Using the Actionable Intelligence Approach for the DPI of Cybercrime Insider Investigation

Da-Yu KAO

Department of Information Management, Central Police University, Taoyuan 333, Taiwan

dayukao@gmail.com

***Abstract*—Cybercrime threats are often originating from trusted, malicious, or negligent insiders, who have excessive access privileges to an organization's network, system, or data. The sophistication of insider threats has led to cybercrime issues. Even when an incident is detected, the follow-up countermeasures are required to analyze the results. The analysis of cybercrime insider investigation presents many opportunities for actionable intelligence on improving the quality and value of digital evidence. There are several advantages of applying Deep Packet Inspection (DPI) methods in cybercrime insider investigation. This study discusses the importance of actionable intelligence to conduct investigations and addresses the countermeasure of a cybercrime insider investigation with DPI to detect anomalies in network packets.**

***Keyword*—Deep Packet Inspection, Digital Evidence, Insider Investigation, Actionable Intelligence, Network Forensics**

Da-Yu Kao received the B.S. and M.S. degree in Information Management from Central Police University, Taiwan, in 1993 and 2001, the Ph.D. degrees in Crime Prevention and Correction from Central Police University, Taiwan, in 2009, respectively. From 1993 to 1996, he was with Taipei City Police Department, Taiwan, where he was an information technology police officer involved in the development of policing information systems. From 1996 to 2007, he was with Criminal Investigation Bureau, National Police Administration, Taiwan, where he was a detective and forensic police officer in cybercrime investigation and digital forensics. From 2007 to 2013, he was with Maritime Patrol Directorate General, Coast Guard Administration, Taiwan, where he was an information technology section chief in the department of information and communication. Since 2013, he has been with Central Police University, Taiwan, where he is currently an associate professor in the Department of Information Management. His research interests include cybercrime investigation, digital forensics, digital evidence, information management, criminal profiling, and cyber criminology.