C11 A Forensic Analysis of Digital Speech Standard (DSS) Files

Catalin Grigoras, PhD, National Center for Media Forensics, University of Colorado Denver, Denver, CO 80204; Cole Whitecotton, MSc, National Center for Media Forensics, University of Colorado Denver, Denver, CO 80204; Jeff M. Smith, MS, The MITRE Corp, McLean, VA 22182; Douglas S. Lacey, MS, BEK TEK LLC, Stafford, VA 22556-1353; Bruce E. Koenig, MFS, BEK TEK LLC, Clifton, VA 20124-1947; James Zjalic, MSc, Verden Forensics, Edgbaston, England B15 1TH, UNITED KINGDOM*

Learning Overview: After attending this presentation, attendees will better understand the unique properties that the DSS and DSS Pro (DS2) file formats contain in order to better assist with authentication of such recordings.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by providing detailed authentication information for forensic analysts to use while following best practices for authentication of recordings purported to be from these types of recorders.

This work presents an extensive study on DSS and DS2 files created with Olympus® and Philips digital audio recorders. The authenticity of digital audio recordings can be challenged or should be verified either before being accepted as evidence in legal proceedings or in ascertaining the veracity of an unknown file's meaning.[1] The framework for forensic authentication of digital audio includes the structure and format analysis that requires the investigation of the suspected recording device as well.[2] Sometimes the suspected recorder is not available for test reference recordings, which could lead some labs to reject the request for analysis. One of the goals of this study is to provide the scientific community with a framework to better help authenticate known and unknown recordings from the listed recorder types/models.

Over 1,000 sample recordings were taken from multiple models of both Olympus® and Philips digital audio recorders. Careful consideration for the various recording quality settings was used, ensuring that sufficient amounts of recordings were made at each level of quality available with each recorder. These are usually listed as Standard Play (SP), Long Play (LP), or Quality Play (QP) quality in the devices. Many settings remained consistent across the brands/models, but it was made sure that samples were collected from any setting that resulted in a DSS or DS2 file format. The only settings not used were those that resulted in something other than a DSS or DS2 file format, such as MP3, WMA, PCM-WAV, etc. A large subset of these recorders was also tested with both internal and external microphones to determine if the recorder left any traces of recording source in the metadata. The models tested include: (1) Olympus® DSS: DM-1, DM-10, DS-2, DS-20, DS-330, DS-2200; (2) Philips DSS: DPM-6000, DPM-930, DPM-9450, DPM-9600; and (3) Philips DS2: DPM-6000, DPM-9600.

This presentation continues previous research on WAV, MP3, WMA, and AAC files.[3] It presents the principles followed to collect and analyze reference samples, reports the findings, and proposes a methodology to analyze DSS and DS2 file structure and format for forensic purposes.

Reference(s):

1. Scientific Working Group on Digital Evidence (SWGDE). 2018. *Best Practices for Digital Audio Authentication*, Version 1.3.
2. Grigoras, C. et al. 2012. Analytical Framework for Digital Audio Authentication. *AES 46th International Conference, Denver, CO.*
3. Grigoras, C. et al. 2017. Large Scale Test of Digital Audio File Structure and Format for Forensic Analysis. *AES Conference on Audio Forensics, Arlington, VA.*

Audio Authentication, Metadata, Digital Audio Recorders

*Presenting Author