Informe 2 – Tercer Parcial

Yadier Stiven Mayoral Palomeque

Facultad de Ingeniería, Universidad Tecnológica del Chocó Diego Luis Córdoba

2720409: Seguridad y Auditoria de Redes

Docente: Rafael Sandoval Morales

Quibdó, Chocó

Octubre 2025

Tabla de Contenido

Pag.

Tabla de Ilustraciones

Pag.

Introducción

En este laboratorio se desarrolló una práctica orientada al uso de herramientas forenses en entornos controlados, con el propósito de comprender el proceso de adquisición, verificación y análisis de una memoria USB.

Para ello se emplearon **Autopsy**, tanto en sistemas operativos Linux como Windows y **FTK Imager**, herramientas ampliamente utilizadas por profesionales de la ciberseguridad y el análisis forense. A través de estas, se realizó la revisión de una imagen forense de una memoria USB, la verificación de su integridad mediante algoritmos de hash, y el posterior análisis del contenido de la imagen digital.

Objetivos

Objetivo General

Realizar un proceso completo de análisis forense sobre una memoria USB utilizando las herramientas Autopsy y FTK Imager, con el fin de aprender cómo se obtiene, se protege y se estudia la información de un dispositivo sin dañarla ni modificarla y cómo verificar si fue alterada.

Objetivos Específicos

Identificar y montar la memoria USB en el entorno de trabajo de Kali Linux para su análisis.

Generar el hash original del dispositivo USB y compararlo con el hash de su imagen forense para verificar la integridad de los datos.

Crear una imagen forense del dispositivo USB utilizando el comando dd en Kali Linux.

Analizar la imagen forense con Autopsy en entornos Linux y Windows, reconociendo las diferencias entre ambos sistemas.

Instalar y utilizar FTK Imager para examinar la imagen forense, identificando posibles archivos relevantes y comprendiendo la estructura del análisis digital.

Entorno

Se trabajó en un entorno controlado conformado por una máquina virtual Kali Linux ejecutada en VirtualBox, en la se desarrolló una actividad de auditoria forense.

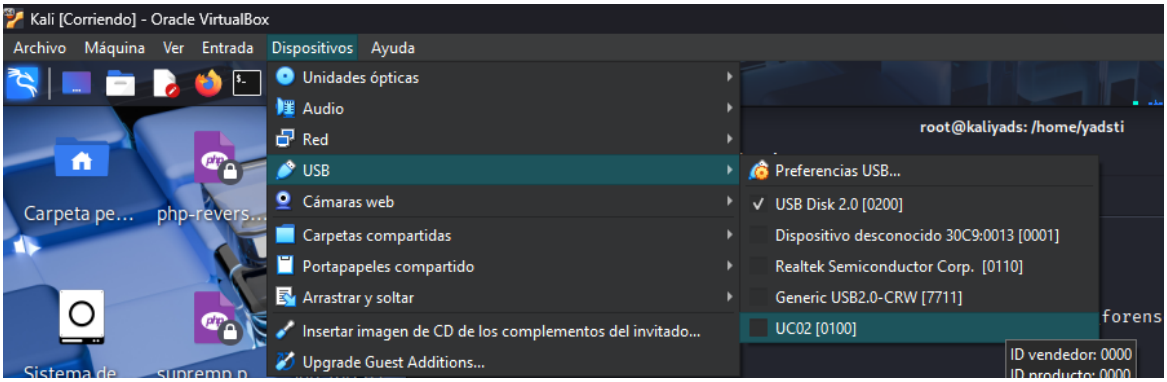
Desarrollo

Capítulo 1 – Autopsy Kali Linux

Identificación de USB y Creación del Hash

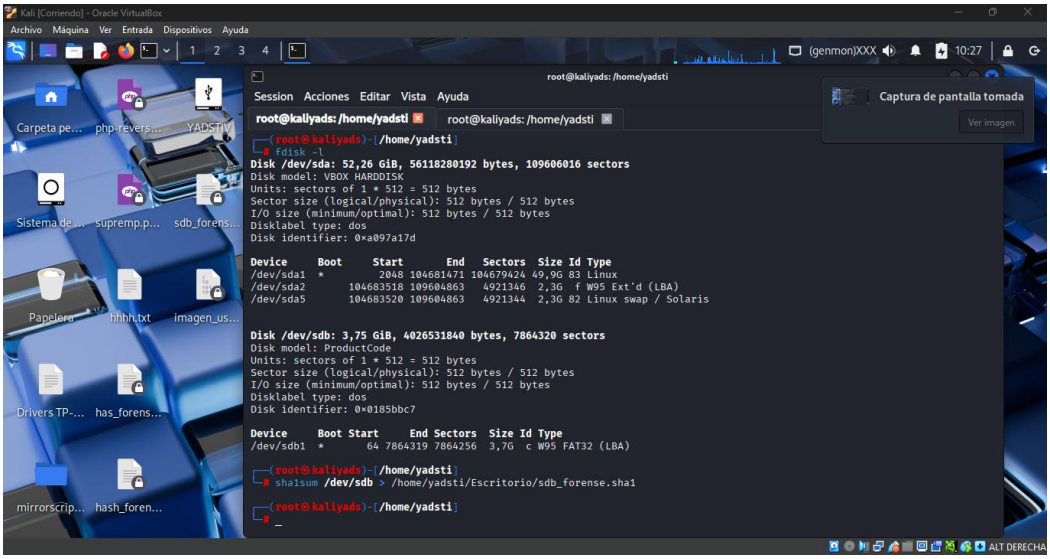
Luego iniciar la máquina virtual, se oprime la opción de **dispositivos** del virtual box, luego **USB** y se selecciona el dispositivo USB.

Ilustración 1 Selección de dispositivo USB



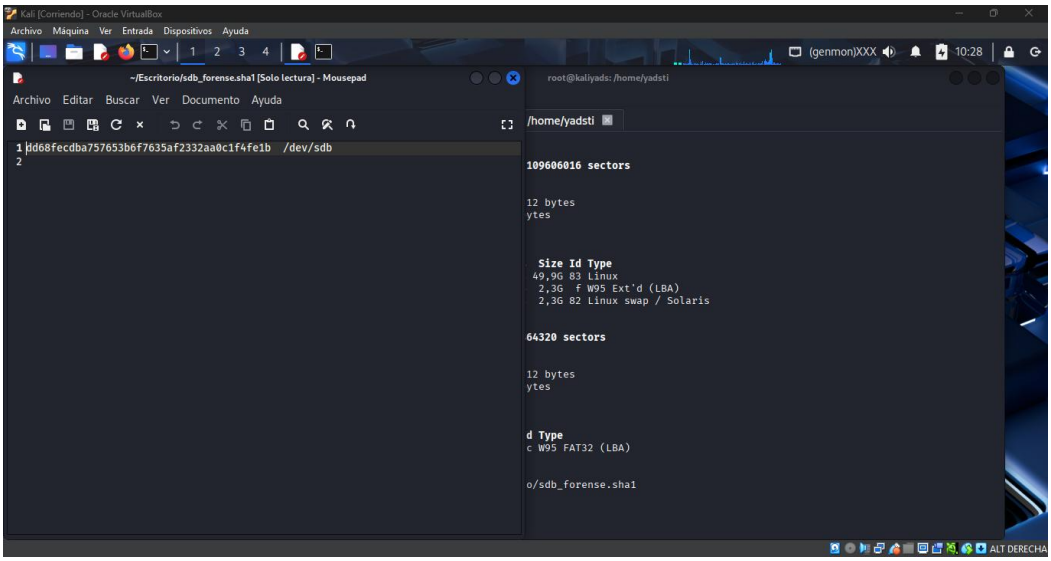
Posteriormente se abre una terminal y se ejecuta el siguiente comando **fdisk -l**, este comando lista los discos y USB presentes en el sistema. De igual manera se observa que la USB es el **Disk /dev/sdb**. A esta USB se procede a hacerle un hash, utilizando el comando **sha1sum /dev/sdb > /home/yadsti/Escritorio/sdb_forense.sha1.** Este comando crea un archivo con el nombre **sdb_forense.sha1** que contiene el hash de la USB.

Ilustración 2 Identificación de memoria USB y creación del hash1



El contenido del archivo **sdb_forense.sha1** es el siguiente:

Ilustración 3 Hash1 USB



Creación de la Imagen de la USB

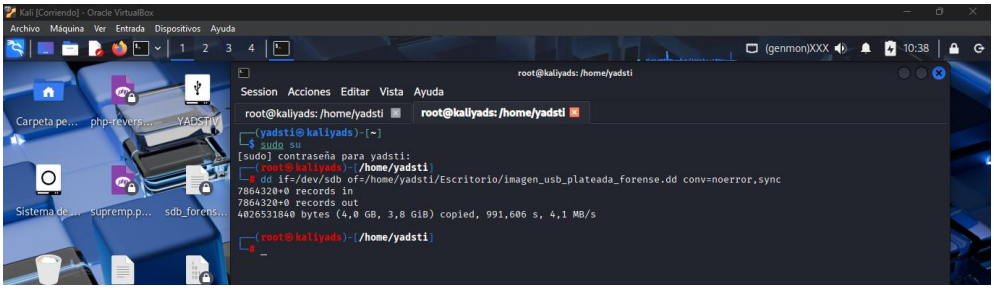
Ahora se le sacará una imagen (copia) a la USB y luego a esa imagen se le saca un hash. El hash original y el hash de la imagen deben de ser el mismo.

Para crear la imagen se utiliza el siguiente comando:

dd if=/dev/sdb of=/home/yadsti/Escritorio/imagen_USB_plateada_forense.dd conv=noerror,sync

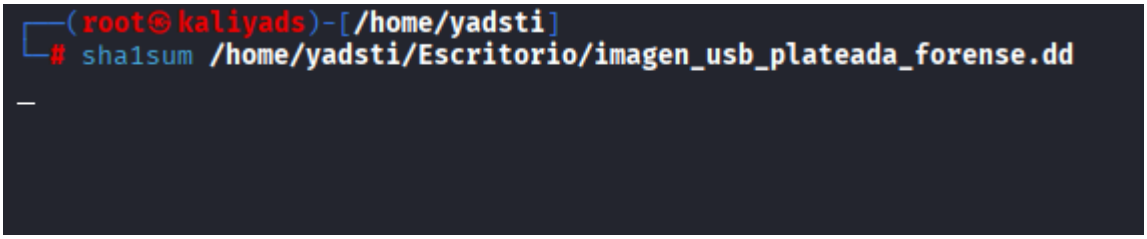
Este comando crea una imagen con el nombre **imagen_USB_plateada_forense.dd**

Ilustración 4 Creación de imagen USB



Al terminar la creación de la imagen, queda un archivo con el nombre **imagen_USB_plateada_forense.dd.** A continuación, se procede con la creación del hash de esta imagen de la USB, utilizando el comando: **sha1sum /home/yadsti/Escritorio/imagen_USB_plateada_forense.dd**

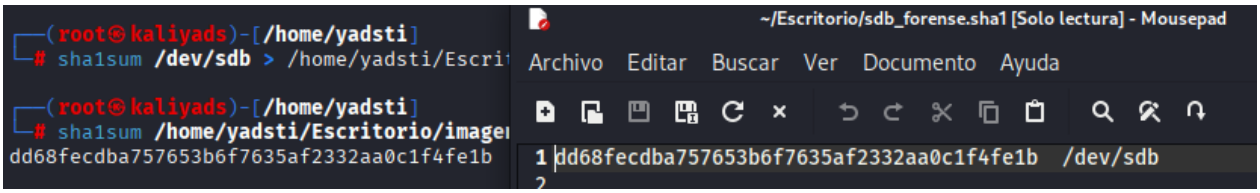
Ilustración 5 Creación de hash de imagen



Comparación de Hash Original y Hash de la Imagen (Copia)

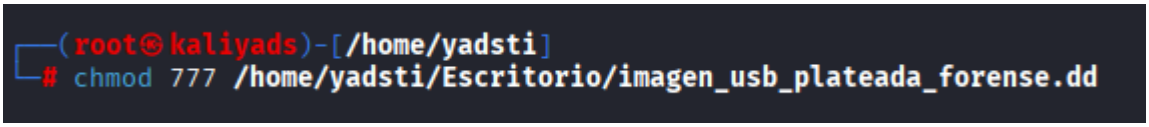
Una vez el proceso de elaboración del hash se procede con la comparación del hash original y el hash de la imagen, y cómo se evidencia el hash coincide, lo que quiere decir que la USB no ha sido modificada, su información sigue siendo integra.

Ilustración 6 Comparación de hash original y hash imagen USB



Se procede a desbloquear la imagen, que es básicamente es darle todos los privilegios y permisos utilizando el siguiente comando: **chmod 777 /home/yadsti/Escritorio/imagen_usb_plateada_forense.dd**, como se evidencia la siguiente ilustración:

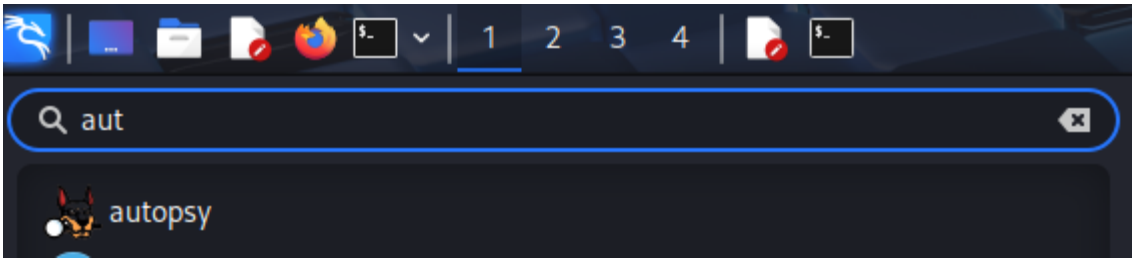
Ilustración 7 Asignación de privilegios y permisos imagen



Autopsy

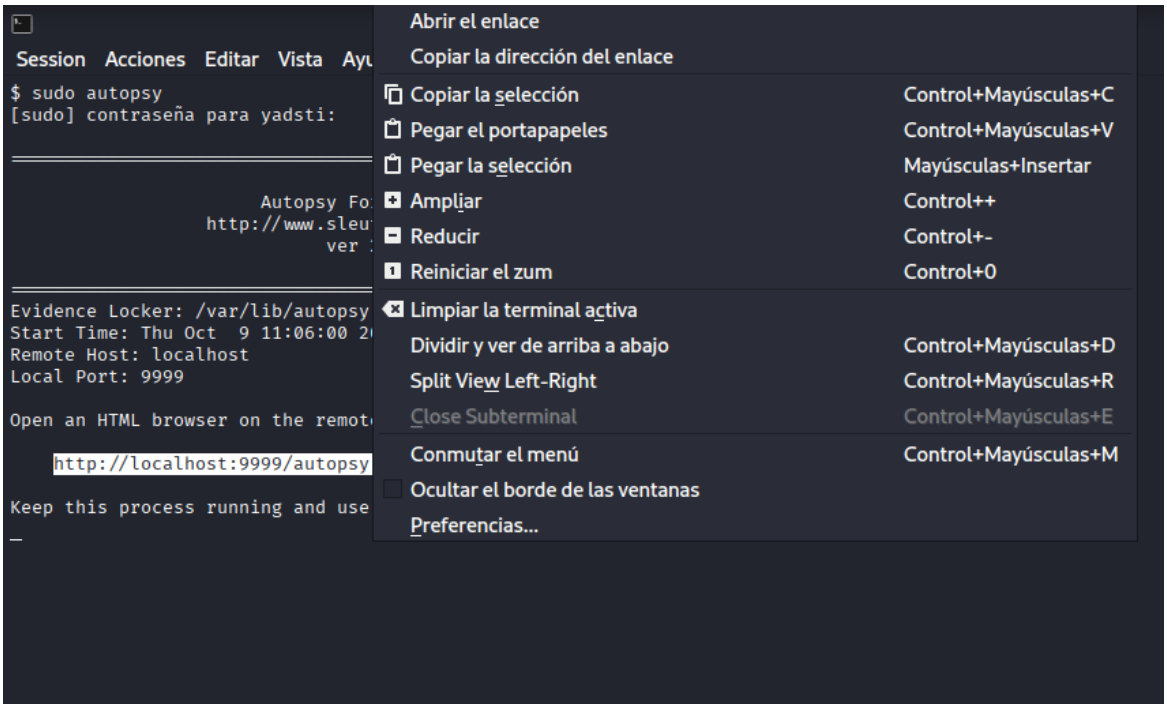
Luego de que se le dan todos los permisos y se desbloquea el archivo (imagen de la usb), se procede a buscar en el menú de Kali Linux la herramienta de autopsy y se ejecuta.

Ilustración 8 Búsqueda de autopsy



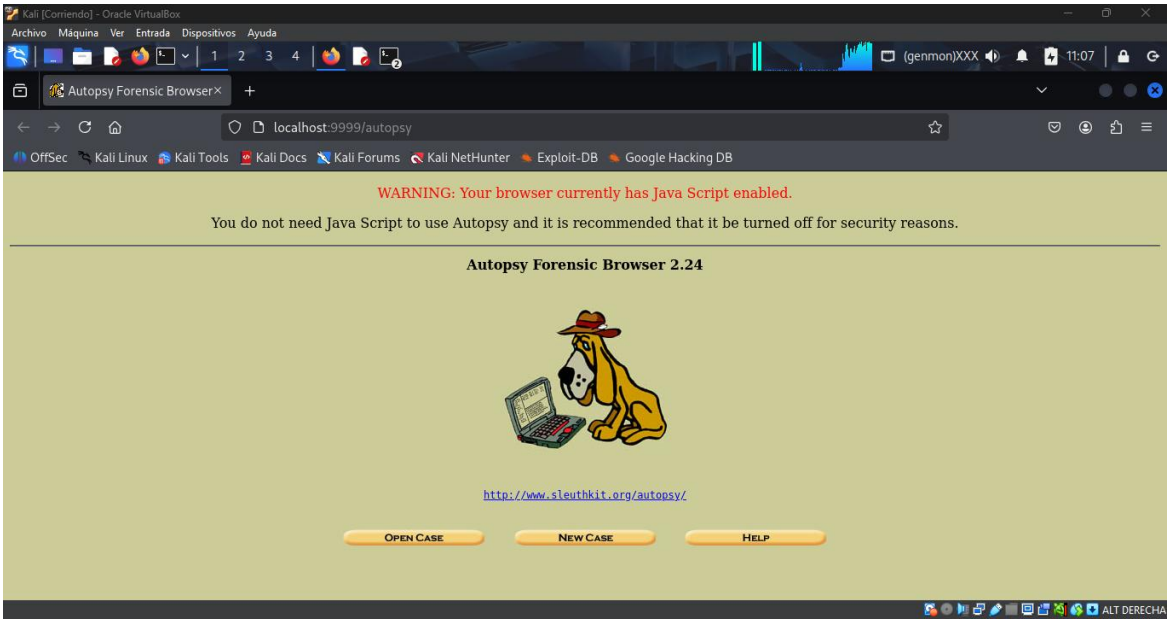
Al ejecutar la herramienta de autopsy, automáticamente se abre una consola de comando, que pide autenticación sudo, luego de la autenticación exitosa, se evidencia un saludo y adicional un enlace que es lo importa.

Ilustración 9 Consola autopsy



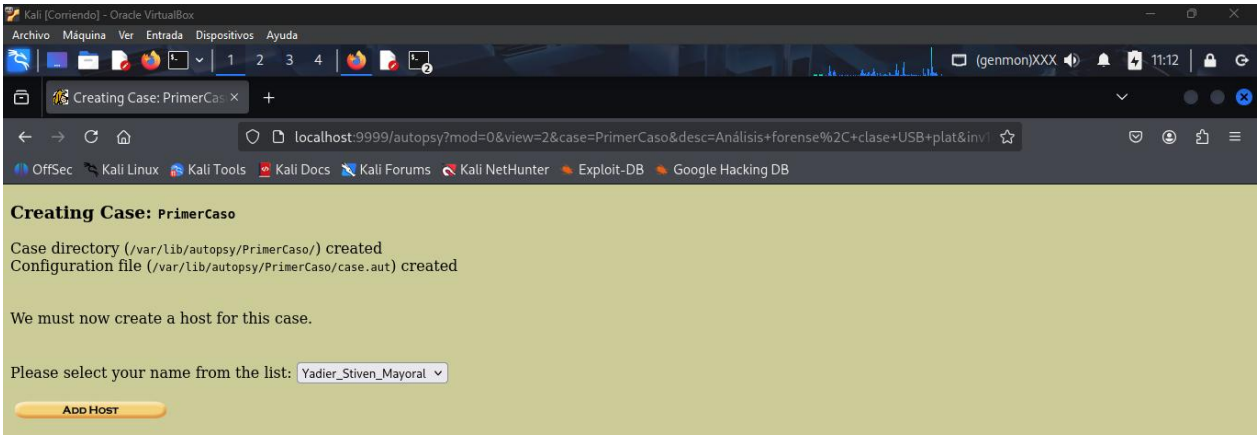
Cuando se ingresa a la URL se observa la pagina de autopsy, aparecen tres diferentes opciones (open case, new case, help), en este caso se selecciona la opción de new case.

Ilustración 10 New case



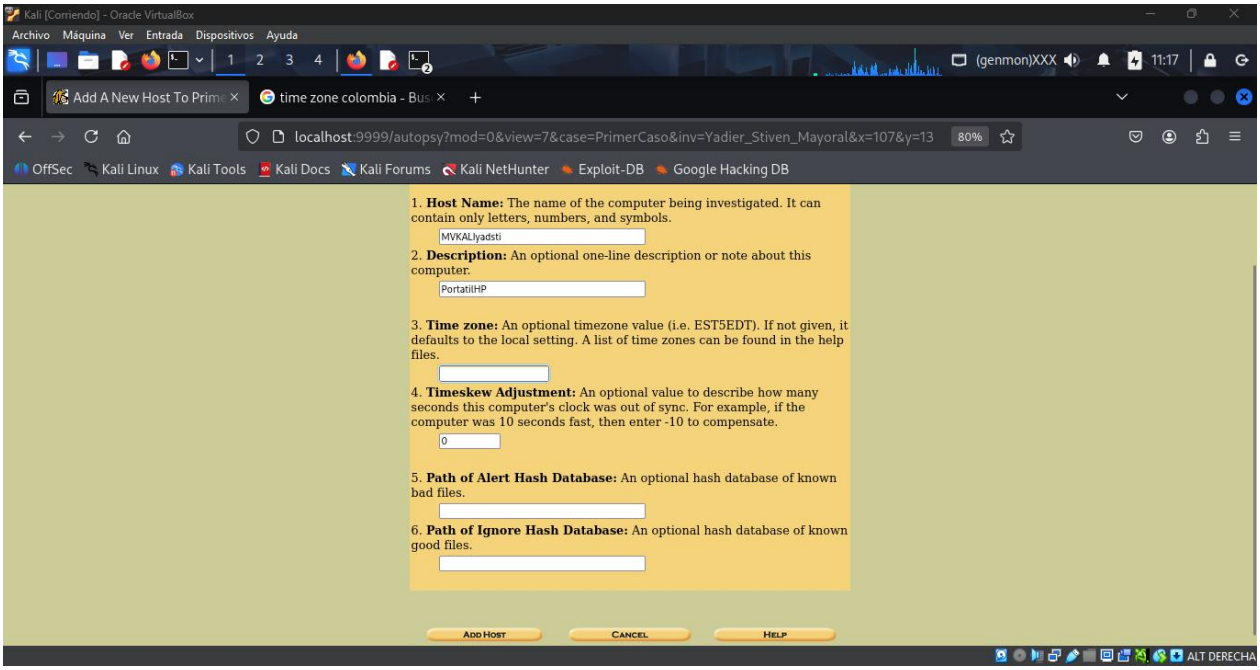
Luego de crear el case, el sitio lleva a una página que contiene información del caso que se está creando, adicionalmente el nombre de quien está creando el caso y una opción de add host (añadir dispositivo).

Ilustración 11 añadir dispositivo



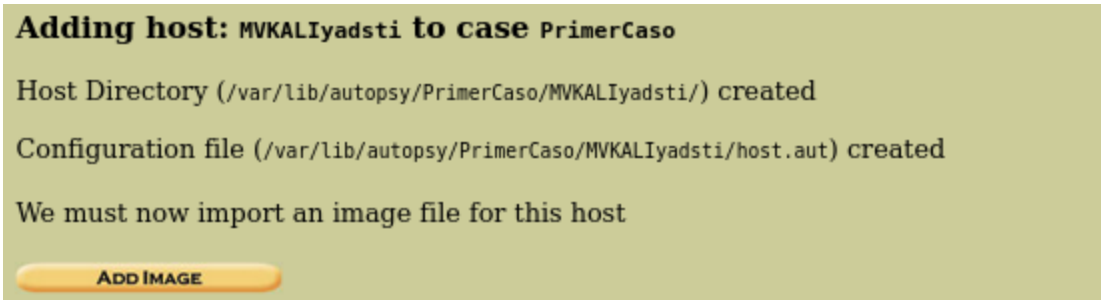
Al oprimir dicha opción se abre una nueva pagina que pide el nombre del dispositivo, descripción, entre otros datos. Se llenan los que se deseen y nuevamente se oprime la opción de add host.

Ilustración 12 new host



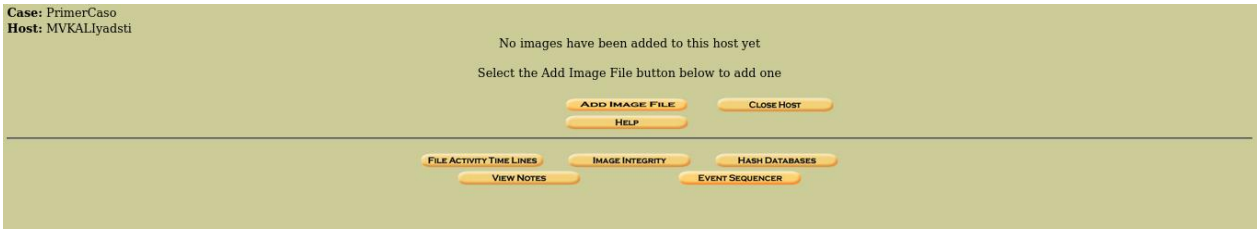
Se oprime la opción de add image.

Ilustración 13 add image



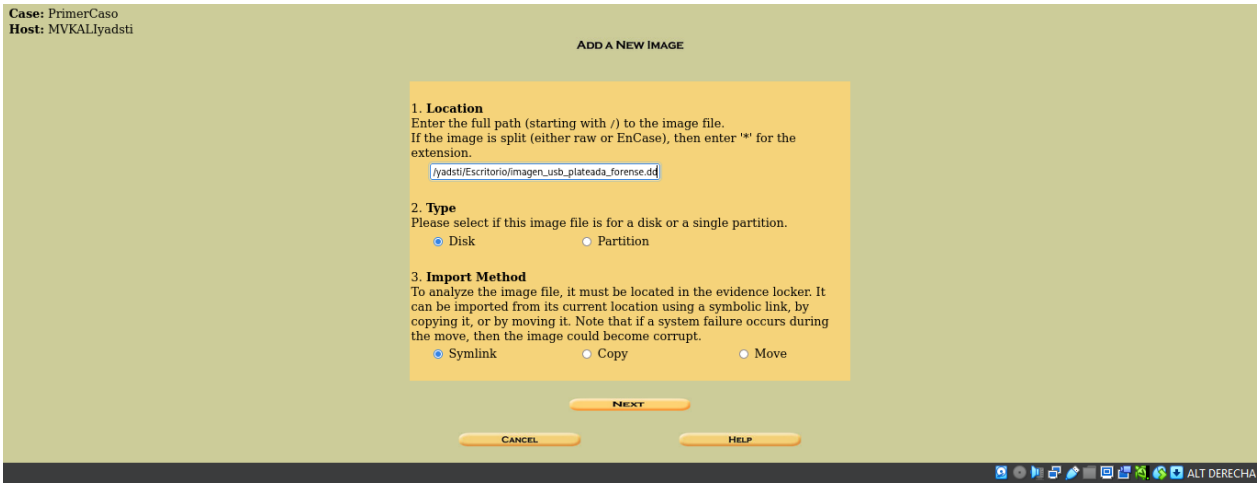
Se oprime el botón de add image file.

Ilustración 14 image file



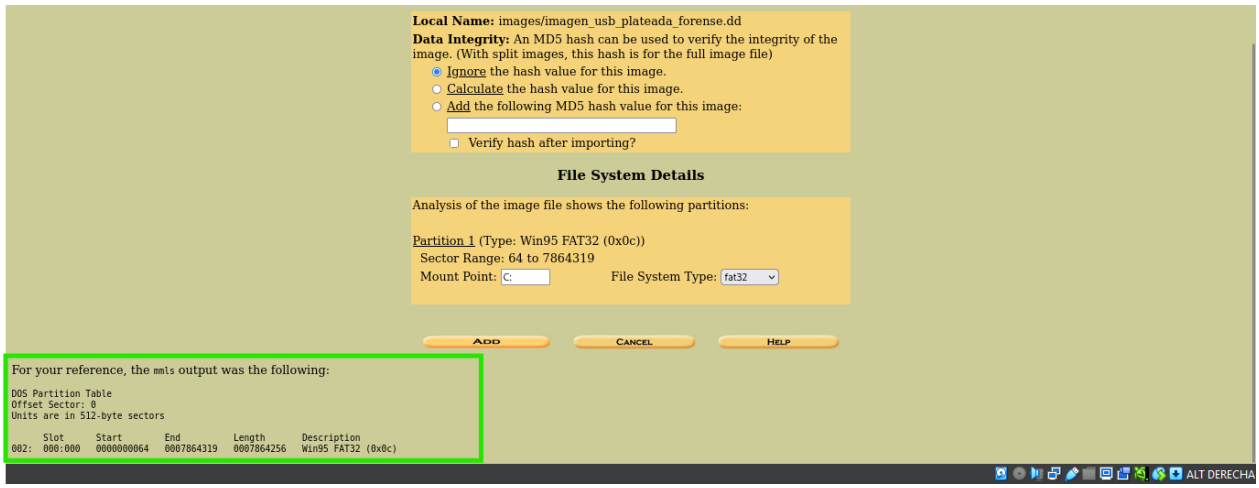
El formulario solicita la ruta de la imagen creada anteriormente, el tipo, se selecciona disk, y luego pide el método de importación, se selecciona el primero.

Ilustración 15 ruta imagen



Luego aparece un resumen y muestra características de la imagen, como por ejemplo el sistema de archivos.

Ilustración 16 resumen imagen

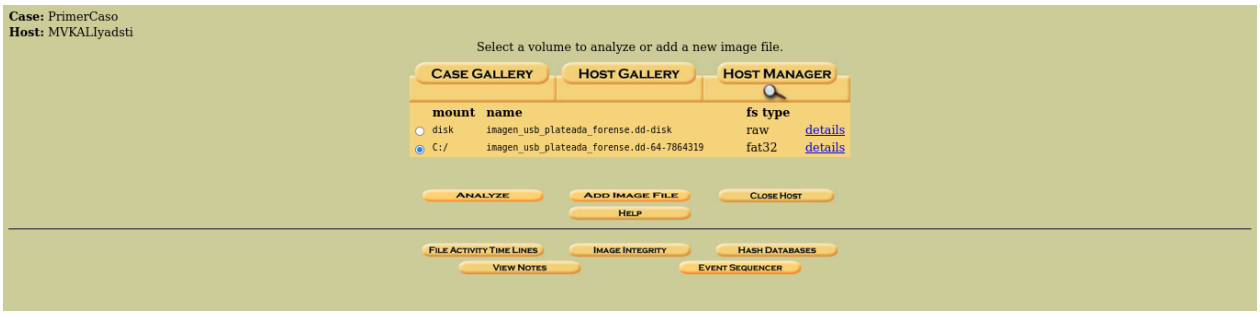


Una vez se ve el resumen, se oprime la opción de add, luego aparece una descripción de la imagen, se oprime la opción de add image.

Ilustración 17 Información adicional

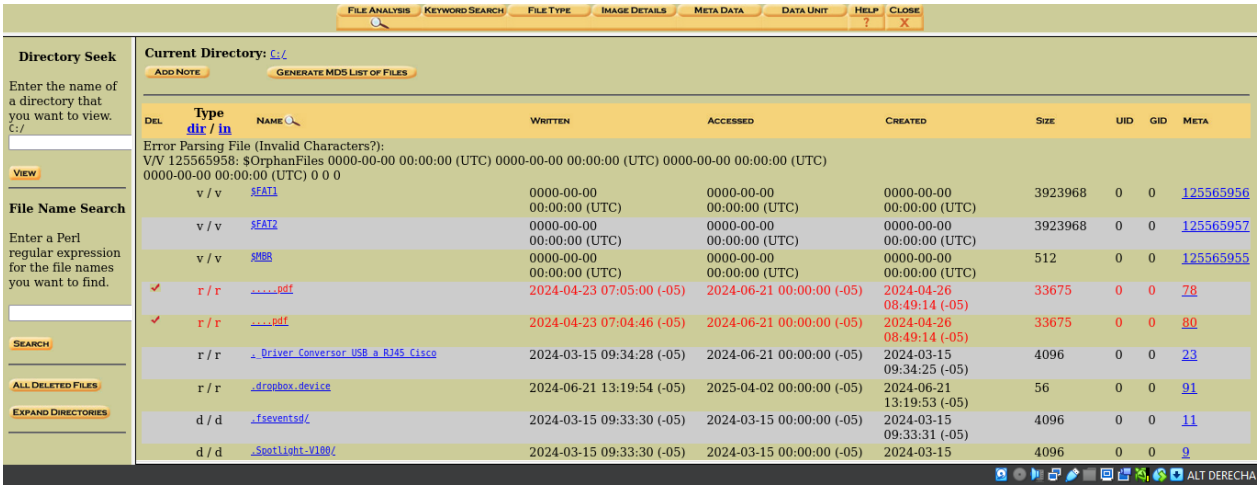
Una vez hecho eso, redirige a la siguiente ventana y se selecciona la opción de C:/ y se oprime analyze.

Ilustración 18 Análisis



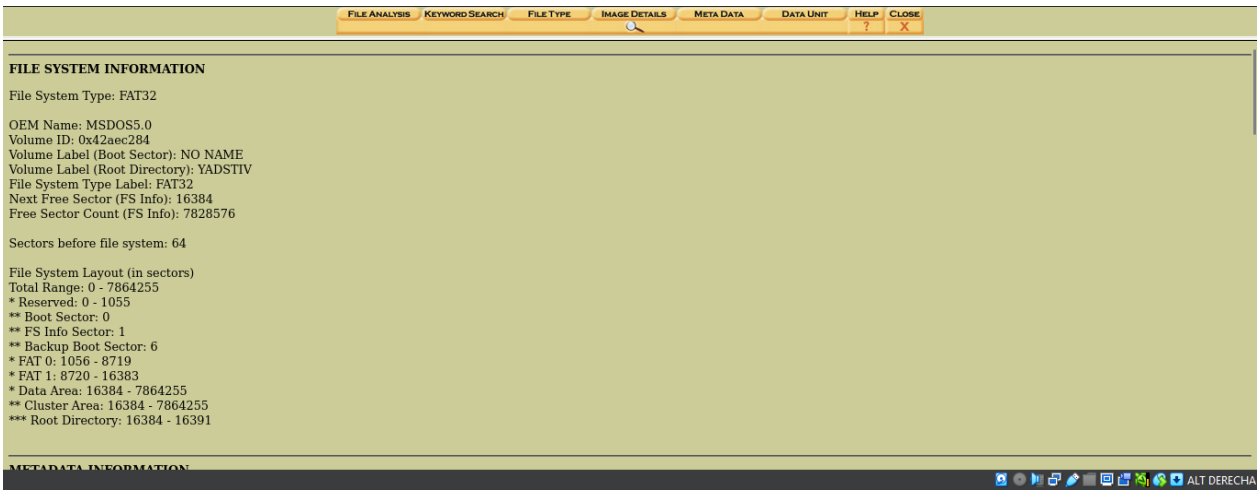
Se selecciona File Analysis y ahí aparecen los archivos que tiene la imagen actualmente, los eliminados subrayados en rojo, la fecha de escritura, de acceso, de creación, tamaña, entre otros datos relevantes.

Ilustración 19 File Analysis



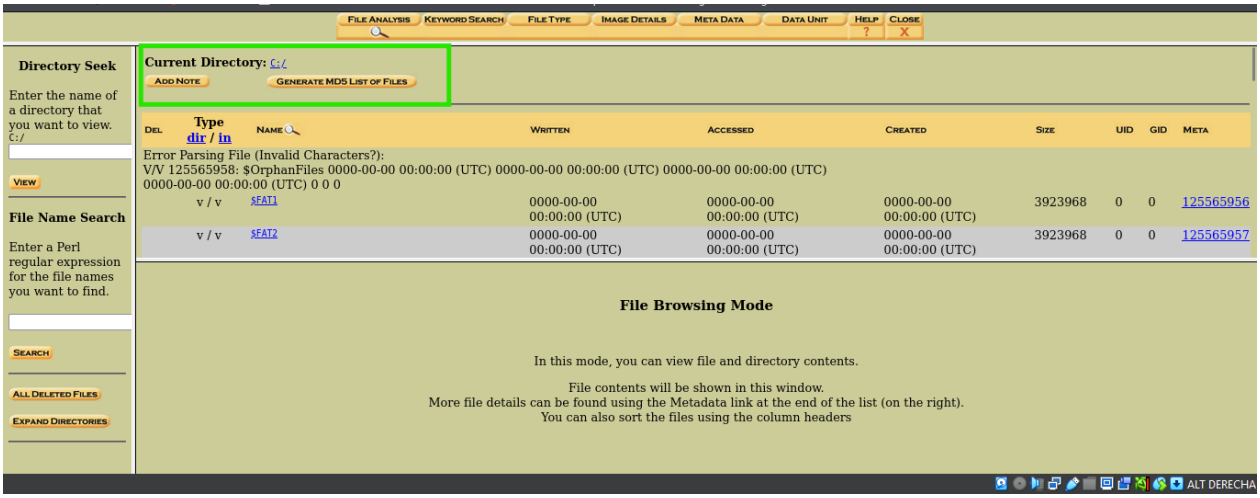
Luego se selecciona la opción de detalles de imagen, donde se obtiene información del tipo de sistema de archivos, el nombre del dispositivo.

Ilustración 20 Image Details



En la opción de File Analysis en la parte superior izquierda aparece la opción de Generate MD5 LIST OF FILES, esa opción generara el hash MD5 de los archivos a los que se accedieron como se evidencia a continuación:

Ilustración 21 Generate MD5



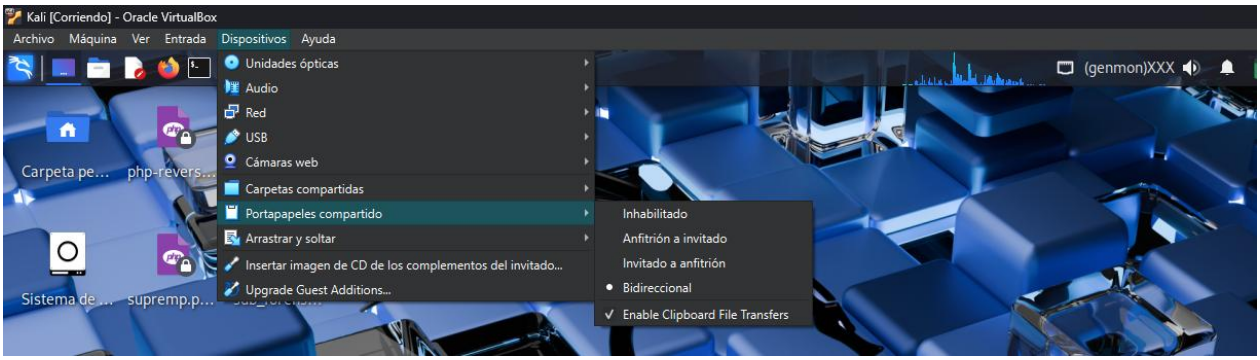
La opción genera los siguientes hashes:

Ilustración 22 Hash MD5 de archivos revisados

Pasando imagen de Kali a Linux

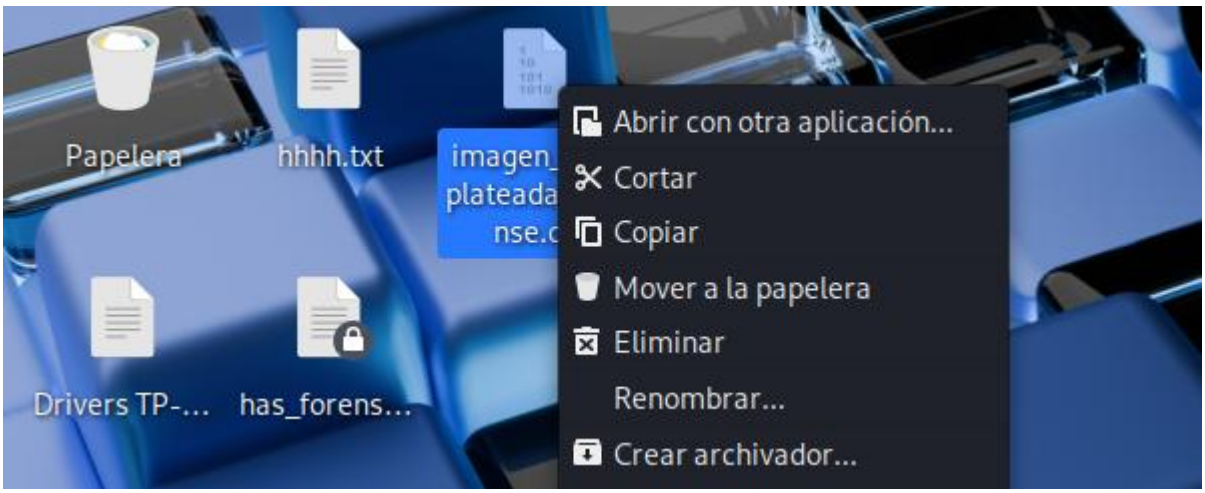
Para ello se oprime la opción de dispositivos, luego portapapeles compartido y se verifica que este en modo bidireccional y que tenga activada la opción de Enable Clipboard File Transfers, esta opción se activa para pasar archivos copiándolos desde Kali y pegándolos en el dispositivo principal.

Ilustración 23 Portapapeles compartido



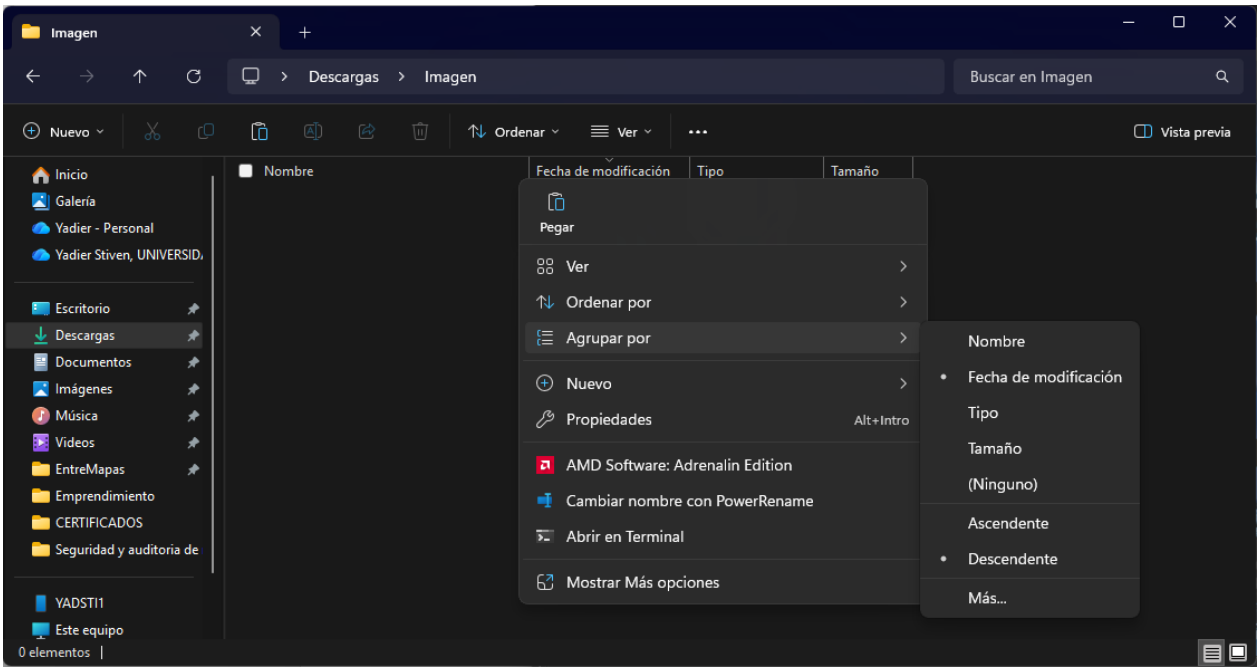
Luego hay que posicionarse sobre el archivo que quiere compartirse, en este caso el archivo llamado imagen_usb_plateada, click derecho sobre el archivo y se selecciona la opción de copiar.

Ilustración 24 Copiar imagen



En Windows se selecciona la carpeta donde se va a pegar el archivo y click derecha para seleccionar la opción de pegar y eso es todo. De esa forma se comparte la imagen de la usb.

Ilustración 25 Pegar imagen 1



El proceso de pegado inicia.

Ilustración 26 Pegando imagen

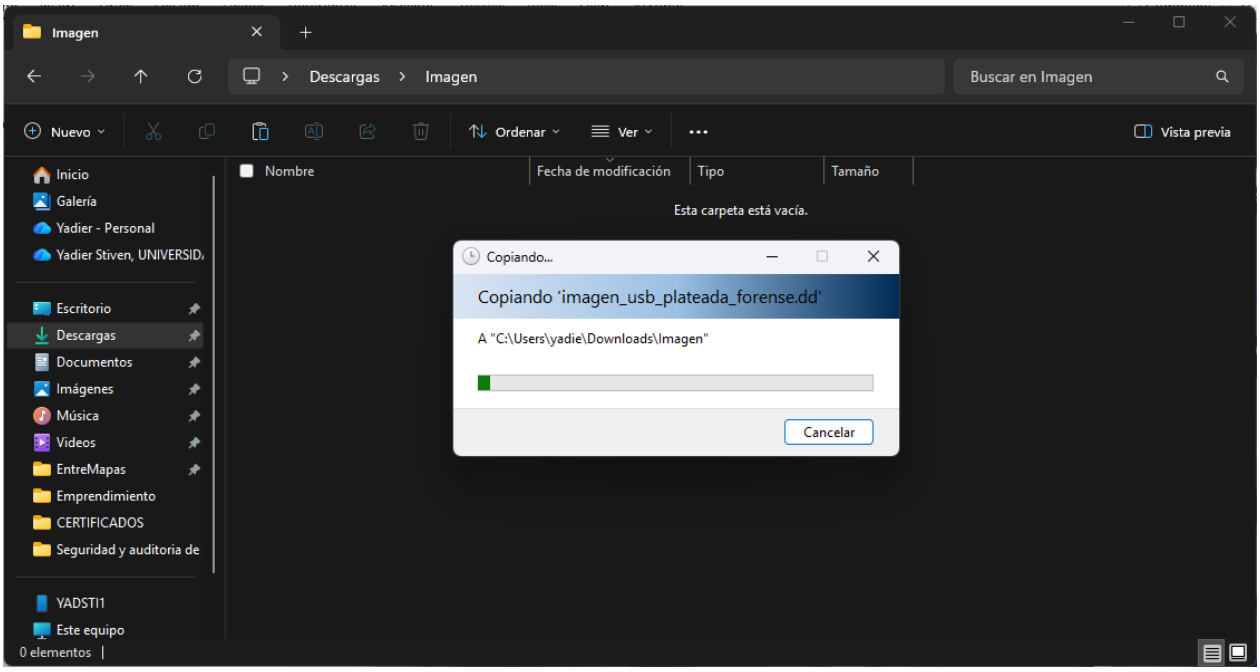
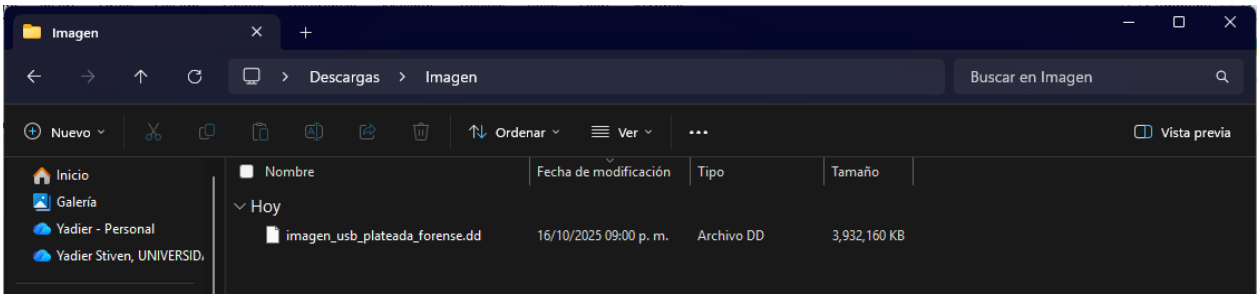


Ilustración 27 Imagen en windows

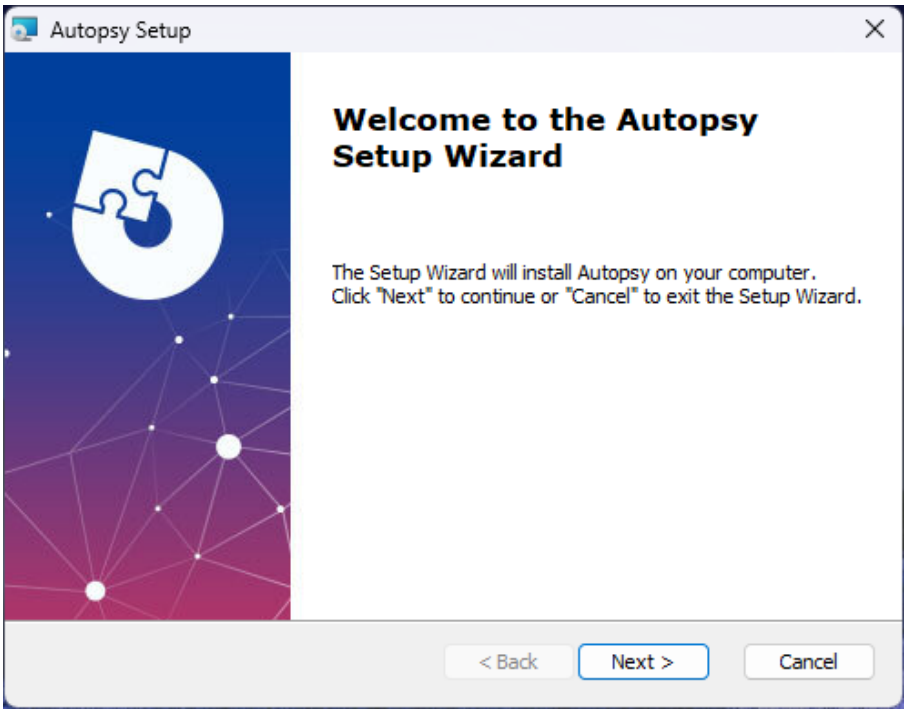


Ya con la imagen en Windows se puede proceder con lo demás.

Capitulo 2 – Autopsy en Windows (Instalación y revisión de imagen)

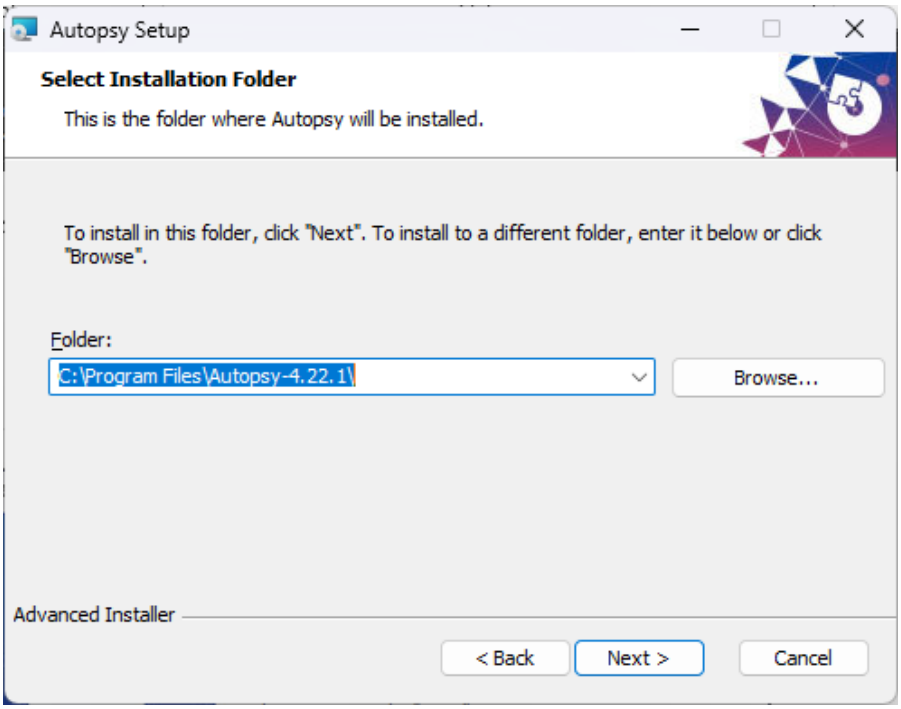
Instalación

El primer paso es ejecutar el instalador de Autopsy previamente descargado.



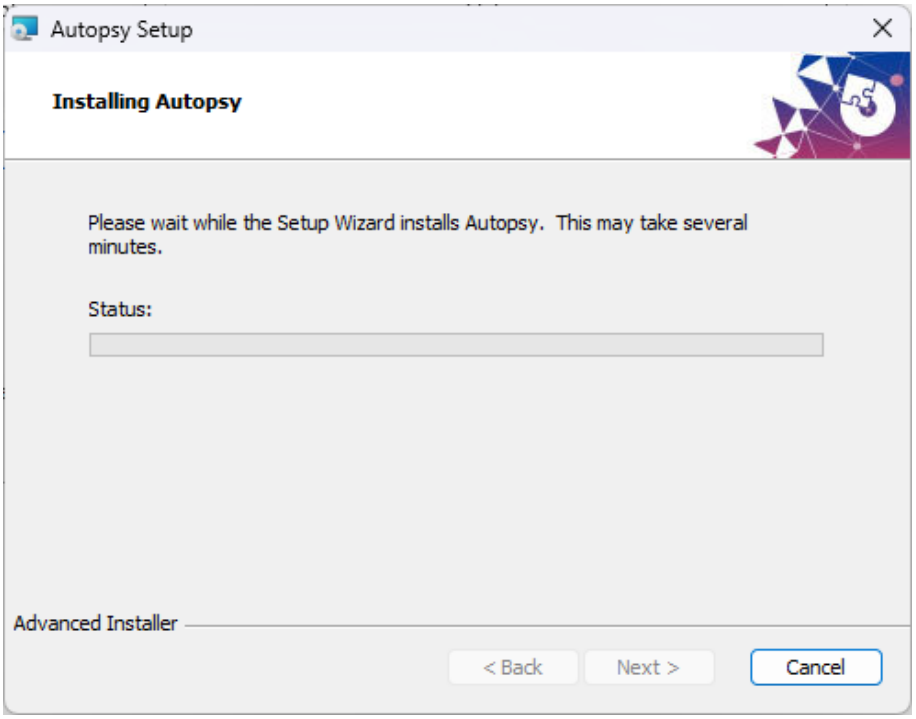
Se oprime la opción de next y luego se selecciona la ruta donde se desea instalar autopsy, en este caso se deja la ruta por defecto y next.

Ilustración 28 Ruta de instalación



El proceso de instalación inicia y solo queda esperar.

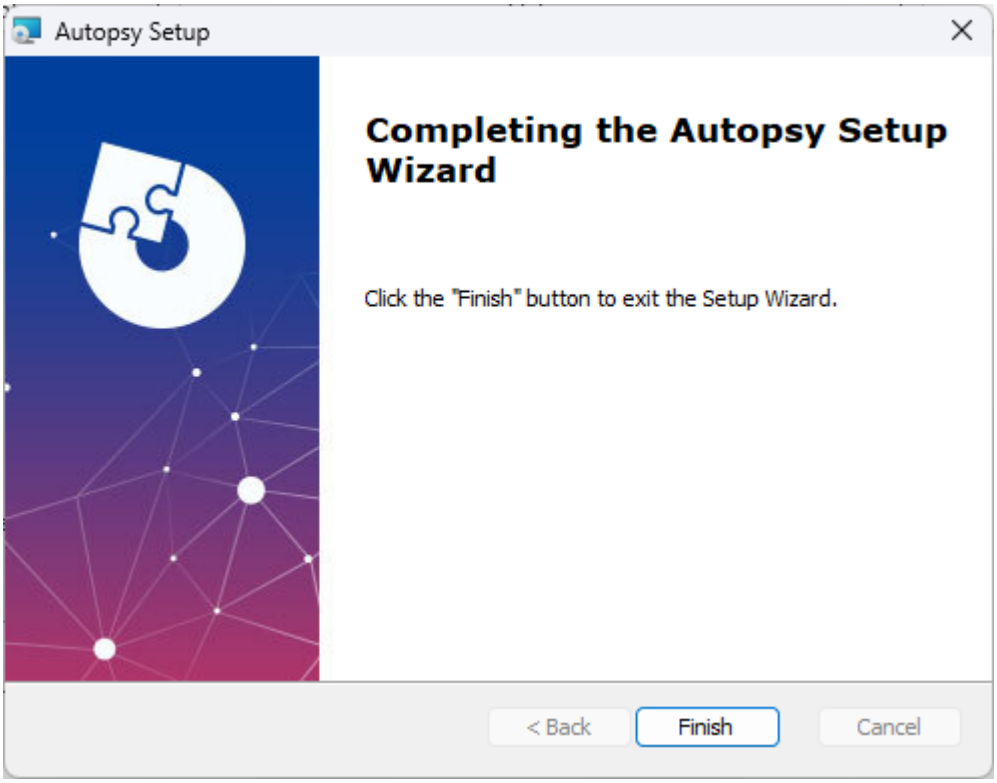
Ilustración 29 Inicio proceso de instalación



Aparece un mensaje del sistema pidiendo permiso y se acepta.

Una vez instalado aparece finalizado y se cierra

Ilustración 30 Autopsy instalado

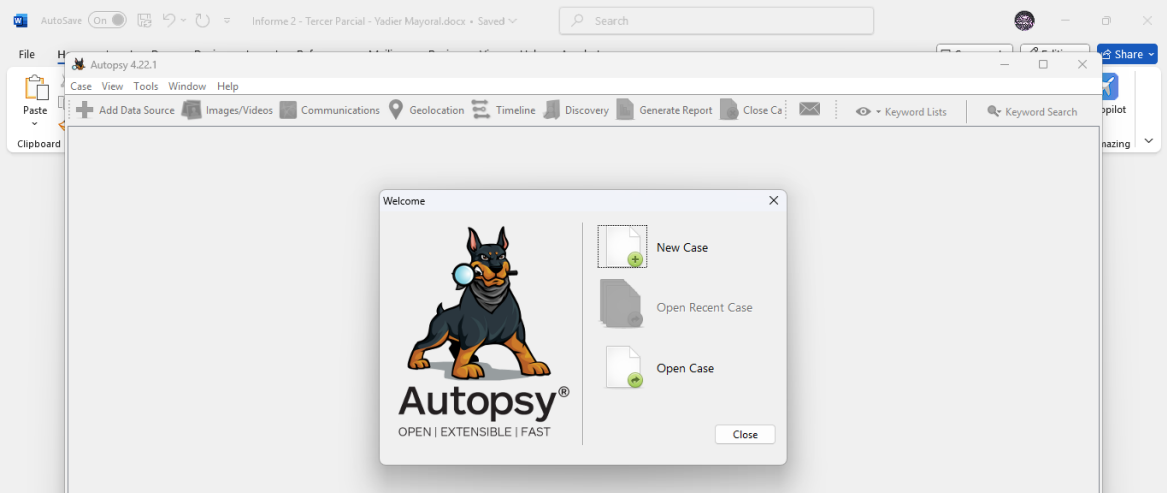


Luego se ejecuta la aplicación.

Análisis

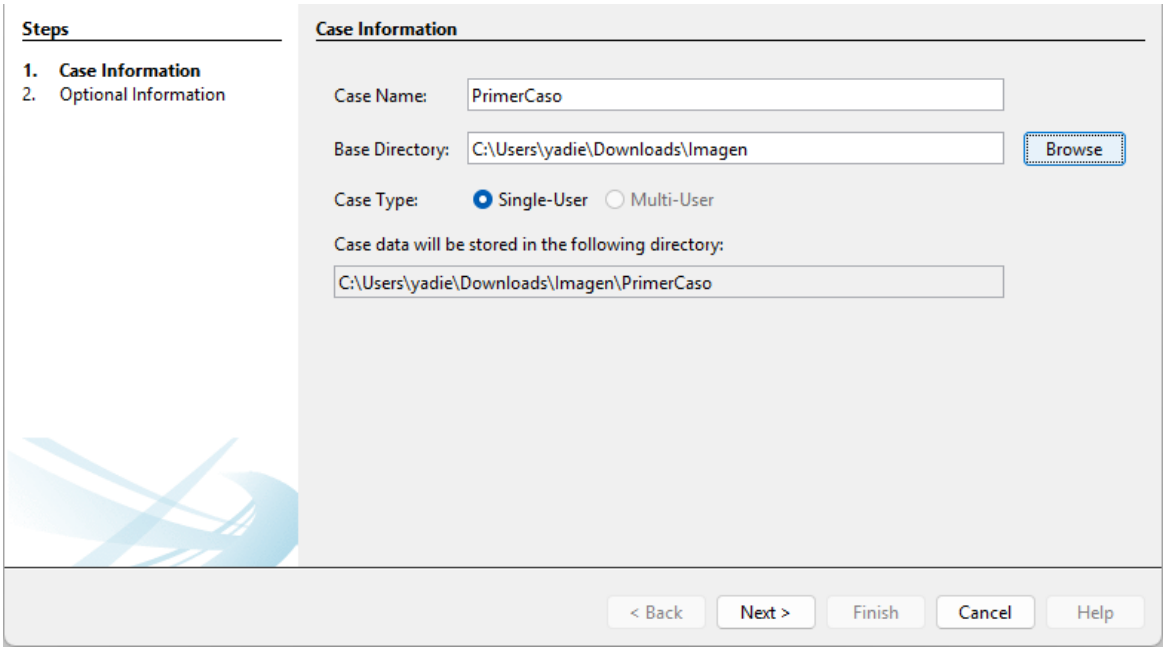
Se procede con la creación de un nuevo caso. Para ello se selecciona la opción de New Case.

Ilustración 31 New Case



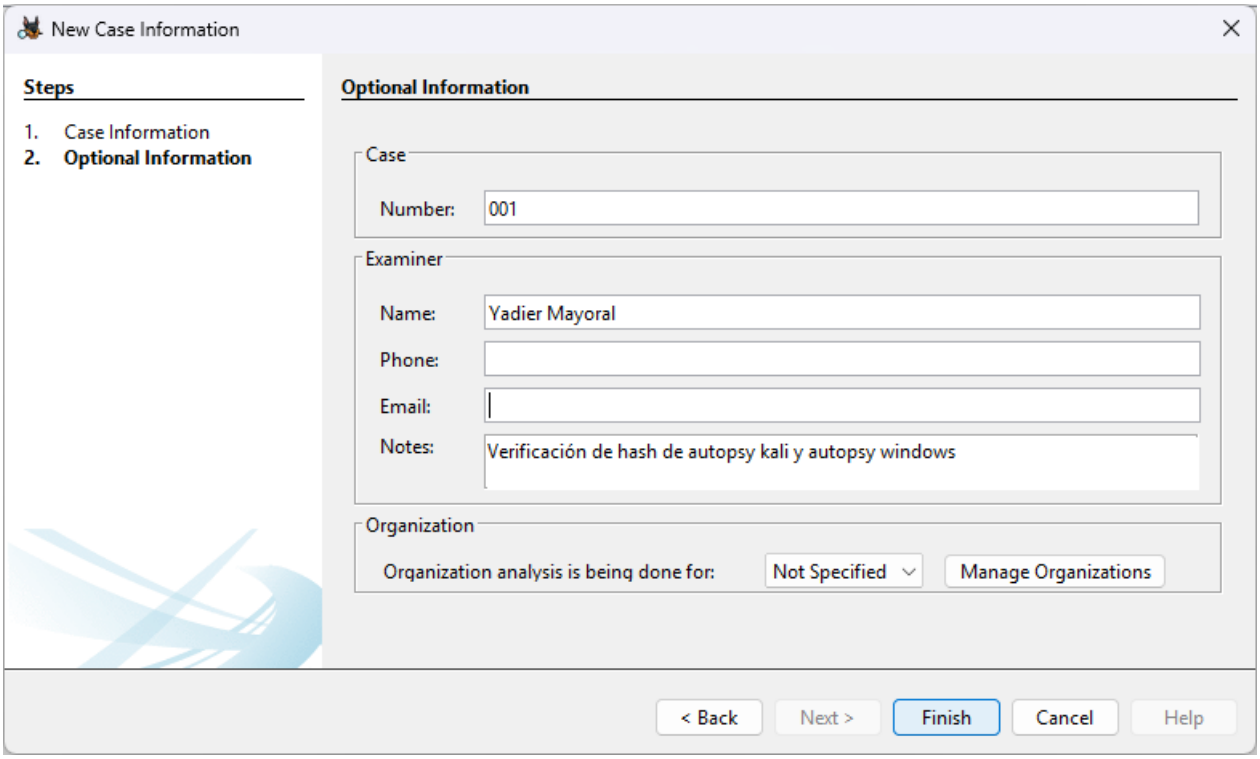
Se llena la información del caso, se selecciona el directorio del caso y se ve la ruta donde se va a almacenar todo.

Ilustración 32 Información del caso



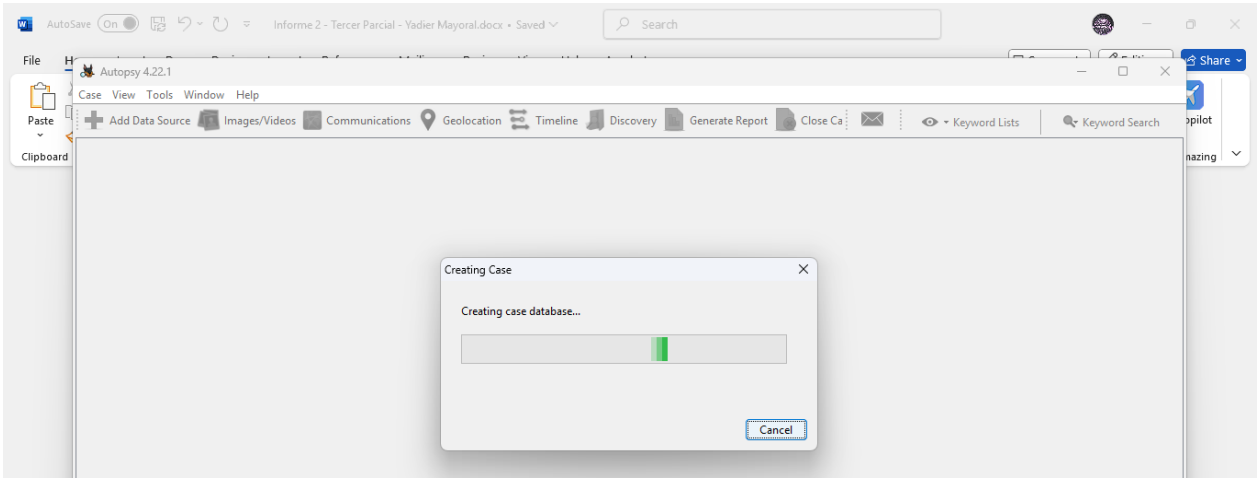
Luego se llena información adicional, como el nombre y otros datos del examinador.

Ilustración 33 Datos examinador



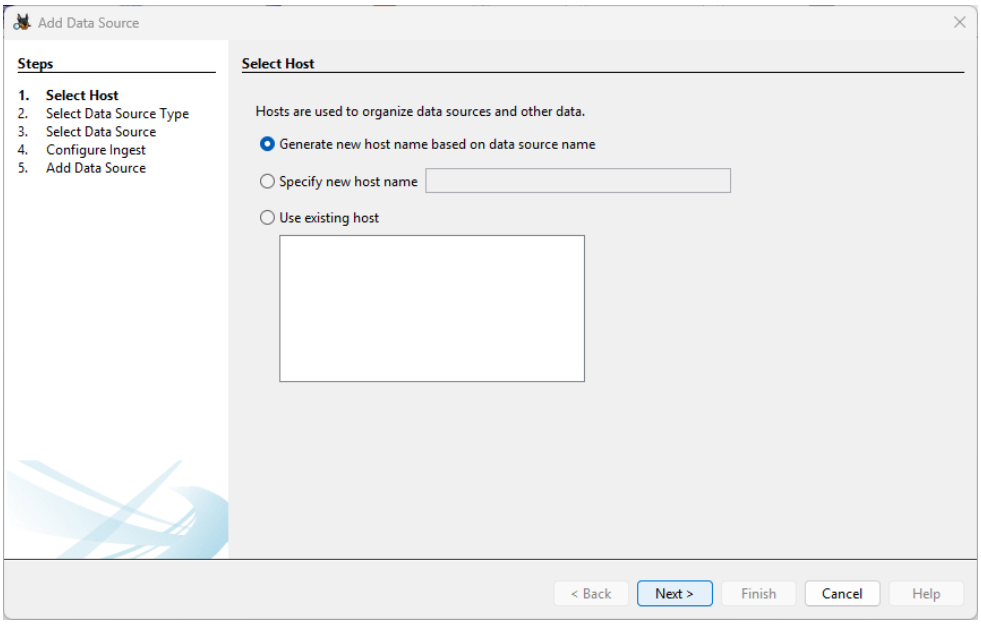
Luego el caso inicia su creación.

Ilustración 34 Creación del caso



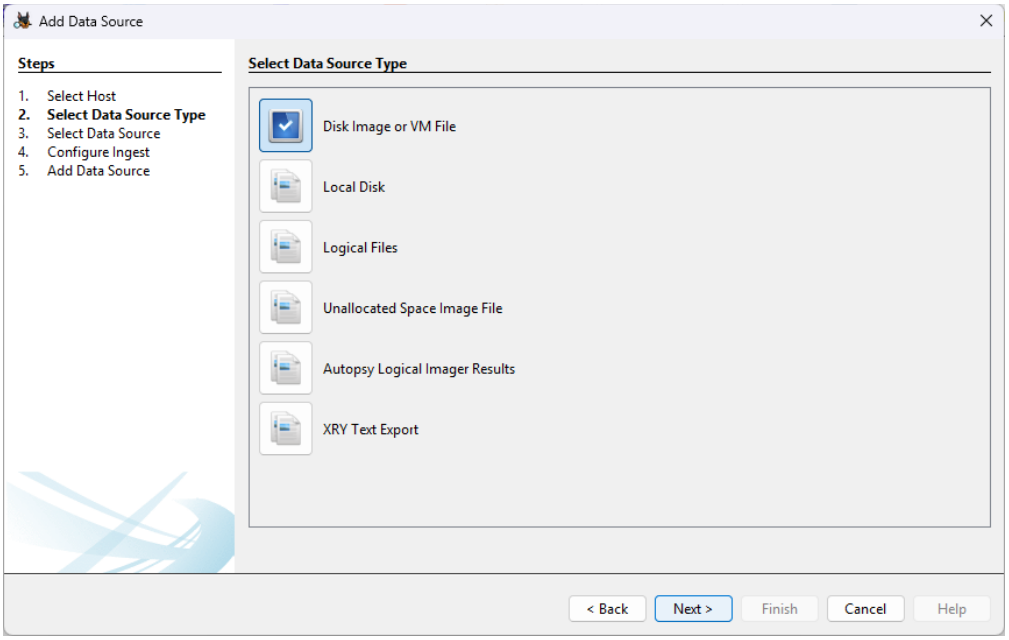
Una vez el caso se termina de crear se procede con la elección del dispositivo, se selecciona la primera opción y siguiente.

Ilustración 35 Seleccionar dispositivo



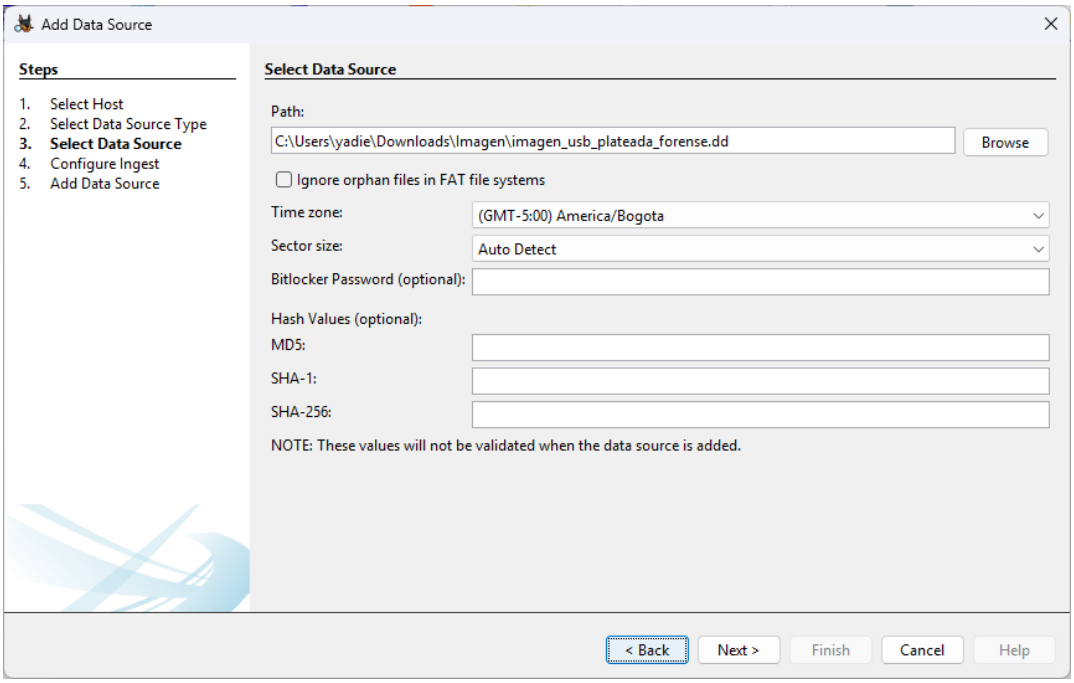
Primera opción nuevamente, ya que se va a analizar la imagen de un dispositivo.

Ilustración 36 Selección de tipo de origen de datos



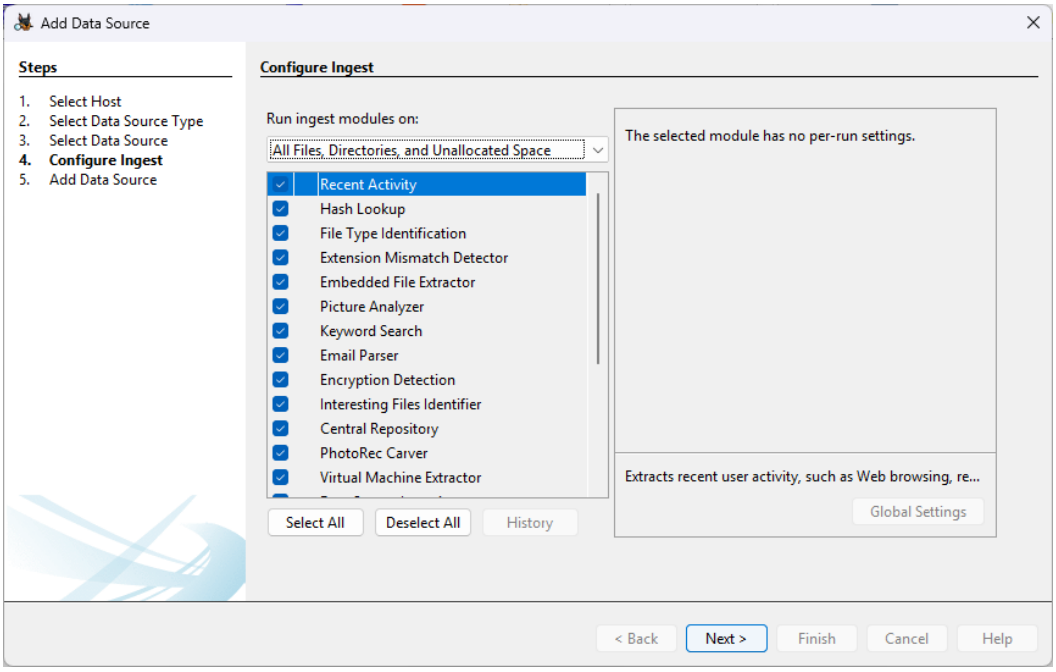
Luego se procede con la selección del archivo de la imagen como se evidencia a continuación.

Ilustración 37 Selección de imagen



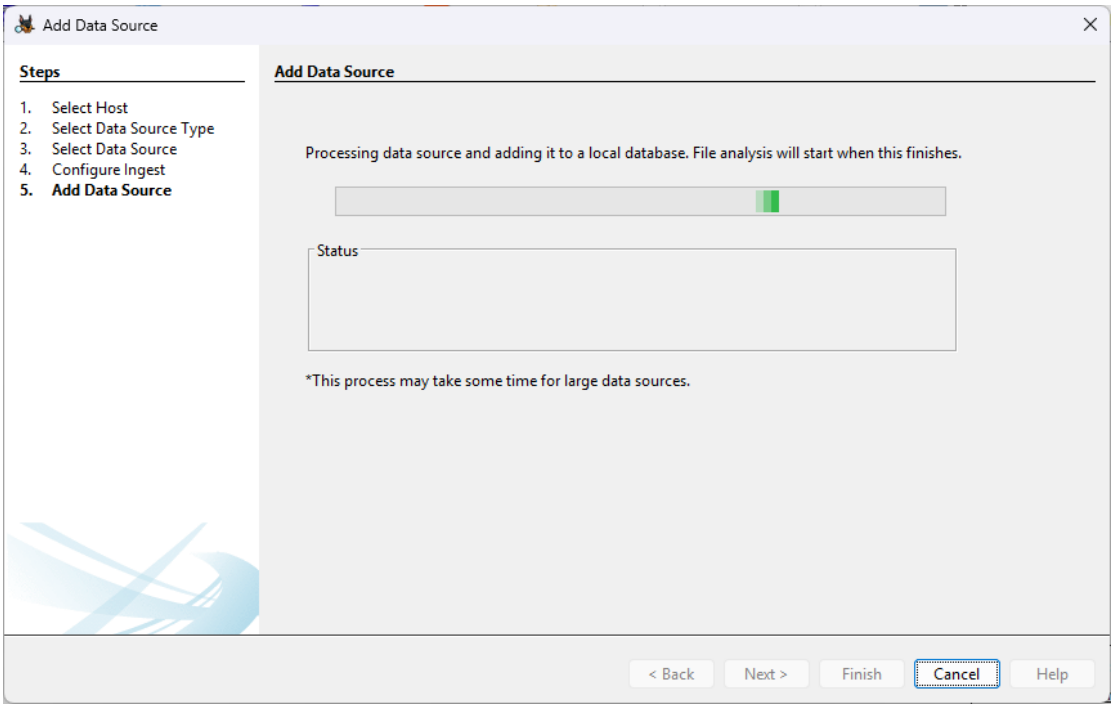
Luego se procede a configurar los tipos de análisis a realizar, se seleccionan todos.

Ilustración 38 Selección de tipos de análisis



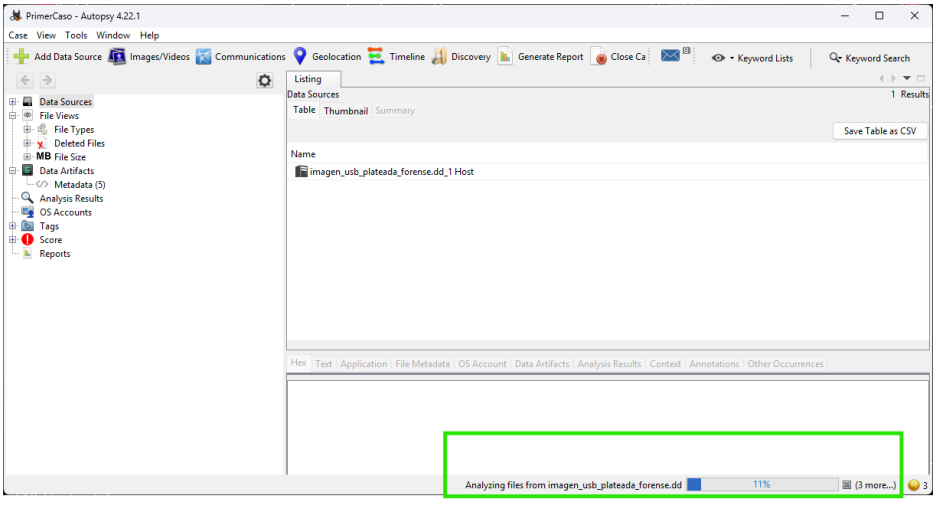
Inicia el proceso de cargue de la imagen en Autopsy.

Ilustración 39 Imagen cargando



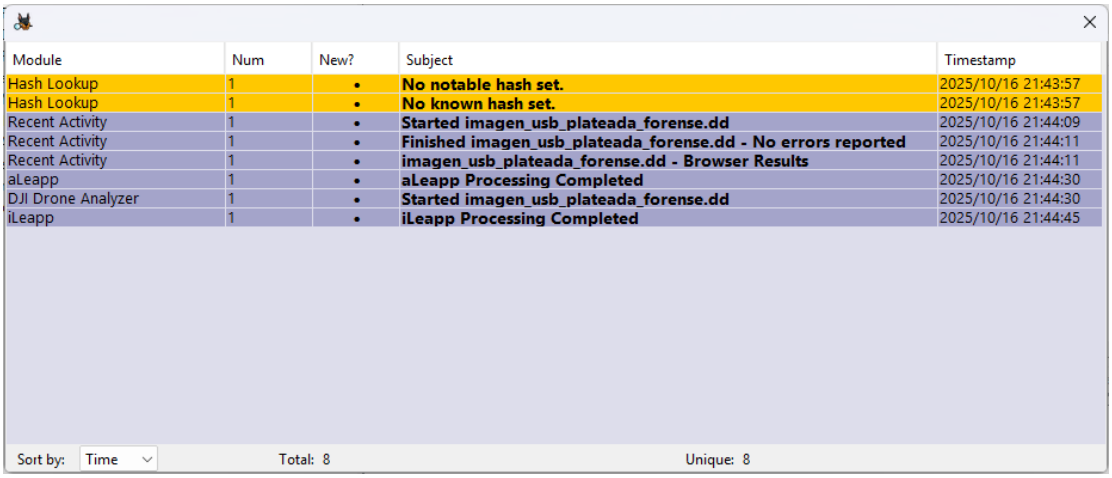
Una vez el proceso de cargue de la imagen sea satisfactorio aparece una ventana dando dicho mensaje, se cierra y se inicia con la exploración de Autopsy. Como se puede evidenciar tiene un panel izquierdo donde aparece un árbol de información, como la entrada de datos, los tipos de datos, los tipos de archivos, la cantidad, los eliminados, entre otros. El análisis de la información apenas comienza.

Ilustración 40 Inspección



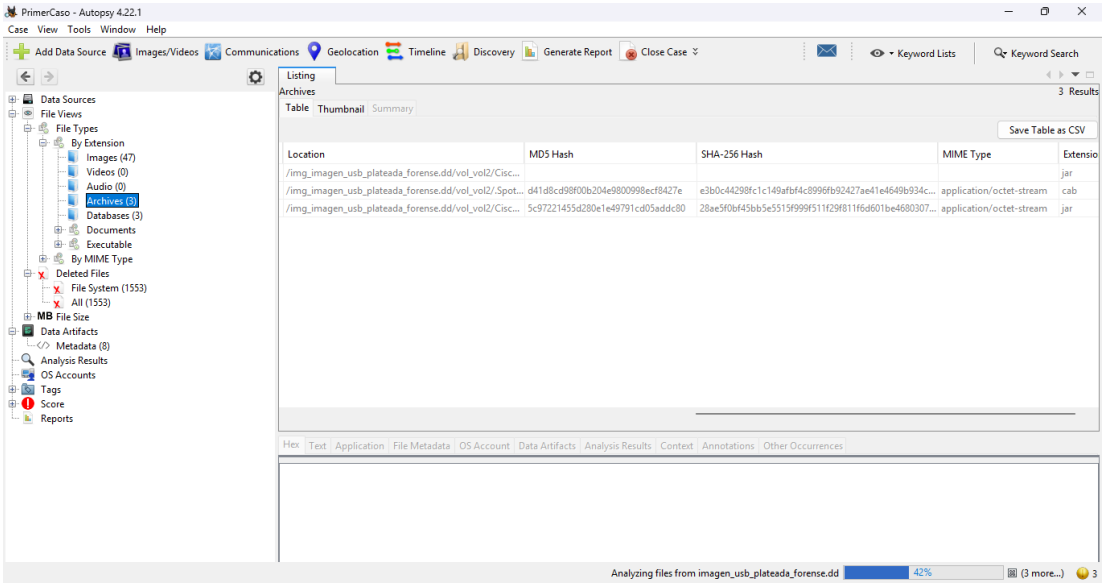
Autopsy automáticamente inicia con el análisis de la imagen y muestra una ventana donde detalla el módulo, el asunto y la fecha de lo que va haciendo.

Ilustración 41 Log de análisis



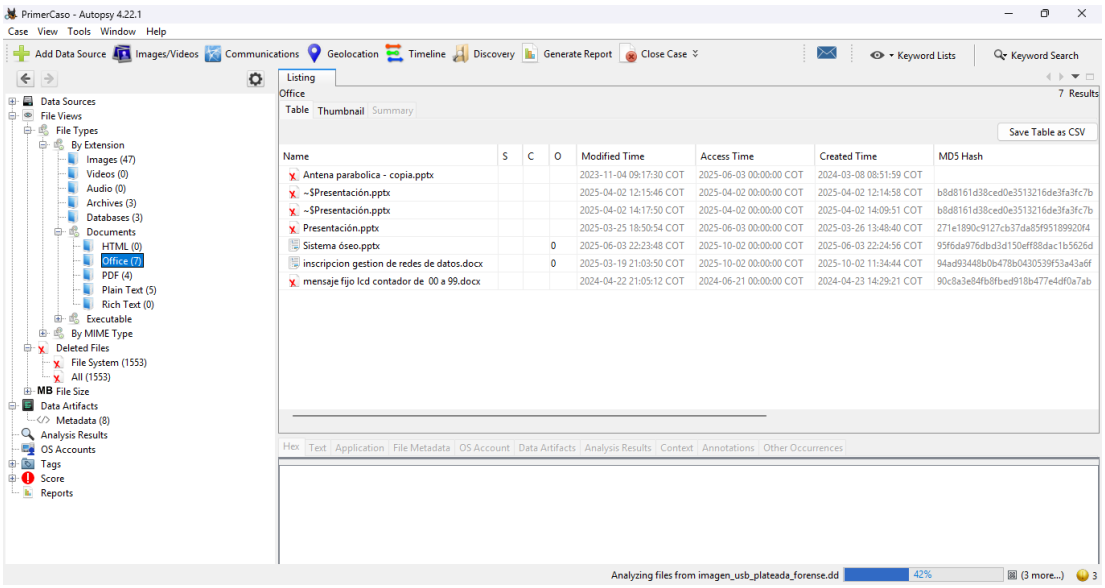
Este proceso tarda dependiendo de las capacidades del dispositivo donde se están haciendo las labores del análisis forense.

Ilustración 42 Inspección de archivos por extensión



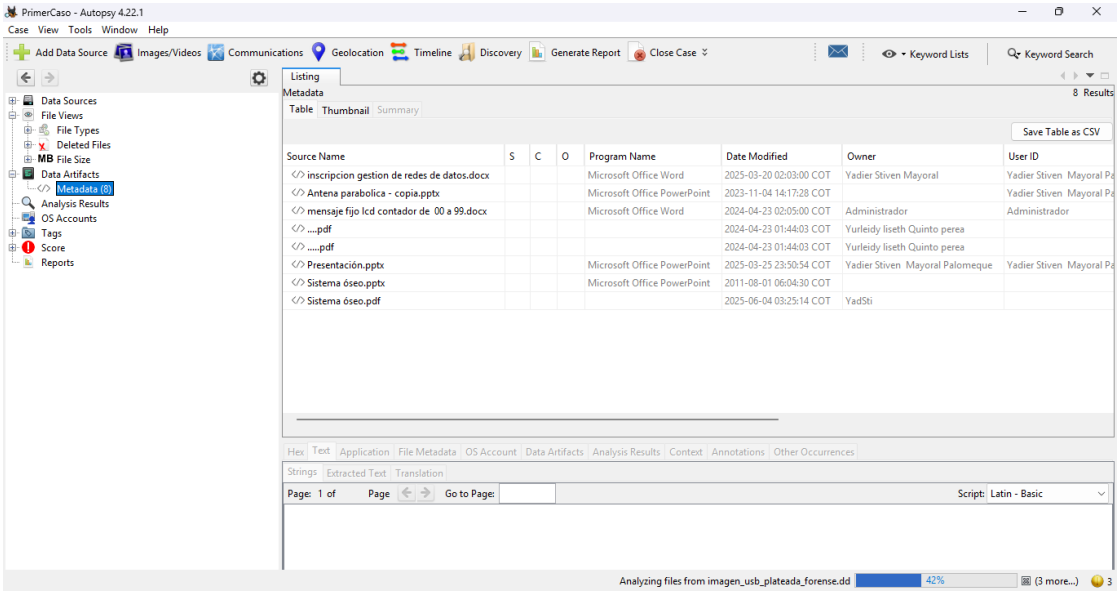
Se procede a verificar que los hashes generados en autopsy de Kali Linux, sean los mismos en autopsy de Windows, para ello hay que seleccionar los datos tipo office que fueron los datos a los que se les generaron hash y se puede evidenciar que los hashes coinciden.

Ilustración 43 Verificación de hash



Con autopsy también se pueden obtener metadatos como se evidencia en la siguiente ilustración.

Ilustración 44 Metadatos



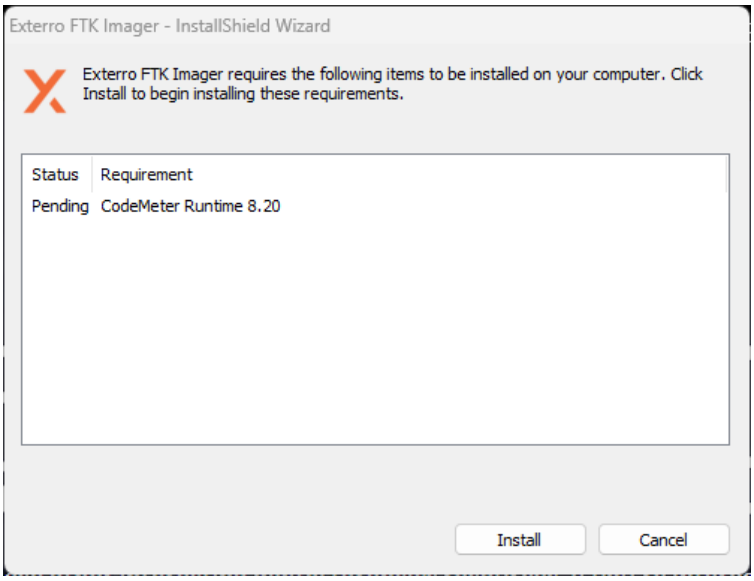
Autopsy independientemente del sistema operativo tiene las mismas funcionalidades en todos, lo que cambia es la forma en como los procesos se llevan a cabo y su interfaz.

Capítulo 3 – FTK IMAGER (Instalación y análisis)

Instalación

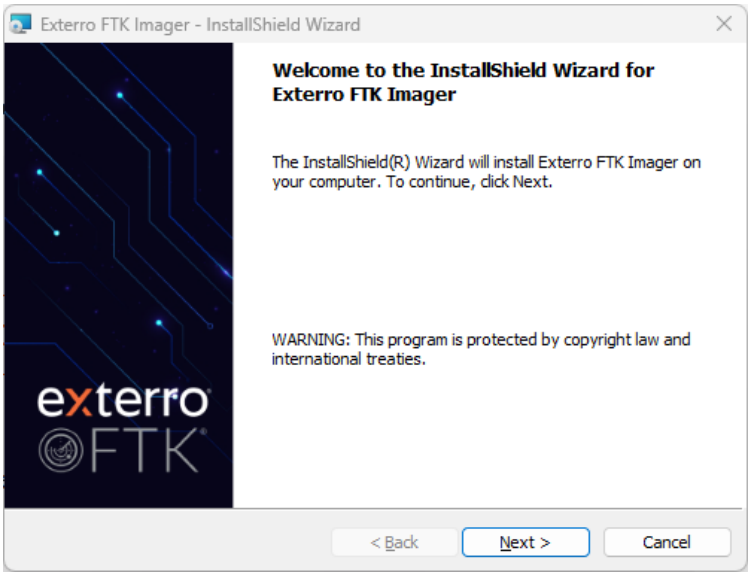
Se ejecuta el instalador, aparece que FTK necesita un complemento, se oprime la opción de instalar.

Ilustración 45 Instalación de complemento



Una vez se instala el complemento, se procede a instalar FTK ahora sí.

Ilustración 46 Instalación FTK

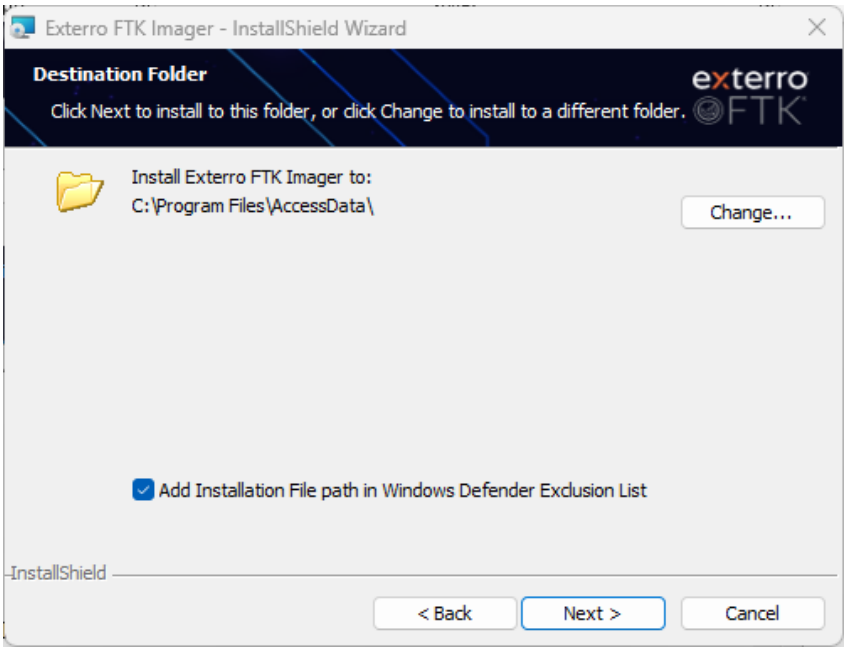


Se aceptan los términos y condiciones.

Ilustración 47 Términos y condiciones

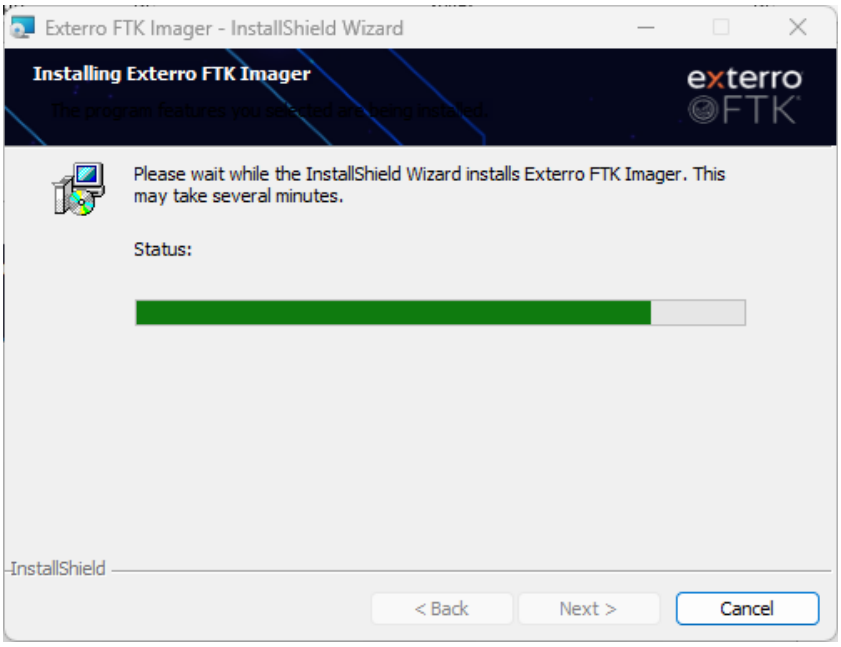
Se añade al archivo de lista de exclusiones de Windows Defender para que pueda operar con normalidad.

Ilustración 48 Añadir a lista de excepciones



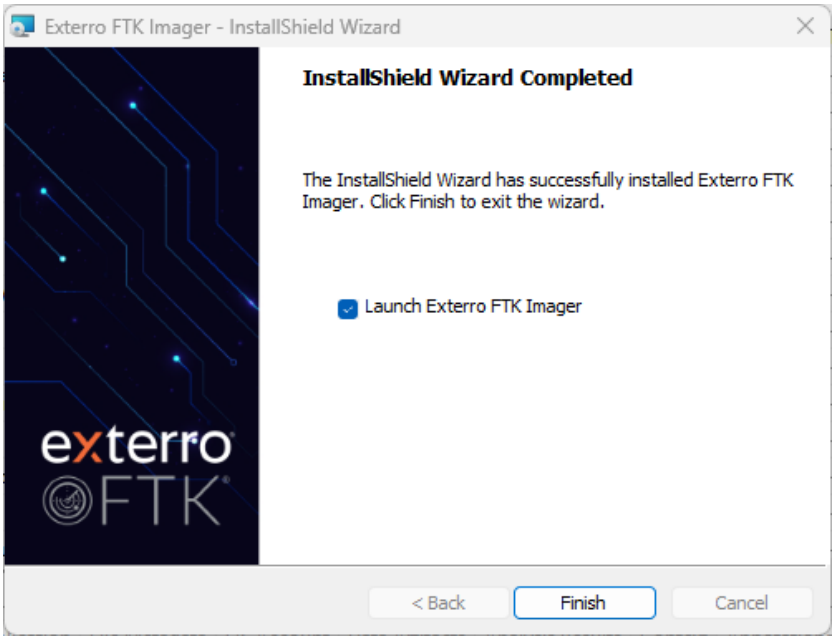
Luego inicia el proceso.

Ilustración 49 Cargando



Finalmente, la instalación finaliza y se inicia el aplicativo de una vez.

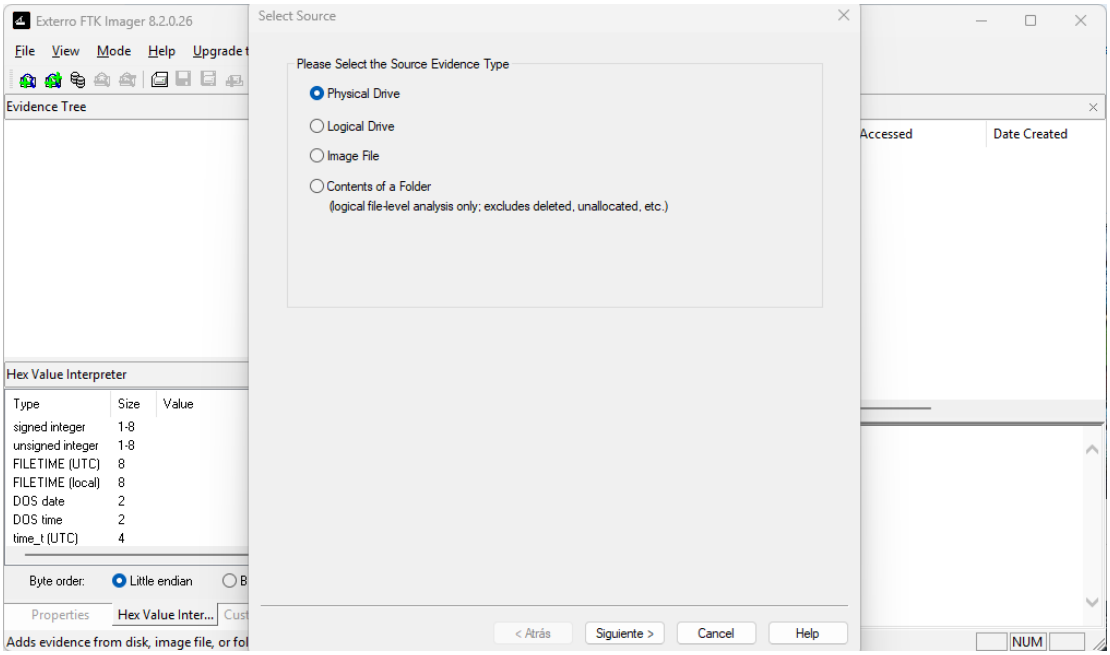
Ilustración 50 Finalización



Análisis de la imagen

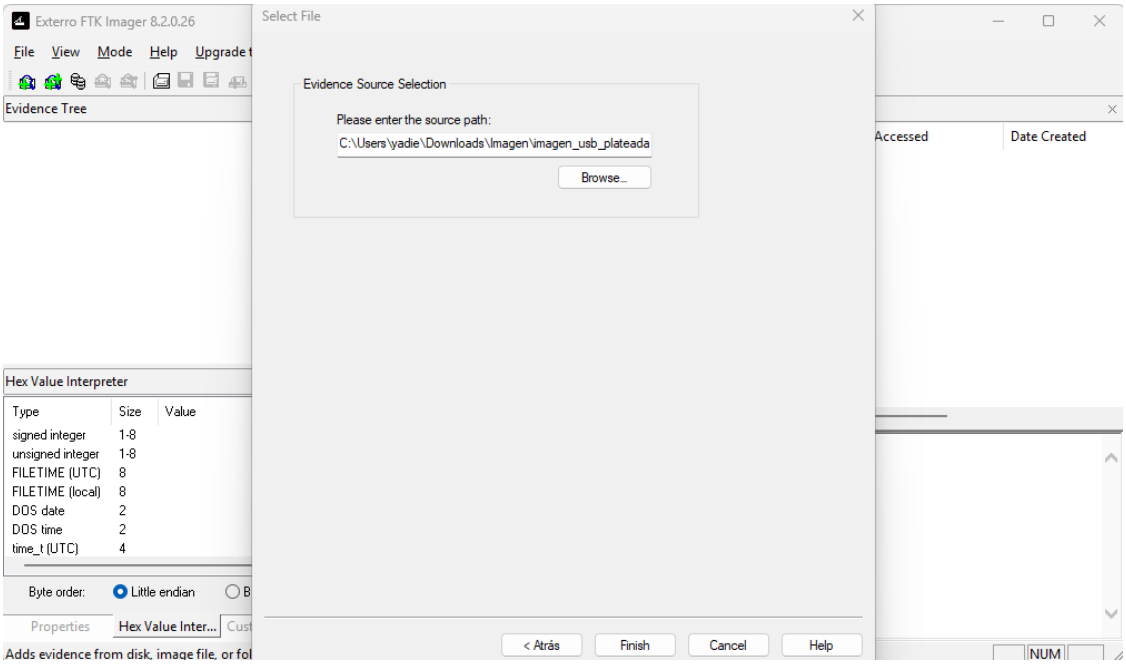
Se selecciona el archivo del tipo de evidencia (la imagen), en este sentido dispositivo físico. O sea la primera opción.

Ilustración 51 Selección de tipo de evidencia

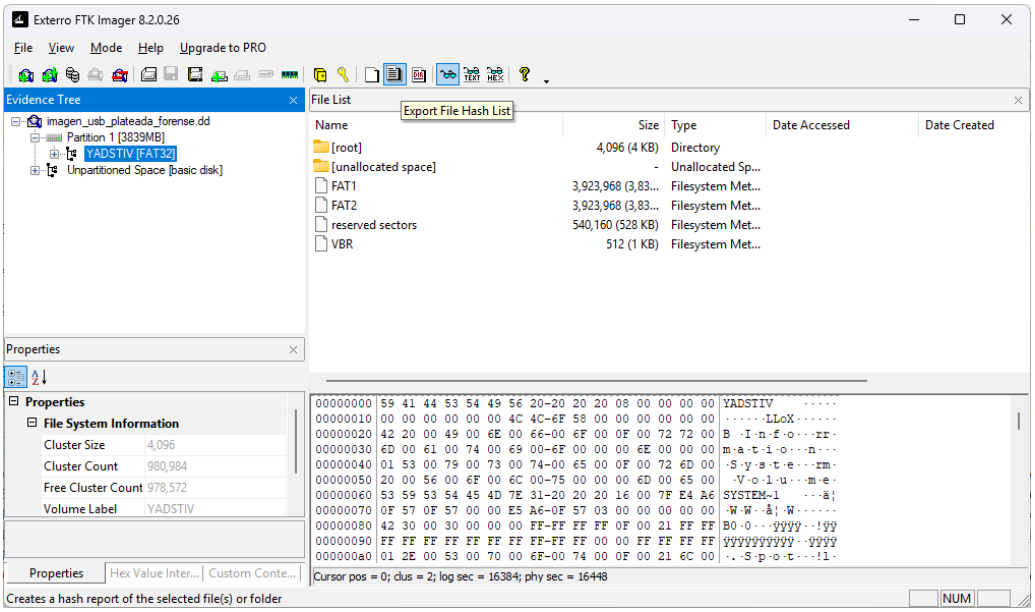


Luego se selecciona el archivo de la imagen.

Ilustración 52 Selección de imagen

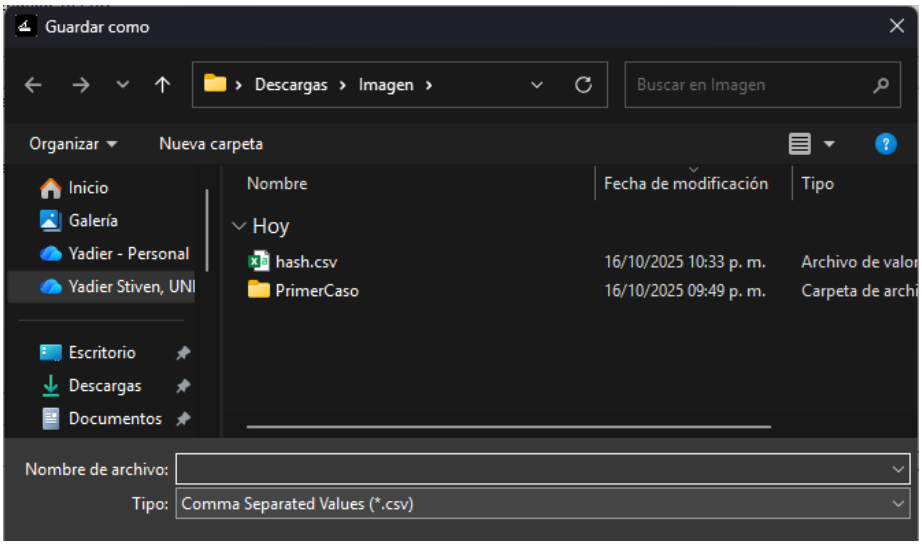


En el panel izquierdo aparece el nombre del dispositivo, al oprimirlo se desprenden unas ramas, donde se pueden inspeccionar todas las carpetas presentes en la imagen e inspeccionar cada una al igual que los archivos.



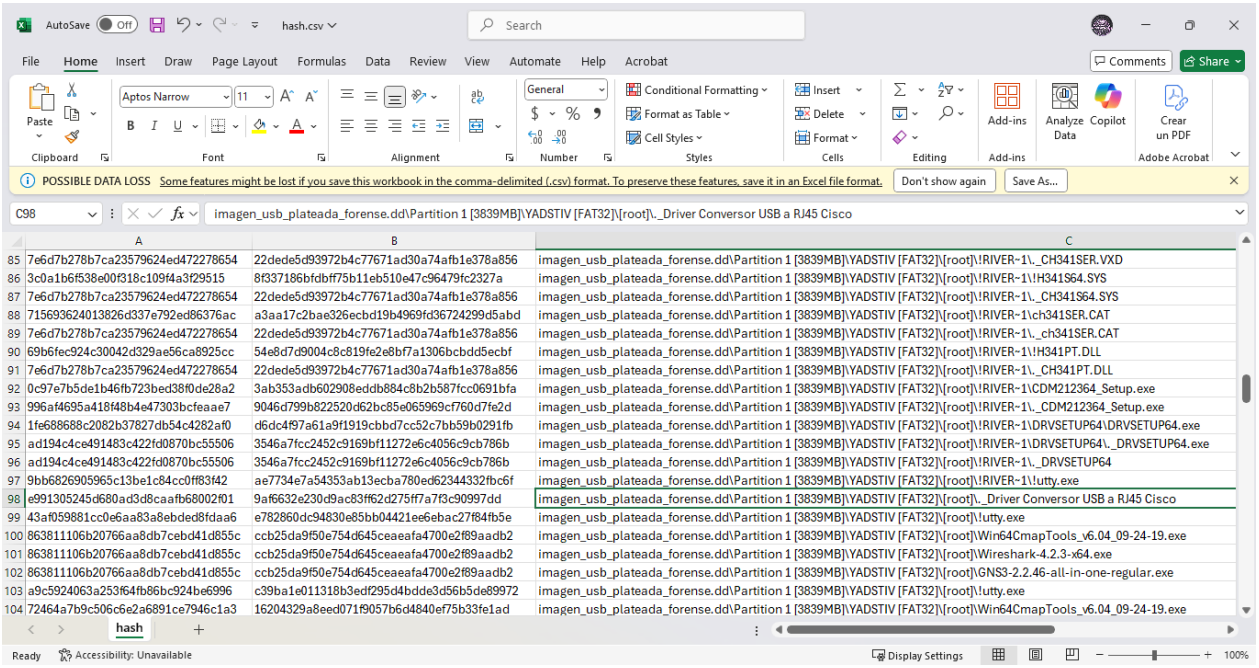
En este caso lo que interesa es obtener los hashes, para ello se selecciona el nombre original de la imagen, en este caso Yadsti, se oprime la opción de exportar lista de hash de archivos y se genera un documento csv. Se nombra

Ilustración 53 Archivo csv



Se obtiene el siguiente documento, con este se puede cotejar y corroborar que los hashes siempre y cuando la información se preserve, se trate de forma adecuada y no se altere, en cualquier aplicativo será la misma.

Ilustración 54 Csv de hashes



	A	B	C
85	7e6d7b278b7ca23579624ed472278654	22dede5d93972b4c77671ad30a74afb1e378a856	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\._CH341SER.VXD
86	3c0a1b6f538e00f318c109f4a3f29515	8f337186bfdbff75b11eb510e47c96479fc2327a	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\!H341S64.SYS
87	7e6d7b278b7ca23579624ed472278654	22dede5d93972b4c77671ad30a74afb1e378a856	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\._CH341S64.SYS
88	715693624013826d337e792ed86376ac	a3aa17c2bae326ecbd19b4969fd36724299d5abd	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\ch341SER.CAT
89	7e6d7b278b7ca23579624ed472278654	22dede5d93972b4c77671ad30a74afb1e378a856	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\._ch341SER.CAT
90	69b6fec924c30042d329ae56ca8925cc	54e8d7d9004c8c819fe2e8bf7a1306bcbdd5ecbf	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\!H341PT.DLL
91	7e6d7b278b7ca23579624ed472278654	22dede5d93972b4c77671ad30a74afb1e378a856	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\._CH341PT.DLL
92	0c97e7b5de1b46fb723bed38f0de28a2	3ab353adb602908eddb884c8b2b587fcc0691bfa	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\CDM212364_Setup.exe
93	996af4695a418f48b4e47303bcfeaae7	9046d799b822520d62bc85e065969cf760d7fe2d	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\._CDM212364_Setup.exe
94	1fe688688c2082b37827db54c4282af0	d6dc4f97a61a9f1919cbbd7cc52c7bb59b0291fb	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\DRVSETUP64\DRVSETUP64.exe
95	ad194c4ce491483c422fd0870bc55506	3546a7fcc2452c9169bf11272e6c4056c9cb786b	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\DRVSETUP64\._DRVSETUP64.exe
96	ad194c4ce491483c422fd0870bc55506	3546a7fcc2452c9169bf11272e6c4056c9cb786b	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\._DRVSETUP64
97	9bb6826905965c13be1c84cc0ff83f42	ae7734e7a54353ab13ecba780ed62344332fbc6f	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!RIVER-1\!utty.exe
98	e991305245d680ad3d8caafb68002f01	9af6632e230d9ac83ff62d275ff7a7f3c90997dd	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\._Driver Conversor USB a RJ45 Cisco
99	43af059881cc0e6aa83a8ebded8fdaa6	e782860dc94830e85bb04421ee6ebac27f84fb5e	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!utty.exe
100	863811106b20766aa8db7cebd41d855c	ccb25da9f50e754d645ceaeafa4700e2f89aadb2	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\Win64CmapTools_v6.04_09-24-19.exe
101	863811106b20766aa8db7cebd41d855c	ccb25da9f50e754d645ceaeafa4700e2f89aadb2	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\Wireshark-4.2.3-x64.exe
102	863811106b20766aa8db7cebd41d855c	ccb25da9f50e754d645ceaeafa4700e2f89aadb2	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\GNS3-2.2.46-all-in-one-regular.exe
103	a9c5924063a253f64fb86bc924be6996	c39ba1e011318b3edf295d4bdde3d56b5de89972	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\!utty.exe
104	72464a7b9c506c6e2a6891ce7946c1a3	16204329a8eed071f9057b6d4840ef75b33fe1ad	imagen_usb_plateada_forense.dd\Partition 1 [3839MB]\YADSTIV [FAT32]\[root]\Win64CmapTools_v6.04_09-24-19.exe

Conclusión

El desarrollo del laboratorio permitió afianzar los conocimientos sobre los procedimientos técnicos y éticos involucrados en la auditoría forense digital. Se evidenció la importancia de garantizar la integridad de la evidencia mediante la generación y comparación de hashes, así como la necesidad de trabajar en entornos controlados para evitar alteraciones de la información.

El uso de Autopsy y FTK Imager demostró cómo las herramientas forenses facilitan la recolección, análisis y presentación de datos digitales de manera estructurada, contribuyendo a la detección de incidentes de seguridad y al fortalecimiento de la ciberseguridad organizacional.

En conclusión, esta práctica reforzó la comprensión de las etapas del análisis forense, identificación, preservación, adquisición y análisis, resaltando su relevancia dentro de los procesos de seguridad y auditoría de redes.

Referencias

Sandoval Morales, R. (2025). *Seguridad y Auditoria de Redes. Quibdó*

netcat | Kali Linux Tools. (n.d.). Kali Linux. https://www.kali.org/tools/netcat/

Davidochobits. (2021, November 4). *Uso del comando Ncat (nc) en Linux con ejemplos - ochobitshacenunbyte*. Ochobitshacenunbyte. https://www.ochobitshacenunbyte.com/2021/11/04/uso-del-comando-ncat-nc-en-linux-con-ejemplos/

Ejemplos de comandos WC: contar el número de líneas, palabras y caracteres. (n.d.). https://es.linux-console.net/?p=20171

Kumar, A. (2024, September 28). *How I used monitor mode on TP-Link WN722N for fun*. It's FOSS. https://itsfoss.com/monitor-mode-fun/?utm_source=chatgpt.com