Performance of Forensic Investigation Tools on SSD Storage Using NIST Method

Bashor Fauzan Muthohirin1, a) Fajar Mayda Salam1, Imelda Azalia Rahma1

Author Affiliations

1 Informatics, Universitas Muhammadiyah Malang, Malang City, Indonesia

Author Emails

a) Corresponding author: bashorfauzan@umm.ac.id

b) fajarmayda14@gmail.com

c) imeldaazaliyaa@gmail.com

**Abstract.** Storage media has a very crucial role in storing important data, one type of storage is Solid State Drive (SSD), SSD is widely used because of its speed and efficiency. Because of this, SSD becomes a storage media that can be used to store evidence of fraud. Therefore, a digital forensics process is needed to acquire data from SSD. This is a challenge in itself because the storage mechanism is different from traditional media. This study analyzes the performance of three forensic tools, namely FTK Imager, Autopsy, and ProDiscover, in the data acquisition process on SSD. The evaluation was carried out by comparing the time required for each tool to acquire various types of files with the same size and format. This study uses the National Institute of Standards and Technology (NIST) standard method, which consists of the Collection, Examination, Analysis, and Reporting stages. The results of the study showed that of the 16 types of files tested, Autopsy had the fastest acquisition time, which was 6 minutes 44 seconds, while FTK Imager and ProDiscover took longer. These findings provide insight for forensic practitioners in choosing the most efficient tools for the data acquisition process on SSDs, as well as highlighting the importance of optimizing forensic methods in digital investigations.

# Introduction

The rapid advancement of the digital world has led to an increase in cybercrime, making it one of the major threats to data and information security. Cybercrimes include data theft, malware distribution, and hacking[1]. To mitigate these threats, digital forensics plays a crucial role in legal investigations. The primary objective of forensic analysis is to identify all relevant events, assess their impact on the system, and gather necessary evidence to prevent future incidents by detecting malicious techniques. Digital forensics applies scientific methods and computer technology to investigate digital crimes through computer networks, aiding in reconstructing criminal events and preventing unauthorized activities that could compromise system operations[2][3].

Research conducted by digital forensics [4] performed a qualitative review of various studies related to digital forensics and identified major challenges, particularly in the acquisition and pre-processing of evidence due to counter-analysis methods and difficulties in collecting data from devices and cloud storage. In addition to technical issues, procedural challenges were also highlighted, including readiness, reporting, presentation, and ethical concerns, particularly regarding privacy[5][6].

Research by [7] highlighted that while SSDs offer significant advantages over HDDs in terms of size, speed, and ease of use, they also present challenges for digital forensics. Forensic tools that were previously effective for HDDs have become less efficient in analyzing SSD. This research evaluated the effectiveness of forensic tools in analyzing data from both HDDs and SSD by comparing the results obtained from each storage type [8][9].

Research by [10] compared the impact of enabling and disabling the TRIM function on NVMe SSDs to assess the effectiveness of forensic and data recovery tools in retrieving digital evidence. The findings indicate that when the TRIM function is disabled, digital evidence remains intact, as demonstrated by identical hash values between the original and recovered files. Conversely, when TRIM is enabled, files become corrupted and irrecoverable, compromising the integrity of digital evidence[11][12].

Research by [13], forensic evidence was retrieved from an SSD configured with Deep Freeze. The results revealed that features such as TRIM, garbage collection, and wear leveling on SSDs can automatically delete data, making digital forensic recovery more challenging. Of the four tools tested, only Autopsy and Photorec successfully recovered deleted files[14][15].

Research by [16] successfully developed a Detection and Investigation Model (DIM) for identifying and investigating attacks on hard disk drives (HDDs) using the FTK Imager forensic tool. This model consists of three main phases: detection, data collection, and analysis. Evaluation through real-world scenarios demonstrated that DIM effectively detects and investigates HDD attacks. Therefore, organizations can adopt this model to enhance security and forensic investigations related to HDD threats [12][17].

Research by [18] assessed the efficiency and effectiveness of ProDiscover in investigating workplace cybercrimes, using a case research of an employee suspected of downloading unauthorized content. ProDiscover successfully recovered deleted image files from diskettes, demonstrating its capability to support forensic investigations and strengthen information security[19][20].

Reseach by [21] This research highlights the challenges in the forensic acquisition process on SSDs using the NIST method. The study identifies gaps in the guidelines currently used by organizations, including the Cyber Security Framework (CSF)[22], which need to be updated to address evolving cybersecurity threats. The results of this study emphasize the importance of updating forensic guidelines to better align with modern storage technologies, thereby increasing the effectiveness of forensic investigations and incident response[23].

Based on previous research, This research aims to evaluate the performance of forensic tools FTK Imager, Autopsy, and ProDiscover in the data acquisition process on Solid State Drive (SSD). The method used in this research is the National Institute of Standards and Technology (NIST), this research will ensure that forensic investigations are carried out in a structured and standardized manner. This research will compare the number of files successfully acquired and the time required by each tool in performing various types of files. The results of this research are expected to provide insight into the efficiency and reliability of each tool in digital forensic analysis on SSD storage media.

## RESEARCH METHOD

In this research, the National Institute of Standards and Technology (NIST) methodology was applied. Implementing a method that adheres to standard procedures for acquiring digital evidence in the form of forensic data significantly impacts the success of an investigation [24]. The NIST methodology consists of a series of structured procedures, including the stages of identification, acquisition, analysis, and reporting of digital evidence [25]. With a focus on maintaining data integrity through techniques such as hashing and strict documentation. The NIST stages are as shown in Figure 1:

Reporting

Analysis

Examination

Collection

**Figure** 1. Process Flow in the NIST Method

**Collection**

The first phase of this process involves identifying, tabulating, and acquiring data from relevant sources while adhering to guidelines and procedures that ensure data security. Forensic tools such as FTK Imager, Autopsy, and ProDiscover are then prepared to assist in the collection and analysis of digital evidence from the suspect’s device*.*

**Examination**

The second phase, examination, involves processing large volumes of forensic data using tools such as FTK Imager, Autopsy, and ProDiscover while maintaining data integrity. The roles of these forensic tools in this phase are as follows:

* + FTK Imager is used to perform in-depth analysis of the collected data. FTK Imager allows researchers to process data quickly and efficiently, and extract deleted information.
  + Autopsy acts as a forensic analysis platform that allows researchers to explore collected data and extract relevant information using a variety of built-in plugins and tools. Autopsy also supports a variety of file systems and data formats.
  + ProDiscover is another tool used in this phase to extract digital evidence from various devices. This tool is very useful for in-depth analysis of system files and metadata, and to ensure that no important data is missed.

**Analysis**

At this stage, researchers analyze the evidence acquired using forensic tools. The roles of digital forensic tools in this phase are as follows:

* + FTK Imager: Provides a variety of analysis tools that allow researchers to quickly identify and retrieve digital evidence. FTK Imager has the ability to analyze a variety of data types, including images, and deleted files, and can create indexes that make it easier to find specific information.
  + Autopsy: Facilitates forensic analysis with an easy-to-use interface and a variety of powerful analysis features. Autopsy allows investigators to extract and interpret information such as user activity.
  + ProDiscover: Used to perform in-depth analysis of file structures and metadata, providing insight into how and when data was created, modified, or accessed. This tool can also be used to identify anomalies or patterns that may indicate illegal or suspicious activity.

**Reporting**

The final phase involves documenting and reporting the findings of the forensic investigation. This includes detailing the procedures followed, the tools utilized, and the results obtained, ensuring that all forensic evidence is presented clearly and comprehensively.

## RESULTS AND DISCUSSION

In this research process there are the following scenarios:

**SSD**

Akusisi FTK Imager

Autopsy

ProDiscover

**Figure** **2.** scenario research

Figure 2 illustrates the process of collecting evidence stored in the suspect's SSD and acquiring it using the specified forensic tools. The SSD used in this scenario is an M.2 NVMe 2242 SSD. In this process, the researcher inputs various file types before performing data acquisition using the selected forensic tools.

**Collection**

The collection phase involves systematically gathering data to be used as digital evidence from the SSD. To ensure data authenticity, all evidence is hashed. Table 1 presents the results of the file hashing process.

**Table** 1. Hashing of evidence files

|  |  |  |
| --- | --- | --- |
| **No** | **File name and type** | **Hash files** |
| 1 | archive.zip | a6903046ec2479db908804c870c4c00b |
| 2 | HOUSE PRICES IN SOUTH JAVA.xlsx | 607096e1d5db1d549bfc358c82bfdecd |
| 3 | How to Cover Up a Murder in 24 Hours.mp4 | 69ad4b7293a62c47e1530490539541fd |
| 4 | How To Hide Stuff from The Police (r\_AskReddit).mp4 | 7d8b5593ba583db157b36b8f9427c5e3 |
| 5 | images (1).jfif | 3cdf89c2ba7aa3780e6b3440eb1ac40f |
| 6 | images (2).jfif | 29cfbbe91efedf267b01e1e8bf7642a5 |
| 7 | images (3).jfif | 2423c7c87edae2050316124d6d4d86d5 |
| 8 | images (4).jfif | 192118c73606df4f3fbc5c5d0d4969b5 |
| 9 | images.jfif | 6dc0d7c3485e393d8d92af2d48d9383f |
| 10 | home journal.docx | a7ccf64f1acc430031cc98872d98881d |
| 11 | making an Axe from a disk.mp4 | 38ae26be312ad7203edacf31bcd85136 |
| 12 | repair.rar | 1e00b0ca3f276d95a67e48d371849f9d |
| 13 | Screenshot (60).png | 72f326471a2c83af56dda4abf3b68fb4 |
| 14 | setup\_mobileditphonemanager\_10.8.0.29556\_win32.exe | d4068b0e0bf624951811bc312308e3c2 |
| 15 | videoplayback.mp3 | c950ffd4b228ae59351f8f9dbd271130 |
| 16 | videoplayback2.mp4 | ec4088338878a449bd813d9316fc7e3e |

**Examination**

At this stage, forensic analysis is conducted using three predetermined tools, with test results obtained from each tool as follows:

* + FTK Imager : The following image shows the results of data acquisition using the FTK Imager forensic tool.

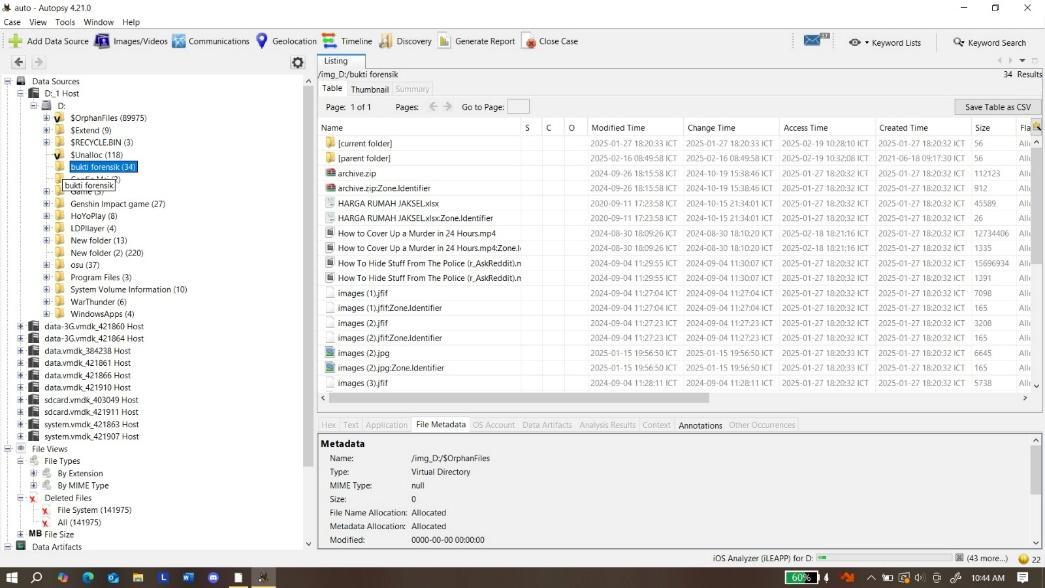
A screenshot of a computer

AI-generated content may be incorrect.

**Figure** 3. FTK Imager acquisition results

Figure 3 presents the results obtained from the FTK Imager forensic tool. The tool successfully extracted evidence, including images, videos, applications, zip files, and other data types.

* Autopsy : Figure 4 illustrates the acquisition results using Autopsy, where the tool successfully recovered various types of digital evidence, including images, videos, applications, zip files, and other files.



**Figure** 4 results of autopsy tools acquisition

Figure 4. This is the result of acquisition using autopsy tools, the tools successfully obtained evidence such as images, videos, applications, zip files and others.

* ProDiscover : The following is an image of the results of data acquisition using the ProDiscover forensic tool.

**A screenshot of a computer

AI-generated content may be incorrect.**

**Figure** 5 results of Discovery tools acquisition

Figure 5 illustrates the results of data acquisition using ProDiscover, where the tool successfully extracted digital evidence, including images, videos, applications, zip files, and other file type.

**Analysis**

Based on the results of forensic tool testing conducted on SSD, the following are the findings in the form of table 2.

Table 2. Hashing Results of Digital Evidence Files

|  |  |  |  |
| --- | --- | --- | --- |
| **Acquisition Results** | **FTK Imager** | **Autopsy** | **Prodiskcover** |
| archive.zip | 1 | 1 | 1 |
| HOUSE PRICES IN SOUTH JAVA.xlsx | 1 | 1 | 1 |
| How to Cover Up a Murder in 24 Hours.mp4 | 1 | 1 | 1 |
| How To Hide Stuff from The Police (r\_AskReddit).mp4 | 1 | 1 |  |
| images (1).jfif | 1 | 1 | 1 |
| images (2).jfif | 1 | 1 | 1 |
| images (3).jfif | 1 | 1 | 1 |
| images (4).jfif | 1 | 1 | 1 |
| images.jfif | 1 | 1 | 1 |
| home journal.docx | 1 | 1 | 1 |
| making an Axe from a disk.mp4 | 1 | 1 | 1 |
| repair.rar | 1 | 1 |  |
| Screenshot (60).png |  | 1 |  |
| setup\_mobileditphonemanager\_10.8.0.29556\_win32.exe | 1 | 1 | 1 |
| videoplayback.mp3 | 1 | 1 | 1 |
| videoplayback2.mp4 | 1 | 1 | 1 |

**Reporting**

FTK Imager successfully acquired 15 files from the SSD, requiring 16 minutes and 15 seconds for the data acquisition process. Autopsy successfully identified all 16 files, completing the acquisition in 6 minutes and 44 seconds. ProDiscover successfully recovered 13 files, with a total processing time of 7 minutes and 23 seconds.

## CONCLUSION

The implementation of NIST methodology in SSD forensics involves analysis using forensic tools and thorough documentation to ensure the validity of evidence. Based on the analysis of 16 acquired files using FTK Imager, ProDiscover, and Autopsy, each tool demonstrated distinct strengths and limitations. FTK Imager allows direct data review without requiring a copy but has a longer processing time of 10 minutes 25 seconds and struggles to recover deleted files. ProDiscover, while user-friendly, required 9 minutes 12 seconds to complete the acquisition and could only detect 13 files due to its limitations in data analysis. Autopsy proved to be the most efficient, completing the acquisition in 6 minutes 44 seconds, successfully identifying all 16 files, recovering deleted files, and generating comprehensive reports. Given its superior performance in forensic analysis, Autopsy is recommended for SSD investigations. To enhance forensic accuracy, continuous updates to forensic tools, integration of advanced technologies, and adherence to NIST guidelines remain essential

# References

[1] D. C. Raj Singh Deora, “Brief Study of Cybercrime on an Internet,” *JoCES*, no. 11, 2021.

[2] H. Himanshu, S. Bhatt, and L. Negi, “Digital Forensics Techniques and Trends: A Review,” *IAJIT*, vol. 20, no. 4, 2023, doi: 10.34028/iajit/20/4/11.

[3] K. Modi, K. Shukla, and F. Fiadufe, “Forensic investigation and analysis of malware in Windows OS,” *International Journal of Electronic Security and Digital Forensics*, vol. 17, pp. 169–182, Dec. 2024, doi: 10.1504/IJESDF.2025.143477.

[4] F. Casino *et al.*, “Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews,” *IEEE Access*, vol. 10, pp. 25464–25493, 2022, doi: 10.1109/ACCESS.2022.3154059.

[5] S. Erinfolami, O. S. Onyenaucheya, A. Adams, and O. E. Abudu, “Digital Forensics in Cybersecurity,” vol. 8, no. 6, 2024.

[6] A. I. H. Nasrullah, B. F. Muthohirin, and H. A. Humaidi, “Optimization of Thin-Walled Battery Protector Design for Electric Vehicles Under Ground Impact Conditions Using Genetic Algorithm,” 2025. doi: 10.2139/ssrn.5101261.

[7] M. Jazzar and M. Hamad, “Comparing HDD to SSD from a Digital Forensic Perspective,” 2022, pp. 169–181. doi: 10.1007/978-981-16-7136-4\_14.

[8] S. R. Kasenda, H. P. Lumi, L. V. Wawointana, R. Kohongia, L. F. Sabonbaly, and R. P. Djafar, “Effect of Ssd Vs Hdd Selection on Computer Boot Speed,” *JSA*, vol. 5, no. 12, pp. 5440–5443, Dec. 2024, doi: 10.46799/jsa.v5i12.1871.

[9] Srinivas University, India, A. S. Pallivalappil, J. S N, and Srinivas University, India, “SSD DISCORE - A SCORING METHOD FOR SSD’S DATA INTEGRITY VALIDATION USING DIFFERENT SMART ATTRIBUTES IN THE DIGITAL FORENSICS PROCESS,” *IJCT*, vol. 15, no. 1, pp. 3126–3131, Mar. 2024, doi: 10.21917/ijct.2024.0465.

[10] W. Pranoto, I. RIadi, and Y. Prayudi, “Live Forensics Method for Acquisition on the Solid State Drive (SSD) NVMe TRIM Function,” *KINETIK*, pp. 129–138, May 2020, doi: 10.22219/kinetik.v5i2.1032.

[11] S. Zhai, D. Shang, S. Wang, and S. Dong, “DF-SSD: An Improved SSD Object Detection Algorithm Based on DenseNet and Feature Fusion,” *IEEE Access*, vol. 8, pp. 24344–24357, 2020, doi: 10.1109/ACCESS.2020.2971026.

[12] H. J. Hadi, N. Musthaq, and I. U. Khan, “SSD Forensic: Evidence Generation and Forensic Research on Solid State Drives Using Trim Analysis,” in *2021 International Conference on Cyber Warfare and Security (ICCWS)*, Islamabad, Pakistan: IEEE, Nov. 2021, pp. 51–56. doi: 10.1109/ICCWS53234.2021.9702989.

[13] M. Iqbal and Benfano Soewito, “Digital Forensics on Solid State Drive (SSD) with TRIM Feature Enabled and Deep Freeze Configuration Using Static Forensic Methods and ACPO Framework,” Nov. 2020, doi: 10.5281/ZENODO.4428140.

[14] X. Zhang *et al.*, “Storage Abstractions for SSDs: The Past, Present, and Future,” *ACM Transactions on Storage*, vol. 21, Dec. 2024, doi: 10.1145/3708992.

[15] N. Liana, Rahmayanti, Ade Ira Octa Femi, Rifki Mulia, Rusli, and Muhammad Hatta, “The Role Of Forensic Autopsy In Proof Of The Crime Of Planning Murder,” *IJLSH*, vol. 1, no. 2, pp. 91–99, Nov. 2024, doi: 10.70193/ijlsh.v1i2.161.

[16] A. Alshammari, “Detection and Investigation Model for the Hard Disk Drive Attacks using FTK Imager,” *IJACSA*, vol. 14, no. 7, 2023, doi: 10.14569/IJACSA.2023.0140784.

[17] A. L. M. Abdon, J. C. M. Ang, K. N. Domingo, and J. E. Gutierrez, “Automated Windows-Based Timelining Tool for Memory and Disk Image Analysis: Leveraging Timsort Algorithm with WinPmem, FTK Imager, Volatility 3 and The Sleuth Kit,” *IJCSMC*, vol. 13, no. 8, pp. 16–22, Aug. 2024, doi: 10.47760/ijcsmc.2024.v13i08.002.

[18] B. S. Fakiha, “Cybersecurity: Analysis and Application of ProDiscover Forensic Toolkit,” *SM*, vol. 15, no. 3, pp. 146–152, Jun. 2022, doi: 10.71164/socialmedicine.v15i3.2022.1453.

[19] G. R. Panigrahi, N. K. Barpanda, and P. K. Sethy, “Navigating the cyber forensics landscape a review of recent innovations,” *IJ-ICT*, vol. 13, no. 1, p. 27, Apr. 2024, doi: 10.11591/ijict.v13i1.pp27-33.

[20] G. A. Halefom, “Verification of commonly used artifacts in Windows Forensics using open-source tools,” Nov. 2021.

[21] A. S. Pallivalappil, “Procedures for Digital Forensics and Incident Response on Including Data Integrity Constraints on Solid-State Drives (SSD) - A Literature Review,” vol. 6, no. 1, 2022.

[22] W. Sawangphol, A. Khurat, and N. Niampradit, “SecSAGE: NIST Cybersecurity Framework Visualization on SAGE2,” *ECTI-CIT Transactions*, vol. 18, no. 3, pp. 417–428, Aug. 2024, doi: 10.37936/ecti-cit.2024183.256034.

[23] D. Dunsin, M. C. Ghanem, K. Ouazzane, and V. Vassilev, “Reinforcement learning for an efficient and effective malware investigation during cyber incident response,” *High-Confidence Computing*, p. 100299, Jan. 2025, doi: 10.1016/j.hcc.2025.100299.

[24] Aljumaiah, O., Jiang, W., Addula, S. R., & Almaiah, M. A. (2025). Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework. J. Cyber Secur. Risk Audit, 2025(2), 12-26.

[25] Vrana, G., Lou, D., & Kuang, R. (2025). Raw qpp-rng randomness via system jitter across platforms: a nist sp 800-90b evaluation. Scientific Reports, 15(1), 27718.