Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 01, January -2018

Importance of Forensic Image of Hard Disk Using Different Forensic Tools By Preserving The Integrity of Digital Evidence

Ketan N. Mahajan[1] , *Suraj S. Chafale*[2], *Vitthal G. Mulik*[3],

V. S. Pawade[4], *Dr. K. V. Kulkarni*[5]

Directorate of Forensic Science Laboratory, Mumbai, Home Department, Maharashtra State.

Abstract:-*Forensic science is the application of science relates to the criminal investigation by a court of law. Cyber forensic is a branch of forensic science technology. The digital media are used to perform cybercrime as a target or source. The investigation of such type of crime is carried out by using thedigital storage media which used in this crime such as hard disk, pen drive, CD or DVD etc. In this paper, we use the different forensic tool to createa forensic image of the hard disk for further analysis in digital crime investigation, which result in same MD5 hash value. Here we also describe the importance of forensic image in the process of investigation of digital crimes.*

Keywords: *forensic image, imaging tools, MD5 hash value, cyber forensic.*

I. INTRODUCTION:

Nowadays, forensic science is a wide area so many researcher has more attention to this field. Cyber forensic is a branch of forensic science technology. The digital media are used to perform crime as a target or source. The criminal activity is carried out by using computer, mobile phones or internet. There are mainly three types of cyber forensic i.e. computer cyber forensics, mobile forensic and network forensic. In a computer forensic [2], criminal activity is performed using computer. In mobile forensic, mobile phones are used to perform criminal activity.Mobile Forensics is defined as the science of recovering digital evidence from a mobile phone under acceptable condition [1].The digital storage media used in computer forensic to performing cybercrime which are hard disk, tape drive, floppy disk, optical disc or USB flash drive,pendrive, memory cards, CD,DVD etc.

The mobile phones, smart phones, SIM card and memory card used as a source or target to perform criminal activity in mobile forensic. Network forensics is a branch of digital forensics, which relates to the monitoring and analysis of computer network traffic for the purpose of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information.Digital forensic investigation is process of determine and relates extracted the information and digital evidence to establish factual information for judicial review [10].

The cyber forensic steps which are used in digital forensic investigation, are described below in Figure1.1:

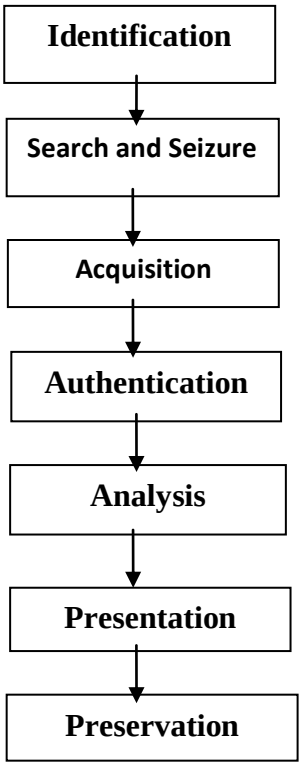

Figure 1. ***Digital forensic investigation steps***

A Disk image or aforensic image is a file containing the contents and structure of a disk volume or of an entire data storage device, such as a hard disk drive, tape drive, floppy disk, optical disc, Memory card or USB flash drive. Depending on the disk image format, a disk image may span one or more computer files [3].

The aim of forensic image acquisition is to maintain integrity of digital evidence and ensure legally admissible evidence in court of law.Disk images are used to transfer a data present in the hard drives for various reasons. A disk image can be used in for many reasons, including: restoration of a hard drive's contents during disaster recovery, for the transfer of hard drive data or content from one computer to another, if hardware has updated or repaired then after performing this task disk images is used to restore the contents of a hard drive. It can be used for creatinga replica of a hard drive or other device (CD, memory card, etc.) in the course of investigation for analysis purpose [3]. In the forensic analysis, there uses disk images rather than directly working on the source drives or the primary evidence.The reason of taking the disk images are avoid data loses, avoid in tempering in data or content present in the drives and keep the proper dates of file creation and data accessed dates that helps in proper investigation and finding the evidences present in the source drives. The hash is most important term in forensic science for identification disk Image or other digital media image for integrity and authenticity of digital evidence.

MD5 (Message Digest 5) hash value:MD5 is a hash algorithm is an enhanced version of its predecessor MD4. MD5 is widely used in several public key cryptographic algorithms and Internet communication in general [4].
Md5 is widely used technique of calculating the hash value of the file and its security is suspect [5]. It compresses a piece of information with plain code and random length into 128 bits value by hash algorithm, which is called information distract. MD5 algorithm is irreversible and cannot recover the original plain code information from information abstraction, thus it is always secure and safe [5].

II. RELATED WORK

In a tutorial [3], the author discussed about disk image acquisition of hard disk using FTK Imager. In this tutorial authors also discussed about the hashing, importance of hashing and details of creation of image.
In this paper [4], authors discussed about the MD5 algorithm resistivity and safety has been analyzed based on FPGA implementations. They have been investigated different parallel architecture for implementing the algorithm. There is also testing of different sets of strong and weak password for testing the performance of architecture. For indicating the performance of algorithm the time for cracking the cipher has been measured.
In this paper [5], the authors discussed the important role of MD5 algorithm in the application of password authentication. This paper also analyses the security features of the passport authentication and also discuss about the methods of application safety improvement of MD5 algorithm in password authentication, thispaper has analyzed the application of MD5 algorithm and security in the password authentication, and suggests the method of the process of exchanging or interfering MD5 pointed to collision attack and dictionary attack to improve the application of MD5 and security.

III.PROPESED *WORK*

Here we are create the forensic image of hard disk which has capacity of 40 GB by using different forensic tools such as tableau forensic duplicator, image master solo4, AccessData® FTK® Imager and Encase 7 for further forensic analysis. We use different types of forensic tool to make the forensic image. We take the hard disk as source which has capacity of 40 GB and destination hard disk has capacity of 80 GB. The working of these tools is explained below:

3.1. Tableau forensic duplicator:

Built on the strength and reputation of the original Forensic Duplicator, the newly released TD2 Forensic Duplicator delivers advanced functions and exceptional performance in a compact, durable and easy-to-use package [6]. This second-generation product was designed for imagingboth SATA and IDE/PATA hard drives at speed up to 9GB/min. Utilizing the same protocol modules as the original Forensic Duplicator, investigations can (optionally) include USB and SAS suspect drives. The Forensic Duplicator 2 is an intelligent alternative to higher-priced disk imaging solution. The Forensic Duplicator 2 support hash (SHA-1 & MD5) duplication of IDE or SATA HDD's. The Forensic Duplicator provides the flexibility of cloning (disk-to-disk) or imaging (disk-to-FAT32 file system) of hard drives. Source and destination drives may be in any combination of SATA or IDE. The Forensic Duplicator supports 1:1 drive duplication and will prompt users when spanning of multiple destinations drives [5].
Here we create the evidence file by using the disk to file (D2F) functionality of tableau Duplicator. This tool is also use towipe and format the digital storage media as well as to calculate the hash value of digital storage media. This tool is shown in following figure 2.when the forensic image is complete with the help of this tool,it gives same verification md5 hash value and acquisition md5 hash value.

Fig.2*Forensic imaging using TD 2*

Evidence file format is created by EnCase Forensic, an application used to collect, process, analyze, and report forensics information; contains sensitive digital forensics, cyber security and e-discovery information; that includes case information such as the examiner's name, date, time of acquisition and notes of the acquisition[8].

EX01 files are use in judicial environment to preserve and present digital evidence. The EX01 file is an exact copy of the contents extracted from a subject device's disk and can be mounted and read by EnCase Forensic or another tool that supports the EX01 format[8].

The EX01 format replace the .E01 format with the release of Encase 7. The new format provide advanced security features such as AES256 encryption with keypairs or passwords, LZ compression and the option for MD5 or SHA-1 hashing[8].

3.2. Image Masster solo4:

The Image MASSter™ Solo-4 is a high speed forensic hard drive duplicator that givesthe image of one suspect to two different evidence drives or the image of different suspect to the different evidence drives simultaneously [7]. The Image MASSter™ Solo4 forensic hard drive duplicator has features of built-in support for SAS, SATA and USB drive. It authenticates the hash value of SHA-1, SHA-2 and MD5. It also support IDE, RAID, e-SATA drives as well as a variety of Micro Media cards. With the help of this tool we can create exact copies, Linux DD images and E01 image files of suspect drive [7].

Here we use this tool to create the forensic image of same source hard disk which has the capacity of 40 GB. This tool is shown in following figure 3.

Fig.3 Forensic imaging using Image Masster SOLO 4

3.3. Image MASSter SOLO4 G3 SLIM:

TheImage MASSter SOLO4 G3 SLIM is advanced version of Image masster solo4. It gives same functionality as Image Masster solo4 but also have some additional features. This tool is shown in following figure 4.

Fig.4 Forensic imaging using Image MASSter SOLO4 G3 SLIM

3.4.AccessData® FTK® Imager:

AccessData® FTK® Imager is the software tool use to the make the acquisition of digital storage media (Hard disk, pen drive, memory card etc.). With the help of Tableau Write blocker (also known as Tableau fast blocker) weconnect the source hard disk which has the capacity 40 GB to the forensic workstation. Then add this source hard disk to this software to createforensic image of source hard disk at a particular location.The tableau write blocker is shown in figure 5. The Forensic imaging using AccessData® FTK® Imager is shown in Figure.6.The hardware write blocker device is use to attach source hard disk to forensic workstation, which prevent the possible modification before, current and after the acquisition process [11].

Figure 5.Tableau write blocker.

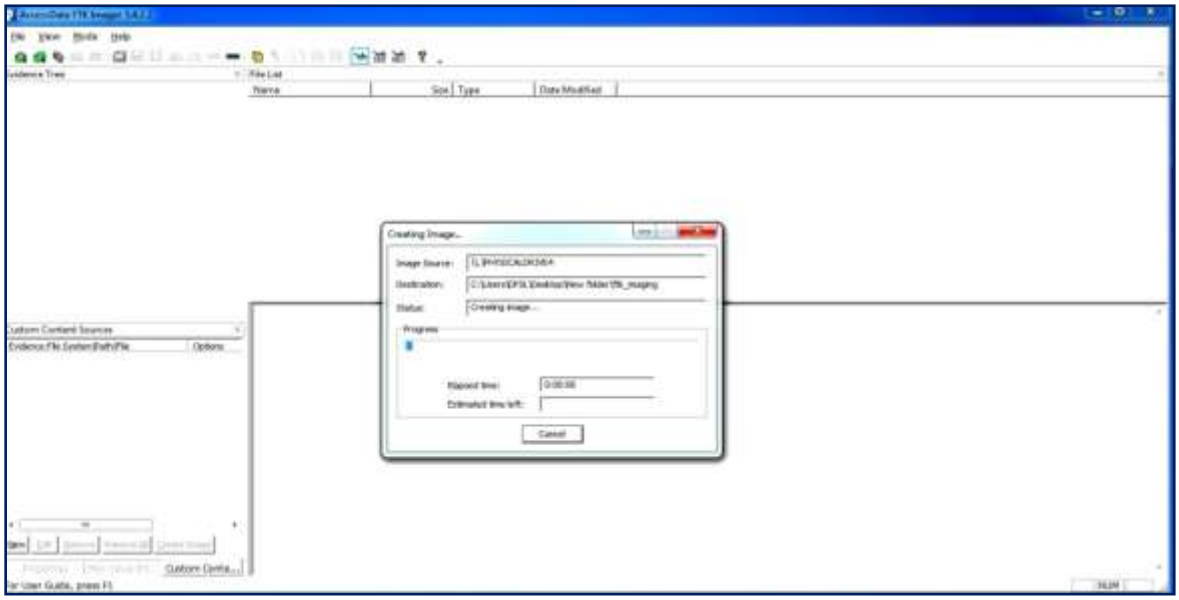

Figure 6. Forensic imaging using AccessData® FTK® Imager

3.5. Encase 7:

EnCase® Forensic v7 is the most flexible digital investigation solution available on a variety of different computer configuration [9].Here we use the software name as Encase 7 to create the forensic image of Source hard disk. We connect the hard disk to forensic workstationwith the help of tableau write blocker.Then we create the forensic image (.E01 or .EX01) of source hard disk using Encase 7. Thisacquisition processof Encase 7 is same as the the acquisition process of AccessData® FTK® Imager. This tool is shown in following Figure 7.

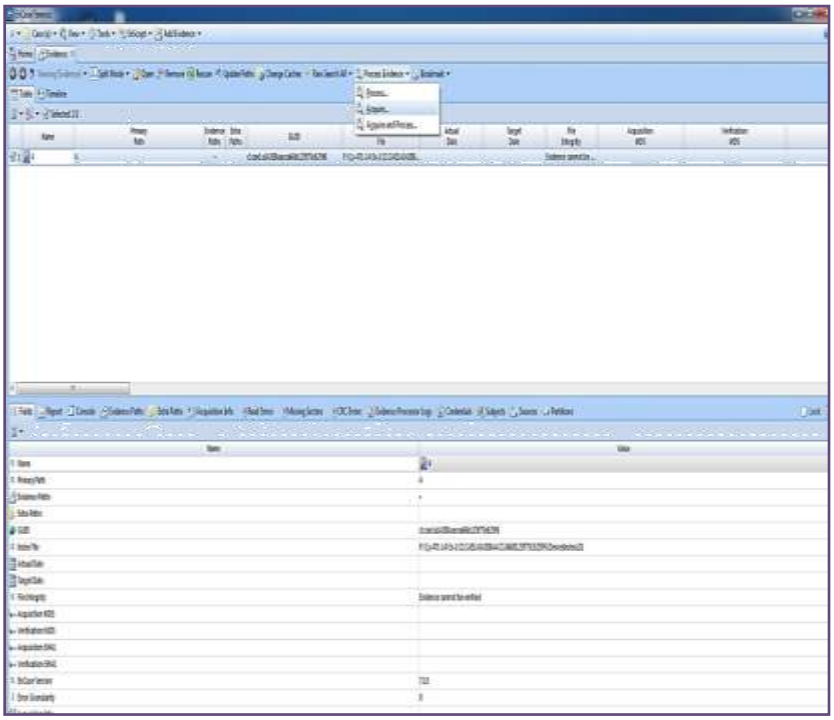

Figure 7.Forensic Imaging using Encase 7.

IV. RESULTAND DISSCUION

Here we use the different types of forensic tool to create the forensic image (also known as acquisition of digital storage media) of hard disk which has capacityof 40 GB. The results of acquisition of hard disk using different forensic tools are in given in table 1.1.

Sr.No.	Forensic Imaging Tools	Version	Results
1.	Tableau forensic duplicatorTD2	TD2	**Md5 Hash value :**6C7AD7355A6134D6E522588699CD901D
			Total sectorread :78,125,000
			Time taken to create image: 18 Minutes
2.	Image Masster solo4	4.12.62.0	**Md5 Hash value :**6C7AD7355A6134D6E522588699CD901D
			Total sectorread :78125000
			Time taken to create image : 0 hours 27 minutes 1 seconds.
3.	Image MASSter SOLO4 G3 SLIM	4.12.117.0	**Md5 Hash value :** 6C7AD7355A6134D6E522588699CD901D
			Total sector read : 78125000
			Time taken to create image : 20 minutes 42 seconds.
4.	AccessData® FTK® Imager	3.4.2.2	**Md5 Hash value**: 6C7AD7355A6134D6E522588699CD901D
			Total sector read : 78,125,000
			Time taken to create image : 19 minutes 57 seconds
5.	Encase 7	7.10	**Md5 Hash value:** 6C7AD7355A6134D6E522588699CD901D
			Total sector read : 78,125,000
			Time taken to create image: 24 minutes 35 seconds

Table 1. Result of hard disk acquisition using different forensic tools

Table 1.shows the total sector read by the above forensic toolsin the process of acquisition of source hard disk are same but it gives different acquisition time .The tableau forensic duplicator gives the less time for acquisition than other forensic tools. The Image masster solo4and Image MASSter SOLO4 G3 SLIMhas multitaskingability so we can perform the other task such as disk image, format or to wipe disk and to calculate hash value . The AccessData® FTK® Imager gives the less time for acquisition than others software forensic tools. The Encase 7 is software forensic tool which is used for the further analysis and helps to find the digital evidence in forensic investigation.

V. CONCLUSION

The hash value is most important term in digital forensic science for integrity and authentication of digital evidence.The above mentioned forensic tools are used to create the forensic image of hard disk which gives the sameMD5 hash valuewhich is used to maintain integrity and authenticity of digital evidence.

REFERENCES

[1]Forensic-as-a-Service for Mobile Devices (Literature Survey) Prashant N. Ninawe et al/(IJCSIT) International journal of computer science and information technologies, vol. 5(6) 2014, 7776-7778.

[2] http://www.isfs.org.hk

[3] http://nest.unm.edu/files/5513/9251/4756/Tutorial_1_-_FTK_Imager_-_Imaging.pdf.

[4] Analysis of MD5 Algorithm Safety against Hardware Implementation of Brute Force Attack, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013.

[5] XiaolingZhengJidongJin,Research for the Application and Safety of MD5 Algorithm in Password Authentication , 9th InternationalConference on Fuzzy Systems and Knowledge Discovery (FSKD 2012)

[6] https://www.digitalintelligence.com/products/forensic_duplicator_2/

[7]http://www.datadev.com/hard-drive-forensic-solo4-ruggedized.html

[8] https://fileinfo.com/extension/ex01.

[9] https://www.digitalintelligence.com/files/EnCase7_Specifications.pdf

[10] DHS. Test results for digital data acquisition tool:tableau td3 forensic imager version 1.3.0. 2014. URL: https://www.dhs.gov/sites/default/files/publications/508_Test%20Report_NIST_Tableau%20TD3%20Forensic%20Imager%201.3.0_August%202015_Final_0.pdf.

[11] ‘‘Deleting collected digital evidence by exploiting a widely adopted hardware write blocker’’, Christopher S. Meffert, Ibrahim Baggili, Frank Breitinger, DFRWS USA 2016 d Proceedings of the 16th Annual USA Digital Forensics Research Conference,1742-2876/© 2016 The Author(s). Published by Elsevier Ltd.

