Abstract

Nowadays, Instant Messenger (IM) applications (apps) have always been a main area of research for forensic examiners. IM apps are used by most of the people in the world since its' low cost to operator centered messaging services. Digital forensic examiners often conduct forensic analysis of Instant Messenger application for Android devices. After considering the existing research work in this field, this paper focused on conducting forensic analysis on IM's for android devices IMO. Tests were conducted on two android devices. The tests consisted of installing the IMO application on each Android device, conducting common user activities through the application, acquiring the physical image of each acquired logical image. The forensic analysis was aimed at finding the ways of determining the structure of folders in IMO application. If so, what and where are the contents of those folders to be used as forensic evidence? The test results show that the structure of folders in IMO application can be analyzed by acquisition process and it is stored on internal memory of Android devices in which it has consisted of 6 folders, in which 2 folders of them have subfolders that are consisted of image and videos from user activities and it could be studied by forensic examiners.
Forensics Acquisition and Analysis Method of IMO Messenger

References

Index Terms

Computer Science  Communications

Keywords

Instant messenger application, Android, IMO, forensic examiners.