SOUTH AFRICAN INSTITUTE OF ELECTRICAL ENGINEERS

Reference Architecture for Android Applications to Support the Detection of Manipulated Evidence

H. Pieterse, M.S. Olivier and R.P. van Heerden

Defence, Peace, Safety and Security, Council for Scientific and Industrial Research, Pretoria, South Africa E-mail: hpieterse@csir.co.za
Department of Computer Science, University of Pretoria, Pretoria, South Africa E-mail: molivier@cs.up.ac.za
Meraka Institute, Council for Scientific and Industrial Research, Pretoria, South Africa E-mail: rvheerden@csir.co.za

Abstract

Traces found on Android smartphones form a significant part of digital investigations. A key component of these traces is the date and time, often formed as timestamps. These timestamps allow the examiner to relate the traces found on Android smartphones to some real event that took place. This paper performs exploratory experiments that involve the manipulation of timestamps found in SQLite databases on Android smartphones. Based on observations, specific heuristics are identified that may allow for the identification of manipulated timestamps. To overcome the limitations of these heuristics, a new reference architecture for Android applications is also introduced. The reference architecture provides examiners with a better understanding of Android applications as well as the associated digital evidence. The results presented in the paper show that the suggested techniques to establish the authenticity and accuracy of digital evidence are feasible.