Identification of Suspected Files using Timeline Construction Approach

Gaurav Balaiwar and Upasna Singh
Dept. of Computer Engineering,
Defence Institute of Advanced Technology (DU),
Girinagar, Pune, India
{mcse12gaurav, upasnasingh}@diat.ac.in

As the usage of computer increases, the chances of these systems being involved in criminal activity also increase. So there is need to detect the evidence out of these cybercrime activities and convict the criminal in a court of law. The principal challenge in this field is to collect the evidences from large volumes of drive and convert them into human readable formats that can make it acceptable in a court of law. From the viewpoint of digital forensics, hard drives store large amount of information that can be considered as a useful thing in digital investigations. A digital timeline is defined as the representation of time-based details of any digital information described in a human-readable manner. It contains useful information related to a specific suspected event. Timestamps in digital investigation are vibrant for deciding not only when an event happened, but also in what order multiple events took place. This paper describes the automated approach which will detect the evidences from suspected system. The detected evidence is indexed by its time variables and plotted on a timeline. Python library is used to implement the proposed approach.