International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Solid State Drive (SSD) Forensics Analysis : A New Challenge

Ravi Kant Chaurasia[*1], **Dr. Priyanka Sharma**[2]
[*1]M.Tech Cyber Security, Raksha Shakti University, Ahmedabad, Gujarat, India
[2]Professor & Head (IT & Telecommunication), Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT

There is a need of digital forensics approach to solve the cases of crime investigation based on the computer and mobile phones, which involves advanced to sophisticated digital misuse of systems. Digital forensics is always a advanced field as a career in forensics with the rise of laws that can take control on legal cases and computer technology that is becoming ubiquitous. This paper tells the studies of important techniques used over traditional Hard Drive Disk and upgraded technique needed over Solid State Drives to perform digital forensics investigation.
Solid States Drives introduces a new 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 and 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. Obtaining effective information from Solid State Drives (SSD) is a challenging forensic assignment. SSD's may be deleting the evidences usually and even after sanitization of SSDs, information may be recovered.

Keywords: Computer Forensics, Digital Forensics, Flash memory, Solid State Drive

I. INTRODUCTION

Solid State Drives SSD are dependent on non-volatile memory flash memory have overtaken the conventional spindle platter hard disks to become a major storage device used in computers and laptops present in the market. Nowadays tablet smartphone and notebook devices wouldn't stay without the flash memory for the hard disk drives.Solid state drives don't have any movable parts such as magnetic disks are movable read and write heads which used to be existing in conventional hard drives like HDD's or floppy drives.

In the conventional magnetic hard disk covered in a magnetic material contains data in the patterns of 0' and 1' so having the inability to write in the same texts at every location anytime. [1] [2] When data is been deleted it would marked as erased but will be available on an unused sector where these deleted files will be recoverable at any time. The TRIM performs a deletion of invalid data from the memory of SSD's pages to assure that the rewrite operation can be well performed regularly. That feature is commonly called as garbage collection self-corrosion in SDD's which also permanently eliminates the deleted data in the background from that sector within few minutes or immediately of the data being removed. Based on the data gathered it declares that decompose the of proof issue in non-volatile memory and refined use TRIM command causes the hardening of a forensics investigation. The efficiency of TRIM mechanisms could have a main distinction once enable for file system whereas collecting the deleted data that sometimes gets stores even when deletion. "The technology of the SSD devices leads to vital impacts on the capability of forensic investigators and analysts to search out and perceive the information hold on SSD devices" [1].This may additionally justify to an explicit extend however coming flash memory used in SSD are difficult for forensic analyses.

II. COMPONENTS OF SSD'S

1. Flash memory:

The flash memory that deletes data at block level are referred to as non-volatile storage. Data stored in a flash memory should be erased initially and most largely to be rewritten again into those memories that exist usually in modern SSD.

2. Partition alignment:

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 whichiscontained 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" [5]. 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 [3] [4].

3. Embedded controller:

It exists among SSD to performs the read and write operation all over the microchip, so that it also manages the wear leveling of a hard drive.

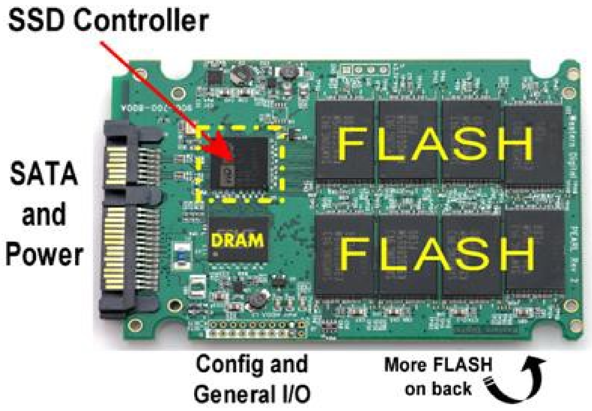


Figure 1. SSD Controller [8]

4. Wear leveling:

It refers to a memory management ways developed to increase the life of flash memory [7]. The supplier frequently provides additional storage when designing hard drives that are inaccessible by traditional ways could improve the wear leveling a lot better. Usually in SSD's, data are keep in blocks which may be wipe away and rewritten number of times. The wear leveling would handle and ensure that the deletion and rewritten cycles (based upon TRIM command uses) area unit in an evenly distributed order to perform efficiently and also extend the lifespan of a hard drive. There'stwo kind of wear leveling techniques: Dynamic and Static. Also, manufacturer would have data and techniques on how to access and utilize those additional storages by exchanging with live storage which might improve the wear leveling.

5. TRIM Function:

It is a procedure by which the flash memory controller deletes the information present on the block sector which has been erased by the users and is marked as deleted. It is referred in SSD's implement deterministic Zeroes after TRIM (DZAT) or deterministic read after TRIM (DRAT) returning all zeroes directly when TRIM query is fired on a certain block of data. SoSSD's will return original data which is based on the garbage collection formula applied in the different operating systems. There are specific concerns for encrypted volumes on SSD's, as various crypto containers implement vastly totally different methods of handling SSD TRIM commands." [7]

6. 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 [7].

7. 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 collectionswill delete all the data instantly that is deleted by users and marked as invalid by the operating systems [7] [4]. 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 [8]. The garbage collection and the wear leveling are the main reason for the data to be written on the same blocks in SSD's.

8. Encryption:

Encryption of drives could be a may be a of applying secret key or password to acquire data security to improve computer hard disks security from intrusion. It safeguards the disk drive by the implementation of protection to every sector that also challenges the forensic investigation. SSD's performs marking the data which is erased data as invalid but not necessary erase from the page in the flash storage. So, if data is not well encrypted at all time during the complete process of managing and deleting of data then it may be recovered in the conventional hard drives [1] [9] [8]. Skilled peoplesuses encryption methods and third party tools like TrueCrypt, PGP, BitLocker and another normal tool to achieve the highest level of data security in SSD's. These are new factors which would bring more complications and challengesduring forensics examination of data analysis of SSD's.

Thus, data collected will show however non-volatile storage, controller, TRIM flash memory, self-corrosion, wear leveling garbage collection, encryption and other new features by which,SSD operates creates a tough challenges for forensic examiner throughout an investigation.

III. RELATED WORK

Solid state hard drives concerning with the forensics investigation for recovering the deleted files in the past. The steps taking place during the collection of evidence require acquisition, authentication, and analysis of hard drives also needs an update with the rising use of hybrid drive such as SSD's in the new coming laptops and computers. There have been numerous investigations involving digital examinations of hard disks for evidence of crime to prove in the court to punish the culprit. Most of researches have shown toward getting the most advancement of the forensics analysis of the regular hard drives. Research studies have led the forensic investigation to require carving techniques or mechanisms to acquire essential content of the SSD drives which could help simplify task during forensics examinations [7]. While research studies have shown that TRIM would require the supporting operating systems, specific disk format and cable connections, storage controller configuration to be configured in IDE or ACHI mode and also supporting firmware to perform it tasks [10] [12].

It is find by the research that SSD supports data retention with TRIM enabled file systems to ease any digital investigation of hard drives. How enable TRIM causes the operating systems to delete file every time, which the sector remains empty at all time to re-write contains in those sectors. Modern SDD are capable of self-corrosion which makes difficult for a providing strong evidence to the court through forensic investigation. The current SSD have a garbage collection which would hold the data that are marked as deleted, but can be permanently deleted by overwriting mechanism to have that sector as new at the time [4] [6]. These would make the forensic investigator tough for recovering evidence from an SDD causing the evidence to be tampered during a court case [1].

Overall, the research approves how flash technology in SSDs differs from the traditional HDDs and makes it complicated for recovering evidence during a forensic investigation [9]. Researches accepts how immoral people with advance expertise level can completely wipe off the HDD so that the deleted content couldn't be recover under any circumstances later [3] [4]. It is identified that manufacturers of SSD's eliminate away their implementation methods of the hard drives making it difficult for forensics examiners to extract recoverable data from it [4] [6].

IV. ANALYSIS

This review paper will provide detail analysis and study of results as listed below:

i. Primarily, explanation the use and live response of enabling/disabling of TRIM functionality, garbage collection, self-corrosion.

ii. To identify a kind of hard drive that is newly hybrid, traditional HDD or SSD to improve the performance of analysis.

iii. Recommendations to overcome the challenges with TRIM on modern SSD's forensics.

iv. Difference between traditional HDD overSSD'sabout forensics investigation.

v. To provide challenges for SSD forensics which is needed in the investigation w.r.t its multiple storage, firmware, embedded controller and other factors.

V. SOLID STATE DRIVE Vs. TRADITIONAL HARD DISK DRIVE

The traditional disk drive would work on a magnetic disk platter where the platters are coated each side thus as to store data in a magnetic form. So, all data are stored on both upper and lower surface of the platters as tracks that is further divided into individual sectors. When an operating machine is power on the disk comes in use, and the OS needs to be able to scan the correct sector by spinning as fast as it can.

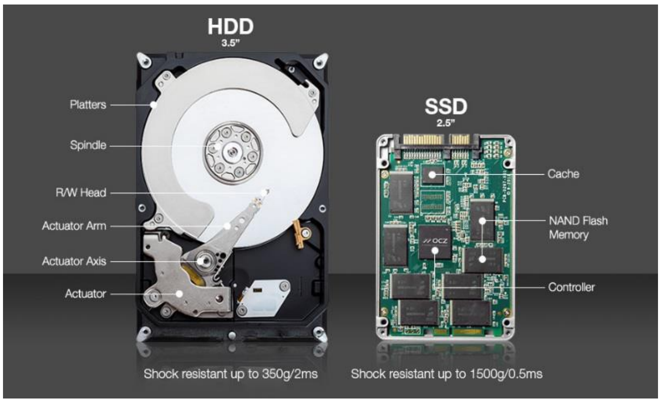


Figure 2. Magnetic Disk Vs. Flash Memory [10]

In the case ofsolid state drive, it works on flash storage which would not have any moving parts or spindle platter like in traditional hard drives. The problems which were arise from the movements of plates while reading in the disk of HDD is solved by SSD's. The key elements of an SSD are significantly the controller and the memory to store the data.

Figure 3 shows a detail view of SSD device architecture and the way modern SDD would have its feature like flash memory, wear leveling, controller, garbage collector referred to as block manager are separate and not compact under identical magnetic disk like in traditional HDD.

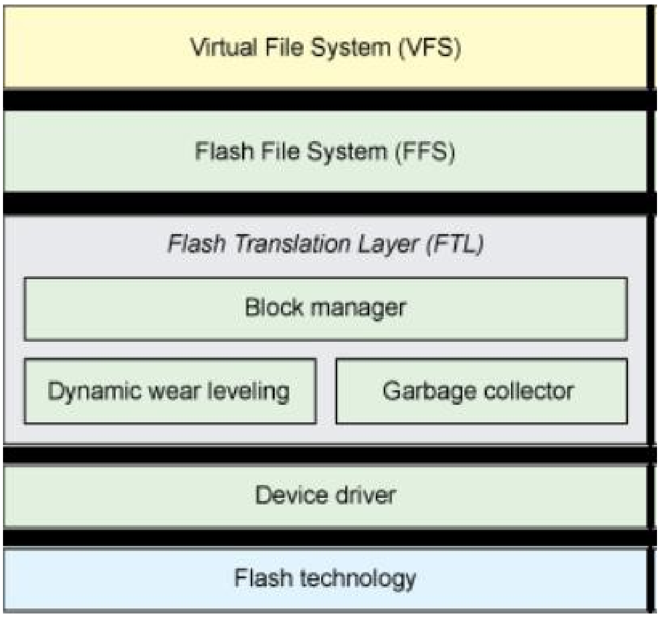
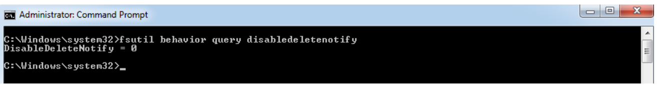


Figure 3. SSD Device Architecture [10]

VI. FORENSICS FOR TRADITIONAL HARD DRIVES

The main goal of a forensics investigation is toapply extensive methods that could recover the deleted files to prosecute criminals in the court. As the amount of data that needs to be analysed, examined and processed could be massive amount, and the variety of data types could be huge, forensic investigation team always need to stay ahead of the game which is played by the criminals. The forensic examination of hard drives by examiner has followed strictly based on performing the authentication, acquisition and analysis followed by a chain of custody with complete documentation in place, that is considered as a standard [7] [4]. The easy way of obtaining evidence from a suspected HDD would involve imaging of that hard drive followed by detailed analysis with standard evidence discovery tool such as EnCase, Belkasoft.

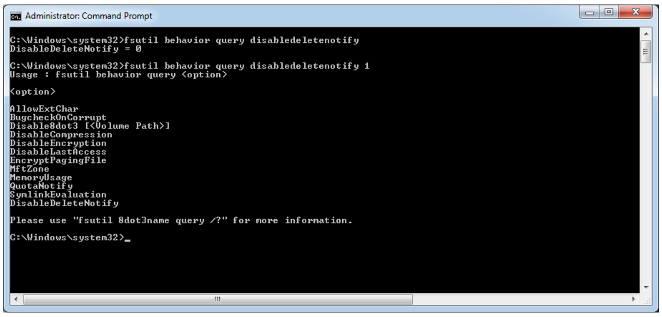
Figure 4, 5 shows how to enable and disable TRIM in Windows 7 machine



```
C:\Windows\system32>fsutil behavior query disabledeletenotify
DisableDeleteNotify = 0

C:\Windows\system32>_
```

Figure 4. Enabling/Disabling TRIM in windows 7 machine



```
C:\Windows\system32>fsutil behavior query disabledeletenotify
DisableDeleteNotify = 0

C:\Windows\system32>fsutil behavior query disabledeletenotify 1
Usage : fsutil behavior query <option>

<option>

AllowExtChar
BugcheckOnCorrupt
Disable8dot3 [<Volume Path>]
DisableCompression
DisableEncryption
DisableLastAccess
EncryptPagingFile
MftZone
MemoryUsage
QuotaNotify
SymlinkEvaluation
DisableDeleteNotify

Please use "fsutil 8dot3name query /?" for more information.

C:\Windows\system32>_
```

Figure 5. Enabling/Disabling TRIM in windows 7 machine

VII. CHALLENGES OF SSD FORENSICS AND POSSIBLE SOLUTIONS

The execution of NAND non-volatile memory with pages to store and reuse blocks in SSD's would make it tough to apply forensics techniques and methodologies compared to a traditional hard drive. More, it gets complicated encryption methods and sophisticated third party tools are making it tougher to obtain complete memory analysis from a regular hard drive now a days.

Although, the IDE allows the forensic examiner to perform logical data read which is present on the of SSD for acquiring of data but also can hide internal data structures, which could make the investigation difficult. As, some generators of SSD's makes the SSD in a form that it is almost impossible to retrieve the data reads to protect their implementation details it makes tougher for forensics examiners [11]. With the rapid use of SSD with newer operating systems such as Windows and linux, which are supporting enable, TRIM by default allows the deleted data to be fully wiped making it a dead end to examiners.

The manufacturer additionally would need to implement a way to disable self-corrosion by default therefore suspected criminals should be prosecuted for evidence being store and retrieved by the police. Also, the over provisioning provided by the manufacturer should be in a very efficient manner so forensic examiners able to retrieve the implementation and storage access when needed throughout a criminal investigation.

VIII. CONCLUSION

The improvement of the hard drive from old-fashioned to most recent SSD have increased drastically that the method is applied to preserve, identify and to extract the recoverable deleted data from modern hard drivesare almost impossible or none to today's date. As we have seen that TRIM functionality usage over disk formats isto identify the challenges toward forensic investigation of modern SSD's.

From the analysis it is shown how to use enabling/disabling TRIM command for reduce and improve the read and write achievements in SSD's with the use of different operating Systems.

It is also seen that new SSD's which are coming in the market would be all right without TRIM functions enable as long as the controller performs a fully delete and rewrite operations to the pages working as similar to garbage collections.

IX. REFERENCES

[1]. Fulton, John William "Solid State Disk Forensics: Is there a Path Forward?" Utica College, May 2014.

[2]. "SSD vs HDD: Difference. Advantages. What to Choose for Hosting a Website?" Web Hosting Reviews Discount Coupons RSS.

[3]. 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.

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

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

[6]. "Recovering Evidence from SSD Drive in 2014: Understanding TRIM, Garbage Collection and Exclusions." Forensic Focus Articles. Belkasoft, 23 Sept. 2014.

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

[8]. Rent, Thomas M. "SSD Controller." SSD Controller. Storage Review.

[9]. Nisbet, Alastair, Scott Lawrence, and Matthew Ruff "A Forensic Analysis And Comparison of Solid State Drive Data Retention With Trim Enabled File Systems" Site. Edith Cowan University.

[10]. "SSD vs HDD – Why Solid State Drive." SSD vs HDD. A Toshiba Group Company.

[11]. "Anatomy of Linux Flash File Systems." Anatomy of Linux Flash File Systems. IBM DeveloperWorks.

[12]. "SSD vs HDD: Difference. Advantages. What to Choose for Hosting a Website?" Web Hosting Reviews Discount Coupons RSS.

[13]. Mao, Chau-yuan "SDD TRIM Operations: Evaluation and Analysis" Site. Natinal Chiao Tung University, July 2013.