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 prevails. 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.
Survey of Forensic tools on the basis of metadata extraction property.

References


Proceedings of the Second Intl. Workshop on Systematic Approaches to Digital Forensic
Engineering (SADFE ’07).
Research: DFRWS Technical Report, DTR - T001-01 FINAL
Carver, Paper presented at the 5th Annual Digital Forensics Research Workshop (DFRWS ’05)
the 3rdAnnual Digital Forensic Research Workshop (DFRWS ’03).
Research Workshop (DFRWS ’06) 3(Supplement 1), pp. S65-S70.
27. CarrierBD,(2003), Sleuthkit,http://www.sleuthkit.org/sleuthkit/, last retrieved on July 12,
2011
0-32-126817-2
XML-based indexing and querying for digital forensics. Digital Investigation, The Proceedings of
the 6th Annual Digital Forensic Research Workshop (DFRWS ’06), 3(Supplement 1), pp. 50-58.
32. www.freeviewer.org/bkf last retrieved on March 12, 2016
33. https://www.foxtonforensics.com/browser-history-capturer/ last retrieved on March 12,
2016
Based Associations in Digital Evidence, In Proceedings of the 2013 8th International Workshop
on Systematic Approaches to Digital Forensics Engineering (SADFE), IEEE
35. Minack E., Pau R., Cost ache S., Demartini G., Gaugaz J., Ioannou E., Chirita P-A, and
Nejdl W., (2010), Leveraging personal metadata for Desktop Search: The Beagle ++ System,
Journal of Web Semantics: Science, Services, and Agents on the WWW, Elsevier Science
36. Zander S., Nguyen T. And Armitage G. (2005)., Automated Traffic Classification and
Application Identification using Machine Learning, In Proceedings of the IEEE Conference on
250-257.


**Index Terms**

Computer Science

Databases

**Keywords**

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