Abstract

Since the lives of the persons are on the edge after being convicted in digital crimes. The main goal of digital forensics is to extract accurate evidence which determines whether the convict is guilty or not. The recent challenge is due to the big size of data that the investigator may deal with. These data stored in unnoticeable tiny devices such as USB sticks which may lead to a muddled decision because of the tediousness of the investigation. Fortunately, in Windows Operating systems, all users' transactions are stored in a central point which is known as Windows Registry. It stores all hardware and software configurations, user activities, and transactions. Therefore, digital forensics based on Windows registry is considered as a hot research field. This paper presents a proposed framework for digital crime investigation based on Fuzzy logic. It helps the investigator in the decision making phase about the evidence. This deals with the extracted evidence from relevant Windows Registry keys. Also, tracking the usage of USB devices for data theft was presented. Finally the proposed framework was tested on a simulated case study.
References

- Mathieu Gorge: USB and other portable storage device usage: Be aware of the risks to your corporate data in order to take pre-emptive and/or corrective action, Elsevier Vol 2005(Issue 8), Pages 15-17, (2005)
- Zhenhua Tang Hong Ding, Ming Xu, Jian Xu: Carving the Windows Registry Files Based on the Internal Structure&apos;, in The 1st international conferences on information science & engineering, ed., The 1st international conferences on information science and engineering, pp: 4788- 4791, (2009)
- George J. Silowash, and Christopher King &apos;Insider Threat Control: Understanding Data Loss Prevention (DLP) and Detection by Correlating Events from Multiple Sources&apos;, Technical report, Carnegie Mellon University, pp:1-17, (2013)
- Peter Hipson. Mastering Windows XP Registry, SYBEX Inc. (2002)


Index Terms

Computer Science

Fuzzy Systems
Keywords

Computer forensics  Crime investigation  Fuzzy logic  Data theft based on USB storage