Mobile and Forensics
Vol. 7, No. 1, March 2025, pp. 1-11
ISSN: 2714-6685 (online), 2656-6257 (print)
DOI: http://dx.doi.org/10.12928/mf.v1i1.11307

ANALYSIS OF INSTAGRAM MESSAGES IN DRUG CASES USING NIST METHODS

[1,*]Muhammad Raihandaffa Dzikrianasa, [2]Eko Aribowo
[1,2]Industrial Technology Faculty, Universitas Ahmad Dahlan, Indonesia
[1,*]m.raihandaffa1@gmail.com, [2]ekoab@tif.uad.ac.id
[*]correspondence email

Abstract

The advancement of communication technology has had a significant impact on all levels of society, particularly through the use of social media platforms such as Instagram. However, this application also has negative impacts, including its misuse by criminals to facilitate the distribution of drugs, leading to transactions where anti-forensics measures are employed by sellers during conversations. This research utilizes the National Institute of Standards and Technology (NIST) method, which consists of the steps of collection, examination, analysis, and reporting. This method is applied to identify and uncover evidence in drug transaction cases on Instagram. The researchers focus on messages between buyers and sellers, whether they have been deleted or not. The results of the study indicate that digital forensic steps using the NIST method can be applied in the process of retrieving digital evidence from the Instagram application on the smartphones of buyers and sellers. The digital forensic tools used successfully revealed relevant digital evidence on the Instagram application.
Keywords: Digital Forensics, Mobile Forensics, National Institute of Standards and Technology (NIST), Instagram

INTRODUCTION

The advancement of communication technology has had a significant impact on all levels of society, and some aspects have changed the way people live [1]. One of the most notable technological advancements is the emergence of smartphones, devices used for various purposes by their users [1]. With the wide range of available features, smartphones can also be used as tools for cybercrime [1]. When a narcotics user utilizes a smartphone, they use social media to purchase illegal goods.

Instagram is a photo and video sharing service owned by the American company Meta Platforms [2]. However, this platform is also used as a venue for drug transactions. Dealers openly sell drugs. Such crimes inevitably leave digital evidence, which is then used in court as reports of digital media crimes [3]. Digital forensics has emerged as a high-tech field or science and technology of crime detection to obtain digital evidence that can be used against criminals [4].

Mobile forensics is a sub-discipline of digital forensics that aims to discover and analyze digital evidence related to cybercrime cases so that it can be legally proven [5]. Mobile device forensic examinations involve extracting forensic data from phones that can be used as evidence. Several studies have been conducted in recent years, aiming to perform mobile forensic analysis to collect valid digital evidence [6]. When choosing research approaches, studies, and models in digital forensics, it is essential to always consider the methods used and the quality standards followed [4]. Based on the above issues, this research will be conducted on a dummy case scenario, aiming to assist the mobile forensic process in resolving problems that occur in the media [7]. Cybercrime

Article History: *Received August 7, 2024; Revised Agust 12, 2024; Accepted January 20, 2025*

that violates the rules and norms of society [8]. The handling of cybercrime cases is carried out through investigative activities known as digital forensics [9].
Digital forensic analysis is a crucial tool for law enforcement that can aid in identifying crimes potentially committed using digital information [10]. To address this issue, appropriate prevention and handling efforts are necessary. One method that can be used to obtain evidence is the National Institute of Standards and Technology (NIST) method [3]. The forensic process using the NIST steps includes collection, examination, analysis, and reporting [11]. NIST has a well-defined workflow for extracting digital forensic data [4]. And the process of acquisition and analysis using recognized and commonly used forensic tools, namely Belkasoft Evidence Center and MOBILedit Forensic Express [12].

METHODS

The stages of this research use the methodology shown in Figure 1 below:

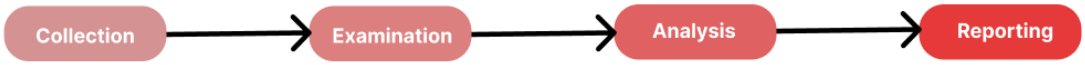


Fig 1 *National Institute of Standards and Technology Methodology*

This methodology is studied and developed to explain how the steps of this research are conducted to obtain further information about the systematically performed steps, which can serve as a guide to address the challenges of this research.

1. Collection
   At the stage of the collection process, the customer (informant) provides the investigator with a Xiaomi Redmi 4A smartphone. The next step is for the investigator to begin gathering additional evidence, if any, and to securely isolate all obtained evidence.
2. Examination
   In this step, the investigator begins the acquisition by imaging and recovering data from the smartphone using the digital forensic tool MOBILedit Forensic Express version 7.4.0.20393. During this process, the investigator will search for several text messages, images, and files needed for this case from the smartphone.
3. Analysis
   At this stage, the investigator will begin analyzing the results of the acquisition. This includes determining how many accounts, messages, and images appear on Instagram. Additionally, the investigator will check for any suspicious information, such as deleted text messages or images. The analysis will continue until the transaction and the delivery of the item to the buyer (informant) are identified.
4. Reporting
   At the reporting stage of the analysis results, the investigator describes the investigation conducted, explains the digital forensic tools used, outlines the sequence of steps taken, and determines the next actions to be performed. In the final investigation, the investigator provides suggestions and recommendations to improve procedures, forensic tools, policies, and other forensic aspects.

Scenario

In this study, a drug transaction case is simulated, involving a buyer who is also an informant and a suspected dealer communicating via the social media platform Instagram. The scenario starts with the pre-incident, followed by the incident, and then the post incident. The details are as follows.

1. Before The Incident
   Initially, there was a buyer who acted as an informant and opened the Instagram app. Then a notification appeared from an account requesting to follow the informant's account. The informant noticed the suspicious name of the account, so to find out more, the informant

accepted the friend request from that account and then followed it back. Shortly after, the informant's account received a friend request from that account.

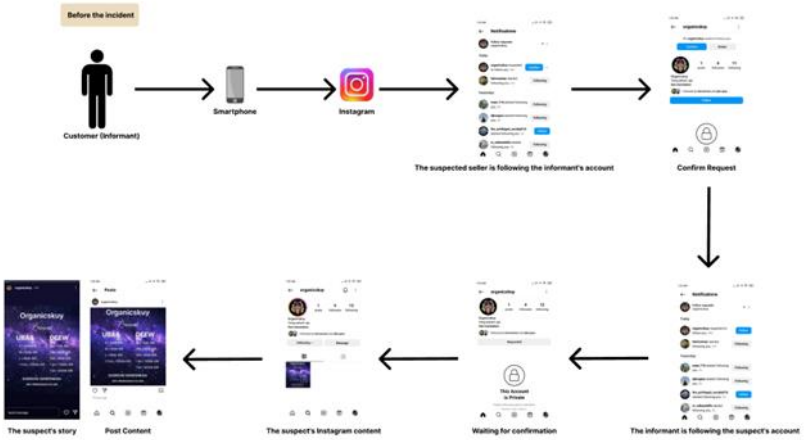


Fig 2 *A suspicious account is following the buyer's Instagram*

After that, the informant began to view the stories and posts from the suspected seller. From what the informant saw through the stories and posts, it increasingly indicated that the account was indeed involved in selling drugs.

2. Incident

In this part, the buyer (informant) views the seller's story posts. Then, the buyer inquires whether there is a discount package commonly referred to as "pahe." Shortly after, the seller responds that there is one and provides the price. The buyer then asks about the payment method, and eventually, a transaction occurs. The conversation continues until the seller sends an image, which is quickly deleted, increasing suspicion. Below is an image of the incident scenario as shown in Figure 3 Incident.

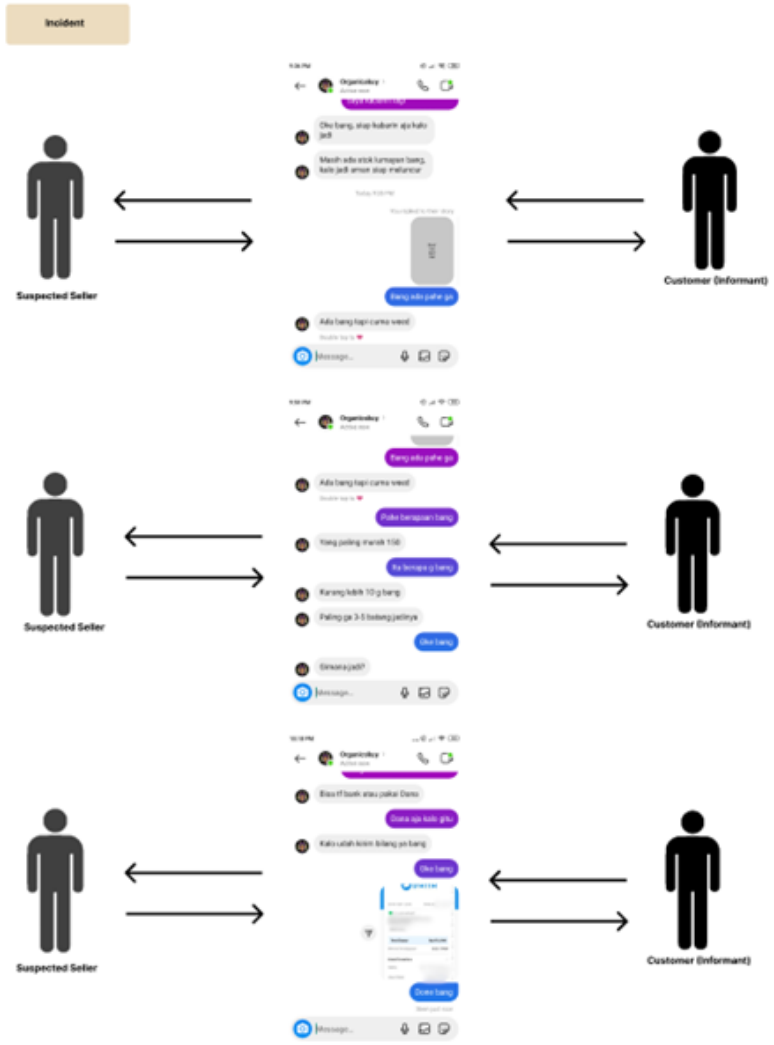


Fig 3 *Communication between a drug buyer and seller*

After a lengthy conversation between the buyer (informant) and the seller, the package eventually arrives, allowing the buyer (informant) to obtain the seller's address. Subsequently, an arrest is made by the authorities. Digital forensics is then conducted on both smartphones belonging to the buyer (informant) and the seller.

3. After The Incident

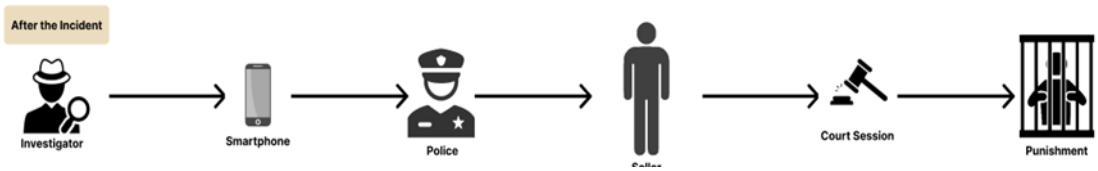


Fig 4 *The investigation process up to the applicable legal proceedings*

At this stage, the buyer will hand over the smartphone to the investigator, who will then conduct the investigation. After determining that the account indeed engaged in anti-forensic activities, which further clarified the indications of drug trafficking, the investigator eventually obtains the seller's smartphone. The seller's smartphone is then acquired, and a digital forensic process is conducted to obtain evidence. Finally, the trial process concludes,

and if the decision is made to impose a prison sentence, the seller will be placed in detention according to the legal ruling.

RESULT AND DISCUSSIONS

In this chapter, we discuss the analysis and discussion of a drug trafficking case on the social media platform Instagram, where the seller performed several anti-forensic actions. Through the application of the NIST methodology, forensic analysis can be conducted to deeply understand how sensitive information that has undergone anti-forensic measures can be recovered. The results of this analysis will be presented from two perspectives, namely from the buyer's side and the seller's side, to obtain valid evidence.

1. Collection

   Collection is the initial stage in the NIST framework. At this stage, the investigator will collect and document the evidence obtained. In this study, the evidence used is a gold Xiaomi Redmi 4A smartphone. The evidence was obtained from the buyer (informant) and handed over to the investigator. After collecting the physical evidence, the investigator will proceed with the documentation process to record the specifications, brand, model, IMEI, and other details related to the smartphone.

Fig 5 *Smartphone*

The specifications of the smartphone, which serves as evidence, are documented for record-keeping purposes. Table 1 is the smartphone specifications table. This table details everything from the smartphone model to its weight.

Table 1 Spesifikasi

Model	Xiaomi Redmi 4A (Rooted)
Chipset	Qualcomm Snapdragon 425 1.40 GHz
CPU	Quad-core Max 1.40 Ghz
GPU	Adreno 308
RAM	2 GB
Versi Android	7.1.2 (*Nougat*)
Memori Internal	16 GB
MIUI Version	MIUI Global 10.2.3
Warna	Gold
IMEI 1	865407038971868
IMEI 2	865407038971876
Berat	131 g

After completing the documentation process, the next step is to isolate the smartphone to prevent anything that could compromise the integrity of the physical or digital evidence.

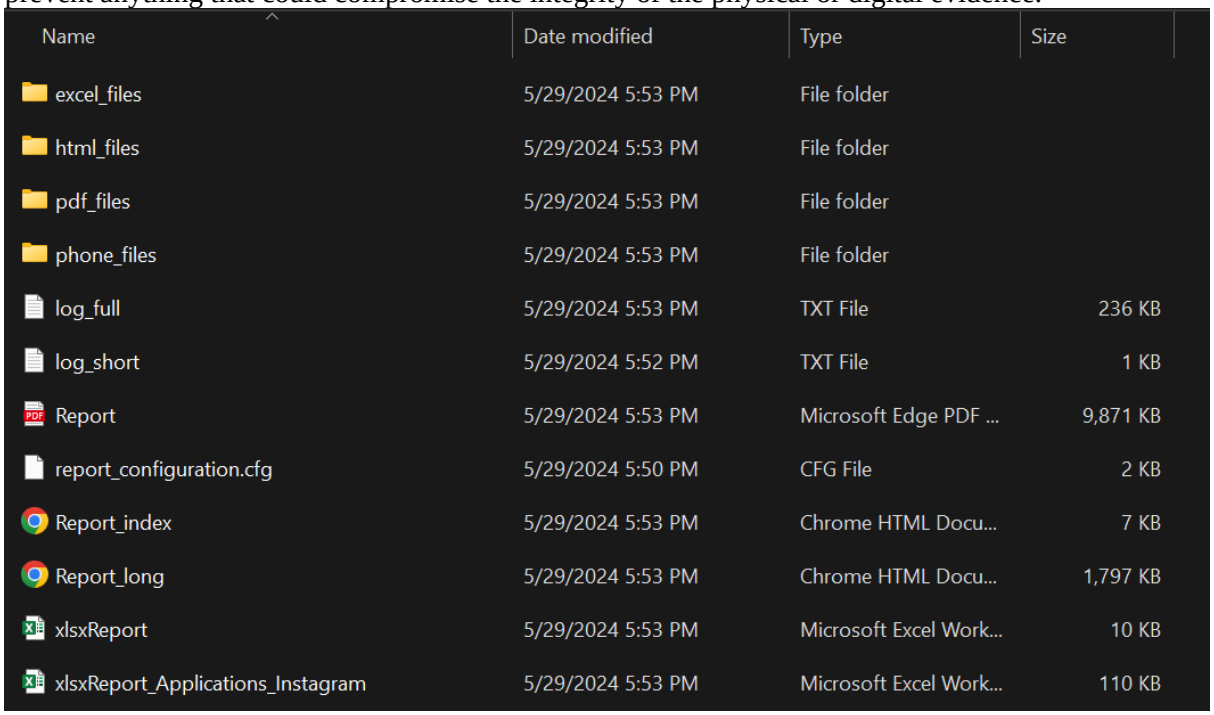


Fig 6 *Smartphone Acquisition Results*

The directory phone_files\phone\applications0 in Figure 1 contains a folder named "com.instagram.android," which holds detailed data about the Instagram application. This folder includes comprehensive information on the application's activities, settings, and related data installed on the smartphone. Further investigation of the contents within this folder can provide deep insights into the use of the application by the smartphone's owner during the relevant period of the investigation.

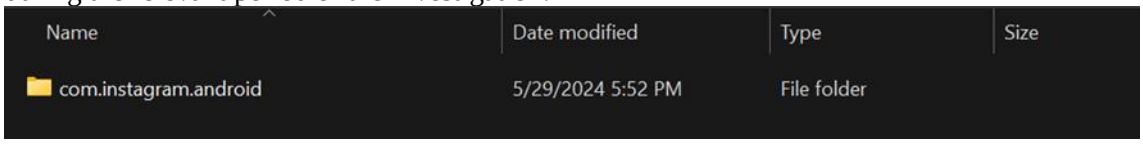


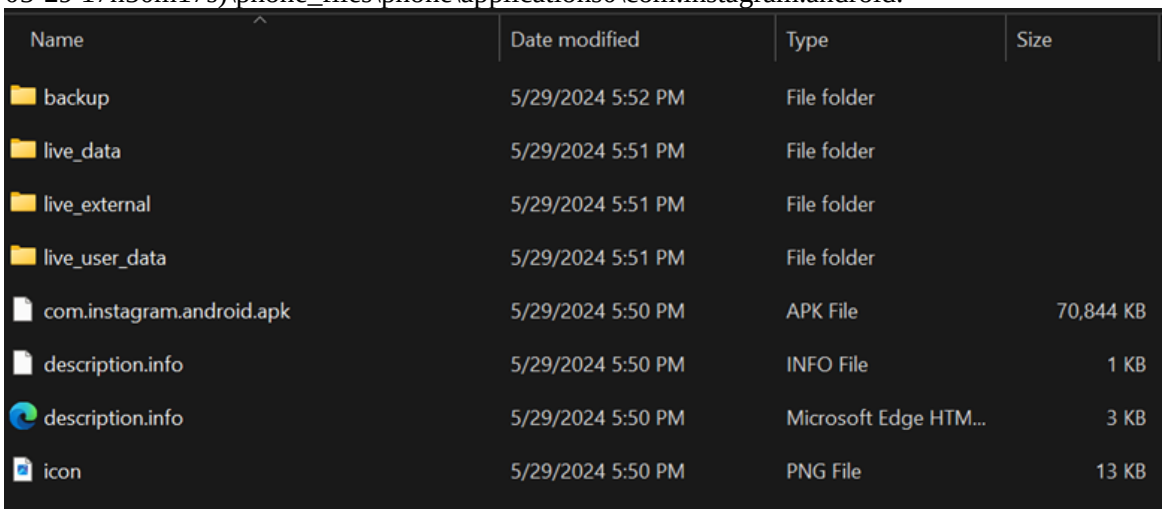
Fig 7 *Details of the phone_files Directory*

In digital forensics, the phone_files directory is crucial for uncovering and analyzing data stored on a smartphone. This directory typically contains various subdirectories and files that provide insight into the device's data structure and contents. Forensic investigators carefully

examine these directories to retrieve relevant information, such as application data, system logs, and user files. By analyzing the phone_files directory, forensic experts can reconstruct events, identify anomalies, and provide valuable evidence for investigations, ensuring that the digital evidence remains intact and reliable.

2. Examination

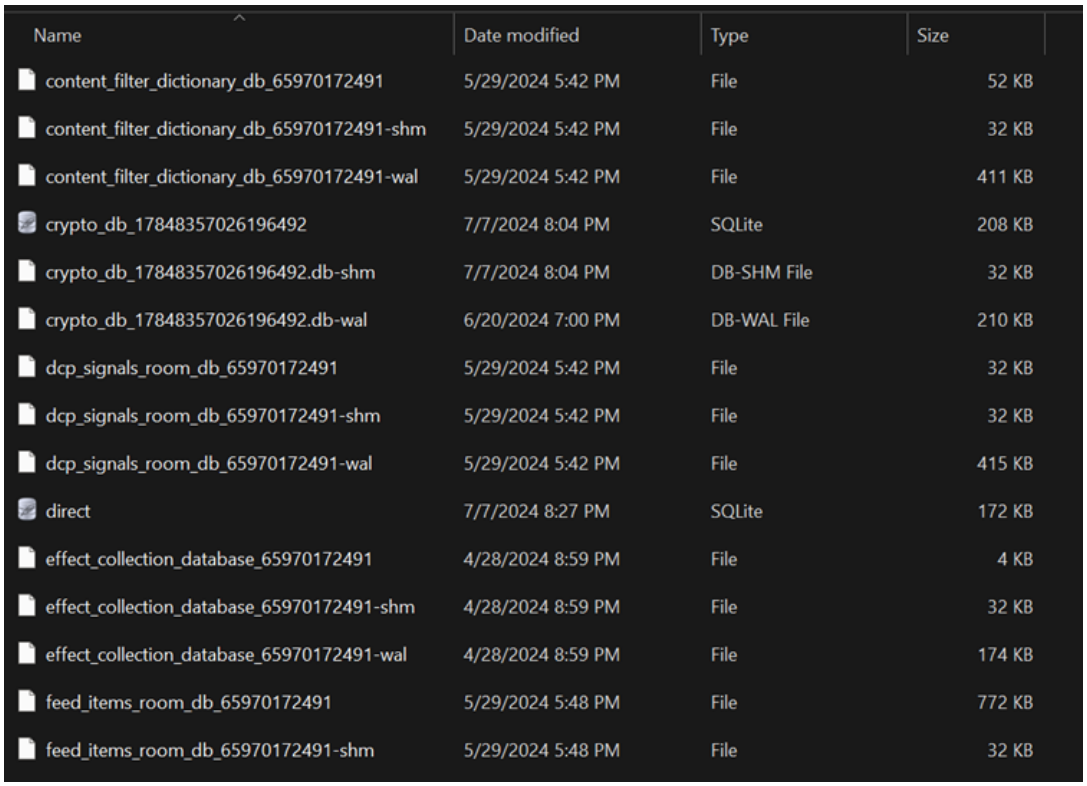
In the Examination process, which is the second stage in the NIST framework, the focus is on analyzing the data obtained during the Collection stage, which was performed using MOBILEdit Forensic Express. At this stage, the investigator begins to search for and extract important information while preserving the integrity of the data. The smartphone acquisition results are stored in the folder Xiaomi Redmi 4A (2024-05-29 17h50m17s). The data to be further investigated is related to Instagram from the Instagram application. Instagram data is located in the directory D:\MOBILedit Forensic Express Report\Xiaomi Redmi 4A (2024-05-29 17h50m17s)\phone_files\phone\applications0\com.instagram.android.



Name	Date modified	Type	Size
backup	5/29/2024 5:52 PM	File folder	
live_data	5/29/2024 5:51 PM	File folder	
live_external	5/29/2024 5:51 PM	File folder	
live_user_data	5/29/2024 5:51 PM	File folder	
com.instagram.android.apk	5/29/2024 5:50 PM	APK File	70,844 KB
description.info	5/29/2024 5:50 PM	INFO File	1 KB
description.info	5/29/2024 5:50 PM	Microsoft Edge HTM...	3 KB
icon	5/29/2024 5:50 PM	PNG File	13 KB

Fig 8 *Instagram Application Folder Structure*

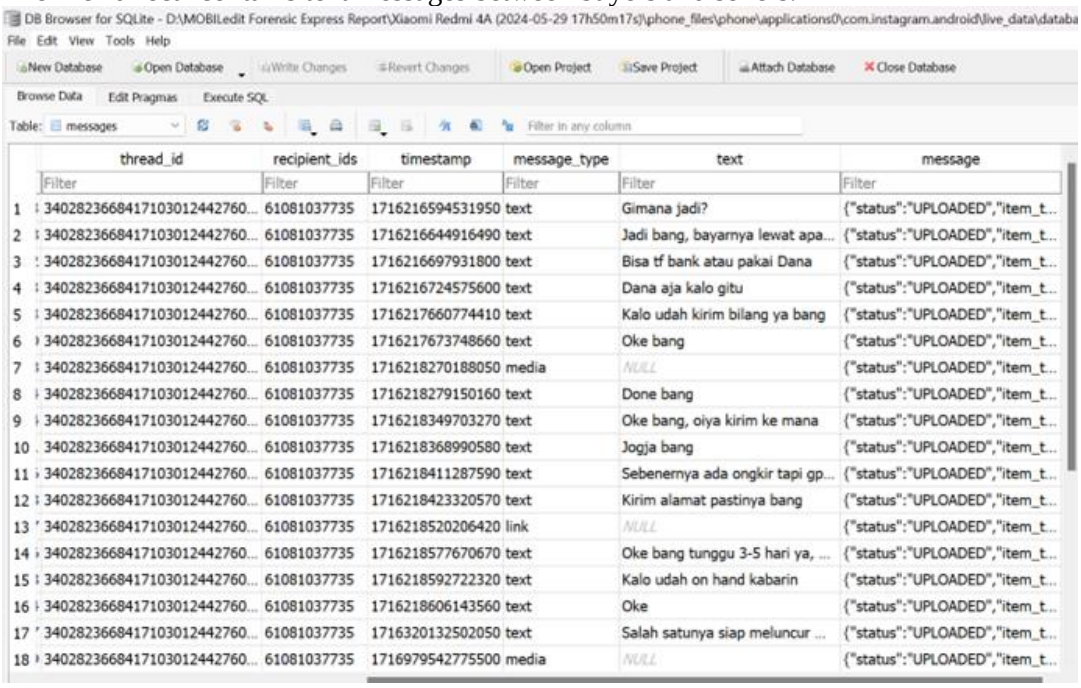
Figure 8 shows the folder structure of D:\MOBILedit Forensic Express Report\Xiaomi Redmi 4A (2024-05-29 17h50m17s)\phone_files\phone\applications0\com.instagram.android. There is a folder named "live_data" which stores data from the Instagram application, containing various types of data ranging from databases to application caches from the smartphone.



Name	Date modified	Type	Size
content_filter_dictionary_db_65970172491	5/29/2024 5:42 PM	File	52 KB
content_filter_dictionary_db_65970172491-shm	5/29/2024 5:42 PM	File	32 KB
content_filter_dictionary_db_65970172491-wal	5/29/2024 5:42 PM	File	411 KB
crypto_db_17848357026196492	7/7/2024 8:04 PM	SQLite	208 KB
crypto_db_17848357026196492.db-shm	7/7/2024 8:04 PM	DB-SHM File	32 KB
crypto_db_17848357026196492.db-wal	6/20/2024 7:00 PM	DB-WAL File	210 KB
dcp_signals_room_db_65970172491	5/29/2024 5:42 PM	File	32 KB
dcp_signals_room_db_65970172491-shm	5/29/2024 5:42 PM	File	32 KB
dcp_signals_room_db_65970172491-wal	5/29/2024 5:42 PM	File	415 KB
direct	7/7/2024 8:27 PM	SQLite	172 KB
effect_collection_database_65970172491	4/28/2024 8:59 PM	File	4 KB
effect_collection_database_65970172491-shm	4/28/2024 8:59 PM	File	32 KB
effect_collection_database_65970172491-wal	4/28/2024 8:59 PM	File	174 KB
feed_items_room_db_65970172491	5/29/2024 5:48 PM	File	772 KB
feed_items_room_db_65970172491-shm	5/29/2024 5:48 PM	File	32 KB

Fig 9 *Contents of the Instagram Databases Folder*

Figure 9 shows the contents of the Instagram database folder from the directory D:\MOBILedit Forensic Express Report\Xiaomi Redmi 4A (2024-05-29 17h50m17s)\phone_files\phone\applications0\com.instagram.android\live_data\databases. The file "direct" contains text messages between buyers and sellers.



DB Browser for SQLite - D:\MOBILedit Forensic Express Report\Xiaomi Redmi 4A (2024-05-29 17h50m17s)\phone_files\phone\applications0\com.instagram.android\live_data\databa

File Edit View Tools Help

New Database | Open Database | Write Changes | Revert Changes | Open Project | Save Project | Attach Database | Close Database

Browse Data | Edit Pragmas | Execute SQL

Table: messages | Filter in any column

	thread_id	recipient_ids	timestamp	message_type	text	message
1	340282366841710301244276...	61081037735	1716216594531950	text	Gimana jadi?	{"status":"UPLOADED","item_t...
2	340282366841710301244276...	61081037735	1716216644916490	text	Jadi bang, bayarnya lewat apa...	{"status":"UPLOADED","item_t...
3	340282366841710301244276...	61081037735	1716216697931800	text	Bisa tf bank atau pakai Dana	{"status":"UPLOADED","item_t...
4	340282366841710301244276...	61081037735	1716216724575600	text	Dana aja kalo gitu	{"status":"UPLOADED","item_t...
5	340282366841710301244276...	61081037735	1716217660774410	text	Kalo udah kirim bilang ya bang	{"status":"UPLOADED","item_t...
6	340282366841710301244276...	61081037735	1716217673748660	text	Oke bang	{"status":"UPLOADED","item_t...
7	340282366841710301244276...	61081037735	1716218270188050	media	NULL	{"status":"UPLOADED","item_t...
8	340282366841710301244276...	61081037735	1716218279150160	text	Done bang	{"status":"UPLOADED","item_t...
9	340282366841710301244276...	61081037735	1716218349703270	text	Oke bang, oiya kirim ke mana	{"status":"UPLOADED","item_t...
10	340282366841710301244276...	61081037735	1716218368990580	text	Jogja bang	{"status":"UPLOADED","item_t...
11	340282366841710301244276...	61081037735	1716218411287590	text	Sebenernya ada ongkir tapi gp...	{"status":"UPLOADED","item_t...
12	340282366841710301244276...	61081037735	1716218423320570	text	Kirim alamat pastinya bang	{"status":"UPLOADED","item_t...
13	340282366841710301244276...	61081037735	1716218520206420	link	NULL	{"status":"UPLOADED","item_t...
14	340282366841710301244276...	61081037735	1716218577670670	text	Oke bang tunggu 3-5 hari ya, ...	{"status":"UPLOADED","item_t...
15	340282366841710301244276...	61081037735	1716218592722320	text	Kalo udah on hand kabarin	{"status":"UPLOADED","item_t...
16	340282366841710301244276...	61081037735	1716218606143560	text	Oke	{"status":"UPLOADED","item_t...
17	340282366841710301244276...	61081037735	1716320132502050	text	Salah satunya siap meluncur ...	{"status":"UPLOADED","item_t...
18	340282366841710301244276...	61081037735	1716979542775500	media	NULL	{"status":"UPLOADED","item_t...

Fig 10 *Messages Contained in the Instagram Direct File*

Figure 10 represents a deeper investigation conducted on the "direct" file from the buyer's smartphone using the DB Browser for SQLite tool. There are several types of messages in the conversation between the buyer and the seller that include media and links.

3. Analysis

The third stage in the NIST framework is the analysis process of digital evidence obtained from the examination stage. This analysis aims to identify and collect relevant digital evidence that can support the case under investigation, ensuring that the evidence can be used in court proceedings.

Time	User	Chat	Status
20 Mei 2024, 21.49	Organicskuy (Penjual)	Gimana jadi?	Tersedia
20 Mei 2024, 21.50	Bagus Setiadi (Pembeli/Cepu)	Jadi bang, bayarnya lewat apa bang?	Tersedia
20 Mei 2024, 21.51	Organicskuy (Penjual)	Bisa tf bank atau pakai Dana	Tersedia
20 Mei 2024, 21.52	Bagus Setiadi (Pembeli/Cepu)	Dana aja kalo gitu	Tersedia
20 Mei 2024, 22.07	Organicskuy (Penjual)	Kalo udah kirim bilang ya bang	Tersedia
20 Mei 2024, 22.07	Bagus Setiadi (Pembeli/Cepu)	Oke bang	Tersedia
20 Mei 2024, 22.17	Bagus Setiadi (Pembeli/Cepu)		Null
20 Mei 2024, 22.17	Bagus Setiadi (Pembeli/Cepu)	Done bang	Tersedia
20 Mei 2024, 22.19	Organicskuy (Penjual)	Oke bang, oiya kirim ke mana	Tersedia
20 Mei 2024, 22.19	Bagus Setiadi (Pembeli/Cepu)	Jogja bang	Tersedia
20 Mei 2024, 22.20	Organicskuy (Penjual)	Sebenernya ada ongkir tapi gpp kali ini ada diskon khusus free ongkir	Tersedia
20 Mei 2024, 22.20	Organicskuy (Penjual)	Kirim alamat pastinya bang	Tersedia
20 Mei 2024, 22.22	Bagus Setiadi (Pembeli/Cepu)		Null
20 Mei 2024, 22.22	Organicskuy (Penjual)	Oke bang tunggu 3-5 hari ya, habis ini langsung packing	Tersedia
20 Mei 2024, 22.23	Organicskuy (Penjual)	Kalo udah on hand kabarin	Tersedia
20 Mei 2024, 22.23	Bagus Setiadi (Pembeli/Cepu)	Oke	Tersedia
22 Mei 2024, 02.35	Organicskuy (Penjual)	Salah satunya siap meluncur bang	Tersedia
29 Mei 2024, 17.45	Bagus Setiadi (Pembeli/Cepu)		Null
29 Mei 2024, 17.47	Bagus Setiadi (Pembeli/Cepu)	Oh hand bang, sorry baru sempet kabarin	Tersedia
29 Mei 2024, 17.48	Organicskuy (Penjual)	Oke siap bang	Tersedia

Fig 11 *Conversations Obtained on the Smartphone*

Figure 11 shows the conversation results between the buyer and seller on the platform, analyzed from the seller's smartphone. This conversation includes various messages sent and received by both parties. In this analysis, it is evident that some messages have a null status. This null status indicates that these messages are not regular text but contain media such as images, videos, or links to external sources. On the other hand, an available status indicates messages that can be read by forensic tools because they are in text form.

Fig 12 *Deleted Image Messages from the Seller*

Figure 12 shows image messages that have been deleted by the seller, as well as some image messages still present in the conversation between the buyer and the seller. In this analysis, the image img_5751 represents a message deleted by the seller because the image refers to a cache file located at https%253a%252f%252finstagram.fjog3-1.fna.fbcdn.net%252fv%252ft1.15752-

9%252f441432071_2119151978484484_1774265882646766731_n.jpg%253fstp=dst-jpg_e15&ccb=1-7_-1_-1. Despite its deletion, the digital footprint of these messages can still be found and analyzed. The deleted image message may contain important information that the seller did not want to be visible or known to others.

4. Reporting
   The reporting stage involves documenting the results of the analysis that has been performed. This stage includes a description of the case, the forensic methodology used, the techniques and forensic tools employed, and any procedures, guidelines, devices, actions, and other relevant aspects. This stage also covers a summary of the smartphone used, in accordance with the forensic procedures conducted with the forensic tools employed. Each piece of evidence, such as the smartphones used, will be reported.

Table 2 Number of Artifacts Obtained

No	Application	Artifact	Acquisition Result
1.	Buyer's Instagram	Account	1
		Message	20
		Image	4
2.	Seller's Instagram	Account	1
		Message	20
		Image	4

The examination followed specific procedures, including acquiring smartphones with signal blocking enabled, imaging them using MOBILedit Forensic Express, and analyzing Instagram data with the same tool. The analysis uncovered various digital artifacts, which are summarized in Table 2 This table lists the number of artifacts recovered from each Instagram account, including user accounts, messages, and images, showing the extent of data retrieved from both the buyer's and seller's smartphones.

CONCLUSIONS

The digital forensic analysis conducted on the Xiaomi Redmi 4A smartphones, which served as physical evidence in this investigation, yielded valid and reliable results in retrieving digital evidence from the Instagram application. The analysis followed the National Institute of Standards and Technology (NIST) methodology, successfully extracting accounts, messages, and images from both the buyer's and seller's devices. The forensic tool, MOBILedit Forensic Express version 7.4.0.20393, demonstrated its capability to effectively analyze Instagram data, identifying one account, 20 message, and images for both the buyer and seller.

REFERENCES

[1] Riya Majalista and Tata Sutabri, "Smartphone Data Search Analysis Using NIST for Digital Forensic Investigation," J. Inform. Teknol. dan Sains, vol. 5, no. 1, pp. 81–85, 2023, doi: 10.51401/jinteks.v5i1.2200.

[2] W. Prihatiningsih, "Motives for Using Social Media Instagram Among Teenagers," Communication, vol. 8, no. 1, p. 51, 2017, doi: 10.36080/comm.v8i1.651.

[3] R. A. Bintang, R. Umar, and A. Yudhana, "Analysis of Facebook Lite Social Media with Forensic Tools using the NIST Method," Techno (Journal of the Faculty of Engineering, University of Muhammadiyah Purwokerto), vol. 21, no. 2, p. 125, 2020, doi: 10.30595/techno.v21i2.8494.

[4] R. Bramesta Kusumadewa and Z. Sari, "Comparative Analysis of Forensic Digital Evidence on Android Smartphone based Instant Messaging Using NIST Framework," *REPOSITOR*, vol. 4, no. 3, pp. 407–422, 2022.

[5] D. Mualfah, Muhammad Iqbal Syam, and Baidarus, "Comparison Analysis of Mobile Forensic Tools Using the National Institute of Justice (NIJ) Method," J. CoSciTech

(Computer Science and Information Technology), vol. 4, no. 1, pp. 283–292, May 2023, doi: 10.37859/coscitech.v4i1.4767.

[6] R. B. Kusumadewa and S. Syaifuddin, "Comparison Analysis of Digital Forensic Evidence on Android-Based Smartphone Instant Messaging using the NIST Framework," Seminar on Engineering, Professional Engineer Program, vol. 2, no. 1, pp. 1–11, 2022, doi: 10.22219/skpsppi.v3i1.5061.

[7] Jeki Kuswanto, Nur Asyifa, and I. Hadi Purwanto, "Acquisition of Google Drive on Android Using Oxygen and MOBILedit with the National Institute of Justice Method," J. Inform. Teknol. dan Sains, vol. 5, no. 1, pp. 141–147, 2023, doi: 10.51401/jinteks.v5i1.2523.

[8] S. P. F. W. Pratama, I. G. N. A. C. Putra, M. A. Hamid, C. Christian, and I. K. K. Merdana, "Digital Forensic Analysis of the Twitter Application on Android as Digital Evidence in Handling Online Prostitution Cases," JELIKU (Journal of Computer Science, Udayana), vol. 10, no. 3, p. 271, 2022, doi: 10.24843/jlk.2022.v10.i03.p03.

[9] N. Iman, A. Susanto, and R. Inggi, "Analysis of the Development of Digital Forensics in Cybercrime Investigation in Indonesia (Systematic Review)," J. Telekomun. dan Komput., vol. 9, no. 3, p. 186, 2020, doi: 10.22441/incomtech.v9i3.7210.

[10] M. Marzuki and T. Sutabri, "Forensic Analysis of Michat Social Media Using the Integrated Digital Forensic Investigation Framework (IDFIF)," Blantika Multidisciplinary Journal, vol. 2, no. 1, pp. 56–70, 2023, doi: 10.57096/blantika.v2i1.11.

[11] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *Natl. Inst. Stand. Technol.*, 2006.

[12] M. N. Fadillah, R. Umar, and A. Yudhana, "Forensic Analysis of Digital Wallet Applications on Android Smartphones Using the DFRWS Method," Kumpul. J. Ilmu Komput., vol. 9, no. 2, pp. 265–278, 2022.