Digital Forensic Analysis of Online Dating Applications on Android Using the Digital Forensic Research Workshop 2001 Investigation Model

1st Nafiz Feizal Mahendra
Cybersecurity Engineering
Politeknik Siber dan Sandi Negara
Bogor, Indonesia
nafiz.feizal@student.poltekssn.ac.id

2nd Rizka Khairunnisa
Cryptographic Hardware Engineering
Politeknik Siber dan Sandi Negara
Bogor, Indonesia
rizka.khairunnisa@bssn.go.id

Abstract—**One kind of internet dating service used to find a partner is Tantan and Omi. Tantan and Omi application users are required to enter and display personal data in the form of name, age, photo, origin, and gender to provide information to other users about the partner being sought. This provides an opportunity for criminals to utilize the Tantan and Omi applications to launch their crimes. Crimes can be uncovered with digital evidence obtained by conducting digital forensics on the device used. The research was performed using the Digital Forensic Research Workshop (DFRWS) investigation model with the implementation of three research scenarios. The forensic process is assisted by using the MOBILedit Forensic tool to identify and find digital evidence. The results of the digital evidence found have an accuracy of 85.7% in scenario 1 Tantan, 57.1% in scenario 2 Tantan, 0% in scenario 3 Tantan, and 100% in scenario 1 Omi, 100% scenario 2 Omi, and 0% scenario 3 Omi.**

Keywords—Tantan, Omi, Digital Forensic, DFRWS Investigation Model, MOBILedit Forensic, Digital Evidence.

I. INTRODUCTION

An online dating app is an application on a smartphone that is used to search for and find a partner [1]. The popularity of online dating apps increased significantly from 2017 to 2021; in 2021, there were 323.9 million active users on online dating apps [2]. Online dating apps have a variety of functions that are unique to their users; for example, the matching feature between users based on interests, location, preferences, and gender [3]. In using the application, users must provide personal information such as name, age, photo, gender, and place of residence.

Online dating apps can harm their users through security risks that arise because most dating apps are designed with poor security systems [4]. They are also often used by criminals to perpetrate their crimes. This is because the use of online dating apps is used as an attempt to establish a physical and face-to-face relationship after communicating online [5]. Based on a survey conducted by the Australian Institute of Criminology (AIC) and participated in by 9,987 respondents of online dating applications, three out of four respondents admitted that they experienced sexual violence from partners who had just met through online dating applications, and 12.4% of the entire sample of respondents reported that there were requests for sexual exploitation of children on online dating applications in the last five years [6]. In October 2022, there was a case of the rape of a student from Madiun by a meatball seller known from the Tantan application [7]. Then, in November 2022, there was a case of the theft of a motorcycle by a woman from Kediri who was originally known from the Omi application [8].

To investigate criminal cases such as those that occur on online dating applications, forensic analysis is needed to obtain digital evidence that can be used as valid evidence in court proceedings. This is explained in Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008, where Article 5 paragraph (1) states that Electronic Information and/or electronic documents and/or their printouts are valid legal evidence [9].

Forensic analysis of Tantan and Omi applications on Android-based smartphone devices has the aim of finding digital artifacts, which are then analyzed into digital evidence. Digital artifacts are digital information that can be such things as text, images, sound, video, and various other types of digital data [10]. The stages used in this research use the Digital Forensic Research Workshop (DFRWS) Road Map investigation model. This investigation model was established at the first open workshop devoted to digital forensics in 2001 by the DFRWS organization [11]. The workshop produced a consensus document entitled A Road Map for Digital Forensic Research, which contained a model of the digital forensic science investigation process consisting of six stages.

II. LITERATURE REVIEW

A. Digital Forensic

Digital forensics is a branch of forensic science that deals with legal evidence that is still contained in digital storage media [12]. Digital forensics is also said to be a scientific methodology for identifying, searching and retrieving, and analysing evidence from computer storage media or other electronic devices and presenting the findings according to standards set by the court. The term digital forensics was originally synonymous with computer forensics, but today, the term has expanded to all devices that can store digital data [13].

B. Mobile Forensics

Mobile Forensics is one type of forensic science branch related to the recovery of digital evidence in the form of data from mobile devices [14]. This type of forensics will study the investigation, analysis, recovery, and management of data from digital media after a criminal offense. Mobile forensics will help the process of collecting digital data on cell phones in the form of text messages, call logs, media files, browsing history, GPS location, and so on without having to sacrifice the integrity of the data [15].

C. Digital Evidence

Digital evidence and digital forensics are two things that are interrelated, but both have different definitions or

meanings. Digital evidence will be found after the digital forensics process. Digital evidence from the acquisition must be well documented to be used as evidence in court. This digital evidence in Law No. 11 of 2008 concerning Electronic Information and Transactions is known as electronic information and electronic documents [16].

D. DFRWS 2001 Investigation Model

The Digital Forensic Research Workshop (DFRWS) is the first forensic investigation model formulated at the first workshop in 2001 [11]. The formulation produced a consensus document, A Road Map for Digital Forensic Research. DFRWS is a digital forensic science that relies on a method and has been scientifically proven to provide efficient steps or stages to support the digital evidence cycle [17]. These stages consist of Identification, Preservation, Collection, Examination, Analysis, and Presentation.

Fig. 1. DFRWS Investigation Process [11]

E. Tantan

Tantan is an online dating application developed by Tencent, a Chinese multinational technology company, in June 2014 [18]. Privacy management is used by Tantan by enforcing strict rules when choosing trusted people to maintain the privacy of their data [19].

F. Omi

Omi is an online dating application that can help someone find a partner. This application originated in Singapore and was released in 2019 by Wink Technology [20]. The app has excellent features, namely Match, Dating Quiz, Omi Clic, and Telepath. The feature matches ideas, interests, and similar moods between other users. Omi provides free, premium, and supreme service categories for its users to get different features from each of the available services.

G. MOBILedit Forensic

MOBILedit Forensics is a forensic tool that can be used to perform data acquisition from smartphone devices, smartwatches, and the cloud [21]. The data acquisition process can be done physically or logically. The way to use this forensic tool is quite simple: by connecting the smartphone to be used for forensics, MOBILedit Forensics will extract all data and produce a forensic report that is ready to be presented in court [22].

III. METHODOLOGY

The research was conducted using the research engineering stages and the Digital Forensic Research Workshop (DFRWS) investigation model.
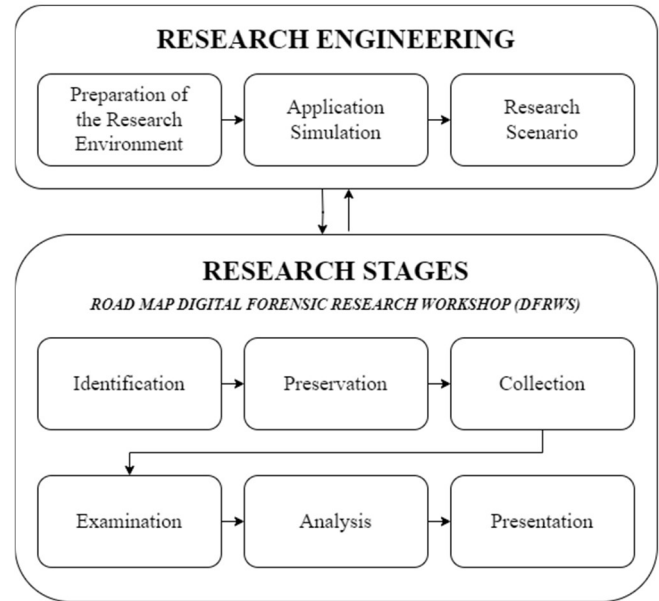

Fig. 2. Research Methods

The research stages were carried out using MOBILedit Forensic tools used in the Collection and Examination stages. The devices and tools used and required in the research are outlined in Table I.

TABLE I. SOFTWARE AND HARDWARE

Software/ Hardware	Function	Description
Lenovo S340	Device for forensic analysis.	Windows Version: 11 64-bit Processor: AMD Ryzen 3 RAM: 8GB
Samsung Galaxy J4	Primary device for Tantan and Omi installation.	Android Version: 10 RAM: 2GB Internal Storage: 32GB Root: Yes
Tantan	Target of forensic analysis.	Version 5.6.9.1
Omi	Target of forensic analysis.	Version 6.27.2
USB Cable	Connector cable for mobile device on PC.	USB Type Micro
Tool MOBILedit	Forensic acquisition and analysis tools.	Version 7.4

IV. RESULT AND ANALYSIS

A. Research Engineering

Research engineering is carried out to form a set of steps to support developing research designs. In this stage, a scenario will be produced that will be used in testing.

1. Preparation of the Research Environment

Prepare a forensic device, namely a Lenovo S340 Laptop that is installed with MOBILedit Forensic tools. Then, the Samsung Galaxy J4 android smartphone device as a forensic target that is already rooted and installed Tantan and Omi.

2. Application Simulation

The initial simulation process is carried out by creating an account for each Tantan and Omi.

The victim and perpetrator will do these things below when using Tantan and Omi.

- Send and receive text messages.
- Send and receive photo messages.
- Send and receive video messages.
- Send and receive voice messages.
- Send and receive location via Google Maps.
- Make voice calls.
- Swipe friends and match friends.

Next, the process of searching and matching users in Tantan and Omi and then the swipe friend feature is run to bring the two users together so that the scenario can be run.
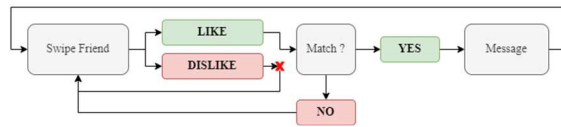

Fig. 3.   Flow of Application Simulation

After the two users meet and can send messages to each other, the message is sent by the two users according to the message scenario in Fig. 4.
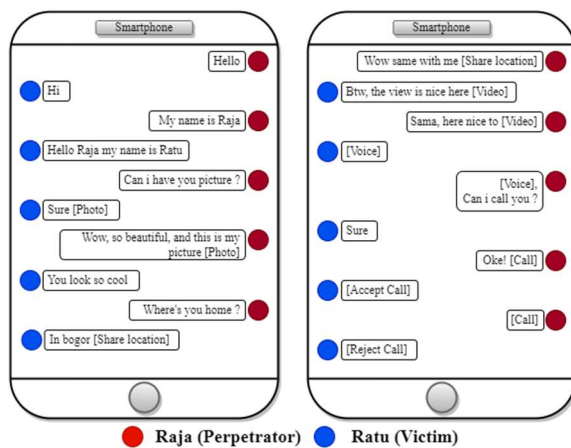

Fig. 4.   Message Scenario

Several image and video files used for sending messages between users have been prepared for the message scenario.

3. Research Scenario

Three scenarios are used in this research, as listed in Table II. The scenarios are run sequentially on the perpetrator's device, from Tantan to Omi.

TABLE II.   RESEARCH SCENARIOS

Name	Condition
Scenario 1	No data deleted
Scenario 2	Message history deleted
Scenario 3	Data and cache are deleted through the application manager settings

B. Research Stages

1. Identification

The identification process is carried out to collect data and resources needed during the evidence investigation. This process is done by checking the smartphone's hardware, software, and settings. In this stage, the smartphone's specifications and conditions are obtained.

2. Preservation

The preservation stage is a stage that aims to ensure and maintain the integrity of evidence or data that has been found so that it does not change and is damaged. This process is carried out by :

- Take pictures and videos of all the evidence.
- Disconnect all network connections and activate airplane mode.
- Turn off the device to save the remaining battery life and secure the device.
- Isolate the evidence by storing it in a safe place where it can only be accessed by the authorized party.

In this stage, the smartphone is secured and unconnected.

3. Collection

It is the acquisition process of digital evidence that has been secured at the preservation stage. The method used is logical acquisition by making acquisitions only in the Tantan and Omi research scenarios. The logical acquisition process is carried out by connecting the smartphone and laptop using the analysis application feature of MOBILedit Forensic, as seen in Fig. 5.
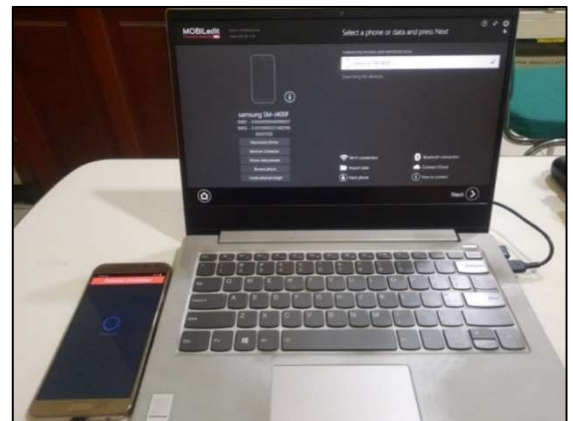

Fig. 5.   Collection Stage

The smartphone is connected while it is on and in airplane mode. This stage produces 6 data consisting of 3 data from Tantan and 3 data from Omi, as seen in Fig. 5. The resume of this stage is stated in the Report.pdf file. The example of the Report.pdf file is shown below in Fig. 6.

Scenario 1 Omi (2023-05-29 19h51m25s)	06/07/2023 08:54	File folder	
Scenario 1 Tantan (2023-05-29 20h01m12s)	06/07/2023 08:54	File folder	
Scenario 2 Omi (2023-05-30 07h01m53s)	06/07/2023 08:54	File folder	
Scenario 2 Tantan (2023-05-30 06h50m54s)	06/07/2023 08:54	File folder	
Scenario 3 Omi (2023-05-30 19h02m09s)	06/07/2023 08:55	File folder	
Scenario 3 Tantan (2023-05-30 18h49m20s)	06/07/2023 08:55	File folder	

Fig. 6.   Result of Collection Stage

Fig. 7.   Report.pdf file

4.   Examination

The examination stage is carried out by checking the Report.pdf file as a resulted in the collection stage and selecting specific data, which becomes the digital evidence. As seen in Fig. 8, a description media file that includes the file name, file location, file size, URL link, and file source is also available for examination.

Filename	e7hcFC6tqFlvzRCj3XE5Df5DknM.cnt
Path	phone/applications0/sg.omi/live_external/cache/imagepipeline_cache/v2.ols100.1/10/e7hcFC6tqFlvzRCj3XE5Df5DknM.cnt
Size	11.7 KB
Modified	29/04/2023 22:09:51 (UTC+7)
Accessed	29/04/2023 22:09:51 (UTC+7)
Width	960 px
Height	1200 px
Format	webp

Fig. 8.   Description Media File Example

Then, the digital evidence is classified based on the following scenarios.

a.   Scenario 1 (Data not deleted)

Forensic results from scenario 1 on Omi, all data can be recovered, while on Tantan, there is data that cannot be found, namely the call history made by the perpetrator and victim. The scenario 1 result is listed in Table III.

TABLE III.   SCENARIO 1 RESULT

File Type	App	Total	Description
Photo	Tantan	4	• 1 Profile photo Perpetrator • 1 Profile photo Victim • 1 Photo Perpetrator • 1 Photo Victim
	Omi	4	• 1 Profile photo Perpetrator • 1 Profile photo Victim • 1 Photo Perpetrator • 1 Photo Victim
Video	Tantan	2	• 1 Video Perpetrator • 1 Video Victim
	Omi	2	• 1 Video Perpetrator • 1 Video Victim
Voice	Tantan	2	• 1 Voice Note Perpetrator • 1 Voice Note Victim
	Omi	2	• 1 Voice Note Perpetrator • 1 Voice Note Victim
Text	Tantan	16	• 9 Conversation message Perpetrator • 7 Conversation message Victim
	Omi	16	• 9 Conversation message Perpetrator • 7 Conversation message Victim
Location	Tantan	2	• 1 Location Perpetrator • 1 Location Victim
	Omi	2	• 1 Location Perpetrator • 1 Location Victim
Call Log	Tantan	-	-
	Omi	2	• 1 Incoming calls • 1 Missed calls

b.   Scenario 2 (Clear chat history)

Forensic results from scenario 2, listed in Table IV, show that on Omi, all data can be recovered. At the same time, on Tantan, there is data that cannot be found, namely chat history, location, and calls made by the perpetrator and victim.

TABLE IV.   SCENARIO 2 RESULT

File Type	App	Total	Description
Photo	Tantan	4	• 1 Profile photo Perpetrator • 1 Profile photo Victim • 1 Photo Perpetrator • 1 Photo Victim
	Omi	4	• 1 Profile photo Perpetrator • 1 Profile photo Victim • 1 Photo Perpetrator • 1 Photo Victim
Video	Tantan	2	• 1 Video Perpetrator • 1 Video Victim
	Omi	2	• 1 Video Perpetrator • 1 Video Victim
Voice	Tantan	2	• 1 Voice Note Perpetrator • 1 Voice Note Victim
	Omi	2	• 1 Voice Note Perpetrator • 1 Voice Note Victim
Text	Tantan	-	-
	Omi	16	• 9 Conversation message Perpetrator • 7 Conversation message Victim
Location	Tantan	-	-
	Omi	2	• 1 Location Perpetrator • 1 Location Victim

Call Log	Tantan	-	-
	Omi	2	• 1 Incoming calls • 1 Missed calls

c. Scenario 3 (Delete data and cache)

The forensics from scenario 3 show no results from either Tantan or Omi. Table V shows this empty result.

TABLE V.   SCENARIO 3 RESULT

File Type	App	Total	Description
Photo	Tantan	-	-
	Omi	-	-
Video	Tantan	-	-
	Omi	-	-
Voice	Tantan	-	-
	Omi	-	-
Text	Tantan	-	-
	Omi	-	-
Location	Tantan	-	-
	Omi	-	-
Call Log	Tantan	-	-
	Omi	-	-

5. Analysis

From the examination stage, it can be concluded as described below.

- MOBILedit Forensic can recover undeleted and deleted data from Omi.
- MOBILedit Forensic can recover undeleted and deleted data from Tantan, except the call log.
- MOBILedit Forensic cannot recover data if the application is in precise data and cache condition.

The success of data recovery can be seen by comparing the file results obtained in scenarios 1 and 2, as listed in Table 6 below.

TABLE VI.   DIGITAL EVIDENCE COMPARISON

6. Presentation

In this stage, a summary of the anlysis results presented in Table VII below. The summary is shown based on the simulation conducted by the perpetrator and victim based on the parameters.

TABLE VII.   DIGITAL EVIDENCE BY PARAMETER

Evidence	Scenario Tantan			Scenario Omi		
	1	2	3	1	2	3
File Photo	√	√	x	√	√	x
File Video	√	√	x	√	√	x
File Voice	√	√	x	√	√	x
Swipe Friend	√	√	x	√	√	x
Location	√	x	x	√	√	x
Message Text	√	x	x	√	√	x
Voice Call	x	x	x	√	√	x

The calculation of the accuracy index of the digital evidence obtained from each scenario is carried out with the following formula [23].

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

Desc :
Par = Percentage of the scenario
$\sum ar0$ = Digital evidence found
$\sum arT$ = Digital evidence total

Based on calculating the accuracy of each forensic scenario using the MOBILedit Forensic tool, the data is obtained as in Table VIII. The accuracy index value is only a reference for information on how much results have been obtained from digital forensic analysis of the Tantan and Omi.

TABLE VIII.   ACCURACY INDEX VALUE

Tools	Application	Scenario	Accuracy Index Value
MOBILedit Forensic	Tantan	1	85,7%
		2	57,1%
		3	0%
	Omi	1	100%
		2	100%
		3	0%

V. CONCLUSIONS

Digital evidence can be found from crime scenarios in Tantan and Omi using MOBILedit Forensic tools by logical acquisition methods. It can be obtained and recovered as long as the data and cache are not deleted from the application manager. The outcomes show that the data in scenario 1 and 2 of Omi can be 100% recovered. Tantan has different results in scenario 1 and 2, where scenario 1 has a result of 85.7% and scenario 2 gets a result of 57.1%. In scenario 3 no results are obtained for both applications, which means that the data has been completely blocked and cannot be acquired with MOBILedit Forensic tools by logical acquisition methods. It is easier to recover data from Omi than Tantan. With these results, it is hoped that it can become a reference and help forensic investigators find digital evidence from similar scenarios.

This research has a limitation in that it cannot find a definite reason why the results are different among Tantan and Omi. This may be due to the internal condition and programming of these two applications, considering that the same device and forensic tools are used. Further study may be conducted to find the reason. Also, it is necessary to construct more scenarios and do the test on similar dating applications.

REFERENCES

[1] L. Portolan and J. McAlister, "Jagged Love: Narratives of Romance on Dating Apps during COVID-19," *Sex Cult*, vol. 26, no. 1, pp. 354–372, Feb. 2022, doi: 10.1007/s12119-021-09896-9.

[2] M. A. Rizaty, "Pengguna Aplikasi Kencan Online Tembus 323 Juta Orang pada 2021," 2022. https://databoks.katadata.co.id/datapublish/2022/02/14/pengguna-aplikasi-kencan-online-tembus-323-juta-orang-pada-2021 (accessed Dec. 13, 2022).

[3] S. Knox, S. Moghadam, K. Patrick, A. Phan, and K. K. R. Choo, "What's really 'Happning'? A forensic analysis of Android and iOS Happn dating apps," *Comput Secur*, vol. 94, Jul. 2020, doi: 10.1016/j.cose.2020.101833.

[4] R. Shetty, G. Grispos, and K.-K. R. Choo, "Are You Dating Danger? An Interdisciplinary Approach to Evaluating the (In) Security of Android Dating Apps," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 2, pp. 197–207, Dec. 2017, doi: 10.1109/tsusc.2017.2783858.

[5] A. Phan, K. Seigfried-Spellar, and K. K. R. Choo, "Threaten me softly: A review of potential dating app risks," *Computers in Human Behavior Reports*, vol. 3. Elsevier Ltd, Jan. 01, 2021. doi: 10.1016/j.chbr.2021.100055.

[6] C. Teunissen, H. Boxall, S. Napier, and R. Brown, "The sexual exploitation of Australian children on dating apps and websites," 2022.

[7] S. Harianto, "Mahasiswi Asal Madiun Diperkosa Penjual Pentol yang Dikenal Lewat Tantan," 2022. https://www.detik.com/jatim/hukum-dan-kriminal/d-6376689/mahasiswi-asal-madiun-diperkosa-penjual-pentol-yang-dikenal-lewat-tantan (accessed Nov. 16, 2022).

[8] A. Saichu, "Kenalan Lewat Aplikasi OMI, Motor Wanita Kediri Dibawa Kabur Pria Nganjuk - Koran Memo," Nov. 13, 2022. https://www.koranmemo.com/daerah/pr-1925574307/kenalan-lewat-aplikasi-omi-motor-wanita-kediri-dibawa-kabur-pria-nganjuk (accessed Nov. 16, 2022).

[9] *Undang-Undang No.19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*. 2016.

[10] B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations: Processing Digital Evidence*, 6th Edition., vol. Six Edition. 2019.

[11] G. L. Palmer, "A Road Map for Digital Forensic Research," *Technical Report (DTR-T001-01) for Digital Forensic Research Workshop (DFRWS)*, 2001.

[12] R. Meiyanti and Ismaniah, "Perkembangan Digital Forensik Saat Ini dan Mendatang," *Jurnal Kajian Ilmial UBJ*, vol. 15, no. 2, Sep. 2015.

[13] N. Aisyah *et al.*, "Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review," *Jurnal Esensi Infokom*, vol. 6, no. 1, p. 22, May 2022.

[14] F. Gustav Hikmatyar and B. Sugiantoro, "Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases," *International Journal on Informatics for Development (IJID)*, vol. 7, no. 2, pp. 64–67, 2018.

[15] S. C. Sathe and N. M. Dongre, "Data Acquisition Techniques in Mobile Forensics," *Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018)*, 2018.

[16] *Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. 2008.

[17] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, "Mobile Forensics: Advances, Challenges, and Research Opportunities," 2017. [Online]. Available: www.computer.org/security

[18] Anonymous, "Tantan," 2020. https://tantanapp.com/en/about (accessed Dec. 02, 2022).

[19] A. E. S. Murwani, "Manajemen Privasi Dalam Aplikasi Tantan (Kajian Gendered Criteria dalam Teori Communication Privacy Management)," *Jurnal Professional FIS UNIVED*, vol. 7, no. 2, Dec. 2020.

[20] Anonymous, "Omi - Dating, Friends & More," 2022. https://omi.sg/why (accessed Nov. 22, 2022).

[21] Anonymous, "Forensic Express — MOBILedit," 2022. https://www.mobiledit.com/forensic-express (accessed Dec. 02, 2022).

[22] M. Wazid, A. Katal, R. H. Goudar, and S. Rao, "Hacktivism Trends, Digital Forensic Tools and Challenges: A Survey," *Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013)*, p. 1326, 2013.

[23] A. Yudhana, I. Riadi, and R. Y. Prasongko, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," *Jurnal Informatika: Jurnal pengembangan IT (JPIT)*, vol. 7, 2022.