



Assess of Forensic Tools on Android Based Facebook Lite with the NIST Method

Rauhulloh Ayatulloh Khomeini Noor Bintang^{1*}, Rusydi Umar², Anton Yudhana³

^{1,2}Department of Informatics, Universitas Ahmad Dahlan, Indonesia

³Department of Electrical Engineering, Universitas Ahmad Dahlan, Indonesia

Abstract

Purpose: The increase in social media use of Facebook lite by using Android-based smartphones is quite high. Activities when communicating through the social media network Facebook Lite. Facebook lite can send a text message, image, or video. Not a few Facebook users lite social media abusing this app to commit fraud crimes, pornographic acts, or defamation actions from social media users Facebook lite. In such cases, it can be a digital forensic benchmark to get results from digital evidence from the Facebook lite application.

Methods: In this investigation, National Institute of Standards and Technology (NIST) research methods with various stages, namely Collection, Examination, Analysis, and Reporting.

Result: Comparison and results of data conducted with forensic tools Magnet Axiom Forensic and MOBILedit Forensic Express Pro in the form of parameter data specified. Axiom Forensic Magnet data is 57.14%, while MOBILedit Forensic Express Pro data is 85.71%.

Novelty: This data is the data of the performance results of both forensic tool applications in obtaining digital evidence on Facebook lite application.

Keywords: Forensic Digital, Social Media, NIST, Mobile Forensic

Received October 2020 / **Revised** February 2021 / **Accepted** February 2021

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).



INTRODUCTION

Technology in Smartphones has grown very rapidly and is little by little began to replace the function of desktop computers by improving the functions that exist on smartphones and improving the app features available in the Google Play store on mobile devices [1, 2]. A smartphone device is equipped with various features to send messages, emails, telephone, social media, or other applications [3]. As seen in statistics on Hootsuite We Are Social, the number of daily active users in the quarterly report in 2019 reached 1.62 billion, certainly up from 1.50 billion the previous year. This present shows 66% of Facebook's worldwide use of the app every day [4]. On the official site, we are a social statistics global digital report showing statistics on the active use of Facebook social media in Figure 1.

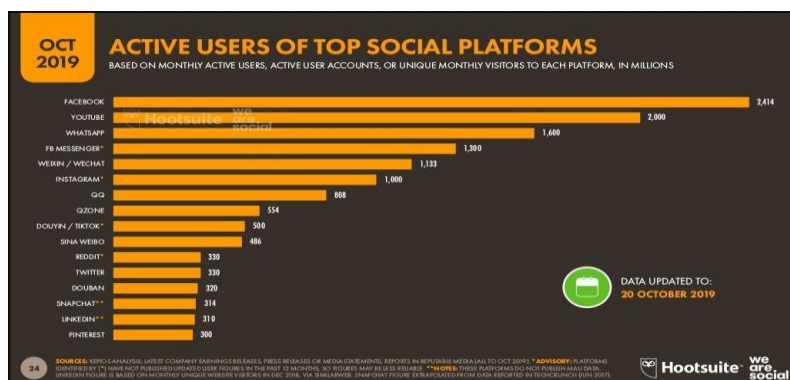


Figure 1. Social media active user 2019

*Corresponding author.

Email addresses: rahullbintang5@gmail.com (Bintang), rusydi_umar@rocketmail.com (Umar), eyudhana@ee.uad.ac.id (Yudhana)

DOI: 10.15294/sji.v8i1.26744

The number of smartphone-type uses globally continues to increase year on year. In 2019, at least touched the figure of 3.2 billion users, up 5.6% from the previous year. Meanwhile, active Smartphone users are expected to reach 3.8 billion in units. China is becoming a country with several smartphone users scattered. Total smartphone users in that country control at least 27% of the total existing users. In 2022, the number of smartphone phone users will reach 3.9 billion users [5]. From databooks, namely the number of world smartphone users as figure 2 showed.

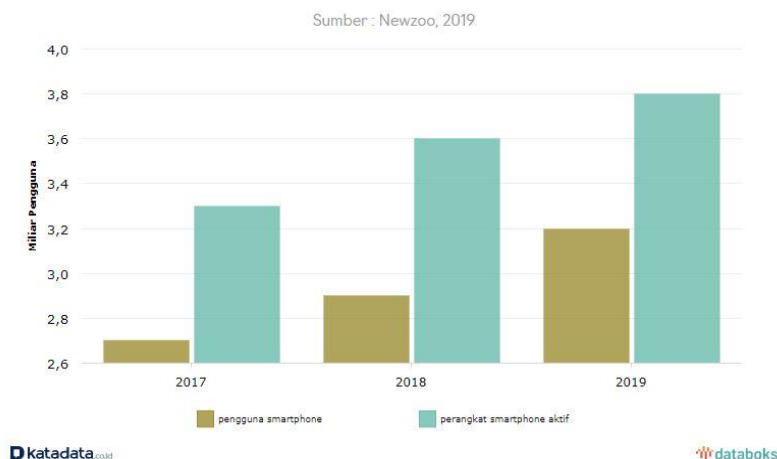


Figure 2. Smartphone user statistics

Smartphone devices in today's era have different types of functions similar to computers. It makes Facebook active user using their smartphone instead of using a computer because using a smartphone can already access sending pictures, messages, text, audio, and video between fellow users of social media Facebook lite. With the feature on Facebook Lite makes it easy for us to send messages in chats and picture messages personally, Facebook Lite's social media almost has similarities to other social media such as Twitter, Instagram, and Whatsapp [6]. It is easy for social media users to access Facebook lite in communicating, but the more accessible and more activity in using Facebook Lite social media can potentially lead to irresponsible users in crime in social media. Crimes on social media have various factors such as pornography crime, online bullying, and selling scams, defamation crimes, and other crimes. They are using the features in the Facebook lite app by sending or uploading defamation posts or images that can harm other readers. It can make it a criminal case in the form of defamation that can be convicted through a local court.

Based on the above problems, forensic mobile confectionery is needed to help solve defamation cases through social media, especially against social media Facebook Lite through mobile smartphones as the initial access of media used by criminals. The authors developed the study using the NIST method. They conducted tests using two forensic tools, the Axiom Forensic Magnet tool, and MOBILedit Forensic Express Pro. It can compare the results of each forensic tool from the data angle on Facebook Lite social media in a defamation case in the form of messages, images, audio, and video that will be digital evidence under trial [7, 8].

Digital forensics is the forensic science of computer technology for legal proof, proving the case for crimes on social media committed by the offender [9, 10]. One of the fields of digital forensic science is mobile forensics, and digital forensics is part of the science that uses initial conditions of the original data by investigating the items found in digital. The process that helps in disclosing the events of a particular crime is digital forensics [11]. The recovery of digital evidence Smartphone device can be called cellular forensics using the method specified by the researcher devices in smartphones using the prescribed method. In the next stage of retrieving forensic data via smartphone from the data in the social media application Facebook Lite that has been attached to smartphones [12].

Social media Facebook lite is an application service for sharing photos that allow others to take pictures that we upload. At the moment, the social media app Facebook Lite can be said to be a social media with a

high level of users on social media used by the community. The main factor of people using the Facebook Lite app is for communication media by sending chats, photos, and status with other users of the Facebook lite app [13]. An Android operating system is a mobile phone that is popular enough for users to run various applications [14]. Advancing by features on the platform's operating system in android, an open android platform, gives developers the freedom to do developers in an android system [15].

The technology on android gives app developers an expanded use of social media apps, specifically on the Android Operating system on Facebook lite social media [16]. Chating application on an Android smartphone on the app can send a message and picture very quickly for the message receiver, Facebook Lite is one of the following applications [17]. Cybercrime crimes can occur on any electronic device, such as an Android smartphone [18]. In cybercrime, the term activity is carried out by criminals by conducting computers or computer networks. Examples of cybercrime cases include drug trafficking, online trafficking fraud, pornography, and defamation.

METHODS

This research refers to the performs stages on NIST National Institute of Standard and Technology forensic analysis methods. The primary stages of the digital forensic process method using stages using the Collection, Examination, Analysis, and Reporting stages. Figure 3 shows the stages of the forensic process.

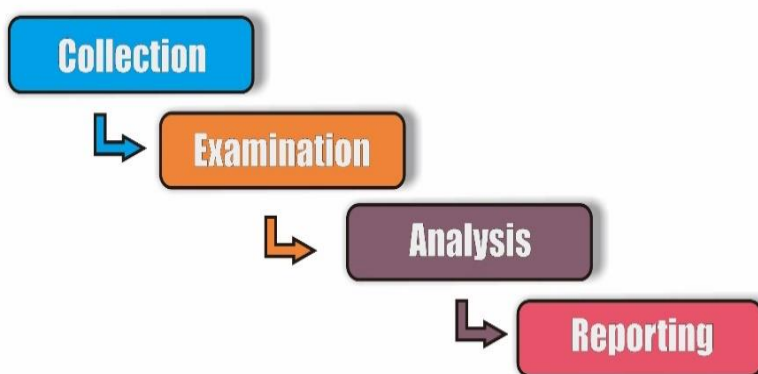


Figure 3. NIST method stages

National Institute of Standards and Technology (NIST) method has a collection, examination, analysis, and reporting stages as follow:

1. Collection
This stage of the collection is the stage of collecting data, identifying data, labeling data, recording data, and retrieving data from the original data source i.e. with smartphone devices, by maintaining the integrity of the original data.
2. Examination
This examination stage is the examination stage of data that has been collected through forensic means using automatic or manual data that digital forensics needed while maintaining data integrity.
3. Analysis
This analysis stage analyzes the results obtained by using legally and technically lawful methods to obtain quality information and value for the benefit of investigators.
4. Reporting
This stage is the stage of reporting on the results obtained in the analysis, including describing the research carried out, explaining the forensic tools used, a series of selected stages, then determining the following action that must be taken. And provide suggestions and recommendations on the final research to improve procedures, forensic tools, policies, and other forensic aspects.

Scenario Process Case

The study was conducted by simulating a crime case of defamation committed by the sexes using Facebook Lite social media accounts. The simulation process is used to facilitate research in determining the stages of the forensic process that will occur against the case of defamation crimes. The flow of cases in the simulation process can be seen in the image below Figure 4.

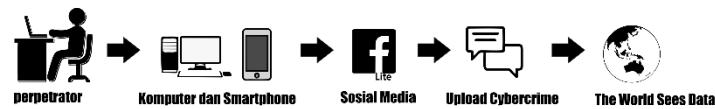


Figure 4. Crime scenarios

Based on the simulation of the case against the scenario of the case, there is a criminal message sending a criminal message by posting defamation using a Smartphone with the brand Samsung Galaxy J2 with model SM-J200G. The perpetrator created a Facebook Lite social media account from the Facebook lite account. The perpetrator posted or uploaded pictures or posts through the features in the social media app Facebook Lite. After the perpetrator uploads defamation in the form of a picture of the message or writing, the user immediately deletes the data to remove the existing evidence. Next, some feel aggrieved at what the perpetrator did and report directly to the authorities. And authorities immediately received a report to secure a Smartphone belonging to a user used to commit a crime on Facebook Lite social media. Furthermore, and on this smartphone, electronic evidence will be used. For policy steps that will be used next will be checked on the offender's smartphone. To be identified and restoring digital evidence in the form of messages, images, and audio that the perpetrator has deleted from the smartphone. Once the case is indicated, a defamation case can be committed in court. Based on the chronological simulation in the case, it can be put in the NIST method by going through the stages Collection, Examination, Analysis, and Reporting stages.

Comparison Method

Comparison using digital forensic tools based on each available forensic data. Comparisons to determine the results of quantitative numbers need to use the percentage formula in equation (1).

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

Information:

Par = Accuracy index figures on forensic tools that have been used

$\sum ar0$ = Number of material parameters detected

$\sum arT$ = Total number of material parameters used

RESULT AND DISCUSSION

Collection

The stage of collecting physical evidence against smartphones, namely digital evidence that will be needed to help collect digital evidence that will be expected. This research using Smartphones using the Android operating system with Samsung Galaxy J2 brand with model number SM-J200G can be seen in Figure 5.



Figure 5. Electronic proof smartphones

In this study, the electronic device to be used is a smartphone type using the Android operating system that has installed the Facebook Lite app is a social media communication tool that has been used for defamation crimes on social media. The data in the following polsel android will extract data by cloning data to not change data or the disappearance of data. The data will then be used as digital evidence in data acquisition through forensic tools such as Magnet Axiom and MOBILedit Forensics.

Examination

The test that will be carried out at this stage is testing the evidence of the forensic tool to be used, namely in the form of a smartphone. The data contained on a smartphone phone Forensic data will be taken using forensics tools to obtain the digital evidence data that has been expected. The first process is to back up all data through Imaging contents in the smartphone to be guarded the integrity of data so that there and did not make changes to forensic data from the original forensic data in carrying out research work. Figure 6 shows the process carried out using Axiom Magnet forensic tools.

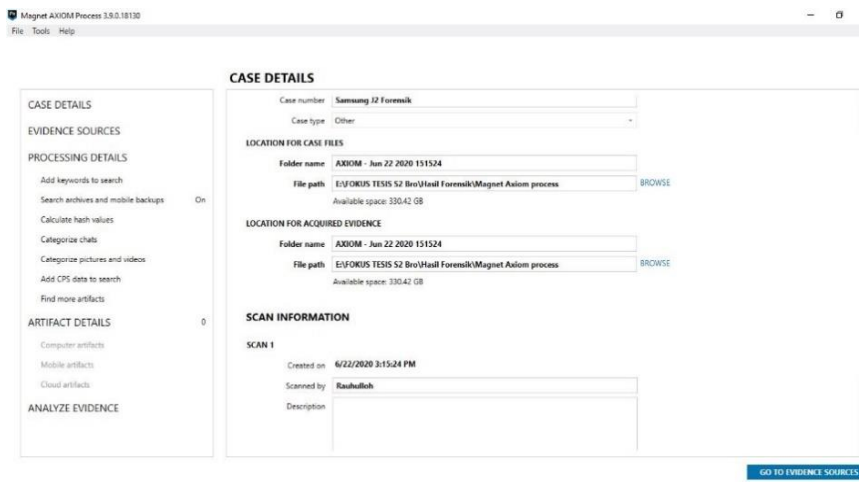


Figure 6. Examination magnet axion

Extract such data can be done if the smartphone electronic proof device has been connected using a USB data cable. Using a forensic Magnet Axiom Express tool installed on a computer then operating it automatically by searching for devices on a smartphone can be seen in the image above. The data imaging process at the next stage uses the Axiom Magnet forensic tools to produce the data results in the form of a complete image, as shown in Figure 7.

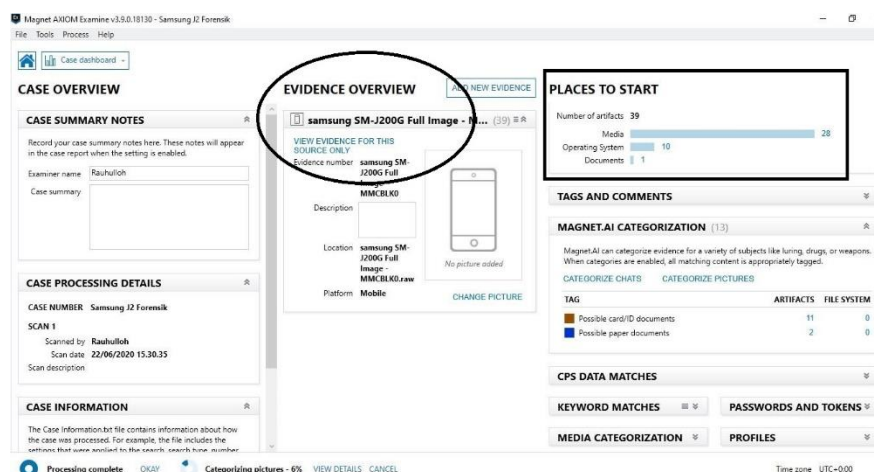


Figure 7. Full Image magnet axion

Image data using the forensic Magnet Axiom tool intended to back up data from a smartphone by cloning data to resemble the original data. The results of data processing through imaging are not intended to be

changed or added, or decreased. They can be opened through a designated forensic tool to perform digital data forensic examinations.

The result of the process that has been done by imaging the resulting data will be preserved in the form of a file using the type of data required in the study. Furthermore, in this stage, it can also be used to recover data that has been deleted, in this case depending on the ability of the forensic tools used to recover data or as data. To know in detail, there needs to be a comparison of other forensic tools that will be used to extract the data obtained. Here is an example of data extraction in other forensic applications, namely the Forensic MOBILedit tool as in Figure 8.

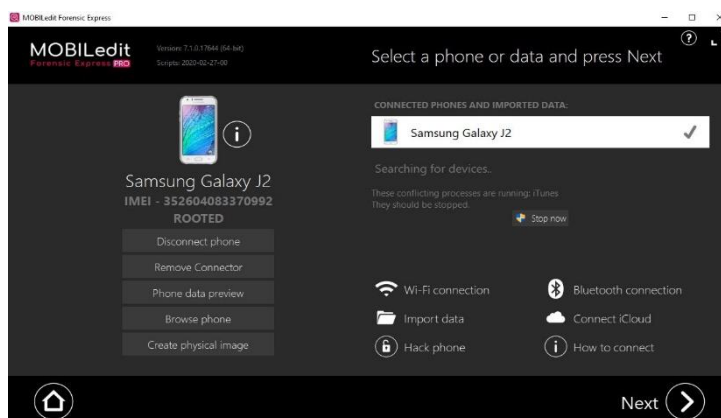


Figure 8. Process Imaging MOBILedit Forensic

Data extraction conducted by magnetic axiom tools and MOBILedit forensic has similarities to connecting a Smartphone with a USB cable and using forensic tool software inside a computer. Through the features available in the forensic tool, data processing can be done in the forensic software will get results on the data in the form of image, text, or audio files. Extraction on the Galaxy J2 Smartphone is a digital electronic evidence tool belonging to the perpetrator that aims to obtain digital forensic evidence in the form of images, text, and audio. The use of these two forensic tools can produce the data needed in the smartphone, which then in the next stage can be analyzed and can become a valid digital evidence report. The process conducted in this study is offline, where smartphones connected to the computer use USB cables and use forensic tools that are already installed on a computer.

Analysis

Then in the following analysis stages are the stages to determine the results of the previous process in the stage of looking for digital evidence in detail in the process carried out earlier [19]. The test results using the Forensic Axiom Magnets can get results from some data from an image that has been done, which has been successfully obtained through a predetermined forensic tool. In Figure 9, you can see the results of the tests that have been carried out by obtaining digital forensic data.

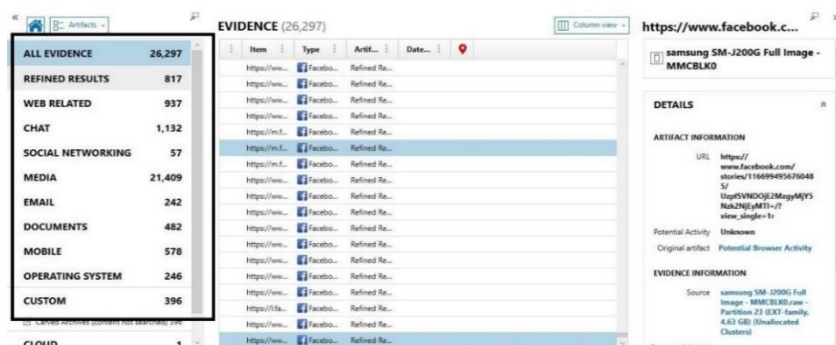


Figure 9. Analysis magnet axiom

The results that have been extracted using magnetic axiom forensic software are found in All Evidence, Web, Chat, Social Network, Media, email, and document. This picture shows as a form of digital evidence

by getting the results from the Axiom Magnet software. Axiom magnet software will analyze photos, text, media, time, and the Facebook lite account itself. Successful data will be used as digital evidence. The analysis MOBILedit forensic can be shown in Figure 10.



Figure 10. Analysis MOBILedit forensic

In figure 10, analysis results obtained from forensic software data MOBILedit Forensic in the form of the content report and can know the content of the message, type of message, Account ID, but the display on MOBILedit forensic express software is different from magnet axiom application. It will make the digital evidence by comparing each forensic tool of the two forensic tools determined.

Reporting

The Reporting Stage describes the stages of the completed analysis results. This stage analyzes Facebook lite account data in the form of Version Info, Application Size, Cache Files, Accounts, Facebook IDs, Pictures, Audio, Videos, RAM Usage, Photos, Conversations, Delete Posts, URLs, and Emails. There are not as many detailed parameters as forensic tools. Table 1 shows the success data from the results of the two forensic software.

Table 1. Results of analysis of both forensic software

No.	Detail Parameter	Tools Forensic	
		MOBILedit Forensic Express Pro	Magnet Axiom Forensics
1.	Version Info	V	X
2.	Application Size	V	X
3.	Chace File	V	X
4.	Account	V	V
5.	Facebook ID	V	V
6.	Images	V	V
7.	Audio	V	V
8.	Video	V	V
9.	RAM Usage	V	X
10.	Photo	X	V
11.	Convertation	V	X
12.	Delete Post	V	X
13.	URL	X	V
14.	Email	V	V

The overall results can be obtained based on tracing with digital evidence available by investigators and using forensic tools parameters determined as evidence. Furthermore, the measurement of the accuracy index to measure the ability of each tool can be calculated using the following formula [20] in equation (2) and equation (3).

$$\text{Magnet Axiom Forensic} \quad Par = \frac{\sum^8}{\sum^{14}} \times 100 \% = 57.14\% \quad (2)$$

$$\text{MOBILedit Forensic Express Pro} \quad Par = \frac{\sum^{12}}{\sum^{14}} \times 100 \% = 85.71\% \quad (3)$$

In the calculation and label above is digital evidence obtained using these forensic tools. Digital forensic evidence has been obtained and analyzed the specification of the parameters of the tools to be used. Each predetermined parameter will be compared with the two forensic tools: Axiom Forensic forensic tool and MOBILedit Forensic.

Based on the results of comparisons on digital evidence, it is known that the forensic tools have a MOBILedit forensic tool whose level of completeness is more specific than the Axiom Forensic forensic tools. Magnet Axiom Forensic has an axiom index of 57.14%, while MOBILedit Forensic has an accuracy index of 85.71%.

CONCLUSION

The study matched the performance results of each digital forensic tool from a Facebook lite app that had been installed on a Samsung Galaxy J2- SM-J200G smartphone. The forensic process stage uses NIST mediate through collection, examination, analysis, reporting. Data from applications Magnet Axiom Forensic 57.14%, while MOBILedit Forensic is 85.71%. For research development, it is recommended to add various types of forensic tools and add research methods to obtain so that the data is more reliable as digital forensic evidence.

REFERENCES

- [1] 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.
- [2] Masanam, S. Lakshmi, and P. Rajesh, "A Forensic Approach to perform Android Device Analysis," *Int. Int. J. Recent Technol. Eng.*, vol. 7, no. 6, pp. 227–234, 2019.
- [3] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3991–4003, 2018.
- [4] I. Riadi, A. Fadlil, and A. Fauzan, "A study of mobile forensic tools evaluation on android-based LINE messenger," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 10, pp. 201–206, 2018.
- [5] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 3–8, 2017.
- [6] I. Riadi, A. Yudhana, and M. C. F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," *Sci. J. Informatics*, vol. 5, no. 2, pp. 235–247, 2018.
- [7] I. Firdonsyah, A., & Riadi, "Analisis Forensik Bukti Digital Blackberry Messenger Pada Android," in *Cyber Learning & It Computer Karawang*, 2016, pp. 25–29.
- [8] E. Akbal, I. Baloglu, T. Tuncer, and S. Dogan, "Forensic Analysis of BIP Messenger on Android," *Aust. J. Forensic Sci.*, vol. 52, no. 5, pp. 590–609, 2019.
- [9] A. Yudhana, A., Umar, R., & Ahmadi, "Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ)," *J. CorellIT*, vol. 4, no. 1, pp. 8–13, 2018.
- [10] S. Jey Yang and J. Ho Choi, "Acquisition of main memory data from Android smartphones and smartwatches," *Digit. Investig.*, vol. 23, pp. 50–62, 2017.
- [11] F. G. Hikmatyar, "Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases," *Int. J. Informatics Dev.*, vol. 7, no. 2, pp. 64–67, 2018.
- [12] I. Yadi and Y. Kunang, "Analisis Forensik Pada Platform Android," in *Konferensi Nasional Ilmu Komputer (KONIK)*, 2014, pp. 141–148.
- [13] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilmu Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, pp. 1–10, 2017.
- [14] A. Yudhana, I. Riadi, and I. Zuhriyanto, "Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)," *Techno (Jurnal Fak. Tek. Univ. Muhammadiyah Purwokerto)*, vol. 20, no. 2, pp. 125–130, 2019.
- [15] R. Umar, I. Riadi, and G. Zamroni, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, pp. 69–75, 2017.
- [16] I. Riadi, A. Yudhana, and M. C. . Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)," *JUTISI J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 219–227, 2018.
- [17] R. Rizal, I. Riadi, and I. Prayudi, "Network Forensics for Detecting Flooding Attack on Internet of

- Things (IoT) Device,” *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 4, pp. 382–390, 2018.
- [18] F. Norouzizadeh Dezfouli, A. Dehghantanha, B. Eterovic-Soric, and K. K. R. Choo, “Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms,” *Aust. J. Forensic Sci.*, vol. 48, no. 4, pp. 469–488, 2016.
- [19] M. Haryanto, I. Riadi, and Y. Prayudi, “Forensics Acquisition and Analysis Method of IMO Messenger,” *Int. J. Comput. Appl.*, vol. 179, no. 47, pp. 9–14, 2018.
- [20] A. Marfianto and I. Riadi, “WhatsApp Messenger Forensic Analysis Based on Android Using Text Mining Method,” *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 3, pp. 319–327, 2018.