Actividad 1. Adquisición de evidencias digitales

Informe de adquisiciones

Alumno: Julio Ortiz Bort
Asignatura: Informática Forense
Fecha: 29 de noviembre de 2025

Objetivos

Practicar y documentar la adquisición forense de evidencias digitales:

- Adquisición forense de un dispositivo de almacenamiento externo (bloqueo contra escritura).
- Adquisición en caliente (live acquisition) de la memoria RAM y del disco de un sistema encendido.
- Registrar todas las precauciones y procedimientos para evitar la alteración de la evidencia.

Resumen ejecutivo

Se realizaron dos tipos de adquisición:

1. Imagen forense de un pendrive (dispositivo externo) usando bloqueo contra escritura.
2. Adquisición en caliente de memoria RAM y del disco principal de una máquina virtual encendida, usando herramientas forenses reconocidas.

Materiales y herramientas

- Equipo análisis (PC forense): *Asus Rog Strix / Windows 11 Home/ 23H2*.
- Dispositivo de evidencia: pendrive (modelo: TDK LoR TF10 USB).
- Herramientas software:
  - Duplicado/clonado: `Exterro FTK Imager`
  - Borrado seguro: `HDShredder`
  - Hashes: `Exterro FTK Imager`
  - Captura de RAM: `FTK Imager`

Precauciones generales para no alterar la evidencia

- Mantener cadena de custodia documentada (persona, hora, lugar).
- Usar guantes y herramientas limpias para manipular dispositivos físicos.
- Evitar conectar el dispositivo a sistemas no forenses que modifiquen metadatos.
- Preferir bloqueadores hardware contra escritura; si no están disponibles, usar adaptadores read-only o herramientas que no monten el sistema de archivos.
- Registrar inmediatamente hora y fecha (UTC) y calcular/guardar hashes de la evidencia.
- Para adquisiciones en caliente: documentar todos los pasos porque se modifica el estado del sistema por definición; minimizar la interacción.

Procedimiento 1 — Adquisición de dispositivo externo (pendrive)

1. Preparación

1. Identificación y etiquetado del dispositivo (ID, fecha, hora y caso asignado).
2. Ejecución de un borrado seguro completo del pendrive mediante **HDShredder**, garantizando la eliminación previa de cualquier información residual.
3. Preparación del equipo forense, verificando la integridad del sistema y asegurando que se utiliza un entorno forense limpio.
4. Aplicación del bloqueo de escritura del dispositivo mediante los **scripts personalizados** desarrollados previamente.
5. Confirmación de que el dispositivo queda correctamente en modo de solo lectura antes de realizar la adquisición.

2. Adquisición mediante FTK Imager

Con la protección contra escritura activa, se realiza la adquisición forense utilizando **FTK Imager**, evitando en todo momento montar el dispositivo o alterar su contenido.

1. Detección del dispositivo mediante la función *Create Disk Image*.
2. Selección del origen de adquisición como *Physical Drive*, correspondiente al pendrive analizado.
3. Generación de la imagen forense en formato **E01**.
4. Activación del cálculo automático de hashes proporcionado por FTK Imager.
5. Obtención de los tres hashes de integridad:
   - **MD5**
   - **SHA1**
6. Conservación del archivo de log generado por FTK Imager con el detalle completo del proceso.

3. Verificación de integridad

La verificación consiste en comparar los valores hash generados en el proceso de adquisición con los recalculados posteriormente, confirmando la autenticidad y consistencia de la imagen obtenida.

4. Documentación

- Identificador del dispositivo: TDK LoR TF10 USB Device
- Número de serie del pendrive: 0274073540A0
- Fecha/hora de inicio de adquisición: Fri Nov 28 17:55:07 2025
- Fecha/hora de finalización: Fri Nov 28 18:04:25 2025
- Herramienta usada para la adquisición: **FTK Imager**
- Formato de imagen generado: E01
- Hashes obtenidos:
  MD5: 88630a879e6741830ec20a7984fd792d
  SHA1: 3696d7ea76dda0b4f3b4d6bb423a12ea7709fd8e
- Ubicación de la imagen forense: D:/EVIDENCIA/PENDRIVE.E01

Procedimiento 2 — Adquisición en caliente (RAM y disco) sobre máquina encendida

Contexto

Se tomó como objetivo una máquina con sistema operativo **Windows 11** y usuario conectado en el momento del incidente. Debido a que la adquisición en caliente altera el estado, se aplicaron las siguientes reglas: documentar todo; usar herramientas que minimicen la sobrescritura; obtener primero la memoria volátil y luego una imagen lógica/imagen del disco en caliente.

1. Captura de memoria RAM

- Justificación: la RAM contiene procesos en ejecución, credenciales en memoria, certificados temporales y artefactos que desaparecen al apagar.
- Herramienta utilizada: `FTK Imager` (Windows)
- Hora de inicio/fin de la captura RAM: Fri Nov 29 13:30 2025.
- Herramienta y versión: **FTK Imager**.
- Hashes del volcado:

Archivo	**MD5**	**SHA1**
memcapture.ad1	a91890a06873d1915e9368a3908259f8	90c458a4be83785cccd942f12bcbf3da411d252a
memcapture.ad1.txt	4b2dc271e868eea7c7587efb11fd4327	a7966c0ef5066010339600eae06f5774c7350d72
memcapture.ad2	b36efe7f885882e2e1ed0465f8495376	27c0b636f17fc55e77fabc9bce82537fb73d300e
memcapture.ad3	63058972672001f766311769616aa1af	75d4817b07e5a42d364fc8462af95219eac878f8
memdump.mem	d1940626f7665c4bc5150a38d4eb9cca	71a73deeb28a09434a0f49294264e088fbc37cf5
pagefile.sys	0de0387e8d010ee6147568bb62480d17	ed04afd779afc57587763b5ef8ce75339bb1cf7a

Cuadro 1: Hashes MD5 y SHA1 de los archivos adquiridos

2. Adquisición en caliente del disco

- Método: realización de una **adquisición en caliente** del disco del sistema Windows utilizando la herramienta **FTK Imager** ejecutada directamente sobre el equipo encendido. Este procedimiento permite obtener una imagen del disco sin apagar el sistema, preservando el estado operativo en el momento de la intervención.
- Tipo de adquisición: se seleccionó la opción **Physical Drive** en FTK Imager para generar una imagen física completa del disco del sistema.
- Formato utilizado: se optó por la creación de una imagen en formato **E01 (Expert Witness Format)**, debido a su compresión, metadatos integrados y soporte para múltiples hashes.
- Integridad: durante la adquisición se activó el cálculo automático de hashes **MD5 y SHA1** ofrecidos por la herramienta.

Procedimiento en FTK Imager

1. Ejecutar `FTK Imager` como Administrador desde un dispositivo externo.
2. Seleccionar `File → Create Disk Image`.
3. Elegir `Physical Drive` y seleccionar el disco del sistema (normalmente *Disk 0*).
4. Establecer metadatos del caso (ID, examinador, notas).

5. Seleccionar el formato `E01`.
6. Activar el cálculo de hashes: `MD5, SHA1`.
7. Guardar la imagen en un disco externo dedicado a evidencias.

Verificación posterior

Una vez generada la imagen, se realizaría la verificación manual de los hashes usando PowerShell:

```
Get-FileHash E:\adquisicion_disk0.E01 -Algorithm MD5
Get-FileHash E:\adquisicion_disk0.E01 -Algorithm SHA1
```

Se compararían los valores con los generados automáticamente por FTK Imager para confirmar la integridad de la evidencia obtenida.

Documentación

Se documentaron: fecha y hora de inicio y fin de la adquisición, tamaño de la imagen, hashes generados, número de serie del dispositivo de destino, versión de FTK Imager utilizada y cualquier observación relevante detectada durante el proceso.

Cadena de custodia

Completar tabla para cada elemento de evidencia:

ID evidencia	Descripción física	Recogido por	Fecha/Hora	Ubicación / Observaciones
EVID-001	Pendrive 32GB Lexar	Julio Ortiz Bort	Nov 28 18:04:25 2025	En bolsa antiestática, bloqueador aplicado
EVID-002	Volcado RAM — ROG Strix G531GT_G531GT	Julio Ortiz Bort	Nov 29 13:30 2025	Archivos: Evidencias/Memoria_RAM/

Anexos (capturas)

Script general para bloqueo de escritura en dispositivos USB

Descripción

El siguiente script en **BAT/Windows** permite activar la protección contra escritura en todos los dispositivos USB de almacenamiento conectados al sistema. Este método modifica la clave del registro `StorageDevicePolicies` para impedir cualquier intento de escritura.

Script .BAT para bloquear escritura

Listing 1: Script BAT para bloquear escritura en todos los dispositivos USB

```
@echo off
echo Activando proteccion de escritura en dispositivos USB...

REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   red↪ StorageDevicePolicies" ^
/v WriteProtect /t REG_DWORD /d 1 /f

echo Escritura bloqueada correctamente.
```

```
pause
```

Script .BAT para desbloquear escritura

Listing 2: Script BAT para restaurar escritura en dispositivos USB

```
@echo off
echo Desactivando proteccion de escritura en dispositivos USB...

REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   red↪ StorageDevicePolicies" ^
/v WriteProtect /t REG_DWORD /d 0 /f

echo Escritura permitida nuevamente.
pause
```

Notas

- Ambos scripts requieren ejecución como **Administrador**.
- La protección afecta a cualquier dispositivo USB de almacenamiento conectado al sistema.
- Tras aplicarlo, es recomendable desconectar y volver a conectar el pendrive para que el bloqueo surta efecto.

Fin del informe.

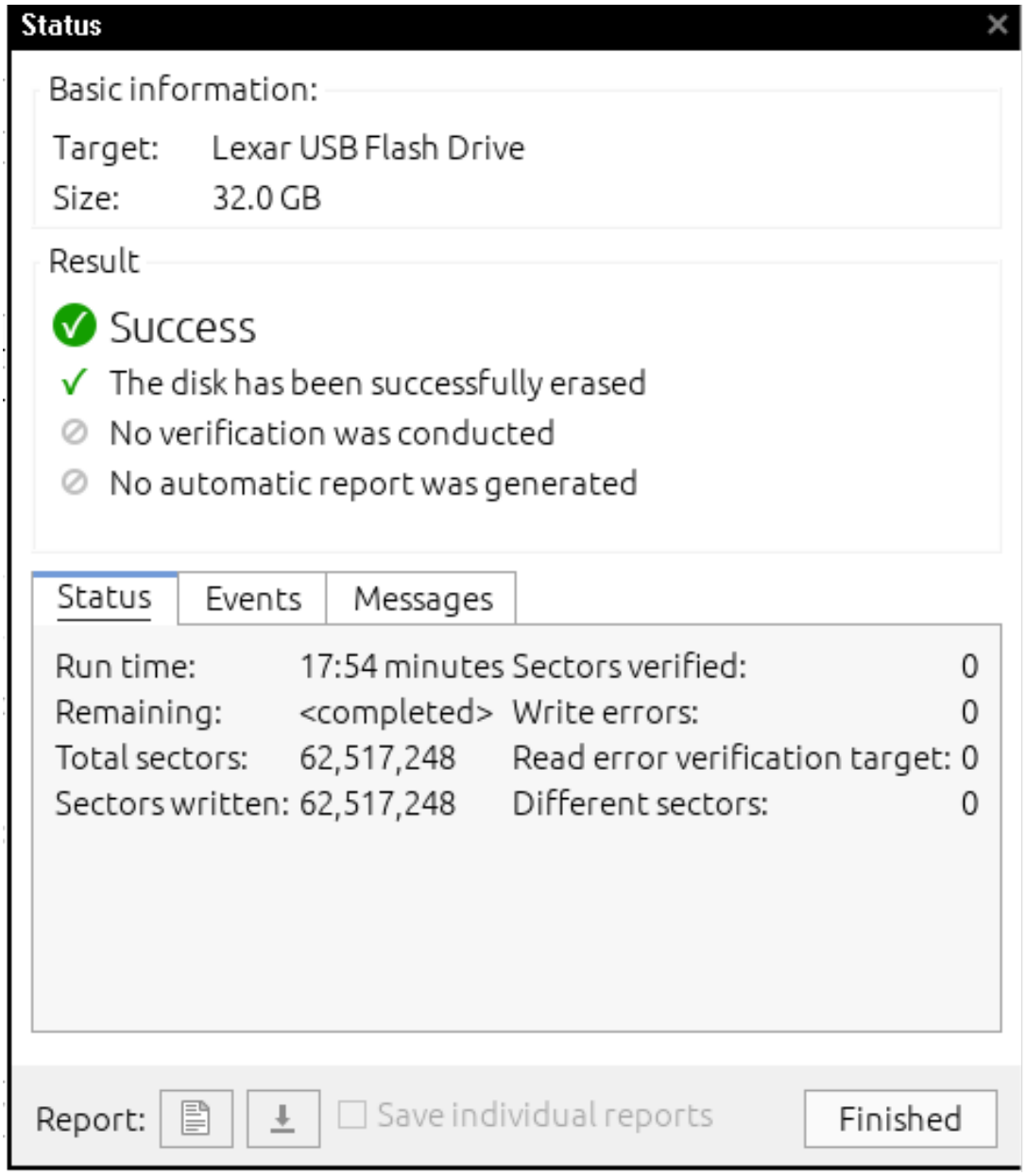

Figura A.1 — Borrado seguro del pendrive donde alojar el duplicado.

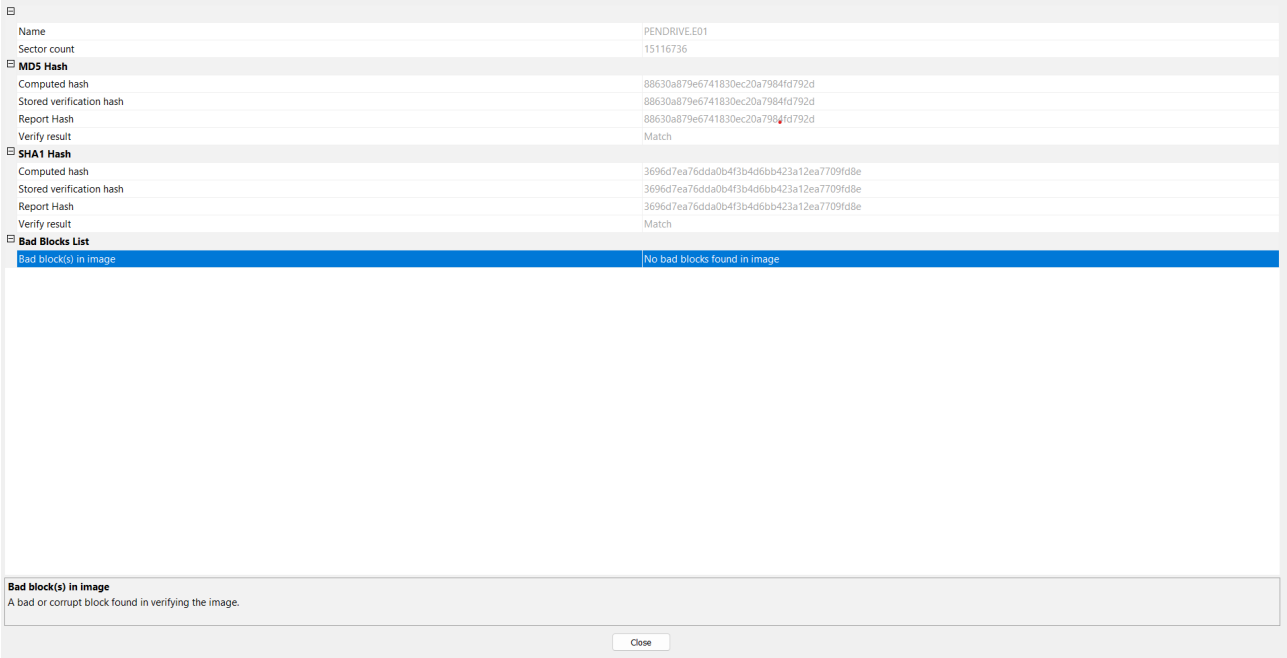

Figura A.2 — Hashes obtenidos mostrando que la la información duplicada es idéntica a la original.

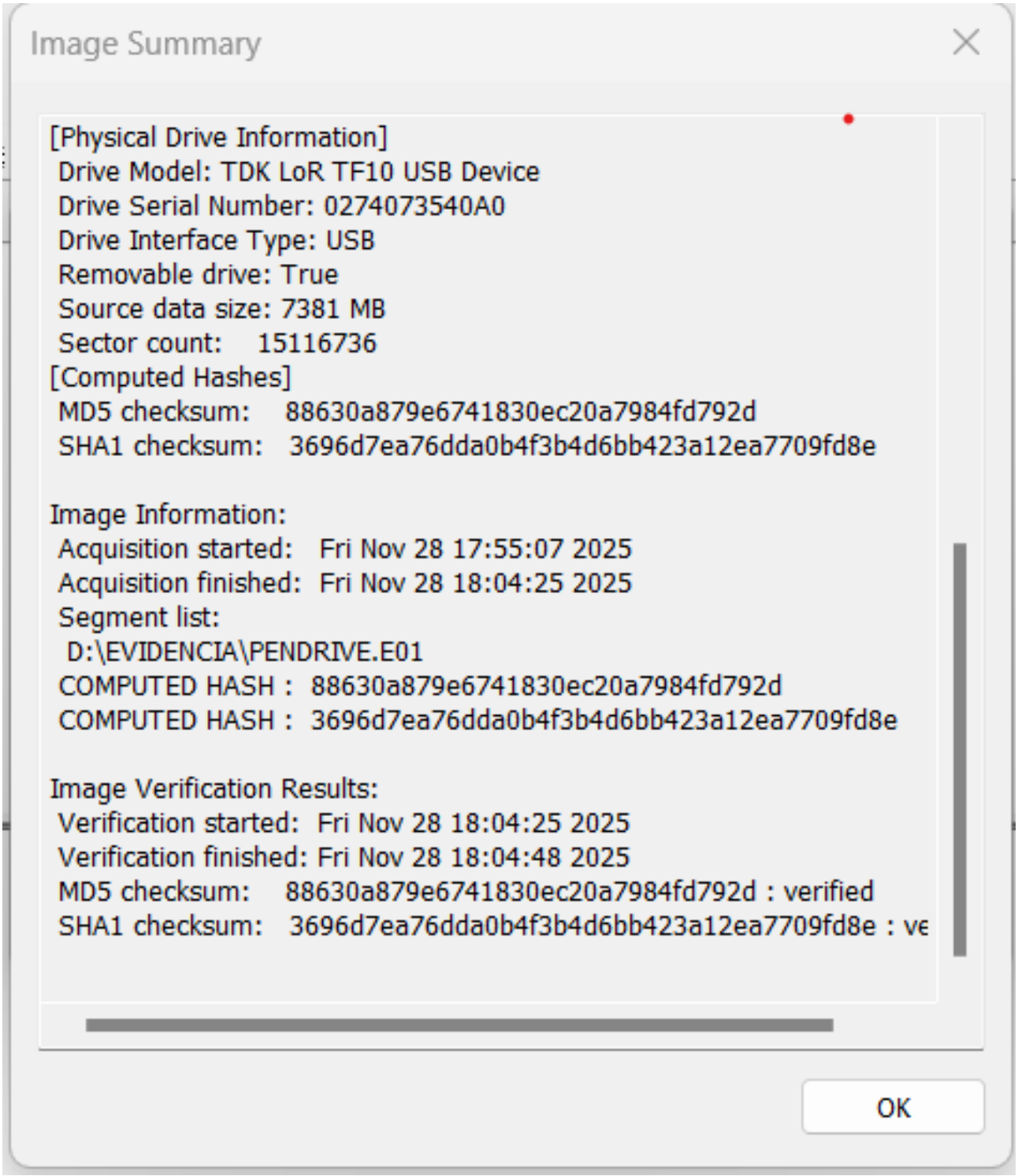

Figura A.3 — Resumen del proceso de duplicado.

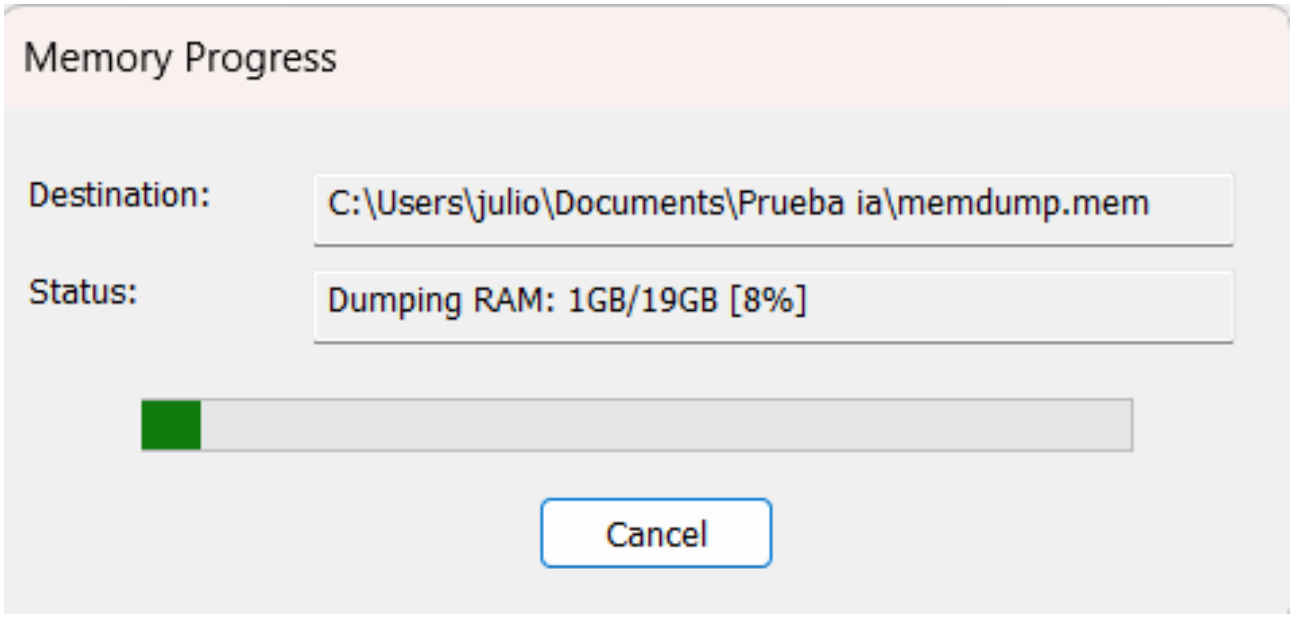

Figura B.1 — Proceso de captura y duplicado de la memoria RAM.

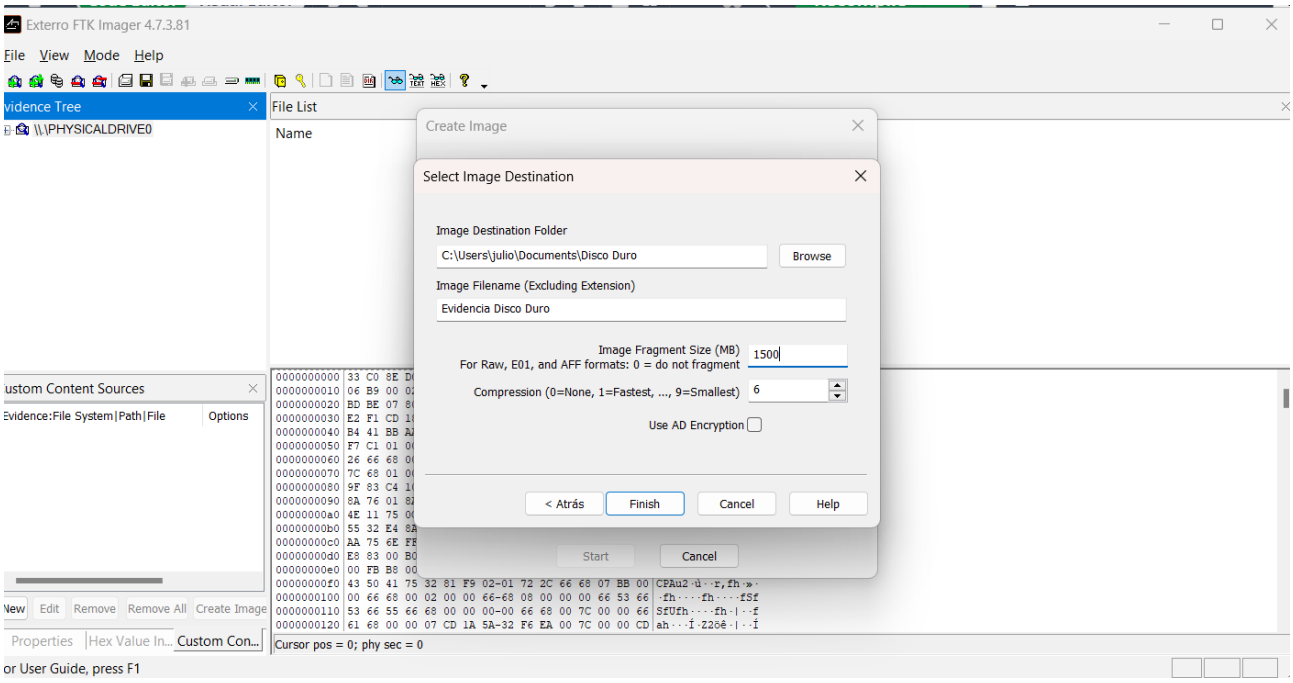

Figura B.2 — Captura del proceso de duplicado del disco duro en caliente.