應用程式雲客戶端資料之鑑識

鄧思源[1*]、陳受湛、劉秉昕[2]
[1]中央警察大學鑑識科學研究所
法務部調查局台北市調查處
[2]法務部調查局資通安全處
[1]mjib.teng@gmail.com、[2]m43074@mjib.gov.tw

摘要

目前雲端運算技術發展日益成熟，相關服務更是不斷推陳出新，由軟體即服務(SaaS)雲端服務架構下又衍生出如 AaaS(Apps as a Service)、aPaaS(Application Platform as a Service)或 MAaaS(Mobile Applications as a Service) 等不同之雲端服務架構，讓使用者隨時隨地可以使用任何數位裝置上的瀏覽器透過網際網路連接即可使用這些雲端服務上的應用程式，目前較知名 SaaS 供應商所提供的應用程式雲服務如 GoogleApps、Apple iCloud、MicroSoft Office 365 及 Salesforce App Cloud 等，但可使用之應用程式的種類大部分都限縮在辦公室應用程式或雲端儲存服務，軟體數量亦有所不足，因此目前有部分雲端服務業者推出類似 Google Docs 及微軟 Office 365 等雲端應用程式概念的應用程式雲，強調在任何地方不論使用任何平台都可透過網際網路執行任何桌面程式(run application anywhere or online)，讓使用者可從雲端服務提供者以隨用隨付制為基礎免費或付費購買、租用應用程式服務。所有的硬體基礎結構、中介軟體、應用程式軟體以及應用程式資料皆位於雲端服務提供者的資料中心。由於應用程式雲具有使用便利、機動性高、隱匿及不易確認等特性，因此在可見的未來，應用程式雲很有可能成為不法犯罪份子用於規避犯罪調查的選項之一，因此對於應用程式雲架構與相關服務之數位調查及如何蒐集與鑑識使用此類雲端服務客戶端數位證據，實有必要加以研究，本篇論文將針對市面上較具代表性的 Cameyo、rollapp 及 Turbo 等 3 種應用程式雲進行實驗與分析，期提供可參考利用的應用程式雲客戶端之數位證據保全、蒐集與鑑識的步驟與程序，以協助數位鑑識實務操作人員在處理與應用程式雲有關之鑑定案件時，有一可供參考之鑑識方法。

關鍵詞: 數位證據、SaaS、AaaS、應用程式雲、應用程式虛擬化、數位鑑識、反鑑識。

* 通訊作者 (Corresponding author)

A Forensic Analysis of Application Cloud Service in Client Data

Teng,Szu-Yaun[1†]、Chen,Sou-Chan、Liu,Ping-Hsin[2]
Investigation Bureau, Ministry of Justice
[1]mjib.teng@gmail.com、[2]m43074@mjib.gov.tw

Abstract

At present, the development of cloud computing technology is becoming mature, and the related services are innovating. A similar cloud services architecture such as AaaS (Apps as a Service), aPaaS (Application Platform as a Service), or MAaaS (Mobile Applications as a Service) is derived from the Software Services (SaaS) cloud service architecture, so that users can use any browser on any digital device to connect to these applications by the Internet, which is now available from more well-known SaaS vendors of the application cloud services such as GoogleApps, Apple iCloud, MicroSoft Office 365 and Salesforce App Cloud. Most of the types of apps that can be used are limited to office applications or cloud storage services, and the number of software is inadequate. Some cloud service providers launched applications such as Google Docs and Microsoft Office 365 and other type of application cloud, emphasizing to use any platform to run any application anywhere, so that the user can purchase or rent the application from the cloud service provider on a per-use basis. All hardware infrastructures, mediation software, app software, and application data are located in the cloud service provider's data center. Because the application cloud service has the advantages of ease of use, high mobility, hidden and difficult to confirm, the application cloud service is likely to be one of the options for criminals to avoid crime investigations in the foreseeable future, Therefore, it is necessary to study the digital data of the cloud service client and how to collect and authenticate the application of cloud architecture and related services. This paper will experiment and analyze three application clouds service, such as Cameyo, rollapp and Turbo, and provide the steps and procedures for the preservation, collection and identification of digital evidence that can be used by the application cloud service client data to assist in the implementation of digital forensic practitioners have a reference method when encountered the application cloud service case.

Keywords: Digital Evidence, SaaS, AaaS, Application Cloud Service, Application Virtualization, Digital Forensics, Anti-forensics

† 通訊作者 (Corresponding author)

壹、 前言

目前雲端及虛擬化運算技術發展與服務不斷推陳出新，美國國家標準局(NIST)認為雲端運算有「依需求自助服務」、「廣泛網路存取」、「動態資源池」、「快速伸縮性」及「可計量服務」等 5 大特色，並提供「基礎架構即服務」(IaaS)、「平台即服務」(PaaS) 及「軟體即服務」(SaaS)等 3 種服務模式，以及有「私有雲」、「社群雲」、「公有雲」及「混合雲」等 4 種佈署模型。其中，IaaS 係指將運算、儲存、網路及系統等軟硬體資源轉化為標準化服務，以提供企業或使用者使用。PaaS 則為在雲端基礎設施之上，業者提供整合的 API 開發平台，以撰寫程式與服務支援雲端應用的不同功能，可以讓客戶的應用程式放在平台代管，以節省成本。SaaS 則為透過雲端應用程式來提供各種服務，使用者不需要下載或安裝任何程式，就可以直接透過瀏覽器存取雲端應用程式所提供的功能與服務[6]，例如 Google 所提供 的 Google MAP、Google Docs 及 Gmail 電子郵件服務、WhatsApp、LINE 及 WeChat 等網頁版即時通訊軟體服務、以及 Facebook、Twitter 等社群網路服務。依據美國國家標準技術研究所(NIST)雲端鑑識科學工作小組於雲端鑑識科學的挑戰報告中定義所謂「雲端鑑識科學乃是應用科學的原理、技術的執行及可被證明的方法，藉由數位證據的識別、蒐集、保存、審查、解譯與報告，重建過往所發生的雲端事件」[8]，但目前雲端鑑識實務上並無可資應用的標準指南，因此針對不同雲端服務模式之鑑識作業程序需求，雲端安全聯盟參照國際標準化組織和國際電工委員會於 2012 年 10 月 15 日聯合公布的 ISO/IEC 27037:2012 標準[5]，提出「Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing」指引[3]，以解決在實體資訊環境中，如何將傳統的數位鑑識作業程序套用在雲端服務的環境中之議題，針對 3 種雲端服務之識別、收集、獲得與保存等不同階段之作業程序，亦提出鑑識與注意事項。

雲端安全聯盟認為 SaaS 雲端服務供應商(CSP)在雲端鑑識的過程中，必須提供給客戶或司法調查機關的紀錄資料應包括：(a)網頁伺服器日誌；(b)應用伺服器日誌；(c)資料庫日誌；(d)客戶端作業系統日誌；(e)主控端存取日誌；(f)虛擬平台日誌及 SaaS 入口網站日誌；(g)網路封包資料；(h)帳單紀錄等資料。由於雲端鑑識面臨無法實體接觸、需依靠雲端服務供應商提供日誌、日誌分層存放、鑑識工具無法支援、雲端服務多租戶情況、跨境執行鑑識法律問題、客戶租約問題等困境，在鑑識過程中供應商應提供資料很多都無法完整取得，因此如何從使用者所在的客戶端中識別、蒐集與擷取有關 SaaS 雲端服務相關資料，成為應用程式雲鑑識作業所需面對的挑戰。由於應用程式雲端服務具有使用便利、機動性高、易於隱匿等特性，因此在犯罪案件的偵查或鑑識作業中，往往不易確認其使用方式與資料來源，如何透過分析客戶端在使用應用式雲所產生的各種檔案、數位紀錄與殘留數位痕跡，以瞭解可能使用之犯罪手法與工具，甚至有機會可以取得案關資料檔案等數位證據。

目前有部分雲端服務業者推出類似 Google Docs 及微軟 Office 365 等雲端應用程式概念的應用程式雲，強調在任何地方不論使用任何作業平台都可透過網際網路執行任何

桌面程式(run application anywhere or online)，讓使用者可從雲端服務提供者以隨用隨付制為基礎免費或付費購買、租用應用程式服務。所有的硬體基礎結構、中介軟體、應用程式軟體以及應用程式資料皆位於雲端服務提供者的資料中心。由於應用程式雲具有使用便利、機動性高及隱匿及不易確認等特性，因此在可見的未來，應用程式雲很有可能成為不法犯罪份子用於規避犯罪調查的選項之一，因此對於應用程式雲架構與相關服務之數位調查及如何蒐集與鑑識使用此類雲端服務客戶端數位證據，實有必要加以研究，本篇論文將針對市面上較具代表性的 Cameyo、rollapp 及 Turbo 等 3 種應用程式雲進行實驗與分析，期提供可參考利用的應用程式雲客戶端之數位證據保全、蒐集與鑑識的步驟與程序，以協助數位鑑識實務操作人員在處理與應用程式雲有關之鑑定案件時，有一可供參考之鑑識方法。

貳、 文獻探討

目前有關 SaaS 服務之學術研究主要是在 SaaS 雲端環境中，如何識別、蒐集與擷取及保存數位證據。巴西學者 José Antonio 及 Marcelo Beltrão 等人[7]以 SaaS、PaaS 及 IaaS 等 3 種服務模式中針對識別、保存、蒐集及檢驗與分析程序，提出如何由 CSP 取得相關數位證據之實務建議。但是德國學者 Birk[2]認為在 SaaS 及 PaaS 環境下，對於系統狀態及記錄檔之取得顯有困難，因為此二種服務模式對於客戶端之存取有較多限制，相對而言，IaaS 模式之客戶端反而較能取得更多數位證據。馬來西亞學者 Damshenas[4]建議在 SaaS 環境中從客戶端去識別潛藏的數位證據是相當重要的，因此如何設計與設定內建應用程式紀錄功能，便於去記錄如使用者通訊資料等潛藏數位證據是需要的。但是這些紀錄並無法說明這些應用程式執行的細節。目前對於應用程式雲客戶端資料之研究，並未相關文獻可供參考。

應用程式雲作為本研究之研究標的，會有實體檔案的存取需求，而目前分別利用特定之雲端硬碟服務及瀏覽器作為檔案上傳及下載之儲存空間，有關由 SaaS 衍伸出的 StaaS 雲端服務之鑑識研究，目前學術上有許多文獻可供參考，例如澳洲學者 D. Martini, and K.-K. R. Choo 等人[9]以儲存、上傳及存取 Dropbox、Microsoft SkyDrive 及 Google Drive 等雲端硬碟資料時，對客戶端紀錄軟體、預執行檔(prefetch files)、快捷檔(link file)、網路封包及記憶體擷取等可能潛藏的服務進行識別，來探討客戶端雲端數位證據留存資料；印尼學者 Amirullah Amirullah 等人[1]針對 DropBox, Copy and CloudMe 等雲端硬碟服務在微軟 Windows 10 作業系統上以雲端硬碟客戶端應用程式、MicroSoft Edge 瀏覽器及 Mozilla Firefox 瀏覽器利用檔案上傳及刪除功能，來探討檔案系統及記憶體中資料留存之情形。

上述有關 StaaS 雲端服務之研究並未觸及應用程式雲可能留存之潛藏數位證據。目前市面上已經出現數種提供應用程式雲之線上服務，透過這些網站，使用者可在不同作業平台上使用瀏覽器即可執行所需之應用程式，而無須真正安裝應用程式在實體裝置中

(如電腦及行動裝置)，因此不管是案件調查人員或是數位鑑識人員對於目前所流行的應用程式雲服務需有相當之認知，如此在接觸與處理該類 SaaS 雲端服務數位證據時，才不會使鑑識作業程序有所疏漏，錯失重要數位證據。接下來將針對 Cameyo、rollapp 及 Turbo 等 3 種應用程式雲，以 Google Chrome、Mozilla Firefox 及 MicroSoft Edge 等 3 種瀏覽器進行相關實驗與觀察，歸納及整理可供之鑑識特徵值，使數位鑑識人員在鑑識此類物證時，有一可供參考之數位鑑識程序與方法。

2.1 Cameyo 應用程式雲簡介

Cameyo 公司的應用程式虛擬化產品在 2010 年開始推出，Cameyo 公司亦是最早將應用程式虛擬化、雲端儲存系統及 HTML5 連結在一起的先驅者之一，強調應用程式虛擬化能提供高擴展性，並降低資訊成本，Cameyo 透過離線打包程式(Cameyo.exe)將欲執行的應用程式，輸出為一個獨立的 EXE 執行檔，檔案中包括虛擬化引擎和原始軟體的檔案及登錄檔，可以直接在微軟視窗作業系統平台上執行，也可將獨立的執行檔上傳到 Cameyo 所提供的 SaaS 應用程式雲，並以 HTML5 的方式發佈，使用者即可透過瀏覽器執行虛擬應用程式[12]。Cameyo 應用程式雲強調可以讓使用者以線上或離線方式來使用虛擬應用程式，亦即使用者在線上無須下載程式就可在應用程式雲中執行任何應用程式，如果使用者想在目標機器上離線執行虛擬應用程式，亦可從應用程式雲下載使用。另外 Cameyo 應用程式雲整合 Dropbox 及 Google 雲端硬碟，讓使用者從應用程式雲上傳或下載資料至雲端硬碟中。目前 Cameyo 應用程式雲亦可在 Chromebook，Linux，Android，Mac iOS 等非視窗作業系統平台上執行，具有跨平台能力。

2.2 rollapp 應用程式雲簡介

rollApp 建構了一個線上應用程式虛擬化平台，允許在任何連網設備上透過瀏覽器執行任何應用程式。在 rollApp 應用程式運行時的行為方式與本地安裝相同。只需點擊一下即可從應用程式雲點選播放數百個應用程式。另外 Rollapp 應用程式雲同時整合 Google Drive、Dropbox、OneDrive 及 Box 等雲端硬碟，使用者可以從任何設備同時執行 3 個應用程式，並在上述 4 種雲端硬碟中存取、編輯與保存相關文件[10]。

2.3 Turbo 應用程式雲簡介

Turbo 允許使用者將應用程式及其相依項目打包成一個稱為“容器”的輕量級隔離虛擬環境檔。使用者可以在任何安裝了 Turbo 應用程式的微軟視窗作業系統平台上執行已經容器化的應用程式，不論底層硬體基礎架構如何改變，都可以執行。Turbo 容器建構在 Turbo 虛擬機之上，在 Turbo 虛擬機中執行的應用程式與由 SVM 提供的虛擬化檔案系統，註冊表，網路和執行緒環境互動，而不是直接與主機作業系統互動。

Turbo VM 與諸如 Microsoft Virtual PC 和 VMWare 之類的硬體虛擬化系統或 Hyper-V 等虛擬機管理程式系統不同，Turbo VM 在執行堆疊的基礎上運行，並將應用程式執行所需的特定作業系統功能虛擬化。這使得虛擬化應用程式能夠有效地運行，具有與本地執行檔相同的特性。

Turbo 的傳統應用程式虛擬化工具叫做 Turbo Studio。與其他應用程式虛擬化系統一樣，Turbo Studio 為基於虛擬應用程式配置的「靜態」模型。通過抓取實體系統的快照建立虛擬機狀態。這類似於此類別中的其他產品（如 Microsoft App-V 和 VMware ThinApp）所使用的流程。但這種方法的主要缺點是需要使用乾淨的實體或虛擬機作為「抓取」的目標。

Turbo 容器另提供"動態"配置模型，使用者可以看到一個乾淨的容器基本映像，讓用戶在該容器內安裝，配置和執行應用程式。與傳統的應用程式虛擬化模型相比，容器模型提供了顯著的優勢，因為無需建立虛擬環境即可將機器還原到啟始狀態。Turbo 容器是輕量級的，可以快速實例化，提交並通過 Web 共享到集線器。

Turbo 提供所謂 Turbo Hub 的應用程式雲，亦即為一個線上容器儲存庫，Hub 中的容器都可以共享與同步，並允許在不同設備之間可以繼續執行容器。目前在 Turbo 免費註冊的使用者只能在 Hub 中使用下載容器檔案至本機端之 Turbo 虛擬機中使用，無法在 Turbo 公司所提供的應用程式雲中執行容器檔案。[11]

參、應用程式雲之數位鑑識價值

由於應用程式雲及虛擬化應用程式軟體不斷進步與流行，使用者隨時隨地即可使用任何數位裝置，透過網站所提供應用程式之雲端服務即可執行各種應用程式，包括文件編輯、轉檔、列印及存放於雲端硬碟等工作，甚至有些應用程式雲可提供瀏覽器上網、使用 Line、Skype 等即時通訊軟體進行對話，而這些透過雲端服務所產生的文件檔案或是對話紀錄是否會在本機端留存，亦或是否會留下使用之數位軌跡以供追查。如果有心人士透過此種應用程式雲服務，將具營業機密或敏感性資料之檔案，編輯、轉檔或列印至特定雲端硬碟，則該如何從其所使用之數位裝置中取得使用應用程式雲之相關數位證據，非常值得深入探究。本研究擬透過簡易之鑑識步驟及鑑識程序來找出本機端在使用應用程式雲服務後可能留存之特定數位證據紀錄或殘存之數位痕跡，或由應用程式雲產生及儲存於雲端硬碟或本機端硬碟之文件檔後設資料，並利用鑑識分析來找尋可供利用之鑑識特徵，以識別與確認所用之犯罪手法與工具，亦為本研究之目的。

肆、應用程式雲客戶端之鑑識流程與方法

本研究有關應用程式雲實驗所使用之作業平台為 Windows 10，並使用 Vmware Workstation 虛擬機來模擬部份實驗環境，設定使用 Google Chrome、Edge 及 Firefox 等 3 種瀏覽器用於存取實驗之應用程式雲。本研究以 Cameyo、rollapp 及 Turbo 等 3 個應用程式雲作為實驗之標的，本篇研究將以數位鑑識實務上常用之程序與方法，針對上述 3 類型服務的軟體，安裝於視窗作業系統時，以 Google Chrome、Mozilla Firefox 及 MicroSoft Edge 等 3 種瀏覽器進行相關實驗與觀察，以找出可能會留存相關鑑識資料之檔案路徑或是值得注意之鑑識特徵值。

使用應用程式雲服務時，本機端視窗作業系統之數位鑑識步驟說明如下：

(1) 取得所欲鑑識之應用程式雲安裝程式，並記錄相關之版本資訊。
(2) 於虛擬機中先啟動 Systracer 系統快照程式，並執行第一次系統快照，執行完後再啟動 Disk pulse 程式，並開啟檔案及資料夾監控功能，啟動 WireShark 封包擷取軟體，來擷取網路封包
(3) 在虛擬機中分別以 3 種瀏覽器執行應用程式雲服務，並在 Disk Pulse 程式中觀察檔案及資料夾變化情形
(4) 在不關閉瀏覽器下使用 Process explorer 擷取應用程式雲之瀏覽器記憶體及利用 FTK Imager 擷取系統記憶體。
(5) 瀏覽器登出應用程式雲服務，擷取瀏覽器記憶體，關閉瀏覽器後，在擷取系統記憶體，停止 Disk Pulse 程式的檔案及資料夾監控功能，並將所記錄到之檔案及資料夾變化紀錄為報表檔，停止 WireShark 封包擷取功能，將封包紀錄存成檔案，以供後續分析。
(6) 使用 Systracer 快照程式進行第二次系統快照，快照結束後直接使用比較功能分析登錄檔在安裝驅動程式或軟體之前後差異處，並產生報表檔。
(7) 分析上述步驟所產生之報表檔，整理及歸納該種應用程式雲可供鑑識之特徵項目。

伍、實驗設計與結果討論

5.1 實驗設計

在安裝及測試應用程式雲時，使用的數位鑑識工具建議除了 X-Ways Forensics 等整合性鑑識軟體之外，對於登錄檔、資料夾及檔案之變化亦應一併觀察，檔案監控軟體紀錄相關檔案系統之變化情形，登錄檔之變動情形可用 Systracer 快照程式，進行相關記錄觀察與比較，檔案及資料夾之變動情形則可用 Disk Pulse 等程式來進行觀察及記錄，對於網路封包資料則以 WireShark 程式進行擷取，對於瀏覽器記憶體則以 Process explorer 進行擷取，對於系統記憶體擷取則使用 FTK Imager Capture Memory 功能來完成，從檔

案內容、登錄檔內容、封包資料及記憶體資料等 4 方面之比較分析來找出可供鑑識參考的特徵項目。

5.2 實驗結果

Cameyo、rollapp 及 Turbo 應用程式雲服務分別以 Google Chrome、Mozilla Firefox 及 MicroSoft Edge 等 3 種瀏覽器進行登入、使用應用程式、使用雲端硬碟儲存、以瀏覽器下載應用程式編輯檔案等不同狀態，分別實驗並觀察值得注意鑑識特徵項目，實驗結果資料整理如表一至三所示：

表一: Cameyo 服務重要鑑識項目

Google Chrome 瀏覽器留存檔案分析		
重要檔案或資料夾名稱	重要存放路徑	鑑識價值
所有檔案與資料夾	使用者帳號\Users\AppData\Local\Application Data\Google\Chrome\User Data\Default\Local Storage\	識別使用者是否安裝及使用此 Cameyo 雲服務
所有檔案 data_1 data_2 data_3	Users\使用者帳號\AppData\Local\Google\Chrome\User Data\Default\Cache	可在此識別與擷取使用 Cameyo 雲服務後之快取資料
History History Provider Favicons Cookies	Users\使用者帳號\AppData\Local\Google\Chrome\User Data\Default\	可在此識別與擷取使用 Cameyo 雲服務後之 history、cookie 等資料
saturn.cameyo[1].xml.lnk	\Users\使用者帳號\AppData\Roaming\Microsoft\Windows\Recent\	記載使用 Cameyo 雲服務之應用程式資料
Mozilla Firefox 瀏覽器檔案系統分析		
places.sqlite formhistory.sqlite cookies.sqlite	\Users\使用者帳號\AppData\Roaming\Mozilla\Firefox\Profiles\5ioupts8.default\	可在此識別與擷取使用 Cameyo 雲服務後之 history、cookie 等資料
所有檔案	\Users\使用者帳號\AppData\Local\Mozilla\Firefox\Profiles\5ioupts8.default\cache2\entries\	可在此識別與擷取使用 Cameyo 雲服務後之快取資料

MicroSoft Edge 瀏覽器檔案系統分析		
payment[2].js	\Users\使用者帳號\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cache\T5ITB1VJ\	記載使用 Cameyo 雲服務之應用程式資料
\Cache\ \Cookies\ \History\ \Preferences\等資料夾	\Users\使用者帳號\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge]	啟動及使用 Cameyo 雲服務，會在 Cache、Cookie、History 及 Preferences 等資料夾中留下相關資料
cameyoGuacamoleHandler[1].js cameyoapp[1].js	\Users\使用者帳號\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cache\RV8K5RP5\	使用 Cameyo 雲服務之應用程式之程式碼資料
登錄檔機碼及檔案系統分析		
重要機碼或檔名	登錄檔位置或檔案路徑	鑑識價值
(Default)	HKCR[\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\Children\001\InternetExplorer\EdpDomStorage]\cameyo.com\ []\online.cameyo.com\ []\saturn.cameyo.com\	確認使用 Cameyo 應用程式雲服務
pagefile.sys	系統根目錄	虛擬記憶體中可發現 Cameyo 雲服務之相關資料
cameyo.lnk	\Users\使用者帳號\AppData\Roaming\Microsoft\Windows\Recent\	識別是否使用 Cameyo 雲服務資料
WebCacheV01.dat *.log	\Users\使用者帳號\AppData\Local\Microsoft\Windows\WebCache\	紀錄檔記載 Cameyo 雲服務之使用狀況

網路封包分析			
特定網址	開啟之特定連線埠	憑證協定	鑑識價值
Online.cameyo.com (158. 69.27.194)	SSL 443	TlsCertificate	確認設備是否使用此應用雲服務，並可用以作為檢索記憶體中之帳號及密碼之基準
www.cameyo.com (168.62.48.183)	HTTP 80	無	
Saturn.cameyo.com (188.165.210.198)	HTTP 80	無	
記憶體分析			
瀏覽器種類	瀏覽器是否關閉	帳號及密碼狀態	鑑識價值
Google Chrome	瀏覽器未關閉，且曾登入及登出帳號	可發現登入之帳號及密碼，密碼以 utf-16 編碼存在	可取得 Cameyo 網站登入帳號及密碼，可取得應用程式雲服務上之檔案資料
	曾入及登出帳號，但瀏覽器已關閉	可取得登入帳號，但無法取得密碼資料	
Mozilla Firefox	瀏覽器未關閉，且曾登入及登出帳號	可發現登入之帳號及密碼，密碼以 big-5 及 utf-16 編碼存在	
	曾入及登出帳號，但瀏覽器已關閉	可取得登入帳號，但無法取得密碼資料	
MicroSoft Edge	瀏覽器未關閉，且曾登入及登出帳號	未發現明文密碼資料，但疑似有編碼之密碼存在	
	曾入及登出帳號，但瀏覽器已關閉	可取得登入帳號，但無法取得密碼資料	

表二: rollapp 服務重要鑑識項目

Google Chrome 瀏覽器檔案系統分析		
重要檔案或資料夾名稱	重要存放路徑	鑑識價值
所有檔案與資料夾	\AppData\Local\Application Data\Google\Chrome\User Data\Default\Local Storage\	識別使用者是否安裝及使用此 rollapp 雲服務
Top Sites Shortcuts Preferences Network Action Predictor History-journal History Provider Cache History Favicons Cookies	\Users\使用者帳號\AppData\Local\Google\Chrome\User Data\Default\	可在此識別與擷取使 rollapp 雲服務後之 history、cookie 等資料
所有*.js data_1 data_2 data_3	使用者帳號[\AppData\Local\Google\Chrome\User Data\Default\Cache	可在此識別與擷取使用 rollapp 雲服務後之快取資料
WebCacheV01.dat *.log	\Users\使用者帳號\AppData\Local\Microsoft\Windows\WebCache\	紀錄檔記載 Tonido 個人雲服務之使用狀況
Mozilla Firefox 瀏覽器檔案系統分析		
places.sqlite	\Users\使用者帳號\AppData\Roaming\Mozilla\Firefox\Profiles\5ioupts8.default\	可在此識別與擷取使用 rollapp 雲服務後之 history、cookie 等資料
所有檔案	\Users\使用者帳號\AppData\Local\Mozilla\Firefox\Profiles\5ioupts8.default\cache2\entries\	可在此識別與擷取使用 rollapp 雲服務後之快取資料
MicroSoft Edge 瀏覽器檔案系統分析		
ui[1].js signin[2].js	\Users\使用者帳號\AppData\Local\Packages\Microsoft.	使用 rollapp 雲服務之應用程式之程式碼資料

signin[1].js rollmyfile[1].js rollmyfile-upload[1].js rollapp-html5client.min[1].js rollapp-html5client.min[1].css desktop[1].css	MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cache\T5ITB1VJ\		
\Cache\ \Cookies\ \History\ \Preferences\	[\Users\使用者帳號\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge]		啟動 rollapp 雲服務，會在 Cache、Cookie 及 History 等資料夾中留下相關資料
spartan.edb	\Users\使用者帳號\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\120712-0049\DBStore\		識別是否使用 rollapp 雲服務資料
登錄檔機碼及檔案系統分析			
重要機碼或檔名	登錄檔位置或檔案路徑		鑑識價值
UPDATER.EXE-58AE5631.pf	\Windows\Prefetch\		啟動 rollapp 雲服務
rollapp.lnk	\Users\使用者帳號\AppData\Roaming\Microsoft\Windows\Recent\		識別是否使用 rollapp 雲服務資料
網路封包分析			
特定網址	開啟之特定連線埠	憑證協定	鑑識價值
www.rollapp.com[api.rollapp.com](52.52.97.52)	SSL 443	TlsCertificate	確認設備是否使用此應用雲服務，並可用以作為檢索記憶體中之帳號及密碼之基準

記憶體動態分析			
瀏覽器種類	瀏覽器是否關閉	帳號及密碼狀態	鑑識價值
Google Chrome	瀏覽器未關閉，且曾登入及登出帳號	可發現登入之帳號及密碼，密碼以 utf-16 編碼存在	可取得 rollapp 雲服務網站登入帳號及密碼，可取得應用程式雲服務上之檔案資料
	曾入及登出帳號，但瀏覽器已關閉	可取得登入帳號，但無法取得密碼資料	
Mozilla Firefox	瀏覽器未關閉，且曾登入及登出帳號	可發現登入之帳號及密碼，密碼以 utf-16 編碼存在	
	曾入及登出帳號，但瀏覽器已關閉	可取得登入帳號，但無法取得密碼資料	
MicroSoft Edge	瀏覽器未關閉，且曾登入及登出帳號	未發現明文密碼資料，但疑似有編碼之密碼存在	
	曾入及登出帳號，但瀏覽器已關閉	可取得登入帳號，但無法取得密碼資料	

表三、Turbo 服務重要鑑識項目

Google Chrome 瀏覽器檔案系統分析		
重要檔案或資料夾名稱	重要存放路徑	鑑識價值
所有檔案與資料夾	\AppData\Local\Application Data\ Google\Chrome\User Data\ Default\Local Storage\	識別使用者是否安裝及使用 Turbo 雲服務
content.js content.js.template	\Users\使用者帳號\AppData\ Local\Google\Chrome\User Data\ Default\Extensions\ldibmiofagdkgiphkcokpooepankmacl\3.3.3.1113_0\	使用 Turbo 雲服務之應用程式之程式碼資料
所有檔案 data_1 data_2 data_3	使用者帳號 [\AppData\Local\Google\Chrome\User Data\Default\Cache	可在此識別與擷取使用 Turbo 雲服務後之快取資料
History History Provider Cache History-journal Favicons Cookies DownloadMe Tadata Last Session Last Tabs Login Data Network Action Predictor Preferences Shortcuts Top Sites	使用者帳號 [\AppData\Local\Google\Chrome\User Data\Default\	可在此識別與擷取使 Turbo 雲服務後之 history、cookie 等資料
WebCacheV01.dat	\Users\使用者帳號\AppData\ Local\Microsoft\Windows\	紀錄檔記載 Turbo 雲服務之使用狀況

*.log	WebCache\	
Mozilla Firefox 瀏覽器檔案系統分析		
extensions.json	\Users\使用者帳號\AppData\Roaming\Mozilla\Firefox\Profiles\5ioupts8.default\	紀載使用 Turbo 應用程式雲之網址資訊
所有檔案	\Users\使用者帳號\AppData\Local\Mozilla\Firefox\Profiles\5ioupts8.default\cache2\entries\	
formhistory.sqlite permissions.sqlite places.sqlite *.js	\Users\使用者帳號\AppData\Roaming\Mozilla\Firefox\Profiles\5ioupts8.default\	可在此識別與擷取使用 Turbo 雲服務後之 history、cookie 等資料
MicroSoft Edge 瀏覽器檔案系統分析		
payment[2].js	\Users\使用者帳號\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cache\T5ITB1VJ\	使用 Turbo 雲服務之應用程式之程式碼資料
\Cache\ \Cookies\ \History\ \Preferences\	\Users\使用者帳號\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge	啟動 Turbo 雲服務，會在 Cache、Cookie 及 History 等資料夾中留下相關資料
登錄檔機碼及檔案系統分析		
重要機碼或檔名	登錄檔位置或檔案路徑	鑑識價值
url	HKCR[\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\MicrosoftEdge\TypedURLs\]	確認使用 Turbo 應用程式雲服務
turbo.net.lnk	\Users\使用者帳號\AppData\Roaming\Microsoft\Windows\Recent\	
ksync.exe *.json	\Users\使用者帳號\AppData\Local\Spoon\3.33.1488.17__\	Turbo 雲服務在客戶端安裝之資料夾

Spoon-Console.exe			
NTUSER.DAT	\Users\使用者帳號\AppData\Local\Spoon\Sandboxes\		由登錄檔中可發現使用者使用 Turbo 雲服務。
turbo_*.log *.json	\Users\使用者帳號\AppData\Local\Spoon\Logs\		使用 Turbo 雲服務之相關紀錄(log)
網路封包分析			
特定網址	開啟之特定連線埠	憑證協定	鑑識價值
Turbo.net(4.53.147.210)	SSL 443	無	確認設備是否使用此應用雲服務，並可用以作為檢索記憶體中之帳號及密碼之基準
blog.turbo.net(4.53.147.241)	SSL 443	無	
記憶體動態分析			
瀏覽器種類	瀏覽器是否關閉	帳號及密碼狀態	鑑識價值
Google Chrome	瀏覽器未關閉，且曾登入及登出帳號	可發現登入之帳號及密碼，密碼以 utf-16 編碼存在	可取得 Turbo 網站登入帳號及密碼，可取得應用程式雲服務上之檔案資料 鑑識價值
	曾入及登出帳號，但瀏覽器已關閉	可取得登入帳號，但無法取得密碼資料	
Mozilla Firefox	瀏覽器未關閉，且曾登入及登出帳號	可發現登入之帳號及密碼，密碼以 utf-16 編碼存在	
	曾入及登出帳號，但瀏覽器已關閉	可取得登入帳號，但無法取得密碼資料	
MicroSoft Edge 瀏覽器種類	瀏覽器未關閉，且曾登入及登出帳號	可發現登入之帳號及密碼，密碼以 utf-16 編碼存在	

	瀏覽器是否關閉	可取得登入帳號，但無法取得密碼資料	

實驗結果顯示以 Google Chrome、Mozilla Firefox 及 MicroSoft Edge 等 3 種瀏覽器，分別連接至本研究標的 Cameyo、rollapp 及 Turbo 等 3 個應用程式雲，可發現在不同瀏覽器的 Cookie、Histroy、Cache 等存放路徑仍可發現使用此等應用程式雲之痕跡，另由登錄檔及檔案系統部分檔案資料亦可發現使用上述 3 種應用程式雲之數位痕跡，由記憶體分析發現，使用 Google Chrome 及 Mozilla Firefox 瀏覽器只要曾經登錄使用上述 3 種應用程式雲，且未關閉狀態，仍有可能從瀏覽器應用程式記憶體中擷取應用程式雲之帳號及密碼資料，但如使用 MicroSoft Edge 存取前述 2 種應用程式雲，則無法取得明文密碼資料，但存取 Turbo 雲服務，則可取得登入之帳號及明文密碼。由網路封包資料分析發現，使用者在應用程式雲上之資料傳輸都以 SSL 加密協定運作，因此如果想透過封包側錄來取得使用者在應用程式雲上活動情形與傳遞資料，顯有困難。

由實驗發現 Cameyo、rollapp 等 2 種應用程式雲可使用 Google、Facebook 等第三方驗證帳號登入，因此如果調查人員在現場可取得該等帳號及密碼，將可用於登入使用者所使用之上述 2 種應用程式雲，另上述 3 種應用程式雲亦提供使用者可設定 Google Drive、Dropbox、OneDrive 及 Box 等雲端硬碟，以作為使用應用程式產生之檔案儲存空間，亦可直接使用瀏覽器下載所產生之檔案，因此有關客戶端系統之同步雲端硬碟資料夾或預設下載資料夾，亦必須加以檢查。而有關上述雲端硬碟之資料擷取與保存方法請參考相關文獻。

陸、結論與未來研究方向

本研究對於應用程式雲之鑑識研究，目前在學術上僅有部分研究資料可供參考，因此嘗試以數位鑑識實務作業之程序與方法，透過簡易之數位鑑識工具，在應用程式雲啟動、下載及安裝軟體及執作時，從檔案系統、瀏覽器、網路封包及記憶體等 4 方面比較分析可能潛藏數位證據之檔案、資料夾、系統登錄機碼及網路連線等資料，並嘗試個化出具鑑識價值之特徵項目，實驗結果顯示本研究所列之應用程式雲使用之 SaaS 技術雖有所不同，但仍可透過數位鑑識之程序與方法解析使用該等雲端服務後在客戶端所留存之數位證據與相關紀錄。本實驗應用程式雲之使用均係透過瀏覽器使用，而登入之帳號及密碼資訊可由瀏覽器中擷取，但如果瀏覽器關閉，則無法獲知使用者使用之密碼資訊，因此如何不透過明文密碼之解析，而透過封包分析及檔案分析來找尋使用者留存於系統之 token 資料，有關此部分之研究，值得做為後續深入的研究方向。

參考文獻

[1] A. Amirullah, I. Riadi and A. Luthfi, "Forensics Analysis from Cloud Storage Client Application on Proprietary Operating System", *International Journal of Computer Applications*, Volume 143 – No.1, June 2016.

[2] D. Birk and C. Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments" In: *2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 1–10. IEEE, Okland, CA, 2011.

[3] Cloud Security Alliance, Incident Management and Forensics Working Group, "Mapping ISO27037 to Cloud Computing Environments", June 2013.

[4] M. Damshenas, A. Dehghantanha, R. Mahmoud and S. Shamsuddin, "Forensics Investigation Challenges in Cloud Computing Environments," In: *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference* on IEEE, pp. 190–194, Kuala Lumpur, 2012.

[5] International Standard, "ISO/IEC 27037 Information technology—Security techniques, Guidelines for identification, collection, acquisition and preservation of digital evidence", 2012.

[6] P. Mell and T. Grance, "The NIST definition of cloud computing," http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, 2011.

[7] J. Milagre and M. Caiado, "Cloud Computing Forensics. Best Practice and Challenges for Process Efficiency of Investigations and Digital Forensics," *The Eighth International Conference on Forensic Computer Science – ICoFCS*, pp 18-26, 2013

[8] National Institute of Standards and Technology, "NIST Cloud Computing Forensic Science Challenges," Available at: http://csrc.nist.gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf, June 2014

[9] D. Quick and K. K. R. Choo, "Google Drive: Forensic analysis of data remnants," *Journal of Network and Computer Applications*, 2013.

[10] rollApp, "Run Desktop Applications Online," https://www.rollapp.com/home,2017.

[11] Turbo Containers, "Run Applications Anywhere," https://turbo.net/docs, 2017.

[12] Wikipedia, "Cameyo wiki:history and operations," https://en.wikipedia.org/wiki/Cameyo, 2017.