C31 Rapid Differential Forensic Acquisition Using Limited Resource Computing

Mark D. Guido, MS, The MITRE Corporation, Mclean, VA 22102; Vikram Harichandran, MS, Fairfax, VA 22031; Glenn A. Melton, BS, The MITRE Corporation, Mclean, VA 22102*

Learning Overview: The goal of this presentation is to describe further development of a previously presented topic, Rapid Differential Forensic Imaging, to be applied on an appliance-based computer with limited computing resources.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by demonstrating a reference architecture addressing a limited resource computing environment typically found during forensic investigations.

In 2016, an automated differential forensic acquisition technique and algorithm that uses baseline datasets and hash comparisons to limit the amount of data sent from a mobile device to an acquisition endpoint was introduced. It was possible to produce forensically validated bit-for-bit copies of device storage in significantly reduced amounts of time compared to common commercial products. For example, using this technique, an average initial imaging rate of less than seven minutes per device for a corpus of actively used, real-world 16 GB Samsung™ Galaxy smart phones was successfully achieved. If the need arose for further acquisitions of the same device, then the timeframe for those acquisitions would be significantly quicker due to the information gained and utilized from the initial acquisition. A reference implementation of the algorithm and architecture was developed, and the technology has been successfully transferred to customers and industry.[1]

Now, a new implementation of the software running on a tiny form-factor limited-resource computing device is introduced. The device chosen was a Raspberry PI3 Model B, although it is thought that most low-resource computing platforms would be able to identify and host this described reference implementation. This device is considered an appliance-based form of the original algorithm and software, where power considerations, processing power, persistent storage, and volatile memory all needed to be refactored to make a viable solution. This addresses the use case of a limited resource environment typically found when forensic acquisition is required in the field. The process for forensic acquisition had to change when no longer provided the luxury of always-on connectivity between the front-end client and back-end server and storage was no longer provided. It was also necessary to monitor the consumption of power, processing, storage, and memory so as not to enter an exhausted state.

Details of the architectural changes, resource considerations, and in-field testing are documented herein. The changes made for the limited computing reference implementation can also address other use cases in which one or more resources may be reduced or limited, as is the case for low bandwidth, cross-geographic communications of forensic images. Those use cases will also be briefly addressed.

Reference(s):

1. Guido, M., J. Buttner, and J. Grover. Rapid Differential Forensic Imaging of Mobile Devices. *Digital Investigation.* 18 (2016): S46-S54.

Differential Forensics, Acquisition, Appliance

*Presenting Author