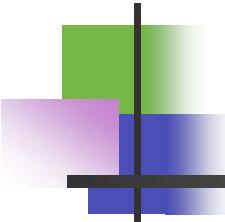


數位鑑識之平板應用程式-玩與完



DOP Shiu-Jeng WANG / 王旭正

- 
- 中央警察大學 資訊管理系
 - 中華民國資訊安全學會 (www.ccisa.org.tw, 理事 (2000-2012)
 - 中華民國資訊安全學會 副理事長 (www.ccisa.org.tw, 2012-)
 - Visiting Scholars at FSU and UF in USA, 2002, 2004, 2010.
 - Academic tour for International Project Inspection at CMU in USA, 2007
 - Columnists of Domestic Information-tech Magazines, <http://www.netadmin.com.tw/>
網路通訊/iThome/網管人雜誌, 2002-2006, 2007-至今
 - Director of ICCL, <http://hera.im.cpu.edu.tw>
(Information Cryptology and Construction Lab.)
 - sjwang@mail.cpu.edu.tw, <http://www.wretch.cc/blog/icclsjwang>

Outline

- ICCL-FROG
- Forensics and Evidence (軌跡)
- Anti-Forensics (滅跡)
- IM Forensics
- Case Study
- iPhone Discussions
- Conclusions

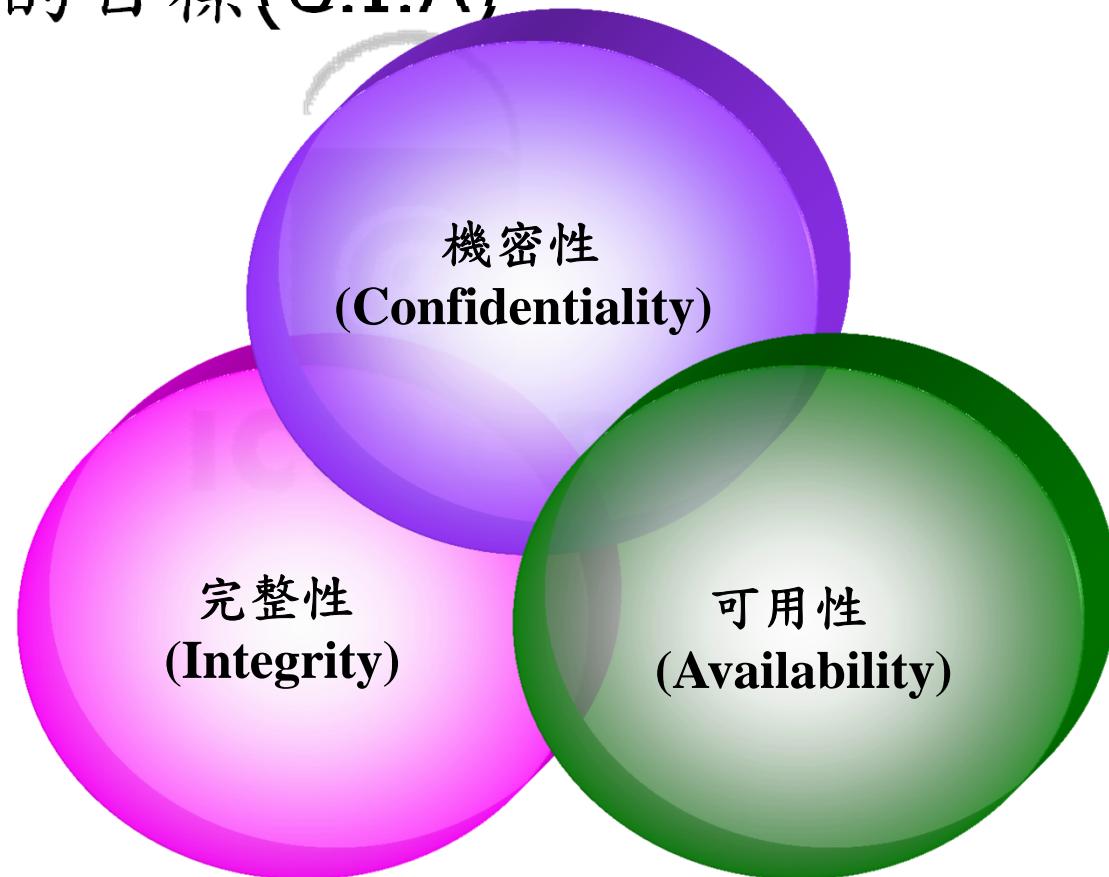


MY FROG and the FROG with you



C.I.A.

■ 資訊安全的目標(C.I.A)



Managements & Sensitive

“TIME”:

- T:
- I:
- M:
- E:



ICCL@B

How about C.I.A.

- 機密性
- 完整性
- 可用性

Cyber Crime

- 電腦犯罪日漸嚴重(調查報告)
 - 調查報告美國在西元兩千年後因電腦犯罪所產生的財產損失即增加43%，由 \$US265 million 增加為 \$US378 million (FBI案件統計)
 - 美國85% 的企業及政府機構曾偵測到計算機系統遭到入侵
- 資料來源: <http://www.smh.com.au/icon/0105/02/news4.html>

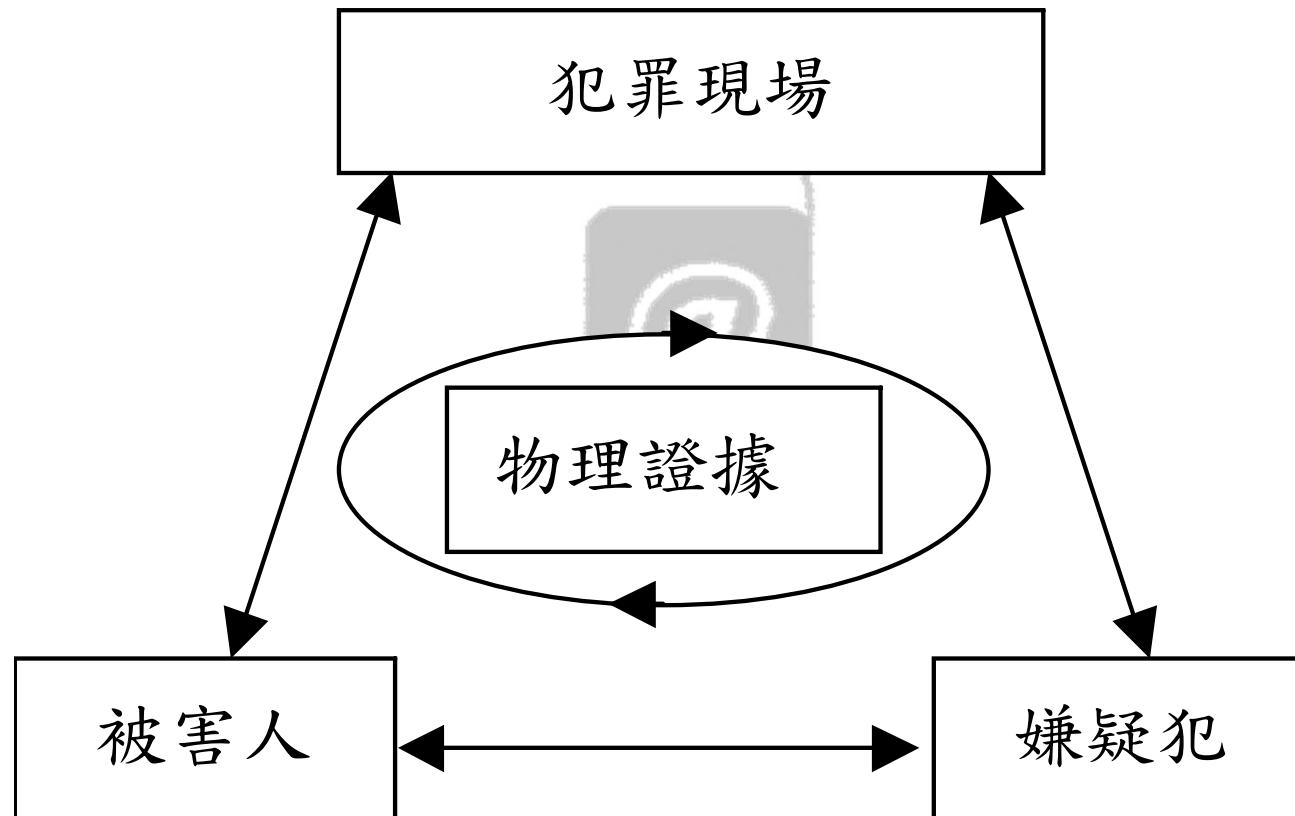
鑑識科學(Forensic Science)

■ 定義

- 運用科學於執法
- 科學：化學，生物學，物理學，地理學，...
- 目標：確定**犯罪現場及相關證物之證據能力**

 ICCL@B

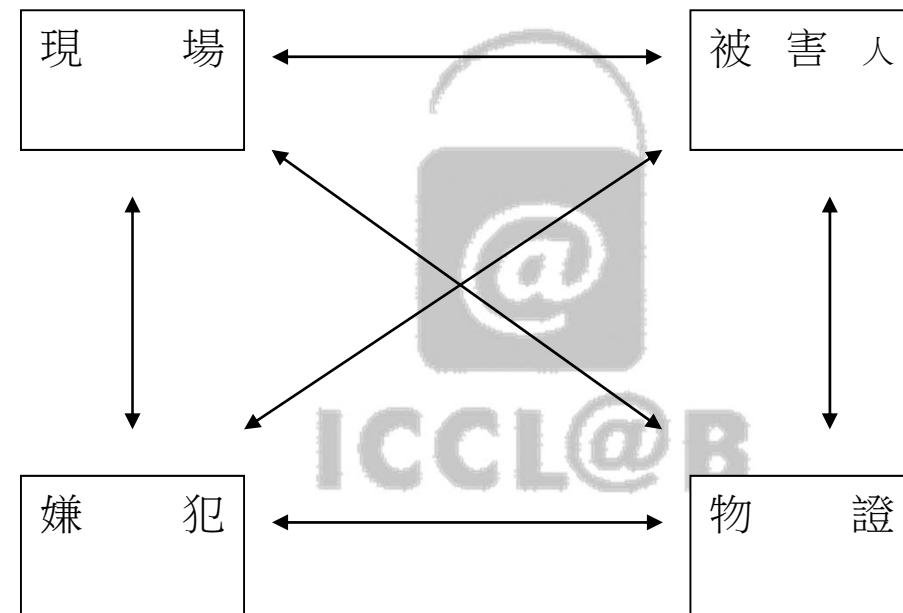
鑑識科學 (Locards's Exchange Principle)



Implications

- 多方面偵查，**勿勿下結論**:除數位證據之外，仍需訪問受害人、目擊證人、以及檢視相關之**物理證據**。
- 探討**犯罪者之行為特質**，可據以作為推論犯罪模式
 - 犯罪地點及型態
 - 接近及控制被害者之方式
 - 犯罪者之作為、不作為、及反應。
- 探討**被害者之特質**
ICCL@B
 - 可藉以了解犯罪者，及其與被害者之關係。
 - 網路跡證與被害者之關係。
 - 可藉以推測受害者之類型並提出警告。
 - 犯罪者之**冒險因素**及被害者之**危險因素**。

犯罪現場的立即偵查



四相面間連接方式基本原則

Computer Forensics

(Warren, G. Kruse ii and Jay G. Heiser, 2002, *Computer Forensics – Incident Response Essentials*, Addison Wesley)

■ 定義：

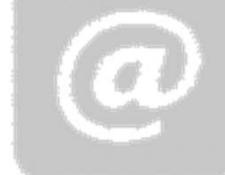
- 以周延的方法及程序**保存, 識別, 抽取, 記載, 及解讀**電腦媒體證據與分析其成因之科學

■ 方法與基本原則：

- 在不改變或破壞證物的情況下**取得原始證物**
- **證明**所抽取的證物來自扣押的證物
- 在不改變證物的情況下**進行分析**

證物之抽取

- 從電腦系統抽取證物
 - 是否即刻關機或斷絕網路連線需視情況而定
 - 從運行中的系統抽取證物
- 證物處理:
 - 證物鏈之管理
 - 採證
 - 證物之識別
 - 證物之運輸
 - 證物之保存
 - 偵查活動之記載



ICCL@B

證物之分析

- 將原證物完整拷貝兩份
 - 包含正常檔案,刪除檔案, 及硬碟之其他部分
- 重複鑑定證物



ICCL@B

Example to digital information

- 通連紀錄
- 交易紀錄(如提款、購物、轉帳等等)
- 電子郵件備份
- 網路連線紀錄
- BBS 備份
- 機密文件



ICCL@B

數位證物鑑識之目的

- 確認嫌犯
- 起訴犯罪者
- 保護無辜
- 了解犯罪行為與動機



數位證據與物理證據之比較

- 為物理證據之一種
- 易於複製與修改
- 不易證實其來源及完整性
- 無法直接被人類所感知、理解的內容



ICCL@B

數位證據與犯罪重建

- 重建被刪除、破壞、隱藏或加密之資料。
 - 利用特殊工具。
 - 利用公用程式。
 - 破解密碼(猜解密碼)。
- 推論犯罪事實 (5W1H)
 - 何事(What)
 - 何人(Who)
 - 何時(When)
 - 何地(Where)
 - 如何(How)
 - 為何(Why)



ICCL@B

檔案系統證物之蒐集

- 正常檔案：搜尋，文件分析，...
- 加密檔案：密碼分析與破解，...
- 已刪除檔案
- 剩餘空間(slack space)之資料



討論

- 司法與執法機關對泛電腦/網路犯罪行為上，已開始利用鑑識工具對數位證據進行分析
- 利用六何(5W1H)要件作為分析條件，以求獲取相關電腦網路證據。
- 法律並非打擊犯罪的唯一手段，正確的網路倫理及使用方式才是抗泛電腦/網路犯罪的重要概觀。

Outline

- ICCL-FROG
- Forensics and Evidence
- **Anti-Forensics** (滅跡)
- IM Forensics
- Case Study
- iPhone Discussions
- Conclusions



滅跡(Anti-Forensics)

- 反鑑識(Anti-Forensics)的概論與分類
- 資料偽裝的功能與作用
- 數位證據與數位鑑識之相關性



ICCL@B

Anti-forensics

- 反鑑識指「任何在鑑識工作過程當中，意圖干涉鑑識工作，對證物的取用和存取嘗試以干涉鑑識工作者稱之。」
- 反鑑識的運作策略
 - 對資料的攻擊
 - 對工具的攻擊
 - 對分析者的攻擊

反鑑識的運作策略

■ 對資料的攻擊

- 刪除或者竄改可能的證物，讓這些資料變得無法理解，而導致該證物在法庭上失去證據效力

■ 對工具的攻擊

- 利用電腦鑑識工具漏洞或弱點，試圖更改鑑識作為，以產生偽造的鑑識成果或報告

■ 對分析者的攻擊

- 透過產生大量無意義的資料來混淆視聽，或者質疑鑑識工作的有效度和可信度，以擾亂鑑識工作者

反鑑識的分類

■ 資料隱藏

- 證據透過某些技術，藏匿於系統當中的磁碟、殘存空間 (Slack Space)、隱匿資料、轉換頻道或者是Rootkit當中

■ 資料抹除

- 為了要避免被追蹤出身分，最好的方法就是刪除掉所有關於他在別人電腦的活動記錄了。
 - 有「簡單地刪除」和「安全地刪除」二種方法。

■ 蹤跡混淆

- 目的為混淆執法人員執行反鑑識程序
 - 零足跡、清除記錄器、錯誤資訊的創造、木馬命令、阻礙證據的取得等方法

資料偽裝的功能與作用

- 廣義的資訊隱藏指將**敏感／重要**的資料藏於無害的溝通訊息中的一門藝術，它能讓資料維持其機密性。
- 把所欲隱藏的機密資料藏於平常中無奇的資料中，那麼被偵測到的機會就會大為降低。
- 原本檔案（掩體）只是用來分散注意力而已，它可以是任何東西，例如一張山水風景照片、一封情書、一則簡訊、一則影片……等。
- 檔案的寄送者可以利用目前已經相當成熟的軟體工具來藏匿、加密保護檔案，經過相同的工具和金鑰解密之後，收件者就能夠解密並且了解文件當中想表達的真正含意。

資料偽裝的利與弊

- 資訊隱藏是一種一體兩面的反鑑識手法。所謂「一體兩面」即資訊隱藏為反鑑識帶來了好處與壞處。
- 資料偽裝好處：
 - 敏感性資料可透過電子郵件、網路或是可攜式儲存裝置傳遞
 - 保護有價值的機密防止遭受破壞
- 資料偽裝壞處：
 - 電腦犯罪者可躲避網路或是電子郵件的偵測
 - 電腦犯罪者利用反鑑識工具來消除他們犯案的痕跡並且防止監控

資料偽裝的應用－數位浮水印

- 數位浮水印的目的為版權宣告與防護。其技術為在檔案上加入著作者個人資訊。
- 可分為可視型與不可視浮水印二種。



+ Copyright©National Palace Museum
All Rights Reserved =



資訊偽裝的面向

資訊隱藏有許多應用，根據其應用上的不同，
我們將它們分為不同的面向：

- 資料串接
- 資料替換
- 資料延伸



ICCL@B

資訊偽裝的面向－資料串接

- 在資料中額外增加一些重要訊息，且重要訊息皆會被應用程式所忽略，應用程式如：word、網路瀏覽器等。

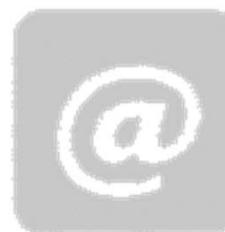


ICCL@B

- 優點：
 - 可以盡可能地隱藏更多的訊息
- 缺點：
 - 因隱藏大量的訊息導致檔案大小異常的增大

資訊偽裝的面向－資料替換

- 將攜帶有隱藏資訊的檔案內較為不起眼的或是較不重要的資料刪除，留出空間給欲隱藏的資訊



ICCL@B

- 優點：
 - 可隱藏較大量的訊息
 - 檔案大小固定（不因隱藏較大量的訊息而增加檔案的大小）

資訊偽裝的面向－資料延伸

- 產生了一新的偽造檔案或訊息，這些檔案可能看起來就只是普通的電子郵件、一首詩、或是一封不起眼垃圾郵件而已



- 範例：spam mimic 網站為例
(<http://www.spammimic.com>)

資訊偽裝的面向－資料延伸(Cont.)

■ 首頁

The screenshot shows the homepage of spammimic.com. At the top, there is a logo consisting of the words "spam" and "mimic" in a stylized font, with "spam" above "mimic" and a small circle between them. Below the logo, a horizontal line separates it from the main content area. The main content area has a dark blue background. It contains the text "First time here? ... Read the [explanation](#). Hope you're using the secure connection." followed by two buttons: "Encode" and "Decode". The "Encode" button is associated with the text "Turn a short message into spam" and the "Decode" button is associated with "Turn spam back into the original message". Below these buttons is another horizontal line. At the bottom of the page, there is a navigation bar with links to "home", "encode", "decode", "explanation", "credits", "faq & feedback", "terms", and "Français". A copyright notice "Copyright © 2000-2010 spammimic.com, All rights reserved" is also present. In the bottom right corner of the main content area, there is a white rectangular box containing links to "Email Hosting", "Data Recovery Software", "HP Printers", and "Allen Collins Psychiatrist".

資訊偽裝的面向－資料延伸(Cont.)

■ 訊息偽裝

The screenshot shows the homepage of the **spam mimic** website. At the top, there's a logo with the words "spam" and "mimic". Below it, a horizontal bar contains the word "Encode" in green and three small circles. The main area has a teal background. It asks "Enter your short secret message:" and has a text input field containing "hello! word" with a blue "Encode" button next to it. Below this, under "Alternate encodings:", is a list of options: "Encode as spam with a password", "Encode as fake PGP", "Encode as fake Russian", and "NEW Encode as space". At the bottom, there's a navigation bar with links: "home | encode | decode | explanation | credits | faq & feedback | terms | Français". Below that, a copyright notice reads "Copyright © 2000-2010 spammimic.com, All rights reserved". At the very bottom, there's a white rectangular box containing links to "Email Hosting", "Data Recovery Software", "HP Printers", and "Allen Collins Psychiatrist".



資訊偽裝的面向－資料延伸(Cont.)

■ 偽裝後訊息



Encoded

Your message hello! word gets encoded into spam as:

Dear Decision maker , We know you are interested in receiving amazing intelligence . This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 1625 ; Title 4 ; Section 302 . THIS IS NOT MULTI-LEVEL MARKETING ! Why work for somebody else when you can become rich as few as 33 WEEKS ! Have you ever noticed how many people you know are on the Internet and most everyone has a cellphone . Well, now is your chance to capitalize on this ! WE will help YOU use credit cards on your website and deliver goods right to the customer's doorstep ! The best thing about our system is that it is absolutely risk free for you . But don't believe us ! Prof Simpson who resides in Washington tried us and says "My only problem now is where to park all my cars" . We assure you that we operate within all applicable laws ! We implore you - act now ! Sign up a friend and you get half off . Thanks .

Decode

Mail it

(Zap this message into your mailer
...but it won't be sent until you click on
Send)

or

You can copy the message out of the text
box and paste it into a mail.

- Launch your mail program
- How to copy and paste in Windows
- How to copy and paste in X
- How to copy and paste on a Mac

數位證據

- 「數位證據」指存在於電子儲存媒體中的**磁性狀態、數位訊號**等資料，憑藉這些證據可與電腦犯罪做連結。
- 數位證據具有下列幾項特色：
 - 現代化
 - 多樣化
 - 不穩定性

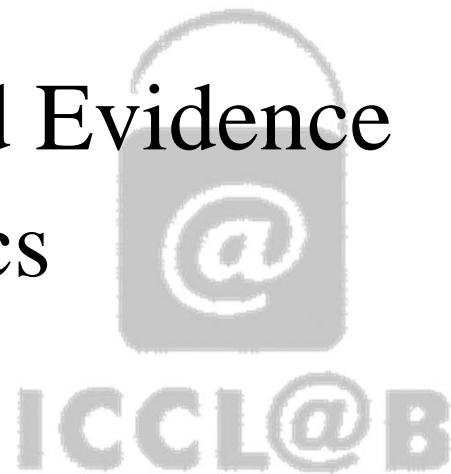
ICCL@B

數位鑑識

- 數位鑑識工作的目的為擷取、整理、分析這些和犯罪行為有關的資訊，並讓這些資訊在調查程序中還原真相，而使之具有證據能力。
- 數位鑑識的程序，目前的法律還沒有一定之規範，因此，如何讓鑑識的程序合法化一直是目前數位鑑識工作者努力的目標。

Outline

- ICCL-FROG
- Forensics and Evidence
- Anti-Forensics
- IM Forensics
- Case Study
- iPhone Discussions
- Conclusions



Memory的資料佈局

- 存儲器資料的收集
 - 實體存儲器傾印工具：win32dd
 - ✓ 與windows 系統是高相容性
 - ✓ 不需要重開機或是做額外的設定而產生 Microsoft 的crash dump 檔案

Memory的資料佈局 in case of MSN

蒐集到的數位證據：

- Windows Live Messenger所登入的帳號及密碼：以嫌犯的身份登入即時通訊服務，進而蒐集到更多的資訊，如E-mail或網路銀行。
- Windows Live Messenger的聯絡人清單：可以勾勒出嫌犯的社交網路圈以及聯絡人間的鏈結關係
- 與其他聯絡人的聯絡內容：深入了解嫌犯在網路上與他人的互動細節、關係背景、聯絡頻率等

Summary

- 電腦和數位裝置被拿來當成犯罪活動的使用已無可避免。因此，實體Memory可以被拿來當做一個證據的來源。
- Windows Live Messenger是一種相當普遍的即時通訊軟體，本文著重在從網頁版Windows Live Messenger的資料回復，企圖找出相關資訊，蒐集具易揮發性資料，並重建使用者使用MSN的過程，進而解決鑑識調查的需求。

Outline

- ICCL-FROG
- Forensics and Evidence
- Anti-Forensics
- IM Forensics
- **Case Study**
- iPhone Discussions
- Conclusions



Case Study

■ 案例說明：

- 大○發公司是P產品的大盤商，每個月依照不同的需求向生產P產品的A工廠與B工廠進貨。而A工廠與B工廠會依照庫存狀況決定供應大○發公司P產品的數量。
- 現今A工廠發現其銷售量逐月下降，因此，A工廠決定潛入B工廠的系統中，竄改庫存量，而造成B工廠減少提供P產品的數量，導致大○發公司向A工廠增購P產品的數量

Case Study (Cont.)

- A工廠在入侵與竄改B工廠的資料庫同時，為了避免被發現行蹤，因此，A工廠也同時竄改了資料庫中的「最後存取時間」、「存取事件之型態」等登錄檔案。
- B工廠對於商品庫存資料庫內容也定期逐月更新與備份。
- 某天，B工廠發現該工廠的產品訂單需求量有異常時，B工廠就開始清查所有的記錄。

Case Study (Cont.)

- B工廠首先檢視其庫存記錄資料庫，發現某月的產量異常下降，與生產線運做確認後，比對生產部呈交的產品資料與庫存資料，發現有不一致的情況。
- B工廠就調閱備份資訊，發現資料庫的資料已經遭受他人更改，但資料庫系統的登入檔卻均符合正常的輸入與輸出。此時，B工廠也開始懷疑登入檔的正確性。

Case Study (Cont.)

- B工廠平常的登入檔資訊以資訊隱藏技術偽裝到圖片中。如圖示：



未隱藏資訊之圖形

隱藏資訊後之圖形

Case Study (Cont.)

- B工廠調閱出偽裝的圖形檔，並從圖形中擷取出登入檔的資料，並與資料庫顯示之登入檔有異，如下表一，二所示。

ID	Administrator
Date	2011.05.01 08:02:30
Sever	record
File route	Production
type	writes

表一 備份之登入檔資訊

ID	unknown
Date	2011.05.01 08:40:24
Sever	record
File route	Production
type	writes

表二 資料庫所顯示之登入檔資訊

- 從對照發現，資料庫中的登入檔確實遭受到竄改，究其原因，應是競爭者刻意更改記錄。

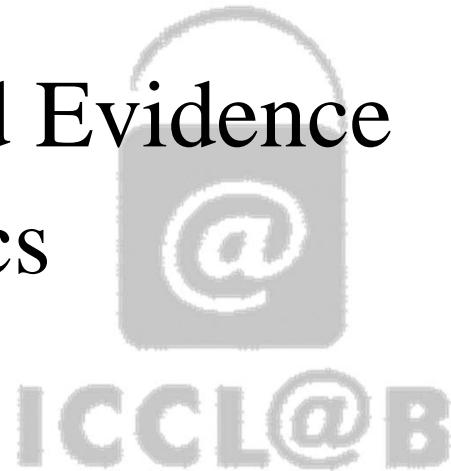
Case Study (Cont.)

- 從案例中，B工廠利用資料偽裝技術防護與保存重要資料。
- B工廠可以憑藉所保存重要資料與電腦犯罪做連結，因此，能夠追溯出可能的涉嫌者-A工廠。

ICCL@B

Outline

- ICCL-FROG
- Forensics and Evidence
- Anti-Forensics
- IM Forensics
- Case Study
- iPhone Discussions
- Conclusions



數位鑑識之平板應用程式-玩與完



王旭正

大綱

- 1. Technology-Time, Mobile Forensics-iPhone
- 2. iPhone 相關背景介紹
- 3. 應用程式備份檔案
- 4. 案例說明
- 5. 結論



ICCL@B

前言

- 至2016年，包括手機和平板電腦的應用程式下載量將達到440億次。
- 目前，最重要的app下載來源為Apple公司的App Store以及Google的Android Market，兩大平台的app下載量分別為100億以及42億，app的數量分別為35萬與33萬。
■ From美國聯合商業情報研究公司(Allied Business Intelligence Research, ABI Research) 的統計

前言 (續)

- iPhone手機裡有哪些東西?
 - 聯絡人通訊錄、備忘錄、簡訊、通話紀錄、圖片、電子郵件、GPS定位資訊以及網頁瀏覽紀錄等等。
- iPhone轉變為重要且關鍵的數位證據?
 - 被犯罪者作為溝通的平臺
 - 如何取得App相關數位證據From iPhone?

iPhone 數位鑑識方法

- 手機端(須有手機)
 - 手動萃取
 - 實體工具
 - Jailbreak
 - 邏輯萃取
 - 鑑識軟體工具
- 電腦端(不需手機)
 - Apple iTunes備份檔案



ICCL@B

手動萃取

- 數位證據的特性：無法透過人類的感知而獲知證據內容-須透過媒介
- 鑑識人員直接操作
- 許多畫面圖片資訊
- 需經由鑑識人員理解、彙整與轉化
- 易發生人為錯誤

實體萃取

- iPhone手機的內部記憶體被分為兩個區塊。
 - 系統分區，存放iPhone手機的作業系統以及必要的應用程式，只保留原廠的設定而不包含使用者資訊。
 - 使用者分區，包含所有使用者相關檔案、應用程式及手機相關使用資訊。
- 必須嘗試在系統分區中安裝鑑識工具。
- 「越獄」(Jailbreak, 簡稱JB)的程序

越獄是什麼？

- 一種針對iOS進行破解的技術程序
- 透過越獄可以獲得使用產品的最高權限，解開功能限制，能安裝並執行App Store以外之軟體
- 透過JB在系統分區安裝鑑識軟體，方能執行實體萃取，但卻有爭議性
- JB是否合乎數位鑑識程序？
- JB是否會對使用者分區資訊造成更動？
 - 完成後需重開機

邏輯萃取

- 依照檔案系統的邏輯架構儲存方式
- 透過作業系統所編制的目錄與路徑執行數位證據的萃取
- 若檔案或資料已被刪除，則因其索引目錄已遭刪除，**無法取得已被刪除的檔案**
- 邏輯萃取的優點在於對鑑識軟體工具的高支援度

軟體工具

- 瑞典Micro Systemation公司
 - XRY商業手機鑑識工具組



- 美國Paraben公司
 - Device Seizure工具組。



Apple iTunes與iPhone備份檔案

- Apple iTunes是電腦端應用軟體
- 產品與個人電腦介接的驅動程式與管理平台
- 具備有完整的影音播放器功能，並具備同步、備份、燒錄、共享與瀏覽App Store的功能
- 備份資訊
- 應用程式本身非備份項目
- 應用程式相關資訊為備份標的







iPhone應用程式主體

- 應用程式的主體會被放置在預設的路徑中，不會被iTunes備份到「Backup」資料夾中。
- 應用程式主體會因作業系統的不同而有不同的儲存路徑

作業系統	路徑
Mac	~/使用者/(使用者名稱)/音樂/iTunes/iTunes Media/Mobile Applications
Windows XP	C:\Documents and Settings\使用者名稱\My Documents\My Music\iTunes\iTunes Media\Mobile Applications\
Windows Vista、 Windows 7	C:\使用者\使用者名稱\My Music\iTunes\iTunes Media\Mobile Applications\

iPhone備份檔案

- 備份檔案會因作業系統不同而儲存在電腦中不同的路徑中
- 應用程式相關資訊也會被存放到此路徑下



作業系統	路徑
Mac	~/使用者/資源庫/Application Support/MobileSync/Backup/
Windows XP	\Documents and Settings\ (使用者名稱) \Application Data\Apple Computer \MobileSync\Backup\
Windows Vista、 Windows 7	\Documents and Settings \使用者\ (使用者名稱) \App Data\Roaming\Apple Computer\MobileSync\Backup\

- 「Backup」裡有一個以16進位的數字與字元所組成(0-9與a-f)，長度為40個字元的資料夾名稱
- 備份檔案同樣也是40個16進位的字元組成
- SHA-1

名稱	修改日期	類型	大小
0b68edc697a550c9b977b77cd012fa9a0557dfcb	2011/5/9 下午 05...	檔案	1 KB
0ba0507b7b46ab4bc1378adb3a9431cd145ad405	2011/5/9 下午 05...	檔案	1 KB
0dc926a1810f7aee4e8f38793ed788701f93bf9d	2011/5/10 上午 1...	檔案	1 KB
0fb54654b97099d34461570fab859a2b0570ed1f	2011/5/9 下午 02...	檔案	1 KB
0fc8189497f46a2e2511c846acbbb318d3a43ec3	2011/5/9 下午 05...	檔案	12 KB
1d6740792a2b845f4c1e6220c43906d7f0afe8ab	2011/5/9 下午 05...	檔案	2 KB
2a5ca91efd7dfa5b59d01f04fa1194a85b76b667	2011/5/9 下午 02...	檔案	23 KB
2a041bfd473c7a136dff7b42e616c84344d7f27a	2011/5/9 下午 02...	檔案	679 KB
2b2b0084a1bc3a5ac8c27afdf14afb42c61a19ca	2011/5/10 上午 1...	檔案	28 KB
2b86f69160b7cf7a32d89cd36d44a412806cbd61	2011/5/9 下午 05...	檔案	52 KB

- 在iPhone手機的檔案系統，以兩種不同的檔案格式儲存資料。
- 手機中的設定值、狀態資訊、應用程式設定與偏好設定是以XML或plist的格式儲存於plist檔案中
- 手機內容、通話紀錄、備忘錄、應用程式相關紀錄、行事曆與簡訊等則是以SQLite的資料庫格式所儲存

開啟備份檔案

- plist檔，可選用「plist Editor」
 - 需要安裝
 - 免付費
- SQLite資料庫，可選用「SQLite Browser」
 - 免安裝
 - 免付費
 - 提供SQL語法指令
- 圖片與影片檔
 - 在備份檔案名稱後面加上相對應之副檔名即可直接開啟

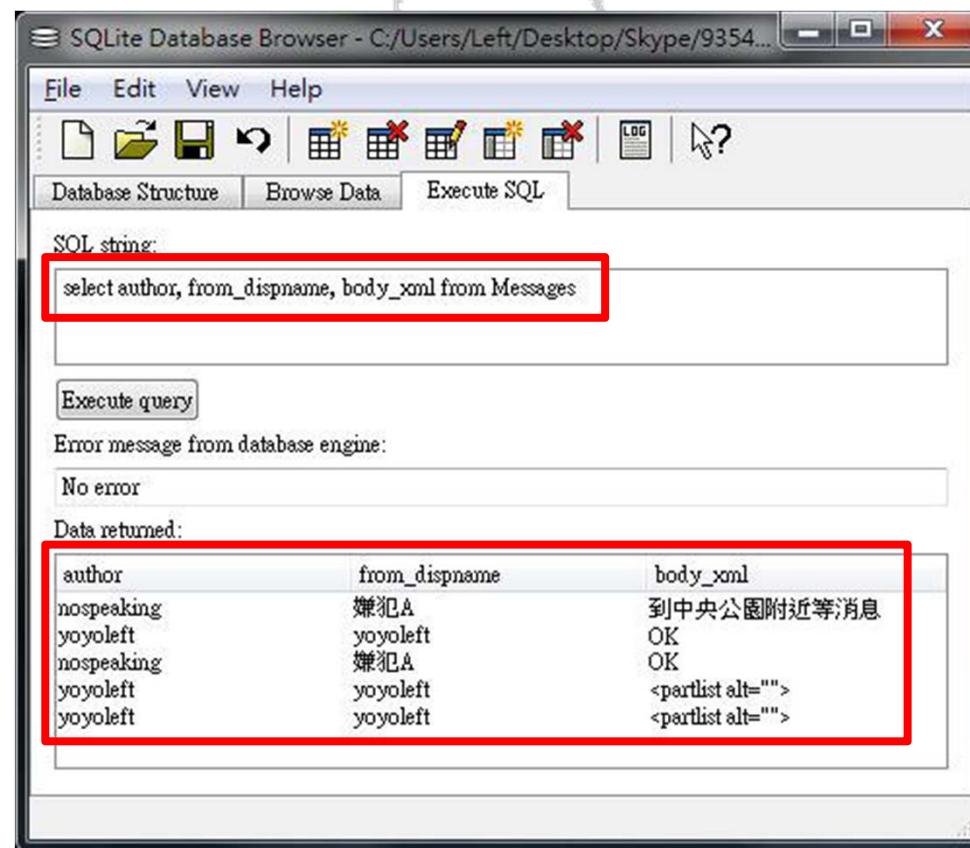


範例

- 嫌犯A為詐騙集團的首腦，平常均使用iPhone手機的社交類型應用程式作為與車手間聯繫用途，令執法人員難以掌控，現被執法人員查獲
- 經由上述的應用程式儲存路徑得知嫌犯A有使用Facebook、Skype、Viber、Windows Live Messenger與WhatsApp Messenger等5種社交類型應用程式
- 我們針對應用程式作深入分析，目的是找出嫌犯A曾與哪幾位車手有過聯繫

Skype

- 使用「SQLite Browser」軟體開啟「9354ca8233 18edc67ec21744fa9589758e6612d6」



WhatsApp Messenger

- 開啟「1b6b187a1b60b9ae8b720c79e2c67f472bab09c0」，發現嫌犯A與電話號碼「886972」開頭的人使用文字訊息聯繫

The screenshot shows the SQLite Database Browser interface with the database file 'WhatsApp/1b6b187a1b60b9ae8b720c79e2c67f472bab09c0' open. The table 'ZWAMESSAGE' is selected, displaying a list of messages. The columns are: GROUPMEMBER, ZMESSAGEDATE, ZTOJID, ZFROMJID, ZTEXT, and ZSTANZAID. The 'ZTEXT' column contains the message content. Two specific rows are highlighted with red boxes: row 3 contains the message '先在中正路郵局等消息' and row 4 contains the message 'Ok'. Both of these messages have '886972' in their ZTOJID field.

GROUPMEMBER	ZMESSAGEDATE	ZTOJID	ZFROMJID	ZTEXT	ZSTANZAID
1	339610121	886972		□	1317917188-14
2	339611184.90000	886972		□□	1317917188-43
3	339611190.981344	886972		先在中正路郵局等消息	1317918379-21
4	339611195.976220	886972		Ok	1317917188-51
5	339611224.021245	886972			1317917188-56
6	339611253.065862	886972			1317917188-61

Viber

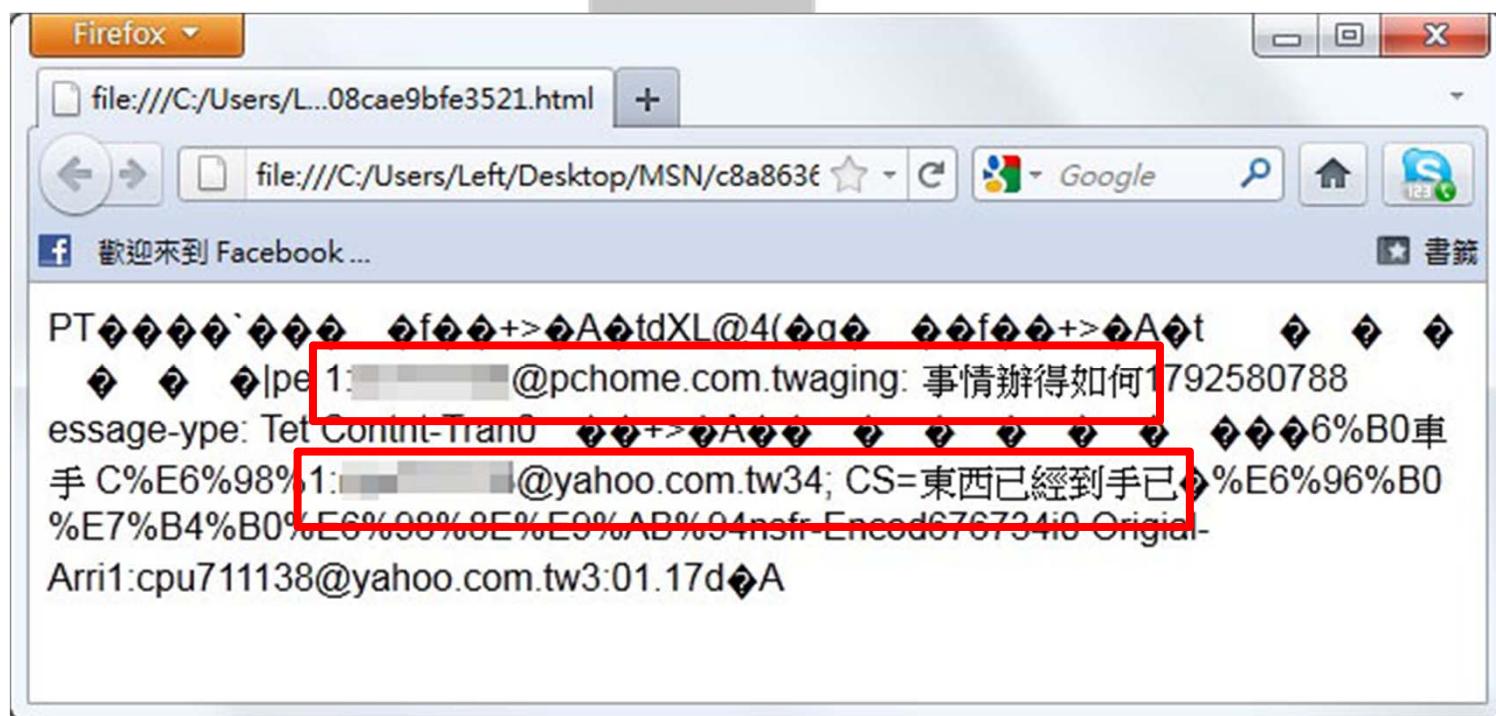
- 開啟「b39bac0d347adfaf172527f97c3a5fa3df726a3a」的資料庫中切換至「ZTEXTMESSAGE」

The screenshot shows the SQLite Database Browser interface with the title bar 'SQLite Database Browser - C:/Users/Left/Desktop/Viber/b39bac0d347adfaf172527f97c3a5fa3df726a3a'. The menu bar includes File, Edit, View, Help. The toolbar has icons for New Record, Delete Record, and other database operations. The main window displays the 'ZTEXTMESSAGE' table with the following data:

	ZPHONENUMINDI	ZDATE	ZSTATEDATE	ZTEXT	ZPHONENUM	ZSTATE
1	7007388	1	339611787	339611787 我到了	0972	received
2	1825154	1	339611801.465415	339611801 Ok	0972	delivered

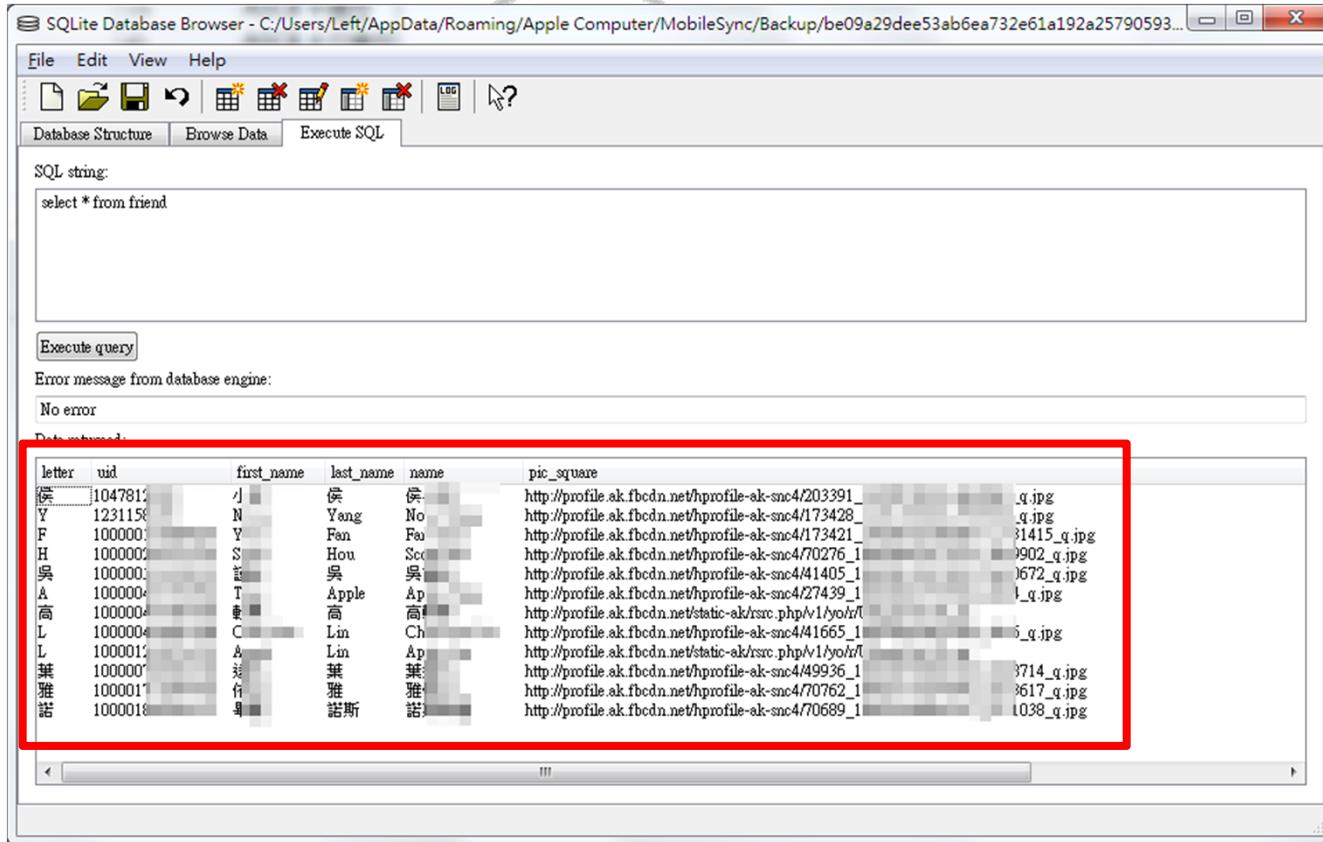
Windows Live Messenger

- 使用Firefox開啟檔案名稱為「c8a86367 39ba60336b2090abceb08cae9bfe3521」的檔案



Facebook

- 開啟「6639cb6a02f32e0203851f25465ffb89ca8ae3fa」



The screenshot shows the SQLite Database Browser interface with a query results window. The query 'select * from friend' has been run, and the results are displayed in a table. A red box highlights the first few rows of the table.

letter	uid	first_name	last_name	name	pic_square
侯	104781	小	侯	侯	http://profile.ak.fbcdn.net/hprofile-ak-snc4/203391_q.jpg
Y	1231158	N	Yang	No	http://profile.ak.fbcdn.net/hprofile-ak-snc4/173428_q.jpg
F	100000	Y	Fan	Fan	http://profile.ak.fbcdn.net/hprofile-ak-snc4/173421_31415_q.jpg
H	1000002	S	Hou	Sco	http://profile.ak.fbcdn.net/hprofile-ak-snc4/70276_1902_q.jpg
吳	100000	詠	吳	吳	http://profile.ak.fbcdn.net/hprofile-ak-snc4/41405_1672_q.jpg
A	100000	T	Apple	Ap	http://profile.ak.fbcdn.net/hprofile-ak-snc4/27439_1_l_q.jpg
高	100000	重	高	高	http://profile.ak.fbcdn.net/static-ak/rsrc.php/v1/yo/hr/l
L	100000	C	Lin	Ch	http://profile.ak.fbcdn.net/hprofile-ak-snc4/41665_1_5_q.jpg
L	100001	A	Lin	Ap	http://profile.ak.fbcdn.net/static-ak/rsrc.php/v1/yo/hr/l
葉	100000	達	葉	葉	http://profile.ak.fbcdn.net/hprofile-ak-snc4/49936_1_714_q.jpg
雅	100001	伟	雅	雅	http://profile.ak.fbcdn.net/hprofile-ak-snc4/70762_1_617_q.jpg
諾	1000018	畢	諾斯	諾	http://profile.ak.fbcdn.net/hprofile-ak-snc4/70689_1_l038_q.jpg

- 經由圖4至圖7，鑑識人員可發現曾與嫌犯A通訊過的3名可疑人員
 - 「yoyoleft」
 - 電話號碼「0972」開頭的人
 - 使用「yahoo.com.tw」帳號的人
- 透過應用程式的相關資訊，可協助鑑識人員後續的調查方向

結論

- 數位鑑識之軌跡與滅跡(反鑑識)的概觀。
- 完整的數位證據保全／防護機制，對於在電腦/網路犯罪的案件調查具有關鍵性地位，可成為法官採信的依據並影響審理的結果。
- 建立受信任的保全／防護機制，將提高數位證據在法庭上被採信的程度。

結論（續）

- 在反鑑識領域中極為重要的一項技術---資訊隱藏；資訊隱藏並不只被拿來用作反鑑識功用，也可被用來保護隱私資料、著作權的宣告與防護等。
- 反鑑識並不一定代表就是壞處，所以我們舉了一個有關於多媒體影像反鑑識的正面應用，技術只是個工具，端看這個工具被運用在何種應用上。
- 數位影像資訊隱藏技術仍正在蓬勃發展階段，我們對於數位影像資訊隱藏技術的了解，尚有進步空間，即所謂「知己知彼」，同時研究鑑識以及反鑑識技術，是可持續發展的目標！

結論（續）

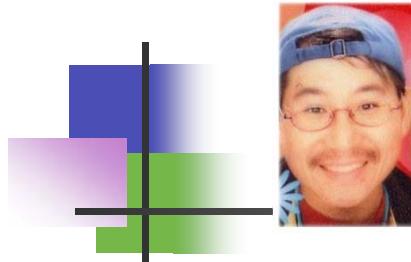
- 隨著科技的快速發展，智慧型手機的功能也日益強大，人們對於手機的依賴已經不可同日而喻。
- 平板應用程式具有諸多的功能與便利性，卻也保留了相當多的線索與蛛絲馬跡
- 若透過平板應用程式提供的便捷與強大的功能來做為非法的用途，則平板應用程式本意的玩樂，也將能提供足夠的數位證據來讓犯罪者完蛋！

5W1H with researches and lives

- “*Think why you are here*”.
- “*Find where you are interested in here*”.
- “*Marry whom you look for here*”.
- “*Get what you want to have here*”.
- “*Honor here when you own something special with knowledge*”.
- *HAKUNA MATATA – “H”*

References

- 王旭正, 楊中皇, 雷欽隆 and ICCL (資訊密碼暨資料建構實驗室), 電腦與網路安全實務, 博碩文化出版社, [ISBN: 978-986-201-254-3](#), Aug., 2009.
- 王旭正, 林祝興 and ICCL (資訊密碼暨資料建構實驗室), 數位科技安全與鑑識-高科技犯罪預防與數位證據偵蒐, 博碩文化出版社, [ISBN: 978-986-201-196-6](#), March 2009.
- 王旭正, 柯永瀚, and ICCL (資訊密碼暨資料建構實驗室), 電腦鑑識與數位證據-資安技術、科技犯罪的預防、鑑定與現場重建, 博碩文化出版社, [ISBN: 978-986-201-004-4](#), June, 2007.
- 王旭正, 柯建萱, and ICCL (資訊密碼暨資料建構實驗室), 資訊媒體安全-偽裝學與數位浮水印, 博碩文化出版社, [ISBN: 978-957-527-980-6](#), July, 2007.
- 王旭正 (資訊密碼暨資料建構實驗室), “資訊安全鑑識程序建立與有效證據萃取作業(IVL)－網路鑑識趨勢及無線入侵之鑑識,” 網管人雜誌, <http://www.netadmin.com.tw/>, 城邦文化電腦雜誌系列, Jan., 2011.
- 王旭正 (資訊密碼暨資料建構實驗室), “資訊安全鑑識程序建立與有效證據萃取作業(XXXXXIII)－資訊隱藏於數位鑑識之運用,” 網管人雜誌, <http://www.netadmin.com.tw/>, 城邦文化電腦雜誌系列, Dec., 2010.
- 王旭正 (資訊密碼暨資料建構實驗室), “資訊安全鑑識程序建立與有效證據萃取作業(XXXXXXII)－Evidence Seizure from Metadata in Computer Forensics,” 網管人雜誌, <http://www.netadmin.com.tw/>, 城邦文化電腦雜誌系列, Nov., 2010.
- 王旭正 (資訊密碼暨資料建構實驗室), “資訊安全鑑識程序建立與有效證據萃取作業(XXXIV)－諜對諜：影像玄機對壘鑑識分析,” 網管人雜誌, <http://www.netadmin.com.tw/>, 城邦文化電腦雜誌系列, to appear in May, 2009.
- 王旭正 (資訊密碼暨資料建構實驗室), “資訊安全鑑識程序建立與有效證據萃取作業(XXXIII)－直擊Unix/Linux系統入侵Using the Power of TCT鑑識,” 網管人雜誌, <http://www.netadmin.com.tw/>, 城邦文化電腦雜誌系列, April, 2009.
- 王旭正 (資訊密碼暨資料建構實驗室), “資訊安全鑑識程序建立與有效證據萃取作業(XXXII)－即時通訊媚力vs. 數位鑑識魅力,” 網管人雜誌, <http://www.netadmin.com.tw/>, 城邦文化電腦雜誌系列, to appear in March, 2009.
- H.M. Sun, C.Y. Weng, S.J. Wang, and C.H. Yang, “Data Embedding in Image-media using Weight-function on Modulo Operations,” [ACM Trans. on Embedded Computing Systems](#), accepted in March, 2011. (SCI)
- W.J. Wang, C.T. Huang, and S.J. Wang, “VQ Applications in Steganographic Data Hiding upon Multimedia-images,” accepted in [IEEE System Journals](#), March 2011. (SCI)
- S.J. Wang and D.Y. Kao, “The IP Address and Time in Cyber-crime Investigation,” [Policing: An International Journal of Police Strategies & Management](#), to appear in Vol 32. Issue 2, 2009. (SCI).
- S.J. Wang, “Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crime,” [International Journal Computer Standards & Interfaces](#), Vol. 29, Jan. 2007. (SCI)
- S.J. Wang, H.J. Ke, J.H. Huang, and C.L. Chan, “Hash Cracking and Aftereffect on Authentication Procedures in Cyberspace,” [IEEE Transactions on Aerospace and Electronic Systems](#), Jan. 2007. (SCI)



- **Dr. Professor Shiuh-Jeng WANG**
- PhD. National Taiwan University, Taiwan, 1996
- Full Professor, Central Police University, Dept. of Information Management
- Director Information Crypto and Construction Lab
- Chair of ICCL-FROG (Forensic Research development task force Group)
- Vice-President, Chinese Cryptography Information Security Association (www.ccisa.org.tw)

- Chairs of IEEE-CS/LNCS Proceedings, Internat'l confs.
<http://www.sercs.org/SH08/> <http://www.ftrg.org/MPIS2009>
<http://ncs2009.ntpu.edu.tw/CI/CI.htm> <http://www.ftrg.org/futuretech2010>
<https://sites.google.com/site/uicuipm2012/> IEEE-sponsored,
<http://www.ftrai.org/music2012>
- Editor-in-Chief AT JITAS (<http://jitas.im.cpu.edu.tw>)
- SCI-Journals, Guest-editors,-
 - IEEE J-SAC, <http://www.comsoc.org/livepubs/sac/index.html>
http://hera.im.cpu.edu.tw/sjw_2006/meeting_report/IEEE-GUEST-EDITORIAL-0808-2011-.pdf
 - Journal of Internet Technology (JIT)
<http://jit.ndhu.edu.tw/callforpaper/April-2011-SI-JIT.pdf>
 - The Computer Journal, <http://comjnl.oxfordjournals.org/>
 - Springer Telecommunication Systems
<http://www.springer.com/business/business+information+systems/journal/11235>
 - The Journal of Supercomputing,
<http://www.springer.com/computer/swe/journal/11227> (Springer)
 - Peer-to-Peer Networking and Applications,
<http://www.editorialmanager.com/ppna/> (Springer)