World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:14, No:10, 2020

A Novel Methodology for Browser Forensics to Retrieve Searched Keywords from Windows 10 Physical Memory Dump

Authors : Dija Sulekha

Abstract : Nowadays, a good percentage of reported cybercrimes involve the usage of the Internet, directly or indirectly for committing the crime. Usually, Web Browsers leave traces of browsing activities on the host computer’s hard disk, which can be used by investigators to identify internet-based activities of the suspect. But criminals, who involve in some organized crimes, disable browser file generation feature to hide the evidence while doing illegal activities through the Internet. In such cases, even though browser files were not generated in the storage media of the system, traces of recent and ongoing activities were generated in the Physical Memory of the system. As a result, the analysis of Physical Memory Dump collected from the suspect's machine retrieves lots of forensically crucial information related to the browsing history of the Suspect. This information enables the cyber forensic investigators to concentrate on a few highly relevant selected artefacts while doing the Offline Forensics analysis of storage media. This paper addresses the reconstruction of web browsing activities by conducting live forensics to identify searched terms, downloaded files, visited sites, email headers, email ids, etc. from the physical memory dump collected from Windows 10 Systems. Well-known entry points are available for retrieving all the above artefacts except searched terms. The paper describes a novel methodology to retrieve the searched terms from Windows 10 Physical Memory. The searched terms retrieved in this way can be used for doing advanced file and keyword search in the storage media files reconstructed from the file system recovery in offline forensics.

Keywords : browser forensics, digital forensics, live Forensics, physical memory forensics
Conference Title : ICCFCS 2020 : International Conference on Cyber Forensics and Cyber Security
Conference Location : London, United Kingdom
Conference Dates : October 22-23, 2020

Open Science Index, Computer and Information Engineering Vol:14, No:10, 2020 publications.waset.org/abstracts/128686.pdf