社群媒體鑑識
—以行動上網為例—

王朝煌／中央警察大學資管系教授

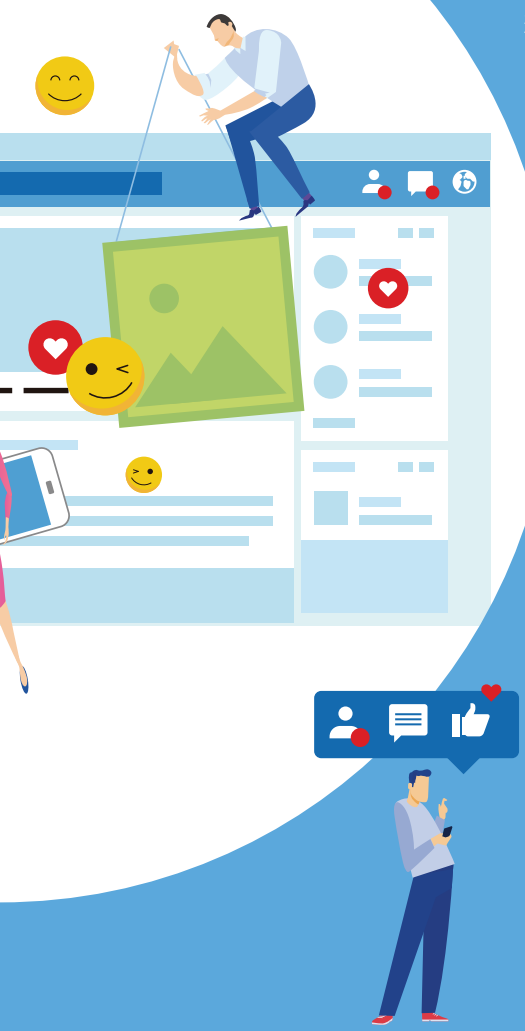
摘要

由於社群媒體資料的高動態性，以及社群媒體資料分散儲存於行動裝置、網站系統、雲端系統或資料中心等特質，導致傳統查扣主機及將硬碟作位元串流拷貝的取證方法已不敷使用，必須研擬新的蒐證技術。本文蒐集社群媒體鑑識相關文獻，以行動上網為例，整理社群媒體犯罪蒐證相關議題及其鑑識方法，包括社群媒體資料內容及證據價值、鑑識範圍與國內的法律規範，並介紹社群媒體快照鑑識方法。

關鍵詞 數位鑑識，社群媒體，社群媒體鑑識，社群媒體快照。

一、緒論

隨著社群媒體的廣為應用，人類行為涉及社群媒體的比例不斷增加。由於社群媒體具有快速與跨越國境的優勢，以及具隱密、匿名等特性，致使社群媒體逐漸成為有心人遂行犯罪的工具與管道。近年來社群媒體相關的犯罪案件呈現日漸增加的趨勢，社群媒體鑑識的重要性因而與日俱增。犯罪者利用社群媒體進行網路詐騙、恐嚇、及霸凌等行為屢見不鮮，甚至有利用社群媒體聚眾鬥毆，或散布假消息企圖影響大選等等，不一而足。蒐尋社群媒體的資料以佐證犯罪，乃成為執法機構追訴犯罪與釐清相關當事人責任的重要工作之一。



社群媒體犯罪依攻擊的來源，可分為內部攻擊及外部攻擊[7]。內部攻擊乃社群媒體使用者間的犯罪行為，例如網路霸凌、網路詐騙、網路身分竊盜、或散播不實消息等等。外部攻擊乃針對社群媒體平台業者網站系統的攻擊行為，例如運用分散式阻斷服務攻擊（Distributed Denial-of-Services, DDoS）癱瘓網站系統的正常運作，或駭入網站系統盜取使用者的註冊資料等等。社群媒體的犯罪依攻擊對象可分為：對社群媒體使用者的攻擊及對社群媒體平台業者網站系統的攻擊。社群媒體平台業者網站系統通常擁有強而有力的安全防禦措施，一般比較不會成為犯罪者的攻擊對象。然而由於社群媒體使用者的組成來源非常廣泛與多元，且使用者的資訊安全觀念與防護措施均較平台業者薄弱，比較容易成為犯罪者的攻擊對象。社群媒體犯罪攻擊對象的特質與犯罪類型歸納詳如表1。

表1. 社群媒體犯罪

攻擊對象 / 特質及攻擊來源	社群媒體使用者	社群媒體平台業者
特質	1.組織鬆散的網路鄉民 2.資訊安全觀念薄弱，一般僅具基本的帳號密碼防護措施	1.有組織的工商企業或團隊 2.資訊安全觀念較強，且具備強大的安全防禦措施
攻擊來源	1.社群內部 2.群組成員對其他成員的攻擊（如霸凌、詐騙、及竊用身份）	1.社群外部 2.有競爭關係的同業或有敵意或不滿意的網路鄉民的攻擊（如DDoS）

本文探討以社群媒體使用者為攻擊對象的社群媒體犯罪鑑識課題，並以行動上網為例說明社群媒體犯罪的鑑識方法。另外，本文也整理國內有關社群媒體蒐證的法律規範與實務見解，期能作為數位鑑識學術研究及鑑識實務之參考。本文組織如下：第二節探討社群媒體及其證據價值，第三節說明社群媒體鑑識範圍與規範，第四節介紹社群媒體的鑑識方法，第五節為結語。

二、社群媒體及其證據價值

1. 社群媒體

社群乃一群人基於共同興趣或目標而成立的組織，成員間透過共同活動來強化社群組織的凝聚力。根據維基百科[1]，社群媒體乃社群化媒體，能夠以多種不同形式呈現，包括文本、圖像、音樂和影片等。常見的Facebook、Line、Instagram、Plurk、Twitter、Google+、Snapchat、Dcard、LinkeIn、PTT及Weibo等等，乃以提供虛擬空間（或網路空間）給網路鄉民建立網路社群，以及提供社群成員互動管道服務的社群媒體平台業者。以台灣盛行的Line為例，網路鄉民在安裝Line APP軟體並完成註冊後，即成為社群媒體的使用者，可以成立群組及邀請好友組成社群。群組成員針對群組發表或轉傳訊息，群組成員藉由線上交換訊息產生更多的內容。群組的內容既面向群組，也來自群組。群組內部存在著頻繁的內容生產和訊息交換的活動，這種訊息交換方式為群組成員對群組成員，是“多對多”訊息交換型態。

近年來社群媒體如Facebook（臉書）、Twitter（推特）、Weibo（微博）、Line、及Whatsapp等等，如雨後春筍般地蓬勃發展。目前臉書全球約有25億的使用人口，推特及微博也各擁有約3億及4億個註冊用戶。以臉書為例，台灣註冊帳號數已接近2,000萬。根據台灣網路資訊中心2019年「台灣寬頻網路使用調查」報告顯示[2]：台灣地區家戶上網率達90.1%；個人上網率也高達88.8%。台灣社群媒體使用率高達89%，在亞洲地區排名第一。社群媒體市場概況為「Facebook」使用率為 98.9%，其次「Instagram」使用率為38.8%。台灣社群媒體市場的使用率詳如圖1所示。由於國內使用社群媒體及通訊軟體的人數逐漸增加，不法份子也開始利用這些管道來進行犯罪行為，主要犯罪類型包括：不法蒐集、利用他人個人資料，實施詐騙行為，實施性交易相關行為，以及發表妨害名譽言論等[3]。

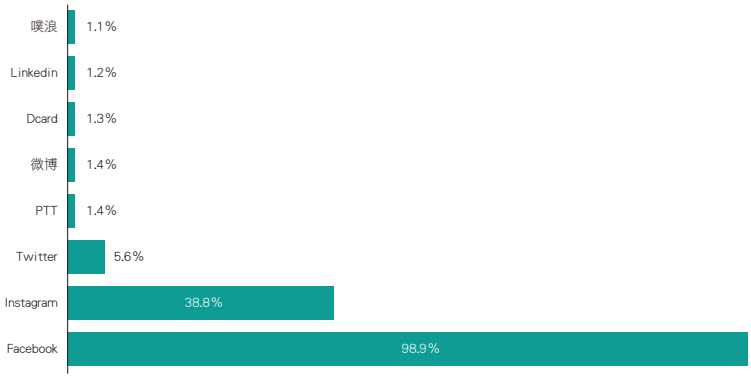


圖 1、台灣社群媒體市場使用率
（圖來源：台灣網路資訊中心）

2. 社群媒體的組成

社群媒體的組成，除了社群媒體使用者及社群媒體平台業者外，通常還包括提供資訊軟硬體基礎設施的雲端業者，如圖2所示。社群媒體平台業者，除了可以選擇購置軟硬體設備作為建置網站系統的基礎設施外，也可以選擇租用雲端業者的軟硬體設備作為建置網站系統的基礎。由於社群媒體的資料量非常龐大，通常一個使用者所需的儲存空間即可達10MB以上，有些使用者的儲存空間甚至超過100MB。為滿足眾多社群媒體使用者的儲存空間需求，社群媒體平台業者或雲端業者通常將資料以分散的方式儲存在眾多的電腦系統或資料中心。

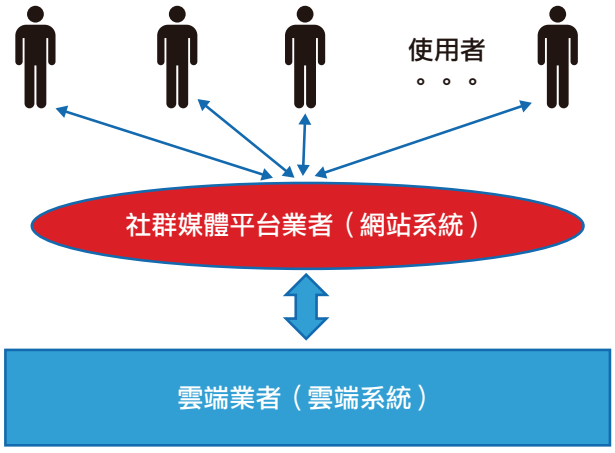


圖2、社群媒體架構示意圖

社群媒體資料分散的儲存方式，不但增加了社群媒體犯罪取證的複雜度，也使數位鑑識面臨新的挑戰。由於社群媒體的資料已不再僅儲存於少數的電腦系統硬碟，傳統查扣主機及將硬碟作位元串流拷貝的取證技術乃不敷使用。社群媒體的資料除了一部份儲存於搭載社群媒體APP的電腦系統或行動裝置外，使用者的註冊資料、活動內容、以及資料變動的歷史紀錄等等，一般儲存於社群媒體平台業者的網站系統。且網站系統通常以分散的方式將資料儲存在眾多的電腦系統或資料中心。因此，傳統查扣主機及將硬碟作位元串流拷貝（bit-stream copy）的取證方法，已不足以應付社群媒體犯罪的取證工作[6,7]。

3. 社群媒體的證據價值

社群媒體資料包括：使用者的基本資料、活動資料、網絡關係資料、貼文內容、及詮釋資料（metadata）等等[5]。使用者基本資料如姓名，生日，電子郵件信箱，居住城市等等。活動資料如使用者活動的相關資料，如上網時間、上網地點、及貼文（發文、推文、或貼文）的時間、地點等等。網絡關係資料：以Line為例，如隸屬群組，群組成員，我的最愛、及好友關係等等；以臉書為例，如朋友清單，共同好友，校友關係等等。貼文除發文內容外，還包括按讚、按倒讚、及上傳的圖像與影片等等。詮釋資料如網路活動的相關資訊：包括發文或上網的時間戳記（timestamp）、地點標註（location tag）、上網的設備（電腦、手機、或平板）、及所使用IP位址與網路等等。

社群媒體的證據價值包括：根據使用者的通訊可以探知一個人的心理狀態（計畫、故意、

或無知）；日常的線上活動紀錄可以推論一個人的在場或不在場證明；上傳的日常照片可以佐證一個人的生活花費型態，或推論其經濟狀況，以及推論其身體健康情形；上傳的日常照片也可以證明一個人的活動軌跡，及佐證與其互動的夥伴與關係；網路行為也可佐證一個人是否涉及網路霸凌、網路騷擾、或是網路詐騙；社群網站的註冊資料可以佐證一個人是否涉及假冒他人名義，或是盜用他人身分，此外註冊資料也可以用來檢查涉嫌者或證人的背景；貼文的時戳資料可以重建事件發生的先後次序，釐清涉嫌者究為原創或者單純轉傳行為[5]。隨著社群媒體的多元應用，社群媒體的犯罪型態也將漸趨多元化，社群媒體資料的證據種類與價值亦將呈現逐漸增加的趨勢。

三、社群媒體蒐證範圍與規範

1. 社群媒體證據蒐集範圍

社群媒體證據的蒐集範圍，除了螢幕畫面的截圖外，還需蒐集相關的輔助證據，才能提供足夠的資訊作為起訴或審判的依據[5]。由於數位證據易於更改的特性，增加了其證據力的不確定性，因此相關輔助證據的蒐集亦極為重要。例如除了螢幕畫面截圖的證據外，如有目擊證人（witness）的證詞，可增加截圖的證據力。另外，被告或嫌犯的註冊資料、上網設備及上網IP位址、及網站的日誌資料等等，亦可以作為間接證據，以確認被告或嫌犯的網路活動，或證明被告或嫌犯的帳號乃遭到盜用所致。此外，被告或嫌犯的貼文時戳，以及貼文的來源，可以作為推論被告或嫌犯為貼文的原創且另有圖謀，或僅為單純轉傳的散布行為，以釐清涉案人的責任。

2. 社群媒體證據蒐集規範

社群媒體證據，除了部分儲存於使用者（被害人、被告或嫌犯）的上網設備外，大部分儲存在社群媒體平台業者的網站系統。被告或嫌犯上網設備的證據蒐集，可依刑事訴訟法第122條第一項以及第133條有關搜索、扣押之相關規定蒐集。社群媒體平台業者網站系統的資料除可依刑事訴訟法第122條第二項、第133條及第135條等搜索、扣押相關規定蒐集外，亦可透過社群媒體平台業者網站系統的應用程式介面（Application Programming Interface, API）蒐集之[5,6,7]。

另外，社群媒體即時通訊的監察，以及使用者間私密留言的監察，也須依通訊保障及監察法的相關規定辦理。通訊保障及監察法第三條第一項規定，通訊的定義為：利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信，郵件及書信，言論及談話等；第二項規定保護的要件：需有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。據此，社群媒體的即時通訊受到通訊保障及監察法的保護，應無疑義。另外，社群媒體的留言紀錄，可分為公開的群組留言及私密留言兩部分。群組留言的對象為所有好友（或群組成員），本質屬公開性質，因不具隱私或秘密之合理期待的要件，不在通訊保障及監察法的保護範圍，應無疑義。使用者間私密留言所留下的紀錄，實務上認為本質乃已儲存在某寄件者或收件者電腦中之電子郵件，屬範圍、對象均已特定之「既存證據」，而不在通訊保障及監察法的保護之列[4]。因此社群媒體既存的群組或私密留言紀錄，可以依刑事訴訟法第122條、第133條及135條等搜索、扣押相關規定進行蒐證。但如預定在一特定的期間對使用者間的私密留言進行監察，則仍應依通訊保障及監察法的規定辦理。刑事訴訟法及通訊保障及監察法中有關社群媒體蒐證的規定詳如表2。

表2、社群媒體蒐證相關規範

法規與條目	條文內容
刑事訴訟法 第122條	對於被告或犯罪嫌疑人之身體、物件、電磁紀錄及住宅或其他處所，必要時得搜索之。 對於第三人之身體、物件、電磁紀錄及住宅或其他處所，以有相當理由可信為被告或犯罪嫌疑人或應扣押之物或電磁紀錄存在時為限，得搜索之。
刑事訴訟法 第133條	可為證據或得沒收之物，得扣押之。 為保全追徵，必要時得酌量扣押犯罪嫌疑人、被告或第三人之財產。 對於應扣押物之所有人、持有人或保管人，得命其提出或交付。 扣押不動產、船舶、航空器，得以通知主管機關為扣押登記之方法為之。 扣押債權得以發扣押命令禁止向債務人收取或為其他處分，並禁止向被告或第三人清償之方法為之。 依本法所為之扣押，具有禁止處分之效力，不妨礙民事假扣押、假處分及終局執行之查封、扣押。
刑事訴訟法 第135條	郵政或電信機關，或執行郵電事務之人員所持有或保管之郵件、電報，有左列情形之一者，得扣押之： 一、有相當理由可信其與本案有關係者。 二、為被告所發或寄交被告者。 但與辯護人往來之郵件、電報，以可認為犯罪證據或有湮滅、偽造、變造證據或勾串共犯或證人之虞，或被告已逃亡者為限。 為前項扣押者，應即通知郵件、電報之發送人或收受人。但於訴訟程序有妨害者，不在此限。
通訊保障 及監察法 第 3 條	本法所稱通訊如下： 一、利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信。 二、郵件及書信。 三、言論及談話。 前項所稱之通訊，以有事實足認受監察人對其通訊內容有隱私或秘密之合理期待者為限。

四、社群媒體鑑識方法

本文以行動裝置上網的社群媒體為例，說明社群媒體證據的蒐證方法。行動上網的社群媒體架構如圖3所示。如前所述，社群媒體資料除了部份儲存於搭載社群媒體APP的電腦或行動裝置外，社群媒體使用者的註冊資料、活動資料、以及資料變動的歷史紀錄等等，大部分儲存於社群媒體平台業者的網站系統。另外，搭載社群媒體APP的電腦或行動裝置，以及社群媒體平台業者的網站系統上的資料狀態，隨時都會因為使用者的訊息接收或傳遞而更動。另外如前所述，社群媒體平台業者網站系統的資料，極可能分散儲存於為數眾多的電腦系統或資料中心，使得傳統查扣主機及將硬碟作位元串流拷貝的取證方法，已不敷使用，必須研擬新的蒐證技術。

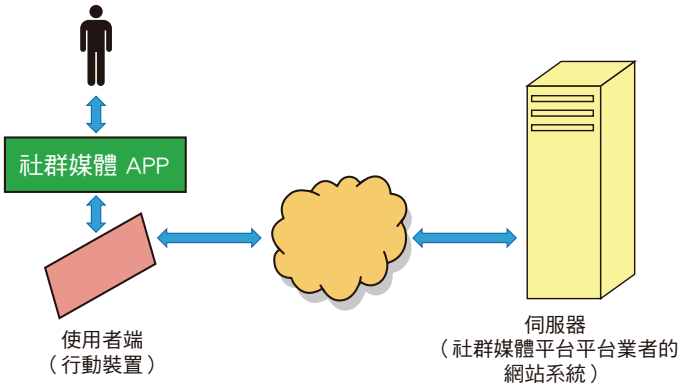


圖3、以行動裝置上網的社群媒體架構

由於數位證據易於更改的特性，僅僅提供使用者端行動裝置的螢幕畫面相片或截圖，一般已不足以讓法官採信作為審判的依據，還需蒐集相關的輔助證據，進一步佐證被告或嫌犯的網路活動，才能增加證據的證明力。由於大部分的輔助證據，例如被告或嫌犯的註冊資料、上網設備及上網IP位址、及網站的日誌資料，儲存於社群媒體平台業者的網站系統。因此除了蒐集使用者端行動裝置上的資料之外，社群媒體平台業者網站系統上證據的蒐集，也是重要的一環。

被告或嫌犯行動裝置上的證據蒐集，如前述，可依刑事訴訟法第122條第一項及第133條有關搜索、扣押之相關規定，可以查扣主機及將硬碟作位元串流拷貝加以蒐集，在此不再贅述。社群媒體平台業者網站系統證據的蒐集，如果業者在台灣設置有分公司及聯絡窗口，可依刑事訴訟法第122條第二項、第133條及135條等搜索、扣押相關規定，備妥令狀函請社群媒體平台業者提供被告或嫌犯網站的相關資料。如果業者在台灣沒有設置分公司及聯絡窗口，一般只能透過社群媒體平台業者網站系統的應用程式介面（API），以社群媒體快照（social snapshots）方式加以蒐集[6,7]。

由於社群媒體的資料具高動態性，隨時都會因為使用者的訊息接收或傳遞而跟著更動，因此一般只能採集某一時間點的網站資料內容狀態，稱之為社群媒體快照（social snapshot）[6]。換言之，社群媒體快照乃在沒有加工或編輯的情境下，社群媒體網站在一時間點的內容，包括

文本、圖像、音樂和影片等等。社群媒體快照的蒐證方法，乃撰寫蒐證程式，透過呼叫社群媒體平台業者網站系統的應用程式介面，下載社群媒體網站的內容。此外，蒐證程式在呼叫應用程式介面時必須提供使用者的認證資料（如帳號密碼或權杖），以及欲取得的網站資料參數。使用者網站的認證資料，可以徵詢使用者的同意提供，或從查扣的被告或嫌犯的行動裝置中查找。知名的鑑識廠商Cellebrite最近發表的UFED Cloud Analyzer，即透過呼叫社群媒體平台業者網站系統的應用程式介面的蒐證工具。UFED Cloud Analyzer可利用蒐集到的驗證碼或帳號密碼登入Gmail、Google drive、Facebook、Twitter、Dropbox、及Kik等網站，並下載相關訊息內容及其歷程，文件及通聯紀錄[5]。綜合而言，目前市面上的社群媒體鑑識工具仍然不多，仍有待進一步研發。

五、結語

由於數位證據易於更改的特性，社群媒體證據的蒐集範圍，除了螢幕畫面的截圖外，還需蒐集相關的輔助證據，才能提供足夠的資訊作為起訴或審判的依據。以行動上網為例，社群媒體資料分別儲存於搭載社群媒體APP的電腦或行動裝置，以及社群媒體平台業者的網站系統。電腦或行動裝置及網站系統的社群媒體資料均須加以蒐證，以提供足夠的佐證資訊作為起訴或審判的依據。另外，由於社群媒體資料的高動態性以及社群媒體資料的分散儲存方式，只能採集某一時間點的社群媒體快照作為證據。本文探討行動裝置蒐證及社群媒體網站系統蒐證相關的法律規範與實務見解，並介紹社群媒體快照與其蒐證方法。除了期盼能提供數位鑑識學術界及鑑識實務界參考外，也企盼能拋磚引玉，激發數位鑑識領域先進，更深入研究社群媒體快照蒐證技術。FACT

中英文參考文獻

1.MBA智庫百科，https://wiki.mbalib.com/zh-tw/社群媒體。（參考日期：2020.02.20）

2.台灣網路資訊中心，2019，台灣網路報告，https://report.twnic.tw/2019/。（參考日期：2020.04.01）

3.全國法規資料庫，社群網站犯罪行為，https://law.moj.gov.tw/SmartSearch/Theme.aspx?T=40。（參考日期：2020.04.01）

4.法務部，2017，法檢字第 10604533580 號函，https://mojlaw.moj.gov.tw/LawContentExShow.aspx?media=print&id=B%2C20171002%2C003&type=Q。（參考日期：2020.04.01）

5.Humaira Arshad, Aman Jantan, Esther Omolara, 2019, "Evidence collection and forensics on social networks: Research challenges and directions," Digital Investigation, vol. 28, pp. 126-138.

6.Markus Huber, Martin Mulazzani, Manuel Leithner, Sebastian Schrittwieser, Gilbert Wondracek, Edgar Weippl, 2011, "Social Snapshots: Digital Forensics for Online Social Networks," Proceedings of the Annual Computer Security Applications Conference.

7.Urjashee Shaw, Dolly Das, Smriti Priya Medhi, 2016, "Social Network Forensics: Survey and Challenges," International Journal of Computer Science and Information Security, pp. 310-316.