2012

IPad2 Logical Acquisition: Automated or Manual Examination?

Somaya Ali
Zayed University

Sumaya AlHosani
Zayed University

Farah AlZarooni
Zayed University

Ibrahim Baggili
University of New Haven, ibaggili@newhaven.edu

Comments

Dr. Baggili was appointed to the University of New Haven's Elder Family Endowed Chair in 2015.

iPAD2 LOGICAL ACQUISITION: AUTOMATED OR MANUAL EXAMINATION?

Somaya Ali
somayz@gmail.com
P.O. Box 144426
Abu Dhabi
U.A.E

Sumaya AlHosani
ms.sumaya@gmail.com
P.O. Box 144426
Abu Dhabi
U.A.E

Farah AlZarooni
f.alzarooni@gmail.com
P.O. Box 144426
Abu Dhabi
U.A.E

Ibrahim Baggili
ibrahim.baggili@zu.ac.ae
P.O. Box 144534
Abu Dhabi
U.A.E

Advanced Cyber Forensics Research Laboratory
Zayed University

ABSTRACT

Due to their usage increase worldwide, iPads are on the path of becoming key sources of digital evidence in criminal investigations. This research investigated the logical backup acquisition and examination of the iPad2 device using the Apple iTunes backup utility while manually examining the backup data (manual examination) and automatically parsing the backup data (Lantern software - automated examination). The results indicate that a manual examination of the logical backup structure from iTunes reveals more digital evidence, especially if installed application data is required for an investigation. However, the researchers note that if a quick triage is needed of an iOS device, then automated tools provide a faster method for obtaining digital evidence from an iOS device. The results also illustrate that the file names in the backup folders have changed between iOS 3 and iOS 4. Lastly, the authors note the need for an extensible software framework for future automated logical iPad examination tools.

Keywords: iPad, forensics, logical backup, iOS, manual examination.

1. INTRODUCTION

The popularity of the iPad continues to rise. Consumers are attracted to its unique features, such as increased storage capacity, user-friendliness, and the incorporation of an interactive touch screen. It is considered to be more personal than a laptop and more advanced than a mobile phone (Miles, January 27, 2010). The rapid distribution of tablets to businesses and individual utilization is primarily due to the Apple iPad device (Pilley, October 8, 2010). When Apple first released the iPad, they targeted consumer sectors rather than business sectors. Their advertisements and marketing campaigns reflected this strategy. However, the iPad is currently being adopted by an extensive scope of consumers, ranging from children to executives. It is also employed in unconventional settings, like in the hands of restaurant waiters as they take your order, or in boutique windows showcasing promotional material (Geyer & Felske, 2011).

Since 2010, more than 25 million iPads have been sold in the US (KrollOntrack, 2011). Furthermore, 70% of the iPad2 buyers were new to the iPad world and 47% purchased a 3G model. This demonstrates that not only are more buyers attracted to the iPad, but that consumers are looking for always-connected iPad devices (Elmer-DeWitt, March 13, 2011). Due to the ubiquity of these devices, criminals are starting to target iPad users, thereby committing a wider range of crimes (Pilley, October 8, 2010). Hence, digital forensic scientists need to focus on investigating these emerging devices. Fortunately, new digital forensic tools and methods are being developed by researchers and private corporations to help law enforcement officers forensically examine iPads, despite the challenging fact that the iPad technology is continuously changing (Pilley, October 8, 2010).

2. RESEARCH QUESTIONS

This research focused on logical forensic methods for examining iPad devices. This research intended

on answering the following questions:

- What is the difference between using automated logical analysis of the backup files versus using a manual approach?
- What data is saved in the backup folder of an iPad2?
- Where is the data saved and how can it be extracted?
- What is the difference between the backup structure of the old iOS and the new iOS?

3. BACKGROUND

3.1. iPad

On January 27, 2010, the late CEO of Apple, Steve Jobs, announced the launch of a new tablet device called iPad. On March 2, 2011, the second generation iPad2 was launched. Users could enjoy features such as browsing the Internet, watching videos, viewing photos, and listening to music (Apple, 2011a).

With two cameras, high definition (HD) video recording capabilities, a dual core A5 chip, extended battery life, WiFi Internet connectivity, third generation (3G) mini SIM card, an endless variety of applications, and a thin and light design, the iPad2 stormed the technology market and created a new era in the tablet world (Apple, 2011b). The iPad2 was released with the new version of Apple's operating system, iOS 4.3 (Halliday, March 2, 2011).

The following section explores the iOS file system in more detail.

3.1.1. The iOS File System

In 2008, Apple released iOS – an operating system for the iPhone, iPod, and iPad. This did not trouble forensic investigators since the iOS used on the iPad was the same as that of the iPhone. Therefore, at the time, no further studies were required, as they had been previously performed for the iPhone and iPod touch. In April 2010, Apple took a major step by releasing iOS 4 which introduced further notable features, such as multitasking, gaming features, video possibilities, and others (Morrissey, 2010).

Being familiar with all the features and having a good understanding of the Apple ecosystem was a fundamental requirement for establishing a solid understanding of iOS forensics (Morrissey, 2010). The iOS is a mini version of the OS X, which uses a modification of the Mac OS X kernel and its development is based on Xcode and Cocoa (Morrissey, 2010). iOS is composed of four main components; Cocoa Touch, Media, Core Services, and the OS X kernel. The first component, Cocoa Touch, provides the technological infrastructure to employ the applications' visual interface (Hoog & Strzempka, 2011). The second component, Media, contains graphics, audio and video technologies consisting of OpenAL, video playback, image files formats, quartz, core animation, and OpenGL (Morrissey, 2010). According to Hoog & Strzempka (2011), the third component, Core Services, delivers the primary system services for applications such as networking, SQLite databases, core location, and threads. The OS X kernel which is the fourth component, delivers low level networking, peripheral access, and memory management/file system handling (Hoog & Strzempka, 2011). It consists of TCP/IP, sockets, power management, file system, and security (Morrissey, 2010).

Morrissey (2010) stated that the Hierarchical File System (HFS) was developed by Apple in order to support the increased storage requirements of people. HFS formatted disks at the physical level are in 512 byte blocks, which is identical to Windows based sectors. An HFS system has two kinds of blocks, logical blocks and allocation blocks (Morrissey, 2010). The logical blocks are numbered from the first to the last on a given volume. They are static and are 512 bytes in size, just as the physical blocks. On the other hand, allocation blocks are used by the HFS system to reduce fragmentation.

They are collections of logical blocks joined together as clusters (Morrissey, 2010).

The HFS file system manages files by using balanced tree (B*tree), which is a catalog file system that uses a catalog file and extents overflows in its organization scheme (Morrissey, 2010). B*trees consist of nodes that are assembled together in a linear manner. This linear method increases the data access speed by continuously balancing the extents when data is deleted or added. The HFS file system gives a unique number (catalog ID number) for every file that is created, and increases by one each time a file is added. The numbering of the catalog ID is tracked by the HFS volume header (Morrissey, 2010).

| 1024 Reserved |
| Volume Header |
| |
| Allocation File |
| |
| Extents Over Flow File |
| |
| Catalog File |
| |
| Attributes File |
| |
| Startup File |
| |
| |
| Alternate Volume Header |
| |
| Reserved 512 Bytes |

| | Data |

Figure 1. Structure of HFS+ file system
Adapted from IOS Forensic Analysis: for iPhone, iPad and iPod Touch, by Morrissey, S, 2010: Apress. Copyright 2010 © by Sean Morrissey

Figure 1 illustrates the structure of an HFS+ file system as illustrated by Morrissey (2010). The boot blocks retain the first 1024 bytes. The subsequent 1024 bytes are retained for the volume header as well as the last 1024 bytes of the HFS volume, which is reserved as a backup volume header. The volume header stores information about the structure of the HFS volume. Next is the allocation file which traces the allocation blocks that the file system is using. The following is the extents overflow file which traces all the allocation blocks that belong to a file's data forks. A list of all extents used by a file and the connected blocks in the proper order is stored in this file.

The catalog file stores the volume files and folders' information that are in a hierarchical system of nodes. There is a header node, an index node, leaf nodes, and map nodes. The attributes file is reserved for future use of data forks, and the start up file is designed to boot a system which does not have a built-in ROM support. The space after start up file is used by the file system for saving and tracking all the data in a volume. The alternate volume header, as mentioned previously, is where the backup of the volume header is retained. Disk repair is the main purpose for the alternate volume header. Finally, the last chunk of HFS file system structure are the 512 bytes, which are reserved (Morrissey, 2010).

The file system for Apple portable devices is HFSX, but has one main difference from the HFS+. The difference is that the HFSX is case sensitive, thereby allowing the file system to distinguish between

two files that have the exact identical name. For instance, both test.doc and Test.doc can be created on the HFSX file system (Morrissey, 2010).

According to Cellebrite (2011), two partitions are included in the Apple devices. The first partition is the system partition, which is about 1 GB. The iOS and basic applications are stored in the first partition (G´omez-Miralles & Arnedo-Moreno, 2011). Although encryption may be enabled on the iDevice, the system partition is not encrypted (Cellebrite, July 3, 2011). However, the second partition is the one of interest, as it holds all the user data that can have evidentiary value. This partition includes all the photos, messages, GPS, videos, and other data that is generated by the user (Cellebrite, July 3, 2011). Extracting the protected files can be a challenge if encryption is enabled (Cellebrite, 2011).

3.1.2 Related Work

A paper by Luis G´omez-Miralles and Joan Arnedo-Moreno explored the method of obtaining a forensic image of the iPad using a Camera Connection Kit. The advantage of their method was the ability to decrease time by attaching an external hard disk to the iPad using a USB connection. Their method consisted of two parts. The first part was setting up the device by jailbreaking it. The second part was to acquire a forensic image, by connecting Apple's Camera Connection Kit, which was used to mount the USB hard drive. Next, was to obtain a forensic image using the dd command (G´omez-Miralles & Arnedo-Moreno, 2011).

Another research study by Mona Bader and Ibrahim Baggili, explored the forensic processing of the third generation of Apple iPhone 3GS 2.2.1 by using the Apple iTunes backup utility to retrieve a logical backup. Their research showed that the Backup folder with its backup files contains data that has evidentiary value, as the iPhone file system saves the data in binary lists and database files. Additionally, their results showed that XML format plist files are used to store device configuration, status, and application settings. Bader and Baggili (2010) stated that the backed up files from the iPhone contain information that could have evidentiary significance such as text messages, email messages, and GPS locations. The manual examination introduced in this paper is an extension of their work to the iPad2 device.

4. DESIGN – METHODS AND PROCEDURES

The methodology in this research takes into consideration the Computer Forensics Tool Testing guidelines established by the National Institute of Standards and Technology (NIST) (NIST, 2003). At a high level, the authors followed the following procedures:

1. Certain scenarios were entered onto three iPad2 devices

2. The devices were backed up (logically acquired)

3. The backup folders were then parsed using automated forensic tools and manually

4. The results were compared

After the scenario was created, the iPad2 was geared up for logical acquisition. The specifications of the devices used in the acquisition process are listed in Table 1. Then, the forensic tools were chosen to perform the logical acquisition. After reviewing some of the available tools' specifications and their ability to support iPad logical data extraction, Katana Forensic Lantern was chosen.

Table 1. Hardware Specifications

Device	Specification
Forensic Workstation	MacBook Pro Mac OS X Version 10.6.8 Processor: 2.26 GHz Intel Core 2 Duo Memory: 2 GB 1067 MHz DDR3
iPad	iPad 3G + WiFi Storage: 64 GB iOS: 4.10.01

Table 2. Software Specifications

Software	Details
Katana Forensic Lantern	Version 2.0 operatable on: Minimum of Intel based Mac OS X 10.6 with preferably 4GB memory Downloaded from: http://katanaforensics.com/
iTunes	iTunes 10 version 10.4.1 (10)
iPhone Backup Extractor	Version 3.0.8 Downloaded from: www.iphonebackupextractor.com
PlistEdit Pro	Version 1.7 (1.7) Downloaded from: http://www.fatcatsoftware.com/plisteditpro/
SQLite Database Browser	Version 1.3 Downloaded from: http://sqlitebrowser.sourceforge.net
Google Earth	Version 6.0.3.2197 Downloaded from: http://www.google.com/earth/download/ge/agree.html

Logical Acquisition Approach

Logical backups contain a vast amount of data that includes all sorts of evidence (Bader & Baggili, 2010). They are able to connect many dots, in any case, by providing further information about the computer that was previously used to synchronize the iDevice, and the owner of the device, including his/her interests and whereabouts (Bader & Baggili, 2010).

The logical backup was captured through the iTunes utility using a Mac OS X version 10.6.8. The system utilizes Apple's synchronization protocol in order to have all of the iDevice's data copied to the forensic workstation (Bader & Baggili, 2010).

It is important to note that any automatically initiated backup on iTunes may contaminate the iDevice by transferring data from the forensic workstation to the iDevice as a part of the synchronization (Bader & Baggili, 2010). This was noted, and steered clear of, prior to connecting the iPad to the forensic workstation by disabling the synchronization option in iTunes.

The logical backup folder was parsed using different methods: first, by using Katana Forensic Lantern. This software directly acquires the backup from the iDevice – provided that the automatic synchronization with iTunes is turned off; second, by using the iPhone Backup Extractor tool that

presents the backup data in a more visually appealing form than the original data; and third, through a manual examination of the backup folder.

Other software and tools were required to manually investigate the backup data such as the SQLite Database browser, PlistEdit Pro, and TextEdit as mentioned in Table 2. In order to prepare the iPad2 and backup data, a scenario was created on the iPad, by adding notes, email accounts, address book entries, photos (taken with the location option being On and Off), calendar entries and bookmarks. Then, the backup process was initiated using Mac OS X version 10.6.8 through iTunes version 10.4.1 (10). More specifications are included in Tables 1 and 2.

It must be noted that all the tests were conducted under forensically acceptable conditions, thereby avoiding any illegal access to the device through jailbreaking, especially since the main objective was to not contaminate the original data stored on the iPad2. According to Kruse & Heiser (2002), there are four key phases to follow in computer forensics processes, which are, access, acquire (logical), analyse, and report. These steps were followed in this research.

4.1. Instruments

4.1.1. Katana Forensic Lantern

Lantern is one of the iOS forensic solutions currently available on the market, developed by Katana Forensics. It is well known for its low cost, yet fast and effective results. It enables acquiring the logical portion of three different iOS devices: iPhones, iPads and iPod Touch (Morrissey, 2010). After the device is connected to the forensic computer, Lantern backs up the files and allows the examination of data while it is still processing. Timeline analysis and geographic data features are also supported (KatanaForensics, 2011b).

The software has an intuitive user interface. It is as simple as opening a new case, entering the case and evidence details, and then acquiring the device (KatanaForensics, 2011b). The maximum time for acquiring the iDevice ranges between 5 to 30 minutes, depending on the size of the device (Morrissey, 2010).

4.1.2. iTunes

Media player, digital media organizer, and iPhone/iPod/iPad content manager, are the features that the iTunes application offers since its introduction in 2001. It also connects to the iTunes Store and enables online content purchases (Apple, 2011c).

iTunes operates on both iOS and Windows, and is available for download, with no charges, through Apple's portal. It is primarily used to maintain media, applications, books, and content purchases, and are all synchronized with the owner's Apple devices. It creates backups of all the settings and media of the connected devices such as iPods, iPhones and iPads. These backups restore the captured settings and details of the devices (Apple, 2011c).

4.1.3. iPhone Backup Extractor

iPhone Backup Extractor is a freely available tool that can parse data from the iPhone's backup folder (ReincubateLtd, 2011). According to Morrissey (2010), it has the ability to convert the backup folder into CSV, VCard, or ICAL formats, so they can be easily viewed. It can also convert Keyhole Markup Language (KML) files for use with Google Earth if any location data is included. KML is an XML markup language used by map-related software for marking maps (Goldberg & Castro, 2008). Although iPhone Backup Extractor it is not considered to be a forensic tool, it provides means for examiners to analyse backup folders (Morrissey, 2010).

4.2. Data Collection and Analysis

4.2.1. Katana Forensic Lantern

When the acquisition process was complete, the following extracted data was shown:

Device Information: It provided general information about the device being acquired such as device name, type, model, serial number, and software version.

Contacts: This pane showed the phone book saved on the iDevice. It also showed all the related data to a contact in one single screen.

Notes: Thoughts, ideas, points, lists, and many more things can be typed in this application and may be used as evidence in an investigation.

Calendar: The calendar may include a great sum of information. It may contain appointments, events, notes, and important dates synchronized from many different devices and applications used by the user. Lantern's software parses all the data and alerts if they are occurring (Morrissey, 2010).

Internet: Considering the nature of the investigation being carried on, this section is of great importance. Lantern provides a clear list of all Internet bookmarks, displayed pages, and browsing history from the web surfing program on the iPad, which is Safari.

Gmail: This pane shows all the registered email accounts on the iPad. In this case, the tested device had a Gmail account set up, and all related emails, their contents, sender and receiver related information were displayed.

Dictionary: Each time text is typed on the iPad, it is logged and saved, and can be acquired during the investigation. Those entries can appear from texts typed into the device and are ordered in the dynamic dictionary file.

Maps: iPad users may record maps and routes into their handheld devices. All those details are parsed and can be exported to Google Maps to show more graphical details and more specific locations. Those details, in turn, can be exported to Google Earth so they can be plotted on a map.

WiFi: Shows a chronological order of all the WiFi connections attempted using the iPad, SSID, BSSID, and the security of that connection. This can be useful in capturing the access points the device was connected to.

Photos: This pane may be one of the most important panes for the investigator due to the richness of the information that it offers. All images taken with the built-in camera include Exchangeable Image File Format (EXIF) and embedded geographical data (KatanaForensics, 2011b). Those images can be identified using Lantern and are also clearly viewed within the program itself. Lantern can extract the geographical data from EXIF so that the location can be easily plotted on Google Maps, illustrating where the photo was taken (Morrissey, 2010).

Google Earth: Interesting data was found within the Exif associated photos taken using the built-in camera of the iPad. If the location service is on, it records the longitude and latitude of the exact location of where the photo was taken, along with other details about the camera type, aperture value, and many more related data. This data may be exported into a *.kmz* format, which then could be opened using Google Earth and show its exact location on the map.

Report: Lantern provides an option of exporting all the acquired data into html format. This summarizes all the panes and their related data into one page – which is easier to navigate through. It also provides the source file from which the data was extracted.

Third Party Applications: Although Lantern was of a great assistance in examining the evidence on iDevices, it did not provide significant details about third party applications installed on the iPad. Yet, it was possible to manually navigate through the exported report and find some related data to those applications.

4.2.2. iPhone Backup Extractor

iPhone Backup Extractor is not intended to serve as a forensics tool (Morrissey, 2010). It essentially parses the extracted backup folder into useful folders and file formats that, in turn, make it easier for

the examiner to go through (ReincubateLtd, 2011). Moreover, it parses the data in a more organized way and sorts it neatly e.g. *.plist, .sqlite3, & .db* files (Morrissey, 2010). iPhone Backup Extractor is not complicated and does not need any special knowledge to run and use (ReincubateLtd, 2011).

The following descriptions are files of interest extracted using the iPhone Backup Extractor:

Keychain-backup.plist: This file contains important tables such as the *genp* and *inet*. The tables contain accounts, their encrypted passwords, and related services (Bader & Baggili, 2010).

Library: This folder contains most of the important data that can be found within the backup, such as the saved entries in the Address Book (and the related images to each entry), Calendar, Keyboard entries, Notes, Safari and more. The files are in *.sqlite3* format and *.db* or *.plist.*

Media: Media folder parses the photos and their data into their relative folders.

Ocspcache.sqlite3: This database seems to include the digital certificates.

SystemConfiguration: This folder shows a collection of PList files that contain data about networks the device is connected to, their preferences, and the power management details.

TrustStore.sqlite3: This database contains the CA certificates that the iPad trusts. The CA certificates are used for security credentials and message encryption by using public keys (SearchSecurity.com, 2011).

Com.facebook.Facebook: This backup folder holds all the data related to the facebook account associated with the iPad under investigation. A database of all the facebook friends' networks can also be found in *.db* format.

Dynamic-text.dat file (Dictionary): Any text entered in the iPad is logged into a file called dynamic-text.dat. This file can be of a great help to the investigator due to the insight it provides about the suspects usage of the device. It can potentially direct the whole investigation into the proper path by providing solid facts.

com.skype.Skype: Skype provides video calls, screen sharing, and many more features. It can potentially reveal a lot about the suspect's personality and provide corroborating evidence. The database contains many tables such as Accounts, CallMembers and ChatMembers.

com.apple.ibooks: This database mainly holds details about all electronic books and *.pdf* files added to the iBook application. It shows plenty of interesting related details such as the title of the item, the author, and the categories. This could provide further details about the personality of the suspects and their interests.

Com.linkedin.Linkedin.plist: This PList file holds details of the Linkedin account used on the iDevice. It mainly shows general user profile details such as user name, job title, associated twitter accounts, pictures, and a link to the user profile and photo URL.

4.2.3. Manual Examination of iTunes Backup Folder:

A manual examination of the iTunes backup folder was conducted without using any automated tools to parse the files. The backup folder contained more than 2000 files. These files consisted of different kinds of files, such as PLists, SQL databases, images, HTML files, and more.

As a part of the backup folder, three main PList files were generated; Info.plist, Status.plist, and Manifest.plist. In Manifest.plist, a metadata file identifies the *.mddata* and *.mdinfo* files. The Status.plist file holds the status of the backup, i.e. if it was completed successfully, and the date and time of the backup.

Another file contained within the backup folder was the Info.plist. This plist file holds details about the backup and other information regarding the iDevice (GitHub, 2011). Other files found in the backup folder are Manifest.mbdb and Manifest.mbdx. These are binary index files that contain the

names and paths of the files in the backup (LeMere, 2010). It also contains the real names of the files representing the random strings in the backup folder (Ley, 2011). The *.mbdb* file holds the data of the original files, and the *.mbdx* contains pointers to those files in the *.mbdb* file as well as the hex file names included within the backup folder (ROYVANRIJN, April 21, 2011). Furthermore, the *.mbdb* also contains a file header which holds the version number of mbdx and the number of records present in the mbdx file (LeMere, 2010).

The following is the list of some of the files of interest found using the manual examination method:

Dynamic Dictionary: Found in *0b68edc697a550c9b977b77cd012fa9a0557dfcb*.

iBooks: The SQLite database of iBooks is contained within the file *1c955dc79317ef8679a99f24697666bf9e4a9de6.*

Skype: Many files related to the Skype application were found and examined – most of which were text files containing encrypted data, except the user names involved in the video calls were in clear text. In addition, a SQLite database was found with relevant data to the calls carried out, the duration, involved usernames, and language used. The SQLite DB had the following name: *a6414be1fc3678b0ea60492a47d866db3a6d4818* file and its related Plist file had the following name: *5c7504d4b4aa4395d7b3651bc0d523de121c3159*. It was also found that the hash value of the application was not constant amongst multiple tested devices.

Bookmarks: Bookmarks database is contained within the file named *d1f062e2da26192a6625d968274bfda8d07821e4* and contains many different tables within its database with data related to the bookmark URL and the title of each link.

Notes: Contains details about the notes saved on the device. The SHA-1 value is *ca3bc056d4da0bbf88b5fb3be254f3b7147e639c*

Twitter: Twitter data was in PList format and contained the usernames and content of tweets exchanged amongst them. The related SHA-1 values for the twitter application files were as follows:

1ae8b59701a8ef5a48a50add6818148c9cbed566

2ba214fcde984bbc5ea2b48acd151b61b651c1c8

4eb24cb35ff5209d08774a6d2db4c98a0449a9ff

7a0c2551ecd6f950316f55d0591f8b4922910721

71127e4db8d3d73d8871473f09c16695a1a2532c

c5dc95a1b0c31173c455605e58bffcca83d8b864

Connection WiFi: The file *3ea0280c7d1bd352397fc658b2328a7f3b1243b* in all three tested iPads contained related data to the WiFi and network connections.

Gmail Contacts List: An interesting finding of the manual examination was a SQLite database file containing email accounts, names, and mobile numbers of the registered Gmail account on the iPad. The findings contained information that was not initially entered for each contact in the list but was synchronized with a Blackberry device Address Book of the owner.

The Gmail account is set up on the Blackberry and is synchronized with the device's contact list. All contacts' mobile numbers were found in the backup folder since that Gmail account was also set up on the iPad under examination. This could lead an investigator to find a suspect's contact numbers, so long as they were mainly saved on his/her mobile device.

Linkedin: The relative PList file to this application is named *9c404eb0aa691005cdbd1e97ca74685c334f3635* and provides details such as the first name, last name, user name, profile URL, and the job title.

Calendar: The calendar contains two relative files in the backup folder, a SQLite database and PList. The former is saved under *2041457d5fe04d39d0ab481178355df6781e6858* and the latter under *d351344f01cbe4900c9e981d1fb7ea5614e7c2e5*.

Keychain: This file was found in *51a4616e576dd33cd2abadfea874eb8ff246bf0e* and contains genp, cert, inet, and keys tables. These tables provide more data about the accounts registered on the device along with their relative passwords and details.

Table 3. Backup files and their relative applications

Backup	File Type	Backup File
Keychain	PList	51a4616e576dd33cd2abadfea874eb8ff246bf0e
WiFi Connections	PList	3ea0280c7d1bd352397fc658b2328a7f3b1243b ade0340f576ee14793c607073bd7e8e409af07a8
Dynamic Dictionary	Text	0b68edc697a550c9b977b77cd012fa9a0557dfcb
iBooks	SQLite	1c955dc79317ef8679a99f24697666bf9e4a9de6
	PList	51fca3a3004e8f8e08f37a0a5ac3d7512274ee24
Twitter	PList	1ae8b59701a8ef5a48a50add6818148c9cbed566 2ba214fcde984bbc5ea2b48acd151b61b651c1c8 4eb24cb35ff5209d08774a6d2db4c98a0449a9ff 7a0c2551ecd6f950316f55d0591f8b4922910721 71127e4db8d3d73d8871473f09c16695a1a2532c c5dc95a1b0c31173c455605e58bffcca83d8b864
LinkedIn	PList	9c404eb0aa691005cdbd1e97ca74685c334f3635
Bookmarks	SQLite	d1f062e2da26192a6625d968274bfda8d07821e4
Google+	PList	5f0a990d1c729a8b20627e18929960fc94f3ee6b
Mail Accounts	PList	5fd03a33c2a311065035895730451500c740721dd
Airplane Mode	PList	06af93e6265bf32205de534582c3e8b8b3b5ee9e
Browser History	SQLite	19cb8d89a179d13e45320f9f3965c7ea7454b10d
Keyboard options	PList	36eb88809db6179b2fda77099cefce12792f0889
Notes	PList	52c03edfc4da9eba398684afb69ba503a2709667
	SQLite	ca3bc056d4da0bbf88b5fb3be254f3b7147e639c
Last Sleep	PList	06642c767b9d974f12af8d72212b766709ba08fe
Audio Player details	PList	59445c4fae86445d6326f08d3c3bcf7b60ac54d3
Calendar	SQLite	2041457d5fe04d39d0ab481178355df6781e6858
	PList	d351344f01cbe4900c9e981d1fb7ea5614e7c2e5
Safari Active Documents	PList	9281049ff1d27f1129c0bd17a95c863350e6f5a2
Mailbox details	PList	a2d4e045244686a6366a266ba9f7ef88e747fe4b
Photos	SQLite	bedec6d42efe57123676bfa31e98ab68b713195f
Dropbox	PList	d00b419a7c5cbffd19f429d69aff468291d53b00
Ocsp	SQLite	f936b60c64de096db559922b70a23faa8db75dbd

4.3. Challenges

Generally, investigators may face challenges no matter what device is being examined. However, since criminals continue to develop novel methods to cover their tracks, digital forensics has to constantly evolve with many technologies being introduced to defend against those harmful attacks (Husain, Baggili, & Sridhar, 2011).

A challenge that can be faced in a case is a locked iPad device. Since this is a user entered PIN, there are no default codes provided in the user manual providing an investigator with a limited number of attempts to try different passwords. As a security precaution offered by Apple on all iDevices, multiple unsuccessful attempts may lead to erasing all data on the device.

Examiners should consider the following when a locked iDevice is being investigated (Apple, September 22, 2011):

- Repeatedly entering the wrong password on the iDevice will lead it to being disabled for a certain period of time, starting with 1 minute. The more the unsuccessful attempts, the longer the disabled interval will be.

- Too many unsuccessful attempts will lead to not being able to gain access to the iDevice until it is connected to the computer it was originally synchronized with.

- The user may have configured the device to erase itself after a certain number of consecutive unsuccessful attempts.

There are many ways to obtain the PIN of a locked device during an investigation (Punja & Mislan, 2008):

- Using common PIN numbers, such as the last 4 digits of the owner's phone number, the year of birth, or any other related PIN that is found during the investigation.

- Obtaining it directly from the owner.

- Brute force attack (but may be inapplicable in case of having a limited number of attempts).

Few software vendors claim now to provide features that take the investigation further by decrypting the forensic images captured and obtaining the passcode within 20-40 minutes depending on the passcode complexity through brute-force. Katana Forensics provides a complimentary application to their original Lantern program that images iOS devices. Since the complimentary software was released after the completion of this experiment, the newly added features were not tested.

Another software, Elcomsoft iOS Forensic Toolkit, provides similar features to Lantern Lite. The former has iOS 4.x and iOS 5 Passcode Recovery. This forensic tool also performs a brute-force attack, even for complex passcodes. It also obtains the encryption keys from the iDevice.

Another challenge is the differences in the iPhone backup structures depending on the installed iOS version. Since the early versions of the Apple firmware, there have been changes in the backup formats and structures. It started with .mdbackup files to .mddata and .mdinfo in the 3G iPhone and iOS 3.0. The former file type contained data related to the phone, where the latter held the respective metadata (Morrissey, 2010).

Once iOS 4.0 was released, a new backup structure was introduced. The hashed filenames still held the data but without the .mddata and .mdinfo extensions (Morrissey, 2010). Instead, everything was stored in manifest.mbdb. This database contains the full path and filenames, and could be viewed using TextEdit (Hoog & Strzempka, 2011).

5. SUMMARY OF FINDINGS

We share below the summary of our findings from performing this research. A comparative summary is also provided in Table 4.

Katana Forensic Lantern:

- Provides detailed, neat, and well organized results.

- Exports the output into an html file that is very easy to scroll and navigate through.

- Easy to export photos and WiFi connections data into a *.kmz* file that views their locations on

the map using Google Earth.

- Limits previewing data related to third party applications in the main results window. But it is possible to navigate for third party details manually in the extracted reports from the tool itself.

- Requires third party applications to view PList and SQLite files.

iPhone Backup Extractor:

- Organizes the backup folder into sub folders, separating third party applications from the iOS files, which contains most of the iDevice related data.

- Some files found using this tool were not captured through backup folder manual examination such as TrustStore.sqlite3.

- The output does not transmit the files to their related files in the backup folders and their related SHA-1 file names.

- It is not considered as a forensics tool.

Manual Examination:

- Provides a lot of data which could be considered both good and bad. It is good because the logical backup data is not missed if fully examined. It could be considered bad because it is messy, randomly spread, and cumbersome to manually examine since the Backup folders contain thousands of files.

- Provides more digital evidence than other built-in applications installed on the device like Twitter, Skype and Linkedin. Evidence includes user interactions with the application, such as chat details, private messages sent/received, usernames and the date/time stamps associated with these digital evidence.

- Some of the databases found through manual examination contained information synchronized between the user's handheld mobile phone and the email address set up on the iDevice. This can be of great relevance to certain investigations.

- If certain installed application evidence is needed for an investigation, then this is the most appropriate method for an investigator to use.

Differences between iOS 3 and iOS 4:

Previously conducted research on the backup folder of the iOS resulted in relating the backup files to certain file names in SHA-1 hash values. It proved that those SHA-1 values were constant amongst certain applications in any backup folder, which made it easier to fetch the desired data directly from the backup folder without the need to go through each and every file.

This research revealed some changes to the iOS backup structure and illustrated how some of those related SHA-1 values have changed across some applications as shown in Table 5.

Table 4. Comparison between the tools

	Katana Forensic Lantern	iPhone Backup Extractor	Manual Examination
Cost	Government Rate $599.00 Corporate Rate $699.00	Free Edition Registered $34.95	Free
Data Acquisition			
Logical Acquisition	Yes	Yes	Yes
Physical Acquisition	*Released Post Experiment	No	No
Analysis			
Automated	Yes	No	No
Built-in Image Viewer	Yes	No	No
Built-in Text Viewer	Yes	No	No
Deleted Data Recovery	No	No	No
File Sorting	Yes	Yes	No
Third-party applications data (e.g. twitter, LinkedIn, Skype, etc…)	Partial	Partial	Yes
Report Export (HTML)	Yes	No	No

Table 5. iOS 4 backup files compared to iOS 3 backup files

Backup	File Type	iOS 4.10.01	iOS 3.1.2	Match?
Notes	SQLite	ca3bc056d4da0bbf88b5fb3be254f3b7147e639c	ca3bc056d4da0bbf88b5fb3be254f3b7147e639c	Yes
	PList	52c03edfc4da9eba398684afb69ba503a2709667	N/A	N/A
Calendar	SQLite	2041457d5fe04d39d0ab481178355df6781e6858	2041457d5fe04d39d0ab481178355df6781e6858.mddata	Yes
	PList	d351344f01cbe4900c9e981d1fb7ea5614e7c2e5	N/A	N/A
Bookmarks	SQLite	d1f062e2da26192a6625d968274bfda8d07821e4	N/A	N/A
	PList	5d04e8e7049cdf56df0bf824820cddb1db08a8e2	04cc352fd9943f7c0c3f0781d4834fa137775761.mddata	No
History	SQLite	01e25a02a0fccbd18df66862ad23a2784b0fe534	N/A	N/A
	PList	bdadf7ce9d86a2b33c9ba6537311538f48e03996	1d6740792a2b845f4c1e6220c43906d7f0afe8ab.mddata	No

6. CONCLUSION

In sum, automated tools provide instant and visual evidentiary data from investigated iPads. Each automated tool has different capabilities; therefore different sets of results can be obtained from each tool. However, the manual examination provides more thorough and detailed evidentiary data from investigated iPads. This research points out that forensic software developers need to advance the capabilities of their automated tools. A robust technology that is capable of easing the manual examination process is needed. Overall, the authors propose that if a quick triage of an iOS device is needed, then an automated tool would suffice. However, if a more thorough examination is needed, especially if unique installed application data is needed, then the manual examination process should be utilized.

7. FUTURE WORK

On April 12, 2011, AccessData released the "Mobile Phone Examiner Plus (MPE +)," which is a standalone cell phone forensics application (AcessData, April 12, 2011). The main feature of this software solution is its ability to obtain the physical image of the iPad, iPhone and iPod Touch without jailbreaking the iOS device (AccessData, 2011). Another software application that supports the physical acquisition of iOS devices is the Lantern Light Physical Imager, which was due to be released in mid October 2011 (KatanaForensics, 2011a). These tools should be tested in order to assure that they are operating as required (Baggili, Mislan, & Rogers, 2007). Further studies should attempt to examine the error rates in the forensic tools used when examining iOS devices. Lastly, this research points to the direction of creating an extensible software framework for examining digital evidence on iOS devices. This framework should allow the forensic software to continuously be updated with backup file signatures depending on the version of the iOS. It should also allow the software to update signatures of backup files for newly released iOS applications.

REFERENCES

AccessData. (2011). MPE+ MOBILE FORENSICS SOFTWARE SUPPORTS 3500+ PHONES, INCLUDING IPHONE®, IPAD®, ANDROID™ AND BLACKBERRY® DEVICES, from http://accessdata.com/products/computer-forensics/mobile-phone-examiner

AcessData. (April 12, 2011). ACCESSDATA RELEASES MOBILE PHONE EXAMINER PLUS 4.2 with PHYSICAL IMAGING SUPPORT FOR IPHONE®, IPAD® AND IPOD TOUCH® DEVICES.

Apple. (2011a). Apple Launches iPad 2, from http://www.apple.com/pr/library/2011/03/02Apple-Launches-iPad-2.html

Apple. (2011b). iPad Technical Specification from http://www.apple.com/ipad/specs/

Apple. (2011c). iTunes, from http://www.apple.com/itunes/

Apple. (September 22, 2011). iOS: Wrong passcode results in red disabled screen, from http://support.apple.com/kb/ht1212

Bader, M., & Baggili, I. (2010). iPhone 3GS Forensics: Logical analysis using Apple iTunes Backup Utility. *SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, 4*(1).

Baggili, I. M., Mislan, R., & Rogers, M. (2007). Mobile Phone Forensics Tool Testing: A Database Driven Approach. *International Journal of Digital Evidence, 6*(2).

Cellebrite. (July 3, 2011). Cellebrite Physical Extraction Manual for iPhone & iPad.

Elmer-DeWitt, P. (March 13, 2011). Piper Jaffray: iPad 2 totally sold out, 70% to new buyers, *Cable News Network*. Retrieved from http://tech.fortune.cnn.com/2011/03/13/piper-jaffray-ipad-2-totally-sold-out-70-to-new-buyers/

G´omez-Miralles, L., & Arnedo-Moreno, J. (2011). *Universal, fast method for iPad forensics imaging via USB adapter*. Paper presented at the 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Korea

Geyer, M., & Felske, F. (2011). Consumer toy or corporate tool: the iPad enters the workplace. *interactions, 18*(4), 45-49. doi: 10.1145/1978822.1978832

GitHub. (2011). mdbackup-organiser, from https://github.com/echoz/mdbackup-organiser

Goldberg, K. H., & Castro, E. (2008). *XML*: Peachpit Press.

Halliday, J. (March 2, 2011). iPad 2 launch: live coverage of Apple's announcement. Retrieved from http://www.guardian.co.uk/technology/2011/mar/02/ipad-2-launch-apple-announcement-live

Hoog, A., & Strzempka, K. (2011). *IPhone and IOS Forensics: Investigation, Analysis and Mobile Security for Apple IPhone, IPad and IOS Devices*: Elsevier Science.

Husain, M. I., Baggili, I., & Sridhar, R. (2011). *A Simple Cost-Effective Framework for iPhone Forensic Analysis*. Paper presented at the Digital Forensics and Cyber Crime: Second International ICST Conference (October 4-6, 2010) Abu Dhabi, United Arab Emirates. http://books.google.ae/books?id=fiDXuEHFLhQC

KatanaForensics. (2011a). Lantern Light, from http://katanaforensics.com/forensics/lantern-lite/

KatanaForensics. (2011b). Lantern Version 2.0, from http://katanaforensics.com/forensics/lantern-v2-0/

KrollOntrack. (2011). Tablet Forensics – A Look at the Apple iPad®, from http://www.krollontrack.com/resource-library/legal-articles/imi/tablet-forensics-a-look-at-the-apple-ipad/?utm_source=Newsletter&utm_medium=Email&utm_campaign=IMI-Sept2011&utm_content=image

LeMere, B. (2010). Logical Backup Method, from http://dev.iosforensics.org/acquisition/acquisition_logical_method.html

Ley, S. (2011). Processing iPhone / iPod Touch Backup Files on a Computer from http://www.appleexaminer.com/iPhoneiPad/iPhoneBackup/iPhoneBackup.html

Miles, S. (January 27, 2010). Apple tablet unveiled as the iPad, *Pocket-lint* Retrieved from http://www.pocket-lint.com/news/31084/steve-jobs-launches-ipad-apple-tablet

Morrissey, S. (2010). *IOS Forensic Analysis: for IPhone, IPad and IPod Touch*: Apress.

NIST. (2003). CFTT Methodology Overview, from http://www.cftt.nist.gov/Methodology_Overview.htm

Pilley, J. (October 8, 2010). iPad and Smartphone Digital Forensics, from http://www.articleslash.net/Computers-and-Technology/Computer-Forensics/578641__iPad-and-Smartphone-Digital-Forensics.html

Punja, S. G., & Mislan, R. P. (2008). Mobile Device Analysis. *SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, 2*(1).

ReincubateLtd. (2011). iPhone Backup Extractor, from www.iphonebackupextractor.com

ROYVANRIJN. (April 21, 2011). Reading iPhone GPS data from backup (with Java), from http://www.redcode.nl/blog/2011/04/reading-iphone-gps-data-from-backup-with-java/

SearchSecurity.com. (2011). certificate authority (CA), from
http://searchsecurity.techtarget.com/definition/certificate-authority