http://doi.org/10.35784/iapgos.7223 *received: 06.02.2025 | revised: 29.10.2025 | accepted: 18.11.2025 | available online: 30.06.2026*

STATIC FORENSIC ANALYSIS OF FILE CARVING ON SSDs USES NIST AND ACPO METHOD

Khoirul Anam Dahlan[1], Anton Yudhana[2], Herman Yuliansyah[2]
[1]Institut Teknologi Statistika dan Bisnis Muhammadiyah Semarang, Department of Software Engineering, Semarang, Indonesia, [2]Universitas Ahmad Dahlan, Department of Informatics, Yogyakarta, Indonesia

Abstract. *Solid State Drive (SSD) recovery is challenging due to a lower success rate than traditional storage devices. Latest file carving techniques, such as those used in Foremost and Autopsy software, offer a solution for recovering lost files, whether intentionally or unintentionally deleted, on SSDs. The study compares approaches to recovering deleted data from SSDs. NIST method provides accountable reporting for legal proceedings and ACPO framework guides the recovery process through planning, capture, analysis, and presentation stages. In an experiment using a 120 GB Geniune SATA SSD and a 512 GB Eaget mSATA SSD with NTFS, 88 lost files were recovered. Foremost successfully restored 46 files (52.27%), while Autopsy recovered 81 files (92,05%), with success measured by matching MD5 hash values and ensuring files were accessible. Despite not reaching 100% recovery as seen in HDDs, the findings highlight the promise of Autopsy in digital forensics and legal evidence. The recovery process was conducted using Ubuntu and Windows OS, indicating the potential for improved SSD recovery.*

Keywords: system recovery, image forensics, digital storage, solid state drives, flash memories, digital information

STATYCZNA ANALIZA KRYMINALISTYCZNA METODĄ WYODRĘBNIANIA PLIKÓW Z DYSKÓW SSD Z WYKORZYSTANIEM METOD NIST I ACPO

Streszczenie. *Odzyskiwanie danych z dysków półprzewodnikowych (SSD) stanowi wyzwanie ze względu na niższy wskaźnik powodzenia w porównaniu z tradycyjnymi nośnikami danych. Najnowsze techniki odzyskiwania fragmentów plików, takie jak te stosowane w oprogramowaniu Foremost i Autopsy, oferują rozwiązanie pozwalające na odzyskanie utraconych plików – zarówno tych usuniętych celowo, jak i przypadkowo – z dysków SSD. W niniejszym badaniu porównano różne podejścia do odzyskiwania usuniętych danych z dysków SSD. Metoda NIST zapewnia rzetelne raportowanie na potrzeby postępowań sądowych, a ramy ACPO kierują procesem odzyskiwania na etapach planowania, przechwytywania, analizy i prezentacji. W eksperymencie z wykorzystaniem dysku SSD Geniune SATA o pojemności 120 GB oraz dysku SSD Eaget mSATA o pojemności 512 GB z systemem plików NTFS odzyskano 88 utraconych plików. Foremost pomyślnie przywrócił 46 plików (52,27%), podczas gdy Autopsy odzyskał 81 plików (92,05%), przy czym sukces mierzono poprzez dopasowanie wartości skrótów MD5 i zapewnienie dostępności plików. Pomimo nieosiągnięcia 100% odzysku, jak ma to miejsce w przypadku dysków HDD, wyniki podkreślają potencjał Autopsy w kryminalistyce cyfrowej i dowodach prawnych. Proces odzyskiwania przeprowadzono przy użyciu systemów operacyjnych Ubuntu i Windows, co wskazuje na potencjał w zakresie ulepszonego odzyskiwania danych z dysków SSD.*

Słowa kluczowe: system odzyskiwania danych, analiza obrazów, pamięć cyfrowa, dyski półprzewodnikowe, pamięci flash, informacje cyfrowe

Introduction

Hard Disk Drives (HDD) are increasingly being phased out due to their slower speeds and noise during high-speed operation [22]. This shift is due to Solid State Drives (SSD) faster read and write capabilities, with conventional HDDs averaging around 200 Mb/s for read speeds, while SSDs can reach 500 Mb/s for read and 250 Mb/s for writing speeds [16, 30]. In contrast, SSDs are gaining traction because they offer greater efficiency in size and performance. In 2022, HDDs held a 60% market share, while NAND Flash, a key component of SSDs, accounted for only 25%. Despite this, SSDs are becoming more popular each year [12]. NAND Flash technology enables SSDs to expand their storage capacity using Multi-Level Cell (MLC), Triple-Level Cell (TLC), and Quad-Level Cell (QLC) configurations, which also lowers production costs compared to HDDs [17]. NAND Flash typically provides ten times faster speeds than HDDs, prompting many companies to adopt SSDs for social media data centres and entertainment platforms to improve performance and reduce latency [23].

SSD data transfers utilize a Flash Transfer Layer (FTL) system, allowing multiple NAND Flash layers to operate simultaneously [15]. However, faster SSDs generate more heat, typically operating between 50–55°C and functioning Generally in a range of 0–70°C. If temperatures exceed 70°C, the SSD performance may degrade, potentially becoming slower than HDDs [2]. As a result, heatsinks are necessary to dissipate heat and ensure stable performance, particularly during benchmarking tests, which demonstrate consistent results [3, 7]. The increase in SSD sales and decreases in HDD sales are shown in Fig. 1.

While SSDs consist of NAND memory that is shock-resistant and consumes less power than HDDs, some NAND types require an "erase before write" capability, complicating data recovery, Moreover, the system damage on SSDs exacerbates recovery challenges [10, 21]. Digital forensics involves the investigation of crimes through the recovery of digital evidence, which may often be blocked, deleted, hidden, or overwritten [24, 26]. This scientific endeavour aims to recover and investigate materials for digital evidence, providing options and recommendations to judges to unveil criminal cases [18].

The growing prevalence of cybercrime is a by product of advanced technology, highlighting the relationship between cybercrime and data storage technologies, both volatile and non-volatile [8, 27]. Digital evidence is any information with evidentiary value derived from electronically processed binary data [11, 29].

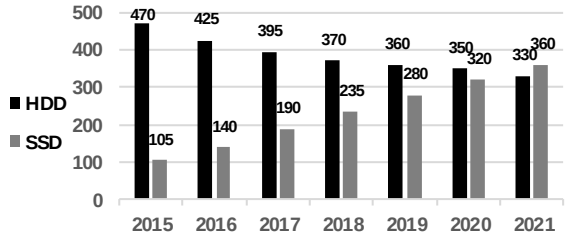

Fig. 1. Sales comparison SSD and HDD 2015 until 2021 in millions

This study incorporates quotations from various prior works on digital forensics, such as the recovery on physical devices like SSD, which is not always about how to recover the device but also the hardware condition of the device itself [28]. Damage like short circuits, burning, and water on a device could make recovering files impossible. Time is the main factor in a successful recovery. The shorter the time between damage and recovery time, the higher the chance of data recovery [25].

Foremost are file carving tools that could identify file signatures based on start and end points. The tools effectively recovered variation files like jpg, png, zip, doc, pdf, ppt, and xls extension. The method recognizes the header and footer standard [6]. Autopsy module accesses smartphones with Android 7+ version. The smartphone has a photo, short message service (SMS), and multimedia messaging service (MMS). The smartphone analysed with autopsy runs on Windows 10/18.03

[1, 13]. The research results are 25 photos, SMS, and MMS in the last 30 days. Contact database store on SQLite3 database on Windows 10. The phone was recoverable with Python script with your phone analyser (YPA) on the Autopsy module [4, 5].

Md5 used to be a one-way cryptographic tool for maintaining data integrity. The method uses a hash function to provide validation code by generating a random matrix. Code contains some keys that create unique code to improve the function [14, 19]. Digital forensic investigations rely on several widely used frameworks, including those from the National Institute of Standards and Technology (NIST), the Digital Forensics Research Workshop (DFRWS), the Association of Chief Police Officers (ACPO), and the National Institute of Justice (NIJ). These frameworks help streamline the forensic process to meet specific needs [9, 20].

This study simulates the retrieval of digital data from 128 GB Geniune Sata SSD and 512 GB Eaget external SSD. The experiment focuses on recovered data with zip, rar, docx, pdf, pptx, xls, gif, jpg, png, avi, mov, and mp4 extension, with the expectation that some digital evidence may have been deleted, or the device has been formatted. This study uses NIST and ACPO research methods. The research is structured into five sections, beginning with an introduction, followed by a review of several studies relevant to the topic, an outline of three research methodologies, the presentation of four key results, and a conclusion with the final analysis.

1. Method

This study applied experimental methods to analyse the ability of two digital forensic tools to collect digital evidence from SATA SSD and external SSD. Examining acquiring digital data based on the NIST and ACPO Method.

1.1. Hardware, software, and object research

The hardware accommodates Windows and Ubuntu operation systems. Most tools are run on Ubuntu, Autopsy, and MD5, and they run on the same Windows operating system. It has been used several times to run the research. Hardware and software are shown in Tables 1 and 2.

Table 1. Hardware tools

Hardware	Description
Notebook, Intel i7-7700HQ CPU @2.80 GHz 16 GB RAM	Workstation
SATA SSD, Geniune 120 GB	Physical Evidence
External SSD, Eaget	Physical Evidence
SATA Docking Station	Connecting SATA SSD to notebook

Table 2. Software tools

Software	Version	Description
Windows	10 22H2 64bit	Workstation
Ubuntu	22.0.4	Workstation
Foremost	1.5.7	Forensic tool
Autopsy	4.21.0	Forensic tool
MD5	V1.20	Hashing tool

This study aims to recover digital data from SSDs that have been deleted or formatted. The tools recovered erased digital data from SSD to evaluate the efficacies. The data collected and analysed were used to make certain about the evidence contained in digital crime.

1.2. NIST method

The method used to analyse digital evidence, encompassing stages such as collecting digital media evidence, examining it, analysing the obtained information, and reporting the analysis results, is known as the NIST method. NIST, a U.S.-based organization, is responsible for developing and promoting technical standards and guidelines, including digital forensics. The NIST method in digital forensic analysis provides a structured approach for examining and analysing digital evidence with measurable, repeatable steps. By following this methodology, investigators can ensure that their analysis is consistent and that the results are reliable for legal purposes.

Fig. 2. NIST stages

NIST stages on Fig. 2 show that collection phase is the first step in the digital investigation process, focusing on gathering data to support the investigation and locate evidence of digital crime. Once evidence is collected, the next step is to verify the authenticity of the data while maintaining its integrity. The subsequent phase involves analysing data related to the crime case, and the analysis results are then considered scientifically and legally recognized digital evidence.

Digital evidence recovery includes File Carving, a technique that restores data by identifying and reconstructing files that have been deleted, hidden, or formatted back to their original state. While carving and recovery techniques are similar, recovery only restores deleted data, whereas carving does not rely on file system metadata and instead analyses each byte on electronic storage media. However, carving cannot preserve metadata such as filename, timestamp, existence/deletion status, or fragmentation.

This study uses software tools such as Foremost, which employs commands to recover files from various file systems, including FAT and EXT3. Autopsy is used to analyse images and other media, and it can extract data like browser history and cookies. Both software tools are quick and user-friendly.

To validate the authenticity of digital evidence, the MD5 method is used to check for consistency between the media hash and the image acquisition result. Hashing tools are also used to collect data, where investigators ensure integrity evidence by calculating and verifying cryptographic hashing results, which provide a unique, fixed mathematical value from a random input set.

The research framework includes several stages. The initial stage involves simulating a digital crime and propaganda case on SSD storage. The second stage involves using forensic tools to analyse the SSD to obtain digital evidence.

1.3. ACPO method

The ACPO Good Practice Guide for Digital Evidence outlines seven stages for supporting crime and security incident investigations in cybersecurity. These stages include the Application of Guide, Principles of Digital Evidence, Plan, Capture, Analyse, Present, and General. The ACPO method can be condensed into four main stages: Plan, Capture, Analysis, and Present.

Fig. 3. ACPO stages

Each stage in the ACPO method is interconnected, as illustrated in Fig. 3. The Planning stage focuses on preparing research plans to achieve optimal results and enhance success, involving preparing necessary hardware and software. The Capture stage seeks to obtain evidence related to the investigation, including records, storage devices, interrogations, and other sources to Substantiate Criminal activity. In the Analysis stage, the investigator examines captured data to identify digital evidence relevant to the case, using the original evidence for accurate assessment. Finally, the Present stage ensures the findings are accurately reported or presented, with the evidence being reliable and valid for forensic and legal purposes.

This research involves photos and videos stored on an external Eaget mSATA-type SSD with a capacity of 512 GB and an NTFS file system, which was found during the investigation. The files on the SSD had been deleted and formatted, with the trim status disabled by default, allowing data to be recovered directly from the device without additional tools. When examined using a computer, the SSD appeared empty, raising suspicions that its contents had been intentionally deleted to destroy evidence. Digital forensic investigators conducted further research and successfully recovered several files containing substantial evidence from the SSD. This research primarily focuses on the effectiveness of forensic techniques in recovering deleted data to enhance law enforcement efforts. The findings aim to contribute to developing standard protocols for future digital forensic investigations.

1.4. Method comparation

The NIST and ACPO methods offer structured approaches in digital forensics, each with unique strengths. The NIST method focuses on standardization, ensuring evidence integrity through clearly defined, repeatable stages, making it a reliable, widely applicable framework for investigators. As a U.S. federal agency, NIST standards significantly impact national and international forensic practices.

The ACPO method, developed in the UK, provides a more flexible, adaptable framework with four main stages: Plan, Capture, Analyse, and Present. This approach emphasizes planning and adaptability, supporting legally defensible evidence collection. While NIST is known for its stringent standards, ACPO is particularly influential in UK law enforcement for its practical, scenario-based approach. Both methods are essential, with usage determined by each case's specific legal and procedural needs.

The NIST and ACPO methods share vital similarities, both of which are designed to ensure the integrity and reliability of digital forensic investigations through a structured, multi-stage process that guides examiners in evidence handling, analysis, and reporting. This approach promotes consistency and thoroughness, helping investigators maintain a defensible chain of custody and uphold evidentiary standards. Both methods also prioritize the authenticity and integrity of digital evidence by including steps to preserve the original evidence, often using hashing and secure handling practices to ensure it remains unaltered and admissible in court. Ultimately, NIST and ACPO aim to establish the best practices in digital forensics, supporting investigators in delivering reliable, legally compliant results. Fig. 4 illustrates the stages of the research scenario, including file carving simulation, case simulation, planning, evidence collection, evidence analysis, and reporting show on Fig. 4.

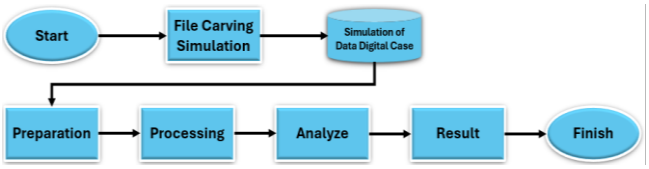

Fig. 4. General step of NIST and ACPO method

2. Results and discussion

2.1. NIST method

From the research conducted using Foremost and Autopsy software on deleted data from an external SSD storage device, Table 1 provides information on the hardware, operating system, and software used in this study.

1) Collection

In the data collection simulation process, a 120 GB SATA SSD with an NTFS file system was used. Storage media used in the research contained several files saved before the formatted process.

After the SSD was formatted, the files within it were erased, indicated by the absence of any items aside from the default file structure. The total capacity used, initially 1.3 GB, was reduced to just 88 bytes on SSD properties. Only blank white circle appears, with no coloured sections, confirming that the files were completely deleted and not merely hidden.

2) Examination

The examination process for the 120 GB SATA SSD, branded as Geniune, was conducted using Foremost and Autopsy software.

```
Disk /dev/sdc: 111,79 GiB, 120034123776 bytes, 234441648 sectors
Disk model: G
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: gpt
Disk identifier: AA494B67-A2C0-4020-BCBD-171D0ED0165A

Device     Start       End   Sectors   Size Type
/dev/sdc1     34     32767     32734    16M Microsoft reserved
/dev/sdc2  32768 234438655 234405888 111,8G Microsoft basic data

Partition 1 does not start on physical sector boundary.


Disk /dev/loop19: 55,66 MiB, 58363904 bytes, 113992 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
wsb-komputer@wsbkomputer-Lenovo-Y520-15IKBN:~$
```

Fig. 5. Reaching process of external SSD

Fig. 5 displays the storage code used to execute the recovery command. In the figure, the SSD shows a volume of 111.78 GiB, close to the labelled 120 GB capacity. The storage code in Linux is designated as /dev/sdc, with the local disk labelled /dev/sdc2.

```
anam@debian:~$ wsb-komputer@wsbkomputer-Lenovo-Y520-15IKBN:~/Desktop$
sudo foremost -t jpeg,png,gif,docx,xlsx,pptx,avi,mov,
mp4,pdf,rar,zip -o foremostgeniune -i /dev/sdc2
Processing: /dev/sdc2
|*****
```

Fig. 6. File carving process

Fig. 6 shows the file carving process using Foremost, executed with the command: "sudo foremost -t jpeg,png,gif,docx,xlsx,pptx,avi,mov,mp4,pdf,rar,zip -o foremostgeniune -i /dev/sdc2". File carving process using Autopsy, where users must select the local disk before beginning file recovery, as shown in the file explorer.

3) Analysis

This step analyse Recovered file names, file types, sizes, and additional details, all documented in a file.txt report saved within the "foremostgeniune" folder, following the command executed in the Foremost application.

The "audit.txt" file for Foremost version 1.5.7, initiated on April 30, 2024, details the recovery process of files from a 120 GB SSD (specifically /dev/sdc2) using the command "foremost -t jpeg, png,gif,docx,xlsx,pptx,avi,mov,mp4, pdf,rar, zip -o foremostgeniune -i /dev/sdc2" executed in the output directory "/home/wsb-komputer/Desktop/foremostgeniune". The recovery process began at 20:01:41 and concluded at 20:28:05, resulting in the successful extraction of 86 files, including 15 files in the .jpg format, 21 in .png, 6 in .zip, 5 in .gif, and 4 in .avi. Additionally, there are 8 files with the .pdf extension, 6 in .docx, 8 in .pptx, 6 .mov extension and 7 in .xlsx. The SSDs total length was confirmed to be 111 GB, closely matching the stated capacity. The report provides details on each recovered file, including names, sizes, and file offsets, demonstrating the effectiveness of Foremost in retrieving deleted data.

Autopsy recovered various file types, with the zip extension achieving 10 files from 10, the rar extension salvaging 3 files from 10, and the docx, xlsx, pdf, pptx, jpg, png, and avi extensions all recovering 7 files from 7. The gif extension recovered 5 files from 5, while the mov and mp4 extensions recovered 7 files from 7 respectively

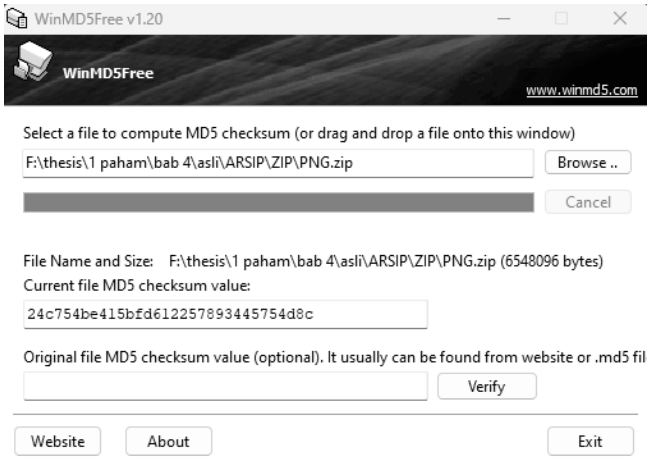

Fig. 7. Original hashing file

Hashing on original files using MD5 is necessary to ensure the recovery files are unchanged. This step is for looking at value, in Fig. 7 shows that the value of the "PNG.zip" file is "24c754be415bfd612257893445754d8c". Value doesn't change if we change the name of files or just open the file without changing the content. The value changes if we change the content, although just space. If we change the content and return to "original" like we add space, save the file delete space then save again, the value doesn't return to the original value.

Autopsy successfully returned files, one of them name is "681-f1731432_PNG.zip" which the recovered from the "PNG.zip" file. The WinMD5v1.20 software shows that the "681-f1731432_PNG.zip" is matched with the original file that has the same value at "24c754be415bfd612257893445754d8c". WinMD5 shows that two files have the same value. We click verify, the pop up of WinMD5 show if 2 files are "Matched!".

Recovered file name "1791231.zip" has "e1cfbbeb282f16a0d98c7ed217012947" value which recovered has from the "PNG.zip" is "Not Matched!" because have difference value. Foremost have failed to recover the file, so it has a difference value. File also cannot be opened because the file is corrupted.

4) Reporting

After obtaining the checksum value, it is entered into an Excel application to compare the hash value of the original file with that of the file recovered using Foremost and Autopsy. In Excel, the original files hash value is compared with the recovered files hash value. If the hashes match, the cell value will display "1," indicating identical hashes. However, if the file was not successfully recovered or the hash values do not match, the cell value will show "0," indicating that the file has been altered show on Fig. 8.

Original File	Original Hashing Value	Foremost file name	Autopsy file name
avi	6fd661b82895bef2f2e55226e6b462f6		674-f0872200_avi
doc	52fc6fa2366665dfeca1ccf4d9599840	'01237736	675-f1186912_doc
gif	a375cc5b49701bf7b7626cd2c648c6ec	'01239592	676-f1188768_GIF
jpeg	8ff452e0db3279027cf8bebeafb3f9cf	'01259068	677-f1206208_JPEG
mov	e1fa20e0573110f9473555721608 4507		678-f1208968_mov
mp4	6e18e97ddb470a591deb26533ca1b88a		679-f1522888_mp4
pdf	38fb9ec357f60eaee22b2e6aeace96f8	'01780072	680-f1729248_pdf
png	24c754be415bfd612257893445754d8c	'01791231	681-f1731432_PNG
ppt	380c56fcbc3ac41c1064db11f02e26b0	'01795056	682-f1744232_PPT
xls	52b8cff0f93e21f047b38b420b29150a	'01795552	683-f1744728_xls
Foremost Hashing Value	**Autopsy Hashing Value**	**Foremost result**	**Autopsy result**
	6fd661b82895bef2f2e55226e6b462f6	0	1
52fc6fa2366665dfeca1ccf4d9599840	52fc6fa2366665dfeca1ccf4d9599840	1	1
a375cc5b49701bf7b7626cd2c648c6ec	a375cc5b49701bf7b7626cd2c648c6ec	1	1
4cc981b0cfd3b7eb2a6048278db886e5	8ff452e0db3279027cf8bebeafb3f9cf	0	1
	e1fa20e0573110f9473555721608 4507	0	1
	6e18e97ddb470a591deb26533ca1b88a	0	1
38fb9ec357f60eaee22b2e6aeace96f8	38fb9ec357f60eaee22b2e6aeace96f8	1	1
e1cfbbeb282f16a0d98c7ed217012947	24c754be415bfd612257893445754d8c	0	1
380c56fcbc3ac41c1064db11f02e26b0	380c56fcbc3ac41c1064db11f02e26b0	1	1
52b8cff0f93e21f047b38b420b29150a	52b8cff0f93e21f047b38b420b29150a	1	1
		50%	100%

Fig. 8. Value details of ZIP file

The zip extension has 10 original files with 10 hashing values that are compared to recovered files. Foremost successfully recovered 7 files and Autopsy 10 files. Although Foremost could recover 7 files, it just had 5 files with the same value. 2 recovered files of foremost which do not have the same value are corrupted and cannot be opened. Foremost successfully recovered 5 of 10 files that were confirmed to have the same value which same value as 50%. Autopsy perfectly recovered 10 out of 10 with 100% rate shown on Fig. 9.

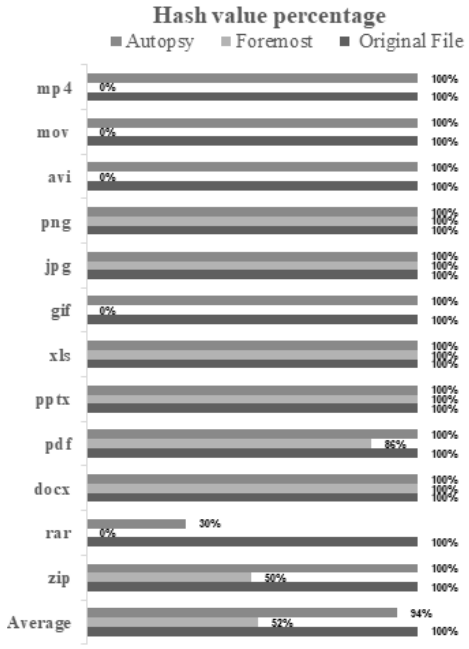

Fig. 9. Foremost and autopsy hash percentage

Foremost and Autopsy successfully recovered seven files in each format from docx, pptx, xls, jpg, and png, achieving a 100% recovery rate for these types. However, Foremost was unable to recover any zip or rar files, and it failed to retrieve ten pdf files, seven files each in avi, mov, and mp4 formats, and five gif files. In contrast, Autopsy successfully recovered all formats except for rar, where it managed to recover only three out of ten files in an intact state, resulting in a 30% recovery rate for rar files. Overall, Autopsy achieved a success rate of 94%, whereas Foremost achieved only 52%.

2.2. ACPO method

Stage of Association of Chief Police Officers (ACPO) digital forensics method for an external SSD involves a series of interconnected and sequential stages, each with its specific function. These stages work together to ensure the proper handling and analysis of digital evidence, maintaining its integrity throughout the process.

1) Plan

In the initial stage, hardware and software are prepared to conduct the investigation. The scenario involves documenting evidence, specifically an external SSD and a Type C data cable. SSD identified as a blue 512 GB Eaget external drive, is accessible via a computer. This device was found at the simulated crime scene as part of the research process.

The SSD is connected to a computer running the Ubuntu operating system to examine its contents. Ubuntu is chosen to minimize the risk of any potential viruses on the SSD spreading to the computer. No files were visible when the external SSD was checked. The SSD properties indicated that it was empty, except for a system folder labelled "volume information," which contained three files with a combined size of 88 bytes.

2) Capture

The capture process involves recovering files that the perpetrator intentionally deleted to destroy digital evidence. Investigators performed the file recovery twice, using different software and operating systems, aiming to achieve the best comparative results. The goal was to identify the most effective software for restoring the deleted files from the SSD.

Foremost operates on the Linux platform, and this research utilized the Ubuntu 22.04 operating system, running through the terminal. Password input is required in the terminal to execute commands. As shown in Fig. 10, the "lsblk" command is used to list all partition codes on the computer. The target partition is identified as "sdb" for the SSD and "sdb1" as the specific partition code for the recovery process.

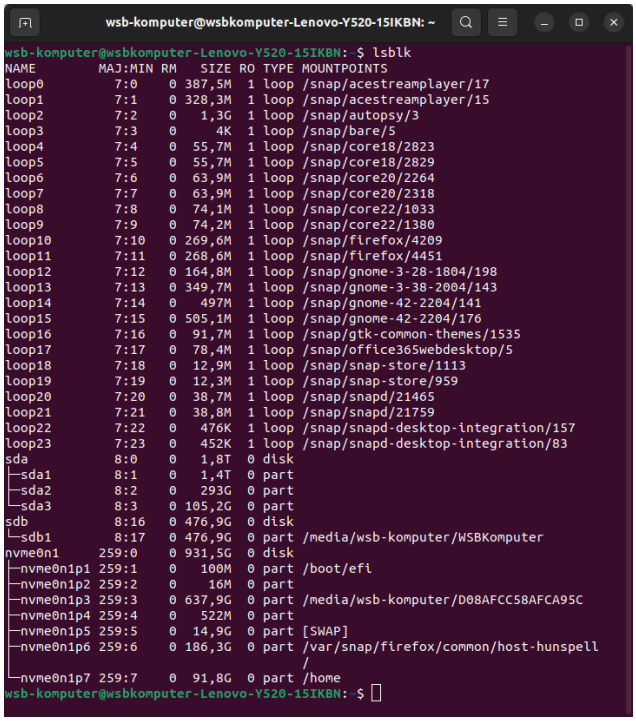

Fig. 10. External SSD partition search

Fig. 11 illustrates the command "sudo parted /dev/sdb1 print." The "parted" command is used to select a specific partition, with "/dev/sdb1" indicating the location of the target partition. The "print" command displays the contents of that partition. The purpose is to verify that the partition is correctly identified with a 512 GB capacity, which matches the size of the Eaget SSD used in the research.

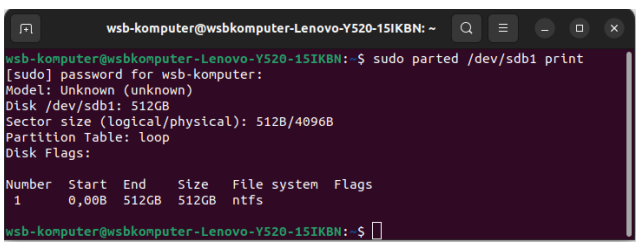

Fig. 11. External SSD detail

Fig. 12 displays the command "sudo Foremost -t jpeg, png, gif, docx, xlsx, pptx, avi, mov, mp4, pdf, rar, zip -o foremosteaget -I /dev/sdb1." The command "sudo foremost" initiates the Foremost software, while "-t jpeg, png, gif, docx, xlsx, pptx, avi, mov, mp4, pdf, rar, zip" specifies the file types to be recovered. The "-o foremosteaget" line designates the location where the recovered files will be stored, creating the "foremosteaget" folder on the desktop if no other folder is specified. The command "-I /dev/sdb1" indicates the partition to be recovered.

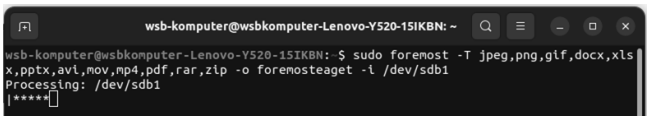

Fig. 12. Start recovering with foremost

Fig. 13 displays the recovery results from the Foremost software, organized into separate folders according to file extensions. The image categorizes the folders as follows: jpeg, png, and gif for image formats; docx, xlsx, pptx, and pdf for document formats; avi, mov, and mp4 for video formats; and rar and zip for archive formats. This organization facilitates the sorting of digital evidence for analysis and allows for easier reporting of the recovery process in the form of "audit.txt.".

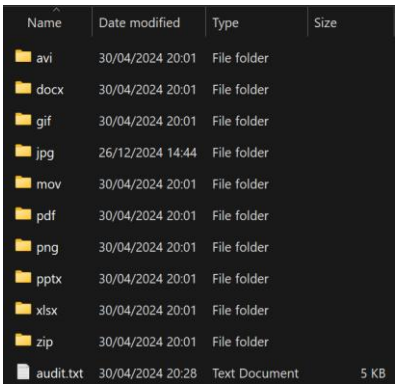

Fig. 13. Result of foremost recovery

Autopsy software version 4.2.1 operates on the Windows 10 64-bit operating system. Software displays initial interface of the Autopsy software. Investigators can select "new case" to initiate a completely new case, choose "open recent case" to access a case that has been previously conducted on the current computer, or click "open case" to load a case saved from another computer for analysis on the system running Autopsy.

To begin using Autopsy software, the investigator selects "new case" and enters the "case name" specific to the investigation. For simplicity, the case name can reflect related project or object names. In this instance, the title "Recovery SSD Eaget" is used as the project name, with the "base directory" designating the project's storage location, as shown in Fig. 14.

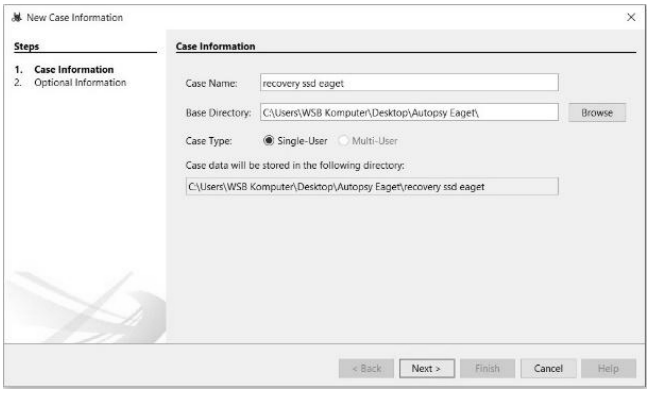

Fig. 14. New project

Next, select "local disk" by clicking on "select disk" and locating the partition to restore. Fig. 15 displays a 476.9 GB capacity, which is close to the listed 512 GB capacity of the external SSD. It's essential for investigators to identify the external SSD by its name, "WSBKomputer." The SSD partition "H" is designated for object recovery.

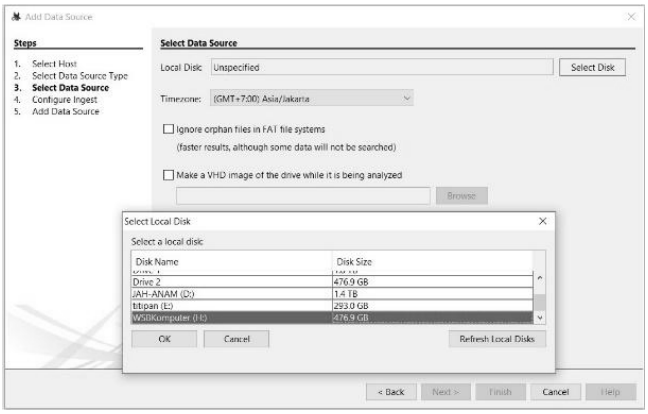

Fig. 15. Recovery partition section

Fig. 16 illustrates the types of recovery options available for restoring the necessary data. Investigators can check the boxes for specific items they wish to recover, while unchecking those not needed. This allows the recovery process to focus only on required files, optimizing time. The more items selected, the more data is extracted from the SSD, which increases both storage requirements and recovery time.

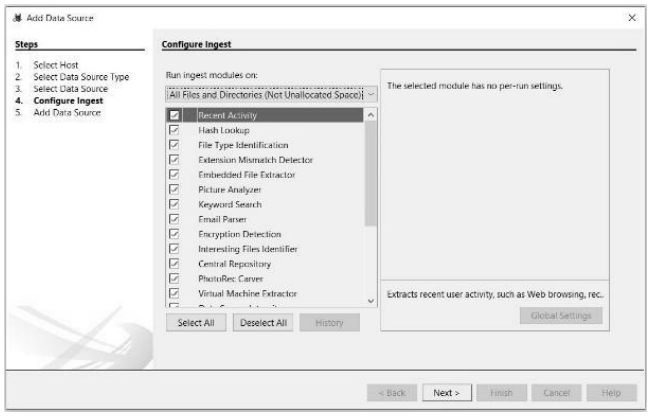

Fig. 16. Recovery type section

Fig. 17 demonstrates the data recovery process in Autopsy software. The duration of the recovery process depends on the storage capacity, as well as the size and number of deleted files. The selected storage and recovery methods in Autopsy can extend the process over several days. Investigators should ensure that the destination storage for recovered files has sufficient capacity to avoid any interruptions.

Fig. 17. Autopsy recovery process

Fig. 18 shows the complete recovery process in Autopsy software. The software displays the number of successfully recovered files by type and records each file extension. Investigators should organize the recovered files by selecting and moving them to designated folders, allowing for easier management. Unnecessary files from the recovery can then be deleted from the software to prevent the computer storage capacity from becoming full.

Fig. 18. The result of recovery

3) Analyse

The analysis of case recovery on SSD external drives utilizes WinMD5 software to obtain hash values. Fig. 19 demonstrates the process of retrieving the hash value for a file, confirming that Marking file hash aligns with the original files hash. However, during recovery, some files can be opened but show a different hash value, indicating a discrepancy. Although these files may appear identical at first, altered hash suggests possible modifications to the files content, either due to deliberate tampering or corruption. Such corruption may result from system errors during recovery or a virus affecting the file.

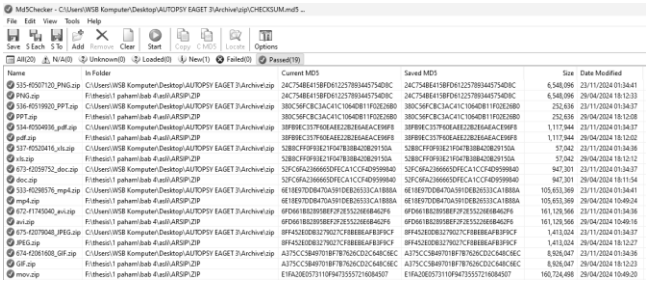

Fig. 19. Hashing process

The obtained hash for Marking file is entered into Microsoft Excel, as shown in Fig. 20. The investigator verifies that the restored files hash matches the original files hash, assigning a value of 1 to files with identical hashes. Although file names may change, the consistent hash indicates the file content remains unchanged. Conversely, a value of 0 is assigned to files with differing hash values, which may result from corruption, intentional modification, or unsuccessful recovery by Foremost or Autopsy software.

No	Original File Name	Original Hash Value	Original Score	Persentage
1	avi	6fd661b82895bef2f2e55226e6b462f6	1	
2	doc	52fc6fa2366665dfeca1ccf4d9599840	1	
3	gif	a375cc5b49701bf7b7626cd2c648c6ec	1	
4	jpeg	8ff452e0db3279027cf8bebeafb3f9cf	1	
5	mov	e1fa20e0573110f94735557216084507	1	100%
6	mp4	6e18e97ddb470a591deb26533ca1b88a	1	
7	pdf	38fb9ec357f60eaee22b2e6aeace96f8	1	
8	png	24c754be415bfd6122578934457548c	1	
9	ppt	380c56fcbc3ac41c1064db11f02e26b0	1	
10	xls	52b8cff0f93e21f047b38b420b29150a	1	
No	**Foremost File CarvingName**	**Foremost Hash Value**	**Foremost Score**	**Persentage**
1			0	
2	01453384.zip	52fc6fa2366665dfeca1ccf4d9599840	1	
3	01455240.zip	a375cc5b49701bf7b7626cd2c648c6ec	1	
4	01474716.zip	4cc981b0cfd3b7eb2a6048278db886e5	0	
5			0	50%
6			0	
7	01995720.zip	38fb9ec357f60eaee22b2e6aeace96f8	1	
8	02006879.zip	e1cfbbeb282f16a0d98c7ed217012947	0	
9	02010704.zip	380c56fcbc3ac41c1064db11f02e26b0	1	
10	02011200.zip	52b8cff0f93e21f047b38b420b29150a	1	
No	**Autopsy File CarvingName**	**Autopsy Hash Value**	**Autopsy Score**	**Persentage**
1	672-f1745040_avi.zip	6FD661B82895BEF2F2E55226E6B462F6	1	
2	673-f2059752_doc.zip	52FC6FA2366665DFECA1CCF4D9599840	1	
3	674-f2061608_GIF.zip	A375CC5B49701BF7B7626CD2C648C6EC	1	
4	675-f2079048_JPEG.zip	8FF452E0DB3279027CF8BEBEAFB3F9CF	1	
5			0	
6	533-f0298576_mp4.zip	6E18E97DDB470A591DEB26533CA1B88A	1	90%
7	534-f0504936_pdf.zip	38FB9EC357F60EAEE22B2E6AEACE96F8	1	
8	535-f0507120_PNG.zip	24c754be415bfd6122578934457548c	1	
9	536-f0519920_PPT.zip	380C56FCBC3AC41C1064DB11F02E26B0	1	
10	537-f0520416_xls.zip	52B8CFF0F93E21F047B38B420B29150A	1	

Fig. 20. Matching process

4) Present

The hash values were entered into Microsoft Excel and assigned numerical value. To calculate the successful percentage of file restoration, the formula used is the sum of files successfully restored with matching hash values divided by the total number of original files, then multiplied by 100%. This formula is shown as Formula 1.

$$P_{\alpha r} = \frac{S_{\alpha r}0}{S_{\alpha r}T} \times 100\% \quad (1)$$

$P_{\alpha r}$ = percentage of success software recovery, $S_{\alpha r}0$ = amount file successful, $S_{\alpha r}T$ = total number of files.

The data converted into a success percentage for each software using Pαr formula, which accumulates the recovery results from both Foremost and Autopsy.

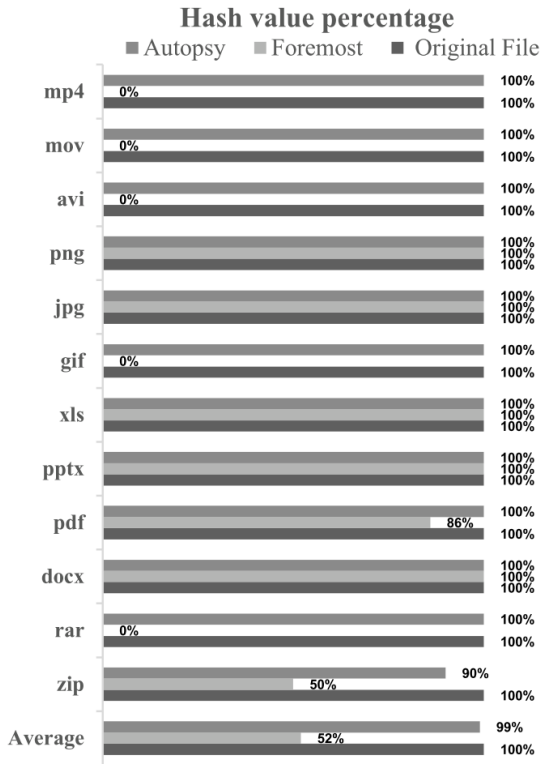

Fig. 21. Percentage of recovered file

Fig. 21 compares the recovery capabilities of Foremost and Autopsy software across various file types. For zip files, Foremost achieved a 50% recovery rate, while Autopsy recovered 100%. Foremost was unsuccessful in recovering any rar files, whereas Autopsy retrieved ten rar files, although only three retained matching hash values, giving rar files a 30% success rate in Autopsy. Both software programs successfully restored docx, pptx, xlsx, jpg, and png files with a 100% recovery rate. Foremost achieved an 86% success rate for pdf files, compared to Autopsy 100%. Foremost failed to recover gif, avi, mov, and mp4 files, while Autopsy recovered them all with 100% success. Overall, Foremost had a 52% recovery success rate, while Autopsy achieved 92%, showing Autopsy superior performance.

Further analysis of the zip files in Autopsy revealed that one file was not recovered, which was the reason not particularly found. Mov.zip is smaller than avi.zip, but avi.zip is recovered successfully with the same hash value as the original file. For the rar extension, ten files were restored without issues. docx, xlsx, pptx, and pdf files were each recovered as 2 identical files with different names and the same hash value. Each extension has 14 files from 7 original files. Autopsy also recovered twice the expected number of avi and mp4 files, generating 14 files from the original seven. Similarly, Autopsy produced 7 mov extension copies from 7 originals. Image file recovery varied by type, with GIF files showing 10 copies instead of the expected 5. jpg and png files have the same pattern recovering 14 files from 7 files each, but jpg has 8 extra files with 2 different images and 4 copies of each image that are extracted from docx, pptx, and pdf files. The last is png have 4 extra files with 2 different images that come from the Screenshot that crop become 8 extra images in jpg.

2.3. Result comparation

Foremost and Autopsy recovery software have different approaches, Foremost runs on Ubuntu recovering files on the base layer which from 1.25 GB with 89 files original files recovered 214 MB with 84 files on SATA SSD and 490 MB with 100 files on External SSD. Although External SSD seems to have bigger recovering files, the files successfully recovered with the same hash value indicate the same percentage, because some of the previous files before the research step are also recovered. External SSDs have more recovered file capacity because the SSD is used as a media to store data, and it's formatted before research begins. The SATA SSD is a brand-new SSD filled with research files. The reason of choosing Foremost as recovery software is it run on Linux which Prevent viruses on the SSD for change and or damaging the system or data on Windows.

Autopsy is a comprehensive digital forensics tool that operates on the Windows platform, used extensively for file recovery and analysis. In this research Autopsy version 4.2.1 was employed to examine a 120 GB SATA SSD and a 512 GB external SSD. The software's capabilities were assessed for its effectiveness in recovering deleted data and maintaining the integrity of the recovered files shown on Table 3 and 4 for comparison.

Table 3. Time of recovery

Storage Type	Foremost	Autopsy
SATA SSD	30 April 2024 20:01:41 – 30 April 2024 20:28:05 (26 minutes 24 second)	29 April 2024 14:20:00 – 29 April 2024 18:11:20 (3 hours 51 minutes and 20 seconds)
External mSATA SSD	19 June 2024 13:51:50 – 22 June 2024 19:25:27 (3 days 5 hours 33 minutes and 37 seconds)	15 November 2024 22:41:28 – 17 November 2024 15:57:18 (1 day 17 hours 15 and 50 seconds)

Table 4. Result of recovery

Storage Type	Foremost	Autopsy
SATA SSD	214 MB 86 recovered files and 1 audit file	3.95 GB (876 files total) with 2.18 GB (213 recovered files)
External mSATA SSD	489 MB 100 recovered files and 1 audit file	202 GB (441,202 Files total) with 32.9 GB (19.281 recovered files)

3. Conclusion

In the field of digital forensics, the deletion or formatting of data on storage media poses significant challenges for the recovery and analysis of digital evidence. As a result, forensic investigations must be conducted meticulously using standardized procedures. ACPO has utilized research on Foremost and Autopsy software to recover data from formatted SSDs. Detailed file recovery steps can assist researchers and computer technicians in supporting law enforcement agencies. Created and modified times detail on recovered files not changed, files can be used in investigative work to proof valid evidence. Findings indicate Autopsy outperformed Foremost, achieved higher success rate of 94% and 99% compared to Foremost 52% for both SATA SSD and mSATA SSD. This is attributed to Autopsy's advanced recovery tools, which enable deeper data recovery, while Foremost relies on basic recovery methods targeting files with identical hash values.

In conclusion, Autopsy proves to be more effective in retrieving deleted or formatted files, providing reliable evidence for law enforcement. Future research could focus on improving recovery success rates across various SSD types and other NAND flash devices, such as smartphones and flash drives. Additionally, advancements in AI and machine learning could offer automated and accurate solutions for detecting and recovering deleted or corrupted files, further enhancing digital forensic practices.

References

[1] Barr-Smith, F., Farrant, T., Leonard-Lagarde, B., Rigby, D., Rigby, S., & Sibley-Calder, F. (2021). Dead Man's Switch: Forensic Autopsy of the Nintendo Switch. *Forensic* Science *International: Digital Investigation*, *36*, 301110. https://doi.org/10.1016/j.fsidi.2021.301110

[2] Brown, D., Walker, T. O., Blanco, J. A., Ives, R. W., Ngo, H. T., Shey, J., & Rakvic, R. (2021). Detecting firmware modification on solid state drives via current draw analysis. *Computers & Security*, *102*, 102149. https://doi.org/10.1016/j.cose.2020.102149

[3] Chamkha, A., Veismoradi, A., Ghalambaz, M., & Talebizadehsardari, P. (2020). Phase change heat transfer in an L-shape heatsink occupied with paraffin-copper metal foam. *Applied Thermal Engineering*, *177*, 115493. https://doi.org/10.1016/j.applthermaleng.2020.115493

[4] Domingues, P., Andrade, L. M., & Frade, M. (2021). Microsoft's Your Phone environment from a digital forensic perspective. *Forensic Science International: Digital Investigation*, *38*, 301177. https://doi.org/10.1016/j.fsidi.2021.301177

[5] Domingues, P., Frade, M., Andrade, L. M., & Silva, J. V. (2019). Digital forensic artifacts of the Your Phone application in Windows 10. *Digital Investigation*, *30*, 32–42. https://doi.org/10.1016/j.diin.2019.06.003

[6] Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, *48*, 301675. https://doi.org/10.1016/j.fsidi.2023.301675

[7] Genç, A., Doğan, H., Turhan, L., Kocakuşak, A., & Helhel, S. (2024). Investigation of the radiated emission of honeycomb structured aluminum foam/cellular heatsinks at 1–10 GHz. *Materials Chemistry and Physics*, *324*, 129614. https://doi.org/10.1016/j.matchemphys.2024.129614

[8] Gnani, E., & Baccarani, G. (2024). Memory devices—Non-volatile memories. In *Encyclopedia of Condensed Matter Physics* (pp. 552–575). Elsevier. https://doi.org/10.1016/B978-0-323-90800-9.00236-5

[9] Gonzales, L., LaTourrette, N., & Doherty, B. (2025). AKF: A modern synthesis framework for building datasets in digital forensics. *Forensic Science International: Digital Investigation*, *55*, 302004. https://doi.org/10.1016/j.fsidi.2025.302004

[10] Gruber, J., Hargreaves, C. J., & Freiling, F. C. (2023). Contamination of digital evidence: Understanding an underexposed risk. *Forensic Science International: Digital Investigation*, *44*, 301501. https://doi.org/10.1016/j.fsidi.2023.301501

[11] Horsman, G. (2021). Digital evidence and the crime scene. *Science & Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

[12] Kim, D., Kim, J., Choi, K., Han, H., Ryu, M., & Kang, S. (2024). Dynamic zone redistribution for key-value stores on zoned namespaces SSDs. *Journal of Systems Architecture*, *152*, 103159. https://doi.org/10.1016/j.sysarc.2024.103159

[13] Kim, S., Jung, J., Kang, H., Yoon, Y., Cho, S., Park, M., & Han, S. (2025). An effective automotive forensic technique utilizing various logs of Android-based In-vehicle infotainment systems. *Forensic Science International: Digital Investigation*, *55*, 301990. https://doi.org/10.1016/j.fsidi.2025.301990

[14] Kumar, U., & Venkaiah, V. Ch. (2022). An Efficient Message Authentication Code Based on Modified MD5-384 Bits Hash Function and Quasigroup: *International Journal of Cloud Applications and Computing*, *12*(1), 1–27. https://doi.org/10.4018/IJCAC.308275

[15] Li, X., Kim, M., Lee, S., Zhai, Z., & Kim, J. (2025). Program context-assisted address translation for high-capacity SSDs. *Future Generation Computer Systems*, *162*, 107483. https://doi.org/10.1016/j.future.2024.107483

[16] Liu, J., Wang, T., Chen, X., Li, C., Shen, Z., & Zhang, Z. (2024). H 2 -RAID: Improving the reliability of SSD RAID with unified SSD and HDD hybrid architecture. *Microprocessors and Microsystems*, *105*, 104993. https://doi.org/10.1016/j.micpro.2023.104993

[17] Luo, L., Li, S., Lv, Y., & Shi, L. (2023). Performance and reliability optimization for high-density flash-based hybrid SSDs. *Journal of Systems Architecture*, *136*, 102830. https://doi.org/10.1016/j.sysarc.2023.102830

[18] Miller, C. M. (2023). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy*, *6*, 100296. https://doi.org/10.1016/j.fsisyn.2022.100296

[19] Mohammed Ali, A., & Kadhim Farhan, A. (2020). A Novel Improvement With an Effective Expansion to Enhance the MD5 Hash Function for Verification of a Secure E-Document. *IEEE Access*, *8*, 80290–80304. https://doi.org/10.1109/ACCESS.2020.2989050

[20] Park, A., Ryu, H., Park, W., & Jeong, D. (2023). Forensic investigation framework for cryptocurrency wallet in the end device. *Computers & Security*, *133*, 103392. https://doi.org/10.1016/j.cose.2023.103392

[21] Park, J., Kim, S., Cho, T., & Kang, M. (2025). Optimization of read operation for low power consumption in 3D NAND flash memory. *Microelectronic Engineering*, *298*, 112324. https://doi.org/10.1016/j.mee.2025.112324

[22] Ryu, J., Noh, D. K., & Kang, K. (2024). FlashPage: A read cache for low-latency SSDs in web proxy servers. *Engineering Science and Technology, an International Journal*, *51*, 101639. https://doi.org/10.1016/j.jestch.2024.101639

[23] Santikellur, P., Buddhanoy, M., Sakib, S., Ray, B., & Chakraborty, R. S. (2023). A shared page-aware machine learning assisted method for predicting and improving multi-level cell NAND flash memory life expectancy. *Microelectronics Reliability*, *140*, 114867. https://doi.org/10.1016/j.microrel.2022.114867

[24] Sokol, P., Antoni, Ľ., Kríďlo, O., Marková, E., Kováčová, K., & Krajči, S. (2023). Formal concept analysis approach to understand digital evidence relationships. *International Journal of Approximate Reasoning*, *159*, 108940. https://doi.org/10.1016/j.ijar.2023.108940

[25] Solodov, D., & Solodov, I. (2021). Data recovery in a case of fire-damaged Hard Disk Drives and Solid-State Drives. *Forensic Science International: Reports*, *3*, 100199. https://doi.org/10.1016/j.fsir.2021.100199

[26] Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, *49*, 105801. https://doi.org/10.1016/j.clsr.2023.105801

[27] Tok, Y. C., Zheng, D. Y., & Chattopadhyay, S. (2025). A Smart City Infrastructure ontology for threats, cybercrime, and digital forensic investigation. *Forensic Science International: Digital Investigation*, *52*, 301883. https://doi.org/10.1016/j.fsidi.2025.301883

[28] Wickramasekara, A., Breitinger, F., & Scanlon, M. (2025). Exploring the potential of large language models for improving digital forensic investigation efficiency. *Forensic Science International: Digital Investigation*, *52*, 301859. https://doi.org/10.1016/j.fsidi.2024.301859

[29] Xi, J., Siegel, M., Labudde, D., & Spranger, M. (2025). Towards a joint semantic analysis in mobile forensics environments. *Forensic Science International: Digital Investigation*, *52*, 301846. https://doi.org/10.1016/j.fsidi.2024.301846

[30] Yun, W., Kang, J., Lee, S., & Park, J. (2025). Digital forensic approaches to Intel and AMD firmware RAID systems. *Forensic Science International: Digital Investigation*, *54*, 301971. https://doi.org/10.1016/j.fsidi.2025.301971

M.Sc. Khoirul Anam Dahlan
e-mail: khoirul.anam@itesa.ac.id

A lecturer at Institut Teknologi Statistika dan Bisnis (ITESA) Muhammadiyah Semarang, Indonesia. He is an early-career researcher whose interests include system recovery, image forensics, and digital storage technologies. He has published several papers in national journals.

https://orcid.org/0009-0001-3535-965X

Ph.D. Anton Yudhana
e-mail: eyudhana@mti.uad.ac.id

Associate professor in electrical engineering at Universitas Ahmad Dahlan and Head of the Institute for Research and Community Service (LPPM). He received the Gold Winner award in the Academic Leader DIKTISAINTEK 2024 competition. His h-index is 30. His research interests include multimedia communications, signal processing, and wireless communications.

https://orcid.org/0000-0001-5451-454X

Ph.D. Herman Yuliansyah
e-mail: herman.yuliansyah@tif.uad.ac.id

Earned his S.T. from Universitas Muhammadiyah Yogyakarta in 2007 and his M.Eng. in information technology from Universitas Gadjah Mada in 2011. He is currently pursuing a Ph.D. at Universiti Kebangsaan Malaysia and has been a lecturer at Universitas Ahmad Dahlan since 2011. His h-index amounts to 12.
He is a lecturer and researcher whose interests focus on complex networks, link prediction, social computing, and text mining.

https://orcid.org/0009-0008-9114-4742