Abstract

Computer forensics can be defined as obtaining computer storage media so that data can be used as evidence in court. Traditionally the analysis of sources of digital evidences is done by examining the artefacts and metadata of artefacts for authenticating the gathered information and sequencing them in the manner they occurred. Analyzing the information acquired by forensic investigator in traditional way is a cumbersome task but it can be overcome if all the related artefacts are grouped together on the basis of metadata information they prevail. This paper is mainly focused on metadata based association of digital evidences which can simplify the task of forensic investigator and can also help in reducing human intervention making the process automatic. The main objective of this paper is to study working principal and compare different existing forensic tools on the basis of various parameters such as capability for accessing digital evidence, sources they can examine, metadata parsing capability, and analyzing them that whether they can provide grouping of different artefacts present in same or different investigating sources on the basis of metadata they contain. General Terms
Survey of Forensic tools on the basis of metadata extraction property.

References

32. www.freeviewer.org/bkf last retrieved on March 12, 2016


Index Terms

Computer Science  Databases

Keywords

Digital evidence, Binary abstraction, File system and schema support, Metadata, Evidence composition