Abstract

Internet is the most powerful medium as on date, facilitating varied services to numerous users. It has also become the environment for cyber warfare where attacks of many types (financial, ideological, revenge) are being launched. The e-commerce transactions being carried out online are of major interest to cybercriminals. The Internet needs to be protected from these attacks and an appropriate response has to be generated to handle them to reduce the impact. Network forensics is the science that deals with capture, recording, and analysis of network traffic for investigative purpose and incident response. There are many tools which assist in capturing data transferred over the networks so that an attack or the malicious intent of the intrusions may be investigated. This paper presents a generic framework for network forensic analysis by specifically identifying the steps connected only to network forensics from the already proposed models for digital investigation. Each of the phases in the framework is elucidated. A comparison of the proposed model is done with the existing models for digital investigation. Research challenges in various phases of the model are approached with specific reference to network forensics.
Reference

- PyFlag, http://www.pyflag.net
- SiLK, http://silktools.sourceforge.net/
- SiLK, http://tools.netsa.cert.org/silk/

**Index Terms**

Computer Science  
Security

**Key words**

Network Forensics  
Traffic Analysis  
Traceback  
Attribution  
Incident Response