

**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

|      |                                                       |    |
|------|-------------------------------------------------------|----|
| 1.   | INTRODUCCIÓN .....                                    | 6  |
| 2.   | OBJETIVO GENERAL .....                                | 7  |
| 3.   | OBJETIVOS ESPECIFICOS.....                            | 7  |
| 4.   | PLANTEAMIENTO DEL PROBLEMA .....                      | 8  |
| 5.   | MEMORIA USB .....                                     | 9  |
| 5.1  | CONFIGURACIÓN DE LA MEMORIA USB EN KALI LINUX .....   | 9  |
| 5.2  | DETECTANDO DISPOSITIVOS CONECTADOS EN KALI LINUX..... | 10 |
| 5.3  | CREACIÓN DEL HASH DE LA MEMORIA USB .....             | 11 |
| 5.4  | CREACIÓN DE LA IMAGEN DE LA MEMORIA USB .....         | 12 |
| 6.   | AUTOPSY EN KALI LINUX .....                           | 13 |
| 6.1  | CREACIÓN DE NUEVO CASO EN AUTOPSY.....                | 14 |
| 6.2  | AGREGANDO UN HOST PARA EL CASO .....                  | 15 |
| 6.3  | AGREGANDO LA IMAGEN DE LA USB .....                   | 17 |
| 6.4  | DETALLES DE LA IMAGEN .....                           | 17 |
| 6.5  | ARCHIVOS DE LA MEMORIA USB EN AUTOPSY .....           | 19 |
| 6.6  | GENERANDO EL MD5 DE LA IMAGEN .....                   | 20 |
| 7.   | AUTOPSY EN WINDOWS.....                               | 20 |
| 7.1  | INSTALANDO AUTOPSY .....                              | 21 |
| 7.2  | INSTALACIÓN COMPLETADA DE AUTOPSY .....               | 22 |
| 7.3  | INICIANDO AUTOPSY DE WINDOWS.....                     | 23 |
| 7.4  | CREANDO UN NUEVO CASO .....                           | 24 |
| 7.5  | AGREGANDO EL HOST .....                               | 26 |
| 7.6  | SELECCIÓN DE IMAGEN Y MÓDULOS .....                   | 27 |
| 7.7  | ARCHIVOS EN LA IMAGEN .....                           | 28 |
| 7.8  | FTK IMAGER .....                                      | 28 |
| 7.9  | INSTALACIÓN DE FTK IMAGER .....                       | 29 |
| 7.10 | INSTALACIÓN FTK IMAGER PREPARADA .....                | 30 |
| 7.11 | INICIANDO FTK IMAGER .....                            | 31 |
| 7.12 | SELECCIÓN DE LA IMAGEN FTK IMAGER.....                | 32 |

|     |                      |    |
|-----|----------------------|----|
| 8.  | RECOMENDACIONES..... | 33 |
| 9.  | CONCLUSIÓN.....      | 34 |
| 10. | BIBLIOGRAFIA.....    | 35 |

## TABLA DE ILUSTRACIONES

|                                                                                                   |    |
|---------------------------------------------------------------------------------------------------|----|
| <a href="#"><u>Ilustración 1: Delantera Kingston</u></a> .....                                    | 9  |
| <a href="#"><u>Ilustración 2: Trasera Kingston</u></a> .....                                      | 9  |
| <a href="#"><u>Ilustración 3:Dispositivos</u></a> .....                                           | 10 |
| <a href="#"><u>Ilustración 4:Selección de memoria usb</u></a> .....                               | 10 |
| <a href="#"><u>Ilustración 5:Memoria Kingston</u></a> .....                                       | 11 |
| <a href="#"><u>Ilustración 6:Comando fdisk -l (listar dispositivos conectados)</u></a> .....      | 11 |
| <a href="#"><u>Ilustración 7:Creación de carpeta</u></a> .....                                    | 12 |
| <a href="#"><u>Ilustración 8: Comando sha1sum</u></a> .....                                       | 12 |
| <a href="#"><u>Ilustración 9: Comando cat (visualizando el hash en pantalla )</u></a> .....       | 12 |
| <a href="#"><u>Ilustración 10: comando dd (creación de la imagen de almacenamiento)</u></a> ..... | 13 |
| <a href="#"><u>Ilustración 11:Comando sha1sum (hash de la imagen)</u></a> .....                   | 13 |
| <a href="#"><u>Ilustración 12: autopsy (atajos)</u></a> .....                                     | 14 |
| <a href="#"><u>Ilustración 13:Autopsy</u></a> .....                                               | 14 |
| <a href="#"><u>Ilustración 14:Creación del nuevo caso</u></a> .....                               | 15 |
| <a href="#"><u>Ilustración 15:Create a new case</u></a> .....                                     | 15 |
| <a href="#"><u>Ilustración 16:Caso creado (selección de investigador)</u></a> .....               | 16 |
| <a href="#"><u>Ilustración 17:New host</u></a> .....                                              | 16 |
| <a href="#"><u>Ilustración 18:Añadir imagen</u></a> .....                                         | 17 |
| <a href="#"><u>Ilustración 19:Add image file</u></a> .....                                        | 17 |
| <a href="#"><u>Ilustración 21:Detalles de la imagen</u></a> .....                                 | 18 |
| <a href="#"><u>Ilustración 22:Información técnica de la imagen</u></a> .....                      | 18 |
| <a href="#"><u>Ilustración 23:Testin de partición</u></a> .....                                   | 18 |
| <a href="#"><u>Ilustración 24:Selección del volumen</u></a> .....                                 | 19 |
| <a href="#"><u>Ilustración 25:Archivos de la imagen</u></a> .....                                 | 19 |
| <a href="#"><u>Ilustración 26:Generar md5</u></a> .....                                           | 20 |
| <a href="#"><u>Ilustración 27:MD5 generado</u></a> .....                                          | 20 |
| <a href="#"><u>Ilustración 28:Descarga de autopsy para Windows</u></a> .....                      | 21 |
| <a href="#"><u>Ilustración 29:Ventana principal del instalador</u></a> .....                      | 21 |
| <a href="#"><u>Ilustración 30:Ruta de instalación del autopsy</u></a> .....                       | 22 |
| <a href="#"><u>Ilustración 31:Instalación lista para comenzar</u></a> .....                       | 22 |
| <a href="#"><u>Ilustración 32:Instalando autopsy</u></a> .....                                    | 23 |
| <a href="#"><u>Ilustración 33:Instalación completada</u></a> .....                                | 23 |
| <a href="#"><u>Ilustración 34:Icono autopsy</u></a> .....                                         | 24 |
| <a href="#"><u>Ilustración 35:ventana principal de autopsy</u></a> .....                          | 24 |
| <a href="#"><u>Ilustración 36:Nuevo caso</u></a> .....                                            | 25 |
| <a href="#"><u>Ilustración 37:Información del nuevo caso</u></a> .....                            | 25 |
| <a href="#"><u>Ilustración 38:selección de host</u></a> .....                                     | 26 |

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| <a href="#"><u>Ilustración 39:selección de tipo de dato</u></a> .....         | 26 |
| <a href="#"><u>Ilustración 40:selección de la imagen</u></a> .....            | 27 |
| <a href="#"><u>Ilustración 41:Modulos</u></a> .....                           | 27 |
| <a href="#"><u>Ilustración 42:Configuracion finalizada</u></a> .....          | 28 |
| <a href="#"><u>Ilustración 45:Formulario de descarga FTK imager</u></a> ..... | 29 |
| <a href="#"><u>Ilustración 46:Instalador de FTK imager</u></a> .....          | 29 |
| <a href="#"><u>Ilustración 47:Instalador de FTK imager abierto</u></a> .....  | 30 |
| <a href="#"><u>Ilustración 49:Ruta de instalación</u></a> .....               | 30 |
| <a href="#"><u>Ilustración 50:comenzando con la instalación</u></a> .....     | 31 |
| <a href="#"><u>Ilustración 52:Icono FTK imager</u></a> .....                  | 31 |
| <a href="#"><u>Ilustración 53:FTK imager abierto</u></a> .....                | 31 |
| <a href="#"><u>Ilustración 54:Selección de la imagen</u></a> .....            | 32 |

## **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 análisis forense es de la marca **Kingston** con la capacidad de almacenamiento de **16GB** de color plateado de alineación metálica con la cual se trabajará en el trayecto del laboratorio en **kali linux**.

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



*Ilustración 1: Delantera Kingston*

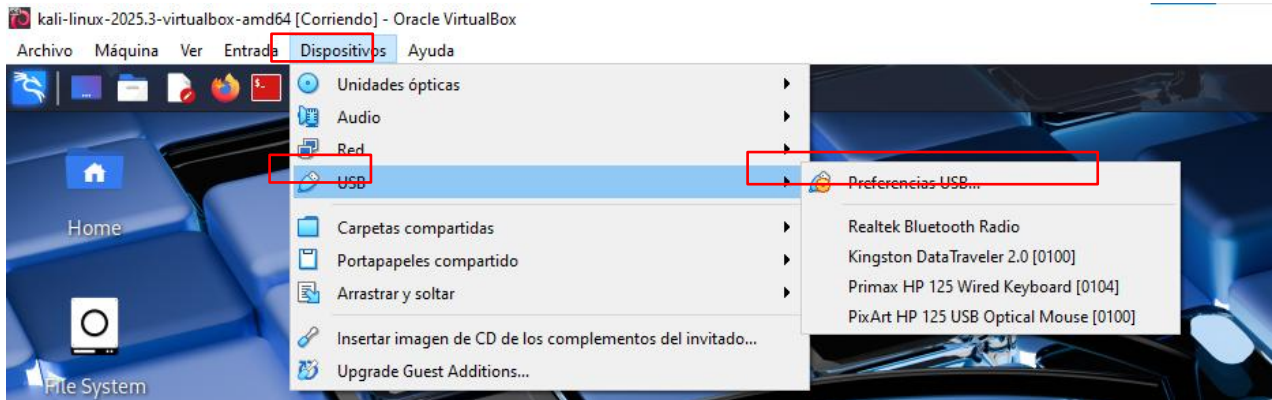
Esta es la parte trasera de la memoria **Kingston**:



*Ilustración 2: Trasera Kingston*

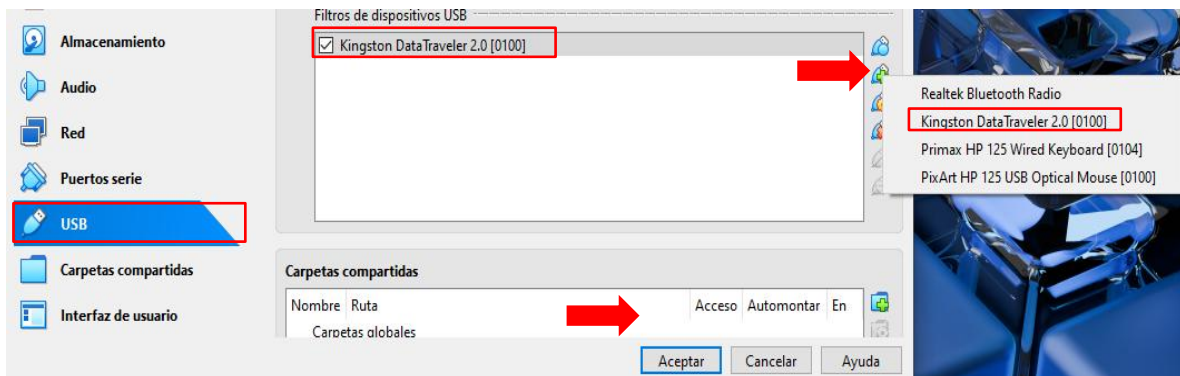
### 5.1 CONFIGURACIÓN DE LA MEMORIA USB EN KALI LINUX

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 análisis 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**.

```
(root@kali)-[/home/kali/Desktop]
# mkdir mariana

(root@kali)-[/home/kali/Desktop]
# 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.

```
(root@kali)-[/home/kali/Desktop/mariana]
# sha1sum /dev/sdb > /home/kali/Desktop/mariana/análisis_forense_hash.sha1
```

*Ilustración 8: Comando sha1sum*

Ahora para visualizar el hash generado ingresaremos el comando **cat** **análisis\_forense\_hash.sha**.

```
(root@kali)-[/home/kali/Desktop/mariana]
# cat análisis_forense_hash.sha1
ebb007786281e4f623204f95ed46dcc81824c48d /dev/sdb

(root@kali)-[/home/kali/Desktop/mariana]
#
```

*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.

```
(root@kali)-[/home/kali/Desktop/mariana]
# dd if=/dev/sdb of=/home/kali/Desktop/mariana/imagen_usb_forense.dd
30497664+0 records in
30497664+0 records out
15614803968 bytes (16 GB, 15 GiB) copied, 3924.1 s, 4.0 MB/s

(root@kali)-[/home/kali/Desktop/mariana]
#
```

*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 ( **ee627779cbbdbf57258d48545f099ef9f9bea9faa** ) puede variar según el tipo de almacenamiento y memoria.

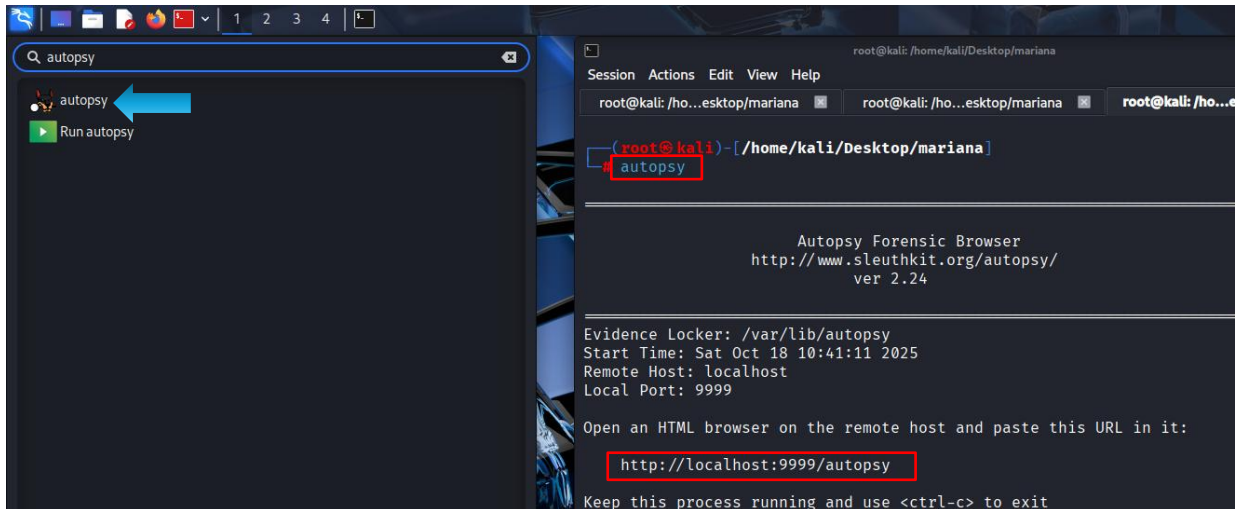
```
(root@kali)-[/home/kali/Desktop/mariana]
# ls -la
total 15248848
drwxrwxrwx 2 root root      4096 Oct 17 17:47 .
drwxr-xr-x 3 kali kali      4096 Oct 16 18:53 ..
-rw-rw-r-- 1 root root       51 Oct 17 16:13 analisis_forense_hash.sha1
-rw-rw-r-- 1 root root 15614803968 Oct 17 18:52 imagen_usb_forense.dd

(root@kali)-[/home/kali/Desktop/mariana]
# sha1sum imagen_usb_forense.dd
ee627779cbbdbf57258d48545f099ef9f9bea9faa  imagen_usb_forense.dd
```

*Ilustración 11: Comando sha1sum (hash de la imagen)*

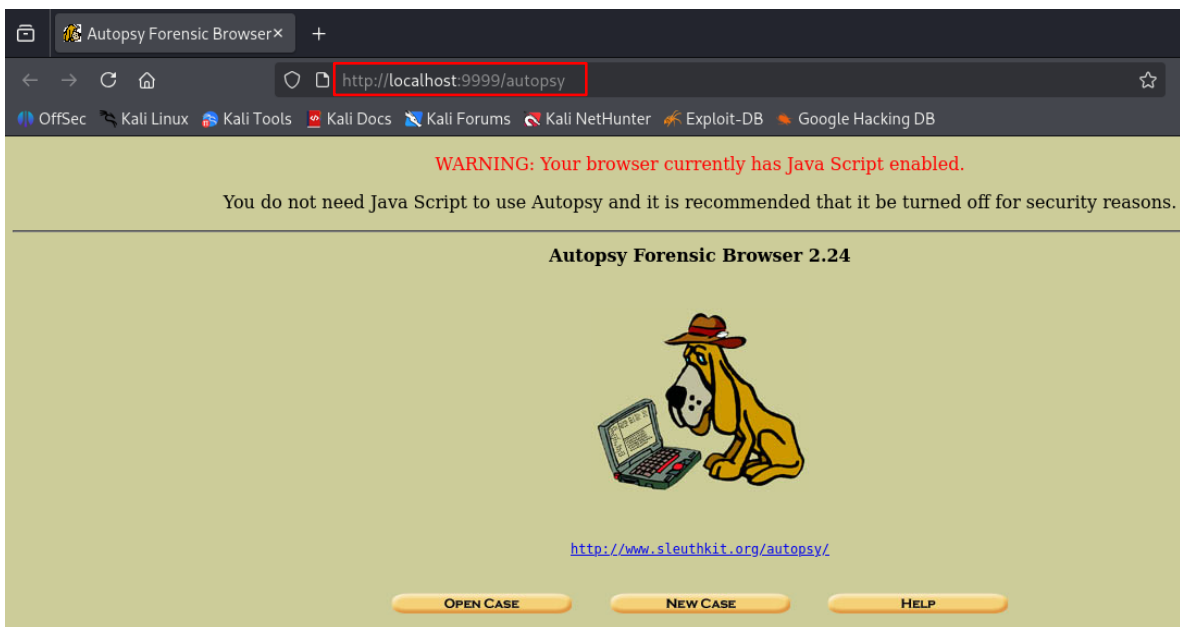
## 6. AUTOPSY EN KALI LINUX

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)*

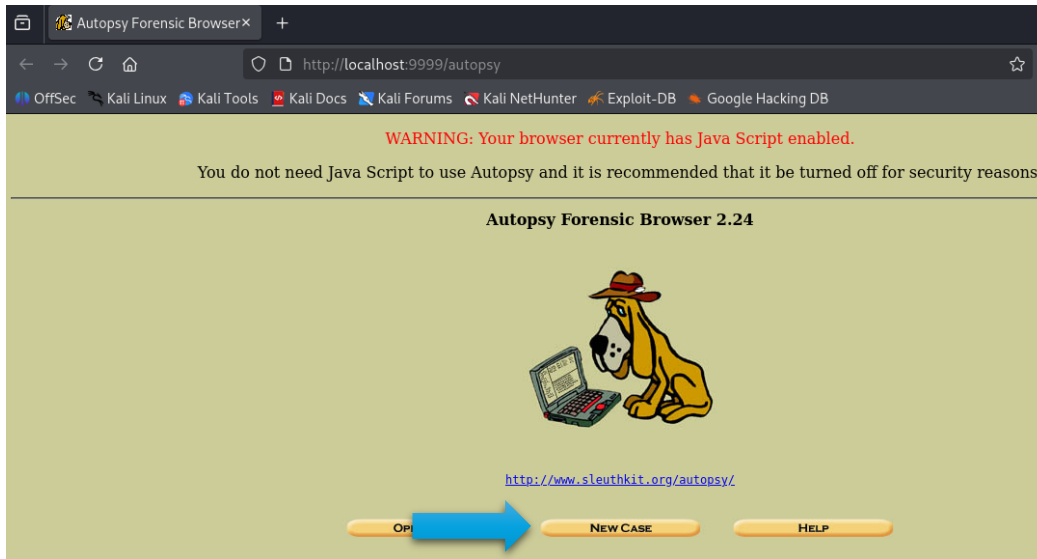
Con la url que se muestra ( **http://localhost:9999/autopsy** ) la ingresaremos en el navegador, dando como inicio la herramienta de **autopsy**



*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.

**Creating Case: primerCaso1**

Case directory (/var/lib/autopsy/primerCaso1/) created  
Configuration file (/var/lib/autopsy/primerCaso1/case.aut) created

We must now create a host for this case.

Please select your name from the list: Mariana\_sanchez ▼

**ADD HOST**

Mariana\_sanchez  
Mani\_pasas

*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**.

**ADD A NEW HOST**

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.  
laptop\_HP

2. **Description:** An optional one-line description or note about this computer.  
computador HP

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.  
0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

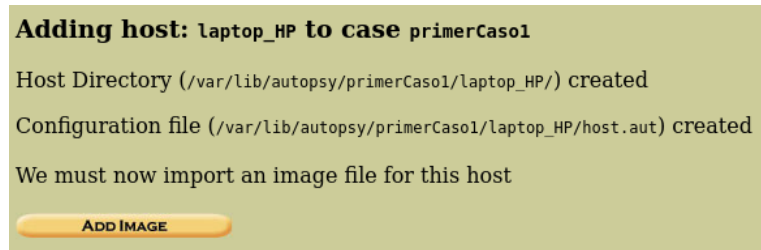
6. **Path of Ignore Hash Database:** An optional hash database of known good files.

**ADD HOST** **CANCEL** **HELP**

*Ilustración 17: New host*

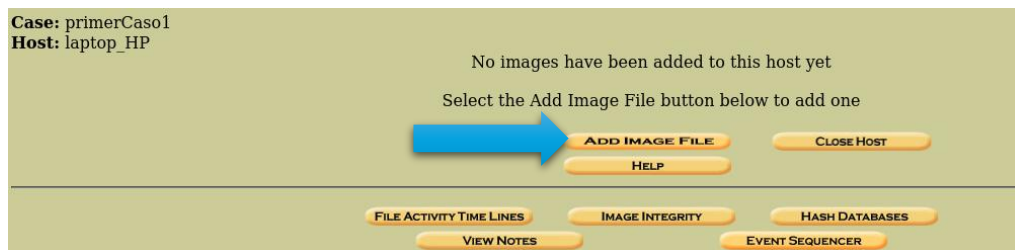
### 6.3 AGREGANDO LA IMAGEN DE LA USB

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 a 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**

**Image File Details**

**Local Name:** images/imagen\_usb\_forense.dd

**Data Integrity:** An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

☒ Ignore the hash value for this image.  
☐ Calculate the hash value for this image.  
☐ Add the following MD5 hash value for this image:  
  
☐ Verify hash after importing?

**File System Details**

Analysis of the image file shows the following partitions:

Partition 1 (Type: Win95 FAT32 (0x0c))  
 Sector Range: 8064 to 30497663  
 Mount Point: C: File System Type: fat32

ADD CANCEL HELP

*Ilustración 20: Detalles de la imagen*

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

For your reference, the mmls output was the following:

DOS Partition Table  
 Offset Sector: 0  
 Units are in 512-byte sectors

|      | Slot    | Start      | End        | Length     | Description        |
|------|---------|------------|------------|------------|--------------------|
| 002: | 000:000 | 0000008064 | 0030497663 | 0030489600 | Win95 FAT32 (0x0c) |

*Ilustración 21: Información técnica de la imagen*

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

Testing partitions  
 Linking image(s) into evidence locker  
 Image file added with ID img1

Disk image (type dos) added with ID vol1

Volume image (8064 to 30497663 - fat32 - C:) added with ID vol2

OK ADD IMAGE

*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**.

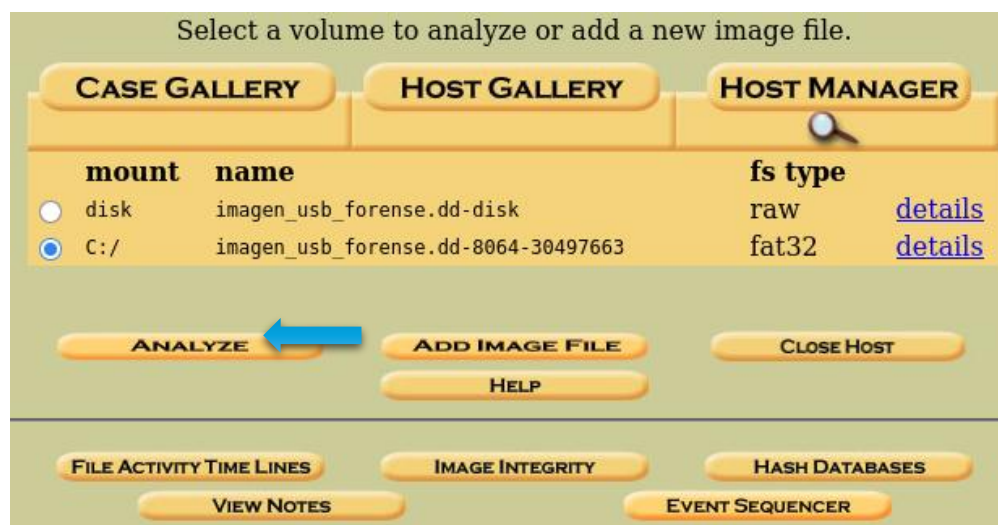


Ilustración 23: Selección del volumen

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.

| File Analysis                                                                       |                                                                                     |                               |                              |                              |                              |                              |                                                                                       |                                                                                       |                           |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------|
| Keyword Search                                                                      |                                                                                     |                               | File Type                    | Image Details                | Meta Data                    | Data Unit                    | Help                                                                                  | Close                                                                                 |                           |
|  |                                                                                     |                               |                              |                              |                              |                              |  |  |                           |
|                                                                                     |                                                                                     |                               |                              |                              |                              |                              |                                                                                       |                                                                                       |                           |
| Directory Seek                                                                      |                                                                                     |                               |                              |                              |                              |                              |                                                                                       |                                                                                       |                           |
| Enter the name of a directory that you want to view.<br>C:/                         | v / v                                                                               | \$FAT2                        | 00:00:00 (UTC)               | 00:00:00 (UTC)               | 00:00:00 (UTC)               | 7614464                      | 0                                                                                     | 0                                                                                     | <a href="#">487309317</a> |
|                                                                                     | v / v                                                                               | \$MBR                         | 00:00:00 (UTC)               | 00:00:00 (UTC)               | 00:00:00 (UTC)               | 512                          | 0                                                                                     | 0                                                                                     | <a href="#">487309315</a> |
|                                                                                     | d / d                                                                               | <a href="#">.Trash-1000/</a>  | 2025-10-16<br>23:16:42 (EDT) | 2025-10-16<br>00:00:00 (EDT) | 2025-10-16<br>23:16:43 (EDT) | 8192                         | 0                                                                                     | 0                                                                                     | <a href="#">16</a>        |
|                                                                                     |  | r / r                         | <a href="#">_guacate.jpg</a> | 2025-10-16<br>18:08:06 (EDT) | 2025-10-16<br>00:00:00 (EDT) | 2025-10-16<br>18:13:09 (EDT) | 194753                                                                                | 0                                                                                     | 0                         |
|  | r / r                                                                               | <a href="#">fresa.jfif</a>    | 2025-10-16<br>18:07:44 (EDT) | 2025-10-16<br>00:00:00 (EDT) | 2025-10-16<br>18:13:09 (EDT) | 13471                        | 0                                                                                     | 0                                                                                     | <a href="#">10</a>        |
|  | r / r                                                                               | <a href="#">fruta.jpg</a>     | 2025-10-16<br>18:07:16 (EDT) | 2025-10-16<br>00:00:00 (EDT) | 2025-10-16<br>18:13:09 (EDT) | 61561                        | 0                                                                                     | 0                                                                                     | <a href="#">7</a>         |
| File Name Search                                                                    | r / r                                                                               | KINGSTON (Volume Label Entry) | 2025-10-16<br>18:09:10 (EDT) | 00:00:00 (UTC)               | 00:00:00 (UTC)               | 0                            | 0                                                                                     | 0                                                                                     | <a href="#">3</a>         |
|                                                                                     | r / r                                                                               | <a href="#">kiwi.webp</a>     | 2025-10-16                   | 2025-10-16                   | 2025-10-16                   | 18112                        | 0                                                                                     | 0                                                                                     | <a href="#">14</a>        |
| Enter a Perl regular expression for the file names you want to find.                |                                                                                     |                               |                              |                              |                              |                              |                                                                                       |                                                                                       |                           |
|                                                                                     |                                                                                     |                               |                              |                              |                              |                              |                                                                                       |                                                                                       |                           |
|                                                                                     |                                                                                     |                               |                              |                              |                              |                              |                                                                                       |                                                                                       |                           |

Ilustración 24: Archivos de la imagen

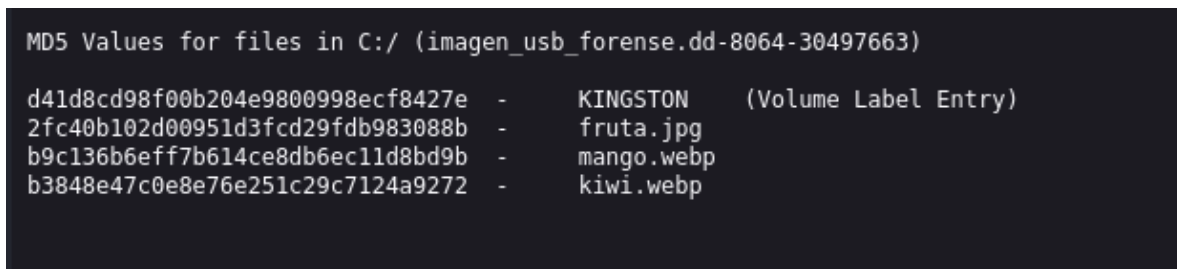
## 6.6 GENERANDO EL MD5 DE LA IMAGEN

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*

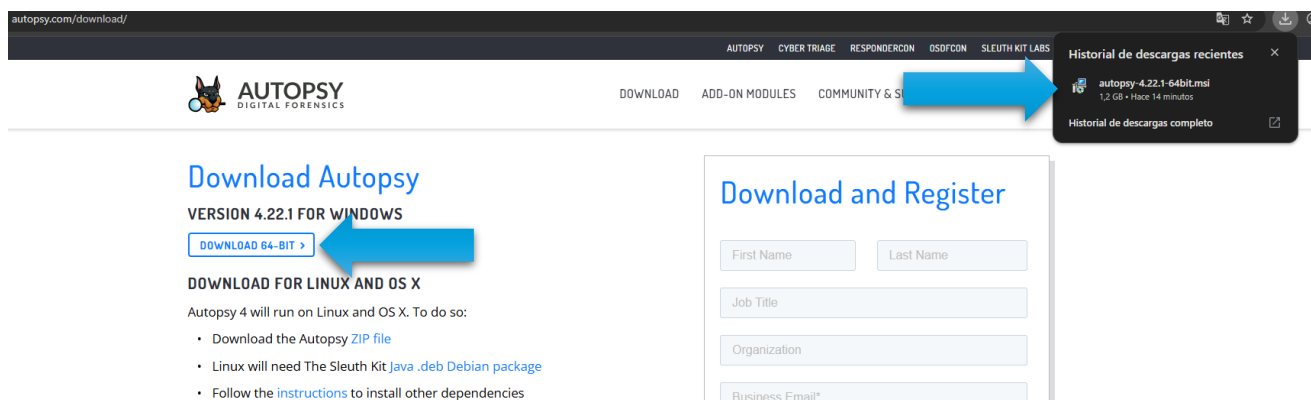
Este genera el MD5 de la imagen y de los archivos que están en la imagen, cada uno con el hash de cada archivo encontrado.



*Ilustración 26: MD5 generado*

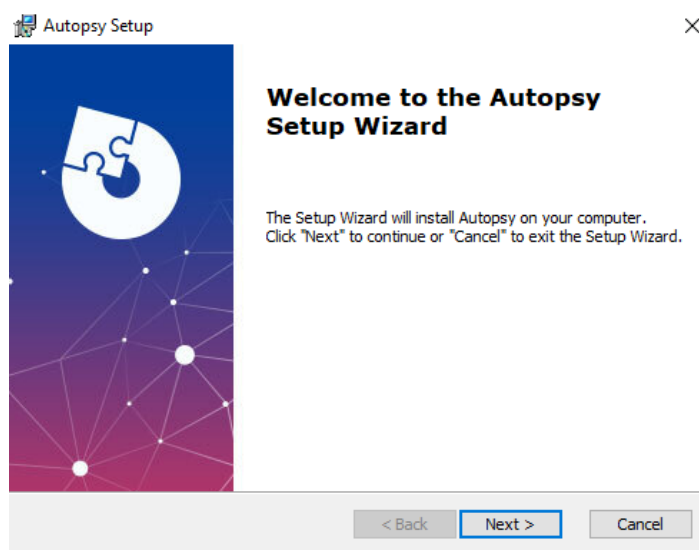
## 7. AUTOPSY EN WINDOWS

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*

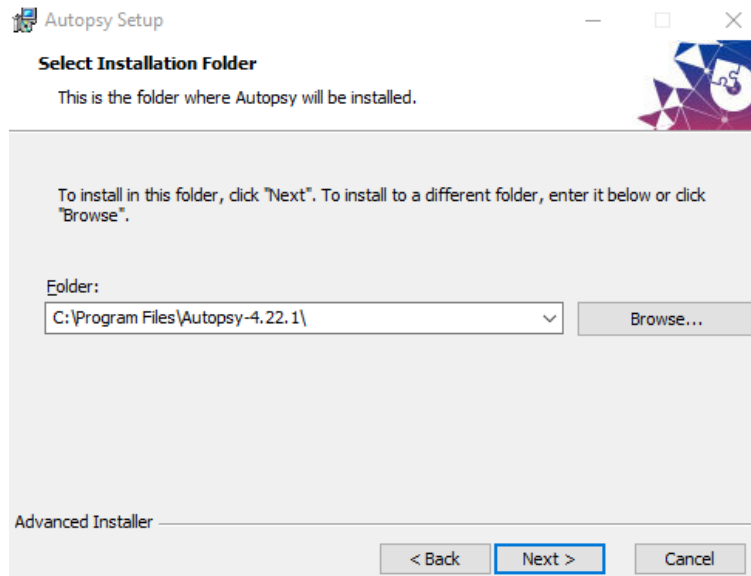
Ejecutaremos el instalador de autopsy que acabamos de descargar, este apartado muestra la ventana de bienvenida, donde vamos a pulsar en el botón de **Next**



*Ilustración 28: Ventana principal del instalador*

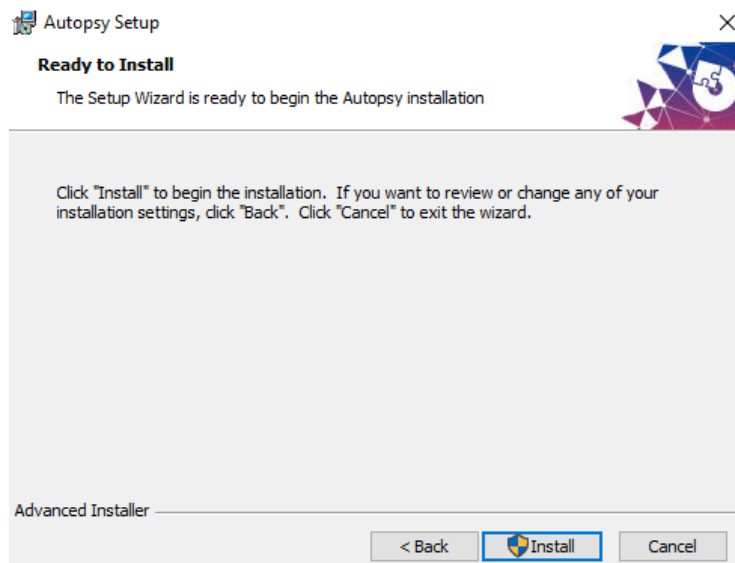
## 7.1 INSTALANDO AUTOPSY

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*

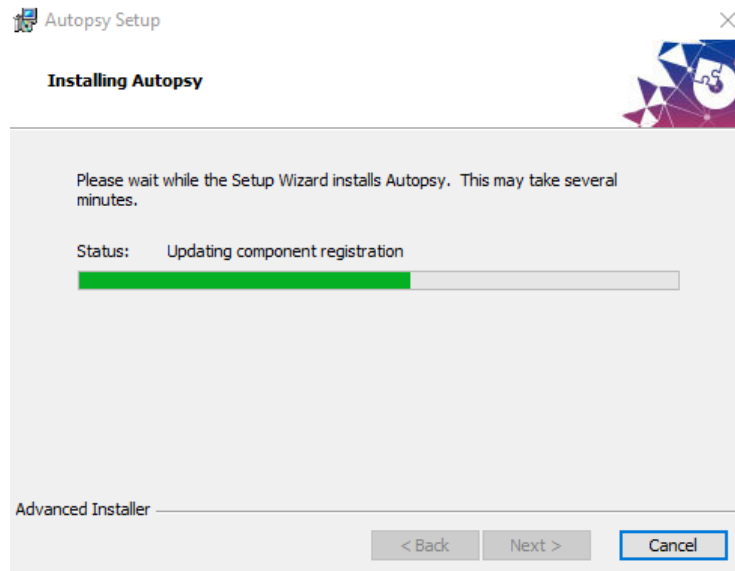
Finalmente tendremos el autopsy listo para su instalación, ahora vamos a pulsar en el **Install**.



*Ilustración 30: Instalación lista para comenzar*

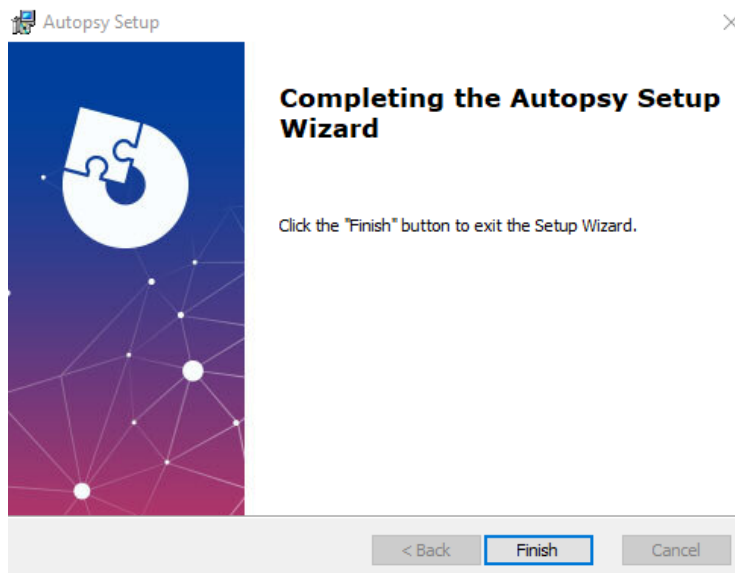
## 7.2 INSTALACIÓN COMPLETADA DE AUTOPSY

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



*Ilustración 31: Instalando autopsy*

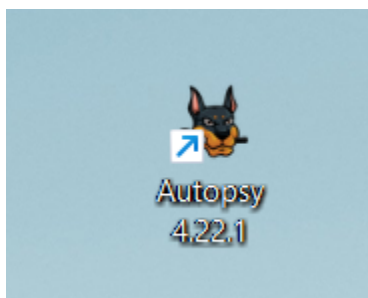
Finalmente, la instalación de autopsy se ha completado correctamente, pulsaremos en **Finish**, para cerrar el instalador después de completada la instalación.



*Ilustración 32: Instalación completada*

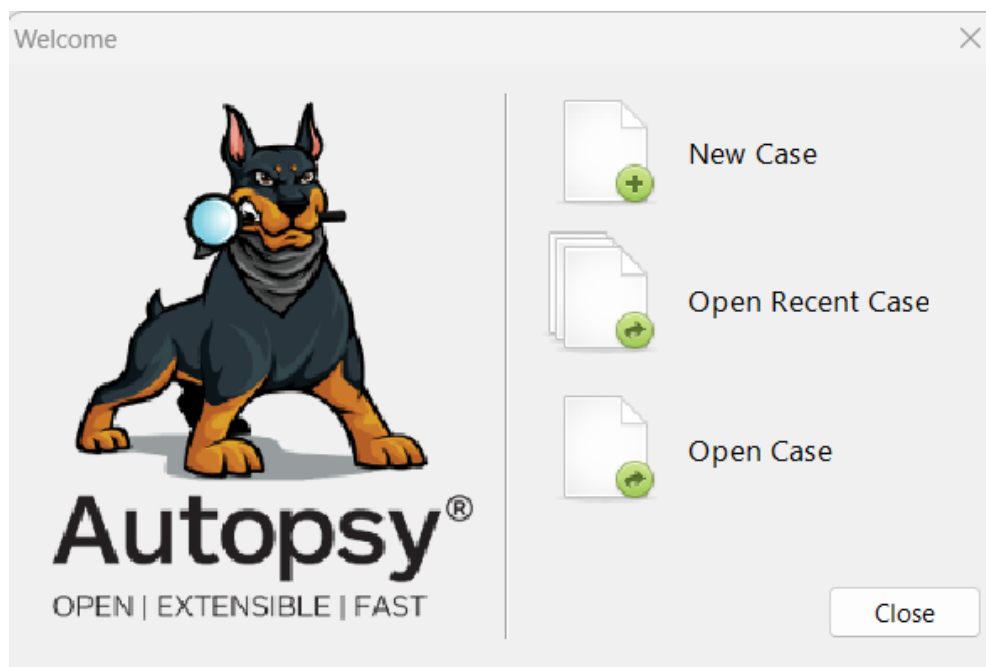
### 7.3 INICIANDO AUTOPSY DE WINDOWS

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.

**New Case Information**

**Steps**

1. **Case Information**
2. Optional Information

**Case Information**

Case Name:

Base Directory:

Case Type: ☒ Single-User ☐ Multi-User

Case data will be stored in the following directory:

< Back **Next >** Finish Cancel Help

*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**

**New Case Information**

**Steps**

1. Case Information
2. **Optional Information**

**Optional Information**

Case

Number:

Examiner

Name:

Phone:

Email:

Notes:

Organization

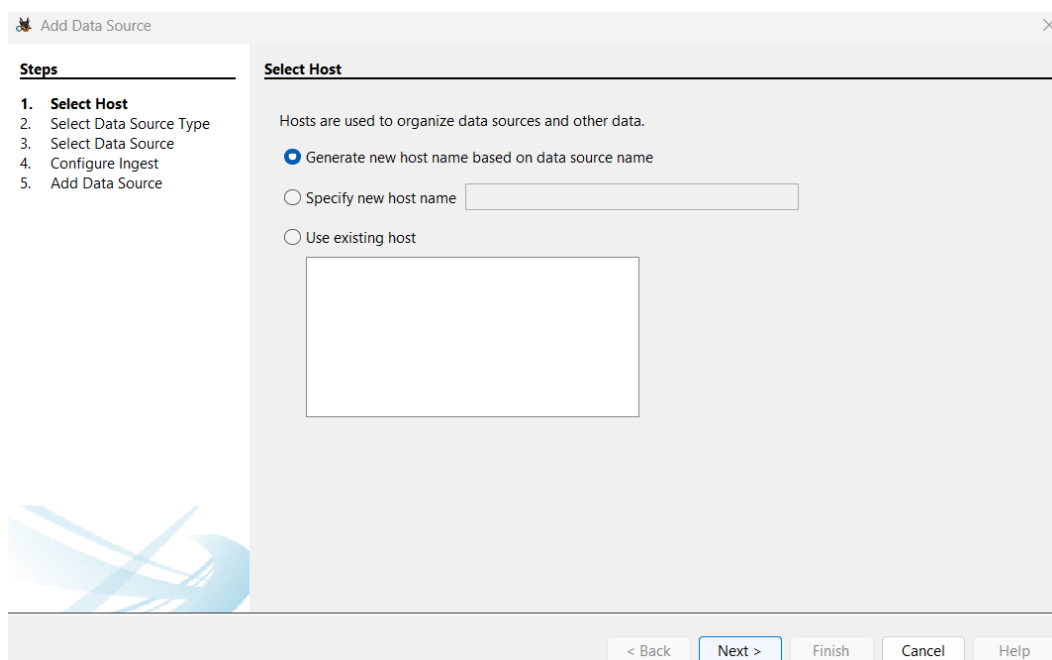
Organization analysis is being done for:

< Back Next > **Finish** Cancel Help

*Ilustración 36:Información del nuevo caso*

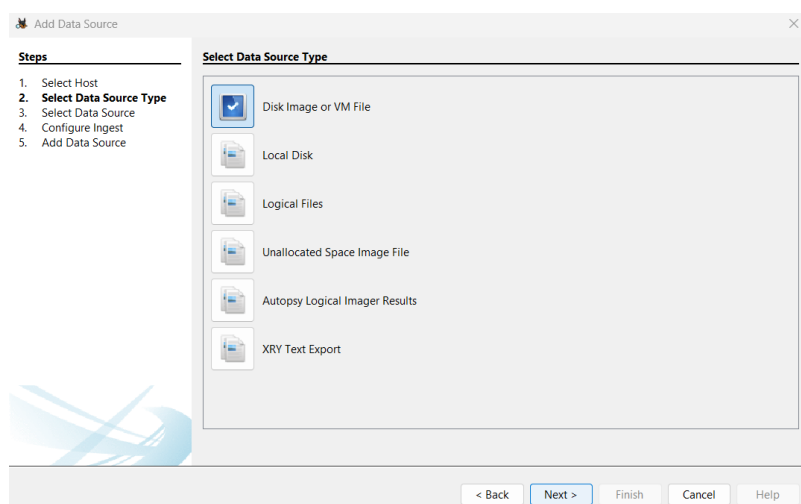
## 7.5 AGREGANDO EL HOST

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



*Ilustración 37:selección de host*

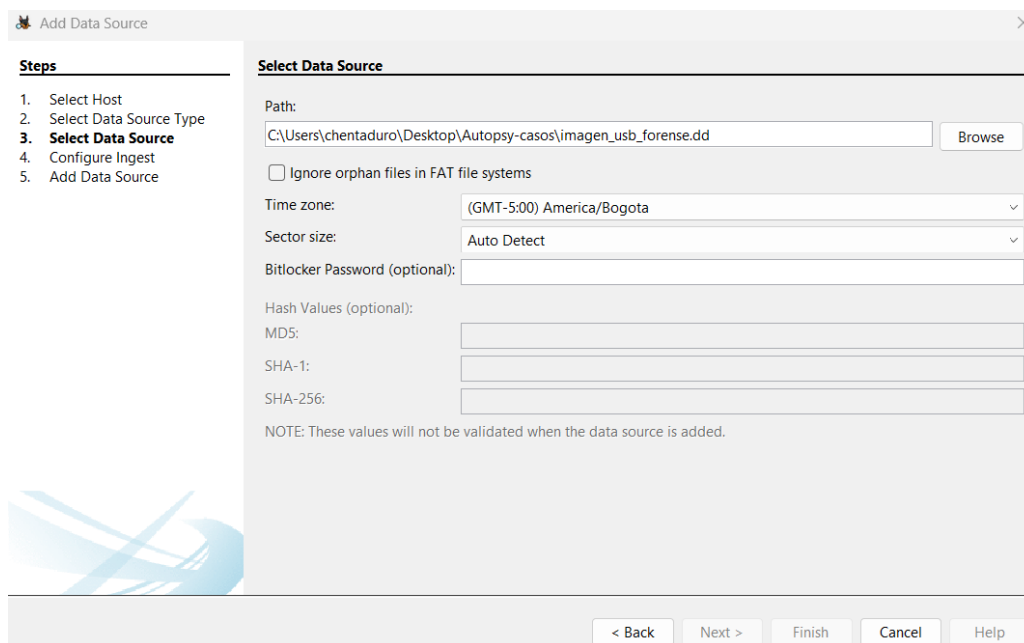
En la selección del tipo de dato con el vamos a trabajar, en este caso, con una memoria usb **Kingston** de **16GB** de almacenamiento vamos a seleccionar, **Disk Image or VM File**, pulsaremos en **Next**.



*Ilustración 38:selección de tipo de dato*

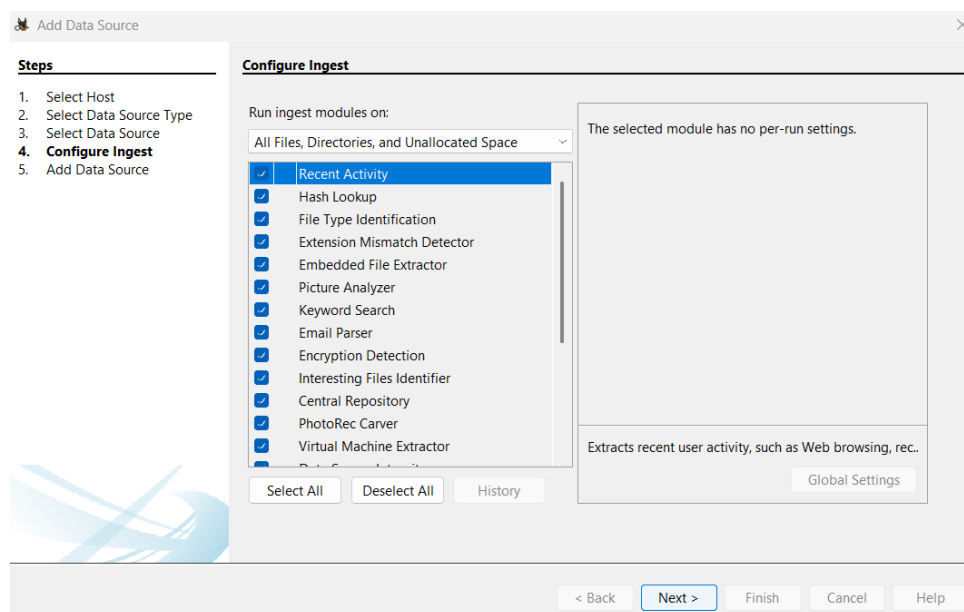
## 7.6 SELECCIÓN DE IMAGEN Y MÓDULOS

En 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*

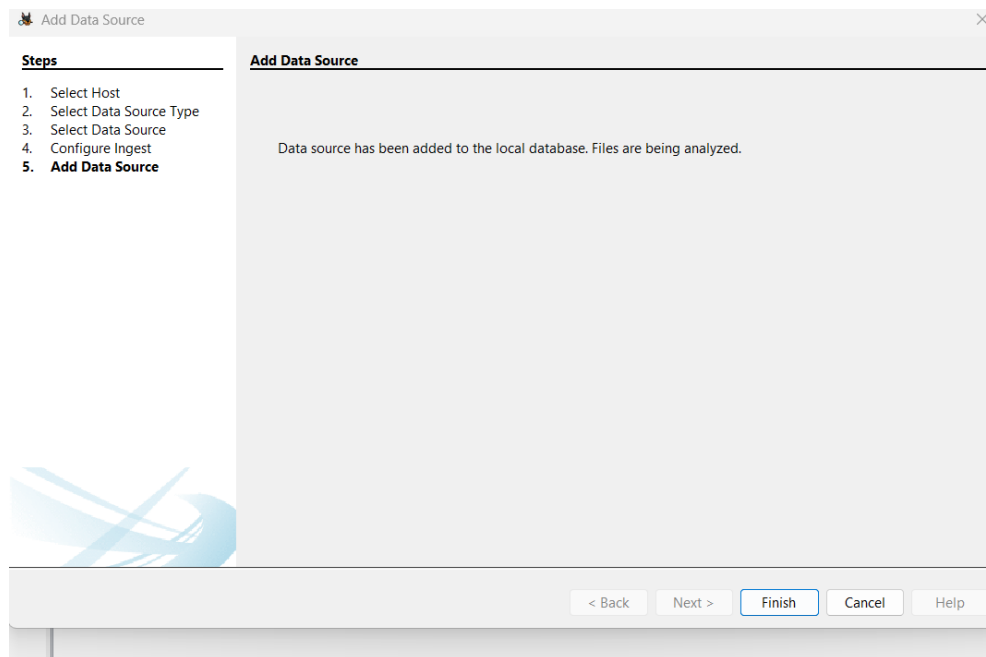
Ahora dejamos seleccionados los módulos con los cuales autopsy necesitará para trabajar, seguidamente solo pulsaremos en **Next**.



*Ilustración 40: Módulos*

## 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**.



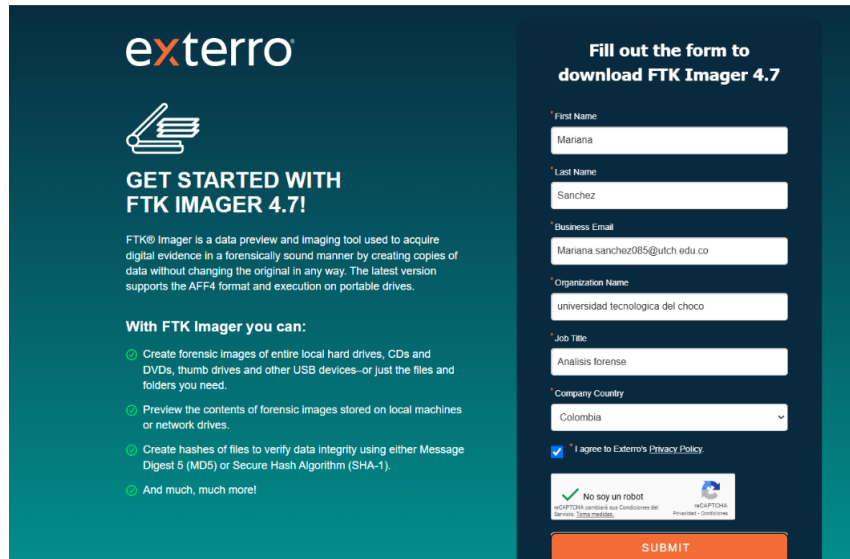
*Ilustración 41: Configuración finalizada*

## 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.



**exterro**

**GET STARTED WITH FTK IMAGER 4.7!**

FTK® Imager is a data preview and imaging tool used to acquire digital evidence in a forensically sound manner by creating copies of data without changing the original in any way. The latest version supports the AFF4 format and execution on portable drives.

**With FTK Imager you can:**

- ✓ Create forensic images of entire local hard drives, CDs and DVDs, thumb drives and other USB devices—or just the files and folders you need.
- ✓ Preview the contents of forensic images stored on local machines or network drives.
- ✓ Create hashes of files to verify data integrity using either Message Digest 5 (MD5) or Secure Hash Algorithm (SHA-1).
- ✓ And much, much more!

**Fill out the form to download FTK Imager 4.7**

\*First Name  
Mariana

\*Last Name  
Sanchez

\*Business Email  
Mariana.sanchez085@utch.edu.co

\*Organization Name  
universidad tecnologica del chocó

\*Job Title  
Analisis forense

\*Company Country  
Colombia

☒ I agree to Exterro's Privacy Policy.

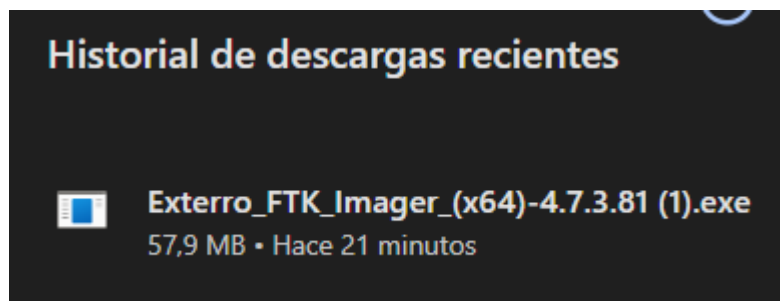
☒ No soy un robot

**SUBMIT**

*Ilustración 42:Formulario de descarga FTK imager*

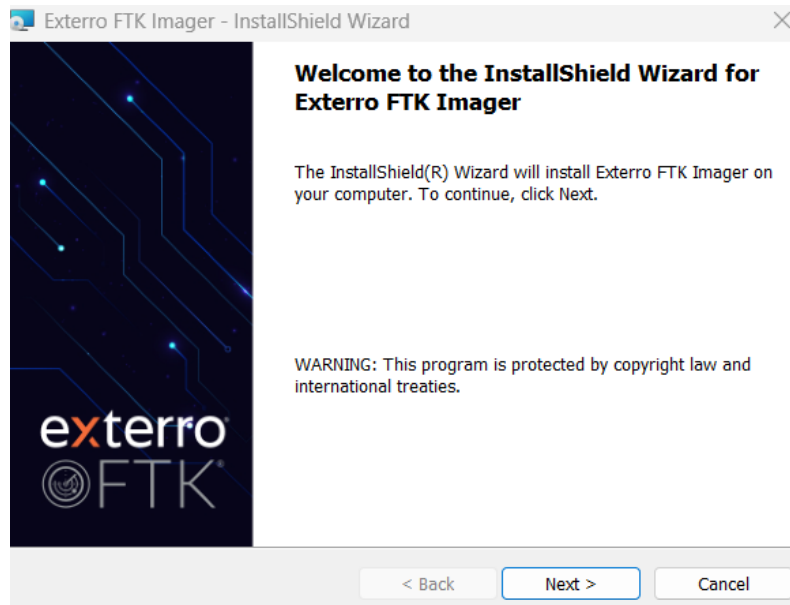
## 7.9 INSTALACIÓN DE FTK IMAGER

Este instalador de **FTK imager** quedara descargado **Exterro\_FTK\_Imager\_(x64)-4.7.3.81**.



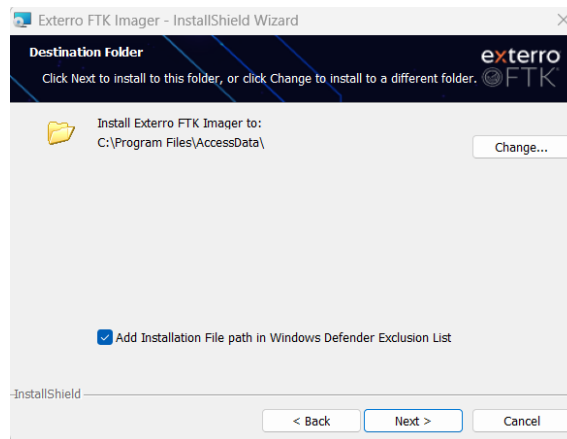
*Ilustración 43:Instalador de FTK imager*

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*

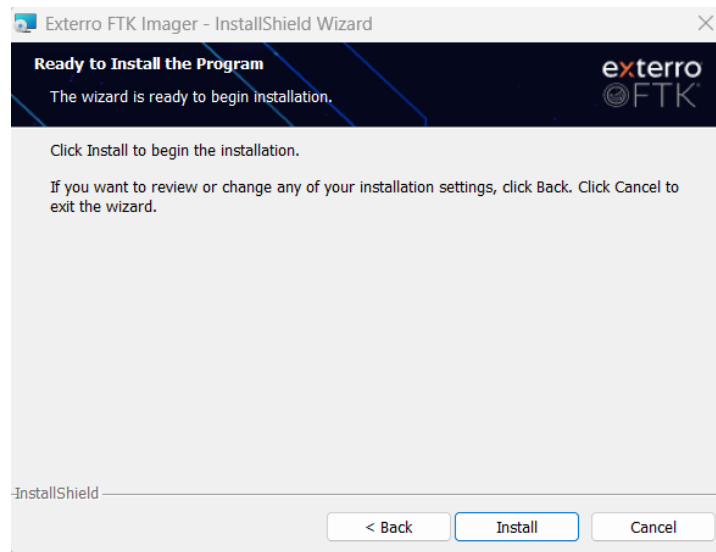
Aquí tendremos que seleccionar donde queremos que se instale el **FTK imager** , es recomendable dejar la ruta predeterminada que esta seleccionada por defecto, ahora pulsaremos en **Next**.



*Ilustración 45: Ruta de instalación*

## 7.10 INSTALACIÓN FTK IMAGER PREPARADA

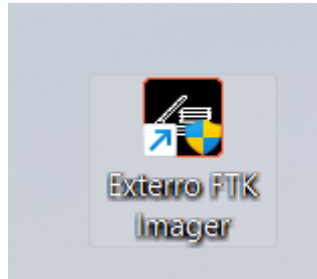
El paquete de instalación estará preparada para dar inicio con la instalación de los componentes, pulsaremos en **Install**.



*Ilustración 46:finalizando con la instalación*

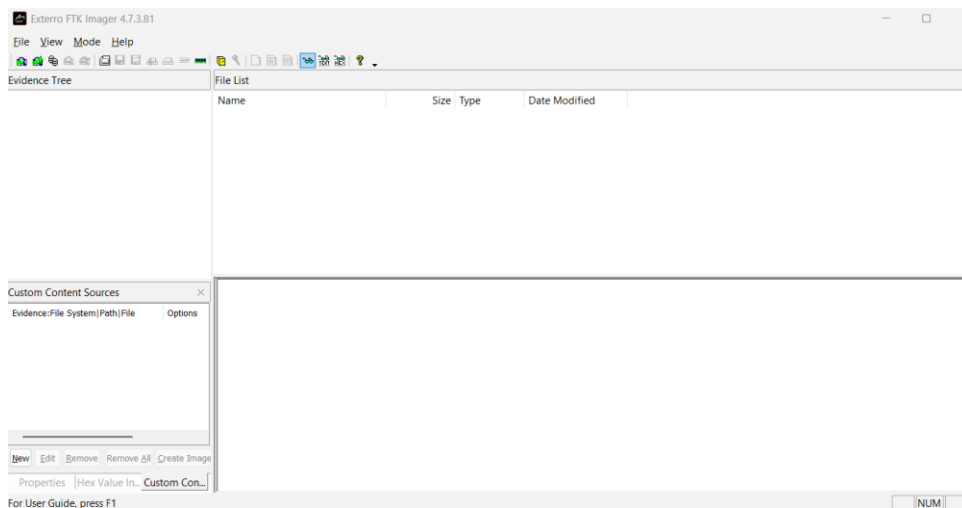
## 7.11 INICIANDO FTK IMAGER

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



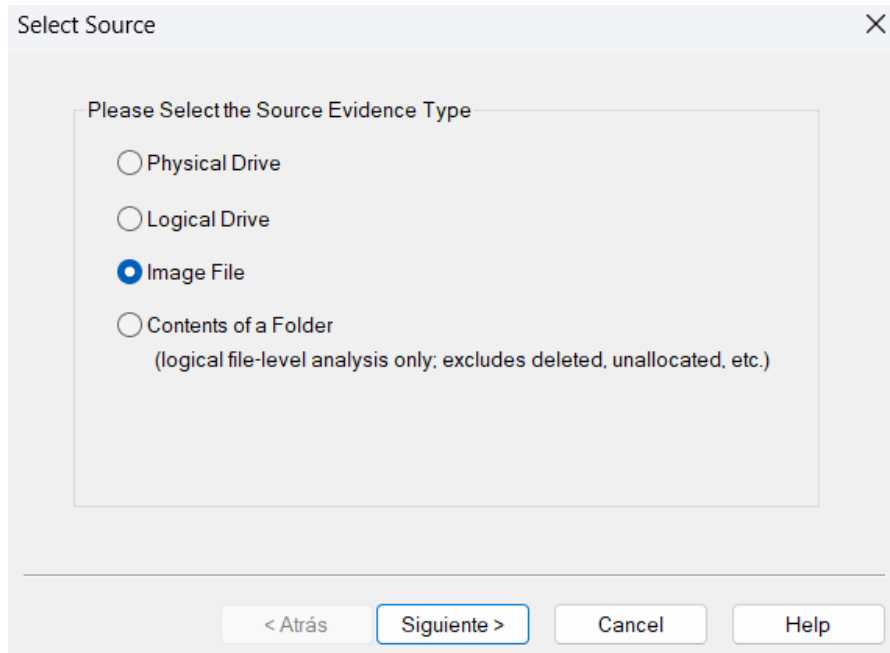
*Ilustración 47:Icono FTK imager*

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

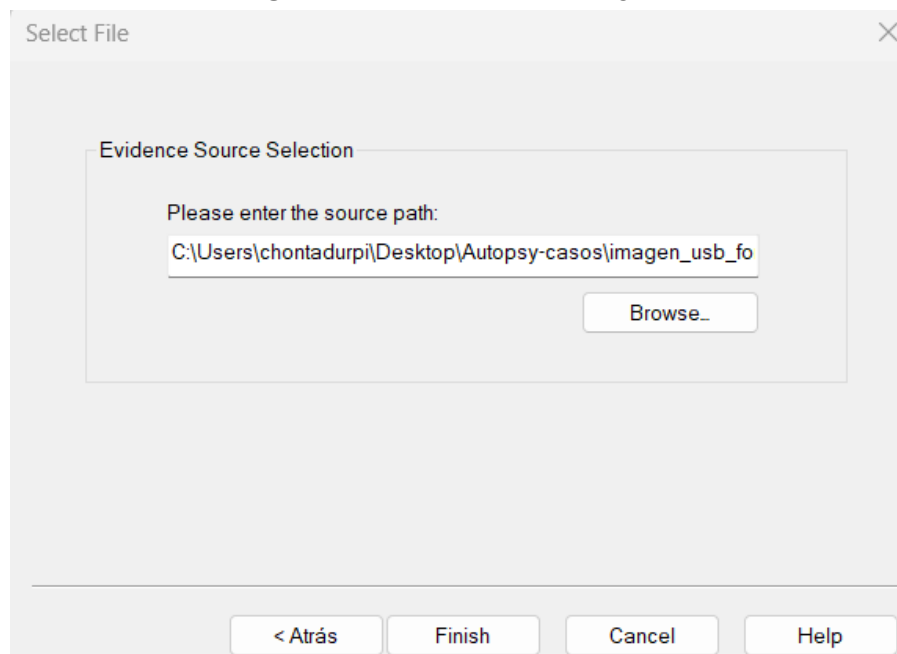


## 7.12 SELECCIÓN DE LA IMAGEN FTK IMAGER

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 usb en este caso usaremos la misma que generamos en Kali Linux que se llama **imagen\_usb\_forense.dd** , luego pulsamos en **Finish**.



*Ilustración 49:Seleccin 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.