International Journal of Advances in Data and Information Systems
Vol. 5, No. 2, October 2024, pp. 113~122
ISSN: 2721-3056, DOI: 10.59395/ijadis.v5i2.1328

Forensic Analysis of the WhatsApp Application Using the National Institute of Justice Framework

Muhammad Fahmi Mubarok Nahdli[1], Imam Riadi*[2], Muhammad Kunta Biddinika[3]
[1] Master Program of Informatics, Universitas Ahmad Dahlan, Indonesia
[2] Department of Information System, Universitas Ahmad Dahlan, Indonesia
[3] Master Program of Informatics, Universitas Ahmad Dahlan, Indonesia

Article Info

Article history:

Received Jun 25, 2024
Revised Sep 09, 2024
Accepted Oct 30, 2024

Keywords:

Digital Forensic
Drug Trafficking
National Institute of Justice
Smartphone
WhatsApp

ABSTRACT

The advancement of communication media has rapidly evolved with the emergence of various communication applications on smartphones, which have now surpassed mere communication functions to become complex social media platforms. This change has transformed the way we interact, not only through messages and voice but also through the exchange of videos and images. However, along with these developments, there has been a surge in digital crimes such as defamation, fraud, and drug trafficking. This investigation aims to compare the performance of forensic tools in obtaining digital evidence by utilizing applications like Mobiledit, Belkasoft, Mobile Forensic SPF, and Magnet Axiom, and by applying the National Institute of Justice framework, which consists of five stages: identification, collection, examination, analysis, and reporting. The output of the investigation is presented through reports and evidence, resulting in text chat files, contacts, images, audio, and view-once images. Forensic tools have a 100% success rate in finding pieces of evidence. The comparison of the four tools showed different percentages: Mobiledit Forensic 40%, Magnet Axiom 80%, Belkasoft 60%, and Mobile Forensic SPF 60% in obtaining evidence. Digital evidence can be used as strong support in court proceedings.

Corresponding Author:

Imam Riadi,
Department of Information System,
Universitas Ahmad Dahlan,
Jl. Ringroad Selatan, Kragilan, Tamanan, Banguntapan, Bantul, Special Region of Yogyakarta.
Email: imam.riadi@is.uad.ac.id

1. INTRODUCTION

The use of mobile devices has become an unavoidable need and is in great demand in Indonesia, especially with the population reaching 276.4 million in 2023, more than 353.8 million people use smartphones as a means of mobile connection. Most individuals own more than one smartphone device. Internet users account for 212.9 million people, while 167.0 million Indonesians are active on various social media platforms, especially to communicate via messaging media (we are social & Hootsuite, 2023), which can be seen in Figure 1.

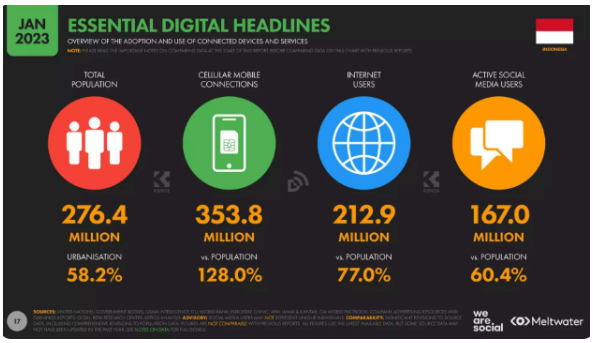

Figure 1. Smartphone user data

As smartphone use increases, Android applications continue to experience rapid development. One example is an instant messaging application that allows communication via chat. WhatsApp is the most widely used application in Indonesia, holding the top spot in terms of usage [1]. The growing use of short messaging applications also comes with growing security risks. Several parties utilize WhatsApp for cybercrimes, such as online prostitution, cyberstalking [2]-[3], sextortion, and drug trafficking [4], [5]. Figure 2 shows application usage ranking data from similarweb.com, with WhatsApp having the most users in Indonesia.

	App and Publisher	Category
1	WhatsApp Messenger WhatsApp LLC	Communication
2	Google Chrome: Fast & Secure Google LLC	Communication
3	Messenger Meta Platforms, Inc.	Communication
4	WhatsApp Business WhatsApp LLC	Communication
5	Telegram Telegram FZ-LLC	Communication
6	Gmail Google LLC	Communication
7	Vivo Browser PT. Vivo Mobile Indonesia	Communication

Figure 2. Statistics of popular applications in Indonesia
Source link https://www.similarweb.com/top-apps/google/indonesia/communication

The top messaging application in Indonesia is WhatsApp, as demonstrated in Figure 2. However, with the increase in the number of available instant messaging applications, security concerns are on the rise. This leads some people to abuse instant messaging apps to carry out criminal activities. One common application used for this purpose in Indonesia is WhatsApp [6]. WhatsApp is often used to commit cybercrimes, with drug trafficking being a particularly serious concern [7]. To address this issue, there is a need for analytical and forensic methods that can help uncover criminal activities on social media platforms like WhatsApp. While WhatsApp allows for text communication and image sharing, it also introduces security vulnerabilities.

Digital forensics involves using computer technology to gather legal evidence, employing advanced technology and computers to prove crimes, and utilizing digital evidence to catch criminals. Mobile Forensics is a branch of digital forensics that aims to discover and identify cybercrimes. Its goal is to legally process the evidence [8]. Digital evidence often exists as electronic data, including documents, emails, contacts, text messages, and media files like sound, images, and videos. In Cybercrime investigations, it is emphasized that having a structured forensic framework is crucial to enhance the efficiency and effectiveness of the investigation process [9], [10]. Researchers commonly utilize various well-known structures, such as the National Institute of Justice

(NIJ) [11], the National Institute of Standards and Technology (NIST) [12], the Digital Forensics Research Workshop (DFRWS) [13], the Association of Chief Police Officers (ACPO) [14], [15], and the Integrated Digital Forensic Investigation Framework (IDFIF) [16].

The research previously conducted was titled " Google Drive Android Acquisition Using Oxygen and Mobiledit with the National Institute of Justice Method ". This research aims to gather evidence of digital crimes stored on Google Drive using acquisition tools such as Oxygen Forensics and Mobiledit [17]. Another study with a similar focus is entitled " Comparison of Android-based Instagram Digital Forensics Tool with approach from NIST [18]. This research outlines the use of forensic tools to recover digital evidence from the Instagram platform. The third research entitled "Forensic Analysis of the MiChat Application Using the Digital Forensics Research Workshop Method", this research was conducted on the MiChat application using the approach from the Digital Forensic Research Workshop (DFRWS). This research aims to uncover evidence related to drug trafficking that occurs on the MiChat platform [19]. The following research, titled "Digital Forensic Analysis of the WhatsApp Application on iOS-Based Smartphones Based on the Association of Chief Police Officers (ACPO)", aims to investigate criminal acts such as revenge porn crimes on the WhatsApp application [20]. The latest research entitled "Comparative Analysis of Recovery Tools For Digital Forensic Evidence Using NIST Framework" aims to compare the performance of forensic tools in recovering deleted data in the form of contact data, call logs, and messages used as evidence in trials [21].

The relevance of this research to previous research in the field of digital forensics. Research on Google Drive acquisitions using Oxygen and Mobiledit with NIJ methods shows similarities in Mobiledit's use of forensic tools to collect digital evidence from different platforms. A comparative study of Android-based Instagram digital forensic tools that adopt the NIST approach emphasizes the importance of forensic standards, as does this research that uses the NIJ framework. Other studies using the DFRWS method for the MiChat application and the ACPO approach for WhatsApp highlight the use of different forensic methodologies to collect digital evidence from the same or different applications for similar purposes. Additionally, this study also compared the performance of several forensic tools, similar to studies comparing data recovery tools using the NIST framework, demonstrating consistency in the evaluation of the effectiveness of forensic tools.

Application of the framework developed by the National Institute of Justice (NIJ) for handling criminal cases involves five stages of the forensic process [22]. The initial stage is Identification, where the case is identified at the scene of the crime. The next stage is Collection, wherein physical and digital evidence is gathered and recorded. The third stage is the Examination phase, during which digital data is gathered and stored as a backup [23]. Stage four involves Analysis, during which digital evidence is examined using forensic tools [24]. The final stage is Reporting, where a detailed report is made about the entire forensic process that has been carried out [25].

Therefore, what differentiates this research from previous ones is the use of evidence acquisition tools and adding research material in the form of image view once in each acquisition process. This investigation aims to compare the performance of the MOBILedit Forensic, Belkasoft Evidence, Mobile Forensic SPF, and Magnet Axiom tools in acquiring digital evidence, as well as carrying out forensic analysis on the WhatsApp application. This research adopts the National Institute of Justice framework to recover digital evidence in drug trafficking cases.

2. RESEARCH METHOD

Using the right framework in the digital evidence collection process can increase accuracy in data collection. Figure 3 shows the steps for implementing the NIJ framework. Figure 3 explains the application of the NIJ framework that investigators tried in the process of investigating drug sales cases on the WhatsApp application. The flow in the NIJ framework has five processes which can be seen in Figure 4.

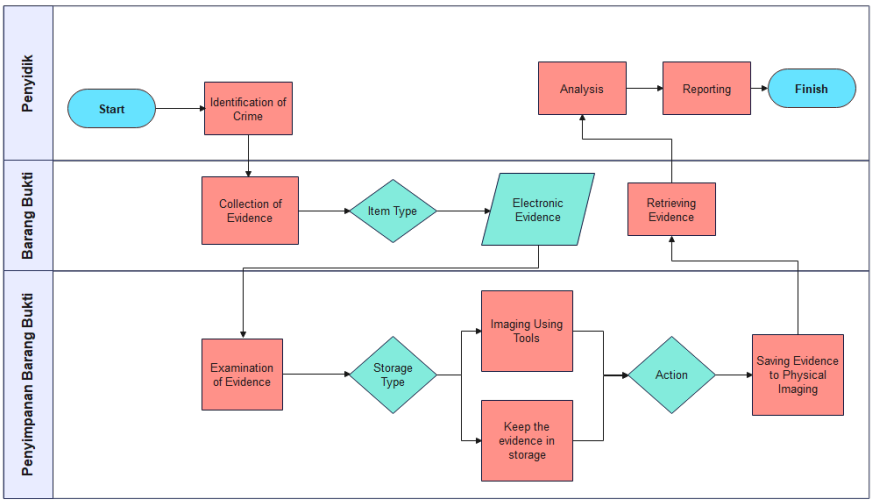

Figure 3. Implementation of the National Institute of Justice Framework

Figure 4. National Institute of Justice Methods

a. Identification

The identification stage is grouping evidence of digital crimes and collecting data that supports investigations to find evidence of digital crimes. At this stage, including the process of identification, labeling, and recording to ensure the integrity of the evidence is maintained, in this research, the evidence was in the form of a smartphone.

b. Collection

During the collection stage, various activities are carried out to gather data supporting the investigation process for digital crime evidence. This involves retrieving data from relevant sources and ensuring the integrity of the evidence.

c. Examination

The examination stage involves forensic examination and data collection from physical evidence. To maintain data integrity, utilize a combination of scenarios, either automatically or manually. At this stage, a forensic process is also carried out using four software.

d. Analysis

The stage of analysis is carried out after obtaining the desired digital files or data from the previous examination. Next, the data is analyzed in detail and comprehensively using technically and

legally appropriate methods to provide strong evidence for the data. The results of the analysis of the digital data are then considered as digital evidence that can be scientifically and legally accountable.

e. Reporting

The reporting stage is carried out after obtaining digital evidence from the inspection process and involves thorough analysis. At this stage, analysis results are reported which include an explanation of the actions taken, a description of the tools and methods used, an identification of supporting actions taken, and recommendations for improving policies, procedures, tools, or other supporting aspects in the digital forensic action process.

The research subject in this instance is the WhatsApp application. The institution responsible for development and security standards is NIJ, which has the authority to refer to digital forensics [26].

2.1 Research Tools and Materials

This research involves the use of several tools including the Oppo a37f mobile device, HP core i7 laptop, USB connector, and other supporting devices, namely the WhatsApp application, MOBILedit Forensic, Belkasoft Evidence, Mobile Forensic SPF, and Magnet Axiom. These forensic analysis tools are listed in Table 1.

Table 1. Research Tools and Materials

Tools and Software	Information
Oppo A37f	Object of research
Laptop Hp	Windows 11, 64 Bit, 8 GB RAM
USB Connector	Connection Smartphone
WhatsApp Messenger	Software test
Mobiledit Forensic Express	Tool Forensic
Belkasoft Evidence	Tool Forensic
Mobile Forensic SPF	Tool Forensic
Magnet Axiom	Tool Forensic

The use of the four forensic tools in Table 1 is based on their respective advantages in digital data analysis. Mobiledit Forensic has the advantage of extracting data from various mobile devices. Belkasoft Evidence Center is strong in in-depth analysis of various types of data, including chat and social media. Mobile Forensic SPF focuses on recovering deleted or damaged data. Magnet Axiom offers cross-platform analytics that integrates data from mobile devices, computers, and the cloud. This combination ensures a comprehensive approach to collecting and analyzing digital evidence, supporting the accuracy of forensic research results.

2.2 Case Simulation

Simulation of drug trafficking cases via the WhatsApp application between one seller (perpetrator) and one buyer (victim). Figure 5 shows the interaction between sellers and buyers in sending chat messages. The simulation of this drug sales case is seen in Figure 5.

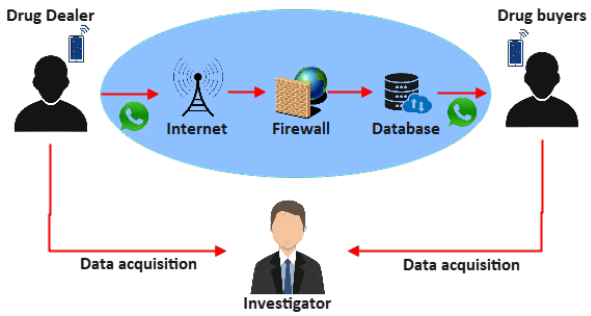

Figure 5. Simulation of drug trafficking cases on WhatsApp

Figure 5 explains a case simulation on the WhatsApp application installed on a smartphone, where an individual acts as a drug seller who carries out transactions via text, and audio conversations, as well as sending photos of types of illegal drugs to interested users. After the drug user is caught by the police, the drug seller deletes several messages that have been sent. Therefore, the police need an investigator or investigator to help collect the digital evidence needed to solve the case.

3. RESULTS AND DISCUSSION

This section should explain the research conducted comprehensively, covering various sub-topics. In addition, presenting findings and analysis in the form of figures and tables will provide strong visual support for the results obtained. It is hoped that the results and discussions from this research will make a major contribution to the understanding and development of this field.

3.1. Identification

This study uses simulated cases on mobile devices as physical evidence in drug trafficking cases. It considers digital evidence such as text chats, contacts, images, viewed images, and audio as relevant parameters. Figure 6 presents specific information about the Oppo A37f smartphone.

Manufacture	**Oppo**
Product	**Oppo_A37f**
Platform	**Android**
Serial Number	**438d155**
IMEI1	**864877032648772**
IMEI2	**864877032648764**
SIM Card	**Yes**

Figure 6. Evidence of smartphone specifications

3.2. Collection

The second stage is data collection which includes identifying digital evidence originating from the WhatsApp application. The digital evidence acquisition process carries high risks, including the possibility of serious errors occurring which could result in loss or damage to data on digital evidence that cannot be read by forensic tools. Therefore, investigators must conduct physical imaging or perform backup steps, also known as logical acquisition. Magnet Axiom is a tool used to perform the backup process, providing a reliable backup system for mobile devices to ensure the security and reliability of the obtained evidence. The results of this acquisition are stored in zip file format, the importance of the authenticity of the evidence is very sensitive, because changes to the original evidence are considered as changes to the evidence presented. Figure 7 is the acquisition process using Magnet Axiom with the output in the form of a zip file.

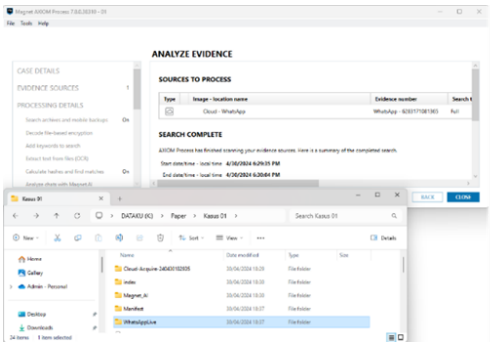

Figure 7. Acquisition Process in Magnet Axiom Software with Zip file output

3.3. Examination

Examination is the stage where investigators examine digital evidence collected through a scanning framework with the actions taken in artifact acquisition. Artifact selection is an important step because various types of artifacts are produced from the extraction process, such as log records and databases obtained in the backup file folder. Investigation procedures involve the use of forensic tools to analyze and process evidence data, such as filtering hash files, and investigators carrying out extraction using appropriate software or tools such as the Magnet Axiom tool. Extracted data files include conversation text files, contact files, image files, audio files, and view-once image files. The authenticity of each piece of digital evidence will be verified using a hash generator tool to ensure that the digital evidence has not been altered. The extraction process was carried out using the Magnet Axiom tool, which can be seen in Figure 8.

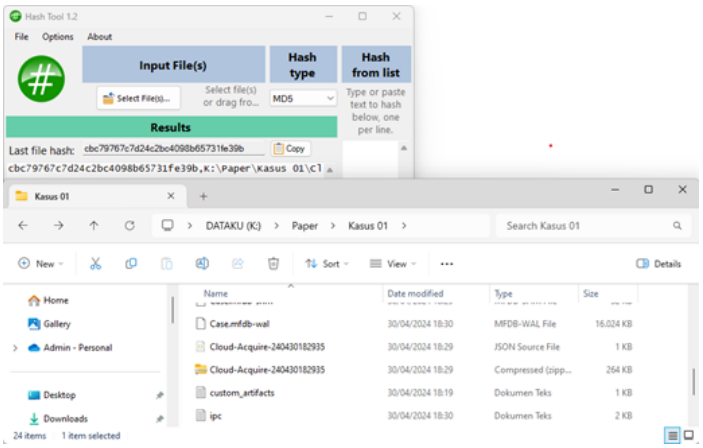

Figure 8. Checking hash value of evidence file

Table 2. Artifact Extraction Results and Evidence Validation

Evidence	Directory	File Name	Hashing File
Text Chat	phone\applications0\ com.whatsapp.im\backup\db\ 3817535436356331social.db	38175354363 56331social.db	cbc79767c7d24c2bc40 98b65731fe39b
Contact	phone\applications0\ com.whatsapp.im\backup\db\ 7909537856358531social.db	79095378563 58531social.db	cbc79767c7d24c2bc40 98b65731fe39b
Images	phone\applications0\ com.whatsapp.im\ live_external\cache\uil-images\ 6jpj7po8stzthepm24kffhn7h0	6jpj7po8stzth epm24kffhn7h0	ed9dbb3a490317532dbfg8f a647d906e
Audio	phone\applications0\ com.whatsapp.im\live_external\ files\audio\4273\ F8g13859757148722.ogg	F8g1385975 7148722.ogg	89738e796942a64e9743a6 09254c40cc
Image view once			

3.4. Analysis

Analysis is data that comes from the extraction results during the examination session which are explained in detail according to the procedure. All information uncovered during the examination process is interconnected to determine if it aligns with the predetermined research procedures and simulations for identifying digital evidence. Investigators used four forensic applications, namely Mobiledit Forensic, Magnet Axiom, Belkasoft, and Mobile Forensic SPF. The analysis procedure involves further investigation based on determined parameters, such as conversation text and telephone numbers. Investigators analyzed the search and matching of evidence related to images, audio, and image view once using the Magnet Axiom device. Afterward, all the collected evidence will be compiled and presented in a report by investigators, aiming to facilitate comprehension for non-experts. The results of the analysis of each software used are stated in Table 3.

Table 3. Acquisition results of each forensic tools

Digital Evidence	Digital evidence obtained				Evidence
	Mobiledit Forensic	Magnet Axiom	Belkasoft	Mobile Forensic SPF	
Text Chat	0	27	0	0	27
Nomor Telephone	0	1	1	1	1
Image	1	1	1	1	1
Audio	1	1	1	1	1
Image View Once	0	0	0	0	1
Percentage of Success	**40%**	**80%**	**60%**	**60%**	**100%**

Based on Table 3. The digital evidence obtained was text chats sent by 27 chats found using the Magnet Axiom tools. 1 contact file was successfully found, and 1 contact and 1 image file were found by the four tools, namely MOBILedit Forensic, Magnet Axiom, Belkasoft, and Mobile Forensic SPF. The audio file evidence found was 1 audio file using the MOBILedit Forensic tool, 1 audio file using Magnet Axiom, 1 audio file using Belkasoft, 1 audio file using Mobile Forensic SPF, and 1 file sent. 1 Image view once file cannot be found in all tools because in this study the rooting process was not carried out on mobile devices, and the function of forensic tools was limited. Evidence of text chat, contact, and image view once, cannot be read or found due to the limited functionality of the MOBILedit Forensic tool. Axiom Magnet tools cannot find the Image view once file. Furthermore, the evidence that could not be found by the Belkasoft and Mobile Forensic SPF tools was the text chat file and image view once file. The percentage of digital image views once evidence is 0%. Comparing the parameters of the evidence found with the parameters of the four tools used to find the evidence sent, the overall success rate is 100% because each tool still has weaknesses in finding evidence. Achieving a higher level of success depends on the capabilities of the forensic tools used. A comparison of forensic tools for digital evidence can be seen in Table 4.

Table 4. Forensic Tools Comparative Acquisition Results

	Forensic Tools			
Results	**Mobiledit Forensic**	**Magnet Axiom**	**Belkasoft**	**Mobile Forensic SPF**
Text Chat	not found	found	not found	not found
Nomor Telephone	not found	found	found	found
Image	found	found	found	found
Audio	found	found	found	found
Image View Once	not found	not found	not found	not found

Based on Table 4, various indicators are utilized as forensic evidence in drug trafficking cases. Discrepancies in the results obtained from the four forensic tools such as Mobiledit Forensic, Magnet Axiom, Belkasoft, and Mobile Forensic SPF. MOBILedit Forensic found evidence in the form of images and audio as much as 2 out of 5 digital pieces of evidence according to the case simulation which was the parameter. Magnet Axiom found 4 out of 5 pieces of evidence for the parameters sought, Belkasoft successfully identified 3 out of the 5 key parameters, while Mobile Forensic SPF found 3 out of the 5 key pieces of evidence. In the given scenario, it can be inferred that the tools have the following accuracy levels in acquiring evidence: 40% for Mobiledit Forensic, 80% for Magnet Axiom, 60% for Belkasoft, and 60% for Mobile Forensic SPF.

3.5. Reporting

Reporting is an evaluation of evidence obtained in this simulation, involving an Oppo A37f cellphone that is not rooted. It can be concluded that the forensic framework is still able to reveal some digital evidence such as conversation text, images, and audio used in drug buying and selling activities.

Table 5. Information report on drug trafficking cases

Information	Evidence	Result
Oppo A37f	Smartphone Android	✓
Nomor Handphone	08371754598	✓
Account name	Elephent	✓
Conversation Time	-	-
Chat Evidence File	27	✓
Contact Proof File	1	✓
Image Evidence File	1	✓
Audio Evidence Files	1	✓
Image View Once Evidence File	1	-
Tools Forensic	Mobiledit Forensic, Magnet Axiom, Belkasoft, dan Mobile Forensic SPF	✓

A comparison of the results of the performance of tools on the Oppo A37f smartphone when rooting was not carried out using four forensic applications to restore data, namely Mobiledit Forensic 40%, Magnet Axiom 80%, Belkasoft 60%, and Mobile Forensic SPF 60%.

4. CONCLUSION

Based on the results of investigations into drug trafficking crime cases using the WhatsApp application with the NIJ framework, several tools such as MOBILedit Forensic, Magnet Axiom, Belkasoft, and Mobile Forensic SPF were used to obtain digital evidence such as text chat files, contacts, images, audio, and image view once. Overall, the authenticity of evidence can be verified by hashing files, and the success rate in finding evidence based on parameters reaches 100% according to the capabilities of forensic tools. The research results were by the research objectives, and investigators found that the Magnet Axiom tool had the highest success rate, namely 80%. However, the weakness of this research is that the four forensic tools used were unable to find image views once in the WhatsApp application.

ACKNOWLEDGEMENTS

This research was supported by the Direktorat Riset, Teknologi, dan Pengabdian Masyarakat (DRTPM) Direktorat Jenderal Pendidikan Tinggi, Riset, dan Teknologi, Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi under Penelitian Tesis Magister (Master's Thesis Research) with grant number: 070/PTM/LPPM-UAD/VI/2024 (15 Juni 2024).

REFERENCES

[1] D. Sulisdyantoro and M. I. Marzuki, "Identification of Whatsapp Digital Evidence on Android Smartphones using The Android Backup APK (Application Package Kit) Downgrade Method," *J. Integr. Adv. Eng.*, vol. 3, no. 1, pp. 7–22, 2023, doi: 10.51662/jiae.v3i1.70.

[2] V. RODRIGUES, "Cyber Stalking Issues of Enforcement in Cyber Space," 2020.

[3] A. Becker, J. V. Ford, and T. J. Valshtein, "Confusing Stalking for Romance: Examining the Labeling and Acceptability of Men's (Cyber)Stalking of Women," *Sex Roles*, vol. 85, no. 1–2, pp. 73–87, 2021, doi: 10.1007/s11199-020-01205-2.

[4] M. Marzuki and T. Sutabri, "Analisis Forensik Media Sosial Michat Metode Digital Forensik Integrated Investigation Framework (Idfif)," *Blantika Multidiscip. J.*, vol. 2, no. 1, pp. 56–70, 2023, doi: 10.57096/blantika.v2i1.11.

[5] Sakshi, A. Vashishth, and Teena, "An Analysis of Cyber Crime with Special Reference to Cyber Stalking," *J. Posit. Sch. Psychol.*, vol. 6, no. 4, pp. 1279–1287, 2022.

[6] A. Alhusaini and I. Riadi, "Forensic Mobile Drug Trafficking WhatsApp Services using National Standard of Technology Method," *Int. J. Comput. Appl.*, vol. 183, no. 40, pp. 56–62, 2021, doi: 10.5120/ijca2021921801.

[7] C. Hu, B. Liu, Y. Ye, and X. Li, "Fine-grained classification of drug trafficking based on Instagram

hashtags," *Decis. Support Syst.*, vol. 165, no. February 2022, p. 113896, 2023, doi: 10.1016/j.dss.2022.113896.

[8] I. Riadi, H. Herman, and I. A. Rafiq, "Mobile Forensic Investigation of Fake News Cases on Instagram Applications with Digital Forensics Research Workshop Framework," *Int. J. Artif. Intell. Res.*, vol. 6, no. 2, 2022, doi: 10.29099/ijair.v6i2.311.

[9] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive review of cybercrime detection techniques," *IEEE Access*, vol. 8, pp. 137293–137311, 2020, doi: 10.1109/ACCESS.2020.3011259.

[10] G. M. Zamroni and I. Riadi, "Mobile Forensic Tools Validation and Evaluation for Instant Messaging," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 10, no. 5, pp. 1860–1866, 2020, doi: 10.18517/ijaseit.10.5.7499.

[11] H. Nurhairani and I. Riadi, "Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method," *Int. J. Comput. Appl.*, vol. 177, no. 27, pp. 35–42, 2019, doi: 10.5120/ijca2019919749.

[12] A. Yudhana, I. Riadi, and I. Zuhriyanto, "Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)," *J. TECHNO*, vol. 20, no. 2, pp. 125–130, 2019.

[13] G. Zaida Muflih, "Comparison of Forensic Tools on Social Media Services Using the Digital Forensic Research Workshop Method (DFRWS)," *JIKO (Jurnal Inform. dan Komputer)*, vol. 6, no. 1, pp. 52–61, 2023, doi: 10.33387/jiko.v6i1.5872.

[14] M. S. Jafri, S. Raharjo, and M. R. Arief, "Implementation of ACPO Framework for Digital Evidence Acquisition in Smartphones," *CCIT J.*, vol. 15, no. 1, pp. 82–105, 2022, doi: 10.33050/ccit.v15i1.1586.

[15] R. Y. Prasongko, A. Yudhana, and I. Riadi, "Analisis Penggunaan Metode ACPO (Association of Chief Police Officer) pada Forensik WhatsApp," *J. Sains Komput. Inform.*, vol. 6, no. 2, pp. 1112–1120, 2022.

[16] F. F. Febrian and J. Sidabutar, "Comparative Analysis of Forensic for Whatsapp Desktop on Mac OS and Windows Using IDFIF V2," *Proc. - 2023 IEEE Int. Conf. Cryptogr. Informatics, Cybersecurity Cryptogr. Cybersecurity Roles, Prospect. Challenges, ICoCICs 2023*, pp. 327–331, 2023, doi: 10.1109/ICoCICs58778.2023.10276727.

[17] Jeki Kuswanto, Nur Asyifa, and I. Hadi Purwanto, "Akuisiss Google Drive Android Menggunakan Oxygen dan Mobiledit dengan Metode National Institute of Justice," *J. Inform. Teknol. dan Sains*, vol. 5, no. 1, pp. 141–147, 2023, doi: 10.51401/jinteks.v5i1.2523.

[18] Irhash Ainur Rafiq, Imam Riadi, and Herman, "Perbandingan Forensic Tools pada Instagram Menggunakan Metode NIST," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 2, pp. 134–142, 2022, doi: 10.14421/jiska.2022.7.2.134-142.

[19] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *J. Media Inform. Budidarma*, vol. 6, no. 2, p. 1263, 2022, doi: 10.30865/mib.v6i2.3946.

[20] F. Dwi, R. Rini, R. Wilis, and R. A. Wildana, "Analisis Forensik Digital Aplikasi WhatsApp pada Smartphone Berbasis iOS Berdasarkan ACPO," vol. 1, no. 7, pp. 740–749, 2024.

[21] M. Surya, J. Sidabutar, and N. Qomariasih, "Comparative Analysis of Recovery Tools For Digital Forensic Evidence Using NIST Framework 800-101 R1," *Proc. - 2023 IEEE Int. Conf. Cryptogr. Informatics, Cybersecurity Cryptogr. Cybersecurity Roles, Prospect. Challenges, ICoCICs 2023*, pp. 258–262, 2023, doi: 10.1109/ICoCICs58778.2023.10276447.

[22] M. E. Apriyani, R. A. Maskuri, and M. H. Ratsanjani, "Forensic Digital Analysis of Telegram Applications Using the National Institute of Justice and Naïve Bayes Methods," vol. 5, no. 2, pp. 21–30, 2023.

[23] S. Soni, Y. Fatma, and R. Anwar, "Akuisisi Bukti Digital Aplikasi Pesan Instan 'Bip'Menggunakan Metode National Institute Of Justice (NIJ)," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 3, no. 1, pp. 34–42, 2022, doi: 10.37859/coscitech.v3i1.3694.

[24] Y. Marumo, "Forensic Examination of Soil Evidence," *Japanese J. Forensic Sci. Technol.*, vol. 7, no. 2, pp. 95–111, 2015, doi: 10.3408/jafst.7.95.

[25] J. Ropero-Miller, "NIJ's CJTEC: Enabling Informed Decisions About Technology-centric Procurement and Practices," *Forensic Sci. Int. Synerg.*, vol. 4, p. 100260, 2022, doi: 10.1016/j.fsisyn.2022.100260.

[26] G. LaPorte and H. Waltke, "National Institute of Justice: An Update on Forensic Science Resources," *Forensic Sci. Int. Synerg.*, vol. 1, no. 2019, p. S15, 2019, doi: 10.1016/j.fsisyn.2019.02.043.