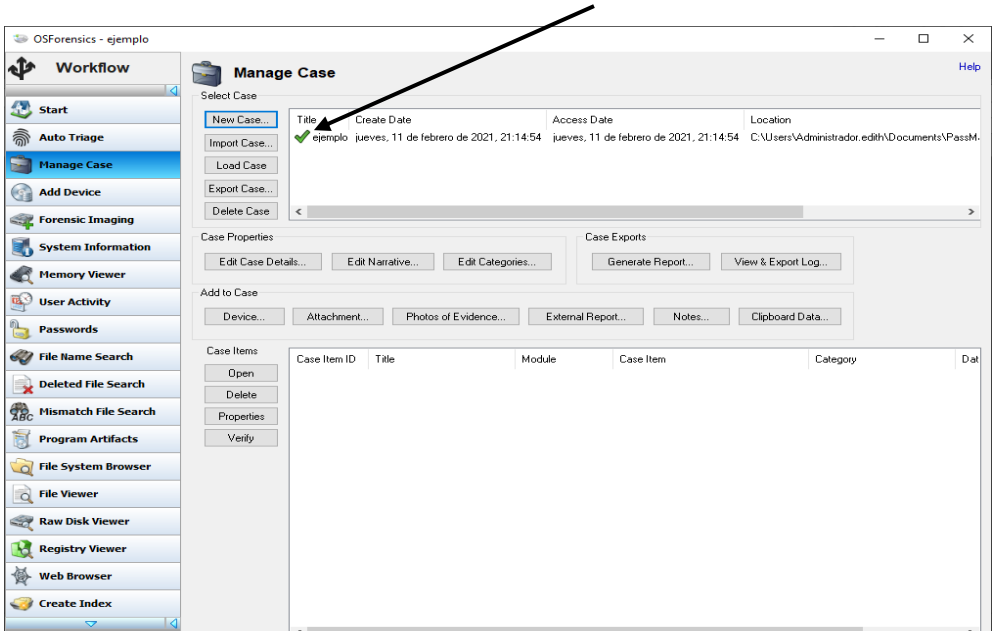
- El sistema al abrir muestra esta menu de opciones que nos permite tener una mayor experiencia al momento de interactuar con el usuario
- Para este ejemplo crearemos uno desde cero
- CREATE CASE



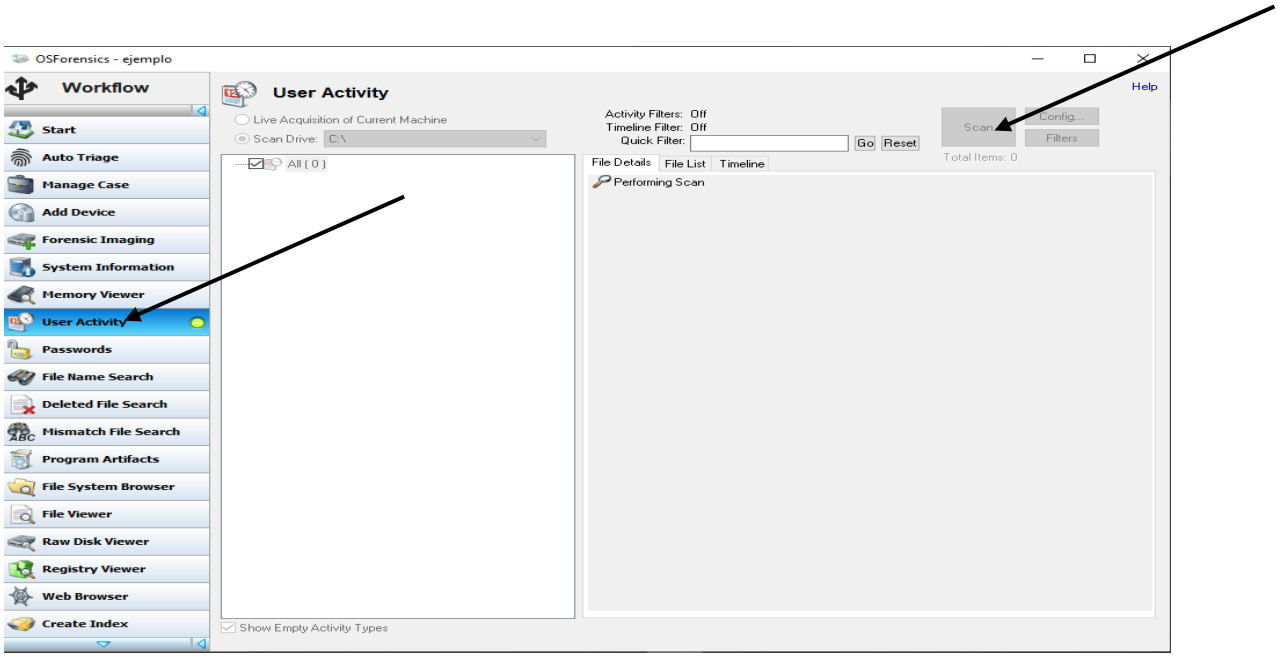
- Completamos la opción en este caso ponemos el nombre de EJEMPLO para nuestra primera prueba
- Los demás campos son opcionales
- Si queremos cambiar en que memoria guardar el archivo, se cambia en la opción BROWSE .en este caso lo cambiamos a la opción memoria USB
- Luego click en el botón OK

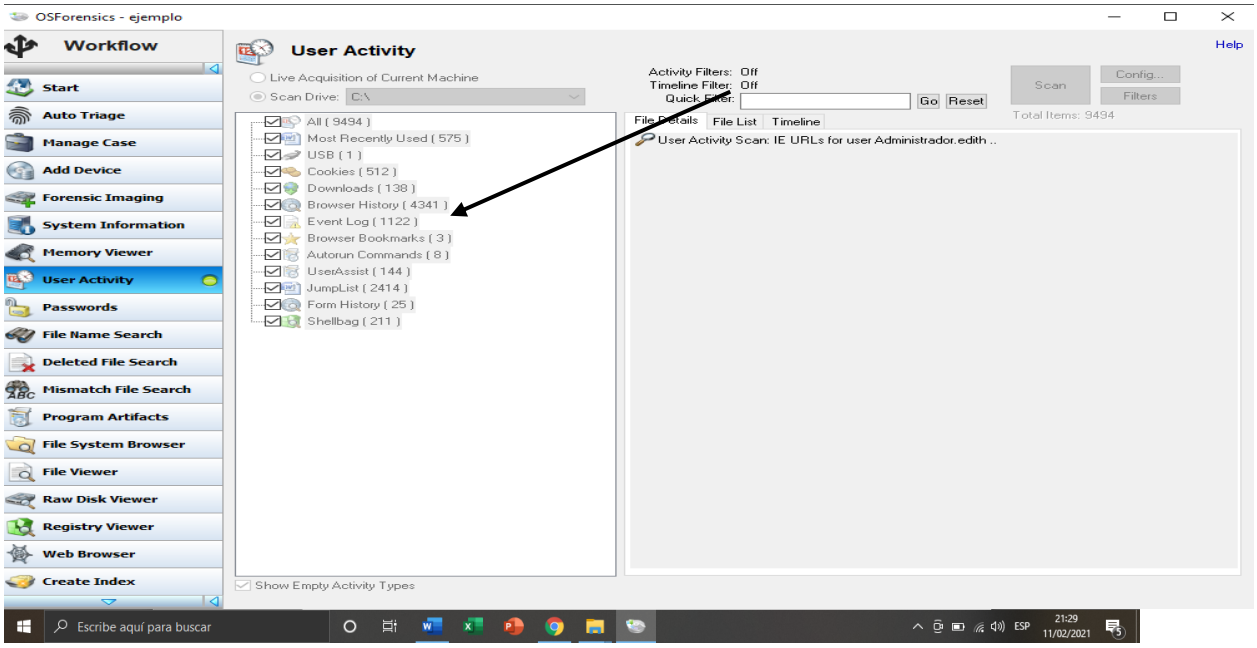


- Aquí ya nos señalan con la palomita de check de color verde ,eso nos dice que ya podemos hace el analisis de archivo

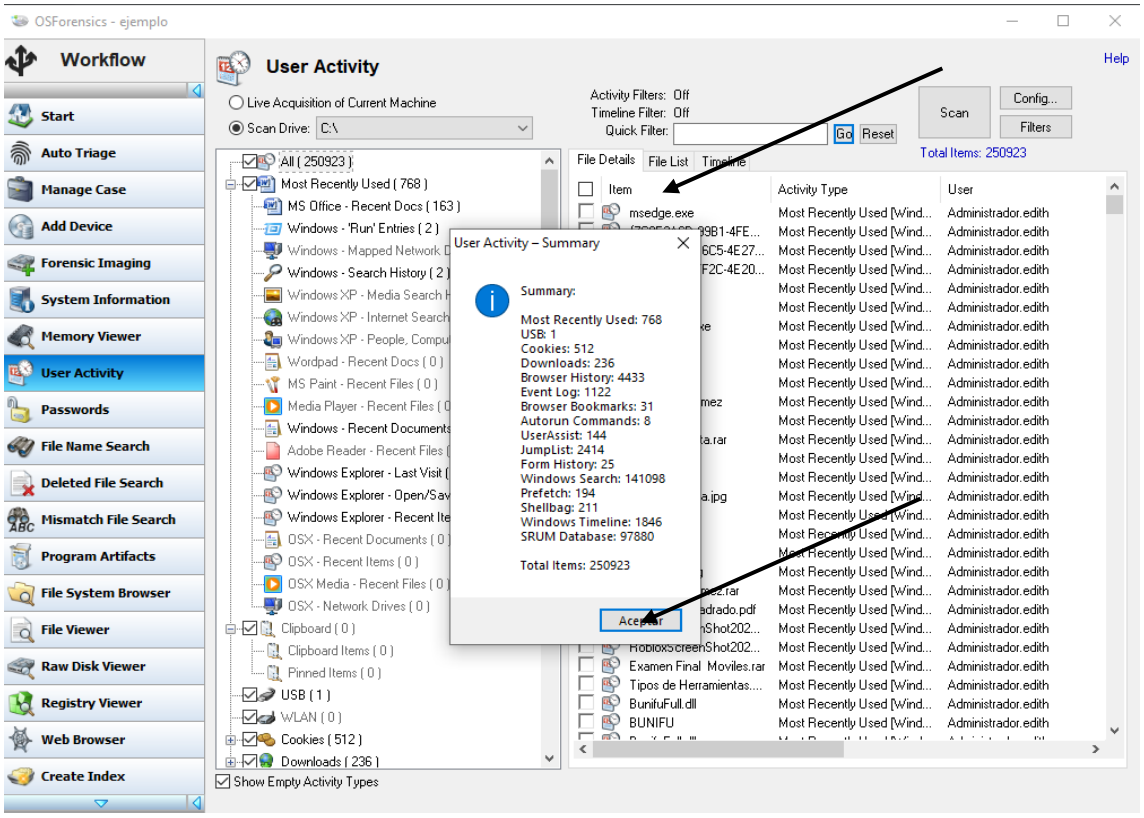


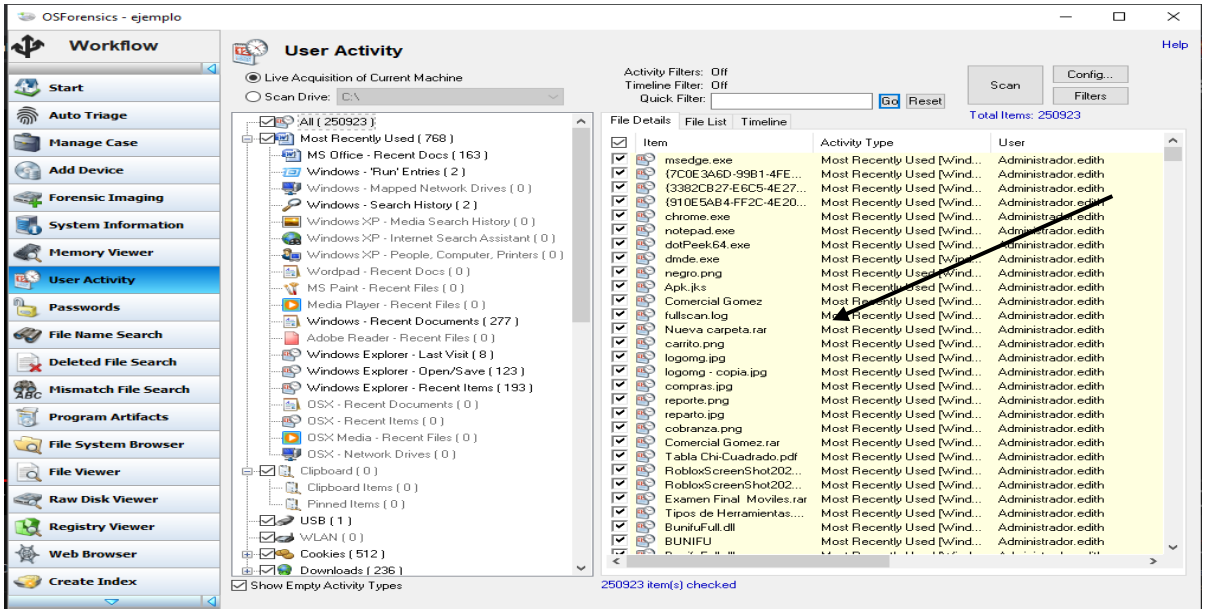
- Continuación nos vamos a la opción USER ACTIVITY
- Luego a la opción SCAN y así podrá escanear todos los archivos



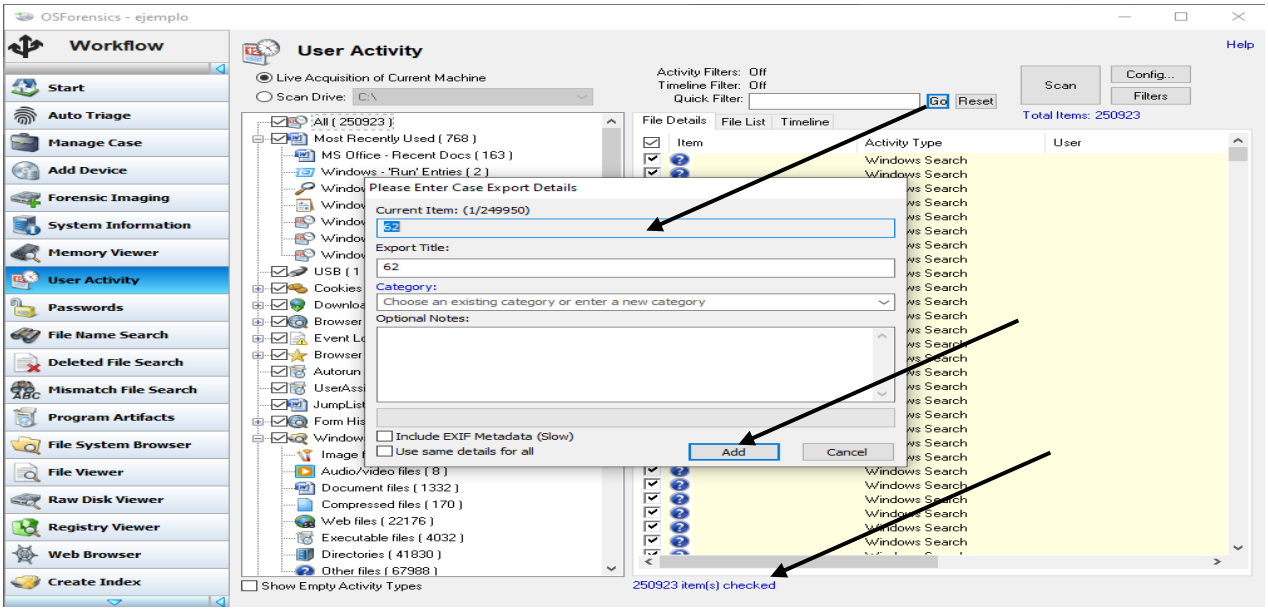


- Aceptamos la opción después de el escaneo
- Y en la opción ITEMS asemos click y seleccionamos todo

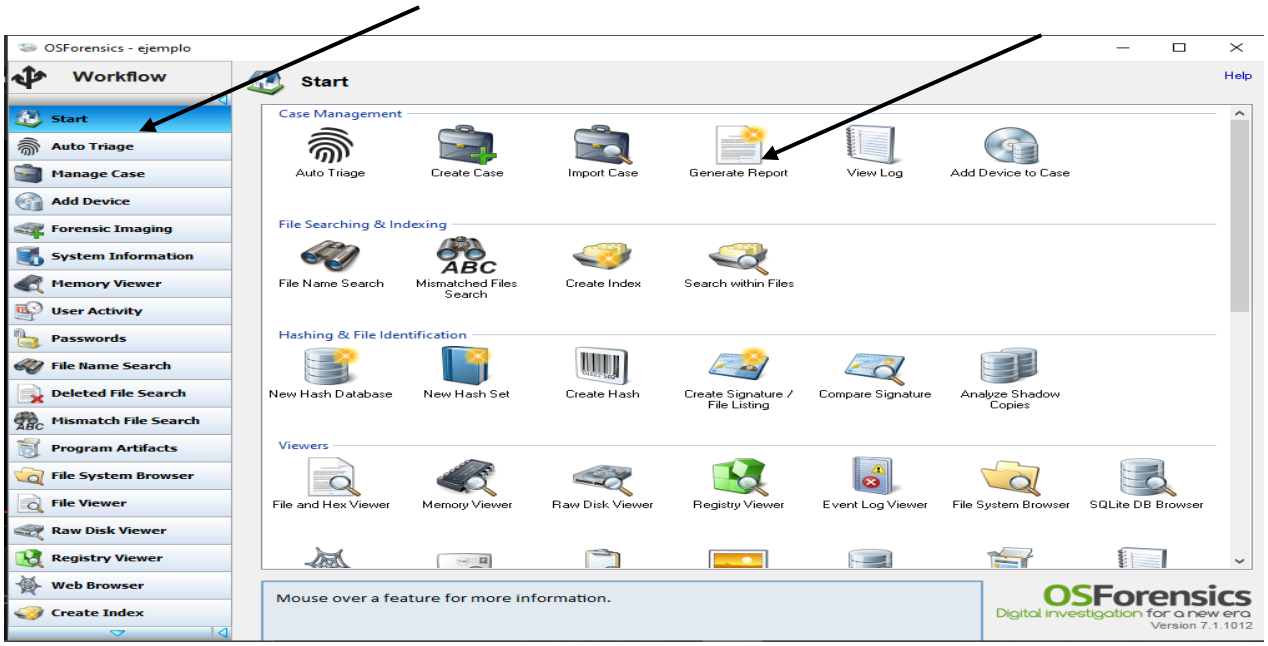




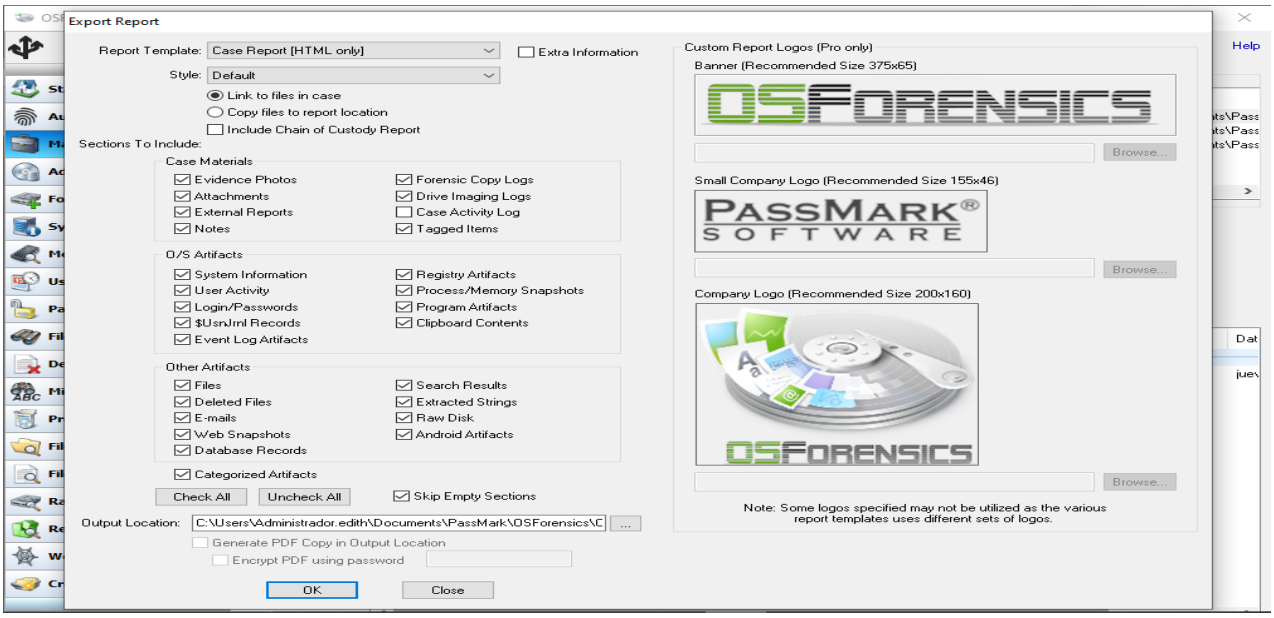
- Anticlick
- Nombre
- Y agregas ADD

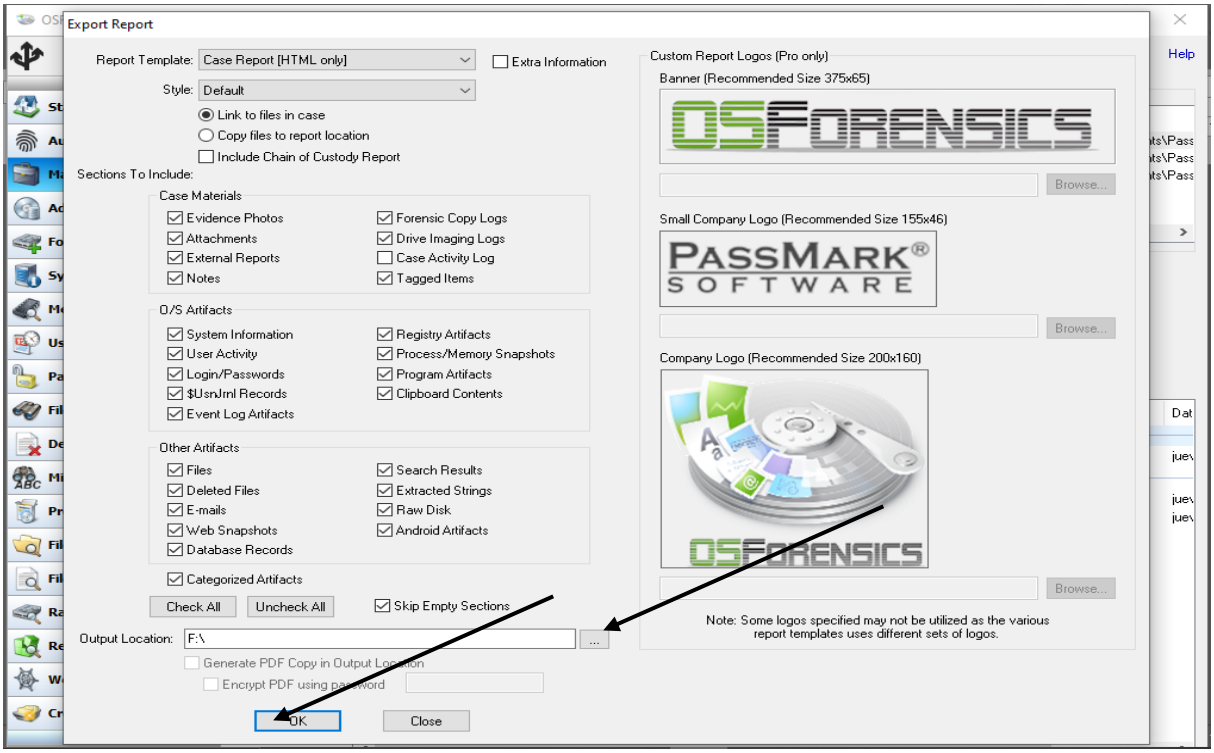


- Luego nos vamos a la opcion STAR y escogemos la opcion GENERAR REPORTE

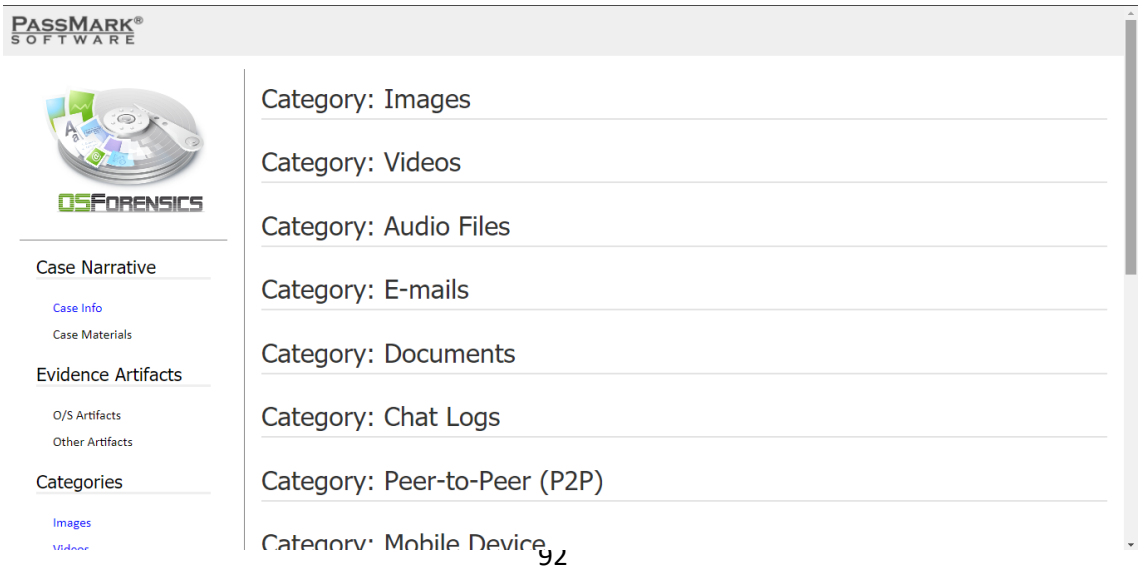


- Le cambiamos la direccion donde se guardara y en este caso lo cambiamos a la memorio USB
- Luego le damos en la opcion OK





- Automáticamente nos lleva al navegador con todas las opciones que cargamos n el ejemplo



- Luego revisamos en la memoria verificamos que se guardó la carpeta con el nombre de EJEMPLO donde se guardan todos los archivos guardados previamente