GOCE DELCEV UNIVERSITY - STIP
FACULTY OF COMPUTER SCIENCE

The journal is indexed in
EBSCO

ISSN 2545-4803 on line
DOI: 10.46763/BJAMI

BALKAN JOURNAL OF APPLIED MATHEMATICS AND INFORMATICS (BJAMI)

BALKAN JOURNAL
OF APPLIED MATHEMATICS AND INFORMATICS

YEAR 2024

VOLUME 7, Number 2

AIMS AND SCOPE:
BJAMI publishes original research articles in the areas of applied mathematics and informatics.

Topics:
1. Computer science;
2. Computer and software engineering;
3. Information technology;
4. Computer security;
5. Electrical engineering;
6. Telecommunication;
7. Mathematics and its applications;
8. Articles of interdisciplinary of computer and information sciences with education, economics, environmental, health, and engineering.

BALKAN JOURNAL
OF APPLIED MATHEMATICS AND INFORMATICS
(BJAMI), Vol 7

ISSN 2545-4803 on line
Vol. 7, No. 2, Year 2024

EDITORIAL BOARD

CONTENT

Balkan Journal of Applied Mathematics and Informatics Online ISSN 2545-4083
Volume 7 Number 2 Year 2024 UDC:343.98:[004.451.9Android:621.395.721.5

DIGITAL FORENSICS ON ANDROID DEVICE

MILAN MLADENOVSKI AND SASO GELEV

Abstract. The science of digital forensics is an ever-changing and complex field which demands continuous advancements and development. It involves examining and extracting data from electronic devices which can consequently be used as digital evidence in the investigation of potential criminal activities. The forensic experts work tirelessly on finding new and improved tools which can make the research in the field more effective and the practical work of the examiners more productive. The processes and procedures are also constantly updated to follow technological advances, to keep up with the trends led by the manufacturers of electronic devices. The following research paper provides detailed description of the process of examination and extraction of data from mobile phones with android operating system. The detailed description explains the standardized procedures in stages, categorized in logical and chronological order to depict the work tasks of a digital forensic examiner. In addition to the theoretical explanation, this paper also offers practical examples of digital forensic examination. This practical examination was conducted to support the key points of the elaborated research.

1. Introduction

The technological advances in the telecommunication industry have contributed to the increased use of mobile devices for daily communication. It is of utmost importance to understand that mobile phones have become a necessity in the dynamic life of every individual. However, mobile phones are not only used for telecommunication purposes [3]. They are constructed to be more complex devices with internal storage and access to the internet, thus making them potential points of interest in every investigation. Through examination of a mobile phone of a potential suspect, the investigators can search and find evidence of the perpetrated crime and/or communication with other people involved in the investigated felony. If, for example, the investigators are searching for evidence in illegal distribution of narcotics, the mobile phone records can provide information about the calls a suspect has made at the time of the crime. These types of devices store and can provide the content of text messages between potential suspects, thus proving or disapproving the guilt of the people who are involved in the investigated case. This data usually comes with information about the specific names, time, location, amount, and other details about the illegal distribution, which makes the work of the investigators easier and the proof more concrete and sustainable in court. The fact that these devices can provide such details which are useful for the investigation in every type of a crime makes them indispensable in the field of digital forensics. They are considered a great asset, and forensic experts rely on extraction of evidence from mobile phones to regain proof of any type of criminal activities.

Date: November 10, 2024.
Keywords: digital forensics, criminal investigation, mobile phone, android operating system.

Since mobile phones are very useful in the digital forensics laboratory, the forensics experts are constantly working on improving the tools which are used daily for extraction of data from the internal storage of this type of devices. The tools which are available at present can both extract and analyze evidence from a confiscated mobile phone. However, there is an increased need for developing and use of more reliable and validated forensic tools and procedures to improve the investigation and interpretation of the data extracted from these complex devices. It is important to point out that there is not, at present, a single solution or a tool which can be used for every mobile phone on the market. Rather than that, the digital forensic experts need to create different approaches for every new case and follow unique protocols for every investigation. Creativity is the best tool available when dealing with the complexity of mobile phones.

2. **Research methods**

Any electronic device can provide data which, if needed, can be used as digital evidence for a particular crime. Mobile phones are electronic devices that store this type of information. Individuals who use mobile phones, willingly or unknowingly, store sensitive information on the internal storage of the mobile phone [2]. In an investigation, the mobile phone with its internal storage of sensitive information becomes a precious safe which keeps digital evidence of potential criminal activity. The number of manufacturers of mobile phones and the models of mobile phone devices is increasing daily in present time. Therefore, it is very difficult to select a single forensic model which can be used to collect digital evidence from all models of mobile phones [1]. This research provides information about a forensic model which is intended to be used on mobile phones with the Android operating system. The procedure of the proposed investigative model consists of five stages that are described in detail in the following sections of this research paper.

2.1Preparation and preservation

The first stage is the part of the preparation phase and encompasses the identification of the potential source of digital evidence, exploring the device, documentation of the entire process and the actual collecting of the digital evidence. If the integrity of the investigated electronic device, in this case a mobile phone, is in any way damaged and/or the investigator fails to preserve the integrity of the device, the process might harm the entire investigation of the potential criminal activity. In this case, the extracted evidence is considered compromised, thus it cannot be used in the court of law. The digital forensic expert, in this situation, has the responsibility to retain the integrity of the collected data by following the agreed protocol for the first stage of preparation and collection of data from an electronic device. To be accepted by the court of law, the investigation must be led by an official order from a public prosecutor or a corresponding judge [10].

There are numerous situations when the physical integrity of the mobile phone can be endangered. For example, the device which is a part of the investigation can be found submerged in liquid. The first step to resolve this situation is to instantly remove the battery. However, when the mobile phone is found submerged in a destructive liquid, the

device needs to remain in the same position until a forensic expert is available for extraction and examination. For the procedure to be valid, the model of the mobile phone needs to be identified together with the manufacturer and its serial number. The digital forensic examiner needs this information to determine the most suitable forensic tool to proceed with the extraction of data and further analysis of the electronic device.

Another risky situation can occur when the mobile phone is recovered when it is switched on. In this situation, the forensic examiners need to work to assure that the mobile phone receives uninterrupted power to properly work on the device. However, it is also important to isolate and shield the device from any radio signals to ensure that it cannot be accessed through the internet. Even if it is being accessed remotely, this can result in altering or deleting data which can be found in the internal storage of the mobile phone. This procedure of isolation from radio signals is done by placing the examined electronic device in a suitable Faraday bag. When the mobile phone is retrieved while being switched off, it should be secured with all the additional equipment found at the investigating site. Any electronic device which works on a battery can run out of power during the examination procedure. This is the reason why digital forensic examiners need to have reliable external power supply available at any time. The condition of the mobile phone must be preserved in the primary position until the digital forensic examiner makes the assessment following the above-described procedure of preparation. If done properly, the integrity of the device and the extraction of the data are conducted in a satisfactory mode. This will result in digital evidence which are not compromised and are considered valid to be used in the court of law.

2.2 Acquisition

The second stage of the procedure is the process of acquisition. There are two types of acquisition: logical and physical. The first type, logical, means creating an image of file system partitions and information is extracted from the existing data on the device. With the physical acquisition, the entire memory of the device is imaged, including the unallocated spaces [11]. The acquisition process starts when the device is properly retrieved from the crime scene and is handed over to the forensic expert. Firstly, the forensic expert decides on the most appropriate acquisition tool for the device which is being examined. He/she also decides which is the best practice, and, consequently, does a test with the chosen tool on a similar device before using it on the device which is being examined. It is important for the examiner to assure the integrity of the device and the information in this stage. This is the reason why the process of selection of appropriate tools is more time consuming, and it may be necessary for a trial version of the examination to be done on a similar device, to provide a safe procedure which follows the acquisition process. A very useful technique which is used to preserve the validity of the data is the use of write blockers which eliminate the chance of writing of new data to the examined device. There are two types of write blockers: hardware and software write blockers.

In addition, the integrity of the digital evidence can be preserved by hashing the retrieved evidence and by controlling and verifying it on regular basis, to secure the primary value and to prove that it has not been altered during the investigation.

It is very common to have situations when a confiscated mobile phone is protected by a PIN or other type of protection such as pattern, password, etc. In order to remove this type of protection by obtaining the PIN or password from the device, the investigators use certain interrogation techniques to question the user of the device or people who are in any way related to potential suspects involved in the crime. The digital forensic examiners can also use tools provided by the manufacturers of the model of mobile phone which is being examined to gain access to the internal storage and data stored in the hardware or the software of the device. At this point of time in the examination of the mobile phone, the device needs to be set on debug mode, and, if synchronization options are on, they need to be disabled. This will ensure the preservation of the integrity of the collected data. The next step is to take a physical image, and then the forensic expert can enable the synchronization and commence the logical acquisition of data. What can create some problems and complications for the examiner at this point of the investigation is the fact that most mobile phones store their data on volatile memories such as RAM memory. Collecting data from this type of memory can be considered problematic since it has a very dynamic nature of repetitive writing and rewriting data in the assigned memory storage space. In order to extract valid digital evidence from a volatile memory of a mobile device, the examiner must use a combination of forensic acquisition techniques. When extracting digital evidence from permanent memory, the data is retrieved from mobile phone storage and SD memory cards.

2.3Examination

The following stage is titled examination and is the third in a row when discussing the investigative process on mobile phones used in potential harmful and criminal activities. This stage involves examination of the digital evidence that has been retrieved from a mobile phone. In addition, there is a process of extraction of relevant data which can be useful for investigators. The investigators rely on relevant information to create hypothesis about criminal activities and to support the investigative process in the next stages. Digital forensic examiners make backup copy of the phone, called image, before even starting with their examination. The digital forensic examiners usually start by data filtering techniques, keyword searches, and pattern matching, to create a bank of data that will have a manageable size for the investigation. At this point in the examination of the device, the examiners need to be sure that the device has not been tampered with and that the phone’s system has not been modified without authorization. Other crucial elements which need to be checked are whether data has been deleted from the device, and whether data obfuscation techniques have been used. The forensic examiners must be able to reveal hidden data from the mobile device, which can be a very challenging task. Choosing the most appropriate examination tool is also very challenging and extremely important, especially when there is a need for deep investigation of unusual files in the storage of the electronic device [9]. These are the factors which influence the success of the stage of examination of the retrieved mobile phone.

2.4 Analysis

The following stage is very complex and probably the most time-consuming part of the investigation. It is considered qualitative research of the data collected from the device. The first part of this stage is the technical examination of the collected data and the results from the examination process [4]. The next step involves analysis of the hidden data discovered in the examination stage. Another step is the comparative analysis of the retrieved information to prove whether there is a connection and meaning to the digital evidence extracted during the previous stage. The investigators, then, start with the reconstruction of the timeline of the criminal activities to come up with conclusions and proofs supporting their hypothesis. This part of the analysis sets standards for further examination of the criminal activities, and investigators decide whether there is a need to have a more extensive investigation [10].

2.5 Reporting

The following step includes external individuals, usually legal representatives and/or police officials who are actively involved in the investigation of criminal activities. The gathered digital evidence is, later, distributed to the court of law or the appropriate investigation team when the potential criminal activity is investigated by internal branches in an organization. Digital evidence, if applicable to the situation, can serve as proof to help the court of law or the organization to decide on any repercussions or consequences for the suspects and the perpetrators. When the forensic examiner delivers the digital evidence to the outside representatives, he/she must produce a report which will enclose all processes and procedures which have been done during the investigation. This report must also include all the conclusions which were revealed during the stage of analysis of the retrieved data from the examined mobile phone. In our legal system, this procedure is initiated and controlled strictly with the order of a judge or a public prosecutor. After the examiner writes the expert report, it is submitted only to them by their order.

3. Where is digital evidence hidden in mobile phones with Android OS

The following segment presents a comparative analysis of the way data can be extracted from mobile phones with Android OS. The data that can be recovered can come in a form of SMS, call history, emails, GPS locations, photos, social network logins, internet history, Wi-Fi data, Bluetooth paired devices etc. [7]. The most used method is offline research, which is proven to be very effective in this kind of examination. However, there are certain limitations which occur when using the offline research method:

- ADB bridge on Android device must be enabled to access data via USB port. The device needs to be rooted to detect and fix system related information.
- In super user privilege mode, the forensics expert can obtain all system partitions and files.

The forensic examiner must specify what information is being retrieved at the outset. That way, he/she will decide what plain expressions can be used to obtain such evidence [8]. The phrase regular expression is used for a group of characters that are used to locate

the data that needs to be retrieved. With the use of appropriate regular expressions, digital forensic experts can examine the image created as a result at the end of the process.

3.1 Analysis of device information

The ADB shell command can be very helpful when retrieving information about the manufacturing details of the device. It can also provide information about the serial number and the model of the mobile phone, and about the network carrier used by the owner of the mobile phone. This information is very useful to the forensic expert and the investigators of the criminal activity. The following Table 1 shows some of the most used ADB shell commands for retrieving relevant data from a mobile phone with Android OS.

Table 1. *Most used ADB shell commands*

adb shell getprop …	Retrieved data concerning the mobile device
ro.build.fingerprint	Device Build
ro.bootloader	Boot loader information
ro.build.date	Build date
ro.build.version.release	Android version installed in the phone
ro.product.brand	The Product brand
ro.product.manufacturer	Phone manufacturer
ro.product.model	Product Model
ro.product.name	Product Name
ro.serialno	The serial number
	Network information
dhcp.wlan0.dns1	IP address
dhcp.wlan0.gateway	Gateway IP address
dhcp.wlan0.mask	Subnet mask
net.hostname	Hostname for internet connection

Since the list is quite extensive, this research paper contains only the most commonly used ADB commands which are used to retrieve only essential data from the mobile phone. If more specific commands are needed, they can easily be found with a simple online search.

3.2 Contact list and call list

Information about the list of contacts on a mobile phone using Android OS is stored together with the call list information in the contacts2.db database. This is very useful data for the forensic examiner and the investigators since it can help with the creation of the timeline for the potential criminal activities which are being investigated. This data is located at /data/data/com.android.providers.contacts/databases/. The digital forensic examiner can also retrieve deleted contacts from the mobile phone memory. This database which can be accessed to retrieve deleted contacts is stored and located in deleted_contacts.

3.3Messaging

Another very important asset in the mobile phone's memory are the messages which can reveal information about the criminal activity, the suspect's whereabouts and possible connections with other potential people of interest. All the messages written, sent and received from the mobile phone are stored in the com.android.providers.telephony package. This database of messages is in the /data/data/com.android.providers.telephony directory. Both types of messages, SMS and MMS, are stored in this directory and there are 2 separate SQLite databases, one for SMS and a separate one for MMS.

3.4Instant messaging

The digital forensics expert can also retrieve messages from instant messaging applications. The most used instant messaging application, which can effectively be examined and can be a source of digital evidence, is WhatsApp. It has more than two billion users, which makes it a very common instant messaging application, widely spread with users from all around the world. This application collects and stores data in an SQLite database in the directory /data/data/com.whatsapp/databases/. When the forensic examiner needs to retrieve information from this application, he/she can access the two potential databases for analysis. Messages are being stored in the database mgstore.db. Information about saved contacts in the application can be accessed in the database wa.db. Additional files which were transferred through this application can be retrieved from the internal memory of the mobile phone in the following locations:

- Audio: WhatsApp/Media/WhatsApp Audio
- Video: WhatsApp/Media/WhatsApp Video
- Voice Messages: WhatsApp/Media/WhatsApp Voice Notes
- Calls: WhatsApp/Media/WhatsApp Calls
- Images: WhatsApp/Media/WhatsApp Images

Every folder contains Sent sub folder. This folder stores files that were sent by the user. Information of the time and date when a certain contact was added in the memory can be found in a log file data/com.whatsapp/files/Logs/whatsapp.txt. The forensic examiner can then do a comparative analysis to see whether the log file and the contact table have discrepancies, and then it can be deduced whether certain contacts were deleted.

3.5E-Mail

Regular users of mobile phones with Android OS know that their accounts are usually created using a Gmail address by logging in on the Gmail application. This application collects and stores data in an SQLite database which can be retrieved from the /data/data/com.google.android.gm/databases directory. Android OS devices also contain another built-in e-mail application. With this application, users can access non-Google accounts, such as work accounts based on their organization's server. This data is being collected and stored in a separate directory which can be found in /data/data/com.android.email/databases. This database can be also used to retrieve email addresses from the Gmail application. The data related to passwords is stored only on Google servers. However, this stored data is used only for user authentication. When the

authentication process is done, the application creates a token which is used for subsequent login and access. The authentication token is then saved in place of the password and can be retrieved from the account's database located in the /data/system/users directory.

3.6 Browser

The mobile phones with Android OS come with a built-in search application which is based on the WebKit open source project. This search application belongs to the com.android.browser package and can be accessed in the /data/data/com.android.browser folder. In more recent models of mobile phones, Google Chrome is used as the default browser for Android devices. The majority of information related to Google Chrome are saved and located in the /data/data/com.android.chrome/app_chrome/Default directory.

3.7 Social networking applications

Social networking applications, like instant messaging applications are the most widely spread means of communication at present time. This is why it is important for the forensic expert to understand the storing and retrieval of data from these applications. The necessary data from applications such as Facebook and X (Twitter) can be retrieved by using a regular expression. If accounts on these applications are being accessed from their websites and through a search engine, the forensic examiner can retrieve more information by analyzing the data from the search engine. Facebook and X login records are located in /data/system/users/0/accounts.db database. However, password information is not stored. Data related to Facebook can be retrieved from the two available locations /data/data/com.facebook.katana and /data/data/com.facebook.orca when the user has Facebook Messenger installed. Data related to X can be retrieved from the directory /data/data/com.twitter.android. This database contains records of published tweets, images, followers and other information related to the user and his/her activity on the application.

4. Practical example

In order to illustrate the procedures mentioned in the previous section, a practical example has been presented with the following image. In Figure 1, there is an actual screenshot of a SMS sent from a Nokia 2.2 device with an Android OS [6]. For this example, Magnet AXIOM software tool [5] has been implemented as an appropriate and effective forensic tool to retrieve the relevant data. The content of the sent message that was: Test KAOS. The retrieval was successful and the results of the forensic examination and analysis are shown in the images below.

Figure 1 shows the test results section of the mobile device. The part of interest, the SMS sent to one of the contacts that was saved in the device, is intentionally highlighted. In the section labeled as COMUNICATION, found on the left side of the image, there is an Android SMS/MMS (Content Provider) 1. The number 1 shows that there is only one SMS or MMS on the phone.

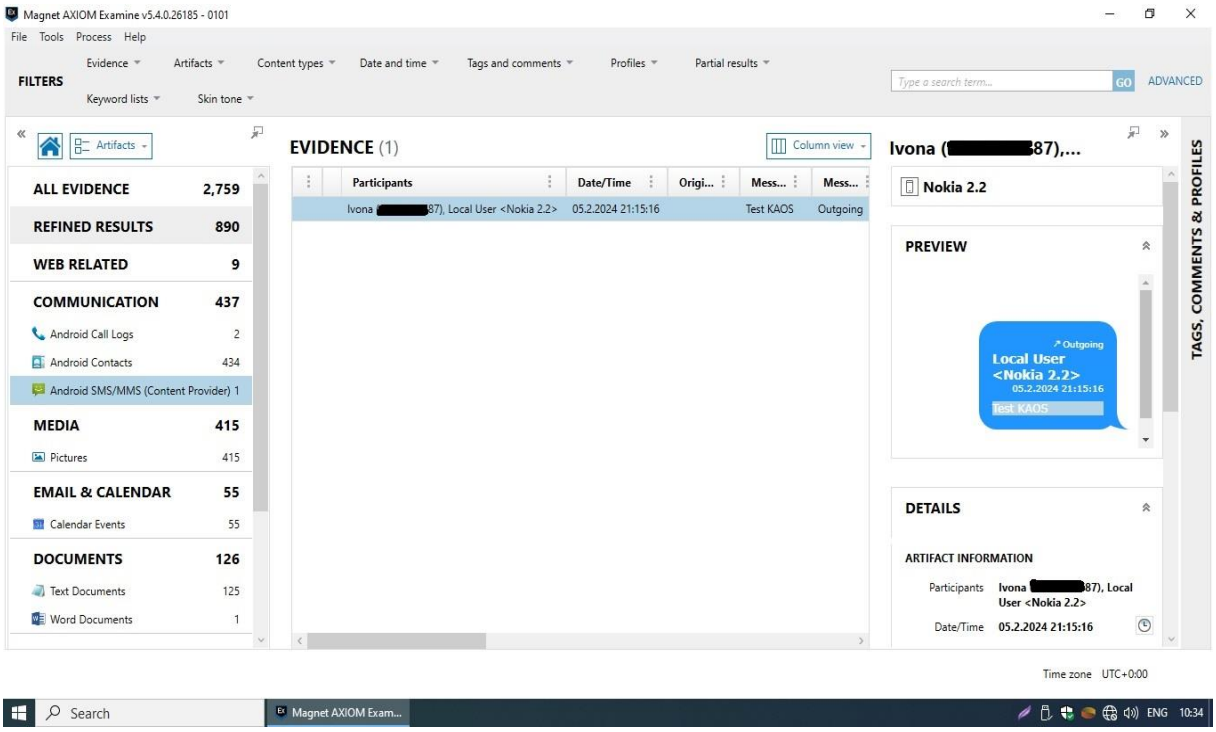

Figure 1. *Display of found artifacts*

Figure 2 shows the review of the evidence found. It shows, in more detail, where the evidence was extracted from, what was the content of the message, who is the sender of the message, who received the content of the message. The image also shows the time of sending and whether the message was sent or received.

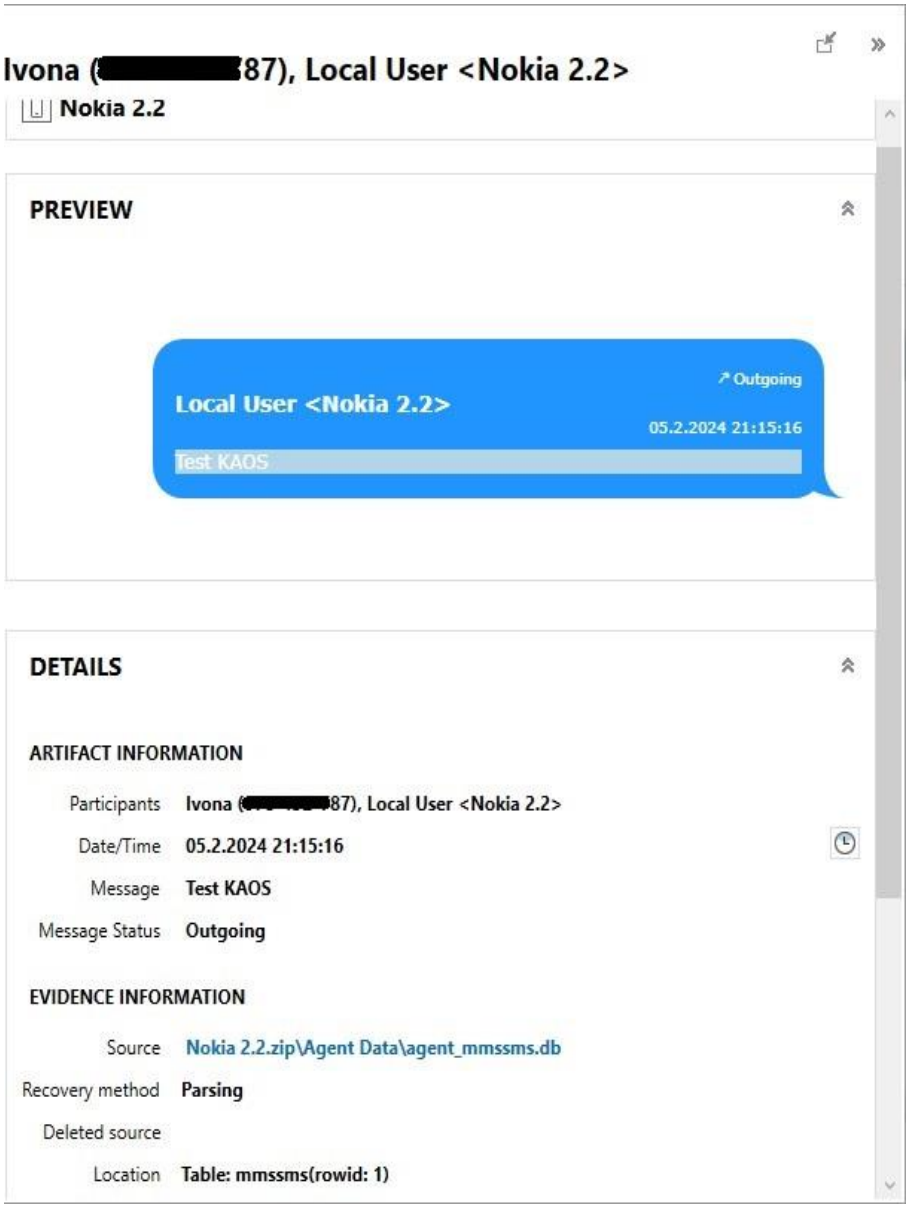

Figure 2. *Details for the SMS found*

Figure 3 shows a more detailed description of the event. It shows where the information was extracted from, whether it is still saved on the device, or it has been deleted and it also shows the path where the message is actually saved.

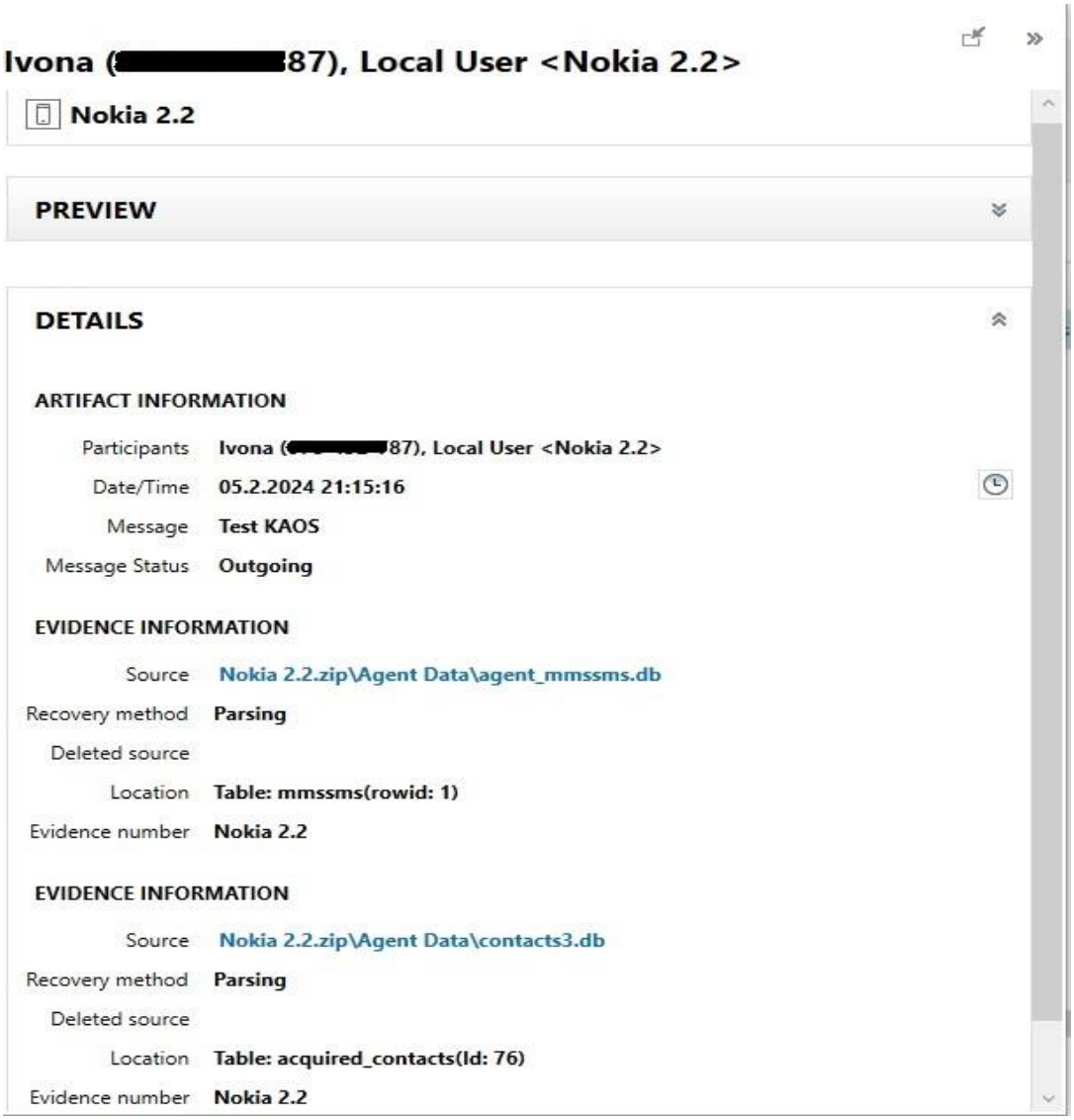

Figure 3. *Details for the SMS message status in the phone*

5. **Conclusion**

The fast pace of technological advances creates complications in the everyday work tasks of every digital forensic examiner. The industry of mobile phones and the manufacturers of electronic devices are in a constant battle to create a new and improved model of a mobile phone in order to attract customers. This dynamics has been so far very effective in increasing the productivity of manufacturers who strive to fulfill the needs and wishes of their buyers. It can be stated that the mobile phones with Android OS

outnumber any other group of mobile phones, which makes them more susceptible to forensic research and examination. It is evaluated that, by the beginning of 2024, there were almost 3.5 billion users of electronic devices with Android OS, which is an enormous number compared to other manufacturers and providers of OSs. As a logical turn on this point, it can be stated that the greater the number of Android device users, the greater the number of criminals using Android devices. Digital forensics follows this trend with increasing the examination on android devices.

This research paper was written with the goal of introducing the interested parties with general information about digital forensic investigation. It also contains a detailed description of the stages of forensic investigation led by digital forensic experts. These stages also depict the way examination of retrieved data is conducted. By the analysis of the examiners, this data can be used as digital evidence in investigation by police officials and presented in the court of law in order to support the resolution of the related criminal activities.

The research and content of the paper mainly concentrates on the analysis of information from mobile phones with Android OS. The digital forensic examiners who work on mobile phones with Android OS are uncovering evidence from a crime scene. They also provide information which helps investigators to create a timeline of the criminal activities. They can also reveal any accomplices and prove connections between several potential suspects. All digital evidence, written in an expert report is then submitted to investigators and law enforcement agencies. During the process of examination and analysis, forensic experts may encounter certain limitations and barriers that can be quite challenging. Some of the limitations can be of a technical nature such as encrypted data, device routing, and user-applied safeguards. It is the dedication and hard work of the forensic expert that ultimately removes all these limitations and, by selecting appropriate tools and methods, combination of several techniques such as data extraction, system log analysis, he/she can produce the desired results. Another very important link of the whole process is the collaboration between forensics experts, manufacturers of devices, police officials and representatives of the court of law. This connection is crucial when trying to have a successful investigation.

The research needs to continue since technology is rapidly evolving. The science behind digital forensics on Android devices is a dynamic field where forensics experts must work on improving the existing procedures, methods and techniques, but also work on creating new and improved models of investigation in order to follow the evolution of technology.

References

[1] Terrorgum.com.: Practical Mobile Forensics ebook, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj62a_ExZGE

AxWcVvEDHVdEDLMQFnoECBQQAQ&url=https%3A%2F%2Fterrorgum.com%2Ftfox%2Fbooks%2Fpracticalmobileforensics_ebook.pdf&usg=AOvVaw1yuYz8hafMyrb8Gls lGJcy&opi=89978449

[2] Researchgate.net.: Android digital forensics – Simplifying Android forensics using regular expressions, https://www.researchgate.net/profile/Neera-Jeyamohan/publication/322511440_Android_digital_forensics_-_Simplifying_Android_forensics_using_regular_expressions/links/5bbc776aa6fdcc9552dcb635/Android-digital-forensics-Simplifying-Android-forensics-using-regular-expressions.pdf

[3] Ieeexplore.ieee.org.: Android Mobile Device Forensics: A Review, https://ieeexplore.ieee.org/document/8757493

[4] Researchgate.net.: Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases, https://www.researchgate.net/publication/330558290_Digital_Forensic_Analysis_on_Android_Smartphones_for_Handling_Cybercrime_Cases

[5] Magnetforensics.com.: Magnet AXIOM User Guide, https://docs.magnetforensics.com/docs/axiom/html/Content/Resources/PDFs/Magnet%20AXIOM%20User%20Guide.pdf

[6] Magnetforensics.com.: Advanced Mobile Acquisition for Android, https://www.magnetforensics.com/resources/advancedmobile/

[7] Digitpol.com.: Android Forensics, https://digitpol.com/android-forensics/

[8] Medium.com.: Android Forensics Part I— Android Acquisition Methods, https://medium.com/@praveenadithyav/android-forensics-in-criminal-investigations-3cc9b8c1818b

[9] Sciencedirect.com.: A Systematic Literature Review on Digital Forensic Investigation on Android Devices, https://www.sciencedirect.com/science/article/pii/S1877050924008020

[10] Media.neliti.com.: Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases, https://media.neliti.com/media/publications/417394-digital-forensic-analysis-on-android-sma-d767ba6b.pdf

[11] Researchgate.net.: Challenges in Android Forensics, https://www.researchgate.net/publication/320952681_Challenges_in_Android_Forensics

Saso Gelev
Goce Delcev University
Faculty of Electrical Engineering
Stip, North Macedonia
saso.gelev@ugd.edu.mk

Milan Mladenovski
Ministry of Internal Affairs
Department of Forensic Examinations
Sector for Digital Examinations
milan_mladenovski@moi.gov.mk