Xournals

Academic Journal of Forensic Science

ISSN: 2581-4273 | Volume 06 | Issue 01 | April-2023

Analysis of FTK Imager as a Recovery Tool for Different Storage Devices

Niranjan[1], Ankit Tripathi[2]

Available online at: www.xournals.com

Received 31st January 2023 | Revised 21st February 2023 | Accepted 10th March 2023

Abstract:

The Forensic Toolkit (FTK) Imager is an open-source software program developed by Access Data used to create exact copies, or forensic images, of digital data without altering the original. The image of the original evidence stays consistent, enabling us to copy data at a much faster rate, which can be quickly maintained and can be investigated further. FTK imager not only creates an exact copy or image of the data, but it also recovers erased data from the given exhibit. It is an open-source software application that recovers deleted data. This investigation was carried out by experimenting on certain samples, such as USB devices, Micro SD cards, CD/DVD, and hard disks, to determine whether the erased and destroyed data could be recovered.

Keywords: *Forensic Toolkit (FTK) Imager, Access Data, Data recovery.*

Authors:

1. *B.Sc, Forensic Science, Garden City University, INDIA*
2. *Senior Scientific Officer, Sherlock Institute of Forensic Science, INDIA*

Introduction

FTK Imager is a powerful and widely used digital forensic tool for acquiring and analyzing digital evidence from a variety of sources. The tool is user-friendly and intuitive, making it suitable for both novice and experienced users. FTK Imager is widely used by law enforcement, government agencies, and private organizations to investigate and prosecute criminal activity, as well as for internal investigations and audits.

Access Data, a leading provider of digital forensic software and services, created the tool. FTK Imager is part of the Forensic Toolkit (FTK) suite of tools, which also includes FTK Enterprise, FTK Forensic, and FTK Portable. FTK Imager is a stand-alone tool for acquiring and analyzing digital evidence from a variety of sources, including hard drives, memory cards, USB drives, and other storage media. One of FTK Imager's key features is its ability to create forensic images of digital devices **(Dodt, 2021)**.

These images are exact copies of the original data and can be used to analyze and investigate digital evidence without causing any changes to the original data. FTK Imager can generate forensic images in various formats such as RAW, E01, DD, and SMART. The program also works with a variety of file systems, including NTFS, FAT, HFS+, and EXT **(www.hackingarticles.in).**

FTK Imager also includes a variety of analysis tools for investigating digital evidence. Keyword searching, file filtering, and timeline analysis are among the tools available. The program also includes a hex viewer and a file viewer for viewing and analyzing individual files and data structures. FTK Imager's ability to analyze and recover deleted files is another key feature. The program employs sophisticated algorithms to locate and recover deleted files, even if they have been overwritten or partially destroyed. This feature is especially useful in cases where suspects have attempted to conceal or destroy evidence. FTK Imager is also designed to be highly customizable, with a plethora of options and settings that can be tailored to the specific requirements of each investigation. The tool also includes a scripting language for automating repetitive tasks and customizing its functionality. To summarise, FTK Imager is a powerful and versatile digital forensic tool widely used in law enforcement, government agencies, and private organizations to investigate and prosecute criminal activities, as well as conduct internal investigations and audits. Because of its user-friendly interface, advanced analysis tools, and customizable features, the tool is a must-have for anyone involved in digital forensics **(www.hacknos.com).**

One of the most important steps in the investigation of digital forensics is forensic imaging. It involves the process of creating an archive or copy of the complete hard disk. It is a data file containing all of the information required to boot into the operating system. However, for this imaged disc to work, it must be implemented to the hard disk drive. The disc image files cannot be used to recover a hard drive since they must be opened and loaded on the drive with an imaging application. A single hard disk may hold a large number of disc images. Disk images may additionally be stored on larger-capacity flash drives **(www.studocu.com)**.

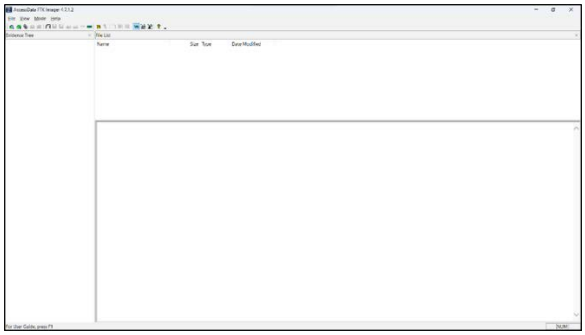


Figure No. 1: FTK Imager Interface

Objectives

The focus of the research conducted up to this point has been on the operation of the application. In this study, the potential is to recover deleted data from the digital evidence or storage device. After gathering image data from multiple instruments, the necessary observations and analyses are conducted.

The objective of the work is -

- To create an image file from the provided exhibits like USB devices, Micro SD cards, CD/DVD, and hard discs, decrypt and extract the image file to readable form and analyze them.

- To format or delete certain data from the provided exhibits and extract deleted and erased file present in the created image file and compare them.

Methodology

- This is a research-based study. We have considered devices such as USB drives, SD cards, CDs, and DVDs.

- The data-recovering feature of the open-source FTK imaging software was analyzed. Every storage device connected to FTK for imaging was checked for its recovery of the deleted files in it.
- Files were created in every device and deleted and then imaged in FTK to see whether the recovery takes place or not.
- Accordingly, every analysis was done and observations made are discussed in the paper.
- First, three folders were created and named 'Can this file be recovered 1, 2 and 3', respectively.
- Then the image has been created and the image dump was analyzed as shown below:-

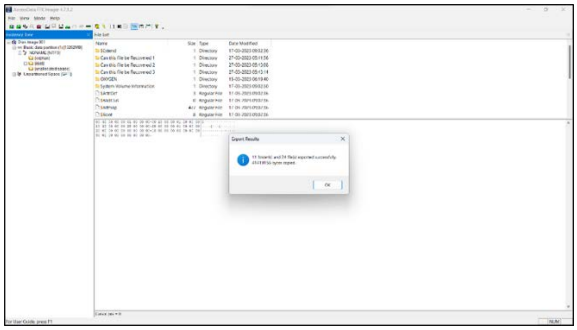


Figure No. 2: Created files

Steps To Create A Forensic Image Or Disk Image

Forensic imaging is considered to be amongst the most important steps in digital forensics **(www.geeksforgeeks.org).**

1. Open Access Data FTK imager → File → create disk image.
2. Select the source from the drive.
3. Select the Drive either Physical or Logical → NEXT.
4. Select the Drive from which the image copy is to be made → FINISH.
5. Click on Add → Enter the Destination path for the image that is to be created.
6. The created file should be duplicated to a different hard disk, and several backups of original evidence must be generated to prevent evidence loss.
7. Select the format → NEXT.
8. Now add the details accordingly → NEXT.
9. Click on Browse → add a destination for the image file → name the image file → FINISH
10. Once the destination path has been added → Start → check the 'Verify images after they are created' box only and uncheck the rest.
11. Wait until the image is created.
12. A hash result that checks the MD5 hash, SHA1 hash and the existence of any flawed sectors is generated once the image has been formed.

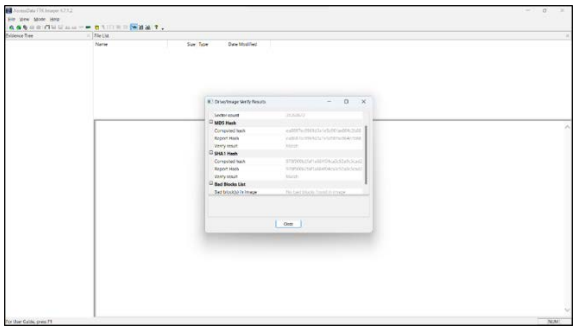


Figure No. 3: Hash Value of the created image

Steps To Decrypt Or Analyze An Image Dump

Once the RAW image has been created by using FTK Imager. Now decrypt the following data from non-readable to readable form by using the following steps **(www.geeksforgeeks.org).**

1. Open FTK imager → File → add Evidence Item.
2. Select on Image file → NEXT
3. Browse → choose the Path of the Image file that had been created → FINISH
4. Once the Image file is attached to the Evidence Tree or the Analysis Part, the contents of the file of the RAW Image will be seen, and also contains 'Deleted data from the source'.
5. Select the root → right click → Export Files → choose the destination to export the file.
6. The files will be exported to the given destination in the readable form where they can be used to analyze the Data.

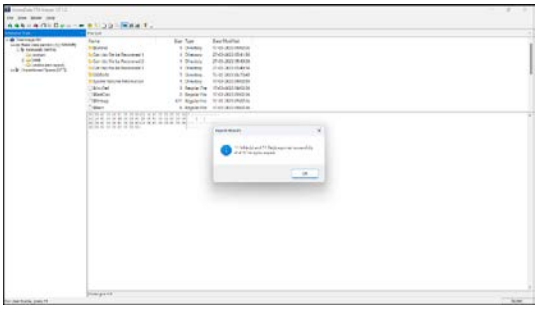


Figure No. 4: Decrypted image dump

Results and Discussion

- FTK can restore deleted data files from digital evidence in addition to making an exact copy or image of digital data.

- The files are deleted and the samples are formatted to check whether FTK can recover the deleted files.
- The samples taken are USB devices, SD Cards, CDs, and DVDs.
- FTK has recovered all the files that has be deliberately destroyed
- The deleted data are marked as X on the folders by the FTK imager based on the data formats indicates as deleted or destroyed digital evidence. sample example has been shown below:-

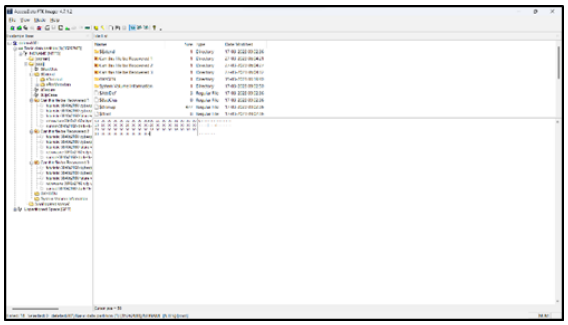


Figure No. 5: USB device

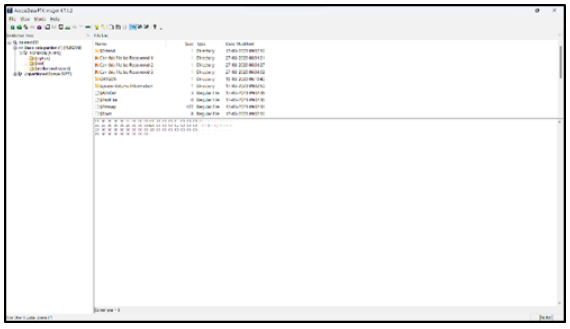


Figure No. 6: SD card

- The deleted files of the CDs/DVDs that are recovered from FTK are not marked as X as the data format of the CDs/DVDs differs from other devices.

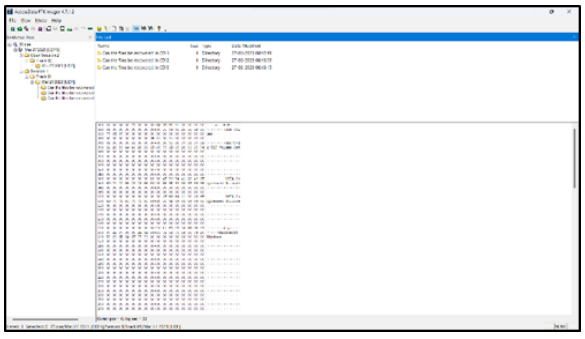


Figure No. 7: CD

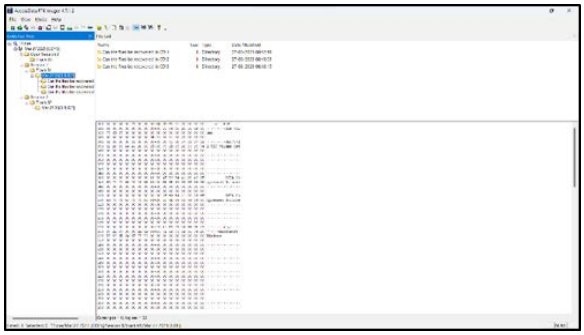


Figure No. 8: DVD

- The hash value of the deleted data recovered from the FTK Imager will differ from the original hash value. This is because when data is deleted from a hard drive, it is not removed from the drive but rather marked as free space. When the recovery deleted data using FTK Imager, we are essentially copying this data from the free space to another location. This means that the hash value of the recovered data will be different from the original hash value because it has been moved to a different location on the hard drive. On the other hand, if a forensic image of the hard drive is made before retrieving deleted data and then the hash values of the original image and the recovered data are compared, they should match if the original picture has not been altered.

- As the data was erased for conducting the research the hash value differs

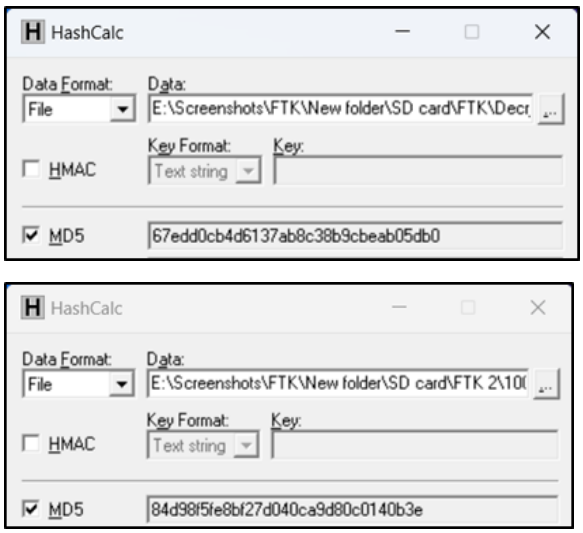
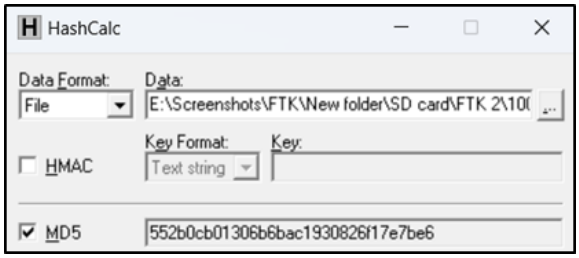


Figure No. 9 & 10: Hash value of the original and deleted data of USB drive



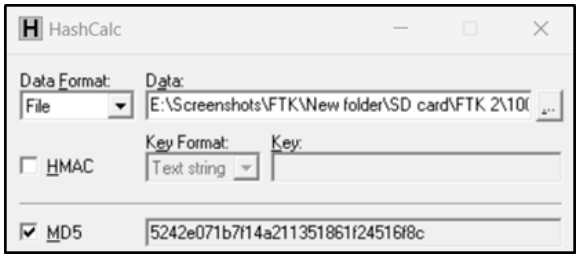
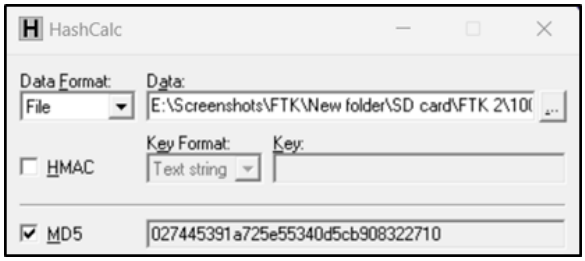


Figure No. 10 & 11: Hash value of the original and deleted data SD card



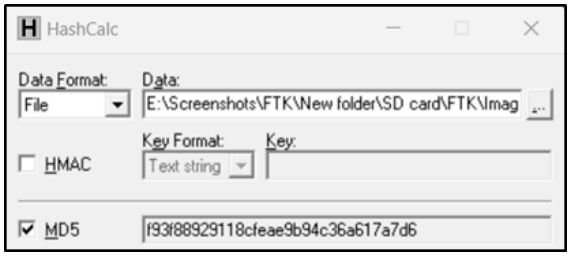
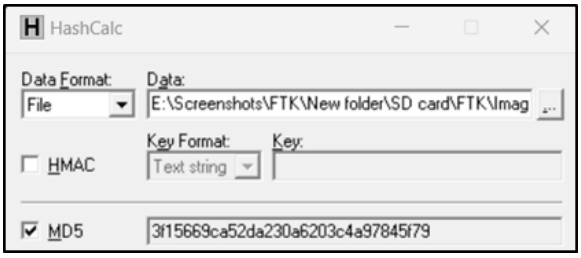


Figure No. 13 & 14: Hash value of the original and deleted data CD

- If the analysis process gets interrupted or discontinued due to any errors, it can be restarted from where the error has occurred.
- As FTK is open-source software so it can not only create an image of the digital evidence but, it can also recover the deleted data from it.
- The hash value is generated automatically but it differs from the original Hash value of the evidence only if the file has been deleted before analyzing on the FTK software.



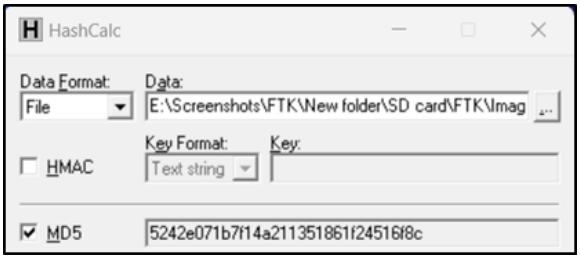


Figure No. 15 &16: Hash value of the original and deleted data DVD

Conclusion

FTK imager not only creates an exact copy or image of the data, but it also recovers destroyed data from the given exhibit. It is an open-source software application that recovers deleted or erased data. This investigation was carried out by experimenting on certain samples, such as USB devices, Micro SD cards, CD/DVD, and hard disks, to determine whether the erased and destroyed data could be recovered. After a thorough experiment on the given samples mentioned above, I conclude that the FTK imager recovers the deleted data from the storage devices and also analyses the data for free.

References:

"Forensics Practical - Practical 1 Creating Forensic Images FTK Imager Allows You to Write an Image." Studocu, https://www.studocu.com/in/document/university-of-mumbai/basics-of-digital-cyber-forensics-file-systems-networking-introduction-to-internet-cyber-crime-digital-evidence/forensics-practical/9270738.

GeeksforGeeks. "How to Create a Forensic Image with FTK Imager." GeeksforGeeks, Sept. 2022, www.geeksforgeeks.org/how-to-create-a-forensic-image-with-ftk-imager.

Dodt, Claudio. "Computer Forensics: FTK Forensic Toolkit Overview [Updated 2019] | Infosec Resources." Infosec Resources, 10 July 2021, resources.infosecinstitute.com/topic/computer-forensics-ftk-forensic-toolkit-overview.

Chandel, Raj. "Comprehensive Guide on FTK Imager." Hacking Articles, 6 Nov. 2020, https://www.hackingarticles.in/comprehensive-guide-on-ftk-imager/.

Gehlaut, Rahul. "Use of FTK Imager Forensic Tool." HackNos, Sept. 2021, www.hacknos.com/use-of-ftk-imager-forensic-tool.