Evidence Investigations in Forensics in Case of Clouding Access with Data Synchronizations

鐘敏如　　王旭正*
中央警察大學資訊管理學系
n397148625@hotmail.com　　sjwang@mail.cpu.edu.tw
* whom correspondence

摘要

雲端儲存服務提供組織或個人一個低成本且免費的存取及儲存和分享資料的功能，像是微軟的 Skydrive、Google 的 Google drive 或是 Dropbox。但在存取資料的同時，也會留下相當多的數位跡證。本文研究如何在電腦找到與雲端檔案同步後所留下的數位證據，及 Windows Phone8 對檔案更動後的情況，並分析當非法者利用 Skydrive 及 Windows Phone8 對 Office 檔案進行修改時，鑑識單位可以找出留存在電腦的數位證據，確認非法者的確有使用雲端儲存軟體進行溝通與管理。

關鍵詞：雲端儲存軟體、數位鑑識、Skydrive、Dropbox、Google Drive

1. 前言

雲端服務發展的目的主要是為了節省成本、避免風險並有效利用資源，在網際網路時代，無論是個人或組織都擁有屬於自己的資料，要有效儲存和管理這些資料，雲端服務就是一個很好的選擇。根據國際數據資訊中心（International Data Corporation）的調查資料中指出，未來五年亞太地區花費在雲端服務上的費用將成長四倍，並將在 2014 年以前達到 46 億美元；市場調查機構 Gartner 也預估雲端運算（Cloud Computing）市場規模於 2014 年達 1500 億美元。雲端儲存服務在近幾年越來越流行，使用者使用這些雲端服務來儲存、分享資料，在不同地方利用同步的特性存取相同的檔案。同步，是雲端儲存服務所共有的一項特性，使用者只要將桌面上的檔案移至雲端資料夾內，其檔案都會立即同步至雲端。不同以往需要利用隨身碟或其他裝置存取檔案，雲端儲存服務可以線上存取、同步、分享或儲存檔案，不論到何地都能進行操作。

目前較主流的、擁有最多使用者的雲端儲存服務分別為微軟的 Skydrive[1]、Dropbox[2-3] 及 Google 的 Google Drive[4]，三者支援平台都相當完整，除了在電腦上使用外，也提供平板及手機端的 APP 服務。近年來 3G 上網及無線上網服務的普及，大部分使用者多會利用電腦或手機將資料備份到雲端儲存軟體上。因此當非法者利用雲端運算服務進行非法行為時，相關的數位跡證不若以往個人電腦犯罪環境較易留下數位痕跡或範圍固定，取而代之是，非法行為可以在任何地點（Any Where）、任何時間（Any Time）利用雲端資源達成非法目的，且不易留下犯罪跡證[5-6]。這對鑑識單位來說是一項新的挑戰，要如何利用本地電腦端找出數位證據來證明非法者的非法行為就變得相當的重要。本文將研究與分析使用這些雲端儲存服務後，在電腦中遺留哪些數位證據，而這些證據與非法行為之間的關聯。

本文的結構如下:第二節介紹雲端儲存服務的相關背景。在第三節說明我們的鑑識方法，指出雲端儲存服務的證據隱藏在電腦端的何處。第四節討論分析。第五節則為本文的結論。

2. 相關背景

雲端儲存服務是一個新興的鑑識領域，雲端儲存服務的特點是能隨時隨地在有網路的情況下存取雲端內的資料，也由於這個特性，要正確找出數位證據證明非法者的行為就變得相當不容易。透過雲端資料夾，只要使用者進行檔案上傳或下載的動作，都會立即進行同步，更新雲端內的檔案，因此可以利用這個特性，找出使用者做了哪些新的更新。而其中證據的驗證、獲取和保存都可能在過程中被非法者給破壞，故本文以三種雲端儲存軟體分別為 Skydrive、Dropbox 及 Google Drive 為例，並運用 Quick 及 Choo [7-8]提到的鑑識方法為基礎，找出雲端儲存軟體遺留在電腦的數位證據，使得這些證據能清楚指出非法的活動，並得以實現鑑識還原事件真相的目的。

2.1 雲端儲存軟體

(1) Skydrive

Skydrive[1]是微軟提供的一個雲端儲存服務，它提供 7GB 的免費儲存空間，可在電腦及手機等平台使用。透過 Skydrive 同步應用程式的安裝，會在電腦端建立一資料夾，在此資料夾可以上傳及下載所有檔案。Skydrive 的另一特色是可在網頁中使用 Office Web Apps 服務直接檢視、建立、及編輯 office 文件。

(2) Google drive

Google drive[4]為 Google 所提供的雲端硬碟服務，提供 5GB 的免費儲存空間。除提供 Google 文件的建立及編輯外，還可設定與其他

使用者共用檔案，並調整共用的權限。Google drive 也可與 Gmail 及 Google+對應，直接在 Gmail 及 Google+附上 Google drive 的連結，達到文件、影片與相片的分享。

(3) Dropbox

Dropbox[2]是一個線上資料同步軟體，提供 2GB 的免費儲存空間。若使用者想增加雲端服務的儲存空間，可透過推薦好友使用 Dropbox 再獲得額外的空間。Dropbox 透過同步軟體的安裝，可以直接在電腦端產生一資料夾，在此資料夾可以進行資料的上傳、下載及同步功能。或是利用網頁登入方式，在不同的地方，存取相同的檔案，達到異地備份。

這三個雲端儲存軟體都是利用同步的概念來達到資料的儲存與分享，不管是在網路上或是電腦上將檔案作處理，只要將檔案放進雲端資料夾內，皆可立即進行同步，除了能立即備份外，同時讓檔案處於一個最新的狀態。

2.2 Quick- Choo 鑑識研究

在 2013 年，Quick 及 Choo[7-8]提到目前雲端儲存服務對鑑識領域來說是一項新的挑戰，非法者會利用雲端服務來製造實行非法行為的機會，例如在海外、在不同國家進行非法行為，這都將影響鑑識人員及司法人員的證據蒐集及調查。直接向雲端服務商取得數位證據並不是那麼的容易，而且會耗費相當多的時間，在這過程中數位證據就有被覆蓋或修改的可能。

Quick 及 Choo[7-8]提出了針對電腦端蒐集雲端儲存服務的數位證據方法，他們提出了一個分析的架構，以 Skydrive 為對象，從一開始的確定範圍，接著準備相關環境及作業，驗證和收集這些環境產出的證據，到事後的保存、分析、展現和回饋都是一步接一步，當分析遇到問題時，重新回到準備環境的環節，去修改實驗的狀況，依此循環，完成整個蒐集證據的程序。Quick 及 Choo[7-8]是利用 Virtual Machine 將雲端儲存軟體的使用情況先進行分類，探討使用者在利用電腦端和網頁登入 Skydrive 進行上傳、存取或下載資料後會遺留哪些數位證據，再對各個 VM 產生的 VMEM 檔及 VMDK 檔進行證據的獲取、驗證及保存，也利用 MD5 檢視檔案完整性，並針對電腦端的 log 檔、RAM 紀錄、網路端及瀏覽紀錄進行證據搜尋及探討，確定雲端儲存軟體在不同環境下的確會留下相當多證據。

2.3 Platforms in our Scheme

本文利用虛擬機器做為實驗的工具，主要是為了在不同雲端儲存軟體萃取證據時能夠不互相影響，以達到證據的完整性。並以 Windows Phone8 為主要的操作手機。

(1) 虛擬機器(Virtual Machine)

虛擬機器是虛擬化技術的其中一種軟體，它可以在主機上或是終端伺服器與終端使用者之間建立一種環境，創造出一台虛擬的硬體機器。目前市面上有許多不同的虛擬機器軟體能選用，例如 VMware、Microsoft、Citrix…等。以 VMware Workstation 為例，運行 VMware 後，會在電腦中留下相關操作、設定之檔案，例如: Vmdk、Vmem 檔。Vmdk 檔在虛擬機器中的角色如同電腦中的硬碟，Vmem 則扮演虛擬機器中的記憶體角色，它記錄虛擬機器存放於記憶體的資料，而本文中，也包含透過 Vmem 檔分析雲端儲存軟體的數位跡證。

(2) Windows Phone8(WP8)

Windows Phone8 為微軟所推出的以 Windows 為作業系統的手機，採用與 Windows 8 相同的核心。其特色包括可以自由更動動態磚的大小及位置，利用 Office365 直接在手機上建立、編輯 Office 文件，並選擇要將文件儲存在手機或雲端上。

本文除了以 Quick 等學者提到的鑑識方法為基礎，找出三種雲端儲存軟體遺留在電腦的數位證據外，並進一步找出當使用智慧型手機 Windows Phone8 存取雲端儲存服務時，會在電腦端留下哪些新證據，及如何找出這些證據，而這些證據與雲端檔案的關聯。

3. Forensic Scheme in Clouding Access of Data Synchronizations

我們所提出的雲端數位證據鑑識方法，以三種雲端儲存軟體，Skydrive、Dropbox 及 Google Drive 為例，透過相關檔案的建立及編輯過程，在三種 Virtual Machine 類型下找出遺留在 Client、Browser 及 RAM 的數位證據。利用檔案會立即在雲端資料夾內同步的特性，找出使用者在異地做了哪些新更動，並進行數位證據差異性的探討，鑑識方式:

(1) 將 VM 做三種類型區分。

(2) 運用檔案會進行同步的特性，找出這三種 VM 類型下，Skydrive、Dropbox 及 Google Drive 在 Client、Browser 及 RAM 的數位證據。

(3) 進行數位證據差異探討。

3.1 Model Organization

我們以 VMware Workstation9 建置 Windows8 作業系統，其硬體設定為 60GB 的硬碟空間及 1GB 大小的記憶體來進行存取三種雲端儲存軟體的證據蒐集。為了清楚界定證據蒐集的情況，我們將此次實驗分為三個方向，如表 1 所示:

(1) 至雲端儲存服務的網站下載同步軟體，透過此同步軟體產生在電腦端的資料夾，進行上傳檔案的動作，命名為 Upload-VM。

(2) 至雲端儲存服務的網頁，透過網頁直接登入，在瀏覽器上進行存取檔案的動作，命名為 Access-VM。

(3) 為第二種實驗的延伸，除了在網頁端存取檔案外，並將這些檔案下載至電腦裡，命名為 Download-VM。

第二種及第三種方向又可分為透過 Mozilla Firefox(FF)及 Google Chrome(GC)兩種瀏覽器登入

[9]。我們將電腦端產生的證據分為 Client Software Information 產生的紀錄檔、Browser Information 登錄的證據及 RAM Analysis 隨取記憶體的證據、跡證下去做說明。

表 1、Model setting

VM 類型	存取檔案方式	電腦端證據
Upload-VM	下載同步軟體並安裝置電腦，進行上傳檔案的動作	1.Client Software Information 產生的紀錄檔 2.Browser Information 登錄的證據 3.RAM Analysis 隨取記憶體的證據、跡證
Access-VM	透過網頁(FF、GC)直接登入，在瀏覽器上進行存取檔案的動作	
Download-VM	在網頁端(FF、GC)存取檔案外，並將這些檔案下載至電腦裡	

我們也進行以 Windows Phone8 存取雲端裡相同的檔案後，檢視是否會在電腦端留下新的數位證據。

藉由三種雲端儲存軟體在電腦中留存證據的比較，並檢視利用手機將雲端檔案做修改後在電腦的留存情況，能在電腦中找到相關證據，證明除了電腦可找到相關證據外，智慧型手機等可攜式裝置對檔案進行修改後也會在電腦端留下證據，並由這兩項證據來證明使用者或非法者確實有利用電腦及手機使用雲端儲存服務。

3.2 Evidence Investigations

我們將說明與比較三種實驗方向 Upload-VM、Access-VM 和 Download-VM，在三種雲端儲存服務 SkyDrive、Dropbox 和 Google Drive 在電腦裡的證據留存情況，而 Windows Phone8 對雲端檔案的修改將會在 RAM Analysis 隨取記憶體的證據、跡證下作探討:

(1) Skydrive

1. Client Software Information 產生的紀錄檔

Upload-VM 安裝同步軟體後會在電腦端產生一同步資料夾，資料夾的路徑為 C:\Users\[usersame]\SkyDrive。而 SkyDrive 相關資料會存在路徑為 C:\Users\[usersame]\AppData\Local\Microsoft\SkyDrive 之下，如圖 1 所示。

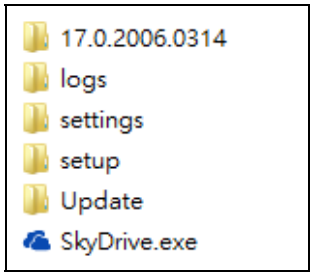

圖 1 SkyDrive 相關資料路徑

其中 17.0.2006.3004 為 Skydrive 的版本，logs 檔案夾裡面存在一 SyncDiagnostics.log 的檔案，裡面列出所有在 SkyDrive 的雲端和本地端檔案資訊，包括檔案大小、日期及時間，如圖 2 所示(檔案的日期及時間為 Unix 格式，使用者可透過時間轉換找出實際的時間)。4E2E9F3A273D1AC 為使用者使用 Skydrive 的 Owner ID，此 Owner ID 也同樣存在於 settings 資料夾下的.dat 及.ini 檔案裡，如圖 3 所示。

圖 2 SyncDiagnostics.log 檔案

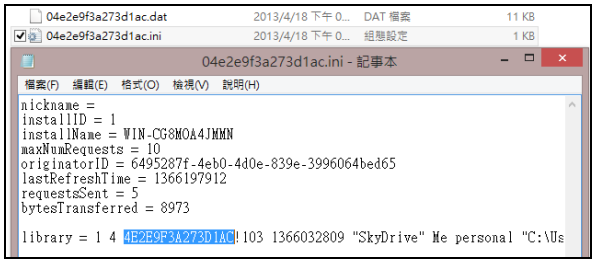

圖 3 .dat 及.ini 檔案

在微軟系統中，對於曾執行過的程式均會產生相對應的 PF 檔，因此可透過「.PF」檔檢查使用者是否曾經在電腦上執行 Skydrive，而產生的 PF 檔存放在「C:\WINDOWS\Prefetch」路徑下，如圖 4 所示，Skydrive 確實有在電腦上安裝、執行。

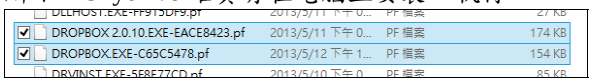

圖 4 Skydrive 的 Prefech 檔案

2. Browser Information 登錄的證據

Access-VM 和 Download-VM 分別利用 Firefox 及 Chrome 登入 Skydrive，可以在 Formhistory.sqlite 及 Web Data 找到使用者名稱。SQLite manager 直接檢視 Formhistory.sqlite 可以看到使用者登入的 Email，如圖 5 所示。SQLite Browser Database 檢視 Web Data 中的 Autofill 欄位也可以看到使用者登入的 Emai1，如圖 6 所示。

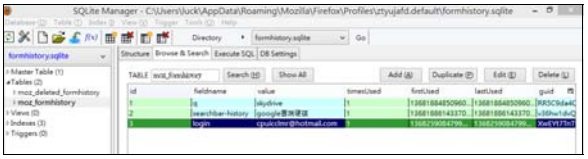

圖 5 Formhistory.sqlite 檔案

圖 6 Web Data 的 Autofill 欄位

3. RAM Analysis 隨取記憶體的證據、跡證

在 Winhex 下分析 Vmem 檔，Upload-VM 的使用者名稱及密碼會出現在&login 及&password 旁，如圖 7 所示。Access-VM 和 Download-VM 只能到使用者名稱。在 Download-VM 下，直接在 Skydrive 資料夾下找尋完整檔案內容。在 Access-VM 中，直接在線上的 Office web app 對檔案進行編輯，檔案的內文可以利用<w:t>或</w:t>來對 Vmem 檔搜尋，如圖 8 所示，出現在這中間的文字，及為檔案內的片段內文，再利用這些找到的片段內文拼湊起來，即為檔案的內文。對同步資料夾中的檔案進行編輯或是透過 WP8 手機對檔案進行編輯，相關的內文也都會以明文方式留存在電腦端的 RAM 記錄裡，對 RAM 進行搜尋時，也可以利用<w:t>或</w:t>這兩個關鍵字，拼湊出原始檔案內容。利用檔名在 RAM 裡進行搜尋，可以找到一些關於該檔案的，如圖 9 所示。

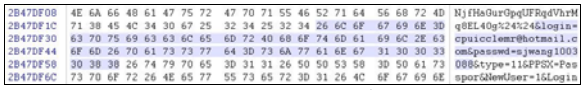

圖 7 Upload-VM 的使用者名稱、密碼

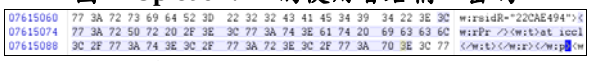

圖 8 線上 Office web app 編輯的內文

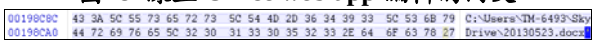

圖 9 檔案資訊

(2) Dropbox

1. Client Software Information 產生的紀錄檔

Upload-VM 安裝了同步軟體後會在電腦端產生一同步資料夾，資料夾的路徑為 C:\Users\[usersame]\Dropbox。而 Dropbox 相關資料會存在路徑為 C:\Users\[usersame]\AppData\Roaming\Dropbox 之下。我們可以檢驗 Dropbox 裡預設檔案的 MD5 value，檢驗的目的是當之後 Dropbox 版本更新時，檔案的 MD5 value 也會跟著改變，因此可透過這個方法確認 Dropbox 版本是不是有更動。在 Dropbox 資料夾下，.dbx 檔表示已經過加密，例如:儲存同步檔案名稱的 filecache.dbx。而.db 檔雖然未經過加密，例如:儲存檔案路徑的 host.db，但 Dropbox 目前已將這些資訊經過處理，我們無法解讀內文。這其中的原因可能來自 Dropbox 除了使用者本身使用之外，也可能與其他人共用檔案，為了保護相關資料的安全，所以 Dropbox 將這些檔案進行加密，避免發生例外的非法行為。

Dropbox 的 PF 檔存放在「C:\WINDOWS\Prefetch」路徑下，如圖 10 所示，Dropbox 確實有在電腦上安裝、執行。

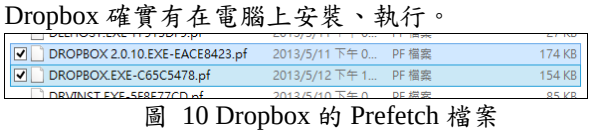

圖 10 Dropbox 的 Prefetch 檔案

2. Browser Information 登錄的證據

Access-VM 和 Download-VM 分別利用 Firefox 及 Chrome 登入 Dropbox，可以在 Formhistory.sqlite 及 Web Data 找到使用者名稱。SQLite manager 直接檢視 Formhistory.sqlite 可以看到使用者登入的 Email，如圖 11 所示。SQLite Browser Database 檢視 Web Data 中的 Autofill 欄位也可以看到使用者登入的 Emai1，如圖 12 所示。利用網頁登入也可以在記憶體裡面找到使用者名稱，使用者名稱存在關鍵字 login_email 旁，如圖 13 所示。

圖 11 Formhistory.sqlite 檔案

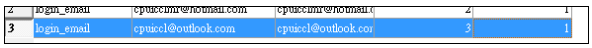

圖 12 Web Data 的 Autofill 欄位

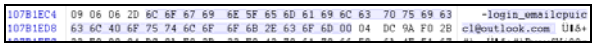

圖 13 記憶體裡的使用者名稱

3. RAM Analysis 隨取記憶體的證據、跡證

Upload-VM 登入 Dropbox 使用服務後，會在記憶體留下一些數位證據，在 'u' email ':' 關鍵字旁為使用者登入的名稱，'u' displayname ':' 旁為使用的電腦名稱，如圖 14 所示。

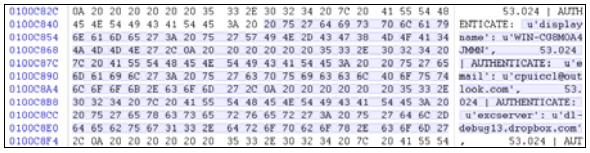

圖 14 Upload-VM 的 RAM

目前 WP8 手機內的 Dropbox APP 對 Office 的文件可以進行編輯，但由於設定的關係，檔案都為會以唯讀方式開啟，要再將修改後的檔案覆蓋原本 Dropbox 裡的原始檔案並不允許，只能將檔案存在手機上或是另存到 Skydrive 雲端空間，因此這部分對於 WP8 手機在同一檔案修改後本地電腦端記憶體留存的情況無法做進一步的驗證。

(3) Google Drive

1. Client Software Information 產生的紀錄檔

Upload-VM 安裝了同步軟體後會在電腦端產生一同步資料夾，資料夾的路徑為 C:\Users\[usersame]\ Google 雲端硬碟。而 Google Drive 相關資料會存在路徑為 C:\Users\TM-6493\AppData\Local\Google\Drive 之下。

2. Browser Information 登錄的證據

Access-VM 和 Download-VM 利用瀏覽器登入後，會在 C:\Users\TM-6493\AppData\Local\Google\Drive 資料夾下的 snapshot.db、sync_config.db 兩個 SQLite 的檔案留下紀錄。利用 SQLite manager 解讀後發現 snapshot.db 中的 cloud entry 和 local entry 儲存了 Google Drive 裡檔案的相關資訊。cloud entry 紀錄如圖 15 所示，其中各欄位的對照表如表 2 所示。

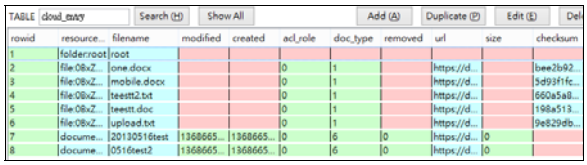

圖 15 cloud entry 紀錄

表 2 欄位資訊對照表

filename	檔案名稱
modified	修改時間
created	建立時間
Doc type	檔案類型
url	存取網址
size	大小
Checksum	雜湊值

各欄位說明如下：

(1) Filename：檔案名稱。值得注意的是不是每個檔案的副檔名都有顯示。事實上，所有從雲端上創造的檔案都沒有顯示副檔名，而是以 doc type 做區分。

(2) Modified：檔案被修改的時間，時間格式為 unixtime。

(3) Created：檔案被建立的時間。如果檔案是從本機端放進雲端則不會顯是建立時間。然而，不論在雲端或本機端修改都會顯示。

(4) Document type：建立的檔案類型。只有在雲端上建立的檔案才會有數字。檔案類型對照如表 3 所示。

表 3 檔案類型對照表

Doc type	檔案類型
0	資料夾
1	.doc、.xls 等多種副檔名皆適用
2	Google Presentation
3	無資料
4	Google Form
5	Google Drawing
6	Google Document
7	Google Table

(5) Size：檔案大小。若是資料夾，有檔案在裡面也不會顯示大小。

(6) Checksum：檔案的 MD5 雜湊值。從雲端上創造的檔案沒有 MD5 雜湊值，只有從本機端放置或上傳的才會有。

snapshot.db 中的 local_entry，如圖 16 所示，這區塊內含有本機端對 Google Drive 的操作行為。Filename 的部分可看見.doc 與.gdoc 的差別，.gdoc 為在雲端上直接建立的 Google 檔案。

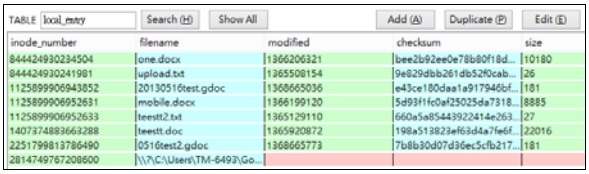

圖 16 local_entry

sync_config.db 檔案中存有使用者登入 Google Drive 的帳號，如圖 17 所示。

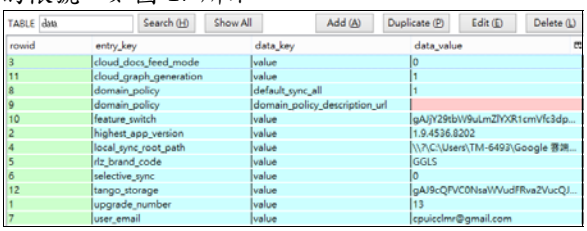

圖 17 sync_config.db

3. RAM Analysis 隨取記憶體的證據、跡證

Upload-VM 登入 Google drive 使用服務後，使用者登入的帳號可利用<email>及</email>關鍵字進行搜尋，結果如圖 18 所示。利用檔名做搜尋，相關的檔案資訊如圖 19 所示。

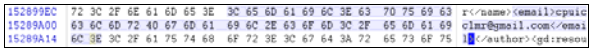

圖 18 使用者登入帳號

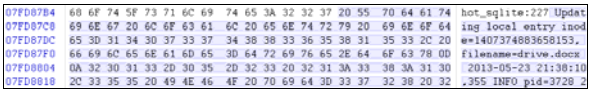

圖 19 檔案資訊

Google Drive 可以直接線上新增 Google 的文件或表單， 但目前 Google Drive 在 Windows Phone8 的 APP 還未完全支援，因此無法針對在 Windows Phone8 中的 Google 檔案進行修改是否會在本地端電腦的 RAM 中留下紀錄做驗證。

3.3 Report summaries

由實驗結果呈現，我們可以知道在不同的雲端儲存軟體下，在電腦中會找到不同的數位證據。在三種雲端硬碟下，皆可以找到雲端硬碟的相關檔案資料夾、Prefech 檔案、使用者利用瀏覽器登入的名稱及 E-mail，也找到一些關於各雲端硬碟獨有的數位證據，因此我們將這些結果整理成表格，如表 4 所示。

表 4 雲端儲存服務數位證據比較

	Client Software Information	Browser Information	RAM Analysis
Skydrive	同步資料夾、log 檔案、OwnerID、prefech	使用者名稱、登入的 E-mail	使用者名稱、密碼、與手機編輯後的檔案內文、檔案紀錄
Dropbox	同步資料夾、prefech、無法解讀的加密檔	使用者名稱、登入的 E-mail	使用者名稱、使用的電腦名稱
Google Drive	同步資料夾、prefech	檔案資訊、登入的 E-mail	使用者名稱、檔案紀錄

由表 4 中可以看到，這些雲端儲存軟體皆會產

生一同步資料夾，這個同步資料夾除了可以同步檔案外，我們也可以利用同步的特性，找出一些關於檔案更動後的數位跡證。使用者登入的名稱及E-mail也同樣可以被找到，這些登入名稱可以證明使用者或非法者曾經利用瀏覽器登入過雲端儲存軟體。我們可以發現Skydrive相較於其他兩種儲存軟體可以找到多一點的數位證據，在Skydrive下的RAM Analysis可以找到手機編輯後的內文，這個內文雖然是在手機裡面進行編輯的，但當電腦端將這個檔案打開後，這些被手機編輯過後的內文，依舊會出現在RAM紀錄裡，利用這個特性，可以證明非法者即使在其他地方編輯過相同檔案，其相關的紀錄還是會因電腦端開啟等修改、檢視動作留下些蛛絲馬跡。

4. 討論與分析

本文以三種雲端儲存軟體為例，探討數位證據留存在電腦中的情況，由我們的方法可以找到在Client Software Information產生的紀錄檔、Browser Information登錄的證據及RAM Analysis隨取記憶體的數位證據。雲端硬碟的相關檔案資料夾、Prefech檔案、使用者利用瀏覽器登入的名稱及E-mail及一些獨有的數位證據皆能被找到來證明使用者的使用情形。這些數位證據可以克服無法直接向雲端服務商取得證據時派上用場，透過這些證據的蒐集，將使用過的紀錄及內文突顯出來，證明使用者或非法者確實曾經使用過雲端儲存軟體。

實驗過程中發現Windows Phone8目前只支援Skydrive APP的檔案內文直接編輯，還未能直接編輯Dropbox及Google drive APP內的檔案。而本文也找了Android手機及iPhone來進行測試。發現Android手機無法支援Skydrive APP的檔案內文直接編輯，但能對Dropbox及Google drive APP裡的檔案進行下載檔案後再更新上傳的動作。iPhone無法支援Skydrive、Dropbox APP的檔案內文直接編輯，但在Google drive內能對Google文件進行編輯。相關差異比較如表5所示。這些差異是因為目前手機作業系統及APP支援程度不同所造成的影響，未來的研究將朝此方向繼續發展，比較多台手機對多種雲端儲存軟體數位證據的比較或是進行共同作者對雲端檔案編輯後的數位證據情況。

表 5 雲端軟體與手機 APP 支援程度

	Windows Phone8	Android	iPhone
Sky drive	可直接進行線上編輯	只能觀看文件內容，無法直接編輯	只能觀看文件內容，無法直接編輯
Dropbox	可編輯，但無法以修改後檔案覆蓋原始檔案。	可以編輯並上傳	只能觀看文件內容，無法直接編輯
Google Drive	App還未完全支援	可以編輯Google檔案；Office檔案可以編輯，但無法上傳覆蓋原本檔案	可以編輯Google檔案；Office檔案只能觀看文件內容

5. 結論

雲端儲存服務越來越多元，使用人數也隨著時間逐步成長，除了利用電腦上的雲端資料夾來備份資料外，有行動裝置的使用者也會使用雲端儲存服務來儲存、備份資料。但是使用這些雲端服務帶來便利的同時，也可能成為非法者的非法工具，例如拿來記錄或輔助非法行為等等。蒐集雲端上的數位證據並不是那麼容易，利用本研究提出的方法可以克服無法向雲端服務商獲取證據時使用。本文利用三種常見的雲端儲存服務軟體Skydrive、Dropbox及Google drive結合相關研究為基礎，進一步對雲端檔案操作後的數位證據進行探討，發現每個雲端儲存軟體皆會在電腦端、記憶體及瀏覽器留下獨有的數位證據。本研究提出的鑑識方法可以使鑑識人員在面對非法者利用雲端進行非法行為時，有一套依循的證據蒐集方法，利用本方法能證實非法者的確有使用雲端儲存軟體，而操作雲端儲存軟體的相關證據，即使非法者將雲端檔案進行刪除，其相關的非法行為依然可依本研究蒐集重要證據以為還原真相的依據。

參考文獻

[1] Skydrive Inc. Retrieved May 23, 2013, from http://windows.microsoft.com/zh-tw/skydrive/download

[2] Dropbox Inc. Retrieved May 23, 2013, from https://www.dropbox.com/

[3] McClain, F., Dropbox forensics. Forensic Focus, 2011, from http://www.forensicfocus.com/Dropbox-forensics.

[4] Google drive Inc. Retrieved May 23, 2013, from http://www.google.com/intl/zh-TW/drive/start/

[5] Chung, H., Park, J., Lee, S., and Kang, C., “Digital forensic investigation of cloud storage services, ” *Digital Investigation*, Vol. 9, Issue 2, November 2012, pp. 81–95.

[6] Reilly, D., Wren, C., and Berry, T. , “Cloud computing: Pros and Cons for computer forensic investigations, ” *International Journal of Multimedia and Image Processing (IJMIP)*, Vo. 1, Issue 1, March 2011, pp. 26-34.

[7] Quick, D., and Choo, K. K. R., “Dropbox analysis: Data remnants on user machines,” *Digital Investigation*, Vol. 10, Issue 1, June 2013, pp. 3–18.

[8] Quick, D., and Choo, K. K. R., “Digital droplets: Microsoft SkyDrive forensic data remnants,” *Digital Investigation*, Vol. 29, Issue 6, August 2013, pp. 1378–1394.

[9] Birk, D., and Wegener, C., “Technical issues of forensic investigations in cloud computing environments,” *In Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on* , May 2011, pp. 1-10.