B10 Exploiting Metadata to Recover Multimedia From 3GP Fragment

Michael Piper, BA, United States Secret Service, 950 H Street, Northwest, Suite 4200 - FSD, Washington, DC 20223*

After attending this presentation, attendees will gain an understanding of how 3GP multimedia files, commonly used in cell phones, are structured and how that structure can be exploited to recover the audio and video contents of fragmented files.

This presentation will impact the forensic science community by bridging the gap between computer forensics and multimedia forensics within the digital and multimedia sciences by demonstrating a methodology for recovering the multimedia payload within a damaged or partially recovered 3GP file.

Cell phone forensics examinations are performed every day to recover existing and deleted data. Reviewing file fragments can be problematic depending on the type of data in the file and the scheme used to encode it. ASCII text characters have a direct representation in digital data and can be interpreted easily. Multimedia information (audio and video) is more complex. Audio and video encoders have evolved to exploit research into human perception with that from data redundancy reduction. This results in algorithms that are highly complex and have many variable options. Knowing the state of these variables distinguishes streaming multimedia from gibberish.

In this case study, a cell phone was recovered from a crime scene. A computer forensic analyst recovered one intact audio/video recording in the 3GP file format[1,2] (K1) and another fragment of a 3GP file (Q1). Attempts to play the fragment directly were not successful, but did suggest that information relevant to the crime was present. The two files were evaluated to recover the complete recording. This was done using the following steps: (1) examine the intact file to understand how this particular phone implements the 3GP standard; (2) examine the fragment to determine which 3GP structures are present and which are missing; and (3) use the structure of the intact file to infer or compute the missing Q1 metadata. Analysis of the fragment revealed that the “Media Data Box”, the audio/video payload of the file, was completely intact, but the “Movie Box”, the metadata describing the payload’s format and structure, was truncated.

Successful recovery was dependent upon three assumptions: (1) The Q1 audio and video data are interleaved within the Media Box, as in K1; (2) the Q1 audio data is encoded using adaptive multi-rate compression (AMR)[3], as in K1; and (3) the audio data in Q1 is structured similarly to that in K1. Since some of the metadata concerning the video payload of Q1 survived the truncation, these assumptions about the remaining audio structure were all that was required to recalculate the missing metadata to play the audio/video payload. Even though the image sizes were different between the intact file and the fragment, the process successfully recovered all of the audio/video data. The consistency of the 3GP implementation and the available redundancy of formatting information within the metadata were exploited to fill in the gaps. By successfully reconstructing the metadata, a standard multimedia viewer could be used to play the recording.

References:

[1] 3GPP TS 26.244 V7.2.0 (2007-06).
[2] ISO-14496-12:2005/ISO-14496-12:2005.
[3] 3GPP TS 26.090 V7.0.0 (2007-06).

Multimedia, Metadata, Cell Phone