Ghufron Zaida Muflih

by Jiko jurnal

Submission date: 12-Mar-2023 11:31PM (UTC-0400)
Submission ID: 2014770803
File name: 5872-15751-1-SM.docx (1.68M)
Word count: 4160
Character count: 23957

JIKO (Jurnal Informatika dan Komputer)
Vol. x, No. x, April 2019, hlm. x-x
DOI: 10.33387/jiko

AccreditedKEMENRISTEKDIKTI, No.36/E/KPT/2019
p-ISSN: 2614-8897
e-ISSN: 2656-1948

Comparison of Forensic Tools on Social Media Services Using the Digital Forensic Research Workshop Method (DFRWS)

Ghufron Zaida Muflih[1], Sunardi[2], Imam Riadi[3], Anton Yudhana[4]

[1]Teknik Informatika, Fakultas Teknik, Universitas Ma'arif Nahdlatul Ulama Kebumen, Jawa Tengah
[2,4]Teknik Elektro, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta
[3]Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan, Yogyakarta
[1]ghufron.zaida@umnu.ac.id ,[2]sunardi@mti.uad.ac.id, [3]imam.riadi@mti.uad.ac.id, [4]eyudhana@mti.uad.ac.id

(Received: dd mmm yyyy, Revised: dd mmm yyyy, Accepted: dd mmm yyyy)

Abstract

Social media applications currently play a role and become part of various human activities, on the other hand social media is also very vulnerable to various crimes. Some crimes on social media can be in the form of hate speech, defamation, fraud, gambling, pornography, and other harmful actions. This research applies the Digital Forensic Research Workshop (DFRWS) method to search for all data on twitter social media services running on the Android operating system using MOBILedit Forensic Express and Belkasoft Evidence Center tools. Twitter social media services in this research are used for activities by utilizing all the features in it. Activities carried out by twitter users become evidence that will be acquired using MOBILedit Forensic Express and Belkasoft Evidence Center tools. From the two tools used, a comparison was obtained that MOBILedit Forensic Express found more data on twitter social media than Belkasoft Evidence Center, the findings in these two tools made several contributions to social media investigations that run on the android operating system.

Keywords: *Forensics, DFRWS, Twitter, MOBILedit, Belkasoft*

**Corresponding Author*: *Author1*

1. INTRODUCTION

The rapidly growing technology of Smart Devices or smartphones also has an impact on the development of various supporting applications to run on them, various applications for work and even entertainment are increasingly available on sales applications from the Operating system itself, such as social media [1], Social media plays a role and becomes part of various human activities such as socialising group chats, commercial activities, advertising media, education, and other creative content, on the other hand, it is prone to various crimes [2][3]. Twitter, which is one of the most widely used social media in Indonesia, reaches 19.5 million users [4], Twitter provides features allowing users to express their emotions, feelings, share whatever is around them quickly and easily [5]. Apart from being entertainment, social media also has the potential to become a place or medium for crime. Some types of crimes that occur on social media through smartphones can be in the form of hate speech, defamation, fraud, gambling, pornography, or other things that are detrimental [6]. Ministry of Communication and Informatics Twitter was reported through the content complaint channel in December 2018 [7], UNICEF reported in 2017 that 40% of Indonesian children were victims of bullying due to the impact of cyberaggression from social media use, 32% of children reported being physically abused [8].

According to data from 9 March to 14 April 2019, Indonesian internet users reached 171.17 million people or 64.8% of the total Indonesian population of 264.16 million people in 2018 (BPS projections), the contribution of the most users in Java 55.7%, followed by Sumatra 21.6%, Sulawesi-Maluku-Papua 10.9%, Kalimantan 6.6%, and Bali-NTT 5.2%. The most internet-connected devices are smartphones 93.9% per day, laptop computers 17.2% with a range of more than 8 hours. Harassment or bullying also occurs a lot on social media at 49%, pornographic content 55.9%. The main reason for using the internet is communication through messages with a portion of 24.7%, social media

18.9% and looking for job information 11.5%. Second as much as 19.1% to access social media, 16.4% for communication via messages and 15.2% to fill spare time, entertainment content that is often visited watching films / videos and playing video games, the most frequently visited social media is Facebook 50.7%, Instagram 17.8% YouTube 15.1% Twitter occupies the fourth position 1.7% [9]. Security is a challenge for forensic information technology and law enforcement to investigate devices used in a crime case [10]. Crimes will generally leave traces that can be used as evidence, which can be electronic or digital evidence [11].

Examples of crimes include manipulating email headers or forging emails sent with web hosting services [12]. This kind of case is a challenge for law enforcement and digital forensic experts to investigate a crime case, because there are many cases of deletion of criminal evidence to eliminate traces [13]. Some forensic frameworks or methods used to obtain digital evidence such as the Digital Forensics Research Workshop (DFRWS), even build frameworks by developing pre-existing ones and combining with specialised techniques for certain evidence, e.g. audio evidence [14]. Related to digital evidence research on social media twitter and facebook to find digital evidence related to several text and image uploads and compare the tools used [3]. In addition to the Android operating system also on Firefox OS with the results of evidence stored in volatile memory [15]. Knowing which tool to use to search for digital evidence on the device is important, although most tools provide reasonable evidence on one tool alone, it is also necessary to compare with other tools [16]. Forensic tools such as Belkasoft Evidence Centre for searching digital evidence such as locations, photos, messages or internet searches [17] or MobileEdit Forensics with some similar functions to Belkasoft Evidence Centre such as retrieving device information, application extraction, application analysis and data reporting [18].

This research implements the Digital Forensics Research Workshop (DFRWS) forensic analysis method. This method is to explain the stages of research to be carried out so that the steps and flow of research become systematic and can be used as guidelines in solving problems. In addition, it aims to find all the data in the Twitter social media application that runs on the Android operating system by applying the DFRWS method, and comparing the forensic tools MOBILedit Forensic Express and Belkasoft Evidence Centre. Forensic tools are used to retrieve data uploaded to the Twitter social media application by testing experimental scenarios in the form of adding image, video, and text data and performing several data deletions.

2. RESEARCH METHOD

2.1. Method

This research uses the Digital Forensics Research Workshop (DFRWS) method with six stages starting from the identification stage to the presentation stage. The use of the DFRWS method to carry out the preservation, validation, identification, analysis, interpretation, documentation and presentation processes of all digital evidence obtained to deepen the reconstruction of an event suspected of being a crime, in order to anticipate future crimes [19][20][21].

The stages of research using the DFRWS method as shown in Figure 1.

Figure 1. Stages of the DFRWS

The stages of the Digital Forensic Research Workshop (DFRWS) are divided into 6, with the following explanation:

1. Identification stage, by determining the needs required in the investigation of the case and the search for digital evidence.
2. The evidence maintenance stage, after the identification stage is completed with the aim of ensuring the authenticity of the evidence that has been obtained and can be used to refute if the evidence has been sabotaged.
3. The stage of collecting evidence that has been obtained previously and has gone through the maintenance stage. At this stage, certain parts of the digital evidence will be identified and the source data will be identified.
4. Examination of evidence that has been identified by determining data filters on certain parts of digital evidence and data sources, carried out by changing the shape of the data without changing the data content, with the aim of maintaining the authenticity of the data.
5. Analyse the data by determining how and where it was generated, by whom it was generated, and why it was generated.
6. Presentation is the final stage of the DFRWS method by presenting all the information that has been obtained from the analysis stage.

Digital evidence in this research is not obtained in the actual environment or the results of actual crimes. The acquisition of evidence is obtained from scenarios using Twitter and utilising all the features in it. The twitter social media application features used in the scenario are sharing images, text, videos, commenting, sending messages, and deleting them. The following scenario is carried out on a Twitter account as shown in Figure 2.

Figure 2. Usage scenario of twitter app

Preparation of equipment used for the forensic process or data retrieval from smartphones using software and hardware. Several devices used in the research are MOBILedit Forensic Express. Mobiledit Forensic Express tool allows to get data logically, check the contents of the device, system or device information even messages and contacts, create images, backups, and clone devices, using several USB and wireless connectivity mechanisms [22]. Another tool is Belkasoft Evidence Center, it can also be used to search, analyse and store digital evidence from smartphones or computers, retrieve digital evidence, such as device information, IMEI, can find more than 700 artefacts and 100 mobile applications [23][24] by analysing hard drives, memory dumps, and saving in a report [25].

3. RESULT AND DISCUSSION

3.1. Identification

Identification stage requires a smartphone that has been installed on twitter social media and has been used for various activities by utilising the features in it, which is the source of digital evidence search.

1. Smartphone Device

Smartphones as electronic evidence use an android operating system that has Twitter installed. Steps that need to be taken to avoid deleting or changing data on the device, can be cloned or full backup using MobileEdit Forensic, in table 1 below are the smartphone specifications used.

Table 1. Specifications of the smartphone device

No	*Manufacture*	*EVERCROSS detail model*
1	*Product*	B75
2	*HW Revision*	LMY47D
3	*Platform*	Android
4	*SW Revision*	5.1(22)
5	*Serial Number*	0123456789ABCDEF
6	*Unlocking Pattern*	3452
7	*IMEI*	358441061746404
8	*Rooted*	Yes
9	*SIM Card*	Yes
10	*Operator*	3, MCC:510, MNC:89
11	*IMSI*	510897263097260
12	*ICCID*	89628990007753870152

2. Twitter app

Microblogging with 554.7 million active users worldwide, 58 million collective "tweet" posts daily [26]. There are many services that can be used in it such as posting user information, connecting with influential people in the world, distant friends, sharing information, commenting, liking a post, sharing posts via private message, bookmarking, or sharing with other applications, search features, notifications, responding to certain posts, in the form of text, images, polls, and sharing locations [27].

3. Forensic tools

The use of forensic tools to retrieve digital evidence in the investigation process from smartphone devices as shown in Table 2.

Ttable 2. *Forensic tools that are used*

No	*Tools*	Version
1	MOBILedit Forensic Express	5.1.1
2	Belkasoft Evidence enter	Belkasoft Evidence Center 9.6 Build 3981 x64

3.1 Evidence Mintenance

The maintenance stage aims to maintain digital evidence or all data on the device. The maintenance stage is carried out by isolating or keeping the device from communication from outside to inside or vice versa, avoiding the installation of applications, uninstalling applications, adding or deleting data by parties who are not responsible or do not have authority. One way to do this is by enabling airplane mode on the device.

3.2 Collecting

The process of collecting digital evidence from the device by cloning the device, physical image, or full backup of the device to maintain authenticity. This stage uses MOBILedit Forensic Express and Belkasoft Evidence Centre forensic tools. At this stage, all communication from outside or inside the device is turned off to avoid hacking or deleting evidence.

3.4 Examination

The examination stage after the data collection stage is complete, from the MOBILedit Forensic Express and Belkasoft Evidence Centre tools, data is obtained from smartphone devices based on the features in twitter as in Table 3.

Table 3. Examination results with both tools

No	The results obtained	Tools	
		MOBILedit Forensic Express	Belkasoft Evidence Center
1.	*Application info*	√	×
2.	*Account info*	√	×
3.	*Twitter ID*	√	√
4.	*Friends*	√	×

5.	*User/ Follower/Following*	√	√
6.	*Conversation/Direst Messages*	√	√
7.	*Cached Search*	√	×
8.	*Audio*	×	×
9.	*Video*	√	×
10.	*Text*	√	√
11.	*Picture*	√	√
12.	*Deleted Messages/Tweets*	√	√
13.	*IP Adress*	×	×
14.	*url*	√	√
15.	*Email/Phone Number*	√	×
16.	*Location*	√	×

3.5 Analyse

The digital evidence that can be retrieved using MOBILedit Forensic Express and Belkasoft Evidence Centre is very limited. Not all of the data within the device or Twitter app was recovered and provided clear information and some data was unreadable.

1. MOBILedit Forensic Express

Using the MOBILedit Forensic Express tool, we obtained twitter application information with the installed version, application type, application size, data size, cache size, the first date Twitter was installed, updates and the last time Twitter was used as shown in the figure 3.

Label	**Twitter**
Package	**com.twitter.android**
Version	**8.13.0-release.00**
Application Type	**User Application**
Application Size	**50.1 MB**
Data Size	**8.1 MB**
Cache Size	**88.8 MB**
First Installed	**2019-07-16 16:32:30 (UTC+7)**
Last Updated	**2019-09-20 18:25:28 (UTC+7)**
Last Active	**2019-09-26 15:43:00 (UTC+7)**

Figure 3. Application information

Figure 4 shows the registered twitter account information such as twitter account name, ID, account description, number of followers, following, number of messages, and image or profile url.

Nickname	Wicakson8
Twitter ID	1151071365593628678
Description	J'-J!Karna Soto Ayam Tak Pernah Bohongl^\XIM^.XI^.X◆*◆*◆*XX
Number of Followers	4
Following	5
Favorites	12
Number of Messages	46
Created	2019-07-16 17:09:34 (UTC+7)
Modified	2019-09-26 17:09:15 (UTC+7)
Picture Url	https://pbs.twimg.com/profile_images/1176690821690576900/hFI

Figure 4. Account information

Other information that can be retrieved using MOBILedit Forensics Express is the friendship network information as shown in Figure 5.

Nickname	NHKWORLD_News
Twitter ID	546657547
Address (Google Maps)	Tokyo, Japan
Url	https://t.co/SQLqauwejw
Description	J'-j~NHK WORLD's official news account brings you current events from Japan, Asia and beyond. Terms of use: https://t.co/ThOWdGYROzH^.Mf.\'\-/\'.g\'.g\'.~J'-https://t.co/ThOWdGYROzjhttps://www3.nhk.or.jp/nhkworld/en/terms/8'-www3.nhk.or.jp/nhkworld/en/te... XXI\'.g\'.~XXII'.\'.◆◆XI'.XM'.X◆\'.◆\'.XX
Number of Followers	43043
Following	0
Number of Messages	43311
Modified	2019-09-25 10:37:34 (UTC+7)
Following User	✖ no
Followed by User	✔ yes
Picture Url	https://pbs.twimg.com/profile_images/781790577390039040/5-Umq3Kb_normal.jpg
Number of Messages	61

Figure 5. Friendship networking information

Figure 6 provides information on conversations with other users, the time of the conversation, as well as the contents of messages that are not read and there is a message deletion mark.

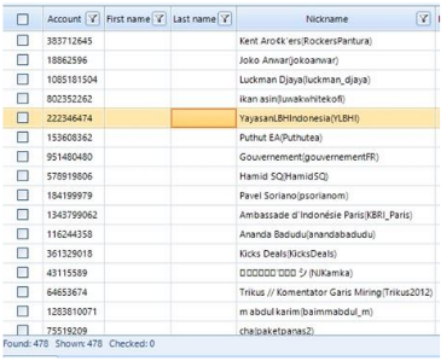
Figure 6. Conversation information

In addition to conversations, other data that can be retrieved from twitter is a cache of tweets or timeline which contains several information including the user's name, tweets or status uploaded, the date of uploading the tweet status, hastags, language, number of retweets or how much it is re-uploaded, links that lead to user tweets, as in Figure 7.

Figure 7. Other evidence obtained in the form of tweet caches

2. Belkasoft Evidence Center

The results of data retrieval using Belkasoft Evidence Centre obtained less information than retrieval using the MOBILedit Forensic Express tool as shown in Figure 8. Obtained some account ID information that shows the account name, as well as found how many accounts are connected.



Account	First name	Last name	Nickname
383712645			Kent Aro6k`ers(RockersPantura)
18862596			Joko Anwar(jokoanwar)
1085181504			Luckman Djaya(luckman_djaya)
802352262			ikan asin(juwakwhitekofi)
222346474			YayasanLBHIndonesia(YLBHI)
153608362			Puthut EA(Puthutea)
951480480			Gouvernement(gouvernementFR)
578919806			Hamid SQ(HamidSQ)
184199979			Pavel Soriano(psorianom)
1343799062			Ambassade d`Indonésie Paris(KBRI_Paris)
116244358			Ananda Badudu(anandabadudu)
361329018			Kicks Deals(KicksDeals)
43115589			□□□□□□ □□□ シ (NIKamka)
64653674			Trikus // Komentator Garis Miring(Trikus2012)
1283810071			m abdul karim(baimmabdul_m)
75519209			cha(paketpanas2)

Found: 478 Shown: 478 Checked: 0

Figure 8. Account Information

The next information is the form of conversation activity by the user, it can be read the message sent by the account owner, the date the conversation took place, the direction of outgoing and incoming conversations as in Figure 9.

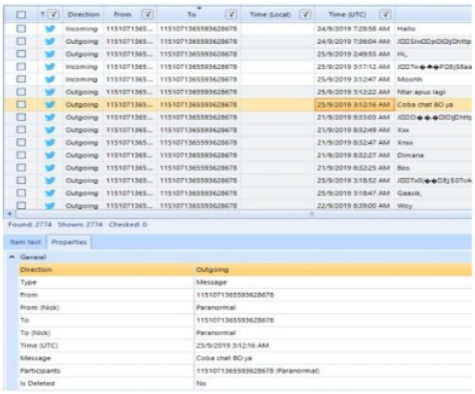


Figure 8. Informasi percakapan

Other data that was successfully obtained using Belkasooft is the email of several connected accounts, in addition to email there are several data such as links, telephone numbers, the number of followers of an account, the number of follows and the number of messages as in Figure 10.

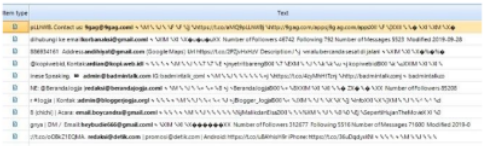


Figure 9. Informasi email akun

Other information shows that links that lead to account id and status sharing activities or other activities appear on the timeline as shown in Figure 11.

Figure 10. Account activity links

3.6 Presentation

Regarding user activities to be used as digital evidence, the results of data acquisition using MOBILedit Forensic Express and Belkasoft Evidence Centre have advantages and disadvantages. Examples of the results of obtaining data or information from each tool are presented in a table to make it easier to observe.

1. MOBILedit Forensic Express

The results of data retrieval using the MOBILedit Forensic Express tool are in the form of account info details, account names, friendships, other users who enter the timeline, conversations, private messages and phone numbers, as in Table 4.

Tabel 4. Data Retrieval Results from MOBILedit Forensic Express

Evidences	MOBILedit Forensic Express	*Result*
Detail Account info	Account	1
	User Account	Paranormal
	Friends	6
	Users	587
	Conversation	4 conversation, 23 messages, 1 deleted
	Cached Tweets	852, 13 deleted
	Messages	23, 1 deleted
	Cached Searches	2
	List of Analyzed files	8 files
Account Name (1)	Nickname	Wicasono8
	Twitter ID	1151071365593628678
	Description	J□j!Karna Soto Ayam Tak Pernah BohongI□□XIM□XI□X□*□*□*XX
	Follower	4
	Following	5
	Favorite	12
	Number of Messages	46
	Created Date	2019-07-16 17:09:34 (UTC+7)
	Modified Date	2019-09-25 10:40:25 (UTC+7)
	Picture ID	https://pbs.twimg.com/profile_images/1176690821690576900/hFbrBj3H_normal.jpg
Friends (6)	Nickname	fauzangustafi
	Twitter ID	2455017384
	Adress(google maps)	Boyolali
	Description	J□j□Bio : I'm Awesome!I□□XIM□XI□X□□□□□XX
	Number of Followers	26
	Following	36
	Number of Messages	174
	Modified	2019-09-25 09:48:43 (UTC+7)
	Following User	Ok
	Followed by User	Ok
	Picture URL	https://pbs.twimg.com/profile_images/653594881508577281/qEdYmv0d_normal.jpg
	Number of Messages	20
User (587)	Nickname	PartaiSocmed
	Twitter ID	869327120
	Adress(google maps)	Indonesia
	Url	https://t.co/aDu3oGTVHr
	Description	J□j□Social Media Party | Objectivity, Fairness and Justice for All | Non-Populist Party | Common Sense Party | Empowering People | No = 99I□□XIM□XI□X□□□□□□XX
	Number of Followers	173470
	Following	3007
	Number of Messages	352939
	Modified	2019-09-24 14:02:56 (UTC+7)
	Picture URL	https://pbs.twimg.com/profile_images/1137182440907108352/iFHhYIh-_normal.jpg
Conversation (4 convers, 23 messages, 1 delete)	Sent Message	N/A
	Received Message	N/A
	Draft	N/A
	Failed Message	N/A
	Unknown Message	N/A
	Deleted Message	OK
	Conversation ID	2455017384-1151071365593628678
	Date/ Time	2019-9-24 14:36:04 (UTC+7)
	Participants	Paranormal, Fauzan
Cached tweets (852, 13 deleted)	Status/ timeline	OK
	Nama Akun	Rudiantara (Rudiantara)
	Tanggal Update	2019-09-25 20:15:31 (UTC+7)
	Words Status	J□k□□Teman2, situasi sdh kondusif shg pembatasan akses fitur video & gambar pd medsos & instant messaging difungsikan kembali. Mari senantiasa jaga dunia maya digunakan unt hal2 yg positif. Mari perangi hoaks, fitnah, info2 yg memprovokasi spt yg banyak beredar saat kerusuhan kemarin.I□□XII□XI□XI□XI□XI□XXX
	Hastag	NOK
	Language	In
	Url	https://twitter.com/Rudiantara/status/1132273995712090113
	Favorites	4078
	Retweet Count	1299
	Deleted/ Received	Received
Messages (23, 1 deleted)	Chat/ Sent-Received	Convesation ID Conversation: 2455017384-1151071365593628678
	Content	j6https://twitter.com/messages/media/1176399887899848710j□pic.twitter.com/G1SSNctA22□□Si^
Cached Searches	Hastag	
	Account	OK
Application info	Label	Twitter
	Package	Com.twitter.android
	Version	8.13.0-release.00
	Application Type	User Application
	Application Size	50.1 MB
	Data Size	8.1 MB
	Cache Size	88.6 MB
	First Installed	2019-07-16 16:32:30 (UTC+7)
	Last Updated	2019-09-20 18:25:28 (UTC+7)
	Last Active	2019-09-25 11:26:00 (UTC+7)
Video		ok
Gambar		Ditemukan
Suara		Nok
Email		andihiyat@gmail.com
Url		https://twitter.com/Rudiantara/status/1132273995712090113

IP Adress	-
Kontak Telepon	0812 8899 3248

2. Belkasoft Evidence Center

The information in Table 5 contains account names, account ids, user activities, directions to private messages, status changes, emails, links and timelines. This is the data that can be retrieved using Belkasoft Evidence Centre, the amount of data is less than the retrieval using MOBILedit Forensic Express. More specific data searches on Belkasoft will take a lot of time in analysing, especially if the user has done a lot of activities on their twitter account..

Tabel 5. Hasil pengambilan data dari Belkasoft Evidence Center

Evidences	Belkasoft Evidence Center	Result
Nama Akun	Found	Paranormal
ID Akun	found	1151071365593628678
User Activity	Status changed	Message; Jj Besok gowesIXIIXIXIXIXXX
Incoming Messages	Found	gaasik
Outgoing Messages	Found	Baku hantam, minat?
Status change/ tweets	Found	Jj4Maunya apa ?@rudiantara_id #saveri #freedominternetIMJ Uij rudiantara_idj RudiantaraXXIXMJ#jsaveriXXI#XMJ$$4jfreedominternetXXI$4XXIIXIXI@XI @XI XIXXX;
Email	Found	korbanaksi@gmail.com
Detail account	Found	Follower 46742; messages 5523 modified 2019-09-28
Url	Found	https://pbs.twimg.com/profile_images/852355177260621824/usivwpwx_normal.jpg
Timeline	Found	JjTKampus A "Initiate Retreat!" Kampus B "Request Back Up!" anak STM "LAUNCH ATTACK!!!"IMJ d jmeisya and 666 othersXXIXXIIXIXI[XIXIXX

4. CONCLUSION

Based on the research conducted, information and data have been obtained on the twitter social media application using MOBILedit Forensic Express and Belkasoft Evidence Centre forensic tools by applying the Digital Forensic Research Workshop (DFRWS) method. The acquisition of information can be used as digital evidence. From the results of experiments that have been carried out previously on twitter accounts to upload status, conversations, friendships and use of some existing features, it shows that with the MOBILedit Forensic Express tool more data is found, such as detailed application information, account information with account ID, friend or follower list, conversations, timeline cache that has been seen by the account owner, status text, messages that have been deleted even though they are not read, email, location and telephone number. In the Belkasoft Evidence Center tool, some data cannot be obtained such as application info, friendships, info account details, recent searches, video, audio and location, but conversations are obtained in private messages that cannot be read in MOBILedit Forensic Expess. The findings of these two tools make some contribution to the investigation of twitter devices or social media that run on the android operating system and are still very standard, it is recommended that further research be carried out with broader tools on different operating systems.

REFERENCE

[1] I. Riadi, A. Yudhana, dan M. C. 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, no. 2, hal. 219–227, 2018, doi: 10.28932/jutisi.v4i2.769.

[2] N. Anwar dan I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, hal. 1, 2017, doi: 10.26555/jiteki.v3i1.6643.

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

[4] Kementrian Komunikasi dan Informasi, "Kominfo : Pengguna Internet di Indonesia 63 Juta Orang," *Website Resmi Kementerian Komunikasi dan Informatika RI*, 2013. .

[5] M. Cindo, D. P. Rini, dan Ermatita, "Sentiment Analysis On Twitter By Using Maximum Entropy And Support Vector Machine Method," *Sinergi*, vol. 24, no. 2, hal. 87–94, 2020, doi: 10.22441/sinergi.2020.2.002.

[6] A. Fauzan, I. Riadi, dan A. Fadlil, "Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime," in *Annual Research Seminar (ARS)*, 2016, vol. 2, no. 1, hal. 159–163.

[7] Kementrian Komunikasi dan Informasi, "SIARAN PERS NO. 08/HM/KOMINFO/01/2019 Warganet Paling Banyak Laporkan Akun Twitter," *Kementrian Komunikasi dan Informasi*, 2019. [Daring].

Tersedia pada: https://www.kominfo.go.id/tautan. [Diakses: 01-Feb-2019].

[8] I. Saputra dan M. N. Azhar, "Analisis dan Investigasi Forensik Digital Live Memory untuk Deteksi Tingkah Laku Agresi Pada Aplikasi Whatsapp," *Semin. Nas. dan Disk. Panel Multidisiplin Has. Penelit. Pengabdi. Kpd. Masy.*, hal. 119–125, 2018.

[9] APJII, "Penetrasi & Profil Perilaku Pengguna Internet Indonesia Tahun 2018," Indonesia, 2018.

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

[11] I. Riadi, R. Umar, dan I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, hal. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.

[12] A. L. Suryana, R. El Akbar, dan N. Widiyasono, "Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS)," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, hal. 111–117, 2016, doi: 10.26418/jp.v2i2.16821.

[13] I. Riadi, S. Sunardi, dan Sahiruddin, "Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST," *J. Teknol. Inf. dan Ilmu Komput.*, vol. x, no. 30, hal. 1–8, 2020, doi: 10.25126/jtiik.202071921.

[14] R. Inggi, B. Sugiantoro, dan Y. Prayudi, "Penerapan System Development Life Cycle (Sdlc)Dalam Mengembangkan Framework Audio Forensik," *semanTIK*, vol. 4, no. 2, hal. 193–200, 2018, doi: 10.5281/zenodo.2528444.

[15] M. N. Yusoff, A. Dehghantanha, dan R. Mahmod, "Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp and Line as Case Studies," in *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, vol. 4, no. 4, Elsevier, 2017, hal. 41–62.

[16] P. Salave dan Atisha Wakdikar, "Memory Forensics: Tools Comparison," *Int. J. Sci. Res.*, vol. 6, no. 6, hal. 5–8, 2017.

[17] P. Brankica Popović dan P. Kristijan Kuk, "Comprehensive Forensic Examination With Belkasoft Evidence Center," in *International Scientific Conference "Archibald Reiss Days" Thematic Conference Proceedings of International Significance*, 2018.

[18] I. Riadi, A. Fadlil, dan A. Fauzan, "A study of mobile forensic tools evaluation on android-based LINE messenger," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 10, hal. 201–206, 2018, doi: 10.14569/IJACSA.2018.091024.

[19] A. C. K. Wardana, R. Pedrason, dan T. B. Prasetyo, "Implementation of Digital Forensic Brunei Darussalam in Building Cyber Security," *J. Prodi Perang Asimetris*, vol. VOL 4, no. 1, hal. 1–22, 2018.

[20] R. Harris, "Arriving at an Anti-forensics Consensus," in *DFRWS 2006 Conference proceedings*, 2006.

[21] G. Palmer, "A Road Map for Digital Forensic Research Report From the First Digital Forensic Research Workshop (DFRWS)," Utica, New York, 2001.

[22] A. Yudhana, R. Umar, dan A. Ahmadi, "Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method," *Sci. J. Informatics Vol.*, vol. 6, no. 1, hal. 54–63, 2019, doi: 10.15294/sji.v6i1.17767.

[23] I. F. Editia Kurdiat, N. Widiyasono, dan H. Mubarok, "Analisis Proses Investigasi Dekstop PC Yang Terhubung Layanan Private Cloud," *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. 2, hal. 221–230, 2016, doi: 10.28932/jutisi.v2i2.463.

[24] R. Umar, I. Riadi, dan G. Maulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, hal. 69–75, 2017, doi: 10.14569/ijacsa.2017.081210.

[25] M. Parekh dan S. Jani, "Memory Forensic: Acquisition and Analysis of Memory and its Tools Comparison," *Int. J. Eng. Technol. Manag. Res.*, vol. 5, no. 2, hal. 90–95, 2018, doi: 10.5281/zenodo.1198968.

[26] P. E. Walck, "Book Review: Social Communication in the Twitter Age," *Int. J. Interact. Commun. Syst. Technol.*, vol. 3, no. 2, hal. 66–69, 2013.

[27] H. Basri, "Peran media Sosial Twitter dalam Interaksi Sosial Pelajar Sekolah Menengah Pertama di Kota Pekanbaru (Studi Kasus Pelajar Smpn 1 Kota Pekanbaru)," *J. Online Mhs. Fak. Ilmu Sos. dan Ilmu Polit.*, vol. 4, no. 2, hal. 1–15, 2017.

Ghufron Zaida Muflih

ORIGINALITY REPORT

13%	11%	5%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	jurnal.iaii.or.id Internet Source	2%
2	www.indikatorntb.com Internet Source	1%
3	Submitted to Universitas Islam Lamongan Student Paper	1%
4	www.ijcaonline.org Internet Source	1%
5	jtiik.ub.ac.id Internet Source	1%
6	staticxl.ext.xlaxiata.co.id Internet Source	1%
7	ejournal.poltektegal.ac.id Internet Source	1%
8	twitter.com Internet Source	1%
9	lifescienceglobal.com Internet Source	<1%

10	Submitted to University of Hong Kong Student Paper	<1 %
11	journal.unnes.ac.id Internet Source	<1 %
12	publishing-widyagama.ac.id Internet Source	<1 %
13	ijece.iaescore.com Internet Source	<1 %
14	Imam Riadi, Herman, Nur Hamida Siregar. "Mobile Forensic Analysis of Signal Messenger Application on Android using Digital Forensic Research Workshop (DFRWS) Framework", Ingénierie des systèmes d information, 2022 Publication	<1 %
15	arxiv.org Internet Source	<1 %
16	repository.up.ac.za Internet Source	<1 %
17	Joko Triyanto, Sunardi Sunardi, Imam Riadi. "Analisis Investigasi Cyber Espionage Pada Facebook Menggunakan Digital Forensics Research Workshop (DFRWS)", Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto), 2022 Publication	<1 %
	conveyindonesia.com	

18	Internet Source	<1%
19	journal.iapa.or.id Internet Source	<1%
20	Mustafa Mustafa, Imam Riadi, Rusydi Umar. "Header investigation for spam email forensics using framework of national institute of standards and technology", ILKOM Jurnal Ilmiah, 2021 Publication	<1%
21	archive.org Internet Source	<1%
22	biologi.unnes.ac.id Internet Source	<1%
23	core.ac.uk Internet Source	<1%
24	www.jurnal.uts.ac.id Internet Source	<1%
25	Imam Riadi, Herman Herman, Irhash Ainur Rafiq. "Mobile Forensic Investigation of Fake News Cases on Instagram Applications with Digital Forensics Research Workshop Framework", International Journal of Artificial Intelligence Research, 2022 Publication	<1%

26	Maghvirna Rafika Dhewi Qibriya, Awalludiyah Ambarwati, Kunto Eko Susilo. "Analisis Forensik Digital Pada Aplikasi Instant Messaging Di Smartphone Berbasis Android Untuk Bukti Digital", Jurnal Teknologi Informasi, 2021 Publication	<1%
27	Sunardi, Herman, Syifa Riski Ardiningtias. "A Comparative Analysis of Digital Forensic Investigation Tools on Facebook Messenger Applications", Journal of Cyber Security and Mobility, 2022 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Ghufron Zaida Muflih