iOS 取證概要

OSSLab
http://www.osslab.com.tw/
::OSSLab::開放軟體實驗室
thx@osslab.com.tw

【目錄】

*

【iOS基本介绍】

iOS系统

iOS是蘋果公司為iPhone/iPod/iPad開發的移動終端操作系統，以Darwin為基礎，屬於類Unix的商業操作系統，隨第一代iPhone於2008年6月發佈。

截止至2011年11月，根據Canalys的數據顯示，iOS已經佔據了全球智能手機系統市場份額的30%。

*

【iOS基本介绍】

文件系统

HFS+（HFS PLUS）是蘋果公司為蘋果公司為他們的分層檔系統(HFS)開發的一種檔系統，主要運用於Mac os電腦和iphone等終端上。

System分區

System分區為系統分區，大小為1G左右，主要包含iOS的系統檔。

User分區

User分區為用戶分區，大小取決於設備的型號，一般為15G、31G、64G，主要存儲用戶的個人數據，大多數User分區的個人檔都是加密。iPhone3G除外，因為iphone3G沒有加密模組。

*

【取證工具介紹】

Forensic Tookit

Elcomsoft iOS Forensic Toolkit是一套針對iOS的取證設備，致力於使iOS取證變的更簡單，這個工具箱包含一個Ramdisk和一系列工具，將ramdisk加載到iPhone上。

Ramdisk加載到**iOS**完成後，工具箱可以實現以下功能：

1、獲取**root**分區和**user**分區的物理轉存檔

2、獲取**user**分區的邏輯快照

3、提取**user**分區檔系統解密需要的驗證檔

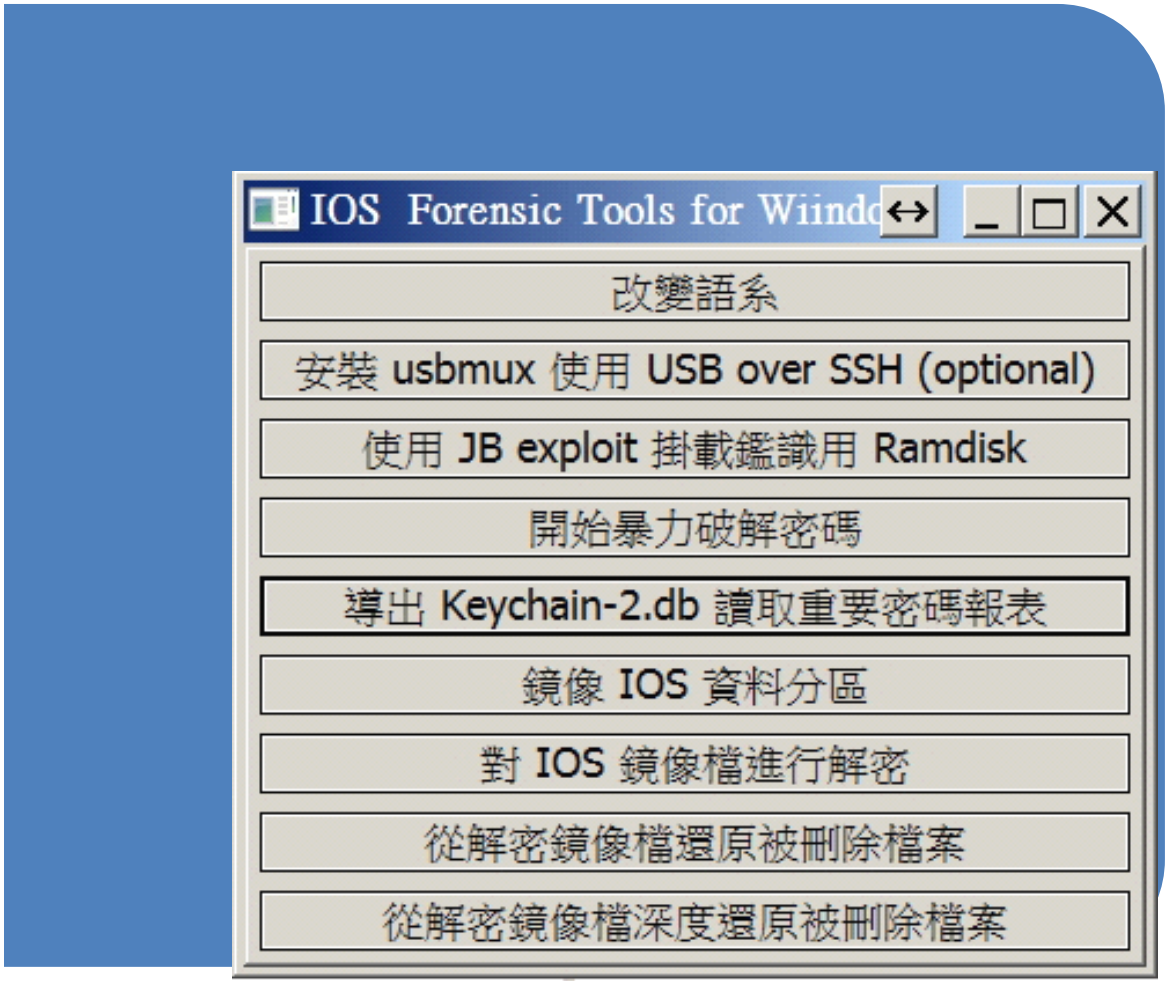
4、恢復**iOS**的密碼

*

【iOS取證軟體比較】

	UFED	.XRY	Elecomsoft	OSSLab IOS 取證軟體	效率源 SD Iphone Mobile	Oxygeoxygen forensic suite
網址	連結	連結	連結	連結	連結	連結
價格	US 10000	US 8000	US 700	司法單位免費	US 500	US 700
攜帶性	X	X	O	O	O	O
解鎖密碼	O	O	O	O	X	X
做IOS裝置RAW鏡像	O	O	O	O	X	X
取出重要密碼	O	O	O	O	X	X
鏡像解密	O	O	O	O	X	X
恢復被刪檔案	X	X	X	O	X	X
易用性	X	X	X	O	O	O
深度恢復掃描	X	X	X	O	X	X
可客製化	X	X	X	O	X	X
獲取通訊+簡訊錄	O	O	X	O	X	O
非JB 裝置可用	O	O	O	O	X	X
IOS 4 +5 支持	O	O	O	O	X	O
中文介面	X	X	X	O	O	X

【取證過程】



使用JB exploit

破解密碼

讀取密碼報表

鏡像IOS資料分區

對IOS鏡像檔進行解密

解密鏡像還原

深度還原

*

【取證過程】

進入DFU模式

進入DFU模式

iOS設備取證的第一步就是讓設備進入DFU（Development FirmwareUpgrade）模式，在主菜單上選擇，然後按照螢幕提示操作：

1、確保iOS設備電源已經關閉並且通過usb線連接到電腦；

2、同時按住電源鍵和HOME鍵持續10秒鐘；

3、鬆開電源鍵繼續按住HOME鍵10秒鐘；

此時iOS設備應該已經進入DFU模式，如果螢幕沒有任何顯示表面設備已經進入DFU模式；

PS:當設備進入DFU模式後螢幕顯示空白，iOS設備開起來向關機狀態。如果設備顯示iTunes或者Apple logo則說明設備沒有進入DFU模式，請重試進入DFU模式；

*

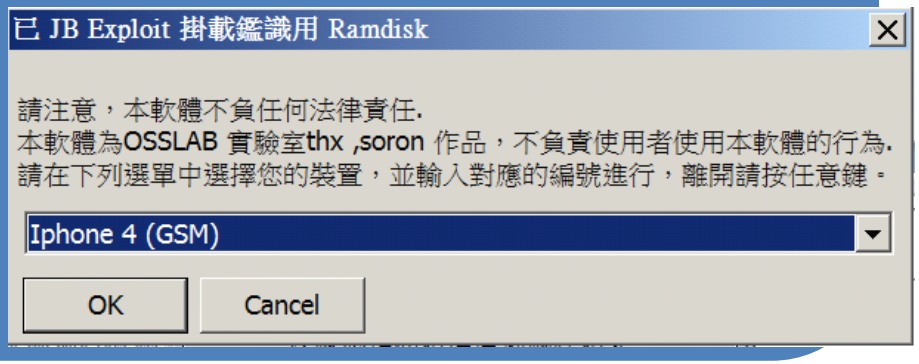
【取證過程】

加載ramdisk

加載toolkit ramdisk

NOTE:設備必須進入DFU模式才能加載ramdisk（RAM盤是通過使用軟體將RAM模擬當做硬碟來使用的一種技術，將系統記憶體當做硬碟來使用）；

iOS設備進入DFU模式之後，在主菜單上選擇2然後輸入”Y”開始加載ramdisk。我們將看到所有支持的設備列表，選擇我們連接的設備，選擇之後ramdisk開始加載，iOS螢幕變成白色，當ramdisk加載完成後，iOS設備螢幕將顯示蘋果Logo和一個空進度條。



*

【取證過程】

獲取檔鏡像

NOTE:設備必須進入DFU 模式才能進行檔系統的鏡像操作。

iOS設備進入DFU模式之後，在主菜單上選擇，我們將看到當前設備的磁片分區列表。User分區大小取決於設備型號，大小通常為15GB、31GB、64GB。User分區包含了大量的用戶個人數據，因此是取證的主要獲取對象。

IOS 4之後.大多數User分區的檔都是加密的，解密這些檔所需要到的key都必須從這臺設備裏面獲取。

工具箱同樣支持iPHone 3G的檔系統物理鏡像功能，但是由於iPhone3G設備沒有加密模組，所以即使iPhone 3G設備運行了iOS 4.X，User分區也是沒有加密的。

選擇我們需要鏡像的分區，輸入需要保存的鏡像檔的路徑和名稱，並以.dmg為擴展名，保證硬碟有足夠的空間容納dmg檔。接下來就是系統檔鏡像就開始了，所需要的時間與我們所選擇的分區以及設備型號有關

*

【取證過程】

獲取檔鏡像


IOS Forensic Tools for Wiindo
改變語系
安裝 usbmux 使用 USB over SSH (optional)
使用 JB exploit 掛載鑑識用 Ramdisk
開始暴力破解密碼
導出 Keychain-2.db 讀取重要密碼報表
鏡像 IOS 資料分區
對 IOS 鏡像檔進行解密
從解密鏡像檔還原被刪除檔案
從解密鏡像檔深度還原被刪除檔案

*

【取證過程】

Key和keychain

提取加密key和keychain data

NOTE:設備必須進入DFU 模式，加載ramdisk後才能開始提取key和keychain data。
iOS設備進入DFU模式之後，在主菜單上選擇，我們可以提取解密User分區檔和keychain數據所需要的keys，確定ramdisk已經加載後，我們將看到以下資訊：
iOS 設備密碼：如果你知道設備密碼，你可以輸入密碼，如果你不知道設備密碼，或者說設備沒有密碼保護，這裏可以為空。
Escrow檔：如果你能接觸到iOS設備連接和同步過的電腦，那麼你可以利用從這些電腦中獲取Escrow檔無需設備密碼即可解密所有存儲在iOS設備上的檔，Escrow file的檔以設備的UUID來命名。
Escrow檔的路徑為
win xp： %ALLUSERSPROFILE%\Application Data\Apple\Lockdown\
win 7 ： %ALLUSERSPROFILE%\Apple\Lockdown\

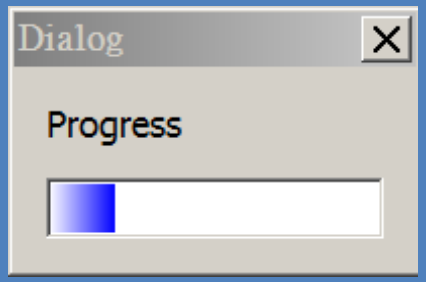
*

【取證過程】

密碼恢復

NOTE: 設備必須進入DFU 模式，加載ramdisk後才能開始恢復設備的密碼。

iOS設備進入DFU模式之後.確定ramdisk已加載成功後，主菜單上選擇,設備的密碼恢復操作開始，程式將會常識恢復4位數的簡單密碼，恢復4位數的簡單密碼所需要的時間一般不超過10到30分鐘取決於設備的類型。



*

【取證過程】

鏡像解密

NOTE:解密已經加密的分區鏡像需要提供已加密的分區鏡像和設備key，解密過程可以不連接iOS設備完成。

在主菜單上選擇選項，便會解密完成後。

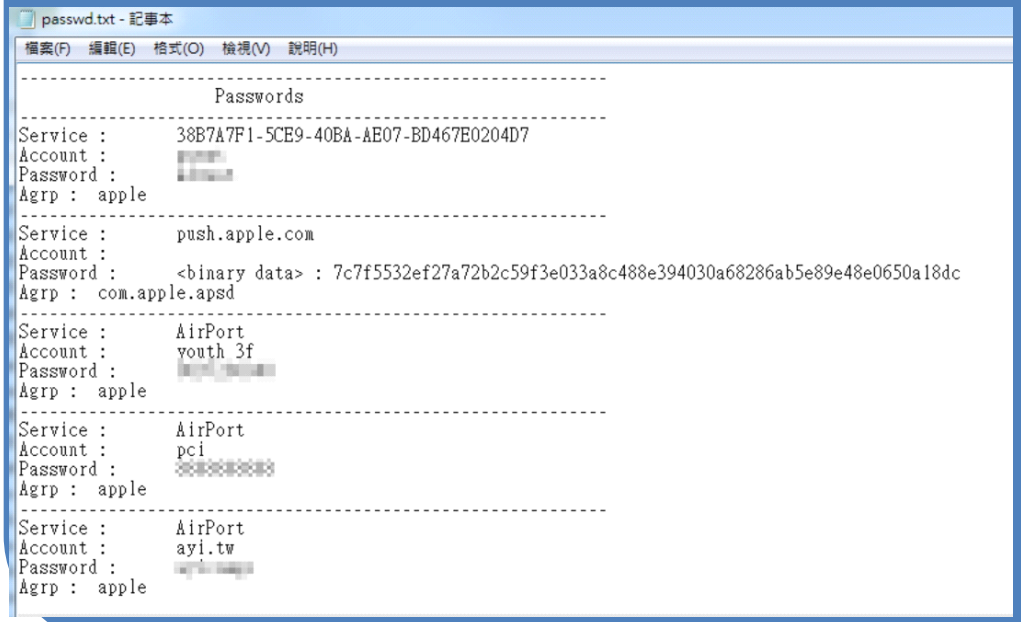
*

【效果展示】

Wifi與apple ID

wifi帳號密碼和APPLE ID帳號

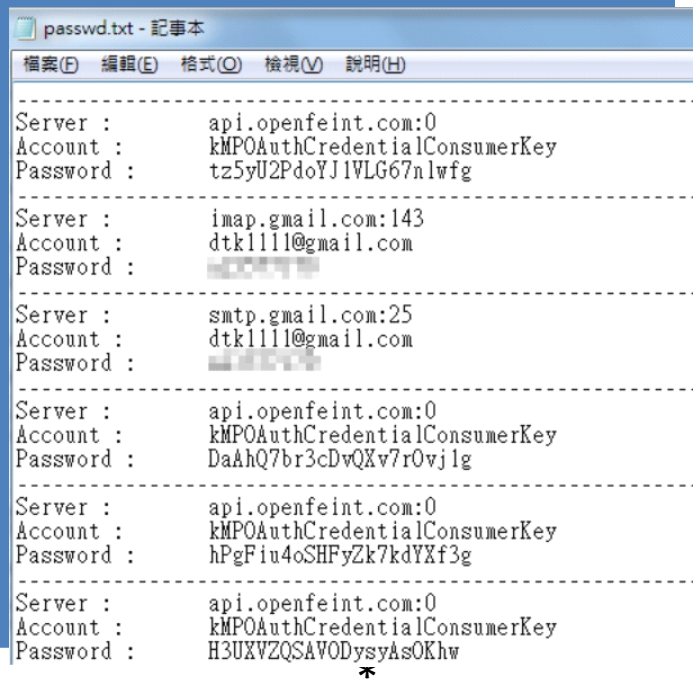
從提取到的keychain.txt裏面可以查看到iOS設備的wifi連接的帳號密碼以及APPLE ID:



passwd.txt - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

```
---------------------------------------------------------
                    Passwords
---------------------------------------------------------
Service :       38B7A7F1-5CE9-40BA-AE07-BD467E0204D7
Account :       [illegible]
Password :      [illegible]
Agrp :  apple
---------------------------------------------------------
Service :       push.apple.com
Account :
Password :      <binary data> : 7c7f5532ef27a72b2c59f3e033a8c488e394030a68286ab5e89e48e0650a18dc
Agrp :  com.apple.apsd
---------------------------------------------------------
Service :       AirPort
Account :       youth 3f
Password :      [illegible]
Agrp :  apple
---------------------------------------------------------
Service :       AirPort
Account :       pci
Password :      [illegible]
Agrp :  apple
---------------------------------------------------------
Service :       AirPort
Account :       ayi.tw
Password :      [illegible]
Agrp :  apple
```



passwd.txt - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

```
---------------------------------------------------------
Server :        api.openfeint.com:0
Account :       kMPOAuthCredentialConsumerKey
Password :      tz5yU2PdoYJ1VLG67n1wfg
---------------------------------------------------------
Server :        imap.gmail.com:143
Account :       dtk1111@gmail.com
Password :      [illegible]
---------------------------------------------------------
Server :        smtp.gmail.com:25
Account :       dtk1111@gmail.com
Password :      [illegible]
---------------------------------------------------------
Server :        api.openfeint.com:0
Account :       kMPOAuthCredentialConsumerKey
Password :      DaAhQ7br3cDvQXv7rOvj1g
---------------------------------------------------------
Server :        api.openfeint.com:0
Account :       kMPOAuthCredentialConsumerKey
Password :      hPgFiu4oSHFyZk7kdYXf3g
---------------------------------------------------------
Server :        api.openfeint.com:0
Account :       kMPOAuthCredentialConsumerKey
Password :      H3UXVZQSAVODysyAsOKhw
```

【效果展示】

系統密碼與key.plist

❖系統鎖屏密碼，

利用工具箱可以暴力破解系統密碼

❖獲取到解密用的key.plists

iOS設備的Escrow檔

XML View

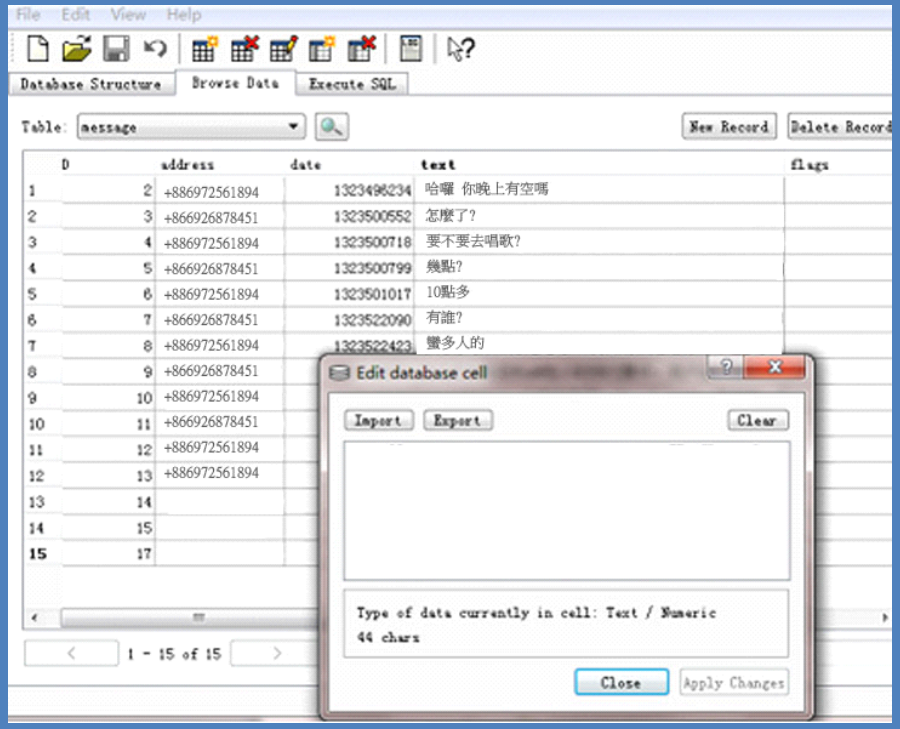
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>DerivedKeys</key>
    <dict>
        <key>2101</key>
        <data>
        4nRkLHDmMagIBmzSAeGg+w==
        </data>
        <key>2102</key>
        <data>
        ucgB4a3ESJzWpkvaiXHldw==
        </data>
        <key>2104</key>
        <data>
        dH7rHX4/QHvsfm8EALjGNQ==
        </data>
        <key>2201</key>
        <data>
        QiLO7yHDq/CVvq/WfG6P7Q==
        </data>
        <key>2202</key>
        <data>
        vakiDTZdAa204WDKk9BL0Q==
        </data>
        <key>2203</key>
        <data>
        4SRBqsIbhwIRcaPDuUo8tA==
        </data>
    </dict>
    <key>EffaceableStorage</key>
    <data>
    a0w0ADFHQUIxR0FC1bON1jQ1F/4/SQ4ImqCmDpyqBVNJRtZP0N67Q5oZdG64J59a7hSP
    8qtqhGJRZOaCa0woAHlla8TcG18JsCoTEEdhy6SRZwHFwi4Q3t39rvQH5A+YtyKAvrmP
    C7QsdRzRa0wkACFGTcUgAAAALnO6JcPqUHrwU1le2hPNTfr/FSgneEPKsa1bhIJZaxBr
```

*

【效果展示】

短信

在3gs_user.tar\mnt2\mobile\Library\SMS目錄下的sms.db中存放著設備的短資訊，可以用sqllite工具查看



*

【效果展示】

通話記錄

在3gs_user.tar\mnt2\wireless\Library\CallHistory下的call_history.db中存放有系統的通話記錄檔，可以用sqllite工具查看

Table: call

New Record | Delete Record

	ROWID	address	date	duration	flags	id	name
1	1	+8615172320747	1328793499	456	5	-1	
2	2	15172320747	1328796301	128	4	-1	
3	3	+8615172320747	1328796858	3509	5	25	
4	4	18801168963	1328801073	2376	5	54	
5	5	+8615221580201	1328845470	29	5	47	

*

【效果展示】

通訊錄

在user.tar\mnt2\mobile\Library\AddressBook下的AddressBook.sqlitedb中存放著設備的通訊錄，可以用sqllite工具查看

File Edit View Help

Database Structure | Browse Data | Execute SQL

Table: ABMultiValue New Record Delete Record

	ecord_id	property	identifier	label	value
1	1	3	0	1	+8618271213159
2	2	3	0	1	13903527844
3	3	3	0	1	+8613083068102
4	4	3	0	1	15104048111
5	5	3	0	1	13517299442
6	6	3	0	1	13806669838
7	7	3	0	1	15821216138
8	8	3	0	1	13871085265
9	9	3	0	1	15872123792
10	10	3	0	1	13515963631
11	11	3	0	1	18621360376
12	12	3	0	1	13545295312
13	13	3	0	1	+8615021009715
14	14	3	0	1	13599399588
15	15	3	0	1	18602108331
16	16	3	0	1	13971349515
17	17	3	0	1	18672870045

*

【效果展示】

Browser書簽

在3gs_user.tar\mnt2\mobile\Library\Safari下的Bookmarks.db保持著流覽器的書簽，可以用sqllite工具打開查看

Database Structure | Browse Data | Execute SQL

Table: bookmarks

New Record | Delete Record

	e	title	url	num_children	editable	deletable	hidden
1	1	Root		10	1	1	
2	1	BookmarksBar		1	0	0	
3	0	hao123-－我的上	http://www.hao12	0	1	1	
4	1	BookmarksMenu		0	0	0	
5	0	手機騰訊網	http://info50.3g	0	1	1	
6	0	hao 123導航	http://m.hao123.	0	1	1	
7	0	網易郵箱手機智能	http://smart.mai	0	1	1	
8	0	ipad 破解遊戲	http://www.macre	0	1	1	
9	0	愛 APP - 專注限	http://www.iapps	0	1	1	
10	0	創意產品 - 創意	http://www.xiank	0	1	1	
11	0	樂視網-中國第一	http://m.letv.co	0	1	1	

*

【效果展示】

歷史訪問記錄

在3gs_user.tar\mnt2\mobile\Library\Safari下History.plist中可以查看流覽器的訪問歷史，直接用記事本即可打開查看

XML View

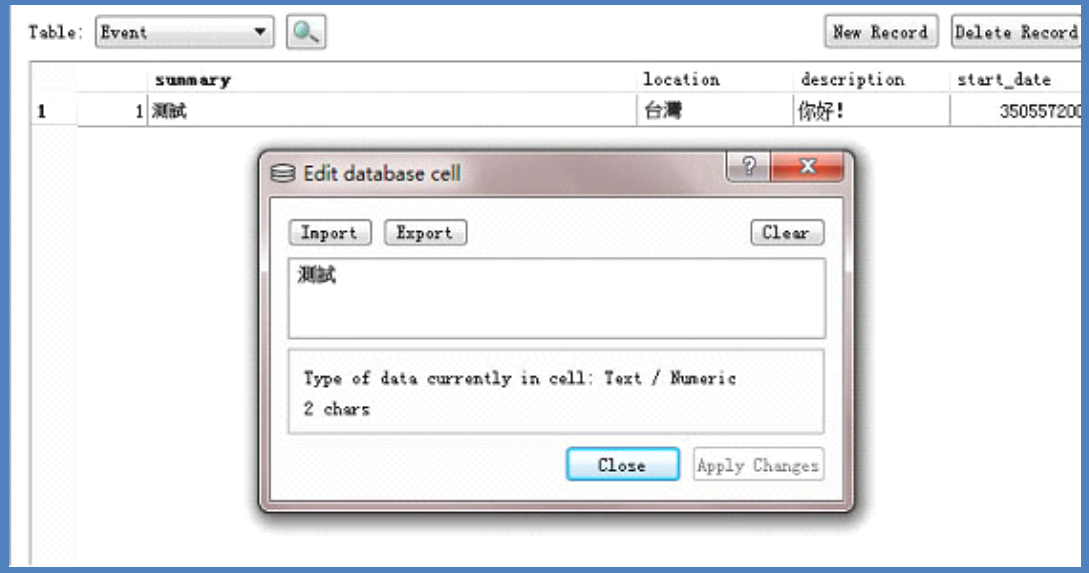
```
285        <array>
286            <string>http://info50.3g.qq.com/g/s?sid=AQHeBmLaDj93XEg_UOpUQGG7&amp;aid=index&amp;g_ut=3&amp;f=index&amp;g_f=6483</st
287        </array>
288        <key>title</key>
289        <string>手机腾讯网</string>
290        <key>visitCount</key>
291        <integer>1</integer>
292    </dict>
293    <dict>
294        <key></key>
295        <string>http://3g.sina.com.cn/</string>
296        <key>D</key>
297        <array>
298            <integer>1</integer>
299        </array>
300        <key>lastVisitedDate</key>
301        <string>350663858.4</string>
302        <key>title</key>
303        <string>手机新浪网</string>
304        <key>visitCount</key>
305        <integer>1</integer>
306    </dict>
```

*

【效果展示】

日曆

在3gs_user.tar\mnt2\mobile\Library\Calendar下的Calendar.sqlitedb檔中保存著系統的日曆檔，可以利用sqllite工具查看



*

【效果展示】

圖片和語音

❖照片和圖片

在3gs_user.tar\mnt2\mobile\Media下的DICM和photo中分別保存著相機照片和相冊檔，可以直接下載流覽

❖電子書和PDF檔

在3gs_user.tar\mnt2\mobile\Media\Books目錄下保存著epub格式的電子書和PDF檔，可以直接打開流覽

❖錄音檔

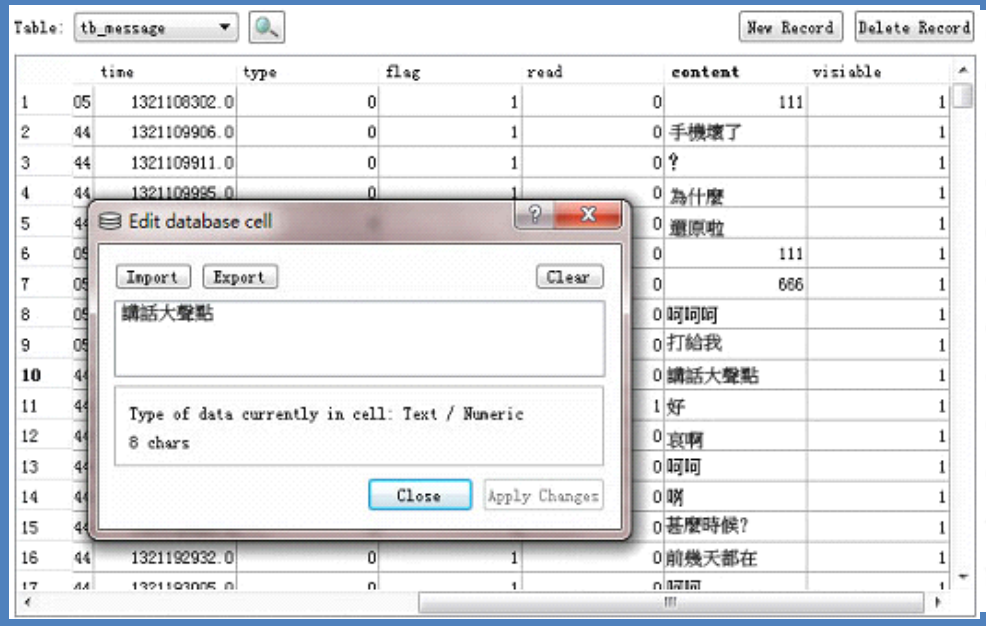
在3gs_user.tar\mnt2\mobile\Media\Recordings中保存著系統的錄音檔，可以直接打開；

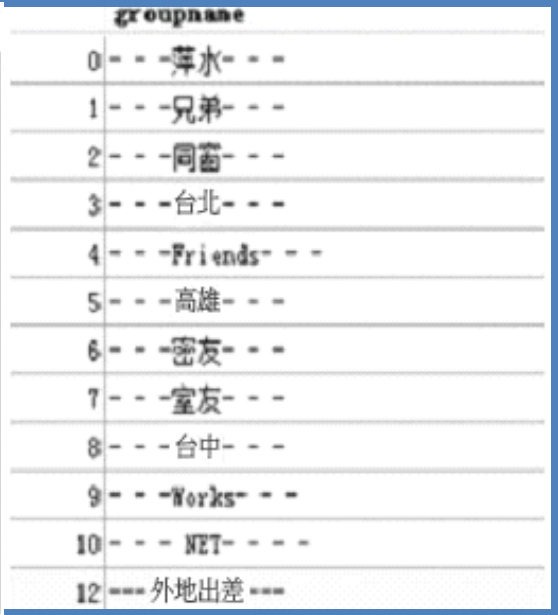
*

【效果展示】

QQ聊天記錄

3gs_user.tar\mnt2\mobile\Applications\D77E043F-0B98-4C3C-8520-A9CBBB5091B0\Documents\contents下的QQ號碼檔夾中保存著QQ的聊天記錄





*

【效果展示】

飛信密碼

3gs_user.tar\mnt2\mobile\Applications\F48E4B33-D9BE-4A4E-91C3-3EB4EF82555D\Library\Caches\com.tencent.qqmail下的cache.db中存放中郵箱的郵件資訊

XML View

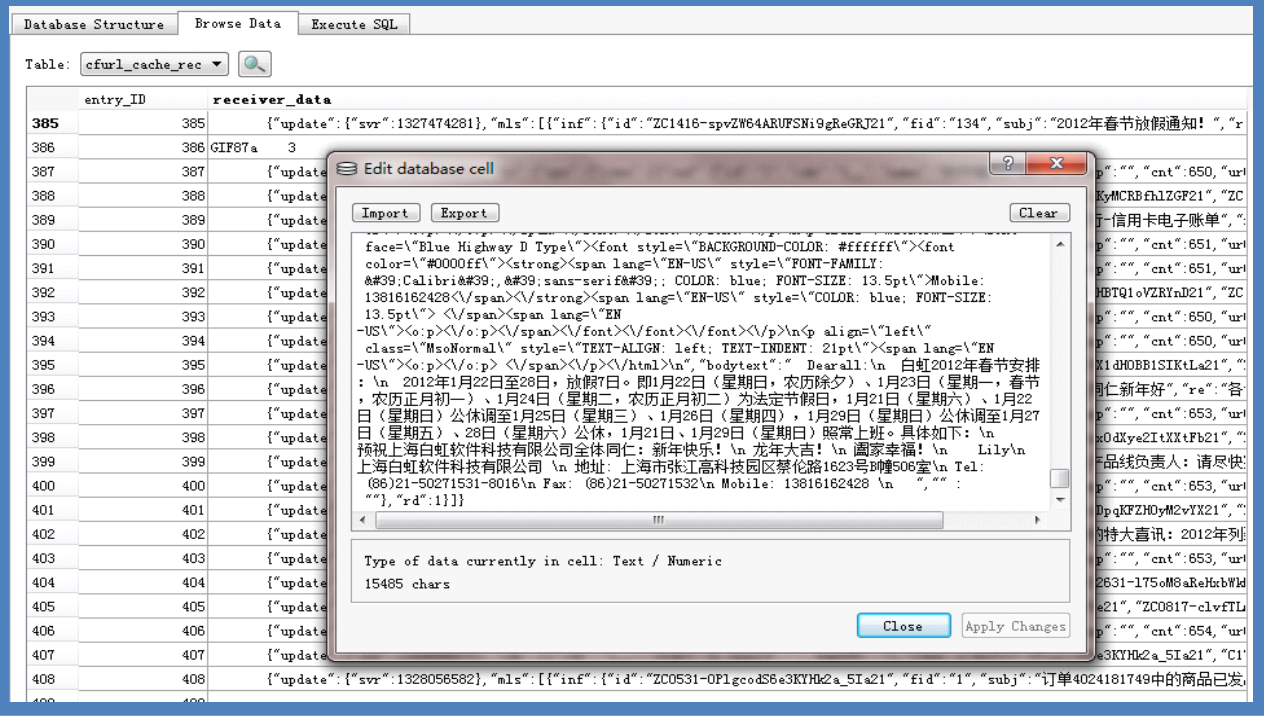
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>algrithm</key>
    <string>SHA1-sess-v4</string>
    <key>clientCnonce</key>
    <string>997581414</string>
    <key>keyValue</key>
    <string>BFD4E0E76087F557A4F0B53A9485CBBF2FADCFEB6711EEFB4698E5410071BF6E5146F6B10E6118B377E930117F8DC65028591ABE5BBA0CEA48F69CE27
    <key>psw</key>
    <string>a19881011</string>
    <key>reg2Data</key>
    <data>
    wMKASXBob251AIEyLjMuNACCd3JpdGVfbW9kaWZ5X291bVRhZwCKYXBuPTEA4sODNDAw
    MDE3AOPEg0YA5MXGhTAAhnY0ZGVmYXVsdADmx4UwAId2NGR1ZmF1bHQA5+XIyYM0MDAA
    iADp6MqFMADq0pNmZXRpb24uY29tLmNuO2kuc2hlcXUuMTAwODYuY24A8tWYMQCZMQCa
    MQD14A==
    </data>
    <key>response</key>
    <string>86094133989FD1EE20AF13FC703B5AADA8459036789E04A42165B4CAFF0758F9C19CDB1C63BF1D044BAA0BB635F64AEE1390287062B837333F6BDA22
    <key>sNonce</key>
    <string>6CC9935A32FF6BD16A4296D07D95EA63</string>
    <key>signature</key>
    <string>880BA29D1CD1BB2089DF60946716C6F0CCC4968707D7AD38C4BAF56A68895DCC658C36C973B2578B0F8EF696384EA7EA2679F348F271F7D177CCC936I
</dict>
```

*

【效果展示】

QQ郵件內容

3gs_user.tar\mnt2\mobile\Applications\F48E4B33-D9BE-4A4E-91C3-3EB4EF82555D\Library\Caches\com.tencent.qqmail下的cache.db中存放中郵箱的郵件資訊



*

【iPhone關鍵檔案位置】

文件路徑

/private/var/mobile/Library/AddressBook → 聯繫人
/private/var/mobile/Library/CallHistory → 通話記錄
/private/var/mobile/Library/SMS → 短信
/private/var/mobile/Library/Notes → 備忘錄
/private/var/mobile/Library/Safari → Safari 流覽器保存的書簽等
/private/var/mobile/Library/Mail → 電子郵件 還需備份
/private/var/mobile/Library/Preferences/com.apple.accountsettings.plist(郵箱設置)
/private/var/mobile/Library/Calendar→ 日曆
/private/var/mobile/Media/DCIM →照片裏面的膠捲（包括3GS攝像）
/private/var/mobile/Media/Photos →照片裏面的圖片
/private/var/mobile/Media/Videos →Cycorder攝像機軟體拍攝檔保存路徑
/private/var/root/Library/MMSApp →SwirlyMMS彩信管理 彩信資料夾
/private/var/mobile/Library/Preferences/com.apple.mobilephone.speeddial.plist →個人收藏（快速撥號）
/private/var/mobile/Media/Recordings→3系固件原生錄音檔

*

【免費索取方法】

下載連結