IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 27, No. 6, December, 2022, pp. 903-913
Journal homepage: http://iieta.org/journals/isi

Mobile Forensic Analysis of Signal Messenger Application on Android using Digital Forensic Research Workshop (DFRWS) Framework

Imam Riadi[1], Herman[2], Nur Hamida Siregar[2*]

[1] Department of Information System, Universitas Ahmad Dahlan, Yogyakarta 55164, Indonesia
[2] Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta 55164, Indonesia

Corresponding Author Email: nur2007048007@webmail.uad.ac.id

https://doi.org/10.18280/isi.270606

Received: 10 November 2022
Accepted: 20 December 2022

Keywords:
android, COVID-19 vaccine, cybercrime, DFRWS framework, hoax, mobile forensic, signal messenger

ABSTRACT

Cybercrime is a crime committed using equipment connected to the internet. One of the cybercrimes that occured during the COVID-19 pandemic was the spread hoaxes about the Covid-19 vaccine which caused panic in society. Signal Messenger is one of the social media that has become a trending topic since the number of personal data security issues and the emergence of end-to-end encryption features. This research aims to find digital evidence on Signal Messenger application installed on the perpetrator's Android smartphone. This research uses Belkasoft, Magnet AXIOM, and MOBILedit Forensic Express tools and implements the Digital Forensics Research Workshop (DFRWS) framework in each stage of the research experiment. The research was carried out according to the case scenario with 11 predetermined parameters. Digital evidence is found from the Signal Messenger application: application information, account information, chat, pictures, videos, contacts, and stickers. The results of this research indicate that Belkasoft Evidence Center forensic tool is better, with an accuracy rate of 78.69%, while Magnet AXIOM is 26.23% and MOBILedit Forensic Express is 9.84%. The results of this research can be used as a reference for other forensic researchers/experts in handling similar crime cases on the Signal Messenger application to get better results.

1. INTRODUCTION

Pandemic comes from the Greek word consisting of the words "pan" and "demos", which can be translated as "all the people." A pandemic is an illness that strikes and then leaves the human population [1]. The continuing coronavirus disease 2019 (COVID-19) pandemic is affecting people worldwide and has spread to Indonesia. On March 2, 2020, Indonesian authorities discovered their first COVID-19 positive case. The discovery of this case was confirmed through reports of the first two cases of COVID-19 infection in Indonesia by President Joko Widodo that day, which until April 2 had reached 1790 confirmed cases [2]. As of April 9, when the pandemic had spread to 34 provinces, DKI Jakarta, West Java, and Central Java were the Indonesian provinces most exposed to the coronavirus [3]. The government is attempting to promptly handle the situation by creating a team to manage COVID-19, directly directed by the President. At the same time, the World Health Organization (WHO) declared the first step in combating the pandemic is to hygiene measures, hand washing, and people should respect social distancing rules by at least one meter to stop the transmission of COVID-19 worldwide so that it can slow the spread of the virus pandemic [4, 5]. The government also requires the public to use well-fitting masks, always apply hand hygiene rules, and avoid contact with others (physical distancing) [6]. Implementing physical distancing rules makes people work at home, change home activities such as shopping at the market into online shopping, and change some activities into other activities that they can do online. This activity makes people today prefer to use smartphones to overcome monotony.

Technological developments are one of the reasons behind the increase in smartphone technology. Smartphones have increased in terms of power, speed, and storage space, and more features and applications are available so that most people use their smartphones for various activities such as bill payments, online shopping, chatting, making calls, email, sharing social media, and communication via instant message [7-9]. Social media significantly influences people's lives because social media is used to build wider connections [10]. Figure 1 shows data on the usage of smartphones (mobile devices), the internet, and social media worldwide.

Figure 1. Global social media and internet users in 2022

Social media usage increased significantly by 10.1%, from 4.20 billion active users in 2021 to 4.62 billion active users in February 2022 [11]. Lastly, a report in April 2022 showed active social media users approximately 4.65 billion [12]. Social media has positive and negative impacts. The positive side is that it encourages economic growth in digitization, innovation, and information technology development. The negative side is social media facilitates the development of serious malicious activity and cybercrime [13].

Cybercrime is a criminal act carried out using any equipment as long as the equipment is connected to the internet [14]. Cybercrimes tend to be more difficult to prove than real-world crimes. Cybercrime is often defined as "a hidden crime [15]". One of the many examples of cybercrime during the COVID-19 pandemic is the spread of false information. False information is popularly and widely known as a hoax [16]. A hoax is an untrue information or fake news that has no certainty, and the spread of hoaxes aims to cause panic or unrest in the community. Currently, there is a term that is well known as "infodemic." Infodemic is a term for the spread of hoaxes or rumors, and stigma during a pandemic [17].

Since the launch of the COVID-19 vaccine in Indonesia, false information has emerged that has spread through the media. Mostly on social media. Some of the news circulating is: First, vaccine safety cases claim that many people died due to vaccine injections. Second, the status of the COVID-19 vaccine, which contains pork oil, so it is not halal to use. Third, the video cases show empty syringes without liquid vaccine content. Fourth, the conspiracy about the COVID-19 vaccine is a product of propaganda. Social media users have been inundated with false information and left in fear. Information of every type spreads more quickly than viruses do [18]. One of the most widely spread types of vaccine hoaxes on social media today is a hoax that states the COVID-19 vaccine contains a magnetic chip. Some people have even tried to prove this theory by making videos showing a coin or spoon stuck to their arm [19]. Since the discovery of the first COVID-19 case in Indonesia, news about COVID-19 has spread faster and created uncertainty due to limited knowledge and information about the pandemic situation [20]. Social media exacerbates the spread of hoaxes when all countries worldwide are experiencing difficult times due to the COVID-19 pandemic. Undeniably, the widespread hoaxes are caused by the increased usage of social media applications. Social media applications currently provide online-based short messages or instant messaging (IM), which offers convenient communication. The features provided by various IM applications are the main attraction of this application. Therefore, user policies when using IM applications are essential. While using IM applications, users share their personal data without realizing it, leaving any personal data on their mobile devices [7]. Thus, the right solution is to choose an IM application that upholds personal data privacy to prevent users from experiencing material or immaterial losses.

With concerns about users' personal data privacy, many developers are competing to build and launch new IM applications that incorporate end-to-end encryption and add encryption to their protocols to protect communications to servers that deliver messages [21]. Signal Messenger is one of the most popular end-to-end encrypted IM applications and is well-known for its privacy features. A new privacy feature introduced by Signal makes it more challenging to identify a sender. The privacy feature is the reason for the spike in downloads of the Signal application on the Google Play Store and App Store, along with the change in WhatsApp's data sharing policy in January 2021 [22]. Users (both employees and the general public) of their own volition are starting to switch to using Signal Messenger because the services of this application are more reliable. This reason also allows cybercriminals to use this application because it is more secure. Perpetrators usually delete messages after committing cybercrime to erase all traces of their activity. The increasing problem of cybercrime indirectly increases the necessity of mobile forensics [23]. Also, it creates opportunities for using techniques and forensic tools to investigate this cybercrime so that the artifacts found can be used as digital evidence and accepted by the courts [24].

Several previous studies that conducted forensic analysis using the Digital Forensic Research Workshop (DFRWS) framework showed different results. A research about mobile forensics on an Android-based IMO messenger application using MOBILedit forensic express, DB Browser for SQLite, AccessData FTK imager, and Belkasoft obtained evidence in the form of chat files, images, audio, video belonging to the perpetratos accounts, and chat times that have been deleted from a smartphone device in root condition [25]. Meanwhile, another research conducted on digital forensic investigation on the Android-based instagram with the DFRWS using the Oxygen tool obtained chats and pictures/photos, while the Json viewer only obtained chats data [26]. The difference in the results of forensic evidences with the same framework from these studies underlies the researcher to conduct further research on forensic analysis of the Signal messenger application on android using the DFRWS framework.

Based on the increasing use of social media phenomena, problems of widespread COVID-19 vaccine hoaxes, and the growing use of Signal Messenger application, and research gaps, the researchers investigated the simulation of vaccine hoax cases on Signal Messenger application. Forensic analysis of a vaccine hoax case simulation was carried out using the Digital Forensic Research Workshop (DFRWS) framework. This research used three forensic tools to get digital evidence from Signal Messenger application. The forensic tools used are Belkasoft Evidence Center, Magnet AXIOM, and MOBILedit Forensic Express. This research aims to demonstrate the ability of forensic tools to find digital evidence (artifacts) from the Signal Messenger application. The main contributions of this paper are as follows: 1) In previous research, many papers have been published discussing forensic analysis on WhatsApp, Twitter, Facebook, Instagram, Blackberry Messenger, and IMO Messenger. The researcher analyzes the current popular Signal Messenger instant messenger application in this paper. 2) This paper demonstrates the effective framework used in mobile forensics for instant messenger applications to research and investigation experts. 3) As a complement to previous research related to Signal Messenger, it can show the ability of forensic tools to find digital evidence. The capabilities of the forensic tools used are compared in this paper. 4) This paper can be a reference for investigators and researchers when they see cybercrime cases on the Signal Messenger application.

This paper consists of five sections. The first section is the introduction which describes the background of the problem, research gaps, research aims, and the contribution of this paper. The second section describes materials related to the research and previous similar studies. The third section presents the experiment research stages, the case scenario, and the research tools used. Section four is the results and discussion of the

section report preparation of case scenarios and the results obtained from the forensic analysis process. Meanwhile, the last section describes conclusions and suggestions for future research .

2. LITERATURE REVIEW

2.1 Signal

Signal is a social media application that provides IM services. It is a free and open source IM created by the Signal Technology Foundation and can be accessed on iOS, Android, and a Google Chrome extension [21, 27]. Common features of the Signal service include texts, stickers, media messages, voice messages, audio calls, video calls, typing indicators, and more. Each communication has a security number that may be checked between the persons involved [28].

Signal encrypts all communication end-to-end using the Signal protocol, encrypts SQLite databases using SQLCipher, and keeps media and file attachments as encrypted blobs inside the application sandbox. Signal offers the messenger lock feature, enabling users to open the messenger application by entering the pin, password, or fingerprint associated with their Android device [27].

2.2 Mobile forensic

The tremendous growth in all fields of science and technology is known as technological advancement. The modern era of the fourth industrial revolution with new and enabling technologies and systems, such as artificial intelligence (AI), virtual/augmented reality, machine learning, cloud computing, blockchain, big data, Internet of Things (IoT), 5G, and cyber security gives a profoundly positive impact on improving the quality of life and experience [29]. However, advances in Information and Communication Technology (ICT) and the emergence of IoT devices have increased the misuse of mobile technology and applications for criminal acts. The significant increase in smartphone storage capacity and the number of installed applications on smartphones make it difficult for investigators to conduct investigations to identify data related to criminal acts. Investigators are also hindered by security and privacy concerns when obtaining crucial digital evidence from encrypted devices or encrypted messaging apps, which can even stop the inquiry. As a result, the need for mobile forensics has risen steadily over recent years.

Mobile forensics is the process of recovering digital information or data that is frequently used as evidence in criminal cases [30]. Mobile forensics can also be interpreted as a term to describe the seizure, collection, and analysis of evidence held on mobile devices for use in court [31]. Therefore, mobile forensics is closely related to digital forensics. Critical forensics investigations are conducted on mobile devices since they hold much important personal information [32].

2.3 DFRWS framework

The goal of DFRWS is to promote the exchange of knowledge and concepts about digital forensic research [32]. The first DFRWS was held in 2001 in Utica. This workshop, located in Utica, New York, discussed the digital forensics conditions at that time. The stages of the DFRWS framework can be seen in Figure 2.

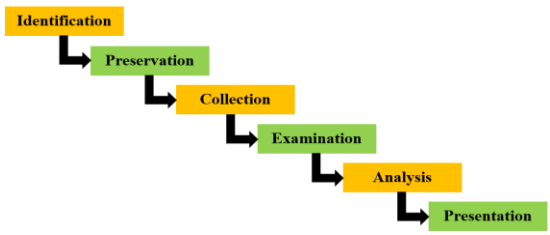


Figure 2. The DFRWS framework stages

The DFRWS framework consists of six stages and begins with the identification stage [33]. The identification stage's primary objective is to identify the objects, elements, and information connected to a crime. It is important to follow the correct procedures when taking photos and documenting the crime scene and the evidence. Second, the preservation stage by carrying out the preservation process to prevent the evidence that has been obtained and ensure the authenticity and integrity of the evidence to avoid unauthorized parties so that the evidence is not contaminated and is truly valid and legitimate. The validity of evidence and allegations of tampering with evidence can be confirmed and disproved using proper chain of custody documentation. In addition, the risk that the evidence will not be admissible in court is reduced because it offers complete information about the ownership and placement of evidence during the case. The next stage is the collection stage. The collection stage is the process stage of collecting evidence samples suspected that have the potential as strong evidence. The fourth and fifth stages are the examination stage and the analysis stage. The examination and the analysis stages are crucial stages of the DFRWS framework. The process of tracking evidence, validating evidence, and recovering hidden or encrypted data is carried out at this stage. The last stage is presentation, a process related to documentation, testimony from experts, etc.

2.4 Previous studies

Riadi et al. conducted a forensic analysis of the Instagram application following the stages of the National Institute of Standards and Technology (NIST). The Oxygen Forensic tool found digital evidence of images and chats with a performance level of 84%. Meanwhile, using Magnet AXIOM tool, it can find digital evidence of images and chats with a performance level of 100% [34]. Umar et al. conducted mobile forensics on a smartphone using WhatsApp Key/DB Extractor forensic tool and Belkasoft Evidence with NIST forensic methods to extract the latest WhatsApp artifacts. In their study, the capabilities of forensic tools were evaluated and compared. With WhatsApp Key/DB Extractor, it obtained only two of four artifacts (text message and image). Meanwhile, Belkasoft Evidence obtained three artifacts (image, video, and document) [7].

In their research, Ichsan and Riadi only used three stages of the DFRWS method. The three stages include identification, preservation, and collection. This research used two smartphones with root (seller/perpetrator) and non-root (buyer/victim) conditions with IMO Messenger application installed. Evidence from the narcotics transaction case scenario was obtained using four forensic tools: AccessData FTK Imager, Belkasoft, DB Browser for SQLite, and MOBILedit Forensic Express. Digital evidence includes the

perpetrator's account, chat files, chat time, pictures, audio, and deleted video from the perpetrator's smartphone device. The index number for AccessData FTK Imager performance is 33.33%, Belkasoft is 83.33%, DB Browser for SQLite is 33.33%, and MOBILedit forensic express is 100% [25]. Previous research about mobile forensic analysis of Signal services on smartphones is as follows. Azhar et al. attempted to perform a forensic analysis on Android and iOS smartphones using NIST measurements. For iOS smartphones, the messaging applications investigated are Snapchat, Cyberdust, and Confide. Meanwhile, for Android smartphones, the applications investigated are Facebook Messenger, Wire, Confide, and Signal. The Android smartphone is already rooted. Forensic analysis of the Signal application using Oxygen Forensic tool. However, the analysis results did not get any relevant data related to conversations and account information [35].

Riadi et al. explained mobile forensics on Signal Messenger application installed on the Samsung J1 Ace smartphone (rooted condition). Forensic analysis was carried out according to the DFRWS stage and using the forensic tools Magnet AXIOM and MOBILedit Forensic to obtain digital evidence (artifacts) from deleted messages on the perpetrator's smartphone. MOBILedit Forensic gets any digital evidence (application information and contact) with a forensic tool performance value of approximately 22.22%. Meanwhile, AXIOM's Magnet tool revealed no digital evidence (artifacts) related to the deleted message [36].

3. THE PROPOSED APPROACH

The research aimed to conduct mobile forensic experiments to obtain digital evidence from cases of spreading COVID-19 vaccine hoaxes on the Signal Messenger application.

3.1 Experiment research stages

The forensic process that was carried out in this research adopted the DFRWS framework. The experimental workflow of the research is shown in Figure 3.

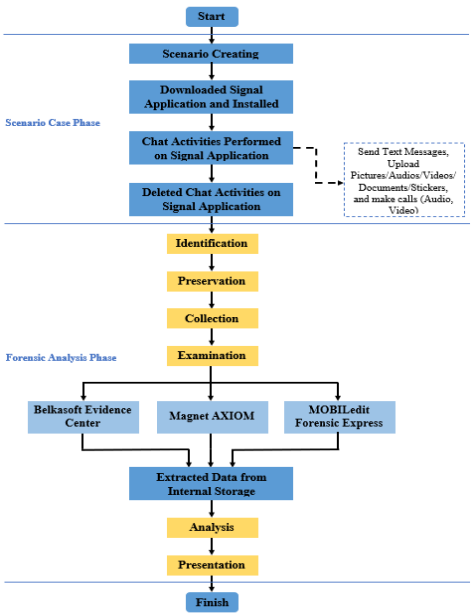


Figure 3. Flowchart of experiment research stages

Figure 3 shows how experiment research is conducted systematically so the stages can be used as guidelines to overcome the problems in this research. Researchers divided the stages of this experimental research into two phases.

1. *Scenario Case Phase* is where experiment research begins. In this phase, researchers design case scenarios to serve as guidelines, so case simulations run better and are more focused. Researchers also prepare tools used for case simulation. Next, the Signal Messenger application is downloaded and installed on the mobile device. Then proceed with carrying out a case simulation (conversation between the perpetrator and the victim) according to the designed case scenario and finally delete the conversation on the signal messenger application on the perpetrator's android smartphone.
2. *Forensic Analysis Phase* is where the DFRWS framework is implemented, namely identification, preservation, collection, examination, analysis, and presentation.
   a. *Identification*, determining the objects, component and information related to a crime.
   b. *Preservation*, preventing the evidence obtained from being contaminated and guaranteeing the authenticity and integrity of the evidence.
   c. *Collection*, acquiring and extracting data on the perpetrator's smartphone to collect data that is believed to be related to the crime.
   d. *Examination*
   The extraction process at the examination stage was carried out using three forensic tools two times. The forensic tools used were: Belkasoft Evidence, Magnet AXIOM, and MOBILedit Forensic Express.
   e. *Analysis*
   The repetition of the extraction process is intended to confirm the validity of the forensic tool. The results are analyzed to determine the advantages and disadvantages of each forensic tool in finding digital evidence from the signal messenger application.
   f. *Presentation*
   Presentation stage involves reporting the case analysis results, conducting discussions, and providing conclusions. The purpose of the presentation stage is to communicate the process analysis results in a way that the public can easily understand.

3.2 Case scenario

Case scenarios aim to simplify the identification process when analyzing digital evidence. The evidence secured was an Android smartphone. A perpetrator uses smartphones to communicate with victims, so the crime of spreading COVID-19 vaccine hoaxes runs smoothly. Here is Figure 4 shows the case scenario in this research.

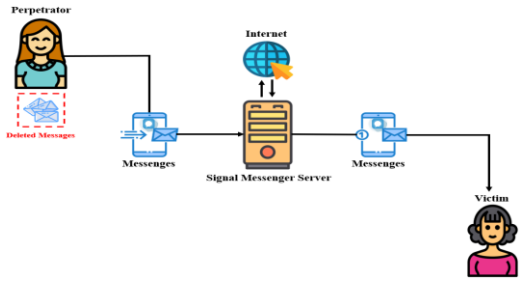


Figure 4. Case scenario of hoax vaccine simulation

The case scenario begins with the perpetrator chatting with the victim. At first, the perpetrator asked whether the victim had been vaccinated or not. Furthermore, a perpetrator scared the victims by spreading hoaxes about the COVID-19 vaccine. A perpetrator not only sends images, videos, audio, and documents but also makes voice calls and video calls to convince victims that vaccines are dangerous. The perpetrator also ordered the victim to spread the dangers of the vaccine to others. The scenario case ends with the perpetrator deleting all the contents of the conversation between himself and the victim in the signal messenger application. After the researcher got a smartphone, a mobile forensic process was conducted to obtain appropriate evidence of a crime. The results of the evidence will be presented as additional evidence at trial.

3.3 Research tools

This research uses hardware and software tools to get signal messenger artifacts. The tools used are shown in Table 1.

Table 1. Research tools

Tools	Description
Xiaomi Redmi 9T	Research Object
Lenovo	Workstation
USB Connector	Connector
Signal Messenger	Instant Messaging Application
Belkasoft Evidence Center	Forensic Tool (Trial Version)
Magnet AXIOM	Forensic Tool (v5.4)
MOBILedit Forensic Express	Forensic Tool (v7.4)

The datasets from the research tools used to perform a series of simulations are listed in Table 1. The tools consist of Xiaomi Redmi 9, Lenovo, and a USB connecter as hardware. In contrast, the software includes Signal Messenger as the software to be tested. Meanwhile, Belkasoft Evidence Center, Magnet AXIOM, and MOBILedit Forensic Express are mobile forensic software (forensic tools). Belkasoft Evidence Center is a forensic software for acquiring, examining, analyzing, and displaying digital evidence from cloud services and primary sources such as computers, RAM, and mobile devices in the proper way, from a forensic perspective [37].

Magnet AXIOM is one of the most widely used forensic tools by professionals in the digital forensics field to search for evidence that other forensic applications cannot find. Deleted data can be quickly recovered using Magnet AXIOM. Digital forensic experts can also use this software to make reports, examine digital evidence, and distribute portable case files [38]. MOBILedit Forensic is a mobile forensic tool created by Compelson to search, evaluate, and report data in a single solution [39]. MOBILedit Forensic is exceptional for advanced application analyzers, live updates, deleted data recovery, concurrent phone processing, fine-tuned reports, a wide range of supported phones, including most feature phones, and an easy-to-use user interface. Connecting the software with the phone can be done through an infrared connector, Bluetooth connection, Wi-Fi connection, or wired interface. Usually, after the connection, the identified phone model is a related device image, the manufacturer, serial number (IMEI), model number, and phone status.

In facilitating the search for evidence, the focus is on search variables (parameters) consisting of application information, account information, chat, images, audio, video, documents, voice call history, video call history, contacts, and stickers. The ability of the three forensic tools to find digital evidence according to predetermined parameters is calculated using index number calculations (weightless index). The results of this calculation validate the performance of forensic tools. The forensic tool index number is calculated using Eq. (1).

$$P = \frac{\sum N_r}{(N_t)} x\ 100 \quad (1)$$

P is the accuracy index number (%), N_r is the number of found artifacts, and N_t is the total number of artifacts.

4. RESULT AND DISCUSSION

This research uses the DFRWS framework to organize the research steps in order to obtain digital evidence from the signal messenger application. Here is an analysis of the results of mobile forensics on the perpetrator's smartphone.

4.1 Preparing case scenario

In the first stage, case scenarios are prepared. Next, install the Signal Messenger application on the smartphone. After that, the chat activity starts with creating an account, then sending messages (text/images/video/audio/documents), as well as audio calls and video calls. The perpetrators implemented the spread of the COVID-19 hoax according to the scenario shown in Figure 3. The perpetrator's smartphone was in root condition before the case simulation.

The process of "rooting" enables users of Android-powered smartphones, tablets, and other devices to take more control (sometimes referred to as "root access") over some Android subsystems. A system account called "root" has the authority to access and run every command, every system, and every file in a Linux-based operating system. In addition, users with root access have the unrestricted ability to update, remove, add, or modify any files or data on the Android operating system.

4.2 Forensic analysis

4.2.1 Identification

Identifying evidence begins with securing the crime scene, which aims to prevent entry access for people who do not have a permit at the location. Next, search for evidence by looking at the entire crime scene and everything at the crime scene that has the potential to be evidence. Electronic evidence (the perpetrator's smartphone) was found based on the search results, as shown in Figure 5. Furthermore, the evidence found is identified in terms of type, brand, specifications, and other supporting information to serve as authentic evidence during the investigation process. The researcher also prepares materials and tools for the forensic process at this stage, as seen in Table 1.

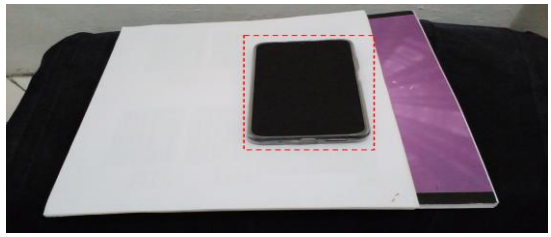


Figure 5. Evidence of the perpetrator's smartphone

4.2.2 Preservation

The preservation process is carried out to maintain and secure the authenticity of the physical evidence obtained at the identification stage so that data integrity is maintained until the analysis process is carried out. The preservation process is done by disabling the smartphone data channel (activating airplane mode). Activating airplane mode aims to isolate the device so it can not receive messages and calls from outside, or in other words, to prevent incoming and outgoing data. Digital evidence is volatile and has the risk of being lost or damaged, so isolation is important to prevent damage and maintain the authenticity of digital evidence. The activation of airplane mode on physical evidence (the perpetrator's smartphone) is shown in Figure 6.

Figure 6. Active airplane mode on the device

4.2.3 Collection

At the collection stage, the researcher collects data that is believed to be related to the crime committed. The collection process is done by acquiring and extracting data on the perpetrator's smartphone to search for and obtain digital evidence. The process of data acquisition and extraction of physical evidence (the perpetrator's smartphone) was carried out using Belkasoft Evidence Center, Magnet AXIOM, and MOBILedit Forensic tools.

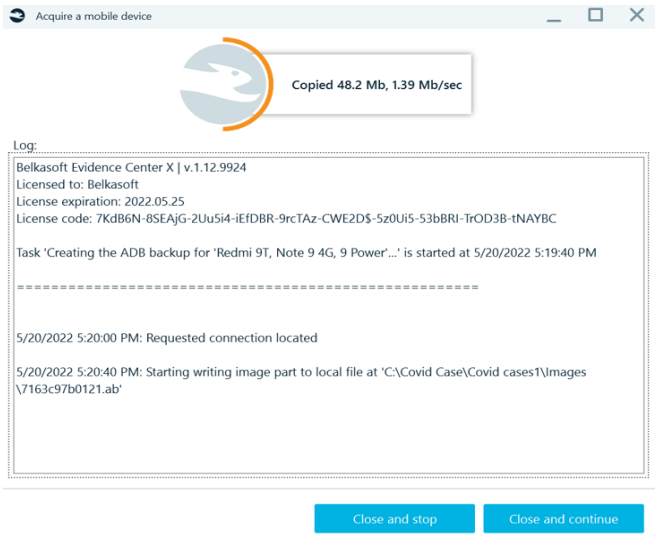


Figure 7. Acquisition process using Belkasoft

Figure 7 shows the acquisition process using Belkasoft Evidence Center. The acquisition method used is ADB backup. The time required for data acquisition is 12 minutes and 06 seconds.

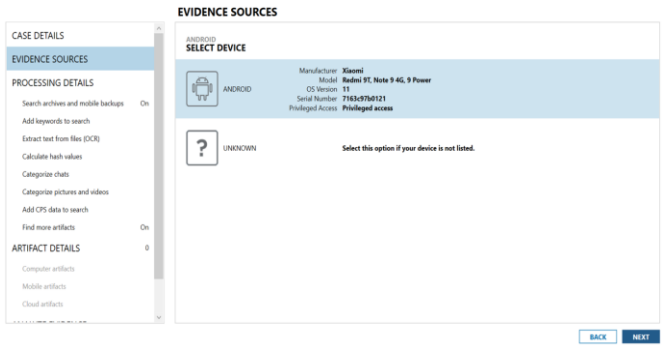


Figure 8. Acquisition process using Magnet AXIOM

The Magnet AXIOM acquisition process in Figure 8 uses the ADB (Unlocked) acquisition method for smartphones with root status. The acquisition process takes 5 minutes. Information obtained from the acquisition process: the smartphone is made by Xiaomi with the Redmi 9T model. It has an OS version of 11 with the serial number 7163c97b0121. Smartphones also have privileged access. Meanwhile, the acquisition process using MOBILedit Forensic is shown in Figure 9. With MOBILedit Forensic, get information about smartphones: The Xiaomi 9T smartphone model has an IMEI of 862965058072027, an IMSI of 510104662316464, and the smartphone status is rooted. The acquisition process takes approximately 6 minutes.

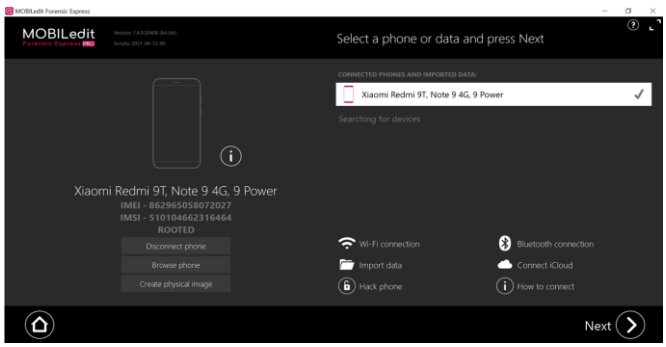


Figure 9. Acquisition process using MOBILedit Forensic

4.2.4 Examination

The results of the extraction that has been carried out will appear in the form of a full report in .pdf format. The display of the extracted data file is shown in Figure 10.

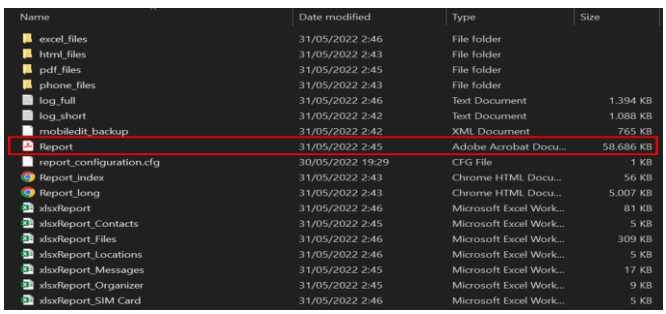
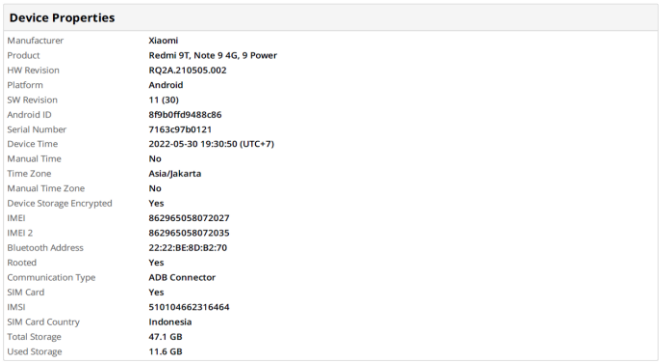


Figure 10. Extraction result using MOBILedit Forensic

The results of the Report.pdf report show that the smartphone used is the Xiaomi brand with detailed specifications. Meanwhile, Figure 11 provides other

information such as time zone, serial number, IMEI, IMSI, storage, and others.



Device Properties	
Manufacturer	Xiaomi
Product	Redmi 9T, Note 9 4G, 9 Power
HW Revision	RQ2A.210505.002
Platform	Android
SW Revision	11 (30)
Android ID	8f9b0ffd9488c86
Serial Number	7163c97b0121
Device Time	2022-05-30 19:30:50 (UTC+7)
Manual Time	No
Time Zone	Asia/Jakarta
Manual Time Zone	No
Device Storage Encrypted	Yes
IMEI	862965058072027
IMEI 2	862965058072035
Bluetooth Address	22:22:BE:8D:B2:70
Rooted	Yes
Communication Type	ADB Connector
SIM Card	Yes
IMSI	510104662316464
SIM Card Country	Indonesia
Total Storage	47.1 GB
Used Storage	11.6 GB

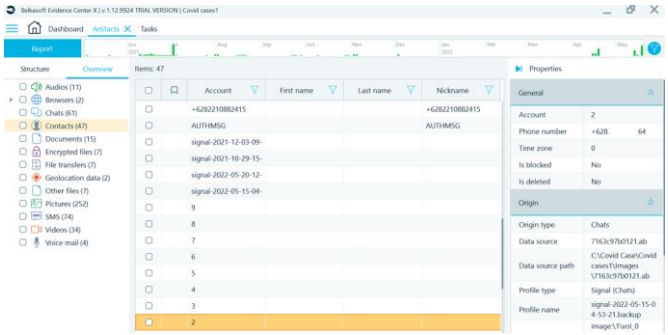
Figure 11. Pdf report about smartphone

4.2.5 Analysis

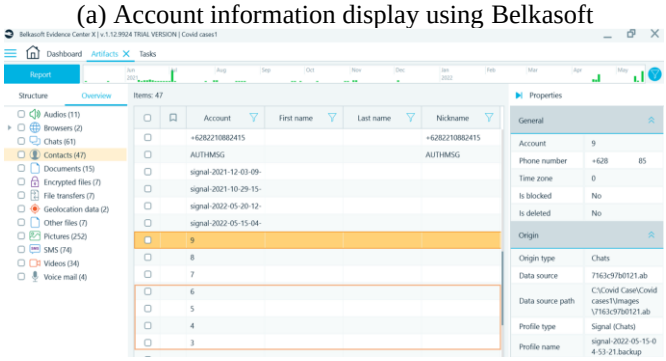
This analysis stage describes and discusses the results of the Signal Messenger application analysis using three different forensic tools.

1. Belkasoft Evidence Center

The analysis results of the Signal Messenger application using the Belkasoft tool get account information and contact. However, the information only shows the phone number, according to Figure 12.



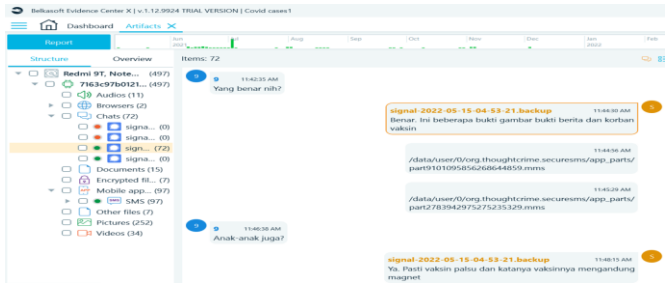
(a) Account information display using Belkasoft



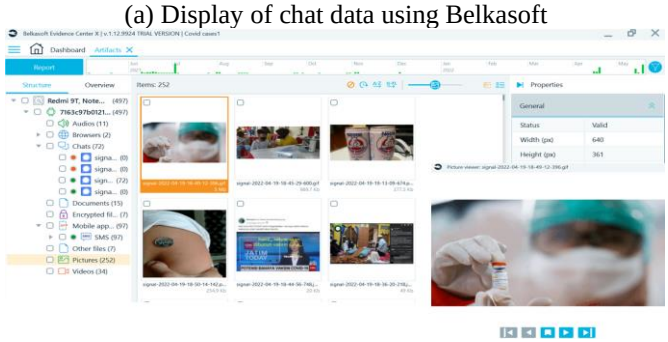
(b) Contact information display using Belkasoft

Figure 12. Display of account and contact information

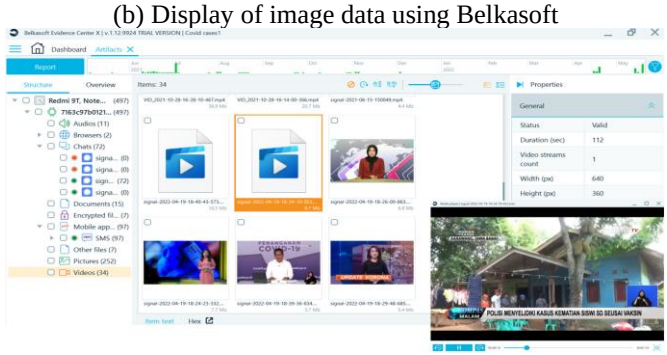
The Signal Messenger application has a backup feature. If this feature is enabled, this application will create a database backup with a key that the researcher can use to open the backup file. This backup file can be an alternative for researchers to view the data contained in Signal Messenger if the data from the Signal Messenger application database is not readable. Belkasoft's latest edition (trial version) has a feature that can open backup files. However, only some data can be found, such as chat data, images, videos, and stickers. Meanwhile, Belkasoft could not find any information regarding the data of documents, audio, voice calls, and video calls in the backup file.



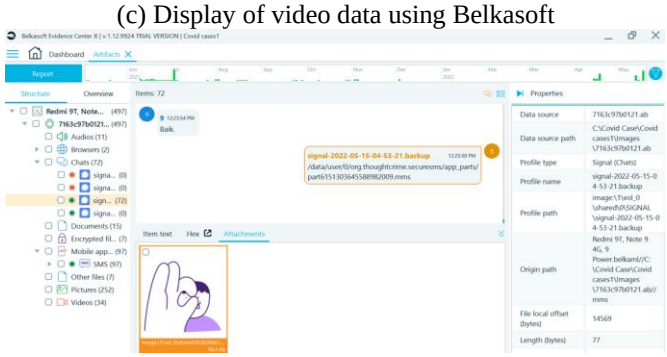
(a) Display of chat data using Belkasoft



(b) Display of image data using Belkasoft



(c) Display of video data using Belkasoft



(d) Display of sticker data using Belkasoft

Figure 13. Display of data obtained from backup file

Figure 13 (a) shows evidence of deleted chat data. Using Belkasoft, chat data can be displayed again, making it easier to find previously deleted evidence. The chat evidence found on the Signal Messenger application shows 29 messages from the perpetrators. In addition to finding chat data, the analysis results with this tool also found media in the form of images, videos, and stickers. The media evidence in the Signal Messenger application consists of six images, six videos, and one sticker, as shown in Figures 13 (b), 13 (c), and 13 (d). The image artifact provides information about the file name, width, height, and file size. The size of the image artifact is the same as the original image size and can be seen clearly and even zoomed in if needed. Similar to image artifacts, video artifacts

provide information about file name, duration, width, height, and file size. The video artifact size is different from the original video size but can be played clearly. Therefore, image and video artifacts can be used as evidence in court.

2. Magnet AXIOM

Similar to the Belkasoft tool, Magnet AXIOM can also open backup files. The result of the Signal application analysis that can be obtained is Signal Messenger account information. Figure 14 shows information about the account, including the username, package name, and last login.

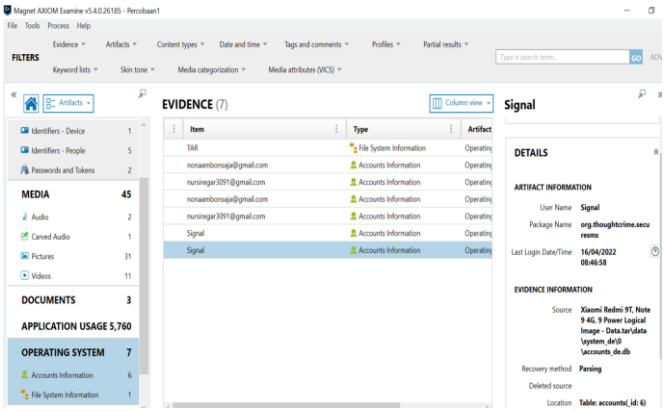
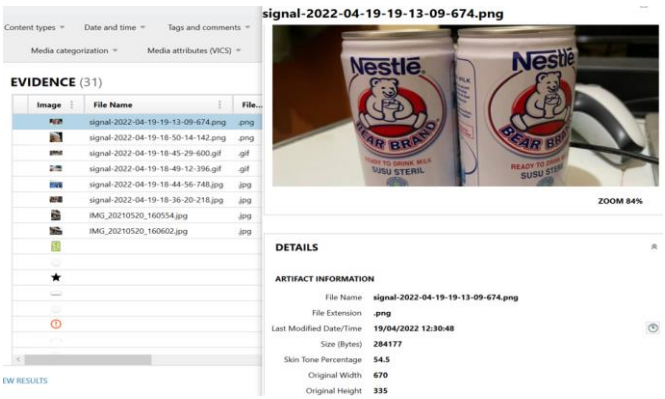
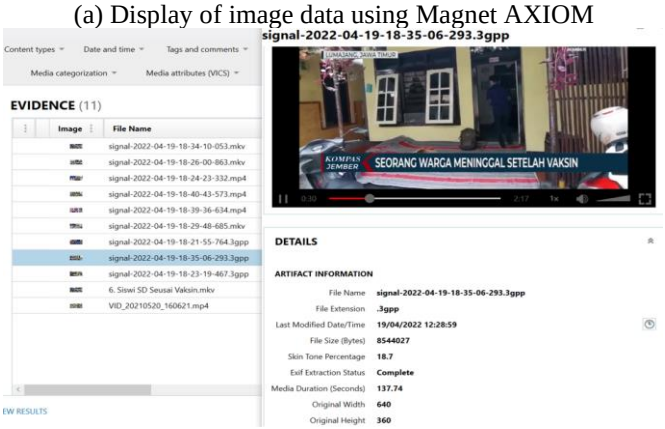


Figure 14. Account information display using AXIOM

In addition to account information, this tool gets evidence of deleted image and video data from the Signal Messenger application, as shown in Figure 15. Magnet AXIOM could only get six images and nine videos. In contrast, this tool can not find other data evidence.



(a) Display of image data using Magnet AXIOM



(b) Display of videos using Magnet AXIOM

Figure 15. Display of image and video data

Figure 15 shows information related to video artifacts such as file name, file extension, last modified date and time, file size, original width, and original height. Information about video artifacts is also the same as image artifact information; it only differs in a statement: media duration (for video artifacts). The image and video artifacts are the same size as the original image and video.

3. MOBILedit Forensic

Unlike the two tools above, MOBILedit Forensic can only find signal application information and contact information. The results of the Signal application analysis obtained from report.pdf are information that shows the package, the application version used is 5.34.10, and the application size is 49.8 Mb, as shown in Figure 16.

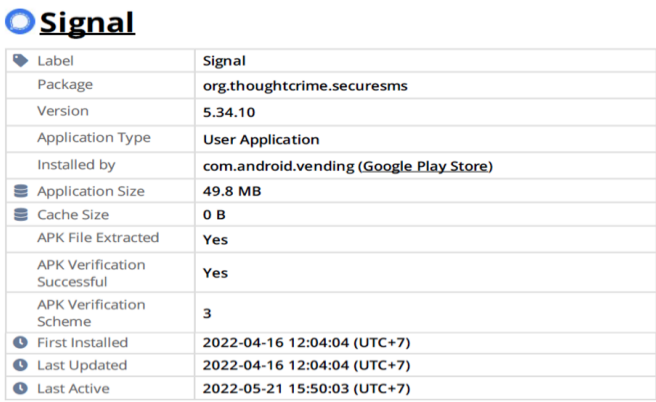


Figure 16. Application information using MOBILedit

The analysis results found five pieces of evidence of contact data, each of which contained a name, phone number, and modified time information, which can be seen in Figure 17.

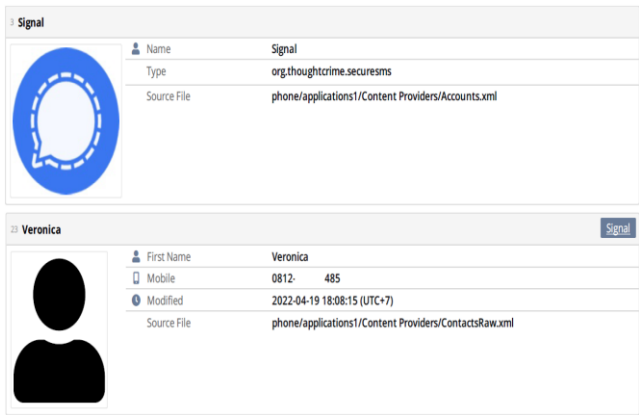


Figure 17. Contact information using MOBILedit

4.2.6 Presentation

Documentation about the results obtained from the acquisition process using Belkasoft, Magnet AXIOM, and MOBILedit Forensic tools is carried out at the presentation stage. Data obtained from smartphones with an installed signal messenger application becomes digital evidence for the crime simulation of spreading COVID-19 vaccine hoaxes. Digital evidence is obtained in various forms: chat data, images, videos, and sticker. The finding results of evidence on Belkasoft Evidence Center, Magnet AXIOM, and MOBILedit Forensic Express using predetermined parameters are shown in Table 2.

Table 2. Comparison of extraction results

Artifact Type (Parameters)	Amount of Data	Belkasoft Evidence Center	Magnet AXIOM	MOBILedit Forensic
Application Infomation	1	-	-	1
Account Information	1	1	1	-
Contact	5	5	-	5
Chat	29	29	-	-
Image	6	6	6	-
Audio	4	-	-	-
Video	10	6	9	-
Document	2	-	-	-
Voice Call History	1	-	-	-
Video Call History	1	-	-	-
Sticker	1	1	-	-
Total	61	48	16	6
Accuracy (%)		78,69	26,23	9,84

Based on Table 2, the results obtained are: Belkasoft was able to find six parameter variables, including account information (1), contacts (5), chats (29), images (6), videos (6), and stickers (1) with a total data of approximately 48. Magnet AXIOM found three parameter variables: account information (1), images (6), and videos (6), with a total data of approximately 16. Meanwhile, MOBILedit Forensic only found two parameter variables: application information (1) and contacts (5), with a total data of approximately 6.

Table 2 also shows there is an accuracy index calculation. The accuracy index measures each detection tool's ability for forensics. The calculation of the forensic tool accuracy index in Table 2 is calculated using Eq. (1) as follows:

Belkasoft Evidence Center: $P = \frac{48}{61} x\ 100 = 78{,}69\%$

Magnet AXIOM: $P = \frac{16}{61} x\ 100 = 26{,}23\%$

MOBILedit Forensic Express: $P = \frac{6}{61} x\ 100 = 9{,}84\%$

From the calculation above, only Belkasoft Evidence tool can find digital evidence with a better accuracy rate of 78.69%. The lack of the ability of both forensic tools to read deleted data and recover lost data proves that the Signal Messenger application is a social media application with the highest level of personal data security compared to other social media applications. Personal data security is an essential factor that must be owned by social media applications, mainly social media applications that are used simultaneously as instant messaging. The ease of obtaining data currently makes irresponsible parties steal someone's personal data to be used in various types of crimes.

5. CONCLUSIONS

Based on the results of mobile forensics on the Signal Messenger application by implementing the DFRWS framework and using different forensic tools, the researcher can conclude that Belkasoft and Magnet AXIOM can carry out forensic investigations on Signal Messenger quite well. Meanwhile, MOBILedit Forensic, although unable to read the Signal application database and file backups, can read additional information, namely signal application information and contact information. With this information, at least there is evidence that the Signal Messenger application with the last active time was installed on the perpetrator's smartphone. The victim's number is also stored in the Signal application, which means there is evidence of the possibility of the perpetrator spreading the COVID-19 vaccine hoax to the victim. The Belkasoft application obtained a higher accuracy of 78.69% with six parameter variables obtained from 11 variables; Magnet AXIOM obtained an accuracy of 26.23% with three parameter variables obtained from 11 variables, and MOBILedit Forensic Express got an accuracy of 9.84% with two parameter variables obtained from 11 variables. The artifact evidence obtained from this research can be used as evidence from the Signal Messenger application in court. In addition, it can be used as a reference for investigators in finding evidence of the widespread COVID-19 hoax, so the handling of the criminal case goes well.

From the results and conclusions presented, by conducting this experiment, we can find out which forensic tools support and are capable of finding digital evidence from the Signal Messenger application. In addition to knowing the capabilities of each forensic tool used. The benefit of this research is that if one day in real life (real world), we experience a crime when running a business or in an industry that uses Signal Messenger as a medium, then we know and can take the right action/attitude in overcoming the problem. Selection and use of appropriate forensic tools to find digital evidence from the Signal messenger application are very useful if you experience legal problems that require evidence to be presented in court. This research's limitation is the lack of forensic tool capabilities in conducting forensic analysis. Therefore, it is recommended for future research to use methods, frameworks, and other forensic tools with the latest versions to adapt to the latest versions of the signal messenger application, so further forensic researchers/experts get better and more complete results.

REFERENCES

[1] Okafor, S.O., Ugwu, C.I., Nkwede, J.O., Onah, S., Amadi, G., Udenze, C., Chuke, N. (2020). COVID-19 public health and social measures in Southeast Nigeria and its implication to public health management and sustainability. Oppor Chall Sustain, 1(1): 61-75. https://doi.org/10.56578/ocs010107

[2] Djalante, R., Lassa, J., Setiamarga, D., Sudjatma, A., Indrawan, M., Haryanto, B., Mahfud, C., Sinapoy, M. S., Djalante, S., Rafliana, I., Gunawan, L. A., Surtiari, G.A. K., Warsilah, H. (2020). Review and analysis of current responses to COVID-19 in Indonesia: Period of January to March 2020. Progress in Disaster Science, 6: 100091. https://doi.org/10.1016/j.pdisas.2020.100091

[3] Jaya, I. (2021). Strengthening the Health System in Controlling COVID-19. http://p2p.kemkes.go.id/penguatan-sistem-kesehatan-dalam-pengendalian-covid-19/, accessed on June 15, 2022.

[4] Mekahlia, F.Z., Bouzama, M.Z., Nechar, S. (2022). Impact of vaccination on COVID-19 spread in real time: visualization and analysis tool. Ingénierie des Systèmes d'Information, 27(2): 293-301.

https://doi.org/10.18280/isi.270213
[5] Chakraoui, M., Mouhni, N., Elkalay, A., Nemiche, M. (2022). Deep negative effects of misleading information about COVID-19 on populations through Twitter. Ingénierie des Systèmes d'Information, 27(2): 185-192. https://doi.org/10.18280/isi.270202
[6] WHO. (2020). Coronavirus disease 2019 (COVID-19) situation report-91, World Health Organization, Indonesia.
[7] Umar, R., Riadi, I., Zamroni, G. M. (2018). Mobile forensic tools evaluation for digital crime investigation. International Journal on Advanced Science Engineering Information Technology, 8(3): 949-955. https://doi.org/10.18517/ijaseit.8.3.3591
[8] Eriş, F.G., Akbal, E. (2021). Forensic analysis of popular social media applications on android smartphones. Balkan Journal of Electrical and Computer Engineering, 9(4): 386-397. https://doi.org/10.17694/bajece.761271
[9] Riadi, I., Umar, R., Firdonsyah, A. (2017). Identification of digital evidence on android's blackberry messenger using NIST mobile forensic method. International Journal of Computer Science and Information Security, 15(5): 155-160.
[10] Sheikhi, S. (2020). An efficient method for detection of fake accounts on the Instagram platform. Revue d'Intelligence Artificielle, 34(4): 429-436. https://doi.org/10.18280/ria.340407
[11] Kemp, S. (2022). Digital 2022: Indonesia. https://datareportal.com/reports/digital-2022-indonesia
[12] Statista. (2022). Global Digital Population as of April 2022. https://www.statista.com/statistics/617136/digital-population-worldwide/, accessed on June 18, 2022.
[13] Yas, H., Jusoh, A., Streimikiene, D., Mardani, A., Nor, K.M., Alatawi, A., Umarlebbe, J.H. (2021). The negative role of social media during the COVID-19 outbreak. International Journal of Sustainable Development and Planning,16(2): 219-228. https://doi.org/10.18280/ijsdp.160202
[14] Candiwan, C., Azmi, M., Alamsyah, A. (2022). Analysis of behavioral and information security awareness among users of zoom application in COVID-19 era. International Journal of Safety and Security Engineering, 12(2): 229-237. https://doi.org/10.18280/ijsse.120212
[15] Li, X.G. (2018). Crucial elements in law enforcement against cybercrime. International Journal of Information Security Science, 7(3): 140-158.
[16] Nadzir, I., Seftiani, S., Permana, Y.S. (2019). Hoax and misinformation in Indonesia: insights from a nationwide survey. Researchers at Iseas, 2019(92): 1-12.
[17] Islam, M.D., Sarkar, T., Khan, S.H., Kamal, A.H.M., Hasan, S.M.M., Kabir, A., Yeasmin, D., Islam, M.A., Chowdhury, K.I.A., Anwar, K.S., Chughtai, A.A., Seale, H. (2020). Covid-19-related infodemic and its impact on public health: a global social media analysis. Am J. Trop Med Hyg, 103(4): 1621-1629. https://doi.org/10.4269/ajtmh.20-0812
[18] Sirait, F.E.T., Sanjaya, R. (2021). Case study in Covid-19 infodemic in Indonesia. Nyimak Journal of Communication, 5(1): 1-14. http://dx.doi.org/10.31000/nyimak.v5i1.2652
[19] Ravelo, J.L. (2021). A Hoax Killed My Father: Uncovering another pandemic in Indonesia. https://www.unicef.org/indonesia/id/coronavirus/cerita/hoaks-membunuh-ayahku-menyingkap-pandemi-lain-di-indonesia?gclid=Cj0KCQjwidSWBhDdARIsAIoTVb3F3m07VbjDWKOodHe7KeQ62RPcz8QE31Fhu0XY5s5YCjIX8jLT1IcaArN6EALw_wcB, accessed on June 17, 2022.
[20] Rosemary, R., Rochimah, T.H.N., Susilawati, N. (2022). Efficacy information in government's initial responses to covid-19 pandemic: A content analysis of the media coverage in Indonesia. International Journal of Disaster Risk Reduction, 77: 1-7. https://doi.org/10.1016/j.ijdrr.2022.103076
[21] Rösler, P., Mainka, C., Schwenk, J. (2018). More is less: on the end-to-end security of group chats in signal, whatsapp, and threema. 2018 IEEE European Symposium on Security and Privacy (EuroS&P), 2018: 415-429. https://doi.org/10.1109/EuroSP.2018.00036
[22] Shu, C. (2021). Signal, the encrypted messaging app, is currently down for many users (update: it's back). https://techcrunch.com/2021/09/26/signal-the-encrypted-messaging-app-is-currently-down-for-many-users/.
[23] Almehmadi, T., Batarfi, O. (2019). Impact of android phone rooting on user data integrity in mobile forensics. 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019: 1-6. https://doi.org/10.1109/CAIS.2019.8769520.
[24] Menahil, A., Iqbal, W., Iftikhar, M., Shahid, W. B., Mansoor, K., Rubab, S. (2021). Forensic analysis of social networking applications on an android smartphone. Wireless Communications and Mobile Computing, 2021(4): 1-36. https://doi.org/10.1155/2021/5567592
[25] Ichsan, A.N., Riadi, I. (2021). Mobile forensic on android-based IMO messenger services using digital forensic research workshop (DFRWS) method. Scientific International Journal of Computer Applications, 174(18): 34-40. https://doi.org/10.5120/ijca2021921076
[26] Pambanyun, S., Riadi, I. (2020). Investigation on instagram android-based using digital forensics research workshop framework. International Journal of Computer Applications, 175(35): 15-21. https://doi.org/10.5120/ijca2020920904
[27] Son, J., Kim, Y.W., Oh, D.B., Kim, K. (2022). Forensic analysis of insta nt messengers: decrypt signal, wickr, and threema. Forensic Science International: Digital Investigation, 40: 1-12. https://doi.org/10.1016/j.fsidi.2022.301347.
[28] Afzal, A., Hussain, M., Saleem, S., Shahzad, M.K., Ho, A.T.S., Jung, K.H. (2021). Encrypted network traffic analysis of secure instant messaging application: A case study of signal messenger app. Applied Sciences, 11(17): 1-24. https://doi.org/10.3390/app11177789
[29] Kunle, A., Titilope, A.F. (2022). Technological advancement and risk management in composite insurance companies in Nigeria. J. Corp. Risk Manag., 9(S1): 112-125. https://doi.org/10.51410/jcgirm.9.1.7
[30] Judge, S.M. (2017). Mobile forensics: Analysis of the messaging application signal. Master Thesis, Master of Science in Forensic Science, University of Central Oklahoma, Edmond, Oklahoma, USA Pawlaszczyk, D. (2022). Mobile forensics – the end of a golden age?. Journal of Forensic Sciences and Criminal Investigation, 15(4): 555917. https://doi.org/10.19080/JFSCI.2022.15.555917.

[31] Barmpatsalou, K., Cruz, T.J., Monteiro, E., Simoes, P. (2018). Current and future trends in mobile device forensics: A survey. ACM Computing Surveys, 51(3): 1-31. https://doi.org/10.1145/3177847

[32] Gde, A.A., Rahaditya, J., Sasmita, A., Made, G., Pratama, E., Agus, I.P. (2016). Prototyping SMS forensic tool application based on digital forensic research workshop 2001 (DFRWS) investigation model: Case study: SMS togel in indonesia. 2016 International Conference on Information Technology Systems and Innovation (ICITSI), PP.1-6. https://doi.org/10.1109/ICITSI.2016.7858226

[33] Tanner, A., Dampier, D. (2009). Concept mapping for digital forensic investigations. IFIP Advances in Information and Communication Technology, 306: 291-300. https://doi.org/10.1007/978-3-642-04155-6_22

[34] Riadi, I., Yudhana, A., Putra, M.C.F. (2018). Forensic tool comparison on instagram digital evidence based on android with the NIST method. Scientific Journal of Informatics, 5(2): 235-247. https://doi.org/10.15294/sji.v5i2.16545

[35] Azhar, H., Cox, R, Chamberlain, A. (2020). Forensic investigations of popular ephemeral messaging applications on android and iOS platforms. International Journal on Advances in Security, 13(1&2): 41-53. http://www.iariajournals.org/security/sec_v13_n12_2020_paged.pdf.

[36] Riadi, I., Herman, Siregar, N.H. (2022). Mobile forensic of vaccine hoaxes on signal messenger using DFRWS framework. Matrik, 21(3): 489-502. https://doi.org/10.3081/matrik.v21i3.1620

[37] Belkasoft. Belkasoft Evidence Center X. https://belkasoft.com/x, accessed on June 12, 2022.

[38] Magnet Forensics. Magnet AXIOM Recover & Analyze Your Evidence in One Case. https://www.magnetforensics.com/products/magnet-axiom/, accessed on June 12, 2022.

[39] Shukla, U., Mandal, B., Kiran, K.V.D. (2018). Perlustration on mobile forensics tools. In: Smys, S., Palanisamy, R., Rocha, Á., Beligiannis, G.N. (eds) Computer Networks and Inventive Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies, 58: 1225-1231. Springer, Singapore. https://doi.org/10.1007/978-981-15-9647-6_97