WhatsApp Network Forensics: Discovering the Communication Payloads behind Cybercriminals

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

Department of Information Management, Central Police University, Taiwan

*Corresponding Author: dayukao@gmail.com, Tel: +886 3 328 2321*5100*

***Abstract*—The ubiquity of instant messaging (IM) apps on smart phones have provided criminals to communicate with channels which are difficult to decode. Investigators and analysts are increasingly experiencing large data sets when conducting cybercrime investigations. Call record analysis is one of the critical criminal investigation strategies for law enforcement agencies (LEAs). The aim of this paper is to investigate cybercriminals through network forensics and sniffing techniques. The main difficulty of retrieving valuable information from specific IM apps is how to recognize the criminal' IP address records on the Internet. This paper proposes a packet filter framework to WhatsApp communication patterns from huge collections of network packets in order to locate criminal's identity more effectively. A rule extraction method in sniffing packets is proposed to retrieve relevant attributes from high dimensional analysis regarding to geolocation and pivot table. The results can support LEAs in discovering criminal communication payloads, as well as facilitating the effectiveness of modern call record analysis. It will be helpful for LEAs to prosecute cybercriminals and bring them to justice.**

***Keyword*——Cybercrime Investigation, Network Forensics, Packet Analysis, VoIP, WhatsApp, Lawful Interception**

Fu-Ching Tsai is a technical specialist in the Computer Center at Central Police University, Taiwan. He received his PhD degree in information management from National Cheng Kung University, Taiwan in 2013. His research interests include big data analysis, data mining, text mining, and artificial intelligence.

En-Cih Chang is a student at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan.

Da-Yu Kao is an Associate Professor at Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. 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.