Informe de Auditoría Forense en Autopsy y FTK Imager

Universidad Tecnológica del Chocó Diego Luis Córdoba

Estudiantes:

Franklin Mosquera Blandón

Profesor:

ING Rafael Sandoval Morales

Asignatura:

Seguridad y Auditoria en Redes

Facultad de Ingeniería

Programa:

Ingeniería de Telecomunicación e Informática

Fecha:

16 de Octubre del 2025

Tabla de Contenido

Tabla de Ilustraciones

1 Introducción

El presente informe describe el proceso completo de una auditoría forense digital realizada sobre un dispositivo de almacenamiento USB, utilizando las herramientas Autopsy y FTK Imager en diferentes entornos operativos.

El propósito principal del ejercicio fue aplicar los procedimientos fundamentales de la informática forense para la obtención, preservación, análisis y verificación de evidencias digitales, asegurando su integridad mediante la comparación de hashes generados antes y después del análisis.

Durante el desarrollo, se emplearon plataformas tanto en Kali Linux como en Windows, lo que permitió comparar la funcionalidad de las herramientas forenses en distintos sistemas operativos y comprobar la coincidencia de los resultados obtenidos. Este trabajo forma parte del aprendizaje práctico en el curso de Seguridad y Auditoría en Redes, y busca fortalecer las competencias técnicas en la aplicación de metodologías forenses y en el manejo ético de evidencias digitales.

2 Objetivos

2.1 Objetivo General

Realizar una auditoría forense a un dispositivo USB empleando las herramientas Autopsy y FTK Imager en entornos Linux y Windows, con el fin de verificar la integridad de los datos mediante la generación y comparación de hashes y evidenciar la capacidad de estas herramientas para la identificación y recuperación de información.

2.2 Objetivo Específico

1) Generar una imagen forense de la memoria USB y crear los respectivos hashes para garantizar la integridad de la evidencia digital.
2) Ejecutar el análisis forense con Autopsy en Kali Linux y documentar los resultados obtenidos.
3) Repetir el análisis con Autopsy en Windows, utilizando la misma imagen forense, para comparar los resultados y validar la coincidencia de los hashes.
4) Realizar un tercer análisis con FTK Imager en Windows, verificando nuevamente la integridad de los archivos y los hashes generados.

3 Descripciones Generales

El siguiente informe, muestra el análisis forense realizado a un USB micro HC RNL Modelo AS-98. El análisis consistía en mostrar la información de esta USB y observar si se había modificado, eliminado algún archivo de esta USB.

La USB analizada era color amarillo con blanco, de la empresa Kinston y con 4GB de almacenamiento. En la imagen siguiente se puede observar la USB a la cual se le realizo este análisis.

Ilustración 1 USB analizada

Para realizar este análisis, primeramente, en Kali Linux como máquina virtual, se creó un hash a la USB y luego a esa USB se le creo una imagen y por último a la imagen se le creo un nuevo hash y este debía coincidir con el primer hash y así verificar que la USB no había recibido alguna modificación.

Una vez que se verificara que ambos hashes coincidían, se realizó el análisis forense en Kali Linux con la herramienta Autopsy, luego con la misma imagen que se generó en Kali Linux, se debía realizar el mismo análisis con la herramienta Autopsy, pero en Windows y por último realizar este mismo análisis con la herramienta FTK Imager en Windows y en cada uno de los análisis el resultado de los hashes de todos los archivos debía ser el mismo.

4 Capítulo 1 Auditoria Forense con Autopsy en Kali Linux.

El primer capítulo del informe muestra como fue el análisis de la USB en Kali Linux.

Para ello, primero con el comando fdisk -l, se verifico que la maquina estuviera leyendo la USB una vez conectada y efectivamente la USB la maquina estaba leyendo la USB, y el nombre de esta USB era Disk /dev/sdb con 3,75 GB de almacenamiento.

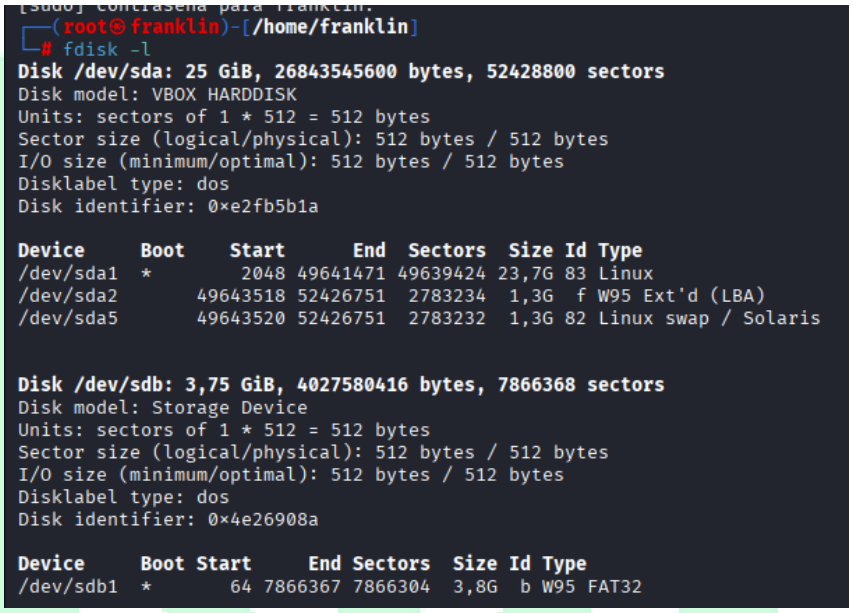


Ilustración 2 Auditoria Forense con Autopsy en Kali Linux parte - 1

Una vez que verifique que la USB se estaba leyendo correctamente, con el comando sha1sum /dev/sdb (nombre de la USB) > /home/franklin/Escritorio/hash_forense.sha1 (directorio y nombre de donde se iba a guardar el hash) cree el hash de la USB.

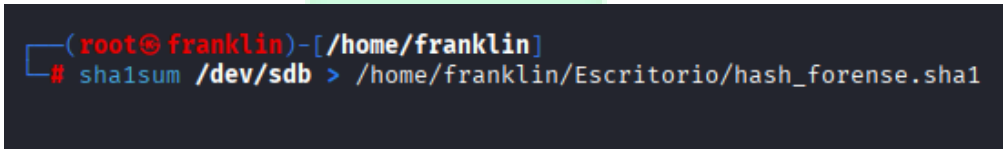


Ilustración 3 Auditoria Forense con Autopsy en Kali Linux parte - 2

Y el hash generado es el que se observa en la siguiente imagen.

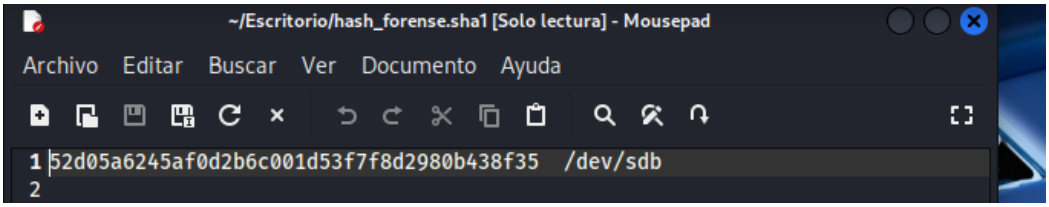


Ilustración 4 Auditoria Forense con Autopsy en Kali Linux parte - 3

Después de crear el hash de la USB, con el comando dd if=/dev/sdb of=/home/franklin/Escritorio7imagen_usb_forense.dd conv=noerror,sync cree la imagen de la USB y luego con el comando sha1sum /home/franklin/Escritorio7imagen_usb_forense.dd cree el hash de la imagen de USB, y así comprobé que la USB no había sido modificada porque tenia el mismo hash, tanto la imagen como la USB.

```
┌──(root㉿franklin)-[/home/franklin]
└─# dd if=/dev/sdb of=/home/franklin/Escritorio/imagen_usb_forense.dd conv=noerror,sync
7866368+0 records in
7866368+0 records out
4027580416 bytes (4,0 GB, 3,8 GiB) copied, 625,505 s, 6,4 MB/s

┌──(root㉿franklin)-[/home/franklin]
└─# sha1sum /home/franklin/Escritorio/imagen_usb_forense.dd
52d05a6245af0d2b6c001d53f7f8d2980b438f35  /home/franklin/Escritorio/imagen_usb_forense.dd

┌──(root㉿franklin)-[/home/franklin]
└─#
```

Ilustración 5 Auditoria Forense con Autopsy en Kali Linux parte - 4

Cuando comprobé que la USB no había sido modificada, empecé a realizar el análisis de esta misma.

Primero abrir la herramienta Autopsy luego de buscarlas en las herramientas de Kali Linux.

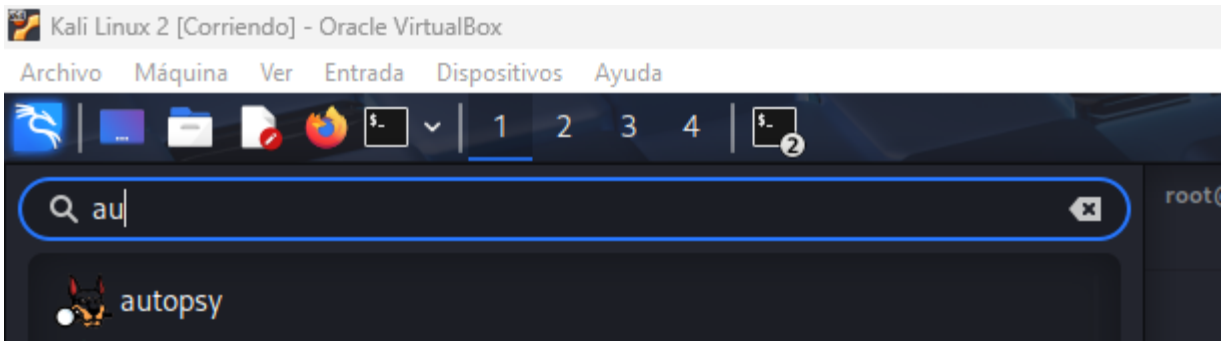


Ilustración 6 Auditoria Forense con Autopsy en Kali Linux parte - 5

Al abrir la herramienta, este mostro una nueva terminar mostrando información sobre la herramienta.

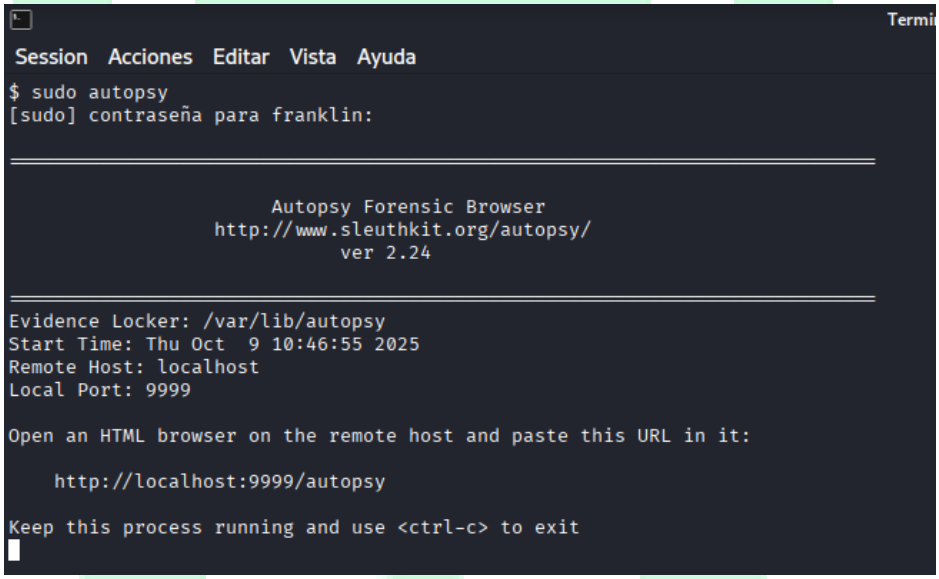


Ilustración 7 Auditoria Forense con Autopsy en Kali Linux parte - 6

Dentro de toda esa información, seleccione el link que había allí dentro acerca de Autopsy.

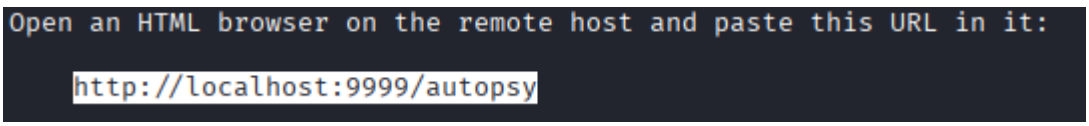


Ilustración 8 Auditoria Forense con Autopsy en Kali Linux parte - 7

Una vez seleccionado el enlace, oprimí el botón izquierdo del teclado y luego oprimí la opción abrir el enlace.

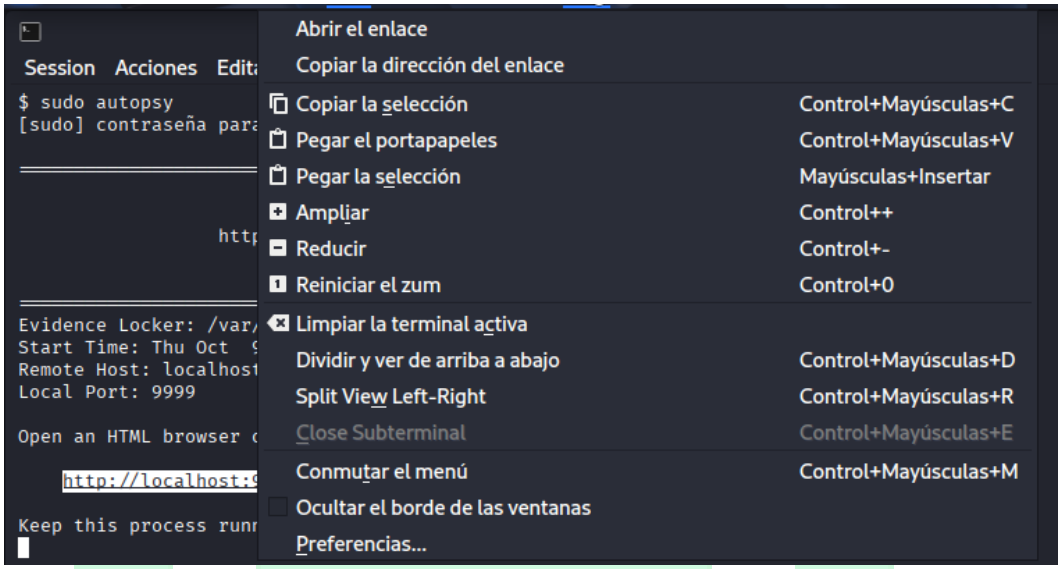


Ilustración 9 Auditoria Forense con Autopsy en Kali Linux parte - 8

Y al abrir ese enlace navegue a la pagina de Autopsy. Allí tenía la opción de abrir un caso o de crear uno, pero como era el primer caso de análisis que iba a realizar seleccione la opción NewCase o crear nuevo caso.

Ilustración 10 Auditoria Forense con Autopsy en Kali Linux parte - 9

Al seleccionar esa opción, el aplicativo me mostro un formulario donde debía poner el nombre del caso, la descripción y los nombres o el nombre del investigador. En el nombre puse MiPrimerCaso, en la descripción pude Análisis Forense USB clase y en los investigadores, puede mi nombre Franklin_Mosquera y por último oprimir el botón NewCase.

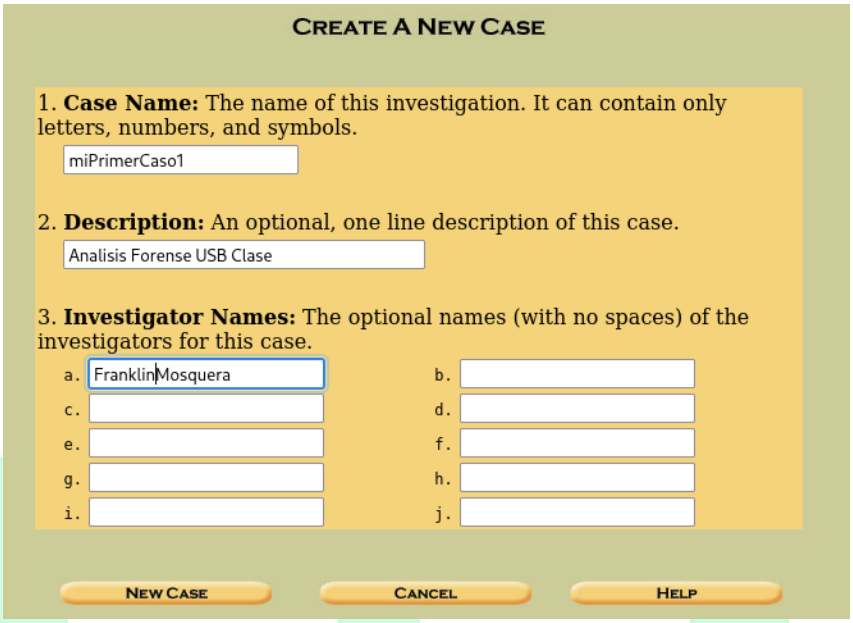


Ilustración 11 Auditoria Forense con Autopsy en Kali Linux parte - 10

Luego, la herramienta me mostro una ventana donde estaba el directorio del caso y el archivo de configuración, una vez observé esa información oprimí el botón ADD HOST o agregar un nuevo host.

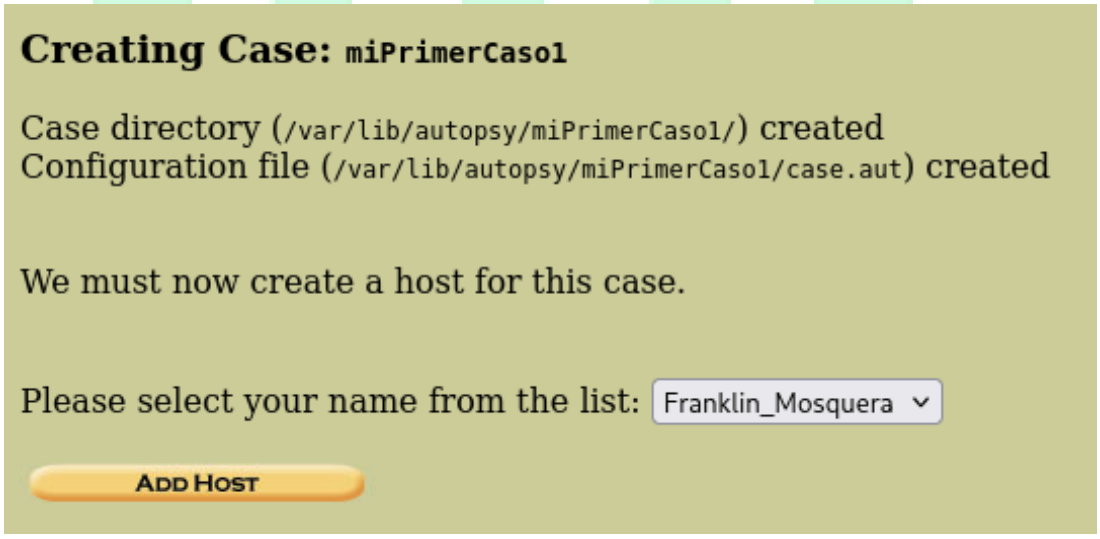


Ilustración 12 Auditoria Forense con Autopsy en Kali Linux parte - 11

Al nombre del host, se puse MVKaliPITI1 y en la descripción Portatil_HP.

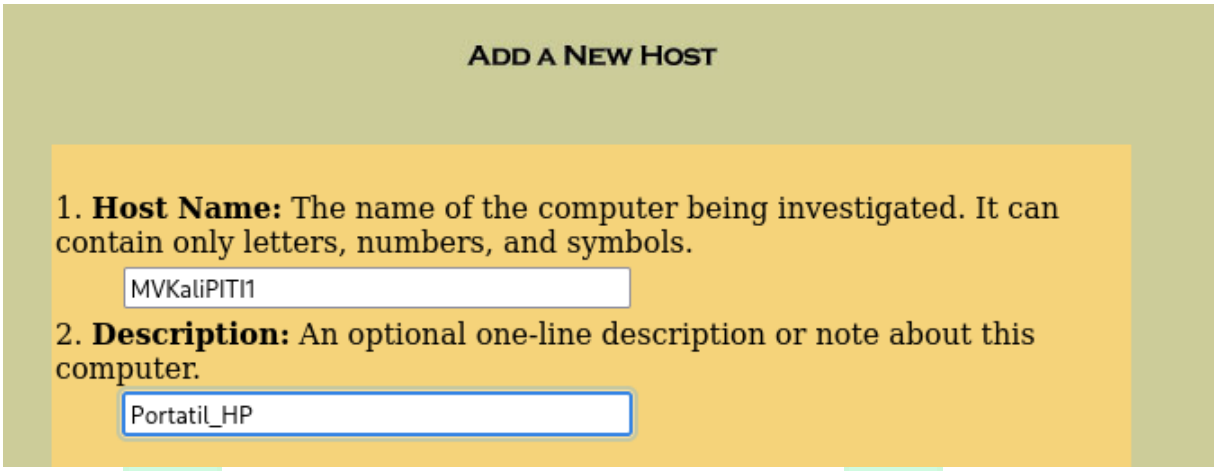


Ilustración 13 Auditoria Forense con Autopsy en Kali Linux parte - 12

Y en las otras opciones como en la zona horara no digite ninguna información y despues oprimí el botón ADDHOST.

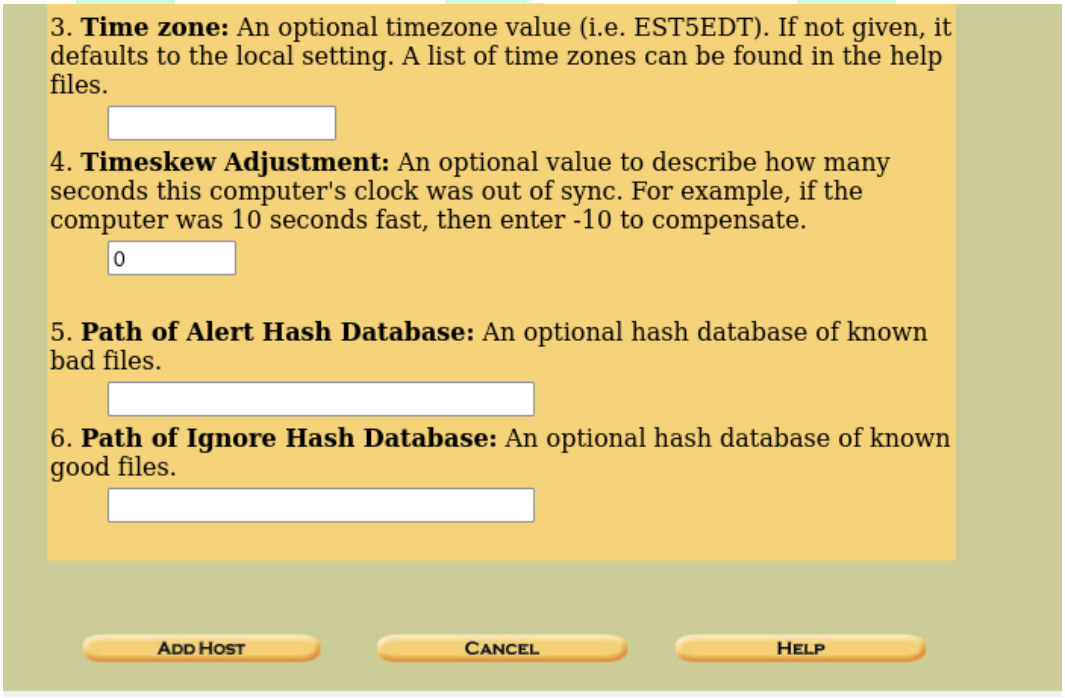


Ilustración 14 Auditoria Forense con Autopsy en Kali Linux parte - 13

Cuando agregué el host la herramienta me mostro en una nueva ventana el directorio del host y el archivo de configuración, al terminar de ver esta información, procedí a agregar la imagen oprimiendo el botón ADD IMAGEN.

Ilustración 15 Auditoria Forense con Autopsy en Kali Linux parte - 14

Al oprimir ese botón, Autopsy me mostró varias acciones que podía realizar, yo decidí dar clic en el botón ADD IMAGUE FILE, para elegir la ruta de la imagen a la cual se le iba a realizar el análisis.

Ilustración 16 Auditoria Forense con Autopsy en Kali Linux parte - 15

Efectivamente, elegí la ruta de la imagen de la USB.

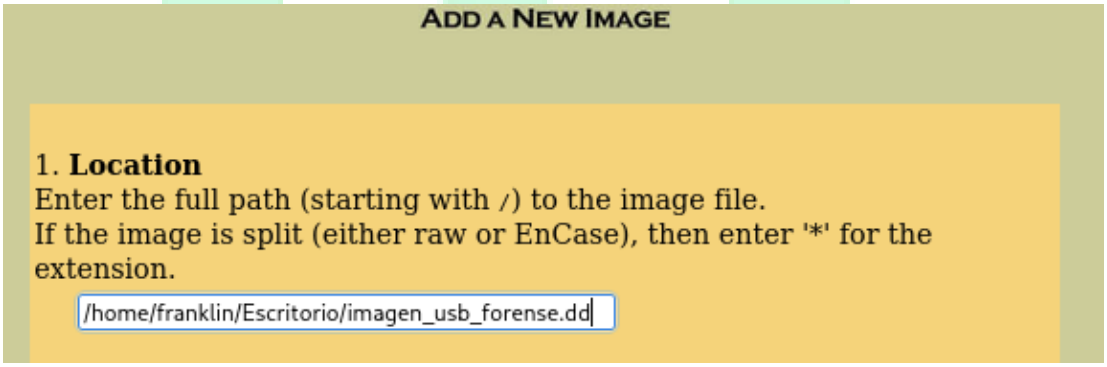


Ilustración 17 Auditoria Forense con Autopsy en Kali Linux parte - 16

Además, elegí el tipo de imagen es decir Disk o disco y también el método de importación el cual fue Symlink y luego oprimí el botón next.

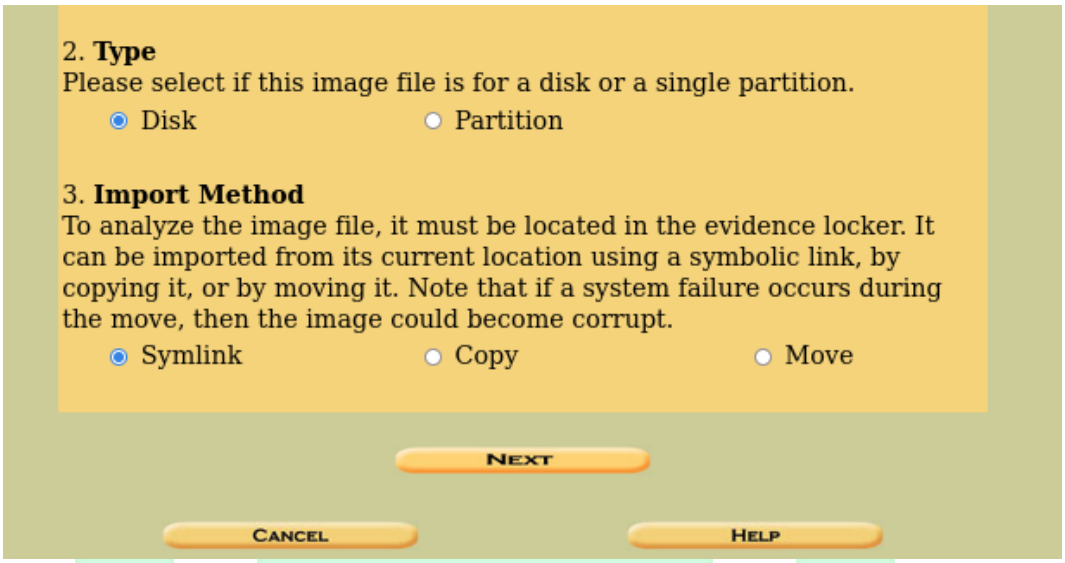


Ilustración 18 Auditoria Forense con Autopsy en Kali Linux parte - 17

Al dar clic en next, la herramienta me mostro la información de la imagen como la descripción donde esta USB tenia como sistema de archivo FAT32.

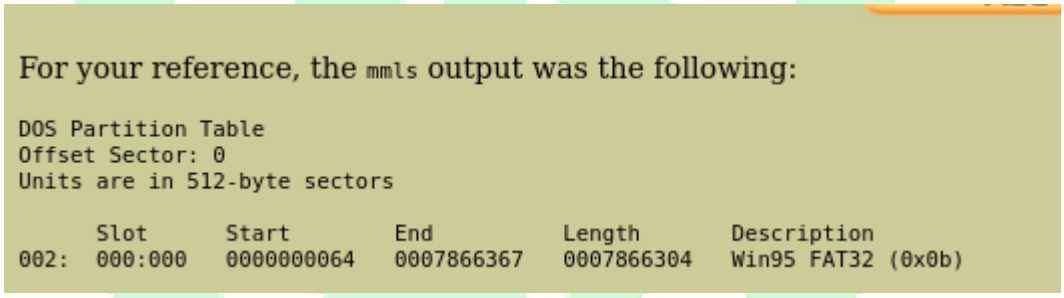


Ilustración 19 Auditoria Forense con Autopsy en Kali Linux parte - 18

Además, en esa ventana pude observar detalles de la imagen como el nombre local, me pedía que, si quería agregar, calcular o ignorar un hash con MD5 y seleccione la opción de ignorar o Ignore.

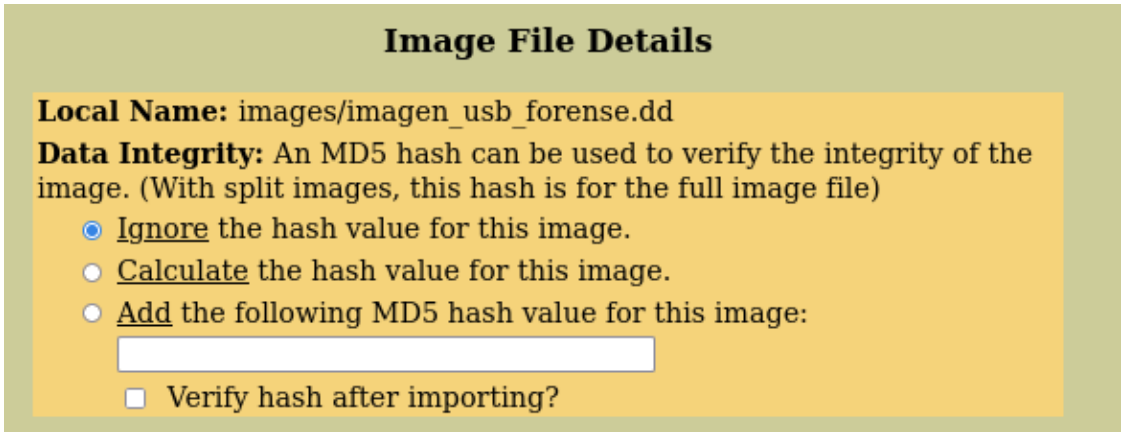


Ilustración 20 Auditoria Forense con Autopsy en Kali Linux parte - 19

Además, debía elegir el tipo de sistema de archivo y seleccioné fat32 y por último oprimí el botón ADD.

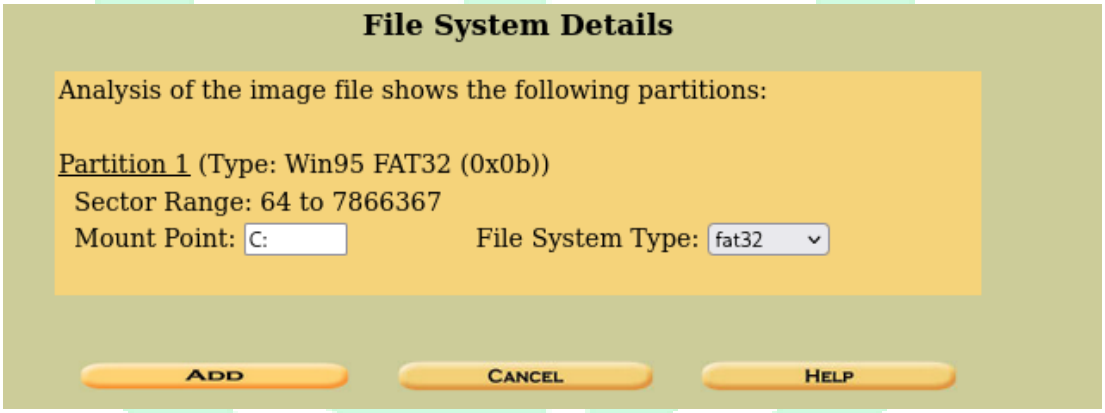


Ilustración 21 Auditoria Forense con Autopsy en Kali Linux parte - 20

Una vez adicionada la imagen, Autopsy mostro información de esta misma en una nueva ventana y allí oprimí el botón OK.

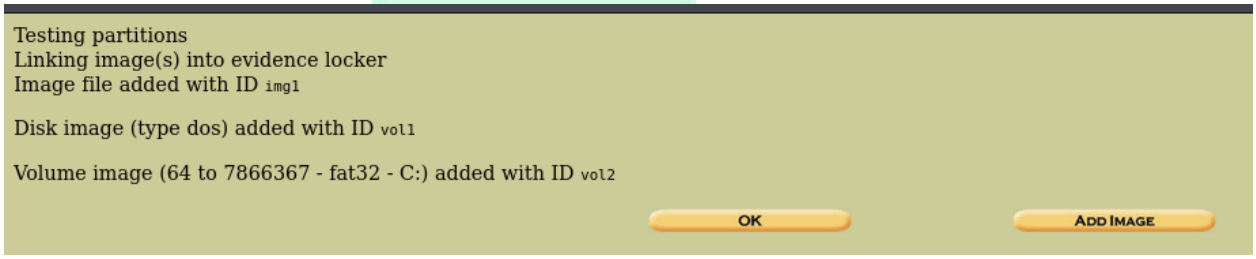


Ilustración 22 Auditoria Forense con Autopsy en Kali Linux parte - 21

EL siguiente paso contaba de primero seleccionar el disco C:/ y luego oprimí el botón ANALYZE para realizar el análisis.

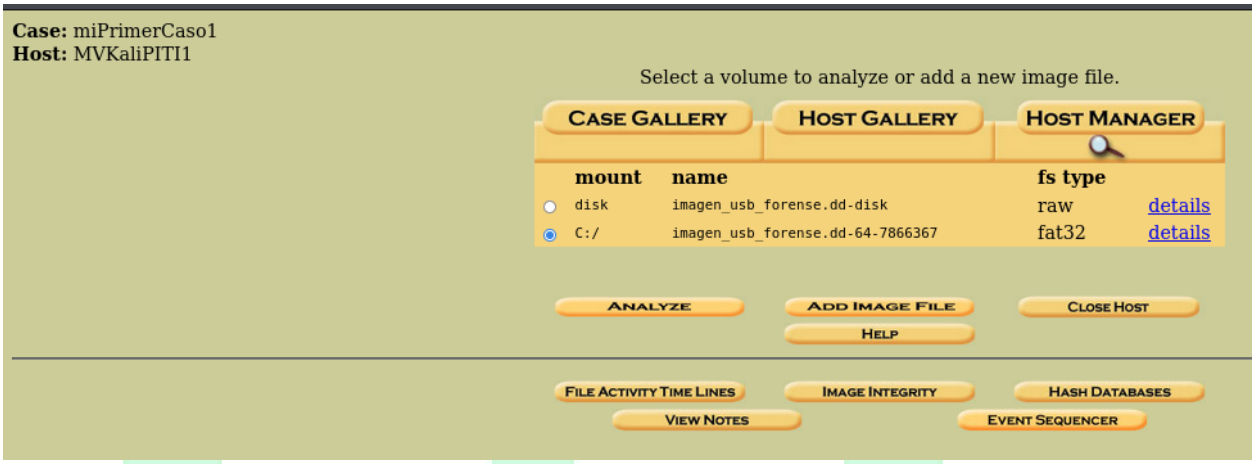


Ilustración 23 Auditoria Forense con Autopsy en Kali Linux parte - 22

La herramienta me mostro la siguiente ventana y allí oprimí el botón FILE ANALISIS, para realizar el análisis de los archivos.

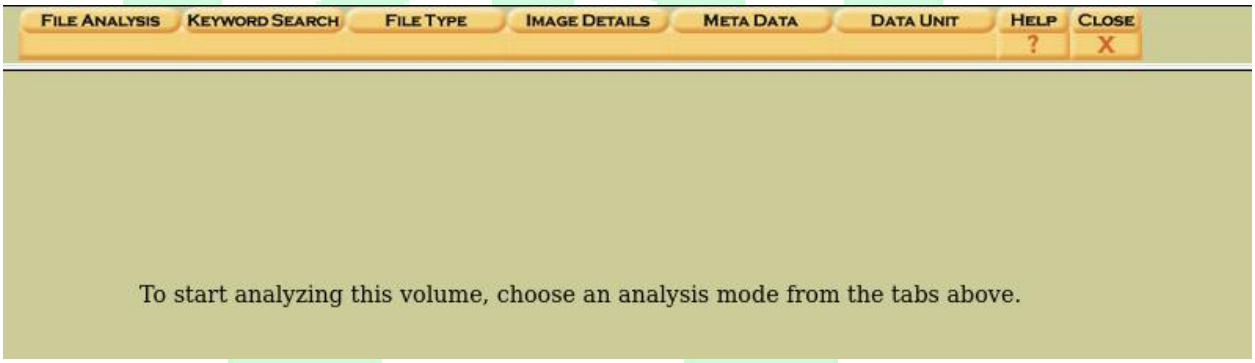


Ilustración 24 Auditoria Forense con Autopsy en Kali Linux parte - 23

Al ingresar a esta venta, puede observar todos los archivos de esa imagen o se la USB, como por ejemplo los que se habían eliminado y entre otro.

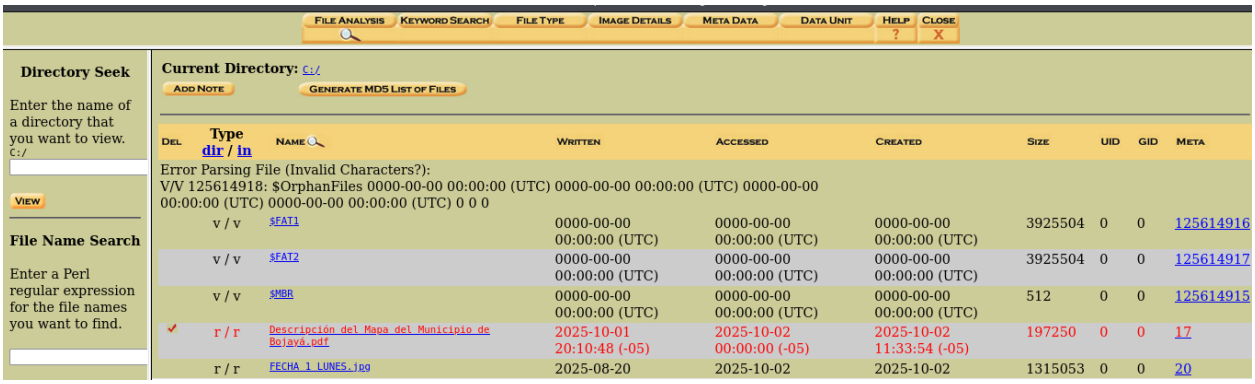


Ilustración 25 Auditoria Forense con Autopsy en Kali Linux parte - 24

Decidí, regresar atrás, seleccione nuevamente el disco C:/ y esta vez ingrese a la ventana HASH DATABASE.

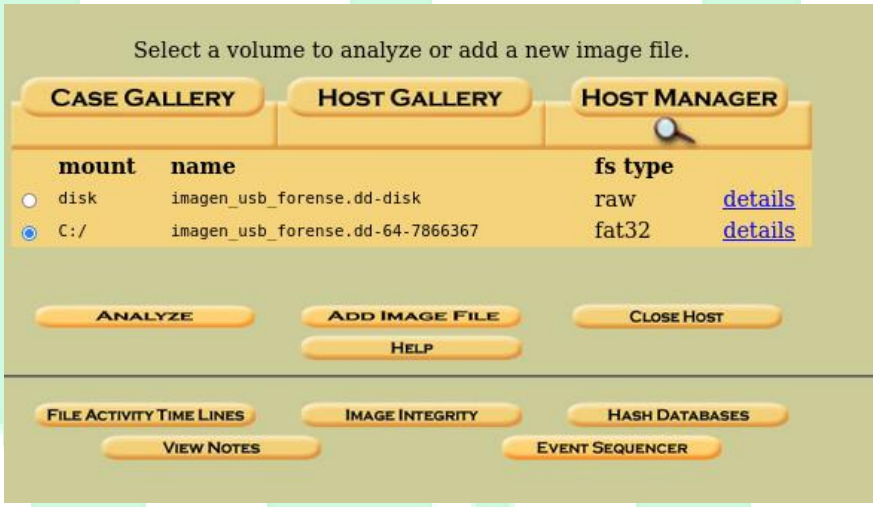


Ilustración 26 Auditoria Forense con Autopsy en Kali Linux parte - 25

Allí me mostraba la imagen antes seleccionada o agregada y oprimí el botón CALCULATE, para general un hash con MD5 para la imagen.

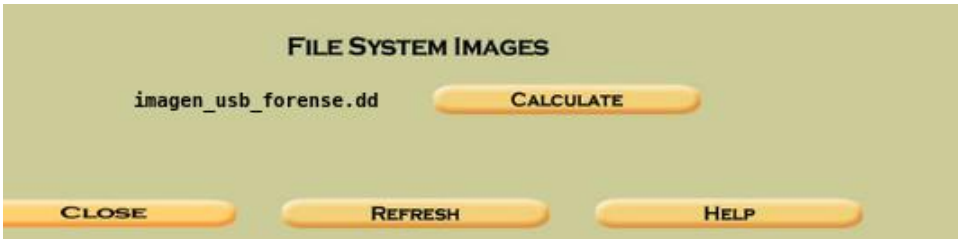


Ilustración 27 Auditoria Forense con Autopsy en Kali Linux parte - 26

En la imagen siguiente se puede ver, el hash generado.

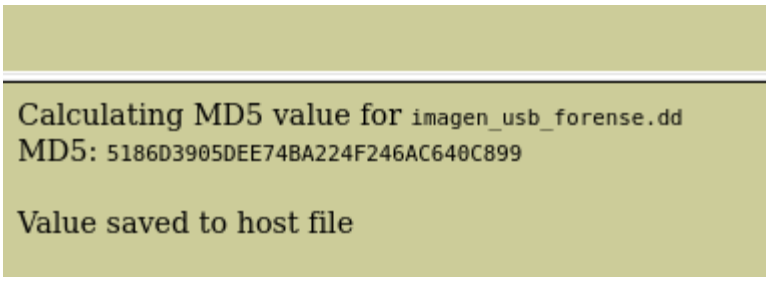


Ilustración 28 Auditoria Forense con Autopsy en Kali Linux parte - 27

Volví a ingresar a la ventana de ANALITY FILE y allí dentro oprimí el botón GENERATE MD5 LIST OF FILES, para observar los hash de cada uno de los archivo.

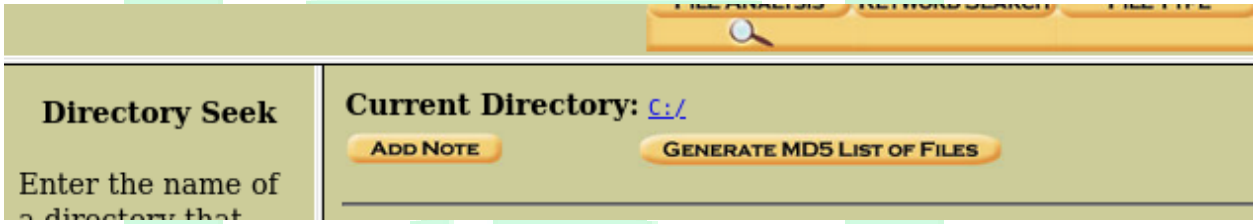


Ilustración 29 Auditoria Forense con Autopsy en Kali Linux parte - 28

Y la herramienta genero los siguientes hashes que se ven en la imagen que sigue.

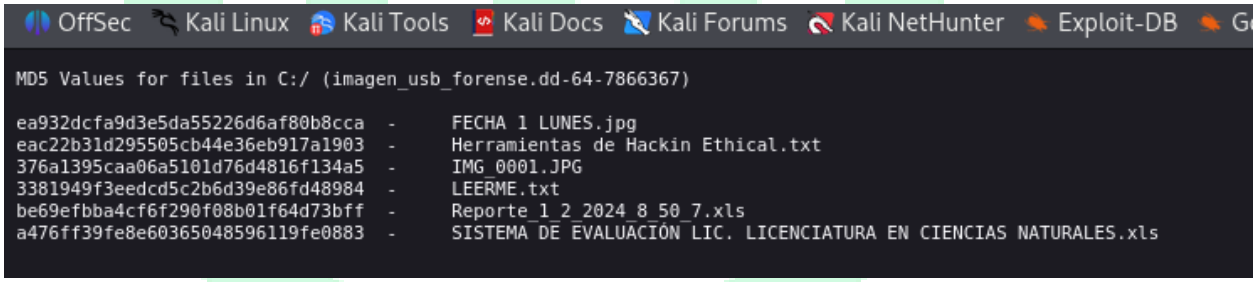


Ilustración 30 Auditoria Forense con Autopsy en Kali Linux parte - 29

Este mismo hash, debían resultar con el análisis de la USB peor en Autopsy en Windows y FTK Imager en también en Windows.

Y así es como se realizó este análisis de la USB con Autopsy en Kali Linux. Donde se pudo observar los archivos eliminados de la USB y los que seguían activos.

5 Capítulo 2 Auditoria Forense con Autopsy en Windows.

El segundo capitulo del informe, muestra como realice el análisis forense de la USB, pero en Autopsy de Windows. Es importante mencionar que para este análisis se utilizo la misma imagen que se creó en Kali Linux.

Pero para realizar este análisis, primero descargue e instale Autopsy en Windows.

Primero ingrese al navegador de Google y allí busque Autopsy y luego ingrese a link que decía Autopsy – Download.

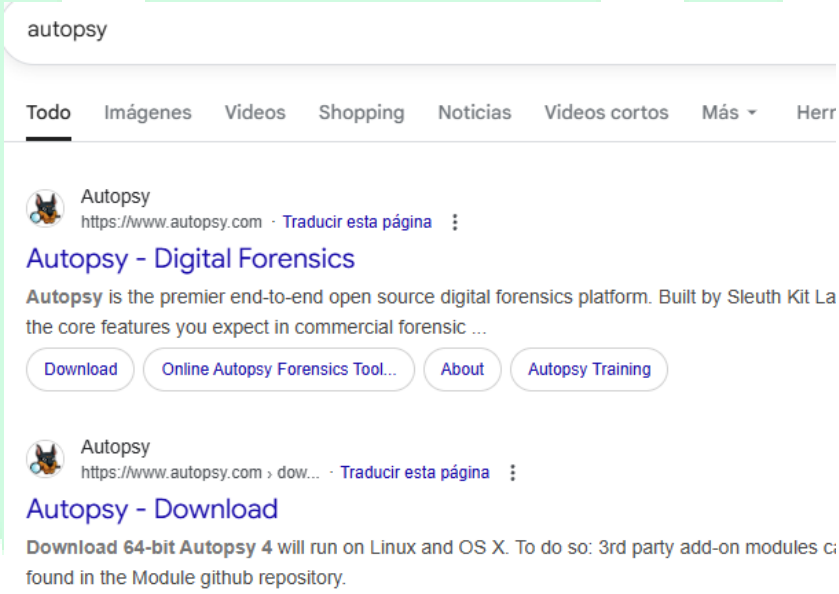


Ilustración 31 Auditoria Forense con Autopsy en Windows parte 1

Una vez dentro de la vista, oprimí el botón que decía Download 64-Bit.

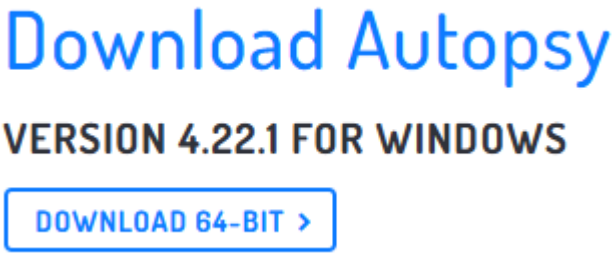


Ilustración 32 Auditoria Forense con Autopsy en Windows parte 2

Y empezo a descargar el instalador de la heramienta.

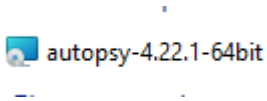


Ilustración 33 Auditoria Forense con Autopsy en Windows parte 3

Después de haber terminado de descargar el instalador, lo selección y oprimí el botón izquierdo del teclado y luego oprimí el botón abrir.

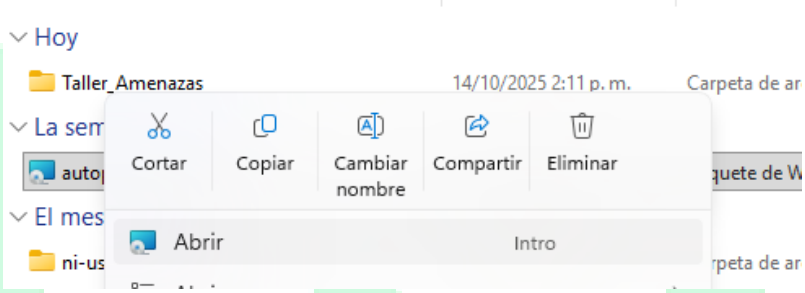


Ilustración 34 Auditoria Forense con Autopsy en Windows parte 4

Al abrir el instalador, mostro la ventana emergente para poder instalar la herramienta en Windows.

En la primera ventana que me daba la bienvenida, oprimí el botón next o continuar.

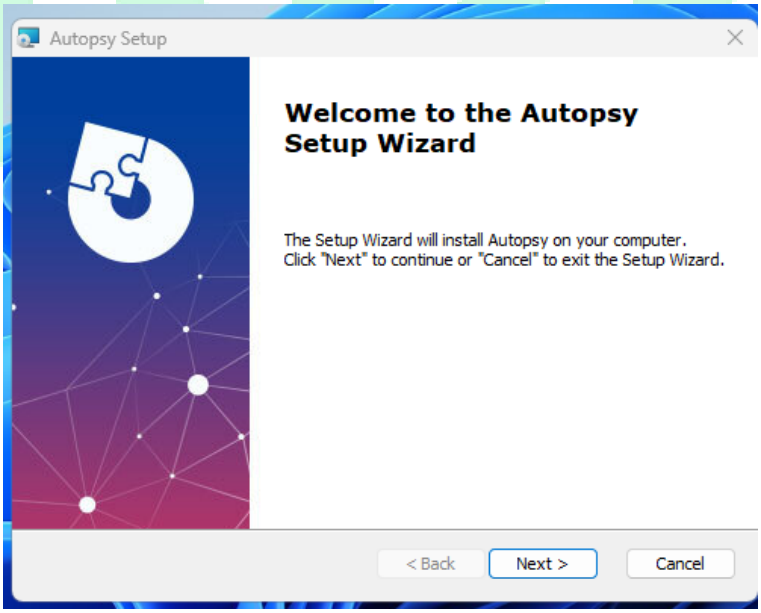


Ilustración 35 Auditoria Forense con Autopsy en Windows parte 5

Luego de el botón next en el paso atrás, el programa mostro una nueva ventana emergente donde debía elegir la ruta donde iba a quedar el programa, lo dejé por defecto y oprimí nuevamente el botón next.

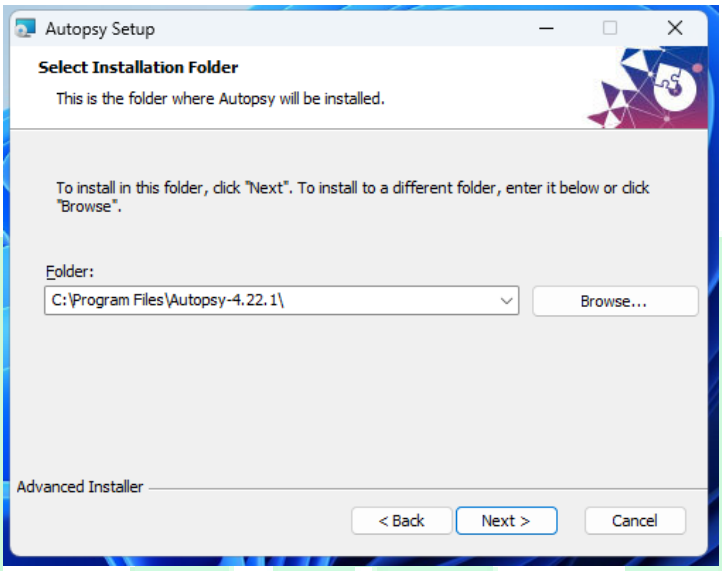


Ilustración 36 Auditoria Forense con Autopsy en Windows parte 6

después, me pregunto que, si quería instalar el sistema o quería cancelar la acción, y oprimí el botón install para continuar la instalación del programa.

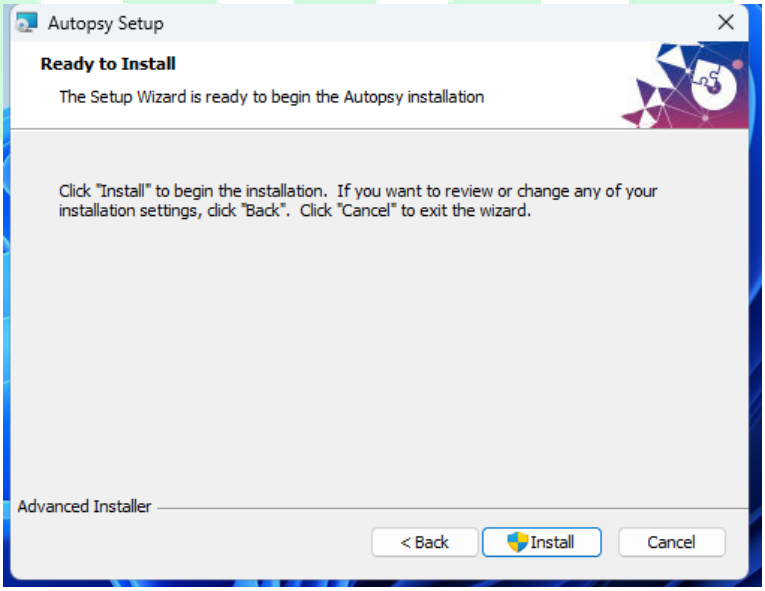


Ilustración 37 Auditoria Forense con Autopsy en Windows parte 7

Y cuando termino de instalar el programa, seleccione el botón finish para terminar con el proceso.

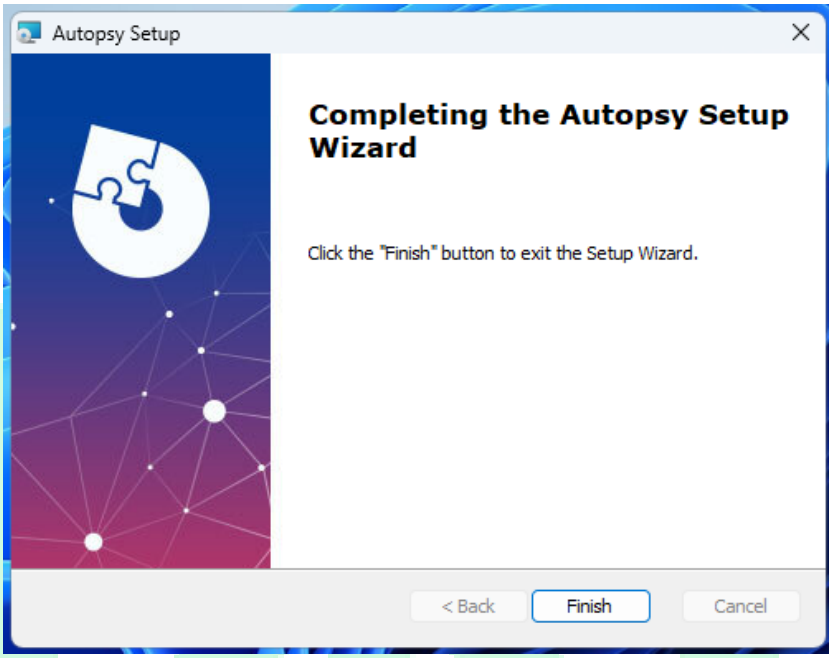


Ilustración 38 Auditoria Forense con Autopsy en Windows parte 8

Y automáticamente se instalo el programa o herramienta en Windows.

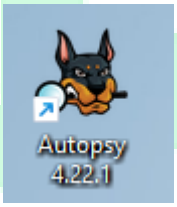


Ilustración 39 Auditoria Forense con Autopsy en Windows parte 9

Antes de empezar con el análisis, cree la ruta o carpetas en donde iba a guardar cada uno de los casos. En el disco local, cree la carpeta Cases.

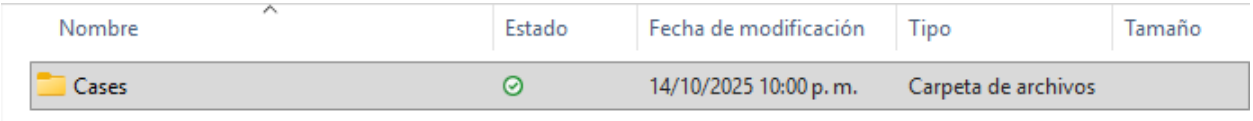


Ilustración 40 Auditoria Forense con Autopsy en Windows parte 10

Dentro de la carpeta Cases, cree la carpeta Case01.

Ilustración 41 Auditoria Forense con Autopsy en Windows parte 11

Y dentro de la carpeta Case01, cree la carpeta Autopsy.

Ilustración 42 Auditoria Forense con Autopsy en Windows parte 12

Luego de crear la ruta donde se guardarían todos mis casos, abrí la herramienta Autopsy y oprimí el botón New Case para crear un caso nuevo.

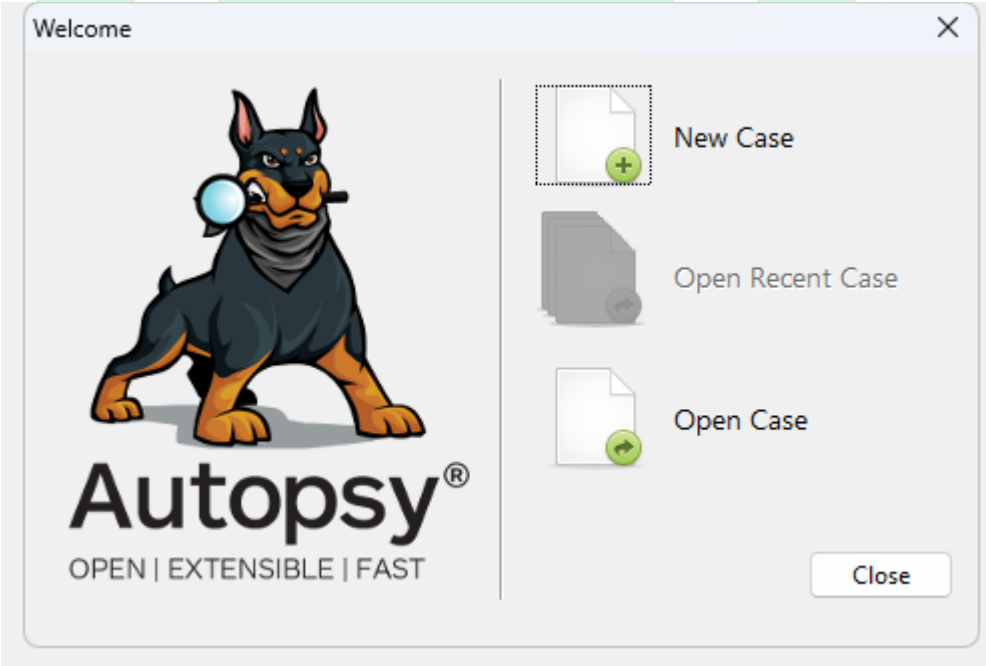


Ilustración 43 Auditoria Forense con Autopsy en Windows parte 13

Luego, debía poner el nombre del caso el cual fue MiPrimerCaso, además debía seleccionar la ruta donde se iba a guardar y allí puse la ruta de las carpetas que antes mencioné y también debía seleccionar el tipo de caso y seleccioné la opción Single-Use y por ultimo oprimí el botón next para conteniar.

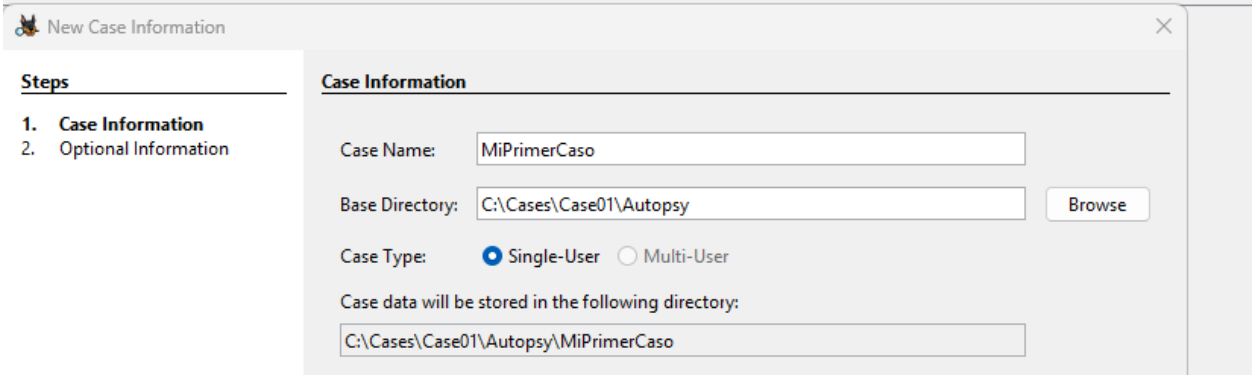


Ilustración 44 Auditoria Forense con Autopsy en Windows parte 14

En la siguiente ventana, debía establecer el numero del caso y escribí 01, además debía poner los datos del analizar o investigador, allí puse mi nombre, un correo y un número telefónico y una breve descripción, también debía seleccionar una organización, pero como no pertenecía a ninguna, seleccioné la opción Not Specified y luego oprimí el botón finish para terminar con el proceso.

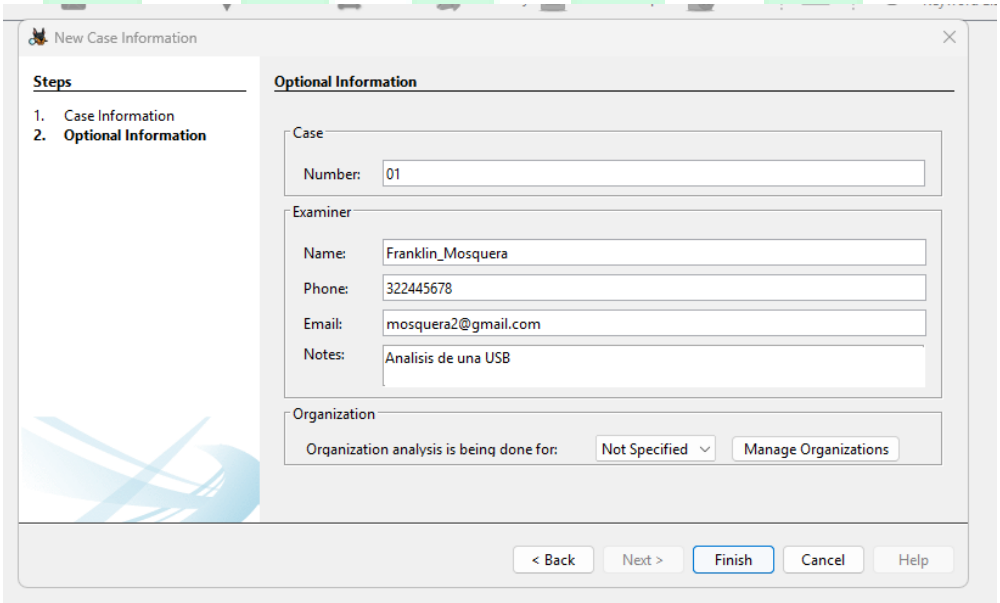


Ilustración 45 Auditoria Forense con Autopsy en Windows parte 15

Una vez terminado el proceso anterior, debía seleccionar un host para el caso, como no tenía ninguno seleccioné la opción que decía Generate new host name base don data source name y luego oprimí el botón next para continuar con el proceso.

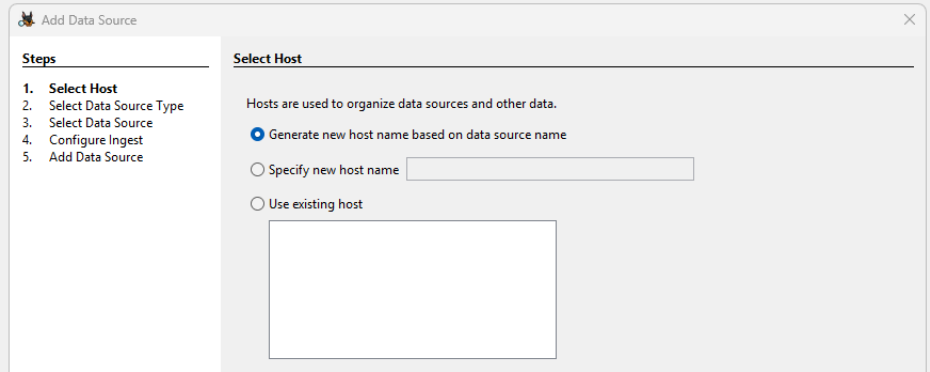


Ilustración 46 Auditoria Forense con Autopsy en Windows parte 16

El siguiente paso era seleccionar que tipo de dato se iba a analizar, en este caso como se iba a analizar la imagen de la USB que habíamos generado en Kali Linux como máquina virtual, seleccione la opción que decía Disk Image or VM File y luego oprimí el botón next para conteniar con el proceso.

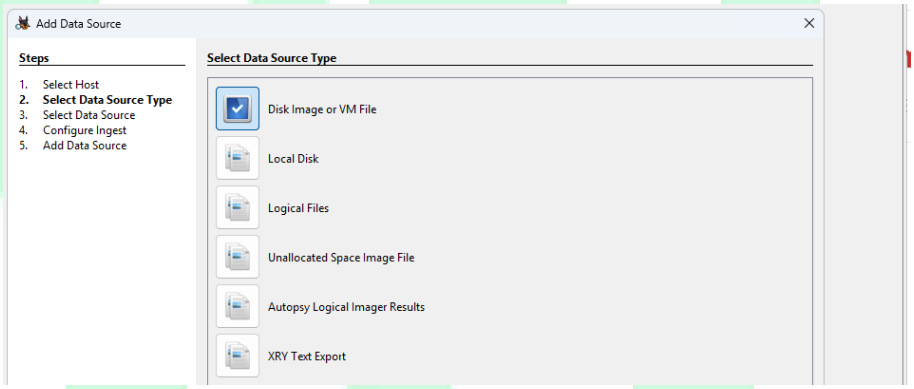


Ilustración 47 Auditoria Forense con Autopsy en Windows parte 17

Como debía utilizar la imagen de la USB que genere el Kali Linux, debía compartir ese archivo a mi maquina física. Para eso cree una carpeta en la maquina física con nombre Imagen_Autopsy.

Ilustración 48 Auditoria Forense con Autopsy en Windows parte 18

Luego en Kali Linux utilicé la opción de tiene VirtualBox de compartir carpeta y compartí la carpeta que había creado

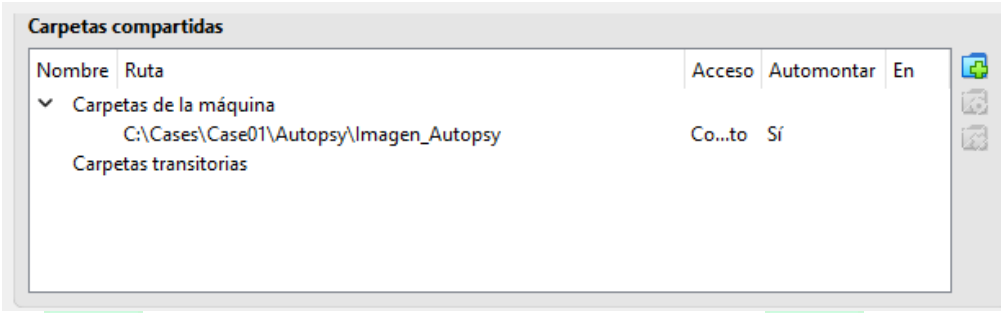


Ilustración 49 Auditoria Forense con Autopsy en Windows parte 19

Una vez que la carpeta la pude observar dentro de Kali Linux, como se ve en la siguiente imagen.

Ilustración 50 Auditoria Forense con Autopsy en Windows parte 20

Copie el archivo de la imagen dentro de la carpeta.

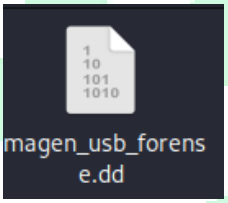


Ilustración 51 Auditoria Forense con Autopsy en Windows parte 21

Y en mi maquina física ya podía tener acceso a esa imagen.

Ilustración 52 Auditoria Forense con Autopsy en Windows parte 22

Volví nuevamente a la herramienta Autopsy y en la venta que me pedía seleccionar la imagen, la seleccioné de la carpeta antes mencionada, luego oprimí el botón next para continuar con el proceso.

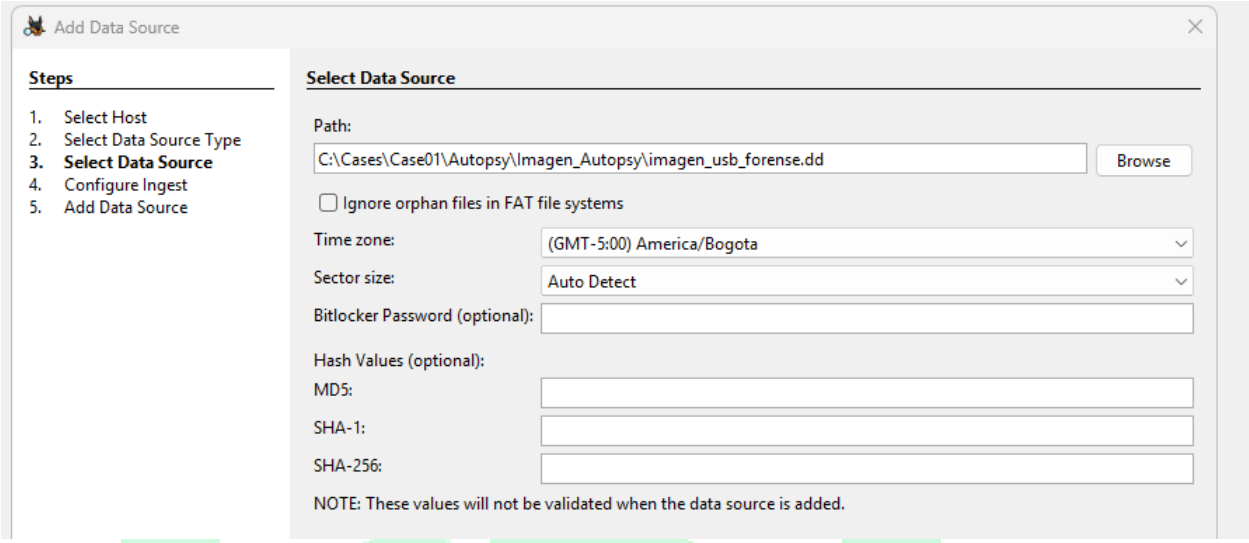


Ilustración 53 Auditoria Forense con Autopsy en Windows parte 23

Luego de seleccionar la imagen de la USB, debía seleccionar los módulos para realizar el análisis. Seleccioné todos los módulos, menos los que realizan análisis a equipos móviles como Androip Analyzer entre otro, por último, oprimí el botón next para continuar con el proceso.

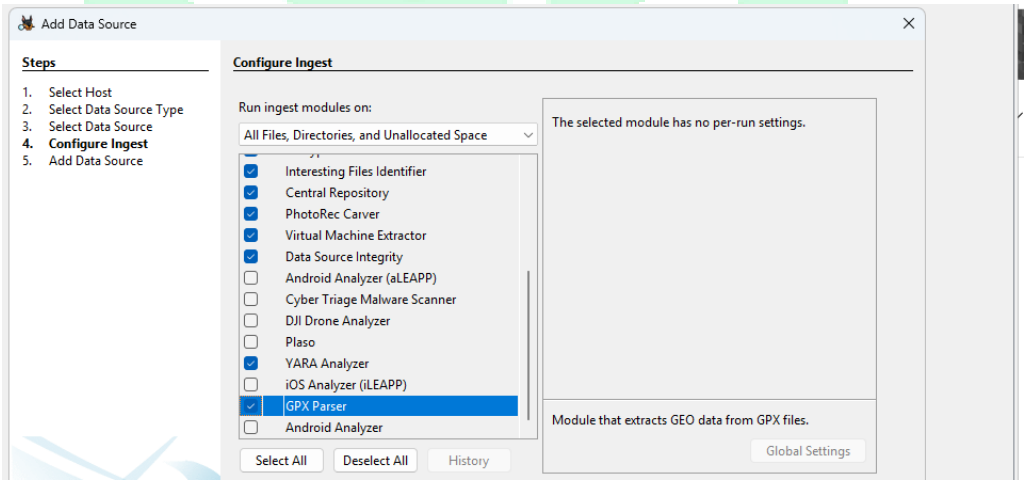


Ilustración 54 Auditoria Forense con Autopsy en Windows parte 24

Y, por último, solo debía esperar que la Autopsy realizara el análisis y me mostrara los resultados.

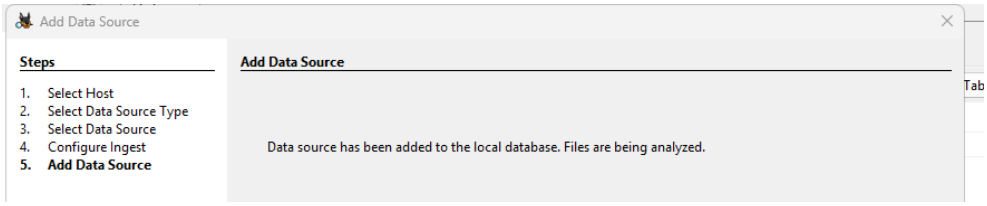


Ilustración 55 Auditoria Forense con Autopsy en Windows parte 25

Una vez Autopsy termino de realizar el análisis, puede observar la venta donde podía ver los resultados de ese análisis.

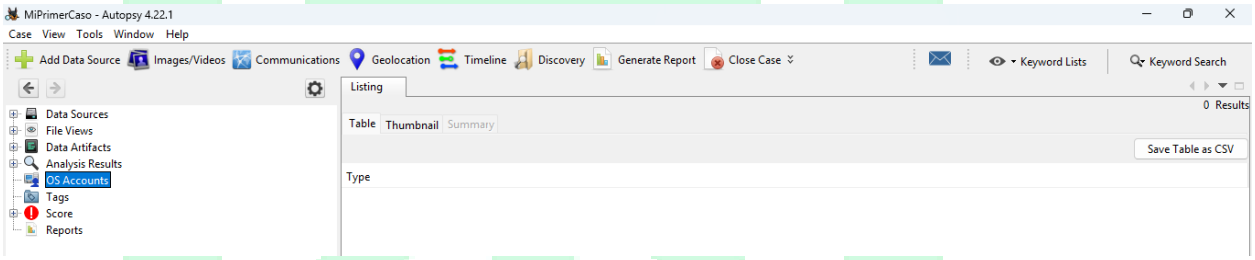


Ilustración 56 Auditoria Forense con Autopsy en Windows parte 26

Allí dentro, seleccione el incono que decía Data Source y puede observar la imagen que había seleccionado y esta tenía dos particiones.

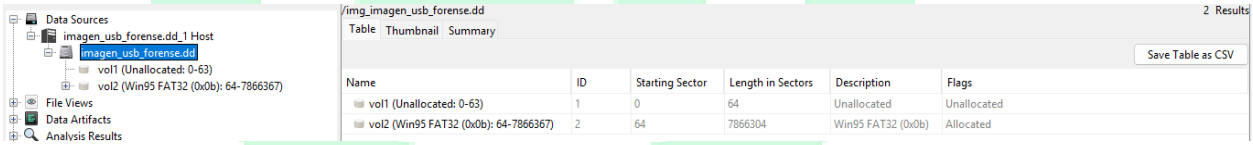


Ilustración 57 Auditoria Forense con Autopsy en Windows parte 27

Seleccioné la primera partición y allí pude observar un archivo que se había eliminado de la USB.

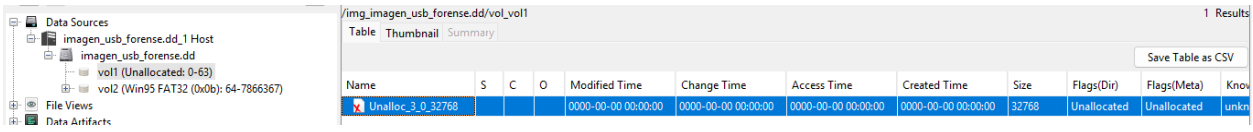


Ilustración 58 Auditoria Forense con Autopsy en Windows parte 28

Después, seleccioné la segunda partición y allí pude observar una gran cantidad de archivo que tenía la USB, como imágenes, documento de texto y algunos elementos eliminados.

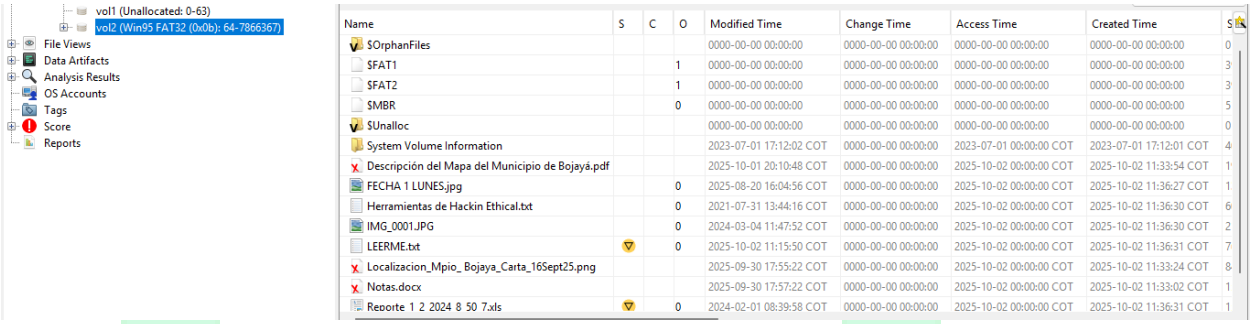


Ilustración 59 Auditoria Forense con Autopsy en Windows parte 29

Y es esa partición, además, pude observar los hashes de cada uno de los archivos que estaban en la lista y allí pude observar que esos hashes eran el mismo hash generados para los documentos en Autopsy de Kali Linux.

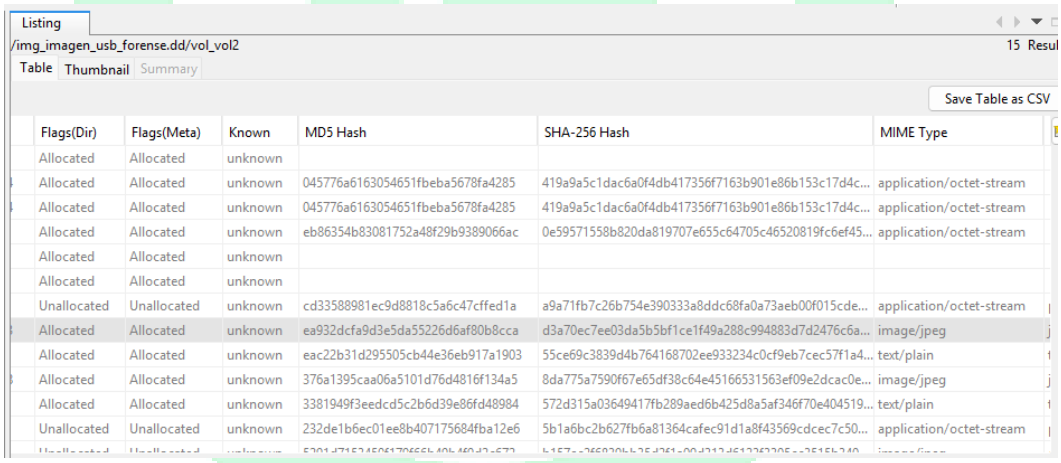


Ilustración 60 Auditoria Forense con Autopsy en Windows parte 30

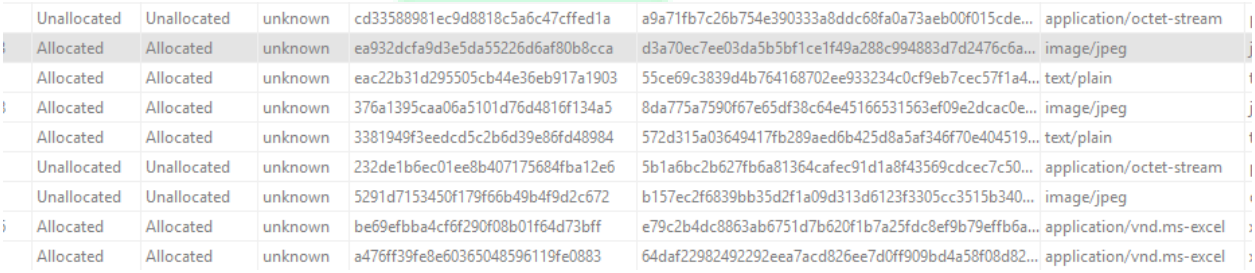


Ilustración 61 Auditoria Forense con Autopsy en Windows parte 31

Y así es como realice el análisis de la USB en Autopsy, pero en Windows, arrojando el mismo resultado que el análisis de Autopsy en Kali Linux.

6 Auditoria Forense con FTK Imager en Windows.

El tercer capítulo consta de mostrar el análisis forense hecho a la imagen de la USB antes mencionada, pero en este caso en la herramienta FTK Imager.

Pero para hacer ese análisis, primero descargue e instale la herramienta, para eso ingrese al navegar de Google y busque la herramienta, e ingrese al primer enlace.

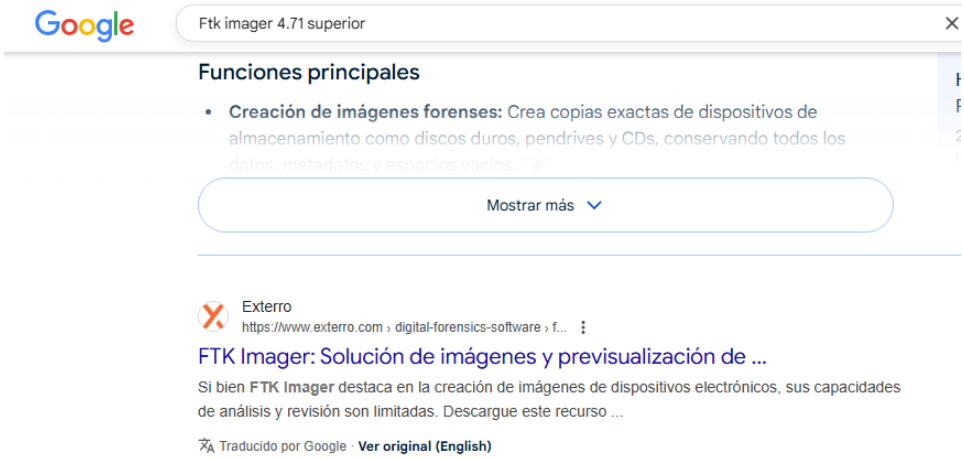


Ilustración 62 Forense con FTK Imager en Windows parte 1

Una vez ingresé al enlace en la ventana siguiente, oprimí el botón Free Download.

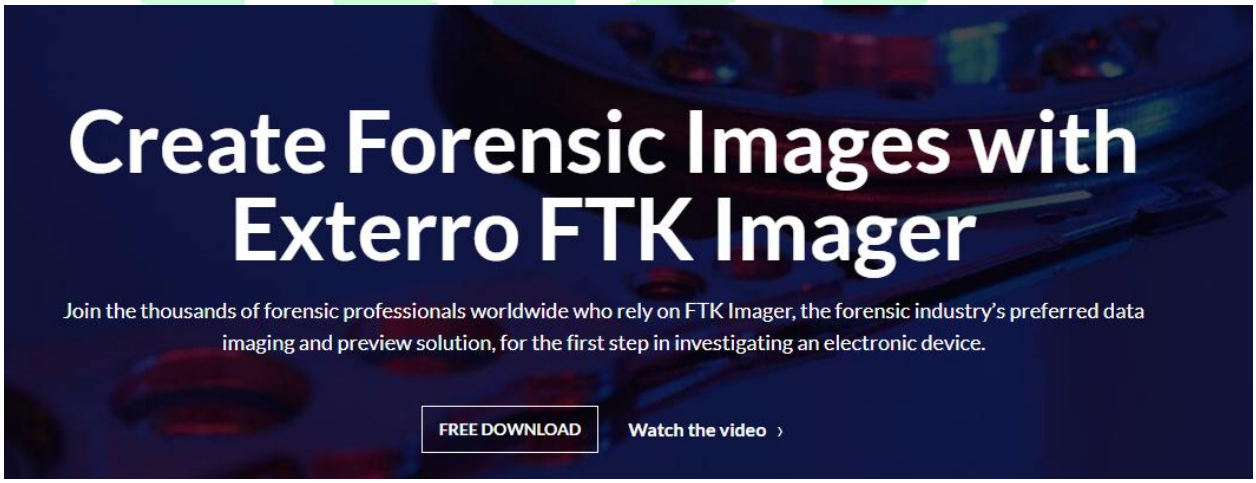


Ilustración 63 Forense con FTK Imager en Windows parte 2

Ese enlace me dirigió a un formulario que debía llenar antes de empezar a descargar el instalador. Allí puse, mi nombre, apellidos, correo electrónico, el título del trabajo y el país y por último, envié el formulario dando clic en el botón enviar.

Ilustración 64 Forense con FTK Imager en Windows parte 3

Ilustración 65 Forense con FTK Imager en Windows parte 4

Y automáticamente, empezó a descargar el instalador de la herramienta FTK Imager.

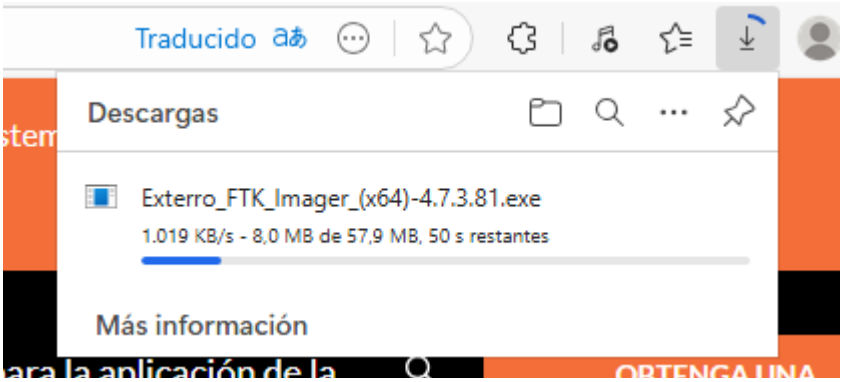


Ilustración 66 Forense con FTK Imager en Windows parte 5

Luego de descargar el instalador del programa.

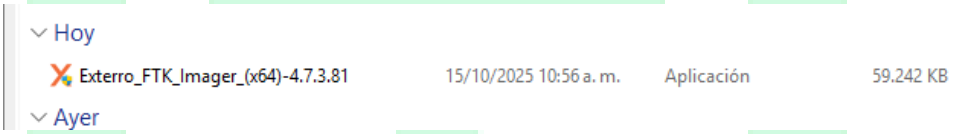


Ilustración 67 Forense con FTK Imager en Windows parte 6

Seleccioné este mismo dando clic izquierdo sobre él y luego oprimí el botón ejecutar como administrador.

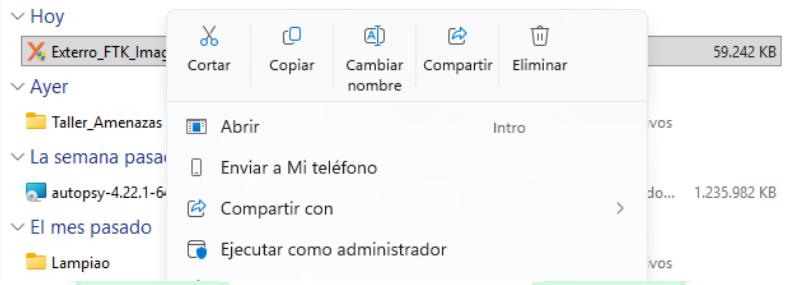


Ilustración 68 Forense con FTK Imager en Windows parte 7

Al ejecutar el archivo, este mostro una ventana emergente donde me daba la bienvenida, allí oprimí el botón next para continuar con el proceso.

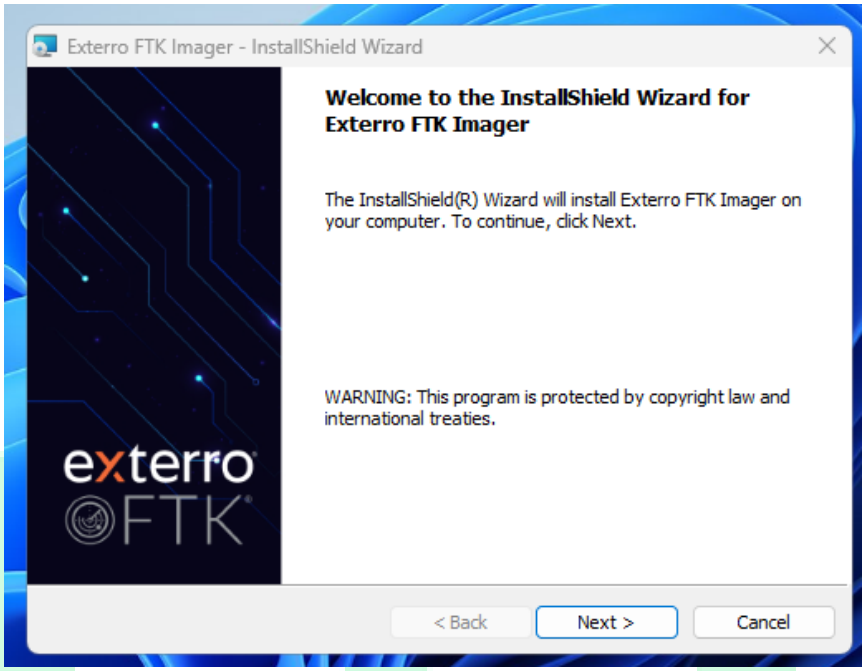


Ilustración 69 Forense con FTK Imager en Windows parte 8

En la siguiente ventana, acepte los termino y condiciones y luego seleccione el botón next para continuar con el proceso.

Ilustración 70 Forense con FTK Imager en Windows parte 9

En la siguiente ventana, debía seleccionar la ubicación del archivo, lo dejé por defecto y nuevamente oprimí el botón next para continuar con el proceso.

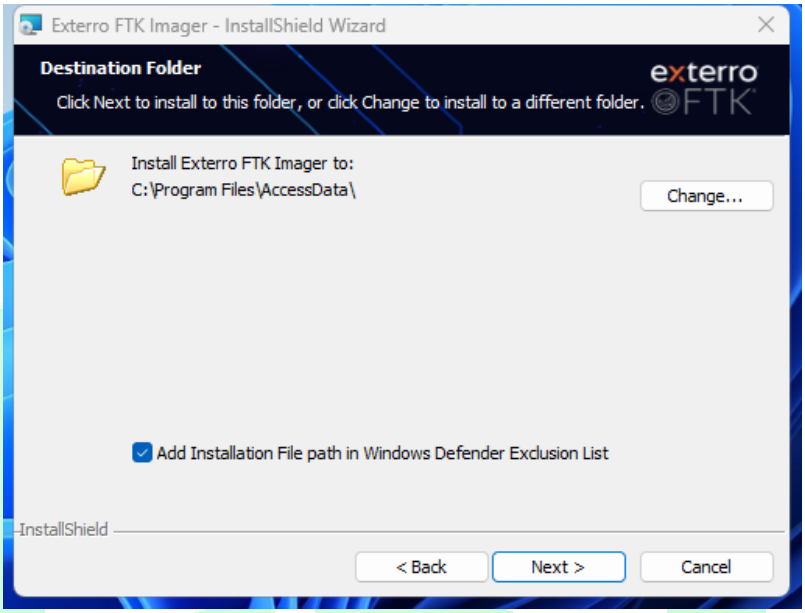


Ilustración 71 Forense con FTK Imager en Windows parte 10

Y en la ventana siguiente, seleccione la opción install para instalar definitivamente el programa.

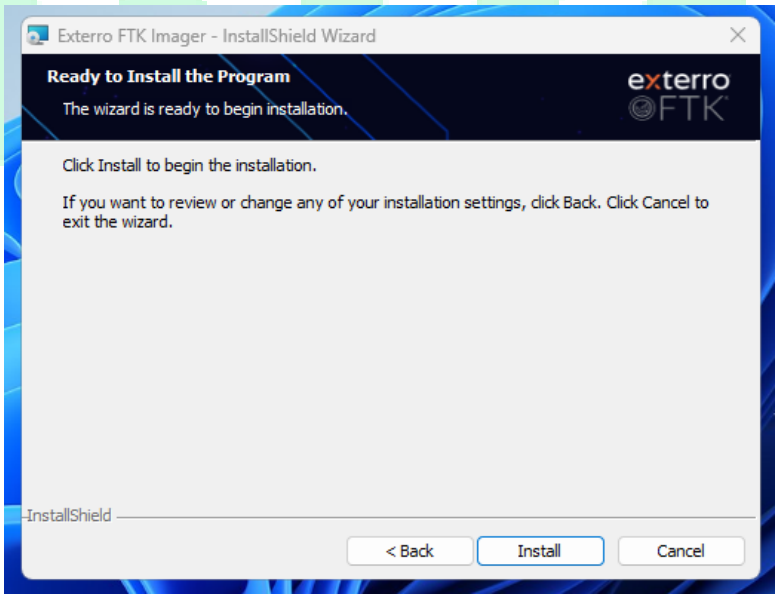


Ilustración 72 Forense con FTK Imager en Windows parte 11

Y una vez termino de instalar, selección el botón finish para terminar con la instalación definitivamente.

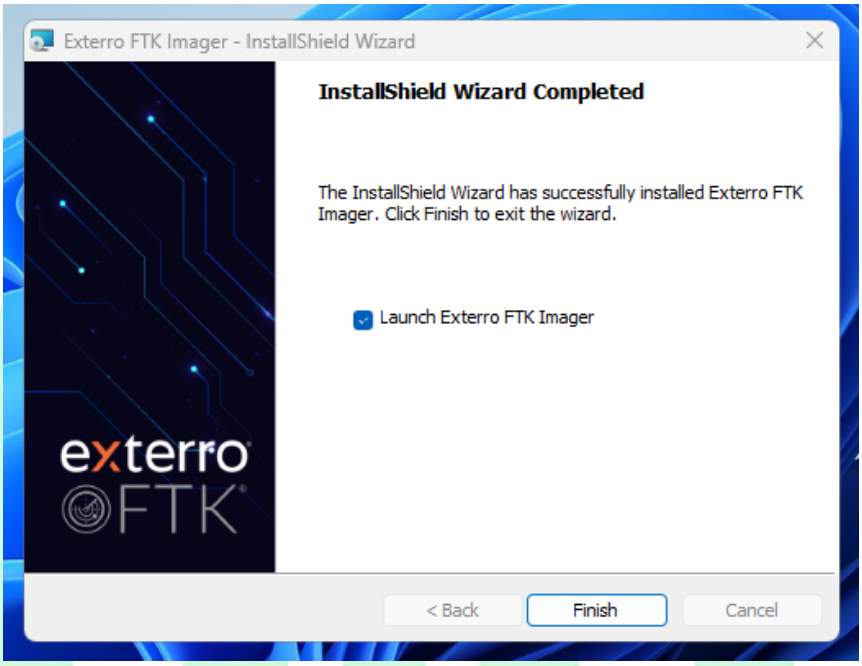


Ilustración 73 Forense con FTK Imager en Windows parte 12

Y automáticamente, pude observar la herramienta FTK Imager instalada en el computador.

Ilustración 74 Forense con FTK Imager en Windows parte 13

Cuando ya la herramienta estaba instalada, la ejecute para empezar a realizar el análisis.

Una vez dentro del programa añadí un nuevo caso, oprimiendo el icono verde y azul con forma de un más.

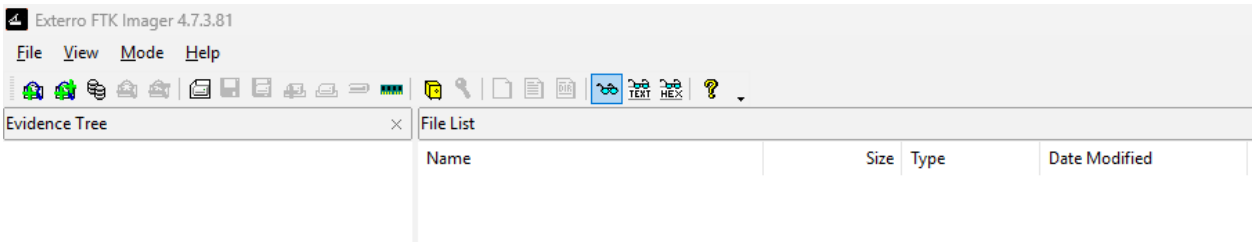


Ilustración 75 Forense con FTK Imager en Windows parte 14

Luego, seleccione el tipo de disco que se iba a analizar y allí seleccione la opción de image file y luego le di clic en siguiente.

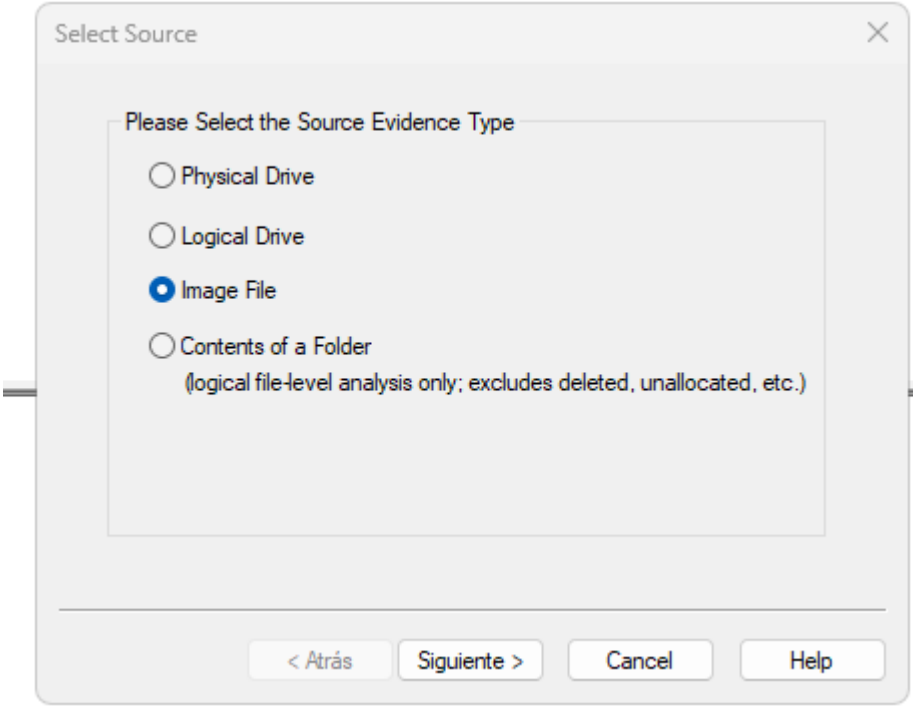


Ilustración 76 Forense con FTK Imager en Windows parte 15

después, seleccioné la ruta de la imagen que es la misma ruta que seleccionamos en los análisis anteriores y por último, oprimí el botón finish para terminar el proceso.

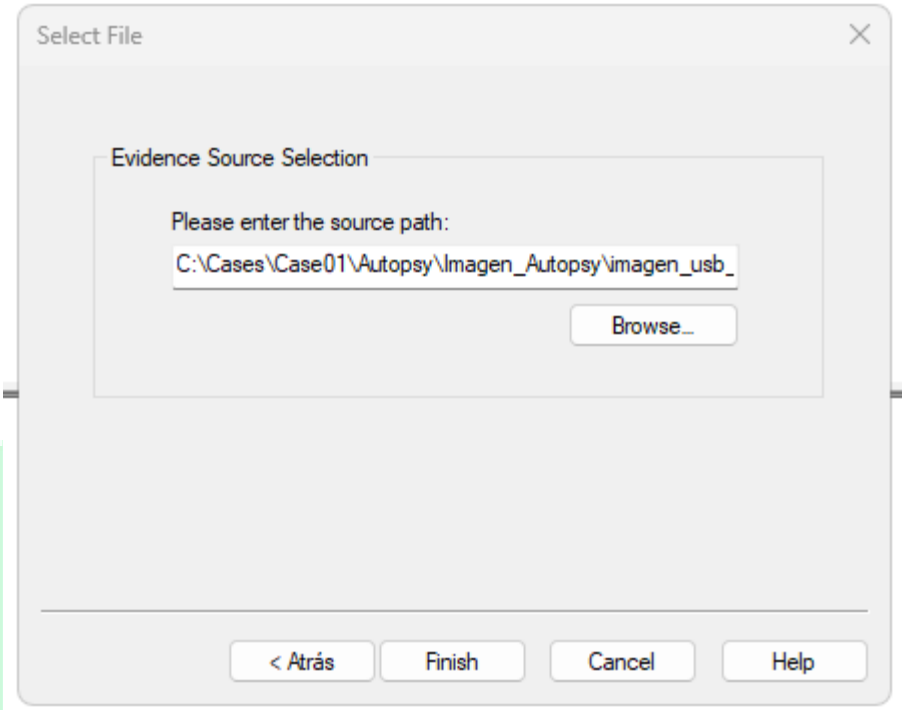


Ilustración 77 Forense con FTK Imager en Windows parte 16

Una vez finalizado el análisis por parte de la herramienta FTK Imager, procedí a observar los resultados.

Primeramente, pude ver la imagen seleccionada.

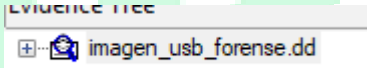


Ilustración 78 Forense con FTK Imager en Windows parte 17

Oprimí el signo mas que estaba junto a la imagen y me mostro la particion de esa imagen.

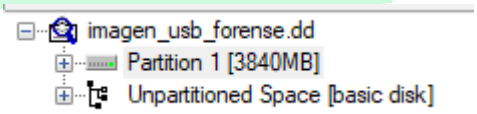


Ilustración 79 Forense con FTK Imager en Windows parte 18

Al dar clic en esa partición, observa dos carpetas y otros tipos de archivos.

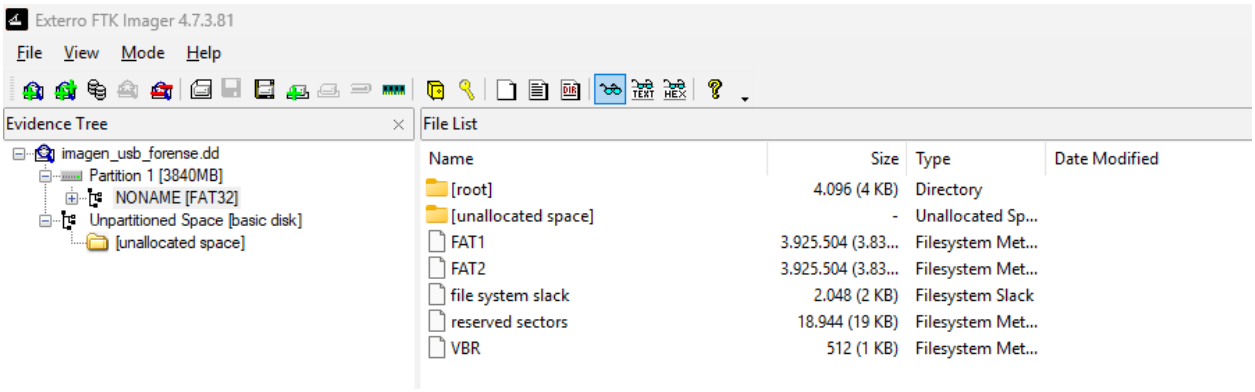


Ilustración 80 Forense con FTK Imager en Windows parte 19

Oprimí la carpeta llamada root y allí dentro estaban todos los archivos de la USB, las imágenes, documentos de Excel, Word, Text y los que se habían eliminado de la carpeta también.

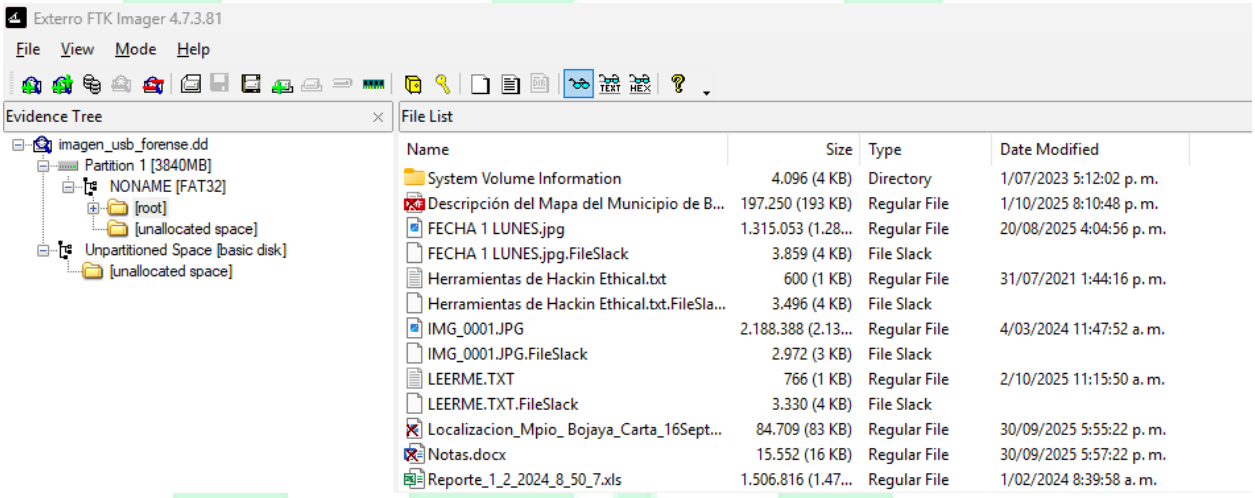


Ilustración 81 Forense con FTK Imager en Windows parte 20

Selección el archivo Notas.docx y no se observó nada de información allí.

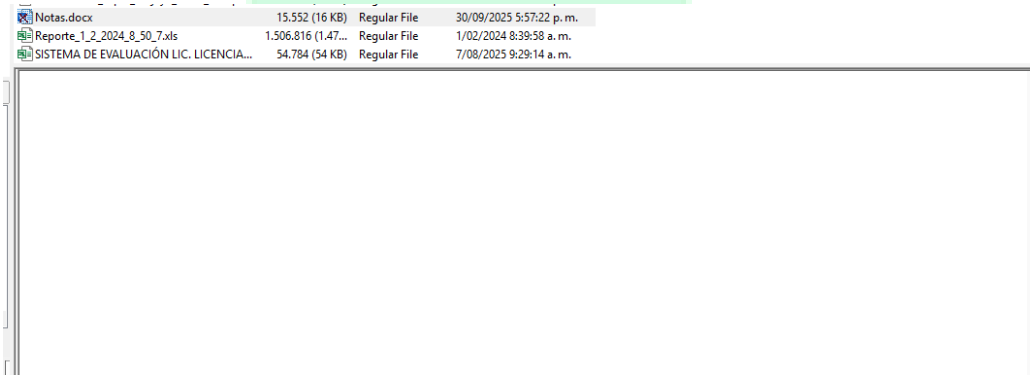


Ilustración 82 Forense con FTK Imager en Windows parte 21

También oprimí el archivo LEERME.TXT.FileSlack y observa datos binarios.

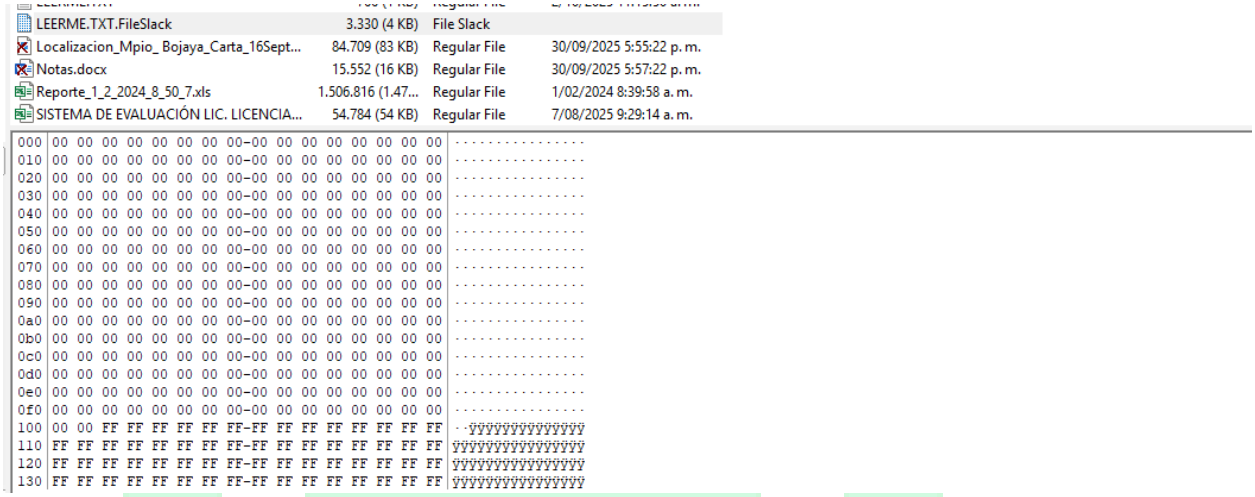


Ilustración 83 Forense con FTK Imager en Windows parte 22

Como necesitaba llegar al hash de cada uno de los archivos, los seleccione todos y cada uno los archivos.

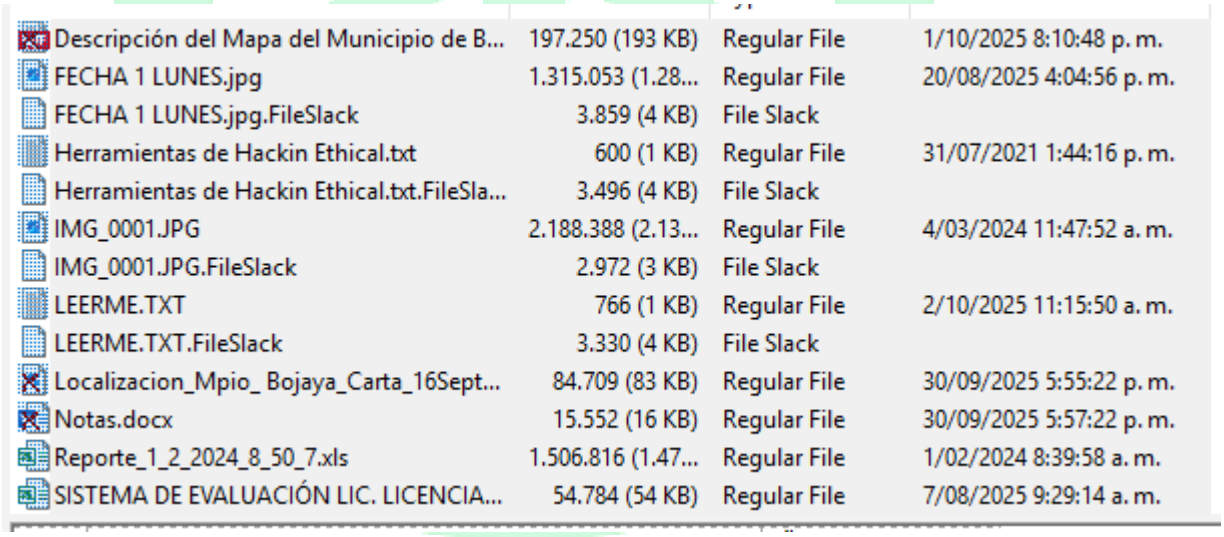


Ilustración 84 Forense con FTK Imager en Windows parte 23

Y luego exporte el hash de cada uno, oprimiendo el icono en forma de libro rallado.

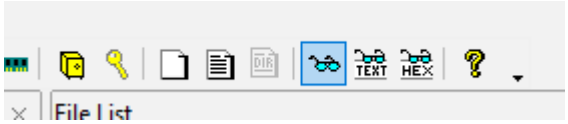


Ilustración 85 Forense con FTK Imager en Windows parte 24

Cree una carpetada para guardar rl archivo llamada FTK Forense.

Ilustración 86 Forense con FTK Imager en Windows parte 25

Luego seleccione la carpeta.

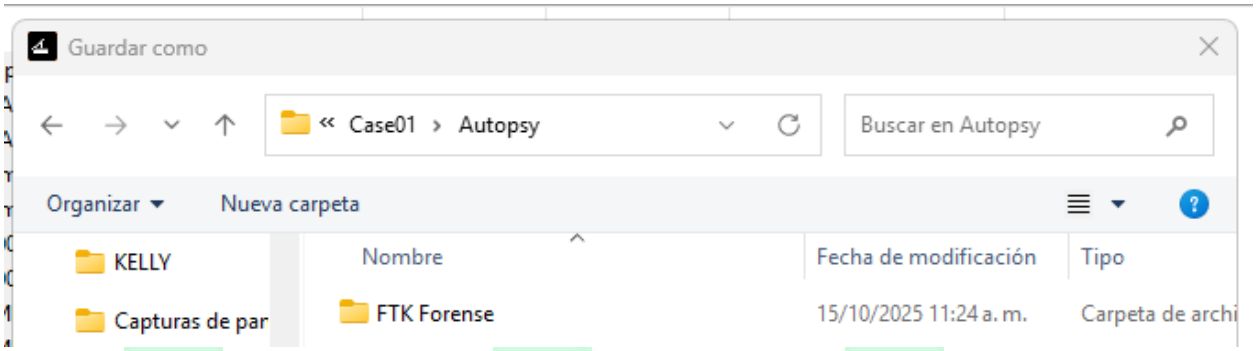


Ilustración 87 Forense con FTK Imager en Windows parte 26

Y guarde los hashes con el nombre de Hash.

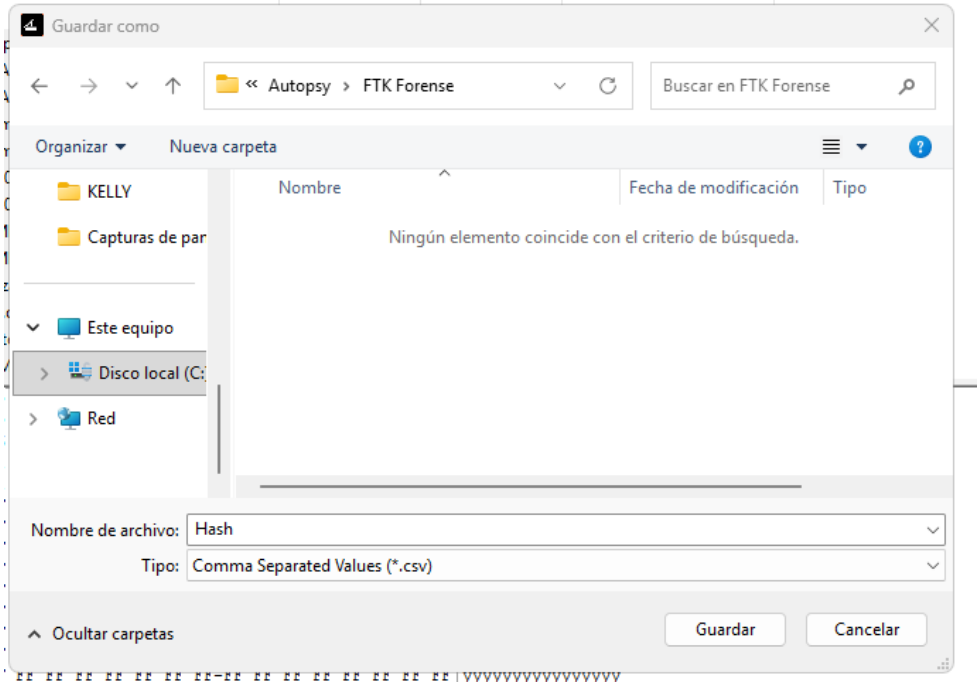


Ilustración 88 Forense con FTK Imager en Windows parte 27

Y dentro de la carpeta estaba el documento.

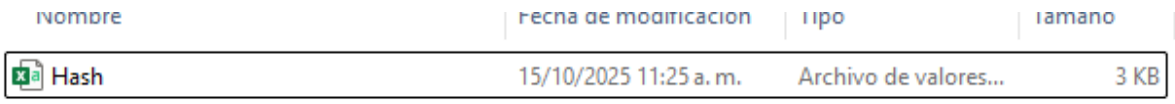
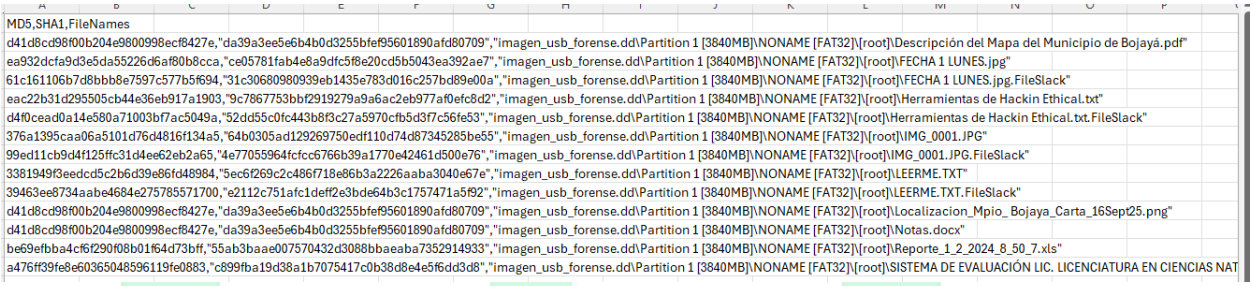


Ilustración 89 Forense con FTK Imager en Windows parte 28

Abrí el archivo y dentro de este estaban todos los hashes de cada uno de los archivos y lo mejor fue que coincidían con los hashes de Autopsy en Kali y en Windows.



MD5,SHA1,FileNames
d41d8cd98f00b204e9800998ecf8427e,"da39a3ee5e6b4b0d3255bfef95601890afd80709","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\Descripción del Mapa del Municipio de Bojayá.pdf"
ea932dcfa9d3e5da55226d6af80b8cca,"ce05781fab4e8a9dfc5f8e20cd5b5043ea392ae7","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\FECHA 1 LUNES.jpg"
61c161106b7d8bbb8e7597c577b5f694,"31c30680980939eb1435e783d016c257bd89e00a","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\FECHA 1 LUNES.jpg.FileSlack"
eac22b31d295505cb44e36eb917a1903,"9c7867753bbf2919279a9a6ac2eb977af0efc8d2","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\Herramientas de Hackin Ethical.txt"
d4f0cead0a14e580a71003bf7ac5049a,"52dd55c0fc443b8f3c27a5970cfb5d3f7c56fe53","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\Herramientas de Hackin Ethical.txt.FileSlack"
376a1395caa06a5101d76d4816f134a5,"64b0305ad129269750edf110d74d87345285be55","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\IMG_0001.JPG"
99ed11cb9d4f125ffc31d4ee62eb2a65,"4e77055964fcfcc6766b39a1770e42461d500e76","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\IMG_0001.JPG.FileSlack"
3381949f3eedcd5c2b6d39e86fd48984,"5ec6f269c2c486f718e86b3a2226aaba3040e67e","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\LEERME.TXT"
39463ee8734aabe4684e275785571700,"e2112c751afc1deff2e3bde64b3c1757471a5f92","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\LEERME.TXT.FileSlack"
d41d8cd98f00b204e9800998ecf8427e,"da39a3ee5e6b4b0d3255bfef95601890afd80709","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\Localizacion_Mpio_ Bojaya_Carta_16Sept25.png"
d41d8cd98f00b204e9800998ecf8427e,"da39a3ee5e6b4b0d3255bfef95601890afd80709","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\Notas.docx"
be69efbba4cf6f290f08b01f64d73bff,"55ab3baae007570432d3088bbaeaba7352914933","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\Reporte_1_2_2024_8_50_7.xls"
a476ff39fe8e60365048596119fe0883,"c899fba19d38a1b7075417c0b38d8e4e5f6dd3d8","imagen_usb_forense.dd\Partition 1 [3840MB]\NONAME [FAT32]\[root]\SISTEMA DE EVALUACIÓN LIC. LICENCIATURA EN CIENCIAS NAT

Ilustración 90 Forense con FTK Imager en Windows parte 29

Y así es como realice el análisis forense de la USB en FTK Imager.

7 Conclusiones

El proceso de auditoría forense permitió comprobar la importancia del uso de herramientas especializadas para el manejo de evidencias digitales.

La generación de imágenes forenses y el uso de funciones hash como SHA1 y MD5 garantizaron la integridad de los datos, confirmando que la información del dispositivo USB no fue modificada durante el proceso.

Tanto Autopsy en Linux y Windows como FTK Imager demostraron ser soluciones confiables para el análisis de dispositivos extraíbles, permitiendo visualizar archivos eliminados, existentes y sus respectivos hashes.

Los resultados obtenidos en los tres entornos fueron coincidentes, evidenciando la validez del procedimiento y la correcta aplicación de la metodología forense.

Este ejercicio refuerza la relevancia de mantener procedimientos estructurados y reproducibles en toda investigación digital, así como la necesidad de documentar cada paso para asegurar la trazabilidad y confiabilidad de la evidencia.

8 Referencias Bibliográficas

Carrier, B. (2023). *Autopsy Digital Forensics Platform*.

AccessData. (2023). *FTK Imager User Guide*.

Kaur, M. & Singh, G. (2021). *Digital Forensics: Tools and Techniques*. International Journal of Computer Applications.

Stallings, W. (2022). *Computer Security: Principles and Practice*. Pearson Education.