

Lab 2

Introduction to Forensics Tools and Data Acquisition

Mina Salehi

University of Maryland Baltimore County

CYBR 642 Introduction to Digital Forensics

Presented to: Gina Scaldaferri

02/12/2025

Introduction

Digital Forensics and Incident Response (DFIR) tools play a vital role in investigating and preserving digital evidence in cybersecurity and legal contexts. This lab focuses on acquiring and analyzing images of USB storage devices using FTK Imager and ProDiscover to uncover previously deleted data.

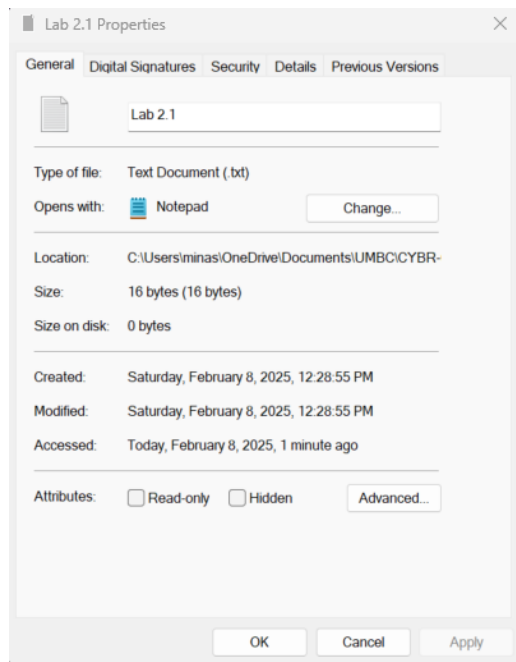
Understanding the process of data imaging ensures that investigators can create accurate copies of digital evidence while maintaining its integrity. By simulating a real-world forensic investigation, this lab enhances students' ability to acquire, verify, and analyze digital evidence while ensuring its integrity and admissibility in legal proceedings (Nelson et al., 2020).

Pre-Analysis

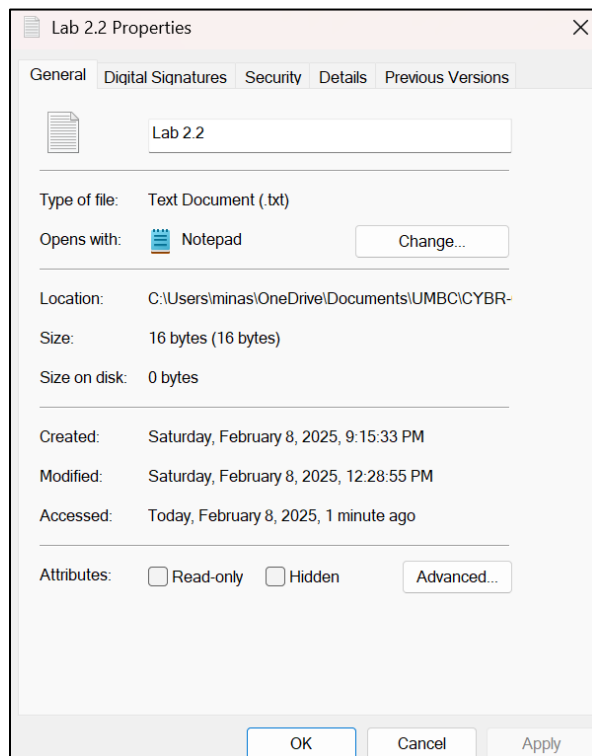
In digital forensics, validating tools and evidence is essential to maintaining data integrity and ensuring that forensic processes are repeatable and verifiable (Nelson et al., 2020). One of the most crucial techniques for preserving evidence is hashing, which generates a unique digital fingerprint for files, ensuring integrity throughout an investigation (Casey, 2011). This lab demonstrates the significance of hash values by comparing the MD5 and SHA1 hashes of multiple text files under different conditions. By analyzing how various modifications impact hash values, forensic investigators can understand how to authenticate digital evidence and detect unauthorized changes effectively (Schneier, 1996).

Step-by-Step Procedure for Hash Verification and Analysis

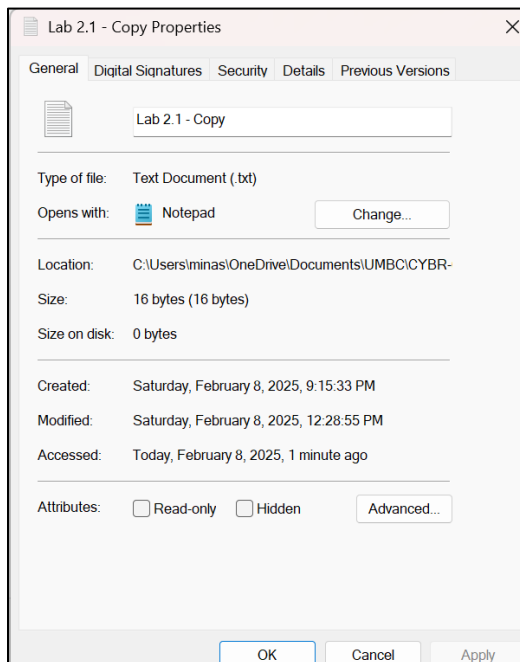
Step 1: Open Notepad, enter a random phrase, and save the file as "Lab 2.1".



Step 2: Wait for one hour, create an exact copy of the original file and rename it to "Lab 2.2".



Step 3: Create a copy of the original text file, add a new phrase to the document and save it as “Lab 2.1 - Copy”.



Step 4: On the browser go to the following website: <https://www.pelock.com/products/hash-calculator>, upload the files, and capture the MD5 and SHA1 hash values for all 3 files.



LAB 2.1

- MD5: 0EE29CB68A578231D6493250C881BC2E
- Sha1: 49610AA094CF072E857C01D8DC5F60BADEF627D2

md5	16	0EE29CB68A578231D6493250C881BC2	
sha1	20	49610AA094CF072E857C01D8DC5F60B	



Lab 2.2

- MD5: 0EE29CB68A578231D6493250C881BC2E
- Sha1: 49610AA094CF072E857C01D8DC5F60BADEF627D2

md5	16	0EE29CB68A578231D6493250C881BC2	
sha1	20	49610AA094CF072E857C01D8DC5F60B	

Lab 2.1 Copy

- MD5:C07162ABAACE4A60C8735D2EA5815C93
- Sha1:E8721014F4036513AEA58800C5DD43DC26954C87

md5	16	C07162ABAACE4A60C8735D2EA5815C93	
sha1	20	E8721014F4036513AEA58800C5DD43DC26954C87	

1. Were text file 1 and text file 2 hash values the same? Why or why not?

Yes, the hash values of text file 1 and text file 2 were the same. This is because renaming a file does not alter its contents—only its file system metadata, such as the file name, is modified. Hashing algorithms generate a unique fingerprint based solely on a file's content, not its name or location (Baryamureeba & Tushabe, 2004).

2. Was the hash the same for text file 1 and text file 3? Why or why not?

No, the hash values of text file 1 and text file 3 were different. This is because text file 3 contained additional data, meaning its binary representation changed. Hash functions, such as MD5 and SHA1, are designed so that even the smallest change in a file's content results in an entirely different hash value (Schneier, 1996).

3. Why are hash values important in digital forensics?

Hash values are critical in digital forensics because they ensure data integrity, authenticity, and verification of digital evidence (Nelson et al., 2020). By hashing files before and after forensic analysis, investigators can prove that evidence was not altered, ensuring admissibility in court.

4. What actions change the hash value of a file and why?

Any modification to a file's content—such as editing, appending text, deleting characters, or altering its encoding—will change its hash value. This occurs because hash algorithms process a file's binary data and generate a unique fingerprint for its exact content. Even a single character change results in a completely different hash, a property known as the avalanche effect in cryptographic hashing (Schneier, 1996).

5. What doesn't change the hash value of a file and why?

Renaming a file, changing its location, or altering its metadata (such as access or modified timestamps) does not change its hash value. This is because hashing algorithms only process the actual contents of a file, not its external attributes. Forensic tools rely on this property to verify data integrity while allowing files to be copied or moved without altering their hash values (Baryamureeba & Tushabe, 2004).

Analysis

This lab focuses on using ProDiscover and FTK Imager to acquire forensic images of two USB drives that may contain evidence related to a fraud investigation. Additionally, the lab emphasizes the importance of hash values to verify the integrity of forensic images, ensuring that no alterations occur during acquisition. By following structured imaging procedures, investigators can maintain the chain of custody, making the evidence admissible in court and useful in cybersecurity investigations (Casey, 2011).

Step-by-Step Procedure for Imaging USB Drives Using ProDiscover

Step 1: Setting Up the Image Acquisition Area

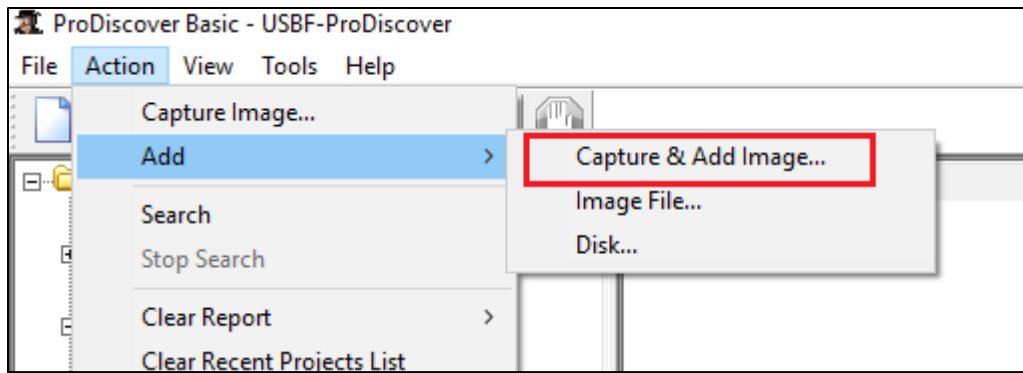
1. Open the Windows Virtual Machine (VM).
2. Navigate to the Desktop and create a new folder named Image_File.
3. Inside the Image_File folder, create two subfolders: ProDiscover
4. Inside the ProDiscover folder, create two additional subfolders: USBF (for USB drive F) and USBU (for USB drive U)

Step 2: Acquiring a Forensic Image of USB Drive F Using ProDiscover

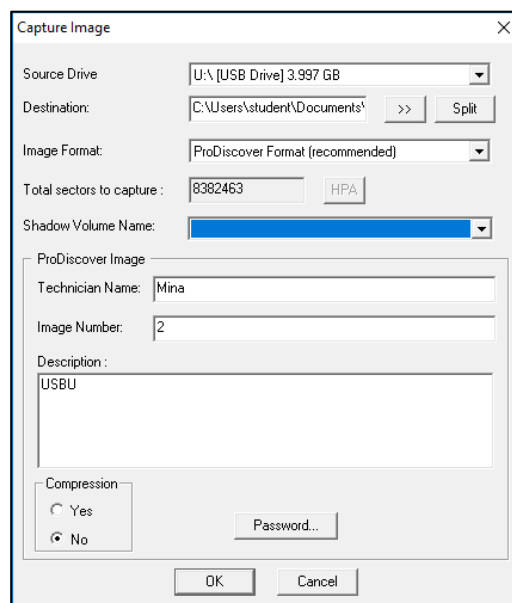
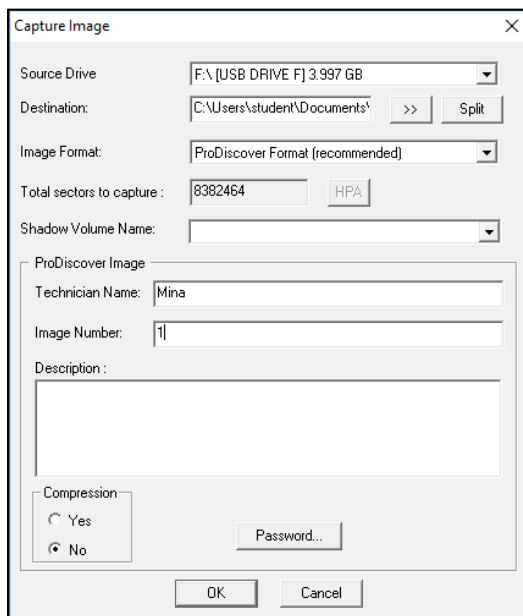
1. Open ProDiscover Basic from the start menu.
2. Click on File → New Project to create a new project.
3. In the Project File Name field, entered "USBF_ProDiscover."



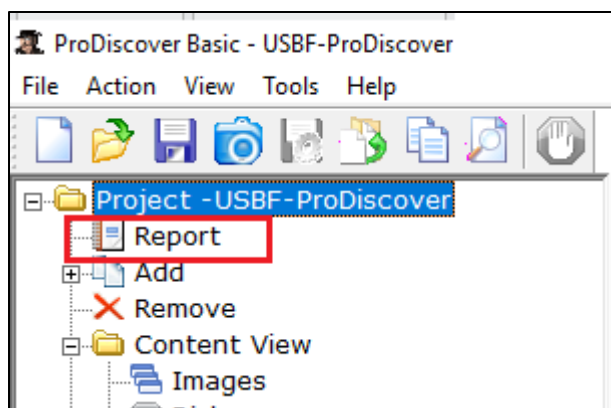
4. In the Action menu, select Add → Capture & Add Image.



5. In the Capture Image dialog box: Select USB drive (F:) as the Source Drive.
6. Navigate to C:\Users\student\Documents\Image_File\ProDiscover\USBF.
7. Enter USB-Pro-F in the File Name text box.
8. In the Technician Name field, typed Mina.



9. After imaging is complete, clicked on Report from the side menu.



10. Repeated steps 2-9 above for USBU and named the project file USBU_ProDiscover.

Step 3: Verify the Image Format and Hash Value for USB Drive F and USBU

Evidence Report for Project: USBF-ProDiscover

Project Number: USBF

Project Description:

Image Files:

File Name: C:\Users\student\Documents\Image_File\ProDiscover\USBF\USBF.eve

Image File Type: DFT Image

File Number: 1

Technician Name: Mina

Date: 02/08/2025

Time: 13:41:34

MD5 Checksum: e9cd3adcec8238201d9eca1994f077db

Checksum Validated: No

Compressed image: No

Time Zone Information:

Time Zone: (GMT-05:00) Bogota, Lima, Quito (SA Pacific Standard Time)

Daylight savings (summertime) was in effect: No

Time Zone information obtained automatically from remote system/image.

Hard Disk: C:\Users\student\Documents\Image_File\ProDiscover\USBF\USBF.eve

Volume Name: NO NAME

Volume Serial Number : D630-76B6

File System: FAT32

Bytes Per Sector: 512

Total Clusters: 1044736

Sectors per cluster: 8

Total Sectors: 8382464

Hidden Sectors: 2048

Total Capacity: 4191232 KB

Start Sector: 0

End Sector: 8382463

Evidence Report for Project: USBU-ProDiscovery**Project Number:** USBU**Project Description:****Image Files:****File Name:** C:\Users\student\Documents\Image_File\ProDiscover\USB\ProDiscover-USB.eve

Image File Type: DFT Image

File Number: 2

Technician Name: Mina

Date: 02/08/2025

Time: 16:38:29

MD5 Checksum: 6ab43cbcea475d2ccdbf2011a9eee562

Checksum Validated: No

Compressed image: No

Time Zone Information:

Time Zone: (GMT-05:00) Bogota, Lima, Quito (SA Pacific Standard Time)

Daylight savings (summertime) was in effect: No

Time Zone information obtained automatically from remote system/image.

Hard Disk: C:\Users\student\Documents\Image_File\ProDiscover\USB\ProDiscover-USB.eve

Volume Name: USB Drive

Volume Serial Number : 4AE2-34AD

File System: NTFS

Bytes Per Sector: 512

Total Clusters: 1047807

Sectors per cluster: 8

Total Sectors: 8382463

Hidden Sectors: 2048

Total Capacity: 4191231 KB

Start Sector: 0

End Sector: 8382462

1. What is the resulting file format of the image?

The resulting file format for the ProDiscover forensic image is .eve. This format is specific to ProDiscover and is used for forensic disk imaging, allowing the preservation of evidence in a structured manner (Nelson et al., 2020).

2. What is the hash of the image?

USBU-ProDiscover MD5 Checksum: 6ab43cbcea475d2ccdbf2011a9eee562

USBF-ProDiscover MD5 Checksum: e9cd3adcec8238201d9eca1994f077db

3. Why is the hash value important in digital forensics?

Hash values are critical in digital forensics because they:

- Ensure data integrity by confirming that the image has not been altered (Casey, 2011).
- Provide verification that the forensic copy is an exact replica of the original evidence.
- Maintain chain of custody, making the evidence admissible in court.
- Facilitate duplicate detection, ensuring forensic analysts do not analyze redundant data.

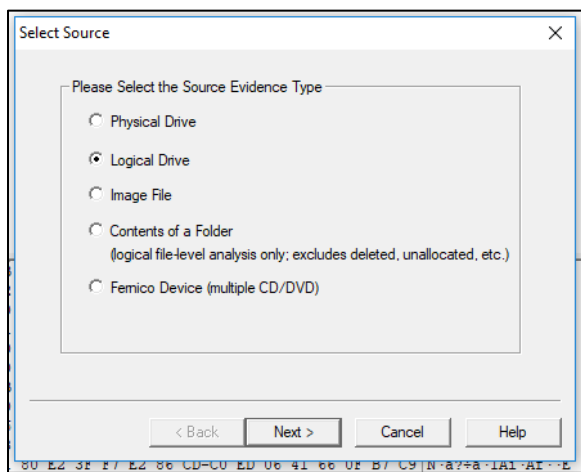
Step-by-Step Procedure for Imaging USB Drives Using FTK Imager

Step 1: Setting Up the Image Acquisition Area

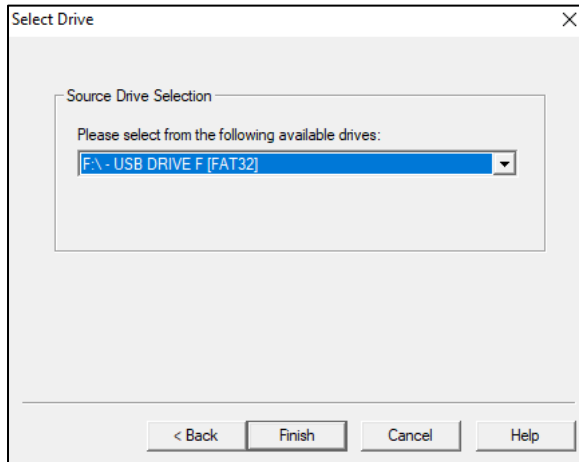
1. Open the Windows Virtual Machine (VM).
2. Navigate to the Desktop and create a new folder named Image_File.
3. Inside the Image_File folder, create a subfolder named FTKImager.
4. Inside the FTKImager folder, create two additional subfolders: USBF (for USB drive F) and USBU (for USB drive U)

Step 2: Acquiring a Forensic Image of USB Drive F Using FTK Imager

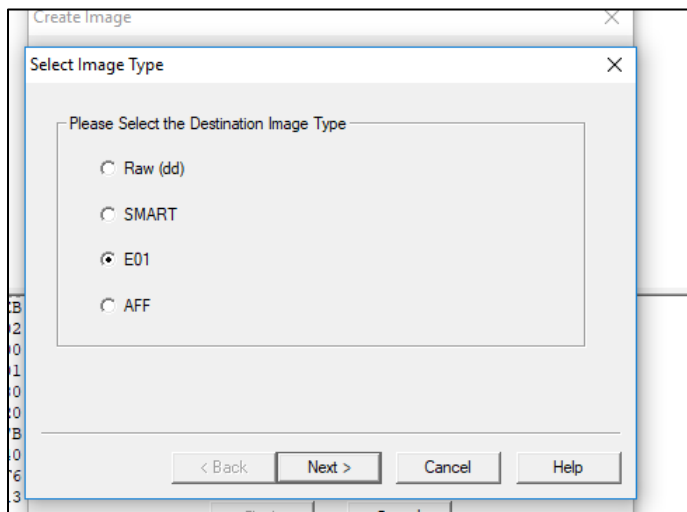
1. Open FTK Imager.
2. Click File → Create Disk Image to begin the imaging process.
3. In the Select Source dialog, choose the Logical Drive option and click Next.



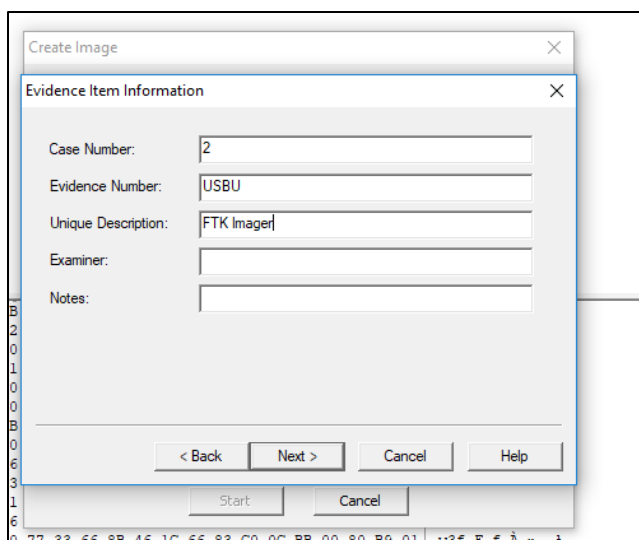
4. In the Select Drive dialog, select the F:\-USB Drive F from the list, then click Finish.



5. In the Create Image dialog, click Add.
6. For Image Type, select E01 (EnCase Image File Format) and click Next.



7. In the Evidence Item Information dialog box: Type your name as the Examiner.
8. For the Case Number and Evidence Number, enter USBF-FTK.



9. Click Next to proceed.

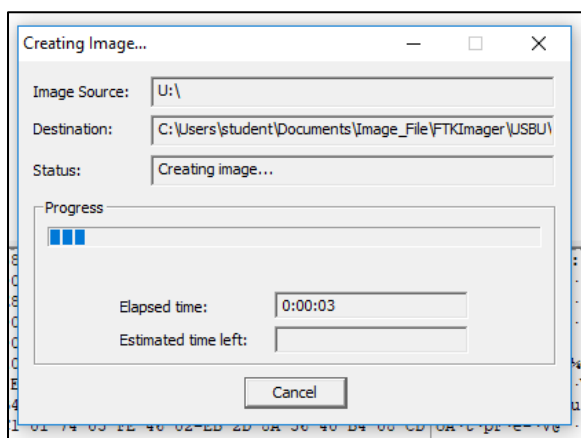
10. In the Image Destination Folder: Select

C:\Users\student\Document\Image_File\FTKImager\USBF as the destination folder.

11. In the Image File Name text box, type USBF-FTK.

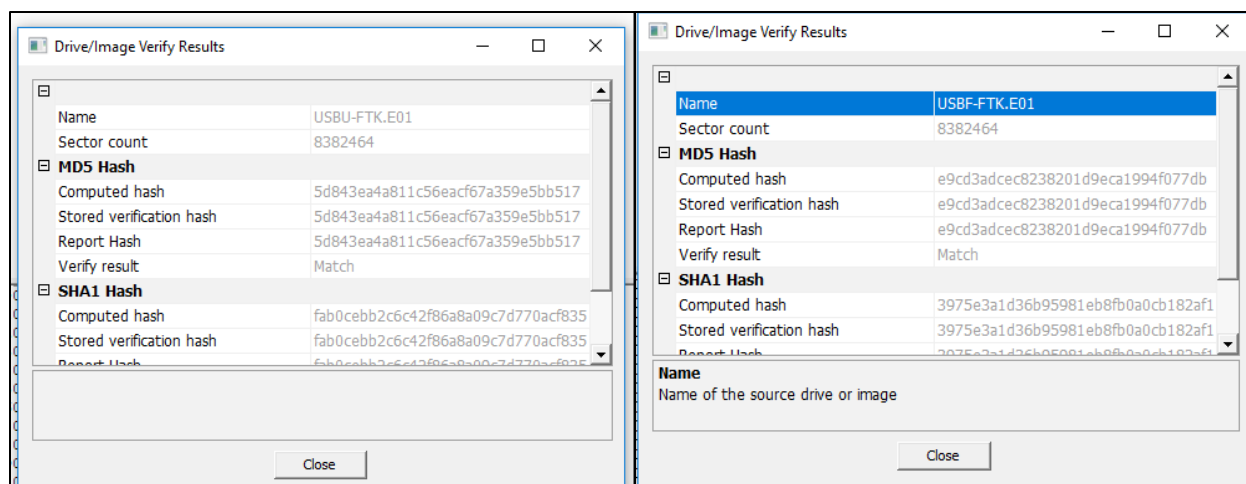
12. Click Finish.

13. When returned to the Create Image dialog, click Start to begin the imaging process.



14. Once imaging is completed, document the process and verify the hash value to ensure the integrity of the image.

15. Repeat Steps above for USBU, name the project file USBU-FTK.



What is the resulting File format of the image?

The resulting file format of the forensic image created using FTK Imager is E01. The E01 file extension stands for EnCase image file format used by EnCase software. The file is used to store digital evidence including volume images, disk image, memory and logical files. (WhatIsFileExtension.com, n.d.)

What is the hash of the image?

USBF:

MD5 checksum: e9cd3adcec8238201d9eca1994f077db

SHA1 checksum: 3975e3a1d36b95981eb8fb0a0cb182af194ff014

USBU:

MD5 checksum: 5d843ea4a811c56eacf67a359e5bb517

SHA1 checksum: fab0cebb2c6c42f86a8a09c7d770acf83505e328

Comparing Hash Values

1. Is the hash for USB F in ProDiscover the same as the hash for USB F in FTK Imager? Why or why not?

Yes, the hash for USB F in ProDiscover and FTK Imager were the same. This is because both tools created a forensic image of the same USB drive without modifying its contents. Hash values are generated based on the actual data on the drive, not the imaging tool used. Since the imaging process was properly executed in both programs, the integrity of the data remained intact, resulting in the same MD5 and SHA1 hash values.

2. Is the hash for USBU in ProDiscover the same as the hash for USB U in FTK Imager? Why or why not?

No, the hash for USB U in ProDiscover and FTK Imager were different. This indicates that something changed between the imaging processes. Possible reasons include:

- ProDiscover and FTK Imager use different imaging techniques that may affect the final image hash.
- FTK Imager creates forensic images in the E01 format (EnCase format), which supports compression and embedded metadata.
- ProDiscover may capture a raw sector-by-sector copy, preserving all sectors differently than FTK Imager.
- Even if the file contents are identical, slight variations in how the tools capture disk sectors or store image metadata can cause hash mismatches.
- FTK Imager allows for compression when storing forensic images in the E01 format, which can alter the final image hash.
- Some forensic tools recover and store deleted files differently.
- ProDiscover and FTK Imager may handle unallocated space, slack space, and deleted file records in different ways.
- If the USB device had fragmented files, ProDiscover and FTK Imager may reconstruct them differently.

3. If they were not the same would you expect them to be?

Yes, the hash values should have been the same if both tools imaged the exact same data in an identical manner. However, there might be differences in imaging methods between two different tools to handle sectors or capturing allocated data.

4. Which program did you prefer to use ProDiscover or FTK Imager?

I prefer FTK Imager for forensic imaging because it provides stronger compatibility, industry-standard formats (E01), and metadata-rich reporting.

Conclusion

This lab illustrates the significance of hash values in digital forensics by demonstrating how file modifications impact cryptographic fingerprints. Investigators can use hashing techniques to authenticate evidence and detect unauthorized changes in digital files. By ensuring that digital evidence remains unaltered and verifiable, forensic analysts maintain the chain of custody and uphold the integrity of investigations. Understanding how and why hash values change is fundamental to ensuring that forensic processes are repeatable, defensible, and legally admissible in a court of law.

In pre-analysis, we observed that modifications to a file's content result in different MD5 and SHA1 hash values, whereas certain changes, such as renaming the file, do not alter the hash values. In the analysis, we compared hash values for USB drives using ProDiscover and FTK Imager to demonstrate the importance of consistent forensic imaging practices to ensure hash values remain the same across tools. While USB F maintained identical hash values across both tools, USB U showed a variation, highlighting potential issues such as file system differences, metadata changes, or imaging methodology variations. This experiment emphasizes the need for strict forensic protocols, proper evidence handling, and verification techniques to maintain digital evidence integrity.

Glossary

Chain of Custody - The chain of custody is the documented process that tracks the handling, control, and integrity of evidence from its collection to its presentation in court. Maintaining a strict chain of custody ensures that digital evidence remains unaltered and admissible in legal proceedings (Casey, 2011).

E01 (EnCase Image Format) - The E01 format is a forensic disk image file format used to store complete forensic copies of digital evidence. It supports compression, metadata storage, and verification hash values, making it a standard format in digital forensics (Nelson et al., 2020).

Forensic Imaging - Forensic imaging is the process of creating an exact copy of a storage device, preserving all data, including deleted files, unallocated space, and system metadata. This technique is used in digital investigations to ensure that analysis does not alter the original evidence (Casey, 2011).

Hash Value - A hash value is a fixed-length, unique string generated by a cryptographic hashing algorithm (e.g., MD5, SHA-1, or SHA-256) that represents a file's contents. Hashing is used in digital forensics to verify the authenticity and integrity of evidence (Schneier, 1996).

MD5 (Message Digest Algorithm 5) - MD5 is a cryptographic hashing algorithm that produces a 128-bit hash value. It is used to verify file integrity in forensic imaging, although it is considered cryptographically weak due to its vulnerability to hash collisions (Wang & Yu, 2005).

Metadata - Metadata is data about data, providing information such as timestamps, file size, and access history. In forensic analysis, metadata helps investigators determine when, where, and how a file was created, modified, or accessed (Casey, 2011).

RAW Image Format - The RAW format is a bit-for-bit copy of a storage device without any additional metadata or compression. While RAW images maintain exact copies of the original data, they require more storage space compared to compressed forensic image formats like E01 (Casey, 2011).

SHA-1 (Secure Hash Algorithm 1) - SHA-1 is a cryptographic hash function that produces a 160-bit hash value. It is used in forensic investigations to verify data integrity, though it has been replaced by SHA-256 due to vulnerabilities in its security (Schneier, 1996).

Reference

Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model.

Digital Investigation, 1(1), <C:\research\papers\paper1.DVI>

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press.

Nelson, B., Phillips, A., & Steuart, C. (2020). Guide to computer forensics and investigations (6th ed.). Cengage Learning.

Schneier, B. (1996). Applied cryptography: Protocols, algorithms, and source code in C (2nd ed.). John Wiley & Sons.

Wang, X., & Yu, H. (2005). How to break MD5 and other hash functions. *Advances in Cryptology – EUROCRYPT 2005*, 19-35.

WhatIsFileExtension.com. (n.d.). *What is .E01 file extension? EnCase image file format.* from <https://www.whatisfileextension.com/e01/>