IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.8, Issue.9, September 2020 E-ISSN: 2347-2693

Forensic Analysis of WhatsApp Messenger on iOS Smartphones

Ziya UYSAL[1*], İlyas ÇANKAYA[2], Baha ŞEN[3]

[1]Dept. of Electrical and Electronics Engineering, Institute of Science, Ankara Yıldırım Beyazıt University, Ankara, Turkey
[2]Dept. of Electrical and Electronics Engineering, Faculty of Engineering and Natural Sciences, Ankara Yıldırım Beyazıt University, Ankara, Turkey
[3]Dept. of Computer Engineering, Faculty of Engineering and Natural Sciences, Ankara Yıldırım Beyazıt University, Ankara, Turkey

[*]*Corresponding Author: ziyauysal06@gmail.com, Tel.: +90-532-616-0392*

DOI: https://doi.org/10.26438/ijcse/v8i9.110 | Available online at: www.ijcseonline.org

Received: 31/Aug/2020, Accepted: 12/Sept/2020, Published: 30/Sept/2020

***Abstract*—**Mobile devices, which are used by almost everyone for both private and professional intention, have become an indispensable part of people's life. Today, one of the most important and primary features for smartphone users is that they communicate with each other through social media applications. Used by billions of people, these applications provide a lot of personal information about its user. Mobile device forensic is a significant subset of digital forensic. It is concerned with the acquisition and analysis of digital evidence on mobile devices. Commonly used by many people for messaging, calling and sharing photos/videos, WhatsApp Messenger contains several evidences for mobile forensic and is an important data mine for forensic professionals. In this study, WhatsApp Messenger, which is the most widely used instant messaging application in the world, was examined in terms of digital forensic by using popular forensic tools Cellebrite UFED and Magnet AXIOM on iPhone 5s (A1457) model smartphone with iOS operating system. Sent, received and deleted data (messages, images, videos, calls, etc.) obtained from WhatsApp Messenger application's files, databases and logs in the internal memory of the smartphone was analysed. The acquired results were given comparatively with details. The results and comparison of current commercial forensic software will help forensic experts in subsequent data analysis.

***Keywords*—**Mobile Device Forensic, iOS Forensic, Instant Messenger Applications, WhatsApp Messenger, Forensic Tools

I. INTRODUCTION

Digital forensic is a science based on the collection, acquisition, analysis and reporting of data that is legally acceptable in electronic or digital devices under forensic conditions [1]. Digital forensic is classified into various sub-branches with respect to the kind of digital devices; computer forensic, mobile device forensic, network forensic, cloud forensic and so on. Computer forensic is a collection, identification, acquisition, storage, examination and submission of all kinds of information objects consisting of audio, video, data, information or a combination of these, which are stored or transmitted in computer or digital storage media [2]. The discipline generally involves analysis of computers, embedded systems, data storage device (HDD, RAM, USB). Network forensic is a digital forensic sub-branch that deals with the listening and examination of network traffic, both local and remote internet, for the goal of collecting data, detecting legal evidence and interference attacks [3]. Different from other field of digital forensic, network researches interested in transient and dynamic information. Network traffic data is transmitted and later lost. Therefore, network forensic is generally a proactive examination [4]. Cloud forensic is the implementation of digital forensic in cloud computing as a sub-branch of network forensic [5]. From a technical aspect, cloud forensic comprise of a hybrid forensic attitude (e.g., remote, virtual, network, live) towards the producing of digital evidence [6].

Mobile device forensic is the recovery of digital data or evidence from a mobile device under forensically proper circumstances using approved processes [7]. With the sudden increase in the popularity and usage of smartphones in the world, this forensic branch has become one of the newest and most important parts of digital forensic. The term mobile device is generally used for mobile phones, but also refers to any device capable of both internal memory and communication skill, comprising tablet computers and personal digital assistant. Mobile device forensic is relatively different from computer forensic, and it has become more important and popular with the advanced features of mobile phones. Many problems and questions can arise during mobile phone forensic but the most important factor in answering these questions and solving problems is a good understanding of the hardware and software features of mobile phones.

Smartphones are advanced mobile devices with various hardware and software in addition to the classic features provided by mobile phones. With the rapid development of technology, software and hardware features such as mobile operating systems, applications, games, advanced camera technologies, high resolution display panels, wireless charging technologies, fingerprint and face recognition systems have been added to smartphones. Smartphones have their own mobile operating systems. Because of this feature, they can be used in different ways for various purposes and can have many applications for each feature. The most distinctive features of smartphones compared to

regular phones are special operating systems. Mobile operating systems are used for mobile phones, tablets, smartwatches and other mobile devices. Most smartphones today have almost Android or iOS operating systems. Android operating system is a Linux-based open-source and cost-free mobile operating system developed by Google (GOOGL) and the Open Handset Alliance (OHA) for use with touch-screen devices such as smartphones, tablets and wristwatches [8]. iOS is a Darwin-based closed-source mobile operating system created and developed by Apple Inc. especially for own mobile devices. It is the second most used mobile operating system after Android worldwide among mobile operating systems. App Store, which contains millions of different applications, enables the downloading of mobile applications on the iOS [9].

One of the most important features of smartphones is the applications installed on them. In today's era, most commonly used applications is social media applications, which are basically found on almost every smartphone and enable people to communicate with each other visually and in writing. The basic features of mobile phones, short messaging and voice speaking, are now being realized through instant messaging applications due to the widespread use of the internet and providing free services worldwide. Instant messaging applications are a type of online chat technology that offers messaging, speaking, file sharing and similar services in real time via the Internet. WhatsApp Messenger is a mobile instant messaging application that is popular worldwide and has millions of users. Because it is used by millions of people around the world to communicate, share files and media, it keeps a lot of personal information on the phone. WhatsApp's databases are today one of the leading sources of evidence for forensic science specialists, as it is so widely used and contains a wide range of personal data. The results obtained from the application accelerate the judicial processes and help to solve judicial cases.

Smartphones with various software and hardware are examined by experts in terms of mobile forensic. There are major mobile forensic software and hardware that assist the digital forensic specialists during this review. In parallel with the increase in the usage and technological features of mobile devices, the properties of the tools used in the mobile forensic examination of these devices have also improved. The tools used may consist of both hardware and software parts, the hardware section forms equipment such as write-block devices and special cables connecting the device to the device for examination, while the software part constitutes special purpose software which performs operations such as analysing and reporting the evidence obtained from the device. Since it is impossible for any mobile forensic tool to obtain all the evidence from all mobile devices on the market today, it is recommended that mobile forensic experts have a variety of commercial and open source forensic software and various hardware with different functions. Cellebrite UFED and Magnet AXIOM are among the most popular commercial forensic tools currently used by digital forensic experts. Cellebrite UFED is a forensic tool used in forensic investigations conducted on mobile phones, tablets, drones and other mobile devices. Thanks to the wide mobile device support, it enables to create images in various ways on the mobile device which is evidence and to obtain critical data from the received image file and perform forensic analysis. Magnet AXIOM is a forensic tool that recovers and analyses digital evidence from smartphones, computers, cloud services and other digital devices. It recovers and analyses the digital data in it after the evidence is obtained. It can then report the analysed data in the appropriate case file format. Both of them is used by specialist working in the digital forensic field such as military, law enforcement agency, intelligence and information security departments of institutions / companies.

In this study, forensic analysis of WhatsApp Messenger application on smartphone with iOS operating system has been realized by using current forensic tools. The rest of this paper is structured as follows: In Section 2, related works on forensic analysis of WhatsApp Messenger application are presented. In Section 3, WhatsApp Messenger application is introduced. In Section 4, information is given about the iOS operating system and statistic are presented. In Section 5, the digital forensic tools used in the study is explained. In Section 6, how the working methodology is revealed and the digital forensic phases are given. In Section 7, the hardware and software used in the study are listed and explained in detail. Preparations to create the test environment are mentioned. In Section 8, how the data is obtained from the test evidence and how the analysis is carried out by using digital forensic tools on the data obtained is shown. In Section 9, Important information obtained as a result of the analysis has been revealed. In Section 10, the results of the study conducted in terms of digital forensic are evaluated and what the future work are mentioned.

II. RELATED WORKS

Nowadays, instant messaging applications, especially WhatsApp Messenger, are increasingly popular, therefore forensic analysis of these applications has become a hot topic in the field of digital forensic. In the literature, there are various studies on the analysis of WhatsApp Messenger in terms of digital forensic. Sgaras et al. realised forensic analysis and comparison of four instant messaging applications (WhatsApp, Viber, Skype and Tango) and VoIPs on two different operating systems, iOS and Android [10]. In this study, as a result of forensic analysis of four instant messaging applications whose total number of users exceeds 1 billion, it is shown that what kind of data can be accessed, how and where the evidence is stored, how it is obtained and analysed and also compared in different operating systems. Walnycky et al. performed forensic study on twenty social messaging applications, containing WhatsApp, that are popular in the Google Play Store on the Android mobile phone [11]. In the research, twenty applications were examined through

network traffic and device storage analysis, and then various results were reached by evaluating the security of applications in data sending/receiving and the confidentiality of applications in data storage. Anglano analysed the data that WhatsApp Messenger has left on smartphones with Android operating system [12]. In the study, he presented how to interpret and resolve the differences by analyst if any changes are made by the users in the databases where the contact list and messages are kept. Mahajan et al. carried out the forensic analysis of two popular messaging programs WhatsApp and Viber in three different versions of the android operating system [13]. In the article, as a result of the tests and analyses on the internal memory of mobile devices show that which of the various data can be accessed such as messages, photos, videos and similar information received and sent through the specified applications. Tso et al. reviewed five of the most widely used social networking applications, including WhatsApp, on iPhone mobile devices [14]. In the study, the diversity between the data that remains after it was installed-and-used and the data that remains after it was deleted was observed by performing analysis of iTunes backup files on iPhone devices.

III. WHATSAPP MESSENGER APPLICATION

WhatsApp was founded by Jan Koumand and Brian Acton, former employees of Yahoo! in 2009 in California, United States. It was purchased by Facebook in 2014 for roughly US$ 19.3 billion, its largest acquisition to date [15]. More than 2 billion people use WhatsApp to communicate in over 180 countries. WhatsApp offers an easy, secure and reliable messaging and calling service that can be used on phones all over the world [16]. By year of 2020, WhatsApp is the most popular global mobile messaging application worldwide, reaching around 2 billion monthly active users, outperforming Facebook Messenger with 1.3 billion users and WeChat with 1.2 billion users, as shown in Figure 1 [17].

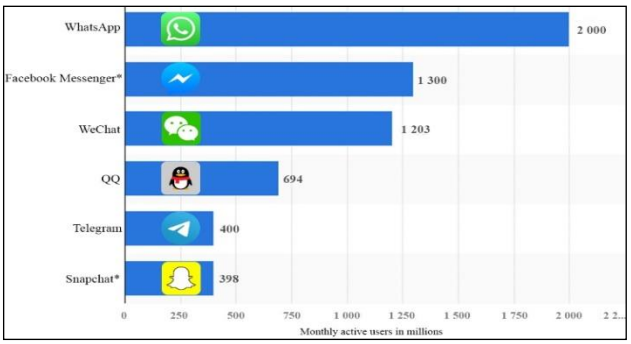

Figure 1. Most Popular Global Mobile Messenger Apps as of July 2020

WhatsApp Messenger is a free software multi-platform instant messaging, voice and video communication service for mobile devices over internet protocol (IP). It is an application that enables users to send text messages and sound recording, make video and voice calls, share documents, photos, videos, real-time location information and contacts among themselves or in groups. The application requires users to register and verify a cellular mobile phone number from a device to use their accounts. It supports Android, BlackBerry, iOS, Windows Phone and Nokia phones. WhatsApp's client application works on mobile devices as well as when the QR code is scanned and synchronized to the computer, it can be used on the desktop application (WhatsApp Web) by stay in connected to the Internet.

IV. IOS OPERATING SYSTEM

Apple was founded by Steve Jobs, Steve Wozniak and Ronald Wayne in 1976 in California, United States [18]. Apple introduced first mobile operating system for iPhone mobile phones under the name "iPhone OS 1" on 29 June 2007. After, the operating system was also used on the company's mobile devices such as iPod Touch and iPad. iOS is a Unix-like Darwin (BSD) based closed source mobile operating system. The structure of the iOS operating system, derived from Mac OS X, consist of four main layers; Core OS, Core Services, Media Layer and Cocoa Touch. Due to the iOS operating system structure, applications cannot be installed from anywhere other than App Store and iTunes. It is the second most popular mobile operating system which has 25% market share worldwide after the Linux based open source Android operating system which has 74.5% market share, as shown in Figure 2 [19].

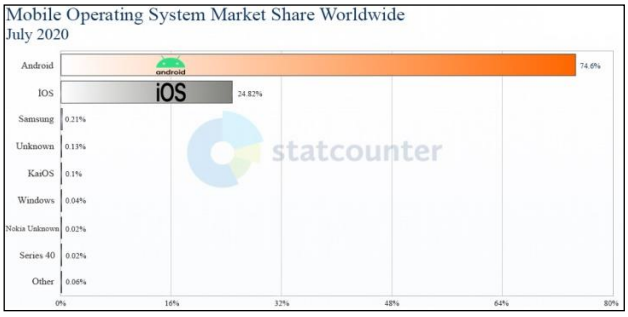

Figure 2. Mobile Operating System Market Share Worldwide on July 2020

The App Store is digital distribution store, created and developed by Apple Inc., which allows mobile device users with iOS operating system to view and download mobile apps. Although the App Store was launched in 2008 with 500 apps available, it has developed rapidly and is the second largest application store worldwide after the Google Play Store, with nearly 2 million apps, as can be seen in below Figure [20].

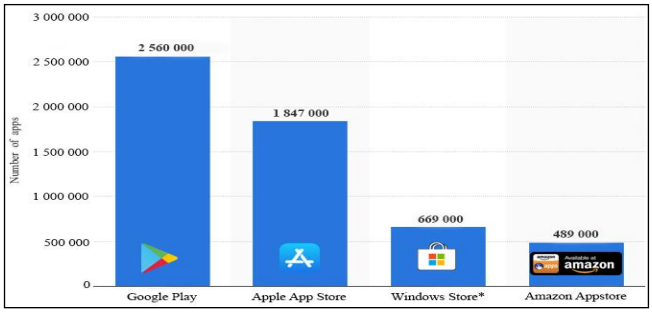

Figure 3. Number of Apps Available in Leading App Stores as of 1st Quarter 2020

As of 2020, WhatsApp Messenger, which is the subject of this research, was the most downloaded application on the App Store among the applications developed for iPhone [21].

V. FORENSIC SOFTWARE USED IN MOBILE DEVICES

A. CELLEBRITE UFED

Cellebrite Mobile Synchronization is an Israeli company, founded by an experienced team in 1999, which has made great strides in the telecom and mobile device technologies industry. The company produces hardware and software that data extraction, content transfer and analysis for mobile devices. Mobile forensic products were announced in 2007 under the brand name of 'Universal Forensic Extraction Device' (UFED) by Cellebrite's Mobile Forensic. UFED is a forensic tool for mobile phone, smartphone and PDA, recovering hidden and deleted data, decrypting password-protected device and encrypted information, as well as extracting both logical and physical data. The UFED can extract, recover, decrypt and analyse International Mobile Equipment Identity (IMEI), electronic serial numbers (ESN), SIM GPS information, time/date stamps and personal data (contacts, messages, call logs, emails and all kinds of multimedia content) from device memory. The UFED supports all cellular protocols, especially GSM, TDMA, CDMA, IDEN and can communicate with various operating systems (iOS, Android OS, BlackBerry OS, Symbian and Windows Mobile) [22]. The UFED enables the recovery of subject data by way of logical, file system and physical extraction (a bit-to-bit copy of a mobile device storage). Mobile device's passwords can be bypassed and SIM PIN numbers can be decrypted with the UFED's physical extraction feature. In addition, since most of the chipsets for mobile phones are manufactured in China, it is capable of digital forensic in compliance with the brand model phone manufactured in China.

B. MAGNET AXIOM

Magnet Forensics is a Canadian company, founded in 2009, and has started the forensic industry with the solution to find the Internet file remains on computers. Since 2011, the company has developed further and began to provide forensic analysis in the areas of computers and mobile devices for the public and private sectors, especially law enforcement officers. Magnet AXIOM is a forensic tool that recovers, analyses and reports evidence from the most data sources, such as smartphones, computers or the cloud. Evidence can be reported clearly and directly in the appropriate file format. The AXIOM can automatically generate important data during examinations through additional features such as Connections, Timeline, and Magnet.AI module. Magnet AXIOM consist of two main parts, AXIOM Process and AXIOM Examine. AXIOM Process performs the task of acquiring and processing the data to be used in the examination stage, while AXIOM Examine performs the analysis and reporting of the data obtained from the evidence. AXIOM Process can acquire image from mobile devices running iOS or Android, computers with Windows, OSX and Linux operating system, hard drives such as HDDs and SSDs, and removable medias such as USB flash drives. The AXIOM Process enables the recovery and processing more than 750 types of artifacts [23]. AXIOM Examine can quickly and efficiently analyse large-size data, and thanks to the Magnet.AI module, the machine learning technology, it can quickly identify priority texts and visuals such as weapons, drugs and sexuality. AXIOM Examine reporting tools, such as Portable Case, provide information in a format that non-technical stakeholders can understand.

VI. WORKING METHODOLOGY

The aim of this article is to determine what should be the analysis of WhatsApp Messenger, which has the most active users among the instant messaging applications on the smartphone with iOS operating system, and what evidence can be obtained using popular forensic tools, UFED and AXIOM. The methodology of this study is basically consisting of four stages. These stages are respectively preparation, acquisition, analysis and reporting phase, as can be seen in Figure 4.

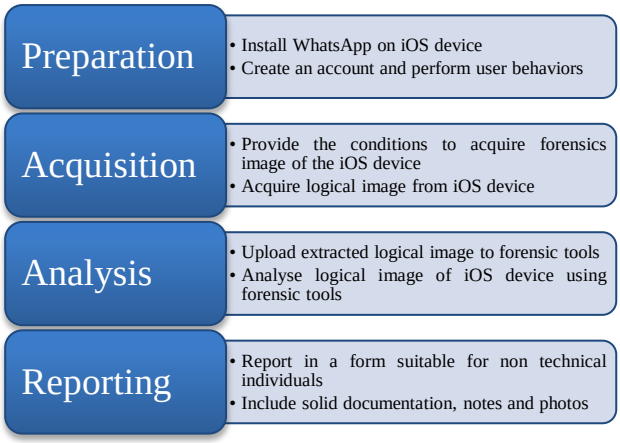

Figure 4. The Implementation Steps of This Study

The first stage is the preparation phase where the application was installed and user behaviour was performed. At this stage, WhatsApp application has been login and important information (user behaviours) has been created in mobile device forensic. Thus, the iOS device became an evidence ready to enter the mobile review process. Then, the mobile device was switched to flight mode and the communication with the outside world was interrupted and thus the second stage, the acquisition phase, was started. After the device was isolated from external environment, its logical image was acquired by use of mobile forensic tool to be used in this article. The image obtained with write-blocked tool was uploaded to the mobile forensic tools for examination and so the third stage of this study, the analysis stage, was passed. The image of the mobile device was analysed by using Cellebrite UFED and Magnet AXIOM forensic tools and the obtained data were examined. The file carving process also was realized to obtain more data from the image.

Then, the data obtained was analysed in detail and the answers to below questions were sought.

- What kind of data were obtained?
- Which data structure were determined?
- Is the data obtained timestamped?
- How evidence is stored in databases?
- Is the data in the database stored encrypted?
- Can deleted data be recovered?

After finding the appropriate answers to the above questions, the last stage of mobile forensic investigation, reporting phase, was began. The obtained results were reported in a suitable format to be understood by those who do not have sufficient technical knowledge on this subject. In order to present the results in a more understandable and supportive way, explanatory information notes, related photographs and detailed tables were presented.

VII. WORKING REQUIREMENT & PREPARATION

In order to carry out the article study, the test environment was prepared. Firstly, a mobile device with iOS operating system was provided. iPhone 5s (A1457) model smartphone with iOS 12.4.4 operating system has been selected for analysis in test environment. There were two main reasons for selecting this device statically and logically. The first reason is that in the case of an older model phone, it is no longer available in the market, it is not used much by people, it does not support current operating system versions, and it is assumed that the data to be obtained will not benefit in theory / practice. The second reason is that in the case of a latest model phone, it is new in the market, it is not yet in use by many people, and the results can be misleading due to the fact that errors / vulnerabilities found in the latest operating system versions. In addition, it should be noted that the device used as test evidence has not been jailbroken and no password has been set. Because jailbreak is a process that allows device users with iOS operating systems to download and use additional applications / content that are not available in the Apple App Store or are not included due to restrictions, and allows users to "root" access to operating and file system. This process is carried out by installing unaccredited applications and unverified software on the phone. It can also change the data on the device or even force the data partition to be erased before allowing jailbreaking. Even if the jailbreak process is completed successfully, stability and security problems may occur in the device, there may be excessive slowing, unresponsiveness or locking, and there may be a problem with return from backup. It should not be forgotten that while the jailbreak operation is performed successfully, it provides access to more data, but if it fails, the data can be deleted or create various problems on the phone. Although each method has different effects, success rates will vary depending on the tool used, the method applied, and the brand, model and operating system version of the device. In the field of digital forensic, jailbreak process is not preferred by digital forensic experts unless it is necessary. Due to the fact that intervention by installing third party applications and software that are not verified, leaving traces in the system logs, and there are risks such as loss of access or locking of device. Also about password, If the mobile device to be examined has a password, it is usually obtained from the suspect through the court and it is out of the scope of this research subject because of the use of different devices and software in the password bypassing process and the process takes a long time. Then, WhatsApp Messenger application, was downloaded to the smartphone free of charge and the user behaviours / personal data to be analysed in the test environment were created by logging into the application.

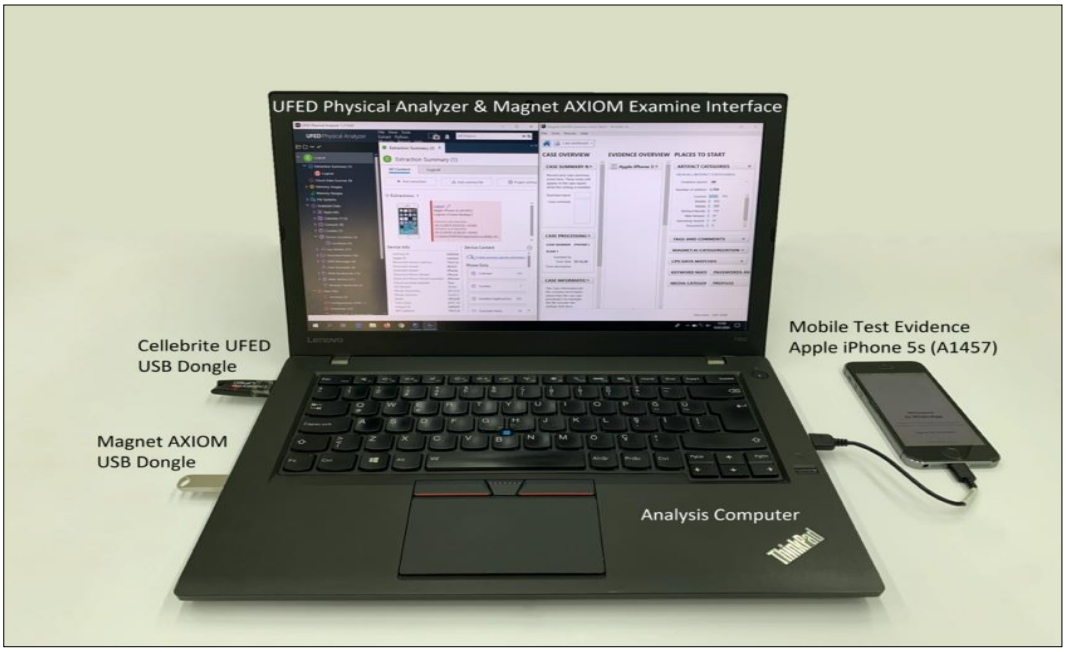

Figure 5. Mobile Forensic Test Environment and The Tools Used

Next, mobile forensic tools that will be used to create the image of the smartphone and analyse the data obtained from the image was provided. Two of the most used tools in the field of mobile forensic have been preferred in order to perform these procedures and present the results to be obtained comparatively. The first is Cellebrite UFED and the second is Magnet AXIOM. Finally, the software used in the field of mobile forensic was installed on the workstation to obtain data from the iPhone 5s smartphone, which is the test evidence, and then analyse it. Thus, the preparatory phase, which was the first step of the article study, has been completed, as shown in Figure 5.

Table 1. List of the Equipment

Hardware	**Purpose of Usage**
Lenovo ThinkPad T460, x64 Intel Core i7-6600U CPU, 8 GB RAM, Windows 10 Enterprise Operating System	Data Acquisition and Analysis
Apple iPhone 5s (A1457) Space Gray, 16GB Capacity, A7 chip with 64-bit architecture, iOS 12.4.4 Operating System	Test Evidence
Turk Telekom Nano SIM Card	Login and Use WhatsApp Messenger
Software	**Purpose of Usage**
Cellebrite UFED 4PC version 7.27.0.53	Data Acquisition
Cellebrite Physical Analyzer version 7.27.0.87	Data Analysis
Magnet AXIOM Process version 3.8.0.16657	Data Acquisition
Magnet AXIOM Examine version 3.8.0.16657	Data Analysis
WhatsApp Messenger version 2.20.11.4	Test Application

VIII. ACQUISITION & ANALYSIS

The second stage of this research topic is the acquisition phase, which is to create a copy or image of the data in the device to examine the user behaviours created using the WhatsApp application on the smartphone during the preparation process. In digital forensic, the process of making an exact copy of a device is called an image. Due to the developing technology and increasing device diversity, obtaining data from the mobile device differs according to the brand and model, especially the operating system of the mobile phone. There are two basic methods of obtaining data from the phone, logical and physical acquisition. Logical acquisition is the process of making a bit-to-bit copy of the logical area that the operating system allows the user to access logical storage objects such as files and directories. Physical acquisition is the process of making a bit-by-bit copy of the whole physical storage that it permits the examination of deleted folders and any available data residues such as unallocated or file system memory. Cellebrite UFED 4PC and Magnet AXIOM Process software were used to perform image acquisition. The test evidence, iPhone 5s smartphone, has iOS 12.4.4 operating system. Cellebrite UFED 4PC and Magnet AXIOM Process forensic tools provide logical acquisition for iPhone 5s model smartphone with iOS 12.4.4 operating system, but not support physical acquisition. For this reason, in this study, logical acquisition of test evidence was taken with digital forensic tools, as can be seen in Figure 6. Thus the acquisition phase, which is the second step of the article study, was completed. In addition, the hardware and software used in this study are listed in Table 1.

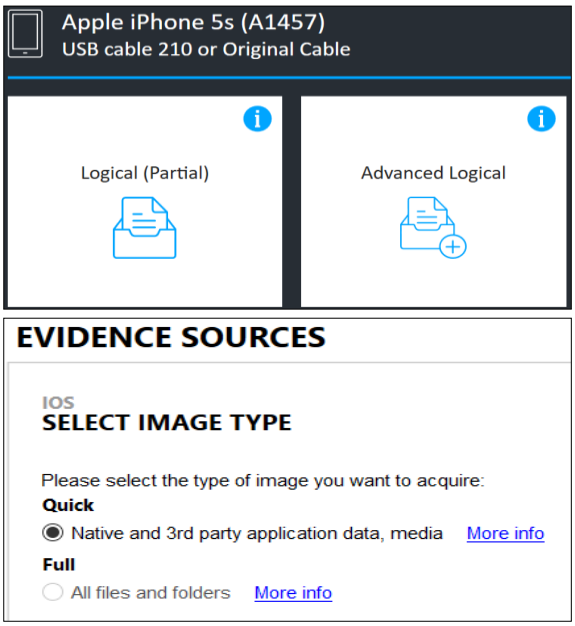

Figure 6. UFED 4PC and AXIOM Process Acquisition Types

The third stage of this research topic is the analysis phase, which is to examine the data of the WhatsApp application on the mobile device, which logically obtained a copy of. The analysis of the logical extraction files obtained was carried out by using Cellebrite UFED Physical Analyzer and Magnet AXIOM Examine forensic tools. By analysing the file system, WhatsApp data was detected in the group.net.whatsapp.WhatsApp.shared folder under the *"iPhone/Applications/group.net.whatsapp.WhatsApp.shared"* directory. When this folder was examined in detail, "ChatStorage.sqlite" and "ContactV2.sqlite" databases and the file named "call.log" containing the log records of the call logs were detected. In addition, important data has been identified in the "Message/Media" and "Library/Preferences" subfolders in the "group.net.whatsapp.WhatsApp.shared" folder. When the analysis of ChatStorage.sqlite database was performed, it was determined that it contains information about personal and group messages in the ZWAMESSAGE table. Among these information, as shown in Figure 7; there is a lot of information about the message content, especially the text message, the date/time of the message, from whom the message came from, to whom the message was sent. "JID" expression that expresses the WhatsApp identity is used for users and groups. While WhatsApp contacts are stated as "phone number@s.whatsapp.net", the groups are expressed as "the phone number of the person who created the group - group establishment timestamp@g.us".

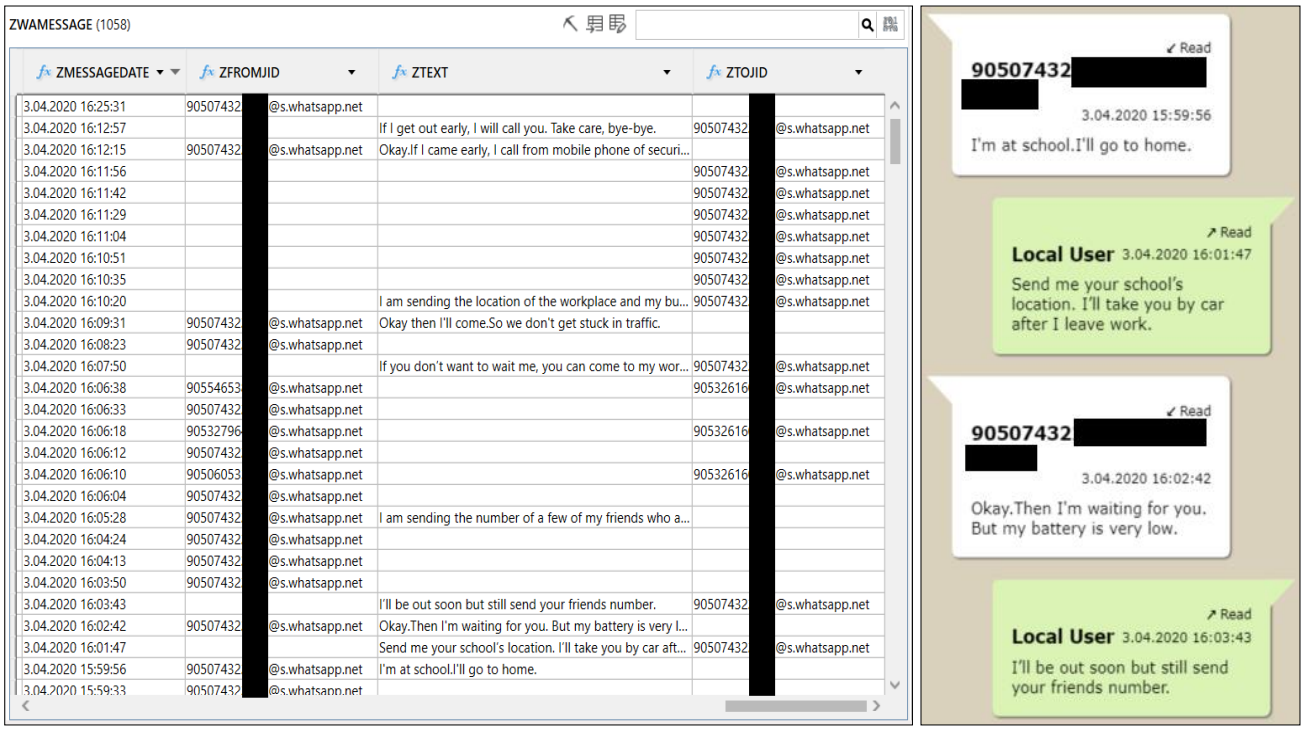

Figure 7. UFED Physical Analyzer ZWAMESSAGE Table Database Screen and AXIOM Examine Chat Preview

When the ContactsV2.sqlite database was examined, the names, phone numbers, nicknames and contact status information of the users in the WhatsApp application was determined in the ZWAADDRESSBOOKCONTACT table. When the file named "call.log", in which the log records of voice and video calls were kept, was examined, the type, direction and duration of call, time information, and caller or dialled number information were seen, as shown in Figure 8.

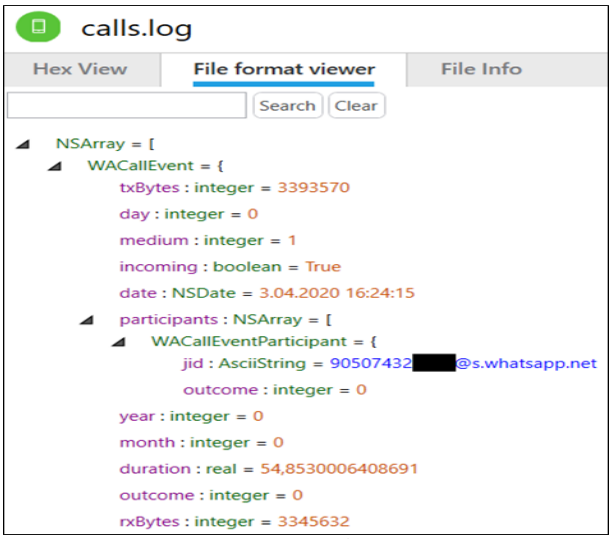

Figure 8. File Format View of WhatsApp Call Data

It was observed that the information belonging to WhatsApp user account and behaviors was found in the file in the /Applications/group.net.whatsapp. WhatsApp.shared/Library/ Preferences/group.net.whatsapp.WhatsApp.shared.plist.Wh

en the shared media is analyzed, it is seen that the media (documents, photos, videos, sound recordings) and location information shared via WhatsApp application are stored in "/Applications/group.net.whatsapp.WhatsApp.shared/Message/Media" folder. The shared data is stored in subfolders under the Media folder named "phone number@s.whatsapp.net" for individuals, and "the phone number of the person who created the group – group establishment timestamp@g.us" for groups, as shown in Figure 9.

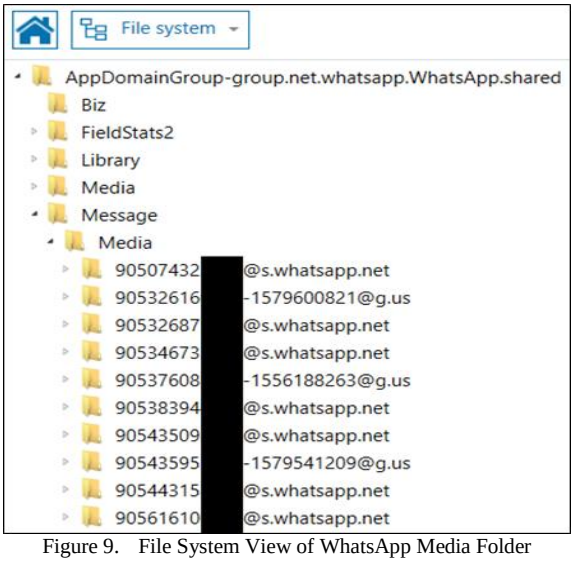

Figure 9. File System View of WhatsApp Media Folder

Records of shared data such as photos, videos, documents, location and contact as text are kept in the ZWAMEDIAITEM table in the ChatStorage.sqlite database, as shown in Figure 10.

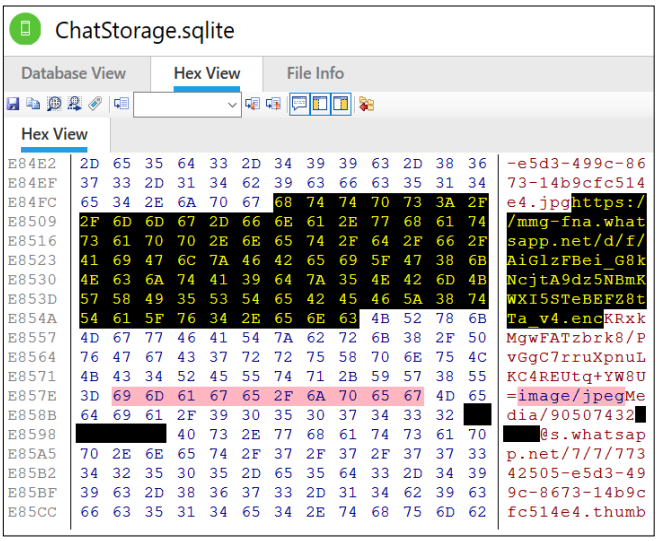

Figure 10. Hex View of Shared Image in ChatStorage.sqlite

By determining the files and databases of WhatsApp Messenger application over the acquired mobile phone image, the data of user behaviour such as messaging, calling, data sharing were analysed. Thus, the analysis phase, which is the third step of the article study, has been completed.

IX. REPORTING

The final stage of this research topic is the reporting phase, where the data analyse are appropriately presented for consideration as evidence. The results obtained should be reported in a more descriptive way for judges and lawyers who do not have sufficient technical knowledge. In addition, the analysed data should be supported by adding brief explanations, related photos and detailed tables in the report. In this study, due to the operating system version of the smartphone, which is the test evidence, it was seen that the physical acquisition of the mobile device could not be obtained without any external intervention using mobile forensic tools. When the analysis of the smartphone, which was logically image acquired, was performed, it was determined that there are existing user behaviour data in the mobile device. It was observed that text messages, call records, and the information such as timestamp and file path of the obtained data were stored unencrypted in the databases and the shared data such as media and document were classified according to the phone number of the person.

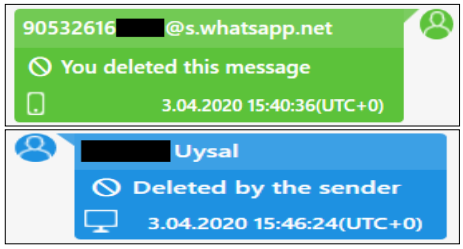

Figure 11. Chat Preview of Deleted Data

While the existing data in the device can be accessed, the content of the data deleted by the users cannot be accessed. As can be seen in Figure 11, while the content of the data cannot be determined, various information about the data such as receiver or sender information, timestamp can be determined. In some studies, in the literature, when the devices with the old iOS operating system version, and various devices with the android operating system that allows physical image acquisition were analysed, it has been seen that the contents of this deleted data can also be viewed. In this study, the physical image acquisition process of the device could not be performed with current forensic information tools, therefore, its logical image was obtained and analysed. After the analysis, the results obtained regarding user behaviour are summarized in Table 2 in a way that people without technical knowledge can understand.

Table 2. Analysis Results of WhatsApp User Behaviors

Cellebrite UFED & Magnet AXIOM Results			
User Behaviours	**Send**	**Receive**	**Deleted**
Text messages via private chat	✔	✔	✗
Text messages via group chat	✔	✔	✗
Images	✔	✔	✗
Videos	✔	✔	✗
Documents	✔	✔	✗
Location information	✔	✔	✗
Live location information	✔	✔	✗
Contact information	✔	✔	✗
Voice calls	✔	✔	✗
Video calls	✔	✔	✗
Sound recordings	✔	✔	✗
Profile information	✔	✔	✗

If the evidence is not obtained in the analysis and if it is desired to access the deleted data, firstly bit-by-bit copy of the mobile device should be physical acquired. Since the mobile test device does not allow physical acquisition with its current version, it must intervene externally in the device. Technically, this intervention is called "jailbreak". If this operation is performed successfully, the physical acquisition of the device can be taken and more data can be obtained including deleted data by making detailed analysis. Logically acquired mobile test evidence was analysed, then the data were supported with obtained photos and tables, short explanations in a clear language were added and was made it ready for the court. Thus the reporting phase, which is the last step of the article study, was completed.

X. CONCLUSION & FUTURE WORK

In this study, WhatsApp Messenger v.2.20.11.4 instant messaging application was installed on Apple iPhone 5s (A1457) model smartphone with iOS 12.4.4 operating system and user behaviours were analysed according to mobile forensic standards. First of all, the user behaviours / personal information to be analysed were prepared by realizing the application features such as messaging, calling, and media sharing offered to the users during the preparation phase. Then, the logical image was acquired

using Cellebrite UFED 4PC v.7.27 and Magnet AXIOM Process v.3.8 software during the acquisition stage, because the current version of the mobile device does not support physical acquisition. The analysis of this image was carried out using Cellebrite UFED Physical Analyzer v.7.27 and Magnet AXIOM Examine v.3.8 tools and the data obtained were evaluated in terms of digital forensic. During the analysis phase, the media folders, log files and databases of the WhatsApp Messenger instant messaging application on the smartphone with iOS operating system were examined in detail. It has been determined that the user behaviour data of WhatsApp Messenger application, which is important for mobile device forensic, is located in the *"iPhone/Applications/group.net.whatsapp.WhatsApp.shared"* directory. The ChatStorage.sqlite database under this directory and, the ZWAMESSAGE and ZWAMEDIAITEM tables contained in it are important for us. Because it has been determined that private and group chat text messages and information about messages are kept in the ZWAMESSAGE table, and information about shared media such as images, documents, voice recordings and location are kept in the ZWAMEDIAITEM table. The content of these shared media is stored in the Media folder under the Message folder in the same directory, according to the phone numbers of users or shared groups. In the ZWAADDRESSBOOKCONTACT table in the Contacts V2.sqlite database in the same directory, information about the names of users of the application, phone numbers, and contact status (as text) are included. User profile pictures and group icons are also stored in thumbnail format in the Profile folder under the Media folder in the same directory. All incoming / outgoing voice and video calls, and information such as timestamp, direction and duration of these calls are kept in the file called calls.log. In addition, information about WhatsApp user profile and behaviours has been determined in the group.net.whatsapp. WhatsApp.shared.plist file in the Preferences folder under the Library folder in the same directory. Finally, the analysis of the important data in accordance with the digital forensic principles and the presentation of them in evidence in the court were described during the reporting phase. The obtained data was explained by adding technical explanations, supporting with relevant visuals and summarizing as tables, and reporting in accordance with justice personnel who have no detailed knowledge about digital forensic, such as judges and lawyers. Thus, the data of the popular instant messaging application in a mobile device has been analysed by adhering to the forensic information principles and processes, and detailed to assist the forensic science experts in their work.

In this study, the existing data in the device was analysed in detail due to the logical acquiring, and the content of the deleted data could not be accessed. However, if the desired evidence cannot be obtained with the existing data, it may be necessary to obtain and analyse the deleted data. As it can be understood from the literature and this work, it is necessary to obtain the physical image of the mobile device as bit by bit in order to obtain the deleted data. Physical image acquisition can be done on phones that do not have the current operating system version, using the popular forensic computing tools, while it can cause problems for phones with the latest version. The fact that mobile device manufacturers and application owners direct their users to update their existing systems when they release new versions, or that the automatic update option of the devices is active in the default settings when the update is published causes problems for mobile forensic experts to examine the phones with the current operating system. On devices with iOS operating system, jailbreak operation is applied to overcome this problem. This process can be defined as getting rid of the software limitations of the operating system and escalating the privilege by accessing the operating system with "root" authority. Thanks to the jailbreak process, access to the deleted data can be obtained with a physical image, but if the operation fails, there may be various problems on the phone and even the risk of not being able to access the data or deleting the data. The subject of future works may be how to access deleted data, pros & cons of jailbreak process and suitability of this process for forensic examinations, access to deleted data using different methods, obtaining and analysing the data on the device after returning the mobile device to factory settings, forensic analysis on devices with a more current operating system and application version, forensic examination of existing and deleted data on mobile devices with different operating systems. Obtaining data from a mobile device using password bypass techniques is another issue, but it has an important place in digital forensic science. It is certain that performing the technical analysis of the mentioned studies in detail will be very useful for forensic experts in their next forensic analysis.

REFERENCES

[1] W. Jansen, R. Ayers, "*Guidelines on cell phone forensics*", NIST Special Publication 800-101, Vol.**1**, No.**1**, pp.**1-104**, **2007**.

[2] M. G. Noblett, M. M. Pollitt, L. A. Presley, "*Recovering and examining computer forensic evidence*", Forensic Science Communications, Vol.**2,** Issue.**4**, **2000**.

[3] G. Palmer, "*A road map for digital forensic research*", In the First Digital Forensic Research Workshop, New York, **USA**, pp.**27-30**, **2001**.

[4] E. Casey, G. Palmer, "*The investigative process*", Digital Evidence and Computer Crime, Elsevier Academic Press, **Amsterdam**, **2004**.

[5] Bhanushree V.K, Minavathi, "*Cloud packets forensics through NIDS and NIPS with honeypot*", International Journal of Computer Sciences and Engineering, Vol.**8**, Issue.**4**, pp.**119-122**, **2020**.

[6] NIST Cloud Computing Forensic Science Working Group, "*NIST cloud computing forensic science challenges*", Draft NISTIR 8006, **2014**.

[7] R. Ayers, S. Brothers, W. Jansen, "*Guidelines on mobile device forensics*", NIST Special Publication 800-101 Revision 1, Vol.**1**, No.**1**, pp.**1-85**, **2014**.

[8] N. Gandhewar, R. Sheikh, "*Google Android: An emerging software platform for mobile devices*", International Journal on Computer Science and Engineering, Vol.**1**, No.**1**, pp.**12-17**, **2010**.

[9] M. Nosrati, R. Karimi, H. A. Hasanvand, "*Mobile computing: principles, devices and operating systems*", World Applied Programming, Vol.**2**, Issue.**7**, pp.**399-408**, **2012**.

[10] C. Sgaras, M. Kechadi, N. A. Le-Khac, "*Forensics acquisition and analysis of instant messaging and VoIP applications*", In the Computational Forensics, Cham, **Switzerland,** pp.**188-199**, **2016**.

[11] D. Walnycky, I. Baggili, A. Marrington, J. Moore, F. Breitinger, "*Network and device forensic analysis of android social-messaging applications*", Digital Investigation, Vol.**14**, pp.**S77-S84**, **2015**.
[12] C. Anglano, "*Forensic analysis of WhatsApp Messenger on Android smartphones*", Digital Investigation, Vol.**11**, Issue.**3**, pp.**201-213**, **2014**.
[13] A. Mahajan, M. S. Dahiya, H. P. Sanghvi, "*Forensic analysis of instant messenger applications on android devices*", International Journal of Computer Applications, Vol.**68**, No.**8**, pp.**38-44**, **2013**.
[14] Y. C. Tso, S. J. Wang, C. T. Huang, W. J. Wang, "*iPhone social networking for evidence investigations using iTunes forensics*" In the Proceedings of the 6th International Conference on Ubiquitous information management and Communication, New York, **USA**, pp.**1-7**, **2012**
[15] Facebook, "*Facebook to acquire whatsapp*", Available at: https://newsroom.fb.com/news/2014/02/facebook-to-acquire-whatsapp/ [Accessed on 24 August 2020]
[16] WhatsApp, "*About WhatsApp*", Available at: https://www.whatsapp.com/about/?lang=en [Accessed on 24 August 2020]
[17] Statista, "*Most popular global mobile messenger apps as of July 2020, based on number of monthly active users (in millions)"*, Available at: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ [Accessed on 24 August 2020]
[18] My Assignment Help, "*Business performance of iphone 7*", Available at: https://myassignmenthelp.com/free-samples/business-performance-of-iphone-7?cv=1&access-library-email= [Accessed on 24 August 2020]
[19] Statcounter, "*Mobile operating system market share worldwide*", Available at: https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-202007-202007-bar [Accessed on 24 August 2020]
[20] Statista, "*Number of apps available in leading app stores as of 1st quarter 2020*", Available at: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ [Accessed on 24 August 2020]
[21] Independent, "*Apple reveals its best and most popular iPhone apps in 2019*" Available at: https://www.independent.co.uk/life-style/gadgets-and tech/news/iphone-best-apps-2019-apple-app-store-most-popular-a9230706.html [Accessed on 24 August 2020]
[22] Wikipedia, "*Cellebrite*", Available at: https://en.wikipedia.org/wiki/Cellebrite [Accessed on 24 August 2020]
[23] Magnet AXIOM, "The evolution of IEF", Available at: https://irp-cdn.multiscreensite.com/ad68eab3/files/uploaded/MagnetAXIOM_e-brochure.pdf [Accessed on 24 August 2020]

AUTHORS PROFILE

Ziya UYSAL was born in Ankara, Turkey, 1993. He received the B.Sc. degree in Electrical and Electronics Engineering from Ankara Yildirim Beyazit University, Ankara, Turkey in 2016. He is currently an M.Sc. student in Ankara Yildirim Beyazit University, Institute of Science. He is currently working as Scientific Programs Assistant Expert in TUBITAK, Department of Information Technologies, Directorate of Information Security. His research interests are Information Technologies (IT), Digital Forensic, Cyber Security, System and Network Penetration Tests, Security Information and Event Management (SIEM), ISO/IEC 27001 Information Security Management System (ISMS).

İlyas ÇANKAYA has been working at the Department of Electrical and Electronics Engineering, Ankara Yıldırım Beyazıt University, Turkey. He received his PhD degree in 1998 from The University of Sussex. His current research interests include Control Systems, Nonlinear Frequency Response Analysis, Signal and Image Processing. He has two books and more than 75 publications.

Baha ŞEN received the Ph.D. degree from Gazi University. He is an Associate Professor with the Ankara Yıldırım Beyazıt University, Turkey. Previously, he was a academic member with Karabuk University. Also He worked for Logo Business Solutions, Havelsan as a software engineer. His research interests include the software engineering, parallel programming, gpu optimization, image processing, signal processing and advanced data mining. Assoc. Prof. Şen is member of the IEEE Computer Society.

