International Journal of Informatics and Computation (IJICOM)
Vol. 8, No. 2, 2026
ISSN: 2685-8711, E-ISSN: 2714-5263 DOI: 10.35842/ijicom

Analysis of Digital Evidence on SATA Solid State Drives with TRIM Using the DFRWS Framework

Muhdini Wakhid[1]*, Rusydi Umar[2], Imam Riadi[3]

Abstract

Solid State Drives (SSDs) use firmware-controlled mechanisms such as TRIM, the Flash Translation Layer, and garbage collection that can affect the availability of deleted digital evidence before forensic acquisition. This study evaluates the effect of TRIM configuration on evidence recovery and integrity on a SATA SSD running Windows 11 Pro 24H2. We applied the Digital Forensic Research Workshop (DFRWS) framework through Identification, Preservation, Collection, Examination, Analysis, and Presentation. The experiment used a WD Green 240 GB SATA SSD, FTK Imager, Autopsy, HashMyFile, Windows Disk Management, and the fsutil utility. Twenty test files were permanently deleted under TRIM Enabled and TRIM Disabled conditions. With TRIM Disabled, we recovered all 20 files (100%), preserved all metadata (100%), and obtained MD5 matches for all recovered files (100%). With TRIM Enabled, we recovered no files (0%), while Autopsy identified metadata for 19 of 20 files (95%). Because no valid file content was recovered under TRIM Enabled, we did not calculate a recovered-file hash-match rate for this condition. The findings show that TRIM configuration directly affects deleted-data availability and demonstrate that metadata persistence does not guarantee content recovery. This paper also shows that DFRWS provides a reproducible structure for acquisition, examination, integrity validation, and forensic interpretation.

Keywords:

SSD, TRIM, DFRWS, Digital Forensics, Digital Evidence

1. Introduction

The increasing use of digital devices has made electronic storage media an important source of evidence in cybercrime investigations. Digital evidence can include documents, images, videos, metadata, and system artifacts. Investigators must acquire and analyze these artifacts without compromising their integrity. A forensic investigation therefore requires a systematic procedure that preserves evidence from the initial identification stage through final presentation. The growing complexity of cyber incidents also increases the need for reproducible forensic methods that can demonstrate how evidence is acquired, preserved, and analyzed. In this context, digital forensic frameworks provide a structured basis for maintaining evidential reliability and supporting the admissibility of digital evidence in legal proceedings. The issue becomes more complex when storage devices perform internal operations that can modify or remove evidence without direct user interaction. [1], [2], [3]

The development of information systems also introduces new challenges for digital investigations. Modern cyber incidents generate large volumes of digital artifacts, while

Corresponding Author: Muhdini Wakhid, Universitas Ahmad Dahlan, Indonesia (2576048025@webmail.uad.ac.id)
1 Muhdini Wakhid, Universitas Ahmad Dahlan, Indonesia (2576048025@webmail.uad.ac.id)
2 Rusydi Umar, Universitas Ahmad Dahlan, Indonesia (rusydi@mti.uad.ac.id)
3. Imam Riadi, Universitas Ahmad Dahlan, Indonesia (imam.riadi@uad.ac.id)

investigators must determine which artifacts remain reliable and relevant. Research on intrusion detection, DDoS detection, and IoT security demonstrates the increasing complexity of digital environments and the need for dependable security and investigation mechanisms. However, identifying an artifact does not automatically guarantee its forensic value. Investigators must also demonstrate that the artifact remains authentic and that the acquisition process does not alter its original state. This issue is particularly important when investigators examine deleted files because the availability of file metadata does not necessarily indicate that the original file content remains intact. Therefore, forensic procedures must consider both artifact availability and evidence integrity during the investigation. [4], [5], [6]

The emergence of Generative Artificial Intelligence (GenAI) further expands the challenges associated with digital evidence. Generative systems can create or modify text, images, audio, video, and other digital content, which complicates the assessment of authenticity and provenance. Recent forensic research identifies deepfakes and AI-generated media as important challenges for digital investigations. Large Language Models (LLMs) also provide opportunities for artifact interpretation, classification, and forensic reporting, but their probabilistic outputs require careful validation. A recent review of LLM applications in digital forensics highlights the need to distinguish AI-assisted interpretation from deterministic evidence validation. This issue suggests that investigators should establish the availability and integrity of digital evidence before applying AI-assisted analysis. Without reliable source artifacts, AI-based interpretation may introduce additional uncertainty into the forensic process. [7], [8], [9]

The transition from Hard Disk Drives (HDDs) to Solid State Drives (SSDs) creates another important forensic challenge. SSDs use NAND flash memory and provide faster access, lower power consumption, and greater resistance to mechanical damage than HDDs. However, their internal architecture changes the way deleted data persists and can be recovered. SSDs use a Flash Translation Layer (FTL), wear leveling, garbage collection, and other firmware-controlled mechanisms to manage data storage. These processes operate differently from conventional magnetic storage and can modify the physical state of stored data without direct operating-system control. As a result, conventional assumptions about deleted data persistence on HDDs cannot be directly applied to SSDs. Investigators therefore need to understand the storage architecture before interpreting recovery results from SSD-based evidence. [10], [11], [12]

The TRIM command represents one of the most important storage-level factors in SSD forensic investigations. When the operating system deletes a file, it can send a TRIM command to inform the SSD that the associated logical blocks are no longer required. The SSD controller can then mark these blocks as invalid and process them through garbage collection. This mechanism improves storage performance and supports efficient block management, but it can also reduce the availability of deleted digital evidence. Investigators may still identify file-system metadata after deletion even when the corresponding file content is no longer recoverable. Previous research therefore shows that TRIM configuration can create a substantial difference between metadata availability and actual content recovery. The main issue is that forensic investigators cannot assume that successful identification of a deleted file means that its content remains intact. [10], [13], [14]

Garbage collection further complicates the recovery process because the SSD controller manages invalid memory pages internally. The controller can consolidate valid data and reclaim blocks that contain invalid pages. These operations occur at the firmware level and may continue without direct user interaction. Park and Kim reported the importance of garbage collection in SSD memory management and its relationship with TRIM-based storage operations. From a forensic perspective, such background processes can change the physical state of deleted data before investigators acquire the device. This

behavior creates a timing problem because the condition of the SSD at the time of acquisition may differ from its condition immediately after file deletion. Consequently, forensic investigators need to document storage conditions and acquisition procedures carefully to determine whether evidence loss results from the deletion process, TRIM, garbage collection, or other SSD management mechanisms. [14], [15]

Although previous studies have examined SSD recovery and TRIM behavior, several issues remain insufficiently addressed. Existing investigations have frequently focused on NVMe SSDs, while SATA SSDs receive less attention. Previous experiments have also used earlier Windows environments, creating a need to examine current Windows 11 configurations. In addition, many studies focus primarily on whether deleted files can be recovered, without jointly examining metadata availability, file-content recovery, and hash integrity. The choice of forensic framework also affects the structure and reproducibility of an investigation. The DFRWS framework provides a systematic sequence covering Identification, Preservation, Collection, Examination, Analysis, and Presentation, but its application to TRIM-based evidence recovery on SATA SSDs under Windows 11 remains limited. These gaps create a need for a controlled investigation that evaluates both evidence availability and evidence integrity under different TRIM configurations. [11], [12], [16], [17]

Based on these issues, this study analyzes the effect of TRIM configuration on deleted digital evidence stored on a 240 GB SATA SSD running Windows 11 Pro 24H2. We apply the DFRWS framework to structure the investigation from identification through presentation and maintain the same hardware, operating system, file system, dataset, and forensic tools across the experimental conditions. We compare TRIM Enabled and TRIM Disabled configurations using three complementary indicators: file recovery, metadata preservation, and hash integrity. This approach allows the study to distinguish between the presence of deleted-file metadata and the actual recovery of intact file content. Our approach also establishes evidence integrity before further forensic interpretation, which is particularly relevant when AI-assisted forensic techniques are considered. Through this controlled workflow, the study aims to provide practical evidence of how TRIM affects forensic recovery on SATA SSDs and to support more reliable interpretation of SSD-based digital evidence in Windows 11 environments. [1], [13], [18].

2. Related Works

King and Vidas investigated the forensic impact of TRIM and garbage collection across sixteen SSDs from different manufacturers. Their empirical study showed that SSD implementations handled TRIM and background garbage collection differently. These differences produced varying levels of deleted-data recovery across devices. The study also found that SSDs supporting TRIM generally retained only a small portion of deleted data after deletion. This work provided important evidence that forensic recovery cannot rely on a single recovery behavior for all SSDs. Its main strength was the use of multiple SSD devices, which exposed differences in controller and firmware behavior. However, the study did not focus specifically on SATA SSDs operating under Windows 11 or evaluate the evidence using the DFRWS framework. It also emphasized data recoverability rather than a combined assessment of metadata preservation and hash integrity. [11]

Vieyra, Scanlon, and Le-Khac examined SSDs from a broader digital forensic perspective. They showed that investigators could not treat SSDs in the same way as traditional HDDs because SSDs performed internal processes such as wear leveling, garbage collection, and TRIM. These processes could continue to modify storage contents even after investigators secured the device with a write blocker. Their study highlighted an important forensic limitation: the examiner could not assume that the physical state of an SSD remained unchanged after acquisition. The work strengthened the understanding of SSD-specific evidence behavior and emphasized the need to consider device architecture

during forensic acquisition. However, the study provided a general forensic analysis of SSD behavior rather than a controlled comparison of TRIM-enabled and TRIM-disabled conditions on a SATA SSD. It also did not specifically evaluate Windows 11 Pro 24H2 or combine recovery, metadata, and hash-based integrity measurements. [15]

Zhetpisbayeva et al. further examined the relationship between TRIM and deleted-data recovery in modern SSDs. Their comparative experiments showed that TRIM significantly reduced the availability of deleted data because SSD controllers could identify unused blocks and process them through internal storage-management operations. The study also discussed firmware behavior, block management, and erase-before-write operations as important factors in forensic recovery. These findings demonstrated that the controller and firmware could influence evidence availability independently of the investigator's acquisition procedure. The main strength of this work was its focus on contemporary SSD behavior and controller-level limitations. Nevertheless, the study also showed why a universal recovery method remained difficult to establish across different SSD implementations. It did not specifically address the combination of SATA storage, Windows 11, DFRWS, metadata preservation, and cryptographic hash integrity examined in the present study. [19]

Hadi, Riadi, and Sunardi investigated deleted-data recovery from NVMe SSDs under different TRIM configurations. They used forensic tools such as Autopsy and RecoverMyFile to examine the availability of deleted digital evidence. Their results showed that the TRIM-enabled condition provided very limited recovery, while disabling TRIM allowed investigators to recover substantially more deleted files. The study provided practical evidence that TRIM configuration directly affected forensic recovery performance. It also demonstrated the usefulness of forensic recovery tools for examining deleted artifacts on SSD-based systems. However, the researchers focused on NVMe storage rather than SATA SSDs. Their work also did not evaluate the investigation through the complete DFRWS workflow or examine metadata preservation and hash integrity as separate evidence indicators. These limitations left room for a controlled SATA-based investigation under a current Windows environment. [18]

Riadi, Sunardi, and Hadi examined the effect of file deletion procedures on the integrity of recovered digital evidence. Their study showed that the deletion process influenced the condition of recovered artifacts and the validity of their hash values. This finding was important because successful file recovery did not necessarily mean that the recovered artifact remained identical to its original form. The study therefore connected recovery availability with evidence integrity, which represented a more complete forensic perspective than recovery rate alone. Its practical contribution also supported the use of hash verification during forensic examination. However, the study did not specifically investigate how TRIM affected the relationship between metadata availability and file-content integrity on SATA SSDs. It also did not examine this issue within a controlled Windows 11 environment using the DFRWS investigation phases. [18]

Ardiansyah and Marzuki applied the Digital Forensics Research Workshop (DFRWS) framework to an SSD investigation involving a hard-format operation. Their experiment reported approximately 29% recovery when TRIM remained enabled and approximately 88% recovery when TRIM was disabled. These results provided strong evidence that TRIM configuration affected the availability of deleted digital evidence. The use of DFRWS also demonstrated the value of a structured forensic workflow for organizing identification, preservation, collection, examination, analysis, and presentation activities. The study therefore provided a direct methodological basis for applying DFRWS to SSD investigations. However, the experiment focused on a hard-format scenario rather than normal file deletion. It also did not specifically evaluate a SATA SSD running Windows 11 Pro 24H2 or jointly measure file recovery, metadata preservation, and hash integrity. [18]

Other Indonesian forensic studies applied structured methodologies to different digital evidence environments, including smartphones, instant messaging applications, and live forensic investigations. These studies showed that investigators could improve evidence acquisition, integrity verification, and reporting by following defined forensic procedures. The smartphone and messaging studies demonstrated the importance of preserving application artifacts and validating extracted evidence. Live forensic research further showed the need to consider evidence that could change during an investigation. These studies strengthened the methodological foundation for structured digital forensic analysis. However, their investigated platforms differed from SATA SSD storage. They therefore provided methodological support rather than direct evidence about TRIM behavior. The present study extended this structured approach to SSD storage by applying DFRWS to a controlled TRIM comparison. [1], [2], [17]

The reviewed studies revealed several limitations that motivated the present research. Previous SSD investigations frequently examined NVMe devices, while SATA SSDs received less attention. Several studies also used earlier Windows environments, while evidence behavior under Windows 11 remained less explored. In addition, previous research often emphasized recovery rates and did not jointly evaluate metadata preservation and cryptographic hash integrity. The reviewed works also used different forensic frameworks and acquisition strategies, which made direct comparison difficult. This study addressed these limitations through a controlled comparison of TRIM-enabled and TRIM-disabled conditions on a 240 GB SATA SSD running Windows 11 Pro 24H2. We kept the hardware, operating system, file system, dataset, and forensic tools consistent between the two conditions. We then evaluated file recovery, metadata availability, and hash integrity within the DFRWS workflow. This approach provided a more integrated assessment of how TRIM affected the availability and integrity of deleted digital evidence. [11], [15], [18], [19].

3. Proposed Method

This study employed an experimental design to examine how TRIM-enabled and TRIM-disabled configurations affected the availability of digital evidence on SATA SSDs running Windows 11. We maintained the same storage media, operating system, forensic tools, dataset, and deletion procedure in both conditions. This controlled design allowed us to attribute differences in forensic results to the TRIM configuration. Experimental approaches have supported controlled evaluation of digital forensic procedures while maintaining evidence integrity throughout the investigation process [1], [2].

We applied the Digital Forensics Research Workshop (DFRWS) framework to structure the investigation from identification to presentation [20]. The framework guided six sequential phases: Identification, Preservation, Collection, Examination, Analysis, and Presentation. This structure allowed us to document the evidence condition before acquisition, create forensic images, examine recovered artifacts, validate their integrity, compare the two experimental conditions, and present the findings. DFRWS served as the methodological framework rather than a recovery algorithm, while TRIM configuration represented the experimental treatment and FTK Imager, Autopsy, and HashMyFile served as the operational tools.

The Digital Forensic Research Workshop (DFRWS) framework provides a systematic model for conducting digital forensic investigations through six sequential phases: Identification, Preservation, Collection, Examination, Analysis, and Presentation [20]. Each phase defines a specific investigation activity and supports consistent evidence handling throughout the forensic process [16]. Previous studies have applied similar structured workflows to mobile, live, and network forensics and demonstrated their value in maintaining evidence integrity, improving examination consistency, and organizing forensic findings [1], [18], [21]. In this study, we applied DFRWS to examine deleted digital evidence

on a 240 GB WD Green SATA SSD running Windows 11. The Identification phase defined the storage device, operating system, NTFS file system, TRIM configuration, forensic tools, and experimental file types. During Preservation, we documented the storage characteristics, verified the TRIM configuration, and generated reference hash values for the original files. The Collection phase then used FTK Imager to create a forensic image of the SSD. We performed the subsequent investigation on this image to minimize the risk of modifying the original evidence [11]. Autopsy supported the Examination phase by extracting deleted files, metadata, directory structures, and other relevant forensic artifacts [18], [21].

The Analysis phase compared the forensic results from the TRIM-enabled and TRIM-disabled conditions. We evaluated recovered files, metadata availability, and file integrity by comparing hash values between the original and recovered artifacts. Hash verification provided an objective measure for determining whether recovered files retained their original content [2]. The Presentation phase then organized the results into tables, figures, and discussions to describe how TRIM configuration affected digital evidence availability on the SATA SSD. This study therefore used DFRWS as an investigation framework rather than as a recovery technique. Each phase supported a specific forensic objective, from identifying the storage environment to presenting validated findings. The sequential structure also helped us distinguish evidence acquisition from evidence recovery and integrity assessment. This approach provided a consistent basis for comparing the two TRIM configurations while maintaining the same storage device, operating system, dataset, and forensic tools throughout the experiment.

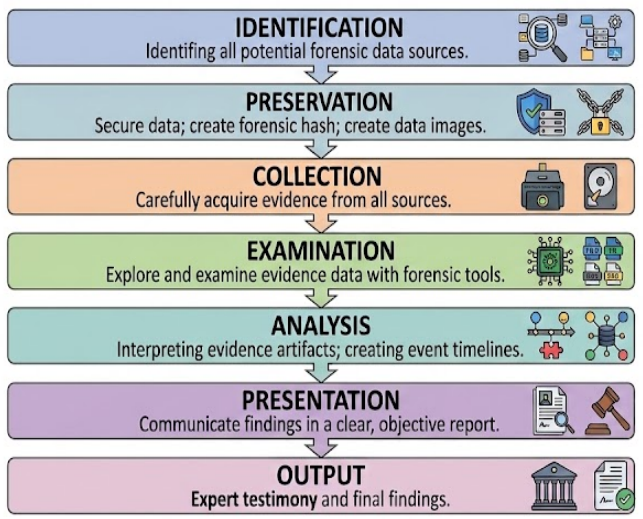

Fig. 1. DFRWS Framework Stages

The experimental evaluation is formalized through three primary metrics. Let N_T denote the total number of test files, N_R the number of successfully recovered files, N_M the number of files for which metadata remains identifiable, and N_H the number of recovered files whose hash value matches the corresponding original file.

Recovery Rate (R):

$$R = \frac{N_R}{N_T} \text{ X } 100\% \quad (1)$$

Metadata Preservation Rate (M):

$$M = \frac{N_M}{N_T} \text{ X } 100\% \quad (2)$$

Hash-Match Rate (H):

$$H = \frac{N_H}{N_R} \text{ X } 100\%, when\ N_R > 0 \quad (3)$$

For this experiment, the independent variable X is TRIM configuration, where X ∈ {Enabled, Disabled}, and the evidence outcomes are represented by Y = {R, M, H}. The experimental objective can therefore be expressed as $Y = f(X|\ C)$, where C represents the controlled conditions of hardware, operating system, file system, dataset, deletion procedure, and forensic tools. The formulation does not claim that DFRWS itself is a mathematical algorithm; instead, the equations quantify the evidence outcomes produced within the DFRWS investigation process. For the final dataset of 20 files, TRIM Enabled produced R = (0/20) × 100% = 0% and M = (19/20) × 100% = 95%. TRIM Disabled produced R = (20/20) × 100% = 100% and M = (20/20) × 100% = 100%. Because no valid file content was recovered under TRIM Enabled, H is reported as not applicable for recovered-file integrity rather than as 0/0.

4. Experimental Setup

1. Materials

The The experimental environment used a 240 GB WD Green SATA SSD running Windows 11 Pro 24H2 with NTFS on a laptop. FTK Imager created the forensic images, Autopsy examined and recovered artifacts, and HashMyFile verified file integrity through hash comparison. Windows Disk Management handled SSD initialization and partition management, while Command Prompt (`fsutil`) controlled the TRIM configuration. The dataset contained document, image, multimedia, and compressed archive files. These tools supported standardized acquisition, artifact examination, and evidence integrity validation [1], [2], [22]. The hardware and software specifications are presented in Table 1.

Table 1. Research Tools and Materials

No.	Tool/Material	Function
1	WD Green 240 GB SATA SSD	Storage medium used as the research object
2	Windows 11 Pro 24H2	Experimental operating system
3	FTK Imager	Creating forensic images of the SSD
4	Autopsy	Examination and recovery of digital artifacts
5	HashMyFile	Validating file integrity using hash values
6	Windows 11 Disk Management	SSD initialization and partition management
7	Command Prompt (fsutil)	Enabling and disabling TRIM configurations
8	Laptop/Notebook	Experimental platform

The storage medium used in this study was a WD Green 240 GB SATA SSD with the NTFS file system. The digital artifacts consisted of document files, image files, multimedia files, and compressed files representing common file types encountered during digital forensic investigations.

2. Research Scenario

The experimental scenario simulated a realistic cybercrime environment in which a user intentionally attempted to remove digital evidence before forensic acquisition [11], [15], [2]. We divided the experiment into a digital crime simulation and a forensic investigation. The simulation used a laptop with a 240 GB WD Green SATA SSD under two conditions: TRIM

Disabled and TRIM Enabled. This paper stored DOCX, PDF, TXT, JPG, PNG, MP4, ZIP, and 7Z files on the SSD, manipulated the files, and permanently deleted them using Shift + Delete before shutting down the system. The forensic investigation followed the DFRWS framework.

We configured the SSD with NTFS, generated initial hash values using HashMyFile, and controlled TRIM through the `fsutil` command in Windows 11. FTK Imager then created an E01 forensic image, while Autopsy examined the image to identify recoverable artifacts, metadata, and directory structures. Finally, we compared the hashes of recovered and original files and reported the recovery rate, hash validity, metadata condition, and differences in digital evidence availability between the two TRIM configurations. availability. This scenario was designed to simulate the actions of perpetrators attempting to remove digital evidence after conducting illegal activities on a computer.

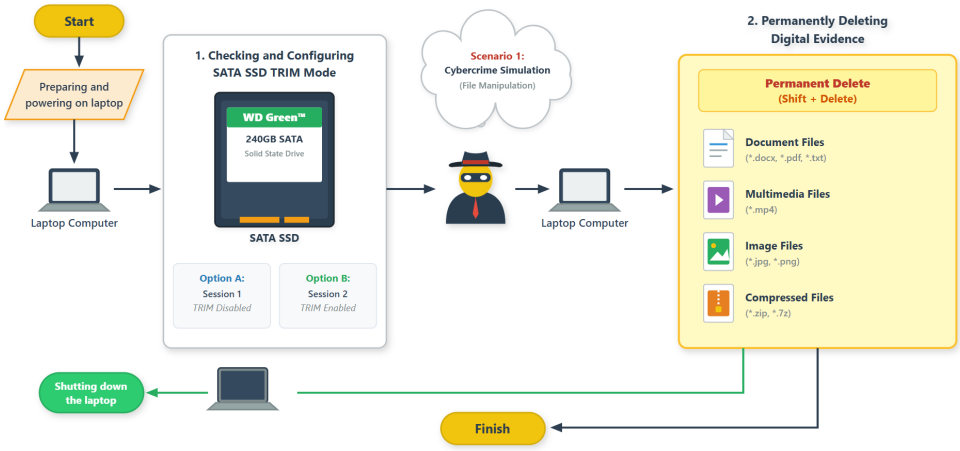

Fig. 2. Digital Crime Simulation Scenario

Based Based on Fig. 2, the simulation used a laptop equipped with a WD Green 240 GB SATA SSD under two experimental conditions: Scenario A with TRIM Disabled and Scenario B with TRIM Enabled. We copied predefined digital artifacts to the SSD, including document files (*.docx, *.pdf, *.txt), image files (*.jpg, *.png), multimedia files (*.mp4), and compressed files (*.zip, *.7z). The simulation then introduced file or document manipulation to represent digital crime activities, followed by permanent deletion using Shift + Delete to bypass the Recycle Bin. After deletion, we shut down the computer before starting the digital forensic investigation. This scenario represented a storage condition similar to real-world cases in which perpetrators attempt to remove digital evidence before forensic examination. Permanent deletion through Shift + Delete also represented a common anti-forensic action for removing digital artifacts from storage media [15].

The digital forensic investigation process was conducted using the DFRWS framework according to the stages illustrated in Fig. 3.

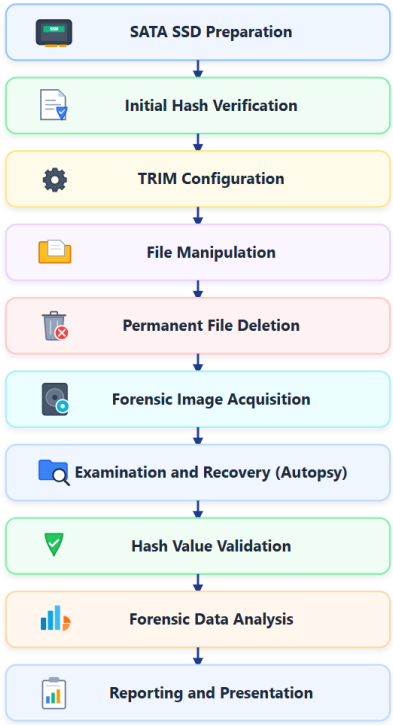

Fig. 3. Investigation Workflow Using DFRWS

The investigation followed eight sequential stages, from SSD preparation to result reporting. This paper used a 240 GB WD Green SATA SSD with the NTFS file system and stored predefined documents, images, multimedia, and compressed files. HashMyFile generated the initial hash values as reference data. We then configured the SSD with TRIM Enabled and TRIM Disabled using the fsutil command in Windows 11. After permanent deletion with Shift + Delete, FTK Imager created an E01 forensic image. Autopsy subsequently examined the image to identify recoverable files, metadata, directory structures, and other digital artifacts.

The validation stage compared recovered files with their original hash values using HashMyFile to assess evidence integrity [2]. This study calculated the recovery rate, examined metadata availability, and verified hash validity for both TRIM configurations. We then compared the results to determine differences in evidence availability and integrity. The final analysis presented the findings using tables, figures, and concise descriptions. This approach allowed us to evaluate the effect of TRIM on deleted-data recovery while keeping the hardware, dataset, tools, and experimental procedures consistent.

5. Result and Analysis

The experiment was conducted using a 240 GB WD Green SATA SSD running Windows 11 Pro 24H2 with the NTFS file system under two configurations: TRIM Enabled and TRIM Disabled. We used the same set of digital artifacts in both scenarios, including document files (.docx, .pdf, .txt), image files (.jpg, .png), multimedia files (.mp4), and compressed archives (.zip, .7z). Before the experiment, we copied all files to the SSD and recorded their hash values as reference values. We then permanently deleted the files using Shift + Delete, acquired forensic images with FTK Imager, examined the images using Autopsy, and validated the recovered files using HashMyFile.

This study first identified the storage environment and its relevant forensic characteristics before acquisition. Particular attention was given to TRIM because SSDs use NAND flash memory, Flash Translation Layer (FTL), wear leveling, and garbage collection, which can affect the availability and persistence of deleted data. We therefore documented the SSD configuration and TRIM status before proceeding with the subsequent forensic stages. The experiment used identical hardware, software, file system, and digital artifacts in both configurations, so differences in artifact recovery and evidence integrity could be examined in relation to the TRIM mechanism. This identification process established a consistent and reproducible foundation for the preservation, collection, examination, and validation stages of the DFRWS investigation [13], [20].

The Preservation stage ensured the integrity and authenticity of the digital evidence before further forensic analysis. Following the DFRWS framework, we first generated MD5 hash values for all original files using HashMyFile and verified the TRIM status through Command Prompt using the `fsutil` utility. We then permanently deleted the files using Shift + Delete under both TRIM Enabled and TRIM Disabled conditions. Before and after forensic imaging, we generated MD5 and SHA-1 hash values to verify evidence integrity. FTK Imager was subsequently used to acquire forensic images of the SSD in E01 format. The acquisition process completed without errors, and the Verify Image results confirmed that the forensic images retained hash values identical to the source storage media. Therefore, the subsequent examination was performed on the forensic images rather than the original SSD, while the original evidence remained preserved throughout the investigation [20], [22], [23].

The examination phase was conducted using Autopsy 4.23.1 on the forensic images acquired during the collection phase. Under the TRIM Enabled condition, Autopsy successfully identified the metadata and deleted file entries, mainly within the Meta Unallocated and Deleted Files directories. However, hash validation showed a 100% MD5 mismatch with the original files, indicating that the file contents had been modified or erased while portions of the metadata remained accessible. Under the TRIM Disabled condition, Autopsy recovered the files and metadata in a more complete state, and most files could be opened while retaining their original structure. Hash validation also showed a 100% MD5 match with the original files.

Table 2. SSD Acquisition Results

Parameter	TRIM Enabled	TRIM Disabled
Image Format	E01	E01
Software	FTK Imager	FTK Imager
Verification Status	Successful	Successful
Image Integrity	Valid	Valid

As presented in Table 2, forensic acquisition was completed successfully in both experimental scenarios without any imaging errors. The E01 forensic images generated using FTK Imager produced identical verification results, indicating that the acquisition process preserved the integrity of the storage media. This finding demonstrates that the observed differences in subsequent recovery results were not caused by acquisition failures but by differences in the TRIM configuration. Therefore, the forensic images obtained in both scenarios were considered valid and suitable for further examination using Autopsy.[22]

The quantitative results show a complete separation in file-content recovery between the

two configurations. Under TRIM Enabled, none of the 20 deleted files were recovered as valid original content, giving a recovery rate of 0%. Nevertheless, metadata for 19 of the 20 files remained identifiable, giving a metadata preservation rate of 95%. Under TRIM Disabled, all 20 deleted files were recovered, giving a recovery rate of 100%, and all 20 recovered files matched their original MD5 values, giving a 100% hash-match rate. The results show why metadata identification should not be equated with successful recovery of the underlying digital evidence.

Table 3. Quantitative comparison of digital evidence availability

Metric	TRIM Enabled	TRIM Disabled
Total test files	20	20
Recovered files	0	20
Recovery rate	0%	100%
Metadata identifiable	19	20
Metadata preservation	95%	100%
Hash-identical recovered files	Not applicable	20
Hash-match rate	Not applicable	100%
Evidence availability	Low	High

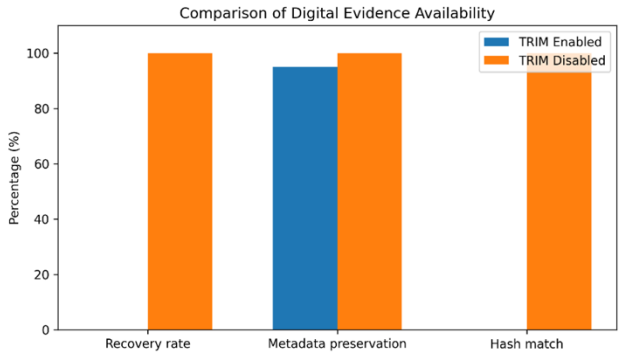

Fig. 4. Quantitative comparison of recovery, metadata preservation, and hash-match outcomes

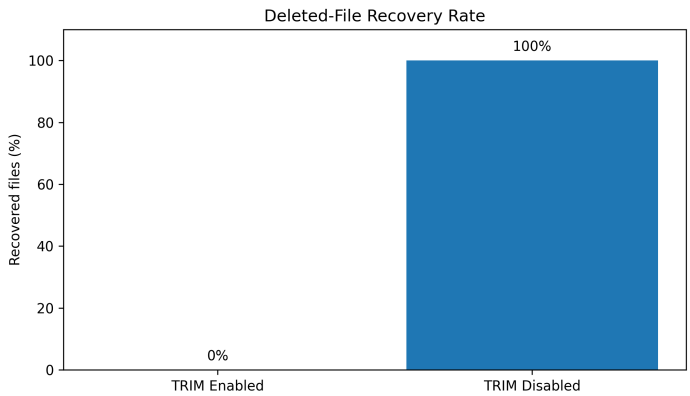

Fig. 5. Deleted-file recovery rate under the two TRIM configurations

The observed difference reflects SSD storage-management behavior. After deletion, TRIM informs the controller that specific logical blocks are no longer needed. The controller can then mark these blocks as invalid and reclaim them through garbage collection. Although this study did not directly observe NAND-page erasure, the 0% content recovery and 95% metadata identification under TRIM Enabled indicate that file-system records remained accessible while the underlying content was no longer recoverable. In contrast, TRIM Disabled allowed deleted content to remain available during forensic acquisition.

These results agree with previous studies. King and Vidas (2011) and Vieyra et al. (2019) showed that TRIM and SSD architecture affect data retention and forensic recovery. Pranoto et al. (2020) and Ardiansyah and Marzuki (2020) also reported higher recovery under TRIM Disabled, with 88% versus 29% recovery in the latter study. Zhetpisbayeva et al. (2025) further identified TRIM and controller behavior as key recovery factors. This study extends these findings to a SATA SSD running Windows 11 Pro 24H2 by evaluating recovery, metadata preservation, and hash integrity together. The complete hash divergence under TRIM Enabled also agrees with Pallivalappil and Jagadeesha (2024), while the difference between 0% content recovery and 95% metadata identification supports Dahlan et al. (2026).

The presentation phase summarized the findings from the DFRWS investigation. FTK Imager successfully produced valid forensic images in both experimental scenarios.The TRIM-disabled condition preserved more complete digital artifacts and higher file integrity than the TRIM-enabled condition, as confirmed by HashMyFile. These findings indicate that investigators should consider TRIM during forensic examinations of SATA SSDs running Windows 11, because SSD garbage collection can reduce recovered file integrity even when metadata remains available.

6. Conclusion

This study investigated the effect of TRIM configuration on deleted digital evidence stored on a 240 GB SATA SSD running Windows 11 Pro 24H2. We applied the DFRWS framework across Identification, Preservation, Collection, Examination, Analysis, and Presentation. Our method used FTK Imager, Autopsy, HashMyFile, Windows Disk Management, and fsutil under controlled experimental conditions. DFRWS provided a structured and reproducible workflow for evidence acquisition, examination, integrity validation, and reporting.

The experimental results showed a clear difference between the two TRIM conditions. TRIM Enabled produced 0/20 recovered files (0%), while metadata for 19/20 files remained identifiable (95%). TRIM Disabled produced 20/20 recovered files (100%), complete metadata preservation (100%), and 20/20 hash matches (100%). Because no valid file content was recovered under TRIM Enabled, a conventional file-level hash-match rate was not applicable. These results demonstrate that metadata persistence does not necessarily indicate successful recovery or content integrity.

This paper contributes controlled evidence from a SATA SSD under Windows 11 Pro 24H2 and evaluates three forensic indicators: recovery rate, metadata preservation, and hash integrity. We also operationalized DFRWS as a reproducible framework for examining the effect of a storage-level variable. Future studies should test different SSD vendors, controller architectures, NVMe and PCIe Gen4 devices, and additional file systems. Further research can examine BitLocker, acquisition tools, recovery tools, and different delays between deletion and acquisition. Our method also provides a basis for studying GenAI-assisted artifact triage and forensic interpretation while maintaining deterministic acquisition, cryptographic validation, reproducibility, human oversight, and legal admissibility.

References

[1] R. Umar, I. Riadi, and R. S. Kusuma, “Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method,” *IJID (International Journal on Informatics for Development)*, vol. 10, no. 1, pp. 53–61, Jun. 2021, doi: 10.14421/ijid.2021.2423.

[2] I. Riadi and A. Dahlan, “Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ),” *JURTI*, vol. 3, no. 1, 2019.

[3] I. Riadi and A. Hadi, “Analisis Bukti Digital Trim Enable SSD NVME Menggunakan Metode Static Forensics (Analysis of Digital Evidence Trim Enable on SSD NVME Using Static Forensics Method).”

[4] S. Riadi and M. N. Fawaiq, “Intrusion Detection System in Network Security Using Naive Bayes and Support Vector Machine,” 2024.

[5] I. Nahak and M. H. Wathan, “Detection of DDoS Attacks Using Hybrid LSTM and SVM Algorithm,” *International Journal of Informatics Engineering and Computing (IJIMATIC)*, vol. 2, no. 2, p. 2025, doi: 10.70687/ijimatic.

[6] P. Lacks, “IoT Intrusion Detection Model Using RNN Algorithm,” 2024.

[7] G. Bendiab, H. Haiouni, I. Moulas, and S. Shiaeles, “Deepfakes in digital media forensics: Generation, AI-based detection and challenges,” *Journal of Information Security and Applications*, vol. 88, p. 103935, Feb. 2025, doi: 10.1016/J.JISA.2024.103935.

[8] A. Wickramasekara, F. Breitinger, and M. Scanlon, “Exploring the potential of large language models for improving digital forensic investigation efficiency,” *Forensic Science International: Digital Investigation*, vol. 52, p. 301859, Mar. 2025, doi: 10.1016/J.FSIDI.2024.301859.

[9] H. Studiawan, F. Breitinger, and M. Scanlon, “Towards a standardized methodology and dataset for evaluating LLM-based digital forensic timeline analysis,” *Forensic Science International: Digital Investigation*, vol. 54, p. 301982, Oct. 2025, doi: 10.1016/J.FSIDI.2025.301982.

[10] C. King and T. Vidas, “Empirical analysis of solid state disk data retention when used with contemporary operating systems,” in *DFRWS 2011 Annual Conference*, Digital Forensic Research Workshop, 2011. doi: 10.1016/j.diin.2011.05.013.

[11] F. Albanna and I. Riadi, “Forensic Analysis of Frozen Hard Drive Using Static Forensics Method.” [Online]. Available: https://sites.google.com/site/ijcsis/

[12] A. S. Pallivalappil and J. S.N., “SSD Discore - A Scoring Method for SSD’s Data Integrity Validation Using Different Smart Attributes in The Digital Forensics Process,” *ICTACT Journal on Communication Technology*, vol. 15, no. 1, pp. 3126–3131, Mar. 2024, doi: 10.21917/ijct.2024.0465.

[13] J. Vieyra, M. Scanlon, and N.-A. Le-Khac, “Solid State Drive Forensics: Where Do We Stand?”

[14] J. K. Park and J. Kim, “SSD Garbage Collection Detection and Management with Machine Learning Algorithm,” *International Journal of Control and Automation*, vol. 11, no. 4, pp. 197–206, Apr. 2018, doi: 10.14257/ijca.2018.11.4.18.

[15] T. Rochmadi and Y. Prayudi, “Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser,” 2017.

[16] I. Riadi, A. Yudhana, and G. P. Inngam Fanani, “Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation,” *International Journal of Safety and Security Engineering*, vol. 13, no. 1, pp. 11–19, Feb. 2023, doi: 10.18280/ijsse.130102.

[17] A. Kurniawan and I. Riadi, “Detection and Analysis Cerber Ransomware Based on Network Forensics Behavior,” *International Journal of Network Security*, vol. 20, no. 5, pp. 836–843, 2018, doi: 10.6633/IJNS.201809.

[18] I. Riadi, R. Umar, and I. M. Nasrulloh, “Analisis Forensik Digital pada Frozen Solid State Drive dengan Metode National Institute of Justice (NIC),” *Elinvo (Electronics, Informatics, and Vocational Education)*, vol. 3, no. 1, pp. 70–82, Jul. 2018, doi: 10.21831/elinvo.v3i1.19308.

[19] A. Zhetpisbayeva, I. Shayea, and A. Baibussinov, “The Effect of TRIM Function on Data Recovery from SSD Solid-State Drives,” Oct. 06, 2025. doi: 10.21203/rs.3.rs-7419937/v1.

[20] G. Palmer, “Digital Forensic Research Conference : A Road Map for Digital Forensic Research,” 2001.

[21] A. Fauzan, I. Riadi, and A. Fadlil, “Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime,” 2016. [Online]. Available: http://ars.ilkom.unsri.ac.id

[22] I. Riadi, R. Umar, and A. Firdonsyah, “Forensic tools performance analysis on android-based blackberry messenger using NIST measurements,” *International Journal of Electrical and Computer Engineering*, vol. 8, no. 5, pp. 3991–4003, 2018, doi: 10.11591/ijece.v8i5.pp3991-4003.

[23] W. Pranoto, I. RIadi, and Y. Prayudi, “Live Forensics Method for Acquisition on the Solid State Drive (SSD) NVMe TRIM Function,” *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, pp. 129–138, May 2020, doi: 10.22219/kinetik.v5i2.1032.

[24] C. King and T. Vidas, “Empirical analysis of solid state disk data retention when used with contemporary operating systems,” in *DFRWS 2011 Annual Conference*, Digital Forensic Research Workshop, 2011. doi: 10.1016/j.diin.2011.05.013.

[25] J. K. Park and J. Kim, “SSD Garbage Collection Detection and Management with Machine Learning Algorithm,” *International Journal of Control and Automation*, vol. 11, no. 4, pp. 197–206, Apr. 2018, doi: 10.14257/ijca.2018.11.4.18.

[26] M. Ihsan Marzuki, T. Elektro, F. Pascasarjana, U. Mercu Buana Jl Raya Meruya Selatan No, and J. Barat, “Analisis Forensik Komputer pada Hard Format Solid State Drive Menggunakan Metode Digital Forensics Research Workshop,” *Jurnal Ilmu Teknik dan Komputer*, vol. 4, no. 2, 2020.

[27] K. A. Dahlan, A. Yudhana, and H. Yuliansyah, “Static Forensic Analysis of File Carving on SSDs uses NIST and ACPO Method,” *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska*, vol. 16, no. 2, pp. 68–75, Jun. 2026, doi: 10.35784/iapgos.7223.