A NEW APPROACH FOR RESOLVING CYBER CRIME IN NETWORK FORENSICS BASED ON GENERIC PROCESS MODEL

Mohammad Rasmi[1], Aman Jantan[2], Hani Al-Mimi[3]

[1, 2]School of Computer Sciences, Universiti Sains Malaysia
[3]Faculty of Science & Information Technology, Al-Zaytoonah University
[1, 2]Penang /Malaysia, [3]Amman /Jordan

Abstract

[1]mr77mr@hotmail.com, [2]aman@cs.usm.my, [3]hani_mimi@yahoo.com

Current network forensics approaches are costly and time consuming. Normally, these approaches use active and reactive processes to resolve cyber-crimes. Such processes start after the cyber-crime has been identified, which makes identifying useful evidence difficult. Moreover, the information required to understand and resolve cyber-crimes are limited. This paper proposes a new approach to resolve cyber-crime in network forensics. The proposed approach aims to use cyber-crime evidence to help investigators to resolve cyber-crime efficiently. The paper presents the current network forensics approaches and various existing digital forensics models in order to determine the suitable process to be used in the proposed approach. Thus, the proposed approach is based on a generic and modern process model for network forensics.

Network Security, Cyber-crime, Network forensics.