南華大學科技學院資訊管理學系

碩士論文

Department of Information Management
College of Science and Technology
Nanhua University

Master Thesis

高科技犯罪之研究－探討以行動通訊裝置 APP 為犯罪工具之偵查困境與因應作為

Study on High-Tech Crimes--Discussion on the Investigation Challenge and Correspondence of Using Mobile Applications as a Criminal Tool

梁哲賓

Che-Pin Liang

指導教授：吳光閔 博士

Advisor: Kuang-MinWu, Ph.D.

中華民國 108 年 6 月

June 2019

南 華 大 學

科技學院資訊管理學系

碩 士 學 位 論 文

高科技犯罪之研究－探討以行動通訊裝置 APP 為犯罪工具之偵查困境與因應作為

Study on High-Tech Crimes-Discussion on the Investigation Challenge and Correspondence of Using Mobile Applications as a Criminal Tool

研究生：梁哲嘉

經考試合格特此證明

口試委員：許瑞榮

謝定助

吳光陽

指導教授：吳光陽

系主任(所長)：陳世良

口試日期：中華民國 108 年 5 月 29 日

南華大學碩士班研究生

論文指導教授推薦函

資訊管理 系碩士班 梁哲賓 君所提之論文

係由本人指導撰述，同意提付審查。

指導教授 吳光閔

108 年 4 月 26 日

南華大學資訊管理學系碩士論文著作財產權同意書

立書人：梁哲賓　之碩士畢業論文

中文題目：高科技犯罪之研究-探討以行動通訊裝置 APP 為犯罪工具之偵查困境與因應作為

英文題目：Study on High-tech Crimes-Discussion on the Investigation Challenge and Correspondence of Using Mobile Applications as a Criminal Tool

指導教授：吳光陸 博士

學生與指導老師就本篇論文內容及資料其著作財產權歸屬如下：

☐ 共同享有著作權

☐ 共同享有著作權，學生願「拋棄」著作財產權

☑ 學生獨自享有著作財產權

學　　生：梁哲賓　（請親自簽名）

指導老師：吳光陸　（請親自簽名）

中華民國 108 年 5 月 29 日

高科技犯罪之研究－探討以行動通訊裝置 APP 為犯罪工具之偵查困境與因應作為

研 究 生：梁哲賓　　指導教授：吳光閔 博士

南 華 大 學 資訊管理學系碩士班

摘　　要

歹徒利用高科技的技術來遂行其犯罪行為已成常態，有關這類型的犯罪行為並非僅使用電腦為其犯罪工具，也會使用到較特殊的高科技性電子產品，如行動通訊、數位的攝影設備及各種智慧卡（Smart Card）等。近來的發現則以行動通訊裝置 APP 為犯罪工具的情形最為嚴重，在我國運用這類高科技作為其犯罪工具者又以詐欺、毒品犯罪、賭博、網路援交等 4 類較多。目前只要擁有社群網路服務（例如 Facebook）或者網路即時通訊服務（例如 LINE）者，幾乎人人接過詐騙訊息，另外，如比特幣洗錢、網路勒索、竊盜個資等也都是運用高科技犯罪方式在進行著。可惜的是在法令規範不完備及偵辦技術未獲突破狀況下，司法人員在偵辦以行動通訊裝置 APP 為犯罪工具之案件遭受重大挑戰，其實對辦案人員而言，高科技犯罪偵查重點在先瞭解傳送訊息者之真實身分（個化使用者）與他目前的地理位置（追蹤他的位置）較重要。

時下各式各樣社群網路、網際網路應用服務（APP）的大量使用，在運

用加密、匿名網路，且 APP 服務提供者大多位於國外及雲端儲存下，數位偵查與鑑識已更加困難，治安機關面臨難以透過封包解譯或網路接取服務提供者調閱通聯紀錄而追蹤個化使用者之困境。因此，有必要從不同的出發點，發展新的數位偵查與鑑識方法。

關鍵詞：高科技犯罪、行動通訊裝置 APP、社群網路、加密、匿名網路

Study on High-Tech Crimes-Discussion on the Investigation Challenge and Correspondence of Using Mobile Applications as a Criminal Tool

Name of Student: Che-Pin Liang Advisor: Kuang-Min Wu, Ph.D.

Department of Information Management
Nanhua University
Master Thesis

ABSTRACT

Gangsters use high-tech technology to carry out their criminal activities. This type of crime is not only a crime of using computer crime but also uses special high-tech electronic products, such as smartphone, digital photography equipment, various smart cards, etc. Recently, investigators discovered that more and more suspects in Taiwan have used mobile devices as their criminal tools, especially in fraud, drug, gambling, and prostitution cases are the most broadly used. Everyone received those fraudulent messages if he/she has social media or instant messaging account. In addition, bitcoin laundering, ransomware, personal data stealing are also using high-tech to crime. It is a pity that under the condition that the laws and regulations are incomplete and the investigation techniques have been limited, the investigators have encountered major challenges in such cases. In fact, the most important thing to the

investigators is identified of who has sent the message (the individual user) and where the suspect (or tracking his location) is.

Nowadays, a large number of social networks and Internet application services (APPs) are widely used, and encryption and anonymous networks are used, and APP service providers are mostly located in foreign countries and in the cloud. Digital investigation and forensics have become increasingly difficult, and law enforcement agencies are faced with the difficulty of tracking individualized users through packets reconstructed or Internet access service providers. Therefore, it is necessary to develop new methods of digital investigation and forensics from different starting points.

Keywords: Hi-tech crime, Mobile application, Social network, Encryption, Anonymous network

目錄

表目錄

圖目錄

第一章 緒論

內政部警政署統計 2018 年通訊監察數有 32126 件 52692 線，而 2019 年 1-3 月則有 7381 件 12964 線（如表 1-1），可見司法人員藉由通訊監察手段分析案情已是重要辦案方式。資訊科技之快速進步，讓很多產業發生很大的變革，以通訊而言，行動通訊裝置 APP 的發明與運用，帶給人們許多的方便性，也取代了過去以行動電話互通的通訊以及傳統的語音聯絡的通話方式，同時也取代了以簡訊聯絡通訊方式，其具互動性及多媒體特點帶給我們隨時隨地應用的方便性（翁豪健，2015）。

表 1-1 內政部統計資料

年度	單位	警察	調查局	檢察署	其他	總計
2016	件	19116	5451	126	3692	28385
	線	25451	7728	162	7164	40505
2017	件	20696	5693	43	4128	30560
	線	31006	7561	45	8381	46993
2018 年	件	21422	6088	19	4597	32126
	線	34419	8565	28	9680	52692
2019 年 1-3 月	件	5052	1372	0	957	7381
	線	8490	2175	0	2299	12964

（資料來源：內政部）

因為行動通訊裝置 APP 使用之方便性廣為一般民眾喜愛，卻也成為犯罪者犯罪工具，相對的，這類的高科技犯罪行為，形成對犯罪偵防的司法人員在辦案時帶來相當程度的困境,直接的衝擊是造成監聽作為上的限制，導致當辦案人員在偵查時發現到監察目標時，歹徒如使用行動通訊裝置 APP 實施語音通訊，或是以文字傳送犯罪之文字訊息，做為其同夥之通聯時，礙於科技技術，往往就不易有效的對犯罪者實施持續的追查與偵辦（侯友宜，2011），學者 Bromby(2006)特別強調就高科技犯罪問題上，參與執法的所有單位應不斷發展新的科技技術，以積極辦理犯罪偵查與犯罪防治工作。

另外,對於偵辦中已被鎖定的以高科技犯罪目標常會造成辦案的障礙，究其原因常是受限法令規範不明確或未授權，因為目前法令對行動通訊裝置 APP 的業者，並無明確規定其具有協助提供犯罪偵辦之義務，另外行動通訊裝置 APP 軟體不斷更新或加密,導致偵辦中的案件無法繼續往下追探，對此，應如何因應這類的高科技犯罪，便已經成為目前司法人員辦案的重要議題。

至於總公司大多設在國外的行動通訊裝置 APP 業者，請其協助辦理相關案件，也成為另一案件偵辦的困境（黃茂穗，2014），在執法人員面臨上述的問題時往往帶給滿腔熱血的司法人員重大辦案障礙。目前除了行動通訊裝置 APP 案件偵辦上常遇到辦案瓶頸外，亦須面對許多艱困挑戰。

第一節 研究背景

壹、以行動通訊裝置 APP 為犯罪工具嚴重影響治安

時下智慧型手機以及平板電腦等的相繼出現，提供消費者在通訊上更多的方便性，這些產品大多結合行動通訊裝置 APP（蘭文裡，2011）。通訊產品已不再只有通話功能，其多項性以及方便性，讓通訊裝置帶領我們持續往新的科技領域前進（馬克・古德曼，2016），科技的進步為時代趨勢，現今影響我們生活較大者為通訊方式，通訊科技會不斷的以代差方式演化（蔡明德等，2010）。另外，過去以簡訊方式發送訊息方式，現在已由行動通訊裝置 APP 的文字訊息來使用，這類高科技的使用方式，較以前方便許多，卻也提供欲從事犯罪宵小另一聯繫方式，藉由資訊的方便性以及普遍性，嫌犯深知這類行動通訊裝置的優點，並已廣為應用這類通訊軟體，藉以做為其犯罪之工具，嚴重影響治安（黃逸玲，2018）。

貳、法令與技術限制對案件偵辦造成障礙

法令是用來保護善良民眾的，但執法單位宥於法令的修編趕不上實務上的需要，破案的件數亦未獲突破，導致司法人員面對這類高科技犯罪往往束手無策，但又礙於職責所在，基於剷奸除惡為司法人員本職工作，必須尋求解決之道，卻又因受到法令制約因素，稍一不慎即可能觸犯法令，為執勤人員帶來莫大障礙（陳鼎駿，2012）。目前行動通訊裝置 APP 進行犯罪行為已儼然成為高科技犯罪常態。

從警政署 107 年 1-5 月警察機關受理 LINE 詐欺案件概況分析（嫌疑人及被害人均以男性及「18-39 歲」年齡層為主）107 年 1-5 月警察機關受理 LINE 詐欺案件發生數計 450 件，較上年同期增加 16.16 個百分點。107 年 1-5 月 LINE 詐欺案件嫌疑人與被害人 18-23 歲 32.75%，

24-29 歲 24.57%，30-39 歲 24.57%，其他 18.11%，嫌疑人 403（男性占 71.71%）。30-39 歲 23.76%，24-29 歲 23.08%，18-23 歲 21.20%，其他 31.97%，被害人 585（男性占 62.22）（如圖 1-1）。

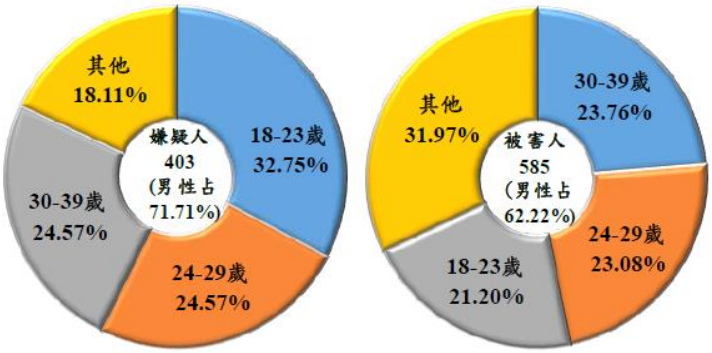


圖 1-1 嫌疑人與被害人相關資料統計

（資料來源：內政部）

同期 LINE 詐欺犯罪方法以「假網路拍賣（購物）詐欺」占 26.44%最多，「色情應召詐財」占 22.67%次之，「假冒名義詐欺」占 20.00%居第 3，3 者合占 7 成。

同期嫌疑犯計 403 人，以男性嫌疑犯占 71.71%居多，年齡層則以「18-39 歲」占 81.89%為主；被害人計 585 人，亦以男性占 62.22%居多，年齡層「18-39 歲」占 68.03%。

隨著智慧型手機與平板電腦等行動通訊裝置的普及，通訊軟體也成為生活及工作上常用的溝通工具，尤其使用 LINE 者眾多，故容易成為詐騙集團的犯罪工具。為避免民眾受騙，警政署與 LINE 公司合作，採取驗證簡訊中文化、換機密碼、其他裝置試圖提醒等多項措施外，另於 165 官網、165 反詐騙 APP、165 臉書粉絲專頁及 165 LINE 反詐騙宣導群組，每週定期更新「千萬別加好友」之詐騙 LINE ID，並將資

料同步置於「政府資料開放平臺」及「內政部資料開放平臺」，提供多元化查詢管道。

但 LINE 詐欺案件發生數自 104 年 703 件逐年上升至 106 年 1,325 件，自 104 年 49.22%上升至 106 年 74.26%。利用行動通訊裝置 APP 為犯罪工具之詐騙案似乎仍不斷在增加中。

警政署亦再進一步分析以 LINE 進行詐欺案件，其相關分析如下：

一、嫌疑人及被害人均以男性及「18-39 歲」年齡層為主，分析原因為此一階層民眾為行動通訊裝置 APP 忠實愛用者，同時也表示這一階層的犯罪嫌疑人熟悉以行動通訊裝置 APP 為犯罪工具。

二、破獲率的分析上，所顯示的意義為在以詐欺案件的犯罪行為中歹徒使用的通訊方式是以行動通訊裝置 APP 作為其主要通聯，並非其通訊軟體LINE遭破解而破案，另經統計，在這些破案的例子中，全無歹徒在使用通訊軟體中遭解密或其通聯內容遭司法人員即時攔阻而破案者（梁哲賓，2019）。

參、群組互聯加深辦案困難

雖然近年來通訊監察核准執行情形有增加，但是增加數卻與實際執行數同時成長，在同一時間辦理在執行監察的門號中，只有監聽語音以及非通話事件，跟其他有數據通訊資料分析，卻是呈現一比較特殊的情形，探究原因是瀏覽數據有增加的情形，另同一案件偵辦人員在監聽期間，發現到嫌犯為關機狀況，而是在未更換門號情形下，但是語音的通話流量卻減少，統計中也發現通話內容與犯案有關資訊有

顯著減少，實際上群組互聯（如圖 1-2）為犯罪之行為仍在進行，經由司法人員的辦案經驗與逮獲嫌犯之供詞可確認其以行動通訊裝置 APP 進行犯罪行為（梁哲賓，2019）。

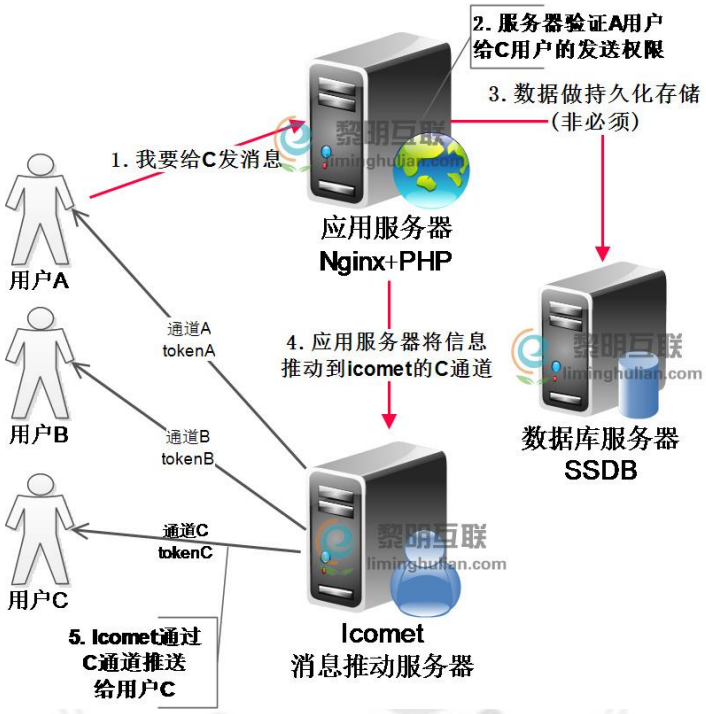


圖 1-2 群組互聯為犯罪聯繫

（資料來源：智庫百科）

目前市面上的智慧行動電話業者，為吸引消費者及擴展業務，不斷的為其功能推陳出新，以通訊而言，行動通訊裝置 APP 基本上具有以免付費之功能與他人通話的基本特性，比較特殊的更是具備以多向方式，也就是以群組互聯的通訊模式，並且可以兩人以上相互重送訊息，以這種群呼模式的通訊，對兩人以上的犯罪行為有其助益，就如同對講機使用的方便性，而且功能更先進，有犯意者自然趨之若鶩，尤其詐欺與販毒，但是司法人員礙於法令與技術的限制，雖然通訊監察同意書的申請比率增加了，但對案件偵破卻未見增加，辦案人員除

了傳統通聯簡訊紀錄外，如何針對上述軟體進行資料之蒐集也是大課題（黃翰文，2013）。

肆、司法人員無法突破瓶頸被迫回到傳統辦案方式

因辦案人員對高科技犯罪案件未能有效突破，案件偵辦人員手中有案件偵辦，卻無法施展，辦案成效無法從案件中獲取績效，是導致破案率無法提升原因，只能回到傳統辦案方式，也就是依照刑事訴訟法規定以申請搜索票的模式辦案，但這種傳統辦案方式，往往對於高科技犯罪的偵防成效有限，不然就是耗時甚鉅，如果順利結案，可能就此斷線，但以辦案經驗而言，案件是越辦線索越多，一個案件往往可由蛛絲馬跡中另闢多個辦案線索，如前面所言，犯罪偵查中對高科技犯罪的案件偵辦施展不開，線索可能會隨時斷線無法再辦下去（朱子函，2017）。

我國行動通訊由民國 80 年代 2G、3G 到 4G，與時俱進地配合國際通訊標準，適時調整通話品質與功能，通訊業者為求通訊服務能夠滿足消費者需要，因應業務拓展不斷的擴充基地臺，同時更新通訊設施，尤其目前的 4G 系統已經跳出了過去的以語音傳送模式，改以封包（如圖 1-3）傳送模式進行通訊，其通話品質與速度及功能性，均是過去無法比擬的（蘇俊吉，2016）。

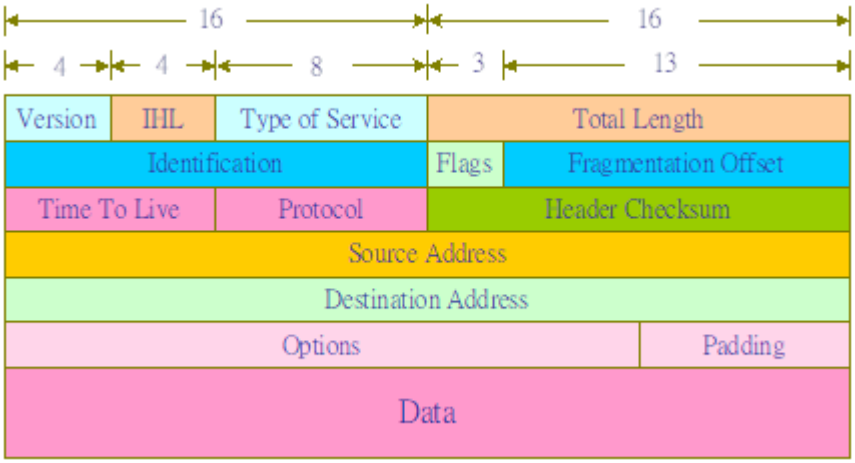


圖 1-3 IP 封包結構

伍、加密通訊軟體無解密技術

辦案者要瞭解歹徒犯罪內容，必須要實施解密或解譯程式，這樣就造成辦案人員困擾，以對通訊軟體之解密而言，因為要有業者的程式，不然將無法破解，或需費時甚久，LINE Event Delivery Gateway(LEGY)伺服器處理所有經過 LINE 的訊息，負責將不同類型訊息傳送至後端的伺服器，當用戶的設備中的 LINE APP 連線到 LINE 的服務時，重要的資料傳輸都會透過 LEGY 伺服器來處理，因此，為了確保傳輸的效率與安全，LEGY 協定根據通訊軟體的特性修改了部分 SPDY 的功能來降低網路傳輸的延遲，透過 LEGY 協定，LINE 可以將訊息都放置於加密的 TCP 通道中傳輸而不會因為加密而犧牲太多的通訊品質(如圖 1-4)。APP 加密特性可避免其通聯之內容遭解譯而還原，犯罪者常藉此一特性以規避通訊監察（田哲夫，2008），但目前國人使用的 LINE 公司在日本，礙於國情，要求其提供協助有相對的困難性(黃茂穗，2014)。

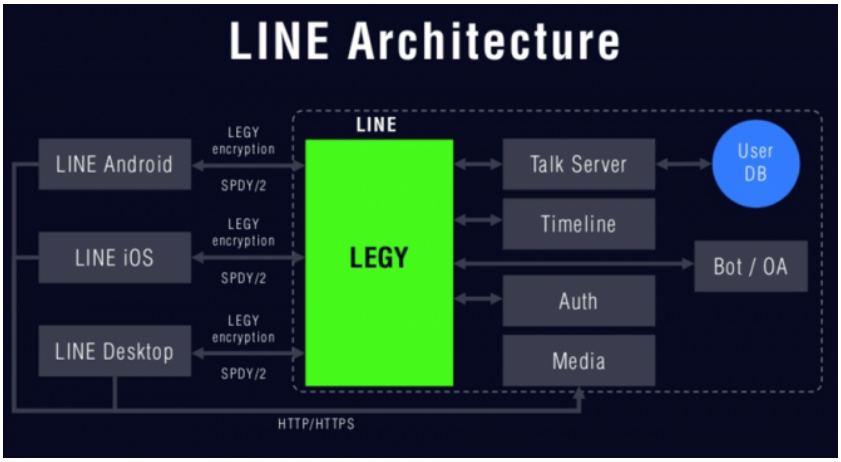


圖 1-4 LINELEGY(LINE event delivery gateway)

有鑑於行動通訊軟體因不易解譯（密）造成辦案困擾，為尋求解決方式，專責重大刑事案件偵辦的刑事警察局通訊監察科為解決上述問題研發破解程式，於民國 102 年間曾就安卓系統以單一型號智慧手機，成功破解 LINE 之通話內容與圖檔（如圖 1-5），但消息傳出後，卻造成一般民眾誤以為司法單位已具破解LINE能力(蘋果日報，2013)，如屬實，將嚴重影響人民通訊自由，同時引起民意代表的關切，殊不知刑事警察局通訊監察單位該次對 LINE 文字與圖檔的破解成功後，爾後就從未能再成功破解，但是消息卻造成社會大眾的高度關切，足見民眾對通訊隱私的重視。

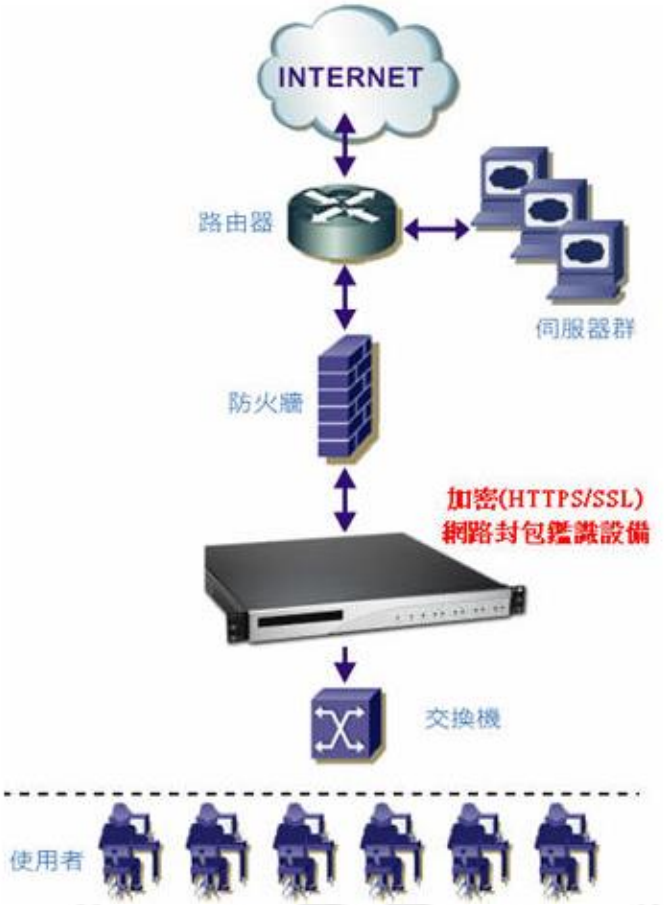


圖 1-5 HTTPS/SSL 加密網路封包鑑識設備

陸、隱私權限縮執法作為

犯罪偵防為司法人員本職，惟科技之進步快速，相對而言，這類以科技的犯罪行為也常因帶有科技背景，導致偵辦的困難（陳順和，2015），另一方面，由於法令常跟不上犯罪的腳步，常常無相關法令可適用，再來就是牽涉隱私權問題，因時代的進步與對隱私權的保護，只要有關個人權益與隱私的相關議題一披露，常常未能在真相獲得證實前，已被負面的討論，間接引發民意代表的抵制，徒增辦案的困擾。

以偵辦行動通訊裝置 APP 為工具的相關犯罪行為而言，往往牽涉的層面較大，因此，常引起涉及有關隱私甚或與憲法保障人權的議題，

同時要考慮依法辦案的原則，無論通聯調閱或監票申請，都要依照通保法規定（黃逸玲，2018），辦案人員常疑惑的是在辦理高科技犯罪案件時，往往本身雖有良好辦案技巧，但法制規定卻反而成為辦案的絆腳石（王澤鑑，2007）。

對於偵辦以行動通訊裝置 APP 為犯罪工具偵查權限問題，如何依法偵辦才不致於違法，甚至辦案人員辛苦取得的資料常最後變成無證據的能力，以及遭到質疑因辦理這類案件遭當事人懷疑侵害隱私權的問題等困境，在審視我國的法令對於行動通訊裝置 APP 的偵查規範，其實並無較明確的法規適用，通保法以及刑訴法亦不例外，因此，形成爾後司法人員在辦理這類高科技犯罪案件時，將遭到如同偵辦海巡人員因辦案使用 GPS 遭告案件的偵辦困擾（自由時報，2016）。

以往司法人員在案件偵辦上常依賴傳統的電話監聽（黃冠傑，2018），但是運用網路之通訊軟體犯案已經成為犯嫌最重要的聯繫方式，因通訊軟體採用封包來傳送資訊，與傳統的監聽模式為使用線路語音交換聯繫模式已有不同，也常造成辦案的困擾。

第二節 研究目的

壹、應用傳統通訊監察於行動通訊裝置 APP 犯罪效益不佳

科技的進步在通訊領域的發展更是快速，就如前述，在經過短短幾年的時間，行動通訊已由 2G 進入到目前的 4G，甚至 5G，5G 將在民國 109 年釋照 110 年即要開始商轉（自由時報，2019）。

行動通訊 2G 與 3G 通訊傳輸是以線路交換方式進行，但是到了 4G

的應用，為求速度更快，頻寬更大，已改為封包方式傳送，行動通訊裝置 APP 即是以網路封包傳送，因此，以傳統的線路交換的通訊監察模式，是無法達到監聽的效果。

貳、尋求解決行動通訊裝置 APP 偵查上的困境與破案技術

在以封包傳送模式另一特點，就是可以有效的加密，針對這樣的特點，目前時下的行動通訊裝置 APP 的應用上，業者為爭取消費者的信賴，幾乎都有加密，執法人員如無法取得解密方式，對案件的偵辦將遇到難以突破的瓶頸，對犯罪偵查產生一定衝擊（劉孟奇，2013），尤其國人常用的行動通訊裝置 LINE，其公司設在日本，因國情不同，該公司大可不理我國司法單位對其要求的協助，因此，司法人員在辦案時，如遇到這類的行動通訊裝置，礙於技術與法令的限制，只能繞回以傳統跟監方式，或案件快收網時，以定位方式處理，這樣的態樣明白的說，就是對行動通訊裝置 APP 犯罪無有效因應之道。

我國目前負責通訊監察的單位，分別是法務部調查局及內政部警政署刑事警察局通訊監察科，依據分工（如表 1-2），法務部負責中華電信及亞太電信業務，刑事警察局負責（王澤鑑，2007）臺灣大哥大、遠傳電信及臺灣之星等 3 家通訊業者相關業務（行政院 102 年院會院長裁示），依目前該 2 個負責通訊監察業務單位，建置通訊監察能量，對於行動通訊之語音與簡訊部分的監察，均可有效掌握監聽效能，但在以行動通訊裝置 APP 所傳送的語音、圖檔或文字等訊息，卻無法有效解密。

表 1-2 通訊監察分工

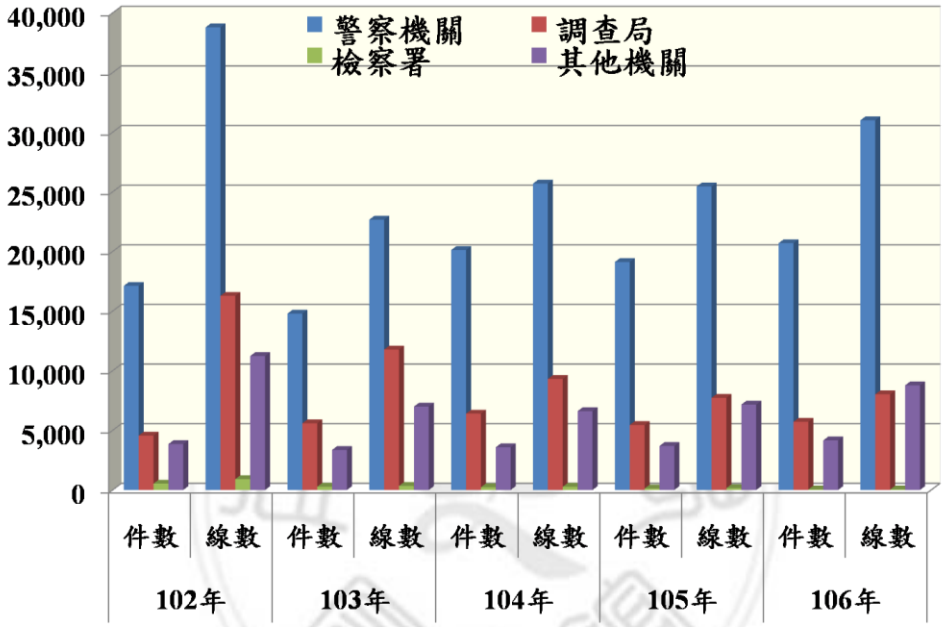
1. 建置機關 / 系統別		內政部警政署刑事警察局 通訊監察科	法務部調查局 通訊監察處
行動電話		台灣大哥大 遠傳電信 台灣之星電信	中華電信 亞太電信
市內電話			中華電信
中華電信HiNet及NGN		前端共建，後端分建	前端共建，後端分建
民營固網		台灣固網 新世紀資通	亞太電信
室內網路業務（小固網）	集團業者	凱擘 台灣大寬頻 台灣寬頻通訊	中嘉網路集團 台灣數位光訊科技
	非集團業者	大台中數位（原威達雲端） 其餘輪流建置	輪流建置

有鑑於國際間之先進國家在刑事偵查與鑑識技術方面不斷地研發精進，為解決行動通訊裝置 APP 犯罪問題，本研究創新理論研擬各項實驗分析平臺，並經驗證後建置社群網路偵查暨鑑識能量系統等平臺，目的為透過 IP 連線資料保存等方式執行 APP 犯罪案件偵辦，對於帶動國內整體刑事偵查科技品質的提升，有相當的指標與實質意義；對於國內目前盛行的網路犯罪之偵查技術研究方面，亦可引導國內司法機關同步邁向新的發展方向。

司法單位辦案應用通訊監察每年統計線數基本上以傳統語音為主（如表 1-3），惟近來歹徒以通訊軟體作為其犯罪聯繫，司法單位在這方面所遇到的難題造成案件偵辦產生諸多盲點與困境，尤以近來刑事

警察局在偵破多件的電信詐欺與毒品走私，以及非法槍械走私等重大危害社會治安與國家安全的案件中，均發現嫌犯都利用行動通訊裝置APP 進行其犯罪聯繫，解決偵查上的困境與破案技術是本研究目的。

表 1-3 通訊監察年度件線數統計



第三節 研究流程

本研究共六章，分別為第一章緒論、第二章文獻探討、第三章研究方法與設計、第四章偵查問題與困境、第五章實驗平臺與實證平臺建置、第六章結論與建議，各章研究範圍如下：

第一章、緒論：本章在敘明本文將研究背景與動機，研究之目的，以及研究流程，另對本研究之初步對論文所欲說明的內容，並概要說明研究之重要部分，藉以將研究的主要目的與想要達成的研究效果表達出來，連

貫研究主題顯現出與欲陳述之研究內容，明確地表達司法人員在偵辦案件的困境與需要。

第二章、文獻探討：高科技犯罪為目前犯罪趨勢之一，如毒品及詐欺犯罪等，而行動通訊裝置 APP 常為其犯罪使用之工具，但是行動通訊裝置 APP 為近來才發展出來的新形態科技軟體，在法令未能與時俱進做出適當修改狀況下，導致相關法規對司法人員在偵辦以行動通訊裝置 APP 為犯罪工具常受限制，此為本研究所重視議題之一。

另因本研究為探討行動通訊裝置 APP 相關研究，因此文獻探討中亦做有關行動通訊進程的研究，基本原理等問題，最後則是以技術創新（科技技術創新）因應以行動通訊裝置 APP 為犯罪行為之探討，並以小結作為本章綜整。

第三章、研究方法與設計：在研究方法的規劃，是以文獻分析法及系統科學分析法規劃，至於研究設計則是藉由行動通訊之發展與犯罪之關係敘述，以及執法之困境與因應做法。

第四章、偵查問題與困境：本章首先探討通訊監察國際標準，再就刑事警察局通訊監察科作業流程分析說明，分析目前行動通訊裝置 APP 偵查困境，法令部分包含通保法規定不夠周延以及偵辦第二類電信困境，實務上在偵辦以行動通訊裝置 APP 為犯罪工具辦案困境等等。

第五章、實驗平臺與實證平臺建置：區分兩個區塊，分別為可行性驗證及實證部分，內容為建置監察行動 APP 通訊軟體實驗平臺等偵查與分析平臺，研究如下：

建置監察行動 APP 通訊軟體實驗平臺，包含：行動 APP 通訊軟體實驗

平臺、行動 APP 通訊軟體監察技術實驗平臺、社群網路偵查暨鑑識技術實驗平臺、戰術型 WiFi 網路 APP 偵查系統規劃與驗證計畫、跨境戰術型 IP 通訊監察系統、行動裝置及其應用程式安全性分析運用雛型實驗平臺及提升新世代社群網路偵查暨鑑識能量計畫（建置雲端與 IP 定位資料保存規範機制實驗平臺）經由所獲之實驗成果技轉到建置偵查與分析平臺。

偵查與分析平臺，包含：社群網路偵查暨鑑識能量建置、遠傳電信、臺灣大哥大及臺灣之星 4G 後端通訊監察系統、網路封包分析、可攜式封包解譯系統等。

第六章、結論與建議：綜合前述各章節之研究，並以目前實務上在偵辦案件上所遇到之問題，以及各種因應措施提出研究結論，並經由研究成果提出理論貢獻與實務貢獻，最後針對本研究未盡部分提出建議，期使爾後案件偵辦人員在面對高科技犯罪之案件，不致綁手綁腳而能有積極之作為，同時彰顯降低犯罪率與提高破案率的目標。

第二章 文獻探討

本研究經過前述有關研究背景與動機的闡敘，並確定研究目的後，本章將針對與研究主題蒐集相關資料彙整文獻探討，以利進一步建構研究全形。本章內容依序為第一節高科技犯罪、第二節法規對行動通訊裝置 APP 執法之限制、第三節行動通訊進程、第四節如何以行動通訊裝置 APP 為犯罪工具、第五節創新技術因應以行動通訊裝置 APP 為犯罪行為與結合上述文獻探討彙整為本章第六節小結。

第一節 高科技犯罪

壹、何謂高科技犯罪

較易聯想到是電腦犯罪(Computer Crime)，但電腦犯罪只能稱為高科技犯罪之一種犯罪。完整說法應是利用科技的技術來遂行其犯罪行為。因這類型的犯罪行為並非僅是只使用電腦犯罪，也會使用到較特殊的高科技性電子產品，如行動通訊、數位的攝影設備，各種智慧卡(Smart Card)等。但因大多數案件其最後的處理平臺往往都會使用到電腦，所以這類型的高科技犯罪行為才會被大多數人歸類為電腦犯罪（王勁力，2010）。

貳、高科技犯罪的特性

網路和電腦通信科技的日新月異，具有「隱匿性、任意性、無特定性、間接性、高知識性」等的特徵，另包括具有「科技犯罪趨平民化」、「不知觸法無罪惡感」、「犯罪行為不易明察」、「證據難採易被銷

毀」及「逆蹤反查困難度高」等特性，因而使得警察單位偵查困難、破案不易，而且打破傳統犯罪需有加害人與被害人在時空（即犯罪發生的時間、地點）聚合的因素；而犯罪人付出的成本小、障礙低廉，但是卻常為獲得高報酬的犯罪所得吸引，使犯罪人趨之若鶩，加上其型態可以一直不斷隨著網路和電腦通信科技的發達而不斷更新，所以對於社會的影響層面快速的擴張，同時會提昇民眾的恐懼感，影響我國治安甚鉅。

有關高科技犯罪相關文獻彙整如下：

一、Leibowitz, W. R.(1999)高科技這種犯罪行為模式，是有科技背景存在，讓一些缺乏訓練的警務人員很難去偵辦這些高科技犯罪，其中有很大比例的網路型犯罪並沒有被發現到。

二、Rosoff, S., Pontell, H., & Tillman, R. (2002)多種形式的創新網路犯罪，已經在最近的這幾年紛紛出籠，這些網路犯罪類型不只是限於以下內容：盜版、身分盜用、金融犯罪、駭客行為、挪用公款和間諜活動等高科技犯罪。

三、Quayle, E., & Taylor, M.(2003)網路犯罪也包括生產和持有兒童色情製品，這類犯罪模式是高科技方式進行，對社會危害甚大。

四、Hinduja, S. (2004)為防制高科技犯罪，這些可以包括普通網路犯罪的工作隊，或專門任務部隊針對某些類型的特殊工作隊(例如兒童色情)。

五、Broadhurst, R. (2006)因為層出不窮的犯罪事件之後，一些的執法機關也成立了一些針對網路犯罪所設立的高科技特別的專案處理小組，這種作法對防制高科技犯罪是有積極作用。

六、Finkelhor, D., et al (2007)為了有效地調查和逮捕高科技罪犯，執法人員需要一些專業的培訓，且因為網際網路的特性，也對於警政單位形成了非常大的執法挑戰。

七、（美）米歇爾・紐頓(2007)飛速發展的現代科技是一把雙刃劍，給人類生活帶來了無窮便利，也給犯罪分子提供了新的犯罪手段。魔高一尺，道高一丈，高科技犯罪自從誕生那一刻起，執法機構運用高科技手段打擊犯罪越來越高明，因應這些犯罪行為，司法人員要有新做法。

八、Katos, V., & Bednar, P. (2008)之前的犯罪往往都只侷限在某個國家或者是地區，但在網路世界中無遠弗屆，可能犯罪的地點是在非常遠的地方，因此警政單位必須要學習新的知識與能力以面臨未來的挑戰。

九、馬進保(2012) 科技的進步帶動許多新科技產品的問世，行動手機是一種普及化的科技產品，而且已深入每個人生活中，因為不斷進步，人們已極度的依賴這類高科技產品，他帶給人們方便，但相對的也提供犯罪者運用為犯罪工具的機會，行動手機可以與電腦連線，可以相互互聯，更會造成執法單位辦案的障礙，這些障礙包含不易找到嫌犯真實位置與真實身分，犯罪預防與犯罪偵查

為司法人員職責，警察機關對於高科技犯罪技術的突破更應有具體做法與創新思維。

十、林俊峰(2009)拜現代科技進步之賜，商業交易模式愈加複雜，因此跨國洗錢犯罪行為亦隨之日趨嚴重，而洗錢不僅係黑錢漂白的工具，更是犯罪滋養的溫床，此從國內近年連續爆發的多起重大金融洗錢的案件所造成的危害，即可得知洗錢犯罪所造成嚴重性。尤其，近年來由於國際間恐怖攻擊事件頻傳，諸如在美國所發生的九一一事件及倫敦地鐵爆炸案等，因此如何從防制洗錢面，切斷資助恐怖分子之組織活動，更係美國及國際組織間之重點工作項目。科技為偵查插上翅膀，智慧乃是偵查之靈魂，現代化之科學技術能給偵查插上翅膀，使刑事偵查對犯罪事實之發現，能「觀之有形，聽之有聲，查之有據」，使犯罪者無所遁形。為了因應高科技進步所帶來之衝擊與效應，諸多法律的思考層面，便須跳脫傳統法學的思考方式，以便因應防制高科技犯罪之需求。

十一、張志欶(2012) 科技不斷的創新與進步，帶來更便利的生活方式，相對的高科技犯罪者常利用資訊網路與行動通訊等資通合流科技從事犯罪；高科技犯罪具有高度隱匿性、無國界和不易發現證據之特質，從而導致偵查機關破獲率偏低；面對高科技時代的來臨，偵查機關亦需以「運用高科技的力量，防制高科技犯罪」之前瞻性作為，提昇高科技偵查技能及加速培訓高科技偵查人才，將成為未來決戰犯罪之首要；唯有不斷推動與落實高

科技偵查工作，以提昇警察的整體犯罪偵查技能，始能達成維護臺灣科技化社會之治安任務。

十二、陳建舜(2011)當前我國高科技犯罪者多以電信、資訊網路資通合流科技犯罪，以藏匿行蹤方式從事不法之犯罪活動，危害社會治安甚鉅。政府有必要提供全面性的瞭解與說明，藉此探討為何造成網路詐欺犯罪有增無減之現況。

十三、左育丞(2012) Apple 公司所出產的 I Phone 即為最熱門的智慧型手機之一。然而，隨著科技的進步，使用者的科技水平提升，相對的也使犯罪者的手法隨之進化。當犯罪者使用智慧型手機做為平臺，透過高科技平臺的輔助進行犯意溝通的連繫或直接使用智慧型手機做為犯罪的工具時，如何從中發掘有效且關鍵的數位證據，協助數位鑑識調查與證據取證，將會是一大挑戰。

十四、王旭正(2013) 由於電腦與網路的快速發展和普及應用，依賴傳統證據為主的鑑識方法，已經不足以對抗科技導向的資訊犯罪案件，基於現今人們交流的資料大都已電子化，一旦稍有不慎都將導致資訊犯罪案件不斷出現。為了因應新型態的高科技犯罪，要具備電腦犯罪、網路安全、鑑識理論與數位證據偵蒐程序有相應之本職外，更應進一步對智慧手機、社交平臺與雲端存取實務的認識，期能在各種可能情境下，如何於不同的作業系統平臺(MOBILE OS/WINDOWS/UNIX/LINUX)，進行高科技犯罪的趨勢研究與數位鑑識。

十五、張謹名(2014)高科技的發展與電腦及網路使用普及，雖然帶給我們極大的便利,卻也出現了一些利用網路來從事犯罪行為之人，這些犯罪帶給人們的損害，較以往傳統犯罪更是為甚，學者之間便稱此類犯罪為「網路犯罪」。關於「網路犯罪」，因其多為利用電腦系統之操作進而連結至網路，近來更可連結到智慧手機，在網路進行犯罪之行為。

十六、陳瑞金(2015)「科技建警」、「偵防並重」是現階段警政署重要的治安策略，透過科技辦案，更能有效杜絕犯罪。並為因應新興科技犯罪，積極培訓科技人才，擴充軟硬體設施，強化情資分析整合能力，目標在於精進整體科技偵防能力，推動科技犯罪偵查專責隊法制化。惟如何實現「科技建警」、「偵防並重」之治安政策，整合刑警與科技，建立科技警察制度，積極培訓科技警察專業人才及提升犯罪偵查效能，將是警政革新暨網際網路良性發展的一大課題。

十七、賀宇才(2017) 21 世紀電腦網路科技的快速發展，資訊科技已普及到日常生活，各種行業對電腦資訊的依賴越來越深，隨著相關科技產業蓬勃發展，電腦已成為大眾普遍使用的工具。而資訊科技的建設與網際網路的高度應用，使得國內上網人數從 1996 年經常上網人口不到 60 萬人，10 年呈高度成長；資訊科技的到來，以及近年來電腦和網際網路的普及，不僅使竊盜、假冒、詐騙和色情等傳統犯罪有了新的型態，擁有新科技和新

技能的人數大幅成長，這更意味著更多潛在的高科技犯罪者。而高科技犯罪問題仍以網路犯罪為目前最為常見之犯罪類型案件。

高科技犯罪係相對於一般傳統的犯罪類型，或有直接稱其為非傳統犯罪類型，此犯罪類型行為的成立，包含有高科技技術的使用。而且隨著時代日新月異，高科技的技術逐漸發展與普及，除了受惠於一般大眾外，亦讓犯罪人受惠，使之得以有更多的工具與手法應用於犯罪行為上，不僅方便其犯罪行為的進行，同時亦提高偵查的困難度（梁哲賓，2019）。最常見遭利用於犯罪行為的科技技術為通訊及資訊兩種，前者包括電信、廣播電視、及衛星廣播等，後者則指電腦以及網路等，因此，高科技犯罪即指使用通訊與資訊技術於犯罪行為的新型態犯罪手法。

參、犯罪學觀點分析高科技犯罪與網路犯罪

從犯罪學的觀點來看高科技與網路犯罪的特性，發現有下述幾項特徵：

一、高科技與網路犯罪為智慧型犯罪。

二、高科技犯罪歹徒所需付出之成本及遭遇之障礙較為低廉。

三、高科技犯罪黑數（未經披露）常是不知情、被害人顧忌信譽、秘密、不敢報案...等因素。

四、兒童上網人數的大量增加及賭、色情、毒品或各類隱藏其中之犯

罪廣告、包裝過之犯罪資訊隨處可得，無法禁斷。

五、高科技與網路犯罪行為無明顯國界領域，犯罪行為與結果地廣泛，衍生管轄權問題。

六、缺乏執法機構合作機制，犯罪嫌疑人跨國合作，網路空間為重複犯罪的好地方。

七、具分散性、立即性、互通性、隱密性。

八、犯罪證據之偵查、及蒐證困難度高（例如網路加值語音服務 VOIP 或 P2P 之通訊聯絡方式）。

九、容易造成國家安全、社會安全一次性的重大損害（例如散佈網路病毒、駭客入侵或癱瘓網路運作等）或對個人生命、身體自由、財產上所衍生的危害。因高科技犯罪具有任意性、隱匿性及間接性特質，而資、通訊紀錄掌控於民間業者手中，加上警方偵查設備無法及時更新，往往造成員警偵查上的困難，因此其犯罪成本與障礙相較傳統犯罪類型低，但卻有高報酬的吸引力，使犯罪人趨之若鶩（張承瑞等，2010）。

肆、高科技犯罪大致分類（張承瑞等，2010）：

一、舊式的犯罪行為，這一類型犯罪屬於較傳統之犯罪行為，但還是有利用到新式電腦設備與網路等等高科技，以作為其犯罪之工具與媒介。例如使用信用卡詐欺、利用黑函勒索（如圖 2-1）、以網路聯繫援交等。

圖 2-1 勒索提示框

二、新式的犯罪行為，這一類型犯罪方式是以電腦設備與網路等等高科技為工具，對司法單位形成較大的困難與挑戰。例如以未經授權進入他人電腦系統、散播電腦病毒程式及阻斷服務式的攻擊（如圖 2-2）與竄改網頁等。

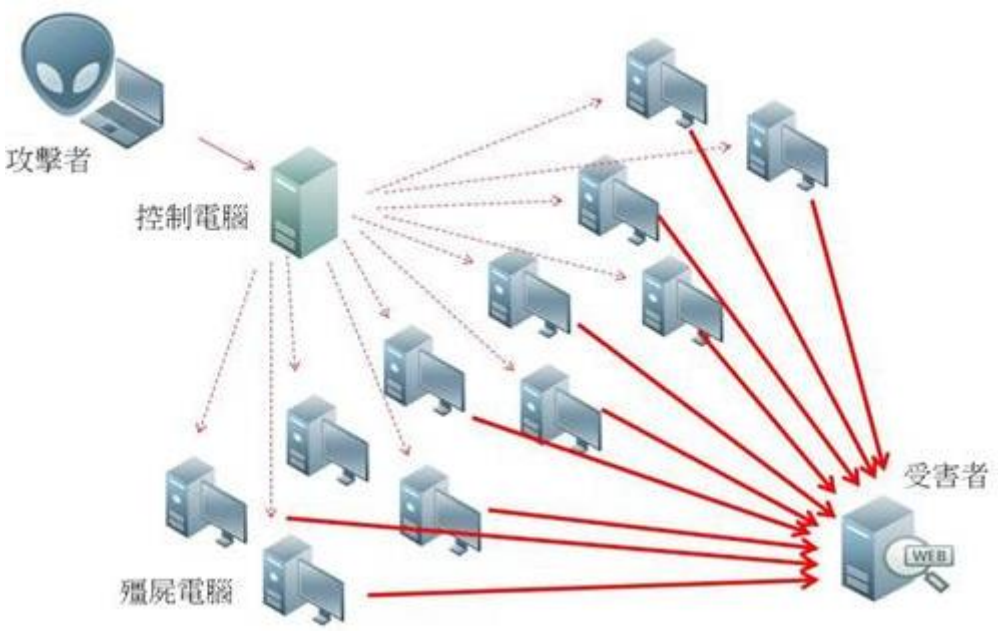


圖 2-2 dos 阻斷服務攻擊
（資料來源：淩群電子報）

伍、國內外高科技犯罪情形

高科技犯罪行為往往以網路作為其通訊傳輸媒介，並利用網路無實體國界之分的特性，同時因為網路具有高度的匿名性。犯罪者很容易將本身的真實身分與犯案所在地，予以隱藏在不容易察覺的無形網路後（陳子雄，2010）。

在網路犯罪行為之範圍，是可以用國際與國內作區分。國際犯罪之領域，需要各個國家之執法單位間共同偵辦，國內犯罪則需要本國司法人員與相關業者共同合作合力偵辦才能有效達成破案目標。

第二節 法規對行動通訊裝置 APP 執法之限制

壹、相關專家學者對行動通訊裝置 APP 執法見解

一、林天福(2011)警察查證新興詐欺犯罪利用各種通訊科技及金融服務，藉由運用人性心理的弱點，結合當前時勢，創造各種虛擬情境，不斷翻新詐欺模式，讓民眾防不勝防，亦讓政府相關部門疲於奔命。對詐欺犯罪的組織與分工、犯罪特色及犯罪模式作為，司法單位有必要積極偵辦，而法令規章更應該適時修改以做為辦案人員辦案之依據。

二、Todd G. Shipley(2014)即時通訊軟體、IRC(Internet Relay Chat)、FTP(File Transfer Protocol)和聊天室多使用主從式架構。主伺服器具有連結數個使用者之功能，當用戶加入連結，主伺服器通知其他用戶有人傳送連結，使雙方可以連結。但即時通訊軟體亦有使

用點對點連結方式(P2P)，但僅限於傳送檔案時，雙方得使用軟體直接連繫對方，無須透過伺服器，但點對點連結方式，會曝露雙方之 IP 地址，且每一通訊軟體公司均有其獨立通訊協定，因此不同公司之通訊軟體間無法互傳訊息。即時通訊軟體係藉由用戶登入訊息伺服器或是登入用戶端之電腦或手機運作，當訊息伺服器確認用戶之聯絡人名單，回傳聯絡人何人已登入於伺服器中，用戶選擇聯絡人後告訴系統連結聯絡人，雙方即可互傳訊息，但法令對犯罪行為卻無明確規範。

三、黃茂穗(2014)在行動通訊裝置 APP 犯罪偵防衝擊與預防策略部分，發現行動通訊裝置 APP 對犯罪偵防的困境在「缺乏規範」問題，由於行動通訊裝置 APP 的便利及匿名性，加上行動通訊裝置 APP 在法律未有明確規範，欠缺有效管理機制且權責主管機關不一，更有行動通訊裝置 APP 提供者設於境外所衍生的管轄權等問題，致使偵查單位無法發揮有效的防制作為，遂導致行動通訊裝置 APP 淪為犯罪集團的利器。

四、王晴玲(2015)APP 發展一日千里，因應使用者需求或是軟體程式錯誤修正，手機通訊軟體不僅需推陳出新，連舊軟體亦不斷更新。為監察而破解應用程式往往緩不濟急，且偵查單位花費人力、物力破解應用程式後，程式又再更新，形同所有努力付諸流水。且通訊軟體數量驚人、發展蓬勃，而通訊監察建置機關有限，通訊軟體實為現在實務上通訊監察之漏洞。所謂加密係指雙方在進行

網路通訊時，使用相同資料編碼加密和解碼規則。當寄送方將訊息傳送出去，該訊息被內建之加密規則予以編碼，收受者因具有相同解碼規則之裝置，在接收訊息時，自動將加密之訊息解碼，因此收受者得以閱覽訊息，但第三人之裝置內因不具備同一編碼設置，縱然截收到訊息，仍是一堆亂碼。對於加密之行動通訊裝置 APP 犯罪案件之偵辦，已造成辦案人員困擾，追根究底在於法令增修跟不上時代。

現今軟體開發商為保護通訊安全，且運算功能提高，為軟體加密輕而易舉，是通訊軟體多以加密方式傳送。以往電信業者依通訊監察及保障法第 14 條，對於執行監聽有協力義務，提供解密金鑰，然而目前國外軟體商並不願提供解密金鑰，一來此舉將降低民眾使用其軟體之意願，另一方面，我國通訊保障及監察法對軟體商是否有強制力，仍有疑義。

五、王旭正(2016)智慧型手機的普及，及無線網路技術的成熟，生活中的工作及食衣住行育樂等各項活動，皆與其脫離不了關係，且近年來行動通訊軟體發達，讓手機成為人與人間通訊的主要工具，聯繫的方式，也從電話、SMS 訊息，逐漸變成各種即時通訊軟體，如 LINE、WhatsApp、FB Messenger、Skype、WeChat、U 通訊等，這些通訊軟體除可傳文字訊息外，亦可傳送圖片 、語音訊息等，使得各類資訊快速流通。然而新型態的高科技犯罪，隨著這波科技潮流快速發展，智慧型手機通訊軟體及通訊聊天等訊息之犯罪

行為進行研究,除針對手機日誌檔內容的萃取判別外,並利用 ADB 備份工具、Cygwin、 SQLite Database Browser 等 OSINT 工具，對聊天紀錄內容進行備份、解壓縮、資料庫分析等工作，可提供第一線調查人員快速度找出其手機使用行為，證明其與交通事件或犯罪行為之關連性。但對加密應用軟體的偵辦，無法解密是重大難題，法令應適時修正。

六、張雅昕(2016)許多的即時通訊軟體陸續推出電腦版的版本，讓使用者能在手機上與電腦上使用，形成多樣化的使用方式，而藉由即時通訊軟體在網路間的傳遞可能存有潛在的犯罪，犯罪者可能透過通訊軟體互相聯繫談話或直接透過通訊軟體進行網路犯罪的行為，而警察人員進行偵辦網路犯罪時，可以檢視即時通訊紀錄是否有不法之證據，這些可能成為重要的數位證據，協助案件之偵查。法令如未有明確之規定，案件恐將無法持續偵辦。

七、黃逸玲(2018)行動通訊裝置 APP 問世，確實為用戶帶來便利性，也取代過去僅以手機、市話之傳統語音通話及簡訊作使用，且於實施犯罪偵查時延伸另一個難題，主因是近來行動通訊裝置 APP 引來犯罪者覬覦，被運用為犯罪工具，成為現今許多犯罪型態的溫床，以致於逐漸成為讓犯罪者躲避警方追查犯罪的一項利器。目前礙於我國實施監聽時，倘若察覺受監聽對象可能藉由行動通訊裝置 APP 撥打網路語音通話或傳送文字訊息，作為雙方聯繫管道，仍無法對其做後續追查及蒐集犯罪事證；對現今多數犯罪者

以轉移利用起行動通訊裝置 APP，從事犯罪行為，偵查中並非毫無察覺，國內受限於對此實施犯罪偵查及行動通訊裝置 APP 業者協助義務並無明確法規規範，偵查人員該如何偵查及無從取得國外通訊裝置 APP 業者協助，都成為現階段問題所在，相對之下，對熱心辦案之偵查人員而言， 將面臨無計可施的困境。

從現有實施監聽或案件偵查中感受到犯罪者已轉移至行動通訊裝置 APP，歷經該過渡時期，常於辦案時遭逢此問題，仍舊有種無力感，惟有從現今偵查困境，找出因應對策才行；所以本文研究欲從行動通訊裝置 APP 發展趨勢做為開端，就偵查現況、隱私權保障、法律之不足...等方面做延伸，歸納實務上之偵查困境，再就行動通訊裝置 APP 偵查之困境比較檢討，呈現國內法制面與技術面之不足，尋求因應對策，作為未來修法及實務偵查之參考，讓偵查人員能有所依循，不再手足無措，錯失破案機會。

貳、法令的規範

一、蘇三榮(2012)通訊隱私為隱私權之其中一個面向，對通訊隱私之定義為：是對個人領域的私人通訊事務之控制權。詳言之，其主體為個人，客體為私人通訊事務，作用則是控制。首先，所謂個人應指自然人，通訊保障及監察法第 4 條規定：本法所稱受監察人，除第五條及第七條所規定者外，並包括為其發送、傳達、收受通訊或提供通訊器材、處所之人。因為僅有自然人方能憑藉自由意識，與通訊相對人溝通、傳遞訊息，做意思交流。而法人僅為法

律上擬制之人格，無機關之輔助即無法發出訊息。縱以法人名義和他人通訊，須由自然人代為之，實際上仍是自然人之通訊。

二、調查局(2014)行動通訊軟體屬電信業務範疇，其應以電信相關法規管理，無需疊床架屋另立新法，但因現行電信法規陳舊，致使行動通訊裝置 APP 業者未納入第一、二類電信業者管理，導致行動通訊軟體業者雖是電信相關行業，卻不用受電信法規規範，在法源上無法令規定需提供解密方法，無法由電信法管理，自然無法以通保法所規範要求業者配合司法機關，目前僅能以協商等方法向業者索取資料，故唯有修法將行動通訊軟體業者納入電信法規管理，才能從根本解決現有困境，讓行動通訊軟體可依電信法規定，要求行動通訊軟體業者配合司法機關進行通訊監察，若有廠商拒絕配合司法單位實施通訊監察，將可依電信法規處罰違法廠商。

三、傅美惠(2014)我國憲法第 12 條規定人民有秘密通訊之自由，即係指人民對於通訊之內容甚至對通訊之雙方擁有保密，不必向國家機關告知之權利。通訊之秘密，係屬國民隱私之重大權益，故憲法明文加以保障，使國民間以書信、電話、電報或利用電子網路為傳遞、接收通訊之活動，不受開拆、檢閱、監聽或截取等不當之干涉及介入。特別是從保障言論自由之觀點，秘密通訊是傳達、表現言論及思想之重要管道，故通訊自由之保障，實質上亦可達到確保言論自由之目的。

因此，利用電話等通訊設備所為之通訊秘密，直接受到憲法第 12 條之保護，以電訊截收的通訊監察行為，顯然干涉國民秘密通訊之自由，應無疑義。憲法第 12 條既然明文保護人民有秘密通訊之自由,則國家機關運用各式各樣之方法介入人民間之秘密通訊時，即是對於人民之通訊權有所侵害，但並非謂國家機關對此種權利不能侵害，亦即此種秘密通訊權仍有其保障之限制，惟應符合憲法第 23 條之規定。故凡國家對涉及個人資料之取得、儲存、處理與傳遞，即使在不為人所知悉之情況，因客觀上已造成對私人資料之除隱私權化及對該除隱私權化之持續化，皆應得到法律之授權及限制。

四、王晴玲(2015)隨著資訊科技進步，為查緝犯罪所需，在技術上得採取之偵辦手段經緯萬端，像植入木馬程式、後門程式即為一例。惟當執法機關以駭客手法取得犯罪證據,固然在技術上不成問題，惟在現行法之框架下，仍需進一步思考。

參、其他牽涉案件偵辦規範

一、第 1、2 類電信的區分

電信法第十一條：「電信事業分為第一類電信事業與第二類電信事業，第一類電信事業指設置電信機線設備，提供電信服務之事業...，第二類電信事業指第一類電信事業以外之電信事業。」，上述條文已說明只要具電信機線設備（含基礎之設備等，如有線傳輸網路以及無線電頻率與衛星等）可提供用戶之通訊服務即是

屬第一類電信，而第二類電信是要向第一類電信事業者對其要有租用電信之機線設備的業者，並以提供公眾通信服務者；而第二類電信業者其在第二類的電信事業管理的規則內又將其服務再分為一般業務及特殊業務，至於本研究是要對特殊業務中之網路電話的服務作探討，因為其通訊方式與行動通訊裝置 APP 之網路的語音通話較相似，是可區別。

二、真實的 IP 模式及虛擬的 IP 模式

近來常有發現犯罪之嫌疑犯，已經不再使用傳統的通訊做為其犯罪之聯繫，而是另尋其他的通聯方式，藉以規避查緝，以目前所遇到狀況，嫌犯較偏向以第二類電信使用之網路電話為其犯罪連絡之通訊，這種方式是以網路電話支援有類比訊號傳送之聲音，轉換為數位訊號傳送，是以數據封包方式重送的，經過 IP 在網路上傳送，是由網路協定傳送，又可歸類為以網路電話互打，與使用網路電話撥給傳統電話。

在探討利用網路電話方式打給網路電話之互連狀況下，所保留的通信紀錄為研究重點，不討論以網路電話與傳統電話之聯繫行為，有關網路電話之互連兩者間之發送與接收，都是以網路進行傳送，受話者亦以經由網路將其數位程式接收聲音的訊號，這種方式稱為真實的 IP 模式及虛擬的 IP 模式，兩者間差異在於應用的網路電話屬真實 IP 或是虛擬的 IP 之差別而已，至於真實 IP 的模式是在用戶兩者間建一網路的聯繫電話，但是封包的訊息資料是不會經由二類電信的伺服器的，目前我國網路電話又可分為軟

體式的網路電話及硬體式的網路電話，與本研究議題相關者為偏於軟體式的網路電話的行動通訊裝置 APP 問題探討，因為其特點在於不必購置實體使用的網路電話，只要將軟體安裝在電腦就可以使用，Skype 為在國內較早被使用的軟體，跟目前時下流行使用的行動通訊裝置APP的狀況相似，該軟體除了可以安裝在電腦上，亦可安裝在智慧手機以及平板上。

三、第 1、2 類電信業者對辦案協助

經查過去國內司法人員在辦案時，申請之通訊監察種類其所占申請數最多為市話與行動電話門號，第二為行動通訊的國際識別碼，第三為網路電話帳號，也就是俗稱的 Skype 帳號，這也代表國內過去的通訊監察的範圍涵蓋網路電話 Skype 帳號，經司法院在民國 103 年至 105 年間法院辦理通訊監察的案件統計，得知其所占申請監察狀況有成長(黃逸玲，2018)。

依電信法第十一條規定，「Ⅰ…。Ⅱ第一類電信事業指設置電信機線設備，提供電信服務之事業。Ⅲ前項電信機線設備指連接發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備、以及二者之附屬設備」。以目前司法單位在偵辦案件如有需對行動通訊裝置 APP 實施監聽，如欲採架設方式以代理伺服器之(Proxy Server)實施攔截封包，其與第一類電信業者之機線的設備，包含發、受之兩端的網路傳輸之設備、交換設備與其附屬設備均有相關性，確有獲得第一類電信之業者協助的必要，例如：中華電信、遠傳電信…等，因此辦理這類案件時與國內相

關電信業者聯繫仍然是重要的。

目前第一類電信業者只剩下固網通訊與行動電話業者，亦即是架設實體線路之固網與實體的無線電的基地臺，其所經營的電話或是經營網際網路的相關業務的業者；另外第二類電信因其並非架設實體的線路的固網或是擁有實體無線的基地臺，因此第二類電信業者需要向第一類電信業者租用固網的基地臺，或無線基地臺的門號或是頻寬用來經營本身電話或網際網路之業務，例如使用 Seednet 之無架設本身的固網，卻是要向中華電信公司租用固網頻寬經營本身的網際網路之業務。

因應行動通訊裝置APP的通訊，擇要透過網際網路始能運作，也因為過去電信網路所使用的語音通訊服務多為實體層的 Bearer Service，即是基本的電信服務。為了提供這項服務有必要架設 Circuit Switch 為電路交換的設備與實體線路，藉以連結兩個戶端之電話，這種架構方式是符合國內電信法之對於第一類電信事業所下的定義。但是考慮到 Internet 的服務或另外的分封式交換電路的網路服務，則是使用 OSI 之通訊協定所規範的第三層之上，因其架構之設置為分封式的交換設備，為數據電路的終端，網路架構上符合國內電信法之對於第二類電信所下的定義，其服務又被稱之為加值型的服務。

四、國家通訊傳播委員會對第一類及第二類電信與即時通訊軟體界定

國家通訊傳播委員會（簡稱為通傳會或 NCC）特別針對即時通訊軟體（也包含行動通訊裝置 APP），表示只提供網際網路的基

礎服務，但實際上即時通訊軟體並非電信法上的第一類與第二類電信。通傳會卻在民國 106 年 3 月份函知高檢署，並敘明行動通訊裝置 APP 所使用之即時通訊軟體，或一般社群軟體其通訊方式，本質上即是使用者在利用行動通訊裝置 APP 的開發商家提供的「資訊服務」，以進行資訊的聯繫，無需向通傳會申請其電信經營的執照，因此通傳會是無法實施監理與管理上的工作；通傳會在電信事業技術之可行的範圍，有義務配合通訊監察建置機關建置其所需的系統，但是行動通訊裝置 APP 之開發商其運用的通訊軟體是網際網路，電信業者因其所提供的服務是最底層之「通訊服務」，所以雙方間是有區別的，因此第一類及第二類電信與即時通訊軟體是有區別的。

肆、以行動通訊裝置 APP 為犯罪工具案件偵辦之新挑戰

目前通訊方式亦與時俱進，早期的犯罪方式其犯罪之聯繫大都是利用市區電話或行動手機電話通話，過去國內對這類的犯罪並無法律上的規範，造成司法人員在辦理詐欺與販毒等案件有諸多障礙，為解決這類問題，經多方努力直到通保法與電信法的立法之後，司法人員在辦案時才獲得法令的支援，在實施犯罪的偵查時較不致礙手礙腳。

對辦案人員而言，有許多案件並非破案就結案，其原因是有很多狀況須為追根究底要向上溯源，例如以毒品案件的偵辦，往往要耗費相當多的時間對毒品來源探究其源頭與其參與犯案同夥之關係，並追查通聯，這些工作甚為重要，對於嫌犯以市話或是行動手機做為其犯罪之連結，案件偵辦過程中如實施通訊監察時，蒐證到的資訊只侷限

在雙方的語音通訊內容，以及使用者資料跟雙方的通信紀錄，這在民國 103 年前 4G 通訊未商轉前對辦案還未造成重大困擾，主要原因在於傳統 2G 與 3G 的通話方式是經由線路交換來做為傳送，雙方互為聯繫的資料，最後都存放犯罪者各自使用的電信業者，像是通信使用者資料以及通信紀錄，都是可以事後經由向各相關的電信業者來調閱取得。

經由上述之敘述得知歹徒通話只要合法並以正常法律程式向電信業者調閱相關資料即可，犯罪的歹徒間之通訊內容是不會存放在電信業者資料庫，但是因為資料是經過線路交換傳送的，司法人員在偵辦案件時需對某一嫌犯之通訊內容實施監聽時，必須經過合法的法律申請程式，向法院聲請案件之令狀經核准之後，才可經由電信業者由租用之各家業者的線路介接通訊監察的機房，再對監聽對象實施現譯並錄製通訊監察光碟，藉以蒐證保全。

國家通訊傳播委員會在民國 102 年開放行動寬頻之 4G 釋照標售給國內各電信業者，當時由六家的電信業者所得標，包含中華電信、臺灣大哥大、遠傳電信、國基電子、亞太電信與臺灣之星移動電信等公司。4G 商轉前逐步退回過去的通訊世代，分別是 3G 與 2G，惟自民國 102 開始 4G 商轉後，行動通訊裝置 APP 因方便性前所未有，所以業者對這類軟體開發出來的種類也不斷增多，雖然目前許多的行動通訊裝置 APP 開發商其公司都在國外，發話及收話之兩端都是走網際網路，以封包傳輸來做為通訊方式，對於嫌犯使用行動通訊裝置 APP 之網路語音的通話或是以文字做為犯意的溝通管道，雖然以行動通訊裝置

APP 作為通訊之聯繫會留下犯罪跡證，但是以封包傳送方式與以傳統語音傳送是不同的，重點是封包需要解譯且需要先攔截封包再進行解密與讀取，至於案件偵辦人員對於涉及有關行動通訊裝置 APP 之案件可否偵破，則有賴於偵查法令規範、辦案程式，以及破案技術...等問題獲得解決。

第三節 行動通訊進程

壹、行動通訊的世代演進

近代之行動通訊發展基礎就是以「數位通訊」的技術在演進，不論是第三代(3G)或第四代(4G)，甚至未來的第五代(5G)通訊，都是以更複雜的數位訊號調變技術來增加資料傳輸的速率，讓連線上網更快速方便（曲建仲，2015）。

一、訊號數位化

環境中的所有資訊，包括我們聽到的聲音、看見的影像、皮膚感受的觸覺、電腦儲存的資料，以及手機傳送的訊息等，都是一種「訊號」，人講話的聲音是連續的，因為聲音可能是漸漸變大或漸漸變小。產生連續的電壓變化，這種「連續的訊號」為類比訊號(Analog Signal)。大自然裡一切的訊號，包括聲音和影像，都屬於類比訊號。

而經由加工處裡以後，可以將連續的類比訊號變成「0」與「1」兩種不連續的訊號，就稱為數位訊號(Digital Signal)。例如電腦在

運算時，就只有低電壓（0V 代表二進位的數字 0）與高電壓（1V 代表二進位的數字 1）兩種情況，訊號可以由 0 直接跳到 1，也可以由 1 直接跳到 0，得到的是一個不連續的電壓變化，這種「不連續的訊號」就是數位訊號。目前所有電子產品裡的處理器都是使用數位訊號來進行運算（曲建仲，2015）。

將類比訊號轉換成數位訊號的過程就稱為訊號數位化(Signal Digitization)，不論那種類比訊號數位化以後，都只剩下 0 與 1 兩種訊號。

二、類比通訊

類比訊號的調變就是俗稱的「類比通訊」，包括傳統電話、類比收音機(AM & FM)、類比無線電視、無線對講機，甚至早期我們所使用的第一代行動電話，俗稱「黑金剛」，體積堅固碩壯，兼具通訊與「防身」的功能，這些都是我們使用將近一個世紀的通訊元件。

類比通訊的缺點

以 AM 無線通訊為例，其設備都會有天線與功率放大器，傳送端訊號會先經由放大器將訊號放大，再經由天線傳送，經數十公里後訊號會衰減，且因建築物反射或繞射產生雜訊；當接收端收到後，會經由功率放大器將訊號放大，同時連雜訊也一起放大，造成訊號失真（如圖 2-3），這是類比通訊最大的缺點。

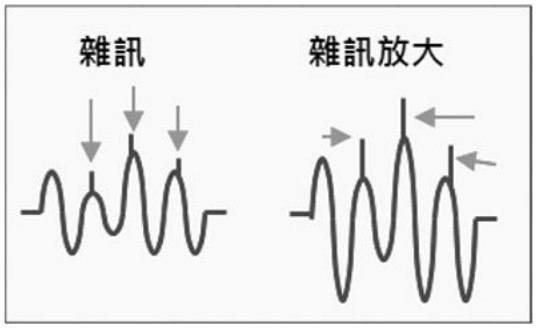


圖 2-3 類比通訊雜訊波

三、數位通訊

數位訊號的調變就是俗稱的「數位通訊」，包括 2G 行動電話、3G 行動電話、4G 行動電話、無線式行動電話、無線區域網路、數位電視等，數位通訊是未來的趨勢。

數位通訊的優點

其優點是容易校正、可偵錯與除錯、加密與解密、壓縮與解壓縮等。數位訊號調變的電磁波在傳送的過程中若因干擾產生雜訊，很容易經由校正將雜訊去除（如圖 2-4）。以 ASK 無線通訊為例，因訊號只有 0 與 1 兩種，所以接收端只要接收到的電磁波振幅小於 50%則判斷為 0，大於 50%則判斷為 1（這種技術為校正）。

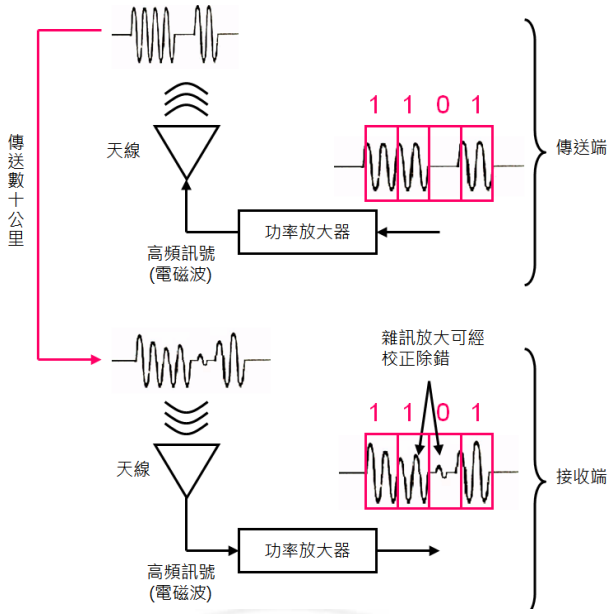


圖 2-4 數位通訊傳送與接收

四、通訊傳輸速度持續加快

依電磁波的理論 $C = f \cdot \lambda$ ，其中 $C = 3\times10^{8}$ m/sec 是光速，f 是電磁波的頻率，λ 是電磁波的波長。電磁波的正弦波形，會同時隨時間與空間改變震盪形狀，並以接近光速的速度往前傳播。頻率 f 是指電磁波在一秒內完整震盪次數，震盪次數越多代表頻率越高。λ 則是電磁波在空間上一個完整震盪的長度，f 與 λ 恰巧成反比，f 越高 λ 則越短。按通訊技術後如果 f 越高，則每秒調變在載波上的資料串就可以越多（顏春煌，2008）。所以 1983 年第一代行動通訊(1G)系統的載波頻率 f 是 100000000 赫茲（八個零），而 2020 年第五代行動通訊(5G)系統的載波頻率 f 會是 10000000000 赫茲（十個零），這意味 5G 系統的載波頻率整整比 1G 系統的載波頻率，足足提升了一百倍。

科技技術目前已經能將網際網路與行動通訊裝置有系統的結

合，同時進步到以語音經由網路來通話的功能，這種方式是以封包傳送的，是用以取代過去的傳統語音通話的一種新科技技術，目前行動通訊是以第 4 代 4G 行動通訊為主，因經過多年的市場使用且不斷的精進，其系統已相當穩定，而且傳輸速度亦符合消費者需要，有關第一代至第五代行動通訊的演進（如表 2-1）略述如下。

表 2-1 從 1G 到 5G 的技術參數

名稱	電磁波頻率（載波頻率）	啟用年	資料傳輸量
第一代行動通訊，1G(1st Generation)	150MHz(1.5×108Hz)	1983	類比式行動電話系統。
第二代行動通訊，2G(2nd Generation)	450MHz(4.5×108Hz)	1991	數位元系統，語音+文字簡訊。 靜止資料傳輸速度 40Kbps (4.0×104 bits/sec)
第三代行動通訊，3G(3rd Generation)	1900MHz(1.9×109Hz)	2001	數位系統，語音+圖片。 移動資料傳輸速度 144 Kbps (1.44×105 bits/sec） 靜止資料傳輸速度 2 Mbps (2.0×106 bits/sec)
第四代行動通訊，4G(4th Generation)	2600MHz(2.6×109Hz)	2009	數位系統，語音+影片。 資料傳輸速度：1000 Mb (1.0×109 bits/sec)
第五代行動通訊，5G(5th Generation)	28GHz(2.8×1010Hz)	2020	數位系統，語音+影片+物聯網。 資料傳輸速度：20 Gbps (2.0×1010 bits/sec)

第一代行動通訊（稱為 1G）：是一種類比式的系統，無法做資料傳輸，只能以一般語音作傳輸服務，為蜂巢式的系統，將傳送的聲音以調頻的方式變調，但是這種的保密性不佳（賴柏洲，2016），如第三者欲接收其通話內容調整與其相同頻道，即可竊聽或予以電波干擾，第一代行動通訊起源於西元 1980 年代，為藉由雙方之間建立一專線通訊方式通訊，這種方式是採用線路交換的。

第二代的行動通訊系統（稱為 2G）： 有關行動網路通訊在早期開始於類比之通訊技術，惟自第二代行動通訊(2G)開始有變化，就是進步到以數位應用的通訊技術，稱為 GSM 系統。其發展自西元 1992 年之後，因為類比的系統已經演變成了數位系統，其進步幅度已由較先進式的行動電話的服務以及全球的應用行動通訊系統以及分碼多重之擷取系統的連續進步程式，並且可以提供包含語音以及數據跟傳真等等的服務以及其他附屬服務，這些均有高度通訊的保密特性以及增加容量在傳輸速度上，並且已經可以有效的傳輸在數位的資訊，其主要是採用了 2 種的包含 TDMA 以及 CDMA28 的技術，已經不是應用第一代的類比之通訊可支應，而是一種數位式的通訊，其上網傳輸之速度在臺灣 GSM 之技術架構下已經開發 900MHz 和 1800MHz 兩個使用頻段，但是仍無法使用封包之交換模式傳輸語音通訊，以致第二代行動通訊依然是使用線路交換的方式；另因 GSM 上網將帶來高費用以及傳輸數據之速度變慢，演進到以封包為傳輸基礎 2.5 代新通訊技術，其速度高達 171Kbps，是使用上傳與下載之封包量來作為其計價之

標準。

第三代及第四代（稱為 3G 及 4G）行動通訊之發展：第三代(3G)的行動網路，其傳輸量已由上一代的 40kbit/s 提升到 30Mbit/s 左右，有將近千倍的成長。3G 在西元 1996 年以後發展，有第二代功能以及服務，能提供高速率的資料之傳輸頻寬以及多媒體服務，並先開發了可在未來使用之公眾陸地的行動通訊系統，以 IMT-2000 提升無線接取(Wireless Access)技術，提高通訊產品之相容性，與高通訊品質等，具 2Mbps 之封包(Packet)的數據傳輸速度與可傳送語音以及數據與影像、多媒體、和使用在網際網路上之各種服務。

另第四代 4G LTE 行動網路，實體層傳輸之速度提升到 150Mbit/s。使用 LTE(Long Term Evolution)技術，在資料碼與傳輸上，都是使用先進的技術，可調配傳輸量至不同使用者，讓傳輸之效率更高（楊家驤，2015）。

行動通訊的 3G 及 4G 出現的時間雖然有先後的順序，但同屬於數位式的通訊，其語音通訊是採行了封包傳輸，並非傳統線路交換可完成，在第三代的行動通訊在數據傳輸之速率上較第二代更快，其平均速率在 300kbps 以上，並以 CDMA 的技術發展，目前市面上的 4G 手機及通訊 APP 均結合成為行動通訊裝置 APP，經過其用戶以網路使用網路語音的通訊或文字訊息來傳送，與傳統手機通訊的蒐證模式。

從 3G 演進到 4G 後，使用者感受到最明顯的差異就是速度，

資料下載的速度會變快很多，觀看線上影音資料時也不會感受到延遲(Latency)的現象。代表雲端系統的運用會更加普遍，因不管是將資料備份到雲端資料庫，或是使用雲端軟體，使用過程都更加順暢，包括最新的擴增實境(Augmented Reality)科技或是手機互動遊戲，在生活與休閒應用上開啓了更多的可能性。這代表了雲端系統的運用會更加普遍，因為不管是將資料備份到雲端資料庫，或是使用雲端軟體，使用過程都會更加順暢，讓使用者感受更輕鬆愉快，包括最新的擴增實境(Augmented Reality)科技或是手機互動遊戲，在生活與休閒應用上開啓了更多的可能性（蔡志宏，2014）。

目前 4G 仍面臨著一些尚未排除的問題，第一個就是頻寬。在通訊科技中，頻寬是個很重要的關鍵，由於目前尚有很多條線道被 2G 的電信業者所承租，無法被 4G 科技所利用，造成頻寬仍然不夠（陳志仁等，2015）。

五、未來 5G 科技的發展

5G 與 4G 相比概念是連線容量有提升，由仰賴物聯網的需求而建設成形。屆時所有物品之間的連結均可容納。下一代行動網路聯盟(Next Generation Mobile Networks Alliance)定義了 5G 網路的要求（維基百科，2019）：

（一）、以 10Gbps 的資料傳輸速率支援數萬用戶；

（二）、以 1Gbps 的資料傳輸速率同時提供給在同一樓辦公的成

員；

（三）、支援數十萬並發連接以用於支援大規模傳感器網路的部署；

（四）、頻譜效率比 4G 顯著增強；

（五）、覆蓋率比 4G 提高；

（六）、信令效率得到加強；

（七）、延遲顯著低於 LTE。

下一代行動網路聯盟認為，5G 應會在 2020 年陸續推出，以滿足企業和消費者的需求。除了簡單的提供更快的速度，預測 5G 網路還需要滿足新的使用案例需求，如物聯網（網路裝置建築物或 Web 存取的車輛）、廣播類服務，以及在發生自然災害時的生命線等。

（一）、5G 將採用 512-QAM 或 1024-QAM 更高的資料壓縮密度調變/解調變器，目前 4G 使用 256-QAM 或 64-QAM 的調變以壓縮傳輸資料，因此頻譜效率每 Mbps/100MHz 的利用效率更高，提高更多傳輸速率。

（二）、5G 將採用 28GHz 毫米波通訊，比如目前 4G 使用 700MHz、900MHz、1800Mhz、2600Mhz 等低頻段，雖然電波繞射能力比較高，但是在低頻上頻譜資源卻相當有限，在高頻的毫米波大多是軍用戰鬥機雷達或測速照相等少數裝置，

頻譜寬度更高，而且更容易找到連續頻譜，使空白頻譜非常容易取得。

（三）、波束指向配合多輸入多輸出(Multi-input Multi-output ；MIMO)相控陣列天線，MIMO 多輸入多輸出利用電磁波的空間多工和路徑不同，多天線系統提高傳輸速率，類似在軍用領域的技術，將延伸出商用技術版本。

（四）、波束自適應和波束成形，能夠提高特定方向的波束至最佳化傳輸距離。

（五）、新材料將使用 GaN 氮化鎵或是 GaAs 砷化鎵材料的 RF 射頻天線和功率放大器，此材料的 RF 射頻天線能在更高的頻段有更高的能源效率，裝置會比較省電。

（六）、為了適應工業物聯網、無人駕駛汽車、商用無人機等新技術的應用，網路延遲時間將降低到 1 毫秒以下。

貳、行動通訊裝置 APP 發展

一、行動通訊裝置 APP 使用情形

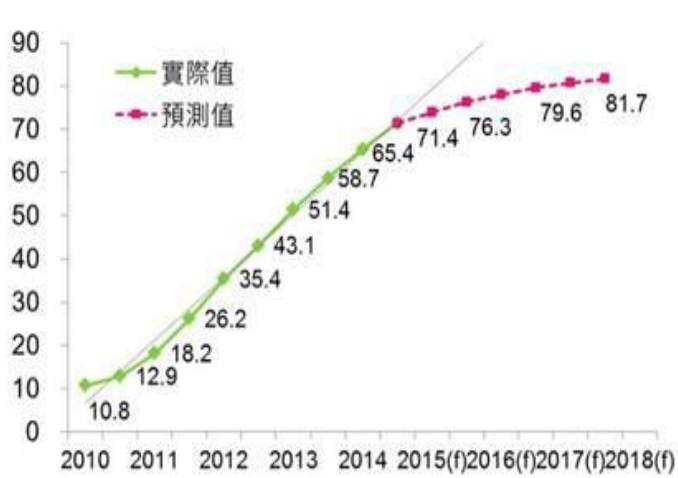
APP 是英文 Application 的簡稱，也就是應用的意思，泛指智慧手機的協力廠商應用程式，也就是類似於平時我們電腦上的應用軟體。比較著名的 APP 商店有 APPle 的 I Tunes 商店，Android 的 Android Market，諾基亞的 Ovi Store，還有 Black Berry 用戶的 Black Berry APP World，以及微軟的應用商城(APP-Mba 智庫百科，

2019)。

過去的即時通訊為電腦系統提供使用者一種專用服務，但隨著資訊普及以及網路流通方便，即時通訊成為溝通的主要管道之一，並在 2003 年以後與電子郵件和全球的資訊網路共同為網際網路使用主流，在 2008 年因智慧型手機已普及，傳統使用 SMS 及 MMS 資訊服務也被協力廠商服務的網路架構所取代，同時開始有行動通訊裝置 APP 的出現，但因為開發地區的不同，在發展行動通訊裝置 APP 的種類也不同。

行動通訊裝置 APP 的崛起是近幾年最熱門話題，但是增長速度並沒有放緩，且活躍度越來越高。它們的功能已經擴展到電商、實體物品、虛擬物品、遊戲、支付等一系列十分龐大的產品線（陳月香等，2017）。

隨著行動裝置時代的來臨，持有智慧型行動裝置的人越來越多，個人電腦(PC)市佔率不斷下滑。目前各國的行動通訊裝置 APP 發展蓬勃，我國資策會在民國 105 年調查顯示臺灣持有平板電腦以及持有智慧手機的人數達到 1,004 萬人（創市際雙週刊，2016）（如圖 2-5）。



年度	普及率(%)	推估人口(千)
2010	10.8	2,296
2011H1	12.9	2,743
2011H2	18.2	3,870
2012H1	26.2	5,571
2012H2	35.4	7,527
2013H1	43.1	9,165
2013H2	51.4	10,712
2014H1	58.7	12,252
2014H2	65.4	13,549
2015(F)	71.1	14,799
2016(F)	75.3	15,798
2017(F)	79.6	16,498
2018(F)	81.7	16,918

圖 2-5 2010-2018(f)臺灣智慧型手機普及率發展趨勢及預測

根據 E Marketer 在 2016 年 9 月的估計，臺灣有 73.4%的人口使用智慧型手機。是亞太地區榜首。高於新加坡的智慧手機使用者有 71.8%，南韓的智慧手機使用者有 70.4%，美國的智慧手機使用者有 63.9%，中國的智慧手機使用者有 43.8%（如圖 2-6）。

Mobile Phone* and Smartphone Users in Taiwan, 2015-2020**

	2015	2016	2017	2018	2019	2020
Mobile phone users*	**19.7**	**19.8**	**19.9**	**20.0**	**20.1**	**20.2**
—% of population	84.1%	84.5%	84.8%	85.0%	85.3%	85.5%
—% change	1.0%	0.7%	0.5%	0.4%	0.5%	0.3%
Smartphone users**	**16.4**	**17.2**	**17.8**	**18.3**	**18.6**	**18.8**
—% of population	69.9%	73.4%	75.8%	77.6%	78.9%	79.9%
—% of mobile phone users	83.1%	86.8%	89.3%	91.3%	92.5%	93.4%
—% change	8.3%	5.2%	3.4%	2.6%	1.8%	1.4%

*Note: *individuals of any age who own at least one mobile phone and use the phone(s) at least once per month; **individuals of any age who own at least one smartphone and use the smartphone(s) at least once per month*
Source: eMarketer, Sep 2016

215560 www.eMarketer.com

圖 2-6 2015-2020 臺灣行動電話及智慧型手機普及率發展趨勢及預測

在使用行動通訊裝置 APP 上則以 LINE 最多，足見已廣為臺灣民眾所接受與喜好，另最為犯罪者所運用的行動通訊裝置 APP 為 LINE、Facebook Messenger、WeChat、WhatsAPP 等行動通訊裝置 APP （內政部警政署，2018）。

手機網路通訊應用程式數量成長快速，2013 年 Google Play 與 APPle APP Store 約各有 80 萬個應用程式可供下載安裝。2017 年 Google Play 與 APPle APP Store 已超過 220 萬個應用程式可供下載安裝，且不斷更新（如圖 2-7）。

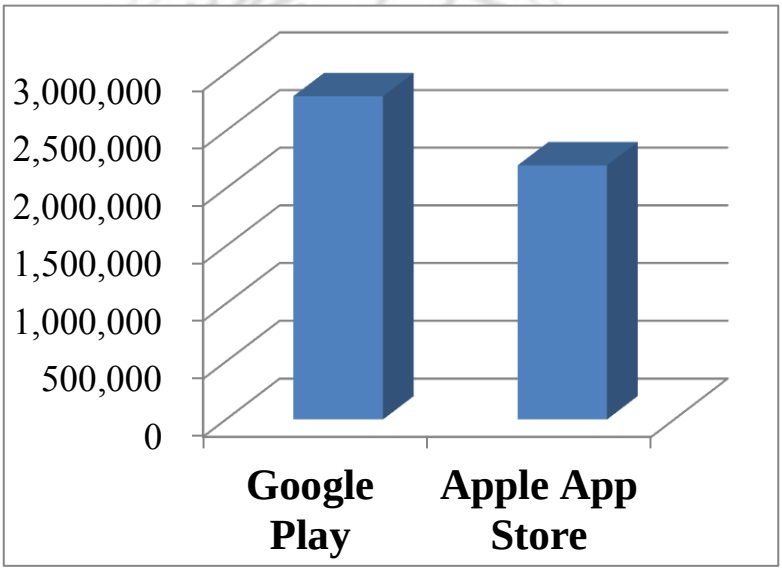


圖 2-7 應用軟體可下載數統計

目前行動通訊裝置相關程式可由公司或個人提供，並具有加密通訊機制。民眾通訊行為改變，使用的社群媒體與即時通訊軟體已成為主流。

資策會創研所 FIND 團隊在 2017 年分析 4G 用戶使用智慧型手機及平板電腦的行為發現：名列前三名的使用行為依序如下：

一、智慧手機

撥打/接聽電話(93.5%)、即時通訊聊天/通話(88.2%)、連結社群網站(76.6%)。

二、平板

連結社群網站(69.2%)、玩平板遊戲(67.7%)、即時通訊聊天/通話(61.6%)。

國內常見之社群媒體及即時通訊軟體，臺灣網路資訊中心(TWNIC)「2017 年臺灣寬頻網路使用調查報告」指出當前民眾最 常使用的社群媒體及即時通訊軟體如下：

(一)、社群媒體：

Facebook (95.7%)、LINE (52.8%)Google+ (3.7%)、Twitter (3.4%)。

(二)、即時通訊軟體：

LINE (97.1%)、Facebook Messenger (27.5%)、WeChat (12.1%)、Skype (8.0%)、WhatsAPP (3.0%)。

LINE 等通訊軟體為國人最常使用之軟體，分別就 LINE WeChat WhatsAPP Facebook Messenger 等通訊軟體之發展略作敘明：

1、.LINE 是在民國 100 年的 6 月在日本發表的行動通訊軟體，為一免通訊費，可在網路實施語音通話與簡訊的傳送，在經過3年後，又有平板電腦版及一般電腦版上市，

可經由行動通訊裝置 LINE 傳送簡訊及圖檔與文字，但是語音的使用因為要使用智慧型手機才能用，所以到了民國 102 年 5 月以臺灣連線股份有限公司的名義在臺灣成立分公司，可使用個人電腦與行動通訊裝置，共有 9 個作業的系統，在臺灣的使用上是最受重視的智慧型手機的應用軟體之一，其用戶在民國 103 年 10 月統計更達到 5 億 6 千萬個用戶，在臺灣則有 1 千 700 萬個用戶，統計到民國 105 年全球則有超過 10 億個用戶。

2、WeChat 是由大陸在民國 99 年 10 月份由深圳騰訊控股公司研發上市的通訊軟體，該軟體是以匯入智慧型行動手機通訊錄的方式用以取得用戶資料，在 100 年的 8 月則增加可檢視附近人對非熟人的交友功能，其用戶到了民國 101 年 3 月統計用戶達 1 億戶以上，而在同年的 4 月該公司為將其產品推向國際，以 WeChat 為名的英文版登記，另在民國 101 年以多種語言方式支援並增加了視訊通話的功能及網頁，在民國 102 年成為當時全球用戶最多的行動通訊軟體，其在中國的滲透率達到 9 成 3，到 104 年的 6 月份在全球有超過 6 億用戶。

3、WhatsAPP 為設置在美國加州的一家行動通訊軟體公司，在民國 103 年的 2 月被臉書所收購，在同年的 11 月推出已讀見過 READ 等功能，卻引起許多用戶不滿，所以改為隱藏方式設定，104 年 1 月推出 WhatsAPP 的網

頁版本，其功能具有與其他應用軟體等使用平臺的用戶可互通及具語音通話之功能，行動通訊裝置 APP 可由 3G 及 4G 網路資訊之用量以 Wi-Fi 之連線方式與各地使用者相互通話且無需付費，如用戶需要更改 WhatsAPP 在內的變更密碼的選擇功能，可在手機上轉移帳號付款的資料，以及對話的紀錄資料至新的電話號碼的帳單上，到民國 105 年的 2 月 WhatsAPP 在全球用戶已達到 10 億以上。

4、Facebook Messenger 在民國 100 年的 8 月上市，使用的用戶無需額外付費，只要透過網站與行動裝置即可與用戶相互傳送文字圖檔與動畫以及聲音視頻等，亦可用語音通話，該軟體於民國 103 年 11 月時統計到使用用戶已達到 5 億戶。

參、行動通訊裝置 APP 的特性及功能

一、LINE 可不受到時空的限制，可經由傳送文字、語音、視訊、圖檔等等功能，且都是免費的，可裝置於時下廣為使用的各種智慧型手機，也能用於電腦版本，除了可一對一互通，亦具有一對多群組的聊天通訊功能，使用 2048Bit RSA 或 1024 的加密版本，如要破解需要很長的時間與人力，另外其不只通訊內容加密，Wi-Fi3GILTE 等通訊的環境下其資料亦均有加密。

二、WeChat 電腦與手機均可使用，具有免費的通話，傳送文字簡訊、

語音以及群組相互聊天功能，同時以低費率在全球撥打手機，但市區電話可能會有區域限制，具有支援 20 種以上語言的介面，也可提供即時位置，在全球使用的客戶有 1 億以上，微信亦是全球首先通過 TRUSTe 認證之即時通訊軟體(DPM,Date Privacy Management)，在獲得認證同時使用用戶的個人資料並受到有效管制，在以 WeChat 社交之工具可與好友以文字或語音相互溝通，該認證之範圍為 WeChat 等多種的不同行動通訊裝置之作業系統。

三、WhatsAPP 其使用方式和 LINE 與 WeChat 一樣的，是可以在電腦上使用的，可以以連線方式經由網路進行免費傳送資訊、通話、照片分享、語音及圖檔等，亦能進行群組聯線聊天，因有兩端之間的加密，所以訊息不至外洩，甚至 WhatsAPP 本身也無法得知訊息之內容。

四、Facebook Messenger 可在電腦版及智慧手機上使用的軟體，有免費視訊、通話、群組間聊天、相片傳送、語音錄製及轉寄訊息等功能，另在對話中相片不會出現在對話之其他人視訊，另具有定位服務以及悄悄話的服務功能，能經雙方接收及傳送加密資訊。

第四節 如何以行動通訊裝置 APP 為犯罪工具

當智慧型手機逐漸成為人手一機的同時，它也變成各類犯罪利用的管道，讓這些犯罪手法從原本透過電腦網路的 MSN、即時通等，變成經由 LINE、WeChat 等行動通訊裝置 APP 進行犯罪，內政部警政署發現歹徒透過這些工

具犯案，以詐騙犯罪為最大宗，其次為販毒、色情，而運用在監控與駭客入侵竊取個資的行為，近來也陸續傳出個案，智慧型手機上行動通訊裝置APP，其實僅是歹徒運用的工具，從最早的電話、簡訊，到電腦網路、網路電話，轉變成現今的智慧型手機 APP（陳子雄，2017）。

智慧型手機上的行動通訊裝置 APP，目前已成為歹徒常用犯罪工具（邱俊福，2013），歹徒在使用通訊為犯罪工具的歷史軌跡隨著時代進步而在改變，由於手機有移動之特性，加上 APP 通訊軟體網頁內容，主機大都設置在國外，增加調閱、查緝的困難度，包括網拍、團購等普遍的詐騙手法，都逐漸從其他工具轉移至此。

前行政院長張善政在民國 105 年 2 月 25 日主持治安會報，聽取內政部「行動 APP 對通訊監察之衝擊與因應」報告後表示，本案涉及很多政策、技術、經費編列及 APP 業者配合等問題，邀集內政部、國家通訊傳播委員會、科技部、行政院資通安全辦公室等相關機關（單位），研議短、中、長期計畫方案，期在該年 520 前完成可行性評估（張善政，2016）。

智慧型手機可安裝許多微型的應用程式(APP)，其中提供語（影）音通話與即時訊息功能的免費 APP 已高達數百種，也改變了民眾通訊方式。犯罪者會利用行動通訊裝置 APP 規避偵查，司法單位已正視此問題並研提因應策略及作為。

壹、行動通訊裝置 APP 是以封包傳送

一、需有攔截封包工具及解密後讀取

無論犯罪者早期利用市話或手機通話達成犯罪目的，延續至

今，我國從一開始的無法律規範，到後來電信法和通保法的立法後，才給了偵查人員該方面實施犯罪偵查時能有所依循，向上溯源，針對犯罪或手機通話做為各類犯罪聯繫方式，偵查時蒐證資料不再於雙方通訊內容，還包括通信使用者資料以及通信紀錄...等，主要在於傳統式通話是藉由線路交換做為傳遞，而雙方互為聯繫的資料，大多最後都存放於犯罪者各自使用電信業者，像是通信使用者資料以及通信紀錄，都是可以事後經由向各電信業者調閱取得。

若在犯罪偵查過程中需上述資料作為協助辦案及蒐集犯罪事證，依據相關法律及正常程式向電信業者做資料調閱即可，至於雙方的通訊內容雖不會存放於各自電信業者，但因其也是經由線路交換做傳送，偵查時需對某人通訊內容進行監聽時，均需符合法律程式，經向法院聲請令狀核准後，再經電信業者拉線路至我國的監察機房（內政部警政署通訊監察科或調查局），讓偵查機關能針對核准後的受監聽對象進行通訊內容現譯或錄製後監聽，以利偵查人員對這方面的蒐證保全。

截至目前行動通訊裝置 APP 種類愈來愈多，亦是本研究欲探討之主要對象，雖行動通訊裝置 APP 多數由外國公司所開發，發話端和受話端雙方均須透過網際網路，並經由封包傳輸做為雙方溝通的方式，其功能上較常被歸類為網路語音通話以及文字訊息兩種；對於犯罪者利用行動通訊裝置 APP 網路語音通話或文字訊息做為犯罪間溝通聯繫的管道，在犯罪偵查上藉由行動通訊裝置

APP 聯繫可能留下犯罪事證，但卻有別於傳統通訊監察，從線路掛線是無法獲取，仍要透過攔截封包及解密後讀取，偵查人員對於涉及行動通訊裝置 APP 之案件能否偵破取決於國內偵查規範，依據偵查程式及攔截後解密技術...等問題，這是偵查成敗關鍵。

二、歹徒運用行動通訊裝置 APP 犯罪已成趨勢

行動通訊裝置 APP 因搭配行動裝置，不受時空限制，因此廣受大眾喜愛，雖大多數使用者會以自身行動裝置之電信門號做註冊，但若為犯罪者有心躲避，也能以臉書帳號或 Google 信箱方式註冊後登入，藉此多一道防護，讓警方更加難以偵查，直到 4G 時代來臨，流量傳輸穩定後，更確立行動通訊裝置 APP 的地位，雖使用者轉移至行動通訊裝置 APP，也屬於行動通訊的一種，但也因此對各大電信業者帶來衝擊。

貳、行動通訊裝置 APP 傳輸與儲存方式

面對新的標的物，偵查人員欲藉由偵查手法取得犯罪事證，已不是件容易的事，在無偵查規範前提下，寸步難行，對於該如何修法，將成為趨勢，行動通訊裝置 APP 法制面重要性，須先瞭解該行動通訊裝置 APP 開始，雙方使用行動通訊裝置 APP 之通話內容或文字時，如何傳輸以及儲存型態、位置，正所謂「知道欲蒐集資料放置何處，才能知道往哪裡尋找」，無論傳統或網路語音通訊，均為嫌犯間之通訊方式，但兩者之間資訊傳輸動向以及存儲型態、位置各有不同，相形之下，對於所欲採行之偵查手法不盡相同；首先由雙方傳輸動向開始，

繼而瞭解資料儲存型態、儲存後放置何處...等方面。

第五節 創新技術因應以行動通訊裝置 APP 為犯罪行為

壹、以創新理論創新因應技術

行動通訊裝置 APP 幾乎都存在加密問題，對辦理這類案件的司法人員，能獲解密金鑰是最好方式，惟事涉商業經營信譽，除非國家有特別法令規定，要廠商提供金鑰不易做到，刑事警察局通訊監察單位研究發現，可透過封包保存與過濾方法，藉以辨識網路上使用者真實身分，同樣可追查出可疑之嫌犯（梁哲賓，2019）。這種技術創新的方式對案件偵辦具積極效果，尤其在運用社群網路偵察既鑑識平臺藉以找出嫌疑犯與社群網路之時間關聯性，在偵辦行動通訊裝置 APP 上有一定助益。

為因應網路已普遍採用加密、代理伺服器與匿名網路下，造成難以追查犯罪者真實身分與定位追蹤，惟有持續研究突破偵查技術才能有效因應。

貳、找出節點研發技術（梁哲賓，2019）

一、各式社群網路或即時通訊等行動通訊裝置 APP 犯罪，已造成我國治安重大問題，透過封包蒐集再由封包保存與過濾方法，可追查出可疑之嫌犯。

二、有關社群網路 APP 運行的特點如下：

（一）、即時訊息傳送並非點對點(Point to Point)傳送，而是 Client-

Server 架構。

（二）、傳送過程加密。

而歹徒詐騙的躲避手法為：

（一）、金融方面利用國外帳戶（金融帳戶，遊戲幣帳戶等）、人頭帳戶、比特幣等方式交易，使辦案人員難以追蹤。

（二）、網路技術方面，透過盜用他人帳號（例如 LINE、Facebook 帳號）、代理伺服器、匿名網路（Tor）方式躲避他人追蹤。

舉例來說，一犯罪者會先盜取與受害者有關的第三者帳號密碼，一般是受害者在以即時通訊 APP LINE 上的朋友，再透過這位無辜的第三者在 APP LINE 上與受害者聯絡。在此情形下，因為犯罪者盜用無辜的第三者的帳號，因此不需要去查無辜的第三者帳號的真實身分。傳統偵查上，對於網路架構不熟悉之調查者，期望從被害者端擷取的封包獲得傳遞者（犯罪者）的 IP、Port 與傳遞的時間，藉以向電信業者（例如中華電信）調取看封包是誰發出的。因為即時通訊是 Client-Server 架構，因此傳遞的封包一定是 APP LINE 主機，因此這種偵查手段並無必要。傳統上，辦案人員向 APP LINE 服務提供者請求調閱通訊紀錄，期望能查出是從哪裡發出訊息給被害者的，這時會遇到另一個障礙，犯罪者是透過代理伺服器發出即時訊息，代理伺服器如果是在德國，代理伺服器業者毋須配合犯罪調查。這種跨境追查路由方式，在我國外交處境下，幾乎無法追查，縱使透過路由能夠一路追查下去，耗時甚

多，很多犯罪紀錄早已抹去，犯罪者早已不知去向，或者早已把不法所得花光。另一種方式是透過金流方式追查，如果金流是透過匿名網路，透過地下匯兌，一般的偵查作為也無法發揮最用。

三、透過 IP 連線資料保存(或稱為網際網路連線紀錄保存、IP Meta Data 保存)，利用犯罪者留下的時間標記與使用 APP 的種類，依照以上兩特徵，利用加害者與受害者通訊間時間的關聯性，於 IP 連線資料保存中，透過不同的時間點間逐步交集，從眾多可疑者逐步過濾出加害者真實IP，再透過網際網路接取服務業者(如遠傳電信)，登錄之 IP、Port、時間對應身分 ID 服務，來獲得網路上虛擬歹徒的真實身分，並達成定位追蹤的目的。

四、以資料保存方式偵辦是突破困境方式之一。資料保存(DR，Data Retention)在傳統的電信領域通常是指保留用戶的通話紀錄(CDR，Call Detail Record)；對網際網路接取服務提供商(ISP，Internet Service Provider) 而言，Data Retention 則可延伸成為 IP 連線資料保存 IPDR(IP Data Retention)的概念，也就是保留網際網路的連線紀錄、Email 紀錄、網站瀏覽紀錄等。有了 IPDR 的完整紀錄後，可以利用加害者與被害者通訊時間「時間關聯性」，或者是嫌疑犯（鎖定的目標）使用社群網路的時間點（目標與社群網路之時間關聯性)，找出可疑的目標或至少縮小偵查範圍。例如：可以蒐集嫌疑犯（鎖定的目標）在 Facebook 網站上多次留言的時間，利用這些時間序列資訊去搜尋出在這些時間點有上傳資料到 Facebook

網站的電信用戶，並依出現次數多寡排序；出現次數越多的用戶，就越有可能是我們要找的目標。而且還可以比對同一個用戶在不同社群網站的留言時間，進一步增加比對的可信度。此外，一般人通常在不同的網站會以相同或類似的帳號/密碼登入，所以針對未加密的網站帳號資料進行保存，通常也有助於找出可疑目標（如圖 2-8）。

圖 2-8 嫌疑犯與社群網路之時間關聯性

第六節 小結

通訊系統經過 4 個世代演進，經由傳統語音傳送，到以封包傳輸時代，同時以行動通訊裝置 APP 犯罪快速增長，手法快速變化、科技化、專業化、與全球化時代，行動通訊裝置 APP 犯罪問題已為警政工作的嚴重挑戰之一。其中又以網路詐欺最為嚴重，時下擁有智慧手機者，只要有下載社群網路服務（例如 Facebook）或者網路即時通訊服務（例如 LINE）者，幾乎人人

接過詐騙訊息，另外，如比特幣洗錢、網路勒索、竊盜個資等。而高科技犯罪偵查之一重點為知道傳送訊息者之真實身分（個化使用者）與他目前的地理位置（追蹤他的位置）。

但由於各式各樣社群網路、網際網路應用服務(APP)的大量使用，在運用加密、匿名網路、且 APP 服務提供者大多位於國外及雲端儲存下，數位偵查與鑑識已愈發困難，治安機關面臨難以透過封包解譯或網路接取服務提供者調閱通聯紀錄而追蹤個化使用者之困境。因此，有必要從不同的出發點，發展新的數位偵查與鑑識方法。

在隨著市面上行動通訊裝置 APP 種類眾多，使用者廣泛，從一開始少數犯罪運用，到現今已逐漸增加犯罪類型。在面對歹徒以行動通訊裝置 APP 為犯罪工具的違法行為，治安單位必須要深刻思考因應之作為。

第三章 研究方法與設計

第一節 研究方法

壹、研究方法

本研究之研究方法是以文獻分析及系統科學分析法進行研究闡述，藉以文獻分析法為窺探本研究關心之主軸，另從執法上所遇之法規與技術困境上探討，以找出司法人員在因應科技犯罪之因應方式，另為解決行動通訊裝置 APP 辦案困境，以實驗方式建置驗證平臺再將驗證成果運用於實務建案，以有效偵辦行動通訊裝置 APP 犯罪。

一、文獻分析法

文獻的原意為典籍，從學術的角度來看，則是為官方或民間收藏用來記錄群體或個人在政治、經濟、軍事、文化、科學或是宗教等方面活動的文字或其它載體的材料，對此，文獻分析法係指根據一定的研究目的或課題，透過蒐集有關資訊、調查報告、圖書、期刊與學術論文等文獻資料，從而以系統、客觀的界定，全面且精準地鑑別和掌握所想要研究的議題現象，並且就上揭資料加以研究歸納、整理分析，以增進對於科學有所認識的一種方法。

文獻分析法主要目的在於了解過去、洞察現在和預測未來，對此，蒐集內容儘量要求豐富及廣博，經過分析後歸納統整，再分析事件的淵源、原因、背景、影響及其所隱含的結構意義等，

除此之外，因為文獻分析法不與文獻中記載的人、事有所接觸，因此，又稱為非接觸性研究方法，至於，文獻分析法包括閱覽與整理(Reading and Organizing)、描述(Description)、分類(Classfying)以及詮釋(Interpretation)等四大步驟。綜合以上，文獻分析法的特性如下：

（一）它所研究的事件是過去而非目前發生，亦即，文獻分析超越過去時空的限制，紀錄的是過去的社會事實；

（二）文獻分析可超越個人經驗與視野；

（三）文獻分析可超越調查互動中的不良影響；

（四）文獻分析其作用是可提

供詳實可靠的背景資料。文獻分析對研究資料收集是重要的，在獲得資料後再予歸納分析，同時文獻分析與實際的做法也是一項資料收集的「技術」，對此，一般研究中的文獻分析法經常也會和相關的研究方法相互搭配，例如深度訪談法、問卷調查法、電話調查或焦點團體訪談法等，藉此讓資訊或資料的收集更為完整（林萬青，2009）。

文獻分析法係廣為蒐集與研究主題相關之文獻資料，經由分析其內容與綜整研究，來取得研究需要之相關的資料，同時對蒐集而來的文獻做一有系統且客觀的敘述的研究方式，這種做法可有效分析到文獻之內容，並經由所得資料進行有系統地陳述，可推論內容對研究該論文過程中具有甚麼樣之影響（蔡明月等 ，

2013）。

本文研究主題為有關司法人員偵辦案件實務上對行動通訊裝置 APP 在遭遇到難以克服的問題，以及延伸的相關問題，對司法人員在偵辦案件所造成的衝擊等，並分析有關高科技犯罪目前已逐漸成為趨勢，尤其歹徒在以行動通訊裝置 APP 犯罪進行探討。

從實務案件偵辦中發現，歹徒已藉由行動通訊裝置 APP 為其犯罪使用之工具，但是行動通訊裝置 APP 是近年來才開發出來的新形態科技軟體，在法令未能與時俱進地配合執法的狀況下，導致司法人員在偵辦以行動通訊裝置 APP 為犯罪工具時常受限制，這些問題亟需解決。

本研究為探討行動通訊裝置 APP 相關研究，文獻分析中亦探討有關行動通訊進程的研究，基本原理與傳輸的方式以及儲存犯罪數據等等問題，再就以行動通訊裝置 APP 為犯罪工具進行研究分析，但就案件偵辦中較常見的犯罪行為則為毒品及詐欺等類型為主，最後則是以技術創新（科技技術創新）因應以行動通訊裝置 APP 為犯罪行為作探討分析。

本研究最後則是因應行動通訊裝置 APP 犯罪在通訊監察過去的建案與未來應做之研究提出相對之看法與分析。

二、系統科學分析法

系統科學是一門總結複雜系統的演化規律，研究如何建設、管理和控制複雜系統的科學。以系統為研究對象的基礎理論和應用開發的學科組成的學科群。它著重考察各類系統的關係和屬性，

揭示其活動規律，探討有關系統的各種理論和方法（維基百科，2019）。

20 世紀，系統論、控制論、資訊論等橫向科學的迅速發展，為發展綜合思維方式提供了有力的手段，使科學研究方法不斷地完善。而以系統論方法、控制論方法和資訊論方法為代表的系統科學方法，又為人類的科學認識提供了強有力的主觀手段。它不僅突破了傳統方法的局限性，而且深刻地改變了科學方法論的體系。這些新的方法，既可以作為經驗方法，作為獲得感性材料的方法來使用，也可以作為理論方法，作為分析感性材料上升到理性認識的方法來使用，而且作為後者的作用比前者更加明顯。它們適用於科學認識的各個階段，因此，稱為系統科學方法(BONI CHEN ，2012)。

行動通訊裝置 APP 的應用在目前已是相當普及，同時在國外這類通訊軟體亦是同樣受到歡迎，近來的犯罪趨勢進行分析可發現，國內許多為非作歹分子為遂行其犯罪行為，在應用行動通訊裝置 APP 的情形，更是有增無減，以目前的治安狀況而言，對司法人員在偵查案件上，遭遇到的以行動通訊裝置 APP 從事犯罪部分，主要有使用網路上之語音的通訊與圖檔，以及文字等，但礙於業者有對其加密做法，因此在蒐證上有相當等困難，為解決行動通訊裝置 APP 監察技術突破，本研究創新研究方法，先進行可行性驗證，再將驗證可行之研究成果以建置實證平臺。

首先在可行性驗證方面先建置行動 APP 通訊軟體實驗平臺、

行 動 APP 通訊軟體監察技術實驗平臺、社群網路偵查暨鑑識技術實驗平臺、戰術型 WiFi 網路 APP 偵查系統規劃與驗證計畫、跨境戰術型 IP 通訊監察系統、行動裝置及其應用程式安全性分析運用雛型實驗平臺、提升新世代社群網路偵查暨鑑識能量計畫（建置雲端與 IP 定位資料保存規範機制實驗平臺）進而建置偵查與分析平臺。

建置實證平臺是以實驗平臺獲得可信之驗證成果後，再以偵查與分析行動通訊裝置 APP 建置實務應用平臺，包含社群網路偵查暨鑑識能量建置、遠傳電信、臺灣大哥大及臺灣之星 4G 後端通訊監察系統、網路封包分析以及可攜式封包解譯系統等，均為司法人員在偵辦以行動通訊裝置 APP 為犯罪工具之偵辦提供莫大助力。

貳、研究架構

本研究共六章，分別為第一章緒論、第二章文獻探討、第三章研究方法與設計、第四章偵查問題與困境、第五章實驗平臺與實證平臺建置及第六章結論與建議，研究架構如下（如圖 3-1）。

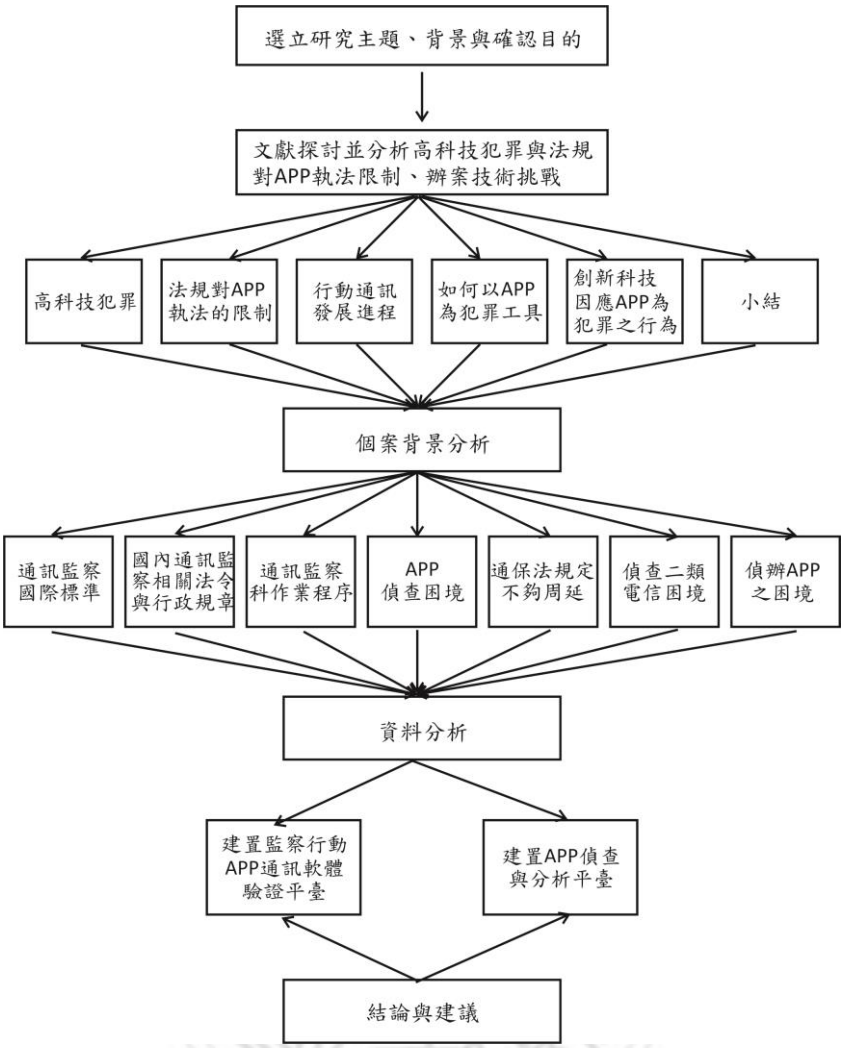


圖 3-1 研究架構圖

第二節 研究設計

本研究是針對以行動通訊裝置 APP 的高科技犯罪研究，首先，將以行動通訊裝置 APP 在國內的發展談起，這部分的研究範圍包含行動通訊以及其基本原理、如何傳輸以及儲存方式，現有之偵查狀況，再就司法人員在面對以行動通訊裝置 APP 進行犯罪連結，在偵辦過程中所面臨的困境進行分析犯罪行為與因應，這些偵辦高科技犯罪相關單位所建立的研發與建置的驗證平臺、破案技術分析等，尤其研究發展高科技犯罪的因應模式與技

術。

另外，有關犯罪偵查之法令檢討，以及我國目前所面臨相關法令不足之因應作為進行分析檢討，並提出改進面向，藉以補足我國對這方面之不足，期望爾後在修法上能對行動通訊裝置 APP 犯罪行為有明確規範，便於司法人員在辦理相關案件時不致受到法令的牽制，相對地法令應該作為執法人員執法的有力後盾，才是制訂該項法令目的之一，另外，因應辦案需要，也期望政府儘早與行動通訊裝置相關業者能達成協助義務，如同通保法所規定電信業者有協助通訊監察機關建置通訊監察義務一樣。

再就實務面的研究，可從因應偵查科技犯罪區分兩個區塊，分別為可行性驗證及實證建置監察行動 APP 通訊軟體實證平臺 。

誠如司法人員是以偵辦案件為其應具有之本職學能，但礙於高科技犯罪行為，歹徒其使用工具與技術不斷在更新，因此，就目前刑事警察局研究或建案之對於行動通訊裝置 APP 的解譯分析，與對辦理這類案件有助益的實務做法，在本研究中加以討論。

第四章 偵查問題與困境

我國通訊規格是依據歐盟標準建置，如 3GPP LTE(Long Term Evolution)的相關技術規範（工業技術研究院 2009 年 5 月），歐盟標準是建置案基礎，本研究面向與通訊相關，自應撰文研析通訊之規格與標準。

國際標準組織 ETSI TISPAN(European Telecommunications Standards Institute；Telecommunications and Internet Converged Services and Protocols for Advanced Networking)提出 Next Generation Network(NGN)架構，並與 3GPP(3rd Generation Partnership Project) 共同制定 IP Multimedia Subsystem(IMS)，成為 IMS based IPTV 系統的技術標準。ETSI TISPAN 所制定的 NGN 通訊網路技術標準，係一基於封包傳輸的網路架構，除了既有電信語音服務之外，並可以提供具有加值應用服務與寬頻接取的特性，以及 QoS 的傳輸技術。無論是無線網路或是固定網路，各種多媒體資料流皆可透過 NGN 網路，達到匯流的功效。

繼 GSM、UMTS/HSPA 之後，LTE 成為 3GPP(H. Zarrinkoub2014)所制定的新一代行動寬頻通訊系統的標準技術。2004 年在加拿大多倫多市所舉行的第三代行動通訊系統暨無線電接取網路研討會，由電信營運商、系統製造商與相關研究機構等超過 40 個組織或機構，針對 UTRAN 的演進提出各項技術演進之建議，並規劃 LTE 系統的推展(H. Zarrinkoub，2014)。全球無線通訊的標準在 3GPP 成功的推廣下建立 2G 至 4G 的標準，以相同成功的模式將持續發展下世代通訊標準(5G)。為強化臺灣在標準制定參與的強度，在經濟部技術處推動成立「臺灣資通產業標準協會 TAICS」，協會的目的是

對內建立臺灣資通技術產業標準制定的平臺，整合我國參與國際標準會議的資源與力量，對外成為代表臺灣對國際組織的單一窗口。最終的目的是希望成為 3GPP 的組織夥伴，進而具有決策主導權（如圖 4-1）

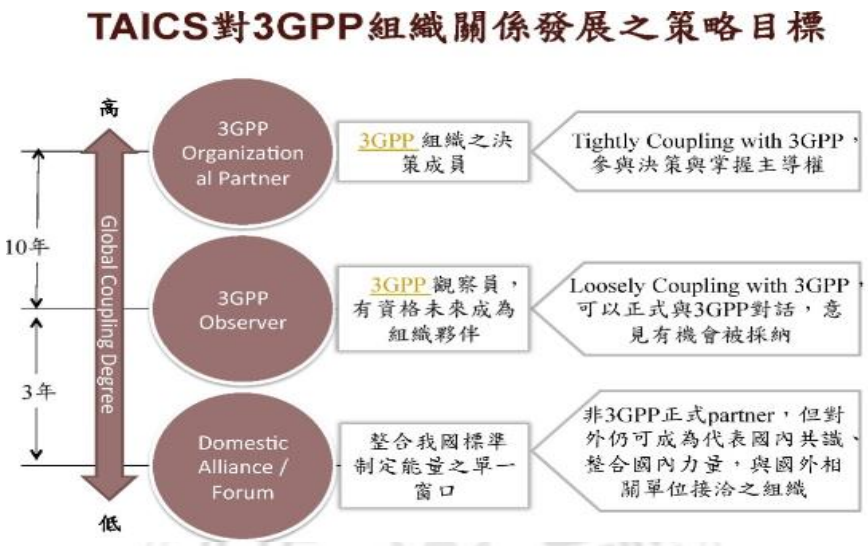


圖 4-1 臺灣資通產業標準協會參與 3GPP 的策略與目標

第一節 通訊監察國際標準

歐洲電信標準協會(ETSI，European Telecommunications Standards Institute)是歐洲地區各種通訊標準（如無線通訊、廣播、以及電信等）的制定組織(ETSI - Cellular History ，2015)，創建於 1988 年。除了各種通訊標準的制定外，對應的通訊監察標準制定也是該組織的工作範疇。以電信監察為例，就有 ETSI ES 201 671(Handover Interface for the Lawful Interception of Telecommunications Traffic)；在數據網路的監察方面，則有 ETSI TS 101 232-1、ETSI TS 101 232-2、ETSI TS 101 232-7(Handover Interface and Service-Specific Details for IP Delivery)等通訊監察標準；在數位電視寬頻纜線接取方面，則有 ETSI TS 101 909-20-1 與 ETSI TS 101 909-20-2 等通訊監

察標準文件。

此外，歐盟部長理事會(European Council of Minister)於 2006 年 2 月正式生效「通聯資料保存法」(Directives on the Retention of Data，2006/24/EC)。此法令之目的，主要在統合歐盟會員國賦予其國內電信業者或網路服務提供者，對所擁有通訊資料的保存義務，並確保這些通聯資料能及時被用於協助檢警進行重大犯罪偵察與起訴。此法已融合參照其他歐洲各國的通訊監察相關規範並做為未來各國相關法規的重要依據。

ETSI 也根據此依法令的公佈，制定了通聯資料交換介面相關的標準：ETSI TS 102 656(Requirements of Law Enforcement Agencies for Handling Retained Data)、ETSI TS 102 657 (Handover Interface for the Request and Delivery of Retained Data)等。

通聯資料保存及調閱可以彌補部分通訊監察的不足：通訊監察只能蒐集特定嫌犯現在或未來的通聯資料與內容；而通聯資料保存及調閱則廣泛蒐集不特定對象的通聯資料，缺點則是無法大量保存通聯內容。兩者在犯罪偵防及國土安全的應用上可說是相輔相成。

壹、通訊監察標準制定組織簡介

針對通訊監察標準制定之相關組織及其背景做簡單的介紹，條列如下：

一、歐洲電信標準協會(ETSI，European Telecommunications Standards Institute)：

ETSI 創立於 1988 年，有 688 個成員來自全球 55 個不同的國家，

不論是製造業者、網路工程師、行政人員、服務維修人員、研究機構，都是在 ICT(Information and Communication Technologies)領域不可或缺的重要角色。ETSI 是獨立於企業、政府機構且被 EFTA(European Commission & European Free Trade Association)許可的非營利性質組織，主要是制定適用於現今及未來的通訊標準。

二、第三代合作夥伴計畫(3GPP，3rd Generation Partnership Project)：

GPP 是在 1998 年 12 月成立，最初由歐洲的 ETSI、日本的 ARIB、日本的 TTC、韓國的 TTA、美國的 ATIS 等五個標準化組織發起，其後中國的 CCSA 也加入，主要是制定以 GSM 標準為基礎的無線通信第三代技術規範。

貳、ETSI 通訊監察標準

ETSI 所制訂的通訊監察標準眾多，檔內容涵蓋範圍包含：通訊監察概念說明、通訊監察主管機關需求、通訊監察網路功能、資料分配管理系統接入介面、針對某一特定網路架構的通訊監察網路功能等。以下將根據上述分類條列其中常見的通訊監察標準如下：

一、通訊監察概念說明

ETSI TR 101 943 V2.2.1 “Lawful Interception(LI)；Concepts of Interception in a Generic Network Architecture”.

二、LEA(Law Enforcement Agency)對於通訊監察的需求

ETSI TS 101 331 V1.2.1 “Lawful Interception (LI)；Requirements of

Law Enforcement Agencies”.

三、通訊監察網路功能

ETSI ES 201 158 V1.2.1 “Telecommunications Security；Lawful Interception (LI)； Requirements for Network Functions”.

四、針對 IP 網路之通訊監察網路功能

ETSI TR 102 528 V1.1.1 “Lawful Interception (LI)； Interception Domain Architecture for IP Networks”.

五、針對 IP 網路之通訊監察資料分配管理系統接入介面

（一）、ETSI TS 102 232-1 V2.4.1 “Lawful Interception (LI)；Handover Interface and Service-Specific Details(SSD)for IP Delivery；Part 1：Handover Specification for IP Delivery”。

（二）、ETSI TS 102 232-2 V2.3.1 “Lawful Interception(LI)；Handover Interface and Service-Specific Details(SSD)for IP Delivery ； Part 2 ： Handover Specification for E-mail Ervices”。

（三）、ETSI TS 102 232-3 V2.2.1 “Lawful Interception(LI)；Handover Interface and Service-Specific Details(SSD)for IP Delivery；Part 3：Service-Specific Details for Internet Access Services”。

（四）、ETSI TS 102 232-4 V2.1.1 “Lawful Interception(LI)；

Handover Interface and Service-Specific Details(SSD)for IP Delivery；Part 4：Service-Specific Details for Layer 2 Ervices”。

（五）、ETSI TS 102 232-5 V2.3.1 “Lawful Interception (LI)；Handover Interface and Service-Specific Details(SSD)for IP Delivery；Part 5：Service-Specific Details for IP Multimedia Services”。

（六）、ETSI TS 102 232-6 V2.3.1 “Lawful Interception(LI)；Handover Interface and Service-Specific Details(SSD)for IP Delivery；Part 6：Service-Specific Details for PSTN/ISDN Services”。

（七）、ETSI TS 102 232-7 V2.1.1 “Lawful Interception(LI)；Handover Interface and Service-Specific Details(SSD)for IP Delivery；Part 7：Service-Specific Details for Mobile Services”。

六、通訊監察資料分配管理系統接入介面

(一)、ETSI ES 201 671 V3.1.1 “Lawful Interception(LI)；Handover Interface for the Lawful Interception of Telecommunications Traffic”。

(二)、ETSI TS 101 671 V3.4.1 “Lawful Interception(LI)；Handover

Interface for the Lawful Interception of Telecommunications Traffic”。

參、3GPP 通訊監察標準

3GPP 的其中一個成員就是 ETSI，因此 3GPP 的通訊監察標準大多由 ETSI 提出，經 3GPP 認可後成為 3GPP 的通訊監察標準。3GPP 的通訊監察標準主要分為三類：通訊監察需求、通訊監察網路功能、通訊監察資料遞交介面。以下將根據上述分類條列其標準：

一、通訊監察需求 for UMTS

3GPP TS 33.106 V8.1.0 “Lawful Interception Rrequirements”.

二、通訊監察需求 for GSM/GPRS

3GPP TR 41.33 V8.0.0 “Lawful Interception Requirements for GSM”.

三、通訊監察網路功能 for UMTS

3GPP TS 33.107 V8.8.0 “Lawful Interception Architecture and Functions”.

四、通訊監察網路功能 for GSM/GPRS

3GPP TS 42.33 V8.0.0 “Lawful Interception(LI)；Stage 1”.

3GPP TS 43.33 V8.0.0 “Lawful Interception(LI)；Stage 2”.

五、通訊監察資料分配管理系統接入介面

3GPP TS33.108 V8.7.0 “Handover Interface for Lawful Interception(LI)”.

第二節 國內通訊監察相關法令與行政規章

壹、法規嚴格規範通訊監察

隨著科技不斷創新與日新月異，運用高科技技術來維護國家安全或進行犯罪偵防之比例亦大幅增加。其中通訊監察技術之運用，更是犯罪偵查機關在破獲許多重大案件中，不可抹滅的重要功臣。然而，水能載舟，亦能覆舟，通訊監察技術若在違法或不當運用之下，對於憲法上所保障之人民基本權利侵害甚鉅。因而，藉由一套健全而完善之法律制度，使犯罪偵查機關不僅能善用偵查科技來有效打擊犯罪，同時又能確保憲法對於人民所保障的基本權利不受侵害，實屬刻不容緩。

貳、制定更多行政規章

我國已於民國 88 年 7 月 14 日制訂公佈了「通訊保障及監察法」（又簡稱「通保法」）。此項法制之訂定，為我國邁向民主法治國家、充分落實人權保障之重要里程碑之一，不但對人民之秘密通訊自由之憲法權利有更明確的保障，同時使得執法機關實施通訊監察有了法律依據及規範。

基於通保法，行政機關也制訂了許多相關行政規章，通訊監察相關法令與行政規章如以下所列：

一、通訊保障及監察法。

二、通訊保障及監察法施行細則。

三、固定通信業務管理規則。

四、警察機關執行通訊監察管制作業要點。

五、內政部警政署警察機關執行中華電信固網通訊監察作業要點。

六、內政部警政署警察機關查詢電信通信紀錄及使用者資料管制作業要點。

第三節 刑事警察局通訊監察科作業流程

壹、刑事警察局通訊監察科為通訊監察建置機關刑事警察局通訊監察科為國內主要提供協助執行通訊監察作業機關之一。在確保通訊監察作業合法性的前提下，通訊監察科制定了一套可有效協助執行單位的通訊監察作業與稽核流程。經過通訊監察科長期規劃與有效執行的努力耕耘，所有的作業流程都已建置相對應的資訊系統，使得通訊監察作業得以合法化、透明化、系統化地有效執行。本節將簡介主要作業流程與相對應之資訊系統（圖 4-2）。

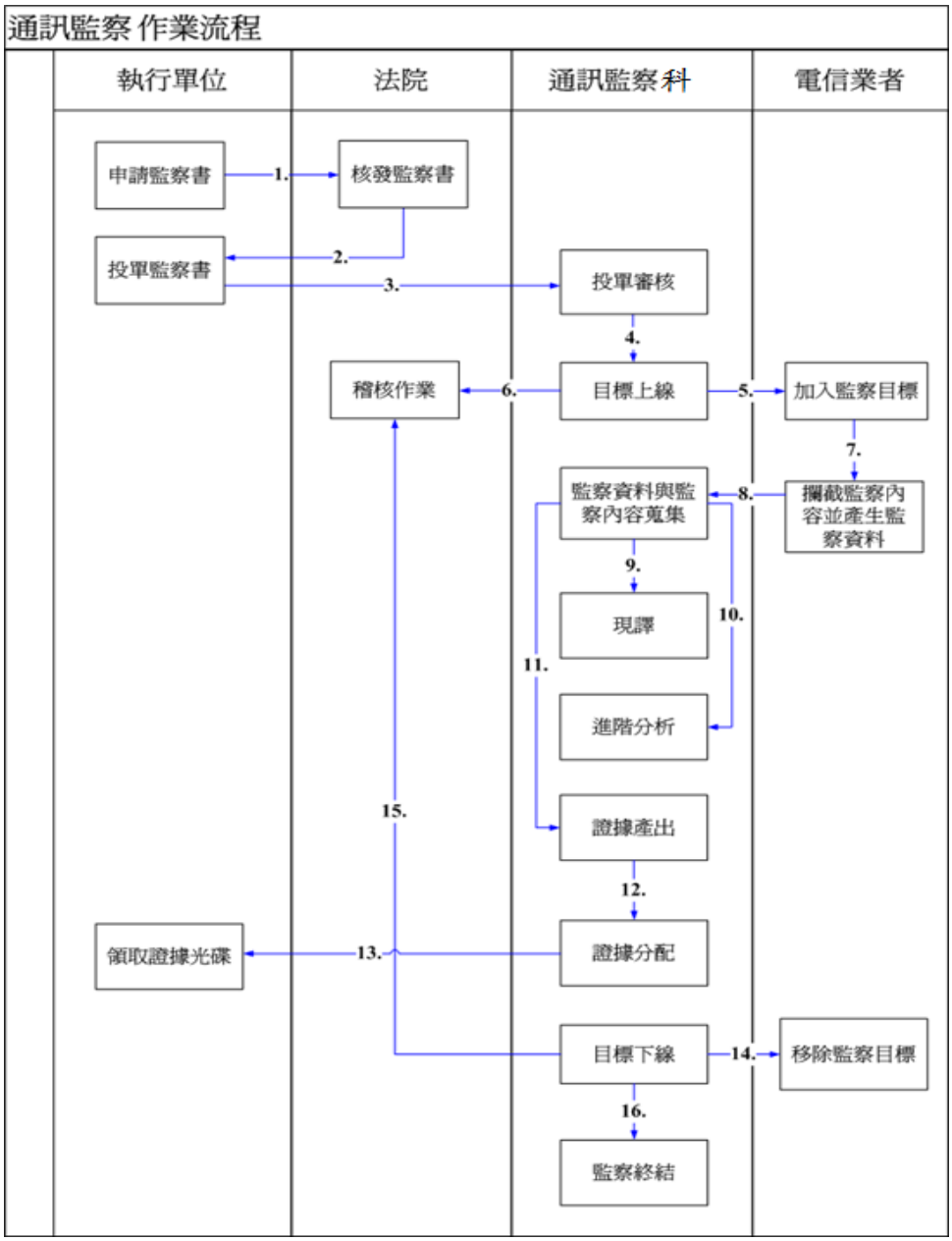


圖 4-2 刑事警察局通訊監察科作業流程圖

貳、通訊監察科目前之通訊監察作業流程（圖 4-3）：

一、基於確保人民隱私權及秘密通訊自由，依據「通訊保障及監察法」之規範，在監聽之前偵查人員須先向法院申請通訊監察書。

二、當申請所提供之舉證資料，有足夠事實可以證明嫌犯有足夠的罪

嫌與監察的必要，法院將核發通訊監察書。

三、偵查人員取得監察書後，攜帶監察書正本至該各縣市投單業務承辦人處，該承辦人即可利用投單作業管理系統輸入監察書詳細資料、監察目標資料，並上傳監察書掃瞄檔案，進行投單。再由通訊監察科上線審查人員負責審核監察書內容，決定是否受理該監察作業申請單。

圖 4-3 投單作業流程管理系統畫面

四、上線審查人員審核並受理監察作業申請單後，將投單資料從投單作業管理系統匯出成 XML 檔案，再手動將 XML 檔匯入監察資料管理系統。為確保通訊監察系統的安全，投單作業管理系統與通訊監察系統即現行監察資料管理系統（圖 4-4）必須實體隔離。投

單資料手動匯入監察資料管理系統後，上線審查人員必須再一次確認投單內容的正確性，以確保通訊監察作業的合法性，並對系統資源作最佳的分配。投單資料內容包括監察書核准文號、申請單位、核准單位、監察目標、以及監察起迄時間等重要資訊。審核完成的投單將被儲存到監察系統資料庫，準備上線監察。

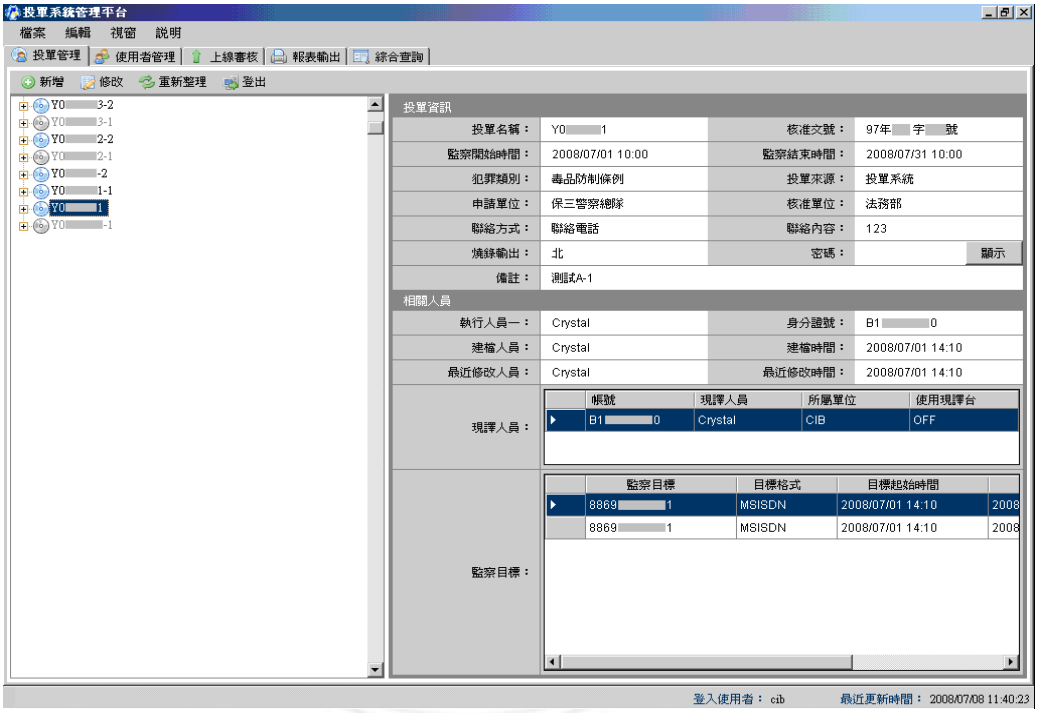


圖 4-4 監察系統管理工作站

五、投單資料審核完畢後，通訊監察系統依監察目標所設定的監察開始時間，將監察目標設定至電信業者端的通訊監察設備，電信業者所建置之監察設備隨即啟動目標之監察功能。電信業者端的通訊監察設備可以是仲介系統(MD，Mediation Device)或交換設備的內部監察功能模組(IIF，Internal Interception Function)。

六、基於「通訊保障及監察法」規範，通訊監察科於執行通訊監察時

應遵循「合法」、「必要」之原則。因此，司法院與法務部最高檢察署可透過線上稽核機制，確保所有通訊監察作為的合法性。

七、當被監察目標進行通話時，電信業者端之監察設備會攔截監察目標所產生的監察相關資料(IRI，Interception Related Information)與通訊內容(CC，Content of Communication)。

八、監察資料收集系統透過通訊監察標準介面，接收電信業者端目標監察之結果,從目標上線監察到目標所產生的各種監察相關資訊，進行完整的接收與解譯，最後並將監察所得全部儲存於監察資料儲存系統中，以供後續現譯或分析人員使用。

九、各執行單位可指派偵查人員透過現譯臺，監聽監察目標線上即時通話或檢視歷史通聯紀錄等工作（圖 4-5）。

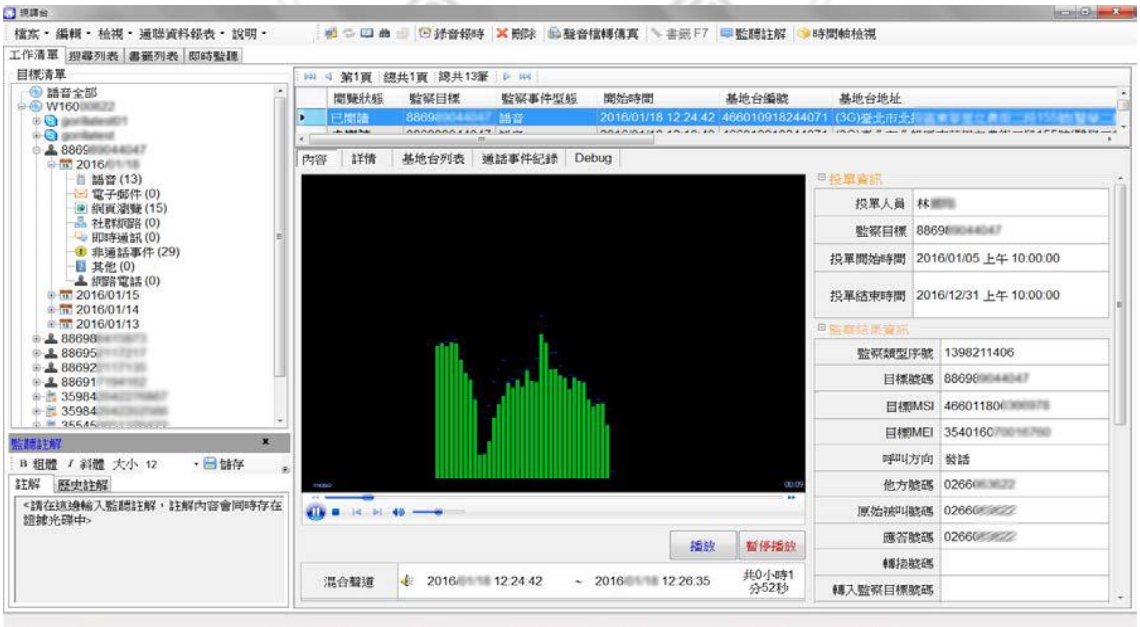


圖 4-5 現譯臺系統畫面

十、配合多媒體中央資料庫所提供的連結分析系統、地理資訊分析系統等分析工具，協助案件偵辦人員分析監察系統所攔截到之監察資料與內容，以取得有利於刑案偵辦的線索。

十一、通訊監察所得會經由週期性證據產出系統，以投單為單位，週期性且自動化地燒錄在 DVD 光碟內，並依照所屬之投單申請單位將產出的證據光碟予以編號。每一張證據光碟都有唯一的條碼，以方便後續分配領取等管理作業（圖 4-6）；此外，光碟內容也經過加密保護，可確保通訊監察資料與內容不會在未經許可的情況下被不當使用。

圖 4-6 光碟產出系統

十二、管理人員可透過證據光碟分配管理系統將週期性證據產生系統所產生的證據光碟依投單申請單位快速分類，以利後續光碟領取作業；同時，並產出當次光碟分配之報表以作為證據光碟數量核對之用（圖 4-7）。

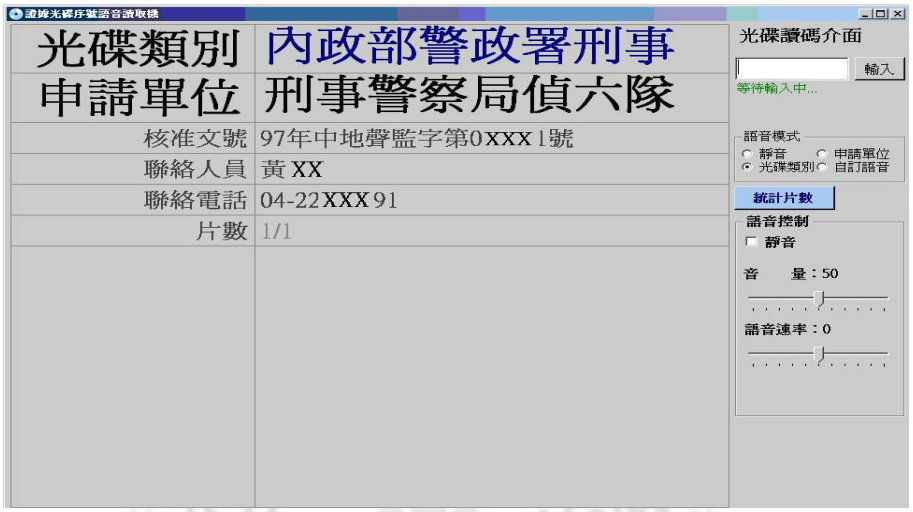


圖 4-7 證據光碟分配管理系統工作畫面

十三、當投單申請單位領取人員至通訊監察科領取證據光碟時，負責證據光碟管理作業的出帶人員，可經由證據光碟領取查詢系統協助處理證據光碟領片管理作業，並產生所領單位之領據供領取人員簽核。出帶人員並可利用查詢功能查詢系統中尚未領取的庫存片數、已領取片數統計及已領片數明細及所需之報表（圖 4-8）。

圖 4-8 光碟所屬單位查詢

十四、當目標監察結束時，通訊監察系統會將該監察目標從電信業者端的監察設備移除。目標移除後，該目標的通聯資料與內容將不會再傳送至通訊監察系統。

十五、司法院與法務部最高檢察署可透過線上稽核機制得知監察目標下線之狀態以及通訊監察產出光碟數量資訊。

十六、當投單中所有的監察目標已達申請之法定監察結束時間，或監察目標因偵查需求而提前結束監察時，投單監察作業將立即終止。

第四節 行動通訊裝置 APP 偵查困境—對具加密功能之通訊軟體監聽的困難

壹、業者配合意願低

以我國目前使用頻率最高前幾名通訊軟體而言，其軟體業者或是主機均設在國外，如 LINE 為韓國公司、WhatsAPP 係美國公司、WeChat

是中國大陸廠商開發、Facebook Messenger為美國公司，主機均在海外，開發軟體商為外國公司，不受本國法律之監督，再因國內外法律有差異，外國公司根本不受約束，例如在美國，任何人均可合法持有槍枝，若我國以持有槍械為申請調閱之理由向 Facebook 申請調取資料，極可能會被以與該國法令有違而拒絕。

貳、APP 發展一日千里

因應使用者需求，或是軟體程式錯誤修正，手機通訊軟體不僅需推陳出新，連舊軟體亦不斷更新。為監察而破解應用程式往往緩不濟急，且偵查單位花費人力、物力破解應用程式後，程式又再更新，形同所有努力付諸流水。且通訊軟體數量驚人、發展蓬勃，而通訊監察建置機關有限，通訊軟體實為現在實務上通訊監察之漏洞。

參、通訊軟體加密破解困難

現今軟體開發商為保護通訊安全，且運算功能提高，為軟體加密輕而易舉，是通訊軟體多以加密方式傳送。以往電信業者依通訊保障及監察法第 14 條，對於執行監聽有協力義務，提供解密金鑰，然而目前國外軟體商並不願提供解密金鑰，一來此舉將降低民眾使用其軟體之意願，另一方面，我國通訊保障及監察法對軟體商是否有強制力，仍有疑義。

網路服務提供業者配合實施通訊監察法源依據，在通訊保障及監察法第 14 條規定，而其具體配合義務，則規定於通訊保障及監察法施行細則第 21 條、26 條，電信事業應使其通訊系統之軟硬體設備具有配

合執行通訊監察時所需之功能，並於執行機關執行通訊監察時予以協助，必要時並應提供場地、電力及相關介接設備。具體配合項目，前交通部電信總局為因應網路科技發展及配合網路犯罪偵查之需要，於93 年 7 月 22 日增列幾項通訊監察項目：

一、網路電話服務

網路電話服務中提供 PC to Phone 或 Phone to PC 服務者需能自業者設備端（如 TDM Switch 或 VoIP Gateway），將依通訊保障及監察法特定監察對象於通訊監察書許可期間內將通話內容、時間及傳送路徑紀錄儲錄或轉送至通訊監察機關。

二、語音單純轉售服務

需能將依通訊保障及監察法特定之監察對象於通訊監察書許可期間內通話內容、時間及傳送路徑紀錄儲錄或轉送至通訊監察機關。

三、電子郵件服務

需能提供依通訊保障及監察法特定之監察對象於通訊監察書許可期間內收、送電子郵件內容、時間及傳送路徑紀錄儲錄或轉送至通訊監察機關。

民國 95 年 10 月 14 日國家通訊傳播委員會復公告非 E.164 用戶號碼網路電話服務（不含不透過業者 VoIP Gateway 直接於網際網路間互相傳輸語音者）、E.164 用戶號碼網路電話服務、語音單純轉售服務及由網際網路接取服務經營者附加提供之電子郵件服

務等 4 種第二類電信事業。

雖然依前揭前交通部電信總局之函文或國家通訊傳播委員會之公告，要求網路服務提供業者配合實施通訊監察之項目已包含網路電信、語音單純轉售服務及電子郵件收、送內容等，惟實務上網路服務提供業者實際配合實施通訊監察項目，仍僅侷限於協助監看電子郵件及上網瀏覽紀錄，對於日益盛行之即時通訊，業者並無法實施通訊監察。

又通訊軟體廠商是否為通訊保障及監察法所稱之「電信事業」?依國家通訊傳播委員會於民國 103 年 8 月 20 日通傳法務字第 10300514490 號函覆法務部之意見，答案似乎是否定。國家通訊傳播委員會認為網際網路服務提供業者(Internet Service Provider, ISP)可分為 4 種：網際網路接取服務提供者(Internet Access Service Provider, IASP)、網際網路平臺提供者(Internet Platform Provider, IPP)、網際網路內容提供者(Internet Content Provider,ICP)及應用服務提供者(APP Lication Service Provider, ASP)，僅 IASP 屬於電信法第 2 條第 5 款所稱之電信事業，因此依國家通訊傳播委員會見解，應用服務提供者並非電信事業，自不受通訊保障及監察法約束，而負監聽之協力義務。

肆、接取速度增加

臺灣 4G 高速上網服務已經上路，加上光纖技術成熟，民眾使用 4G 或是申請 50M 以上寬頻網路已是趨勢，惟使用高速網路傳輸，對於監聽亦是一大挑戰，常有監聽對象以通訊軟體傳送大量影音檔案或是

觀看影音服務等與監聽無關之內容，為保有監聽之完整性，因此此等內容亦一併傳輸至建置機關，造成建置機關設備之負荷，亦無法達成即時截收監聽資料目的。再自大量資料中，篩選過濾可用線索，亦如大海撈針。另如前述，網際網路係以封包方式傳輸資料，若僅欲截取某特定應用程式內容，因封包到達時間不一，該應用程式之訊息截收會有資訊不連貫之情況。

伍、難以定位追蹤與個化加密通訊軟體使用者

智慧型手機多具備兩種上網功能：4G 與 Wi-Fi，加上可選擇之通訊軟體眾多，當監察對象同時使用數種通訊軟體加上不同上網方式，增加監聽之困難度。另現在免費 Wi-Fi 隨處可見，通訊軟體使用者只要連上免費、匿名網路，則對於通訊軟體使用者更是難以追查。

一、服務與接取提供者分離

欲監察對象若使用同一通訊軟體，惟通訊時變換連線方式，如 4G 與 Wi-Fi，則偵查人員需逐層進行資料調閱，先向通訊軟體業者調閱該用戶所使用之 IP 資料，再向該 IP 之接取提供者（如 4G 業者）調閱用戶資料及即時位置。惟通訊軟體業者不願配合提供用戶資料時，即難個化分析何人為該通訊軟體之使用人。

二、跨層 ID 無法對應

各項通訊服務使用者均有不同帳號名稱，而這些帳號名稱常無直接關聯性，如知悉嫌疑人之 IP 位址，但不知嫌疑人係使用何種通訊軟體，或是僅知道通訊軟體之帳號名稱，不知對應之 IP，亦是

徒勞無功。

陸、跨國犯罪使犯罪更難偵查

所謂網路無國界，犯罪者使用通訊軟體犯罪不侷限在單一國家，此種跨國性犯罪，須透過國際合作機制，一來我國處境特殊，難完全突破跨國合作之困境，二是網路犯罪偵辦首重時效，方能第一時間確實掌握犯罪者，若需透過層層公文往返，恐緩不濟急。

上述之對具加密功能之通訊軟體監聽困難需再全盤檢討，本研究重點提出是以司法人員在辦理以行動通訊裝置 APP 為犯罪工具時，就其所遇到之困境做分析檢討。

第五節 通保法規定不夠周延

行動通訊裝置 APP 無法監察之問題是司法人員在偵辦該類型案件的絆腳石，內政部警政署為使辦案人員對該類案件偵辦的人員提供基本的法律保障，於民國 107 年研擬通保法修法，除建議納入安裝軟體之監察方法外，亦配合立法院審議中之電信管理法及數位通訊傳播法草案，將設置公眾電信網路者及數位通訊傳播服務提供者納入準用通保法第十四條第二項，協助執行通訊監察及調取相關紀錄之義務第四項，配合建置相關監察等系統之義務及第三十一條違反義務之罰則之範圍。

壹、通保法的規定

通訊監察為偵辦犯罪之重要利器，應用於犯罪調查已行之有年，近年來，對於隱私權保護意識高漲，我國通訊保障及監察法近年因而多次修正，聲請監察票、調取票之要件更趨嚴格。

另一方向，通訊保障及監察法制定之初，網路尚未發展成熟，惟現今許多犯罪手法皆以網路為主要媒介，以傳統電話監聽為我國監聽之主要模式，已不敷目前辦案所需，是以有必要針對網際網路監察方式及法制進行檢討。

現今網際網路通訊已不再侷限於住處、辦公處所使用電腦上網，而是使用手機通訊、瀏覽網頁，惟因通訊軟體之特殊性，更增添對於加密通訊軟體實施監聽之困難度。

是以，就實務作法，進行分析及辨證，並對加密之通訊軟體之監察方式，及修法建議，並增強科技技術面之實施，以期在日後偵辦犯罪時能更兼顧隱私權之保障與犯罪調查之衡平（王晴玲，2015）。其做法如下。

一、對具加密功能之通訊軟體實施監察，於現行法規範下之可行性，以後門程式進行監聽加密通訊軟體固然可行，惟此舉端賴軟體商之配合，願意在通訊軟體開啟後門程式，就美國而言，甚至以國家安全為由要求蘋果公司、谷歌公司配合，仍引起軒然大波。我國對於通訊監察之方式，並無太多限制，此可就通訊保障及監察法第 13 條第 1 項本文：「通訊監察以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法為之」可見一斑，是以，植入木馬程式使其複製受監察人使用通訊軟體之通訊再回傳建置機關，似符合「截收」之方式，惟使用木馬程式之功能凡幾，有些甚可開啟麥克風及通話功能，如此即有違通訊保障及監察法第 13 條第 1 項但書：「但不得於私人住宅裝置竊聽器、錄影

設備或其他監察器材。」以手機充作竊聽器。或有謂網路監察記載「受監察處所」有其困難，惟在實務上，受監察處所欄位均填載「電話裝機處」，即可表示受監察之客體為何，因此，如以植入木馬程式作為通訊軟體之監察方式，僅需填載通訊軟體裝設處即可（蘇三榮， 2012）。使用木馬程式做為犯罪調查工具，有其優缺點，優點是，以往可以逍遙法外之罪犯，得以因新科技而被逮捕，且可以達到其他監聽工具無法達成之目的。然而，使用木馬程式較有爭議處在於，木馬程式常會截取將整個電腦或手機之資料而取得與本案無關之內容，因此在使用木馬程式上應特別注意受監察客體之特定。

二、行政部門對目前建議修法說明

（一）、近年來國內接連發生重大國際駭客資安事件，例如第一銀行自動提款機盜領案、券商集體遭 DDoS 攻擊勒索案、想哭(WannaCry)勒索軟體案、遠東銀行遭駭盜領案等，國際駭客利用進階持續性威脅(APT)攻擊潛伏監控各政府機關及民間企業，依據趨勢科技調查，臺灣高科技製造業遭駭潛伏時間平均多達六百四十七天，其中最長案例甚至長達四千二百二十二天，政府機關平均遭駭時間約六百七十天，最長案例也有四千一百七十四天，加上國內電子商務客戶資料被盜致民眾遭詐騙案件層出不窮，是類資安事件發生時，因電信事業並無保留連線資訊，於後續案件追查時，

僅能從被害人報案範圍獲取情資，難以有效回溯辨識攻擊者手法、受害情況及未被發現之潛在受害者，無法進行整體損害控管、後續預警及防禦作為，已成為國家安全及資安維護一大隱憂。

（二）、社群媒體及行動通訊裝置APP軟體（例如Facebook、LINE、WeChat等）提供語音通話及文字等通訊服務，因非 電信事業，又屬外國業者，遇有犯罪案件時，難以要求其配合我國執法機關調取相關通信紀錄，致無法具體化通訊嫌疑人之身分或所使用之通信服務，係當前反毒、反詐騙等偵查實務最嚴峻困境之一，連線資訊可由電信事業現有網路設備所產生的網路流量紀錄資訊（例如：NetFlow 功能）取得，係使用者使用期間內發送方(Source)、接收方(Destination)之網際網路位址(IP Address)、通訊埠(Port)、協定(Protocol)、通信日期、通信起迄時間(Start/End Time)、封包大小、封包數量(Number of Packets)，以及功能變數名稱伺服器(Domain Name Server)查詢(Request)與回應(Response)等欄位資訊，未涉及通訊內容，相關資訊目前已被廣泛用於資安維護上。

（三）、澳洲已於 2015 年通過相關法案(Telecommunications Interception and Access) Amendment(Data Retention) Act 2015)，英國亦於2016年通過相關法案(Investigatory Powers

Act 2016)，且根據歐盟促進基本人權署(The European Union Agency for Fundamental Rights)指出，歐盟多數國家都認為資料保存是保護國家安全、確保公共安全及處理犯罪案件有效的途徑，顯見其對於治安維護及資安防護確實有重要意義。綜上所述，修正第二項及第四項，明訂電信事業除配合通訊監察外，亦具有保存及提供通信紀錄及連線資訊之義務，俾符合國家整體資安防護、反恐及治安維護需求。

（四）、另依機關組織法規管轄及業務權責，電信事業之目的事業主管機關為國家通訊傳播委員會(NCC)；郵政事業之目的事業主管機關為交通部，為期明確，有必要將第三項、第五項之交通部修正為目的事業主管機關。

三、現行通保法第十四條的條文規定

通訊監察之執行機關及處所，得依聲請機關之聲請定之。法官依職權核通訊監察書時，由核發人指定之；依第七條規定核發時，亦同。

電信事業及郵政事業有協助執行通訊監察之義務；其協助內容為執行機關得使用該事業之通訊監察相關設施與其人員之協助。

前項因協助執行通訊監察所生之必要費用，於執行後，得請求執行機關支付；其項目及費額由交通部會商有關機關訂定公告

之。

電信事業之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性。

前項協助建置通訊監察系統所生之必要費用，由建置機關負擔。另協助維持通訊監察功能正常作業所生之必要費用，由交通部會商有關機關訂定公告之。

貳、內政部警政署對法務部修正通保法建議說明

修正建議係由警政署提出，主要目的為明確化電信事業協助執行通訊監察、保存及提供通信紀錄、通信使用者資料及網際網路連線資訊之義務，亦有協助建置機關建置及維持相關系統之義務。

另行政院於 106 年 11 月 20 日函請立法院審議之「電信管理法草案」第 9 條及第 22 條增加「設置公眾電信網路者」亦有依通保法相關規定辦理之義務，另同一時間報請行政院審議「數位通訊傳播法草案」第 5 條第 1 項第 3 款亦規定數位通訊傳播服務提供者（網路業者）應就刑事犯罪之偵查、審判或執行等事項依法配合政府辦理，惟現行法規均無明文規定網路業者有配合通訊監察及調取通信紀錄等資料之義務，且考量現行電信法及通保法均無是類主體，爰建議比照電信管理法草案第 22 條第 2 項，新增本條第 6 項，以資明確。

第六節 偵辦第二類電信困境

壹、法令不明確

交通部於民國78年6月起,採用逐項方式開放電信加值網路服務，採用逐項方式開放電信加值網路服務。臺灣電信產業於民國 85 年通過電信三法後開啟電信自由化發展，後隨一連串電信業務開放民營，加上電腦網路與電信科技的快速發展，不管有線或無線寬頻逐漸滲透民眾日常生活當中。其中於民國 85 年 2 月電信法中第 11 條規定將電信事業分為第一類電信事業以及第二類電信事業，交通部並於 86 年 2 月 18 日依電信法第十七條第二項規定，訂定發布「第二類電信事業管理規則」，同時廢止「電信加值網路業務管理規則」。民國 90 年 6 月配合 WTO 修正發布「第二類電信事業管理規則」開放語音轉售服務，包括語音單純轉售服務、網路電話服務及批發轉售服務（如電話卡、公用電話等）等，對於治安之衝擊甚鉅。

依據國家通訊傳播委員會統計資料（97 年 7 月）顯示，臺灣寬頻上網人口數已經突破六百八十萬人。隨著寬頻時代來臨，一般民眾除了一般資料傳輸外（如文字、圖片、檔案、e-mail…等），繼之而來的網路電話與多媒體影像傳輸的方式，即將成為民眾平常生活所不可或缺的溝通方式。因應通訊技術發展，交通部前於 90 年 6 月 28 日開放網路電話服務，提供經營者可透過網際網路傳送與接收所提供之語音服務予國人使用，是為網路電話正式服務開始。

據統計，截至民國 94 年 8 月止，我國電信市場已有八十餘家經營者提供此項服務。行政院財經會報於 93 年 11 月 1 日第五次會議決議

「請交通部儘速完成規劃網路電話服務之號碼核配措施，俾實現有線及無線網路電話服務」，為配合政策目標、引進寬頻創新應用服務，豐富國人選擇電信服務權利，提高市場競爭強度，爰參考日本、韓國及德國等國作法，核配 E.164（為國際電信聯合會對電信號碼編定規格書之編號）用戶號碼予網路電話服務，交通部電信總局業於民國 94 年 11 月 15 日開放 E.164 用戶號碼網路電話服務之申請，核配 070 字頭 11 碼長之 E.164 用戶號碼予網路電話服務。目前合法二類電信業者已達四百多家。

網路電話服務係指透過網際網路所提供之語音服務，由於網際網路具有全球相連之特性，以及易於整合語音、數據及影像訊號進行處理與傳輸之優勢，因此網路電話服務較傳統公眾電話 PSTN 或行動電話服務更能符合整合性(Convergence)、全球化(Globalization)、即時性(Immediacy)與移動性(Mobility)之通訊市場主流趨勢，因此，IP(Internet Protocol)技術未來將成為通信技術主流。

有鑒於IP網路電話與網路影像，由於傳輸成本比傳統便宜非常多，加上寬網路的普及，所以很快吸引大量使用者使用。網路電話服務已經成為語音通信的主流聯繫方式，國際間曾熱列討論相關監理議題。網路電話究竟能不能配合警察機關監聽，是各國防制網路電話流於犯罪溫床的防制重點。隨著網路電話與多媒體溝通工具普及，以往政府仰賴傳統電信監理來預防與打擊犯罪的機制，可能產生非常大的漏洞。雖然國際間針對網路電話服務所衍生的問題，猶處於研究階段，尚未有明確規範，仍應密切觀察國際間之發展，並著手研究相關議題之可

能解決方案。

貳、第二類電信監察之特性與問題

一、隱匿性

網路通訊係在虛擬的網路世界進行，和現實世界申，傳統電話通訊的概念有所不同。然而目前通訊監察書之記載，皆是以現實世界為準，在適用到虛擬的網路世界時，即會發生困難。

故通訊監察的對象很容易利用各種方式隱匿自己的存在，逃避司法機關的偵查。在通訊監察聲請書中，有關監察對象、監察通訊種類及號碼等足資識別之特徵與監察處所等內容即難以確定，例如行為人是利用區域網路所分配的虛擬IP,那麼所能追查到的，便只有對外連線的實體 IP 住址，或者行為人使用的是隨機配發 IP 住址的上網服務，也不能單就 IP 住址直接特定出網路使用者，而必須搭配 ISP 業者所留存的通訊記錄與客戶資料加以交叉比對才可能得知使用者的身分，再者，網路使用人也可能使用隱藏 IP 的軟體，便可能造成追查上的困難。除此之外，行為人亦可能透過後門程式來遠端遙控該 IP 住址所代表的電腦進入網際網路，在這種情形下,該IP住址所代表的電腦只不過是犯罪行為人的「跳板」，並不是真正的通訊來源，即便被得知入侵該「跳板」電腦，入侵之人也可能以斷線等各種方式來擺脫執法者的追蹤偵查而不留痕跡。再者，即便該 IP 住址真的是通訊來源，如果該 IP 住址所代表的電腦是多數人或不特定人所得操作者，例如圖書館、網咖等，

由於使用者眾多，因此亦不能直接由 IP 住址得知何人為真正的網路使用者。

故相較於傳統電話、行動電話等通訊設備，網路通訊具有較高的不特定性，犯罪當事人雙方若每次進行犯罪聯絡時，都在不同的地點上網，且網路犯罪者得利用特殊之電腦技術，使執法者難以在同一節點進行攔截追蹤，如此一來，要選擇哪一個節點進行截取通訊內容，就發生實際運作上的困難，自然加深偵查的困難度。

二、資料重要性

第二類電信業者提供多樣化的上網服務，理論上，只要某一用戶連接上網路後，該用戶的一舉一動，都會被業者所記錄下來，個人在網路上的虛擬行蹤，可說是無所遁形。如此資料量暴增所帶來的衝擊，已遠遠超過傳統通聯記錄所能涵蓋的範圍。如此巨大的量變，也就連帶產生了質變。故網路上的個人資料之重要性，已不能等閒視之。而目前法制關於偵查機關調閱個人資料程式上，顯得太過容易、簡略，既沒有相當的要件要求，亦無專責的監督機關。故這樣的制度，可能必須有所改變。

三、分散性

由於傳統電信網路和 IP 電信網路的架構上之差異，IP 網路的電信監察和傳統電信網路的電信監察在技術上有很大的差異。傳統電信網路是所謂的電路交換(Circuit Switch)網路，通話內容會經

由固定的線路進行傳輸，監聽通話內容必須先判別傳輸所使用的實體線路,然後從實體線路上分接的監聽線路上監錄通話的內容。而 IP 網路則是屬於分封交換(Packet Switch)網路,通訊的內容會分解成多個封包在 IP 網路中傳輸，其封包資料會在發話端和收話端之間直接傳輸，且其傳輸的路徑由 IP 網路中的各個節點決定，語音資料不會經過單一固定伺服器瑞，也無法保證其傳輸路徑。

故網路電話因為 IP 網路交換原理，係以分散式的方式運作，這與傳統電信網路交換係以集中式的方式不同，以往電信監察、警調單位所仰賴之電信監察系統將不足以應付。亦造成傳統電信監理實務上所使用的方法，不足以應付 IP 網路上之新型態犯罪方式，原先適用於傳統語音電信技術監察的規範與機制亦出現不合時宜之現象。警調、監察體系需要針對 IP 網路特性，利用更先進的通訊監理技術加以補強，以便更有效率的來因應 IP 網路普及所衍生帶來的新型態犯罪手法。

若偵查機關以攔截封包之方式執行網路監察，容易攔截到不相干第三人之資訊，引發過度侵害隱私權及不符合最小手段性之質疑。

四、普遍性

所謂普遍性，是指配合執法機關進行通訊監察者，不再僅限於如中華電信公司之傳統電信業者，許多 ISP 業者、網路內容服務提供者(Internet Content Provider)等網際網路業,都可以利用各種網路監看設備，過濾、分析、監看自己系統中的網路狀況，以電

子郵件為例，電子郵件主要在郵件伺服器內進行操作，此種郵件伺服器不僅中華電信可以提供服務，許多民間業者都可以提供相同的服務。另以網路聊天室為例，許多聊天室由於技術層面不高，不需要中華電信等大型電信公司才有能力架設，一般私人亦可成立聊天室，因此網路通訊監察與電話不同，不再由中華電信公司等傳統電信業者獨占。

故在此情形下，需要配合通訊監察之業者數量大幅增加，衍生出第二類電信業者如何配合通訊監察，以及經費負擔之問題。尤其在第二類電信業者的資本額普遍不大的情況下，如何配合犯罪偵查，又不至於讓第二類電信業者負擔過重，是個重要問題。

五、跨國性

由於網路無國界的特性，許多網路上犯罪可能存在於單一國家，但也可能不再侷限於某一特定國家或某一特定區域，而跨越國界成為跨國性的犯罪，例如跨國性的毒品案件偵查，販毒者可能分別身處在 A 國與 B 國，但是通訊監察的節點可能必須在第三國 C 國。針對此種跨國性的犯罪，必須透過國際合作的機制，才能在第一時間確實掌握犯罪者的動態。因此，傳統的犯罪偵查模式在網路世界中已經逐漸無法完全適用，若無法突破跨國合作之困境，網路將可能成為犯罪的天堂。

六、不同領域的競合

第二類電信服務通訊監察涉及許多層面，有賴不同領域間的

合作，傳統電信通訊監察法規多著墨在第一類電信服務，然而隨著現今社會趨勢，網路電話多媒體溝通工具蔚為風潮，相關通訊監察法規制定後，方有合適法源及程式可遵守；由於網路電話與傳統電信運作方式大不相同，因應偵查實務進行，現行通訊技術與設備，亦需發展出進一步系統化的通訊監察技術；有完善法源依據及先進設備的支持，偵查才得以順利展開。

七、不同利益的拉鋸

第二類電信服務通訊監察亦涉及不同利益問的衝突，以犯罪追訴觀點出發，第二類電信服務的特色使得通訊監察包含範圍越廣，越有利於犯罪偵查與起訴，然於此就進逼人權保障的壁壘，侵犯人民隱私與通訊自由；再相對應電信經營業者，為配合犯罪偵查需建置與維持系統，經費負擔是否過重，又該如何平衡；電信經營業者為配合檢察機關或內部分析,保存大量用戶私人資料，是否有侵害個人隱私之嫌；相對地若追求人權保障的完整，犯罪追訴難度勢必增加，三者之問的利益拉鋸就此而生。

參、預期達成之目的

傳統電信監察機制只針對第一類電信業者所經營的語音業務與系統進行監察。但科技進步，IPBased 的語音電話監察技術卻與以往第一類電信語音服務的監察技術極大不同，且難度頗高，因為 IP 網路交換原理是分散式的，並不同於以往第一類電信語音服務所使用的系統是集中式的架構。加上 IP 網路服務多樣性，遠遠超出以往第一類電信服

務的電信系統。

因應 IP 電信網路技術發展現況與未來趨勢，進行 IP 電信網路監察技術評估與相關現有法制分析，針對現有電信網路監察法制與程式機制，因為 IP 網路發展而不足之電信網路監察法制與程式機制，提出相關建議。

肆、目前辦理第二類電信服務通訊監察案困境

歹徒為阻礙司法單位追查其行蹤，會利用人頭或偽造身分證至電信公司申請固網電話、080 多功能免付費電話及行動電話，再利用電信公司便利客戶之漏洞，將前述電話以多層次轉接方式，或自行組裝行動電話轉接器架設於固定機房及行動機房，將電話轉接至歹徒之犯罪場所的行動電話中，甚至大陸沿海地區，因為行動電話通聯紀錄所顯示基地臺位置為一定範圍內，無法正確顯示詐欺集團之犯罪處所，因此，造成司法單位偵查上極大困擾（許芳雄，2009）。

工研院研發的通訊軟體揪科(Juiker)，曾經遭立法院爆出是使用 Juiker（揪科）的「金色會員」還可用較便宜費率撥打國際電話、行動電話，主打企業市場，遭立法委員質疑源思科技公司沒有申請第二類電信執照卻無照跨足第二類電信服務疑慮，引發很多爭議。當時這個案發之後 NCC 表示，包含現在許多通訊軟體，都有提供語音通話功能，上述軟體更可轉打一般電話，因牽涉長遠監理方向，希望能釐清究竟這類服務屬於資訊還是通訊服務，過去租用第一類電信業者線路提供服務的第二類電信服務定義，未來執行上會有困難之處。

而 NCC 在討論上述「以應用程式(APP)提供網路電話服務，涉未

經許可擅自經營第二類電信事業案件審理原則」一案，會中決議辦理公聽會事宜；至於有關工研院及源思科技以應用程式(Juiker)提供網路電話服務，涉未經許可擅自經營第二類電信事業案，待後續公聽會辦理完竣再行處理。NCC 曾表示，在傳統電信管制中，要求第一類電信及特定第二類電信事業承擔較重的普及服務及配合政府各類公共政策等公共責任，其理由無非以第一類電信事業為特許事業地位而課予公共責任，第二類電信事業亦是因符合嚴格條件而取得許可，因而課予公共責任，兩者均以相當嚴格而不易取得的參進市場條件間接限制合格事業家數。

鑒於目前通訊傳播技術及相關應用的快速發展，第二類電信事業所提供極多樣化的即時通訊及影音串流等應用皆可補充甚至替代原僅有電信事業所提供的電信服務。傳統電信管制思維僅針對電信業者課予公共責任，目前已難以繼續維持。

因此，NCC 也研訂匯流五法相關法案，對於不涉及路權、頻率及號碼等資源的各種通訊傳播服務及基礎設施，除資安、消保等一般義務及責任外，原則上均大幅解除管制。

NCC 認為，以往傳統管制所立基的封閉型公眾電信交換系統及實體網路架構，已非唯一區分電信（或一般通訊傳播）服務種類的主要判斷根據，所以傳統不分重要性高低全面納管的細密規範，無論必要性、正當性及合理性均日益降低，因此，應該要比照國際同儕通訊傳播監理機關與時俱進，不宜再一味沿用過去監理方式，但是，有關第二類電信事業管理規則，規定了公眾電信網路仍以語音為主要服務型

態時所訂定,且規範該等服務係藉由第一類電信事業所建構實體網路，以批發或轉售形式,於服務層面開放競爭,藉以吸引更多消費者使用；但是，基於通訊傳播監理機關不能扼殺所有通訊傳播的創新服務，而以過時的事業別電信管制模式強加於各種創新應用服務，阻礙產業發展及消費者選擇，觀察通訊傳播匯流趨勢，該規則亟需與時俱進。

第七節 偵辦以行動通訊裝置 APP 為犯罪工具辦案困境

壹、法制未有明確規範之困境

科技進步，行動通訊裝置 APP 已取代以傳統語音傳輸及簡訊傳送之市話與行動電話功能，確實給消費者帶來許多便利性，但是也引起犯罪者不法之意圖，因為行動裝置可作為其聯繫犯意之工具，因而形成了各類犯罪溫床,也成為歹徒用以躲避司法人員偵辦案件之避風港，遂成為司法人員實務上偵辦案件之困境,但是,就如同前述章節所述，因目前國內的相關法制未有明確規範，且對這類高科技犯罪之監察系統建案未能順利建立,導致遇到這類案件就給案件偵辦人員帶來困擾，也給辛苦辦案的司法人員帶來痛苦打擊，在網路犯罪快速增長，手法快速變化、科技化、專業化、與全球化時代，網路犯罪已為警政工作的嚴重挑戰之一。我國高科技犯罪其中又以網路詐欺最為嚴重，只要擁有社群網路服務（例如 Facebook）或者網路即時通訊服務（例如 LINE)，幾乎人人接過詐騙訊息，另外，如比特幣洗錢、網路勒索、竊盜個資等。而高科技犯罪偵查之一重點為知道傳送訊息者之真實身分（個化使用者）與他目前的地理位置（追蹤他的位置)。

但由於各式各樣社群網路、網際網路應用服務(APP)的大量使用，在運用加密、匿名網路、且 APP 服務提供者大多位於國外及雲端儲存下，數位偵查與鑑識已愈發困難，治安機關面臨難以透過封包解譯或網路接取服務提供者調閱通聯紀錄而追蹤個化使用者之困境。因此，有必要從不同的出發點，發展新的數位偵查與鑑識方法。

貳、偵辦即時通訊與分即時通訊之困境

目前歹徒常用的行動通訊裝置 APP，為雙方犯意之聯繫傳輸的方式，可分為即時通訊與分即時通訊兩種，如果是以傳統的語音通訊則已為網路通話所取代，簡訊傳送方式被文字的傳輸所取代，司法人員在實務上偵辦案件所用之案件偵辦方式各有所不同，尤其網路的語音通話行為往往稍縱即逝，如未掌握時間實施監聽作為，過了通話時間其通話資料將無法保存，這樣的通話方式，就稱之為即時通話，但如果是以行動通訊裝置 APP 的文字之訊息來作為其訊息的表達平臺，那麼其犯意之聯繫就可能留存在行動裝置內，以及雲端或是伺服器內，所以對司法人員辦理案件在蒐集罪證一定要瞭解案件之種類與資料，以及其存取之空間等，如此對於案件之偵辦才有所助益，司法人員在偵辦以智慧行動通訊之犯罪案例中，發現到以行動通訊裝置 APP 為犯罪工具是目前最常使用之聯繫方式，而辦案人員亦在最近發現的是歹徒如欲以語音通話，大多不在通話內容中敘述犯案內容，另外就是歹徒會用同一電話，但是以不同門號之 SIM 卡及人頭機，藉以規避司法人員之追辦，但這種狀況目前都變少，歹徒改以行動通訊裝置 APP 為其犯案之聯繫，上述情形並非歹徒不在犯案，而是轉移聯繫之管道，

改以行動通訊裝置 APP 之 LINE 或 Facebook 等通訊軟體犯案。

目前案件偵辦上可分為以監聽方式偵查稱之為主動偵辦，另一為以就嫌犯所保留之與犯罪有關之資訊為被動之偵查（圖 4-9），但因國內目前並無專法，只能以通保法及刑訴法辦理，至於以行動通訊裝置 APP 犯案者，則法令未明，導致辦案人員無以適從，對嫌犯之手機內容，刑訴法之搜索扣押為另一找尋犯罪事證之方法，如以通訊監察方式，則以通保法為主要適用法律，刑訴法著重於網路虛擬空間，另通保法則著重於載臺之電磁紀錄，不同於二法公佈施行之初期，行動通訊裝置 APP 尚未出現，如直接以現行之法律套用，定有所疏漏。

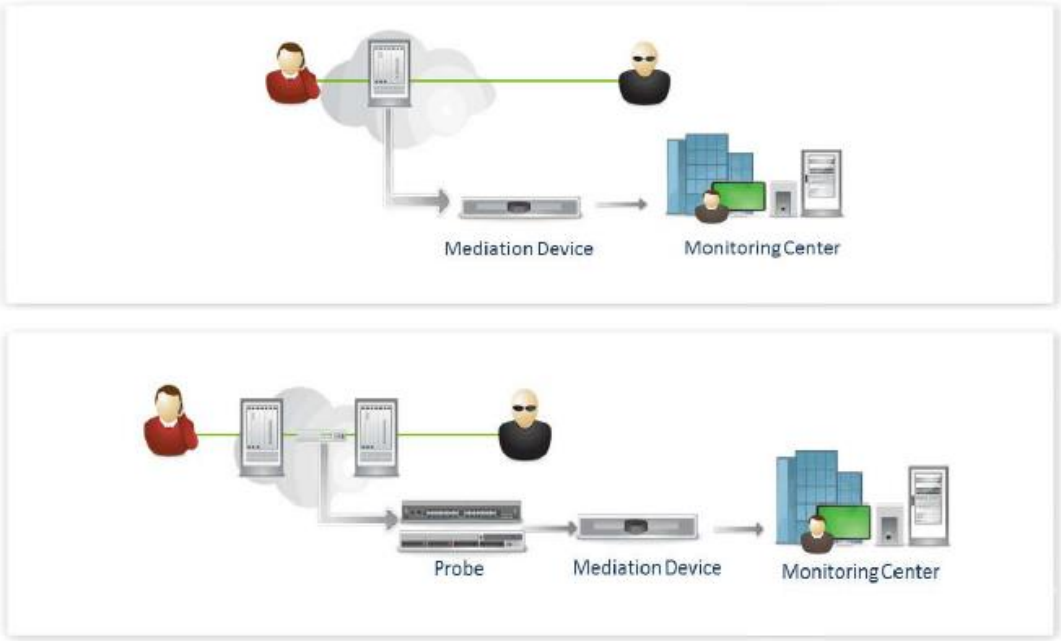


圖 4-9 主動式監察與被動式監察

第五章 實驗平臺與實證平臺建置

本章先分析有關行動 APP 通訊軟體監察技術實驗平臺，再分析行動通訊裝置 APP 解譯（密）技術之社群網路偵查暨鑑識能量、遠傳電信、臺灣大哥大及臺灣之星 4G 後端通訊監察系統、通訊監察內容分析平臺、建置 M 化系統、可攜式封包解析設備建置系統等針對以行動通訊裝置 APP 為犯罪工具之因應措施。

第一節 建置監察行動 APP 通訊軟體實驗平臺

壹、行動 APP 通訊軟體監察技術實驗平臺

行動 APP 通訊軟體監察技術實驗平臺建置案，其專案範疇為因應行動 APP 加密通訊日益風行而建構新一代通訊監察系統，此平臺為研究與驗證相關技術為主，其內容說明如下：

一、因應行動 APP 加密通訊的衝擊，研究新一代合法通訊監察的架構與機制：

在保障人民秘密通訊自由不受非法侵害，並確保國家安全，維護社會秩序前提下，研究如何將行動 APP 加密通訊反制技術，納入現有歐洲電信(ETSI)、3GPP 及 3GPP2 之通訊監察標準與架構。研究行動通訊裝置 APP 實際可行的通訊監察技術。

二、針對大多數行動通訊裝置 APP 皆有加密機制，研擬解決方案：

由於裝置效能大幅提升，保密通訊藉由簡單的程式碼即可以完成，

應用開發者為確保通訊的安全性皆會內嵌加密技術，使得大多數的 APP 皆有加密機制。傳統通訊監察對於加密機制會要求電信業者提供解密金鑰，然大多數 APP 提供者並不會願意提供金鑰，因此執法機關難以解析其內容，如此低成本的加密通訊，已成為犯罪者躲避通訊監察（偵查）的安全通訊管道，本平臺將探討反制行動 APP 加密通訊是否可行，分析現在所有的技巧是否可以用來獲得破解加密的通訊，探討其優缺點，以及未來實務上施行的前提條件，研擬面對加密機制的反制策略。

貳、社群網路偵查暨鑑識技術實驗平臺

社群網路偵查暨鑑識技術實驗平臺建置案的範疇，為建置一個社群網路偵查暨鑑識技術實驗平臺，以因應目前行動通訊環境與社群網路服務的複雜多變。本研究平臺以 3G 網路為例，其系統架構、資料處理流程，與系統元件功能如下（如圖 5-1）。

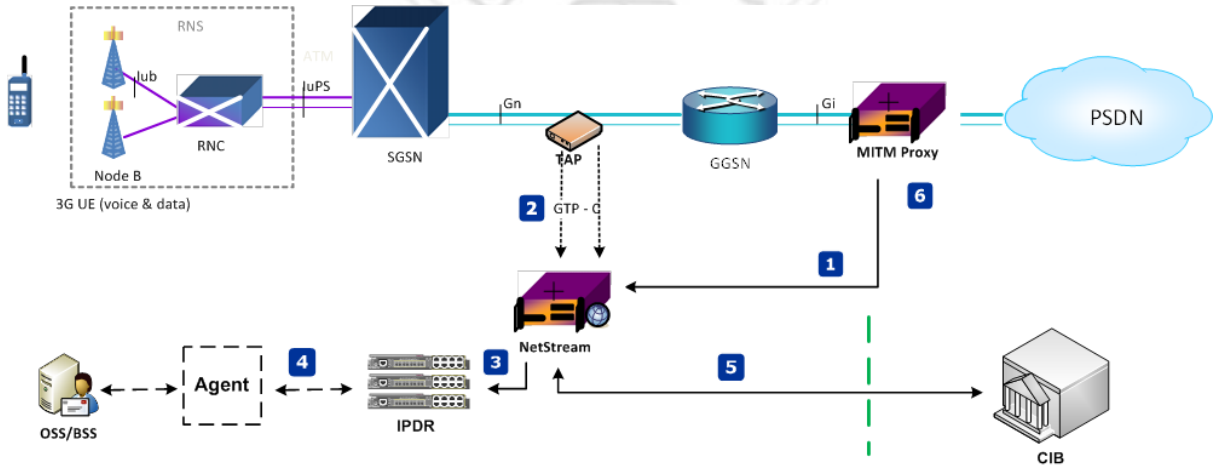


圖 5-1 社群網路偵查暨鑑識技術實驗平臺架構圖

一、3G 行動裝置（UE，User Equipment。如：智慧型手機）上網的過程中，資料換以無線電(Radio)形式傳送到基地臺(Node B)，經過 RNC (Radio Network Controller)再到 SGSN(Serving GPRS Support Node)，最後經由 GGSN(Gateway GPRS Support Node)進入 PSDN (Public Switched Data Network. Internet 即為一種 PSDN)；反之，從 PSDN 往 3G 行動裝置的資料則以相反的順序傳遞。

二、在 3G 核心網路架構中 SGSN 與 GGSN 之間是以 GTP (GPRS Tunnelling Protocol)協定來封裝與傳輸網路封包，而 GTP 通訊協定可以再細分為負責控制訊號傳遞的 GTP-C (GTP Control Plane) 協定與負責傳遞使用者資料的 GTP-U (GTP User Plane)協定。可以從 GTP-C 中獲得行動裝置以 MSISDN 或 IMSI （即 3G 接取網路的 Access ID）對 GGSN 註冊取得 IP 位址的溝通資訊。而 GGSN 與 PSDN 網路中則是行動裝置實際上網的 IP 封包。

三、上述架構圖中不屬於 3G 網路元件的模組，包含 TAP、NetStream、IPDR 等為本案的交付項目，而 MITM Proxy 則為刑事警察局「行動 APP 通訊軟體監察技術實驗平臺建置暨驗證計畫」成果中對應功能的設備，以期讓經費與資源最有效地利用與發揮。TAP 的功能主要是將網路封包複製一份下來，並往 NetStream 傳送。

四、NetStream 具備封包分析、紀錄 DNS 查詢紀錄、TCP 連線紀錄、網路應用層帳號與 IP 對應紀錄、以及使用者管理與查詢介面等功能。IPDR 則負責儲存 NetStream 解析出來的各種紀錄 （DNS 查

詢、TCP 連線、網路網路應用層帳號與 IP 對應等） 並提供快速的讀取介面。

MITM Proxy 提供封包 Pass Through 介面將 GGSN 與 PSDN 之間的 IP 封包複製一份給 NetStream 處理；此外，並提供以中間人技術將特定目標的加密封包解密成為明文(Plaintext)資料的功能。Agent 主要負責與電信業者端的 OSS/BSS 系統整合，取得用戶的接取資訊(Access Information)紀錄。

參、戰術型 WiFi 網路 APP 偵查系統規劃與驗證計畫

「戰術型 WiFi 網路 APP 偵查系統規劃與驗證計畫」之架構設計與規劃，為了延伸「行動 APP 通訊軟體監察技術實驗平臺建置暨驗證計畫」獲得的成果，在其基礎下開發各種進階的技術，能涵蓋更多的行動 APP 通訊軟體，進而研提可以實際協助犯罪偵查的工具及平臺並進行概念驗證(Proof of Concept, POC)。

一、研提可在 WiFi 網路下之行動 APP 通訊偵查系統規劃：

可在 WiFi 網路下之行動 APP 通訊偵查系統，依法執行，以提升犯罪偵查效能。並針對已經可以解密的行動 APP 通訊軟體（包含：LINE、Facebook / Facebook 即時通、Skype、Gmail、Chrome / Firefox、Yahoo Messenger、WhatsAPP、WeChat 等），進行解譯(Protocol Decoding)，使通訊內容可以方便閱讀(Human-Readable)。

二、提出可針對行動網路 APP 加密通訊協定的反制方法：

兩大類針對行動網路 APP 加密通訊協定的反制方法分別為：

（一）、針對 SSL/TLS 加密通訊技術的反制。

（二）、使用其他加密通訊技術的反制。

能涵蓋更多的行動 APP 通訊軟體(More Mobile APPs, Especially VoIP)。其中，針對 SSL/TLS 加密通訊技術的反制方法主要是透過Inline佈署中間人代理伺服器方式達成；而針對其他加密通訊技術的反制的方法，則是以反編譯/反組譯搭配逆向工程，分析出行動網路 APP 的行為特性，再加以突破。

肆、行動裝置及其應用程式安全性分析運用雛型實驗平臺

「行動裝置及其應用程式安全性分析運用雛型實驗平臺」之架構設計與規劃，以「行動 APP 通訊軟體監察技術實驗平臺建置暨驗證計畫」及「戰術型 WiFi 網路 APP 偵查系統規劃與驗證計畫」已經獲得之成果,在其基礎下針對常見的行動裝置及其應用程式進行安全性分析，研究已知的安全性問題是否仍存在，研提可以實際協助犯罪偵查的工具及平臺並進行概念驗證(Proof of Concept, POC)。

經由系統架構（如圖 5-2）顯示。包括規畫建置於刑事警察局端的行動 APP 安全性分析平臺及移動式分析工作站，並整合前案交付之 WiFi 戰術型系統，以驗證系統在實驗環境中可執行通訊監察功能。

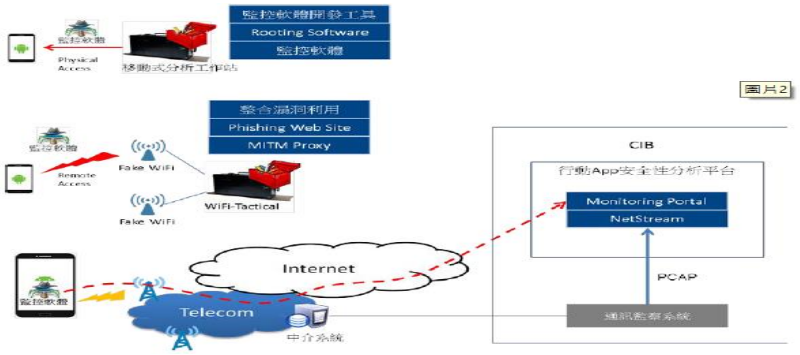


圖 5-2 行動裝置及其應用程式安全性分析運用雛型實驗平臺系統架構圖

實驗平臺主要功能分述如下：

一、行動通訊裝置 APP 安全性分析平臺

（一）、CIB 通訊監察系統整合

行動 APP 安全性分析平臺可以整合 CIB 通訊監察系統，可以透過 Pcap 匯出工具取得監察目標的原始網路封包，對監察目標進行網路封包鑑識等偵查行動。

（二）、網路封包鑑識

行動 APP 安全性分析平臺具備網路封包鑑識模組，可以對監察目標的網路封包進行分析，對監察目標的網路行為進行偵查，收集關於監察目標的重要情資，作為後續評估目標手機及 APP 安全性評估的依據。

（三）、目標監控管理系統(Monitoring Portal)

偵查人員透過移動式分析工作站或者 WiFi 戰術型系統所將監控軟體（包含經過逆向工程修改過的行動 APP 或特製的監控程式） 以不同的手法植入目標手機（如：社交工程、

取得實體手機、或手機的安全性漏洞等)。

二、移動式分析工作站

移動式分析工作站主要提供研究人員分析 Android 裝置、軟體開發、以及測試的環境，其中包含網路上可取得的免費工具、商業授權軟體、以及經逆向工程修改之行動 APP。

三、WiFi 戰術型系統整合

如果無法實體接觸監察目標的行動裝置，則必須透過遠端存取的方式進行監控軟體安裝，這時可以整合 CIB WiFi 戰術型系統，利用 Fake WiFi AP 攻擊，強制監察目標透過 WiFi 戰術型系統連上網際網路，並進行中間人攻擊 Man-in-the-Middle (MITM) Attack，透過 MITM Proxy 與網路封包解譯/還原模組，將 Https 加密通訊解密後，再解譯與還原，可以進一步取得監察目標常用的網路帳號，如 Email 帳號、Facebook 帳號等個人資訊。

伍、跨境戰術型 IP 通訊監察系統

戰術型監察系統的特性為可以根據實際需求進行系統的佈署，其設計為根據 2 家電信業者跨境 IP 骨幹網路現況，於臺灣固網佈署 1 套跨境戰術型 IP 通訊監察系統，於新世紀資通佈署 3 套跨境戰術型 IP 通訊監察系統，當中包含 2 臺網路封包鑑識與 IP 連線資料保存伺服器，重點說明如下：

一、高速封包過濾設備提供 4 臺，每臺具 4 個 10Gbps 埠及 20 個可選擇為 10Gbps 或 1Gbps 埠的設備，每個埠也可以根據實際需求，設

定為輸入埠或輸出埠，超出 RFP 要求，扣除必要的網路連線埠與輸出埠，每臺高速封包過濾設備最多可以規劃 18 個輸入埠，提供 9 組 Tx+Rx 的 10Gbps 封包輸入介面。

二、本系統可以透過模組化方式擴充或升級，且提供符合 ETSI TS 102 232-1 之標準介面，以對未來整體建置完成後之後續擴充所造成干擾降到最低，因此規劃的戰術型 IP 監察系統，包含 2 個子系統，分別是戰術型 IP 監察仲介系統與戰術型 IP 監察資料管理系統，原因就是戰術型 IP 監察仲介系統與戰術型 IP 監察資料管理系統之間是透過符合 ETSI TS 102 232-1 之標準 HI 介面進行介接，以因應未來大規模建置跨境 IP 通訊監察系統時，可以符合通訊監察科的規劃，方便系統擴充。

三、網路封包鑑識與 IP 連線資料保存伺服器，專門用來接收自高速封包過濾系統產生的針對性攻擊封包，並透過知名的 IDS 軟體 Snort 即時進行針對性攻擊分析，即時產生 Alert，建置有專門的資安與威脅分析，可提供一些 APT 攻擊分析規則，例如以 SMTP、FTP、HTTP、TFTP、IRC、SSDP 等通訊協定 Port 加上已知的特定中繼網站清單組合而成的條件為規則。除了針對性攻擊行為分析，近年來社群網路 APP 的盛行也同時伴隨產生透過社群網路 APP 的隱匿性而進行的網路犯罪，網路封包鑑識與 IP 連線資料保存伺服器也同時安裝協力廠商既有的 IP 連線資料保存系統 IPDR，可以針對特定社群網路 APP 的 Server IP 進行過濾，保存所有 DNS 紀錄

與特定社群網路 APP 的 IP 連線紀錄資料，可以用來進行社群網路 APP 使用者帳號與實際連線 Client IP 的對應分析。

四、根據臺灣固網、新世紀資通的跨境機房的網路架構與路由複雜度，將四套跨境戰術型 IP 通訊監察系統，分成臺灣固網 1 套，新世紀資通 3 套的方式去佈署。

五、臺灣固網針對跨境網路設備規畫採用 Network Traffic Monitoring 設備，該設備可以透過指令進行封包過濾的條件，過濾的條件設定的參數以 IP 位址為主，且臺灣固網可以配合將符合監察目標條件的封包過濾後分別從中和機房與內湖機房各 2 個 10Gbps 的 Ports 導出，且集縮至內湖的 IDC 機房本案交付的設備機櫃，因此只需 1 套即可。

六、基於上述說明，規劃於臺灣固網的跨境戰術型 IP 通訊監察系統佈署（如圖 5-3）。

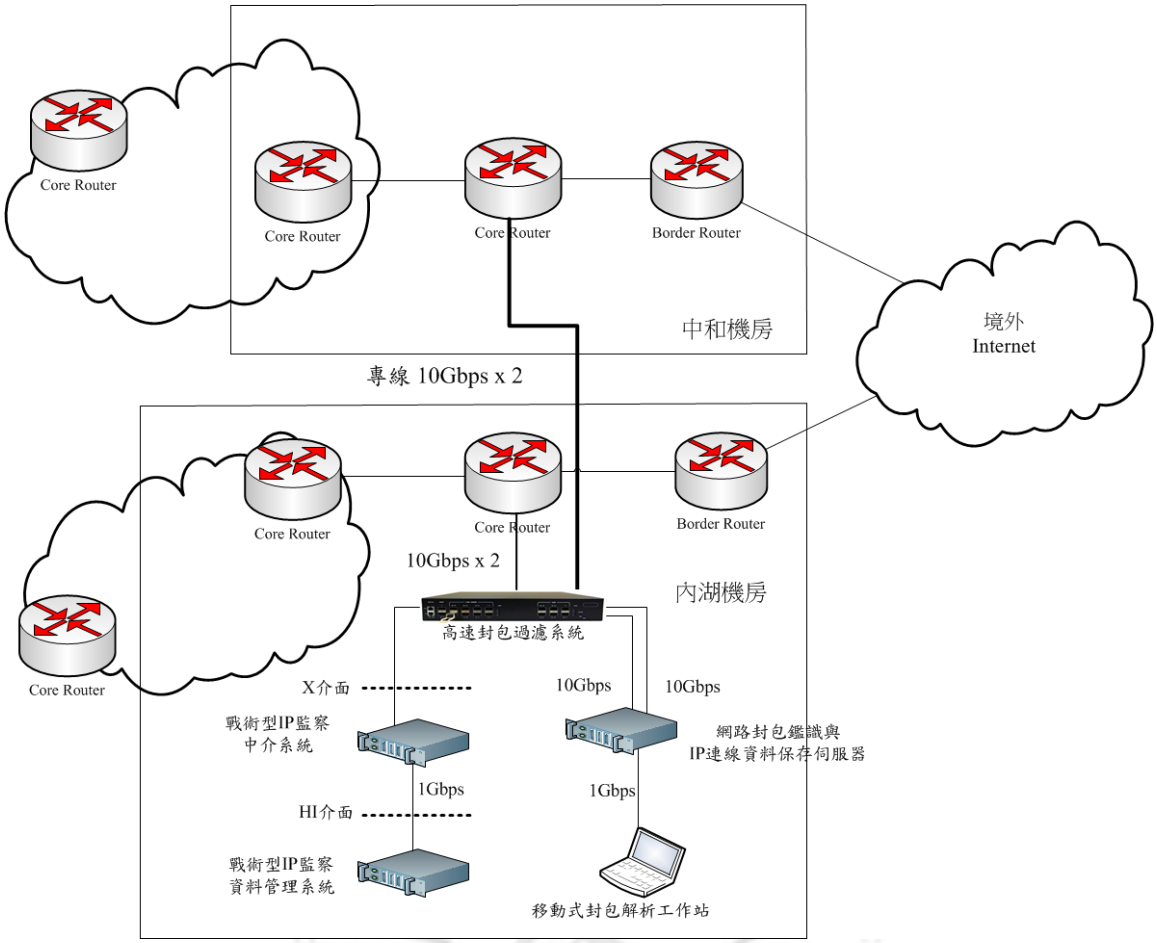


圖 5-3 臺灣固網跨境戰術型 IP 通訊監察系統佈署規劃圖

七、新世紀資通針對跨境網路設備並無規畫 Network Traffic Monitoring 設備，只規劃自行建置 Optical Passive Tap 且可以配合將符合監察目標條件的封包過濾後，因此需依賴交付的高速封包過濾系統進行封包過濾的功能，並且新世紀資通跨境的 10Gbps 線路總數超出本案交付設備的容量且路由複雜度，同一 Session 由內往外的 IP 封包與由外往內的 IP 封包可能會走不同的路由，如果同一 Session 的 2 個路由分別被 2 臺高速封包過濾系統進行過濾，而分別被不同的戰術型 IP 監察系統監察，就會造成某個監察 Session 的封包只攔截到到由內往外或由外往內的封包。

八、基於上述原因，本案規畫建置於新世紀資通的系統可以很彈性的將 3 套系統完全整合成 1 套系統佈署在一個機房，包含 1 臺網路封包鑑識與 IP 連線資料保存伺服器，如圖 5-4。

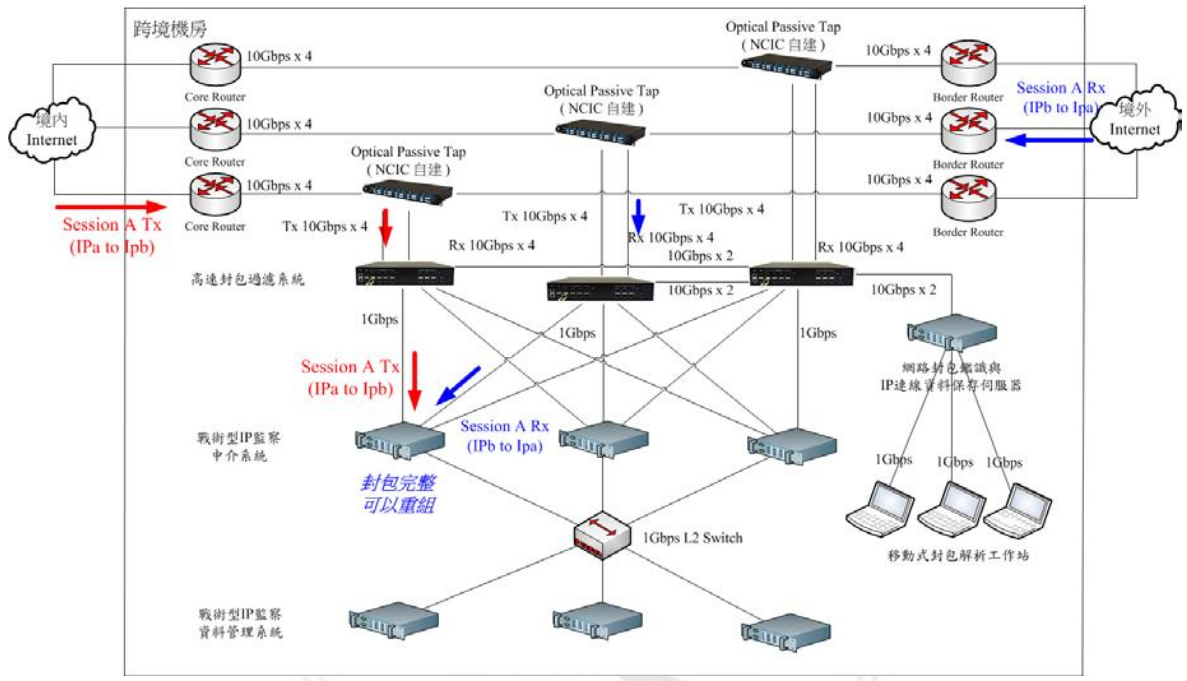


圖 5-4 新世紀資通跨境戰術型 IP 通訊監察系統佈署規劃圖

九、3 臺高速封包過濾系統針對通訊監察的部分，可以同時接受 3 臺戰術型 IP 監察仲介系統的監察目標設定，所以如果某一個監察目標的 Session 經由不同的高速封包過濾系統，最後會回到同一臺戰術型 IP 監察仲介系統。

十、此外，3 臺戰術型 IP 監察仲介系統可以整合成一個具備 High Availability、Load Balance 的 Master/Slave 架構的監察仲介系統，3 臺戰術型 IP 監察仲介系統都可同時擔任 Master 與 Slave 角色，但同一時間只其中 1 臺同時擔任 Master 與 Slave，另外 2 臺只擔任

Slave，當擔任 Master 的 Server 異常時，可以改由另一 Server 擔任 Master，監察目標的分配是由 Master 平均分配給 Slave，由 Slave 負責對高速封包過濾系統進行監察目標的設定與監察結果的接收與轉換成 HI 介面的處理。

十一、3 臺戰術型 IP 監察資料管理系統可以整合成具有 Target-Based 的 Load Balance 架構的監察資料管理系統，具備集中管理、集中儲存、集中使用者操作介面、集中監控的運作方式。未來戰術型 IP 監察資料管理系統甚至可以部署在通訊監察科機房，並與既有的通訊監察系統無縫整合。

十二、3 臺高速封包過濾系統針對網路攻擊分析的封包與社群網路 APP 連線資料的封包，則會先集縮至其中 1 臺高速封包過濾系統，再導給網路封包鑑識與 IP 連線資料保存伺服器。

陸、提升新世代社群網路偵查暨鑑識能量計畫（建置雲端與 IP 定位資料保存規範機制實驗平臺）

在進行網路犯罪偵查時由於眾多社群網路、APPs 服務提供者大都位於國外，因此用戶資料與使用紀錄調閱不易。本案延續建置之平臺結果，藉由刑事局已建置「跨境戰術型 IP 通訊監察系統」於電信業者網路之重要節點搭配儲存 IP 通聯紀錄，建構雲端與 IP 定位資料保存規範與機制，以輔助執法機關在雲端世界定位與追蹤目標之執行，提供社群網路或 APPs 帳號通信紀錄、IP 個化與追蹤定位之功能，以利符合實際辦案之環境。

本案將支援固網網路架構，透過在固網實驗網路環境下驗證系統功能，進行大量資料分析與過濾，不得影響（或影響微乎其微）網路服務品質，且尖峰流量每秒超過 10Gbps，快速封包過濾。同時考量個人隱私的保障，在不違反個資法的前提下，兼顧犯罪偵查的需求與個人隱私的保障（如圖 5-5）。規劃重點如下：

一、整合刑事警察局之「跨境戰術型 IP 通訊監察系統」。

二、於固網業者網路之重要節點儲存 IP 通聯紀錄。

三、提供社群網路或 APPs 通信紀錄，以符合實際辦案之環境。

四、整合並延續過去所施作之技術與系統。

五、支援固網網路架構，研究團隊須在固網實驗網路環境下驗證系統功能。

六、尖峰網路流量必須超過 10 Gbps 以上的網路負載能力。

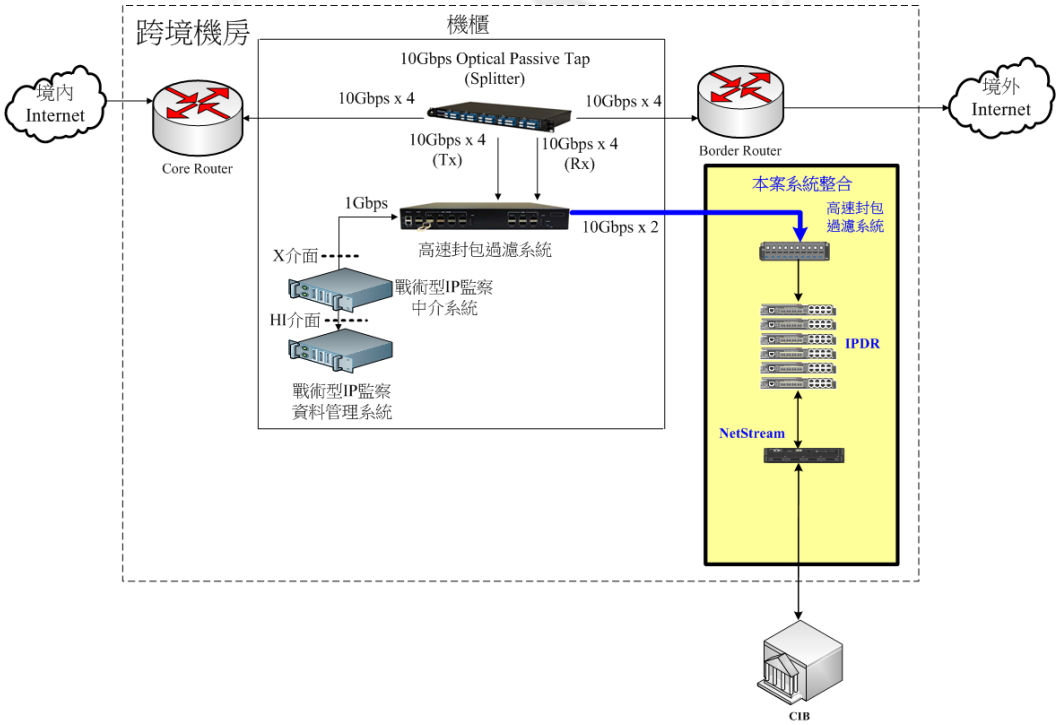


圖 5-5 支援固網網路架構系統整合示意圖

本案將透過高速封包過濾設備將 2 個 10Gbps 實體埠輸入的封包資料流經過 IP/Port Based 的過濾條件(Filter Rule)，進行過濾(Filter)後（如圖 5-6）再以 Session-Based 負載平衡方式分流(Dispatch)至 18 個 1Gbps 的實體埠輸出至 IP 資料保存系統，過濾條件(Filter Rule)則透過 NetStream 對高速封包過濾設備進行設定（如圖 5-7）。

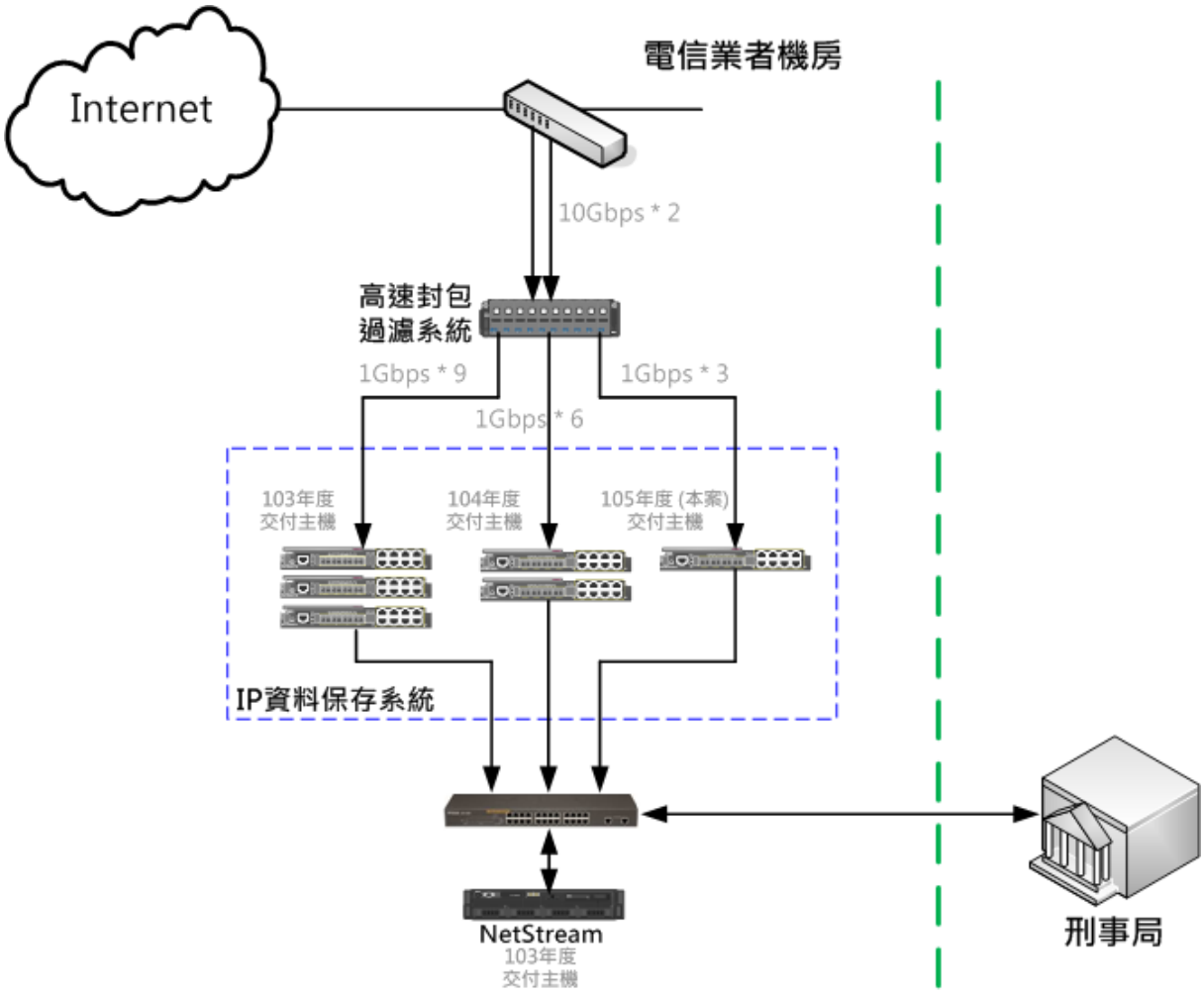


圖 5-6 封包過濾系統整合示意圖

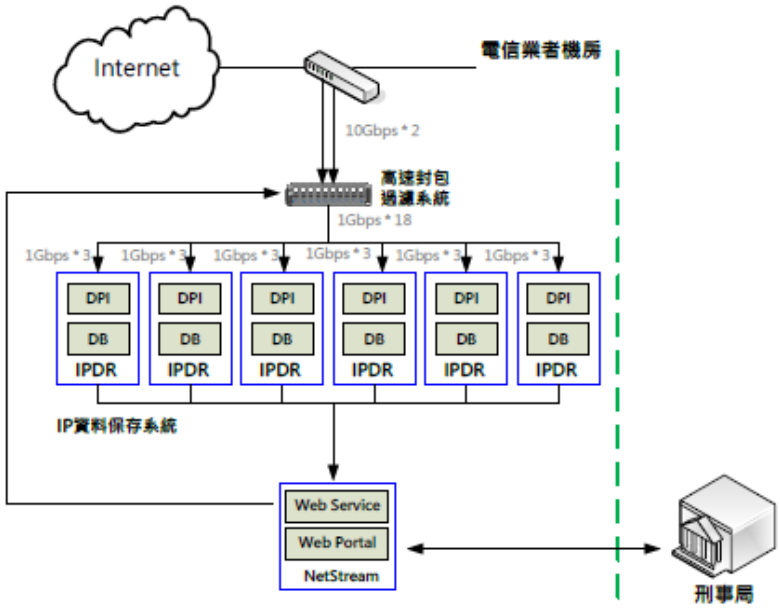


圖 5-7 IP 資料保存

上述架構圖中，NetStream 及 IPDR 為刑事警察局「建置社群網路偵查暨鑑識技術實驗平臺(SNIF-1)」及「建置驗證大量資料分析技術與過濾機制平臺(SNIF-2)」成果中對應功能的設備，以期讓經費與資源最有效地利用與發揮。NetStream 具備使用者管理與查詢介面等功能。高速封包解釋系統具備封包分析、記錄 DNS 查詢紀錄、TCP 連線紀錄、網路應用層帳號與 IP 對應紀錄等功能。IPDR 則負責儲存高速封包解譯系統解析出來的各種紀錄（DNS 查詢、TCP 連線、網際網路應用層帳號與 IP 對應等）並提供快速的讀取介面。

第二節 偵查與分析平臺

壹、社群網路偵查暨鑑識能量建置

計畫重點描述

由於各式各樣社群網路、網際網路應用服務(APP)的大量使用，在

運用加密、匿名網路、且 APP 服務提供者大多位於國外及雲端儲存下，數位偵查與鑑識已愈發困難，治安機關面臨難以透過封包解譯或網路接取服務提供者調閱通聯紀錄而追蹤個化使用者之困境。因此，有必要從不同的出發點，發展新的數位偵查與鑑識方法。

本案延伸 103~105 研究（如圖 5-8），提出自動化社群網路資訊分析實驗平臺（如圖 5-9），發展 Tor 匿名網路之偵測，及 IP 連線資料保存之應用，期能發覺歹徒真實身分。

圖 5-8 103~105 年度建置計畫

一、社群網路偵查暨鑑識能量建置目的

為透過 IP 連線資料保存 （本研究或可稱為網際網路連線紀錄保存、IP Meta Data 保存），發展社群網路數位鑑識技術，獲取社群網路使用者之真實身分，進而達成定位追蹤之效益。目前網際網路封包加密，無法再透過解析封包方式探知社群網路行為模式；而社群網路或 APP 服務提供者也往往位於國外，難以透過司法互助的方式取得相關資訊；進一步的說，犯罪者往往盜用他人社群網路帳號，讓犯罪調查更加困難，本案建置目的即為克服上述問題之影響。

圖 5-9 自動化社群網路資訊分析實驗平臺

（一）、目前，識別一個人的身分，往往透過該人的生物特徵。從犯罪偵查的角度來看，這些生物特徵會在犯罪現場發生特徵轉移，鑑識人員即透過擷取到之生物特徵轉移，還原誰經過犯罪現場。本計畫也運用相同之原理，網路使用者會

有他的使用特徵，只要利用他的使用特徵，於網路上將他的個人特徵識別出來，使對方無法隱藏真實身分。網路特徵的更複雜運用，可以用來面對網路更複雜的情況或需要，以在網路上識別一個人之真實身分。

（二）、在網路犯罪快速增長，手法快速變化、科技化、專業化、與全球化時代，網路犯罪已為警政工作的嚴重挑戰之一。因此，網路犯罪偵查是治安重點工作之一。我國網路犯罪其中又以網路詐欺最為嚴重，只要擁有社群網路服務（例如 Facebook）或者網路即時通訊服務（例如 LINE）者，幾乎人人接過詐騙訊息，另外，如比特幣洗錢、網路勒索、竊盜個資等。而高科技犯罪偵查之一重點為知道傳送訊息者之真實身分（個化使用者）與他目前的地理位置（追蹤他的位置）。

（三）、在智慧型手機（或其類似設備，如平板電腦）已逐漸成為現今社會不可或缺之重要用品，因其除具備一般傳統行動通話功能外，還可以讓使用者在手機上利用 APP 服務連接社群網路與他人聯繫。雖然科技的發展促進生活便利，然而由於雲端服務之特性，這些 APP 服務提供廠商皆設立於國外，且其服務伺服器也不在本國境內，以致當本國執法機關面對嫌犯運用此類通訊工具犯案，需要調閱通聯記錄或請求協助取得通訊內容時，這些提供者大多以不符公司

所在該國法規為由不願提供協助。

（四）、目前警方執行傳統的數位鑑識任務主要依賴於電腦硬體設備上擷取可能的跡證，並運用雜湊函數的特性來確保數位證據的可靠度。然而此傳統方法並無法複製運用上述之雲端運算服務以及其分散國外各地的伺服器與資料儲存中心。目前情況，為了進行社群網路或相關APP服務的偵查，在法院批准司法警察機關可在網路上監察嫌疑犯之通訊資料後，多使用被動式介接網路層截取資料的方式。但是此方法效果有限，其需要花費大量的時間蒐集資料，而且幾乎是不可能蒐集到完整資料。此外，現在很多社群網路或相關 APP 服務都提供加密的資料通訊方式，如 HTTPS，這讓被動式截取網路資料的方法毫無用武之地。又是類服務在網際網路通訊過程中皆有加密，服務提供者也不願提供解密金鑰，在此情形下警方偵辦案件面臨嚴重的挑戰。

（五）、匿名網路 Tor 近幾年來興起，其特性為通訊的雙方，都無法知道對方身分及來源的 IP 為何，本身的連線採用加密的方式，通訊經由數個國家路由，提供路由服務者為保密等種種因素，一旦歹徒透過匿名網路通訊，幾乎無法追查其身分與位置，根據 2014 年 10 月 31 日報導，社群網路 Facebook 已能透過 Tor 進行瀏覽。於 2016 年 4 月 22 日 Facebook 官方公佈，已經有 100 萬人透過 Tor 網路連結

Facebook。匿名網路對治安造成的嚴重影響，已引起許多國家注意，美國聯邦調查局(FBI)在 2014 年 11 月 7 日，公佈新聞:「聯邦調查局已經對超過 400 個 Tor 匿名服務（位址為.Onion），包含數十個黑市(Dark Market）網站進行掃蕩行動…。」Tor 洋蔥路由器是實現匿名通訊的自由軟體，用戶通過 Tor 可以在網際網路上進行匿名交流。

根據以上分析，由於各式各樣社群網路、網路即時通訊服務等網際網路應用服務(APP)在運用加密，匿名網路、且 APP 服務提供者大多位於國外及雲端儲存下，數位偵查與鑑識已愈發困難，治安機關面臨難以透過現有數位鑑識技術、封包解譯、或網路接取服務提供者調閱通聯紀錄而追蹤個化使用者之困境。因此，有必要從不同的出發點，發展新的數位偵查與鑑識方法。本案提出構想，透過 IP 連線資料保存（如圖 5-10），利用加害者與受害者通訊間的關聯性，不同的時間點間逐步交集，從眾多可疑者逐步過濾出加害者真實 IP，再透過網際網路接取服務業者（如遠傳電信），登錄之 IP、Port、時間對應身分 ID 服務（刑事局已建置相關系統），來獲得網路上虛擬歹徒的真實身分，並達成定位追蹤的目的。

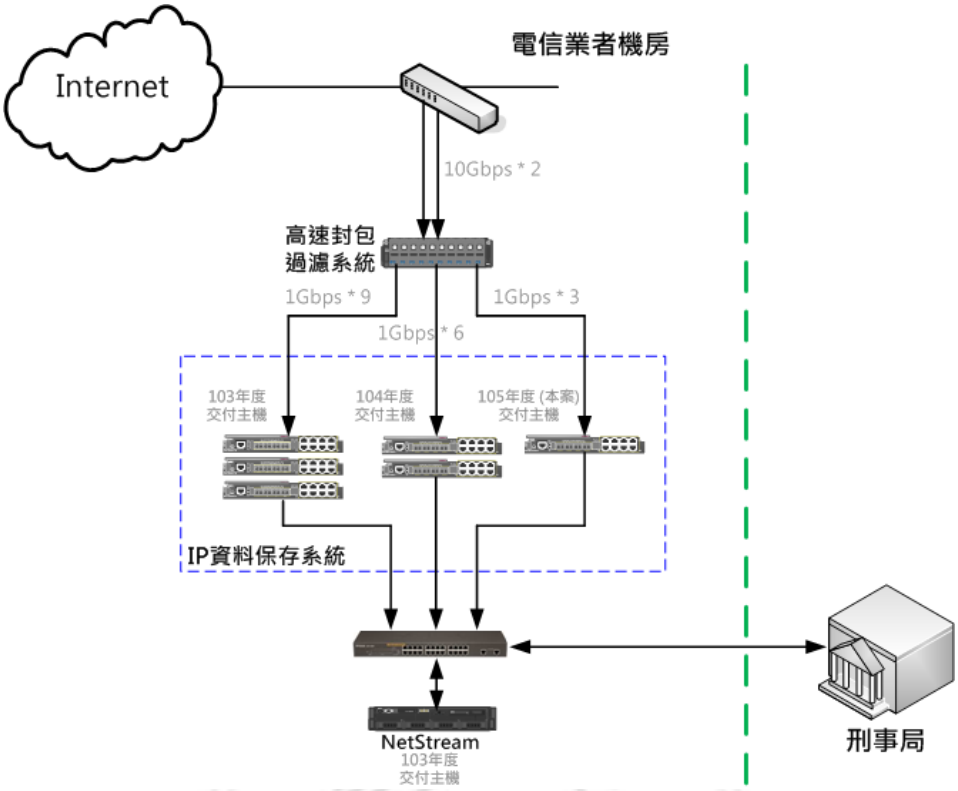


圖 5-10 IP 資料保存系統架構

二、本案延續 4 年（103~106 年）計畫大流量網路封包環境分析

為執行規畫項目將建案畫為 4 年(103~106 年)計畫，103~106 年各年執行順序為，「社群網路偵查暨鑑識技術實驗平臺」、「建構大量鑑識資料分析技術與過濾機制」、「驗證雲端與 IP 定位資料保存機制」、與「強化社群網路資訊分析機制」(如圖 5-11)，期能透過本計畫的執行，進一步提升高科技犯罪偵查與鑑識能力，並將其結果提供有關單位做為訂定方案或為修法參考。

圖 5-11 前案 103-106 年度成果圖

三、本案包含兩個方向，Tor 匿名網路之偵測，及 IP 連線資料保存之應用。

為避免匿名網路的危害，能夠判斷匿名網路連線以保護組織之安全，已是資訊安全重要的一環。

（一）、Tor 匿名網路之偵測的效益為可預防以下之資安事件：

1、勒索病毒(Ransomware)：

例如 CryptoWall 4.0 依舊使用 Tor 匿名網路，而且持

續利用受到危害的各網頁來散佈。而 EslaCrypt，每一位受害者都會被提示要繳出等值於 500 美元的比特幣贖金，才能讓被加密的檔案解密。

2、公司內部攻擊：

員工透過 Tor 連結公司內部網路，無法掌握從何處連上公司網路，是否為公司員工，還是只是盜用帳號密碼連結。另外，也無從知道透過公司網路連往何處。

3、殭屍網路與 APT 攻擊：

公司內部資源被利用來當作殭屍網路的一部分，或更進一步的被拿來發動進階持續性滲透攻擊。

4、品牌危害(Brand Damage)：

公司網頁遭竄改，或者是被流言重傷。

5、網路間諜(Cyber Espionage) ：

網路間諜同樣會利用匿名網路隱藏行蹤，攻擊政府機關或重大產業，從中獲取國防機密或商業情報。

6、執法機關面對網路戰：

維護網路國土安全，避免國土遭受恐怖分子網路攻擊或利用匿名網路進行犯罪連絡。

（二）、IP 連線資料保存效益如下：

1、彌補 IP 通訊紀錄缺口：

傳統電信領域語音通訊（室內電話，3G、4G 行動電話）擁有通聯紀錄(CDR：Call Detail Record)可供查詢，

網際網路卻沒有對應之連線紀錄可供查詢，目前電信業者僅能提供簡單的上網時間、下線時間、地點等資訊，卻無法查詢犯罪嫌疑人何時上甚麼社群網站、應用甚麼通訊軟體、與誰連絡等。

2、回溯網路犯罪使用者真實身分，降低向國外 APP 服務提供者調閱通訊紀錄的依賴：

網際網路透過代理伺服器(Proxy)、匿名網路、VPN 等方式組合運用，輔以盜取他人的帳號，難以回溯到底是誰與被害者溝通、誰要求了這個服務、惡意程式的攻擊起點等。

利用時間關連，過濾多筆 IP 連線資料保存，獲得可疑人物之 IP 位址，透過電信業者現有調閱機制，有機會回溯出可疑對象。此一應用，恰可減少向國外 APP 服務提供者調閱通訊紀錄的依賴。

3、強化網路使用者行為分析：

透過IP 連線資料保存,可以分析使用者可能的朋友、生活作息、上網行為，常使用的 APP（應用服務）等透過這些訊息來拼湊歹徒的樣貌，對於犯罪調查相當有幫助。

網路通訊內容加密，分析 IP 連線資料保存已為犯罪偵查重要手段，有些案件，只需進行連線紀錄分析，無需使用通訊監察。

4、強化網路惡意攻擊後災情評估。

2017 年 2 月 7 日我國 13 證券業者遭 DDoS 攻擊並遭勒索，此事件司法單位即介入調查。司法單位的介入調查其最終目的為知道誰或哪個團體發起網路惡意攻擊事件，惟目前我國警方仍然還未能對這種網路惡意攻擊事件能有效進行調查。

以上述 2 月 7 日證券業者造受 DDoS 攻擊為例，我們在面對攻擊時，需要知道攻擊範圍、攻擊中與攻擊後所造成的損害。從證券商的角度，他只需要知道自己的損害。根據研究發現，DDoS 攻擊很可能只是掩飾其它網路攻擊的手段，例如 APT 攻擊，因此證券商還要仔細巡視是否具有其他安全性漏洞，並進行受災狀況評估(Compromise Assement)。同樣的對網路接取服務提供商（例如中華電信股份有限公司），他也有需要做的受災狀況評估，其中之一是他必須考量是否符合與客戶間的服務層級協議(Service Level Agreement)。而在執法單位，惡意攻擊發生時，須從國家社會的角度，建議其處理步驟，發生時、發生後同樣也必須做相關受災狀況評估，供政府知道受災範圍（哪些團體、用戶被攻擊）、受災深度（如系統停擺、資料遭竊取）與後續處理方法，後續處理方法其中之一為調查是誰或者哪個團體發動此次惡意攻擊

事件。在此類網路犯罪調查中，如一般犯罪調查一樣，收集情資是非常重要一件事，因此，透過 IP 連線資料保存，建立網路威脅情資資料庫為強化網路犯罪調查重要的一環。

（三）、其他之效益如下：

1、強化高科技犯罪偵查能力，如生物鑑識一樣，透過指紋、虹膜等可以識別一個人的身分。透過本案，還原犯罪現場，掌握正確偵查方向，使社群網路犯罪無所遁形。本案至目前所產生的相關思維與技術，強化使用者應用與感知能力，目前已強化現有系統並運用中。

2、厚植警察機關對新興網路犯罪之偵查與鑑識研究發展能量，培訓第一線執法人員面對社群網路平臺上之犯罪行為時，具有犯罪資料之蒐集、處理與分析能力，強化社群網路犯罪偵查能量。

3、發展社群網路犯罪偵查之工具，增強應用現有資源應用，如通聯調閱、封包解析、公開源資料收集，及手機電腦數位鑑識採證等，強化社群網路犯罪偵查技巧與資料來源，輔佐傳統犯罪偵查手法之不足。

4、社群網路技術日新月異，警察機關如未能持續研究新興科技，將無法遏制歹徒運用此新興科技進行犯罪逃避員警查緝，造成政府公權力喪失。因此強化員警社

群網路犯罪偵查能量、提升刑事科技偵查水準，可讓社會公平正義得以伸張。

四、對辦案技術重大突破

提供第一線執法人員面對社群網路平臺上之犯罪行為時，具有犯罪資料之蒐集、處理與分析能力，強化社群網路犯罪偵查能量：

（一）、強化社群網路犯罪偵查模式，培育社群網路犯罪偵查專才並發展偵查作為所需之資訊技術。

（二）、發展社群網路犯罪偵查之工具，強化社群網路犯罪偵查技巧與資料來源，輔佐傳統犯罪偵查手法之不足。

（三）、社群網路技術日新月異，警察機關如未能持續研究新興科技，將無法遏制歹徒運用此新興科技進行犯罪逃避員警查緝，造成政府公權力喪失。因此強化員警社群網路犯罪偵查能量、提升刑事科技偵查水準，可讓社會公平正義得以伸張。

（四）、29 種應用服務分析：本計畫至 106 年截止，識別 Plurk、PTT、Facebook、Twitter、LINE、WhatsAPP、Gmail、Google+、Yahoo Messenger、WeChat、QQ、Telegram、Juiker、Skype、Instagram、Flickr、YouTube、Google Drive、Yahoo Mail、AOL Mail、Outlook、網易郵箱、Hangouts、Mobile01、17

直播、LinkedIn、M+ Messenger、Tor 洋蔥路由器等應用服務，經驗證可找出可疑目標的時間不到 1 秒，且縮小可疑目標數量，DPI(Deep Packet Inspection)最大的流量可達 12.5Gbps。

結合現有資源，簡化使用者資料匯入、匯出、轉碼等繁複的操作，可大為提升辦案的效率，此細節也為本案關注的重點，系統整合包含：證據光碟資訊、通聯調閱與定位資訊、社群網路公開訊息蒐集等。

五、後續精進措施

（一）、匿名網路 Tor 近幾年來興起，其特性為通訊的雙方，都無法知道對方身分，來源的 IP 為何，本身的連線採用加密的方式，通訊經由數個國家路由，提供路由服務者為保密等種種因素，一旦歹徒透過匿名網路通訊，幾乎無法追查其身分與位置。

（二）、匿名網路使用已逐漸造成我國治安重大問題。因此，繼續對匿名網路提出防制方法，為未來重要課題。

（三）、透過匿名網路進行比特幣之交易，已成為犯罪分子洗錢、非法交易、綁票勒贖的安全管道，如何進行比特幣金流之管制與追蹤，為未來可以繼續精進的方向。

（四）、目前國家正推動 DNS Log 保存，期能於未來研究利用 DNS

Log 進行犯罪追蹤方法。

六、階段性目標達成情形

（一）、103 階段性目標達成情形

103 年度規劃為「社群網路偵查暨鑑識技術實驗平臺」，其目的為建置對應之實驗平臺，以利後續進行 104~106 年度規劃部分之概念驗證(Proof of Cconcept,POC)，設計採跨網路環境架構設計，可用於 3G 實驗網路、企業網路與 WiFi 無線網路進行各項驗證。本階段順利達成階段目標。

103 辦理之重要成果

103 年度已建置完成新世代社群網路對應之平臺，模擬大量資料分析技術與在社群網路、雲端服務構架下，針對雲端大量資料分析技術做初步驗證與探討，且隨著網際網路普及化與社群網路通訊工具方便且多樣化，常用社群網路分析與過濾需持續更新，以利符合實際辦案環境。本案能夠培養警政機關防制網路犯罪的能力，對於日益普及的新世代網路應用以及相應的網路犯罪，具有關鍵性的影響。

本案共規劃數十項測試項目驗證系統功能，共涵蓋 3 種網路實驗環境（3G、企業網路、WiFi）、常見社群網路 APP （如 LINE、WhatsAPP）與平臺（如 IOS、Android）。

因社群網路為因應使用者需要，常不斷改版，故本案

開發過程中，需常針對社群網路 APP 改版進行系統部分功能重新設計、改良，極具技術挑戰性。

派員前往參加歐洲 Intelligence Support System Training 研習課程以廣泛蒐集國際上最新技術，提升國內刑事科技與偵查犯罪能量，並和與會各國司法機關建立跨境打擊犯罪、資訊交換等國際合作管道。

（二）、104 階段性目標達成情形

本研究案「提升新世代社群網路偵查暨鑑識能量」最主要為「驗證大量資料分析技術與過濾機制」。為了延伸 103 年度已獲得的成果，在其基礎下開發對於大量資料分析技術與在社群網路、雲端服務構架下，驗證雲端大量資料分析技術。

在高速網路大量資料下（如圖 5-12），即時封包擷取保存，並進行分析與過濾。在社群及雲端應用之高速網路，一般的 Sniffer 工具無法應付即時性高速網路封包擷取，容易產生漏封包現象，進而影響鑑識可靠度。因此，選擇交大校園網路並採用 DPI(Deep Packet Inspection)進行初次高速網路驗證（如圖 5-13）。

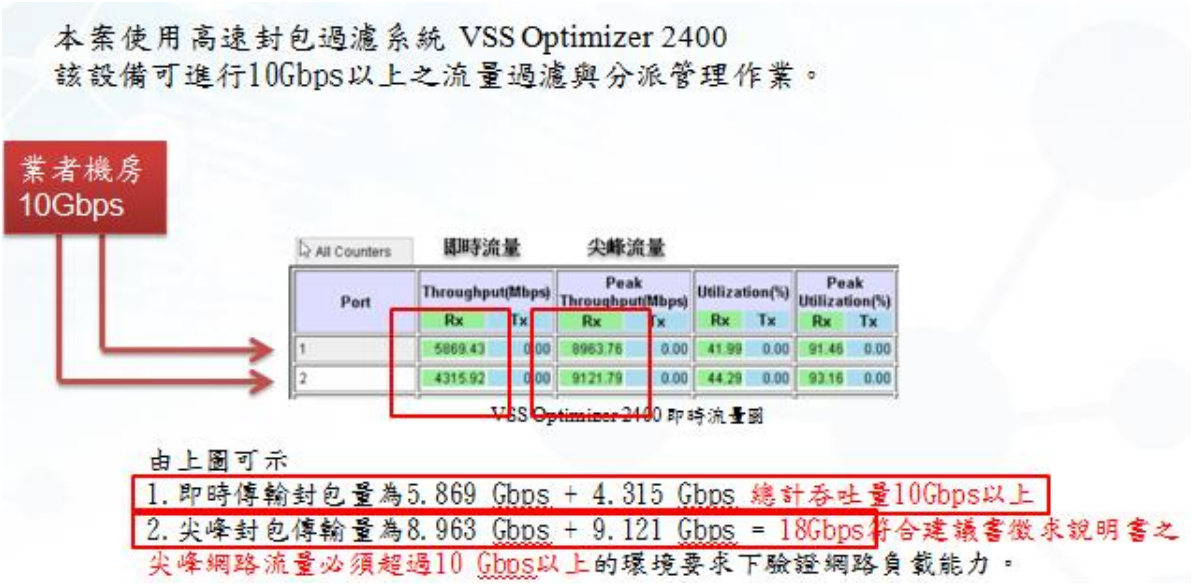


圖 5-12 大量數據驗證－封包來源

圖 5-13 DPI 封包過濾分析

本案六臺主機共 16 個網路埠，可負載尖峰流量 10Gbps 以上之網路封包過濾分析，符合建議書徵求說明書之尖峰流量 10Gbps 流量之過濾分析。

104 辦理之重要成果

1、隨著網際網路普及與社群網路多樣化，提供人們方便且

多型態的通訊工具，增加支援更多常用社群網路分析與過濾需持續更新以利符合實際辦案環境，支援多數常用的社群網路應用，如 Facebook、Plurk 等，並涵蓋更多的社群網路應用，包含 Gmail、Hangouts、Yahoo Messenger、Yahoo Mail、Outlook.com、Google Drive、Flickr、Instagram、AOL Mail、YouTube、網易郵箱等，以邁向真實環境下運作之方向，進而研提可以實際協助犯罪偵查的工具及平臺並進行概念驗證。

2、透過本研究案技術，在給定一個網路應用層帳號，循序找出該帳號使用的 IP，接取層識別碼 （Access ID，如 MAC 位址、MSISDN、線路編號等），以及實際用戶身分與所在位置，探討大量資料分析技術與過濾機制是否可行。

3、本案透過大學校院之校園網路收集大量真實網路環境資料，進行大量資料分析與過濾，不影響（或影響微乎其微） 網路服務品質，且尖峰流量每秒超過 1Gbps，快速封包過濾。

4、派員前往參加美洲 Intelligence Support System Training 研習課程以廣泛蒐集國際上最新技術，提升國內刑事科技與偵查犯罪能量，並和與會各國司法機關建立跨境打擊犯罪、資訊交換等國際合作管道。

（三）、105 階段性目標達成情形

本研究案「提升新世代社群網路偵查暨鑑識能量」研究目標為「建構雲端 IP 定位資料保存機制」，其因社群網路、APPs 服務提供者大都位於國外，因此用戶資料與使用紀錄調閱不易。傳統偵查、數位鑑識方式已無法直接提供社群網路或 APPs 帳號通訊內容、個化與追蹤定位之功能，亦即無法提供該帳號是誰所使用、以及該帳號的實體位置，因此亟需建構雲端 IP 定位資料保存機制。

為建構雲端 IP 定位資料保存機制，另在網路使用逐年爆增情況下，鑑識過程所需儲存的資料量越來越多，為強化與真實環境聯結，105 年度於電信業者端（遠傳電信）進行技術驗證。

105 辦理之重要成果

1、繼續強化社群網路應用服務分析能力，達 18 種應用服務分析：本案至 105 年截止，識別 Plurk、PTT、Facebook、Twitter、LINE、WhatsAPP、Google Service、Yahoo Messenger、WeChat、Juiker、Skype、Instagram、Flickr、YouTube、Yahoo Mail、AOL Mail、Outlook、網易郵箱等應用服務。

2、105 年透過擷取並過濾封包一個月，經驗證可縮小可疑目標數量，找出可疑目標的時間不到 1 秒，且 DPI(Deep Packet Inspection)運用分散式處理技術，最大的流量可

達 12.5Gbps，每日資料庫儲存容量達 20GB，資料庫規模到達 116TB。

3、繼續強化權限管理與系統管理功能，以因應犯罪偵防權責區分，包含使用者權限區分、角色與帳號管理、系統紀錄與系統異常告警機制。

4、透過遠傳電信接取網路收集大量真實網路環境資料，進行大量資料分析與過濾，不影響（或影響微乎其微）網路服務品質。

（四）、106 階段性目標達成情形

運用網路匿名化的技術，達成保護網路通訊的隱私，卻也造成執法單位難以追查到底是誰做了這一件非法事情，也就是難以追蹤個化使用者困境。延伸過去研究成果對匿名網路追蹤進行研究，並獲得相當的成果。

傳統電信領域具備通訊監察與通聯調閱，透過通聯調閱可知道某人何時何地與誰聯絡，通聯分析一直在犯罪偵查與緊急救難中，扮演非常重要的角色。本階段透過 IP 連線資料保存發展其相關應用並獲得相當的成果。

106 辦理之重要成果

1、Tor 匿名網路之偵測，完成：

(1)、公開節點之收集。

(2)、自動化私密結點之收集。

(3)、憑證辨識。

2、IP 連線資料保存之應用，完成：

(1)、不得影響 （或影響微乎其微） 網路服務品質；且在尖峰流量超過 10Gbps 的情況下，可快速過濾封包。

(2)、給定一個社群網路應用帳號（對象），應於合理時間內循序找出或推論該帳號（對象）的擁有者的電信業者發給之 IP。

(3)、支援代理伺服器(Proxy)、加密及匿名網路（例如 Tor）等。

3、結合現有資源，強化犯罪偵查分析：

結合現有資源，簡化使用者資料匯入、匯出、轉碼等繁複的操作，可大為提升辦案的效率，此細節也為本案關注的重點，系統整合包含：證據光碟資訊、通聯調閱與定位資訊、社群網路公開訊息蒐集等。

4、強化嫌犯行為分析：支援目標之 APP 使用分析。

如生活作息，從嫌犯使用手機何時上網、何時沒有使用手機等時間、目前移動的速度、目前的所在位置，可以推估目前活動的性質，例如是在搭公車、計程車，或在搭捷運、火車，或目前可能在銀行洽公、或是待在辦公室。因此，可以推估客戶的作息時間。

5、個化分析：

如嫌犯好友分析，透過網際網路連線紀錄的儲存，也可以知道在同一個網路接取服務提供商下，誰與嫌犯聯絡（以下稱與嫌犯聯絡的人為聯絡者）。透過聯絡者與嫌犯聯絡的密集度、時間、地點，還有嫌犯與聯絡者兩者個人的喜好、習慣等訊息等，可以進一步判斷是否為男女朋友關係、朋友關係、是否同一個家庭等。

七、辦理本案延伸之可偵查高科技犯罪之技術

（一）、本研究案（103~106 年）目的為發掘出網路犯罪者的真實身分，達到個化與追蹤的目的。是對於利用匿名網路(Tor)犯罪者，可達成個化與追蹤的目的。

近期從犯罪偵查資料顯示，嫌犯使用匿名網路(Tor)進行通訊有愈來愈多的趨勢。且 APP 服務提供者大多位於國外及雲端儲存下，數位偵查與鑑識已愈發困難，治安機關面臨難以透過封包解譯或網路接取服務提供者調閱通聯紀錄而追蹤個化使用者之困境。因此，有必要從不同的出發點，發展新的數位偵查與鑑識方法。本研究案提出構想，透過 IP 連線資料保存，利用加害者與受害者通訊時間的關聯性，在不同的時間點間逐步交集，從眾多可疑者逐步過濾出歹徒真實 IP。例如在第一個加害者與被害者通訊時間點，透過 IP 連線資料保存資料庫查知在該時間點有哪些 IP

有連線上網（假設有 10000 個 IP），在第二個通訊時間點假設有 7000 個 IP 連線上網，在第三個通訊時間點假設有 12000 個 IP 連線上網，在這三個通訊時間點的 IP 取交集，符合這三個通訊時間點的 IP 上網連線，就是我們要的 IP。再透過網際網路接取服務業者（如遠傳電信），登錄之 IP、Port、時間對應身分 ID 服務（刑事局已建置相關系統），來獲得網路上虛擬歹徒的真實身分，並達成定位追蹤的目的。上開技術同樣可應用於匿名網路(Tor)的追蹤上。

（二）、本次執行案件最主要為發展 Tor 匿名網路之偵測（如圖 5-14），及 IP 連線資料保存之應用網路匿名化的技術。

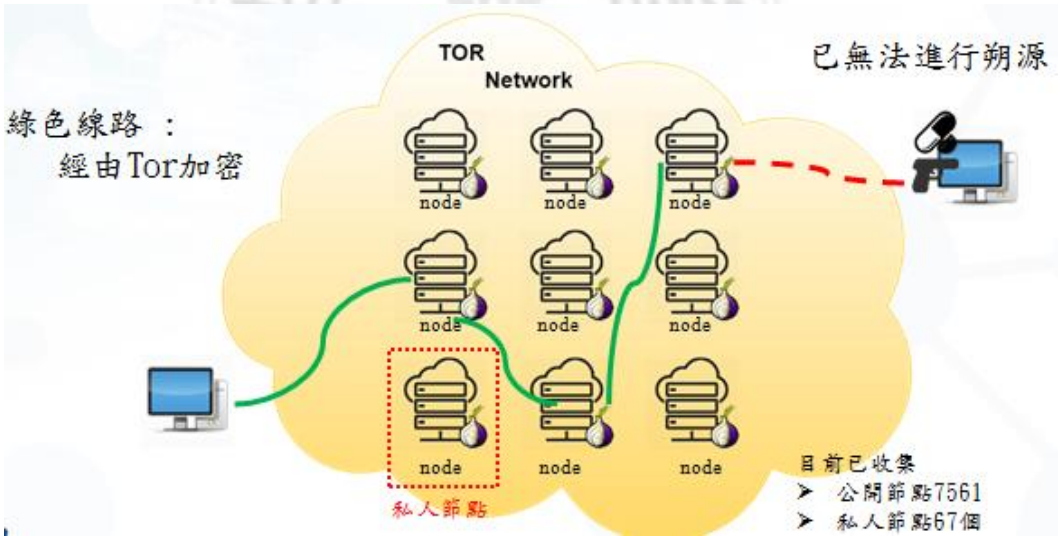


圖 5-14 封包過濾：支援代理伺服器(proxy)、加密及匿名網路（如 Tor）

Tor 匿名網路在分類上屬於暗網(Dark Web：The Dark Web Then is Classified as a Small Portion of the Deep Web that has Been Intentionally Hidden and is Inaccessible

Through Standard Web Browsers)，其上網頁無法透過一般搜尋引擎例如 Google，Yahoo，Bing 搜尋，必須透過 Tor 瀏覽器進行搜尋，因此許多犯罪分子喜歡透過 Tor 匿名網路交易，從事見不得人的事，因此，他被稱為暗網（從事見不得人的事）。Tor 匿名網路又稱為洋蔥路由是因為 Tor Client 與 Server 間通訊時，Tor Client 會與其間的 Tor 路由作密鑰交換，在 Tor Client 端傳送訊息前會透過這些密鑰層層加密， 每經過一個 Tor 路由就解密一層，就像剝洋蔥一樣。Tor 匿名網路因為採用洋蔥式加密與會晤點的方式並可以搭配代理伺服器(Proxy)，具有難以追蹤來源端或目地端的特性。

1、Tor 洋蔥路由器是實現匿名通訊的自由軟體，用戶通過 Tor 可以在網際網路上進行匿名交流。與過去加密的最大不同是，再經過洋蔥網路的一層層代理連接，無法進行來源反求。

2、Tor 的組成是透過 7 千多個公開節點加上無數的私人節點。如過去知名的暗網：絲路就是透過此技術在網路上進行犯罪交易或是最近的的一篇新聞-英國籍模特兒在綁架過後在暗網中被進行拍賣，Tor 匿名網路偵測在保護網路安全，免於遭收勒索病毒、公司內部攻擊、殭屍網路與 APT 攻擊、公司品牌危害、網路間諜等資安事件並可協助追蹤與定位，故列為本案研究重要課題。

（三）、本次 IP 連線資料保存之作為

1、29 種應用服務分析：

本案至 106 年截止，識別 Plurk、PTT、Facebook、Twitter、LINE、WhatsAPP、Gmail、Google+、Yahoo Messenger、WeChat、QQ、Telegram、Juiker、Skype、Instagram、Flickr、YouTube、Google Drive、Yahoo Mail、AOL Mail、Outlook、網易郵箱、Hangouts、Mobile01、17 直播、LinkedIn、M+ Messenger、Tor 洋蔥路由器等應用服務。透過利用加害者與受害者通訊時間的關聯性，在不同的時間點間逐步交集，經驗證可找出可疑目標的時間不到 1 秒，過濾之 DPI(Deep Packet Inspection)最大的流量可達 12.5Gbps。

2、結合現有資源，強化犯罪偵查分析：

結合現有資源，簡化使用者資料匯入、匯出、轉碼等繁複的操作，可大為提升辦案的效率。系統整合包含：證據光碟資訊、通聯調閱與定位資訊、社群網路公開訊息等（如圖 5-15）。

圖 5-15 結合現有刑事警察局監察工具

3、強化嫌犯行為分析：嫌犯生活作息（如圖 5-16）：

從觀察嫌犯使用手機何時上網、網路流量改變、目前移動速度、目前所在位置，可推估目前活動的性質，例如是在搭公車、計程車，或在搭捷運、火車，可推估其作息時間。

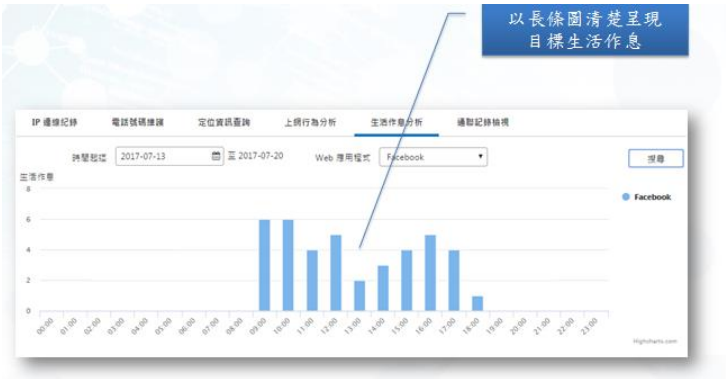


圖 5-16 嫌犯生活作息分析

4、嫌犯好友分析：

透過 IP 連線資料保存（如圖 5-17），也可獲知在同一個網路接取服務提供商下，誰與嫌犯聯絡（聯絡者）。透過各方面收集之資料，如聯絡者與嫌犯聯絡的密集度、時間、地點，雙方之性別、喜好、習慣等訊息等，可以進一步判斷是否為男女朋友關係或者一般朋友關係等。

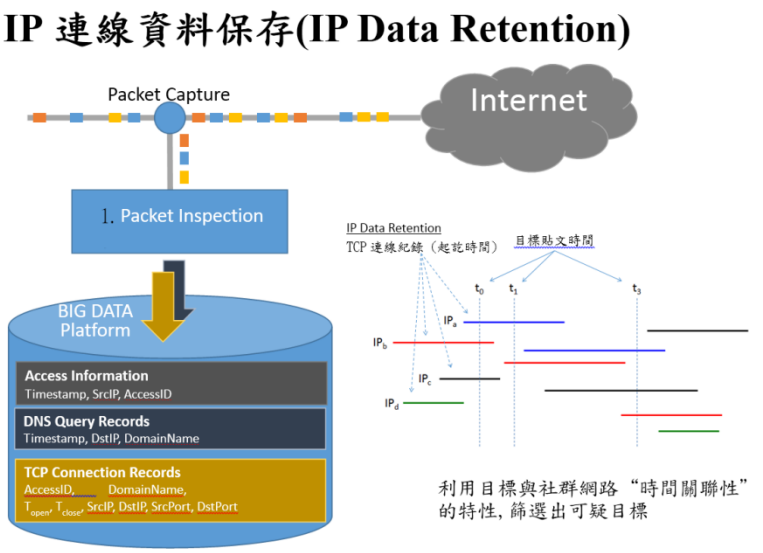


圖 5-17 IP 連線資料保存

5、嫌犯上網行為分析（如圖 5-18）：

瞭解嫌犯 APP 或上網的喜好，例如，某人大部分社 群媒體都是 Facebook，又喜歡瀏覽瑜珈之類或美食等網站，這些資訊在配合辦案相關技術下將相當具有價值。

圖 5-18 嫌犯上網行為分析

（四）、未來可持續發展之犯罪偵防重點工作列舉如下。

1、比特幣透過匿名網路(Tor)交易已成為歹徒最佳的洗錢工具，研究其定位追蹤對犯罪偵查有極大助益。

2、目前國家正推動 DNS Log 功能變數名稱系統資料保存，駭客往往利用跳板進行各式駭客攻擊（例如 DDOS 分散式阻斷攻擊），DNS Log 會紀錄誰的電腦（伺服器）被利用來當作跳板，故深入研究利用 DNS Log 進行犯罪追蹤方法，也為未來重要的課題。

八、主要內容

（一）、執行內容

1、Tor 匿名網路之偵測（如圖 5-19），工作項目包含：

(1)公開節點之收集（如圖 5-20），目前已收集 7561 節點。

(2)自動化私密節點之收集（如圖 5-21）。

(3)憑證辨識（如圖 5-22）。

圖 5-19 連線至公開節點(1)

使用者直接開啟 Tor Browser 預設將會直接連線至公開節點(Exit Node)。

圖 5-20 連線至公開節點(2)

已收集公開節點共計 7561 個並加入封包過濾清單，連線行為：連線至公開節點數量大約 7 千多個。

2、定期使用程式去爬網頁中的節點資料進行資料更新。

(1)、什麼是私人節點：因網路管理人員最常見的封阻方式為阻斷公開節點，因此使用者也可使用私人節點進行連線。

(2)、針對私人節點連線進行兩種辨識方法。

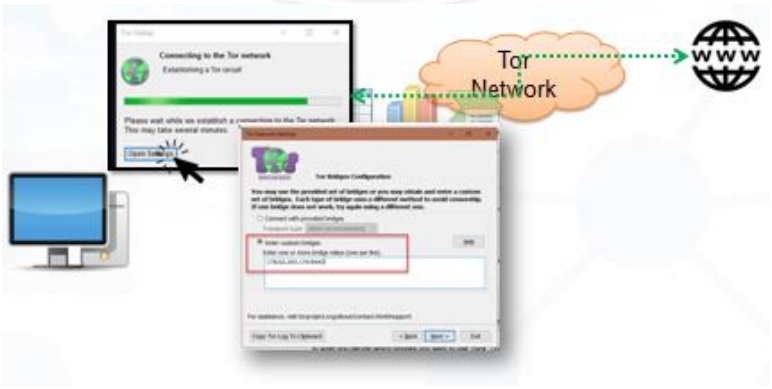


圖 5-21 連線至私人節點

使用者直接開啟 Tor Browser 後點選”setting”即可輸入私人節點資料

序號	使用者連線方式	現有偵測情形
1	連線至公開節點(public node)	驗證通過可成功辨識
2	連線至私人節點(private node)	驗證通過可成功辨識
3	連線至未登錄之私人節點-憑證辨識	驗證通過可成功辨識
4	Pluggable Transport : obfs3/ScrambleSuit/obfs4	無法辨識
5	Pluggable Transport : meek	無法辨識
6	Pluggable Transport : FTE	無法辨識

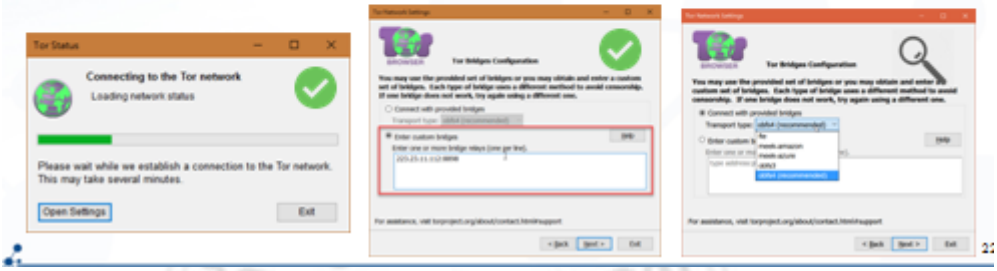


圖 5-22 Tor 辨識成果說明

3、繼續強化社群網路應用服務分析能力，達 29 種應用服務分析：

本案至 106 年截止，識別 Plurk、PTT、Facebook、Twitter、LINE、WhatsAPP、Gmail、Google+、Yahoo Messenger、WeChat、QQ、Telegram、Juiker、Skype、Instagram、Flickr、YouTube、Google Drive、Yahoo Mail、AOL Mail、Outlook、網易郵箱、Hangouts、Mobile01、17 直播、LinkedIn、M+ Messenger、Tor 洋蔥路由器等應用服務，經驗證可找出可疑目標的時間不到 1 秒，且縮小可疑目標數量，DPI(Deep Packet Inspection)最大的流量可達 12.5Gbps。

4、結合現有資源，強化犯罪偵查分析：

結合現有資源，簡化使用者資料匯入、匯出、轉碼等繁複的操作，可大為提升辦案的效率，此細節也是本案關注的重點，系統整合包含：證據光碟資訊、通聯調閱與定位資訊、社群網路公開訊息蒐集等。

5、嫌犯行為分析：

(1)、嫌犯生活作息：從嫌犯使用手機何時上網、何時沒有使用手機等時間、目前移動的速度、目前的所在位置，可以推估目前活動的性質，例如是在搭公車、計程車，或在搭捷運、火車，或目前可能在銀行洽公、或是待在辦公室。因此，可以推估客戶的作息時間。

(2)、嫌犯好友分析：透過網際網路連線紀錄的儲存，也可以知道在同一個網路接取服務提供商下，誰與嫌犯聯絡（以下稱與嫌犯聯絡的人為聯絡者）。透過聯絡者與嫌犯聯絡的密集度、時間、地點，還有嫌犯與聯絡者兩者個人的喜好、習慣等訊息等，可以進一步判斷是否為男女朋友關係、朋友關係、是否同一個家庭等。

(3)、嫌犯上網行為分析：瞭解嫌犯 APP 或上網的喜好，例如，某人大部分上網時間社群媒體都是在用 Facebook，又喜歡瀏覽瑜珈之類或美食等網站，

這些資訊在配合辦案相關技術下將相當具有價值。

強化權限管理與系統管理功能，以因應犯罪偵防權責區分，包含「使用者值」與「知覺風險」的變數。

6、權限區分、角色與帳號管理、系統紀錄與系統異常告警機制。

(1)、系統需檢查登入使用者是否有權限進行查閱。

(2)、使用者區分一般使用者、系統管理者兩類，還需要支援不同的角色，以對應實際上管理的組織單位（含群組或組織單位組合）

(3)、提供角色管理功能，至少包含角色新增、修改、查詢、刪除、權限設定等功能。

(4)、提供帳號管理功能，至少包含帳號查詢、帳號鎖定、解除鎖定、設定使用者所屬的使用者群組、設定權限。

(5)、使用者登入資訊詳細記錄，包含使用者帳號、登入及登出時間、登入 IP 位址、登入狀態結果（成功或失敗）。

(6)、帳號登入錯誤多次，則進行系統告警，並鎖定該帳號。

(7)、可將系統紀錄之項目內容進行查詢，並可列印與匯出。

(8)、當系統發生異常狀態時，進行告警提示。

7、支援查詢功能。

(1)、系統需針對應用程式上網連接時間段，進行連接數量統計調查，並可查閱該統計之設備詳細上網清單，且提供該統計結果 Excel 下載格式。

(2)、系統須能查詢社群帳號在特定時間段使用狀況，並需可支援關鍵字查詢。

(3)、使用者自定義查詢時間段，使用者可自訂欲查詢之時間點之前後時間區間。

九、技術創新（科技技術創新）

（一）、辨識網路上使用者真實身分：

1、透過各式社群網路或即時通訊等應用軟體 APP 實施詐騙，已成為我國治安重大問題，本案技術，透過封包保存與過濾方法，可追查出可疑之嫌犯。

2、有關社群網路 APP 運行的特點如下：(1)即時訊息傳送並非點對點(Point to Point)傳送，而是 Client-Server 架構。(2)傳送過程加密。而歹徒詐騙的躲避手法為：(1)金融方面利用國外帳戶（金融帳戶，遊戲幣帳戶等）、人頭帳戶、比特幣等方式交易，使辦案人員難以追蹤。(2)網路技術方面，透過盜用他人帳號（例如 LINE、Facebook 帳號）、代理伺服器、匿名網路(Tor)方式躲避

他人追蹤。舉例來說，一犯罪者會先盜取與受害者有關的第三者帳號密碼，一般是受害者在如即時通訊 APP LINE上的朋友,再透過這位無辜的第三者在APPl LINE上與受害者聯絡。在此情形下，因為犯罪者盜用無辜的第三者的帳號,因此不需要去查無辜的第三者帳號的真實身分。傳統偵查上，對於網路架構不熟悉之調查者，期望從被害者端擷取的封包獲得傳遞者(犯罪者)的 IP、Port 與傳遞的時間，藉以向電信業者（例如中華電信）調取看封包是誰發出的。因為即時通訊是 Client-Server 架構，因此傳遞的封包一定是 APP LINE 主機，因此這種偵查手段並無必要。傳統上，辦案人員向 APP LINE 服務提供者請求調閱通訊紀錄,期望能查出是從哪裡發出訊息給被害者的，這時會遇到另一個障礙，犯罪者是透過代理伺服器發出即時訊息,代理伺服器如果是在德國，代理伺服器業者毋須配合犯罪調查。這種跨境追查路由方式，在我國外交處境下，幾乎無法追查，縱使透過路由能夠一路追查下去，耗時甚久，很多犯罪紀錄早已抹去，犯罪者早已不知去向，或者早已把不法所得花光。另一種方式是透過金流方式追查，如果金流是透過匿名網路，透過地下匯兌，一般的偵查作為也無法發揮效用。

3、本案在透過 IP 連線資料保存，利用犯罪者留下的時間

標記與使用 APP 的種類，依照以上兩特徵，利用加害者與受害者通訊間時間的關聯性，於 IP 連線資料保存中，透過不同的時間點間逐步交集，從眾多可疑者逐步過濾出加害者真實 IP，再透過網際網路接取服務業者（如遠傳電信），登錄之 IP、Port、時間對應身分 ID 服務，來獲得網路上虛擬歹徒的真實身分，並達成定位追蹤的目的（如圖 5-23）。

4、有關資料保存 (DR，Data Retention) 在傳統的電信領域通常是指保留用戶的通話紀錄 (CDR，Call Detail Record)；對網際網路接取服務提供商 (ISP，Internet Service Provider) 而言，Data Retention 則可延伸成為 IP 連線資料保存 IPDR (IP Data Retention) 的概念，也就是保留網際網路的連線紀錄、Email 紀錄、網站瀏覽紀錄等。有了 IPDR 的完整紀錄後，本案可以利用加害者與被害者通訊時間「時間關聯性」，或者是嫌疑犯（鎖定的目標）使用社群網路的時間點（目標與社群網路之時間關聯性），找出可疑的目標或至少縮小偵查範圍。例如：本案可以蒐集嫌疑犯 （鎖定的目標）在 Facebook 網站上多次留言的時間，利用這些時間序列資訊去搜尋出在這些時間點有上傳資料到 Facebook 網站的電信用戶，並依出現次數多寡排序；出現次數越多的用戶，就越有可能是案件要找的目標。而且實證還可以比對同一

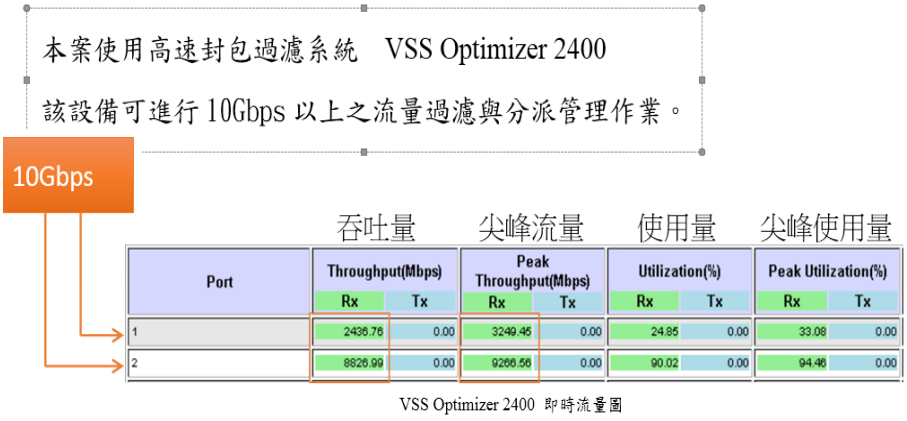
個用戶在不同社群網站的留言時間，進一步增加比對的可信度。此外，一般人通常在不同的網站會以相同或類似的帳號/密碼登入，所以針對未加密的網站帳號資料進行保存，通常也有助於找出可疑目標。本案嫌疑犯與社群網路之時間關聯性。

圖 5-23 嫌疑犯與社群網路之時間關聯性

（一）、29 種應用服務分析：

本案至 106 年截止，識別 Plurk、PTT、Facebook、Twitter、LINE、WhatsAPP、Gmail、Google+、Yahoo Messenger、WeChat、QQ、Telegram、Juiker、Skype、Instagram、Flickr、YouTube、Google Drive、Yahoo Mail、AOL Mail、Outlook、網易郵箱、Hangouts、Mobile01、17 直播、LinkedIn、M+

Messenger、Tor 洋蔥路由器等應用服務，經驗證可找出可疑目標的時間不到 1 秒，且縮小可疑目標數量，DPI(Deep Packet Inspection)最大的流量可達 12.5Gbps。（如圖 5-24）所示最大的流量可達 12.5Gbps。



VSS Optimizer 2400 即時流量圖

由上圖可示

1. 即時傳輸封包量為 2.436 Gbps + 8.826 Gbps 總計吞吐量 11Gbps 以上

2. 尖峰封包傳輸量為 3249.45 MBps + 9266.56 Mbps = 12515.56MBps ≒ 12.5Gbps

符合建議書徵求說明書之尖峰網路流量必須超過 10 Gbps 以上的環境要求下驗證網路負載能力。

圖 5-24 最大的流量可達 12.5Gbps

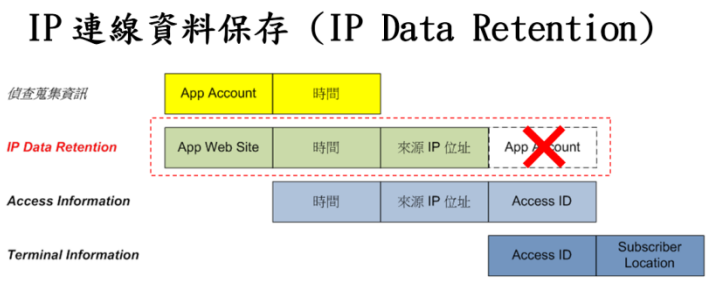


圖 5-25 IP 連線保留資料

（二）、雲端運算及 IP 連線資料保存資料庫：

本案透過雲端運算保留 IP 連線資料，該資料庫保留網際網路連線之 Meta Data，接取層的訊息、DNS Query、TCP Conection 等，透過時間關聯性，尋找出犯罪者（即為鎖定的目標）的真實身分。（如圖 5-25）所示，IP 連線保留資料。

（三）、結合現有資源，強化犯罪偵查分析：

結合現有資源，簡化使用者資料匯入、匯出、轉碼等繁複的操作，可大為提升辦案的效率，此細節也為本案關注的重點，系統整合包含：證據光碟資訊、通聯調閱與定位資訊、社群網路公開訊息蒐集等。

（四）、強化嫌犯行為分析：

1、嫌犯生活作息：

從嫌犯使用手機何時上網、何時沒有使用手機等時間、目前移動的速度、目前的所在位置，可以推估目前活動的性質，例如是在搭公車、計程車，或在搭捷運、火車，或目前可能在銀行洽公、或是待在辦公室。因此，可以推估客戶的作息時間。

2、嫌犯定位資訊（如圖 5-26）：

透過網際網路連線紀錄的儲存（Data Link Layer 的資訊），不透過 GPS 同樣可獲取客戶之定位資訊。

圖 5-26 地理位置顯示

3、嫌犯好友分析：

透過網際網路連線紀錄的儲存，也可以知道在同一個網路接取服務提供商下，誰與嫌犯聯絡。透過聯絡者與嫌犯聯絡的密集度、時間、地點，還有嫌犯與聯絡者兩者個人的喜好、習慣等訊息等，可以進一步判斷是否為男女朋友關係、朋友關係、是否同一個家庭等。

4、嫌犯上網行為分析。

5、瞭解嫌犯 APP 或上網的喜好，例如，某人大部分上網時間社群媒體都是在用 Facebook，又喜歡瀏覽瑜珈之類或美食網站，這些資訊在配合辦案相關技術下將相當具有價值。

（五）、強化封包分析能力：

為應付大量封包過濾解析與即時性，利用 DPI(Deep Packet Inspection)與分散式架構，俾符合未來擴充系統至全國網路接取服務者。DPI(Deep Packet Inspection)與分散式架構（如圖 5-27）。

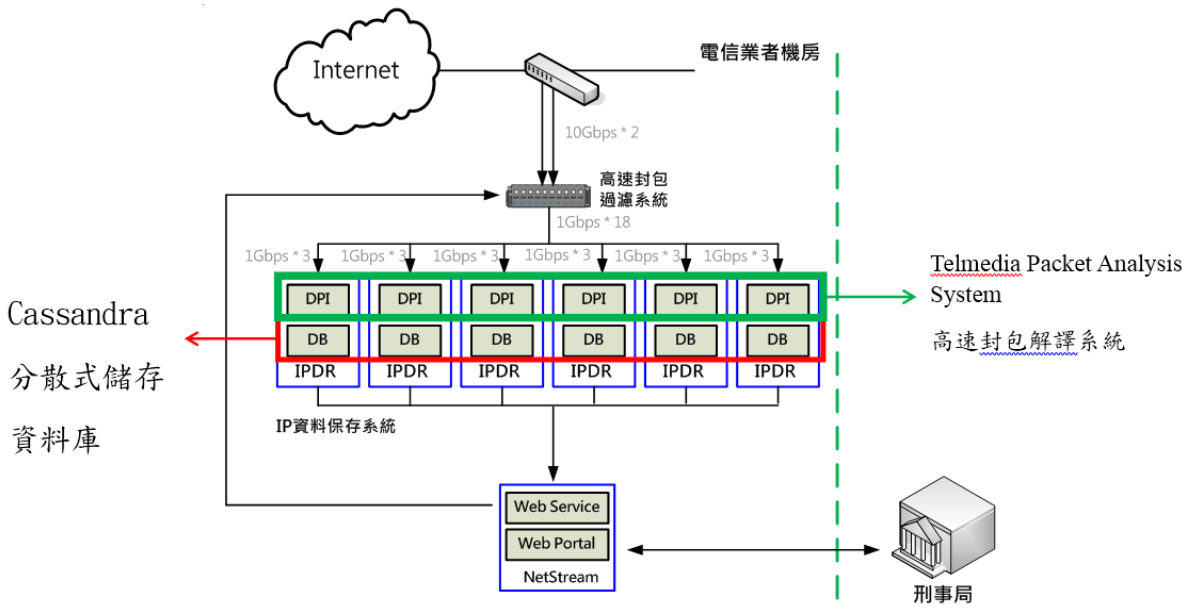


圖 5-27 DPI(Deep Packet Inspection)與分散式架構

（六）、力求測試環境與未來全面佈建環境相似：

1、透過電信業者網路收集大量真實網路環境資料，進行大量資料分析與過濾。

2、不得影響（或影響微乎其微）網路服務品質；且在尖峰流量超過 10Gbps（可達 12.5Gbps）的情況下，可快速過濾封包。

十、經濟效益（經濟產業促進）

（一）、因應網路已普遍採用加密、代理伺服器與匿名網路下，造成難以追查犯罪者真實身分與定位追蹤議題。運用大數據分析與 DPI 等相關技術，所獲得的成果，同樣可運用於商業發展上。現今在我國網路接取服務提供商（如 5 大電信業者），為因應大數據時代的來臨及掌握商機，目前也積

極打造網路資訊分析之機制。而本案發展之技術，正好也發展為商品，將應用於產業上。本案所獲技術可獲取之經濟效益例如：

1、各 APP 使用的流量統計資訊：對於網路接取服務提供商（例如遠傳電信），明白哪一個 APP 在甚麼時候耗掉大量頻寬，或者耗掉多少頻寬，是一件很重要的事，如果該 APP 耗掉大量頻寬造成廣大用戶使用其他服務不便，可以跟該 APP 服務提供者商業談判或者限制頻寬。

2、客戶的定位資訊：透過網際網路連線紀錄的儲存 Data Link Layer 的資訊），不透過 GPS 可獲取客戶之定位資訊。

3、客戶的喜好：透過客戶瀏覽的網站，可以某種程度知道客戶的喜好，例如經常瀏覽美食網站，可以知道客戶很喜歡美食。

4、客戶 APP 的使用喜好：瞭解客戶 APP 的使用喜好，對於網路接取服務提供商提供加值服務具有相當的助益。例如，某人大部分上網時間社群媒體都是在用 Facebook，又喜歡瀏覽瑜珈之類或美食等網站，服務提供商可以依使用者之需求，提供相關訊息給使用者。

5、客戶的作息時間：從客戶使用手機何時上網、何時沒

有使用手機等時間、目前移動的速度、目前的所在位置，可以推估目前活動的性質，例如是在搭公車、計程車，或在搭捷運、火車，或目前可能在銀行洽公、或是待在辦公室。因此，可以推估客戶的作息時間，再配合客戶的地理位置、客戶的喜好等，可以在客戶的可能出沒地點提供適當的服務，例如用戶正在等公車，而又知道客戶有看股票的習慣，可以提供客戶股市行情等相關訊息。

6、客戶的交友圈：透過網際網路連線紀錄的儲存，也可以知道在同一個網路接取服務提供商下，誰與客戶聯絡（以下稱與客戶聯絡的人為聯絡者）。透過聯絡者與客戶聯絡的密集度、時間、地點，還有客戶與聯絡者兩者個人的喜好、習慣等訊息等，可以進一步判斷是否為男女朋友關係、朋友關係、是否同一個家庭等。例如若為男女朋友關係、並且又判斷目前正在一起用豪華大餐，可以在這個時候推薦其他類似的餐廳或者是提供目前用餐餐廳的評價等。

7、交通路線提供：由網路接取服務提供商們聯合提供用路資訊，與地圖業者合作，告知客戶道路壅擠狀況，提供適合之路線資訊。

8、急難救助：GPS 定位資訊，一般使用者只會提供給例如 Google Map 等或有要求提供之 APP 使用，電信業者

或者各警政單位，並無法直接取得使用者之 GPS 定位資訊，因此，遇到緊急危難使用者又發不出求救訊號時（例如使用者已經昏迷或遭歹徒挾持），透過網際網路連線紀錄之即時查詢，便可獲知使用者之即時位置，而達到緊急救難之目的。

因此，在巨量資料的時代，網路接取服務提供者（如電信業者），若能進行網際網路資料之保存與分析，對該公司的營運發展，同樣有正面的發展（這種分析可以無需知道使用者知真實身分，故不牽涉到個資外洩問題）。

（二）、數位鑑識、資訊安全領域之運用：

1、惡意病毒分析研判：某種程度上，建立全國性的網際網路連線紀錄保存，透過分析，有機會追蹤調查惡意病毒的源頭。

2、謠言來源分析：如何追查謠言的源頭，可以廣泛的運用在治安、經濟等各層面。

（三）、匿名網路 Tor 之偵測可以預防相關資安事件：

1、勒索病毒(Ransomware)：例如 CryptoWall 4.0 依舊使用 Tor 匿名網路，而且持續利用受到危害的各網頁來散佈。而 TeslaCrypt，每一位受害者都會被提示要繳出等值於 500 美元的比特幣贖金，才能讓被加密的檔案解密。

2、公司內部攻擊：員工透過 Tor 連結公司內部網路，無法掌握從何處連上公司網路，是否為公司員工，還是只是盜用帳號密碼連結。另外，也無從知道透過公司網路連往何處。

3、殭屍網路與 APT 攻擊：公司內部資源被利用來當作殭屍網路的一部分，或更進一的被拿來發動進階持續性滲透攻擊。

4、品牌危害(Brand Damage)：公司網頁遭竄改，或者是被流言重傷。

5、網路間諜(Cyber Espionage) ：網路間諜同樣會利用匿名網路隱藏行蹤，攻擊政府機關或重大產業，從中獲取國防機密或商業情報。

6、執法機關面對網路戰：維護網路國土安全，避免國土遭受恐怖分子網路攻擊或利用匿名網路進行犯罪連絡。

貳、遠傳電信、臺灣大哥大及臺灣之星 4G 後端通訊監察系統（如圖 5-28）

除建置遠傳電信、臺灣大哥大及臺灣之星等 3 家 4G 電信業者之後端通訊監察系統，並與前端通訊監察系統整合，另可提供各警察機關線上查詢該 3 家 4G 電信業者之 4G GMLC 即時定位功能。此外，後端通訊監察系統可針對4G網路封包進行分析與APP軟體解譯辨識功能，其中除包含傳統通訊協定解譯的能力外，針對封包中可解析出之元素（如：圖片、檔案、文字、時間、地理位置資訊、身分識別資訊等）加以自動化整理及關連，於無法完整還原封包內容情況下，仍能提供

偵查人員有關嫌犯相關的各種人、事、時、地、物之資訊，以因應未來通訊監察需求，提升偵辦案件人員封包分析與解析相關證據之研究能力。

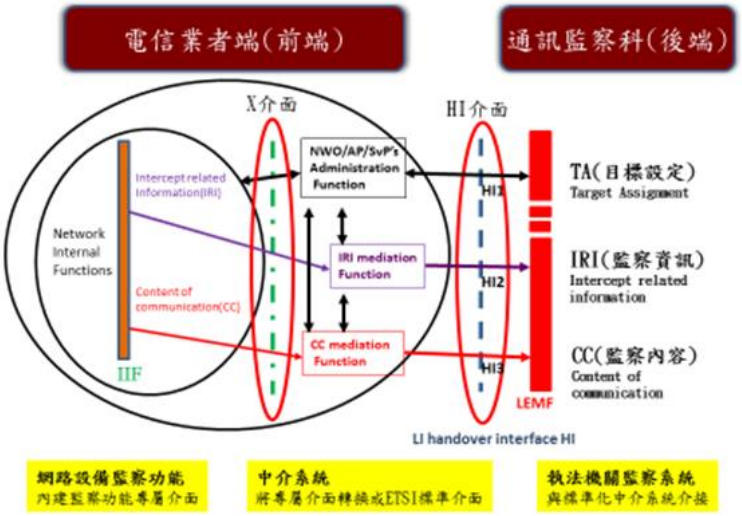


圖 5-28 通訊監察前後端介面

一、主要內容

（一）、臺灣大哥大及臺灣之星「4G GMLC 即時定位」功能，以及「3 家業者 4G 後端通訊監察系統」之軟硬體設備功能，3 家電信業者後端通訊監察系統之數據監察資料儲存量合計可達設定 7,500 線以上。

（二）、遠傳電信「4G GMLC 即時定位」功能，以及遠傳電信「4G 前端通訊監察系統」，3 家電信業者後端通訊監察系統之數據監察資料儲存量合計可達設定 15,000 線以上。

（三）、相關內容

1、符合 ETSI 及 3GPP 標準訂定，且為國際通用之監察標

準。

2、通訊監察系統包括：收集(Collection)、處理(Processing)、儲存(Storage)、操作(Operation)和分析(Analysis)等功能。系統須能將監察功能區分在不同的實體位置，刑事警察局通訊監察科北部機房負責彙集、處理及儲存功能；操作、分析及證據產出功能則分散在北、中、南機房。

3、4G 行動寬頻通訊網路及語音具備完整通訊監察能力之整合性功能，包括：

(1)、可在 4G 行動寬頻通訊網路設定監察目標（MSISDN、IMEI、IMSI、國際門號）。

(2)、收集監察內容(Content of Communication，CC)及監察資訊(Intercept Related Information，IRI)。

(3)、儲存與解譯監察資料。

(4)、讀取及管理通訊監察所得資料之工具。

(5)、證據光碟燒錄及管理。

(6)、IRI 與地理資訊分析。

(7)、針對電信業者提供之 VoLTE、CSFB 等語音通訊服務具備通訊監察能力。

(8)、能依據電信業者提供之監察目標授權數進行設定及監察。當監察目標數到達上限時，須提供警示訊息。管理人員可檢視各家電信業者的監察目標數量與上限。

4、完善報表與管理運作功能，包含投單與目標管理、電力設備、網路設備、通訊監察設備等之監控管理功能。

5、執行監察活動不影響電信業者網路之正常運作，且受監察用戶不會察覺。

6、模組化，且具擴充性，以因應未來更高階的系統容量及新型電信監察服務之輸入需求。

7、具備高度相容性，對既有系統造成之干擾降到最低。

8、完全協同運作(Interoperability)，以利集中管理、集中儲存、集中使用者操作介面與集中監視系統。

9、對所有輸入類型具有一致化的管理應用程式，使目標設定與定義、使用者管理及系統管理等功能達成一致性之運作及操控。

10、使用者操作程式是採用圖形化介面設計，使用者可透過統一的圖形化介面(GUI)呈現監察資料，如影音播放、資料瀏覽、轉譯等。圖形化介面(GUI)使用語言須為中文，呈現方式是配合需求進行客製化，具整合式的報表功能。

11、具線上即時監察資料儲存系統，並具備搜尋、分析及列印之功能，同時可支援監察對象內容之即時監察、記錄、儲存歸檔、可轉錄放映、分析、事後處理及解譯文檔的功能。監察資料儲存系統應具有資料備份及系統備援能力。

12、採「模組化」與「分散式」架構，其架構範圍為自最小單一工作站至超過 250 臺工作站的局部區域網路/廣域網路(LAN/WAN)技術連接用量標準，安全性登入以及遠端控制及監控使用狀態之資訊。每臺工作站均能操作此系統所提供之功能，遠端工作站能夠做開機登入動作，且系統功能均與近端的工作站相同。

13、證據產出系統以及分配與查詢功能結合光碟燒錄設備產出證據光碟。

14、開放性之介面，支援資料庫連結與具備資料匯入與匯出功能，可將資料輸出到其他系統。

15、有資訊安全相關防護措施，如建立防火牆，須安裝國際業界認證的防毒軟體套件，可設定當插入所有可抽換儲存媒體時能自動掃描所有儲存媒體。

（四）、收集與媒介子系統

1、能與 4G 前端通訊監察系統進行介接，其介面符合 ETSI 及 3GPP 所制定的通訊監察標準，包括（如圖 5-29）：

(1)、目標監察設定介面(HI1)：HI1 介面執行傳遞監目標指令至前端監察系統中，並具備手動與前端交換機或仲介系統同步監察目標之功能。

(2)、IRI 蒐集介面(HI2)：HI2 介面收集 IRI 並儲存於後端監察系統中。

(3)、CC 蒐集介面(HI3)：HI3 介面收集 CC 並儲存於後

端監察系統中。

2、系統介接服務供後端投單系統傳送監察目標資訊至前端系統。

3、正確的設定監察目標資訊於前端業者交換機設備上。

4、將監察目標產生之 IRI 及 CC，依據 HI2 與 HI3 標準傳送至後端系統。

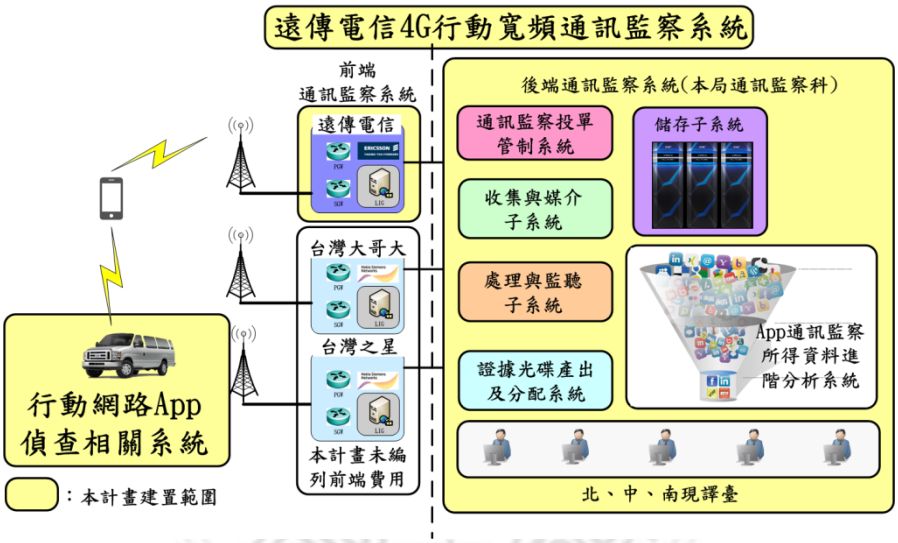


圖 5-29 收集與媒介子系統

二、處理與監聽子系統（如圖 5-30）

支援電信業者系統所提供之所有服務，系統可自動偵測所有不同訊號格式、資料連結協定、序列連結協定；將收集之語音、封包等資料與 IRI 進行處理關聯。

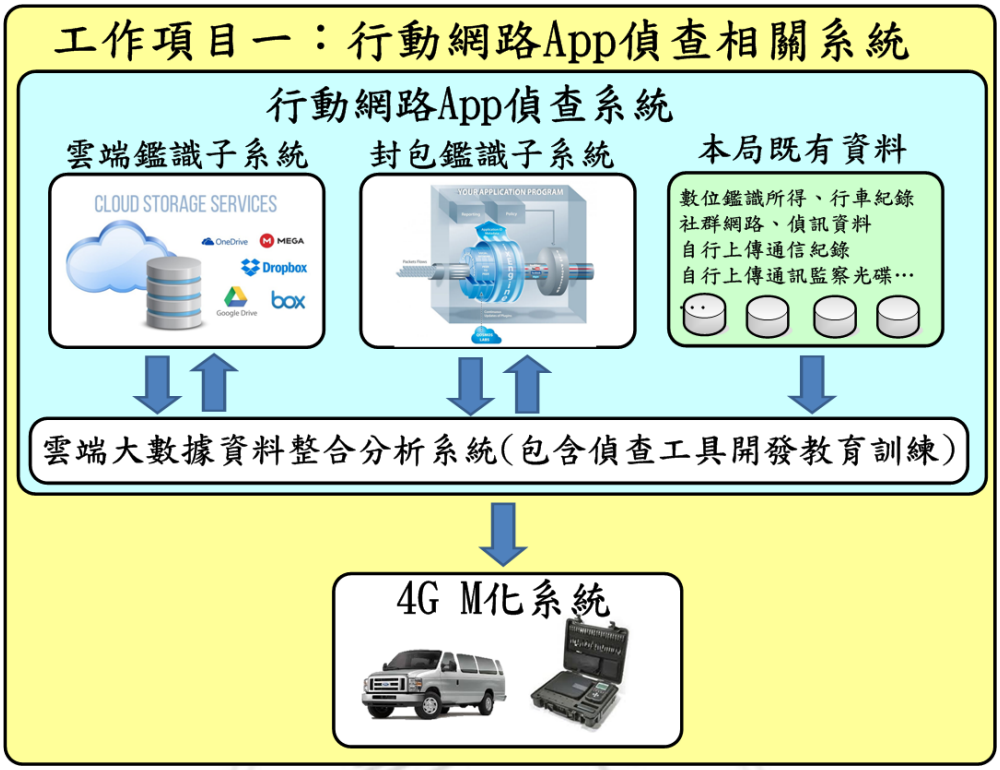


圖 5-30 處理與監聽子系統

三、M 化系統

（一）、系統設計需求：本案於現有電信業者之行動網路(3G/4G)或固網架構下（如圖 5-31），依所列目標，設計相關雛型臺。

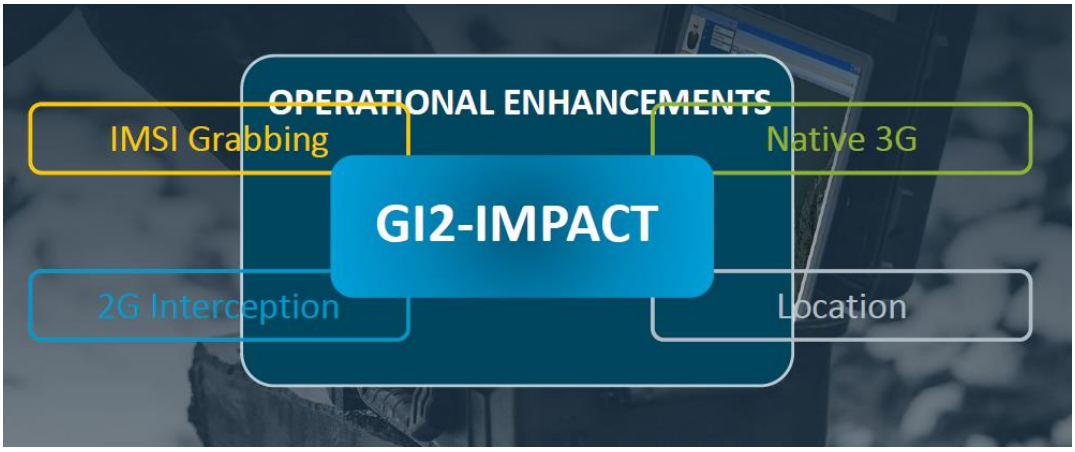


圖 5-31 M 化系統可操作管理

（二）、參考符合歐洲電信標準機構(ETSI)所訂定，為國際通用之

（三）、設計完善之管理運作功能。

（四）、執行監察活動不影響電信業者網路之正常運作，且電信網路用戶難以察覺。

（五）、為模組化之一部分，具彈性及擴充性，以因應未來更高階的系統容量及新型電信監察服務之輸入需求。

（六）、可以透過模組化方式擴充或升級，且對未來整體建置完成後的後續擴充所造成干擾降到最低。

（七）、未來相關設備可相互結合及協同運作。例如：集中管理、集中使用者操作介面與集中監控系統。

（八）、安裝國際業界認證的防毒軟體套件，可設定當插入所有可抽換儲存媒體時可以掃描所有硬體。

（九）、對所有輸入類型具有一致化的管理應用程式，該程式將使目標設定與定義功能、使用者管理功能及系統管理功能達成一致之運作及操控功能。

（十）、本平臺之操作者工作站程式為採用圖形化使用者介面之程式，使用者可透過統一的圖形操作介面（如圖 5-32）產生連線資料如影音播放、資料瀏覽、轉譯等(GUI)。

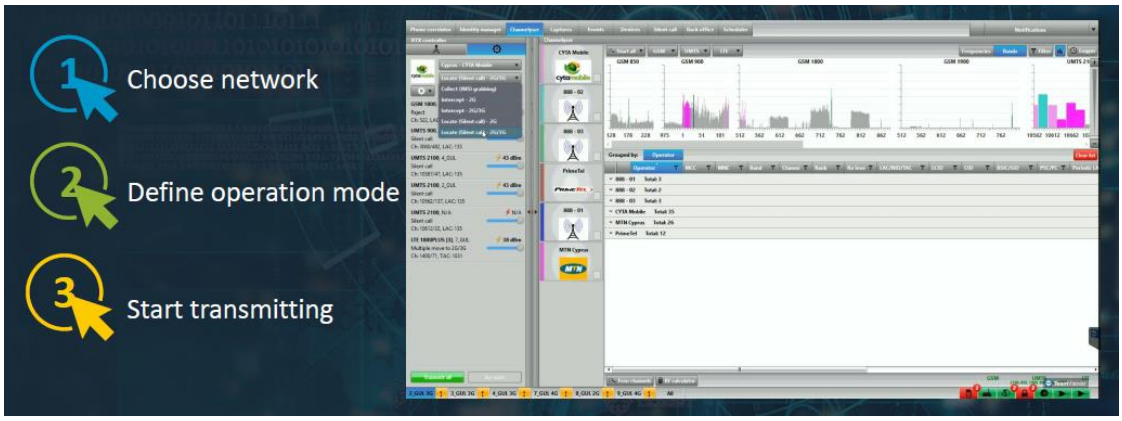


圖 5-32 M 化系統操作介面

（十一）、平臺之圖形操作介面(GUI)使用中文。

（十二）、系統功能需求外，配合將相關資料包含於「系統整合計畫」中作為測試驗收項目。

規格包含項目

規劃行動裝置及其應用程式安全性分析運用雛型實驗平臺系統架構如下（圖 5-33）所示。其中包括規畫建置於刑事警察局端的行動通訊裝置 APP 安全性分析平臺及移動式分析工作站，並整合前交付之 WiFi 戰術型系統，以驗證系統在實驗環境申可執行通訊監察功能。

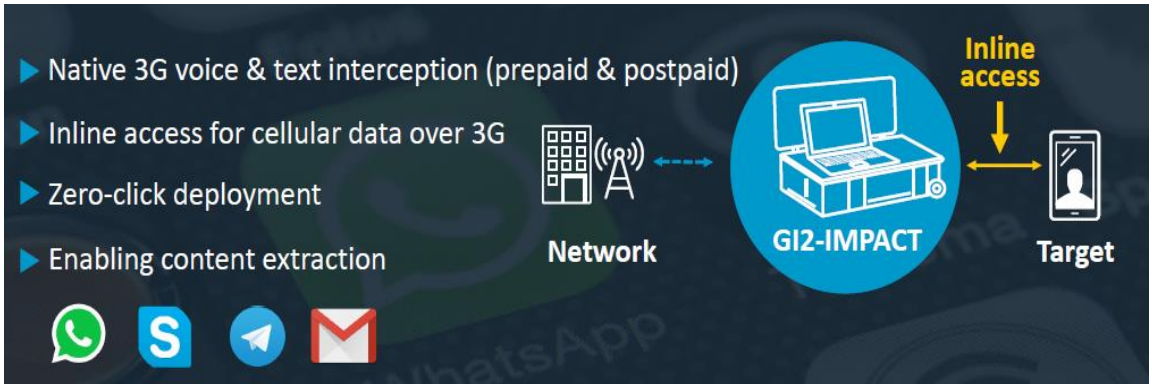


圖 5-33 經由 M 化系統可操作模式

以歐洲電信標準機構(ETS)所訂定，為國際通用之監察標準。

WiFi 戰術型監察系統(WiFi Tactical)為工作站等級的筆記型電腦，為設計完善的管理運作功能，對所有監察資料輸入類型具有一致化的管理應用程式，主要功能模組化包含（圖 5-34）：

1、WiFi 網路偵察：WiFi AP 掃描測試，阻斷 Target 原本使用的 WiFi AP 無線網路服務，讓 Target 連到 Fake AP。

2、封包擷取：所有封包或特定目標。

3、加密封包鑑識，針對使用「標準 SSL/TLS 加密通訊」的行動通訊裝置 APP：透過中間人手法(MITM)進行解密。

4、加密封包鑑識，針對使用「其他加密通訊」的行動 APP：透過反編譯(Decompile)或反組譯(Disassembly)，再進行逆工程(Reverse Engineertng)，進而達到針對加密通訊監控的反制。

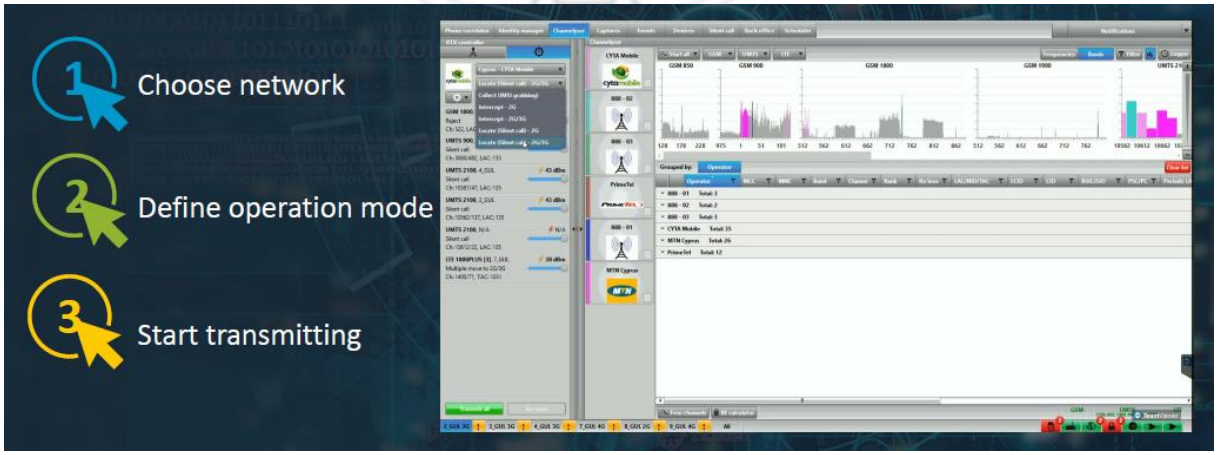


圖 5-34 功能模組化

管理偵查資料軟體功能包含：蒐集與匯入監察目標之封包、

封包（含 LS/SSL）解譯與還原（如 IM、Social Network、Email 等）、監察內容(偵查結果)呈現(依時間或依通訊協定類型檢視)、解譯與還原資料呈現（圖 5-35）。

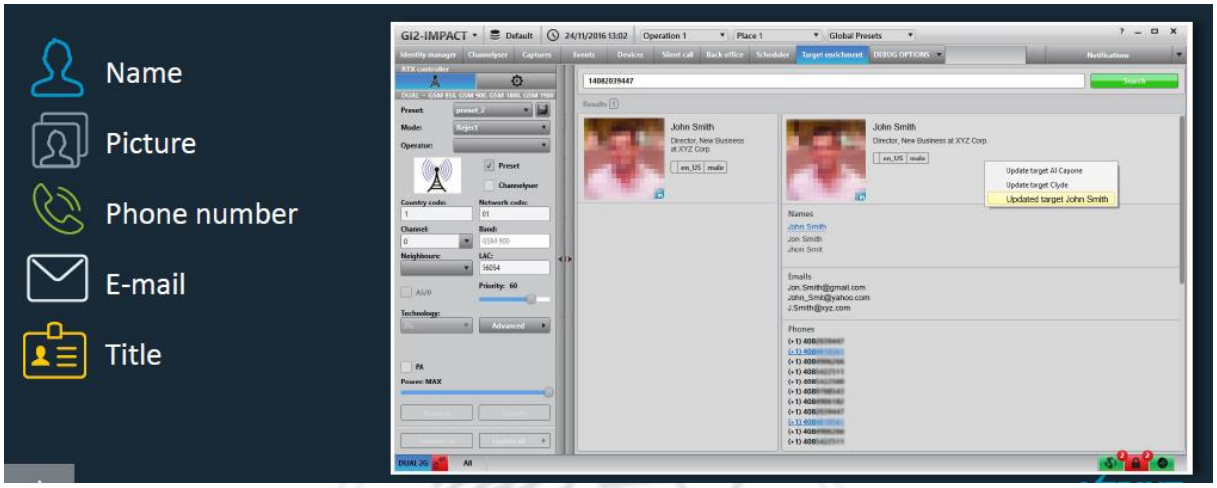


圖 5-35 個化分析操作

行動通訊裝置 APP 安全性分析平臺具備網路封包鑑識模組，可以對監察目標的網路封包進行分析，對監察目標的網路行為進行偵查，收集關於監察目標的重要情資，作為後續評估目標手機及 APP 安全性評估的依據。

四、M 化系統各種應用裝置

（一）、本案以常見的行動裝置作業系統（IOS 6.0 或 Android，且適用的作業系統版本至少分別為 IOS 6.0 6.0 以上或 Android 4.0 以上）或應用程式仍可供利用的安全性問題進行研究。

（二）、針對前項所提供安全性問題進行完整分析測試，以瞭解所

存在與適用的環境（包含作業系統與應用程式版本及裝置廠牌型號等）。

（三）、對前述交付可供利用之安全性問題，設計成為可供實驗環境中執行合法通訊監察工具，並提出完整報告，其內容至少包含交付之每個工具的功能（包含所能取得的資訊）、運作原理、限制條件、工作流程與具體執行步驟等。

（四）、因應行動裝置上的程式多變性，備有至少 3 套分析所需之移動式分析工作站及 3 組(6 臺)常見(IOS 6.0 或 Android）作業系統之行動裝置（應包含行動上網接取功能）（如圖 5-36)，並安裝相關工具軟體，以利改版時仍能分析其運作方式（如圖 5-37)；其中移動式分析工作站之規格至少包含如下：

1、中央處理器：Intel Core i7 或以上。

2、記憶體：8GB（含）以上（含擴充槽）。

3、硬碟：256GB SSD 或以上。

4、具備光碟機。

圖 5-36 各型機動 M 化系統

圖 5-37 M 化系統主機及應用

（五）、為避免目標察覺，提供相關機制或功能應有之偵測器材。

（六）、提供適當的監察所得資料顯示介面，以便驗證執行情況（如圖 5-38）。

（七）、相關功能供使用種類應盡可能囊括目前市面所常見的行動裝置與應用程式；其原理、所需設備、運作流程與方式及

執行時之限制。

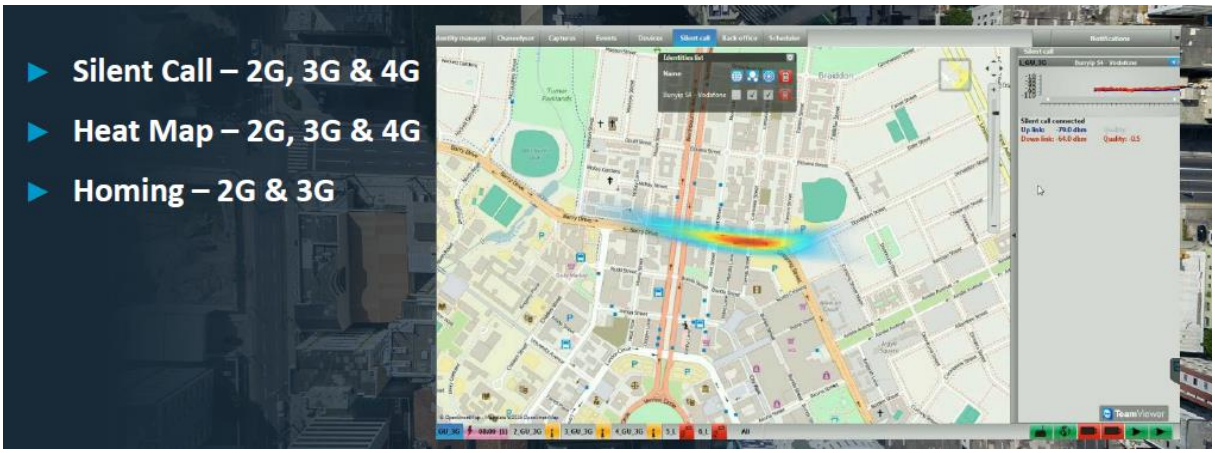


圖 5-38 監察所得資料顯示介面地理位置分析與搜尋

執行任務需求規格

WeChat 5.4.066(Android 4.4.2)：可攔截到文字訊息及多媒體（照片、語音、影片）內容。

LINE 4.6.1(Android 4.4.2)：可攔截到文字訊息及多媒體(照片、語音、影片）內容。

整合 CIB 通訊監察系統：目標監控管理系統(Monitoring Portal)

偵查人員透過移動式分析工作站或者 WiFi 戰術型系統所將監控軟體（包含經過逆向工程修改過的行動通訊裝置 APP 或特製的監控程式）以不同的手法植入目標手機（如：社交工程、取得實體手機、或手機的安全性漏洞等)。這些監控軟體會將目標手機的資料回傳到目標監控管理系統。

參、通訊監察內容分析平臺

網路封包是網路上用來傳輸資料的最小單位，網路封包(Packet)因為不同的應用服務或通訊協定，而有各種不同的大小與樣態。依據不

同的通訊協定，其網路封包的結構會有些許的差異。一個網路封包是由標頭(Header)和資料(Data)所組成，網路封包的屬性被詳細地定義在標頭中，包括其使用的通訊協定(Protocol)、來源 IP 位址(Source IP Address)、來源通訊埠(Source Port Number)、目的地 IP 位址(Destination IP Address)、目的地通訊埠等欄位(Destination Port Number)。

網路封包分析對於犯罪偵查，在於網路封包分析除了能夠找出異常之網路行為和網路流量外，也可以分析出 IP 通聯，強化犯罪偵查作為。一般常見的網路封包分析工具有 Tcpdump、NetworkMiner、Ethereal、Wireshark 等。網路封包分析工具已被廣泛應用於犯罪偵查上的網路封包解析，網路封包分析工具能支援解析的通訊協定多寡，決定了此網路封包分析工具可使用的範圍。另外網路封包分析工具通常都會提供一些條件過濾的功能，讓使用者針對特定的目標來分析網路封包，此有助於發現網路通訊的異常行為。

通訊監察面臨之困境

4G LTE 行動無線寬頻網路帶動行動通訊裝置 APP 蓬勃發展，通訊軟體提供網路電話、文字及多媒體訊息等資訊分享，因其免費、方便，又具備加密機制，已成為時下最流行的溝通方式。也因通訊軟體的加密特性，導致大量犯罪者運用各種通訊軟體進行犯意聯繫，躲避司法人員之犯罪偵查。且通訊軟體的服務廠商多處境外，由於相關法令尚未完備、無法要求業者提供通訊內容紀錄與解譯，遂衍生出通訊軟體通訊之監察結果無法解譯的問題。

另外，目前網站多半採用 HTPPS 加密通訊協定，同樣造成此行為

之通訊監察結果無法解譯、監察光碟內容呈現亂碼的情況；且在通訊軟體之加密機制無法突破的情況下，為獲取有效之偵查情資，故採取網路封包分析方法，以協助第一線偵查人員從中擷取偵查情資，提供犯罪偵查使用。

若欲進行通訊監察內容之網路封包解析，需要具備相關網路通訊基礎知識。然而目前第一線偵查人員多非資通訊相關背景人員，為解決通訊軟體加密、無法通訊監察之問題，以及第一線偵查人員多不熟悉網路封包分析相關技巧等狀況，刑事警察局通訊監察科根據通訊監察光碟內容格式，發展網路封包分析工具；令第一線偵查人員在進行通訊監察後，能夠運用此工具進行通訊監察內容的解析。

一、光碟內容的解析

通訊監察證據光碟是將通訊監察所得之內容（包含CircUitSwitch 與 PacketSwitch 的資料），以影音、文字或圖片等形式呈現，供第一線偵查人員辦案使用。通訊監察所得資料依所屬資料類型可分為「語音」、「電子郵件」、「網頁瀏覽」、「社群網路」、「即時通訊」、「非通話事件」與「其他」。其內容分述如下：

（一）、語音：語音 (Circuit Switch)、手機簡訊、影像電話、SIP 網路電話、傳真等。

（二）、電子郵件：使用 Outlook、Outlook Express 等電子郵件傳送或接收之資料。

（三）、網頁瀏覽：網頁信箱，以及所有以網頁瀏覽之資料皆歸屬

在此類型。

（四）、社群網路：Plurk、Twitter、Facebook 等。

（五）、即時通訊：使用 MSN、Yahoo Messenger 等即時通訊內容。

（六）、非通話事件：包含 CS(Circuit Switch)、PS (Packet Switch)之非通話事件。

（七）、其他：包含 FTP、Telnet、Multimedia、Http 傳輸的 File、P2P 等未歸屬在（一）至（六）項類型之資料。

DPI Viewer 工具之系統功能說明

刑事警察局通訊監察科提供的網路封包分析工具，其名為 DPI Viewer，就是要將證據光碟中的網路封包 (PacketSwitch) 部分進行分析解譯。透過證據光碟中通訊監察內容的網路封包分析與解譯，可提供第一線偵查人員更多元化的犯罪偵查情資來源，是為本工具 DPI Viewer 開發之目的與目標。

DPI Viewer 的操作方式如下：第一線偵查人員在取得證據光碟後，輸入該證據光碟之帳號密碼，在成功掛載虛擬硬碟 Q 槽後，可使用選項匯入證據光碟選項，會自動列出該證據光碟中所有之通訊監察目標，勾選欲分析之通訊監察目標後，將進行網路封包資料彙整，並進行網路封包解譯與結果呈現。

二、資料來源：封包分析工具 DPI Viewer 可透過下列三種方式取得欲分析的網路封包資料。

（一）、Pcap 檔案：直接匯入 Pcap 網路封包檔。而 Pcap 網路封包檔可透過多種方式取得，例如運用 Wireshark 軟體進行網路封包錄製。

（二）、通訊監察證據光碟：直接匯入通訊監察過程取得的證據光碟中所錄製的網路封包資料，選擇證據光碟中欲匯入的監察目標資料。

（三）、LIFS 資料檔：直接選取 LIFS 資料夾，本工具可直接讀取該資料夾中相關的網路封包資料，進行解譯作業。

三、網路連結分析：可對連結特定目標網站的網路封包進行檢視，進而瞭解監察目標之使用的網頁網址觀察活動狀態。

四、DNS 使用歷程：可解譯出監察目標所使用的相關 DNS 資訊歷程，進而確認監察目標使用的戶與 Hostname 資料內容。

五、網頁瀏覽歷程：可檢視該監察目標其網路封包所連上之網頁歷程以及該網頁之 Host 資料。

六、圖片解譯：DPI Viewer 可檢視該監察目標其網路封包中所接收傳送的圖片資訊。通訊軟體如 LINE 所傳送的部分圖片也可透過系統進行顯示呈現。在圖片解譯部分，DPI Viewer 提供的功能有：依不同網站/APPs 將圖片分類；依據影像類型瀏覽；依據 URL 或時間進行排序；提供三種不同大小的影像縮圖；單擊圖片顯示影像相關資訊，如 Host、User Agent 以及 Data Time 等；雙擊圖片可單獨進行

瀏覽；依據不同社群進行分類，方便瀏覽相關圖片（如圖 5-39）。

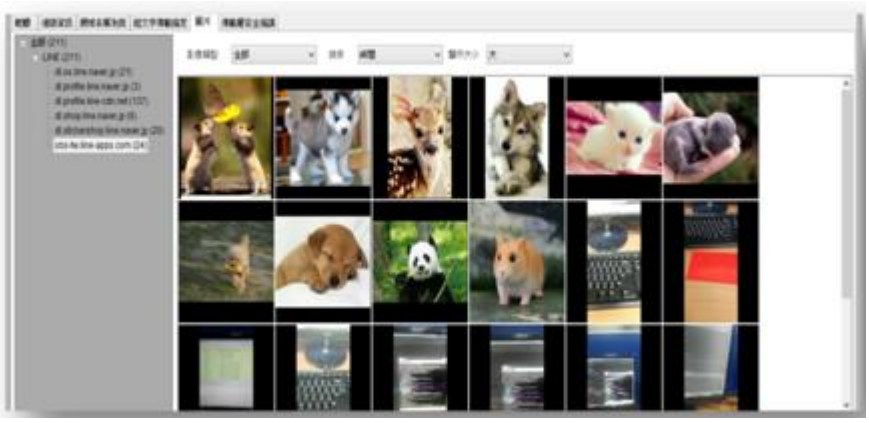


圖 5-39 封包分析軟體能還原封包內未加密之圖片/電子郵件/網頁

七、通訊協定使用歷程：DPI Viewer 可呈現各種通訊協定使用的歷程。

八、過濾檢視：如網路封包資料量過大，可透過 DPI Viewer 的過濾功能進行結果篩選後再呈現。

九、清單：此功能可顯示網路 Domain (DNS)、Email、lD/Password、電話等資訊。

在監察到加密的通訊內容時，雖然從證據光碟中無法解譯其通訊內容，但可運用此加密的通訊內容之網路封包以萃取出可用資訊，並以此資訊建構出可能的偵查線索。但有時加密之通訊軟體無法解密，亦會造成偵查困境之問題。

此外，網路封包分析軟體並不會主動偵測異常網路封包的行為，當運用網路封包分析軟體進行網路資料分析時，網路封包分析軟體並不會主動警告異常的訊息，而是要運用此分析軟體的特性與功能，由資料分析者尋找可能存在的異常情況。DPlViewer

是要幫助第一線偵查人員以通訊監察證據光碟為資料來源，運用此工具找出網路封包中可能存在線索的地方。

肆、可攜式封包解析設備建置

IP(Internet Protocol)網路技術的成熟，使得網際網路(Internet)變得普及，幾乎目前所有類型的接取技術，如 xDSL、Cable、3G、4G 等都可以支援 IP 通訊協定。在 IP 通訊協定之上各種多樣化的應用技術，如電子郵件(Email)、全球資訊網(World Wide Web)、網路電話(VoIP)即時通訊(Instant Messaging)、社群網路(Social Network)等，讓資訊的取得以及人與人之間的溝通變得更加容易。犯罪集團已逐漸走向大量運用新興科技工具，介入傳統犯罪的趨勢，例如利用簡訊、即時訊息、社群網路散佈訊息進行網路詐欺、透過 VoIP 電信詐欺，以及透過網路進行下單、簽賭，散播非法色情，散播「假新聞」、駭客攻擊、甚至販毒、綁票勒索等跨國犯罪等案件（如圖 5-40）。

圖 5-40 可攜式封包解析設備

為避免二類電信、IDC 機房或其他網路服務提供者成為歹徒規避偵查的管道，因此建置「可攜式封包解析設備購置計畫」，建構「可攜帶」之通訊偵查設備，透過封包解析以追查犯罪行為（如圖 5-41）。

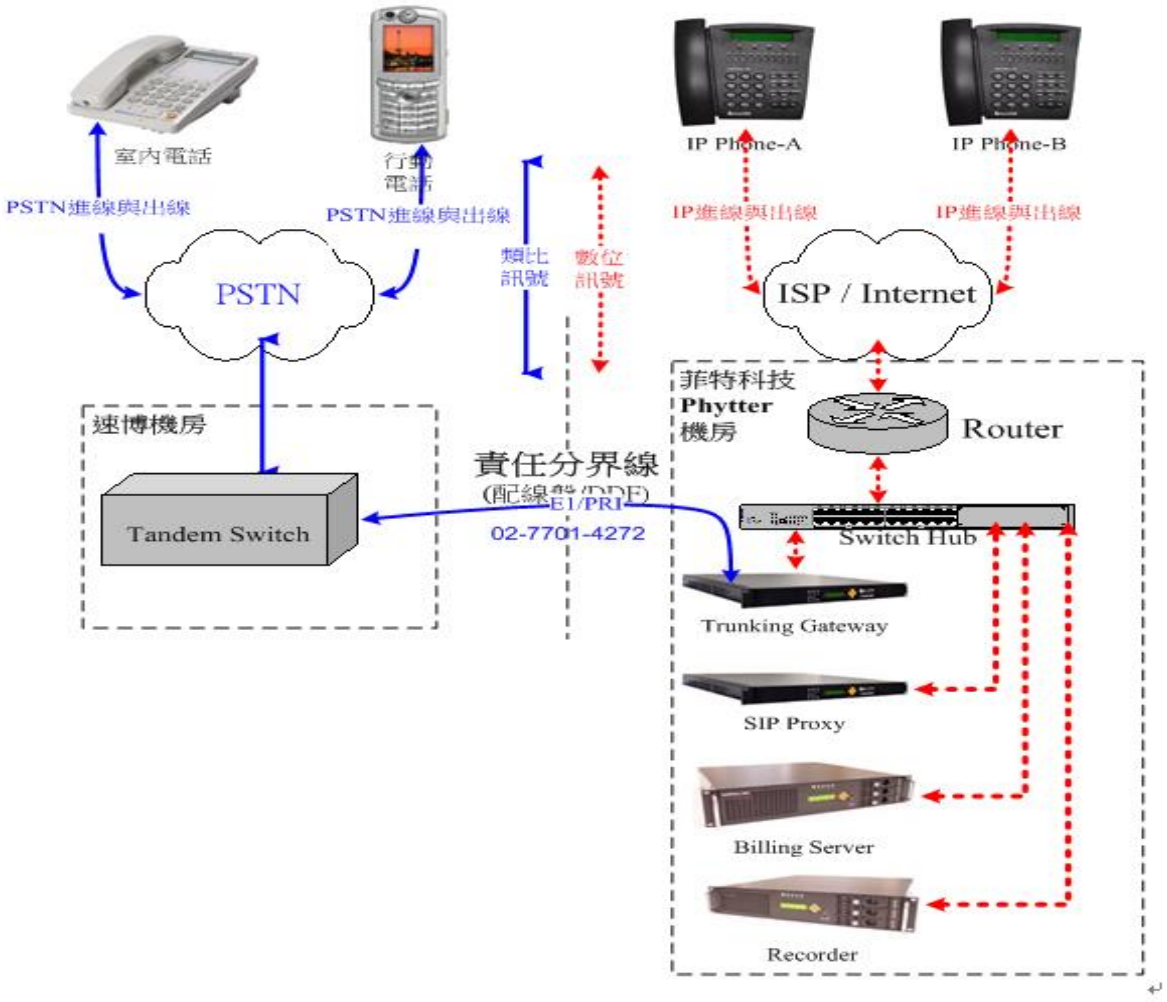


圖 5-41 封包解析設備通訊監察架構圖

一、為何及何時使用戰術型：

二類電信之網路電話業者（E.164 或非 E.164），依 NCC 規定需建置通訊監察系統並通過刑事局或調查局之審驗，故不一定需要戰術型設備，而網際網路接取服務的業者（如有線電視公司、主機代管業者等），並未建置通訊監察系統，故以戰術型設備進行通訊監察。

二、網路架構示意

可攜式封包解析設備本身可支援目標或鏈路封包解譯、分析等功能，並回傳通訊監察科後端系統（如圖 5-42）。

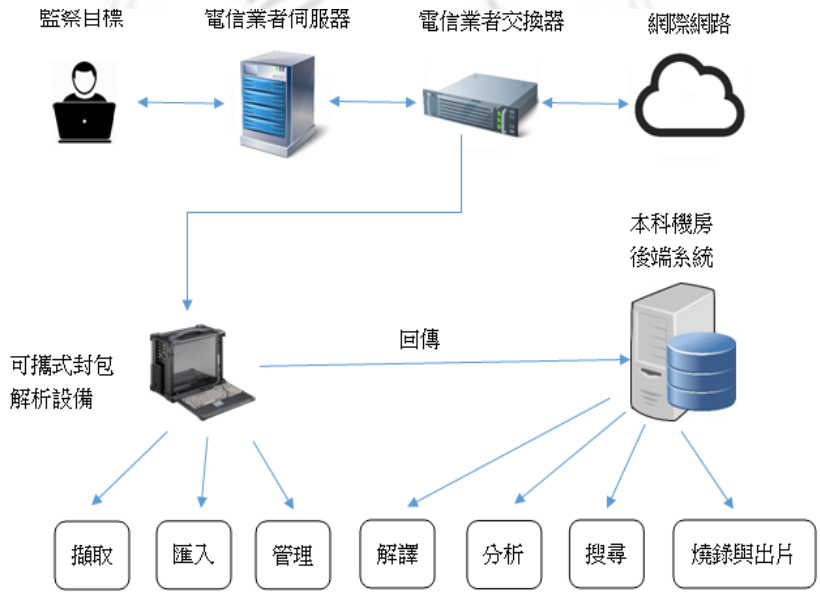


圖 5-42 可攜式封包解析設備網路架構

三、資料回傳檢視

監察資料均須燒錄成監察光碟再提供予案件承辦人，以便於管制。案件承辦人親至通訊監察科取回光碟，監察光碟內附有軟體，可解析監察資料。

第六章 結論與建議

第一節 結論

壹、積極發展新的數位偵查與鑑識方法

隨著資訊科技進步，為查緝犯罪所需，在技術上得採取之偵辦手段經緯萬端，惟當執法機關以駭客手法取得犯罪證據，固然在技術上不成問題，惟在現行法之框架下，仍需進一步思考，本研究已就我國通訊監察之困境而提出之可能改變方向。

對司法人員而言，科技蒐證設備是水能載舟，亦能覆舟，雖然科技能蒐集數位證據，而數位證據在現今所有犯罪類型，扮演極重點之角色，但司法人員應該對於科技蒐證設備之挑戰有警覺性，過去不曾被質疑監聽工具現在飽受爭議，以往一些法律要件被視為常規而理所當然被忽視的，而今卻屢屢有爭執空間，就新型態之數位證據蒐集工具方面，司法人員辦理以行動通訊裝置 APP 為犯罪工具之案件應對於法官的懷疑，以及辯護人的異議要有準備，不可不慎。

帶動整體刑事偵查科技品質的提升，是本研究目的之一；對於國內目前盛行的行動通訊裝置犯罪之偵查技術研究方面，本研究亦期能引導國內司法警察機關提升科技辦案能力，在以行動通訊裝置為犯罪工具快速增長，手法快速變化、科技化、專業化、與全球化時代，這類犯罪已為警政工作的嚴重挑戰之一，行動通訊裝置犯罪偵查也為辦案重點工作之一。

我國行動通訊裝置犯罪其中又以詐欺最為嚴重，只要擁有社群網路服務（例如 Facebook）或者網路即時通訊服務（如 LINE）者，幾乎人人接過詐騙訊息，另外，如比特幣洗錢、網路勒索、竊盜個資等。而科技犯罪偵查重點之一為須知道傳送訊息者之真實身分（個化使用者）與目前的地理位置（追蹤他的位置）。

由於各式各樣社群網路、網際網路應用服務(APP)的大量使用，在運用加密、匿名網路、且 APP 服務提供者大多位於國外及雲端儲存下，數位偵查與鑑識已愈發困難，治安機關面臨難以透過封包解譯或網路接取服務提供者調閱通聯紀錄而追蹤個化使用者之困境。因此，有必要從不同的出發點，發展新的數位偵查與鑑識方法。

貳、本研究所獲成果

一、本研究中因應行動通訊裝置 APP 為犯罪工具提出構想，透過 IP 連線資料保存（或稱為網際網路連線紀錄保存、IP Meta Data 保存），來獲得網路上虛擬歹徒的真實身分，並達成定位追蹤的目的。本實務應用平臺為延伸 103~105 年的驗證研究，提出行動通訊裝置 APP 自動化社群網路資訊分析實驗平臺，發展 Tor 匿名網路之偵測，及 IP 連線資料保存之應用，期能對發覺歹徒真實身分，提供相關機關偵辦行動通訊裝置 APP 及建立（或修法）網際網路連線紀錄保存之參考。

二、經由遠傳電信、台灣大哥大及台灣之星 4G 業者之通訊系統，除了建置遠傳電信、台灣大哥大及台灣之星等 3 家 4G 電信業者之後端

通訊監察系統，並與前端通訊監察系統整合，另可提供警察機關線上查詢該 3 家 4G 電信業者之 4G GMLC 即時定位功能。此外，後端通訊監察系統應可針對 4G 網路封包進行分析與 APP 軟體解譯辨識功能，其中除包含傳統通訊協定解譯的能力外，針對封包中可解析出之元素（如：圖片、檔案、文字、時間、地理位置資訊、身分識別資訊等）加以自動化整理及關連，於無法完整還原封包內容情況下，仍能提供偵查人員有關嫌犯相關的各種人、事、時、地、物之行動通訊裝置 APP 偵查系統：包含雲端鑑識子系統、封包鑑識子系統，以及雲端大數據資料整合分析系統。

三、本研究參考符合歐洲電信標準機構(ETSI)所研發，為國際通用之監察標準。建立 4G M 化定位。以主動出擊方式機動定位並以智慧手機漏洞中間人攻擊法木馬程式蒐集歹徒 APP 資訊。

四、在監察到加密的通訊內容時，雖然從證據光碟中無法解譯其通訊內容，但可運用此加密的通訊內容之網路封包以萃取出可用資訊，並以此資訊建構出可能的偵查線索。但有時加密之通訊軟體無法解密，亦會造成偵查困境之問題。「可攜式封包解析設備購置計畫」，建構「可攜帶」之通訊偵查設備，透過封包解析以追查犯罪行為。

第二節 本研究貢獻

壹、理論貢獻

對創新概念的理解最早主要是從技術與經濟相結合的角度，其在

於探討技術創新在經濟發展過程中的作用，主要代表人物是現代創新理論的提出者約瑟夫·熊彼特。獨具特色的創新理論奠定了熊彼特在經濟思想發展史研究領域的獨特地位，也成為他經濟思想發展史研究的主要成就。

創新的五種情況：熊彼特進一步明確指出創新的五種情況：後來人們將他這一段話歸納為五個創新，依次對應產品創新、技術創新、市場創新、資源配置創新、組織創新，而這裡的組織創新也可以看成是部分的制度創新，當然僅僅是初期的狹義的制度創新。

本研究為突破對歹徒以行動通訊裝置 APP 為犯罪工具之偵查盲點，先行應用創新理論建置監察行動 APP 通訊軟體實驗平臺、行動 APP 通訊軟體監察技術實驗平臺、社群網路偵查暨鑑識技術實驗平臺、戰術型 WiFi 網路 APP 偵查系統規劃與驗證計畫、跨境戰術型 IP 通訊監察系統、行動裝置及其應用程式安全性分析運用雛型實驗平臺與提升新世代社群網路偵查暨鑑識能量計畫（建置雲端與 IP 定位資料保存規範機制實驗平臺）等實驗平臺，經驗證可行性後，再將驗證成果技轉建制偵查與分析平臺。

經實驗平臺技轉之驗證偵查與分析平臺為社群網路偵查暨鑑識能量建置、遠傳電信、臺灣大哥大及臺灣之星 4G 後端通訊監察系統（含M化偵測系統與子系統）、網路封包分析平臺、可攜帶封包解譯系統等，為司法人員在偵辦歹徒以行動通訊裝置 APP 為犯罪工具案件之偵辦提供莫大助力。

貳、實務貢獻

對辦案技術重大突破培訓第一線執法人員面對社群網路平臺上之犯罪行為時，具有犯罪資料之蒐集、處理與分析能力，強化社群網路犯罪偵查能量：

一、強化社群網路犯罪偵查模式，培育社群網路犯罪偵查專才並發展偵查作為所需之資訊技術。

二、發展社群網路犯罪偵查之工具，強化社群網路犯罪偵查技巧與資料來源，輔佐傳統犯罪偵查手法之不足。

三、社群網路技術日新月異，警察機關如未能持續研究新興科技，將無法遏制歹徒運用此新興科技進行犯罪以逃避員警查緝，造成政府公權力喪失。因此強化員警社群網路犯罪偵查能量、提升刑事科技偵查水準，可讓社會公平正義得以伸張。

四、29 種應用服務分析：完成識別 Plurk、PTT、Facebook、Twitter、LINE、WhatsAPP、Gmail、Google+、Yahoo Messenger、WeChat、QQ、Telegram、Juiker、Skype、Instagram、Flickr、YouTube、Google Drive、Yahoo Mail、AOL Mail、Outlook、網易郵箱、Hangouts、Mobile01、17 直播、LinkedIn、M+ Messenger、Tor 洋蔥路由器等應用服務，經驗證可找出可疑目標的時間不到 1 秒，且縮小可疑目標數量，DPI(Deep Packet Inspection)最大的流量可達 12.5Gbps。結合現有資源，簡化使用者資料匯入、匯出、轉碼等繁複的操作，可大為提升辦案的效率，系統整合包含：證據光碟資訊、通聯調

閱與定位資訊、社群網路公開訊息蒐集等。

本研究在經由實務驗證平臺分析結果顯示在辨識網路上使用者真實身分、雲端運算及 IP 連線資料保存資料庫、結合現有資源，強化犯罪偵查、強化封包分析能力、強化嫌犯行為分析、力求測試環境與未來全面佈建環境相似偵查環境等，這些成果對於歹徒利用簡訊、即時訊息、社群網路散佈訊息進行網路詐欺、透過 VoIP 電信詐欺，以及透過網路進行下單、簽賭，散播非法色情，散播「假新聞」、駭客攻擊、甚至販毒、綁票勒索等跨國犯罪等案件之偵辦具有積極效果，足以提供實務單位作為高科技犯罪之犯罪偵查的應用與辦案方式之參考。

第三節 建議

壹、延續本研究成果繼續辦理

目前本研究所得成果，已初步應用於犯罪偵查上，惟如果要能夠更有效之應用，需有我國網路接取服務提供商配合建置。警政單位（內政部警政署刑事警察局）應積極與相關主管機關，研商配合事項。

本研究中之網路 Meta Data 大數據分析應用問題，應用於辨識犯罪者之真實身分與定位追蹤，是一個理論與實務並重之應用科技，匿名網路與加密的發展，不易研究個體與群體網路行為。故持續加強與學界互動，應能對本研究再更進一步有實質的提升，對於 Meta Data 可有更豐富之研究。

透過匿名網路進行比特幣之交易，已成為犯罪分子洗錢、非法交易、綁票勒贖的安全管道，如何進行比特幣金流之管制與追蹤，為未

來可以繼續精進的方向。另目前國家正推動 DNS Log 保存，期於未來研究利用 DNS Log 進行犯罪追蹤方法，惟項目複雜目前並未有接續計畫。

貳、放寬網路通訊監察限制

一、因使用網路從事犯罪行為，緝捕時機稍縱即逝，且現今通訊容易不只文字，尚有圖片、語音、影像等，通訊內容因容量龐大而保存不易，如通訊監察時，固守監察通訊種類及號碼等足資識別之特徵，恐失制敵機先之時效，是在網路通訊監察或是通訊軟體監察時，不妨引進美國「機動式監察(Roving Wiretap)」方式，在限定之重罪，不特定通訊監察之地點、方式，僅針對所觸犯之罪名進行監聽，在犯罪嫌疑人頻頻更換通訊方式，或通訊種類時，方能收監聽之效。

二、行動通訊軟體業者大部分是國外業者，公司及伺服器放置於國外，執法機關因管轄權問題，無法源向相關業者要求提供通訊監察協助，實務上通常透過協商方法，請外國業者配合。立法機構應參考網路犯罪協定等跨國追緝犯罪國際公約，制訂符合追緝跨國犯罪國際公約之法律以利與國際司法機構接軌，並透過外國司法機構向相關業者要求進行通訊監察。另行動通訊軟體若在國內無任何分公司或窗口可供聯繫，應於電信法規修訂國內第 1、2 類電信業者可封鎖該軟體於國內散佈使用條款，以確保犯罪者無法利用通訊軟體逃避追查。

參、配合辦理

一、法令的規定嚴格的限制了偵查作為與偵查技術研發，尤其通保法自民國 103 年修正後，對司法人員在偵辦案件所加諸的限制與程序大幅增多，確保了人權與隱私，卻限制了辦案人員的作為，援此，今後對於相關法令的增修，行政與立法部門應積極配合，與時俱進。

二、行動通訊裝置軟體很多公司設於國外，其配合本國司法機關辦理犯罪偵查之意願不高，嚴重影響辦案期程，政府相關部門應挺身協調辦理。

參考文獻

一、中文部分

1.翁豪健（2015），APP 行動學習於能源教育之應用，國立高雄應用科大學電機工程系博碩士班碩士論文，高雄市，取自 https：//hdl.handle.net/11296/sdtr2c。

2.侯友宜(2011)，網路電信偵查理論與實務，警政署內部資料，未發行。

3.黃茂穗（2014），智慧手機興起對通訊監察的挑戰與因應之研究，中央警察大學犯罪防治研究所博士論文，桃園市。

4.蘭文裡(2011)，百里九十：我愛APP，臺北市:數位典藏與學習電子報。

5.馬克.古德曼（2016），未來的犯罪，臺北市：木馬文化出版。

6.蔡明德、許博堯、張簡耀暉(2010)，電信號碼於異質網路之整合研究，國家通訊傳播委員會九十九年委託研究報告，臺北市：財團法人電信技術中心，取自 https：//www.ncc.gov.tw/chinese/files/11021/1813_19071_110217_1.pdf。

7.黃逸玲（2018），行動通訊 APP 偵查與對策之研究，中央警察大學研究所碩士論文，桃園市，取自 https：//hdl.handle.net/11296/jyt6w4。

8.陳鼎駿（2012），網路監聽範圍之研究─以我國「通訊保障及監察法」為中心，世新大學法律研究所碩士論文，臺北市，取自 https：//hdl.handle.net/11296/r5ra68。

9.梁哲賓（2019），通訊監察與犯罪分析，警政署內部資料，未發行。

10.黃翰文(2013)，android phone 的即時通訊應用程式訊息紀錄鑑識方法，臺北市：刑事雙月刊，頁 38-43。

11.朱子函(2017)，我國網路通訊監察困境之研析，臺北市：刑事雙月刊，頁 56-59。

12.蘇俊吉(2016)，行動通信的演進歷程，臺北市：科學發展月刊 9 月號，頁 58-63。

13.田哲夫（2008），科技犯罪防制工作中程計畫簡介，臺北市：刑事雙月刊第 27 期，頁 12-15。

14.蘋果日報（2013），調查局語出驚人 LINE、WhatsApp、WeChat 都能監聽，蘋果新聞網，102 年 10 月 10 日。

15.陳順和（2015），行動電話簡訊詐欺犯罪問題之成因與對策探討，臺灣大學政治學研究所碩士論文，臺北市。

16.王澤鑑（2007），人格權保護的課題與展望（三）-人格權的具體化及保護範圍（6）-隱私權（上）、（中），臺北市：臺灣本土法學雜誌 96、97 期。

17.自由時報（2016），岸巡士官為績效偷裝 GPS 被認定違法，105 年 10 月 21 日。

18.黃冠傑（2018），論修正通訊保障及監察法－監聽之審查與實施，臺北市：48 期學員法學研究報告，未出版。

19.自由時報（2019），5G 商轉時間，5G 賽跑美國領先韓、日，英緊追，108 年 4 月 20 日。

20.劉孟奇（2013），資訊通信科技與犯罪率之實證研究，臺北市：犯罪學期刊第 16 卷第 1 期，頁 1-27。

21.王勁力（2010），論我國高科技犯罪與偵查－數位證據鑑識相關法制問題，臺北市：探究台灣／科技法律評析/第 3 期/，頁 209-273。

22.米歇爾・紐頓著（2007），刑偵高科技犯罪百科全書，上海：科學技術文獻出版社。

23.馬進保（2012），高科技犯罪研究，中國人民公安大學出版社。

24.林俊峰（2009），跨國洗錢之研究，建構網路詐欺犯罪整合偵查流程之探討－以我國 93-105 年網路詐欺案件為例，法務部 98 年選送檢察官出國進修計畫。

25.張志炁（2012），我國高科技犯罪偵查能量之研究-以網路犯罪為例，華梵大學資訊管理碩士論文，新北市。

26.陳建舜(2011)，以灰預測探討網路犯罪之研究，中華大學資訊管理學系碩士論文，新竹縣。

27.左育丞（2012），行動 iPhone 之高科技犯罪與數位鑑識研究，中央警察大學研究所碩士論文，桃園市。

28.王旭正（2013），科技犯罪安全之數位鑑識：證據力與行動智慧應用，臺北市：博碩文化股份。

29.張謹名（2014），科技犯罪與防制-電腦與網路犯罪初探，國立臺北大學犯罪學研究所碩士論文，新北市。

30.陳瑞金（2015），網路詐欺犯罪模式分析與偵查模式之研究， 宜蘭大學多媒體網路通訊數位學習碩士在職專班學位論文，宜蘭縣。

31.賀宇才（2017），建構高科技犯罪鑑識標準作業程序與案例，華梵大學資訊管理碩士論文，新北市。

32.張承瑞等（2010），科技犯罪偵查暨數位鑑識出國參訪報告書，行政院及所屬各機關出國報告。

33.陳子雄（2010），使用公開來源情資技術於社群網路身分解析與應用，臺北市：刑事雙月刊，頁 40。

34.林天福（2011），新興詐欺犯罪之研究-以通訊科技方式詐騙為中心，中央警察大學研究所碩士論文，桃園市。

35.黃茂穗（2014），從智慧型手機的興起論新世代網際網路通訊監察挑戰與政府因應作為，刑事科學 74 期，臺北市：內政部警政署刑事警察局。

36.王晴玲（2015），對以具加密功能之通訊軟體之通訊監察之理論與實務，出國報告。

37.王旭正（2016），科技犯罪安全之數位鑑識：證據力與行動智慧應用，臺北市：博碩文化股份出版。

38.張雅昕（2016），LINE即時通訊軟體鑑識之研究，中央警察大學資訊管理研究所碩士論文，桃園市。

39.蘇三榮（2012），網路時代通訊監察與個人資料保護之法制研究，國立交通大學科技法律研究所碩士論文，新竹市。

40.調查局（2014），業務報告，未發行。

41.傅美惠（2014），通訊保障及監察法之修法動向兼論通訊保障及監察法

修正施行後對偵查及查賄工作影響之探討，臺北市：2014全方位成功國際學術研討會論文集，頁199-214。

42.曲建仲（2015），你真的都搞懂了嗎？臺北市：數位通訊新世代科學月刊4月號，取自 http：//scimonth.blogspot.com/2014/09/blog-post_3.html。

43.顏春煌（2008），行動與無線通訊，第 3 版，臺北市：基峰資訊股份有限公司，頁 10-2-10-19。

44.賴柏洲（2016），光纖通信與網路技術，臺北市：全華圖書出版。

45.楊家驤（2015），通訊原理，臺北市：城邦出版集團，頁 118-119。

46.蔡志宏（2014），103 年度「我國 3G 頻譜屆期釋出規劃及 4G/5G 規範與發展研究 4G/5G 規範發展與應用推廣情形」研究報告，臺北市，頁 17-20。

47.陳志仁、張正武(2015)，103 年度「我國 3G 頻譜屆期釋出規劃及 4G/5G 規範與發展研究－我國未來頻譜政策規劃」研究報告，臺北市：臺灣野村總研諮詢顧問股份有限公司。

48. 維基百科系統（2019），科學研究法，取自 https：//zh.wikipedia.org/wiki/%E7%B3%BB%E7%BB%9F%E7%A7%91%E5%AD%A6。

49.智庫百科(2019)，什麼是APP，取自https：//wiki.mbalib.com/zh-tw/APP。

50.陳月香、江佩蓁、梁佳玲（2017），App 軟體使用分析之研究-以大學生為例，高雄市：黃埔學報。

51.創市際雙週刊（2016），第(七)、(八)、(十)期，臺北市：2016 年 12 月 30 日發行。

52.內政部警政署（2018)，107年犯罪數據統計。

53.陳子雄（2017），Tails與現場數位勘察的應用，臺北市：刑事雙月刊。

54.張善政（2016），105 年 2 月 25 日主持治安會報。

55 林萬青（2009），領導之研究，臺灣師範大學政治學研究所碩士論文，台北市。

56.BONI CHEN（2012），論文的研究方法有哪些?取自 http：//ntnumot.blogspot.com/2012/02/blog-post.html#!/2012/02/blog-post.html。

57.許芳雄（2009），兩岸特殊關係下跨境犯罪之研究－以新興詐欺集團為例研究，中華玄奘大學 98 學年度公共事務管理學系碩士在職專班，新北市。

二、英文部分

1.Bromby, R. (2006) .The wait goes on for AMI. The Australian, 11 July 2006.

2.Leibowitz, W. R. (1999). Technology transforms writing and the teaching of writing. Chronicle of Higher Education, 46(14), A67–A68. Lenneberg, E. H. (1967).

3.Rosoff, S., Pontell, H., & Tillman, R. (2002) .Profit Without Honor. White -Collarcrime and the Looting of America r, 2nd ed, Upper Ssaddle Rriver r,Nj：Prentice Hall.

4.Quayle, E & Taylor, M (2003) . 'Model of problematic Internet use in people with a sexual interest in children' CyberPsychology and Behavior, vol. 6, no. 1, pp.

5.Hinduja, S. (2004). Perceptions of Local and State Law Enforcement. Concerning the Role of Computer Crime Investigative Teams. Policing-an International Journal of Police Strategies & Management, 27(3), 341-357.

6.Broadhurst, R (2006).'Crime and Security in Asia: Diversity and Development', Asian Journal of Criminology, vol. 1, no. 1, pp. 1-7.

7.Finkelhor, D., Ormrod, R. K., & Turner, H. A. (2007). Poly-victimization:A neglected component in child victimization Child Abuse &Neglect, 31(1), 7-26.

8.Katos, V & Bednar, P (2008). 'A cyber-crime investigation framework', Computer Standards & Interfaces, vol. 30, no. 4, pp. 223-228.

9.Todd G. Shipley(2014). Art Bowker,Investigating Internet Crimes-An Introduction to Solving Crimes in Cyberspace,p346.

10.H.Zarrinkoub2014 Understanding LTE with MATLAB：From Mathematical Modeling to Simulation and Prototyping. John Wiley & Sons, 2014.

11.“ETSI - Cellular History,” ETSI. [Online]. Available：http：//www.etsi.org/technologies-clusters/technologies/past-work/cellular-history. [Accessed：09-Jun-2015].

12.“About 3GPP Home,” 3GPP. [Online]. Available：http：//www.3gpp.org/about-3gpp/about-3gpp. [Accessed：09-Jun-2015].

13.Specifications Groups Home,” 3GPP. [Online]. Available：http：//www.3gpp.org/specifications-groups/specifications-groups. [Accessed：10-Jun-2015].

14.H. Zarrinkoub, Understanding LTE with MATLAB：From Mathematical

Modeling to Simulation and Prototyping. John Wiley & Sons, 2014. “ETSI - Cellular History,” ETSI. [Online].
15. Stephen A. Saltzburg Daniel J. Capra, American Criminal Procedure：Adjudicative,West Academic Publishing.
16. Russell L. Weaver, Leslie W. Abramson, John M. Burkoff, CatherineHancock,Principles of criminal procedure,St.Paul,MN：West,c2012.
17. Wayne Lafave,CriminalProcedure, 5th,HornbookSeries, Student Edition, 2014 Pocket Part,West Academic.
18. Lafave, Wayne；Israel, Jerold；King, Nancy,LaFave, Israel, King and Kerr'sCriminalProcedure, 5th(HornbookSeries),West Academic.

三、網路文獻

1.警政署犯罪數據統計資料 https：
//www.npa.gov.tw/NPAGip/wSite/ct?xItem=87750&ctNode=12594&mp=1
2.群組互聯為犯罪聯繫 https：//www.google.com.tw/search-10804102300
3.IP 封包結構 http：
//www.tsnien.idv.tw/Internet_WebBook/chap5/5-2%20IP%20%E9%80%9A%E8%A8%8A%E5%8D%94%E5%AE%9A.html
4.LINELEGY(LINE event delivery gateway)https：
//engineering.linecorp.com/zh-hant/blog/line-safty-security/
5.HTTPS/SSL 加密網路封包鑑識設備 http：
//www.internet-recordor.com.tw/htts.html10.804102340
6.APP-MBA 智庫百科，什麼是 APP，取自 https：
//wiki.mbalib.com/zh-tw/APP