WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. (2010)
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/wcm.954

The digital forensics of portable electronic communication devices based on a Skype IM session of a pocket PC for NGC

Hai-Cheng Chu[1], Der-Jiunn Deng[2] and Han-Chieh Chao[3*,†]

[1]*Department of Information Management/International Business, Tunghai University, Taiwan, R.O.C.*
[2]*Department of Computer Science and Information Engineering, National Changhua University of Education, Taiwan, R.O.C.*
[3]*Institute of Computer Science & Information Engineering and Department of Electronic Engineering, National ILan University, I-Lan, Taiwan, R.O.C.*

Summary

Portable electronic communication devices can be used for many purposes and they are capable of integrating with ubiquitous computing (UC) infrastructures to carry on mobile multimedia communications. As those devices become prevalent, they incur potential network security threatening to organizations. Nowadays, the Skype is the most popular P2P VoIP application program, which is being used by millions of global users to place IP phone calls, transfer files, or communicate *via* instant messaging (IM). This phenomenon already generates imminent network security issues that are indispensable to digital forensics researchers or the law enforcement agencies worldwide. Cellular phones, smart phones, and personal digital assistants (PDAs) are the representative ones of those devices and there are some open sources or commercial software toolkits that can be utilized to proceed the forensics investigation concerning the electronic crimes in next generation communications (NGCs). A case review was conducted to illustrate the hidden digital trails within the PDA from the *Registry* of the *Windows Mobile* and volatile data in the RAM to discover the possible network security leakage scenarios that resulted in the vandalism of intangible digital assets of the organization. Copyright © 2010 John Wiley & Sons, Ltd.

KEY WORDS: portable electronic communication device forensics; mobile computing; network forensics; Skype instant messaging; next generation communications

1. Introduction

Portable electronic communication devices are becoming affordable and they are capable of integrating with ubiquitous computing (UC) infrastructures [1] to carry on multimedia communications from leisure motivations to business professional purposes. Portable electronic communication devices encompass from PDA (personal digital assistant), cellular phones to handheld GPS (Global Positioning System) enabled devices [2].

Portable electronic communication devices can be used for many purposes ranging from sending and

*Correspondence to: Han-Chieh Chao, Department of Electrical Engineering, National Don Hwa University, Hualien, Taiwan, R.O.C.
†E-mail: hcc@niu.edu.tw

receiving e-mails, delivering presentations, storing documents, and surfing on the web sites. Simultaneously, they also incur potential network security threatening to organizations. Electronic crimes come with the popularity of handheld mobile communication devices utilizing the easily accessible wireless networks. Obviously, the Skype is a popular P2P VoIP (Voice over Internet Protocol) application program, which is being used by millions of global users to place IP phone calls, transfer files, establish video conferencing and communicate *via* IM (instant messaging), which most PDAs are capable of launching this the most dominant P2P software suite regarding VoIP, especially in next generation communications (NGCs).

PDAs store user data in a solid-state memory rather than hard disk and the running processes could hibernate in order to conserve battery power and avoid the time-consuming rebooting process in order to efficiently complete the tasks [3]. Alternatively, PDAs might temporarily store some user data in volatile memory, which will be lost once the power is off. However, even the data saved in nonvolatile memory will also be vanished if the PDA is hardware reset. Generally speaking, a PDA is designed to synchronize to a desktop PC and automatically settles and replicates data between them. Although a PDA can be regarded as a miniature of a desktop PC with incredible computing power, there are still some issues that distinguish those two [4]. Currently, the popular operating system (OS) being used by PDA is composed of *Windows Mobile*, *Palm OS*, or *Linux-based* platforms [5].

From hardware design point of view, PDAs are equipped with a microprocessor, ROM (Read Only Memory), RAM (Random Access Memory), a touch-sensitive LCD, and a slot for the removable memory card as an additional storage space. The RAM is aimed to sustain running processes data, whereas the ROM keeps core OS codes and libraries, the *Registry*, databases, and user files. Several varieties of ROM are utilized including Flash ROM, which is the nonvolatile memory that could be re-written or re-programmed electronically when OS is updated [3,6]. From digital forensics (DF) point of view, the removable memory card can be regarded as a disk drive, which can be imaged and analyzed with conventional forensic toolkits.

Demonstrably, PDAs are mobility oriented and the duration of operation depends entirely on battery power that becomes the natural limitation of PDAs. Nowadays, a PDA emphasizes on wireless connectivity *via* hot spots of Bluetooth, IrDA (Infrared Data Association), or Wi-Fi (Wireless Fidelity). The data stored in the RAM is volatile in its nature. As multimedia files become prevalent, portable electronic communication devices need memory cards to permanently and securely store huge amount of user data in the NGC environment. Currently, memory cards have varieties in the market including compact flash (CF) card, multi-media card (MMC), SD (secure digital) card, miniSD card, and memory stick. Each one of them has its distinct hardware specifications for different purposes.

Embedded with similar functionalities to those of desktop computers, the portable electronic communication devices provide state-of-the-art NGC power with compact size and integrated modern features. The Federal Bureau of Investigation (FBI) of U.S.A. has highlighted the issue of growing crimes involving portable electronic communication devices in their computer crime surveys [7]. Today, people are using those portable devices to access the e-mail, proceed IM, access the web sites, download business data or even to place a VoIP call by ubiquitous networks while they are transporting. Indeed, the portable electronic communication devices become a wealthy information depository where sensitive or decisive information could be discovered if necessary. In some cases, those digital evidences could be extremely crucial and admissible to a court of law for a certain digital investigation of an electronic crime. Undoubtedly, the DF specialists have to apply forensically sound software suites to collect, extract, and analyze the digital trails that were left behind [8] inside the portable electronic communication devices when they deal with the fledging electronic crimes. Accordingly, the portable electronic communication devices pose great challenges for digital investigators and law enforcement agencies worldwide.

As technologies keep progressing, for those PDAs that have built-in cellular communications capability are generally considered to be smart phones. Basically, smart phones are mobile phones with additional advanced functionaries equipped that are similar to those of desktop PCs. Hence, the performance of a smart phone symbolizes a miniature desktop PC based on the embedded application programs. As communication technology advances and becomes much more ubiquitous, the smart phone is the representative of modern handheld mobile communication devices with heterogeneity of the hardware design as well as the corresponding OS being installed. The OS of a smart phone also has varieties based on the hardware manufacturers. Current popular

DOI: 10.1002/wcm

OS for a smart phone could be *Symbian OS*, *iPhone OS*, *BlackBerry*, *Windows Mobile*, *Linux*, *RIM*, or *Palm WebOS*. Under such circumstances, Mobile Equipment (ME) acquisition becomes a challenging task in terms of DF. MEs are referred to as the combinations of cellular phones with PDA functionalities. These smart phones also support the varied types of memory to store the data, which can be acquired by the DF specialists. Those types of memory encompass the SIM (subscriber identify module) card, the memory card (CF, MMC, SD, or miniSD, etc.), and the internal memory. The amount and type of data stored on a SIM card varies by manufacturers and the cellular phone carriers.

As the network forensics and DF in NGC become much more emphasized in order to mitigate the imminent threatening from insidious high-tech cyber crimes syndicate, there are some differences between the computer forensics and portable electronic communication devices forensics, which have varieties in their embedded OS as we stated above. Moreover, they emerge with new models from time-to-time and wider range of hardware and accessories than desktop PCs. In addition, user files are often stored in volatile memory, unlike those are saved in the hard disk of a desktop PC. Especially for PDAs, once they have been powered on, the devices will be always in an active mode with some processes may be running in the background or even hibernate after a certain period of time, which is quite distinguished from desktop PCs. Unlike desktop PCs, the portable electronic communication devices do not have hard drives, which could be isolated during the digital investigation.

In this paper, we are focusing on the application of a PDA with IM service executing to commit cyber crimes from DF point of view. Without loss of generality, we utilized a popular PDA, *HP iPAQ*, and the embedded *Windows Mobile* OS running *Skype for Pocket PC* as an example, which is becoming more dominant in NGC of electronic crimes. A case review was conducted to illustrate the DF staff trying to disclose the hidden digital trails within the PDA from the *Registry* of the *Windows Mobile* [9] and volatile data in the RAM. The research methodologies provided in this paper could be migrated to other PDA models. Additionally, we also reconstructed the crime scene based on the digital evidences that were collected, analyzed, and preserved to discover the possible network security leakage scenarios that resulted in the vandalism of intangible digital assets of the organization.

2. Related Researches of Portable Electronic Communication Devices Forensics

According to the United States juridical systems, the authentication of electronically stored information (ESI) becomes critical when pursuing the truth in resolving civil disagreements concerning small scale digital devices such as cellular phones or PDAs [10] and this highlights the importance of DF for portable electronic communication devices. Some researchers classify portable electronic communication devices into three categories: cellular phones, PDAs, and smart phones, which are recognized as the hybrid between cellular phones and PDAs [11]. Most mobile phones are similar to PDAs except that they have the radio interface to cellular telecommunications networks and their screens are not touch-sensitive. We illustrated the above concepts as Figure 1 depicted.

Compared to desktop PCs, the forensics tools for portable electronic communication devices are fewer due to the varieties of manufacturers in this field. The essential role of the DF with respect to portable electronic communication devices is the acquisition of data from those devices. Generally speaking, the DF expert will focus on data that was stored at removable memory card, internal memory, and the SIM card if the portable electronic communication device is a smart phone. The acquisition of the memory card can be seized by a MMC or SD card reader combining with a bit-stream imaging toolkit. The acquisition of the SIM

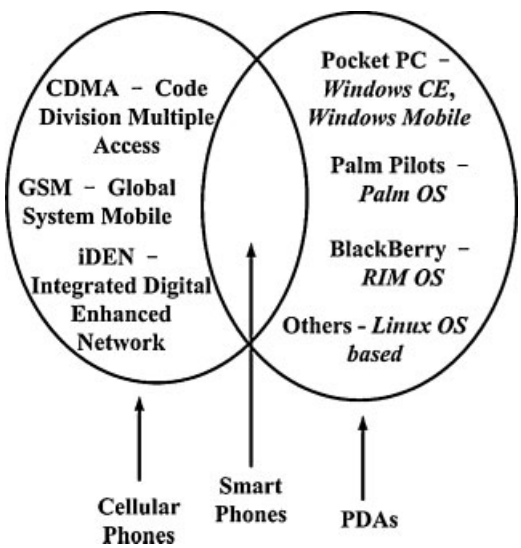

Fig. 1. Three categories of portable electronic communication devices forensics arena.

DOI: 10.1002/wcm