Extracting Suspicious IP Addresses from WhatsApp Network Traffic in Cybercrime Investigations

Da-Yu KAO*, En-Cih CHANG*, Fu-Ching TSAI**

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

*** Department of Criminal Investigation, Central Police University, Taoyuan 333, Taiwan*

dayukao@gmail.com, dorislovesnoopy@gmail.com, fctsai@mail.cpu.edu.tw

***Abstract*—Sniffers are among the commonest approaches for capturing network traffic activities and collecting digital evidences in cybercrime investigations. The ubiquity of instant messaging (IM) apps on smartphones has provided criminals with communication channels that are difficult to decode. Moreover, investigators and analysts of cybercrimes are encountering increasingly large datasets. To combat criminal activity, law enforcement agencies (LEAs) often rely on call-record analysis. In this paper, cybercriminals are investigated by network forensics and sniffing techniques. Retrieving valuable information from specific IM apps is difficult because the criminal's IP address records are not easily recognisable on the Internet. Here, a criminal's identity is located more effectively by a packet filter framework that isolates the WhatsApp communication features from huge collections of network packets. A rule extraction method for sniffing packets is proposed that retrieves the relevant attributes from high-dimensional analysis based on geolocation and a pivot table. The utility of this methodology is illustrated on real-time network forensics and a lawful interception system in Taiwan. The methodology also meets the ISO/IEC 27043:2015 standards of fear, uncertainty, and doubt avoidance. Besides supporting LEAs in discovering criminal communication payloads, prosecuting cybercriminals and bringing them to justice, it improves the effectiveness of modern call-record analysis.**

***Keyword*—Cybercrime Investigation, Network Forensics, Packet Analysis, VoIP, WhatsApp, Lawful Interception, ISO/IEC 27043: 2015**

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.

En-Cih CHANG received the B.S. degree in information management from Central Police University, Taiwan, in 2018. In 2018, she is studying in the College of Communication and Information, Florida State University, Tallahassee, FL, USA. Her current research interests include information security, incident response, cybercrime investigation, digital forensics, information systems management, criminal profiling, cyber criminology, and machine learning.

Fu-Ching TSAI received the B.S. degree in Information Management from Central Police University, Taiwan, in 2001, the M.S. and Ph.D degrees in Institute of Information Management from National Cheng Kung University, Taiwan, in 2005 and in 2012, respectively. From 2001 to 2010, he was with Pingtung County Police Bureau, Taiwan, where he was a lieutenant involved in the development of policing information systems. From 2010 to 2014, he was with National Police Agency, Taiwan, where he was a division assistant in network & security incident investigation. From 2014 to 2017, he was with Changhua County Police Department, Taiwan, where he was an Information Management Division chief. Since 2017, he has been with Central Police University, Taiwan, where he is currently an assistant professor in the Department of Criminal Investigation. His research interests include data mining, text mining, digital forensics, social network analysis, and cyber criminology.