Digital Forensics In NVMe SSDs with NVMe WriteBlocker

Ashar Neyaz *axn026@shsu.edu*
Department of Computer Science
Sam Houston State University Huntsville,
TX,77340, USA

Narasimha Shashidhar *nks001@shsu.edu*
Department of Computer Science
Sam Houston State University Huntsville,
TX,77340, USA

Cihan Varol *cxv007@shsu.edu*
Department of Computer Science
Sam Houston State University Huntsville,
TX,77340, USA

Amar Rasheed *axr249@shsu.edu*
Department of Computer Science
Sam Houston State University Huntsville,
TX,77340, USA

Abstract

A non-volatile memory express (NVMe) solid-state drive (SSD) is a new computer device introduced in 2013. It is an upgrade from a standard Serial Advanced Technology Attachment (SATA) solid-state drive. Due to the newness of the NVMe SSD technology, there is a shortage of reliable documentation for forensics investigation on this solid-state storage device. Therefore, we conducted an extensive experiment in this study to see how file recovery is affected when files are deleted from NVMe SSDs that are used as primary boot devices. We're focusing on deleted files on NVMe SSDs because data and file recovery on SSDs isn't always guaranteed. In addition, the behavior of SSDs varies depending on the type of flash storage and controller chips. As a result, we copy and remove files using the Windows 10 operating system and execute forensics examinations using AccessData FTK, Autopsy, and WinHex. Finally, we demonstrate the impact of deletion on various regularly used user files and whether they may be successfully restored over time.

Keywords: Non-Volatile Memory Express (NVMe), NVMe WriteBlocker, Flash Chips, Wear-leveling, TRIM, Autopsy, AccessData FTK, GUID Partition Table.

1. INTRODUCTION

A storage device is a vital component that enables a computer system to temporarily or permanently retain and store digital data. These devices are ubiquitous and an essential part of most digital devices since they allow users to store all types of digital information Robert et al. (2021).

Hard drives (HDDs), memory cards, USB flash drives, solid-state drives (SSDs), and non-volatile memory express solid-state drives (NVMe SSDs) are just a few of the computer storage devices currently on the market. HDDs held the most significant market share in storage devices until the late 2000s, but recently, a progressive movement towards SSDs has occurred Mellor (2020). HDDs may soon become obsolete given the exponential expansion of SSD technologies. The switch from HDDs to SSDs in digital devices is primarily due to the storage media's performance, endurance, and dependability, to name a few characteristics. As a result, as compared to an

HDD, an SSD can complete a task ten times faster Riggs et al. (2020). This can be good news for users, but it might not be so good for digital forensics investigators. Since the development of SSD technology, it has become more difficult for cybercrime investigators to conduct their work.

In the case of hard disk drives, in the event of file deletion, most operating systems do not overwrite the blocks on the hard disk where the deleted file was stored. Instead, they only eliminate the file's reference from the directory that contains it Battula et al. (2009). Thus, regarding file recovery on HDDs, we can be confident that the data will be found because it still resides on the device's storage unit. Deleted data is not always guaranteed to be deleted from the hard drive because only the address reference to the stored information is removed after deletion Carrier (2005). As a result, if we conduct a forensic acquisition of an HDD and try to recover data, we'll eventually discover the data as long as it isn't overwritten. However, this is not the case with SSDs. Non-volatile NAND-based flash memory chips are used in manufacturing SSDs to provide enough density, fast access times, and reduced latency for usage as primary storage devices. The controller, which connects the NAND memory components to a host computer, is a crucial part of an SSD. The controller is a processor integrated into the drive and runs firmware-level programming and operations. The controller's primary tasks mainly involve read and write caching, garbage collection and wear-leveling Nisbet et al. (2013b).

SSDs cells wear out, dramatically shortening the drive's lifespan. Blocks on a drive may lose considerable space if they are repeatedly written to and deleted because individual cells may fail and render an entire block of cells useless. In order to tackle this, the controller chip inside the device constantly shifts data across the flash chips to extend the storage device's life. This is known as the concept of wear-leveling, which the controller implements autonomously. It allows for steady data flow to extend the life of an SSD Valette (2016). As a result, SSDs can sometimes destroy data independently, even if they are not linked. SSDs executes wear-leveling by copying data from a heavily used drive block and writing it to an underused block. When the standard "Garbage Collection" is conducted, zeros are written in the old location where the data was relocated from. Although the disk's lifespan is extended, the amount of data that can be recovered from the drive by a forensic investigator is dramatically decreased. To further extend the drive's life, TRIM can be enabled, which compels the operating system to inform the drive that data has been erased from a spot and allows the drive to flag its location as invalid. This happens soon after the data is removed, conserving space on the device and accelerating the garbage collection process.

SSDs' inherent qualities and cutting-edge characteristics make it incredibly simple for criminals to wipe data permanently in a few seconds. The TRIM function and the SSD's background garbage removal make it challenging to recover deleted artifacts. There is no easy way to prevent the SSD from deleting trimmed blocks. Due to the unpredictable results of data recovery, the SSD has increased uncertainty in digital forensics. Some of the operations that present significant challenges for forensics analysts are the garbage collection process and the SSD TRIM functions. As a result, standard recommendations for preserving digital forensic data on solid-state disks are inadequate. Furthermore, if followed, they may result in possible evidence being lost, destroyed, or corrupted and evidence being declared inadmissible in a court of law. Bednar and Katos (2011). Recent advances in SSDs have seen the growth of a new type of SSD called NVMe SSD. NVMe utilizes PCIe paths for faster data transfers hence providing faster data transfer speeds to users. Thus, there is no prior sound digital forensics study in this area because NVMe SSD technology is relatively new. Thus, this research conducts several experiments, followed by critical observations and recommendations for digital forensic analysts. We aim to achieve the following objectives as we carry out the experiments.

- What is the effect of the TRIM enabled and disabled command on NVMe SSD?
- How does time duration and continuous use of the NVMe SSD affect the chances of recovering deleted artifacts?
- How much NVMe SSD evidence is reliable?

2. LITERATURE REVIEW

The literature review in this chapter summarizes the research studies undertaken by most professionals and researchers in solid-state drive forensics. Their research experiments, tools, and methodologies used, as well as their conclusions, are all clearly stated and provide insights into various experimental works.

In a paper on SSD forensics, Gubanov and Afonin (2014) described the self-corrosion phenomenon in flash storage devices. The authors also went into great depth about the TRIM and garbage collection procedures. In order to avoid running the internal Garbage Collection process, they offered a solution of a chip off of the SSD controller in his study paper. In addition to requiring specialized knowledge and equipment, it is ineffective for drives that contain encrypted data. Additionally, they looked into how the TRIM command affected solid-state media. The research was done on how eMMC chips behaved in comparison to SSD. It was determined that SSD forensics continued to differ from traditional hard disks. Data is destroyed after deletion or formatting with independent background garbage collection behavior in all SSDs.

NVMe (non-volatile memory express) is a relatively recent solid-state drive (SSD). As a result, it has received insufficient attention in digital forensics. Conducting forensic examination on storage media is a difficult task in and of itself. Furthermore, due to the frequent flow of data, the issues in NVMeSSDs are significantly larger. However, just a few researchers have attempted to investigate this possibility.

The authors employed the TRIM ON command on various SATA SSDs to compare their reactions in their study Nisbet et al. (2013a). Multiple file systems support the TRIM command. This includes NTFS, EXT4, and HFS+. When TRIM was enabled, the authors discovered that erased data was purged and became unrecoverable in minutes. This was not the case in EXT4, as commands were given in batches and may not have arrived on time.

Furthermore, Neyaz et al. (2019) studied the behavior of wear-leveling on a triple-level cell (TLC) serial ATA (SATA) SSD as the primary storage device using the NTFS file system. The experiment aimed to recover deleted files by comparing them to the initial count from the Digital Corpora file set and then assessing their chances of recovery from all forensic acquisitions after wear-leveling had occurred in both TRIM ON and TRIM OFF scenarios. In the case of TRIM OFF, all files were recovered; however, in the case of TRIM ON, no data traces were detected. On a SATA SSD, microSD card, SD card, and USB flash drive, Neyaz and Shashidhar Neyaz et al. (2018) conducted studies using TRIM ON and OFF instances, respectively.

Researchers in Shah et al. (2015) looked at the forensic possibilities of standard SATA SSDs from various manufacturers to see if data could be recovered after the SSD was deleted. Data can be recovered from an SSD in the same way that data can be retrieved from an HDD if the SSD does not have background trash collection and TRIM has been turned off. According to them, data on the SSD can also be recovered after it has been formatted.

The empirical study in King and Vidas (2011) shows how much data is maintained on fifteen different SATA SSDs. The authors provided a list of drive models and data on how much data could be recovered with and without the TRIM command enabled. According to the authors, data recovery utilizing TRIM- enabled devices was almost impossible for large disks with a data recovery rate of less than 1%. The results for small files, on the other hand, vary depending on the SSD manufacturer. They also observed that they could retrieve virtually all of the data without using TRIM (on Windows XP). This occurred with both large and small files. Furthermore, it was discovered that the TRIM command rendered all data unrecoverable. However, all data was recoverable when TRIM was disabled.

Nikkel (2016) presents an overview of NVMe technology and investigates its application in digital forensics while exploring digital forensic analysis in NVMe SSDs. This article also discusses the new issues

NVMe technology presents to the digital forensics community, including forensics labs, hardware and software providers, and forensics standards bodies (NIST CFTT).

The authors of Vieyra et al. (2018) learned more about what happens in the background of SSDs during operation and investigation, as well as investigated forensic methods for retrieving artifacts from SSDs in various settings, including data volume, powered effect, and so on.

The researchers in Riadi et al. (2020) builds on their previous work Riadi and Hadi (2019) on experimental forensics investigations using standard SATA SSD disks. However, using the NIJ (National Institute of Justice) framework, this expanded study employs a static forensics method (a procedure that must be followed when handling electronic evidence from a powered-off computer system). Furthermore, this study aims to see how well forensics tools like Autopsy and RecoverMyFile can restore digital evidence from NVMe disks.

We undertake a sound forensic investigation on four NVMe SSDs, Samsung, Seagate, Western Digital, and Silicon Power, which were employed as a primary boot device, to address the problem of file recovery in NVMe SSDs. We want to see how many files can be recovered after removing them from these devices. We use NVMe SSDs with the Windows 10 operating system installed for this reason. We used AccessData FTK, Autopsy, and WinHex disk editor to recover the files and do the forensic examination. We also describe our forensic findings based on observations from four distinct manufacturers of SSDs with various controller chips. We anticipate comparable or dissimilar results, which will be discussed more in this study. Despite the present research in this field, no study on the forensics analysis of NVMe SSDs specifically targeting distinct controller chips has been undertaken to the best of our knowledge. The trials in this study fill the gap mentioned by Vieyra et al. (2018), leaving much room for more research into data recovery in NVMe SSDs for critical cases. We show how to recover deleted files from NVMe SSDs using the latest Windows 10 v21H2 operating system in both TRIM ON and TRIM OFF scenarios.

Terminology

All of the terms used in this study are defined in this section. This will assist readers in becoming familiar with the words and comprehensively understanding the subject matter.

1. **SATA Technology:** Serial Advanced Technology Attachment (SATA) is a command and transport protocol that specifies how data is exchanged between a computer motherboard and mass storage devices such as hard disk drives (HDDs), optical drives, and solid-state drives (SSDs). SATA is based on serial signaling technology, which allows data to be sent in a succession of individual bits. SATA refers to the communication protocol and industry standards manufacturers of SATA- compatible connections, connectors, and drives follow Kranz (2021).

2. **Hard-Disk Drive:** A hard-disk drive or HDD is a computer storage device that stores digital media. HDD is an example of non-volatile storage, i.e., it retains data even when the computer is turned off. HDDs have magnetic platters where the data is stored. In the case of HDDs, there is a surety of data recovery as long as it is not overwritten Gillis (2021). The fundamental unit of data storage in HDDs is a sector. The combination of sectors is called clusters.

3. **Solid-State Drive:** A solid-state drive or SSD is a non-volatile computer storage device for storing digital content. It is the counterpart of HDD. Instead of using mechanical moving parts to store data, SSDs use flash chips to achieve this task. Regarding SSDs, data recovery is a challenging task with no surety whatsoever because the controller chip autonomously wipes the deleted data to increase the lifespan of the drives. The fundamental data storage unit in regular SSDs and NVMe SSDs is page. The combination of pages is called blocks Bahgat (2021).

4. **Non-Volatile Memory Express Solid-State Drive:** An NVMe SSD is a newer and faster

SSD. Like regular SSD, it stores data on flash chips. Moreover, it also has a controller chip responsible for the autonomous behavior of the device. Recovering deleted data is a challenge in these devices too. NVMe SSDs have controller chips made by different makers, making it difficult to predict their behavior in data recovery Kingston Technology (2017).

5. **Wear-leveling:** Wear-leveling is a technique SSD controllers use to extend the device's flash memory lifespan. The concept is straightforward: evenly distribute writing on all blocks of an SSD, so they wear evenly. Solid State Drives (SSDs), SATA SSDs, and NVMe SSDs have flash memory that allows only a limited number of reading and writing operations. This is done to ensure data distribution evenly among all memory cells (the basic unit of data storage in SSDs) to avoid degradation of the SSD Valette (2016).

6. **TRIM:** TRIM is a command that tells an operating system which data blocks on a solid-state drive (SSD) can be erased when no longer needed. TRIM can help SSDs last longer by improving their performance when writing data Silwa (2018).

7. **Triple-Level Cell (TLC):** TLC SSDs write three bits to each cell and are the most common form of SSD. They compress more capacity into a smaller container than SLC and MLC drives, but at the cost of speed, reliability, and durability Paul (2019).

3. EXPERIMENTAL STUDY

This section goes through the equipment used in the experiment, including the four NVMe SSDs. Then, in the methodology section, we have outlined the steps involved in our experiment.

Experimental Setup

Table 1 below enumerates the technical specifications of the equipment used for the experiment in this chapter. Moreover, we have used Wiebetech NVMe WriteBlocker for conducting a series of comprehensive experiments. Figures 1, 2, 3, and 4 show the NVMe SSDs attached to the NVMe WriteBlocker.

Tools	**Name**
NVMe SSD 1	Samsung V-NAND SSD 970 Evo Plus
NVMe SSD 2	Seagate Barracuda 510 250GB NVMe SSD
NVMe SSD 3	Western Digital SN550 250GB NVMe SSD
NVMe SSD 4	Silicon Power 3D-NAND NVMe SSD
Operating System	Windows 10 Pro v21H2
Forensic Analysis Tool	AccessData FTK 7.5, Autopsy and WinHex
Forensics Acquisition Tool	AccessData FTK Imager 4.7
WriteBlocker	Wiebetech NVMe WriteBlocker
Workstation	CPU: Intel Xeon W-2123 — RAM : 80GB

TABLE 1: Equipment used in the experiment with NVMe WriteBlocker.

FIGURE 1: Samsung NVMe SSD attached with NVMe WriteBlocker.

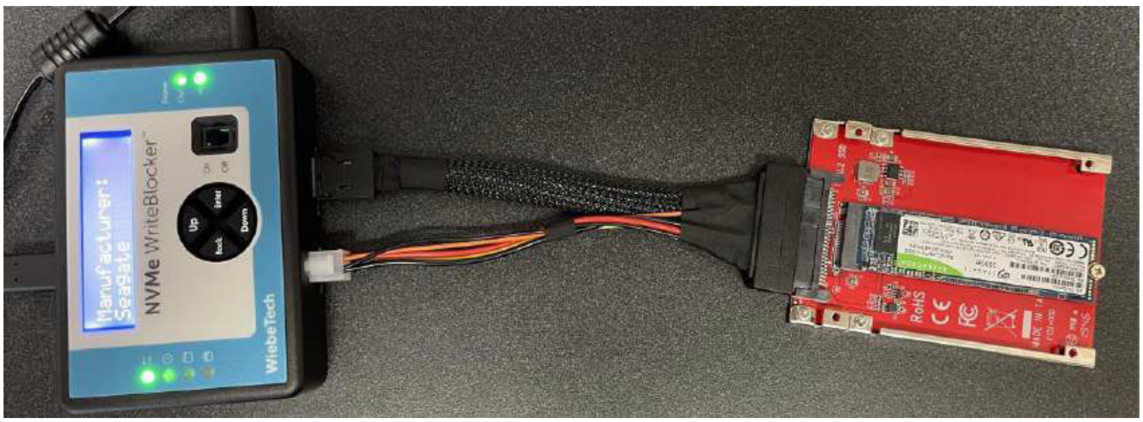

FIGURE 2: Seagate NVMe SSD attached with NVMe WriteBlocker.

FIGURE 3: Western Digital NVMe SSD attached with NVMe WriteBlocker.

FIGURE 4: Silicon Power NVMe SSD attached with NVMe WriteBlocker.

Specifications of NVMe SSDs

The experiment in this research included four NVMe SSD brands, including Samsung, Seagate, Western Digital (WD), and Silicon Power (SP). We chose these drives due to their dense popularity, market share, and dependability. Because the parameters of the SSDs used in the experiment closely mimic those of a standard SSD that a regular user may own, the four manufacturers and models utilized in the investigation were chosen to reflect a real-world scenario. Furthermore, the experiment is more relevant to the digital forensic community because these are the most frequent properties of SSDs found in laptops and desktop computers. Tables 2 and 3 detail the name, model, product number (P/N), storage capacity, number of flash chips, kind of NVMe flash chip, and controller information for NVMe SSDs.

SSD Information	**Samsung NVMe Specification 1.3**
Name	Samsung NVMe V-NAND SSD970 Evo Plus
Model	MZ-V7S250
Product Number	MZVLB250HBHQ
Storage Capacity	250 GB
Number of flash chipsinside	2
Type of NVMe NAND Flash	3D TLC NAND
Controller Information	*Samsung S4LR020 — 2117 ARM — Pheonix*
SSD Information	**Seagate NVMe Specification 1.3**
Name	Seagate Barracuda 510 250GB NVMe SSD
Model	ZP250CM30001
Product Number	2NS312-300
Storage Capacity	250 GB
Number of flash chipsinside	4
Type of NVMe NAND Flash	3D TLC NAND
Controller Information	*SKHynix - H5AN4G6NBJR*

TABLE 2: Information on Samsung and Seagate NVMe SSDs used in the experiment.

SSD Information	**Western Digital NVMe Specification 1.4**
Name	Western Digital SN550250GB NVMe SSD
Model	WDS250G2B0C-00PXH0/21146P801302
Product Number	87161901478830731375399388282263
Storage Capacity	250 GB
Number of flash chipsinside	4
Type of NVMe NAND Flash	3D TLC NAND
Controller Information	*Sandisk 20-82-10023-A1 — 1015ZKLY0KN*
SSD Information	**Silicon Power NVMe Specification 1.3**
Name	Silicon Power 3D-NANDNVMe SSD
Model	A-60
Product Number	SP256GBP34A60M28
Storage Capacity	256 GB
Number of flash chipsinside	2
Type of NVMe NAND Flash	3D TLC NAND
Controller Information	*Phison PS5013-31-C02102E-TB5V79-001BB*

TABLE 3: Information on Western Digital and Silicon Power NVMe SSDs used in the experiment.

Methodology and Experiment Initiation

The methodology and configuration setup assigned during the experiment are listed and explained in this section.

1. The partition scheme used for the NVMe SSDs: **GPT (GUID Partition Table)**
2. The number of partitions in each NVMe SSD: **1**
3. The file system of the partition: **NTFS**
4. Before copying the files to the primary boot devices from Digital Corpora [22], we checked the **TRIM** status in Windows 10 by issuing the following command through the Windows command prompt (CMD).

fsutil behavior query DisableDeleteNotify
**If the output is 1, then TRIM is disabled. If the output is 0, then TRIM is enabled.*
To enable TRIM: fsutil behavior set DisableDeleteNotify 0
To disable TRIM: fsutil behavior set DisableDeleteNotify 1

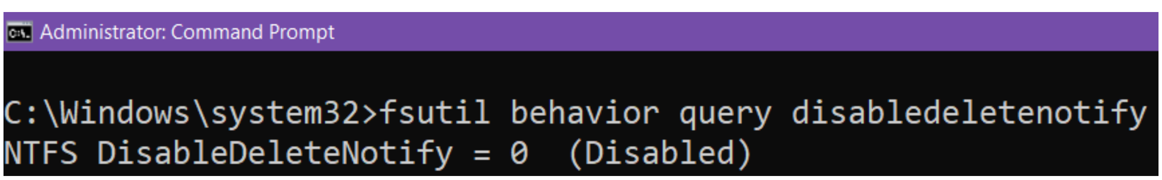

FIGURE 5: The status of TRIM in Windows 10 using the fsutil command issued from CMD.

Case scenario: TRIM ON from Windows 10 operating system with NVMe WriteBlocker

1. We copied the commonly used file types having 160GB of total size from the Digital Corpora dataset Garfinkel et al. (2009) to the four NVMe SSDs.
2. We then kept the system powered on for one day with no user activity.
3. Next, we deleted (shift+delete) the files from the devices and waited for one day before acquiring four forensic images of the four NVMe SSDs, respectively.
   a. We took four forensic images: three consecutive images with one day gap and the last image after a span of four days from the third acquisition.

4. We analyzed the images in AccessData FTK and Autopsy for the NVMe storage devices.
5. We performed file recovery of the deleted files from the forensics images in the TRIM ON case.
6. Based on our results from the file recovery and WinHex analysis we documented the effects of wear-leveling.

Case scenario: TRIM OFF from Windows 10 operating system with NVMe WriteBlocker

1. First and foremost, we disabled TRIM using Windows 10 command prompt (CMD) before copying the files.
2. We copied the commonly used file types having 160GB of total size from the Digital Corpora dataset Garfinkel et al. (2009) to the four NVMe SSDs.
3. We then kept the system powered on for one day with no user activity.
4. Next, we deleted (shift+delete) the files from the devices and waited for one day before acquiring four forensic images of the four NVMe SSDs, respectively.
    a. We took four forensic images: three consecutive images with one day gap and the last image after a span of four days from the third acquisition.
5. We analyzed the images in AccessData FTK and Autopsy for the NVMe storage devices.
6. We performed file recovery of the deleted files from the forensics images in the TRIM OFF case.
7. Like the TRIM ON case, based on our results from the file recovery and WinHex analysis, we documented the effects of wear-leveling.

4. EXPERIMENTAL RESULTS AND ANALYSIS

The results of the file recovery utilizing the AccessData FTK and Autopsy tools are presented in this section. We began by populating the NVMe SSDs with the most frequently used files from the Digital Corpora dataset Garfinkel et al. (2009). We then used the forensics images of the four NVMe SSDs using the NVMe WriteBlocker to undertake a file recovery operation. Tables 4 and 5 present the timeline information of forensic image acquisition in both TRIM ON and TRIM OFF scenarios of Samsung, Seagate, Western Digital (WD), and Silicon Power (SP) NVMe SSDs.

TRIM ON information with NVMe WriteBlocker			
Samsung NVMe	**Time**	**Seagate NVMe**	**Time**
Copy file date	11:49 pm 2/11/22	Copy file date	5:30 pm 2/20/22
Wait for 24 hrs	Waited	Wait for 24 hrs	Waited
Delete files	11:49 pm 2/12/22	Delete files	5:30 pm 2/21/22
Wait for 24 hrs	Waited	Wait for 24 hrs	Waited
1st image	11:49 pm 2/13/22	1st image	5:30 pm 2/22/22
2nd image	11:49 pm 2/14/22	2nd image	5:30 pm 2/23/22
3rd image	11:49 pm 2/15/22	3rd image	5:30 pm 2/24/22
4th image	11:49 pm 2/19/22	4th image	5:30 pm 2/28/22
TRIM OFF information with NVMe WriteBlocker			
Samsung NVMe	**Time**	**Seagate NVMe**	**Time**
Copy file date	11:09 pm 2/28/22	Copy file date	10:23 pm 3/1/22
Wait for 24 hrs	Waited	Wait for 24 hrs	Waited
Delete files	11:09 pm 3/1/22	Delete files	10:23 pm 3/2/22
Wait for 24 hrs	Waited	Wait for 24 hrs	Waited
1st image	11:09 pm 3/2/22	1st image	10:23 pm 3/3/22
2nd image	11:09 pm 3/3/22	2nd image	10:23 pm 3/4/22
3rd image	11:09 pm 3/4/22	3rd image	10:23 pm 3/5/22
4th image	11:09 pm 3/8/22	4th image	10:23 pm 3/9/22

TABLE 4: Timeline information of forensic file acquisition with NVMe WriteBlocker.

TRIM ON information with NVMe WriteBlocker			
Western Digital NVMe	**Time**	**SP NVMe**	**Time**
Copy file date	9:27 pm 2/22/22	Copy file date	1:18 pm 2/25/22
Wait for 24 hrs	Waited	Wait for 24 hrs	Waited
Delete files	9:27 pm 2/23/22	Delete files	1:18 pm 2/26/22
Wait for 24 hrs	Waited	Wait for 24 hrs	Waited
1st image	9:27 pm 2/24/22	1st image	1:18 pm 2/27/22
2nd image	9:27 pm 2/25/22	2nd image	1:18 pm 2/28/22
3rd image	9:27 pm 2/26/22	3rd image	1:18 pm 3/1/22
4th image	9:27 pm 3/2/22	4th image	1:18 pm 3/5/22
TRIM OFF information with NVMe WriteBlocker			
Western Digital NVMe	**Time**	**SP NVMe**	**Time**
Copy file date	8:43 pm 3/2/22	Copy file date	9:59 pm 3/4/22
Wait for 24 hrs	Waited	Wait for 24 hrs	Waited
Delete files	8:43 pm 3/3/22	Delete files	9:59 pm 3/5/22
Wait for 24 hrs	Waited	Wait for 24 hrs	Waited
1st image	8:43 pm 3/4/22	1st image	9:59 pm 3/6/22
2nd image	8:43 pm 3/5/22	2nd image	9:59 pm 3/7/22
3rd image	8:43 pm 3/6/22	3rd image	9:59 pm 3/8/22
4th image	8:43 pm 3/10/22	4th image	9:59 pm 3/12/22

TABLE 5: Timeline information of forensic file acquisition with NVMe WriteBlocker.

Samsung and Seagate TRIM ON analysis with NVMe WriteBlocker

The TRIM ON analysis of Samsung NVMe SSD with NVMe WriteBlocker (WB) shows that most files become unrecoverable even after one day of deletion. Our previous research showed that, in the case of Samsung NVMe SSD used under a USB enclosure, files having file size under 693 bytes stay intact even though they were deleted in the TRIM ON case scenario. However, this is not the case for Samsung NVMe SSDs used as primary boot devices. Recovery with AccessData FTK and Autopsy show similar results. Tables 6 and 7 give the recovery statistics from AccessData FTK and Autopsy of the different files from Samsung NVMe SSD in the TRIM ON case. Surprisingly, all the files were irrecoverable in the TRIM ON case of Seagate NVMe SSD. This is because the Seagate controller chip acted instantly after the files were deleted from the device. The recovery operation from AccessData FTK and Autopsy showed the same results, i.e., there was no recovery possible in the case of Seagate. Tables 8 and 9 give the recovery statistics from AccessData FTK and Autopsy of the different files from Seagate NVMe SSD in the TRIM ON case.

TRIM ON: Samsung FTK Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	0	0	0	0
.vhd	1	0	0	0	0
.ps2	2	0	0	0	0
.aff	16	0	0	0	0
.csv	3184	0	0	0	0
.dbase	480	0	0	0	0
.dmg	32	0	0	0	0
.doc	14592	0	0	0	0
.docx	112	0	0	0	0
.dwf	16	0	0	0	0
.e01	352	0	0	0	0
.eps	640	0	0	0	0
.f	160	0	0	0	0

.fits	16	0	0	0	0
.flv	48	0	0	0	0
.fm	16	0	0	0	0
.gif	5952	0	0	0	0
.gls	32	0	0	0	0
.gz	2176	0	0	0	0
.hlp	112	0	0	0	0
.java	80	0	0	0	0
.jpg	19184	16792*	16792*	16792*	16792*
.key	16	16*	16*	16*	16*
.kml	192	189*	189*	189*	189*
.kmz	320	317*	317*	317*	317*
.log	1680	974*	974*	974*	974*
.mp4	64	30*	30*	30*	30*
.numbers	16	10*	10*	10*	10*
.odt	16	16*	16*	16*	16*
.pages	16	16*	16*	16*	16*
.pcap	32	1*	1*	1*	1*
.pdf	41344	40630*	40630*	40630*	40630*
.png	640	640*	640*	640*	640*
.pps	176	176*	176*	176*	176*
.ppt	9408	9406*	9406*	9406*	9406*
.pptx	16	16*	16*	16*	16*
.xls	10352	10004*	10004*	10004*	10004*
.xlsx	32	32*	32*	32*	32*
*: All files recovered but corrupted.					

TABLE 6: The number of files recovered using AccessData FTK in Samsung NVMe SSD as a primary boot device in Windows 10 TRIM ON case.

TRIM ON: Samsung Autopsy Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	0	0	0	0
.vhd	1	0	0	0	0
.ps2	2	0	0	0	0
.aff	16	0	0	0	0
.csv	3184	0	0	0	0
.dbase	480	0	0	0	0
.dmg	32	0	0	0	0
.doc	14592	0	0	0	0
.docx	112	0	0	0	0
.dwf	16	0	0	0	0
.e01	352	0	0	0	0
.eps	640	0	0	0	0
.f	160	0	0	0	0
.fits	16	0	0	0	0
.flv	48	0	0	0	0
.fm	16	0	0	0	0
.gif	5952	0	0	0	0
.gls	32	0	0	0	0
.gz	2176	0	0	0	0

.hlp	112	0	0	0	0
.java	80	0	0	0	0
.jpg	19184	0	0	0	0
.key	16	16*	16*	16*	16*
.kml	192	64	64	64	64
.kmz	320	317*	317*	317*	317*
.log	1680	19	19	19	19
.mp4	64	0	0	0	0
.numbers	16	0	0	0	0
.odt	16	0	0	0	0
.pages	16	0	0	0	0
.pcap	32	0	0	0	0
.pdf	41344	0	0	0	0
.png	640	0	0	0	0
.pps	176	0	0	0	0
.ppt	9408	0	0	0	0
.pptx	16	0	0	0	0
.xls	10352	0	0	0	0
.xlsx	32	0	0	0	0
*: All files recovered but corrupted.					

TABLE 7: The number of files recovered using Autopsy in Samsung NVMe SSD as a primary boot device in Windows 10 TRIM ON case.

TRIM ON: Seagate FTK Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	0	0	0	0
.vhd	1	0	0	0	0
.ps2	2	0	0	0	0
.aff	16	0	0	0	0
.csv	3184	0	0	0	0
.dbase	480	0	0	0	0
.dmg	32	0	0	0	0
.doc	14592	0	0	0	0
.docx	112	0	0	0	0
.dwf	16	0	0	0	0
.e01	352	0	0	0	0
.eps	640	0	0	0	0
.f	160	0	0	0	0
.fits	16	0	0	0	0
.flv	48	0	0	0	0
.fm	16	0	0	0	0
.gif	5952	0	0	0	0
.gls	32	0	0	0	0
.gz	2176	0	0	0	0
.hlp	112	0	0	0	0
.java	80	0	0	0	0
.jpg	19184	0	0	0	0
.key	16	0	0	0	0
.kml	192	0	0	0	0
.kmz	320	0	0	0	0

.log	1680	0	0	0	0
.mp4	64	0	0	0	0
.numbers	16	0	0	0	0
.odt	16	0	0	0	0
.pages	16	0	0	0	0
.pcap	32	0	0	0	0
.pdf	41344	0	0	0	0
.png	640	0	0	0	0
.pps	176	0	0	0	0
.ppt	9408	0	0	0	0
.pptx	16	0	0	0	0
.xls	10352	0	0	0	0
.xlsx	32	0	0	0	0
None of the files were recovered from AccessData FTK.					

TABLE 8: The number of files recovered using AccessData FTK in Seagate NVMe SSD as a primary boot device in Windows 10 TRIM ON case.

TRIM ON: Seagate Autopsy Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	0	0	0	0
.vhd	1	0	0	0	0
.ps2	2	0	0	0	0
.aff	16	0	0	0	0
.csv	3184	0	0	0	0
.dbase	480	0	0	0	0
.dmg	32	0	0	0	0
.doc	14592	0	0	0	0
.docx	112	0	0	0	0
.dwf	16	0	0	0	0
.e01	352	0	0	0	0
.eps	640	0	0	0	0
.f	160	0	0	0	0
.fits	16	0	0	0	0
.flv	48	0	0	0	0
.fm	16	0	0	0	0
.gif	5952	0	0	0	0
.gls	32	0	0	0	0
.gz	2176	0	0	0	0
.hlp	112	0	0	0	0
.java	80	0	0	0	0
.jpg	19184	0	0	0	0
.key	16	0	0	0	0
.kml	192	0	0	0	0
.kmz	320	0	0	0	0
.log	1680	0	0	0	0
.mp4	64	0	0	0	0
.numbers	16	0	0	0	0
.odt	16	0	0	0	0
.pages	16	0	0	0	0
.pcap	32	0	0	0	0

.pdf	41344	0	0	0	0
.png	640	0	0	0	0
.pps	176	0	0	0	0
.ppt	9408	0	0	0	0
.pptx	16	0	0	0	0
.xls	10352	0	0	0	0
.xlsx	32	0	0	0	0
None of the files were recovered from Autopsy.					

TABLE 9: The number of files recovered using Autopsy in Seagate NVMe SSD as a primary boot device in Windows 10 TRIM ON case.

Samsung and Seagate TRIM OFF analysis with NVMe WriteBlocker

In the TRIM OFF case of Samsung NVMe SSD as a primary boot device, there was a promising sign of file recovery from AccessData FTK. All the files were recovered successfully except .bin, .vhd, .ps2, .aff, and .csv files. However, in the case of .doc, .flv, .numbers, .odt, .pcap, .pdf, .png, .ppt remainder of the files from the original count were corrupted or zeroed out. Unfortunately, Autopsy could not recover any files even from the TRIM OFF case as no recovery was possible. Tables 10 and 11 show the statistics of recovery in Samsung NVMe SSD from AccessDATA FTK and Autopsy.

Furthermore, tables 12 and 13 show the statistics of file recovery from AccessData FTK and Autopsy in Seagate NVMe SSD with NVMe WriteBlocker. The following notable trend was seen from the Access- Data FTK recovery process for the files below (refer to table 12 for statistics):

- **.csv:** Recovered all 3184 files, but file size greater than 391 bytes had content zeroed out.
- **.dbase3:** Recovered all 480 files, but file size greater than 418 bytes had content zeroed out.
- **.gif:** Recovered all 5952 files, but 92 files were zeroed out.
- **.jpg:** Recovered all 19184 files, but 114 files were zeroed out.
- **.png:** Recovered all 626 files, but 14 files were zeroed out.

Controller chips of both Samsung and Seagate NVMe SSD restricted their operation when TRIM was disabled, as observed in our experiment. A similar behavior gave us a surety of finding data with success. However, this trend is not valid for all types of files, as the tables 10, 11, 12 and 13 below demonstrate.

TRIM OFF: Samsung FTK Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	0	0	0	0
.vhd	1	0	0	0	0
.ps2	2	0	0	0	0
.aff	16	0	0	0	0
.csv	3184	0	0	0	0
.dbase	480	480	480	480	480
.dmg	32	32	32	32	32
.doc	14592	14590*	14590*	14590*	14590*
.docx	112	112	112	112	112
.dwf	16	16	16	16	16
.e01	352	352	352	352	352
.eps	640	640	640	640	640
.f	160	160	160	160	160
.fits	16	16	16	16	16
.flv	48	47*	47*	47*	47*
.fm	16	16	16	16	16

.gif	5952	5952	5952	5952	5952
.gls	32	32	32	32	32
.gz	2176	2176	2176	2176	2176
.hlp	112	112	112	112	112
.java	80	80	80	80	80
.jpg	19184	19184	19184	19184	19184
.key	16	16	16	16	16
.kml	192	192	192	192	192
.kmz	320	320	320	320	320
.log	1680	1680	1680	1680	1680
.mp4	64	64	64	64	64
.numbers	16	8*	8*	8*	8*
.odt	16	13*	13*	13*	13*
.pages	16	16	16	16	16
.pcap	32	26*	26*	26*	26*
.pdf	41344	41338*	41338*	41338*	41338*
.png	640	626*	626*	626*	626*
.pps	176	176	176	176	176
.ppt	9408	9335*	9335*	9335*	9335*
.pptx	16	16	16	16	16
.xls	10352	10327	10327	10327	10327
.xlsx	32	32	32	32	32
*: Remainder of the files got recovered but were corrupted/zeroed out.					

TABLE 10: The number of files recovered using AccessData FTK in Samsung NVMe SSD as a primary boot device in Windows 10 TRIM OFF case.

TRIM OFF: Samsung Autopsy Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	0	0	0	0
.vhd	1	0	0	0	0
.ps2	2	0	0	0	0
.aff	16	0	0	0	0
.csv	3184	0	0	0	0
.dbase	480	0	0	0	0
.dmg	32	0	0	0	0
.doc	14592	0	0	0	0
.docx	112	0	0	0	0
.dwf	16	0	0	0	0
.e01	352	0	0	0	0
.eps	640	0	0	0	0
.f	160	0	0	0	0
.fits	16	0	0	0	0
.flv	48	0	0	0	0
.fm	16	0	0	0	0
.gif	5952	0	0	0	0
.gls	32	0	0	0	0
.gz	2176	0	0	0	0
.hlp	112	0	0	0	0
.java	80	0	0	0	0
.jpg	19184	0	0	0	0
.key	16	0	0	0	0

.kml	192	0	0	0	0
.kmz	320	0	0	0	0
.log	1680	0	0	0	0
.mp4	64	0	0	0	0
.numbers	16	0	0	0	0
.odt	16	0	0	0	0
.pages	16	0	0	0	0
.pcap	32	0	0	0	0
.pdf	41344	0	0	0	0
.png	640	0	0	0	0
.pps	176	0	0	0	0
.ppt	9408	0	0	0	0
.pptx	16	0	0	0	0
.xls	10352	0	0	0	0
.xlsx	32	0	0	0	0
None of the files were recovered from Autopsy.					

TABLE 11: The number of files recovered using Autopsy in Samsung NVMe SSD as a primary boot device in Windows 10 TRIM OFF case.

TRIM OFF: Seagate FTK Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	1*	1*	1*	1*
.vhd	1	1	1	1	1
.ps2	2	2	2	2	2
.aff	16	16	16	16	16
.csv	3184	3184	3184	3184	3184
.dbase	480	480	480	480	480
.dmg	32	32	32	32	32
.doc	14592	14592	14592	14592	14592
.docx	112	112	112	112	112
.dwf	16	16	16	16	16
.e01	352	352	352	352	352
.eps	640	640*	640*	640*	640*
.f	160	160	160	160	160
.file	32	32	32	32	32
.fits	16	16	16	16	16
.flv	48	48	48	48	48
.fm	16	16	16	16	16
.gif	5952	5860	5860	5860	5860
.gls	32	32	32	32	32
.gz	2176	2176	2176	2176	2176
.hlp	112	112	112	112	112
.java	80	80	80	80	80
.jpg	19184	19070	19070	19070	19070
.key	16	16	16	16	16
.kml	192	192	192	192	192
.kmz	320	320	320	320	320
.log	1680	1680	1680	1680	1680
.mp4	64	64	64	64	64
.numbers	16	16	16	16	16
.odt	16	16	16	16	16

.pages	16	16	16	16	16
.pcap	32	32	32	32	32
.pdf	41344	41344	41344	41344	41344
.png	640	626	626	626	626
.pps	176	176	176	176	176
.ppt	9408	9408*	9408*	9408*	9408*
.pptx	16	16	16	16	16
.xls	10352	10352*	10352*	10352*	10352*
.xlsx	32	32*	32*	32*	32*
* : Recovered all but the hash of some files were different with wiped out contents.					

TABLE 12: The number of files recovered using AccessData FTK in Seagate NVMe SSD as a primary boot device in Windows 10 TRIM OFF case.

TRIM OFF: Seagate Autopsy Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	0	0	0	0
.vhd	1	1	1	1	1
.ps2	2	1	1	1	1
.aff	16	16*	16*	16*	16*
.csv	3184	3181*	3181*	3181*	3181*
.dbase	480	480*	480*	480*	480*
.dmg	32	32*	32*	32*	32*
.doc	14592	14591*	14591*	14591*	14591*
.docx	112	112*	112*	112*	112*
.dwf	16	16	16	16	16
.e01	352	347	347	347	347
.eps	640	640*	640*	640*	640*
.f	160	160*	160*	160*	160*
.file	32	32	32	32	32
.fits	16	16	16	16	16
.flv	48	48	48	48	48
.fm	16	16	16	16	16
.gif	5952	5871	5871	5871	5871
.gls	32	32	32	32	32
.gz	2176	2176	2176	2176	2176
.hlp	112	112	112	112	112
.java	80	80	80	80	80
.jpg	19184	19183	19183	19183	19183
.key	16	16	16	16	16
.kml	192	192	192	192	192
.kmz	320	320	320	320	320
.log	1680	1680	1680	1680	1680
.mp4	64	64	64	64	64
.numbers	16	16	16	16	16
.odt	16	16	16	16	16
.pages	16	16	16	16	16
.pcap	32	32	32	32	32
.pdf	41344	41344	41344	41344	41344
.png	640	627	627	627	627
.pps	176	176	176	176	176
.ppt	9408	9408	9408	9408	9408

.pptx	16	16	16	16	16
.xls	10352	10348*	10348*	10348*	10348*
.xlsx	32	32*	32*	32*	32*
* : Recovered all but the hash of some files were different with wiped out contents.					

TABLE 13: The number of files recovered using Autopsy in Seagate NVMe SSD as a primary boot device in Windows 10 TRIM OFF case.

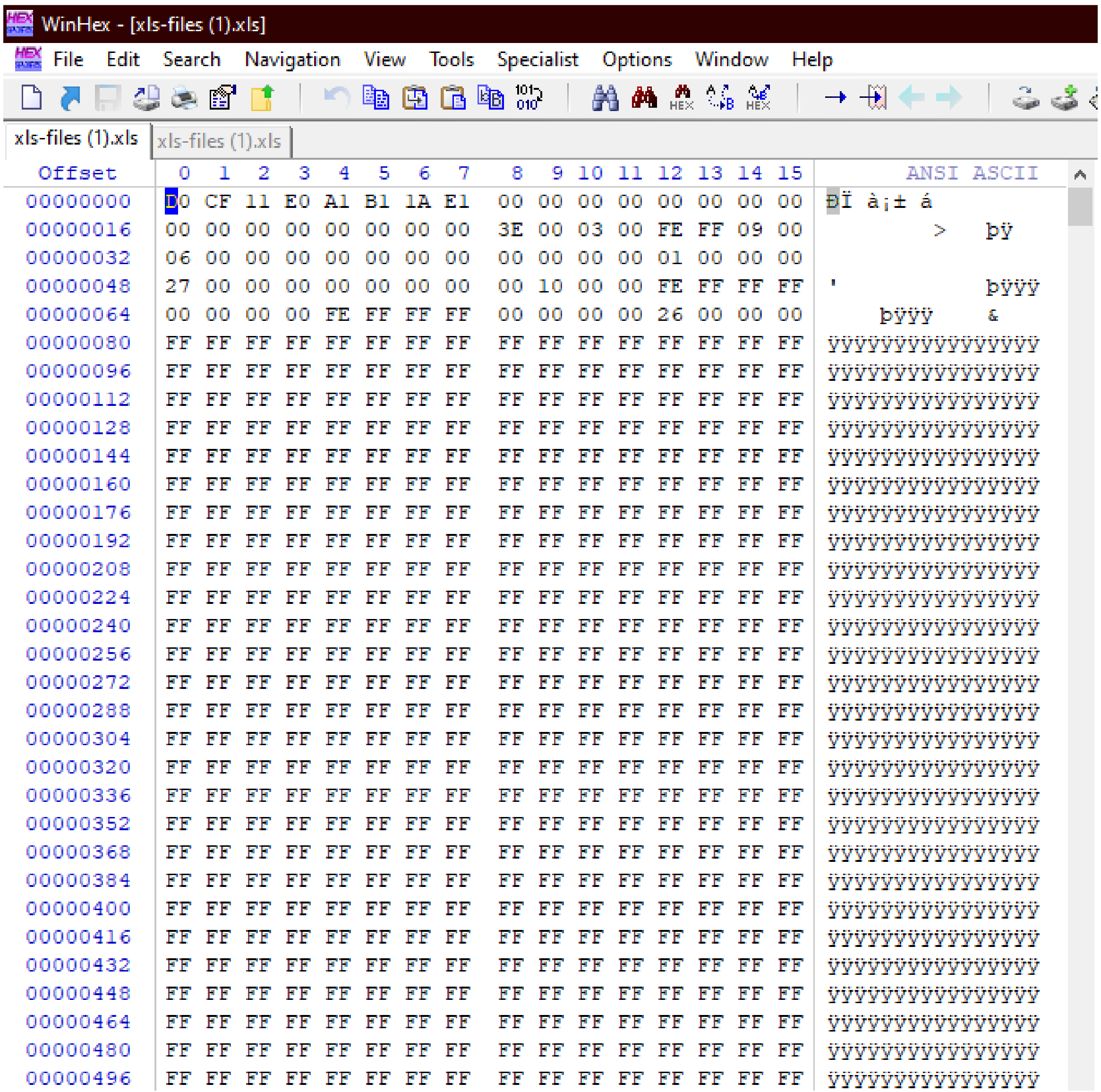

FIGURE 6: Hexadecimal contents of xls-files(1).xls file in the original dataset from Samsung NVMe SSD.

Figure 6 shows a snippet of the original xls-files(1).xls file regarding the Samsung NVMe SSD TRIM ON case in the original dataset. The hexadecimal contents are shown along with ASCII values when a file is opened in WinHex. In this case, the file's original contents are shown in the figure.

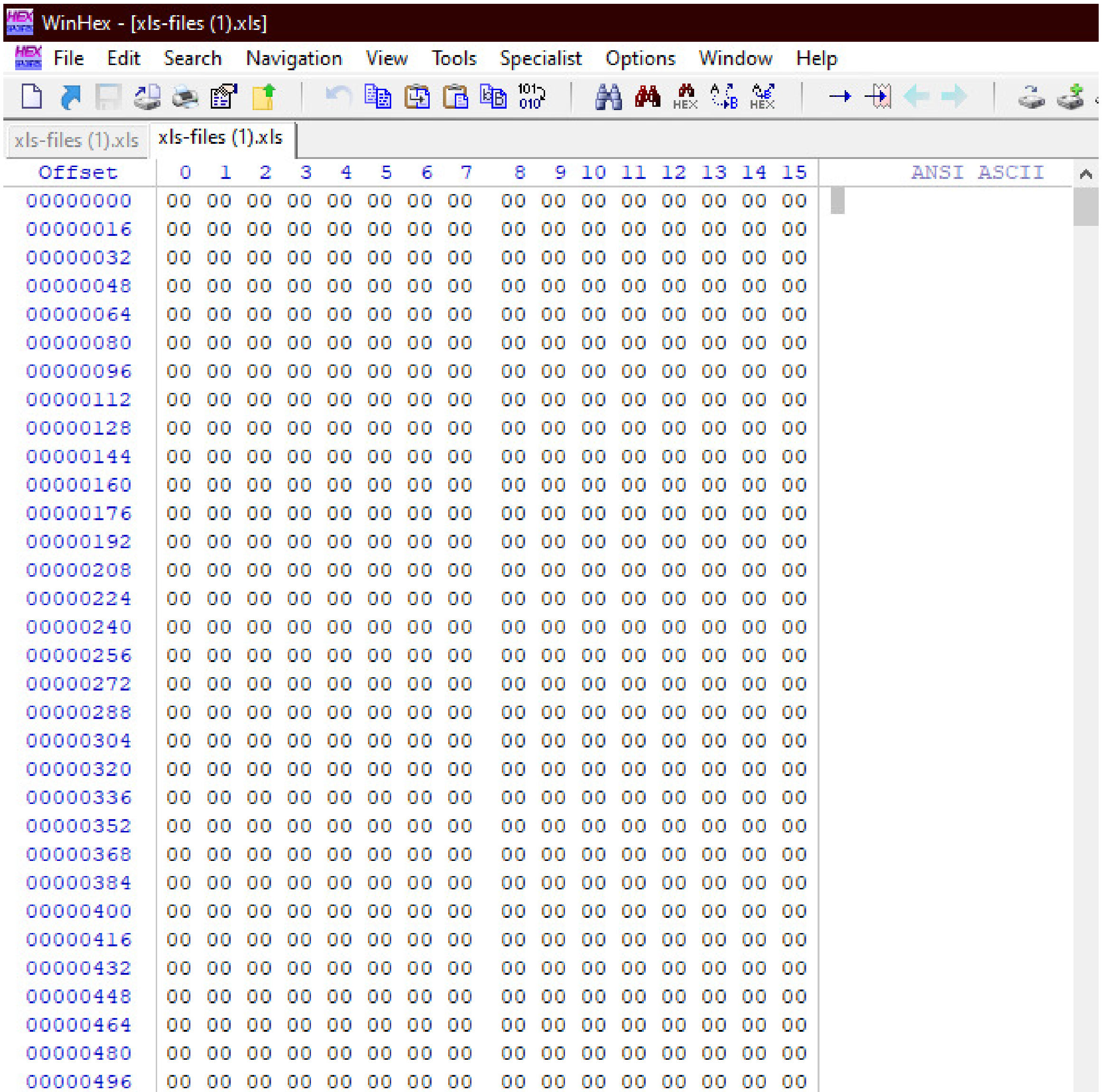

FIGURE 7: Hexadecimal contents of xls-files(1).xls file after recovery from Samsung NVMe SSD TRIM ON case.

Figure 7 shows a snippet of the xls-files(1).xls file after recovery from Samsung NVMe SSD in the TRIM ON case. In this case, the file contents are wiped out for the file, as shown by zeroes in the figure.

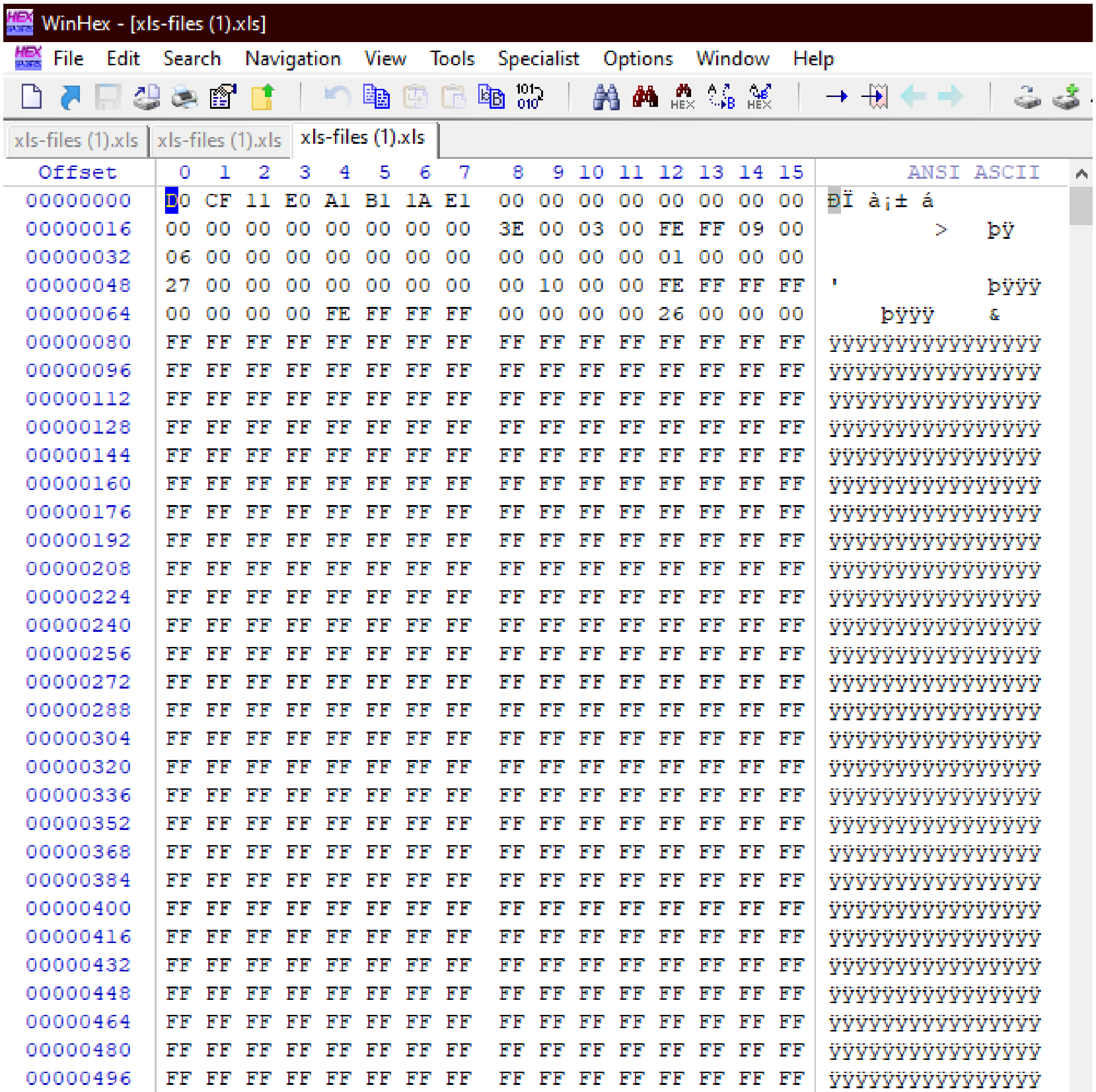

FIGURE 8: Hexadecimal contents of xls-files(1).xls file after recovery from Samsung NVMe SSD TRIM OFF case.

Figure 8 shows a snippet of the xls-files(1).xls file after recovery from Samsung NVMe SSD in the TRIM OFF case. In this case, the file contents are not wiped out as shown in the figure.

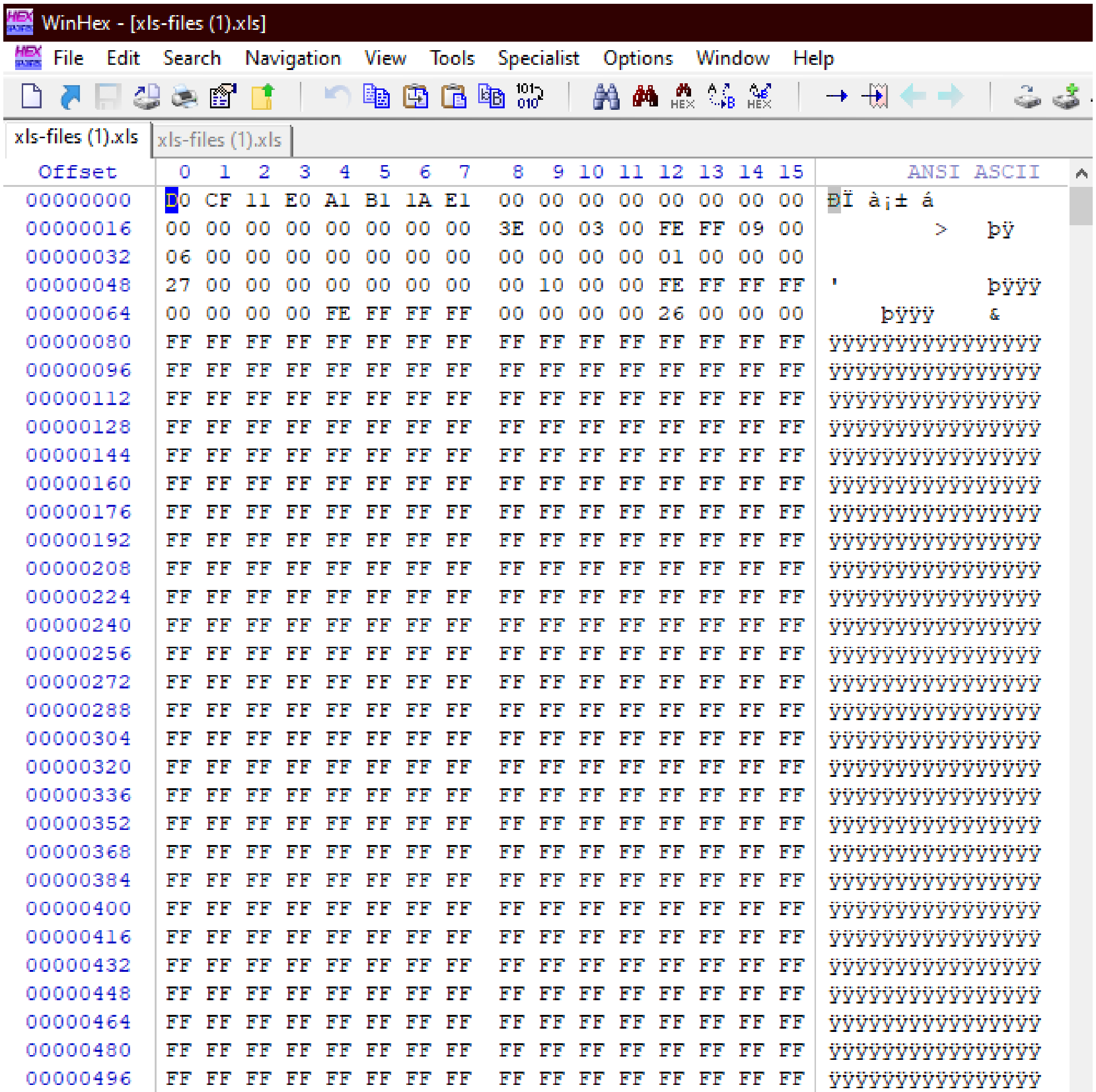

FIGURE 9: Hexadecimal contents of xls-files(1).xls file in the original dataset from Seagate NVMe SSD.

Figure 9 shows a snippet of the original xls-files(1).xls file regarding the Seagate NVMe SSD TRIM ON case in the original dataset. In this case, the file's original contents are shown in the figure. Since there was no recovery of xls-files(1).xls from Seagate NVMe SSD, we could not show the hexadecimal contents of the recovered file.

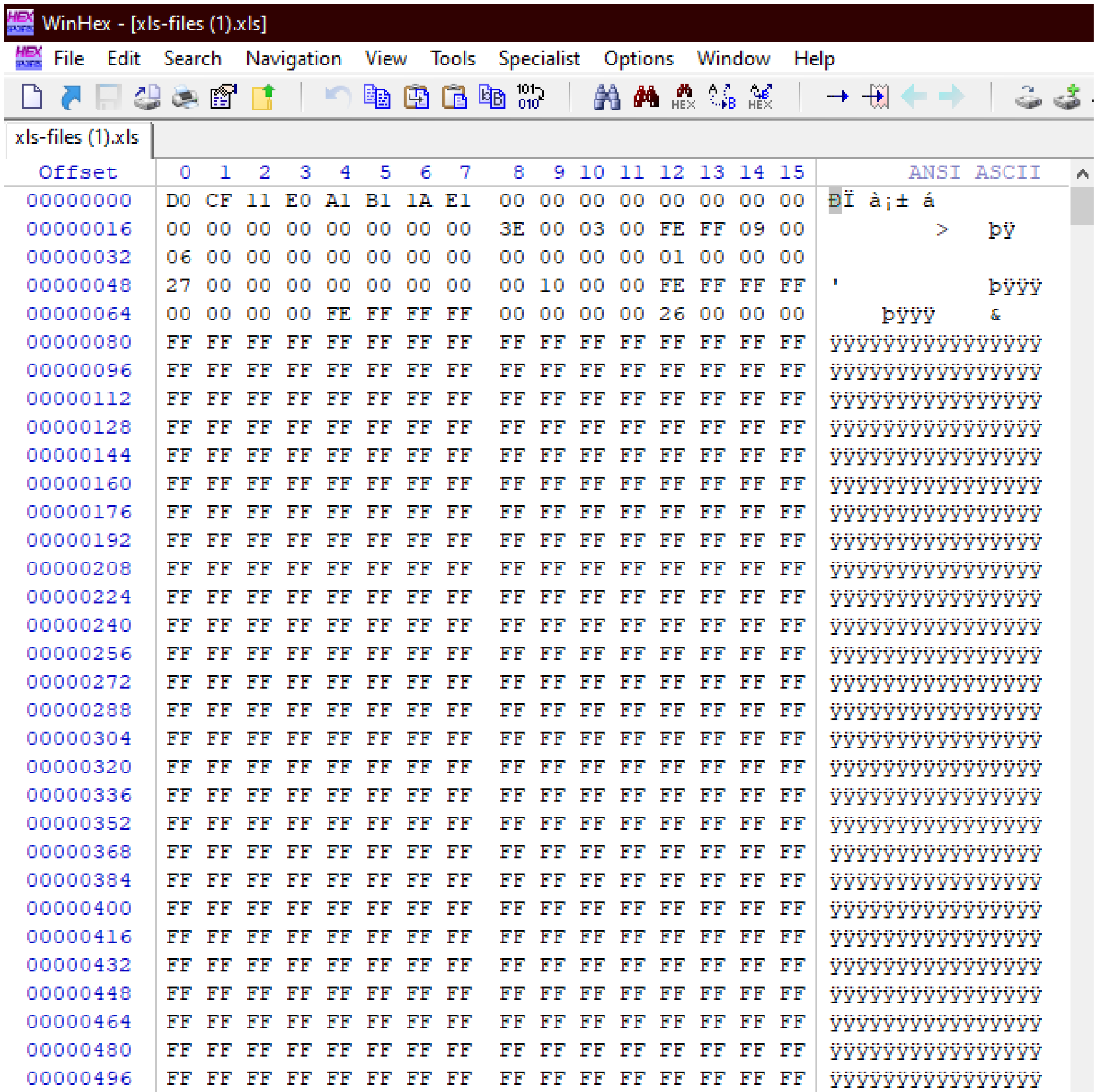

FIGURE 10: Hexadecimal contents of xls-files(1).xls file after recovery from Seagate NVMe SSD TRIM OFF case.

Figure 10 shows a snippet of the xls-files(1).xls file after recovery from Seagate NVMe SSD in the TRIM OFF case. The original contents of the file are shown in the figure above.

Hash Analysis for Samsung and Seagate NVMe SSDS with NVMe WriteBlocker

In this section, we exhibited our findings through the MD5 hash values of the files following the TRIM ON and OFF recovery operations from Samsung and Seagate NVMe SSDs. We used the QuickHash hashing tool to generate the hash values. The MD5 hash value of the original file, followed by TRIM ON and TRIM OFF MD5 hash, and the file size for Samsung NVMe SSD, are shown in figure 11. However, figure 12 shows the hash value of the original file, followed by TRIM OFF MD5 hash, and file size in the Seagate NVMe SSD case. Since xls-files(1).xls file was not recovered in the TRIM ON case, we could not show its hash value in figure 12. The figures aim to validate and verify the claims made due to experimental observation when an NVMe WriteBlocker was used.

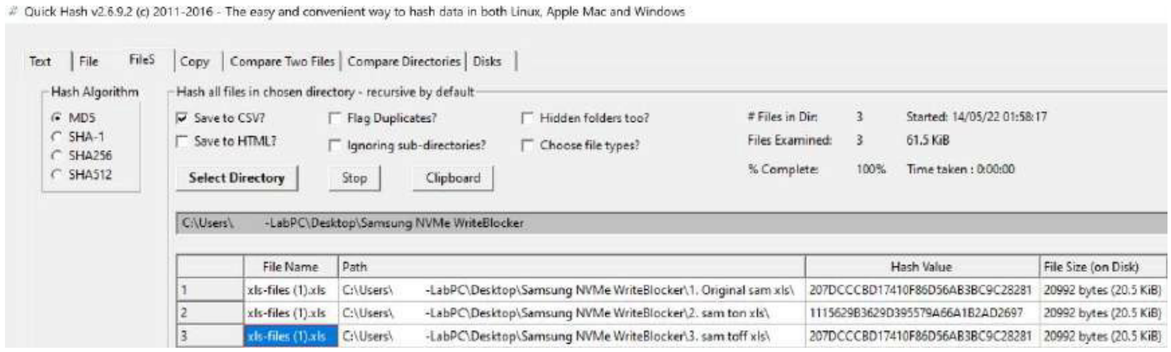

FIGURE 11: Hash values of xls-files(1).xls in Samsung NVMe SSD when using NVMe WriteBlocker.

FIGURE 12: Hash values of xls-files(1).xls in Seagate NVMe SSD when using NVMe WriteBlocker.

Imaging TRIM ON Samsung NVMe SSD with PCIe WriteBlocker using FTK Imager			
File Names	**Type**	**Image Size (KB)**	**MD5 Hash**
ton_wwb-sam_e01_pcie_img_1	e01	12 012 969	db57eed1616f5f6aac5ae9f75b1f2f33
ton_wwb-sam_e01_pcie_img_2	e01	12 012 969	db57eed1616f5f6aac5ae9f75b1f2f33
ton_wwb-sam_e01_pcie_img_3	e01	12 012 969	db57eed1616f5f6aac5ae9f75b1f2f33
ton_wwb-sam_e01_pcie_img_4	e01	12 012 969	db57eed1616f5f6aac5ae9f75b1f2f33
Imaging TRIM ON Seagate NVMe SSD with PCIe WriteBlocker using FTK Imager			
ton_wwb-sg_e01_pcie_img_1	e01	17 075 465	9e8f73e6ab6f9c135536900ee5a5a037
ton_wwb-sg_e01_pcie_img_2	e01	17 075 465	9e8f73e6ab6f9c135536900ee5a5a037
ton_wwb-sg_e01_pcie_img_3	e01	17 075 465	9e8f73e6ab6f9c135536900ee5a5a037
ton_wwb-sg_e01_pcie_img_4	e01	17 075 465	9e8f73e6ab6f9c135536900ee5a5a037
Imaging TRIM OFF Samsung NVMe SSD with PCIe WriteBlocker using FTK Imager			
toff_wwb-sam_e01_pcie_img_1	e01	125 889 025	d4152d87f93ad8fdfee2c97e1d7e7aee
toff_wwb-sam_e01_pcie_img_2	e01	125 889 025	d4152d87f93ad8fdfee2c97e1d7e7aee
toff_wwb-sam_e01_pcie_img_3	e01	125 889 025	d4152d87f93ad8fdfee2c97e1d7e7aee
toff_wwb-sam_e01_pcie_img_4	e01	125 889 025	d4152d87f93ad8fdfee2c97e1d7e7aee
Imaging TRIM OFF Seagate NVMe SSD with PCIe WriteBlocker using FTK Imager			
toff_wwb-sg_e01_pcie_img_1	e01	123 818 402	282e7fc9c54203ba40fd7264e0c16cc1
toff_wwb-sg_e01_pcie_img_2	e01	123 818 402	282e7fc9c54203ba40fd7264e0c16cc1
toff_wwb-sg_e01_pcie_img_3	e01	123 818 402	282e7fc9c54203ba40fd7264e0c16cc1
toff_wwb-sg_e01_pcie_img_4	e01	123 818 402	282e7fc9c54203ba40fd7264e0c16cc1

TABLE 14: Information about forensically acquired image files of Samsung and Seagate NVMe SSDs with NVMe WriteBlocker.

Western Digital and Silicon Power TRIM ON analysis with NVMe WriteBlocker
The TRIM ON analysis of Western Digital (WD) NVMe SSD with NVMe WriteBlocker shows that none of the files could be recovered even after one day of deletion with both AccessData FTK and Autopsy tools. Tables 15 and 16 give the recovery statistics from AccessData FTK and Autopsy of the different files from Western Digital NVMe SSD in the TRIM ON case. In addition, the results of file recovery using AccessData FTK and Autopsy on Silicon Power (SP) NVMe SSD were identical. Tables 17 and 18 show Silicon Power NVMe SSD file recovery statistics using AccessData FTK and Autopsy tools.

The behavior of the controller chips on WD and SP NVMe SSDs exhibited unique results. There were no files recovered from Western Digital NVMe SSD using both AccessData FTK and Autopsy. However, in the case of Silicon Power, file types specifically .csv, .dbase3, .doc, .docx, .eps, .f, .file, .flv, .gif, .gz, .hlp, .jpg, .kml, .kmz, .log, .pages, .pdf, .png, .xls, .xlsx, under 12KB were intact as the controller chip did not clear them out. However, files greater than 12KB were all zeroed out.

TRIM ON: WD FTK Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	0	0	0	0
.vhd	1	0	0	0	0
.ps2	2	0	0	0	0
.aff	16	0	0	0	0
.csv	3184	0	0	0	0
.dbase	480	0	0	0	0
.dmg	32	0	0	0	0
.doc	14592	0	0	0	0
.docx	112	0	0	0	0
.dwf	16	0	0	0	0
.e01	352	0	0	0	0
.eps	640	0	0	0	0
.f	160	0	0	0	0
.fits	16	0	0	0	0
.flv	48	0	0	0	0
.fm	16	0	0	0	0
.gif	5952	0	0	0	0
.gls	32	0	0	0	0
.gz	2176	0	0	0	0
.hlp	112	0	0	0	0
.java	80	0	0	0	0
.jpg	19184	0	0	0	0
.key	16	0	0	0	0
.kml	192	0	0	0	0
.kmz	320	0	0	0	0
.log	1680	0	0	0	0
.mp4	64	0	0	0	0
.numbers	16	0	0	0	0
.odt	16	0	0	0	0
.pages	16	0	0	0	0
.pcap	32	0	0	0	0
.pdf	41344	0	0	0	0
.png	640	0	0	0	0
.pps	176	0	0	0	0
.ppt	9408	0	0	0	0

.pptx	16	0	0	0	0
.xls	10352	0	0	0	0
.xlsx	32	0	0	0	0
None of the files were recovered using AccessData FTK.					

TABLE 15: The number of files recovered using AccessData FTK in Western Digital (WD) NVMe SSD as a primary boot device in Windows 10 TRIM ON case.

TRIM ON: WD Autopsy Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	0	0	0	0
.vhd	1	0	0	0	0
.ps2	2	0	0	0	0
.aff	16	0	0	0	0
.csv	3184	0	0	0	0
.dbase	480	0	0	0	0
.dmg	32	0	0	0	0
.doc	14592	0	0	0	0
.docx	112	0	0	0	0
.dwf	16	0	0	0	0
.e01	352	0	0	0	0
.eps	640	0	0	0	0
.f	160	0	0	0	0
.fits	16	0	0	0	0
.flv	48	0	0	0	0
.fm	16	0	0	0	0
.gif	5952	0	0	0	0
.gls	32	0	0	0	0
.gz	2176	0	0	0	0
.hlp	112	0	0	0	0
.java	80	0	0	0	0
.jpg	19184	0	0	0	0
.key	16	0	0	0	0
.kml	192	0	0	0	0
.kmz	320	0	0	0	0
.log	1680	0	0	0	0
.mp4	64	0	0	0	0
.numbers	16	0	0	0	0
.odt	16	0	0	0	0
.pages	16	0	0	0	0
.pcap	32	0	0	0	0
.pdf	41344	0	0	0	0
.png	640	0	0	0	0
.pps	176	0	0	0	0
.ppt	9408	0	0	0	0
.pptx	16	0	0	0	0
.xls	10352	0	0	0	0
.xlsx	32	0	0	0	0
None of the files were recovered using Autopsy					

TABLE 16: The number of files recovered using Autopsy in Western Digital (WD) NVMe SSD as a primary boot device in Windows 10 TRIM ON case.

TRIM ON: SP FTK Statistics in Windows 10 with NVMe WB					
File Type	Original Image	Image-1	Image-2	Image-3	Image-4
.bin	4	4*	4*	4*	4*
.vhd	1	1*	1*	1*	1*
.ps2	2	2*	2*	2*	2*
.aff	16	16*	16*	16*	16*
.csv	3184	3184	3184	3184	3184
.dbase	480	480	480	480	480
.dmg	32	32*	32*	32*	32*
.doc	14592	14539	14539	14539	14539
.docx	112	112	112	112	112
.dwf	16	16*	16*	16*	16*
.e01	352	352*	352*	352*	352*
.eps	640	640	640	640	640
.f	160	160	160	160	160
.fits	16	16*	16*	16*	16*
.flv	48	48	48	48	48
.fm	16	16*	16*	16*	16*
.gif	5952	5943	5943	5943	5943
.gls	32	0	0	0	0
.gz	2176	1940	1940	1940	1940
.hlp	112	112	112	112	112
.java	80	80*	80*	80*	80*
.jpg	19184	19184	19184	19184	19184
.key	16	16*	16*	16*	16*
.kml	192	192	192	192	192
.kmz	320	320	320	320	320
.log	1680	1676	1676	1676	1676
.mp4	64	64*	64*	64*	64*
.numbers	16	16*	16*	16*	16*
.odt	16	16*	16*	16*	16*
.pages	16	16	16	16	16
.pcap	32	32*	32*	32*	32*
.pdf	41344	41296	41296	41296	41296
.png	640	640	640	640	640
.pps	176	176*	176*	176*	176*
.ppt	9408	9408*	9408*	9408*	9408*
.pptx	16	16*	16*	16*	16*
.xls	10352	10347	10347	10347	10347
.xlsx	32	32	32	32	32
* All files were recovered from AccessData FTK but corrupted.					

TABLE 17: The number of files recovered using AccessData FTK in Silicon Power (SP) NVMe SSD as a primary boot device in Windows 10 TRIM ON case.

TRIM ON: SP Autopsy Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	4*	4*	4*	4*
.vhd	1	1*	1*	1*	1*
.ps2	2	2*	2*	2*	2*
.aff	16	16*	16*	16*	16*
.csv	3184	3184	3184	3184	3184
.dbase	480	480	480	480	480
.dmg	32	32*	32*	32*	32*
.doc	14592	14539	14539	14539	14539
.docx	112	112	112	112	112
.dwf	16	16*	16*	16*	16*
.e01	352	352*	352*	352*	352*
.eps	640	640	640	640	640
.f	160	160	160	160	160
.fits	16	16*	16*	16*	16*
.flv	48	48	48	48	48
.fm	16	16*	16*	16*	16*
.gif	5952	5943	5943	5943	5943
.gls	32	0	0	0	0
.gz	2176	1940	1940	1940	1940
.hlp	112	112	112	112	112
.java	80	80*	80*	80*	80*
.jpg	19184	19184	19184	19184	19184
.key	16	16*	16*	16*	16*
.kml	192	192	192	192	192
.kmz	320	320	320	320	320
.log	1680	1676	1676	1676	1676
.mp4	64	64*	64*	64*	64*
.numbers	16	16*	16*	16*	16*
.odt	16	16*	16*	16*	16*
.pages	16	16	16	16	16
.pcap	32	32*	32*	32*	32*
.pdf	41344	41296	41296	41296	41296
.png	640	640	640	640	640
.pps	176	176*	176*	176*	176*
.ppt	9408	9408*	9408*	9408*	9408*
.pptx	16	16*	16*	16*	16*
.xls	10352	10347	10347	10347	10347
.xlsx	32	32	32	32	32
* All files were recovered from Autopsy but corrupted.					

TABLE 18: The number of files recovered using Autopsy in Silicon Power (SP) NVMe SSD as a primary boot device in Windows 10 TRIM ON case.

Western Digital and Silicon Power TRIM OFF analysis with NVMe WriteBlocker

In this section, we analyzed forensics images taken using NVMe WriteBlocker in TRIM OFF cases of Western Digital (WD) and Silicon Power (SP) NVMe SSDs. The controller chips on WD and SP NVMe SSDs behaved in a distinctive way for this case. As a result, except for a few, most of the files were recovered from Western Digital and Silicon Power devices using AccessData FTK and Autopsy. Tables 19, 20, 21, and 22 show the statistics of file recovery from AccessData FTK and Autopsy.

The controller chip on Western Digital NVMe SSD mostly targeted .bin, .vhd, .ps2, .aff specifically and there were no traces of recovery from AccessData FTK in all of the four forensics images. Furthermore, even though some files were fully recovered, there were found to be corrupted or content wiped out, which happened in the case of, .csv, .dbase3, .dmg, .dmp, .e01, .eps, .f, .hlp, .jpg, .png, .ppt, .xls, and .xlsx. In addition, the recovery process from Autopsy was not up to mark. The tool recovered the files, but their contents were all jumbled up, except for .gif, .jpg. and .key files.

For the controller chip of Silicon Power, the trend of recovery looked quite similar to Western Digital. Files such as .bin, .vhd, .ps2, .aff, .csv, .dbase3, .dmg, .dmp, .doc, .fits, .fm, .java, .numbers, .odt, .pages, .txt could not be said to be fully recovered as they were corrupted, after recovery from AccessData FTK. The recovery from Autopsy showed similar results as shown in the case Western Digital Autopsy recovery. File types such as .bin, .vhd, .ps2, .aff, .csv, .dmg, .dmp, .doc, .eps, .f, .fits, .fm, .jpg, .numbers, .odt, .pages, .png, .ppt, and .xls got mostly affected by the deletion process as their contents were totally jumbled even after full recovery.

TRIM OFF: WD FTK Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	0	0	0	0
.vhd	1	0	0	0	0
.ps2	2	0	0	0	0
.aff	16	0	0	0	0
.csv	3184	2991*	2991*	2991*	2991*
.dbase	480	480*	480*	480*	480*
.dmg	32	32*	32*	32*	32*
.doc	14592	14592	14592	14592	14592
.docx	112	112	112	112	112
.dwf	16	16	16	16	16
.e01	352	352*	352*	352*	352*
.eps	640	640*	640*	640*	640*
.f	160	160*	160*	160*	160*
.fits	16	16	16	16	16
.flv	48	48	48	48	48
.fm	16	16	16	16	16
.gif	5952	5952	5952	5952	5952
.gls	32	32	32	32	32
.gz	2176	2176	2176	2176	2176
.hlp	112	112*	112*	112*	112*
.java	80	80	80	80	80
.jpg	19184	19184*	19184*	19184*	19184*
.key	16	16	16	16	16
.kml	192	192	192	192	192
.kmz	320	320	320	320	320
.log	1680	1680	1680	1680	1680
.mp4	64	64	64	64	64
.numbers	16	16	16	16	16
.odt	16	16	16	16	16
.pages	16	16	16	16	16
.pcap	32	32	32	32	32
.pdf	41344	41344	41344	41344	41344
.png	640	640*	640*	640*	640*
.pps	176	176	176	176	176
.ppt	9408	9408*	9408*	9408*	9408*

ISSN: 1985-2320, https://www.cscjournals.org/journals/IJS/description.php

.pptx	16	16	16	16	16
.xls	10352	10279*	10279*	10279*	10279*
.xlsx	32	32*	32*	32*	32*
*: Recovered all but somefiles were corrupted or contents wiped out with different hash values.					

TABLE 19: The number of files recovered using AccessData FTK in Western Digital NVMe SSD as a primary boot device in Windows 10 TRIM OFF case.

TRIM OFF: WD Autopsy Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	0	0	0	0
.vhd	1	0	0	0	0
.ps2	2	0	0	0	0
.aff	16	0	0	0	0
.csv	3184	2991*	2991*	2991*	2991*
.dbase	480	480*	480*	480*	480*
.dmg	32	32*	32*	32*	32*
.doc	14592	14592*	14592*	14592*	14592*
.docx	112	112*	112*	112*	112*
.dwf	16	16*	16*	16*	16*
.e01	352	352*	352*	352*	352*
.eps	640	640*	640*	640*	640*
.f	160	160*	160*	160*	160*
.fits	16	16*	16*	16*	16*
.flv	48	48*	48*	48*	48*
.fm	16	16*	16*	16*	16*
.gif	5952	5949	5949	5949	5949
.gls	32	32*	32*	32*	32*
.gz	2176	2176*	2176*	2176*	2176*
.hlp	112	112*	112*	112*	112*
.java	80	80*	80*	80*	80*
.jpg	19184	19184*	19184*	19184*	19184*
.key	16	16*	16*	16*	16*
.kml	192	192*	192*	192*	192*
.kmz	320	320*	320*	320*	320*
.log	1680	1680*	1680*	1680*	1680*
.mp4	64	64*	64*	64*	64*
.numbers	16	16*	16*	16*	16*
.odt	16	16*	16*	16*	16*
.pages	16	16*	16*	16*	16*
.pcap	32	32*	32*	32*	32*
.pdf	41344	41344*	41344*	41344*	41344*
.png	640	640*	640*	640*	640*
.pps	176	176*	176*	176*	176*
.ppt	9408	9408*	9408*	9408*	9408*
.pptx	16	16*	16*	16*	16*
.xls	10352	10352*	10352*	10352*	10352*
.xlsx	32	32*	32*	32*	32*
*: Files recovered, but their contents were jumbled.					

TABLE 20: The number of files recovered using Autopsy in Western Digital (WD) NVMe SSD as a primary boot device in Windows 10 TRIM OFF case.

TRIM OFF: SP FTK Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	3*	3*	3*	3*
.vhd	1	1*	1*	1*	1*
.ps2	2	2*	2*	2*	2*
.aff	16	16*	16*	16*	16*
.csv	3184	3184*	3184*	3184*	3184*
.dbase	480	480*	480*	480*	480*
.dmg	32	32*	32*	32*	32*
.doc	14592	14590*	14590*	14590*	14590*
.docx	112	112	112	112	112
.dwf	16	16	16	16	16
.e01	352	352	352	352	352
.eps	640	640	640	640	640
.f	160	160	160	160	160
.fits	16	16*	16*	16*	16*
.flv	48	48	48	48	48
.fm	16	16	16	16	16
.gif	5952	5952	5952	5952	5952
.gls	32	32	32	32	32
.gz	2176	2176	2176	2176	2176
.hlp	112	112	112	112	112
.java	80	80	80	80	80
.jpg	19184	19184	19184	19184	19184
.key	16	16	16	16	16
.kml	192	192	192	192	192
.kmz	320	320	320	320	320
.log	1680	1680	1680	1680	1680
.mp4	64	64	64	64	64
.numbers	16	16*	16*	16*	16*
.odt	16	16*	16*	16*	16*
.pages	16	16*	16*	16*	16*
.pcap	32	32	32	32	32
.pdf	41344	41344	41344	41344	41344
.png	640	626	626	626	626
.pps	176	176*	176*	176*	176*
.ppt	9408	9403	9403	9403	9403
.pptx	16	16*	16*	16*	16*
.xls	10352	10352	10352	10352	10352
.xlsx	32	32	32	32	32
*:Recovered all but some files were corrupted or contents wiped out with different hash values.					

TABLE 21: The number of files recovered using AccessData FTK in Silicon Power NVMe SSD as a primary boot device in Windows 10 TRIM OFF case.

TRIM OFF: SP Autopsy Statistics in Windows 10 with NVMe WB					
File Type	Original Count	Image-1	Image-2	Image-3	Image-4
.bin	4	4*	4*	4*	4*
.vhd	1	1*	1*	1*	1*
.ps2	2	2*	2*	2*	2*
.aff	16	16*	16*	16*	16*
.csv	3184	3184*	3184*	3184*	3184*
.dbase	480	480	480	480	480
.dmg	32	32*	32*	32*	32*
.doc	14592	14592*	14592*	14592*	14592*
.docx	112	112	112	112	112
.dwf	16	16	16	16	16
.e01	352	352	352	352	352
.eps	640	640*	640*	640*	640*
.f	160	160*	160*	160*	160*
.fits	16	16	16	16	16
.flv	48	48	48	48	48
.fm	16	16*	16*	16*	16*
.gif	5952	5949	5949	5949	5949
.gls	32	32	32	32	32
.gz	2176	2176	2176	2176	2176
.hlp	112	112	112	112	112
.java	80	80	80	80	80
.jpg	19184	19184*	19184*	19184*	19184*
.key	16	16	16	16	16
.kml	192	192	192	192	192
.kmz	320	320	320	320	320
.log	1680	1680	1680	1680	1680
.mp4	64	64	64	64	64
.numbers	16	16*	16*	16*	16*
.odt	16	16*	16*	16*	16*
.pages	16	16*	16*	16*	16*
.pcap	32	32	32	32	32
.pdf	41344	41344	41344	41344	41344
.png	640	621	621	621	621
.pps	176	176	176	176	176
.ppt	9408	9403*	9403*	9403*	9403*
.pptx	16	16	16	16	16
.xls	10352	10352	10352	10352	10352
.xlsx	32	32	32	32	32
*: Files recovered, but their contents were jumbled or wiped out.					

TABLE 22: The number of files recovered using Autopsy in Silicon Power (SP) NVMe SSD as a primary boot device in Windows 10 TRIM OFF case.

ISSN: 1985-2320, https://www.cscjournals.org/journals/IJS/description.php

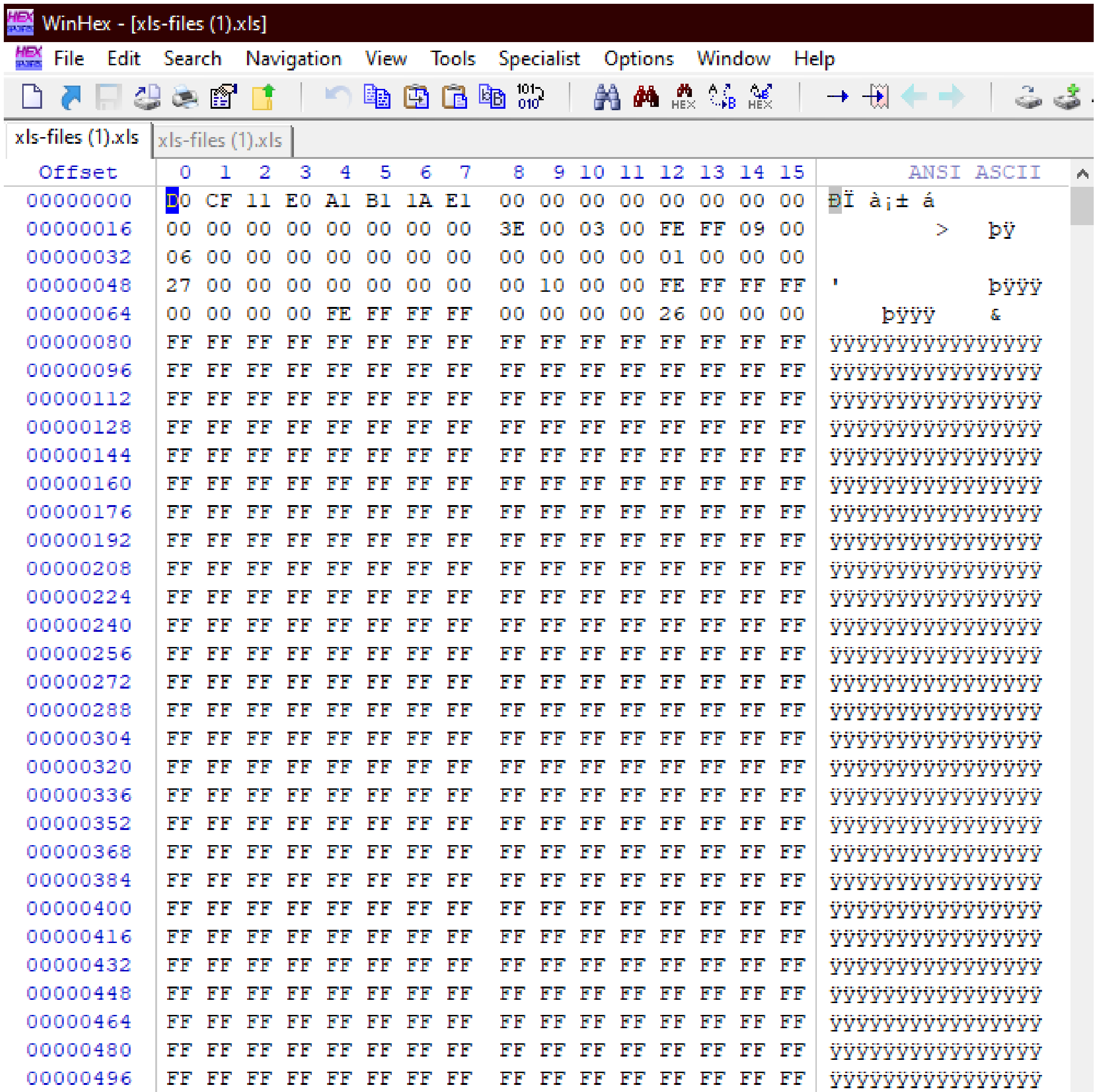

FIGURE 13: Hexadecimal contents of xls-files(1).xls file in the original dataset from Western Digital NVMe SSD.

Figure 13 shows a snippet of the original xls-files(1).xls file with regards to the Western Digital NVMe SSD TRIM ON case in the original dataset. The hexadecimal contents are shown along with ASCII value when a file is opened in a disk editor such as WinHex. In this case, the original contents of the file are shown in the figure.

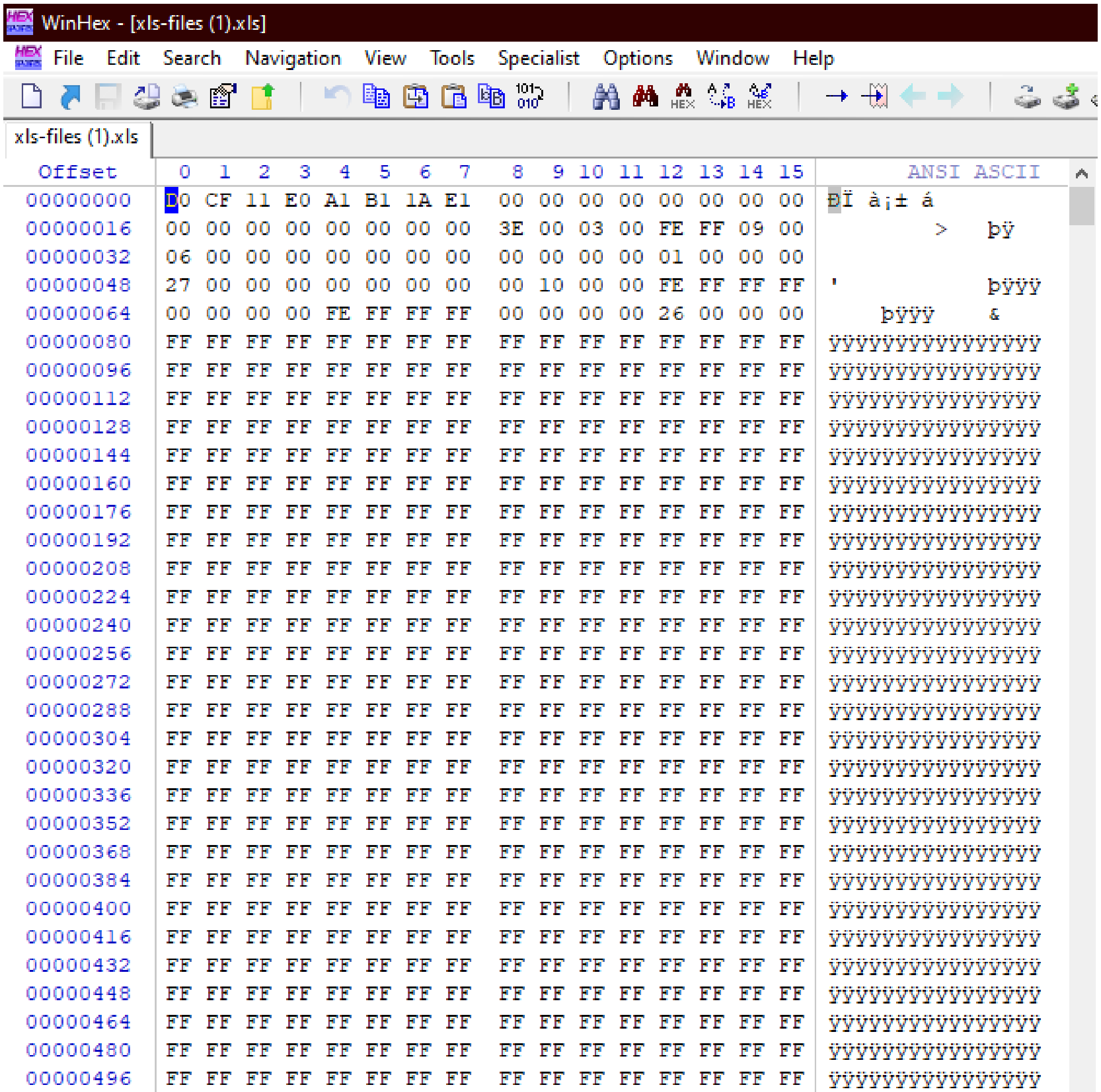

FIGURE 14: Hexadecimal contents of xls-files(1).xls fileof after recovery from Western Digital NVMe SSD TRIM OFF case.

Figure 14 shows a snippet of the xls-files(1).xls file after recovery from Western Digital NVMe SSD in the TRIM OFF case. In this case, the file contents were not wiped out for the file, as shown in the figure.

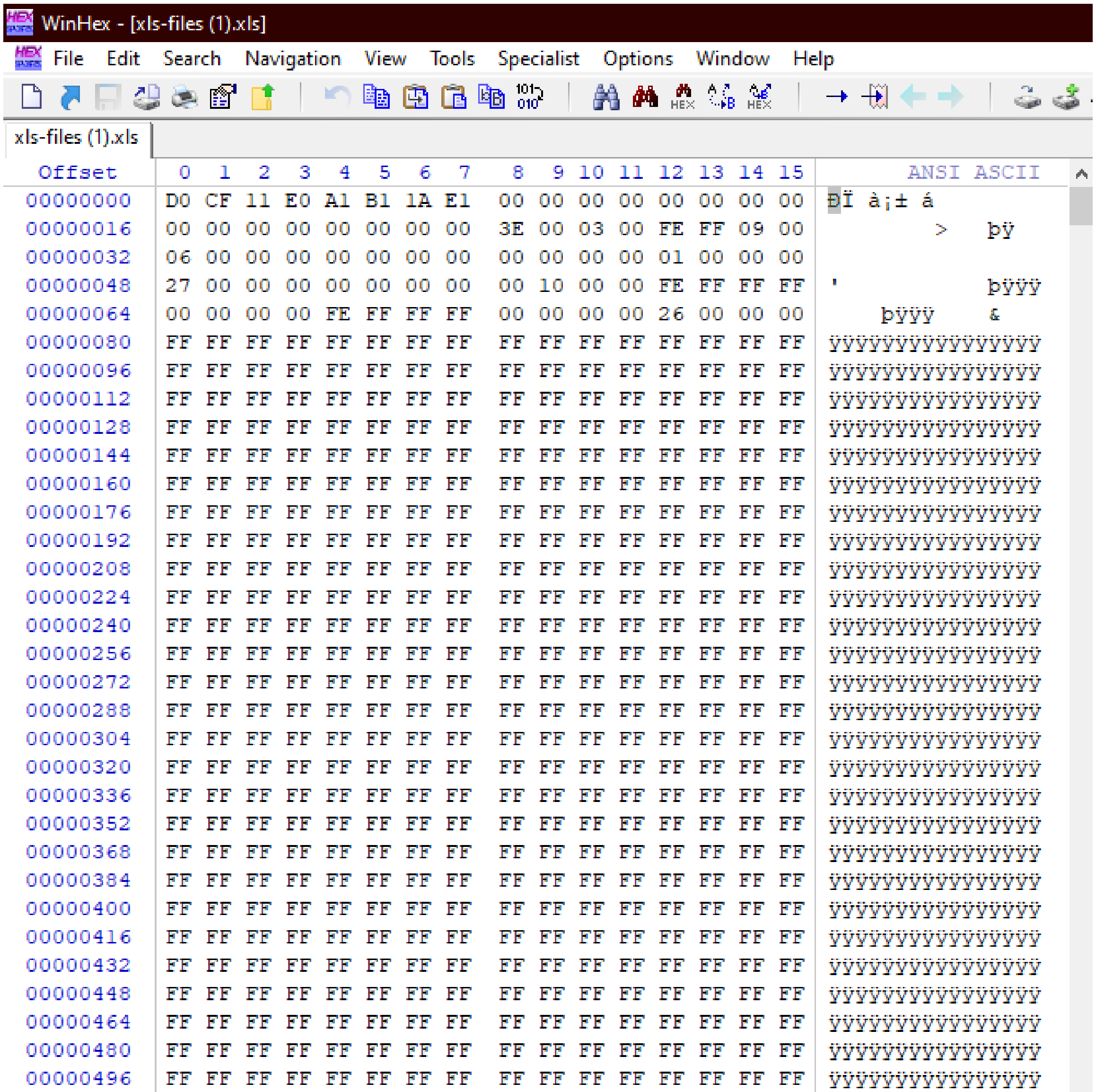

FIGURE 15: Hexadecimal contents of xls-files(1).xls file in the original dataset from Silicon Power NVMe SSD.

Figure 15 shows a snippet of the original xls-files(1).xls file with regards to the Silicon Power NVMe SSD TRIM ON case in the original dataset. The hexadecimal contents are shown along with ASCII value when a file is opened in a disk editor such as WinHex. In this case, the original contents of the file are shown in the figure.

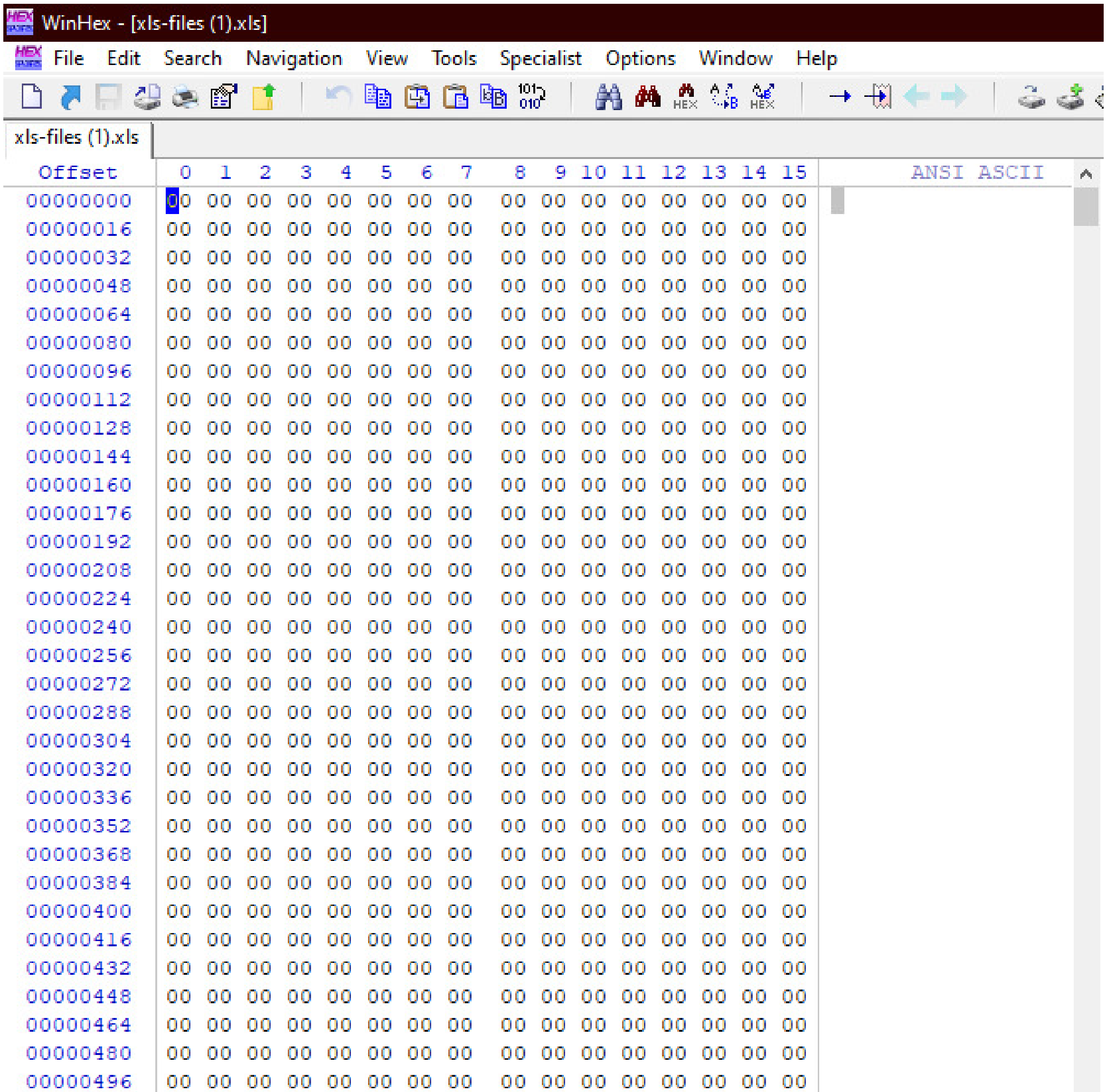

FIGURE 16: Hexadecimal contents of xls-files(1).xls file after recovery from Silicon Power NVMe SSD TRIM ON case.

Figure 16 shows a snippet of the xls-files(1).xls file after recovery from Silicon Power NVMe SSD in the TRIM ON case. In this case, the file contents were wiped out for the file as shown by zeroes in the figure.

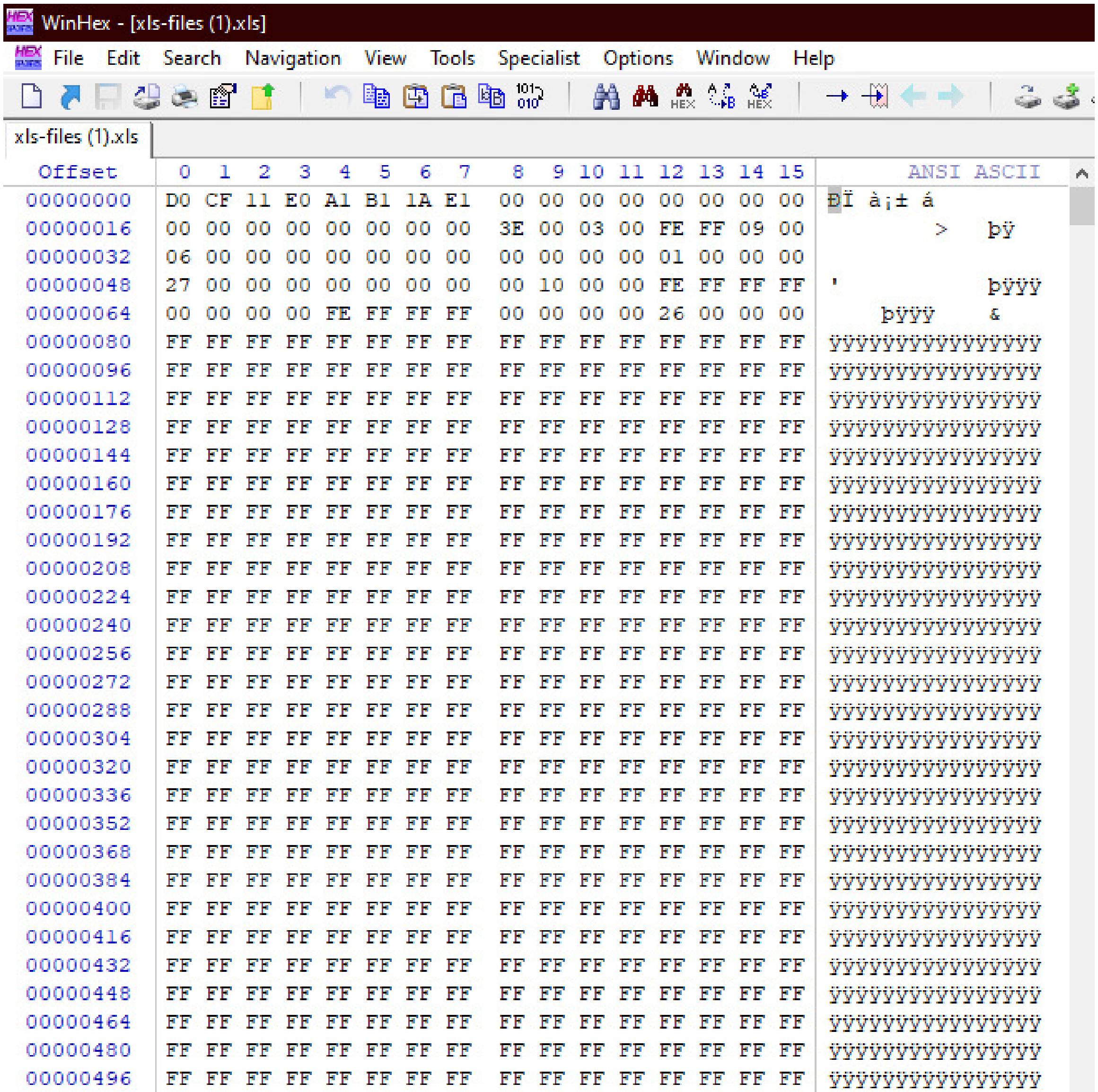

FIGURE 17: Hexadecimal contents of xls-files(1).xls file after recovery from Silicon Power NVMe SSD TRIM OFF case.

Figure 17 shows a snippet of the xls-files(1).xls file after recovery from Silicon Power NVMe SSD in the TRIM OFF case. Again, the original contents of the file are shown in the figure.

Hash Analysis for Western Digital and Silicon Power NVMe SSDS with NVMe WriteBlocker

The MD5 hash values of the files following the TRIM ON and OFF recovery operations from Western Digital and Silicon Power NVMe SSDs are displayed in this part to demonstrate our findings. We used the QuickHash hashing tool to achieve the results. The MD5 hash value of the original file, followed by TRIM OFF MD5 hash, and the file size for Western Digital NVMe SSD are shown in figure 18. Unfortunately, we could not show the TRIM ON hash value due to the absence of recovery of xls-files(1).xls file. However, figure 19 shows the hash values of the original file, followed by TRIM ON and OFF MD5 hash values and file size in the Silicon Power NVMe SSD case, as shown in figure 19. The figures aim to validate and verify the claims made due to experimental observation when using an NVMe WriteBlocker.

FIGURE 18: Hash values of xls-files(1).xls in Western Digital NVMe SSD when using NVMe WriteBlocker

FIGURE 19: Hash values of xls-files(1).xls in Silicon Power NVMe SSD when using NVMe WriteBlocker

Imaging TRIM ON Western Digital NVMe SSD with PCIe WriteBlocker using FTK Imager			
File Names	**Type**	**Image Size (KB)**	**MD5 Hash**
ton_wwb-wd_e01_pcie_img_1	e01	19 373 246	e612c339d9b3001c18b13a8ba3250093
ton_wwb-wd_e01_pcie_img_2	e01	19 373 246	e612c339d9b3001c18b13a8ba3250093
ton_wwb-wd_e01_pcie_img_3	e01	19 373 246	e612c339d9b3001c18b13a8ba3250093
ton_wwb-wd_e01_pcie_img_4	e01	19 373 246	e612c339d9b3001c18b13a8ba3250093
Imaging TRIM ON Silicon Power NVMe SSD with PCIe WriteBlocker using FTK Imager			
ton_wwb-sp_e01_pcie_img_1	e01	16 531 698	14d8b304d966ac894322e359f33cd601
ton_wwb-sp_e01_pcie_img_2	e01	16 531 698	14d8b304d966ac894322e359f33cd601
ton_wwb-sp_e01_pcie_img_3	e01	16 531 698	14d8b304d966ac894322e359f33cd601
ton_wwb-sp_e01_pcie_img_4	e01	16 531 698	14d8b304d966ac894322e359f33cd601
Imaging TRIM OFF Western Digital NVMe SSD with PCIe WriteBlocker using FTK Imager			
toff_wwb-wd_e01_pcie_img_1	e01	125 161 110	025181d55629d0876c881b479c0be4cf
toff_wwb-wd_e01_pcie_img_2	e01	125 161 110	025181d55629d0876c881b479c0be4cf
toff_wwb-wd_e01_pcie_img_3	e01	125 161 110	025181d55629d0876c881b479c0be4cf
toff_wwb-wd_e01_pcie_img_4	e01	125 161 110	025181d55629d0876c881b479c0be4cf
Imaging TRIM OFF Silicon Power NVMe SSD with PCIe WriteBlocker using FTK Imager			
toff_wwb-sp_e01_pcie_img_1	e01	124 938 768	59ec02930b9df63922d4396c4509c00d
toff_wwb-sp_e01_pcie_img_2	e01	124 938 768	59ec02930b9df63922d4396c4509c00d
toff_wwb-sp_e01_pcie_img_3	e01	124 938 768	59ec02930b9df63922d4396c4509c00d
toff_wwb-sp_e01_pcie_img_4	e01	124 938 768	59ec02930b9df63922d4396c4509c00d

TABLE 23: Information about forensically acquired image files of Western Digital and Silicon Power NVMe SSDs with NVMe WriteBlocker.

5. DISCUSSION and COMPARATIVE EVALUATION

Digital storage systems have undergone a revolution in the past few years, significantly improving storage capacities, performance, and dependability. Traditional storage devices included hard disk drives, which are now being replaced by solid state drives at an increasing speed. A new category of solid-state drives that are increasingly becoming popular is the Non-Volatile Memory Express Solid-State Drive (NVMe SSD). NVMe is an interface that utilizes PCIe express for fast data transfers Nikkel (2016). SSDs also use a feature known as TRIM which identifies storage blocks within the SSD that have been marked for removal and deletes the data internally. The TRIM function, however, has a detrimental impact on digital forensics, particularly regarding data recovery. It poses a challenge for digital forensic investigators in obtaining evidence. This research aims to recover deleted digital evidence from four commonly used NVMe SSDs when the TRIM feature is enabled and disabled using different software tools such as Autopsy and Access Data FTK toolkit. Furthermore, to check the integrity of the evidence, we used the QuickHash tool to obtain MD5 hash values.

It is evident, based on the information collected and the methods and scenarios implemented in this study, that the TRIM function poses problems and challenges for digital forensics investigators. As a result, the TRIM function will eliminate obsolete data and internally destroy the data. Among the four different NVMe SSDs chosen for this experiment, no data was recovered in the TRIM ON scenario. Some files were retrieved from Samsung and Silicon Power SSDs but were corrupted and rendered useless. The results in the previous section were generated from the FTK toolkit and Autopsy.

The TRIM OFF scenario was better compared to TRIM ON. With Silicon Power and Seagate NVMe SSDs, all files were recovered, some of which were corrupted. In the case of Samsung and Western Digital NVMe SSDs, some files were not recovered, some were fully recovered, and some were recovered but were corrupted when recovery was performed with AccessData FTK. With the use of Autopsy, the number of files retrieved in this scenario degraded with fewer files being recovered.

In conclusion, the Silicon Power NVMe SSD showed the most promising result among the four NVMe SSDs. The NVMe SSD that came a close second were Seagate and Samsung. In contrast, the controller chips of Western Digital acted quickly as soon as they found deleted data to be purged. Additionally, between the tools used: AccessData FTK and Autopsy, it is safe to say that the FTK toolkit outperformed Autopsy when performing forensics data recovery on different brands of NVMe SSDs.

6. CONCLUSION and FUTURE WORK

For digital forensics investigators, the most recent technological advancements constantly provide new and challenging problems. For extracting evidence, digital forensic specialists rely significantly on highend forensic technology and software tools. Though there are several industry-standard digital forensics tools, none are ubiquitous. They can allow evidence extraction from all electronic devices such as personal computers, laptops, smartphones, etc.

Rapid technological changes are the most challenging problem investigators are facing Kumar (2021). New software, mobile apps, and hardware platforms are introduced daily. However, forensics software updates don’t happen as quickly. The investigators cannot do anything until the updates are made public.

As NVMe SSDs become more popular in consumer computers, the landscape for forensic analysis has shifted. Without any human input, data movement events occur within the SSD. As a result, while performing digital forensics examinations, SSDs can no longer be managed as HDDs can. Therefore, when performing forensics analysis, an investigator must understand and document the events in the background of SSDs. Using the TRIM ON and OFF features of Windows 10 v21H2, we investigated four types of NVMe SSDs: Samsung, Seagate, Western Digital, and Silicon Power. The number of files recovered after deletion in each NVMe SSD was used to examine the results.

The research objectives mentioned in the introduction section can be concluded as follows:

- The TRIM enable and disabled functions have a substantial impact on the ability to recover deleted artifacts from an NVMe SSD. The outcome of TRIM-activated functionality is, however, absolutely uncertain. Because different manufacturers implement wear-leveling functionality in their products differently, it is discovered in the experiment that each SSD exhibits a different set of results.
- The experiment shows that the chances of recovering deleted data from SSD are low as time elapses. This indicates the erasure of contents permanently due to the implementation of wear- leveling in SSDs.
- After in-depth analysis and observation, the files recovered from the SSDs are considered reliable as they have the same MD5 hash values.

We addressed our findings based on the research approach, which aimed to comprehensively understand the file recovery process. We also showed that the hash values did not change in any of the NVMe SSDs up to seven days when images were acquired using the NVMe WriteBlocker. This was one of the unique findings of our research. Usually, when it comes to SSDs, hash values quickly change whenever images are forensics taken between intervals of time. This research could have significant ramifications for digital forensic investigation, particularly in cases where digital data is believed to have been erased by the suspect purposefully or knowingly. As a result, this work contributes to the digital forensics literature by providing valuable results on an area that has received little attention.

In consideration of the results obtained from the experiments, the behavior of wear-leveling in different SSD manufacturers having the same storage capacities does not match. It varies based on the types of files and sizes. The recovery of files from different SSD manufacturers showed different results.

Future work will incorporate further examinations into many other NVMe SSDs of different manufacturers. We would also like to look into the effects of deletion when files are recovered from NVMe SSDs that are used as primary boot devices in a virtualized environment. Finally, we want to use the Cellebrite Inspector and Magnet AXIOM tools to investigate the impact of TRIM functionality in the resilient file system (ReFS) for future analysis and contribution.

7. REFERENCES

Bahgat, A. (2021). What is SSD? Everything You Need to Know About Solid-State Storage. Available at https://kinsta.com/blog/what-is-ssd/.

Battula, B. P., Rani, K., Prasad, S., and Sudha, T. (2009). Techniques in computer forensics: A recovery perspective. *International Journal of Security*, 3(2):27–35.

Bednar, P. and Katos, V. (2011). SSD: New Challenges for Digital Forensics. In *Proceedings of the 8th Conference of the Italian Chapter of the Association for Information SystemsItAIS*.

Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley.

Garfinkel, S., Farrell, P., Roussev, V., and Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. digital investigation, 6. Available at https://digitalcorpora.org/.

Gillis, A. (2021). Hard-Disk Drives. Available at https://www.techtarget.com/searchstorage/definition/ hard-disk-drive.

Gubanov, Y. and Afonin, O. (2014). Recovering evidence from ssd drives: understanding trim, garbage collection and exclusions. *Belkasoft, Menlo Park*.

King, C. and Vidas, T. (2011). Empirical analysis of solid state disk data retention when used with contemporary operating systems. *Digital Investigation*, 8:S111–S117. The Proceedings of the Eleventh Annual DFRWS Conference.

Kingston Technology (2017). Understanding SSD Technology: NVMe, SATA, M.2. Available at https://www.kingston.com/unitedstates/us/community/articledetail/articleid/48543.

Kranz, G. (2021). Serial ATA (serial advanced technology attachment or sata). Available at https:// searchstorage.techtarget.com/definition/Serial-ATA.

Kumar, M. (2021). Solid state drive forensics analysis—challenges and recommendations. *Concurrency and Computation: Practice and Experience*, 33(24):e6442.

Mellor, C. (2020). Hard Disk Drive Shipments Fell 50 percent Between 2012 and 2019. Available at https://blocksandfiles.com/2020/01/14/disk-drive-shipments-50-per-cent-fallfrom-2012-to-2019/.

Neyaz, A., Shashidhar, N., and Karabiyik, U. (2018). Forensic Analysis of Wear Leveling on Solid-State Media. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (Trust- Com/BigDataSE)*, pages 1706–1710.

Neyaz, A., Zhou, B., and Karpoor, N. (2019). Comparative Study of Wear-leveling in Solid-State Drive with NTFS File System. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 4294– 4298.

Nikkel, B. (2016). NVM Express Drives and Digital Forensics. *Digital Investigation*, 16:38–45.

Nisbet, A., Lawrence, S., and Ruff, M. (2013a). A Forensic Analysis and Comparison of Solid State Drive Data Retention with TRIM Enabled File Systems.

Nisbet, A., Lawrence, S., and Ruff, M. (2013b). A forensic analysis and comparison of solid state drive data retention with trim enabled file systems.

Paul, I. (2019). Multi-Layer SSDs: What are SLC, MLC, TLC, QLC, and PLC? Available at https://www.howtogeek.com/444787/multi-layer-ssds-what-are-slc-mlc-tlc-qlc-and-mlc/.

Riadi, I. and Hadi, A. (2019). Analysis of Digital SSD NVMe Evidence on Proprietary Operating Systems Using the Static Forensics Method.

Riadi, I., Sunardi, S., and Hadi, A. (2020). Analysis of Digital Evidence Trim Enable NVME SSD Using Static Forensics Method. *JUITA: Jurnal Informatika*, 8(1):65–74.

Riggs, H., Tufail, S., Parvez, I., and Sarwat, A. (2020). Survey of solid state drives, characteristics, technology, and applications. In *2020 SoutheastCon*, pages 1–6.

Robert, S., Kranz, G., and Raffo, D. (2021). Computer Storage. Available at https://www.techtarget.com/ searchstorage/definition/storage.

Shah, Z., Mahmood, A. N., and Slay, J. (2015). Forensic potentials of solid state drives. In Tian, J., Jing, J., and Srivatsa, M., editors, *International Conference on Security and Privacy in Communication Networks*, pages 113–126, Cham. Springer International Publishing.

Silwa, C. (2018). SSD TRIM. Available at https://www.techtarget.com/searchstorage/definition/TRIM.

Valette, A. (2016). Overview of 'Wear Leveling' with SSD controllers and what is it? Available at https://www.ontrack.com/en-us/blog/wear-leveling.

Vieyra, J., Scanlon, M., and Le-Khac, N.-A. (2018). Solid state drive forensics: Where do we stand? In Breitinger, F. and Baggili, I., editors, *Digital Forensics and Cyber Crime*, pages 149–164, Cham. Springer International Publishing.