Adquisición forense de una memoria USB

Yeray Almoguera Gonzalez

11/11/2024

Introducción

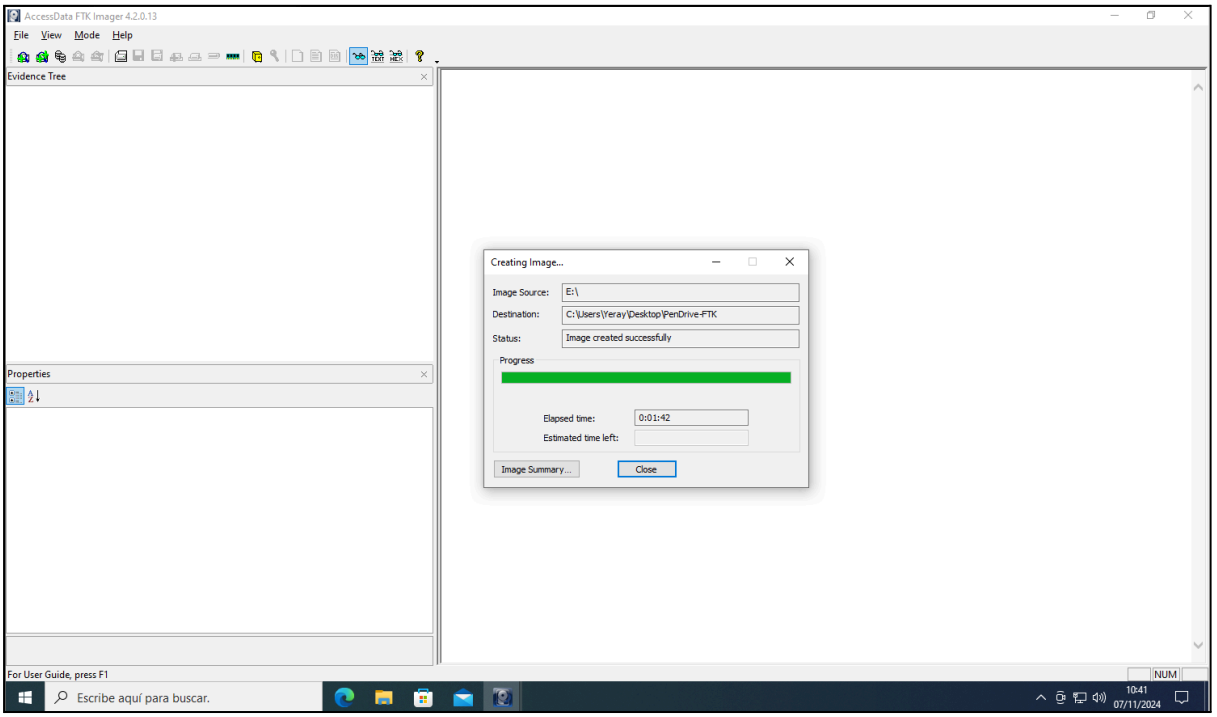
La adquisición forense de dispositivos de almacenamiento, como las memorias USB, es un paso fundamental en el análisis forense digital. Este proceso permite obtener una copia exacta de los datos almacenados, preservando la integridad de la evidencia original y facilitando su análisis posterior sin riesgo de alteración.

En este trabajo práctico, se realizará la adquisición forense de una memoria USB utilizando tres herramientas reconocidas en el campo: FTK Imager, Guymager y dd. El objetivo es comparar el proceso y los resultados obtenidos con cada herramienta, analizando aspectos como la facilidad de uso, velocidad de adquisición, formatos de imagen soportados y metadatos generados.

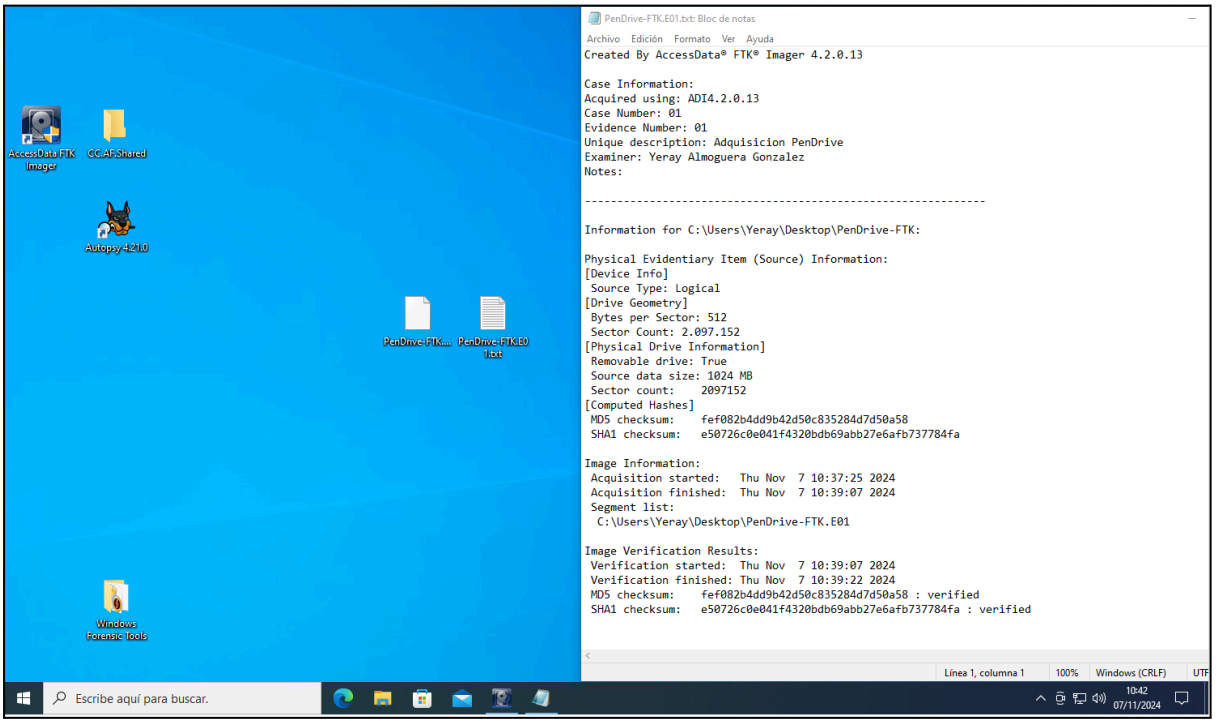
Este ejercicio proporcionará una comprensión práctica de las ventajas y limitaciones de cada enfoque, sentando las bases para seleccionar la herramienta más adecuada en futuras investigaciones forenses. Durante todo el proceso, se seguirán los principios básicos de la informática forense, garantizando la preservación de la evidencia y la documentación detallada de cada paso realizado.

FTK Imager

FTK Imager es una herramienta de software forense de código abierto desarrollada por AccessData, ampliamente utilizada en el campo de la informática forense. Esta herramienta permite crear copias exactas (imágenes forenses) de dispositivos de almacenamiento digital sin modificar la evidencia original.



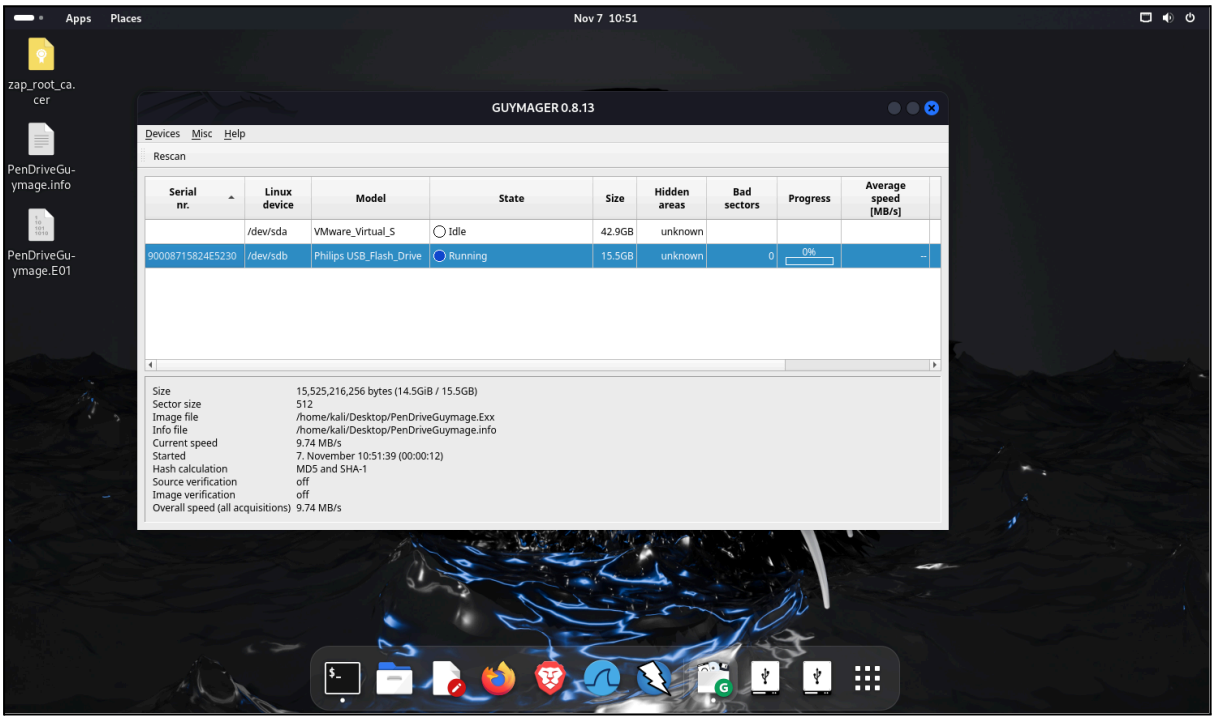
Captura de la herramienta una vez terminado el proceso.



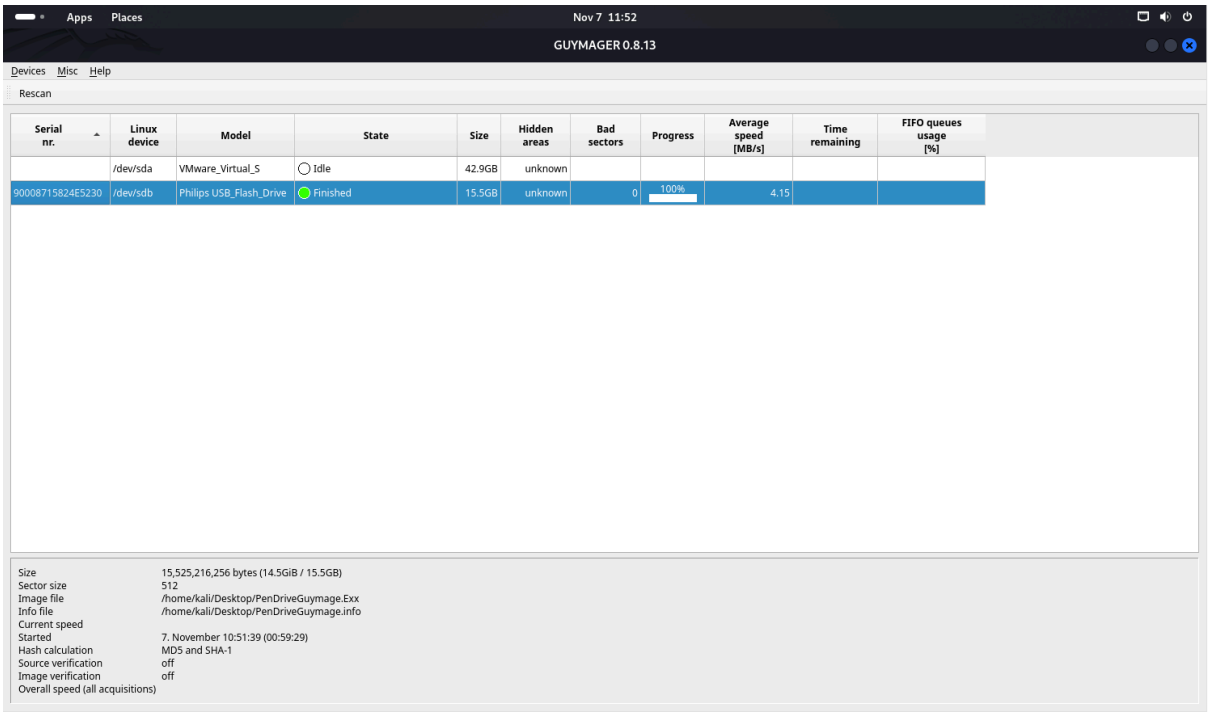
Captura de la adquisición de los archivos y de los hashes generados.

Guymager

Guymager es una herramienta de código abierto especializada en la adquisición de imágenes forenses, diseñada específicamente para sistemas Linux. Esta herramienta se destaca por su interfaz gráfica intuitiva y su eficiencia en la creación de imágenes forenses.



Captura del proceso de adquisición de la herramienta.



Captura de la herramienta una vez finalizado el proceso de adquisición

DD

El comando dd (Data Duplicator) es una herramienta de línea de comandos disponible en sistemas Unix y Linux, utilizada frecuentemente en informática forense para realizar copias bit a bit de dispositivos de almacenamiento. Aunque no es una herramienta específicamente diseñada para fines forenses, su versatilidad y precisión la convierten en una opción popular entre los investigadores forenses.

Captura del comando realizado para la adquisición.

Captura del comando finalizado junto con el archivo adquirido.