- 訊息追追追- 鑑識 & 真假 buddy buddy -

理事長-社團法人台灣 E 化資安分析管理協會
(ESAM, https://www.esam.io/)

中央警察大學資訊密碼暨建構實驗室（ICCL）

＜本文作者：社團法人台灣 E 化資安分析管理協會(ESAM, https://www.esam.io/)，2018 年創立，從事 E 化資訊安全的分析管理與學術研究，並與政府、產學及國際資安機構交流與合作，推廣資訊安全應用與發展，培育資安專業人才，協助企業、產業評估資安分析與風險為宗旨；中央警察大學資訊密碼暨建構實驗室（ICCL），1998 年 12 月成立，目前由王旭正教授領軍，並致力於資訊安全、情資安全與鑑識科學、 資料隱藏與資料快速搜尋之研究，以為人們於網際網路(Internet)世界探索的安全保障（https://sites.google.com/site/iccltogether/）。＞

鑑識這字眼，在資訊網路未如此發達時是個專業，非常地專業的詞兒。直觀上想到他就是社會新聞事件裡的犯罪、非法活動的軌跡，證據裡判斷真假，例如台灣早期發生槍擊事件，那可是不得了呀。在台灣這個槍枝不開放的法令規定裡，私藏擁有槍枝，甚至使用槍枝進行製造各種可能的社會犯罪事件，在槍枝開槍那一剎那，呵，在事件現場裡，即開始有了「鑑識」的字眼出現了。槍枝沒子彈，倒也白搭一場，是的，因為子彈蹤跡，槍枝來源必然是槍擊事件現場所高度興趣的焦點，透過所遺留下的子彈，可以推敲槍枝的種類、槍型，並進一步在彈道落點的曲線，判斷距離等數據都可逐步抽絲剝繭地還原最原始的現場。是呀，這就是「鑑識」給人的印象，專業，判斷真假。

然在這資訊時代裡，鑑識再也不單純的專業形象而已，在人手一機，所有的訊息的通聯中，不經意，那會有各式的互動。訊息的傳遞怎會跟「鑑識」有關係呢？這可是有趣的事呢。還記得我們在前二集中的網路嗎? 是啊，現在的網路，資訊網路無遠弗屆，人們也是人手一機，隨時隨地在滑，我滑、我滑、我滑滑滑、滑手機……。透過手機，隨時在上網找資料，應付工作需求，計畫報告的參考依據……。經常在手機操作裡網路直接下單、交易買賣，手機的網路上網方便，我們不經意的成了訊息、資料的傳送者，亦成是接收者，我們竟也不自覺地竟成了網路裡最佳男女主角呢。 當身為傳送者(即主動的角色)，那即是所知道、所擁有、所經手的訊息，主動的經由網路，在各個時間(anytime)傳遞到各個可到達的人(anyone)與地方(anywhere)。主動裡還有可能誤觸網路裡設下的圈套陷阱，相信您經常聽到的網路釣魚，就是如此，設陷者用各式的盲點，在人眼對文字、圖像辨識的模糊與好奇，例如 “ICCL”與“iccl”, 您有無看到前者的“l” 是 後者的“l” 嗎? yes or no ? 呵呵，讓您不經意中進入異想新鮮的世界，自以為「樂透了」、「中獎了」而喜不自勝。事實上，卻是逐步陷入迷網，被反導入非法惡意程式、病毒，進入主動者的手機(亦或工作，作業的電腦操作平台)反遭監控，破壞，與洩漏主動者的個資資訊。呵呵，有種落入俗話俚語所說的「公親變事主」的無端惹出麻煩來了呢。而當主動者反倒成了被攻擊的受害者時，「鑑識」隨即派上用場，在資訊流、資料流、時間流、啥「關連流」裡，能逐次釐清因果關係，尋出真假異同，那即是鑑識觀念在主動端的重要而並立見真章。

既是網路裡最佳男女主角 當然也會玩起角色互換的遊戲，變身傳送者為被動的接收者角色。在被動者方面，一般有三種型態的訊息，一則是文字訊息，二則是多媒體性訊息，三則是程式碼訊息。就網路資訊傳播發展早期，這三種

型態裡，最令人畏懼的是第三則的「程式碼」訊息，避之唯恐不及呀。為何如此畏懼程式碼，如視為毒蛇猛獸呢。這也實在是有其典故的啦，有道是「一朝被蛇咬，十年怕草繩」的省思呢。咱台灣在這方面，也曾是「台灣之光」，這時「光」字大概得用「兩光」這樣的字義來褪色光環才是呀。

話說病毒的來源，當然我們可回顧一小段故事，那是約 1960 年代時, 由美國電話電報公司(AT&T)貝爾實驗室裡的幾個年輕小伙子生活玩味裡所設計出來。當時的用意或許是遊戲程式的想法，在遊戲中會覆蓋或破壞遊戲玩家的電腦記憶體，由於遊戲程式的原始碼很小，使得這支程式極容易被複製，而具有高存活率。也會因碰到偵測病毒(遊戲)程式，而反而進一步去破壞，攻擊偵測程式，這即是遊戲程式的設計者與遊戲玩家一般認定的遊戲精隨與有趣味之處。相互攻防裡，取得最終的勝利，呵呵，換言之，就是把對方程式完全消滅，即「病毒」成功入侵系統。

1986 年，巴基斯坦人製造 Brain 病毒程式，才正式為個人電腦世界的玩家，使用者注意到，病毒程式對電腦系統所造成不安全性與不穩定性，而影響電腦系統正常運作。咱台灣「兩光」也在 1999 年不遑多讓，有一聞名世界的 CIH 病毒，由台灣年輕人所設計。當時災情可是慘兮兮的，尤以亞洲地區更為慘烈。CIH 病毒能儲存在電腦記憶體中，並感染電腦的輸入/輸出系統，接著摧毀硬碟中的所有資料而癱瘓系統。講起歷史故事，才能「飲水思源」對程式碼訊息得能有更深刻認識與警惕。然而這些程式碼訊息隨著時空，科技的快速翻倍進展，早已是集各家「精華」， 各路「險招」，行極「冰寒」於一身。從歷史故事的遊戲病毒(virus)源起，至進化成木馬程式(Trojan Horse)，網蟲(worm)、攻擊程式(attack programming)，竟也成為現在資安科技、網路攻防戰裡，漏洞問題與攻擊手法的是非泥沼之地。

這「資訊戰」、「網路攻防戰」裡的是非之地，被動者接受訊息的第三則訊息型態，雖是最為人畏怕，卻也因敵在「明」，我們可以藉由一些跡證來清楚辨識訊息「真假」，得以避免踩到資安的埋雷。最直觀的方式，我們總告誡，當收到不明的檔案亦或程式碼，尤其具有程式執行能力的程式碼(一般是檔案附加名具執行的常見設定碼，例如“.exe”等)一旦執行，資訊系統經不經意的執行裡將有高風險的破壞程式感染進而全面癱瘓之禍。當下意識即刻快閃的刪除，免惹「無妄之災」。

再則我們來到被動者接受訊息的第二種型態，那就是多媒體訊息。這多媒體訊息在資安領域裡，是有別於密碼(cryptography)發展的另一分支領域，我們稱之為偽裝學(steganography) 。這門分支與密碼發展最大的不同在於名如其字的「偽裝」二字，可猜得知意為「有看沒有懂」，英文可變出一句話，say it, “Seeing the unseen” 。舉大自然裡的生態為例，許多動植生態都是偽裝專家，以動物裡的變色龍為例，隱藏樹叢、 枯枝中，隨著綠葉、枯樹的色澤有各式的身體顏色調變，讓食物鏈上層的獵食者，永遠摸不著，轉眼間不見了，其實「遠在天邊」,「卻近在眼前」呢。

偽裝的奧妙不只在自然的生態，生存遊戲裡，已是動植物本能的適者自然生存的重要基碼。我們人類歷史與生活的偽裝運用，也是精彩絕倫，尤其在戰爭的史實上，紀載最是豐富，得為嘖嘖稱奇。舉一看似無奇的一頭秀髮，當剃髮至髮底竟能從頭皮處，看到所刻、寫、刺的各式機密或特殊訊息，得以完成戰事攻防裡，秘密通訊傳遞的目的。該是偽裝學裡外表舉止正常裡，卻在頭髮底層，有著完全不為人知的另一個祕密傳遞。從這裡，我們為偽裝學與密碼學做些有趣的區分，那即在偽裝學裡所看到的訊息表象是明顯具有意義的，與實際所不願表現的秘密是不相同的。藉由偽裝的行為，得以隱藏真實的訊息情境。另密碼學裡，訊息經加密後，即是不具意義的文字符號形式，雖無法窺見實際內含，但也因密碼加密裡，加密訊息不知其意，被動者的訊息接受後，卻也能夠因懷疑而可能刪除、直接破壞訊息讓內涵完全消失無作用。所以在現代科技裡，第二種型態的多媒體訊息，當欲進行訊息傳遞時，便可將訊息藏匿於多媒體中，訊息藉多媒體的隱藏，可正常存藏於眼睛看到的影像或圖像中，亦可於耳朵聽到的音樂、音律中。

https://www.instagram.com/p/BGpheOMgbxg/?utm_source=ig_web_copy_link

在多媒體時代，我們所接觸的訊息更具多變化性，真真假假五花八們、花樣多變。為何在多媒體中能夠讓假訊息的多媒體外象如此活躍，以影像圖為

例，主要是因人類眼睛對於色彩具有失真的容忍度，也就是我們常在生活裡，玩笑話裡的「朦朧美」、「霧裡看花、花還是花」的感官意識。對於多媒體影像圖的樣子，當認定具有何含意時，是草、是河、是山、是路、是屋，那是深刻烙印在腦海，不會因一些模糊而改變的印象。而數位時代，構成影像圖的每個數位像素、資料，當改變裡頭一些位元資料時，對於整體影像視覺效果在視覺容忍度與感官意識可接受下，將無法明確識別差異性，多媒體形式的假訊息外象當然可以在其中混水摸魚，逃過一劫，達陣得以真實秘密傳遞的目的。當然對於訊息的暫時接觸者所接觸到的是一張、一份多媒體假訊息的影像圖，所認定也是一份貨真價實的，也具有意義的資訊多媒體，所以暫時接觸者是以為「真訊息」。然對於在達成訊息傳遞協議的通訊雙方, 通訊群體，「訊息」的傳送者與接受者，是讓中間的暫時接觸者，所看到的卻是「假訊息」，誤以為影像圖的意識認定即是「真訊息」。到此，真假之間，是否您也看得霧裡看花，不再是花，而是「霧煞煞」了。呵呵，偽裝的多媒體，令被動的訊息接受者，清楚多媒體印象所呈現的意義，雖偽裝背後所隱藏的真訊息不為人知，卻也可接受多媒體的意識裡外象意境。偽裝之意，在於欺敵，在第二種的多媒體訊息形態裡，或許無誤導(有論無意或蓄意)於呈現多媒體訊息時的具體內容，因該訊息意在偽裝多媒體內涵裡的真實秘密。

然而被動者的訊息接收裡，第一種訊息型態的文字訊息，最是令人毫無防備。當若為假訊息，將是這三種訊息型態中影響最為深遠的訊息。對於假訊息，歐洲理事會有一相關名稱為「資訊失序」/「Disinformation」(原文: Information that is false and deliberately created to harm a person, social group, organization or country) 是經過刻意編造，用以傷害個人、社會團體、組織或國家之訊息，目的在煽惑或鼓動人心，藉以謀取某種政治或商業利益；另外「資訊失序」還有一種描述用語「Misinformation」(原文: Information that is false, but not

created with the intention of causing harm)則是指內容錯誤但目的並非為造成傷害而刻意創建的訊息。在假訊息之要件上，國際組織主張應符合真實性(fidelity)與目的性(intention)，所以「Misinformation」雖內容有虛假嫌疑，惟因缺乏惡意欺騙之意圖，多屬誤傳性質之訊息。而 「Disinformation」是目前較符合國際對假訊息之定義或共識，是有系統性的作假，企圖製造有目的性的損害，能對特定人士、團體或組織引起一定程度的影響，亦為政府部門積極防處之範疇，避免導致社會大眾間的不信任和紊亂。

對於文字的假訊息，咱資安科技裡資安的密碼技術，並不因此坐視不管，反倒有好的因應呢。讓我們回顧上一集的 PK(public key) 。在公開金鑰系統裡 PK 的使用，如果訊息的傳遞，由真實來源的傳送者在傳送的過程中，加上與訊息緊密相關的驗證碼，那麼不就是可以清楚地知道訊息是真、是假，有無被竄改。另外在現代密碼的技術中，有一個重要名詞叫「HASH」，這武器「HASH」是能夠不管訊息有「山這麼高、海這麼深」，都可以變成一個短短的資料量，好像是神奇的魔術一樣。例如一個超大硬碟容量，都可以變成一個短短的東西。只要硬碟裡的一絲點位元或一根寒毛被動到，這個短短的東西就會變得很不一樣。所以如果當訊息在 HASH 第一次運算和 HASH 第二次運算，訊息都一樣，就代表這個硬碟裡的東西沒被動過，很神奇吧！

網路假消息傳遞充斥裡，我們適度運用資安科技裡的密碼技術處理假消息，就不用流於口水戰。有了這兩大法寶,「PK」還有 「HASH」, 這假消息就無所遁形了呀 。任何來源發布訊息使用 PK 系統 然後再進行相關的比對，如果兩邊的內容一樣，就可以證明這真假訊息是否真實的來源端所提供的。處理機制裡，我們可先用 HASH 做訊息的處理，因為一般訊息較長，用 HASH 的技巧可變成比較短的訊息而且用 HASH 也可以用來保證一旦訊息被更改後，可以很快地

發現竄改。因為原始訊息的一個文字或一丁點的位元資料被改變後，整個 HASH 的結果都會被改變而不一樣呢，接下來就是再用 PK 系統來產生驗證碼。在前兩集孫悟空與牛魔王的故事裡我們稍作小技巧，增加了 HASH 可讓您立見真章，一點就通呀 。

這裡我們討論真假訊息的兩種狀況，第一種訊息傳遞是無論訊息真假，但發布訊息的人是假(不對)的，舉例來講: 今天要發佈獎懲訊息，這種訊息不是每個人都可以發布的，一定要是權責單位發布的。假設今天是路人甲乙丙說的, 擅自發佈的訊息都要打個問號? 因為這些人不是權責單位。當然若是權責單位承

辦人，發言人講的，那訊息可信度即是相對提高的。在 PK 系統的驗證碼比對中，真正權責單位的 PK 再搭配 HASH 的處理， 事實將立即擺在眼前。另外訊息傳遞的第二個情形是，權責單位的確發佈事實訊息，但發佈的訊息被蓄意先下架，內容遭竄改後，例如把褒獎令的內容改掉，再進行發佈。此情形裡，發佈的權責單位是對的，但是內容是被改過的。但是這一個過程中加上一個 HASH，就可以把這問題爭議處降到最低，因為依照所提到的密碼技術概念，HASH 這武器可清楚證明訊息是否被造假竄改的判斷依據呢。 例如若今天的褒獎令的訊息裡有相關人物數量的名額是 10 個，被修改成 9 個，就會發現所傳遞褒獎令的訊息經第二次 HASH 的運算後就會很不一樣，因此被發現造假了而被很快淘汰訊息的可信度的，所以搭配 PK 的 HASH 也是解決假訊息的關鍵技巧之一。

訊息飛舞裡，各式傳聞不斷，「真假」、「假真」、「黑白」、「白黑」、「虛實」、「實虛」、「清清楚楚」、「不清不楚」……。在資安科技裡，除了最為直觀認知的重要「隱私」保護外，另一訴求就是「鑑定」，也就是對於來源能清楚，對於訊息的真假判斷能有依據，得具有說服力。而「鑑識」即是在「鑑定」的各式場合、各式情境裡，攸關權益，在人為、人治世界的生活互動裡，無論有意、無意的侵犯裡，所遺留的證據痕跡中，抽絲剝繭的步步推理裡能找到真相、重建現場。資訊生活裡，我們使用的 3C 平台，讓我們更是方便的操作訊息，有時是傳遞訊息的主動者，也是接收訊息的被動者。訊息的多元化，享受知識的普及化，快速汲取知識下，另一類資安危機也浮上檯面。真假訊息在這些年來，成了「網紅」了，也不知覺裡淪為各式可能不當企圖運用的操作，得以混淆人的意識與判斷影響我們生活，甚而造成社會問題與資安的危機淪為科技犯罪所利用得以獲利。現在的「鑑識」與「真假」在人手一機的訊息來回裡，藉由資安的密碼技術發揮，訊息得以鑑識真假。傳統的人腦思維判斷方式已轉化成資安科技的「鑑識」加乘確認，藉此得以保障「真假」訊息傳遞的真

實性，減輕可能的權益損傷，成了資安生活中共生共存的 buddy buddy 新重要搭檔。