

數位鑑識與資料救援前瞻性研究

主講人: thx (張道弘)



什麼是數位鑑識？

- ✦ 數位鑑識也稱為電腦鑑識，是一門有效解決資通安全與電腦犯罪難題的科學。

其定義為：以一定程序保存、識別、抽取、記載及解讀電腦或網路媒體 ...。

- ✦ 數位鑑識以及偵查的方式，在案件的偵查，透過軟體並有流程，拿取一些儲存於儲存裝置，可有

司法單位所用的儲存媒體鑑識技術

- ✦ 使用：Encase，Winhex，R-Studio，FTK imager，Helix Live CD，純軟體做邏輯區分析處理。
- ✦ 資料讀取出來，純做數值運算，撈取資料。如果是主流 File System 現行商用軟體已非常成熟。技術公開透明。

數位鑑識技術生活化應用

以下狀況也會運用到數位鑑識技術，但無故以不正方法侵犯隱私知悉之他人秘密，即為妨害秘密罪

- ✦ 徵信社
- ✦ 商業或特務間諜
- ✦ 公司管理人員查詢使用者電腦行為

數位鑑識法理性流程

由於數位證據容易被修改，因此若要做為法律證物，要有一定流程，校驗程序以保障證物沒被修改。

在設計數位鑑識軟體上因此需加入

- ✦ 專案管理。
- ✦ 對每次數位證據操作有記錄。
- ✦ 對主數位證物檔有 HASH 記錄，以確保數位證據沒被修改。

困難度高的數位鑑識

基層的警員及偵查隊如需處理更高技術層次數位鑑識，須透過專門的偵查部門才有設備跟研究人員以進行取證，會嚴重影響到辦案進度，並且只有重大案件才能取用這些資源。

事實上，透過了解底層技術原理及運作模式，可用普通設備或軟體達到接近專業的效果。

高難度鑑識 :ATA 加密與解密

加密為 ATA 規範的一部分，用於保護硬碟資料。ATA 密碼長度為 32 位元，包括：User Password 和 Master Password (Master Password 僅用於解除 User Password 而並不會鎖住硬碟)。

ATA 密碼的設置是由 ATA Protocol "Security SetPassword" 指令組完成的。執行 Security Set Password 指令後，在硬碟下次重新啟動後密碼就會生效。

ATA Password 存在電路版上外也記錄在碟片模組上（在碟片上的故軀體+參數通稱為模組），因此更換電路版無法解密。

ATA 密碼保護的硬碟初始化 ATA 待命訊號正常,但僅回應有限的 ATA 指令，如設備識別型號指令，序號識別指令等等，但不允許

ATA 加密與解密

用戶如何判斷硬碟被設定 ATA 加密？

- ✦ 硬碟在 BIOS 中可以正確識別（包括型號，序列號，LBA 等等）。
- ✦ 所有的扇區都不可讀取（發生 ABRT 錯誤）。
- ✦ BIOS 可能會提示要求輸入密碼或者直接給出硬碟被密碼保護的訊息；當使用系統安裝碟或者 DOS 啟動碟讀取硬碟時會停止，並提示錯誤訊息，如 Xbox 1 一代的 8 GB Seagate 硬碟就啟用 ATA 加密，在一般電腦上必須解密才可使用。

解開 ATA 加密硬體設備

使用昂貴設備處理如 ACELab PC3000 UDMA

Acclab 由俄國 Таганрогского 無線電工程學院 ТРТИ
教授於 1991 成立，為最早逆向工程硬碟指令公司



使用一般軟體解開 ATA 加密

- ✦ 需要能直接發送ATA Command。HBA 需要關掉AHCI 模式.建議最好用IDE 硬碟介面控制卡。
- ✦ 軟體使用Victoria for windows + MHDD in dos可直接發送ATA Command 指令。

解開 ATA 加密

```
50 ERR INDX CORR DREQ DRSC WRFT DRDY BUSY FWD AMF TONE ABRT IDNF UNCK BBR 00  
[UDC WD1200BEVS-00RST2 ] [ 234,441,648 ] [ ] [ ]  
  
MHDD>cid  
UDC WD1200BEVS-00RST2 LBA:234,441,648 BIOS  
SN:MD-WKEX07318797 FW:00.01600 CACHE:8192KB  
Supports: LBA48 HPA AMN DLNC LBA HS16 DMA (UDMA6,NUMA2)  
SMART: Enabled SelfTest: Supported ErrorLog: Supported  
Security: high, ON. Size = 114473MB  
  
WARNING: THIS DRIVE IS LOCKED BY ATA PASSWORD  
  
MHDD>
```

| Take a screenshot : (F10) | 20:06:56

在MHDD下 顯示 硬碟已被加密

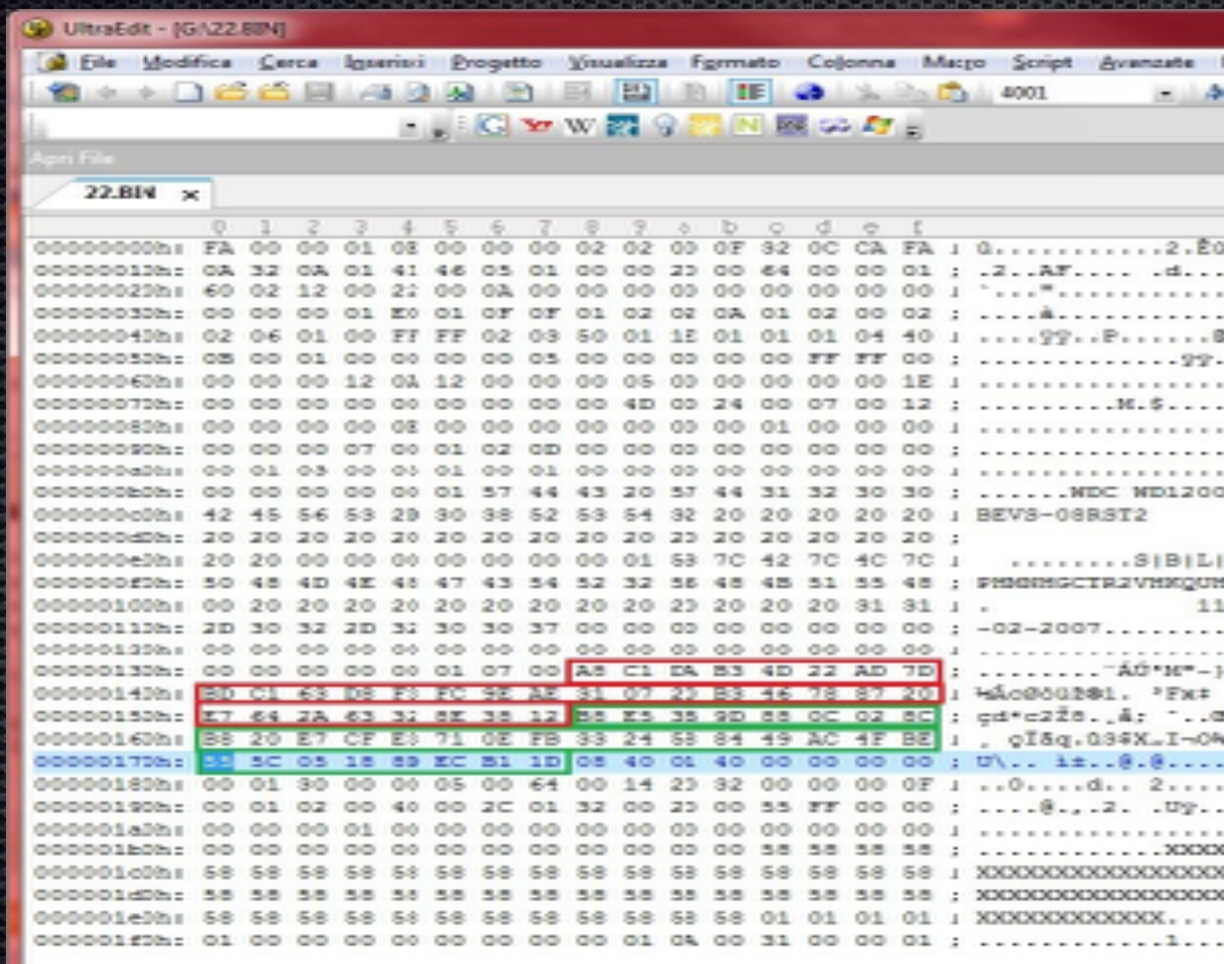
解開 ATA 加密

```
50 ERR INDX CORR DREQ DASC MKPT DADT BUSY PWD AMHF TDRF ADBT TDNF UNCR BDR 0
[WD0 WD1200MEUS-0BRSTZ ] [ 234,441,640 ] [ ] [ ]
Script: DUMP
-----
LINE 1: RESET
LINE 2: WAITBSY
LINE 3: REGS = $45 $0B $00 $44 $57 $A0 $00
LINE 4: WAITBSY
LINE 5: REGS = $06 $01 $0E $4F $C2 $A0 $00
LINE 6: WAITBSY
LINE 7: CHECKDRQ
LINE 8: SECTORSPROM = CS.BIN
LINE 9: REGS = $05 $01 $0F $4F $C2 $A0 $00
LINE 10: WAITBSY
LINE 11: CHECKDRQ
LINE 12: SECTORST0 = 21.BIN
LINE 13: REGS = $05 $01 $0F $4F $C2 $A0 $00
LINE 14: WAITBSY
LINE 15: CHECKDRQ
LINE 16: SECTORST0 = 22.BIN
-----
All done.
MHDD>
| MHDD 4.5 (c) Mulfon Postlewa | PREPARE | 20:07:0
```

執行如圖 ATA Command 指令集

產生出 21.bin 及 22.bin 兩個檔案此為硬碟模塊檔

解開 ATA 加密

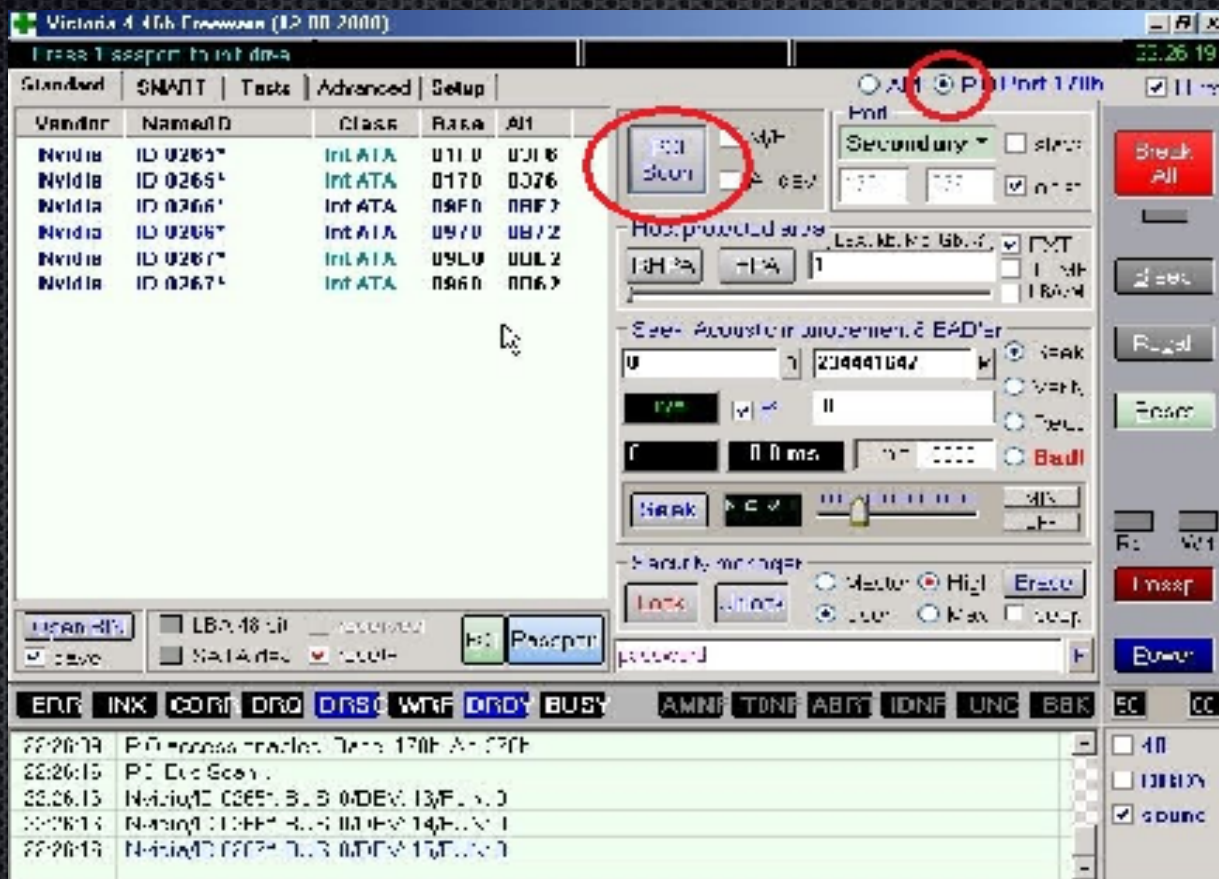


用 UltraEdit 打開 22.bin

解開 ATA 加密

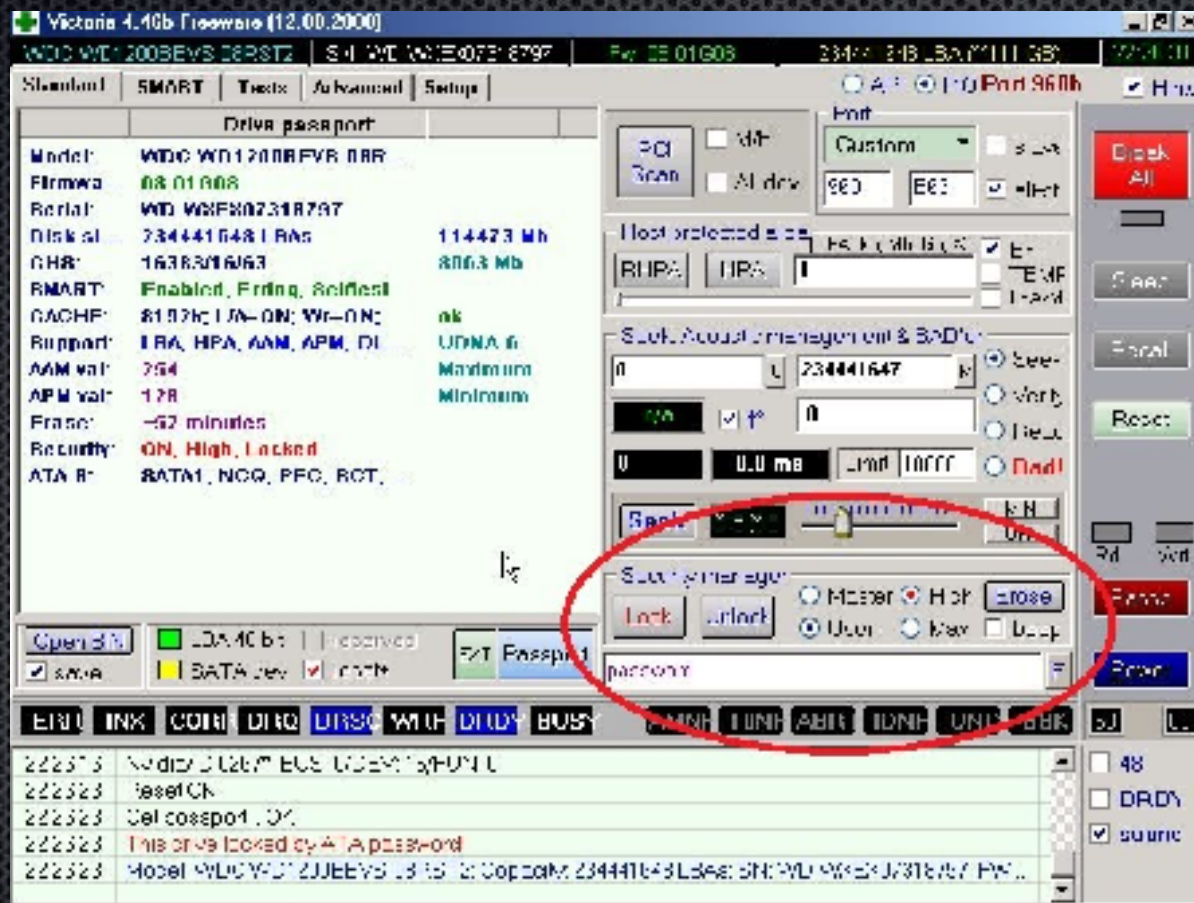
- ✦ 密碼起始位置可能不同，但排列與長度是相似。
- ✦ 0x137 偏移位置 07 指出 ATA 加密等級。
- ✦ 紅色區域為 User Password 使用者密碼。
- ✦ 綠色區域為 Master Password 主密碼。
- ✦ 選擇紅色+綠色區域並另存檔案。
- ✦ 執行 Victoria in Windows。

解開 ATA 加密



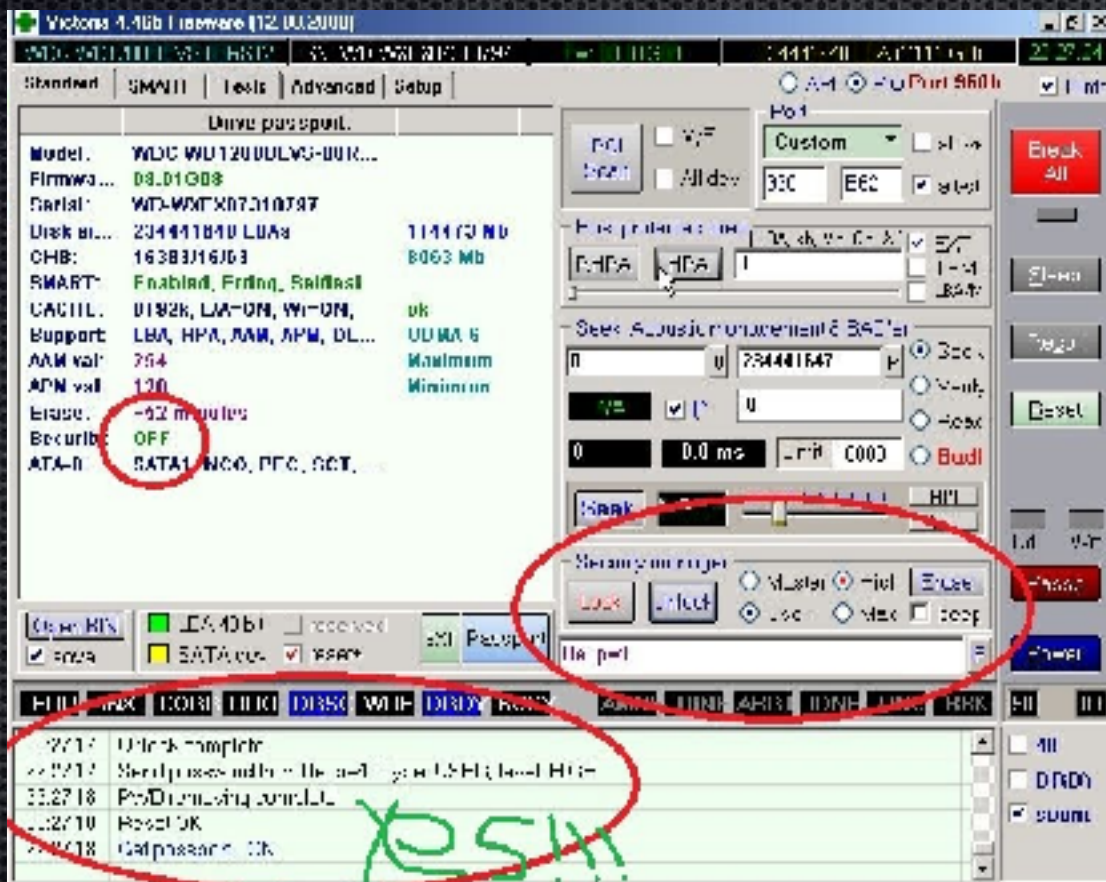
必需以PIO方式連接硬碟

解開 ATA 加密



點擊右下 F 鍵導入密碼檔

解開 ATA 加密



成功解除ATA Password

原理：28 bit ATA Command Set

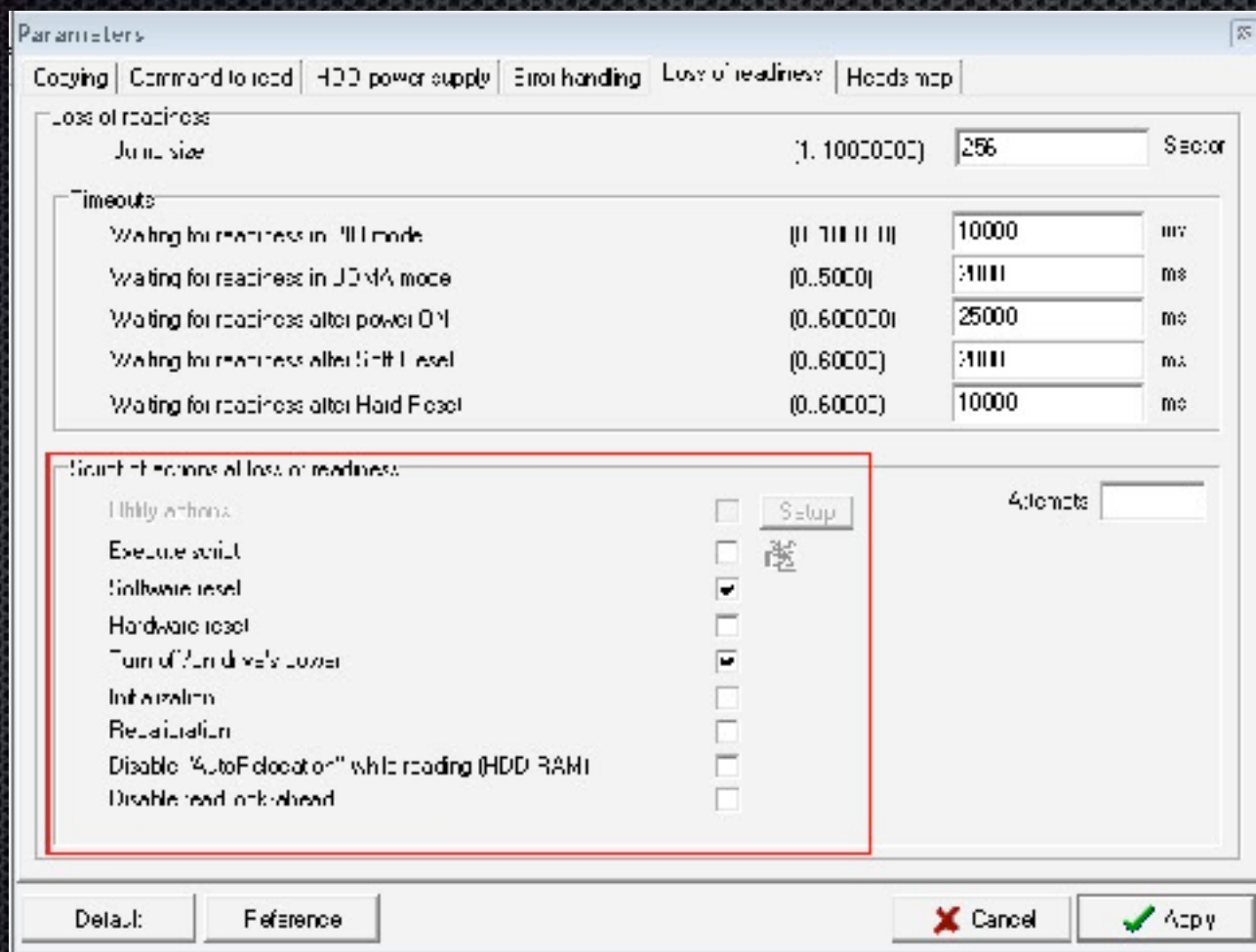
Word	Name	Description
00h	Feature	In ATA/ATAPI-7 this was the Feature register. Each transport standard shows how the Feature field is mapped for proper functionality. The transport documents also show how 28-bit commands are mapped differently from 48-bit commands.
01h	Count	In ATA/ATAPI-7 this was the Sector Count register. Each transport standard shows how the Count field is mapped for proper functionality. The transport documents also show how 28-bit commands are mapped differently from 48-bit commands.
02h	LBA	(MSB) In ATA/ATAPI-7 this was the LBA Low, LBA Mid, LBA High, and Device (3:0) Registers. For many commands this is the address of first logical sector to be transferred. Bits 47:28 shall be cleared to zero for 28 bit commands. Each transport defines how these 48-bits are mapped to the appropriate fields or registers. (LSB)
03h		
04h		
05	Device	In ATA/ATAPI-7 this was the Device register. This standard includes bits 3:0 of the ATA/ATAPI-7 Device register as a part of the LBA field. Each transport standard shows how the Device field bits 7:4 are mapped for proper functionality
	Command	Bit 7:0 - The command number goes here.

數據恢復資料數據導引

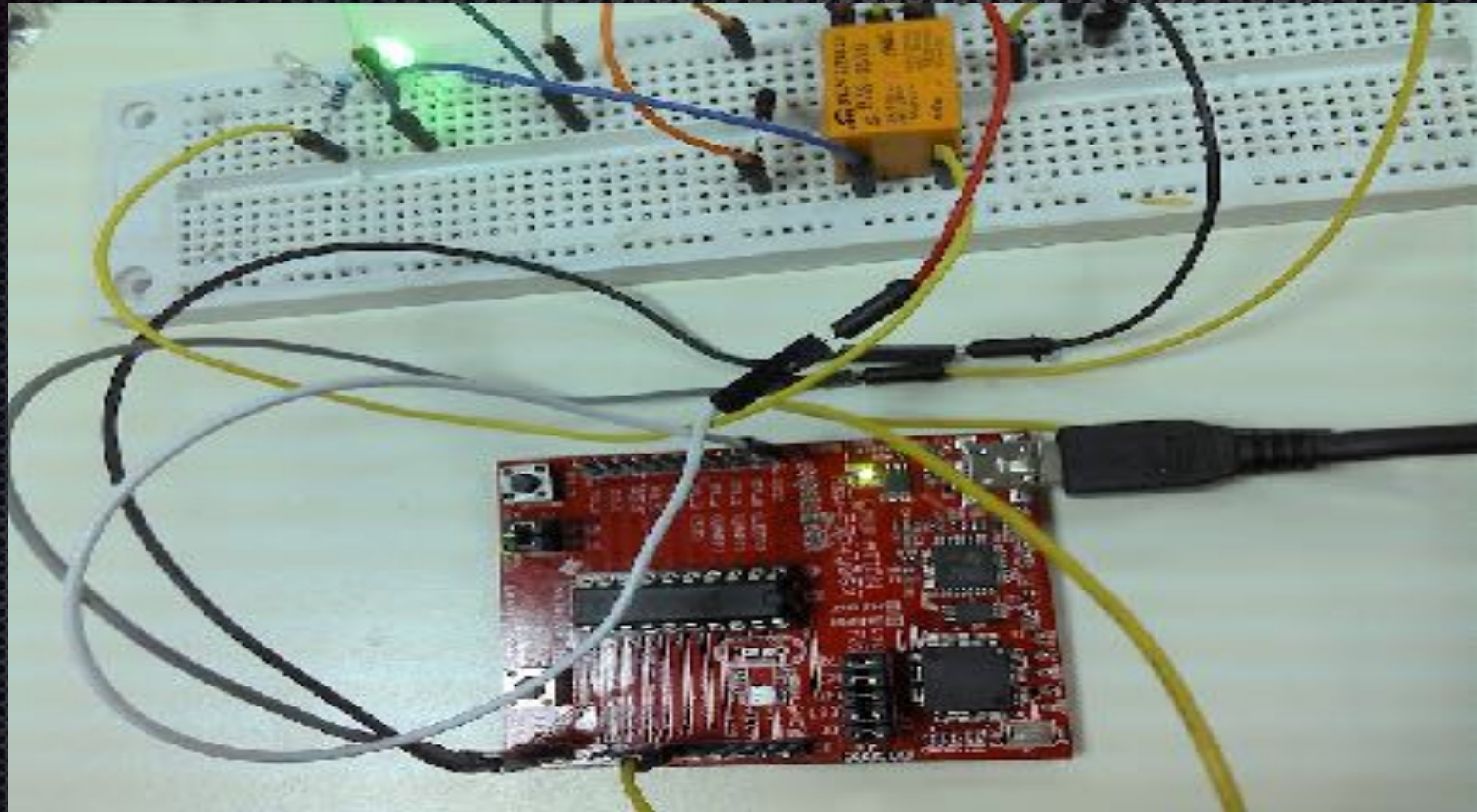
對於讀取不良的硬碟，通常需要專業的數據導出設備才能達到目的，主要概念為跳過不可讀出的區域。有下面幾種方法：

- ✦ ATA Hardware Reset
- ✦ ATA Software Reset
- ✦ Power Reset
- ✦ 磁頭區 Zone 計算，可關閉不正常讀寫頭運作

UDMA DE 強拷資料操作畫面



強拷機自製硬碟斷電電路



自行撰寫強拷程式

```
// Get pid
$pr = proc_get_pid($proc);
$pid = $pr['pid'];

$watched = array($pipes[1]);
$null = null;
stream_set_blocking($pipes[1], false);
while({$changed = stream_select($watched, $null, $null, 5)} != false) {
    $watched = array($pipes[1]);
    if ($changed != 1)
        continue;

    $data = stream_get_contents($pipes[1]);
    echo $data;
    if (preg_match('/ successful read:\d+[1-9]+\d+$/', $data))
    {
        posix_kill($pid + 1, SIGINT);
        exec('killall -s SIGINT adrescue');
        exec('killall -9 blkid');
        echo date(DATE_RFC1036) . " - Hardware failure detected! MUST RESET!\n";
        exec('notify-send "Saving data" "Hard disk must be restarted to continue" -u critical -i system-shutdown');
        break;
    }
}

echo "          ... stopping adrescue ({$pid}) ";
fclose($pipes[0]);
```

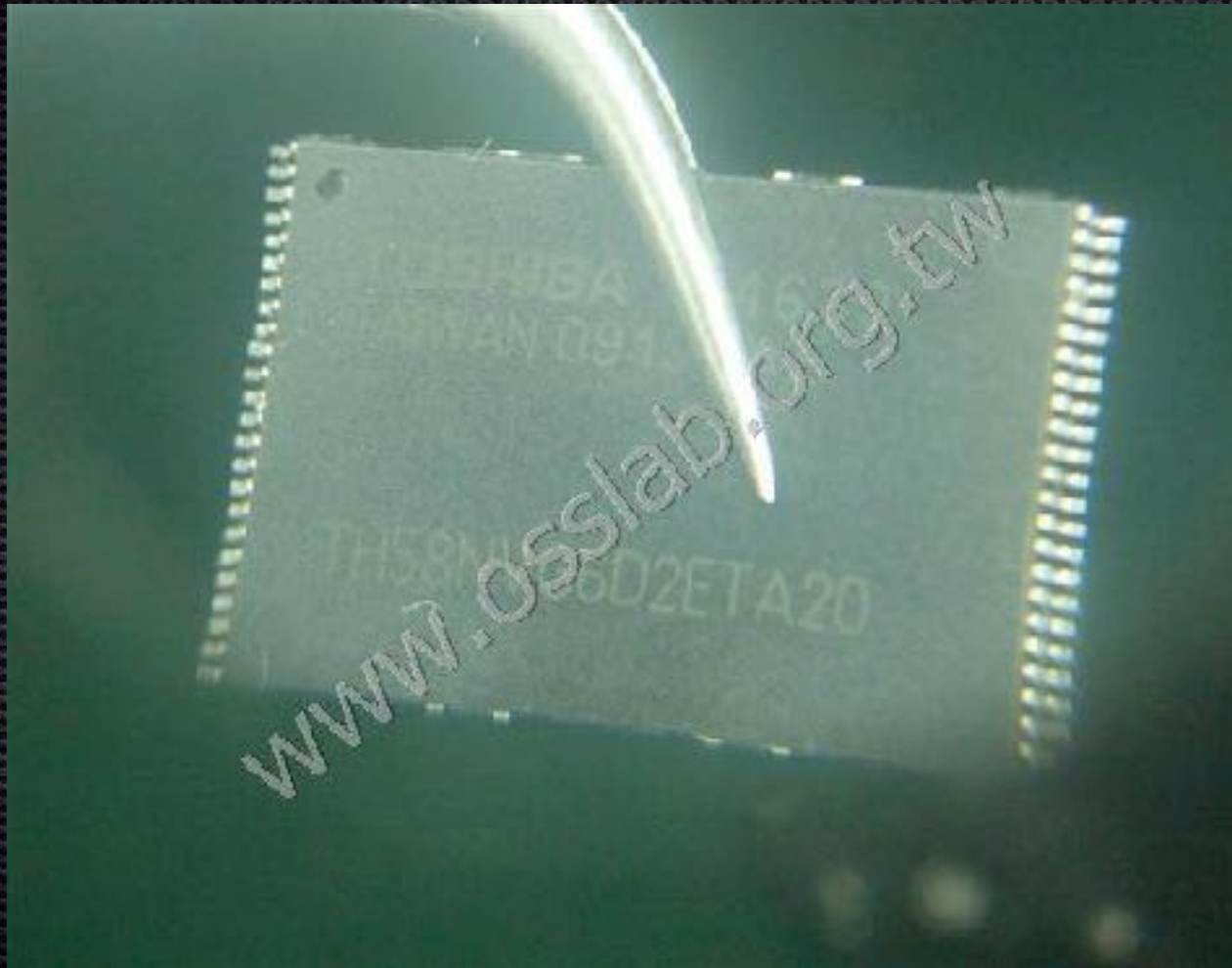
Flash 資料救援取證



SD Card PCB 板



8GB Nand Flash



將晶片放入編程器



iOS 數位鑑識方法與原理

蘋果公司的 iOS 產品相當熱門，且市占率較高，所以在數位鑑識以及蒐證時常常會遇到這類設備，由於蘋果IOS為封閉式的系統，相較於 Android 系統在取證上以及破解上難度較高。

iOS 文件分區系統

HFS+ (HFS PLUS) 是蘋果公司為蘋果公司為他們的分層檔系統 (HFS) 開發的一種檔案系統，主要運用於蘋果電腦 (Mac OS)



System分區為系統分區，大小為1G左右，主要



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 之前的硬體則沒有加密硬體。

iOS Raw Disk 的加密

在 iOS 4 + A4 CPU 之後，有鑑於安全考量，蘋果對於 NAND Flash 做了扇區 AES 加密。

解密前

```
$ hexdump -C mobile/Library/SMS/sms.db | head
00000000 09 7d b1 05 48 b1 bb 6d 65 02 1e d3 50 67 da 3e |.)..H..me...Pg.>
00000010 8c 99 cb 3c 9f 41 fa c7 91 c4 10 d6 b2 2f 21 b2 |n..<.A...../!.
00000020 39 87 12 39 6d 5c 96 7d 4a bd a1 4a ea 49 ba 40 |9..9m\.)J..J.I.G
00000030 96 53 c4 d3 81 0d 6e 73 98 6c 91 11 db e0 e2 3d |.S.....s.l.....=
00000040 7a 17 82 35 18 59 fb 17 1a b2 51 89 fc 8b 55 5a |z..5.Y....Q...Uz
00000050 9b 04 a0 d6 2d d5 8a 6c e8 ad 65 df ea b4 a8 8b |.....-..j!..e.....
00000060 7e de c1 d2 b2 8a 30 e9 84 bb 09 9a 58 9a ad ba |^.....C.....X...|
00000070 bb ba b1 9e 2a 95 67 d7 be a1 4b a7 de 41 05 56 |.....*.q...K..A.V
00000080 ca 4e 8b d6 3a 57 4a d2 76 4e 67 c0 8b 10 45 c9 |.N.:NE.VNg...E.
00000090 7b 2a c3 c9 11 f4 c5 f0 56 8f 86 b7 46 fe 56 e8 |{^.....V...P.V.
```

解密後

```
$ hexdump -C mobile/Library/SMS/sms.db | head
00000000 53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 |SQLite format 3.
00000010 10 00 02 02 00 40 20 20 00 00 00 02 00 00 00 01 |.....@ .....
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....
00000030 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |.....
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....
00000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 |.....
00000060 00 2d e2 1f 0d 00 00 00 00 10 00 00 00 00 00 |.-.....
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....
```

iOS 鑑識軟體原始碼

不管是 5 ~ 40 萬數位鑑識軟硬體都是使用

Sogeti 研究室的 iPhone data protection 自由軟體專案

專案位置

<http://code.google.com/p/iphone-dataprotection/>

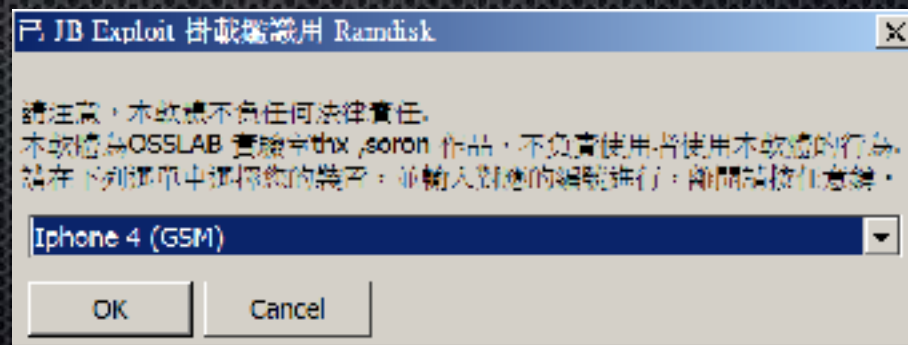
可自由下載

加載 Ramdisk

由於原始 iOS kernel 有加密 AES 加密核心。

目前 iOS A4 CPU 之前機種，由於有 bootrom exploit，因此可使用自定 Kernel 啟動後做 NAND Disk Image Dump 與分析破解。

iOS 設備進入 DFU 模式之後，會自動呼叫出 Redsn0w 軟體，Redsn0w 會對 DFU 模式下做 bootrom exploit，就可掛載 ramdisk。不同的設備，所需 RAM DISK 也不同，軟體已經簡化，圖形選擇正確的型號之後便可，ramdisk 掛載完成後，iOS 設備



A4 CPU 獲取檔鏡像

iOS 設備進入定製 Kernel RAM DISK 開機後，就可對系統做直接操作。User 分區包含了大量的用戶個人資料，因此是取證的主要獲取對象。

iOS 4之後，User 分區的檔都是加密的，解密這些檔所需要到的金鑰都必須從這臺設備裏面獲取。

iPhone 3G 之前的設備沒有加密硬體，所以即使 iPhone 3G設備

Key 和 Keychain

擷取加密金鑰和 keychain data

設備進入 DFU 模式，掛載 Ramdisk後 提取 key 和 keychain data。

iOS 設備進入 DFU 模式之後，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，我們將可以獲得以下資訊：

iOS 密碼：可以透過暴力破解來獲得密碼。

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

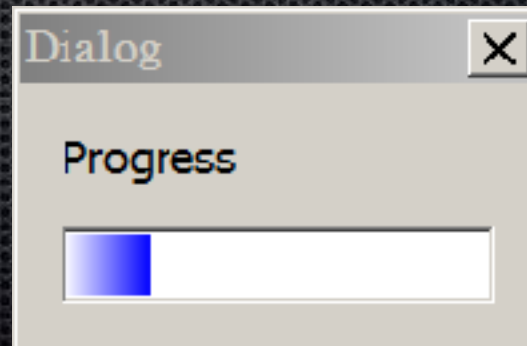
win xp： %ALLUSERSPROFILE%\Application Data\Apple\Lockdown\

win 7： %ALLUSERSPROFILE%\Apple\Lockdown\

暴力密碼破解

加載ramdisk後執行暴力破解程式可恢復設備的密碼。

iOS設備進入DFU模式，確定 Ramdisk 已加載成功後，主選單上選擇，設備的密碼恢復操作開始，程式將會常識恢復 4 位數純數字簡單密碼，恢復 4 位數的純數字所需要的時間一般不超過 10 到 30 分鐘，取決於設備的類型。



鏡像解密

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。



數位鑑識軟體開發思維

此為某位講者開發商業軟體操作說明 ,前線調查人員會有辦法熟練應用?

```
./win32/itunnel_mux.exe --decrypt --wtf common/WTF.8900 --  
ibss
```

```
common/iBSS.n82 --kernelcache common/kernelcache.n82 --  
devicetree
```

```
common/DeviceTree.n82 --ramdisk common/ramdisk-4.dmg  
.\win32\ssh.exe -c null -m hmac-md5-96 -p 2022 root@localhost  
dd
```

```
bs=1M if=/dev/rdisk0s1s1 | .\win32\dd.exe bs=1M of=output-file  
--
```

數位鑑識軟體開發思維

就算使用 DOS，執行批次檔也能符合簡易使用的需求



```
系統管理員: IOS forensic Tools for Win V0.2 beta powered by OSSLab soron and Thx
IOS forensic Tools for Windows V0.2 beta
By thx@oss-lab.com.tw from Taiwan
soron255054@hotmail.com   soron<凌羽> from Taiwan
http://www.oss-lab.com.tw

special thanks   jean.sig   and   jb security labs

-----
                MENU
-----

1  以JB exploit進行鑑識Hootdisk 載入
2  掛載usb 終端ssh port
3  開始進行暴力破解
4  對IOS手持裝置鏡像
5  進行IOS鏡像解密恢復被刪檔案
6  結束本程式(EXIT)

請選擇你要進行的動作:
```

數位鑑識軟體開發思維

改以 wx python 開發批次
檔直接轉譯，

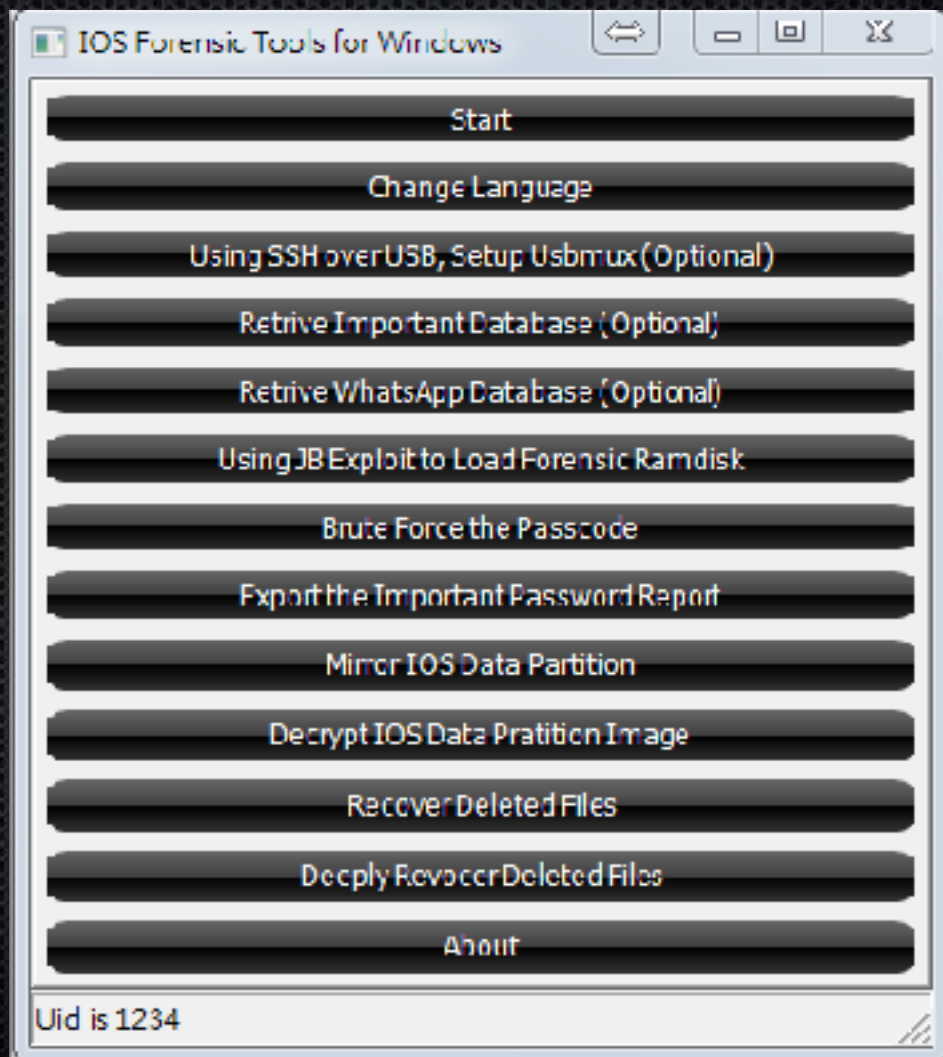
可看到大部分都是相同的
選項。



數位鑑識軟體開發思維

再修正版增加了許多功能：

- ✦ 專案建檔與管理多語系的支援。
- ✦ 免暴力破解，快速讀取重要資訊。
- ✦ Whatsapp 讀取解密。



WIFI 與 Apple ID

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：

```
password.txt - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
-----
Passwords
-----
Service : 3837A7F1-SCH9-403A-AB07-ED467BD204D7
Account : guest
Password :
Agrp : apple
-----
Service : push.apple.com
Account :
Password : <binary data> : 7c7f3532ef27a72b2c59f3a033a8c488e394030a68286a35a89e48e0690a18dc
Agrp : com.apple.push
-----
Service : AirPort
Account : south 3f
Password :
Agrp : apple
-----
Service : AirPort
Account : tel
Password :
Agrp : apple
-----
Service : AirPort
Account : sji.ta
Password :
Agrp : apple
```

```
password.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 : KMPCAutKCredentialConsumerKey
Password : tz3yU2P4cYJ1VLG67a1wfg
-----
Server : imap.gmail.com:143
Account : dt11111@gmail.com
Password :
-----
Server : smtp.gmail.com:25
Account : dt11111@gmail.com
Password :
-----
Server : api.openfeint.com:0
Account : KMPCAutKCredentialConsumerKey
Password : (aANQ/s/3cDwQ)v/r0vjlg
-----
Server : api.openfeint.com:0
Account : KMPCAutKCredentialConsumerKey
Password : hPgFiu4eSHPy2L7kdY2f3g
-----
Server : api.openfeint.com:0
Account : KMPCAutKCredentialConsumerKey
Password : 43U7XVZQSAVQ0y3yAa0Khw
```


用戶如何判斷硬碟被設定 ATA 加密？

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

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
3 <plist version="1.0">
4 <dict>
5 <key>DerivedKeys</key>
6 <dict>
7 <key>1101</key>
8 <data>
9 4nRkLHDeMaqIBmzSaeGq-u==
10 </data>
11 <key>1101</key>
12 <data>
13 ucq84a3E5JzWpkvaIXHldu==
14 </data>
15 <key>1104</key>
16 <data>
17 dHTxHX4/QHvzfm8EALjGUQ==
18 </data>
19 <key>2201</key>
20 <data>
21 QiLO7yHDq/CVvq/WFG6P7Q—
22 </data>
23 <key>2202</key>
24 <data>
25 vakiD7ZuRz204WDSL98L0Q—
26 </data>
27 <key>2203</key>
28 <data>
29 4SRBqzIbtwIRowPDuUoSt&—
30 </data>
31 </dict>
32 <key>EffaceableStorage</key>
33 <data>
34 a0w0RDFHQUI&R0FC1B0NLjQLF/4/SQ4LmqCuDpyqBVMJRLIP0N67Q5uZdG64J59&7hSP
35 8qtqhqJR20wCw0w&HL1&8DuG18JwCuTREDhy6SP2wBFWL4QSt39&vQH5A-Tly&Kw&uP
36 CTQ&uR&R&0w&ACFCT&Ug&AAAA&06J&DyUH&uU1&e2hPNTL/FSy&wEPK&w1bbI&JZ&w&B&
```

AFC

iOS 上運作的 AFC (Apple File Connection) 服務是從 iPod (2001) 時代就有的,其協定為 usbmux

越獄後程式會對 iOS 啟動增加名為 AFC2 服務
為了求整個系統掌控權，

AFC2 會修改

/System/Library/Lockdown/Services.plist

增加 root 權限

JB 後對 AFC 的影響

iOS 裝置在越獄後檔案系統權限取得最大

可以使用 AFC 直接拉取 iOS 整個檔案權限 並且鎖屏密碼也無效

下面為重要的個人資料檔案

/private/var/mobile/Library/AddressBook → 通訊錄

/private/var/mobile/Library/CallHistory → 通話記錄

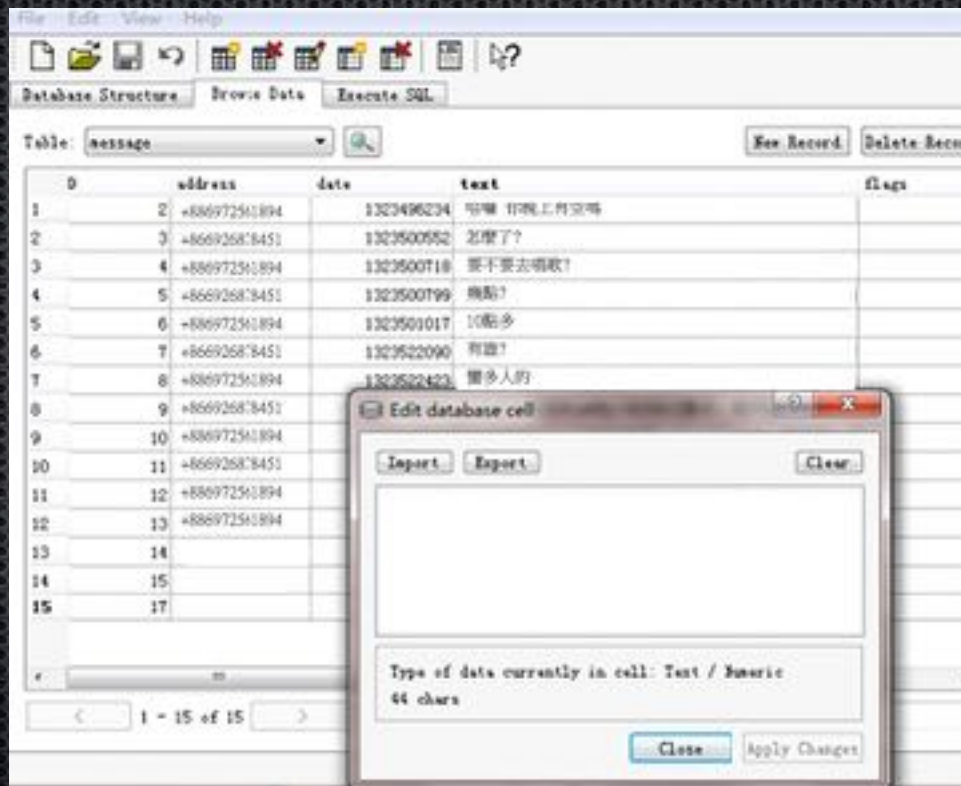
/private/var/mobile/Library/SMS → 訊息

/private/var/mobile/Library/Calendar → 日曆

因為越獄後 AFC2 服務就會自動啟動，不需要額外裝 cydia 套

SMS

在 /private/var/mobile/Library/SMS 目錄下的 sms.db 中存放著設備的短資訊，可用 sqlite 工具查看



The screenshot shows a database browser window with a table named 'message'. The table has columns for ID, address, date, text, and flags. The data is as follows:

ID	address	date	text	flags
1	+886972501894	1323496234	智障 打個上打空嗎	
2	+866926878451	1323500952	怎麼了?	
3	+886972501894	1323500718	要不要去唱歌?	
4	+866926878451	1323500799	地點?	
5	+886972501894	1323501017	10點多	
6	+866926878451	1323522090	有誰?	
7	+886972501894	1323522423	蠻多人的	
8	+866926878451			
9	+886972501894			
10	+866926878451			
11	+886972501894			
12	+886972501894			
13				
14				
15				

An 'Edit database cell' dialog box is open, showing the current cell's data type as 'Text / Numeric' and its length as '44 chars'. The dialog has 'Import', 'Export', and 'Clear' buttons at the top, and 'Close' and 'Apply Changes' buttons at the bottom.

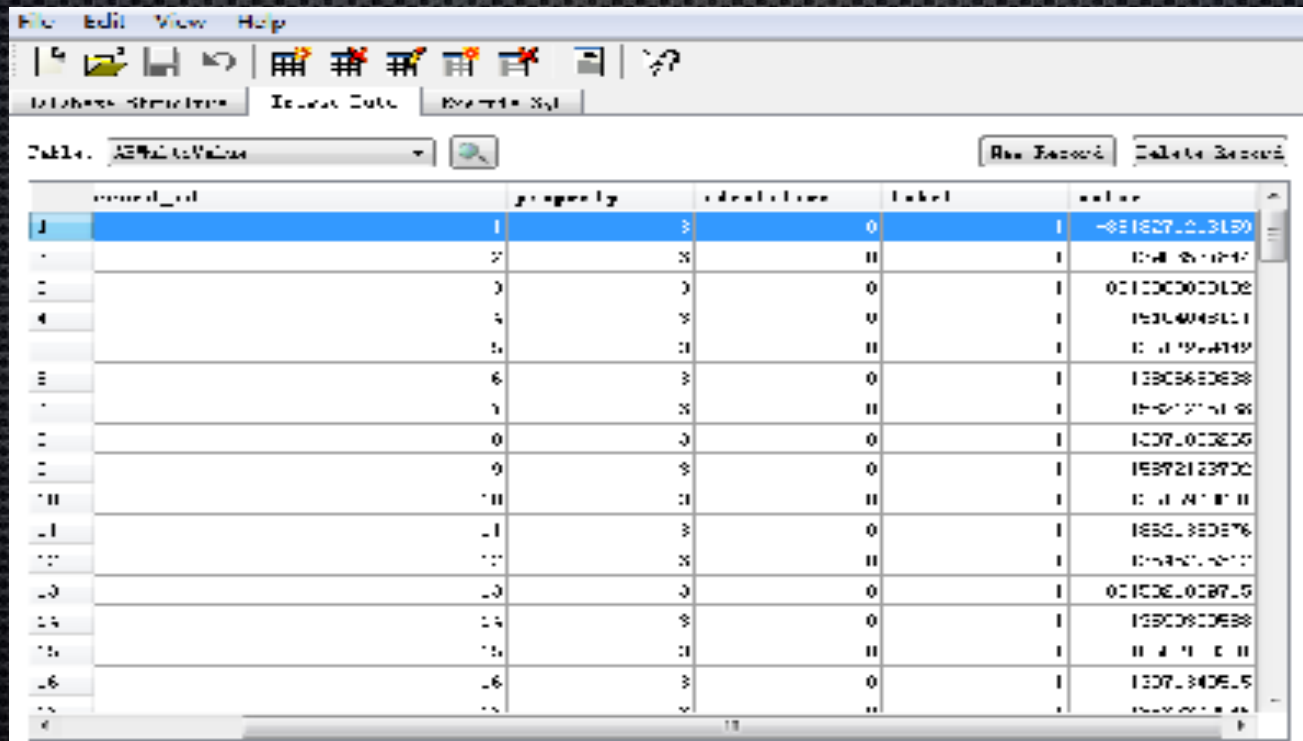
通話記錄

在 /private//var/wireless/Library/CallHistory 下的 call_history.db 中存放有系統的通話記錄檔，可以用 sqlite 工具查看

ROWID	address	date	duration	flags	id	name
1	+8615172320747	1328793499	456	3	-1	
2	+8615172320747	1328796001	190	4		
3	+8615172320747	1328796858	3500	3	25	
4	+8615221580201	1328801013	2376	3	-4	
5	+8615221580201	1328845470	29	3	17	

通訊錄

在 /private//var/mobile/Library/AddressBook 下的 AddressBook.sqlitedb 中存放著設備的通訊錄，可以用 sqlite 工具查看

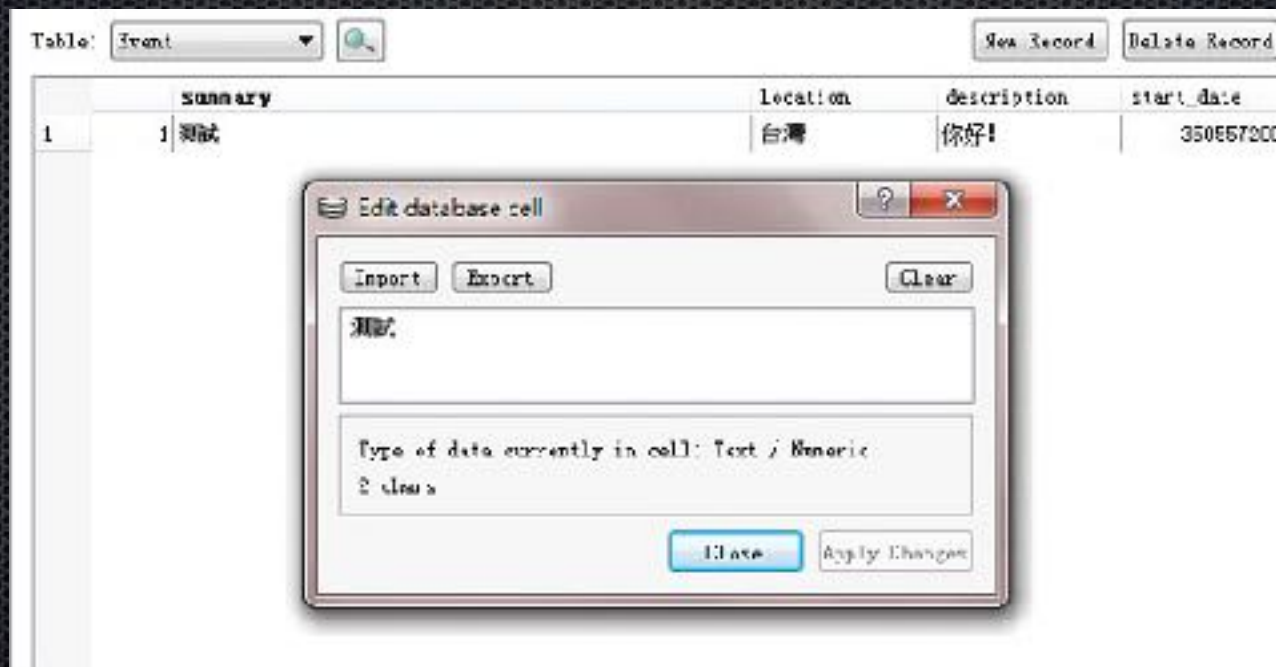


The screenshot shows a SQLite database viewer interface. The table name is 'AB%AddressValues'. The columns are 'rowid', 'group_id', 'index', 'label', and 'value'. The data is as follows:

rowid	group_id	index	label	value
1	1	0	1	081827.0.3159
2	2	0	1	074 810247
3	3	0	1	001000000000
4	4	0	1	1506048011
5	5	0	1	0 0 1924149
6	6	0	1	1390680688
7	7	0	1	1507270196
8	8	0	1	1007_000000
9	9	0	1	15972123900
10	10	0	1	0 0 1 1 1 1 1 1
11	11	0	1	1650_300076
12	12	0	1	074801_0011
13	13	0	1	001000_0000_0
14	14	0	1	1390680688
15	15	0	1	0 0 1 1 0 1 1
16	16	0	1	1007_3400_5

日曆

在 `/private//var/mobile/Library/Calendar` 下的 `Calendar.sqlitedb` 檔中保存著系統的日曆檔，可以利用 `sqlite` 工具查看



瀏覽器書籤

在 /private/var/mobile/Library/Safari 下的Bookmarks.db 保持著
瀏覽器的書籤，可以用 sqlite 工具打開查看



The screenshot shows a SQLite browser window with the following interface elements:

- Navigation tabs: structure, Browse & Search, Execute SQL, DB Settings
- Table name: bookmarks
- Buttons: Search (H), Show All, Add (A), Duplicate (P), Edit (E), Delete (L)
- Table columns: id, special..., parent, type, title, url, num ch..., editable
- Table data (rows 12-22):

id	special...	parent	type	title	url	num ch...	editable
12	0	11	1	yamaha		0	1
13	0	12	0	功學社音樂網站	http://www.khs-music.com.tw/index.htm	0	1
14	0	12	0	功學社音樂網站 2	http://www.khs-music.com.tw/index.htmSyncId=8E5D...	0	1
15	0	12	0	山葉鋼琴廠原廠研討新行	http://www.yamahapiano.com.tw/frame7.htm	0	1
16	0	12	0	山竹樂器網站首頁	http://www.yamahomusic.com.tw/SyncId=567F9EE5 ...	0	1
17	0	12	0	功學社山竹樂器廠與國產樂器網站	http://www.yamaha-mt.org.tw/SyncId=D089E5E9-07...	0	1
18	0	12	0	山竹樂器網站首頁	http://www.yamahomusic.com.tw/	0	1
19	0	12	0	功學社山竹樂器廠與國產樂器網站	http://www.yamaha-mt.org.tw/	0	1
20	0	11	1	學校		5	1
21	0	20	0	新竹國英小學	http://www.hsps.hc.edu.tw/	0	1
22	0	20	0	新竹國英小學 2	http://www.hsps.hc.edu.tw/SyncId=41E1230B-3DF7 5...	0	1

瀏覽歷史紀錄

在 /private/var/mobile/Library/Safari 下 History.plist 中可以查詢網頁瀏覽器的瀏覽紀錄，直接用記事本即可打開查詢

```
2/</dict>
<dict>
  <key></key>
  <string>http://www.google.com.tw/url?sa=t&source=web&cd=4&
  <key>D</key>
  <array>
    <integer>1</integer>
  </array>
  <key>lastVisitedDate</key>
  <string>362113495.9</string>
  <key>redirectURLs</key>
  <array>
    <string>http://iphone4.tw/forums/showthread.php?t=181818</string>
  </array>
  <key>title</key>
  <string>[求助] 備份了，回復後~可是照片全消失了!!有辦法救回來嗎??</string>
  <key>visitCount</key>
  <integer>1</integer>
</dict>
```

圖片和語音

- ✦ 照片和圖片

在 `/private/var/mobile/Media` 下的 `DICM` 和 `photo` 中分別保存相機照片和相冊檔，可直接下載瀏覽

- ✦ 電子書和PDF檔

在 `/private/var/mobile/Media/Books` 目錄下保存著 `epub` 格式的電子書和 `PDF` 檔，可以直接打開瀏覽

- ✦ 錄音檔

在 `/private/var/mobile/Recordings` 中保存著系統的錄音檔，可以直接打開

What's App 解密

2012-01-08 17:24:15	[REDACTED]	及備份... 備份... 95WAK99
2012-01-08 17:25:30	[REDACTED]	Agaib
2012-01-08 18:55:21	[REDACTED]	你到了?
2012-01-09 09:56:00	[REDACTED]	有做出?
2012-01-09 09:58:37	[REDACTED]	有耶，但那是從外接的 ntfs 格式拉出來的，然後件事那兒也有另外一半找到，還在記憶卡裡這樣。
2012-01-10 21:37:48	[REDACTED]	G6 似乎沒辦法去插那張 iSCSI 卡。
2012-01-10 21:46:04	[REDACTED]	另外，我還要多拿一個usb外接盒，及帶一個60g硬碟。
2012-01-10 23:15:22	[REDACTED]	Intel 網卡被掉 換上boardcom 2 port or boardcom 1 port 這在塑膠櫃內
2012-01-10 23:17:39	[REDACTED]	 Image
2012-01-10 23:17:51	[REDACTED]	Ok
2012-01-10 23:19:20	[REDACTED]	把 G6 的 iSCSI 換掉?
2012-01-10 23:20:12	[REDACTED]	還是 i7 上的?
2012-01-10 23:25:24	[REDACTED]	開機了。
2012-01-10 23:39:08	[REDACTED]	我走囉。

充電器可能暗藏陷阱

既然IOS 取證程式在 Windows 下工作正常, 我們研究是否能在 embedded system 上工作.

當已越獄 iOS 行動裝置插上偽充電器 (實際是 embedd system)

在"充電"時, 此系統就會自動把重要資料如通訊錄, 簡訊, 連絡人, whatsapp 記錄等備份在 embedded 設備內

使用一般電腦上瀏覽器 再連入此"充電器" 直接觀看所有記錄。



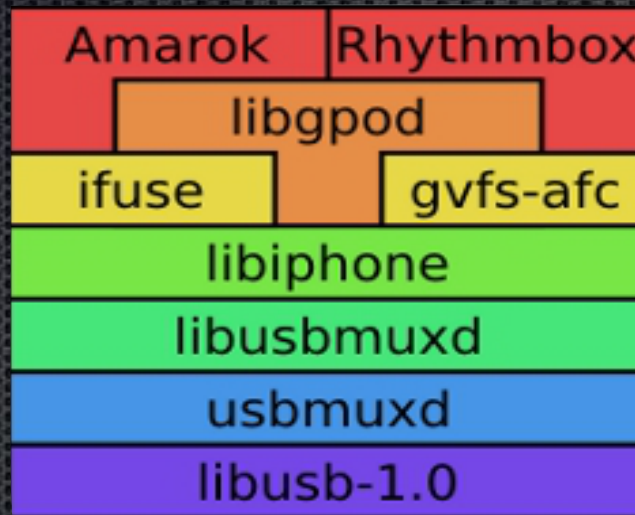
被刪檔案的恢復

Per file encryption extension added to the HFS filesystem in iOS 4. Each file gets a unique file key used to encrypt its data fork. File keys are stored (wrapped) in an extended attribute named `com.apple.system.cprotect`.

libimobiledevice + usbmuxd

使用迷你嵌入式系統偽裝充電器

工作原理:



本演講的部份程式碼,與詳細原理

歡迎到 <http://www.osslab.com.tw/> 參考

