HACKER
ACADEMY

DATA CLONING AND FORENSIC IMAGING

Forensic Module - 4

PRESENTED TO

Keerthi TR

APPORVED BY

Ayush Singh

HACKER ACADEMY

TABLE OF CONTENTS

DISCLAIMER

The First Response and Containment Lab trains individuals to handle cybersecurity incidents, focusing on swift threat identification, containment, and mitigation. It provides hands-on experience with simulated attack environments, forensic analysis tools, and documentation systems. Key objectives include immediate threat detection, rapid containment, evidence preservation, and effective communication. Training modules cover incident detection, containment strategies, evidence collection, recovery, and communication protocols. The lab equips responders with the skills and knowledge to manage and resolve security incidents efficiently, ensuring robust incident response and improved security posture.

TECHNICAL ANALYSIS

1.An affected folder is selected from the system which has critical data.

2.FTK imager is downloaded and the particular folder is added to image it.

3.Checked whether the file integrity is maintained by looking at MD5 and SHA algorithm

Windows 11 in Base System

Specification :

Manufacturer - HP

Processor -Intel(R) Core(TM) i3

Installed RAM - 8'00 GB

System type - 64-bit operating system, x64-based processor

OS - Windows 11 Home Single Language

Evidence Source and Analysis -FTK Imager

TECHNICAL TIMELINE

- 18-05-2024/02:50 PM – Folder having critical data is identified
- 18-05-2024/03:20 PM – FTK imager is used to image the folder
- 18-05-2024/03:56 PM – Imaging process is started
- 18-05-2024/04:20 PM- IMAGING PROCESS IS COMPLETED AND DATA INTEGRITY IS VERIFIED

TOOLS USED

Ø Windows 11 as base Operating System

· Windows 11 represents Microsoft's latest iteration of its flagship operating system, succeeding Windows 10. It brings a range of new features, enhancements, and a fresh user interface design to the Windows ecosystem

· Windows 11 represents a significant step forward for the Windows platform, offering users a more modern and intuitive experience, enhanced productivity features, and improved gaming capabilities, while also providing developers with new opportunities to create and distribute apps.

Ø FTK Imager

· . FTK Imager is a digital forensic software tool developed by AccessData. It is widely used by forensic investigators, law enforcement agencies, and cybersecurity professionals for acquiring and analyzing digital evidence from various storage media and file systems.

IDENTIFICATION

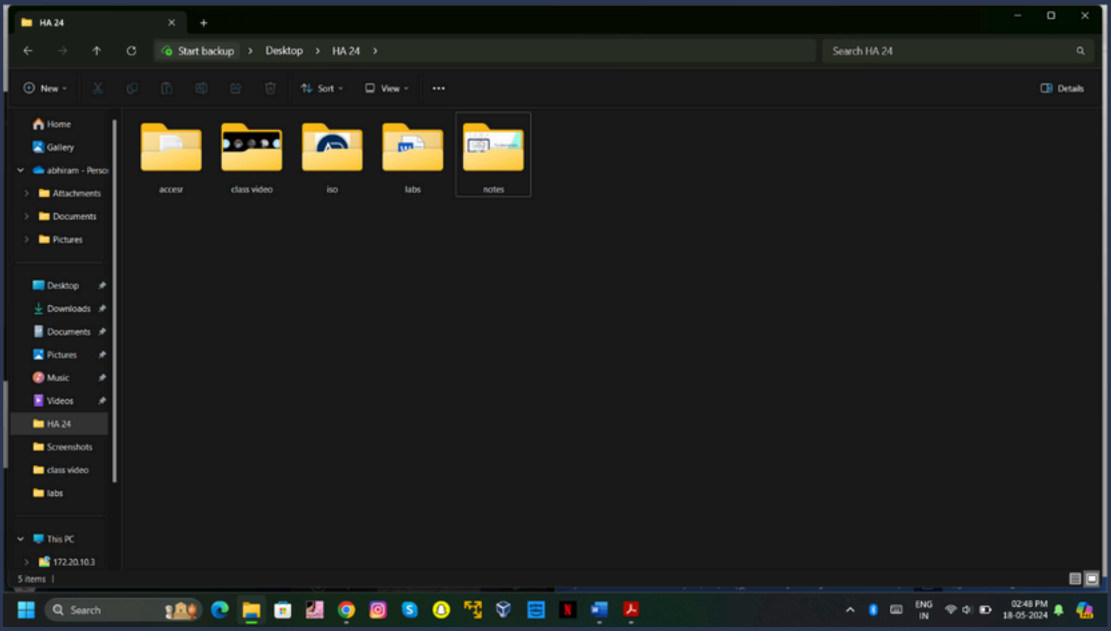


FIG:1 FOLDER HAVING CRITICAL DATA

As custodians of this critical data, it is imperative that we prioritize its security and protection. Any compromise or unauthorized access to these folders could have severe consequences, including financial loss, damage to our reputation, and legal ramifications.

Protecting folders containing critical data is not just a responsibility; it's a fundamental requirement for safeguarding our organization's interests and maintaining the trust of our stakeholders.

METHODOLOGY

•Download FTK Imager version 4.7.1.2 from https://www.exterro.com/ the official website for downloading different and latest version of FTK imager.

•Install FTK imager from the setup file which was downloaded from the previous steps.

•After installation the software GUI will look like the image below

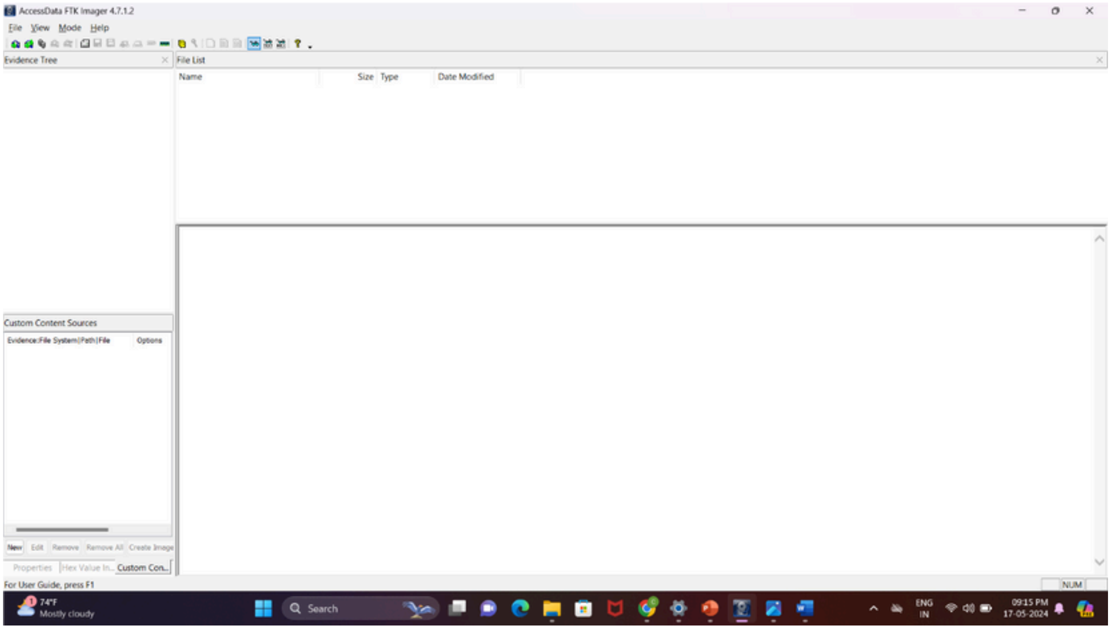
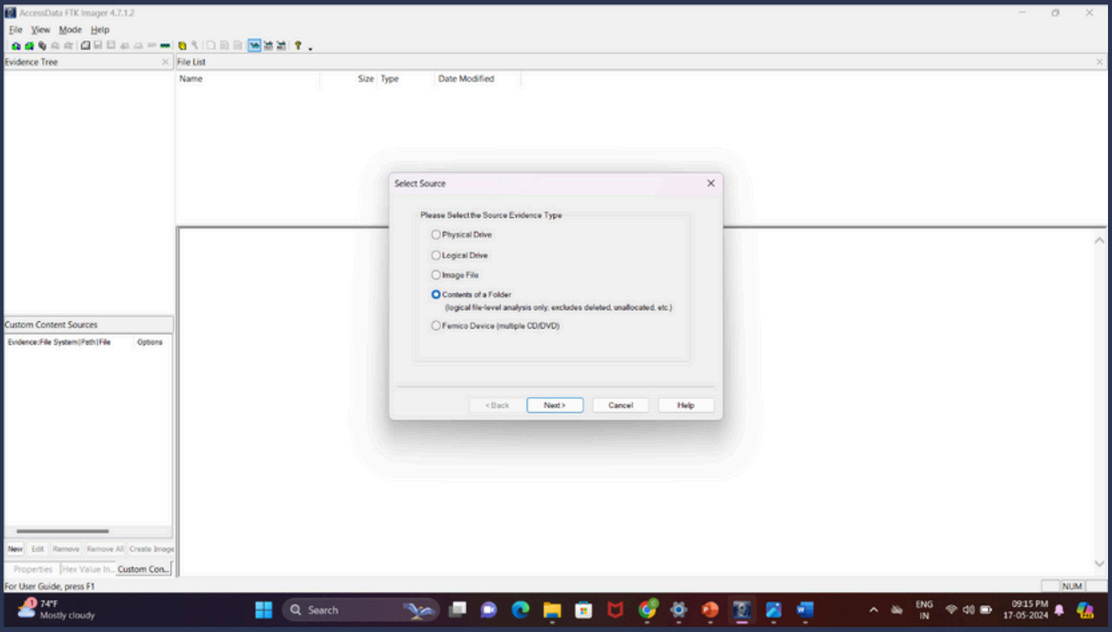


Fig:2 GUI for FTK Imager

· The next step is to create a disk image for theparticular file that needs to be imaged.



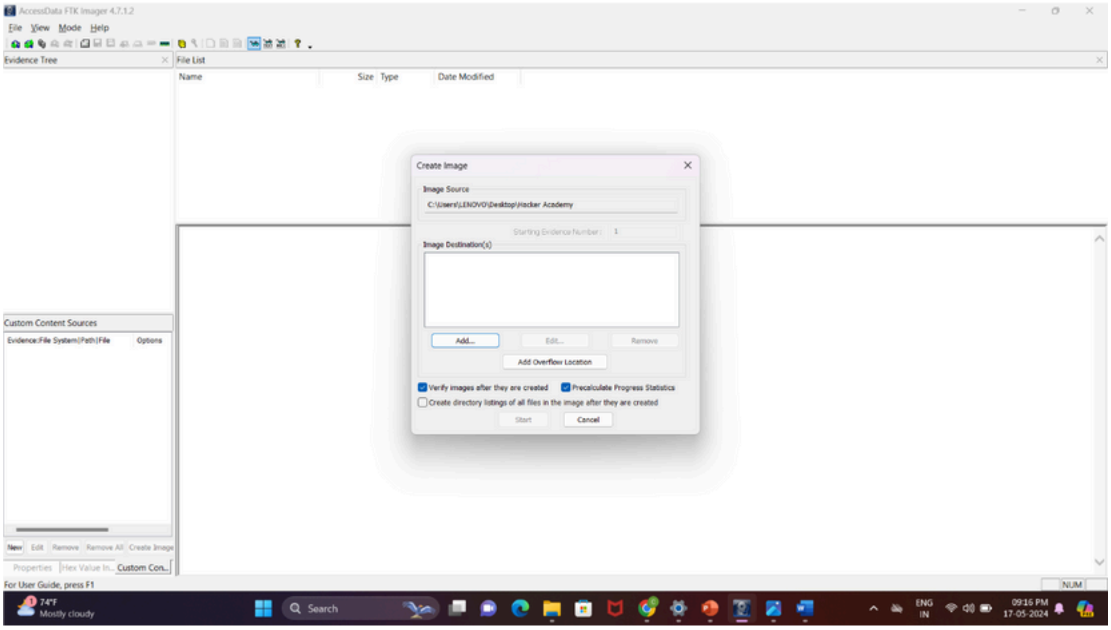
Select Source

Please Select the Source Evidence Type

○ Physical Drive
○ Logical Drive
○ Image File
● Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
○ Femico Device (multiple CD/DVD)

Fig:3 Choosing the source evidence type

·When choosing the source evidence type in a digital forensic investigation, several factors need to be considered to ensure the accuracy, integrity, and relevance of the evidence collected ,investigators can choose the most appropriate source evidence type to support their digital forensic investigation effectively. This ensures that relevant evidence is collected in a legally sound and forensically sound manner, facilitating the resolution of the case and supporting any subsequent legal proceedings.



Create Image

Image Source

C:\Users\LENOVO\Desktop\Hacker Academy

Starting Evidence Number: 1

Image Destination(s)

Add... Edit... Remove

Add Overflow Location

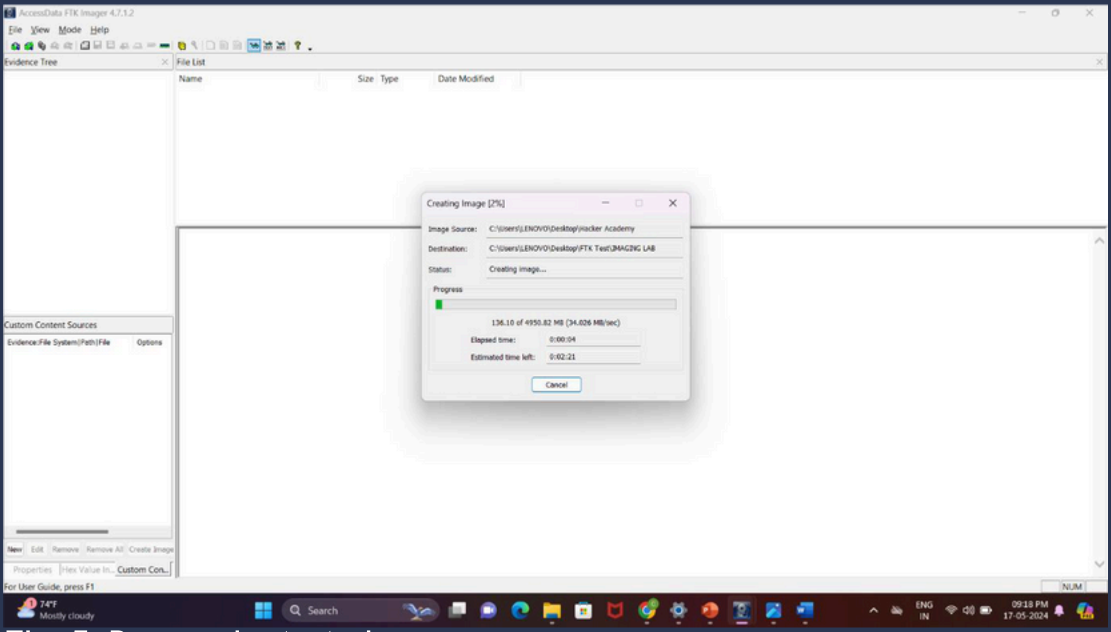
☑ Verify images after they are created ☑ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

Start Cancel

Fig:4 Source is added

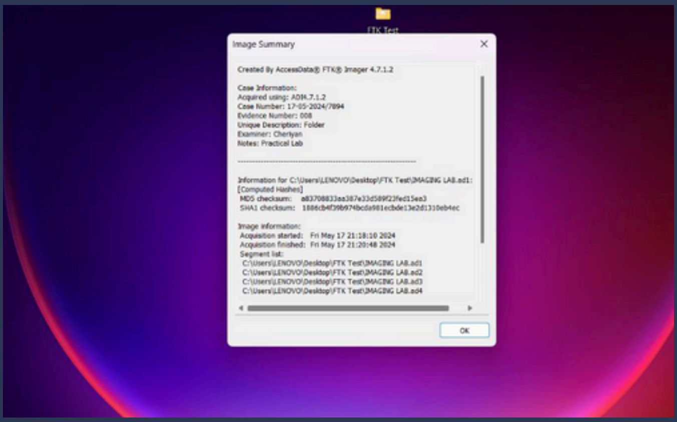
·If the source has been added to your digital forensic investigation, it's essential to verify and document its integrity and relevance before proceeding further,you can ensure that the added source is thoroughly examined, validated, and documented, laying the foundation for a comprehensive and effective digital forensic investigation.


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
Name
Size Type
Date Modified
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value In... Custom Con...
For User Guide, press F1
NUM

```
Creating Image [2%]

Image Source:   C:\Users\LENOVO\Desktop\Hacker Academy
Destination:    C:\Users\LENOVO\Desktop\FTK Test\IMAGING LAB
Status:         Creating image...

Progress
        136.10 of 4950.82 MB (34.026 MB/sec)
    Elapsed time:          0:00:04
    Estimated time left:   0:02:21

                 Cancel
```

Fig: 5 Process is started

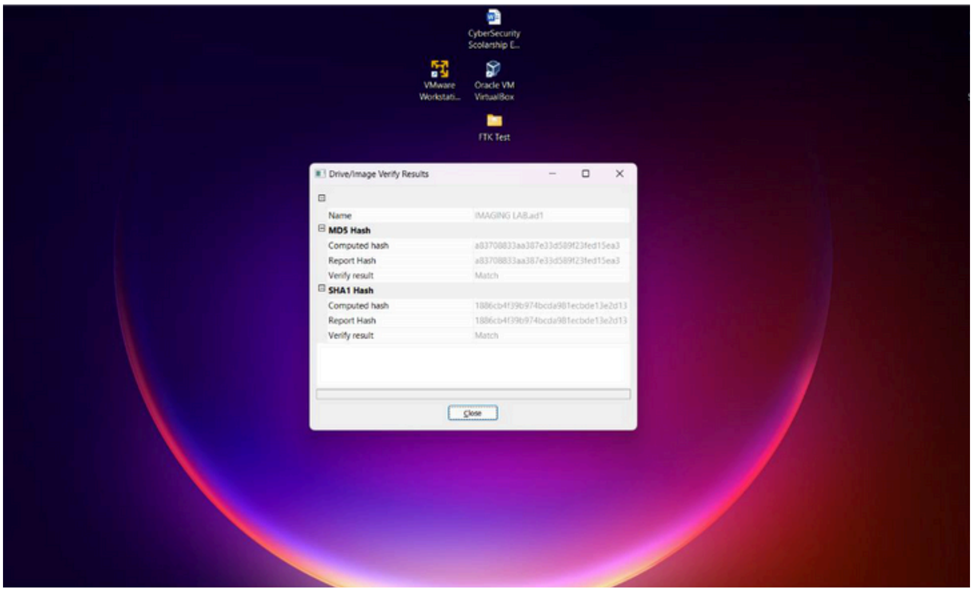
· As we can see from the image that a total of4950.82MB of data needs to be imaged and it will take considerable amount of time for the process to be completed. As the file size increases the time taken for imaging also increases.



```
Image Summary

Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 17-05-2024/7894
Evidence Number: 008
Unique Description: Folder
Examiner: Cheriyan
Notes: Practical Lab

--------------------------------------------------------------

Information for C:\Users\LENOVO\Desktop\FTK Test\IMAGING LAB.ad1:
[Computed Hashes]
 MD5 checksum:    a83708833aa387e33d589f23fed15ea3
 SHA1 checksum:   1886cb4f39b974bcda981ecbde13e2d1310eb4ec

Image information:
 Acquisition started:   Fri May 17 21:18:10 2024
 Acquisition finished:  Fri May 17 21:20:48 2024
 Segment list:
  C:\Users\LENOVO\Desktop\FTK Test\IMAGING LAB.ad1
  C:\Users\LENOVO\Desktop\FTK Test\IMAGING LAB.ad2
  C:\Users\LENOVO\Desktop\FTK Test\IMAGING LAB.ad3
  C:\Users\LENOVO\Desktop\FTK Test\IMAGING LAB.ad4

                                              OK
```

Fig: 6 Image Summary

·Data cloning and forensic imaging are techniques used in the field of digital forensics to create exact copies or images of digital data for analysis and investigation purposes



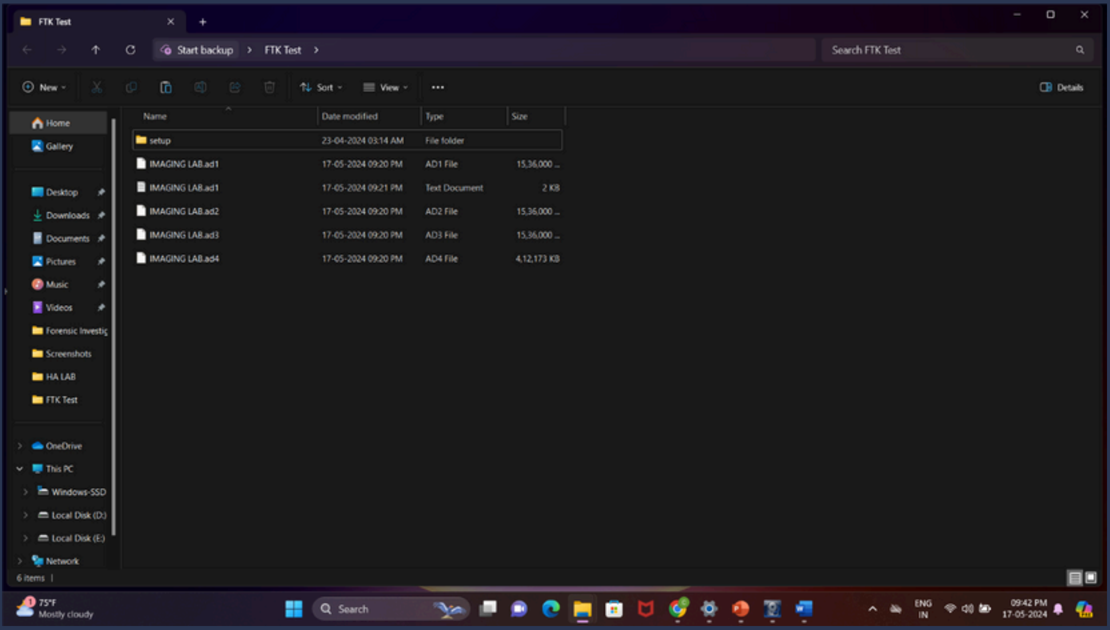
Drive/Image Verify Results

Name	IMAGING LAB.ad1
MD5 Hash	
Computed hash	a83708833aa387e33d589f23fed15ea3
Report Hash	a83708833aa387e33d589f23fed15ea3
Verify result	Match
SHA1 Hash	
Computed hash	1886cb4f39b974bcda981ecbde13e2d13
Report Hash	1886cb4f39b974bcda981ecbde13e2d13
Verify result	Match

Fig:7 Checking of file integrity

- Checking file integrity is a crucial step in digital forensics and data security to ensure that files have not been altered, corrupted, or tampered with. Several methods and techniques can be employed to verify file integritydigital forensic investigators can effectively verify the integrity of files and maintain the integrity of evidence throughout the investigation process.

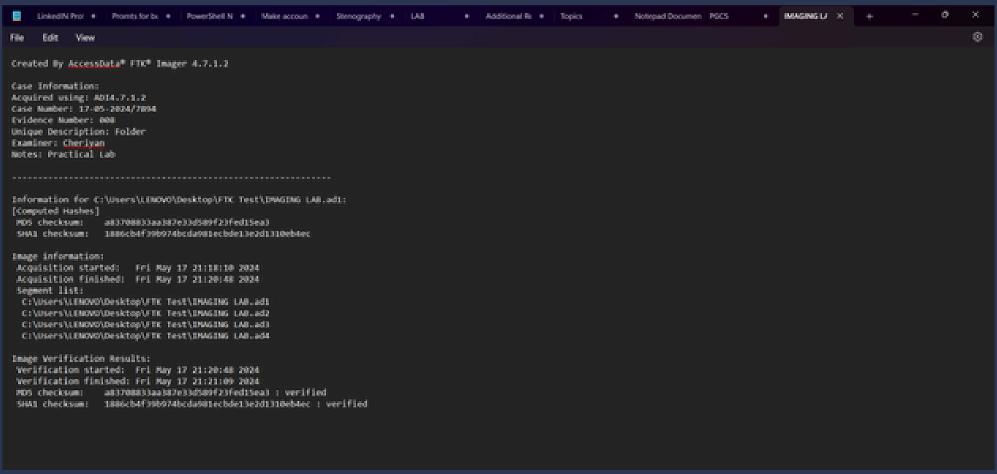
- FTK Imager uses MD5 Hash and SHA1 Hash algorithm to check for file integrity. As we can see after checking the hash of both the original folder and the imaged file the hashes are matching and hence the file integrity is maintained.



Name	Date modified	Type	Size
setup	23-04-2024 03:14 AM	File folder	
IMAGING LAB.ad1	17-05-2024 09:20 PM	AD1 File	15,36,000 ...
IMAGING LAB.ad1	17-05-2024 09:21 PM	Text Document	2 KB
IMAGING LAB.ad2	17-05-2024 09:20 PM	AD2 File	15,36,000 ...
IMAGING LAB.ad3	17-05-2024 09:20 PM	AD3 File	15,36,000 ...
IMAGING LAB.ad4	17-05-2024 09:20 PM	AD4 File	4,12,173 KB

fig:8 Imaged File

•As we can see that the original folder i.e. Hacker Academy is now been imaged and it is sub divided into 4 segments along with a text document that gives the details of the process.



```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 17-05-2024/7894
Evidence Number: 008
Unique Description: Folder
Examiner: Cheriyan
Notes: Practical Lab

--------------------------------------------------------------

Information for C:\Users\LENOVO\Desktop\FTK Test\IMAGING LAB.ad1:
[Computed Hashes]
 MD5 checksum:    a83708833aa387e33d589f23fed15ea3
 SHA1 checksum:   1886cb4f39b974bcda981ecbde13e2d1310eb4ec

Image information:
 Acquisition started:   Fri May 17 21:18:10 2024
 Acquisition finished:  Fri May 17 21:20:48 2024
 Segment list:
  C:\Users\LENOVO\Desktop\FTK Test\IMAGING LAB.ad1
  C:\Users\LENOVO\Desktop\FTK Test\IMAGING LAB.ad2
  C:\Users\LENOVO\Desktop\FTK Test\IMAGING LAB.ad3
  C:\Users\LENOVO\Desktop\FTK Test\IMAGING LAB.ad4

Image Verification Results:
 Verification started:  Fri May 17 21:20:48 2024
 Verification finished: Fri May 17 21:21:09 2024
 MD5 checksum:    a83708833aa387e33d589f23fed15ea3 : verified
 SHA1 checksum:   1886cb4f39b974bcda981ecbde13e2d1310eb4ec : verified
```

Fig: 9 Text file containing imaging information

Above is an example of what information could be included in a text file containing imaging information for forensic purposes

```
==========================================================
          FORENSIC IMAGING INFORMATION
==========================================================
Case ID:             [Case Identifier]
Date of Imaging:      [Date]
Imaging Technician:   [Technician Name]
Imaging Tool Used:    [Tool Name and Version]
Imaging Method:       [Methodology Used, e.g., Bit-By-Bit Imaging]
Hash Algorithm:       [Hash Algorithm Used, e.g., SHA-256]
-----------------------------------------------------
          DEVICE INFORMATION
-----------------------------------------------------
Device Type:          [Type of Device, e.g., Hard Drive, USB Drive]
Device Model:         [Model Number]
Serial Number:        [Serial Number]
Capacity:             [Storage Capacity]
File System:          [File System Type, e.g., NTFS, FAT32]
-----------------------------------------------------
        IMAGING DETAILS
-----------------------------------------------------
Imaging Target:       [Target Device/Partition/Volume]
Imaging Destination:  [Destination Drive/Location]
Imaging Start Time:   [Start Time]
Imaging End Time:     [End Time]
Imaging Duration:     [Duration of Imaging Process]

Hash Values:
Original Device:      [Hash Value of Original Device]
Image File:           [Hash Value of Image File]
-----------------------------------------------------
        ADDITIONAL NOTES
-----------------------------------------------------
```

This template provides a structured format for documenting key information related to the imaging process, including case details, device information, imaging details (such as start and end times), hash values for verification, and any additional notes or observations made during the imaging process. Using such a template ensures consistency and completeness in documenting forensic imaging procedures, which is essential for maintaining the integrity and admissibility of digital evidence in legal proceedings.

LESSON LEARNED

In conclusion, data cloning and forensic imaging are indispensable techniques in the field of digital forensics, essential for preserving, analyzing, and presenting digital evidence in legal proceedings. These processes involve creating exact copies or images of digital data while maintaining the integrity and authenticity of the original evidence. Through meticulous documentation, verification, and adherence to legal and ethical standards, forensic investigators can ensure the reliability and admissibility of cloned data and forensic images.

The key lessons learned from data cloning and forensic imaging underscore the importance of preserving original evidence, maintaining a clear chain of custody, verifying integrity through checksums and hash functions, and adhering to legal and ethical standards. By following best practices, continuously improving processes, and staying abreast of advancements in technology and methodology, forensic investigators can enhance the efficiency, accuracy, and reliability of data cloning and forensic imaging procedures.

Ultimately, data cloning and forensic imaging play a critical role in facilitating thorough and effective digital forensic investigations, enabling investigators to uncover evidence, analyze digital artifacts, and establish facts in support of legal proceedings. These techniques contribute to the pursuit of justice, the protection of individuals' rights, and the maintenance of trust and confidence in the integrity of digital evidence.