Abstract

As existing technology used by criminal rapidly changes and growing, digital forensics is also growing and important fields of research for current intelligence, law enforcement and military organizations today. As huge information is stored in digital form, the need and ability to analyze and process this information for relevant evidence has grown in complexity. During criminal activities crime committed use digital devices, forensic examiners have to adopt practical frameworks and methods to recover data for analysis which can comprise as evidence. Data Preparation/ Generation, Data warehousing and Data Mining, are the three essential features involved in the investigation process. The purpose of data mining technique is to find the valuable relationships between data items. This paper proposes an approach for preparation, generation, storing and analyzing of data, retrieved from digital devices which pose
as evidence in forensic analysis. Attribute classification model has been presented to categorized user files. The data mining tools has been used to identify user ownership and validating the reliability of the pre-processed data. This work proposes a practical framework for digital forensics on hard drives.

References

- Data Mining Concepts and Techniques, 2ed by Jiawei Han, Kamber M Morgan 2005. Kaufmann Publishers.
Identification of User Ownership in Digital Forensic using Data Mining Technique

of the ACM Conference on Knowledge Discovery and Data Mining (KDD).

Index Terms

Computer Science  
Security

Keywords

Digital Forensic  Hard Drive  Framework  Data Preprocessing