

An ordered selective imaging and distributed analysis computer forensics model

ABSTRACT

The traditional computer forensics procedures and tools collect and analyze the entire user data. This scenario has been proven to be not appropriate any more due to increased size of user data and storage. Accordingly, selective imaging and distributed analysis concepts have been introduced in the literature to reduce the digital evidences collection and analysis costs (time and resources). Current selective imaging approaches image the relevant data according the order of their selection and not according to their physical offsets order inside the targeted storage. Furthermore, integrating the selective imaging and distributed analysis has not been considered yet. This study proposed a computer forensics investigation process that provides an efficient imaging and scalable analysis. The selected data artifacts are first ordered upon their physical offsets. Then, based on the selected data size and available investigation time, the selected data are imaged into one or more partial forensic image in such a way that the produced images can be analyzed by different investigators and using several machines. An Advanced Forensic File Format 4 (AFF4) is used as a container for the collected relevant data. An experiment study has been used to evaluate the performance of the selected imaging process. The result shows that, even if ordering the selected digital evidences has a small performance negative impact but it has a positive effect on the performance of the selective imaging process itself. A qualitative study has been also used to evaluate the system and management scalability of the distributed analysis.

Keyword: Computer forensics; Selective imaging; Digital evidences; Efficiency; Distributed analysis