www.eysglobal.com

MÓDULO 3
PRÀCTICA 1:

Realización práctica del proceso de recopilación de evidencias y análisis de las mismas. Los asistentes se familiarizan con el proceso y con las herramientas más comúnmente utilizadas en el Análisis Informático Forense.

3.1 Recopilación de evidencias

- Metodología de trabajo
- Diferentes herramientas para clonado de discos duros y teléfonos móviles
- 3.2 Análisis de datos y reconstrucción de evidencias

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

Autopsy es un programa fácil de usar, basado en GUI que le permite analizar de manera eficiente discos duros y teléfonos inteligentes. Tiene una arquitectura de plug-in que le permite encontrar módulos complementarios o desarrollar módulos personalizados en Java o Python.

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

Algunas de las características de Autopsy

- **Casos multiusuario**: colabore con otros examinadores en casos grandes.
- **Análisis de línea de tiempo:** muestra los eventos del sistema en una interfaz gráfica para ayudar a identificar la actividad.
- **Búsqueda de palabras clave:** extracción de texto y los módulos de búsqueda de índice le permiten buscar archivos que mencionan términos específicos y encontrar patrones de expresiones regulares.
- **Artefactos web :**extrae la actividad web de los navegadores comunes para ayudar a identificar la actividad del usuario.

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

- **Análisis del registro:** utiliza RegRipper para identificar los documentos y dispositivos USB a los que se accedió recientemente.
- **Análisis de archivos LNK:** identifica accesos directos y documentos accedidos
- **Análisis de correo electrónico**: analiza mensajes en formato MBOX, como Thunderbird.
- **EXIF:** extrae la ubicación geográfica y la información de la cámara de archivos JPEG.
- **Clasificación de tipo de archivo**: agrupe los archivos por su tipo para encontrar todas las imágenes o documentos.
- **Análisis robusto del sistema de archivos:** Admite sistemas de archivos

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

- **Análisis robusto del sistema de archivos:** Admite sistemas de archivos comunes, incluidos NTFS, FAT12 / FAT16 / FAT32 / ExFAT, HFS +, ISO9660 (CD-ROM), Ext2 / Ext3 / Ext4, Yaffs2 y UFS de The Sleuth Kit.

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

Descarga, instalación y prueba con Autopsy

1. Nos dirigimos al enlace de descarga
https://www.sleuthkit.org/autopsy/download.php

Imagen : Captura descarga de autopsy

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

Se elige 32 -bit o 64-bit, dependiendo del sistema operativo que se tenga.

Imagen : Elección Sistema Operativo

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

2. Instalación de Autopsy

Buscar el archivo que se descargó y dar click para abrir el asistente de instalación. Click en Next.

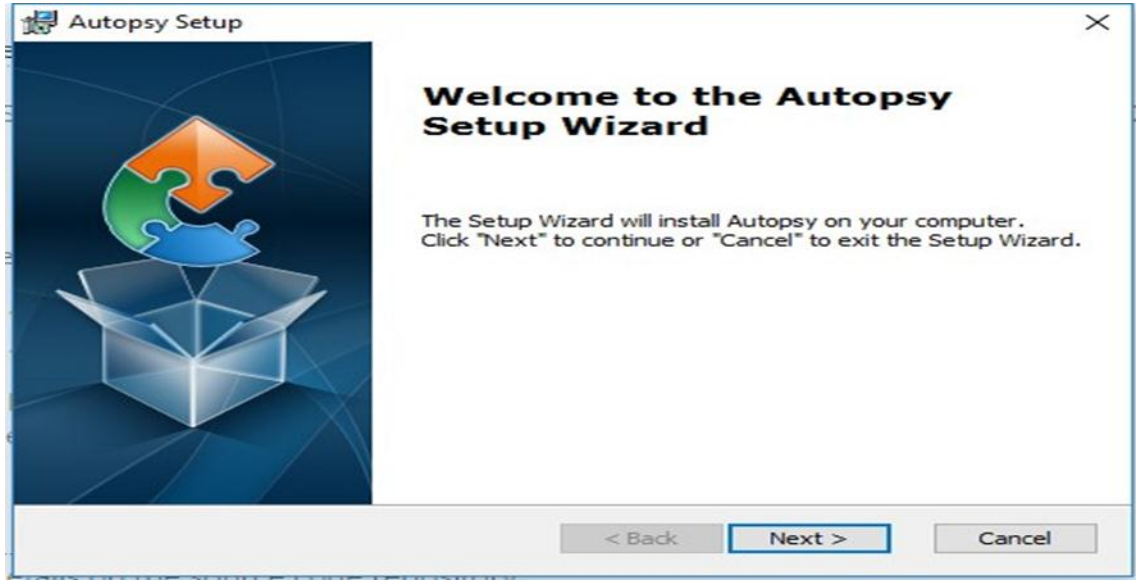

Imagen : Captura instalación autopsy

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

3 Se elige la ruta donde quedará instalado, click en next.

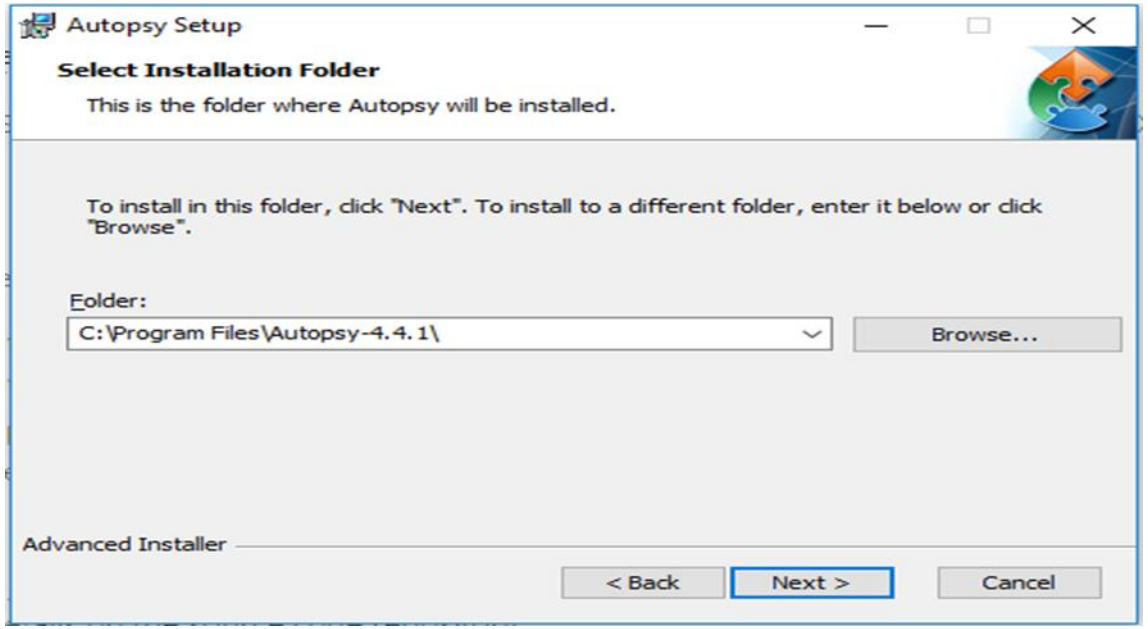

Imagen : Captura ruta instalación

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

4. Click en Install, para iniciar la instalación.

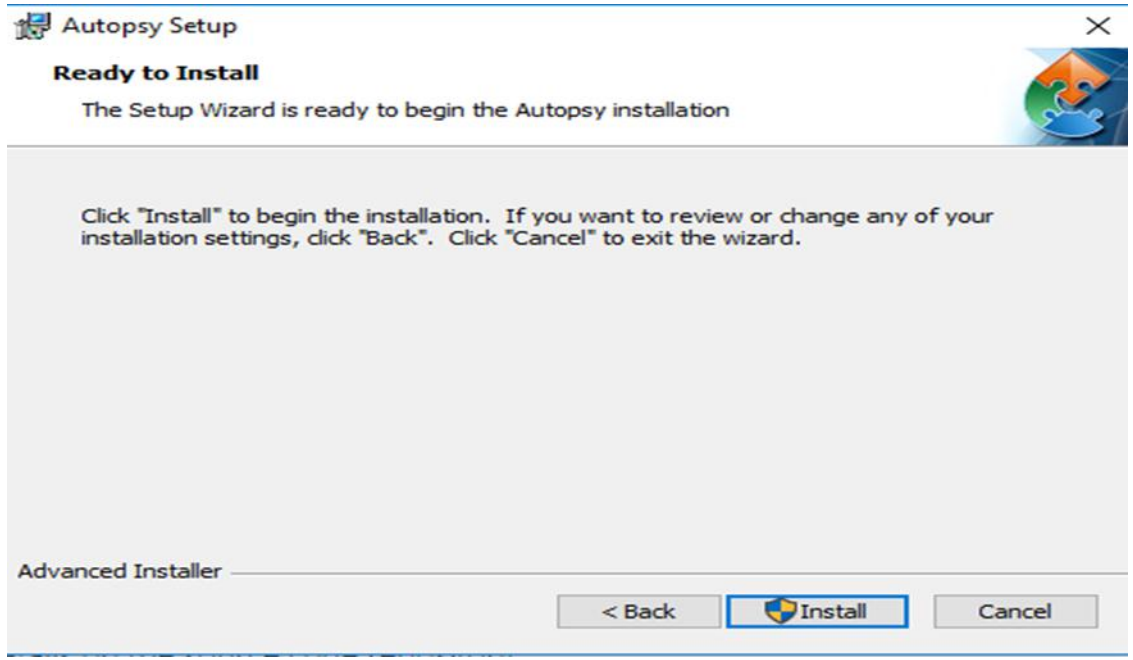

Imagen : Instalación

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

5. Se espera que termine el proceso de instalación.

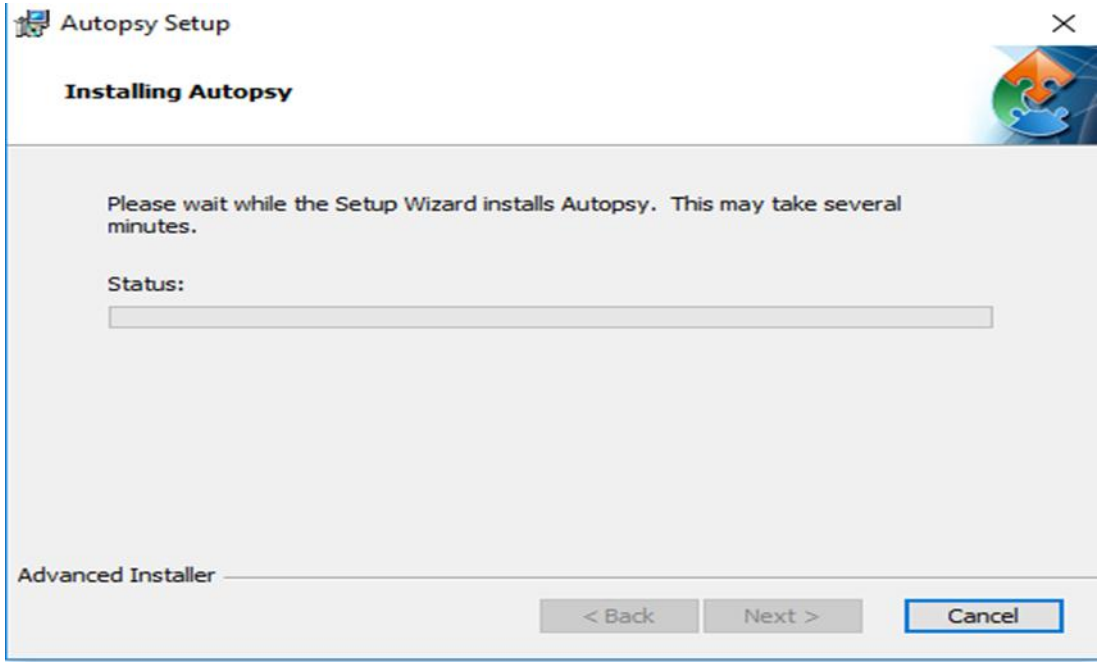

Imagen : Proceso de instalación

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

6. Click en finalizar

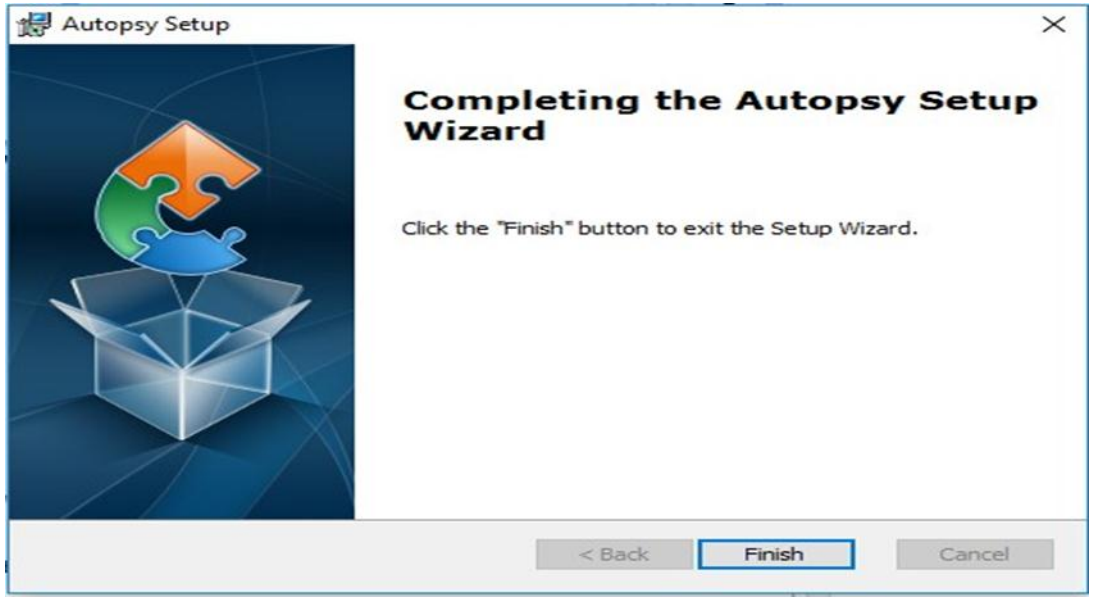

Imagen : Finalización de la instalación.

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

Prueba de Autopsy

Autopsy crea una imagen del disco que se va a analizar con toda la información que este contiene, con el fin de analizarla y así no alterar la información que se encuentra en el disco original, esta herramienta es muy útil para realizar análisis forense en casos judiciales o a empleados que estén afectando una empresa ya que con esta se puede realizar el análisis sin alterar la evidencia original

Para la prueba se va a utilizar un disco duro con sistema operativo Windows 7, extraído de un computador portátil HP.

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

Disco Duro

Imagen : Disco Duro para pruebas

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

1.Se abre el programa y se le da la opción “Create New Case” (Crear un caso nuevo) o si ya tiene un caso abierto se le da en “Open existing Case” (caso existente).

Imagen : Captura creación caso autopsy

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

2.Se coloca el nombre del caso o procedimiento que se va a realizar, la ruta donde se va a guardar la imagen y click en “Next”.

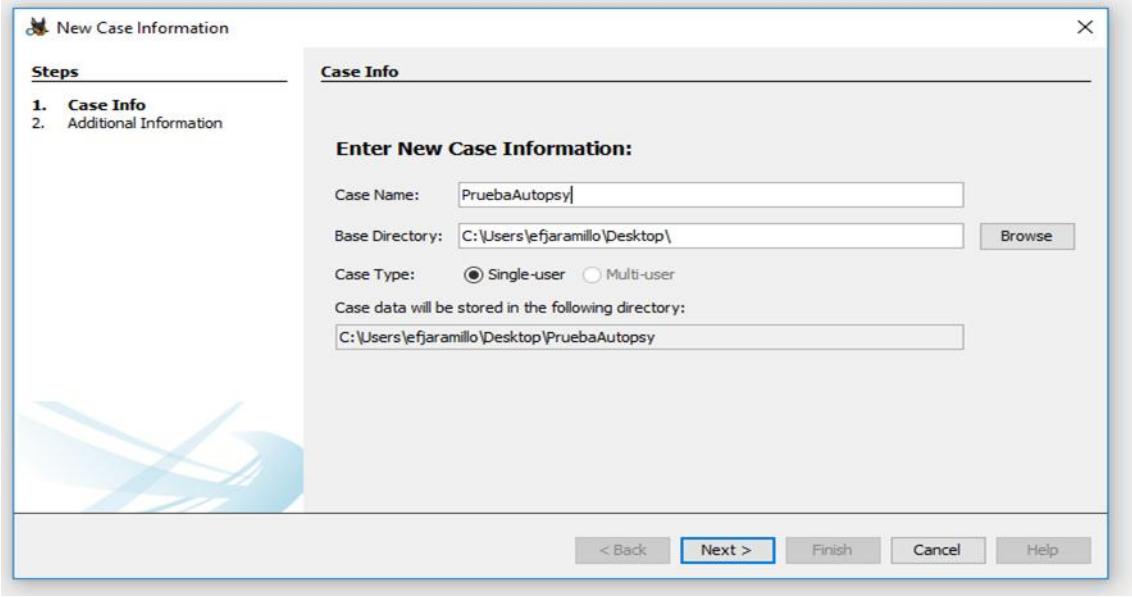

Imagen : Captura Ruta del caso autopsy

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

3.Se coloca el número del caso y quien lo está realizando y click en “finish”.

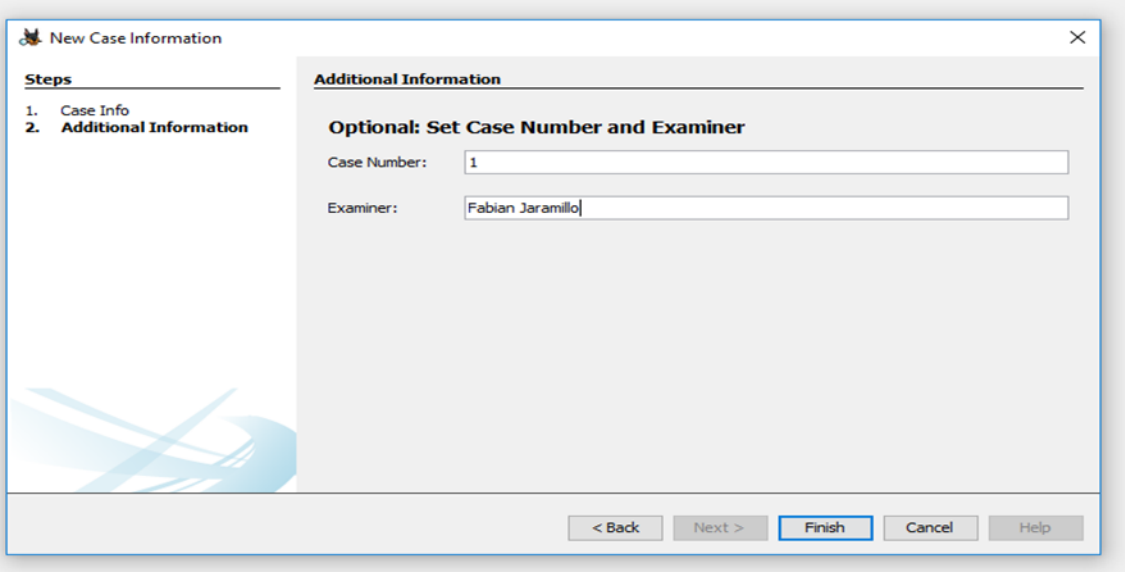

Imagen: Captura número de caso autopsy.

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

4.Comienza la creación del caso.

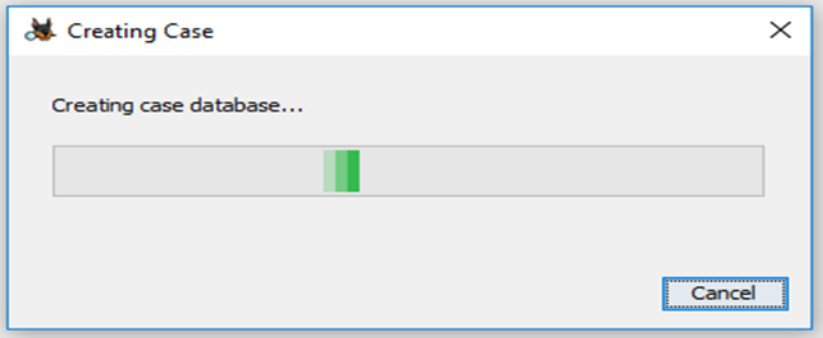

Imagen : Captura creación base datos del caso

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

5. En esta parte se va a elegir la fuente de donde se va a sacar la imagen la cual va a ser analizada, tiene 4 opciones.

- Disco de máquinas virtuales
- Disco Local
- Archivos Lógicos
- Archivo de imagen de espacio sin asignar.

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

En este caso se va a utilizar un disco físico, por tanto, seleccionamos la segunda opción “Local Disk” y click en “Next”.

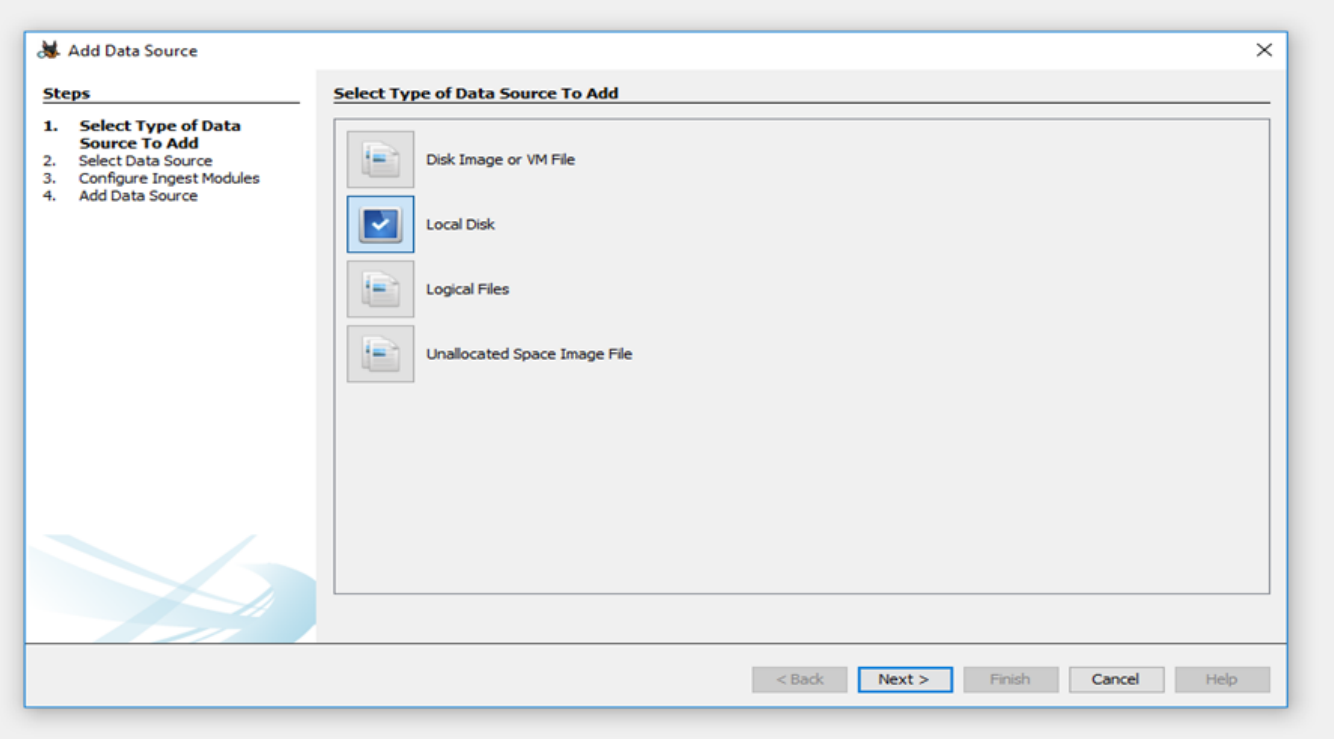

Imagen : Captura opciones del caso

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

6.Seleccionamos la unidad a la cual se le va a sacar la imagen, en este caso es la unidad Disco Local (I:), y click en “Next”.

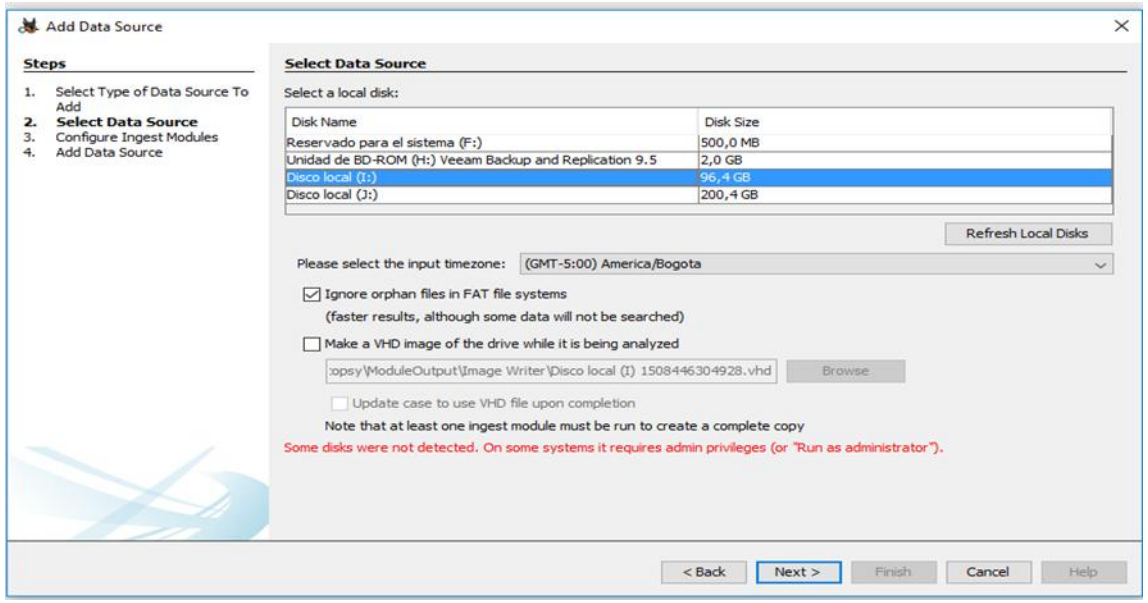

Imagen : **Captura de lo que va a escanear el programa**

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

7.La siguiente ventana muestra la configuración de los módulos que van a ser analizados en la imagen, se seleccionan los necesarios y click en “Next”.

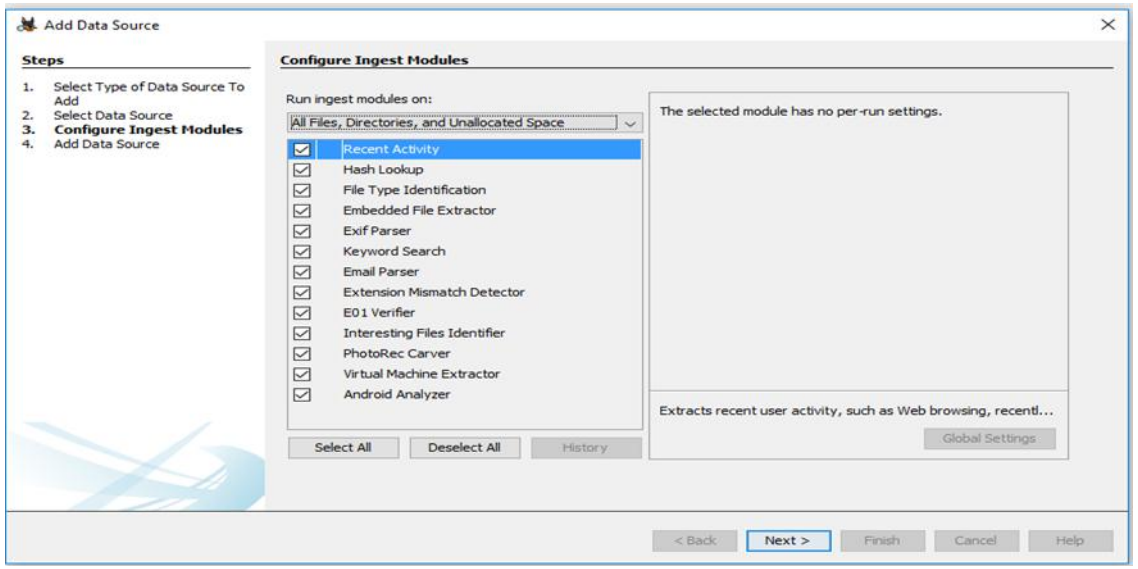

Imagen : Captura de lo que va a escanear el programa

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

8. Comienza el proceso de creación de la imagen a analizar, el disco original se entrega para su custodia, así no sufrirá ninguna alteración.

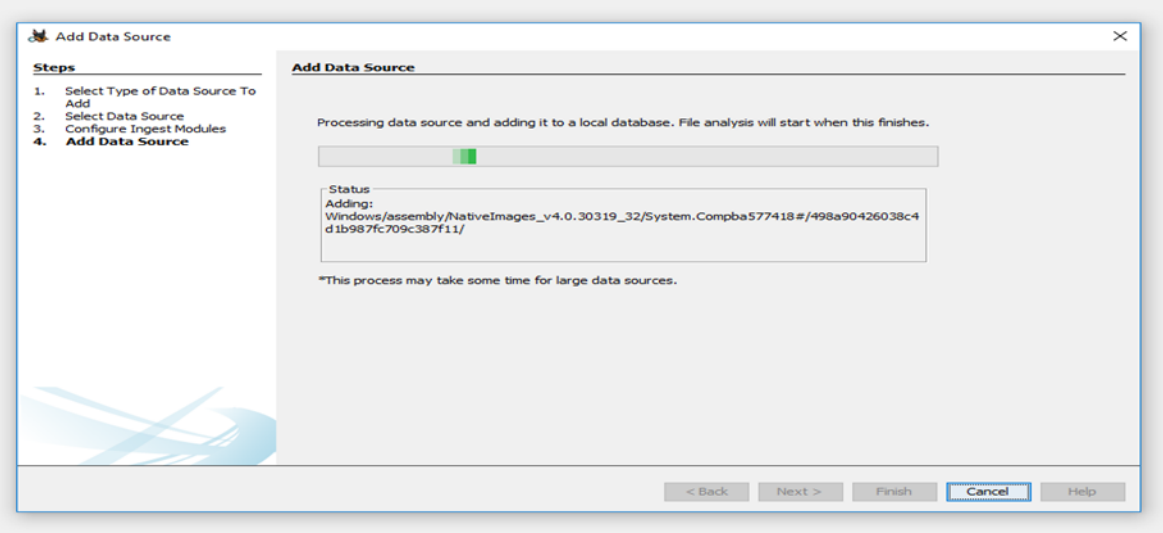

Imagen : Captura del proceso de creación de disco virtual

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

9. Termina la creación del disco, clic en “Finish”.

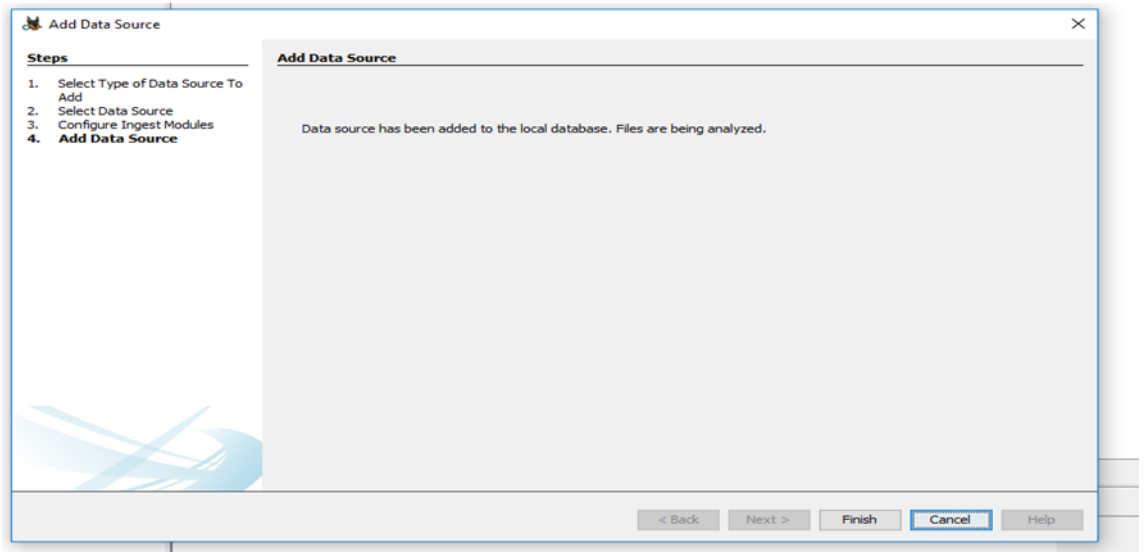

Imagen : Captura finalización de la creación del disco virtual

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

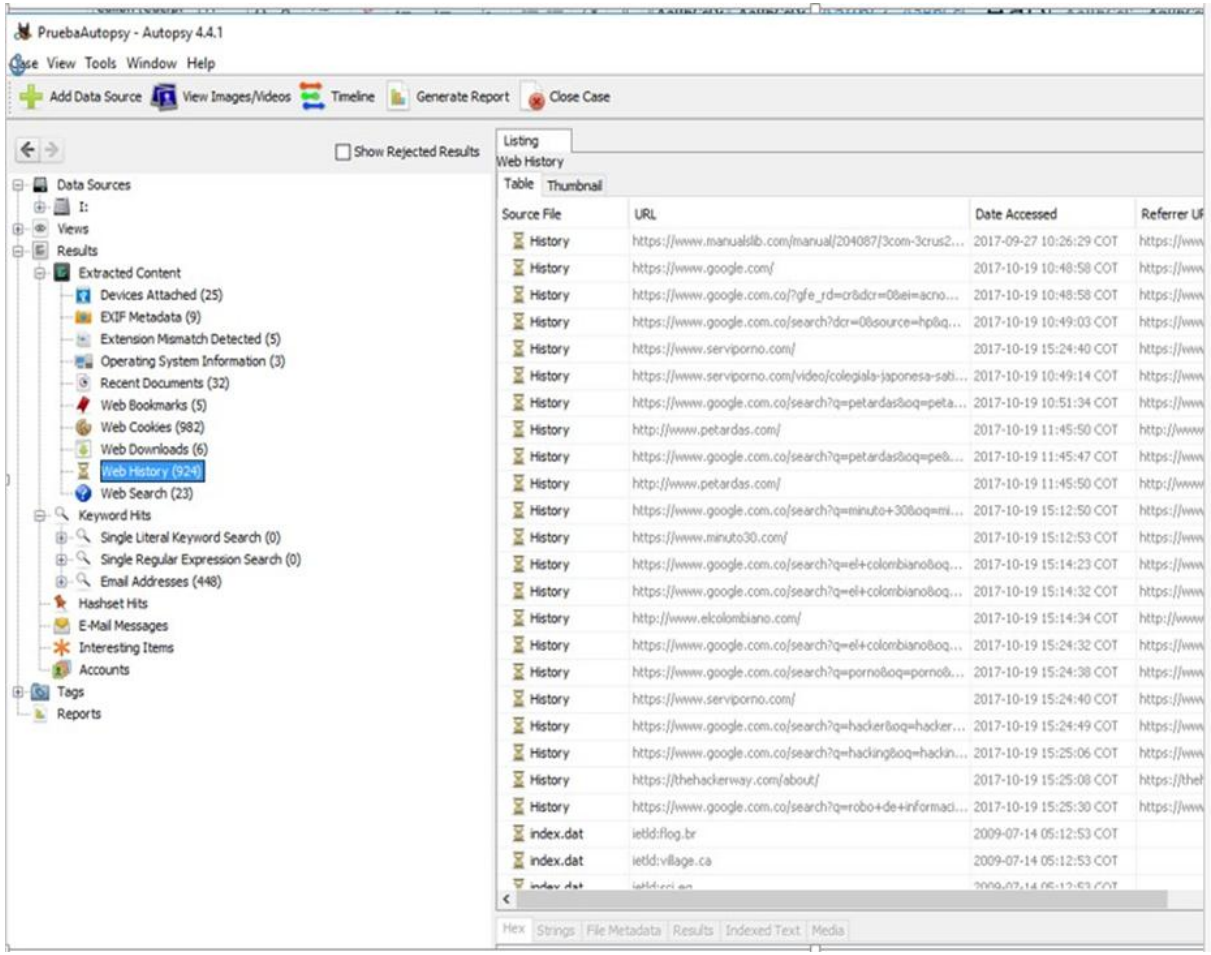

Imagen : Captura historial web

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

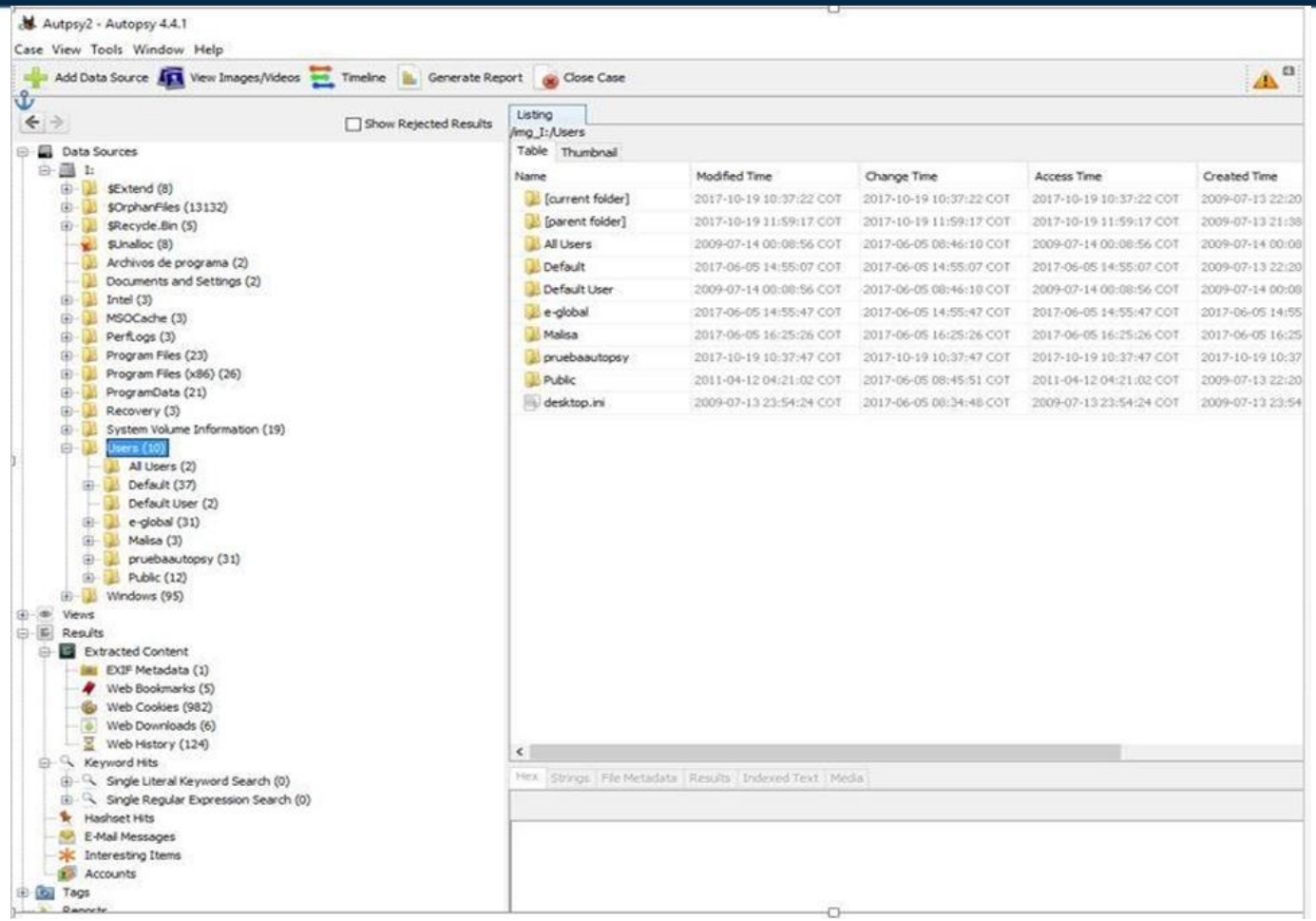

Imagen : Captura usuarios en el disco

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

Listing

Data Sources

Table | Thumbnail

Name	Type	Size (Bytes)	Sector Size (Bytes)	MD5 Hash	Timezone	Device ID
I:	Image	103477188608	512		America/Bogota	300545cd-d7fc-40e0-9934-776b73ed0555

Listing

Operating System Information

Table | Thumbnail

Source File	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Tags
SYSTEM	E-GLOBAL-PC		Windows_NT	AMD64	%SystemRoot%\TEMP	I:	
SYSTEM	E-GLOBAL-PC		Windows_NT	AMD64	%SystemRoot%\TEMP	I:	

Imagen : Captura tamaño del disco y formato

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

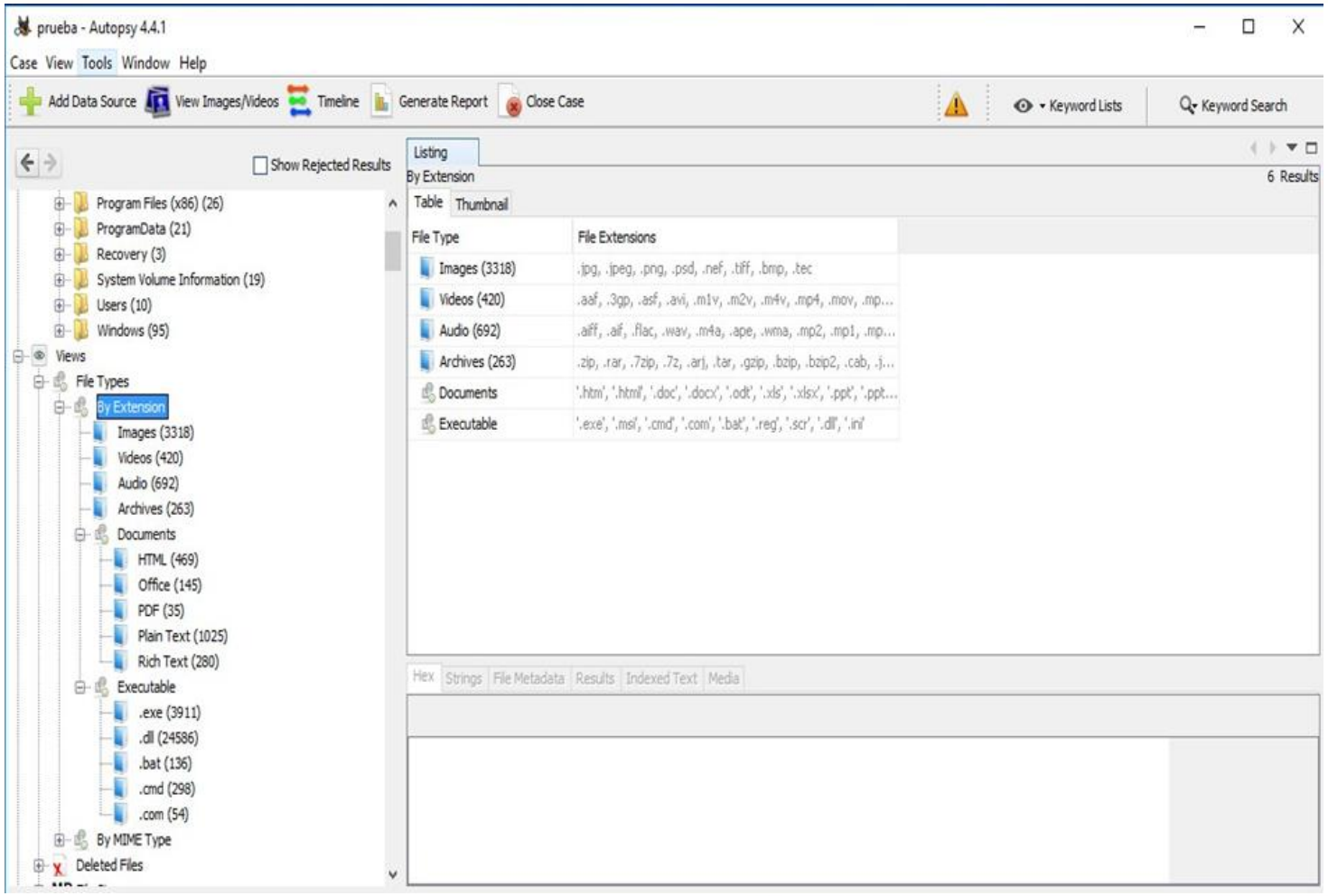

Imagen : Captura total de archivos en el disco

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

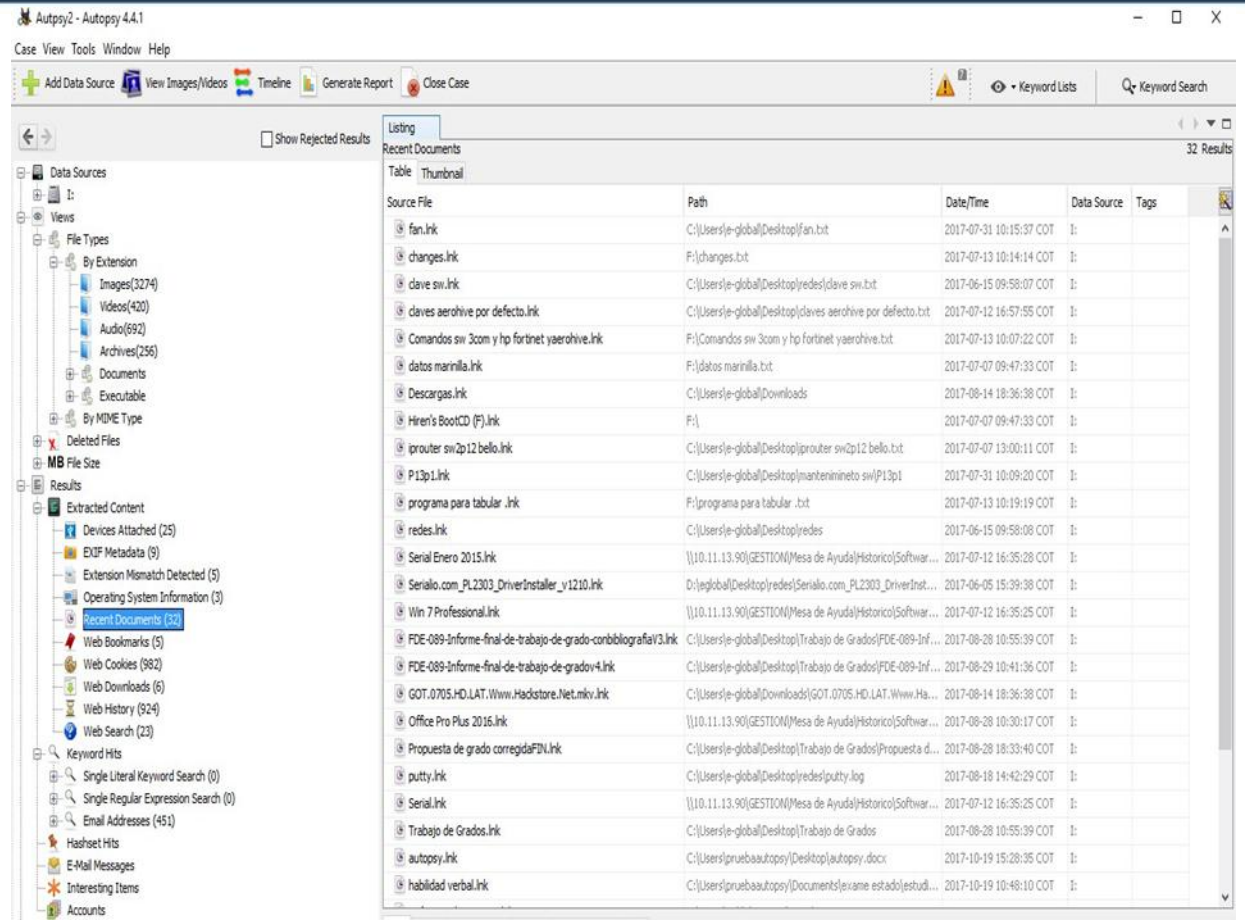

Imagen : Captura archivos abiertos recientes

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

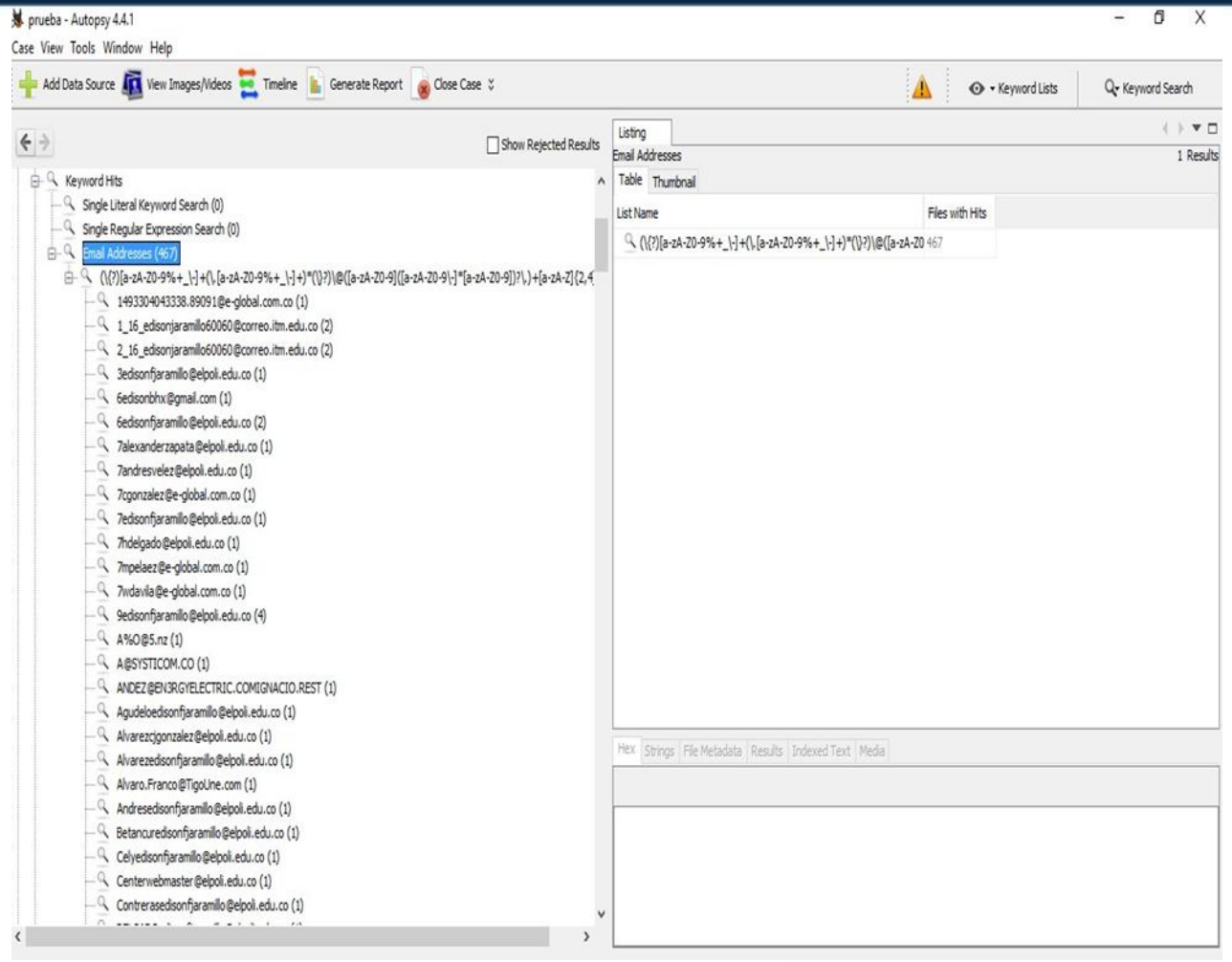

Imagen : Captura Direcciones de correo usadas

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

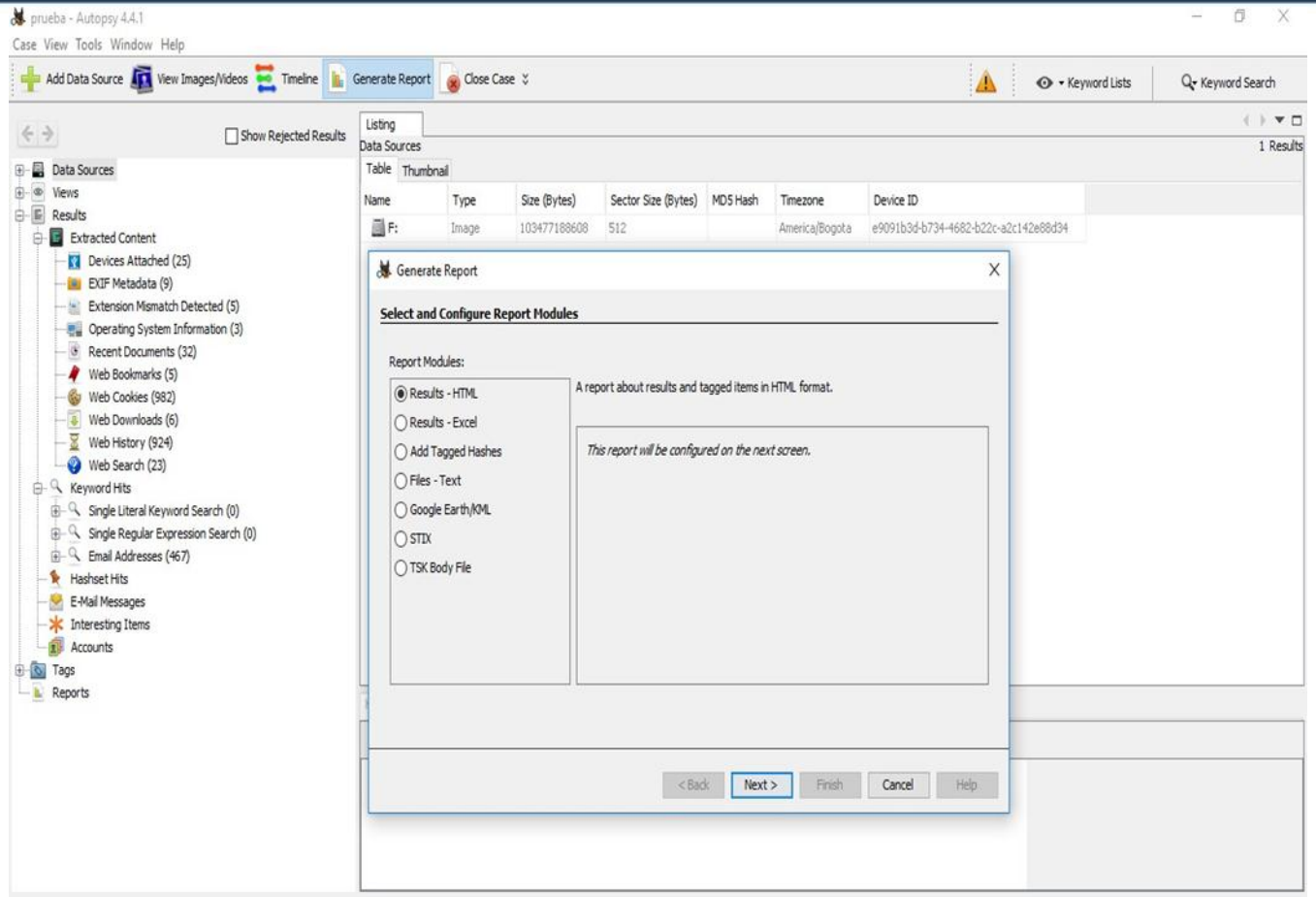

Imagen : Captura formatos de exportar los resultados

DESCARGA, INSTALACIÓN Y PRUEBA CON AUTOPSY

Conclusión de la herramienta Autopsy

De acuerdo con los resultados de la prueba con Autopsy, se puede decir que es una herramienta muy completa para un análisis forense, ya que recopila mucha información importante para la investigación y que pueden ser evidencias. Una de sus ventajas es que no se altera la información en el disco original, ya que crea una imagen, el origen queda intacto, respetando la cadena de custodia.