Android 應用程式安全性分析—以 Juiker 即時通訊軟體為例

Security Analysis of Android Application— a Case Study of Juiker Instant Messaging Software

謝濱燦	吳順成	陳憲洲
德明財經科技大學 資訊管理系	德明財經科技大學 資訊管理系碩士班	國防部國防採購室
bintsan@takming.edu.tw	scotte1105@gmail.com	s925014@gmail.com

摘要

隨著智慧型手機的普及化，其作業系統仍以開放原始碼之 Android 為主流，導致 Android 應用程式發展迅速，人們得以透過行動裝置及雲端相關 App 經由網際網路達到即時通訊之效果，並可隨時隨地的存取或分享資料。在目前網際網路與行動通訊蓬勃發展的情況下，即時通訊服務逐漸成為人們常用的溝通方式，然而資訊安全議題近年來備受重視，在使用即時通訊軟體談話中，有意或無意的洩漏秘密或隱私，加上手機軟、硬體本身安全性上的設計考量，使得 Android 應用程式資訊安全儼然成為新興資安議題。本研究採用封包擷取之方法蒐集 Juiker 資料傳送的封包，藉由封包分析嘗試瞭解 Juiker 安全性的弱點。依據本研究封包擷取與分析方法，希望能應用在其他 Android 應用程式的安全性分析，以檢視 App 對於機敏資訊防護是否安全，而不被輕易顯露於網路封包中。

關鍵詞：Android、Juiker、封包擷取、封包分析。

ABSTRACT

With the popularization of smartphones, the open source Android still dominated all the operating systems, which leads to the rapid growth of Android apps. Instant messaging could be exchanged online via mobile devices and cloud-related apps so that information could be accessed and shared anytime and anywhere. Under the circumstance that internet and mobile communications are booming, the instant messaging service has gradually become a common way of communication. The issue of information security is highly emphasized. However, while using the instant messaging software, privacy and confidential have been leaked intentionally or unintentionally. In addition, for the design consideration of software and hardware on smartphones, the information security of Android application has been an emerging event. In the study, we adopt the method of packet capture to collect the packets of Juiker data transmission and go further to find out Juiker's security weakness by packet analysis. This study, based on the methodology of packet capture and analysis, aims to apply the security analysis to Android applications for examining whether the apps are safe enough to protect the confidential information from exposing to network pockets.

1. 前言

1.1 研究背景

人們對於手機的使用目的已不再是簡單的撥打電話或傳簡訊，而是提升為瀏覽網頁、收發電子郵件、即時網路通訊等更多元化的用途，因此造就如今的智慧型手機，改變人們使用通訊產品的習慣及方式，並且能夠更快速、更容易地從任何地點與他人取得聯繫、獲得資訊等，智慧型手機也已成為人們日常生活與工作中不可或缺的重要裝置。

1.2 研究動機

根據趨勢科技發表「2016 年資安預測報告」資料顯示，行動惡意程式數量將成長至 2,000 萬，主要肆虐地區為中國，而新的行動支付系統將成為全球駭客的新一波攻擊目標；隨著越來越多消費型智慧裝置進入我們的日常生活，2016 年至少將發生一件重大的消費型智慧裝置故障事件，這數據突顯了智慧型手機應用程式安全防護的問題。

此外，因網際網路的普及與行動通訊的盛行，人們得以透過行動裝置及雲端相關App經由網際網路達到即時通訊之效果，並可隨時隨地的存取或分享資料。在目前網際網路與行動通訊蓬勃發展的情況下，即時通訊服務逐漸成為人們常用的溝通方式，其中由工研院研發的Juiker(揪科)，為第一個國產即時通訊軟體，可說是傳統傳訊軟體的全方面擴大延伸應用，同時也具備了市面上所有主流傳訊軟體的優點，相較於Line在一般民眾使用較為普遍的情況下，Juiker則已在國內政府體系各公務部門人員使用群組通訊服務中推廣行之有年，對於資料檔案傳輸與分享的便捷性，即時通訊軟體已成為不可或缺的必備工具。

2. 研究目的

有鑑於 Android 發展與即時通訊軟體應用之趨勢，本研究將針對 Android 行動裝置上的 Juiker App 做為主要的研究標的。經由分析 Juiker 資料傳送的封包，嘗試瞭解其可能面臨之資訊安全問題，除提供使用者對於 Juiker 更進一步的瞭解外，亦可提供相關即時通訊軟體開發者做為資訊安全防護所需考量的問題。

3. 研究方法

本研究架構敘述如後：

一、說明研究動機與背景、研究目的、研究方法與步驟及研究範圍與限制。

二、針對本研究相關論文、期刊與學術文章等文獻加以蒐集、整理、研讀及歸納，並分別探討 Android 系統架構、應用程式及網路傳輸協定，另說明網路封包擷取做為研究方法運用之基礎。

三、說明本研究之實作環境係以 Windows 8 作業系統與 HTC 手機為平台，將以封包擷取的實作方式蒐集 Juiker 資料傳送的封包，並詳細說明封包擷取之步驟。

四、針對擷取封包內容進行探究，以期能知曉資料傳送過程時是否安全及可能面臨的安全性弱點。

五、第五章結論與建議，將前述做一歸納性整理，就研究發現做成結論，並對後續研究者提出未來研究建議。

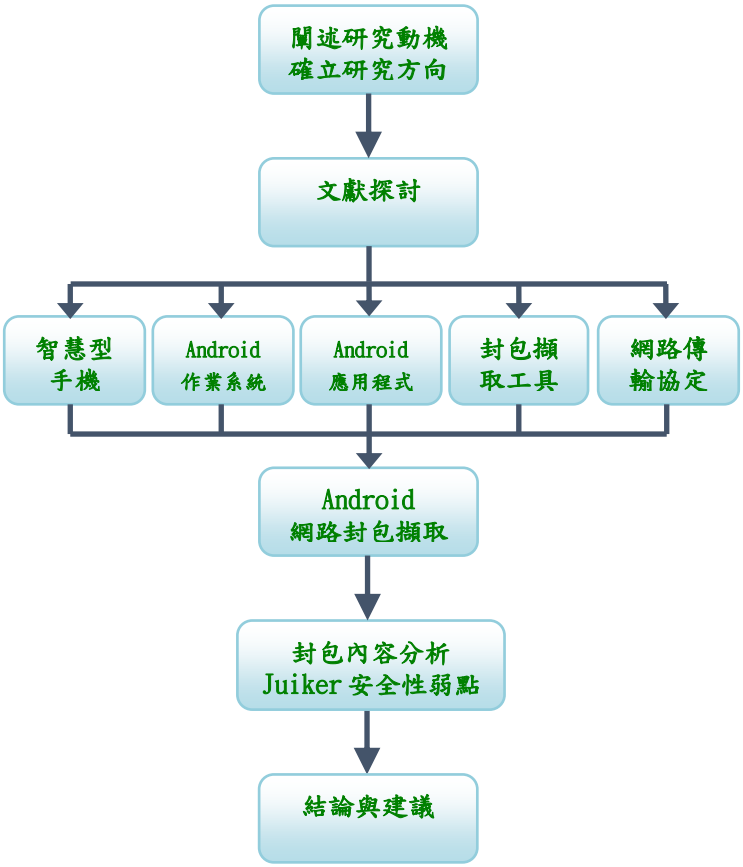

圖 1 研究架構圖

4. 實作環境

本研究之實作環境係以 Windows 8 作業系統筆電及 HTC 手機為平台，網路環境則以手機無線網路做測試。將以網路封包擷取之實作方式探究與分析 Juiker 資料傳送機制所可能面臨的資訊安全問題。

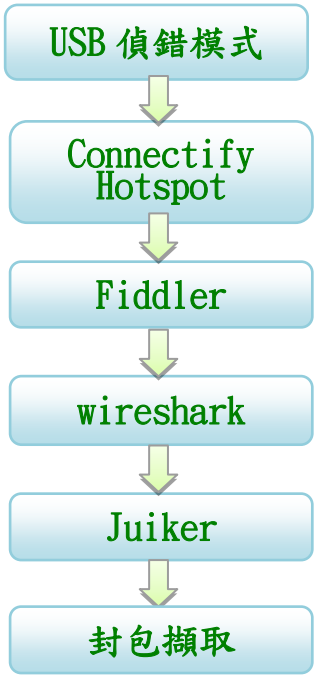

圖 2 網路封包擷取流程

圖 3 開啟 USB 偵錯

圖 4 筆電安裝 Connectify Hotspot 軟體，使筆電成為無線基地台

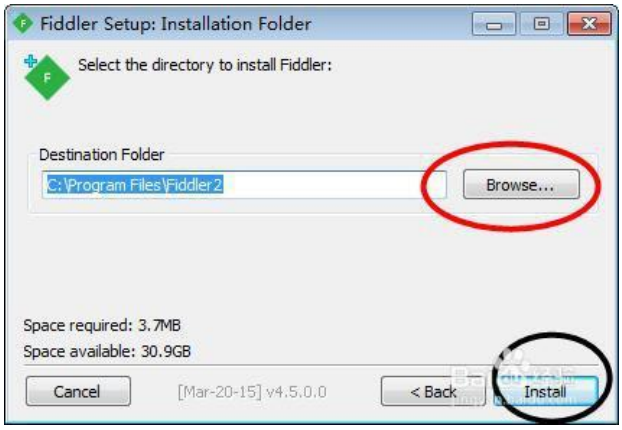

圖 5 安裝 Fiddler 軟體

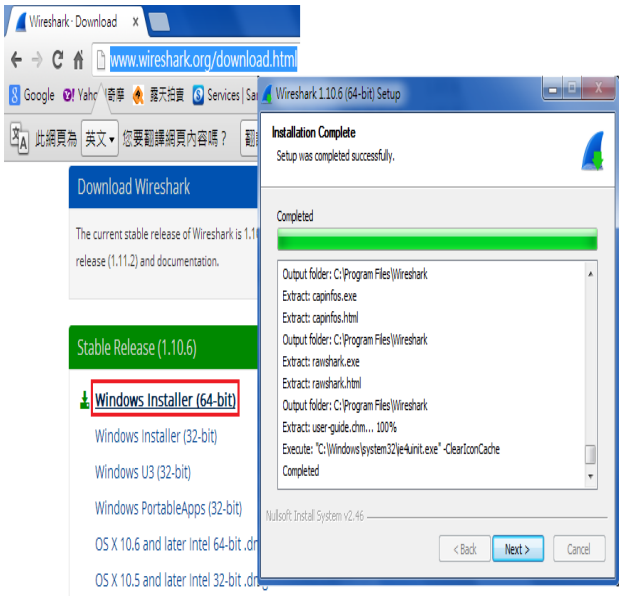

圖 6 安裝 wireshark 軟體

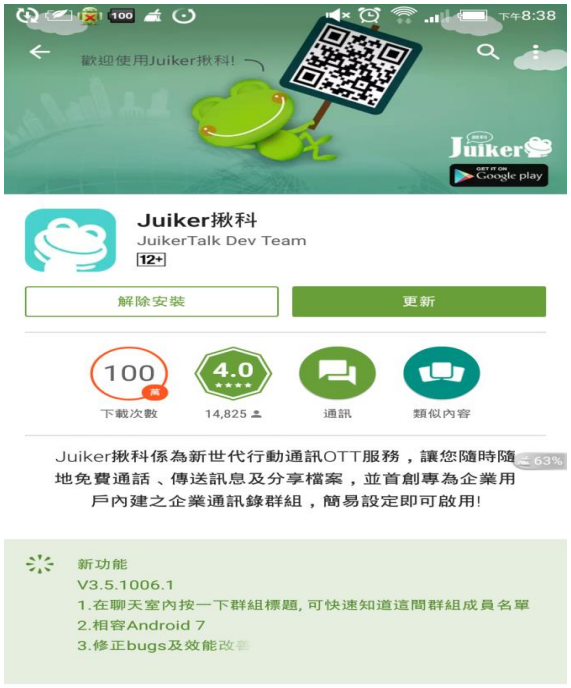

圖 7 下載安裝 Juiker

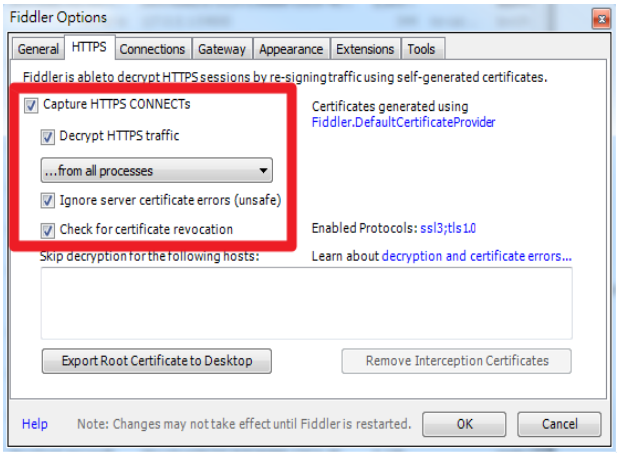

圖 8 封包擷取前步驟 1：HTTPS 設定

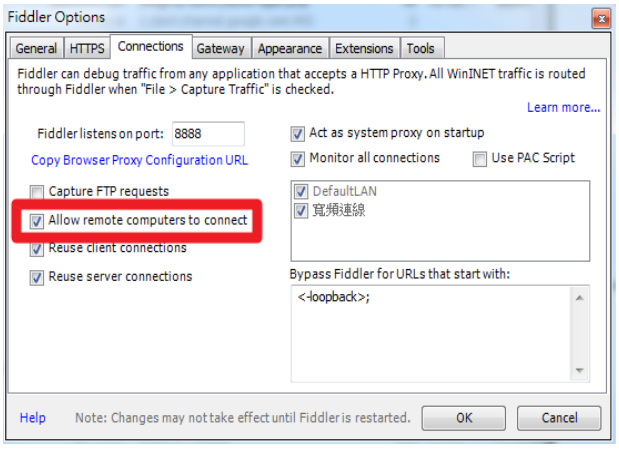

圖 9 封包擷取前步驟 2：Connections 設定

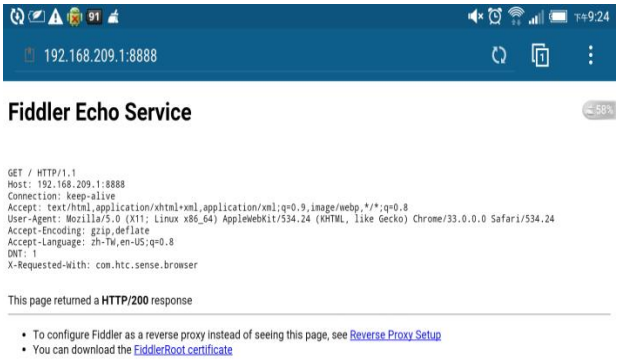

圖 10 封包擷取前步驟 3：手機連線至筆電無線基地台並安裝憑證

5. 實作成果

登錄 Juiker 後分別使用 Fiddler、wireshark 軟體進行封包擷取及分析：

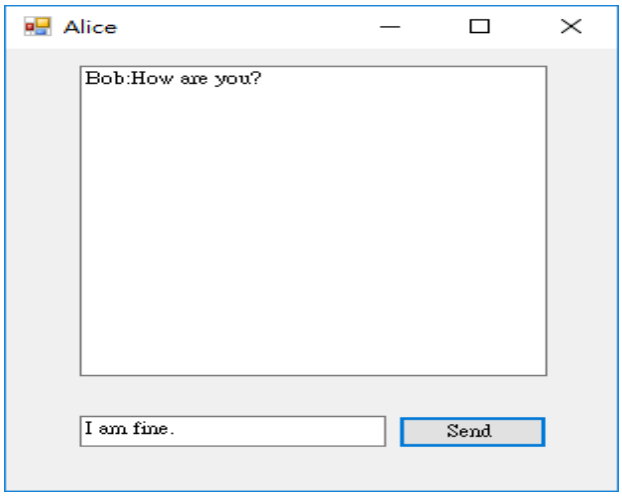

圖 11 以 visual studio 設計之簡易通訊軟體實例

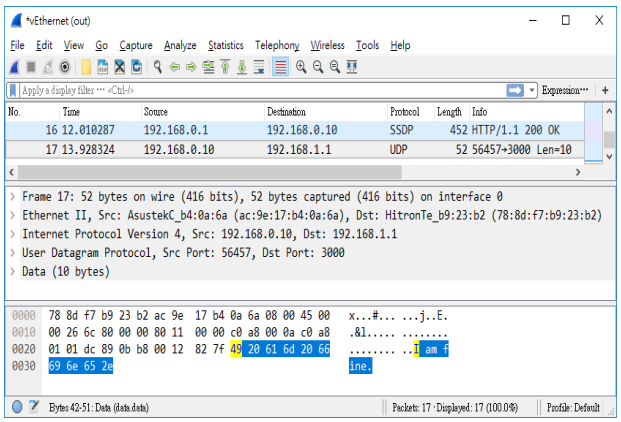

圖 12　wireshark 分析結果顯示若無加密機制等資安防護，可輕易解析出傳送明文封包

圖 13 登錄 Juiker 進行文字、語音訊息及圖片檔案傳送

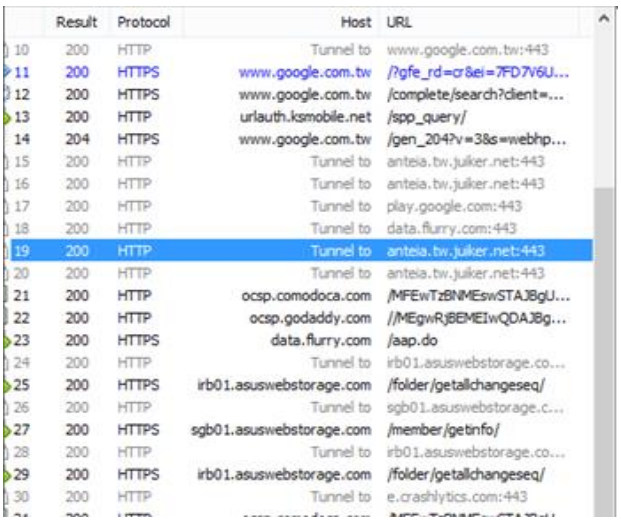

圖 14 開啟 Fiddler 軟體，進行封包擷取

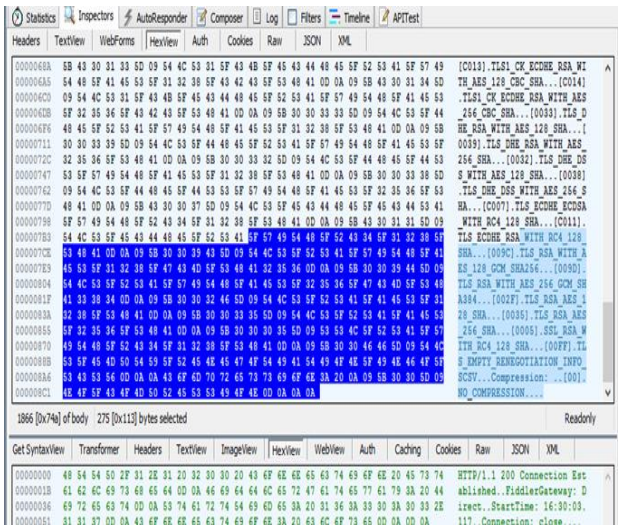

圖 15 Fiddler 分析結果 Juiker 加密演算機制嚴謹，無法發現帳號及密碼等資訊

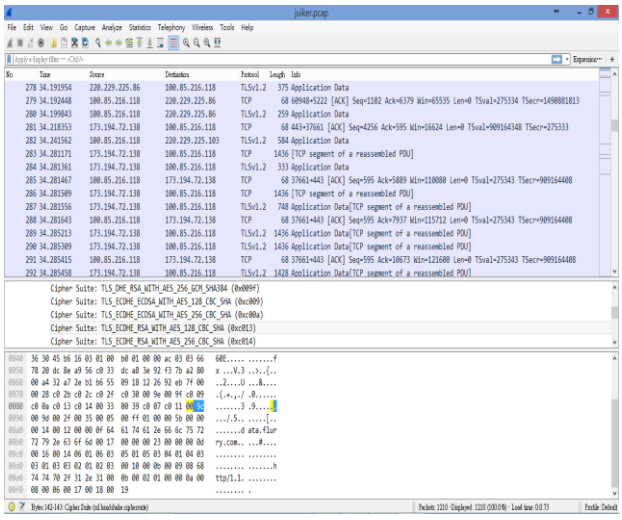

圖 16 wireshark 分析結果 Juiker 加密演算機制嚴謹，無法發現帳號及密碼等資訊

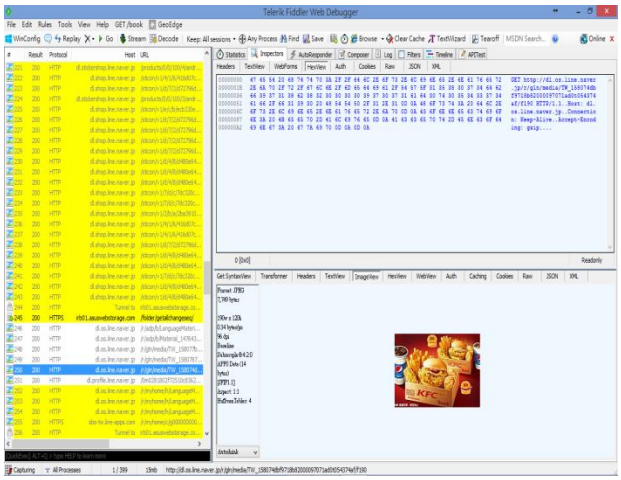

圖 17 Fiddler 分析 Line 結果發現傳送圖片時，未經加密可解析為明文檔案

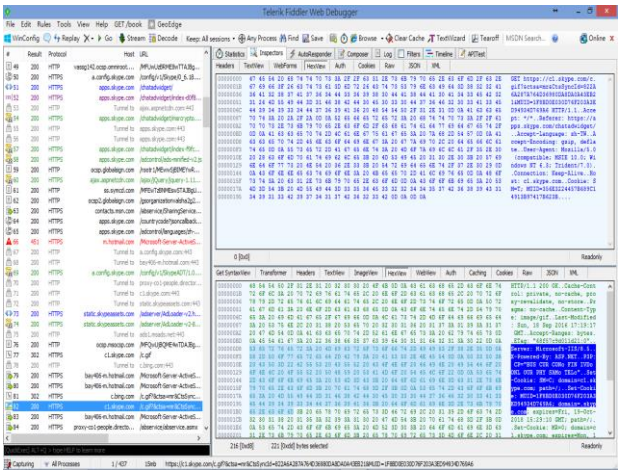

圖 18 Fiddler 分析 Skype 結果發現以 microsoft 帳號登錄，可解析部份明文訊息

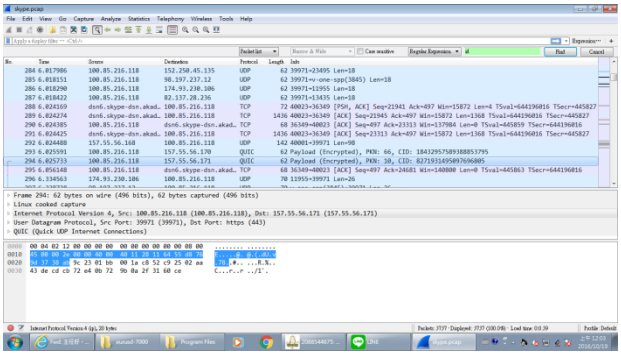

圖 19 wireshark 分析 Skype 結果發現「CID：……」疑似帳號資訊

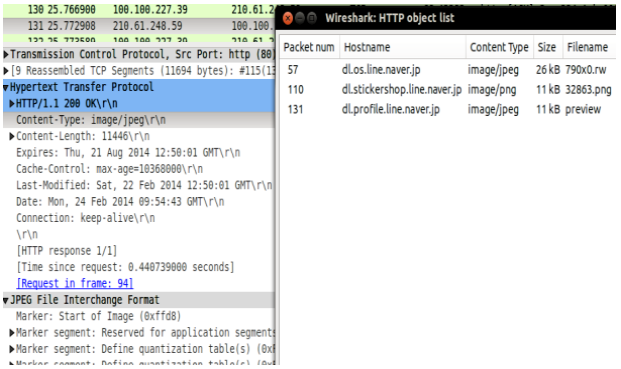

圖 20 wireshark 分析 Line 結果發現動態時報好友或自己張貼圖片為明碼

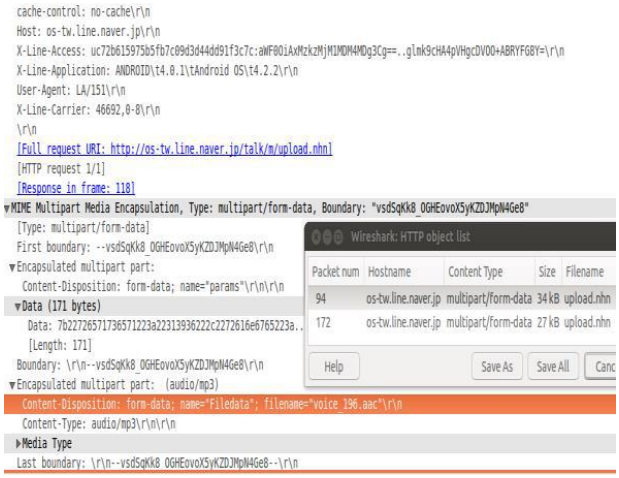

圖 21 wireshark 分析 Line 結果發現在 3G 行動網路模式下的語音留言訊息未加密

6. 結論

經由比較其他即時通訊軟體（Line、Skype）擷取資料傳送網路封包內容之分析結果顯示，部分封包內容仍可解析出其傳遞資訊之部份明碼；而Juiker採用高規格的加密機制，安全傳輸訊息、語音保護機制與密碼鎖設定，無法分析出登錄帳號、密碼及資料傳送的任何資訊，可見其資安防護機制具有相當程度的強度，由此可知目前政府機關等各公務部門群組通訊使用Juiker，的確有其可靠性及安全性，雖然在一般民眾使用即時通訊上以Line較為常見，Juiker相對並不普及，但經其安全性分析結果，仍可期待未來Juiker的推廣使用上，可達到使用資訊便利及兼顧資訊安全的雙贏層面。

7. 參考文獻

[1] 楊銀濤，2009，智慧型手機發展趨勢研究，國立成功大學企業管理研究所碩士論文。

[2] 林愷庭，2012，Android智慧型手機應用程式逆向工程之研究，中央警察大學資訊管理研究所碩士論文。

[3] 陳會安，2012，新觀念Android SDK程式設計範例教本，臺北市：旗標出版股份有限公司。

[4] 王傑民，伍立鈞，李泓瑋，吳育松，2014，Line即時通訊軟體之通訊協定與安全性分析，第24屆全國資訊安全會議。