C19 Android™ Thumbnails: Is There More? An In-Depth Analysis of the Android™ Photo Gallery and Camera Processes Looking for Metadata

Mary F. Horvath, MFS, 10035 Via Colomba Circle, #203, Ft. Myers, FL 33966; and Steven B. Watson, BA*, VTO, 325 Interlocken Parkway, Bldg C, Broomfield, CO 80021-8042*

After attending this presentation, attendees will expand their general understanding of how the Android™ mobile operating system's Gallery application interacts with the camera application/device and how to identify metadata that has being missed in current forensic software tools.

This presentation will impact the forensic science community by providing advanced forensic processing techniques intended to be used to recover critical metadata never before seen in mobile device analysis and image recovery. It will provide an in-depth understanding of the Android™ image processing subsystems as well as provide novel techniques for the manual analysis of the related data files.

The forensic analysis of mobile devices is one of the most critical components of many criminal investigations but never more so than with those involving child exploitation. With the ease of use and access to mobile devices, combined with the inexpensive availability of large data storage, cameras on mobile devices are becoming the default mechanism for picture taking by many communities, especially those which partake in matters of child pornography and exploitation.

One such case involves pictures of a missing girl assumedly taken with, and later deleted on, a Samsung™ mobile phone running the Android™ operating system. The thumbnail images were easily recovered through the use of common forensic software tools; however, since the images were recovered from the Gallery application's cache files, no metadata was recovered that was directly connected to the images in question. The question arose as to whether it can be proven that the actual camera on the cell phone took the pictures and whether the pictures could have been taken around the same time the child went missing. The answers to these questions could provide demonstrable proof of a suspect's participation with a victim at the time of a suspected criminal act.

Deleted pictures on a mobile phone are not uncommon and often only the thumbnail images remain recoverable by current forensic software tools. Thumbnail image recovery is a common technique utilized by mobile forensic analysts during typical cell phone examinations and is usually completed through the carving of graphic file formats from cached storage areas on the device, such as a thumbnail cache. On an Android™ operating system, this is usually accomplished by performing a carving process on the "imgcache" file (a common name, not literal filename) or set of files. While the cache file itself has been fairly well documented, the processes behind the creation and writing to these files and the entire Gallery cache subsystem, as well as what interactions with the device impact these files and how, have not been documented in much detail. There are multiple files that can be impacted by the Gallery application, one of which has been overlooked to date, and it may hold the clues to a missing girl's demise.

The files created by the Gallery application were analyzed for this research to determine whether metadata beyond the thumbnail image itself can be recovered. The entire Gallery process was researched, tested, and analyzed to make a more thorough determination as to the operations of the Gallery application, its interaction with the camera subsystem, and whether advanced forensic processing techniques could be used to successfully recover critical metadata never before seen. This presentation will provide the methods of testing designed and implemented to attempt to answer the investigative questions and determine whether additional metadata is available for recovery. The results of the testing processes and research will be provided, along with new defined processes that can be implemented for data recovery and extraction.

The opinions or assertions contained herein are the private views of the author and are not to be construed as official or as reflecting the views of the author's employer. Names of commercial manufacturers or products included are incidental only, and inclusion does not imply endorsement by the authors or their employer.

Digital Evidence, Mobile Forensics, Data Recovery

*Presenting Author