INFORME CON AUTOPSY

MARIANA SÁNCHEZ MURILLO

SEGURIDAD Y AUDITORIA DE REDES

RAFAEL SANDOVAL MORALES

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ “DIEGO LUIS CÓRDOBA” INGENIERIA DE TELECOMUNICACIONES E INFORMATICA

QUIBDÓ-CHOCÓ

2024-2

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

Este informe presenta el proceso de adquisición, preservación y análisis de una memoria USB marca Kingston de 16 GB, utilizando herramientas especializadas como Autopsy (en sus versiones para Kali Linux y Windows) y FTK Imager. El propósito principal de este estudio es identificar, recuperar y documentar evidencia digital que permita determinar posibles actividades maliciosas, archivos eliminados o información relevante que pueda contribuir al esclarecimiento de un caso hipotético de seguridad informática.

Durante el desarrollo de la práctica, se aplican los conocimientos adquiridos a lo largo de las clases de SEGURIDAD Y AUDITORIA DE REDES. Se busca demostrar el proceso completo que un perito digital debe seguir para realizar un análisis técnico riguroso.

2. OBJETIVO GENERAL

Realizar un análisis forense completo de una memoria USB Kingston de 16 GB utilizando las herramientas FTK Imager y Autopsy, con el fin de identificar, recuperar y documentar evidencia digital relevante siguiendo los procedimientos establecidos en la informática forense.

3. OBJETIVOS ESPECIFICOS

- Crear una copia forense del dispositivo USB usando FTK Imager, asegurando que los datos no se alteren mediante el uso de valores hash.
- Comprobar que la copia forense es idéntica al USB original, comparando los valores hash obtenidos antes y después del proceso.
- Analizar la imagen forense con Autopsy en Windows y Kali Linux para revisar de forma organizada su contenido, recuperar archivos eliminados o sospechosos e identificar posibles evidencias.

4. PLANTEAMIENTO DEL PROBLEMA

En la clase de SEGURIDAD Y AUDITORIA DE REDES, se pide realizar un análisis forense sobre una memoria USB, asegurando la integridad de los datos y validez de estos.

Por ello, este trabajo busca aplicar herramientas especializadas como FTK Imager y Autopsy para demostrar el proceso del análisis forense digital, garantizando resultados verificables y útiles para una posible investigación formal.

5. MEMORIA USB

La memoria **USB** que se usará para el analisis forense es de la marca **Kingston** con la capacidad de almacenamiento de **16GB** de color plateado de alineanción metalica con la cual se trabajara en el trayecto del laboratorio en **kali linux**.

Esta es la parte delantera de la memoria **Kingston**:

Ilustración 1: Delantera Kingston

Esta es la parte trasera de la memoria **Kingston**:

Ilustración 2: Trasera Kingston

5.1 CONFIGURACIÓN DE LA MEMORIA USB EN KALI LINUX

En la parte superior del Kali Linux entre las opciones seleccionaremos **Dispositivo (**donde podremos conectar la memoria usb **Kingston** a la máquina virtual de **Kali Linux)** luego se despliega un menú en el cual elegiremos la opción de **USB** , finalmente pulsaremos en el botón **Preferencias USB** como podremos observar a continuación:

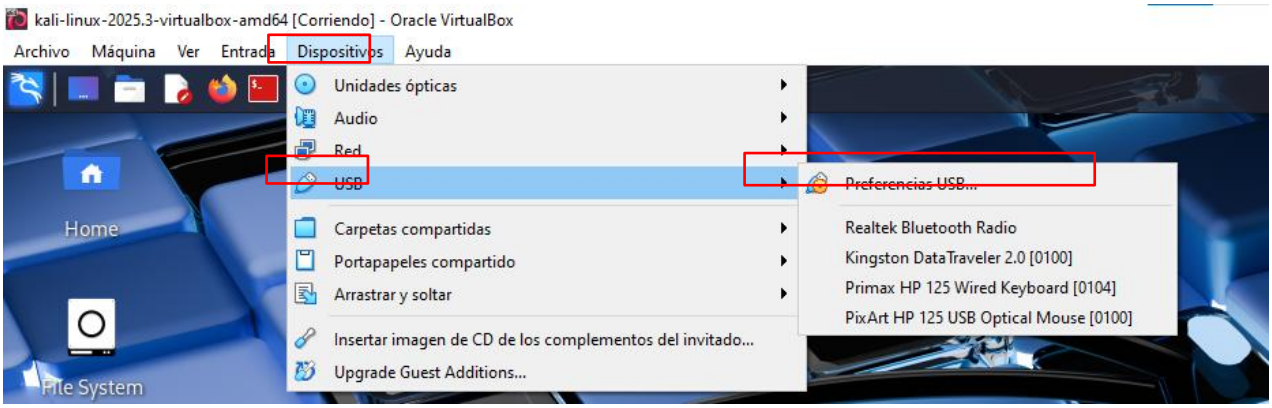


Ilustración 3:Dispositivos

Luego en **Filtros de dispositivos USB** vamos a pulsar en el botón de **usb con el símbolo +,** en el menú que se desplegó aparecen los dispositivos que podremos agregar, buscaremos la memoria en este caso se busca por la marca llamada **Kingston Data Traveler 2.0 [0100],** terminamos pulsando en **Aceptar.**

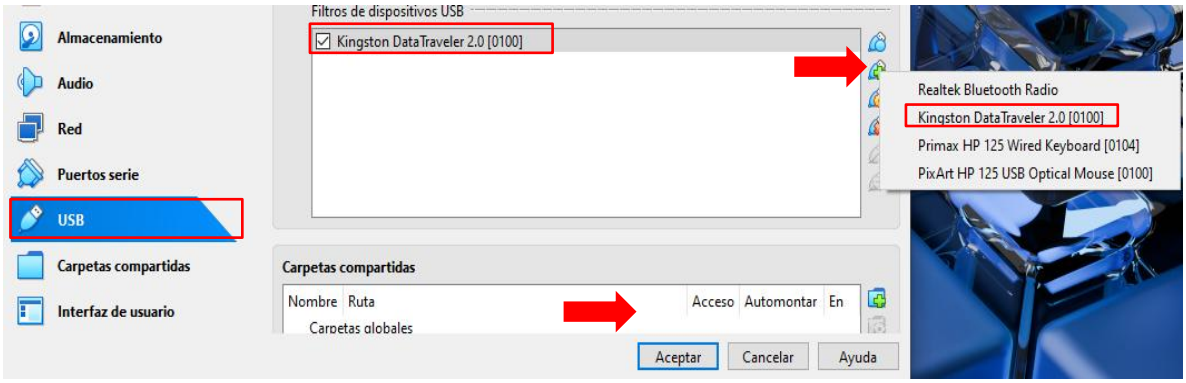


Ilustración 4:Selección de memoria usb

5.2 DETECTANDO DISPOSITIVOS CONECTADOS EN KALI LINUX

Finalmente tendremos la memoria usb **Kingston** en el entorno de **Kali Linux** lista para el analisis forense.

Ilustración 5:Memoria Kingston

Con el comando **fdisk -l** listaremos todos los dispositivos que están conectados en la máquina virtual de **Kali Linux,** en este caso la memoria **Kingston** es **Disk /dev/sdb: 14.54 GiB** (podremos encontrarlo más fácil si nos fijamos en la capacidad de almacenamiento de nuestra memoria USB en este caso la memoria tiene 16GB que equivale en Kali Linux en **14.54 GiB**)

```
┌──(root㉿kali)-[~]
└─# fdisk -l
Disk /dev/sda: 80.09 GiB, 86000000000 bytes, 167968750 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x06c77605

Device     Boot Start       End   Sectors  Size Id Type
/dev/sda1  *     2048 167968749 167966702 80.1G 83 Linux


Disk /dev/sdb: 14.54 GiB, 15614803968 bytes, 30497664 sectors
Disk model: DataTraveler 2.0
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0f1d95ca

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdb1        8064 30497663 30489600 14.5G  c W95 FAT32 (LBA)
```

Ilustración 6:Comando fdisk -l (listar dispositivos conectados)

5.3 CREACIÓN DEL HASH DE LA MEMORIA USB

Creamos la carpeta donde guardaremos el **hash** con el comando **mkdir mariana**, luego accedemos a la carpeta con **cd mariana**.

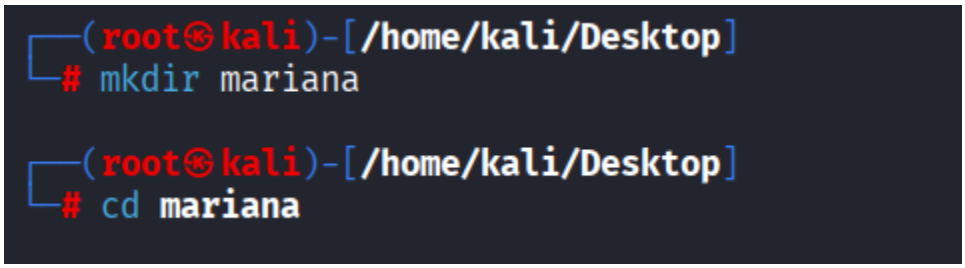


Ilustración 7:Creación de carpeta

En el comando estará incluida la ruta en donde queremos que se guarde y el nombre del archivo que en este caso es **análisis_forense_hash.sha1**), el formato **sha1** es el formato del hash.

Ilustración 8: Comando sha1sum

Ahora para visualizar el hash generado ingresaremos el comando **cat análisis_forense_hash.sha.**

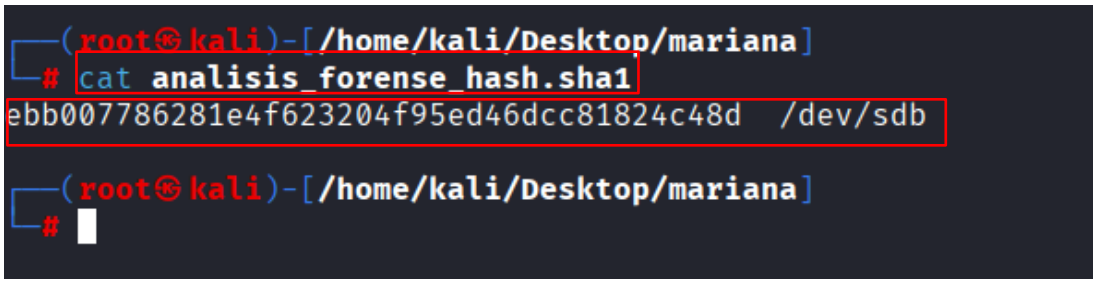


Ilustración 9: Comando cat (visualizando el hash en pantalla)

5.4 CREACIÓN DE LA IMAGEN DE LA MEMORIA USB

Continuamos con el comando **dd if=/dev/sdb of=/home/Kali/Desktop/mariana/imagen_usb_forense.dd** , (el comando debe ir con la ruta donde se guarda y el nombre del archivo con su formato **dd**), creando una imagen completa de todo el almacenamiento de la memoria usb que en este caso es **Kingston** de

16GB de almacenamiento, la imagen en formato **dd** tendrá todos los archivos que estuvieron y están en la memoria, el peso de la imagen dependerá de las **GB** de la memoria.

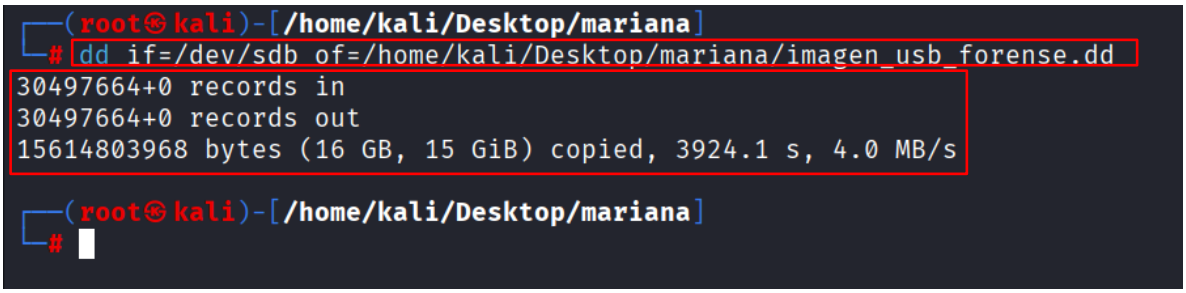


Ilustración 10: comando dd (creación de la imagen de almacenamiento)

Ahora listaremos los archivos que tendremos dentro de la carpeta con **ls -la** , luego de listar el contenido, específicamente seleccionamos la imagen y verificamos el hash con el siguiente comando **sha1sum imagen_usb_forense.dd** el resultado del hash de la imagen (**ee627779cbbdbf57258d48545f099ef9fbea9faa**) puede variar según el tipo de almacenamiento y memoria.

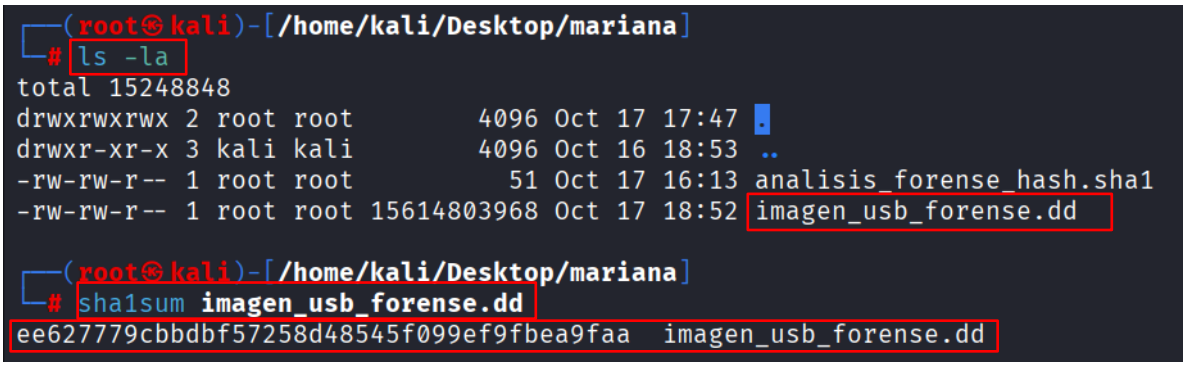


Ilustración 11:Comando sha1sum (hash de la imagen)

6. AUTOPSY EN KALI LINUX

Ahora buscaremos **autopsy** en nuestra barra de búsqueda que tiene como icono un perro, este abre una Shell que muestra el servicio activo con la **url (http://localhost:9999/autopsy),** también se puede iniciar la herramienta con el comando **autopsy** que muestra la misma Shell con la misma **url (http://localhost:9999/autopsy)**

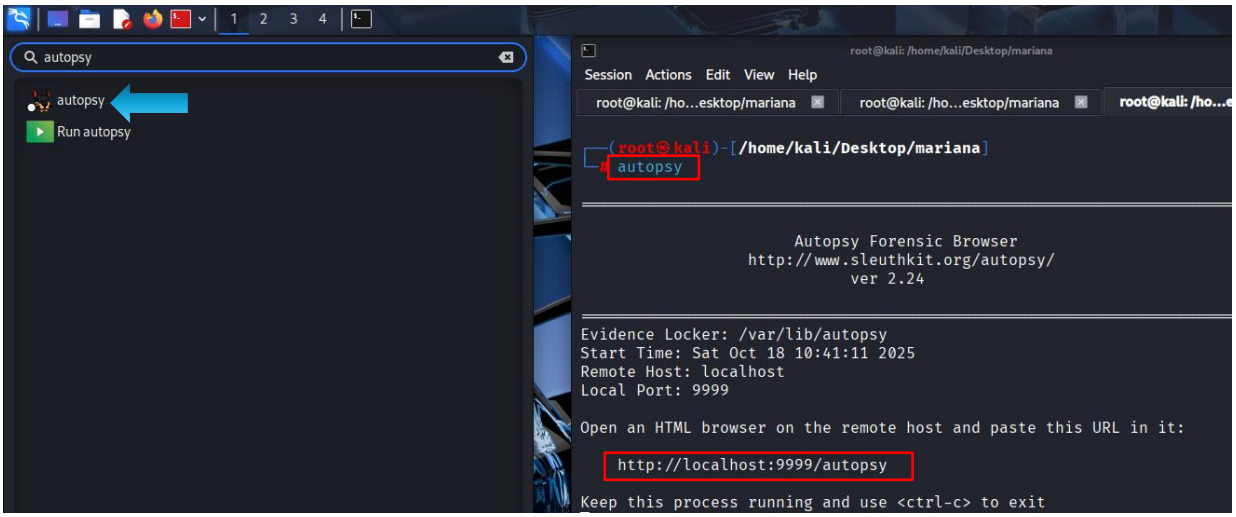


Ilustración 12: autopsy (atajos)

Con la url que se muestra (**http://localhost:9999/autopsy**) la ingresaremos en el navegador, dando como inicio la herramienta de **autopsy**

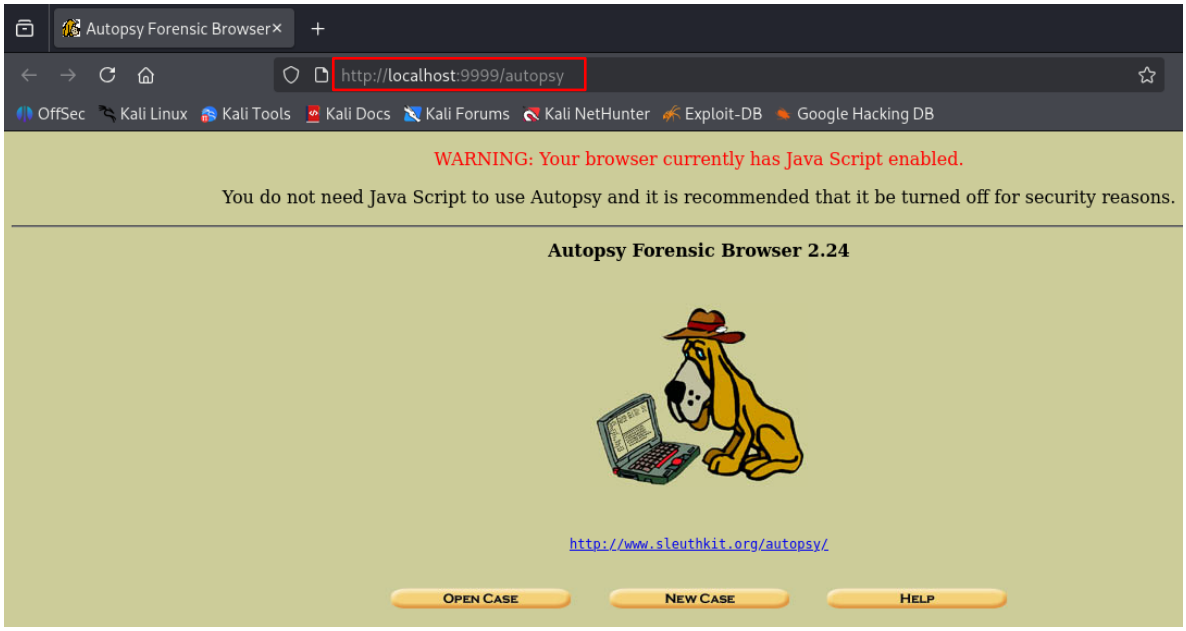


Ilustración 13:Autopsy

6.1 CREACIÓN DE NUEVO CASO EN AUTOPSY

Para poder trabajar con la herramienta iniciaremos un nuevo caso pulsando en el botón **NEW CASE**, (la imagen que se creó de la imagen servirá para examinar o recuperar los archivos que estuvieron o están en la memoria usb **Kingston**).

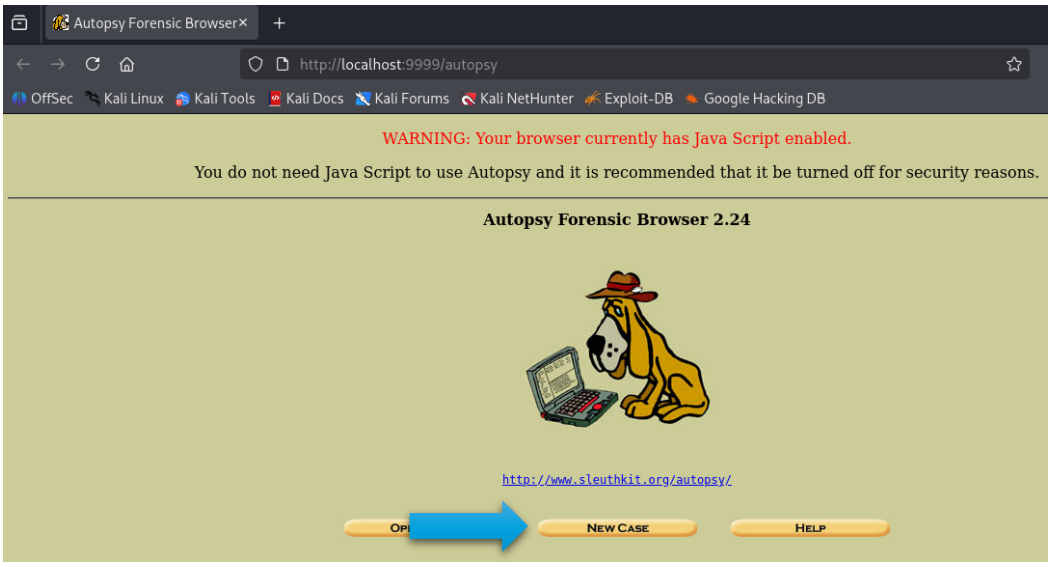


Ilustración 14:Creación del nuevo caso

En el campo **Case name** ingresaremos un nombre para el caso **primerCaso1,** el siguiente campo **Description** ingresaremos una descripción breve del tipo de tema que se estará desarrollando en este primer caso, en los campos de **Investigator Names** ingresaremos los nombres de los participantes, generamos este caso pulsando en **NEW CASE**.

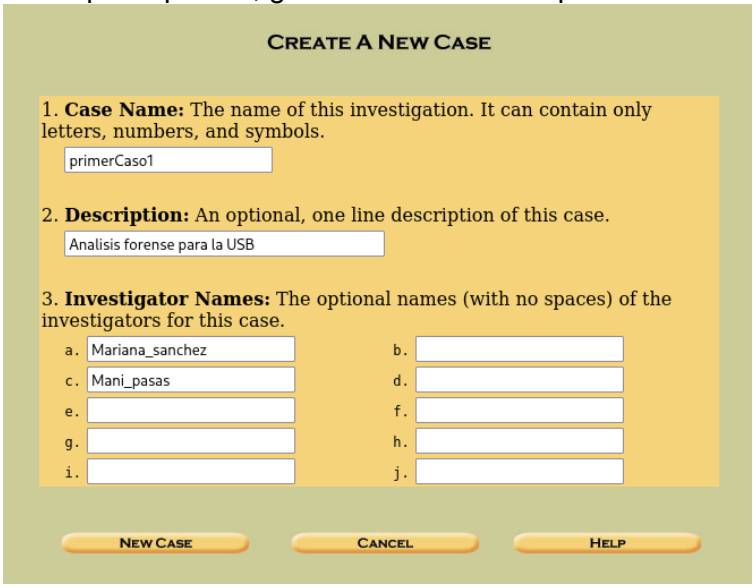


Ilustración 15:Create a new case

6.2 AGREGANDO UN HOST PARA EL CASO

Luego de que el primer caso este creado vamos a agregarle un **host** a nuestro caso, dependiendo de cuantos investigadores, vamos a seleccionar el perfil de usuario con el que

se trabajara en este caso seleccionaré **Mariana_sanchez,** pulsaremos en el botón **ADD HOST** para agregar el host a trabajar para este caso.

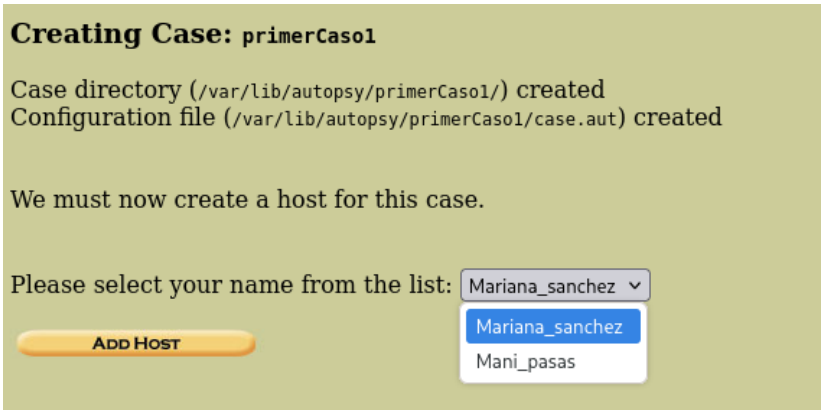


Ilustración 16:Caso creado (selección de investigador)

En este apartado para agregar un nuevo host, completaremos el campo de **Host Name** ingresando el nombre del dispositivo donde estamos realizando el análisis forense en este caso (**laptop_HP**) en el campo de **Description** pondremos una descripción de este host, por ultimo pulsamos en **ADD HOST.**

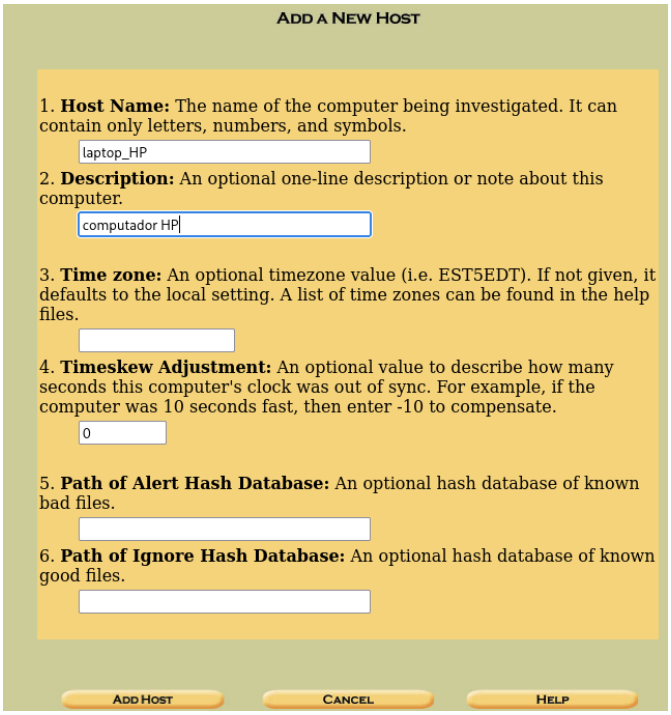


Ilustración 17:New host

6.3 AGREGANDO LA IMAGEN DE LA USB

Después de establecer los parámetros del host, vamos a añadir la imagen pulsando en el botón **ADD IMAGE.**

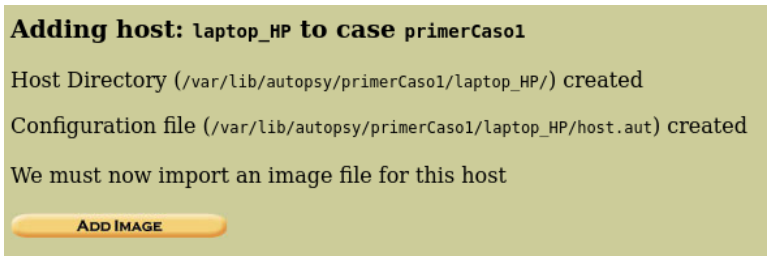


Ilustración 18:Añadir imagen

En este siguiente apartado vamos a pulsar en el botón de **ADD IMAGE FILE** para poder buscar la imagen de la memoria que generamos anteriormente que está en formato **dd**.

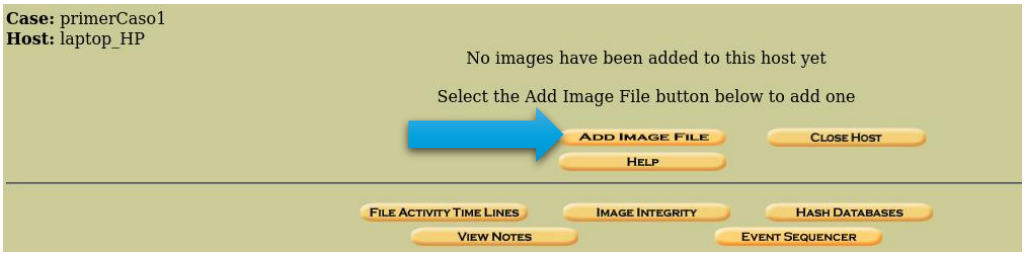


Ilustración 19:Add image file

En **Location** vamos agregar la ruta donde creamos la imagen **home/kali/Desktop/imagen_usb_forense.dd** en **Type** seleccionamos el **Disk** que se trata del tipo de dispositivo ya sea disco duro o memoria usb, en **Import Method** seleccionamos el **symlink** luego daremos en **NEXT.**

6.4 DETALLES DE LA IMAGEN

En este apartado podremos ver los detalles por defecto de la imagen, en este caso del apartado **File System Details** podremos ver el tipo de formato que se usa en la memoria usb **Kingston** en el campo **File System Type** muestra el tipo de formato **fat32**

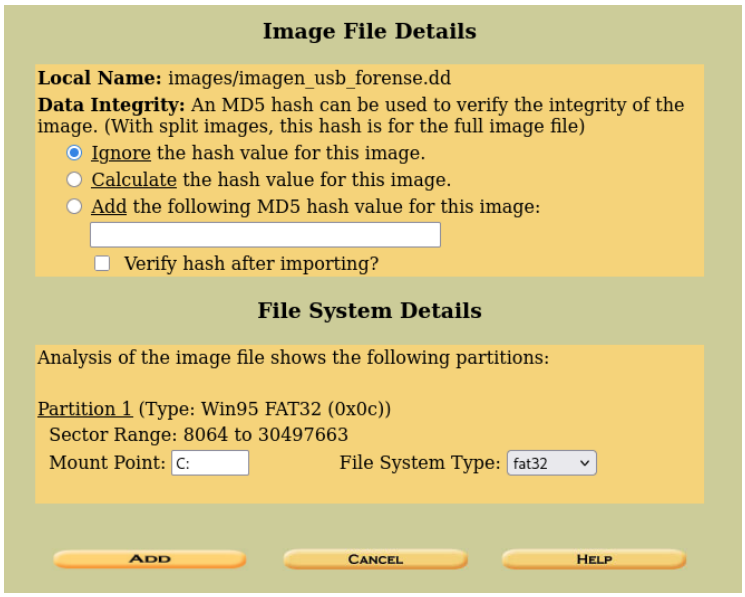


Ilustración 20:Detalles de la imagen

Aquí también se encontrará información más técnica acerca del formato **fat32**

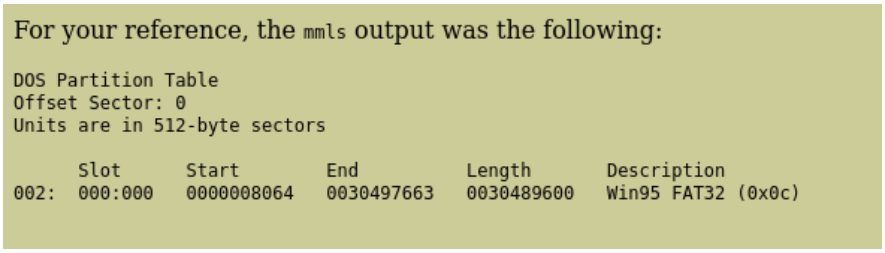


Ilustración 21:Información técnica de la imagen

Ahora confirmaremos la configuración para el análisis pulsando en el botón de **ok.**

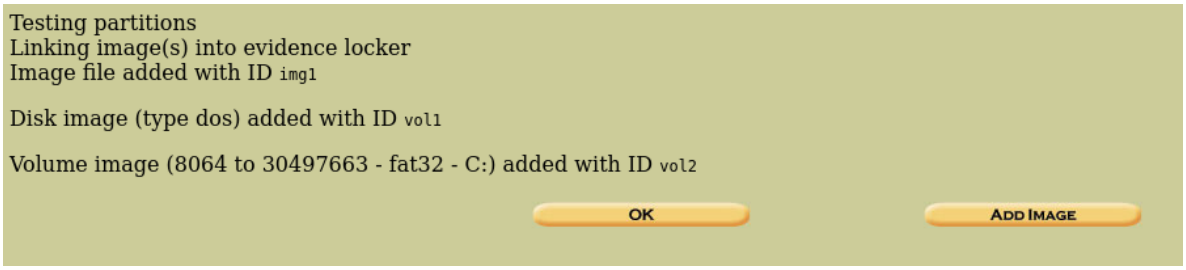


Ilustración 22:Testing de partición

6.5 ARCHIVOS DE LA MEMORIA USB EN AUTOPSY

Luego en esta ventana seleccionaremos el volumen en el que tenemos la imagen, en este caso, el volumen de la imagen fue con el formato **fat32** , para comenzar con el análisis pulsaremos el botón **ANALYZE.**

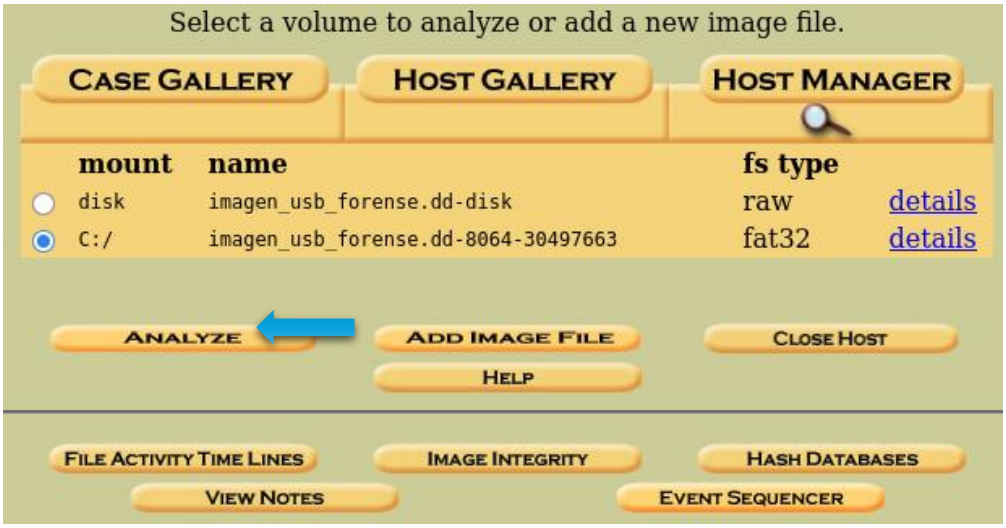


Ilustración 23:Selección del volumen

Ahora seleccionaremos la opción de **FILE ANALYSIS**, en este, se encuentra todo el contenido que se encuentra en el almacenamiento de la memoria usb que extrajo la imagen, los archivos que se marcan de color rojo son los que fueron eliminados anteriormente de la memoria usb **Kingston** y los de color azul son los que aun permanecen en la memoria.

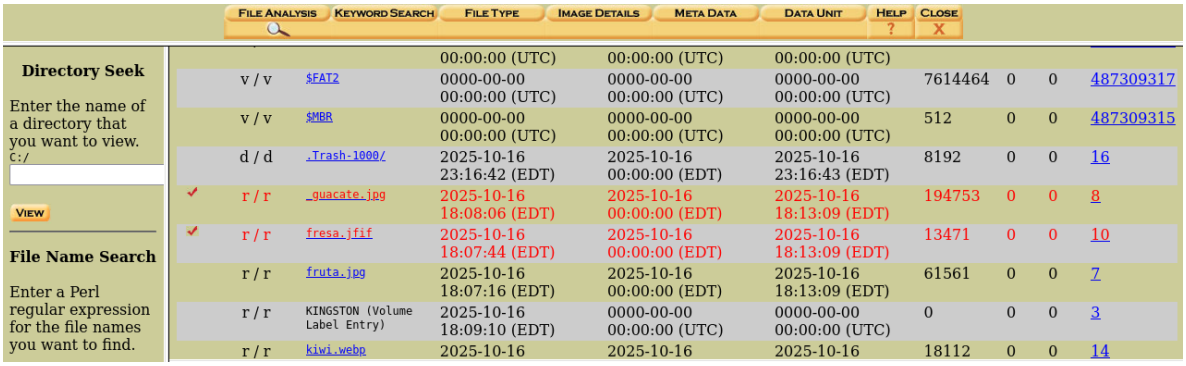


Ilustración 24:Archivos de la imagen

6.6 GENERANDO EL MD5 DE LA IMAGEN

En la parte superior de la ventana pulsamos en el botón **GENERATE MD5 LIST OF FILES** esto nos sirve para genera el **MD5** de la imagen.

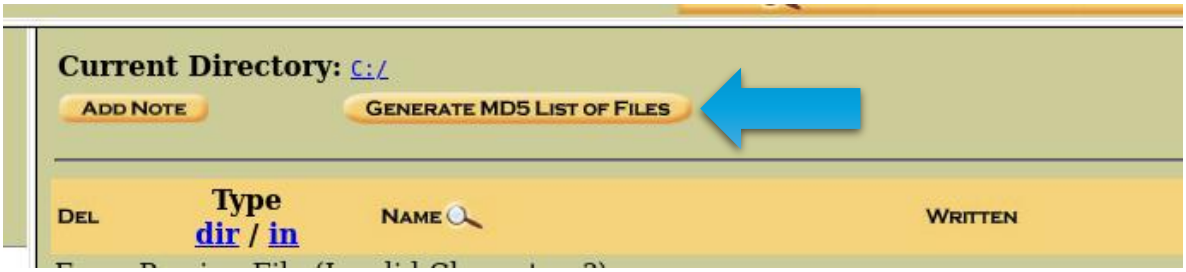


Ilustración 25:Generar md5

Este genera el MD5 de la imagen y de los archivos que están en la imagen, cada uno con el hash de cada archivo encontrado.

```
MD5 Values for files in C:/ (imagen_usb_forense.dd-8064-30497663)

d41d8cd98f00b204e9800998ecf8427e  -     KINGSTON    (Volume Label Entry)
2fc40b102d00951d3fcd29fdb983088b  -     fruta.jpg
b9c136b6eff7b614ce8db6ec11d8bd9b  -     mango.webp
b3848e47c0e8e76e251c29c7124a9272  -     kiwi.webp
```

Ilustración 26:MD5 generado

7. AUTOPSY EN WINDOWS

Vamos a la página de descarga de autopsy **https://www.autopsy.com/download/** iremos directamente a descargar autopsy pulsando en el botón **DOWNLOAD 64-BIT >** la descarga depende de la velocidad del internet, luego de la descarga tendremos un instalador llamado **autopsy-4.22.1-64bit.msi**

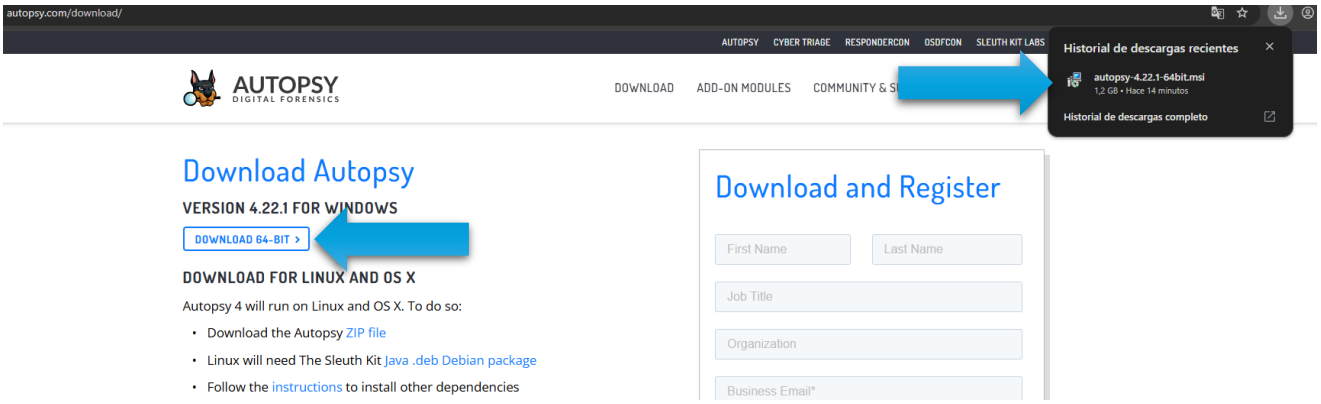


Ilustración 27:Descarga de autopsy para Windows

Ejecutaremos el instalador de autopsy que acabamos de descargar, este apartado muestra la ventana de bienvenida, donde vamos a pulsar en el botón de **Next**

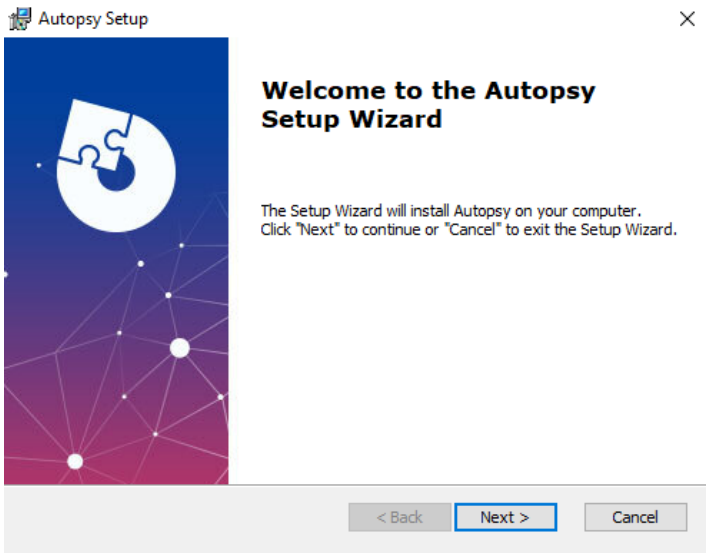


Ilustración 28:Ventana principal del instalador

7.1 INSTALANDO AUTOPSY

La siguiente ventana muestra donde queremos que se instale el autopsy, en este caso se dejará en la ruta por defecto **C:\Program Files\Autopsy-4.22.1** luego pulsamos en **Next** para continuar con la instalación.

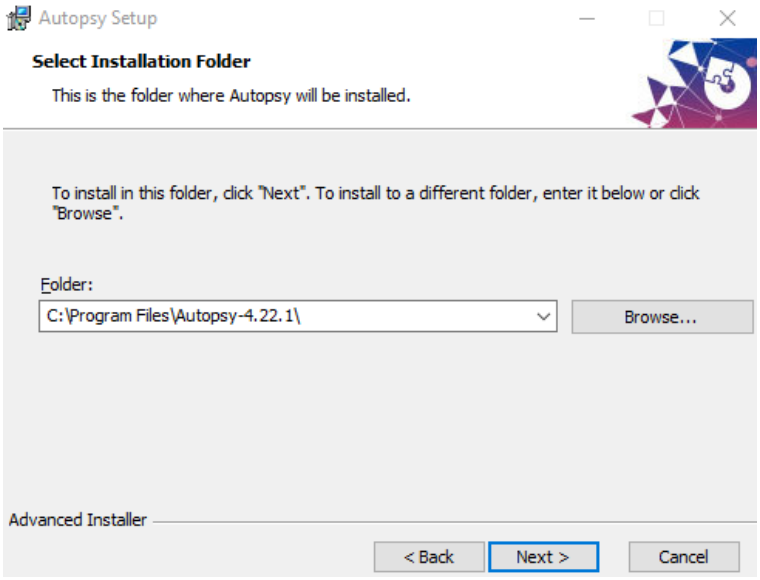


Ilustración 29:Ruta de instalación del autopsy

Finalmente tendremos el autopsy listo para su instalación, ahora vamos a pulsar en el **Install.**

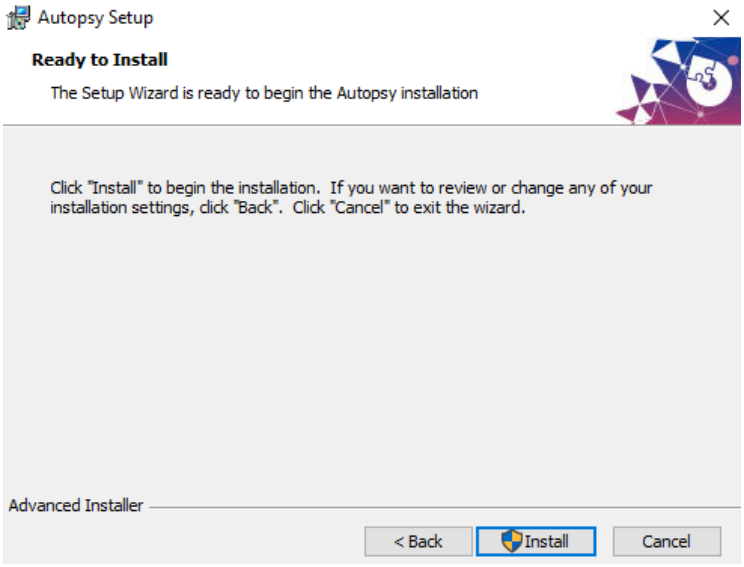


Ilustración 30:Instalación lista para comenzar

7.2 INSTALACIÓN COMPLETADA DE AUTOPSY

La ventana muestra el proceso de todos los componentes necesarios para que el autopsy se instale correctamente.

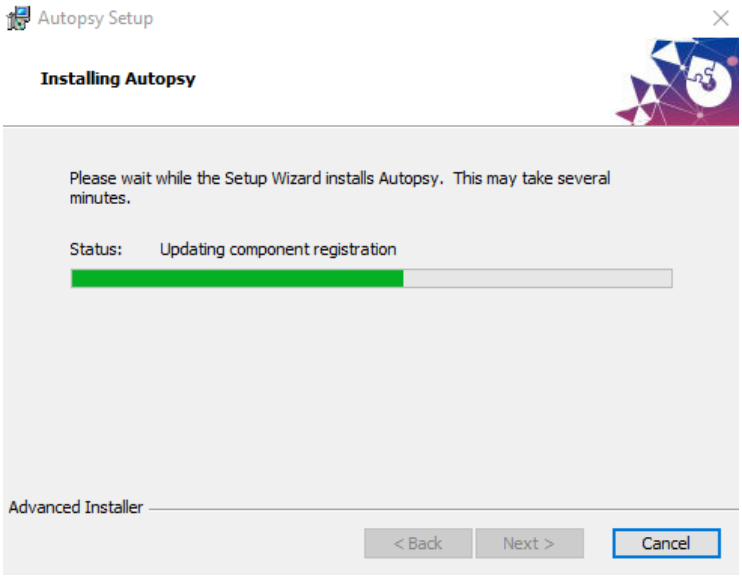


Ilustración 31:Instalando autopsy

Finalmente, la instalación de autopsy se ha completado correctamente, pulsaremos en **Finish**, para cerrar el instalador después de completada la instalación.

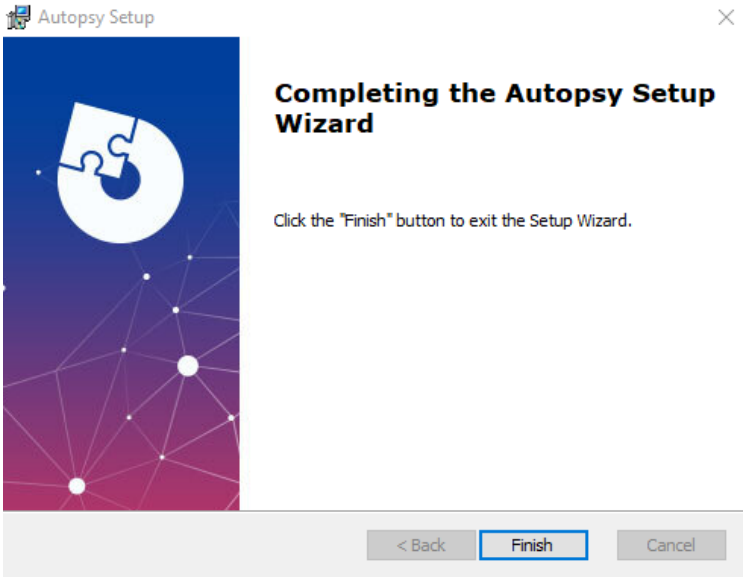


Ilustración 32:Instalación completada

7.3 INICIANDO AUTOPSY DE WINDOWS

Después de instalado el autopsy, saldrá con el icono de un perro, al igual que en Kali Linux

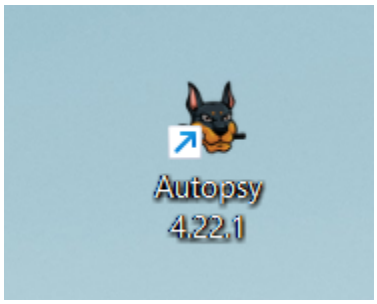


Ilustración 33:Icono autopsy

Cuando abramos **Autopsy** saldrá este menú para crear un caso o abrir un caso, seleccionaremos en **New Case**

Ilustración 34:ventana principal de autopsy

7.4 CREANDO UN NUEVO CASO

En el campo de **Case Name** pondremos un nombre para el nuevo caso que estamos creando (**Caso1**), luego seleccionaremos la carpeta donde estará guardada nuestro caso en el campo de **Base Directory** ¸ en este caso estará guardado en **C:\Users\chontaduro\Desktop\Autopsy-casos\Autopsy\,** luego daremos en **Next** para continuar.

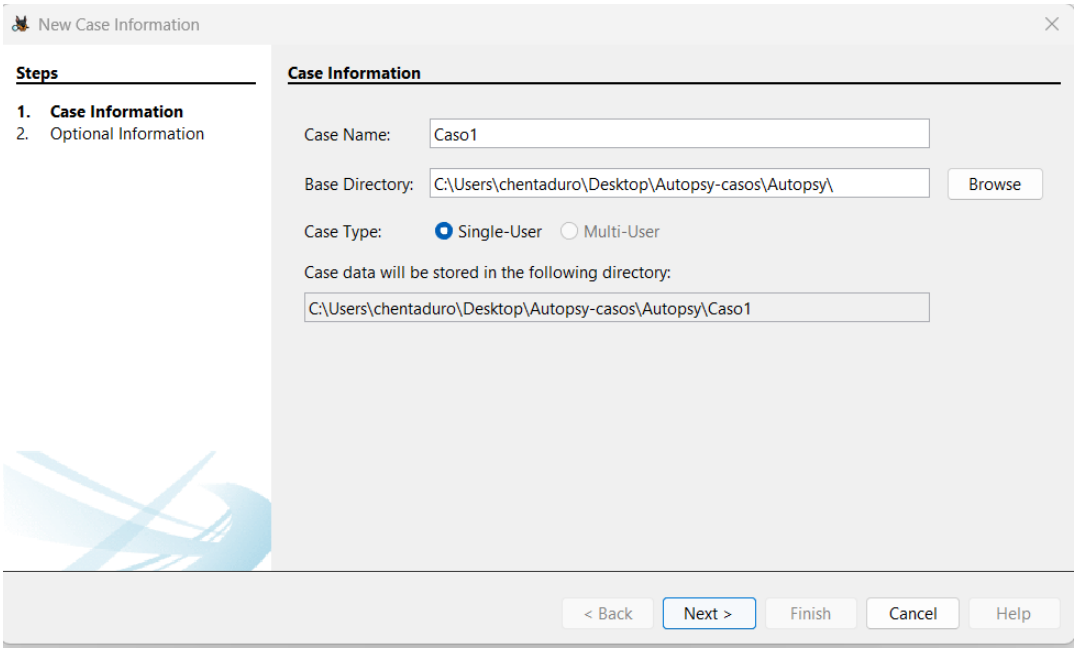


Ilustración 35:Nuevo caso

Aquí podremos información acerca de nuestro caso y el nombre del investigador luego de rellenar los campos daremos en finalizar en el botón **Finish**

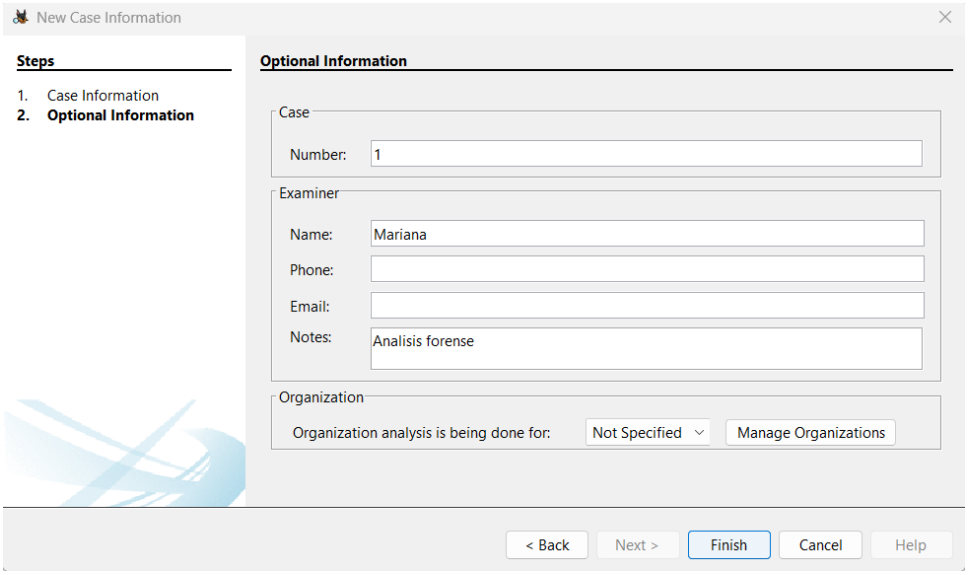


Ilustración 36:Información del nuevo caso

7.5 AGREGANDO EL HOST

Dejaremos la opción de **Generate new host name base don data source name** seleccionada por defecto, esto genera un host automáticamente para nuestro primer caso, presionaremos en **Next.**

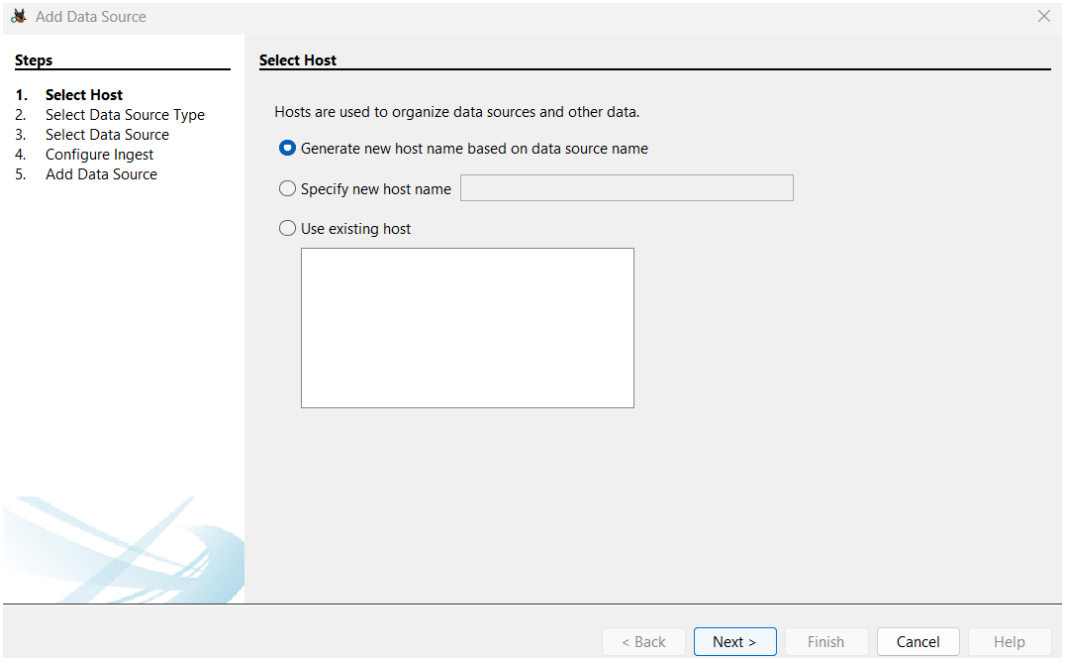


Ilustración 37:selección de host

En la selección del tipo de dato con el vamos a trabajar, en este caso, con una memoria usb **Kingston** de **16GB** de almacenamiento vamos a seleccionar, **Disk Image or VM File,** pulsaremos en **Next.**

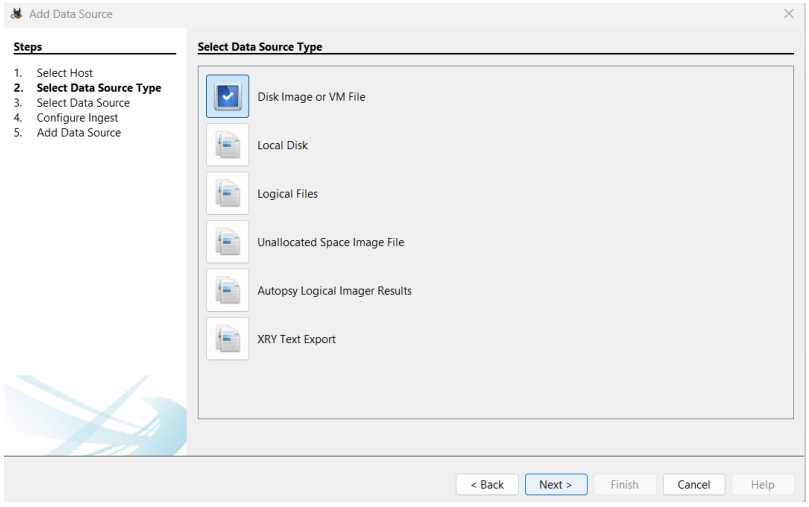


Ilustración 38:selección de tipo de dato

7.6 SELECCIÓN DE IMAGEN Y MÓDULOS

Esta siguiente ventana vamos a poder seleccionar nuestra imagen que generamos a partir de la memoria usb **Kingston** , la seleccionaremos en el campo de **Path**, luego daremos en **Next.**

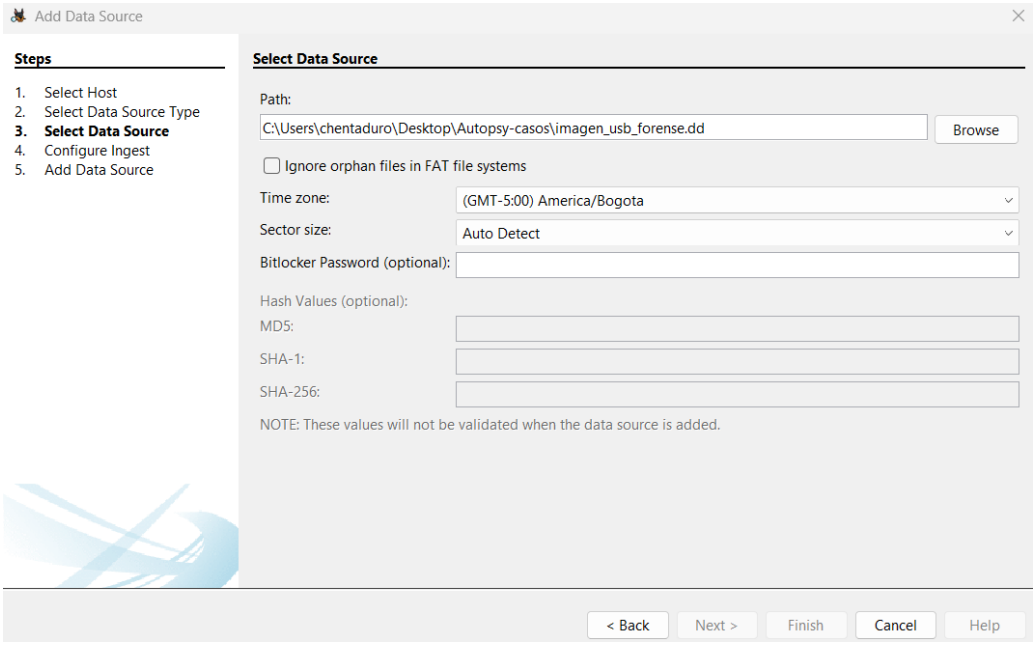


Ilustración 39:selección de la imagen

Ahora dejamos seleccionados los módulos con los cuales autopsy necesitará para trabajar, seguidamente solo pulsaremos en **Next.**

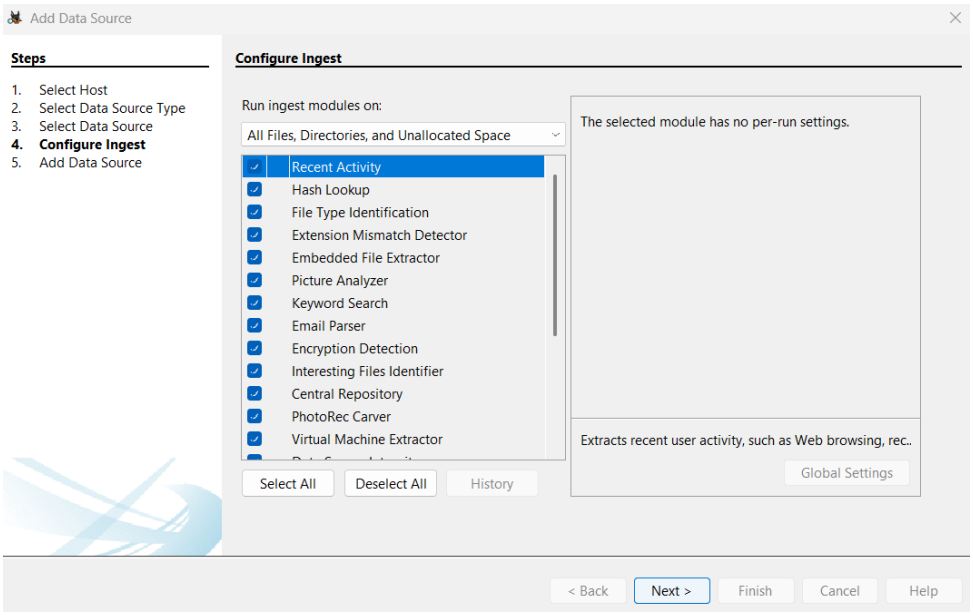


Ilustración 40:Modulos

7.7 ARCHIVOS EN LA IMAGEN

Ya tendríamos todo listo para empezar a examinar dentro de los archivos que la imagen capturó, entonces presionaremos **Finish.**

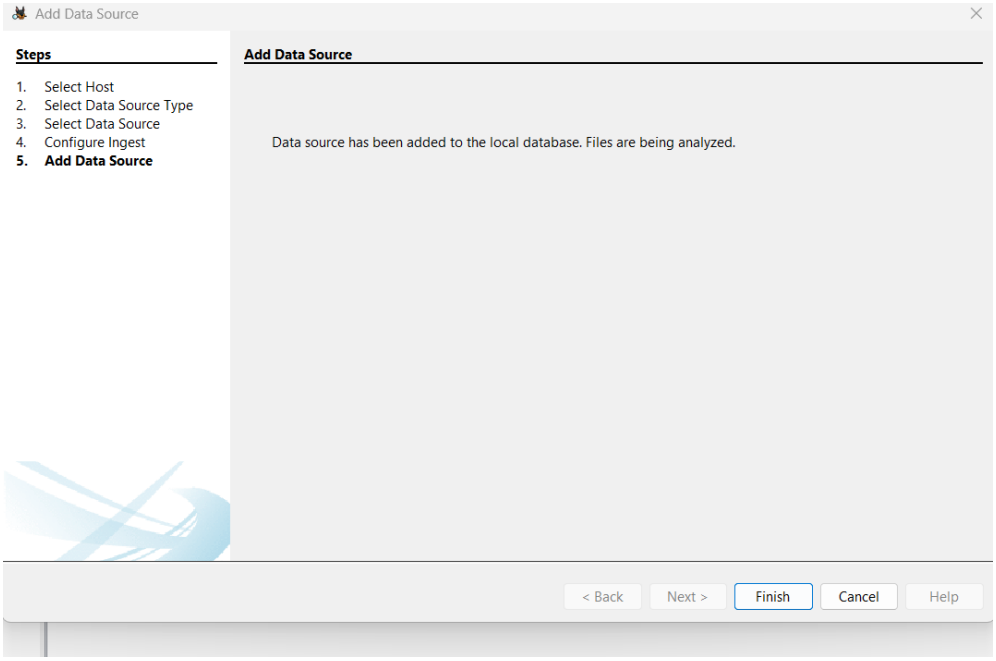
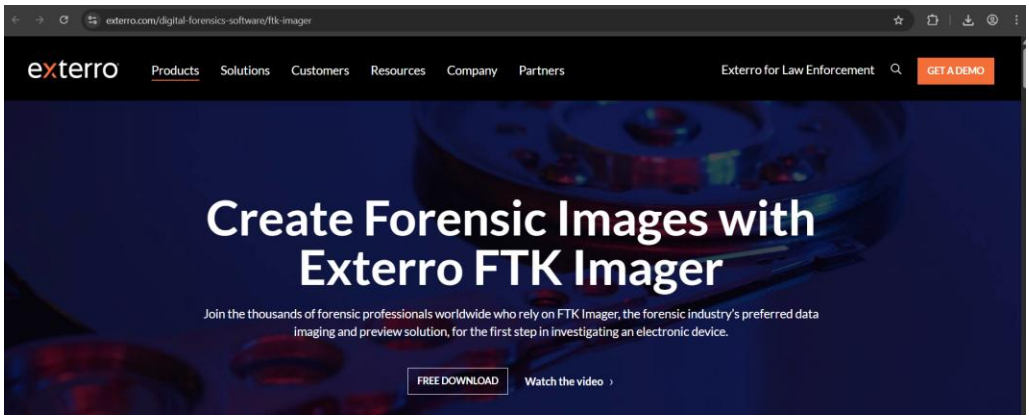


Ilustración 41:Configuración finalizada

7.8 FTK IMAGER

Esta nueva herramienta **FTK imager** que descargaremos también servirá para el análisis forense al igual que el funcionamiento que hace **autopsy,** iremos a esta página (**https://www.exterro.com/digital-forensics-software/ftk-imager**), en la pagina pulsaremos el botón **FREE DOWNLOAD.**



Luego en este apartado vamos a diligenciar los datos que se pide en el formulario.

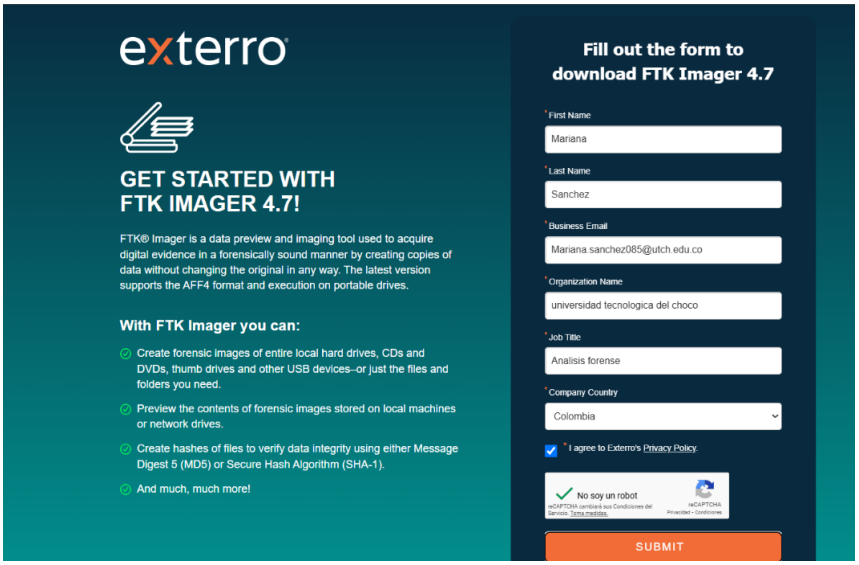


Ilustración 42:Formulario de descarga FTK imager

7.9 INSTALACIÓN DE FTK IMAGER

Este instalador de **FTK imager** quedara descargado **Exterro_FTK_Imager_(x64)-4.7.3.81.**

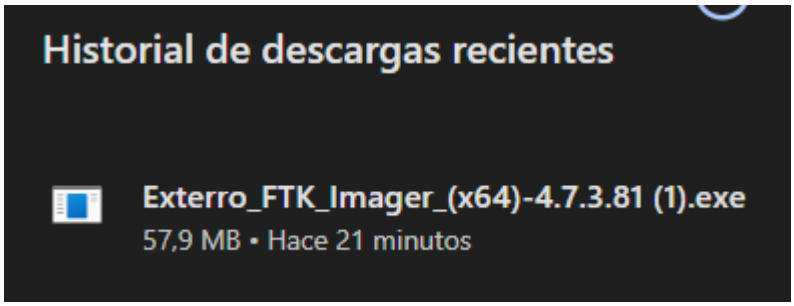


Ilustración 43:Instalador de FTK imager

Abriremos el instalador de **FTK IMAGER,** comenzara con un mensaje de bienvenida, ahora procederemos con la configuración para la instalación pulsaremos en **Next**

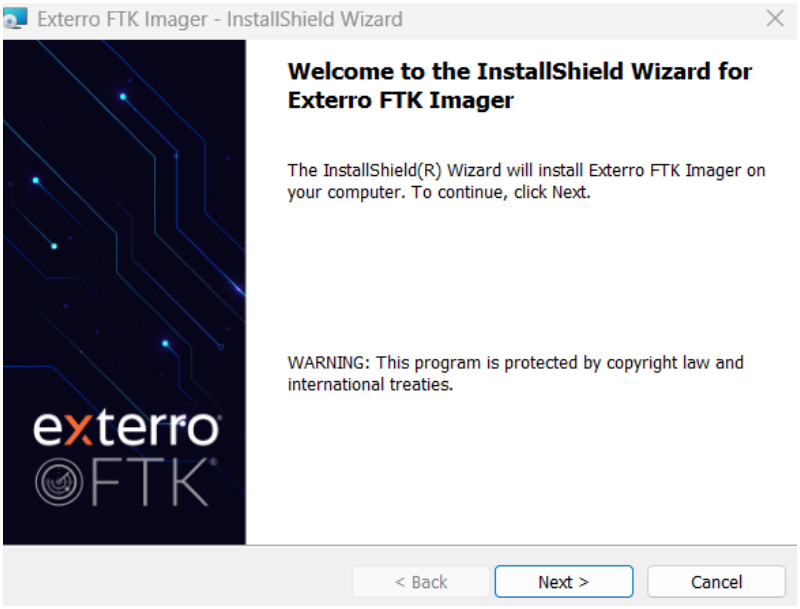


Ilustración 44:Instalador de FTK imager abierto

Aquí tendremos que seleccionar donde queremos que se instale el **FTK imager** , es recomendable dejar la ruta predeterminada que esta seleccionada por defecto, ahora pulsaremos en **Next.**

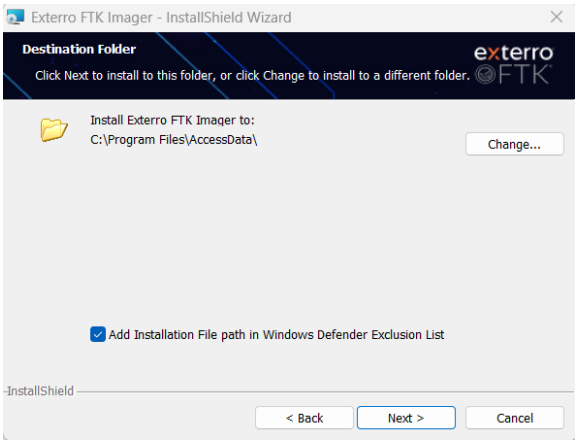


Ilustración 45:Ruta de instalación

7.10 INSTALACIÓN FTK IMAGER PREPARADA

El paquete de instalación estará preparada para dar inicio con la instalación de los componentes, pulsaremos en **Install.**

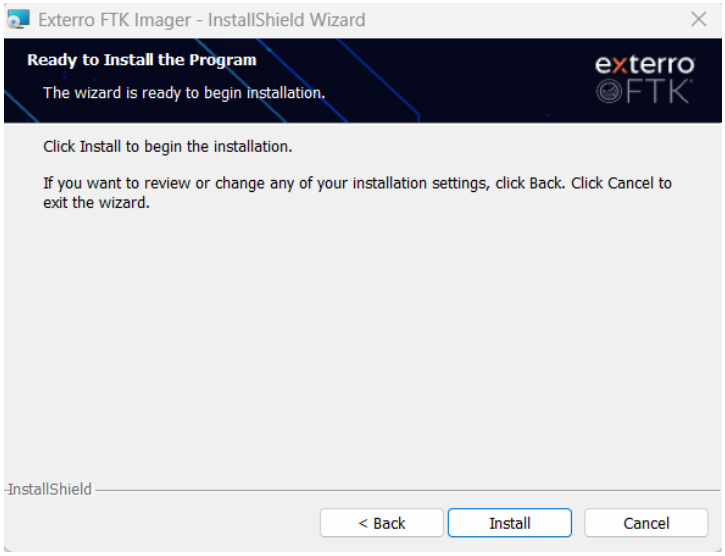


Ilustración 46:finalizando con la instalación

7.11 INICIANDO FTK IMAGER

En el escritorio quedara el icono de la aplicación indicando que ya podremos usarlo correctamente **Exterro FTK Imager.**

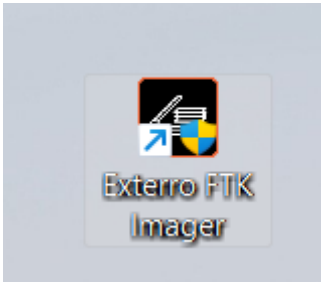
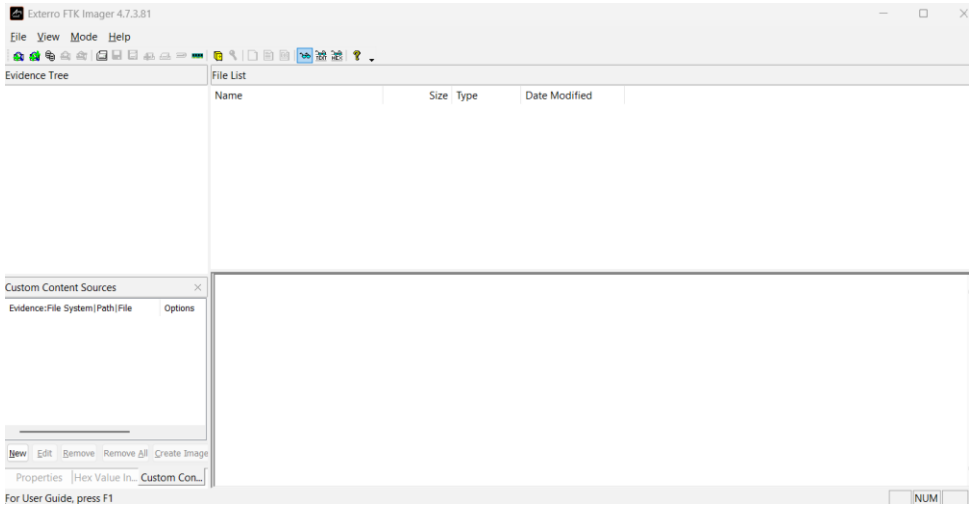


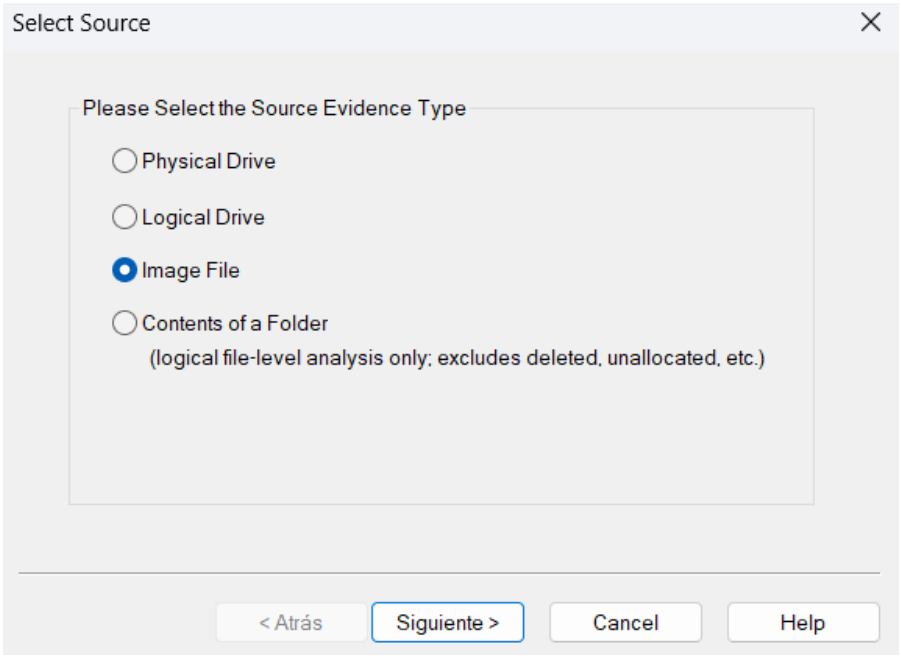
Ilustración 47:Icono FTK imager

Abriremos **FTK Imager** , luego de que este abierto para empezar a trabajar vamos a seleccionar el icono que tiene un signo **+** de color verde.



7.12 SELECCIÓN DE LA IMAGEN FTK IMAGER

Aquí vamos a seleccionar en la opción de **Image File** , le estaremos diciendo que vamos a trabajar con un archivo de imagen, luego daremos clic en **Siguiente.**



En el apartado de **Evidence Source Selection** pulsaremos **Browse** para buscar la imagen que tenemos extraída de la memoria ubs en este caso usaremos la misma que generamos en Kali Linux que se llama **imagen_usb_forense.dd** , luego pulsamos en **Finish.**

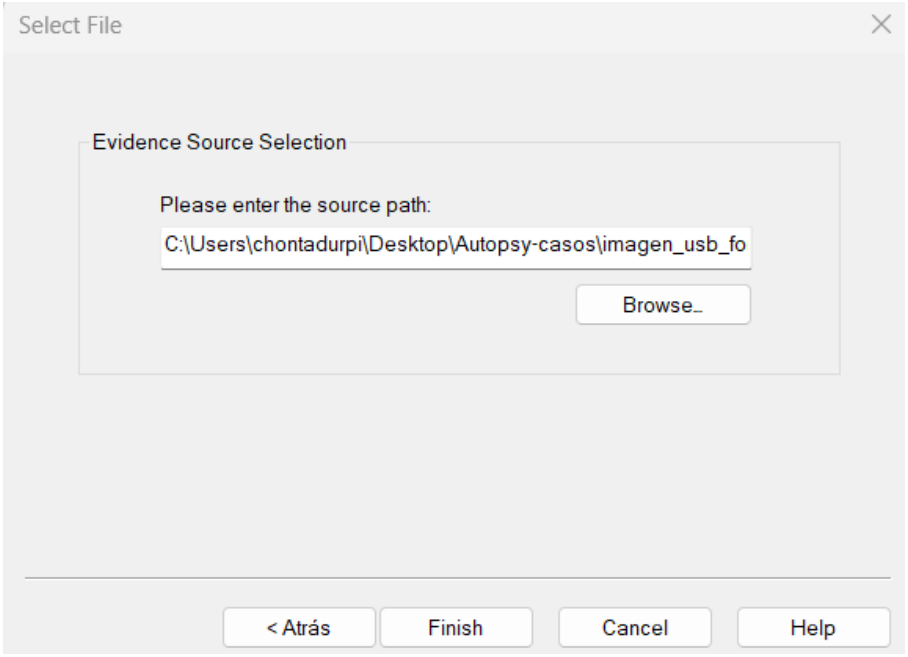


Ilustración 49:Seleccion de la imagen

8. RECOMENDACIONES

Hacer los laboratorios a tiempo.

9. CONCLUSIÓN

Finalmente, se concluye que la aplicación de una metodología forense rigurosa, acompañada del uso adecuado de herramientas como FTK Imager y Autopsy, permite preservar la integridad de la evidencia, recuperar información crítica y generar reportes técnicamente sólidos y reproducibles, contribuyendo al desarrollo de competencias profesionales en el ámbito de la informática forense.

10. BIBLIOGRAFIA

Rafael Sandoval Morales.