- 錯錯錯- 資安的迷思「秘密是秘密嗎」 -

-

- 社團法人台灣 E 化資安分析管理協會 理事長
- 中央警察大學資訊密碼暨建構實驗室 (ICCL) 王旭正教授

出了題目, 你寫了哪些題呢? 「我寫了三題」, 寫了哪三題，以及題目是什麼? 「我寫了-電腦病毒、網蟲（蠕蟲），以及 Diffie – Hellman 這三題，也就是第十八題、第十三題與第十四題」。「而第十三題和第十四題的題目有點像，跟電腦病毒有關」。歐, 看了看題目, 原來第十八題: Diffie 與 Hellman 在資安領域裡是那號人物? 有何特殊生平事蹟? 第十三題: 說明 Rootkit 在電腦病毒的議題中扮演角色為何? 第十四題: 電腦病毒、網蟲、木馬程式的意義為何?有何差異與比較?

我們資安生活即面對這裡的第十三題和第十四題的題目, 然第十八題可是資安科技的先驅者, 該再找機會好好做介紹呢。我們就來談談這個 RootKit 揭開這次的「秘密是秘密嗎」? 這 RootKit（隱藏程式）比較趨向反鑑識(Anti-forenscics)的概念，他不能讓別人知道他，但是他又嘗試在裡面扮演重要的角色。那你說明一下為什麼 RootKit 有點像反鑑識。「反鑑識主要是隱藏自己的身份不讓別人知道」。是啊, RootKit 是「隱藏程式」的概念，那 RootKit 的這種隱藏程式是為了做壞事？還是在必要的時候讓自己發揮作用？其實 RootKit 以正面的角度來看，是系統管理者的重要助手，管理者是正面的機制，入侵者是負面、破壞者。RootKit 本用於隱藏行程的功能，可對系統進行存取或將系統核心中所使用的行程隱藏起來，避免使用者在操作時不小心而影響到系統運作，出發點並非惡意。我們這個社會是一個正面的正義模式，當我們社會機制遭到破

壞的時候，就可以透過這個正義模式的機制，讓破壞攻擊降到最低。但如果有人有心將這個正面的機制拿來破壞社會次序，那他還是會變成負面的。例如今天一個警察代表正義的力量，但若被他人收買，那就會變成負面的去做壞事造成更大的社會危機。引用這些譬喻是為了說明當駭客利用此手法變向操作 RootKit 發展為將木馬程式等隱藏到作業系統中，從而造成意料之外的危險，那麼 Rootkit 將被視為是非常危險的惡意軟體。

鑑識（Forensics）與反鑑識可概念地想像為正反兩面 。傳統的鑑識，不需與和數位或電腦系統直接聯想也不常發生，例如槍支走火的判定、火災的火源在哪裡。卻在數位洪流裡，在身邊, 在不知不覺裡, 在把玩手機裡就會有鑑識問題跑出來，諸如大家的生活好朋友 LINE, FB 遭盜用, 莫名的成為入侵攻擊事件的主角、也會習慣性地 google 網路期能得科技法律的諮詢與瞭解, 尋求保障個人資料的安全與對隱私的重視等。所以 Security 和 Forensics 是搭檔而經常是綁在一起，將這 2 個詞合成在一起: 「SecForensics」是趨勢也是資安生活時勢裡最重要核心觀念與共通認知, 未來在新科技字典裡看到這個字可是預見未來的必然呢。科技越是發達, 隱私越是具價值, 「個人隱私」, 「家庭隱私」, 「國家隱私」, 「國際隱私」 真是呼應古云一句「修身」,「齊家」,「治國」,「平天下」的現代資安科技的重要最佳寫照, 似乎也自然地畫點出「資安就是國安」的精髓, decode it in total！

資安裡的鑑識有著電腦鑑識(Computer Forensics)、網路鑑識(Network Forensics)，是現在正夯的議題。鑑識無時無刻不在，當我們想著 iOS, 那可是 iOS 愛與恨 (你非常喜歡 iOS，但是 iOS 也可以做很多的壞事而恨之入骨呢)。無所不在的無線網路，但是不用錢的最貴，不要為了省錢，資料全部都被截走了還不自知呢！情報都是有價值的，要防止訊息被截走，要養成習慣不要輕易去

用免費的無線網路。我們台灣的生活模式裡 LINE 已經取代了很多我們生活上原本的習慣，例如打電話、看新聞、購物…等。由於現代人使用手機非常的普遍（在某種程度上可以說是「氾濫」），而在使用手機的過程當中，會很容易跟別人連上線，會互相傳送訊息，手機在不知不覺當中就會造成資安事件的入侵嫌疑者或被害者。在 LINE 裡，雖然大部份都是好朋友的 LINE，但是好友列表裡面也有可能是一些是不經意之中加入的 LINE，例如去買東西、逛街，加店家的 LINE 有打折，就會提供一些好處、優惠的方案給你，但 10 個好處裡面，或許有那麼一兩個是準備要在你的手機裡面植入木馬。「最便宜的最貴」！就是抓住人們貪小便宜的心態，就這麼不經意之中加入了一些 LINE 帳號而無時無刻不在發生資安生活的入侵事件。

這些商家，偶爾會送些訊息到你的手機，可能會再提供一些網址請你按連結，不知不覺當中，你的手機就會被植入木馬，不經意就被入侵了。這個就是透過手機的數位訊號達成的入侵行為。如果被入侵的人覺得不舒服，這時就需要「數位鑑識」了。反過來有時候我們也可能錯誤操作流程裡「不小心」入侵了別人的手機、電腦，雖非是故意的，但行為上就是已經被對方覺得你是在干擾他、入侵他了。無心之間擾亂了別人的系統，對方覺得就是你在作怪，入侵對方系統，無緣無故就被對方告了！「數位鑑識」裡讓證據會說話可還你清白，卻也顯露了驚人的現世報-「秘密已經不再是秘密」。

現在科技的環境之下，為什麼「秘密已經不再是秘密」?手機可以是一個資料庫、資訊的來源，另一方面也是貼心的工具存有許多的秘密。而且如果真的成功的將木馬植入到別人的手機裡，就可以完全知道別人手機裡的狀況。手機還可以透過一些 APP 的小程式，就可以去定位別人。這些軟體並非木馬程式看似好用，可以直接呼朋引伴，也能你在哪裡啊…，秘密已經不再是秘密了

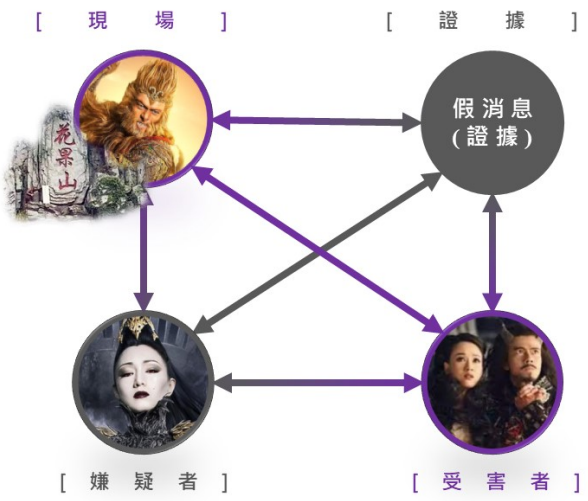
呀。秘密與鑑識可真是有趣, 在資安生活中想要秘密, 卻又不知覺裡全都露呢! 上網的時候，我們會存「我的最愛」選單，其實這會洩露我們的秘密，不知不覺變成日後的證據、情報。例如非法製造槍枝或非法栽種大麻的調查裡可以很快被定位出線索與蛛絲馬跡，證據就是這樣蒐集到的。無形當中，我們已經放置了太多的證據在網路上、電腦中卻渾然不知。「魚與熊掌」vs. 「秘密與鑑識」, 呵呵，…不就異曲同工之妙。

數位鑑識乃使用科學技術進行搜集、鑑定、找出關聯性、運用各種技術將數位證據文件化，並找出與案件所需且相關的數位證據。數位證據有如電腦結構中之硬體，這些硬體散落在犯罪現場，需要靠鑑識人員細心的將所有的證據一一找出，電腦結構中空有硬體而沒有軟體的輔助，電腦硬體也是英雄無用武之地，從這個觀點我們可以知道電腦結構中，硬體跟軟體是相依並存的，缺少了那一部分都無法發揮其功能，由於電腦硬體與軟體的天作之合，開啟了電腦世代的新紀元。反觀「鑑識」與「證據」的組合，互依互存有如天作之合的軟體「鑑識」與硬體「證據」，少了其中一種就無法發揮其作用。因此如果沒有「證據」的殘屑佇留，何來「鑑識」之推敲、溯衍，另一方面沒有「鑑識」的抽絲剝繭，碎屑依然散落，就算有再多的證據也無「證明力」來證明犯罪事實。

瞭解了數位鑑識與證據之關係，最重要的工作是如何從眾多的證據中找到足以證明犯罪的事實，另一方面是利用數位鑑識工具及方法所萃取出來的證據，如沒有妥善保存則會失去其證明犯罪之證據力及證明力。其中證據力，是一個水平的概念; 證明力，則是垂直的概念。掌握愈多證據，愈多元化，就有愈強的證據力。什麼是垂直的證明力？你可以從一根頭髮，辨別出性別判斷他是男生或女生（第一層）、年齡層（第二層），或是分析出這個人有哪些疾病（第

三層），掌握愈多層次，代表證據明力愈強！

「鑑識」是將事情弄得清清楚楚，是一個流程、一個說法，而整個過程當中，要有一些東西是實質、眼睛看得到的，就是所謂的「證據」。所以，要構成犯罪，需要具備的四個元素，第一個：真實的犯罪現場（網路上的虛擬、想像的，沒有留下痕跡的，是不成立；當有留下痕跡、紀錄、文字等，即可為成為證據的基本依據！）；第二個：被害人；第三個：嫌疑人；第四個：證據。我們將整個過程、這四個原素的來龍去脈、兩兩的互動關係上，描述得非常清楚，這樣的一套過程模式，就是「鑑識」。所以當今天是手機犯罪，就需要將手機扣押，撈出各種可能的證據，再去定位一下犯罪的現場在哪裡? 誰是被害者? 誰是可能的嫌疑人? 到底做了什麼事的證據痕跡？嘗試將證據和現場的關係在那裡？證據和被害人的關係在那裡？證據和嫌疑犯的關係在那裡？還有嫌疑犯和被害人的關係？被害者為什麼會在這個現場？嫌擬犯為什麼會在現場？全部弄得清清楚楚，整個過程是很完整的時候，才是真正的犯罪了。圖一中, 我們以數位鑑識的 K_4 完全圖說明如下, 其中孫悟空的花果山為事件現場; 白骨精為發布訊息的嫌疑者; 發布的訊息經資安的鑑識檢驗為假消息證據; 牛魔王與芭蕉公主為假消息事件的受害者，此四元素的關係得呈現完全的相互關連性。



圖一 數位鑑識的 K_4 完全圖

數位鑑識與反鑑識在資安生活, 並不是狹隘的相反定位而是相互為用。反鑑識主要用意是保護商業利益，隱藏一些機密的資訊，反鑑識裡證據不能被找到。反鑑識的作為是往社會價值的正面方向發展，而不是只就「把犯罪的證據藏起來」這樣的角度來看而已。如果說「反鑑識是把犯罪的證據藏起來」，大帽子一扣，聽到「犯罪」這兩個字，大家都會怕，聽了會心驚膽跳。例如一間商店寫「殺人放火店」，裡面賣凶器，一定會倒, 因為非社會正義當然立即被取締關門的。又若你貼文在 FB 上標明「殺人放火店」，按讚的人也都可能被調查是否有犯罪動機。現在的巡邏有所謂的「網路巡邏」，換言之不再只有傳統的巡邏，科技-資安-鑑識已是資訊科技國際化的趨勢，所以傳統巡邏也早在資訊時代洪流裡活化成網路巡邏。我們剛才說的 FB，一旦在 FB 上的 貼文中具有擾亂社會秩序的嫌疑時該也很快地被社會公權力單位所關注並迅速地抑制。藉此我們想說明「反鑑識」，並不是狹隘地將證據湮滅掉，鼓勵犯罪，而是在保護商業利益方面的智慧財產權（例如網站新聞內容是有財產權的），資訊隱藏、資料偽裝亦或是，軍事間諜、線民臥底等，也就是反鑑識的正面價值觀，是協助情報

偵蒐, 裡應外合地破案，透過迂迴的方式打擊非法的危害社會秩序的各式行為。我們在此次資安生活裡一開始的提到開場 rootkit 也即是我們「反鑑識」的最原始正面價值觀用意了。

生活中一直都存在傳統的犯罪，有了電腦犯罪之後，還是會有西瓜刀、棒球棍。總不能拿手機對砍吧，哈！但科技的犯罪遠比傳統的犯罪誇張，無遠弗屆，產生的後遺症，不是棒球棍打一打就可了結的，幾乎都是幾億起跳的經濟成本損失。「高科技方式搶銀行」(可不是以前戴著鴨舌帽搶銀行，是用高科技方式，網路入侵搶銀行…）如同「運籌帷幄，決勝於千里之外」，然秘密或證據的天知-地知-你知-我知的時空背景也在數位鑑識時代裡成了錯-錯-錯的大家都知道的秘密，「秘密不再是秘密」。證據就在你-我-他，在系統、手機、電腦、網路的存留裡, 近在我們身邊呢。我們生活裡，資安科技與個資已是密不可分的重要貼身好朋友。 懂資安, 找證據(鑑識), 保障個資秘密(反鑑識)成為現在科技生活保護自己的重要常識，藉此當然也自在的得以享受科技與掌握科技 。