Investigating the Impact on Data Recovery in Computer Forensics

1st Semi Yulianto
Computer Science Department
Graduate Program, Doctor of Computer Science, Bina Nusantara University
Jakarta 11480, Indonesia
semi.yulianto@binus.ac.id

2nd Benfano Soewito
Computer Science Department
Graduate Program. Master of Computer Science, Bina Nusantara University
Jakarta 11480, Indonesia
bsoewito@binus.edu

2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs) | 979-8-3503-3943-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICoCICs58778.2023.10276573

Abstract – **Defragmentation can potentially be employed as a tactic by perpetrators to conceal, misrepresent, or eliminate digital evidence. This study explores the effects of minor defragmentation, a potential method to conceal digital evidence, on recovering file system data in digital forensics. Our investigation sought to determine the influence of minor defragmentation on the effectiveness of data recovery and to identify methods that can augment the success rate post-defragmentation. We limited the scope of this study to defragmentation in Hard Disk Drives (HDDs), solid-state drives (SSDs), and USB drives. A mixed-method approach employs a literature review, case studies, and controlled experiments. Comparative analysis was used as the main data analysis technique to investigate its impact. Preliminary findings suggest that minor defragmentation hampers data recovery; however, certain strategies can augment success rates. These results can significantly influence the development of data recovery policies, particularly those of digital forensic analysts and law enforcement. The primary objective of this study is to bolster the efficiency and dependability of file system data recovery post-defragmentation while upholding ethical and legal standards.**

Keywords—**defragmentation, data recovery, computer forensics, digital evidence, antiforensic**

I. Introduction

Digital forensic investigations often require data recovery from digital devices tampered with or intentionally destroyed. However, defragmentation poses significant challenges to the data-recovery capability of computer forensics. Defragmentation is a process that rearranges data on a hard drive or solid-state drive to improve performance. However, this has the potential to fragment and overwrite files, which would cause difficulties when attempting to recover data using standard techniques. To ensure no trace is left behind, suspects usually resort to various methods, including deleting files and encrypting the remaining files so that anyone else cannot access them easily. In addition, they may even use software programs specialized for erasing the hard drive, making it almost impossible for anyone other than them to recover any information from it. They even proceed with practices such as concealing information within unused storage spaces using advanced techniques such as steganography. Therefore, they rarely use defragmentation to achieve this particular aim. Therefore, people rarely use defragmentation to accomplish this specific aim. To achieve successful data recovery in digital forensics, understanding the impact of defragmentation is crucial.

Recent studies have examined several facets of digital forensics, including exploring various techniques to recover files/data while devising forensic analysis methods/anti-forensic measures. Additionally, researchers are making efforts toward developing efficient metadata-based recovery frameworks and formulating strategies for recovering the loss of information from particular DB systems. Further research is necessary to explore how disk defragmentation affects data recovery in forensics studies. This study intends to improve on prior research by investigating different methods for recovering data and utilizing defragmentation software. The key objective is to obtain significant insights into the impact of defragmentation on data recovery in computer forensic examinations. Finally, this study identifies the best approaches and techniques that increase the likelihood of victorious data restoration under such conditions.

This study has two primary objectives. First, it aims to demonstrate how criminal offenders can employ disk fragmentation to hinder forensic inquiry, thereby reducing the chances of successfully retrieving information. Second, it highlights how disk fragmentation on SSDs and flash drives offers no significant advantage in improving the chances of information retrieval. This study utilized a blend of qualitative and quantitative methodologies to meet these aims, which extensively examined the existing literature, conducted case studies, and conducted controlled experiments. To complete these experiments successfully, we used established disk images, various defragmentation tools, and various data recovery methods such as metadata analysis or file carving. Treatment approaches included deleting data with and without defragmentation. The aim is to fulfill the goals by combining qualitative and quantitative methods via a comprehensive review of existing literature, case studies, and controlled experiments. We utilized the prominent disk images and defragmentation tools in the experiments performed during the survey alongside data recovery techniques, such as file carving and metadata analysis. Additionally, we used different treatment methods, including deleting data either with or without defragmentation, during the procedures, which involved deleting data and performing disk defragmentation, based on the findings of this study.

II. Literature Review

This literature review provides an extensive analysis of computer forensics, which investigates the impact of defragmentation on data recovery while delving into the existing methods and approaches used for recovering lost or deleted information. Through a literature review, we can gain insight into the impact of defragmentation on data recovery and identify methods for effectively recovering lost or damaged information from fragmented hard drives. We conducted a comprehensive analysis of all relevant studies through our systematic review. Digital forensics has seen significant advancements in research, contributing enormously to cybersecurity. Researchers have presented various methodologies and frameworks to bolster the credibility and integrity of digital evidence [1]-[23]. Salman and Al Essa [1] introduced a distributed methodology for disk defragmentation. Their research was subsequently expanded by Park and Eom [14], who proposed a novel defragmentation tool for contemporary storage devices. Other researchers have focused on different aspects, such as detecting concealed information in FAT by Kuznetsov et al. [21] and the analysis of WannaCry ransomware's infection, propagation, persistence, and recovery prevention mechanisms by Akbanov et al. [23]. Alghamdi [24] further explores the role of digital forensics in cybersecurity, elucidating the recent trends, threats, and opportunities.

Artificial intelligence (AI) and machine learning have also been applied to digital forensics, creating new possibilities. For instance, Nikolakakis et al. [5] discussed learning tree structures from noisy data, while Maulik et al. [30] suggested using probabilistic neural networks for data recovery. Furthermore, Bozkir et al. [39] presented an approach for malware detection, integrating memory forensics, manifold learning, and computer vision. Pagani et al. [32] discussed a novel aspect of forensic analysis that integrated a temporal dimension into memory forensics.

The emergence of cloud computing and Internet of Things (IoT) technologies has created fresh challenges in digital forensics. Baldwin et al. [2] conducted a bibliometric analysis of cloud forensics research, while Gill et al. [10] provided a bibliometric analysis for mobile forensics. Additionally, various frameworks and solutions for cloud forensics were surveyed by Khanafseh et al. [25]. Prakash et al. [36] investigated the challenges and open problems in cloud and edge computing-based computer forensics. In the context of IoT forensics, MacDermott et al. [28] discussed the challenges faced in the IoA era, and Yaqoob et al. [47] conducted a comprehensive survey on IoT forensics, elaborating on recent advancements, taxonomy, requirements, and ongoing challenges.

The concept of anti-digital forensics is becoming increasingly important in digital technology, and researchers compared digital forensic methods to those of anti-digital forensic methods [12]. Their study also examined the limitations and recommendations of their respective techniques. The methodologies for digital forensics and anti-fraud are summarized by Majed et al. [29] as they go into further detail about this subject. A related study by Peng et al. [35] introduces a generative adversarial network that targets the regeneration of facial images as a means of anti-forgery. By illustrating how important it is to understand both creating and evading digital evidence, these studies also exemplify how the landscape for researching in this field has evolved.

Several studies on digital forensics offer valuable insights across various areas and highlight the challenges and strategies for recovering information from fragmented hard drives by exploring the impact of defragmentation on data recovery. Artificial intelligence, machine learning for cloud forensics, and cybersecurity developments are presented, along with the progress achieved in IoT forensics. Applying artificial intelligence (AI) and machine learning (ML) methods to digital forensics is promising. While acknowledging challenges and open problems in cloud and IoT forensics, these studies underscore the significance of specialized methodologies, revealing a dynamic field where researchers continually focus on improving data recovery methods and analytical techniques while addressing new challenges facing digital forensics.

This study differs from previous studies by focusing specifically on how defragmentation impacts data recovery in digital forensics. In addition, we designed this study to examine different levels of defragmentation for both HDDs and SSDs, aiming to provide a comprehensive understanding of their impact on data recovery efficiency and effectiveness. Unlike general overviews that offer only an overview without specifics, this study goes beyond identifying defragmentation's effects on data recovery processes. It also provides valuable insights into improving post-defragmentation data recovery by outlining various strategies and techniques. After conducting qualitative and quantitative analyses such as case studies and controlled experiments, we have suggested actionable recommendations to improve the success rate of data recovery post-defragmentation.

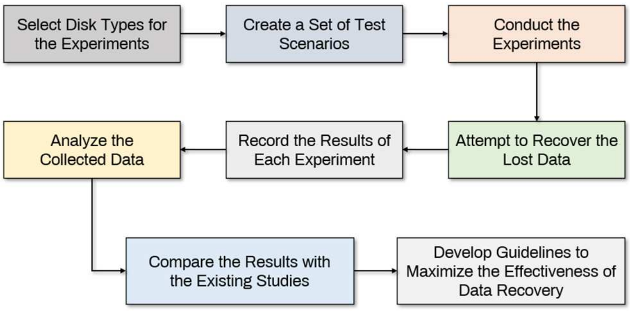
Additionally, this research has provided guidelines applicable for defragmentation for data recovery policies and procedures, which are useful for academics and professionals in digital forensics. It has also contributed to ethical and legally compliant digital forensic investigations by addressing practical considerations and societal implications in previous studies often overlooked. This study offers important observations and helpful recommendations for improving data retrieval in the context of defragmentation.

III. Methodology

The system requires selecting the correct disk types for experiments and designing multiple testing conditions. Once completed, we conducted the experiments with subsequent attempts to recover any potentially lost data, and we carefully documented and thoroughly analyzed the data obtained from each test. We compared the results with those from prior studies to assess their significance. Developing a set of best practices for optimizing data recovery initiatives is the result of these analyses, and these practices endeavor to enhance the data recovery process within the realm of digital forensics.

Figure I illustrates the methodology used in the controlled experiments. When conducting a controlled experiment, researchers must create an isolated and replicated system that resembles the original digital environment of the examined scenario. Investigators can run various tests or simulations while maintaining control over the variables involved; when performing a controlled experiment in computer forensics, the aim is to gather reliable and reproducible evidence while validating forensic techniques and assessing how different actions impact digital evidence, thereby drawing accurate conclusions based on empirical data.

We achieved a systematic and controlled approach to investigating by managing various factors. Based on the nature of our investigation, we monitored several elements such as environmental variables and data samples along with procedures and tools/software to achieve specific research objectives, and better comprehension of digital systems' behavior is possible for investigators by managing variables and conditions. In addition, it aids in assessing forensic tool reliability and testing the validity of specific investigative procedures.



Select Disk Types for the Experiments
Create a Set of Test Scenarios
Conduct the Experiments
Attempt to Recover the Lost Data
Record the Results of Each Experiment
Analyze the Collected Data
Compare the Results with the Existing Studies
Develop Guidelines to Maximize the Effectiveness of Data Recovery

Fig. 1. Approach For Conducting The Controlled Experiments

The experimental setup necessitated the use of specialized hardware, such as a laptop that had the latest components, such as a powerful Intel Core-i7 Processor clocked at a base frequency rate@2.8GHz (Quad-Core) that had cache memory upto@12MB to enhance its performance. Additionally, we equipped the laptop with an Integrated Power Unit (IPU) supporting high speeds up to @4.7Ghz, 16GB DDR4 RAM, and the latest Operating System, Windows 11 Pro (64-bit). We tested various forensic and data recovery tools during the evaluation phase, including commercial and open-source alternatives and custom-made scripts. We utilized digital forensic platforms, such as The Sleuth Kit, Autopsy, enCase, and Forensic Toolkit (FTK), to conduct fast yet comprehensive investigations on hard drives. In addition, we utilized specialized tools for performing tasks such as file carving, data refining, and metadata analysis to achieve greater efficiency. Examples of metadata analysis tools include Metadata Anonymization Toolkit (MAT) and ExifTool, while commonly used file carving tools include Foremost, Scalpel, and PhotoRec.R-studio and GetDataBack are two popular tools for data carving besides TestDisk. However, one should remember that depending on the disk type under analysis and the specific circumstances will determine how effectively such a tool operates. As a result, it is necessary to decide on the right tool accordingly.

To replicate various forms of data tampering in controlled experiments, we carefully selected magnetic disks (HDDs), solid-state disks (SSDs), and memory sticks (flash disks) as suitable disk types, each represented by three disks, for a total of nine disks. Each disk underwent preparational steps before starting the experiments to ensure that the disk was clean and sanitized. Owing to several limitations, other types of disks, such as hybrid drives, were not included in our experiments and might be included in our future work. The experiments employed different approaches, including two 1 TB HDDs, two 1 TB SSDs, and two 32 GB flash disks. The dataset comprised files in various formats, such as Microsoft Word documents (docx), Microsoft Excel documents (xlsx), Bitmap files (jpg), Text files (txt), and VMware Virtual Disk, with a total size of 2.08 GB (refer to Table I for details).

As part of the preparatory steps, we subjected the disks within each category to certain processes before undertaking data recovery and forensic analysis. The task sequence includes erasing and formatting data, defragmenting one disk while leaving another as is, and duplicating the disks using the bit-stream copy method to ensure a precise replication of all disk regions and the original data. The primary objective was to compare the results between disks with deleted data that underwent defragmentation and those that did not. We meticulously recorded and analyzed the findings from each experiment to establish guidelines and best practices for optimizing data recovery rates in defragmentation scenarios.

TABLE I. STORAGE AND FILE SYSTEMS SUMMARY

Disk Type	Storage Capacity	File System	Description
Magnetic Disk (HDD)	1 Terabyte (1 TB)	NTFS	The total size of the data is 2.08 GB, comprising ten files in various formats such as Microsoft Word documents (docx), Microsoft Excel documents (xlsx), Bitmap files (jpg), Text files (txt), and VMware Virtual Disk.
Solid-State Disk (SSD)	1 Terabyte (1 TB)	NTFS	
Memory Stick (flash disk)	32 Gigabytes (32 GB)	FAT32	

The study aimed to create test scenarios that simulated real-life situations where data loss occurs, and individuals may utilize defragmentation to impede forensic investigations. The experiments employed different treatment methods, including deleted data without defragmentation and deleted data with defragmentation. In addition, we intentionally defragmented some disks while leaving others unaltered, enabling a comparison of outcomes. Various data recovery techniques, such as file carving, metadata analysis, and data carving, were evaluated using open-source and commercial tools previously mentioned (e.g., PhotoRec, Foremost, Scalpel, Autopsy, ExifTool, MAT, TestDisk, GetDataBack, and R-Studio).

Table II shows different data recovery techniques commonly used in digital forensics investigations to recover deleted or damaged data from various storage devices. Each method has its strengths and weaknesses and should be selected based on the specific scenario and type of storage device involved.

TABLE II. DATA RECOVERY TECHNIQUES

Data Recovery Technique	Description
File Carving	A data recovery technique involves searching for files in a hard drive's disk image or unallocated space by looking for specific patterns of file headers and footers. We can use it to recover individual files or complete file systems.
Metadata Analysis	A data recovery technique involves examining file system metadata to determine which files were present on a disk before they were deleted or modified. We can use it to recover files that have been recently deleted or modified but not overwritten.
Data Carving	A data recovery technique involves searching for data in a hard drive's disk image or unallocated space by looking for specific patterns of data signatures or unique identifiers. We can use it to recover individual files or fragments of files that have been partially overwritten or fragmented.

The research methodology focuses on enhancing data recovery rates in scenarios involving defragmentation, a prevalent data recovery issue. The comparison of results between disks with and without defragmentation gives valuable insights into the efficiency of recovery techniques. This approach establishes a sturdy foundation for future research in data recovery techniques.

The study utilized a quantified approach to collect and analyze data obtained from simulations and experiments. We used a 1-to-5 scale rating system to measure defined variables, with higher scores indicating more positive results. The Likert scale, a widely used type of 1 to 5 scale rating system in surveys and evaluations, was utilized in the study. A recent review highlighted the continued use and development of the Likert scale and its variations in research and practice [17].

IV. Results

Defragmentation improves efficiency in Hard Disk Drives (HDDs) but harms Solid-State Drives (SSDs) and flash disks. Due to their structure, SSDs and flash disks are negatively affected by defragmentation, which can reduce their lifespan. On HDDs, data recovery, especially after defragmentation, allows for more favorable results because it can recover deleted data until it gets overwritten. However, the combination of wear leveling and TRIM functions in SSDs and flash disks complicates data recovery, with defragmentation potentially decreasing the chances of successful recovery by overwriting data. Despite SSDs and flash disks' advantages in speed and durability, HDDs have an advantage in data recovery following defragmentation.

TABLE III. COMPARISON OF DATA RECOVERY EFFECTIVENESS

Disk Type	WOD	WID	Data Recovery Techniques			Recovery Effect.	Score
			FC	MA	DC		
Magnetic Disk (HDD)	√		√			85%	4 (Great)
	√			√		80%	4 (Great)
	√				√	75%	3 (Good)
		√	√			70%	3 (Good)
		√		√		80%	3 (Good)
		√			√	75%	2 (Fair)
Solid-State Disk (SSD)	√		√			40%	2 (Fair)
	√			√		35%	1 (Poor)
	√				√	30%	1 (Poor)
		√	√			25%	1 (Poor)
		√		√		30%	1 (Poor)
		√			√	25%	1 (Poor)
Memory Stick (flash disk)	√		√			25%	1 (Poor)
	√			√		20%	1 (Poor)
	√				√	15%	1 (Poor)
		√	√			10%	1 (Poor)
		√		√		15%	1 (Poor)
		√			√	10%	1 (Poor)

[a] Treatment Type: WOD=Deleted Data without Defragmentation, WID=Deleted Data with Defragmentation

[b] Data Recovery Technique: FC=File Carving, MA=Metadata Analysis, DC=Data Carving

[c] Scale: 1=Poor; 2=Fair; 3=Good; 4=Great; 5=Excellent

Table III presents a comparative analysis of data recovery effectiveness, focusing on different disk types. The recovery effect serves as a metric to gauge the efficiency of data recovery techniques. The table outlines the recovery effects and corresponding scores associated with Magnetic Disks (HDD), Solid-State Disks (SSD), and Memory Sticks (flash disks). Recovery effects for Magnetic Disks range from 85% (Great) to 70% (Good), contingent upon supported techniques like File Carving (FC), Media Analysis (MA), and Deleted Files Recovery (DC). The corresponding scores span from 4 (Great) to 3 (Good). In the case of Solid-State Disks, recovery effects are comparatively lower, varying from 40% (Fair) to 25% (Poor), with scores ranging from 2 (Fair) to 1 (Poor). Memory Sticks exhibit the least favorable recovery effects, ranging from 25% (Poor) to 10% (Poor), with scores of 1 (Poor). We can calculate the recovery effect by evaluating the supported techniques for a specific disk type and assigning the highest score to them. Remember that the table provides general estimates and might not encompass every possible scenario or unique aspect of each technique.

Based on the information provided in Table III regarding various disks and the types of treatment applied to them for data recovery purposes, we can conclude that effectiveness varies depending on these factors. Restoring deleted data from magnetic disks can be effectively performed through file carving or metadata analysis techniques without performing any defragmentation (WOD). The former has attained an impressive recovery rate of up to 85%, whereas the latter has achieved almost 80 %. However, compared with these methods, data carving is not reliable. Defragmentation (WID) decreases the recoverability of all techniques employed, while file-carving and metadata analysis achieve recoverability rates of 75% and 70 %, respectively, and data-carving proves less effective. To recover data from solid-state disks and memory sticks, file carving and metadata analysis methods are superior to the data carving method, and WID has significantly lower recovery rates than WOD. While the former ranges between only 30 -1%, the latter offers higher success, with rates ranging up to as much as %40

The summary results presented in Table IV indicate that magnetic disks or hard disk drives (HDD) had the greatest possibility for successful data recovery among all three disks at a rate of 78%. In contrast, hard drives and tape backups boast higher recovery rates than the devices previously mentioned in the sentence; solid-state disks (SSD) stand out with their low recovery rate of only 31%. Memory sticks or flash drives fare even worse, with a mere 16%, and the likelihood of prosperous data recovery from SSDs and memory sticks may be relatively low for digital forensic investigators; hence, they must exercise caution during such procedures.

TABLE IV. SUMMARY OF THE AVERAGE EFFECTIVENESS OF DATA RECOVERY

Disk Type	Recovery Effectiveness
Magnetic Disk (HDD)	**78%**
- w/ Defragmentation	80%
- w/o Defragmentation	75%
Solid-State Disk (SSD)	**31%**
- w/ Defragmentation	27%
- w/o Defragmentation	35%
Memory Stick (flash disk)	**16%**
- w/ Defragmentation	12%
- w/o Defragmentation	20%

Significant differences exist between the recovery effectiveness scores of each disk type's different data recovery techniques. For Magnetic Disks (HDD), file carving (FC) and metadata analysis (MA) techniques have higher recovery effectiveness scores compared to the data carving (DC) method. However, the effectiveness of the strategies depends on whether the disk has undergone defragmentation (WID) or not (WOD). For example, the FC and MA techniques have higher recovery effectiveness scores for WOD than WID. For Solid-State Disks (SSD) and Memory Sticks (flash disks), the DC technique has the lowest recovery effectiveness scores compared to FC and MA techniques. The DC technique is generally less effective in recovering data from SSDs and flash disks than magnetic disks.

The analysis suggests that although defragmentation enhances the efficiency of data on Hard Disk Drives (HDDs), it hinders retrieving such information on Solid-State Drives (SSDs) and flash disks. These driving characteristics, such as wear leveling and TRIM, can explain why they are attributed. The intended use of TRIM functionality in solid-state drives (SSDs) is to provide information on safe-to-delete unused data

979-8-3503-3943-7/23/$31.00 ©2023 IEEE

blocks to optimize drive performance. In contrast, the impact of defragmentation on all storage devices, including SSDs and flash disks, where there is an increase in data overwriting and accelerated memory cell wear, significantly reduces the odds of recovering lost or deleted files. SSDs and flash disks offer less promising prospects for data retrieval post-defragmentation despite their advanced speed and durability than HDDs.

The study clarifies that the given effectiveness scores pertain to the scenarios and disk types under investigation. Other elements like the disk's size and complexity and the data recovery tool employed can influence the success of recovery techniques. As such, digital forensic examiners should meticulously evaluate each case's unique aspects to select the most suitable data recovery strategy. Customizing the data recovery approach to align with the situation, disk type, and handling method can increase the chances of successful data retrieval and minimize potential data loss. The study's findings also expose criminals' possible misuse of defragmentation to obstruct forensic investigations, consequently lowering the data recovery success rate. Finally, we also determined that defragmentation does not considerably benefit or influence data recovery from SSDs and flash disks.

While defragmentation is typically discouraged, perpetrators may use it to disrupt forensic investigations. However, when defragmentation is not a problem, techniques like file carving, metadata analysis, and data carving can effectively recover data from magnetic disks. However, such methods are less effective in SSDs and flash disks, which inherently show lower data recovery rates. Therefore, we recommend alternative methods for data recovery from magnetic disks. Furthermore, regularly backing up critical files and data and choosing reliable storage devices can help reduce the likelihood of data loss.

V. Conclusion And Future Work

This research highlights the significant impacts of defragmentation on forensic inquiries, underscoring the difficulties it introduces to data retrieval efforts. The evidence suggests that defragmentation can obstruct investigations and complicate the data recovery process, raising the possibility of its exploitation by offenders to impede forensic analyses; this necessitates a heightened awareness among forensic investigators. The study uncovers that more than defragmentation's efficacy in enhancing data recovery rates is needed for SSDs and flash drives. These storage types show a lower data recovery efficiency than their magnetic disk counterparts. Consequently, the study advocates for the thoughtful selection of data recovery methods tailored to the unique circumstances and traits of the disk under investigation.

Research on data recovery methods and techniques using technology-based tools requires adherence to strict guidelines regarding the privacy and confidentiality of collected information. Additionally, we should consider ethical considerations such as transparency and accountability. Obtaining permission is part of responsible research, and preserving data integrity and confidentiality is important. Additionally, ensuring accountability and transparency is crucial for adhering to legal procedures while upholding intellectual property rights. We should always avoid discrimination and entrust skilled professionals with research. These ethical measures were in place to ensure credible and ethical data recovery.

While the study offers insightful revelations, its limitations include small sample size, limited examination of disk types, focused perspective on data recovery efficiency, and absence of statistical analysis and external validation. Future studies should strive for a broader approach by using statistical methods, increasing sample size and diversity of disk types studied, expanding the research scope to include aspects like data security and privacy, seeking external validation, and addressing pertinent ethical considerations in data recovery.

We recommend several potential research avenues. Given their increasing popularity, it is essential to prioritize the development of novel data recovery strategies specifically designed for solid-state disks (SSDs) and flash drives. Also, a comprehensive evaluation of the impact of different defragmentation techniques on the efficacy of data recovery on magnetic disks (HDD) is warranted. Furthermore, exploring the effectiveness of data recovery techniques in various scenarios, including different types of disks like hybrid drives and under diverse techniques such as encryption and compression, could lead to the invention of more specialized and efficient methods.

Lastly, with the rising global interest in data privacy and security, it is paramount for future research to investigate the implications of data recovery techniques in these areas, particularly in the realm of digital forensics. Such research will strive to balance effective forensic investigation and respect for privacy rights. These suggested directions for future research could greatly benefit the field, equipping investigators to tackle better the challenges posed by defragmentation.

References

[1] A. Salman and H. A. Al Essa, "A Distributed Approach for Disk Defragmentation," Journal of University of Babylon for Pure and Applied Sciences, vol. 26, no. 3, pp. 1-5, 2018.

[2] Baldwin, O. M. Alhawi, S. Shaughnessy, A. Akinbi, and A. Dehghantanha, "Emerging from the cloud: A bibliometric analysis of cloud forensics studies," Cyber threat intelligence, pp. 311-331, 2018.

[3] Duan and X. Zhang, "Research on computer forensics technology based on data recovery," in Journal of Physics: Conference Series, vol. 1648, no. 3, p. 032025, 2020.

[4] Đuranec, D. Topolčić, K. Hausknecht, and D. Delija, "Investigating file use and knowledge with Windows 10 artifacts," in 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2019, pp. 1213-1218.

[5] E. Nikolakakis, D. S. Kalogerias, and A. D. Sarwate, "Learning tree structures from noisy data," in The 22nd International Conference on Artificial Intelligence and Statistics, 2019, pp. 1771-1782.

[6] Englbrecht, G. Langner, G. Pernul, and G. Quirchmayr, "Enhancing credibility of digital evidence through provenance-based incident response handling," in Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019, pp. 1-6.

[7] G. Shrivastava, K. Sharma, M. Khari, and S. E. Zohora, "Role of cyber security and cyber forensics in India," in Handbook of Research on Network Forensics and Analysis Techniques, pp. 143-161, IGI Global, 2018.

[8] G. Shrivastava, P. Kumar, B. B. Gupta, S. Bala, and N. Dey, Eds., Handbook of research on network forensics and analysis techniques, IGI Global, 2018.

[9] H. T. T. Binh, P. D. Thanh and T. B. Trung, "Effective multifactorial evolutionary algorithm for solving the cluster shortest path tree problem," in 2018 IEEE Congress on Evolutionary Computation (CEC), 2018, pp. 1-8.

[10] J. Gill, I. Okere, H. HaddadPajouh, and A. Dehghantanha, "Mobile forensics: A bibliometric analysis," Cyber Threat Intelligence, pp. 297-310, 2018.

[11] J. Kävrestad, Fundamentals of Digital Forensics. Springer International Publishing, 2020.

[12] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Digital forensics vs. Anti-digital forensics: Techniques, limitations and recommendations," arXiv preprint arXiv:2103.17028, 2021.

[13] J. Park and Y. I. Eom, "Anti-aging lfs: Self-defragmentation with fragmentation-aware cleaning," IEEE Access, vol. 8, pp. 151474-151486, 2020.

[14] J. Park and Y. I. Eom, "Fragpicker: A new defragmentation tool for modern storage devices," in Proceedings of the ACM SIGOPS 28th Symposium on Operating Systems Principles, 2021, pp. 280-294.

[15] J. R. Ragini, P. R. Anand, and V. Bhaskar, "Big data analytics for disaster response and recovery through sentiment analysis," International Journal of Information Management, vol. 42, pp. 13-24, 2018.

[16] Jarrett and K. K. R. Choo, "The impact of automation and artificial intelligence on digital forensics," Wiley Interdisciplinary Reviews: Forensic Science, vol. 3, no. 6, e1418, 2021.

[17] Jebb, A. T., Ng, V., & Tay, L. (2021). A review of key Likert scale development advances: 1995–2019. Frontiers in psychology, 12, 637547.

[18] K. Sharma, M. A. Joseph, B. Jacob, and B. Miranda, "Emerging trends in digital forensic and cyber security-an overview," in 2019 Sixth HCT Information Technology Trends (ITT), pp. 309-313, 2019.

[19] K. Yarlagadda, D. Güera, D. M. Montserrat, F. M. Zhu, E. J. Delp, P. Bestagini, and S. Tubaro, "Shadow removal detection and localization for forensics analysis," in ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 2677-2681, 2019.

[20] Kang, H. Pan, S. C. Hoi, and Z. Xu, "Robust graph learning from noisy data," IEEE transactions on cybernetics, vol. 50, no. 5, pp. 1833-1843, 2019.

[21] Kuznetsov, K. Shekhanin, O. Smirnov, and I. Chepurko, "Detecting Hidden Information in FAT," ISCI'2019: INFORMATION SECURITY IN CRITICAL INFRASTRUCTURES, p. 412, 2019.

[22] Lin, X. Lin, and Lagerstrom-Fife, Introductory Computer Forensics. Springer International Publishing, 2018.

[23] M. Akbanov, V. G. Vassilakis and M. D. Logothetis, "WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms," Journal of Telecommunications and Information Technology, no. 1, pp. 113-124, 2019.

[24] M. I. Alghamdi, "Digital forensics in cyber security—recent trends, threats, and opportunities," Cybersecurity Threats with New Perspectives, 2021.

[25] M. Khanafseh, M. Qatawneh, and W. Almobaideen, "A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics," International Journal of Advanced Computer Science and Applications, vol. 10, no. 8, 2019.

[26] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191-1221, 2020.

[27] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191-1221, 2020.

[28] MacDermott, T. Baker, and Q. Shi, "Iot forensics: Challenges for the ioa era," in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018,pp. 1-5.

[29] Majed, H. N. Noura, and A. Chehab, "Overview of Digital Forensics and Anti-Forensics Techniques," in 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-5.

[30] Maulik, K. Fukami, N. Ramachandra, K. Fukagata, and K. Taira, "Probabilistic neural networks for fluid flow surrogate modeling and data recovery," Physical Review Fluids, vol. 5, no. 10, 104401, 2020.

[31] P. A. E. Pratama, "Computer Forensic Using Photorec for Secure Data Recovery Between Storage Media: a Proof of Concept," International Journal of Science, Technology & Management, vol. 2, no. 4, pp. 1189-1196, 2021.

[32] Pagani, O. Fedorov, and D. Balzarotti, "Introducing the temporal dimension to memory forensics," ACM Transactions on Privacy and Security (TOPS), vol. 22, no. 2, pp. 1-21, 2019.

[33] Pasquier, X. Han, T. Moyer, A. Bates, O. Hermant, D. Eyers, ... and M. Seltzer, "Runtime analysis of whole-system provenance," in Proceedings of the 2018 ACM SIGSAC conference on computer and communications security, 2018, pp. 1601-1616.

[34] Paul Joseph and J. Norman, "An analysis of digital forensics in cyber security," in First International Conference on Artificial Intelligence and Cognitive Computing: AICC 2018, Springer Singapore, 2019, pp. 701-708.

[35] Peng, L. P. Yin, L. B. Zhang, and M. Long, "CGR-GAN: CG facial image regeneration for antiforensics based on generative adversarial network," IEEE Transactions on Multimedia, vol. 22, no. 10, pp. 2511-2525, 2019.

[36] Prakash, A. Williams, L. Garg, C. Savaglio, and S. Bawa, "Cloud and edge computing-based computer forensics: Challenges and open problems," Electronics, vol. 10, no. 11, p. 1229, 2021.

[37] Quick and K. K. R. Choo, "IoT device forensics and data reduction," IEEE Access, vol. 6, pp. 47566-47574, 2018.

[38] R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," IEEE Access, vol. 10, pp. 11065-11089, 2022.

[39] S. Bozkir, E. Tahillioglu, M. Aydos, and I. Kara, "Catch them alive: A malware detection approach through memory forensics, manifold learning and computer vision," Computers & Security, vol. 103, p. 102166, 2021.

[40] S. Cho, "An Arbitrary Disk Cluster Manipulating Method for Allocating Disk Fragmentation of Filesystem," Journal of Korea Society of Digital Industry and Information Management, vol. 16, no. 2, pp. 11-25, 2020.

[41] S. Cho, "Experimental Method of Disk Defragmentation for Robustness Test of Data Hiding Method in Slack Space of File System," in Proceedings of the Korean Society of Computer Information Conference, 2020, pp. 65-66.

[42] Setayeshfar, C. Adkins, M. Jones, K. H. Lee, and P. Doshi, "Graalf: Supporting graphical analysis of audit logs for forensics," Software Impacts, vol. 8, p. 100068, 2021.

[43] Shan, A. N. Bhagoji, H. Zheng, and B. Y. Zhao, "Poison forensics: Traceback of data poisoning attacks in neural networks," in 31st USENIX Security Symposium (USENIX Security 22), pp. 3575-3592, 2022.

[44] Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," Computers & Electrical Engineering, vol. 71, pp. 28-42, 2018.

[45] Suprem, J. Arulraj, C. Pu, and J. Ferreira, "Odin: Automated drift detection and recovery in video analytics," arXiv preprint arXiv:2009.05440, 2020.

[46] Tan, B. Wang, J. Wen, Z. Yan, H. Jiang, and W. Srisa-an, "Improving restore performance in deduplication-based backup systems via a fine-grained defragmentation approach," IEEE Transactions on Parallel and Distributed Systems, vol. 29, no. 10, pp. 2254-2267, 2018.

[47] Yaqoob, I. A. T. Hashem, A. Ahmed, S. A. Kazmi, and C. S. Hong, "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges," Future Generation Computer Systems, vol. 92, pp. 265-275, 2019.