Chapter 4
Forensics Challenges for Mobile Phone Security

Halim M. Khelalfa
University of Wollongong in Dubai, UAE

ABSTRACT

This chapter provides a complete reference on mobile phone forensics to students, researchers, lawyers, forensics examiners, information security officers, as well as organizational security personnel.

First, the author reviews the currently used guidelines and procedures in digital forensic investigations, and then presents their current adaptations to mobile phone forensics, including criteria for the selection of forensics tool for mobile phone. Due to the world popularity of GSM phones, a detailed description of the SIM file system is presented. The forensic strength and weaknesses of the classes of physical and logical forensic tools are discussed .Current approaches to overcome the impediments of both classes are reviewed in terms of usability and forensic soundness. Then, the newest challenge to the digital forensic community, anti-forensics (AF) is raised, including the risks faced by mobile phone forensics investigation. Finally, the author addresses the issue of current research as well as trends on mobile phone forensics.

INTRODUCTION

This information age is witnessing a revolution within the information revolution: the mobile information age. According to GSM association, (GSM-1, 2011) the total number of phone connections has reached well over 4.94 billion connections in March 2011. The three billion mark was reached just a year ago on April 16, 2009. One needs to consider that this landmark has been reached, only 17 years after the first GSM network was launched in 1991. Four years later, GSM users reached one billion in 2004; two years later, GSM users passed the two billion mark in the first quarter of 2006, and one year and half

DOI: 10.4018/978-1-61350-507-6.ch004

later, GSM users reached 3.5 billion in January 2009. According to the same source, the world counts more than seven hundred mobile operators in more than two hundred and eighteen countries and territories. We witness on average fifteen new connections per second or one million three hundred thousand new connections daily. The mobile phone market is no longer restricted to the seven most industrialized countries. It spans the entire world. Today, the GSM has about 85% of the global mobile services market. Each year, more than one billion new mobile handsets are sold. They make more than 7 trillion minutes of calls and send about 2.5 trillion text messages (Mullins, 2007).

The current advances of mobile broadband services with higher speed and larger bandwidth will offer more Internet based services with richer multimedia to an ever wider fringe of the world population. GSM is just one of the cell network technologies used for mobile telephony. The ever increasing growth and popularity of using mobile phones has led to having mobile phones being involved in criminal incidents. Law enforcement officials, information security officers, lawyers, and researchers are faced with a series of new challenges: mobile phone forensics (Zhihong, 2008).

This challenge is particularly crucial for the newly emerging offspring of e-commerce, the mobile commerce where transactions are made using mobile devices such as PDA and cell phones (Dai-Yon Cho, 2007). Several facts back up the importance of digital forensics in mobile commerce. First, it is predicted that by the end of 2013, revenues from mobile services will reach well over one trillion of US dollars; an ideal target for cybercriminals. Second, mobile commerce involves three main actors: *the mobile customer, the mobile vendor, and the cellular network provider* (Tindale, 2005). A major factor in the adoption by consumers of mobile commerce is trust in the other two actors; that is trust in mobile technology and in mobile vendors.

The purpose of this chapter is to provide a wide spectrum of end users with a complete reference on mobile phone forensics. End users include students, researchers, incident response team members from private and governmental institutions, lawyers, forensics examiners, information security officers, as well as organizational security personnel.

A particular effort aims at enhancing organization capabilities for elaborating appropriate security policies for mobile phones, and providing forensic specialists and incident response team members with recommendations and guidance on how to address security incidents involving digital information residing on mobile phones and other related medias.

Several challenges face the investigator of mobile phone forensics. The forensic professional should keep up with:

- an ever evolving technology and changes,
- a widespread use of mobile phones,
- a wide variety of mobile phones,
- an increased sophistication of criminals who use the technology gap to enhance their stealth.

First, there exist different types of cellular networks with different characteristics. They include: GSM, 3GSM, CDMA, CDMA 1x, CDMA 1X EV-D0, TDMA, PDC, iDEN, and analogy.

Second, mobile phones can be divided into three main types: basic, intermediate, and smart. Each type has specific hardware and software characteristics. Some of the hardware characteristics include processor speed, memory capacity, display features, card slots, interfaces, battery type, battery location, interfaces, text input, camera options, and wireless capabilities. Some of the software characteristics include: operating systems and application software. Both types of software can be proprietary, open source or commercial like windows mobile.