ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 7, No. 2, 127-132 (2022)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Forensic Analysis of "WhatsApp" Artifacts in Android without Root

Mohammad Shadeed *, Layth Abu Arram, Majdi Owda

Department of Natural, Engineering and Technology Sciences, Arab American University Palestine, Ramallah, Palestine

ARTICLE INFO

Article history:
Received: 14 October, 2021
Accepted: 26 November, 2021
Online: 12 April, 2022

Keywords:
WhatsApp Forensics
Smart Phones Forensics
Databases Forensics
Mobile Forensics
Android Forensics

ABSTRACT

WhatsApp application is considered the largest messaging application around the world and an important source of information, they just incorporated a new technique that operates on end-to-end encryption, which presents a significant problem for forensic investigators and analysts. This study describes how to recover the encryption key from WhatsApp to decrypt WhatsApp databases and retrieve important artifacts displayed and saved in the Android system without rooting the device. As a means of presenting and analyzing artifacts taken from the most recent version of WhatsApp to signs of fresh and important evidence and artifacts to assist investigators and forensic analysts in the investigation. As a result, various techniques, devices, and software may now be utilized for WhatsApp digital forensics. The findings of this study showed a variety of artifacts in the internal memory unit utilized by the Android system for the WhatsApp application, which might aid digital forensic examiners in their examination of WhatsApp on the Android system without the need to root the device.

1. Introduction

With over one billion users, the WhatsApp instant messaging program is one of the most popular in the world. The application was founded in 2009, and Facebook bought it in February 2014 for $ 19 billion. In exchange, Google's Android operating system is one of the most successful and well-known in smartphones throughout the world, with a market share of almost 80%, and because of the widespread use of Android devices and the services they provide, such as instant messaging, particularly the WhatsApp application, where users send and receive instant messages in their everyday lives and other activities [1], [2]. The world has well and truly entered the field of technology and its digital age, where this technology that has covered all stages and endings and forms of life is constantly presented and our main purpose is the positive use of this technology, contrary technology has facilitated our daily lives, but it has also given contributions and solutions to resist terrorist activities and electronic crimes. Specifically, this occurs as a result of technological advancements all around the world [3], [4]. According to information security experts, many crimes are committed over the Internet. Criminals may commit their crimes using a variety of channels, including the Internet, mobile devices, and instant messaging apps such as WhatsApp. With the rapid expansion of cybercrime, it has become important and urgent to begin conducting studies and research specialized in evaluating the WhatsApp program since it is regarded as the most popular application in the world that is easily utilized [5], [6].

The WhatsApp program for instant messaging is one of the most significant and popular applications in the world, with over a billion users worldwide. Because of this development and the massive amount of information and data that is sent instantly around the world, forensic investigators and researchers have a profound and major challenge, in addition to the artifacts left inside the phone devices, which play an important role in any suspense.

This paper will provide a search for digital evidence and artifacts for the WhatsApp application, to assist digital investigation professionals and analysts in gaining access to clear scientifically proved digital evidence. Furthermore, this article will concentrate the research on artifacts from internal memory by extracting artifacts as digital evidence installed for the WhatsApp program that runs on the Android operating system. Overall, this will provide a new dimension to the digital forensic examination of the WhatsApp program.

2. Literature review

2.1. Background

This section will provide a specific and comprehensive definition of digital forensics as well as a definition of smartphones forensics. In addition, a brief description of the forensic techniques and smartphone devices data acquisition techniques used by digital forensic investigators will be provided.

2.2. Digital forensics

Digital forensics can be defined as an applied and practical use of reliable and proven methods for digital devices, and this action has been done in several ways, the most important of which are verification, identification, analysis and interpretation, and then the digital evidence that has been and derived from digital data is presented. It is the reconstruction of the events that

* Corresponding Author: Mohammad Shadeed, Email: shadeedmohammad@gmail.com

show the crime, or that helps in the anticipation of the unauthorized procedures[7]-[10]

2.3. Mobile forensics

Mobile forensics is defined as the science of digital evidence likely to be obtained from portable devices using techniques similar to digital forensic investigations. Mobile device models vary, depending on where the storage is located, so that it can be stored on the internal or external memory card, and the phone memory may be volatile or non-volatile[11]-[13].

2.4. Mobile Device Data Acquisition Techniques

Obtaining digital forensics data from mobile devices must include the use of the two main technologies, mainly logical acquisition and physical acquisition, and each of these features has its advantages [14], taking a logical copy of the device may not need to root the device and it can give us the virtual files of the stored data on the memory, while the physical version (bit by bit) needs to root the device and enables us to root the device and may cause problems on mobile devices [15]-[17].

2.5. WhatsApp forensics

Many different tools support acquisition data in the WhatsApp application, and the main goal of using these tools is to access the data stored in the protected logic of the mobile device to obtain WhatsApp data. The way these tools work depends on two methods, namely rooting the Android device and going back to the previous version of the WhatsApp application, and the use of these two methods is completely related to obtaining the data from the WhatsApp application and understanding the method on which the structure of the WhatsApp application depends. This section will discuss the WhatsApp application, and then the main mechanisms used to obtain data and items from the WhatsApp application will be clarified [18]. The WhatsApp application is an application that works on instant messaging and is free of charge, as it allows users to receive and send messages, whether text, images, audio or video clips and many other files in a very easy way, as this application is available for all operating systems around the world such as (Windows, Android, iOS). Often thinking about how messages are transmitted from phones through the receiving servers, without thinking about what is the invisible mechanism that may take place in the phones, in fact when the sender presses the send button and directly sent the message and it is being stored inside a file and this file is being Stored inside both devices the sender and the receiver, The Figure (No.1) WhatsApp transmission. Shows Explain the process of sending and encrypting the sent message and transferring it to the WhatsApp server and then sending it to the receiver, decoding it and displaying it to the user [19]-[21].

Usually, forensic investigators are interested in locating the places where messages are stored, so they can obtain them and then run them according to WhatsApp policy, so all sent and received messages are stored in the servers of the WhatsApp application temporarily. WhatsApp servers contain a large number of evidence usually stored in servers for a very short period. In addition, investigators need to refer to the owner company directly and adhere to the company's privacy policy to retrieve any evidence in their servers, and that is a very difficult procedure. Here comes the importance of investigating the sender and receiver's devices because the sent and received messages are kept in mobile devices, so that WhatsApp users stores many artifacts of high value as proof for the investigation, as the files that are saved are the message log and the database For all conversations and correspondences (sent and received), The Figure (Figure 2) WhatsApp databases structure. shows the database structures stored in the internal memory of the mobile device hierarchically. As shown in that figure, on three levels, the first level contains the main WhatsApp data hall. The second level contains the sub-databases, and the third level, located at the bottom level of the hierarchy, shows the other sub-files [18].

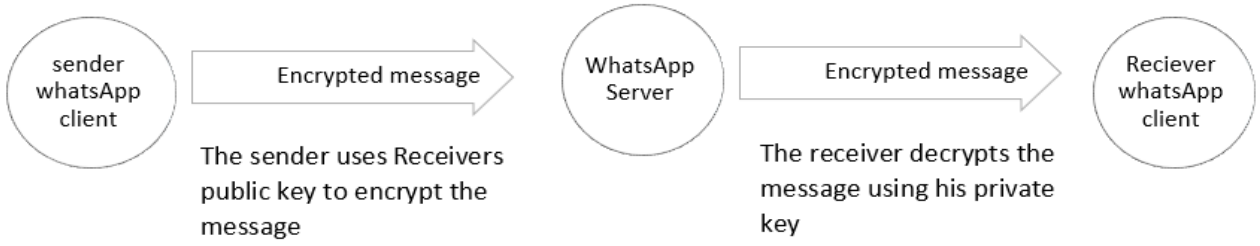

Figure 1: WhatsApp transmission

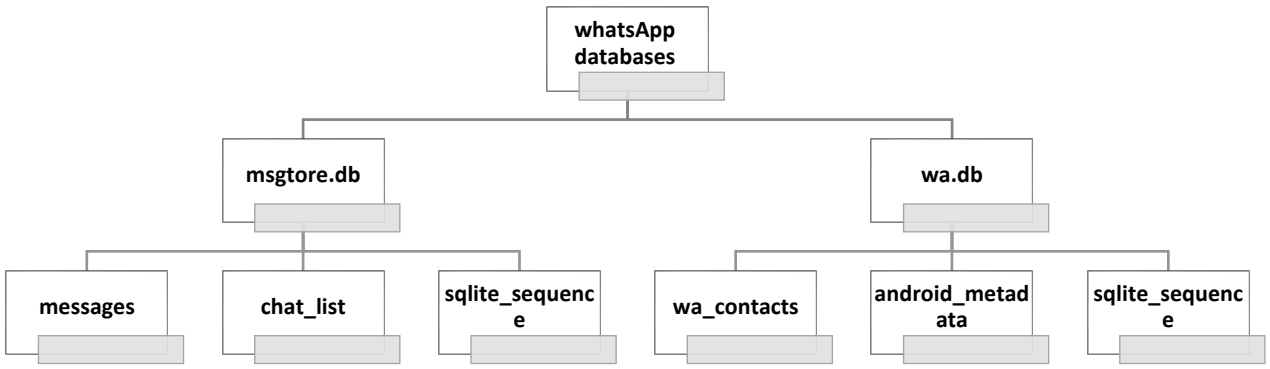

Figure 2: WhatsApp databases structure

3. Related works

There are some studies and researches that indicated this topic as a part of their efforts were unable to access or obtain sufficient antiquities as definitive digital evidence, Others have reached a portion of the artifacts. The following are some of the previous studies that were found and relevant to this research.

indicates that the data stored in the memory includes lines with characters that cannot be read by humans because it contains binary data for the full object storage array of the origin inside the database. However, the records that are observed are valuable for forensic investigation, the indexed database for WhatsApp contains with it a set of important elements that can be used as evidence of a crime after it has been presented and analyzed in the style of the time frame, and the database in WhatsApp is a valuable source of information that is used for forensic investigations and therefore the database is very important to know and see what is inside and analyze it to reach important results that may be based on the case [22]. indicate that the evidence was obtained through backup without rooting the device, and it was stored in another storage unit, and the analysis was started by open-source forensic tools, and the results showed that part of the conversations was encrypted and there were challenges in showing the results. It is not encrypted and the deleted conversations did not appear in the results, and the results indicate that to recover the deleted conversation, the device must be rooted [23]. indicates that a backup copy of Android was obtained and saved on an external memory card and analyzed on the open-source forensic analysis tools and that the database of correspondence and conversations was obtained, and even if the results obtained from Android are encrypted, the elements are evidence of correspondence, and here this study indicates that the device has not been rooted [24]. mentioned that the data of the WhatsApp conversations can be depicted in the form of a table in the memory and the chronology of the application is placed. Identification of it, and it is also possible to refer to all relevant data and what is the period for it, and this is considered as evidence or proof of my investigation for the case. Also, this method added the nature of exploration and understanding of the data in determining the time of the crime [25]. clarified that digital evidence can provide any information that has great

inferential value and showed how to interpret these data that were stored in contacts and databases of conversations and chat, and the study showed the correlation between this evidence and its connection with others to collect sufficient information that can be deduced during the examination and relates it to the event itself. Once collected, it allows the investigator to determine which messages have been deleted and remain in the log wallet in the database and log files [26]. Another research study was able to get the main supporting data from the database that contains the contacts, artifacts, and conversations that make up the WhatsApp application, and the data is in the form of a backup database and it contains relevant driver files such as images, chats, audio and video, and was able to analyze it using the applications and special tools that support to achieve the goal of the study, and that was using free tools used in digital forensics, namely (FTK) and (SQLite) browser [27]. conducted a forensic analysis process in the WhatsApp application and obtained evidence from the Android operating system on mobile devices, and the data was extracted using Python software [28]. shows the decryption of the encrypted WhatsApp database that is used in Android devices without rooting the device, and the required results were extracted, but this method does not extract the deleted messages, but after rooting the device and using the same method, the deleted messages can be retrieved [29]. carried out a forensic analysis in WhatsApp application, where the chat and stored conversations were extracted through the internal and external memory using WhatsApp key extractor, where the decryption process was carried out and the backup database was converted into a text database so that it can be seen in the SQLite database. was based on researching the behavior of tools that use forensic evaluation in the form of extracting artifacts in the form of messages, images, or videos from Android devices. The tools (ADB WhatsApp Key / DB Extractor 4.7 and Belkasoft) were used, and all of these tools were free versions, Where the tools were tested, the WhatsApp database was extracted and decrypted, and the process of updating it using end-to-end encryption (crypt12) These results will be compared with the results obtained in this study [30].

4. Research Problem

With the ever-increasing popularity of smartphones and people's reliance on instant messages in their everyday lives, quick updates of instant messages increase the features of the application and entice users to continue using their product. On the other hand, the majority of these characteristics will provide a significant challenge to digital forensic practitioners and specialists. Many studies have been done to acquire data from older versions of the WhatsApp program. Many security measures arose with the introduction of new versions of WhatsApp, making it difficult for mobile forensic practitioners to gather information and evidence that live in internal storage. This study proposed new techniques for obtaining data from the WhatsApp application on the Android system without rooting on the latest WhatsApp application in which encrypted datasets used the new approach i.e. using crypt12 architecture.

5. Research Objectives

In this study, we will collect and analyze artifacts from the most recent release of the WhatsApp program operating on an Android machine. This study uses a variety of approaches and instruments to achieve the following goals:

- The extraction of logical WhatsApp's encrypted database, which is operating on an Android smartphone.
- Analyze and correlate the artifacts generated by the database to generate additional useful evidential trails that aid in the investigation without the usage of rooting the device.

6. Research Question

What approaches, methodologies and tools can be used in android forensics to recover artifacts from the WhatsApp Instant Message program operating on an android smartphone without rooting?

7. Methodology

The main purpose of this study is to search and find new techniques, tools, and methods to recover the artifacts of recent versions of the WhatsApp application that works in the Android operating system environment, and to extract the artifacts located in WhatsApp from the internal memory of the device. Various devices, tools, equipment, software are free and open-source and focused mainly on restoring all the artifacts that can be obtained from the latest versions of the WhatsApp application installed in the Android operating environment.

As the digital artifacts finding tools were taken through the process of logical exploration of the Android operating system. figure (NO.3) shows the approach through which the data was acquired, as it checks whether the device is rooted or not, and if it is rooted, a physical copy is taken, but if it is not rooted, a logical copy is acquired and the last stage is access to the database. And shows how the artifacts were acquired and analyzed, which were created using the WhatsApp application on smart mobile phones, in both physical and logical ways [31].

8. Requirements and Experimental Setup and Analysis

The process of forensic investigation of mobile devices is not very different from that of laptops, but some of the tools that are used in mobile forensics are somewhat different, as most mobile operating systems are closed, so it becomes difficult to understand the file system and the structure of phones. There are many open-source Android operating systems and there are some tools that are used in digital forensic for Android operating systems, which are available for users and are paid and unpaid tools, before starting the process of data extraction, backup operations, etc.

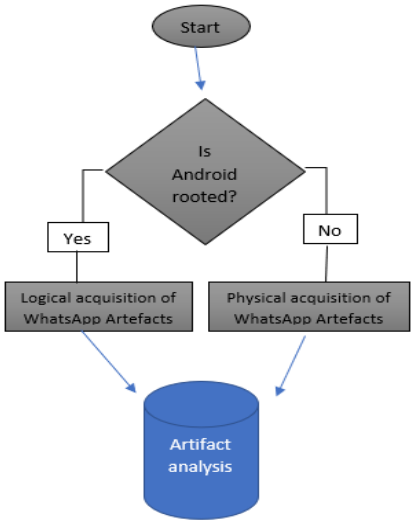

Figure 3: Methodology Design of Acquiring and Analysis of WhatsApp Artefacts

8.1. Requirements and Research tools & Devices

Table No. (I) will show the tools, software, and devices that were used in this research.

Table 1: Research tools & Devices

No.	Tools & devices	Info.
1	Redmi Note 8 (4GB RAM, 64GB) OS Android 11	Smartphone mobile
2	USB Cable	USB connector to connect phone device and computer
3	Belkasoft Evidence	Analysis tool
4	WhatsApp ver. 2.21.12.21	Messaging application
5	SQLite Studio	Analysis tool
6	SQLite Database Recovery v1.2	Tool for Database Recovery
7	Andriller	Analysis tool
9	Root Explorer 3.8	Analysis tool
10	Autopsy 4.4	Analysis tool
11	FINALMobile Forensics4	Analysis tool
12	WhatsApp viewer	Db viewer
13	DB Extractor	Database extractor
14	Dback	Backup viewer

8.2. Logical copy acquisition and analysis

Usually, information is stored in Android phones in different formats and ways, as a kind of security and confidentiality, so we will be careful not to change anything unnecessary on the device, it requires obtaining a logical copy by connecting the phone to the computer via a USB cable directly, from Through several tools and applications, the most important of which is to install the following tools to avoid rooting the mobile device (android-ADB, ADB fastboot, java JDK, python), and then the researcher will do an in-depth analysis of the version to obtain the (WhatsApp Artifacts) files.

This research is concerned with searching for WhatsApp artifacts in the permanent storage memory without expanding to the volatile random memory since in this research experiments were conducted on a (Xiaomi) mobile device. Application stores the data of the user (the target of this study) in a database (SQLite) called the database (msgstore.db).

After making the backup, we will find the following files

/ sdcard/WhatsApp/Databases

/ sdcard/WhatsApp/media

/ sdcard/WhatsApp/Backups

After we were able to get WhatsApp database files from the Android backup without rooting the device as shown in Figure (4), in this section of the study we will start the decryption procedures (msgtore.db) so that we can get the artifacts .

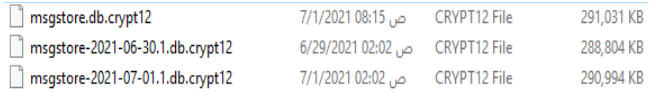

Figure 3: Whatsapp database

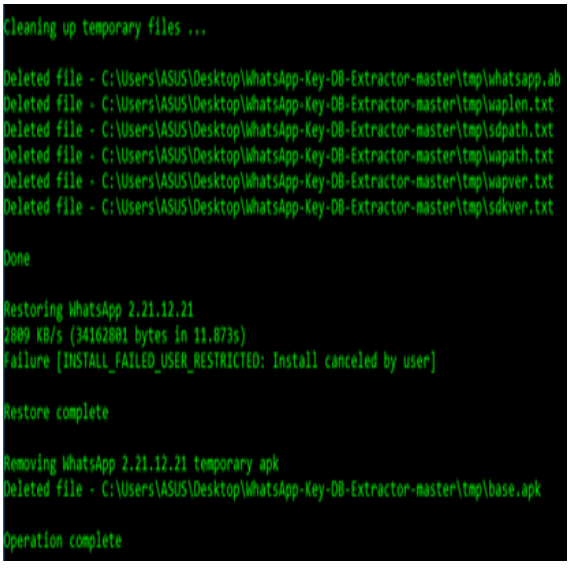

Figure 4:Extracting database

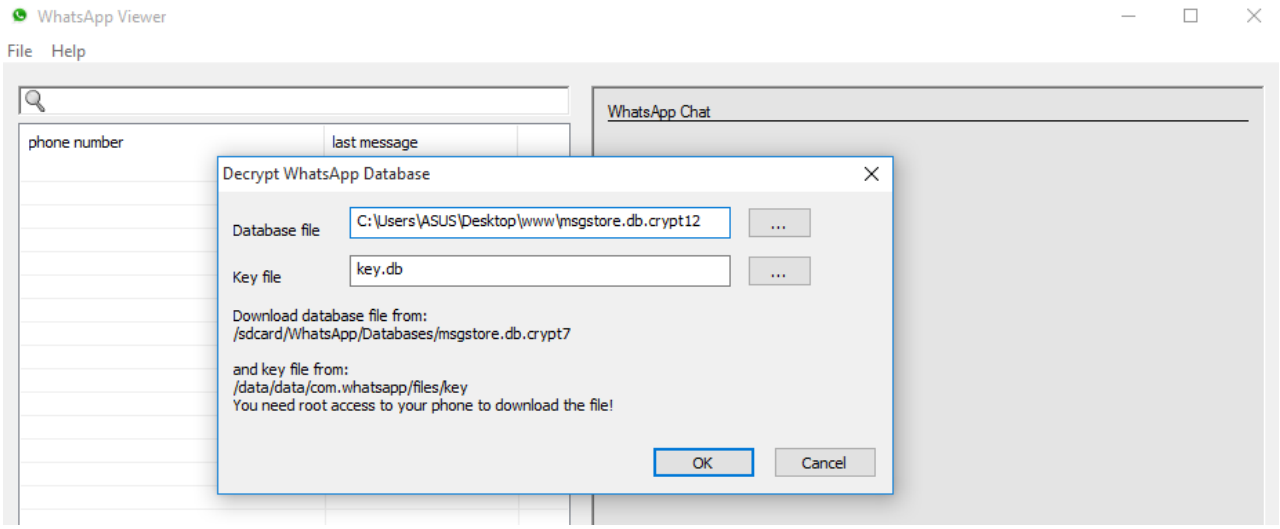

Figure 5 : To decrypt WhatsApp databases

Figure (5) shows extracting and retrieving a database opener (msgstore.db) using the specialized tool (DB Extractor) to decrypt and display WhatsApp databases. And after we were able to get the key of the database (msgstore.db) we need to decrypt the database with the same key through the (WhatsApp viewer) tool as shown in Figure (6), we will open it in order to be able to view its contents through the same tool as shown in Figure (7).

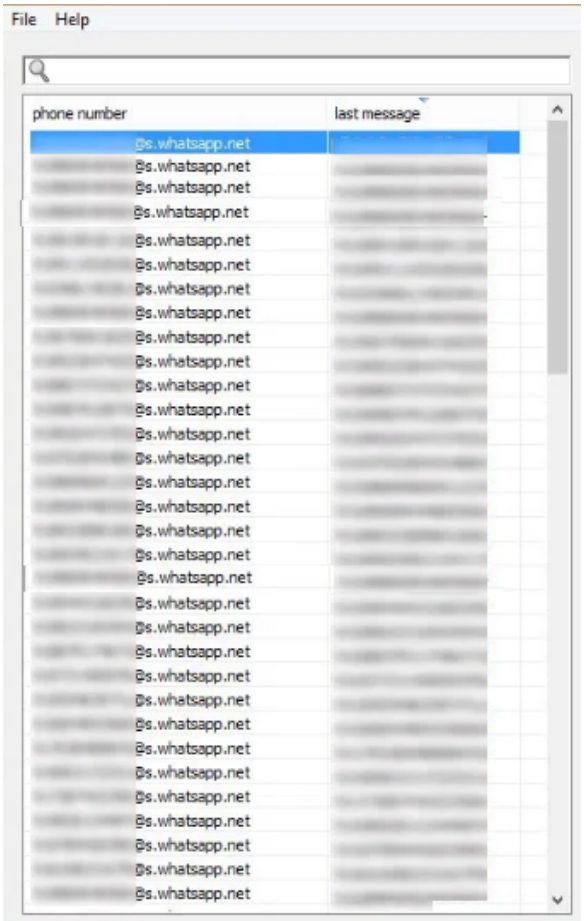

Figure 6: Open WhatsApp Database

9. Conclusion and Future Work

In this research we focused on obtaining artifacts from the device's fixed memory for the WhatsApp application, which has become well known to more than a billion users through which an individual can communicate in all formal and informal matters by sending texts, images, documents, videos, and others. This research shows that a person can access to all the materials in WhatsApp and use other social networking applications such as Skype, Viber and Telegram that work in the operating environments of mobile devices.

All the results of this research are important and valuable results for digital forensics that can be extracted directly from smartphones that works on Android system.

As it also has been mentioned previous research's, the password will not be a black box for the device, so for a specialist to crack or overstep the password to get all the valuable user information in addition to that, files can be obtained from volatile memory (RAM) [32], [33].

Although message ,text ,user phone number and time/date of transmission are considered an important and great service provided by this study for digital forensics, but there are other matters are no less important than this, such as the deleted messages and the geographical location at the time of sending the message.

For future works. researchers will do additional researches to retrieve the deleted data in addition to the random access memory data that humans can read. There are still some experiments that can be analyzed through the volatile memory (RAM) of the device in order to obtain more artifacts that considered useful for digital forensics.

References

[1] A.A. Ahmed, A.. Al-Qadhi, M.. Janardhana, "Geotechnical Characterization of The Volcaniclastic Rocks in and around Taiz City, Yemen," Global Journal of Advanced Engineering Technologies and Sciences, **3**(4), 14–31, 2016.

[2] E. Casey, M. Bann, J. Doyle, "Introduction to Windows Mobile Forensics," Digital Investigation, **6**(3–4), 136–146, 2010, doi:10.1016/j.diin.2010.01.004.

[3] R. Broadhurst, Y.-C. Chang, "Cybercrime in Asia: Trends and Challenges," SSRN Electronic Journal, 1–26, 2012, doi:10.2139/ssrn.2118322.

[4] J. Liu, M. Travers, L.Y.C. Chang, "Comparative Criminology in Asia," Comparative Criminology in Asia, (October), 2–3, 2017, doi:10.1007/978-3-319-54942-2.

[5] R. Sarre, L.Y.C. Lau, L.Y.C. Chang, "Responding to cybercrime: current trends," Police Practice and Research, **19**(6), 515–518, 2018, doi:10.1080/15614263.2018.1507888.

[6] H. Osborn Quarshie, A. Martin- Odoom, "Fighting Cybercrime in Africa,"

Computer Science and Engineering, **2**(6), 98–100, 2012, doi:10.5923/j.computer.20120206.03.
[7] N.V. Vukadinovic, WhatsApp Forensics: Locating Artifacts in Web and Desktop Clients, Master's Thesis, Purdue University Graduate School, 2019.
[8] N. Beebe, "Digital forensic research: The good, the bad and the unaddressed," IFIP Advances in Information and Communication Technology, **306**, 17–36, 2009, doi:10.1007/978-3-642-04155-6_2.
[9] TraceGen: User Activity Emulation for Digital Forensic Test Image Generation, Jan. 2022.
[10] S. Omeleze, H.S. Venter, "Testing the harmonised digital forensic investigation process model-using an Android mobile phone," 2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference, 2013, doi:10.1109/ISSA.2013.6641063.
[11] R. Singh, An Overview of Android Operating System and Its Security Features, Engineering Research and Applications, **4**(2), 519–521, 2014.
[12] A. Al-Dhaqm, S.A. Razak, R.A. Ikuesan, V.R. Kebande, K. Siddique, A review of mobile forensic investigation process models, IEEE Access, **8**, 173359–173375, 2020, doi:10.1109/ACCESS.2020.3014615.
[13] K. Kumar, "A Discourse of Tools for Mobile Forensic Investigation," Researchgate.Net, (March), 1–7, 2020.
[14] N. Anwar, I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika, **3**(1), 1, 2017, doi:10.26555/jiteki.v3i1.6643.
[15] M. Saifizi, W. Azani Mustafa, N. Syahirah Mohammad Radzi, M. Aminudin Jamlos, S. Zulkarnain Syed Idrus, "UAV Based Image Acquisition Data for 3D Model Application," IOP Conference Series: Materials Science and Engineering, **917**(1), 2020, doi:10.1088/1757-899X/917/1/012074.
[16] L.H. Lee, Y. Zhu, Y.P. Yau, T. Braud, X. Su, P. Hui, "One-thumb Text Acquisition on Force-assisted Miniature Interfaces for Mobile Headsets," in 18th Annual IEEE International Conference on Pervasive Computing and Communications, PerCom 2020, 2020, doi:10.1109/PerCom45495.2020.9127378.
[17] V. Arista Yuliani, I. Riadi, "Forensic Analysis WhatsApp Mobile Application On Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework," International Journal of Cyber-Security and Digital Forensics, **8**(3), 223–231, 2019, doi:10.17781/p002615.
[18] K. Alissa, N.A. Almubairik, L. Alsaleem, D. Alotaibi, M. Aldakheel, S. Alqhtani, N. Saqib, S. Brahimi, M. Alshahrani, "A comparative study of WhatsApp forensics tools," SN Applied Sciences, **1**(11), 2019, doi:10.1007/s42452-019-1312-8.
[19] D. Wijnberg, N.A. Le-Khac, "Identifying interception possibilities for WhatsApp communication," Forensic Science International: Digital Investigation, **38**, 301132, 2021, doi:10.1016/j.fsidi.2021.301132.
[20] I.C. pada W.M.D. Forensics, Hasil cek24_60010313, 2020.
[21] T. Sutikno, L. Handayani, D. Stiawan, M.A. Riyadi, I.M.I. Subroto, WhatsApp, viber and telegram: Which is the best for instant messaging?WhatsApp, viber and telegram: Which is the best for instant messaging?, International Journal of Electrical and Computer Engineering, **6**(3), 909–914, 2016, doi:10.11591/ijece.v6i3.10271.
[22] F. Paligu, C. Varol, "Browser forensic investigations of whatsapp web utilizing indexeddb persistent storage," Future Internet, **12**(11), 1–17, 2020, doi:10.3390/fi12110184.
[23] M. Iqbal, I. Riadi, "Forensic WhatsApp based Android using National Institute of Standard Technology (NIST) Method," International Journal of Computer Applications, **177**(8), 1–7, 2019, doi:10.5120/ijca2019919443.
[24] J.K. Alhassan, B. Abubakar, M. Olalere, M. Abdulhamid, S. Ahmad, "Forensic Acquisition of Data from a Crypt 12 Encrypted Database of Whatsapp," 2 Nd International Engineering Conference, (October), 2017.
[25] H. Shidek, N. Cahyani, A.A. Wardana, "WhatsApp Chat Visualizer: A Visualization of WhatsApp Messenger's Artifact Using the Timeline Method," International Journal on Information and Communication Technology (IJoICT), 6(1), 1, 2020, doi:10.21108/ijoict.2020.61.489.
[26] S. Adwan, F. Salamah, Z. Akbar, I. Krisnadi, J.K. Alhassan, B. Abubakar, M. Olalere, M. Abdulhamid, S. Ahmad, K. Alissa, N.A. Almubairik, L. Alsaleem, D. Alotaibi, M. Aldakheel, S. Alqhtani, N. Saqib, S. Brahimi, M. Alshahrani, C. Anglano, D.A.O. and A. Castro2, Fitria, H.A. Ghannam, A. Hamid, F. Ahmad, K. Ram, A. Khalique, M. Mirza, F.E. Salamh, U. Karabiyik, et al., Forensic analysis of whats app messenger on Android smartphones, International Journal on Information and Communication Technology (IJoICT), 6(1), 1–17, 2020.
[27] B. Actoriano, I. Riadi, "Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2," International Journal of Cyber-Security and Digital Forensics (IJCSDF), **7**(4), 410–419, 2018.
[28] M.S. Sahu, "An Analysis of WhatsApp Forensics in Android Smartphones," International Journal of Engineering Research, **3**(5), 349–350, 2014, doi:10.17950/ijer/v3s5/514.
[29] K. Rathi, U. Karabiyik, T. Aderibigbe, H. Chi, "Forensic analysis of encrypted instant messaging applications on Android," 6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding, 2018-January, 1–6, 2018, doi:10.1109/ISDFS.2018.8355344.
[30] R. Umar, I. Riadi, G.M. Zamroni, "Mobile forensic tools evaluation for digital crime investigation," International Journal on Advanced Science, Engineering and Information Technology, **8**(3), 949–955, 2018, doi:10.18517/ijaseit.8.3.3591.
[31] H.A. Ghannam, "Forensic Analysis of Artifacts of Giant Instant Messaging 'WhatsApp' in Android Smartphone," Journal of Applied Information, Communication and Technology, **5**(2), 63–72, 2018, doi:10.33555/ejaict.v5i2.55.
[32] O. Wee Sern, N. Hidayah Ab Rahman, F. Sains Komputer dan Teknologi Maklumat, U. Tun Hussein Onn Malaysia, P. Raja, B. Pahat, "A Forensic Analysis Visualization Tool for Mobile Instant Messaging Apps," Intl. Journal on ICT, **6**(2), 78–87, 2020, doi:10.21108/IJOICT.2020.00.530.
[33] R.D. Thantilage, N.A. Le Khac, Framework for the retrieval of social media and instant messaging evidence from volatile memory, Proceedings - 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering, TrustCom/BigDataSE 2019, 476–482, 2019, doi:10.1109/TrustCom/BigDataSE.2019.00070.