C29 Examination of Unknown Video Formats and Broken Video Streams

Zeno J. Geradts, PhD, and Rikkert Zoun, MS*, Netherlands Forensic Institute, Laan van Ypenburg 6, Den Haag, 2497 GB, Netherlands*

Methods for examination of unknown video files and the possibilities to examine the files in depth will be presented. The presenter will demon- strate a method of examination will result in more evidence in the court of information that was not visible before.

With the expanded use of different CCTV-systems and many new formats and CODECs for video streams and video files on the internet, examination of these files and streams is a non-trivial task.

CCTV-manufacturers often use proprietary formats in their systems, in such a way that the video files can only be viewed with their software. In practice, manufacturers will help by providing the software, or in some cases the software is already in the laboratory from an earlier case. If the software for viewing the images is not available, the file should be examined otherwise. The possibilities for this are very much manufacturer dependent. One method is with trial and error by using a database of available players. The risk with this method is that not the best quality is displayed on the screen, and that not all information (such as timelines) is available from the file. The other method entails examination of the file with software tools such as a hex viewer. In some systems, known headers, such as those from JPEG-images, can be retrieved and the information can be viewed. Often this kind of reverse engineering is too time consuming and will not work in practical cases. In theory however, one may find time- lines and other information from these streams.

With files that are examined from computers that are confiscated or even intercepted data streams, no information may be available on players that can be used. One can test the file with the known players, such as Microsoft Media Player and other available players. It is often necessary to examine the file to find information on the file format and the CODEC that has been used. If the file is from a known type such as AVI or MPEG, the structure of the file is known, and the file can be viewed. Examination of the file itself can also reveal more information of the origin of it, which is important in examination of movies containing child pornography and snuff movies.

It becomes more difficult if the streams or files are damaged. The files should be repaired to view them. In case of an AVI-stream the header might not be available anymore. In this case a header should be composed to view the video stream.

At the Netherlands Forensic Institute researchers started the devel- opment of a software tool to examine video files. This tool should recognize the format of video files and the CODEC that has been used, and will also repair broken or incomplete video streams from AVI and MPEG-2. This should result in a standard method of investigation of such video material. For forensic work, tools will be developed for the open source community, if possible. The reason is that anyone interested can verify the software for quality assurance and validation purposes and that others can also develop new functionality.

Formats and CODECs, Digital Evidence, Video

 ** Presenting Author*