運用 Android 仿真器做為數位犯罪工具之研究

鄧思源[1*]、林育梨[2]
[1]法務部調查局臺北市調查處、[2]法務部調查局資通安全處
[1] mjib.teng@gmail.com、[2] m42062@mjib.gov.tw

摘要

智慧型行動裝置已廣泛應用於各個層面，也成為大眾日常生活中不可或缺的數位裝置之一，而運行在這些行動裝置上的行動作業系統(mobile operating system)目前以 Android 市占率最高。Android 行動作業系統除了可安裝於實體行動裝置外，市面上亦可發現為數不少的 Android 仿真器(emulator)存在，使用者可將各種應用程式(APP)安裝於此類仿真器中，即可便捷使用，有心犯罪者如以 Android 仿真器安裝無線檔案傳送(Wifi file transfer)之應用程式竊取機密檔案或使用具有資訊隱藏術(Steganography)之應用程式以傳遞犯罪訊息規避犯罪調查時，如何分析與解譯在仿真器中所存在的犯罪訊息紀錄，將成為數位犯罪調查作業之必要鑑識作為。數位鑑識人員於數位證據鑑識分析作業中，如何確認犯罪者安裝在實體機器上 Android 仿真器及解譯應用程式之內部資訊，實為數位鑑識作業之一大挑戰。本篇研究旨在探討如何應用數位鑑識實務作業中之數位鑑識工具及鑑識程序，對市面上數種常見之 Android 仿真器安裝無線檔案傳送及資訊隱藏應用程式進行鑑識分析，整理及歸納出可用於數位鑑識作業之鑑識項目與應用程式特徵值，以協助數位鑑識人員於實務上可參用之鑑識方法。

關鍵詞：虛擬行動裝置、Android 仿真器鑑識、反鑑識、無線檔案傳輸程式鑑識、資訊隱藏程式鑑識

The Research of Using Android Emulator as Criminal Tools

SZU-YUAN TENG[1*], YU-LI LIN[2]
[1 2] Investigation Bureau, Ministry of Justice
[1] mjib.teng@gmail.com、[2] m42062@mjib.gov.tw

Abstract

Mobile devices have been become a very popular and indispensable tool in daily life and work. Android is currently the number one mobile phone platform with highest market share. Android OS can be installed in the mobile devices and Android emulator. Users can download

any kind of application to install on Android emulator. Several criminals use WiFi file transfer program on Android emulator or Steganographic techniques as tools to deliver criminal data. Traces and evidence left by these programs can be held on mobile phones and retrieving those potential evidences with right forensic technique is strongly required. In this paper, we focus on conducting forensic data analysis of 2 widely used applications on Android emulator: WiFi file transfer program and Steganographic technique.

Keywords: Virtual mobile device, Android emulator, Anti-forensics, WiFi file transfer program, Steganographic technique

壹、前言

目前行動裝置上常見的主流行動作業系統(mobile operating system)可概分為 Android、iOS、Windows 10 Mobile、BlackBerry 10、webOS 及 Firefox OS 等，而市占率最高的當屬 Android，此種行動作業系統除了可安裝於實體行動裝置外，市面上亦可發現為數不少的 Android 仿真器(emulator)存在，使用者可將各種應用程式(APP)安裝於仿真器中。

仿真器主要功能為用於模擬 Android 行動裝置(手機/平板)的各種軟硬體環境，主要目的為方便程式設計師開發、測試 Android 應用程式。目前市面上常見之仿真器主要在於提供使用者能從 Google Play 商店下載及使用各種遊戲與應用程式。Android 仿真器包含完整的 Android 架構，例如 Linux Kernel、Native Library、Dalvik VM、Android 應用程式架構等，除撥出電話功能外，仿真器可以模擬 1 台 Android 行動裝置的所有軟硬體功能，例如：存取網路、播放影音、存取記憶卡等。

近年來不管是個人資料或國家機密資料大量外洩之資安事件不斷發生，究其外洩管道及原因多不勝數，而行動裝置其功能性與便利性之控管措施需特別處理，因此常成為資安防護作業所忽視之部分。有鑑於此，目前實體行動裝置控管(MDM)可分為功能管理與內容管理，其常見之控管政策又可分為安全性、隱私權、鎖定、同步、備份還原、文件、APP 及檔案等 8 種。上述控管政策能否應用於安裝在實體機器上的虛擬行動裝置或仿真器殆有疑義。

當有心犯罪之不法份子利用此類 Android 仿真器安裝如無線檔案傳送之應用程式竊取機密檔案或使用具有資訊隱藏術之應用程式以傳遞犯罪訊息以規避犯罪調查等目的時，此種利用新型態虛擬行動裝置為犯罪工具之案件調查與該如何進行鑑識，實值得吾等從事數位鑑識實務工作人員深入探討與研究。

貳、文獻探討

2.1 常見之 Android 仿真器種類說明

2.1.1 用於軟體開發之仿真器

(1)Android Studio

Android Studio 為 Google 公司免費提供給 Android 平台開發程式人員的一種整合式開發環境軟體，該軟體在工具選項下提供 Android Virtual Device(AVD) Manager 功能，可供使將所開發之程式於內建之手機、平板、穿戴及電視等仿真器中進行測試[1]。

(2)Visual Studio Emulator for Android

Visual Studio Emulator for Android，是微軟提供予 Android 平台開發程式人員的一種整合式開發環境軟體，必須搭載 Virsual Studio 軟體使用，提供與 x86、Hyper-V 相容能力，同時支援不同 Android 版本、螢幕尺寸及硬體特性，可供使用者在客製化的仿真器中測試程式[2]。

(3)Manymo Emulator

Manymo Emulator 是 Manymo 公司所開發的一個 Android 線上仿真器，可在瀏覽器快速啟動，並支持 73 種不同的螢幕尺寸與作業系統版本，給予應用程式開發人員網站嵌入式 App 的開發、合作、自動化測試與品質管制等作業[3]。

2.1.2 可安裝及使用 APP 之仿真器

(1)AMIDuOS

AMIDuOS 為可安裝在微軟視窗作業系統下的一種 Android 仿真器，目前提供 Lollipop 及 Jelly Bean 等二種版本，使用者均需付費使用，該仿真器強調幾乎所有 Android 應用程式都可在該公司的仿真器中執行，程式相容性相當高，同時執行仿真器的效能也是最佳速度最快，另外仿真器亦提供支援平板與檔案儲存與分享功能[4]。

(2)Andy

Andy 是一種比較新型的 Android 仿真器，可在微軟視窗作業系統及蘋果 OSX 作業系統下運行使用，功能強調提供桌面與行動裝置的無縫同步作業，在任何桌面瀏覽器下載的 App 都可直接安裝在仿真器中，隨時確保使用的 Android 作業系統為最新版本[5]。

(3)BlueStacks App Player

BlueStacks App Player 為最早出現在市面上的 Android 仿真器其中之一，目前亦是最有名及應用最廣泛的仿真器，可在微軟視窗作業系統及蘋果 OS X 作業系統下運行使用，依照該公司的說明，在 Google Play 商店中 96%的 App 以及 86%的 Android 遊戲都可安裝在 BlueStacks App Player 仿真器中[6]。

(4)Droid4x

Droid4x 又稱海馬玩仿真器，為市面上由中國大陸所開發的較新型的仿真器，號稱迄今為止在性能、兼容性與操控體驗方面最好的 Android 仿真器，提供 ARM 程序在 X86 架構下運行，並可兼容市面現有 99%以上的應用與遊戲程式，亦提供多重開機管理器，使用者可同時執行多個仿真器，但該仿真器目前只在微軟視窗作業系統下安裝執行[7]。

(5)Genymotion

Genymotion Android Emulator 係由法國 GenyMobile 公司針對 Android 系統平台開發人員、測試人員、銷售人員甚至是遊戲用戶所開發的一種仿真器，目前支援微軟視窗、蘋果 OSX 和 Linux 等作業系統，具有容易安裝和使用的特性，Genymotion 號稱為目前啟動速度最快的 Android 仿真器。使用者必須先至 GenyMobile 公司註冊成為會員後，才可安裝免付費的 Genymotion Android Emulator 版本，目前提供 29 種不同版本的手機及平板仿真器[8]。

(6)KOPLAYER

KOPLAYER 係由中國大陸福州靠譜網路有限公司所開發之新型仿真器，支援 Intel 及 AMD CPU，支援所有 Google Play 商店中的應用與遊戲程式的使用，但目前僅提供微軟視窗作業系統版本[9]。

(7)Memu

Memu 係由中國大陸上海邁微軟體科技有限公司所開發之新型仿真器，強調比 BlueStacks App Player 及 Droid4X 更為穩定，比最新的 Android 旗艦手機效能更佳，基準可達 2 倍，支援不同的硬體組態，可與大部分的應用程式相容，與 Droid4X 一樣，提供多重開機管理器功能，使用者可同時執行多個仿真器，目前只提供微軟視窗作業系統版本[10]。

(8)Nox App Player

Nox App Player 由中國大陸北京多點在線科技有限公司所開發的仿真器，強調高效能與相容極致性，目前僅能安裝在微軟視窗作業系統，要使用 Nox App Player 仿真器之前，必須先安裝 Oracle VirtualBox 虛擬機器軟體[11]。

(9)Windroy

Windroy(又名文卓爺)由中國大陸北京文安卓立科技有限公司所開發的仿真器，目的是將 Android 系統運行於個人電腦機上，並帶來大螢幕特有的使用體驗。

在技術路線上，Windroye 採用了虛擬機技術，更注重應用兼容性，滿足用戶的功能需求和一流的用戶體驗[12]。

(10)Xamarin Android Player

Xamarin Android Player 由 Xamarin 公司所開發的仿真器，可安裝在微軟視窗及蘋果 OSX 作業系統下，與 Genymotion Android Emulator 一樣，主要是聚焦在應用程式開發人員部分，希望提供一種簡單使用者的經驗，要使用 Xamarin Android Player 仿真器之前，必須先安裝 Oracle VirtualBox 虛擬機器軟體[13]。

(11)YouWave Android

YouWave Android 由美國加州 Youwave 公司所開發的商業用仿真器，支援 Android 5.1 Lollipop 及 4.0 ICS 版本，目前只能安裝在微軟視窗作業系統下，要使用此軟體前，必須先安裝 Oracle VirtualBox 虛擬機器軟體[14]。

(12)Andro VM

Andro VM 是 Genymotion Android Emulator 仿真器母計畫的研究成品，只能安裝在 Linux 作業系統下，不像 Genymotion 是透過雲端佈署安裝於使用者的個人電腦中。使用者可以使用 Andro VM 離線安裝所需要的仿真器[15]。

2.2 Android 仿真器與無線檔案傳送及資訊隱藏術應用程式之文獻探討

Android 仿真器目前主要應用之範圍，包括應用程式之開發、遊戲娛樂及各類應用程式之使用。有關 Android 仿真器概念性的證據蒐集與分析方法之相關研究，目前學術界並未相關文獻加以探討。大部分有提及 Android 仿真器的相關研究，主要是將 Android 仿真器做為研究使用工具，而非研究對象。目前有許多無線檔案傳送及資訊隱藏術應用程式可在 Android 平台下執行，有關此類應用程式在仿真器中的鑑識研究，較無相關文獻探討，本研究將藉由 Android 仿真器鑑識，即在仿真器中安裝及使用無線檔案傳送與資訊隱藏術之應用程式等相關文獻之探討，歸納出目前之相關研究成果與可能遭遇之挑戰。

關於 Android 仿真器之研究方面，學者 Al-Saleh 及 Forihat [16] 利用 Eclipse 3.7.2 Indigo tool 的仿真器進行 Skype 即時通訊軟體的研究，研究結果顯示在 Android 仿真器的變動性 (RAM)及非變動性(NAND flash)記憶體資料中，可以發現撥打電話及對話等相關紀錄是以明文呈現，但對於仿真器內的檔案結構並未有所說明。

學者 Sara、Vance 及 Fenger [17]同樣利用 Eclipse IDE AVD 仿真器進行 Dropbox 應用程式檔案殘留物的鑑識分析研究，同樣只是利用仿真器做為研究工具，並未對於仿真器檔案結構有所探討。

在 Android 行動裝置無線檔案傳送應用程式之研究，學者 Al-Hadadi 及 Al-Shidhani[18]等人利用 Oxygen and UFED 手機鑑識工具針對特定手機進行鑑識分析，

發現可找尋到使用 WiFi 連線存取點的紀錄，但對於無線傳送檔案內容並沒有做相關研究。

學者 Andriotis、Oikonomou 及 Tryfonas[19]等人針對 Android 手機之無線與藍芽通訊網路以 4 種假定之情境進行鑑識分析，並依照 ACPO 準則歸納出可供鑑識參考之資料檔案與存放路徑。但是對於無線檔案傳送應用程式之研究並未進行相關探討。

學者 Busstra、Le-Khac 及 Kechadi[20]等人提出在 Android 手機無法使用 USB 連接線擷取資料時，可以該利用具有 WiFi 傳送功能的軟體來進行資料擷取作業，在此以 SSHDroid 應用程式作為無線傳輸資料擷取工具，但同樣此研究對於利用無線檔案傳送應用程式進行資料傳送與接收作業時，會存在哪些值得參考的鑑識資訊，亦無相關涉獵。

在 Android 行動裝置資訊隱藏應用程式之研究，學者 Mazurczyk 及 Caviglione [21]等人研究整理於 2005 年至 2014 年期間所發展出及運行在智慧型手機上的資訊隱藏技術，依不同的方法及裝置進行分群說明隱藏資訊，可分為 3 個不同隱密通道，亦即位置、物件及網路，在論文最後以未來發展方向來說明此期間廣泛使用可用以嵌入秘密資料到載體的應用程式。Mazurczyk 等人整理的資訊隱藏技術資料堪稱豐富，但是對於如何應用數位鑑識技術，找到這些資訊隱藏應用程式可能存在於智慧型手機的方法與程序，並未說明。

學者 Chowdary 及 Liu [22]等人針對 Android 手機利用 SMS 應用程式可以識別文字簡訊中的 ASCII 及 UTF-8 編碼字元之特性，發展出可以嵌入秘密資訊到載體訊息的資訊隱藏方法。本研究同樣地為著重於方法之開發，對於如何發現具鑑識價值的資訊隱藏資料未多加探討。

學者 Ghare、Bansode、Bombale 及 Chandargi [23]等人提出可應用於 Android 手機上的 LSB 資訊隱藏技術，也就是將要傳遞之機密影像與載體影像透過 LSB 演算法進行加密成為藏密影像(Stego Image)，同樣地，經過反向的程序可以將機密影像與載體影像分離。本研究還是著重於資訊隱藏技術演算法之開發，對於如何發現手機中有關資訊隱藏資料亦未有所探討。

由上述 Android 仿真器、行動裝置無線檔案傳送應用程式及資訊隱藏應用程式之文獻探討可知，目前僅有些許研究內容可供參考，因此本研究將針對安裝於 Android 仿真器中之行動裝置無線檔案傳送應用程式及資訊隱藏應用程式等進行識別、蒐集、檢驗及分析，歸納具參考價值之鑑識資訊，並提出在檢驗上述鑑識項目之相關建議。

參、研究架構

依上述文獻研究內容可知，Android 仿真器通常安裝於本機端使用，因此本研究將識別、蒐集與擷取、檢驗與分析 Android 仿真器於安裝與運行在本機端之相關數位證據

跡證，以及識別、蒐集與擷取、檢驗與分析在 Android 仿真器中安裝及使用無線檔案傳送及資訊隱藏應用等應用程式之數位證據跡證，提出面對此類數位證據之鑑識實務相關建議。

3.1 研究方法

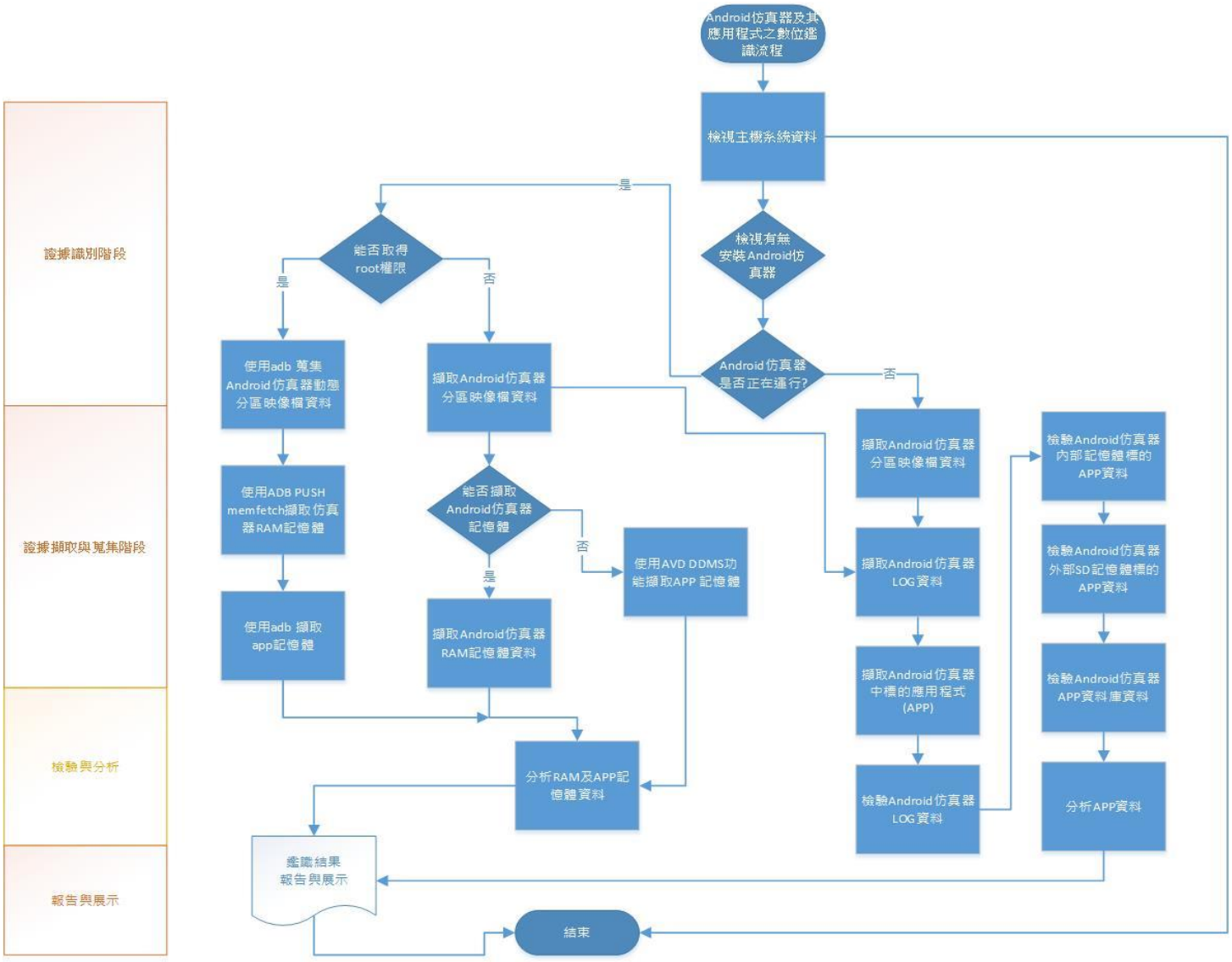
本研究將以數位鑑識實務上的程序與作法，針對 Android 仿真器軟體安裝於本機端微軟 Windows 7 作業系統時進行相關實驗與觀察，以找出可能會留存鑑識資料之檔案名稱與路徑。在安裝及測試 Android 仿真器軟體時，使用的數位鑑識工具建議除以 X-Ways Forensics 整合性鑑識軟體進行分析外，對於本機端之系統登錄檔、系統開啟之連接埠、資料夾及檔案之變動情形亦應加以記錄及分析，有關系統登錄檔之變化，可採用 Regshot 進行相關記錄與比較，對於系統開啟之連接埠採用 Currports 來觀察，對於檔案及資料夾之變化則採用 FolderChangesView 及 Disk Pulse 等程式來進行觀察及記錄，亦可使用如 SysTracer Pro 等商業軟體同時對登錄檔、檔案及應用程式進行快照、監控與比較結果。仿真器實驗步驟如下：

- 取得所欲鑑識之新型態 Android 仿真器軟體，並記錄版本。
- 於本機端中先啟動 Regshot 登錄檔快照程式，並執行第一次登錄檔快照，執行完後再啟動 Currports、FolderChangesView 及 Disk Pulse 等程式，並開啟檔案監控功能。
- 在本機端中安裝 Android 仿真器軟體之執行檔，並在 FolderChangesView 及 Disk Pulse 程式中觀察檔案變化情形。
- 仿真器軟體安裝程序結束後，停止 FolderChangesView 及 Disk Pulse 等程式的監控功能，並將所記錄到之檔案及資料夾變化紀錄為報表檔。
- 使用 Regshot 登錄檔快照程式進行第二次快照，快照結束後並直接使用比較功能分析登錄檔在安裝軟體之前後差異處，並產生報表檔。
- 分析前二步驟之報表檔，整理及歸納該種 Android 仿真器軟體之重要檔案資訊，並找出可供鑑識參考之資料項目並加以記錄。

針對安裝於 Android 仿真器中之無線檔案傳輸及資訊隱藏應用程式相關實驗與觀察，以找出可能會留存鑑識資料之檔案名稱與路徑。在安裝及測試無線檔案傳輸及資訊隱藏應用程式時，使用的數位鑑識工具建議除以 X-Ways Forensics 整合性鑑識軟體進行分析外，對於 Android 仿真器檔案系統變動可藉由 AVD DDMS 加以記錄及分析。應用程式實驗步驟如下：

- 取得所欲鑑識之無線檔案傳輸及資訊隱藏應用程式，並記錄版本。
- 於本機端中先啟動 AVD DDMS 之 Logcat 功能，監控檔案系統變化情形。

- 在本機端中安裝無線檔案傳輸及資訊隱藏應用程式之 apk 檔，並在 AVD DDMS Logcat 觀察檔案變化情形，並將所記錄到之檔案及資料夾變化紀錄為報表檔。
- 執行無線檔案傳輸及資訊隱藏應用程式前、中、後分別下載應用程式記憶體內容(hprof)。
- 分析檔案系統及記憶體內容。



圖一：Android 仿真器及其應用程式研究方法

3.2 本機端實驗模擬環境說明

本研究使用微軟視窗作業系統做為本機端實驗環境，並於本機端中安裝系統登錄

檔、系統連接埠監控、檔案變化監控、AVD DDMS 及整合性鑑識分析等軟體，以觀察與紀錄與本研究有關之 Android 仿真器，於安裝及運行在本機端實驗環境中，所產生之檔案資料變動情形。

3.3 實驗 Android 仿真器軟體

目前安裝及使用 App 之 Android 仿真器日益盛行,因此本研究挑選 Andy v46.2.207、AmiDuos v3.1.30、BlueStacks v2.0、Genymotion v2.6.0 及 Memu v2.6.5 等 5 種市面上常見之 Android 仿真器進行實驗與分析。

3.4 實驗無線檔案傳送應用程式

目前可在 Android 系統下執行無線檔案傳送功能之應用程式相當多，本研究選擇 Smartdroid WiFi Transfer v1.0.9 及 Airdroid v3.2.2.1 等 2 種常見之無線檔案傳送應用程式進行實驗與分析，在本機端使用 Google Chrome 瀏覽器做為測試之檔案傳送平台。

3.5 實驗資訊隱藏應用程式

目前可在 Android 系統下所開發之資訊隱藏功能應用程式種類頗多，本研究選擇 Steganography Master v1.3 及 Stegais v1.2.2 等 2 種以隱藏文字於圖檔中之應用程式進行實驗與分析。

肆、研究發現

4.1 Android 仿真器之重要數位證據跡證

4.1.1 Andy

表一: Andy 仿真器重要鑑識項目

檔案系統分析		
重要檔案或資料夾名稱	存放路徑	鑑識價值
所有資料夾及 status.txt	C:\Users\ USER ACCOUNT}\AppData\Roaming\Andy	識別使用者是否使用及該仿真器之狀態資料
HandyAndy.ini	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\HandyAndy	記載仿真器安裝路徑，版本、虛擬機使用路徑
所有附檔名為.log及.txt檔	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\Logs	仿真器使用之相關紀錄

所有之檔案	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\machines\af48496a-085f-4698-8d8a-4d6ce371c7a0(GUID)\images	仿真器使用之檔案系統
android_system_disk.vmdk	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\machines\af48496a-085f-4698-8d8a-4d6ce371c7a0(GUID)\images	仿真器Android系統資料儲存空間
android_data_disk.vmdk	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\machines\af48496a-085f-4698-8d8a-4d6ce371c7a0(GUID)\images	仿真器模擬行動裝置之內部儲存空間
android_flash_disk.vmdk	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\machines\af48496a-085f-4698-8d8a-4d6ce371c7a0(GUID)\images	仿真器模擬行動裝置SD卡空間
564df9e3-68da-5860-e773-60cc09f7ed74(GUID).vmem	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\machines\af48496a-085f-4698-8d8a-4d6ce371c7a0(GUID)\images	仿真器模擬行動裝置之記憶體資料
登錄檔機碼分析		
重要機碼	登錄檔位置	鑑識價值
BuildID IMEI InstallerGuid MAC UID	HKEY_CURRENT_USER\Software\Andy\	仿真器重要系統資訊
InstallLocation Publisher RegCompany	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Andy OS\	提供仿真器安裝資訊
程序及網路埠分析		
啟動程序名稱	使用之連接埠	鑑識價值
AndyConsole.exe	5905	識別仿真器是否運行及與本機端之連接埠
Adb Shell連接		
可否使用 adb shell	adb connect 連接埠	可否 root
可以	5555	可以

4.1.2 AMIDuOS

表二:AMIDuOS 仿真器重要鑑識項目

檔案系統分析		
重要檔案或資料夾名稱	存放路徑	鑑識價值
所有檔案與資料夾	C:\ProgramData\AMI\DuOS\ C:\Users\{USER ACCOUNT}\.DuOS	識別使用者是否使用及該仿真器之狀態資料
config.xml	C:\ProgramData\AMI\DuOS\config	記載仿真器相關路徑資訊
rootfs.vdi	C:\ProgramData\AMI\DuOS\imgs	仿真器Android檔案系統
datafs.vdi	C:\ProgramData\AMI\DuOS\imgs C:\Users\{USER ACCOUNT}\.DuOS	仿真器模擬行動裝置之內部儲存空間
backup.vdi	C:\ProgramData\AMI\DuOS\imgs C:\Users\{USER ACCOUNT}\.DuOS	仿真器Android檔案系統備份空間
sdcard.vdi	C:\ProgramData\AMI\DuOS\imgs C:\Users\{USER ACCOUNT}\.DuOS	仿真器模擬行動裝置SD卡空間
登錄檔機碼分析		
重要機碼	登錄檔位置	鑑識價值
Android Apps DuOS Installed Directory	HKEY_CURRENT_USER\Software\AMI\DuOS\DuOS\	仿真器重要系統資訊
DisplayName DisplayVersion InstallDate InstallLocation	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\684C246D733528847A3F194A7C79BAAF\Features\	提供 仿真器安裝資訊
程序及網路埠分析		
啟動程序名稱	使用之連接埠	鑑識價值
DuOS.exe	3600	識別仿真器是否運行及與本機端之連接埠
DuoVMHeadless.exe	10088	識別仿真器是否運行及與本機端之連接埠
Adb Shell連接		

可否使用 adb shell	adb connect 連接埠	可否 root
可以	5564	可以

4.1.3 BlueStacks App Player

表三:BlueStacks App Player 重要鑑識項目

檔案系統分析		
重要檔案或資料夾名稱	存放路徑	鑑識價值
所有檔名為”HD-*.exe”之執行檔	C:\Program Files (x86)\BlueStacks	識別使用者是否使用及該仿真器之狀態資料
所有資料夾與檔案	C:\ProgramData\BlueStacks\Logs\	使用者資料與記錄資訊
Root.fs	C:\ProgramData\BlueStacks\Android	Android仿真器檔案系統
Prebundled.fs	C:\ProgramData\BlueStacks\Android	Android仿真器檔案系統
kernel.elf	C:\ProgramData\BlueStacks\Android	Android仿真器檔案系統
initrd.img	C:\ProgramData\BlueStacks\Android	Android仿真器檔案系統
Store	C:\ProgramData\BlueStacks\Android\Data.sparsefs	仿真器模擬行動裝置之內部儲存空間
Store	C:\ProgramData\BlueStacks\Android\SDCard.sparsefs	仿真器模擬行動裝置SD卡空間
登錄檔機碼分析		
重要機碼	登錄檔位置	鑑識價值
DataDir InstallDir LogDir USER_GUID UserDefinedDir	HKEY_LOCAL_MACHINE\SOFTWARE\BlueStacks\	仿真器重要系統資訊
BootParameters Initrd Kernel Memory	HKEY_LOCAL_MACHINE\SOFTWARE\BlueStacks\Guests\Android\	提供仿真器安裝資訊

程序及網路埠分析		
啟動程序名稱	使用之連接埠	鑑識價值
HD-Frontend.exe	53306	識別仿真器是否運行及與本機端之連接埠
Adb Shell連接		
可否使用adb shell	Adb connect 連接埠	可否 root
可以	5554	可以

4.1.4 Genymotion Emulator

表四:Genymotion Emulator 重要鑑識項目

檔案系統分析		
重要檔案或資料夾名稱	最要存放路徑	鑑識價值
所有檔案與資料夾	C:\Users\{USER ACCOUNT}\AppData\Local\Genymobile\Genymotion	識別使用者是否使用仿真器及該仿真器之狀態資料
所有資料夾	C:\Users\{USER ACCOUNT}\AppData\Local\Genymobile\Genymotion\deployed	仿真器使用之檔案系統
android_data_disk.vmdk	C:\Users\{USER ACCOUNT}\AppData\Local\Genymobile\Genymotion\deployed\Samsung Galaxy Note 3 - 4.3 - API 18 - 1080x1920	仿真器模擬行動裝置之內部儲存空間
android_sdcard_disk.vmdk	C:\Users\{USER ACCOUNT}\AppData\Local\Genymobile\Genymotion\deployed\HTC One - 4.2.2 - API 17 - 1080x1920	仿真器模擬行動裝置SD卡空間
android_system_disk.vmdk	C:\Users\{USER ACCOUNT}\AppData\Local\Genymobile\Genymotion\deployed\HTC One - 4.2.2 - API 17 - 1080x1920	仿真器 Android 系統資料儲存空間
sdcard.vdi	C:\Users\{USER ACCOUNT}\AppData\Local\Genymobile\Genymotion\deployed\HTC One - 4.2.2 - API 17 - 1080x1920	仿真器模擬行動裝置SD卡空間
logcat.txt	C:\Users\{USER ACCOUNT}\AppData\Local\Genymobile\Genymotion\deployed\HTC One - 4.2.2 - API 17 - 1080x1920	仿真器檔案系統使用記錄資料
{351ebd77-cd26-489f-9464-37	C:\Users\{USER ACCOUNT}\AppData\Local\Genymobile\	用於存放仿真器記

ef670018e4}.vmdk	Genymotion\deployed\HTC One - 4.2.2 - API 17 - 1080x1920\Snapshots	憶體快照資料
登錄檔機碼分析		
重要機碼	登錄檔位置	鑑識價值
credentials.password credentials.username customer.uuid personaluse.date	HKEY_CURRENT_USER\Software\Genymobile\Genymotion\	仿真器重要系統資訊
DisplayName InstallDate InstallLocation MajorVersion	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6D180286-D4DF-40EF-9227-923B9C07C08A}_is1\	提供仿真器安裝資訊
程序及連接埠分析		
啟動程序名稱	使用之連接埠	鑑識價值
player.exe	56877等多個連接埠	識別仿真器是否運行及與本機端之連接埠
Adb Shell連接		
可否使用 adb shell	Adb connect 連接埠	可否 root
可以	5555	可以

4.1.5 Memu

表五:Memu 重要鑑識項目

檔案系統分析		
重要檔案或資料夾名稱	最要存放路徑	鑑識價值
所有檔案與資料夾	C:\Program Files\Microvirt	識別使用者是否使用及該仿真器之狀態資料
*.log	C:\Users\{USER ACCOUNT}\.MemuHyperv	仿真器使用紀錄資料
MEmu-20160426-disk1.vmdk	C:\Program Files\Microvirt\MEmu\MemuHyperv VMs\MEmu	仿真器模擬行動裝置之內部儲存空間
MEmu-20160426-disk2.vmdk	C:\Program Files\Microvirt\MEmu\MemuHyperv VMs\MEmu	仿真器模擬行動裝置SD卡空間
MEmu-20160426-dis	C:\Program Files\Microvirt\MEmu\MemuHyperv	仿真器 Android 系統資

k3.vmdk	VMs\MEmu	料儲存空間
登錄檔機碼分析		
重要機碼	登錄檔位置	鑑識價值
(Default)	HKEY_CLASSES_ROOT\AppID\{819B4D85-9CEE-493C-B6FC-64FFE759B3C9}\	仿真器重要系統資訊
DisplayName DisplayVersion InstallLocation	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\MEmu\	提供仿真器安裝資訊
程序及連接埠分析		
啟動程序名稱	使用之連接埠	鑑識價值
MEmu.exe	57385、57387、57391	識別仿真器是否運行及與本機端之連接埠
MEmuHeadless.exe	21500等多個連接埠’	識別仿真器是否運行及與本機端之連接埠
Adb Shell連接		
可否使用adb shell	Adb connect 連接埠	可否 root
可以	21503	Y

4.1.6 小結

由上述 Android 仿真器數位證據項目分析可知，在本機端可擷取與蒐集。本研究比對數位證據鑑識項目後彙整關資訊如下表：

表六:Android 仿真器相關資訊彙整

Android 仿真器名稱	Andy	AmiDuos	Blackstacks	Genymotion	Memu
仿真器搭配使用之虛擬機軟體及技術	VmWare (VMDK)	Oralce VirtualBox(VDI)	自行開發之 LayerCake 虛擬技術	Oralce VirtualBox (VMDK)	Oralce VirtualBox(VMDK)
仿真器於本機端留存之數位證據跡證	使用紀錄(Log) 登錄檔機碼 記憶體資料	使用紀錄(Log) 登錄檔機碼 記憶體資訊 檔案及資料夾	使用紀錄(Log) 登錄檔機碼 記憶體資訊 檔案及資料夾	使用紀錄(Log) 登錄檔機碼 記憶體資訊 檔案及資料夾	使用紀錄(Log) 登錄檔機碼 記憶體資訊 檔案及資料夾

	檔案及資料夾				
仿真器記憶體能否直接擷取	可以	否	否	可以	否

本研究針對安裝於微軟視窗作業系統之 Android 仿真器進行數位證據種類分析，可得知在檔案系統中，可能包含數位證據如檔案及資料夾、登錄檔機碼（Registry）、程序及網路連接埠資訊、記憶體及使用紀錄(Log)，其中記憶體資料只有 Andy 及 Genymotion 等 2 種仿真器可直接擷取檢視，其他 3 種仿真器，必須使用植入程式及以 ADB 連接才得以擷取之。

4.2 無線檔案傳輸應用程式之重要數位證據跡證

4.2.1 Smartdroid WiFi Transfer

表七:Smartdroid WiFi Transfer 應用程式重要鑑識項目

仿真器內部檔案系統分析		
重要檔案或資料夾名稱	最要存放路徑	鑑識價值
com.smarterdroid.wififiletransfer 資料夾下所有資料夾與檔案	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\machines\af48496a-085f-4698-8d8a-4d6ce371c7a0(GUID)\images\android_data_disk.vmdk\data\	識別無線檔案傳送應用程式資料存放位置
external-0.db external-0.db-wal	\data\com.android.providers.media\databases	可用以識別傳送至 SD 外部記憶卡之檔案資訊
本機端檔案系統分析		
重要檔案或資料夾名稱	存放路徑	鑑識價值
History Favicons Network Action Predictor Preferences Shortcuts Top Sites Current Session	\Chrome\User Data\Default	可識別上傳之檔案資料及無線網路連線 ip 及連接埠紀錄
Cache 檔 data_1 data_3	\Chrome\User Data\Default\Cache	可識別曾經使用過之連接介面檔案資料及無線網路連線 ip 及連接埠資

		料
*.ldb	\Chrome\User Data\Default\Session Storage	可識別無線網路連線 ip 及連接埠資料
SyncData.sqlite3	\Chrome\User Data\Default\Sync Data	可識別無線網路連線 ip 及連接埠資料
網路連線分析		
App 提供之連線通信協定	遠端連線網址(IP)及預設使用連接埠	鑑識價值
HTTP HTTPS	192.168.189.133:1234 192.168.189.133:2345	識別 Smartdroid 應用程式使用之連線 IP 與連接埠資訊
仿真器及應用程式記憶體分析		
記憶體種類	傳送檔案資訊是否存在及以關鍵字分析	鑑識價值
仿真器記憶體檔(*.VMEM)	存在，能以關鍵字檢索分析	記憶體內容分析可查明傳送檔案資訊與連線紀錄
com.smarterdroid.wififiletransfer.hprof	存在，能以關鍵字檢索分析	記憶體內容分析可查明傳送檔案資訊與連線紀錄

4.2.2 AirDroid

表八:AirDroid 應用程式重要鑑識項目

仿真器內部檔案系統分析		
重要檔案或資料夾名稱	存放路徑	鑑識價值
com.sand.AirDroid 資料夾下所有資料夾與檔案	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\machines\af48496a-085f-4698-8d8a-4d6ce371c7a0(GUID)\images\android_data_disk.vmdk\data\	識別 AirDroid 無線檔案傳送應用程式資料存放位置
transfer.db transfer.db-journal	\data\com.sand.AirDroid\databases	檔案傳送紀錄
external-0.db external-0.db-wal	\data\com.android.providers.media\databases	可用以識別傳送至 SD 外部記憶

		卡之檔案資訊
仿真器外部記憶卡分析		
重要檔案或資料夾名稱	存放路徑	鑑識價值
AirMirror.RemoteInput.log main.log push.log \cache	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\machines\af48496a-085f-4698-8d8a-4d6ce371c7a0(GUID)\images\android_flash_disk.vmdk\Android\data\com.sand.AirDroid\	識別 AirDroid 使用紀錄以及曾經上傳之圖檔資料
所有檔案	\AirDroid\upload\	上載至仿真器的所有檔案資料存放位置
本機端檔案系統分析		
重要檔案或資料夾名稱	存放路徑	鑑識價值
History Favicons Network Action Predictor Last Tabs Shortcuts Top Sites Last Session History Provider Cache	\Chrome\User Data\Default	可識別上傳之檔案資料及無線網路連線 ip 及連接埠紀錄
Cache 檔 data_1 data_3	\Chrome\User Data\Default\Cache	可識別曾經使用過之連接介面檔案資料及無線網路連線 ip 及連接埠資料
*.ldb	\Chrome\User Data\Default\Session Storage	可識別無線網路連線 ip 及連接埠資料
SyncData.sqlite3	\Chrome\User Data\Default\Sync Data	可識別無線網路連線 ip 及連接埠資料
網路連線分析		
App 運作狀態	遠端連線網址(IP)及使用埠	鑑識價值
HTTP	Web.airdroid.com 192.168.189.133:8888	識別 AirDroid 應用程式使用之連線 IP 與連接埠資訊

仿真器及應用程式記憶體分析		
記憶體種類	傳送檔案資訊是否存在及以關鍵字分析	鑑識價值
仿真器記憶體檔(*.VMEM)	存在，能以關鍵字檢索分析	記憶體內容分析可查明傳送檔案資訊與連線紀錄
com.sand.airdroid.hprof	存在，能以關鍵字檢索分析	記憶體內容分析可查明傳送檔案資訊與連線紀錄

4.3 資訊隱藏應用程式之重要數位證據跡證

4.3.1 Steganography Master

表九:Steganography Master 應用程式重要鑑識項目

仿真器內部檔案系統分析		
重要檔案或資料夾名稱	最要存放路徑	鑑識價值
com.dinaga.photosecret 資料夾下所有資料夾與檔案	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\machines\af48496a-085f-4698-8d8a-4d6ce371c7a0(GUID)\images\android_data_disk.vmdk\data\	識別資訊隱藏應用程式資料存放位置
external-0.db external-0.db-wal	\data\com.android.providers.media\databases	可用以識別傳送至 SD 外部記憶卡之資訊隱藏檔案資訊
仿真器外部記憶卡分析		
重要檔案或資料夾名稱	存放路徑	鑑識價值
Steganography Master	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\machines\af48496a-085f-4698-8d8a-4d6ce371c7a0(GUID)\images\ android_flash_disk.vmdk\	識別曾經使用 Steganography Master 所產生之圖檔資料
仿真器與應用程式記憶體分析		
資訊隱藏藏密文字及密碼狀態	在記憶體內之字串特徵值及顯示狀態	鑑識價值
藏密之文字(無設定密碼)	(#*CEVAP*#)資訊隱藏文字之明文內容	記憶體內容分析可解析隱藏之藏密

		文字
藏密之文字(有設定密碼)	(#*CEVAP*#)[!$設定之密碼$!]資訊隱藏文字之明文內容	記憶體內容分析可解析隱藏之藏密文字及密碼

4.3.2 Stegais

表十:Stegais 應用程式重要鑑識項目

仿真器內部檔案系統分析		
重要檔案或資料夾名稱	存放路徑	鑑識價值
com.romancinkais.stegais 資料夾下所有資料夾與檔案	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\machines\af48496a-085f-4698-8d8a-4d6ce371c7a0(GUID)\images\android_data_disk.vmdk\data\	識別 Stegais 無線檔案傳送應用程式資料存放位置
gallery.WL gallery_stegais.WL gallery_最新圖片.WL	\data\cn.xender\files	使用圖庫功能紀錄
external-0.db external-0.db-wal	\data\com.android.providers.media\databases	可用以識別傳送至 SD 外部記憶卡之檔案資訊
mailstore.電子郵件帳號@gmail.com.db mailstore.電子郵件帳號@gmail.com.db-wal	\data\com.google.android.gm\databases	以電子郵件傳送圖檔紀錄
search.db	\data\cn.xender\databases	圖檔搜尋紀錄
仿真器外部記憶卡分析		
重要檔案或資料夾名稱	最要存放路徑	鑑識價值
stegais	C:\Users\{USER ACCOUNT}\AppData\Roaming\Andy\machines\af48496a-085f-4698-8d8a-4d6ce371c7a0(GUID)\images\android_flash_disk.vmdk\	識別 stegais 曾經產生之圖檔資料
仿真器及應用程式記憶體分析		
資訊隱藏加密文字及密碼狀態	在記憶體內之字串特徵值及顯示狀態	鑑識價值
藏密之文字(無設定密碼)	可顯示資訊隱藏文字之明文內容但藏碼文字前後均無特定字串可識別	記憶體內容分析可解析隱藏之藏

		密文字
藏密之文字(有設定密碼)	可資訊隱藏文字之明文內容及密碼,但藏密文字及密碼前後均無特定字串可識別	記憶體內容分析可解析隱藏之藏密文字及密碼
使用資訊隱藏技術之圖檔分析		
圖檔類型	圖檔變化狀態	鑑識價值
原始照片	會新增 APP0 MARKER (FFE1→FFE0)在圖檔檔頭會有 JFIF metadata 產生	顯示圖檔內容可能有遭編修之可能

伍、結論與未來研究方向

本研究針對 5 種 Android 仿真器、2 種無線檔案傳送應用程式及 2 種資訊隱藏應用程式進行實驗,以探究本機端所留存之數位證據項目。由於此類較新型的 Android 仿真器,在學術上並無相關研究資料可供參考,因此本研究嘗試以現行數位鑑識實務作業之程序與方法,找出主機端可能潛藏數位證據之仿真器檔案結構及檔案特徵項目。

實驗結果顯示,5 種仿真器使用之虛擬核心技術有所不同,搭配之虛擬化環境技術亦不相同。但檔案之存取仍依循 Android 平台之檔案系統架構,因此可以數位鑑識之程序與方法取得存放於仿真器中之應用程式資料。對於使用此類 Android 仿真器做為犯罪工具,仍可有效從中擷取數位證據。經實驗得知,Android 仿真器於本機端將留存檔案資料或資料夾、瀏覽器暫存檔、登錄檔機碼、程序及連接埠及記憶體等主要資訊。

本研究所列之 2 種無線檔案傳送應用程式及 2 種資訊隱藏應用程式,經實驗得知仍可由仿真器內部檔案系統、仿真器外部記憶卡、本機端檔案系統、網路連線及仿真器與應用程式記憶體等方面,分析出可能潛藏數位證據之仿真器檔案結構及檔案特徵項目。

實驗結果也顯示無線檔案傳送及資訊隱藏應用程式使用加密通訊協定與加密演算法,則能擷取之數位鑑識項目將相當有限,透過記憶體內容之比對雖可找到有利之鑑識項目與特徵值,但有關記憶體中此類加密字串特徵值仍有待探究,而目前此種新型態應用程式對於檔案與資料庫內容進行加密的情況越來越盛行,對於數位鑑識實務作業實為一嚴峻之挑戰,有關此類應用程式解密之鑑識技術與方法的研究與開展,仍有待深入探究。

參考文獻

[1] https://developer.android.com/studio/index.html(2016/5/15).

[2] https://www.visualstudio.com/en-us/features/msft-android-emulator-vs.aspx(2016/5/15).

[3] https://www.manymo.com/(2016/5/15).
[4] http://www.amiduos.com/(2016/5/15).
[5] http://www.andyroid.net/(2016/5/15).
[6] http://www.bluestacks.com/about-us/app-player.html(2016/5/15).
[7] http://www.droid4x.com/(2016/5/15).
[8] https://www.genymotion.com/(2016/5/15).
[9] http://www.koplayer.com/(2016/5/15).
[10] http://www.memuplay.com/(2016/5/15).
[11] http://noxappplayer.com/(2016/5/15).
[12] http://www.droid4x.com/(2016/5/15).
[13] https://www.xamarin.com/android-player(2016/5/15).
[14] https://youwave.com/(2016/5/15).
[15] http://mirror1.jarfil.net/androvm.org/androvm.org-blog-download-index.html(2016/5/15)
[16] M. I. Al-Saleh and Y. A. Forihat, "Skype Forensics in Android Devices", *International Journal of Computer Applications* (*IJCA*)", vol. 78, no. 7, pp. 38-44, 2013.
[17] S. Treleven, V. Christopher, T. Fenger, J. Brunty, and, J. Price, "Forensic Analysis of Dropbox Application File Artifacts Recovered on Android and iOS Mobile Devices", 2013.
[18] M. Al-Hadadi and A. AlShidhani, "Smartphone forensics analysis: A case study", *International Journal of Computer and Electrical Engineering*, vol. 5, no. 6, p576, 2013.
[19] P. Andriotis, G. Oikonomou, and T. Tryfonas, "Forensic analysis of wireless networking evidence of android smartphones", *IEEE international workshop on Information forensics and security (WIFS)*, pp. 109-114, 2012.
[20] B. Busstra, N. A. Le-Khac, and M. Kechadi, "Android and Wireless data-extraction using Wi-Fi", *Fourth IEEE International Conference on Innovative Computing Technology (INTECH)*, pp. 170-175, 2014.
[21] W. Mazurczyk and L. Caviglione, "Steganography in modern smartphones and mitigation techniques", *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 334-357, 2015.
[22] D. P. Chowdary and Q. Liu, "Exploring Covert Communication in Text Message on Android Smartphones", Space, 32, 36.
[23] R. Ghare, P. Bansode, S. Bombale, and B. Chandargi, "LSB Steganography Using Android Phone", *International Journal of Computer Science and Information Technologies (IJCSIT)*, vol. 6, no. 2, pp. 1027-1029, 2015.