ABSTRACT

Social media platforms and smartphones have been inevitably effecting our lives. Many people prefer to use mobile applications for several reasons. However, they generally do not know the artifacts they left in smartphones. Due to an increasing frequency of encountering smartphones related to various crimes, the need for new approaches in mobile forensics area is increased. Investigating the artifacts of mobile applications may help to find various evidences.

This thesis provides an overview of files and directories created by popular social media applications. Two popular smartphones with six most used social media mobile applications were taken into consideration. Mobile applications were downloaded from official stores and example scenarios were prepared for each. Both logical and physical imaging of smartphones were performed. Low level modifications like rooting and jailbreaking were accomplished for physical imaging. Both commercial and open source tools were used for imaging and analysis.

The results of the research emphasizes that mobile social media applications generally create database files, log files, xml files and plist files to store most of the private and evidentiary data. The contents of these files can be obtained easily. Malware infection or device lost may cause the malicious usage of the private data. Many ethical concerns also come into question for mobile forensic investigators. They should pay attention to the confidentiality of private information irrelevant to the case.