B10 Analysis of Corrupt Video Files With Open Source Initiative Defraser

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

After attending this presentation attendees will explore the forensic possibilities to analyze and restore video from files that are broken.

This presentation will impact the forensic science community by demonstrating the possibilities to investigate broken and partial video files and restoring them properly with less time compared to other methods.

Cameras may be seen in many places, recording persons and events. Sometimes the recordings are helpful as forensic evidence in court, providing insight into what happened at a crime scene, or which scenarios are possible. Also people often record videos of crimes with the purpose of assisting the police, or to record what has happened for other reasons. Sometimes people try to erase the video before it is given to or seized by the police, or the data storage may get corrupted, and the video is not playable anymore. Also, in cases such as lawful internet interception only parts of a video file may be recoverable. Slack space and unallocated clusters on a hard drive may also contain partial video files.

In these cases, the data carriers or damaged files can be examined and fragments that are found may be repaired with a hex editor and the specifications of the video file format. This usually involves a lot of reverse engineering and comparison with reference files from the same recording device or storage device.

For this type of examination the Netherlands Forensic Institute developed the software Defraser (abbreviation for Digital Evidence Fragment Search & Rescue). It helps the digital forensic investigator by searching for fragments of video files and displaying metadata such as recording time and video resolution. In the current version the user can view any valid keyframes that are found. It also allows creating new files by combining syntactic elements (headers) of video file fragments by dragging and dropping. This way, a broken video file can be repaired using headers from valid reference video files that have the same settings. Ideally, such reference files are recorded with the same camera type as the one under investigation. Defraser also has a wizard to help with header replacement. The software can log the links between the output of the software and the source evidence files. In court, such information can be used to completely reconstruct any resulting video files from the source evidence material.

The knowledge about video file formats is stored in plug-ins. Currently there are plug-ins available for the AVI, MPEG-1, 2, & 4, 3GPP/QuickTime/MP4, and ASF/WMV video file formats. A plug-in for H.264 is currently being developed. The software is developed in .NET and C#; and on the software engineering side, the structure is such that new plug-ins can be developed easily without too much rework by software engineers, reducing development time. The software is open source, so it can be downloaded for free from *http://sourceforge.net/projects/defraser*.

The benefits to making it an open source program are to give reviewers and other experts the possibility to do a code review of the forensic software as well as writing new plug-ins for other video formats, and also give vendors the possibility to include it in their software for further development. In practice, the code review does not often happen, since in general codes of thousands of lines are not easy to follow, even if there are many comments included on what exactly happens.

In practice, Defraser has proven to be useful in an increasing number of forensic cases. The approach saves time compared to reverse engineering and working with hex editors. The most notable advantage of Defraser over other recovery software is that it recognizes fragments of video files, as opposed to just full video files.

In this presentation several examples of where it works will be shown, but also cases in which the approach could not be used, as well as guidelines for carving of video files. Examples include cameras that have been used in skimming devices for banking cards and partially erased video files from mobile phones.

Defraser, Video, Multimedia

