Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices

ABSTRACT

In today's Internet-connected world, mobile devices are increasingly used to access cloud storage services, which allow users to access data anywhere, anytime. Mobile devices have, however, been known to be used and/or targeted by cyber criminals to conduct malicious activities, such as data exfiltration, malware, identity theft, piracy, illegal trading, sexual harassment, cyber stalking and cyber terrorism. Consequently, mobile devices are an increasing important source of evidence in digital investigations. In this paper, we examine four popular cloud client apps, namely OneDrive, Box, GoogleDrive, and Dropbox, on both Android and iOS platforms (two of the most popular mobile operating systems). We identify artefacts of forensic interest, such as information generated during login, uploading, downloading, deletion, and the sharing of files. These findings may assist forensic examiners and practitioners in real-world examination of cloud client applications on Android and iOS platforms.

Keyword: Digital forensics; Cloud forensics; Cloud storage applications forensics; Android forensic; iOS forensic