Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi

Pamukkale University Journal of Engineering Sciences

Rating of the relationship between users using the data from the implemented mobile forensic software

Mobil adli bilişim yazılımı geliştirilerek elde edilen veriler ile kullanıcılar arası ilişkilerin derecelendirilmesi

Faruk Süleyman BERBER[1*], *Ecir Uğur KUCUKSILLE*[2]

[1]Department of Informatics, Rectorate, Süleyman Demirel University, Isparta, Turkey.
farukberber@sdu.edu.tr

[2]Department of Computer Engineering, Engineering Faculty, Süleyman Demirel University, Isparta, Turkey.
ecirkucuksille@sdu.edu.tr

Received/Geliş Tarihi: 08.01.2019 Revision/Düzeltme Tarihi: 27.04.2019 doi: 10.5505/pajes.2019.29599
Accepted/Kabul Tarihi: 27.05.2019 Research Article/Araştırma Makalesi

Abstract

During the digital forensic process, different software and hardware tools are used. The devices from which the digital evidences are collected have been varied in parallel with the developments in technology. The issue of identifying the mobile phone owner's friends and assessing his relationship with them with the help of digital evidences collected from the Android mobile phones has been studied in the literature and it is still under investigation. The software developed in this work enables accessing a variety of data that have evidential value in the court proceedings; these include physical and logical acquisition of images from mobile phones with Android operating system, extracting images for investigations, examining different file types in images, and databases. This software can collect and examine the evidences and then produce reports. At the same time, it can identify criminals or people with potentially have connections to those people whose accounts are under investigations by using developed analysis model which examines the relationships between social media applications` data, phone contacts and calling histories collected from the mobile devices. In this work, the evidences examined by using a novel software developed by the authors which performs multiple tasks using a single interface and the corresponding results are presented.

Keywords: Forensic science, Digital forensics, Mobile forensics, Digital evidence analysis, Fuzzy model.

Öz

Adli bilişim sürecinde çok çeşitli yazılımlar ve donanımlar kullanılmaktadır. Teknolojinin hızlı gelişimine paralel olarak dijital delillerin toplandığı cihazlar da hızla çeşitlenmektedir. Android mobil telefonlardan toplanan dijital deliller yardımı ile bu telefona sahip kişinin arkadaşlarının ve bu arkadaşları ile ilişkilerinin derecelendirilerek tespit edilmesi, literatürde çalışılmış ve üzerinde çalışılmaya devam eden konulardan biridir. Bu çalışmada geliştirilen yazılım, Android işletim sistemine sahip mobil cihazlardan fiziksel ve mantıksal imaj alma, imajın incelenmek üzere açılması, imaj içinde farklı dosya türlerinin incelenmesi, veri tabanı incelemeleri gibi dijital delil niteliği taşıyan birçok veriye erişilmesini sağlamaktadır. Delil elde etme, delilleri inceleme ve raporlama işlemlerini yapabilen bu yazılım aynı zamanda geliştirilen analiz modeliyle mobil cihazlardan elde edilen sosyal medya uygulama verileri, telefon rehberi ve görüşme kayıtları arasındaki ilişkileri inceleyerek suçlunun veya hesapları incelenen kişilerin, ilişkili olma ihtimali yüksek kişileri tespit edebilmektedir. Birçok işlemi tek bir ara yüzden yapabilmesi ve veri analiz yöntemi bakımından, özgün bir çalışma olarak gerçekleştirilen yazılımla incelenen deliller ve elde edilen bulgular bu çalışmada sunulmuştur.

Anahtar kelimeler: Adli bilimler, Adli bilişim, Mobil adli bilişim, Sayısal delil inceleme, Bulanık model.

1 Introduction

Digital forensic is defined as a whole process of identifying, collecting, preserving, and analysing the data obtained from a sound, image, text, or any combination of them, which are stored in or transmitted in electromagnetic and electrooptical mediums, to be presented as digital evidences in the court [1].

In digital forensic, the digital forensic process is followed to convert the digital evidences to admissible evidences that can be used in courts. This process is defined as digital forensic investigation phase and after this process the digital evidences are converted to admissible evidences. Digital forensic processes can be divided into 4 main sections. These are acquisition or collection, identification or examination, evaluation or analysis, presentation or reporting [2].

When digital forensic becoming known, it was defined as computer forensics. However, depending to developments in technology, the profile of cybercriminals has changed and the number of cyber-attacks has been increased. As a result, different digital forensics investigation has been caused new terms as network forensics, disk forensics, memory forensics and mobile forensics.

Nowadays, mobile devices have been widely used. Therefore in many digital forensic cases it is necessary to use the evidences collected from the mobile devices to enlighten the cases.

Mobile devices with Android operating system are suitable for such forensic cases since increase in the applications for Android devices has revolutionised our life. These devices have been parts of our daily life therefore they include massive personal data (e.g., instant texting applications). In addition to processing these data, it is highly possible to capture the marks of these data in the local memory.

The most crucial and critical stage is to collect the data in an investigation. An expert has to extract the data in a forensically sound way (without damaging the data) using the most

[*]Corresponding author/Yazışılan Yazar

appropriate technique before analysing them [3]. At this stage, there is a need for digital forensic software tools.

In this work, A software has been developed that takes an image from the devices with Android operating system, opens the image and analyzes the different file types within it. These analyzes are carried out using a fuzzy model developed in the study and a new analysis method which is not in mobile forensics software. Thus, the software estimates the persons who are closely associated with the device user or are likely to be intimate.

The mobile forensic software developed in this work enables acquiring images, analysing different files in the images, and investigating databases and accessing many kinds of data from the devices with Android operation systems that can be used as admissible evidences. The software developed in this work performs multiple works using a single interface therefore it provides more advantages over the existing mobile forensic software tools. Especially, the novelty in this software includes analysing the person or the criminal whose device is under the investigation and the related people. The developed software has the ability to root the mobile devices and acquire the physical images using the exploit method. Although, the software tool has some limitations in the rooting and acquiring the data due to variety of Android mobile devices and also frequent software and hardware updates, this work presents different and novel results compared to the results obtained from the existing mobile forensics software tools.

2 Related works

Grover developed a prototype enterprise monitoring system for Android smartphones. The developed software enabled transferring the data sets which are of interest to many investigators including the forensic investigators from mobile phones to a web server. It was stated that the software can collect data sets that are not found in other available software tools [4].

Scrivens and Lin discussed the methods that are used to acquire information from an Android device for digital forensic investigations and explained their pros and cons. Moreover, they provided information on which data to access and from where after collecting the data. They also demonstrated an example analysis on Facebook Messenger and Google Hangouts [3].

Due to increases in the use of mobile devices and wide spread usage of social media and messaging applications, there has been a strong interest to use data obtained from social media applications in mobile devices for digital forensics investigations. Especially, many works have been done on Whatsapp Messenger [5]-[7]. Telegram [7]-[9], Facebook, Twitter, Instagram [10]-[13] and there are still many ongoing works.

In order to identify the related persons and the relationship between those people by using data stored in the mobile devices collected under the forensic process some works have been performed.

Choi and Lee proposed a method which calculates relation points of people and hence presents the degree of relationships between them using the data collected on calls, sms/mms (KakaoTalk, Viber, Skype, MyPeople, NaverLine, NateOnUC, Joyn), sns (Twitter, Facebook), cloud (Dropbox, uCloud), memo (Evernote, AwesomeNote), schedule (Jorte), map (Daum map, Naver map) and document viewer (AdobeReader, ezPDFViewer, HancomViewer, GoodReader, PolarisOffice). However, in their work, only the information on the number of calls, their durations, and the number of messages was used [14].

Anvar and Abulaish presented a unified social graph-based text mining framework to identify digital evidences from chat logs data. Their proposed framework considers both users' conversation and interaction data in group-chats to discover overlapping users' interests and their social ties [15].

Akbas et al., proposed a friends ranking algorithm which assigns weights to the durations of the calls, video conferences, face-to-face meetings and the sizes of the emails and texts and then depending on the value it finds the friendship levels [16].

Alzaabi et al., proposed a forensic analysis system called CISRI that helps forensic investigators to determine the most influential members of a criminal group using the email exchanges and text messages for the purposes of investigation. It was stated that the proposed system can describe the structural relationships between the members of a criminal group in terms of a graph [17].

Reinhardt et al., utilized a data set including contact names, calls, sms, mms, and emails on personal smartphones to classify users into social relationship categories (acquaintances, work, family, friends, school/university). They used SVM (Support Vector Machine), C4.5 and Naive Bayes algorithms to classify the users and showed that SVM provides the best results [18].

In digital forensic area, there are also some works produced by applying fuzzy logic method.

Barmpatsalou et al., proposed a fuzzy system based suspicious pattern detection in mobile forensic evidences [19].

Stoffel et al., proposed a methodology based on the fuzzy set theory and an automatic procedure for inferring accurate and easily understandable expert-system-like rules from forensic data [20].

Rostamipour and Sadeghiyan proposed a forensic expert system based on fuzzy logic, which is able to automatically detect the origin of attack in single and multi-stage attacks. It was stated that the proposed system is able to indicate the time, origin and scenario of the attack [21].

Liao et al., proposed an approach based on fuzzy logic and expert system for network forensics that can analyse computer crimes in network environment and make digital evidences automatically [22].

3 Mobile forensics

With the development of the mobile device technologies, our daily works and activities can be done in mobile environment. People who use mobile devices can do many of their daily works easier, more cost effective and quicker than those who do not use mobile devices. In the mobile devices, all processed data can be stored in or deleted from the storage media. The possibility of recovering data from these storage areas, the fact that these data are digital evidence and that they are valid in judicial evidence examination processes has brought the concept of mobile forensics to the literature.

Nowadays, there are many software and/or hardware tools used in the mobile forensics area. Almost every day, new tools have been added to these existing tools or the existing tools have been updated by adding new features. Therefore, the evidence collection and analysing phases can be performed in more detail and quicker.

Smartphones used in our daily life contain immense data that can be used as digital evidences in the forensic examination process of mobile devices. These data can be collected by copying and/or investigating the sim cards, operating systems and RAMs of the devices. Investigation in the operating systems also covers the investigation of storage disks of devices therefore it is possible to recover many evidences that can be used to enlighten cases.

4 Non-structural fuzzy decision support system and fuzzy vikor methods

In this work, Non-structural Fuzzy Decision Support System (NSFDSS) developed by Chen [23] and Fuzzy Vikor method [24] were investigated since these theories have been used and accepted in the defining and development stages of the fuzzy method. According to the NSFDSS method developed in 1998, main criteria are dived into sub-branches in order to solve the problem. The problem convergences to a solution if the number of criteria under each sub-branch increases. In this method, simple combinations are used. Using the combinations, a value that shows how much each subcriteria affects the other criteria is calculated. Furthermore, depending on the effect of all subcriteria on the solution of the problem, criteria may be tested and removed from the solution.

The Fuzzy Vikor method is used to help decision makers to solve decision problems with conflicting and noncommensurable (different units) criteria therefore in this work the Fuzzy Vikor method was implemented. Although, Twitter data, Whatsapp data or contact information cannot be enough to make a sensible decision when they are used as separate criteria but when they are evaluated together as a solution equation the problem can convergence to a solution.

5 Mobile forensic software tool development process

In Linux systems, the root account has administrative rights thus it can access all commands and files on the operating systems. As Android operating system is used Linux kernel, the same administrative rights of the root are valid in the Android systems. In the mobile devices, the manufacturers disable the root settings for the uses in order to prevent them to get full control on the devices. Users with no root access cannot make any changes on the systems of the devices however users with root access can make any changes and control everything on the devices. Android root tools show differences depending on the platforms used. In this work, specifically, the root tools for mobile devices have been investigated. Different methods have been chosen to root the smartphones with Android operating system. Some of these methods can be very simple however some of them can be very complex. The easiest way of rooting a device is to use a tool that automatically enables rooting. These cloud-based tools scan the devices and find the best way to enable rooting and then the process is performed by using a brute-force attack method. The difficult process is to flash a custom recovery and install an up-to-date SuperSU. There are commercially available tools that can make these processes easier such as; Kingroot, Cf auto root, One click root, Towelroot and Rescue root.

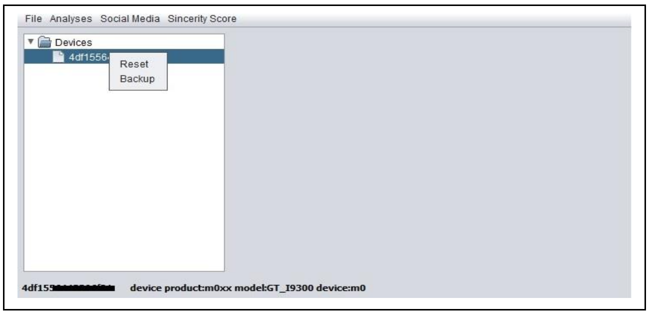
In this work, many rooting tools developed for mobile devices have been investigated and a root module that implements an exploit method was developed and embedded in the developed software tool.

The developed software enables acquisition of logical and physical images from rooted devices however it only acquires logical images from devices without rooting.

By using the developed software, it is possible to analyse the files inside obtained images and databases. Also, it is possible to make analysis on the images obtained from different software tools.

In this work, the Mobile forensic software tool was developed by using Java programming language.

Figure 1 shows a screenshot of the developed software tool. As seen that it has a very simple interface. First, Android devices connected to the computer are identified by the software and then these are listed in the "Devices" section. When the code that belongs to the processed device is selected, information about the selected device is present at the bottom of the interface. Moreover, when device selected in the list, "Reset" (used to restart the device) and "Backup" (used to get images) options will appear.



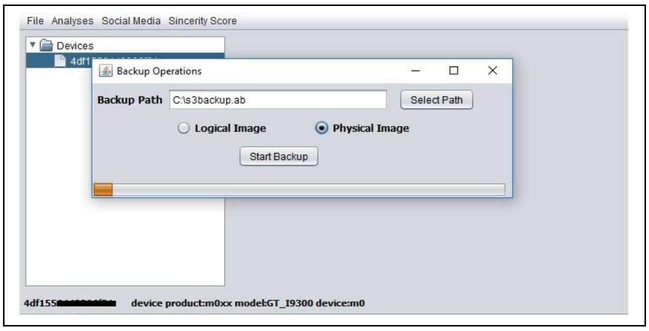
4df155[redacted] device product:m0xx model:GT_I9300 device:m0

Figure 1. Screenshot from the developed software tool.

It is also possible to extract the images obtained from mobile devices in any folder desired by using "Open Backup" option under "File" tab. "Analyses" tab includes sub-tabs which enable examinations on the files required for analysing the evidences and the database files in the extracted image file.

5.1 Image acquisition process

To start image acquisition process, it is selected from "Devices" section and then "Backup" option is enabled. As seen in Figure 2, a backup path and the acquisition type (whether logical or physical) are defined and then the backup process is started.



Backup Path C:\s3backup.ab

○ Logical Image ● Physical Image

4df155[redacted] device product:m0xx model:GT_I9300 device:m0

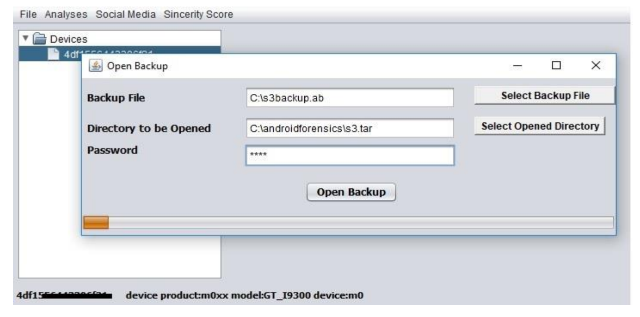
Figure 2. Backup interface.

The main code used to backup files in a selected folder is as follows;

```
adb.exe backup -apk -shared -all -system -f+" "+path
```

5.2 Extracting image files

The images obtained by the developed software are extracted by using a "Open Backup" option under "File" tab as seen in Figure 3.



Backup File: C:\s3backup.ab
Directory to be Opened: C:\androidforensics\s3.tar
Password: ****

4df15[redacted] device product:m0xx model:GT_I9300 device:m0

Figure 3. Interface for extracting backup.

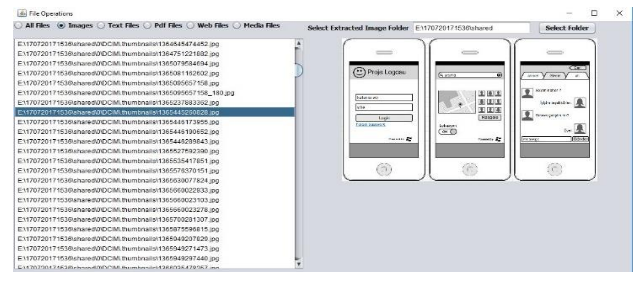
In order to extract the image files into the selected folder the following codes were used;

```
java -jar abe.jar unpack" + " " + bkpFileName +" " + openDrcName + " " + password
```

```
7z.exe x" + " " + openDrcName + " " + "-o" + resultString +" " + "-aoa"
```

5.3 Analysis depending on the file types

For forensic analysis on the extracted files for the examinations of the evidences, a "File Operations" option under "Analyses" is selected. The analysis is performed over primarily defined 5 different file types. Figure 4 shows the interface which enables examination of the evidences depending on the file types.



Select Extracted Image Folder: E:\170720171536\shared

```
E:\170720171536\shared\0\DCIM\.thumbnails\1364645474452.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1364751221882.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365079584694.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365081182602.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365095657158.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365095657158_180.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365237883352.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365445260828.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365446173955.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365446190652.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365446289843.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365527592390.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365535417851.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365578370151.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365630077824.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365660022933.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365660023103.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365660023278.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365700281307.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365875596815.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365949207829.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365949271473.jpg
E:\170720171536\shared\0\DCIM\.thumbnails\1365949297440.jpg
```

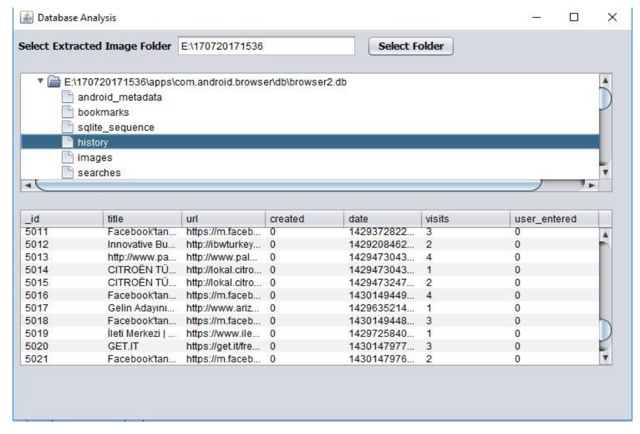
Figure 4. Screenshot from the interface for analysing different file types.

5.4 Database analysing process

An additional module was also developed in order to process the data on the database files which are the one of the most important parts in the forensic analysis since they contain the programmes` recordings, browsing history, search results etc. With the use of this developed module, first of all database files in the image are found, listed and then analysed automatically.

Figure 5 shows an example from the database analysis module which can access many databases for the examination of the evidences. In the module developed for analysis, some of these databases were selected and the analysis was performed by using the relationships between the data obtained from these databases.

The databases, their addresses (url) and contents are summarised as seen in Table 1.



Select Extracted Image Folder: E:\170720171536

E:\170720171536\apps\com.android.browser\db\browser2.db
- android_metadata
- bookmarks
- sqlite_sequence
- history
- images
- searches

_id	title	url	created	date	visits	user_entered
5011	Facebook'tan...	https://m.faceb...	0	1429372822...	3	0
5012	Innovative Bu...	http://ibwturkey...	0	1429208462...	2	0
5013	http://www.pa...	http://www.pal...	0	1429473043...	4	0
5014	CITROËN TÜ...	http://lokal.citro...	0	1429473043...	1	0
5015	CITROËN TÜ...	http://lokal.citro...	0	1429473247...	2	0
5016	Facebook'tan...	https://m.faceb...	0	1430149449...	4	0
5017	Gelin Adayını...	http://www.ariz...	0	1429635214...	1	0
5018	Facebook'tan...	https://m.faceb...	0	1430149448...	3	0
5019	İleti Merkezi | ...	https://www.ile...	0	1429725840...	1	0
5020	GET.IT	https://get.it/fre...	0	1430147977...	3	0
5021	Facebook'tan...	https://m.faceb...	0	1430147976...	2	0

Figure 5. Screenshot from the database files analysing interface.

Table 1. The databases, their addresses (url) and contents.

Database file name	Addresses (url)	Contents
contacts2.db	android.providers.contacts/databases/	Information on phone contacts
contacts2.db	com.facebook.orca/and com.facebook.katana/	Information on the users registered to Facebook
wa.db	com.whatsapp.databases/	Information on the users registered to Whatsapp

5.5 Acquisition of social media data sets and analysing process

In order to obtain social media data, the social media account details of the user were acquired as raw data from the analysis of images and databases. Before estimating possible linked users to the user under investigation, the user`s followers and following were listed. Later, using the obtained data, data for the followers and following of the user`s followers and following were acquired. Using the user social media data and all other data obtained from the databases in the user`s device were analysed by using a developed statistical model and then the users who have potentially close links with the user under investigation were listed with a score.

5.6 Software development for obtaining a list with the followers and following of the criminal by using social media data

A web software which implements the user`s Twitter name and systematically saves the data acquired from the account with the help from Twitter api, was developed in php programming language and then the software was embedded in the mobile forensic software tool. To get the social media data for the user account under investigation, in the mobile forensic software tool, select the "Social Media" tab and then select "Get Twitter Data" option. Figure 6 shows the web interface.

From Table 2 to Table 7 shows the main structure of the mysql database used in the web software.

The developed software first saves the followers and the following of the user account under investigation in the database. Later, the software saves followers of followers, followers of following, following of followers and following of following of the user account under investigation in the database.

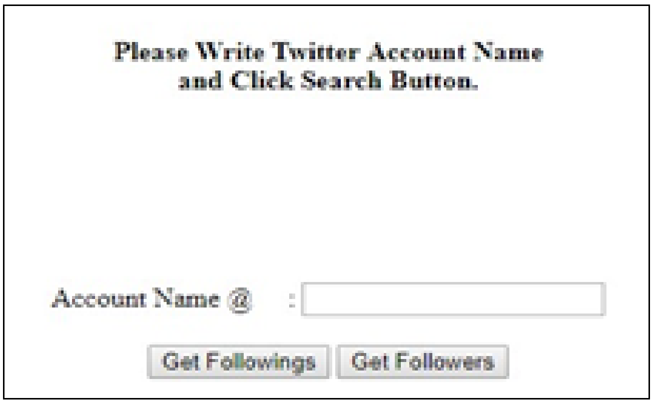

Please Write Twitter Account Name and Click Search Button.

Figure 6. Web interface.

Table 2. The follower account informations of main user.

Table name : Mainfwers		
Field name	Data type	Explanation
mainac	varchar(50)	Main user account
mainacfwer	varchar(50)	Follower account of main user
mainacfwername	varchar(50)	Follower account name of main user
mainacfwerloc	varchar(50)	Follower account location information of main user

Table 3. Informations of main user's following accounts.

Table name: Mainfwing		
Field name	Data type	Explanation
mainac	varchar(50)	Main user account
mainacfwing	varchar(50)	Main user's following accounts
mainacfwingname	varchar(50)	Main user's following accounts name
mainacfwingloc	varchar(50)	Main user's following accounts location information

Table 4. Informations of follower account of main user's following accounts.

Table name : Mainfwing2fwer		
Field name	Data type	Explanation
mainac	varchar(50)	Main user account
mainacfwing	varchar(50)	Main user's following accounts
mainacfwing2fwer	varchar(50)	Follower account of main user's following accounts
mainacfwing2fwername	varchar(50)	Follower account name of main user's following accounts
mainacfwing2fwerloc	varchar(50)	Follower account location information of main user's following accounts

Table 5. Informations of main user's following account's following account.

Table name : Mainfwing2fwing		
Field name	Data type	Explanation
mainac	varchar(50)	Main user account
mainacfwing	varchar(50)	Main user's following accounts
mainacfwing2fwing	varchar(50)	Main user's following account's following account
mainacfwing2fwingname	varchar(50)	Main user's following account's following account name
mainacfwing2fwingloc	varchar(50)	Main user's following account's following account location information

Table 6. Follower account informations of follower account of main user.

Table name : Mainfwers3fwer		
Field name	Data type	Explanation
mainac	varchar(50)	Main user account
mainacfwer	varchar(50)	Follower account of main user
mainacfwer3fwer	varchar(50)	Follower account of follower account of main user
mainacfwer3fwername	varchar(50)	Follower account name of follower account of main user
mainacfwer3fwerloc	varchar(50)	Follower account location information of follower account of main user

5.7 An algorithm for predicting the possible users with closely related to the criminal

Up to now, from the analysis on the mobile device and on the social media accounts of the user; the follower, following, the number of followers and following saved in the phone contacts, the frequencies of the calls with the contacts, interactions with these contacts on the Facebook and availabilities of these contacts on Whatsapp were obtained.

Table 7. Following account informations of main user's followers account informations.

Table name : Mainfwers3fwing		
Field name	Data type	Explanation
mainac	varchar(50)	Main user account
mainacfwer	varchar(50)	Follower account of main user
mainacfwer3fwing	varchar(50)	Following account informations of main user's followers account informations.
mainacfwer3fwingname	varchar(50)	Follower account of main user's following account name
mainacfwer3fwingloc	varchar(50)	Follower account of main user's following account location information

The sincerity criteria (Facebook, Whatsapp, calling and mutual friend criteria) between 3400 different people obtained in this work and analysed, the generated results seemed quite consistent (close). This shows that the Fuzzy Vikor method is very suitable for computing the sincerity scores. The sincerity score can vary severely if the new parameters are added to the data set, e.g., if a user does not need to call a person who is with him almost every day or they can share the same social media accounts. In this case there would be significant differences in the sincerity score, i.e., even the sincerity score can be increased too much therefore the sincerity scores with other uses would be meaningless. Such issues make the problem fuzzy.

The problem analysed in this work can be considered as a decision making based on multiple scores as defined in VICOR and NSFDSS in 1998 and 2007 respectively. However, in this work, to solve the problem, a different approach has been followed from the existing methods when calculating the scores. The solution consists of two main sections; defining the decision-making criteria and making decision with the optimal solution.

5.7.1 Defining the decision-making criteria

The algorithm and the software have been developed with the aim to use it in the process of decision-making based on the sincerity analysis on the suspects or victims. In the developed decision-making process, the primary aim is to find someone who has been contacted the most and the less but may know the user well by correlating the data obtained from the user`s device and other data the user left on the internet on the public sites.

It may not always be possible to perform the sincerity analysis reliable in the decision-making criteria. The reasons depend on many factors such as the user`s reactions on the different events, environment, tendency to use technology, lack of communications in the social media with frequently seen users, etc. The proposed algorithm has an ability to draw a pattern with the use of the data obtained from the users. Formed criteria can be defined as information collected from Twitter, Whatsapp, Phones`s contacts, and Facebook.

A pattern can be detected on the user under investigation using the data obtained from Twitter. In Twitter, the users are most likely follow the people they are interested and want to know more about them. If they follow each other, in this case it is assumed that these users obtain digital information from each other. Even though this variable may not make any sense when is used its own, cross searching on followers of followers, followers of following, following of followers and following of following can provide some clues on the sincerity of each user to the user under investigation. Twitter has more options on sharing information publicly compared to the other social media platforms. This is one of the most important variable used to estimate the uses who have close relationships with the examined user.

The parameters evaluated by using the data obtained from Twitter are defined as follows;

Z_1=the number of mutual followers of followers,

Z_2=the number of mutual following of followers,

Z_3=the number of mutual followers of following,

Z_4= the number of mutual following of following.

Every data obtained from a subcriteria is used as a dependent variable in the other. For example, followers of a user can have the same reason to follow him. Similarly, comparing the data obtained from Z_2, Z_3, Z_4 can be used as criteria even though there is no data in the devices of the users similar to the user under investigation. In this way, it would be possible to determine users who have similar attitudes but they do not follow each other in the digital environment. Furthermore, followers and following of the user are evaluated as separate coefficients. This criterion is defined such that it adds 0.2 to the general score if they follow each other; checking the scores coming from Z_1, Z_2, Z_3, Z_4 criteria, it adds 0.2 to the user with the highest score and adds a suitable weighted coefficient to the other users.

The data obtained from Whatsapp also provides one of the most important criteria used in this work since Whatsapp is one of the most widely used personal messaging application in the mobile devices. Whatsapp provides important information about the users since it is free, users can share files free of charge anywhere they can access the internet, share their location information etc. The data obtained from Whatsapp cannot be used to evaluate the degree of sincerity or relationship itself but when it is cross-evaluated with the data obtained from other applications then it can provide an added value to the solution as an auxiliary criterion. If the users are saved on the contact list on the Whatsapp, this adds 0.2 to the score.

The data obtained from the contact include saved contacts and the number of calls these are the most important variables that can be acquired off-line from mobile devices. From the number of calls, the contribution of the most called person to the sincerity score is evaluated as 1 which is the maximum value and the other numbers of calls are implemented to all people in the contact in proportion to 1. In the contact criteria, being in the contact list adds 0.1 to the total sincerity score and the most called person is evaluated as 0.1 score.

When considering the data obtained from Facebook, the information on being friends on Facebook is evaluated as 0.2

score. In Facebook`s evaluation criteria, different variables can be added such as messages, location information and being including on the photos etc but in this work only being in the friend list was considered and evaluated.

Equation 1 formulises the model developed for the fuzzy score system explained in detail above. The parameter X_{1ort}, which is required to calculate X_1, is calculated by using Equation 2.

$$S = \sum_{i=1}^{4} X_i * 0.2 + \sum_{J=1}^{2} Y_j * 0.1 \; (1)$$

In the above equation, the parameters are defined as follows;

$X_1 = twittersincerity coefficient\left(X_{1ort}/X_{ort[max]}\right)$

$(between\ 0-1)$

$X_{1ort} = twittermean of the number of mutual friends$

$X_{ort[max]} = twittermaximum of the mean of the number$

$of mutual friends$

$X_2 = mutual following(0 or 1)$

$X_3 = whatsapp(0 or 1)$

$X_4 = facebook(0 or 1)$

$Y_1 = contact(0 or 1)$

$Y_2 = calling weight(between\ 0-1)$

$S = Relationship/degree of the sincerity\ (between\ 0-1)$

$$X_{1ort} = \frac{1}{4}\sum_{i=1}^{4} Z_i (2)$$

In the above equation, the parameters are defined as follows;

$Z_i = the number of mutual friends$

$Z_1 = the number of mutual followers of followers$

$Z_2 = the number of mutual following of followers$

$Z_3 = the number of mutual followers of following$

$Z_4 = the number of mutual following of following$

$X_{1ort} = twitter the mean of the mutual friends$

When the common characteristics of the criteria clearly stated in equations are analysed;

- ✓ Every single criterion considered in the evaluation process has a characteristic of being cross-checked with the publicly available data.
- ✓ Every criterion in their own scoring system is scored based on the frequency of computation.
- ✓ As every criterion can be used as its own, this situation can differ depending on the person in terms of coefficient. Therefore, it is clearly seen that in this work, the criteria are divided into the equal coefficients.

When calculating the sincerity score using the criteria defined in this work, the most used platforms and applications were considered. Furthermore, in future it is possible to add new applications to the algorithm in order to increase the number of criteria required for new works or different parameters can be added in the criteria in order to get better results.

5.7.2 Making decision with the optimum convergence approach

One of the most important feature of the developed algorithm which was developed to help the decision makers and investigators to make the decision based on scientifically analysed digital data is that it correlates different applications. Sometimes it is not very possible to directly find the user who has the closest relationship with the user under investigation or this information is not enough.

The algorithm was designed such that it processes the acquired digital data quickly and reaches the defined goals. Thus, it enables reaching the critical points quickly during the decision-making process.

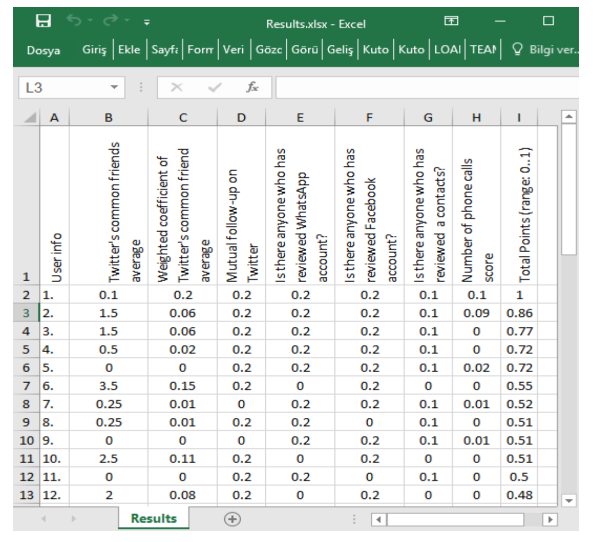
Considering these issues, the pattern generated by the algorithm developed here provides an important step for using information technologies for decision-making process. In forensic investigations, although it is aimed to reach a result within a short time, sometimes it is not possible to analyse the data and find the suspects within such a short time limit.

Taking into account the complexity of the problems, using the algorithm developed in fuzzy structure and its patterns enable making decision quickly and efficiently.

The developed algorithm allows adding new criteria to the system when the data obtained from the mobile devices increases and changes.

“The software for predicting the people in close relation with the criminal” which implements the algorithm defined above starts working by selecting the “Sincerity Score” tab on the main menu of the mobile forensic software and then selecting the “Calculate” option.

The developed software module lists the people who have close relationship with the user under investigation with a score value after “Sincerity Score” is selected and then it reports this list as an excel file as seen in Figure 7.



	A	B	C	D	E	F	G	H	I
1	User info	Twitter's common friends average	Weighted coefficient of Twitter's common friend average	Mutual follow-up on Twitter	Is there anyone who has reviewed WhatsApp account?	Is there anyone who has reviewed Facebook account?	Is there anyone who has reviewed a contacts?	Number of phone calls score	Total Points (range: 0..1)
2	1.	0.1	0.2	0.2	0.2	0.2	0.1	0.1	1
3	2.	1.5	0.06	0.2	0.2	0.2	0.1	0.09	0.86
4	3.	1.5	0.06	0.2	0.2	0.2	0.1	0	0.77
5	4.	0.5	0.02	0.2	0.2	0.2	0.1	0	0.72
6	5.	0	0	0.2	0.2	0.2	0.1	0.02	0.72
7	6.	3.5	0.15	0.2	0	0.2	0	0	0.55
8	7.	0.25	0.01	0	0.2	0.2	0.1	0.01	0.52
9	8.	0.25	0.01	0.2	0.2	0	0.1	0	0.51
10	9.	0	0	0	0.2	0.2	0.1	0.01	0.51
11	10.	2.5	0.11	0.2	0	0.2	0	0	0.51
12	11.	0	0	0.2	0.2	0	0.1	0	0.5
13	12.	2	0.08	0.2	0	0.2	0	0	0.48

Figure 7. Excel list with scores of users.

In the development of this software module, the Python was used due to its advanced library supports.

6 Conclusions

In this work, first a software which acquires physical and logical images from mobile devices and then analyses the data was developed. Next, an algorithm that lists the people in close relation with the user under investigation was developed and then embedded in the main software tool.

This work was performed over three different mobile devices with Android operating system since it takes very long time to acquire images from mobile devices and also it is hard to find sample image sets.

The results for contacts and social media data analysing obtained from the examination of images that acquired from mobile devices by using the developed software tool can be seen in Table 8.

Table 9 shows some sample data generated by analysing the evidences depending on the file types option in the developed software.

Table 10 shows some data obtained from examinations of evidences from database files by using the developed software tool.

Table 11 shows the results on the analysis performed over the data obtained from a Samsung Galaxy S3 using the developed software named as the software for predicting the people in close relation with the criminal.

As seen in Table 11. the mean of the mutual friends value of the first user is 4.75 (as the first user has the highest number of mutual friends it gets the highest score from Twitter). The first user has a sincerity score of 1 and if this value is multiplied by the score of 0.2 for Twitter then the weighted coefficient of the mean of the mutual friends on Twitter is obtained as 0.2. Since the user under investigation and the first user follow each other on Twitter, the mutual follow up score is 0.2. They are friend on Whatsapp and Facebook therefore the first user gets 0.2 score for each criterion. Furthermore, the first user gets 0.1 for being included in the phone contacts of the user under investigation and having the highest number of phone calls with him amongst the all users. Eventually, the first user got 0.2 score from each of 4 parameters (criteria) and 0.2 score from each of 2 parameters so that in total the first user reaches the maximum total value of 1 and hence becomes the one who has the closest relationship with the user under investigation.

Table 8. Data from mobile device (phone contacts and social media).

Device information examined	Number of contacts registered in the Contacts (including 1 more than 1 person's record-not unique)/Qty	Number of friends on Facebook/Qty	Number of contacts on Whatsapp/Qty	Number of accounts followed on Twitter/Qty	Number of Twitter followers /Qty
Samsung Galaxy S3	433	460	418	73	39
Samsung Galaxy Grand Neo	207	119	154	150	79
Samsung Galaxy Note 4	506	510	387	122	37

Table 9. Sample data for the analysis depending on the file types.

Extension of the file	Source of the file	Time the file was created	Time the file was modified	Software or platform in which the file was created
.jpg	GT-I9300	2015-06-19T21:33:30	2015-06-19T21:33:30	I9300XXUGNG3
.jpg	GT-I9300	2015-07-06T23:01:16	2015-07-06T23:01:16	I9300XXUGNG3
.jpg	Facebook	-	May 13 23:08:06 +03:00 2018	-
.jpg	Email	2014-05-26T14:05:19	2014-05-26T11:05:19+03:00	Adobe Photoshop CC
.jpg	Messenger	2014-07-12T04:29:23	2014-07-12T04:29:23	Apple Computer, Inc. User
.pdf	Web	2013-12-19T13:53	2013-12-19T13:53:50	Microsoft Reporting Services 11.0.0.0
.pdf	Web	2008-09-10T11:52:55	2011-02-22T08:13:09	Acrobat Distiller 7.0.5 (Windows)

Table 10. Sample data from the database analysis.

Database name	Data content information	URL or source of address information
browser2.db	User login information	http://uzak.sdu.edu.tr/akademik50/ASPX/Common/login_input.aspx
	Coding theory unit becomes compulsory for primary schools	http://m.hurriyet.com.tr/Haber?id=28636849
	Shocking explanation on Cola - yenisafak.com.tr	http://www.yenisafak.com.tr/hayat/soke-eden-kola-aciklamasi-2117419
	Smartphone, Samsung	http://www.hepsiburada.com/m/samsung-cep-telefonu-smartphone-c-60002330?filtre=[{%22id%22:%22284_dp%22,%22values%22:[%221620megapixel%22]}]#offset=288
	Men shoes models | Onudabunuda.com	http://m.onudabunuda.com/erkek-ayakkabi-modelleri/?&page=2
	Election song of MHP is 'Devlet Baba' – Political videos	http://www.haberturk.com/video/haber/izle/mhpden-secim-sarkisi-mhp-secim-muzikleri-mhp-2015-secim-muzikleri/138785
	How to boil eggs | Classics taste	http://www.klasiktatlar.com/yumurta-nasil-haslanir-1616.html
mmssms.db	250 MB gift offer for mobile started. Your allowance will end after 30 days. Unused allowance cannot be transferred to the next month. If internet usage exceeds 250 MB then the speed of the internet reduces to 5kbps. For more information www.turkcell.com.tr	Turkcell
	3 instalments for clothe shopping 100 TL and over! In the Paraf shops +4 instalments and 2 months postpone options! Benefits in this Paraf!	HALKBANK.
	There is one unpaid receipt for your World card. If it is not paid, your account will be taken to the Bank Tracking System.	YAPIKREDI
	IYASPARK AVM SARAR celebrates you Valentine`s day! The biggest 50% sale is on between 9-14.Do not miss the shocking winter sale.	8505553232
	You have one voice mail. To listen please call 7565.	7565

Table 11. Analysis results.

User info	Twitter's common friends average	Weighted coefficient of Twitter's common friend average	Mutual follow-up on Twitter	Is there anyone who has reviewed WhatsApp account?	Is there anyone who has reviewed Facebook account?	Is there anyone who has reviewed a contacts?	Number of phone calls score	Total Points (range: 0..1)
1.	4.75	0.20	0.20	0.2	0.2	0.1	0.10	1.00
2.	1.5	0.06	0.20	0.2	0.2	0.1	0.09	0.86
3.	1.5	0.06	0.20	0.2	0.2	0.1	0.00	0.77
4.	0.5	0.02	0.20	0.2	0.2	0.1	0.00	0.72
5.	0	0.00	0.20	0.2	0.2	0.1	0.02	0.72

Table 11. Continued.

User info	Twitter's common friends average	Weighted coefficient of Twitter's common friend average	Mutual follow-up on Twitter	Is there anyone who has reviewed WhatsApp account?	Is there anyone who has reviewed Facebook account?	Is there anyone who has reviewed a contacts?	Number of phone calls score	Total Points (range: 0..1)
6.	3.5	0.15	0.20	0	0.2	0	0.00	0.55
7.	0.25	0.01	0.00	0.2	0.2	0.1	0.01	0.52
8.	0.25	0.01	0.20	0.2	0	0.1	0.00	0.51
9.	0	0.00	0.00	0.2	0.2	0.1	0.01	0.51
10.	2.5	0.11	0.20	0	0.2	0	0.00	0.51
11.	0	0.00	0.20	0.2	0	0.1	0.00	0.50
12.	2	0.08	0.20	0	0.2	0	0.00	0.48
13.	1	0.04	0.20	0	0.2	0	0.00	0.44
14.	1	0.04	0.20	0	0.2	0	0.00	0.44
15.	0.5	0.02	0.20	0	0.2	0	0.00	0.42
16.	0	0.00	0.20	0	0.2	0	0.00	0.40
17.	0	0.00	0.20	0	0.2	0	0.00	0.40
18.	0	0.00	0.20	0	0.2	0	0.00	0.40
19.	1	0.04	0.00	0.2	0	0.1	0.00	0.34
20.	3	0.13	0.20	0	0	0	0.00	0.33
21.	0.25	0.01	0.00	0.2	0	0.1	0.00	0.31
22.	1.75	0.07	0.20	0	0	0	0.00	0.27
23.	1.25	0.05	0.20	0	0	0	0.00	0.25
24.	1.25	0.05	0.20	0	0	0	0.00	0.25
25.	1.25	0.05	0.00	0	0.2	0	0.00	0.25
26.	0.75	0.03	0.00	0	0.2	0	0.00	0.23
27.	0.5	0.02	0.20	0	0	0	0.00	0.22
28.	0.5	0.02	0.20	0	0	0	0.00	0.22
29.	0.5	0.02	0.20	0	0	0	0.00	0.22
30.	0.5	0.02	0.20	0	0	0	0.00	0.22
31.	0.25	0.01	0.20	0	0	0	0.00	0.21
32.	0.25	0.01	0.00	0	0.2	0	0.00	0.21
33.	0	0.00	0.20	0	0	0	0.00	0.20
34.	0	0.00	0.20	0	0	0	0.00	0.20
35.	0	0.00	0.20	0	0	0	0.00	0.20
36.	0	0.00	0.20	0	0	0	0.00	0.20
37.	0	0.00	0.00	0	0.2	0	0.00	0.20
38.	0	0.00	0.00	0	0.2	0	0.00	0.20
39.	0	0.00	0.00	0	0.2	0	0.00	0.20
40.	0	0.00	0.00	0	0.2	0	0.00	0.20
41.	1.75	0.07	0.00	0	0	0	0.00	0.07

Table 11. Continued.

User info	Twitter's common friends average	Weighted coefficient of Twitter's common friend average	Mutual follow-up on Twitter	Is there anyone who has reviewed WhatsApp account?	Is there anyone who has reviewed Facebook account?	Is there anyone who has reviewed a contacts?	Number of phone calls score	Total Points (range: 0..1)
42.	1.5	0.06	0.00	0	0	0	0.00	0.06
43.	0.5	0.02	0.00	0	0	0	0.00	0.02
44.	0.5	0.02	0.00	0	0	0	0.00	0.02
45.	0.5	0.02	0.00	0	0	0	0.00	0.02
46.	0.5	0.02	0.00	0	0	0	0.00	0.02
47.	0.5	0.02	0.00	0	0	0	0.00	0.02
48.	0.25	0.01	0.00	0	0	0	0.00	0.01
49.	0.25	0.01	0.00	0	0	0	0.00	0.01
50.	0.25	0.01	0.00	0	0	0	0.00	0.01
51.	0	0.00	0.00	0	0	0	0.00	0.00
52.	0	0.00	0.00	0	0	0	0.00	0.00
53.	0	0.00	0.00	0	0	0	0.00	0.00
54.	0	0.00	0.00	0	0	0	0.00	0.00
55.	0	0.00	0.00	0	0	0	0.00	0.00

The software implements the developed algorithm and performs scoring for the other users in the list based on the user with the highest score. The obtained results and analysis were shared with the owner of the device under investigation and it was stated that 90% of the results on the degree of sincerity are consistent. It was observed that as some user names are different on the phone contacts and on the social media accounts, this affects the failure rates.

Since the developed software has an open source code this allows other researchers to use it for their research.

It is possible to add additional parameters to the algorithm developed in this work from data obtained from different data sources, video and audio in order to increase its reliability.

7 Acknowledgments

This research was funded by a grant (Project Number 4385-D1-15) from the The Scientific Research Projects Coordination Unit of Suleyman Demirel University. This research was performed in cooperation with the Institution.

8 References

[1] Reith M, Carr C, Gunsch G. “An examination of digital forensic models”. *International Journal of Digital Evidence*, 1(3), 1-12, 2002.

[2] Yusoff Y, Ismail R, Hassan Z. “Common phases of computer forensics investigation models”. *International Journal of Computer Science & Information Technology*, 3(3), 17-31, 2011.

[3] Scrivens N, Lin X. “Android digital forensics: data, extraction and analysis”. *The ACM Turing 50th Celebration Conference, Shanghai*, China, 12-14 May 2017.

[4] Grover J. “Android forensics: Automated data collection and reporting from a mobile device”. *Digital Investigation*, 10, 12-20, 2013.

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

[6] Thakur NS. Forensic Analysis of WhatsApp on Android Smartphones. MSc Thesis, University of New Orleans, New Orleans, USA, 2013.

[7] Rathi K, Karabiyik U, Aderibigbe T, Chi H. “Forensic analysis of encrypted instant messaging applications on Android”. *6th International Symposium on Digital Forensic and Security (ISDFS 2018)*, Antalya, Turkey, 22-25 March 2018.

[8] Anglano C, Canonico M, Guazzone M. “Forensic analysis of Telegram Messenger on Android smartphones”. *Digital Investigation*, 23, 31-49, 2017.

[9] Satrya GB, Daely PT, Nugroho MA. “Digital forensic analysis of Telegram Messenger on Android devices”. *International Conference on Information & Communication Technology and Systems (ICTS 2016)*, IEEE, Surabaya, Indonesia, 12 October 2016.

[10] Al Mutawa N, Baggili I, Marrington A. “Forensic analysis of social networking applications on mobile devices”. *Digital Investigation*, 9, 24-33, 2012.

[11] Norouzizadeh Dezfouli F, Dehghantanha A, Eterovic-Soric B, Choo KKR. “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, 2016.

[12] Azfar A, Choo KKR, Liu L. "Forensic taxonomy of android social apps". *Journal of Forensic Sciences*, 62(2), 435-456, 2017.

[13] Azhar MHB, Barton TEA. "Forensic analysis of secure ephemeral messaging applications on Android platforms". *International Conference on Global Security, Safety, and Sustainability*, London, United Kingdom, 18-20 January 2017.

[14] Choi J, Lee S. "A study of user relationships in smartphone forensics". *Multimedia Tools and Applications*, 75(22), 14971-14983, 2016.

[15] Anwar T, Abulaish M. "A social graph based text mining framework for chat log investigation". *Digital Investigation*, 11(4), 349-362, 2014.

[16] Akbas MI, Avula RN, Bassiouni MA, Turgut D. "Social network generation and friend ranking based on mobile phone data". *IEEE International Conference on Communications (ICC 2013)*, Budapest, Hungary, 9-13 June 2013.

[17] Alzaabi M, Taha K, Martin TA. "Cisri: A crime investigation system using the relative importance of information spreaders in networks depicting criminals communications". *IEEE Transactions on Information Forensics and Security*, 10(10), 2196-2211, 2015.

[18] Reinhardt D, Engelmann F, Moerov A, Hollick M. "Show me your phone, I will tell you who your friends are: analyzing smartphone data to identify social relationships". *14th International Conference on Mobile and Ubiquitous Multimedia (MUM 2015)*, Linz, Austria, 30 November-2 December 2015.

[19] Barmpatsalou K, Cruz T, Monteiro E, Simoes P. "Fuzzy System-Based Suspicious Pattern Detection in Mobile Forensic Evidence". *9th International Conference on Digital Forensics and Cyber Crime*, Prague, Czech Republic, 9-11 October 2017.

[20] Stoffel K, Cotofrei P, Han D. "Fuzzy methods for forensic data analysis". *International Conference on Soft Computing and Pattern Recognition (SoCPaR 2010)*, Paris, France, 7-10 December 2010.

[21] Rostamipour M, Sadeghiyan B. "Network attack origin forensics with fuzzy logic". *5th International Conference on Computer and Knowledge Engineering (ICCKE 2015)*, Mashhad, Iran, 29-30 October 2015.

[22] Liao N, Tian S, Wang T. "Network forensics based on fuzzy logic and expert system". *Computer Communications*, 32(17), 1881-1892, 2009.

[23] Chen SY. *Engineering Fuzzy Set Theory and Appli*cation. Beijing, State Security Industry Press, 1998.

[24] Chen LY, Wang TC. "Optimizing partners' choice in IS/IT outsourcing projects: The strategic decision of fuzzy VIKOR". *International Journal of Production Economics*, 120(1), 233-242, 2009.