Implementation of Live Forensic Method on Fusion Hard Disk Drive (HDD) and Solid State Drive (SSD) RAID 0 Configuration TRIM Features

Desti Mualfah[1*], Rizdqi Akbar Ramadhan[2], Muhammad Arrafi Arrasyid[3]

[1,3]Department of Informatics, Universitas Muhammadiyah Riau, Indonesia
[2]Department of Informatics, Universitas Islam Riau, Indonesia

*corr_author: destimualfah@umri.ac.id

Abstract - One of the solutions used for access speeds is to maximize non-volatile storage functions by a conventional Hard Disk Driver with Solid State Drive that has the TRIM architecture using the Redundant Array of Inexpensive Disks 0 configuration or the commonly known RAID 0. RAID 0 is a stripping technique that has the highest speed among other RAID configurations. However, this configuration has a disadvantage in that when there is damage to one of the storage disks all the data will be corrupted and lost. It's becoming one of the challenges in digital forensic investigation when it comes to computer crime. Furthermore, this research uses experimental practices using live forensic methods to perform analysis and examination against the merger of HDD and SSD configuration RAID 0 TRIM features. The expected is an overview of the characteristics of recovery capability to find out the authenticity integrity values of files that have been lost or permanently deleted on both TRIM SSD functions disable and enable. Furthermore, this research is expected to be a solution for the experimental and practical investigation of computer crime especially in Indonesia given the increasing development of technology that is directly compared with the rise in computer crime.

Keywords: HDD, SSD, RAID 0, live forensic, recovery file

I. INTRODUCTION

Computer crime is directly proportional to technological developments. The more sophisticated technology is implemented, the higher and easier it is for the practices of cybercrime to be contraindicated against the investigation of computer crimes in finding the obstacles. Cybercrime can be through social media services, or communication devices such as mobile phones, smartphones, PCs, or other computer users [1].

Computer crime has electronic evidence and digital evidence of a crime in the form of traces of criminal activity, it is necessary to analyze the digital evidence obtained using forensic science and methods [2]. In the field of technology, forensic analysis of digital or electronic evidence is called computer forensics [3]. One of the forensic computers is in the form of storage media (storage device), storage devices have two types of storage, namely volatile memory and non-volatile memory (NVM) [4].

The main forms of non-volatile storage media are Hard Disk Drives (HDD) and Solid State Drive (SSD). HDD has the issue of reliability against shocks, this is because the HDD architecture uses a mechanical system [5][6] where there is the essence of fundamental memory architecture, namely: a rotating disk and a magnetic head that reads data on the disk.

While SSD has a fast data access speed technology compared to HDD. Currently, SSDs are replacing HDDs in the storage media [7]. It is explained that SSD as the main storage medium for computers has a feature called TRIM. In previous research [8] the TRIM feature allows the OS (Operating System) to instruct the SSD regarding which blocks are no longer used. So that when it is written, there is no need to do the deletion process first. The TRIM feature helps to maintain good write performance on SSD drives. The TRIM function deletes blocks that have been marked for deletion by the operating system. According to digital forensics [9], the contradiction of using SSD with its TRIM feature is that the TRIM function hurts forensic analysis, especially in data recovery, on the integrity value of the authenticity of data that has been lost or deleted. Furthermore, deletions are not guaranteed to be recovered as the memory controller system of the SSD decides when and how many blocks are marked for deletion. From previous experiments, it can be seen that the TRIM function has always been a challenge in data recovery [10].

The solution to making the most of these two types of non-volatile memory with different architectures is to perform an HDD and SSD fusion technique using RAID (Redundant Array of Inexpensive Disks) 0 to combine data stored on disk architectures that represent the combination of multiple physical disks into one logical unit. The final results that have been proven by previous research [11] show this method is proven to make performance faster [12], but on the other hand, there is a big question of whether RAID 0 with the TRIM function can be easily carried out live forensic methods that refer to the SNI 27037: 2014 standard in the process of digital forensic investigation of HDD and SSD fusion RAID 0 configuration TRIM feature or has obstacles or challenges that will be proven in this experiment in the data recovery process when cybercrime practices occur. To prove the hypothesis that has been described in the previous sentence, it is necessary to support the software (forensic tools) [13] used in this study are FTK Imager Portable, Sleuth Kit Autopsy, and Recovery Testdisk. This tool is used for investigations in recovering data regarding the integrity value of the authenticity of data that is lost or permanently deleted in the implementation of fusion HDD and SSD RAID 0 TRIM disable and enable functions. The output of this research is a table of data recovery results regarding the integrity value of the authenticity of data that has been lost or permanently deleted on the fusion HDD and SSD RAID 0 TRIM disable and enable functions using the live forensic method for the data recovery process.

II. METHOD

This section explains how researchers apply the live forensic method in recovering HDD and SSD fusion data with RAID 0 configurations with TRIM features based on the guidelines and requirements in the Indonesian National Standard (SNI) 27037:2014 [14]-[15]. These stages can be seen in Fig. 1.

Some previous studies have used live forensic acquisition procedures in accordance with SNI 27037:2014. In the guidelines of SNI 27037:2014, which can provide optimal results in solving the case under study. It is explained that the steps that must be taken for the acquisition process, namely the first is to determine the type of acquisition used, determine the type of data obtained, perform the acquisition procedure, perform the procedure of the data obtained by the seal for the hashing process with MD5 then verify the authenticity of the acquisition file. Fig. 2 shows the stages of examination and analysis that will be carried out to complete this research.

- Preparation stages: Make preparations by providing storage space to store the data to be recovered and extracted.
- Extraction stages: Performing file extraction by identifying and recovering files that have been deleted. File extraction will also reveal the characteristics of the file structure, deleted data, file name, file size, and location.
- Analysis stages: The stage of analysis is the results of files that have been examined. So that it can measure the effectiveness of the TRIM function file extraction disable or enable.

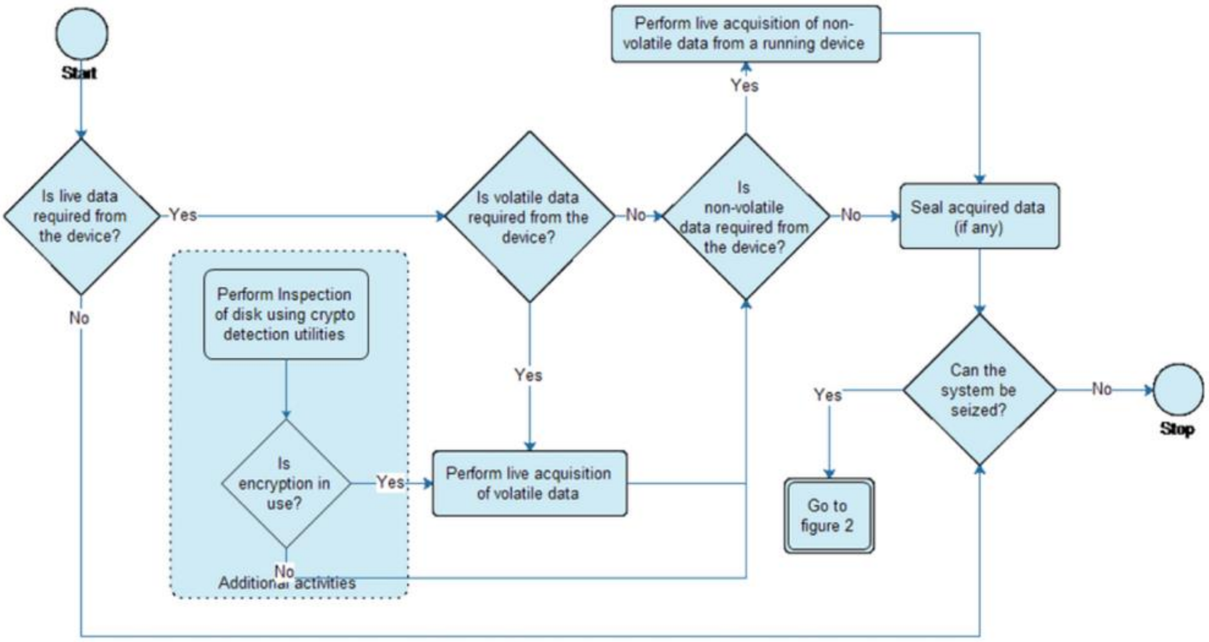

Start
Is live data required from the device?
Yes
No
Is volatile data required from the device?
No
Yes
Is non-volatile data required from the device?
Yes
No
Perform live acquisition of non-volatile data from a running device
Seal acquired data (if any)
Can the system be seized?
No
Stop
Yes
Go to figure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

Fig. 1 SNI acquisition procedure

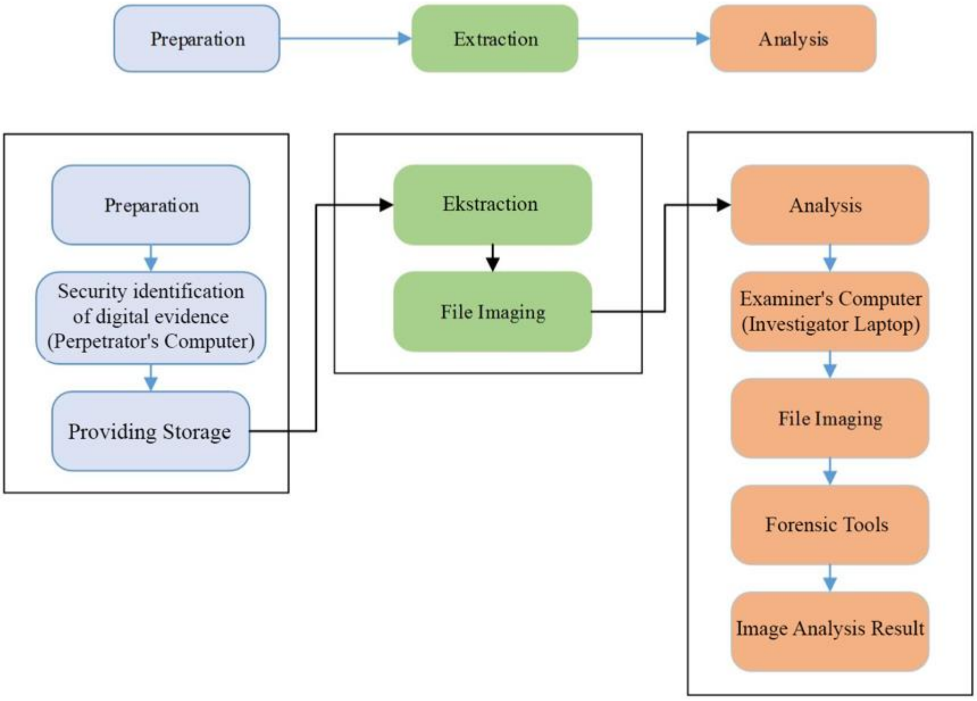


Fig. 2 Examination and analysis stages

A. *System Preparation and Forensic Tools*

It is a stage in preparing hardware and software specifications used in this research such as fusion HDD and SSD RAID 0 configuration and implementation of Non-Vollatille memory analysis used as the object of research [16]. While the forensic tools used are FTK Imager Portable and Testdisk Recovery.

The first step is to prepare the system that will be used in the Live acquisition and Recovery process. The first step is to prepare computer specifications and other supporters to conduct this research. Equipment that needs to be prepared in the form of Table I.

From Table I, then combining (fusion) HDD and SSD RAID 0 configuration techniques by configuring the BIOS and setting the SATA controller by changing from Native IDE to RAID via the F10 command to save it. The following is the process of booting RAID in BIOS, then executing the command (CTRL + F) simultaneously so that the RAID 0 configuration process is successful. Fig. 3 which shows the results of the RAID 0 configuration.

TABLE I
HARDWARE AND SOFTWARE USAGE SPECIFICATIONS

No.	Hardware/Software	Description
1	Personal Computer offender (First Computer)	Hardware
2	HP Pavilion g4 series laptop (Second Computer)	Hardware
3	Solid State Drive (SSD) Kingston SA400S37 120 GB	Hardware Storage
4	Hard Disk Drive (HDD) WDC WD1600BEVT 160 GB	Hardware Storage
5	RAID 0 Configuration in the BIOS of the Performer Computer	Software BIOS
6	1 TB External Backup Hard Disk Drive (HDD)	Hardware
7	Operating System Windows 10 Professional 64bit architecture	Computer Operating System Performer
8	Operating System Windows 10 Professional 64bit architecture	Investigator Computer Operating System
9	FTK Imager Portable for Windows	Forensic Tools
10	Sleuth Kit Autopsy Forensics for Windows	Forensic Tools
11	Test disk Recovery Portable for Windows	Forensic Tools
12	Hashmyfile	Hashing Tools

Fig. 3 shows that the RAID 0 merger has been successful and obtained 237 GB of storage memory by combining 160 GB of HDD and 120 GB of SSD.

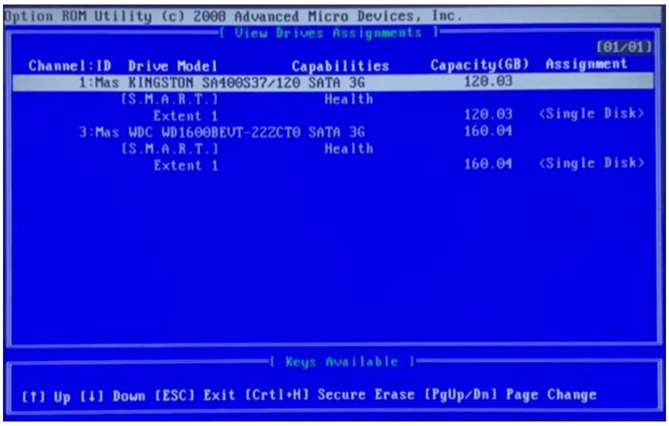
B. Case Simulation (Scenario)

At this stage, the case scenario on storage media fusion HDD and SSD RAID 0 configuration is carried out by deleting files against data stored in storage. The condition of the computer device is found to be on with the storage condition that has been done HDD and SSD fusion with RAID 0 configuration. The following scenario [17] of HDD and SSD in this research scenario can be seen in Fig. 4.

Furthermore, the case scenario with fusion HDD and SSD RAID 0 configuration has 2 stages of simulation as follows:

1) TRIM fusion setting in the form of disabling the TRIM function (TRIM disable) and enabling the TRIM function (TRIM enable). To practice testing the TRIM function on the fusion HDD and SSD RAID 0 configuration, the test file is permanently deleted with the SHIFT + Delete command on both TRIM function settings.

2) Perform live acquisition of fusion HDD and SSD RAID 0 configurations that have been applied to the TRIM function to analyze what files can be recovered after deletion practice. After performing the TRIM function stage, it is carried out to connect the USB External HDD as a medium in performing the backup or imaging process before carrying out the live forensic process of electronic evidence acquisition and live recovery on the perpetrator's computer.



```
Option ROM Utility (c) 2008 Advanced Micro Devices, Inc.
                         [ View Drives Assignments ]
                                                                      [01/01]
  Channel:ID  Drive Model            Capabilities    Capacity(GB)  Assignment
        1:Mas KINGSTON SA400S37/120 SATA 3G             120.03
              [S.M.A.R.T.]             Health
                  Extent 1                              120.03     <Single Disk>
        3:Mas WDC WD1600BEVT-22ZCT0 SATA 3G             160.04
              [S.M.A.R.T.]             Health
                  Extent 1                              160.04     <Single Disk>

                              [ Keys Available ]
 [↑] Up [↓] Down [ESC] Exit [Crtl+H] Secure Erase [PgUp/Dn] Page Change
```

Fig. 3 Storage RAID 0 configuration result

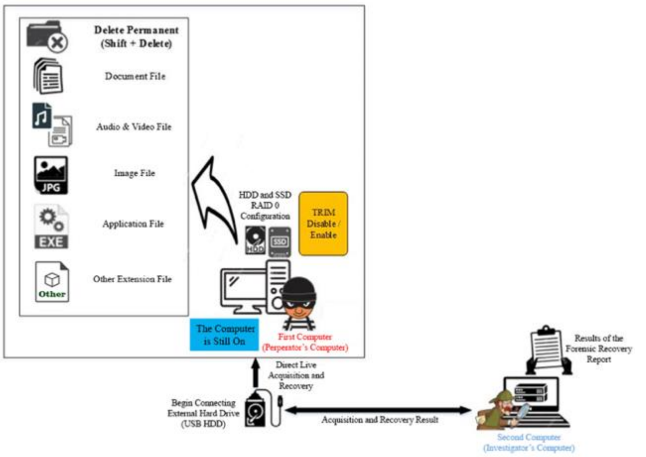

Delete Permanent
(Shift + Delete)
Document File
Audio & Video File
Image File
JPG
Application File
EXE
Other Extension File
Other
HDD and SSD RAID 0 Configuration
HDD
SSD
TRIM Disable / Enable
The Computer is Still On
First Computer (Perpeator's Computer)
Direct Live Acquisition and Recovery
Begin Connecting External Hard Drive (USB HDD)
Acquisition and Recovery Result
Results of the Forensic Recovery Report
Second Computer (Investigator's Computer)

Fig. 4 Fusion HDD and SSD RAID 0 configuration scenario

III. RESULT AND DISCUSSION

The research was carried out by simulating hardware and software packaged in digital forensics. Fundamentally, digital forensics is a theory that directs researchers in this case as a reference. In general, problems/obstacles that are potentially found in real practice will be simulated in this research. Specifically, the results of the research implementation of HDD and SSD fusion RAID 0 configuration is a solution where data is stored on a disk architecture that represents the combination of multiple physical disks into one logical unit. The goal is to improve performance and increase storage capacity.

According to the digital forensic perspective, the contradiction of using an SSD with its TRIM feature [16] has a negative effect on forensic analysis, especially on data recovery regarding the integrity value of the authenticity of data that has been lost or deleted, which means that it is necessary to carry out live forensic techniques in carrying out HDD and SSD fusion analysis. RAID 0 configuration TRIM function which refers to the SNI 27037:2014 standard uses forensic tools Sleuthkit Autopsy and Tesdisk in digital forensic investigations used for data recovery. Furthermore, several samples of original files used in this research experiment are presented in Table II with labels for odd files and even files TRIM disable and enable.

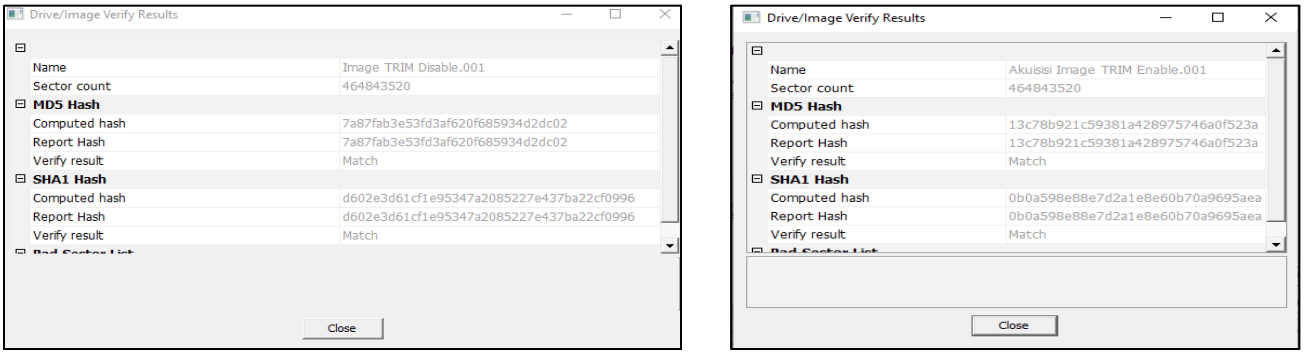
In the simulation case (scenario), the process of activating the TRIM disable and enable functions is carried out by moving files to the D:\ or Data Evidence practitioner. In this research, permanent deletion will be carried out, namely the Data Evidence D:\ partition. In the table above, there are various file type extensions and hash values that will be carried out permanent deletion practices with the SHIFT + DELETE command, to facilitate permanent file deletion, it is necessary to distinguish odd-even file names in order to distinguish TRIM disable or enable file

A. Disable dan enable the TRIM Acquisition Technique

At this stage, the process of acquiring digital evidence contained in the fusion HDD and SSD RAID 0 configuration using External USB HDD SATA docking, USB is integrated with the first computer (perpetrator) to maintain the integrity and authenticity of the data using tools that support live forensic techniques, namely FTK Imager Portable. The stages of the live forensic technique are carried out to obtain files that have been permanently deleted in the fusion HDD and SSD RAID 0 configuration TRIM function disabled and enabled. FTK Portable Imager tools can retrieve data and file information that has been deleted and can support live forensic techniques. Fig. 5 is the result of the camera portrait documentation of the live forensic imaging process of TRIM disabled and TRIM enabled using FTK Portable Imager, and Table III shows the results of the imaging process and the MD5 hash value. The purpose of the imaging process is to avoid damage to the original digital evidence contained within the NVMe SSD during the analysis process.

TABLE II
LIST OF SEVERAL FILE SAMPLES FOR ODD-EVEN LABELS AND HASH VALUES FILE

	File Real Name	**MD5 Value**	**Extension File**
Odd	1 - Copy_1.JPG	bb5eb60148e4cc76d6d5c1eb4e9a7790	JPG
	3888_1.dcm	6bf03f35172084bba87a9f651f952a26	dcm
	ADSL Router Forensics Part 2_ Acquiring Evidence_1.pdf	d5f0e4868a9782b2b21904a755c805e9	pdf
	changelog_1.txt	4027a10da52763d5cecb8755606df739	txt
	IMG_2815_1.HEIC	7cccb4833beccada2002dc077fde2b9b	HEIC
	ExifTool-12.03_1.dmg	94e1a55472a4447e9b0e3cfe5d91e053	dmg
	loading_1.gif	7b9776076d5fceef4993b55c9383dedd	gif
	Materi_about_Abstract_etc_1.pptx	a37909d48174d5c3ccbf937f0b20e82b	pptx
	sang surya umri_1.mp3	d779e13087d8e6d60c73bbf7b85499d7	mp3
	WhatsApp Video 2020-08-07 at 16.30.54_1.mp4	19204bdfc008c2e85aaccf9ba38b6a20	mp4
Even	1 - Copy_2.JPG	bb5eb60148e4cc76d6d5c1eb4e9a7790	JPG
	3888_2.dcm	6bf03f35172084bba87a9f651f952a26	dcm
	ADSL Router Forensics Part 2_ Acquiring Evidence_2.pdf	d5f0e4868a9782b2b21904a755c805e9	pdf
	changelog_2.txt	4027a10da52763d5cecb8755606df739	txt
	ExifTool-12.03_2.dmg	94e1a55472a4447e9b0e3cfe5d91e053	dmg
	IMG_2815_2.HEIC	7cccb4833beccada2002dc077fde2b9b	HEIC
	loading_2.gif	7b9776076d5fceef4993b55c9383dedd	gif
	Materi_about_Abstract_etc_2.pptx	a37909d48174d5c3ccbf937f0b20e82b	pptx
	sang surya umri_2.mp3	d779e13087d8e6d60c73bbf7b85499d7	mp3
	WhatsApp Video 2020-08-07 at 16.30.54_2.mp4	19204bdfc008c2e85aaccf9ba38b6a20	mp4



Drive/Image Verify Results

Name	Image TRIM Disable.001
Sector count	464843520
MD5 Hash	
Computed hash	7a87fab3e53fd3af620f685934d2dc02
Report Hash	7a87fab3e53fd3af620f685934d2dc02
Verify result	Match
SHA1 Hash	
Computed hash	d602e3d61cf1e95347a2085227e437ba22cf0996
Report Hash	d602e3d61cf1e95347a2085227e437ba22cf0996
Verify result	Match
Bad Sector List	

(a)

Drive/Image Verify Results

Name	Akuisisi Image TRIM Enable.001
Sector count	464843520
MD5 Hash	
Computed hash	13c78b921c59381a428975746a0f523a
Report Hash	13c78b921c59381a428975746a0f523a
Verify result	Match
SHA1 Hash	
Computed hash	0b0a598e88e7d2a1e8e60b70a9695aea
Report Hash	0b0a598e88e7d2a1e8e60b70a9695aea
Verify result	Match
Bad Sector List	

(b)

Fig. 5 Imaging results (a) TRIM disable, (b) TRIM enable

TABLE III
RESULTS OF ACQUISITION FUSION HDD AND SSD RAID 0 CONFIGURATION TRIM FUNCTION USING FTK IMAGER PORTABLE

Name Drive Imaging	MD5 Value	Acquisition Process (Time)
Imaging Trim Disable	7a87fab3e53fd3af620f685934d2dc02	7 Hours 25 Minute 33 Second
Imaging Trim Enable	13c78b921c59381a428975746a0f523a	5 Hours 12 Minute 44 Second

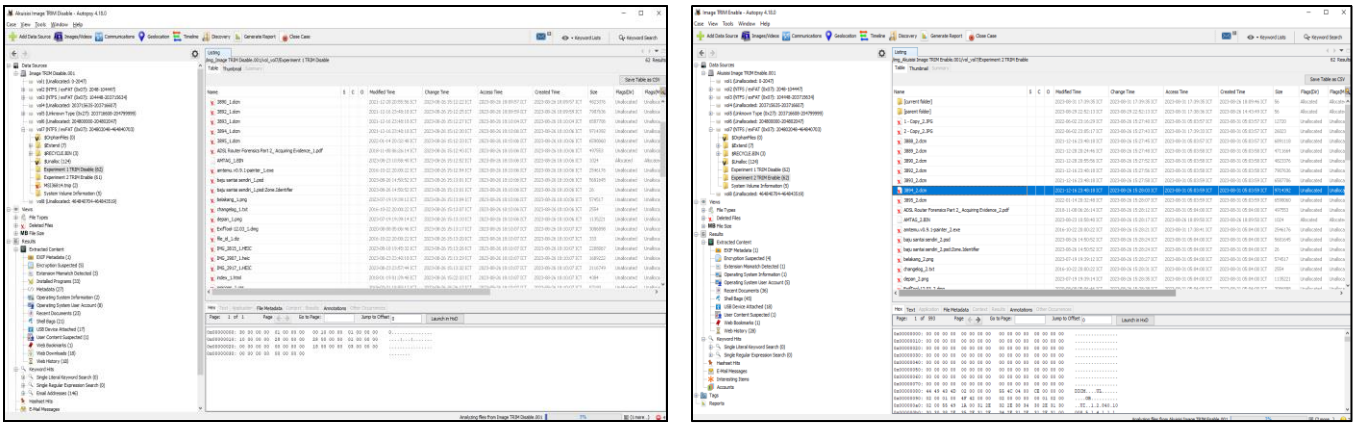
B. Examination and Analysis of Result

After imaging TRIM disabled and enabled, the following is the examination stage to obtain clues or information related to the case. Before examining the acquisition results of TRIM disable and enable, the original imaging results must be duplicated first, and the similarity of the hash value between the original file and the copy to maintain the integrity and authenticity of the imaging. The examination and analysis of the TRIM disable and enable functions of the fusion HDD and SSD RAID 0 configuration of the TRIM feature consists of the acquisition results using the FTK Imager Portable tool which will be examined and analyzed with Sleuth Kit Autopsy [18] and the results of recovery using the Testdisk Recovery tool which will be checked for the integrity of the authenticity of the file by knowing the hash value [19] of the recovered file using the Hashmyfile tool to determine the hash value.

1) Check Using the Sleuth Kit Autopsy Tool to TRIM disable and Enable: Live acquisition of TRIM disable and enable, the researcher performs imaging file extraction which aims to maintain the integrity and authenticity of the evidence [20]. The extracted imaging results are copies of the imaged evidence. Furthermore, the examination and analysis stages were carried out using the Sleuth Kit Autopsy forensic tool. At this stage, it was found that the signature file value had been deleted in the TRIM disable and enable functions. The signature file is a data information value that is used to identify the content of the data [21]. Fig. 6 (a) shows that the signature of the odd label file is not damaged. Thus, it can be concluded that the odd-label file can be read and recovered. Meanwhile, Fig. 6 (b) shows that the signature on the even-label file is damaged or changed so that the file cannot be fully recovered.

The file recovery result analysis stages summarized in Table IV and Table V show the results of the analysis of the TRIM file recovery process disable and enable odd and even labels using the Sleuth Kit Autopsy tool.

The results of TRIM disable and enable odd and even files show that by looking at the authenticity of the evidence as a whole file can be recovered properly using the Sleuth Kit Autopsy tool, it can be assumed that the overall recovery of TRIM disable and enable odd and even label files has an identical MD5 value or in other words, the integrity of the evidence is maintained.



(a) (b)

Fig. 6 Image of the analysis stage (a) recovery of odd files TRIM disable, (b) recovery of even files TRIM enable tool Sleuth Kit Autopsy

TABLE IV
ANALYSIS OF TRIM RECOVERY RESULTS DISABLE ODD FILES USING THE SLEUTH KIT AUTOPSY

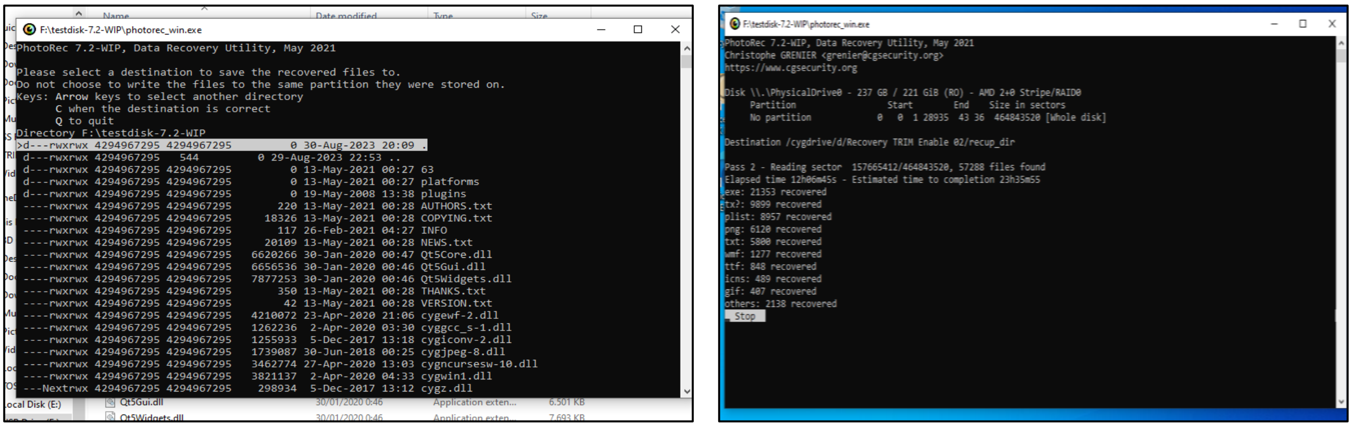
File Name	MD5 Value	Information
343985-1 - Copy_1.JPG	bb5eb60148e4cc76d6d5c1eb4e9a7790	Successfully
3888_1.dcm	6bf03f35172084bba87a9f651f952a26	Successfully
344003-ADSL Router Forensics Part 2_ Acquiring Evidence_1.pdf	d5f0e4868a9782b2b21904a755c805e9	Successfully
344012-changelog_1.txt	4027a10da52763d5cecb8755606df739	Successfully
344019-IMG_2815_1.HEIC	7cccb4833beccada2002dc077fde2b9b	Successfully
344016-ExifTool-12.03_1.dmg	94e1a55472a4447e9b0e3cfe5d91e053	Successfully
344046-loading_1.gif	7b9776076d5fceef4993b55c9383dedd	Successfully
344048-Materi_about_Abstract_etc_1.pptx	a37909d48174d5c3ccbf937f0b20e82b	Successfully
344069-sang surya umri_1.mp3	d779e13087d8e6d60c73bbf7b85499d7	Successfully
344085-WhatsApp Video 2020-08-07 at 16.30.54_1.mp4	19204bdfc008c2e85aaccf9ba38b6a20	Successfully

TABLE V
ANALYSIS OF TRIM RECOVERY RESULTS ENABLE EVEN FILES USING THE SLEUTH KIT AUTOPSY

File Name	MD5 Value	Information
343985-1 - Copy_2.JPG	bb5eb60148e4cc76d6d5c1eb4e9a7790	Successfully
3888_2.dcm	6bf03f35172084bba87a9f651f952a26	Successfully
345133-ADSL Router Forensics Part 2_ Acquiring Evidence_2.pdf	d5f0e4868a9782b2b21904a755c805e9	Successfully
345142-changelog_2.txt	4027a10da52763d5cecb8755606df739	Successfully
345146-ExifTool-12.03_2.dmg	94e1a55472a4447e9b0e3cfe5d91e053	Successfully
345149-IMG_2815_2.HEIC	7cccb4833beccada2002dc077fde2b9b	Successfully
345174-loading_2.gif	7b9776076d5fceef4993b55c9383dedd	Successfully
345178-Materi_about_Abstract_etc_2.pptx	a37909d48174d5c3ccbf937f0b20e82b	Successfully
345199-sang surya umri_1.mp3	d779e13087d8e6d60c73bbf7b85499d7	Successfully
345113-WhatsApp Video 2020-08-07 at 16.30.54_1.mp4	19204bdfc008c2e85aaccf9ba38b6a20	Successfully

2) Check Using the Testdisk Tool to TRIM Disable and Enable: The examination stage using the Test disk tool is used to compare the results of data recovery obtained from the fusion HDD and SSD RAID 0 configuration of the TRIM disable and enable functions for odd and even files. Fig. 7 shows the process analysis (a) recovery of odd files TRIM disable, (b) recovery of even files TRIM enable tool Testdisk.

Based on the observations in this study, Test disk does not have a specific time to recover the data of the fusion HDD and SSD partitions in RAID 0 configuration, because Testdisk rebuilds files on the cache/buffer partition on the SSD architecture controller. Next, Fig. 8 shows the recovery results of the TRIM function disable odd files and the TRIM function enable even files.



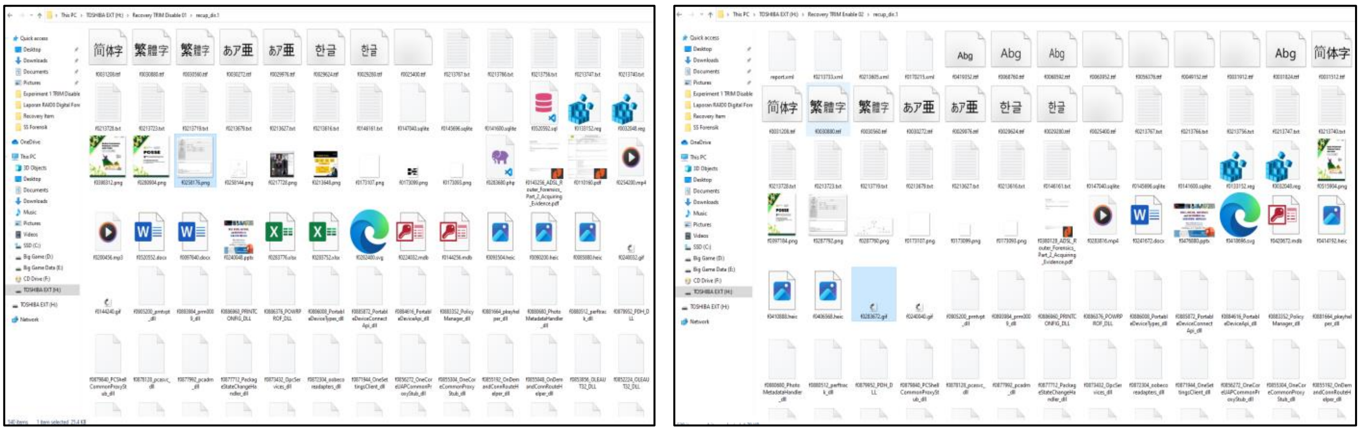
```
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021

Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory F:\testdisk-7.2-WIP
>d---rwxrwx 4294967295 4294967295         0 30-Aug-2023 20:09 .
 d---rwxrwx 4294967295   544         0 29-Aug-2023 22:53 ..
 d---rwxrwx 4294967295 4294967295         0 13-May-2021 00:27 63
 d---rwxrwx 4294967295 4294967295         0 13-May-2021 00:27 platforms
 d---rwxrwx 4294967295 4294967295         0 19-May-2008 13:38 plugins
 ----rwxrwx 4294967295 4294967295       220 13-May-2021 00:28 AUTHORS.txt
 ----rwxrwx 4294967295 4294967295     18326 13-May-2021 00:28 COPYING.txt
 ----rwxrwx 4294967295 4294967295       117 26-Feb-2021 04:27 INFO
 ----rwxrwx 4294967295 4294967295     20109 13-May-2021 00:28 NEWS.txt
 ----rwxrwx 4294967295 4294967295   6620266 30-Jan-2020 00:47 Qt5Core.dll
 ----rwxrwx 4294967295 4294967295   6656536 30-Jan-2020 00:46 Qt5Gui.dll
 ----rwxrwx 4294967295 4294967295   7877253 30-Jan-2020 00:46 Qt5Widgets.dll
 ----rwxrwx 4294967295 4294967295       350 13-May-2021 00:28 THANKS.txt
 ----rwxrwx 4294967295 4294967295        42 13-May-2021 00:28 VERSION.txt
 ----rwxrwx 4294967295 4294967295   4210072 23-Apr-2020 21:06 cygewf-2.dll
 ----rwxrwx 4294967295 4294967295   1262236  2-Apr-2020 03:30 cyggcc_s-1.dll
 ----rwxrwx 4294967295 4294967295   1255933  5-Dec-2017 13:18 cygiconv-2.dll
 ----rwxrwx 4294967295 4294967295   1739087 30-Jun-2018 00:25 cygjpeg-8.dll
 ----rwxrwx 4294967295 4294967295   3462774 27-Apr-2020 13:03 cygncursesw-10.dll
 ----rwxrwx 4294967295 4294967295   3821137  2-Apr-2020 04:33 cygwin1.dll
 ---Nextrwx 4294967295 4294967295    298934  5-Dec-2017 13:12 cygz.dll
```

(a)

```
PhotoRec 7.2-WIP, Data Recovery Utility, May 2021
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive0 - 237 GB / 221 GiB (RO) - AMD 2+0 Stripe/RAID0
     Partition                  Start        End    Size in sectors
     No partition             0   0  1 28935  43 36  464843520 [Whole disk]

Destination /cygdrive/d/Recovery TRIM Enable 02/recup_dir

Pass 2 - Reading sector  157665412/464843520, 57288 files found
Elapsed time 12h06m45s - Estimated time to completion 23h35m55
exe: 21353 recovered
tx?: 9899 recovered
plist: 8957 recovered
png: 6120 recovered
txt: 5800 recovered
wmf: 1277 recovered
ttf: 848 recovered
icns: 489 recovered
gif: 407 recovered
others: 2138 recovered
 Stop
```

(b)

Fig. 7 Process analysis images (a) odd file recovery TRIM disable, (b) even file recovery TRIM enable tool Testdisk



(a) (b)

Fig. 8 Recovery results (a) odd file TRIM disable, (b) even file TRIM enable tool Testdisk

At this stage, analyzing the integrity of file authenticity using the Testdisk recovery tool does not have the advantage of checking the authenticity value of the evidence or MD5 hash on the file, so additional tools are needed, namely Hashmyfile. The recovery results of TRIM disable odd files and TRIM enable even files using the Testdisk tool will be summarized in Table VI and Table VII.

The Table VI and VII are files that can be recovered by the Testdisk Recovery tool and analyzed using the Hashmyfile tool, based on the research conducted, there are quite a lot of files that cannot be opened or are damaged after recovery and also the file name is much changed from the original file name, then there are also quite a lot of files that cannot be recovered using the Testdisk Recovery tool and analysis using the Hashmyfile tool with a permanent deletion scenario implementation on the TRIM Enable function, accounting for around 21 out of 50 files from different extensions that cannot be recovered by Test disk Recovery tool. It can be concluded that the Test disk tool can recover some files but cannot maintain the integrity of the authenticity of evidence from several files in digital forensic analysis. And still has quite a lot of shortcomings because not all file extensions can be recovered and almost all file extensions have hash value results that change from the original file hash value before being permanently deleted. As for Sleuth Kit Autopsy [22], besides having open-source access, this tool also has reliable data recovery capabilities.

TABLE VI
RECOVERY RESULTS ODD FILES TRIM DISABLE USING TESTDISK TOOLS

File Name	MD5 Value	Information
f0258144.png	bb5eb60148e4cc76d6d5c1eb4e9a7790	Successfully
3888_1.dcm	6bf03f35172084bba87a9f651f952a26	Successfully
f0143256_ADSL_Router_Forensics_Part_2_Acquiring_Evidence.pdf	d5f0e4868a9782b2b21904a755c805e9	Successfully
changelog_1.txt	4027a10da52763d5cecb8755606df739	Corrupted File
f0085880.heic	7cccb4833beccada2002dc077fde2b9b	Successfully
ExifTool-12.03_1.dmg	94e1a55472a4447e9b0e3cfe5d91e053	Corrupted File
loading_1.gif	7b9776076d5fceef4993b55c9383dedd	Corrupted File
f0240048.pptx	a37909d48174d5c3ccbf937f0b20e82b	Successfully
f0200456.mp3	d779e13087d8e6d60c73bbf7b85499d7	Successfully
WhatsApp Video 2020-08-07 at 16.30.54_1.mp4	19204bdfc008c2e85aaccf9ba38b6a20	Corrupted File

TABLE VII
RECOVERY RESULTS EVEN FILES TRIM ENABLE USING TESTDISK TOOLS

File Name	MD5 Value	Information
f0287760.png	bb5eb60148e4cc76d6d5c1eb4e9a7790	Successfully
3888_2.dcm	6bf03f35172084bba87a9f651f952a26	Corrupted File
f0380128_ADSL_Router_Forensics_Part_2_Acquiring _Evidence.pdf	d5f0e4868a9782b2b21904a755c805e9	Successfully
changelog_2.txt	4027a10da52763d5cecb8755606df739	Corrupted File
ExifTool-12.03_2.dmg	94e1a55472a4447e9b0e3cfe5d91e053	Corrupted File
f0406568.heic	7cccb4833beccada2002dc077fde2b9b	Successfully
loading_2.gif	7b9776076d5fceef4993b55c9383dedd	Corrupted File
f0476880.pptx	a37909d48174d5c3ccbf937f0b20e82b	Successfully
sang surya umri_1.mp3	d779e13087d8e6d60c73bbf7b85499d7	Corrupted File
WhatsApp Video 2020-08-07 at 16.30.54_1.mp4	19204bdfc008c2e85aaccf9ba38b6a20	Corrupted File

IV. CONCLUSION

Technology in HDD and SSD fusion devices RAID 0 configurations have an important impact on the ability of forensic analysts and investigators to search for and understand data stored on SSD devices. Based on the results of research that has been carried out, technology in HDD and SSD fusion devices with RAID 0 configuration as a solution for optimizing access speed performance for faster reading and writing performance and more storage capacity, has a negative impact when cybercrime occurs so that it is necessary to carry out forensic analysis and investigation to find and understand data stored on storage memory devices when cybercrime occurs. Based on information gathered from literature reviews and experiments implemented in this research, it is proven that the TRIM enable and disable mechanism causes problems in digital forensic investigations, as evidenced by the results of data recovery when TRIM disable and enable is activated, some data cannot be recovered using the Testdisk tool Recovery. Apart from that, the file extension has a hash value that is different from the hash value of the original file before the permanent data deletion attempt, in other words, the file is also not identical to the original file so the integrity of the evidence is not guaranteed. While the Sleuthkit Autopsy tool successfully recovers data on the TRIM disabled and enabled features with the same integrity value, the Sleuthkit Autopsy tool has open-source access and reliable data recovery capabilities. For further research, it is recommended to test the HDD and SDD fusion RAID 0 configuration for the TRIM function using different forensic tools such as Belkasoft Forensic as well as implementation on the Mac OS or Linux operating system by exploring file deletion and recovery in the field of digital forensics.

REFERENCES

[1] D. Mualfah and R. A. Ramadhan, “Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital,” *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 2, pp. 257–267, 2020, doi: 10.31849/digitalzone.v11i2.5174.

[2] D. Mualfah and R. A. Ramadhan, “Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology),” *IT J. Res. Dev.*, vol. 5, no. 2, pp. 171–182, 2020, doi: 10.25299/itjrd.2021.vol5(2).5731.

[3] K. S. Singh, A. Irfan, and N. Dayal, “Cyber Forensics and Comparative Analysis of Digital Forensic Investigation Frameworks,” *... Syst. Comput. Networks ...*, 2019, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9036214/. doi: 3. 10.1109/ISCON47742.2019.9036214

[4] R. A. Ramadhan and D. Mualfah, “Implementasi Metode National Institute of Justice (NIJ) Pada Fitur TRIM SOLID STATE DRIVE (SSD) Dengan Objek Eksperimental Sistem Operasi Windows, Linux dan Macintosh,” *IT J. Res. Dev.*, vol. 5, no. 2, pp. 183–192, 2020, doi: 10.25299/itjrd.2021.vol5(2).5750.

[5] R. A. Ramadhan, Y. Prayudi, and B. Sugiantoro, “Implementasi dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive (SSD),” *Teknomatika*, vol. 9, no. 2, pp. 1–13, 2017, [Online]. Available: http://teknomatika.stmikayani.ac.id/wp-content/uploads/2017/07/1.pdf.

[6] J. Hao, Y. Li, X. Chen, and T. Zhang, “Mitigate HDD Fail-Slow by Pro-actively Utilizing System-level Data Redundancy with Enhanced HDD Controllability and Observability,” *IEEE Symp. Mass Storage Syst. Technol.*, vol. 2019-May, pp. 205–216, 2019, doi: 10.1109/MSST.2019.000-2.

[7] M. Kishani, S. Ahmadian, and H. Asadi, “A Modeling Framework for Reliability of Erasure Codes in SSD Arrays,” *IEEE Trans. Comput.*, vol. 69, no. 5, pp. 649–

665, 2020, doi: 10.1109/TC.2019.2962691.

[8] Y. Zhou, F. Wu, W. Huang, and C. Xie, "LiveSSD: A Low-Interference RAID Scheme for Hardware Virtualized SSDs," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 40, no. 7, pp. 1354–1366, 2021, doi: 10.1109/TCAD.2020.3015908.

[9] A. Singh, R. A. Ikuesan, and H. Venter, "Secure Storage Model for Digital Forensic Readiness," *IEEE Access*, 2022, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9713877/. doi: 9. 10.1109/ACCESS.2022.3151403

[10] Z. Shen, L. Han, C. Ma, Z. Jia, T. Li, and Z. Shao, "Leveraging the Interplay of RAID and SSD for Lifetime Optimization of Flash-Based SSD RAID," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 40, no. 7, pp. 1395–1408, 2021, doi: 10.1109/TCAD.2020.3020495.

[11] C. H. Chang and C. W. Chang, "Adaptive Memory and Storage Fusion on Non-Volatile One-Memory System," *Proc. - 2019 IEEE Non-Volatile Mem. Syst. Appl. Symp. NVMSA 2019*, pp. 1–6, 2019, doi: 10.1109/NVMSA.2019.8863521.

[12] J. Li, Z. Sha, Z. Cai, F. Trahay, and J. Liao, "Patch-Based Data Management for Dual-Copy Buffers in RAID-Enabled SSDs," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 39, no. 11, pp. 3956–3967, 2020, doi: 10.1109/TCAD.2020.3012252.

[13] G. Sibiya, H. S. Venter, and T. Fogwill, *Procedures for a harmonised digital forensic process in live forensics*. researchspace.csir.co.za, 2012.

[14] W. Pranoto, I. Riadi, and Y. Prayudi, "Perbandingan Tools Forensics pada Fitur TRIM SSD NVMe Menggunakan Metode Live Forensics," *It J. Res. Dev.*, vol. 4, no. 2, pp. 135–148, 2020, doi: 10.25299/itjrd.2020.vol4(2).4615.

[15] A. Setya and A. Suganda, "Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014," *JUITA J. Inform.*, vol. 10, no. 1, p. 127, 2022, doi: 10.30595/juita.v10i1.13149.

[16] H. J. Hadi, N. Musthaq, and I. U. Khan, "SSD Forensic: Evidence Generation and Forensic Research on Solid State Drives Using Trim Analysis," *2021 Int. Conf. Cyber Warf. Secur. ICCWS 2021 - Proc.*, pp. 51–56, 2021, doi: 10.1109/ICCWS53234.2021.9702989.

[17] D. Hariyadi, "Komparasi Penanganan Barang Bukti Elektronik dan/atau Barang Bukti Digital sesuai SOP Pusat Laboratorium Forensik Polisi Republik Indonesia," pp. 1–5, 2019, doi: 10.31219/osf.io/37at6.

[18] A. Singh and S. Kumar, "Working Efficiency of the Sleuth Kit in Forensic Data Recovery: a Review," *Researchgate.Net*, no. June, 2020, [Online]. Available: https://www.researchgate.net/profile/Abhinav_Singh24/publication/343040978_Working_Efficiency_Of_The_Sleuth_Kit_In_Forensic_Data_Recovery_A_Review/links/5f1743e645851515ef3c36c5/Working-Efficiency-Of-The-Sleuth-Kit-In-Forensic-Data-Recovery-A-Review.pdf.

[19] W. Y. Sulistyo, I. Riadi, and A. Yudhana, "Penerapan Teknik SURF pada Forensik Citra untuk Analisa Rekayasa Foto Digital," *JUITA J. Inform.*, vol. 8, no. 2, p. 179, 2020, doi: 10.30595/juita.v8i2.6602.

[20] S. Shafar, "Prinsip Dan Prosedur Dasar Penanganan Bukti Digital Dalam Computer Crime Dan Compute Related Crime Prinsip Dan Prosedur Dasar Penanganan Bukti Digital Dalam Computer Crime Dan Compute Related Crime DISUSUN OLEH : UNIVERSITAS ISLAM INDONESIA (UII) YOKYAK," no. January 2014, 2019.

[21] G. Bell and R. Boddington, "Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?," *J. Digit. Forensics, Secur. Law*, vol. 5, no. 3, 2010, doi: 10.15394/jdfsl.2010.1078.

[22] A. Dowling, "Digital forensics: A demonstration of the effectiveness of the sleuth kit and autopsy forensic browser," *Http://Hdl.Handle.Net/10523/1338*, no. August, 2006. doi: 10.30595/juita.v8i2.6602.