ISSN 2614-0047


# Comparison Analysis of Digital Forensic Tools on Instagram Messenger using The National Institute of Standards and Technology (NIST) Method

Harno Supardin [a,1*], Ramdan Satra [a,2], Muh. Arfah Asis [a,3], Ming Foey Teng [b,4]

[a] Universitas Muslim Indonesia, Makassar, Indonesia
[b] American University of Sharjah, United Arab Emirates
[1] harnoshupardin@gmail.com ; [2] mailto.ramdan@umi.ac.id; [3] muh.arfah.asis@umi.ac.id; [4] mteng@aus.edu
* corresponding author

ARTICLE INFO

**Article history**
Received December 18, 2021
Revised January 18, 2022
Accepted February 3, 2022

**Keywords**
Digital Forensic Tools
Instagram Messenger
NIST Method

ABSTRACT

Technological developments from time to time are very rapid, one of which is the development of smartphones constantly evolving in operating systems, features, specifications, and applications. Today's increasingly sophisticated technology has become essential to people's lives. Some people's lives can be carried out by utilizing technology, including committing crimes in cyberspace. One of the most widely used social media applications is Instagram. Instagram messenger causes cybercrime, pornography, fraud, and cyberbullying. This study aims to compare the performance of digital forensic tools in obtaining digital evidence on Instagram messenger using the NIST Method. The results of this study indicate that MOBILedit Forensic and Magnet Axiom have the following accuracy results in restoring deleted data on Instagram messenger, MOBILedit Forensic 69.23% and Magnet Axiom 76.92%.



## 1. Introduction

Technological developments from time to time are very rapid, one of which is the development of smartphones constantly evolving in operating systems, features, specifications, and applications. Today's increasingly sophisticated technology has become essential to people's lives. Some activities in people's lives can be carried out using technology, including committing crimes. The increasingly sophisticated technology is not only used by the community to carry out positive activities, but many also take advantage of the greatness of technology to carry out negative actions that threaten technology users, especially regarding using cybercrime. In layman, cybercrime, known as the internet, has become an essential part of people's daily lives, which not only brings benefits but also threatens the security and human rights of its users. One of the most common threats is the threat of pornography. Users widely use Internet media to access pornographic content that is widespread in cyberspace [1].

Social media, such as Instagram, is the most widely used place by people using smartphones. Instagram is a combination of the words instant-telegram. From the use of the word, it can be interpreted as an application to send information quickly in the form of managing photos, sharing photos, and sharing other social networks [2]. Fig.1 is a graph of Instagram social media users who became the second row after Whatsapp in January 2022.

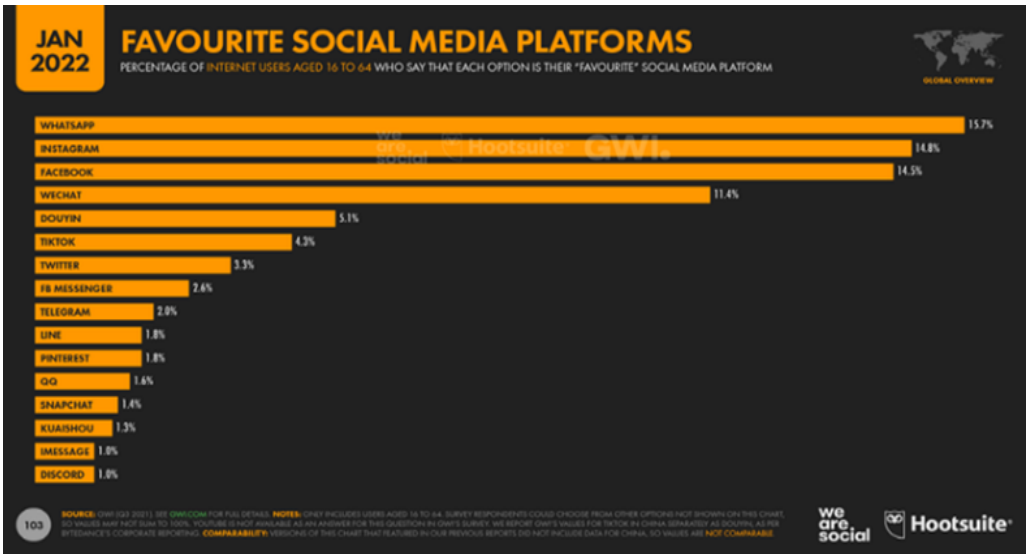


**Fig. 1.**Instagram Social Media User Graph

The graph above explains the development based on the global ad audience reach. Instagram had at least 1.478 billion users worldwide in January 2022. As for Instagram users in Indonesia in 2022, the figures published in the meta-advertising tool show that Instagram had 99.15 million users in Indonesia in 2018. early 2022 [3].

From the problem of cybercrime crime cases, there is a field of science that can assist in proving cybercrime cases, namely digital forensics in helping to solve pornographic crime cases through Instagram messenger social media with smartphone access media [4]. Digital forensics is the study of how to deal with various crimes involving computer technology [5].

The digital forensic analysis is carried out using the National Institute of Standards and Technology (NIST) method because it has superior work techniques and a structured forensic process that ensures investigators are accurate by systematically following research steps to justify the results. This method is widely used in digital crime cases [6].

Previous research conducted by Imam Riadi, Anton Yudhana, Muhamad Caesar Febriansyah Putra (2018) with the title "Analysis of Digital Evidence on Android-Based Instagram Messenger Using the National Institute of Justice (NIJ) Method" in this study took data on Instagram messenger from cyberbullying cases. Using the Oxygen Forensic tool with the NIJ method stages [7].

Then the research was conducted by Anton Yudhana, Imam Riadi, and Ikhwan Anshori (2018) titled "Analysis of Digital Evidence for Facebook Messenger Using the NIST Method". In this study, the tools used were Oxygen Forensic using the National Institute of Standards and Technology (NIST) method [8].

While this study will develop previous research using the NIST method and conduct testing using two forensic tools, MOBILedit Forensic, and Magnet Axiom Forensic, to better compare results from data on pornographic Instagram messengers in the form of text messages, images, and videos digital evidence under court.

Based on the above background, a study titled "Comparative Analysis of Digital Forensic Tools on Instagram Messenger Using the National Institute of Standards and Technology (NIST) Method" was conducted.

## 2. Method

This research uses the National Institute of Standards and Technology (NIST) method. This method describes how, step by step in detail and systematically, to solve existing problems. The stages of the NIST method are Collection, Examination, Analysis, and Reporting. The following are the forensic stages of the NIST method in Fig.2.

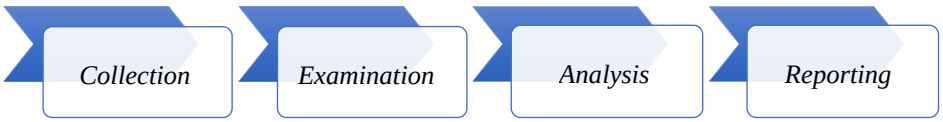


**Fig. 2.**Digital Forensic Stages of the NIST Method

### 2.1. Collection

The collection is the collection or identification of evidence used in the form of a smartphone whose data will be used as digital evidence of a pornographic crime case. This process is carried out by following data integrity security measures.

### 2.2. Examination

The examination is collecting data on evidence using trusted forensic tools so that the data obtained has high integrity.

### 2.3. Analysis

The analysis stage is the process of analyzing and re-evaluating the data found from the examination results.

### 2.4. Reporting

The reporting stage is the process of reporting the results of the analysis of digital evidence that has been found, which is used as the final report of the forensic process that has been carried out.

In this study, the research design used was a case study research design. While handling and analyzing digital evidence, researchers create a scenario of the activities on Instagram messenger, as in Fig.3.

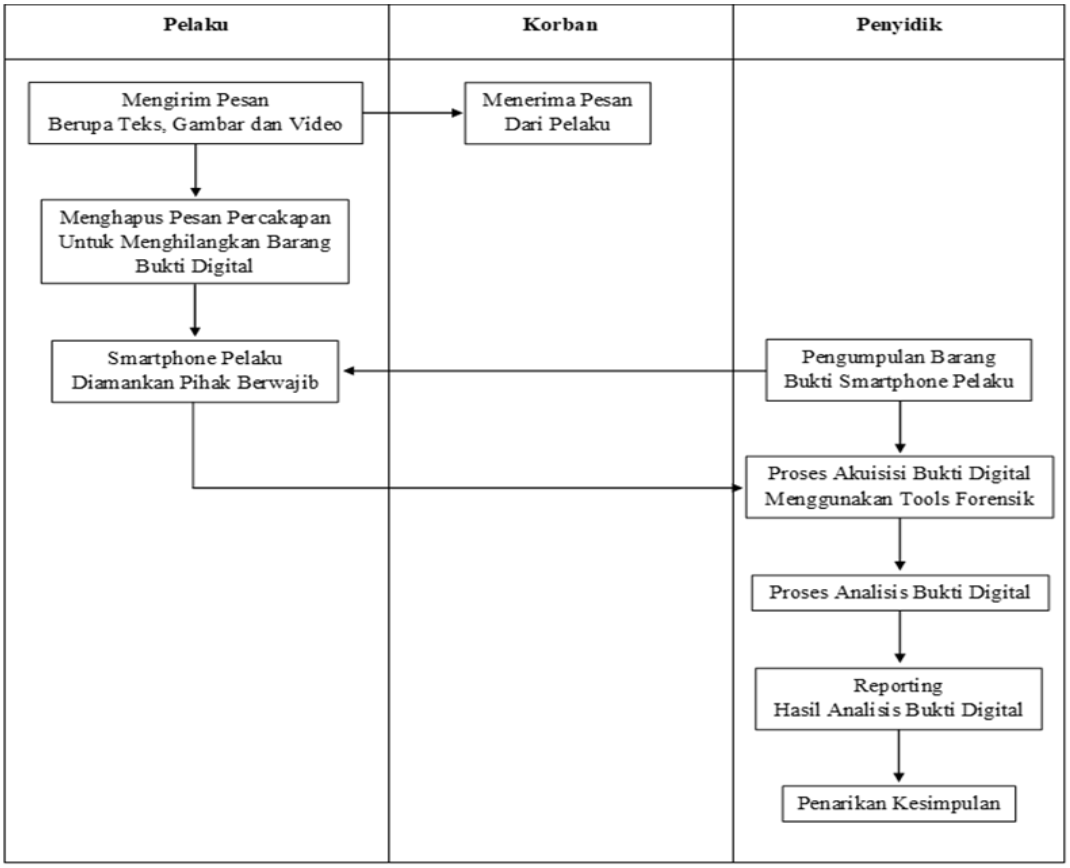


**Fig. 3.**Research Design

In the research design image above, the investigation was carried out from a case scenario of sending pornographic content from the suspect to the victim. In this process, the suspect sent pornographic content to the victim. After the suspect sent it to the victim, the suspect deleted the data from the communication device, namely the smartphone, to remove evidence. Using forensic tools, text messages, images, and videos deleted from Instagram messenger will be recovered from the perpetrator's device.

The acquisition was completed after the perpetrator's smartphone evidence was secured. The acquisition used forensic tools, namely MOBILedit Forensic and Magnet Axiom Forensic. Then the acquisition process results will be analyzed to make a report. Reports from the analysis results are in the form of data information that has been found, forensic methods carried out, and forensic tools used. The conclusion stage in this study is the accuracy of each forensic tool based on digital evidence obtained using the NIST method and forensic procedures performed.

## 3. Results and Discussion

### 3.1. Collection

At this stage, the Xiaomi Redmi Note 7 smartphone is secured for investigation so that the data does not change before being analyzed. Smartphone evidence and specifications can be seen in Fig.4 and Table 1.

**Fig. 4.**Smartphone

**Table.1** Specifications

| Model Perangkat | Redmi Note 7 |
|---|---|
| Ram | 4,00 |
| Versi Android | 10 QKQ1.190910.002 |
| Versi MIUI | MIUI Global 12.5.3 |
| Model | M1901F7G |
| OS | Android |

The smartphone used has been rooted using the Magisk application. Then the preparation for the process of data acquisition from the smartphone.

### 3.2. Examination

The data acquisition process is carried out on the smartphone at this stage. The data acquisition process on the smartphone must be connected to the laptop using a data cable and activate the developer options on the smartphone to connect to the MOBILedit Forensic tools. It can be seen in Fig.5 that the smartphone is already connected to MOBILedit Forensic.

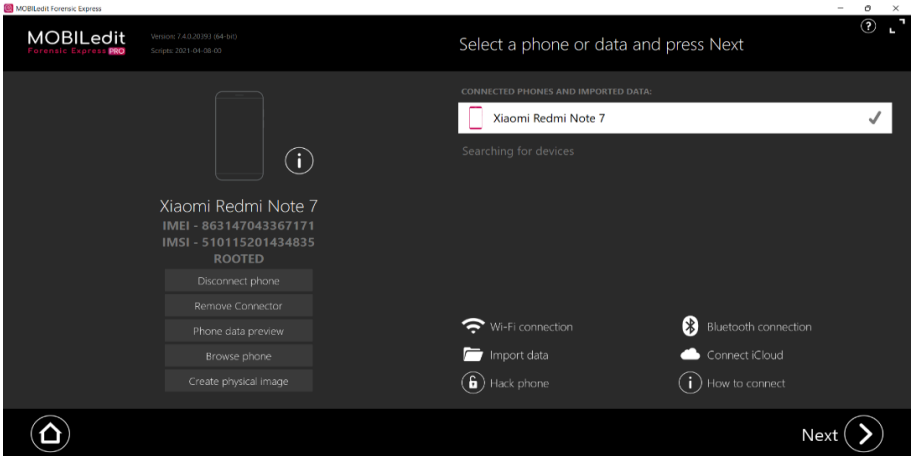


**Fig. 5.**Smartphone Connected with MOBILedit Forensic

After the smartphone is successfully connected to MOBILedit Forensic, information from the connected smartphone will appear, as shown in the image above. The data acquisition process uses Magnet Axiom Forensic tools when the smartphone is connected. The information provided is shown in Fig.6.

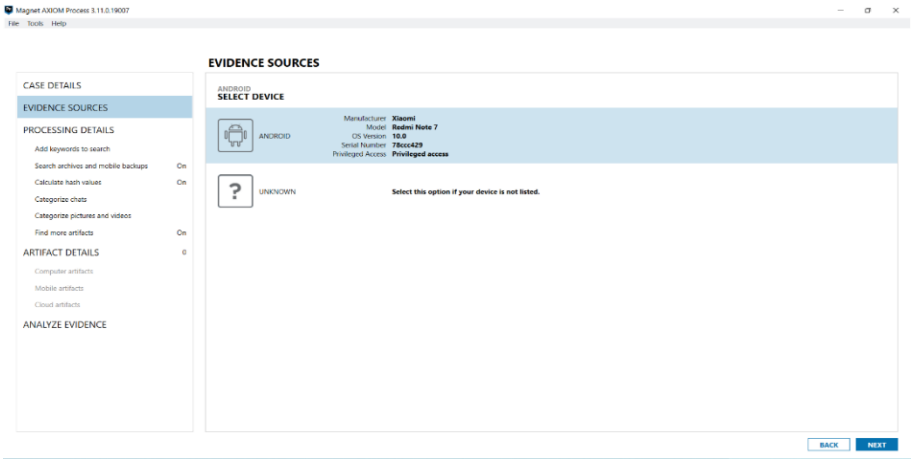


**Fig. 6.**Smartphone Connected with Axiom Forensic Magnet

Furthermore, the data acquisition process is carried out with MOBILedit Forensic on the Instagram application, as shown in Fig.7.

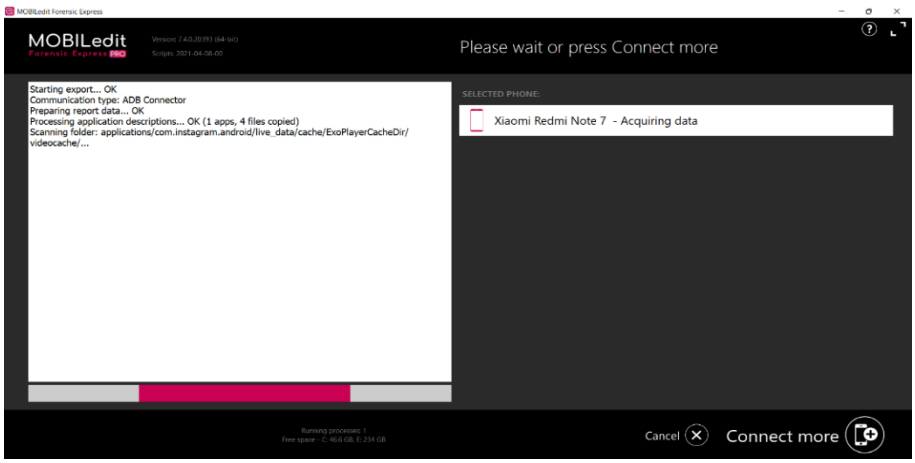


**Fig. 7.**Data Acquisition Process with MOBILedit Forensic

While the data acquisition process with Magnet Axiom Forensic on the Instagram application can be seen in Fig.8.

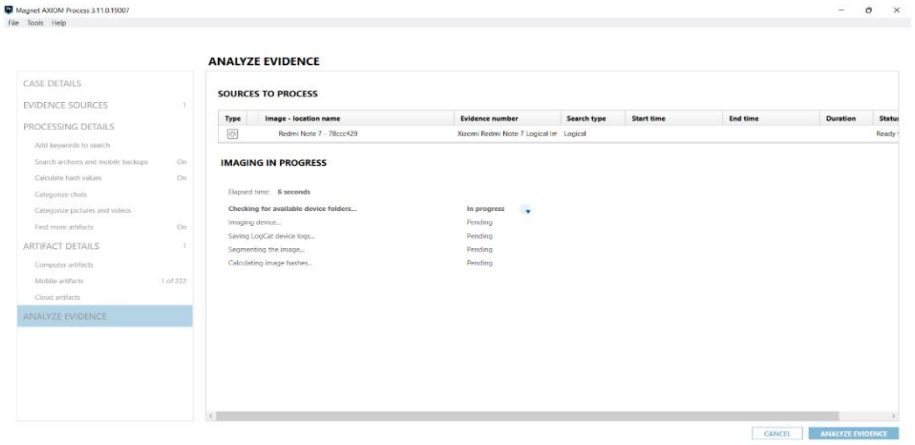


**Fig. 8.**Data Acquisition Process with Axiom Forensic Magnets

After the data acquisition process, several files will be obtained in the folder. The results of the data acquisition process can be seen on the laptop, which has previously determined the storage location of the acquisition results, as shown in Fig.9 and Fig.10.

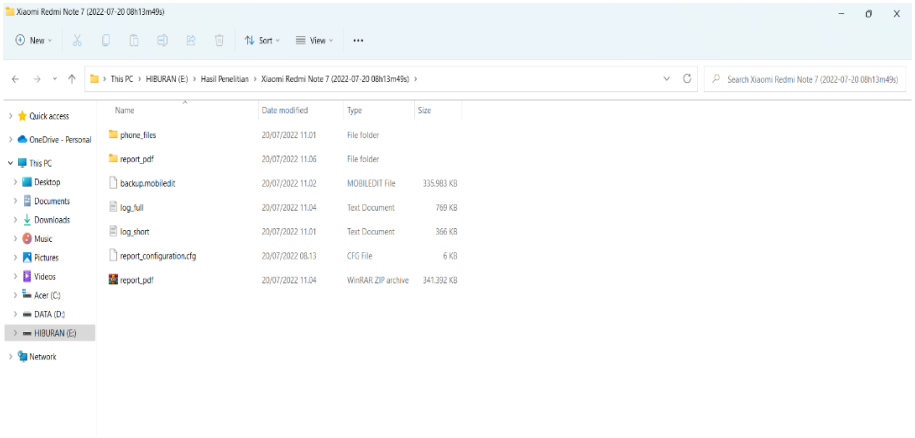


**Fig. 9.**Results of the Data Acquisition Process with MOBILedit Forensic

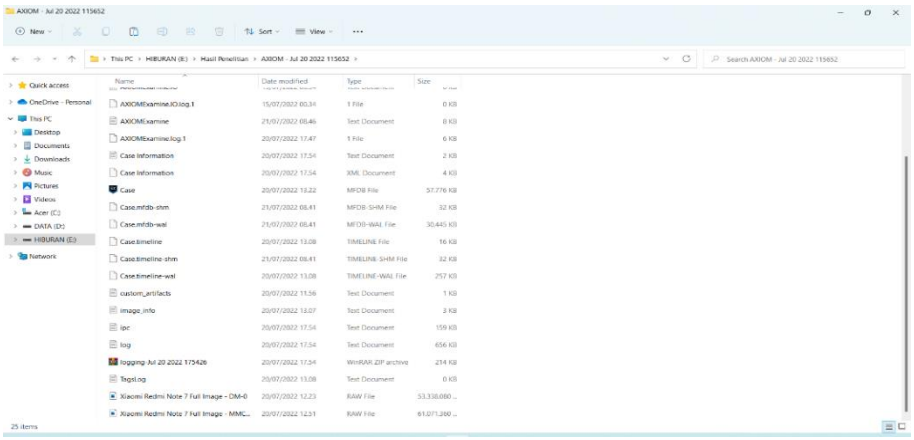

**Fig. 10.** Results of the Data Acquisition Process with Axiom Forensic Magnets

### 3.3. Analysis

At this stage, an analysis of the results of the data acquisition process found on the smartphone is carried out. Digital evidence to be analyzed is text messages, images, and videos. The following is the process of analyzing the digital evidence found from MOBILedit Forensic, which can be seen in Fig.11, Fig.12, and Fig.13.

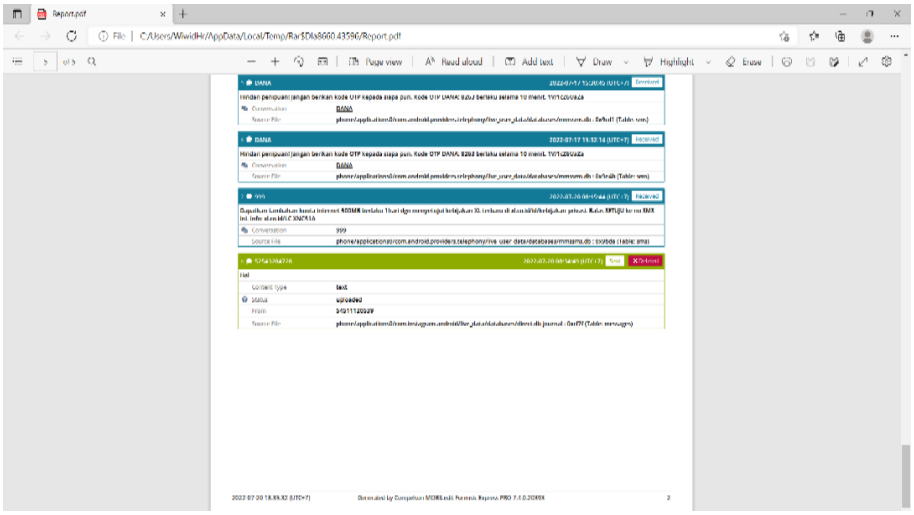

**Fig. 11.** The Process of Analysis of Successfully Found Text Messages on MOBILedit Forensic

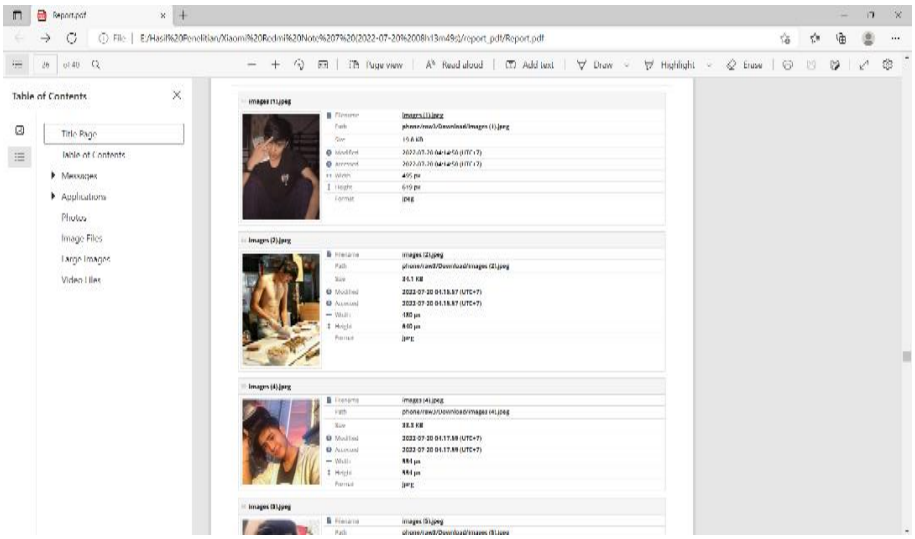

**Fig. 12.** Image Message Analysis Process Found on MOBILedit Forensic

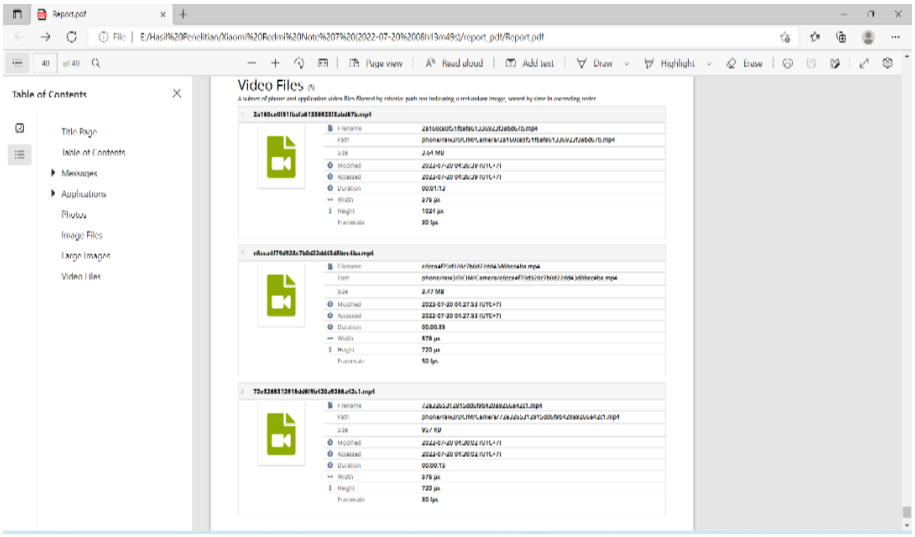


**Fig. 13.** Video Message Analysis Process Found on MOBILedit Forensic

While the analysis process for digital evidence found on Magnet Axiom is almost the same as MOBILedit Forensic, it can be seen in Fig.14, Fig.15, and Fig.16.

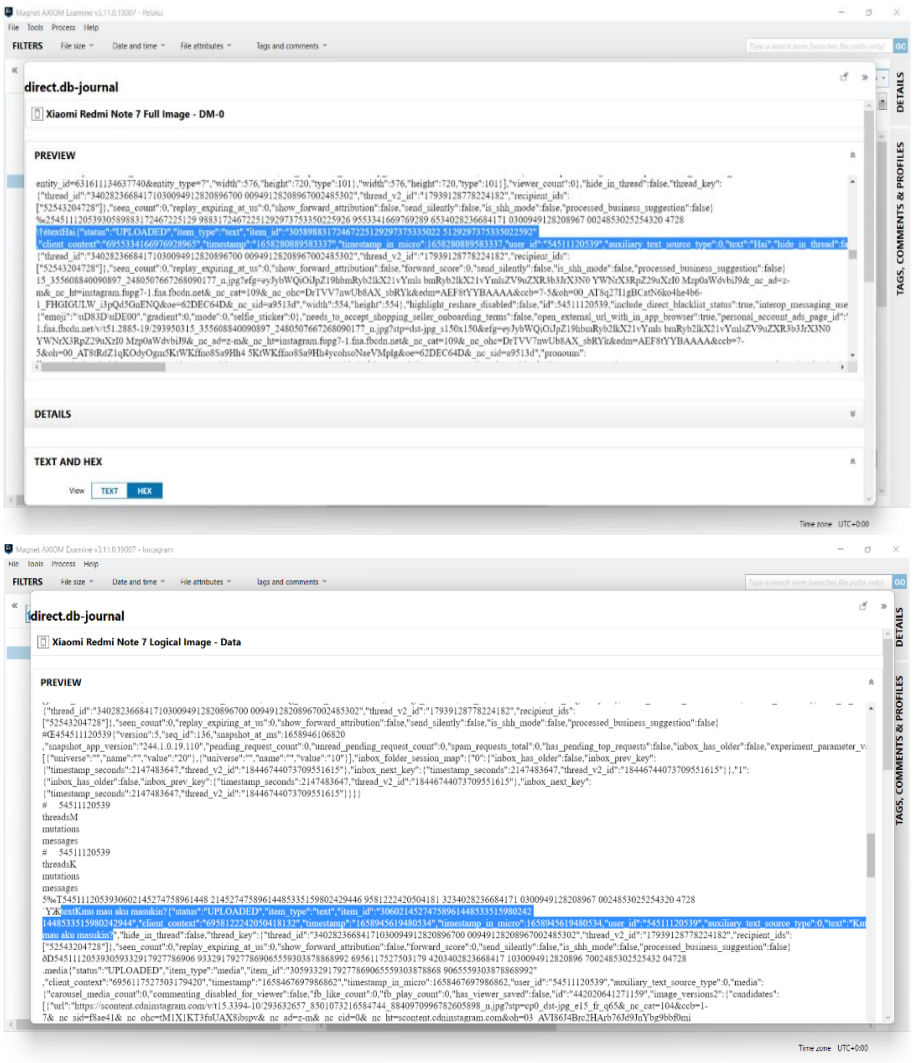


**Fig. 14.** The Process of Analyzing Text Messages Found on Axiom Forensic Magnets

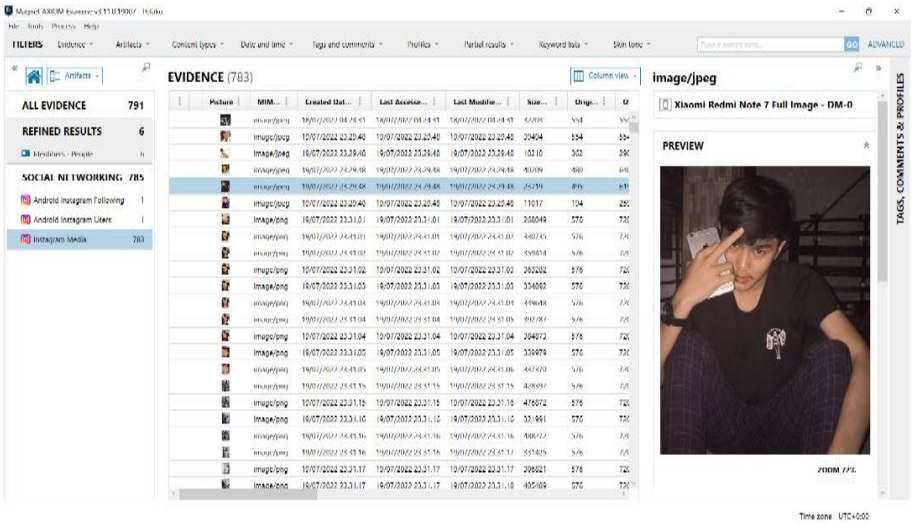


**Fig. 15.** Image Message Analysis Process Found on Axiom Forensic Magnets

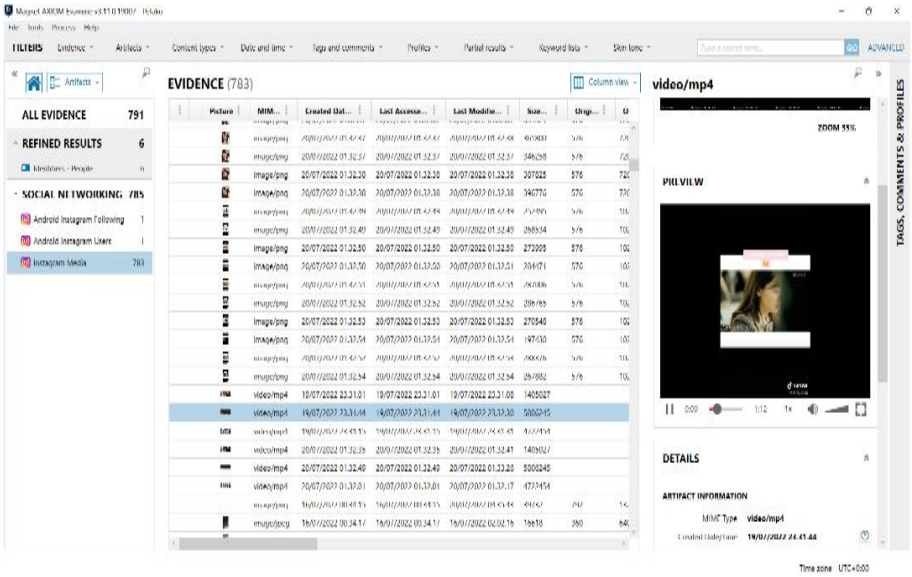


**Fig. 16.** The Process of Analysis of Video Messages Found on Axiom Forensic Magnets

### 3.4. Reporting

This stage reports the results of the analysis process from 13 digital pieces of evidence, which is the focus of the analysis. MOBILedit Forensic returned nine digital pieces of evidence that had been deleted and Magnet Axiom Forensic returned ten digital pieces of evidence that had been deleted. The following compares the performance of the MOBILedit Forensic and Magnet Axiom Forensic tools in restoring deleted data on Instagram messenger, which can be seen in Table 2.

**Table.2** Digital Evidence Results

| No | Digital Evidence | Amount of Digital Evidence Initial Data | MOBILedit Forensic | Magnet Axiom |
|---|---|---|---|---|
| 1. | Text Message | 5 | 1 | 2 |
| 2. | Picture Message | 5 | 5 | 5 |
| 3. | Video Message | 3 | 3 | 3 |

A comparison of the performance results of digital forensic tools on Instagram messenger using MOBILedit Forensic and Magnet Axiom Forensic has the following accuracy results in restoring deleted data. 92%. These results are obtained from the calculation of the comparison of unweighted index numbers with the following formula:

MOBILedit Forensic tools performance calculation $= \frac{9}{13} * 100 = 69,23\%$

Calculation of performance of Magnet Axiom Forensic tools $= \frac{10}{13} * 100 = 76,92\%$

Research conducted by Galih Fanani, Imam Riadi, and Anton Yudhana (2022) with the title "Forensic Analysis of the Michat Application Using the Digital Forensics Research Workshop Method" in this study the tools used for MOBILedit Forensic the results of digital evidence obtained from the perpetrator's smartphone in the form of images and videos. At the same time, digital evidence of text messages was not found [9].

Research conducted by Ikhwan Wiratama Putra, Aries Suharso, and Chaerur Rozikin (2021) with the title "Digital Evidence Acquisition and Image Authenticity Detection on Whatsapp Using the NIST and ELA Methods" in this study, the tools used for Magnet Axiom digital evidence that were successfully obtained from smartphones perpetrators are in the form of accounts, contacts, call history, text messages, digital evidence that was not successfully obtained in the form of images [10].

While in this study, the digital evidence that was successfully obtained on Instagram messenger from the perpetrator's smartphone using the MOBILedit Forensic tools digital evidence that was successfully obtained were text messages, picture messages, and video messages with an accuracy of 69.23% and Magnet Axiom Forensic digital evidence that was successfully obtained, namely text messages, picture messages and video messages with an accuracy of 76.92%.

## 4. Conclusion

The analysis of data deleted on Instagram messenger using the MOBILedit Forensic and Magnet Axiom Forensic tools shows that Magnet Axiom Forensic performance results are more optimal because the accuracy results reach 76.92%, compared to MOBILedit Forensic, the accuracy results only reach 69.23%. MOBILedit Forensic and Magnet Axiom Forensic tools are not good enough to restore deleted data from smartphones in text messages, while picture and video messages can be appropriately restored on the Instagram messenger application. Based on the analysis of research conducted, it is proven that the NIST method can help facilitate investigations from evidence to the stage of reporting digital evidence.

Suggestions for further research are to use smartphones from perpetrators and victims to investigate digital evidence on Instagram messenger to be used as comparison or use other forensic tools to get much more valid evidence.

## References

[1] W. A. Mukti, S. U. Masruroh, and D. Khairani, "Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android," *J. Tek. Inform.*, vol. 10, no. 1, pp. 73–84, 2018, doi: 10.15408/jti.v10i1.6820.

[2] I. Riadi, A. Yudhana, and M. C. F. Putra, "Analisis Recovery Bukti Digital Instagram Messangers Menggunakan Metode National Institute of Standards and Technology (NIST)," *Semin. Nas. Teknol. Inf. dan Komun. - Semant.*, pp. 161–166, 2017. Available at : peradaban.ac.id.

[3] S. Kemp, "Digital 2022: Platform Media Sosial Favorit Dunia," *www.datareportal.com*, 2022. Available at : datareportal.com.

[4] F. Yudha, "Usb Analisys Tool Untuk Investigasi Forensika Digital," *Teknoin*, vol. 21, no. 4, 2015, doi: 10.20885/teknoin.vol21.iss4.art6.

[5] I. Riadi and R. Umar, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method Imam," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 3–8, 2017. doi:10.11591/ijece.v8i5.pp3991-4003.

[6] I. Riadi, A. Fadlil, and M. I. Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode

National Institute of Standard and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 1, no. 10, pp. 820–828, 2021.doi : 10.29207/resti.v4i5.2224.

[7] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, pp. 219–227, 2018. Available at : journal.maranatha.edu.

[8] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[9] 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, pp. 1263–1271, 2022, doi: 10.30865/mib.v6i2.3946.

[10] I. P. Wiratama, A. Suharso, and C. Rozikin, "Akuisisi Bukti Digital Dan Deteksi Keaslian Citra Pada Whatsapp Menggunakan Metode NIST Dan ELA," *J. Sains Komput. Inform.*, vol. 5, no. 2, pp. 712–726, 2021. doi : 10.30645/j-sakti.v5i2.370.