DATA EXTRACTION AND ANALYSIS OF SSD & HDD

[1]Ravi Kant Chaurasia, [2]Dr.Priyanka Sharma
[1]Student, Raksha Shakti University, Ahmedabad,
[2]Professor, Department of IT & Telecommunication, Raksha Shakti University, Ahmedabad
[1]Cyber Security,
[1]Raksha Shakti University, Ahmedabad, India

Abstract: The early 21st century has seen a dramatic increase in new technologies available to consumers and industry alike and Solid State Drives is one of them which is not easily recoverable due to this it is a big challenge into the field of digital forensics specialists. The use of SSD is enough easy accessible and for many purposes it is used as a normal hard disk but many times faster and with the HDD's it needs very low power utilization. But, Solid state drive is not a change of hard disk technology; it is a technology that imitates the behavior of a hard disk. Solid state drive commonly called as SSD's come up with new technologies that are different from the traditional hard disk drives. In the paper we will learn about the storage devices SSD and HDD, however modern storage devices those having flash storage can operate under their own volition without any computer instructions. These operations are extremely destructive of traditionally, also they retrievable information might contaminate evidence, creates validation of digital evidence reports it makes the analysis process recovery tough and might also complicate the post recovery forensic analysis. In this paper we will see the key features that were analyzed in an SSD and HDD and discussed the key features that make SSD to delete its evidence and cause difficulties for forensic Investigations.

***Index Terms*: Computer Forensics, Digital Forensics, Flash memory, Solid State Drive, Hard disk drive, TRIM**

I.INTRODUCTION

In the past few years computer world has seen a dramatic increase in new technologies available to consumers. The consumers are now more knowledgeable about the technologies they are using in everyday life. The manufacturers improves the performance of traditional storage drives (HDD) which, includes speed to access the data, reliable performance, and the high power consumption are combined to inhibit the desired improvements.

These trouble arise from the mechanical components which are used by the HDD, which is having multiple plates rotating on a spindle casing and that can store data magnetically. Solid State Disks (SSD) which, based on flash memory, have been adopted as a solution of these problems. SSD are made up semiconductor chips they uses embedded controller, NAND flash memory and having no rotating parts, are compact in size and uses very less power as compared to HDD.

In this paper we will see the storage devices such as SSD and HDD commonly called as solid state drives and hard disk drives respectively, and problems facing by a forensic investigators in cracking evidence from a solid-state drive when compared to a hard disk drive also, the key factors which are causing risk for the forensic investigators for finding evidence.

II.EXISTING WORK

All laptop and computers runs on a specific storage device called as disk drives. These are of two types hard disk drive and solid state drive. they are responsible to store data on it. Primary work shows that these type of storage behaves in a different manner than existing hard drive technology where we are using a magnetic tape, and presents unique challenges with respect to data retention and forensic investigation [1]. The key component of a solid state disk is its flash memory. This flash-based form of storage exhibits different properties when compared to traditional magnetic storage mediums.

This study demonstrated that a solid state drive is fundamentally different from a magnetic storage drive, and it is possible for the drive controller in one of these devices to manipulate data on its own [1]. Furthermore, the presence of a write-blocker did not seem to prevent irrecoverable data loss from occurring [1].

The contamination of evidence, or self-corrosion of evidence by the solid state drive's controller. Unlike traditional solid state drives, there are many factors that influence the likelihood of data recoverability. The presence and support of the

TRIM command along with the drive usage and operating system configuration will often have a significant impact on forensics efforts. Interestingly, a fully-encrypted SSD is more likely to be able to have data recovered that a non-encrypted one, provided the investigator has access to the decryption key or decryption password for the drive. This is due to the fact that solid state drive controllers are not able to optimize data and TRIM is typically non-functional on a fully encrypted disk [2].

2.1 Partition alignment: refers to the physical sector size of a hard disk that is utilising by the operating systems. The most important difference in HDD and SSD will be the partition of sector which is contained by the hard drive. It is referred in papers that " HDDs uses 4096 byte physical sector size which is translated by firmware to 512 byte sector while the SSD utilizes 16 KB and 8 KB pages almost like that of sectors of HDD" [4]. The partition alignment turns essential at the time when we are copying content from a regular hard drive to SDD as a result of sometime clusters from HDD writes to multiple pages of SDD. The partition alignments are necessary for achieving maximum performance and durability of a hard drive [2] [3].

2.2 Self-corrosion:

The process within which recoverable components within hard drives erased files are removed over time that are essentials for performing arts forensic examinations known as as self-corrosion. In mordern's SSD's Deleted data making it complicated for the forensic examiner to recover it [5].

2.3 Wear levelling:

It refers to a memory management ways developed to increase the life of flash memory [5]. Wear levelling can help extend the useful life of NAND Flash devices and is often necessary to ensure that the devices reach the specified endurance rating by equalizing the wear of good blocks. The use of wear-levelling techniques is imperative in NAND Flash devices, regardless of the individual device's endurance rating [6].

The most effective wear-levelling method is static wear levelling because it typically provides more uniform block usage than dynamic wear levelling. Although dynamic wear levelling is typically inferior to static wear levelling, this method is easier to implement and can still provide enough wear levelling to meet the needs of many applications [6].

2.4 TRIM command:

It enables the OS to notify the SSD that old data is no longer valid about the time it deletes the logical block addresses from its logical table. The advantage of the TRIM command is that it enables the SSD's GC to skip the invalid data rather than moving it, thus saving time not rewriting the invalid data. This results in a reduction of the number of erase cycles on the flash memory and enables higher performance during writes. The SSD doesn't need to immediately delete or garbage collect • these locations it just marks them as no longer valid [3].

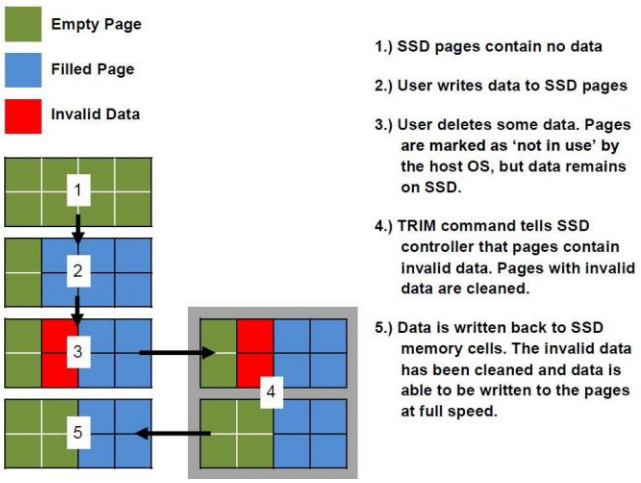

Figure 1: TRIM IMAGE

2.5 Garbage Collection:

In an SSD, the process of the changing or relocating the existing data to a new location and allowing the surrounding data that is invalid to be erased in an SSD is known as Garbage Collection.

The non-volatile memory which is using NAND control, SSD's uses the garbage collection for deleting and rewriting of data into blocks. It is found that Garbage collections will delete all the data instantly that is deleted by users and marked as invalid by the operating systems [3] [5]. The garbage collection isn't considered as the replacement for the TRIM functionality with SSD's, but TRIM would facilitate the garbage collection be additional efficient and improve performance. The garbage collection and the wear levelling are the main reason for the data to be written on the same blocks in SSD's.

III.RESEARCH METHODOLOGY

This study is a comparison of all the evidence which is obtained from a solid state drive and a hard disk drive. In this research we will compare the data statistically. In this study, we will initially send a file which may hold the key evidence required for solving a case, and some random data such as images, text files, documents. These file are copied to both the drive. Both the files are deleted and a random data is being copied on both the drives. Random data is being added along with the evidence by different combinations. The drives are formatted after each combination and refilled with new data.

A forensic tool named FTK imager is used for creating an image of the disk and FTK Toolkit for solving this case by finding the key evidence. The results obtained from HDD are set as a hypothesis for the study. The same process is followed in a solid-state drive. The results obtained in these two cases are compared statistically and it will help us to understand the challenges that are being faced by forensic investigators for cracking the evidence in solid state drives.

For this we needed FTK Toolkit, FTK Imager, SSD-Samsung 256GB, HDD- Seagate 1TB, Operating System Windows 10 Version and a forensics Work Station.

3.1 Data Collection

Data collected is a combination of pdf files, images, word documents, and notepad files. For getting the results used some keywords as the evidence files are created of five different files named as a car, dose, farm house, islands, and mortgage. Both the drive are wiped before process the data as its looks new. All the evidences are passed through HDD and SSD and was deleted. Seven different combination of evidence file, evidence folder, evidence trasher folders is created and passed on both the disks. After all the combination applied on both the disks. Format both the Disk after Data is Being Transferred into HDD and SSD respectively, for getting the evidence after deleting everything from the HDD and SSD.

Creating an Image of the Evidence by FTK Imager to analyze the contents of SSD & HDD.

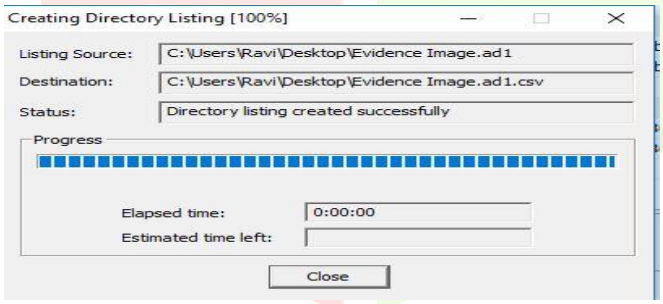

Figure 2: Processing of Image creation of Evidence

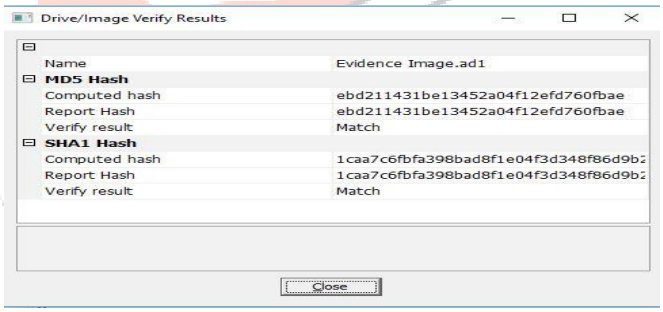

Figure 3: Hash Values are generated by System of Evidence

After this Analysis is performed of the Evidence Image by FTK forensic toolkit.

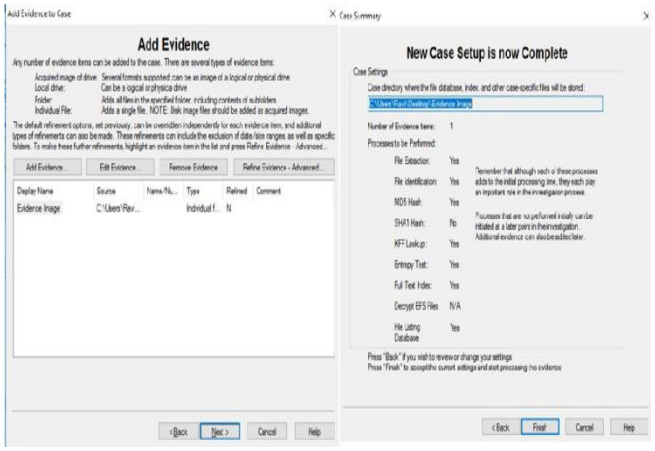

Figure 4: Add Evidence and Start Analyzing of the Image

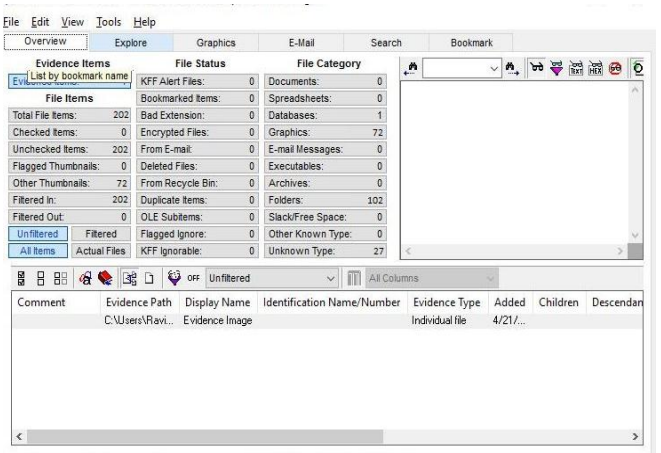

Figure 5: Evidence Analysis in FTK Toolkit

IV.RESULT

Firstly we created an image of SSD and HDD of the evidence on the work station and founded the results as total 10 Images of HDD size 1TB is created and 5 Images of SSD size 256 GB is created.

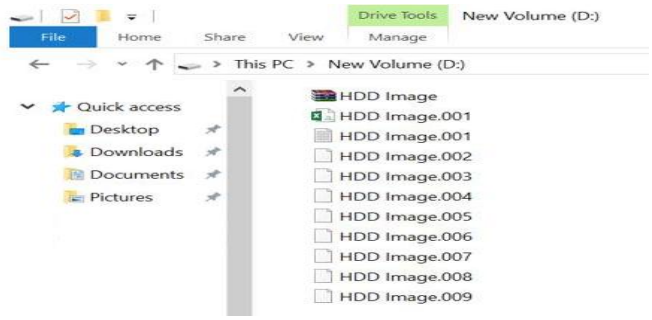

Figure 6: HDD Image

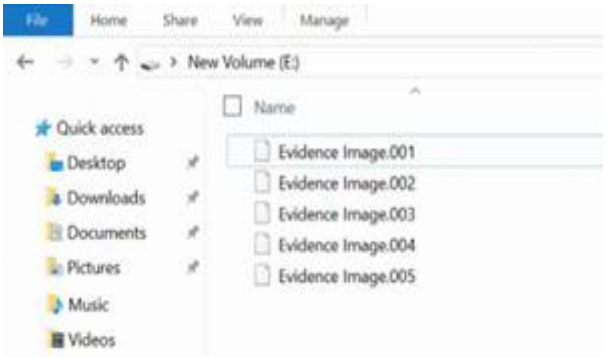

Figure 7: SSD Image

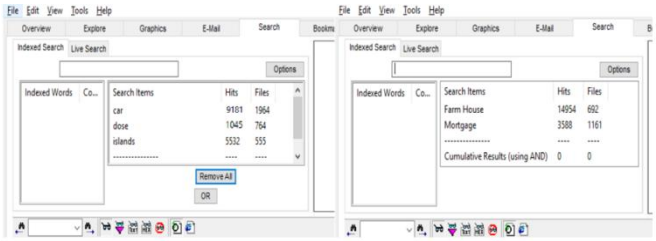

Figure 8: Result Obtained from the Image of Different Combinations Used

After analyzing the results of all the 10 images of HDD, an average of the hits and files identified in all 10 images, and analyzing the results of all the five images of SSD an average of the hits and files identified in all five images is taken and results are all follows is taken and is used for comparison with that of SSD and HDD.

Table 1: Result Obtained from Images of HDD and SSD

Keyword	Original Files	Files in HDD	Files in SSD	Original Hits	Hits in HDD	Hits in SSD
Car	1964	1199	770	9181	5770	1824
Dose	764	490	150	1045	690	215
Islands	555	440	34	5532	3209	623
Farm House	692	467	35	14954	8690	5633
Mortgage	1161	469	30	3588	1458	880

From the above table it was found that the key word Car had 1964 files initially with all the different combinations of evidence folder, evidence trasher folders made and the word car was recognized for 9181 times in all the documents such as images, contents of word documents, excel sheets and note pads that were passed. However, we could find 1199 files out of 1964 files in HDD using FTK Toolkit. So, there were some key evidence files that were missing but it is a pretty good sign that even after formatting the disk after every combination made the FTK toolkit could identify 60% of the files that were deleted. But, this was not the case with SSD, we could only identify 770 files out of 1964 original files in SSD which is less than 40 percent of the original files. It's very difficult for the forensic investigator in this scenario for finding the suspect in a case when we were not able to identify even 50% of the key evidence.

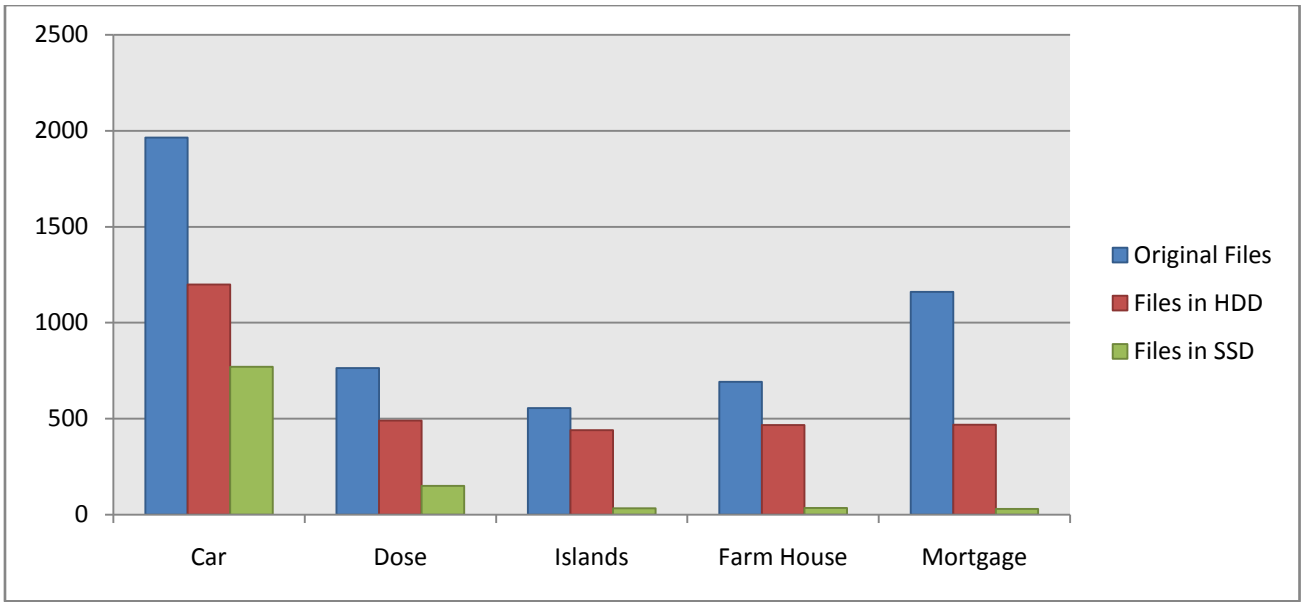

Figure 9: Difference in Results Identified by Number of Files

The graphical representation shown above is the comparison of the number of files that were being identified in the original image with that of identified in HDD and SSD. Considering the key word such as car, Island, it shows the number of files identified in an HDD is about 70-80% of the original files but when compared to that of an SSD we could see there were not even 10% of the files that were in the original folder.

Like the files comparison, the word Car was identified for 9181 times in all different folders, files, word documents, excel sheets, note pad etc. in the original image. We could identify 5770 times in that of an HDD which lands up at 65& of the key word being identified and it is a good sign for the investigator. However, 1824 times the key word was identified in SSD which is less than 20% of the original key word identified. This possesses risk for the investigators in identify the key evidence and proving who the suspect is due to the key features of the SSD.

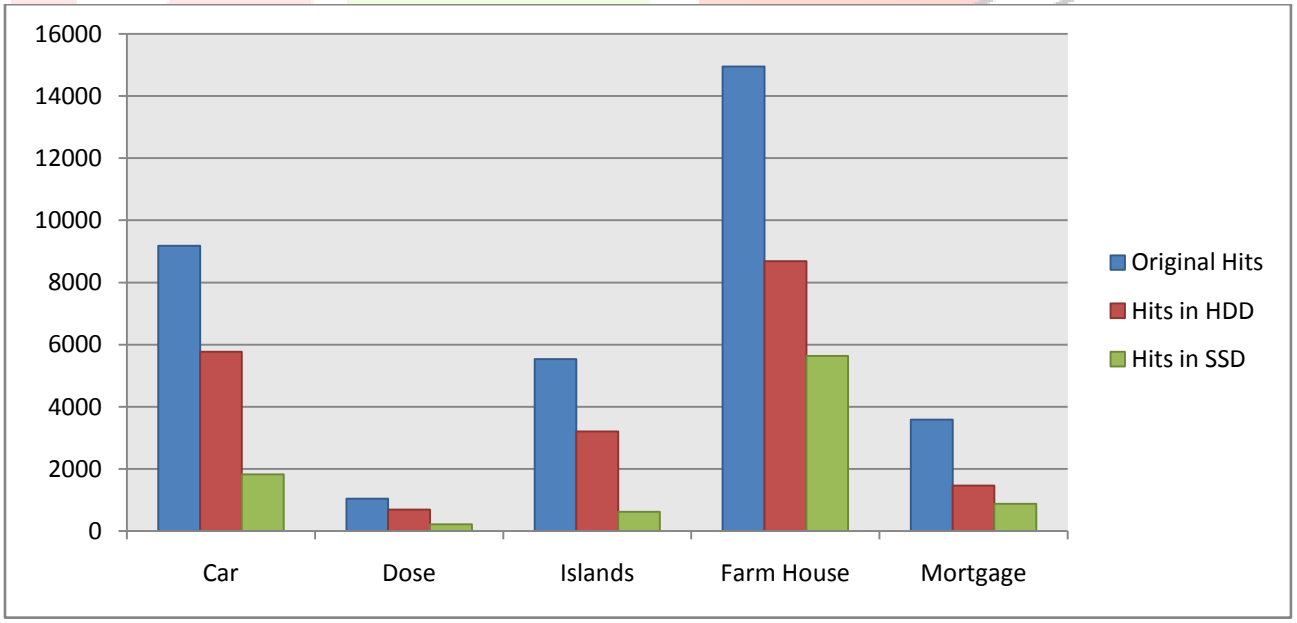

Figure 10: Difference in Results Identified by Number of Hits

The graphical representation shown above is the comparison of the number of hits that were being identified in the original image with that of identified in HDD and SSD. Considering the key word such as Dose, Islands, it shows the number of hits identified in an HDD is about 60% of the original files but when compared to that of an SSD we could see there were not even 10% of the hits that were in the original folder.

The special features in SSD such as wear leveling, garbage collection, self-corrosion, TRIM command help SSD in destructing the key evidence on its own without any instructions from the computer.

V. CONCLUSION

Both the drives HDD and SSD are passed with the same evidence files, formatted at same intervals, and passed with random data and different combination of evidence destruction files are being transferred. Images of the drives are being created using FTK Imager and are carefully being analyzed on the workstation using FTK Toolkit. However, it is clearly noticeable that even after performing the same set of operations on both the drives the results obtained do not match.

Based on results obtained it is proved that SSD's possess evidence destruction phenomenon that creates trouble for the forensic investigators for finding key evidence and resolving cases that were solved by using traditional methods on HDD.

V. FUTURE SCOPE

By performing above experiment we came to know that formal traditional methods used on Hard Disk Drives by forensic investigators for solving the key cases do not hold good in case the of solid state drives. Forensic investigators need to come up with new methods to overcome the destruction capacity of the solid state drives. As researchers stated that solid-state drives are beginning the end of current practice in digital forensic recovery [1], it is the time for forensic investigators to review the current techniques used and emerge with new tools for cracking even the self-destructed files in Solid state drives. If new techniques are not being introduced, it would result in the rise of crimes which do not have evidence to be proven and give chance for crime committers to consider these loop holes and increase the crime rate.

VI. REFERENCES

[1] Bell, Graeme B, and Richard Boddington. "Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?" Perth: Association of Digital Forensics, Security and Law, 2010. 5(3). Journal of Digital Forensics, Security and Law.

[2] Gubanov, Yuri, and Oleg Afonin "Why SSD Drive Destroy Court Evidence and What can Be Done About it." Belkasoft: Evidence Search and Analysis Software for Digital Forensic Investigations. Belkasoft, 1 Oct. 2012.

[3] Wei, Michael, Laura Grupp, Steven Swanson. "Reliably Erasing Data from Flash-Based Solid State Drives." University of California, San Diego.

[4] "Partition Alignment of Intel SSDs for Achieving Maximum Performance and Endurance." Intel, Intel, 1Feb. 2014.

[5] Martin, Nick, and Jeff Zimmerman. "Analysis of the forensic challenges posed by flash devices." University of Nebraska, 15 Nov. 2012

[6]https://www.micron.com/~/media/documents/products/technical-note/nand-flash/tn2942_nand_wear_leveling.pdf