B17 Recovering Multimedia From File Fragments

Michael Piper, BA, United States Secret Service, 950 H Street, Northwest, Suite 4200 - FSD, Washington, DC 20223*

After attending this presentation, attendees will gain an understanding of how multimedia files, commonly used in cell phones, are structured and how that structure can be exploited to recover the audio and video contents of fragmented files.

This presentation will impact the forensic science community by bridging the gap between the computer forensics and multimedia forensics disciplines by demonstrating a methodology for recovering the multimedia payload within damaged or partially recovered files.

Cell phone forensic examinations are performed everyday to recover existing and deleted data. Reviewing file fragments can be problematic depending on the type of data contained within the file and the scheme used to encode it. ASCII text characters have a direct representation in digital data and can be interpreted easily. Multimedia information (audio and video) is more complex. Audio and video encoders exploit human perception to reduce data redundancy. This results in algorithms that are highly complex and have many variable options. Knowing the state of these variables can distinguish streaming multimedia from gibberish.

In this case study, fragments of two deleted files recovered from separate cell phones will be examined – a 3GP file and an MP4 file. In each case, an exemplar file was provided from the phone. Attempts to play these fragments directly were not successful, but suggested that information was present. Successful decoding of the multimedia payload required understanding the file specifications of the data involved, exploiting the exemplar files to form assumptions that reduced the unknown variables, and exploiting existing metadata to calculate the missing metadata. Once sufficient metadata was reconstructed, a standard multimedia viewer could be used to play the recordings. **Multimedia, File Fragments, Recovery**

 ** Presenting Author*