雲端鑑識工具技術之探討研究報告

陳受湛[1] 鄧思源[2] 萬幼筠[3] 陳威棋[4]
法務部調查局資通安全處 勤業眾信聯合會計師事務所
[1] dan-chen@seed.net.tw [2] buyer92@mjib.gov.tw [3] thomaswan@deloitte.com.tw
[4]ikewchen@deloitte.com.tw

摘要

近年來，隨著雲端服務的快速發展，不只改變一般普羅大眾的生活型態，亦改變了犯罪者的犯罪型態，近來多起著名的資料外洩事件亦與雲端服務相關，雲端服務的犯罪模式使得鑑識人員更難以快速且精確的掌握相關跡證。本研究將透過建置模擬環境，實際執行各種雲端服務後取得數位證據留存種類，進而提出相關證據彙整清單，協助鑑識人員快速且精確掌握相關跡證。

關鍵詞：雲端儲存服務、私有雲、雲端鑑識、雲端數位證據

Methodology Research For Cloud Environment Forensic Tools

CHEN, SOU-CHAN[1], TENG, SZU-YAUN[2], Wan, You-Yen[3], CHEN, WEI CHI[4]
Ministry of Justice Investigation Bureau Information Security Department, Deloitte Taiwan
Dan-chen@seed.net.tw[1], buyer92@mjib.gov.tw[2], thomaswan@deloitte.com.tw[3],
ikewchen@deloitte.com.tw[4]

Abstract

With the fast growing of the cloud services from recent years, this does not only changed the lifestyle of the users, but also changed the pattern of the criminals. Recently several well-known data leakage incident also found to be related to cloud services, the crime pattern also made digital forensic personal harder to take control of the evidences promptly and accurately. This research will focus on the types of digital evidences on the cloud service, and through the implementation of virtual environment, and provides related evidence lists to support digital forensic personal with efficiency.

Keywords: Cloud Storage services, Private cloud, Cloud Forensics, Cloud Digital Forensics

壹、 研究動機與目的

隨著資訊科技日新月異，高速網路傳輸與資訊架構虛擬化結合了行動裝置的輕薄可攜，讓資訊傳遞及分享更為快速且方便，進而衍伸出各種雲端服務。

雲端服務的快速發展亦改變普羅大眾的生活型態，一般使用者可藉由各種媒介上傳、下載並分享各種檔案，如：圖片、音樂、影片及文件，企業用戶則可利用雲端服務來達成資訊設備虛擬化，並快速且有彈性的調整軟硬體資源。

面對著的雲端服務與虛擬化技術日益普及，在這些快速、便利的背後，資料外洩、惡意攻擊甚至是隱匿犯罪跡證等事件層出不窮。如何有效蒐集數位證據，了解數位證據之間的關聯性，以及技術方法是否足以對應雲端環境之特殊性都是一大挑戰。為協助執法機關在偵辦案件與執行數位鑑識作業可能遇到之困境，本研究針對雲端服務進行研究，並進一步探討雲端服務所留存之跡證結果，進而提出跡證彙整資訊，以期能協助執法機關快速進行鑑識作業。

貳、 文獻探討

一、 常見之雲端儲存服務及私有雲種類說明

1、 常見雲端儲存服務

(1) Dropbox

Dropbox 為 Dropbox 公司的線上儲存服務，主要可以透過雲端儲存實現網際網路上的檔案同步，使用者可以藉此共享檔案和資料。

(2) Microsoft OneDrive

Microsoft OneDrive，前稱 Windows Live SkyDrive，是微軟所推出的網路硬碟及雲端服務。使用者可以上傳他們的檔案到網路伺服器上，並且透過瀏覽器來瀏覽那些檔案。OneDrive 同步採用 SSL 加密傳輸，儲存則使用 AES-256 進行加密。

(3) Google Drive

Google Drive 是 Google 的一個線上同步儲存服務，同時結合 Google 文件的線上檔案編輯功能，於 2012 年 4 月 24 日起逐漸開放給用戶使用。

(4) Apple iCloud

iCloud 是蘋果公司所提供的雲儲存和雲端運算服務，初始空間有 5GB，可以擴充功能。使用者能在 iCloud 中儲存音樂、相片、App、聯絡

人和日曆等，並推播到使用者所有支援 iCloud 同步的裝置上，而不用使用傳輸線來同步。

iCloud 同步採用 SSL 加密傳輸，儲存則至少使用 AES-128 進行加密，Keychain 等敏感資料則使用 AES-256 進行加密。

(5) ASUS WebStorage

ASUS WebStorage 是華碩雲端股份有限公司開發的線上儲存服務，功能包含了線上備份及同步處理等功能，在安全性的部分則使用了 AES 加密，並且支援線上掃毒及動態密碼等功能。

2、 常見私有雲種類

(1) Amazon EC2

Amazon Elastic Compute Cloud，簡稱 Amazon EC2，是由亞馬遜公司提供的 Web 服務，是一個讓使用者可以租用雲端電腦運行所需應用的系統。EC2 藉由提供 Web 服務的方式讓使用者可以彈性地運行自己的 Amazon 機器映像檔，使用者將可以在這個虛擬機器上運行任何自己想要的軟體或應用程式。

(2) hicloud VPC

hicloud VPC 為中華電信提供之虛擬私有雲服務，提供動態擴充與彈性的雲端運算資源，進而建構企業所需的專屬雲端資料中心，提供企業總部統一控管運算資源、儲存服務、網路服務與資安服務之完整解決方案。

(3) 台灣大哥大之 IaaS 服務

台灣大哥大之 IaaS 服務為台灣大哥大提供之雲端運算服務，提供依需求租用的 IT 基礎設施服務。

台灣大哥大所提供之雲端虛擬主機可隨需求及時增加或升級主機，亦可遠端操作隨時監控主機，並且擁有硬體 HA 機制快速恢復服務。在系統備份方面，可排程定時備份。硬碟則為 RAID 5 方式建置，並可任意掛載主機。除此之外還有雲端附載平衡、監控及防火牆防護等多項服務。

(4) OpenStack

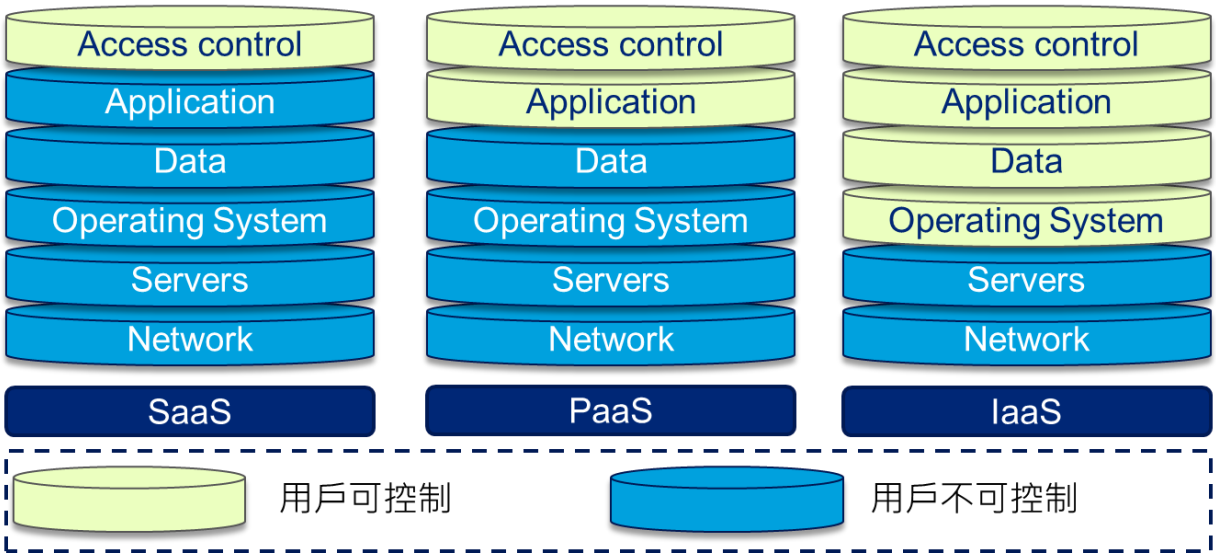
OpenStack 是一個美國國家航空暨太空總署和 Rackspace 合作研發的雲端運算軟體，以 Apache 許可證授權，並且是一個自由軟體和開放原始碼項目。

OpenStack 是 IaaS （基礎設施即服務）服務，讓任何人都可以自行建立和提供雲端運算服務。此外，OpenStack 也用作建立防火牆內的「私有雲」(Private Cloud)，提供機構或企業內各部門共享資源。

二、 雲端鑑識文獻探討

雲端服務的範圍非常廣泛，主要分為分為軟體即服務 (Software as a Service, StaaS)、平台即服務 (Platform as a Service, PaaS)、架構即服務 (Infrastructure as a Service, IaaS) 三種。雲端鑑識的相關研究於近年亦成為諸多學者亟欲研究的項目之一，本研究將藉由雲端鑑識文獻探討來了解目前於雲端鑑識之成果及挑戰。

學者 Zawoad 及 Hasan (2013) [6] 的研究亦指出，三種常見雲端服務於主機端與伺服器端所留存之數位證據，隨主機端可控制之資料越少，表示鑑識人員於該類雲端鑑識案件中，應著重於取得伺服器端之資料，而非主機端，如下圖所示。



圖一：各雲端服務於主機端與伺服器端留存資料比較 [6]

(圖片出處：Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems)

Marturana 及 Me (2012) [4] 利用瀏覽器進入雲端儲存服務，並使用 Nirsoft Live 工具分析來自 IE(8.0.7601.17514)、Mozilla(11.0)、Chrome(18.0.1025.168m) 的瀏覽器記錄，並捕捉雲端跟主機端之間的網路流量(Cache, Cookies, 瀏覽歷史, 下載記錄)。最後得知，於雲端分享檔案、照片及文件時，瀏覽器會儲存相關的日誌及暫存檔等紀錄。

Martini 及 Choo (2013) [3] 針對 OwnCloud 實測則分為本機端鑑識與伺服器端鑑識。本機端鑑識的部分利用三大瀏覽器 (IE, FireFox, Chrome) 進入雲端存取介面，並成功擷取下列資料：

- 整合及檔案管理的元數據
- Cache 檔案
- 雲端服務及認證數據
- 加密數據
- 瀏覽器相關資訊

- 行動裝置本機端資訊
- 網路分析

伺服器端鑑識則使用 ownCloud PHP 軟體於 CentOS 6 虛擬主機，並擷取以下資料：

- 管理者及檔案管理元數據
- 存放的檔案
- 加密元數據
- 雲端登入及驗證資訊

Epifani (2013) [2] 針對透過 Dropbox, Google Drive 及 SkyDrive 用戶端則使用 DiskPulse 追蹤硬碟使用量（創立、修改及刪除檔案），並利用 RegShot 及 RegFromApp 偵測登錄檔的變更。進而發現，DropBox 及 Google Drive 使用 SQLite 資料庫存放檔案資訊。此外，Dropbox 資料庫有時候可經由 Dropbox Decryptor 或 IEF 破解。另外，在 Google Drive Sync_log.log 可以取得刪除的檔案資訊。SkyDrive 則使用二元碼儲存現有的檔案資訊，其日誌檔案也可以取得刪除的檔案資訊。

Zawoad 及 Hasan (2013) [5] 則提到傳統的電腦鑑識，調查人員可完全掌握數位證據。但在雲端中，將牽扯不同服務系統。雲端鑑識中，將很難定義虛擬主機的位置，且即使有位置資訊，則有可能位於不同時區，這些將直接影響監管鏈原則。目前雲端鑑識依靠 CSP（雲端服務提供者）去取得，但這可能造成由 CSP 取得的證據不是正確的資訊，且這些資訊可能無法使用於法庭。此外，雲端鑑識的挑戰包含了：

- 資料擷取方式：揮發性資料擷取，關機後會消失，若沒有做備份，則會失去資料。
- 日誌：多半為分散的、揮發性日誌，日誌取得能力亦須依賴 CSP。
- 保留監管鏈：法令狀必須詳細說明證據位置，但雲端沒有實際位置，且可能包含其他使用者的資料。
- 現有鑑識工具功能不足
- 犯罪現場重建：關機後無法重建。
- 跨界法律：資料儲存中心遍佈全球。
- 證據展示：法院可能沒有足夠知識。

綜觀上述文獻探討之內容可以得知，目前雲端鑑識多分為本機端及雲端（由雲端服務提供商管理），惟雲端上之證據絕大多數由雲端服務提供商管理，因此本研究將針對本機端證據進行識別，並彙整提出相關建議。

三、 國內外雲端鑑識工具說明及功能比較

Passware 推出的 PASSWARE KIT 2015 v.4，可針對 Dropbox 等雲端服務進行檔案擷取等動作。Passware 透過本機端 Registry 取得 Token 後，不須另外輸入使用者帳號

密碼，即可藉由此 Token 下載使用者於 Dropbox 儲存的檔案，甚至連刪除的檔案也有機會還原取出。惟目前 StaaS 服務僅支援 Dropbox，IaaS 部份僅支援 Amazon EC2 之虛擬主機密碼破解。

F-Response 今年(2015)針對 IaaS 雲端服務推出可擷取 Amazon EC2 執行個體之工具(F-Response Universal)。此外，F-Response 的 Cloud Connector 可針對 Azure(PaaS)，Amazon S3、Dropbox(StaaS)以及 Gmail、Yahoo mail(SaaS)等雲端服務進行遠端連線，透過連線後建立虛擬磁碟機之方式，使鑑識人員可透過其他專業鑑識軟體(如 EnCase)進行資料擷取。

OTIXO 為一整合式雲端儲存服務管理介面，使用者僅需一次性登入後，即可統整管理多個雲端儲存服務，目前它提供了與 24 種各類空間連接的服務，如：Dropbox、Google Docs/Drive、SugarSync、Box、SkyDrive、Picasa、Amazon S3、CX、Ubuntu One，及其他 WebDav 和 FTP。雖然該軟體並不以數位鑑識角度進行資料擷取，但其整合式介面可讓鑑識人員快速備份 StaaS 服務中之資料。

由 Guidance Software 推出的 EnCase 支援多種取證模式，可於本機端取證取得相關證據，若使用私有雲，EnCase 亦有遠端取證模式，執行人員則可針對遠端虛擬主機進行遠端取證。

由 AccessData 推出的 FTK，全名 Forensic Toolkit，亦可進行多種取證方式，取得本機端或遠端主機上之證據。執行人員可藉此取得主機的記憶體、硬碟資訊……等相關證據。

此外， Dykstra 與 Sherman [1] 於 2012 的研究中亦使用各項鑑識工具取得 Amazon EC2 雲端虛擬環境中之資料，所需時間，如下表所示：

表一　常用鑑識工具取得 Amazon EC2 之資料所需時間 [1]
(資料出處：Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques)

鑑識工具	所需時間（小時）	最後成果
EnCase	12	成功取得
FTK	12	成功取得
FTK Imager (Disk)	12	成功取得
Fastdump	2	成功取得
Memoryze	2	成功取得
FTK Imager (Memory)	2	成功取得
Volume Block Copy	14	成功取得
Agent Injection	1	成功取得
AWS Export	120	成功取得

參、 研究架構

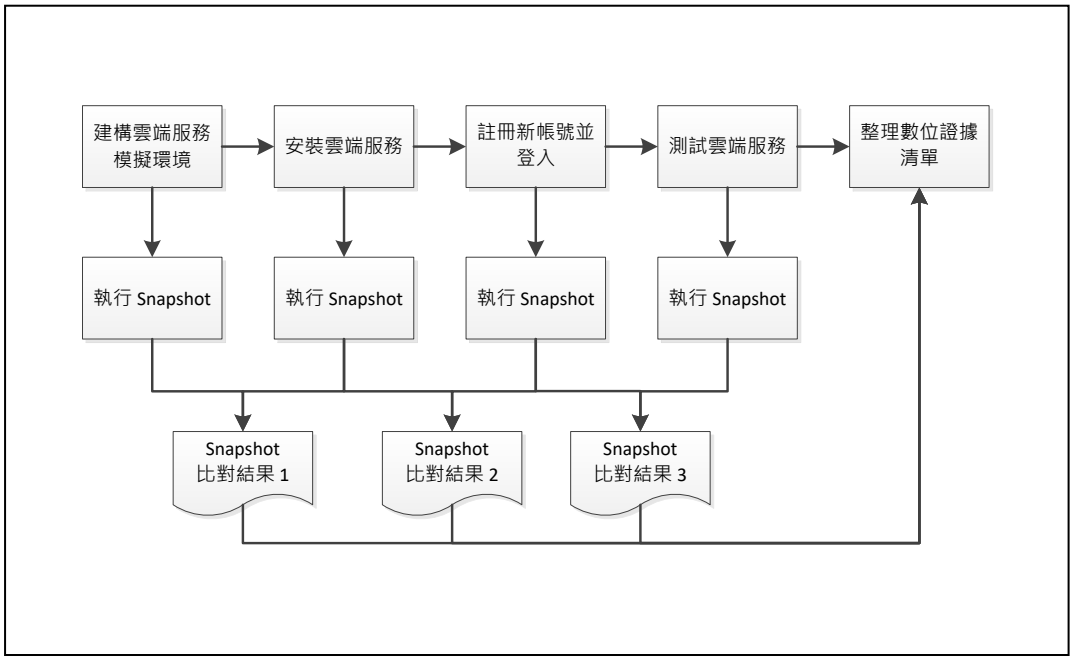
依據過去研究及文獻彙整的結果可得知，雲端證據主要分別存在於本機端及雲端(由雲端服務提供商管理)。由於雲端環境的相關跡證主要由雲端服務提供商管理，因此本研究先從本機端相關跡證著手，取得本機端關鍵的雲端服務跡證，進而提出雲端服務跡證彙整建議。

一、 研究方法

本研究先蒐集並彙整過去有關雲端跡證研究及探討之結論，再蒐集各雲端服務提供者之產品資訊。後續開始建構雲端服務模擬環境、安裝服務、註冊帳號、登入即時測雲端服務。並於重大異動後執行 Snapshot，再將 Snapshot 兩兩比對其差異。如下圖所示：

- 「Snapshot 比對結果 1」為建置環境與安裝雲端服務兩者 Snapshot 差異比對
- 「Snapshot 比對結果 2」為安裝雲端服務與註冊帳號登入兩者 Snapshot 差異比對
- 「Snapshot 比對結果 3」則為登入與實測服務之 Snapshot 差異比對

執行 Snapshot 比對之後，將比對結果中可清楚識別與該雲端服務相關之異動彙整為數位證據清單，並利用數位證據清單之結果撰寫雲端服務之鑑識流程。



圖二：雲端工具技術研究方法

二、 模擬環境及相關雲端服務版本說明

本研究使用虛擬環境來建立雲端服務所需之環境，將 Windows 7 部署於 VM 中，並將相關雲端服務安裝於 VM 環境中，藉此將雲端服務之環境相互隔離，以避免環境參數相互影響。

三、 實測雲端儲存服務

雲端儲存服務為目前市面上廣受大眾使用的雲端服務之一，且近年來各種雲端犯罪、資料外洩事件都有雲端儲存服務的影子在裡面，因此本研究針對雲端儲存服務挑選五種國內外常見之雲端儲存服務進行實測：Dropbox, OneDrive, Google Drive, Apple iCloud, ASUS WebStorage

四、 實測私有雲部署

除雲端儲存服務以外，目前企業用戶最常使用的雲端服務還有私有雲的部分，針對目前市面上常見私有雲部屬實測，本研究選擇下列幾項私有雲服務：Amazon EC2, hiCloud VPC, 台灣大哥大之 IaaS 服務, OpenStack

本研究所實測之私有雲部署，除 hiCloud VPC 於實測期間與 Google Chrome 瀏覽器出現不相容情況以外，其餘皆透過 Google Chrome 瀏覽器執行。因此除 hiCloud 部署實測透過 MS Internet Explorer 執行瀏覽器暫存檔案分析以外，其餘皆透過 Chrome 執行相關測試。

肆、 研究發現

一、 雲端儲存服務之常見數位證據種類

1、 安裝前後差異比較

(1) Dropbox

表二 ：Dropbox 安裝前後差異比較

狀態	類型	位置
安裝	Registry	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\
安裝	Registry	HKEY_USERS\S-1-5-21-2020062809-1800262464-634923857-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\
安裝	Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\DropBoxExt1\

(2) OneDrive

表三 ：OneDrive 安裝前後差異比較

狀態	種類	位置
安裝	Registry	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\
安裝	Registry	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\
安裝	Registry	HKEY_USERS\S-1-5-21-2020062809-1800262464-634923857-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\
安裝	Registry	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2
安裝	Registry	HKEY_USERS\S-1-5-21-2020062809-1800262464-634923857-1000\Software\ Microsoft\Windows\CurrentVersion\Explorer\StartPage2
安裝	Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\OneDrive

(3) Google Drive

表四 ：Google Drive 安裝前後差異比較

狀態	種類	位置
安裝	Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders
安裝	Registry	HKEY_CURRENT_USER\Software\Google\Drive
安裝	Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\GoogleDriveBlacklisted
安裝	Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\GoogleDriveSynced
安裝	Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\GoogleDriveSyncing
安裝	資料夾	C:\Program Files\Google\Drive
安裝	資料夾	C:\Users\<username>\Google
安裝	資料夾	C:\Users\<username>\Desktop\Google
安裝	檔案	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Google Drive\Google Drive.lnk
安裝	資料夾	C:\Users\<username>\AppData\Local\Google\Drive
安裝	檔案	C:\Users\<username>\AppData\Local\Google\Drive\user_default\snapshot.db
安裝	檔案	C:\Users\<username>\AppData\Local\Google\Drive\user_default\sync_config.db
安裝	檔案	C:\Users\<username>\AppData\Local\Google\Drive\user_default\sync_log.txt
安裝	檔案	C:\Users\<username>\AppData\Local\Google\Drive\upgrade_log.log

(4) Apple iCloud

表五 ：Apple iCloud 安裝前後差異比較

狀態	種類	位置
安裝	Registry	HKEY_CLASSES_ROOT\iCloudServices.AccountInfo\
安裝	Registry	HKEY_CLASSES_ROOT\Installer\Products\F855C33BF27780340A9593F0FBB9AAEA\
安裝	Registry	HKEY_CURRENT_USER\Software\Apple Inc.\Internet Services\iCloud Photos\
安裝	Registry	HKEY_CURRENT_USER\Software\Apple Inc.\Internet Services\iCloud Photos\Settings\
安裝	Registry	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\
安裝	Registry	HKEY_USERS\S-1-5-21-2020062809-1800262464-634923857-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\
安裝	Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\iCloudServices.EXE\
安裝	Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\iCloudServices.AccountInfo\
安裝	Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\iCloudServices.AccountInfo\CLSID\
安裝	Registry	HKEY_USERS\S-1-5-21-2020062809-1800262464-634923857-1000\Software\Apple Inc.\Internet Services\iCloud Photos\
安裝	檔案	C:\Documents and Settings\<username>\AppData\Local\Application Data\Temp\icloudXXX.log
安裝	資料夾	C:\Users\<username>\AppData\Roaming\Apple Computer\Logs\
安裝	資料夾	C:\Program Files (x86)\Common Files\Apple\Internet Services\iCloud.resources\
安裝	資料夾	C:\Program Files (x86)\Common Files\Apple\Internet Services\iCloudDrive.resources\

(5) ASUS WebStorage

表六 ：ASUS WebStorage 安裝前後差異比較

狀態	種類	位置
安裝	Registry	HKEY_CURRENT_USER\Software\ECAREME\OmniStore\yostore
安裝	Registry	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage\NewShortcuts\
安裝	Registry	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\!AsusWSShellExt_B
安裝	資料夾	C:\Asus WebStorage\
安裝	資料夾	C:\Asus WebStorage\<username>
安裝	資料夾	C:\Program Files (x86)\ASUS\WebStorage\2.2.4.537\
安裝	檔案	C:\windows\prefetch\ASUSWEBSTORAGESYNCAGENT2.2.4.-7AAB6CF1.pf
安裝	檔案	C:\windows\prefetch\ASUSWSPANEL.EXE-B6FFA74A.pf
安裝	檔案	C:\windows\prefetch\ASUSWSSERVICE.EXE-13C9B8DF.pf
安裝	Registry	HKEY_CURRENT_USER\Software\ECAREME\OmniStore\yostore\
安裝	Registry	HKEY_CURRENT_USER\Software\ECAREME\OmniStore\yostore\<user account>
安裝	資料夾	C:\Users\<username>\AppData\Roaming\WebStorage\Logs

2、 執行雲端服務前後差異比較

(1) Dropbox

表七 ：Dropbox 執行雲端服務前後差異比較

狀態	類型	位置
登入	Registry	HKEY_CURRENT_USER\Software\Dropbox\ks1\
登入	Registry	HKEY_CURRENT_USER\S-1-5-21-2020062809-1800262464-634923857-1000\Software\Dropbox\ks1

(2) OneDrive

表八 ：OneDrive 執行雲端服務前後差異比較

狀態	種類	位置
登入	Registry	HKEY_USERS\S-1-5-21-2020062809-1800262464-634923857-1000\Software\Microsoft\OneDrive\Accounts\Personal
同步	Registry	HKEY_CURRENT_USER\Software\Microsoft\OneDrive
同步	Registry	HKEY_USERS\S-1-5-21-2020062809-1800262464-634923857-1000\Software\Microsoft\OneDrive
同步	Registry	HKEY_CURRENT_USER\Software\Microsoft\OneDrive\Accounts\Personal

(3) Google Drive

表九 ：Google Drive 執行雲端服務前後差異比較

狀態	種類	位置
同步	資料夾	C:\Users\<username>\Google 雲端硬碟
同步	檔案	C:\Users\<username>\AppData\Local\Google\Drive\user_default\snapshot.db
同步	檔案	C:\Users\<username>\AppData\Local\Google\Drive\user_default\sync_config.db
同步	檔案	C:\Users\<username>\AppData\Local\Google\Drive\user_default\sync_log.txt

(4) Apple iCloud

表十 ：Apple iCloud 執行雲端服務前後差異比較

狀態	種類	位置
同步	資料夾	C:\Users\<username>\AppData\Roaming\Apple Computer\Logs\
同步	資料夾	C:\Documents and Settings\<username>\Pictures\iCloud Photos
同步	資料夾	C:\Documents and Settings\<username>\iCloudDrive\

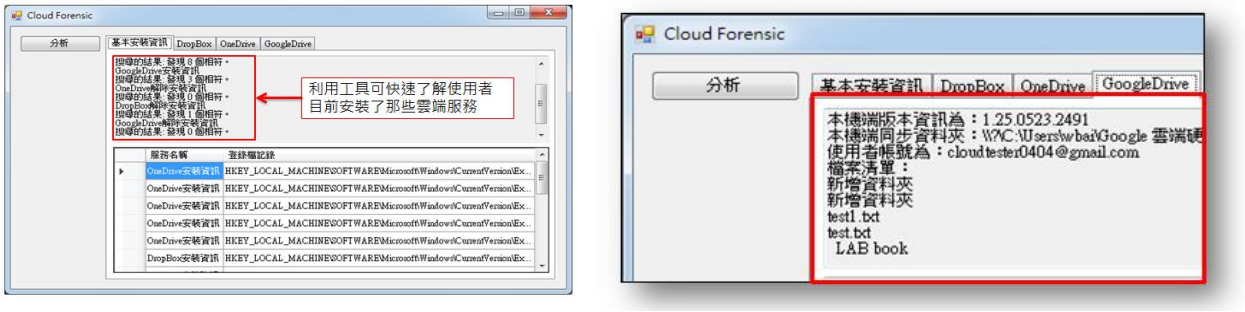
(5) ASUS WebStorage

表十一 ：ASUS WebStorage 執行雲端服務前後差異比較

狀態	種類	位置
同步	Registry	HKEY_CURRENT_USER\Software\ECAREME\OmniStore\yostore\<user account>\RecentSyncFiles\Files
同步	Registry	HKEY_USERS\S-1-5-21-2020062809-1800262464-634923857-1000\Software\ECAREME\OmniStore\yostore\<user account>\RecentSyncFiles\Files
同步	資料夾	C:\Asus WebStorage\<user account>\MySyncFolder\
同步	檔案	C:\Users\<username>\AppData\Roaming\WebStorage\Logs\Sync_Activity.Log
同步	檔案	C:\Users\<username>\AppData\Roaming\WebStorage\Logs\AWSService.Log
同步	資料夾	C:\Users\<username>\AppData\Roaming\WebStorage

3、 工具實作

本研究依據上述 Snapshot 差異比較後取得之證據清單，進行工具開發，藉由此工具可快速了解本機端是否使用相關雲端儲存服務。若於本機端安裝 Dropbox, Google Drive, OneDrive 雲端儲存服務應用程式，則可快速取得同步檔案清單，以便執法人員快速掌握目標主機使用雲端儲存服務之相關資訊。除了快速識別目標主機是否使用雲端儲存服務，本研究所實作之工具亦可針對主要雲端服務所留存之 Log 檔進行預覽，以便執法人員快速瞭解目標主機之資訊。實作成果如下圖所示：



圖三 ：雲端鑑識工具示意圖

4、 小結

綜合上述之證據清單可以得知，若安裝雲端儲存服務則留存之 Log 類型不同，資訊含量亦不同，若以瀏覽器使用雲端儲存服務，則本機端留存的 Log 數量將會更少。

本研究比對證據清單後彙整出雲端儲存服務相關資訊如下表：

表十二 ：各雲端儲存服務相關資訊彙整

	Dropbox	Google Drive	MS OneDrive	iCloud	ASUS WebStorage
預設資料夾路徑	C:\Users\<username>\Dropbox	C:\Users\<username>\Google 雲端硬碟	C:\Users\<username>\OneDrive	C:\Documents and Settings\<username>\iCloudDrive\	C:\Asus WebStorage\<username>
本機端留存之跡證類型	Log 登錄檔 同步檔案 記憶體資訊	Log 登錄檔 同步檔案 記憶體資訊	Log 登錄檔 同步檔案 記憶體資訊	Log 登錄檔 同步檔案 記憶體資訊	Log 登錄檔 同步檔案 記憶體資訊
本機端Log是否加密	是	否	否	否	否
本機端主要Log檔案名稱	filecache.dbx	snapshot.db sync_config.db sync_log.log	SyncDiagnositcs.log	asl.141827_27Oct15 icloudXXX.log	Sync_Activity.Log AWSService.Log
本機端log提供之資訊	本機端現有檔案	本機端現有檔案 使用者帳號	傳輸紀錄 資料夾數量 檔案數量	AppleID	本機端現有檔案 使用者帳號

現行市面上常見之雲端儲存服務存取媒介非常之多，諸如：手機、平板、電腦.....等，這些媒介之中的傳輸管道又可分為瀏覽器及應用程式傳輸。惟本研究針對個人電腦中的應用程式方式進行數位證據種類分析，可得知在個人電腦中，若以應用程式執行雲端儲存服務將可能包含數位證據如登錄值（Registry）、同步處理檔案及資料夾、Prefetch檔、記憶體資訊及Log。

二、 私有雲之常見數位證據種類

1、 安裝前後差異比較

如前所述，私有雲之特性皆為透過遠端執行虛擬機器載體，且透過瀏覽器執行虛擬機器設定，無須執行安裝作業，因此本機檔案及登錄值並無太大差異。

2、 執行雲端服務前後差異比較

(1) Amazon EC2

表十三 ：Amazon EC2 執行雲端服務前後差異比較

狀態	類型	位置
登入	檔案	C:\Documents and Settings\<user>\AppData\Local\Application Data\Google\ Chrome\User Data\Default\Local Storage\http_aws.amazon.com_0.localstorage
登入	檔案	C:\Documents and Settings\<user>\AppData\Local\Application Data\Google\ Chrome\User Data\Default\Local Storage\ http_aws.amazon.com_0.localstorage
啟用執行載體	檔案	C:\Documents and Settings\<user>\AppData\Local\Application Data\Google\ Chrome\User Data\Default\Local Storage\https_www.amazon.com_0.localstorage
遠端至VM	檔案	C:\Documents and Settings\<user>\AppData\Local\Application Data\Google\ Chrome\User Data\Default\Local Storage\ https_us-west-2.console.aws.amazon.com_0.localstorage
遠端至VM	Registry	HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default
遠端至VM	Registry	HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers

(2) hiCloud VPC

表十四 ：hiCloud VPC 執行雲端服務前後差異比較

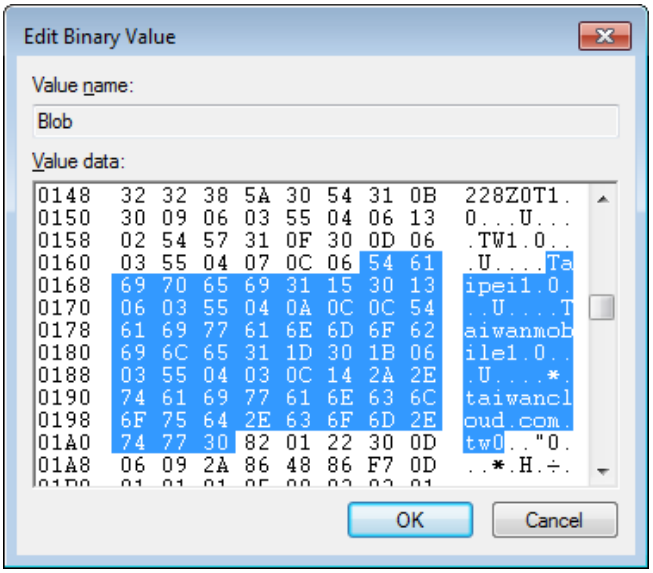
狀態	類型	位置
登入	資料夾	C:\Users\<user name>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5
登入	資料夾	C:\Users\<user name>\AppData\Local\Microsoft\Windows\WebCache
登入	資料夾	C:\Users\<user name>\AppData\Local\Microsoft\Windows\Caches
登入	資料夾	C:\Users\<user name>\AppData\Local\Microsoft\Windows\Explorer
登入	資料夾	C:\Users\<user name>\AppData\Local\Microsoft\Windows\History
遠端至VM	Registry	HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default
遠端至VM	Registry	HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers

(3) 台灣大哥大 IaaS

表十五 ：台灣大哥大 IaaS 執行雲端服務前後差異比較

狀態	類型	位置
登入	檔案	C:\Documents and Settings\<username>\AppData\Local\Application Data\Google\Chrome\User Data\Default\Login Data
登入	檔案	C:\Documents and Settings\<username>\AppData\Local\Application Data\Google\Chrome\User Data\Default\Cookies
登入	檔案	C:\Documents and Settings\<username>\AppData\Local\Application Data\Google\Chrome\User Data\Default\Network Action Predictor
登入	檔案	C:\Documents and Settings\<username>\AppData\Local\Application Data\Google\Chrome\User Data\Default\Web Data
登入	檔案	C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History
登入	Registry	HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\Root\Certificates\EA0CAAE638294899E9376AB14FB6546FE24C4B53
遠端至 VM	Registry	HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default
遠端至 VM	Registry	HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers

台灣大哥大 IaaS 服務於啟用後需另外安裝憑證，以便更方便使用服務，因此本研究於下列登錄值中找到台灣大哥大相關憑證登錄值，更可藉此證實目標主機使用台灣大哥大之 IaaS 服務，如下圖所示：



圖四 ：台灣大哥大 IaaS 服務登錄值憑證相關之資訊

(4) OpenStack

鑑識分析人員若需分析以 Openstack 為架構之虛擬平台時，可透過蒐集 Openstack 中各軟體套件日誌檔與相關設定檔，分析與案件相關之數位證據。建置 Openstack 後，預設之日誌路徑位於/var/log 下分別以各套件為命名之資料夾中，整理相關日誌名稱及路徑如下表：

表十六 ：Openstack 各套件日誌名稱及路徑

節點(Node)種類	日誌名稱	檔案路徑
Cloud controller	nova-*	/var/log/nova
	glance-*	/var/log/glance
	cinder-*	/var/log/cinder
	keystone-*	/var/log/keystone
	neutron-*	/var/log/neutron
	horizon	/var/log/apache2/*.log
All nodes	misc (swift, dnsmasq)	/var/log/syslog
Compute nodes	libvirt	/var/log/libvirt/libvirtd.log
	Console (boot up messages) for VM instances	/var/lib/nova/instances/instance-<instance id>/console.log
Block Storage nodes	cinder-volume	/var/log/cinder/cinder-volume.log

Nova 套件於 Openstack 虛擬平台中扮演重要角色，故以下針對該套件所留存之日誌檔案進一步說明各日誌檔案內容

表十七 ：Nova 套件中各種日誌名稱及路徑

日誌檔案	檔案路徑	敘述
nova-compute	/var/log/nova/nova-compute.log	使用者啟動或運作 Instance 之相關紀錄
nova-network	/var/log/nova/nova-network.log	記錄網路狀態、安全群組(Security group)等網路相關資訊
nova-manage	/var/log/nova/nova-manage.log	記錄使用者執行 Nova 套件之管理模組指令及結果
nova-scheduler	/var/log/nova/nova-scheduler.log	記錄使用者排程執行 Instance 作業或調整資源等資訊
nova-objectstore	/var/log/nova/nova-objectstore.log	記錄存在於 Openstack 之虛擬主機映像檔資訊
nova-api	/var/log/nova/nova-api.log	記錄 Nova-api 套件與其他 Openstack 套件相互作用之資訊
nova-cert	/var/log/nova/nova-cert.log	記錄 nova-cert 之執行結果
nova-console	/var/log/nova/nova-console.log	記錄使用者透過 Nova-console 連線進虛擬主機之作業
nova-consoleauth	/var/log/nova/nova-consoleauth.log	記錄 Nova-console 之帳號認證作業
nova-dhcpbridge	/var/log/nova/nova-dhcpbridge.log	記錄網路之 DHCP 及 Bridge 資訊

Openstack 建置過程中，需分別設定或修改各套件之設定檔案，其中包含可能有助於鑑識分析人員進行後續分析作業之參考設定值，如 IP、帳號密碼或特定資料庫名稱等資訊，整理如下表

表十八 ：Openstack 各設定檔名稱及路徑

設定檔	檔案路徑	敘述
my.cnf	/etc/mysql/my.cnf	mysql 之設定檔
keystone.conf	/etc/keystone/keystone.conf	該檔案中有連線網址、keystone 之帳號及密碼等資訊
creds	N/A	Creds 可由使用者自訂名稱及位置，內有 admin 之帳號密碼
glance-api.conf	/etc/glance/glance-api.conf	內有 Glance 套件之帳號密碼及網路、資料庫等連線資訊
glance-Registry.conf	/etc/glance/glance-Registry.conf	
nova.conf	/etc/nova/nova.conf	該檔案中有 openstack 存放路徑、IP、帳號密碼等多種重要資訊，是 openstack 最重要的設定檔之一
neutron.conf	/etc/neutron/neutron.conf	該檔案中有網路及 neutron 套件之帳號密碼等相關設定
metadata_agent.ini	/etc/neutron/metadata_agent.ini	

3、 小結

目前一般市面上常見的雲端服務提供商所提供之 IaaS 服務多半透過 VM 或 Web 方式存取，然而於本機端之取證絕大多數亦只能分析存取遠端服務之際議題及 Log 資訊，因此非自建之私有雲服務於本機端之鑑識作業多版僅能進行至識別階段。此外，後續取證作業涉及到所有資料都在網路端，建議藉由傳統數位鑑識工具遠端取證。

自建雲雖然自行管理軟硬體，有更多資訊可取得，仍建議先針對虛擬機執行取證，再進行整體雲端架構取證，如：儲存媒體、網路架構、運算資源等資訊之跡證取得。

常見之私有雲無論是自建或是商用，使用者皆由本機端設備透過網路存取雲端上之資訊，因此證據種類大致上皆可分為本機端證據及雲端證據兩面向。其中，本機端證據包含：遠端桌面紀錄、瀏覽器暫存檔案及記憶體資訊；雲端證據包含：虛擬主機資訊、記憶體資訊及儲存空間資訊。

除此之外，若是自建之私有雲，如：OpenStack，則除了上述資訊以外，還包含整體雲端硬體架構資訊。其中更牽涉到硬體架構之模式。因此本研究建議，對於自建私有雲之服務，除蒐集本機端及雲端之軟體資訊外，亦須對實體證據做取證動作。

伍、 結論與未來研究方向

本研究針對雲端儲存服務及私有雲服務進行實作測試，藉此了解雲端服務於本機端及雲端所留存之證據含量。經過部署實測後得知，雲端服務於本機端將留存下列主要資訊包含:應用程式紀錄、瀏覽器暫存檔、登錄檔、Prefetch 檔及記憶體資訊。

以雲端儲存服務而言，其所留存之記錄包含雲端檔案同步歷史資訊，甚至可回復已刪除之檔案。若以私有雲服務來說，則須視雲端服務提供商對於雲端虛擬環境之資料留存狀況而定。在雲端虛擬環境尚未完全刪除虛擬機的情況下，可使用一般數位鑑識工具，有限的擷取曾於虛擬機中刪除之檔案。但若完全刪除雲端虛擬機，則須視雲端服務提供商資料留存方式而定，目前仍未有雲端服務提供商針對已刪除之虛擬機進行資料還原的保證。本研究已進行常見之雲端服務於本機端或雲端所留存之證據進行識別，並將證據進行精簡，以期減少執法人員負擔，並於短時間內快速識別標的主機是否使用雲端服務。

近年來亦陸續有學者提出蒐證雲之概念，執法人員可藉由蒐證雲對標的主機，甚至是虛擬主機進行雲端取證作業。本研究期望後續能利用現有之蒐證程序、證據種類清單及蒐證技術，進一步進行蒐證雲之實作，降低蒐證人員於取證作業上之困難度，確保蒐證程序得以化繁為簡。

參考文獻

[1] J. Dykstra and A. T. Sherman, “Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques,” *Digital Investigation,* vol. 9, pp. S90-S98, 2012.

[2] M. Epifani, “Cloud Storage Forensics,” *SANS European Digital Forensics Summit,* 2013. https://digital-forensics.sans.org/summit-archives/Prague_Summit/Cloud_Storage_Forensics_Mattia_Eppifani.pdf

[3] B. Martini and K.K.R. Choo, “Cloud storage forensics: ownCloud as a case study,” *Digital Investigation,* pp. 287-299, 2013.

[4] F. Marturana, G. Me and S. Tacconi, “A case study on digital forensics in the cloud,” *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery,* pp. 111-116, 2012.

[5] S. Zawoad and R. Hasan, “Digital forensics in the cloud,” *ALABAMA UNIV IN BIRMINGHAM,* 2015. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA590911

[6] S. Zawoad and R. Hasan, “Cloud forensics: a meta-study of challenges, approaches, and open problems,” 2015
http://arxiv.org/pdf/1302.6312v1
[7] 鐘敏如，”檔案資料的雲端鑑識分析研究”，*碩士論文*，中央警察大學資訊管理研究所，2014。
[8] http://www.taiwancloud.com.tw/products/iaas/introduction/index.html (2015/11/18).
[9] http://aws.amazon.com/tw/s3/details/ (2015/11/18).
[10] http://twblog.asuswebstorage.com/2012/08/06/asuswebstoragesecurity/ (2015/11/18).
[11] https://www.asuswebstorage.com/navigate/features/ (2015/11/18).
[12] https://www.dropbox.com/en/help/28 (2015/11/18).
[13] https://support.apple.com/en-gb/HT202303 (2015/11/18).
[14] https://support.asuswebstorage.com/estorage/eservice/1028/FAQViewKBArticle.aspx?kbarticleid=7b59dfc5-caf6-e211-b540-00155d01c002 (2015/11/18).

[誌謝]
本研究承蒙 103 年行政院國家科學技術發展技術管理會補助計畫(計畫編號 MOST 103-3114-Y-138-003)之經費補助，謹此致謝。