AKIRATECH : Journal of Computer and Electrical Engineering
Vol. 2, No. 1 (2025),
e-ISSN 3047-7522

Digital Forensic Analysis of Data Recovery in File Deletion Cases Using the National Institute of Standards and Technology (NIST) Method

Dwingka Audita [1], Poetri Lestari L.B [2], Farniwati Fattah[3]
[1.3]Informatics Engineering Study Program, Universitas Muslim Indonesia,
Jl. Urip Sumoharjo KM.05 , Makassar dan 90231, Indonesia

Article Info

Article history:

Received Maret 5, 2025
Revised Maret14, 2025
Accepted Maret 27, 2025

Keywords:

Digital Forensics
Data Recovery
Grade Forgery
NIST
Smartphone

ABSTRAK

Digital forensics is the application of scientific knowledge and computer technology to support legal processes, with the primary goal of uncovering and proving technology-based crimes. One crucial aspect of digital forensics is data recovery, which enables the retrieval of deleted files as evidence in digital crime investigations. Smartphones are frequently used in criminal activities, including academic grade falsification through digital transactions. This study applies the National Institute of Standards and Technology (NIST) method in digital forensic processes, consisting of the stages of Collection, Examination, Analysis, and Reporting, to recover lost or deleted image data on Android smartphones and support the investigation process. Testing was conducted using two tools, Wondershare Dr.Fone and EaseUS Mobisaver, to recover digital evidence from an Oppo A95 smartphone. The results indicate that both tools successfully retrieved 17 image files of transfer receipts, suspected to be proof of grade-buying transactions. Wondershare Dr.Fone employs a hybrid scan approach and data carving, while EaseUS Mobisaver utilizes metadata-based recovery and partition-based recovery to restore lost data. This study demonstrates that the NIST-based digital forensic method, along with the appropriate tools, can aid in recovering deleted digital evidence. The findings contribute to the advancement of digital investigation techniques, particularly in uncovering academic fraud, such as grade manipulation.

Corresponding Author:
Dwingka Audita,
Faculty of Computer Science, Jl. Urip Sumoharjo KM.05, Makassar 90231, Indonesia
Email: Dwingkaaudita4@gmail.com

1. INTRODUCTION

Digital forensics, also known as computer forensics, is the application of computer science and technology to support legal processes (pro justice). The primary focus of this field is to uncover and prove crimes involving high technology or computers by using digital evidence to prosecute offenders. Essentially, digital forensics is responsible for searching for and identifying digital evidence that can be stored in various media, such as temporary storage, permanent storage, USB drives, CDs, network traffic, and more. This field is a relatively new branch of science that was initially known as **computer forensics**. However, its scope has now expanded to include all forms of digital technology. Meanwhile, computer forensics specifically refers to the techniques and tools used to discover evidence within computer devices [1].

One of the key aspects of digital forensics is the ability to recover deleted data from devices. Even if users have deleted or attempted to erase files, such as image files, forensic experts can still recover them using specialized software or techniques that facilitate the retrieval of evidence [2].

In this era of globalization, technological advancements, especially in the field of communication, are rapidly progressing. One of the fastest-growing technologies is the smartphone, which has become an integral part of everyday life. However, this advancement brings both positive and negative impacts for its users. In the world of crime, smartphones are often exploited as highly effective tools for committing offenses, such as data theft, fraud, and various other forms of crime that use smartphones as their medium [3].

Currently, there are many cases where suspects attempt to delete evidence of their crimes to erase any traces. Data recovery is one of the primary tasks in digital forensics, enabling the retrieval of deleted files for further analysis. Even after deletion, files stored in a storage medium can still be recovered using specific forensic techniques [4].

In the academic realm, the increasing cases of grade manipulation pose a significant challenge in maintaining the integrity of the education system. Students who fear failing often seek instant ways to alter their grades, one of which is by using smartphones to access illegal services.

In line with this phenomenon, previous research on digital evidence analysis has shown that forensic methods can be used to uncover traces of digital crimes. Therefore, this study aims to evaluate the effectiveness of the NIST method in examining digital evidence on smartphones. The primary objective is to recover and analyze deleted files, particularly image files that can serve as evidence in court, using two forensic tools: Wondershare Dr.Fone and EaseUS Mobisaver.

2. METODE

The research stages consist of the steps that will be carried out in this study. The research stages are as follows:

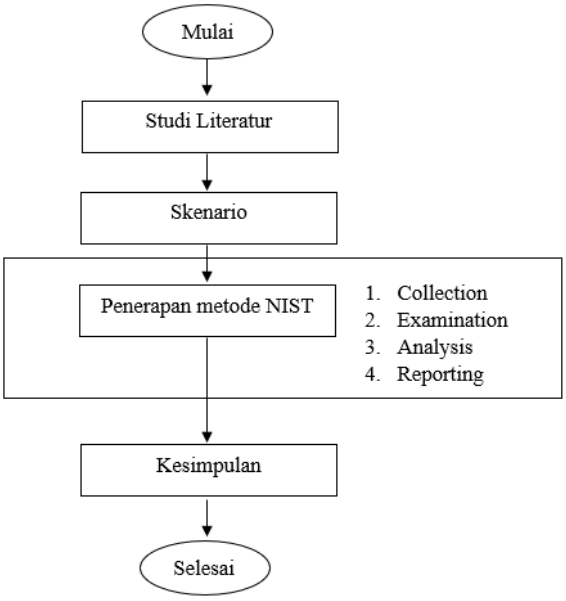

Figure 1. Research Stages

The explanation of the image above is as follows:

1. Literature Review
   In digital forensic research on file deletion using image files, the goal is to analyze cases of grade falsification. In this context, the study will examine various sources and relevant references to understand the techniques and methods used in file deletion, as well as their implications in grade falsification cases within the academic field.
2. Scenario
   In this stage, a scenario is used where several students who never attended lectures still received grades, while other students complained about receiving extremely low grades, putting them at risk of failing the course. These students sought an instant way to improve their grades and discovered an illicit grade-changing service operating secretly within the academic

environment. They then contacted a middleman who facilitated the service. Upon investigation, unauthorized changes to student grades were found without any approval from the respective lecturers. The suspected students were summoned for questioning, but they denied any wrongdoing. To gather evidence, the suspect's smartphone was confiscated to trace any records of financial transactions related to the fraud. However, no evidence was initially found. Based on this, the researchers decided to conduct a digital forensic examination on the suspect's smartphone to investigate the possibility that the evidence had been deleted.

3. Collection

   At this stage, the researchers will collect digital evidence, including the smartphone, student data or files, and other information related to the grade falsification case.

4. Examination

   The examination stage involves inspecting and extracting data from the smartphone to retrieve deleted files. The evidence analysis will be conducted using Wondershare Dr.Fone and EaseUS Mobisaver tools.

5. Analysis

   The next stage involves conducting an analysis after obtaining the necessary digital evidence from the previous investigation phase. The digital evidence will be examined in a manner that ensures its legal accountability..

6. Reporting

   This stage reports the final results of all the steps that have been carried out. The report includes the actions taken, the tools used Wondershare Dr.Fone and EaseUS Mobisaver as well as the NIST method applied in solving the grade falsification case.

7. Conclusion

   The conclusion of this study is that digital forensic analysis was conducted using digital evidence obtained from the predefined scenario by utilizing forensic tools and applying the National Institute of Standards and Technology (NIST) method.

3. RESULTS AND DISCUSSION

The objective of this study is to conduct a digital forensic examination to recover data and investigate deleted evidence from the suspect's smartphone using the NIST method. The stages carried out in this process are as follows:

a. *Collection*

At this stage, evidence collection is carried out. In this case, a smartphone belonging to the suspected grade-changing service provider was found. The device, an Oppo A95, is suspected to be the evidence used for transactions with the students involved.

Table 1. Smartphone Specifications

Spesifikasi	Detail
Nama perangkat	OPPO A95
Penyimpanan	128 GB
Model	CPH2365
Processor	Qualcomm® Snapdragon™ 662 Octa-core
Kapasitas Baterai	5000 mAh(TIP)
Ukuran layar	6,43 inci
RAM	8 GB
Versi android	Android 13
Kamera	Depan 16MP Belakang 48MP+2MP+2MP

b. *Examination*

At this stage, evidence retrieval is conducted using Wondershare Dr.Fone and EaseUS Mobisaver tools. The steps in this investigation are as follows:

1. Gallery Examination

   After seizing the evidence, a search was conducted on the files stored in the smartphone. The investigation team examined the suspect's smartphone gallery but found no evidence. It was indicated that all transaction records had been deleted by the suspect.

2. Smartphone Debugging

   The debugging process involves configuring the smartphone settings to enable access to Android storage, copy data, and track activity logs on the device. By performing debugging, investigators can access and retrieve activity logs, cache, databases, and application files containing sensitive information.

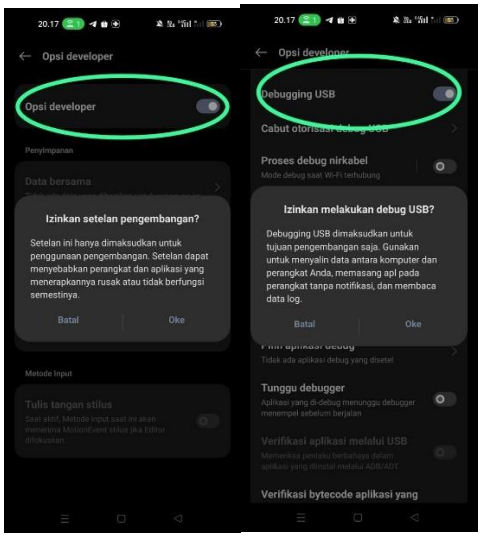

Figure 2. Performing Smartphone Debugging

3. Connecting the Tools to the Suspect's Smartphone

   To extract data from the smartphone, the device must be connected to a laptop using a data cable. Additionally, developer options on the smartphone need to be enabled (as shown in Figure 10) to establish a connection with the Wondershare Dr.Fone tool.

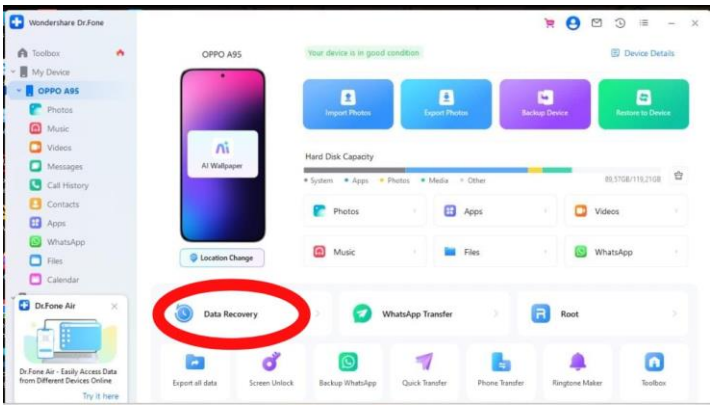

Figure 3. Smartphone Connected to Wondershare Dr.Fone

Once the smartphone is successfully connected to Wondershare Dr.Fone, the device will be automatically detected, and a scanning process will begin to search for deleted files. This process may take several minutes, depending on the storage capacity.

Next, the EaseUS Mobisaver tool is connected. Once the device is recognized, an information display will appear, as shown in the image below. After detection, users will be

directed to a screen where they can select the type of files to recover. Once the file selection is made, EaseUS Mobisaver will initiate a scanning process to locate deleted files.

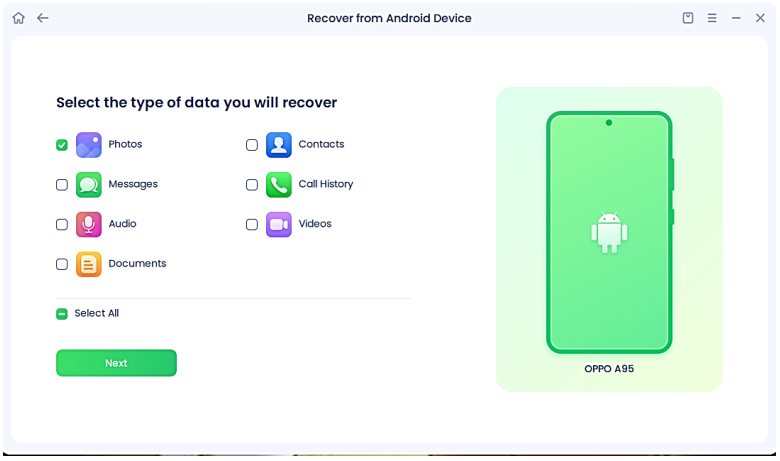

Figure 4. Smartphone Connected to EaseUS Mobisaver

c. *Analysis*

This analysis stage involves using the Wondershare Dr.Fone tool. After debugging, a file digging process is conducted. Wondershare Dr.Fone is a commonly used tool for recovering image files via a laptop. Once the digging process is completed, multiple screenshot files of transfer receipts were discovered.

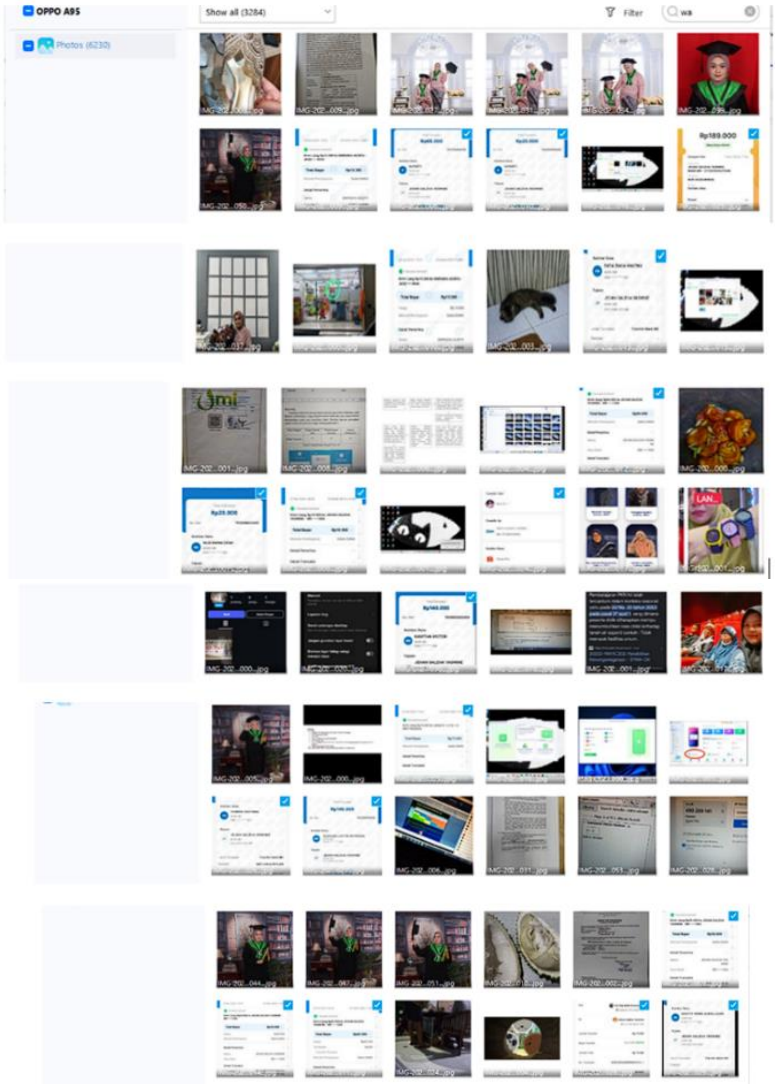

Figure 5. Digging Results Using Wondershare Dr.Fone

Next, to ensure that no evidence was overlooked, investigators conducted a second digging process using a different tool, EaseUS Mobisaver. This was based on the assumption that some evidence files might have been missed during the previous digging process.

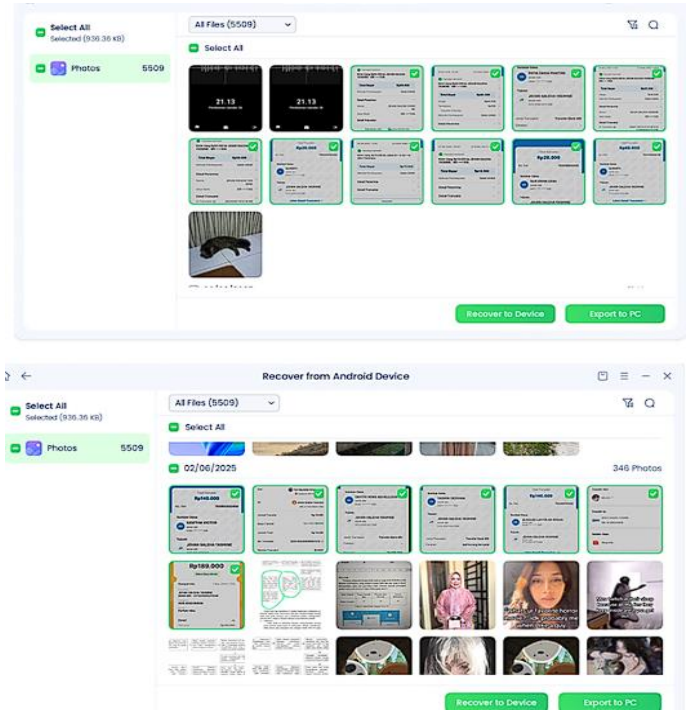

Figure 6. Digging Results Using EaseUS Mobisaver

Based on the digging results, investigators concluded that a total of 17 transfer receipt files were identified as potential evidence. After discovering these files through the digging process, the next step was file recovery to restore the deleted transfer receipts. The recovery process was carried out using two tools, Wondershare Dr.Fone and EaseUS MobiSaver, before the successfully recovered files were transferred to the investigator's laptop storage.

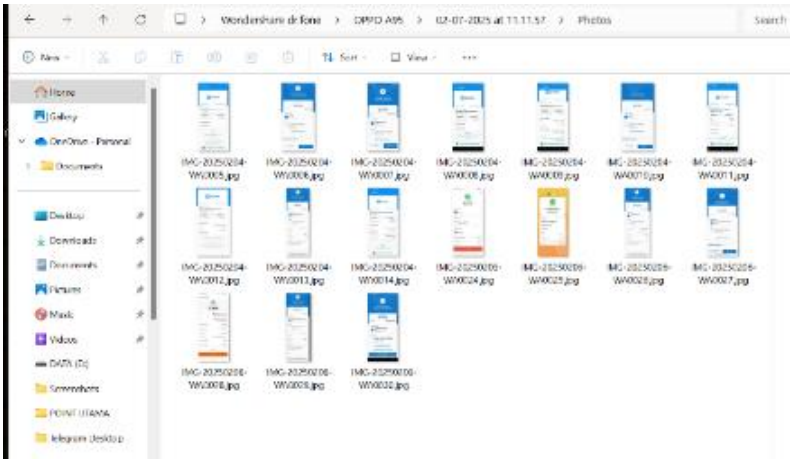

Figure 7. Recovery Results Using Wondershare Dr.Fone

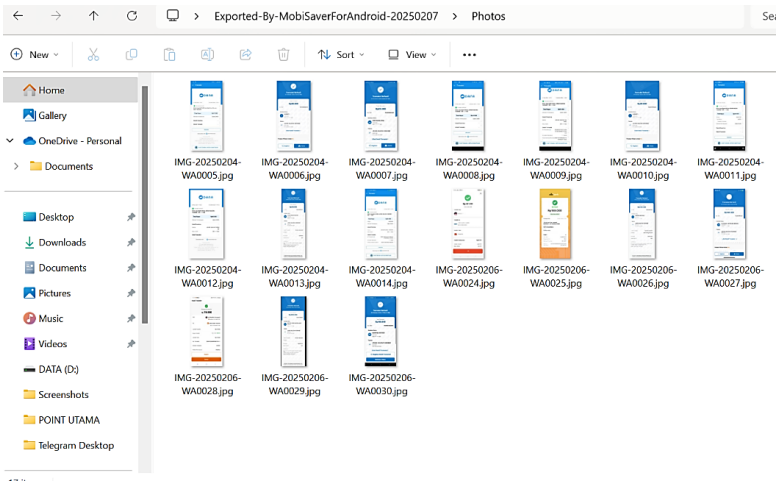

Figure 8. Recovery Results Using EaseUS Mobisaver

The recovered files were then further analyzed. In one of the recovered image files, the name and phone number of a student involved in the grade-buying transaction were identified. The student was found to have conducted a transaction with an unauthorized grade-changing service provider.

Additionally, from the transfer receipts, investigators discovered details about the transaction period, which took place between October 22 and November 5, 2024. Based on these findings, investigators concluded that there was collusion between the suspected student and an academic insider, who deliberately engaged in academic fraud by selling course grades.

d. *Reporting*

The reporting stage presents the results of the analysis conducted in the previous stages. This includes a detailed description of the evidence collected during the investigation. The report on the suspect's device and the forensic tools used can be seen in Table 2.

Bukti Digital	Target Jumlah data	Wondershare Dr.Fone	Easeus Mobisaver
Bukti Transfer	17	17	17

Table 2. Digital Evidence Results from Oppo A95

Reporting the analysis results focuses on the collected evidence. After completing the forensic analysis stages, a report can be made stating that in the search for digital evidence, investigators successfully recovered the deleted digital evidence, specifically the transfer transaction receipts. The analysis results of the recovered digital evidence from the smartphone can be seen in the following images.

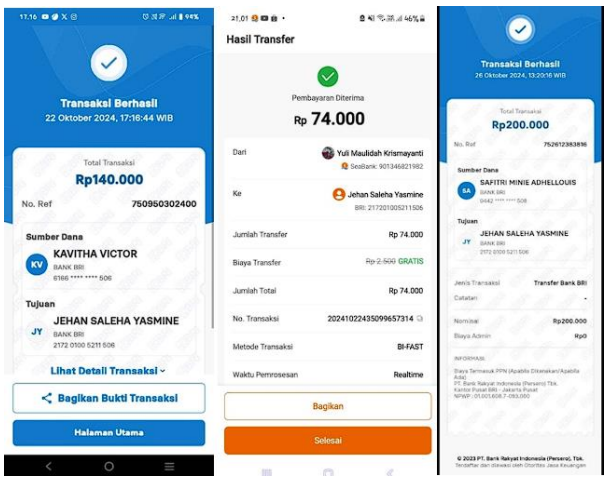

Figure 9. Transaction Evidence Between the First Perpetrator (Student) and the Second Perpetrator (Grade-Changing Broker)

3. Conclusion

Based on the research findings and discussion, the following conclusions can be drawn:

1. This study successfully demonstrated that deleted data from a Smartphone Oppo A95 can be recovered using the NIST method, following the stages of Collection, Examination, Analysis, and Reporting. The forensic testing was conducted using two tools, Wondershare Dr.Fone and EaseUS Mobisaver, both of which produced similar results by successfully retrieving 17 image files containing transfer receipts, suspected to be evidence of grade-buying transactions.
2. The results of this study highlight that the NIST-based digital forensic method, combined with the use of appropriate forensic tools, can effectively uncover deleted digital evidence. This finding demonstrates the significant potential of digital forensic techniques in supporting investigations of cybercrimes, including academic fraud such as the buying and selling of course grades.

Recommendations

To improve future research, the following recommendations are suggested:

1. There are many other forensic tools that can be explored and utilized in future studies. Using a variety of tools is expected to provide more comprehensive results, as each tool has unique characteristics that produce different outputs. This is due to the strengths and limitations of each tool in the data recovery process.
2. This study was limited to the Smartphone Oppo A95 as the test subject. Future research should expand its scope by testing other devices with different security systems to evaluate the consistency of data recovery results across various platforms.

Acknowledgment

We would like to express our gratitude to the Faculty of Computer Science for all the suggestions, input, and assistance in the publication process of this manuscript. Our sincere appreciation also goes to all parties who have supported this research and provided both moral and material assistance.

REFERENCE

[1] Y. Arif, E. I. Alwi, and M. A. Asis, "Analisis Bukti Digital Direct Message Pada Twitter Menggunakan Metode National Institute Of Justice (NIJ)," *INFORMAL Informatics J.*, vol. 8, no. 2, p. 165, 2023, doi: 10.19184/isj.v8i2.34025.

[2] R. N. Dasmen, M. R. Pratama, H. Yasir, and A. Budiman, "Analisis Forensik Digital Pada Kasus Cyberbullying Dengan Metode National Institute of Standard and Technology Sp 800-86," *J. Ilm. Inform.*, vol. 12, no. 01, pp. 68–73, 2024, doi: 10.33884/jif.v12i01.8344.

[3] Sahirudin, I. Riadi, and Sunardi, "Data Recovery Dengan Keamanan Fingerprint," *Pros. SENDI_U 2018*, pp. 978–979, 2018, [Online]. Available: https://semantikom.unira.ac.id/2017/SEMANTIKOM_2017_paper_26.pdf

[4] A. Fitriadi and H. A. Tawakal, "Jurnal Informatika Terpadu," *J. Inform. Terpadu*, vol. 7, no. 2, pp. 62–69, 2021, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[1] Y. Arif, E. I. Alwi, and M. A. Asis, "Analisis Bukti Digital Direct Message Pada Twitter Menggunakan Metode National Institute Of Justice (NIJ)," *INFORMAL Informatics J.*, vol. 8, no. 2, p. 165, 2023, doi: 10.19184/isj.v8i2.34025.

[2] R. N. Dasmen, M. R. Pratama, H. Yasir, and A. Budiman, "Analisis Forensik Digital Pada Kasus Cyberbullying Dengan Metode National Institute of Standard and Technology Sp 800-86," *J. Ilm. Inform.*, vol. 12, no. 01, pp. 68–73, 2024, doi: 10.33884/jif.v12i01.8344.

[3] Sahirudin, I. Riadi, and Sunardi, "Data Recovery Dengan Keamanan Fingerprint," *Pros. SENDI_U 2018*, pp. 978–979, 2018, [Online]. Available: https://semantikom.unira.ac.id/2017/SEMANTIKOM_2017_paper_26.pdf

[4] A. Fitriadi and H. A. Tawakal, "Jurnal Informatika Terpadu," *J. Inform. Terpadu*, vol. 7, no. 2, pp. 62–69, 2021, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[5] S. Marcellino, H. B. Seta, and I. W. Widi, "Analisis Forensik Digital Recovery Data Smartphone pada Kasus Penghapusan Berkas Menggunakan Metode National Institute of Justice (NIJ)," *Inform. J. Ilmu Komput.*, vol. 19, no. 2, pp. 141–156, 2023, doi: 10.52958/iftk.v19i2.4676.

[6] I. Riadi, Sunardi, and Sahiruddin, "Analisis Forensik Pada Platform Android Menggunakan Metode NIJ," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, pp. 87–95, 2019.

[7] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.

[8] I. Riadi, Sunardi, and Sahiruddin, "Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode Nist," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 1, pp. 197–204, 2020, doi: 10.25126/jtiik.202071921.

[9] Riya Majalista and Tata Sutabri, "Analisis Pencarian Data Smartphone Menggunakan Nist Untuk Penyelidikan Digital Forensik," *J. Inform. Teknol. dan Sains*, vol. 5, no. 1, pp. 81–85, 2023, doi: 10.51401/jinteks.v5i1.2200.

[10] A. Syauqi, "Analisis Recovery Bukti Digital Instan Messenger Pada Smartphone Android Menggunakan Metode National Institute of Standards and Technology (Nist) Studi Kasus : Kasus Perselingkuhan," *J. Chem. Inf. Model.*, vol. 1, no. 2, pp. 65–69, 2020.

[11] K. Eka Purnama, C. Rozikin, and A. Ali Ridha, "Analisis Forensic Citra Digital Menggunakan Teknik Error Level Analysis Dan Metadata Berdasarkan Metode Nist," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 2, pp. 1100–1107, 2023, doi: 10.36040/jati.v7i2.6660.

[12] D. Royadi, M. Asfi, and A. Sevtiana, "Implementasi Metode Standar NIST Dalam Analisis Data Forensik Studi Kasus Penipuan Salah Transfer Mencatut Nama Wabup

Pada SMP Ar-rohman Krangkeng," *LOFIAN J. Teknol. Inf. dan Komun.*, vol. 3, no. 1, pp. 12–19, 2023, doi: 10.58918/lofian.v3i1.216.

[13] "Instant Messenging, Mobile Forensics ," pp. 360–371.

[14] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 1, 2016, doi: 10.26418/jp.v2i1.14369.

[15] I. Irwansyah and H. Yudiastuti, "Analisis Digital Forensik Rekayasa Image Menggunakan Jpegsnoop Dan Forensically Beta," *J. Ilm. Matrik*, vol. 21, no. 1, pp. 54–63, 2019, doi: 10.33557/jurnalmatrik.v21i1.518.

[16] M. Mushlihudin and A. Nofiyan, "Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology," *Cybernetics*, vol. 4, no. 02, pp. 11–23, 2021, doi: 10.29406/cbn.v4i02.2287.

[17] Anton Yudhana, Abdul Fadlil, and M. R. Setyawan, "Analysis of Skype Digital Evidence Recovery based on Android Smartphones Using the NIST Framework," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 682–690, 2020, doi: 10.29207/resti.v4i4.2093.

[18] S. R. A. Ardiningtias, Sunardi Sunardi, and Herman Herman, "Investigasi Digital Pada Facebook Messenger Menggunakan National Institute of Justice," *J. Inform. Polinema*, vol. 7, no. 4, pp. 19–26, 2021, doi: 10.33795/jip.v7i4.709.

[19] H. R. Khalifa, F. A. Yulianto, and E. M. Jadied, "Implementasi Teknik Penghapusan Data Dengan Metode DoD 5220 . 22M Pada Sistem Operasi Android Implementation Of Data Deletion Using DoD 5220 . 22M method On Android Operating System," vol. 3, no. 1, pp. 897–913, 2016.