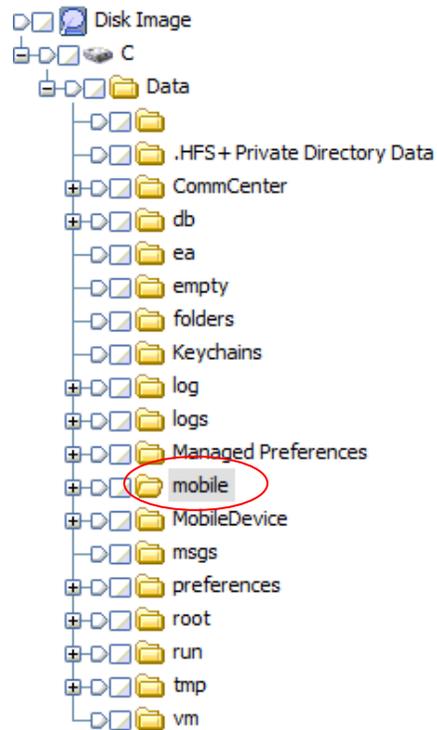


# iPhone Call History

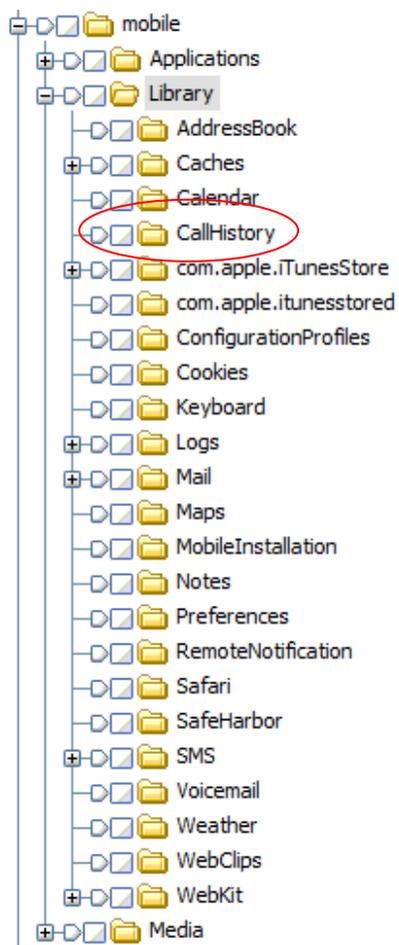
Detective Richard Gilleland  
Sacramento Police Department  
rgilleland@pd.cityofsacramento.org

Examining iPhone dd image call history using Encase

After importing an iPhone dd image into Encase forensic software for examination, the examiner should see a directory structure similar to the one listed below;



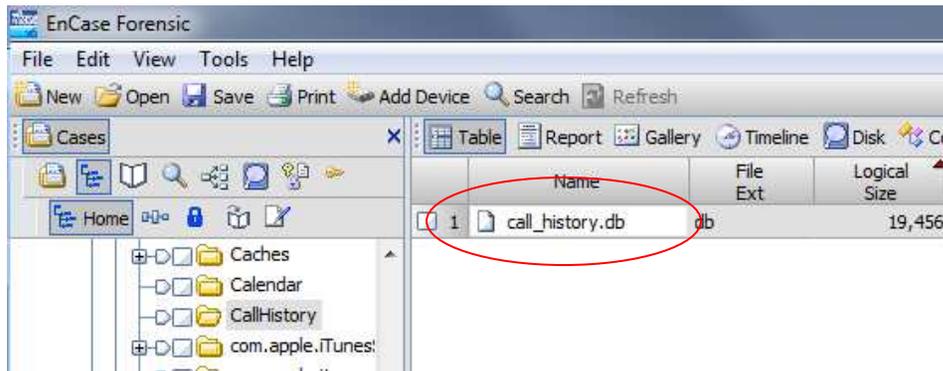
Much of the (undeleted) data of interest will be located in the 'mobile\Library' directory as seen below;



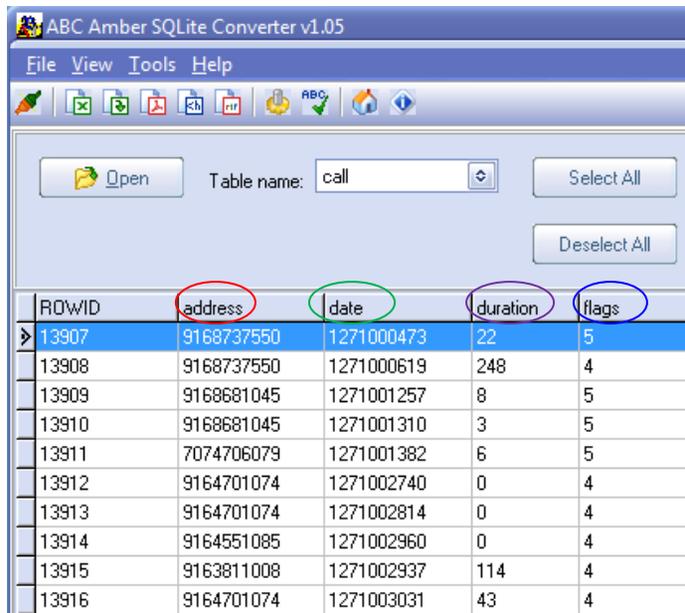
This is where examiners will locate many common cell phone items of interest including;

AddressBook  
CallHistory  
SMS

All of the above listed items are stored in an sqlite database however this document will focus on the **call history** database. Below is a screen capture of what this database looks like when viewed in Encase. One method of viewing this sqlite database is to export the 'call\_history.db' file and use an external sqlite database viewer to view the contents.



For my research, I used ABC Amber SQLite Converter (v1.05) to open the call\_history.db file;



'address' - phone number of the related call

'data' - date and time of the call history entry (stored in Unix date / time format)

'duration' - duration of the call (stored in seconds)

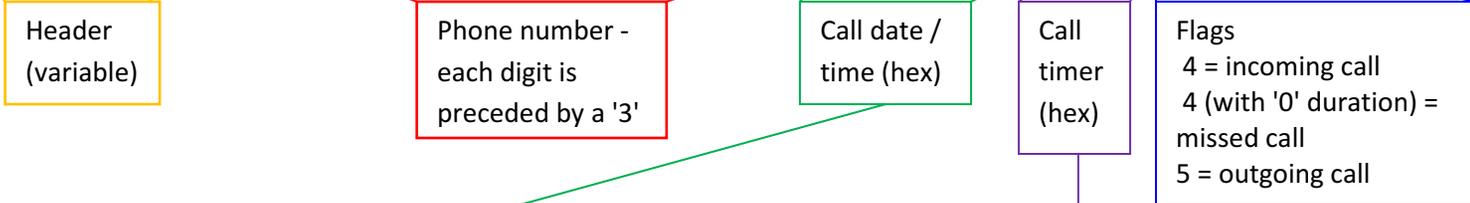
'flags' - determine if the call is incoming / outgoing / missed

Below is a breakdown of how this information is stored and how it can be viewed;

Analysis of iPhone call history dates / times

#	Type	Number	Name	Date & Time	Duration
1	Outgoing	9168737550	* Patricia York	04/11/10 15:41:13 (GMT)	0:00:22

21 04 01 01 01 39 31 36 38 37 33 37 35 35 30 4B C1 ED 99 16 05 06 19 EC 54 07 00



Value  
Hex Characters/Value To Be Decoded  
4B C1 ED 99

Calculate

Hex Little Endian  
 Hex Big Endian  
FAT  
Text

Results

- Filetime (NTFS Time): Not Valid
- Filetime Text (Lo:Hi): Not Valid
- FAT ms + Time + Date: Not Valid
- FAT Time + Date: Try Interpreting As DOS/FAT
- FAT Date Only: Not Valid
- IE(FAT) Date + Time: Try Interpreting As DOS/FAT
- 32 bit time\_t (Unix Time): 2010-04-11 15:41:13

Calculator

View Edit Help

22

Hex  
 Dec  
Oct  
Bin

Qword  
Dword  
Word  
Byte

Not And F 0 . + =

\* 'The Time Lord' (v0.1.5.6) used to convert date / time values.

Below are some examples of hex from various types of calls.

1	Outgoing	9168737550	* Patricia York	04/11/10 15:41:13 (GMT)	0:00:22
---	----------	------------	-----------------	-------------------------	---------

21 04 01 01 01 39 31 36 38 37 33 37 35 35 30 4B C1 ED 99 16 05 06 19 EC 54 07 00 (outgoing)

1	Incoming	9168737550	* Patricia York	04/11/10 15:43:39 (GMT)	0:04:08
---	----------	------------	-----------------	-------------------------	---------

21 04 02 01 01 39 31 36 38 37 33 37 35 35 30 4B C1 EE 2B 00 F8 04 FF 18 EC 55 07 00 (incoming)

10	Missed	9168681045	* Michaelann	04/11/10 18:39:28 (GMT)	N/A
----	--------	------------	--------------	-------------------------	-----

21 04 01 01 01 39 31 36 38 36 38 31 30 34 35 4B C2 17 60 00 04 FF 19 EC 6D 07 00 (missed)

19	Incoming	9168685875	N/A	04/12/10 05:07:46 (GMT)	0:01:17
----	----------	------------	-----	-------------------------	---------

21 04 01 01 01 39 31 36 38 36 38 35 38 37 35 4B C2 AA A2 4D 04 FF 19 ED 2D 07 00 (incoming)

GREP search for call history in Unallocated;

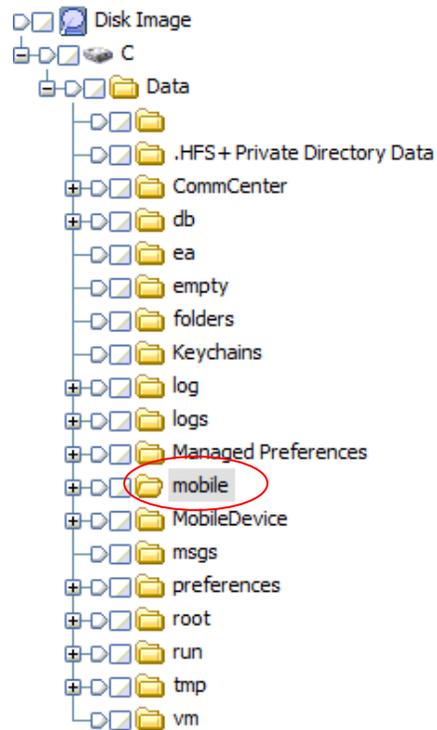
`[\\x21\\x23]\\x04..[\\x01\\x02\\x04][\\x30-\\x39]{9,10}\\. {5,8}[\\x04\\x05\\x08]\\. {4,6}\\x00`

# iPhone SMS History

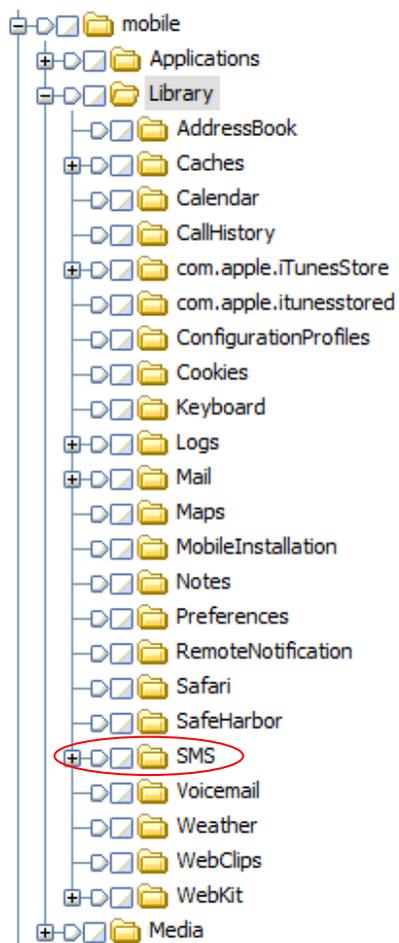
Detective Richard Gilleland  
Sacramento Police Department  
rgilleland@pd.cityofsacramento.org

Examining iPhone dd image call history using Encase

After importing an iPhone dd image into Encase forensic software for examination, the examiner should see a directory structure similar to the one listed below;



Much of the (undeleted) data of interest will be located in the 'mobile\Library' directory as seen below;



This is where examiners will locate many common cell phone items of interest including;

AddressBook  
CallHistory  
SMS

All of the above listed items are stored in an sqlite database however this document will focus on the **text messages (sms)** database. Below is a screen capture of what this database looks like when viewed in Encase. One method of viewing this sqlite database is to export the 'sns.db' file and use an external sqlite database viewer to view the contents.

	Name	File Ext	Logical Size
1	Parts		56
2	Drafts		58
3	sms-legacy.db	db	24,576
4	sms.db	db	65,536

For my research, I used ABC Amber SQLite Converter (v1.05) to open the sms.db file;

ROWID	address	date	text	flags
3728	+19168737550	1270269680	I need to talk to you.	2
3730	+19164701074	1270371090		2
3731	+19164701074	1270376316	Whats up-I do it 4 the dollar	2
3734	+19164701074	1270408237		2
3739	+19164701074	1270421077	Happy easter-I do it 4 the dollar	2
3746	+19164701074	1270457737	Yea whats upper -I do it 4 the dollar	2
3750	+19164701074	1270593510	Where you at-I do it 4 the dollar	2
3753	+19164701074	1270624211	Nobody-I do it 4 the dollar	2
3756	+19164701074	1270678800	Is it good yet-I do it 4 dolla	2
3757	+19164701074	1270678838	yep	3

'address' - phone number of the related call

'date' - date and time of the call history entry (stored in Unix date / time format)

'text' - contents of the text message

'flags' - determine if the text message was sent or received

Below is a breakdown of how this information is stored and how it can be viewed;

Analysis of iPhone sms

1	+19168737550	* Patricia York	04/03/10 04:41:20 (GMT)	Read	Inbox	Phone	Incoming	I need to talk to you.	
---	--------------	-----------------	-------------------------------	------	-------	-------	----------	------------------------	--

31 39 31 36 38 37 33 37 35 35 30 4B B6 C6 F0 49 20 6E 65 65 64 20 74 6F 20 74 61 6C 6B 20 74 6F 20 79 6F 75 2E 02

Phone number -  
each digit is  
preceded by a '3'

Call date /  
time (hex)

Message  
content

flags  
2 - incoming  
3 - outgoing  
0 - Inbox / unread

Value

Hex Characters/Value To Be Decoded

4B B6 C6 F0

Calculate

Hex Little Endian  
 Hex Big Endian  
 FAT  
 Text

Results

Filetime (NTFS Time):	Not Valid
Filetime Text (Lo:Hi):	Not Valid
FAT ms + Time + Date:	Not Valid
FAT Time + Date:	Try Interpreting As DOS/FAT
FAT Date Only:	Not Valid
IE(FAT) Date + Time:	Try Interpreting As DOS/FAT
32 bit time_t (Unix Time):	2010-04-03 04:41:20

\* 'The Time Lord'  
(v0.1.5.6) used to convert  
date / time values.

Below are some examples of hex of sms messages and their values;

1	+19168737550	* Patricia York	04/03/10 04:41:20 (GMT)	Read	Inbox	Phone	Incoming	I need to talk to you.	
---	--------------	-----------------	-------------------------------	------	-------	-------	----------	------------------------	--

31 39 31 36 38 37 33 37 35 35 30 4B B6 C6 F0 49 20 6E 65 65 64 20 74 6F 20 74 61 6C 6B 20 74 6F 20 79 6F 75 2E 02

10	+19164701074	* Canturbury Kris	04/07/10 22:20:38 (GMT)	Sent	Sent	Phone	Outgoing	yep	
----	--------------	----------------------	-------------------------------	------	------	-------	----------	-----	--

31 39 31 36 34 37 30 31 30 37 34 4B BD 05 36 20 20 79 65 70 03

44	+19168737550	* Patricia York	04/12/10 21:20:44 (GMT)	Unread	Inbox	Phone	Incoming	I will be on a later train; I WILL LET YOU KNOW WHICH ONE--It will be after 5:00 p.m.	
----	--------------	-----------------	-------------------------------	--------	-------	-------	----------	--	--

31 39 31 36 38 37 33 37 35 35 30 4B C3 8E AC 49 20 77 69 6C 6C 20 62 65 20 6F 6E 20 61 20 6C 61 74 65 72 20 74 72 61 69 6E  
3B 20 49 20 57 49 4C 4C 20 4C 45 54 20 59 4F 55 20 4B 4E 4F 57 20 57 48 49 43 48 20 4F 4E 45 2D 2D 49 74 20 77 69 6C 6C 20  
62 65 20 61 66 74 65 72 20 35 3A 30 30 20 70 2E 6D 2E 00

While researching this iPhone's sms, I located a number of unique messages that were not captured / reported using either the 'Ike's iPhone SMS parser' or other automated lab tools such as Cellebrite. These sms messages have different file headers and footers however they are still contained within the 'sms.db' file.

The 'unique sms' messages are in a different format as seen below (Encase view);

```
·#·-----17072466118Iüã5Cool·-5·----3|)
·#·'-----17072466118Iüã!Roger, tango!·-5Iüã!·-·=|(
·#·A-----17072466118IüãôLet me know if ya got this·-5·----|·|'·-·#·|I-----17072466118IüãýHey bro, we got cut off. He
re's my shit, hit me up anytime. 707-246-6118 mmekhalian@gmail.com·-5·-----^|"
·#·}-----19169475804IÿiCheck your email and call me after you see the pictures!·-·Iÿi·-·|C|!·-·#·|K-----142376252
74Iøð|I sent you a multimedia message. You can view my message w/in the next 7 days via the web at www.viewmymessage.com
/2 using MSG ID pOrswjqz1 Password tear18chew·-3·----6|·
·#·-----19169475804I+·)Call me at break·-I+·)·-·f|·-·#·|-----19169475804I+icGood because I have devoted my life
to you and all my loyalty!!·-·I+ic·-·/|·
·#·%-----19169475804I+gÉWell i do!! ·-----@|·
·#·A-----19169475804I+g|You had Better Love me!!!!·-·I+g|·-·-·|·
·#·#-----19169475804I+f·Love you! ·-----/|·
·#·%-----19169475804Iö|KStill awake?·-----|·
·#·!-----19169475804Ið zStill up??·-----'|·
·#·-----19169475804Ió,·K·-·Ió,·-·-·;|·
·#·=-----19169475804Ió'»I just sent the pictures·-----=|

·#·A-----19169475804IñGçI love you...and miss you.·-----:|
·#·;-----19169475804IñEãOk.. You are ok though?·-----:|·
·#·5-----19169475804IñE·Everybody is asleep ·-·IñE·-·-·6|·
·#·3-----19169475804IñE~Why didnt you call?·-----@|·
·#·A-----19169475804IñE Goodnight babe I love you!·-·IñE ·-·-·)|·
```

These messages appear to decode as follows;

\*\* some of these messages have associated dates and times while others do not. It appears that incoming messages do not have associated dates / times while many of the outgoing (sent) messages do have recorded dates / times.

```
] -# .....17072466118Iüã5Cool --5 ----3|)
```

31 37 30 37 32 34 36 36 31 31 38 49 FC E3 35 43 6F 6F 6C 02 00 35 00 00 04 00 33 89 29 0D

Phone number -  
each digit is  
preceded by a '3'

Message  
content

flags  
2 - incoming  
3 - outgoing  
0 - Inbox / unread

No  
associated  
date / time

```
] -# ' .....17072466118Iüã!Roger, tango! --5Iüã! --==| (
```

31 37 30 37 32 34 36 36 31 31 38 49 FC E3 21 52 6F 67 65 72 2C 20 74 616E 67 6F 21 03 00 35 49 FC E3 21 00 04 00 3D 89 28

Phone number -  
each digit is  
preceded by a '3'

Message  
content

flags  
2 - incoming  
3 - outgoing  
0 - Inbox / unread

Call date /  
time (hex)

## **GREP expressions**

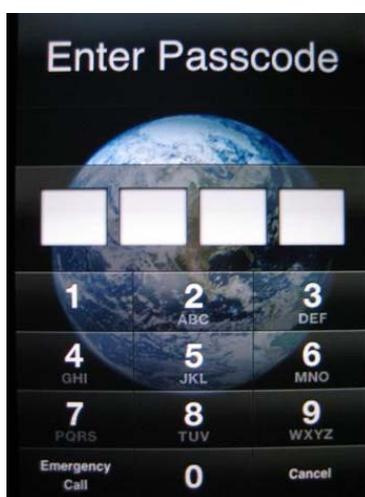
**\x01\x00\x02\x01\x01\x01\x01\x00\x11\x00\x00\x01 (normal sms)**

**\x00\x23\x04..\x01[\x00\x01][\x00\x01\x02].\x01\x01\x01 (additional / unique sms)**



# ***UFED Guide: Bypassing User Passcode on Apple iPhone Devices***

***Overview: Access can be gained to user locked iPhone devices by copying certain .plist files from the user's PC or Mac iTunes directory to a USB Flash Drive. This USB drive can then be used in conjunction with your UFED System as a key, to bypass the user locked iPhone. Please note the .plist files MUST come from the computer which the specific iPhone is synced with, after the user code was enabled.***



1. Connect Apple iPhone (2G, or 3G) to UFED and select to extract desired information.
2. If the user iPhone is passcode locked, and passcode is known, enter it in the iPhone and select "retry"
3. If Passcode is unknown, and access to the user's Mac or PC is available, copy all .plist files in the following directory to the **root directory** of a newly formatted USB flash disk:

***PC iTunes Users: copy all the .plist files in the following directory to root directory of USB drive:***

***Documents and Settings\<User Name>\Application Data\Apple Computer\Lockdown\<Copy all .plist files to USB Drive>***

***Mac iTunes Users: copy all the .plist files in the following directory to root directory of USB drive:***

***VolumeName\Users\<User Name>\Library\Lockdown\<Copy all .plist files to USB drive>***

4. Once the key is made, insert the USB drive in either of the top USB port marked "USB EXT" or the Target USB port, and press F2 to continue. The UFED will use the .plist files to bypass the user lock the iPhone and extract the desired information.