B11 Video File Recovery and Playback of Partly Erased Videofiles

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

After attending this presentation, attendees will have an understanding of methods of repairing video files in forensic casework.

This presentation will impact the forensic science community by presenting an open source approach for the analysis of image and video files.

The use of in digital video is rapidly increasing. Analog CCTV systems are replaced by digital systems, digital cameras are increasingly popular and affordable, many mobile phones now come equipped with a camera, and high-bandwidth internet allows home users to share their recordings and download video material in larger quantities than ever before. When digital video content is an important part of case evidence, such as in cases of recorded child pornography or other recordable crimes, finding every last bit of video data and making it viewable can be crucial to the investigation.

This is not always as easy as simply searching the data carriers using regular operating system functionality. Deleted files can usually be found with typical forensic software, if they are not yet overwritten and still reside intact on an undamaged data carrier. In some cases, however, the deleted video files may be partly overwritten or file systems may be damaged, leaving the investigator only with fragments of files. Recognizing such fragments and rebuilding them to valid files that can be viewed using video playback software requires thorough knowledge of file format specifications and laborious manual data editing. Many digital forensic investigators lack the time to get into such details.

Netherlands Forensic Institute developed Defraser (Digital Evidence Fragment Search & Rescue), an open source software tool to help the investigator by searching for video file fragments and analyzing their integrity. It allows drag-and-drop combining of video file elements to create playable video files. The tool is plug-in-based, allowing users to store and share their knowledge of particular file formats by programming their own plug-ins.

The product can be downloaded including sourcecode from http://sourceforge.net/projects/defraser. This tool was developed open source, so that other people can write plug-ins, and also if other software engineers would like to review the code, this possibility exists, since it is not a black box approach. It can also be implemented in other products, since it is written under BSD license. Also other users with proposals for changes can submit these changes, and they will be implemented.

Within defraser, plug-ins for MPEG-1, 2 & 4,3GPP/QuickTime/MP4 and AVI are implemented, and new plug-ins developed based on casework. The user can also develop their own plug-ins with .net and C#. Examples are provided as reference.

The defraser tool could be developed further, with more plug-ins for other image and video file formats such as JPEG, ASF, FLV and Matroska. Forensic logging: trace results to source evidence files (using hash), and tools to automate the analysis. The tool can be used on large images of unkown data, to extract relevant video data. Since the tools also tries to visualize partly erased video, false hits might occur, and further analysis is necessary. In this presentation some examples will be presented in casework where repair was necessary, and this tool was useful for analysis.

Defraser, Video Streams, Recovery

 ** Presenting Author*