Computers and Mathematics with Applications 63 (2012) 544–553

Contents lists available at SciVerse ScienceDirect

Computers and Mathematics with Applications

journal homepage: www.elsevier.com/locate/camwa

Versatile iPad forensic acquisition using the Apple Camera Connection Kit

Luis Gómez-Miralles, Joan Arnedo-Moreno *

Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya, Carrer Roc Boronat 117, 08018 Barcelona, Spain

ARTICLE INFO

Keywords:
Forensics
IPad
Cybercrime
Digital investigation
Apple

ABSTRACT

The Apple iPad is a popular tablet device presented by Apple in early 2010. The idiosyncracies of this new portable device and the kind of data it may store open new opportunities in the field of computer forensics. Given that its design, both internal and external, is very similar to the iPhone, the current easiest way to obtain a forensic image is to install an SSH server and some tools, dump its internal storage and transfer it to a remote host via wireless networking. This approach may require up to 20 hours. In this paper, we present a novel approach that takes advantage of an undocumented feature so that it is possible to use a cheap iPad accessory, the Camera Connection Kit, to image the disk to an external hard drive attached via USB connection, greatly reducing the required time.

1. Introduction

Portable devices have become a very important technology in society, allowing access to computing resources or services in an ubiquitous manner. In this regard, mobile phones have become the clear spearhead, undergoing a great transformation in recent years, slowly becoming small computers that can be conveniently carried in our pockets and managed with one hand. However, as user requirements started to include new functionalities beyond those that a mobile phone can realistically offer, advanced portable devices have been developed in order to fulfill them. Such devices try to reach a compromise between a high degree of portability, usability and the ability to provide such advanced functionalities (for example, being able to read or process documents).

One of the top devices in the field of embedded portable devices is the Apple iPad, a tablet computer which tries to take advantage of the success of its ancestor, the iPhone. It was announced by Apple in January 2010 and launched in the USA and Europe between April and May 2010. After 80 days in the market, 3 million units had been sold [1]. Given its popularity, it becomes evident that as such devices become widespread, they will also become more common and relevant as sources of evidence from a computer forensic standpoint, providing data about their users. This kind of data can become very important in cases of criminal investigation, where it can be used as evidence in court or provide valuable clues to investigators. Since advanced portable devices are usually closed embedded systems with their own idiosyncracies, not actually being full-fledged PCs, forensic data acquisition presents some interesting challenges. This is especially relevant when it is necessary to use non-invasive methods, maintaining the device in the same state (or as similar as possible) as the one it was in before the analysis began.

Currently, the easiest method to obtain a forensic image of an iPad device (which can also basically be applied to an iPhone) is to install an SSH server and some tools, retrieve its internal storage contents and transfer the data to a remote host via wireless networking. Unfortunately, this is very slow, and can take up to 20 h. More efficient methods exist, but they

* Corresponding author.
E-mail addresses: pope@uoc.edu (L. Gómez-Miralles), jarnedo@uoc.edu (J. Arnedo-Moreno).

0898-1221/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2011.09.053

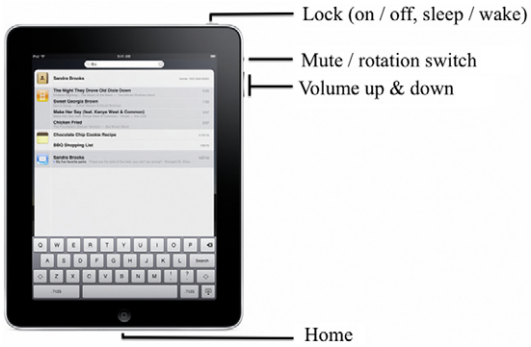

Fig. 1. iPad button configuration (iOS 4 and higher).

are based on closed software, which relies on obscure or undisclosed techniques and is very dependent on the iOS version. As soon as an iOS upgrade becomes available, they can no longer be used until a new version is created.

In this paper, we propose a versatile approach which reaches a compromise between forensic data acquistion speed and an open approach, without the need of vendor specific software or a dependency on a very specific iOS version. Achieved with the help of a cheap and easily available peripheral, the Camera Connection Kit, it is possible to generate a forensic image using an USB connection. Furthermore, this approach still minimizes the amount of data which is modified during the acquisition process.

The paper is structured as follows. Section 2 provides an overview of the iPad architecture, focusing on those characteristics especially relevant from a forensic analysis standpoint. In Section 3, a literature review of the current state of iPhone/iPad forensic imaging techniques is presented. The proposed forensic data acquisition method is described in Section 4. Section 5 provides a brief discussion about which forensic techniques can be applied on the image generated using our method, and, in Section 6, an analysis of its performance is presented. Concluding the paper, Section 7 summarizes the paper's contributions and outlines further work.

2. iPad architecture overview

From the external point of view, the iPad is basically a big (24 × 19 cm.) iPhone with a 9.7″ screen, providing a resolution of 1024 × 768. While its internals are very similar to those of its ancestor, the iPad's larger form factor makes it suitable for longer periods of use, which has motivated the appearance of many different applications of all kinds. Therefore, the iPad is able to perform tasks previously reserved for common computers or, up to some point, netbooks.

2.1. Main features

The basic iPad internals are:

- Processor: A custom Apple *A*4 ARM processor based on a single-core Cortex-A8, running at 1 GHz.
- Volatile storage: 256 MB DRAM.
- Non-volatile storage: 16, 32 or 64 GB solid state storage drive.
- Wireless connectivity: 802.11 a/b/g/n and Bluetooth 2.1, the same as every iPhone.
- In addition, the 3G model features an A-GPS (Assisted GPS), and hardware for communicating over UMTS/HSDPA (820, 1900 and 2100 MHz) and GSM/EDGE (850, 900, 1800 and 1900 MHz).

A second generation hit the market in March 2011, featuring a dual-core Apple *A*5 processor and 512 MB of RAM.

2.2. Connectors and buttons

The iPad connectors and buttons are very similar to the iPhone's. When placed over the short edge with the round button in the center, we find:

- Top left: a 3.5″ jack capable of functioning simultaneously for several audio functionalities.
- Top right: "Lock" button.
- Right edge, near the top: volume controls, and one configurable switch which can either mute the device, or lock the screen orientation.
- Bottom center, front face: round "Home" button.
- Bottom center, in the edge (below the "Home" button): Apple standard 30-pin "Dock" connector, the same as used in every iPhone and most iPods. This is also the port used when referring to the iPhone or iPad's 'serial port'.

Fig. 1 shows the function of each button. Note that the "Lock" button performs several functions: when the device is off, it will turn it on; when the device is on, a short press will put the device to sleep or wake it from sleep and a long