Exploring the Cybercrime Investigation Framework of ATM Heist from ISO/IEC 27043:2015

Da-Yu Kao

Department of Information Management, Central Police University, Taoyuan City 333, Taiwan, ROC
camel@mail.cpu.edu.tw

***Abstract*—Cybercriminals increasingly use sophisticated tools and advanced methods to attack bank systems. This study intends to highlight the cybercrime investigation of ATM heist in Taiwan. A cybercrime investigation framework of bank ATM heist from ISO/IEC 27043:2015 processes class is proposed to address the issue and to help investigators explore the truth. It describes a prototype framework that is current under development, and demonstrates how ISO/IEC 27043:2015 processes class can provide investigators with great abilities to interpret data generated by cyber forensics tools.**

***Keyword*—ISO/IEC 27043: 2015, Cybercrime Investigation, ATM Heist, Malware Family**

Dayu Kao is an Associate Professor at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. He is responsible for various recruitment efforts and training programs for Taiwan civil servants, police officers or ICT technicians. He has an extensive background in law enforcement and a strong interest in information security, ICT governance, technology-based investigation, cyber forensics, human resource development, and public sector globalization. He was a detective and forensic police officer at Taiwan's Criminal Investigation Bureau (under the National Police Administration). With a Master degree in Information Management and a PhD degree in Crime Prevention and Correction, he had led several investigations in cooperation with police agencies from other countries for the past 20 years. He can be reached at camel@mail.cpu.edu.tw.