Lab 4 Report

PART 1: Physical Image of Thumb Drive using FTK Imager

Overview:

I created a physical image of a USB thumb drive using FTK Imager. Before imaging, I installed SafeBlock and configured to ensure the USB ports were write-blocked, preventing any modification to the original data.

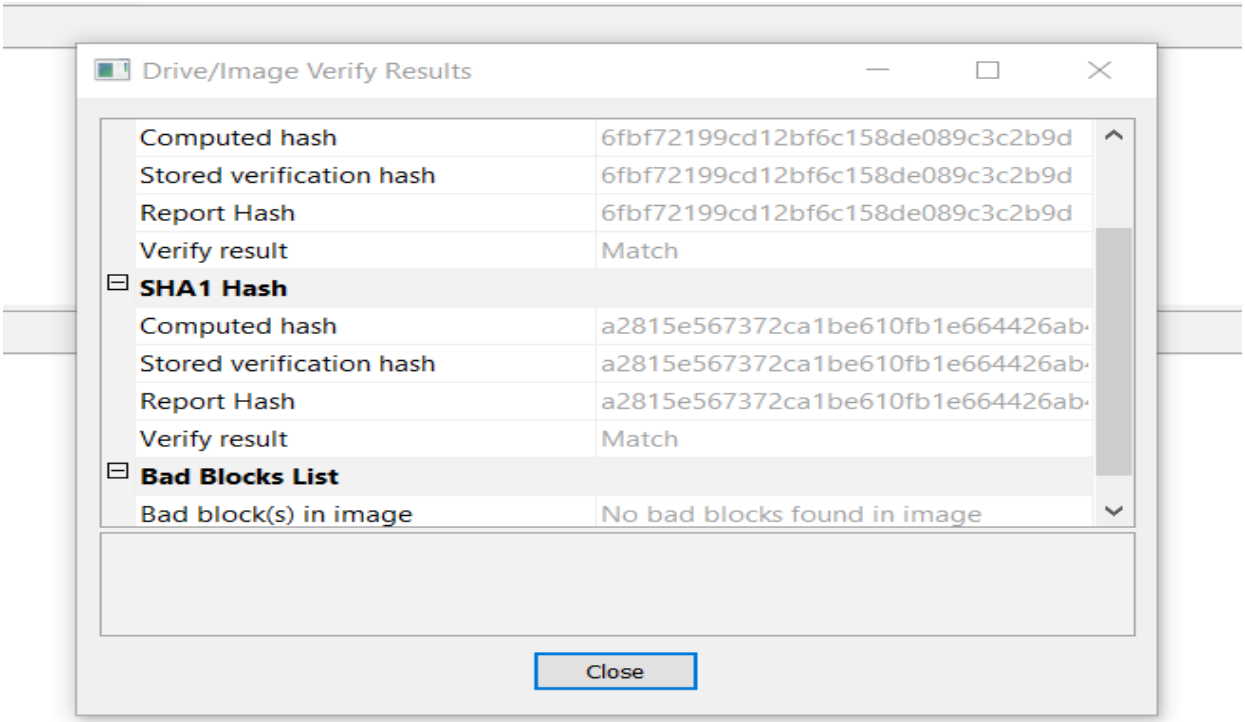
Steps Followed:

1. **Data Preparation:** I used a thumb drive of 16 GB. I then copied files including images, documents, and a PDF to the drive. I then deleted some files so to simulate typical user activity.
2. **Write-Blocking:** |I installed SafeBlock from ForensicSoft. I activated SafeBlock to write-block USB ports.Verified that the thumb drive was accessible but not writeable.
3. **Imaging with FTK Imager:**

   I Opened **FTK Imager**,then navigated to File > Create Disk Image. I then selected **Physical Drive** and chose the USB device. The next step was to set the image type to **E01 (Expert Witness Format)**. After that I added destination path and image name. I then enabled **MD5 hashing** for verification. The imaging process completed successfully.

4. **Result:**
   - ✓ FTK Imager generated an .E01 image file.
   - ✓ Image Summary file was saved (includes size, hash, sector info, etc.).

MD5 Hash:



PART 2: Custom Content Image using FTK Imager

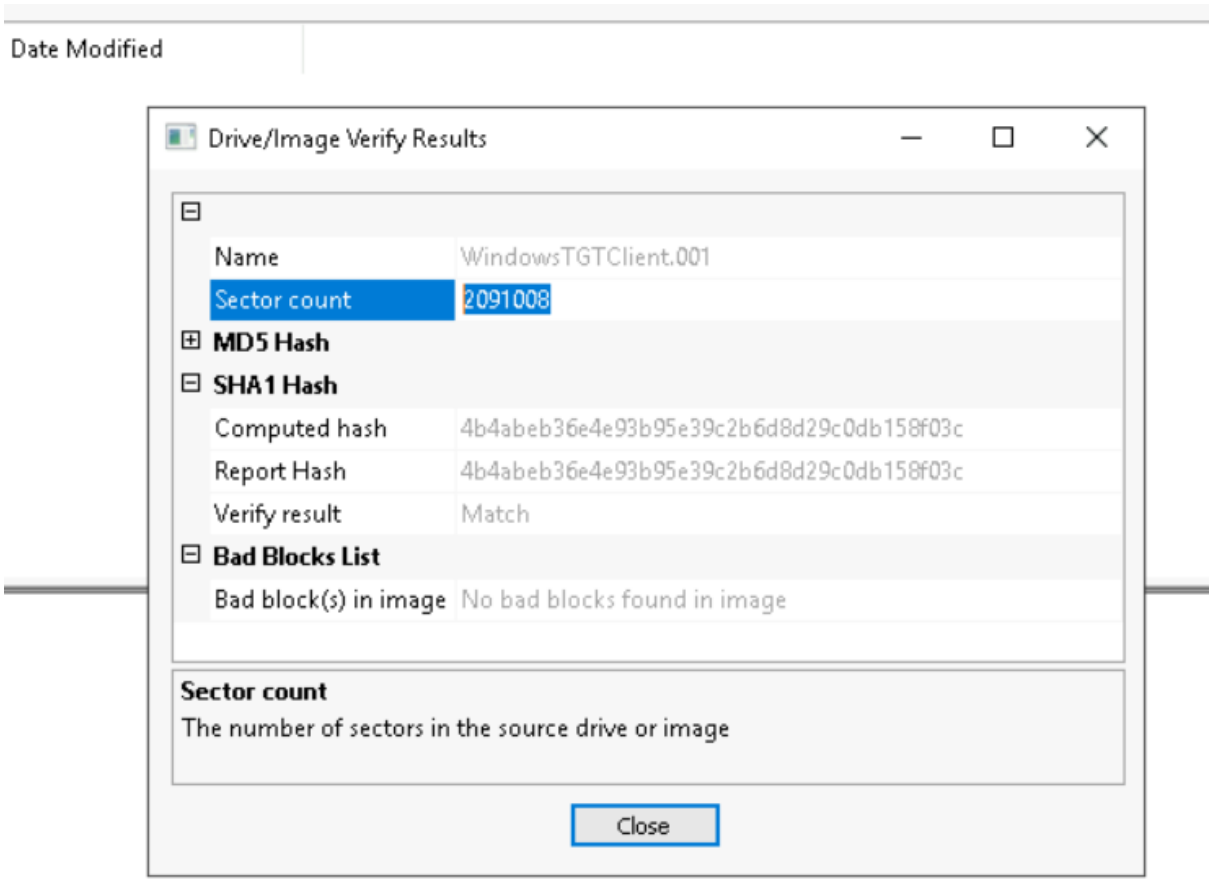
Overview:

I created a custom content image using FTK Imager. I selected specific files from the thumb drive and imaged separately.

Steps Followed:

1. **Selecting Files:**
   i. Choose specific files originally copied to the thumb drive:
      - file1.docx
2. **Creating Custom Image:**
   i. Opened FTK Imager.
   ii. Went to File > Create Custom Content Image.
   iii. Added the selected files.
   iv. Chose E01 format for output.
   v. Set the destination folder and image name.
   vi. Enabled **MD5 hashing**.
   vii. Imaging completed without error.
3. **Result:**
   i. Custom content .E01 image created.
   ii. FTK Imager generated a summary document.

MD5 Hash:



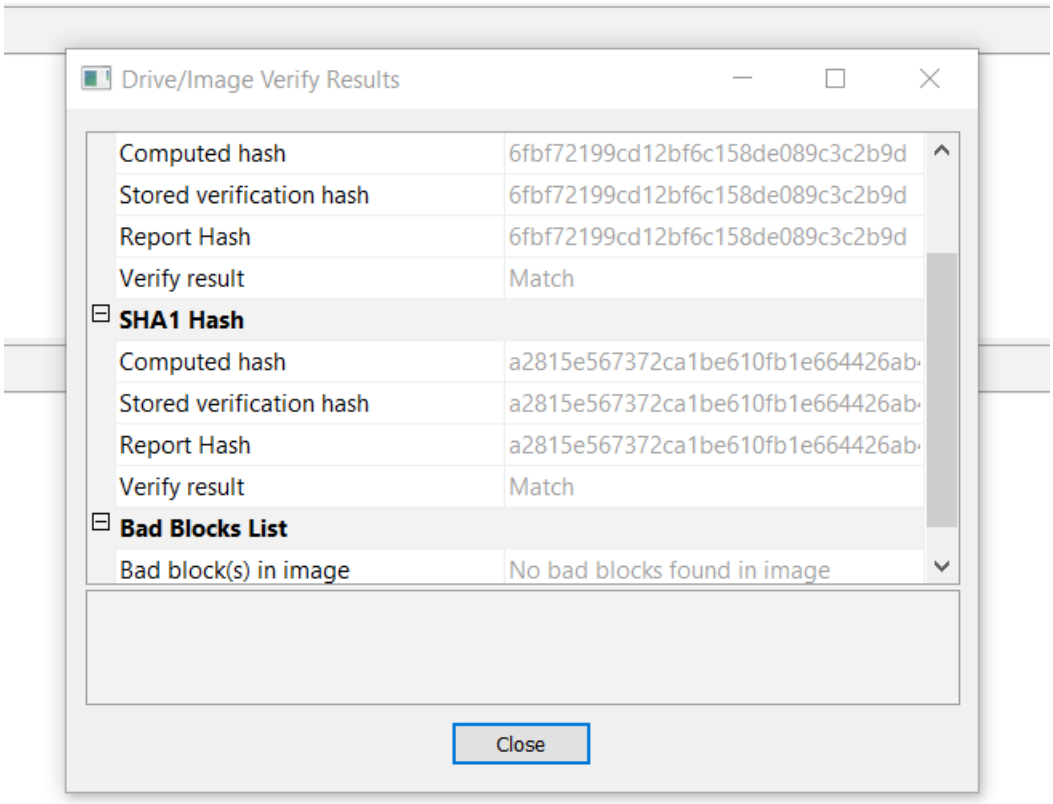
PART 3: Imaging a Non-Thumb Drive Media

I USED A 16GB SDcard and FTK.

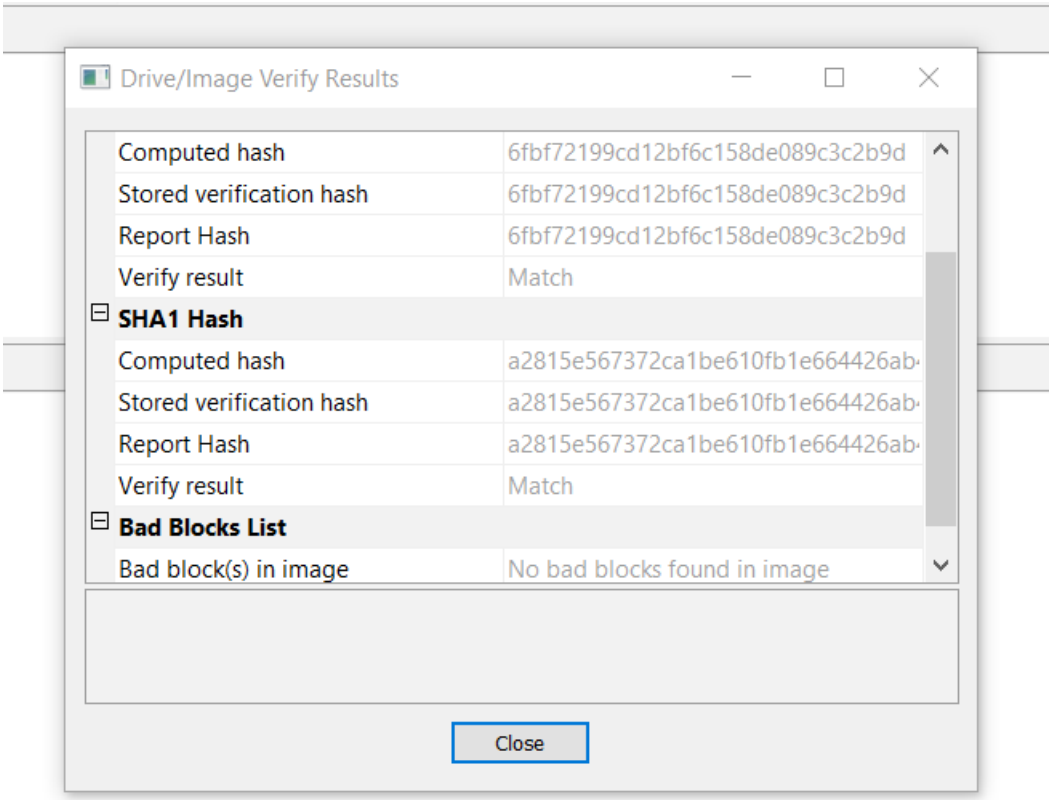
Steps I followed:

1. **Write Protection:**
   - ✓ For SD card: Lock switch enabled.
2. **Imaging:**
   - ✓ Opened FTK Imager.
   - ✓ Choose Create Disk Image.
   - ✓ Selected the correct media under physical drives.
   - ✓ Choose E01 as the image format.
   - ✓ Entered case details and set destination.
   - ✓ Imaging completed successfully.
3. **Output:**
   - ✓ Image file created and saved.
   - ✓ A summary or screenshot was captured for evidence.

MD5 Hash:



Screenshots



All three forensic images were created successfully following best practices. SafeBlock ensured USB devices were properly write-blocked. FTK Imager was used for all imaging tasks, and MD5 hashing was performed to validate the integrity of each image. The project demonstrates practical use of industry tools and methods for handling and preserving digital evidence.

Contact Me if you need assistance:

kibetarwa@gmail.com Email

info@achieve100percent.com

+254754455078 - WhatsApp