BALKAN JOURNAL OF ELECTRICAL & COMPUTER ENGINEERING, Vol. 9, No. 4, October 2021

Forensic Analysis of Popular Social Media Applications on Android Smartphones

Fatma Güneş Eriş and Erhan Akbal

Abstract— **The use of mobile devices as an evidence of crime has increased. Social network forensics is a branch of science that includes accessing and analyzing many personal data that may contain evidence on social networks. Considering the multiplicity of personal data artefact by social networking applications in mobile devices, the importance of examining social media applications in mobile devices emerges. In this study, the necessary processes for the forensic investigation of mobile devices are examined, the necessary procedures for data extraction from mobile devices are explained and it is revealed how the analysis of social media applications in terms of forensic information in mobile devices should be realized. In the implementation part of the study, Facebook, WhatsApp Messenger, Instagram, Twitter applications have been installed to an android device and basic user behavior analysis have been performed. During the investigation phase, Oxygen Forensic, Paraben E3: DS and Magnet Axiom were used as tools for manual data extraction and mobile forensic information. The obtained data by both methods are shown comparatively. It is shown that some important data for forensic investigations can be obtained only by manual extraction.**

Index Terms— **Mobile Forensics, Social Media Application, Android OS, Instant messaging**

I. INTRODUCTION

DEVELOPMENTS IN mobile devices; increased speed, power and storage space led more people to use their devices in a wide variety of personal processes such as online shopping, bill payment, social sharing. According to statistics, 52% of web traffic in the world is performed via mobile phones [1]. With the widespread use of mobile devices, the use of social media applications has also increased. Social media applications encourage users to share their personal data. Thus, people using social media often leave a large number of personal data remains on their mobile devices without being aware of it [2]. This makes mobile devices the priority evidence that must be examined during a crime assessment. On the other hand, mobile devices are known to be used or targeted by cybercriminals for malicious activities such as data leakage, malware, identity theft, piracy, illegal trade, sexual harassment, cyber tracking and cyber terrorism. For all these reasons, studies in the field of mobile forensics are very important for the future of digital forensics examinations [3]. The analysis of social media applications on mobile devices is a stand-alone study area. There are lot of tools developed for mobile device examinations on the market. These tools vary in their ability to extract data from social media applications. Where mobile device examination tools unable to respond to the analyst because of variations in devices and continuous renewal of applications, the analyst may be required to access the data from the file system himself/herself.

Accessing important data is a vital part of forensic investigations. Commonly forensic analysis softwares are used to obtain all available data in a digital media. But forensic analysis softwares sometimes can’t show all related data of social media applications due to very fast updating of social media applications and their storage systems. In response to this problem, the update rate of forensic evidence analysis software is often insufficient. There are also data that cannot be detected by the software and are not available to the analyzer. The main disadvantages of the investigations carried by software tools are that the interpretation in accordance with the case cannot be made by the software and the data that can be called “residual” are ignored by the software.

In this study, data that can be important in the examination of social media applications are shown. In cases where forensic evidence analysis software is deficient, the data to be examined have been identified and their contents are presented. We also compared the manual examination results with results obtained from forensic investigation softwares.

II. RELATED WORKS

With the increase in mobile device usage rates, studies about mobile examinations review have also increased. Mobile forensics includes processes such as data extraction, examination and analysis on mobile devices. And these processes must be well modeled for device examination to be successful.

In 2007, Jansen and Ayers form the basis of this modeling. This model consists of protection, data acquisition, examination & analysis and reporting [4]. Based on this model, Lin et al. proposed another model consisting of four

FATMA GÜNEŞ ERİŞ, is with Department of Digital Forensics Engineering University of Fırat University, Elazığ, Turkey,(e-mail: f.gunes@firat.edu.tr).
https://orcid.org/0000-0002-6048-6060

ERHAN AKBAL, is with Department of Digital Forensics Engineering University of Fırat University, Elazığ, Turkey (e-mail: erhanakbal@firat.edu.tr).
https://orcid.org/0000-0002-5257-7560

Manuscript received July 1, 2020; accepted September 20, 2021.
DOI: 10.17694/bajece.761271

stages: start, preparation, operation and reporting [5]. The operation phase is the most important in this model. This phase consists of three stages: collection, analysis and forensics. The study also compared these two models and argued that the model proposed by Lin was more reliable than the legitimacy of digital evidence.

In his study, Murphy stated that with the increasing demand for the examination of mobile phones and other mobile devices, there was a need to develop processes for the examination of these devices [6]. The developed process consists of nine stages; evidence collection, identification, preparation, isolation, processing, verification, reporting a, presentation and archive stages.

In the study conducted by Sadiq et al., some of the previously used mobile forensic examination models were reviewed and existing models was compared [7]. The advantage of the proposed model is the combination of the extra and repeated stages and stages of the previous models.
Ali et al. [8] developed an approach for mobile forensics. The examination process was simplified and supported the training and knowledge management activities. To achieve this, the authors developed an eight-step mobile forensic examination model. In his study, Pantaleon investigated the effect of rooting process on android mobile devices' user data integrity [9]. In this study, data integrity issues related to user data were examined when a device was rooted before data extraction. As a result, it has been demonstrated that no change is observed in user data when root access is enabled.

Rooting process is essential for application based mobile device examinations. In their work, Wu et al. conducted a review of the WeChat instant messaging application on android devices [10]. In this study, obtaining of user data, decoding of encrypted database and review of interviews were shown. Different versions of the application were examined. Upgrade usually refers to possible changes in the data storage format and data protection measures. Such problems are also seen in the forensic examination of other Android applications. Therefore, it has argued that the reverse analysis and data protection mechanisms of Android applications must be continuously examined to meet the new requirements of the applications.

A study by Ovens and Morison is a reference for forensic computing analysis by accessing and interpreting the data created or modified by Kik messenger on the latest iOS version and iTunes backup files [11]. A detailed description of the findings created or modified as a result of the study is provided. Gregorio et al. conducted a forensic analysis of Telegram Messenger, an instant messaging application built on Windows Phone operating system. The study provides an overview of forensic analysis, while focusing on how the findings are structured and the user, chat and speech data created by the application [12]. Anglano conducted an analysis of WhatsApp Messenger application on android devices. As a result of the study, it was revealed how the findings of WhatsApp application left on the devices should be obtained, examined and analyzed by analysts [13]. Dezfouli et al. examined social networking applications on android and iOS devices. Facebook, Twitter, LinkedIn and Google+ applications were installed on the devices and certain behaviors were performed on these applications [14]. Afterwards, data were searched for devices that might be important in a forensic investigation. In this study, the forensic computing structure developed by Martini and Choo used [15]. Another area of study related to mobile forensics was conducted by Cahyani, et al. [16]. In their study, they investigated the role of mobile forensics in the study of terrorism using cloud storage service and communication applications. In particular, they have demonstrated how mobile forensic techniques used to recover evidences from client devices using a series of tests that are controlled on Android and Windows devices. In its work, Azfar, Choo and Liu have examined 30 popular Android communication applications collected using XRY, a mobile judicial tool commonly used to logically extract images from the Android phone. Various information, such as contact lists and chronology of messages, has been gathered [18]. Finally, the findings described in the study of thirty communication applications are summarized using taxonomy. The most common problem with mobile device examinations is the inability to obtain sufficient information during the examination process [21]. Although the commercial software have certain capabilities, it is not clear which software should be chosen by analyst. In addition, the review process is disrupted when there is no commercial tool. The aim of this study is to show how digital forensic analysis of social media applications on mobile devices. Sony Xperia Z2 device with the Android operating system has been selected for investigations in this study. Because the most widely used operating system on mobile devices in the world is Android. Facebook, WhatsApp Messenger, Instagram and Twitter applications, which are widely used in the world, are used in this study. In this study it is shown that how to perform data extraction from social media applications by using commercial mobile forensic tools and manually viewing files of the applications extracted from the file system of the device. In addition, the performance of the used mobile forensics tools in the application analysis was compared. It has also been shown how the application analysis should be performed manually for those who do not have these tools or when these tools are not sufficient for the analyst. In previous studies in the literature, since the application versions are quite old, there is no information about the additional features added to the applications [23-28]. Our study was carried out using the most current application versions.

The main objective of this work is to show user behaviors who are used Facebook, Twitter, Instagram and WhatsApp. These behaviors are obtained by using mobile forensic software and manually from the application data in the mobile device memory. Therefore, both manual and software tool based mobile investigation are performed for Facebook, Twitter, Instagram and WhatsApp applications in this work. Firstly, physical and logical images of the mobile android device are extracted. Then, the extracted images are examined by using the widely used mobile forensics tools (Oxygen, Paraben, Axiom, Autopsy) and manually. The major contributions of this paper are given as below.

- In the literature, many works and articles have been published about forensics analysis of Facebook, Twitter, Instagram and WhatsApp separately. In this work, we analyzed these popular social media application together.

- Both manual and software examinations are presented in this paper about these applications.
- A comprehensively mobile forensics software benchmark is presented and advantages and disadvantages of these are shown. The widely used mobile forensics application are compared to each other in view of social media applications.
- This paper shows that effective methods about mobile forensics for social media application to investigation experts and researchers.

In this study, forensic analysis of popular social media application is presented. In Section 2 is shown related work. In section 3, methods of obtaining data from mobile devices are shown. Section 4 describes the software used, performed user behaviors, the application environment, manual and software based data acquisition process. In section 5, the results and findings are shown.

III. DATA ACQUSITION METHOD

Four basic methods are used to obtain data from mobile devices. These are logical, file-based, physical, and manual extraction. Logical data extraction is the process of extracting a bit-bit copy of logical storage objects from a mobile device [19]. Logical storage objects include files and directories in the file system. The data extraction tool communicates with the mobile device's operating system and requests information. Logical extraction is performed using the original API (application programming interface) of the manufacturers. Data extraction is easy with this method and applied easily implemented by the examiner. A logical data acquisition does not generate deleted data. When the data is stored in a SQLite database on a mobile device and data is deleted, the data is not overwritten. When data is deleted in this database, it is usually marked as deleted and rewritten later. This means that it is possible to recover deleted data if a file system's data acquisition is provided through the synchronization interface of a mobile device. File system extraction from the mobile device allows performing analysis using Physical data extraction is a method that requires a bit-copy of the physical memory (flash memory) of the device, and this method is very similar to the computer forensic examinations [20]. Physical data extraction allows full access to all files on the device, allowing review of deleted files and data remains. Physical data acquisition is more difficult than other methods. Mobile forensics tool manufacturers develop custom boot installers to perform physical extraction, often allowing access to the mobile device's memory and in most cases bypassing pattern lock or passwords. Physical extraction is not supported for all devices. In this method, the investigator uses the user interface to perform an examination in the phone memory. For this method, there is no need to use tools to convert operating system-specific data. In practice, this method applies to mobile phones, PDAs and navigation systems. The disadvantages are that only the data appears in the operating system is recovered and the process is very time consuming.

IV. IMPLEMENTATION

A. *Experimental Environment And Examination Software*

First, devices to be examined were provided. The necessary applications have been downloaded to these devices and application-specific behaviors have been implemented on the applications. In this case, the logical images of the devices were taken. Then, the necessary software for the mobile examination is installed on the workstation where the review will be carried out. Mobile review was conducted with the help of open source and commercial software. The features of the equipment used in the study are given in Table 1.

TABLE I
HARDWARE AND SOFTWARE USED IN THIS STUDY

Hardware		Purpose of use
Windows 10 Pro, 64-bit processor, 16 RAM Monster Abra A5 Laptop		Workstation
Sony Mobile Xperia Z2 LTE-A (D6503) 16 GB Android 10.0		Device to examine
Vodafone SIM card		SIM card
Software	Version	Purpose of use
Android SDK	-	Geting physical image
Flashtool	9.18.6	Rooting device
DB Browser for SQLite	3.10.1	Examining SQLite database files
HXD Hex Editor	1.7.7.0	Examining file contents in hex format
plistEditor pro	V2	Examining Plist Files
Oxygen Forensic Detective	8.4.0.99 (USB license)	Examination Tool
Paraben’s E3:DS	Aurora 1.4 Edition	Examination Tool
Magnet AXIOM Examine	v1.2.5.8637	Examination Tool
Android Facebook Application	149.0.0.40.71	Application to be examined
Android Facebook Messenger Application	143.0.0.20.69	Application to be examined
Android WhatsApp Messenger Application	2.17.395	Application to be examined
Android Instagram Application	22.0.0.17.68	Application to be examined
Android Twitter Application	7.21.0	Application to be examined

Social media applications to be used in the study are configured Facebook, WhatsApp Messenger, Instagram and Twitter apps have been downloaded from the Google Play Store to the Android device logged in with the mail address. The structures of the applications were examined and the behaviors that could be performed were determined.

B. *Performed User Behaviors*

In the study, Facebook, Facebook Messenger, WhatsApp, Instagram and Twitter applications are installed on the mobile device. There are user behavior models that applications perform individually. In terms of forensic information, the consequences of user behavior are considered evidence. Therefore, each application-specific behavior was performed on the mobile device. The characteristics of the application and the behaviors we have performed are given in Table 2. This table shows commonly accepted user behaviours-actions [29].

TABLE II
USER BEHAVIORS PERFORMED IN APPLICATION

Appl	Application Behaviors	Performed User Behaviors
Facebook	Sharing	Status, Photo, Location sharing performed
	Commenting	Commented on a photo
	Liking	Liked a post
	Adding friends	Adding, deleting, blocking a friend behaviors was performed
	Creating Group	A group was created, shared some posts in this group, one of the posts was deleted
	Story Sharing	A story was shared
	Messaging	Sent messages to a user and deleted one of these messages Sent messages to a group and deleted one of these messages
WhatsApp	Messaging	Message, Photo, location shares have been made. A few of them have been erased
	Creating Group	Messaging performed. A few of messages have been erased.
	Blocking Friends	Performed.
	Video Calling	Performed
	Calling	Performed
	Story Sharing	Performed
Instagram	Sharing	Photos and videos were shared. One of them was erased.
	Status	Statuses shared. One was deleted.
	Liking	A photo is liked.
	Commenting	Commented on a photo and status
	Messaging	Private messages have been sent to a user. 1 of them has been canceled.
	Following	A number of accounts were followed, an account was removed from the follow, an account blocked.
	Saving Posts	A post saved.
	Tagging	A photo was shared with a tag.
Twitter	Tweeting	Some tweets shared and one of them was deleted
	Replying	Replied to a tweet
	Retweeting	Retweeted a tweet
	Liking	A tweet was added to the likes
	Messaging(DM)	Sent DM's to a user. One of them was deleted
	Following	A number of accounts were followed, an account was removed from the follows, account blocked.

C. Data Acquisition Process

In this study, Sony Mobile Xperia Z2 LTE-A (D6503) device with 16 GB capacity and Android 10.0 version was used. During the image acquisition process, Paraben, Oxygen Forensic, Magnet Axiom commercial software and ddtool open source tool were used. Respectively, logical image of device was obtained, device was rooted and physical image of device was obtained.

The logical imaging is the process of getting a copy of the field that contains the files that the operating system allows for the user to access. In this image type, data such as program databases, log files, operating system files are not available. Since the operations to ensure that access to files that is not accessed with a logical image is lead to loss of data in some cases, the image type that should be taken first is the logical image when the evidence begins to be examined. This prevents loss of data that is not difficult to obtain. In this way, the loss of data that is not difficult to obtain is prevented. Therefore, the logical image of each mobile device to be examined should be taken. Data such as messages, pictures, notes, contacts, call records is more easily obtained than the physical image. It has an important place in mobile device investigations as it is sufficient as evidence. In the application, the logical image of the device is taken with Paraben E3: DS and Oxygen Forensic software. Obtaining the physical image of any device means extracting the bit-bit copy of the original device's memory. In addition to the logical image, the physical image provides access to data in the unallocated space, deleted data and application databases. For the physical imaging, Android devices must have root access. The root process is risky in terms of forensics because it will perform some changes on the device, but it is necessary to get the physical image of the device to access all the data on the device. For example, if all data on a device has been manually deleted, logical deduction will not be sufficient to retrieve this data. This data is only accessed using the physical image. Therefore, after logical imaging of device, physical imaging is performed to access deleted data on device.

V. APPLICATIONS ANALYSIS

In this study, the selected social media applications were first examined using manual methods. Subsequently, it was analyzed using commonly used software to show importance of manual examination.

A. Analysis of Facebook

Firstly, it was shown how to acquisition manual data from Facebook. For the forensic examination of the Facebook mobile application, the folders /data/data/com.facebook.katana and /data/data/com.facebook.orca, which is accessed by taking the physical image of the mobile device, are examined. The /data/data/com.facebook.katana folder contains the data for the Facebook application and /data/data/com.facebook.orca contains the Facebook Messenger application data. These folders contain subdirectories such as cache, files, databases folders. The Cache folder contains audio and image files in the cache, and the files folder contains video-cache files without extension. The databases folder contains a list of contact persons, the list of notifications, recorded videos, pages added to favorites, established groups, managed pages, and database files containing many personal data. These directories contain files and folders of particular importance in mobile forensic investigations.

The /files/NewsFeed folder contains video data that falls on the user's home page. However, it is not possible to obtain information about who sent these video files.

The /cache/image folder contains image files that are cached on the user's home page, which are cached from their own profile, the profile of the connected contacts, and other pages that are displayed. These files are saved with .cnt extension.

The /databases folder contains database files. bookmarks_db2 contains a list of pages and groups that the user has subscribed to in the database. Some of the data is automatically generated by the Facebook application, but the data created by the user itself is contained in this database. The most important table of this database is the bookmarks table.

In the Bookmarks table, the bookmark_name column contains bookmark names, the bookmark_url column contains bookmark urls, the bookmark_pic column contains bookmark icon url, and the bookmark_type column contains bookmark type. The bookmark_unread_count column shows how many messages are not seen by the user.

The contacts_db2 database contains all the information about the contacts the user is contacting.

The contents of the columns of the contacts_db2 database shown in Table 3. The fbid column contains unique IDs that are used to identify people in other databases. The first_name, last_name, display_name columns display the names of the contacts. The small_picture_url, big_picture_url, huge_picture_url columns contain links to profile images of people. The Communication_rank column contains the rates that indicate how often the person communicates with the user, taking into account messages, comments, and other possible factors. The Added_time_ms column contains the time to add the contact as a friend. Bday_day and bday_month columns show the date of birth of the person in days and months. The Data column contains a copy of all data in the database together with the location information of the contacts.

TABLE III
FACEBOOK CONTACTS_DB2 DATABASE CONTACTS TABLE COLUMN PROPERTIES

Column name	Content
contact_id	The id assigned to communication between users
fbid	The id assigned to the user by Facebook
first_name	Contact person's name
last_name	Contact person's Surname
display_name	Name displayed in the contact's profile
communication_rank	Frequency of communication with contact
added_time_ms	Time to make friends with the contact person
bday_day	Contact person's birthday
bday_month	Birthmonth of contact person
data	A copy of all data in the database

newsfeed_db is the database containing the data shown to the user on the main page. The home_stories table in this database contains important data, Table 4 shows the column properties of this table. The fetched_at column displays the time that the posts were taken from the servers, and is related to the time that the user uses the application or sees the post. The story_data column contains the post that is stored as a data block. When viewed in a hex or text editor, the sender's username is found, but no data was found in our study in this column. The cache_file_path column contains data paths for cached files. These files are analyzed with a hex editor.

TABLE IV
FACEBOOK NEWSFEED_DB DATABASE HOME_STORIES TABLE COLUMN PROPERTIES

Column name	Content
fetch_at	When posts are taken from servers
cached_id	Cached id of the post
cache_file_path	The data path of the cached file of posts
story_id	Post id
story_type	Post type
seen_state	Seen status of the post
story_data	Post stored as data block

The notifications_db database contains information about notifications. The seen_state column in the gql_notifications table indicates whether the notification is displayed or not. updated column is the column that indicates when the notification was read or sent in Linux epoch format. The Gql_payload column contains the contents of the notification as well as the sender information, similar to the story_data column in the newsfeed_db file. Notification text is obtained more easily from the columns of summary_graphql_text_with_entities and short_summary_graphql_text_with_entities.

profile_picture_url contains a public URL to display the sender's profile picture.

The prefs_db database saves the application settings in the preferences table. The setting names are found in the key column the value column has the status of the setting. Usage data, which are important in forensic examinations, are included in this database. The /config/gk /last_fetch_time_ms row, displays the timestamp that when the application is communicating with the Facebook servers. However, this information does not always guarantee that the user is using the application at this time. Last user activity information is stored in /fb_android/user_last_used_app_time row. /fb_android/last_login_time row shows the time that when the user logged in to application last. The usegae profile of the application is obtained with lots of data such as this. In /audience_prefs/selected_voice_name row the username and in /fb_android/uvm/current_account row e-mail address of the user is stored.

threads_db2 is located in the com.facebook.orca folder. This database contains data such as message contents, contacts or groups communicated via Facebook Messenger. The list of contact persons is found in the thread_users table, while the message contents and search information are contained in the messages table.

The messages table's column properties are given in Table 5.

The call_logs_db database maintains log records for calls. The user_table table, contains information about the call time and how long it takes. To find deleted messages, the threads_db database should be examined.

Secondly, it was shown how data acquisition using software tools from Facebook. When logical image examined with Oxygen Forensic, /sdcard/com.facebook.katana and /sdcard/com.facebook.orca folders is found related to Facebook application. However, there is no significant data in these folders.

TABLE V
FACEBOOK THREADS_DB DATABASE MESSAGES TABLE COLUMN PROPERTIES

Column name	Content
msg_id	A unique id for each message
text	Message content
sender	Name of the person who sent the message
attachmets	Message attachments
timestamp_ms	Sending or receiving time of message
thread_key	Group or user ids
source	Message source

When the physical image is examined, various data is obtained by Oxygen Forensic. This section provides significant convenience to the analyst. The software quickly pulls important data from appropriate databases or files and presents it to analyst. User Data section of Oxygen Forensic software contains contacts information, cookies, and cached image files. The Application Files section contains all the files related to the application.

In the user data section, the contacts are presented with their name, surname, whole name and telephone number, if any, profile image URL, birthday, city, user ID and insertion time information. And other information like cookies, cookie host, cash files are retrieved easily by Oxygen Forensic software.

The Facebook Messenger application keeps the messaging data, and when the data obtained from this application with Oxygen Forensic tool is viewed; in the Attachment section, the additional files are displayed with the message ID information, type, file name, URL. The cached_files section displays cached .cnt image files. In cookies section, the cookie name value, the website it comes from and the creation time are presented to the user. Unlike what is expected in this section, messages between users are not displayed. In the Oxygen Forensic software, the application must be examined manually to view the messaging details.

When the logical image was examined with Paraben, no significant data could be reached. When the physical image is examined, it is seen that the software provides the user with information such as application setting details, contact list, messages with groups and people. Here, under the title of raw_settings, there are Facebook application settings. The Contacts section contains the name, surname, profile name, and user ID of Facebook contacts. The Current Info section of Facebook Messenger contains information such as the user's country code and phone number. Conversations with people and groups are listed with person and group ID numbers in Conversations section. Here you will find the name and ID of the person who sent the message, the content of the message, the conversation in the binary format, the presence of additional files. Groups Conversations List contains information about the ID numbers of the groups that have been created up to this time and the persons included in the group.

In the File browser section, all application files are accessed. The user has access to all detailed data about the location of the application. When the image taken with ddtool is examined with the Magnet Axiom tool, the conversation of the groups, contacts and messages in Facebook Messenger are presented to the user. Messages are shown in detail in a list and in the preview screen messaging are displayed as chat screen. Facebook Messenger Groups includes group ID number, participant IDs, last message sending time, total number of messages. In the Facebook Messenger Messages section, the name of the person sending the message, the sending time, the message content, the type of attachment if any, the id assigned to the message, the source of message, the location information in the message, latitude longitude information is available. Users contacted via Facebook Messenger include the user ID number, name, surname, profile name, user name, profile image URL, whether it is a friend or not, contact frequency with the contact.

In the social network section, there are detailed information about people under Facebook contacts; Under Facebook posts; messaging is available with details. In the corrected results section, Facebook URLs are available to define the activity. Under Facebook contacts, the profile ID, name, surname, profile name, profile image URL, phone numbers information is included.

B. *Analysis of WhatsApp*

Firstly, it was shown how to acquisition manual data from WhatsApp. On Android devices, the WhatsApp application data is accessed from the physical image from the databases under the /data/data/com.whatsapp/databases/ folder. The msgstore.db and wa.db SQLite databases contain data on user interaction that is important for mobile forensics. wa.db contains detailed information about WhatsApp contacts, whereas msgstore.db stores detailed information about chat conversations between the user and contacts.

When wa.db database is examined, it is seen that it contains wa_contacts table. WhatsApp stores the information in the user's phone book in its own database and stores the names and phone numbers and status of the contacts in this table if they are WhatsApp users.

The columns of the wa.db database are shown in Table 6. Jid information is an ID that the WhatsApp application assigns to users and groups. Format of this id is user_phone_number@s.whatsapp.net for users and phone_number_of_creator@g.us for groups.

If the msgstore.db database is examined, the chat_list table contains the information of the contacted people. The key_remote_jid column stores each account that the user communicates in such a way that it starts with the phone number. The group_participants table stores the member information of the groups. The gjid column contains the group id, the jid column contains the id of the persons included in the group, the admin column contains the value of 0 for the others and 1 for creator of group.

TABLE VI
WHATSAPP WA.DB DATABASE WA_CONTACTS TABLE COLUMN PROPERTIES

Column name	Content
jid	Id assigned to the person or group by Whatsapp
status	User status information
Status_timestamp	The latest update time of the status
Display_name	Displayed name of user
number	User phone number

The Messages table contains the details of the messaging records. The column details of the Messages table are given in Table 7. The key_remote_jid column here is the same as that mentioned in the wa.db database.

TABLE VII
WHATSAPP MGSTORE DATABASE MESSAGES TABLE COLUMN PROPERTIES

Column name	Content
key_remote_jid	Id assigned to the person or group by Whatsapp
key_from_me	The direction of the message (0 if message is received, 1 otherwise)
data	Message content
timestamp	Sending or receiving time
media_mime_type	Attached file format
media_size	Attached file size
media_name	Attached file name
latitude longitude	Location latitude and longitude

The key_from_me column specifies the direction of the message. The data column contains the message text. The media_mime_type column contains the file format for attachments sent or received. The media_size and media_name columns contain the size and name of the attcahments. And location inforation is stored in the latitude and longitude columns.

For deleted messages, if msgstore.db database is examined as hexadecimal, the text message and location information that has been sent and deleted in the group has been detected.

Secondly, it was shown how data acquisition using software tools from Whatsapp.

When the logical image was examined with Oxygen Forensic, it was observed that the WhatsApp findings were found under the / sdcard / WhatsApp folder. User data only displays a few image files that have been submitted, while in the Application Files section, all the files that the application has access are displayed.

When the File browser tab is opened, it is seen that there are databases folder and media folder under / sdcard / WhatsApp / folder. The Media folder contains data that is sent or received with the WhatsApp application. Under the Databases folder, the there is a file that contains detailed information about the chat conversations between users and their contacts. This file is the msgstore.db.crypt12 file obtained by encrypting the msgstore database file. This file is opened only with a key file that is accessed after rooting the phone. After the phone is rooted, more database files containing user actions are accessed. Therefore, it is very important to examine the physical image for a detailed analysis of the WhatsApp application.

When the physical image is examined with Oxygen Forensic software; it is seen that within the User data section, account information, WhatsApp contact list, groups, group information, messages with contacts, outgoing calls, media and log information are stored. This section provides significant convenience to the analyst. The software quickly pulls important data from the appropriate databases or files and offers them to analyst. Account section displays contact information, phone number, profile picture of user. In Contact list in WhatsApp Messenger Contacts, the name is displayed along with the account ID (starting with the phone number), phone number, status information and profile pictures. In the WhatsApp Messenger groups, the account id (starting with the number of the person who creates the group), the group name and the id information assigned to the group are displayed. Group Chat info displays the group ID, name, telephone numbers of the members and the names of the members. Media section contains information about the files sent. Log section contains names of log files.

Application files section displays all related files in the application. When the File Browser tab is opened, it is seen that /data/data/com.whatsapp is the location of the files that will allow us to analyze the application.

When the logical image is examined with the Paraben E3 software, the WhatsApp findings is not reached. When The full logical image of the rooted device examined with Paraben E3, the list of contacts, recovered contact list, conversations and recovered conversations are accessed. Contact information in contacts section are contact name, last name, WhatsApp name, WhatsApp ID, status, latest update time and phone number. In the Chats section, the list of contact persons is presented; when they are clicked, the time of the conversation, the identification, the message content, the outgoing / incoming information, when the message was sent / received, the time it was received by the server, the time of being received by user and the Attachment information is presented to the user.

When the image taken with ddtool is examined with the Magnet Axiom tool, the results about WhatsApp is examined under different headings. Under WhatsApp contacts title, users' WhatsApp credentials, phone numbers and names are displayed. Clicking on the contact displays all details about the contact. Under WhatsApp groups, group ID, group name, and group members information are shown.

When the WhatsApp messages heading is examined, the analyst is presented with full details of the messages. The sender / receiver information of the message, the time of sending / receiving, the time of receiving the message of the recipient / server, the message content, the transmission status of the message, if message contains media file its URL and type and database of these information are stored in this section. When the message is clicked, the conversation made with that user is presented to the analyst in chat format. Apart from these, the analyst is presented with an area under the media title, which contains WhatsApp profile pictures. Here you will also find information such as the date when the profile image was created and the size of the image.

C. *Analysis of Instagram*

Firstly, it was shown how to acquisition manual data from Instagram. For the forensic analysis of the Instagram mobile application, the /data/data/com.instagram.android folder and /data/media/0/Android/data/com.instagram.android/ folder, which is only accessed by physical image, are examined. The /data/data/com.instagram.android folder contains subdirectories such as cache, files, databases, shared_prefs folders.

In the databases folder, there is direct.db file which is the only file that the Instagram application stores in the SQLite database. This database stores the messages with the details. The values stored by the columns of the tables of the direct.db database are given in Table 8.

TABLE VIII
INSTAGRAM DIRECT.DB DATABASE MESSAGES TABLE COLUMN PROPERTIES

Column name	Content
User_id	ID assigned to the person by Instagram
timestamp	Message sent time
message_type	Type of message
text	Message content
message	All details about the person who sent the message and the message

Another folder that contains important files in terms of digital forensics is shared_prefs. This folder contains XML files.

/shared_prefs/com.instagram.android_preferences.xml file contains detailed information such as name, biography, followers and follow-up numbers of user and, profile picture url.

6244347999_USER_PREFERENCES.xml is a file containing user-related settings for the application, including the most recent searches with their times, as well as timestamps of uploaded stories.

The file 6244347999_news_feed_notifications.xml contains new notifications with details. 6244347999_video_view.xml is the file where watched videos and their viewing times are stored. In the 6244347999_organic_view.xml file, the displayed photos and videos are included with timestamps. 6244347999_AutoCompleteHashtagService.xml is the file containing the hashtags that have been searched and completed automatically. The unauthenticated.xml file is the file that keeps track of how many times a login has been made with which account.

Another file that contains important data about Instagram is MainFeed.json.0003. This file is located in the /data/data/com.instagram.android/cache/ folder. Within this file there is informations such as the URL of the media falling on the user's home page, the user name of the person sharing the media, the profile picture URL, whether the account is hidden or not, if it is liked or not, the number of comments, the time information and the number of likes.

/data/data/com.instagram.android/cache folder contains images that the user shared in Instagram application. The /data/data/com.instagram.android/cache/blur_icons file contains filter options for the shared images. /data/data/com.instagram.android/cache/images/ folder contains image files related to Instagram. / data / media / 0 / Pictures / Instagram / file includes pictures shared by the user.

Deleted messages were detected when the direct.db database was viewed with hexadecimal to view the contents of the deleted messages.

Secondly, it was shown how data acquisition using software tools from Instagram.

When the logical image is examined with the Oxygen Forensic tool, it appears that there are shared image data and video cache files contained in the /sdcardAndroid /data/com.instagram.android file. When the physical image is examined, User data section contains all Instagram accounts on the phone, the currently used Instagram account, the user's Instagram pictures, the user's search history, and all the pictures displayed on the cache in Instagram. Under All accounts and Current account, the user's full name, user name, profile image URL, number of followers, number of accounts he follows, and user ID are available.

When the physical image is examined with Paraben, the original state of the pictures, all the pictures on Instagram, the conversations, the recovered messages, the accounts logged in this device are displayed. Original Media section includes pictures shared by the user; In Cache media section, images displayed on Instagram and cached clean files are displayed. The Conversations section shows when the last contact with the communicated persons, the person's name in Instagram, the person who invited them to speak, and the credentials assigned to the conversation. Under the heading Conversation, the time of recovered messages, conversation id, message type, message content and raw form of message are present. In the Accounts heading, the user ID, name, whether the user has logged in or not, and the profile picture URL information are stored.

When the image taken with ddtool is analyzed with the Magnet Axiom tool, Instagram user information, direct messages, media and profiles is examined under different headings. In the user information, user name, full name in Instagram, profile image url are available. When direct messages are examined, the sender / receiver information, direction, content, time and type of the message are presented to the analyst.

Instagram Media contains cached images that the person showed on Instagram. A thumbnail of image, type (such as jpeg, png), when image is created / changed and image size information is shown.

Under Instagram profiles, the name of the contacts, contact details, profile image urls, and biography information, if any, are provided.

D. *Analysis of Twitter*

Firstly, it was shown how to acquisition manual data from Twitter. For the forensic analysis of the Twitter mobile application, the /data/data/com.twitter.android/ folder, /data/media/0/Android/data/com.twitter.android/ folders, which is only accessed by physical image, are examined. The /data/data/com.twitter.android/ folder contains subdirectories such as cache, files, databases, shared_prefs. Files and folders that are particularly important in mobile forensic examinations from within these directories are generally in the databases under the /data/data/com.twitter.android/ folder.

The Databases folder contains the application's databases. 921137666602819584-48.db database contains important information. Here the conversation_entiries table contains the contents of the so-called dm (direct message) conversations with the user with their creation time in Linux epoch format. The table's column properties are given in Table 9.

TABLE IX
COLUMN PROPERTIES FOR THE TWITTER CONVERSATION_ENTIRIES TABLE

Column name	Content
entry_id	Id assigned to message
conversation_id	Id of messaging between user and contact person
user_id	Id of the person sending the message
created	Message creation time
data	Message content

The conversation_participants table contains the user IDs of the people who perform the conversations. Conversations table holds the id of the conversations. The conservation_id herein includes the id of the contact person and the id of the user. The Statuses table contains tweets that fall on a person's home page. The table's column properties are given in Table 10.

TABLE X
TWITTER 921137666602819584-48.DB DATABASE, STATUSES TABLE, COLUMN PROPERTIES

Column name	Content
status_id	Unique id assigned to tweet
author_id	Id of who sent the tweet
content	Content of the tweet
source	Source of the tweet
created	Creation time of the tweet
favorited	Whether if the tweet liked or not
retweeted	Retweet status (1 if retweeted 0 otherwise)
favorit_count	Total number of likes for tweet
retweet_count	Total number of retweeting for tweet
lang	Tweet language information
latitude	Location latitude
longitude	Location longitude

The Users table contains the information of persons that the user is interacting with. Table 11 shows the column properties of the table.

The 0-scribe.db database contains logs and IDs in the scribe table. global.db contains the user's account information.

The shared_prefs file contains xml files. com.twitter.android_preferences.xml and 921137666602819584.xml files contain settings and options for the twitter application. /data/media/0/Android/data/com.twitter.android/cache/ stores multimedia files.

TABLE XI
TWITTER 921137666602819584-48.DB DATABASE USERS TABLE COLUMN PROPERTIES

Column name	Content
user_id	Twitter's unique id assigned to the user
username	User's unique username
name	User's name
description	Description part of user's profile
web_url	Web site added in profile
image_url	Profile image url
location	Location in profile
followers	Total followers
friends	Total number of accounts user follows
statuses	Number of tweets shared
favorites	Total number of likes user performed
media_count	Total shared media count

Secondly, it was shown how data acquisition using software tools from Twitter.

When the logical image taken with Oxygen Forensic is examined, it is seen that only access to the pictures and cache files in the folder /sdcard/Android/data/com.twitter.android/cache/ is provided. The physical image should be examined to obtain better data for the application.

When examined the physical image with the. ofb extension taken with Oxygen Forensic, the application offers several categories. Under Users, there are user names, nicknames, descriptions, locations, when created, total number of followers, total number of followers, total number of likes, total number of tweets, and user ID. Under following, only the accounts of the followed accounts are found. Under the Tweets header; tweet content, tweeting time, user name, tweet url, tweet source (which application was discarded), and whether the tweet is read. Search history under Search is given in the form of search information and search time. Under the Messages header, the user's direct message feature provides information about the one-to-one conversations. These are the direction and time information of the message. The cache header contains cached file information.

When the image taken with ddtool is examined with the 'Magnet Axiom' tool, direct messages via Twitter and Twitter friends are given under two headings. When direct messages are examined, it is seen that the tool is not display the contents of the direct messages. The message sender ID, the direction and the name of the message is displayed.

Under the 'Twitter friends' header, the user information of the tweet authors is displayed. It provides information such as the user's identity, name, account creation date, description and web url, location information, followers and number of friends, total number of tweets.

More data is available with the Oxygen Forensic tool, comparing the Oxygen Forensic and Axiom tools that extract the Twitter app data to the user. With Axiom, tweet content, search information, cache files, and cookie information are not shown. The Paraben tool is not extract Twitter application data.

VI. Results

In this study, widely used social media applications in mobile devices analyzed with popular forensic investigation softwares. Findings of different softwares are than compared to show differences in success of these softwares. Because in some cases investigators need to use different applications. After than that same applications were analyzed manually. Results were obtained by checking if the data that created by user behaviors is available or not in software output or manual method.

The results obtained revealed that the success of forensic evidence analysis software may vary depending on the application examined. This highlights the importance of manual examination when software is lacking in analysis. In addition, in cases where the software is insufficient, the findings that can be obtained by manual examination are shown in Table 12-15. Objective of this study is achieved by obtaining more evidence by manual examination. Obtained results and evidences given in this section.

A. Facebook

Application data of the Facebook and user behavior that is detected are given in Table 12.

TABLE XII
ANDROID FACEBOOK APPLICATION DATA AND USER BEHAVIOR

	Oxygen Logical	Oxygen Physical	Paraben Logical	Paraben Physical	Axiom Physical	Manual
App. Data						
Account info	-	+	-	-	-	+
Contact List	-	+	-	+	+	+
Media	-	+	-	+	+	+
Cache files	-	+	-	+	+	+
Message	-	+	-	+	+	+
Group message	-	+	-	+	+	+
Searches	-	+	-	+	+	+
File attachment	-	+	-	-	-	+
		User Behaviors				
Post	-	-	-	-	-	-
Comment	-	-	-	-	-	-
Like	-	-	-	-	-	-
Added Friend	-	+	-	+	+	+
Group sharing	-	-	-	-	-	-
Story	-	-	-	-	-	-
Message	-	+	-	+	+	+
Deleted message	-	-	-	-	-	+
Group message	-	+	-	+	+	+
Deleted group message	-	-	-	-	-	+

When the table is examined, it is seen that the data is not obtained from the logical images taken with the Paraben a nd Oxygen tools. Post, comment and like movements of user behaviors could not be determined during the analysis. Personal information of contacts, media files, cache files, messages and group messages is obtained from both physical images and manual acquisition. Deleted messages is only accessed manual acquisition.

B. WhatsApp

Application data and any detectable user behavior of WhatsApp Messenger are given in Table 13.

TABLE XIII
ANDROID WHATSAPP MESSENGER APPLICATION DATA AND USER BEHAVIOR

Data Acquisition Method	Oxygen Logical	Oxygen Physical	Paraben Logical	Paraben Physical	Axiom Physical	Manual
App. Data						
Account info	-	+	-	-	+	+
Profile pictures	-	+	-	+	+	+
Contact List	-	+	+	+	+	+
Group Information	-	+	-	+	+	+
Group Messages	-	+	-	+	+	+
People messages	-	+	-	+	+	+
Searches	-	+	-	+	+	+
Media	+	+	-	+	+	+
			User Behaviors			
Text Message	-	+	-	+	+	+
Deleted message	-	-	-	-	-	+
Send Photo	+	+	-	+	+	+
Send Location	-	+	-	+	+	+
Group text message	-	+	-	+	+	+
Deleted group text message	-	-	-	-	-	+
Group photo sharing	+	+	-	+	+	+
Blocking friends	-	-	-	-	-	-
Video call	-	+	-	+	+	+
Voice call	-	+	-	+	+	+
Status sharing	-	-	-	+	-	-

When the table is examined, it is seen that the logical image taken by Paraben is accessed the person's information, and from the logical image taken by the Oxygen tool accessed shared image. When physical images are examined, it is determined that the Paraben tool does not present the account information directly to the user unlike other tools, and the deleted messages is only accessed manual acquisition.

C. *Instagram*

Application data for Instagram and user behavior that is detected are given in Table 14.

TABLE XIV
ANDROID INSTAGRAM APPLICATION DATA AND USER BEHAVIOR

	Oxygen Logical	Oxygen Physical	Paraben Logical	Paraben Physical	Axiom Physical	Manual
App. Data						
Account info	-	+	-	+	+	+
Contacted people	-	+	-	+	+	+
Messages	-	+	-	+	+	+
Home page	-	+	-	-	-	+
Search history	-	+	-	-	-	+
Media	+	+	+	+	+	+
Cache pictures	-	+	-	+	+	+
User Behaviors						
Posts	+	+	+	+	+	+
Status	-	-	-	-	-	-
Like	-	+	-	-	-	+
Comment	-	-	-	-	-	+
Message	-	-	-	+	+	+
Canceled message	-	-	-	-	-	+
Follow	-	-	-	-	-	+
Save a post	-	-	-	-	-	-
Tag	-	+	-	-	-	+

TABLE XV
ANDROID TWITTER APPLICATION DATA AND USER BEHAVIOR

	Oxygen Logical	Oxygen Physical	Paraben Logical	Paraben Physical	Axiom Physical	Manual
App. Data						
Account info	-	+	-	-	+	+
Twitter friends	-	+	-	-	+	+
Following	-	+	-	-	-	+
Followers	-	+	-	-	-	+
Tweets	-	+	-	-	-	+
Search history	-	+	-	-	-	+
Direct message	-	+	-	-	+	+
Cache files	+	+	-	+	+	+
User Behaviors						
Tweet	-	+	-	-	-	+
Deleted tweets	-	+	-	-	-	+
Reply	-	+	-	-	-	+
Retweet	-	+	-	-	-	+
Message (DM)	-	+	-	-	+	+
Deleted message	-		-	-	-	+
Follow	-	+	-	-	+	+
Unfollowed	-	+	-	-	+	+

When the table is examined, it is seen that only the shared media is accessed from the logical images taken with the Paraben and Oxygen tools. The status post and saved post from user behavior could not be detected during the analysis. Contact information, media files, cache images and messages is obtained from physical image. Canceled messages is only accessed manually. It is seen that the user is view posts on the homepage, if they are liked by the user, and the tag search features is detected by Oxygen Forensic tool and manual search from physical images.

D. *Twitter*

Application data of the Twitter and user behavior that is detected are given in Table 15. As seen from Table 15, the cached image files of the Android device are not retrieved from Paraben. Paraben tool does not provide to the user by extracting data related to Twitter application, both in its logical and physical images. The Axiom tool only extracts contact information, account information, direct messages and cache files from the physical image to the user. All other features given in the table is accessed with both manual acquisition and the Oxygen Forensic tool.

VII. CONCLUSIONS

In the study, Oxygen Forensic, Paraben and Magnet AXIOM forensics software and manual data extraction methods were analyzed separately for Android device. As a result of the examination of devices, it is aimed to reach the behaviors of users from social media applications. The results obtained were analyzed comparatively in terms of both operating systems and software interpretation. The data that is not interpreted by the software is intended to be manually acquired.

In the examinations, it has been observed that the data which is extracted from the logical images of the device with Android operating system is not passed beyond the limited data that are kept by the application, sometimes even the users are not made available to the user, so the data is insufficient. All images related to the application is accessed from the physical images of the Android device, where physical image is taken. When the physical image is examined, the deleted data of the applications also is viewed. When the analysis of these images was carried out with the tools, it was seen that the extractable data was variable between the tools. When the contents of the application files extracted from the file system are examined manually, it is seen that more data is obtained from the data that is extracted from the tools and some of the data that are deleted as user behavior is accessed.

Compared to the methods used in the analysis, it is seen that manual data acquisition methods and Oxygen forensics are more successful than the others in view of physical image acquisition. While the files extracted from the logical image of the Android device were presented to the user in the Oxygen tool, Paraben left it to the user's own effort. When the physical images of the Android device are examined, it is seen that all three tools have access to the application data. According to the ability of the tool to extract this data and present it to the user under the title of application, Oxygen and Axiom is present the data of Facebook, WhatsApp, Instagram and Twitter applications, while the Paraben tool is not extract Twitter data from them.

REFERENCES

[1] Global digital report 2018. Retrieved 22.04.2018, from https://wearesocial.com/blog/2018/01/global-digital-report-2018

[2] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet: Academic press.

[3] Lohiya, R., John, P., & Shah, P. (2015). Survey on mobile forensics. International Journal of Computer Applications, 118(16).

[4] Jansen, W., & Ayers, R. (2007). Guidelines on cell phone forensics. NIST Special Publication, 800(101), 800-101.

[5] Lin, I.-L., Chao, H.-C., & Peng, S.-H. (2011). Research of digital evidence forensics standard operating procedure with comparison and analysis based on smart phone. Paper presented at the Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on.

[6] Murphy, C. A. (2009). Developing process for mobile device forensics. SANS Digital Forensics and Incident Response.

[7] Sadiq, M., Iqbal, M. S., Sajad, M., Naveed, K., & Malip, A. (2016). Mobile devices forensics investigation: process models and comparison. Theoretical & Applied Science(1), 164-168.

[8] Ali, A., Razak, S. A., Othman, S. H., Mohammed, A., & Saeed, F. (2017). A metamodel for mobile forensics investigation domain. PloS one, 12(4), e0176223.

[9] Hassan, M., & Pantaleon, L. (2017). An investigation into the impact of rooting android device on user data integrity. Paper presented at the Emerging Security Technologies (EST), 2017 Seventh International Conference on.

[10] Wu, S., Zhang, Y., Wang, X., Xiong, X., & Du, L. (2017). Forensic analysis of WeChat on Android smartphones. Digital Investigation, 21, 3-10.

[11] Ovens, K. M., & Morison, G. (2016). Forensic analysis of kik messenger on ios devices. Digital Investigation, 17, 40-52.

[12] Gregorio, J., Gardel, A., & Alarcos, B. (2017). Forensic analysis of telegram messenger for windows phone. Digital Investigation, 22, 88-106.

[13] Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. Digital Investigation, 11(3), 201-213.

[14] Norouzizadeh Dezfouli, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K.-K. R. (2016). Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. Australian journal of forensic sciences, 48(4), 469-488.

[15] Martini, B., & Choo, K.-K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 9(2), 71-80.

[16] Cahyani, N. D. W., Ab Rahman, N. H., Glisson, W. B., & Choo, K.-K. R. (2017). The role of mobile forensics in terrorism investigations involving the use of cloud storage service and communication apps. Mobile Networks and Applications, 22(2), 240-254.

[17] Daryabar, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K.-K. R. (2016). Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices. Australian journal of forensic sciences, 48(6), 615-642.

[18] Azfar, A., Choo, K. K. R., & Liu, L. (2017). Forensic taxonomy of Android social apps. Journal of forensic sciences, 62(2), 435-456.

[19] Bommisetty, S., Tamma, R., & Mahalik, H. (2014). Practical mobile forensics: Packt Publishing Ltd.

[20] Carrier, B. (2005). File system forensic analysis. Addison-Wesley Professional.

[21] Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. Digital Investigation, 9, S24-S33.

[22] Cohen, M., Garfinkel, S., & Schatz, B. (2009). Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow. Digital Investigation, 6, S57-S68.

[23] Kausar, F., & Alyahya, T. N. (2016). Analysis of Physical Image Acquisition Forensic Tools for Android Smartphones. International Journal of Computer Science and Network Security (IJCSNS), 16(11), 38.

[24] Aquila, I., Sacco, M., Gratteri, S., Sirianni, M., De Fazio, P., & Ricci, P. (2017). The “Social-Mobile Autopsy”: The Evolution of Psychological Autopsy with New Technologies in Forensic Investigations on Suicide. Legal Medicine.

[25] Ogazi-Onyemaechi, B. C., Dehghantanha, A., & Choo, K.-K. (2017). Performance of android forensics data recovery tools Contemporary Digital Forensic Investigations of Cloud and Mobile Applications (pp. 91-110): Elsevier.

[26] Quick, D., & Choo, K.-K. R. (2017). Pervasive social networking forensics: intelligence and evidence from mobile device extracts. Journal of Network and Computer Applications, 86, 24-33.

[27] AKBAL, E., DOĞAN, Ş., & BALOĞLU, İ. Android İşletim Sisteminde WhatsApp Uygulamasının Adli Bilişim Açısından İncelenmesi. Bilişim Teknolojileri Dergisi, 11(2), 147-156.

[28] Akbal, E., Baloglu, I., Tuncer, T., & Dogan, S. (2019). Forensic analysis of BiP Messenger on android smartphones. Australian Journal of Forensic Sciences, 1-20.

[29] Larbi, S., AKHROUF, S., BOUBERIMA, F., IMENE, F., & DJAMEL, B. Behavior Analysis of users on Facebook.

BIOGRAPHIES

FATMA GÜNEŞ ERİŞ Trabzon, in 1989. She received the B.S. degrees in computer engineering from the University of Kocaeli, Kocaeli, in 2013, the M.S. degrees in computer engineering from the University of Fırat, Elazığ, in 2018. She is still Ph.D. student in University of Fırat. From 2013 to 2015, she was a Research Assistant in Univertsity of Ardahan. Since 2015, she has been Research assistant in Digital Forensics Engineering department from the Univertsity of Fırat. Her research interests include mobile forensics, network securtiy, machine learning.

Erhan AKBAL was born in Elazig, Turkey, in 1981. He received bachelor's, master's degrees in computer engineering and Ph.D degrees in electrical and electronics engineering from Firat University in Turkey. He has worked as Associate Professor at the Department of Digital Forensics Engineering at Firat University. His research interests include pattern recognition, mobile forensics, network security, and information security.