HASIL CEK_60020397_Point-C36-IRD-850GB-Live forensics method for acquisition on the Solid State Drive (SSD) NVMe TRIM function

by Imam Riadi 60020397

Submission date: 11-Dec-2020 10:18AM (UTC+0700)

Submission ID: 1471668985

File name: acquisition_on_the_Solid_State_Drive_SSD_NVMe_TRIM_function.pdf (857.61K)

Word count: 5077

Character count: 28845

Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 5, No. 2, May 2020, Pp. 129-138

Live forensics method for acquisition on the Solid State Drive (SSD) NVMe TRIM function

Wisnu Pranoto*[1], Imam Riadi[2], Yudi Prayudi[3]
Department of Informatics, Universitas Islam Indonesia, Indonesia[1,3]
Department of Information System, Universitas Ahmad Dahlan, Indonesia[2]

Article Info

Keywords:
Solid State Drive NVMe, Digital Evidence, TRIM, Live Forensics

Article history:
Received 03 January 2020
Revised 21 February 2020
Accepted 13 April 2020
Available 06 May 2020

Cite:
Pranoto, W., Rladi, I., & Prayudi, Y. (2020). Live forensics method for acquisition on the Solid State Drive (SSD) NVMe TRIM function. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 5(2). doi:https://doi.org/10.22219/kinetik.v5i2.1032

*Corresponding author.
Wisnu Pranoto
E-mail address:
17917130@students.uii.ac.id

Abstract

SSD currently has a new storage media technology namely Solid State Drive Non-volatile Memory Express (SSD NVMe). In addition, SSD has a feature called TRIM. The TRIM feature allows the operating system to tell SSDs which blocks are not used. TRIM removes blocks that have been marked for removal by the operating system. However, the TRIM function has a negative effect for the digital forensics specifically related to data recovery. This study aimed to compare the TRIM disable and enable functions to determine the ability of forensics tools and recovery tools to restore digital evidence on the NVMe SSD TRIM function. The operating system used in this study was Windows 10 professional with NTFS file system. Typically, acquisition is conducted by using traditional or static techniques. Therefore, there was a need of a technique to acquire SSD by using the live forensics method without shutting down the running operating system. The live forensics method was applied to acquire SSD NVMe directly to the TRIM disable and enable functions. The tools used for live acquisition and recovery were FTK Imager Portable. The inspection and analysis phases used Sleutkit Autopsy and Belkasoft Evidence Center. This research found that in the recovery process of TRIM disabled and enabled, TRIM disabled could find evidence while maintaining the integrity of evidence. It was indicated by the same hash value of the original file and the recovery file. Conversely, when TRIM is enabled, the files were damaged and could not be recovered. The files were also not identical to the original so the integrity of evidence was not guaranteed.

1. Introduction

According to research and reports of computer crime from ID-CERT [1], occurrences of computer crime are increasing significantly from year to year. Computer crime itself is an illegal act involving technology to manipulate digital data [2].

Computer technology requires speed of accessing its operation. One of the means to achieve the speedy access is SSD storage media [3]. SSD stands for Solid State Drive. It is a media that stores all information data on flash memory chips [4]. Recently, SSD has launched a technology of storage medium namely SSD Non-volatile Memory Express (NVMe). NVMe is an interface that utilizes PCIe paths to do faster data transfers [5][6]. In addition, SSD has a feature called TRIM. The TRIM feature is a command related to the running operating system which is directed to the firmware of SSD [7]. TRIM will identify which blocks are considered obsolete and delete remaining data internally [8][9]. As the consequence, the handling of information data on SSD should be done quickly since the data will immediately lost when the system shut down [8]. Figure 1 below shows the development of SSD usage [10].

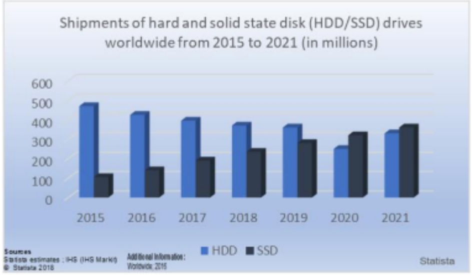


Figure 1. SSD Users Statistic [10]

Digital forensics is a field of science that investigate digital evidence in order to collect, restore and analyze the digital evidence. The digital evidence on computer crime can be retrieved from communication devices such as smartphones, tablets, laptops or other computer users [2][11][12]. The required digital evidence can be obtained using live forensics technique. Live forensics is a method used for handling computer crime and data recovery while the computer system is running [13]. Live forensics technique will be able to improve the results of digital evidence data recovery from the TRIM function on the NVMe SSD. This technique can also guarantee the data integrity without losing the digital evidence [14][15].

Storage media such as SSDs is a non-volatile storage type. Non-volatile means that the stored data can be written and deleted, but the data still exists even if the system is shutting off [16]. This research employed non-volatile storage media on SSD. Ramadhan et al [4] conducted a research on the process of forensic data recovery on SATA SSDs using the static method. The static method includes the traditional stages for processing digital evidence using bit-by-bit images and the forensic process was run when the system is not running [17][18][19]. The research found that SSD had TRIM disabled and enabled features. Another research employing the static method was carried out by Hadi et al [20]. It was a research on the NVMe SSD interface implementing the TRIM function using NIST framework through Collection, Examination, Analysis, and Reporting stages. The study found that Autopsy tool could not recover the entire file that had been deleted with TRIM disabled function, while not all files which had been deleted using TRIM enabled function can be recovered by Sluetkit Autopsy and Belkasoft tools.

In addition to static method, live forensics method can be employed in file recovery process using forensics technique. The advantages of live forensics method include faster investigation process, secure data integrity, more readable encryption technique and less memory imaging capacity compared to traditional forensic techniques [21][22]. In a research conducted by Soni et al [13], live forensics method was applied to perform data recovery while the virtual server was running. The live forensics virtual server process was carried out by using a proxmox virtual machine that provided backup features. This study aimed to restore data when the virtual server was running. The tools were Sluet Kit Autopsy and Belkasoft. The result of the study was successful in reading the entire contents of the imaging file and was able to find the deleted file.

2. Research Method

2.1 Method

In this study, the acquisition method was carried out by applying live forensics method on non-volatile data based on the guidelines and requirements in the Indonesian National Standard (SNI) 27037: 2014 [23]. The stages of the live forensics method according to SNI 27037: 2014 [23] are shown in Figure 2.

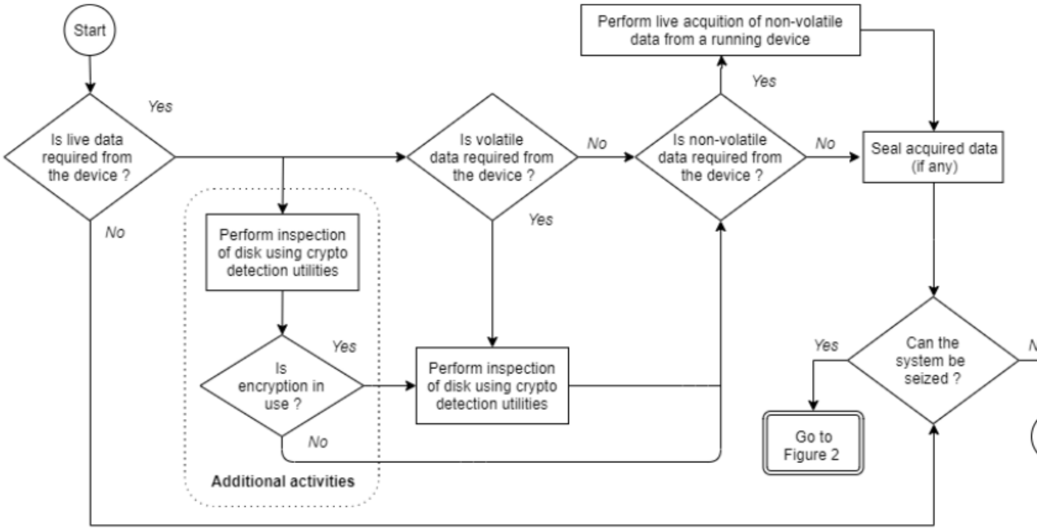

Start
Is live data required from the device ?
Yes
No
Perform inspection of disk using crypto detection utilities
Is encryption in use ?
Yes
No
Additional activities
Is volatile data required from the device ?
No
Yes
Perform inspection of disk using crypto detection utilities
Perform live acquition of non-volatile data from a running device
Yes
Is non-volatile data required from the device ?
No
Seal acquired data (if any)
Can the system be seized ?
Yes
No
Go to Figure 2
Stop

Figure 2. SNI Acquisition 27037:2014 [23]

A number of previous studies had used the procedure of acquisition of live forensics according to SNI 27037: 2014 [14]. In the SNI 27037: 2014 guideline, the stages of NVMe SSD acquisition process including determining the type of acquisition to be used, determining which type of data obtained, performing the acquisition procedure, and seizing the acquisition results for the hashing process with MD5.

Figure 3 below is the stages of examination and analysis employed in this research. Stages of inspection of digital evidence that has been acquired, and later will do extraction to get clues related to the case scenario. Stages of inspection will be carried out on the perpetrator's computer, then the investigator's computer is used for analysis needs. Before examining the acquisition results, the original acquisition results must be published and see the hash value between the original file and the published file, because it needs to be done to maintain the authenticity of the evidence. Furthermore, to maintain the authenticity of the evidence, the examination of the evidence is a copy of the file of the acquisition.

Preparation
Extraction
Analysis

Figure 3. Examination and Analysis Stages

1. Preparation

The preparation was completed by providing storage space for the imaging data which was recovered. This stage was done using the Portable FTK Imaging tool to do the acquisition. FTK Imager supports live forensics to obtain the NVMe SSD imaging file with TRIM disabled and enabled function.

2. Extraction

In this step, extraction of the imaging file was done by identifying and recovering files that had been deleted. File extraction will also reveal the characteristics of the file structure, deleted data, file name, and md5 hash value.

3. Analysis

This stage analyzes the results of the completed extraction process, so that it can measure the effectiveness of the extraction of TRIM function files and recommend which tools were appropriate for file recovery in this study.

The tools and materials required to obtain digital evidence in this study were ASUS X455LN laptop with Windows 10 Education operating system and 64-bit architecture as well as an external USB SSD for live acquisition storage. Forensics tools used were NVMe SSD for acquisition and FTK Portable Imager for imaging. The analysis and recovery of digital evidence were completed by Sluetkit Autopsy, Belkasoft Evidence tools.

2.2 Scenario

In the present study, the researchers conducted the research by using the SSD interface storage media NVMe TRIM function on Windows 10 with the implementation of live forensics method for file recovery of TRIM functions. This research required a scenario to obtain the digital evidence. The scenario was made to cover all activities that run on the NVMe SSD TRIM function. The scenario on the NVMe SSD was intended as a guideline for permanent deletion (shift + delete) of several files to be recovered and analyzed. In order to simplify the deletion of files, the files were distinguished by odd-even naming system. TRIM disabled was applied to odd name files and TRIM enabled was applied to even file name. The hash values of several odd-even files can be seen in Table 1 below. The performed scenario is illustrated in Figure 4.

Steps for the Perpetrator:

1. The Perpetrator used SSD NVMe with the Windows 10 Professional operating system and NTFS file system.
2. The Perpetrator divided the storage into two partitions, Drive C:\ and Drive D:\. The manipulated files were stored in partition Drive D:/.
3. The perpetrator applied the TRIM disabled and enabled functions.
4. The perpetrator permanently deleted (shift+delete) the odd-even label file on the NVMe SSD in the Drive D: \ partition.

Steps for the Investigator:

1. The investigator connects an external USB SSD SATA to the Perpetrator's computer to store the results of file acquisition and recovery.
2. The Investigator conduct acquisition on NVMe SSDs directly on the perpetrator's computer with an external USB SSD SATA and the Portable Imager FTK tool.
3. The Investigator's computer was used to conduct examination and analysis of imaging results by using Sleut Kit Autopsy and Belkasoft Evidence.

Table 1. List of Several File Samples for Odd-Even Labels and Hash Values

File Type	File Real Name	MD5 Value
Document	D:\DOCX 1.docx	6db984ae2628503104cb46fab8b9ef8c
	D:\DOCX 2.docx	6db984ae2628503104cb46fab8b9ef8c
	D:\XLSX 1.xlsx	56c424725531715f142e77ccc5cee774
	D:\XLSX 2.xlsx	56c424725531715f142e77ccc5cee774
	D:\TXT 1.txt	6bb11f42a5b591be9ec1a0e95a5cd00c
	D:\TXT 2.txt	6bb11f42a5b591be9ec1a0e95a5cd00c
Video	D:\3GP 1.3gp	cd5f422a723609bff58c699704f91d88
	D:\3GP 2.3gp	cd5f422a723609bff58c699704f91d88
	D:\AVI 1.avi	72562d25302f0698c19040a6d50ceb0c
	D:\AVI 2.avi	72562d25302f0698c19040a6d50ceb0c
Image	D:\GIF 1.gif	ed28cc871584230543b5a2d8a386a2cb
	D:\GIF 2.gif	ed28cc871584230543b5a2d8a386a2cb
Music	D:\MP3 1.mp3	d004ad9c716fbb7262d09fcd812b7bdb
	D:\MP3 2.mp3	d004ad9c716fbb7262d09fcd812b7bdb
Application	D:\MASTER 1.exe	562f2ea6e41020fd7bf5426bd77cd59c
	D:\MASTER 2.exe	562f2ea6e41020fd7bf5426bd77cd59c
Zip	D:\ZIP 1.zip	47cf035aa29599823cce99bef2467330
	D:\ZIP 2.zip	47cf035aa29599823cce99bef2467330
7z	D:\7Z 1.7z	e2d9c0b0a82113ce52d5334ffd24a876
	D:\7Z 2.7z	e2d9c0b0a82113ce52d5334ffd24a876

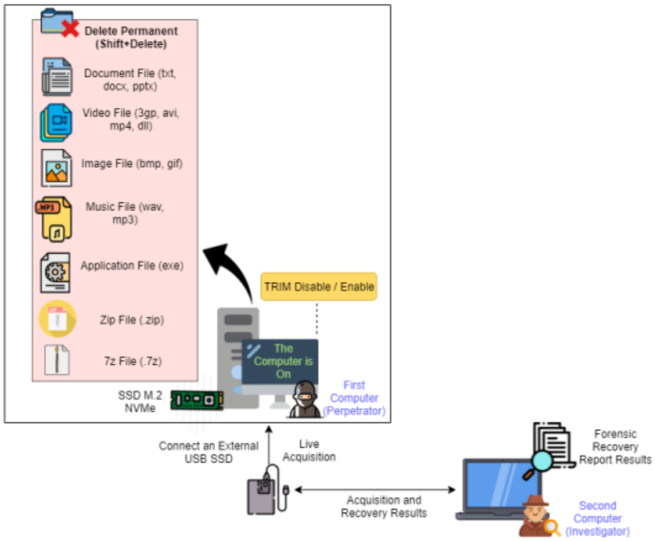

Delete Permanent (Shift+Delete)
Document File (txt, docx, pptx)
Video File (3gp, avi, mp4, dll)
Image File (bmp, gif)
Music File (wav, mp3)
Application File (exe)
Zip File (.zip)
7z File (.7z)
TRIM Disable / Enable
The Computer is On
SSD M.2 NVMe
First Computer (Perpetrator)
Connect an External USB SSD
Live Acquisition
Acquisition and Recovery Results
Forensic Recovery Report Results
Second Computer (Investigator)

Figure 4. SSD NVMe Live Forensics Recovery Scenario

3. Results and Discussion

3.1 Result

This research was conducted with the live forensics method using an external USB SSD to perform live acquisition of the NVMe SSD TRIM function. This was done to avoid damage and loss of digital evidence on the NVMe SSD TRIM function. Based on the predetermined scenario, the investigator performed extraction from the result of the NVMe SSD TRIM disabled and enabled function using Autopsy and Belkasoft tools.

3.1.1 Preparation

At this stage, the acquisition of digital evidence contained in the NVMe SSD was performed using tools which support live forensics techniques such as Portable FTK Imager. Stage of live forensic techniques was carried out to obtain files that had been permanently deleted in the SSD NVMe using TRIM disabled and enabled function. The live forensics tools used in this study was Portable FTK Imager. Since Portable FTK Imager could retrieve data and information files that had been deleted, it could support live forensics techniques. Figure 5(a) and Figure 5(b) below is the documentation result of the live forensics imaging process TRIM disabled and TRIM enabled using Portable FTK Imager. Table 2 shows the results of the imaging process and MD5 hash value. The purpose of the imaging process was to avoid damage to the original digital evidence contained in the NVMe SSD when the analysis process was performed.

Drive/Image Verify Results	
Name	Imaging TRIM Disable.001
Sector count	250067790
MD5 Hash	
Computed hash	5e7d9c116485b5ae0c630b987267d122
Report Hash	5e7d9c116485b5ae0c630b987267d122
Verify result	Match
SHA1 Hash	
Computed hash	859d71959360a8ee192f6b6f2e572202
Report Hash	859d71959360a8ee192f6b6f2e572202
Verify result	Match
Bad Sector List	
Bad sector (s)	No bad sectors found

(a)

Drive/Image Verify Results	
Name	Imaging TRIM Enable.001
Sector count	250067790
MD5 Hash	
Computed hash	4cd76afba35e3ad940de210411c6ca30
Report Hash	4cd76afba35e3ad940de210411c6ca30
Verify result	Match
SHA1 Hash	
Computed hash	d2198208aec4b6bf001e53a14124d8a32
Report Hash	d2198208aec4b6bf001e53a14124d8a32
Verify result	Match
Bad Sector List	
Bad sector (s)	No bad sectors found

(b)

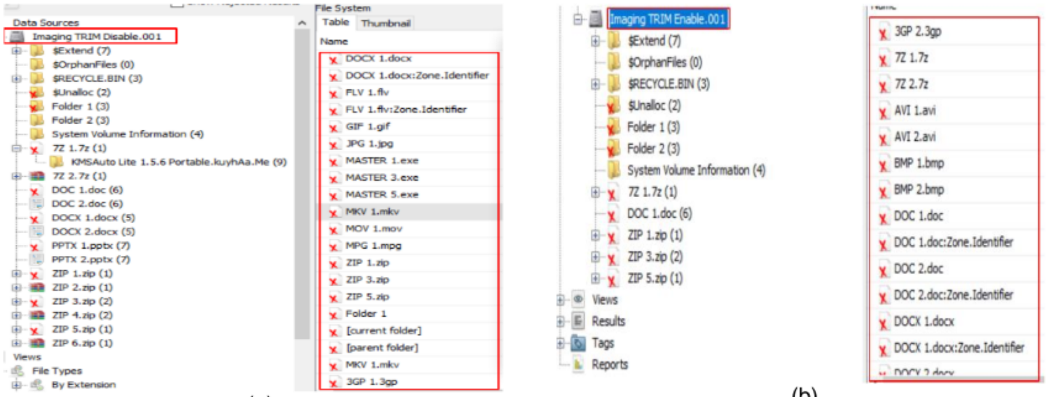
Figure 5. Imaging Results Portable FTK Imager (a) TRIM Disabled, (b) TRIM Enabled

Table 2. Acquisition Results of NVMe SSD TRIM function using Portable FTK Imager

No	Name Drive Imaging	MD5 Value	Acquisition Proses (Time)
a	Imaging TRIM Disable	5e7d9c116485b5ae0c630b987267d122	50 minute 46 seconds
b	Imaging TRIM Enable	4cd76afba35e3ad940de210411c6ca30	50 minute 44 seconds

3.1.2 Extraction

At this stage, the researchers extracted the imaging file. This process aimed to extract the imaging result. In order to maintain the integrity and authenticity of the evidence, the extraction was performed on the duplicates of the imaging result. The tools that helped the process of examination extraction and imaging analysis were Autopsy and Belkasoft. Figure 6 is a check using the Sleuthkit Autopsy tool which shows erased digital evidence, Figure 6(a) TRIM Disabled and Figure 6(b) TRIM Enabled.



Data Sources
Imaging TRIM Disable.001
$Extend (7)
$OrphanFiles (0)
$RECYCLE.BIN (3)
$Unalloc (2)
Folder 1 (3)
Folder 2 (3)
System Volume Information (4)
7Z 1.7z (1)
KMSAuto Lite 1.5.6 Portable.kuyhAa.Me (9)
7Z 2.7z (1)
DOC 1.doc (6)
DOC 2.doc (6)
DOCX 1.docx (5)
DOCX 2.docx (5)
PPTX 1.pptx (7)
PPTX 2.pptx (7)
ZIP 1.zip (1)
ZIP 2.zip (1)
ZIP 3.zip (2)
ZIP 4.zip (2)
ZIP 5.zip (1)
ZIP 6.zip (1)
Views
File Types
By Extension

File System
Table Thumbnail
Name
DOCX 1.docx
DOCX 1.docx:Zone.Identifier
FLV 1.flv
FLV 1.flv:Zone.Identifier
GIF 1.gif
JPG 1.jpg
MASTER 1.exe
MASTER 3.exe
MASTER 5.exe
MKV 1.mkv
MOV 1.mov
MPG 1.mpg
ZIP 1.zip
ZIP 3.zip
ZIP 5.zip
Folder 1
[current folder]
[parent folder]
MKV 1.mkv
3GP 1.3gp

(a)

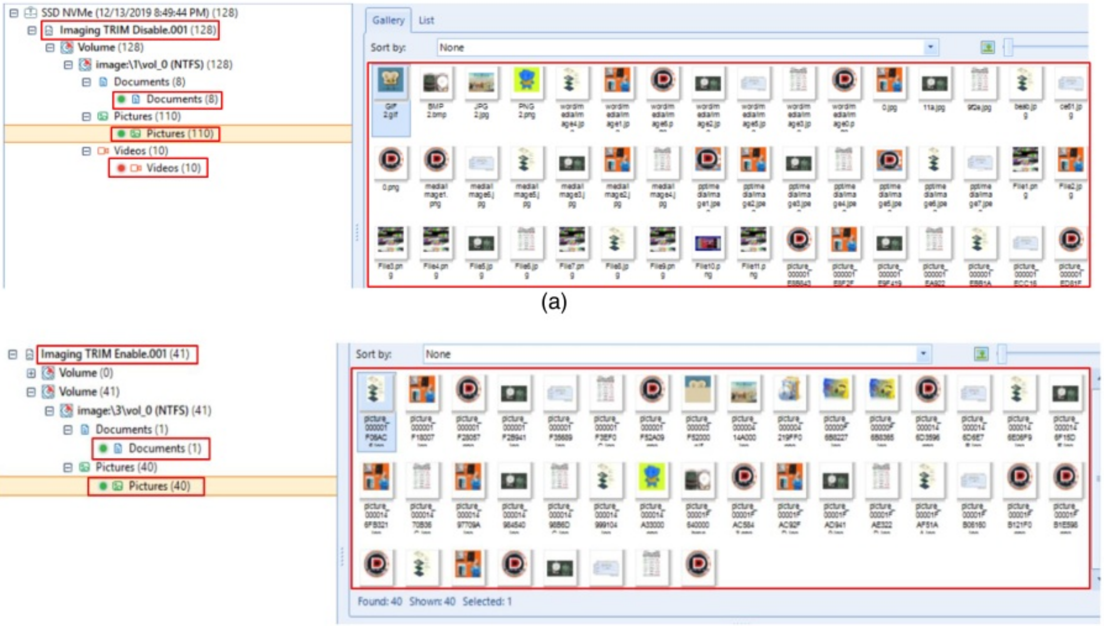
Imaging TRIM Enable.001
$Extend (7)
$OrphanFiles (0)
$RECYCLE.BIN (3)
$Unalloc (2)
Folder 1 (3)
Folder 2 (3)
System Volume Information (4)
7Z 1.7z (1)
DOC 1.doc (6)
ZIP 1.zip (1)
ZIP 3.zip (2)
ZIP 5.zip (1)
Views
Results
Tags
Reports

3GP 2.3gp
7Z 1.7z
7Z 2.7z
AVI 1.avi
AVI 2.avi
BMP 1.bmp
BMP 2.bmp
DOC 1.doc
DOC 1.doc:Zone.Identifier
DOC 2.doc
DOC 2.doc:Zone.Identifier
DOCX 1.docx
DOCX 1.docx:Zone.Identifier
DOCX 2.docx

(b)

Figure 6. Examination of File List of Using Sluekit Autopsy Tool (a) TRIM Disabled, (b) TRIM Enabled

Figure 7 is an examination using the Belkasoft Tool which shows erased digital evidence, Figure 7(a) TRIM Disabled and Figure 7(b) TRIM Enabled.



```
⊟ SSD NVMe (12/13/2019 8:49:44 PM) (128)
  ⊟ Imaging TRIM Disable.001 (128)
    ⊟ Volume (128)
      ⊟ image:\1\vol_0 (NTFS) (128)
        ⊟ Documents (8)
            ● Documents (8)
        ⊟ Pictures (110)
            ● Pictures (110)
        ⊟ Videos (10)
            ● Videos (10)
```

(a)

```
⊟ Imaging TRIM Enable.001 (41)
  ⊞ Volume (0)
  ⊟ Volume (41)
    ⊟ image:\3\vol_0 (NTFS) (41)
      ⊟ Documents (1)
          ● Documents (1)
      ⊟ Pictures (40)
          ● Pictures (40)
```

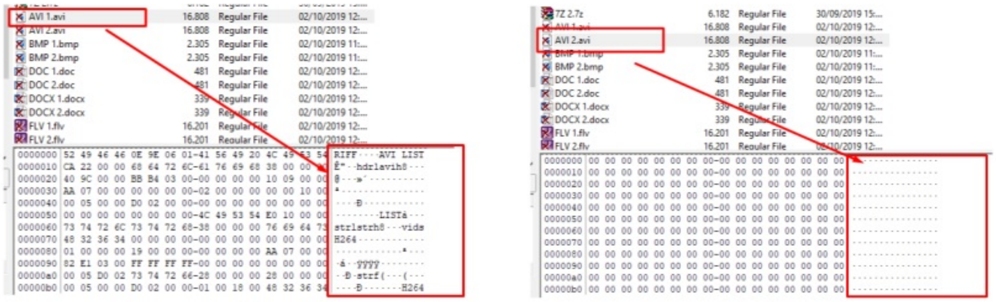
(b)

Figure 7. Examination of File List of Using Belkasoft Tool (a) TRIM Disabled, (b) TRIM Enabled

Based on the results of examination using the Sluetkit Autopsy tool on the TRIM disable function, odd labels could be recovered perfectly while none of the TRIM enabled even labels files could be recovered. Meanwhile, according to the results of examination using Belkasoft tools, none of the odd label TRIM disabled files could be recovered perfectly because these files were separated while only two TRIM enabled even label files could be recovered, but the file name and MD5 hash value were not the same as the original.

3.1.3 Analysis

At this stage, the analysis of the acquisition result was performed by Portable FTK imager. In this stage the value of the signature file that had been deleted by the TRIM disabled and enabled function was found. Signature file was a data information value used to identify content of the data [24][25]. Figure 8(a) is TRIM disabled shows that the signature of the odd label file was not damaged. Therefore, it could be concluded that the odd label file could be read and recovered. Meanwhile, Figure 8(b) is TRIM enabled shows that the signature of the even label file was damaged or modified, so the file could not be recovered.



```
AVI 1.avi      16.808  Regular File  02/10/2019 12:...
AVI 2.avi      16.808  Regular File  02/10/2019 12:...
BMP 1.bmp       2.305  Regular File  02/10/2019 11:...
BMP 2.bmp       2.305  Regular File  02/10/2019 11:...
DOC 1.doc         481  Regular File  02/10/2019 12:...
DOC 2.doc         481  Regular File  02/10/2019 12:...
DOCX 1.docx       339  Regular File  02/10/2019 12:...
DOCX 2.docx       339  Regular File  02/10/2019 12:...
FLV 1.flv      16.201  Regular File  02/10/2019 12:...
FLV 2.flv      16.201  Regular File  02/10/2019 12:...
0000000  52 49 46 46 0E 9E 06 01-41 56 49 20 4C 49 53 54  RIFF····AVI LIST
0000010  CA 22 00 00 68 64 72 6C-61 76 69 68 38 00 00 00  Ê"··hdrlavih8···
0000020  40 9C 00 00 BB B4 03 00-00 00 00 00 10 09 00 00  @···»´··········
0000030  AA 07 00 00 00 00 00 00-02 00 00 00 00 00 10 00  ª···············
0000040  00 05 00 00 D0 02 00 00-00 00 00 00 00 00 00 00  ····Ð···········
0000050  00 00 00 00 00 00 00 00-4C 49 53 54 E0 10 00 00  ········LISTà···
0000060  73 74 72 6C 73 74 72 68-38 00 00 00 76 69 64 73  strlstrh8···vids
0000070  48 32 36 34 00 00 00 00-00 00 00 00 00 00 00 00  H264············
0000080  01 00 00 00 19 00 00 00-00 00 00 00 AA 07 00 00  ············ª···
0000090  82 E1 03 00 FF FF FF FF-00 00 00 00 00 00 00 00  ·á··ÿÿÿÿ········
00000a0  00 05 D0 02 73 74 72 66-28 00 00 00 28 00 00 00  ··Ð·strf(···(···
00000b0  00 05 00 00 D0 02 00 00-01 00 18 00 48 32 36 34  ····Ð·······H264
```

(a)

```
7Z 2.7z         6.182  Regular File  30/09/2019 15:...
AVI 1.avi      16.808  Regular File  02/10/2019 12:...
AVI 2.avi      16.808  Regular File  02/10/2019 12:...
BMP 1.bmp       2.305  Regular File  02/10/2019 11:...
BMP 2.bmp       2.305  Regular File  02/10/2019 11:...
DOC 1.doc         481  Regular File  02/10/2019 12:...
DOC 2.doc         481  Regular File  02/10/2019 12:...
DOCX 1.docx       339  Regular File  02/10/2019 12:...
DOCX 2.docx       339  Regular File  02/10/2019 12:...
FLV 1.flv      16.201  Regular File  02/10/2019 12:...
FLV 2.flv      16.201  Regular File  02/10/2019 12:...
0000000  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000010  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000020  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000030  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000040  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000050  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000060  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000080  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0000090  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00000a0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00000b0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

(b)

Figure 8. Analysis Stage (a) Odd Label TRIM Disabled, (b) Even Label TRIM Enabled

The results of file recovery analysis summarized in Table 3 and Table 4 show the analysis result of the TRIM disabled and enabled file recovery processes that has been performed using the Sleutkit Autopsy tool.

Table 3. List of Analysis and Recovery of Odd Label TRIM Disabled Files with Sleutkit Autopsy Tool

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

The result of the odd label TRIM disabled files analysis indicates that based on the authenticity of the evidence by analyzing the file using Autopsy, it could be assumed that all of the odd label files had an MD5 hash value that was identical or in other words, the integrity of the evidence was maintained.

Table 4. List of Analysis and Recovery of Even Label TRIM Enabled Files with Sleut Kit Autopsy Tool

File Name Recovery Results	MD5 Value	Information
DOCX 1.docx	6db984ae2628503104cb46fab8b9ef8c	Successful recovery
DOCX 2.docx	821d1ae6d9543f57e95a82c26fcbcbb6	Corrupted file
XLSX 1.xlsx	6bb11f42a5b591be9ec1a0e95a5cd00c	Successful recovery
XLSX 2.xlsx	c4e4f86f732fd5873e050500e18bb414	Corrupted file
TXT 1.txt	6bb11f42a5b591be9ec1a0e95a5cd00c	Successful recovery
TXT 2.txt	9ba601b1c111c9ebc50b523d09ea5f21	Corrupted file
3GP 1.3gp	cd5f422a723609bff58c699704f91d88	Successful recovery
3GP 2.3gp	299e23fd97392eae859b7117dfb91634	Corrupted file
AVI 1.avi	72562d25302f0698c19040a6d50ceb0c	Successful recovery
AVI 2.avi	a13a97acca90cce38197742e79ebd152	Corrupted file
GIF 1.gif	ed28cc871584230543b5a2d8a386a2cb	Successful recovery
GIF 2.gif	-	Corrupted file
MP3 1.mp3	d004ad9c716fbb7262d09fcd812b7bdb	Successful recovery
MP3 2.mp3	255f0e8c535c187b3e13adb241eae315	Corrupted file
MASTER 1.exe	562f2ea6e41020fd7bf5426bd77cd59c	Successful recovery
MASTER 2.exe	a6e1964dd6a7e6d0498522db4c157335	Corrupted file
ZIP 1.zip	47cf035aa29599823cce99bef2467330	Successful recovery
ZIP 2.zip	9ba7bb2ab23acedeedb3b9207f51d2c0	Corrupted file
7Z 1.7z	e2d9c0b0a82113ce52d5334ffd24a876	Successful recovery
7Z 2.7z	d184ed7759220cb6d86fae5cb6965174	Corrupted file

All files with odd labels had been successfully recovered without any damage while all the even labels could not be recovered. The odd label file that had been deleted on the TRIM disabled function could be recovered perfectly. Thus, it can be concluded that when deletion of odd label files is done in a disabled state, recovery can be performed perfectly. Meanwhile, because the even label file was deleted when TRIM was enabled, the even label file could not be fully recovered.

Table 5 and Table 6 show the results of analysis and recovery of the TRIM disabled and enabled files using Belkasoft tool.

Table 5. List of Analysis and Recovery of Odd Label TRIM Disabled Files with Belkasoft Tool

File Name Recovery Results	MD5 Value	Information
DOCX 1.docx	-	Corrupted file
XLSX 1.xlsx	-	Corrupted file
TXT 1.txt	-	Corrupted file

3GP 1.3gp	-	Corrupted file
AVI 1.avi	-	Corrupted file
picture_00000414A000.jpg	d4fc57bddd2ed31d53f00002791a245d	Successful recovery
picture_000003F52000.gif	7ac62754ea19fc0fede4f2f902a9be94	Corrupted file
picture_000014A33000.png	ecec4d4b31f17d5123552f4e4cb25edd	Successful recovery
picture_00001F640000.bmp	8cad97ecf36337caebedd53fd81258dd	Successful recovery
MP3 1.mp3	-	Corrupted file
MASTER 1.exe	-	Corrupted file
ZIP 1.zip	-	Corrupted file
7Z 1.7z	-	Corrupted file

Table 6. List of Analysis and Recovery of Even Label TRIM Enabled Files with Belkasoft Tool

File Name Recovery Results	MD5 Value	Information
document_000001F02000.docx	6db984ae2628503104cb46fab8b9ef8c	Successful recovery
MKV1. mkv	081988e8c44e575b84cda8934058e9b	Corrupted file
XLSX 1.xlsx	-	Corrupted file
XLSX 2.xlsx	-	Corrupted file
TXT 1.txt	-	Corrupted file
TXT 2.txt	-	Corrupted file
3GP 1.3gp	-	Corrupted file
3GP 2.3gp	-	Corrupted file
AVI 1.avi	-	Corrupted file
AVI 2.avi	-	Corrupted file
picture_000003F52000.gif	7ac62754ea19fc0fede4f2f902a9be94	Corrupted file
picture_00001F640000.bmp	8cad97ecf36337caebedd53fd81258dd	Successful recovery
MP3 1.mp3	-	Corrupted file
MP3 2.mp3	-	Corrupted file
MASTER 1.exe	-	Corrupted file
MASTER 2.exe	-	Corrupted file
ZIP 1.zip	-	Corrupted file
ZIP 2.zip	-	Corrupted file
7Z 1.7z	-	Corrupted file
7Z 2.7z	-	Corrupted file

At the examination and recovery analysis stage with the Belkasoft tools, recovery on the files that had been permanently deleted by TRIM disabled function could be performed on files with .jpg, .png, and .bmp. extension type. However, the name labels changed into picture_00000414A000.jpg, picture_000003F52000.gif, picture_000014A33000.png, and picture_00001F640000.bmp. It was found that only image files could be recovered. Meanwhile, among the TRIM enabled function files, there were only two files that could be recovered and the file names were not the same as the original, namely document_000001F02000.docx and picture_00001F640000.bmp.

3.2 Discussion

SSD has several features including TRIM disabled and enabled features. The TRIM feature works to identify blocks considered to be obsolete and delete remaining data internally. The TRIM feature poses challenges for investigators in obtaining digital evidence. There are several studies examining TRIM features including acquisition of the TRIM function on SSD using the static method. The purpose of the research is to obtain digital evidence that has been permanently deleted when the TRIM feature is disabled or enabled. The research found that the implementation of the TRIM disabled function could not recover the entire file that had been permanently deleted with the Sluetkit Autopsy tool and that it took 12 hours 24 minutes to check, while TRIM enabled could not recover all files with the Sluetkit Autopsy tool and the process required 13 hours 25 minutes to complete. Therefore, live forensics method is able to improve data recovery results from the TRIM function. Data handling on the SSD must be performed quickly because the data will be lost if the system shut off. The result obtained regarding the TRIM disable function in this study indicates that overall the file could be recovered using the Sluetkit Autopsy tool perfectly and the hash value of the file did not change. The live acquisition of TRIM disabled using FTK Portable Imager tool took 50 minutes 46 seconds. As for the TRIM enabled, the file could be recovered entirely with the Sluetkit Autopsy tool, but the files were corrupted and the hash values were not identical. The live acquisition of TRIM enabled using the FTK Portable Imager tool took 50 minutes 44 seconds.

Based on information collected and described according to the methods and scenarios implemented in this study, it is evident that the TRIM function poses problems and challenges for digital forensics investigators. This is because the TRIM function has a negative influence, that is, TRIM can affect data recovery when TRIM is enabled on the operating system. As a result, the TRIM function will delete data considered to be obsolete and delete the remaining data internally. Technology on SSD storage media has a negative impact, especially in forensic analysis to find information and understand data stored on SSD storage media. It supports the fact that SSD is a challenge for forensic analysis [26].

4. Conclusion

Based on the results of the study, live forensic technique can be applied to the acquisition on the NVMe SSD TRIM function on a professional Windows 10 operating system. The process of examination and analysis on SSD were performed with both TRIM disabled and enabled. The percentage of recovery TRIM disabled uses 100% Autopsy tools, Belkasoft 3%. While the TRIM recovery percentage is enabled using the 99% odd label Autopsy tools and even 0% labels, Belkasoft odd labels 2% and even 0% labels. This research found that in the process of recovery, TRIM disabled could maintain the integrity of the evidence. This is indicated by the identical hash value on the original file and the recovery file. On the contrary, the files with TRIM enabled were damaged and could not be recovered. Moreover, the files are not identical to the original file, so the integrity of evidence was not guaranteed.

For further research, it is recommended to test the implementation of TRIM functions in other operating systems such as iOS and Linux, using different file systems such as ExFat, ReFS and so on, as well as exploring deletion methods, SSD handling methods, and tools used to perform file recovery in digital forensics field.

References

[1] Dwi, "Laporan Dwi Bulan I 2014," Incident Monitoring Report, Pp. 1–9, 2018.

[2] M. Nuh Al-Azhar, Digital Forensic Practical Guildelines for Computer Investigation, No. c. 2012.

[3] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ)," *Elinvo (Electronics, Informatics, and Vocational Education)*, Vol. 3, No. 1, Pp. 70–82, 2018. https://doi.org/10.21831/elinvo.v3i1.19308

[4] R. A. Ramadhan, Y. Prayudi, and B. Sugiantoro, "Implementasi dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive (SSD)," 2016.

[5] B. Nikkel, "NVM express drives and digital forensics," *Digital Investigation*, Vol. 16, Pp. 38–45, 2016. https://doi.org/10.1016/j.diin.2016.01.001

[6] Q. Xu *et al.*, "Performance Analysis of NVMe SSDs and their Implication on Real World Databases," *SYSTOR 2015 - Proceedings of the 8th ACM International Systems and Storage Conference*, 2015. https://doi.org/10.1145/2757667.2757684

[7] R. Hubbard, "Forensics Analysis of Solid State Drive (SSD)," Pp. 1–11, 2016.

[8] F. Geier, "The differences between SSD and HDD technology regarding forensic investigations," Pp. 67, 2015.

[9] R. K. Chaurasia and P. Sharma, "Solid State Drive (SSD) Forensics Analysis : A New Challenge," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, Vol. 6, No. 2, Pp. 1081–1085, 2017.

[10] Statista, "Shipments of Hard and Solid State Disk (HDD/SSD) Drives Worldwide From 2015 to 2021."

[11] M. N. Al-Azhar, "The Essentials of Digital Forensic," 2016.

[12] Y. Prayudi, "Problema dan Solusi Digital Chain of Custody," Senasti - Seminar Nasional Sains dan Teknologi Informasi, No. 2011, 2014.

[13] Soni, D. Sudyana, Y. Prayudi, H. Mukhtar, and B. Sugiantoro, "Server Virtualization Acquisition Using Live Forensics Method," *Advances in Engineering Research*, Vol. 190, Pp. 18–23, 2019. https://dx.doi.org/10.2991/iccelst-st-19.2019.4

[14] D. Sudyana and N. Lizarti, "Digital Evidence Acquisition System on IAAS Cloud Computing Model using Live Forensic Method," *Scientific Journal of Informatics*, Vol. 6, No. 1, Pp. 125–137, 2019. https://doi.org/10.15294/sji.v6i1.18424

[15] I. Riadi and M. E. Rauli, "Live forensics analysis of line app on proprietary operating system," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, Vol. 4, No. 4, Pp. 305–314, 2019. https://doi.org/10.22219/kinetik.v4i4.850

[16] J. Arulraj and A. Pavlo, "How to Build a Non-Volatile Memory Database Management System," *Proceedings of the ACM SIGMOD International Conference on Management of Data*, Vol. Part F1277, Pp. 1753–1758, 2017. https://doi.org/10.1145/3035918.3054780

[17] M. Rafique and M. N. A. Khan, "Exploring Static and Live Digital Forensics: Methods, Practices and Tools," *International Journal of Scientific & Engineering Research*, Vol. 4, No. 10, Pp. 1048–1056, 2013.

[18] A. Nisbet, S. Lawrence, and M. Ruff, "A Forensic Analysis and Comparison of Solid State Drive Data Retention With Trim Enabled File Systems," *Australian Digital Forensics Conference*, P p. 10, 2013. https://doi.org/10.4225/75/57b3d766fb873

[19] A. Faiz and R. Imam, "Forensic Analysis of 'Frozen' Hard Drive Using Deep Freeze Method," No. March, 2017.

[20] A. Hadi and S. Riadi, Imam, "Forensik Bukti Digital Pada Solid State Drive (SSD) NVMe Menggunakan Metode National Institute Standards and Technology (NIST)," Pp. 551–558, 2019.

[21] D. S. Yudhistira, "Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop," 2018.

[22] S. Rahman and M. N. A. Khan, "Review of Live Forensic Analysis Techniques," *International Journal of Hybrid Information Technology*, Vol. 8, No. 2, Pp. 379–388, 2015. https://doi.org/10.14257/ijhit.2015.8.2.35

[23] B. S. Nasional, "Teknologi Informasi – Teknik Keamanan – Pedoman Identifikasi, Pengumpulan Akuisisi, dan Preservasi Bukti Digital," in *SNI 27037:2014*, Jakarta, 2014.

[24] D. Jeong and S. Lee, "Forensic signature for tracking storage devices: Analysis of UEFI firmware image, disk signature and windows artifacts," *Digital Investigation*, Vol. 29, Pp. 21–27, 2019, https://doi.org/10.1016/j.diin.2019.02.004

[25] K. Gary, "File Signature."

[26] Y. Gubanov and O. Afonin, "Recovering Evidence from SSD Drives: Understanding TRIM, Garbage Collection, and Exclusions," 2014.

HASIL CEK_60020397_Point-C36-IRD-850GB-Live forensics method for acquisition on the Solid State Drive (SSD) NVMe TRIM function

ORIGINALITY REPORT

9%	8%	2%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	kinetik.umm.ac.id Internet Source	6%
2	Submitted to University of New England Student Paper	1%
3	Submitted to Melbourne Institute of Technology Student Paper	1%
4	pdfs.semanticscholar.org Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		