Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

The Effect of TRIM Function on Data Recovery from SSD Solid-State Drives

Aliya Zhetpisbayeva

A.Zhetpisbayeva@astanait.edu.kz

Astana IT University

Ibraheem Shayea

Istanbul Technical University

Azamat Baibussinov

National Defense University of the Republic of Kazakhstan

Research Article

Keywords: Computer expertise, Flash memory, Solid state drive (SSD), Digital Forensics, Data recovery

Posted Date: October 6th, 2025

DOI: https://doi.org/10.21203/rs.3.rs-7419937/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

The need for developing computer forensics has emerged due to the growing number of crimes involving advanced digital systems for unauthorized access. In this regard, digital forensics will always be an advanced field as court cases involving computer technology become more widespread. This research paper presents a detailed study of the fundamental method of using SSD drives for computer forensics. Solid-state drives (SSDs) have replaced traditional spinning disk hard drives and have become the standard for storing data in devices. Today, SSD drives are widely used in desktop computers and laptops. SDDs use flash memory therefore they are highly reliable. This study analyzes the allocated and unallocated storage space on SSD with the TRIM function. One of the key problems is the built-in SSD data self-destruction mechanism, which makes it difficult to recover deleted files. In this research paper, we will consider a method that could reduce the impact of all the features described. The result of the study may contribute to the development of more reliable tools in forensic investigations.

1. Introduction

The relevance of the study is due to the growing role of solid-state drives use by users, which has an impact on forensic investigations for the purpose of data recovery. Solid- state drives (SSDs) are a type of secondary memory widely used in modern computing devices. The main difference between SSDs and traditional hard disk drives (HDDs) is that by their design: SSDs have no moving mechanical parts. Therefore, SSDs are faster, quieter, and more resistant to physical impacts since they do not have mechani- cal components. However, these architectural features create significant difficulties for digital forensics, particularly when recovering deleted data. The methods for storing, managing, and deleting information differ between HDDs and SSDs. Since previously developed for hard drives, they are often less effective or even completely inapplicable when working with solid-state drives.

SSD architecture is based primarily on NAND flash memory. Over the years, the development of NAND flash memory has increased performance and reliability, and reduced manufacturing costs. These improvements have allowed SSDs to increase their capacity, which has accelerated their adoption in various fields of application. For example, from regular computers to high-performance enterprise servers.

SSDs use their own data management process, which is different from hard disk drives (HDDs), in which data is stored on magnetic tape and overwritten directly. Before writing new data, an SSD must first erase existing data from the memory cells. Because of the erase-before-write mechanism, write operations can be slower than read operations if free space on the disk is limited. To solve this problem, modern operating systems and SSD controllers use a special command, TRIM. The TRIM command tells the SSD which data blocks are no longer in use and can be erased in advance, thereby increasing the write speed. And this extends the life of the drive.The TRIM utility provides increased performance SSDs and also has a major impact on digital forensics

The main problems associated with SSDs in digital forensics are the lack of stan- dards across manufacturers, as different SSD controllers have different firmware, which limits the applicability of universal recovery methods.Another problem with SSD data recovery is that wear leveling algorithms can move data blocks unpredictably, making forensic analysis more difficult.

This paper evaluates the impact of the TRIM command on the ability to recover deleted data on solid-state drives. The study includes a comparative analysis under two conditions: with TRIM enabled and with TRIM disabled. By analyzing the dif- ferences in recoverable data in these two scenarios, the study aims to gain a deeper understanding of the impact of SSD technology on modern digital forensics and offer recommendations on potential data preservation and recovery strategies during forensic investigations.

2. Background

This section provides a detailed analysis of flash memory in solid-state drives (SSDs), how the TRIM command works, and SSD vulnerabilities. Flash memory stores data in cells that are controlled by the controller, so it requires an erase operation before it can be rewritten. The TRIM utility tells the SSD which blocks are unused, which affects performance but complicates data recovery. SSD vulnerabilities include lack of stan- dardization, different internal processes, and firmware flaws, all of which complicate forensic analysis.

3. Literature Review

A. Flash-memory in SSD

In Flash memory data is deleted at the block level. The data that is stored in flash memory must be deleted first so that it can be overwritten again into the memory that is commonly used in modern solid-state drives. It has been established that devices that use flash memory erase data and overwrite data at the byte level on the block level. In modern SSD solid-state drives, there are two types of flash memory, which are referred to as NAND and NOR. Table I shows the differences between them in the architecture of NAND and NOR flash memory. On the Table №1 shows the difference between NAND and NOR which are types of flash memory. However, SSD is mainly based on NAND because it has advantages such as lower price and is suitable for storing large data [1].

B. Principle of TRIM

The TRIM command performs a process in which flash memory controllers delete data from a block sector that has been marked as deleted, freeing up space for new data records. Figure 1 shows the structure and principle of the TRIM command. This command allows the operating system to notify the SSD drive about what data has become invalid after it has been deleted. During the deletion process, the operating system marks the corresponding sectors as free for writing new data. The operating system

also sends the SSD TRIM command, informing you that certain data blocks are no longer valid. Due to this, the SSD drive does not move data from these files during garbage collection. This reduces the number of write operations, reduces wear on the flash memory, and extends the life of the device. The SSD's response to the TRIM command depends on the controller and the firmware [2]. In general, TRIM is an ATA interface command. When the operating system deletes the file, it can then send a TRIM command to the SSD and mark the corresponding LBAs as "unused". This allows the SSD drive to physically clear the memory areas that are associated with deleted files. As already mentioned, unlike a traditional hard drive, it is impos- sible to directly overwrite data on an SSD first you need to clear the occupied area. If TRIM is not used, the file system does not inform the SSD that certain logical blocks have been deleted. When using TRIM, there is no guarantee that the data will be completely deleted, and the file system does not receive a notification when the process is completed. There are three possible SSD behaviors when reading data after TRIM:return of non-deterministic data (including possible remnants of a deleted file);returning a fixed data template;Returning only zero values. It is important to note that the value returned during reading may not correspond to the actual contents of the physical memory.

C. SSD vulnerabilities

The key components of a solid-state drive are, to a large extent, the controller and data storage memory. Figure 2 shows a detailed representation of the architecture of a solid-state drive and how modern SDDs will have functions such as flash memory, garbage collector, wear leveling, and a controller known as a block manager, which are located separately rather than compactly on a single magnetic disk, as in traditional hard drives. Solid-state drives (SSDs) mark deleted data as invalid. Nevertheless, they do not necessarily have to be erased im- mediately. This is due to the features of NAND flash memory, where deleted files remain in flash cells until the garbage collection or overwriting mechanism is performed. If the data has not been previously encrypted, it is possible that it can be recovered. Using full-disk encryption on an SSD is one of the most effective ways to protect data, as it prevents the possibility of recovering deleted information. However, this complicates the task of computer forensics. Because even if there is deleted data, it becomes almost impossible to decrypt it without a key [3]. Based on the study, vulnerabilities can occur in both hard- ware and software components. Consequently, malicious SSD-related software can occur at the operating system level and in the drive's firmware. Earlier, it was mentioned that the TRIM command is created by the operating system and processed by the SSD firmware. A rootkit attack aimed at the operating system can block the execution of TRIM commands for SSDs [4]. There are well-documented examples of rootkits that can intercept or modify system commands. The probability of such attacks is high enough, which forces SSD manufacturers to implement protection mechanisms, such as a digital signa- ture, to verify the integrity of the firmware. Malware can be masked or hidden from detection at the operating system level and in the SSD firmware. In the field of computer forensics, data recovery, and solid-state drives are difficult. Because SSDs use mechanisms that are not present in traditional hard drives. Many SSD drives' firmware implements encryption, TRIM, and the associated garbage collection process. These mechanisms make data

recovery more complex. An important aspect is that the execution of TRIM and subsequent garbage collection can lead to the deletion of data without recovery.

4. Methodology

This section explains how researchers determine whether is a hard disk drive, a solid- state drive, or a hybrid drive before executing the TRIM command [5]. TRIM's functionality can be affected by various factors, such as the type of operating sys- tem, disk formats, and the cable connected to the SSD. This section provides detailed information about the various experiments and steps to perform these tests, as well as the results [6]. The TRIM command is one of the important components to always maintain the performance of solid-state drives (SSDs). This function allows the SSD system interface to know which data blocks should no longer be used, optimizing storage management, and reducing unnecessary write operations [7]. However, TRIM support varies depending on the operating system, disk format, and connection type.

For optimal SSD performance, it is recommended to use a TRIM-supported operat- ing system and compatible file system.Using non-compatible file systems or interfaces can hinder the benefits of TRIM, potentially reducing the lifespan and efficiency of an SSD over time.In this study, the data collection method was performed using the live forensics method to analyze non-volatile data on an SSD (see Figure 3).In this study, an experiment is being conducted to test TRIM support by various operating systems and analyze the possibility of recovering deleted files when TRIM is turned on and off. The stages of the study include the study and analysis of digital data obtained during the experiment. To test the operation of TRIM, the file deletion command is executed on various operating systems, after which an attempt is made to restore them. The experiment is conducted on a test computer on which TRIM is enabled or disabled, then the results are analyzed on the investigator's computer [8]. Before starting the analysis, the source data and hash values of the files are recorded to ensure the integrity and authenticity of the results. Comparing the hash values before and after deletion allows you to determine whether the data has been permanently deleted or needs to be restored. Copies of the studied data are also used to preserve the authenticity of the experiment. The figure above shows the stages of examination and analysis employed in this research: 1)Preparation: During the preparation phase, a repository was created for the data that needed to be restored. This study used the Portable FTK Imager tool to create a disk image. The experiment was conducted with the TRIM function on and off on an NVMe SSD to test the effect of TRIM on data recovery capability [9]. 2) Extraction: At this stage, data was extracted from the created disk image. Files that were previously deleted were identified and restored. In addition, the characteristics of the file structure, information about deleted data, file names and their checksums (md5 hash) were recorded.3) Analysis: At the final stage, the extraction results were analyzed, which makes it possible to evaluate the effec- tiveness of file recovery depending on the TRIM state. The study helped determine which tools are most suitable for data recovery with different TRIM settings [10].

Stage 1:

1. Download the new version of Windows 7 Professional SP1 to the NVMe SSD drive.

2. Copy the keyword files to the SSD drive.

3. Delete the files and turn off the computer immediately.

4. Copy the SSD to the hard drive in the duplicator program (optional).Compare the SSD and hard disk hashes

5. Connect the SSD to the write blocker and generate a hash.

6. Use the file recovery utility to search keywords.

7. If successful, wait 1 hour, take the hash and compare, and try the search again.

In step 1, we can expect TRIM functions to make files unrecoverable. The figure above shows the output screen. Similarly, in step 2, the TRIM function is disabled so that files can be restored.

Stage 2:

1. Download the new Windows 7 Professional Service Pack 1 to the NVMe SSD.

2. Copy the keyword files to the SSD.

3. Disable the TRIM function.Set the disable delete notify mode to 1.

4. Delete the files and turn off the computer immediately.

5. Copy the SSD to the hard disk in the duplicator program (optional).Compare the SSD and hard disk hashes

6. Connect the SSD to write blocker and generate a hash.

7. Use the file recovery utility to search for keywords.

8. If successful, wait 1 hour, take the hash and compare, try the search again.

At this stage 2, we can expect that the disabled TRIM state will make the files available for recovery.As shown in the image above, we deleted about 380 files and then turned off the computer to get the hashes. We found an important aspect. This is that all about 370 deleted files were fully recovered by Recuva with TRIM enabled. They were available as thousands of file fragments. Of these, 368 were the original files, 13 files were renamed without changes However, 3 files out of 384 files were keeping the original content but renamed. But when we disabled TRIM by repeating the same process on a Windows

computer, we were able to get the same 378 files, of which 381 were the original files, 0 were renamed but unchanged, and three files were renamed with the original contents of the filename.

Stage 3:

1. Download the new version of Linux version 2.6.28 on SVP200S3/60G SSD drive.

2. Determine if TRIM is supported using the following command:

sudo hdparm -I /dev/sda | grep "TRIM supported"

An output should be displayed with the message: “TRIM is supported for data set management (8 block limit)”, otherwise, your SSD drive does not support TRIM.

Stage 4:

1. Create a disk image with Ubuntu versions 15.10 and 14.04.3 and follow the steps below:

(a) Download the new Ubuntu version and use the SVP200S3/60G SSD drive.

(b) Identify each Ubuntu version before proceeding with the following steps.

(c) For Ubuntu 14.10 and later versions, use:

$ tail -n1 /etc/cron.weekly/fstrim

/sbin/fstrim --all || true

For Ubuntu 14.0 and earlier versions, fstream is not avail- able, so you must use the command below: /usr/share/doc/hdparm/contrib/wiper.sh.gz

5. Results

At this stage on the Figure 10, the analysis of the acquisition results was performed using Portable FTK Imager to examine the impact of the TRIM function on file recovery. The analysis focused on identifying signature values of deleted files under two conditions: with TRIM disabled and TRIM enabled.When TRIM was disabled, as shown in Figure 10 (a), the file signature remained intact, indicating that the deleted file could still be read and recovered. However, when TRIM was enabled, as shown in Figure 11 (b), the file signature was either damaged or modified, making file recovery impossible. These results demonstrate the significant impact of TRIM on digital forensics, as enabling TRIM can permanently erase data, reducing the chances of successful recovery.

6. Conclusion

The development of data storage technologies from classic hard drives (HDD) to modern solid-state drives (SSD) has significantly changed the methods of saving, iden- tifying and restoring deleted files. Enabling the TRIM function plays a key role in this process, as it allows the operating system to tell the SSD which data blocks are no longer in use and can be cleaned up immediately. Our research has shown that TRIM support varies depending on the operating system, file system, and connec- tion interfaces. The experiments have demonstrated that enabling TRIM significantly reduces the likelihood of successful recovery of deleted data, since the drive performs an immediate memory release, removing traces of information. At the same time, disabling TRIM leaves data available before it is overwritten, which allows you to partially restore information using specialized software. It was also revealed that the operation of the SSD controller in Garbage Collection mode can additionally affect data deletion, even when the TRIM function is turned off. However, this process does not always guarantee the complete erasure of information. Thus, the TRIM function plays a crucial role in the irre- versible deletion of data from an SSD, and its presence or absence can significantly affect the capabilities of forensic analysis and information recovery. Modern drives, even with- out TRIM, can independently manage memory cleanup, but the speed and efficiency of this process depend on the specific model and algorithms of the controller.

Declarations

Author Contribution

All authors had an impact to the work.

Acknowledgement

This study was carried out with the financial support of the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan under Contract №388/PTF-24-26 dated 01.10.2024 under the scientific project IRN BR24993232 “Development of innovative technologies for conducting digital forensic investigations using intelligent software - hardware complexes”.

References

1. Solodov D, Solodov I (2023) Data recovery in a case of fire-damaged Hard Disk Drives and Solid-State Drives, Forensic Science International: Reports, vol. 3, no. 2, article 100199, Jul. https://doi.org/10.1016/j.fsir.2021.100199
2. Luković V, Jovanović Ž, Đurašević Pešović S, Pešović U, Đorđe- vić B (2025) Solid-State Drive Failure Prediction Using Anomaly Detection. Elec- tronics 14(7). https://doi.org/10.3390/electronics14071433
3. Frimpong T, Mawuli L, Missah Y, Ussiph N, Ahene E (Sep. 2023) Cold Boot Attack on Encrypted Containers for Forensic Investigations. KSII Trans Internet Inf Syst 16(9):3068–3085.

https://doi.org/10.3837/tiis.2022.09.013

4. Chou Y et al (2023) Why and How to Increase SSD Performance Transparency, Proc. ACM. https://doi.org/10.1145/3317550.3321430
5. Tianyu Ren Y, Du J, Cui Y, Lv Q, Li CJ, Xue (2025) Device-Level Optimization Techniques for Solid-State Drives: A Survey, arXiv:2507.10573 [cs.AR], Jul. 10. https://doi.org/10.48550/arXiv.2507.10573
6. Seth S (Jan. 2023) Application of Solid-State Drive to User Experience and User Satisfaction: Literature Review Study. Dinasti Int J Edu- cation Manage Social Sci 4(2):158–167. https://doi.org/10.31933/dijemss.v4i2.1527
7. Kumar M (2024) Solid state drive forensics analysis—Challenges and recommen- dations, Concurrency and Computation: Practice and Experience, vol. 33, no. 24, Jun. article e6442. https://doi.org/10.1002/cpe.6442
8. Jalil H et al (2023) SSD Forensic Evidence Generation and Forensic Research on Solid State Drives Using TRIM Analysis, Proc. IEEE ICCWS. https://doi.org/10.1109/ICCWS53234.2021.9702989
9. Sun Y, Chen H, Wang M (2023) A Survey on SSD Forensic Analysis Techniques. Concurrency Computation: Pract Experience. https://doi.org/10.1002/cpe.6442
10. Chankyu Koh J, Kang T, Kim SW, Han (2024) IEEE Access 12 154 455–154 466, Jan. https://doi.org/10.1109/ACCESS.2024.3482368Temporal-Contextual Attention Network for Solid-State Drive Failure Prediction in Data Centers
11. Owens Walker T, Justin III, Blanco A, Rakvic R, Vanleer A, Brown D, Shey J, Sinsley GL, Hau T, Ngo RW, Ives Classifying Proprietary Firmware on a Solid-State Drive Using Idle-State Current-Draw Measurements, IEEE Access, 8, pp. 31869–31881, Dec. 2019 (published Feb 2023). https://doi.org/10.1109/ACCESS.2020.2973605
12. Abu Hweidi RF, Jazzar M, Eleyan A, Bejaoui T SATA M.2 on Forensics: Trim Function Effect on Recovering Permanently Deleted Files, in (2023) *Inter- national Conference on Smart Applications, Communications and Networking (SmartNets)*, Jul. 25, 2023. https://doi.org/10.1109/ACCESS.2020.2973605
13. Lange T, Naor J, Yadgar G (2025) Optimal SSD Management with Predictions, *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 9, no. 2, article 30, May 29. https://doi.org/10.1145/3727122
14. Microsoft (2023) Support and functionality of the TRIM command in Windows. Microsoft Docs
15. Zhang X, Bhimani J, Pei S, Lee E, Lee S, Seong YJ, Kim EJ, Choi C, Nam EH, Choi J Bryan S. Kim**,Storage Abstractions for SSDs: The Past, Present, and Future,ACM Transactions on Storage, vol. 21, no. 1, article 1:1–1:44, Feb. 17, 2025. https: //doi.org/10.1145/3708992
16. Prophet SSD Failure Analysis and Prediction Guided by Flash Reliability Characteristics in Data Centers, published May 2025 in IEEE Trans Comput. https://doi.org/10.1109/TC.2025.3566871

Tables

Tables 1 to 4 are available in the Supplementary Files section.

Figures

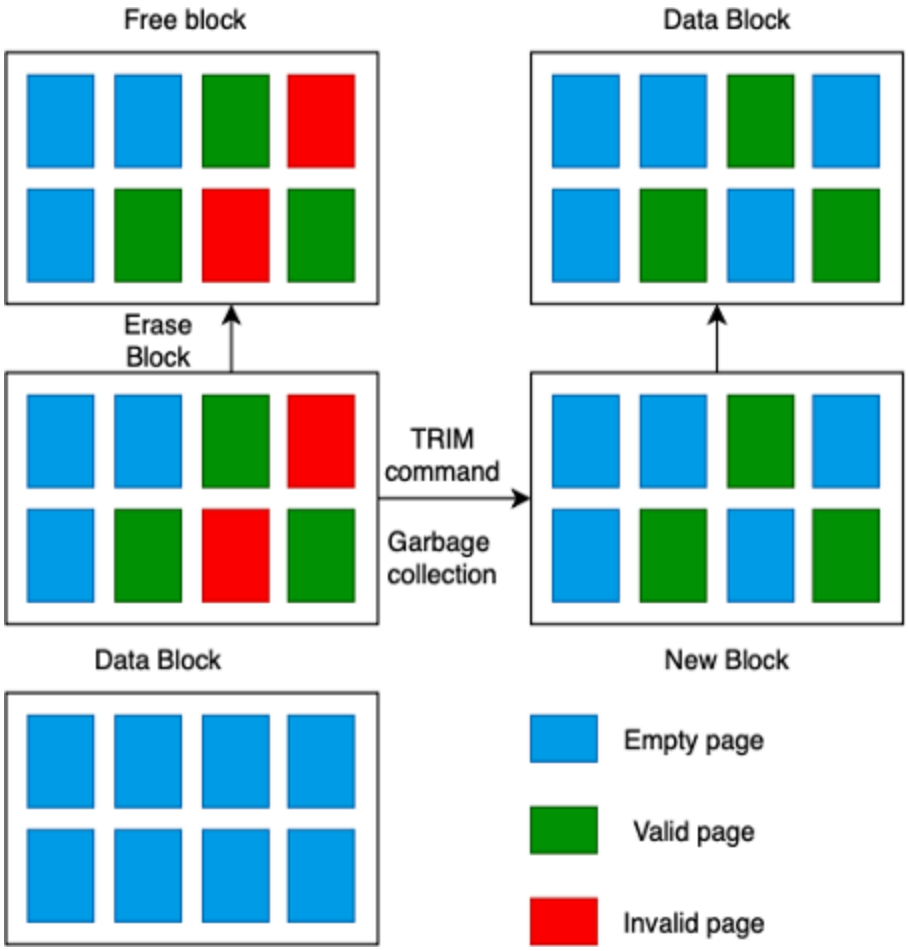


Figure 1

Structure of principle of TRIM

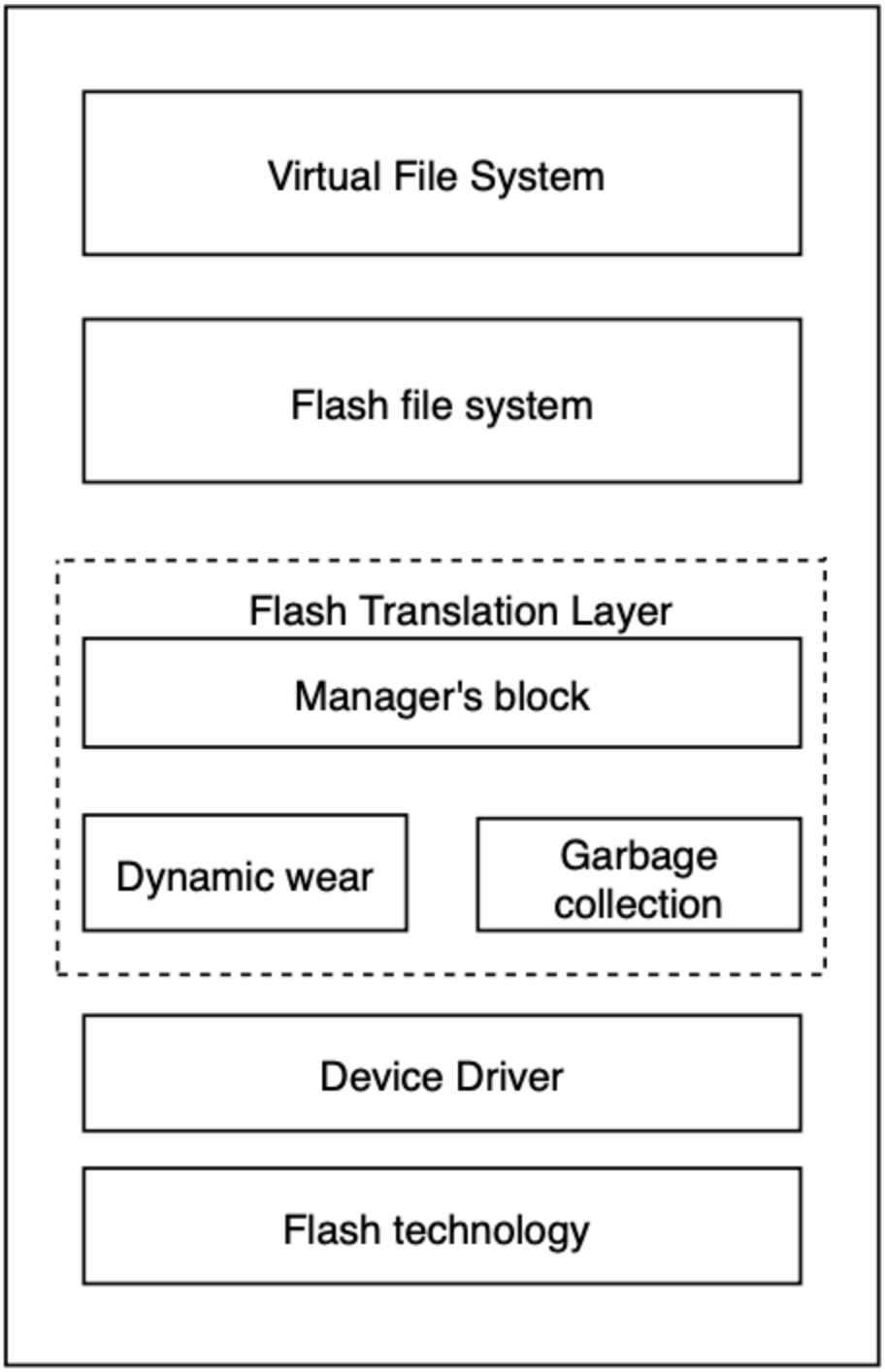


Figure 2

SSD solid-state drive architecture

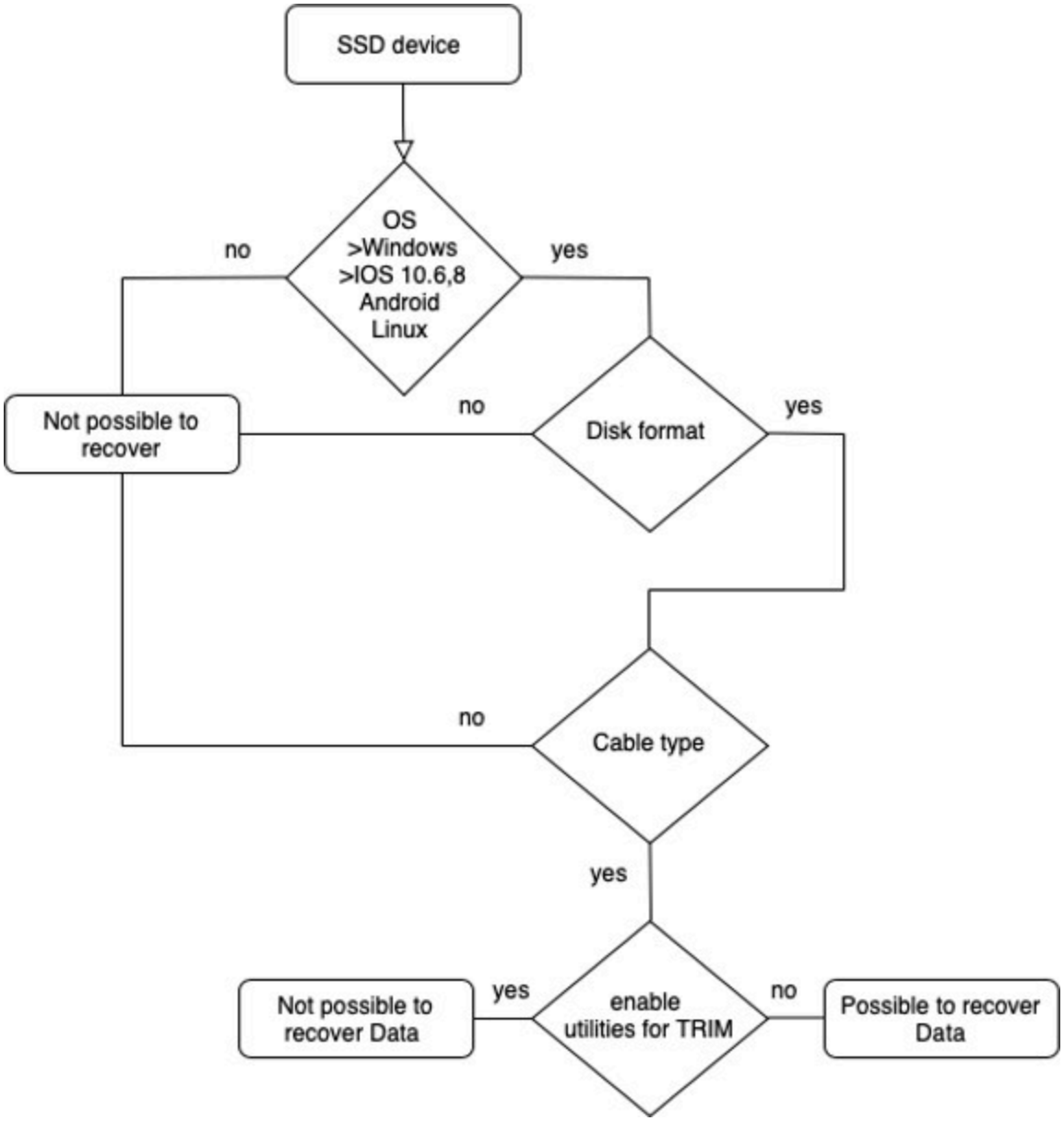


Figure 3

Method of checking TRIM command

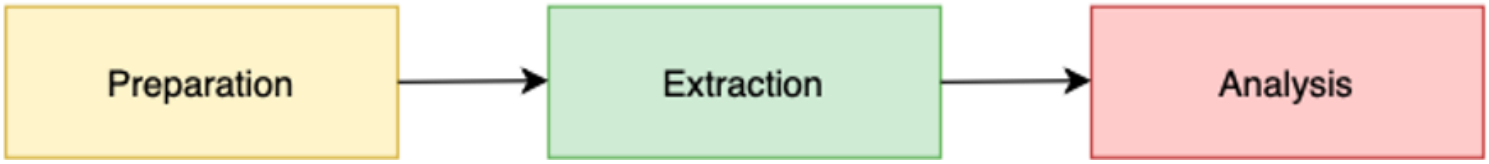


Figure 4

Method of checking TRIM command

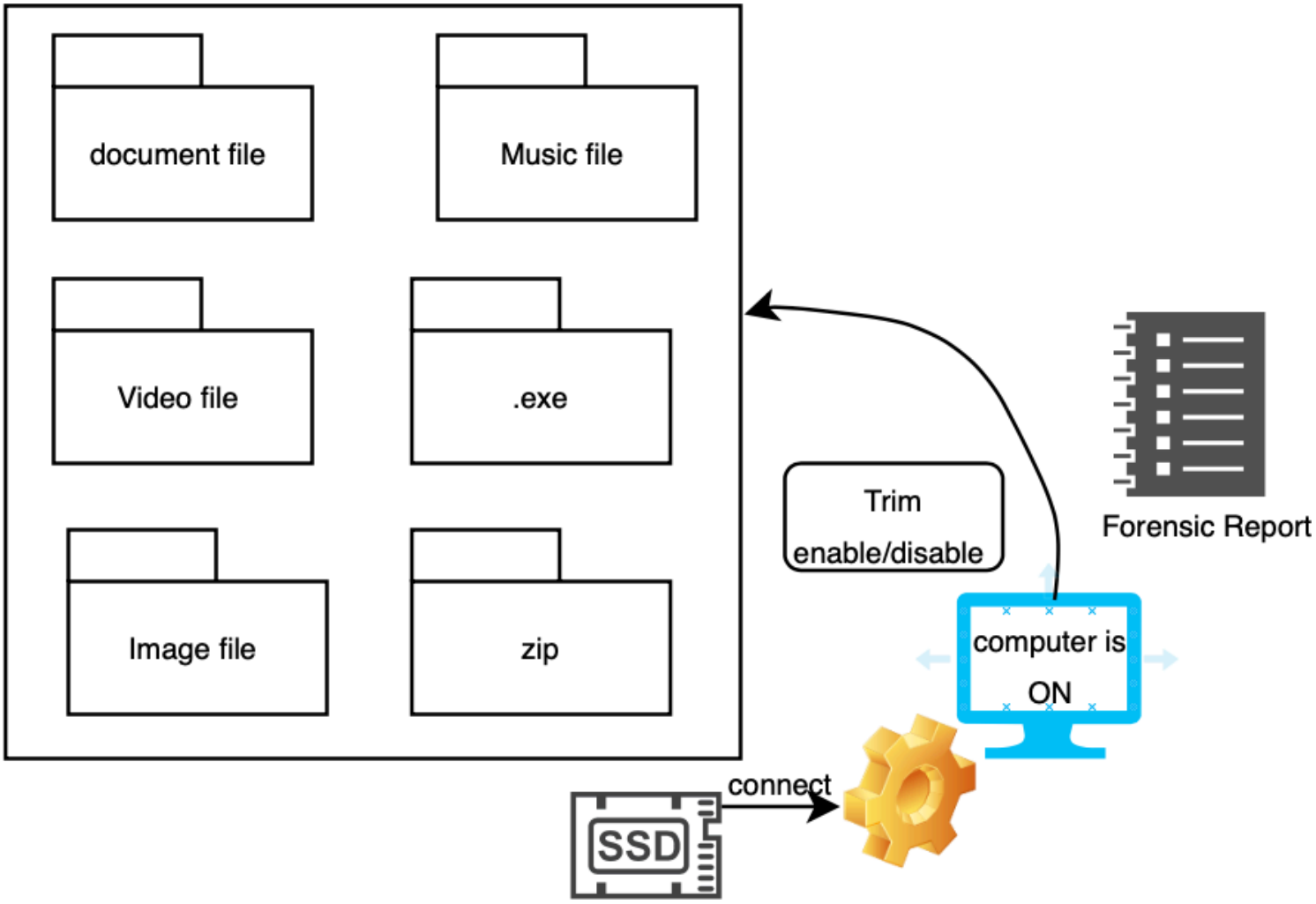


Figure 5

SSD Live Forensics method



Figure 6

Enabling TRIM on a Windows 7 computer and getting a hash

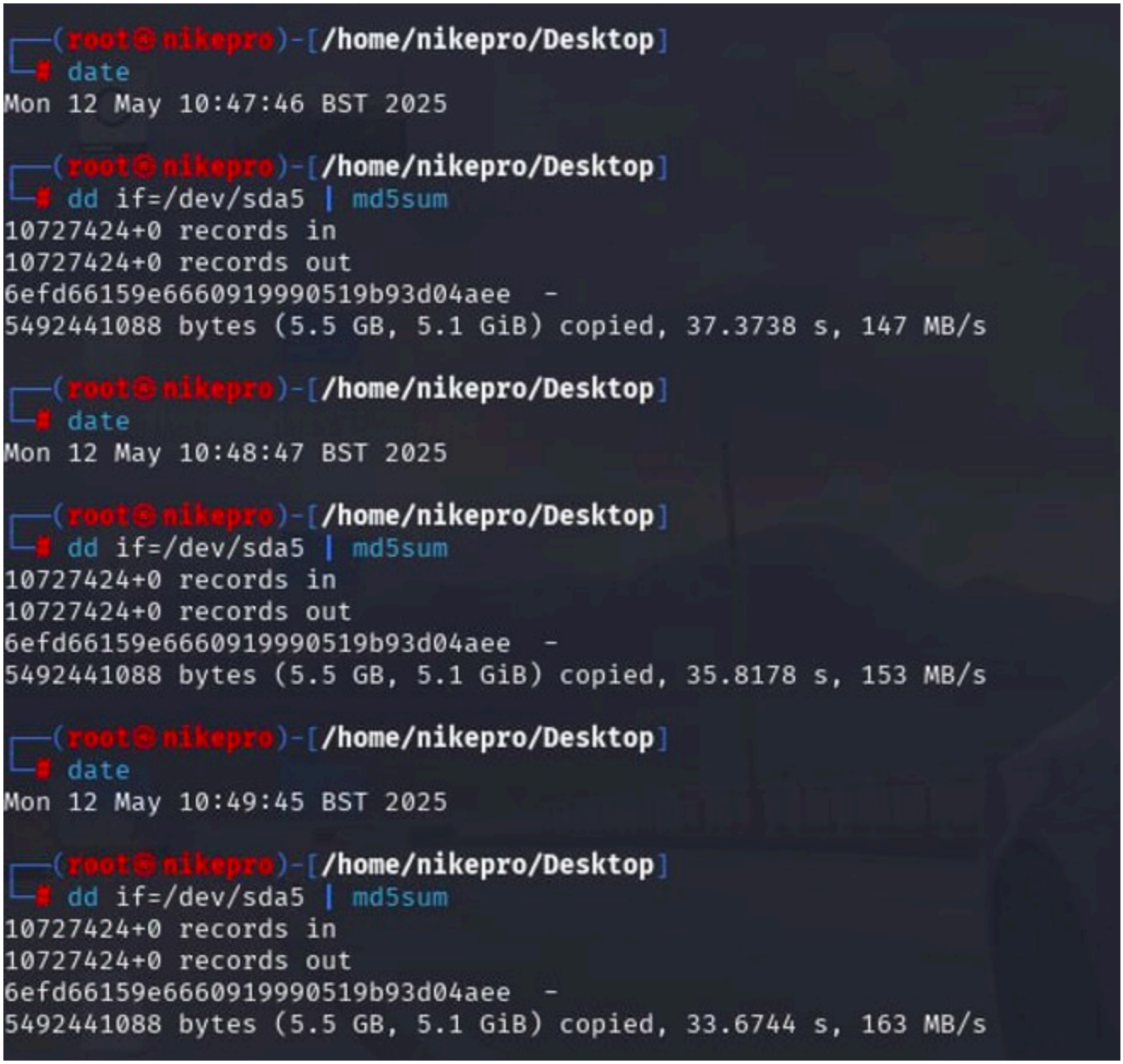


Figure 7

Disabling TRIM on a Windows 7 computer and getting a hash

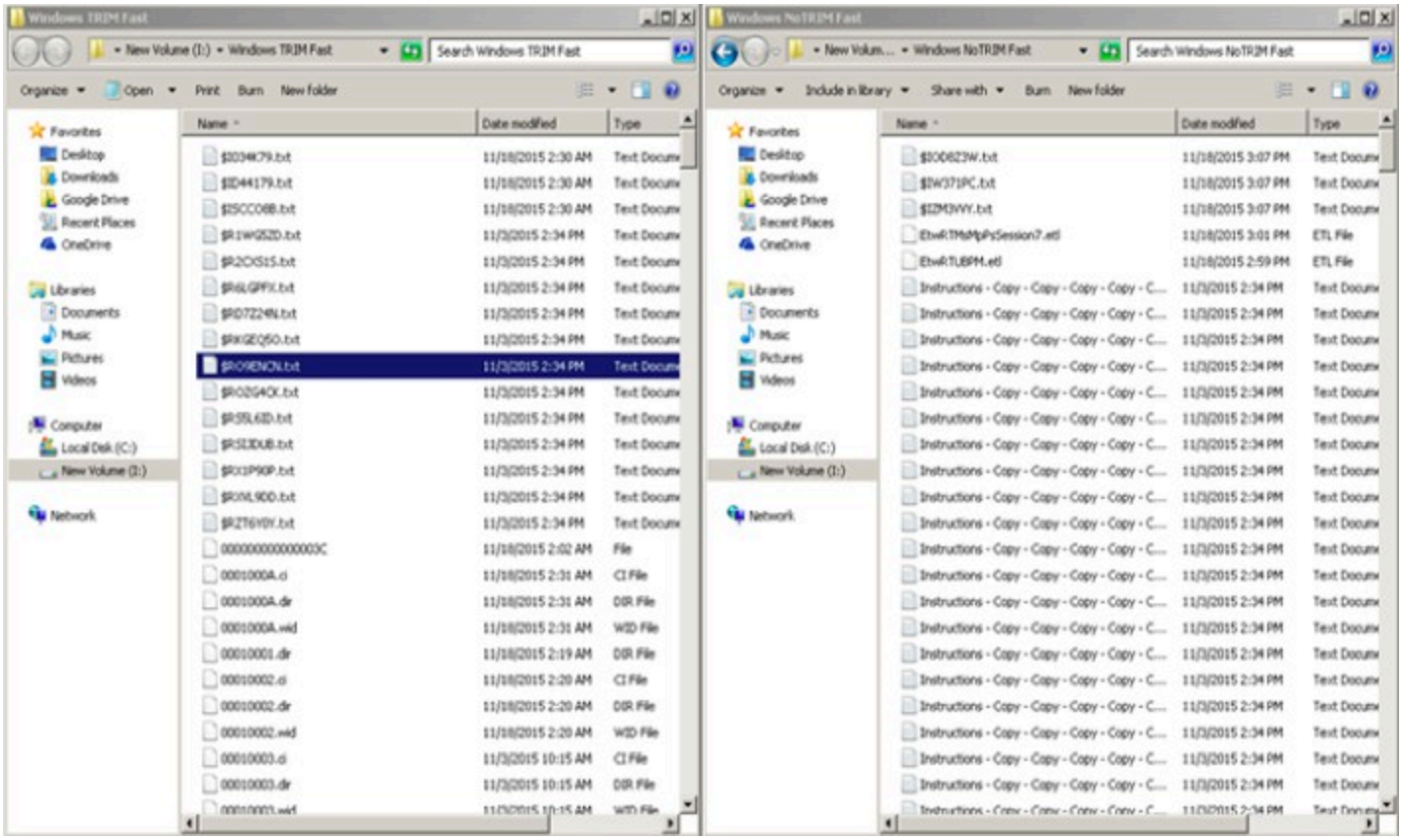


Figure 8

Comparison of Recuva files recovered after using TRIM functions in Windows

```
\u@HackerPro:\w$ cat /sys/block/sda/queue/rotational
0

\u@HackerPro:\w$ grep -i discard /etc/fstab

UUID=39cf109b-62a6-4d0e-b5b8-663f4b744560 /          ext4    errors=remount-ro, discard0     1

\u@HackerPro:\w$ cat /sys/block/sda/queue/discard_zeroes_data
0

\u@HackerPro:\w$ sudo grep -ri fstrim /etc

/etc/e2scrub.conf:# Set this to 1 to enable fstrim for everyone.
/etc/e2scrub.conf:# fstrim=0
/etc/cron.weekly/fstrim:/sbin/fstrim --all || true

\u@HackerPro:\w$ cat /etc/cron.weekly/fstrim
#!/bin/sh
# Trim all mounted filesystems that support it
/sbin/fstrim --all || true

\u@HackerPro:\w$ sudo hdparm -I /dev/sda| grep -i trim
        *    Data Set Management TRIM supported (limit unknown)

\u@HackerPro:\w$
```

Figure 9

TRIM command on Linux (Ubuntu)

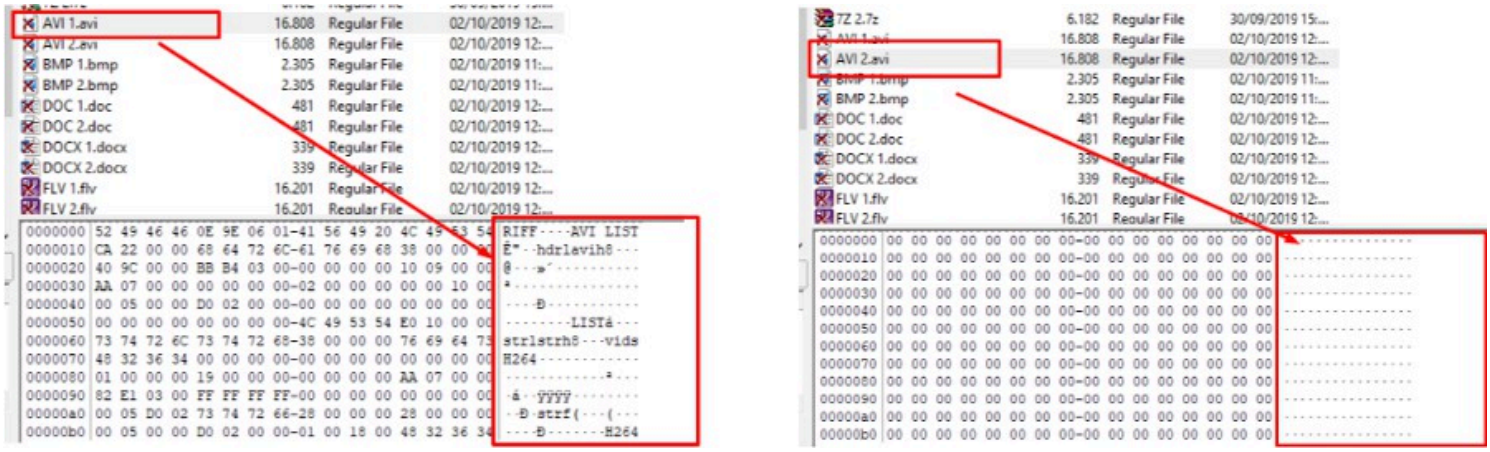


Figure 10

Analysis Stage (a) Odd Label TRIM Disabled, (b) Even Label TRIM Enabled

File Name Recovery Results	MD5 Value	Information
DOCX 1.docx	6db984ae2628503104cb46fab8b9ef8c	Successful recovery
XLSX 1.xlsx	56c424725531715f142e77ccc5cee774	Successful recovery
TXT 1.txt	6bb11f42a5b591be9ec1a0e95a5cd00c	Successful recovery
3GP 1.3gp	cd5f422a723609bff58c699704f91d88	Successful recovery
AVI 1.avi	72562d25302f0698c19040a6d50ceb0c	Successful recovery
GIF 1.gif	ed28cc871584230543b5a2d8a386a2cb	Successful recovery
MP3 1.mp3	d004ad9c716fbb7262d09fcd812b7bdb	Successful recovery
MASTER 1.exe	562f2ea6e41020fd7bf5426bd77cd59c	Successful recovery
ZIP 1.zip	47cf035aa29599823cce99bef2467330	Successful recovery
7Z 1.7z	e2d9c0b0a82113ce52d5334ffd24a876	Successful recovery

Figure 11

List of Analysis and Recovery of Odd Label TRIM Disabled

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- Tables.docx