APTISI Transactions on Technopreneurship (ATT)
Vol. 6, No. 2, July 2024, pp. 169−181
E-ISSN: 2656-8888 | P-ISSN: 2655-8807, DOI:10.34306

Comparative Analysis of NIJ and NIST Methods for MicroSD Investigations: A Technopreneur Approach

Nizirwan Anwar[1*], Agung Mulyo Widodo[2], Binastya Anggara Sekti[3], Muhamad Bahrul Ulum[4], Mosiur Rahaman[5], Hani Dewi Ariessanti [6]
[1]Dept. of Informatics Engineering, Esa Unggul University, Indonesia
[2,4,6]Dept. of Computer Science, Esa Unggul University, Indonesia
[3]Dept. of Information System, Esa Unggul University, Indonesia
[5]Dept. of International Center for AI and Cyber Security Research and Innovations (ICCRI), Asia University, Taiwan
[1]nizirwan.anwar@esaunggul.ac.id, [2]agung.mulyo@esaunggul.ac.id, [3]anggara@esaunggul.ac.id, [4]m.bahrul_ulum@esaunggul.ac.id
[5]mosiurrahaman@asia.edu.tw, [6]hani.dewi@esaunggul.ac.id
***Corresponding Author**

Article Info

Article history:

Submission May 07, 2024
Revised June 24, 2024
Accepted July 01, 2024
Published July 11, 2024

Keywords:

Digital Forensics
National Institute of Justice (NIJ)
National Institute of Standards and Technology (NIST)
MicroSD
Technopreneurship

ABSTRACT

This research aims to compare the performance of two forensic investigation methods, the National Institute of Justice (NIJ) and the National Institute of Standards and Technology (NIST), specifically for evidence analysis of MicroSD cards. **MicroSD cards are frequently** used as external storage in various digital devices, making them critical in digital forensic investigations. The study evaluates the effectiveness of these methods using tools such as Access Data FTK Imager and autopsy. **The NIJ method** enthis comparative passes detailed stages of preparation, collection, examination, analysis, and reporting, while the NIST method includes stages of collection, examination, analysis, and reporting. Results indicate that the NIJ method provides more comprehensive and detailed results, while the NIST method offers a faster investigation process. Additionally, tables and graphs illustrating performance metrics are included to substantiate the findings. **This comparative** analysis provides valuable insights for technopreneurs in optimizing digital forensic methods for better data integrity and efficiency, ultimately enhancing decision-making processes in technological entrepreneurship. Furthermore, this study aligns with the United Nations' Sustainable Development Goals (SDGs), particularly Goal 9: Industry, Innovation, and Infrastructure, by promoting innovative forensic methods that support the development of resilient infrastructure and foster innovation in the digital age. This study highlights the importance of effective forensic methods in supporting technopreneurial ventures.

Corresponding Author:

Nizirwan Anwar (nizirwan.anwar@esaunggul.ac.id)
DOI: https://doi.org/10.34306/att.v6i2.407

1. INTRODUCTION

Digital developments in the modern era are occurring very rapidly in society, facilitated by the widespread use of digital devices. These developments have significantly impacted various fields, including forensics,

where digital forensics has become a critical method for investigating electronic or digital evidence. Digital forensics aims to analyze the authenticity and relevance of evidence obtained to support criminal cases in court. Evidence can consist of both electronic and digital forms, such as computers, laptops, smartphones, hard drives, flash disks, and MicroSD cards. Handling digital evidence is crucial to maintaining its integrity, as it is vulnerable to changes that can affect its authenticity. This study focuses on MicroSD cards, commonly used as external storage in various devices, making them essential in digital forensic investigations [1], [2].

MicroSD cards can be key pieces of electronic evidence due to their data storage capabilities. Digital forensic investigation techniques vary across different branches, such as computer forensics, disk forensics, network forensics, cloud forensics, and mobile forensics [3]. The investigation process can employ various methods, including those established by the National Institute of Standards and Technology (NIST) and the National Institute of Justice (NIJ) [4]. This research aims to compare the NIJ and NIST methods to determine their effectiveness in investigating MicroSD cards. The comparison will provide valuable insights into optimizing forensic methods for technopreneurs, enhancing data integrity, and improving the efficiency of digital investigations [5].

This study highlights the importance of robust forensic methods in supporting technopreneurial ventures. Effective forensic techniques can significantly contribute to the success of technopreneurship by ensuring reliable digital evidence management, which is crucial for informed decision-making in technological entrepreneurship [6]. Furthermore, this research aligns with the United Nations' Sustainable Development Goals (SDGs), particularly Goal 9: Industry, Innovation, and Infrastructure, by promoting innovative forensic methods that support the development of resilient infrastructure and foster innovation in the digital age [7].

This study will evaluate the NIJ and NIST methods using forensic tools such as Access Data FTK Imager and autopsy. The NIJ method involves detailed stages of preparation, collection, examination, analysis, and reporting, while the NIST method includes stages of collection, examination, analysis, and reporting [8]. By comparing these methods, this research aims to provide technopreneurs with the knowledge needed to optimize digital forensic investigations, thereby supporting the broader goals of innovation and sustainable development in the field of technopreneurship [9].

2. LITERATURE REVIEW

2.1. Media Storage

Computer storage media is composed of two types of storage media, namely volatile memory and Non Volatile [10]. Volatile Memory Later data will be lost when there is no electrical power or the electricity supply is interrupted, for example on Random Access Memory (RAM), Dynamic Random access Memory (DRAM), also Static Random access Memory (SRAM) Non Volatile Memory make stored data will remain saved when there is a power failure or disconnected, for example in the form of Hard Drive, Hard Disk, Nand Flash Solid State Drive (SSD), USB flash disk and MicroSD [11].

2.2. Digital Forensics

Digital Forensics is a science of computer technology with a forensic work stage to describe the steps forensics that will be carried out and can find out the research path in a structured manner, so that it can be used as a reference in finish problem in finding evidence electronics of action crime Which already occurred by using advanced technology to prove crimes using electronic evidence Which investigated in order to fight crime [12].

2.3. Disc Forensics

Disc Forensics is a part of forensics focused on analyzing device drives. Memory forensics focuses on analysis of data contained in the memory of the system being studied [13]. Digital forensic type this is relevant by extracting data contained in the storage media through checking active , modified, or deleted. Disc Forensics including SD Card USB Stick, UFS uses CF Card and eMMC NAND flash memory [14]. Disc Forensics is identification a number of source proof digital like hard disk with interface like SATA/SCSI, Compact Disc, Disc Videos Digital, Floppy disk, cell phone, flash drives, PDAs, Card driver's license, storage USB, Tape Magnetic, Zip media drives etc. After confiscating the evidence digital in crime scene [15].

2.4. Proof Digital

Digital evidence is information sent or stored in binary form from the results of investigations carried out stages to protect evidence and minimize damage during the investigation so that the evidence remains

original. Proof required For finish case, Whereas proof electronic very sensitive will change If No handled with Correct so that can influence its authenticity [16]. All type change on proof electronic causes evidence to be useless because it will lead to wrong conclusions. Electronic evidence attached to three main principles in the collection process, namely: the principle of referring to Indonesian National Standards (SNI), namely ISO/IEC 27037:2014 and is also regulated in Law No.11 of 2008 regarding Electronics Information And Transaction [17], [18]. Investigation Which will done that is manifold disk forensics with goods proof electronic form MicroSD as a test parameter investigative methods [19].

2.5. Method Investigation

Study Which related with method investigation digital forensics Already Lots explained on study previously and there are many choices of methods that can be applied to digital forensics [20]. Research on methods digital forensics. Which has studied can produce method new based on study previously or can done comparison method with compatibility method investigation digital forensics, procedure investigation digital forensic evidence, collection and analysis methods, cybercrime behavior analysis and case verification, evidence analysis as well as the judicial juridical procedures [21]. Implement forensic techniques along with forensic analysis according to appropriate methods appropriately, it will have a success rate of almost 100% for carrying out forensic data collection [22], [23]. Related with the digital forensic investigation method chosen then the process of controlling evidence and legality, legal aspects at each stage of the methods that have been applied by investigators involved in handling electronic evidence is the main key in the success of digital forensic investigations and electronic evidence investigations must meet standards proof And acceptance of the claim for prosecution Which success [24], [25].

2.5.1. National Institute Justice (NIJ)

Figure 1. Stage investigation National of Justice (NIJ)

Figure 1 show beginnings of The National Institute of Law Enforcement and Criminal Justice founded on October 21, 1968, as a component of Law Enforcement Assistance Administration (LEAA) and in 1978 changes were made the name became the National Institute of Justice (NIJ) to date. National Institute Method of Justice (NIJ) has five stage in process forensics start from identification, collection, examination, analysis, Also reporting. According to study previously mentioned collection data with very accurate success rate by carrying out forensic techniques along with forensic analysis according to the method which appropriate [26], [27].

2.5.2. National Institute of Standard and Technology (NIST)

Figure 2. Stage investigation National Institute of Standard and Technology (NIST)

The Figure 2 National Institutes of Standards and Technology (NIST) was founded in 1901 and is now part of US department of commerce. NIST is one of the oldest physical science laboratories in the country. Congress did The formation of this agency was to eliminate a major challenge to US industrial competitiveness at that time, class measurement infrastructure Britain's two laggards in capability, Germany, as well as other economic rivals. Smart power grid and records health electronic until O'clock atom, nanomaterials advanced,

And chips computer, product And service Which not counted much depends on the technology, measurements, and standards provided by NIST. The NIST method is used to carry out an investigation process on digital evidence or a process to obtain information from digital evidence [28]. NIST have four process stage investigation namely Collection, examination, analysis and reports.

2.6. Sustainable Development Goals (SDGs)

Digital forensics is a science of computer technology that involves the systematic investigation of electronic or digital evidence to determine its authenticity and relevance in legal contexts [29]. The field encompasses various branches, including computer forensics, disk forensics, network forensics, cloud forensics, and mobile forensics. Each branch employs different techniques and methodologies to handle and analyze digital evidence effectively. The National Institute of Standards and Technology (NIST) and the National Institute of Justice (NIJ) are two prominent institutions that have developed comprehensive methods for digital forensic investigations. These methods aim to ensure the integrity and accuracy of the evidence collected, which is critical for its admissibility in court [30], [31].

Figure 3. Sustainable Development Goals

In Figure 3 with the United Nations' Sustainable Development Goals (SDGs), particularly Goal 9: Industry, Innovation, and Infrastructure, the advancement of digital forensic methods plays a vital role in promoting sustainable industrialization and fostering innovation. By improving the techniques used in digital investigations, we can ensure more reliable and efficient handling of electronic evidence. This not only supports the justice system but also encourages the development of robust digital infrastructures that are essential for modern technopreneurial ventures. As digital technologies continue to evolve, the need for innovative forensic methods becomes increasingly important to maintain the integrity of digital ecosystems and support sustainable development in the digital age. This research aims to contribute to these goals by providing a comparative analysis of the NIJ and NIST methods, thereby offering insights that can enhance the capabilities of technopreneurs in managing digital evidence [32], [33].

3. METHODS

This Figure 4 containing about stages study studies analysis comparison method National Institute of Justice (NIJ) as well as National Institute of Standard and Technology (NIST) for investigation on MicroSD.

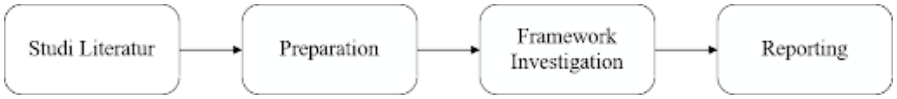

Figure 4. Stage Study

Figure 4 illustrates the stages involved in the comparative study of the National Institute of Justice (NIJ) and the National Institute of Standards and Technology (NIST) methods for investigating MicroSD cards. The process begins with a comprehensive literature review to establish the foundation of existing knowledge and identify gaps. This is followed by the preparation phase, which includes the setup of both hardware and software tools necessary for the investigation. The core of the study involves the framework investigation,

where the methodologies of NIJ and NIST are systematically applied and compared. Finally, the findings are compiled and analyzed in the reporting stage, providing insights into the effectiveness and efficiency of each method. This structured approach ensures a thorough and balanced evaluation of the forensic techniques under consideration.

3.1. Bibliometric Analysis

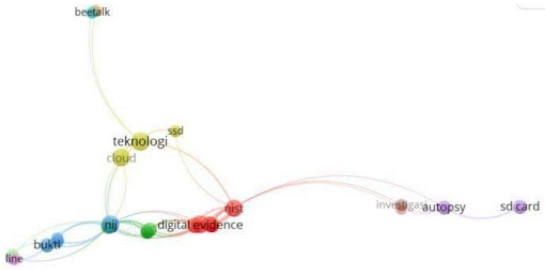

Figure 5. Mapping research

The Figure 5 show about research involves a comprehensive bibliometric analysis of previous studies using tools such as Publish or Perish and VOSviewer [34]. The Publish or Perish tool was used to gather relevant literature, and VOSviewer was employed to map the bibliometric network, which includes journals, researchers, individual publications, and co-authorship relationships. This bibliometric network was visualized to identify similar research related to the use of NIJ and NIST methods in investigating digital evidence, specifically focusing on MicroSD cards. By examining these relationships and citations, the study aims to build on existing knowledge and identify gaps that this research can address, thereby contributing to the broader field of digital forensics and its application in technopreneurship [35].

3.2. Preparation Systems

Preparation system or system preparation in this research is an outline of the system used in investigation. Preparation system shared become two parts, namely:

3.2.1. Preparation Hardware

The hardware requirements for this research include a computer prepared to carry out comparisons between the NIJ and NIST methods for investigating MicroSD cards. The specific device used for this investigation is equipped with an Intel(R) Core(TM) i3-10110U CPU @ 2.10GHz 2.59 GHz processor and 4.00GB of RAM [36]. Additionally, a card reader with a data read speed of 37.4MB/s and a write speed of approximately 17.6MB/s is utilized [37].

3.2.2. Preparation Software

The software preparation for this study includes setting up the operating system and the tools that will be used for the investigation process [38]. The operating system used is Windows 11 Home Single Language version 22H2. The forensic tools utilized in this research are Access Data FTK Imager version 3.1.2.0 and autopsy version 4.20 [39].

3.3. Frameworks Investigation

After preparations are complete, the next stage is to carry out the investigation process. Investigation process there is two stages investigation Which covers that is:

3.3.1. Investigation National Method Institute of Justice (NIJ)

This method outlines the stages of the forensic process, which include preparation, collection, examination, analysis, and reporting [40]. These stages explain how the research was conducted, ensuring that the research flow is systematic and can serve as a guideline for solving the problem at hand [41], [42].

3.3.2. Investigation Method National Institute of Standards and Technology (NIST)

Steps on cloud computing forensics according to NIST among them identification, collection, preservation, examination, interpretation and reporting results from investigations regarding digital evidence. Among the methods which can be used in forensic analysis and identification of digital evidence, this research uses methods mobile forensics which based on availability guidelines and developed by NIST.

4. RESULTS AND DISCUSSION

Scenario case which implemented in study this for simulate case follow crime Which carried out to obtain digital evidence that has been deleted. There has been a crime in the form of embezzlement of money in something company X by perpetrator follow crime initials Q, then injured process search goods proof Then found in place initial crime case T with goods proof form MicroSD and done process investigation.

4.1. Frameworks Investigation

This section will present the research results based on the framework stage investigation by using the method National Institutes of Justice (NIJ) and the National Institute of Standards and Technology (NIST), then carried out a comparison framework investigation And final stage reporting.

4.1.1. National Institute of Justice (NIJ)

Identification in Figure 6 is carried out by selecting electronic evidence in the form of a MicroSD cards with some of the memory data already deleted by the perpetrator, and data selection was carried out in the form of documents in the form of PDF, Docs and CSV during imaging proof digital. Furthermore with preparation tools forensics that is Access Data FTK Imager and autopsy.

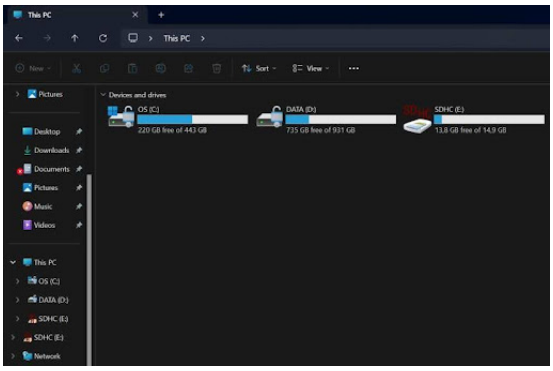

Figure 6. Goods Proof Form MicroSD

Collection MicroSD data collection Investigation in Figure 7 was carried out using Access Data FTK Imager for imaging was carried out first with the source type in the form of physical in E01 format for original digital evidence no damaged.

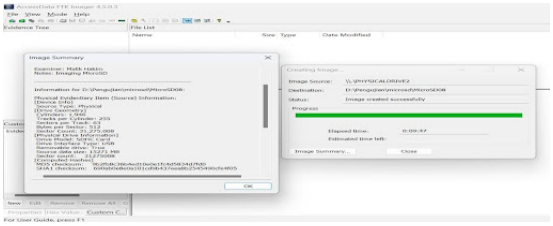

Figure 7. Imaging MicroSD use FTK Imager

Examination in Figure 8 of data from imaging results Access Data FTK Imager examined using forensic tools autopsy. autopsy do ingest modules or analyzing data from data sources imaging results FTK Access data Imager with E01 data format so you will get a number of files on the MicroSD well that's it whether it has been deleted or not yet deleted, then the process of searching for digital evidence in the form of files is

carried out. docx, pdf and csv. Because files the connection with recording Money And there is a possibility connection with the scenario case.

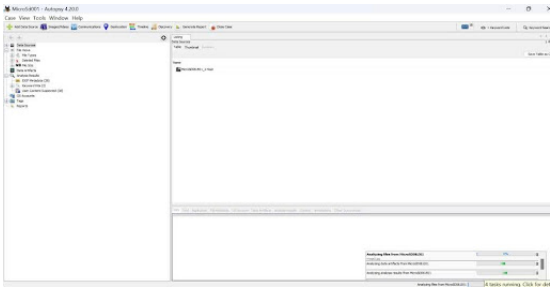

Figure 8. Do inspection data source use autopsy

Analysis The results of digital data in Figure 9 searches through the MicroSD evidence investigation process with forensic tools Access Data FTK Imager and autopsy has discovered digital data that may be related to the scenario case, then an analysis process is carried out on the data that has been obtained to be used as evidence digital.

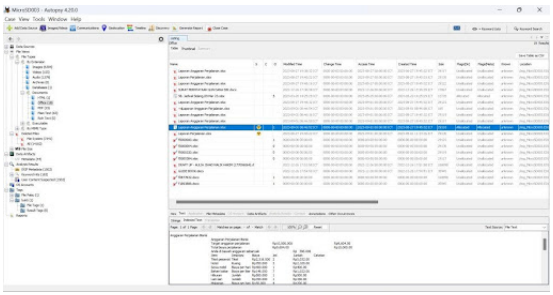

Figure 9. Process Analysis Proof Digital

Reporting Results in Figure 10 is investigation method NIJ has find proof digital through help tool forensics Access Data FTK Imager and autopsy. After carrying out a series of stages of the investigation process, it was discovered Digital evidence is then analyzed, after which a report is created to convey the results of the process investigation Which has done.

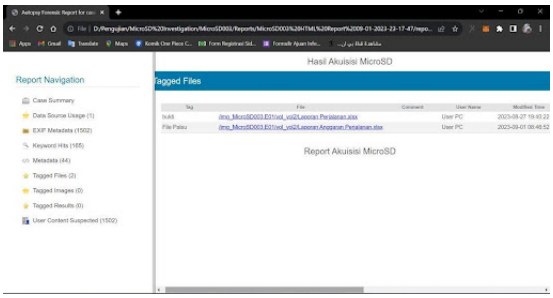

Figure 10. Stage Reporting Results Investigation

Figur 10 shows the results of the investigation report using the NIJ method. Table 1 below summarizes the stages and results of the digital investigation process using the NIJ method.

Table 1. Stage I Investigation National Institute of Justice

No	Stages	Results
1	Identification	Goods proof form flash memory MicroSD and election data digital which will more takes priority in process appointment the data.
2	Collection	Imaging use FTK Imager
3	Examination	Process data results imaging with autopsy
4	Analysis	Look for files which possibility relate with case use autopsy
5	Reporting	Tagging files, generate reports with use autopsy

The table 1 outlines the stages and results of the digital investigation process using the NIJ method. In the identification stage, the focus is on selecting the evidence in the form of a flash memory MicroSD and prioritizing the digital data that needs to be extracted. During the collection stage, the evidence is imaged using FTK Imager, creating a digital copy of the MicroSD to preserve the original data's integrity. The examination stage involves processing the imaged data with autopsy, a forensic tool, to scrutinize the contents of the MicroSD. In the analysis stage, investigators search for files that may be relevant to the case using autopsy. Finally, the reporting stage includes tagging the identified files and generating comprehensive reports using autopsy to document the findings of the investigation.

4.2. National Institute of Standard and Technology (NIST)

Collection This stage carries out data in Figure 11 is retrieval through the use of the Access Data FTK forensic tool Imager to do imaging The evidence that has been obtained is in the form of a MicroSD Card so that integrity data from proof digital which is on MicroSD Card stay awake.

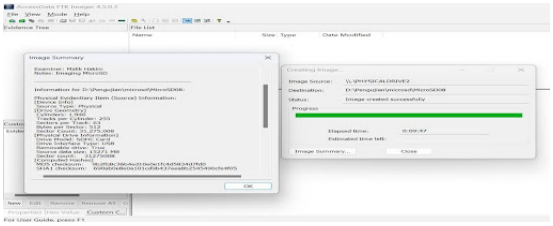

Figure 11. Stage Reporting Results Investigation

Examination from Figure 12 The examination stage is carried out using data from imaging results MicroSD with forensic tools Access Data FTK Imager so that in the process of checking the original data, the integrity of the data is maintained. Data contained in the MicroSD thoroughly checked to obtain the necessary digital evidence with using autopsy forensic tools. autopsy used for checking existing, modified files nor that already deleted on MicroSD to make as evidence digital

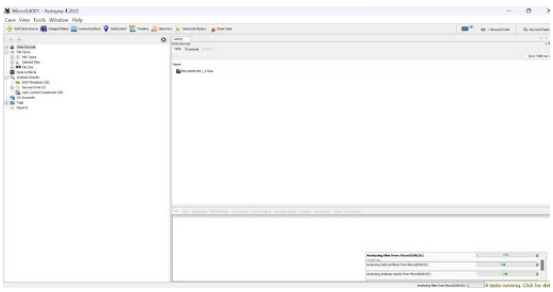

Figure 12. Inspection overall data results imaging use autopsy

Analysis Results from Figure 13 examinations using tools forensic autopsy continued with analysis The digital data found may be related to the case scenario being investigated get a proof digital.

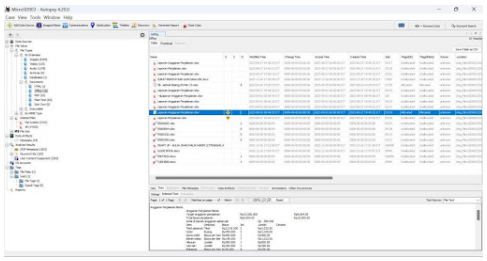

Figure 13. process analysis data MicroSD

Reporting Investigation results from Figure 14 through the use of the NIST method using tools Access Data FTK forensics Imager to use imaging proof digital MicroSD and next with inspection use autopsy. The investigation was carried out in accordance with the stages of the process of searching for digital evidence by carrying out stages collection that is identify digital evidence without making data changes and maintain authenticity data.

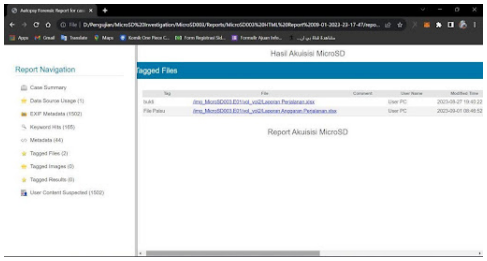

Figure 14. NIST Investigation Report

The report generated as shown in Figure 14 demonstrates the results of the investigation conducted using the NIST method. The process involved utilizing Access Data FTK Forensics Imager to image the digital evidence stored on the MicroSD card, followed by a detailed inspection using the Autopsy tool. Each stage of the investigation adhered to the NIST guidelines, ensuring that digital evidence was collected in a manner that preserved its integrity and authenticity. This approach minimizes data alterations and ensures that the findings remain reliable and valid for forensic analysis.

Table 2. Stages I Investigation National Institute of Standart and Technology (NIST)

No	Stages	Results
1	Collection	Imaging use FTK Imager
2	Examination	Process data results imaging with autopsy
3	Analysis	Look for files which possibility relate with case use autopsy
4	Reporting	Tagging files, generate reports with use autopsy

After that with stage examination that is manage and look for on data source which already done imaging moreover first, then do the steps analysis namely analyzing data from the results of data source management which has It is possible that the files obtained are related to the case scenario and reporting stage namely reporting all results investigation which already done in Table 2.

4.3. Comparison Frameworks Investigation

From Table 3 Stages This done comparison method investigation NIJ And NIST use hardware and software Which has explained. Comparison two that method for look for evidence on goods proof micro SD.

Table 3 presents a comparative analysis of the NIJ and NIST methods used for investigating MicroSD cards. The comparison is structured across five key stages: Identification, Collection, Examination, Analysis, and Reporting. Both methods employ similar tools and procedures, such as using FTK Imager for imaging and Autopsy for examination and analysis. However, the NIJ method includes an additional identification stage

Table 3. Comparison Ramework Invesrigation

No	Method			
	National Institute of Justice (NIJ)		*National Institute of Standard and Technology (NIST)*	
	Stages	**Results**	**Stages**	**Results**
1	Identification	Goods proof form flash memory MicroSD and election data with format, docx, pdf and csv.	Identification	-
2	Collection	Imaging use FTK Imager	Collection	Imaging use FTK Imager
3	Examination	Process data results imaging with autopsy	Examination	Process data results imaging with autopsy
4	Analysis	Look for files which possibility related to the case use autopsy	Analysis	Look for files which possibility related to the case use autopsy
5	Reporting	Tagging files, generate reports with use autopsy	Reporting	Tagging files, generate reports with use autopsy

where the type and format of data are specified, whereas the NIST method begins directly with the collection stage. Both methods ultimately aim to identify, collect, and analyze digital evidence efficiently, ensuring data integrity and reliability throughout the investigation process.

4.4. Reporting

Based on the case scenario, an investigation is carried out using National Institute method of Justice (NIJ) and National Institutes of Standards and Technology (NIST) has obtained results as in table 3. Each method has its own advantages, if you want to get more detailed results then it is recommended to do it the investigation uses the NIJ method because it has more complete stages and if you want to save time It is recommended that investigations use the NIST method because it has fewer investigation stages than the method NIJ thus speeding up time investigation process.

5. MANAGERIAL IMPLICATIONS

The findings of this study offer valuable insights for managers and technopreneurs in the field of digital forensics. The comparative analysis of the NIJ and NIST methods highlights that the NIJ method is advantageous for comprehensive and detailed investigations, ensuring thorough examination and accurate reporting of digital evidence. Conversely, the NIST method provides a more streamlined approach that saves time and resources, beneficial for fast-paced environments.

Managers should leverage these insights to choose the appropriate method based on their specific needs, ensuring optimal efficiency and accuracy in forensic investigations. Additionally, investing in advanced forensic tools and training can enhance the capabilities of their teams, maintaining a competitive edge in the evolving digital landscape. Aligning these practices with the Sustainable Development Goals (SDGs), particularly goal 9: Industry, Innovation, and Infrastructure, supports sustainable technological advancement and robust infrastructure development.

6. CONCLUSION

The comparative analysis of the NIJ and NIST methods for MicroSD card investigations reveals distinct advantages and drawbacks for each approach. The NIJ method with its comprehensive stages of preparation, collection, examination, analysis, and reporting, demonstrates superior thoroughness and detail making it ideal for situations where the accuracy and completeness of digital evidence are critical. On the other hand, the NIST method's streamlined process focuses on efficiency and speed, offering a practical solution for scenarios where time is a significant constraint. These insights are particularly valuable for technopreneurs who need to balance meticulous forensic investigations with operational efficiency, enhancing their capability to manage digital evidence effectively.

Furthermore, this research underscores the importance of adopting advanced forensic tools like Access Data FTK Imager and autopsy to ensure robust and reliable digital investigations. By integrating these tools into their investigative practices, technopreneurs can significantly improve data integrity and support sustainable business operations. This study also aligns with the United Nations' Sustainable Development Goals (SDGs), particularly Goal 9, by promoting innovative forensic methods that contribute to the development of resilient infrastructures and foster technological innovation. Overall, the findings of this study provide a strategic framework for technopreneurs to optimize their forensic methodologies, thereby supporting informed decision making and sustainable technological entrepreneurship.

7. DECLARATIONS

7.1. Disclosure Statement

No potential conflict of interest was reported by the author(s).

7.2. ORCID

Nizirwan Anwar https://orcid.org/0000-0003-1189-9093
Agung Mulyo Widodo https://orcid.org/0000-0002-9792-7114
Binastya Anggara Sekti https://orcid.org/0000-0001-5489-4888
Muhamad Bahrul Ulum https://orcid.org/0000-0001-9595-1332
Mosiur Rahaman https://orcid.org/0009-0002-4306-0356
Hani Dewi Ariessanti https://orcid.org/0000-0002-0565-9248

7.3. Author Contributions

Conceptualization: N.A.; Methodology: A.M.W.; Software: B.A.S.; Validation: M.B.U. and M.R.; Formal Analysis: H.D.A. and N.A.; Investigation: A.M.W.; Resources: B.A.S.; Data Curation: M.B.U.; Writing Original Draft Preparation: M.R. and H.D.A.; Writing Review and Editing: N.A. and A.M.W.; Visualization: B.A.S.; All authors, N.A., A.M.W., B.A.S., M.B.U., and M.R., H.D.A have read and agreed to the published version of the manuscript.

7.4. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.5. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.6. Institutional Review Board Statement

Not applicable.

7.7. Informed Consent Statement

Not applicable.

7.8. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] S. Sunardi, I. Riadi, R. Umar, and M. F. Gustafi, "Audio forensics on smartphone with digital forensics research workshop (dfrws) method," *CommIT (Communication and Information Technology) Journal*, vol. 15, no. 1, pp. 41–47, 2021.

[2] A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari, and A. E. Rajput, "Mf-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture," *IEEE Access*, vol. 9, pp. 103 637–103 650, 2021.

[3] D. S. S. Wuisan, R. A. Sunardjo, Q. Aini, N. A. Yusuf, and U. Rahardja, "Integrating artificial intelligence in human resource management: A smartpls approach for entrepreneurial success," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 334–345, 2023.

[4] M. Naz, F. A. Al-zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shafiq, "A secure data sharing platform using blockchain and interplanetary file system," *Sustainability*, vol. 11, no. 24, p. 7054, 2019.

[5] B. Rawat, A. S. Bist, B. S. Riza, A. Oktariyani, and U. Rahardja, "Analysis of examination process during covid and post covid in indian context," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2021, pp. 1–5.

[6] F. Bahtiar, N. Widiyasono, and A. P. Aldya, "Forensic volatile memory for malware detection using machine learning algorithm," *Jurnal Rekayasa Sistem & Industri (JRSI)*, vol. 6, no. 01, pp. 52–57, 2019.

[7] A. Ruangkanjanases, A. Khan, O. Sivarak, U. Rahardja, and S.-C. Chen, "Modeling the consumers' flow experience in e-commerce: The integration of ecm and tam with the antecedents of flow experience," *SAGE Open*, vol. 14, no. 2, p. 21582440241258595, 2024.

[8] M. Dalal and M. Juneja, "Steganography and steganalysis (in digital forensics): a cybersecurity guide," *Multimedia Tools and Applications*, vol. 80, no. 4, pp. 5723–5771, 2021.

[9] P. A. Sunarya, U. Rahardja, S. C. Chen, Y.-M. Lic, and M. Hardini, "Deciphering digital social dynamics: A comparative study of logistic regression and random forest in predicting e-commerce customer behavior," *Journal of Applied Data Sciences*, vol. 5, no. 1, pp. 100–113, 2024.

[10] M. Tanque and P. Bradford, "Virtual raspberry pi-s with blockchain and cybersecurity applications," in *Advances in Computers*. Elsevier, 2023, vol. 131, pp. 201–232.

[11] C. Lukita, L. D. Bakti, U. Rusilowati, A. Sutarman, and U. Rahardja, "Predictive and analytics using data mining and machine learning for customer churn prediction," *Journal of Applied Data Sciences*, vol. 4, no. 4, pp. 454–465, 2023.

[12] M. S. Mazhar, Y. Saleem, A. Almogren, J. Arshad, M. H. Jaffery, A. U. Rehman, M. Shafiq, and H. Hamam, "Forensic analysis on internet of things (iot) device using machine-to-machine (m2m) framework," *Electronics*, vol. 11, no. 7, p. 1126, 2022.

[13] M. G. Christopher and K. Raychaudhuri, "A digital forensic approach for examination and analysis of frozen hard disk of virtual machine." *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 4, pp. 262–273, 2019.

[14] I. Riadi, I. A. Rafiq *et al.*, "Forensic mobile analysis on social media using national institute standard of technology method." *International Journal of Safety & Security Engineering*, vol. 12, no. 6, 2022.

[15] U. Rahardja, N. Lutfiani, A. S. Rafika, and E. P. Harahap, "Determinants of lecturer performance to enhance accreditation in higher education," in *2020 8th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2020, pp. 1–7.

[16] S. Kosasi, I. D. A. E. Yuliani, U. Rahardja *et al.*, "Boosting e-service quality of online product businesses through it leadership," in *2022 International Conference on Science and Technology (ICOSTECH)*. IEEE, 2022, pp. 1–10.

[17] N. Y. Ahn and D. H. Lee, "Forensics and anti-forensics of a nand flash memory: From a copy-back program perspective," *IEEE Access*, vol. 9, pp. 14 130–14 137, 2021.

[18] R. Shree, A. K. Shukla, R. P. Pandey, V. Shukla, and D. Bajpai, "Memory forensic: Acquisition and analysis mechanism for operating systems," *Materials Today: Proceedings*, vol. 51, pp. 254–260, 2022.

[19] L. Rosselina, Y. Suryanto, T. Hermawan, and F. Alief, "Framework design for the retrieval of instant messaging in social media as electronic evidence," in *2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI)*. IEEE, 2020, pp. 209–215.

[20] I. G. N. G. Wicaksanaa and I. K. G. Suhartanaa, "Forensic analysis of telegram desktop-based applications using the national institute of justice (nij) method," *Jurnal Elektronik Ilmu Komputer Udayana p-ISSN*, vol. 2301, p. 5373, 2020.

[21] U. Rahardja, C. T. Sigalingging, P. O. H. Putra, A. Nizar Hidayanto, and K. Phusavat, "The impact of mobile payment application design and performance attributes on consumer emotions and continuance intention," *Sage Open*, vol. 13, no. 1, p. 21582440231151919, 2023.

[22] A. N. Ichsan and I. Riadi, "Mobile forensic on android-based imo messenger services using digital forensic research workshop (dfrws) method," *Int. J. Comput. Appl*, vol. 174, no. 18, pp. 34–40, 2021.

[23] R. Tarmizi, N. Septiani, P. A. Sunarya, and Y. P. A. Sanjaya, "Harnessing digital platforms for en-

trepreneurial success: A study of technopreneurship trends and practices," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 278–290, 2023.

[24] K. D. O. Mahendraa and I. K. A. Mogia, "Digital forensic analysis of michat applications on android as digital proof in handling online prostitution cases," *Jurnal Elektronik Ilmu Komputer Udayana p-ISSN*, vol. 2301, p. 5373, 2021.

[25] U. Rusilowati, F. P. Oganda, R. Rahardja, T. Nurtino, and E. Aimee, "Innovation in smart marketing: The role of technopreneurs in driving educational improvement," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 305–318, 2023.

[26] D. Uroz and R. J. Rodríguez, "On challenges in verifying trusted executable files in memory forensics," *Forensic Science International: Digital Investigation*, vol. 32, p. 300917, 2020.

[27] B. K. Bintoro, N. Lutfiani, D. Julianingsih *et al.*, "Analysis of the effect of service quality on company reputation on purchase decisions for professional recruitment services," *APTISI Transactions on Management*, vol. 7, no. 1, pp. 35–41, 2023.

[28] A. S. Pallivalappil and S. Jagadeesha, "Procedures for digital forensics and incident response on including data integrity constraints on solid-state drives (ssd)-a literature review," *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, vol. 6, no. 1, pp. 328–350, 2022.

[29] V. Meilinda, S. A. Anjani, and M. Ridwan, "A platform based business revolution activates indonesia's digital economy," *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 2, pp. 155–174, 2023.

[30] 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.

[31] N. Ramadhona, I. Erliyani *et al.*, "Exploring the components of management information systems: Software, database, and brainware-a literature review," *International Transactions on Education Technology*, vol. 2, no. 1, pp. 65–70, 2023.

[32] A. 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. 11 065–11 089, 2022.

[33] H. A. Winata and F. Simon, "Influence of profitability, audit quality, and corporate governance on earnings management," *APTISI Transactions on Management*, vol. 8, no. 2, pp. 93–104, 2024.

[34] F. Adam and G. Ray, "The role of information and communication technology (ict) in enhancing the innovative learning process," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 2, no. 1, pp. 54–60, 2020.

[35] A. W. Malik, D. S. Bhatti, T.-J. Park, H. U. Ishtiaq, J.-C. Ryou, and K.-I. Kim, "Cloud digital forensics: Beyond tools, techniques, and challenges," *Sensors*, vol. 24, no. 2, p. 433, 2024.

[36] B. Rawat and D. Maulidditya, "Entrepreneurship in information technology as a method for improving student creativity in the digital economy," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 4, no. 1, pp. 32–37, 2022.

[37] G. Kim, S. Kim, M. Park, Y. Park, I. Lee, and J. Kim, "Forensic analysis of instant messaging apps: Decrypting wickr and private text messaging data," *Forensic Science International: Digital Investigation*, vol. 37, p. 301138, 2021.

[38] M. S. Chang and C. P. Yen, "Linkedin social media forensics on windows 10." *Int. J. Netw. Secur.*, vol. 22, no. 2, pp. 321–330, 2020.

[39] A. A. Mughal, "A comprehensive study of practical techniques and methodologies in incident-based approaches for cyber forensics," *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries*, vol. 2, no. 1, pp. 1–18, 2019.

[40] G. P. Widodo and M. Syukri, "Elements of commerce shows enterprise development innovation efficient auditing and the way of the future," *ADI Journal on Recent Innovation*, vol. 3, no. 1, pp. 97–104, 2021.

[41] A. Menahil, W. Iqbal, M. Iftikhar, W. B. Shahid, K. Mansoor, and S. Rubab, "Forensic analysis of social networking applications on an android smartphone," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, p. 5567592, 2021.

[42] N. N. Rafiana, "Technopreneurship strategy to grow entrepreneurship career options for students in higher education," *ADI Journal on Recent Innovation*, vol. 5, no. 2, pp. 110–126, 2024.