JIKO (Jurnal Informatika dan Komputer) Accredited KEMENDIKBUD RISTEK, No.105/E/KPT/2022
Vol. 6, No. 1, April 2023, hlm. 52-61 p-ISSN: 2614-8897
DOI: 10.33387/jiko.v6i1.5872 e-ISSN: 2656-1948

# COMPARISON OF FORENSIC TOOLS ON SOCIAL MEDIA SERVICES USING THE DIGITAL FORENSIC RESEARCH WORKSHOP METHOD

**Ghufron Z Muflih[1], Sunardi[2], Imam Riadi[3], Anton Yudhana[4], Himawan I Azmi[5]**

[1]Informatics Engineering, Faculty of Engineering, Ma'arif Nahdlatul Ulama Kebumen University, Central Java
[2,4]Electrical Engineering, Faculty of Industrial Technology, Ahmad Dahlan University, Yogyakarta
[3]Information Systems, Faculty of Applied Science and Technology, Ahmad Dahlan University, Yogyakarta
[5]Master of Informatics, Faculty of Science and Technology, Sunan Kalijaga State Islamic University, Yogyakarta
Email: [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, [5]22206052004@student.uin-suka.ac.id

(Received: 8 March 2023, Revised: 24 March 2023, Accepted: 28 March 2023)

**Abstract**

Social media applications currently play many roles and are part of various human activities, on the other hand social media is also very vulnerable to various crimes. Crimes that can occur on social media can include hate speech, defamation, fraud, gambling, pornography, and other harmful actions. This research applies the Digital Forensic Research Workshop (DFRWS) method to search for digital evidence on twitter social media application services that run on the Android operating system. Using MOBILedit Forensic Express and Belkasoft Evidence Center tools to search and analyse digital evidence. Utilising twitter social media application services such as sending messages, creating short statuses or tweets and retweeting. Activities performed by users on twitter social media application services become digital evidence acquired using MOBILedit Forensic Express and Belkasoft Evidence Center tools. Digital evidence retrieval using MOBILedit and Belkasoft tools obtained a comparison that MOBILedit Forensic Express found more data on the twitter social media application than the Belkasoft Evidence Center tool. The findings of digital evidence make several contributions to social media investigations that run on the Android operating system.

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



**Corresponding Author: Ghufron Z Muflih*

## 1. INTRODUCTION

The rapid growth of smartphone technology has led to the development of various supporting applications to run on it. The development of mobile applications for various services such as applications for work and even entertainment is increasingly available in the application store of the operating system itself, such as social media applications [1]. Social media plays a role and becomes part of various human activities such as socialising using group chat, commercial activities, advertising media, education, and other creative content. Social media, on the other hand, is a place that is prone to various crimes [2] [3]. Twitter is one of the social media in Indonesia with 19.5 million users [4]. Twitter social media provides services that allow its users to utilise it in their daily activities such as sharing whatever is around them quickly and easily [5]. Apart from being a place to seek entertainment or obtain information, social media also has the potential to become a place and even a medium for crime. Crimes that can occur on social media through smartphones can be in the form of hate speech, spreading false news, defamation, fraud, gambling, pornography, or other detrimental things [6]. According to the Ministry of Communication and Informatics, twitter social media was widely reported through the content complaint channel in December 2018 [7]. Social media such as twitter is a fertile ground for verbal bullying cases to grow [8]. Unidentified cases of bullying and cyberbullying in Indonesia lead to the emergence of various bullying phenomena and end up with cases of depression and death of victims [9].

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 happens a lot on social media at 49%, pornographic content 55.9%. The main reason for using the internet is for 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 is 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% [10]. Security issues are a challenge for forensic information technology and law enforcement to investigate devices involved in a crime case [11]. Crimes will generally leave traces that can be used as evidence, which can be in the form of electronic or digital evidence [12].

Examples of digital crimes such as, email header manipulation or spoofing emails sent with web hosting services [13]. This kind of digital crime case is a challenge for law enforcement and digital forensic experts to conduct investigations in a crime case, because many cases of deletion of digital crime evidence to eliminate traces [14]. Forensic frameworks or methods for obtaining digital evidence such as the Digital Forensics Research Workshop (DFRWS) framework, even building on pre-existing frameworks and combining with specialised techniques for specific evidence, e.g. audio evidence [15]. Related to digital evidence research on social media twitter and facebook to find digital evidence related to some text and image uploads and compare tools to retrieve digital evidence [3]. The operating system that runs on devices other than Android is also the Firefox OS operating system with the results of evidence stored in volatile memory. [16]. Knowing the tools to search for digital evidence on the device is important, although most tools give reasonable evidence on one tool only, it is also necessary to compare with other tools [17]. Forensic tools such as Belkasoft Evidence Center for searching digital evidence such as locations, photos, messages or internet searches [18]. MOBILedit Forensic tool with some functions similar to Belkasoft Evidence Center to search and retrieve digital evidence such as retrieving device information, application extraction, application analysis and report data [19].

This research implements the Digital Forensics Research Workshop (DFRWS) forensic analysis method. This method is to explain the stages of research carried out so that the steps and flow of research become systematic and can be used as guidelines in solving digital crime problems. In addition, it aims to find all data or evidence in the Twitter social media application that runs on the Android operating system by applying the DFRWS method, and comparing MOBILedit Forensic Express and Belkasoft Evidence Center forensic tools. MOBILedit Forensic Express and Belkasoft Evidence Center forensic tools to retrieve digital evidence or data uploaded to the twitter social media application after going through experimental scenarios of using services such as uploading images, videos, text, sending messages and doing some deletion activities.

## 2. RESEARCH METHOD

### 2.1. Method

This research uses the Digital Forensics Research Workshop (DFRWS) method with six stages starting from the identification, preservation, evidence collection, examination, analysis and presentation stages. The use of the DFRWS method to carry out the process of preservation, validation, identification, analysis, interpretation, documentation and presentation of all digital evidence obtained to deepen the reconstruction of an event suspected of being a crime, in order to anticipate future crimes [20] [21] [22].

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

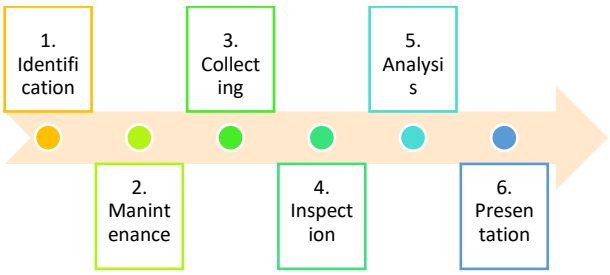



Figure 1. Stages of the DFRWS

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. 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 digital evidence are identified and data sources are identified.
4. Examination of evidence that has been identified by determining data filters on certain parts of digital evidence and data sources. This stage is carried out

by changing the form 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 is important in computer crime cases [23]. Digital evidence in this research is not obtained in the actual environment or the results of actual crimes. The acquisition of digital evidence is obtained from scenarios using twitter social media by utilising services such as sharing images, text, videos, commenting, sending messages, and deleting them. The scenario carried out on the twitter social media application is as shown in Figure 2.

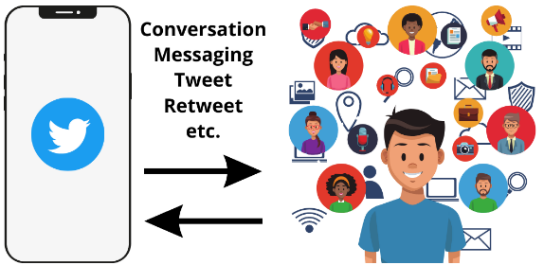



Figure 2. Scenario of using twitter social media services

Preparation of equipment for the forensic process or retrieval of evidence from smartphones using software and hardware. The hardware in the research is a smartphone with an operating system that runs is android, and uses a usb cable. The smartphone has a twitter social media application installed. The software or tool for retrieving digital evidence is MOBILedit Forensic Express which makes it possible to get data logically, examine 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 [24]. The second software is Belkasoft Evidence Center 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 [25] [26] by analysing the hard drive, memory dump, and saving in a report [27].

## 3. RESULT AND DISCUSSION

### 3.1. Identification

The identification stage requires a smartphone that has a twitter social media application installed. Smartphones that have twitter social media applications installed have gone through a series of scenarios to share images, text, videos, comment, send messages, and delete messages. Twitter social media application services that are the source of digital evidence searches.

1. Smartphone Device

Smartphones as electronic evidence use an android operating system that has a twitter social media application 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 is the specification of the smartphone.

Table 1. Specifications of 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 dail Microblogging with 554.7 million active users worldwide, 58 million collective "tweet" posts daily [28]. Twitter as a social media platform is widely utilised by the government, civil and private sectors. Twitter social media provides benefits as an intermediary for disseminating information, news, and current situations because it can reach users more quickly and effectively [29]. Services on twitter social media that users can utilise such as changing profiles, exchanging information, sending messages, posting images, text, video and sound and can also share locations. Another service is the base as a gathering place for users with the same hobbies or interests to provide information and messages to each other [30].

3. Forensic tools

The successful retrieval of evidence in the investigation process is also supported by the use of forensic tools [31]. The use of forensic tools or tools to retrieve digital evidence in the investigation process from smartphone devices as in Table 2.

Ttable 2. *Forensic tools*

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

### 3.1 Mintenance

The maintenance stage aims to maintain digital evidence or all data on smartphone devices. 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 isolate communication is by activating airplane mode on the device.

### 3.2 Collecting

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

### 3.4 Examination

The examination stage was carried out after the digital evidence collection stage was completed using MOBILedit Forensic Express and Belkasoft Evidence Center tools. The results of the examination obtained data from smartphone devices based on service features in the twitter social media application as in Table 3.

Table 3. Examination results

| 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

An analysis was carried out from the results of the examination stages, the digital evidence obtained using MOBILedit Forensic Express and Belkasoft Evidence Center was very limited. Not all data on the device or twitter application was successfully found and provided clear information, even some data could not be read.

1. MOBILedit Forensic Express

Analysis using MOBILedit Forensic Express tools obtained twitter social media application information including the installed application version, application type, application size, data size, cache size, the first date the twitter application was installed on a smartphone device, twitter application updates and the last twitter application operated, as in 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 owner's information, such as twitter account name, ID, account description, number of followers, number of follows, number of messages, date the account was created and updated and the image or profile url.

| | |
|---|---|
| Nickname | Wicakson8 |
| Twitter ID | 1151071365593628678 |
| Description | J'¡Karna Soto Ayam Tak Pernah Bohongl' |
| 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/11 |

Figure 4. Account information

Other information obtained using MOBILedit Forensic Express is the friendship network information as shown in Figure 5. The account name, twitter ID, map address, url, description, number of followers, number of follows, number of messages, last update and profile picture were obtained.


Figure 5. Friendship networking information

Figure 6 shows 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..

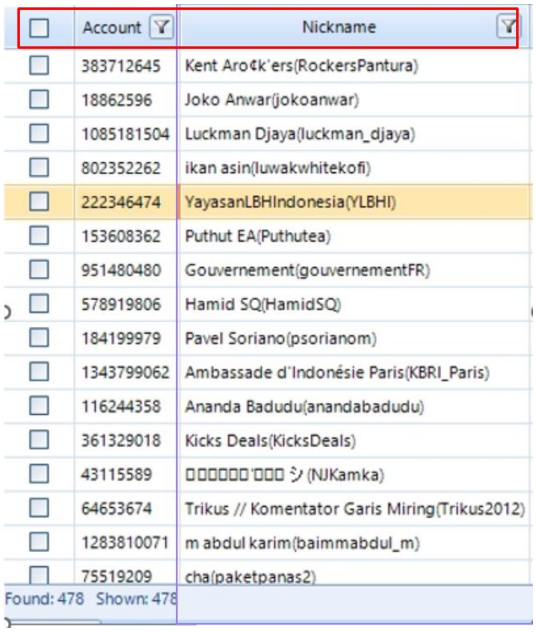

Figure 6. Conversation information

Another information obtained from the twitter application is the cache of tweets or timeline which contains some information including the user's name, tweets or status uploaded, the date of uploading the tweet status, hastags, language, the number of retweets or how much is re-uploaded by other users, links leading to user tweets, also found tweets deleted by the account owner as shown in Figure 7.


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

## 2. Belkasoft Evidence Center

Analysis using Belkasoft Evidence Center obtained less information than evidence retrieval using the MOBILedit Forensic Express tool. Information obtained using Belkasoft Evidence Center is in the form of account ID information that shows the account name, as well as the number of accounts found as shown in Figure 8.

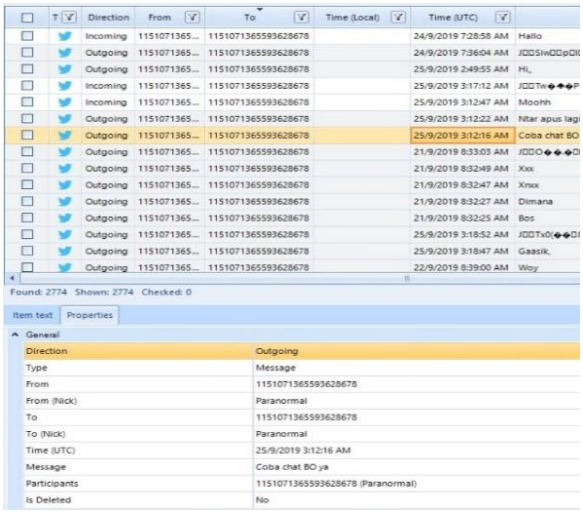


| Account | Nickname |
|---|---|
| 383712645 | Kent Aro¢k'ers(RockersPantura) |
| 18862596 | Joko Anwar(jokoanwar) |
| 1085181504 | Luckman Djaya(luckman_djaya) |
| 802352262 | ikan asin(luwakwhitekofi) |
| 222346474 | YayasanLBHIndonesia(YLBHI) |
| 153608362 | Puthut EA(Puthutea) |
| 951480480 | Gouvernement(gouvernementFR) |
| 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 (NJKamka) |
| 64653674 | Trikus // Komentator Garis Miring(Trikus2012) |
| 1283810071 | m abdul karim(baimmabdul_m) |
| 75519209 | cha(paketpanas2) |

Found: 478 Shown: 478

Gambar 8. Account Information

The results of further analysis obtained the form of user conversation activity. Messages sent by the account owner, the date of the conversation, the direction of outgoing and incoming conversations can be read clearly as in Figure 9 and Figure 10.



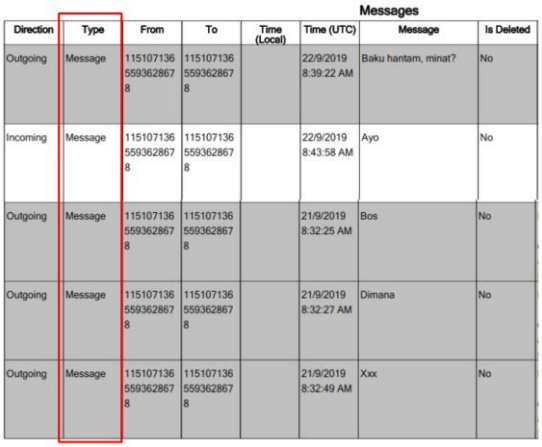
Found: 2774 Shown: 2774 Checked: 0

Item text | Properties

General

| | |
|---|---|
| Direction | Outgoing |
| Type | Message |
| From | 115107136559362867 8 |
| From (Nick) | Paranormal |
| To | 115107136559362867 8 |
| To (Nick) | Paranormal |
| Time (UTC) | 25/9/2019 3:12:16 AM |
| Message | Coba chat BO ya |
| Participants | 115107136559362867 8 (Paranormal) |
| Is Deleted | No |

Figure 9. Conversation information

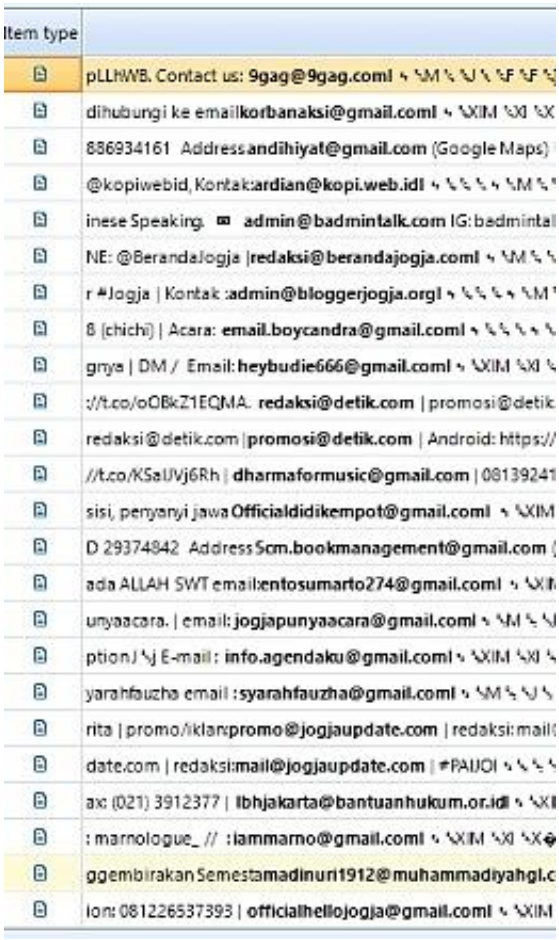


Messages

| Direction | Type | From | To | Time (Local) | Time (UTC) | Message | Is Deleted |
|---|---|---|---|---|---|---|---|
| Outgoing | Message | 115107136559362867 8 | 115107136559362867 8 | | 22/9/2019 8:39:22 AM | Baku hantam, minat? | No |
| Incoming | Message | 115107136559362867 8 | 115107136559362867 8 | | 22/9/2019 8:43:58 AM | Ayo | No |
| Outgoing | Message | 115107136559362867 8 | 115107136559362867 8 | | 21/9/2019 8:32:25 AM | Bos | No |
| Outgoing | Message | 115107136559362867 8 | 115107136559362867 8 | | 21/9/2019 8:32:27 AM | Dimana | No |
| Outgoing | Message | 115107136559362867 8 | 115107136559362867 8 | | 21/9/2019 8:32:49 AM | Xxx | No |

Figure 10. Conversation Information

Analysis using Belkasoft Evidence Center obtained emails from several connected accounts. Evidence other than email obtained some 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 11.

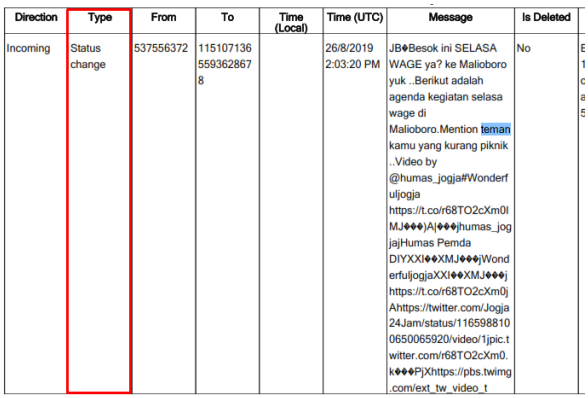


| Item type | |
|---|---|
| | pLLHWB. Contact us: **9gag@9gag.com** |
| | dihubungi ke email**korbanaksi@gmail.com** |
| | 886934161 Address**andihiyat@gmail.com** (Google Maps) |
| | @kopiwebid, Kontak:**ardian@kopi.web.id** |
| | inese Speaking. **admin@badmintalk.com** IG: badmintal |
| | NE: @BerandaJogja \|**redaksi@berandajogja.com** |
| | r #Jogja \| Kontak :**admin@bloggerjogja.org** |
| | 8 (chichi) \| Acara: **email.boycandra@gmail.com** |
| | gnya \| DM / Email:**heybudie666@gmail.com** |
| | ://t.co/oOBkZ1EQMA. **redaksi@detik.com** \| promosi@detik. |
| | redaksi@detik.com \|**promosi@detik.com** \| Android: https:// |
| | //t.co/KSaUVj6Rh \| **dharmaformusic@gmail.com** \| 08139241 |
| | sisi, penyanyi jawa **Officialdidikempot@gmail.com** |
| | D 29374842 Address**5cm.bookmanagement@gmail.com** |
| | ada ALLAH SWT email:**entosumarto274@gmail.com** |
| | unyaacara. \| email:**jogjapunyaacara@gmail.com** |
| | ption/ E-mail : **info.agendaku@gmail.com** |
| | yarahfauzha email :**syarahfauzha@gmail.com** |
| | rita \| promo/iklan:**promo@jogjaupdate.com** \| redaksi:mail |
| | date.com \| redaksi:**mail@jogjaupdate.com** \| #PAIJOI |
| | ax: (021) 3912377 \| **lbhjakarta@bantuanhukum.or.id** |
| | : marnologue_ // :**iammarno@gmail.com** |
| | ggembirakan Semesta**madinuri1912@muhammadiyahgl.c** |
| | ion: 081226537393 \| **officialhellojogja@gmail.com** |

Figure 11. Account email information

User activity is captured in a report generated automatically by the Belkasoft Evidence Center tool that shows the direction of user activity, account ID and

text of tweets shared with other users that appear on the timeline as shown in Figure 12.



| Direction | Type | From | To | Time (Local) | Time (UTC) | Message | Is Deleted |
|---|---|---|---|---|---|---|---|
| Incoming | Status change | 537556372 | 1151071365593628678 | | 26/8/2019 2:03:20 PM | JB◆Besok ini SELASA WAGE ya? ke Malioboro yuk ..Berikut adalah agenda kegiatan selasa wage di Malioboro.Mention teman kamu yang kurang piknik ..Video by @humas_jogja#Wonderfuljogja https://t.co/r68TO2cXm0lMJ◆◆◆)A|◆◆◆jhumas_jogjajHumas Pemda DIYXXl◆◆XMJ◆◆◆jWonderfuljogjaXXl◆◆XMJ◆◆◆j https://t.co/r68TO2cXm0jAhttps://twitter.com/Jogja24Jam/status/1165988100650065920/video/1jpic.twitter.com/r68TO2cXm0.k◆◆◆PjXhttps://pbs.twimg.com/ext_tw_video_t | No |

Figure 12. Account activity links from report file on Belkasoft

### 3.6 Presentation

The final stage of DFRWS is the presentation of the process that has been carried out from the previous stage. User activity on twitter social media is used as digital evidence. The results of obtaining evidence using MOBILedit Forensic Express and Belkasoft Evidence Center have advantages and disadvantages. Examples of the results of obtaining digital evidence or information from MOBILedit Forensic Express and Belkasoft Evidence Center tools are presented in a table for easier observation.

1. MOBILedit Forensic Express

The results of evidence 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 telephone numbers, as in Table 4..

Table 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$^{ɛ}$ɻj!Karna Soto Ayam Tak Pernah BohongI$^{s}$$^{s}$%XIM$^{ɛ}$ɻXI$^{ɛ}$ɻX***XX |
| | Follower | 4 |
| | Following | 5 |
| Friends (6) | Favorite | 12 |
| | Number of Messages | 46 |
| | Created Date | 2019-07-16 17:09:34 (UTC+7) |
| | Modified Date | 2019-09-25 10:40:25 (UTC+7) |
| | Picture ID | https://pbs.twimg.com/profile_images/1176690821690576900/hFbrBj3H_normal.jpg |
| | Nickname | fauzangustafi |
| | Twitter ID | 2455017384 |
| | Adress(google maps) | Boyolali |
| | Description | J$^{ɛ}$ɻj$^{ɛ}$₂Bio : I'm Awesome!I$^{s}$$^{s}$%XIM$^{ɛ}$ɻXI$^{ɛ}$ɻX$^{ɛ}$$^{ɛ}$XX |
| | Number of Followers | 26 |
| | Following | 36 |
| | Number of Messages | 174 |
| | Modified | 2019-09-25 09:48:43 (UTC+7) |
| | Following User | Ok |
| | Followed by User | Ok |
| | Picture URL | https://pbs.twimg.com/profile_images/653594881508577281/qEdYmv0d_normal.jpg |
| User (587) | Number of Messages | 20 |
| | Nickname | PartaiSocmed |
| | Twitter ID | 869327120 |
| | Adress(google maps) | Indonesia |
| | Url | https://t.co/aDu3oGTVHr |
| | Description | J$^{ɛ}$ɻj$^{ɛ}$Social Media Party \| Objectivity, Fairness and Justice for All \| Non-Populist Party \| Common Sense Party \| Empowering People \| No = 99I$^{s}$$^{s}$%XIM$^{ɛ}$ɻXI$^{ɛ}$ɻX$^{ɛ}$$^{ɛ}$$^{ɛ}$$^{ɛ}$$^{ɛ}$$^{ɛ}$XX |
| | Number of Followers | 173470 |
| | Following | 3007 |
| | Number of Messages | 352939 |
| | Modified | 2019-09-24 14:02:56 (UTC+7) |
| | Picture URL | https://pbs.twimg.com/profile_images/1137182440907108352/iFHhYIh-_normal.jpg |
| Conversation (4 convers, 23 messages, 1 delete) | Sent Message | N/A |
| | Received Message | N/A |
| | Draft | N/A |
| | Failed Message | N/A |
| | Unknown Message | N/A |
| | Deleted Message | OK |
| | Conversation ID | 2455017384-1151071365593628678 |
| | Date/ Time | 2019-9-24 14:36:04 (UTC+7) |
| | Participants | Paranormal, Fauzan |
| | Status/ timeline | OK |
| Cached tweets (852, 13 deleted) | Nama Akun | Rudiantara (Rudiantara) |
| | Tanggal Update | 2019-05-25 20:15:31 (UTC+7) |
| | Words Status | J$^{ɛ}$ɻk$^{s}$$^{s}$%Teman2, situasi sdh kondusif shg pembatasan akses fitur video & gambar pd medsos |

| | | |
|---|---|---|
| | | & instant messaging difungsikan kembali.<br>Mari senantiasa jaga dunia maya digunakan unt hal2 yg positif.<br>Mari perangi hoaks, fitnah, info2 yg memprovokasi spt<br>yg banyak beredar saat kerusuhan<br>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

Using Belkasoft Evidence Centre, digital evidence is obtained as shown in Table 5. The digital evidence obtained is the account name, account id, user activity, direction on private messages, status changes, emails, links and timelines. The amount of digital evidence obtained using Belkasoft Evidence Center is limited from the acquisition of evidence using MOBILedit Forensic Express. Searching for more specific information on Belkasoft requires a lot of time in analysing, especially if the user has done a lot of activities on his twitter social media account.

Table 5. Data collection results from Belkasoft Evidence Center

| Evidences | Belkasoft Evidence Center | Result |
|---|---|---|
| Nama Akun | Found | Paranormal |
| ID Akun | found | 1151071365593628678 |
| User Activity | Status changed | Message; Jj Besok gowesIXIIXIXIXIXIXXX |
| Incoming Messages | Found | gaasik |
| Outgoing Messages | Found | Baku hantam, minat? |
| Status change/ tweets | Found | Jj4Maunya apa ?@rudiantara_id #saveri #freedominternetIMJ<br>Uij rudiantara_idj RudiantaraXXIXMJ#jsaveriXXI#XMJ$$4jfreedominternetXXI$4XXIIXIXI@XI s 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!"<br>Kampus B "Request Back Up!"<br>anak STM "LAUNCH ATTACK!!!"IMJ<br>d jmeisyacv jmeisya and 666 othersXXIXXIIXIXI[XIXIXX |

## 4. CONCLUSION

Based on the research conducted, information and digital evidence 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. The results of experiments that have been carried out using services on twitter social media applications such as uploading status or tweets, having conversations, adding friends, retweeting user-generated status, show that with the MOBILedit Forensic Express tool more evidence or information is found. Evidence obtained such as detailed application information, account information with account ID, list of friends or followers, conversations, timeline cache that has been seen by the account owner, status text, messages that have been deleted even though they are not readable, email, location and telephone number. In the Belkasoft Evidence Centre tool, some digital evidence cannot be obtained such as application info, friendships, account details, recent searches, video, audio and location, but conversations in private messages that cannot be read in the MOBILedit Forensic Express tool are obtained. The findings of the MOBILedit Forensic Express and

Belkasoft Evidence Center tools make some contribution to the investigation of mobile devices and twitter social media applications running on the Android operating system and are still very standard. Further research is recommended to use more extensive tools on different operating systems.

## 5. REFERENCES


[1] I. Riadi, A. Yudhana, and 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, pp. 219–227, 2018, doi: 10.28932/jutisi.v4i2.769.

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

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

[4] Kominfo, "Kominfo : Pengguna Internet di Indonesia 63 Juta Orang," *Website Resmi Kementerian Komunikasi dan Informatika RI*, 07-Nov-2013. [Online]. Available: https://www.kominfo.go.id/index.php/content/detail/3415/Kominfo+%3A+Pengguna+Internet+di+Indonesia+63+Juta+orang/0/berita_satker. [Accessed: 27-Mar-2023].

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

[6] I. Wahyudi, A. Muntasa, M. Yusuf, and A. Hamzah, "Mengungkap Dan Menguji Keaslian Bukti Digital Pada Kejahatan Cybercrime Dengan Metode Digital Forensic Research Workshop," *J. Apl. Teknol. Inf. dan Manaj.*, vol. 2, no. 2, pp. 120–127, 2021, doi: 10.31102/jatim.v2i2.1068.

[7] Kementrian Komunikasi dan Informasi, "SIARAN PERS NO. 08/HM/KOMINFO/01/2019 Warganet Paling Banyak Laporkan Akun Twitter," *Kementrian Komunikasi dan Informasi*, 2019. [Online]. Available: https://www.kominfo.go.id/tautan. [Accessed: 01-Feb-2019].

[8] N. N. Ayu Suciartini and N. L. P. Unix Sumartini, "Verbal Bullying dalam Media Sosial," *J. Pendidik. Bhs. Indones.*, vol. 6, no. 2, p. 152, Jan. 2019, doi: 10.30659/j.6.2.152-171.

[9] M. I. Djamzuri and A. P. Mulyana, "Fenomena Cyberbullying Pembiaran Juvenile Deliquency Dalam Teknologi Media Baru," *JISIP (Jurnal Ilmu Sos. dan Pendidikan)*, vol. 7, no. 1, pp. 810–816, Jan. 2023, doi: 10.58258/jisip.v7i1.4801.

[10] M. Nabila, "Survei APJII: Pengguna Internet di Indonesia Capai 171,17 Juta Sepanjang 2018 | DailySocial.id," *Daily Social id*, 16-May-2019. [Online]. Available: https://dailysocial.id/post/pengguna-internet-indonesia-2018. [Accessed: 27-Mar-2023].

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

[12] I. Riadi, R. Umar, and 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, pp. 70–82, Jul. 2018, doi: 10.21831/elinvo.v3i1.19308.

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

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

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

[16] M. N. Yusoff, A. Dehghantanha, and R. Mahmod, "Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp, and Line as Case Studies," *Contemp. Digit. Forensic Investig. Cloud Mob. Appl.*, vol. 4, no. 4, pp. 41–62, 2017, doi: 10.1016/B978-0-12-805303-4.00004-6.

[17] S. Gaur and R. Chhikara, "Memory Forensics: Tools and Techniques," *Indian J. Sci. Technol.*, vol. 9, no. 48, Dec. 2016, doi: 10.17485/ijst/2016/v9i48/105851.

[18] B. Popović, K. Kuk, and A. Kovačević, "Comprehensive Forensic Examination With Belkasoft Evidence Center," in *International Scientific Conference "Archibald Reiss Days" Thematic Conference Proceedings of International Significance*, 2018, pp. 419–433.

[19] 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, doi: 10.14569/IJACSA.2018.091024.

[20] A. C. K. Wardana, R. Pedrason, and T. B. Prasetyo, "Implementation of Digital Forensic Brunei Darussalam in Building Cyber Security," *J. Prodi Perang Asimetris*, vol. 4, no. 1, pp. 1–22, 2018, doi: doi.org/10.33172/pa.v4i1.194.

[21] R. Harris, "Arriving at an anti-forensics consensus:

Examining how to define and control the anti-forensics problem," *Digit. Investig.*, vol. 3, no. SUPPL., pp. 44–49, Sep. 2006, doi: 10.1016/j.diin.2006.06.005.

[22] G. Palmer, "A Roadmap for Digital Forensic Research Report From the First Digital Forensic Research Workshop (DFRWS)," *Digit. Forensic Res. Conf.*, vol. 24, no. 3, pp. 709–719, Jan. 2001, doi: 10.1016/0032-3950(82)90064-8.

[23] A. Ahmadi, T. Akbar, and H. Mandala Putra, "Perbandingan Hasil Tool Forensik Pada File Image Smartphone Android Menggunakan Metode Nist," *JIKO (Jurnal Inform. dan Komputer)*, vol. 4, no. 2, pp. 92–97, 2021, doi: 10.33387/jiko.v4i2.2812.

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

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

[26] R. Umar, I. Riadi, and G. Maulana, "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, doi: 10.14569/ijacsa.2017.081210.

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

[28] S. B. Bullard, "Book Review: Twitter: Social Communication in the Twitter Age , by Dhiraj Murthy," *Journal. Mass Commun. Q.*, vol. 91, no. 4, pp. 861–862, Dec. 2014, doi: 10.1177/1077699014554765p.

[29] N. A. Azmi, A. T. Fathani, D. P. Sadayi, I. Fitriani, and M. R. Adiyaksa, "Social Media Network Analysis (SNA): Identifikasi Komunikasi dan Penyebaran Informasi Melalui Media Sosial Twitter," *J. Media Inform. Budidarma*, vol. 5, no. 4, p. 1422, 2021, doi: 10.30865/mib.v5i4.3257.

[30] R. Fitriana, D. R. Darmawan, E. Efriani, and D. W. Apriadi, "Gejolak Fujoshi Dalam Media Sosial (Peran Media Twitter Dalam Pembentukan Identitas Kelompok Fujoshi)," *Kiryoku*, vol. 5, no. 2, pp. 228–235, 2021, doi: 10.14710/kiryoku.v5i2.228-235.

[31] M. Naufal Bahreisy, R. Rahmadi, and Y. Prayudi, "Analisis Halaman Darkweb Untuk Mendukung Investigasi Kejahatan," *JIKO (Jurnal Inform. dan Komputer)*, vol. 4, no. 1, pp. 1–7, 2021, doi: 10.33387/jiko.v4i1.1817.