C1 Differential Forensic Analysis of Periodic Mobile Forensics Images

Mark D. Guido, MS, The MITRE Corporation, 7515 Colshire Drive, Mclean, VA 22102*

After attending this presentation, attendees will better understand applying comparison forensic images from mobile devices before, during, and after an event/mission for rapid and targeted triage.

This presentation will impact the forensic science community by demonstrating the research and results of an automated mobile forensic image comparison capability.

Differential analysis of forensic images or, in other words, the direct comparison of forensic images before, during, and after an event of interest allows forensic examiners the ability of avoiding analyzing a large amount of information that hasn't changed and instead focus on the data that has changed between images.[1] This has the effect of greatly speeding up analysis and intelligence gathering.

Periodic Mobile Forensics (PMF) is a research project that automates differential analysis to address some new-use cases: (1) mission hotwash — users control the starting point of the device, and compare the device at the end of the mission to gather data, identify usage, and assess whether the device was targeted or compromised during the mission; and, (2) travel to areas of concern — the device is used during travel to potentially hostile areas, when users want to assess whether it was targeted or compromised.

There are a few unique capabilities in PMF's approach to differential analysis. First, in the above used cases, PMF needs only to temporarily modify the device (sometimes even only after mission usage) and can reset the device back to the stock image, with no on-device software indicative of any modifications. Second, PMF is an automated differential analysis system, not based upon changes to files, but rather by blocks (bit runs) of data. PMF hashes the entire Negative And (NAND) storage by offset and only needs to collect the data that has changed on the device during the event of interest. The fact that PMF only needs to collect changed data speeds up collection, allowing PMF to potentially collect over bandwidth constrained mediums (such as mobile broadband), and allows PMF to immediately report on device integrity without having to address what file may have changed on the device.

PMF automates the generation of certain views into the collected data in support of differential analysis. PMF can generate a heat map of the changed data on each of the device partitions. PMF can gather audit information from the device during the usage period between the initial forensic image and the final forensic image, utilizing a series of forensic processes that target-specific and potentially important device usage information. PMF has the ability to target and visualize all added, deleted, or changed files and directories exclusively during the event of interest. These visualizations supplied during differential analysis help forensics examiners to quickly target the forensically significant data.

Reference(s):

1. Garfinkel S., Nelson A.J., Young J. A general strategy for differential forensic analysis. *Digital Investigation* 9 (2012): S50-S59.

Differential Forensics, Post Event, Image Comparison

*Presenting Author