



臺灣大學計算機及資訊網路中心電子報

投稿日期	民國 105 年 2 月 19 日	編 號	請空 白
投稿類別	<input type="checkbox"/> 校務服務 <input checked="" type="checkbox"/> 技術論壇 <input type="checkbox"/> 專題報導		
題目標題	"True Delete" 隱私權與 Line		
摘要	<p>在台灣，24 歲以下的年輕人在社交工具的選擇上，LINE 的使用率高達八成五，僅次於 Facebook 的九成四，並且不同年齡層的使用率相差不到 10%，LINE 儼然成為國人最常使用的手機通訊軟體之一，而資料隱私成為重要課題。</p> <p>因應此趨勢，LINE 5.3 版本中，新增了完整刪除(True delete)功能，本報告將探討有關通訊軟體 LINE 的隱私權相關議題。</p>		
姓名	李美雯		
服務機構/ 職稱	臺灣大學計算機及資訊網路中心		
聯絡電話	0233665010		
電子郵件 信箱	mli@ntu.edu.tw		
聯絡地址	106 台北市羅斯福路四段 1 號		
備註			

"True Delete" 隱私權與 Line

李美雯

臺灣大學計算機及資訊網路中心程式設計師

作者：轉載自臺灣大學計資中心北區學術資訊安全維運中心

1. 智慧型手機即時通訊軟體及 LINE 簡介

根據資策會在 2014 年底進行的調查顯示，截至 2014 年底，台灣智慧手機的普及率已經超過六成五，約有 1355 萬人的使用量，並且預估手機市場未來將在 2016 年左右達到飽和，距離人手一台智慧型手機的目標又更加接近了。

而在手機的產業面上，手機通訊市場向來是廠商非常重視的一級戰區，創市際市場研究顧問公司便針對兩岸在手機即時通訊軟體的使用率進行五百個樣本數的抽樣調查，發現大陸主要由「微信 Wechat」和「QQ」為主，台灣則是幾乎由「LINE」獨佔整個即時通訊市場。

	台灣	大陸
No.1	 82%	 49%
No.2	 10%	 40%
No.3	其他 3%	其他 8%

Base: 台灣受訪者 N=500

大陸受訪者 N=500

圖 1 兩岸最常使用的手機即時通訊軟體（轉載自創市際市場研究顧問）

而天下雜誌在 2015 年時，針對經常使用 3C 產品的民眾進行一萬筆樣本數的抽樣調查，發現 24 歲以下的年輕人在社交工具的選擇上，LINE 的使用率高達八成五，僅次於 Facebook 的九成四，並且不同年齡層的使用率相差不到 10%，LINE 儼然成為國人最常使用的手機通訊軟體之一。

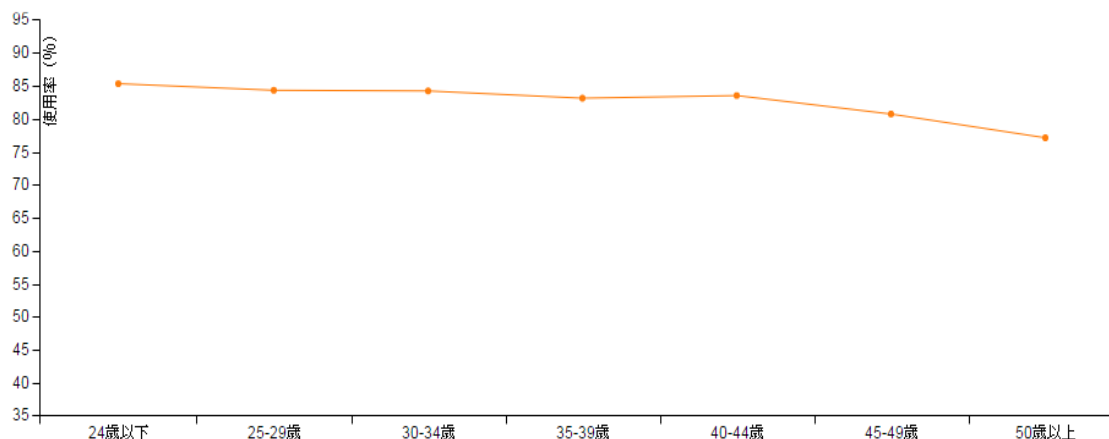


圖 2 各個年齡層 LINE 的使用率分布圖（轉載自天下雜誌）

LINE 最早由 2000 年創立的「ハンゲームジャパン株式會社」所開發，為南韓 Naver 設立於日本的子公司。後續經過改組、整併後，於 2013 年正式更名為「LINE 株式会社」。而 LINE 於於 2011 年 6 月正式對外發表，最初和其他 APP 通訊軟體一樣，強調只需透過網路即可傳遞文字訊息和網頁連結，而其主打的大型「貼圖功能」在當時為數不多的 APP 通訊軟體中算是最引人注目的，當中的可愛貼圖和情境貼圖受到眾多女性使用者的青睞。

LINE 的服務性質類似傳統手機使用的簡訊及多媒體簡訊功能，並且也因為封包是透過網路進行傳輸，所以也具有網路電話的功能，因此在智慧型手機具有上網功能的情況下，LINE 已經開始逐漸取代傳統通訊的高額費用，可以預見在網路費率降低及穩定度提升的未來，LINE 將更能貼近人與人之間的溝通。

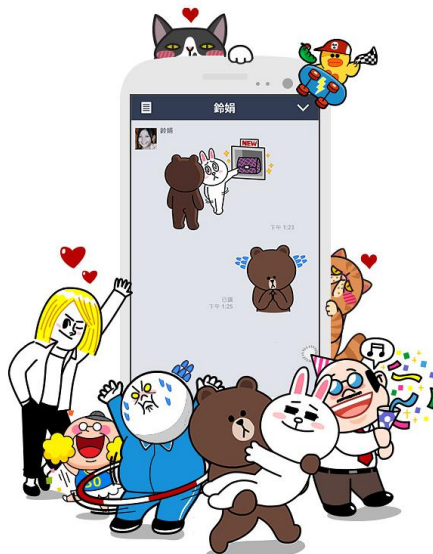


圖 3 LINE 主打的貼圖功能（轉載自 LINE）

2. LINE 訊息儲存與刪除之機制

因 LINE 的方便性而普及率高，卻也衍伸出許多隱私權上的問題。透過手機將 LINE 發送出去，即使事後將該則訊息甚至整個訊息群組刪除，仍然可能被有心人士復原查看內容，例如徵信社透過委託人取得對方手機後，將手機內的資料備份下來分析通訊軟體中是否有相關證據，或是家人之間透過 LINE 傳送信用卡、銀行帳號密碼，在手機遺失後，這些重要的資料被他人抽取出來。而在商業上或是政府機關利用 Line 往來的相關訊息，駭客同樣有可能透過相關手法將資料提取出來，就算事後將訊息刪除了，仍然無法獲得最安全的保障。

LINE 在刪除後仍能將訊息回復，主要原因在於手機系統對資料的管理方式，通常手機為了能方便查閱歷史資料，以及降低訊息傳輸造成的延遲，會將傳送完畢的訊息存放在指定 LINE 資料夾內的 SQLite 上，因此當使用者將視窗往上滑動翻閱歷史訊息時，LINE 便會將 SQLite 內的訊息即時讀取並顯示在螢幕上，就算在沒有網路的環境下，仍然能查閱歷史訊息。

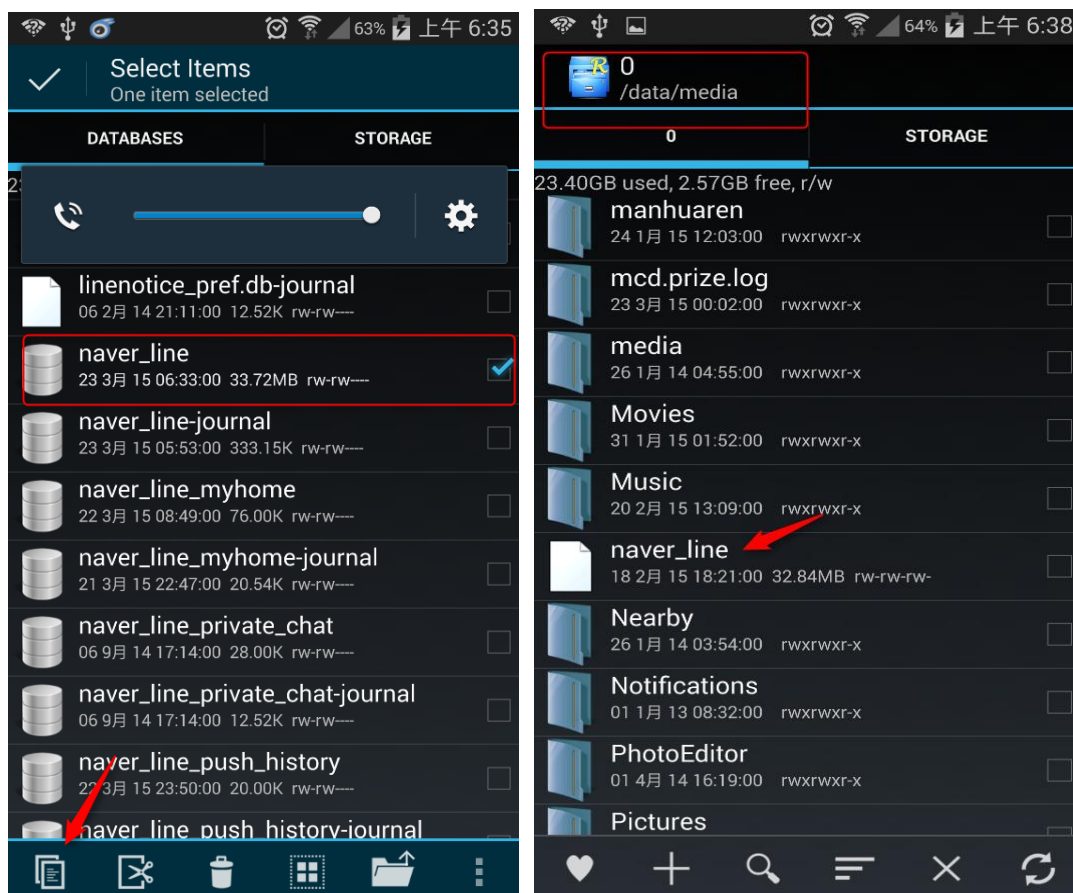


圖 4 位於手機內的 Line SQLite

而手機對於刪除資料的方式其實也與硬碟類似，由下圖中可以看到，當手機

內的資料被要求刪除時，其實只是將裏頭資料區的屬性從 Allocated Data 修改成 Unallocated Data，讓手機未來在儲存資料時，能夠覆寫這一區的內容。換言之，表面上雖然訊息已經被刪除，但除非將新的內容覆寫至原先儲存的訊息的地方，否則刪除的訊息內容仍然會保留在手機內。

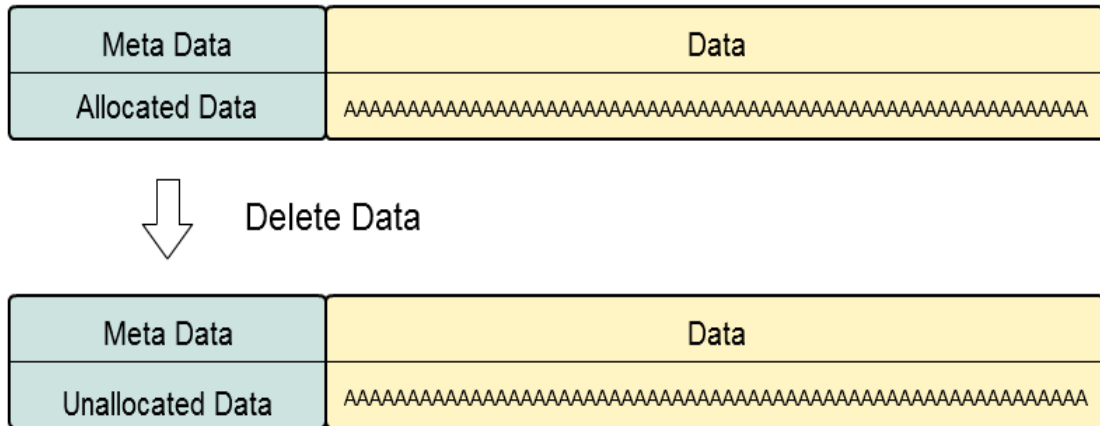


圖 5 手機刪除資料之機制（轉載自 LINE Engineers' Blog）

正因為 LINE 的訊息仍然儲存在 Database 之中，透過相關工具及技巧，一般使用者也能將歷史訊息抹除，但過程繁瑣複雜，對於初次使用的初學者來說很有可能誤刪手機核心資料的風險，加上要存取 LINE 的 SQLite 位置，必須先將手機進行 Root 或 JB，導致手機失去原廠保固，從而讓許多使用者卻步。

3. Line 完整刪除（True delete）功能

近日更新的 LINE5.3 版本中，新增了完整刪除（True delete）功能，以解決上述提到訊息資料未真正刪除的困擾。

想讓手機內的資料無法還原，有覆寫、加密、消磁、物理破壞等四種。新版的完整刪除功能即是使用了覆寫的原理，當使用者透過 LINE 的完整刪除功能刪除聊天訊息時，LINE 會將原先儲存訊息的 SQLite 區塊全部覆寫隨機的字元上去，這樣即使駭客將資料還原，讀取出來的內容也只是毫無意義的資料。

這樣的功能在更新 LINE 後便可達成，並且此預設值是開啟的，LINE 官方宣稱 LINE 使用者的隱私權應該始終受到保護，當然若要關閉此功能也可透過 LINE 的「設定」功能將其關閉。儘管此功能達到資料完全刪除的目的，相對的，當使用者不慎使用完整刪除功能誤刪重要訊息時，這些被刪除的訊息也將無法被救回，因此在使用此功能時需多加留意。

Meta Data	Data
Allocated Data	AA


 Delete Data

Meta Data	Data
Unallocated Data	00

圖 6 True delete 能將資料完全抹除 (轉載自 LINE Engineers' Blog)

4. 驗證完整刪除 (True delete) 功能

因 LINE 手機版的訊息存放於 SQLite 當中，訊息的新增與刪除也都在 SQLite 上進行，然而手機若沒有 Root 並搭配 SQLite 檢視 APP 是沒有辦法檢視 SQLite 內的資料，換言之若要確認 LINE 的訊息是否正確被刪除，則必須要將 SQLite 從手機內讀取出來，再透過 SQLite 讀取工具檢視裡頭的訊息。本專案將採用 Firefox 元件工具-SQLite manager 讀取由手機抽取出的 SQLite 資料庫，首先先在 LINE 視窗中打上一段文字訊息，如下圖所示：

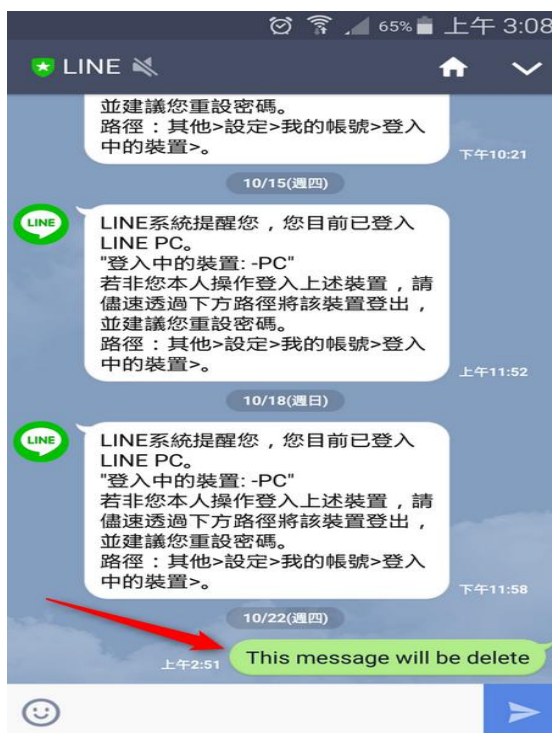


圖 7 即將被刪除的訊息

透過 Firefox 元件工具-SQLite manager 搜尋該聊天室窗，可以看到最末端有訊息內容及訊息時間，而透過 Binary Viewer 可以查詢到該訊息位於 SQLite 的位置，如下圖所示：

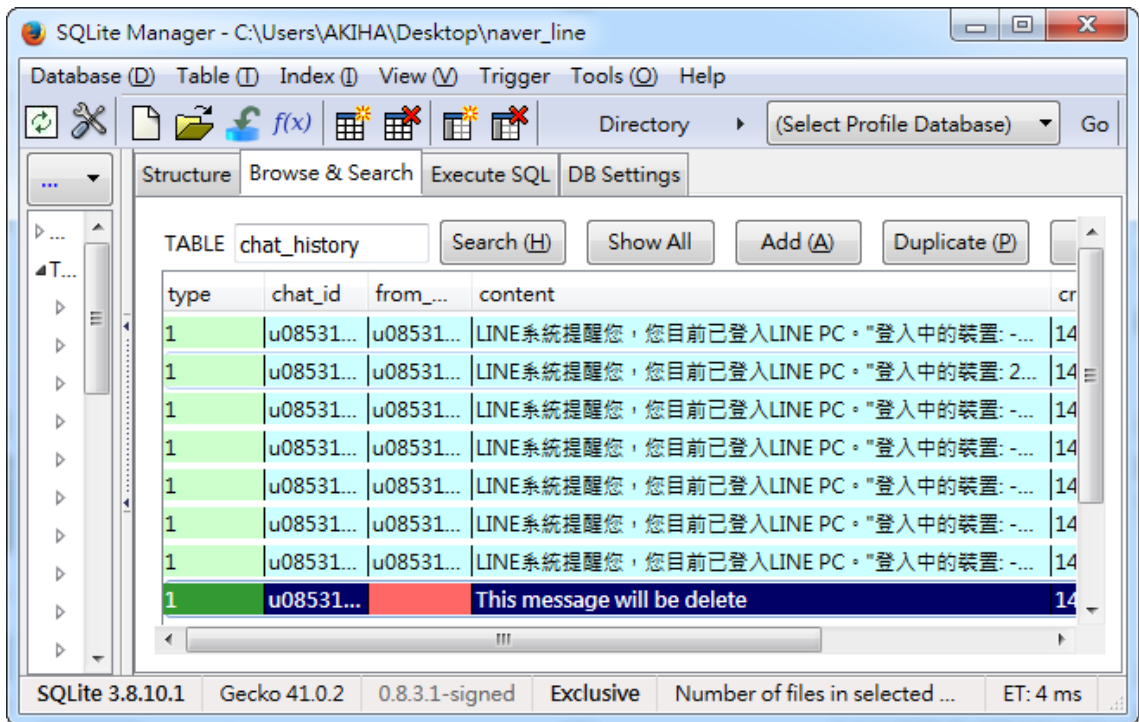


圖 8 透過 SQLite manager 檢視 LINE 資料庫內容

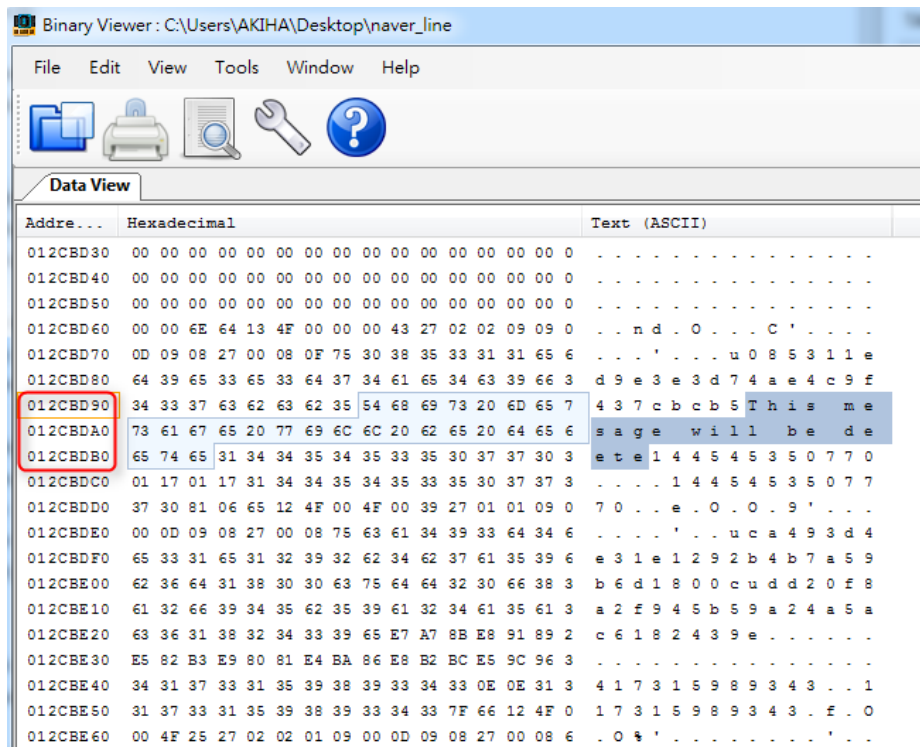


圖 9 由 Binary Viewer 確認訊息所在之位置

接著在 LINE 上將該則訊息刪除，如下圖所示：



圖 1 0 使用刪除功能將訊息刪除

刪除完畢後，同樣透過 SQLite manager 搜尋該聊天室窗，可發現被刪除的訊息已經沒有顯示在 SQLite 當中，如下圖所示：

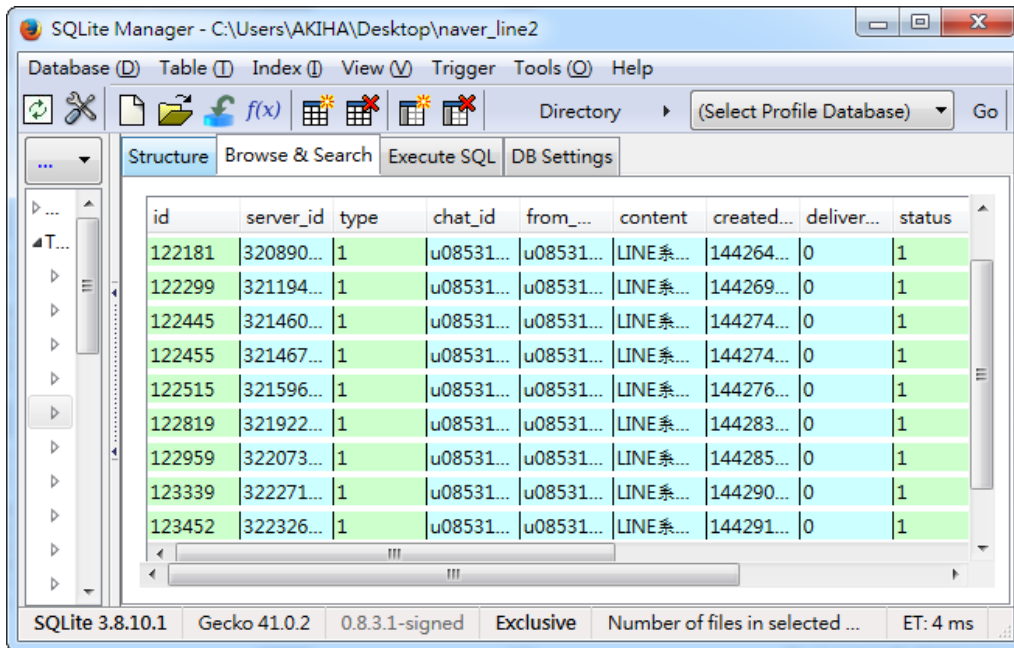


圖 1 1 SQLite 上已無該則訊息

透過 Binary Viewer 查詢原先訊息位於 SQLite 的位置，可發現該位置之內容已被填入無意義之內容，如下圖所示：

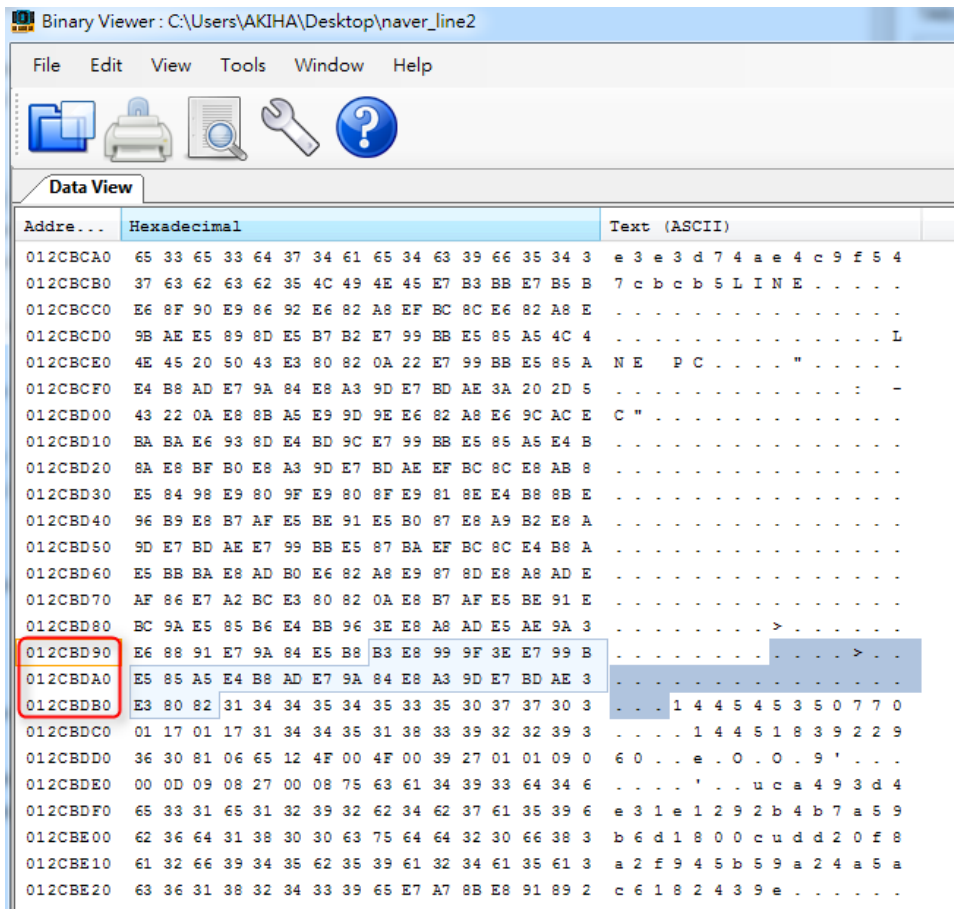


圖 1 2 原先存放訊息位置之內容已被抹除

由此可知 LINE 更新之完整刪除 (True delete) 是可以將欲刪除的訊息完整刪除的。

5. 保護個人隱私的建議

LINE 除了完整刪除功能之外，也提供訊息保護 (Letter Sealing) 的機制，透過 E2EE 的點對點加密技術，訊息經過加密後再傳輸，避免中間人將訊息封包側錄下來。但儘管如此，使用者在使用習慣上仍需注意以下幾點：

5-1. 避免點選 LINE 當中來路不明的網址

使用者若未將 LINE 的「阻擋訊息」功能開啟，將會經常收到陌生人發送的 LINE 訊息，內容除了汽車借貸或是房仲廣告之外，更多的是包含惡意連結的垃圾訊息，除了導致手機被植入木馬之外，更可能因此讓駭客偷走手機內的重要資料。因此當收到不明人傳送的網路連結時，請勿隨意點選，並且

5-2. 避免將重要資料透過 LINE 做傳輸

雖然近期 LINE 透過招募優秀資安防護人員強化在資訊安全的防護上，並且順勢推出各種訊息保護機制，但仍然無法保證這些機制不被駭客破解，或是 LINE 的內部人員透過不法方式將 LINE 的資料盜賣給犯罪集團，2015 年 4 月的 LINE 伺服器被駭事件便是一例。因此，例如家人的帳戶密碼，同事之間往來公務的機敏資料，建議透過當面告知或紙本的方式進行，降低重要資料外流的風險。

5-3. 避免 LINE 的帳號密碼與其他帳號密碼重複

一般人大多為了方便，而將各種不同功能電子商務服務都設相同的帳號密碼，諸如網路拍賣、個人信箱、通訊軟體等皆是如此，但當其中一個平台被破解而讓帳號密碼外洩時，駭客便可用相同的帳號密碼登入被害人的其他平台，因此建議將較為重要的功能服務設定不同帳號密碼，以避免帳號密碼外流時引發的連鎖效應。

5-4. 設定 LINE 的換機密碼

部分使用者在更換新手機時，會將舊有的手機上網拍賣，或交給手機業者回收，這些舊的手機若沒有確實的將裡面的資料予以刪除，便可能被他人所利用。LINE 針對此問題提供了「換機密碼」的功能，當開啟此功能時，使用者將被要求輸入一組 4 位數的換機密碼，當使用者在更換手機並登入 LINE 時，除了原有的帳號密碼進行登入之外，將額外要求輸入一組換機密碼，將 LINE 綁定在新的手機上，才能正常使用此帳號的 LINE 服務。

6. 參考資料

1. 資策會 FIND2014(H2)/「2014 臺灣消費者行動裝置暨 APP 使用行為研究調查報告」，<http://www.iii.org.tw/m/News-more.aspx?id=1475>
2. 天下雜誌-2015 數位生活調查，<http://topic.cw.com.tw/2015digitallife/>
3. 兩岸手機通訊市場有別！台灣一家獨大，大陸兩款瓜分，<http://yahoo-emarketing.tumblr.com/post/120510612931/%E5%85%A9%E5%B2%B8%E6%89%8B%E6%A9%9F%E9%80%9A%E8%A8%8A%E5%B8%82%E5%A0%B4%E6%9C%89%E5%88%A5%E5%8F%B0%E7%81%A3%E4%B8%80%E5%AE%B6%E7%8D%A8%E5%A4%A7%E5%A4%A7%E9%99%B8%E5%85%A9%E6%AC%BE%E7%93%9C%E5%88%86>
4. 我和微信不一样——专注娱乐化的 LINE，<http://www.geekpark.net/topics/1>



[68606](#)

5. 數位鑑識 on LINE 萃取手機即時訊息跡證 - 技術專欄 -網管人 NetAdmin , http://www.netadmin.com.tw/article_content.aspx?sn=1411130004&jump=2
6. LINE Engineers' Blog , <http://developers.linecorp.com/blog/?p=3660>
7. LINE 安心使用方法 1+2 層層保護避免帳號被盜用 , <http://kato3c.pixnet.net/blog/post/302125394-line%E5%AE%89%E5%BF%83%E4%BD%BF%E7%94%A8%E6%96%B9%E6%B3%951%EF%BC%8B2-%E5%B1%A4%E5%B1%A4%E4%BF%9D%E8%AD%B7%E9%81%BF%E5%85%8D%E5%B8%B3%E8%99%9F%E8%A2%AB%E7%9B%9C>