OTT 機上盒侵權與資安數位鑑識架構初探

莊明雄[1*]、林俊賢[2]
[1]刑事警察局電信偵查大隊、[2]中華電信數據分公司
[1]saxbear@email.cib.gov.tw、[2]charleslin@cht.com.tw

摘要

國內近年來大量流行的 OTT 機上盒，不僅透過網路民眾可免費無遠弗屆觀賞線各式影音媒體外，也可能淪為新的物聯網資安威脅，本次探討 OTT 相關 CDN 傳輸技術、內容傳輸合法性、針對以 Android 為主的機上盒進行數位鑑識提權(Root)適法性及從個案進行解析提出初步數位鑑識架構探討，而與其他電腦鑑識不同之處，數位載具(行動裝置、穿戴裝置或機上盒)不應繼續堅持做鏡像後來進行鑑識分析，可引用 ISO/IEC27037 概念直接對於證物進行採證，並仍秉持對於以最小損害性為原則來處理，因此仍循原 NIST 所規範之 ISO 800-86 鑑識指南，從 Collection (收集)、Examination (檢驗)、Analysis(分析)、Reporting(呈現)等 4 個步驟框架進行鑑識下，但對於 Android 機上盒本文中提出另一種鑑識作法，可鑑供作為現行工具不足下之補強方法，以達成數位鑑識的目標。

關鍵詞: OTT、CDN、機上盒、資訊安全、資安鑑識、物聯網

A Study on OTT Box's Infringement and Security of Digital Forensic Framework

[1]Chuang Ming-Shiung, [2]Lin Chun-Hsien
[1]Criminal Investigation Bureau(Telecommunications Investigation Brigade)
[2]Data Communications Branch, Chunghwa Telecom Co., Ltd.
[1]saxbear@email.cib.gov.tw, [2]charleslin@cht.com.tw[2]

Abstract

The new trend of popular OTT Box is such a phenomenon not only for people in Taiwan to have pervasive entertainment with versatile of multimedia content through internet, but, in some way, it also brings the potential security threat of internet of things (IoT). In this paper, we focus on admissibility on rooting Android system for digital forensic purpose with several instants of case study in terms of related technologies in CDN transmission and legality of content transmission in order to propose the primary digital forensic infrastructure on the Android base OTT Box.

Compared to generic computer forensics, the forensic technique used for digital platform, such as mobiles, wearables and setup box, should not stick to the principle of image mirroring first and forensic analysis. We may follow concept of ISO/IEC27037 to collect evidence directly and must handle it by rule of minimal impact: the frame procedure from collection, examination, analysis to reporting by ISO 800-86 forensic guideline of NIST. The alternative way we propose in this paper can be used as complementary way for the existing digital forensic procedure to fulfill the demand of investigation objective.

Keywords: Over The Top, CDN, Tv-Box, Information Security, Digital Forensic, Internet of Thing

壹、前言

各類型的網路平台的興起，帶動多媒體的發展，從傳統的電視媒體的傳播管道至現今以網路平台作為傳播媒介的變革，讓媒體影音的串流技術大步的躍進每個人的生活之中。而近年在各種網路媒體與技術平台互相競爭與彼此影響之下，也使得臺灣各家媒體關注起網路傳播的管道，更重視起 OTT(Over-The-Top)的傳播內容，並以導入數位機上盒設備的策略來搶搭線上影音服務市場。這當中除了背後網路技術與影音串流上的支持外，如何快速將影音媒體導入用戶的裝置中(如電視、平板、手機等)以達到快速且豐富媒體內容的過程，成為了全球媒體產業兵家必爭之地。

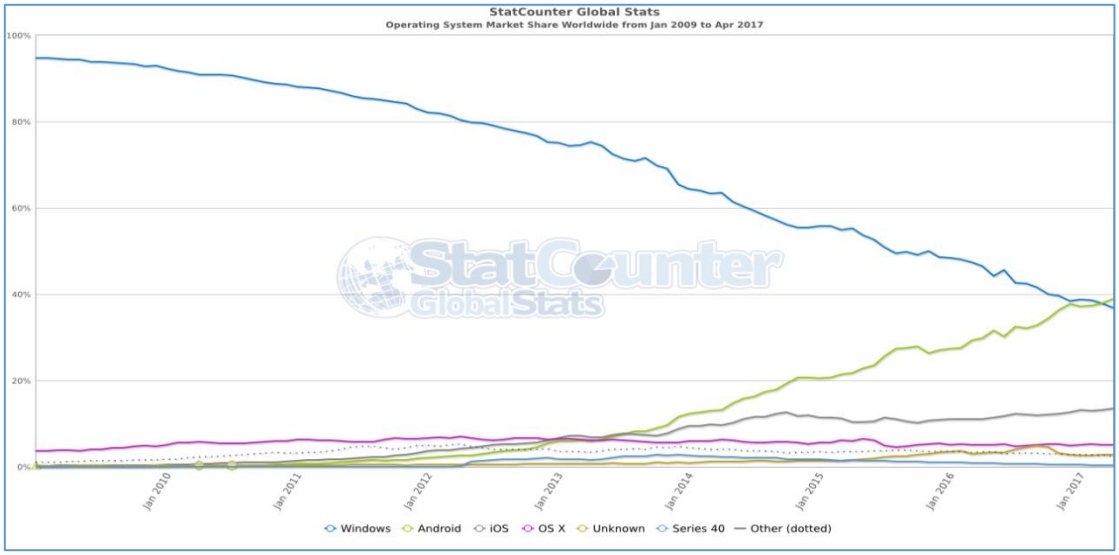
而所謂的 OTT(Over-The-Top)服務，意指服務提供者透過網路技術向用戶提供應用服務(例如聲音、影音與其他類型的媒體內容)，且 OTT 服務主要建構於網路上，不需要特定類型的網路服務提供商(Internet Service Provider，ISP)或是特定的有線電視多系統業者(Multiple-System Operator，MSO)的支持[6]。然而在營運模式上，OTT 業者與內容業者簽約，並透過內容傳遞網路(Content distribution network，CDN)技術把內容透過網際網路傳送至用戶端[7]，也出現很多犯罪者利用 OTT 技術大肆傳遞侵權的內容。

但隨著 OTT 服務正逐漸取代傳統媒體的傳播管道，成為熱門的傳播方式之時，在另一方面的資訊安全危機正悄悄的冒出頭來，大多是硬體設備出產後便停止更新，或開發過程中無妥善的落實隱私保護機制或是使用含有漏洞的作業系統，即 OTT 用戶端多仰賴業者所生產之機上盒讓連接電視或多媒體設備觀看節目，目前來說，機上盒多以 Android 4.0 以上作業系統為主，而蘋果電腦的 APPLE TV 則為另一族群，也有大陸阿里巴巴集團以 Linux 為基礎所研發 YunOS 第三方作業系統，但因為 APP 擴充性及支援性較差，無法廣泛使用，因此本次針對 Android 的 OTT 機上盒進行相關研究，發現普遍存在「舊系統版本資安漏洞」、「無法即時更新並修補漏洞」、「敏感資訊未加密透過網路傳輸」等因素，進而使得駭客有著明顯進攻的目標，也帶來未來嚴重的網路安全威脅。

貳、現行 OTT 發展與技術演進

2.1 OTT 給與行動作業系統新的舞台

近年來行動裝置的盛行，讓使用者越來越青睞 Android 系統，而 2017 年 3 月知名 StatCounter 網站統計 Android 已超過微軟 windows 系統成為全球最盛行的作業系統(如圖一)[5]。除了行動電話的快速發展外，伴隨著電視解析度提高、傳統有線電視類比訊號無法提升高畫質、加速基礎建設頻寬提升等前提因素，國內媒體業者逐漸跟上各國潮流將電視類比訊號轉為數位電視的政策，未來透過網路傳輸將高解析度 1,080p(FULL HD)及 4K 超高解析度(UHD)影音內容透過視訊接收解碼器(俗稱機上盒，Set Top Box, 簡稱 STB)傳輸到民眾家中的 IP-TV 即將展開新的局面，因此開始一波媒體基礎建設新革命，也將重新劃分新的媒體版圖[8]，而這股數位匯流也帶動國內 Over The Top(簡稱 OTT)的風潮，民眾在家中另外購買 OTT 機上盒，透過網路可觀看各種節目，但有別於第四臺業者的機上盒原理，多數節目來自境外，且非全部屬於直播，多透過第三方 APP 來傳送，造成更多造成更多侵權問題。



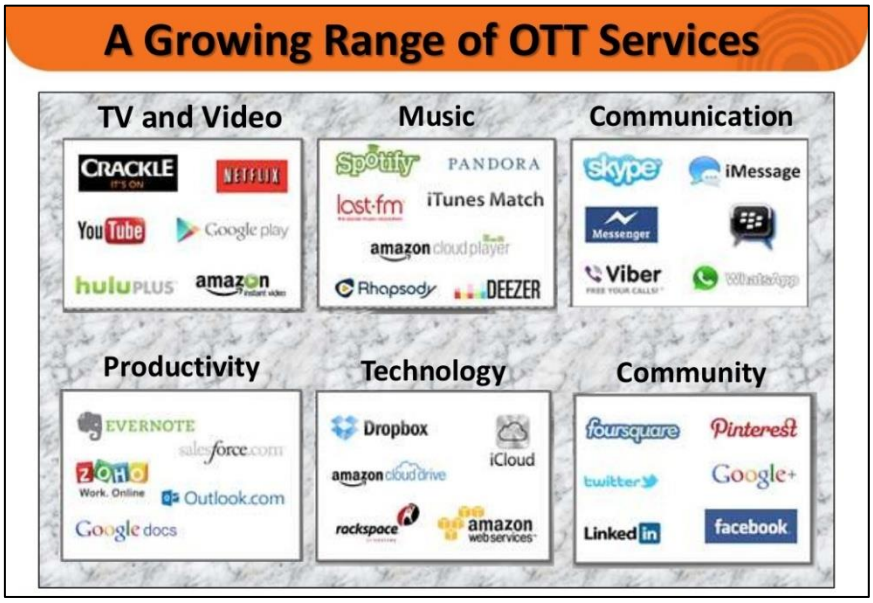
圖一: StatCounter 網站統計全球作業系統發展趨勢

2.2 借助網路技術而生的新興傳播

OTT 的早期發展主要是將內容或服務建置於電信服務上，而不需要電信商的支援，但隨著網路設備急速發展且趨於完善，近年來 OTT 發展成以網路為基礎的服務和內容，向用戶提供多種媒體應用服務，且現在的 OTT 模式只使用 ISP 業者的網路(如中華電信、台灣大哥大、遠傳、亞太)，而服務則由 ISP 業者外的第三方提供，如 Netflix、愛奇藝、YahooTV、KKTV 等。但 ISP 業者也逐漸看到 OTT 的商機，也逐漸布局加入 OTT 的服

務，帶來豐富媒體內容且更為競爭的商業平台。

而 OTT 的崛起已經是不可逆的趨勢產業，它改變了傳統媒體影音技術架構和用戶接收資訊的過程，也改變了用戶接收新知媒體內容的被動方式。透過機上盒及網路輔助可將電視及影像(TV and Video)、音樂(Music)、溝通(Communication)、生產(Productivity)、科技(Technology)、社群(Community)等六種類型傳輸到世界各地[12]



圖二: OTT 服務產業類型

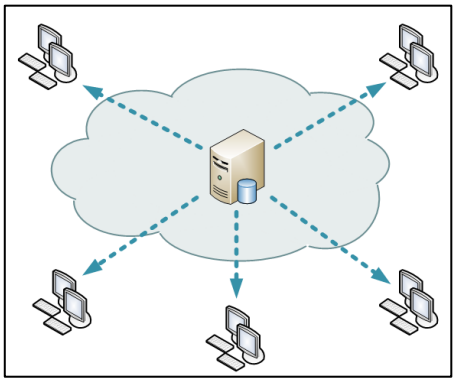
2.3 核心的內容傳遞網路(Content Delivery Network，CDN)

內容傳遞網路 CDN 是主要作為網路流量或頻寬的分流服務，且利用最靠近每一用戶的伺服器，更快速地將媒體內容(如音樂、圖片、影音)、網路應用程式、檔案快速傳遞給用戶，來提供高效能、可擴充性及低成本的網路服務和內容傳遞給用戶。CDN 的技術對於 OTT 的服務是不可獲缺的分流技術服務，因現今網路媒體的快速產生與傳遞過程中，分流技術將影音媒體內容快速導入至用戶接收的平台，以讓用戶第一手接收到訊息且不會產生媒體串流延遲的現象，對於 OTT 服務來說 CDN 是相當重要的技術環節。

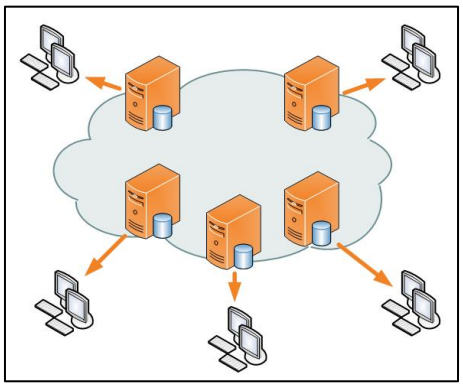
以 CDN 架構為例(如圖四)，當 OTT 服務內容傳輸至用戶端時，經由 CDN 技術，選擇最靠近用戶的伺服器或將網路頻寬作一個分流服務，以達到負載平衡之效果，而不會造成最終用戶接收資料的遲緩，而相較於(如圖三)單一傳輸架構，則容易造成中央伺服器負載過重或同一時間要處理大量用戶請求而使的效能降低，進而影響大量用戶[10]；在 OTT 的服務中，CDN 的技術傳輸是相當重要且不可或缺的角色，假如透過 OTT 機上盒所傳輸的非法侵權影片，雖然影片來源在境外(如大陸土豆、優酷、樂視等)，但是透過境內的 CDN 主機結合快取技術，仍可順暢瀏覽影片內容，另外如犯罪者利用世界各

國的 CDN 主機，傳輸非法內容或者利用某些具備資安弱點的 Android 機上盒，成為新的攻擊武器，則犯罪將更無遠弗屆，讓執法單位追查網路犯罪上形成更大困難。

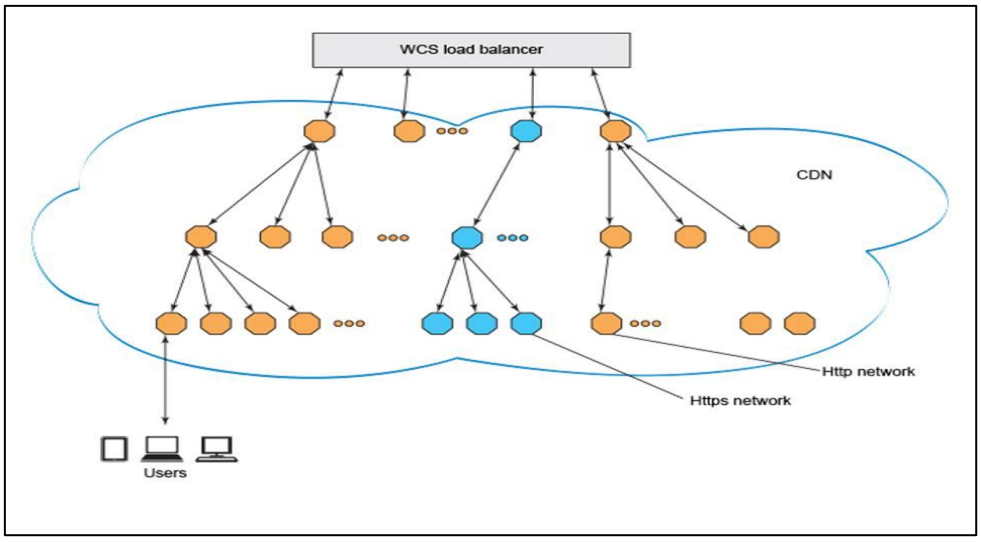
值得探討的是，單一機上盒無法完成，CDN 主機系統(如圖五)包含負載均衡設備、內容 Cache 伺服器、共享存儲等技術，而國際間公有雲收費服務則以 Akami 公司提供 CDN 服務最典型，但近年來私有 CDN 陸續出現，藉由 Open Source 的 CDN 源碼取得，民眾也者可以自行架構，也彼此合作共享資源，因此日後這類犯罪型態也成為重要的數位鑑識範疇。



圖三: 單一傳輸架構



圖四: CDN 傳輸架構



圖五: CDN 運用 http 的技術進行負載分配機制

參、國內外文獻探討與作法比較

3.1 數位鑑識的準則不斷因應科技演進而修正

早在 1910 年法國學者 Edmond Locard(路卡)所提出的 Locard's Exchange Principle(路卡交換原理)就提出凡接觸就會有殘留的物質交換，也就是凡走過必留下痕跡的鑑識初論[13]，因此近年來電腦、數位裝備、穿戴裝置及未來的物聯網均可從相關數位證據中找到活動過的蛛絲馬跡，當然也包含犯罪的痕跡，因此後續在 2006 年美國國家標準技術研究院（National Institute of Standards and Technology，簡稱 NIST），所出版之事件鑑識技巧指南（Guide to Integrating Forensic Techniques into Incident Response，NIST-SP-800-86）[3]，提到幾個電腦鑑識面臨的重要步驟 1.Collection (收集)、2.Examination (檢驗)、3.Analysis(分析)、4.Reporting(呈現)。

後來 2012 年 ISO/IEC 27037 提及數位鑑識人員或數位證據專家為了確保數位證據的完整性與可靠性，提出類似 NIST 所提出的程序，以識別（Identification）、收集（Collection）、獲取（Acquisition）及保存（Preservation）等程序來使數位證據在法院上具備證據能力，且必須遵守下列 4 項原則:1.將對數位證據設備以及數位證據的改變減到最小。2.解釋所有變更並記錄處理數位證據的動作（解釋證據的可靠性）。3.遵循當地對於證據的法律規定 4. 數位鑑識人員或數位證據專家不應採取超出能力的行動[13]，而這些原則多針對電腦本身的相關數位鑑識原理而無牴觸，但初期數位鑑識多在電腦設備以及各種儲存媒體與數位設備進行還原或解析，並在法院上展示出分析結果，近年來軟硬體多樣化，非單一原則可適用所有數位設備鑑識，因此需要與時俱進，尤其對行動或嵌入式系統(Embedded System）裝置要有獨特數位鑑識原則[4]。

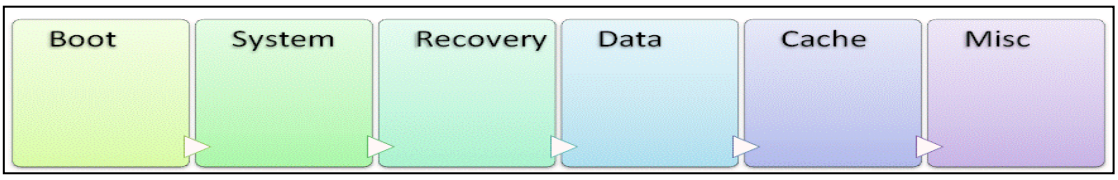
3.2 援用行動裝置的數位鑑識作法

美國國家標準技術研究院在 2014 年公布行動裝置鑑識準則（Guidelines of Mobile Device Forensics，NIST-SP-800-101 Revision 1），這準則中介紹行動裝置特性、處理流程及方式等，其中在檢驗、分析因受限於鑑識工具所能提供的擷取方式，因此在提出有別於電腦的鑑識方法，採取直接連接進行取證，甚至可選擇無線或其他破壞性方式進行，但必須初步評估其風險與影響，所以在不同案類有不同的取證重點，且不影響取證關鍵證據之前提下，可適度修改取證方式，但是取證人員應將取證過程詳細紀錄並負有舉證責任，並在報告中評估鑑識方法可行性之說明。

因此，對於與行動裝置一樣屬 Android 作業系統之 OTT 機上盒，除了透過拍攝證物本身照片直接蒐集證據外，目前鑑識採集的方式可以主要以為實體採集(Physical Acquisition)與邏輯採集(Logical Acquisition)等 2 種為主要[14]，目前大多數 Android 系統設備鑑識軟體都是採用邏輯採集的方式，需將鑑識軟體安裝至載具端方能進行採集動作，因此必須與電腦鑑識作為分野[2]。

3.3 邏輯採證取得最高權限不影響主要存放證據磁區

目前OTT盒子要取得根目錄權限就必需要取得Root控制權，如同Windows系統的Administrator帳號，若無Root權限是無法存取，所以必須要對Android系統進行提權動作，常見方式就是透過刷機方式進行，以上取證方式對於關鍵證據本身並無改變，相較電腦系統(如Windows)將作業系統磁區與資料磁區整合在一區塊，對於系統磁區進行動作是必影響整體證據完整性；反觀Android系統所分配磁區而言，有發生改變的是在系統區（System）與還原區（Recovery），對於雙方所爭論的使用者資料區（Data）是不發生影響或改變，如圖六所示[8]。



圖六: Android 各獨立磁區分配狀況

肆、OTT 盒子數位鑑識框架與個案實作

目前相關文獻對於 OTT 機上盒並無一致性數位鑑識作法，本次將採用行動裝置數位鑑識流程，由於實體採集(Physical Acquisition)實務上並不普遍使用，且目前無工具可從晶片實體層透以物理性汲取內容，故不在本次實驗使用，僅針對取得 Anaroid 機上盒之根目錄內標的物進行邏輯採集(Logical Acquisition)，而本案 OTT 機上盒傳輸內容疑似侵權數位串流內容，對於違法著作權法等事證亦透過動態封包解讀了解運作原理，並對於應用 APP 進行靜態分析，重組伺服主機與終端角色，另外對於 OTT 機上盒因為硬體架構限制，無法升級軟體、韌體導致可能產生的資安問題亦進行討論並分析。

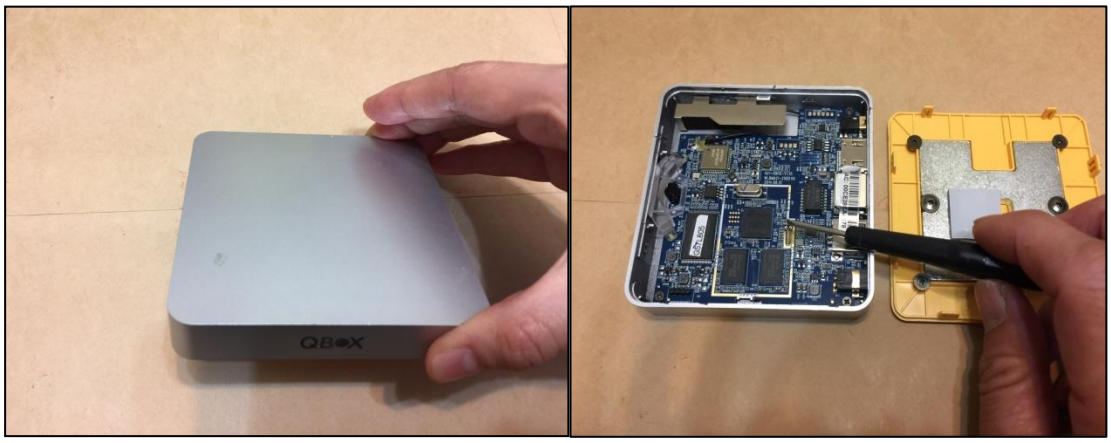
4.1 收集:採取與電腦數位鑑識一致性框架，並以最小變動為原則

數位鑑識依照原則一致性，仍依照 NIST 800-86 所律訂的收集、檢驗、分析、呈現等 4 大步驟來擬定初步的框架，而參考 NIST 800-101 Revision 1 的前提下，會在收集階段針對 OTT 機上盒進行取得 ROOT 的程序，然後取得目錄權限後針對內容進行邏輯數位搜集(如圖七)。

圖七: 本文擬訂之 OTT 機上盒數位鑑識框架

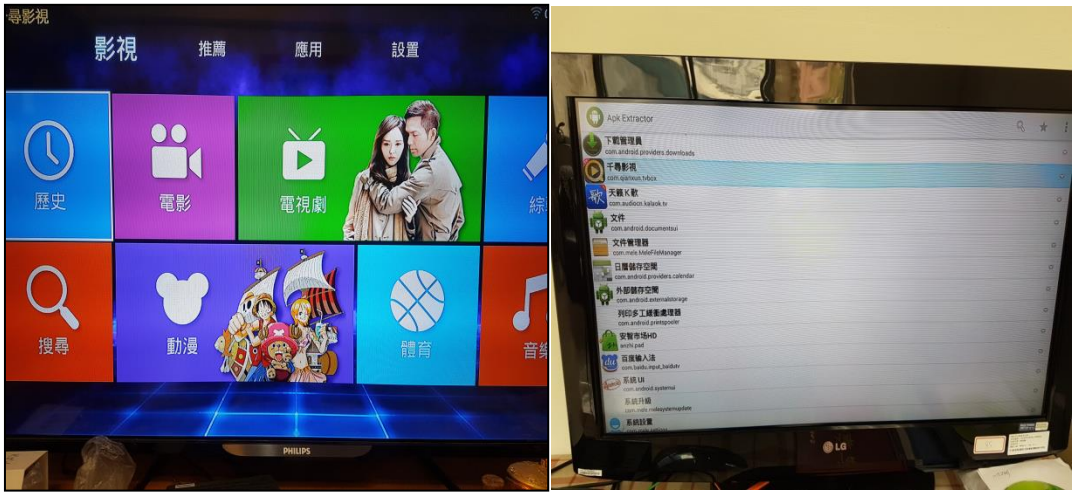
4.2 檢驗:證物進行採集並建立驗證程序，以強化具備不可否認性

從 OTT 機上盒拆開機板外殼，從裡面可以看到千尋盒子 II 係採用晨晶 Amlogic 出產的 S805 編號核心(如圖八)，與近期熱門的小米盒子增強版(2g)係相同核心，其他廠牌(如華為榮耀盒子等)有採用瑞芯、海思、聯發科等廠商研發之核心，但各機上盒仍有所不同，但是可以確認的是這些核心晶片與整體輸出影像品質有關，因此一臺不到新臺幣五千多元的機上盒，很難有升級的機會。



圖八: 本次實驗之 OTT 機上盒

開啟電源後如執行之後會出現圖九的畫面，顯示並非原生整合入系統之的軟體，透過灌載 apk-extractor.apk 的工具針對重要的 app 進行採集，通常這類工具可以預先下載於 USB 碟中，然後灌載於 OTT 機上盒中再進行使用，可以不更動內容狀況下取出 APK 程式。

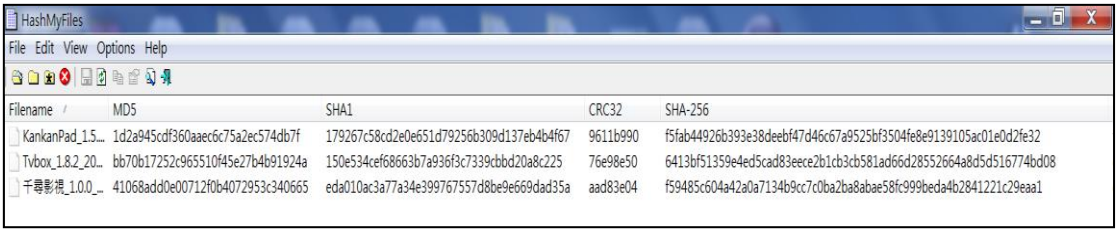


圖九: 本次實驗之 OTT 機上盒開啟後畫面

經發現 OTT 機上盒第一次初始開啟時，僅留存一個 APP，必須由使用者自行安裝，本次在千尋盒子上發現一個檔名為” 千尋影視_1.0.0_1.apk”，經前往該千尋 OTT 業者網頁上下載相同 APK，本次發現該網站有”安卓 pad 版本”及”TV/盒子版本”2 個 apk 版本，下載後名稱為 KankanPad_1.5.1_20170208.apk(pad 版)及 Tvbox_1.8.2_20170426.apk(TV BOX 版)(如圖十)，經以 Nirsoft 公司 hashmyfile 進行雜湊(hash)函數比對，發現從原始網站(https://1kxun.mobi/download/index)下載的 pad 版程式 (SHA1:179267c58cd2e0e651d79256b309d137eb4b4f67)及 TV BOX 版

(SHA1:150e534cef68663b7a936f3c7339cbbd20a8c225)之 APK 檔案，與從取得 OTT 機上盒取得之檔案(SHA1: eda010ac3a77a34e399767557d8be9e669dad35a)驗證 hash 值並不相同(如圖十一)，顯然該機上盒裡面的 APK 應屬客製化，特別針對機上盒所製作之程式，與網路或行動裝置商店所下載的版本並不相同。

圖十: 千尋網站下載的 APP 程式(分為 pad 版及 TV 版)位置

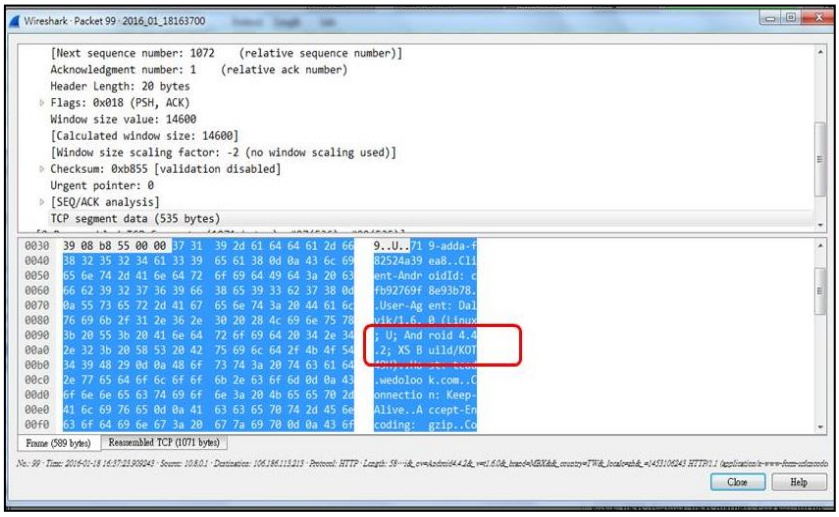


圖十一: 利用 hashmyfile 工具比對千尋網站與 OTT 盒子的檔案是否相同 Hash

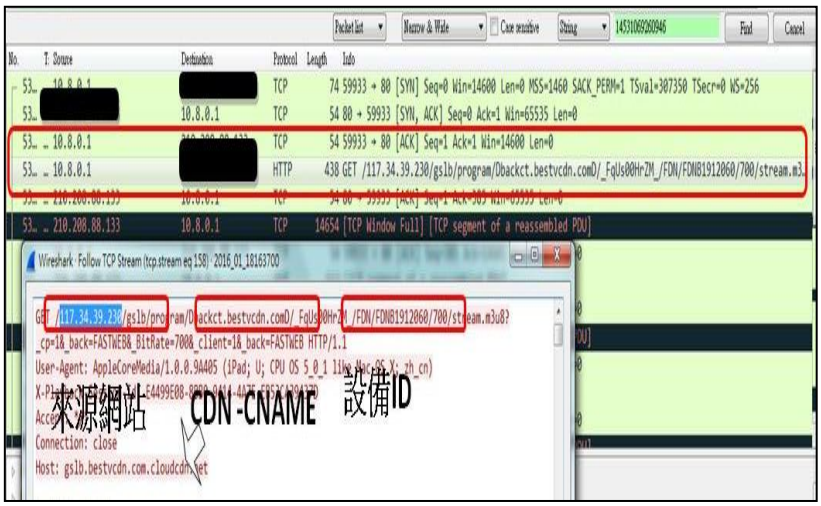
4.3 分析:針對疑似有問題 APK 動、靜態分析，判斷問題所在

這裡所運用的分析，除了針對取得 Root 權限的根目錄進行分析外，亦透過相關稽核紀錄來還原真相，另外我們也透過直接運作機上盒進行封包側錄來找出問題所在，這裡通常進行網路行為活動的偵測或監看(如封包側錄)，透過分析 TCP/IP 的原理分析脈絡，我們稱之為動態分析(Dynamic Analysis)，本案解析 OTT 機上盒內之"千尋影視_1.0.0_1.apk"安裝後之 APP 的封包，發現通訊開始前機上盒會送出作業系統等資訊，如 Android-ID 及作業系統 4.4.2 等版本資訊(如圖十二)，而缺點在於可能因為每次更新或網路傳輸，導致原證物內容檔案或程式有更新、毀(汙)損、覆蓋等風險，而透過封包可以瞭解 CDN 係以 http 為主的傳輸技術，另外從 Get 網址列理面可以看出來源網址、CDN-CNAME 網址、OTT 設備編號等資訊，可釐清網路通訊行為；而封包內容之 URL Get 資訊僅交代訊息來源，如想知道內容傳輸從哪個 IP 傳遞，在 WireShark 讀取封包的格式

中，從傳輸兩端(Source IP v.s Destination IP)IP 則可直接判定來源，可以找出在國內存有內容快取之真實主機(如圖十三)。

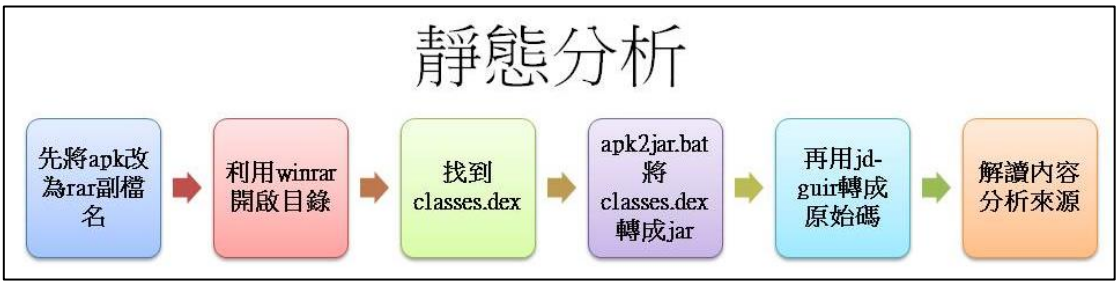


圖十二: 封包中送出的作業系統資訊



圖十三: 封包裡面送出去的來源網站及 CDN 網址資訊

另外一種反組譯安裝在機上盒 APP(通常也可針對惡意 APP 程式)，即透過程式碼追查找出關鍵來源或問題，不需要運作系統或程式本身則取得結果者，稱之為靜態分析(Static Analysis)，這裡會將取得的 APK 先轉為 RAR 壓縮包，然後找到 clesses.dex，再利用 apk2jar 工具將該程式轉成 java 的源碼來進行解讀(圖十四)，但是惟一缺點無法針對運作後產生的行為來實際分析，如實際串流內容或記憶體運作狀況進行瞭解，但如對於程式撰寫有經驗的偵查人員可以瞭解整體程式架構及運作原理，將有效提供作相關分析，以利後續事實佐證。從圖十五可見透過 APK 反組譯可以瞭解(圖十三)串流封包時透過 Http Get 指令所生成之編碼過程與變數，可輔佐動態分析比對網址列語法進行指令分析，以剖繪犯罪樣態行為。



圖十四: 靜態分析反組譯方法

圖十五: 靜態分析傳輸的格式與連結的網域名稱

4.4 呈現:應有具體報告製作及無偏差的結果

對於鑑識結果應歸納成一致性結果，並產出報告(如圖十六)，交由類似經驗的幹部審視作法有無偏差，且製作報告者應該具備一定專業訓練或實務經驗，避免類似過度主觀因素介入，而由於目前對於 Android 的數位鑑識均針對手機裝置有特定工具，如 XRY 或 Cellebrite 等設備，反觀 OTT 機上盒無可使用之工具可供運用，目前僅能針對整體處理過程透過一致性標準作業流程(SOP)作法、鑑識人員專業及結合多種方法(動態、靜態分析)佐證，來強化取得證據之客觀性，並且整體過程應該全程錄影，以利日後檢驗。

圖十六: 數位勘察報告呈現

伍、未來問題與數位鑑識方向

OTT 機上盒不僅衍生新的數位鑑識挑戰，對於資安也是非常大的威脅，趨勢科技曾發現駭客會透過惡意網站散播含有 ANDROIDOS_ROOTSTV.A 惡意程式的應用程式，使用 CVE-2014-7911 這個 Android 系統存在已久的舊漏洞(Lollipop 5.0 之前的版本：從 Cupcake 1.5 至 Kitkat 4.4W.2)進行攻擊，藉此取得裝置的操控權限，可肆意下載其他的惡意應用程式，或是成為攻擊其他家中連網裝置的跳板，日前尚有為數不少的 Android 設備存在漏洞，除了 OTT 機上盒外，很多智慧型電視品牌包括：長虹 (Changhong)、康佳 (Konka)、小米 (Mi)、Philips、Panasonic 以及 Sharp 都暴露在風險之中[9]。

此外，從 Cvedetails.com 網站統計 2009 年以來迄今，Android 系統在公開弱點資料庫（CVE, Common Vulnerabilities and Exposures）就多達 946 個漏洞，其中獲取權限(Gain Privileges)最多、其次代碼執行(Code Execution)[14]，由於 OTT 機上盒成本低廉，晶片廠商多不願花費成本升級，因此許多 Android 機上盒淪為資安孤兒，加上機上盒多持續連線網路或者直接使用固定網際網路 IP，每成為最容易被鎖定的受害對象，未來如無因應作法，恐成為重大資安威脅(圖十七)，因此對於相關事件處理，也本文也提出類似的比照侵權內容之資安數位鑑識架構(圖十八)，可透過檢測與分析找出資安犯罪問題，防止更多威脅出現。

Vulnerability Trends Over Time

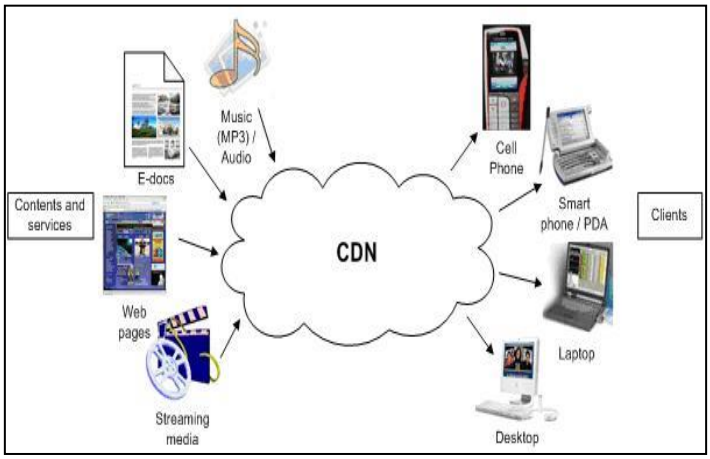
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2009	5	3								1					
2010	1	1	1												
2011	9	1	1		1					3	2	3			
2012	8	5	4	2							1				1
2013	7	1	2	2	2					1	1	3			
2014	13	2	4	1		1				1	2	2			1
2015	125	56	70	63	46					20	19	17			
2016	523	104	73	92	38					48	99	250			
2017	255	38	134	36	25					24	42	34			
Total	946	211	289	196	112	1				98	166	309			2
% Of All		22.3	30.5	20.7	11.8	0.1	0.0	0.0	0.0	10.4	17.5	32.7	0.0	0.0	

圖十七: Cvedetails.com 網站統計 2009 年以來迄今 Android 的漏洞

圖十八: 針對 TV box 資安檢測作法流程圖

陸、結語

對於執法人員來講 OTT 所運用之 CDN 技術，近年來民間廣泛運用，而在刑案上卻是少見，但漸漸地物聯網上逐漸被廣泛使用(如圖十九)，但 OTT 的犯罪對於整體執法工作不再是環繞在單一機上盒的內容傳輸或資安問題，未來 CDN 伺服主機遭到入侵進而控制 OTT 機上盒，可能衍生許多跳板、僵屍網路(Bot Net)、網路攻擊(DDoS)等事件，本次僅針對 OTT(Android)機上盒研擬初步鑑定程序，以提供日後類似資安事件處理或網路犯罪追查參考。



圖十九: IOT 物聯網與 CDN 結合

參考文獻

[1] ISO 27037, “Guidelines for identification, collection, acquisition and preservation of digital evidence,” Retrieved from http://www.iso.org/iso/cat-alogue_detail?csnumber=44381, 2014.

[2] W. Jansen and R. Ayers, “An overview andJune analysis of PDA forensic tools,” *Digital Investigation*, Volume 2, Issue 2, pp. 120-132, June 2005.

[3] K. Kent, S. Chevalier, T. Grance and H. Dang, “Guide to Integrating Forensic Techniques into Incident Response,” *NIST Special Publication* 800-86, National Institute of Standards and Technology, Gaithersburg, Maryland, 2006.

[4] R. McKemmish, “What is forensic computing?,” Australian Institute of Criminology, 1999.

[5] http://gs.statcounter.com/os-market-share#monthly-200901-201704 (2017/04).

[6] http://iview.twnic.net.tw/?page_id=303

[7] http://www.ncc.gov.tw/chinese/files/13102/1245_30727_131023_4.pdf (2013/10/22).

[8] http://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&sn_f=35854 (105/06/29).
[9] https://blog.trendmicro.com.tw/?p=16027 (2016/1/8).
[10] https://en.wikipedia.org/wiki/Content_delivery_network (2017/6/18).
[11] https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224
[12] https://www.slideshare.net/MylesFreedman/sacf-impact-of-ott-services (2016/7/25).
[13] 王旭正、林祝興、左瑞麟合著，*科技犯罪安全之數位鑑識:證據力與行動智慧應用*，博碩文化出版，2013。
[14] 陳詰昌，“數位鑑識「原件不可變動原則」之適用—由行動裝置鑑識與電腦鑑識差異探討”，*司法新聲*，第 119 期，法務部司法官學院，7 月刊載，p42-55，2016。