Scientific Journal of Informatics
Vol. 11, No. 4, Nov 2024
p-ISSN 2407-7658 https://journal.unnes.ac.id/journals/sji/index e-ISSN 2460-0040

Comparison of Digital Forensic Tools for Drug Trafficking Cases on Instagram Messenger using NIST Method

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

Abstract.
Purpose: Cybercrime is an unlawful act that utilizes computer technology and the development of the internet. Cybercrime can occur on all electronic devices, including Android smartphones. Forensic handling, particularly mobile forensics, has become crucial in addressing drug trafficking cases conducted through Instagram. As the primary device for accessing Instagram, smartphones store digital data that can serve as evidence in investigations. This research aims to produce a more accurate comparison of results in analyzing Instagram Messenger data containing content related to drug trafficking.
Methods: The digital evidence data used in this research included five types of data: text chat, account, image, audio, and image view once. The forensic tools for obtaining digital evidence were MOBILedit, Belkasoft, Mobile Forensic SPF, and Magnet Axiom. The method proposed in this research followed the NIST framework, which consists of four stages: collection, examination, analysis, and reporting. This research followed the NIST framework because it is widely recognized in the field of digital forensics and provides a comprehensive guideline for handling digital evidence.
Result: Research results showed that Magnet Axiom had the best performance in digital forensic analysis, with a success rate of 74.1%. MOBILedit Forensic had a success rate of 62.5%, indicating lower performance. Mobile Forensic SPF had a success rate of 44.6%. In comparison, Belkasoft had the lowest success rate of 23.2%, showing that this software could be more effective in detecting and analyzing digital data than the others.
Novelty: In this study, the analysis process was conducted using four digital forensic tools, each showing variations in terms of efficiency and effectiveness. Each tool has advantages and disadvantages regarding speed, accuracy, and ability to extract and manage data.

Keywords: Digital forensic, Drug trafficking, Instagram, National institute of standards and technology, Smartphone
Received September 2024 / **Revised** October 2024 / **Accepted** November 2024

INTRODUCTION

Cybercrime violates the law that exploits computer technology based on the development of internet technology [1]. Cybercrime refers to criminal activities using computers or computer networks as tools, targets, or crime scenes [2], [3]. Cybercrime encompasses various types of offenses, such as online auction fraud, check forgery, credit card fraud, trust fraud, identity theft, drug trafficking, and pornography [4]. Cybercrime can occur on all devices, including Android smartphones [5].

A smartphone is a prevalent type of mobile phone equipped with an operating system that allows users to run various applications, including Android [6], [7]. The open-source nature of the Android operating system provides developers with the freedom to contribute to the rapid growth of the Android ecosystem [8], [9]. Android-based smartphone technology offers opportunities for app developers to expand the use of applications, mainly social media platforms like Instagram, on this platform [10]. Smartphones also provide Instant Messaging (IM) applications that enable fast message and image sharing, such as Instagram [11].

Instagram is an app designed specifically for sharing photos, allowing users to capture images with their device's camera, apply various filters and creative effects, and share them directly on different social networks [12]. Due to its extensive capabilities for self-expression and interaction, Instagram has become

*Corresponding author.
Email addresses: fahmielnahdli@gmail.com (Nahdli), imam.riadi@is.uad.ac.id (Riadi)*, muhammad.kunta@mti.uad.ac.id (Biddinika)
DOI: 10.15294/sji.v11i4.13463

one of the most popular social media platforms among smartphone users [13]. Instagram features have become a factor for many Instagram users aiming to communicate through social media, one of the latest features is Instagram Messenger, which can assist in sending photos or having private conversations between Instagram users [14]. The number of Instagram users worldwide experienced rapid growth in 2024. In April, the number of active Instagram users globally reached 1.69 billion. India ranked first with the most active Instagram users, 388.3 million, while Indonesia ranked fourth with 102.15 million active users (We Are Social & Meltwater). Statistics on the growth of active Instagram users can be seen in Figure 1.

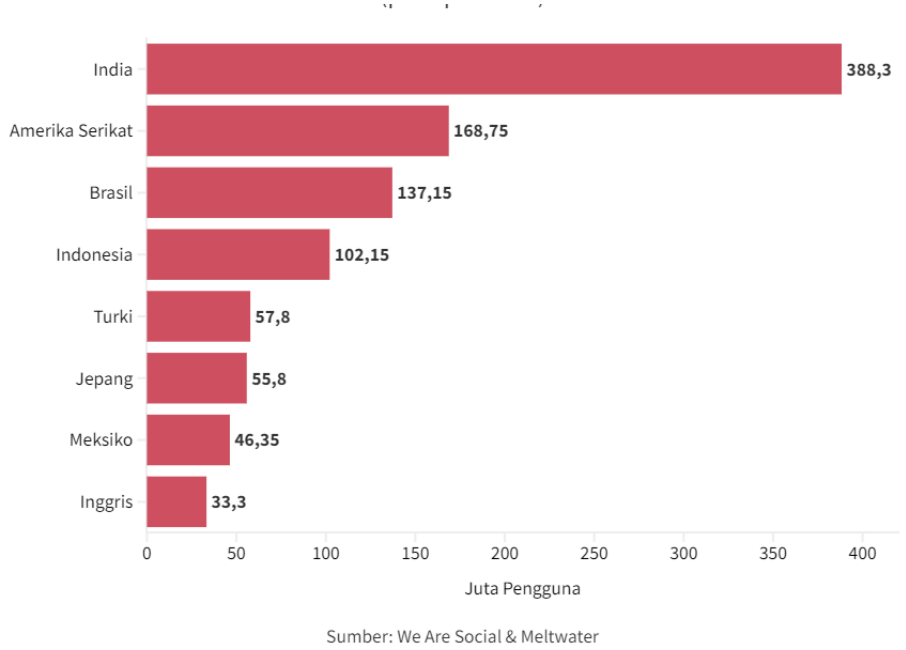

Figure 1. Statistics of Instagram users worldwide

Smartphones now possess capabilities equivalent to computers, making it easier for Instagram users to share photo, video, and communicate [15]. The Direct Message (DM) feature on Instagram Messenger facilitates personal interactions in text, images, videos, and temporary messages automatically deleted after viewing, enhancing user privacy [16]. Instagram has evolved into a dominant social media platform, playing a significant role in content distribution and the development of interpersonal interactions [17].

Instagram Messenger is similar to other Instant Messaging applications like WhatsApp and LINE, allowing for more personal communication among its users [18]. However, the increasing use of this feature also raises the risk of exploitation by irresponsible parties to commit cybercrimes. One potential crime is drug trafficking, where Instagram Messenger is used for drug transactions [19]. This activity can have negative consequences and is illegal, making it a criminal case that may need to be brought to court.

Based on the explanation provided, the need for forensic handling, especially mobile forensics, becomes crucial in solving drug trafficking cases that occur through social media platforms like Instagram. As the primary access tool for Instagram, smartphones store various types of digital data that can serve as evidence in investigations. Therefore, effective and accurate mobile forensic techniques are necessary to identify, collect, and analyze data from these devices. This helps reveal relevant evidence and ensures that the obtained data can be legally accountable in court.

Digital forensic analysis is crucial for uncovering and gathering electronic evidence for criminal investigations [20]. In the context of drug trafficking on Instagram Messenger, digital forensic analysis aims to identify, track, and analyze the digital footprints left by perpetrators on the social media platform [21], [22]. The National Institute of Standards and Technology (NIST) Framework provides a systematic and standardized methodology for conducting digital forensic analysis, ensuring the collected evidence is reliable and admissible in court [23].

Several previous studies comparing digital forensic tools on Instagram Messenger have been conducted using different approaches. One study used NIST to analyze two forensic tools, MOBILedit Forensic and Magnet Axiom Forensic. The results showed that both tools were less effective in recovering deleted text messages from smartphones but were successful in recovering image and video messages [24]. Research on acquiring digital evidence on Instagram Messenger based on Android has been conducted using the National Institute of Justice (NIJ) method. In this study, only one forensic tool, Oxygen Forensic, was used to collect and analyze smartphone digital evidence. The primary goal of this research was to evaluate the tool's effectiveness in recovering various types of relevant data as digital evidence, such as text messages, images, videos, and other information stored in the application [25]. Additionally, a study compared several digital forensic tools using the National Institute of Standards and Technology (NIST) method to analyze digital evidence from Instagram. This research used 12 samples of digital evidence to test the effectiveness of forensic tools, one of which was Belkasoft Evidence. The study found that Belkasoft Evidence had only a 50% accuracy rate in identifying and recovering digital evidence from Instagram Messenger [26].

Previous research comparing forensic tools for Instagram digital evidence on Android used the NIST method [27]. That research only involved the forensic tools OXYGEN and AXIOM Forensic MAGNET, and it relied solely on image and chat data, which demonstrated less accurate performance. Therefore, further development is needed using the same NIST method but with different tools: MOBILedit, Belkasoft, Mobile Forensic SPF, and Magnet Axiom. The development will also be enhanced by incorporating text chat data, images, audio, and image view once.

This research aims to compare the results from four forensic tools in acquiring digital evidence on Instagram in a drug trafficking case study. The study will focus on five data types in the digital evidence text chat, account, image, audio, and image view once. This research will ensure that relevant digital data can be identified by thoroughly analyzing each data type. The results are expected to serve as valid digital evidence admissible in court, providing a solid basis for legal proceedings in drug trafficking cases involving Instagram Messenger.

METHODS

This research used a case study simulation of drug trafficking employing the NIST method to analyze the Instagram Messenger application on smartphones. The study aims to compare the performance of four forensic tools, MOBILedit, Belkasoft, Mobile Forensic SPF, and Magnet Axiom, in locating digital evidence, such as messages and media files used in drug trafficking crimes. Figure 2 illustrates the NIST method and the stages of obtaining digital evidence.

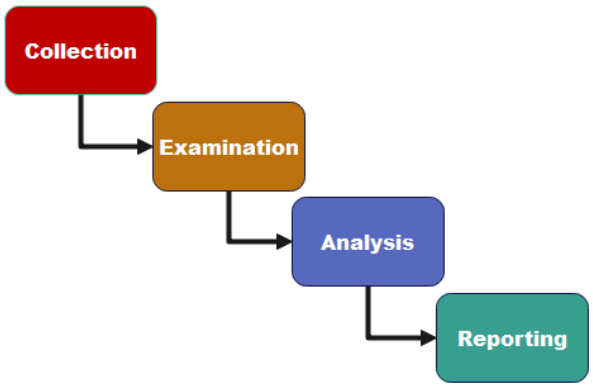

Figure 2. NIST method

Figure 2 NIST method in investigating evidence related to a drug trafficking case on Instagram Messenger. This framework guides the investigator through collecting, examination, analysis, and reporting digital evidence, ensuring a systematic and legally sound approach. The investigation maintains integrity and reliability by adhering to NIST standards, which is crucial for presenting findings in court.

1. The collection involves identifying and extracting evidence from smartphones, ensuring the data is secure and intact. This digital evidence is crucial for drug trafficking cases, as it maintains the integrity needed for legal proceedings, supporting the investigation's credibility and accuracy.
2. The examination stage involves forensic analysis and data collection from physical evidence, ensuring data integrity through automated and manual methods. This stage employs a forensic process using four different software tools, enhancing the accuracy and thoroughness of the investigation by providing diverse analytical capabilities.
3. After obtaining the digital files from the previous examination, a detailed and comprehensive analysis is performed using technically and legally appropriate methods. This process ensures the data provides strong evidence. The analyzed data is then considered digital evidence, scientifically and legally accountable for the case.
4. The reporting stage follows digital evidence acquisition and involves thorough analysis. At this stage, results are documented, detailing actions taken, tools and methods used, supporting actions identified, and recommendations for improving policies, procedures, tools, or other aspects of the digital forensic process.

In this case, the research object is the Instagram app. NIST is the agency responsible for developing standards and ensuring security. NIST holds authority in digital forensics, providing guidelines and protocols for investigating and analyzing digital evidence effectively and reliably [28], [29].

Research case scenario

This research focused on drug trafficking transactions that occur between dealers and users through the Instagram Messenger app. Figure 3 illustrates a conceptual simulation of the case, showing how the communication process occurs between the perpetrators and the victims in message exchanges.

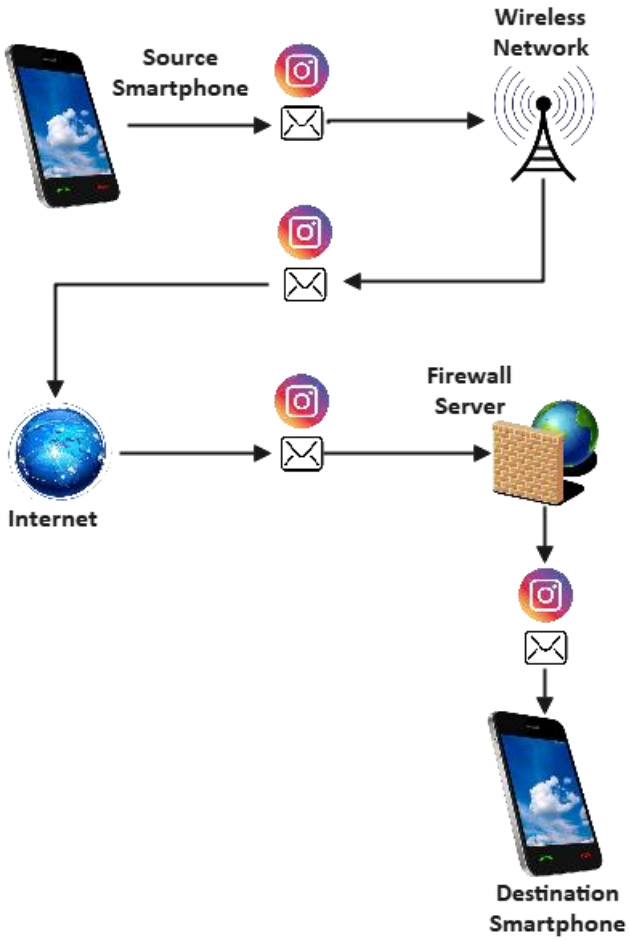

Figure 3. Research scenarios of drug trafficking cases

Two smartphone users are actively using the Instagram app, which is connected to the internet. In this scenario, drug dealers are exploiting the app to facilitate their illegal activities while avoiding detection by cyber police. The transactions take place through the chat feature in Instagram Messenger, where messages are first sent to Instagram Messenger's servers before being delivered to the intended users. As part of the investigation into this drug trafficking case, law enforcement will collect relevant data, including the transcripts of conversations between the drug dealers and their customers. These conversations have been stored in the Instagram database, allowing investigators to analyze the communication patterns and gather evidence against the perpetrators.

Comparison method

This research uses the index number calculation method to evaluate the performance of each forensic tool based on data obtained from the experiments conducted. In this process, Table 2 presents the results of the forensic tool performance evaluation (1).

$$Pon = \frac{\Sigma p_n}{\Sigma p_o} \; x \; 100\% \quad (1)$$

Information:
ΣPo = Refers to the result obtained from data acquisition
ΣPn = Represents the original data collected from a smartphone.
Pon = Indicates the expected percentage results [27].

RESULTS AND DISCUSSIONS

Collection

At this stage, the mobile device serves as physical evidence in the drug trafficking case, with digital evidence being considered as relevant parameters such as text chat, contacts, images, view-once images, and audio. Specific information related to the Oppo A37f smartphone can be seen in Figure 4.

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

Figure 4. Smartphone

The MOBILedit Forensic tool offers capabilities such as creating system backups and collecting smartphone data. It then extracts this data, as illustrated in Figure 5. This figure depicts the detailed process of evidence acquisition, highlighting how the tool systematically retrieves and secures digital information for forensic analysis.

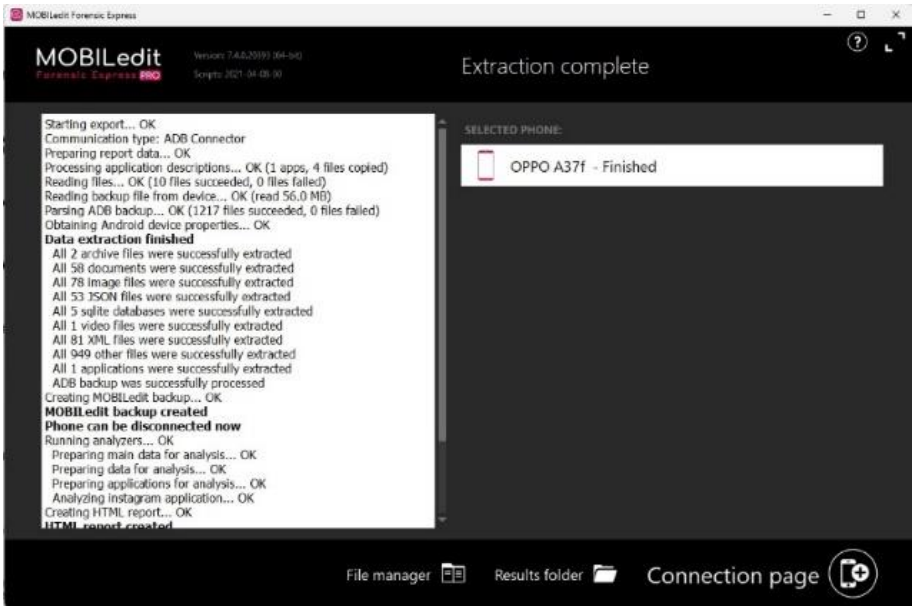

Figure 5. Evidence acquisition process using MOBILedit

Examination

In the examination phase of digital forensics, investigators meticulously analyze digital evidence collected through a scanning framework, executing specific actions during artifact acquisition. This stage is crucial as selecting and evaluating artifacts, like log records and databases from backup files, are pivotal for accurate results. Forensic tools, such as MOBILedit and Magnet Axiom, scrutinize and process evidence, extracting and analyzing various data types, including text conversations, account information, images, and audio files. Each piece of evidence undergoes a rigorous verification process using hash generator tools to confirm authenticity and detect alterations. Figures 6 and 7 illustrate evidence acquisition stages and results, ensuring digital evidence is accurately represented and reliable for investigative purposes.

Name	Date modified	Type
html_files	16/07/2024 15:39	File folder
pdf_files	16/07/2024 15:39	File folder
phone_files	16/07/2024 15:39	File folder
log_full	16/07/2024 15:39	Text Document
log_short	16/07/2024 15:39	Text Document
mobiledit_backup.xml	16/07/2024 15:39	XML File
Report	16/07/2024 15:39	Adobe Acrobat D...
report.ufdr	16/07/2024 15:39	UFDR File
report_configuration.cfg	16/07/2024 15:36	CFG File
Report_index	16/07/2024 15:39	Chrome HTML Do...
Report_long	16/07/2024 15:39	Chrome HTML Do...

Figure 6. Acquisition results of the MOBILedit application

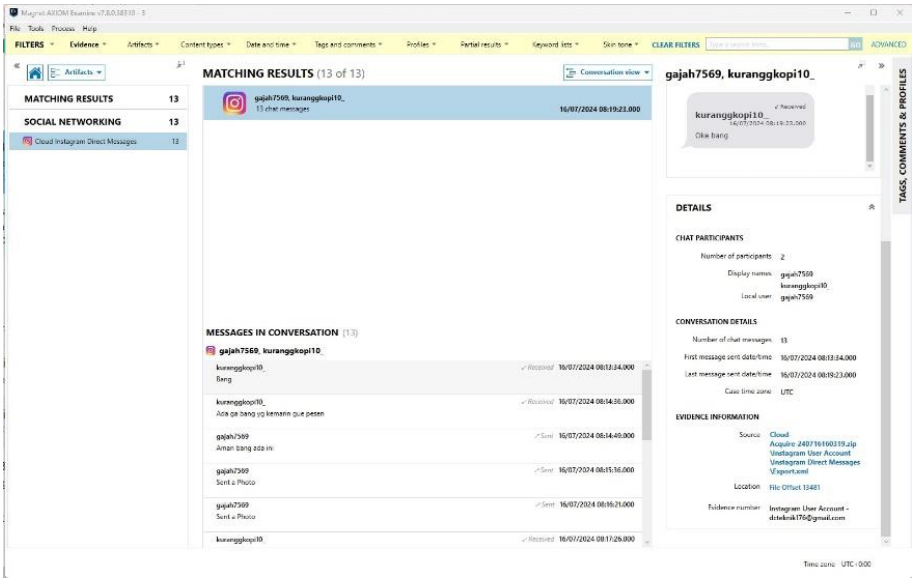

Figure 7. Acquisition of the magnet axiom application

The results from report.pdf identify the smartphone as an Oppo brand, providing detailed specifications. Additionally, other information, such as the time zone, IMEI, storage capacity, and more, is displayed in Figure 8, offering a comprehensive overview of the device's technical details and configuration.

Device Properties

Manufacturer	OPPO
Product	A37f
HW Revision	LMY47V
Platform	Android
SW Revision	5.1.1 (22)
Android ID	87a377b506382ef5
Serial Number	438d155
Device Time	2024-07-16 15:36:43 (UTC+7)
Manual Time	No
Time Zone	Asia/Jakarta
Manual Time Zone	No
Device Storage Encrypted	No
IMEI	864877032648772
Rooted	No
Communication Type	ADB Connector
SIM Card	Yes
IMSI	510092017102478
SIM Card Country	Indonesia
ICCID	89620922102191600624
Total Storage	10.8 GB
Used Storage	5.0 GB

Figure 8. Report smartphone

Table 1. Extraction results and evidence validation

Evidence	Directory	File Name	Hashing File
Text Chat	phone/applications0/com.instagram. android/backup/db/direct.db: 0x139ef	direct.db: 0x139ef	08e8fb083604c28b506 c807acc2d2d0b
Account	phone/applications0 /com.instagram.android/backup/sp /com.instagram.android_preferences.xml	com.instagram.android_ preferences.xml	4389bd5290394a64 17bdfb08dd7d21f5
Images	phone/applications0/ com.instagram.android/backup /f/pending_media_images/ pending_media_-555039710.jpg	pending_media_- 555039710.jpg	66ea35e0cc485435e 3760b45e4cff4e4
Audio	phone/applications0/com.instagram.android /backup/f/67629363470/clips/temp/ raw_karaoke_bleep.mp4	raw_karaoke_bleep.mp4	28b57fb6e880c395f934 66a9761d3c7a
Image view once			

Table 1 presents the results of extracting and validating digital evidence from the Instagram application on a smartphone. The evidence extracted included various data types, such as chats, account information, images, audio, and view-once media. These different types of data were obtained from specific directories within the device's file system, each associated with a unique file name. For instance, files like chats and account data are labelled accordingly, while media files such as images and audio have specific names that reflect their content. To ensure the integrity and authenticity of this evidence, each file was accompanied by a cryptographic hash. This unique hash identifier confirmed that the data remained unaltered throughout the process. Overall, the procedure documents and verifies the extracted digital evidence, ensuring its reliability and integrity in forensic analysis.

Analysis

In forensic investigations, the analysis involves extracting detailed data during the examination stage, following established protocols. Information is meticulously correlated to ensure adherence to research methods and simulations for gathering digital evidence. Investigators utilize four primary forensic applications MOBILedit Forensic, Magnet Axiom, Belkasoft, and Mobile Forensic SPF, to conduct their analyses. This process focuses on scrutinizing text data from conversations, account names, and evidence related to images, audio, and temporary image displays. Magnet Axiom is mainly instrumental in matching such evidence. All collected data is compiled into a comprehensive report designed to present findings clearly and understandably for individuals without technical expertise in digital forensics.

The analysis results of the Instagram application from report.pdf reveal the version used was 278.0.0.22.117, with a data size of 128.4 MB. Access permissions used to access the smartphone are detailed in Figure 9, providing a comprehensive overview of the application's specifications and permissions.

Instagram

Label	Instagram
Package	com.instagram.android
Version	278.0.0.22.117
Application Type	User Application
Installed by	com.android.vending
Application Size	233.7 MB
Data Size	128.4 MB
Cache Size	7.5 MB
APK File Extracted	Yes
APK Verification Successful	Yes
APK Verification Scheme	2
Best Certificate Found	Cert c56fb7d591ba6704df047fd98f535372fea00211, valid from 2012-02-08T01:41:31Z to 2112-01-15T01:41:31Z, Subject: C=US, ST=California, L=San Francisco, O=Instagram Inc, CN=Kevin Systrom, Issuer: C=US, ST=California, L=San Francisco, O=Instagram Inc, CN=Kevin Systrom
	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.GET_ACCOUNTS, android.permission.USE_CREDENTIALS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.FOREGROUND_SERVICE, android.permission.USE_FULL_SCREEN_INTENT, com.google.android.c2dm.permission.RECEIVE, android.permission.BLUETOOTH, android.permission.CAMERA, android.permission.READ_CONTACTS, android.permission.READ_PROFILE, android.permission.ACCESS_FINE_LOCATION, android.permission.RECORD_AUDIO, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.READ_EXTERNAL_STORAGE,

Figure 9. Instagram application

Table 2. Results of forensic analysis tools

Digital Evidence	Digital evidence obtained				Submitted Evidence
	MOBILedit Forensic	*Magnet Axiom*	*Belkasoft*	*Mobile Forensic SPF*	
Text Chat	34	42	0	32	56
Akun Instagram	1	1	1	1	1
Image	25	25	25	17	25
Audio	20	20	0	0	20
Image View Once	0	0	0	0	10
Percentage of Success	**62,5%**	**74,1%**	**23,2%**	**44,6%**	**100%**

Based on Table 2, the findings from digital evidence indicate that out of 56 text chats sent, 42 were successfully found using the Magnet Axiom tool, 34 were found using the MOBILedit tool, and 32 were found using Mobile Forensic SPF. All four forensic tools MOBILedit Forensic, Magnet Axiom, Belkasoft, and Mobile Forensic SPF, successfully identified the name of the Instagram account. A total of 25 image files were discovered by three tools: MOBILedit Forensic, Magnet Axiom, and Belkasoft, while Mobile Forensic SPF found only 17 image files. Regarding audio files, 20 were found using MOBILedit Forensic and Magnet Axiom, but Belkasoft and Mobile Forensic SPF discovered none. Additionally, no view-once image files were found by any of the tools due to the mobile device not being rooted, highlighting the limitations of the forensic tools. This comprehensive analysis underscores the varying capabilities of different forensic tools in uncovering digital evidence from smartphones.

This research revealed specific limitations of various forensic tools in reading or finding digital evidence. The MOBILedit Forensic tool had difficulties locating text chats and view-once images. Similarly, the Magnet Axiom tool was unable to find view-once image files. Belkasoft failed to detect text chats, audio files, and view-once images, while Mobile Forensic SPF could not find audio files and view-once images. The percentage of view-once digital evidence found was 0%. Despite these individual limitations, when comparing the overall evidence parameters found with the capabilities of the four tools used, the overall success rate was 100%. This indicates that while each tool has specific weaknesses in finding particular types of evidence, a higher success rate in forensic analysis depends on the combined capabilities of the forensic tools. The comparison of these forensic tools in terms of their effectiveness in uncovering digital evidence is detailed in Table 4, illustrating the strengths and weaknesses of each tool in the context of digital forensic investigations.

Table 3. Comparison results of forensic tools

Results	Forensic Tools			
	MOBILedit Forensic	*Magnet Axiom*	*Belkasoft*	*Mobile Forensic SPF*
Text Chat	found	found	not found	found
Account Instagram	found	found	not found	found
Image	found	found	found	found
Audio	found	found	found	not found
Image View Once	not found	not found	not found	not found

Based on Table 3, several indicators were used to evaluate forensic evidence tools in drug trafficking cases, revealing differences in the outputs of MOBILedit Forensic, Magnet Axiom, Belkasoft, and Mobile Forensic SPF. MOBILedit Forensic found evidence in Instagram account names, images, and audio, totaling 3 out of 5 pieces of digital evidence according to the case simulation parameters. Magnet Axiom identified 4 out of 5 pieces of evidence, while Belkasoft found only 2 of the five critical parameters. Mobile Forensic SPF discovered 3 of the five key pieces of evidence. Given these findings, the accuracy rates in acquiring evidence were 62.5% for MOBILedit Forensic, 74.1% for Magnet Axiom, 23.2% for Belkasoft, and 44.6% for Mobile Forensic SPF. This analysis highlights the varying effectiveness of these forensic tools in drug trafficking cases, emphasizing the importance of selecting the right tool for accurate digital evidence acquisition.

Reporting

The report evaluates evidence obtained from simulations using a non-rooted Oppo A37f cellphone, concluding that the forensic framework can still reveal digital evidence, such as text conversations,

Instagram account names, images, and audio related to drug trafficking. Table 5 compares the success of forensic tools MOBILedit Forensic, Magnet Axiom, Belkasoft, and Mobile Forensic SPF in finding this digital evidence, highlighting their varying effectiveness in uncovering critical information.

Table 5. Comparison of the success of forensic tools

Information	Evidence	Result
Oppo A37f	*Smartphone* Android	✓
Account name	gajah7569	✓
Conversation Time	-	✓
Chat Evidence File	56	✓
Image Evidence File	25	✓
Audio Evidence Files	20	✓
Image View Once Evidence File	10	-
Tools Forensic	*MOBILedit Forensic, Magnet Axiom, Belkasoft, dan Mobile Forensic SPF*	✓

A comparison of the performance of forensic tools on an unrooted Oppo A37f smartphone shows the following data restoration success rates: MOBILedit Forensic at 62,5%, Magnet Axiom at 74,1%, Belkasoft at 23,2%, and Mobile Forensic SPF at 44,6%. These results were obtained using a specific formula that evaluates the effectiveness of each tool in restoring digital evidence from the device, highlighting their varying capabilities in forensic investigations.

MOBILedit Forensic = $\frac{70}{112} \times 100\% = 62{,}5\%$

Magnet Axiom = $\frac{83}{112} \times 100\% = 74{,}1\%$

Belkasoft = $\frac{26}{112} \times 100\% = 23{,}2\%$

Mobile Forensic SPF = $\frac{50}{112} \times 100\% = 44{,}6\%$

CONCLUSION

Based on the investigation of drug trafficking cases using the Instagram application with the NIST framework, various tools such as MOBILedit Forensic, Magnet Axiom, Belkasoft, and Mobile Forensic SPF were used to obtain digital evidence such as text chat files, accounts, images, audio, and view-once images. The authenticity of the evidence can be verified through file hashing, and the success rate in finding evidence based on parameters was 100% according to the forensic tools' capabilities. The research results align with the research objectives. Investigators from this study found that the Magnet Axiom tool had the highest ability, with a success rate of 74.1%. However, the study had a limitation in that none of the four forensic tools used could find view-once images on the Instagram application. Suggestions for future research include expanding the data to improve the accuracy of digital evidence results, and it is recommended that the rooting process be conducted to obtain more accurate data.

ACKNOWLEDGEMENT

This research was supported by Directorate of Research, Technology, and Community Service Ministry of Education, Culture, Research and Technology, Indonesia under the Grant No. 107/E5/PG.02.00.PL/2024 0609.12/LL5-INT/AL.04/2024; 070/PTM/LPPM/UAD/VI/2024

REFERENCES

[1] M. Dweikat, D. Eleyan, and A. Eleyan, "Digital Forensic Tools Used in Analyzing Cybercrime," *J. Univ. Shanghai Sci. Technol.*, vol. 23, no. 3, pp. 367–379, 2021, doi: 10.51201/jusst12621.

[2] 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.

[3] N. AllahRakha, *Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations*, vol. 16, no. 2. 2024. doi: 10.22201/iij.24485306e.2024.2.18892.

[4] 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.

[5] A. S. Barkah, S. R. Selamat, and Z. Z. Abidin, "Comparative study of digital forensic investigation on cyber criminal," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 1.5 Special Issue, pp. 370–374, 2019, doi: 10.30534/ijatcse/2019/6081.52019.

[6] 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.

[7] R. M. Abou-Elzahab, M. F. Al, R. Taher, and T. Hamza, "Comparative Study of Different Mobile Forensic Tools for Extracting Evidence from Android Devices," *Mjcis*, vol. 16, no. 1, pp. 1–12, 2020.

[8] M. R. Al-Mousa *et al.*, "Examining Digital Forensic Evidence for Android Applications," *Proc. - 2022 23rd Int. Arab Conf. Inf. Technol. ACIT 2022*, pp. 1–8, 2022, doi: 10.1109/ACIT57182.2022.9994221.

[9] R. Padmanabhan, K. Lobo, M. Ghelani, D. Sujan, and M. Shirole, "Comparative analysis of commercial and open source mobile device forensic tools," *2016 9th Int. Conf. Contemp. Comput. IC3 2016*, pp. 1–6, 2017, doi: 10.1109/IC3.2016.7880238.

[10] F. GÜNEŞ ERİŞ and E. AKBAL, "Forensic Analysis of Popular Social Media Applications on Android Smartphones," *Balk. J. Electr. Comput. Eng.*, vol. 9, no. 4, pp. 386–397, 2021, doi: 10.17694/bajece.761271.

[11] H. Zhang, L. Chen, and Q. Liu, "Digital Forensic Analysis of Instant Messaging Applications on Android Smartphones," *2018 Int. Conf. Comput. Netw. Commun. ICNC 2018*, pp. 647–651, 2018, doi: 10.1109/ICCNC.2018.8390330.

[12] M. A. Mubarik, Z. Wang, Y. Nam, S. Kadry, and M. A. Waqar, "Instagram Mobile Application Digital Forensics," *Comput. Syst. Sci. Eng.*, vol. 37, no. 2, pp. 169–186, 2021, doi: 10.32604/csse.2021.014472.

[13] C. Femi-Adeyinka, N. A. Kose, T. Akinsowon, and C. Varol, "Digital Forensics Analysis of YouTube, Instagram, and TikTok on Android Devices: A Comparative Study," *12th Int. Symp. Digit. Forensics Secur. ISDFS 2024*, pp. 1–6, 2024, doi: 10.1109/ISDFS60797.2024.10527244.

[14] A. Menahil, W. Iqbal, M. Iftikhar, W. Bin Shahid, K. Mansoor, and S. Rubab, "Forensic Analysis of Social Networking Applications on an Android Smartphone," vol. 2021, 2021, doi: 10.1155/2021/5567592.

[15] D. Millatina, E. H. Gunawan, and B. Sugiantoro, "Forensic Analysis of WhatsApp, Instagram, and Telegram on Virtual Android Device," *12th Int. Symp. Digit. Forensics Secur. ISDFS 2024*, no. September 2023, pp. 1–4, 2024, doi: 10.1109/ISDFS60797.2024.10527308.

[16] C. Alisabeth and Y. R. Pramadi, "Forensic analysis of instagram on Android," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1007, no. 1, 2020, doi: 10.1088/1757-899X/1007/1/012116.

[17] V. Mishra, V. Singh, S. Kashyap, V. Kumar Sharma, V. Mishra Vivek Singh Sakshi, and V. Kumar Sharma Professor, "Investigating the Performance of Messenger App Security for WhatsApp , Facebook and Instagram Among Indian Users," 2023.

[18] S. Abd Elmonsef Sarhan, H. A. Youness, and A. M. Bahaa-Eldin, "A framework for digital forensics of encrypted real-time network traffic, instant messaging, and VoIP application case study," *Ain Shams Eng. J.*, vol. 14, no. 9, p. 102069, 2023, doi: 10.1016/j.asej.2022.102069.

[19] M. Hachem, R. Mizouni, I. M. Alawadhi, and M. J. Altamimi, "Digital forensic intelligence for illicit drug analysis in forensic investigations," *iScience*, vol. 26, no. 10, p. 108023, 2023, doi: 10.1016/j.isci.2023.108023.

[20] 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.

[21] W. Barkem and J. Sidabutar, "Digital Forensic Analysis of WhatsApp Business Applications on Android-Based Smartphones Using NIST," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 22, no. 3, pp. 615–626, 2023, doi: 10.30812/matrik.v22i3.3033.

[22] J. Son, Y. W. Kim, D. Bin Oh, and K. Kim, "Forensic analysis of instant messengers: Decrypt Signal, Wickr, and Threema," *Forensic Sci. Int. Digit. Investig.*, vol. 40, p. 301347, 2022, doi: 10.1016/j.fsidi.2022.301347.

[23] D. Delija, G. Sirovatka, and M. Žagar, "Forensic Analysis of the NIST Hacking Case: Integrating Autopsy Tools and Artificial Intelligence in Teaching Digital Forensics," *2024 47th ICT Electron. Conv. MIPRO 2024 - Proc.*, pp. 1514–1519, 2024, doi: 10.1109/MIPRO60963.2024.10569327.

[24] H. Supardin, R. Satra, M. A. Asis, and M. F. Teng, "Comparison Analysis of Digital Forensic Tools

on Instagram Messenger using The National Institute of Standards and Technology (NIST) Method," *Bull. Soc. Informatics Theory Appl.*, vol. 6, no. 1, pp. 65–75, 2022, doi: 10.31763/businta.v6i1.534.

[25] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "1490-Article Text-2859-1-10-20190413," *Akuisisi Bukti Digit. Pada Instagram Messenger Berbas. Android Menggunakan Metod. Natl. Inst. Justice*, vol. 4, pp. 219–227, 2018.

[26] I. A. Rafiq, I. 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.

[27] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," vol. 5, no. 2, pp. 235–247, 2018.

[28] I. Fathur Rohman, N. Widiyasono, and R. Gunawan, "Simulasi Analisis Bukti Digital Aplikasi Skype Berbasis Android menggunakan NIST SP 800-101 R1," *J. Sustain. J. Has. Penelit. dan Ind. Terap.*, vol. 8, no. 1, pp. 38–47, 2019, doi: 10.31629/sustainable.v8i1.1156.

[29] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost-benefit analysis into the NIST cybersecurity framework via the gordon-loeb model," *J. Cybersecurity*, vol. 6, no. 1, pp. 1–8, 2020, doi: 10.1093/CYBSEC/TYAA005.