C15 Accurate Video Reconstruction and Metadata Extraction From a Self-Executing Video File

Matthew Case, PhD, Audio and Video Analysis Unit, 1426 Saint Joseph Boulevard, Rm 1340, Ottawa, ON K1A 0R2, CANADA*

After attending this presentation, attendees will understand how video files can be wrapped inside proprietary Windows® executable video players and how the native video data can be extracted to ensure accurate playback and analysis.

This presentation will impact the forensic science community by demonstrating that native video data and metadata can be extracted from proprietary Windows® executable video players, thus allowing for a proper forensic analysis of the video.

Forensic video analysis has evolved in recent years to eschew the use of proprietary video players wherever possible in favor of independent playback using open source multimedia frameworks, such as FFmpeg, that can decode native video data. When analyzing native formats directly rather than through opaque proprietary third-party viewers, accurate metadata, such as storage aspect ratio and frame-level timing data, can often be established explicitly in a reliable and repeatable way, thus allowing for accurate playback and analysis; however, this approach is hindered when video data and player data are wrapped together as a single executable file and the native video data is not immediately identifiable.

This presentation will introduce two ways in which native video data can be contained within Windows® executable files. The first method is when the video data is written directly into the payload of the video player executable, so extraction relies simply on recognizing the video format start codes and carving out the data. With the second method, the executable is simply a data decompression utility, while its payload contains compressed video data along with other compressed files required for playback, such as the player executable itself, associated Dynamic Link Libraries (DLLs), and text files containing supplementary video information. As a result, directly carving out the (uncompressed) video file is not possible.

This second case will be discussed in detail using the "MP4Extract" class of video files as a case study. It will be shown, for this class of videos, how the compressed data can be identified within the executable, carved out and decompressed to yield a non-conforming (i.e., non-playable) MPEG-4 (Part 2) format video file. The metadata of the resulting video file can be fully decoded so all proprietary video information, such as camera number, accurate frame-level timing data and supplementary overlay data, can be exported for reference purposes. Furthermore, the extent of the video file's non-conformity will be presented and a solution to produce a fully conformant, readily playable video file will be outlined.

The approach outlined in this study also has broader implications for forensic video analysis. In particular, application to the authentication of digital video and metadata analysis of proprietary video file formats more generally will be discussed in the time remaining.

Data Carving, Metadata Analysis, Video Reconstruction