International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 3, ISSN No. 2455-2143, Pages 162-165
Published Online July 2020 in IJEAST (http://www.ijeast.com)

AUTHENTICATION OF DIGITAL AUDIO RECORDING USING FILE'S SIGNATURE AND METADATA PROPERTIES

D. P. Gangwar
Central Forensic Science Laboratory
Sector 36-A, Chandigarh 160036
DFSS, MHA, Govt. Of India

Anju Pathania
Central Forensic Science Laboratory
Sector 36-A Chandigarh 160036
DFSS, MHA, Govt. Of India

***Abstract*— the authentication of audio recording plays a very important role in forensic science and for other crime investigation purposes. At present, the forensic experts are exclusively receiving digital recordings for forensic examination. The analog audio recording technique has been entirely replaced by digital recordings. In the present work the audio recordings have been recorded by using different digital voice recorders in different file formats. The original audio recordings were edited by using different software such as *GoldWave, ocenaudio, WavePad Sound Editor,* Audacity and Adobe Audition available in open source platform. The original and edited recordings were analyzed for various file signatures and metadata properties for of the audio files the purpose of authentication purpose.**

Keywords— **Hex Data, Metadata, MediaInfo, File structure, file format, Codec**

I. INTRODUCTION

The digital technology has brought undeniable benefits to our society with continuous advancements in ingenious forgery. The authentication of digital multimedia (i.e., image, audio and video) is an emerging challenge. It has also become extremely easy to manipulate the recorded audio contents using various handy and free software tools. The various types of Audio forgery can be accomplished such as copy-move, deletion, insertion, substitution and splicing etc. The role of an audio recording is very important for criminal investigation agencies and for court of law as it is admissible evidence. Unauthentic and forged multimedia can influence the decisions of courts. It is also fact that the audio recording evidence remains as useless evidence until it is to be proved that the recording is authentic or free from any kind of tampering/editing. The detection of editing in audio recording is a challenging task to forensic scientists, which requires a great attention in this field.

Metadata is the term used to describe traditional descriptive cataloging applied to digital files, in addition to information needed to retrieve, access, and manage those files. The metadata of a digital file is a bunch of information which has hidden inside the file in decrypted form. In audio file, the metadata contained various types of information i.e. file format, file size, duration, audio format, audio codec, format version, format profile, format settings, bit rate mode, bit rate, channel(s), sampling rate, compression mode, writing application, stream Size, created Date, modified date, compression Mode, etc. These file signature details depends upon the recorder's features like type, make, model, version, recording sources types and other parameters. Hence, a multimedia file's signature is a unique value, which distinguishes it from other multimedia files. The file signature consists of three parts such as: file name, file header/footer and file content. The file name allows the computer to identify each file which stores on the disk/drive/storage media. The files' header/footer describes the file type. This is also called the signature of the file and is used to indicate the start (header) and end of the file (footer). File content is the third part of the file structure, from which useful information, like file metadata, can be extracted that includes the size, owner, timestamp, device name, and so forth in addition to whether the file is hidden or not. File signature analysis is the part of forensic analysis where header and extension are compared with a standard file signature database (header and extensions).

In the present work more than 100 digital audio files have studied for file's signature and metadata properties, in two perspectives. Our main aim was to identify the type of equipment (source of recording) which was used to record the audio recording, subsequently to determine whether the recorded audio files are original/modified/edited. Analysis of file signatures and related metadata of different audio files' format were carried out in order to identify the authentication of audio files.

II. RELATED WORK

Bruce e. Koenig et al [1] in his work "Authentication of Forensic Audio Recordings" had described the all methods for authentication of analog audio recording. Eddy B. Brixen [2] in his paper "Techniques for the Authentication of Digital Audio Recordings" has mentioned the basic techniques used for authentication in digital recording including

Header/metadata, ENF-criterion. Marcin Michałek [3] in his work made limited database of recording devices and highlighted the OLYMPUS recorder could be identified from Hex data. D. Hamdi et al [4] in the paper Multimedia File Signature Analysis for Smartphone Forensics has highlighted the different file signature, which could be used for audio authentication with comparison of original files.
The Electric Network Frequency (ENF) Criterion is a recently developed forensic technique for determining the time of recording of digital audio recordings, by matching the ENF pattern from a questioned recording with an ENF pattern database. [5][6][7][8]

III. MATERIALS AND METHODS

Whenever digital equipment is used for audio recording, not only the acoustical signal is recorded. Also, signature of the file, date, time, size etc is found. The present study is based on the analysis of more than 100 audio samples. The audio samples were recorded in controlled manner and few were taken from different actual crime cases received from different investigation agencies from throughout India, in which the voice samples have been recorded using different digital voice recorders and mobile phones, such as SONY Digital voice recorder, SAMSUNG, Vivo, Oppo, Micromax. The audio samples were recorded in AMR, WAV, 3GP, MP3, AAC, M4A, OGG file formats. The Gold-wave, Wave-Pad, Ocenaudio, Audacity, and Adobe-Audition software were used for editing the original audio samples for analysis purpose. The metadata and file signature analysis were carried out using various freeware software such as Media Tab, Media Info, Hex data Viewer, Winhex, Hex Workshop etc. For media Info (HTML & XML) and for Hexdata(ASCII) were respectively used to extract the metadata/file signature. The detailed description of the file should be documented for future reference, and a procedural review should be carried out with relevant information (file format, codec, sample rate, bit depth etc.) for future analysis. Although this is a simple task, but care must be taken. For example, while the file extension may indicate WAV, several compressions format store audio in WAV files such as Microsoft ADPCM, DVI/IMA ADPCM.

IV. RESULT AND DISCUSSION

A. Identification of the Date of Creation (DOC), the Date of Modification (DOM) and Hash Value

The date of creation and the date of modification play an important role in the process of authentication of audio files. If the media file is original and is in original place its date/ & time of creation (DOC) and date of modification (DOM) remains the same (**Table.1**) and it shows only these two dates. When the same file was copied to other destination/media it creates another/different file and the original file remains intact in its original place. Hence, the new created file shows new date of creation but as the file was not edited or modified the date of modification remains the same in the original file (**Table.2**). If the file moved from its original place to other place, its original DOC and DOM remains the same as the original (**Table.3**) because in this case the file has not been created nor be modified. The move, shift or transfer of the file was found possible in some special cases or same storage media. In some mobile devices it is possible to move audio file from its internal memory to its memory card or vice versa. When the file was edited and saved then it's both dates i.e. DOC and DOM will be changed (**Table.4**). The hash value of file depends on the file contents not file name, hence when the file moved, copied or renamed in any media/ destination it's hash value did not changes (**Table.5**).

B. **Identification of the recording source/device** The identification of recording source/device plays an important role for authentication of multimedia files. The digital recording devices generate the device info in its file signature hidden in its metadata. The source of recording/camera, which could be identified using software like Media Tab, Media Info and HXD (**Table.6**). In case of mobile recording the metadata shows only name of android version (**Table.9**). The recording device's make and model were identified in three crime cases which highlighted in Table.8.

C. **Identification of the editing software:** The original audio file contained the metadata of the recording device. The original file can be edited using any software tools and the same can be saved in same or other formats. When the edited audio file saved, its editing software uses different codec. The traces of editing tools can be identified using different software (fig.1.a &1.b).

The examiner can detect a change in the file from the original to the extended version with the help of a hexadecimal reader and the header information of the file format. The file format should match the file name extension. Depending on the device and brand, there may be information about the model, serial number, firmware version, time, date and length of the recording. It is useful to note the time stamps and compare them to the date and time claimed by the recordists as to when the audio was recorded.

D. Analysis of AMR Audio file using different software:

AMR (Adaptive Multi-Rate Codec File) is very common and compressed audio format used by 3G cell phones for call recordings or voice recordings. The AMR format uses a speech coding pattern. It encodes compressed spoken audio data and uses multi-rate codec, such as DTX, ACELP, CNG and VAD. AMR files can be played in a number of Windows-based media players, as well as mobile devices, such as Android, Apple, etc. [9]

File name and format	**01722610334_2019_01_16_09_18_55_694_out.wav**
Created	**16-01-2019 09:19**
Modified	**16-01-2019 19**

Table.1. Original File

File name and format	**01722610334_2019_01_16_09_18_55_694_out.wav**
Created	**26 February 2019, 16:43**
Modified	**16 January 2019, 09:19**
Accessed	**26 February 2019, 16:43**

Table.2. Copied file

File name and format	**01722610334_2019_01_16_09_18_55_694_out.wav**
Location	**Galaxy on seven pro/ToHcallrecorde/newfolder**
Size	**26 February 2019, 16:43**
Created	**16 January 2019, 09:19**
Modified	**26 February 2019, 16:43**

Table.3. Moved File

File name and format	**01722610334_2019_01_16_09_18_55_694_out.wav**
Created	**26 February 2019, 09:03:06**
Modified	**26 February 2019, 09:03:06**
Accessed	**26 February 2019, 09:03:06**

Table.4. Edited file

Track Name	**180904_001**
Performer	**My recording**
Encoded By	**SONY IC RECORDER MP3 3.1.2**

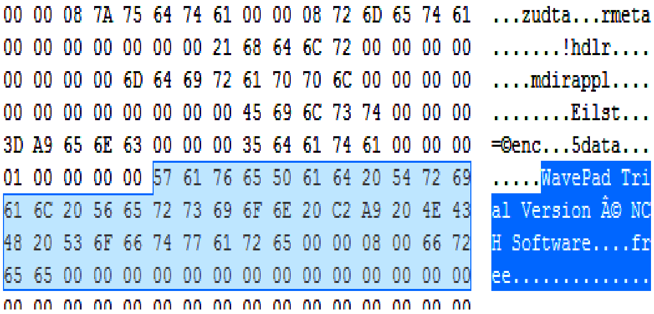
Table.5. Hash value of original and other files

SOURCE	FILE EXTENSION	ASCII	FILE SIGNATURE
SONY IC RECORDER	.MP3	ID3, VGEOB, SFMARKERS	4944 33, 76 47454F42, 53 664D6172 6B65 7273
	.WAV	.WAVEFMT	57 41 56 45 66 6D 74
	.M4A	. FTYPM4A	66 74 79 70 4D 34 41
	AMR		41 4D 52

Table.6. Recording Device Info Present

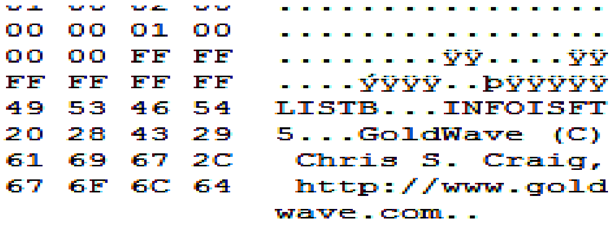
Encoded _Date	**UTC 2019-02-18 04:55:11**
Tagged_Date	**UTC 2019-02-18 04:55:11**
Book	**Bkmk**
com.adnroid	**8.0.0**

Table.7. Editing software details



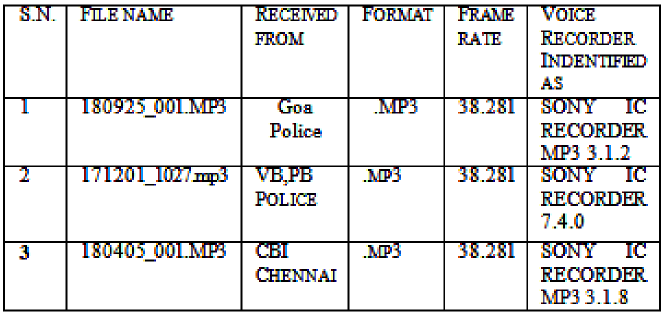
```
00 00 08 7A 75 64 74 61 00 00 08 72 6D 65 74 61  ...zudta...rmeta
00 00 00 00 00 00 00 21 68 64 6C 72 00 00 00 00  .......!hdlr....
00 00 00 00 6D 64 69 72 61 70 70 6C 00 00 00 00  ....mdirappl....
00 00 00 00 00 00 00 00 45 69 6C 73 74 00 00 00  ........Eilst...
3D A9 65 6E 63 00 00 00 35 64 61 74 61 00 00 00  =©enc...5data...
01 00 00 00 00 57 61 76 65 50 61 64 20 54 72 69  .....WavePad Tri
61 6C 20 56 65 72 73 69 6F 6E 20 C2 A9 20 4E 43  al Version Â© NC
48 20 53 6F 66 74 77 61 72 65 00 00 08 00 66 72  H Software....fr
65 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ee..............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Fig. 1.a. Editing Software i.e. Wavepad



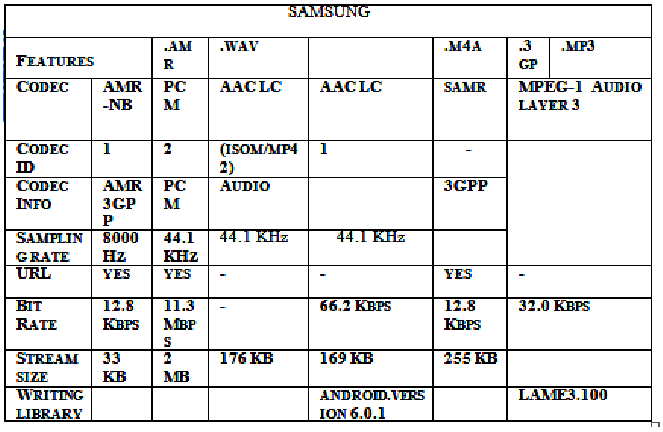
```
                   ................
00  00  01  00     ................
00  00  FF  FF     .........ÿÿ....ÿÿ
FF  FF  FF  FF     ....ýÿÿÿ..þÿÿÿÿÿ
49  53  46  54     LISTB...INFOISFT
20  28  43  29     5...GoldWave (C)
61  69  67  2C      Chris S. Craig,
67  6F  6C  64      http://www.gold
                   wave.com..
```

Fig. 1.b. Editing Software i.e. Goldwave



S.N.	FILE NAME	RECEIVED FROM	FORMAT	FRAME RATE	VOICE RECORDER INDENTIFIED AS
1	180925_001.MP3	Goa Police	.MP3	38.281	SONY IC RECORDER MP3 3.1.2
2	171201_1027.mp3	VB,PB POLICE	.MP3	38.281	SONY IC RECORDER 7.4.0
3	180405_001.MP3	CBI CHENNAI	.MP3	38.281	SONY IC RECORDER MP3 3.1.8

Table.8. Source Identification



SAMSUNG						
FEATURES		.AMR	.WAV		.M4A	.3 GP .MP3
CODEC	AMR -NB	PCM	AAC LC	AAC LC	SAMR	MPEG-1 AUDIO LAYER 3
CODEC ID	1	2	(ISOM/MP4 2)	1	-	
CODEC INFO	AMR 3GPP	PCM	AUDIO		3GPP	
SAMPLING RATE	8000 Hz	44.1 KHz	44.1 KHz	44.1 KHz		
URL	YES	YES	-	-	YES	-
BIT RATE	12.8 KBPS	11.3 MBPS	-	66.2 KBPS	12.8 KBPS	32.0 KBPS
STREAM SIZE	33 KB	2 MB	176 KB	169 KB	255 KB	
WRITING LIBRARY				ANDROID.VERSION 6.0.1		LAME3.100

Table.9. Audio File Signature

V. CONCLUSION

The outcomes of this study reveal that metadata properties and file's signature as well as the HEX data in ASCII (American Standard Code for Information Interchange) was found very helpful for identification of the source of recording. The make & model of the recording device, date of recording, date of modification, date of editing, the details of the software used for editing, including URL address, codec identification, and writing library was used to detect the tampering in the audio file. This simple and small practice was found very helpful for authentication of digital audio recordings and source identification at present juncture.

VI. ACKNOWLEDGMENTS

The authors are thankful to the Director, Central Forensic Science Laboratory, and Chandigarh for his valuable guidance.

VII. REFERENCE

[1] Koenig, B.E ."Authentication of Forensic Audio Recording " Journal of the Audio Engineering Society , Vol 38, no. 1 / 2 (1990).

[2] Eddy B. Brixen "Audio Engineering Society" Convention Paper 7014, presented at the 122nd Convention 2007 May 5–8 Vienna, Austria..

[3] Marcin Michałek " Problems of Forensic Sciences 2016, vol. 105, 355–369

[4] D. Hamdi, F. Iqbal, T. Baker, B. Shah " Multimedia File Signature Analysis for Smartphone Forensics" 2016 9th International Conference on Developments in eSystems Engineering.

[5] Grigoras, C "Digital audio recording analysis – the electric network frequency criterion" International Journal of Speech Language and the Law 12(1), 63–76 (2005.

[6] Kajstura, M., Trawinska, A., Hebenstreit, J. "Application of the Electrical Network Frequency (ENF) Criterion – A case of a Digital Recording" Forensic Science International 155, 165–171 (2005)..

[7] Cooper, A.J. " he electric network frequency (ENF) as an aid to authenticating forensic digital audio recordings – an automated approach, Conference paper" In: AES 33rd International Conference, USA (2008).

[8] D. Hamdi, F. Iqbal, T. Baker, B. Shah "Multimedia File Signature Analysis for Smartphone Forensics" 2016 9th International Conference on Developments in eSystems Engineering.

[9] Marcin Michalek,"Properties of recordind and audio files save in AMR format and an assesment of the possible of applying them in authenticity examination", Problems of Forensic Sciences 2017, vol. 109, 27–42.