

Forensic Acquisition of IOS Devices



Hyndavi Koganti, G Siva Nageswara Rao

Abstract: Apple devices are well known for their high-security features in terms of data storage. IOS devices have some restrictions for their usability. The device contains only internal memory and the users can back up their data into iCloud or iTunes. IOS devices are more secure when compared to other mobile devices. The IOS devices can also be jailbroken for the purpose of removing software restrictions and allows the installation of application from the unknown sources i.e., the app that are not unavailable in Apple App store. After jailbreaking, the device becomes vulnerable and lets the attacker to access the device. Apple provides both hardware and software patches to the vulnerabilities, which means many versions can't be jailbreak so easily. To perform Forensic investigation on the IOS devices, even the forensic investigators need privilege escalation to access the data of the device. The tools which are used to investigate IOS devices are avail as commercial. This project proposes an opensource method to access the IOS device using SSH shell. After the successful mount of device, the data can be acquired for further forensic analysis. Based on the artifacts analysed, the investigators can be able to find the root cause of the crime.

Keywords: iOS, plist, db files.

I. INTRODUCTION

IOS Introduction:

The first iPhone was formally launched and created accessible to the overall public in 2007, and this iPhone and was heralded noticeably at the Macworld of that exact same year. Throughout this first unhitch, the iPhone was accessible among the U. S. of America, UK, Canada, Germany, Norway, Sweden, Finland, France, Spain, European nation and African country. Jobs expressed his belief that pill PCs and ancient PDAs weren't wise choices as high-demand markets for Apple to enter, despite receiving many requests for Apple to create another personal digital assistant.

On January 9, 2007, Steve Jobs declared the first iPhone at the Macworld convention, receiving substantial media attention. Jobs declared that the first iPhone would be discharged later that year. On June 11, 2007, Apple declared at the Apple's Worldwide Developers Conference that the iPhone would support third-party applications pattern the campaign engine. Third parties would be able to turn out web 2.0 applications that

users could access via the net. Such applications appeared even before the discharge of the iPhone; the first of these, mentioned as One Trip, was a program meant to remain track of users' trying lists. On June 29, 2007, Apple discharged version seven.3 of iTunes to coincide with the discharge of iPhone. This unhitch contains support for iPhone service activation and syncing.

IOS Architecture:

iOS is an iPhone operating system and it was created by Apple for the devices which are manufactured in Apple like iPhone, iPad, iPod, etc. Just like other operating system iOS has an architecture and it is a layered architecture.

In iOS architecture there are four different layers and these layers works as intermediate layer between the application and the hardware because the application and the hardware do not communicate each other directly. In this architecture a lower layer provides a normal service and the higher layer provides GUI services.

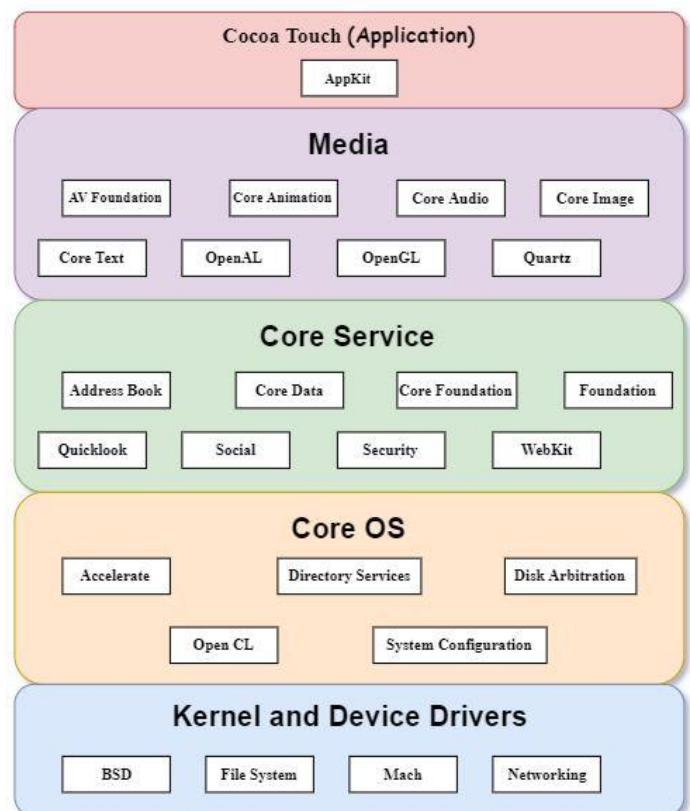


Figure 1: Architecture of iOS

1. Cocoa Touch Layer

The Cocoa bit layer is primarily answerable for the looks of apps. It provides access to main system functions like Contacts, Camera, bit input, shares with different apps, push notifications etc.



Manuscript published on November 30, 2019.

* Correspondence Author

Hyndavi Koganti*, M.Tech - Cyber Security and Digital Forensics, Department of CSE, KLEF, Vaddeswaram, A.P, India. Email: hyndavikoganti@gmail.com

Dr Siva Nageswara Rao, Associate Professor, Department of CSE, KLEF, Vaddeswaram, A.P, India.. Email: sivanags@kluniversity.in

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](https://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

Event Kit framework: This framework is an interface which helps to see and perform the operations related to the calendar.

Game Kit Framework: This framework helps to implement the support to the game centre to share the game related information in online.

iAd Framework: This framework helps and allows to deliver advertisements from application which based on a banner.

Map Kit Framework: This framework gives a scrollable map and that map can also be included into user interface of an application.

Push Kit Framework: This framework will provide a registration support for the application which support VoIP.

Twitter Framework: This framework is an UI which supports to generate tweets and also for creating URLs to access the services provided by Twitter.

UI Kit Framework: This framework is a vital infrastructure to applying any graphical and event-driven applications in iOS. And it has some important functions like multitasking, application management and infrastructure, cut, copy and paste operations and also supports touch and motion events.

2. Media Layer

The Media layer assist you to include second and 3D graphics, animations, image effects, and professional-grade audio and video functionalities into your mobile app.

Graphics Framework:

UI Kit Graphics: This helps to describe the higher-level support for the images which are designed and also for animated images to the content.

Core Graphics framework: This framework is a drawing engine for applications in iOS and it supports 2D vectors and images which are based on rendering.

Core Animation: This framework is an initial technology which optimizes the animation of application.

Core Images: This framework provides an advanced support to control video and motionless images and makes sure that the controlling the images in a non-destructive way.

Open GL ES and GL Kit: This framework is an interface which was accelerated by hardware to manage 2D and 3D rendering.

Metal: This offers a very low overhead access to A7. And also permits to perform sophisticated graphics rendering and computation works in a high level.

Audio Framework:

Media Player Framework: This framework is one of the high-level frameworks and it gives and supports to easy use and access to iTunes library and playing playlist.

AV Foundation: This is an objective interface which handles the recordings and playbacks of audios and videos in the device.

Open AL: This framework is used to provide audio and it is a standard technology from the industry.

Video Framework:

AV Kit: This framework provides collection of user interfaces which are easy to present video.

AV Foundation: This framework provides an advanced capability for recording and video playback.

Core Media: This framework is used to describe the low-level interfaces and to describe data types for operating media.

3. Core Services

The Core Services layer comprises core services like address book, Security, Social and foundation which offer essential options to apps. It offers access to basic resources required for app.

Address book framework: This framework give access to a database which consists the contacts of the user in a programmatically way.

Cloud Kit framework: This framework provides a medium which helps to move data between the user app and iCloud.

Core data Framework: This framework is a technology which manages the Model View Control application's data model.

Core Foundation framework: This framework is an interface which gives fundamental data and service features to the application in iOS.

Core Location framework: This framework gives the information about geographical location and heading information of the applications.

Core Motion Framework: This framework can able to access the data which work based on motion of the device. Using this framework can also be able to access the information which works based on accelerometer.

Foundation Framework: This framework consists the features which were programmed through objective C.

Health kit framework: This framework consists and handles the health-related information of user.

Home kit framework: This framework can able to access the devices which are connected in the user's house.

Social framework: It is an interface for accessing the user social media accounts.

Store Kit framework: This framework supports for buying content and services from inside of iOS apps. Simply it is known as In-App Purchase.

4. Core OS

The Core OS layer comprises technologies and frameworks which offer low-level services associated with low-level hardware and networks. Core OS is the bottom layer and it work just like a foundation to iOS and maintains the other layers on the top of this layer properly. This layer is responsible for memory operations after completion of application like managing, allocating, releasing memory and takes care of the tasks of file systems, and other tasks in OS, and this layer can directly interact with hardware easily.

5. Kernel and Device Drivers

This is very cheap layer of iOS that in the main includes the kernel and device drivers. The kernel atmosphere is constructed on prime of Ernst Mach three.0 (a microkernel that replaces the kernel within the BSD version of Unix) and provides superior networking facilities and support for multiple, integrated file systems.

II. LITERATURE REVIEW

Mobile Forensics is the process of extracting Electronic or Digital evidence from mobile devices under Forensic conditions. These include iPad, iPhone, Smartphones, etc. While performing a forensic investigation, the forensic experts examine the evidence systematically with utmost careful so that evidence will not be modified or damaged.

The investigators will analyse only the particular data related to the case using forensic tools. The extracted data could be application files, SQLite database files, or keychains.

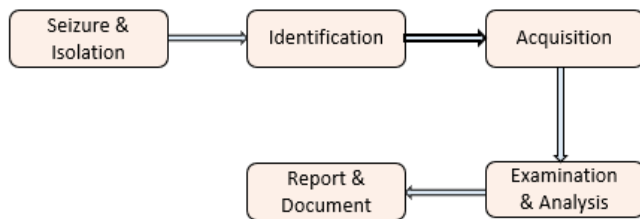


Figure 2: Data Extraction Phases

Seizure & Isolation:

The device should be disconnected from all the network and flight mode must be activated to avoid further communication to the device.

The device must be placed in the Faraday bag to prevent data tampering.

The simcard and memory card should be ejected.

Identification:

In what place does the mobile was identified?

What is the state of the mobile when available?

What data need to be extracted from the device?

Acquisition:

SSH connection should be established between the iPhone and computer to the same local network to maintain data integrity.

The backup of iPhone should be collected.

The passcode needs to be bypassed if passcode is present.

The Application files, SQLite database files, ktx files, etc will be collected and stored.

Examination & Analysis:

The plist files, db files, ktx files will be analysed by using forensic tools and the data is extracted.

The deleted data will be recovered for evidence examination.

Report & Document:

The detailed document of the entire procedure, methods, tools used, the data retrieved will be prepared by the examiners which is a report as well as evidence.

The way to extract the complete data from the mobile device is by using Commercial Forensic tools. The other way of extracting data is possible with the help of jail breaking the device.

Jail breaking is the process of removing software limitations which are obtruded by Apple and performed on iOS devices to gain and attain the privilege escalation of the device. After jailbroken, the device will be ready to access all the data and collect the evidence which can be used in forensic examination.

III. APPLICATION STRUCTURE

IOS Application Structure:

Each and every iOS application operates in its own sandbox.

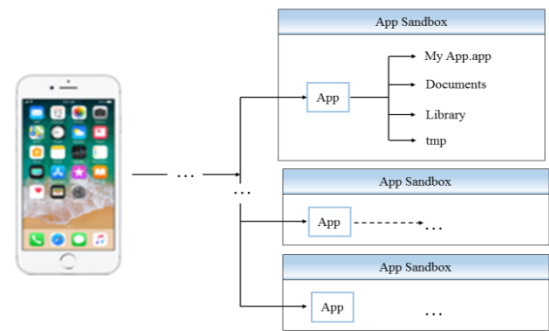


Figure 3: iOS Application Structure

Exception cases:

1. The public system interfaces like contacts, calendars, photo library.
2. Any application can use these interfaces provided when the user approves its access.

iOS Standard Directories:

- /AppName.app: This directory contains the app itself.
- /Documents: This directory stores user documents and data files of applications.
- /Documents/Inbox: This directory is used to read and delete files but it cannot create or write to the files which already exist.
- /Library: This is the top-level directory which contains files but not data files and it is used to create sub directories.
- /tmp: This directory is used to write temporary files that do not persist between the app launched. The files should be removed when they are no longer needed.

IV. DATA ACQUISITION PROCESS

Data Acquisition is the process of imaging the electronic evidence for examining the data present in the device. Extracting information from mobile device is not so easy.

Types:

1. Physical Acquisition:

It is the method which makes a bit-by-bit duplicate of a whole file system, comparable to approach taken in computer forensic examinations.

2. Logical Acquisition:

It is the method of extracting the logical storage objects which resides on the filesystem.

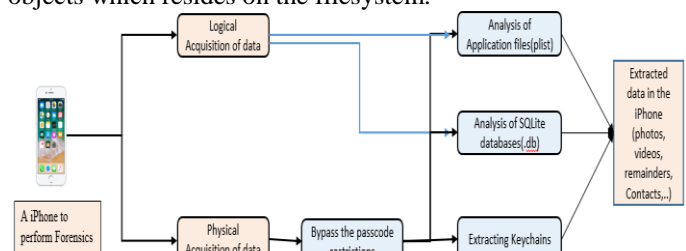


Figure 4: A visual architecture of my proposed mode

After the device is brought to perform forensic investigation, the data can be extracted either in the form of Physical or Logical acquisition methods. If there is passcode restriction, then bypass should be done to read the encrypted file system. Different types of file systems like plist(property list) files, SQLite (.db) Database files, Keychains(a database which stores sensitive information and encrypted with hardware key) will be present. Using different forensic tools, data in iPhone will be extracted.

V. PROPOSED METHODOLOGY

The IOS devices possess the potential shreds of evidences, which are acquired and analyzed for the forensic investigation.

This project proposes an open source approach to perform the forensic analysis of the IOS device. The device can be accessed through the Shell as it has linux kernel. The root of the device is accessed by using SSH shell and the data available in the storage is acquired for further forensic analysis.

The device can be accessed using the IP address of the mobile device through SSH port. Mobile devices store the system data, application data in the database file format. So to analyze the artifacts, those .db files or sqlite files and plist files are acquired. After gaining the shell access to the device, important artifacts like contacts, SMS, media etc., can be extracted.

In order to mitigate the cost effectiveness of existing system and to find artifacts in iPhone for forensics purpose, an open-source approach is designed.

VI. DATA ANALYSIS

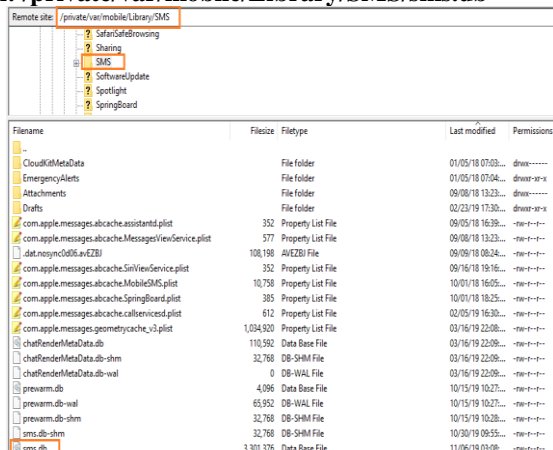
Artifacts Extraction & Analysis

A piece of data that relevant to digital forensic investigation.

SMS: It is used for offline communication to send and receive message.

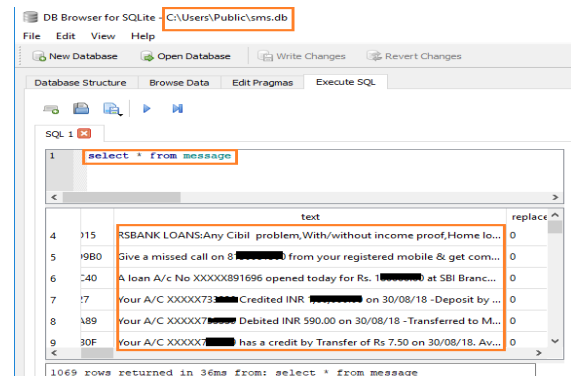
Sms.db: This database file which contains information about sent and received messages. The query used to extract the data is “select * from message.”

Path: /private/var/mobile/Library/SMS/sms.db



Filename	Filesize	Filetype	Last modified	Permissions
CloudKitMetadata		File folder	01/05/18 07:09...	drwxr-xr-x
EmergencyAlerts		File folder	01/05/18 07:04...	drwxr-xr-x
Attachments		File folder	09/08/18 13:23...	drwxr-xr-x
Drafts		File folder	02/23/19 17:30...	drwxr-xr-x
com.apple.messages.assistant.plist	352	Property List File	09/08/18 16:39...	-rw-r--r--
com.apple.messages.assistant.plist	577	Property List File	09/08/18 13:23...	-rw-r--r--
dat.noencyclib.anE2B1	108,198	AV/EBU File	09/08/18 08:24...	-rw-r--r--
com.apple.messages.assistant.plist	352	Property List File	09/16/18 19:16...	-rw-r--r--
com.apple.messages.assistant.plist	10,750	Property List File	10/01/18 16:05...	-rw-r--r--
com.apple.messages.assistant.plist	395	Property List File	10/01/18 16:25...	-rw-r--r--
com.apple.messages.assistant.plist	612	Property List File	02/06/19 16:30...	-rw-r--r--
com.apple.messages.assistant.plist	1,034,920	Property List File	03/16/19 22:08...	-rw-r--r--
chatRenderMetadata.db	110,592	Data Base File	03/16/19 22:08...	-rw-r--r--
chatRenderMetadata.db-shm	32,768	DB-SHM File	03/16/19 22:08...	-rw-r--r--
chatRenderMetadata.db-wal	0	DB-WAL File	03/16/19 22:08...	-rw-r--r--
prewarm.db	4,096	Data Base File	10/15/19 10:27...	-rw-r--r--
prewarm.db-wal	65,952	DB-WAL File	10/15/19 10:27...	-rw-r--r--
prewarm.db-shm	32,768	DB-SHM File	10/15/19 10:28...	-rw-r--r--
sms.db	32,768	DB-SHM File	10/30/19 09:55...	-rw-r--r--
sms.db-shm	3,301,376	Data Base File	11/06/19 03:08...	-rw-r--r--

Figure 5: SMS Path



The screenshot shows the DB Browser for SQLite interface. The file path is C:\Users\Public\sms.db. The query 'select * from message' is entered in the SQL editor. The results are displayed in a table with 9 rows and 3 columns: an index, a text column, and a replace column.

	text	replace
4	115 RSBANK LOANS: Any Cibil problem, With/without income proof, Home lo...	0
5	980 Give a missed call on 8 [REDACTED] from your registered mobile & get com...	0
6	240 A loan A/c No XXXXX891696 opened today for Rs. 1 [REDACTED] at SBI Branc...	0
7	17 Your A/C XXXXX73 [REDACTED] Credited INR [REDACTED] on 30/08/18 - Deposit by ...	0
8	489 Your A/C XXXXX7 [REDACTED] Debited INR 590.00 on 30/08/18 - Transferred to M...	0
9	30F Your A/C XXXXX [REDACTED] has a credit by Transfer of Rs 7.50 on 30/08/18. Av...	0

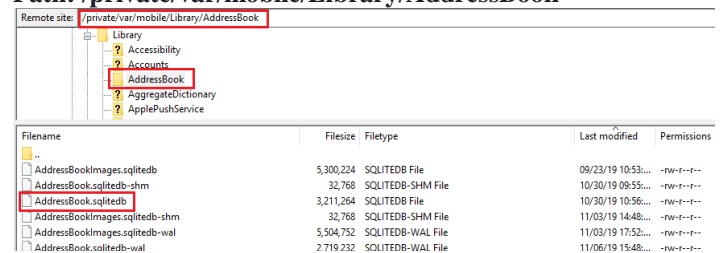
1069 rows returned in 36ms from: select * from message

Figure 6: Data extracted from sms.db

Contacts: The entity which is created for identifying other person.

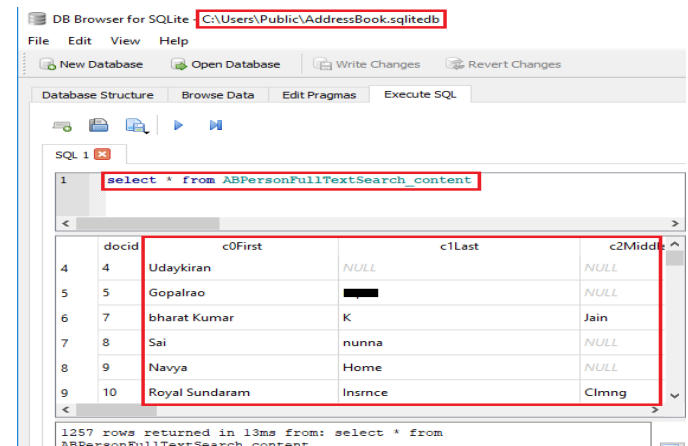
AddressBook.sqlitedb: This database file contains identify of persons which includes mail, Home, multiple storage of numbers. The query used to extract the data is “select * from ABPersonFullTextSearch_content”

Path: /private/var/mobile/Library/AddressBook



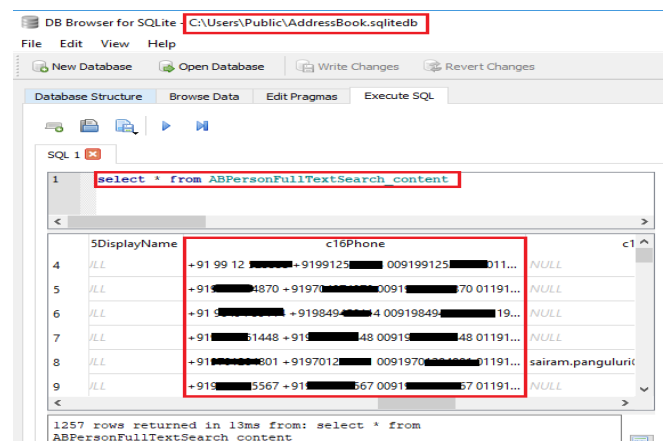
Filename	Filesize	Filetype	Last modified	Permissions
AddressBookImages.sqlitedb	5,300,224	SQLITEDB File	09/23/19 10:53...	-rw-r--r--
AddressBookImages.sqlitedb-shm	32,768	SQLITEDB-SHM File	10/30/19 09:55...	-rw-r--r--
AddressBook.sqlitedb	3,211,264	SQLITEDB File	10/30/19 10:56...	-rw-r--r--
AddressBookImages.sqlitedb-shm	32,768	SQLITEDB-SHM File	11/03/19 14:48...	-rw-r--r--
AddressBookImages.sqlitedb-wal	5,504,752	SQLITEDB-WAL File	11/03/19 17:52...	-rw-r--r--
AddressBook.sqlitedb-wal	2,719,232	SQLITEDB-WAL File	11/06/19 15:48...	-rw-r--r--

Figure 7: Contacts Path



	docid	c0First	c1Last	c2Middle
4	4	Udaykiran	NULL	NULL
5	5	Gopalrao	NULL	NULL
6	7	bharat Kumar	K	Jain
7	8	Sai	nunna	NULL
8	9	Navya	Home	NULL
9	10	Royal Sundaram	Insrnce	Cimng

Figure 8: Contact names from AddressBook.sqlitedb



	SDisplay Name	c16Phone	c1
4	ILL	+91 99 12 [REDACTED] +9199125 [REDACTED] 009199125 [REDACTED] 011...	NULL
5	ILL	+91 [REDACTED] 4870 +91970 [REDACTED] 0091 [REDACTED] 70 01191...	NULL
6	ILL	+91 [REDACTED] [REDACTED] +919849 [REDACTED] 4 00919849 [REDACTED] 19...	NULL
7	ILL	+91 [REDACTED] 1448 +91 [REDACTED] 48 0091 [REDACTED] 48 01191...	NULL
8	ILL	+91 [REDACTED] 301 +9197012 [REDACTED] 0091970 [REDACTED] 01191...	sairam.panguluric
9	ILL	+91 [REDACTED] 5567 +91 [REDACTED] 667 0091 [REDACTED] 67 01191...	NULL

Figure 9: Contact Numbers from AddressBook.sqlitedb

Call Logs: It contains the statistical record information of owner calls in the form of logs.

CallHistory.storedata: This database file contains information about the call statistical record and Timings, Location, Duration. The query used to extract the data is “select * from ZCALLRECORD”

Path: /private/var/mobile/Library/CallHistoryDB

Filename	Filesize	Filetype	Last modified	Permissions
CallHistoryTemp.storedata	94,208	STOREDATA File	03/16/19 22:08...	-rwxr-xr-x
CallHistoryTemp.storedata-wal	0	STOREDATA-WAL File	03/16/19 22:08...	-rwxr-xr-x
CallHistory.storedata	4,067,328	STOREDATA File	03/16/19 18:59...	-rwxr-xr-x
CallHistory.storedata-shm	32,768	STOREDATA-SHM File	10/30/19 08:55...	-rwxr-xr-x
CallHistory.storedata-wal	127,752	STOREDATA-WAL File	10/30/19 12:01...	-rwxr-xr-x
com.apple.callhistory.databaseinfo.plist	298	Property List File	10/30/19 12:01...	-rwxr-xr-x
CallHistoryTemp.storedata-shm	32,768	STOREDATA-SHM File	11/07/19 08:34...	-rwxr-xr-x

Figure 10: Call Logs path

ARTICIPANTUID	ZADDRESS	ZLOCAL_ADDR
28 O	+9163019...	NULL
29 O	+918074...	NULL
30 O	+91988...	NULL
31 O	+91824...	NULL
32 O	+91824...	NULL
33 O	+919885...	NULL

Figure 11: Phone Logs retrieved successfully

Accounts: It contains information about the device and its account holder.

data_ark.plist: This property list file contains information about the name of the system the last iTunes backup was taken and also the details of the iPhone.

Path:

/private/var/root/Library/Lockdown/data_ark.plist

Filename	Filesize	Filetype	Last modified	Permissions
escrow_records		File folder	10/30/19 08:41...	-rwxr-xr-x
pair_records		File folder	10/30/19 08:41...	-rwxr-xr-x
data_ark.plist	1,057	Property List File	10/30/19 10:12...	-rwxr-xr-x

Figure 12: Accounts Path

Key	Type	Value
Root	dict	
com.apple.mobile.restriction-f	boolean	false
com.apple.international-Lang	string	en-IN
com.apple.mobile.iTunes-iTur	boolean	true
com.apple.iTunes.backup-Last	string	PC
com.apple.mobile.restriction-f	boolean	false
-UseRaptorCerts	boolean	true
-DarkProductVersion	string	12.1.2
-ActivationStateAcknowledge	boolean	true
-TimeZone	string	Asia/Calcutta
-HasSiDP	boolean	true
com.apple.mobile.data_sync-c	dict	
-ProtocolVersion	string	2
com.apple.mobile.data_sync-l	dict	
com.apple.mobile.wireless_loc	boolean	false
com.apple.international-Local	string	en-IN
com.apple.iTunes.backup-Last	string	DESKTOP-P6QD3BC
-DeviceName	string	koganti's iPhone
-TimeIntervalSince1970	integer	1568612790
com.apple.mobile.data_sync-c	dict	

Figure 13: Device information from plist file

Photos: It contains user photos which are built via camera, screenshots and WhatsApp.

Path: /private/var/mobile/DCIM/

Figure 14 Photos path id

Filename	Filesize	Filetype	Last modified	Permissions
MISC		File folder	12/26/18 02:05...	-rwxr-xr-x
100APPLE		File folder	01/06/19 13:33...	-rwxr-xr-x
101APPLE		File folder	06/29/19 10:42...	-rwxr-xr-x
102APPLE		File folder	06/29/19 10:42...	-rwxr-xr-x
103APPLE		File folder	06/29/19 10:42...	-rwxr-xr-x
104APPLE		File folder	10/30/19 13:47...	-rwxr-xr-x

entified successfully

Filename	Filesize	Filetype	Last modified	Permissions
IMG_2009.HEIC	642,975	HEIC File	12/22/18 15:36...	-rwxr-xr-x
IMG_2016.JPG	171,720	JPG File	12/23/18 11:24...	-rwxr-xr-x
IMG_2017.HEIC	1,280,404	HEIC File	12/23/18 13:37...	-rwxr-xr-x
IMG_2018.HEIC	1,204,039	HEIC File	12/23/18 13:37...	-rwxr-xr-x
IMG_2019.JPG	85,921	JPG File	12/23/18 14:41...	-rwxr-xr-x
IMG_2020.JPG	157,002	JPG File	12/23/18 14:41...	-rwxr-xr-x
IMG_2021.JPG	130,456	JPG File	12/23/18 14:41...	-rwxr-xr-x
IMG_2022.JPG	158,119	JPG File	12/23/18 14:41...	-rwxr-xr-x
IMG_2023.JPG	180,863	JPG File	12/23/18 14:42...	-rwxr-xr-x
IMG_2026.JPG	109,940	JPG File	12/23/18 15:37...	-rwxr-xr-x
IMG_2754.JPG	168,082	JPG File	12/23/18 20:16...	-rwxr-xr-x
IMG_2037.JPG	35,152	JPG File	12/24/18 12:25...	-rwxr-xr-x
IMG_2039.JPG	181,076	JPG File	12/24/18 12:53...	-rwxr-xr-x
IMG_2040.JPG	209,831	JPG File	12/24/18 13:18...	-rwxr-xr-x
IMG_2041.JPG	162,456	JPG File	12/24/18 13:19...	-rwxr-xr-x
IMG_2042.JPG	168,939	JPG File	12/24/18 13:19...	-rwxr-xr-x
IMG_2047.JPG	47,155	JPG File	12/24/18 17:57...	-rwxr-xr-x

Figure 15 Images are successfully extracted

Passwords: These are used to secure the device or applications and sensitive data. Keychain-2.db file contains data which will be in encrypted form. The query used to extract the data is “select * from synckeys”

Path : /private/var/Keychains

Filename	Filesize	Filetype	Last modified	Permissions
Analytics		File folder	10/30/19 01:22...	-rwxr-xr-x
SupplementalAssets		File folder	09/30/19 13:30...	-rwxr-xr-x
cdts		File folder	11/05/19 17:12...	-rwxr-xr-x
cdts.db	20,480	Data Base File	08/27/19 16:58...	-rwxr-xr-x
com.apple.archive.sqlite3	32,768	SQLite3 File	01/10/19 18:03...	-rwxr-xr-x
com.apple.archive.sqlite3-wal	81,805	SQLite3 File	08/14/19 22:16...	-rwxr-xr-x
cdts.db-wal	32,768	DB-WAL File	10/15/19 08:38...	-rwxr-xr-x
TrustStore.sqlite3	16,384	SQLite3 File	10/17/19 11:50...	-rwxr-xr-x
keychain-2.db-shm	32,768	DB-SHM File	10/30/19 08:55...	-rwxr-xr-x
com.apple.archive.sqlite3-shm	32,768	SQLite3-SHM File	10/30/19 08:55...	-rwxr-xr-x
keychain-ota-backup.plist	883,311	Property List File	10/31/19 08:27...	-rwxr-xr-x
com.apple.archive.sqlite3	53,248	SQLite3 File	11/03/19 17:52...	-rwxr-xr-x
com.apple.archive.sqlite3-wal	593,312	SQLite3-WAL File	11/07/19 08:35...	-rwxr-xr-x
keychain-2.db	5,965,472	Data Base File	11/07/19 08:48...	-rwxr-xr-x

Figure 16: Passwords stored path is identified successfully

ckzone	UUID	keyclass	currentkey
13 AutoUnlock	7C9F65DC-9652-4CE1-8FFB-9B80582E532E	classC	1 DD1C9522-
14 AutoUnlock	DD1C9522-8660-4BA1-BC70-AAB7EF248AD8	tlk	0 DD1C9522-
15 AutoUnlock	B2B09CC4-7DCA-4B7F-A0E8-76772C27F3C3	classA	1 DD1C9522-
16 Health	9B6DA781-CF8D-40EF-9048-B37FD8365E85	classA	1 20631229-t
17 Health	EBCBE88A-B411-4584-AA4B-9C24B108BC3C	classC	1 20631229-t
18 Health	20631229-6A8D-459F-9515-C5DBD9D71606	tlk	0 20631229-t

Figure 17: Password data extracted successfully

Forensic Acquisition of IOS Devices

Third party applications:

These are the applications which are provided by vendors other than Manufacturers. iOS contains AppStore to install Applications onto the devices by secure authentication either to provide Apple password or finger access. The Names of the applications in the path are dynamic which means whenever it is newly connected for forensic purpose the names will be modified but not the data.

Path: /private/var/mobile/Containers/Data/Application

Filename	Filesize	Filetype	Last modified	Permissions
41479A6C-8064-485B-F8B3-8EADFE79415C		File folder	01/05/18 07:03	drwxr-xr-x
7319B8AF-170D-4518-8C6C-90C8B5735C87		File folder	01/05/18 07:03	drwxr-xr-x
E3E91617-5D18-4E30-86D5-30532672329C		File folder	01/05/18 07:03	drwxr-xr-x
FBF8535E-2D7C-4417-909E-07F9C320A5A6		File folder	01/05/18 07:03	drwxr-xr-x
F1071866-C740-433A-A0B9-0EE846E8203A		File folder	01/05/18 07:03	drwxr-xr-x
9743F6E2-88F7-4874-B0D5-0EE61CC0CD53		File folder	01/05/18 07:03	drwxr-xr-x
9743F6EE-6FC9-46AD-AC02-56E788CFAEAC		File folder	01/05/18 07:03	drwxr-xr-x
A8D6FCDA-1683-4543-83B7-F5006E338148		File folder	01/05/18 07:03	drwxr-xr-x
AA3A203A-2687-4DE6-BD51-F38A70BA4244		File folder	01/05/18 07:03	drwxr-xr-x
AFB022AD-5C1F-4002-A659-0848059243C1		File folder	01/05/18 07:03	drwxr-xr-x
B972049E-F00D-4D47-38C2-3A0C39C10237		File folder	01/05/18 07:03	drwxr-xr-x
CAC4BA8AE-6192-4CDA-8A26-788080794882		File folder	01/05/18 07:03	drwxr-xr-x
6C582C2E-C898-4AD8-92F9-167D978B78A4		File folder	01/05/18 07:03	drwxr-xr-x
DE8D8181-C451-4280-AC90-10894A66A538		File folder	01/05/18 07:03	drwxr-xr-x

Figure 18: Vendor Applications Path

WhatsApp: It is a free messaging App which allows users to communicate and share data (photos, videos, GIF, Document, Location, Contacts, Voice Messages) with the help of Internet.

ChatMedia Folder contains media and status of different users.

Path:

/private/var/mobile/Containers/Data/Application/5E66E731-D1DA-4DE5-BC1C-127B44C00332/Library/Caches/ChatMedia

Remote site					
/private/var/mobile/Containers/Data/Application/5686731-DIDA-4DE5-BC1C-127B4AC0332/Library/Caches/ChatMedia					
	ChatMedia				
	? 12962670304@status				
	? 12962670304-1559876945@g.us				
	? 15103207999@status				
	? 19167902129-1460591226@g.us				
	? 19738@s.whatsapp.net				
	? 19738@status				
	? 91[redacted]951@s.whatsapp.net				
	? 91[redacted]951@s.whatsapp.net				
	? 91[redacted]951@status				
	? 91[redacted]76088@status				
	[redacted]				

Filename	Filesize	FileType	Last modified	Permission
91[redacted]927@s.whatsapp.net		File folder	08/27/18 15:58:	dwxon-n-x
91[redacted]928@s.whatsapp.net		File folder	08/28/18 07:51:	dwxon-n-x
91[redacted]200@s.whatsapp.net		File folder	08/29/18 09:52:	dwxon-n-x
91[redacted]44@s.whatsapp.net		File folder	08/30/18 08:26:	dwxon-n-x
91[redacted]928@status		File folder	08/31/18 07:18:	dwxon-n-x
91[redacted]4@s.whatsao.net		File folder	08/31/18 18:07:	dwxon-n-x

Figure 19: WhatsApp path

Remote site: /private/var/mobile/Containers/Data/Application/5666E731-D1DA-4DE3-BC1C-127844C00332/Library/Caches/ChatMedia/...@s.whatsapp.net

? 911...6320@status

911...6020@s.whatsapp.net

? 911...6020@status

? 911...35979@s.whatsapp.net

Filename	Filesize	Filetype	Last modified	Permissions	Owner
..					
3a573165-2690-4640-8674-9109eb043ff.jpg	88,332	JPG File	08/29/18 09:52...	-rw-r--r--	m...
a29a940f-cf49-48b6-bde7-af969563d4ff.jpg	86,105	JPG File	08/29/18 09:52...	-rw-r--r--	m...

Figure 20: Data of One Person

Name	Date modified	Type
.com.apple.mobile_container_manager....	15-10-2019 14:42	Property List File
.mboxCache	15-10-2019 10:23	Property List File
2	15-10-2019 16:20	PNG File
3a573165-2690-4640-8674-9189eb0f43ff	07-11-2019 14:56	JPG File
5b7d55b02b6d7e28c98fccc-e-0	15-10-2019 16:12	PNG File
5b7d55b02b6d7e28c98fccc-e-2	15-10-2019 16:12	PNG File

Figure 21: Extracted data of WhatsApp


Facebook: This is a free, cross-platform application which allows different people to make friends, to follow people,

messaging, sharing images, and comment on photos or posts.

Recent_activites_notifications.txt file contains list of notifications received or popped-up.

Path:

/private/var/mobile/Containers/Data/Application/E0DB4DD7-7175-4153-AFBD-218A1C2CB5CA/Library/Caches



Filename	Filesize	Filetype	Last modified	Permissions
media_publishing_info_cache.24E27679-EAFD-461C-8EED-E...		File folder	07/02/19 23:43...	dneer-a-x
dod_storage_cache.24E27679-EAFD-461C-8EED-E68C6CF4D...		File folder	07/02/19 23:43...	dneer-a-x
inspiration_voyagebit_frame_cache.24E27679-EAFD-461C-8E...		File folder	07/02/19 23:43...	dneer-a-x
dod_metadata		File folder	07/02/19 23:43...	dneer-a-x
compactdisk_bash		File folder	07/02/19 23:43...	dneer-a-x
fbquick-fizz-store	2	STORE File	06/28/19 22:31...	-----
WhistleTt-store	2	STORE File	06/28/19 22:36...	-----
fbastic-store	2	STORE File	06/28/19 12:51...	-----
fb_an_config.plist	2,373	Property List File	10/10/19 22:39...	-----
composer_ras	500	File	11/05/18 17:27...	-----
recent_activities_friending.it	6,945	Text Document	11/05/18 11:32...	-----
recent_activities_notifications.it	106,425	Text Document	11/05/18 11:20...	-----
ZeroToken.dat	1,571	DAT File	12/16/18 23:49...	-----
gck_nearby_devices.plist	281	Property List File	02/18/19 18:14...	-----

Figure 22: Facebook Path and data

Instagram: This Application is used to follow the activities or posts and send messages to different people.

Path:

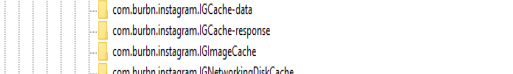
```
/private/var/mobile/Containers/Data/Application/EA14A
BB2-EFDB-4F9F-8E0B-A1D550590E22/Library/Caches
```

Figure 23: Cache Information

Path:

```
/private/var/mobile/Containers/Data/Application/EA14A
BB2-EFDB-4F9F-8E0B-
A1D550590E22/Library/Caches/Snapshots/com.burbn.in
stagram
```

Remote site: /private/var/mobile/Containers/Data/Application/EA144B82-4FDB-4F9F-8E0B-A1D55059E22/Library/Caches/Snapshots/com.burbin.instagram



com.burbin.instagram.IGCache-data
com.burbin.instagram.IGCache-response
com.burbin.instagram.IGImageCache
com.burbin.instagram.IGNetworkingDiskCache
Snapshots
com.burbin.instagram
Preferences
SyncedPreferences
StoreKit

Filename	Filesize	Filetype	Last modified	Permissions
..				
downloaded		File folder	10/17/19 15:14...	drwxr-xr-x
6F19A948-DD3B-44A9-B105-BC04FEC9643D@3x.ktx	7,461	KTX File	03/05/19 10:59...	-rw-r--r--
987122EE-89ED-4F18-8DE1-467430209350@3x.ktx	194,712	KTX File	10/17/19 15:14...	-rw-r--r--

Figure 24: Data Identified

SBI YONO: This Mobile Application of SBI is used to perform monetary transactions, view account balance and place check book requests for bank.

Path:

/private/var/mobile/Containers/Data/Application/0CB96E66-E635-4654-99C8-051168ADD772/Documents/Inbox

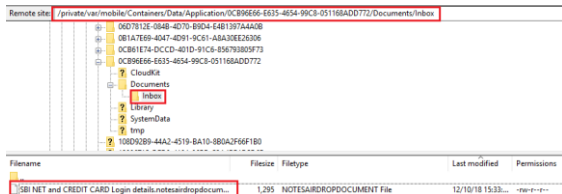


Figure 25: SBI YONO Path

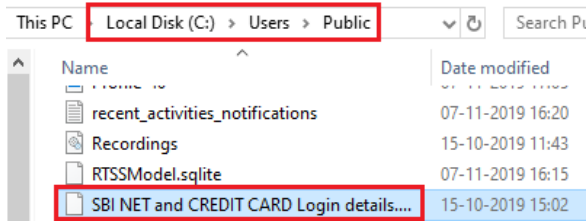


Figure 26: Information extracted

Axisbank: This Mobile Application of AXIS bank is used to transfer money from one account to another account with the help of account numbers, IFSC Code.

Path:

/private/var/mobile/Containers/Data/Application/6C7CC94-0854-476B-AC2E-474024841254/Documents

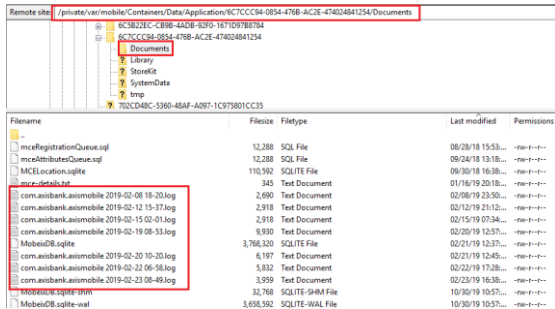


Figure 27: AXIS Bank path and log files

Flipkart: This Shopping Application is used to know the list of items which are searched by user and purchased. The information is stored in flipkart.sqlite.

The query used to extract the data is “select * from ZCROSSPLATFORMCACHE”

Path:

/private/var/mobile/Containers/Data/Application/C0E87A33-ABB6-480C-8BFE-DA2F78443F8E/Library

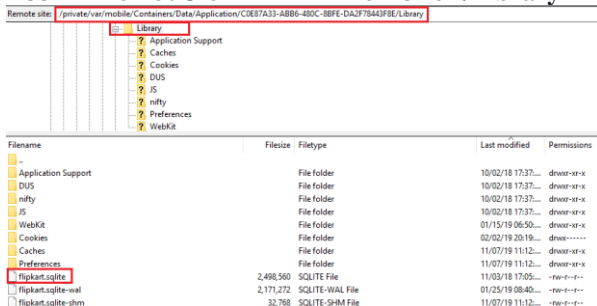


Figure 28: Flipkart Path

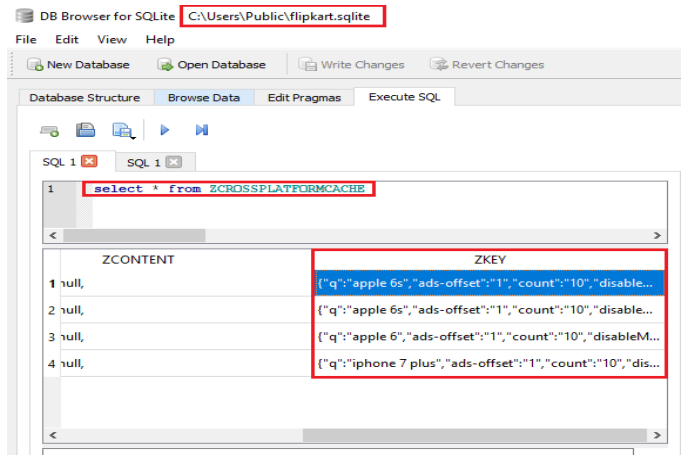


Figure 29: Searched Data of Flipkart

BookMyShow: This Entertainment App is used for checking Movies List, Date and Location for which the user has browsed.

Path:

/private/var/mobile/Containers/Data/Application/91AFD7FD-D91A-4363-BFF7-09B12F36D9FB/Library/Caches

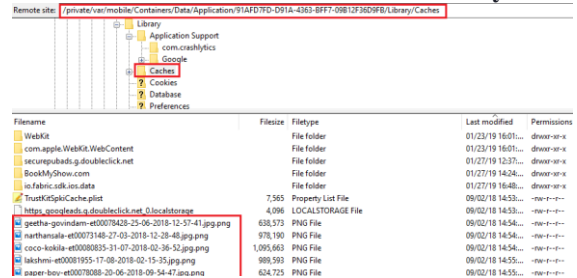


Figure 30: BookMyShow Path and Browsed Information

HPPrinter: This Application is used for printing documents or scanning Applications. Inbox folder contains the list of documents user has taken printout.

Path:

/private/var/mobile/Containers/Data/Application/06D7812E-084B-4D70-B9D4-E4B1397A4A0B/Documents/Inbox

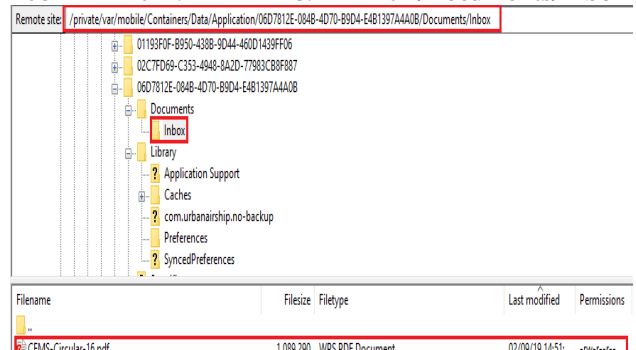


Figure 31: HP Printer Data and Path

FindMyiPhone: This Application is used in iPhones to find the location of the iPhone if the mobile is lost or missing. It requires internet connection and Location needs to be turned on.

FMIP.sqlite folder contains the locations of iPhone.

Path:

/private/var/mobile/Containers/Data/Application/6C5B22EC-CB9B-4ADB-92F0-1671D97B8784/Documents

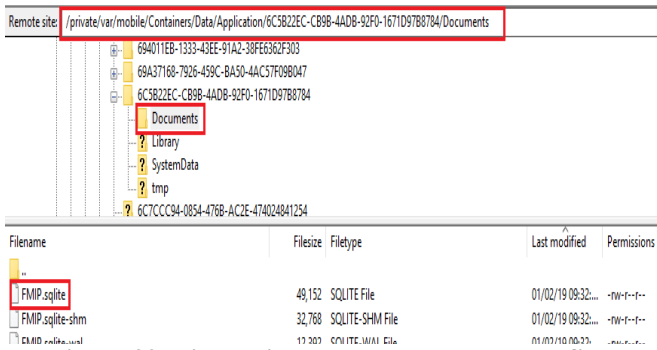


Figure 32: FindMyiPhone Path and database file

Google Maps: This route-map Application is used to find the Locations which are used by the user for travelling or searched.

Com.google.Maps.plist file contains the data when the user has used GoogleMaps.

Path:

/private/var/mobile/Containers/Data/Application/83B0F882-A1B8-4462-9937-B07B9D98ACB9/Library/Preferences

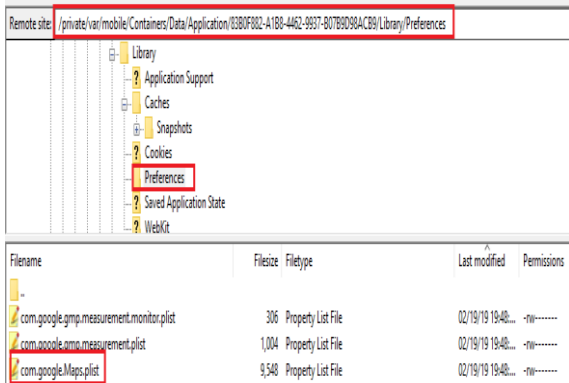


Figure 33: GoogleMaps path

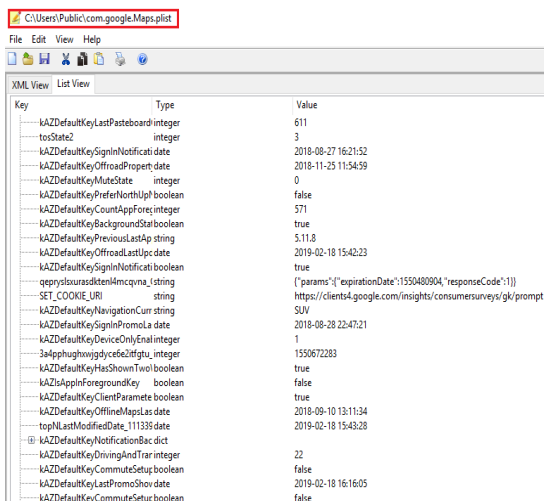


Figure 34: GoogleMaps data from plist file

BSNL: This Application is used to know the connection and registered user details.

BSNL.sqlite database: This file contains information of Service number, Account number and name of the user. The query used to extract the data is "select * from Items"

Path:

/private/var/mobile/Containers/Data/Application/93DD2AFF-86AE-41AD-85F3-43647ABB3AF6/Documents

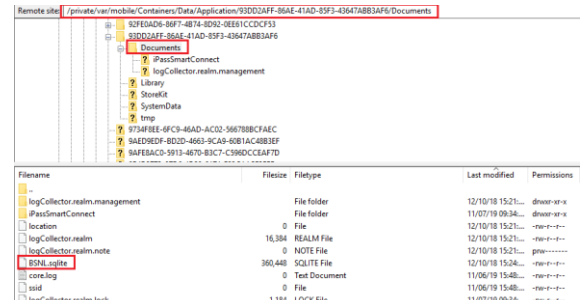


Figure 35: BSNL Path

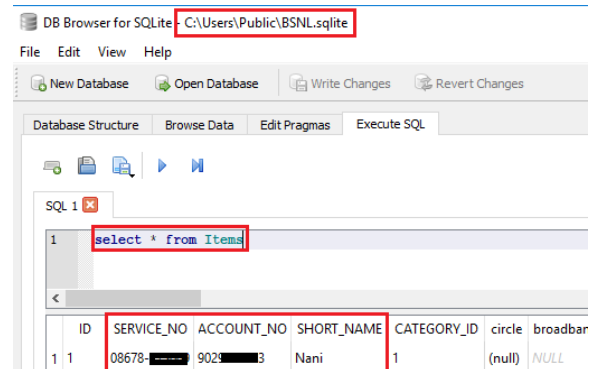


Figure 36: Extracted data

WYNK: This Music App is used to find the list of MP3 songs downloaded and login details of the user.

Path:

/private/var/mobile/Containers/Data/Application/9AFE8AC0-5913-4670-B3C7-C596DCCEAF7D/Documents/stream

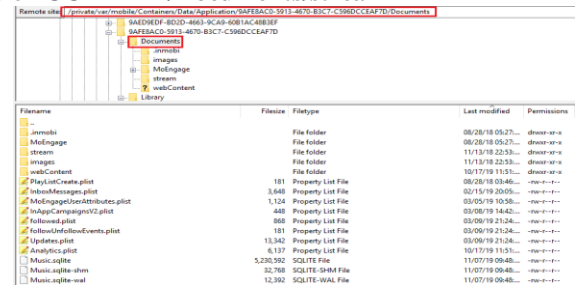


Figure 37: WYNK Path

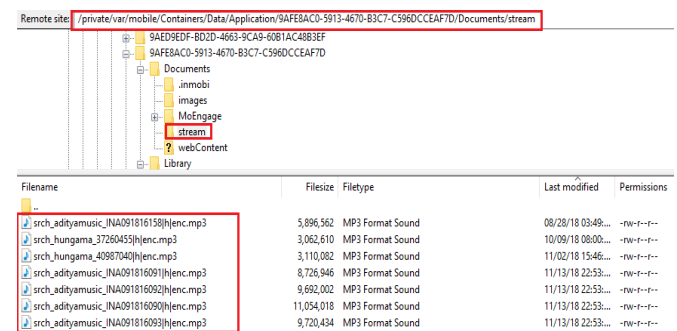


Figure 38: The Downloaded MP3 files

VII. CONCLUSION

Smart phones usage has been expanded vastly with the increase in advanced features like face lock, fingerprint unlock, gaming, and storage capacity etc. Among them iPhone usage is in high growth due to its security policies and features like device encryption.

So, extracting data from iPhone is very challenging in Forensics. By using the method proposed in this paper, the artifacts can be analysed which helps the forensic investigator to extract the data and prepare an evidence.

ACKNOWLEDGEMENTS

This work is assisted by my project guide from Department of Science and Technology and ESF Labs. I would be very grateful to my project guide and the individuals in the company who helped me to complete my project successfully at each and every phase of execution.

REFERENCES

- Ahmad Raza Cheema, Mian Muhammad Waseem Iqbal, Waqas Ali "Analysing iPhone File System files with Open Source Toolkit for Forensic Evidence" – Research Gate
- Feng Liu, Ke-sheng Liu, Chao Chang Wang, Yan Wang "Research on the technology of iOS jailbreak" - IEEE
- Aswami Ariffin, Christian D' Orazio, Kim-Kwang Raymond Choo, Jill Slay "iOS Forensics: How can we recover deleted images files with timestamp in a forensically sound manner" - IEEE
- Ryan R Kubasiak, Sean Morrissey, Walter Barr, James Kelly Brown, Max Caceres, Mike Chasman and James Cornell "Mac OSX, iPod, and iPhone Forensic Analysis"
- Adam Shortall, M A Hannan Bin Azhat "Forensic Acquisitions of WhatsApp data on popular mobile platforms"-IEEE
- M. Bader and I.Baggili, "iPhone 3GS Forensics: logical analysis using Apple iTunes backup utility" Small Scale Digital Forensics
- Christian D' Orazio, Aswami Ariffin, Kim-Kwang Raymond Choo "iOS Anti-Forensics: How can we security conceal, delete and insert data?" -IEEE
- "Mobile Device Forensics", Wikipedia
- "Jailbreaking", Wikipedia
- "iOS Application Structure", <https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/FileSystemProgrammingGuide/FileSystemOverview/FileSystemOverview.html>
- S. Brothers, "Cell phone and GPS Forensic Tool Classification System" – Presentation to Digital Forensics
- Mona Erafani Joorabchi, Ali Mesbah "Reverse Engineering iOS Mobile Applications" - IEEE
- Mohd Shahdi Ahmad, Nur Emyra Musa, Rathidevi Nadarajah, Rosilah Hassan, Nor Effendy Othman "Comparison Between Android and iOS Operating System in terms of security" - IEEE
- Wencheng Yan, Jiankun Hu, Clinton Fernandes, Vijay Sivaraman, Qianhong Wu "Vulnerability Analysis of iPhone 6" - IEEE
- Roy Want "iPhone: Smarter Than the Average Phone" - IEEE
- Anusha, A., Guptha, A., Sivanageswar Rao, G. & Tenali, R.K. 2019, "A model for smart agriculture using IOT", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 6, pp. 1656-1659.
- Daya Sagar, K.V., Siva Nageswara Rao, G., Srikanth, T. & Raghavendra, K. 2014, "A relational analytic platform with Hadoop using the On Demand Integration (ODI) capability", International Journal of Applied Engineering Research, vol. 9, no. 13, pp. 2095-2102.
- Phani Babu, K. & Siva Nageswara Rao, G. 2019, "Smart healthcare system", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 12, pp. 4184-4188.
- Siva Nageswara Rao, G. 2016, "Real time scheduling for dynamic process execution using round robin switching", Journal of Theoretical and Applied Information Technology, vol. 89, no. 1, pp. 60-66.
- Siva Nageswara Rao, G., Jayanth, T.V.M., Shabzan, S. & Supriya, B. 2017, "Airport luggage tracking system using RFID and GSM", Journal of Advanced Research in Dynamical and Control Systems, vol. 9, pp. 748-757.
- Siva Nageswara Rao, G., Kiran Babu, M. & Rao, S. 2019, "Efficient scheduling measures for improving real time systems using prediction process", Journal of Computational and Theoretical Nanoscience, vol. 16, no. 5-6, pp. 1876-1880.
- Siva Nageswara Rao, G., Krishna, C.V.P. & Rao, K.R. 2014, "Extreme Programming for service-based application development architecture", Proceedings of the 2014 Conference on IT in Business, Industry and Government: An International Conference by CSI on Big Data, CSIBIG 2014.
- Siva Nageswara Rao, G., Krishna, C.V.P. & Rao, K.R. 2014, Multi Objective Particle Swarm Optimization for Software Cost Estimation.
- Siva Nageswara Rao, G., Krishna, C.V.P. & Rao, K.R. 2013, "Rational unified process for service oriented application in extreme programming", 2013 4th International Conference on Computing, Communications and Networking Technologies, ICCCNT 2013.
- Siva Nageswara Rao, G., Manojkumar, B., Jaya Raj, R. & Sharma, A. 2018, "IOT based garbage management system", Journal of Advanced Research in Dynamical and Control Systems, vol. 10, no. 4, pp. 31-36.
- Siva Nageswara Rao, G., Srinivasu, N., Girish Kumar, K. & Abhishek, B. 2014, "An enhanced dynamic Round Robin CPU scheduling algorithm", International Journal of Applied Engineering Research, vol. 9, no. 15, pp. 3085-3098.
- Siva Nageswara Rao, G., Srinivasu, N. & Rama Koteswara Rao, G. 2015, "Dynamic time slice calculation for round robin process scheduling using NOC", International Journal of Electrical and Computer Engineering, vol. 5, no. 6, pp. 1480-1485.
- Siva Nageswara Rao, G., Srinivasu, N., Sagar, K.V.D. & Sai Madhuri, P. 2014, "Comparison of round robin CPU scheduling algorithm with various dynamic time quantum", International Journal of Applied Engineering Research, vol. 9, no. 18, pp. 4905-4916.
- Siva Nageswara Rao, G. & Srinivasu, S. 2016, "Task scheduling for real time applications using mean-difference round robin (MDRR) algorithm with dynamic time slice (MDDRWDTs)", International Journal of Pharmacy and Technology, vol. 8, no. 3, pp. 16082-16088.
- Siva Nageswara Rao, G. & Srinivasu, S.V.N. 2017, "Hybrid approach for task scheduling in heterogeneous cloud based systems", Journal of Advanced Research in Dynamical and Control Systems, vol. 9, no. Special Issue 14, pp. 618-625.
- Siva Nageswara Rao, G. & Srinivasu, S.V.N. 2016, "An efficient round robin cpuscheduling algorithm using dynamic time slice", International Journal of Pharmacy and Technology, vol. 8, no. 4, pp. 21461-21469.
- Siva Nageswara Rao, G., Srinivasu, S.V.N., Srinivasu, N. & Naga Raju, O. 2015, "A new proposed Dynamic dual processor based CPU scheduling algorithm", Journal of Theoretical and Applied Information Technology, vol. 73, no. 2, pp. 226-231.
- Siva Nageswara Rao, G., Srinivasu, S.V.N., Srinivasu, N. & Ramakoteswara Rao, G. 2015, "Enhanced precedence scheduling algorithm with dynamic time quantum (EPSADTQ)", Research Journal of Applied Sciences, Engineering and Technology, vol. 10, no. 8, pp. 938-941.
- Srilakshmi, M., VenkataKrishna, S. & Siva Nageswara Rao, G. 2014, "Dynamically managing the software components in deployment based architecture", International Journal of Applied Engineering Research, vol. 9, no. 19, pp. 6139-6148.
- Uppuluri, S., Dilip Raja, K., Sivaleela, D., Suresh Reddy, A. & Siva Nageswara Rao, G. 2015, "Effect of ethanolic pod extract of Canavalia gladiata on peptic ulcer in wistar rats", International Journal of Pharmaceutical and Clinical Research, vol. 7, no. 6, pp. 383-385.
- Venkateswara Rao, C. & Siva Nageswara Rao, G. 2019, "An effective research on data mining techniques for intrusion detection & learning classes", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 11 Special Issue, pp. 845-849.
- Yaswanth, K.B., Manasa, L., Chetan, B.V. & Siva Nageswara Rao, G. 2019, "Modern vehicle tracking and monitoring system using embedded technology", International Journal of Recent Technology and Engineering, vol. 8, no. 1, pp. 1849-1851.

AUTHORS PROFILE



Hyndavi Koganti is a student pursuing her M.Tech in the field of Cyber Security and Digital Forensics - Department of CSE, KLEF, Vaddeswaram, A.P. India. She is a graduate who completed her B.Tech in computer science and engineering at Amrita Sai institute of Engineering and Technology.



Dr. G Siva Nageswara Rao is a professor in CSE department, KLEF, Vaddeswaram, Guntur. He has totally 23 years of experience in teaching and published 21 scopus, 11 non scopus papers. His research area at present is on task scheduling and software engineering.