A Framework for Digital Forensics in I-Devices: Jailed and Jail broken Devices

N. Kala
Scientific Officer,
Computer Forensics Division,
Forensic Sciences Department
Chennai – 4

R. Thilagaraj
Professor and Head
Department of Criminology,
University of Madras,
Chepauk, Chennai – 600 005.

Abstract

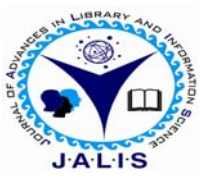
Prevalence and functionality of mobile devices are increasing. idevices such as smart phones, iphones and iPads are now being increasingly referred for digital investigations, since these are being used by terrorists, miscreants and contraband across borders and are also frequently used in prison despite being prohibited. Evidence retrieved from such devices is instrumental in solving grievous crimes such as homicide or suicide. Sometimes data exfiltration also occurs in reputed organizations and corporate sectors using idevices. A formalized triage of acquisition process is the need of the hour. idevices are presenting several challenges to digital forensicators. This paper focuses on the artefacts of forensic significance that are left on the mobile devices such as Apple iPhones and iPad and a framework has been suggested for acquisition of data from jailed and jailbroken devices

Keywords

idevices, iPhone, iPad, jailed, jailbroken, Remote Wiping option, Evidentiary artefacts

Electronic access

The journal is available at www.jalis.in



Journal of Advances in Library and Information Science
ISSN: 2277-2219 Vol. 2. No.2. 2013. pp. 82-93

1. Introduction

iPhone – a fascinating piece of engineering changed the way of telecommuters. iPad is yet another revelation. The rising popularity these devices have made it prevalent more and more in criminal cases. There is an increasing need to develop a framework since there are lots of challenges in performing examination on such devices. Huge volume of data and personal information are stored on these devices and its portability had made the dominance of Apple mobile devices. Individuals store more data on idevices than on their systems or laptops. These activities make the iPhone take the place of personal computers (PCs) (Hoog, 2011) and digital cameras. In addition to the standard capabilities that exist in the iPhone, endless applications are also available for download to assist with finances or organization, or simply for entertainment. Recognizing these advances and capabilities, it is conceivable that these devices could be used to commit or assist in criminal activities. Therefore they must be considered as viable sources of digital evidence and forensically sound procedures should be available to support a forensic analysis on the iphone. Digital forensicators are required to recover data from these devices during an investigation that is crucial to criminal cases today and future. This paper presents a methodology to extract evidentiary data of forensic significance from idevices. This paper describes forensic data extraction from two types of idevices (i.e. iPhone and iPad).

2 iPhone (Smart Mobile Phones)

The first iPhone was referred to as 2G and was capable of second generation cellular network edge. It also uses 802.11 technology, Bluetooth for accessories and hands free handset in September 2007. The main functions was just not cellular communication but web access, email, and PDA functions as well The Apple iPhone also connected to iTunes and YouTube. Prior to AppStore, web applications were being created for iPhones under varying categories such as calculate, games, entertainment, search tools, travel, weather, sports and productivity. The second generation iPhones referred to as 3G that switched to faster 3G network in the year 2008. The iPhone 4 was launched in 2010 with a newer and powerful iOS 4. A new application that allowed for video chat via WI-FI. Changing features of iOS which is the operating system for the iPhone, iPod and iPad are tabulated hereunder:

Table 1: iOS and applications

Series	Version of OS	Applications
1	iOS 1.0	SMS, Calendar, Photos, Camera, YouTube, Stocks, Maps, Notes, Clock, Calculator, Settings, iTunes, Phone, Mail, safari, iPod
2	iOS 2.0	AppStore(a market place for applications that could run on the iPhone), Global Positioning System(GPS), Wi-Fi, airplane mode, Scalable Vector Graphics(SVG), Parental controls and ability to save options from mail application, EXIF data – for images are notable applications and advancement to iOS 2.0
3	iOS 3.0	YouTube, Granular Call history, ability to change My Number field in the phone Settings, video capture with autofocus function to the camera (3GS), ability to use MobileMe to Find My iPhone feature from a setting on the phone and within the Mobile Me account. This is an important feature that allows you to remote wiping and add a passcode, or place a message on the screen of the phone remotely, spot light searching, Tethering, and Voice memos, voice control, encrypted backups, hardware encryption, ability to add devices from USB ports
4	iOS 4	Background audio, Voice over IP, Background location(GPS), Push Notification, Local Notification, Task Completion, iBooks, game centre features, iAd, Media, Enterprise features such as mail encryption, mobile device managementMultiple exchange accounts, SSL VPN Supports, core services such as networking, SQLite databases, Core Location, Threads, OS X Kernel that includes, TCP/IP, Sockets, Power Management, File System and Security

iOs Version and the corresponding name is given in Appendix B and iOS partition directory structure is given in Appendix C. iOS data partition comes from the read write partition also known as data partition. Logical acquisition of the file system can be acquired from this device.

Mobile devices (mobile Phones/Smart Phones) can provide contextual clues about the owners, about the person's the owner knows and communicated with. Investigators are provided with information about owners close associates from the call logs(received, dialled and missed); Short Message Service (SMS) text contents and Multimedia Messages reveal personal communication that the owner never expected others to see. Images and videos reveal what was important to the owner. Audio recordings speak about owner's personality. A thorough inspection of mobile devices produces intelligence that leads to a complete and correct analysis. Evidential points (Mislan, 2010) in the form of data found in mobile devices help construct complete sketch of the suspect or the victim.

2.1 iPad

Originally Apple computers wanted to release the iPad first and then the iPhone. Instead. iPhone was released first and then iPad. It is a tablet device that runs on iOS 3.2 and completed the iDevice line.

3. The Apple App Store

Prior to iPhone 3G there were limited number of applications that were available to the iPhone: Calender, Camera, Weather, Maps, Notes, Clock settings and in the Dock, Phone, mail, iPod. Apple App Store, has actually become one of the greatest success of Apple iPhone using which the store has become digital iTunes of the iPhone. Several Apps were released in the iPhone SDK. Nearly 500 new applications cameup when the developers were called to create the applications for new 3G and iPhone OS. 2.0.

Today there are more than 300,000 applications available from apple app store. User has to create an account by applying through iTunes in order to purchase an applications directly on iPhone, iPod or iPad. This can be done online to the appstore and grab applications either free of cost or paid applications.

There are two ways to get connected to appstore on the phone or ipad. First ways is through connecting the device to the computer and connect to the

appstore. Once it is connected the changes are updated in the next sync. The second way is to add an application to the phone is right from the phone itself. The limitation in this method is that some application larger than 20MB to be downloaded via 3G and wi-fi connection is requested by the app. Apps can be searched by name , category or popularity.

3.2 iTunes interaction

Various functions are offered by iTunes to manage the files, applications or apps as they are called, software versions and the device. Synchronization can be done by the user and this process will create a sync and all apps, videos, audios, images and the like will be loaded depending upon the settings defined by users. iTunes can be configured to perform either an automatic sync every time it is connected or a manual sync.

3.3 iPhone backup

Backups can be created once the iPhone is connected to the system. Automated backups is initiated during a sync process; restore or update, depending upon the Operating system which is running on the user's system in specific location.

4. State of Art Forensic Procedures

With the emergence of diverse nature of the mobile devices, there are several approaches that can be used to acquire the data from devices. A Key component of any acquisition is that the procedure does not modify the source information. Different approaches can be used for acquisition and analysis of information. In the case of idevices, unlike the conventional digital forensics the storage media cannot be removed and imaged and finally analyzed. NIST has instituted the Computer Forensic Tool Testing Program. Many different tools are used intentionally and are relied upon to provide electronic evidence for criminal cases. Considering various types of mobile acquisition tools and the data that can be recovered from, a classification system has been suggested. Accordingly, this classification system provides a framework for forensic examiners. Classification system is represented in Pyramid starting at the bottom and working upward, the methods and tools generally become more technical, invasive, time consuming, forensically sound and expensive (Brothers, 2007). Level 1. At the base is the process of manual extraction. Level 2. Logical analysis is used by most investigators. Level 3 Hex Dump a method that is adopted by the forensic community recently. Level 4 – Chip Off - a new frontier - the process only just available. Finally, Level 5 is rarely performed as it is extremely technical, very expensive and time consuming.

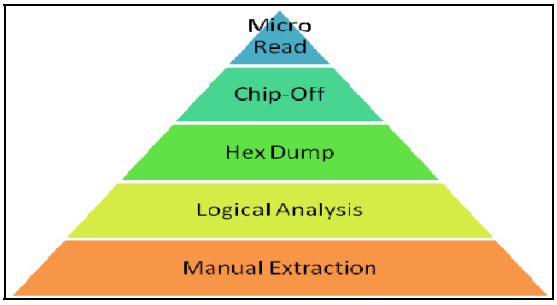


Figure 1 iPhone Levelling (Source Sam Brothers)

Existing forensic tools can be classified under any one of these levels suggested by Sam Brothers. Detailed information (Brothers, 2007) regarding the levels, type of extraction and process are shown in table 2.

Table 2 : Types of extraction process

Level 1	Manual Extraction	A Manual extraction involves visual acquisition of the data content on the phone directly by viewing it on the screen of the device keypad. The information retrieved is manually documented through photography. At this level it is not possible to recover information that are deleted.
Level 2	Logical Extraction	Connectivity to the mobile device established through either a cable or through Bluetooth to the forensic hardware and subsequently analysed in a forensic workstation. A command is initiated
Level 3	Hex Dump	A hex dump also called "Physical Extraction", provides more information about the available data to the investigator. In this process the device is connected to the workstation via a cable. Occasionally this connection is either through the device's

		data port, via Wi_Fi, or even JTAG (an internal test connection. Instead of initiating a command, an agent (unsigned code) is copied to the device memory which enables to copy the users data onto the workstation. The resulting copied data is transferred, stored as a raw disk image.
Level 4	Chip-Off	In this level, acquisition of data from the device's memory chip e.g. iPhone NAND Flash memory. In which case the chip is physically removed from the device and the data stored on it is extracted by a chip reader. With wide variety of available chip types used, the raw binary formats examination is tough and time consuming. Also, there is a risk of causing physical damage to the chip during the extraction process.
Level 5	Micro Read	This process involves manually viewing and interpreting data that is observed on the memory chip. This is done by analysing the physical gates on the chip. The gate status could be translate '0's and '1's to determine the ASCII characters. This process is time consuming and expensive and it requires knowledge of all aspects of Flash memory and the file system. Currently there are no commercial tools available to perform a micro read on an Apple Device.

4.1.3 Physical acquisition

In this process, bit by bit copy of the original file system is made. Most computer forensic tools have the facility to acquire information physically. It involves more complicated process and sophisticated equipment. In this approach it is possible to obtain the deleted information. Any type of data contained on the device can be recovered using this method. Advanced examination of the resulting disk image file also has the potential to recover GPS coordinates and cell tower locations and even deleted text and multimedia messages. Metadata information can be extracted for e.g. timestamp of photo taken on the device. Various files can be pieced together in order to produce additional results. However, the current tools does not support for all types of mobile phones models, non-standard mobile phones or even some specific models of standard mobile phones.

4.1.4 Non Traditional Method

Various security settings are available on iDevices that allow the user to protect unauthorized access to their devices and data. For instance, iPhone user has option to set PIN on their device in order to prevent unauthorized access. PIN is a four digit number by default, a numeric code but by modifying the "Simple Passcode" setting to a variable length. Also by entering the incorrect Passcode more than specified number of times (usually 10 times) the device can be set to automatically erase all the contents. Secure erase is an option that is available on the idevices (iPhone and iPad). It is possible "Reset All Settings" or "Erase All Content and Settings. Data security for iPhone and iPad ensures that secure erase indeed truly wipes the device. Another security feature that is facilitated is the MobileMe membership. MobileMe allows the user to remotely set a Passcode in the event that a device is stolen. Additionally, it is possible to have hardware encryption through a feature "Data Protection". This can be done using a Passcode. Once Passcode is set, the device settings will show "Data Protection enabled". This enables encryption and activates added layer of security for email messages and attachments. Encryption compounds to complexity of forensic acquisition process. The iOS devices contain the hardware encryption from iPhone 4, iPhone 3, iPod Touch, and iPads (Apple Inc, 2010). Additionally, an optional configuration is an automatic lock set after certain period of time. The best practice that should be followed while seizing an iOS device is if it is not locked, it is advisable to immediately set the auto-lock to "never". This will enable the forensic examiner to require not to enter a Passcode to access the device. The Passcode will not be an issue if the physical acquisition, however, in case of logical acquisition it is essential to set the autolock to 'never'. Individual application on idevices also has features to set passcodes so that unauthorized access is restricted.

Some less common methods are available to extract data from idevices. This method involves a process that will modify the firmware on the device to allow for greater functionality. This ruling does not force Apple to cover jailbroken devices under the manufacturer's warranty; it simply means that the individuals who may decide to modify their device in this manner will not be criminally prosecuted. In addition any software downloaded on the device must be legally acquired therefore pirated software is still illegal under this Act (Moren, 2010). Other methods in a jailbroken device from which extraction can be done is to connect to such devices using known commands such as 'ssh' or 'ftp' using applications such as MobileTerminal and OpenSSH. By this way the examiner can view the file system on the device, and the directory structure is similar to performing a physical acquisition not the exactly the same. Both individual files and entire file system can be copied to a forensic workstation.

4.1.5 Forensics using Linux Platform

Linux platform provides extremely powerful tools to assist in forensic investigation. This process involves various stages such as creating a disk image, image verification followed by mounting and unmounting a disk image to view the file contents, file carving and creating a timeline of events. Various stages that are involved are shown in table-3.

Table 3: Various stages

Stage	Stage name	Description
Stage 1	Creating a disk image	The 'dd' command (acquisition utility) can be used to image a device that such as a jailbroken iPhone or iPad (where root access is available for the forensic examiner).
Stage 2	Image Verification	The forensic process involves acquisition of image of device so that it does not modify the original media. Either MD5 or SHA1 hash value may be generated. Linux commands can also be used to determine either of these values on an image or a file.
Stage 3	Mounting and un mounting a disk image	The image must be mounted to view the contents of the file system. Once the image is mounted, the directory files in the OS can be viewed.
Stage 4	File Carving	File carving is a process to recover files signatures, file fragments. This way both active and deleted files can be recovered. It is possible to recover deleted files because the carving of file involves a process that focuses on the files content rather that its metadata. Linux tools are available which will perform this action, and the tools can be run via a command line against an iPhone, iPad or other iOS device image in order to recover valuable files.
Stage 5	Creating a timeline of events	Tools are available that can be run on a disk image and list out each and every file with the file system, both allocated and unallocated. A time line of events could then be created that occurred on the device. This process is typically run against a hard drive, but can also be run on , iPad or other iOS device image
Stage 6	Searching a disk image	Specific keyword search utilities are available. "Strings" command of Linux can be used to extract printable characters and recover individual files. Sometimes a hex editor could be used to a specific area within an image.(e.g. the email address of interest in a case can be searched and subsequently the background information /content could be analyzed.

4.2 Recently developed Methods

Recent addition to mobile phone forensic tools is that of Jonathan Zdziarski(– most popular tool that has been recently tested by the Computer Forensics Tool Testing Program a joint program of the National Institute of Justice and the Department of Homeland Security. The tool developed by Jonathan Zdziarski offers the examiner command line automated tools that can be used on Linux machine or Mac workstation. Physical acquisition of iPhone or iPad with zdziarski method has been tested by National Institute of Standards and Technology (NIST, www.cftt.gov/mobile_devices.htm, 2010)

Release of iOS4 has compounded to the complexity of the forensics in idevices. Hardware encryption is offered with iOS 4 on iPhone 4, 3GS, iPod Touch, and all iPad models. This means even if a full disk image is possible, the data in the devices are still encrypted. There are currently three methods to perform physical acquisition on an iPhone or iPad. They are the Forensic Telecommunication Services (FTS) iXAM software, zdziarski methods or through a jailbroken device. This method requires downloading of "automated tools" from his website. The tools are strictly command line utilities which can be used to acquire bit by bit copy of the user data partition. A recovery agent has to be installed in the file system partition of the device and a recovery script is used to make a raw disk image of the device. This can be copied to the forensic workstation through USB connection. Having copied the image, the device model and firmware version the imaging process begins through the recovery or DFU Mode. Once the imaging is done, the internal data can be analysed. Acquisition can also be done, remotely by creating a wireless network and connecting to the iPhone and then imaging.

Preparation phase requires the knowledge of model and firmware version. This is an important step because in this method, different automated tools are available for unique models and firmware version combination. The model number can generally be seen at the back of the device. It is also essential that the appropriate iTunes be downloaded else, most commercial tools will show up and iTunes error.

4.3 Commercial Tools

The list of commercial tools available is tabulated hereunder:

Table 4: Commercial Tools

S. No	Tool name
1	CelleBrite UFED
2	iXAM
3	Oxygen Forensic Suite 2010
4	XRY
5	Lantern
6	MackLoc Pick
7	Mobilyze
8	Zdziarski Technique
9	Paraben Device Seizure
10	MobileSync Browser
11	CellDEK
12	Encase Neutrino
13	iPhone analyzer
14	iPhone Extractor

4.4 Limitation

Many of the tools do not support iOS 4 until recently. In the case of Jailed idevice if a Passcode is enabled then it is difficult to bypass the Passcode or pattern lock. Only recently XRY from Micro Systemation have launched their product that will enable to read even jailed devices. Even if some of the tools are providing facility to retrieve the information, they support only for specific model.

5. Artefacts of forensic significance

Backup analysis is beneficial when the device is whether unavailable or unable to be imaged for a specific reason. Common data is generally stored in SQlite Databases and Property List files. These two are supported by synchronization protocol. Most of the active data that still remains on the device can be retrieved. In the case of iPhones, by querying the Sqlite databases directrly, SMS, Call Logs, Contact details can be recovered. Various directories are found and in some of them sqlite data bases reside. Directories and corresponding items of interest include CommCenter, Dhcpclient, db, Ea, folders, keychains.db, Log, Logs(General.log contains the OS version and Serial No and the Lockdownd.log conatins the lockdown deamon log), Managed Preferences, Mobile contains the bulk of user data, MobileDevice, Preferences contains the System configuration, Root directory contains the GPS location information cache is available, Lockdown pairing certificates and preferences. The Run directory contains the system log, tmp directory contains Manifes.plist:plist backup, and VM. When it

is plugged in the name of the device, capacity, software version, serial number and phone number (iPhones) are displayed.

The OS image for an iPhone is not backed up on each sync. The image is only backed up when the phone software is upgraded. The image changes only between major version.

The following information are stored in iPhone

- Keyboard cache
- Screenshots (when home button is pressed shows last state of application running when button is pressed
- Images- active or deleted from users library of photos
- Deleted address book entries
- Call history
- Deleted voice mail
- Emails and SMS
- Browser Cache
- GPS locations
- Pairing record
- Phone details
- Latitude and Longitude for some images

5.1 Apps

Upon initial sync with itunes, an acrchive on the computer of all the user appls and data from the phone are created. Files are updated in place with every sync of the phone. This archive is used to recover the phone if needed. Archive is located at /Library/ApplicationSupport/MobileSync/Backup/<phone ID>

5.2 Property List

Apple Property lists are used. iPhones uses 3 main 'Standard' plist. These are

- Info.plist,
- Manifest.plist
- Status.plist

These are plain text XML documents. These can be easily viewed but difficult to decipher. Within this substantial information about Base64 <data> chunks may be stored. When plistlb or python 2.5 is used this can be parsed and the device name, model, GUID etc could be found.

'mdinfo' is another location which is Apple 'bplist' files. This is a special kind of plist which is 'binary packed'. In order to read this, Apple provides an easy to use OSX utility called 'plutil'. It can be obtained using 'plutil – convert xml1 <filename>. This command converts the bplist fire into standard plist in place. Many of bplist files have Base64 encoded <data> property values that are themselves bplists. The SMS db bplist is a file like this one. Another list is the 'mmdata'. These mddata files are renamed copies of whatever the original source file described by the md file was. These contain images, databases, text chunks and specific application such as MOBI ebook. It is possible to open PNGs/JPGs as it is since there is no formatting changes.

5.3 File Name

iOS storage is broken into something called 'Domains' . Each has file name, path, and a particular storage domain. Two primary domains are 'HomeDomain' and 'MediaDomain'. The file names of the mddata and mdinfo files are a SHA1 hash of the full path of the files on handset location and the domain it is located in. Filenames does not appear to change.

5.4 Info.plist

This is an unencoded standard of Apple Property List file(XML text). This contains repository of information about the phone. The following are the details found in this list

- ICCID – Integrated Circuit Card ID – the hardware serial number of the SIM card
- IMEI – International Mobile Equipment Identity, the hardware serial number of the handset.
- Phone Number
- Serial Number – iPhone's Serial number
- Product Type – information about what kind of phone (capacity 8GB 3GS or 8 GB 3G etc)
- Product version – the OS revision number
- Data of last backup
- iPhone preference
- iPhone preferences plist(base 64 encoded embedded plist)
- Misc. Other stuff encoded/binary application specific data

The following screenshot illustrates the info.plist from a jailed iPhone showing the Users name, GUID, IMEI & ICCID number.

5.5 Sqlite Databases

Apple uses sqlite databases extensively across their platforms and application ranges and it is known as 'CoreData'. It is a open source, file based database engine. illustrates the directory list that are available in the backup and the corresponding artefact forensic significance.

Table-5: ARTEFACT FORENSIC SIGNIFICANCE

S.No	Directory Name	Artefact of forensic significance
1	Mobile/Application	Plists: Property list Sqlite Databases:
2	Libraries/Address Book	Contacts and imagesSqlite Databases:
3	Library Cache	Sqlite Database: MapTiles
4	Library/Calendar	Sqlite Database: Events
5	Library/CallHistory	Sqlite Database: CallLogs
6	Library/Carrier Bundles	Carrier information
7	Library/Caches.apple.itunesstored	iTunes purchase information
8	Library/ConfigurationProfiles	Plist: password history
9	Library/Cookies	Plist: Internet cookies
10	Library/DataAccess	Email account information
11	Library/Keyboard	.dat file: Dynamic text
12	Library/Logs	Log files
13	Library/Mail	Logical Data, no artefacts
14	Library/Maps	Plist:Bookmarks, directions, history
15	Library/Mobileinstallation	Plist: Applications that use Locations
16	Library/Notes	Sqlite Databse: Notes content artefacts
17	Library/preferences	Plist: System and user settings
18	Library/RemoteNotification	Plist:apps that have push notification
19	Library/safari	Plist: bookmarks, history
20	Library/SafeHarbor	Location of where app data is stored
21	Library/SMS	SMS and MMS data
22	Library/Voicemail	.amr files: Voice messages
23	Library/Webkit	Sqlite databases: gmail account info, cached email messages
24	Media/DCIM	iPhone Camera Photos
25	Media/PhotoData	Additional photo information and thumbnails

Sqlite database contains information of addressbooks, application, cache,map, calendar events, gmail account info data base etc.

Simple relational database, supports most of SQL-92. Sqlite3 is OS x built into CLI to access SqLite database files. In the CLI, the '.schema' command shows the database and table schemas.In the case of iPhones SMS records are stored in a database called 'sms.db' and it is found in location "HomeDomain-Library/SMS/sms.db". These are updated during a sync in which case the deleted messages are removed and new messages are inserted. However it does not contain MMS information. Simple data structure for the SMS database is tabulated hereunder:

Table 6: Data structure of SMS database

ROWID	Integer
Address	Text
Date	Integer
Text	Text
Flags	Integer
Replace	Integer
Svc_center	Text
Group_id	Integer
Association_id	Integer
Height	Integer
UIFlags	Integer
Version	Integer
Subject	Text
Country	Text
Headers	Blob
Recipients	Blob
Read	Integer

- Address is either source or destination phone number in 11 digit intl.format(18885551212).
- Time is in UNIX epoch format(# of Seconds since 1/1/70 0:00UTC).
- Flags field is used to indicate :
  - '2' = Message received from 'address'
  - '3' = Message sent from handset to 'address'
  - '33' = Message send failure (SMS never sent)
  - '35' = Message deleted (but still appears as a row, - not contents)
  - '129' = Message deleted (but still appears as a row- no contents though)
  - '131 = unknone – no address
- 'Text' field is sometimes a plist – this typically indicates an MMS was received. MMS text/image information is stored separately in 'mmdata' files outside of the SQlite db.

5.6 Third Party application

Friends.db

Friends.db is another database that is located in 'AppDomain-com.Facebook-Documents/friends.db'. This database contains Facebook friends list and tiny bit of extra information (i.e) facebook UID [www.facebook.com/profile.php?id=<fbid>. , directs URL to facebook profile picture and no login is needed. Friends phone numbers as listed in their profile is also viewable. Other data of interest are Voicemail list, call log, SMS data, Notes' App data, Sync'd address book, Facebook App Data, Flightstats info etc., In some version, the passwords and other account details are stored in plain text. E.g. Tweetie and Dailyburn store passwords in plaintext. The tweetie's twitter account information is in the bplist format. Cookies information is also stored in bplist files.

6. Proposed methodology

Depending upon the gravity of the offense, there is an increase in need for using more than one technique to extract the data from idevices. In a hypothetical situation wherein a terrorist is using an idevice and the digital forensicators needs to extract artefacts from these devices as soon as they seize the items or if an abandoned idevice is found at the scene of crime then it is a requirement to check whether these devices are jailed or jailbroken. If they are jailed, currently limited options are available to extract. Commercial tools are only recently being developed. In this proposed methodology a framework is suggested to choose extraction of artefacts of forensic significance from idevices (jailed or jailbroken). The scenarios were created for test purpose and the results obtained are discussed. Attempt was made to extract evidence from both jailed and jailbroken iPhones as well as jailed iPad. For this purpose a combination of different applications and tools were used and the same are tabulated hereunder:

Table 7: Different applications tools

Application tools	Description
iTunes	To take Backup of Jailed iPhone
iFunbox	To take backup of Jailbroken iPhone
iPhone extractor	To extract the phone information
Sqlite browser	To extract the Sqlite databases such as address books, friends.db etc
Skypelog analyser	To extract the skype log, chat information
Windows calendar	To read the calendar information from the extracted database
Google maps	To track geoloction using the lat long coordinates
Belkasoft Forensic Studio	To perform image analysis (searches for images and lists out details of images and checks for pornographic images if any)
Nirsoft Skype analyser	Analyses skypelogs and displays chat log

The framework for idevices forensics is presented in

6.1 iFunbox

iFunbox is AppFile manager for iPhone, iPad and iPod Touch. First version of i-Funbox is released. Introduced are file permission editing and SSH terminal features which can be installed form cydia. Cydia is a software application for iOS that enables a user to find and install software packages on a jailbroken iPhone, iPod Touch or iPad.

6.2 How the idevices communicates with a computer?

idevices communicate through an interface called Apple File Communication Protocol(AFC). This protocol supports a framework called MobileDevice that is installed with iTunes that is default on Apple 's OS X. In order to install firmware upgrades, and to copy music and photos, the protocol uses USB port

and cable when it is connected to the computer. However, the protocol restricts access or communication with the entire iPhone memory area and is limited to few files only. Precisely, iTunes communicates with "jailed" or limited area of the memory, a backup is taken. However this backup is not that effective to extract information from raw devices which is essential to physical image. A slight modification has to be done to the filesystem to gain access into the raw device and get a true physical bitstream copy.

6.3 Jailbreaking

A jailed (chrootjail – borrowed from Linux lexicon) environment means that access to certain areas of memory are restricted. So iTunes accesses the idevices in a jailed environment. This prevents it from accessing the root level or administrative level. Some of the jailbreaks include the following:

- Pwnage
- Qwkpwn
- RedSn0w
- Yellowsn0w
- iLiberty
- Purplera1n
- Blackra1n
- Greenpois0n

All these circumvented the security measures of the idevice by either replacing OS with engineered user created firmware or just patching the kernel and or bootrom, which allows the device to run unsigned code.

Features such as file permissions, ownership and group information, a console for SSH terminal, Enhanced AppFastIn(tm) tech for stability and stop mounting, duplicated devices of iOS beta. If openSSH based feature is used, the ifunbox will promote for SSH password if it is not the default 'alpine'. iFunbox will record the password and, encrypted in
//var/mobile/Media/iFunbox_ssh_record.shadow for future use.

If the device is using the default password 'alpine', iFunbox will automatically modify it to some strong password to protect idevices from attack of malware and worms. It is also possible to manually change the password by 'passwd' command in the SSH terminal. Moreover, the iFunbox supports auto conversion when a binary plist is copied from idevice to PC, resulting in human readable text. It can also be disabled.

6.4 USB Tunnelling

USB tunnelling maps opens Transmission Control Protocol 'tcp' ports on idevices to pc allowing windows program on pc to communicate. Windows program on pc and daemon on iOS need not be aware of the existence of Tunnelling, instead they can communicate as if they are running on the same machine or a WiFi hotspot. Besides OpenSSH, iphone and iPad apps also have built in HTTP/FTP daemons that can be temporarily activated for exchange of files. iFunbox provides USB Tunnel for connecting web browser and FTP client on the PC to these application. The most usual route to use putty to the iphone with openSSH installed. It is advisable to change the root/mobile password after installing OpenSSH.
The first step is to backup the media by using copy to PC. SMS details will be available in
//var/mobile/Library/SMS
Contact list information will be available in
//var/mobile/Library/AddressBook
Step 3 Browse the Raw File System delete the folder iTunes_Control located in
//var/mobile/media/iTunes_Control

6.5 Geospatial location

Geospatial location data is a crucial information of forensic significance to identify a where the device was at a particular point of time. This helps in determining the probable location of the perpetrator during the commission of crime. This artefact is located in the maps application and is stored under the folder /library/Maps. There are three property lists,

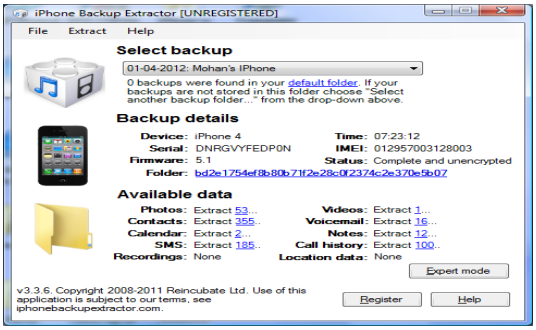
- History.plist
- Directions.plist
- Bookmark.plist

The query on history.plist will give the values for latitude and longitude. When this information retrieved is placed onto google map the location information can be obtained and the probable direction leading to the crime scene can be ascertained. For eg: the data of lat long

Lattitude : 36.160000
Longitude :76.360000

6.6 iPhone Extractor

The iPhone Backup Extractor works on windows (XP, Vista, 7), Mac OS X and Linux with iphone, iPad, iPhone 3G, iPhone 3GS, and Iphone backups from all versions of iTunes. It is capable of extracting contacts, pictures, call histories, MMS, SMS, text messages, video, voicemail, calendar entries, notes, app files, saved games, debug information and data that might be otherwise in accessible. It automatically converts the extracted database into CSV, VCard or ICAL formats, so they can be easily imported into excel, outlook or webmail. The following screen shot illustrates the iPhone Extractor showing the Mobile Equipment ID



It can convert consolidated data into a KML file for use with Google Earth. It also has a feature to extract the files from backups iTunes automatically makes for iPhone, iPad or iPodTouch. This can be used for forensic recovery even if the device is not available, the data from iTunes Backup could be used to recover the data from idevices which might be a clue of forensic significance. KML is an open standard officially names the OpenGIS (R) KML Encodeing Standard (OGC KML). It is maintained by Open Geospatial Consortitum, Inc.(OGC). KMO files can be created with google earth interface. KML is a file format used to display geographic data in an Earth browser such as Google Earth, Google Maps, and Google Maps for mobile. KML uses a tag-based structure with nested elements and attributes and is based on the XML standard. Geospatial information if any in the idevices can be interpreted.

6.7 Address Book artefact

Address book / contact information of the suspect and accomplices could be retrieved from extracting this database. The following screenshot illustrates the addressbook database extracted from jailbroken iPhone. Using this the details such as when a particular contact was saved, when it was modified etc could be ascertained. Here again the time format is in Mac absolute time. The time can be decoded by using tools such as decode and be interpreted in a format that is understandable. Addressbook information is once again stored in the Sqlite database format and can be extracted an viewed using sqlite database browser.

6.8 Calendar artefact

Calendar Events marked by a suspect can be located and retrieved from the idevices, which might be a clinching evidence in a case. The suspect might store information regarding whom he or she has to meet, where they should meet and what date and time? The screenshot below shows the meeting event information as retrieved from the backup of iPad.

6.9 Books Purchased

Certain books have been purchased online from appstore and certain books have been downloaded using a jailed iPad. The date when it was purchased and when it was downloaded can be ascertained by examining the artefact from the ibook database as read by sqlite browser. This artefact can aid in finding whether a copyright book is actually purchased or it has been downloaded. The date can also be ascertained. It will be in the form of Mac absolute time. Tools such as Decode could be used to convert the date to a readable format.

6.10 Bookmarks artefact

idevices could be used to browse the internet. If in case the user has bookmarked the web pages visited, then the details are stored in a database. This can be extracted and viewed in a sqlite browser. The following screenshot illustrates the bookmark artefact indicating the browsing habits of the suspect from a jailbroken iPhone.

7. Conclusion

Technological changes bring new challenges for digital forensicators. Foremost concern of digital evidence is locating evidentiary artefacts. A formalized approach is required in acquiring and analyzing the evidence from these new devices. In this study methods of examination of various artefacts of forensic significance are explored, a frame work of digital forensic process is suggested for acquisition in the case of jailed and jailbroken idevices (iPhone and iPad). In scenarios wherein miscreants, terrorists, copyright violation, data

leakage in corporate sector and other types of case depending upon the gravity of the offense, the proposed method could be used to retrieve evidentiary artefacts from idevices which poses a new challenge in digital forensic investigations.

Reference

1. Hoog, iPhone and iOS Forensics, Investigation, Analysis and Mobile security for Apple iPhone, iPad and iOS Devices, Ed. Robert Maxwell, Syngress publication, 2011.

2. Wired, iPhone timeline highlights the handset through the ages. Wired.com. Retrieved January 19, 2012, from http://www.wired.com/gadgetlab/2008/07/iphonetimeline/

3. Brothers, S. (2007). iPhone tool classification. The Apple examiner. Retrieved January 15, 2012, from http://www.appleexaminer.com/iPhoneiPad/ToolClassification/ToolCla ssification.html

4. Moren, D. (2010, July 26). Jailbreaking officially granted DMCA exemption. Macworld.Retrieved January 24, 2012, from http://www.macworld.com/article/152935/2010/07/jailbreak_exemption.html.jailbreak_exemption.html

5. Apple Inc. (2010). Mac OS X Lion Sneak Peek. Mac OS X Lion. Retrieved December 17, 2010, from www.apple.com/macosx/lion

6. NIJ http://www.nij.gov/pubs-sum/232383.htm Special Report 232383, Test Results for Mobile Phone Acquisition tool – Zdziarski's Method.

7. XRY - MSAB Release notes (29.03.2012) , MSABLabs.com visited on 29.03.2012.

8. Sean Morissey, iOS Forensic Analysis for iPhone, iPad, iPod Touch, APress Publication, page 40, 2010