數位鑑識與資料救援前瞻性研究

主講人: thx (張道弘)





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



- 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 的故朝體+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 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



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。



11

TTD ANNE TONE ABBT IDNE UNCR BBK ERR INDX CORR DREQ DISC WRFT DIDT BUSY TWDC WD1200BEVS-08RST2] [234,441,648] [

MHDDDeid

NDC ND1200BEVS-06RST2 LBA:234,441,648 DIOS SN: ND-UXEX07318797 FW:08.01608 CACHE:8192KB Supports: LBA18 HPA AAN DLNC LBA MS16 DMA (UDMA6, NUDMA2) SMART: Enabled SelfTest: Supported ErrorLog: Supported Security: high, ON. Size = 114473NB

WARNING: THIS DRIVE IS LOCKED BY ATA PASSUORD

MHDD>

I Take a screenshot : ([18)

1 28:86:5

在MHDD下 顯示 硬碟已被加密



LINE 1: RESET	
LINE 2: WAITNESY	
LINE 3: REGS = \$45 500 \$00 \$44 \$57 \$40 \$80	
LINE 4: WAITHESY	
LINE 5: REGS = SD6 S01 SHE S4F SCZ SA0 SD0	
LINE 6: WAITHESY	
LINE 7: CHECKORQ	
LINE 8: SECTORSPRON = CS.BIN	
LINE 9: NEES = \$05 \$01 \$8P \$4P \$C2 \$A0 \$80	
LINE 10: WAITABST	
LINE 11: CHECKDRQ	
LINE 12: SECTORSTO = 21.BIN	
LINE 13: REGS = \$05 \$01 \$8F \$4F \$CZ \$40 \$80	
INE 14: WAITHBSY	
LINE 15: CHECKDRQ	
LINE 16: SECTORSTO = 22.DIN	

hill done. HDD>_

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



	UltraEr	dit - (G	122	80N]																		
1	🔒 Eile	Modif	fica	⊆e.	TC.8	Light 1	rinci	Ð	oget	to	Ymu	alizza	E F	grm	do	Col	onna	- M	lecgy	o Script	Avenas	te Fr
E.	10 I I I I	+	1 68	100	100	10	6 I G		1.5	11	-	222	10		E		Sec.	De.	2	4001		.90
1	-	-			-		-	-	271	-		-	-	1.0			-	-	-			
1	_	_	_		_		100	80 °	6.2	20	w.	R. 8	2		1 820	8						
12																						
	22.8	14 ×	c																			
			Q.	1	2	3	4	5	6	7	8	2	۵.	b	0	d.	0	1				
0	00000	000h #	FA	00	00	01	08	00	00	00	0.2	0.2	00	0F	32	0C	CA	FA	1	Q	2	.Ê0
0	000000	1.0012	OA.	32	OA.	01	41	46	05	01	00	00	22	00	64	00	00	01		.Z AT.		I
0	000000	20h+	60	0.2	12	00	22	00	0A	00	00	00	00	00	00	00	00	00	.1	· · · · * · ·		
0	000000	30012	00	00	00	01	20	01	037	037	01	02	02	OA.	01	02	00	02		· · · · · ·		
10	00000	400h II	0.2	0.6	01	00	77	FF	0.2	0.3	50	01	15	01	01	01	0.4	40	1			
10	000000	5.00% = 1	03	00	01	00	00	00	00	05	00	00	00	00	00	22	22	00				22-
	00000	60th II	00	00	00	12	03	12	00	00	00	05	00	00	00	00	00	1E	1			
	000000	720121	00	00	00	00	00	00	00	00	00	40	00	2.4	00	07	00	12	1.1			
10	00000	80011	00	00	00	00	08	00	00	00	00	00	00	00	01	00	00	00	4			
0	00000	900h = 1	00	00	00	07	00	01	02	OD	00	00	00	00	00	00	00	00				
10	000000	= 10 Cm	00	01	0.5	00	0.5	01	00	01	00	00	00	00	00	00	00	00				
0	000000	both ::	00	00	00	00	00	01	57	44	43	20	57	44	31	32	30	30			IDC ND3	200
10	00000	00th # 1	42	45	5.6	53	29	30	38	52	53	54	32	20	20	20	20	20	1	BEVS-08	BST2	
10	000000	d00h = 1	20	20	20	20	20	20	20	20	20	20	22	20	20	20	20	20	1.1			
0	00000	eDha	20	20	00	00	00	00	00	00	00	01	53	70	42	70	4C	70			SIE	SIL!
	00000	20012	5.0	4.0	40	42	40	47.	43	3.9	52	32	35	48	45	51	33	40	12	PRODUCTION	TR2VH2	NUG
10	00001/	00051	00	20	20	20	20	20	20	20	20	20	22	20	20	20	31	31	4			11
0	00001	1.00% 2 1	20	30	32	20	32	30	30	37	00	00	00	00	00	00	00	00		-02-200	17	
10	00001	2205 =	00	00	00	00	00	00	00	00	0.0	0.0	00	0.0	0.0	0.0	0.0	0.0	4			
	00001	30012	00	00	00	00	00	01	07	00	A.5	C1	DA.	83	40	22	AD	70			- "AO"N	e=-3
10	00001	400h II	RD	C1.	63	D8	ES.	FC	98	A.E.	31	07	20	83	46	78	87	20	1.1	HÃ-08003	181. PF	28.2
	00001	530h = 1	27	-64	28	-6.3	32	32	35	12	38	E.5.	35	9D	0.0	0C	02	8C		çd*c2Žt	1 4.2	
10	00001/	60h+	88	20	E7	CF	E3	71	0E	FB	33	24	58	84	49	AC	47	BE	4	. olaq.	0.34X_J	0%
	00001	700s ::	55	SC.	05	18	60	EC.	51	10	08	40	01	40	00	00	00	00	4	U\ 11		
	00001/	60011	00	01	30	00	00	0.5	00	64	00	14	22	32	00	00	00	0F	4		d 2.	
	000011	900s = :	00	01	02	00	40	00	20	01	32	00	22	00	33	22	00	00		8.,	.20	12
10	00001/	althe	00	00	00	01	00	00	00	00	00	00	00	00	00	00	00	00	1			
	000013	bother	00	00	00	00	00	00	00	00	00	00	00	00	5.0	30	50	30				DOOD
10	00001/	-00th =	5.8	58	5.8	5.8	58	58	58	58	58	58	58	58	58	58	58	58	1	XXXXXXXXX	DOCCOC	XXX
0	00001	d00h = :	50	3.0	50	3.0	50	3.0	3.0	3.0	30	50	35	3.0	30	30	50	3.0	2	2000000	000000	DOOD
0	00001/	eDhill	58	58	58	58	58	58	58	58	58	58	58	58	01	01	01	01	1	XXXXXXXXX	XXXXXX	
	00001	£205 = 1	01	00	00	00	00	00	00	00	00	01	05	00	31	00	00	01				

用 UltraEdit 打開 22.bin



- 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。



I man 1 a	concer to job draip						77 26 19
Glandard	CMART Turke	Advanced	Calur			Q ALL @ PULL of 17th	211
line day	blassed D	Olace .	Date	414	-	Find	. II :
Vender	IN ADDRESS 13	LIANE	пака	A1	- ADF	Secondary * 🗆 stars	and the second second
NVILLE	ID 0265*	INLAIA	0110	0016			DIGER
NYIGIB	ID 0265*	INTATA	0170	0376	- P 05/	127 St. Moter	
Nyidia	10 0366	INT ATA	nse n	INF?	and all an end		_
NVIGIA	ID 0306*	INTALA	0970	UB/2 105	protocoularia	Lea, Mar Mar Gb. 4, 👽 FMT	
NVIU IB	ID 0261*	Int ATA	DOCD	IN IN IN	A -1 A 1	I ME	S ∋ec
INVITUR-	02.0201-	In ala	1124111	- musz		1 BA/M	
				N 899-	Acoustie in baio	cement & EAD'er	Lo. 1
				w u	n 21	iaaatijaz 🚽 🐑 🖙ek	F3
					21 P-	O VERN	
				174	⊘ ≫ II	(C)	Foset
						C PC.	
				· · · ·	0.01055	J of C Badl	
				(Income)		MINING MINI	
				CHR IS			
				- Case			Fi Vet
				C HILL		Mactor (High Eraco	Linear
				Lots	Jinoth @	ur Oka Erra	
Ucen BIS	J LB-0.48 (1)	- received	EC.	Pascorr		and Change and	-
2 :Eve	Selfades	👱 rocele		pere	. · J	F	Ener.
		In the second			INTO PERSON AND		22 22
ELUN II	w feorin ona	Una tion					<u>an</u> m
22-26-39	P.O eccess track	os Dato 17	NH AH C	765			🗆 40
22:26:15	PI Dic Gean .					243	LUBDA
22.26.13	Nvizio/12 C2651, B	. 5 0/DEV. I	3/F. >.)			
Sec. 14.	N-40101 CLOEPER R.	-S 11.1 (EVA 1	4.1	1		1.44	a spine
			Y				

必需以PIO方式連接硬碟





點擊右下F鍵導入密碼檔



					a second
itandaad	SMAII Tests Advanced	Satup		O AH ⊙ Hu Purt 950h	¥ I m
	Drive passport.		- 10-500-F	Pot	
Nodel. Firmwa Serial:	WDC WD12000EVG-80R 08.01608 WD-WXEX07010797		PGI - */* SGA1 - All dev	Custom Custom C	Eleak All
Disk Bi CHB: SWART ⁻	234441840 LUAa 16383/16/63 Enabled, Erring, Selflesi	114479 ND 8063 Mb	- Hospedanias da RHRA (HRA)	0%, ch, v = 0 = 3/1 ≤ 5/7 1 = 31 3847	<u>[]-eo</u>
Support All val	ытаак, шитон, читон, цвл, нил, лли, лиш, dl 264 130	UD MA 6 Maximum Minimum	- Seek Albusiomon	Covernant & BAD'er	້າອຼວ
erase. Becurib ATA-N	-92 moutes OFF SATA1 NGO, PEC, SCT,		V≕ VI(* _ 0 0.0 ms	U O ∹esx ■ _r:# C000 O Budi	Davel
<u>Oper BIN</u> Z Fova	EA 4060 received SATA cive ▼ ####	att Pacoper	Secondy microger	O Millarian (O Hind <u>Ercae</u> O use O Miller II beop I	La 9- Face Face
HI II I	C LOB THE DBSC W	IF DISDY N	Annual TINN A		
-7717 -20717 3.2718 :2710	Uterk complete Sent proses addare the best PoD containg constitution Read OK	ya USH (law-l			L 411 E D RDN E sound
2.9718	Galphasann ON 🛛 🔥	25			

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
03h		Device (3:0) Registers. For many commands this is the address
04h		of first logical sector to be transferred. Bits 47:28 shall be cleared (LSB) to zero for 28 bit commands. Each transport defines how these 48-bits are mapped to the appropriate fields or registers.
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

os ol reacinos		• 1	
Juni size	(1. 10020202)	256	Sector
- Timeouts			
Walng for reacticess in . 'III mode	() 1 11 () ()	10000	107
Waiting for reactness in UDMA mode	(05000)	2000	m*
Waiting for readiness after power ON	(0600000)	25000	mo
Walling for reaccess after Soft Level	(060000)	2000	m.
Waiting for reactiness after Hard Flesser	(060000)	10000	mo
Execute solid Sollware resel Hardware resel Tom of Am dive's cover Initia realization Recarictation Disable "AutoFickeetor" while reading (HDD RAM) Disable read ork-obead			-
		X Cancel	Acres 1

強拷機自製硬碟斷電電路



自行撰寫強拷程式

```
// Get pid
Son = proc_gen_status(Spres);
Spid = Sat['pid'];
$vatched = array($pipes[1]);
$null = null;
stream set blocking($pipes[1], false);
while(($changed - stream select($watched, $null, $null, $)) !-- false) {
    $watched = array($pipes[1]);
    if (Schanged != 1)
       continue:
    $data = stream get contents($pipes[1]);
    echo Sdata:
    if (preg match('| auccessful read:\a+[1-9]+\a+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 -1 system-shutdown');
        break;
echo "
           .... stoping ddrescue ({$pid}) ";
folose ($pipes[0]) ;
```

Flash 資料救援取證







8GB Nand Flash







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。



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。

	\$ hexdump	-C	mol	aile	≥/Li	ibra	ary/	/SMS	3/sm	s.dt	ΣĒ	hea	ıd					
	00000000	09	7d	b1	05	48	b1	bb	Gd	65	02	le	d3	50	67	da	Зe	.)HmePg.>
	00000010	SC.	99	cb	Зс	9f	41	fa	c7	91	c≤	10	d6	b2	2f	21	b2	n<.A/!.
	00000020	39	87	12	39	64	5c	96	7d	4a	bd	al	4a	ea	49	ba	40	99m\.}JJ.I.©
	00000030	96	53	с4	d3	81	0d	۶e	73	98	6c	91	11	db	e0	c2	3d	.S=
崔裕則	00000040	7a	17	82	35	18	59	$_{\rm fb}$	17	la	b2	51	89	fc	$^{\rm 8b}$	55	5a	z5.ĭQUZ
	00000050	95	04	а0	d6	2d	d5	бa	6c	е8	ad	65	df	69	b4	а8	$^{\rm ab}$	jle
	00000060	7e	de	c1	d2	b2	8a	30	e 9	84	bb	08	9a	58	9a	ad	ba	l
	0000070	bb	Da.	b1	9e	2a	95	87	d7	be	al	4b	а7	de	41	05	56	*.gKA.V
1953-88 93-858 -88	00000080	da a	4e	8b	d6	35	57	45	d2	76	46	67	c0	ab	10	45	6.9	.N;WE.VNgE.
	00000090	7b	2a	c3	c9	11	±4	сā	f0	56	84	88	b7	46	fe	56	e8	$ \{1,\ldots,V,\ldots,\mathbb{F},V\} $
											••••		••••					
	5 hexdump	-C	moh	vile	VI.5	bra	1777	/sm	3/en	വം പ്	b I	he	ad	0-0-0		0-0-	n-n-f	*********************
	00000000	53	51	4c	69	74	65	20	66	6f	72	- 6d	61	74	20	33	00	SQLite format 3.
89339325388	00000010	10	00	02	02	00	40	20	20	0.0	00	00	02	00	00	00	01	
	00000020	00	00	00	00	00	00	00	00	0.0	00	00	00	00	00	00	00	
砰宓後	00000030	00	00	0.0	00	00	00	00	01	0.0	0.0	0.0	00	00	0.0	00	00	
	00000040	00	00	0.0	00	00	00	00	00	0.0	00	0.0	0.0	00	0.0	00	00	
	00000050	00	00	00	00	00	00	00	00	0.0	00	00	00	00	00	00	02	
	00000060	00	2d	e2	11	0d	00	00	00	0.0	10	00	00	00	00	00	00	. –
	00000070	00	00	0.0	00	00	00	00	00	0.0	00	00	00	00	0.0	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

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

已 JB Exploit 掛載鑑識用 Ramdisk	×
诸任立,太郎建不会任何法律者任	
本軟體為OSSLAB 實驗室thx ,soron 作品,不負責使用者使用本軟體的	ΠÐ-
請在下列運車中運擇您的裝置,並輸入對應的編號進行,離開精技仁意	第 •
Iphone 4 (GSM)	-
OK Cancel	

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\



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。





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。 **IOS** Forensic Tools for Wiindet \rightarrow **\square** × 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

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

就算使用 DOS,執行批次檔也能符合簡易使用的需求

画 条統管理員: IOS forensic Tools for Wiin V0.2 beta powered by OSSLab soron and Thx 💭 2.5 108 forensic Tools for Windows V0.2 beta By thxBosslab.com.tw from Taiwan 臣 soron255054@hotmail.com soron(凌羽) from Taiwan http://www.osslab.com.tw special thanks jean.sig and jb security labs MENII 以JB exploit 進行繼續Bootdisk 載入 终端sh port 2 3 4 恢復被刪檔案 5 6 ā本程式(EXIT)

請選擇你要進行的動作:

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。

IOS Forensic Tools for Wiindd↔
ひ響語系
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

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.

IOS Forensic Tools for Windows

Ж

 \Leftrightarrow

Start

Change Language

Using SSH over USB, Setup Usbmux (Optional)

Retrive Important Database (Optional)

Retrive WhatsApp Database (Optional)

Using JB Exploit to Load Forensic Ramdisk

Brute Force the Passcode

Export the Important Password Report

Mirror IOS Data Partition

Decrypt IOS Data Pratition Image

Recover Deleted Files

Deeply Revocer Deleted Files

About

Uid is 1234

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:

passudita - E#	1999-1999-1999-1999-1999-1999-1999-199
· (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	111(C) 教授(A) 記句(H)
	Passwords
Service : Actornt : Password : AETP : spile	3887A7F1 - SCE9 - 408A - AR07 - EC/467B020 4D7
Service : Account : Pranword : Agrp : com.spi	push.apple.com «binary data» : 7c7f5532ef27m7252c59f3e033m8c488e394030u68286u55s89e48e0650u183c plc.com
Service : Account : Pramord : Agrp : spyle	AtaPost south 31
Service : Account : Password : Anty : mpile	AllPost. pcl Seascastas
Scrwice : Account : Pagenword : ACTP : apple	AlePost. ari.tv

Dessure.txt-	E##
個為/日 講師(日) 修業(型) 接機(の) 軟明(EC
Server :	api.openfeint.com:0
Account :	kMPCAntkCredentialConsemerKey
Password :	t25yU2P4cYJ1YLG67nlwfg
Server : Account : Pageword :	imsp.gnxil.com:143 dtil1110gmail.com
Server : Account : Password ;	satp.gnail.com:25 dtklill@gmail.com
Server :	abl.openfeint.com:0
Account :	kWPCAntkCredentialConsumerKey
Password :	DakNQ/br3cDMQ2v/rOvj1g
Server :	api.openfeint.com:0
Account :	kMPCAuthCreientialConsumerKey
Password :	hPgFiu4oSHFy2k7kd7%f3g
Server :	ap:.openfeist.com.0
Account :	kKPCAuthCredentialConcunerKey
Password :	H3UXVZQSAVODysyAxONhw

用戶如何判斷硬碟被設定 ATA 加密?

系統密碼與 key.plist

v系統鎖屏密碼,

利用工具箱可以暴力破 解系統密碼

v獲取到解密用的 key.plists

iOS 設備的 Escrow 檔

1	< 7:	xml version="1.0" encoding="0IF-8"?>
2	< 11	DOCTYDE plist DUBLIC "-//Apple//DID DLIST 1.0//EW" "http://www.apple.com/
з	= <p)< th=""><th>list version="1.0"></th></p)<>	list version="1.0">
4	= < <u>d</u> :	tet >
5		<key>DerivedKeys</key>
6	•	<diet></diet>
7		<key>2101</key>
8	-	<data></data>
9		4nRkLHDmMagIBmzSAeGq+u==
10		
11		<key>2102</key>
12	•	<data></data>
13		ucgB4a3ESJzMpkva1XH1du==
14		
15		<key>2104</key>
16	-	<data></data>
17		dR7zH04/QHverm8EAL1CH0==
18		
19		<pre></pre>
20	-	vdatav
21		DIFOL ^A HD ^A /GAA ^A /MTGebJÖ
22		
29		<key~2202× key~<="" th=""></key~2202×>
24	-	vdatav.
25		veliDT2d2e204WDW19BL0g
26		
27		<key:2203< key:<="" th=""></key:2203<>
28	-	vdet ev
28		4SRBqsIbhwIRcsPDaUo8tA
90		
91		s/diet>
92		<key%effeceeblestorege* key%<="" th=""></key%effeceeblestorege*>
99	-	vdatav -
94		w0w0ADFHQUIxR0FC1bOW1jQ1F/4/SQ4TeqCeDpyqBFWJRtZP0W67Q5oZd264J59w7hSP
95		8qtqhGJRZOwCw0woAHllw8TcG18JwCoTEEdhy6SRZwHFw14Q3t39ivQH5A+YtyKAvioP
36	- 333	C7QedRxRx0wkACFGTcUgAAAALnO6JcPqUHrwUile2hPUTfr/FSgneEPKszibhIJZzzBr



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→ 日暦

因為越獄後 AFC2 服務就會自動啟動,不需要額外裝 cydia 套



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

Tuble: messa D	te.			No. Bernet	fact a
D		the second		bes vecoud	Delete Reco
	address	data	text		fLags
1	2 +8869725618	H 1323496234	马啸 的第三方法等		
2	3 +8669268184	1323500552	2度7?		
3	4 +8869725118	H 1323500718	要不要去唱歌?		
4	\$ +86692681343	1222500799	- 病助?		
5	6 +8869725018	1323501017	10船多		
6	7 +86692681843	1323522090	有边?		
7	8 +8869725618	H _1323522423	量多人的		lange in
8	9 +8569268384	Edit dat	tabase cell	See See 2	
9	10 +8869725618	N			
10	11 +8669268.843	11 Inpart	Laport	Clear	
11	12 +8809725038	N			1
12	13 +8869725118	14			
13	14				
14	15				
15	17				
		10000000		and it there are a	



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

Iatic	ecil	•	0		Bev	Celete	Record]
	ROWID	eddress	date	duration	flags	id	nenc
1	:	+8615172320747	1328793499	456	Ξ	-:	
2	۶	15172320747	1020596001	191	4		
3	3	+8615172320747	1328796858	3500	Ξ	25	
ć.	ŧ	18801168165	1328801073	2376	=	- 4	
5	5	+8615221580201	13288-15-170	29	5	ا ۲	



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

file 1	Edit View Help				
6	🚅 🗐 🍽 🎬 🗃 🖬 👔	🖌 🖹 🚀			
LIZEN	an Structure Laws Date Reard	• 351			
7414	. Ali ta Valina 🔹 🔹 🔍			Res Fac	ord [Jalata Bacord
	econd_cd	2 · • • • • • • • •	adeal allows	Lakel	ndar A
1		3	0	1	-8516271013150 😑
•		3		1	0141 (\$11244) 📥
-))	0	1	201000000100
4		×	V	1	15304043121
	5	3	н	1	C 3 9264142
	6	3	0	I	13905650638
	۰ N	s		1	15-54121 bit 93
:	0	3	0	1	10071000205
:	9	\$	0	1	15972123700
. 11				1	C A AS E B
-1		3	0	1	1852_360676
·		x		1	Dester and
.0	د.	3	0	1	0010061008715
14	14	\$	0	I	12500800588
15	·			1	0.4.9.6.0
.6	_6	3	0	1	1207.3405.5
•••					
					P.



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

	210	description	Locat: on		nary	Sunnar	1
3505572		你好!	台灣			洞默	 1
		×	6	database cell	E 54		
		lear		ert Expert	Inp		
					att:		
			l: Text / Bunaria	e of data currently in louis	Tyr 2 v		
		hanger	Date Apply 5				
		hangen	l: Text / Benarie Llase Apply D	a of data currently in News	Tyr 2 v		



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 & Se	arch Ex	ocute SQL D	B Sottings		0000202020	201120105	628
TABLE	bookmarks		Search (H)	Show All	Add (<u>A</u>) Duplicate (P) Ed	il (E)	Delete (L)
id	special	parent	type	title	url	num ch	editable	909
12	0	11	1	yamaha		9	1	
13	0	12	0	功學社會探網站	http://www.khsmusic.com.tw/index.htm	0	1	
14	0	12	0	功學社會等網站 2	http://www.khsmusic.com.tw/index.htmSyncId=8E5D	0	1	
15	0	12	0	山葉對林機定考試 新竹	http://www.yamahapiano.com.tw/frame7.htm	0	1	
16	0	12	0	山谷婆器網站首頁	http://www.yamahamusic.com.tw/EyncId=567F9EE5	0	1	
17	0	12	0	財團法人山葉蒼葉振興憲金會網站	http://www.yamaha-ml.org.tw/SyncId=D089E5E9-67	0	1	
18	0	12	0	山谷婆器網站首頁	http://www.yamahamusic.com.tw/	0	1	
19	0	12	0	<u> </u>	http://www.yamaha-mborg.tw/	0	1	=
20	0	11	1	單校		5	1	
21	0	20	0	新竹園民小學	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	
	-		-			-		



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
     <kev>D</kev>
     <arrav>
           <integer>1</integer>
     </arrav>
     <key>lastVisitedDate</key>
     <string>362113495.9</string>
     <key>redirectURLs</key>
     <arrav>
           <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>
     <kev>visitCount</kev>
     <integer>1</integer>
 dict>
```



■ 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



2012-01-00 17.24.15	10.02	224 BALE - 18-412848 - 4008439 - 1	
2012-01-08 17:25:30		Agaib	
2012-01-08 18:55:21	And a state of the	你到了?	
2012-01-09 09:56:00		有故出?	
2012-01-09 09:58:37	- 00010070100	有那,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,還在記憶卡裡這種。	
2012 01 10 21:37:48	and the second second	GE 似乎沒辦法插那張 ISCSI 卡。	
2012 01 10 21:46:04	Contraction of the local division of the loc	另外,我還要多拿一個usb外接盒 及普一個60g硬碟。	
2012-01-10 23:15:22	-	Intel 網卡紋掉 换上boardcom 2 port or boardcom 1 port 這在塑膠福內	
2012-01-10 23:17:39	-	Image	
2012-01-10 23:17:51	-	Ok	
2012-01-10 23:19:20		把 G6 的15CSI 换掉?	
2012-01-10 23:20:12	and the second second	還是17上的?	
2012-01-10 23:25:24	March 1998	開機了。	
2012 01 10 23:39:08	100 PT 8 PT 10 PT	我走耀。	

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。





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



本演講的部份程式碼,與詳細原理

歡迎到 http://www.osslab.com.tw/ 參考

