A Survey On Solid-State Drive Forensic Analysis Techniques

Avinash Kumar *avinash@shsu.edu*
Department of Computer Science
Sam Houston State University
Huntsville, TX, USA

Ashar Neyaz *ashar.neyaz@shsu.edu*
Department of Computer Science
Sam Houston State University
Huntsville, TX, USA

Narasimha Shashidhar *karpoor@shsu.edu*
Department of Computer Science
Sam Houston State University
Huntsville, TX, USA

Abstract

Solid-state drives (SSD) are predominantly being used as storage devices these days, which uses flash memory to store data. Most digital devices like desktop computers, laptops, tablets, smart phones use SSDs. Unlike traditional hard drives, it is comparably harder to recover deleted data from SSDs, which consequently impacts digital investigations detrimentally. Digital forensic researchers have come up with several strategies to acquire evidence from solid-state drives while maintaining the integrity of the device. In this paper, we present the latest forensic techniques and ideas presented in the literature in the field of solid-state drive forensics.

Keywords: Solid-state Drives (SSD), Digital Forensics, Flash Memory, SRAM, DRAM.

1. INTRODUCTION

Solid-state drives (SSD) use the flash memory to store the data. They are found in desktop computers, laptops, smart phones, flash drives etc. It is easy to recover the deleted data from traditional hard drives because they keep the deleted data in an unused sector. However, the solid-state drives completely erase the files, thus making it almost impossible to recover the deleted files. The TRIM functionality in SSDs deletes the invalid data from the memory to make sure that the new data can be re-written easily and smoothly. There is a feature called self-corrosion and garbage collection in SSDs that can permanently erase the deleted data within no time.

TRIM functionality and the garbage collection work side by side. TRIM marks the deleted files for garbage collection. Garbage collection can occur whenever drive is supplied with power which makes it difficult for digital investigators to perform data acquisition due to various reasons. First, deleted files may be impossible to recover because the process of garbage collection has completely removed the deleted file from the memory. Second, hash values can be different for multiple copies of the SSD image, because garbage collection may have modified the data.

There is a feature called wear leveling in SSDs which can be a challenge for digital investigators. The process of wear leveling can internally move the data among different area of flash memory in the SSD which changes the hash values. This change will make the acquired evidence unfit for an investigation. Therefore, it is necessary to find the technique to acquire the digital evidence from solid-state devices without unintentionally tampering with the evidence. Major features of SSDs are explained below.

1. **TRIM** – This functionality lets the operating system notify the SSD about the deleted blocks in the memory. There is a limitation to SSD where it is necessary to clear the data block before writing into the memory. TRIM functionality overcomes this limitation by clearing the memory block before it can be rewritten. Once the SSD gets the information from the operating system about the free block, memory controller gives the instruction to wipe out the deleted blocks.
2. **Garbage Collection** – TRIM and garbage collection functionalities are interrelated. Garbage collection feature is provided by most of the SSD manufacturers. It speeds up the rewriting process in the memory. Garbage collector monitors the File Allocation table to decide on its own which blocks are no longer in use and perform the operation accordingly.
3. **Wear Leveling** – Wear leveling is an important feature of the SSD which distributes the data onto the whole memory as evenly as possible. The feature of wear leveling is that it checks how many times a flash memory chip in SSD has been written. The new data is stored into the memory space which is either which has not been used or slightly used. This way it prolongs the life of an SSD.

2. LITERATURE REVIEW

Lots of research have been conducted to perform data acquisition from solid-state drives in forensically sound manner. Bell et al. [1] discussed the challenges associated with the solid-state drives for digital forensic investigators. They performed an experimental investigation of solid-state drive and hard drive respectively and provided their recommendations and guidance. Nisbet et al. [2] performed an analysis of SSDs on three TRIM enabled file systems and concluded that TRIM functionality can drastically reduce the deleted data than without TRIM enabled. They tested the SSDs on NTFS, HFS+, and Ext4 file system and found that Ext4 offers better opportunity to recover deleted files as compared to NTFS and HFS+.

King et al. [3] performed an empirical analysis of SSD data retention and found that without TRIM, most of the deleted files were recovered. However, only 27% files were recovered with TRIM enabled. Antonellis [4] conducted research to test the SSD by wiping out the data with single pass followed by formatting and partitioning the SSD as single NTFS partition. The result of this experiment only recovered the file name without file content [4]. Bonetti et al. [5] proposed a methodology to help the digital investigators to assess whether the data acquisition from SSD is expensive or not. Bonetti et al. used the SSD from Samsung, Crucial, and Corsair.

Marupudi [6] compared the Hard Disk Drive and Solid-State Drive and presented the key features of SSD which makes it difficult for digital investigators to acquire the data. Bednar et al. [7] provided an overview of the challenges associated with SSDs for digital investigators. Shah et al. [8] investigated the forensic potential of SSDs by conducting the experiment to identify the behavior of SSDs in various scenarios i.e. behavior of SSDs without TRIM functionality enables and background garbage collector and vice versa.

Fulton [9] put forward the challenge that SSDs will provide to the digital forensic community moving forward. Authors also discussed the complexity of SSDs that can seriously impact the reliability of acquired data and their analysis. Joshi et al. [10] put forward the features of SSD and provided the method which can reduce the impact of TRIM and garbage collection functionality. According to them, data can be completely recovered. Aldaej et al. [11] performed an experiment to recover the data from two partitions in SSDs, data from one partition was deleted and the data in other partition was formatted. They have tried to recover the data from both the partitions directly from disk and repeated the process to recover the data from disk image and found out that disk image is extracting more data [11]. Neyaz et al. [12] examined different types of flash and solid-state drive, connected by USB interface, by filling them up with various file types and conducted exhaustive experiments to identify the probability of recovering and carving once the files were deleted. Neyaz et al. [13] extended their previous work [12], and analyzed the behavior of wear-leveling in a triple-level cell (TLC) SSD with NTFS file system connected via serial-ATA (SATA) interface. This device was used as primary boot/storage device. This research outlined

the comparison of wear-leveling with TRIM ON and TRIM OFF states effecting different file types. Singh et al. [14] presented a sound method for individual file sanitization on solid-state drives. They termed the as FTLSec that integrated a page-based encryption system in the prevalent flash translation layer. The effectiveness of FTLSec was measured using a Flash-Sim solid-state drive simulator. The results were compared with the prominent FAST flash translation layer scheme and page mapped flash translation layer.

3. STATE-OF-THE-ART TECHNIQUES

Researchers have come up with various approaches to perform forensic analysis of SSDs. Bell et al. [1] performed four experiments to address separate issues. Experiment 1 was performed to check whether SSDs store the deleted data in the same manner as traditional hard drives if the SSD was not overwritten. In this experiment, first they have filled each drive with the files containing the word EVIDENCE and then each drive was quick formatted using the command mgmt.msc and the computer was turned off. This step is followed by checking the magnitude of the data still contained in the formatted drives after turning on the computer after 10 seconds. The result of this experiment revealed that the garbage collection has started just after 3 minutes of turning on the computer and almost all the SSD drives were wiped off resulting in zero recovery. However, for traditional hard drives, deleted data was completely recovered. They have used 64 GB P64 Corsair solid-state drive and the 80 GB Hitachi hard disk drive for this experiment. Experiment 2 involved the forensic analysis of same drives by connecting them to the write blocker and forensic SATA Bridge. Image of the drive was taken to do the analysis of image on the clean machine as per forensic guideline. The result of this experiment has approved the fact that garbage collection of SSD has completely wiped out the data. Experiment 3 involved the analysis of SSD after 30 minutes of quick format and the result was almost same as Experiment 1. Finally, they have performed Experiment 4 to test if write-blocker prevents self- corrosion in SSDs. In the previous three experiments, simply turning on the computer was wiping out the unused space from the SSD by internal garbage collector of the drive. This experiment involved the use of write-blocker before turning on the computer. Authors expected that the since the garbage collection is the internal function of the SSD, the result should match with the previous three experiments. The garbage collector worked even after the write-blocker was attached and it wiped out most of the data.

Nisbet et al [2] performed an experiment on three different cases involving three different file system and operating system. All the three platforms supported the TRIM functionality. Three test cases were having different scenarios to test with both the TRIM enabled and disabled. The result of their experiment was almost same for NTFS and HFS+, however it was different for EXT4. In NTFS and HFS+, the TRIM enabled operation removes the marked blocks within minutes. Batch discard implementation in EXT4 file system on Linux has better scope of data recovery. In all the three cases, the wiping out is very aggressive if TRIM command is sent.

King et al. [3] has performed the experiment using three scenarios. They are High Usage scenario, Low Usage scenario, Format scenario. High usage scenario keeps very less free space for use by operating system. The purpose of this scenario is to stress out the garbage collection process because there will be less blocks available to clean. Low usage scenario used the brand-new machine with very less user file. The drive mostly contained the operating system files and this is an ideal situation for garbage collection process because there will be lots of clean blocks available. The third scenario is format where the disk was undergone quick format option on Windows 7 or Ubuntu. Based on these three scenarios, they have proposed three hypotheses. For high usage scenario, they assumed that there will less likely that data will be permanently lost on high usage scenario because of the high usage of garbage collection process. Similarly, for low usage scenario, they assume that the most of the data will be lost. Finally, for the format scenario, they assume that the data recovery will depend on the disk firmware. They have conducted 144 tests and found some interesting results, Data recovery was almost zero on the Windows 7 with TRIM enabled, however without TRIM enabled, there were significant data recovery which is almost 100 percent.

Antonellis et al. [4] performed a set of operations for forensic analysis of SSD. The experiment involved the deletion of all the graphic files and one text file from the drive followed by taking the .dd image and analyzing the image using FTK toolkit. They have found very unexpected and interesting result. FTK has found all the deleted files, however, on opening those recovered files in HEX editor, showed that all those files were having repeated 00s. They have also used the Ontrack's Easy Recovery Professional to recover the deleted files and the result was identical with that of FTK. Apart from these conclusions they have also found that even the single pass erase is sufficient to permanently delete the file in the SSDs.

Benetti et al. [5] have performed their forensic analysis on three different SSDs. They are Corsair F60, Samsung S470, and Crucial M4 respectively. The first experiment was performed to test the TRIM functionality. For NTFS file system on Windows 7 operating system, Samsung S470 and Corsair F60 has very fast deletion. However, Corsair F60 was having drastically different behavior. Some files were deleted very quickly in three seconds while some files were not erased and recovered completely. In the case of EXT4 file system, result was almost same as NTFS wherever quick format was applied. The second experiment was to test the garbage collection with TRIM disabled. The experiment involved filling the drive with JPEG files followed by quick format of the drive. Result of this experiment showed that even after reasonable amount of garbage collection, 100 of files were recovered. Corsair F60 and Samsung S470 were considered to have garbage collection capability as advertised by the vendors, however, the experiment did not show that garbage collection working on these SSDs. After testing the TRIM and garbage collection features in three SSDs in this experiment, next test was performed to test the erasing patterns. In order to test the erasing patterns, the authors formatted the drive first and filled it with the JPEG images followed by deleting those files from specific areas. The result of this experiment showed that only 0.34 percent of erased files were recovered, however almost all the files were recovered from non-erased areas. Next experiment was the test of compression. Only Corsair F60 had the compression capability, however the other two were also having this capability. In terms of wear levelling, all the three drives implemented this feature as proved by the experiment. Finally, the authors have performed the test of file recoverability. Their purpose of this test was to find out the data recoverability difference between traditional hard drives and the SSDs. In SSDs the functionalities such as TRIM, garbage collection and wear levelling negatively impact the file recoverability. Corsair F60 behaved differently than other two SSD vendors in terms of file recoverability. Approximately 71 percent files were fully recovered on Corsair F60, however, 0 percent files were fully recovered on Samsung and Crucial. The file recoverability rate was 100 percent for all the three vendors when TRIM functionality was disabled. Their tests have some limitation in the sense that it was implemented on one operating system and it could have been expanded for many other operating systems and the SSDs models which will help in making a catalog for forensic investigators.

Marupudi [6] adopted a quantitative research approach to compare the evidence obtained from the Hard Disk Drive (HDD) and SSD. This experiment involved the usage of three different computers where two computers were having SSD and one computer were having HDD. Out of the two computers containing SSD, on was an investigator computer. An evidence was copied on both HDD and SSD after formatting them. After copying the evidence, it was deleted both the drives and the drives were formatted. This step was followed by copying the random data along with evidence files in any combination or in some case only random data on both the drives. Both the drives were formatted after copying the data. This process was repeated iteratively 8 times. The previous steps of copying the data followed by formatting the drive is followed by taking the image of both the drives using FTK imager which was analyzed by using FTK toolkit. The evidences from both the drives were compared afterwards. The result of the analysis of evidence obtained from both the drives shows that number of files recovered from HDD were far greater than that of SSD. For example, the key word search for Farm House was performed and the result showed that 70-80% of the original files were identified in HDD, however, in SSD not even 10% of original files were identified. The process of keyword search was repeated for multiple words and the result were almost same which proved that SSD's are posing the threat to the forensic investigators for finding key evidence from the suspects computers.

Bednar et al. [7] discussed the challenges posed by the SSDs to the digital forensic investigators. There can be multiple challenges associated with retrieving evidence from the SSDs. The memory controllers in SSDs have not reached the stage of maturity, therefore, data may or may not get recovered from the SSD which poses the uncertainty and further requires the additional responses and measures. Sometimes, the memory controller completely purges the data from SSD and sometimes they may not. Redundant data may get erased by the host machine by the memory controllers itself and then comes the TRIM command. It can reset the memory cells containing data which the operating systems considers redundant. Authors have suggested few solutions to handle this issue associated with SSDs. In order to prevent the memory controllers from erasing the data digital investigators can disassemble the SSD to read the memory cells without built in controller. There can be another approach to disassemble the memory chip and use the memory controllers deigned for digital investigations. However, this process will require certification, forensic compliance, and validation. This solution would not address the complications associated with the encryption and decryption of input and output data. This feature of encryption and decryption of input and output are provided by some vendors like Samsung. The authors discussed that the development of SSD has not reached its maturity yet because usually SSDs tries to optimize the efficiency and speed by using memory controllers that removes the redundant data from the memory. However, this feature was not there since the beginning of the development of SSDs. It was introduced later on as the technology is getting evolved.

Shah et al. [8] have conducted an experiment to identify the behavior of SSDs. Authors have argued that nobody had conducted the forensic analysis of SSDs by using it as a primary drive with operating system installed on this drive. All the other research have been conducted by using SSD as secondary drive without operating system installed on it. They believed that with the operating system installed on it, the behavior will be completely different than the one without operating system installed because the functionality of garbage collection may behave differently. Secondly, they argued that most of the research had completely filled the SSD and then the quick format technique was applied. According to them it may be possible that garbage collection technique will clear the data to accommodate the new data. Therefore, it can be possible that the garbage collection process may work differently if the SSD was not filled with the data. Finally, the authors would like to test the SSD from different vendors to analyze the garbage collection functionality. The experiment was performed using three different SSDs on two laptops. The SSDs used in this experiment was from three different vendors. They are Crucial, Samsung, and Kingston respectively. There were different set of experiments conducted.

First experiment was connecting all the three SSDs to Laptop using USB port and after performing quick format they have concluded that data will be recovered fully if there will be no garbage collection and TRIM command is disabled and vice versa. The result from the Crucial SSD showed that 17625 out of 17627 pictures were recovered and can be concluded that Crucial has no garbage collector and TRIM command also didn't work. The same experiment was repeated in Samsung SSD and it has been concluded that Samsung also behaved the same way as Crucial where garbage collection and TRIM command didn't work. The experiment with Kingston SSD also showed the result that was consistent with Crucial and Samsung. Second experiment involved the connection of SSDs to the secondary SATA port. The SSD was filled with the data and then quick formatted. Computer was turned off after 15 minutes of quick format. After the computer was fully booted and the test was conducted to check for data recovery. On Crucial SSD, almost all the data got recovered and it behaved similar to the experiment when the SSD was connected to the USB port rather than the secondary SATA port. The same experiment was repeated with Samsung and Kingston SSDs, and the result was consistent with Crucial SSD. TRIM command and garbage collection do not work if the SSD is connected externally to the computer. Final set of experiments were conducted by connecting the SSD to the primary SATA port and installing the operating system on it and TRIM command was also enabled. The experiment involved the copying of data on SSD followed by quick format. Computer was shut down after 15 minutes of quick format and then turned on to recover the files. The result from Crucial SSD showed that TRIM command worked perfectly and none of the data was recovered from the SSD. The result of experiment from Samsung SSD also showed that the TRIM

command worked perfectly fine and none of the data were recovered. The same result was replicated with the Kingston SSD as well.

Fulton [9] discusses that the SSDs are about to replace the traditional hard drives and the challenges associated with the nature of SSDs are profound particularly for the digital forensic community. This research has tried to address couple of issues related to the recovery of the data from SSDs. First addressed issue was to find whether the technology of SSD makes it difficult to recover the deleted data from it. The SSDs uses NAND memory which has a limitation of the erase cycle count to each block which in turn requires the write operations to be distributed across the available memory space. Apart from that the slow write and erase time of NAND memory needs the blocks to be available all the time for next write operation. This requirement removes the unused space from the memory which is a great hurdle for the digital forensic investigators because of the unavailability of the deleted data. Second addressed issue was the role of manufacturers on the data recovery process from the SSDs in a forensically sound manner. The analysis of SSDs without the manufacturers recommended interfaces such as skipping the memory controllers and directly accessing the memory cells can be expensive as well as time consuming and also it may lead to the data modification. Also, the encryption of the SSD memory can be the potential challenges. Market competition among manufacturers doesn't allow the standards which may further help the digital investigators to comprehend the algorithms applied for wear levelling and other functionalities of SSDs. Third addressed issue was that if the advancement in standards can help to improve the situation. The researchers argue that there is a necessity to pre clear the memory blocks in advance, it should not be necessary to erase it right after the deletion of files. The recommendation is to clear the memory blocks just before the write request was made which in turn will help the digital investigators to recover the data before it gets pre cleared. However, they suspect that manufacturers will voluntarily provide the option to disable the clearing of memory blocks because it would not provide any advantages to them.

Joshi et al. [10] has performed couple of experiments such as explaining the response coming out of features like garbage collection, TRIM functionality, and self-corrosion. They have also recommended the solution to get through an issue related to TRIM functionality which is a major hurdle for digital investigators. In addition to that their research also investigate the way to determine whether SSD performs self-corrosion or not. This research also explores the avenue of using write blocker to recover the data from SSDs before it may get erased. Additionally, they also put forwarded the challenges related to SSD forensics involving various factors such as memory controllers, firmware and the effect of encryption. The different experiments showed that the use of TRIM functionality basically gives instruction to an operating system that the invalid or deleted memory blocks should be completely wiped out as soon as device is turned on. Their research has come to a conclusion that if TRIM functionality is enabled in SSD, then it would be difficult to recover the files, however, without TRIM functionality enabled, even if memory controllers, garbage collection, and self-corrosion operate normally, data can be recovered. Their experiment involved the test of SSD from various manufacturers on multiple operating systems.

Aldaej et al. [11] performed an experiment to test the data recovery from the SSD in an open source environment. This experiment involved the data recovery process from two different partitions. Data from one partition was deleted completely and the data form the other partition was formatted. Next step involved the analysis of the data from both the drives. Direct analysis was done on the same partition which was deleted; however, the image was taken of the drive which was formatted and copied on the other machine and was analyzed to recover the data. The result of this experiment has shown that the data recovery was much better from the image than from the deleted drive.

Neyaz et al. [12] used four different flash and solid-state media with different storage space and make, and explained the working of wear-leveling in all of them based on the various file types, file systems, and Windows and Apple macOS operating systems. The recovering and carving of files from these different media showed contrasting results in Windows' TRIM ON and TRIM OFF, and Apple's macOS case scenarios. Furthermore, there was no trace of files found from all the

media, that were previously wiped out. However, some recovering and carving patterns were found according to type of operating system used with all the media.

The subsequent work of Neyaz et al. [13], the authors explored working of wear-leveling in a TLC solid-state drive and designed two case scenarios to conduct experiment in Windows 7 operating system. The forensic evaluation demonstrated the effect of wear-leveling in different file types and estimated when the files will get corrupted due to wear-leveling technique with TRIM being enabled. Additionally, the experimental analysis pointed out the change in hash values in all forensically acquired images. The authors found change in hash values in the case of TRIM ON while on other hand it remained same when TRIM was disabled.

Singh et al. [14] presented FTLSec (file translation layer with secure erase) method that definitively sanitized individual files on a solid-state drive. FTLSec, by integrating a page-based encryption system in the generic flash translation layer attained its functionality. The experiments indicated that the FTLSec has fewer block erasures and garbage collection operations compared to the usual FAST flash translation layer scheme and page-mapped flash translation layer scheme.

Chang [15] performed a set of experiments to observe the effect of TRIM on the performance of the SSD. The experiments were separated into three parts which includes host behavior, device internal behavior, and interface bandwidth. The host behavior is basically about the changes that happens to the file system once users erases something from the SSD. The device internal behavior is the firmware design as well as the behavior of SSD when it receives the TRIM command from the operating system. Interface bandwidth is basically the capacity of SSD to handle the TRIM overhead. Their overall observation was that the SSDs performs much better if TRIM functionality was enabled.

Mitchell et al. [16] propose a method to obtain an image of the SSD in forensically sound manner. The proposed method is called Deconstruct and Preserve (DaP). DaP involves five steps which includes pre-verification, deconstruction, preservation, acquisition, reconstruction, and verification. According to them, Pre-verification is not that important, however it is highly recommended to verify that the evidence was not tampered. The deconstruction step is performed by someone who is trained in DaP. In this step, SSDs are deconstructed to identify all the components of SSD that takes part in the management. The stage of preservation puts the SSD in a stable state to prevent the evidence from tampering. The hash is calculated in this step to verify later on that the evidence is unchanged. The acquisition stage uses write blockers and any NIST approved image taking software and this process is repeated multiple times to get multiple copies. The reconstruction stage of DaP inserts the original element into the preserved SSD to obtain a new image. The new image can be read and analyzed further. Finally, verification is done to match the hash value from the pre-verification stage. Like pre-verification, verification is also not important. However, it is also highly recommended to ascertain the integrity of the image. Their experimental hypothesis that DaP preserves the evidence on TRIM enabled SSD, or any other traditional hard disk drives, or TRIM disabled SSD has been accepted and it has been proven that consistency of evidence is maintained by using DaP.

4. DISCUSSION & RECOMMENDATION

In this section, various approaches applied by the researchers will be categorized and summarized. Apart from that the recommendation will be provided. The primary focus of all the researches were the experiment related to three main features. The three main features were TRIM command, Garbage Collection, and Wear Leveling. Almost all the discussed research found that there will complete recovery of the data if the TRIM command is not enabled and that will be an ideal case for digital investigators. However, most of the data cannot be recovered if the TRIM command is enabled by the operating system.

The other observation is that even if the write blocker is connected to the SSD before taking an image, there is very low chance that data can be recovered because memory controller and

garbage collector wipes out the unallocated memory cells from the SSD. Another observation after studying the researchers' conclusion from their experiments is that even if the functionality of garbage collection, wear leveling, and self-corrosion is active in the SSD, there can full recovery of the data if TRIM command is disabled. Therefore, the TRIM functionality is the main feature of an SSD, which prevents the digital investigators to fully recover the data from the SSDs.

The recommendation of this survey to the digital investigators is that always try to check on the suspects computer is that what type of drive is there. If it is an SSD, then try to check if TRIM command was enabled or not. If TRIM is not enabled, then take an image by applying traditional techniques like using write-blocker and any software to take image. Otherwise, if the TRIM is enabled, then it will very unlikely to recover any deleted from the drive. However, they can still try to take the image for analysis because sometimes memory controller and garbage collector may not act that fast to completely wiping out the data from the drive.

5. CONCLUSION AND FUTURE WORK

The use of SSDs as a storage device is gaining momentum as more and more manufacturers are coming up with different products. There are many advantages of using SSDs in computer systems such as fast data transfer speed, lower latency, less boot time etc. to point a few. However, the technology behind the SSDs pose a threat to the digital forensics' community in terms of deleted data recovery. This paper discussed various researches that took place in the field of data recovery from the SSDs. Out of all the researches discussed few of them provided the framework and guidelines to recover the data from the SSDs. Other researches pinpointed the challenges associated with using the SSDs in terms of data recovery. As the SSD technology is still evolving and it is far from reaching the stage of maturity, the manufacturers always come up with different products using different algorithms. The future work will incorporate more researches that has been going on in the field of SSD forensics.

6. REFERENCES

[1] G.B. Bell, R. Boddington. "Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?". *The Journal of Digital Forensics Security and Law*, Volume 5, Number 3, 2010.

[2] A. Nisbet, S. Lawrence, M. Ruff. "A forensic analysis and comparison of solid state drive data retention with trim enabled file systems." SRI Security Research Institute, Edith Cowan University, Perth, Western Australia, 2013.

[3] C. King, T. Vidas. "Empirical analysis of solid state disk data retention when used with contemporary operating systems". In Proceedings of the eleventh annual DFRWS conference, Aug 2011, New Orleans, LA. p. S111–7.

[4] C. J. Antonellis. "Solid state disks and computer forensics". *ISSA Journal*, pages 36–38, 2008.

[5] G. Bonetti, M. Viglione, A. Frossi, F. Maggi, and S. Zanero. "A comprehensive black-box methodology for testing the forensic characteristics of solid-state drives". In Proceedings of the 29th Annual Computer Security Applications Conference, ACM, 2013, 269–278.

[6] S.S.R. Marupudi. "Solid State Drive: New Challenge for Forensic Investigation". Culminating Projects in Information Assurance. 2017, 30.

[7] P. Bednar, V. Katos, "SSD: New Challenges for Digital Forensics", ItAIS 2011, Proceedings of the 8th Conference of the Italian Chapter of the Association for Information Systems In Information Systems.

[8] Z. Shah, A.N. Mahmood, J. Slay. "Forensic Potentials of Solid State Drives". In: Tian J., Jing J., Srivatsa M. (eds) International Conference on Security and Privacy in

Communication Networks. SecureComm 2014. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 153. Springer, Cham.

[9] J.W. Fulton. “Solid State Disk Forensics: Is there a Path Forward?” Utica College, May 2014. Web. 9 Oct 2015.

[10] B.R. Joshi, R. Hubbard. “Forensics analysis of solid state drive (SSD)”. In Proceedings of Universal Technology Management Conference, Omaha (2016).

[11] A. Aldaej, M.G. Ahamad, M.Y. Uddin, "Solid state drive data recovery in open source environment". Proc. Int. Conf. Anti-Cyber Crimes (ICACC), pp. 228-231, Mar. 2017.

[12] A. Neyaz, N. Shashidhar, U. Karabiyik. “Forensic Analysis of Wear Leveling on Solid-State Media”. In 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 1706-1710. IEEE.

[13] A. Neyaz, B. Zhou, N. Shashidhar. “Comparative Study of Wear-leveling in Solid-State Drive with NTFS File System”. In IEEE International Conference on Big Data (Big Data), 2019, pp. 4294-4298.IEEE.

[14] B. Singh, R. Saharan, G. Somani, G. Gupta. “Secure file deletion for solid state drives”. In IFIP International Conference on Digital Forensics, 2016, pp. 345-362.Springer,Cham.

[15] C. Mao. “SDD TRIM Operations: Evaluation and Analysis” Site. Natinal Chiao Tung University, July 2013. Web. 9 Oct 2015.

[16] I. Mitchell, T. Anandaraja, G. Hadzhinenov, S. Hara, D. Neilson. “Deconstruct and preserve (DaP): A method for the preservation of digital evidence on solid state drives (SSD)”. In Global Security, Safety and Sustainability – The Security Challenges of the Connected World, 2017.