The Study of Audio Recording Apps Installed on Smartphone With Android Operating System in Relation To Forensic Audio Analyses

Amol L. Deokate[1], Y. A. Pawar[2]
[1, 2] Dept of Information Technology
[1, 2] Sanjivani K.B.P. Polytechnic

Abstract- *This Paper Describe evidence recordings made with devices such as smartphones it has significantly increased in recent years. It is a dedicated apps are used for making recordings, which is installed mainly on the Android operating system. During the research paper, we study the properties of free audio recording applications that are often downloaded from the Internet. We can select ten different applications and installed on modern smartphones, followed by making test recordings for further analysis. Despite that the selected applications are rather simple, they all have considerable potential. Half of them have an option to edit their recordings.*

By using the MATLAB environment, our own software was developed for the automatic analysis of the audio files structure in order to search for relevant metadata. This paper also describes the methodology of proceeding with the evidence smartphones and recordings, and, moreover, a way of safely copying data from their memory for further analysis. The obtained results have substantial value for examining the authenticity of audio recordings as part of forensic expert opinions. The acquired recordings also expand the constantly developed database of audio files, which is a useful tool for analyzing the authenticity of recordings.

Keywords- Smart Mobile phone, Android recording app, Digital recording, Authenticity analysis, File structure.

I. INTRODUCTION

The use of small battery-operated portable multimedia players has become widespread since the time when digital technology combined with the miniaturization of devices enabled their construction. Popular MP3 or MP4 players, due to their small size and functionality, have dominated the digital multimedia equipment market. In addition to their ability to play audio or video, or open image files, they are often equipped with an audio recording function. Devices dedicated to audio recording constitute a slightly different group; they are also portable and battery-powered, and are of- ten referred to as digital voice recorders. Only a few years ago, more than three-quarters of digital audio recordings subjected to forensic audio testing were re- corded using the above-mentioned devices. The product market still offers portable media players and voice recorders, but currently evidence recordings from mobile devices usually originate from other sources.

The dynamic development of wireless mobile phone networks and services offered has, in effect, forced manufacturers to introduce phones onto the market that will

Make it possible to make use of the full potential of such networks. Smartphones, i.e. de- vices which combine the function of a mobile phone with that of a portable computer, have gained the greatest popularity, effectively replacing classical mobile phones. Telephone conversations and SMS currently constitute only a part of the capabilities of the average smartphone usually, among the dozens of applications that have been pre-installed on a smart- phone's operating system, and at least one is strictly de- voted to recording sound. In the event of absence of such an application or the need to use another one, Internet services offer many recording applications for the given selected smartphone model and its operating system, and allow you to independently obtain and install one tailored to your preferences. The useful- ness, great adaptability to your own preferences and the general availability of these telephones have made them a basic device in everyday life with many applications. Recent expert opinions in the field of audio forensics suggest that there has been a significant change over the last few years and that currently, among all mobile devices, smartphones are now the primary source of evidence audio recordings, with a negligible share from portable media players and Dictaphones. This has also resulted in a change in the audio saving formats adapted to the operating systems and capabilities of these devices.

Currently, around 2.7 billion people worldwide use 3 billion smartphones. Despite the dynamic situation on the market, for several years now the most popular models of smartphones, both globally and in Poland, have been products of the Korean company Samsung, and subsequent positions in the rankings are occupied by Xiaomi, Huawei or Apple. The current models work mainly under the control of Android or iOS operating systems, which have created a kind of duopoly and serve about 98% of the global smartphone market. Of all the smartphones sold, approximately 85% of devices globally, and 90% in Poland are fitted with the Android operating system (Orange, 2019). The research on smartphone devices presented later in the paper indicates that these statistics are also confirmed in expert practice. Dedicated applications installed by the manufacturer or user are used to record sound in such devices. Experience in the field of making test recordings with the evidence phones studied so far indicates that these are uncomplicated applications with basic functions enabling recording and simple editing. The popular website Google Play (previous name: Android Market) offers about 2.8 million applications, 95% of which are free of charge and can be installed and used in Android systems In this service, searching by keywords, for example, “audio (sound) recorder” or “Dictaphone”, you can find dozens of free applications designed to record audio recordings, which you can easily install on your smartphone on your own. Applications that are pre-installed on new phones (for example: Samsung applications) can also be found on Internet websites.

In this work we have reviewed and selected the most popular applications designed for audio recording working under the Android operating system that can be installed using Internet resources. These applications were installed on a Samsung smartphone, their recording and editing capabilities were established, and then test recordings were made. The principles of procedure during the making of test recordings with the use of such devices have been described. Next, analyses of these applications, and of the parameters of the recordings made with them as well as the properties of audio files and metadata were carried out. Additionally, algorithms and a computer program working in the MATLAB computing environment were developed, designed as a tool for automatic analysis of the structures of saved audio files containing test recordings. The obtained results and observations were evaluated in order to determine the possibility of their use in tests of the authenticity of digital recordings that had mainly been recorded with modern mobile phones.

The main aim of the author was to analyze the properties of generally available applications with audio recording capability and to evaluate whether the obtained results could be applied in the work of audio forensics experts, without any intention to promote or criticize any particular brand, operating system or software.

II. ANALYSIS OF EVIDENCE AND AUDIO TEST RECORDINGS MADE WITH SMARTPHONES

Evidence digital recordings are not usually recorded with high quality professional recorders, but with commonplace equipment. Audio recordings which are currently being examined in the Section of Speech and Audio Analysis of the Institute of Forensic Research have relatively often been re- corded with the use of the new generation of mobile phones that are popular today, i.e. smartphones. Other types of evidence devices containing recordings that have been commissioned for analyses are also submitted to the Section. The technical condition of each piece of evidence is assessed individually, as is the possibility of securing data from the memory. If a phone and its installed memory card (if there is one) are submitted for testing, then the con- tents of both are secured during the examination. If possible, an exact copy of the contents of the entire memory or its accessible part in the form of a so-called image is made. Such a copy is the most useful form of collection for further forensic audio analysis. The image of the memory is treated as a reflection of the content of the medium (data carrier) together with the preservation of the file system structure, the properties of the files and their time signatures, which are of great importance for authenticity testing. Creating an image also makes it possible to determine whether there are any deleted files, including audio files, in a memory copy made in this way, and also makes it possible to attempt to recover them. For the analysed area of the source memory and its image, checksums should be calculated and compared with each other in order to verify the correctness of the copy. If it is not possible to make an image of the memory content, then the data is secured by making a logical copy of copyable files and directories from the analysed data carrier. It is also possible to explore the content of the memory of the evidence carrier, which allows the number and properties of the accessible files to be determined, which has particular significance when it is not possible to carry out the imaging process. Securing the memory content of a device or carrier submitted for examination – and the way in which this is performed – is an important element determining the subsequent forensic audio analysis, in particular the analysis of the authenticity of recordings. When a phone is submitted for examination together with a SIM card, the SIM card is also secured as material evidence, but it is not examined for audio forensic pur- poses, as SIM card memory does not store multimedia files. A write-blocker type device is used for safe exploration and copying of the contents of a smartphone memory, preventing accidental modification of data

On the basis of the smartphones analysed during routine expert opinion activities, it can be concluded that the vast majority of them were Samsung devices, as well as individual models of HTC and Manta brands – all working under the control of the Android operating system. One iPhone 3G device with an iOS operating system was also examined. Each of these devices had one or occasionally two audio recording applications installed. It was noted that these were simple to use applications allowing for basic activities during the recording: starting, pausing and stop- ping the recording. Some of them, mostly installed on Samsung phones, enabled simple editing of the saved recordings, consisting mainly in deletion of fragments of them and saving changes in source files or creating new ones. All applications analysed so far allowed renaming of files containing audio recordings in the course of or after saving them to memory. It was noted, however, that usually the names of files with evidence recordings are default names for installed applications, and correspond to the names of files containing test recordings made by evidence devices during their testing.

Analysis of collected data originating from the memory of smartphones showed that the audio recordings contained there were mainly saved in M4A and 3GP file formats. Audio data of these types of files together with the accompanying metadata were placed in a so-called MPEG-4 multimedia container, linked with ISO standards. M4A and 3GP formats and the MPEG-4 container are very common in modern mobile devices. Files of this type are quite easily converted to uncompressed PCM WAVE format or even played in real time by standard software, which constitutes the basis for further forensic audio analysis

The recognition of recordings as evidence material and the scope of tests defined by judicial bodies makes it necessary to analyse their authenticity. The definition of the authenticity of a recording announced by the Audio Engineering Society (AES) indicates the need to assess the recording's continuity and originality, and the method used to make the recording. Carrying out test recordings is an important part of examinations of both the device itself and the authenticity of the evidence digital recording. They make it possible to determine whether the evidence device could have been used to record the evidence recording and to conduct a comparative analysis of the parameters and structure of the file containing test recordings. They also make it possible to determine whether the device enables the recording of power line hum and to reveal other possible characteristic features, such as a DC offset.

The aspects discussed above also apply to recordings made by smartphones; however, it should be borne in mind that the emergence of new devices recording evidence recordings has forced the development of new ways of preparing and making test recordings. Smartphones are complex multifunction digital devices with their own operating system and with a high probability that every other model will have a different audio recording application installed. If the commissioning party has not submitted the device which was supposed to have been used to make the recording that has been submitted for analysis (most often, s/he has only provided a copy of the recording saved on a different data carrier) and the official request contains questions related to authenticity analysis, s/he should be requested to deliver such a device for testing.

In the process of preparing test recordings on the smartphone, its system settings, including the time clock, and installed applications should be verified. For audio recording applications, the following are established first: the current recording settings, the selected memory and storage folder path, the list of files containing recordings, and possibly other accompanying files, as well as the range of presented information about files. Next, one should determine all possible application settings, such as recording formats and parameters, and file naming, as well as the possible scope of their changes. Before recording "valid" test recordings, which will be subject to later comparative analysis, it is good practice to make a recording or several recordings (at least one for each format) in order to determine which options are available during and immediately after the recording. Experience shows that on smartphones some of the application options are only activated in the course of recording. This also allows determination of how the recordings are saved, i.e. automatically or with user interaction, their real names and readable parameters. Not all applications present the format of recordings or file extensions in a standard way, describing parameters with sometimes enigmatic names in the form of "good quality" or "small files". Familiarisation with the capabilities of a given application allows development of an optimal plan for making test recordings, containing a description of their execution, the sequence of recordings and sequences of reproduced test signals and the application of all possible settings and functions. In practice, test recordings are not stored in the memory built into the evidence smartphone so as not to interfere with its content, but on installed removable microSD memory cards. Cards with a reasonably good saving speed, for example class 10, should be used to in order to ensure that the data stream is saved uninterruptedly on the data carrier. For security purposes, the stage of preparing and making test recordings takes place in a screened chamber without access to the mobile phone network. All tests on the phone are carried out without an in- stalled SIM card or evidence memory cards, and with- out changing the system settings, folder and file con- tents. After the forensic audio tests are completed, the memory status of the smartphone is routinely verified, taking into account the files containing the recordings, both from the level of the recording application and the file manager.

Valid recording of test recordings with the use of a smartphone is a time-consuming task and is preceded by appropriate preparation, but it is important in the process of analysing the device, the application and the saved recordings as well as in the analysis of the authenticity of evidence recordings.

III. MATERIAL FOR TESTING

1. Audio recording device and applications

A popular Samsung smartphone, the Galaxy J3 Dual SIM 2017, constituted the hardware used in the research. At the time of purchase, it had a pre-installed Android version 8.0.0 operating system as well as an application for recording audio: Samsung Voice Recorder version 21.0.22.166.

In order to carry out the intended tests with the use of the Google Play service, descriptions of available applications for making audio recordings were analysed. Next, on the basis of a combined assessment encompassing: number of installations of the given application (popularity), high rating by users and re- viewers, as well as capabilities and functionality, and eight free applications were selected. The names of these

2. Audio recordings

With the help of the above mentioned 10 applications installed on the Android system, 142 audio test recordings were made in 6 different formats. These recordings were made using all possible recording settings and functions available during the recording, such as: start and stop recording, pause function, activation of recording by volume level, overwriting with a newer recording, indexing, automatic saving or with user interaction. After the test recordings were made, they were edited in the following ways with the help of applications which had such a capability: deleting a fragment of the recording, copying and pasting a fragment of the recording, overwriting an already saved recording with a newer recording, or repairing the file header. These recordings contain as wide a range of signals as possible, such as: white noise, low, medium and high frequency tones, speech and intentional interference, both impulse and continuous. To safely explore the contents of the memory containing recordings, and to make copies of the recordings, a write-blocker was used to prevent possible modification of data on these types of carriers.

For the purposes of further research, copies of files were made from a device that recorded onto the hard disk of a computer.

A computer program operating in the MATLAB environment was developed for analysing the data contained in the files with the test recordings. This program enables automatic structure exploration and metadata detection in audio files of any format; how- ever, it was designed primarily for analysis of files saved in MPEG-1 – MPEG-4 and RIFF standards. Files of this kind constitute almost all of the collected research material and may contain more extensive metadata. The operation of the created program can be presented as follows:

1) import of an audio file selected for analysis into a workspace; the import algorithm recognizes the file type on the basis of the file extension and pro- poses an analysis method that is suitable for the given format, with the user also being able to deter- mine the file type and choose the method by them- self,

2) defining of the analysis area, i.e. the whole file or the part of the file containing the metadata; the analysing program may skip the encoded audio data, for example, the whole *mdat* box in MPEG files, and the whole chunk *data* in RIFF files; the file area with encoded media is usually the most extensive part of the file, where there are usually no metadata,

3) exploring a designated area byte by byte and searching for all character strings that may constitute metadata; the detection and decision algorithm is based on the four-character code (FourCC) sequences implemented in the program for boxes and chunks (mainly for MPEG and RIFF) as well as other possible markers, identifiers and tags for all analysed formats; to ensure correct operation, the algorithm also takes into account upper and lower case letters, location in the file, size and interval be- tween consecutive recognized metadata; in the case of detection of a hitherto unknown four-character code sequence, the program also presents it in the results, in order to complete the description and for the user's knowledge; the concepts mentioned here will be discussed in greater detail later in this paper,

4) saving of the metadata structure of the analysed file to a spreadsheet for the purpose of possible further comparative analysis with other files,

5) optional saving to a spreadsheet of metadata indicated by the user, i.e. name, size, location in the file and content.

In the course of the analysis of the collected audio files, the created program was optimized on the basis of a feedback loop with the aim of using it for the analysis of various formats and possible data structures. Apart from the obtained results of the analyses, available research papers and technical documentation were also referred to during development of the program (3GPP, 2010; 3GPP, 2011; ISO/IEC, 1993; ISO/IEC, 2015; Microsoft Corp., 1994; Microsoft Corp., 2010). This program constitute a tool supporting authenticity examinations of audio recordings, which are carried out as part of expert opinion work at the Institute.

IV. CONCLUSION

This paper conclude that the performed research, one may say that it has enabled a broadening of knowledge on the most frequently used applications for making audio recordings that are installed on the Android system. Analysis of selected applications allowed familiarization with their capabilities and the making of test recordings with them. The results of analysis showed that these applications, although free, allow for a relatively broad spectrum of possibilities of audio recording: in 6 different audio formats, with predefined or customised parameters, in high quality uncompressed files or with sound compression, as well as with the possibility of including additional information in their names. Half of the analysed applications enable editing consisting in deletion of a fragment of the recording, copying and pasting it in another place or overwriting it with a new recording. Using system tools and dedicated programs as well as the algorithm developed in the MATLAB environment, properties of the collected recordings and file structures were analysed. On this basis, it was ascertained that it was possible to establish parameters of the test recordings, their time signatures and metadata content. The results of the conducted analyses unambiguously point to the possibility of making use of them in authenticity testing of evidence audio recordings.

First of all, the work carried out allowed for collection and analysis of audio recordings recorded with various mobile applications, which will make it possible to perform comparative analyses of their properties with those of evidence recordings submitted for exam-ination in the future. This will also make it possible to supplement the database of audio recordings which is constantly being developed by the author, and which constitutes an additional tool supporting authenticity testing. Secondly, the analysis of metadata of test files saved in the popular MPEG-4 container allows you to obtain much important information about the recording parameters, time signatures, the device used, and the recording application. It also enables indication of the differences between source recordings and edited recordings. Additionally, each of the installed applications is characterised by at least one feature that distinguishes its files from the rest, which may be helpful in identifying the specific application used to save the given examined audio file. The results obtained are of significant importance, since questions concerning authenticity of recordings are frequently included in the official request of institutions commissioning forensic audio expert opinions.

REFERENCES

[1] 3rd Generation Partnership Project (3GPP). Techni- cal Specification Group Services and System Aspects. (2010). Technical Specification 26.244 V 9.2.0: Transparent end-to-end packet switched streaming service (PSS). April 9, 2020 from: http://www.3gpp.org.

[2] 3rd Generation Partnership Project (3GPP). Techni- cal Specification Group Services and System Aspects. (2011). Technical Specification 26.090 V 10.1.0: Mandatory Speech Codec speech processing functions; Adaptive Multi-Rate (AMR) speech codec; Transcoding functions. April 9, 2020 from: http://www.3gpp.org.

[3] AppBrain. (2020). Android and Google Play statistics. Retrieved April, 10, 2020 from: https://www.appbrain.com/stats.

[4] Audio Engineering Society (AES). (1996). AES *recommended practice for forensic* purposes – Managing recorded audio materials intended for examination, AES27–1996. Audio Engineering Society Inc. Retrieved April 9, 2020 from: http://www.aes.org.

[5] Casey, E. (2010). *Handbook of Digital Forensics and Investigation*. Elsevier Academic Press.

[6] Casey, E., Turnbull, B. (2011). Digital evidence on mobile devices. (In) E. Casey (Eds.), *Digital evidence and computer crime, 3rd Edition* (pp. 603–606). Elsevier Academic- Press.

[7] Cooper, A. J. (2006). Detection of copies of digital audio recordings for forensic purposes, PhD thesis. United Kingdom: Faculty of Technology, Department of Information and Communication Technology, The Open University.

[8] Gloe, T., Fisher, A., Kirchner, M. (2014). Forensic analysis of video file formats. *Digital Investigation*, *11*, 68–76.

[9] Grigoras, C. (2005). Digital audio recording analysis: The electric network frequency (ENF) criterion. *Inter-national Journal of Speech, Language and the Law*, *12*, 64–76.

[10] Grigoras, C., Cooper, A., Michałek, M. (2009). Forensic Speech and Audio Analysis Working Group – Best practice guidelines for ENF analysis in forensic authentication of digital evidence; REF. CODE: FSAAWG-BPM-

ENF-001. Retrieved October 13, 2017 from: http://www. enfsi.eu.

[11] Ho, A. T. S., Li, S. (2015). Handbook of digital forensics of multimedia data and devices. United States of America: John Wiley & Sons.

[12] International Data Corporation, IDC. (2019). Smartphone market share. Retrieved April 10, 2020 from: https://www.idc.com.