

SMARTPHONES AS DISTRIBUTED WITNESSES FOR DIGITAL FORENSICS

Heloise Pieterse and Martin Olivier

Abstract

Smartphones have become an integral part of people's lives during the last few years. Their wide range of capabilities and support of additional applications cause a wealth of information to be stored on these devices. Although tools are available to extract and view the data stored on smartphones, there is currently no comprehensive process that allows for event reconstruction using the collected data. The large volume of data collected from the smartphones come in the structured format of SQLite databases and therefore can be easily transformed. To perform event reconstruction, the various SQLite databases need to be integrated and this is accomplished by using existing knowledge of distributed databases. This paper proposes a new process, called the Mobile Event Reconstruction Process, which allows for the reconstruction of events by querying the integrated SQLite databases collected from multiple smartphones. The outcome of the Mobile Event Reconstruction Process creates a detailed account of the activities that took place before, during and after an incident.