BlackBerry PlayBook Backup Forensic Analysis

Mohamed Al Marzougy[1], Ibrahim Baggili[2], and Andrew Marrington[1]

[1] Advanced Cyber Forensics Research Laboratory, College of Technological Innovation, Zayed University, Abu Dhabi, U.A.E.
Mohamed.Almarzougy@gmail.com, Andrew.Marrington@zu.ac.ae
[2] Tagliatela College of Engineering, Department of Electrical and Computer Engineering and Computer Science, University of New Haven, CT
Ibaggili@newhaven.edu

Abstract. Due to the numerous complicating factors in the field of small scale digital device forensics, physical acquisition of the storage of such devices is often not possible (at least not without destroying the device). As an alternative, forensic examiners often gather digital evidence from small scale digital devices through logical acquisition. This paper focuses on analyzing the backup file generated for the BlackBerry PlayBook device, using the BlackBerry Desktop Management software to perform the logical acquisition. Our work involved analyzing the generated ".bbb" file looking for traces and artifacts of user activity on the device. Our results identified key files that can assist in creating a profile of the device's usage. Information about BlackBerry smart phone devices connected to the tablet was also recovered.

Keywords: BlackBerry, Forensics, PlayBook, Backup.

1 Introduction

The BlackBerry PlayBook is Research in Motion's (RIM) entrant into the heated tablet race which includes the iPad and various Android tablets. One of the main differences between the PlayBook device and other tablets is the ability to tether (via Bluetooth) to a BlackBerry smart phone for network access while away from WiFi networks at home or in the office, as compared to using an on-board 3G modem for that purpose. This tethering is provided by the BlackBerry Bridge feature that extends the functionality of the paired BlackBerry smart phone to the PlayBook's larger screen, enabling the viewing of emails, messages and files stored on the phone.

Although the iPad and the various Android tablets run a tablet-version of an operating system designed for a smart phone, the BlackBerry PlayBook runs a custom operating system. This means that research into the forensic acquisition of BlackBerry smart phones may not be applicable to the PlayBook device. To date, there has been no research performed on the forensic acquisition and analysis of the PlayBook's backup structure. Although the PlayBook has a comparatively small market-share [1], the PlayBook was the first tablet to gain FIPS 140-2 certification and cleared to be used by the U.S. Government [2]. Therefore, it is a worthwhile exercise to study the forensic acquisition, analysis and examination of the device via its backup structure.

M. Rogers and K.C. Seigfried-Spellar (Eds.): ICDF2C 2012, LNICST 114, pp. 239–252, 2013.

This approach has recently been applied successfully to the iPad [3] and we therefore thought to investigate its applicability to the BlackBerry PlayBook.

The remainder of this paper is organized as follows: in section 2 we briefly discuss the literature about the forensic examination of various types of tablet computers. In section 3, we describe the methodology for our experiment and we discuss our findings in section 4. In section 5 we draw conclusions from our work and we finish by discussing future research work into this area of small scale digital device forensics.

2 Background

Mobile phones and tablets are of particular interest to forensic investigations for the simple reason that due to their mobility they are likely to be in regular contact with suspects and/or victims throughout the course of the events under investigation. With enormous diversity in operating system software, hardware specifications, and vendors, small-scale digital devices like smart phones and tablets are an area of serious concern in digital forensic research [4].

Small-scale digital device forensics is a rapidly evolving subfield of digital forensics. The initial popularity of the iPhone and subsequently the iPad led to research into the retrieval and analysis of digital evidence from these devices [5][6][7]. There has been some research into Android devices [8], although it has been almost exclusively focused on phones and much remains to be done before a generalized methodology for Android forensics is possible [9]. There has also been some research on BlackBerry smart phone devices [10], but at the time of writing there is little published research about the BlackBerry PlayBook tablet, which is the focus of this paper.

2.1 iPhone and iPad

The iPhone, iPod Touch, and iPad all run the iOS operating system, and may be conceived of as broadly similar devices from a forensics perspective. All iOS devices interface with a personal computer or accessory peripherals through a proprietary port on the bottom of the device which connects to the computer's Universal Serial Bus (USB) port via a special cable. None of the iOS devices feature removable storage and consequently, any digital forensic examination of the device must take place via this cable.

Physical acquisition for iOS devices is limited to commercial products and law enforcement personnel. Andrew Hoog and Katie Strzempka [11] reviewed most tools that support iOS device forensics using the criteria: installation, acquisition, reporting and accuracy, where they came up with a ranking system they used to rank 13 digital forensics products and methodologies. The Zdziarski method scored the highest (4.1) where the rest averaged 3.3. Zdziarski's iPhone forensics method is one of the few which does not require the target device to be jailbroken - all an examiner has to do is put the device into recovery mode and load Zdziarski's tool into the device's RAM. The technique is conceptually similar to using a boot CD – essentially the device boots to an "alternate" system partition that has all the necessary software to run a