B9 A Case Study in 3GP File Analysis and Repair

Jeffrey M. Smith, MS, 2857 S Steele St, Denver, CO 80210; and Catalin Grigoras, PhD, 1020 15th St, Ste 8I, Denver, CO 80202*

After attending this presentation, attendees will understand some principles in digital data analysis, multimedia file structure and repair, and how to use various software tools to reconstruct multimedia metadata. Attendees will learn the relationship between recorded data and multimedia containers revealing the usefulness of Hex data analysis and the reverse engineering of file formats.

This presentation will impact the forensic science community by discussing a real case involving the analysis and repair of a corrupt 3GP file recorded by a cell phone. An overview of the QuickTime file format specification will be provided along with comparisons to various other format specifications. Hex data analysis of recorded media will be demonstrated, highlighting things to look for when analyzing file formats for repair.

Corrupt or incomplete media files are a common problem encountered during the course of investigations. In these cases, the recorded audio and/or video material may not be playable and, therefore, important information related to a case is irretrievable. File corruption may be due to any one of several reasons, such as: hardware malfunction resulting in the file not properly being closed or wrapped following the recording process, incomplete fragments of recordings were detected and carved from physical media during the course of data imaging and analysis, deletion and overwriting of media files have rendered them corrupt, etc. However, if a forensic media analyst is resourceful, the data structure of the file may be reverse engineered and repaired making playback possible, revealing the otherwise irretrievable recorded contents. In these cases, resourcefulness is the key because the process of file repair depends on the format and codec of the recording, and not all manufacturers implement technical specifications in the same way. This means that two 3GP files, for instance, recorded on different equipment will require different procedures for repair due to inconsistently structured data. When the organization of a media file's data structure is determined, analysis and repair may be possible by referring to available file format specifications and by using Hex viewing/editing software that displays a file's binary data in hexadecimal notation and ASCII text. Last, a software tool for reconstructing large amounts of data may be necessary where manual creation of Hex data is not possible. Once a file has been repaired, investigative review can take place, or further forensic analysis is made possible.

Following the presentation of this background information, technical details regarding the analysis, repair, and reconstruction of the recovered 3GP file in the case study which resulted in making a broken file playable will be discussed. The method used to repair the file is comprised of: hex data comparison of the evidence file to playable exemplar files recorded by the same phone, identification of the missing and inaccurate metadata that made playback not possible, reconstruction of the missing Hex data using Matlab software, and amendment of the corrupt file to make playback possible.

Multimedia Forensics, Audio Forensics, Hex Analysis

* *Presenting Author*