Abstract

Network forensics is a type of digital forensics which goal is to monitoring, correlate, examine and analysis of computer network traffic for various purposes like- information gathering, legal evidence, or intrusion detection. Now a days, various services like email, web, online transactions are used as network communication schemes. The purpose of this paper is to give an overview of different real time security mechanisms for forensic investigation of network communication schemes.

References

Network Forensic System," IP Multimedia Communications, A Special Issue from IJCA
5. "SANS Institute InfoSec Reading Room", SANS Reading Room
10. Udo Payer, "Realtime Intrusion-Forensics,A First Prototype Implementation(based on a stack-based NIDS) " TERENA Networking Conference, 2004
11. Pavel Laskov "Reactive Security and Intrusion Detection," University of Tubingen"

**Index Terms**

Computer Science Networks

**Keywords**

Network forensics, IDS, SIDS, HIDS, AIDS