Windows instant messaging app forensics: facebook and skype as case studies

ABSTRACT

Instant messaging (IM) has changed the way people communicate with each other. However, the interactive and instant nature of these applications (apps) made them an attractive choice for malicious cyber activities such as phishing. The forensic examination of IM apps for modern Windows 8.1 (or later) has been largely unexplored, as the platform is relatively new. In this paper, we seek to determine the data remnants from the use of two popular Windows Store application software for instant messaging, namely Facebook and Skype on a Windows 8.1 client machine. This research contributes to an in-depth understanding of the types of terrestrial artefacts that are likely to remain after the use of instant messaging services and application software on a contemporary Windows operating system. Potential artefacts detected during the research include data relating to the installation or uninstallation of the instant messaging application software, log-in and log-off information, contact lists, conversations, and transferred files.