Laboratorio 23 y 24 Cursos Ciberseguridad

Sesión #23 y 24

Jesús Rodrigo Toro Navarro

Universidad Popular del Cesar

Facultad de Ingeniería y Tecnológica

**Introducción**

En la era digital actual, donde gran parte de la información personal, profesional y gubernamental se encuentra almacenada en dispositivos electrónicos, la seguridad de los datos y la capacidad de investigarlos en caso de incidentes se ha convertido en una prioridad. El análisis forense digital es una rama especializada de la ciberseguridad que se encarga de identificar, recuperar, preservar y analizar datos digitales con el propósito de ser utilizados como evidencia en investigaciones legales o administrativas.

Uno de los escenarios más comunes en este campo es la recuperación de información eliminada de dispositivos de almacenamiento como discos duros, memorias USB, tarjetas SD, entre otros. En este contexto, es fundamental contar con herramientas confiables y eficaces que permitan realizar dichas tareas sin alterar la integridad de la evidencia. Kali Linux, una distribución especializada para pruebas de penetración y análisis forense, ofrece una amplia gama de utilidades para este tipo de actividades.

En el presente laboratorio se llevó a cabo un ejercicio práctico de análisis forense utilizando un dispositivo USB previamente formateado. El objetivo principal fue recuperar los archivos eliminados de dicho dispositivo y analizar los metadatos de los archivos multimedia obtenidos. Para lograrlo, se emplearon herramientas como foremost, encargada de la recuperación de archivos mediante técnicas de carving, y exiftool, que permite extraer y examinar metadatos incrustados en imágenes y otros tipos de archivos.

El procedimiento se desarrolló paso a paso sobre la plataforma Kali Linux, comenzando con la actualización del sistema, la instalación de las herramientas necesarias y la conexión del pendrive a analizar. Posteriormente, se ejecutaron comandos que permitieron visualizar la estructura de datos recuperados, seguido de un análisis detallado de los metadatos, los cuales revelaron información sensible como la fecha de captura de las imágenes, el modelo del dispositivo con el que fueron tomadas e incluso la posible ubicación geográfica.

Este tipo de prácticas no solo permiten comprender el funcionamiento técnico de las herramientas, sino también evidencian la importancia de la protección de la información y las implicaciones que una mala gestión de datos puede tener en términos de privacidad y seguridad. Así, el laboratorio representa una valiosa oportunidad para desarrollar habilidades en análisis forense digital, esenciales tanto en el ámbito académico como profesional.

**Objetivos**

**Objetivo General**

Realizar un análisis forense sobre un dispositivo USB utilizando Kali Linux, con el fin de recuperar archivos eliminados y examinar sus metadatos mediante herramientas especializadas como foremost y exiftool.

**Objetivo Específicos**

Comprender el uso de herramientas forenses en entornos Linux.

Recuperar archivos eliminados de un dispositivo USB formateado.

Analizar los metadatos de los archivos multimedia recuperados para extraer información relevante como fechas, modelos de cámara y ubicación.

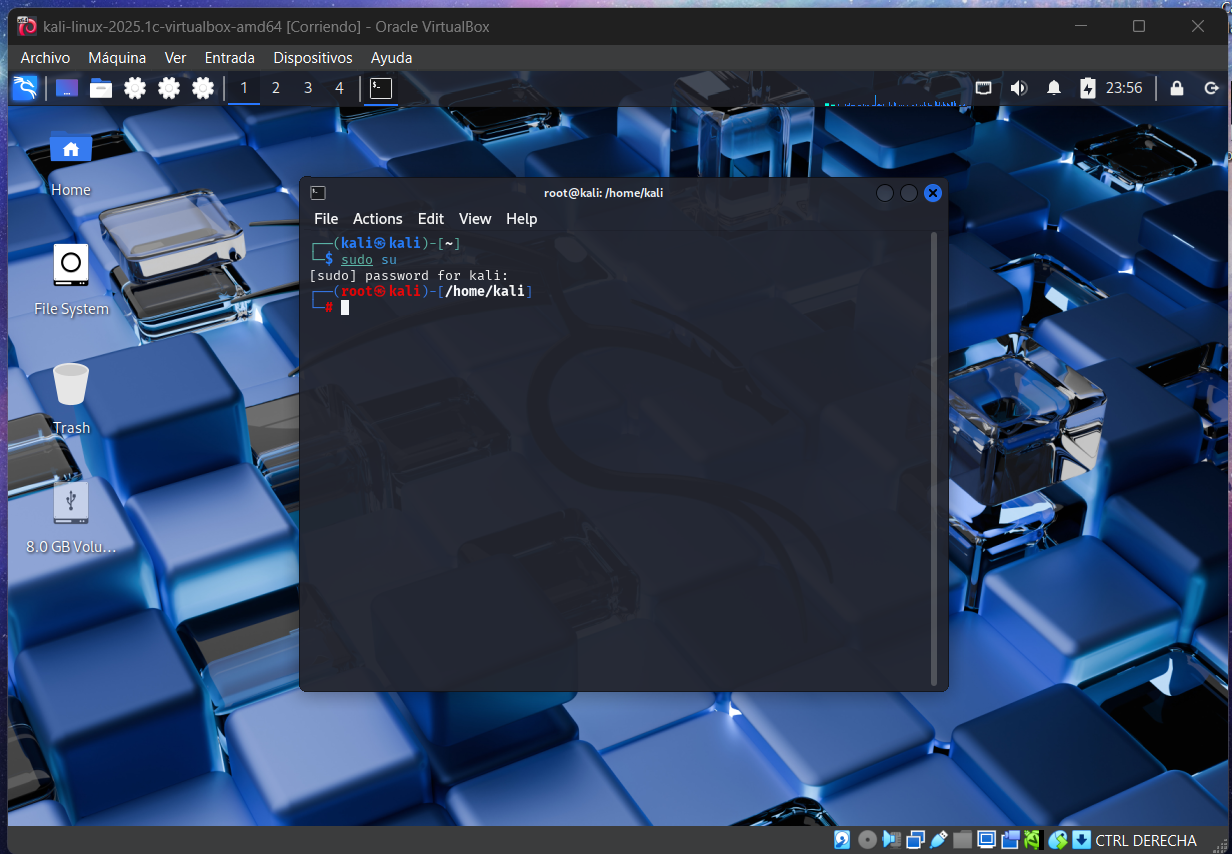
Evaluar la importancia de los datos recuperados en el contexto de una investigación forense digital.

Fomentar buenas prácticas en el manejo de evidencia digital y el uso adecuado de herramientas de análisis.

**Procedimientos**

**Preparación del entorno**

Se utilizo Kali Linux y un pendrive para el laboratorio

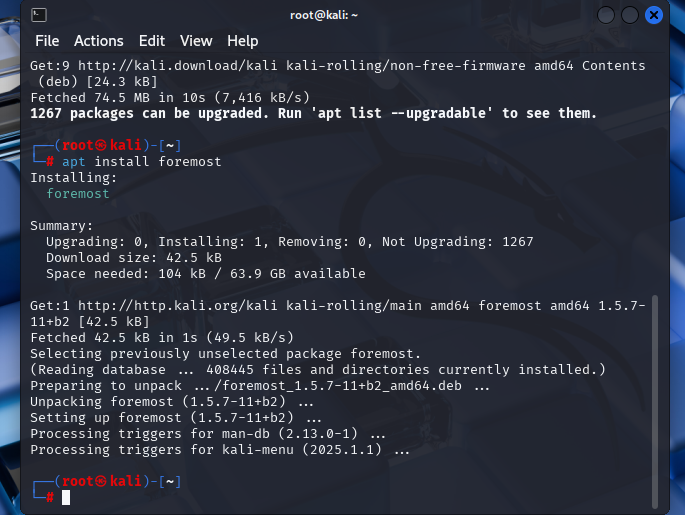


Se actualizan los paquetes de Linux

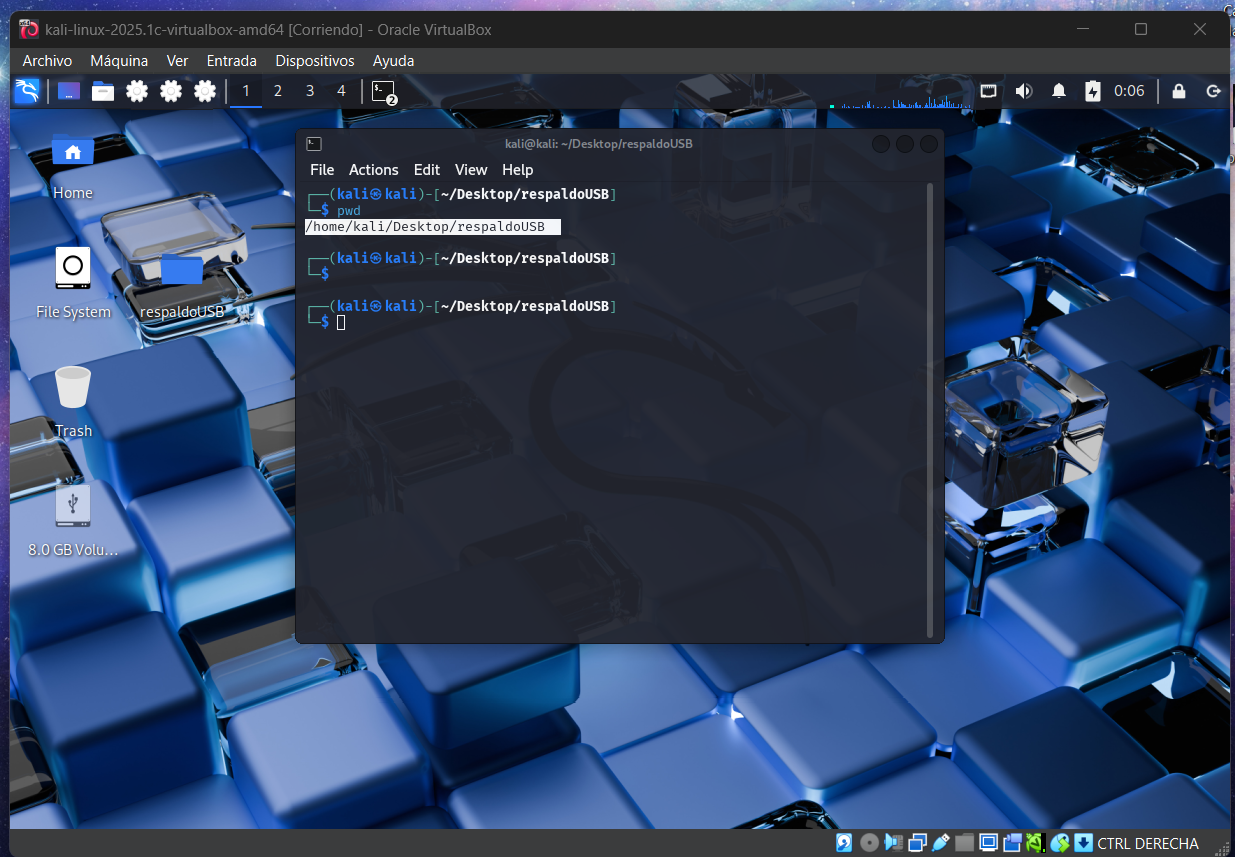
Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

Instalación de herramientas: Instalamos la herramienta foremost

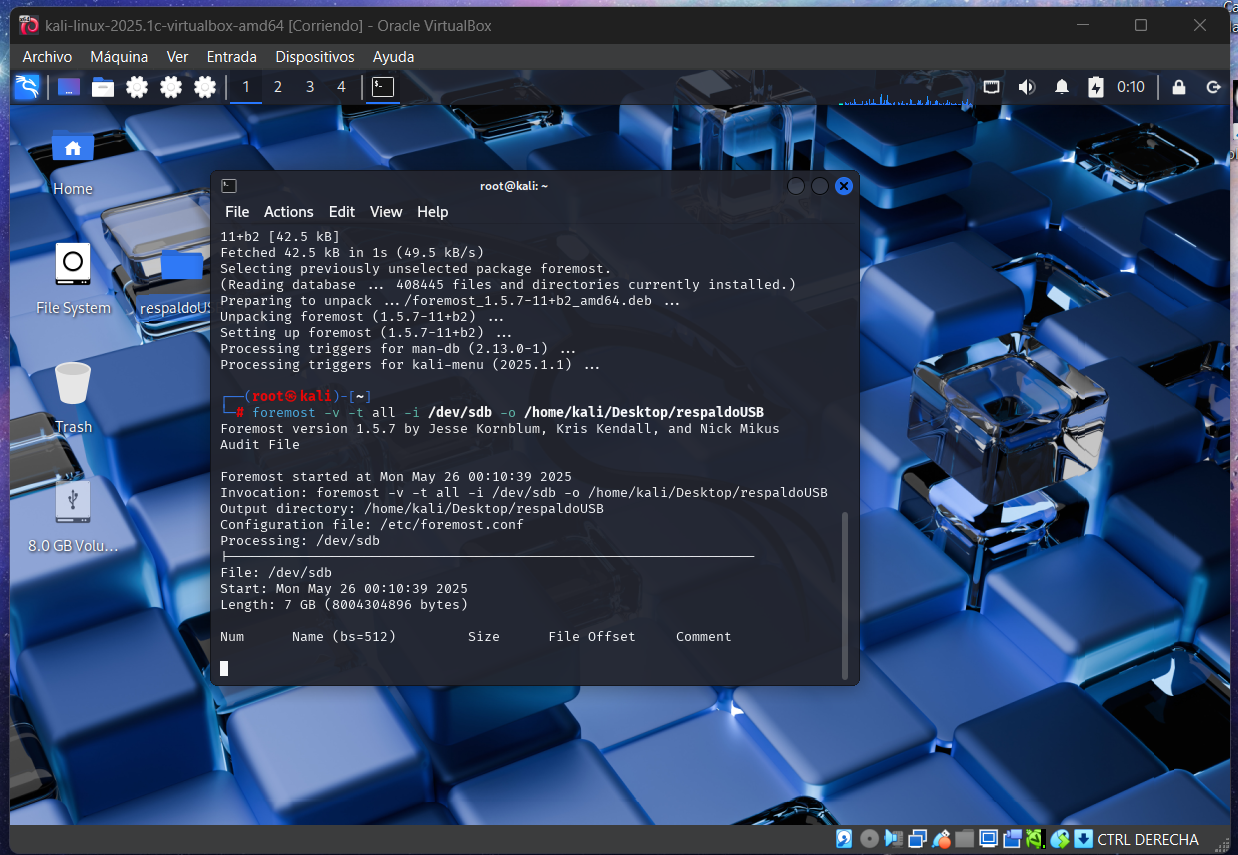


Este laboratorio se trata de recuperar los archivos de un pendrive conectado al equipo, y ver los metadatos de esos archivos recuperados

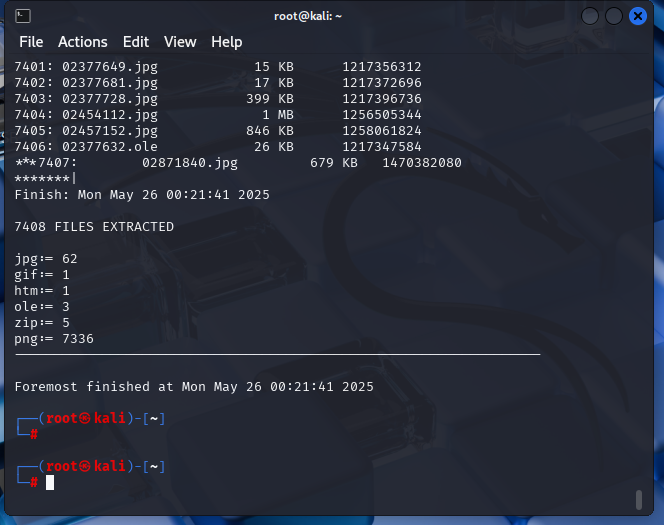
Creamos un carpeta respaldoUSB y vemos su ruta  


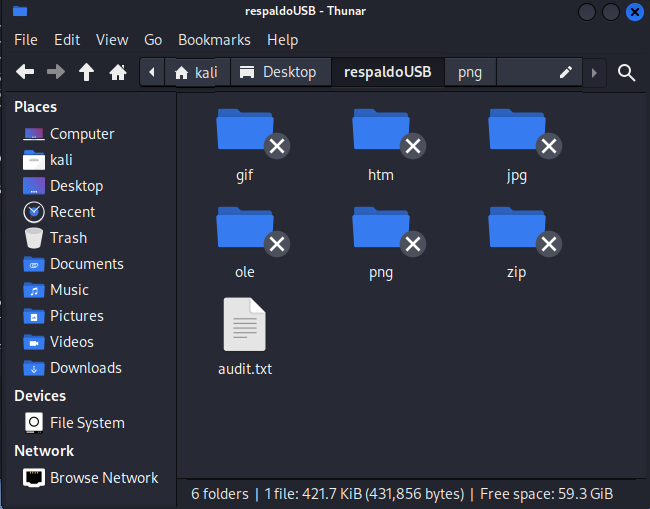
Recuperación de archivos

Usamos la herramienta foremost para recuperar los archivos del pendrive el cual fue formateado



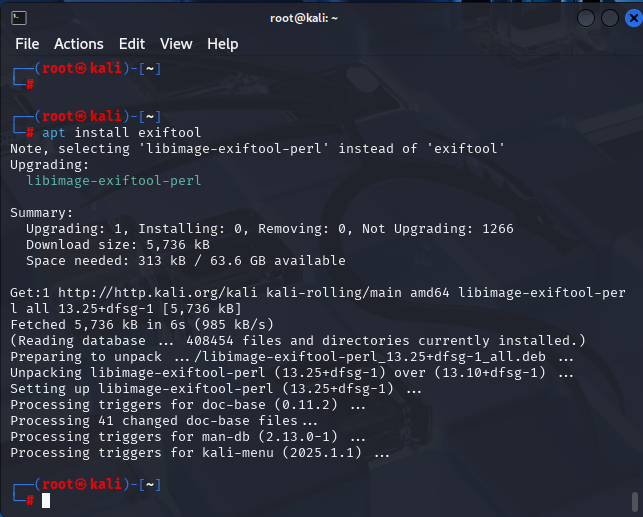
Podemos ver un resumen de lo que se recupero



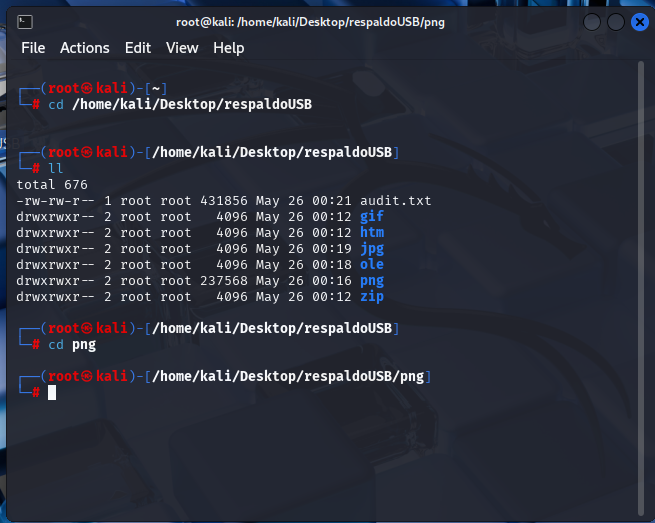


**Análisis de metadatos**

Ahora instalamos la herramienta exiftool, utilizada para extraer metadatos de archivos multimedia.



Nos dirigimos a la carpeta donde se encuentran los archivos pngs recuperados

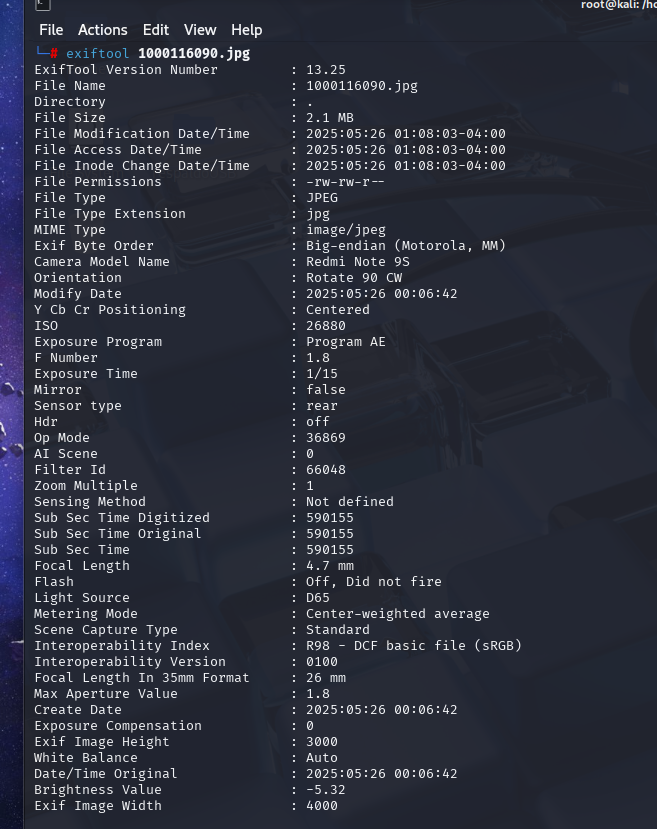


Ejecutamos el comando para poder la información de metados del archivo y realizar un análisis de estos

Texto

El contenido generado por IA puede ser incorrecto.





Texto

El contenido generado por IA puede ser incorrecto.

Analizando otros archivos recuperados se puede visualizar más información, como el modelo de la cámara, fecha en que se tomo la imagen y si en este ejemplo no se encontrara restringida también se podría obtener la dirección de la imagen.  
Toda esta información es de vital importancia para un análisis forense digital

**CONCLUSIÓN**

Este laboratorio demuestra cómo un análisis forense básico en Kali Linux permite recuperar información sensible incluso de dispositivos formateados, subrayando los riesgos asociados a una eliminación inadecuada de datos. Las herramientas foremost y exiftool son potentes recursos para investigadores digitales, ya que permiten no solo recuperar archivos sino también obtener información contextual que puede ser crucial en una investigación. El ejercicio fortalece las competencias en informática forense, enfatizando la importancia de técnicas y herramientas adecuadas para preservar y analizar evidencias digitales.