DOI: 10.21917/ijct.2024.0465

SSD DISCORE - A SCORING METHOD FOR SSD'S DATA INTEGRITY VALIDATION USING DIFFERENT SMART ATTRIBUTES IN THE DIGITAL FORENSICS PROCESS

Abdul Shareef Pallivalappil and S.N. Jagadeesha
Institute of Computer Science and Information Science, Srinivas University, India

Abstract

Solid-state drives (SSD) are replacing hard disk drives (HDD) in the majority of computer systems today. Because SSDs outperform HDDs in terms of efficiency, SSDs are now more necessary to replace HDDs. However, due to uncertain data integrity, SSDs are not forensically sound in design. The data on SSD is continuously changing as a result of Wear Leveling, TRIM and Garbage Collection, which makes data integrity verification in digital forensics challenging. The use of hash algorithms to validate data integrity is crucial in establishing the legitimacy of evidence gathered from suspect systems. In order to shed light on this matter, an experiment was carried out to gather data from an SSD in both user active and user non-active state. The data was then analyzed using the different attributes of Self-Monitoring, Analysis, and Reporting Technology (SMART) to ascertain the data integrity and by proposing a scoring method "SSD DiScore (SSD Data Integrity Score)", which can aid in digital forensic investigation procedure.

Keywords:

SMART, Data Integrity, SSD, Write Blocker, Digital Forensics, SSD DiScore

1. INTRODUCTION

Digital forensics is all about retrieval and examination of information stored in digital devices related to cybercrime, corporate investigations etc. It is the process of finding, protecting, examining, and recording digital evidence. This is done so that evidence may be produced in court when needed [1]. This subject pertains to a distinct subdivision of cyber security that focuses on the consequences of cyber incidents. Using bit-to-bit imaging to retrieve data from suspect devices and use hash algorithms to protect file integrity in an important step in digital forensic investigation process. Law enforcement agencies and enterprises may access and use a range of legislation and standards when it comes to executing incident response processes and digital forensics, respectively. One example of a framework that has received universal acceptability is the Computer Security Incident Handling Guide (NIST-800-61), which is issued by the National Institute of Standards and Technology[2]. However, there is a much stronger connection between the activities described in this framework and Hard Disk Drives (HDD). Solid-state drives (SSD) have supplanted HDD as the preferred secondary storage medium in recent years. This is a result of SSDs' higher load tolerance, speedier performance, and less cost. The increasing popularity of SSDs has prompted concerns regarding the efficacy of digital forensics and incident response techniques in retrieving data from potentially malicious SSDs while maintaining data integrity[3]. Because of the SSD's background garbage collection activity and TRIM operation, it is quite problematic to recover lost artifacts. The background activity is excessive for a typical disk write blocker to stop. The collection of SSD data carries some degree of unpredictability, and it is challenging to verify the SSD's reliability in a court of law; hence, the legality of the SSD is questioned [4].

1.1 DIGITAL FORENSICS ANALYSIS METHOD

- **Identification**: The first step in any forensic process is to identify the digital devices that are being inspected. Searching for, identifying, and recording any possible digital evidence that may be discovered is a step in this process. Setting priorities for the collection of evidence according to its volatility is a significant part of this procedure since it ensures that the evidence is collected in the right order. By doing this, the possibility of damaging the evidence is decreased and the inquiry may provide the best possible findings.
- **Collection**: Determining if any digital evidence would be required in this case is the next step. Devices that could contain digital artifacts are collected and taken for further analysis.
- **Acquisition**: It comprises a partition, a whole HDD or SSD, specific data, actions, and techniques in addition to a bit-by-bit image. Maintaining a thorough record of the process is crucial. The integrity of the collected data must be maintained in order to ensure that the forensic image has not been altered with in any manner and for that purpose hashing algorithms are used such as MD5, SHA1, etc.
- **Preservation**: The preservation technique is the last phase. It is a way to guarantee the safety and security of evidence. A preservation protocol must be created and followed at every step of the way. Additionally, this is required to guarantee the admissibility of digital evidence in court [5].

A forensic image must be validated using a hash algorithm once it has been collected during evidence reconstruction to rule out any possibility of data tampering. The forensic image when compared with previously acquired forensic image should have the same hash value. Because of SSDs architecture, data reading and writing on the drive happens often without requiring user intervention. Because of this, SSD data often changes, causing hash values to vary from when the forensic image was first acquired. The hash findings vary when comparing the imaged copy with the original evidence. This is a difficulty for the corporate investigations, law enforcement, and forensic investigators. So as to differentiate between changes produced by the system and changes made by the user, a clear validation is necessary.

During the early 1900s, Dr. Edmond Locard, a French forensic scientist, put forward the idea that "every contact leaves a trace." This notion subsequently came to be known as Locard's exchange concept, and it forms the basis of modern forensic science practices [6]. It becomes more difficult to get crucial evidence for forensic analysis as technology advances. Notwithstanding the

obstacles in this field, study need to continue in order to identify effective solutions. Since data integrity verifies that no data has been altered, it is a crucial component of digital forensics. To ensure that the evidence obtained from an SSD is reliable, a solution to this issue is required. Hence, this article will address workable solutions to the data integrity validation issues.

2. UNDERSTANDING THE RESEARCH GAP

It is clear to professionals in the field of digital forensics that SSD's are not forensically sound and it is challenging to retreieve deteled data and maintain data integrity. SSDs are becoming more and more frequent in laptops nowadays as opposed to HDDs. The digital forensic technique required to collect artifacts related to the crime and present them as evidence in a court of law is getting more challenging when hackers use PCs with SSDs. However, this has created a problem since SSD is incompatible with the traditional forensic evidence collecting approach. As a result, specific proof on the file integrity of evidence derived from SSDs cannot be provided. Despite the fact that it is important to switch from the typical processes designed for HDDs at this time. Given this, there remains a large amount of untapped potential for study aimed at comprehending and identifying a dependable solution that can facilitate the validation of SSD's data integrity. The procedure need to provide a precise path that the forensic investigators might use in order to ascertain the data integrity validation throughout each phase. In order to shed light on deliberate data tampering, this study attempts to determine the reason behind data change in SSD-equipped systems and develop a scoring scheme to distinguish between user and non-user activity. The digital forensic investigation process can benefit from the use of this data integrity scoring method.

3. OBJECTIVE

The experience of using SSD is completely different. Even when the file is deleted from the system, it will remain just for few minutes. As soon as the blocks in the TRIM queue are removed, the data will be deleted if TRIM is enabled in the operating system, which is usually the case. The exact instant this occurs is controlled by the particular flash memory controller in question. If there is a significant demand for blank pages in SSD, data will be erased during the garbage collection process even if TRIM is deactivated [7].

It is almost impossible to recover deleted information and very difficult to recover erased data due to SSDs' tendency to self-destruct [8]. The fact that write blockers do not stop writing activity in SSDs are another problem brought on by solid-state storage device technology. Acquisitions of digital media is done through connecting a write blocker in forensic acquisition process. This is important since just reading a file might conceal writing to its metadata, especially the access time. The evidence cannot, under any circumstances, be altered because doing so would make it inadmissible in court. It is evident that the write blocker, which is externally applied to the storage device, will not achieve the intended result when implemented on an SSD device. This is due to the fact that the SSD's internal components continue to write data to the storage area despite the presence of the write blocker [9]. Even at a later point when the forensic technique is performed, the evidence from the first collection step should still demonstrate the same data integrity.

Comparing forensic image using a hash algorithm is an essential part of digital forensics, a solution is required to bridge the data integrity validation problem in SSD forensics process. As a result, the study uses SSD's SMART attributes to offer a scoring technique "SSD DiScore (SSD Data Integrity Score)" for data integrity validation. The main contribution of the study are;

- A novel SSD data integrity scoring method using the SMART attributes integrating to the digital forensic process.
- Measuring user active state and user non-active state that led to the change in data integrity value in SSD.
- Formulating equation to measure value of different SMART parameters during digital forensics acquisition process.
- An unequivocal operational level method focusing the challenges in SSD data integrity for social and legal regulatory structures.

4. METHODOLOGY

It is required to create a different solution for the SSD as the designs of an SSD and an HDD differ from one another for digital forensic acquisition process. SSDs will need to be treated the same as any other alterable piece of evidence since there is no reliable method for retrieving the same hash more than once. Reconstructing the methods will be necessary for the investigators to show precisely what actions were taken when dealing with the evidence. It is not optimal for this state of affairs, and it cannot last indefinitely. Ultimately, the firms who manufacture these drives have the undeniable culpability. It is necessary for all controller cards to be capable of receiving a "no erase" command when a write blocker is connected to the SSD. A drive's software would ultimately be cracked, allowing the controller to be programmed to respond negatively to commands anytime they were received. Given that we are just entering a very challenging period, engaging in the field of digital forensics at this time is both intriguing and exhilarating [10]. To establish a solution, one must understand several aspects of the SSD controller's operation, including its ability to track the number of writes performed on the SSD and its implementation of the SSD TRIM function. Given that the most majority of solid-state drives (SSDs) are predominantly made out of NAND flash memory, computations are based on the mean value of NAND write cycles. SSD manufacturers assess disk dependability by gathering data using SMART technology [11].

SMART technology has several attributes such as, how many times data is written, how many times SSD is powered ON etc., [12]. It is recommended that research needs to be done on the technologies and methods, which can be used to evaluate the data integrity in SSDs. Few of such SMART attributes are utilized throughout the forensic imaging process to recognize the data change in SSD is caused by user activity or system activity, perform a deep analysis, and provide data integrity score.

5. RESULTS AND DISCUSSION

Data collecting based on system idle and active states was initiated for the analysis of the SSDs Write Count, Power ON

Count, Power ON Hours from the SMART attributes, along with hash values. CrystalDiskInfo info, a tool for reading and tracking disk drive health status, was used in this process [13]. Real-world experimentation was deemed crucial in this investigation to underscore the significance of the digital forensic process; therefore, an experiment lab was established to carry out the research and gather data in sequential pauses. To gather data on the various attributes of SMART in SSD for the purpose of validating data integrity and distinguishing between user and system activity that results in data modification, experiments were conducted on a dedicated laptop equipped with Windows 10 and an SSD. Files repository included XLS, DOCX, JPEG, and TXT files. By precisely delineating various scenarios in which a laptop is utilized, its image was obtained as if it had transpired in a real-life situation. Following file saving, the internal SSD in the laptop was utilized for multiple experiments aimed at comprehending SSD activity. Once the files were saved, the SSD was immediately disconnected and connected to a forensic workstation using SSD enclosure case and a write blocker to image the SSD. The FTK Imager was used to acquire the image, while the SSD was queried for its hash value and SMART data. Subsequent to this operation, the SSD was reconnected in the laptop's SATA port. The host system was signed in, and the user engaged in laptop activity for a certain duration of time. This is to ascertain the quantity of SMART data, including Power ON count, Host write count, and Power ON hours, that is modified through user activity. Following that, the laptop was turned off and the cover was removed in order to separate the SSD from the laptop port. After that, the device was connected to the forensic workstation via the SSD SATA enclosure case and the SafeBlock write blocker was activated. FTK was used to acquire the image and SMART data was captured. The subsequent step in the investigation was to gather data in order to comprehend the data modification activity occurring on the SSD while it was connected to a Forensic Workstation with the write blocker was deactivated and idle state. Following a period of inactivity on the forensic workstation, an image of the SSD was obtained in addition to SMART data. During the concluding phase of the investigation, the SSD was reconnected to the host laptop, and the laptop performed an hour of user activity. The SSD was then detached from the host laptop once more, connected to the forensic workstation, and SMART and image data were collected. The host laptop did not have the TRIM option disabled in all experiments. The source data collection details are as follows;

Table.1. Source data collection details

SSD Details	ZEB-SD13 2.5 SATA SSD 128 GB
Operating System	Microsoft Windows 10 Home
Write Blocker	SafeBlock
2.5 SATA SSD Enclosure	CSH01
Imaging Software	FTK

5.1 EXPERIMENT 1

Date and Time: 21-11-2023 at 12:39 PM: After saving user generated files, the laptop was turned off and SSD was removed from the laptop. It was then connected to SSD portable case. The portable case is equipped with USB C type connector that can be connected to Forensic Workstation. After connecting to the Forensic Workstation using CrystalDiskInfo the following data was read from the SSD.

Table.2. Experiment 1 Source data collection details

Host Write Count	94 GB
Power ON Count	27 Count
Power ON Hours	12 Hours

After collecting SMART Data, Imaging was carried out using FTK imager by enabling write blocker and hash value was collected as follows:

SHA1 Hash: baae46bbde3837655e511e416801455e4abcd14

5.2 EXPERIMENT 2

Date and Time: 21-11-2023 at 1:11 PM: SSD was connected to host laptop. User activity happened for 60 minutes after the operating system loaded and signed in. After 60 minutes, the SSD was connected to Forensic Workstation at 2:11 PM and following SMART data was collected.

Table.3. Experiment 2 Source data collection details

Host Write Count	99 GB
Power ON Count	29* Count
Power ON Hours	13 Hours

*29 Power ON Count is due to SSD was connected to the host laptop, and then it was connected to Forensic Workstation and hence the value increased. After collecting SMART Data, Imaging was carried out using FTK imager by enabling write blocker and hash value was noted down as follows:

SHA1 Hash : 3dd5de50008bbf387a51ea0169475814102a5296

5.3 EXPERIMENT 3

Date and Time : 21-11-2023 at 3:04 PM: The SSD was not connected back to the laptop. But instead, it was kept connected to Forensic Workstation by disabling write blocker in with no user activity and following SMART data was collected.

Table.4. Experiment 2 Source data collection details

Host Write Count	99 GB
Power ON Count	29 Count
Power ON Hours	14 Hours

Using FTK Imager by enabling write blocker imaging was carried out at and following hash value was recorded.

SHA1 Hash: e9b9a52d9c6e1883a72139a74c94538f4a76d5c0

5.4 EXPERIMENT 4

Date and Time: 21-11-2023 at 4:45 PM: Connected SSD to host laptop at 4:45 PM. Heavy user activity was carried out. Host system was shutdown at 6:18 PM removed SSD and connected to Forensic Workstation at 6:28 PM. Following SMART data was collected.

Table.5. Experiment 2 Source data collection details

Host Write Count	101 GB
Power ON Count	37 Count
Power ON Hours	16 Hours

Using FTK enabling write blocker imaging was carried out with following hash value.

SHA1 Hash: 7848575725067e1beficaae82d5174fb3b42bba8

From experiment 1, 2, 3, and 4 the following summary is created.

Table.6. SMART data summary

Details	Host Write Count	Power ON Count	Power ON Hours	Change in Hash Value (Yes/No)
Exp.1: Initial Acquisition of SSD	94	27	12	Hash Value Generated
Exp.2: (User Active state)	99	29	13	Yes
Exp.3: (No User Activity)	99	29	14	Yes
Exp.4: (User Active State)	101	37*	16	Yes

*In experiment (4) the host system went to sleep mode 8 times in 2 hours resulting the value of Power ON Count to be 37. To generate a score based on the variation in the values of distinct SMART parameters, nine conditions are derived from the data presented in Table.6 and the corresponding hash values. The abbreviations used are as follows:

- *HWC* - Host Write Count
- *POC* - Power ON Count
- *POH* - Power ON Hours
- *HV* - Hash Value

Table.7. DiScore based on the difference in the values of distinct SMART attributes.

Conditions	Di Score
If the HWC value from the previous HWC value > 1, If the POC value from the previous POC value > 1, If the POH value from the previous POH value > 1, If the HV value from the previous HV value is different.	0
If the HWC value from the previous HWC value > 1, If the POC value from the previous POC value > 1, If the POH value from the previous POH value is equal, If the HV value from the previous HV value is different.	1
If the HWC value from the previous HWC value > 1, If the POC value from the previous POC value is equal, If the POH value from the previous POH value > 1, If the HV value from the previous HV value is different.	2
If the HWC value from the previous HWC value > 1, If the POC value from the previous POC value is equal, If the POH value from the previous POH value is equal, If the HV value from the previous HV value is different	3
If the HWC value from the previous HWC value is equal, If the POC value from the previous POC value > 1, If the POH value from the previous POH value > 1, If the HV value from the previous HV value is different	4
If the HWC value from the previous HWC value is equal, If the POC value from the previous POC value > 1, If the POH value from the previous POH value is equal, If the HV value from the previous HV value is different.	5
If the HWC value from the previous HWC value is equal, If the POC value from the previous POC value is equal, If the POH value from the previous POH value > 1, If the HV value from the previous HV value is different	6
If the HWC value from the previous HWC value is equal, If the POC value from the previous POC value is equal, If the POH value from the previous POH value is equal, If the HV value from the previous HV value is different	7
If the HWC value from the previous HWC value is equal, If the POC value from the previous POC value is equal, If the POH value from the previous POH value is equal, If the HV value from the previous HV value is equal	8

Data Integrity Score is a measure of the quality of data. It is used to assess the accuracy, completeness, and reliability of data. A high Data Integrity Score indicates that the data is of good quality and can be trusted. On the other hand, a low Data Integrity Score indicates that the data is of poor quality and may not be reliable for decision-making [14].

In this experiment, a score of 0 indicates an unreliable Data Integrity status, while a score of 8 indicates a reliable Data Integrity status. The score can range from 0 to 8, depending on the given conditions.

A piecewise function is used to calculate the value of the variable *Score* according to various conditions outlined. Every case in the piecewise function corresponds to a specific set of conditions and the corresponding value of *Score* when those conditions are met.

Table.8. Piecewise function to represent the DiScore method

```
Score = {
0 if (HWC > PrevHWC) and (POC > PrevPOC) and (POH > PrevPOH) and (HV != PrevHV)
1 if (HWC > PrevHWC) and (POC > PrevPOC) and (POH = PrevPOH) and (HV != PrevHV)
2 if (HWC > PrevHWC) and (POC = PrevPOC) and (POH > PrevPOH) and (HV != PrevHV)
3 if (HWC > PrevHWC) and (POC = PrevPOC) and (POH = PrevPOH) and (HV != PrevHV)
4 if (HWC = PrevHWC) and (POC > PrevPOC) and (POH > PrevPOH) and (HV != PrevHV)
5 if (HWC = PrevHWC) and (POC > PrevPOC) and (POH = PrevPOH) and (HV != PrevHV)
6 if (HWC = PrevHWC) and (POC = PrevPOC) and (POH > PrevPOH) and (HV != PrevHV)
7 if (HWC = PrevHWC) and (POC = PrevPOC) and (POH = PrevPOH) and (HV != PrevHV)
8 if (HWC = PrevHWC) and (POC = PrevPOC) and (POH = PrevPOH) and (HV = PrevHV)
}
```

Table.9. DiScore result from SMART data collected from experiment 1,2,3 and 4

Experiment	DiScore
SMART data of experiment 2 compared with SMART data of experiment 1. *HWC*=99, *POC*=29, *POH*=13, *HV*=3dd5de50008bbf387a51ea016947 5814102a5296. *PrevHWC*=94, *PrevPOC*=27, *PrevPOH*=12, *PrevHV*=baae46bbde3837655e511e416801455e4abcd14	0
SMART data of experiment 3 is compared with SMART data of experiment 2. *HWC*=99, *POC*=29, *POH*=14, *HV*= e9b9a52d9c6e1883a72139a74c94538f4a76d5c0. *PrevHWC*=99, *PrevPOC*=29, *PrevPOH*=13, *PrevHV*=3dd5de50008bbf387a51ea0169475814102a5296	6
SMART data of experiment 4 is compared with SMART data of experiment 3. *HWC*=101, *POC*=37, *POH*=16, *HV*=7848575725067e1beficaae82d5174fb3b42bba8 *PrevHWC*=99, *PrevPOC*=29, *PrevPOH*=14, *PrevHV*=e9b9a52d9c6e1883a72139a74c94538f4a76d5c0	0

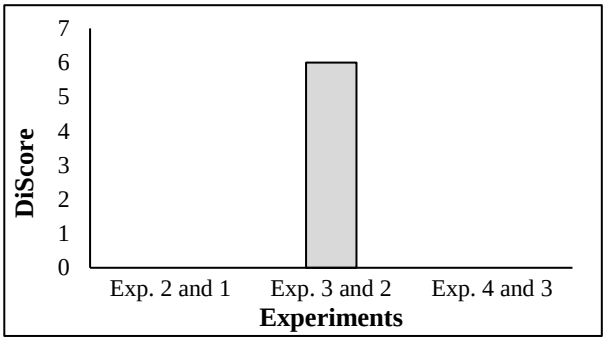

Fig.1. DiScore of Experiment 1,2,3 and 4

The study demonstrates that the hash value consistently changes in all experiments, regardless of whether the system is in a user activity or non-user activity state. SSD data integrity can be challenging to maintain due to its continuous background activity, which causes the data to constantly change, resulting in inconsistent hash values. The results from experiments 2 and 3 indicate that the Write Count and Power ON Count remained unchanged when the system was in a non-user active state, these two parameters from SMART is utmost important as it provides details about data written to the drive from the last acquisition state while powering on the SSD. This has resulted in having a DiScore of 6 which is comparatively a better score to consider digital evidence from SSD in the digital forensics acquisition process. In experiments 2 and 4, there was an observed increase in all the SMART parameters during user activity in the host system which has resulted in DiScore of 0. This indicates that there was a great extent of modification in the data from the previous acquisition state. The SMART data, including Write Count, Power ON Count, Power ON Hours Count, and Hash value must be utilized to assess the extent of modifications made to the SSD's data in order to determine its Data Integrity Score.

6. CONCLUSION

Digital forensics looks for evidence of illegal conduct on digital devices and then tries to identify what kind of evidence it is. It relates specifically to the procedure for finding, archiving, assessing, and documenting digital evidence. This is done in case it becomes necessary to provide evidence in a court of law [15]. The major focus of digital evidence study initially was on computer crimes. However, practically every crime now has a form of digital evidence that may assist law enforcement resolve it. When processing forensic images, digital forensic investigators ought to constantly guarantee the accuracy of the evidence. If the same data needs to be analyzed repeatedly, it must consistently produce the same hash result [16]. The outcomes may compromise one's integrity of evidence if they are not repeatable or validated. Because SSD drives are so often found in laptops and PCs, forensic investigators must deal with certain issues. The design of SSD raises concerns about data integrity during forensic acquisition, and a number of studies have recommended acceptable strategies to address this issue [17].

This experiment demonstrates and proposes that obtaining a forensic image alone won't be sufficient in a real-world situation without changing the TRIM settings in SSD's, which Windows OS by default turns ON. Additionally, the SMART data from the SSD could offer insight into user and system activities that led to the change in image hash value. Hence, the study proposes "SSD DiScore (SSD Data Integrity Score)" method to this novel approach to validate the integrity of data in SSD in digital forensics process.

Through the attainment of an adequate degree of assurance about the proper operation of social and legal regulatory systems, this is a promising outcome for successfully identifying the source of data modification utilizing several SMART attributes in SSDs throughout the digital forensics process.

REFERENCES

[1] EC Council, "What is Digital Forensics - Phases of Digital Forensics", Available at www.eccouncil.org/what-is-digital-forensics, Accessed on 2023.

[2] P. Cichonski, T. Millar, T. Grance and K. Scarfone, "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology", *Computer Security Incident Handling Guide*, Vol. 2, No. 2, pp. 1-12, 2012.

[3] Z. Shah, N. Mahmood, and J. Slay, "Forensic Potentials of Solid State Drives", *Proceedings of International Conference on Security and Privacy in Communication Networks*, pp. 113-126, 2014.

[4] Manish Kumar, "Solid State Drive Forensics Analysis-Challenges and Recommendations", *Concurrency and Computation: Practice and Experience*, Vol. 67, pp. 13-24, 2021.

[5] Akinola Ajijola, Pavol Zavarsky and Ron Ruhl, "A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev. 1: 2014 and ISO/IEC 27037: 2012", *Proceedings of International Conference on World Congress on Internet Security*, pp. 66-73, 2014.

[6] E. Mistek, M.A. Fikiet, S.R. Khandasammy and I. K. Lednev, "Toward Locard's Exchange Principle: Recent Developments in Forensic Trace Evidence Analysis", *Analytical Chemistry*, Vol. 91, No. 1, pp. 637-654, 2018.

[7] Klennet, "Write Blockers are not Effective with SSDs", Available at www.klennet.com/notes/2018-04-16-write-blocking-ssd.aspx, Accessed on 2023.

[8] F. Focus, "Why SSD Drives Destroy Court Evidence, and What Can Be Done About It", Available at www.forensicfocus.com/articles/why-ssd-drives-destroy-court-evidence-and-what-can-be-done-about-it, Accessed on 27 November 2023.

[9] P. M. Bednar, "SSD: New Challenges for Digital Forensics", *Proceedings of International Conference on Association for Information Systems*, pp. 1-9, 2011.

[10] Infosec Institute, "Rock Solid: Will Digital Forensics Crack SSDs, Infosec Resources", Available at www.resources.infosecinstitute.com/topic/ssd-forensics, Accessed on 2013.

[11] K. Vyas, "How Long Does an SSDs Last? Calculate Your SSD's Lifespan", Available at www.enterprisestorageforum.com/hardware/ssd-lifespan-how-long-will-your-ssd-work, Accessed on 2023.

[12] Tech Community Microsoft, "Understanding SSD Endurance: Drive Writes Per Day (DWPD), Terabytes Written (TBW), and the Minimum Recommended for Storage Spaces Direct", Available at www.techcommunity.microsoft.com/t5/user/viewprofilepage/user-id/33564, Accssed on 2023.

[13] Crystal Disk Info, "Crystal Dew World", Available at www.crystalmark.info/en/software/crystaldiskinfo. Accessed on 2023.

[14] Collibra, "Data Quality and Scoring" Available at: www.collibra.com/us/en/blog/the-6-dimensions-of-data-quality, Accessed on 28 November 2023.

[15] Interpol, "Digital forensics," Available www.interpol.int/en/How-we-work/Innovation/Digital-forensics, Accessed on 28 November 2023.

[16] M. Jazzar and M. Hamad, "Comparing HDD to SSD from a Digital Forensic Perspective", *Proceedings of International Conference on Intelligent Cyber-Physical Systems: ICPS 2021*, pp. 169-181, 2022.

[17] R.A. Ramadhan, P.R. Setiawan and D. Hariyadi, "Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037: 2012 and NIST SP800-86 Framework", *IT Journal Research and Development*, Vol. 6, No. 2, pp. 162-168, 2022.