World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:03, 2014

The Use of Ontology Framework for Automation Digital Forensics Investigation

Authors : Ahmad Luthfi

Abstract : One of the main goals of a computer forensic analyst is to determine the cause and effect of the acquisition of a digital evidence in order to obtain relevant information on the case is being handled. In order to get fast and accurate results, this paper will discuss the approach known as ontology framework. This model uses a structured hierarchy of layers that create connectivity between the variant and searching investigation of activity that a computer forensic analysis activities can be carried out automatically. There are two main layers are used, namely analysis tools and operating system. By using the concept of ontology, the second layer is automatically designed to help investigator to perform the acquisition of digital evidence. The methodology of automation approach of this research is by utilizing forward chaining where the system will perform a search against investigative steps and atomically structured in accordance with the rules of the ontology.

Keywords : ontology, framework, automation, forensics
Conference Title : ICCIE 2014 : International Conference on Computer and Information Engineering
Conference Location : Istanbul, Türkiye
Conference Dates : March 24-25, 2014