Important Databases and Files

GETTING STARTED

To view the files in the Encase Image:

1. Locate **Results** in the left-hand navigation.
2. Double-click **Encryption Detected (1)**.
3. In the **Listing** pane, click `documents.zip`.
4. Expand **vol5**.

File Name	Description	File Location
`AddressBook.sqlitedb`	Contact information and personal data like name, email address, birthday, organization	vol5/mobile/Library/AddressBook
`AddressBookImages.sqlitedb`	Images associated with saved contacts	vol5/mobile/Library/AddressBook
`Calendar details and events information`	Calendar details and events information	vol5/mobile/Library/Calendar
`call_history.db`	Incoming and outgoing call logs, including phone numbers and time stamps	vol5/wireless/Library/CallHistory

File Name	Description	File Location
`AddressBook.sqlitedb`	Contact information and personal data like name, email address, birthday, organization	vol5/mobile/Library/AddressBook
`AddressBookImages.sqlitedb`	Images associated with saved contacts	vol5/mobile/Library/AddressBook
`Calendar details and events information`	Calendar details and events information	vol5/mobile/Library/Calendar
`sms.db`	Text and multimedia messages along with their timestamps	vol5/mobile/Library/SMS/
`voicemail.db`	Voicemail messages	vol5/mobile/Library/Voicemail/
`Safari/Bookmarks.db`	Saved URL addresses	vol5/mobile/Library/Safari
`Safari/History.plist`	User's internet browsing history	vol5/mobile/Library/Safari
`vol5/mobile/Library/Safari`	Apple Notes application data	Apple Notes application data
`Maps/History.plist`	Keeps track of location searches	vol5/mobile/Library/Maps
`Maps/Directions.plist`	Saved location searches	vol5/mobile/Library/Maps
`consolidated.db`	Stores GPS tracking data	root/Library/Caches/locationd
`En_GB-dynamic-text.dat`	Keyboard cache	vol5/mobile/Library/Keyboard
`general.log`	Device information (serial #, version #, etc.)	vol5/logs/AppleSupport
`lockdownd.log`	ICCID (integrated circuit card identifier) number identifies each SIM internationally. It is also considered the issuer's identification number.	vol5/logs
`lockdownd.log.1`	Phone number	vol5/logs
`Envelope Index`	Email addresses on phone	vol5/mobile/Library/Mail

File Name	Description	File Location
`AddressBook.sqlitedb`	Contact information and personal data like name, email address, birthday, organization	vol5/mobile/Library/AddressBook
`AddressBookImages.sqlitedb`	Images associated with saved contacts	vol5/mobile/Library/AddressBook
`Calendar details and events information`	Calendar details and events information	vol5/mobile/Library/Calendar
`xxxxx. .emlx`	Email messages	vol5/mobile/Library/Mail/POP□ /INBOX.mbox/Messages
`vol5/mobile/Library/Mail/POP`	Google coordinates of places	root/Library/Caches/locationd

The following sections contain descriptions of the major files and how to access them in Autopsy. Some of the following information is from *iPhone Forensics* by Jonathan Zdziarski, published by O'Reilly Media, Inc., 2008.

CALL HISTORY

One of the most useful databases on the iPhone is the call history. The call history stores the phone numbers of the last people contacted by the suspect. As newer calls are made, the older phone numbers are deleted from the database, but often remain present in the file itself. Querying the database will provide the live call list, while performing a strings dump of the database may reveal additional phone numbers. This can be particularly useful if the suspect cleared the call log. The file `/mobile/Library/CallHistory/call_history.db` contains the call history.

To view in Autopsy:

1. Select **`call_history.db`** in the **Listings** pane.

2. Select **Indexed Text** in the **Data Content** pane and scroll down to call.

EMAIL DATABASE

All mail stored locally on the iPhone (that is, mail that is not downloaded from an IMAP server) is stored in a SQLite database having the filename `/mobile/Library/Mail/Envelope Index`.

Unlike other databases, this particular file has no extension, but it is indeed a SQLite database. This file contains information about messages stored locally, including sent messages and the trash can. Data includes message headers, mailboxes, and the message data itself. This database is somewhat complex and contains six tables: mailboxes, messages, message_data, properties, pop_uids, and threads.

Mail contains the email address used on the phone device. To obtain a list of mailboxes stored on the device:

1. Select **`mobile/Library/Mail`** in the **Directory Tree** pane.
2. Select **`Envelope Index`** in the **Listing** pane.
3. Select **Indexed Text**.
4. Scroll down to mailboxes.

To obtain a list of email messages stored on the device:

1. Select **`mobile/Library/Mail/POP-coralblue..../Messages`** in the **Directory Tree** pane.
2. Select the **EMLX** files in the **Listing** pane.
3. Select **Indexed Text**. The email messages are displayed.

ADDRESS BOOK CONTACTS

The address book contains individual contact entries for all of the contacts stored on the iPhone. The address book database can be found at

`/mobile/Library/AddressBook/AddressBook.sqlitedb`. The following tables are primarily used:

- **ABPerson**: Contains the name, organization, department, and other general information about each contact.

- **ABRecent**: Contains a record of recent changes to properties in the contact database and a timestamp of when each was made.

- **ABMultiValue**: Contains multivalue data for each contact, including phone numbers, email addresses, website URLs, and other data for which the contact may have more than one.

- **ABMultiValueEntry**: Some multivalue entries contain multiple values themselves. For example, an address consists of a city, state, zip code, and country code.

- **ABMultiValueEntrytable**: This table consists of a **parend_id** field, which corresponds to the **rowid** of the **ABMultiValuetable**.

To View in Autopsy:

1. Select **`mobile/Library/Address Book/`** in the **Directory Tree** pane.

2. Select `AddressBook.sqlitedb` in the **Listing** pane.

3. Scroll down to **ABPerson** for a listing of people in the address book.

4. Scroll down to **ABMultiValue** for additional information on each contact in the address book.

SMS MESSAGES

The SMS message database contains information about SMS messages sent and received on the device. This includes the phone number of the remote party, timestamp, actual text, and various carrier information. The file can be found on the iPhone's media partition in `/mobile/Library/SMS/sms.db`.

To View in Autopsy:

1. Select **`mobile/Library/SMS`** in the **Directory Tree** pane.
2. Select **`sms.db`** in the **Listing** pane.
3. Select **Indexed Text**.
4. Scroll down to messages.

To view in SQLite Browser:

1. Application > Database Assessment > SQLite database
2. Open Database > corpus > `sms.db`
3. Execute SQL > select * from message
4. Click the forward triangle.

NOTES

The notes database is located at `/mobile/Library/Notes/notes.db` and contains the notes stored for the iPhone's built-in Notes application. It's one of the simplest applications on the iPhone, and therefore has one of the simplest databases.

VOICEMAIL

The voicemail database contains information about each voicemail stored on the device and includes the sender's phone number and callback number, timestamp, the message duration, the expiration date of the message, and the timestamp (if any) denoting when the message was moved to the trash. The voicemail database is located in `/mobile/Library/Voicemail/voicemail.db`, while the voicemail recordings themselves are stored as AMR codec audio files in the directory `/mobile/Library/Voicemail/`.

Voicemails must be extracted using SQLite.

The audio files themselves can be played by any media player supporting the AMR codec. The most commonly used players include Quicktime and VLC.