Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 21, No. 3, July 2022, pp. 489∼502
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v21i3.1620

Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework

Imam Riadi[1], **Herman**[2], **Nur Hamida Siregar**[3]
Universitas Ahmad Dahlan, Indonesia

Article Info

Article history:

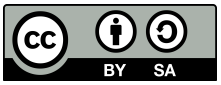
Received December 15, 2021
Revised February 02, 2022
Accepted April 19, 2022

Keywords:

Cybercrime
DFRWS Framework
Mobile Forensic
Signal Messenger
Vaccine Hoax

ABSTRACT

The COVID-19 pandemic is one of the factors that has increased the use of social media. One of the negative impacts of using social media is the occurrence of cybercrime. The possibility of cybercrime can also happen on one of the social media platforms, such as the Signal Messenger application. In the investigation process, law enforcement needs mobile forensic methods and appropriate forensic tools so that the digital evidence found on the perpetrator's smartphone can be accepted by the court. This research aims to get digital evidence from cases of spreading the COVID-19 vaccine hoaxes. The method used in this research is a mobile forensics method based on the Digital Forensic Research Workshop (DFRWS) framework. The DFRWS framework consists of identification, preservation, collection, examination, analysis, and preservation. The results showed that the MOBILedit tool could reveal digital evidence in the form of application information and contact information with a performance value of 22.22%. Meanwhile, Magnet AXIOM cannot reveal digital evidence at all. The research results were obtained following the expected research objectives.



Corresponding Author:

Nur Hamida Siregar
Department of Informatics
Universitas Ahmad Dahlan,Indonesia
Email: nur2007048007@webmail.uad

1. INTRODUCTION

Life at this time has entered the digital era. Humans carry out most of their activities through various internet-based media, including social media. Based on statistical data, internet users worldwide reach 4.540 billion people, and active social media users get 3.8 billion people [1]. Meanwhile, internet users in Indonesia came to 196.7 million people in 2020, an increase of 25.5 million users from the previous year, and active social media users reached 150 million people [2]. The current increase in the use of social media occurs across all types of social media during the pandemic. COVID-19 was initially detected in December in the China city of Wuhan [3]. This virus is a pandemic that is easily spread and contagious. The impact of the COVID-19 pandemic is reducing or minimizing contact with other people, which means not justifying direct contact through handshakes, touching hands, or indirect contact in the form of using facilities and infrastructure together soon. Reducing contact will prevent the spread of the Coronavirus that we are currently experiencing together [4]. The COVID-19 pandemic requires all activities to be carried out online. Instant Messenger (IM) is an online communication application commonly used to send messages, image files, audio files, and videos.

Along with the development of communication technology, application developers compete to create user-friendly applications and uphold user privacy. Signal messenger is one of the social media applications gaining popularity right now. Signal Messenger also provides an IM service. The features of Signal Messenger are the same as WhatsApp (WA). Signal Messenger allows single or group text messages, pictures, video messages, document files, Graphics Interchange Format (GIF), voice and video calls on Android and iOS devices. The number of persons who can participate in a group call is currently limited to five [5]. Now, this application can also be used on the desktop. An user of Signal can operate numerous devices simultaneously, such as one mobile app (iOS or Android) and an unlimited number of Google Chrome extensions [6]. Signal Messenger uses a data connection or WI-FI. This application uses encryption keys to verify each of the end-to-end encryptions. The keys for the encryption arent stored on the developer but on the users mobile device. The purpose of using end-to-end encryption techniques during transmission is to provide Signal Messenger application user data security and privacy [7].

Signal Messenger was used to send an encrypted message for the first time in 2010. It was created by Whisper Systems Moxie Marlinspike and Stuart Anderson and was known as a licensed application with the name TextSecure [8]. Signal Messenger is the first free application on Indonesias Google Play Store and Apple App Store search pages. Signal Messenger application users increased from 0.5 million to 40 million active users. The increase from December 2019 increased drastically in January 2021. The rapid increase in the use of social media has both positive and negative impacts. One of them is cybercrime. Cybercrime is an illegal activity carried out using a computer or electronic device. Cybercrime occurs when a crime involves technology [9]. In other words, cybercrime is a crime that occurs because of the misuse of internet technology [10]. Cybercrime can be in the form of spreading hoaxes, cyberbullying, fraud, extortion, human trafficking, and others that can have fatal consequences, such as murder.

Fake news or hoaxes are information or news containing uncertain things, or thats not facts of what happened. A hoax is also defined as news whose truth cannot be accounted for by the newsmaker. Hoaxes are circulating in society via online media. The spread of hoaxes on the internet uses the most frequently used instrument to spread hoaxes, namely social media. Academics worldwide have been paying close attention to online hoaxes and false information [11]. Hoaxes are made to influence the reader's emotions. Hoax's content is made to look like the readers opinion. The more similar hoax content to the reader's opinion, the opportunity for content to be forwarded or disseminated is getting bigger [12]. Readers with limited health literacy skills are often more likely to fall victim to and spread hoaxes on social media [13].

The increasing use of social media during the COVID-19 pandemic has led to the emergence of several content-containing hoaxes. According to data from the Ministry of Communication and Information Technology Indonesia, the spread of false news/information (hoaxes) in Indonesia is relatively high, specifically about the hoaxes of the COVID-19 vaccine. Based on data from the Ministry of Communication and Information Technology until December 4, 2021, it was found that there were 2,015 COVID-19 hoax issues and 402 COVID-19 vaccine hoaxes [14]. We can quickly get a lot of false news, as has happened in several regions, such as hoax news spreading in big cities like Medan, Lampung, Balikpapan, Jakarta, Surabaya, and other big cities [3]. One of the causes of this case is various social media applications as long as these applications provide IM service features. Signal Messenger is one of the social media platforms that have IM service features. The high number of hoax cases, especially about COVID-19 and the COVID-19 vaccine on social media, is the cause of the investigation of hoax cases through simulation of digital forensics using the Digital Forensic Research Workshop (DFRWS) framework.

In theory, MOBILedit Forensic Express is software used to extract, analyze, and make reports on the results of data extraction on smartphones [15]. MOBILedit Forensic can extract all data from a phone, including deleted data, contacts, call history, text messages, multimedia messages, photos, videos, recordings, notes, reminders, calendar items, data files, passwords, and data from applications like Facebook, WhatsApp, Signal, WeChat, Dropbox, Evernote, Skype, Viber, and other applications. Meanwhile, Magnet AXIOM is a forensic software produced by Magnet Forensic that can process and prepare digital evidence from smartphones and computers into one report document. The Magnet AXIOM is widely used by professionals in the digital forensics field to search

for evidence that cannot be found by other forensic applications, verify data, and integrate images obtained with other tools into a single report document for the examination proces [15]. Meanwhile, based on similar previous research and related to the DFRWS framework, the given results are as below.

The research [16] conducted a live forensic examination of the Twitter application on a browser using the DFRWS method. This research uses the forensic tool FTK Imager and finds images as evidence of a crime. In the research [17], conducted a mobile forensic analysis for Android devices using MOBILedit Forensik Express and Belkasoft Evidence Center. According to the research results, 14 pieces of digital evidence were obtained using MOBILedit Forensic with an accuracy rate of 85.75%. Meanwhile, using Belkasoft, they got seven digital pieces of evidence with an accuracy rate of 43.75%. Subsequent research on digital forensic analysis was conducted by researchers [18]. In this research, the investigation of the Instagram application uses the DFRWS method. The data acquisition process with the Oxygen Forensic tool generates data in the form of conversational texts and images/photos. Meanwhile, the acquisition using JSON Viewer obtains conversational texts only. Another research through cyberbullying investigations on WhatsApp using the DFRWS method could find digital evidence in text form. The difference from this research is the identification of cyberbullying in the text. The forensic tool used in this research is MOBILedit Forensic [19].

Based on the research's description, it can be seen that previous research [15–17] did not test on several parameters, such as application info, contacts, voice call history, and video call history. Even the research on WhatsApp [19] only focuses on text parameters. Previous research [17] have not tried to find evidence using the "MOBILedit Forensic and Magnet AXIOM" tool. Likewise, research on Instagram [16] and research on WhatsApp [19] has not used the "Magnet AXIOM" tool. In addition, all previous research did not validate the forensic results obtained. From the literature review of the previous research, researchers have not found "digital forensic research on Instant Messenger "Signal"' that uses the "DFRWS framework, also MOBILedit Forensic and Magnet AXIOM tools". Therefore, the researchers simulated hoax cases related to vaccines with the DFRWS framework and the two tools, hopeful that the results could be an alternative digital forensic solution in similar cases. Besides that, this simulation is expected to contribute to digital forensic science, especially for combination of the framework and tools in the Signal Messenger application.

Different from previous researchers, the forensic process was carried out using the NIJ framework [15] and the DFRWS framework [16–19]. While, the objects in previous research were Facebook Messenger [15], Browser [16], Twitter [16], Instagram [17], and Whatsapp [19]. This research focuses on the Signal Messenger service with the DFRWS framework, and is limited to research parameters such as text conversations (chats), images, GIFs, PDF documents, videos, voice calls, and video calls. The use of the DFRWS framework is very suitable for finding digital evidence in the COVID-19 vaccine hoax case because this framework has a centralized mechanism for recording the information collected. The use of the Signal Messenger application in this study is because the Signal Messenger application ranks first before WA apps in the category of 10 best encrypted instant messaging apps for Android in 2021 [20] with a much higher security level than other instant messenger (IM) applications, especially WA applications [21]. The higher level of security makes this research difficult to obtain artifacts (digital evidence) because Signal Messenger is encrypted. This research is also a complement to previous research related to WhatsApp (WA) [19] and research related to Instagram [18]. The mobile forensic analysis was carried out on a rooted Samsung J1 Ace device and using forensic tools, namely MOBILedit Forensic and Magnet AXIOM. This research aims to see whether the existing forensic tools are capable of doing forensics. In addition, previous research used forensic tools with old versions of the application, so there is no information about additional features added to the application [15–19]. While this research was conducted using the latest version of the application.

The main objectives of this research are: 1) to conduct a simulation of digital forensics using the DFRWS framework and two forensic tools (MOBILedit Forensic and Magnet AXIOM). 2) to investigate the usability and performance of the combination of the DFRWS framework and the two tools in the case of hoax dissemination of COVID-19 Vaccine using Signal Messenger.

The main contributions of this paper are given as follows. 1) In the literature, much research and articles have been published on forensic analysis of Twitter, Instagram, Facebook, and WhatsApp. In this research, the researcher analyzes today's popular social media application (Signal Messenger) using the latest issue (COVID-19 vaccine hoax). 2) The results of the forensic tool examination are presented in this paper about the Signal Messenger application. 3) Mobile forensics with this forensic tool presents the advantages and disadvantages of this research. Mobile forensics applications are compared with each other in view of the Signal Messenger app. 4) This paper show an effective mobile forensics method for social media applications for investigators and researchers.5) It can be used as a reference for investigators in handling a case related to Signal Messenger, such as the spread of the COVID-19 vaccine hoax or other criminal cases involving Signal Messenger applications in the future. 6) The research was conducted with a validation test twice, and the accuracy was compared to previous research. It is hoped that with this research, future research will find more digital evidence, so the results of forensic analysis obtained will be better.

This research presents four main sections: introduction, research method, results and analysis, and conclusion. This section describes the background of the problem, research gaps, and the aim of research. The solution to the research problem is to perform

a digital forensic simulation using the forensic static method, which in its steps applies the DFRWS framework stages presented in the second section. The third section presents the analysis of the results and a discussion of this research. While the last section is the conclusion.

2. RESEARCH METHOD

This research is a simulation of digital forensics. Simulation of digital forensic research is research that focuses on the investigation and discovery of digital device content and is associated with computer crime. Simulation of digital forensic research with case study techniques was carried out on the vaccine hoax case. The method used in this research is the static forensic method. Statics Forensics uses conventional procedures and approaches where electronic evidence is processed when unconnected to a network. Stages of digital forensic simulation research with forensic static methods using the DFRWS framework in conducting forensic analysis. This research specifically uses Magnet AXIOM and MOBILedit Forensic tools to extract digital evidence from the Signal Messenger application on Android smartphones.

The thing being tested or the focus of the testing in this research is the performance of forensic tools according to the stages of the DFRWS framework to get digital evidence of vaccine hoax cases from the Signal Messenger application. The research stages begin with a literature review, then proceed with case simulation, forensic analysis using the DFRWS framework, and the last forensic results analysis. The research stages can be seen in the flowchart of research stages and can be seen in Figure 1. While the stages of the DFRWS framework can be seen in Figure 2. A detailed explanation can be found in sections 2.1, 2.2, 2.3, and 2.4.

2.1. Method

This research is mobile forensics in the form of a digital forensic simulation. Mobile forensics is a science derived from digital forensics or, more known as computer forensics [22]. Mobile forensics is a branch of science dedicated to recovering digital evidence from mobile devices in a forensically sound manner. Mobile forensics is required as the number of people using mobile-based services grows. As mobile computing and mobile commerce become more widespread, the demand for mobile transactions grows as well [16]. The goal of mobile forensic is to figure out what occurred to the phone and whos to blame. The investigation process in mobile forensics is systematic, with steps of documenting evidence maintained to be utilized as legal evidence in court [17].

The purpose of this research is to conduct a forensic analysis of the Signal Messenger application on an Android smartphone. Forensic tools used in this research are Magnet AXIOM and MOBILedit Forensic. Research stages can be seen in Figure 1.

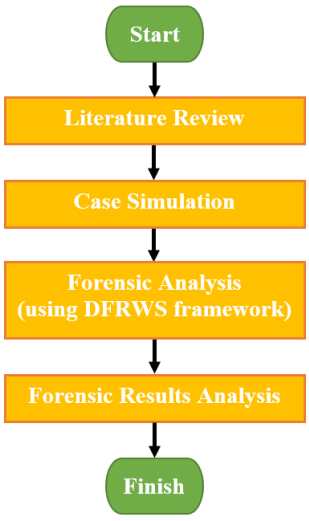


Figure 1. Flowchart of research stages

The explanation of the research stages is as follows. First, the literature review stage. This stage begins by collecting some previous research information as a reference from various sources [18]. The method used in the literature review stage is a systematic review. Systematic begins with a literature search, which is carried out through a general internet searching process and academic

search sites through Google Scholar, ResearchGate, and Science Direct. The search process was carried out using the keywords cybercrime, DFRWS framework, mobile forensics, signal messenger, and vaccine hoax. Information on literature reviews is taken from papers and journals included in reliable national and international journals. The articles used are those published in the last 5 years. Previous research related to mobile forensics and the DFRWS framework can be used as reference material for investigating android-based smartphones. The literature review used as a research reference can be seen in the introduction and research method sections.

Second, the case simulation stage. At this stage, a case scenario is created. This stage is the stage of simulating cases of spreading COVID-19 vaccine hoaxes. The research began by carrying out case simulation according to the case scenario that had been designed previously, which can be seen in Figure 4. The case simulation was carried out using two android smartphones. The victim uses one smartphone, and the perpetrator uses the other. This research case scenario explains that the perpetrator was caught along with an Android-based smartphone, which was used as a evidence. The smartphone will be investigated to search for potential digital evidence contained in the smartphone. The investigation was carried out using a laptop with MOBILedit Forensic and Magnet AXIOM software installed.

Third, the forensic analysis stage. At this stage, the simulation results are analyzed using the Digital Forensic Research Workshop (DFRWS) framework. This research focused on several variables to facilitate the search for digital evidence. The variables sought in this research include application information, contact information, chat, image, GIF, Pdf document, video, voice call history, and video call history. The forensic analysis process uses MOBILedit and Magnet AXIOM tools to find research variables. The last stage is forensic results analysis. The researcher tested the forensic results. The test is in the form of a validation test which is divided into two: repeatability and reproducibility.

2.2. DFRWS framework

The first DFRWS was hosted by G. Palmer, who developed general-purpose digital forensics investigation process. The workshops purpose was to give a freshly created community of academics and practitioners a place to exchange their understanding of digital forensic science [19]. The DFRWS method helps provide evidence and a centralized mechanism for recording the information collected [20]. The DFRWS framework has several stages, as shown in Figure 2.

Figure 2. Six stages of the DFRWS framework

Figure 2 shows the stages of the DFRWS framework, which consists of six main components, namely [21] : First, identification: This stage determines the investigations needs, including the research instruments and materials required. Second, preservation: This stage is carried out to maintain the authenticity of the evidence and refute claims that the evidence has been sabotaged. Third, collection: The collecting stage entails identifying specific components of digital evidence and data sources inside the smartphone database. Fourth, examination: The inspection stage is used to evaluate whether data from Android devices has already been filtered for specified parts of the source data. Fifth, analysis: the stage in which data is discovered and processed, including where data is obtained, who creates data, and how data is generated. The last is the presentation: this stage is for reporting the process analysis results so that the general public can understand them.

2.3. Research materials and parameters

This research uses materials to support the forensic analysis process. Research materials consist of hardware and software. Research materials can be seen in Table 1.

Table 1. The Research Materials

No.	Tools	Category	Description
1	Samsung J1 Ace	Hardware	Research object
2	Lenovo	Hardware	A workstation for forensic analysis
3	USB Connector	Hardware	Media connecting smartphone and workstation
4	Signal Messenger	Software	Software test
5	Magnet AXIOM	Software	Forensic tool
6	MOBILedit Forensic	Software	Forensic tool

While the research parameters sought were limited to text conversations (chats), images, GIFs, PDF documents, videos, voice calls, and video calls. The research parameters are focused on forensic tools. The research parameters are focused on forensic tools. The performance of each forensic tool according to the experimental results is calculated using the index number formula. The calculation of the index number used is an unweighted index, which can be seen in equation (1) [22].

$$P_{ar} = \frac{\sum ar0}{\sum arT} \times 100\% \tag{1}$$

P_{ar} is a forensic tool accuracy index number. $ar0$ is the number of detected variables. Meanwhile, arT is the total number of variables used.

2.4. Scenario cases

This research created a complete manipulation scenario with the activities carried out on the Signal Messenger application. This manipulation scenario is created and executed to obtain digital evidence. The scenario begins with a discussion of the latest information about COVID-19. The perpetrator and victim talk about COVID-19 and the COVID-19 vaccine. The conversation ended when the victim asked the truth about the spread of vaccine information and its effects. In the end, the victim did not get an answer from the perpetrator.

The purpose of the scenario is to make it easier to investigate hoax cases. The scenario is as follows: first, the perpetrator created a Signal Messenger account (account A) on an Android smartphone. Then, the perpetrator chats with the victim (account B) under normal conditions. The perpetrator also sends pictures to the victim. Next, the perpetrator sends chats and images containing hoax content to the victim. Last, the perpetrator deleted 31 chat data, 5 images, 7 GIFs, 1 PDF document, 10 video, 1 audio calls, and 1 video calls containing hoax content from the perpetrators device. The display of the Signal Messenger conversation from the perpetrator's smartphone can be seen in Figure 3.

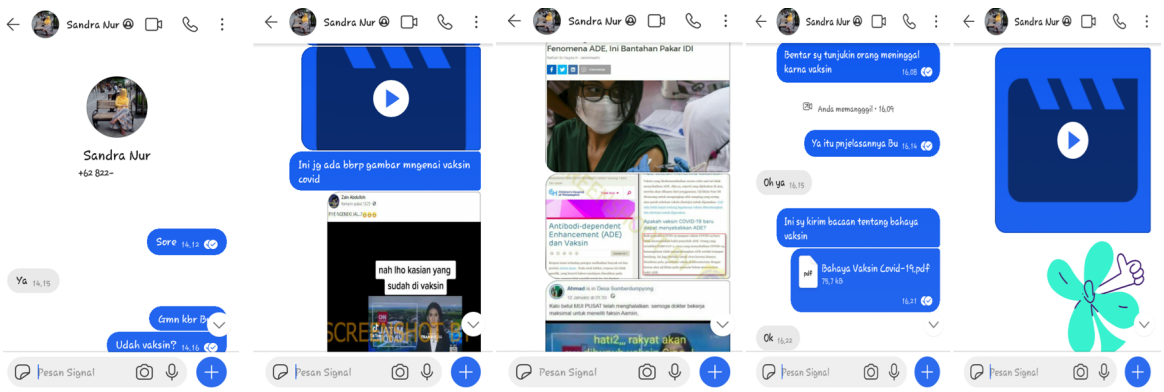


Figure 3. Display of the signal messenger

The conversation text data that has been deleted from Signal Messenger will be revealed from the perpetrators smartphone device using forensic tools. Figure 4 shows the scenario used in this research. Based on the scenario in Figure 3, it can be seen that two smartphone users use the Signal Messenger application to communicate. Account A is used as the perpetrator spreads hoaxes to other users called victims (account B). The perpetrator sends a message to the victim through the internet network, the server will received it. Signal Messenger is then forwarded to the victim.

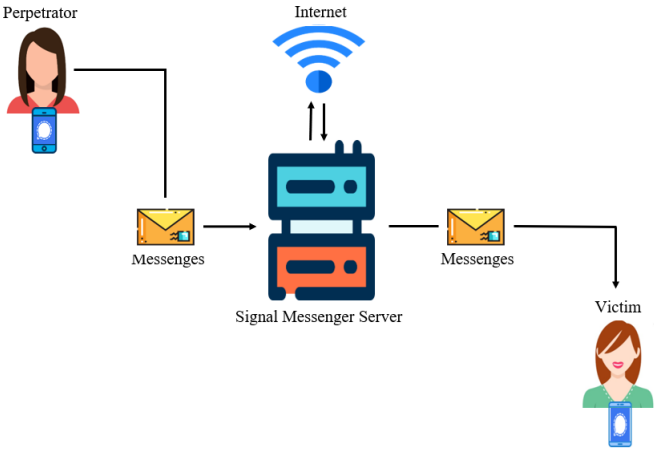


Figure 4. COVID-19 vaccine hoax case scenario

The simulation was carried out according to the COVID-19 vaccine hoax scenario that had been designed. After the simulation process has been completed, it is followed by taking the perpetrators smartphone for forensic analysis. Forensic analysis is carried out to search digital evidence in the form of application information, contact information, chats, images, GIFs, pdf documents, videos, audio call history, and video call history that the perpetrator had deleted. Forensic analyses were carried out according to the DFRWS framework.

3. RESULT AND ANALYSIS

This section discusses the results and analysis of the research. The research results are divided into 2 sections, namely forensic analysis and forensic results analysis. At the forensic analysis stage, the process or description found digital evidence of the hoax vaccine hoax case according to the stages of the DFRWS framework. Meanwhile, in the forensic result analysis section, repeatability and reproducibility validation tests are carried out on forensic results.

3.1. Forensic analysis

The forensic analysis begins when the investigators have arrested the perpetrator and android smartphone evidence. The forensic analysis process is carried out according to the six stages of DFRWS framework. The explanation for the results is as follows.

The smartphone used in this research is rooted. The smartphone is rooted to give full access rights to the investigator. Rooting makes it easier to remove the data that is on a smartphone device. The result of the smartphone rooting process can be seen in Figure 5.

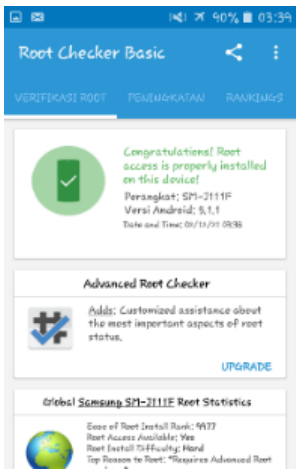


Figure 5. Root checker results

The evidence used to spread the COVID-19 vaccine hoax was the Samsung J1 Ace smartphone with the Signal Messenger application installed. Figure 6 shows evidence of a smartphone that has Signal Messenger installed. The evidence found is secured to maintain the authenticity and integrity of the evidence so that investigators can use it.

Figure 6. Smartphone evidence with the Signal Messenger application

This research uses two tools. MOBILedit Forensic managed to get information about the type and model of smartphone device, operating system version, serial number, and privileged access status. The smartphone is made by Samsung with the SM-J111F model and OS version 5.1.1. The smartphone's serial number is 42005a5eea07a400 and has privileged access. Information on the acquisition process such as the version of the forensic tool used, the date and time of the acquisition, and the duration of the acquisition process can also be known. Information on the acquisition process such as the version of the forensic tool used, the date and time of the acquisition, and the duration of the acquisition process can also be known. MOBILedit Forensic did not get digital evidence (Signal Messenger artifacts) such as chats, emails, images, GIFs, pdf documents, videos, voice call history, and video call

history that the perpetrators had deleted. The reason is that MOBILedit Forensics was unable to successfully decrypt the file because the Signal Messenger artifact was encrypted. However, MOBILedit Forensic has managed to get digital evidence of information on the signal messenger application, as shown in Figure 7.

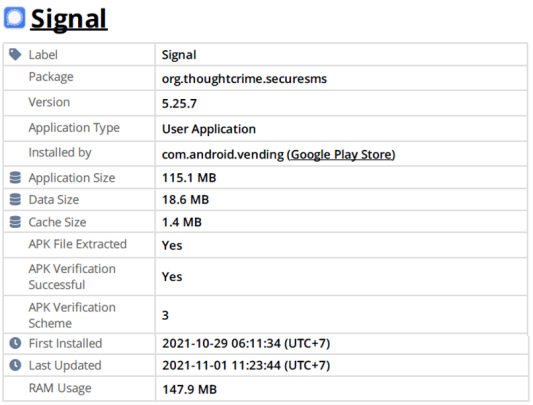


Figure 7. Evidence of application information

Based on Figure 6, it can be seen that the signal messenger application information artifact consists of the application version, application size, data size, first time installing the application, last update time, and the amount of RAM usage. MOBILedit Forensics also managed to get the Signal Messenger contact list artifact, which can be seen in Figure 8. There are ten contacts using the Signal Messenger application. One of the contacts found belonged to the victim of the spread of fake news or hoaxes. The contact list artifact provides metadata such as contact name consisting of first name, middle, and last name, phone number, and the last time the contact was modified. Application information and contact information of Signal Messenger are set to be additional information that can be obtained using the MOBILedit forensic tool so that it can be used as evidence by investigators in court.

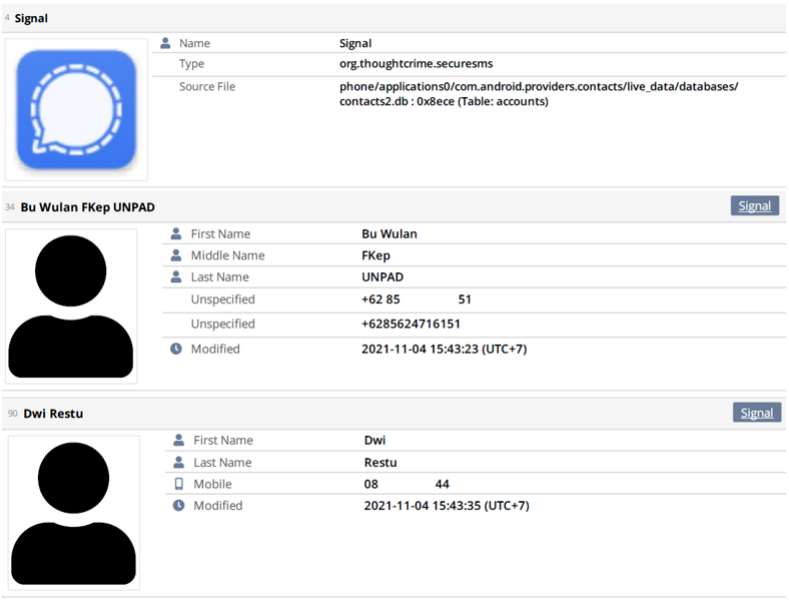


Figure 8. Evidence of contact information

Magnet AXIOM gets image artifacts and video files. Images obtained using Magnet AXIOM have the same quality as the original file. The image file artifact information consists of size, skin tone percentage, original width, original height, MD5 hash, and SHA1 hash. The file can be opened by the investigator so that the image looks clearer. The image file artifacts are shown in Figure 9.

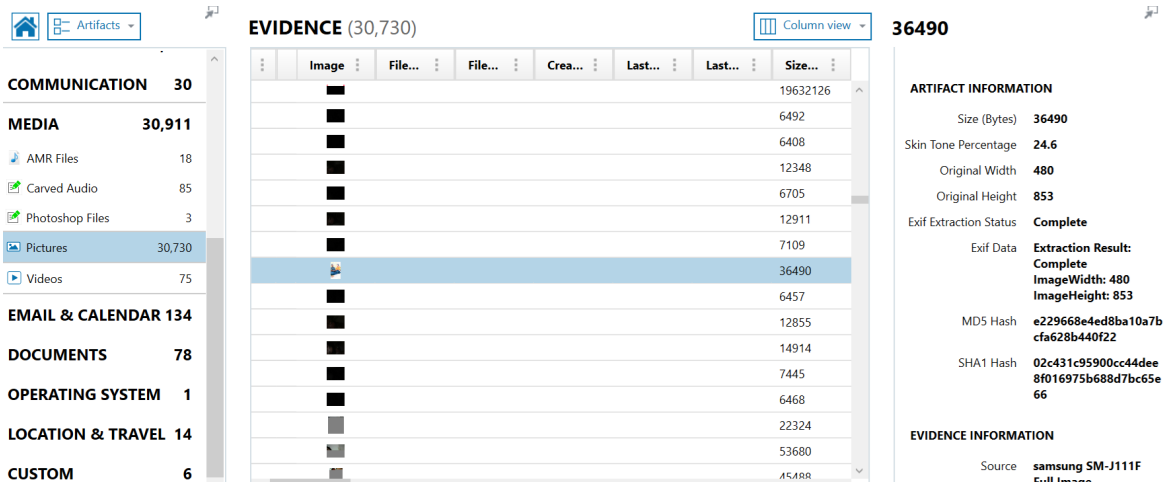


Figure 9. Evidence of picture file artifact

Similar to image file artifacts, video artifacts can also be played so that they can assist investigators in the investigation process. Video file metadata information such as file size, MD5 hash, SHA1 hash, container format, and saved video size. The video file artifacts can be seen in Figure 10. The disadvantage of Magnet AXIOM is that this tool manages to get image files and video files from Android smartphones, but the files obtained are not related to Signal Messenger. Magnet AXIOM was not successful in retrieving Signal Messenger artifacts because this tool did not succeed in decrypting files, or in other words Signal Messenger artifacts were encrypted.

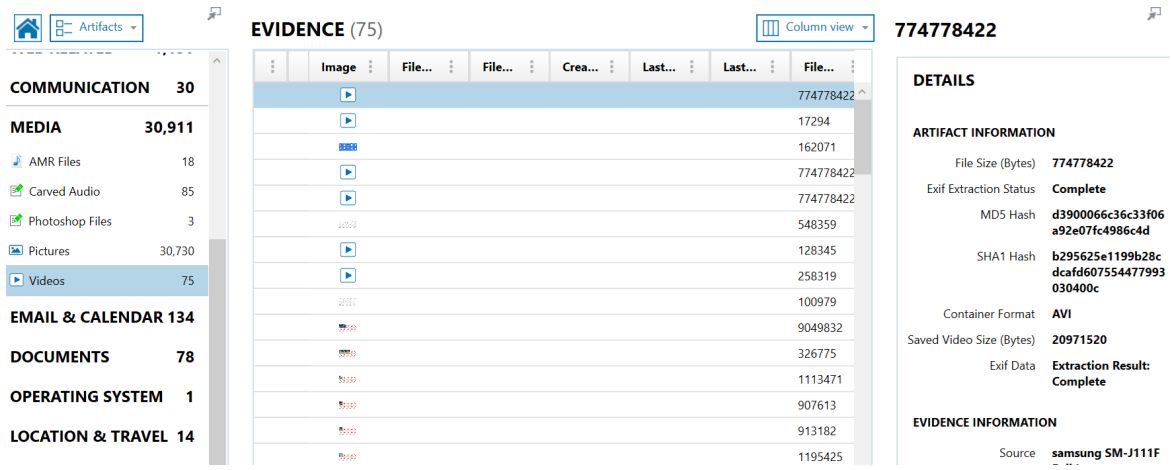


Figure 10. Evidence of video file artifact

From the explanation of the results above, it can be described as follows. The smartphone information used is physical evidence in the form of 1 unit of an Android-based smartphone. Details of the smartphone, namely Samsung J1 Ace J111F with OS version 5.1.1. The application that will be analyzed for digital evidence is the Signal Messenger application installed on an Android-based Smartphone. In the case simulation, digital evidence was created in the form of 1 account, 31 chats, 5 images, 7 GIFs, 1 pdf document, 10 videos, 1 voice call, and 1 video call. The inspection procedure carried out on the smartphone evidence found is as follows: First, the smartphone activates airplane mode to lose signal coverage before being acquired. Second, the smartphone acquisition process uses MOBILedit Forensic and Magnet AXIOM by connecting it to a Lenovo AMDA Ryzen 3 Brand workstation with OS Windows 10 64 bit and 8.00 GB RAM. Third, digital evidence extraction and analysis from the Signal Messenger application were carried out using MOBILedit Forensic and Magnet AXIOM. The smartphone forensic analysis process is carried out based on mobile forensics method procedures with the DFRWS framework. The results of the examination are as follows:

1. Digital evidence was found in the form of information on the Signal Messenger application. Application information consists of the application version, application size, data size, time of first installing the application, last time updating the application, and amount of RAM usage.
2. The forensic analysis results also found digital evidence taken from the Signal Messenger application, namely contact information. There are ten contacts of signal messenger users, and all can be found. Each contact information consists of the name and number of the signal messenger application user.
3. The MOBILedit tool is unable to get digital evidence such as chats, images, GIFs, pdf documents, videos, voice call history, and video call history. Meanwhile, AXIOM's Magnet tool could not find any digital evidence. MOBILedit forensic and Magnet AXIOM tool also cant read an applications local backup folder. A local backup is created by following the first option when creating a local backup. The name and location of the local backup are determined automatically by the application on the internal storage of the smartphone device. Detailed digital evidence can be seen in Table 2.
4. Forensic tools in the form of software used in the digital evidence retrieval process consist of 2 types with various features and capabilities.

Table 2. Forensic Tool Analysis Report Results

No.	Artifact Type	MOBILedit Forensic	Magnet AXIOM
1	Application Information	✓	-
2	Signal Messenger Contact	✓	-
3	Chat	-	-
4	Image	-	-
5	GIF	-	-
6	Pdf Document	-	-
7	Video	-	-
8	Voice Call History	-	-
9	Video Call History	-	-
Performance Index Score		22.22%	0%

The MOBIL edit Forensic Express tool has performance value 22.22% because it can only find two of nine digital evidence parameters sought according equation (1). Meanwhile, the Magnet AXIOM tool did not find any of these nine parameters. The calculation of performance value to measure the ability of each forensic tool can be calculated as follows.

$$\text{MOBIL edit Forensic Express} : Par = \frac{2}{9} \times 100\% = 22.22\%$$

$$\text{Magnet AXIOM} : Par = \frac{0}{9} \times 100\% = 0\%$$

Based on the results of the research, comparisons can be made with previous research. Comparison of research results obtained in other studies using the DFRWS framework, MOBILedit Forensic and Magnet AXIOM can be seen in Table 3.

Table 3. Comparison with The Results of Previous Research

No.	Title	Object	Artifact Type	Forensic Tools used	Result
1	Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop (Ikhsan Zuhriyanto, Anton Yudhana, and Imam Riadi, 2020)	Twitter	14 artifact such as application info, account info, twitter ID, friends, user, conversation (DM), cached search, audio, video, text, picture, tweets, IP adress, url, email, and location	MOBILedit Forensic and Belkasoft Evidence Center	From the MOBILedit forensic tool get14 from 16 artifacts (digital evidence) with an accuracy rate of 85.75%. Meanwhile, the Belkasoft tool get 7 artifacts with an accuracy rate of 43.75%
2	Investigation on Instagram Android-based Using Digital Forensics Research Workshop (Satrio Pambanyun and Imam Riadi, 2020)	Instagram	Photo, video, text, user name, and link	Oxygen forensics and JSON Viewer	From the Oxygen forensic tool get evidence such as photos, videos, text, user names, and links. Meanwhile, the JSON Viewer tool can only find digital evidence such as text, user names, and links
3	Analisis Barang Bukti Digital aplikasi Facebook Messenger pada Smartphone Android Menggunakan Metode NIJ (Ikhwan Anshori, Khairina Eka Setya Putri, and Umar Ghoni, 2021)	Facebook Messenger	Account, chat, and image	MOBILedit Forensic, Magnet AXIOM, and Oxygen Forensic	From the MOBILedit Forensic tool get digital evidence such as accounts (100%), chats (55%), and pictures (86%). Similarly, for the level of accuracy for the AXIOM Magnet tool for each parameter. While the Oxygen Forensic tool gets digital evidence such as accounts (100%), chat (5%), and pictures (86%)
	This Research	Signal Messenger	Application information, contact, chat, image, GIF, pdf document, video, voice call history and video call history	MOBILedit Forensic and Magnet AXIOM	From the MOBILedit Forensic tool get application information and signal messenger contact with a performance value of 22.22%

Based on table 3, it can be seen that the results of the researchers' research were compared with research on the Twitter application [23], research on the Instagram application [24], and research on the Facebook Messenger application [25]. When compared to previous research, this research has a lack, namely the difficulty of finding digital evidence. Researchers only found 2 of 7 digital evidence. Digital evidence can only be found using the MOBILedit forensic tool. This is because the lack of ability of the MOBILedit Forensic tool and the inability of the Magnet AXIOM tool to recover lost data in this research are the reasons for the shortage of forensic tools so that they cannot read the deleted data. In addition, the inability of the tool to restore deleted data is proof that the Signal Messenger application is an application with a very high level of personal data security compared to other instant messenger applications. The level of security of personal data is a supporting factor for switching instant messenger application users, especially WhatsApp application users, to the Signal Messenger application. Personal data security or information security is crucial since it is easy to get data and information this time. Data and information must be protected so that non-interested parties are unaware of their presence [26].

3.2. Forensic results analysis (validation)

Forensic results testing begins with a validation test which is divided into two, namely repeatability and reproducibility. Next, analyze the results of the acquisition of forensic tools using parameters. Research Parameters used is the Signal Messenger artifact that can be used as evidence of a criminal act. The research parameters are application information, contact information, chat, image, GIF, Pdf document, video, voice call history, and video call history. Repeatability validation is done by repeated testing using the same forensic tool. The test was carried out two times. Meanwhile, reproducibility validation is done by testing the same object using

two different forensic tools in a relatively close time. The results of forensic tools' repeatability and reproducibility test can be seen in Table 4.

Table 4. Result of Repeatability and Reproducibility Validation Test

No.	Validation Test	MOBILedit Forensic		Magnet AXIOM	
		Test 1	Test 2	Test 1	Test 2
1	Repeatability	✓	✓	✓	✓
2	Reproducibility	✓	✓	✓	✓

From Table 3, it can be explained that the validation process was carried out on a smartphone using the MOBILedit Forensic and Magnet AXIOM tools. The extraction results using the MOBILedit Forensic tool were carried out twice and found application information and ten Signal Messenger contacts. While using the Magnet AXIOM tool, no digital evidence was found even though two extractions had been carried out. The forensic tools used are declared to have met the reproducibility validation test if the results obtained from each forensic tool are similar and do not change. The forensic process is carried out repeatedly in very close time using the same method and research object with different research tools. The results of this research can be used as a basic reference for further research on Signal Messenger using other forensic tools with the latest versions, which can be supported to get more digital evidence.

Repeatability validation gave positive results so that the performance of the forensic tool was considered feasible to carry out the forensic process on the Signal Messenger application installed on the Smartphone. Similar to reproducibility validation, the forensic tools used are declared to have met the test if the results obtained from each forensic tool are similar and have not changed. This follows the statement and the results of the validation test in the research [27]. In this research, repeatability and reproducibility validation results were the same and did not change.

4. CONCLUSION

Based on the results of the tests carried out on Signal Messenger and the discussion in this research, it can be concluded that MOBILedit Forensic and Magnet AXIOM evidence meets validation tests of repeatability and reproducibility. Magnets AXIOM did not get Signal Messenger digital evidence from the perpetrator's smartphone. But MOBILedit Forensic managed to get application information and contact information of Signal Messenger with a performance value of 22.22%. MOBILedit Forensic and Magnet AXIOM did not get digital evidence such as chat, images, GIFs, pdf documents, video, voice call history, and video call history from Signal Messenger because these tools could not manage to decrypt the file since the Signal Messenger artifact was encrypted. In comparison with previous research, it is proven that the Signal Messenger application is more powerful in terms of security features. For further research, researchers suggest studying mobile forensic methods, frameworks, and using other forensic tools with the latest versions so that they can be expected to provide more accurate results in the process of getting digital evidence.

REFERENCES

[1] Hootsuite, "Digital 2020. Hootsuite," 2020.

[2] D. PPI, "Survei Penetrasi Pengguna Internet di Indonesia Bagian Penting dari Transformasi Digital," 2020.

[3] K. Lutfiyah, "Review Article: Hoax and Fake News During Covid-19: Is the Law Effective in Overcoming it?" *The Indonesian Journal of International Clinical Legal Education*, vol. 2, no. 3, pp. 345–360, 2020.

[4] A. Septiadi and L. Alfarizi, "Pemanfaatan E-KTP Sebagai Alat Bantu Sistem Kehadiran Pegawai dalam Penanggulangan Penyebaran Covid-19," *Matrik: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 1, pp. 159–168, 2020.

[5] H. Wijoyo, "Persepsi Mahasiswa Tentang Aplikasi Chatting Signal," *Jurnal Teknologi dan Informasi Bisnis*, vol. 3, no. 1, pp. 153–156, 2021.

[6] P. Rösler, C. Mainka, and J. Schwenk, "More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema," in *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2018, pp. 415–429.

[7] A. Afzal, M. Hussain, S. Saleem, M. Shahzad, A. Ho, and K. Jung, "Encrypted Netwok Traffic Analysis of Secure Instant Messaging Application: A Case Study of Signal Messenger App," *Applied Sciences*, vol. 11, no. 17, p. 7789, 2021.

[8] M. Kilic, "Encryption Mesthods and Comparison of Popular Chat Applications," *Advances in Artificial Intellegence Research (AAIR)*, vol. 1, no. 2, pp. 52–59, 2021.

[9] Sunardi, I. Riadi, R. Umar, and M. Gustfi, "Audio Forensics on Smartphone with Digital Forensics Research Workshop (DFRWS) Method," *CommIT (Communication & Information Technology) Journal*, vol. 15, no. 1, pp. 41–47, 2021.

[10] P. Pahrudin, "Cybercrime in the Context of Cellular Telephone Scams," *Jurnal Penelitian Pos Dan Informatika*, vol. 10, no. 1, pp. 73–85, 2020.

[11] A. Lee, "Online Hoaxes, Existential Threat, and Internet Shutdown: A Case Study of Securitization Dynamics in Indonesia," *(ISSH), Journal of Indonesian Social Sciences and Humanies*, vol. 10, no. 1, 2020.

[12] A. Davina, S. Suseno, and M. Haffas, "Penerapan Hukum Penyebaran Hoax Mengenai Covid-19 Melalui Facebook Berdasarkan UU ITE dan Hukum Pidana," *Media Keadilan Jurnal Ilmu Hukum*, vol. 12, no. 1, pp. 1–25, 2021.

[13] S. Harnett, "Health Literacy, Social Media and Pandemic Planning," *Journal of Consumer Health on the Internet*, vol. 24, no. 2, pp. 157–162, 2020.

[14] KOMINFO, "Penanganan Sebaran Konten Hoax Vaksin Covid-19," 2021.

[15] I. Riadi, A. Yudhana, and M. Barra, "Forensik Mobile pada Layanan Media Sosial LinkedIn," *JISKa*, vol. 6, no. 1, pp. 9–20, 2021.

[16] A. Al-Dhaqm, S. Razak, R. Ikuesan, V. Kebande, and K. Siddique, "A Review of Mobile Forensic Incestigation Process Model," *IEEE*, vol. 8, 2020.

[17] F. 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.

[18] Sunardi, I. Riadi, and M. H. Akbar, "Penerapan Metode Statics untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS," *Jurnal Resti (Rekayasa Dan Teknologi Informasi)*, vol. 4, no. 3, pp. 576–583, 2020.

[19] S. Rani, "Digital Forensic Models: A Comparative Analysis," *International Journal of Management, IT & Engineering*, vol. 8, no. 6, 2018.

[20] I. Wahyudi, A. Muntasa, M. Yusuf, and A. Hamzah, "Mengungkap dan Menguji Keaslian Bukti Digital pada Kejahatan Cybercrime dengan Metode Digital Forensic Research Workshop," *Jurnal Aplikasi Teknologi Informasi dan Manajemen (JATIM)*, vol. 2, no. 2, 2021.

[21] Sumardi, I. Riadi, and M. Akbar, "Steganalisis Bukti Digital pada Media Penyimpanan Menggunakan Metode Static Forensics," *Jurnal Nasional Teknologi dan Informasi*, vol. 6, no. 1, pp. 1–8, 2020.

[22] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic Tools Performance Analysis on Android-based Blackberry Messenger using NIST Measurements," *International Journal of Electrical and Computer Engineer (IJECE)*, vol. 8, no. 5, pp. 2991–4003, 2018.

[23] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Analisis Perbandingan Tools Forensic pada Aplikasi Twiter Menggunakan Metode Digital Forensics Research Workshop," *Jurnal Resti (Rekayasa Dan Teknologi Informasi)*, vol. 4, no. 5, pp. 829–836, 2020.

[24] S. Pambanyun and I. Riadi, "Investigation on Instagram Android-based Using Digital Forensics Research Workshop Framework," *International Journal of Computer Applications*, vol. 175, no. 35, 2020.

[25] I. Anshori, K. Putri, and U. Ghoni, "Analisis Barang Bukti Digital Aplikasi Facebok Messeger pada Smartphone Android Menggunakan Metode NIJ," *IT Journal Research and Deve;opment (ITJRD)*, vol. 5, no. 2, 2021.

[26] L. Widyawati, I. Riadi, and Y. Prayudi, "Comparative Analysis of Image Steganography using SLT, DCT and SLT-DCT Algorithm," *Matrik: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 1, pp. 169–182, 2020.

[27] I. Riadi, R. Umar, and M. Syahib, "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)," *Jurnal Resti (Rekayasa Dan Teknologi Informasi)*, vol. 5, no. 1, pp. 45–54, 2021.