D76 Examination of Digital Video Formats Such as MPEG-1, MPEG-2, MPEG-4, 3GP, and AVI

Zeno J. Geradts, PhD, Rikkert Zoun, MS, and Jeroen van de Bos, BS, Netherlands Forensic Instistute, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS*

The goals of this presentation are to describe what kinds of video formats exist, explain what to do if a format is not playable, describe how to repair broken video streams, and to discuss integrity.

This presentation will impact the forensic science community by describing methods to repair a broken video stream with provided software.

Nowadays many video streams arrive in the laboratory for examination in digital format. Questions range from analysis of integrity, to finding and repairing fragmented or otherwise damaged video files. The number of digital CCTV-recordings is expanding due to security concerns. In many places surveillance cameras are present that can record crimes scenes. Furthermore, more people have phones with cameras in them.

The formats that are widely used on the market range from MPEG-1, MPEG-2, MPEG-4, 3GP and AVI. Many more formats exist, and sometimes they are also proprietary. Often CCTV-manufacturers have proprietary formats.

For forensic examination of damaged files it is important to know in detail on byte-level how a video file format is built up. The different standards of the file formats describe in detail how the file should be composed. Also manufacturers might implement the video file formats slightly different from the standard, such that regular players of video do not show the files correctly.

Damaged files might be found in unallocated clusters and slack space of hard drives and other data carriers. Also, one may find damaged or fragmented files in drives with a corrupted file system, or when analyzing internet interception data.

For analysis, we have developed the open source software tool DEFRASER, which can be downloaded from http://defraser. sourceforge.net. In this software it is possible to read in files that might include video streams. Also images of hard drives can be searched for video information in them. The different formats: MPEG-1, MPEG-2, MPEG-4, 3GP and AVI are supported. It is expected that other commonly used formats will follow. The software will reduce work that is needed otherwise since the specifications of the formats are included.

Simple actions such as using a header from another video file from the same camera is possible. Also more in-depth analysis of the separate data blocks is possible. It is also possible to write plug-ins for this software to analyze different formats.

In this presentation some examples are given of wiped video files which should be recovered. The software also keeps logs in order to know later how a file has been recovered. It should be combined with the use of regular hex editor, for the final forensic analysis. Hidden data such as date and time-stamps in the video files are important for investigation of integrity.

The tool itself is made open source such that it is easily possible to store and exchange knowledge of file formats for analysis.

Video, Formats, CODECS

 ** Presenting Author*