數位鑑識與資料救援前瞻性研究

主講人: thx (張道弘)

http://www.osslab.com.tw/

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，可有助於案情釐清以及曝光。

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

此外以下狀況也會運用到數位鑑識技術
但是要注意法律: 無故以不正方法侵犯他人隱私
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
家長調查查詢家庭小孩電腦行為

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
1.專案管理.
2.對每次數位證據操作有記錄
3.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

基層的警員以及偵查隊需要做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才能進行取證，會嚴重影響到辦案進度及只有重大案件才能用上這些技術.

實際上 如果瞭解底層技術，透過了解其原理以及運作模式的情況下，可以用普通的設備或軟體達到接近專業效果

OSSLab

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
(在碟片上的故軔體+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，但不允許讀取硬碟上的資料。

OSSLab

ATA 加密與解密

用戶如何判斷硬碟被設定 ATA 加密？

1.硬碟在BIOS中可以正確識別（包括型號，序列號，LBA 等等）。

2.所有的扇區都不可讀取（發生 ABRT 錯誤）。

3. 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

使用昂貴幾十萬的設備處理如 ACELab PC3000 UDMA
Acelab 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
並推出各種Data Recovery領域套裝設備。

OSSLab

可以一般軟體解開 未知ATA 加密

一. 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.

二.軟體使用Victoria for windows+MHDD in dos可直接發送ATA Command 指令

解開 ATA 加密

在MHDD下 顯示 硬碟已被加密

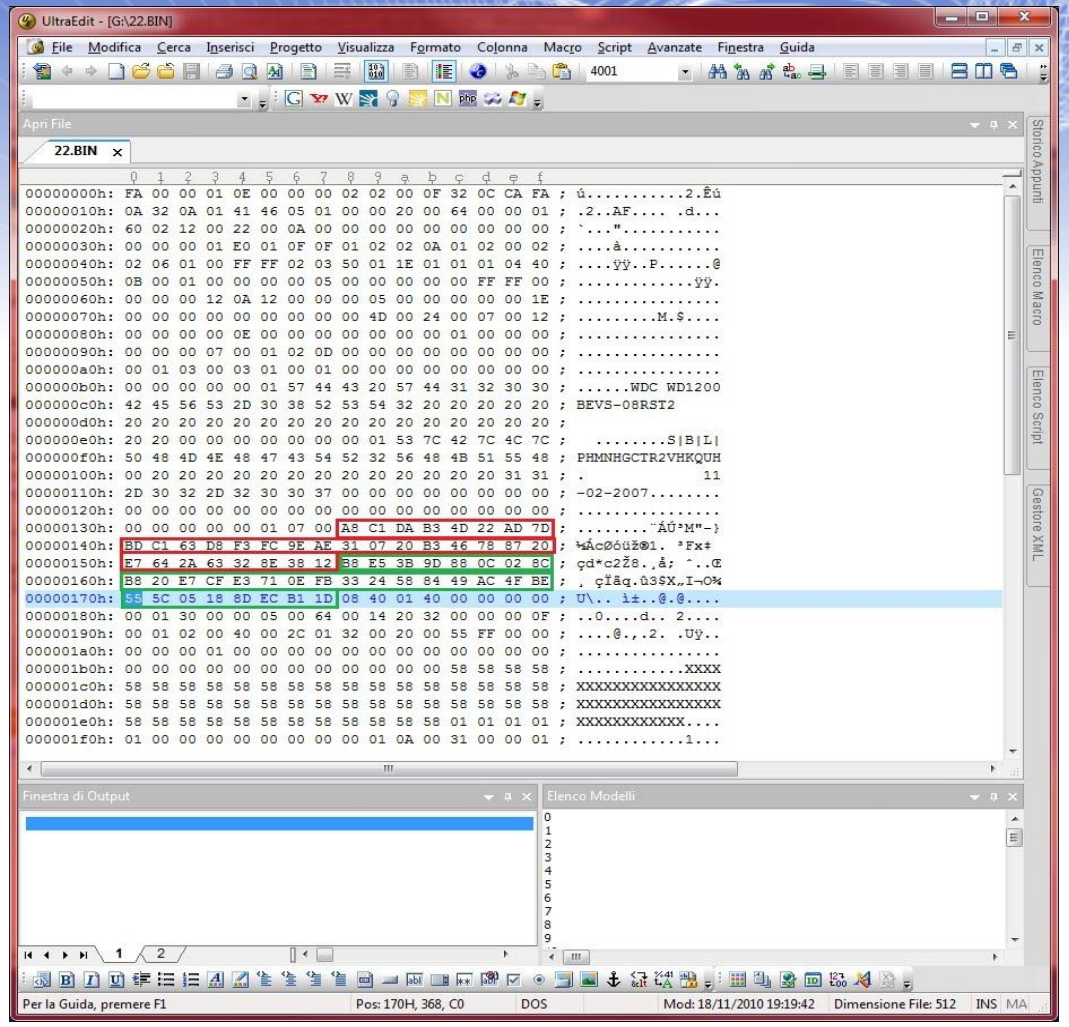
OSSLab

解開 ATA 加密

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

OSSLab

解開 ATA 加密



用 UltraEdit 打開22.bin

OSSLab

解開 ATA 加密

一，密碼起始位置可能不同，但排列與長度是相似.

二，0x137 偏移位置 07指出 ATA 加密等級

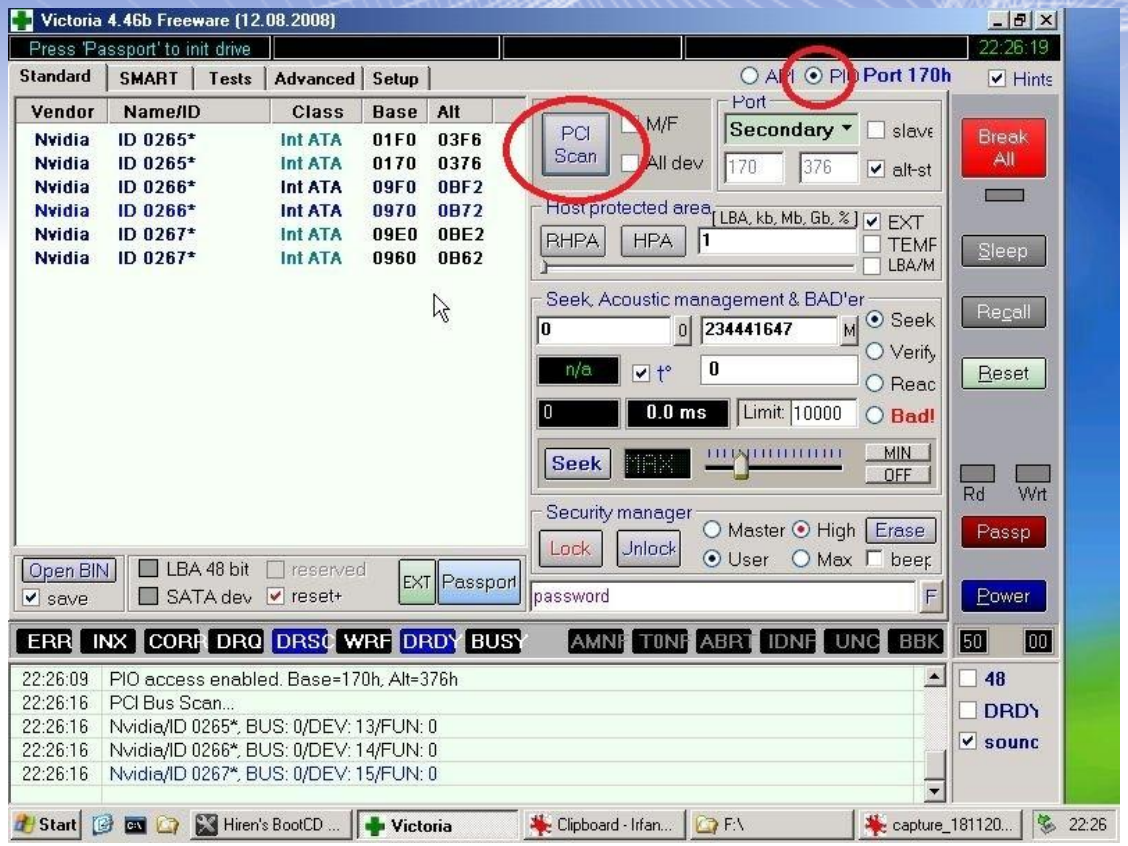
三，紅色區域為User Password使用者密碼

四，綠色區域為Master Password主密碼

五，選擇紅色+綠色區域並另存檔案.

六，執行 Victoria in Windows

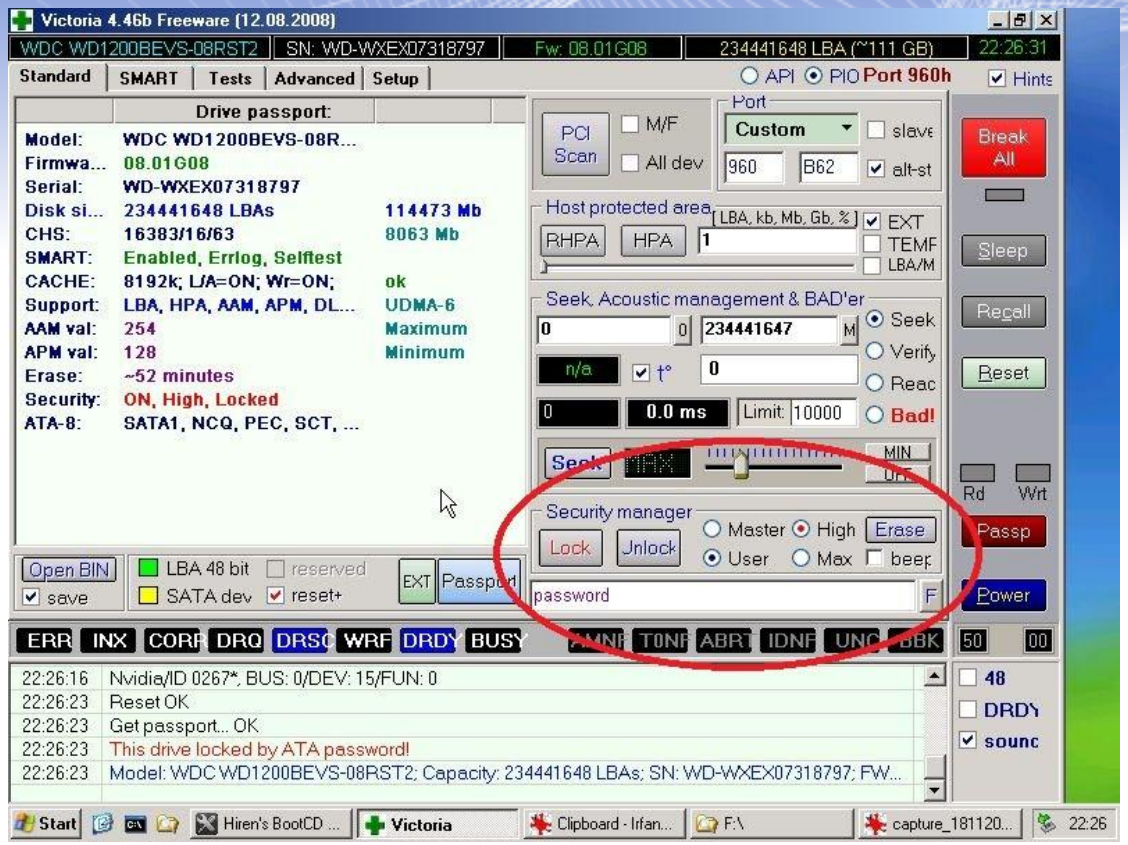
解開 ATA 加密



必需以PIO方式連接硬碟

OSSLab

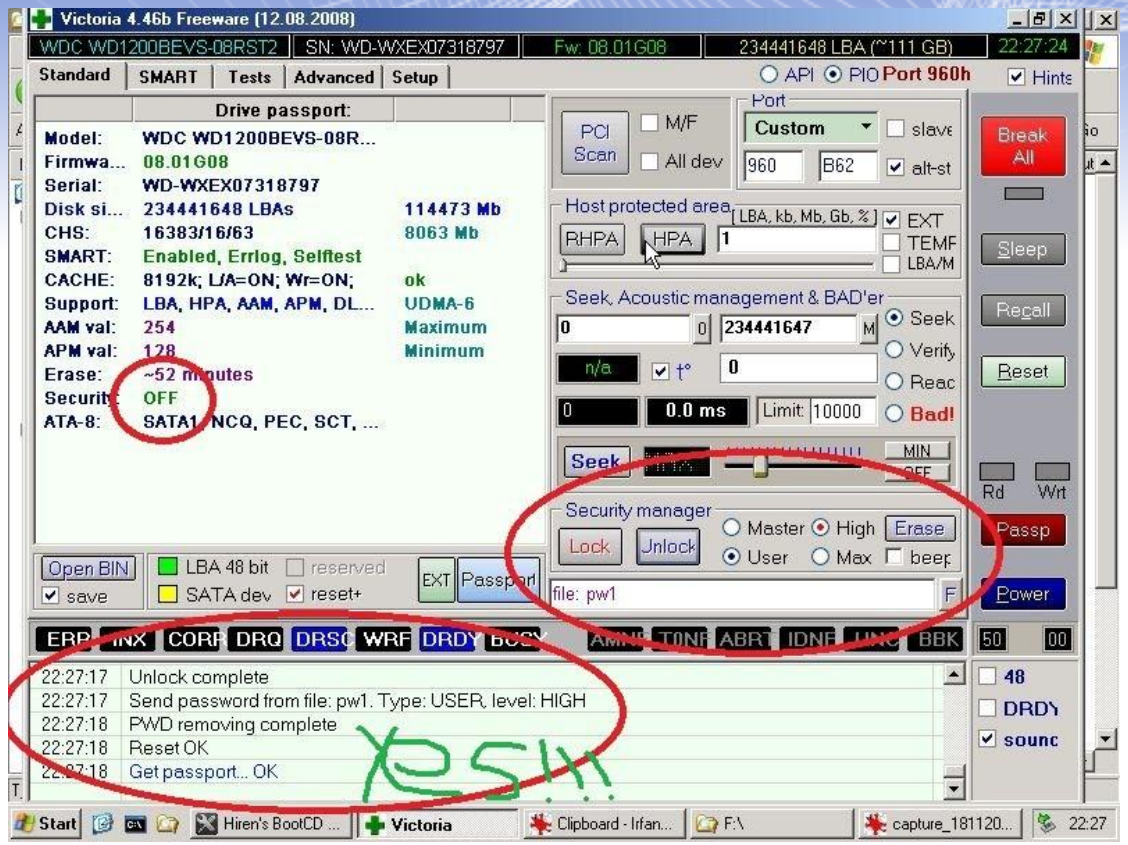
解開 ATA 加密



右下F按下去導入密碼檔

OSSLab

解開 ATA 加密



成功解除ATA Password

OSSLab

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 03h 04h	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)
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

- 對於不良讀取的硬碟

通常需要專業的數據導出設備才能達到 主要概念為跳過不可讀出的區域. 有下面幾種方法.

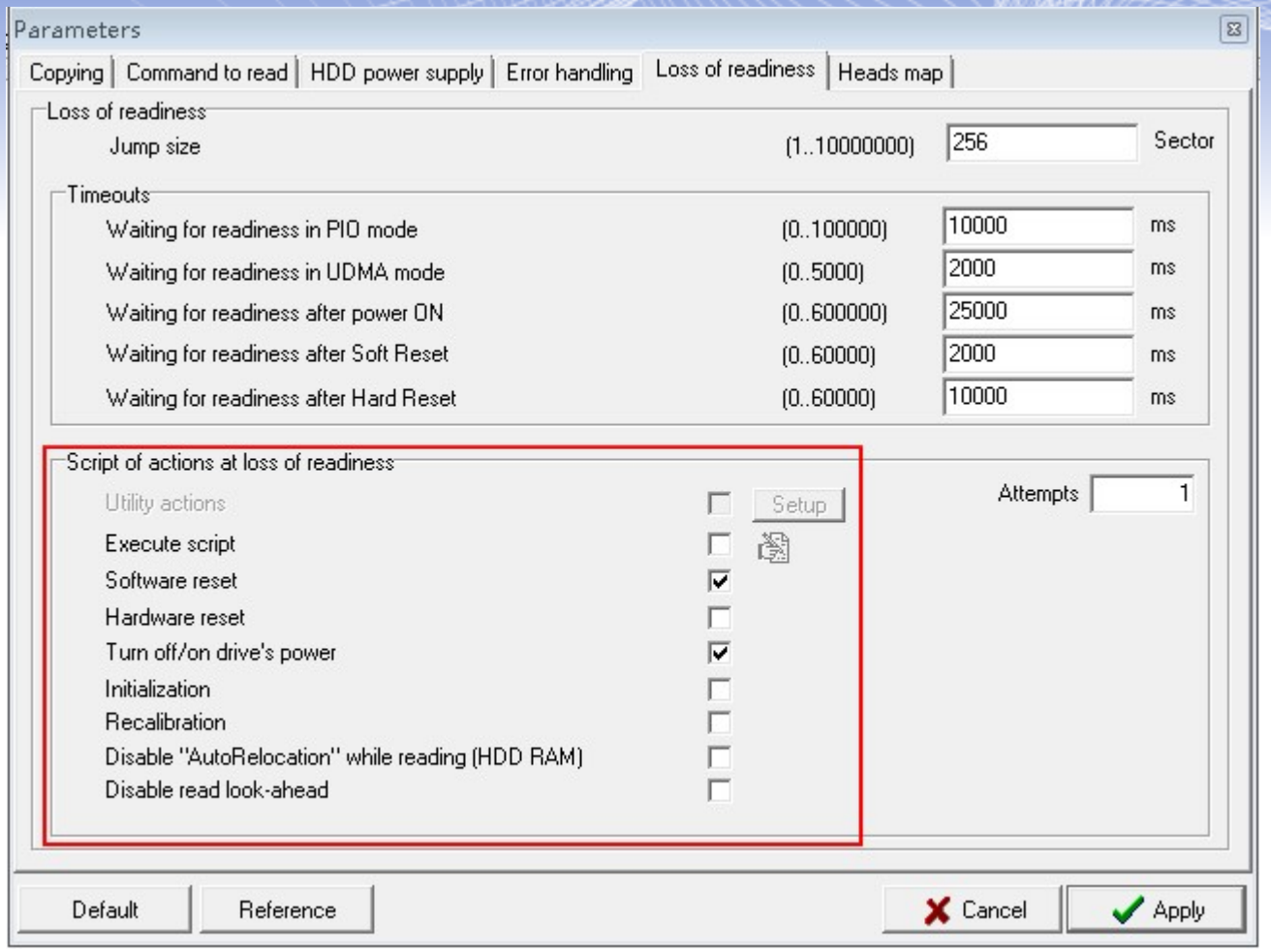
1.ATA Hardware Reset

2.ATA Software Reset

3.Power Reset

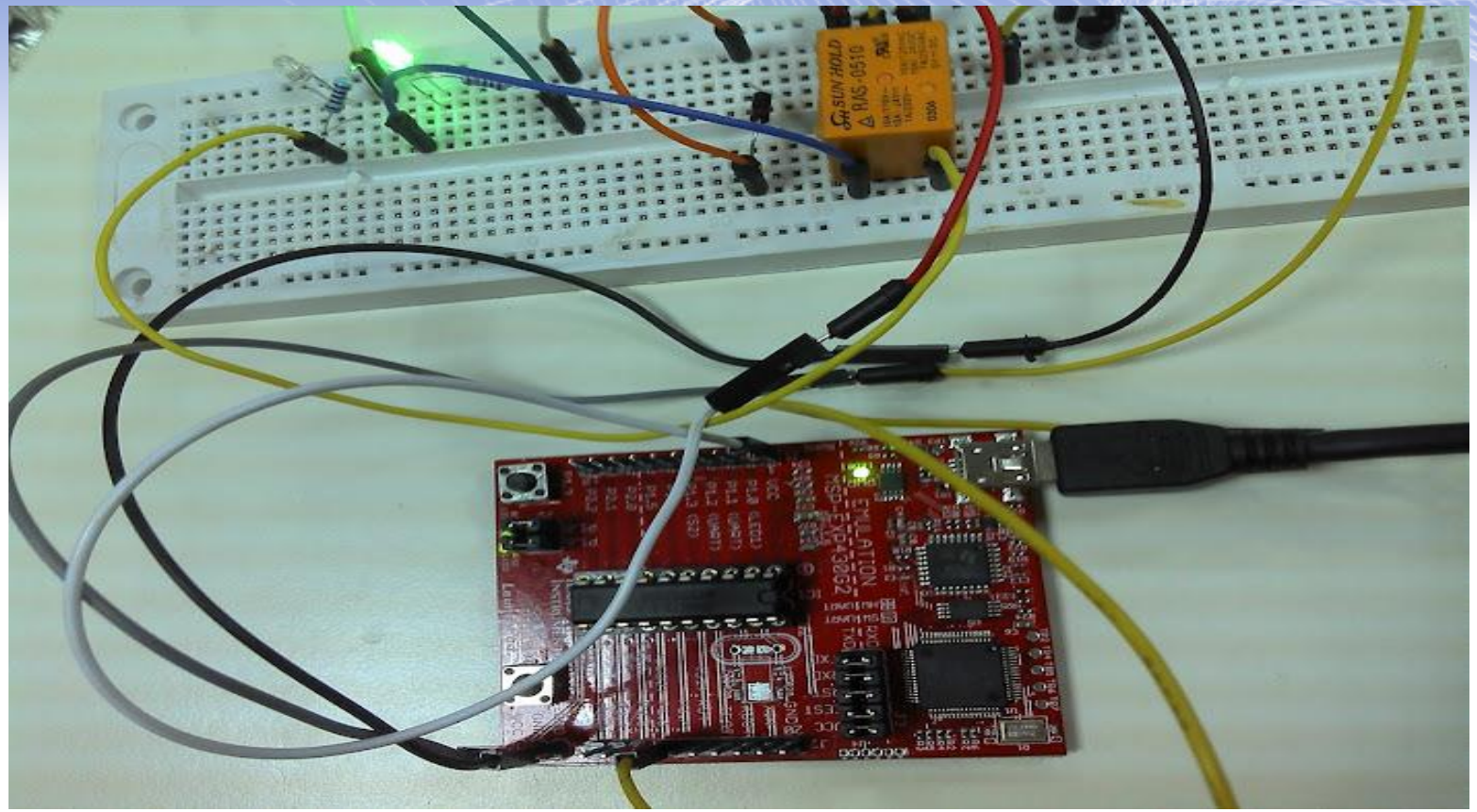
4.磁頭區 Zone 計算，可關閉不正常讀寫頭運作

UDMA DE 強拷資料操作畫面



OSSLab

強拷機自製硬碟斷電電路



OSSLab

自寫強拷程式

```php
// Get pid
$st = proc_get_status($proc);
$pid = $st['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:\s+[1-9]+\s+s#', $data))
    {
        posix_kill($pid + 1, SIGINT);
        exec('killall -s SIGINT ddrescue');
        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 "       ... stoping ddrescue ({$pid}) ";
fclose($pipes[0]);
```

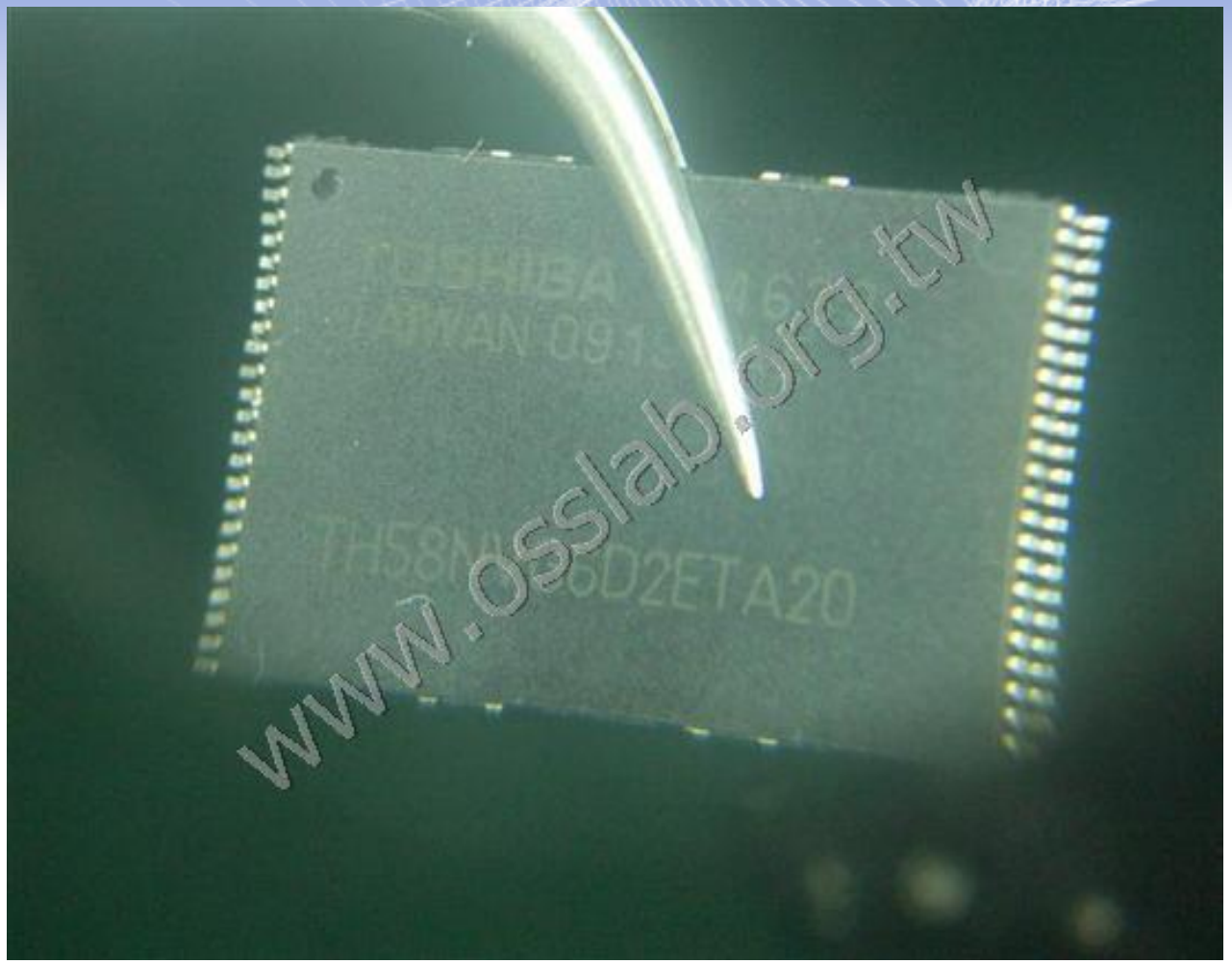
Flash 資料救援取證

OSSLab

SD Card PCB 板

OSSLab

8GB Nand Flash



OSSLab

將晶片放入編程器

OSSLab

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)開發的一種檔系統，主要運用於Mac os電腦和iphone等終端上。

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沒有加密硬體。

iOS Raw Disk 的加密

在IOS 4 + A4 CPU 之後,蘋果有鑑於加密問題.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  6e 99 eb 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.@|
00000030  96 53 c4 d3 81 0d 6e 73  98 6c 91 11 db e0 c2 3d  |.S....ns.l.....=|
00000040  7a 17 82 35 18 59 fb 17  1a b2 51 89 fc 8b 55 5a  |z..5.Y....Q...UZ|
00000050  95 04 a0 d6 2d d5 6a 6c  e8 ad 65 df ea b4 a8 8b  |....-.jl..e.....|
00000060  7e de c1 d2 b2 8a 30 e9  84 bb 08 9a 58 9a ad ba  |~.....0.....X...|
00000070  bb ba b1 9e 2a 95 67 d7  be a1 4b a7 de 41 05 56  |....*.g...K..A.V|
00000080  d5 4e 8b d6 3b 57 45 d2  76 4e 67 c0 8b 10 45 d9  |.N..;WE.vNg...E.|
00000090  7b 2a c3 c9 11 f4 c5 f0  56 84 86 b7 46 fe 56 e8  |{*......V...F.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 00  |................|
00000030  00 00 00 00 00 00 00 01  00 00 00 00 00 00 00 00  |................|
00000040  00 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 00 02  |................|
00000060  00 2d e2 1f 0d 00 00 00  00 10 00 00 00 00 00 00  |.-..............|
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```


*

OSSLab

IOS鑑識軟體 原始碼

不管是5-40萬數位鑑賞軟硬體 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

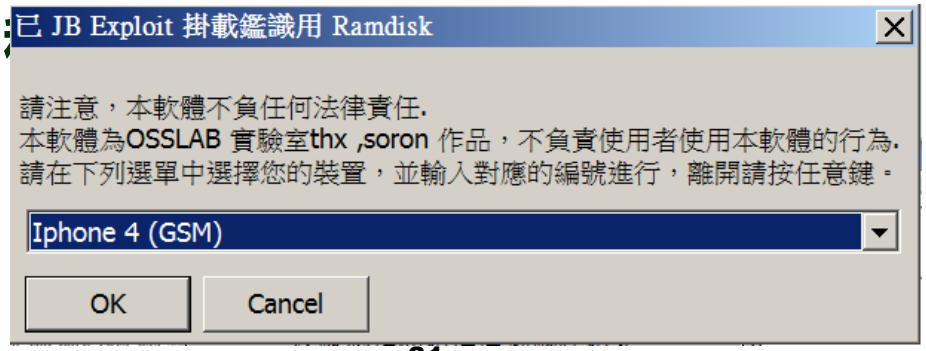
OSSLab

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Redsnow軟體,Redsnow 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 設備螢幕將顯示蘋果 Logo



*

OSSLab

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。

iPhone3G 設備沒有加密硬體，所以即使iPhone 3G設備運行了iOS 4.X，User 分區也是沒有加密的。

Key和keychain

擷取加密金鑰和keychain data
設備進入DFU 模式，加載ramdisk後 提取key和keychain data。

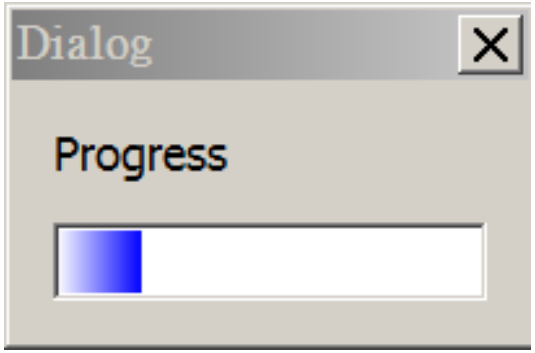
iOS設備進入DFU模式之後，我們可以提取解密User分區檔和keychain數據所需要的keys，確定ramdisk已經加載後
我們將可以獲得以下資訊：
iOS 密碼：可以透過暴力破解來獲得密碼。
Escrow檔：如果你能接觸到iOS設備連接和同步過的電腦，那麼你可以利用從這些電腦中獲取Escrow檔無需設備密碼即可解密所有存儲在iOS設備上的檔，Escrow file的檔以設備的UUID來命名。
Escrow檔的路徑為
win xp： %ALLUSERSPROFILE%\Application Data\Apple\Lockdown\
win 7 ：%ALLUSERSPROFILE%\Apple\Lockdown\

*
OSSLab

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。



*

OSSLab

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 -- progress

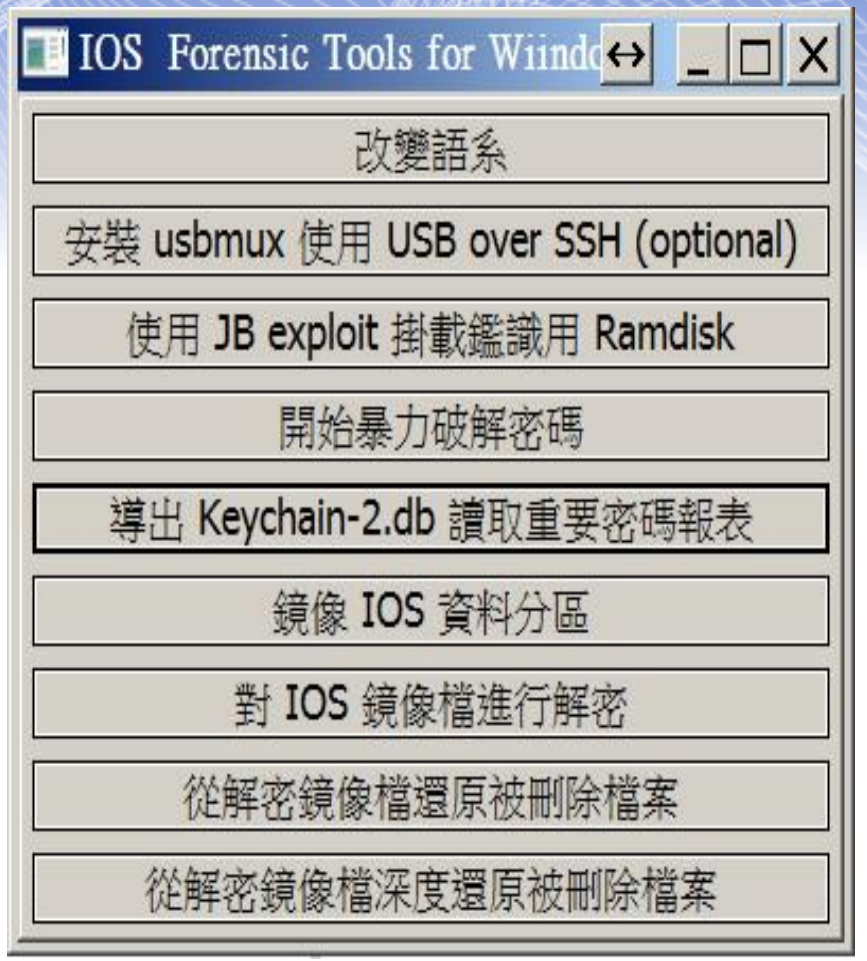
數位鑑識軟體開發思維

就算只是用DOS批次檔,能合需求

OSSLab

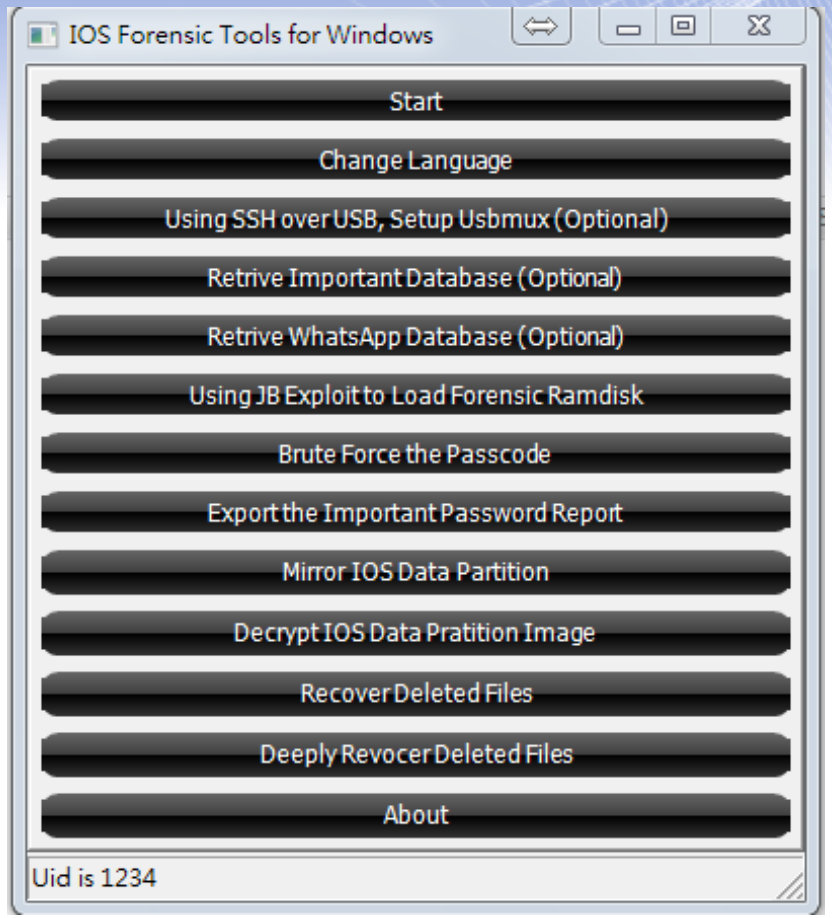
數位鑑識軟體開發思維

改以wx python 開發
批次檔直接轉
可以看到大部分都是相同的選項



OSSLab

數位鑑識軟體開發思維



再度修正版

在這版本已經增加了許多功能
包含專案建檔與管理
多語系的支援
免暴力破快速讀取重要資訊
Whatsapp 讀取解密.

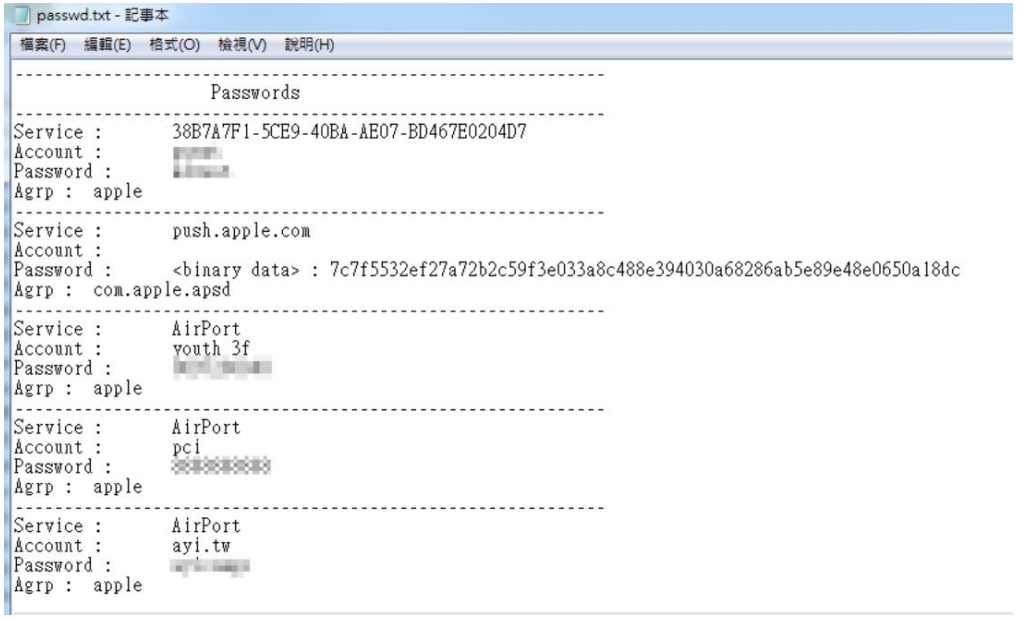
OSSLab

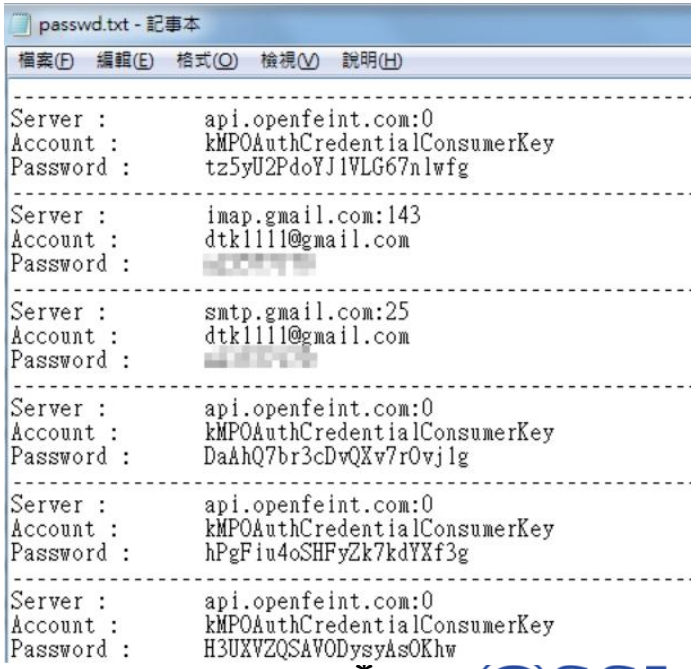
Wifi與apple ID

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:





*

OSSLab

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
```


*

OSSLab

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

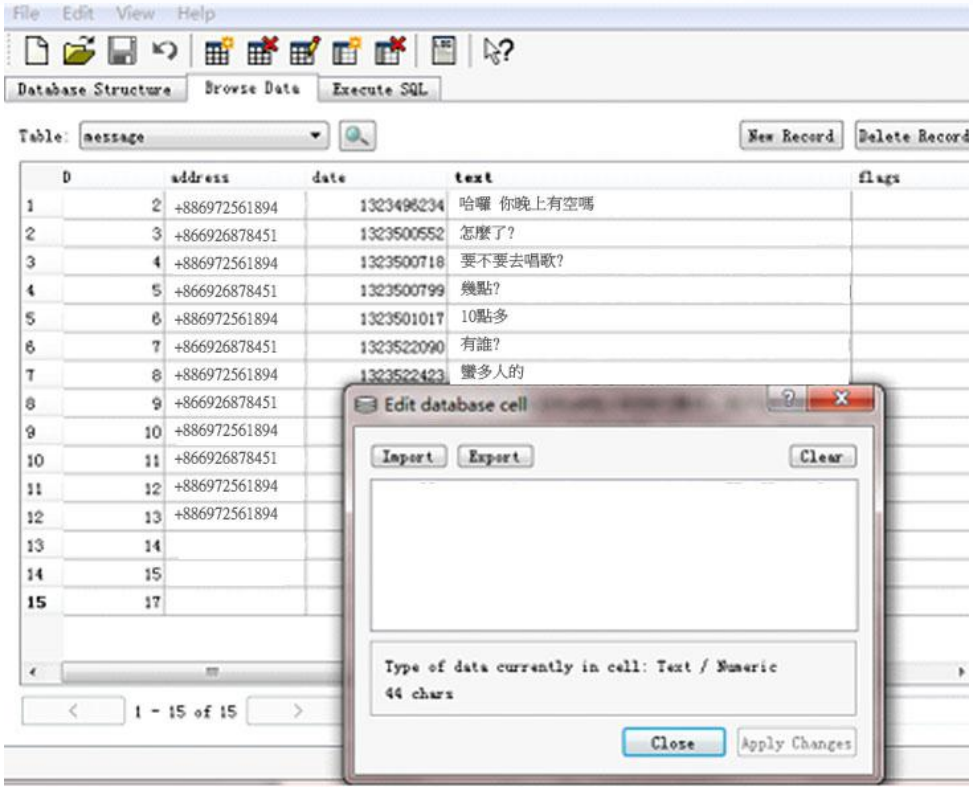
/private/var/mobile/Library/Calendar→ 日曆

因為越獄後 AFC2 服務就會自動啟動,不需要額外裝cydia 套件 .如 openssh server ,或是修改root password也無用

也可應用於A5 硬體IOS裝置 做為數位鑑識應用

SMS

在 /private/var/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



*

OSSLab

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

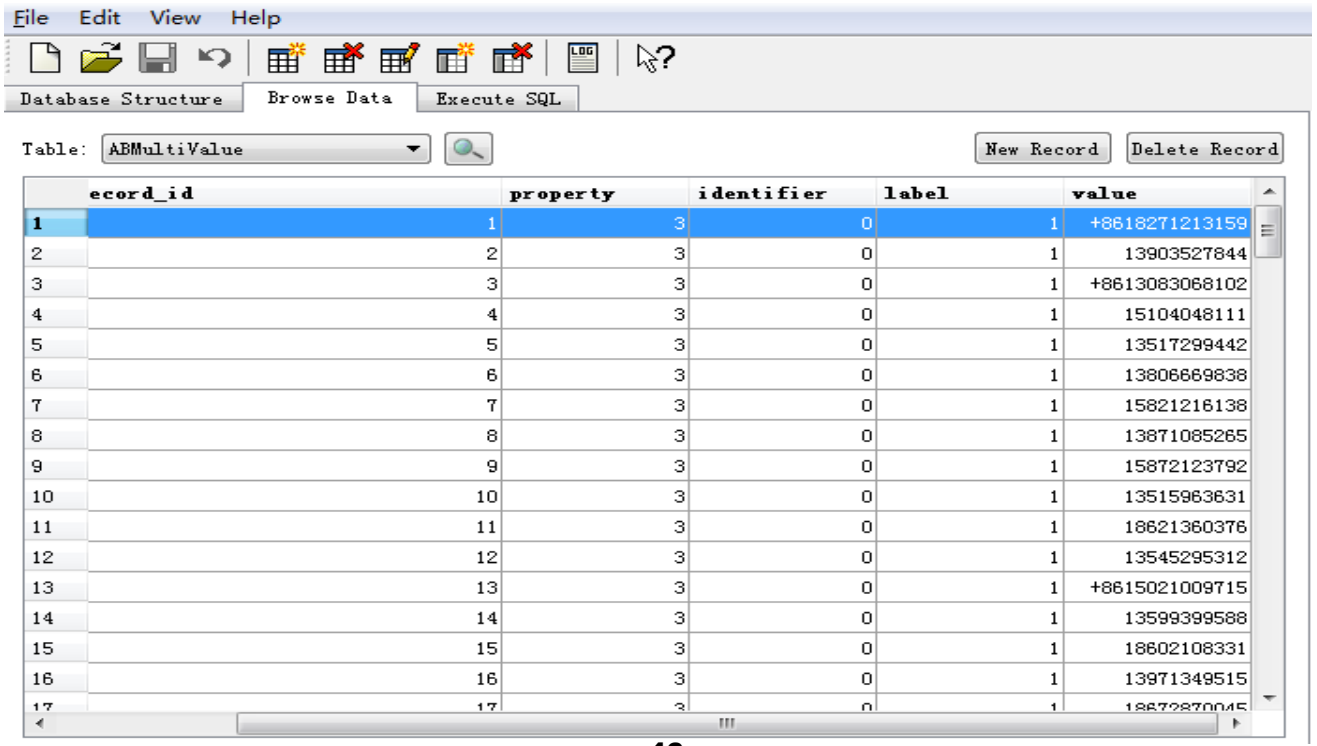
Table: call

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	

通訊錄

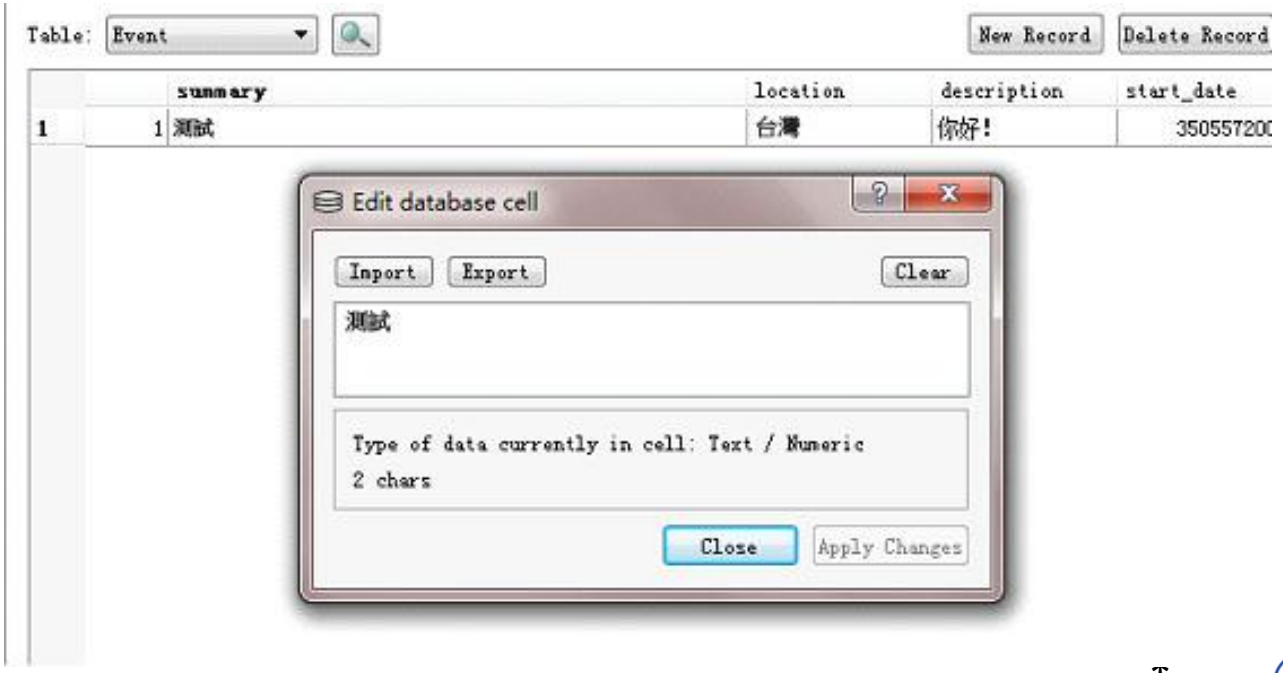
在 /private//var/mobile/Library/AddressBook下的 AddressBook.sqlitedb 中存放著設備的通訊錄，可以用 sqllite 工具查看



	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

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 sqllite 工具查看



OSSLab

Browser書簽

在 /private/var/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

tructure | Browse & Search | Execute SQL | DB Settings

TABLE bookmarks | Search (H) | Show All | Add (A) | Duplicate (P) | Edit (E) | Delete (L)

id	special...	parent	type	title	url	num_ch...	editable
12	0	11	1	yamaha		9	1
13	0	12	0	功學社音樂網站	http://www.khsmusic.com.tw/index.htm	0	1
14	0	12	0	功學社音樂網站 2	http://www.khsmusic.com.tw/index.htmSyncId=8E5D...	0	1
15	0	12	0	山葉鋼琴檢定考試 新竹	http://www.yamahapiano.com.tw/frame7.htm	0	1
16	0	12	0	山谷樂器網站首頁	http://www.yamahamusic.com.tw/SyncId=567F9EE5-...	0	1
17	0	12	0	財團法人山葉音樂振興基金會網站	http://www.yamaha-mf.org.tw/SyncId=D089E5E9-67...	0	1
18	0	12	0	山谷樂器網站首頁	http://www.yamahamusic.com.tw/	0	1
19	0	12	0	財團法人山葉音樂振興基金會網站	http://www.yamaha-mf.org.tw/	0	1
20	0	11	1	學校		5	1
21	0	20	0	新竹國民小學	http://www.hsps.hc.edu.tw/	0	1
22	0	20	0	新竹國民小學 2	http://www.hsps.hc.edu.tw/SyncId=41E1230B-3DF7-5...	0	1

歷史訪問記錄

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

```
</dict>
<dict>
	<key></key>
	<string>http://www.google.com.tw/url?sa=t&amp;source=web&amp;cd=4&amp
	<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</strin
	</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

Whatspp 解密

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，然後同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，及借一個60g硬碟。
2012-01-10 23:15:22	[redacted]	Intel 網卡拔掉 換上boardcom 2 port or boardcom 1 port 這在塑膠框內
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 拔掉?
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。

OSSLab

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

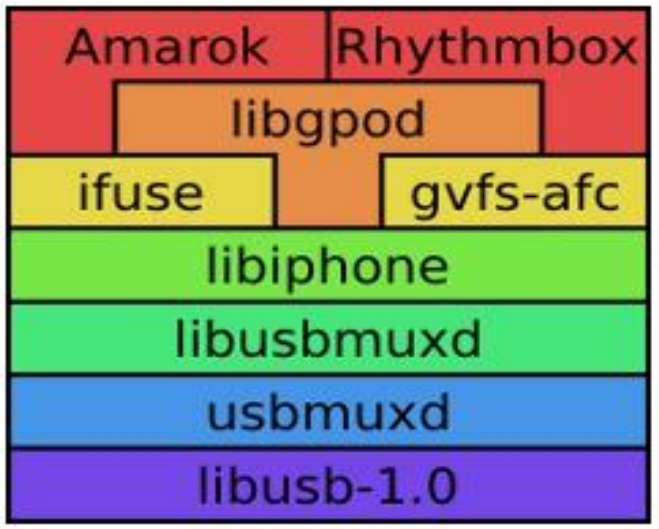
使用一般電腦上瀏覽器 再連入此"充電器" 直接觀看所有記錄。

OSSLab

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

OSSLab