



D29 Analysis and Visualization of Defective Digital Image Data

Stefan W. Ott*, Bundeskriminalamt, KI 22, Wiesbaden, Hessen D-65173, Germany

After attending this presentation, attendees will understand how to deal with digital image data, which are rejected, misinterpreted, or shown incompletely by standard image viewers, with emphasis on the JPEG file format.

This presentation will impact the forensic community and/or humanity by demonstrating the use of advanced tools for image data analysis and restoration, and how this extends the capabilities of forensic examinations to cases where no other method has a chance to recover the original visual information. This represents an important advantage in areas where image information is crucial for evidence and the risk of trying to destroy the data is high, e.g. in child pornography.

The introduction will sum up the main limitations of standard image viewers, give some typical reasons for the appearance of defective image files, and emphasize the importance of the JPEG standard. Some examples of visualizations of defective image files produced by standard viewers, compared with the results of thorough analysis and restoration, will be used to illustrate the potential gain.

An overview of useful tools will be given, including hex editors, graphic file format descriptions and analyzer tools, reconstruction software for image memory cards, scanner for image file signatures, image processing software with import functions for raw format, and so on. The capabilities and limitations of the different tools will be described and the missing functionality will be derived from a list of requested features.

Examples like AVIs with MJPEG, video surveillance data and fragments of JPEG streams, will illustrate the methods to identify and process case data where only moderate knowledge is required for successful recovery and restoration such as a single obvious wrong parameter in the file header or a false file extension. Additionally, these examples will demonstrate how hopeless cases, e.g. those where strong cryptography is involved, only small fragments are available or compressed data has been badly corrupted are recovered.

A relatively detailed examination of the structure of a JPEG stream, the important elements and their role in the decoding process will lay the foundation for a successful application of the JPEG toolkit JLab. For details the audience will be referred to the literature. Examples are demonstrated with screenshots of JLab-Sessions. The distribution policy of JLab will be explained and the use of JLab will be encouraged. A live demonstration with JLab will be given by Bernd Rieger in his contribution "A Presentation of JLab: Restoring Selected Examples of Corrupt JPEG Data." The problem of evidential proof will be discussed. The goal of the operation is not the perfect reconstruction but the correct visualization of the available image data. The conclusion will show that a perfect solution will never exist, describe the current state-of-the-art in image data analysis, and the plans for the further development of image data analysis tools.

Image File Analysis, Defective Image Files, Image File Restoration