A Simple Cost-Effective Framework for iPhone Forensic Analysis

Mohammad Iftekhar Husain[1], Ibrahim Baggili[2], and Ramalingam Sridhar[1]

[1] Department of Computer Science and Engineering, University at Buffalo,
The State University of New York, Buffalo, NY 14260
[2] College of Information Technology, Zayed University, UAE
{imhusain,rsridhar}@buffalo.edu, ibrahim.baggili@zayed.ac.ae

Abstract. Apple iPhone has made significant impact on the society both as a handheld computing device and as a cellular phone. Due to the unique hardware system as well as storage structure, iPhone has already attracted the forensic community in digital investigation of the device. Currently available commercial products and methodologies for iPhone forensics are somewhat expensive, complex and often require additional hardware for analysis. Some products are not robust and often fail to extract optimal evidence without modifying the iPhone firmware which makes the analysis questionable in legal platforms. In this paper, we present a simple and inexpensive framework (iFF) for iPhone forensic analysis. Through experimental results using real device, we have shown the effectiveness of this framework in extracting digital evidence from an iPhone.

Keywords: iPhone, Forensics, Smartphone, Jailbreaking, iTunes.

1 Introduction

The Apple iPhone is among the most popular smart phones on the market, since its release in July 2007. According to a recent report on market share of mobile devices by Gartner [1], Apple's share of worldwide smart phone sales grew from 5.3 percent in the first quarter of 2008 to 10.8 percent in the first quarter of 2009. In terms of unit sales, iPhone jumped from 1.7 million in the first quarter of 2008 to 3.9 million during the same period in 2009. Though many smart phones have functionalities similar to iPhone, user interface and prevalence of numerous applications make them popular among many. The iPhone 3rd Generation Cellular Communication device, widely known as iPhone 3G was released in July, 2008 which has featured GPS service and faster Internet connection. Considering the mobility and functional similarity to standard computing devices, experts predict that iPhone can soon become a handy choice for cyber criminals. So, it is important for forensic community to focus on developing sound forensic methods for iPhone, forecasting the potential use of it in cyber crimes.

There are efforts from both commercial and individual forensic experts on iPhone forensics. Commercial products include Aceso by Radio Tactics [2], UFED from Cellebrite [3], Device Seizure by Paraben [4], .XRY by Micro Systemation [5] and

I. Baggili (Ed.): ICDF2C 2010, LNICST 53, pp. 27–37, 2011.

CellDEK by LogiCube [6]. However, these products can be expensive (up to multiple thousand dollars), requires additional hardware and functionality is limited only to the built-in features provided. Also, some approaches alter the firmware of iPhone to access the storage area using a method widely known as "jailbreaking" which is copyright infringement and illegal [7]. It also violates the Association of Chief Police Officers (ACPO) guideline for computer forensics and electronic evidence [8], which clearly states that "No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may be subsequently be relied upon in court."

In this paper, we propose a forensic framework for iPhone which simple to perform and free from the requirement of additional devices. In addition, this approach does not alter the iPhone firmware which keeps the digital evidence acceptable in legal venues. Using an iPhone device, we show the effectiveness of the framework in retrieving various digital artifacts. Additionally, we show the soundness of the evidence through comparisons to existing approaches using forensic standards. A preliminary version of this framework was tested on iPhone instant messaging forensics in [9].

2 Literature Review

The Apple iPhone OS is an optimized version of Mac OS X. There are two partitions on the iPhone storage device. The first partition is the system partition (approx. 300 MB). This partition includes the operating system and the default applications. The remaining space is partitioned as the user data (or media) partition. This space is where all music, contact, SMS as well as other user data are stored. When an iPhone is connected to a computer, it communicates with it using Apple File Communication protocol and creates a backup folder of user and device configuration data on it. Forensic acquisition of iPhone data can take different approaches such as acquiring the backup folder to analyze available data or obtain a physical image of the storage device.

Commercially available iPhone forensic products such as Aceso, UFED, Device Seizure, .XRY and CellDEK have some common drawbacks. Some products require additional hardware to perform the forensic analysis such as Aceso, UFED and CellDEK . Prices of most products vary from one to fifteen thousand USD according to our survey [10]. In addition, none of these solutions guarantees a complete recovery of device data.

Individual effort such as Zdziarski [11] approaches this problem through a bit-by-bit copy of the physical data in the iPhone. However, this approach modifies a read-only system partition which may eventually make the evidence questionable at legal venues. Forensic experts [12] extensively reviewed this approach and commented "I feel certain that without 15+ years of highly technical experience, I would have likely failed or would have certainly taken much longer to succeed (and perhaps sacrifice the iPhone data a few times along the way)." Efforts that use "jailbreaking" modify the user data partition of the iPhone opening it for legal challenges according to ACPO guideline.