International Journal of Safety and Security Engineering
Vol. 12, No. 6, December, 2022, pp. 707-713
Journal homepage: http://iieta.org/journals/ijsse

# Forensic Mobile Analysis on Social Media Using National Institute Standard of Technology Method

Herman[1*], Imam Riadi[2], Irhash Ainur Rafiq[1]

[1] Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta 55164, Indonesia
[2] Department of Information System, Universitas Ahmad Dahlan, Yogyakarta 55164, Indonesia

Corresponding Author Email: hermankaha@mti.uad.ac.id

https://doi.org/10.18280/ijsse.120606

**Received:** 17 July 2022
**Accepted:** 26 September 2022

***Keywords:***
*social media, android, forensic mobile, NIST, cybercrime*

**ABSTRACT**

Instagram and WhatsApp have become popular social media applications, and the number of active users grows significantly each year. The increased use of Instagram and WhatsApp has increased the number of digital crimes, which are frequently committed by utilizing information obtained and available through the social media accounts of potential victims. Special forensic tools are required for digital crime policing using smartphones. As a result, it is necessary to investigate the functionality of existing forensic tools for processing digital crime cases involving Android phones, particularly for the social media platforms Instagram and WhatsApp. The goal of this study was to evaluate and compare two forensic technologies for obtaining digital evidence from Instagram and WhatsApp using experimental methods. Magnet Axiom discovered 92.31% of all digital evidence, whereas MOBILedit Forensic discovered 79.49% of digital evidence. Using the process of comparing the two study outcomes with forensic technology, Magnet Axiom outperforms MOBILedit Forensic in detecting digital evidence of Instagram and WhatsApp since MOBILedit Forensic cannot restore video data for more than 20 minutes.

## 1. INTRODUCTION

Social media is an instant messaging service that allows users to easily send voice messages, texts, make phone calls, and share pictures and videos, which have become an integral part of everyone's existence [1]. Social media is currently a new medium for digital crimes such as buying and selling narcotics, hate speech, pornography, fake news, and so on [2]. Instagram is one of the most popular social media applications in the community.

Active social media users are mostly indifferent to the importance of maintaining data and information that is private, this is based on the habits of social media users, especially Instagram, who often upload photos or videos located around the residential area or where the user was at that time. This information that is considered trivial is often used by criminals because they already have information on the whereabouts of their potential victims.

The convenience provided by Instagram to users also has a risk of digital crime attacks because of the large amount of personal information uploaded and can be found by others [3-5]. Habits of using social media on mobile connected to the internet has resulted in increased targets for digital crime attacks, as in Figure 1 [6] shows the number of mobile cyber-attacks against users globally increased.

It is very clear that mobile is often the target of cyber-attacks as shown in Figure 1 the number of cyber-attacks on mobile always reaches millions of cases every year. Recently, Instagram has often become a medium for digital crimes, and information and media that have been uploaded can be used as material for forensic investigations [7]. Table 1 shows some personal information that may be utilized as a resource for social media attacks and the many types of attacks that can be employed. Digital forensics is very challenging because of security vulnerabilities in the data to be searched [8]. Digital forensics is a forensic science that aims to find evidence of crimes in the digital world [9]. Mobile Forensics is a subfield of digital forensics that focuses on mobile devices such as smartphones [10, 11].

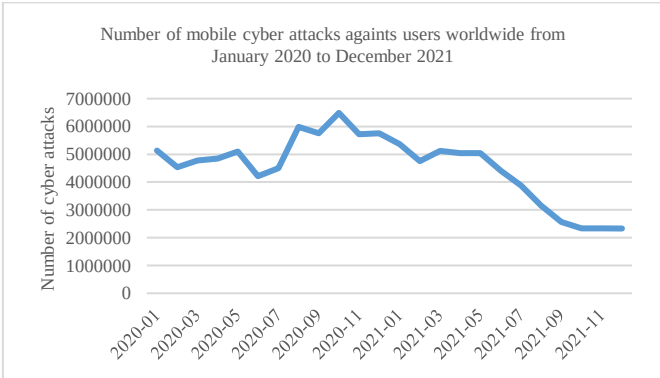


**Figure 1.** From January 2020 to December 2021, the number of mobile cyber-attacks against users globally increased

**Table 1.** List of risky privacy data and attack type

| No | Risky data | Attack type |
|---|---|---|
| 1 | Photo or Video | Online prostitution and fraud<br>Spam |
| 2 | Email and phone number | Phising<br>Spear Phising<br>Business Email Compromise (BEC) |

Digital data that can be used as digital evidence can be in the form of images, videos, text, sounds, documents, call history, and user information [12, 13]. Data acquisition basically has four methods, namely logical, file-based, physical, and manual extraction [14, 15].

## 2. LITERATURE REVIEW

This study adopts quotes from several previous studies related to digital forensics and mobile forensics, including;

The first study, in their research, Riadi et al. conducted digital forensics on smartphone devices with the Android operating system, in order to obtain digital evidence on the Line Messenger application with the help of MOBILedit Forensics as a means of acquiring data on smartphones, the digital evidence obtained is available. The research is in the form of text messages and pictures, then the name of the sender and the time of sending and receiving the message, this study concludes MOBILedit Forensics has weaknesses in the data sorting process [16].

The second study, Bača et al. analyzed the forensic results on Facebook or Instagram social networks obtained from several forensics tools, namely Andriller, Androphsy, Cellebrite UFED, Oxygen Forensics Suite, Paraben Mobile Forensics Tools, MSAB, Lime, Autopsy, MOBILedit Forensics, and Belkasoft Evidence by following the NIST framework, the results obtained are in the form of user account information, open source, root required, Call Logs, SMS/MMS, Contacts, Browser History, Photos, Facebook Messages, Instagram Messages, Deleted Data, Recovery of Data and Presentation [17].

The third study, Chang conducted a forensic investigation on WhatsApp on an android smartphone, this research carried out two simulation modes on his smartphone, rooted and non-rooted mode which then used the forensic tools Autopsy, WinHex, and XRY for the data acquisition process and analysis results from the data. which obtained digital proof from acquisition using XRY there is no difference between rooted and non-rooted whereas WinHex can't get the digital evidence at all on non-rooted mode and Autopsy on non-rooted still gets some digital proof [18].

The fourth study, Marrington and Mehtre melakukan investigasi forensic terhadap aplikasi Facebook, Twitter dan MySpace pada Smartphone BlackBerry, iPhone, dan Android. Penelitian ini hanya melakukan pengambilan data secara logical acquisition. Hasil yang didapat smartphone BlackBerry tidak ditemukan data apapun dari Facebook, Twitter dan MySpace [5].

Investigations forensic on mobile has several popular frameworks including; The National Institute of Standards and Technology (NIST), Digital Forensics Research Workshop (DFRWS), Association of Chief Police Officers (ACPO), and National Institute of Justice (NIJ) this framework can facilitate the process of forensic according to their needs.

This study simulates the retrieval of digital data on the Samsung Galaxy Tab A8 smartphone device in the form of user information, and digital data from social media applications WhatsApp and Instagram, it is hoped that some digital evidence has been deleted from the smartphone. The research is written into five parts, starting with an introduction and then listing several studies related to this research, the three research methodologies, the four results, and the fifth conclusion from this research.

## 3. RESEARCH METHOD

This study used experimental methods to investigate the capacity of two digital forensic tools to gather digital evidence in the Instagram and WhatsApp programs, as well as the process of acquiring digital data using the NIST Method.

### 3.1 Research object

This study's research objects were digital data that had been removed from the Instagram and WhatsApp social media apps on Android devices. Researchers collect digital data and then analyze it to determine whether it contains evidence of digital crime. The tool's effectiveness to recover erased digital data on mobile devices was also evaluated.

### 3.2 Experiment research stages

This study seeks to implement the process of data acquisition from smartphones with the Android operating system, in the data acquisition process using the tools Magnet Axiom and MOBILedit Forensics based on the NIST framework to structure the process. Mobile forensics with the NIST framework have four stages as shown in Figure 2.


**Figure 2.** Mobile forensics steps from NIST framework

1. Collection

Collection is the initial stage of the NIST framework, at the collection stage, collection, documentation, isolation and preservation of evidence are carried out.

2. Examination

Examination is the second stage with actions taken including backup and an imaging system that supports image and can be used with tools formatting.

3. Analysis

The step of analysis is when the findings of the examination are gathered and evaluated using legally permissible means to get meaningful information.

4. Reporting

Reporting is the last stage carried out to provide detailed reports of each forensic stage that has been carried out to provide recommendations for improving policies, procedures, tools, and other aspects of forensics.

The data acquisition process uses several hardware and software to obtain results from research, hardware, and software used as shown in Tables 2 and 3.

**Table 2.** Hardware research tools

| No | Hardware | Description |
|---|---|---|
| 1 | Tab Samsung Galaxy A8 | Physical evidence rooted |
| 2 | Laptop, Intel i3 -1005G1 CPU @ 1.20GHz 1.19 GHz 4 GB RAM | Workstation |
| 3 | USB Connector | Connecting device smartphone to laptop |

**Table 3.** Research support software

| No | Software | Version | Description |
|---|---|---|---|
| 1 | WhatsApp | 2.22.4.74 | Social Media |
| 2 | Instagram | 299.0.0.11.111 | Social Media Object |
| 3 | Magnet Axiom | 4.10.0.23663 | Forensic Tool |
| 4 | MOBILedit Forensics | 9.0.0.21797 | Forensic Tool |

It can be seen in Table 2 that this study uses a Samsung Galaxy A8 smartphone unit which functions as physical digital evidence and is a source of digital data that will be acquired in the study. In this case, the status of the Samsung Galaxy A8 smartphone is in a Rooted so that extraction data then there is a laptop unit with an intel core i3-1005G1 chipset with a capacity of 4 GB RAM which functions as a workstation when acquiring data and there is also a USB Connector type E unit to connect a smartphone with a laptop.

Table 3 is a list of software used in acquiring and extracting data. This study uses two social media applications WhatsApp and Instagram as sources of digital evidence to be sought and two forensic tools namely Magnet Axiom and MOBILedit Forensics which are used to acquire data on the Samsung Galaxy A8 smartphone.

The National Institute of Standards and Technology (NIST) defined the must-have capabilities of a forensic tool and test design in assessing the performance of forensic tools in a document titled "Mobile Device Tool Test Assertions and Test Plan ver. 2" 24and "Mobile Device Tool Specification ver. 2"25. Based on the findings of each test plan, NIST provides a total of 42 measurement variables and techniques for measuring the performance of forensic instruments. This study only takes several related variables, the variables used in this study are as presented in Tables 4.

**Table 4.** NIST standard forensics tool specifications and test plans

| ID | Mobile Device Tool-Core Requirement (MDT-CR) | |
|---|---|---|
| **MDT-CR-01** | A mobile device forensic tool shall have the ability to recognize supported devices via suggested interfaces (e.g., cable, Bluetooth) | |
| **MDT-CR-02** | A mobile device forensic tool shall have the ability to notify the user of connectivity errors between the device and application during data extraction | |
| | Mobile Device Tool-Requirement Optional (MDT-RO) | |
| **MDT-RO-01** | A mobile device forensic tool shall have the ability to perform a physical data extraction for supported devices | |
| | **Mobile Device Tool-Core Assertion (MDT-CA)** | |
| **ID** | **Test Assertion** | **Comments** |
| **MDT-CA-01** | If a mobile device forensic tool provides the user with an "Acquire All" data objects acquisition option then the tool shall complete the logical/filesystem acquisition of all data objects without error. | Select Acquire all; Begin acquisition |
| **MDT-CA-02** | If a mobile device forensic tool provides the user with a "Select All" individual data objects then the tool shall complete the logical/filesystem acquisition of all individually selected data objects without error. | Select all supported data objects; Begin acquisition |
| **MDT-CA-03** | If a mobile device forensic tool provides the user with the ability to "Select Individual" data objects for acquisition then the tool shall complete the logical/filesystem acquisition for each exclusive data object without error. | Select one or more supported |
| | **Mobile Device Tool-Assertions Optional (MDT-AO)** | |
| **MDT-AO-1** | If the mobile device forensic tool supports a physical acquisition of the target device, then the tool shall complete the physical acquisition without error. | Select Physical Acquisition; Begin acquisition |
| **MDT-AO-2** | If connectivity between the mobile device and mobile device forensic tool for a physical acquisition is disrupted then the tool shall notify the user that connectivity has been disrupted. | Begin acquisition; Disconnect interface or interrupt connectivity (i.e., unplug cable) during acquisition |
| **MDT-AO-3** | If a mobile device forensic tool completes physical acquisition of the target device without error, then the tool shall have the ability to present acquired data objects in a useable format via a preview-pane, generated report or output file. | Perform physical acquisition; Review data for readability in a useable format |

Table 4 is the six specifications or capabilities that must exist and additional capabilities for a forensic tool issued according to NIST standards, as well as several tests carried out to measure the performance of a digital forensic tool.

Testing the ability of forensic tools according to NIST standards consisting of Connectivity testing with ID MDT-CA-01, MDT-CA-02, MDT-CA-03, MDT-AO-01, MDT-AO-09, MDT-AO-10, MDT-AO-11, MDT-CA-04, MDT-AO-02 and MDT-AO-15, Data Acquisition and Interpretation with ID MDT-CA-05 MDT-AO-03 MDT-AO-16 MDT-CA-06 MDT-AO-04 MDT-AO-17 MDT-CA-07 MDT-AO-05 and MDT-AO-18, Presentation of Non-ASCII Characters with IDs MDT-CA-08 MDT-AO-06 and MDT-AO-19 , Hashing with ID MDT-CA-09 MDT-AO-07 and MDT-AO-20, Case File/Data Protection with ID MDT-CA-10 MDT-AO-08 and MDT-AO-21, UICC PIN/PUK Authentication with ID MDT-AO-12 MDT-AO-13 and MDT-AO-14, Authentication Mechanism Bypass with ID MDT-AO-22.

In this study, we will not carry out all testing processes on the NIST standard, researchers only take processes that are in accordance with the state of the hardware and application objects in this research, the testing phase consists of connectivity tests with ID MDT-CA-01, MDT-CA- 02, MDT-AO-01, and MDT-CA-04, Data Acquisition and Interpretation with ID MDT-CA-05, MDT-AO-03, MDT-CA-06, MDT-AO-04, MDT-CA-07 and MDT-AO-05, Presentation of Non-

ASCII Characters with ID MDT-CA-08, Hashing with ID MDT-CA-09 and Authentication Mechanism Bypass with ID MDT-AO-22. This study did not apply the Case File/Data Protection and UICC PIN/PUK Authentication tests because the data taken all came from internal memory so there was no data retrieval process from UICC.

This study adds several types of digital data that have been determined as search targets during the digital forensic, this is done so that the accuracy measurement process of the forensic tools used is more specific and clearer, and the original data used in the data acquisition process is as in Table 5.

**Table 5.** Deleted digital data that will be searched

| No | Data | | | Amount |
|---|---|---|---|---|
| | Digital Data | Meta Data | | |
| 1 | Messages | Sender | 50345927492/inyong2269 | 3 |
| | | Receiver | irhashainur | |
| | | Timestamps | 06/12/2021 | |
| 2 | Images | MIME Type | image/jpeg | 5 |
| | | Timestamps | 26/04/2022 | |
| | | Size (byte) | 50055 | |
| | | Resolution | 1080x1920 | |
| | | Extension | .mp4 | |
| 3 | Videos | Timestamps | 27/04/2022 | 5 |
| | | Size (byte) | 837263 | |
| | | Duration | 2.73 | |
| | | Resolution | 1088X1088 | |
| | Supplementary Data | | | |
| 4 | Account | inyong2269 | | |
| 5 | Url | https://www.instagram.com/ | | |

Digital data that shown in Table 4 is the target of searching for digital data from smartphone Samsung Galaxy A8, there is a list of data in Table 5 so that the process of calculating the level of accuracy between forensic tools Magnet Axiom and MOBILedit Forensics are more specific and fairer. The data provided is in the form of three digital message data, five images, five videos, and some personal data on Instagram and WhatsApp social media accounts.

## 4. RESULTS AND DISCUSSION

This research is carried out according to the framework provided by the NIST framework with the following four stages:

1. Collection

Physical evidence that has been collected in the form of a Samsung Galaxy A8 smartphone, the actions taken at this stage are to maintain the condition of the authenticity of the evidence, both physical and digital data. Efforts made to maintain the physical authenticity of the evidence are documentation in the form of photos of each side of the evidence so that when the evidence is brought to the legal process the authenticity of the evidence can be guaranteed, then efforts to maintain the authenticity of digital data by isolating the evidence or converting it into mode aircraft so that no data exchange flows occur on the smartphone during the forensic investigation process. From the results of the investigation at the collection of physical evidence, data is obtained as shown in Table 6.

**Table 6.** Device specs of cybercrime suspects

| No | Information | Descriptions |
|---|---|---|
| 1 | Manufacturer | Samsung |
| 2 | Product Model | SM-P355 |
| 3 | Operating System | Android |
| 4 | OS Version | 7.1.1 (Nougat) |
| 5 | Serial Number | RR2G600K09A |
| 6 | IMEI | 359896060XXXXXX |
| 7 | Rooted | Yes |

Information obtained in the collection must be maintained until the legal process because it will be one of the factors that the evidence brought to the legal process will be accepted or not, if during the legal process the evidence changes and is not the same when it is first discovered, all data and information obtained from the physical evidence will most likely be rejected in the legal process.

2. Examination

After the physical condition of the smartphone is recorded in detail along with its specifications and has been changed in airplane mode so that no data exchange flows occur again on the smartphone, the next process is to acquire data using forensics tools Magnet Axiom and MOBILedit Forensics as shown in Figures 3 and 4.

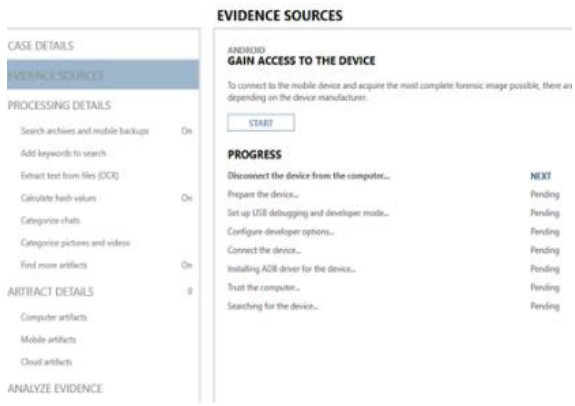


**Figure 3.** Data acquisition process on magnet axiom

The acquisition process carried out with Magnet Axiom is Physical Imaging, this process can be carried out with the condition of the smartphone being rooted, and the data can be retrieved with the following conditions: This is all data to system data and data that has been deleted.

The data acquisition process with MOBILedit Forensics as well as Physical Imaging smartphone condition rooted, by performing Physical Imaging it is hoped that the data obtained

is all data on the smartphone so that digital evidence that has been deleted can be returned again.

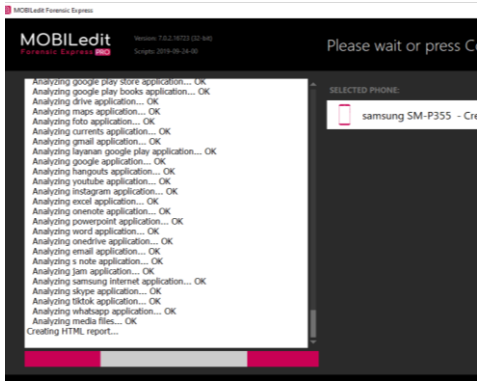


**Figure 4.** Data acquisition process in mobiledit forensics

3. Analysis

The acquisition data obtained from Magnet Axiom is located at E:\MAGNET\AXIOM - May 09 2022 170838\ samsung SM-P355 Full Image - MMCBLK0.raw, the analysis process can be carried out directly using the Magnet Axiom and an export file of the acquired data is also provided at E:\MAGNET\AXIOM - May 09 2022 170838\Export\Report.HTML and MOBILedit Forensics located at E:\New Folder3\Samsung SM-P355 (2022-05-12 12h01m29s)\Report_index.html The results of the analysis of data acquisition using Magnet Axiom and MOBILedit Forensics are as shown in Table 7.

Artifacts obtained from the WhatsApp application are indicated as digital evidence derived from call records and also incoming and outgoing messages containing suspicious photos and videos, the digital data was found in the WhatsApp application database as in Table 8.

**Table 7.** WhatsApp artifacts found

| WhatsApp | Magnet Axiom | | | MOBILedit Forensics | | |
|---|---|---|---|---|---|---|
| **User Activity** | **Artifacts Related** | **Source** | **Table** | **Artefacts Related** | **Source** | **Table** |
| Uploaded Status | Not Found | - | - | Not Found | - | - |
| Calling log | Found | \data\com.android.providers.contacts\databases\calllog. db | Calls | Found | phone/applications0/com.android.providers.contacts/live_data/databases/calllog.db | Calls |
| Message log | Found | \data\com.whatsapp\databases\msgstore.db \media\0\WhatsApp\Media\WhatsApp Images\ \media\0\WhatsApp\Media\WhatsApp Video\ | Messages | Found | phone/applications0/com.whatsapp/live_data/databases/msgstore.db | Messages |

**Table 8.** Instagram artifacts found

| Instagram | Magnet Axiom | | | MOBILedit Forensics | | |
|---|---|---|---|---|---|---|
| **User Activity** | **Artifacts Related** | **Source** | **Table** | **Artefacts Related** | **Source** | **Table** |
| Uploaded Story | Found | - | - | Found | - | - |
| User Following | Found | \data\com.instagram.android\shared_prefs\50345927492_usersBootstrapService.xml | - | Found | \data\com.instagram .android\shared_prefs\50345927492_usersBootstrapService.xml | - |
| User Followers | Found | \data\com.instagram.android\shared_prefs\50345927492_usersBootstrapService.xml | - | Found | data\com.instagram.android\shared_prefs | . |
| Uploaded Feeds | Found | 50345927492p_userdata\com.instagram.android\cache\ | - | Found | phone/applications0/com.instagram.android/live_data/cache/images/ | - |
| Direct Message | Found | \data\com.instagram.android\cache\ | - | Found | phone/applications0/com.instagram.android/live_data/databases/direct. db | - |
| Live Stream | Not Found | - | - | Found | phone/applications0/com.instagram.android/live_data/cache/http_responses/ | - |
| Reels | Not Found | - | - | Not Found | - | - |

Table 8 contains the results of extraction data analysis using Axiom Magnets and MOBILedit Forensics found digital data on the Instagram application consisting of Story, User Following, User Followers, Feeds, and Direct Messages data.

The results of the analysis of extraction data with Axiom Magnets and MOBILedit Forensics successfully found several variables given by NIST as parameters for measuring the performance of forensics tools, namely MDT-CA-01, MDT-CA-02, MDT-CA-03, MDT-CA-04, MDT-CA-05, MDT-CA-06, MDT-AO-12, MDT-RO-01, MDT-RO-02, and MDT-RO-03.

4. Reporting

The final stage in the NIST framework is reporting. At this point, all analysis results from Magnet Axiom and MOBILedit Forensics are provided in full in line with this research to compare the performance of forensics tools employed in the WhatsApp and Instagram programs. The report results are based on NIST parameters such as in Table 9.

**Table 9.** Evaluation results

| Parameters of Core Measurement | | Magnet Axiom | MOBILedit Forensics |
|---|---|---|---|
| Connectivity | MDT-CA-01 | √ | √ |
| | MDT-CA-02 | √ | √ |
| | MDT-AO-01 | √ | √ |
| Data Acquisition and Interpretation | MDT-CA-04 | √ | √ |
| | MDT-CA-05 | √ | √ |
| | MDT-AO-03 | √ | √ |
| | MDT-CA-06 | √ | √ |
| | MDT-AO-04 | √ | √ |
| | MDT-CA-07 | √ | √ |
| | MDT-AO-05 | √ | √ |
| Non-ASCII Character Presentation | MDT-CA-08 | - | - |
| Hashing | MDT-CA-09 | √ | √ |
| Authentication Mechanism Bypass | MDT-AO-22 | - | - |
| Case File/Data Protection | | x | |
| UICC PIN/PUK Authentication | | x | |

Axiom Magnets have the same performance as MOBILedit Forensics, this is evidenced by the similarity of test results based on NIST standards Axiom Magnets and MOBILedit Forensics successfully passed the connectivity, Data Acquisition and Interpretation, and Hashing tests but did not pass the Non-ASCII Character Presentation because Axiom Magnets and MOBILedit Forensics could not provide the original form of the successfully found NON-ASCII data, also failed the test in the Authentication Mechanism Bypass because Axiom Magnets and MOBILedit Forensics must obtain prior approval from the device if they want to connect which does not allow this when the device is locked.

Testing of Case File / Data Protection and UICC PIN / PUK Authentication was not carried out because the device conditions were not met, firstly this study did not use third parties to modify the data on the device, and secondly all data taken in this study came from the Instagram and WhatsApp applications installed on the internal memory.

The important point in testing using NIST standards is in Connectivity and Data Acquisition and Interpretation if in these two test points there are those that are not met then the data obtained from the forensic tool will be very doubtful of its veracity because There is an issue with the device's connection to the forensic tools then the data presented cannot be presented properly and clearly. Based on additional data provided in this study with the measurement method using an index number based on the results of the trial. The index number utilized in the computation is a weightless index, as stated in Eq. (1).

$$\text{Par} = \frac{\sum \text{ar0}}{\sum \text{arT}} \times 100\% \quad (1)$$

Par is the value of the accuracy of forensic applications
ar0 is the number of variables detected
arT is the number of variables used

By following Eq. (1) the level of accuracy and performance of MOBILedit Forensics and Magnet Axiom in obtaining digital data as follows.

Magnet Axiom

$$\text{Par} = \frac{36}{39} \times 100\% = 92.31\%$$

MOBILedit Forensics

$$\text{Par} = \frac{31}{39} \times 100\% = 79.49\%$$

Table 10 presents the details of the performance analysis of the Magnet Axiom and MOBILedit Forensics tools in obtaining digital data from the WhatsApp and Instagram programs to retrieve the digital data presented in this study.

**Table 10.** Performances index result

| | Artifacts | Amount | Magnet Axiom | MOBILedit Forensics |
|---|---|---|---|---|
| WhatsApp Artifacts | Chat | 5 | 5 | 5 |
| | Images | 5 | 5 | 3 |
| | Videos | 5 | 5 | 3 |
| Instagram Artifacts | Uploaded Story | 5 | 5 | 3 |
| | Uploaded Feeds (Images) | 5 | 5 | 5 |
| | Uploaded Feeds (Videos) | 5 | 5 | 3 |
| | Direct Message | 6 | 6 | 6 |
| | Comment | 3 | - | 3 |
| Performance Index Results | | 39 | 92.31% | 79.49% |

The results of measuring the performance of forensics tools with the index number comparison method in Table 10 show that the value obtained by Axiom Magnet is 92.31% and MOBILedit Forensics is 79.49% the difference in this value is not too far because the ability of these two tools is almost the same as each digital data category, only at the end of the test the amount of digital data that was successfully obtained had a slight difference in the amount, namely more Axiom Magnets until they got a higher value.

## 5. CONCLUSIONS

Magnet Axiom and MOBILedit Forensics can both return deleted digital evidence of the same type by using the NIST method in the data recovery process, but MOBILedit Forensics has the limitation of not being able to recover digital evidence

of videos longer than 20 minutes, whereas Magnet Axiom can obtain all digital evidence of video. MOBILedit Forensics has a value of 79.49%, whereas Magnet Axiom has a score of 92.31%. Based on these findings, Magnet Axiom outperforms MOBILedit Forensics in retrieving digital evidence from the Instagram and WhatsApp applications, particularly when the digital evidence is in the form of videos longer than 20 minutes.

## REFERENCES


[1] Alisabeth, C., Pramadi, Y.R. (2020). Forensic analysis of Instagram on android. In IOP Conference Series: Materials Science and Engineering, 1007(1): 012116. https://doi.org/10.1088/1757-899X/1007/1/012116

[2] Fayyad-Kazan, H., Kassem-Moussa, S., Hejase, H.J., Hejase, A.J. (2022). Forensic analysis of Whatsapp SQLite databases on the unrooted android phones. HighTech and Innovation Journal, 3(2): 175-195. https://doi.org/10.28991/hij-2022-03-02-06

[3] Riadi, I., Umar, R. (2018). Forensic tools performance analysis on android-based blackberry messenger using NIST measurements. International Journal of Electrical and Computer Engineering, 8(5): 3991. https://doi.org/10.11591/ijece.v8i5.pp3991-4003

[4] Mehrotra, T., Mehtre, B.M. (2013). Forensic analysis of Wickr application on android devices. In 2013 IEEE International Conference on Computational Intelligence and Computing Research, 1-6. https://doi.org/10.1109/ICCIC.2013.6724230

[5] Al Mutawa, N., Baggili, I., Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. Digital Investigation, 9: S24-S33. https://doi.org/10.1016/j.diin.2012.05.007

[6] Monthly mobile cyber attacks 2021, Statista. https://www.statista.com/statistics/1305965/mobile-users-cyber-attacks/, accessed on Jun. 08, 2022.

[7] Mahendraa, K.D.O., Mogia, I.K.A. (2021). Digital forensic analysis of Michat applications on android as digital proof in handling online prostitution cases. Jurnal Elektronik Ilmu Komputer Udayana, 9(3): 381-390. https://doi.org/10.24843/jlk.2021.v09.i03.p09

[8] Zamroni, G.M., Riadi, I. (2020). Mobile forensic tools validation and evaluation for instant messaging. International Journal on Advanced Science Engineering and Information Technology, 10(5): 1860-1866. https://doi.org/10.18517/ijaseit.10.5.7499

[9] Srivatsa Raju, S., Koundinya, R., Bharathi, R. (2020). Gathering evidence from Android OS for mobile forensics. International Journal of Computer Science and Network, 9(4): 163-166.

[10] Riadi, I., Umar, R., Firdonsyah, A. (2017). Identification of digital evidence on android's blackberry messenger using NIST mobile forensic method. International Journal of Computer Science and Information Security (IJCSIS), 15(5): 3-8.

[11] Li, E. (2021). A hands-on mobile device forensics course in cybersecurity education. TALE 2021 IEEE International Conference on Engineering, Technology and Education, Proceedings, pp. 1006-1010. https://doi.org/10.1109/TALE52509.2021.9678660

[12] Anglano, C., Canonico, M., Guazzone, M. (2020). The android forensics automator (AnForA): A tool for the automated forensic analysis of android applications. Computers & Security, 88: 101650. https://doi.org/10.1016/j.cose.2019.101650

[13] Chakraborty, N., Sheth, R.K., Mane, S.B. (2019). Framework for data extraction and analysis of damaged android mobile device. Int J. Res. Appl Sci. Eng Technol., 7(5): 306-311. https://doi.org/10.22214/ijraset.2019.5050

[14] Eriş, F.G., Akbal, E. (2021). Forensic analysis of popular social media applications on android smartphones. Balkan Journal of Electrical and Computer Engineering, 9(4): 386-397. https://doi.org/10.17694/bajece.761271

[15] Lwin, H.H., Aung, W.P., Lin, K.K. (2020). Comparative analysis of Android mobile forensics tools. In 2020 IEEE Conference on Computer Applications (ICCA), pp. 1-6. https://doi.org/10.1109/ICCA49400.2020.9022838

[16] Riadi, I., Fadlil, A., Fauzan, A. (2018). Evidence gathering and identification of line messenger on android device. Int. J. Comput. Sci. Inf. Secur. (IJCSIS), 16(5): 201-205.

[17] Bača, M., Cosic, J., Cosic, Z. (2013). Forensic analysis of social networks (case study). In Proceedings of the ITI 2013 35th International Conference on Information Technology Interfaces, 219-223. https://doi.org/10.2498/iti.2013.0526

[18] Chang, M. (2019). Digital Forensic Investigation of WhatsApp on Android. Scholars Journal of Engineering and Technology, 7(3): 74-84. https://doi.org/10.21276/sjet.2019.7.3.2