The Journal of International Scientific Researches
2019, 4(3)

Review of Mobile Malware Forensic

Mobil Zararlı Yazılımların Adli İncelemesi

Abstract

Developments in the world of information technology have brought security needs, ethical and social responsibilities, risks and inconveniences. The dramatic increase and spread of smartphone usage, especially in line with advances in mobile technology, has led to an increase in IT crimes committed on smartphones. The increase in the processing of information crimes via smartphones has necessitated the investigation of informatics crimes and produced many analysis softwares&methods. Particularly in Turkey, by the usage of ByLock and Eagle apps by FETO criminals, mobile forensic became the most important proof of evidence of being a member of the terroristic organization. Afterwards, it was discovered that the malicious software was infected to some of nun-member suspects' mobile phones by Morbeyin operation which was discovered and revealed by mobile malware forensic experts. Thousands of innocents have suffered because of this malware. This kind of threats is also considered to have some negative impact of m-government solutions and development. In the field of forensic crimes, there has been a subcategory of investigation of smart phones and mobile phones. In this study, the important details about the examination of smartphones within the scope of forensic computing are analyzed by comparing various mobile software, applications and studies.

Öz

Bilgi teknolojisi dünyasındaki gelişmeler yeni güvenlik gereksinimlerini, etik ve sosyal sorumlulukları, riskleri ve tehditleri de birlikte getirmiştir. Özellikle mobil teknolojideki gelişmelere paralel olarak akıllı telefon kullanımının çarpıcı şekilde artması ve yaygınlaşması, akıllı telefonlarda işlenen bilişim suçlarında bir artışa neden olmuştur. Bilişim suçlarının akıllı telefonlar üzerinden işlenmesindeki artış, bilişim suçlarının araştırılmasını gerekli kılmış ve bu kapsamda birçok analiz yazılımı ve yöntemi üretmiştir. Özellikle Türkiye'de, FETO suçluları tarafından ByLock ve Eagle uygulamalarının kullanılmasıyla, mobil teknik tahkikat, terör örgütüne üye olmanın en önemli kanıtı olmuştur. Ancak daha sonraki süreçte örgüt üyesi olmayanların telefonlarına da bulaştırılabildiği adli bilişim uzmanlarında ortaya çıkarılan Morbeyin anlaşılabilmiştir. Binlerce masum vatandaş bu zararlı yazılım yüzünden büyük sıkıntı çekmiştir. Bu tür tehditlerin, m-devlet çözümlerinde ve gelişiminde bazı olumsuz etkilerinin olabildiği düşünülmektedir. Adli bilişim suçları alanında, akıllı telefon-ların ve cep telefonlarının soruşturma alt kategorisin oluşturulmuştur. Bu çalışmamızda, akıllı telefonların adli analiz kapsamındaki incelemesiyle ilgili önemli ayrıntılar, çeşitli mobil yazılımlar, uygulamalar ve çalışmalar karşılaştırılarak sunulmaktadır.

Ahmet Efe
PhD, CISA, CRISC, PMP, Ankara Development Agency, Ankara
Turkey
e-mail: icsiacag@gmail.com

Ayşe Nur Dalmış
Department of Computer Engineering University of Yildirim Beyazit, Ankara, Turkey
e-mail: aysnrdalmis@gmail.com

Article Type / Makale Türü
Research Article / Araştırma Makalesi

Keywords
Mobile forensic, digital forensic, malware, mobile world, m-government security.

Anahtar Kelimeler
Adli bilişim, dijital tahkikat, kötü amaçlı yazılım, mobil dünya, m-devlet güvenliği.

JEL: H12, K14, K22, M15, O32

Acknowledgement
Manuscript received August 12, 2018; accepted Nov 16, 2018.
DOI: 10.17694/bajece.419538

Submitted: 16 / 05 / 2019
Accepted: 10 / 10 / 2019

Introduction

Smartphones have come out of being only communication tools and have become an alternative to computers thanks to the innovative hardware and software features that are increasing day by day. Governments are also encouraging usage of mobile government applications in order to decrease transaction costs and increase the level of satisfaction of citizens. In today's technology world, users can easily do all kinds of operations with computers through smart phones. The convenience provided by mobile technology has also brought new security risks. The use of smartphones and social media has increased, causing the increase in information crime and victims. With the malicious software for smartphones, the bank account information of the people can be

accessed, the personal information (picture, video) can be accessed without permission and the e-mail address of the person can be seized and e-mail can be sent to other users. Today more than 70% of committed crimes are related to mobile device crimes. While smartphones are closely related to such a large percentage of crimes committed, investigations of information crimes have become so important.

The introduction of mobile devices into every aspect of our lives has made it easier for our lives and other positive consequences as well as difficulties to control. Especially in 2005, the rapid increase in the use of smartphones caused criminal offenses to have a large share in other committed crimes. Mobile applications exceeding millions have added to my life convenience, fun and enthusiasm, while also introducing serious security threats. Even with a simple application you download, this malicious software can infect your device and sometimes it can be applied to your system with a mailed attachment and sometimes a downloaded file when you click a link. In this study, malware analysis will be performed on mobile devices with forensic hardware and software (Ganesh&Chakrabarti, 2017).

Mobile government applications have been put into use so that citizens can access and benefit from the services provided by Public Institutions and Organizations anytime and anywhere without the time and space restrictions. Mobile Government applications aim to enable citizens to access the information needed by a wide range of telephone support, even where no computer is available.

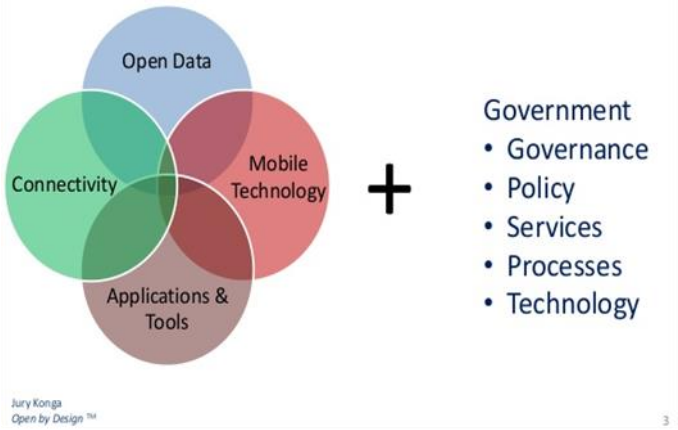

Fig 1. M-Government Key Infrastructure Components
Source: Konga, J., (2013)

Mobile government applications can be accessed in two ways. These are the WAP page that you can access with the installed internet browser on your phone and the other is the JAVA application you can download to your phone. The WAP page can be used with any mobile device that has a WAP browser with XHTML support. In addition, it is also possible to use with devices (PDA, SmartPhone etc.) which include a standard web browser. Java application is supported by all mobile phones, which can run Java applications and support MIDP 2.0 and CLDC 1.0 protocols. All mobile government applications in Turkey with internet connection is available only via the operator, for safety reasons the wireless network (WLAN) connections over are blocked (Seo& Lee&Yim, 2012)

1. Mobile Devices and GSM Technology

1.1. Mobile GSM History

GSM is a worldwide cellular system primarily designed by Ericsson and Nokia in Europe.28 The basis of mobile communication technology has been launched in the 1980s and is a communication protocol called the Global System for Mobile Communications. The mobile communication protocol we call the global communication network was approved by the EU "European Union" in 1982. Priority European Telecommunications Standards Committee-Group Speciale Mobile has been known as a global name after the sub-organization name has moved on

GSM. As of today, the most common mobile phone communication standard is used by 2 billion people in 212 countries.

In 1988, standards were set by the EU and in 1990, 1800 Mhz frequency was adhered to the GSM network by the UK proposal. For the first time with GSM technology, on July 1, 1991, Finnish Prime Minister Harri Holkeri made his first GSM call with equipment provided by Nokia via the local GSM operator Radiolinja.

In 1989, this technology was accepted by the EU as the international global communication network standard. It started with an interview over GSM 1900 frequency. The 1900 band was added to the 800 and 900 Mhz GSM bands by the USA. Japan has used its own systems that are not compatible with GSM technology despite these developments. More care have be given when using smartphones as all smartphone users can become a part of the informed conscious or unconscious act of crime (Ganesh&Chakrabarti, 2017).

In this study, the "mobile devices" function was used in the sense of "smart phones and mobile phones" in order to use a plain and clear narration without any sense of confusion.

In Turkey, 1G (NMT) and 2G have been widely used and the first GSM meeting was held between the Prime Minister and the President on 23 February 1994.TURKCELL has started to serve for the first time in our country. Since then, various generation GSM technologies have been used. On September 10, 2007, the Ministry of Transport opened 3G tender and the license was purchased. With the use of 3G and 4G, smartphones have started to be used and the number transfer between operators "TURKCELL, AVEA and VODAFONE" have begun (Usom, 2014). Turkey has already started to develop the super internet infrastructure of 5G which is very crucial for IoT, smart city and industry 4.0 applications.

In the first generation systems called 1G, analog data stream is used. Numerical data streams are used in second generation systems called 2G.Refers to networks that include packet-based data communication (GPRS, EDGE) in addition to circuit-switched systems in second generation systems called 2.5G. GSM is a second generation system that falls into the 2G and 2.5G categories. With the third generation system called 3G, faster data transfer and more efficient use of bandwidth have been possible. With the fourth generation system called 4G, it is expected that the problems that cannot be solved with 3G, especially the coverage area, will be solved. Usage of mobile devices is increasing dramatically. As is seen in the fig. below, the mobile market is becoming of the leading sectors in the global economy.

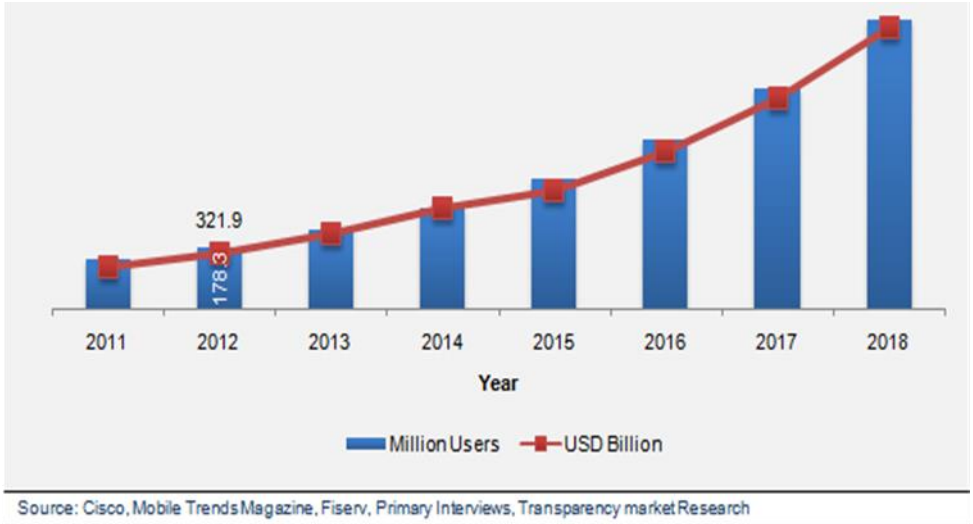

Fig 2. Global Mobile Wallet Market, 2011-2018 (million users) (USD Billion)

As the usage of mobile phones is increasing the mobile payments are also increasing as the percentage of usage.

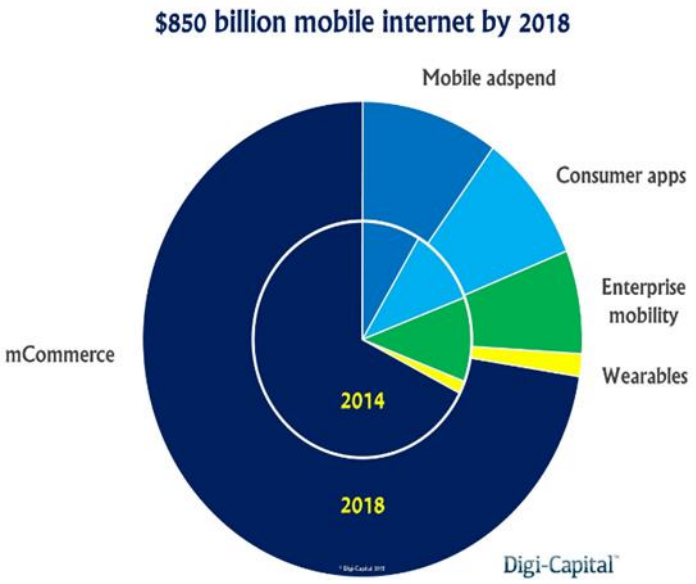

Fig 3. $ 850 Billion Mobile Internet by 2018
Source: https://www.digi-capital.com/reports/#augmented-virtual-reality

As is demonstrated the fig.3 above, in comparison with 2014, mCommerce is dramatically increasing. This brings new threats and risks to be associated with usage of mobile devices since the trend of breaches is surely increased by mobile apps and mobile malware. This tendency requires the security experts focus on the structure and development of mobile hardware and software to find vulnerabilities and countermeasures against threats exploiting open vulnerabilities.

1.2. Mobile Device Hardware and Operating Systems

Smart phones are small, battery-powered lightweight devices that are designed for Mobility. Many mobile devices have a number of comparable features. They include a microprocessor, read only memory (ROM), random access memory (RAM), radio module, digital signal processor, G sensor, microphone and speaker, interfaces with various hardware keys LCD screen is available.

While a mobile device operating system can be stored in NAND and NOR memory, transaction execution and functionality take place in RAM. Thanks to its internal SD memory card slots, there is memory support available that can be up to various capacities. The availability of non-cellular wireless (infrared, bluetooth, Nfc) and wireless networking (Wi-Fi) makes it possible to share a wide variety of data types (graphics, audio, video and various file formats).

Different mobile devices have different technical and physical features (size, weight, and processor speed and memory capacity. Mobile devices can offer a variety of expansion capabilities to provide additional functionality. Mobile devices also include global positioning system (GPS), cameras (photo camera, camcorder) Etc. In general, the primary purposes of a mobile device may be classified as voice and message communication, but also as a feature phone or a smartphone with more advanced features and multimedia services similar to personal computers.

In addition to voice and message communication protocols, smartphones also support applications such as phone book and calendar, which are PIM-Personal Information Management (PIM) applications, and run applications that serve a wide variety of general and very specific purposes, similar to personal computers. Smartphones are physically larger, supporting higher video resolution and have a touchscreen feature. Smartphones support running a wide variety of applications that can be downloaded with an app store tool. For example (Google Play vs.)

Normally telephones use closed operating systems with documentation. Several companies specializing in embedded software offer real-time operating systems for mobile device manufacturers. Smartphones can use any proprietary or open source operating system. The operating systems commonly used on smartphones are as follows: Android, IOS, Windows Phone, Blackberry, Symbian, WebOS. Unlike normal telephones, these operating systems are full-featured

systems with advanced simultaneous multi-tasking capabilities that can capture the capabilities of advanced mobile devices. Many smartphone operating system manufacturers offer the software development kit (SDK-Software, Development KIT) together.

There is software on the whole electronic device that provides control of the equipment and fulfills the commands. Technology needs to be controlled with more sophisticated software technology. Over time, devices that work with very simple software have now become more sophisticated software systems.

1.2.1. Android

Open Handset Alliance (OHA) is an open source operating system written by Google and based on the kernel of Linux (2.6 kernel).

Android Operating system versions are marketed with android Market and can run on many applications with multi-touch, multitasking and flash support. The Android operating system consists of system libraries, kernel, application development frameworks and built-in applications.

The Android operating system uses Linux kernel for kernel. The codes and libraries added for Android are distributed free / under the General Public License (GNU).

The Linux core directly provides direct input to device drivers and input-output operations for connection with the underlying security, process and memory filing controls. The main areas customized for the Android kernel are shared memory and power control.

The most important structure of the Android architecture is the libraries written in C programming language. System libraries are listed below;

- Webkit for the operation of Internet browser engines,
- Surface Manager created for imaging,
- OpenGL, which performs graphics operations,
- Media Framework, which performs audio and video operations,
- SQLite that controls and regulates data structures

Runtime layer is the layer where the Linux kernel libraries are combined with Java, and there are two important components. One of them is the basic Java libraries, and the other is the Dalvik Virtual Machine.All applications on the mobile phone are executed by the virtual "Dalvik Virtual Machine". Java applications are compiled, the Java code is compiled into Bytecode files and these files are translated into a dex file to compile the Dalvik Virtual Machine so that it can be understood / run (Grace at. Al, 2012).

The Android operating system supports GSM, 3G, Bluetooth, EDGE and Wi-Fi connections as mobile communications for data storage purposes. Android is based on open source WEB KIT application framework. It supports many multimedia, audio, picture and video file formats (MPEG-4, MP4, MP3,H.264 and AAC, AMR, JPEG, PNG, GIF, etc.).Android operating systems recognize the ease of application developers with its advanced Application Programming Interfaces (APIs). Examples of Android APIs that have Java as an application development language include face identification and various applications. Java developers can easily android-compatible applications because Java integrates successfully into the Android Operating system. The Android Developer Kit (SDK), the Java Developer Kit (JDK), and the Android Developer Tools Chip for Eclipse (ADT-Android Development Tools Plugin) are sufficient.

1.2.2. IOS

Mac OS X (Unix variant) operating system developed by Apple company. It can only be used by devices manufactured in the Apple family. The applications developed by the third parties in their initial versions were not supported. Then, this version of the released version of the closed attitude has been abandoned. Modify kernel and system libraries according to ARM processor. IOS basically consists of 4 layers. These layers are Core OS, Core Services, Media, and Cocoa Touch layers.

Core OS layer is the base layer of the operating system. Other layers are built on these technologies. The layer closest to the hardware layer. Kernel, drivers, low-level interfaces, security features, all devices that can be connected to the device, accessories are routed to the Core OS layer. (Grace at. Al, 2012).

The services required for the operation of the applications are in this layer. The Core Component Framework, which manages user logins, SQLite, which is a storage library, Core Location Framework, which manages domain location and location processes, Address Book Framework, which manages address books, Core Telephone Framework, which provides APIs for basic phone operations, System Configuration Framework Is a Core Services layer that enables transactions.

Compose libraries on the phone that are related to audio, video and video operations. Core libraries such as Core Graphics, Media Player, Core Media, Core Audio, Core Video, and OpenGL are important for iOS. Cocoa Touch layer is the application layer in which high-level system services include important services such as touch screen, feedback, and simultaneous multi-tasking.

Smartphones have two processors. Some of these are features of the phone like a computer; while the other is used to manage the base station and operator related operations of the phone. To take smartphones as a combination of a phone and a computer, there is a need for a processor for both the phone and the computer. These processors are called Application Processor and Baseband Processor.

The Application Processor is the processor that is used to carry out phone communications and processes outside of GSM. All applications and control of the operating system are provided by this processor. The Base Processor is also known as the Communication Processor. The GSM-antenna is the processor that performs the required operations. This processor has its own RAM and NOR flash storage. To unlock a device that has a SIM lock, you need to process the Baseband firmware.

Storage NAND flash on iOS, which has two partitions: the first part contains user files and the second part contains system files.

System Part: The part where applications belonging to iOS operating system and operating system are located. The system partition is read-only. An Applications directory appears when you SSH an iOS device and go to the root directory. Applications in this directory include applications in the system partition. Messaging, phone, maps etc. Operating system applications such as this are on this list.

User Part: On the devices, the writable partition under the / private / var directory is known as the user partition. Under the User directory (/ private / var / mobile directory) there is also the application "Applications" directory. In this case, there are applications that the user has installed. Third party applications are kept here. Every application installed on the phone is loaded in a unique directory called UUID. When / private / var / mobile / Applications is accessed.These files can be seen. The name of this directory / folder where the applications are installed is dynamically created during installation at every install. When these applications are removed from the device and re-installed, the directory name changes. Thus, it was tried to prevent the attackers from making a conclusion about the applications (Grace at. Al, 2012).

Users: There are basically two users in the iOS operating system. These are defined as root and mobile. Root works with iOS authorized user right. If the user is a mobile named user, all operations except the operations performed by the root user are called low authorized with the user. All running applications are assigned to mobile group and mobile user. All applications on iOS are run with the mobile user. On the contrary Android applications are run with each new user. However, for this reason, it is very important that the "sandbox" mechanism works correctly, and if all the applications are created with the mobile user as a problem that can occur in the sandbox mechanism, the result of accessing all applications by another application will come out and endanger the security of the phone.

2. Types of Digital Evidence That Are Likely to Be Found on Mobile Deviceshones (PDAs, PALMs, PocketPCs, etc.).

Such devices are mobiles that run small and unique operating systems on them and have data storage units. They may contain a variety of data in external and internal data storage units which may serve as evidence according to the characteristics of the devices. The storage of these devices is very flexible and they can use additional memory cards that are open to development.

On PDA mobile devices:
- Address and phone information
- Task and To-do list
- Personal notes, documents
- E-mail and Chat Recordings
- Voice recordings
- Deleted data (in some cases)
- Other files if connected to the

PC on PALM and POCKET PC:
- Documents, Word processor files, images, audio and video files
- Small database files, database access records
- E-Mail or chat records, Internet History.
- Access passwords and user names.
- Deleted files and deleted disk areas.
- Encrypted or Encrypted files
- File privileges and dates (creation, access, deletion, etc.)
- System Registration information (Registery, Temp Log, etc.)
- Virus, Trojan, SpyWare, etc., such as malicious software.
- Software installed on the system
- Address and phone information
- Task and to do list
- Mobile phone messages (if GSM feature)
- SMS records (including deleted)
- GPRS and GPS access logs

Some of these devices have modular access to wireless computer networks and can be used very easily to commit an information crime. In this direction, an investigation will be performed and it will be healthy to search for evidence-based digital data.

On Mobile Phones:
- Address and Phone information
- Personal information, Notes Calendar entries
- Message details, Deleted Messages
- Last call list (Missed, called, dialed)
- Wap, GPRS history, Internet Access log
- Picture, Video and Voice recordings, Memory cards, if available

The digital evidence that can be obtained from mobile phones is of great importance in the connection of the crime in the investigation of the crime. Forensic IT science in the memory of mobile phones and on sim cards is newly developed but it is possible to conduct scientific studies.

3. Security Threats on Mobile Devices

The use of mobile communication has been increasing day by day, leaving behind all the communication and computer technology systems before it, and it has become a simple communication tool. Moreover, it has been realized that information security is not only a technology problem, but human factors in cyber space in recent years have also been the subject of information security research.

In Turkey, some terrorist organizations or underground structures are also included in security breaches of mobile phones. Many government staff have been ousted and captured after the 2016 July 15 coup attempt due to their IP signals from Bylock servers which were later captured from Lithuania by government cyber army. This software built by FETÖ members as an internet-based encrypted messaging program was produced in Turkey. The program was written before the 2014 High Council of Judges and Prosecutors (HSYK) elections and all members of the organization were instructed to use the application after December 17-25. Designed for both Android and iOS-based devices, the program can only be downloaded from sites containing jailbreak applications to desktop

computers., this application cannot be downloaded directly to the phone from Apple Store and Google Play. To download the application, an invitation must be sent by the FETÖ member. So it was very clandestine just to their secret network.

The Ankara Chief Public Prosecutor's Office had announced that FETÖ's Purple Brain software has identified that 11,408 GSM users are routed to ByLock IPs against their will. After the release of the ominous trap by mobile forensic experts, thousands of innocent people were released from prisons throughout the country. This is an outstanding example of high level of mobile risks and threats in the history.

Here are the example applications prepared by FETÖ's Mor Beyin software team that developed 8 programs to install bylock on people's mobile phones as follows;

1- Best Free Music (Search & Play) (Java class name com.morbeyin.freezy.en)
2- Freezy-Find Music Listen (Java class name com.morbeyin.freezy.tr)
3- Freezy-Play Free Music Online (Java class name com.morbeyin.music_player_best)
4- Mor German English Dictionary (Java class name com.morbeyin.english_german)
5 - Cheapest Price (Java class name com.kimeneki.enucuz)
6 - Purple German-Turkish Dictionary (Java class name com .morbeyin.alman ACE)
7 - Music Search-Beta (Java class name com.morbeyin.music_play)
8 - Araba2.Co I (Java class name com.araba2)

If you downloaded these programs to your mobile phone before you know define the vulnerability every time you use the program in the background the morbeyin server connects you to the Bylock server. It is very dangerous and many people have taken to jail for more than 6 months just to wait for mobile malware forensic investigations to be completed.

Environments where digital evidence for a mobile messaging application found can be evaluated in three different classes. These are;

- Devices used by the user (end-user devices such as mobile phones, computers, etc.)
- Network components used for accessing the relevant messaging environment (network components operated by GSM operators and / or Internet service providers and allowing users to access the Internet)
- Mobile messaging application that is running the server portion of usually located on the internet and application servers.

The hardware and operating systems of mobile devices have almost reached the same capacities and capabilities as those of computers and the increasing functionality and capacity of these devices have made it possible to start many processes in the computer environment with these devices and to protect the personal / institutional data from unauthorized access. For this reason, especially in the field of mobile information security, there is a great demand for researching human factor and perception.

Major threat methods in the field of mobile devices are manifold. We can summarize them under the headings of malware, direct attacks, data interception, exploitation and social engineering. Apart from these, the main and most important are the security weaknesses caused by the lack of sufficient technological knowledge of the users.

As innovative technology develops and spreads, day-to-day work is carried to electronic environments and information becomes easy to access, making it a top priority. As a result, the security of the information contained in the digital environment has increased in importance and threats, in numbers, quality and variety. We will try to explain the main threat methods in the following headings.

3.1. Malware

Malware and spyware software are threatening threats to smart devices. It is important for users to know and recognize these software and its effects, and it is necessary to take the necessary precautions.

Malicious software, malware, is the name given to all malicious software known as viruses, worms (worms), trojans and spyware. It is possible to disrupt the running of systems or to disable them at all by accessing the infected systems via the network.

The names of these software are "worms", "trojans", viruses, spam, rootkits, keyloggers, spyware, browser hijacking Are common malware. Almost every programming language can be written and infected with many file types.

3.2. Direct Attacks

In this method, called Direct Attack, an attacker aims to obtain unauthorized access and information using a known application vulnerability or operating system vulnerability.

This type of attack uses the most SQL injection (SQL injection) and service vulnerability methods that accept external connections. If mobile devices are connected to the Internet through a wi-fi network that has been opened for general use, and if the software is internetworking with a software such as a hotspot, the attacker may be the target by detecting the IP by an attacker very easily.

It is possible to attack Dos (Denial of Service) which is known as a service disruption to these devices and the device can be made unusable. Or you can run an application where the device is not aware of what the background user is spending.

Disabling SMS service is an example of a DoS attack. For this you need to obtain certain mobile phone numbers and there are different ways of doing this.

DoS attack can also be performed using Bluetooth technology (detected by sniffing bluetooth signals). Below are the types of attacks that can be performed via Bluetooth.

BlueJacking: Seize the device by sending an anonymous message or data to another user in the coverage area. The purpose is not to hurt.

BlueSnarfing: The purpose is to capture phone book, e-mail and text messages via bluetooth without the user's knowledge and without permission.

BlueSpam: The process of sending unnecessary advertising messages via Bluetooth. Sending is done using OOP (Obex Object Push) and / or OBEX-FTP (OBEX File Transfer Protocol) (Murynets & Jover, 2012).

3.3. Data Communication Listening (Data Interception) and Spyware

Another major threat in mobile devices is data interception. In this method, the packets on the network are collected and analyzed, the network is infiltrated and the data is seized.

In some cases, the easiest way to attack a mobile device is to perform an indirect offensive attack. All mobile devices are now compatible with other devices such as Wi-Fi, 3G, and bluetooth and so on. It can communicate with the technology. Wi-Fi connectivity poses a threat to smart devices. Nearly 90% of smartphones with Wi-Fi capabilities have a known danger of Wi-Fi sniffing and interception.

Since the connections to people and institutions using this technology are not secure, all information needs to be encrypted. Workings have shown that once a mobile device connects to a Wi-Fi network, it makes it sensitive to man-in-the-middle (MITM) intervention.

Particularly in the communal Wi-Fi areas, the threat of intervention in communication is more likely. The best way to secure Wi-Fi network connection is to use technologies such as Wi-Fi Protected Access 2 (WPA2). In this way, the network can be securely connected and the data can be encrypted to provide secure communication.

Spyware is also software for monitoring and recording all data and movements on the device without user permission. These software, which is called “malware” in the IT sector, is the fearful dream of many individuals and institutions. Data that may not be seen by others on your device may be transmitted to other people or persons through this spyware. If there are movements on your mobile phone that catch your attention and are out of control, it is highly likely that this is ”Spyware”. Although there are many answers to the question of how to install on my device, the most common reason is the permissions you have given to an application that you do not know and trust. With these permissions, the program allows you to actually control all the data on your phone. These software that users install on their mobile phones for unknown reasons bring together many negative results. Detection of such malicious software can be detected by forensic experts. If there is any data that you suspect is in the possession of someone else, we advise you to consult a frensic specialist immediately. So, what can cause negative consequences to the information in your mobile phone?

- Picture Files,
- Banking information,
- Video Files,
- Messaging data,
- Guide Information,
- Social media activities and information,
- Listening to the interview records,
- Switching the device camera on and off in the background, etc.

All activities can take place and your private data can be passed on to others.

4. The Various Types and Methodologies of Evidence/Data Collection in Mobile Forensic

Although it is important to understand acquisition techniques and methods with Mobile Forensic Software, a forensic expert needs a variety of tools to complete the task on time. Forensic tools not only save time but also facilitate the process. Today, many tools such as Elcomsoft iOS Forensic Toolkit, Cellebrite UFED, BlackLight, Oxygen Forensic Suite, AccessData MPE +, iXAM, Lantern, XRY, SecureView, Paraben iRecovery Stick are used to examine mobile devices. Almost all of these software support the following features.

- Supports logical acquisition.
- Enables password capture.
- Can read backed up data.
- With a timeline, data can be accessed in a single region.
- It leaves no trace or change after the procedure.
- Automatically recovers deleted data.
- Provides access to raw files for manual analysis.
- Provides a user-friendly interface.
- It has keyword lists and library features for searching.
- The report can be presented in various formats (Microsoft Excel, PDF, HTML, etc.).

There are several methods that can be used by forensic IT specialists when trying to collect evidence from a device, but the most obvious methods of data collection are:

- Manuel
- Logical
- File system
- Physical
- Brute force

Each of these types of data collection has its own advantages and disadvantages, as well as the conditions to be used. We will look at each of these methods separately and give a brief explanation of when a forensic expert is likely to use a particular type of acquisition method.

4.1. Manual Data Collection

Manual data collection is used when a mobile device is functional and not encrypted or physically damaged and no special software or software tools are required as the device can be navigated through the graphical user interface (GUI). Content, such as images, documents, call records, or other data and features accessible to the user, can be viewed by the researcher. In most cases, screen captures are captured from the device via the digital camera or video adapter to an external display using image capture software.

This is not necessarily a comprehensive detection method because unreadable data to the operating system of the device will not be accessible to the investigator during this process. Deleted items cannot be recovered at this level, which means that more technical methods should be used if this is a requirement. When the investigator uses the mobile device in this way, there is a risk that data may be compromised by accidentally deleting files or changing timestamps.

Another critical factor is the time-consuming nature of manual data collection. This is because a researcher must manually tackle potentially large data stores and manually capture a screenshot of each piece entered in the evidence. In cases where there are several hundred pictures, e-mails or

messages, it becomes clear that a large amount of time is required to complete a meaningful investigation. For these reasons, a forensic researcher can only use this method as a last resort when all other means are already exhausted.

4.2. Logical Data Collection

This method involves connecting a mobile device to the forensic researcher's workstation with a wired USB, Lan, or RS 232 connection. Depending on the researcher's requirements and the capabilities or limitations of the device under investigation, wireless connections such as Wi-Fi, IrDA (infrared) or Bluetooth may also be used. Each method uses its own communication protocol and can package the data differently to transmit the data of the mobile device at the bit level.

Each mobile operating system has an associated SDK (software development kit) that forensic researchers can install on their workstations. The SDK provides manufacturer-level access to the hardware and software of the mobile device, because it interacts naturally with the mobile device's API (application programming interface) and means that it will respond to commands issued remotely from the forensic workstation.

This method is especially useful when you need to review SMS, MMS and call histories. The researcher can remotely load the operating system-specific forensics into the device and run forensic reports in a variety of formats, such as CSV or XLS format documents that will not affect the file structure of the mobile device. These are human readable documents and excellent sources of information. Where SMS or text messaging data needs to be reviewed, document fields can include the time sent, received time, status (read or unread), message size, message content (what is said in the message), protocol, and more. Forensic application installed on the device can be removed after review and evaluation is complete without affecting the integrity of the mobile device.

4.3. File System Data Collection

This method is an excellent way to recover deleted files from a mobile device. In most digital systems, a deleted file is usually not deleted at all, but a flag is assigned to the system indicating that it can be safely overwritten. When this overwrite occurs, depending on many factors, the actual file varies depending on how much data is copied to the device after the file is deleted and the writing efficiency of the marked data occurs.

Android and IOS devices share a common database structure based on the SQLite schema. The synchronization interface determines whether a file is ready to overwrite and is responsible for marking deleted items. If forensic researchers can successfully access them, they can potentially copy these "deleted" files, such as browser history, images, messages, and many other items of interest to do more research from the mobile device.

4.4. Physical Data Collection

Physical data collection is a bit by bit copy or clone of the file system and directory structure of a mobile device. It can be thought of as a hard disk copy of a normal computer system. Once this data has been copied, it can be indexed with expert forensic tools. For example, if instant messages are a field that a researcher is interested in, these tools can compile all messages in different instant messaging applications into a regular, logical list for the researcher to start searching for.

This method is advantageous because the risks associated with data integrity are compromised, which can be completely avoided by using a write blocker in the interface used for copying. However, some details need to be addressed when using logical data collection. When the status of a message needs to be determined (read or unread), the investigator should ensure that the copying method used does not change the marked state of the message and that the forensic tool used in compiling and displaying is used. The message can also maintain this message status.

Another critical factor is the timestamps of the files in question. All must comply with the timestamp of the mobile device and must not be regulated by judicial means used in the copying process or investigation. Problems when the date and time of the copy process changes the original timestamps of the mobile device under review and this can seriously impede the progress of a judicial investigation.

4.5. Brute Force Data Collection

This method mostly refers to a password or password enforcement action and is very successful where relatively small number combinations are required. Many phones have a four-digit PIN that ranges from 0000 to 9999. This means that there are 10,000 possible combinations to be predicted by the forensic investigator, and most mobile devices have a security feature that locks the phone completely after the threshold.

A device must be connected to the investigator's workstation and started in bootstrap or equivalent mode. An application on the workstation then mounts the file system of the mobile device, finds the encrypted password file, and starts the attack, or temporarily loads a mobile boot ROM specific to the mobile device itself, and uses the mobile device's CPU to perform the attack. In either case, this does not take too long, as the CPU can perform multiple attempts per second and can be as fast as a few minutes or a few hours, depending on several factors.

5. Phases of Digital/Mobile Forensic Investigations

As is similar with the digital forensic phases, mobile forensic requires certain steps be followed such as intake, identification, preparation, isolation, processing, verification, documentation, reporting, presentation and archiving. The tools that are being used for mobile forensic should provide those phases to be followed.

Table 1. Phases and Descriptions of Mobile Forensic

Phases	*description*
Intake	entails request forms and paperwork to document ownership information and the type of incident the mobile device was involved in, and outlines the type of data or information the requester is seeking
Identification	identifying the legal authority, The goals of the examination, The make, model, and identifying information for the device, Removable and external data storage, Other sources of potential evidence
Preparation	research regarding the particular mobile phone to be examined and the appropriate methods and tools to be used
Isolation	Network isolation is advisable. This can be done by placing the phone in radio frequency shielding cloth and then placing the phone into airplane or flight mode.
Processing	If physical acquisition is not possible or fails, an attempt should be made to acquire the file system of the mobile device. A logical acquisition should always be obtained as it may contain only the parsed data and provide pointers to examine the raw memory image.
Verification	Verify the accuracy of the data extracted from the phone to ensure that data is not modified. All image files should be hashed after acquisition to ensure data remains unchanged
Documentation	Document Examination start date and time, The physical condition of the phone, Photos of the phone and individual components, Phone status when received—turned on or off, Phone make and model, Tools used for the acquisition, Tools used for the examination, Data found during the examination
Presentation	Findings should be clear, concise, and repeatable. Timeline and link analysis, features offered by many commercial mobile forensics tools, will aid in reporting and explaining findings across multiple mobile devices.
Archiving	The data is retained in a useable format for the ongoing court process, for future reference, should the current evidence file become corrupt, and for record keeping requirements.

When identifying the appropriate tools for the forensic acquisition and analysis of mobile phones, a mobile device forensic tool classification system (shown in the following figure) developed by Sam Brothers comes in handy for the examiners (Murynets & Jover, 2012).

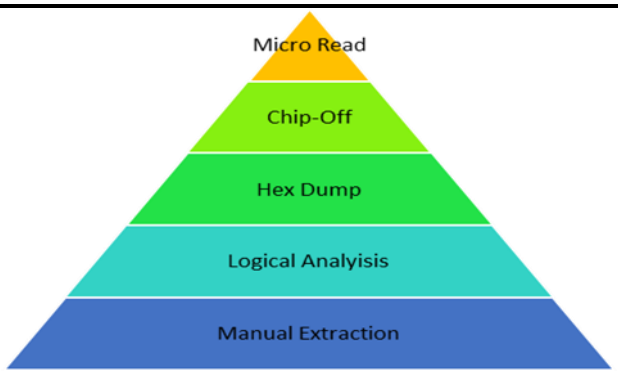

Fig 4. Cellular Phone Tool Leveling Pyramid
Source: https://www.sciencedirect.com/topics/computer-science/mobile-device-forensics

Starting at the bottom of the classification and working upward, the methods and the tools generally become more technical, complex, and forensically sound, and require longer analysis times.

Manual extraction involves simply scrolling through the data on the device and viewing the data on the phone directly through the use of the device's keypad or touchscreen. Logical extraction involves connecting the mobile device to forensic hardware or to a forensic workstation via a USB cable, RJ-45 cable, Infrared, or Bluetooth. A hex dump, also referred to as a physical extraction, is achieved by connecting the device to the forensic workstation and pushing unsigned code or a bootloader into the phone and instructing the phone to dump memory from the phone to the computer. Chip-off refers to the acquisition of data directly from the device's memory chip. At this level, the chip is physically removed from the device and a chip reader or a second phone is used to extract data stored on it. Micro read involves manually viewing and interpreting data seen on the memory chip. The examiner uses an electron microscope and analyzes the physical gates on the chip and then translates the gate status to 0's and 1's to determine the resulting ASCII characters.

6. General Properties of Mobile Forensic Software / Equipment

Tools like XRY, XAMN and XEC that seem to be fast, reliable and efficient solutions built to help forensic experts recover evidence from mobile devices in a forensically safe manner. Whether there is an unauthorized entry to a system and whether the initiatives are external or internal or if there is a problem, whether it is from the system or from a human source, this field provides "memory analysis, harddisk analysis, log analysis, Mobile forensics and image review "and personal information on the phone can be evidence in a forensic examination of voice calls and directory information. This will allow us to see what we can bring back under the system title, and of course we can see all the evidence and it does not mean we can save it.

6.1. Cellebrite

Founded in 1999 by a highly experienced team, a company makes great strides in the sector with mobile device technologies. The Cellebrite 'Universal Forensic Extraction Device' (UFED) software is both hardware and software capable of performing physical and logical deductions. Cable support is provided. Cellebrite supports more than 2,500 mobile phone brands / models (including GSM, TDMA, CDMA, iDEN) as of September 2010. In over a decade, CelineBrite's technology for analysis on mobile devices has technology that has a say in the market. It has been recognized by industry experts as "Best Phone Forensic Computing Review Hardware / Software" on the market: 2009, 2010, 2011, 2012.108Cellebrite is software that provides forensic information integrity guarantee with write-protected functionality provided by the mobile forensics industry. For the first time on more than 200 Android devices, it has the title of software that can perform forensic computing by bypassing the pin and password lock from the physical and file system. With advanced application solution capabilities, it can perform malware analysis with the analysis of Facebook, WhatsApp, Viber, Fring, Tiger Text, Waze, Skype, Google+ and more applications. Also many chipsets for mobile phones are produced in China and cellebrite The UFED Series police units are being used by

"military, police, intelligence" organizations and other institutions and forensic experts, with more than 30000 units deployed in 100 countries.

6.2. XRY

XRY computer software tools "can extract physical and logical data from SIM / USIM cards with more than 5000 different brand model mobile devices including GSM, CDMA, UMTS, IDEN and 3G phones Provides cable support XRY to Infrared (IR (IMEI), Subscriber Identity (IMSI), manufacturer's code, device time, and so on that specify the model of the connected phone after the connection establishment has been made. PC clock etc. Information obtained from mobile phone devices is stored in XRY format and cannot be changed but can be exported to third party applications. After a successful review, the following fields may be available in the information fields depending on the functionality of the phone: Screen summary, case given Contacts, Information, Contacts, Calendar, SMS, Pictures, Sound, Files, Notes, Tasks, MMS, Network Information, Video, etc. The data field contents can be seen. Also, after reviewing the graphics files, audio files and other data found on the phone, the enclosure can be exported and stored for further investigation. XRY is used by Police, Military, State Intelligence units and Forensic Computing Laboratories in 60 countries. This system consists of a PC for data analysis, a hardware device for connecting software and phones.

6.3. Oxygen Forensics Suite

This product is capable of physical and logical derivation. If evidence will be gathered from a mobile device for a case, the software that will help you and accomplish this process can perform Oxygen Forensic Software. The Oxygen suite is the most preferred forensic software by many agencies, law enforcement, tax, customs and other government departments in the UK, Germany, Australia, Sweden and Finland in many European countries.113 With its specific features, the device manufacturer, operating system, IMEI and serial number, Contacts, messages (e-mail, sms, mms), deleted messages, call records, calendar information, and scheduled tasks. At the same time, the file tracking feature has the ability and ability to obtain data in many formats that allow access and analysis of images, videos, documents and databases. When the Oxygen Forensic Software is run; when the 'Connect to new device' button on the menu bar is clicked and run, a helper wizard tool is launched and the device type is selected to start the forensic examination process.

6.4. EnCase Neutrino

EnCase, designed to conduct forensic investigation analysis for mobile devices, has over 30,000 licensed users of the encase software, which has become a powerful industry leader. With advanced hardware features, forensic analysis of the hardware of the most common mobile device manufacturers, including Motorola, Nokia, Siemens, Samsung, LG, Palm, BlackBerry, HTC, Sony Ericsson, UTStarcom brands and even more, is available. Encase solutions are designed to make mobile devices forensic computing operations become the industry leader. Unlike other software, the process starts with SIM and then continues with the device.

6.5. Android Debug Bridge (ABD)

This tool is a multipurpose command line tool that lets you communicate with connected Android-powered device. Throughout a forensics examination the investigator may come across and need to interact with debugging mode of the android platform to pull out some files or to check the value of a certain parameter. The ABD tools are also used by the majority of smartphones‟ forensic framework as the main subcomponent to communicate with the android platform. The ABD tool can be used to fulfil the data acquisition step.

6.6. Open Source Android Forensics (OSAF)

This tool is an open source unified android forensic that its main focus on investigating malware with in android applications. It follows a standardized process for forensic investigation and a set of best practices for analyzing Android applications OSAF can be used for forensic analysis and presentation of evidences steps (Osaf-community, 2015).

6.7. Andriller

This tool is a utility with a group of forensic tools for smartphones. Part of these bundled tools is specialized in android forensic. It performs read-only, forensically sound, non-destructive

acquisition from Android devices. It has other features, such as powerful Lock screen cracking for Pattern, PIN code, or Password; custom decoders for applications from android smartphones. Beside data acquisition, Andriller can also be used for data recovery, forensic analysis and presentation of evidences steps (Andriller, 2015).

6.8. AFLogical

This tool is an open source extraction tools, available on GitHub that can be used to extract calls, SMS, MMS, MMS parts and contacts from android mobile phones. It creates a directory named with time and date of extraction. It can be used for forensic analysis and presentation of evidences steps.

6.9. Whatsapp Extract

This tool is an open source tool for WhatsApp extraction and analysis. It's able to display in an HTML document of all WhatsApp messages extracted from an android phone and iPhone as well. Nowadays, WhatsApp is a wide used instant messaging application. This tool is specialized on forensic analysis and presentation of evidence that could be found on WhatsApp application.

6.10. Skype Extractor

This tool is an open source tool for extracting skype application data. It can be used to analyze skype application on an android phone. It can extract data such as Account info, contacts info, calls, chats, file transfer, voice mails and deleted and modified messages. This tool is specialized on forensic analysis, data recovery and presentation of evidence that could be found on skype application. Generally, Android Forensic tools should be able to investigate various types of data in the android smartphone.

6.11. Android Data Extractor Lite

ADEL is a forensic tool that has the ability to automatically dump selected SQLite database files from Android devices and extract the contents stored within the dumped files. It makes use of the Android Software Development Kit (Android SDK) and the ADB deamon to dump database files to the investigator's machine. It can recover and analyses the following data: Telephone and SIM-card information (e. g. IMSI and serial number), Telephone book and call lists, Calendar entries, SMS messages, GPS locations from different sources on the smartphone.

7. Malware Analysis in Mobile Devices

The growing number of smartphone users is becoming an attractive area for cyber criminals. Smartphones can be infected with spyware or malicious code, opening a photo in the email attachment, visiting the malicious code embedded web page, bluetooth connection, multiple multimedia messages and clicking on a link in the message. The most important reason why cyber criminals infect harmful code to smartphones lies in the aim of reaching banking ciphers.

In the past, hackers could get internet banking information (Bank account number and user password) by infiltrating the users' computers but nowadays internet banking and mobile banking transactions are made with disposable passwords transmitted via SMS except for the password that the user creates. When the hackers enter the bank sites from the malware infected computer to reach these ciphers, a new window is opened by the hackers that indicate that the malicious software is the bank's security practice. The user is required to enter the cell phone number, mobile phone brand and model information in this window. When the user inserts the desired information into the corresponding boxes and sends the form, an SMS is sent to the user's mobile phone and a message indicating that the virus is linked is displayed in the form of "SMS received link containing E-security certificate link, click link in SMS message to continue installation". The user who downloaded the application by clicking on the link in the message content is infected with malware on the mobile phone. The malware infected with mobile phones and the disposable SMS passwords are transmitted to a different mobile phone number.

In the example shown in fig. 5, a malicious message is displayed as if the malicious software was accessed from the infected system by the user accessing the bank site and the malicious software was coming from the bank.

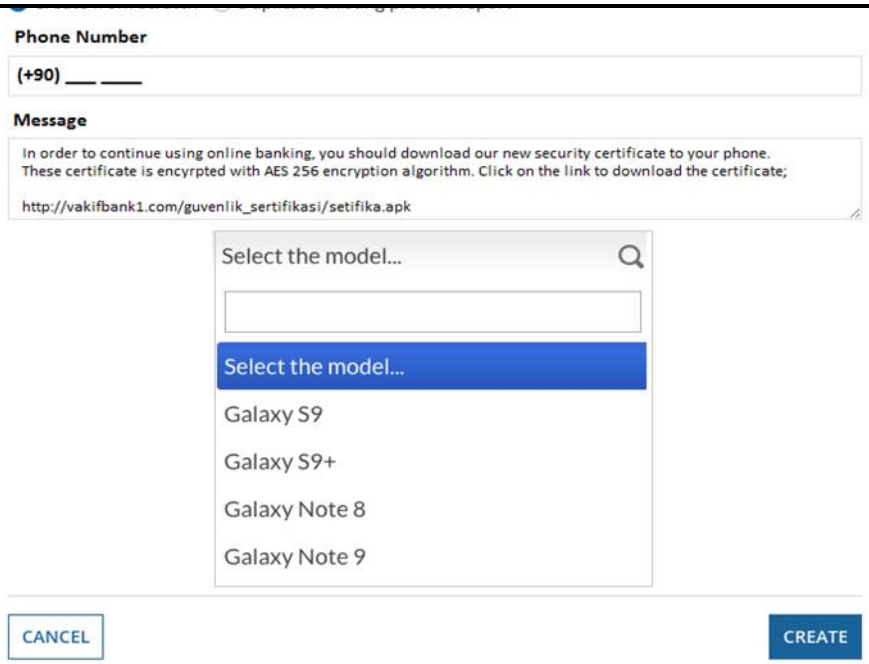

Fig 5. Fraudulent Message Shown to The User by Malware

The user is provided with a SMS containing a link to the mobile phone that when filling in the information shown in fig. 5 and pressing the create button.

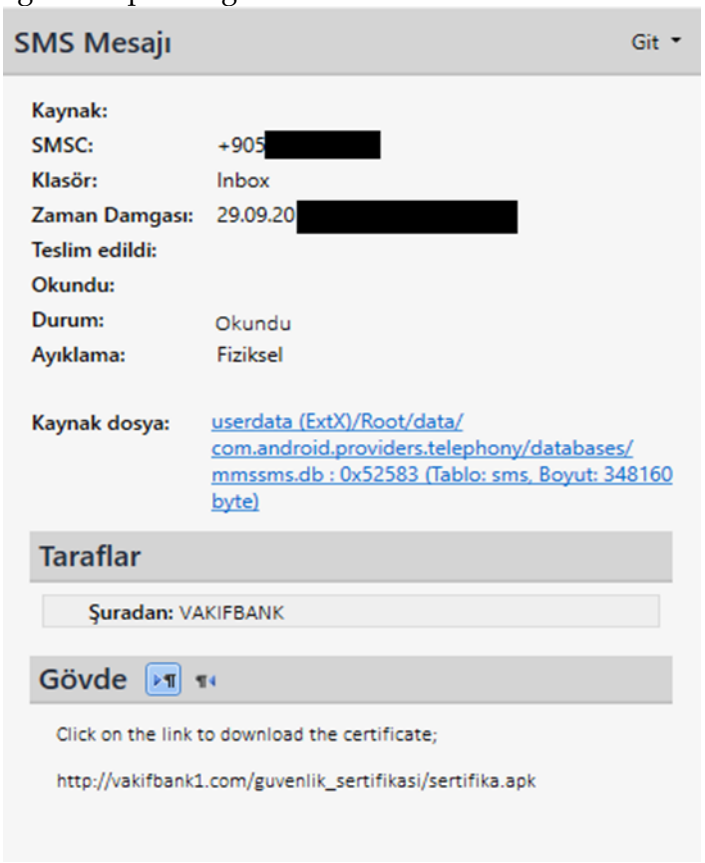

Fig 6. SMS Containing Malicious File Link Sent to Mobile Phone

When the user clicks the link provided by the SMS shown in fig. 6, the malicious software is downloaded to the internal memory or the memory card of the mobile phone.

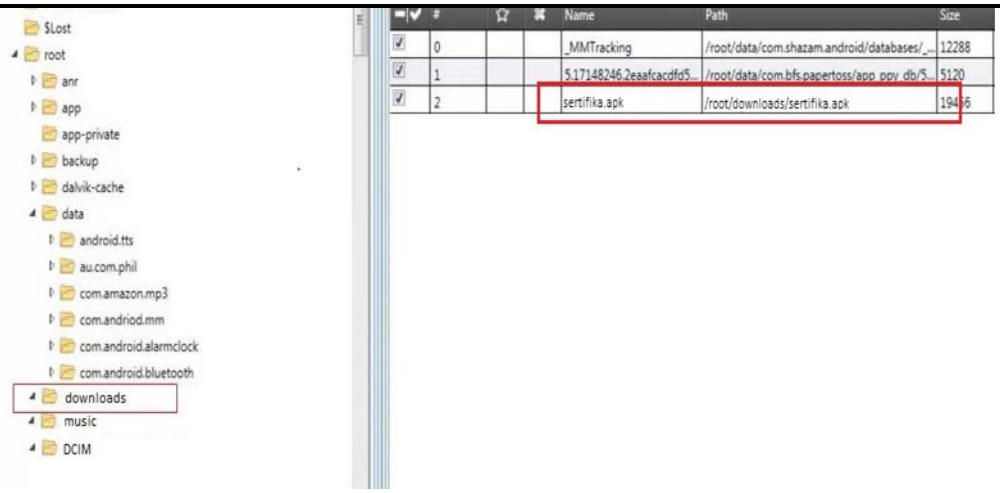

Fig 7. Records of Malware on The Memory Card

The malware scan on the physical output of the mobile phone belongs to the user, the malware found on the link, and the memory card detected in the internal memory of the mobile phone is detected in fig 8.

Fig 8. Records of Harmful Writing in The Physical Extraction of The Mobile Phone

As Fig. 9 shows that, the malicious software uses the authority to write, send and receive SMS in the user's mobile phone.

```
<uses-permission
      android:name="android.permiss
ion.WRITE_SMS"/>

<uses-permission
      android:name="android.permiss
ion.SEND_SMS"/>

<uses-permission
      android:name="android.permiss
ion.RECEIVE_SMS"/>
```

Fig 9. Records of Harmful Writing in The Physical Extraction of The Mobile Phone

Fig. 10 shows that the malicious software authorized a number in the mobile phone of the user as Admin and sent a copy of all the messages to the user in this number.

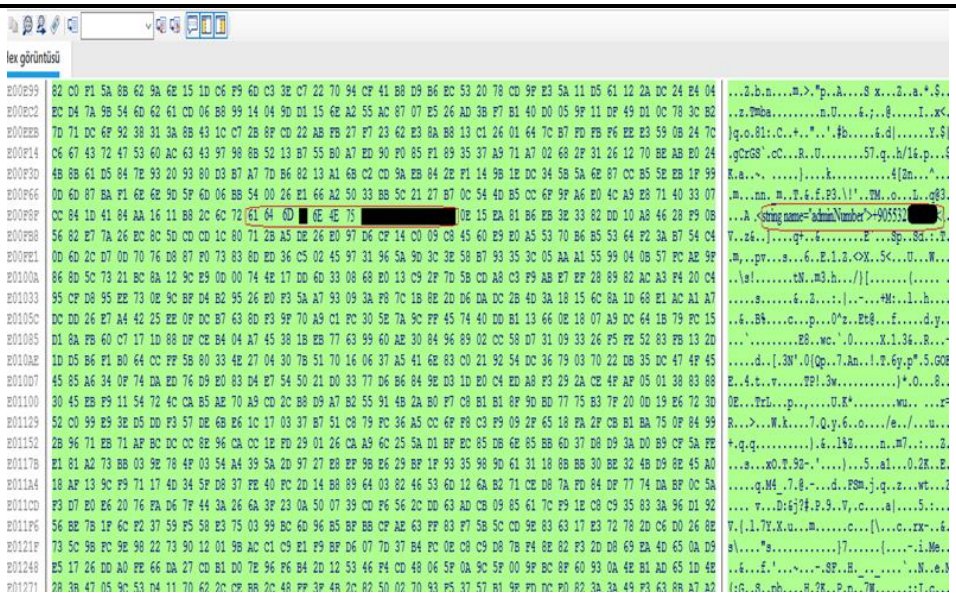

Fig 10. The Admin Number Assigned by The Malware

Conclusion

Mobile device (mobile phone, tablet, etc.) is often associated with criminal information investigation. However, internal investigations, military and private investigations, criminal defense, divorce cases and so on. It is also applied and used in many different areas. There are a number of challenges for mobile forensic IT specialists. Specific features of mobile operating systems, manufacturers' operating system security and data security specific measures are some of these. Depending on these, it is one of the pending decisions of the forensic IT specialist to choose which tools to obtain the appropriate data from the device.

Forensic information can be defined as examining and evaluating the data in order to ensure the security of existing data in electronic environment in a way that can help the legal process. Nowadays, programs and applications which are widely used in electronic environment have their own special filing and coding structure. If a forensic IT specialist can analyze the file structure of these common applications properly and in accordance with certain standards, both the legal process will be accelerated and the intended data can be obtained.

It is almost impossible to detect malware on most of phones without using special hardware and software. These hardware and software are expensive and extremely complicated and difficult to use. Training programs, special materials and laboratory environments should be set up to increase the number of specialists.

The conveniences and possibilities provided by information technology have also brought new security risks. Especially with mobile technology that is increasing pervasively day by day, there are also huge increases in security breaches and crimes in this area. Increased skills of the technology and the attackers have increased the need for specialist staff trained in this area to be able to detect crime and guilt. This threat becomes more serious considering the shift from e-government services towards m-government mobile applications. Therefore, it is crucial for government agencies to have a process for mobile forensics and develop their own human resources for this purpose.

One of the most challenging sub-areas of the forensic world is the examination of "Mobile Devices". The most important reason for this is that there are too many brand-model devices in the market and these are constantly updated different operating system versions. At the beginning of the problems encountered during the examination of these devices to review the necessary copies (forensic images) is to take. Forensic IT experts in this field are the biggest helpers of open source software as well as commercial companies that offer both software and hardware products. The biggest advantage of the commercial software produced is to facilitate and speed up the work of forensic IT specialists trapped in a large number of case files in the conduct of mobile forensic processes.

The rapid and effective examination of a case file is to allow criminals to be caught quickly without attempting new action or following an action. Criminals can use a variety of ways of communication to avoid being caught. However, even without having to do so much effort to follow the technology closely enough to take them one step forward. Forensic review of a newly installed phone can sometimes be a challenging process.

The recent problem in Turkey regarding the investigation of ByLock and Morbeyin operations against FETÖ contains many lessons learned for proactively taking proper measures both for people and government. If the mobile malware forensic does not define the evidence, then it is really a critical problem both for the government and also for the innocent citizens. For effective jurisdiction and legislation, the IT and mobile forensic infrastructure both for human capital expertise and tools-techniques need to be effective either.

The problem of forensic IT experts here is that a phone that is not supported by the software in their hands has to be examined. Considering the wearables and mobile IoT devices to be a major target for hackers, there need to have a security plan and programme for departments responsible on m-government processes and applications. Threats facing mobile devices should be addressed at an adequate level, awareness should be established both for people and government agencies, and information about the measures to be taken should be provided y process owners. Companies using these technologies in sub-structures should be provided with necessary security measures. Governments should encourage citizens for the usage of mobile apps with security considerations.

References

Andriller.com. (2015). Andriller. Available: https://andriller.com/

Azfar A., Choo K. R, and Liu L. (2016). "An android social app forensics adversary model."

Berber, F. "Adli Bilişim Nedir", http://fatihberber.com/ (accessed 10.06.2019)

Digital-forensics.sans.org. (n.d.). (2017). Advanced Smartphone Forensics Most Relevant Evidence per Gıgabyte. Available: https://digital-forensics.sans.org/media/DFIR-Smartphone-Forensics-Poster.pdf

Effecthacking.com. (2017). Android Data Extractor Lite – An Open Source Forensic Tool For Android. Avaible: http://www.effecthacking.com/2017/06/android-data-extractor-lite.html

Forensicswiki.org. (2017). Cellebrite UFED. Available: http://www.forensicswiki.org/wiki/Cellebrite_UFED

Ganesh B., Chakrabarti A., Dr. Divya. (2017). "A Survey On Varıous Mobıle Malware Attacks And Securıty Characterıstıcs".

Grace M., Zhou Y., Zhang Q., Zou S., and Jiang X. (2012). "Riskranker: scalable and accurate zero-day android malware detection on Mobile systems, applications, and services."

Guidance Software. (n.d.). EnCase Neutrino. Available: http://www.guidancesoftware.com/product.aspx?B=Product&Product_S=AccordianTwo&menu_id=117&id=348&terms=mobile+devices

Konga, J., (2013) M-Government- Connecting Bits With Community, https://www.slideshare.net/JuryKonga/mgovernment-open-government-open-data

Murynets I., Jover R. P. (2012). "Crime Scene Investigation: SMS spam data analysis".

Osaf-community.org/. (2015). OSAF Open Source Android Forensics. Available: http://osaf-community.org/wiki/tikiindex.php

Oxygen Forensic. (n.d.). Oxygen Forensic. Available: http://www.oxygen-forensic.com/

S. Seo, D. Lee, and K. Yim. (2012). "Analysis on maliciousness for mobile applications".

Usom.gov.tr. (2014). Akıllı Telefonlarda Güvenlik. Available: https://www.usom.gov.tr/dosya/1418807372-USOM-SGFF-004-Akilli%20Telefonlar%20ve%20Guvenlik.pdf

Wikipedia.com. (n.d.). SIM Kart. Avaible: http://tr.wikipedia.org/wiki/SIM_kart/

Wilson R., Chi H. (2017). "A Case Study for Mobile Device Forensics Tools ".

Wikipedia.com. (n.d.). GSM. Avaible: http://tr.wikipedia.org/wiki/GSM/