Forensics Analysis from Cloud Storage Client Application on Proprietary Operating System

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 143 - Number 1

Year of Publication: 2016

Authors:
Amirullah Amirullah, Imam Riadi, Ahmad Luthfi

10.5120/ijca2016907696
{bibtex}2016907696.bib{/bibtex}

Abstract

Increased use of cloud storage services have become a necessity alternative that complements the main storage media in everyday activities because it offers ease of doing automatic backups, sharing files and photos and so forth on a variety of computing devices and smartphones. It is very possible loopholes for criminals to store illegal files or matters relating to such activities. There are various types of cloud services with each type having a different potential use in criminal activities. One area of difficulty is the identification and acquisition of potential data when different services can be exploited by criminals. Because geographically cloud servers scattered in various regions. This causes difficulties for digital forensic investigators will add time and expense, to contact all potential service providers to determine whether the data stored in the server cloud services. This paper presented at a target on the client side user application to help find the data remnant on the use of cloud storage applications of various service provider on the proprietary operating system focuses on the Windows 10 platform. Results from this research include a variety of state after the install, deleted and uninstall web browser and memory, in order to find digital evidence. Based on the
test results the success index average was 82.63% and the remaining can not be analyzed, the results depend on various state, procedures and tools that are used, the research can be carried out smoothly.

References


Index Terms
Keywords