秘密已經不再是秘密？

◆ 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

科技越發達，隱私越具價值。現代資安科技重視「個人隱私」、「家庭隱私」、「國家隱私」、「國際隱私」，恰對照古云「修身」、「齊家」、「治國」、「平天下」，也自然畫點出「資安就是國安」的精髓。

Security 和 Forensics 是搭檔 成為「SecForensics」趨勢

傳統鑑識（Forensics）不需與數位或電腦系統直接聯想，也不常發生，例如槍枝走火的判定、火災的火源在哪裡；然而，如今在數位洪流裡，卻在身邊、在把玩手機時，不知不覺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，莫名地成為入侵攻擊事件的主角；民眾也會習慣性地藉 google 網路，期能獲得科技法律的諮詢與了解，進而尋求保障個人資料的安全等。所以 Security 和 Forensics 現今已是搭檔，經常綁在一起，兩者合體即為「SecForensics」，這詞是趨勢，也是資安生活時勢裡最重要核心觀念

在臺灣，LINE 已成為生活上不可或缺的手機軟體，諸如通話、視訊、看新聞、購物等各種應用皆會透過 LINE，其普及率已讓其容易成為資安事件的嫌疑者或被害者。

與共通認知，未來在新科技字典裡看到這個字可是預見的必然。

科技越是發達，隱私越具有價值，「個人隱私」、「家庭隱私」、「國家隱私」、「國際隱私」是現代資安科技呼應古云「修身」、「齊家」、「治國」、「平天下」的最佳寫照，似乎也自然地畫點出「資安就是國安」的重要精髓，decode it in total ！

與手機的愛恨情仇

資安鑑識有分電腦鑑識（Computer Forensics）、網路鑑識（Network Forensics），是現在正夯的議題。鑑識無時無刻不在，當我們想著手機，那可是與手機的愛與恨，即你非常喜歡手機，然手機也可以做很多的壞事而讓你恨之入骨呢。

無所不在的無線網路，便捷又免費，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！情報都是有價值的，要防止訊息被截走，不要輕易去用免費的無線網路。在臺灣，LINE 已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普遍（甚可說是「氾濫」），在使用手機的過程當中，會很容易跟別人連上線、互相傳送訊息，手機在不知不覺當中就會成為資安事件的入侵嫌疑者或被害者。

在 LINE 裡，雖然大部分是好朋友，但在好友列表裡面也有可能是不經意加入的 LINE 好友。例如加商家為好友才能下載免費貼圖，逛街買東西要加店家的 LINE 才有打折等等。商家總會提供一些好處、優惠的方案給你。但在 10 個好處裡面，總有那麼一、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，才會無時無刻有駭客入侵事件發生。

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，不知不覺中，你的手機就會被植入木馬，不經意地被入侵了。這時就需要「數位鑑識」來解救了。

手機可以是一個資料庫、通訊器，但同時亦可能成為祕密暴露的出口。

驚人的現世報—祕密已經不再是祕密

反過來，有時候我們也可能流程操作錯誤，而「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，對方卻覺得就是你在作怪，入侵對方系統，無緣無故就被對方告了！「數位鑑識」裡證據會說話，可還你清白，卻也顯露了驚人的現世報—「祕密已經不再是祕密」。

為何「祕密已經不再是祕密」？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，能幫你存有許多不欲人知的祕密。而且如果真能成功地將木馬植入別人手機裡，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 小程式去定位別人。這些軟體看似好用，可以直接呼朋引伴，也能清楚知道你在哪裡。啊，如此一來，祕密就已經不再是祕密了呀。

軟體「鑑識」與硬體「證據」相輔相成

數位鑑識乃是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，電腦若僅有硬體而沒有軟體的輔助，電腦硬體就像是英雄無用武之地，也由於電腦硬體與軟體的天作之合，才得以開啟電腦世代的新紀元。

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。

「鑑識」就是將犯罪現場、證據及被害者與嫌疑人之間的關係與來龍去脈描述清楚。

如何從眾多證據中，找到證明犯罪事實

了解數位鑑識與證據之關係後，最重要的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，好好保存以免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。而什麼是垂直的證明力？你可以從一根頭髮，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，代表證據證明力愈強！

「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：被害者；第三個：嫌疑人；第四個：證據。我們將整個過程、這四個元素的來龍去脈、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」。

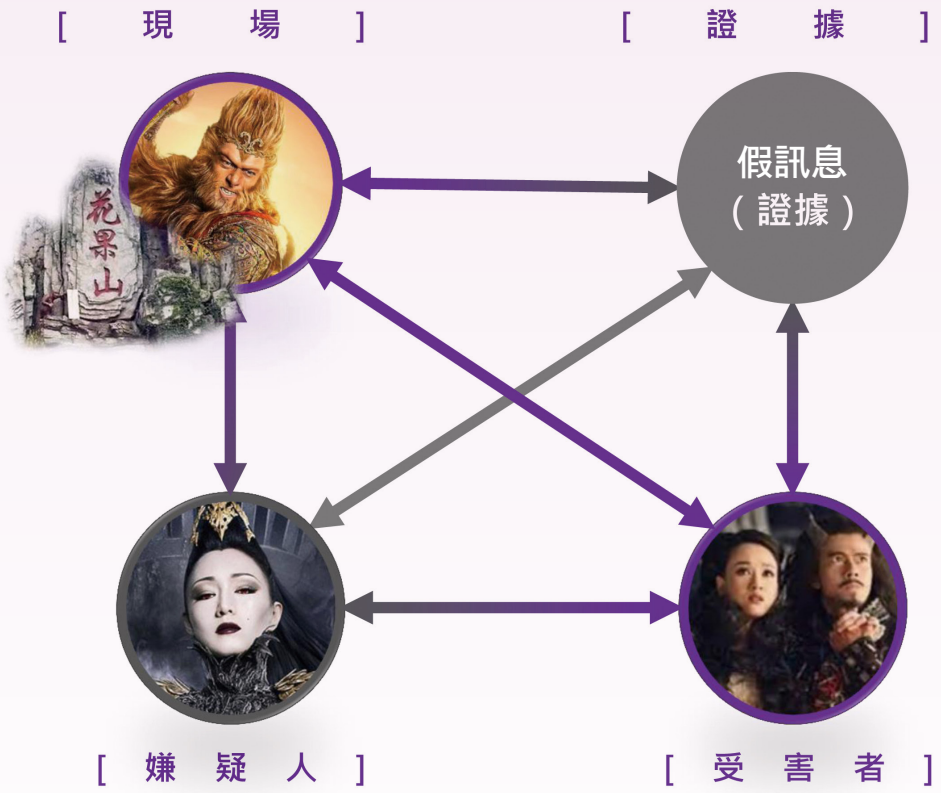

圖 1　數位鑑識的 K_4 系統面相

所以當手機犯罪，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？證據和現場的關係？證據和被害者的關係？證據和嫌疑人的關係？還有嫌疑人和被害者的關係？被害者、嫌擬人為什麼會在現場？當把全部證據找得完完整整，整個犯罪過程弄得清清楚楚，才能真正地說服所有人。

圖 1 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人，發布的訊息經資安的鑑識檢驗為假訊息證據，牛魔王與芭蕉公主為假訊息事件的受害者，此四元素的關係得呈現完全的相互關連性。

由 RootKit 談「反鑑識」概念

數位鑑識也有「反鑑識」的概念，RootKit（隱藏程式）就是比較趨向反鑑識（Anti-forensics）的概念，它不能讓別人知道它，但是它又嘗試在裡面扮演重要的角色。為什麼 RootKit 有點像反鑑識？「反鑑識主要是隱藏自己的身分不讓別人知道」。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，那它還是會變成負面的。例如警察向來代表正義力量，但若他被人收買，變成負面的去做壞事，反而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 時，反會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。

反鑑識的正向價值觀

數位鑑識與反鑑識，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，反鑑識裡的證據不能被找到。然反鑑識不是「把犯罪的證據藏起來」，因為如果說「反鑑識是把犯罪的證據藏起來」，大帽子一扣，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，

```
static int __init procfs_init(void)
        {
                //new entry in proc root with 666 rights
                proc_rtkit = create_proc_entry("rtkit", 0666, NULL);
                if (proc_rtkit == NULL) return 0;
                proc_root = proc_rtkit->parent;
                if (proc_root == NULL || strcmp(proc_root->name, "/proc") != 0) {
                return 0;
        }
        proc_rtkit->read_proc = rtkit_read;
        proc_rtkit->write_proc = rtkit_write;

        //MODULE INIT/EXIT
        static int __init rootkit_init(void)
        {
                if (!procfs_init() || !fs_init()) {
                        procfs_clean();
                        fs_clean();
                        return 1;
                }
                module_hide();

                return 0;
        }

        static void __exit rootkit_exit(void)
        {
                procfs_clean();
                fs_clean();
        }

        module_init(rootkit_init);
        module_exit(rootkit_exit);
```

RootKit 是系統管理者的重要助手，但若遭入侵者利用，就會變成危險的破壞者。（Photo Credit: Christiaan Colen, https://www.flickr.com/photos/christiaancolen/21133308006）

一定會倒，因為非社會正義當然立即會被取締關門。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。

現代巡邏有所謂的「網路巡邏」，在「科技—資安—鑑識」已是國際化的趨勢下，傳統巡邏也在資訊時代洪流裡演化成網路巡邏。就如剛才所說，若在 FB 上張貼具有擾亂社會秩序嫌疑內容時，也會很快被社會公權力單位之網路巡邏者發現，並迅速地被抑制。

藉此我們想說明「反鑑識」，並不是狹隘地將證據湮滅掉來鼓勵犯罪，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，也有反鑑識的正面價值觀，能協助情報偵蒐，裡應外合地破案，透過迂迴方式以打擊危害社會秩序的各式非法行為，這也是「反鑑識」的最原始正面的價值觀。

運籌帷幄，決勝於網路之內

生活中一直都存在傳統犯罪，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！但科技犯罪遠比傳統犯罪誇張、無遠弗屆，戴著鴨舌帽搶銀行的行為已落伍，以「高科技方式搶銀行」正時興，如同「運籌帷幄，決勝於千里之外」，在看不到的地方算計才是勝敗關鍵。而網路犯罪產生的經濟災損，幾乎都是上億元起跳，超乎想像，也不是以棒球棍回擊就可了結的。

祕密或證據從「天知、地知、你知、我知」之時空背景，在數位鑑識時代裡成了「錯、錯、錯、錯」之大家都知道的祕密，「祕密已經不再是祕密」；證據全留存在系統、手機、電腦、網路，近在我們身邊！資安科技與個資已是密不可分的重要貼身好朋友，而懂資安、找證據（鑑識）、保障個資祕密（反鑑識）成為在現代生活中保護自己的必備武器，藉此，也才能自在地享受科技帶來的便利。

社團法人台灣 E 化資安分析管理協會（ESAM）

中央警察大學資訊密碼暨建構實驗室（ICCL）