

- 年輕人的新天堂—Instagram 的一線情：鮮與險 -

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

柯宏叡-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/>)。 >

摘要

Instagram 是以分享圖片、影片為主的社交網路 App，近年來的使用者成長快速，並且相當受到年輕人的歡迎。然而 Instagram 也可能被用來進行人身攻擊等行為，因此我們需要解析 Instagram 來查知犯罪者行為。而由於 Instagram 多是以手機 App 進行操作，因此如何透過分析 Instagram 在手機中所儲存的資訊，藉此分析出手機使用者從事的社交活動來幫助釐清事情真相，更是相形重要。因此我們將就使用者操作 Instagram 的 App 時產生的相關訊息所儲存在手機記憶空間的位置進行實測，找出可能的相關跡證。

壹、前言

智慧型手機在這十幾年來已逐步成為許多民眾的基本需求，許多智慧型手機的使用者不只依靠手機來瀏覽網站、收發電子郵件，更是花費大量的時間使用不同的社交網路應用程式（Social Networking Applications，SNAs），諸如 Facebook、LINE、Instagram、Twitter 等。依據 DATAREPORTAL 網站的資訊（<https://datareportal.com/social-media-users>），至 2020 年 4 月已有 38 億的社交網路使用者，將近全球 49% 的人口！相較 2019 年的使用者數更是增加了約 3 百多萬人，增幅約 8.7%。

然而高度使用社交網路平臺也導致的新型態的網路犯罪事件發生，例如網路霸凌、社交騷擾、暴力行為現場直播等。對於許多使用者來說，尤其是青少年，智慧型手機最大的用途是社交。SNAs 允許使用者建立帳號，上傳圖片、影片、所在位置等個人資訊，並通過私人訊息或公開貼文分享這些資訊。這種現象給犯罪者提供了一個公開的機會來取得使用者的個人資訊，從而引起通過 SNAs 進行網路欺凌、跟蹤、性騷擾和侮辱等行為。因此，我們有需要能對可能涉及犯罪的智慧型手機及所安裝的 SNAs 進行鑑識分析。若由執法單位進行鑑識，通常會透過專業鑑識工具如 Magnet Axiom、Autopsy、XRY 等來進行，對於在手機蒐證上更為容易。然而這些專業鑑識工具有有的所費不貲，有的安裝使用上較為難以上手，故為使讀者們也能一同了解鑑識的標的與方法，在本文中僅就 Android 智慧手機上的 Instagram 進行鑑識分析，透過資料夾與檔案的分析檢視，來找出 Instagram 有那些資料存在於設備的內部記憶體中可做為重要的證據。

另外 Facebook 也正在推動整合 Instagram 與 Facebook 的聊天功能，這些的因素都將對鑑識人員造成相當的挑戰，也惟有持續努力跟上最新的系統、程式與工具，方能讓犯罪者無所遁形。

貳、背景知識

一、Android 系統

目前的智慧型手機主要可分為 Android、iOS 這兩種系統，其中 Android 原是 Google 公司基於 Linux 核心所開發的軟體平台和作業系統，之後並與硬體製造商、軟體開發商及電信營運商成立「開放手機聯盟（Open Handset Alliance）」來共同研發改良 Android 系統。因 Android 為開放原始碼，Google 公司將 AOSP（Android Open-Source Project）免費提供給全球廠商使用，因此相當受到許多廠商的歡迎，在全球智慧手機市場中已佔有約八成的比重。

Android 是以 Linux 為核心所建構的開放原始碼作業系統，系統架構分為四層，包含最底層的 Linux 核心（Linux Kernel）、第二層為 C 語言函式庫（Libraries）及執行環境（Android Runtime）、第三層為應用程式框架（JAVA API Framework），而最上層是應用程式（System Apps），如電話、相機、電話簿、電子郵件等，也是我們最能直接使用的部分。



圖 1： Android 系統架構

Android 系統中每個應用程式會分配到一個獨特的 id (Uid)。每個應用程式都在一個單獨的行程中運行，因此沒有那一個應用程式可以直接取得其他應用程式的資料。對於鑑識人員來說，Android 手機的資料夾結構是最值得探索的區域，相關的資訊或是潛在的證據都可能在相關的資料夾中取得。手機 App 可以通過多種方式儲存資料，通過對 App 進行鑑識分析，鑑識人員可以瞭解 App 的使用情況，以及取得使用者的相關資料，如使用者什麼時候在那一個特定的地點，或者他們何時與誰進行交流以及曾經發布那些訊息等。這些重要的證據與相關的訊息大都直接存放於手機內的資料夾，因此鑑識人員即使擁有強大的鑑識工具軟體，也需要去了解 App 的資料儲存架構，才能便於萃取出相關跡證。本文將以 Android 手機為主進行數位鑑識，並利用 Android 手機數位鑑識技術進行社群網站 App 的鑑識，而能在基本工具操作下得以萃取出 Instagram 中的相關資訊。

二、Instagram

Instagram 是由 Kevin Systrom 和 Mike Krieger 所共同創立，並於 2010 年 10 月首次推出，是一個提供免費線上圖片及視訊分享的社交應用程式。使用者可以用智慧型手機拍下照片，再利用其內建的濾鏡效果添加到照片上，分享至 Instagram 或其他社交網路，也可以關注其他使用者的分享、建立好友關係、互相分享或收藏等等。Instagram 為專門發表圖片或短片的應用程式，內建的相機濾鏡功能，能夠為相片營造不同效果；另外無需提供詳細的個人資料，介面相對簡單易用，使得 Instagram 相當受到歡迎，據報導全球使用者已超過 10 億，而且是每個月都會上線的使用者。即使在 2012 年時，Facebook 以 10 億美金收購了 Instagram，Instagram 的使用者還是持續高速成長，而當時的使用者數還不到 4,000 萬個。

依據台灣網路資訊中心發佈「2019 台灣網路報告」，12 歲以上上網率達 88.8%，行動上網率亦有 85.2%。在「社群媒體」的調查結果，社群使用率達 79.2%，可見台灣目前不論是上網人口還是社群軟體使用者均相當普及。在各個社群媒體中，使用最高的是 Facebook，使用率達 98.9%，各個年齡層的使用率均超過 9 成，

最低的使用率是 95.7%，落在 15 至 19 歲這個年齡層。其次則是 Instagram 的 38.8%，其他的社群媒體如 Twitter、PTT、Dcard 等使用率均低於 10%，落差相當明顯。

Instagram 的使用率雖然落後 Facebook，但還是遠高於其他社交媒體，而在使用的年齡層上，多落在 12 至 34 歲的年輕族群，40 歲以上的使用率低於 3 成，而最高的使用率 72%則是落在 15 至 19 歲，與 Facebook 的年齡層分布有很大的不同。Instagram 與 Facebook 相較，主要的不同點如下：

1. 操作方式：Instagram 的界面設計較適合以手機操作，使用者也多以手機 App 來拍照分享，配合內建濾鏡與調整明暗對比就能完成美照。Facebook 有符合一般電腦的操作界面，使用者不一定會使用手機的 APP 來使用。
2. 成長幅度：Instagram 的使用者數成長幅度均較 Facebook 來得高。Facebook 於 2012 年的使用者數達 10 億，迄今已達到 26 億，成長約 2.6 倍；Instagram 從 2012 年的使用者數 3000 萬迄今達 10 億，成長約 33 倍！
3. 操作界面：Instagram 操作方式較為簡便，主要是以照片分享為主；相較 Facebook 複雜的版面，Instagram 顯得簡單明瞭。
4. 標籤（#）：Instagram 許多人會使用標籤（hashtag），只要在字句前加上#，便形成一個標籤，透過標籤來標定特定主題或特定人，其他使用者就可以很快找到相關貼文進行互動。
5. 聊天功能：對於手機使用者來說，Facebook 的聊天目前皆需另外下載 Messenger 這個 App 來進行；而 Instagram 的聊天功能目前相對單純，也還無需另外下載其他 App 來進行聊天。

在此，我們彙整上述訊息，將 Facebook 與 Instagram 的比較簡要列出如表 1 所示。

對於年輕人來說，Instagram 顯得更為「新鮮」且較為「酷炫」，可與同儕比較誰帥誰美、誰的穿著更好、誰又去吃美食等等，而且使用者年齡層較輕，因此

更容易找到年齡相近的朋友並獲得認同。內建的濾鏡效果降低了使用者調整相片的門檻，也讓使用者為了展示出較佳的相片，願意花更多的心思去調整，好吸引別人的注目，也因此貼文的量不太會多，使用者較能看到想到的訊息，而不會被太多無關的廣告干擾。另外，Instagram 上目前沒有太多長輩加入，所以年輕人更可以在這個平臺上貼上充滿自信的照片並與朋友互動，而不用擔心被長輩責問。這些與 Instagram 相關訊息、互動等，由於多是透過手機 App 來進行，因此對於鑑識人員來說，若要找出相關跡證，如何手機上針對 App 進行鑑識更是相當重要。

表 1：Instagram 與 Facebook 比較

比較	Instagram	Facebook
成立時間	2010 年 10 月 6 日	2004 年 2 月 4 日
使用者數（每用活躍用戶）	約 10 億	約 26 億
年齡族群	以年輕人為主	各年齡層皆有
操作方式	以手機 App 為主	電腦、手機
成長幅度	快速	趨緩
貼文	需有照片或影片	無照片亦可
頁面	簡單明瞭	複雜，廣告較多
儲存照片	不行	可
聊天功能	Direct	Messenger
標籤（#）	較多人使用	較少人使用
搜尋功能	方便找相關主題	方便找到個人帳號
社團	無	有

三、Instagram 的操作使用

在手機上透過 Play 商店安裝 Instagram，完成安裝後先申請帳號後進行登入

就可使用。接著，可以利用下方的工具列來搜尋、發佈貼文、好友活動等，如圖 2 所示。還可以使用內建的相機或直接上傳來分享相片，利用其內建的濾鏡功能修改圖片，並在圖片上標註人名、地點以及附加相片解說等，如圖 3 所示。



圖 2：Instagram 主畫面



圖 3：Instagram 貼文

參、鑑識討論

一、進行鑑識方法包括三個步驟，下面進行說明。

- (一)、 場景建立：通過在應用程式上執行常見的使用者活動來建立調查場景。應用程式安裝在手機上從 Play 商店。安裝完成後，我們開始操作建立帳號、上傳圖片與影片、追蹤好友動態、進行搜尋、瀏覽動態消息、查看使用者資料、傳送訊息給朋友等操作。我們的操作環境與軟體版本如表 2 所示。
- (二)、 獲取權限：為了最大限度的獲取設備內部記憶體資料，我們需要能對設備進行高權限的存取，以獲得完整的資料。為此，我們使用第三方的 TWRP 復原模式，藉此在復原模式下安裝 SuperSU 或 Magisk 對手機進行 root，以獲得超級使用者的權限，也才能存取系統的資料夾。
- (三)、 分析階段：在分析階段，我們就 Instagram 所可能存取的資料來找出對應的資料夾，藉此發掘可能可以做為證據的資訊。

表 2：實驗環境

裝置或工具	說明	版本
Samsung Galaxy S10	Android 系統手機	Android 5.1.1
Instagram	社交軟體	158.0.0.30.123
DB Browser for SQLite	SQLite 資料庫管理工具	3.12.0
Root Explorer	瀏覽資料夾工具	4.8.2

二、鑑識結果分析

在 Instagram 中，每個使用者也都有一個 id 做為識別，我們這裡的使用者 ID

為 38943837947，透過這個 ID 我們就能逐步解析出使用者的相關紀錄軌跡，相關的資料所在目錄如表 3 所示。

表 3：Instagram 相關資料夾

目錄	相關資訊
/data/data/com.instagram.android/databases/direct.db	訊息傳送者與接收者的 id 及時戳
/data/data/com.instagram.android/databases/direct.db-journal	與其他使用者傳訊的紀錄，包括 id 與時戳
/data/media/0/Android/data/com.instagram.android/files/	使用者上傳影片的預覽圖
/data/com.instagram.android/cache/images	使用者所瀏覽過的影像
/data/com.instagram.android/shared_prefs/rti.mqtt.ids.xml	connection key 與 device id
/data/com.instagram.android/shared_prefs /com.instagram.android_preferences.xml	使用者近期的登入紀錄
/data/com.instagram.android/shared_prefs/ 38943837947_usersBootstrapServices.xml	使用者所追蹤的帳號資料
/storage/sdcard0/Pictures/Instagram/	使用者上傳的相片
/storage/sdcard0/Movies/Instagram/	使用者上傳的影片

需要注意的是，Android 系統內的時間表示並不是直接採用年月日的方式，多是採用時戳的方式來顯示。我們以 rti.mqtt.ids.xml 為例如圖 4 所示，我們可以見到 timestamp 的值為 1594366368373，這個數值通常被稱為 Unix 時間戳（Unix Timestamp）。這個時間戳是自 1970 年 1 月 1 日（00:00:00 GMT）以來的秒數，透過轉換工具後我們可以得到：2020 年 07 月 10 日 15 點 32 分 48 秒，也就是這個時戳所代表的時間。

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="/settings/mqtt/id/connection_key">407350448330517</string>
  <string name="/settings/mqtt/id/mqtt_device_id">9dae70a8-b568-4b0a-ba5a-a9a115ead5b2</string>
  <long name="/settings/mqtt/id/timestamp" value="1594366369373"/>
  <string name="/settings/mqtt/id/mqtt_device_secret">ebQNYNXOVbXOUWUKlBm8wX6Kc/s=</string>
  <string name="/settings/mqtt/id/connection_secret">LCJa6tx43pBuwcIqLm1TdGFLCf4=</string>
</map>
```

圖 4：rti.mqtt.ids.xml 內容

肆、模擬情境

甲與乙兩位男姓員工為公司同事，然而為了丙女爭風吃醋，甲男與乙男於口角之後，甲男就於 Instagram 對乙男傳訊威脅訊息，並傳送不雅相片。乙因此氣憤不過報告上級經理處理。

經理詢問甲是否有傳訊威脅訊息時，甲則是辯稱是帳號被盜用所致。為此，經理請甲交出手機予資訊部門查核。資訊部門在獲得的甲的同意之下取得 root 權限，透過相關的資料夾與檔案分析。首先在：

/data/data/com.instagram.android/databases/direct.db

這個資料夾下就找到相關的傳訊紀錄，包括使用的 ID 與時戳，如圖 5 所示。接下來資訊部門再找尋近期的使用紀錄，在資料夾：

/data/com.instagram.android/shared_prefs/com.instagram.android_preferences.xml

中找到近期的使用時間（時戳）為 1600227080150，如圖 6 所示。1600227080150 換算過來的時間為 2020 年 9 月 16 日 11 時 31 分。之後資訊部分再清查相關的快取檔案，在資料夾：

/data/com.instagram.android/cache/images

發現到所上傳的不雅相片。由於 Instagram 相片上傳均需透過手機 App 操作，因此證據只會留存在這臺手機上，即使使用者刪除了原本的檔案，但在 cache 資料夾還是可以發現蹤跡。至此，甲終於承認的確是他個人的行為，願意接受公司的處分。

	_id	user_id	server_item_id	client_item_id	thread_id	recipient_ids	timestamp	message_type
1	150	38943837947	29471381515096811296643681542471680	6701016315051777132	340282366841710300949128387524022450417	1473458064	15997646793240855	text
2	151	38943837947	29510104377551988040728410207551488	6709820893363179851	340282366841710300949128387524022450417	1473458064	1599745963820793	text
3	152	38943837947	29510104433620147229749717671870464	6709820906434860896	340282366841710300949128387524022450417	1473458064	1599745966860254	text
4	153	38943837947	29510104677265074996698802187927552	6709820961808103109	340282366841710300949128387524022450417	1473458064	1599745980068272	text
5	154	38943837947	29511019776561090532843870304075776	6710029032277086573	340282366841710300949128387524022450417	1473458064	1599795587700511	text
6	155	38943837947	29511021728000327321762236207202304	6710029475866589267	340282366841710300949128387524022450417	1473458064	1599795693488244	text
7	156	38943837947	2951102211668733968089529660211200	6710029538641250703	340282366841710300949128387524022450417	1473458064	1599795714286950	media

圖 5：Instagram 傳訊紀錄

```
<int name="preference_referral_logging_attempt_count" value="0" />
<string name="arlink_model_version">2.2.1</string>
<long name="last_app_start_timestamp" value="1600227080150" />
```

圖 6：Instagram 上線使用時間

伍、結語

使用智慧手機和 SNA 的網路犯罪增加，進行鑑識分析人員需要對相關產品與系統的發展都要有相當的認知，方能事半功倍進行證據萃取。然而目前市場上不斷有新的智慧手機推出，造成了設備製造商之間的激烈競爭，導致使用者頻繁更換手機，追求更好的作業系統、系統晶片、資料儲存、使用者體驗等等。Instagram 透過簡單明瞭的界面，方便好用的濾鏡等功能，擄獲年輕人喜好「新」、「酷」、「簡單易用」的心，因此在許多的社交網路應用程式中脫穎而出。然而年輕人有時的一時衝動，直接透過 Instagram 就發動了犯罪行為，殊為可惜。本文中，我們透過案例來說明，透過 Instagram 的犯罪行為，即使非專業的執法機關，也能運用相關的技術與知識來找出潛在的證據，讓犯罪者無所遁形。藉此對於現今方便的社交網路應用程式，年輕族群的使用過程得更是謹慎！