社群網路犯罪鑑識與未來挑戰

張明桑 博士 / 中央警察大學資訊管理學系 教授
張智彥 碩士 / 台灣大學電信工程學研究所

摘要

近年來科技急速地發展，人們利用電腦網路溝通愈趨頻繁，尤其在社群網路興起後，人們彼此之間的聯繫方式起了極大的變化，造成許多犯罪轉移至社群網站。本文探討網路鑑識偵查模式，並以社群網路為例子提出說明。網路鑑識在社群網路上有關特性，如資料量大、各網站伺服器所顯示時間不一致、朋友關係清單等，都是社群網路不同一般網路的附加特性。本文除了探討社群網路鑑識偵查模式外，亦介紹一些網路鑑識工具，並提出網路鑑識的未來挑戰，以提供對網路鑑識有興趣的人員參考。

關鍵詞 網路鑑識、社群網路、數位鑑識、網路犯罪、網路封包。

一、前言

近年來，社群網路的蓬勃發展，已經改變了許多人們彼此之間的互動方式，現今大多數的網路使用者藉由社群網路彼此聯繫。著名的社群網站如Facebook、YouTube、Twitter、Instagram、LinkedIn等等，每一個社群網站均可讓使用者高度個人化地去使用，同時亦可讓使用者在網站內部互相通訊。

依據We Are Social和Hootsuite兩大網站近期共同發布「2017全球網路使用調查報告」，報告指出，2017年網路的使用人口數已經超過全球人口數的一半。並隨著社群網站貼文的成長，全球的網路使用人口中近乎28億人，每月至少使用一次社群網路[1]。在各種不同社群網路，我們不難發現除了Facebook是較無國界限制的平台外，其他社群平台如QZone、LINE、VKontakte大多在特定國家才有較多的用戶，普及度仍遠遠不及Facebook[2]。

社群網路定義為以網路為基礎所提供之服務，在這些網站內，每個人都可使用已經界定好的系統範本，去建立一個公開或半公開的個人檔案，並列出所有分享同一關係的使用者，可以檢視這些或由其他人建立的朋友（關係）清單；每個不同社群網站針對人與人之間關係所定義的本質與術語都會有所不同[3]。

由於社群網路蓬勃發展，隨之而來的犯罪，包括盜用個資、違法交易、網路追蹤、網路詐騙等。這類的犯罪方式越變越複雜，因為犯罪者開始會使用相關的技巧隱匿地實行網路犯罪，避免警方的調查。在虛擬網路世界之中，現今的人們已習慣透過電腦網路進行通訊與交易，許多詐騙者便利用此機會去施行網路詐欺，或利用社群網站系統漏洞直接盜取個人資料等犯罪行為。社群網路發展規模與日俱增，如何於社群網路中找出相關罪證，便成為具有挑戰性的議題。

對於數位鑑識偵查人員而言，發展出一個系統化的偵查模式，去偵查並解決社群網站上的網路犯罪案件，有其必要與價值，且必須確認蒐集的數位證據都可用於法庭中，此證據對於系統稽核人員、IT管理人員、網路安全維護人員都是可信賴與可用的。

本文主要以社群網路為例子，探討網路鑑識偵查模式。並以社群網路上有關的特性，如資料量大、各網站伺服器所顯示時間不一致、朋友關係清單等，說明網路鑑識流程。本文除了探討社群網路鑑識偵查模式外，亦介紹一些網路鑑識工具，並提出網路鑑識的一些未來挑戰，期能透過闡述社群網路鑑識相關的概念與網路鑑識未來挑戰，提

供對此議題有興趣的人士，繼續研究的參考。

二、社群網路犯罪之特性

社群網站可讓使用者在創造個人檔案時，公開正確的細節，包括完整的姓名、照片、出生日期、現居地、電話號碼、手機號碼、住址、辦公室地址，這些個人檔案的資料可協助找到朋友，將使用者連結起來。使用者也可將他們的個人資料設為隱私，但這樣會影響到他們對其他人的連結，無法順利找到朋友們，然而，他們亦可將個人資料設為公開，則任何人都可看到他們的個人資料，並可送訊息給他們。

所有這些個人的資訊都可被犯罪者用以辨別出某一特定使用者。 Athanasopolous et al.[4] 指出，社群網路包含有一些固有的特性，這讓社群網路成為被對手利用（開發）的理想選擇。一些較值得注意的特性如：

（1）一個極為龐大且高度分散的用戶群。

（2）一群享有相同社會利益的使用者。

（3）社群網站為公開平台，可散佈假資源或假的應用程式，誘騙使用者去安裝。

顯而易見地，以上所列之特性皆使得社群網路易於被利用，成為網路犯罪的溫床。

一般的網路鑑識大多致力於截取網路流量或日誌檔，然而，面對社群網路或是雲端服務鑑識時，需要一個新的方式截取有用的資料，目前許多網路鑑識方式仍以客製化的網頁抓取為主，這樣直接的方式可能會產生下列問題：

（1）龐大的網路流量：若藉由傳統的網頁抓取程式，截取到社群網站上個人資料的網頁，十分地耗時且所需花費之成本極高，更會導致在單一網路上會有數量龐大之連線，有一些社群網站若偵測到單一IP位址所發出之連線數過高，會阻檔該IP位址之用戶連線，導致連線中斷無法獲取更多的資料。

（2）多餘、隱藏的資料：這些在社群網站上會產生的多媒體資訊，如產生時戳或是其他的辨別標籤，通常有助於辦案人員重建現場，網頁抓取的方式，除網頁本身之外，無法抓到網頁中的多媒體資料。

（3）可維護性：網站的結構與佈置，會隨著時間經過迅速地改變，除此之外，動態的或需要編譯的（如JavaScript）內容，通常要讓客製化網頁抓取程式不斷地維護、更新。

社群網路的鑑識在許多案例中，皆依賴一定限制的資料來源，無法取得伺服器所有紀錄的資料，若欲於伺服器取得使用者的資料，需要提供該服務之公司的配合。

社群網路犯罪與一般網路犯罪之間有若干性質重疊部分，但仍可以分析出下列幾種特性。

（1）隱匿性

使用者可以在社群網路分享自己或其他網友的創作，但於申請帳號時，不一定要使用個人真實資料，使用者可以虛報姓名、

年齡、 性別，甚至盜用他人照片作為大頭貼，以一個虛假的分身隱藏現實的身分，故社群網路擁有網際網路的匿名性質。

（2）散佈性

社群網路本質是分享的精神，所以也加劇犯罪行為散播的結果。人們在分享資訊時，只要按個按鍵，就能將之分享傳播，又因網路普及，使散佈的力量更為強大，一個有趣的資訊，經常能獲得幾萬個「讚」或轉載[4]。

（3）證據易遭銷毀

電磁紀錄可以輕易刪除或變更，具有相當大的變動性。而社群網站資料，更只要使用者一個按鍵就能刪除，雖然社群網站管理者通常有備份使用歷程，但不一定能完整重現原始情況。

（4）犯罪行為跨區域性

社群網路架構於全球性的資訊網路上，產生網路無國界的特性，聯繫了世界各國使用者的關係，並輕易地跨越地域及國家進行。因此，衍生出司法管轄權的問題，同一行為在不同國家，可能有不同的規範或刑責，各國管轄規範為屬人主義或屬地主義，亦各有不同。在社群網路上犯罪，該歸何地管轄，且刑責規範應適合哪個國家規定，此種情形即是跨區域性所造成的問題[5]。

（5）犯罪結果廣泛性

社群網路輕易傳遞資訊，它提供使用者十分便利的操作方式，但也因此容易煽動犯罪或集結群眾。埃及的茉莉花革命、臺灣的太陽花學運，都可以了解社群網路影響甚鉅的力量。

（6）偵查不易

社群網路犯罪基於電腦網路之應用，電磁紀錄易遭刪除、修改，證據較易銷毀。且社群網站大都架設於國外，偵查人員必須大費周章透過管道，向外國社群網站公司申請調閱使用者資料，國外的公司不見得配合，造成偵查過程曠日廢時。另一方面，社群網路犯罪多為資訊專業領域，並非每位偵查人員均具備有足夠的專業知識、能力來偵辦此類案件。

（7）對犯罪行為無知

隨著電腦和網路的普及，每個人使用網路更為頻繁，也更依賴電腦、網路。社群網路使用者有時因與網友爭鬥，於線上留言污辱對方，其他網友只是對別人發佈之污辱留言按「讚」或轉貼，便讓自己觸犯刑法誹謗罪、公然侮辱罪[6]。有些人則是在社群網路上發佈援交訊息或分享色情照片、影片，也在不經意之間觸犯兒童及性交易防制條例。社群網路犯罪者對自己犯罪行為的無知，總認為自己的行為無傷大雅，但卻常讓自己身陷泥淖[7,8]。

三、社群網路偵查模式

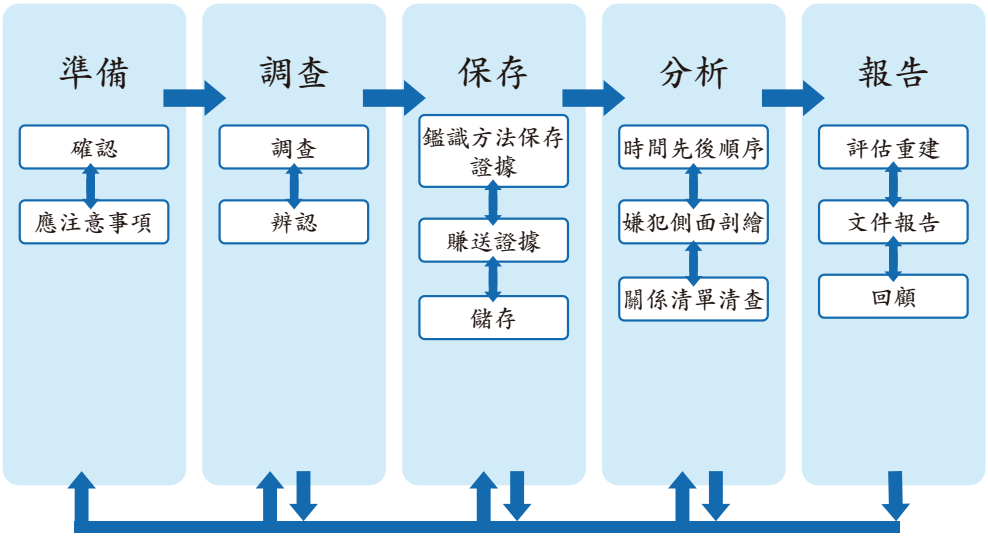
社群網路的偵查缺乏標準及相關理論性的框架，使用一個特製的方法或工具以萃取數位證據，會限制了證據的可靠度與可信度[9]。由一些相關數位鑑識的文獻可歸納出數位鑑識偵查模型的共同特徵[10,11,12,13]，同時亦可歸納出社群網路偵查模型附加的功能如下：

（1）從社群網路的使用帳號裡可獲得各式各樣的資訊，對於調查是十分地有幫助，此類資料包括：使用者個人檔案， 其中有全名、住家地址、電話號碼、位置、學歷以及工作，使用者與其他使用者的關係清單、共同參與的社團。

（2）調查在於上線的模式下啟動，大部分的資料都儲存在社群網路供應商的資料庫之中。

（3）資訊與證據的搜尋是一個循環的過程，偵查人員會先搜尋特定使用者的個人檔案，然後再找特定使用者的朋友的個人檔案，並找朋友的朋友其個人檔案，如此反覆查找，調查的深度視被調查的事件而定。

為了涵蓋這些附加的特性，本文提出社群網路的偵查模型，包含了五個過程，分別為準備、調查、保存、分析、報告，如圖一所示。



圖一、社群網路偵查的數位鑑識模型

社群網路之偵查模型詳細敘述如下。

1. 準備

在事件發生之後，觸發整個模型的執行，調查便從初始過程開始，在這個過程要準備、驗證、衡量並制定要執行的策略。一般由傳統數位鑑識調查所使用的方法，包含驗證事件，在訂定出適當的偵查策略之前先評估整個狀況，然後隨之而來的是 確認偵查上所需的所有需求，如人力資源、 特別的器材、法源依據等，在社群網路的數位鑑識調查中，調查人員要決定在社群網路之中要找到什麼，調查活動可能包括計劃要先專注哪一個個人檔案，或是在個人檔案之中要找到哪一種資訊，可能需要找到毒品交易資訊、清查朋友清單以找到相關人員，或是找出帳號盜用記錄，這一切都依據要被調查的事件而定。

2. 調查

調查過程是由關於在社群網路調查中的數種活動所組成，本過程的目標，即假設並辨別出真正與潛在的數位證據與在調查過程中所需之資訊。在這個過程中，下列事項都必須在步驟中被執行：

（1） 伺服器上的資料量極大，社群網站用戶眾多，資料流動極為迅速，應先確認事件主要發生之時間點，再辨別時間點前後所須取用資料的時間區間。

（2） 線上搜尋使用者或是目標的個人檔案，在目標間的連結，可能會成為被調查事件中有貢獻的資訊，以及所有從個人檔案得到的潛在證據與資訊。

（3） 若是為了從一個以上的個人檔案收集資訊與證據，必要時應重複這些步驟。

3. 保存

保存過程即調查過程後關於保存證據的步驟，以及所須記錄的文件，在社群網路上所調查到資料的時序，在電腦中萃取出的資料，本過程的目的是要收集並儲存證據，以利後續偵查及起訴。在這個過程中，下列事項都必須在步驟中被執行：

（1） 任何潛在的證據都應該以鑑識的手法收集，確保證據在法庭上或是任何訴訟相關的過程皆是可被信賴且可被呈現。

（2） 一但潛在的證據已被找到，一定要將其儲存， 並考慮證據無法被直覺瞭解，而將該證據轉換以利分析。

（3） 在保存或轉送證據時，注意到證據動態，很可能會影響到證據，將證據動態減到最低，盡可能保存其原始的狀況。

4. 分析

分析的過程是整個鑑識調查中很重要的一部分，在此過程，偵查人員需要個化、類化出所被找到的證據與資訊，與所調查之事件相關，傳統調查活動在於分析之過程通常會包括證據檢查，並分析證據，以決定其價值與對案情的影響。在社群網路數位鑑識偵查模型分析過程中，將進行的步驟如下：

（1） 將所有證據排出時間順序，以釐清所有事件發生的先後順序。

（2） 若是於不同的網站中找到證據，應先辨別該社群網站所顯示的時間軸是參照

網站伺服器之時間，或是參照使用者所使用之電腦上的時間，例如Facebook上之時間軸即參照其網站伺服器的Unix時間。可自行上該社群網站，並藉由發出評論上所顯示的時間，得知該社群網站時間參照方式，再將所得證據依偵查人員所選定的時間軸平移事件到該時間軸，確立同一時間軸上的事件發生先後順序。

（3）向社群網站所屬之公司調閱使用者登入、登出 IP記錄與流程，查明登入使用者帳號所用IP，清查相關資料。

（4）藉由記錄任何從其他個人檔案所找到的證據， 對嫌犯的資訊做側面的剖繪，推測嫌犯上網時間、喜歡的社團傾向、被標示之照片顯示常出沒的地區。

（5）在某些事件之中，為了要獲得有建設性的證據，可透過拼湊嫌犯的個人檔案與其他人的關係。

（6）清查嫌犯的朋友清單，除了可直接透過該清單找出直接有聯絡的關係人之外，可以將其朋友的關係清單與嫌犯的關係清單作比對，找出隱性關係，可能兩人在表面上完全沒聯絡也沒有關係連結，但是實際上的連繫是透過彼此的朋友相互傳遞訊息。

（7）分析的關係清單夠多時，可以借用兩個人之間的互動多寡，作為關係比重，可能找到多個關係所連結成的集團，第一種是中心的角色彼此之間的連結十分密切，可能集團的核心人物有兩個以上，但在中心角色旁所形成的集團十分地稀疏；第二種是中心角色只有一個，所有人直接跟核心人物連繫；第三種是關係清單中的角色，因所在地區不同或是在集團中所擔任的職務不同（如販賣者、車手、洗錢），各自形成一個子集團，再連到上游的連繫者，而形成一個網路。借用此方式，可找出集團的運作模式，進而找出其他嫌犯。

5. 報告

社群網路的數位鑑識偵查報告過程，在這個過程裡，偵查人員在分析過程後，試著重建犯罪當時之情況，回顧所有過程有無遺漏錯誤，並將關鍵的證據列入文件和報告中展現，在訴訟中，偵查人員藉由展現可靠的、可信賴的證據與資訊，確保目標已達成。

四、 網路鑑識工具

網路鑑識過程於蒐集各種數位證據時，在每個不同的蒐證階段應該使用何類型工具都會有所不同，本節將依蒐集記錄檔證據、網路封包及流量、阻斷攻擊等列出不同鑑識工具並概略說明相關工具的功能以提供鑑識之參考[14]。若想對更多的鑑識工具，更進一步瞭解與應用，可參考文獻[14]。以下介紹幾種不同鑑識工具。

1. 記錄檔證據蒐集工具：

（1）Syslog-ng：是一種彈性且可擴展的審計處理（audit-processing）工具， 它提供了一個集中且安全性的網路設備的存儲日誌。

（2）Socklog：是一個小而安全的工具，可替代syslogd， 它可在Linux上運行。

（3）Kiwi Syslog Daemon：是Windows的免費軟體，它接收來自路由器、交換機、UNIX主機和任何其他啟用了系統日誌的設備的Syslog信息。

（4）Microsoft Log Parser：是一款功能強大的命令行工具，提供SQL界面對不同日誌文件格式，快速分析日誌檔。

（5）Firewall Analyzer：是一種基於Web的防火牆監控和日誌分析工具，用於收集，分析和報告有關企業級防火牆，代理服務器和RADIUS服務器的信息。

2. 網路封包及流量證據蒐集工具：

（1）Tcpdump：是一個執行在命令列下的嗅探工具，它允許用戶攔截和顯示傳送或收到通過網路連線到該電腦的TCP/IP和其他封包。tcpdump 適用於大多數的類Unix系統，作業系統：包括Linux、Solaris、BSD、Mac OS X、HP-UX和AIX 等等。在這些系統中，tcpdump 需要使用libpcap這個捕捉資料的函式庫，其在Windows下的版本稱為WinDump，它需要WinPcap驅動，相當於在Linux平台下的libpcap。

（2）NetIntercept：是一個網絡分析工具， NetIntercept使用在以太網路卡設置在混雜的模式（promiscuous mode）以收集LAN流量。

（3）Wireshark：是一個免費開源的網路封包分析軟體，可用來檢測網路問題，資訊安全相關問題及學習網路協定的相關知識。

（4）SoftPerfect Network Protocol Analyzer：用來偵測、維護、分析和監控區域網路和網際網路連接的流量，它蒐集通過的網路封包，分析並以易於閱讀的形式表示。

（5）Iris Network Traffic Analyzer：提供網絡流量分析和報告功能，該工具可蒐集網絡流量，並且可以自動將其重新組合到其本機格式（native format），從而更容易地分析跨網絡的數據。 調查員可以讀取正確發送的電子郵件的實際文本，或者重建用戶訪問過的HTML頁面。

3. 阻斷攻擊證據蒐集工具：

（1）Nmap：可以檢測目標主機是否上線及通訊埠開放情況，偵測執行的服務類型及版本資訊，偵測作業系統與裝置類型等資訊。

（2）DoSHTTP：是Windows的HTTP Flood DoS測試工具，包括URL驗證，HTTP重定向，端口指定，性能監控和增強報告。

（3）IPHost Network Monitor：允許郵件、資料庫和其他伺服器的可用性和性能監控。

（4）Admin’s Server Monitor：是監視經由網路儲存到伺服器硬碟的封包流量工具，它即時收集範圍的數據是從十秒開始到一整個月。

（5）Tail4Win：是UNIX tail -f命令的Windows版本，它是一個即時日誌監視器和查看器。

網路鑑識工具是依OSI （Open System

Interconnection） 通訊協定的各個層次的規範去設計的，以上僅列出部份軟體工具供參考，讀者若對網路鑑識工具想要更進一步的瞭解及應用，可參考相關的文獻與書籍。

五、 網路鑑識的挑戰

社群網站廣泛地提供了各式各樣的功能，且社群網路亦擁有一些特性如本文第二節所述。社群網路可視為網路所有應用的分支，因此，社群網路犯罪鑑識屬於網路犯罪鑑識的一環，社群網路犯罪鑑識遭遇的問題，亦涵蓋於網路犯罪鑑識之挑戰的一部分。本節將不侷限於社群網路犯罪鑑識可能遭遇的問題，而以網路鑑識技術層面，全面來探討網路鑑識可能遭遇的挑戰。

在網際網路中，不同類型的網路鑑識之挑戰如圖二所示[15]。我們將從技術面來探討網路鑑識的挑戰，下面幾點為網路鑑識可能遭遇的問題：（1）高速資料傳輸 （2）網路設備上的資料儲存能力 （3）資料完整性 （4）資料隱私 （5）訪問IP地址 （6）資料蒐集位置 （7）智能網絡鑑識工具。

圖二、網路鑑識的挑戰

以下說明這些網路鑑識可能遭遇的問題與挑戰：

1. 高速資料傳輸

蒐集和保存高速率的網路流量以供網路鑑識相對的困難。數量龐大的封包通過數千個互聯網路設備，這些互聯網路設備作為網路鑑識的證據蒐集及分析有一定的困難。這些網路設備需要記錄所有高速網路封包而不會遺失任何封包，這是一項具有挑戰性和耗時的任務。大多數公司通過連接多個分散式基礎架構來擴展和增強其網路結構，這些連接設備具有高速率，即10 GB的數據或以上。因此，網路流量無法被安全設備完全捕獲，這導致網路數據流量的日誌不完整。這些不完整的記錄使得重建可疑攻擊更加困難，從而識別來源入侵者變得困難。為了克服高速封包傳輸相關的網路鑑識問題，有幾種解決方案：（1）部署專門的資料蒐集設備，以蒐集高速網路流量並在FPGA （Field-Programmable Gate Array）可程式化處理元件中分析封包，以期過濾特定封包，並執行快速反應的即時分析。（2）透過部署在用戶端的軟體蒐集高速網路流量，它有助於主動和被動網路監控。（3）分散式封包蒐集技術用於捕獲在不同的網路節點之間高速網路流量，並降低記憶體和CPU的成本。

2. 網絡設備上的資料儲存

蒐集和分析網路大量資料，並從中提取證據，這樣的作為使網路鑑識的情況變得複雜化。例如，蒐集的資料需要存儲在大容量的儲存設備上，而網路互連設備的儲存容量有限，因此，必須要減少儲存網路上資料

量的問題。為了克服儲存容量相關的問題，有幾種解決方案：（1）高速並行處理分析封包，以減少駐留在儲存設備的時間 （2）應用單線程（thread）和多線程封包處理方式，並在即時情況下搜索特定封包以降低了儲存問題。

然而，網路蒐集的資料是由路由器、入侵偵測系統、防火牆、伺服器、主機等設備蒐集網路封包。這些設備都必須包含足夠的存儲空間來儲存高速率進入網路的封包。在這種情況下，設備包含的緩衝區大小，可能無法適應這麼大量的網路封包，特別是在負載較重的網路。因此，各個設備之存儲空間用於網路鑑識仍是一大挑戰。

3. 資料完整性

資料完整性在網路鑑識的過程中至關重要。完整性是保持資料準確、完整和一致性的能力，要證明網路上捕獲的資料完整性是網路鑑識的關鍵且具有挑戰性的任務。網路蒐集數據的範圍、大小和速度，讓保持資料的完整性成為挑戰。資料完整性受軟硬體錯誤，惡意攻擊，系統故障及行動設備不斷移動的影響。資料完整性是網路數據本身的揮發性和動態性質，綿延不斷的封包以高速率無時無刻的傳輸，它會因關閉會議（close session）而丟棄封包，這會增加蒐集資料完整性的複雜度，特別是包含在數千個鏈接的分散式網路，這是極具有挑戰性的議題。

4. 資料隱私

資料隱私是網路鑑識過程中的一個重要因素。蒐集企業網路中的資料可能會違反公司隱私政策，因此，企業或機構不願允許網路鑑識人員執行蒐集重要資料之行為。這是因為在企業網路中蒐集的資料可能包含其他重要的文件，例如財務記錄和員工記錄。因此，企業或機構傾向於不允許任何第三方調查員蒐集其網路資料進行調查。此外，蒐集網路資料可能進一步延遲網路並造成的不同法律問題，包括用戶資料的隱私和機密性。蒐集的文件可以包含用戶密碼，電子郵件內容，銀行記錄及其他各種個人記錄。因此，鑑識人員需要足夠的網路鑑識技術來監控和收集網路流量，而不會對用戶造成任何違規隱私和組織政策。

5. 訪問IP地址

查出入侵者的IP地址是網路鑑識中的重要一環，辨識攻擊來源的IP地址有助於阻止入侵者的攻擊。入侵者採用不同的方法來隱藏他的原始來源IP地址，此方法一般是用於DDoS攻擊，以阻斷網路系統提供的服務。假冒的IP地址使得鑑識人員在確定原始來源IP地址變得複雜，特別是在大型分散式網路環境中。 此外，一些入侵者利用多個來源IP地址，以增加網路取證人員辨識虛假的IP地址的困難度，同時產生更多的惡意封包導致系統過載，特別是在DDoS攻擊中。因此，識別正確的來源IP地址，來確定攻擊的來源是一個挑戰。另外，大多數系統在網路以動態方式分配IP地址，因此它可能在攻擊時具有其他IP地址，而不是目前的IP地址，這增加了驗證正確的系統的正確IP地址的複雜性。

6. 資料蒐集位置

網路的分散性和虛擬化特性，使得如何從適當的節點取得網路證據複雜化。網路以高速鏈路連接數千個節點，每秒傳輸數億萬個封包，要確定網路的適當節點蒐集資料分析封包，是網路鑑識的根本挑戰。此外，許多網路設備用於收集網路鑑識的資料，包括路由器、入侵偵測系統、防火牆、網路鑑識分析工具、協議分析器、封包嗅探器等，如何選定在正確的節點安裝適當的工具，收集來自網路的資料，進行調查和重建攻擊路線極具有挑戰性。確定正確的資料蒐集位置，使用正確的工具，並在正確的時間收集適當的證據，是非常重要的且是網路鑑識的一項挑戰。

7. 智慧網路鑑識工具

目前的網路鑑識分析工具需要蒐集完整的封包。這樣的作法衍生出存儲大量數據及時間延遲的問題。一個智慧網路鑑識工具應根據調查情況，蒐集選擇性的網路流量。例如，蒐集感興趣的特定封包，並進一步分析和視覺化數據。這將減少封包儲存，計算資源的利用，頻寬利用率，時間延遲等鑑識問題。

六、結論

本文說明社群網路鑑識的偵查模式，以及網路鑑識工具及未來之挑戰。社群網路的使用人口數已經超過全球網路的使用人口數的一半，亦即全球每月至少使用一次社群網路的人口近乎28億人，有鑑於於社群網路蓬勃發展，隨之而來的犯罪，包括盜用個資、違法交易、網路追蹤、網路詐騙等，這類的犯罪方式也越趨複雜，因而社群網路鑑識的可靠性也越趨重要。

現今社會正邁入一個以人工智慧主導的數位時代，新的數位科技如機器人、物聯網、行動網路和雲端運算等等不斷地推陳出新。此外我們也正面臨網路犯罪的快速增長，各種威脅及詐騙也不斷地擴散及潛藏於雲端和社群媒體中。網路鑑識需採用新的智慧工具、硬體和軟體、以及新的方法和程序來因應網路鑑識的需求與挑戰。雖然網路鑑識工具和科技，在數位偵查扮演關鍵的角色，然而除了具備智慧的工具和技術外，也需要訓練成熟的技術團隊，才能有效地進行網路鑑識工作。因而，充實鑑識科學教育與訓練也是極其重要的一環。FACT

參考文獻

1.Digital in 2017 Global Overview report from We Are Social and Hootsuite, 2017. https://wearesocial.com/special-reports/digital-in-2017-global-overview 。

2.World map of social networks, 2018. http://vincos.it/world-map-of-social-networks/ 。

3.D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," Journal of Computer-Mediated Communication, vol. 13, pp. 210-230, 2008.

4.E. Athanasopoulos, A. Makridakis, S. Antonatos, D. Antoniades, S. Ioannidis, K. Anagnostakis, and E. Markatos, "Antisocial Networks: Turning a Social Network into a Botnet," in Information Security, 2008, pp. 146-160.

5.鄭嘉逸，「網際網路管轄權之擴張與緊縮」， 經社法制論叢，民國98年01月，第127~159頁。

6.蘇慧婕，淺論社群網路時代中的言論自由爭 議：以臉書「按讚」為例，臺灣法學雜誌 ， 民國101年12月15日，第28~37頁。

7.張謹名，「科技犯罪與防制-電腦與網路犯罪初探」，Field Study in Criminal Justice Institute，2007。

8.聯晟法網，網路犯罪的特性。
http://www.rclaw.com.tw/postList-0-686-p-1-t-%E7%B6%B2%E8%B7%AF%E7%8A%AF%E7%BD%AA%E7%9A%84%E7%89%B9%E6%80%A7 。

9.M. Karyda and L. Mitrou, "Internet Forensics: Legal and Technical Issues", International Workshop on Digital Forensics and Incident Analysis, 2007.

10.B. Carrier and E. Spafford, "Getting Physical with the Digital Investigation Process", International Journal of Digital Evidence, Vol.2, No.2, 2003.

11.Eoghan Casey, "Digital Evidence and Computer Crime" 3rd Edition, 2011.

12. V. Baryamureeba and F. Tushabe, "The Enhanced Digital Investigation Process Model", Proceedings of The Digital Forensic Research Conference, 2004.

13.National Institute of Justice, "Results from Tools and Technology Working Group", Governors Summit on Cybercrime and Cyberterrorism, Princeton NJ, 2002.

14.Computer Forensics: Investigating Network Intrusions and Cybercrime (CHFI), 2nd Edition by EC-Council, 2017.

15.S. Khan, A. Gani, A. Wahab, M. Shiraz, and I. khan “Network Forensics: Review, Taxonomy, and Open Challenges”, Journal of Network and Computer Applications Vol. 66, pp. 214-235, 2016.