QR Code Forensics in the case of On-Line Game

鐘敏如　　王旭正*
中央警察大學資訊管理學系　　中央警察大學資訊管理學系
n397148625@hotmail.com　　sjwang@mail.cpu.edu.tw
* whom correspondence

摘要

QR code 現今已隨處可見，但使用者在掃描 QR code 的同時通常未具備警覺心，使得非法者利用此特性對使用者進行危害。本文透過相關的鑑識程序證明非法者即使利用 QR code 來當作犯罪的媒介，其相關的證據依舊會留存在電腦中。並以填寫遊戲網站所提供之 QR code 問卷網頁被盜取帳號為例，證實非法企圖者確實能夠利用 QR code 來從事非法行為，而鑑識人員也能在事後找出相關的蛛絲馬跡。除能警惕非法者外也能讓使用者了解使用 QR code 的方便與風險，以提升使用者未來在面對 QR code 的警覺性。

關鍵詞：QR code、非法行為、Encase

1. 前言

早期 QR code 是被用來做商品存貨管制的。憑藉它能隱含大容量的資訊以及能被快速解碼的特性，使用率越來越高。隨著時代進步，它的應用也不再限於存貨管理上面。因為不只是英數字，就連漢字、符號等都能編碼成 QR code。再搭配網際網路，使得 QR code 還被拿來應用在當作廣告文宣、快速網路購物與下載連結。除了網際網路之外，QR code 能夠快速發展的主要因素，就是因為智慧型手機的市佔率越來越高。要解碼 QR code 的條件相當簡單，只要具備 30 萬畫素以上的相機鏡頭之裝置，就能夠執行 QR code 的解碼程式。根據 IDC（國際數據資訊）研究指出，截至 2012 第一季為止，智慧型手機在台市佔率已達到 7 成。想當然爾，由於智慧型手機的鏡頭都具備超過 30 萬畫素的鏡頭。所以全國有將近 7 成的人都可以藉由手上的手機解碼 QR code。智慧型手機的普遍性再搭配網際網路，造就了現今 QR code 極為廣泛的應用。現在不管各處都能看到 QR code 的身影，有興趣的人即可利用手機掃瞄 QR code 將其解碼，就能輕易的取得相關資訊或是連接到對應的網站。然而若是非法企圖者利用這些特性從事非法行為[3][8]呢？本篇文章將介紹利用 QR code 所能從事的非法行為，並針對非法者在進行非法行為時所遺留的證據進行鑑識。本研究利用鑑識工具：EnCase，找出遺留在電腦裡的證據，而這些證據除了能證明非法者的確有從事非法行為外，將來也能讓鑑識人員做進一步的使用。

本文的結構如下。第二節介紹相關背景。在第三節說明非法者該如何利用QR code從事非法行為，以及指出該非法行為的證據隱藏在何處。第四節將提出一情境，模擬非法行為並利用EnCase找出證據。第五節為結論。

2. 相關背景

本節將介紹 QR code 以及本次實驗所會用到的鑑識工具：EnCase。

2.1 QR code 介紹

QR code 是 1994 年日本 Denso-Wave 公司所發明的一種二維條碼[2]。QR 是 Quick Response 的縮寫，命名的由來是希望 QR code 能夠快速的被解碼。早先是汽車製造業用來追蹤零件的，之後逐漸被廣泛的使用在各行各業

的存貨管理。QR code 的結構如圖 1 所示。

圖 1、QR code 結構圖

其中每一個黑點或白點為一組成單元稱做 module，整個 code 分成 7 個部分，以下將為大家做介紹：

1.位置偵測圖案(Position Detection Patterns)

每一 QR code 會有 3 個位置偵測圖案，是方便 QR code 掃描器做定位用的，也由於此 3 個圖案，使得在掃瞄 QR code 的時候使用者不需要調整鏡頭方向，掃描器即可正確判讀。

2.版本資訊(Version Information)

這部分說明該 QR code 的版本（總共有 40 種版本）。

3.調準圖(Alignment Pattern)

當版本(Version)變大時，幫助定位調校。

4.分配圖(Timimg Pattern)

由黑白相間的單元(module)所組成，幫助掃描器判斷黑白單元(module)的比率。

5.編排資訊(Format Information)

說明此 QR code 的容錯率、儲存資料的類型以及資料遮罩。

6.資料與錯誤修正(Data and Error Correction Part)

儲存資料以及幫助修正錯誤的地方。

7.空白區域(Quiet Zone)

而整個 QR code 外圍的空白部分是用來幫助位置偵測圖案更快速的被辨識出來。

可以編碼成 QR code 的資料有數字、字母、二進位數以及漢字。隨著不同的版本，可以儲存的資料量也不同。總共有 40 個版本，版本越大可以儲存的資料量越多。而其所能儲存的最大資料容量，如表 1 所示。

.

表 1、QR code 最大資料容量

QR code(Version 40，character)	
數字	7089
字母	4296
二進位數	2953bytes
日本漢字/片假名	1817(Shift JIS)
中國漢字	984（UTF-8）
	1800（BIG-5）

其中上述所提及的錯誤修正有四種等級供製作者自行選擇，等級越高可以修正的程度越大，所需佔的總體容量也越大，如表 2 所示，其中 L 可修正的錯誤容量最低，H 可修正的錯誤容量最高。

表 2、QR code 修正容量

等級	可修正錯誤之容量
L	7%
M	15%
Q	25%
H	30%

2.1.1 QR code 應用

QR code 的應用到現在已不再僅限於存貨管理，以下是目前 QR code 更廣泛的應用：

- **自動化文字傳輸**

不單單是簡訊、電子郵件，只要是 QR code 能夠編譯的文字都可以藉由 QR code 產生器製作出來。一旦經過掃瞄之後即可將訊息送出，如傳送訊息、交換名片等。

- **數位內容下載**

大多是電信公司及數位影音公司所提供，只要用戶付費之後掃瞄對方所提供之 QR

code（大多會在帳單上面）即可連結至下載網頁開始下載所購買的數位內容。

- **網址快速連結**

可以將網址編譯成 QR code，使用者只要掃瞄該 QR code 即可快速連結至網頁讓使用者瀏覽。

- **身份鑑別與商業交易**

這是現在許多公司在推行的機制，如高鐵車票，消費者在 ibon 付費購買車票之後在票據上會有著一個 QR code 當作購票證明以供掃瞄進出車站；而目前還有著做商品驗證的功能，消費者可以透過該 QR code 連結至驗證中心作確認。

除了以上四種面向的應用之外，如現在著名的手機社交應用程式「Line」也有使用 QR code 來幫助使用者進行加入好友、或是身份的認證等。所以爾後勢必會有更多 QR code 之應用在科技與生活上。

2.1.2 自行製作 QR code

QR code 的製作非常容易，任何人都可以利用網路所提供的 QR code 產生器，產生屬於自己設定的 QR code。在網路上更有著許多提供線上製作 QR code 的網站，如圖 2 所示。

圖 2、QR code 製作(以 http://www.calm9.com/labs/qrcode 網站製作 QR Code)

如圖 2 所示，可設定要儲存連結、書籤、文字、郵件、電話、簡訊或是地理座標，可選擇要開啟的類型，包括網頁、FTP 或 Android Market，並可在下方選擇尺寸、版本、容錯率及圖檔格式，產出的 QR code 即為當初所設定的內容。另外近來也有廠商提供客製化及彩色 QR code 的製作，讓 QR code 變得越來越多元。QR code 的產生很便利也很容易，但相反的也可能被有心人士拿來當作犯罪的媒介。

2.2 EnCase

Guidance software 公司所生產之 EnCase[5]軟體在電腦鑑識領域享富盛名，此軟體的評價深受全世界肯定。此軟體為目前台灣地區警政署、法務部調查局及國安局等相關單位最常使用之電腦鑑識軟體，同時也是國際大多數國家的法庭上最具公信力之電腦鑑識軟體之一。其主要的特色可歸納如下：(1)以具有法律效益的鑑識方法取得鑑識資料，並為世界各地之法院採證。(2)在不變動證據的前提下進行物證分析。(3)以鑑識的角度取得資料，不管被隱藏、刪除或是覆蓋之檔案。(4)檢閱功能可幫助非鑑識操作人員很容易的檢視證物。(5)可快速簡單的產出完整鑑識報告。

EnCase 採用 Windows 圖形作業平台，如圖 3 所示，此軟體提供如預覽、分析、記錄報表、映像副本、還原、驗證等功能，並可支援鑑定於 Windows FAT 及 NTFS 檔案系統格式、UNIX、LINUX 與 Macintosh 之多種作業系統檔案，為一整合多項功能之鑑識軟體，以下將對於其功能分述之。

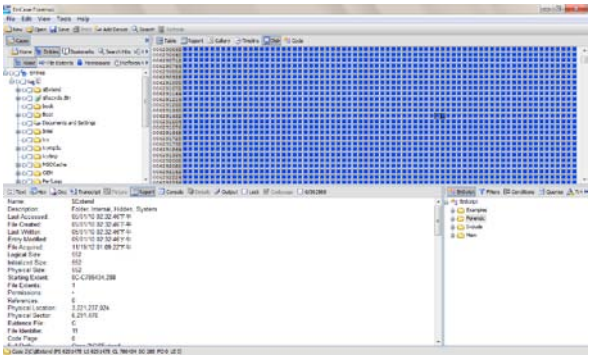


圖 3、Encase 鑑識軟體使用介面

(一)預覽(preview)：能對於所要進行鑑識之儲存媒體做一系統與設定的簡介，利用樹狀結構圖形呈現檔案層次關係。

(二)檢視(survey)：將所有檔案依序排列，並設定檔案特性之欄位，利用選取方式選定特殊排列順序方式，如檔案名稱、大小、格式、最後存取時間、MD5 驗證數值等設定欄位配合偵查需求進行排序。

(三)映像複本：Encase 在進行磁碟、檔案鑑定時，會先建立一個證據映像複本來作為鑑定目標，並同時利用 MD5Hash 函式產生驗證碼，當證據複本內容有相異將無法產生相同之驗證碼，以保全證據之完整性與證據力之呈現。

(四)關鍵字搜尋(text and GREP search)：Encase 可利用特定關鍵字對鑑識磁區進行檔案搜尋，包含隱藏檔案及殘餘空間之刪除檔案，以增進搜尋檔案或相關資訊之效率。

(五)修復被刪除檔案(recover deleted files)：Encase 可對於磁碟中剩餘空間進行刪除檔案之搜尋，並可將已刪除之檔案修復以茲進行偵查，然若刪除檔案磁區已遭覆寫，則只可修復部分檔案內容資訊以供調查。

(六)影像檔案瀏覽(gallery view)：Encase 對於搜尋所得之影像檔案可以圖形呈現，對於影像檔案證據鑑識之動作能有所助益。

(七) 磁碟清除功能(wipe dive)：現行電腦犯罪儲存媒體少則數十 GB 計算，對於在進行案例副本的資源上往往造成經濟支出的負擔，而證據副本磁碟的再利用又容易造成內容資訊可信度的懷疑，因此可利用 Encase 的磁碟清除功能將已偵查終結之證據副本儲存媒體進行清除，以提供下次證據副本之儲存媒體，節省偵查機關儲存媒體購買支出與實體占用空間的節約。

3. Our Scheme-QR forensics

使用者通常會不加思索的用手機去掃瞄 QR code，並不會質疑其真確性，接著開始使用該 QR code 所提供的服務。讓此部分成為非法者詐騙個資、財產的溫床，主要的攻擊手法可分為兩部分[1][7]，一為直接對掃瞄 code 的裝置造成損害，二為對使用者造成威脅。以下將針對這兩部分做說明，並在最後說明鑑識人員如何搜索非法者遺留之證據。

3.1對掃瞄的裝置造成損害

這方面的攻擊是對於數位裝置系統上的漏洞以及在 QR code reader 處理步驟的程序做攻擊。並有以下幾類：

- **阻斷式服務攻擊**

對系統提出大量的服務請求，但卻不具任何意義。這樣的舉動會讓系統不斷處理該服務請求，導致延誤或是終止其他程序。

- **SQL injection**

在輸入的字串中加入SQL語法，讓設計不良的程式忽略了檢查，使得資料庫系統在編譯的時候就會將其當作正常的SQL語法而執行。

- **惡意程式**

攻擊者會將惡意程式隱藏入網頁當中。只要使用者開啟該網頁，即會自動執行惡意程式。其主要的危害有：

- 破壞系統
- 佔據記憶體
- 耗費資源
- 侵害使用者個資

3.2利用QR code攻擊使用者

不同於上述的手法，攻擊手機系統的漏洞讓手機受到危害。這此，攻擊者利用人必須藉助QR code reader才能取得相對應的服務之特點，使其作為媒介設法從中對人的個人資料或財產給予迫害。

- **網路釣魚**

非法者偽造知名的公司或網站，讓使用者在沒發現其真偽的情況下，就填入自己的個

人資料、信用卡卡號、帳號、密碼等。非法者會將偽造的網站設計成假可亂真的模樣，同樣的 LOGO 文宣，同樣的頁面布置，使得使用者若不仔細檢查網址根本分辨不出是假冒的網站。或是只置換知名網頁所提供的 QR code，讓使用者在未察覺的情況下就連結到非法者所設計的釣魚網頁。甚至非法者會利用 JavaScript 的技術置換網址，讓偽造的網址與官方的網址一模一樣，識破的機率更小。非法者就可以輕易的取得使用者不加思索輸入的帳號、密碼或是信用卡安全碼。

網路釣魚的主要目的就是設法取得使用者的個人資料與財產相關的資訊，主要的危害有：

- 身份盜用
- 財產損失
- 網路詐騙
- 讓社交工程式更易實行

  網路釣魚也能利用QR code來實行。攻擊者可將偽造的網站網址轉換成QR code發佈，而警覺性不夠的受害者掃瞄之後，輸入的相關資料全部交到了攻擊。

- **詐騙**

非法者試圖以奪人耳目的廣告文宣吸引受害者。諸如參加活動、販賣商品、購買商品給予極高的優惠。但事實上整件事情都是捏造的，利用人貪小便宜的特性下手所實行的手法。使用者會根據所指示的步驟輸入資料、登入、付款繳費，但卻完全得不到任何回應。但驚覺時已經完成輸入資料的動作，造成資料與財產的損失。

3.3 非法者遺留之證據

非法者遺留之證據主要可分為兩部分，第一部分為線上製作 QR code 所遺留之證據，第二部分為以 QR code 作媒介所獲取的不法資料。以下將針對這兩部分進行說明。

- 製作 QR code 所遺留之證據

QR code 的製作目前都以線上居多，不論是在電腦端或手機端都必須連上網路進行操作，因此在產生 QR code 的過程中一定會留下一些蛛絲馬跡。首先利用 QR code 關鍵字搜尋網頁瀏覽紀錄[10]，如圖 4 所示，確定非法者的確有利用線上產生器製作 QR code。接著利用搜尋檔案類型格式 png、jpg 的方式，找出可疑的 QR code，如圖 5 所示。掃描這些 QR code 以確定是否與從事非法行為的 QR code 有相關，若有則可確定非法者的確是利用產生器產生出 QR code。

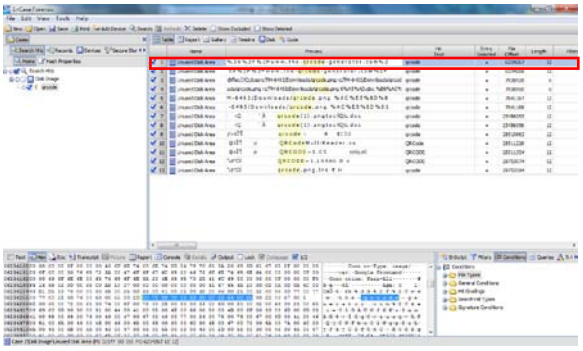


圖 4、瀏覽 QR code 網頁紀錄

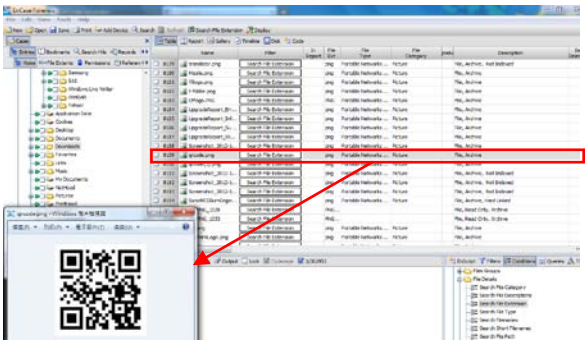


圖 5、QR code 儲存紀錄

- 以 QR code 作媒介所獲取的不法資料

非法者獲取不法資料後，可能透過網頁瀏覽這些資料，或是轉存成檔案存在電腦裡，因此本研究即利用這些特性，進行記憶體傾映或是針對被刪除的檔案進行復原[6]，並利用關鍵字搜尋使用者填入的相關資料，找出非法者的犯罪證據。

Example

A 君是位網路遊戲愛好者，在一次因緣際會下得知官網目前正在進行贈送虛擬寶物的

活動，只要掃描網頁中出現的 QR code，並填問卷就可立即獲得虛擬寶物，如圖 6 所示。於是 A 君不加思索的拿出手機掃描官網上的 QR code，並一步步填入所需資料，如圖 7 與圖 8 所示。但 A 君並不知道官網的 QR code 已被非法者置換，其所填入的資料都會被非法者蒐集起來。

圖 6、A 君掃描 QR code 之網頁

掃描成功後，透過手機進入該網頁，填寫問卷。如圖 7 所示。

圖 7、利用手機填寫問卷

而非法者就在最後設下陷阱，讓 A 君留下在遊戲中的帳號、密碼及基本資料。如圖 8 所示。

圖 8、A 君利用手機填寫問卷內之基本資料

非法者利用網路來檢視所得的資料，只要玩家一送出問卷，所有的資料都會一筆一筆記錄下來，如圖 9 所示。非法者利用所獲得的帳號密碼登入遊戲，竊取帳號內的寶物。

圖 9、非法者從問卷中蒐集的資料

由於會盜用寶物者多為同遊戲內的玩家，故鑑識人員與遊戲廠商聯繫，過濾出近期虛擬寶物大量增加的玩家，一一清查後查到該非法者 IP 所在地，並前往該名非法者家中搜索。

當非法者察覺自己已被鑑識人員鎖定時，立即關閉網路瀏覽器及所有相關的證據，為了找出非法者蒐集資料的證據，鑑識人員利用免費軟體「MANDIANT Memoryze」[4]（可以在網路上直接下載：http://www.mandiant.com/products/free_software)中的「MemoryDD.bat」程式，對非法者之電

腦進行Memory Dump(記憶體傾印)。如圖10所示。將揮發性記憶體中的資料在不干擾原電腦的前提下擷取出來，並輸出成一完整大小之映像檔(image file)，如此一來，才可進一步載入Encase等鑑識軟體中進行分析。

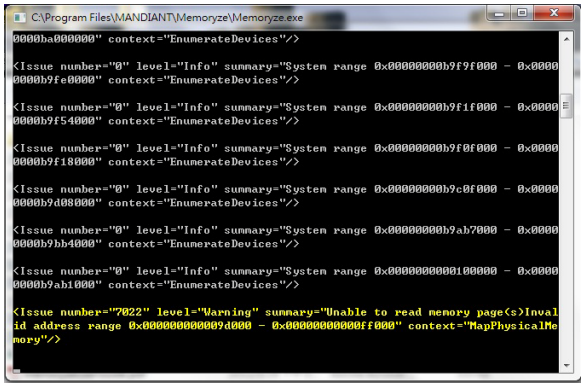


圖 10、對非法者電腦進行記憶體傾映

將產生出的映像檔，載入到鑑識工具「Encase」中進行分析，利用 Encase 的關鍵字搜尋功能[9]，在「Keywords」中建立 A 君被盜用的帳號及密碼等當作關鍵字，如「posthotdog」、「touihf」、「fopto」。如圖 11 所示。並將其一一打勾，開始著手進行搜尋。

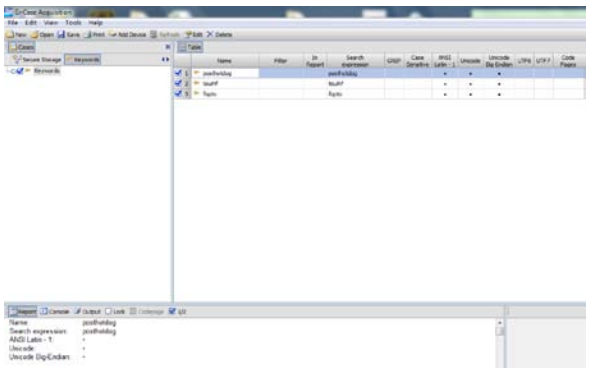


圖 11、Encase 設置關鍵字之介面

利用「Search」功能，勾選好下列的選項後，便按下「Start」開始搜尋，而左下方的「Compute hash value」則可在搜尋時同時計算該映像檔之 Hash 輸出值，確保該映像檔之完整性。如圖 12 所示。

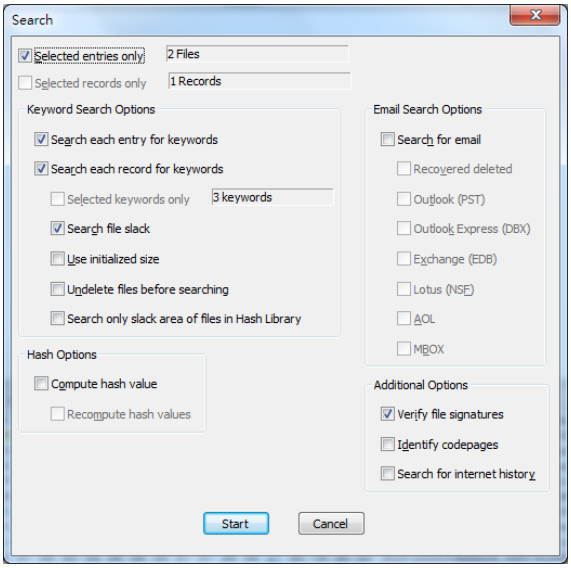


圖 12、 Encase 設置搜尋之畫面

視窗右下方會顯示搜尋的進度及剩餘的時間，待搜尋完成後，便會出現一「Searching」的視窗告知最後搜尋的結果。如圖 13 所示。而「Search Hits」便是在這次搜尋中，符合條件的關鍵字總數。

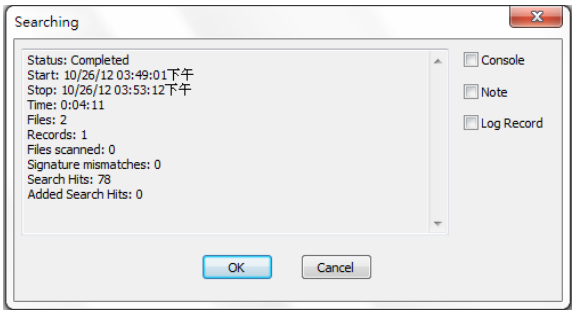


圖 13、 Encase 搜尋完成之畫面

接著選擇「Search Hits」功能，並將剛剛選擇的搜尋條件一一打勾，接著在左下角選擇「HEX」即十六進位之編碼方式加以檢視，符合之關鍵字將會用黃底加以標示。而我們便可以發現，A 君當初所填入的資料。如圖 14 所示。包括「posthotdog」、「touihf」、「fopto」相互在鄰近的位置出現。觀察這些帳號密碼關鍵字附近的編碼，皆有「</td></tbody>」的 html 編碼，因此再以此編碼作為關鍵字搜尋是否還有其他使用者帳號被盜用。

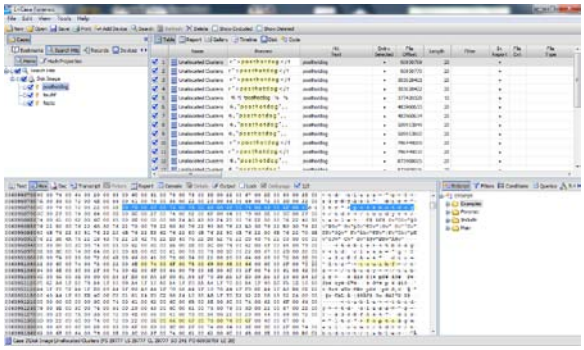


圖 14、 Encase 所搜尋到之關鍵字

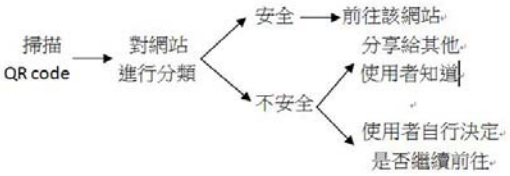
非法者利用置換 QR code 的方式，讓使用者在不注意的情況下進入錯誤的問卷網頁並填入資料。為了找出非法者的犯罪證據，鑑識人員透過記憶體傾印輸出一映像檔，載入 Encase 鑑識工具並進行關鍵字搜尋，找出多筆使用者填入的相關資料。因此鑑識人員可以確定非法者的確有利用家中電腦進行蒐集非法資料的證據。由實驗結果，使用者輸入的資料都出現在 Encase 分析的結果裡，這對鑑識人員來說，是很重要的證據來源。

4.討論與分析

經由 Example 說明之後，可以知道非法者要利用 QR code 來從事非法行為是很容易的。雖然非法者的相關證據可以在事後被鑑識人員找到，但是對使用者來說，能避免一切被攻擊的行為一定是最好的。本文提出兩個方法，如表 3 所示，讓使用者在面對惡意的 QR code 時免於被攻擊，第一個方法介紹一款能在 Android 及 ios 系統上安裝用來過濾掃描 QR code 進入網站的 app：Norton Snap QR code Reader。這款 app 掃描 QR code 後能對網站做安全等級的分類，如果該 QR code 屬於不安全，讓使用者自行決定是否要繼續前往該網站，或是將惡意的 QR code 分享出去給其他人知道，避免其他使用者上當，如圖 15 所示。但只單靠 app 來過濾網站並不能保證絕對的安全，當然還要搭配使用者本身對 QR code 來源的警覺性。第二個方法即是使用者需具備基本的資訊安全觀念。因為一般的 QR code 大多是吸引使用者造訪活動網站或參加活動，留下的資料多為姓名或 E-mail 等聯絡方式，但非法者即會利用使用者疏於注意的習慣，建立一些陷阱讓使用者將較機密的個人資料填入，並在日後將這些資料拿來從事其他非法行為。

圖 15、Norton Snap QR code Reader 掃描後畫面

表 3、面對惡意 QR code 的方法

方法一	利用 Norton Snap QR code Reader 掃描 
方法二	使用者具備資訊安全觀念，對機密資料的警覺性。

5. 結論

QR code 目前在生活中已隨處可見，無論是報章雜誌、廣告看板都可以看到 QR code 的身影，但使用者很少去注意 QR code 的安全性，常常會因為受到廣告字眼及背後所帶來的

優惠給吸引，而輕易掉入非法企圖者所設下的陷阱。在本篇研究中所提出的犯罪手法確實能夠對使用者造成危害，取得使用者的私密個人資料。而鑑識人員在事後確實能利用鑑識工具 EnCase 從非法者使用的電腦中取得證明其非法行為的證據。而最後提供使用者在面對惡意 QR code 的因應方法，可以讓使用者免於被攻擊。根據本篇研究，可以了解到利用 QR code 從事非法行為的手法其實要求的技術並不高，但是對使用者造成的危害與影響卻是相當大的。所以使用者在面對眼前的 QR code 應提高警覺性，因為它有可能是非法者用來詐取個人資料的利器。

參考文獻

[1] Alvin, S., “Porting of an iPhone Application to Android,” Degree Project, 2011.

[2] Chang, Y. H., Chu, C. H., and Chen, M. S., “A General Scheme for Extracting QR Code from a non-uniform background in Camera Phones and Applications,” Multimedia, 2007. ISM 2007. Ninth IEEE International Symposium on, pp.123-130, 2007.

[3] Chen, C.N., Lin, J.S., and WANG, S.J., “iPhone Forensics in QR Code Security,” presented in Proceedings of 2012 Conference in R.O.C. Military Academy, Taiwan, May, 2012.

[4] Hejazi, S., Talhi, M. C., and Debbabi M., “Extraction of forensically sensitive information from windows physical memory,” Digital Investigation, Vol. 2009, No. 6., S121-S131.

[5] Arthur, K.K., and Venter, H.S., “An Investigation into computer forensic tools,” Information and Computer Security Architectures (ICSA) Research Group.

[6] Pal, A., and Memon, N., “The evolution of file carving,” Signal Processing Magazine, IEEE, pp.59-71,2009.

[7] Peter, K., Manuel, L., Martin, M., Lindsay, M., Sebastian, S., Mayank, S., and Edgar, W., “QR Code Security,” MoMM '10 Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia , pp.430-435, 2010.

[8] Steven, F., “Disguising the dangers: hiding attacks behind modern masks,” Computer Fraud & Security, Vol. 2012, No. 6. (June 2012), pp. 9-13.

[9] Tiwari, L. K., Samaddar, S. G., Singh, A. K., and Dwivedi, C.K., “Evidentiary Usage of E-mail Forensics: Real Life Design of a Case ,” presented in IITM 2010 - Intelligent Interactive Technologies and Multimedia.

[10] Zeng, H. J., He, Q.C., Chen, Z., Ma, W.Y., and Ma, J., “Learning to Cluster Web Search Results,” presented in Proceedings of the 27th annual international ACM SIGIR conference on Research and development in information retrieval, pp.210-217, 2004.