ACTA INFOLOGICA 2022;6(2):189-198
dergipark.org.tr/acin

İSTANBUL UNIVERSITY PRESS

DOI: 10.26650/acin.1109682

RESEARCH ARTICLE

Digital Forensic Analysis of Discord Mobile Application on Android Based Smartphones

Android Tabanlı Cep Telefonlarında Discord Uygulamasının Adli Bilişim Analizi

İlker Kara[1]

[1] (Dr.), Çankırı Karatekin Üniversitesi, Eldivan Vocational School of Health Services, Cankiri, Turkiye

ORCID: E.E. 0000-0003-3700-4825

Corresponding author:
İlker KARA
Çankırı Karatekin Üniversitesi, Eldivan Vocational School of Health Services, Cankiri, Turkiye
E-mail address: karaikab@gmail.com

Submitted: 27.04.2022
Revision Requested: 03.08.2022
Last Revision Received: 08.09.2022
Accepted: 19.08.2022
Published Online: 31.10.2022

Citation: Kara, İ. (2022). Digital forensic analysis of discord mobile application on android based smartphones. *Acta Infologica, 6*(2), 189-198. https://doi.org/10.26650/acin.1109682

ABSTRACT

Nowadays, the spread of social media in all areas of society and becoming a part of life has led to creative and innovative changes in the fields of communication. Instant messaging applications are widely used in communication between users around the world, and the Discord application is one of them. With the Discord application, more than 300 million registered users benefit from many services such as gaming, messaging, and video chat. The use of Discord by cybercriminals has also become one of the most common applications in forensic investigations. In this study, by examining the structure of the Discord application used in Android devices, a methodology has been presented on how to extract data and how to examine these data in terms of forensic analysis. The proposed analysis methodology shows how communication analytics, contact information, message information, deleted messages, group messages, how messages are extracted and how to examine these data structures, permissions, user information, and communication protocols can be analyzed. In the results of the study, a comprehensive analysis of the Discord application in terms of judicial reviews is presented.

Keywords: Digital Forensic, Mobile Forensics, Discord, Instant Messaging

ÖZ

Günümüzde sosyal medyanın toplumun her alanında yaygınlaşarak yaşamın bir parçası haline gelmesi iletişim alanının yaratıcılık ve yenilikçi değişimlere yol açmıştır. Dünya genelinde kullanıcılar arasında uçtan uca iletişimde anlık mesajlaşma uygulamaları yaygın olarak kullanılmakta ve Discord uygulaması da bunlardan birisidir. Discord uygulaması ile oyun, mesajlaşma, görüntülü sohbet gibi birçok hizmetlerden 300 milyondan fazla kayıtlı kullanıcısı yaralanmaktadır. Bu nedenle Discord uygulaması siber suçlular tarafından da kullanılması adli incelemelerde en sık karşılaşılan uygulamalardan biri haline gelmiştir. Bu çalışma Android telefonlarda kullanılan Discord uygulamasının yapısı incelenerek adli analiz açısından Discord uygulamasından elde edilen verilerin çıkarılması ve nasıl incelenebileceğini gösteren bir metodolojisi sunar. Önerilen analiz metodolojisi iletişim analizlerini, iletişim bilgilerini, mesaj bilgilerini, silinen mesajları, grup mesajlarını, mesaj gönderme ve alma süreçlerini, veri yapısını, izinler, kullanıcı bilgileri, iletişim bilgileri, iletişim protokollerini nasıl analiz edilebileceğini gösterilmektedir. Çalışmanı sonuçlarından Discord uygulamasının adli incelemeler açısından kapsamlı bir analiz sunulmuştur.

Anahtar Kelimeler: Adli İnceleme, Adli Mobil İnceleme, Discord, Anlık Mesajlaşma

This work is licensed under Creative Commons Attribution-NonCommercial 4.0 International License

1. INTRODUCTION

Nowadays instant messaging programs are the most popular communication tools for smartphone users.(Nogubha et al. 2022). The most essential function is that it can exchange not only text messages, but also multimedia communications such as image, audio, and video contents with other people regardless of distance by using smart mobile phones (Sahu 2014). Because instant messaging services are more difficult to identify actual users than traditional communication tools, they are also commonly employed by cybercriminals (Reust 2006). As a result, forensic analysis of instant messaging programs has recognized as a crucial study field in mobile forensic investigations. Discord is developed so that online users may communicate in groups for free using the servers. Another advantage of the newly created Discord servers is that they limit the traffic density which may occur on a single channel. Discord application runs on many servers, because of that users can chat in a variety of groups, such as online gaming platforms, education platforms, technology, and software platforms, and also they can create and communicate through hidden groups, based on their interests. Users can communicate using multiple usernames depending on the server they join. Furthermore, users may create their own groups and communities by inviting people to their Discord server.

The Webhook feature is also available in the Discord application, so users can send automatic messages to the channels by using Webhook. To engage with other platforms, the functionality can send automated messages from Discord application. Although platforms like GitHub, CircleCI, and DataDog enable this feature, it is not available on YouTube or Facebook (Wulanjani 2018).

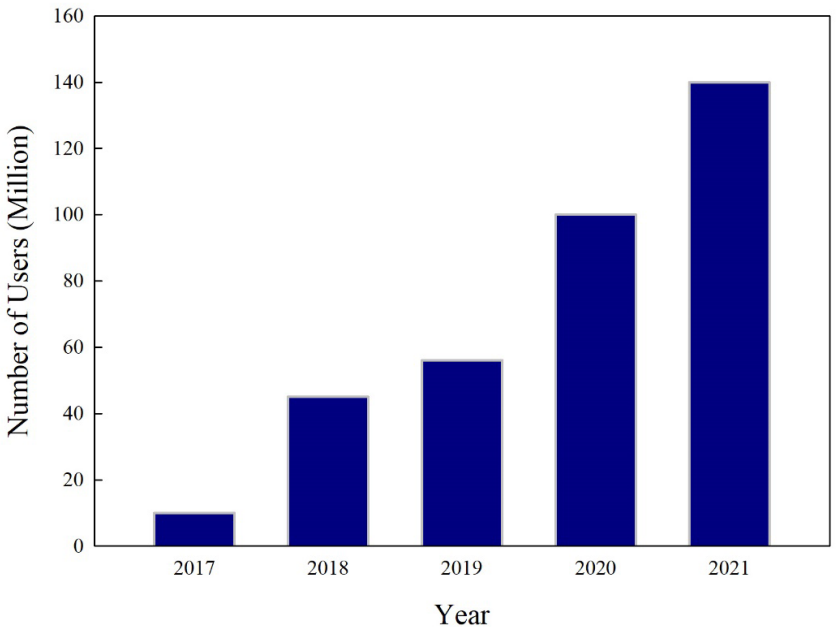

Figure 1. Discord Application Usage Rates Between 2017-2021

According to the Discord Transparency Report, which was released in the first quarter of 2019, there were over 50000 users who were subjected to harassment, threats, and abuse (Discord 2019). As a result, 10642 users were prohibited (Iqbal et al. 2021). These rates are expected to rise as the application becomes more widely used (Figure 1). Because it is more difficult to trace the users than other programs, Discord application is extensively used for instant chat among criminals. This issue requires a detailed check of Discord program in order to avoid and fight cybercrime. Looking over the literature has made it clear that there are relatively few scholarly publications in this topic. Taking all of these into account, this study provides three contributions;

This study focuses on how to conduct forensic examination of Discord application on Android-based smart mobile phones.

- We examined the structure and features of Discord application.
- We proposed a method for forensic investigation of Discord application and applied analysis for detection and extraction of messaging traffic between users. With the proposed method, it has been shown that forensic analysis can be done by transferring Discord application data to a computer instead of performing analysis on the mobile phone with the Discord application installed.
- As a result of the study, the file structure of the Discord application was analyzed, and it was seen that deleted messages could be accessed by defining the messaging protocol. It has been proven that the obtained data can be used in forensic analysis.

This study is organized as follows: In Chapter 2, important related studies are presented. The analysis methodology and tools are examined in Chapter 3 and discussions are made in Chapter 4. Finally, in Chapter 5, the study ends with evolutions of the obtained results.

2. LITERATURE REVIEW

In this section, it is briefly reviewed by focusing on some of the important studies in the field of forensic analysis of instant messaging applications in the literature.

In courts, data analysis and forensic reports received from smartphone apps that provide instant messaging services are accepted as acceptable evidence (Iqbal et al. 2021). The information received as a result of data extraction from these applications enables the user to be recognized and to access the contents of interpersonal communication. However, acquiring this data and performing forensic analysis might be challenging (Kara 2015). In the literature, various analytic softwares are utilized for forensic investigation of instant messaging systems. SQLite browser (Iqbal et al. 2021), ES File Explorer (Mushcab et al. 2015), Cellebrite UFED, and MSAB XRY are the most popular ones (Anglano et al. 2016).

In the study conducted by Anglano et al., ChatSecure application used on Android smartphones have been analyzed (Anglano et al. 2016). In the study, they developed an experimental methodology that can decrypt the end-to-end AES-256 encrypted database.

In a similar study, Wu et al. analyzed WeChat, an instant messaging application developed in China which can be used on android smartphones, iPhone, BlackBerry and Windows Phone and Symbian operating system (Wu et al. 2017). As a result of the study, they showed how to access the database of the applications, data tables, data collection ways, communication methods, and user information.

In another study, Gregorio et al. analyzed the instant messaging mechanism in the Telegram Messenger application used on smart mobile phones with the Windows operating system (Gregorio et al. 2017).

In a similar study, Ovens et al. examined the Kik Messenger (v9.6.0) application used on smartphones (Ovens et al. 2016). In the study, the open source code of the application was used, and they obtained the instant messaging mechanism in a meaningful way with database analysis. As a result of the study, they analyzed the database of the Kik messenger (v9.6.0) application and explained the database content in detail which was installed on iOS platforms.

Anglano examined the WhatsApp Messenger application on smartphones in terms of forensic analysis (Anglano, 2014). The study also showed that user contact information, messages (blocked, deleted), message chat history, message settings and preferences can be accessed on Android platforms.

In another study, Akbal et al. performed a forensic analysis of the BiP Messenger application used on a smart mobile phone with the Android platform (Akbal et al. 2020). In the study, they proposed a methodology for forensic analysis of instant messaging service in BiP Messenger application. This proposed analysis method is compatible with the analysis methodology used in our study. As a result of the study, they showed that forensic analysis of instant messaging applications can be done.

3. ANALYSIS METHODOLOGY AND TOOLS

In this study, a forensic examination of the Discord application used on a smart mobile phone has been performed. In particular, the instant messaging service used in the application, message traffic, deleted messages, user ID (identification) information, user name, user profile picture information, and user group information were focused on. A scenario has been implemented to obtain this data in the Discord application. After performing the scenario, the data produced by the Discord application was taken from mobile devices and analyzed.

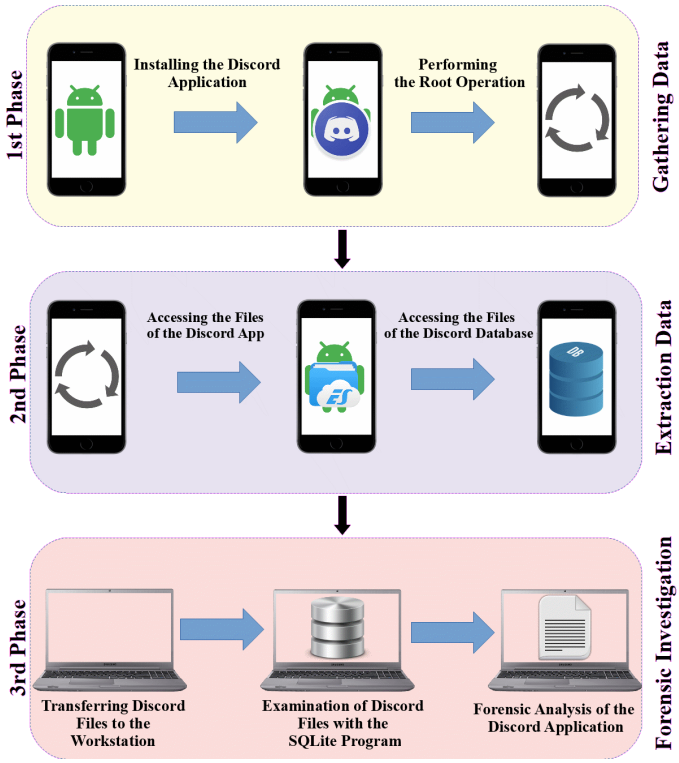

Figure 2. Commonly Employed Workflow of Analysis Approach

Mobile forensic technologies such as XRY, Oxygen Forensics, and Paraben do not identify all data created by instant messaging services (Agrawal et al. 2018). This is also true for the Discord application. In forensic investigations, this condition is viewed as a problem. To address this issue, we presented a Discord application forensic analytical method. Figure 2 shows the suggested analytical method, process, and system. The total project is divided into three sections.

Step 1: The Discord application was downloaded to the Android-based smartphone. The downloaded Discord application was extracted using the ES File Explorer file manager program. In order to copy the files of the extracted Discord application to the inspection computer, root process was applied to the smartphone.

Step 2: Before transferring the files to be analyzed to the analysis computer, the data extraction process must be performed. Database files were obtained from the application files extracted with the ES File Explorer program. After this step, the data obtained from the application were copied to the analysis computer.

Step 3: In the last stage, forensic examination of the Discord application is carried out. The data obtained from the Discord application were analyzed using the SQLite program, and the results were presented as a forensic report.

The analysis computer has an Intel Core i7 8700 32GB 1TB + 256GB SSD with Windows 10 pro operating system. Samsung Galaxy S5 brand, SM-G900FQ model with Android 6.0.1 on which the Discord application was installed, was used.

3.1. Discord Installation and File Structure on Android Devices

Depending on the operating system of the smartphone, the Discord application can also be downloaded from the play store or app store. It may be found on the app store at https://apps.apple.com/tr/app/discord-talk-chat-hang-out/id985746746?l=tr. The link https://play.google.com/store/apps/details?id=com.discord&hl=tr&gl=US was used to download the program from the Google Play Store. On Android devices, the Discord program is saved at data/data/com.discord. Table 1 displays the content of the Discord application's directories and files.

In order to examine the file structure of the Discord instant messaging application, it is necessary to perform root operation on phones with Android operating system. Rooting the Android operating system allows the user to access and modify system files. The directories obtained as a result of rooting are shown in Figure 3.

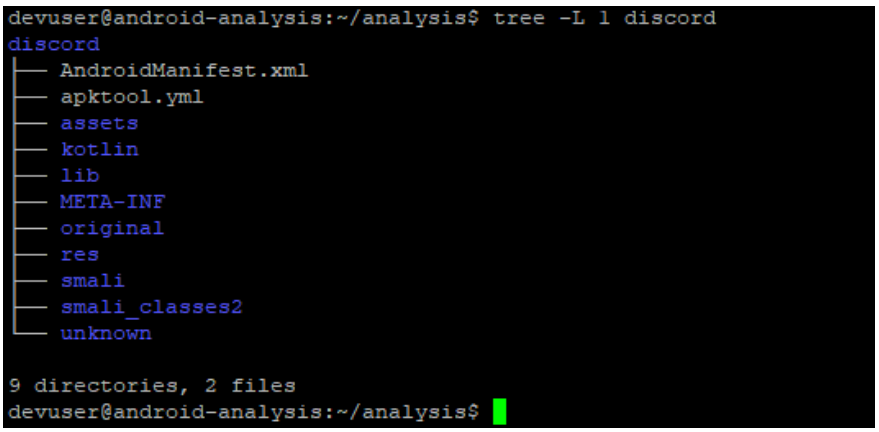

Figure 3. The directory structure of the Discord application on the rooted device

3.2. Instant Messaging Protocol in Discord App

The Discord program is an instant chat application that is accessible for both iOS and Android smartphones. The application recognizes the user based on their phone number. It features a verification mechanism that works by sending a verification code to the user's phone number and typing this code into the program. Furthermore, the contacts recorded in the phone book of the smartphone on which the program is used are added to the application's access list. A server may be created via the Discord application, or it can join an existing group's server. Voice and text messaging software are available for free on the internet (Figure 4).

Instant chatting is handled by servers in the Discord application. Users interact by either joining pre-existing servers or building new ones. There are two types of servers: private and public. Users can access public servers whenever they wish, but private servers require an invitation code and can be accessed for a limited or unlimited length of time. When a user sends a message, it is saved on Discord's application servers. The server delivers this message several times until the receiving device accepts it. When the message is accepted, the server sends it to the recipient.

Figure 4. Discord application user verification process

Table 1

User Activities of Discord Application on Rooted Device

Index Name	Index URL	Content
user_id_cache	shared_prefs/com.discord_preferences.xml	User ID cache information
email_cache	privatelvar/mobile/Containers/Data/Application	User email information
username_cache	Users_USERNAMEYAppData/Roaming/discordlcache	Structure of user information gathering
messages_cache	privatelvartrnoblre/Containers/DatatAppllcatloni_UUIDJ/libraiy/ Caches	User messaging cache information
log_cache	Users/USERNAMEJAppData/Roaming/Discord/local_Storager.log	User log records cache

3.3. Discord Application Network Communication Analysis

The Discord program features a user verification mechanism that confirms or validates a user's identity. It performs a user authentication procedure to check user information for this purpose (Figure 4).

During this process the user's ID (ID number), user name, information about whether there is a picture in the user profile or not, the user's 4-digit discord-tag id (user tag), public flag information, connected accounts information, flags information, and user information to determine if the user is in the same group are all returned in response to the verification request. Also, it is possible to find out if the user account is Premium or not.

In addition, when a request is made, data which is encoded with base64 is sent under X-Super-Properties header. Base64 Encoding is widely used in techniques which are storing or transmitting binary data by converting it into text. When the data encoded with Base64 are decoded, the model of the user device, operating system and version information which are transmitted to the Discord server can be displayed. (Figure 5).

Figure 5. Results of the Analysis of User Data base64 encoding Method in Discord Application

3.4. Messaging Analysis

Discord application stores sent and received messages under the relevant directories. There are three Discord app messaging types available. These are;

a) User-to-user messages,

b) User to server group - From server groups to user,

c) User service messages.

In terms of forensic science, the user number, chat content, and timestamp are critical when investigating the Discord application. This request is repeated at the stages of showing the user's incoming message, displaying the deleted message in the user's messaging history, and seeing the altered message once the message has been edited. Figure 6 shows the request and answer made by the user while submitting an instant messaging request using the Discord application. When a user wishes to send an instant message, the content of the Discord application is displayed in Figure 6.

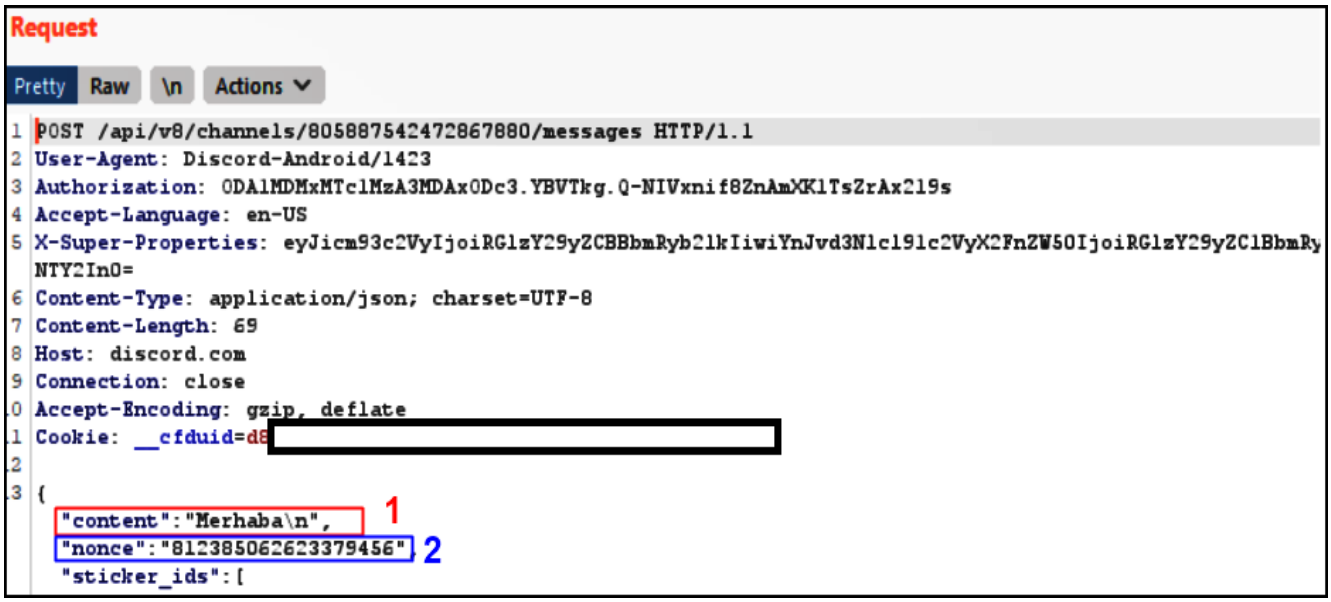

Figure 6. The Request and Response of the User in Sending a Message in the Discord Application

In this section, we observe (1) the content of the message sent by the user and (2) the procedure of the message as it is transmitted to the server. The value Nonce ("Number Only Used Once") is delivered to the server with the message. The nonce value is a one-time use numeric number. This number is used in IM apps, authentication protocols, and encryption hash (digest validation value) functions.

Users communication actions are saved in "messages" and "server-groups". In the message event, you may access all data relating to the message's content, registered contacts, date and time, and contact information. Past communications or deleted message information may also be viewed using the Discord application. Because prior communications information is requested, a request is made in the Discord program, as seen in Figure 7.

Figure 7. Request Information by Application to Display Messaging Information

When it is desired to access the past or deleted messaging information, a request is made to the server where the messaging history is located. As a result of the request, the messaging is opened on the server where the history is located. As can be seen in Figure 7, the directory "cookie:_cfduid:d" has been reached. In addition, it has been determined that the data kept on the server changes when the message is edited or deleted.

4. DISCUSSIONS

The structure of the Discord application used on Android-based mobile phones was investigated in this study, and it was described how to extract and evaluate the data collected from the Discord program in terms of forensic analysis. The user's contact information, sent/received message information, deleted messages, in-group messaging information, and communication protocols were all thoroughly examined in the Discord application. This information, which is particularly obtained for the Discord application, is critical in terms of forensic computing.

Barbaros et al. in their study examined the messaging application of the Discord application in android-based operating systems in terms of forensics with paid analysis tools (Barbaros et al. 2019). This study has two important shortages. The study is that the discord application focuses only on the messaging application, and the software used in the analysis is paid only for private users (such as police and military forces). In this study, it shows a comprehensive file-directory structure and network communication analysis in addition to the instant messaging application in the discord application on android-based operating systems. Since a paid analysis tool is not used in the proposed analysis method, it is important that it can be repeated by researchers and used in different applications.

On the other hand, forensic analysis of instant messaging applications has some difficulties. Since these applications, which are widely used today, contain their own special file structure, the forensic analysis approach of each application may contain differences. In addition, due to the storage methods and access limits of the user's messaging content of some applications, especially accessing and analyzing deleted data is insufficient.

Knowing the structure of the instant messaging application, what the application file contents consist of and in which areas they are kept will facilitate the examination in forensic analysis.

5. RESULTS

Forensic mobile investigations are defined as the study and reporting of digital evidence related to a crime in a form that may be utilised in legal proceedings. While evolving, technology drives the development of numerous apps, particularly in

the field of mobile communication. The fact that these programs have their own file formats complicates forensic investigations. Forensic specialists' capacity to access and correctly analyze the file structures of mobile applications is critical for achieving speedier outcomes in legal procedures.

In this study, an Android-based mobile phone with Discord application was analyzed and evaluated in terms of forensic computing. In terms of forensic computing, knowing what the file structure and contents of the Discord application are, especially where information such as messaging service, message traffic, deleted messages, user's information, user name, and user profile are kept will facilitate investigations.

Discord application analysis, which has a small number of publications in the literature in this field, has focused especially on the messaging application. In addition, in the studies, Discord application analyzes were examined with forensic methods on mobile devices. In this study, in addition to the messaging application of the Discord application, the forensic analysis of the messaging protocol, File Structure, and Network Communication analysis, which is important in forensic investigations, is presented. As a result of the study, the file structure of the Discord application was analyzed, and it was seen that deleted messages could be accessed by defining the messaging protocol.

Forensic analyzes on mobile devices involve some difficulties. In general, for crimes that can be committed through messaging and file sharing on a mobile phone with the Discord application, which is the subject of crime in forensic investigations, evidence is collected only from mobile devices at hand. In this study, it has been shown that evidence can be obtained from the examinations made by downloading Discord application data to the computer in accordance with forensic standards.

This situation is seen as an issue that should be evaluated because it can be an alternative to the examination difficulties on mobile devices (such as new security mechanisms, password, PIN code, PUK code, screen pattern, biometric lock (fingerprint) security policies, new features, or changes in the operating system's data storage) that forensic experts frequently encounter. Finally as a result, the proposed method is thought to be an alternative to forensic examination on mobile devices.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Grant Support: The author declared that this study has received no financial support.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazar çıkar çatışması beyan etmemiştir.
Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

References/Kaynaklar

Agrawal, A. K. Khatri, P., S. Sinha, R. (2018). Comparative study of mobile forensic tools. In Advances in Data and Information Sciences, Springer, Singapore.39-47, 2018. doi: 10.1007/978-981-10-8360-0_4

Akbal, E., Baloglu, I., Tuncer, T., Dogan, S. (2020). Forensic analysis of BiP Messenger on android smartphones. Australian Journal of Forensic Sciences, pp. 590-609, 2020. doi: 10.1080/00450618.2019.1610064

Anglano, C.(2014). Forensic analysis of whatsapp messenger on android smartphones. Digital Invest. 11(3),201-213, 2014. doi:10.1016/j.diin.2014.04.003.

Anglano, C., Canonico, M., Guazzone. M. (2016). Forensic analysis of the ChatSecure instant messaging application on android smartphones. Digital Invest. 19:44-59. 2016. doi:10.1016/j. diin.2016.10.001.

Al Mushcab, R., Gladyshev, P.(2015). The significance of different backup applications in retrieving social networking forensic artifacts from Android-based mobile devices. In 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), IEEE, 66-71, 2015. doi: 10.1109/InfoSec.2015.7435508

Barbaros, İ., & Yükseloğlu, E. H. Discord Mesajlaşma Uygulamasının Mobil Cihazlarda Adli Bilişim Yönünden İncelenmesi.

Discord, "Discord Transparency Report," Nelly, Discord Blog, 2019.

Gregorio, J., Gardel, A., Alarcos. B.(2017). Forensic analysis of telegram messenger for windows phone. Digital Invest. 22:88-106, 2017. doi:10.1016/j.diin.2017.07.004.

Iqbal, F., Motyliński, M., MacDermott, Á. (2021). Discord Server Forensics: Analysis and Extraction of Digital Evidence.

In 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS) 1-8, 2021.

Kara, I. (2015). Türkiye'de Zararlı Yazılımlarla Mücadelenin Uygulama ve Hukuki Boyutunun Değerlendirilmesi. Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi, 87-98, 2015.

Nogubha, M., Mhlana, S. (2022). Effective Use of E-tutoring System: Social WhatsApp Messenger on Social Identity Development. In IOT with Smart Systems, 729-737, 2022. doi.org/10.1007/978-981-16-3945-6_72.

Sahu. S. (2014). An analysis of whatsapp forensics in android smartphones. Int. J. Eng. Res. 348-350, 2014. doi:10.17950/ijer.

Reust. J. (2006). Case study: AOL instant messenger trace evidence. Digital Invest. 238-243, 2006. doi:10.1016/j.diin.2006.10.009.

Ovens, K. M., Morison, G.(2016). Forensic analysis of kik messenger on ios devices. Digital Invest. 17:40-52. 2016. doi:10.1016/j.diin.2016.04.001.

Wu, S., Zhang, Y., Wang, X., Xiong, X., Du, L.(2017). Forensic analysis of wechat on android smartphones. Digital Invest. 21:3-10, 2017. doi:10.1016/j.diin.2016.11.002.

Wulanjani, A.N.(2018). Discord application: Turning a voice chat application for gamers into a virtual listening class. In English Language and Literature International Conference (ELLiC) Proceedings. 2,115-119, 2018.