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.**

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

I. INTRODUCTION

Call record analysis is one of the critical criminal investigation strategies for law enforcement agencies (LEAs). Call records provide important information, such as dates, times, and lengths of outgoing and incoming calls, which is highly relevant for examining crime scene [1]. However, the ubiquity of instant messaging (IM) apps on smart phones has provided criminals to communicate with channels which are difficult to track using traditional investigation technologies. Nowadays, most of the criminals use IM apps instead of voice phones to prevent been targeted by LEAs. Finding the identity of cybercriminal without foreign authority's help is difficult on the Internet, which provides complete anonymity and privacy and causes some challenges during investigation [2]. Developing new techniques to analyse modern call records is an urgent task.

The main difficulty of retrieving valuable information from specific IM apps is how to filter mass network connection records on the Internet. The captured raw data from the Internet is full of packets which produced by different apps from various devices. The protocols, ports, connection frequencies are all varied from different apps. Moreover, smartphones can even establish connections through its different networks interfaces. Although retrieving call records or network connection logs from smartphones is great challenge, its data is capable of providing more advanced and detailed information than traditional phone records. For example, the GIS or IP address reveals the locations of the calls and the captured network packets provide the multimedia content of the communications.

WhatsApp is a cross-platform application for instant communications on electronic devices, including smartphones, tablet computers and personal computers. There are more than 1.3 billion active WhatsApp users for July 2017. Its worldwide popularity is not only because the low cost subscription model, but also its new features which allow people to group chat and send text, pictures and other multimedia elements along with messages. Since WhatsApp was acquired by Facebook in 2014, the snowball effect brings even more users to communicate with this platform. Unfortunately, its characteristics of convenient and well-functioning also contributes the wild usage of criminals to communicate with each other in a more effective and secret way.

This research tries to recognize WhatsApp communication patterns from huge collections of network logs and packets in order to locate criminal activities more effectively. Discovering criminal communication contents from vague connections helps LEAs to filter criminal activities more effectively. The structure of this paper is organized as follows. Section 2 provides a review of network sniffing protocols and analysing tools. Section 3 describes the specifics of research framework. Section 4 demonstrates the experimental results. Finally, the last section concludes the paper and makes some suggestions for future work.

II. LITERATURE REVIEWS

Packet analyzers are wild applied in network security field to analyze raw traffic, detect attacks, sniffing and network roubleshooting [5].

Figure 1. The function of packet analyzers

Figure 1 demonstrates the functions of packet analyzer. Packet analyzers can be used for different kinds of roles in various applications. For the moral perspective, packet analyzer helps perform a security audit through packets; for network administrators, it becomes a tool to diagnose problems in a network. For white-hat hackers, the reports from packet analyser help to find vulnerabilities of software applications which are able to build an early warning before cyber-attackers lunch the serious attacks. For protocol developers, packet analyzers can be used to diagnose protocol-related issues. Packet analyzer can also be used in immoral way, for example, inspecting packet payload to decrypt passwords or sniffing the traffic to deploy man-in-the-middle attack.

Describing the process of capturing and interpreting live data as it flows across a network in order to better understand what is happening on that network, packet analysis is typically performed by a packet sniffer, which is a tool used to capture raw network data going across the wire or wireless interfaces. Packet analysis can help with understanding network characteristics, determining who or what is utilizing available bandwidth, finding unsecured and bloated applications, identifying summit network usage times, or figuring out malicious activities.

There are various types of packet-sniffing programs, including both free and commercial ones. Each program is designed with different goals in mind. A few popular packet-analysis programs are Tcpdump, OmniPeek, and Wireshark. Tcpdump is a command-line program, while OmniPeek and Wireshark have graphical user interfaces [9].

Wireshark is one of the most well-known open source packet analyzers. Wireshark provides both easy-to-use GUI and a command-line utility with very active community support [6]. In addition, it supports offline and online mode for flexible capturing operations. There are some of the important features listing in the figure 2.

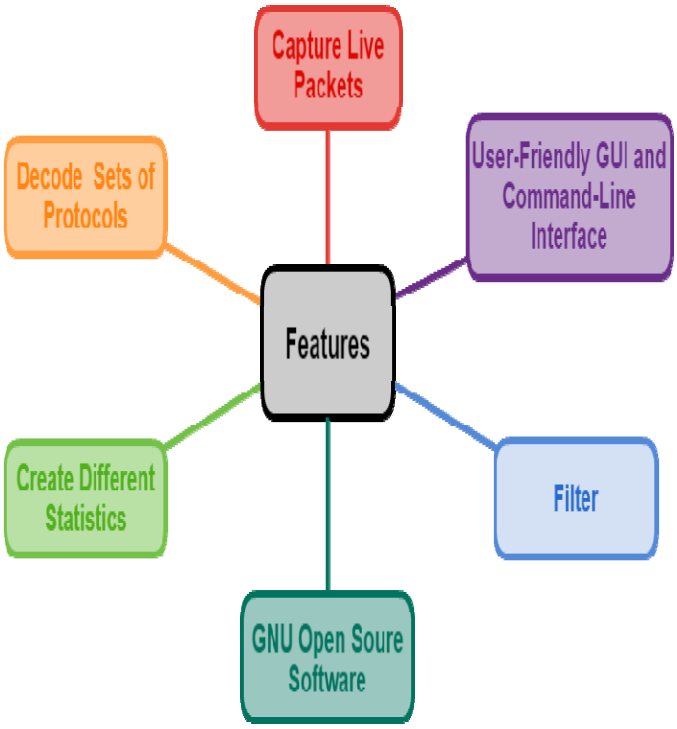


Figure 2. Wireshark features

VoIP, an abbreviation of Voice over Internet Protocol, sends voice over an IP-based network, which is totally different from the circuit-switched public telephone network [7]. Circuit switching allocates resources to each individual call; however, IP networks are packet switched, and each packet sent is semi-autonomous, which has its own IP header, forwarding separately by routers.

VoIP employs session control and signalling protocols to manage the signalling, set-up, and tear-down of calls. It works with several protocols called SIP (Session Initiation Protocol), H.323, SDP (Session Description Protocol), RTP (Real-time Transport Protocol), Inter-Asterisk eXchange (IAX) and so on.

A traditional system involves a lot of control signalling to accomplish the various tasks required, while VoIP takes all of these signalling messages and places them inside IP packets. It is also worth mentioning that since the Internet Protocol can and does run over almost every single type of low-layer communication architecture, VOIP can as well.

By the VoIP architecture, researchers can side-by-side compare the topologies and a short list of the basic skills required to work on VoIP and traditional telephony. The equipment used in each, while serving the same functions, performs these functions differently and in fact operates using a completely different set of protocols [3].

The most frequent feature of WhatsApp is voice calling. While users start a call using private IP address behind the firewall, STUN (Session Traversal of UDP through Network Address Translations) protocol should be used for assisting devices behind a NAT firewall or router with their packet routing. It allows an end computer to discover its public IP address, and to permit NAT traversal for applications of real-time voice, message, and other interactive communications. RFC 5389 redefines the term STUN as 'Session Traversal Utilities for NAT' [8][10].

III. RESEARCH FRAMEWORK

This paper simulates the scene of communications between victim and suspect and tries to retrieve the patterns as the rules to filter WhatsApp packet in order to help LEAs target suspects more effectively. Figure 3 shows the 3 steps of our research framework, i.e. data collection, data preparation and pattern recognition.

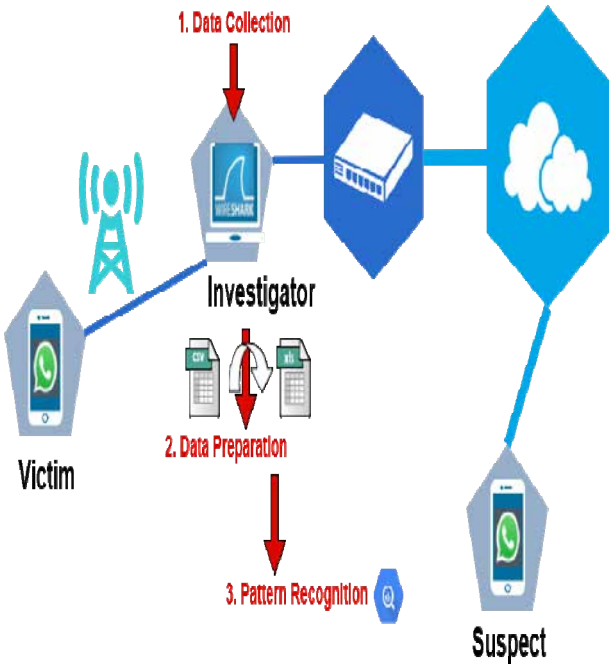


Figure 3. Research framework

A. Data Collection

In the data collection step, researchers use Wireshark to capture all network traffic from the route between victim and suspect. Setting a middle point for packet sniffing is one of the law enforcement strategies for investigating criminal behaviour. In the procedures of two users making voice calls through WhatsApp, researchers assume the node of Wireshark deployment is under lawful interception warrant procedures. Since WhatsApp doesn't support making voice calls from personal computers, we are not able to set up our experiment to start capturing packets using Wireshark which should only be installed in personal computers. We choose to make a personal computer as a hotspot for sharing network connections to the cell phone and as the node for capturing network packets utilized by Wireshark.

B. Data Preparation

In the data preparation step, the pcap data which is the captured packets file format is imported to Wireshark to demonstrate the information of header and payload. Since the operation of voice calls relates to STUN protocol, the protocol filtering function of Wireshark is applied to further analyse STUN packets. Figure 4 demonstrates the STUN packets list ordered by timestamp from imported pcap files.

Besides the STUN packets filtering, the geolocation of an IP address plays an important role to transform locations from network space to physical space. Originally started in Unix, Whois database has become the most common mechanism for locating the registration information for IP resources registered with Internet number resources organizations. By querying registries into one of the open-source Whois Lookup tools, it returns all sorts of geolocation information, including domain ownership, addresses, locations, and phone numbers.

For analysing high dimensional data, the pcap files are further exported to excel for applying Pivo table to view data from different angles.

C. Pattern Recognition

In the pattern recognition phase, researchers investigate the packet records to identify patterns which generated by WhatsApp in order to facilitate the efficiency to identify the suspect's IP address. As shown in Figure 5, there are 90 attributes in the flat file. After deeper analysis with applying Pivo table to view data from different angles, we have found some key attributes for construct patterns for LEAs, i.e. "Differentiated Services Field", "Flags", and "Differentiated Services Codepoint". Differentiated services is for providing low-latency to critical network traffic such as voice or streaming media while providing simple best-effort service to non-critical services such as web traffic or file transfers. The meaning of the field value contained within the flag is often defined in the section related to the data structure, and the bit field is usually associated with a property or privileges.

D. Evaluation Results

We conduct the experiment to evaluate the effectiveness of the proposed framework. We collect network packets in the period of 34.505698 seconds which contains the WhatsApp communication. Although the traffic is only captured from the local area network, the IP list is very complicated due to additional connections with its software companies and internet service providers. The results of the geolocations of IP address in this experiments, which transformed by whois lookup tools, are shown in Table 1.

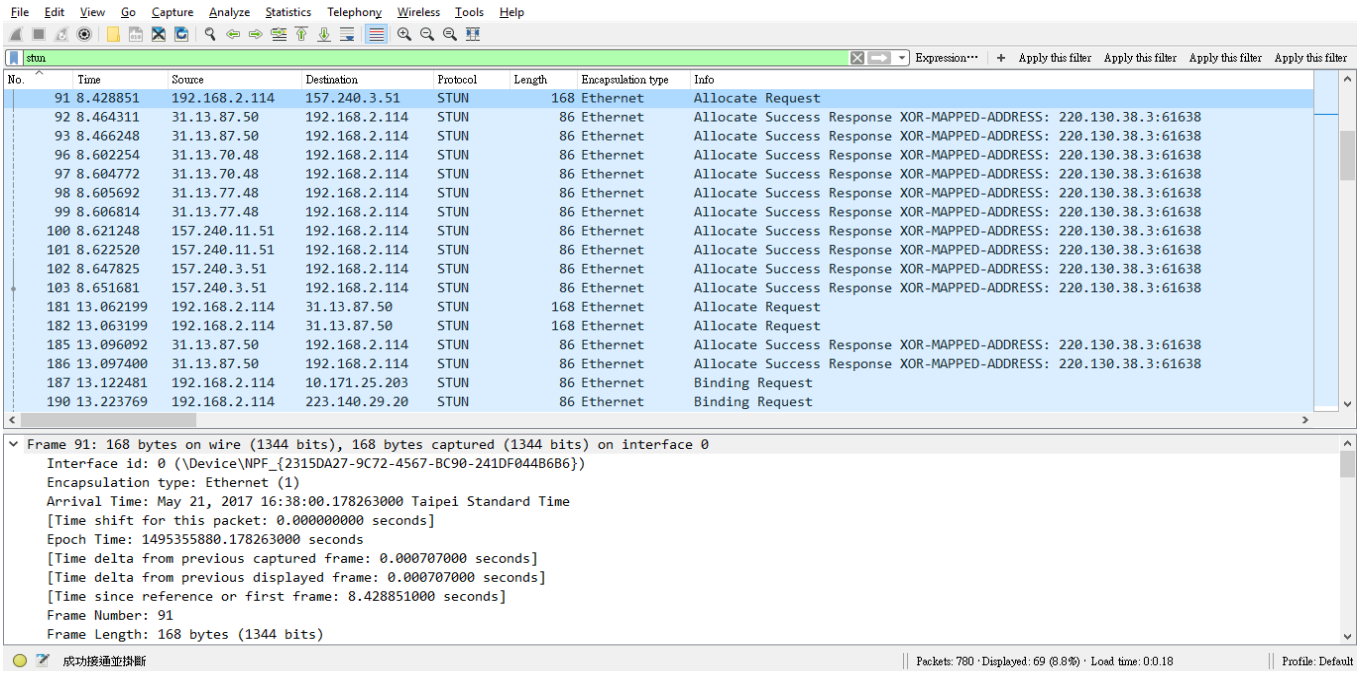


Figure 4. Packet of STUN Protocol

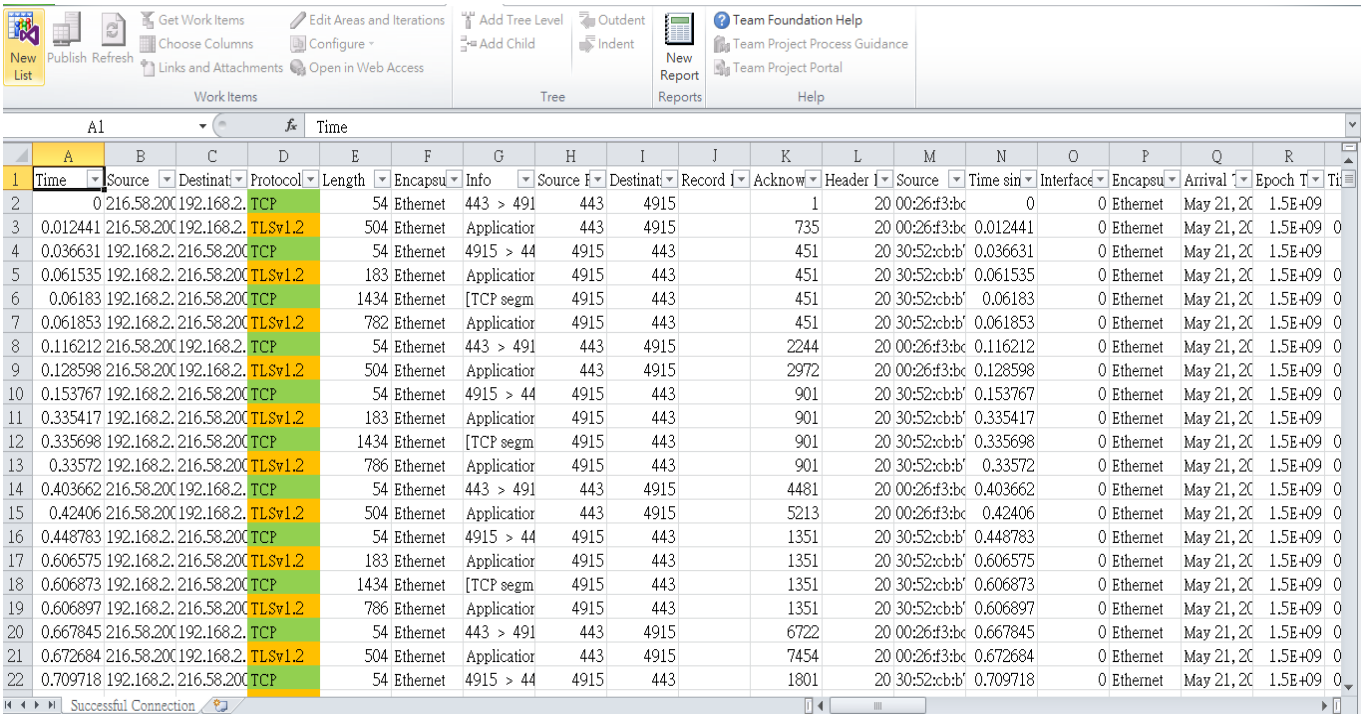


Figure 5. A flat file for pattern recognition

TABLE 1. THE GEOLOCATIONS OF IP ADDRESSES

IP Address	Whois Lookup
192.168.2.114	Victim
223.140.29.20	Suspect(EMOME-IP.hinet.net, Taiwan)
157.240.3.51	United States Menlo Park Facebook Inc.
31.13.87.50	Taiwan, Province Of China Taiwan, Province Of China Taipei Facebook Ireland Ltd
31.13.70.48	United States United States Los Angeles Facebook Ireland Ltd
157.240.11.51	United States United States Menlo Park Facebook Inc.

In order to investigate the patterns of WhatsApp communications, we further imported the headers and payloads of the captured packets into Pivo table. With the frequency distribution analysis, we discover that most of the packet fields consist of random values which are not applicable for identifying communication patterns. However, the values of several attributes, such as Differentiated Service Field, Flags, and Differentiated Services Codepoint, are fixed. The attributes with fixed values are selected as the criteria for pattern recognition of WhatsApp communications. The derived packet attribute and its content are shown in Table 2.

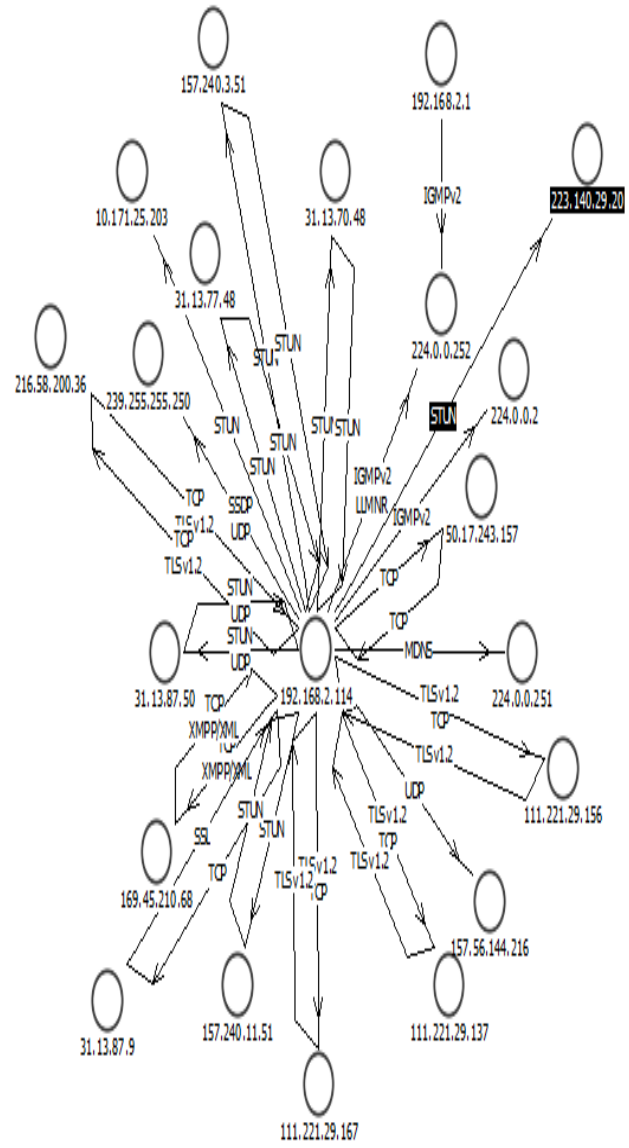
TABLE 2. THE CRITERIA OF THE CONTENT

Packet attribute	Content
Differentiated Services Field	0x38
Flags	0x00
Differentiated Services Codepoint	Assured Forwarding 13

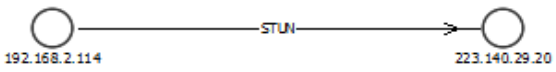
We further generate the rules by applying the derived criteria from packet analysis as shown in Table 3. The purpose of the rules is to target WhatsApp communications from the Internet more effectively. The noise connections which produced by software companies, manufactures of network devices or ISPs are supposed to be filtered when the rules are implemented. In order to demonstrate the effect, we apply the generated rules to the collected packets which containing WhatsApp communications. Figure 6 shows the network topology before and after implementing the rules. The results demonstrate that the proposed rules are successfully pruning the complicated topology and reveal the connections between victim and suspect. The above findings are helpful for LEAs to investigate cybercrime while the criminals are using WhatsApp to contact each other.

TABLE 3. THE RULES

Rule 1	IF Differentiated Service Field = 0x38 Flags = 0x00 Differentiated Services Codepoint =Assured Forwarding 13 THEN Source IP address = suspect
Rule 2	IF Protocol = STUN Length = 86 Info = Binding Request THEN Destination IP address = suspect



(a) Before the rule implementation



(b) After the rule implementation

Figure 6. The network topology of WhatsApp communication

IV. CONCLUSION AND FUTURE WORKS

Modern call record analysis is one of the future trends of criminal investigation strategies. Recognizing communication patterns between IM software on smart phones is essential to reveal the locations of suspects which is capable of providing clues for LEAs to facilitate the efficiency of investigative

work. In this study, we develop a rule extraction framework to reveal the WhatsApp communications and eliminate the impact from the disordered connections on the Internet. The results from the experiments show that the generated rule successively simplify the complexed network topology to a simple connection between suspect and victim. The criteria which discovered from the sniffed packets provide instructive information to identify the characteristics of WhatsApp communication. Furthermore, the proposed framework can be applied to explore patterns produced by other IM software. The evidence of connections between criminals will be helpful for LEAs to raise prosecution and conviction rate.

Due to rapid development of IM software, the future research should consider the software upgrade problem to eliminate impact from IM software updating. In addition, the impact of applying the proposed framework to encrypted communication should be examined in various perspectives. Since the proposed methodology is crucial for LEAs, and thus future studies should consider other IM software to provide more complete coverage of IM pattern recognition applications.

ACKNOWLEDGMENT

This research was partially supported by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-107) and the Ministry of Science and Technology of the Republic of China under the Grants MOST 106-2221-E-015-002-.

REFERENCES

[1] Casey, E., Digital Evidence and Computer Crime, Elsevier Inc., pp. 727-735, 2011.
[2] EC-Council, Computer Forensics: Investigating Network Intrusions and Cyber Crime, EC-Council I Press, pp.11-4, 2010.
[3] Hartpence, B., Packet Guide to Voice over IP: A System Administrator's Guide to VoIP Technologies, O'Reilly Media Inc., pp. 2-5, 2013.
[4] Kao, D. Y. and Wu, W. Y., "Practical Packet Analysis: Exploring the Cybercriminal behind the LINE Voice Calls," 2017 19th IEEE International Conference on Advanced Communications Technology (ICACT), Pyeong Chaung, South Korea, Feb. 19-22, 2017, 2011.
[5] Kizza, J. M., A Guide to Computer Network Security (3rd Edition), Springer-Verlag London Ltd., pp. 1-60, 2009.
[6] Nath, A., Packet Analysis with Wireshark, Packet Publishing, pp. 56-146, 2015.
[7] Rahbar, A. G., Quality of Service in Optical Packet Switched Networks, IEEE Press, pp. 19-43, 2015.
[8] Roy, R. R., Handbook on Session Initiation Protocol: Networked Multimedia Communications for IP Telephony, CRC Press, pp. 1-350, 2016.
[9] Sanders, C., Practical Packet Analysis_ Using Wireshark to Solve Real-World Network Problems, pp. 2, 2011.
[10] Walker, M., Certified Ethical Hacking Certification, McGraw-Hill Education, pp.54-59, 2014.

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.