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。



數位鑑識技術生活佔應用

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



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。

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加密便體設備

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。

NON CONTRACTOR



可以一般軟體解開未知不為加密

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



解開入口名加密



在MHDD下 顯示 硬碟已 被加密



解開入口和密

LINE 1: I	RESET			
LINE 3: I	REGS = \$45 \$08 \$00 \$4	4 \$57 \$A0 \$80		
LINE 4: I	WAITNBSY			
LINE 5: I	REGS = ŞD6 Ş01 ŞBE Ş4	F ŞCZ ŞAO ŞBO		
LINE 6:	WAITNESY			
LINE 7:	CHECKURY			
LINE OF	<u>Secturgenun - Ca.din</u> PFCS - SD5 SA1 S <u>BF</u> SA	F \$C2 \$44 \$84		
TINE 10.	HAITNESY	T YOL QUO QUO		
LINE 11:	CHECKDRO			
LINE 12:	SECTORSTO = 21.BIN			
LINE 13:	REGS = \$D5 \$01 \$BF \$	4F SC2 SAO SBO		
LINE 14:	WAITNBSY			
LINE 15:	CHECKDRQ			
LINE 16:	SECTORSTO = 22.BIN			

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

🕐 UltraEdit - [G:\22.BIN]	- x
🚺 File Modifica Cerca Inserisci Progetto Visualizza Formato Colonna Macro Script Avanzate Finestra Guida	- 8 ×
Apri File	. n × 10
22.000	torio
22.BIN X	O A
0173456789abcdef	p
00000000h; FA 00 00 01 0E 00 00 00 02 02 00 0F 32 0C CA FA; U	12
00000040h: 02 06 01 00 FF FF 02 03 50 01 1E 01 01 04 40 ; VVP@	1
00000050h: 0B 00 01 00 00 00 00 05 00 00 00 00 00 FF FF 00 ;	nco
00000060h: 00 00 00 12 0A 12 00 00 00 05 00 00 00 00 00 1E ;	M a
00000070h: 00 00 00 00 00 00 00 00 00 4D 00 24 00 07 00 12 ;	ICTO
00000080h: 00 00 00 00 0E 00 00 00 00 00 00 00 01 00 00 00 ;	E
00000090h: 00 00 00 07 00 01 02 0D 00 00 00 00 00 00 00 00 ;	
000000a0h: 00 01 03 00 03 01 00 01 00 00 00 00 00 00 00 00 ;	(III)
000000bbh: 00 00 00 00 00 01 57 44 43 20 57 44 31 32 30 30 ;WDC WD1200	enc
000000001: 42 45 56 53 2D 30 38 52 53 54 32 20 20 20 20 20 ; BEVS-08RST2	0
	спр
	-
0000010h: 00 20 20 20 20 20 20 20 20 20 20 20 31 31 :	
00000100h; 2D 30 32 2D 32 30 30 37 00 00 00 00 00 00 00 00 ; -02-2007	G
00000120h: 00 00 00 00 00 00 00 00 00 00 00 00 00	est
00000130h: 00 00 00 00 00 01 07 00 A8 C1 DA B3 4D 22 AD 7D ;	ore
00000140h: BD C1 63 D8 F3 FC 9E AE 31 07 20 B3 46 78 87 20 ; \Acobitation / Fx+	XM
00000150h: <mark>E7 64 2A 63 32 8E 38 12 B8 E5 3B 9D 88 0C 02 8C</mark> ; cd*c2Ž8.,å; ^C	1
00000160h: B8 20 E7 CF E3 71 0E FB 33 24 58 84 49 AC 4F BE ; , çĨăq.û3\$X"I-O%	
00000170h: <mark>55 5C 05 18 8D EC B1 1D</mark> 08 40 01 40 00 00 00 ; U\ ì±@.@	
00000180h: 00 01 30 00 00 05 00 64 00 14 20 32 00 00 00 0F;d. 2	
00000190h: 00 01 02 00 40 00 2C 01 32 00 20 00 55 F 00 00 ;	
000001001: 58 58 58 58 58 58 58 58 58 58 58 58 58	
000001e0h: 58 58 58 58 58 58 58 58 58 58 58 58 58	
000001foh: 01 00 00 00 00 00 00 00 01 0A 00 31 00 00 01 ;	
* <u> </u>	
Finantina di Gutenati anna a su Elenco Modalli -	
	Ē
23	
4	
5 6	
7	
8	
	INS MA
Posi 1/01, 500, C0 0/05 Widu: 10/11/2010 19:19:42 Dimensione Pile: 512	IND IVIN

用 UltraEdit 打開22.bin



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



解開入人加密

<table-cell-rows> Victoria</table-cell-rows>	4.46b Freev	ware (12.	08.2008)						_ 8 ×
Press 'Pa	issport' to in	nit drive							22:26:19
Standard	SMART	Tests	Advanced	Setup]		O Al¶ ⊙ PI	Port 170h	✓ Hints
Vendor	Name/ID)	Class	Base	Alt		- Port	1]	
Nvidia	ID 0265*		Int ATA	01F0	03F6	PCI - MYF	Secondary *	slave	Break
Nvidia	ID 0265*		Int ATA	0170	0376	Scan All di	ev 170 376	alt-st	All
Nvidia	ID 0266*		Int ATA	09F0	OBF2				
Nvidia	ID 0266*		Int ATA	0970	0872	Host protected a	rea [LBA, kb, Mb, Gb, %	JV EXT	
Nvidia	ID 0267*		INT ATA	0950	UBE2	RHPA HPA	1	TEMF	Sleep
INVIUIA	10 0207		IIII ATA	0900	0002	7		LBA/M	
					2	CSeek, Acoustic m	nanagement & BAD's	er	Recall
					~~	0 0	234441647 M	Seek	
								O Verify	
							U	O Reac	<u>H</u> eset
						0 0.0 1	ns Limit 10000	O Bad!	
								KAINI I	
						Seek		OFF	
						0			Rd Wrt
						Security manage	Master 💿 High	Erase	Passo
		1011		2. P		Lock Jnlock	• User O Max	L heer	
Open BIN		48 bit	i reserved	EX	Passport		0,000,000		
Save		IAdev	reset+			password		F	Power
ERR	X COR	DRQ	DRSC W	RF DF	DY BUSY		ABRT IDNE U	NC BBK	50 00
22:26:09	PIO acces	s enable	d Base=17	0h Alt=3	176b				48
22:26:16	PCI Bus Sc	can	.u. Duse-17	on, mitte	a off.				
22:26:16	Nvidia/ID (0265*, BL	JS: 0/DEV: 1	3/FUN:	0				
22:26:16	Nvidia/ID (0266*, Bl	JS: 0/DEV: 1	4/FUN:	0				I sounc
22:26:16	Nvidia/ID ()267*, Bl	JS: 0/DEV: 1	5/FUN:	0				
Mar 1 1			n						
Start [a ன 🔁 🗍	Hiren'	s BootCD	Ticte	ona	📌 Ulipboard - Irfan	La FO	📌 capture_	181120 🦻 22:26

必需以PIO方式連接硬碟



解開ATA加密

Victoria 4	4.46b Free	ware (12.	08.2008)					_ 8 ×
VDC WD1:	200BEVS-	08RST2	SN: WD-W	/XEX07318797	Fw: 08.01G08	234441648 LBA (~111	GB)	22:26:31
tandard	SMART	Tests	Advanced	Setup		O API ⊙ PIO Port	960h	 Hints
		Drive pa	assport:			Custom T	lav.c	
lodel: 'irmwa Serial:	WDC WI 08.01G0 WD-WXE	D1200BI 18 Ex07318	EVS-08R		Scan All dev	960 B62 V a	lt-st	All
isk si HS: Mart:	2344410 16383/1 Enabled	648 LBA 6/63 I, Erriog	s , Selftest	114473 Mb 8063 Mb	Host protected area	⁸ [LBA, kb, Mb, Gb, %] ♥ E; ┃	XT EMF BA/M	<u>S</u> leep
ACHE: upport: AM val:	8192k; I LBA, HP 254	JA=ON; A, AAM,	Wr=ON; APM, DL	ok UDMA-6 Maximum Minimum	Seek. Acoustic man	agement & BAD'er 234441647 M • S	eek	Re <u>c</u> all
rase: ecurity: TA-8:	~52 min ON, Hig SATA1, I	utes <mark>h, Locke</mark> NCQ, PE	d C, SCT,	MINIMUM	n/a v t° 0 0.0 ms	0 0 P	eniy leac l <mark>ad!</mark>	<u>R</u> eset
				Ν	Seek TINK .			Rd Wrt
)pen BIN) 🗖 LB/	48 bit	reserved		Lock Jnlock	O Master	eer	Passp
] save	SA"	TA dev	🖌 reset+	EXI Passpor	password		F	Power
RR	X COR	R DRQ	DRSC W	RF <mark>DRDY</mark> BUSY	MINE TONE A		BBK	50 00
2:26:16	Nvidia/ID I	0267*, Bl	JS: 0/DEV: 15	i/FUN: 0				48
::26:23 1:26:23 1:26:23	Reset OK Get passp <mark>This drive</mark>	ort OK locked b	iy ATA passv	vord!				□ DRD\ ✓ sounc
2:26:23	Model: W[DC WD1:	200BEVS-08F	RST2; Capacity: 23	4441648 LBAs; SN: WE	D-WXEX07318797; FW	-	
Start 📴	🔤 🙆	🔀 Hiren':	s BootCD	Victoria	🍀 Clipboard - Irfan 📔	🔉 F:\ 🛛 👫 o	apture_	181120 🛛 🕉

右下F按下去導入密碼檔



解開ATA加密

🚽 Victoria 4.46b Freeware (12.)	08.2008)			
WDC WD1200BEVS-08RST2	SN: WD-WXEX07318797	Fw: 08.01G08	234441648 LBA (~111 GB)	22:27:24
Standard SMART Tests	Advanced Setup		O API O PIO Port 960h	Hints
Model: WDC WD1200BE Firmwa 08.01608 Serial: WD-WXEX07318 Disk si 234441648 LBAs CHS: 16383/16/63 SMART: Enabled, Errlog,	EVS-08R 797 s 114473 Mb 8063 Mb Selftest	HPCI M/F Scan All dev Host protected area	Custom □ slave 960 B62 ✓ alt-st .BA, kb, Mb, Gb, % ✓ EXT .TEMF IBA/M	Break All Sleep
CACHE: 8192k; L/A=ON; ' Support: LBA, HPA, AAM, / AAM val: 254 APM val: 128 Erase: ~52 moutes Securit: OFF ATA-8: SATA1_NCQ, PE	Wr=ON; ok APM, DL UDMA-6 Maximum Minimum	Seek, Acoustic manae 0 0 23 n/a v t* 0 0 0.0 ms	gement & BAD'er 4441647 M ● Seek ○ Verify ○ Reac Limit 10000 ○ Bad!	Re <u>c</u> all <u>R</u> eset
Open BIN ■ LBA 48 bit	reserved ▼ reset+ EXT Passpa	Seek Control C	Master O High Erase User O Max Deep	Rd Wrt Passp
	DRSC WRF DRDY DC			50 00
22:27:17 Unlock complete 22:27:17 Send password froi 22:27:18 PWD removing con 22:27:18 Reset OK 22:27:18 Get passport OK	m file: pw1. Type: USER, leve			☐ 48 ☐ DRD\ ☑ sounc
🥙 Start 🔞 🔤 🏠 💥 Hiren's Bo	ootCD 🛉 Victoria	🍀 Clipboard - Irfan 🛛 🎑 F:\	 	120 🕉 22:

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		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 強装資料操作畫面

rameters			8	
opying Command to read HDD power supply Error handling	Loss of readiness Heads ma	p)		
Loss of readiness		-		
Jump size	(110000000)	256	Sector	
Timeouts				
Waiting for readiness in PIO mode	(0100000)	10000	ms	
Waiting for readiness in UDMA mode	(05000)	2000	ms	
Waiting for readiness after power ON	(0600000)	25000	ms	
Waiting for readiness after Soft Reset	(060000)	2000	ms	
Waiting for readiness after Hard Reset	(060000)	10000	ms	
Utility actions Execute script Software reset Hardware reset Turn off/on drive's power Initialization Recalibration Disable "AutoRelocation" while reading (HDD RAM) Disable read look-ahead		Attempts	1	
Default Reference		🗙 Cancel	🗸 Apply	
20				O SSL:

強拷機自製硬碟斷電電路







```
// Get pid
$st = proc get status($proc);
$pid = $st['pid'];
$watched = array($pipes[1]);
Snull = null:
stream set blocking($pipes[1], false);
while(($changed = stream select($watched, $null, $null, $)) !== 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:
       ... stoping ddrescue ({$pid}) ";
echo "
fclose($pipes[0]);
```



Flash資料救援取證





SD Card PCB





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 文件分置系统

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.

\$ h e	exdump -Cr	nobile	e/Lib	rary	/SMS	S/sm	s.db		hea	ıd					
0000	0000 09 1	7d b1	05 4	8 b1	bb	6d	65 (02	1e	d3	50	67	da	3e	.}HmePg.>
0000	0010 6e 9	99 eb	3c 9	f 41	fa	с7	91 (с4	10	d6	b2	2f	21	b2	n<.A/!.
0000	0020 39 8	37 12	39 6	d 5c	96	7d	4a k	bd	al	4a	ea	49	ba	40	99m\.}JJ.I.@
0000	0030 96 5	53 c4	d3 8	1 0d	6e	73	98 (6c	91	11	db	e0	c2	3d	.Sns.l=
)0040 7a 1	L7 82	35 1	8 59	fb	17	la k	b2	51	89	fc	8b	55	5a	z5.YQUZ
	0050 95 ()4 a0	d6 2	d d5	6a	6c	e8 a	ad	65	df	ea	b4	a8	8b	jle
)0060 7e d	de cl	d2 b	2 8a	30	e9	84 k	bb	80	9a	58	9a	ad	ba	~0X
0000	0070 bb k	ba bl	9e 2	a 95	67	d7	be a	al	4b	a7	de	41	05	56	*.gKA.V
0000)0080 d5 4	le 8b	d6 3	b 57	45	d2	76 4	4e	67	с0	8b	10	45	d9	.N;WE.vNgE.
0000	0090 7b 2	2a c3	c9 1	1 f4	c5	f0	56 8	84	86	b7	46	fe	56	e8	{*VF.V.

\$ 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 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 00 2d e2 1f 0d 00 00 00 00000060 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



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/iphonedataprotection/ 可自由下載



JI Brandisk

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	已 JB Exploit 掛載鑑識用 Ramdisk	
	請注意,本軟體不負任何法律責任. 本軟體為OSSLAB 實驗室thx, soron 作品,不負責使用者使用本軟體的行為. 請在下列選單中選擇您的裝置,並輸入對應的編號進行,離開請按任意鍵。	
	Iphone 4 (GSM)	
	OK Cancel	
	21	

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。

ο

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 Alkeychain

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。





鏡像解密

35

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 Wiindd↔ _ □ ×

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

SSLab

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

■ 系統管理員: IOS forensic Tools for Wiin V0.2 beta powered by OSSLab soron and Thx 😂 💷 😐	23
IOS forensic Tools for Windows VO.2 beta By thx@osslab.com.tw from Taiwan soron255054@hotmail.com soron(凌羽) from Taiwan http://www.osslab.com.tw	4 III
special thanks jean.sig and jb security labs	

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 可以看到大部分都是相同的選項

■ IOS Forensic Tools for Wiindc↔ _ □ × 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



數位鑑識軟體捐發思維

■ IOS Forensic Tools for Windows 😂 🗖 🖻 🔀
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

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.



Wifi Apple ID

wifi帳號密碼和APPLEID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 : Account : Password : Agrp : apple	38B7A7F1-5CE9-40BA-AE07-BD467E0204D7
Service : Account : Password : Agrp : com.app	push.apple.com <binary data=""> : 7c7f5532ef27a72b2c59f3e033a8c488e394030a68286ab5e89e48e0650a18dc le.apsd</binary>
Service : Account : Password : Agrp : apple	AirPort youth 3f
Service : Account : Password : Agrp : apple	AirPort pci
Service : Account : Password : Agrp : apple	AirPort ayi.tw

📄 passwd.txt - 記	事本
檔案(F) 編輯(E)	格式(Q) 檢視(V) 說明(H)
Server : Account : Password :	api.openfeint.com:0 kMPOAuthCredentialConsumerKey tz5yU2PdoYJ1VLG67nlwfg
Server : Account : Password :	imap.gmail.com:143 dtk1111@gmail.com
Server : Account : Password :	smtp.gmail.com:25 dtk1111@gmail.com
Server : Account : Password :	api.openfeint.com:0 kMPOAuthCredentialConsumerKey DaAhQ7br3cDvQXv7rOvj1g
Server : Account : Password :	api.openfeint.com:0 kMPOAuthCredentialConsumerKey hPgFiu4oSHFyZk7kdYXf3g
Server : Account : Password :	api.openfeint.com:0 kMPOAuthCredentialConsumerKey H3UXVZQSAVODysyAsOKhw *

系統密碼與key.plist

系統鎖屏密碼,



力破解系統密碼

獲取到解密用的

key.plists

檔

iOS設備的Escrow

/ 😭	NMX 🖣	1L View	
1		<pre>count version="1.0" encoding="UTE_P"2></pre>	
-		<pre>clant version= 1.0 encourned off = :/ clant version= 1.0 encourned off = :/ clant version=</pre>	1 0 d+d">
5	_	<pre>cplot varanter "1"></pre>	1.0.464 >
4	_	vdiat	
-	-		
ě	_	<pre> dist</pre>	
7	_	<hr/>	
6	_	data data data data data data data data	
6	_		
10			
11		<pre>chansel (here)</pre>	
12	_	(data)	
13			
14		<pre>/data></pre>	
15		<pre><pre>>>104</pre></pre>	
16		(data)	
17		dH7rHX4/OHysfm8FALiGNO==	
18			
19		<pre><pre>/kev></pre></pre>	
20	_	<data></data>	
21		OiLO7vHDg/CVvg/WfG6P70==	
22			
23		<pre>kev>2202</pre>	
24	_	<data></data>	
25		vakiDT2dAa204WDKk9BL00==	
26			
27		<kev>2203</kev>	
28		<data></data>	
29		4SRBgsIbhwIRcaPDuUo8tA==	
30			
31			
32		<key>EffaceableStorage</key>	
33	-	<data></data>	
34		a0w0ADFH0UIxR0FC1b0N1j01F/4/S04ImgCmDpvgBVNJRtZP0N6705oZdG64J59a7hSP	

a0w0ADFHQUIxR0FC1bON1jQ1F/4/SQ4ImqCmDpyqBVNJRtZP0N67Q5oZdG64J59a7hSP

- 8qtqhGJRZOaCa0woAH11a8TcG18JsCoTEEdhy6SRZwHFwi4Q3t39rvQH5A+YtyKAvrmP
- C7QsdRzRa0wkACFGTcUgAAAALnO6JcPqUHrwU1le2hPNTfr/FSgneEPKsa1bhIJZaxBr

*

35

36

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



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



able:	aessage		• 🔍		New Record	Delete Recor
D	1	address	date	text		flags
1	2	+886972561894	1323496234	哈囉 你晚上有空嗎		1
2	3	+866926878451	1323500552	怎麼了?		
3	4	+886972561894	1323500718	要不要去唱歌?		
4	5	+866926878451	1323500799	幾點?		1
5	6	+886972561894	1323501017	10點多		
6	7	+866926878451	1323522090	有誰?		
т	8	+886972561894	1323522423	蠻多人的		and the second se
8	9	+866926878451	Edit dat	abase cell	2 - X	
9	10	+886972561894				
10	11	+866926878451	Import	Export	Clear	
11	12	+886972561894				
12	13	+886972561894				
13	14					
14	15					
15	17					
•	(]1-	II 46 15	Type of 44 char	data currently in cell: Text / S	lumeric	

*



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	New Record Delete R				
	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	





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

<u>F</u> ile I	Edit View Help				
Databa	🎽 🔚 🍤 📑 醋 🖬 🖬 use Structure – Browse Data – Execut	📸 🛅 🎝?			
Table	ABMultiValue 🔻 🔍			New Rec	ord 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		1	18672870045
4			111		4





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

		sunmary		location	description	start_date
1	1	演試		台灣	你好!	35055720
			Edit database cell		Clear	
			測試			
			Type of data current 2 chars	ly in cell: Text / Numeric		
				Close Apply (Changes	

Lab

Browser書簿

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

Rowse & Search Events COL DR Catting

inucture	provise a se	aren Exe		ob Settings			
TABLE	bookmarks		Search (<u>H</u>)	Show All	Add (<u>A</u>) Duplicate (<u>P</u>) Ed	it (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
00		100			the second the second states.		4



*

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>
     <arrav>
           <integer>1</integer>
     </array>
     <key>lastVisitedDate</key>
     <string>362113495.9</string>
     <key>redirectURLs</key>
     <arrav>
           <string>http://iphone4.tw/forums/showthread.php?t=181818</strine
     </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>
```

SLab



◆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 解答

	2012-01-00 17.24.15	100771217.0771		l
	2012-01-08 17:25:30	-	Agaib	
	2012-01-08 18:55:21	Allocation and	你到了?	
	2012-01-09 09:56:00	100	有做出?	
	2012-01-09 09:58:37	-	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	Concernance of the local diversion of the loc	G6 似乎沒辦法插那張 ISCSI 卡。	
-	2012-01-10 21:46:04	CONTRACTOR OFFICE	另外,我還要多拿一個usb外接盒,及借一個60g硬碟。	l
	2012-01-10 23:15:22	100	Intel 網卡拔掉 換上boardcom 2 port or boardcom 1 port 這在塑膠櫃內	
	2012-01-10 23:17:39	-	Image	
	2012-01-10 23:17:51		Ok	l
	2012-01-10 23:19:20	- and the second second	把 G6 的 ISCSI 换掉?	l
-	2012-01-10 23:20:12	the second states	還是17上的?	l
	2012-01-10 23:25:24	the second second	開機了。	
	2012-01-10 23:39:08	AND PERSONNEL OF THE PERSON NAMED	我走囉。	1



充電器可能暗意陷阱

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λ 止" 布雷器" 直接觀看所有記錄。





bimobiledevice--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

