C10 Forensic Analysis of Digital Audio File Structures and Formats

Catalin Grigoras, PhD*, 1020 15th Street, Ste 8I, Denver, CO 80202; and Jeff M. Smith, MS, National Center for Media Forensics - CU Denver, 1150 10th Street, Ste 177, Denver, CO 80217

After attending this presentation, attendees will better understand the process for building and deploying a database of audio samples for forensic purposes, specifically for use in the analysis of multimedia metadata, its structure, and characteristics of file formats.

This presentation will impact the forensic science community by disseminating results from the mass analysis of audio files in the Waveform Audio File Format Pulse-Code Modulation (WAV PCM) format produced/prepared by various recorders and software editors.

This presentation describes an extended study on the WAV PCM file structure and format analysis for forensic purposes. In conjunction with other analyses largely involving time and frequency domain measurements/plots, a framework for the authentication of digital audio includes analysis of the file structure and format as well as investigation of the suspected recording device itself.[1,2] Forensic audio is now commonly recorded as uncompressed .WAV files on small digital recorders and authentication of this evidence can end up being crucial in the courtroom. It is also common for digital audio recording systems that store data using a proprietary format and/or encoding to use custom software for conversion to WAV PCM. In the interest of authentication and establishing digital provenance of recordings, examples of traces left by different digital audio editors and converters will be presented.

The following table shows an example of the structure analysis results for four digital audio recorders from Alesis®, Olympus®, Marantz®, and Sony®, along with one Toshiba® audio converter. The preliminary results indicate that while some recorders and editors share the same file structure, other recorders and editors create files with additional metadata.

Alesis® PalmTrack	Olympus® DM-520	Marantz® PMD620	Sony® ICD-SX750	Toshiba® DMR-SX1
Ofs: 0 -> RIFF Ofs: 8 -> WAVE Ofs: C -> fmt Ofs: 24 -> data	Ofs: 0 -> RIFF Ofs: 8 -> WAVE Ofs: C -> fmt Ofs: 24 -> olym Ofs: 2D -> dss Ofs: 38 -> DM520 Ofs: 52 -> *timestamp* Ofs: 3F8 -> data	Ofs: 0 -> RIFF Ofs: 8 -> WAVE Ofs: C -> fmt Ofs: 24 -> bextZ Ofs: 154 -> *timestamp* Ofs: 386 -> data	Ofs: 0 -> RIFF Ofs: 8 -> WAVE Ofs: C -> fmt Ofs: 24 -> JUNK Ofs: 7F8 -> data	Ofs: 0 -> RIFF Ofs: 8 -> WAVE Ofs: C -> fmt Ofs: 26 -> data

Findings from an extensive study will be presented on the structure and format for WAV PCM files created by 31 commercially available digital audio recorders (example brands: Alesis®, Marantz®, Olympus®, Philips®, Roland®, SanDisk®, Sony®, Tascam®, Zoom®, etc.) and 20 processing and converting softwares (e.g., Adobe® Audition, DCLive Forensics, FFmpeg, Goldwave®, Olympus® DSS Player Pro, Sound Forge™, etc.). In addition to these findings, principles that can be followed in the collection and maintenance of reference sample databases for forensic analysis and how to use them in real cases when the suspect recorder is not available will also be shared.

Reference(s):

1. Grigoras C., Smith J.M. (2013) *Audio Enhancement and Authentication*. In: Siegel JA and Saukko PJ (eds.) Encyclopedia of Forensic Sciences, Second Edition, pp. 315-326. Waltham: Academic Press
2. Grigoras C., Rappaport D., Smith J. (2012) Analytical Framework for Digital Audio Authentication, *AES 46th International Conference*, Denver, USA

Audio Authentication, Multimedia Forensics, File Structure Analysis

*Presenting Author