行政院國家科學委員會專題研究計畫期中報告

一、基本資料：

申請條碼：96N011 96N011 NSC96-2623-7009-007-D

本申請案所需經費(單選)	A 類(研究主持費及執行計畫所需經費)				
計畫類別(單選)	一般型研究計畫				
研究型別	個別型計畫				
計畫歸屬	人文處				
申請機構/系所（單位）	國立交通大學　資訊管理研究所				
本計畫主持人姓名	羅濟群	職稱	教授	身分證號碼	*******558
本計畫名稱 中文	無線區網通信內容監聽技術研究 (第 24-6 項)				
本計畫名稱 英文	A Study of Interception methodology for Wireless Communication				
整合型總計畫名稱					
整合型總計畫主持人				身分證號碼	
全程執行期限	自民國 96 年 1 月 1 日起至民國 96 年 12 月 31 日				
研究學門(請參考本申請書所附之學門專長分類表填寫)	學門代碼	名稱(如為其他類，請自行填寫學門)			
	7F	電子與資訊系統			
研究性質	應用研究				
本年度申請主持國科會各類研究計畫(含預核案)共 2 件。(共同主持之計畫不予計入) 本件在本年度所申請之計畫中優先順序(不得重複)為第 2 。					
計畫連絡人	姓名：羅濟群　電話：(公) 03-5731909 (宅/手機)03-5783481				
通訊地址	新竹市大學路 1001 號交通大學資管系				
傳真號碼	03-5723792	E-MAIL	cclo@faculty.nctu.edu.tw		

研究計畫摘要

一、 中文摘要

隨著網路通訊環境的成熟，現有的網路架構已經將行動通訊結合既有的網路環境，包含有線與無線網路，構成嚴密的網路拓樸。在目前的技術環境下，無線區網僅作為有線網路的補充，隨著 Wimax 與 802.11n 等新技術發展，未來無線網路將逐漸取代有線網路的佈建。

無線區網通訊的涵蓋區域有一定的範圍，且只要在範圍內的人都可以容易聽到訊號，非常有可能遭受到有心人士的截取與竊聽。對軍方而言，資訊安全的考量甚為重要，當無線區網的應用更廣泛後，所有的陸上通訊設備與無線區網相互連結，有效監聽無線區網與相關安全管理問題，將是重要的關鍵議題。

本研究預期將現有無線網路的軟、硬體設備進行監聽技術的研究，在 ETSI 與 IEEE 802.11 規範下，完成無線區網的監聽佈建。本研究以一個適用於此通訊架構下的無線區域網路監聽管理機制，使得它能處理監聽管理問題與提供完善的環境供管理者來管理此網路環境。

關鍵字： 無線區網、監聽方法、監聽架構、安全管理

二、 英文摘要

Along with the maturity of the communications network, the mobile communication incorporates with the existing networks, wired and wireless, to construct the network topology tightly in the modern network. In the current technological environment, the wireless LAN only as a wired network in the region, adding that the development of new technologies such as Wimax and 802.11n, the deployment of wireless LAN will gradually replace the wired network in the future.

Wireless LAN has certain scope of its coverage, and everyone could sense the signal and listen the information in the area. It is very possible to be intercepted by the hackers. For the army, the most critical concern issue is the information security. When the Wireless LAN application has become to be more diversity, all the communication devices would connect each other over the land. It would become the most key issue for effective interception of wireless LAN and security management.

This research is expected to study the intercept techniques of wireless LAN software and hardware, and under ETSI and IEEE 802.11 standards to construct the interception framework in wireless LAN. Therefore, we will propose the network management schemes to support the underlying communication environment, to deal with the interception management, and to satisfy the network managers while managing the networks.

Keywords: WLAN、Interception methodology、Interception framework、Security management

1. 研究計畫緒論

1.1 研究計畫之動機

對國軍而言，應用無線區域網路架構從事資訊情報傳輸有其戰略的考量。然而無線網路先天設計上是以無線電技術為基礎，利用空氣作為介質，無線電波具有一定穿透性，這使得攻擊者得以無線電波涵蓋的範圍內進行通訊內容的監聽。如果使用者未將傳送的資訊適當的進行加密，則入侵者很容易便可以竊取所有的通訊內容，並進行監控或網路監聽，分析網路通訊流量和內容，例如密碼分析。將造成資訊安全上一大威脅，故無線網路監聽機制就顯得相當重要。此外，由於無線通訊只要電波收訊範圍內即可使用，管控上易出現困難，管理者無法完全的進行存取控制。

因此，希望藉由本研究從管理面與技術面探討監聽的技術與方法、安全管理機制之研究，提供一個可進行無線區網監聽及具資訊安全的傳輸平台。

1.2 研究計畫之目標

依無線區網不同的拓樸、組成成員以及特性，建立監聽系統架構與相關監聽機制技術。透過監聽技術的研究藉以加強反監聽機制，並反制未經驗證來源或非法使用者對於無線區網內傳送資料之威脅，包含修改/擷取/阻斷服務/竊取封包等，以有效防止敵方入侵。

本計畫為設計能符合無線網路環境所需的通訊架構，並依貴單位所提之需求進行相關性之研究，包括：

(1) 無線區網系統架構及國軍通信安全需求探討；

(2) 無線區網上安全通信架構與協定研究；

(3) ETSI 對監聽機制與技術上之規範與架構研析；

(4) 監聽技術機制探討與效益評估分析；

(5) 無線區網監聽技術探討與情資蒐集可行性分析；

(6) 依國軍需求及無線區網特性研討監聽防護機制。

1.3 重要性

隨著網路科技的進步及基礎平台建構，特別是無線網路與行動通訊的出現，使得無線區域網路的應用在網路環境的建置上提供了更快速方便的解決方案。無線網路也為大型和中小企業組織帶來明顯的好處，它不但可在部署區域網路時免除線路、插頭、交換器和施工(例如在牆上鑽孔)的需要，以節省大量時間與金錢，還能讓內部人員獲得充份自由，即使在辦公室大樓內也能行動上網，遠離進行會議或簡報時需要實際『插入』網路的不便，能更有效率地完成任務。

尤其在面對新一代無線網路通訊因應大規模新穎功能應用開發之際，現階段實有必要依據 IEEE 802.1x 無線網路管理標準。未來將參照貴單位之管理上之需要，長久的在無線網路監聽、控管上的發展進行規劃佈建，以配合國軍之運作管理，不但能增進國軍作業之效率，透過了解監聽的運作進而達到監聽反制的功能，更能夠有效的防止重要資料外漏。

2. 文獻探討

2.1 無線區域網路

無線區域網路 (WLAN) 是指使用高頻無線電波、而不得使用網路線在網路客戶端和裝置間通訊、傳輸數據的區域網路。它是一種彈性的通訊系統，用於擴充、或替代有線的區域網路。WLAN 藉由無線射頻(RF)銜接各種區域網路設備，如:個人電腦、集線器(Hub)、交換器(Switch)等，或是提供不同的區域網路彼此之間數位資料分享的網路系統，可免除佈線困擾，克服環境上障礙，提供漫遊使用者(Roaming user)隨時隨地的網路環境，將傳統網路和行動技術加以結合。

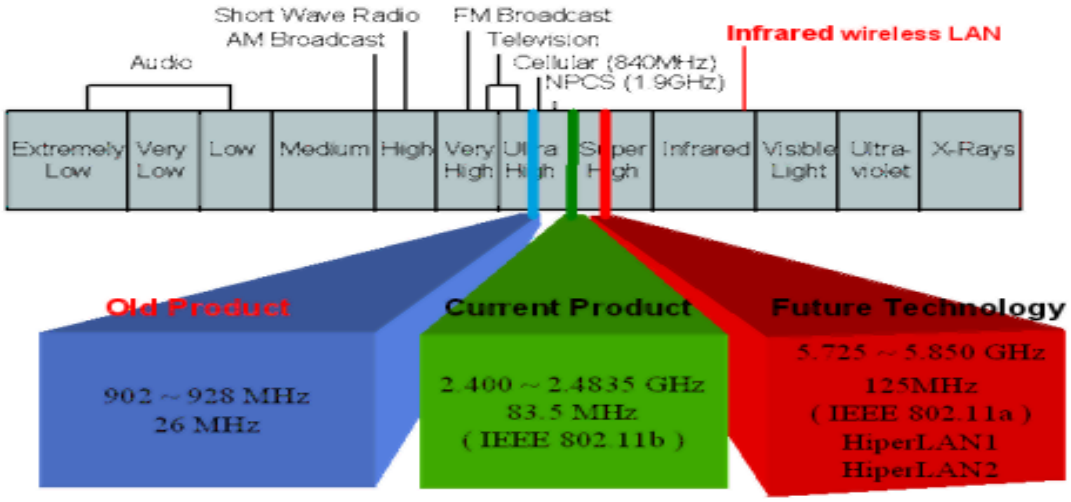


圖 1: 頻譜分佈示意圖

WLAN 的技術有兩大分類:無線電波(窄頻微波、展頻 HomeRF、HyperLAN 以及藍芽技術)與光傳導(紅外線與雷射光)，其中以展頻為目前 Wireless LAN 使用最廣泛的傳輸技術，原先由軍方發展用以避免信號的擁擠與被監聽，分為「跳頻技術」及「直接序列」兩種方式。圖 1 頻譜分佈示意目前無線網路頻段使用的狀況；ISM 頻段(Industrial Scientific Medical Band)，(包含三個頻帶 902～928MHz, 2.4～2.4835GHz, 5.725～5.850GHz)主要是開放給工業，科學、醫學，三個主要機構使用，依據美國聯邦通訊委員會(FCC)所定義出來，屬於免申請執照(Free License)，沒有所謂使用授權的限制。

(1) 802.11 相關標準

IEEE 802.11 是由美國電子電機工程學會於 1990 年 11 月召開 802.11 委員會開始制訂無線區域網路標準，該標準訂定 OSI (Open System Interconnection) 7 層通訊架構中的實體層 (Physical Layer)及資料連結層(Data Link Layer)中的媒介存取控制(Medium Address Control，MAC)子層之規範。每一個小組用一個

字母標示其所發展的標準，下表 1 列舉 IEEE 在推動 802.11 相關標準的歷史和目前的活動情形，並詳列較耳熟之標準。

表 1: 802.11 相關標準

標準	制定	頻帶	傳輸速度	調變方式	備註
802.11	1997	900MHz	2Mbps	FHSS	已廢棄不用
802.11a	1999	5GHz	54Mbps	OFDM	低傳輸距離、高傳輸率
802.11b	1999	2.4GHz	11Mbps	DSSS	和 802.11g 相容
802.11g	2003	2.4GHz	54Mbps	OFDM	和 802.11b 相容
802.11d	著重在延伸無線技術到 IEEE 無法涵蓋到的國家				
802.11e	著重在改善多媒體上的傳輸及服務品質				
802.11f	著重在加強無線網路基地台之間的漫游和廠商間的互信				
802.11h	著重在制定 5GHz 的動態頻率選擇技術及能源控管機制				
802.11i	著重在加強安全性，內容包改善金鑰分佈方法和一些進階加密技術				

IEEE 802.11a 該標準規定無線區網工作頻段在 5.15～5.825GHz，資料傳輸速率達到 54 Mbps/ 72Mbps (Turbo)，傳輸距離控制在 10～100 米。802.11a 採用正交頻分複用(OFDM)的獨特擴頻技術。

IEEE 802.11b 該標準規定無線區網工作頻段在 2.4～2.4835GHz，資料傳輸速率達到 11Mbps，是對 IEEE 802.11 的一個補充，採用點對點模式和基本模式兩種運作模式，在資料傳輸速率方面可以根據實際情況在 11Mbps、5.5Mbps、2Mbps、1Mbps 的不同速率間自動切換，而且在 2Mbps、1Mbps 速率時與 802.11 相容。 802.11b 使用直接序列(Direct Sequence) DSSS 作為協定。802.11b 和工作在 5GHz 頻率上的 802.11a 標準不相容。802.11b 最為普及，也稱為 Wi-Fi。

IEEE 的 802.11g 標準是對流行的 802.11b(即 Wi-Fi 標準)的提速(速度從 802.11b 的 11Mb/s 提高到 54Mb/s)。802.11g 接入點支援 802.11b 和 802.11g 客戶設備。同樣，採用 802.11g 網卡的筆記型電腦也能訪問現有的 802.11b 接入點和新的 802.11g 接入點。

IEEE 802.11i 標準是結合 IEEE 802.1x 中的用戶端身份驗證和設備驗證，對無線區網 MAC 層進行修改與整合，或稱為 WPA2。802.11i 的元件包括:

- 已發行的 IEEE 802.1X 連接埠為基礎的驗證架構
- 暫存金鑰完整性通訊協定 (TKIP)
- 金鑰階層和管理功能

- 密碼檢索本和驗證談判

(2) 無線區網組成元件

IEEE 802.11 無線區域網路包含四種主要的實體元件:傳輸系統、基地台、無線媒介、工作站。

1. 傳輸系統（Distribution system）

傳輸系統是屬於 IEEE 802.11 的邏輯元件，負責將訊框(frame)轉送到目的地，當幾部基地台串連以覆蓋較大區域時，彼此之間必須互通訊息，才能掌握行動式工作站的行蹤，因傳輸系統是基地台間轉送訊框的骨幹網路，所以又稱為骨幹網路（Backbone Network）。

2. 基地台（Access Point，AP）

IEEE 802.11 網路所使用的訊框必須經過轉換，才能夠將封包傳遞至其他不同規格的網路，其最主要的功能是作為無線網路到有線網路的橋接器。AP 主要是提供驗證(Authentication)與連接(Association)功能，就如同網際網路內的 Bridge 或 Router 功能。驗證程序將確認發出請求的電腦有權限進入。連接程序提供個人電腦與 AP 相互間的資料交換。

3. 無線媒介（Wireless medium）

IEEE 802.11 標準是以無線媒介在工作站之間傳遞訊框，如紅外線實體層及射頻實體層，其中以射頻實體層最受歡迎。

4. 工作站（Station）

所謂的工作站是指配備有無線網路介面的計算裝置，通常是指筆記型電腦或個人行動秘書亦可能是桌上型電腦。

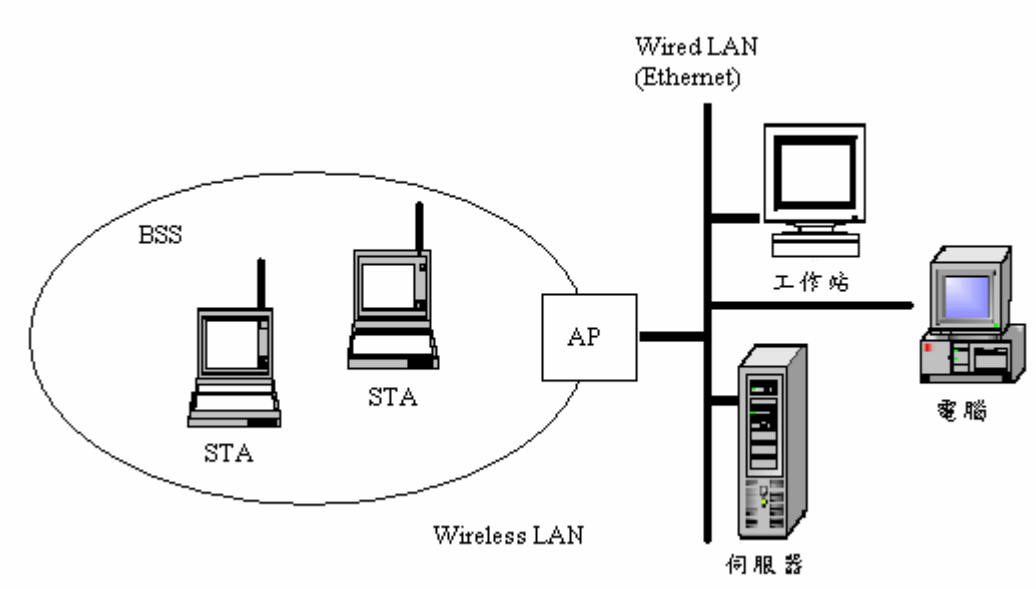
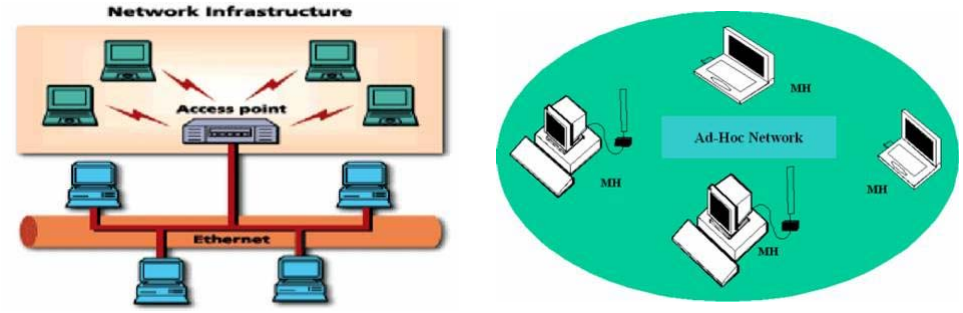


圖 2: 無線區網組成元件架構

無線區域網路組成元件之架構則如圖 2 所示，一個 AP 所涵蓋之區域稱為基本服務組合(Basic Service Set，BSS)，BSS 的功能與角色有如 GSM 蜂巢式通訊系統內的細胞(Cell)。由裝置有無線網卡的電腦連結上 AP，AP 連接區域網路 LAN (Local Area Network)，再透過區域網路連結網際網路(Internet)。

(3) 無線區網架構

IEEE 802.11制訂出兩種不同類型的無線區域網路基本架構，如圖1-3所示:



(a) Infrastructure 模式　　(b) Ad Hoc 模式

圖 3 :無線區域網路模式架構

1. 有基礎架構的無線區域網路 (Infrastructure Wireless LAN)

圖 3(a) Infrastructure 模式較常被普遍使用及架設，由 AP 為訊號發射中心，有如路由器般將訊號送至每一台無線網路節點，負責無線網路中各個節點的資料封包轉送。而 AP 本身也能夠連接傳統區域網路，做無線資料與有線資料格式的轉換。而各網路節點需要用一些特定方式向 AP 登記，當取得 AP 的服務組合識別碼(Service Set identifier，SSID)後就可以由 AP 連接 ISP 提供的服務或是連結 Internet。一般 AP 通常也具有 RJ45 連接埠，可以提供傳統 Ethernet 10/100Mbps 連線服務，所以 AP 本身具有將無線網路封包及有線網路封包相互轉換的功能。

在 Infrastructure 的網路架構下，通常 AP 與區域網路內的乙太網路相連結，此時的乙太網路在 802.11 的標準內稱為 DS (Distribution System)，同一個區域可能同時安裝許多 AP，由每個 AP 構成的 BSS 與 DS 共同組成延伸式服務組合(Extended Service Set，ESS)，在同一個 ESS 內所有的電腦都必須設定成 Infrastructure 的連結，並選擇相同的 ESS ID 號碼。為了避免各個 AP 發射電波在相同的頻率，造成訊號間互相干擾，各個 AP 必須設定成不同的頻道。

2. 無基礎架構的無線區域網路(Ad Hoc Wireless LAN)

無基礎架構的無線區域網路主要是要提供即時架設起無線通信網路，其點對點(Ad hoc)模式不需要無線網路基地台 AP 作為傳輸中繼，而可由兩台以上具有無線網路連線功能的電腦(以下簡稱節點)進行此模式，組成一小型區域網路，

每一個網路節點都能夠轉送資料到其他的節點，其資料的傳輸路徑將會動態的由當前的傳輸狀態或連線情形來決定。此模式的優點為容易架設，便於在緊急情況(軍事狀況、緊急醫療行動)或是需要快速分享資料(戶外會議)的時機使用。只要將全部的網路節點都給定相同的 BSSID，Ad Hoc 網路即架設完成，如圖 3 (b)。

2.2 無線網路安全

(1) 無線網路所面臨的攻擊型態

無線網路面臨的攻擊手法和有線網路其實大同小異，隨著無線網路設施的普及化，無線網路中的攻擊行動與種類隨著時間而不斷翻新，也有各種開發完成的輔助工具能用來進行攻擊。這些攻擊雖然可能表面上看起來方式不同，其實掌握的仍是無線網路的幾個主要弱點。以下介紹無線網路的幾個主要威脅類型:

1. 網路分析

這是無線網路攻擊的必要先行項目之一，在此階段，攻擊者很難被察覺。攻擊者為了得到此網路的相關資訊，特別是由 802.11 MAC Header 中提供的資訊，會將其節點的 Wireless NIC 設定成雜聽(Promiscuous)模式，收集網路上來往的資料封包。一般來說只需要一台移動性佳的網路節點如 Notebook 或 PDA，搭配上具備聆聽功能的無線網路介面，再加上一具簡單的指向性天線，就能夠進行網路分析。網路分析的重點在於找尋到無線網路的存在並利用 MAC Header 中紀錄的資訊進行整個網路的分析，為接下來的攻擊行動做準備。例如:從標頭中可得知此網路是否受到 WEP 加密保護，或是此無線網路的 AP 實體位址。

2. 被動式竊聽

與網路分析不同的是，攻擊者在此階段積極的收集網路上的 Session 資訊與其資料酬載。假使封包在沒有加密的狀況下，重要的資訊在此時就能被攻擊者完整的接收下來；若資料有進行加密，則可以讓攻擊者耗費一些時間在解密的進行上。同樣的，此類攻擊也很可以很難被察覺或掌握，利用指向性天線，攻擊者可以在無線網路有效理論距離外進行資料的竊取。被動式竊聽也可以收集到相當數量的封包資訊，這對於破解 WEP 加密有相當程度的幫助。由於 WEP 加密採用的是人工管理金鑰以及固定數量的起始向量值(IV)，在一定數量的封包中有機會能夠重複，因此給了攻擊者相當大的機會能夠破解。一但破解後將會揭露其下保護的上層 Layer 標頭資訊，如 Source IP address、Destination IP Address 等等，攻擊者將握有更多資訊來發動更進一波攻勢。

3. 主動式竊聽

被動式竊聽因為完全不對網路發送任何資訊，所以可以幾乎不被任何人察覺。主動式竊聽則將會對網路進行一些設計過的訊息發送或是發送被修改過的封

包，例如 IP Spoofing 就是主動式竊聽的利用。所謂的 IP Spoofing 主要是更改封包的標頭，讓整個攻擊封包看起來像是來自可信任的網域，而被允許進入 Router 或 防火牆(Firewall)，直接攻擊網路主機。

4. MAC Spoofing

攻擊者可利用改變自己的實體位址來加入一個無線網路，甚至進入無線網路後端的有線網路。進行此攻擊通常不具有很大的威脅，但緊接著攻擊者便可以藉由在網路中的存取權進行其他的攻擊行動。

5. Man-in-the-Middle(MITM)攻擊

藉由分析攻擊目標與 AP 之間的封包往來，攻擊者可以得到完整的 Session 資訊。當 Session 再度開始時，攻擊者發送干擾封包將目標與 AP 之間的 Session 中斷並阻斷其與 AP 之間的連線路徑，並將其導引到攻擊者自己的網路節點中。在此同時攻擊者開始假冒目標的身分和 AP 進行身分認證，並重新啟動 Session。此時目標將以為 Session 將繼續進行，但其實資料的交換完全透過攻擊者的機器進行處理，而攻擊者可完整得到攻擊目標與 AP 之間傳送的所有 Session 資料。為了達成目標，攻擊者必須先使用 ARP Spoofing 將原有的 IP/MAC 對映資料破壞，以故意發送 ARP Reply 的手法更新 AP 的 ARP Cache，就可能將封包和 Session 重新導向至攻擊者希望的節點當中。

6. 綁架 Session

假設攻擊者由之前的準備工作取得了足夠的身分認證資料，可以假冒攻擊目標對 AP 進行身分確認時，攻擊者可以在目標進行 Session 時將其 Session 中斷，目標雖知 Session 已經中斷但無法察覺 Session 的控制權已遭到搶奪。此攻擊方式需要預先取得大量關於使用者的資訊，因此需要完美的竊聽、封包分析和解密工作；一但取得所有需要的資訊，攻擊者將可以利用攻擊目標的 Session 進行任何工作，損失將難以估計。攻擊者也可以採用 Replay 的攻擊方式，不中斷目標 Session 但在其 Session 結束後再進行開啟 Session 的工作，將更難以被使用者察覺有異。

以上攻擊手法通常是針對具有 AP 的 Infrastructure 無線網路，若無線網路不具備任何加密手法或保護使用者的身分認證機制，對於攻擊者而言將輕而易舉能進入網路取得其所需而徹底不被察覺。而即使具有完好的加密手法，也難以保證完全不可能被攻擊者所破解。因此主動式的防護與多層的資料保護手法仍是不可或缺的安全要素，能夠提早杜絕未經過授權的使用者或在其下手前使其現形，成為無線網路安全的主要目標。基本上攻擊者的攻擊模式除了完全靜默的竊聽之外，如果要實際進行具有威脅性的攻擊必定需要親自進入網路發送某些資訊，此類資訊必定不是網路的正常行為，因此網路監察者藉由對該網路一定程度的觀察

還有行為的統計分析後建立網路行為模式參照表，必定可以比對出資料流中這些異常的資訊內容。

(2) 無線網路安全機制

在無線通訊中，傳輸資料被竊聽是常見的現象。由於無線電波的廣播特性，任何欲竊聽者只要將其竊聽器的接收頻率調至傳送頻率即可順利進行竊聽的工作。為了解決這個問題，IEEE 802.11 標準中制定了一個與有線網路具同等功效的資料保密演算法。也就是要保護無線網路之授權使用者，使之免於被竊聽的煩惱。有線網路上要進行竊聽的工作至少要連接到線上，這種不方便性在某種程度上也可說是一種安全屬性。無線網路雖然不具備這種特有的安全屬性，802.11 卻希望能提供與此功能相當的安全性。大多數的 WLAN 設備都是以 IEEE 802.11 協定為基礎的，該標準為解決 WLAN 的安全問題，提出了一系列的安全機制，IEEE 802.11 的安全相關機制分述如下:

1. MAC Address Filtering

在 IEEE 802.11b 中，使用者認證較明確的是透過 AP 記錄每個授權用戶端的 MAC address 於資料庫， 只有加入 Access Control List (ACL)中的 MAC address 才可被允許對此 AP 作存取及認證動作。但由於其資訊獲取比較容易，而且利用軟體就可以對其進行修改，因此目前普遍均認為這種方法要達到安全性要求的效果並不大。

2. Service Set Identification (SSID)

SSID 是一個由某一群無線區域網路子系統設備所共用的網域名稱，可以提供最基本的存取控制。利用 SSID 當作網路的主要存取控制機制是一種危險的作法，因為 SSID 基本上不具備周密的安全性，其原本應用在同一個區域對多個無線 LAN 網路進行分組的，並非認證功能。此外，SSID 只要在接入點不“禁止 SSID 的自動檢測”，SSID 資訊就可以在用戶端被顯示出來。

3. Wired Equivalent Privacy (WEP)

有線等效加密(WEP)是為了保護在無線區域網路的資料傳輸安全所設計的加解密系統。WEP 機制本身是屬於一種對稱式(Symmetric)的密碼系統(Crypto system)，意即用來加密及解密的密鑰是相同的。明文(Plaintext)經過密鑰加密(Encryption)之後得到密文(Ciphertext)，而密文亦使用相同密鑰來解密(Decryption)以還原得到明文。

WEP 加密的步驟如下:

a. 首先將明文經過 CRC-32(cyclic redundancy check)演算法的處理產生長 4 Bytes 的完整性檢查值(Integrity Check Value，ICV)。

b. 將明文與 ICV 合併起來。

c. 隨機選取一長度為 24 bits 的初始向量值(Initialization Vector，IV)，然後將 AP 及工作站(Station)之間共享之 40 或 104 位元的 WEP Key 合併。
d. 將 IV+WEP Key 合併起來的 64 或 128 位元資料，輸入密碼器以產生加密用的位元組串流(byte stream)。
e. 將合併過 ICV 的明文與 RC4（Rivest Cipher 4）產生的位元串流做 XOR 運算求出密文。
f. 最後將 IV 置於密文前面即為最終傳送的資料訊框(data frame)。

WEP 解密的步驟如下:

a. 將 IV 及 WEP Key 合併。
b. 將 IV+WEP Key 導入 RC4 密碼器以產生位元組串流。
c. 將位元組串流與密文做 XOR 的動作，可以得到明文 ICV。
d. 將解出的明文 CRC-32 演算法處理求得新的 ICV'。
e. 若 ICV=ICV'，則接收的資料正確；否則，即丟棄此資料訊框，並送出錯誤訊息給原來的工作站。

資料在經過 WEP 加密過後，預期達到的主要目標有下列三點:

a. 機密(Confidentiality):這是 WEP 最主要的目的，將資料加密防止竊聽。
b. 存取控制(Access Contorl):僅允許合法用戶存取網路。
c. 資料完整性(Data Integrity):防止資料在傳輸途中遭他人惡意竄改。

要達成上述三項“宣稱”的目標，則依賴於 WEP Key 是否會被輕易解開的程度，以下列舉兩項已知的方法，根據現今電腦的運算能力、金鑰的長短及網路流量，甚至可於數十分鐘內破解 WEP 加密。

- 暴力攻擊法(Brute Force)

所謂的暴力攻擊法，指的是靠電腦的運算能力，在有限的密鑰空間內，找出使用者所選用的密鑰。

- 已知 IV 攻擊法(Known IV Attack)

所謂的已知 IV 攻擊法，是藉由特定 IV 型式的封包，來反推出使用者設定的密鑰，當封包收集量愈多，找出原來使用者密鑰的可能性就愈高。此法發現 RC4 用來產生密鑰的演算法有缺陷，在選用某些 IV 的情況下，使用者密鑰的某部份仍會出現在最後產生的位元串流組裡，這類密鑰在密碼常上稱為弱密鑰(Weak Key)，只要收集這些並研究這些弱密鑰加密後的資訊，便可以反推出使用者密碼。這本來不是件容易的工作，但拜 WEP 並未將 IV 加密之賜，而是以明文傳遞的方式，使得這方法的可行性大為增加。目前網路上已有公開可取得對破解工具，例如 WEPCrack、AirSnort 等。近來發生的公開攻擊事件更進一步證明了 WEP 這項協定比原本各界所以為的更為脆弱且易於破解。WEP 的加解密步驟與破解之方法將於後段章節進行實作的說明。

4. IEEE 802.1x

為解決IEEE802.11安全性不足的問題，因而產生了一個新的標準– IEEE 802.1x-「以連接埠為基準的網路存取控制」(Port-Based Network Access Control)。也就是透過驗證方式來保護網路的一種連接埠存取通訊協定。它和WEP最大的不同點在於，WEP只認WEP Key，也就是只對裝置做認證；而802.1x則藉由使用者輸入帳號／密碼或提供X.509認證，來達到『認人』的進階安全。如果有某個無線網路使用者經由 802.1x 驗證進行網路存取，在存取點上就會開啟一個允許通訊的虛擬連接埠。如果授權不成功，就不會提供虛擬連接埠，而通訊就會受到阻擋。

802.1x 驗證有三項基本要件:

a. 申請者(Supplicant):請求網路存取權，並且需接受 Authenticator 的認證稽核，例如無線工作站。
b. 驗證者(Authenticator):要求並且接受未受信任端網路節點的認證請求的實體，例如無線存取點(AP)。
c. 驗證伺服器(Authentication Server):驗證資料庫，通常是一個 Radius 伺服器，例如 Cisco ACS*、Steel- Belted Radius* 或 Microsoft IAS* 。

在 IEEE 802.1x 標準所控管的網路下，使用者必須透過 EAPOL(Extensible Authentication Protocol Over LAN)，藉由無線擷取器或無線頻寬路由器來提供使用者帳號與密碼或數位憑證(Digital Certificate)至後端 Radius Server。Radius Server 即根據這些資訊對使用者進行認證，認證通過的合法使用者方可被授權使用該無線區域網路，此外 Radius Server 亦會記錄每個使用者的登入與登出之時間資訊,作為日後計費或網路資源使用情形的監控之用。因此透過 IEEE 802.1x 協定的施行以及 Radius Server 與使用者帳號資料庫的配合使用，一般企業、ISP 乃至各無線區域網路服務提供者均可以有效管理行動使用者在該網路的存取行為。

5. EAP (Extensible Authentication Protocol)

EAP(Extensible Authentication Protocol)提供一個可彈性選擇認證機制的架構。申請者 (無線工作站) 與驗證伺服器之間會使用 EAP 來傳遞驗證資訊。EAP 類型會定義及處理實際的驗證，其類型可採取多種型式:

- MD5:使用密碼對網路的單向驗證

MD5 是一種 One Way Hash Function，輸入 n bits 長度的資料，輸出 128 bits 的電子指紋。當它應用在 EAP 中，提供了一種最簡單的實作模式。首先，Authentication Server 必須存放每一位使用者的 Identity／MD5 of password pair，當提出 MD5 挑戰後，使用者輸入他原本的 password，這個 password 經運

算成 MD5 碼送出後即視為對伺服器的回應。這樣做的用意是，即使在傳輸過程中資料遭竊取，攻擊者也無法經由 MD5 反推算出使用者的密碼。

EAP-MD5 是種非常普遍的方法，因為它不僅實作簡單，在使用上也相當方便，使用者僅僅需要輸入 ID 及 password 即認證完畢。但過於簡單的相反面顯露出安全性的不足，它只提供了伺服器對使用者的認證，無法提供使用者對伺服器的雙向認證(Mutual Authentication)，這個弱點導致它容易遭受偽造伺服器的 Man in the Middle Attack。此外，攻擊者雖然無法得知原始密碼，但只要有帳號及 MD5 碼，仍然可以偽裝成合法使用者(Relay Attack)。

- EAP-TLS:兩方使用者或用戶端和驗證伺服器端以憑證為基礎的驗證

EAP-TLS 較 EAP-MD5 提供了更完善的安全機制，包括雙向認證及通道加密。在此模式下運作，Supplicant 及 Authentication Server 都必須擁有憑證，當它們相互認證之後，便可在兩者之間建立 TLS tunnel 加密。這種作法類似 SSL 的加強版，而實際上，確實也有許多 EAP-TLS 模組底層實作 OpenSSL (http://www.openssl.org/)。Supplicant 還可以進一步再對網路做認證，必須是擁有憑證者才是合法的 AP，就可以避免偽冒 AP 的攻擊。EAP-TLS 提供了很好的防護，但它同時必須額外維護憑證，這是實作上必須考量的地方。

- EAP-TTLS 及受保護 EAP (PEAP)

EAP-TTLS 和 PEAP 概念十分類似，分為兩個階段。在第一階段 Supplicant 及 Authentication Server 建立連線並互相認證；在第二階段，會使用在第一階段協調好的密鑰建立通道，將使用者的帳號／密碼傳送給認證伺服器。不同的地方在於，PEAP 只能使用 EAP protocol(for example,EAP-MS-CHAP-V2)，而 EAP-TTLS 則無此限制。

6. 802.11i

過去企業採用無線網路時，由於 WEP Key 的內容都是固定的，為了避免惡意的入侵，網管人員必須每隔一段時間通知使用者更換加密的 WEP Key，進而降低被入侵的風險。有鑑於此，IEEE 802.11i 針對無線網路原本所具備的弱點加以補強，在 WIFI 的推動下，制訂了 WPA(WIFI Protected Access)標準，以 IEEE 802.11i Draft 為藍圖，去建構出一個符合現今需求，具備更進一步安全性的無線網路環境。

目前802.11i主要定義的加密機制可以分為TKIP (Temporal Key Integrity Protocol，暫時密鑰集成協定) 與AES(Advanced Encryption Standard，高級加密標準)。WPA 是由 TKIP 與 IEEE 802.1X 技術所組成，解決了 WEP 的安全瑕疵，改善資料的加密與身份認證。TKIP主要的設計是相容於原本802.11的硬體產品，透過韌體與軟體升級來提高加密的安全，一樣是透過RC4加密，但是可以讓

每個封包都提供不同的加密Key值。原本的WEP加密使用24-bit的IV值，目前的TKIP使用48-bit IV值，如此大幅減低IV值重複的問題。

2004 年 9 月 Wi-Fi 聯盟宣佈支援 WLAN 安全國際標準規格 IEEE802.11i 的安全規定 WPA2（Wi-Fi Protected Access 2）開始進行認證作業，Wi-Fi 聯盟表示，此項認證的目的是讓政府等公共機構和企業重要部門等需要嚴格保密的組織也能用上比較安全的 WLAN。WPA2 要求產品支援加密演算法 AES。AES 於 2002 年 5 月被美國商務部定爲美國政府的標準密碼，它以美國政府的安全標準“FIPS 140-2”爲基準。隨著 WPA2 的亮相，美國政府以及採用 FIPS 140-2 標準的機構、企業就可以使用符合標準規格的 WLAN。WPA2 也支援 RC4，具有對 WPA 的向下相容性，能連接 WPA 支援產品及 WPA 的安全級別。但 WPA2 不相容 WPA 的前身 WEP。

WPA2 PSK（Pre-Shared Key），PSK 會同時以用戶端與存取器的密碼或識別碼（亦稱為通關密語）來確認使用者。假如用戶端的密碼符合存取器的密碼，即可存取網路。PSK 也提供TKIP 或AES 為各個封包的傳輸資料產出加密碼的密鑰素材。PSK 比靜態WEP 更安全，但兩者都儲存於用戶端，一旦用戶端設備失竊，PSK 同樣會被破解。建議使用混合字母、數字與非字元符號的複雜化PSK 通關密語。

(3) 無線網路的安全弱點

雖然 802.11 有提供基本的安全機制，但是也有已被證實其漏洞存在的機制，無法確保所使用的無線區域網路的安全性，以下就無線區網的架構分別探討關於現存安全機制潛在的問題:

1. Infrastructure 無線網路存在著 AP，AP 通常是接上有線網路以提供無線網路存取外界資訊，每隔一定時間會送出一個 Beacon Frames，用以宣佈 802.11 網路的存在，內容包含有 Relay Information、Timestamp、SSID 等。其中 SSID 可阻擋無 SSID 的用戶端設備的存取動作。但存取器預設以標識來廣播 SSID，也就是即使關閉了 SSID 的廣播，攻擊者仍能透過嗅探(Sniffing)作法，或在不被偵測的情況下對網路進行監看，來偵測出 SSID。

部分WLAN 供應商支援以用戶端網路介接卡的實際位址或MAC 位址進行驗證。存取器也僅允許符合驗證清單的用戶端MAC 位址進行連結。但MAC 驗證仍非完善的安全作法，因為MAC 位址可被偽造，而網路介接卡也可能失竊。

此外，AP 和無線網路裝置之間要做任何的連線，必須要先經過一段協調過程(Associating)。預設的機制是 Open System Authentication，使用這個機制的話任何人都可以透過 AP 進行連線，不提供任何安全機制，任何人只要有正確的

SSID 就可以透過 AP 進行網路的存取，在這種狀況下等於是毫無保障可言。

如果設定為 Shared Key Authentication，AP 和使用者之間就會開始進行一段 Challenge-Response 的認證過程，如 WEP 安全機制的弱點，攻擊者竊聽這整個過程就有辦法取得整個加密過程中三個變數中的兩個，再將其套入 RC4 的運算式中，攻擊者就有辦法得到 shared key，接下來所有的通訊內容都有辦法被反解回明文。

2. Ad hoc network 代表這個網路不需要 AP 來控管這個網路，每個節點各自組織，互相轉傳，由於 Ad hoc network 上的弱點，造成的攻擊問題包括:

a. 黑洞問題(Black hole):被入侵的節點利用無基礎行動網路路由協定發送假冒的路由資料，使其他節點對於最短路徑的判斷錯誤，將資訊送到錯誤的路徑而無法正確傳輸。

b. 阻斷式服務攻擊(Denial of service):攻擊者由外部網路或被入侵的結點，發送大量控制訊息封包，使得頻寬被佔據而無法傳送資料。

c. 溢滿式路由攻擊(Routing table overflow):被入侵的節點藉由偽造的路由資訊，使欲攻擊的節點誤以為有另外一條路徑存在，而將資料送往不正確的路徑。

d. 仿冒節點問題(Impersonation):一個惡意節點偽造假的控制封包，更新附近節點的路由資訊，使得原本應該傳給某個特定節點的資訊，轉送到惡意節點。用以竊取某些特定資訊。

e. 資訊外流問題(Information disclosure):無基礎行動網路需要藉著其他節點協助進行資料傳遞。因此中繼節點可截取傳輸的資訊，若傳送者與接收者中間必須透過某些未被身分認證的節點傳送時，資訊即有可能外流而造成傷害。

2.3 監聽機制

就無線區網監聽而言，係可經由監聽工具來攔截封包、複製封包、儲存封包、分析封包等程序達成。攔截封包，必須在監察對象的封包可能會經過的節點上或在相同的區域涵蓋範圍內，設置或具有截收能力的設備，攔截並過濾出被截收目標的封包，此時，截收設備可將攔截到的封包先暫存至儲存媒體，待稍後分析，再轉換為欲監聽對象的監察資料，如各式不同的檔案格式的儲存體，例如：text、picture、voice。

實務上在監聽了一段時間後，便可以找到資料傳輸的 key 值，IV 值，只要能找到一組，就有 5%機會找出真正 key 值。而整個具監聽機制的系統依監聽的方式不同，系統種類可概分為兩種，包括:轉送型監聽系統與分散式同步截收型

監聽方式。監聽內容的程序分為兩階段式，在第一階段，會依照管理系統提供條件，來過濾出特定對象是否有進行網路傳送資料的行為，如果判讀出設定監察對象有進行傳送資料立即觸發第二階段的截收動作，也就是開始截收封包資料，並由截收伺服器開始同步解碼，儲存等動作，完成整個監聽的動作。監聽架構的後台管理系統提供使用者介面，設定截收配方組合，例如:來源號碼，目的 IP 位址、監聽時段等條件，並遙控其開始與結束，檢索監聽內容等。

轉送型監聽系統，利用轉向功能設計，執行對特定對象的監聽，不需要攔截所有的封包。轉送型監聽又可細分為側錄型監聽與會議型監聽兩種方式，分別如下所介紹:

(1) 側錄型監聽系統環境

當監聽單位建立欲監聽對象之列表，提供給網路管理者，匯入其使用身份至監聽管理名單中，當這些受監聽的使用者開始傳送資料時，經判別為需要被監聽之對象時，會把原來該建立到目標的連線，強制改建立到一台為監聽目的所設置的伺服器上，而該伺服器是一台具有側錄能力的 Relay Server，再由該側錄伺服器中介代理建立連線到真正撥打目的對象,所有的語音封包都會透過該側錄伺服器轉送，而該閘道可以將談話內容側錄一份，完成監聽動作。在無線區域網路中的 Relay Server 最佳設置點就如同 AP 的角色，不論是無線區網內或是向外傳送的資料都會經過 AP，此時，可將欲監聽對象的封包側錄下來後，再進行後處理與資料分析。

(2) 會議型監聽系統環境

無線區網在 Ad-hoc infrastructure 下，可以不用透過 AP 轉送，是可以直接建立一個雙向連線到目的點去，和側錄型監聽的模式相比，必需是在被監聽的使用者的傳輸範為內，可減少使用者查覺到自己被監聽的可能性。轉送的好處是只適用於監聽對象內容，無關者不會被連帶受監聽的問題，爭議較少。

在建立監聽系統安全機制的設計上必須滿足下列的準則:

1. 建立轉送連線時間(call setup time)不能過長。
2. 減少傳送的即時控制訊號（real-time signaling）
3. 減少服務提供商(service provider)與網路作業人員的工作負擔。
4. 必須管理監察的監聽名單。
5. 反監聽的分配與更換方式需非常容易。
6. 監聽資料需有標準化訂定和部份需要進一步符合秘密通訊自由之保障。
7. 提供版本控制的管理方法，以利將來機制的更新與修正。
8. 必須符合我國的法規限制，如監察資料內容管制、合法監聽等功能。

2.4 無線封包分析

(1) 監聽軟體簡介

無線網路進行監聽大多可以利用工具監聽封包的資訊，以企圖從封包內容中獲取重要的資訊，例如:使用者帳號、密碼、IP位址，或是即時通訊的談話內容。以下將列舉常使用的監聽工具，並簡介其功能和運作平台。

1. Wireshark

a. 簡述

Ethereal 是目前最多人所使用的 Sniffing Tool，已經廣泛用於區域網路封包解析作業。於 2006 年夏天改名為 Wireshark。它可以設定尋找的封包類型來進行封包過濾，甚至可以即時的在擷取封包時進行過濾。它具有相當完整的封包解析能力，能將封包先歸類，再以樹狀結構的方式將封包的資料解開讓使用者能一目了然其中的內容。Wireshark 可辨識包括 TCP/IP 在內的 759 種通訊協定，除了 802.3 和 Wi-Fi 無線網路之外，它還能夠對 FDDI、PPP、Token Ring、X.25 以及 ATM 網路進行封包分析，可算是目前能力最強以及用途最廣的 Sniffing Tool。

b. 運作平台

- Windows (Win32) Wireshark 具有 Win32 的版本，但需要 WinPcap 輔助才能進行作業。WinPcap 是符合工業標準的資料鏈結層(Data Link Layer)存取介面，運作於 Win32 環境，能讓應用程式跳過普通傳輸協定直接從鏈結層中進行例如核心層級的封包過濾或統計作業。
- Linux (Unix):為 Wireshark 官方建議使用的平台，因為 Linux 容許應用程式在有介面的情況下直接使用連線於平台上的硬體設施，無須透過如 Win32 平台的動態連結庫等繁瑣的措施。Wireshark 的 Linux 版本需要以下需求:
  - GTK+和 Glib:負責 Wireshark 的 GUI 環境。
  - LibPcap:用途如 Win32 的 WinPcap。
  - Perl: Ethereal 須利用 Perl 進行文件的編製動作。
  - Zlib(optional):當 Wireshark 進行蒐集的資料壓縮時需使用。
  - NET-SNMP(optional):需要分析 SNMP 資料時 Wireshark 需要使用此項。

c. 優缺點分析

在純粹 802.11 無線網路監聽的功能上，Wireshark 仍舊可以勝任，只要準備好可進入運作模式的無線網路介面(WNIC)即可開始進行監聽和攔截封包的工作。Wireshark 只要鎖定 NIC 就可以從 NIC 中開始擷取它所收到的任何封包，並

在停止後按照一一詳列在主視窗中，讓使用者能點取並由外而內檢查封包的內容。Wireshark 發展至今已經相當純熟，由於其簡單的操作和介面相當容易上手，可使用在各平台上的版本易於取得再加上功能強大，故也廣為被網路犯罪者所使用。而因為其自由軟體的身分，也更無法控制使用者的領域或素質。在可以輕易取得的情況下，Wireshark 除了是優異的網路監察工具外，相對的亦是功能強大的網路犯罪工具。

2. NetStumbler

a. 簡述

NetStumble 是廣為被推薦的小型偵測軟體。它的主要功能是探測節點一定範圍內的所有 802.11(a/b/g)無線電波訊號，對於進行無線網路部署有相當程度的助益。主要用途如:

- 視察無線網路部署情況
- 探測強弱訊號的極限範圍
- 探測其他無線網路用以預估可能遭遇的訊號干擾
- 探測工作範圍內其他私設 AP 的位置
- 幫助偵查指向性天線的存在
- 用來進行 War-driving

Netstumbler 程式可提供的資訊大多與 AP 有關，包括訊號強弱的圖表、訊號頻道、SSID、有無啟用加密 WEP 協定等，對於測知 AP 的作業狀況能有一定程度的掌握，幫助工程師進行無線網路的調整。

b. 運作平台

NetStumbler 目前僅限 Windows 平台使用，故僅推出 Win32 的 Beggarware 版本(不同於免費的自由軟體)。使用條件相當容易達成，僅需要可進行運作的無線網路介面即可，若有 Promiscuous 模式更佳。

c. 優缺點分析

由於軟體本身用途為協助進行 AP 的部署以及設定，NetStumbler 的功能僅限於探測並找出 AP 的存在，顯示各 AP 的資訊，不具其他額外功能。但若搭配上 GPS 裝置，Netstumbler 將能夠搭配 GPS 提供的 NMEA 格式訊號來對 AP 進行定位，幫助尋找非經允許而架設的 AP 裝置。對於需要進行網路偵防工作的人而言，此軟體的用途單一而小巧，無法提供執法人員太多資訊。

3. Kismet

a. 簡述

Kismet 是 802.11 Layer 2 的無線網路偵測、監聽軟體，同時也是入侵偵測系統，對於 802.11/a/b/g 無線網路都可進行 Sniffing 的工作。 Kismet 的監聽技術，主要是利用被動 (Passive) 模式，收集無線網路的封包，偵測標準的開放網路、隱藏網路，藉由資料封包的分析，還能夠偵測到將一些關閉 Beacon 基地台的隱藏無線網路。

Kismet 對於其他網路監察工具也有相當的支援度，可以讀取或儲存與 Ethereal、Tcpdump 及 AirSnort 格式相容的紀錄檔，使其成為相當強大的封包分析軟體和 WEP 加密分析軟體。

b. 運作平台

目前 Kismet 僅限於 Linux 平台使用，同時必須倚賴以下幾項必備元件才能正常運作:

- Libpcap
- Wireshark
- Gpsdrive(Optional):幫助 Kismet 使用連接上的 GPS 設備，幫助對已經偵測過的無線網路實際區域製作地圖。

c. 優缺點分析

Kismet 的功能相當強大，由於其整合各類網路監察工具的功能與用途，使其幾乎能夠滿足各種網路偵防工作。使用者需要在 Linux 平台上才能使用，故對於其他平台的使用者(如 Win32)就必須進行平台轉移。Kismet 除了具備基本的 Sniffing 與封包分析技術外，它還可以幫助使用者分析並找出 WEP 加密的金鑰並將蒐集到的封包加以解密，所以對於網路監察而言它無疑是一把最好的工具。但同樣的，頂尖的技術若為不法人士所使用，則將對於網路所有的使用者將造成相當嚴重的威脅。

4. AirSnort

a. 簡述

AirSnort 屬於破解加密系統的工具。WEP 已經被證實為不安全的加密方式，但事實上它仍在被廣泛使用，AirSnort 針對了 WEP 的弱點進行封包的破解工作。首先必須要蒐集超過 300 萬到 500 萬個封包，隨後 AirSnort 便能夠由這些封包資料中推算找出此 WEP 加密密碼。AirSnort 推出主要是為了展示 WEP 加密系統的弱點，雖然有很多軟體早已達成這個目標，但它是目前能夠同時捕捉封包與進行加密的唯一工具。

b. 運作平台

使用者只能夠在 Linux 平台中使用 AirSnort，需要一連串繁瑣的設定。

c. 優缺點分析

為了完成功能，AirSnort 各版本幾乎都提供簡便的 Command Line 控制，直到最近的版本才提供 GUI，在安裝設定上對 Linux 新手而言實屬困難。當一切安裝與設定過程結束後，AirSnort 能夠完全掌控 Wireless NIC，使其進入 promiscuous mode 來進行封包的捕捉，當取出足量封包後進行處理，直到列出最後一筆 IV 值為止，再由使用者利用 Script 進行破解。在新版(2+)的 AirSnort 當中更新增了 SSID 偵測與 AP 實體位址(MAC)偵測，也提供 GUI 讓喜歡圖形介面的使用者使用。AirSnort 本身唯一目標是用來破解 WEP 加密取得金鑰的軟體，對於其他功能無太多著墨。

5. AirCrack-NG

a. 簡述

NG 是下一代的意思，AirCrack-NG 是一個相當完整的無線網路攻擊工具組，不但可以利用來做 WEP 加密金鑰的破解，也可以做 WPA-PSK 金鑰的字典攻擊，其工具套件包括 airodump-ng、aireplay-ng、aircrack-ng、airmon-ng 等。

AirCrack-NG 的基本原理是首先收集足夠多的加密資料包，然後通過統計學計算恢復 WEP 的 IVs。對於 40 位元 WEP 通常需要 30 萬個 IVs（Initialization Vector），對於 104 位元 WEP 則需要 150-200 萬個 IVs。

b. 運作平台

AirCrack-NG 有 Linux 版本，還有 Windows 版本，另外也有人寫了 Windows AirCrack 的 GUI 程式，叫做 WinAirCrack，搭配 AirCrack-NG 的使用。Linux 版的 AirCrack-NG 提供的工具較為完整，包含了以下的幾個程式:

- Airodump-ng: 802.11 封包截取程式
- Aireplay-ng: 802.11 封包注入程式
- Aircrack-ng: WEP 及 WPA-PSK key 破解主程式
- Airdecap-ng: WEP/WPA 封包解密程式
- Airmon-ng: 802.11 網路監聽程式
- Packetforge-ng: 802.11 封包製造程式
- Airtun-ng: 802.11 加密封包蒐集及封包注入程式
- Tools:其他相關工具

c. 優缺點分析

不同於早期被動的收集封包，AirCrack-NG 在 WEP 加密金鑰的破解，可以採取更『主動』的封包注入的方式，製造偽造的 ARP Request 的封包，使得 AP 回應這樣的請求，而發出 ARP Reply 的封包，而當 AP 發出回應封包時，駭客就可以收集更多的『 IV 值』，加速 WEP 加密金鑰的破解，以一個 128 Bits 的 Key，可能在三十分鐘之內被破解。

Aircrack-NG 在處理 802.11 認證時存在漏洞，遠端攻擊者可能利用此漏洞在運行 Aircrack-NG 的機器上執行任意指令。僅在將 Airodump-ng 配置為以-w 或 --write 選項記錄且無線設備以 monitor 模式抓包的情況下才可能出現這個漏洞。

(2) 封包分析

探討 802.11 的封包結構，得先從其 MAC 訊框(Frame)介紹，圖 4 為 802.11 之 MAC Frame。

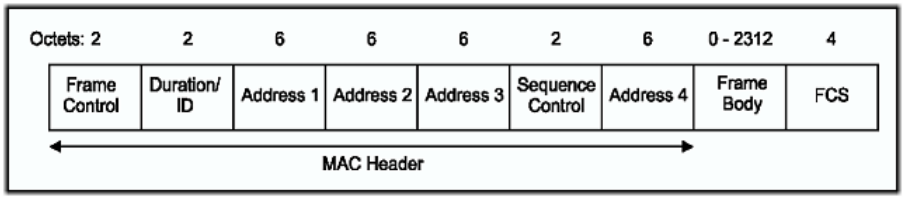


圖 4: MAC Frame

802.11 MAC 標頭(MAC Header)定義了 Frame Control、Duration ID、Sequence ID 以及 Source 和 Destination Address 等等的重要資訊，總長 30 Bytes。故可以提供資訊說明此封包的來源和目的地為何，由於進行此標頭封裝的層級是在網路架構中的第二層(Data Link Layer)，以未加密或破解加密後的情況考量，標頭資料將可以使得到此封包的人了解標頭所提供的資訊，這也是我們接收到封包後可以最先進行分析的部份。詳細的 MAC 標頭介紹如下:

1. Frame Control 欄位:總長 2 Bytes 的欄位，記錄了多項關於此封包的身分資料，可分為 11 個小欄位。
   a. Protocol 欄位:總長 2 Bits，說明此 MAC 訊框版本。
   b. Type 及 Subtypes 欄位:兩者共長 6 Bits，用來標示此 Frame 的種類與種類用途，以代碼來進行分類。
   c. ToDS 及 FromDS 欄位:用來指出這個封包是否是傳到一個 Infrastructure 無線網路中的 Distribution Set(通常是 AP)。
   d. More Fragments 欄位:這裡記錄此封包是否為已經分割過的封包，若上層協定中的封包內容已經遭到分割，則除了分割的最後一個段落或無分割外，此欄位的值都為 1。
   e. Retry 欄位:若此訊框內裝的是送方重送的封包，則值為 1。
   f. Power Management 欄位:此欄位說明該節點在此封包傳送結束後是否

進入省電狀態，若是則此值為 1。

g. More Data 欄位:若有目標正從省電狀態中醒來且接收封包，則 AP 會將其送出封包的這個欄位值設為 1，以讓目標節點得知在其睡眠時有一個以上的封包等待它接收。

h. WEP 欄位:若此值為 1 則說明此封包經過 WEP 加密，送至目的地時需要解密才能獲得封包內容。

i. Order 欄位:當封包使用分割傳送時，如果採取前後有順序的傳送(Strict Order)，則此值為 1。

2. Durarion/ID 欄位:此欄位有三種不同的作用，分別是設定 Network Allocation Vector(NAV)、標明是否為免競爭期(Contention-free)發送的訊框以及 PS-Poll 訊框。設定 NAV 代表此封包標明了網路介質將有多少忙碌時間而不能被使用，而在免競爭期中會將此 NAV 數目設定為一極大值，以避免他人佔用網路產生干擾。PS-Poll 訊框則負責紀錄網路節點的省電睡眠期，在節點被喚醒時傳送堆積的資料封包。

3. 四個 Address 欄位:承襲了 Ethernet 的特性，WLAN 的位址表示仍使用 48Bits 的數值來表示實體位置(MAC/Physical Address)，如果第一個傳送的數值是 0，則代表為 Unicast；若數值為 1，Multicast；若全部的數值都為 1，則代表此次傳送為 Broadcast。在 WLAN 中的四個 Address 欄 位會因為不同類型的封包而有不同的代表意義，但總括來說它們會分別裝載以下資訊:

a. 目的地位址:封包最後抵達的位址

b. 來源位址:封包送出的來源位址

c. 收取者(Receiver)位址:此位址指出該封包該由何無線網路中繼站傳送，通常為 AP 位址。

d. 發送者(Transmitter)位址:此位址指出該封包是由何中繼站送出，通常只用在無線橋接器 (Bridge)之間封包的傳送。

e. Basic Service Set ID(BSSID):若在同一個地理區域範圍內有多個無線網路存在，則每一個無線網路被稱做一個 Basic Service Set (BSS)。在 Infrastructure 網路中，BSSID 即代表 AP 所使用的 MAC 實體位址；在 Ad Hoc 網路中則用用亂數產生 48Bits 的資料再套用部份規則以形成 BSSID。

一般來說這四個 Address 欄位在不同類型的訊框下會有不同的表現，有時某些欄位不帶有任何資料，會視該訊框的作用而定。由此可知 Address 的內容和欄位出現數也可用來判斷此封包的性質，幫助進行封包分析的工作。例如管理訊框和資料訊框，至少會有三筆 Address 分別有不同的作用，而控制訊框上記載的

Address 則可能只有一至兩個。

4. Sequence Control 欄位:主要和封包的分割傳送有關，其內容關係到如何將分割過的封包資料重組或丟棄重複接收到的封包區塊。

以上是 MAC 標頭的各欄位主要作用，不論是用什麼方法接收到的封包都能先對標頭資訊做分析，利用得到的資料判斷是否該進行更深入的分析或丟棄封包。惡意的攻擊者也可以從標頭資訊得到網路的部份資料，用以部署其攻擊行動。但若真要分析封包內夾帶的重要資訊內容，在有加密的情況下就得開始著手解密的工作，將耗費一定的時間成本。所以加密的動作仍可以對封包做一定程度的保護，視所使用的加密方法而定。

MAC 訊框除了包含 MAC 標頭資訊外，還有訊框主體(Frame Body)。這裡裝載了此封包內含的資料酬載(Payload)或其他內容。訊框主體的內容分別定義了三種 802.11 運作模式的封包結構，分為: 控制訊框(Control Frame)，管理訊框（Management Frame），以及資料訊框（Data Frame）。控制訊框是用來作為頻道的宣告，載波感測的維護，以及資料接收的回應等工作，而管理訊框主要是用來執行管理功能用，例如加入或離開某一個無線區域網路，與擷取點的連接，身分認可等工作。另外，資料訊框就是一般用來傳遞網路上層所託付的資料的訊框格式，以下是 802.11 相關的訊框:

a. 控制訊框:控制訊框的型別辨識碼為01b，如表2:

表2: 控制訊框

序號	子型別辨識碼	訊框名稱
01	1010	PS-Poll
02	1011	RTS
03	1100	CLS
04	1101	ACK
05	1110	CF End
06	1111	CF End+CF-Ack

b. 管理訊框:管理訊框的型別辨識碼為00b，如表3所示:

表3:管理訊框

序號	子型別辨識碼	訊框名稱
01	0000	Association Request
02	0001	Association Response
03	0010	Reassociation Request
04	0011	Reassociation Response

05	0100	Probe Request
06	0101	Probe Response
07	0110-0111	Reserved
08	1000	Beacon
09	1001	ATIM
10	1010	Disassociation
11	1011	Authentication
12	1100	Deauthentication
13	1101-1111	Reserved

c. 資料訊框:資料訊框的型別辨識碼為10b，如表4所示:

表4:資料訊框

序號	子型別辨識碼	訊框名稱
01	0000	Data
02	0001	Data+CF-Ack
03	0010	Data+CF-Poll
04	0011	Data+CF-Ack+CF-Poll
05	0100	Null Function (no data)
06	0101	CF-Ack (no data)
07	0110	CF-Poll (no data)
08	0111	CF-Ack+CF-Poll (no data)
09	1000-1111	Reserved

3. 無線區網監聽系統架構

3.1 無線區網監聽雛型系統架構

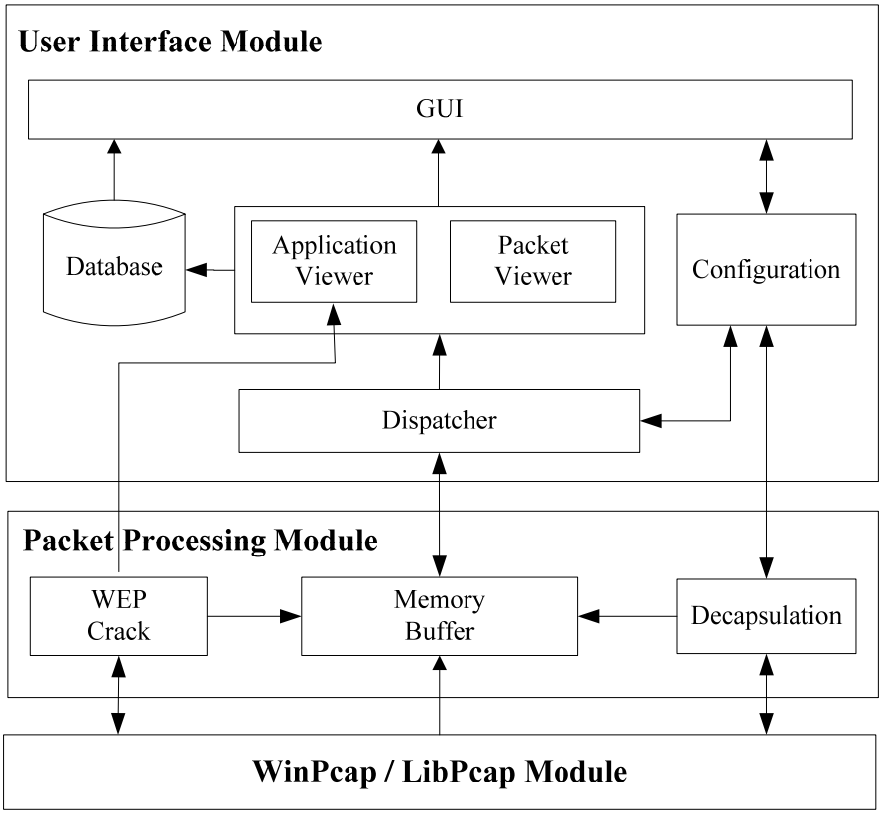


圖 5: 無線區網監聽雛型系統架構

本研究無線區網監聽雛形系統之架構如圖 5 所示。其包含使用者介面、無線封包處理和無線封包截聽三個模組。此架構將結合現行工具來達成無線區網封包擷取和 WEP 破解之功能。各模組內容如下:

(1) 無線封包截聽模組(WinPcap / LibPcap Module)

Pcap 是封包擷取函式庫，WinPcap 是一個針對 Win32 平台上封包擷取和網路分析的架構，它的主要功能就是讓網路卡所收到的封包能夠傳至系統中，讓系統知悉這個封包的完整架構以及內容。利用 WinPcap 的核心:網路封包過濾器(Netgroup Packet Filter，NPF)處理網路上傳輸的封包，並且提供可擷取(Capture)、發送(Injection)和分析性能(Analysis Capabilities)，此模組負責截聽收集無線封包，再提供至無線封包處理模組進行解封裝。

(2) 無線封包處理模組(Packet Processing Module)

1. Decapsulation 元件

解封裝模組所支援解析的協定包含第二層 802.11 (含 LLC SNAP 封裝) 協定

的解封裝處理單元；第三層 IPv4 協定的解封裝處理單元；第四層 TCP 與 UDP 協定的解封裝處理單元。

本系統內部以通訊協定描述子（Protocol Descriptor）資料結構表示封包的封裝資訊，而封裝資訊包括通訊協定類別、起始位址與長度。解封裝模組以解封裝處理單元建置表示封包封裝結構的通訊協定描述子串列資料結構。

封裝處理單元資料結構如下:

```
typedef struct 80211ProtocolDesc
{
unsigned int type;/* Header type,i.e IEEE802_11*/
unsigned int len;/* Header length */
unsigned int bytesoffset;/* Start offset*/
80211ProtocolDescriptor *next; /* Next header */
} *80211ProtocolDescr , **80211ProtocolDescr;
```

圖 6 為解封裝(Decapsulation)元件對 IPv4 封包的解封裝流程。首先解封裝模組由 WinPcap / LibPcap 模組取得 IPv4 封包 (如(1))，並由 802.11 處理單元開始進行解封裝處理。802.11 處理單元建構 80211 通訊描述子結點(如(a)) ，並經由 802.11 Type 標頭欄位得知其上層為 IPv4 格式，然後將封包交由 IPv4 處理單元(如(2))。IPv4 處理單元建構 IPv4 通訊描述子結點(如(b))，並經由 IPv4 NextHeader 標頭欄位得知其上層為 TCP 格式，然後將封包交由 TCP 處理單元(如(3))。TCP 處理單元建構 TCP 通訊描述子結點(如(c))，然後將封包捨去前端所有通訊協定標頭以取得 TCP 酬載(Payload)，並加上 TCP 酬載通訊描述子結點(如(d))，如此完成通訊描述子串列資料結構的建置。最後通訊描述子串列資料結構將存放於記憶體緩衝區中提供使用者介面模組進行後續的分析處理(如(4))。

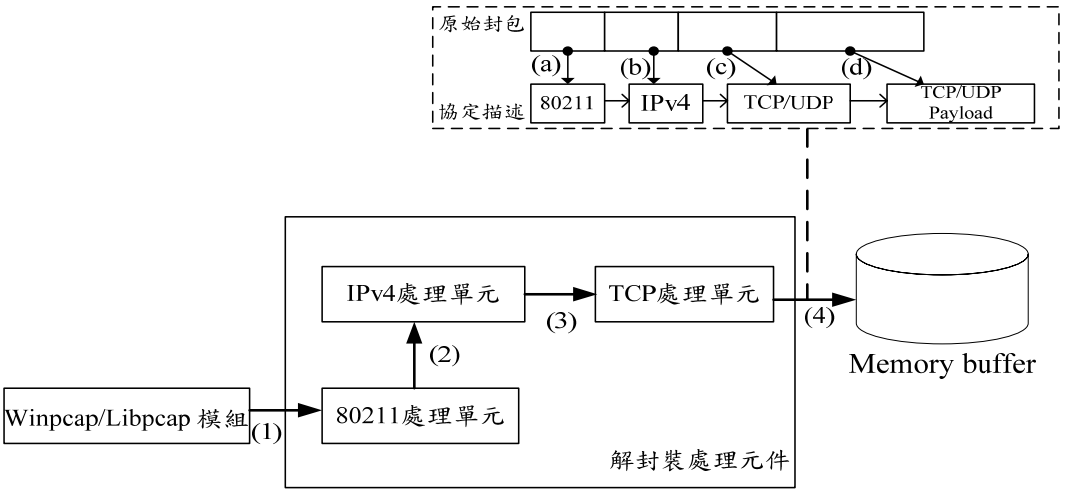


圖 6: 解封裝處理元件

2. WEP Crack 元件

利用現有工具 Aircrack-ng 實作功能達成破解 WEP 金鑰，WEP Cracker 定期從 Memory Buffer 或封包暫存磁碟檔案取得 WEP IV，在評估加密長度所需要的 WEP IV 量達到後，WEP Crack 並進行破解運算，並輸出至 Application Viewer 元件，Application Viewer 內含一個 WEP 金鑰與 Access Point 對照表。或輸入已破解之 WEP IV 可提供 WinPcap/LibPcap 模組進行截聽。

(3) 使用者介面模組(User Interface Module)

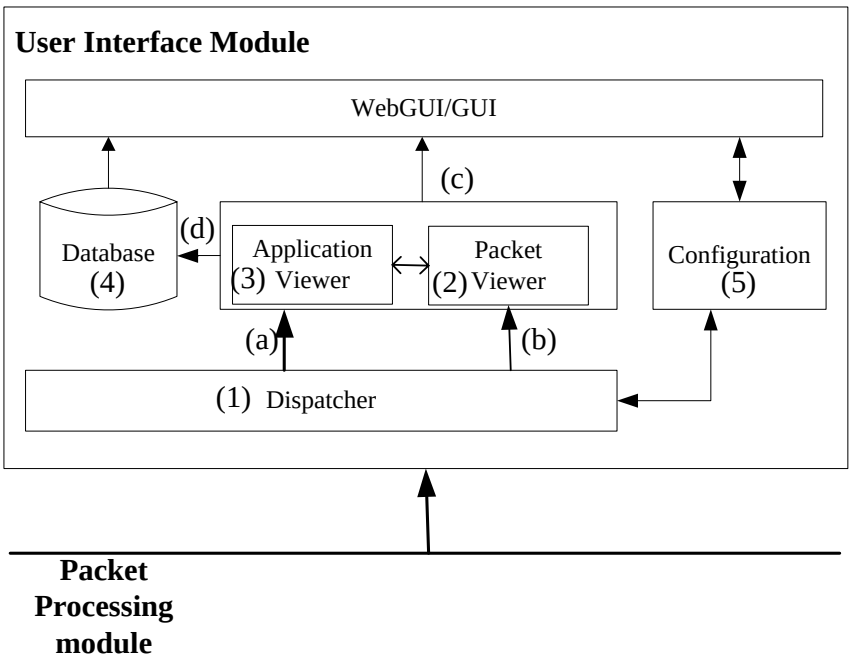


圖 7 :使用者介面模組

圖 7 為使用者介面模組，其元件功能描述如下:

1. Dispatcher 元件

Dispatcher 元件以詢問方式檢查到記憶體緩衝區內是否有新收集的封包，並從記憶體緩衝區取出新收集的封包。Dispatcher 元件會將封包傳送至 Packet Viewer 元件與 Application Viewer 進行封包應用層分析檢視之工作。

2. Packet Viewer 元件

Packet Viewer 元件首先將封包儲存成暫存檔，然後以現行軟體 Wireshark 封包分析器對暫存檔解析。最後將 Wireshark 封包分析器的協定解析輸出與封包的第二層、第三層、第四層通訊協定標頭傳到 GUI 元件並與 Application Viewer 元件分享解析資訊(如(b))。

3. Application Viewer 元件

Application Viewer 元件將 Packet Viewer 元件解析出的資訊取出應用層資料，並針對應用層協定封包進行應用層的重組還原。協定重組分析將於 4.4 章詳

細描述，將 Payload 分析並還原成 HTTP、FTP、SMTP/POP3、MSN 等協定。並將應用層資料，存入資料庫中(如(d))。並由 WebGUI 讀取資料庫中，應用層協定的監聽資料。

Application Viewer 亦接受 WEP Crack 的輸入，並使用 Hash dictionary 資料結構記錄金鑰與 AP、時間的對照表，如表 5。

表 5: Application Viewer 記錄表

AP BSSID	ESSID	Timestamp	Key	Encrption
00:14:6C:04:57:9B		2007/6/14 11:22:34	AE:66:5C:FD:24:E3:92:A 9:14:39:D4:27:4B	WEP (684002 IVs)

Application Viewer 元件首先解析應用層的通訊協定來判斷封包是否為 HTTP、SMTP、POP3、MSN 協定。例如:封包為 HTTP 協定，Application Viewer 元件根據封包中的 Sequence number 與 Acknowledge 標頭欄位將封包以 HTTP Session 分類並重組，並更新 HTTP 對話的 HTTP 封包計數器。最後將 HTTP 資訊結果傳到資料庫中。

4. 資料庫

資料庫接受 Application Viewer 的 SQL 輸入，將應用層資料轉存至資料庫。以下列表 6~12 為無線封包監聽資料庫之資料綱要，依通訊協定之特性進行欄位的記錄，可對照資料庫設計。

表 6 為 WEP 金鑰管理之資料表。

表 6: WEP 金鑰管理

AP BSSID	ESSID	Timestamp	Key	Encrption
00:14:6C:04:57:9B		2007/6/14 11:22:34	AE:66:5C:FD:24:E3:92:A 9:14:39:D4:27:4B	WEP (684002 IVs)

表 7 記錄 POP3 清單每封所寄出 email 的基本資訊，包括收信日期、時間、寄件者、寄件者 IP、收件者、副本、密件副本、主旨、大小和附加檔。

表 7:收件[POP3]

時間	寄件者	收件者	副本	主旨	信件內文	附加檔
2006-10-14 10:34:50	aaa@hotmail.com	bbb@cmo.com	NONE	test	Test…	Test.doc

表 8 記錄 SMTP 清單每封所寄出 email 的基本資訊，包括收信日期、時間、寄件者、寄件者 IP、收件者、副本、密件副本、主旨、大小和附加檔。

表 8: 寄件[SMTP]

時間	寄件者	收件者	副本	主旨	信件內文	附加檔
2006-10-14 10:34:50	aaa@hotmail.com	bbb@cmo.com	NONE	test	Test…	Test.doc

FTP 清單可記錄使用者每筆上/下傳的檔案記錄，包括日期時間、使用者帳號、使用者密碼、上/下傳模式、FTP 伺服器、檔案名稱，如表 9 所示。

表 9: FTP 記錄

日期	使用者帳號	使用者密碼	模式	伺服器	檔名
2006-10-14 10:34:50	anaon	541234	上傳	ftp.cvs.com	Upload.php

Website 記錄共有 2 個部分:

- 網頁記錄 [HTTP]

HTTP 網頁清單可記錄瀏覽網頁之網址、時間和使用 IP，如表 10 所示。

表 10: HTTP 網頁記錄

IP	時間日期	URL
192.168.0.1	2007-04-01 13:34:45	www.tomcat.com.tw

- 網頁內容記錄 [HTTP (Dynamic)]

在網頁內容記錄的資料中，系統會記錄網頁內容的文字部分，並將非文字部分加以過濾處理，以減少硬碟空間使用，如表 11 所示。

表 11: HTTP 內容記錄

IP	時間日期	URL	離線瀏覽
192.168.0.1	2007-04-01 13:34:45	www.tomcat.com.tw	/flash/index.htm

MSN 清單可記錄使用者每筆交談記錄，包括對談日期時間、發話者帳號、收話者帳號、交談內容 、交談筆數，如表 12 所示。

表 12:MSN 內容記錄

IP	時間日期	發話帳號	收話帳號	交談內容	交談筆數
192.168.0.2	2007-04-01 13:34:45	ss@hotmail.com	sbver@hotmail.com	會議延期	5

5. Configuration 元件

使用者透過 GUI 可以設定無線封包監聽之篩選(Filter)條件，此 Configuration 元件會傳遞指令於 Dispatcher 元件使符合使用者監聽需求之封包將傳送至 Packet Viewer 元件與 Application Viwer 於 GUI 進行封包應用層分析檢視之工作。

3.2 監聽流程

監聽流程如圖 8 表示:監聽活動一開始會將偵測出監聽範圍內之 AP 與 Client，即將監聽目標之相關資訊提供給封包截聽模組進行抓取封包，封包截取並儲存成 pcap 檔案再提供封包處理模組進行分析，顯示至使用者介面。

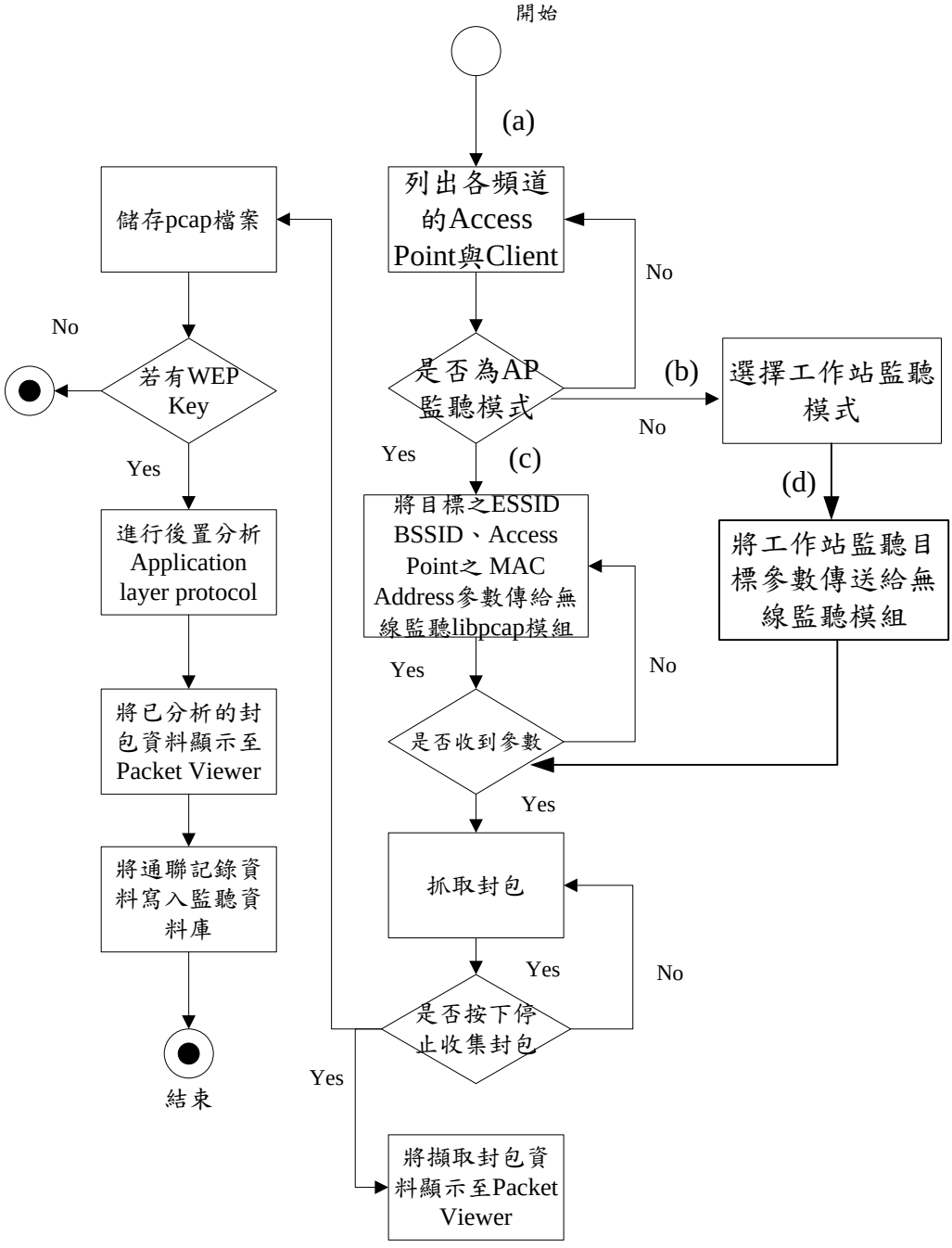


圖 8: 監聽流程

監聽流程(a)為啟動監聽介面，若為選擇 AP 監聽模式針對所選擇偵測 AP 目標，系統即開始進行資料偵測。在ＡＰ監聽模式中，可選擇依無線基地台的頻道 (By Channel) 為偵測目標， 選擇清單內無線基地台頻道值，按下送出監聽參數鈕，系統即開始針對頻道進行偵測。表 13 為 AP 監聽模式的功能欄位:

表 13: AP 監聽模式功能

AP 監聽模式功能項目說明			
對象	無線基地台監聽模式		
擷取封包量	封包流量大小	**自動收集**	自動模式下系統裝置、存取設定，開始/停止執行。
及時監聽條件	及時監聽設定規則條件	**BSSID**	顯示 AP MAC 值
收集過濾條件	設定一般側錄條件	**頻道**	顯示 AP Channel 值
儲存 scan 資料	AP、STA 資訊儲存清單	**MB/S**	顯示頻寬速率
更新頻率	設定更新時間頻率/每秒	**金鑰**	顯示 WEPKEY 狀態值
開始/結束	啟動/停止	**強度**	顯示訊號強度
By Channel	設定依選擇頻道側錄	**BEACONS**	顯示 Beacon 封包
By Channel + Ap	設定 Channel +AP	**封包量**	顯示封包數量
Ap	設定 AP 目標標示功能	**ESSID**	AP ID
掃瞄	顯示訊號強度偵測表	**STA**	顯示目前連結 AP 的使用者數量

若選擇圖 8 流程(b)，則在 STA 工作站端監聽模式(MODE STA)，針對所選擇監聽 Client 目標(流程(d))，按下送出監聽參數，系統即開始進行資料偵測。表 14 說明 STA MODE 功能項目。

表 14: STA MODE 功能

STA MODE 功能項目說明			
對象	STA:Client 端監聽模式		
擷取封包量	封包流量大小	**自動收集**	自動模式下系統裝置、存取設定，按下開始/停止執行。
及時監聽條件	及時監聽設定規則條件	**CLIENT MAC**	顯示 Client 端網卡 MAC 值 # :顯示網卡資訊 ip:顯示網卡 ip 資訊
收集過濾條件	設定一般側錄條件	**強度**	顯示訊號強度

儲存 scan 資料	AP、STA 資訊儲存清單	**封包量**	顯示封包數量
更新頻率	更新時間頻率/每秒	**BSSID**	顯示 AP 的 MAC 值
開始/結束	啟動/停止	**金鑰**	顯示 WEPKEY 狀態值
STA	設定 Client 目標標示功能	**頻道**	顯示 AP Channel 頻道值
掃瞄	顯示訊號強度偵測表	**ESSID**	AP ID

選定目標之後，按下系統參數送出按鈕，主控台會將參數送給監聽擷取封包主機並開始擷取封包資訊(流程(c))。圖 9 顯示無線區網監聽之主控台；透過主控台進行 AP 監聽或工作站端監聽。

圖 9: 主控台畫面

4. 無線區網監聽環境建置

4.1 監聽設備-網路卡介紹

(1) 網路卡類型

在 WLAN 中，裝設無線網卡即經由空氣中的頻道傳送和接收資料和 WLAN 通訊。欲執行無線監聽攻防將必須使用特殊的網路卡才能擷取到封包，表 15 整理目前較容易取得且實際可執行監聽的網卡資訊，供參考以進行選購。

表 15: 網路卡類型整理

晶片組	廠牌	型號	介面類型	備註
Acx100 (802.11b)	D-Link	DWL-120+	USB	
		DWL-520+	PCI	
	Samsung	2350c	CF	
		SWL-2300P	PCI	
Cisco	Cisco	Aironet 340	PCMCIA PCI	
Prism/2/2.5/3 (802.11b)	D-Link	DWL-122	PCMCIA	
	Senao	NL-2511CDPLUS	PCMCIA	200Mw 高功率 (收訊範圍大)
IPW2100/2200/2915/3945	Intel (Centrino)	Intel PRO/Wireless 2915 (a/b/g)	Chipset	
		Intel PRO/Wireless 2200 (b/g)		
		Intel PRO/Wireless 2100		
		Intel PRO/Wireless 3945(a/b/g)		
Atheros	D-Link	DWL-G650	PCMCIA	H/W: B1, B2, C1, C3
Orinoco	Agere (Lucent, Proxim)	Silver/Gold	PCMCIA/USB	
	HP/Compaq	W200	USB	
		WL215		
	Melco	BUFFALO WLI-USB-L11G-WR		
Ralink	D-Link	DWL-G122	USB	H/W: B1 F/W: 2.0.3
	ASUS	WL-167G	USB	

(2) 網路卡模式

網路卡在正常運作的情況下只會接收要送給自己的封包(當然也包括廣播與群播的訊息)，為了使網路卡能夠監聽網路上傳送的訊息，首要之務是要讓網路卡變成無所不收的型態運作。這樣的運作型態我們稱之為 Promiscuous mode。

進行監聽活動捕捉封包，首先需將無線介面切換為監聽模式(Monitoring Mode)，相當於Ethernet 介面的封包捕捉模式 (Promiscuous Mode)。啟動監聽模式的方法，會依無線驅動程式而異。並不是每一張網路卡都可以修改成 Promiscuous mode 運作，這樣的功能取決於網路卡製造商是否有提供開啟此項功能的機制，尤其是無線網路卡。目前已知提供Promiscuous mode 運作的802.11b無線網路卡有所有使用PRISM II 系列晶片的無線網路卡在Linux 上皆有提供這樣的機制，其他像Cisco 或 ORINOCO 有其他Windows 上的應用程式可以支援如Sniffer, AiroPeek 等等。以下列舉Prism與Atheros晶片組的網卡監聽模式設定。

1. Prism 無線網卡

採用 Prism 晶片組的網卡有兩種驅動程式可使用 :linux-wlan-ng (http://www.linux-wlan.org) 以及 HostAP 驅動程式 (http://hostap.epitest.fi)。linux-wlan-ng 驅動程式在 0.1.15 版本之後，將監聽列入為基本功能。它的啟動透過 wlanctl-ng 命令。

```
# wlanctl-ng wlan0 lnxreg_wlansniffer enable=true channel=6
```

若要關閉監聽模式:

```
# wlanctl-ng wlan0 enable=false
```

使用 Prism 晶片組的網卡可搭配 HostAP 驅動程式進行監聽。可自訂 private system call (類似無線延伸功能) 來啟動監聽模式。只要傳送監聽模式命令 (2 或 3) 給網卡，就可以啟動監聽模式。 模式 2 可以監聽所有標頭，模式 3 用來監聽 802.11 標頭。要關閉監聽模式，可以將模式設定為 0:

```
# iwpriv eth1 monitor mode
```

```
# iwpriv eth1 monitor 0
```

2. Atheros 無線網卡

Atheros 晶片組的網卡使用 MADwifi 驅動程式。2005 年 11 月版本之前的驅動程式可以用 iwconfig 命令將網卡切換為監聽模式。並可以使用 iwconfig 指定所要監聽的頻道，命令如下：

```
# iwconfig ath0 mode monitor
```

```
# iwconfig ath0 channel 11
```

2006 年之後的版本改用其他指令啟動監聽模式，改變模式指令如下：

```
# ifconfig ath0 down
```

```
# wlanconfig ath0 destroy
```

```
#wlanconfig ath0 create wlandev wifi0 wlanmode [sta|adhoc|ap|monitor|wds|ahdemo]
```

因此改變成 monitor mode 需先建立一個 VAP device，上一行最後模式選擇 monitor:

```
#wlanconfig ath0 create wlandev wifi0 wlanmode monitor
```

4.2 監聽環境架構

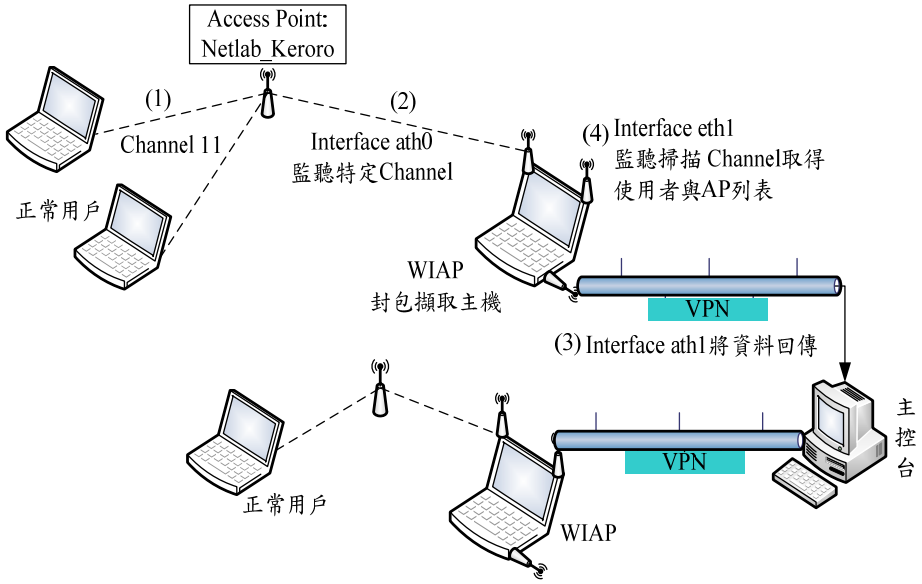


圖 10: 本研究監聽環境架構

(1) 環境簡述

- 正常用戶:作業平台 Windows XP。
- 封包擷取主機(WIAP): 為 Wireless Intercepted Access Point 縮寫命名。作業平台 Ubuntu Linux 7.04 (Kernel 2.6.20)，設置有三個無線網路介面卡，運行軟體：Kismet Server、Aircrack-ng (破解 WEP、WPA)、命令伺服器。
- 主控台:作業平台 Windows XP。主控台為控制監聽動作的用戶端軟體。

本研究之監聽環境架構如圖 10 所示，Wireshark 封包擷取主機設置有三個無線網路介面卡，介面 ath0 負責監聽無線網路頻道 11 收集 802.11 封包，介面 eth1 監聽掃描取得使用者行動運算主機識別碼(MAC 位址)與 Access Point 之 ESSID、BSSID 以及 MAC 位址。其圖中之虛線傳輸內容說明如下(編號並無順序意義):

- (1)正常用戶透過 Netlab_Keroro AP 存取無線網路；
- (2)封包擷取主機(WIAP)之介面 wlan0 監聽無線網路 Channel 11，收集 802.11 封包；介面 wlan1 監聽所有頻道的 Access Point，掃描取得使用者行動運算主機識別碼(MAC 位址)與 Access Point 之 ESSID、BSSID 以及 MAC 位址。
- (3)封包擷取主機(WIAP)之介面 wlan0 將已擷取封包資料存檔並新增為一筆監聽紀錄。在 WIAP 與主控台無線網路涵蓋範圍之內，WIAP 與主控台

連結方式可以 VPN 無線網路連結。若 WIAP 與主控台在無線網路涵蓋範圍之外，則可考慮使用增益天線以增加接收範圍。若使用增益天線使涵蓋範圍增大亦無法達成傳輸工作，則應考慮 WIAP 收集封包資料採離線方式傳送處理。

- (4)介面 wlan1 監聽掃描頻道取得使用者與 AP 列表。

啟動背景程序為剖析遠端系統收集封包(pcap 檔案格式)，當使用者有需要作監聽資訊的上層協定處理，如:還原封包或將封包內的應用程式資訊重組時，後置背景程序將需要啟動。

通常無線網路監聽主控台啟動的時候，會先啟動接收程序，分為一般 AP 資訊接收，以及截聽檔案由移動式封包收集電腦後送回來。背景程序會將收到的 pcap 檔案，作重組還原。執行此動作的前提是要有已破解的 WEP/WPA 金鑰。若無金鑰資料，則無法還原。先將收集到的資料歸檔為待處理資料。

4.3 無線封包解密/分析實作

(1) 實驗器材

硬體平台

1. [筆記型電腦] Acer TravelMate 290 (Intel Centrino 1.5Ghz / 1256MB RAM)。
2. [Wireless 網卡] D-Link DWL-G650 PCMCIA 介面 (H/W version: C3 F/W version: 4.3.1)。
3. [Wireless AP] Buffalo G54 Airstation (支援 802.11b/g) 開啟 WEP 加密，AP 名稱為 Netlab_Keroro。

軟體平台/工具

1. Ubuntu 7.04 Fiesty Fawn / Linux Kernel v2.6.20-15
2. aircrack-ng v0.6.2
3. kismet v2006.04.R1
4. WireShark v0.99.4

(2) 實驗步驟

1. 將 Wireless 網卡設定為 Monitor mode

利用 aircrack-ng 提供的 airmon-ng 可以將 DWL-G650 設定為 Monitor mode。DWL-G650 提供之介面名稱有 athX 與 wifiX，請依照以下步驟將 wifiX 衍生出另一 athX 介面來進入 Monitor mode，原有的 athX 介面並不提供 Monitor mode 切換。(假設原有介面名稱為 ath0 及 wifi0)

```
root# airmon-ng start wifi0
```

wifi0 介面會衍生出另一 ath1 之模擬介面，可將 ath1 切換為 Monitor mode。

```
root# iwconfig ath1 mode Monitor
```

此時可在 iwconfig 中看到 ath1 介面模式已切換為 Monitor (Mode: Monitor)。

2. 利用 kismet 偵測空間中有哪些正在活動中的 Wireless Device

kismet 可以解析空間中傳送的 beacon frame，分析其來源然後列於使用介面中。首先需要更改 kismet 的設定檔，使其利用 DWL-G650 進行擷取封包的工作:
修改/etc/kismet/kismet.conf (line 22):

source=**madwifi_ag,wifi0,kismet**

存檔後執行 kismet:

```
root# kismet
```

kismet 會開始蒐集空間中由各種 Wireless Device 中來往的 Probe request 與 response，作成 SSID 列表，如圖 11 為 kismet 搜尋無線網路的所在，偵測出無線

基地台設備。

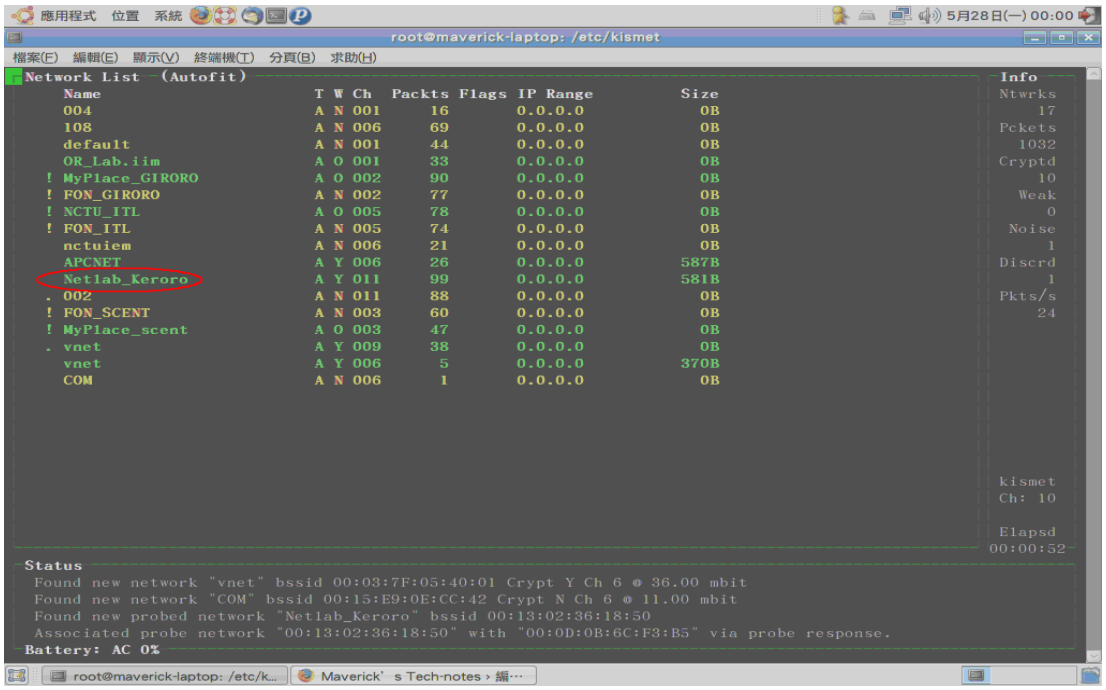


圖 11: Kismet 無線網路偵測

當無線網路蒐集到一定的量時，就可以開始進行各種排序(按 s 切換排序)，並選定 SSID 後按 Enter 可以進入該網路察看細節內容，圖 12 為 Netlab_Keroro 之 BSSID、網路形式、Channel、訊號強弱等 AP 資訊。在此我們用 kismet 選定 SSID(或 Channel)，使擷取封包的步驟能縮小範圍。

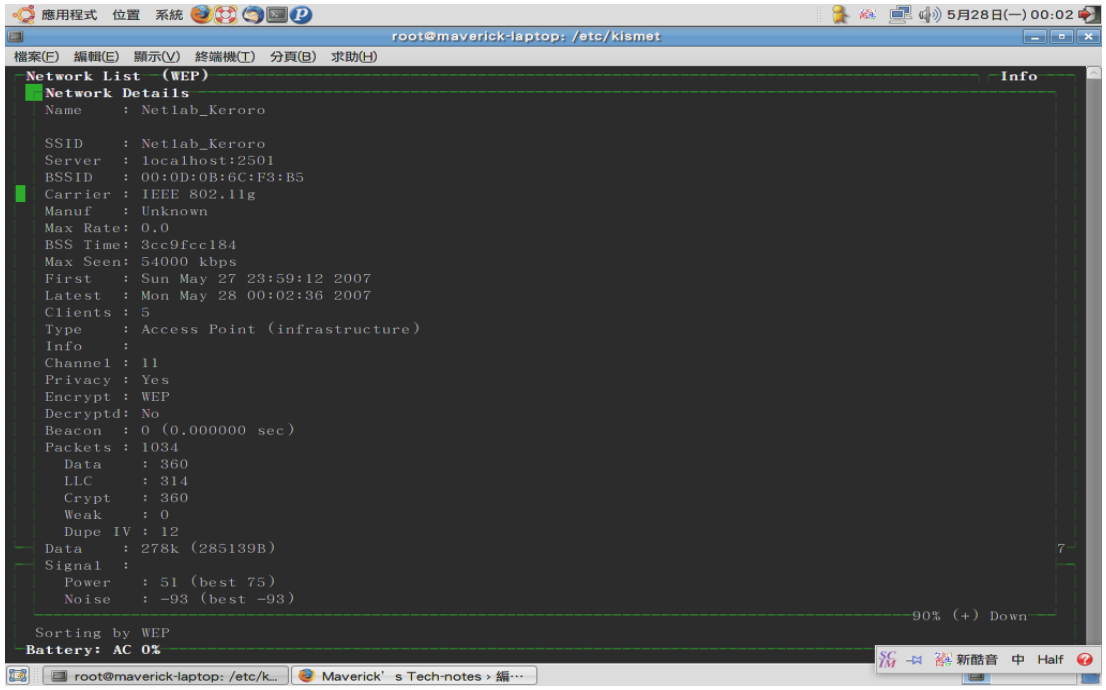


圖 12: Netlab_Keroro AP 資訊

3. 選定 Channel(SSID)進行擷取封包與 WEP 破解

由 kismet 中我們選定 Channel 11 作為無線網路卡監聽的頻道，在此頻道中我們以擷取 **Netlab_Keroro** 此 AP 的封包資訊進行 WEP 破解，如圖 13 顯示出頻道 11 的無線網路。

利用 aircrack-ng 中提供的 airodump-ng 可以鎖定 channel 或 ESSID 作為擷取封包的 filter，而我們只需要它存下封包中的 IV 值，依以下指令 airodump-ng 即開始擷取空間中 Channel 11 內的封包資料:

root# airodump-ng --ivs --channel 11 --write wifi0

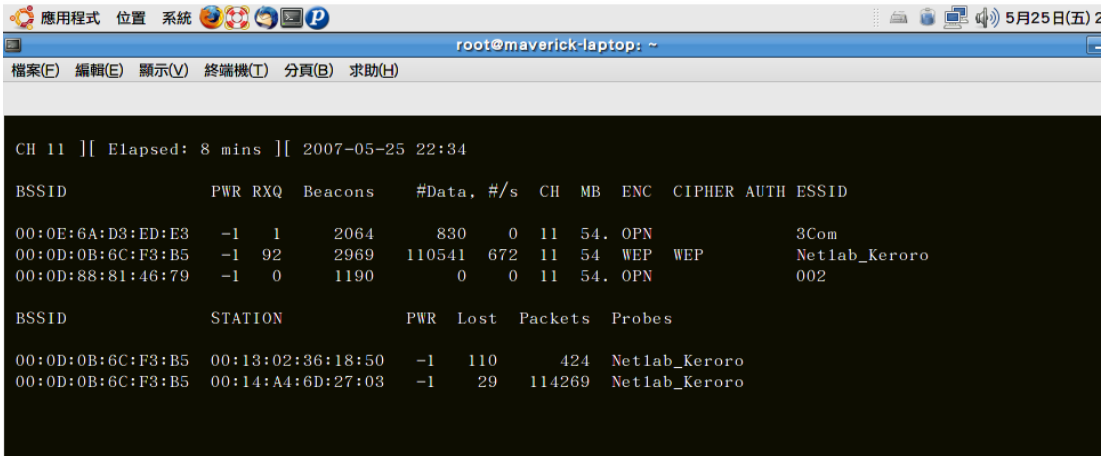


圖 13: 監聽頻道 11

由於 WEP 破解需要數萬到十萬個封包不等，才能獲得足夠的 IV 進行比對運算。當擷取的封包數量足夠後可按 Ctrl + c 跳出 airodump，所有的 IV 會儲存於目前所在目錄下之.ivs 檔案當中。這時可以透過 aircrack-ng 來進行 WEP 的破解運算，由於預先已知此 Network 的 WEP 屬於 64bit 加密，所以在參數中設定為 64bit 資料長度，以節省時間。

root# aircrack-ng -a 1 -n 64 -f 2 wifi0.ivs (wifi0.ivs 為擷取之 IV 檔案)

aircrack-ng 找出 WEP 加密金鑰，如圖 14 所示(Hex 與 ASCII):

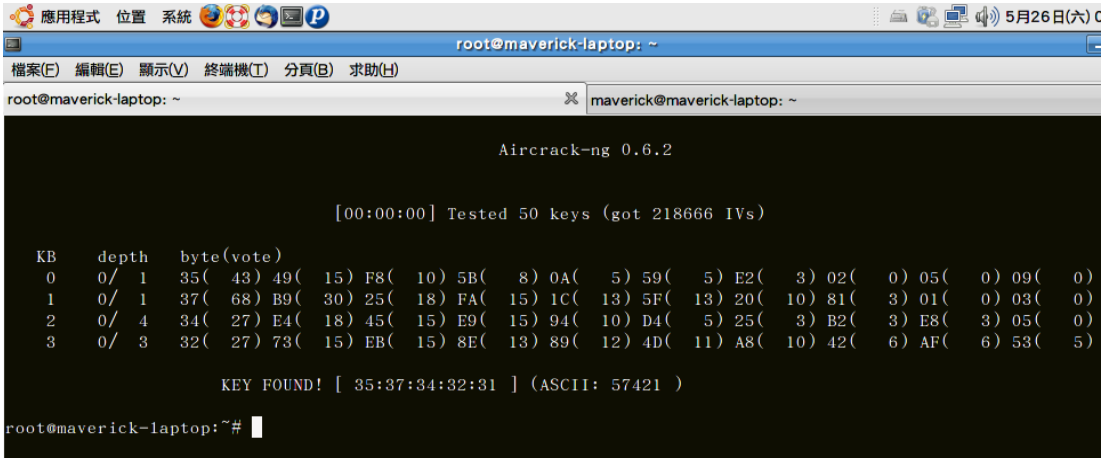


圖 14: Aircrack-Ng WEP 破解

4. 利用 WireShark 抓取封包後進行解析

WireShark(前身為 Ethereal)可以同樣進行封包擷取的動作，但其可以將封包解構，讓使用者看見封包內的樹狀結構與內文。而 WireShark 在 802.11 協定封包的解構中也支援使用預先填入的 WEP key 來對已經被 WEP 加密過的封包進行解析，解析後的 802.11 封包就會有可以展開分析的內文。

首先必須要開啟 WireShark，在 Preference 的 Protocols 中點選 IEEE 802.11 選項，接著利用先前 aircrack-ng 破解出的 WEP 金鑰以 ASCII 的 HEX 原碼方式輸入。如圖 15 所示，輸入 WEP 金鑰: 57421。

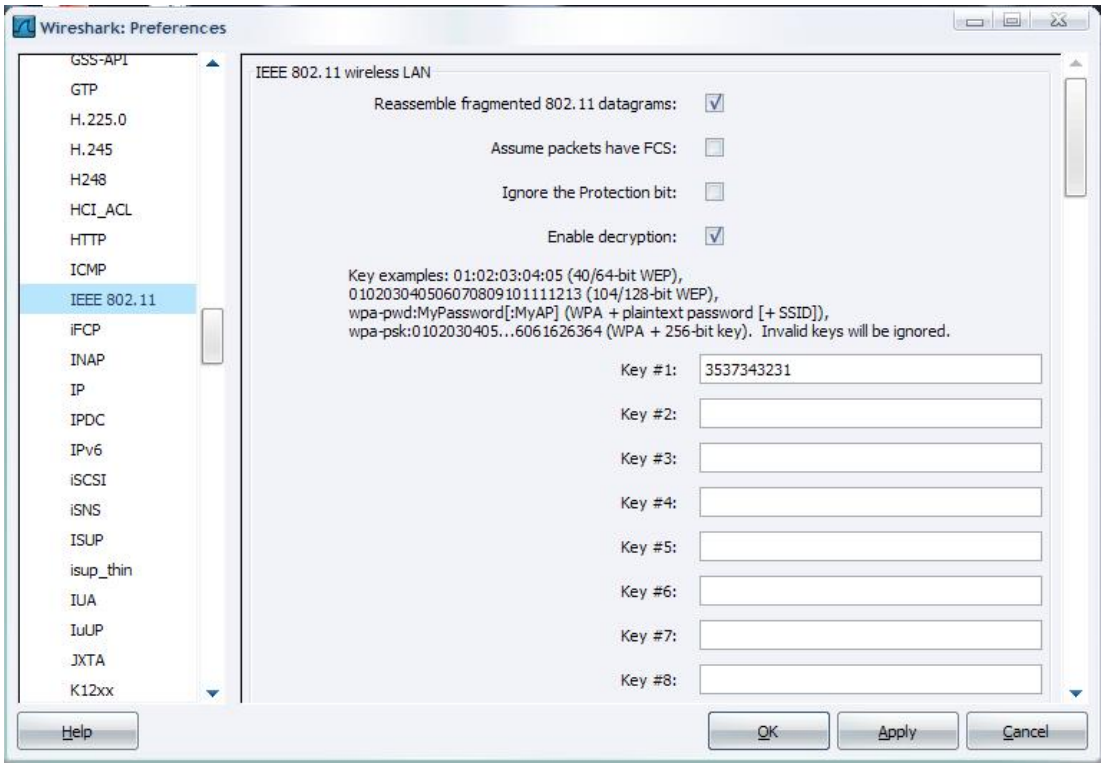


圖 15 : Wireshark wep 記錄金鑰畫面

接著開始使用 DWL-G650 擷取封包資料，當擷取到一定數量後就可以開始進行分析，WireShark 會自動將收集到的封包以我們輸入的 WEP Key 先行解碼後再顯示於視窗中，我們就可以清楚的看見這些封包的內文。圖 16 是收集 SMTP(E-mail)一連串通訊過程的封包，可以清楚的看見被解碼的信件內文。

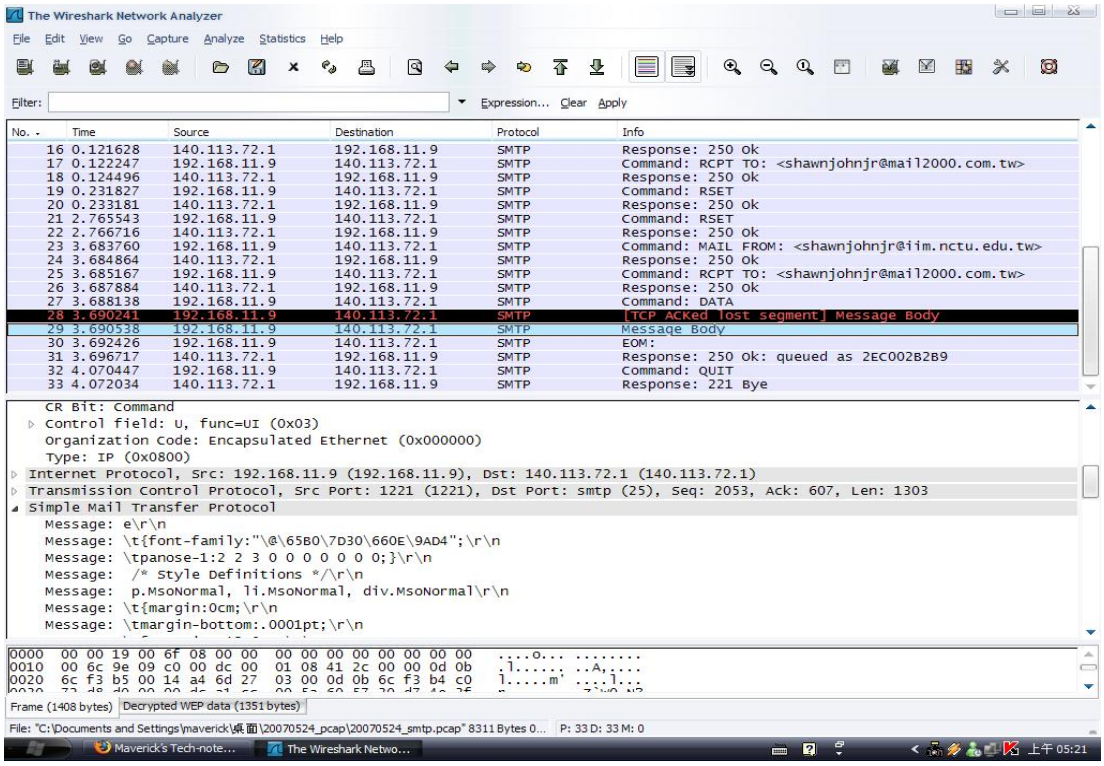


圖 16: SMTP 通訊封包

(3) 補充說明

本次實驗流程著重於利用 aircrack-ng 進行 WEP 金鑰破解，以及破解後的利用。如果需要在 Win32 環境下進行本次實驗，除了必須將無線網路卡設定成監聽模式以外，尋找 Wireless Network 的工作可以由簡單的 NetStumbler 等 War-Driving 工具來進行，而 aircrack-ng 和 WireShark 也已經出現 porting 到 Win32 平台(cygwin)的版本。所以如果位於 Wireless Network 傳輸量大的地區，進行無線網路的合法/非法監聽是相當容易的，特別是 aircrack-ng 已經具備破解 WPA/WPA2 的能力，且即使在資料傳輸量不大的地區，aircrack-ng 中附帶的 aircrack-ptw 工具也能自行對目標 Wireless Network 的 AP 傳送 ARP request，在短時間內也能獲得相當多的封包數量。

本系統預期能針對 WPA 加密的 PSK 模式(又稱為個人模式)進行金鑰破解，預先共用密鑰模式(pre-shared key，PSK， 又稱為個人模式) 是設計給負擔不起 802.1X 驗證伺服器的成本和複雜度的家庭和小型公司網路用的，每一個使用者必須輸入密語來取用網路，而密語可以是 8 到 63 個 ASCII 字元、或是 64 個 16 進位數字 (256 位元)。

WPA-PSK 的破解需要透過對 AP 的有效介入才能進行，必須使用 De-authentication 的手法先破壞一個 Wireless NIC 與 Access Point 的連線，再使用 replay 的手法攔截到 Access Point 與 Wireless NIC 之間的 WPA handshake 內容，一旦 handshake 內容資料被攔截到了以後就可以用來進行 WPA PSK 的破解。理論上欲進行此種破解手法，監察人員必定會影響到正常使用無線網路的使用者，所以並不建議實際的大規模使用，且此行動將會有機會被相關的無線網路管理者所發現。

4.4 通訊協定辨識

4.4.1 封包分類

網路是依層（layer）或級（level）的方式來組織，每一層的目的都是向它的上一層提供一定的服務，而把如何實作這一服務的細節對上一層加以隱藏。TCP/IP 參考模型中把網路體系分為了應用層、傳輸層、網路層和資料鏈結層。

當應用程序用 TCP 傳送資料時，資料被送入協定堆疊 (Protocol Stack)中，然後逐步通過每一層直到被當作一串 byte stream 送入網路。其中每一層對收到的資料都要增加一些標頭信息，TCP 傳給 IP 的資料單元稱作 TCP segment，IP 傳給網路介面的資料單元稱作 IP datagram，通過 Ethernet 傳輸的 byte stream 稱作訊框 (Frame)。

同樣在分解過程中，當目的主機收到一個 Ethernet 資料訊框時，資料就開始從協定堆疊中由下層往上，同時去掉各層協定加上的標頭。每層協定都要去檢查標頭中的協定標識 (Protocol Flag)，以確定接收資料的上層協定。

表 16 : TCP/IP 封包

<table>
<tr><td rowspan="2">傳輸層</td><td colspan="3">TCP header</td><td>Application data</td></tr>
<tr><td colspan="3"></td><td>TCP Payload</td></tr>
<tr><td rowspan="2">網路層</td><td>IP header</td><td>TCP header</td><td colspan="2">Application data</td></tr>
<tr><td></td><td colspan="3">IP Payload</td></tr>
<tr><td rowspan="2">資料鏈結層</td><td>Ethernet header</td><td>IP header</td><td>TCP header</td><td>Application data</td></tr>
<tr><td></td><td colspan="3">Ethernet Payload</td></tr>
</table>

表 16 為 TCP/IP 封包，資料鏈結層封包包覆著 IP 和 TCP 標頭。通過 WinPcap 得到的是 Ethernet 訊框，我們可以根據協定中的目的埠號、來源 IP 地址和來源埠號進行分解封包，過濾掉不包含 HTTP datagram 的 Ethernet 訊框，並抓取包含 HTTP 資料的資料部分。

封包分類主要是根據網路管理者所訂定的規則，將資料流區分為多種類別，具有分析封包標頭、以及檢視應用層內容的能力。封包分類的功能可以實作在硬體環境上，也可以是軟體的模組(Module)。一般來說，封包分類是以封包在網路層與傳輸層(Transport layer)標頭中的欄位作為分類的依據。找到封包符合的規則後，再執行相對應的分類政策(Policy)處理。執行的分類政策可能是為封包提供前述的進階網路服務，或者是網路管理者自訂的管理方式，比如將流經封包的相

關資訊存放進記錄檔中。

封包分類的發展傾向於檢視封包應用層(Application layer)內容所挾帶的資訊，進行樣式比對(Pattern Matching)。進行應用層內容檢視(Content Inspection)，即能辨識使用非標準通訊埠的通訊協定，如使用通訊埠編號為 1111 的 HTTP；或是辨識使用隨機決定通訊埠編號的通訊協定，如點對點(Peer-to-Peer) 應用軟體。將控制訊息的規格訂定在應用層的通訊協定日漸增加。從較早提出的 FTP、SMT P、HTTP 等，都是屬於應用層通訊協定的範圍。因此，若希望無線監聽系統有能力分類出應用層通訊協定，封包分類功能就必須從傳統上的網路層、傳輸層的檢視，進階至應用層。

4.4.2 HTTP

(1) HTTP 協定特徵

HTTP的特徵，首先可以透過網站伺服器(Web Server) 使用TCP 連線與編號為80的標準通訊埠進行判斷。如果並非使用標準的通訊埠編號，可以在TCP連線完成三次握手協定之後，取得封包的應用層內容，檢視是否含有”H T T P / 1.1 ”字串。然而，HTTP 基本上是屬於無狀態的通訊協定:每一個HTTP要求(HTTP Request) 都是獨立的，網站伺服器也不會儲存HTTP Request的歷史記錄。圖17為HTTP狀態圖。

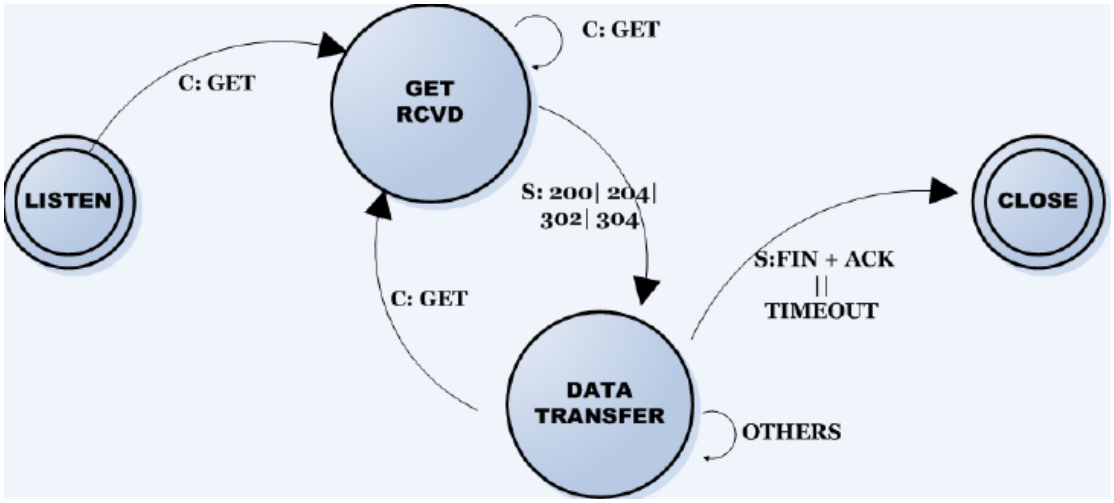


圖 17: HTTP 狀態圖

判斷 HTTP 協定之正規表示式，依照:

Status-Line = HTTP-Version SP Status-Code SP Reason-Phrase CRLF (rfc 2616)

```
http/(0\.9|1\.0|1\.1) [1-5][0-9][0-9] [\x09-\x0d -~]*(connection:|content-type:|content-length:|date:)|post [\x09-\x0d -~]* http/[01]\.[019]
```

較快速度的版本:

```
http/(0\.9|1\.0|1\.1) [1-5][0-9][0-9]|post [\x09-\x0d -~]* http/[01]\.[019]
```

(2) HTTP 協定分析

HTTP 使用 TCP Port 80 來進行資料傳輸。利用 WinPcap 程序設計時可以直接實作對 Port 資料的過濾，按照 HTTP Request 和 Response 格式抓獲所有的 HTTP 訊息。但是有大量使用代理進行網頁瀏覽的機器可能不通過 80 Port 來傳輸 HTTP 資料。

1. IP 與 TCP

每接收到一個 Ethernet 訊框，資料從協定堆疊中由底向上檢查 datagram 標頭的標識，去掉各層協定的 datagram 標頭，將不符合條件的封包丟棄，只保留運

行 HTTP 協定的封包。從資料鏈結層中的訊框標頭擷取 Ethernet 類型，判斷是否為 IP 封包。如果是 IP 封包，去除此訊框標頭，否則棄之。接著分析 IP 封包的標頭，如果 IP 標頭中的協定區段是 TCP 協定，則去掉 IP 標頭得到 TCP 封包，否則棄之。分析 TCP 封包的標頭，如果 Port 為 80，則截去 TCP 標頭，獲取 TCP 資料。

2. HTTP Message

HTTP 有兩類訊息封包，從客戶到伺服器的 Request 封包和從伺服器到客戶端的 Response 封包。客戶端發出一個 Request 封包給伺服器端，然後伺服器端再根據所收到的 Request 回應 Response 封包給客戶。

表 17: Request/Response 封包內容

Request 封包	GET /blogbus/blog/diary.php?diaryid=182145 HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0) Opera 7.20 [zh-tw] Host: www.blogbus.com Accept: text/html, application/xml;q=0.9, application/xhtml+xml;q=0.9, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: en Accept-Charset: utf-8, utf-16, iso-8859-1;q=0.6, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Cache-Control: no-cache Connection: Keep-Alive, TE TE: deflate, gzip, chunked, identity, trailers
Response 封包	HTTP/1.1 200 OK Date: Tue, 06 Jul 2004 07:34:30 GMT Server: Apache/1.3.29 (Unix) PHP/4.1.1 X-Powered-By: PHP/4.1.1 Connection: close Transfer-Encoding: chunked Content-Type: text/html <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"> <html> <head>

如表 17 為 Request/Response 封包內容。Request 封包的第一行為 Request 行，Request 行以下是 Request 封包的標頭，在標頭後有一空行。Request 行由 Request 類型、連接地址和版本號組成。其中通過代理的 Request 行中的鏈接地址顯示為絕對路徑，沒有通過代理的 Request 行的鏈接地址顯示相對路徑，主地址在標頭的「Host:」字段之後。上表中的範例是沒有通過代理的 (HTTP Proxy)。

Response 封包的第一行為狀態行，由 HTTP 版本號、狀態碼和狀態字串組成，狀態行之後直到空行為狀態行標頭。空行之後就是 HTTP 資料。當 HTTP Response 封包標頭的 Content-Type 為 text/html 時，Response 封包的內容就是 html 檔案。網頁檔案寫在<html>和</html>標籤之間，<head></head>標籤定義了檔案的標頭。當 Content-Type 為 image/gif 時，表示 Response 封包的內容是 image 圖片且是 gif 格式的。常見的圖片格式還有.jpg 和.bmp。有無代理的情況稍有不同，只是在有代理的 Request 行中，鏈接地址為絕對路徑。

(3) HTML 頁面還原

瀏覽網頁時，客戶端首先向伺服器發出 HTTP Request 封包，伺服器做出相應的 Response，以 HTTP Response 封包返回。Response 封包的序列號 (Sequence number)等於相應的 Request 封包的確認號 (ACK number)。然而 IP datagram 最大為 1500B，一般的頁面內容卻都在 10KB 以上，要用多個 Response 封包才能完成一個頁面的傳輸。頁面傳送時，資料被分割了成多個 IP datagram。接受端收到這些資料後按照封包序列的順序將它們重新組合起來，然後以 HTML 頁面返回給客戶端。TCP 在三次握手(three-way handshaking)建立連接時確定了開始傳輸第一個 segment 的序列號和確認號。由於 TCP 連接完全是雙向的，傳輸過程中雙方資料是獨立的，因此傳輸同一頁面的所有 segment 的確認號不會改變，序列號依次增加。

重組頁面就可以根據確認號判定傳輸該頁面的所有封包。首先根據客戶端的 Request 得到與 Request 封包對應的第一個 Response 封包，依照該頁面的確認號，查找最近接收到的相同確認號的封包，這些封包都是用來傳輸同一頁面的。然後按照包的序列號的順序，將封包中傳輸資料部分依次保存下來，這樣就完成了頁面內容的恢復。

網路資料處理的流程如下表 18 所示。在程序中，使用 WinPcap.dll 提供的 API 函數設置和抓取網路設備上傳輸的資料。主要的函數有 pcap_findalldevs、pcap_open_live 和 pcap_loop 等。依照 HTTP 訊息所在封包在訊框標頭、IP 標頭和 TCP 標頭的 FLAG，過濾掉不包含 HTTP 訊息的封包。也可以用 pcap_compile 和 pcap_setfilter 直接設定封包過濾的表達式 (Expression)。

表 18: HTML 頁面重組流程

處理流程	內容描述
封包抓取	利用 pcap 函數庫從 WLAN 中截獲封包
封包過濾	分析封包並擷取 Port 為 80 的 TCP 資料
HTTP 訊息解析	確定 Request 包與 Response 包的確認號和序列號
HTML 頁面瀏覽	以 Response 包的序列號重組、HTML 頁面並顯示

4.4.3 FTP

(1) FTP 特徵

FTP 通訊協定是由 RFC 959 File Transfer Protocol（FTP）所定義。圖 18 為 FTP 傳輸架構，Server 端與 Client 端之間共建立兩個 Socket 連結，一個以 FTP 通訊協定預設之通訊埠 21 作為兩者間之通訊連線，另一個連結則是作為 Client 端傳送指令與 Server 端回應結果之用。

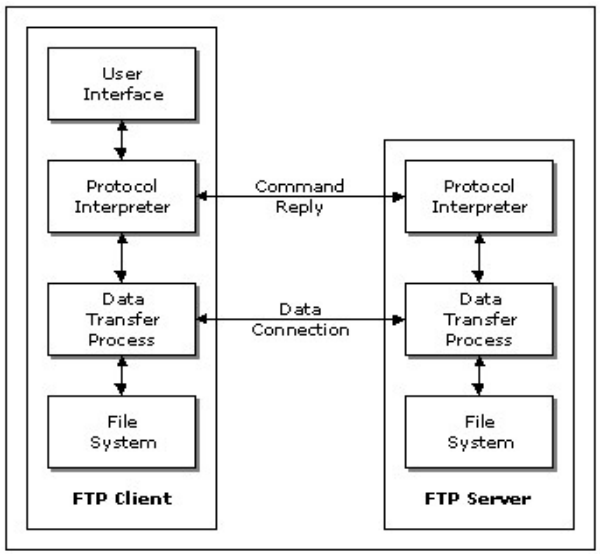


圖 18 : FTP 架構

Client 透過 FTP 通訊協定傳至 Server 端的指令如表 19 是經過對應轉換的:

表 19 : FTP 客戶端與伺服器端指令對照表

Client	Server	說明
User <username>	USER <username>	使用者帳號
Password <password>	PASS <password>	使用者密碼
bye/quit	QUIT	登出 FTP Server
ascii	TYPE A	ASCII 模式
binary	TYPE I	Binary 模式
get <filename>	RETR <filename>	下載檔案
put <filename>	STOR <filename>	上傳檔案
dir	LIST	瀏覽 FTP Server 目錄
ls	NLST	瀏覽 FTP Server 目錄

cd <pathname>	CWD <pathname>	變更 FTP Server 目錄
pwd	XPWD	顯示 FTP Server 目前的工作目錄

Server 端 FTP 指令均以大寫表示，分別對應於一個 Client 端指令，共分為以下幾大類:

- 存取控制指令(Access Control Command):定義使用者的登錄名稱及密碼。
- 傳輸指令（Transfer Command）:定義資料或檔案的傳輸模式。
- 服務指令（Service Command）:定義處理檔案如上傳（Upload）、下載（Download）等的指令。

在此只針對傳輸檔案指令描述，由於上傳下載均為監聽 FTP 協定最重要之指令，故描述服務指令 (Service command) 如下:

1. RETR:為 Retrieve（取得）的縮寫，用於自 FTP Server 下載檔案之用，下表 20 為 RETR 的語法以及與 Client 端指令的對應:

表 20: RETR 語法

Client	**Server**
get <filename>	RETR<filename>

2. STOR:為 Store（儲存）的縮寫，用於上傳檔案至 FTP Server 之用，表 21 為 STOR 的語法以及與 Client 端指令的對應:

表 21: STOR 語法

Client	**Server**
put <filename>	STOR <filename>

3. APPE:為 Append（附加）的縮寫，當執行上傳檔案指令時，若該檔案已存在於 FTP Server 端，則會附加於原本的檔案內容之後，其語法為:

```
APPE <filename>
```

4. ABOR:為 Abort（中斷）的縮寫，用於中止 FTP Server 執行之前 Client 端所下的指令。

5. RNFR、RNTO:分別為 Rename From 與 Rename To 的縮寫，用於變更 FTP Server 端的檔案名稱，其語法為:

```
RNFR <filename>
```

RNTO <filename>

6. DELE:為 Delete（刪除）的縮寫，用於刪除 FTP Server 端檔案，表 22 為 DELE 的語法以及與 Client 端指令的對應:

表 22: DELE 語法

Client	**Server**
delete<filename>	DELE<filename>

7. LIST:列出 FTP Server 端目錄與檔案的詳細內容，包括建檔日期、時間、檔案大小、目錄與檔案名稱等，LIST 語法與 Client 端指令的對應如表 23。

表 23: LIST 語法

Client	**Server**
dir [<pathname>]	LIST [<pathname>]

若系統分析以上 FTP control command 並監聽對應的 Data connection tcp port，便可追蹤無線網路使用者使用 FTP 傳輸檔案。

(2) 判斷 FTP 協定之正規表示式

^220[\x09-\x0d -~]*ftp

此規則可判斷較多，但較慢

^220[\x09-\x0d -~]*ftp|331[\x09-\x0d -~]*password

此規則更精準判斷，但需要較久的時間 (3 個封包)

^220[\x09-\x0d -~]*\x0d\x0aUSER[\x09-\x0d -~]*\x0d\x0a331

此規則精準判斷，但需要較久的時間 (2 個封包)

^220[\x09-\x0d -~]*\x0d\x0aUSER[\x09-\x0d -~]*\x0d\x0a

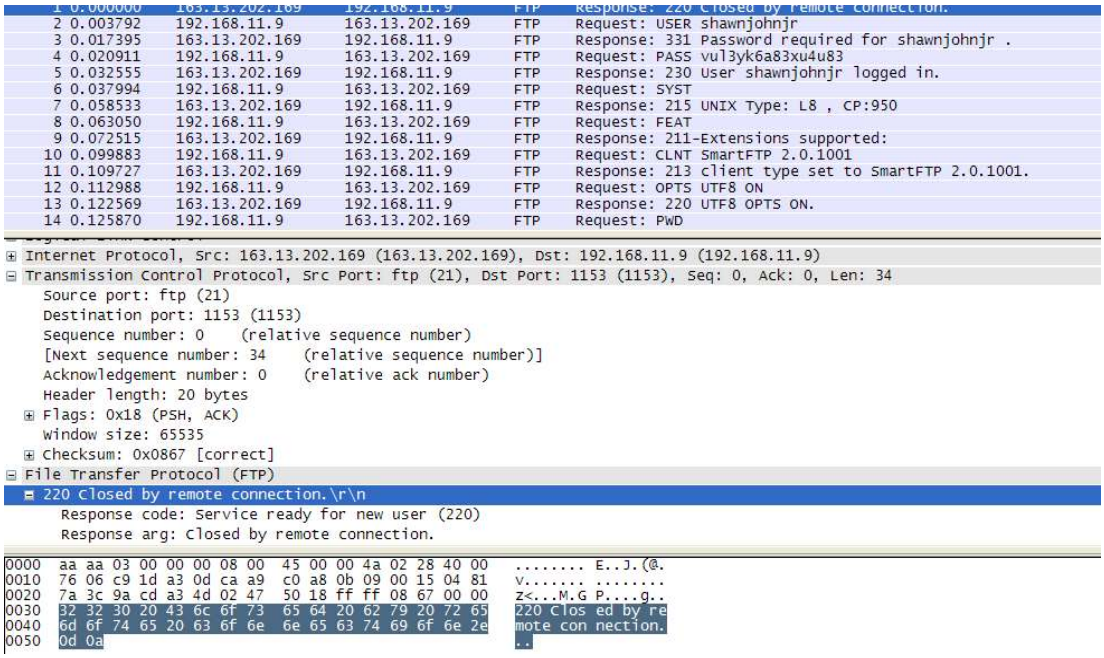


圖 19 :220 Response 220 Closed remote connection 封包訊息

如圖 19 所示為 Response 擷取封包訊息，封包訊息為 220 closed by remote connection。

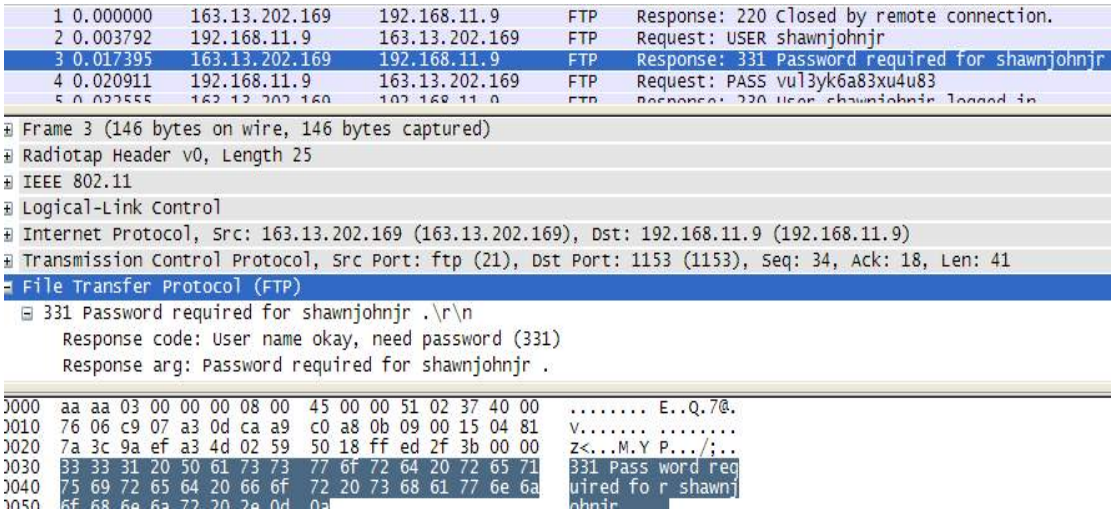


圖 20 :331 Password required

圖 20 為 Response: 331 Password required，訊息為 331 Password required for shawnjohnjr。

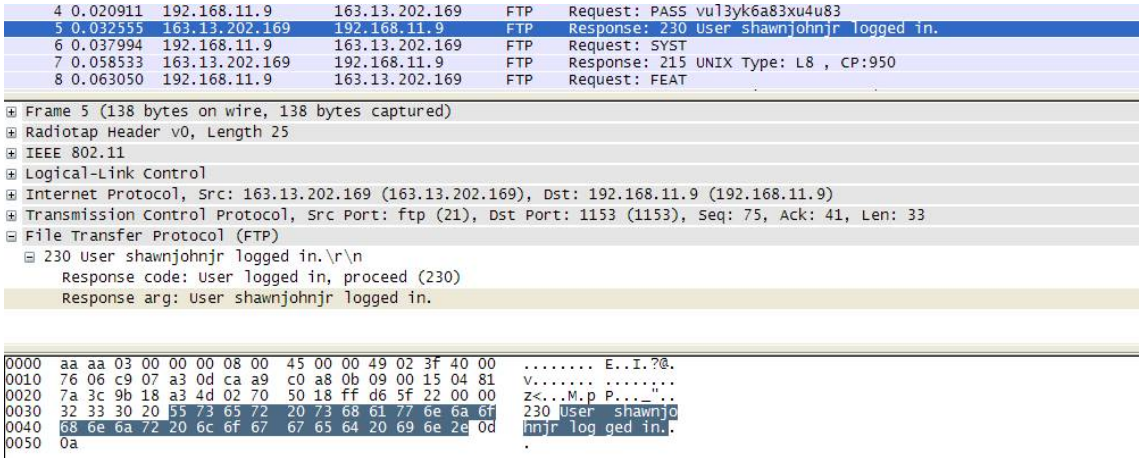


圖 21 : 230 Response user logged in

如(Response user logged in)封包擷取圖 21 所示，FTP 訊息主體為 230 shawnjohnjr logged in。

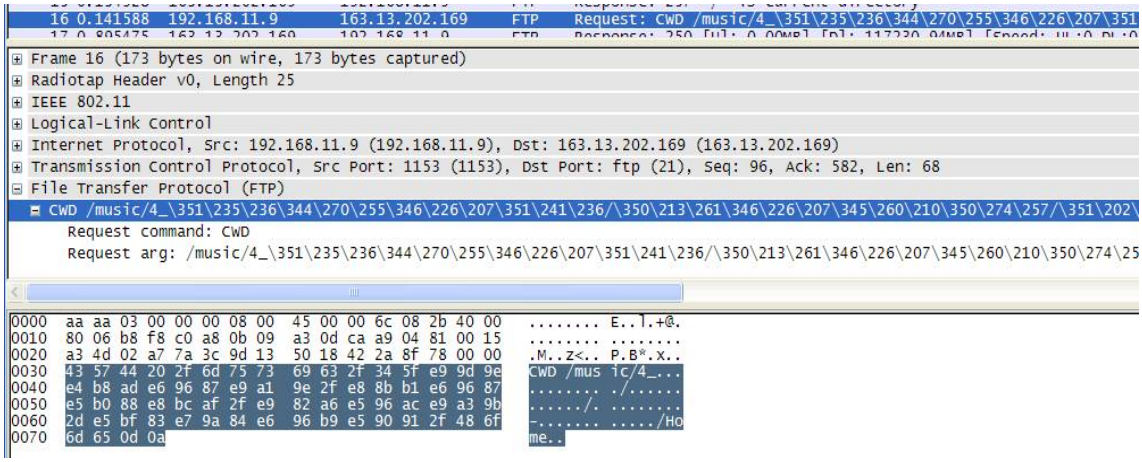


圖 22 : Change working directory

Request file 封包擷取如圖 22 中所示，FTP 訊息主體為 CWD + 目錄路徑。

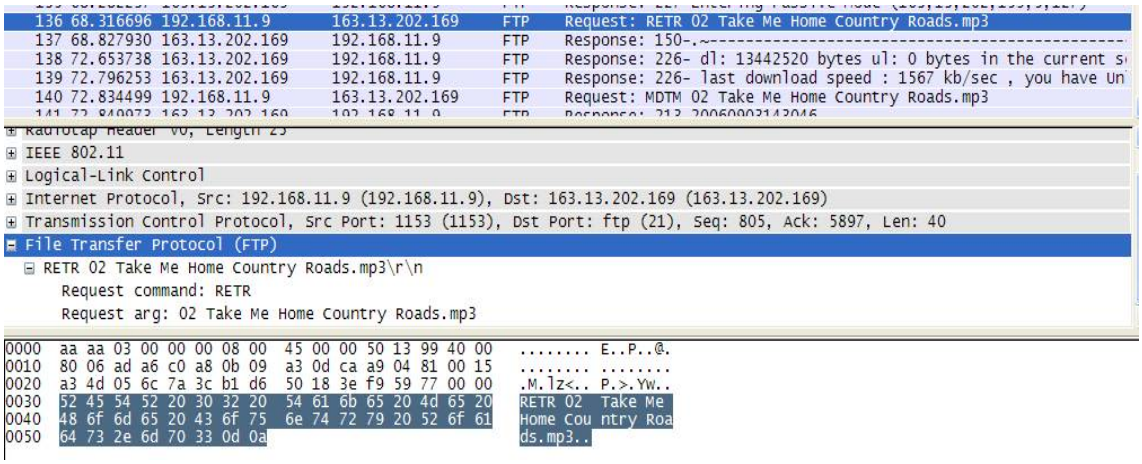


圖 23 : Retrieve data

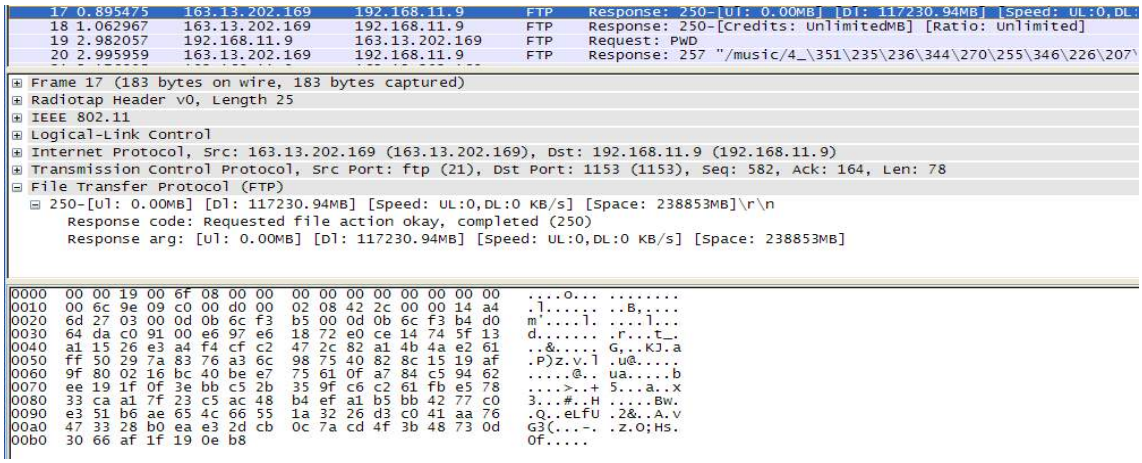


圖 24: 250 完成傳檔

從圖 23 封包細節內容可以獲知 mp3 檔案的傳輸；圖 24 檔案傳輸完成。

以下為 FTP Application 層傳輸範例:

USER shawnjohnjr

331 Password required for shawnjohnjr .

PASS vul3yk6a83xu4u83

230 User shawnjohnjr logged in.

SYST

215 UNIX Type: L8 , CP:950

FEAT

211-Extensions supported:

SIZE

MDTM

MDTM YYYYMMDDHHMMSS filename

LIST -laT

STAT -laT

MLST type*;lang*;size*;modify*;create*;UNIX.mode*;UNIX.owner*;UNIX.group*;WIN32.ea*

MLSD

REST STREAM

XCRC filename;start;end

XMD5 filename;start;end

TVFS

CLNT client_type

LANG EN;FR;JA;DE;IT;SV;ES;RU;ZH-TW;ZH-CN

UTF8

EPRT

EPSV

211 END

CLNT SmartFTP 2.0.1001

213 client type set to SmartFTP 2.0.1001.

OPTS UTF8 ON

220 UTF8 OPTS ON.

PWD

257 "/" is current directory

CWD /music/4_...../...../.....-...../Home

250-[Ul: 0.00MB] [Dl:117230.94MB][Speed: UL:0,DL:0 KB/s] [Space: 238853MB]

250-[Credits: UnlimitedMB] [Ratio: Unlimited]

250 "/music/4_...../...../.....-...../Home" is current directory.

PWD

257 "/music/4_...../...../.....-...../Home" is current directory

TYPE A

200 Type set to ASCII.

PASV

227 Entering Passive Mode (163,13,202,159,5,122)

MLSD

150 Opening ASCII data connection for ls /music/4_...../...../.....-...../Home.

226-free disk space under this directory : 238853 mb

226 Transfer finished successfully. Data connection closed .

CWD /music/4_...../...../.....-.....

250-[Ul: 0.00MB] [Dl: 117230.94MB] [Speed: UL:0,DL:0 KB/s] [Space: 238853MB]

250-[Credits: UnlimitedMB] [Ratio: Unlimited]

250 "/music/4_...../...../.....-....." is current directory.

PWD

257 "/music/4_...../...../.....-....." is current directory

PASV

227 Entering Passive Mode (163,13,202,159,5,123)

MLSD

150 Opening ASCII data connection for ls /music/4_...../...../.....-.....

226-free disk space under this directory : 238853 mb

226 Transfer finished successfully. Data connection closed .

CWD /

250 "/" is current directory.

PWD 257 "/" is current directory PASV 227 Entering Passive Mode (163,13,202,165,54,177)	MLSD 150 Opening ASCII data connection for ls /. 226 Transfer finished successfully. Data connection closed .

4.4.4 SMTP

(1) SMTP 協定特徵

SMTP的特徵，首先可以透過郵件伺服器(Mail Server) 使用TCP連線與編號為25的標準通訊埠來進行判斷。如果並非使用標準的通訊埠編號，可以在TCP連線完成三次握手協定之後，取得封包的應用層內容，檢視是否為SMTP的固定訊息格式，如220 Server Ready Code、250 OK Code，或是EHLO、MAIL、RCPT、DATA 等……SMTP命令，如圖25為SMTP 協定狀態圖。如果符合的話，即可辨別此連線為SMTP通訊協定。SMTP 屬於狀態化的通訊協定，客戶端與伺服器端都會共同維持通訊協定狀態的變化。

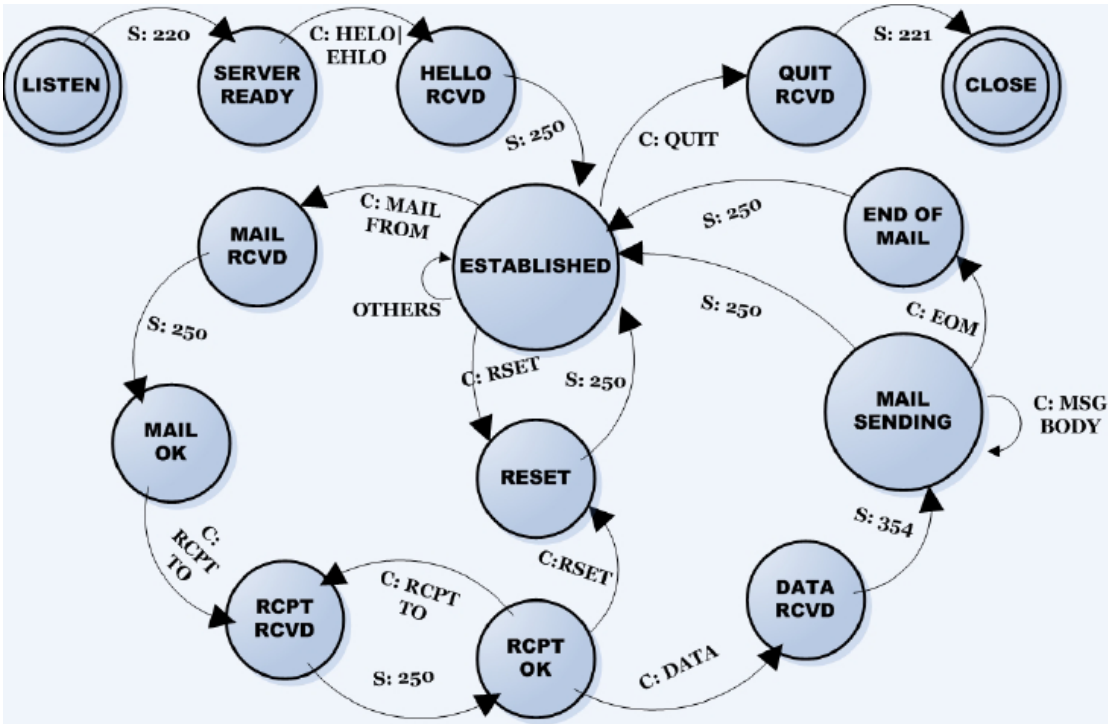


圖25 : SMTP 協定狀態圖

根據SMTP RFC中的所訂的規格敘述，SMTP 協定判斷正規表示式如下，表24為SMTP命令:

```
^220[\x09-\x0d -~]* (e?smtp|simple mail)
userspace pattern=^220[\x09-\x0d -~]* (E?SMTP|[Ss]imple [Mm]ail)
userspace flags=REG_NOSUB REG_EXTENDED
```

表 24 : SMTP 命令

SMTP 命令	命令功能
HELO	由用戶端傳送的命令，可識別其本身，通常會包含網域名稱。
EHLO	讓伺服器識別它對延伸的簡易郵件傳送通訊協定(ESMTP)命令的支援。
MAIL FROM	識別郵件寄件者；使用格式為 MAIL FROM:。
RCPT TO	識別郵件收件者；使用格式為 RCPT TO:。
TURN	允許用戶端及伺服器互換角色,並反向傳送郵件,而不需建立新的連線。
ATRN	ATRN (已驗證的 TURN) 命令會選擇性地取用一或多個網域作為參數。如果工作階段尚未經過驗證，則必須拒絕 ATRN 命令。
SIZE	提供機制，讓 SMTP 伺服器可用來指出所支援的郵件大小上限。相容的伺服器必須提供大小延伸，以指示可接受的郵件大小上限。用戶端不應傳送大於伺服器所指示之大小的郵件。
ETRN	SMTP 的延伸。ETRN 是由 SMTP 伺服器所傳送，用以要求其他伺服器傳送所有它擁有的電子郵件。
PIPELINING	提供傳送一串命令，而不需在傳送每個命令後等待回應的能力。
CHUNKING	取代 DATA 命令的 ESMTP 命令。如此 SMTP 主機就不需要持續掃描資料的結尾，因為此命令傳送的 BDAT 命令會具有內含郵件之總位元組數的引數。接收伺服器會計算郵件中的位元組數，而在郵件大小等於 BDAT 命令所傳送的值時，伺服器會假設它已收到所有的郵件資料。
DATA	由用戶端所傳送，用以初始化郵件內容的傳輸。
DSN	啟用傳遞狀態通知的 ESMTP 命令。
RSET	讓整個郵件交易無效，並重設緩衝區。
VRFY	驗證信箱是否可用來進行郵件傳遞；例如，vrfy ted 會驗證 Ted 的信箱是否位於本機伺服器上。在 Exchange 實作中預設會關閉此命令。
HELP	傳回 SMTP 服務可支援的命令清單。
QUIT	終止工作階段。

以下為SMTP協定通訊格式範例，底線文字為SMTP Server 發出的訊息:

220 mx.iim.nctu.edu.tw ESMTP Postfix

EHLO squareimshawn

250-mx.iim.nctu.edu.tw

250-PIPELINING

250-SIZE 10240000

250-VRFY

250-ETRN

250-STARTTLS

250-AUTH LOGIN PLAIN GSSAPI OTP DIGEST-MD5 CRAM-MD5

250-AUTH=LOGIN PLAIN GSSAPI OTP DIGEST-MD5 CRAM-MD5

250 8BITMIME

AUTH DIGEST-MD5

334 bm9uY2U9IkFmdUN1VnRkSk1GYWdpbS8zTkJTVnVLWmEyL2Y5WFZjT0tRY0M3WngyZlE9IixyZW
FsbT0ibXguaWltLm5jdHUuZWR1LnR3Iixxb3A9ImF1dGgiLGNoYXJzZXQ9dXRmLTgsYWxnb3JpdGhtPW1kNS1zZXNz

dXNlcm5hbWU9InNoYXduam9obmpyIixyZWFsbT0iIixub25jZT0iQWZ1Q3VWdGRKTUZhZ2ltLzNOQlNWd
UtaYTIvZjlYVmNPS1FjQzdaeDJmUT0iLGRpZ2Vzdc11cmk9InNtdHAvaWltLm5jdHUuZWR1LnR3Iixjbm9uY2U9IjA3Zj
FhNmU4ZWYwYjBlODJjZjY4NzdhOTE2ODY2YmFmIixuY
z0wMDAwMDAwMSxyZXNwb25zZT0wMGJhZTkwZm
M0YjQ4NTUxYTY4Yjg2Y2IwOTM3MGYwMSxxb3A9YX
V0aCxjaGFyc2V0PXV0Zi04

AUTH LOGIN

334 VXNlcm5hbWU6

c2hhd25qb2huanI=

334 UGFzc3dvcmQ6

RT1NKkNzaGFud2pvaG5qcio=

235 Authentication successful

MAIL FROM: <shawnjohnjr@iim.nctu.edu.tw>

250 Ok

RCPT TO: <shawnjohnjr@mail2000.com.tw>

250 Ok

RSET

250 Ok

RSET

250 Ok

MAIL FROM: <shawnjohnjr@iim.nctu.edu.tw>

250 Ok

RCPT TO: <shawnjohnjr@mail2000.com.tw>

250 Ok

DATA

From: "shawn" <shawnjohnjr@iim.nctu.edu.tw>

To: <shawnjohnjr@mail2000.com.tw>

Subject: test1234

Date: Thu, 24 May 2007 23:56:28 +0800

Message-ID:
<000001c79e1c$17459ee0$45d0dca0$@nctu.edu.tw
>
MIME-Version: 1.0
Content-Type: multipart/alternative;
Content-Type: text/plain;
.charset="us-ascii"
Content-Transfer-Encoding: 7bit

testtestesttesttest

QUIT

此範例中，DATA命令之後的區塊(斜體字) 為使用者寄送的原始信件內文，如圖26。系統透過可監聽SMTP 命令與E-mail 信件內容，如圖27。透過分析SMTP命令:DATA (信件內文開始傳輸)，以及信件內文傳輸結束 EOM (0d0a0d0a)可判斷原始信件內文，如圖28。

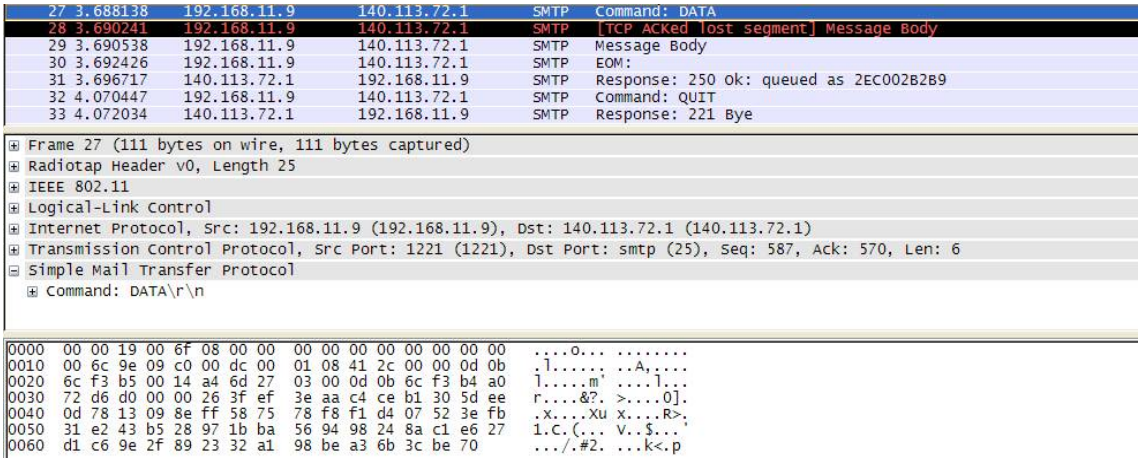


圖 26: SMTP 命令:DATA

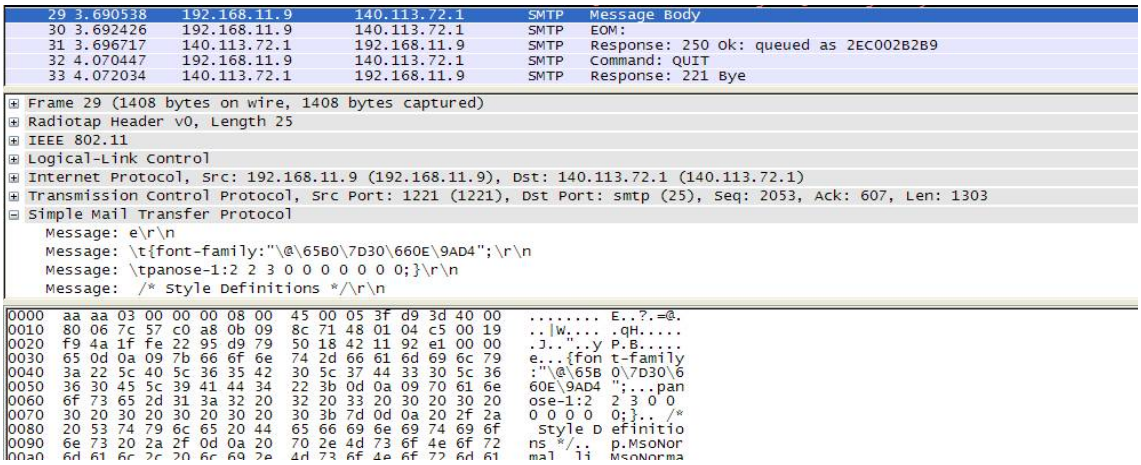


圖 27: SMTP 信件內文

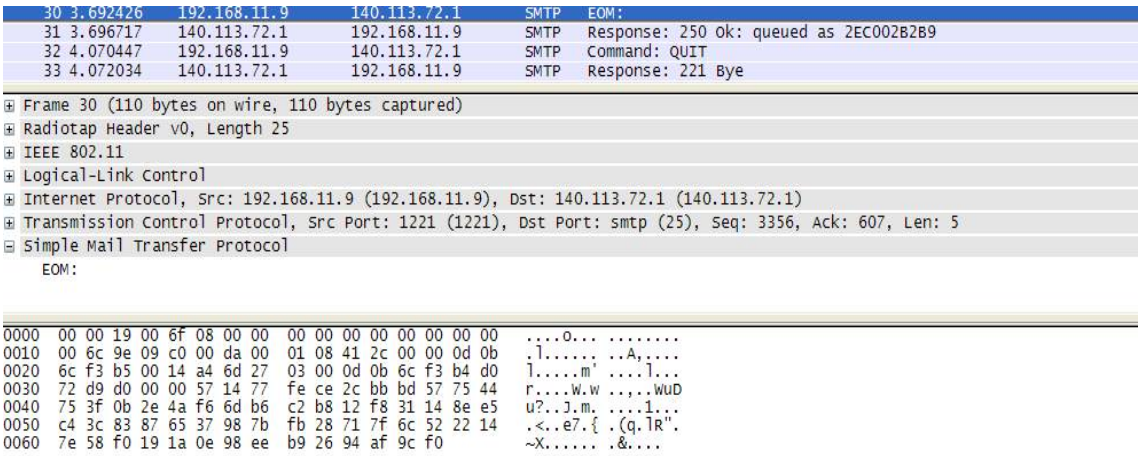


圖 28 :傳輸 SMTP 信件內文結束

4.4.5 MSN

(1) MSN 協定特徵

MSN Messenger Service Protocol 是微軟提出的通訊服務協定，1999 年微軟向 IETF 提交 1.0 版草案，此後就再也沒有公開過後續版本的細節。

1. 連線

協定建立在 TCP/IP 上，除了文件傳輸與語音聊天是 p2p 外，其它全都通過伺服器進行。

伺服器主要有 3 種:

- Dispatch Server，派遣伺服器，簡稱 DS，客戶端最初連接的伺服器，負責給客戶端分配合適的通知伺服器。有固定的域名與端口。完成派遣任務後切斷 TCP 連接。(新版現在已經沒有 DS 了)
- Notification Server，通知伺服器，簡稱 NS，客戶端需要一直保持連接的伺服器，很多任務都在這個會話內完成，但其不負責傳輸與訊息實體相關的數據。
- Switchboard Server，接線伺服器，簡稱 SB，客戶端之間聊天使用的中轉伺服器，每開一個聊天窗口，客戶端和伺服器就建立一個 TCP 會話。開始聊天前，發起方必須先申請並連接這個伺服器。

2. 命令

MSN 的命令使用 ASCII 碼，遇到非 ASCII 碼字元就使用 URL 編碼。格式基本是這樣的:

```
XXX TrID Param1 Param2 ... \r\n
```

命令以三個字元的命令 ID 開頭，例如 CAL、USR。TrID，全名為 Transaction ID，用在比對 Client 端的命令與 Server 端的回應(ACK)。 這是一個介於 0 到 4294967295 之間的整數，跟在每個命令與訊息後面，Server 端收到並做出處理後，要回覆 Client 端，並附帶這個 ID，如此 Client 端就可以識別出伺服器是對哪條命令的回應了。每次客戶端向伺服器發送一次命令或訊息後，TrID 自動加 1。

3. 承載資料命令(Payload Commands)

多數命令都是一行的，資料命令不同，它在命令後面會攜帶資料，Length 指明了後面資料的長度（不包括命令行本身）。此外資料後面不需要\r\n。基本格式如下:

```
XXX TrID Param1 Param2 ... Length\r\n
\r\n
Data
```

4. 訊息 Messages

訊息是一條以 MSG 開頭的 Payload Command，資料部分又分為 Header 和 Body。不同類型的訊息有不同的 Header，對即時訊息來說，比較重要的是 Content-Type 與 X-MMS-IM-Format，分別指定了訊息類型/編碼（通常是 UTF-8）與格式資訊。Body 與 Header 之間以一個空行分隔，內容是 UTF-8 編碼格式的訊息內容。

5. 接收即時訊息

接收的即時訊息是以如下形式由 SB 服務器發送到本機的:

```
MSG SenderEmail SendName Length\r\n
MIME-Version: 1.0\r\n
Content-Type: text/plain; charset=UTF-8\r\n
X-MMS-IM-Format: FN=...; EF=...; CO=...; CS=...; PF=...\r\n
\r\n
Message
```

關於 X-MMS-IM-Format 中的各項參數如下:

FN=Font，字體，要經過 URL 編碼。如新細明體是

%E6%96%B0%E7%B4%B0%E6%98%8E%E9%AB%94。

EF=Effects，字體特效，粗體或傾斜等，每種以一個字元標識，不區分順序。

CO=Color，顏色，16 進制 RGB 組合，如紅色是 ff0000。

CS=Character Set，字元集，預設為 UTF-8。

PF=Pitch and Family，與字元間距相關的一些格式設定。

6. 傳外訊息 (Outgoing messages)

新版 Windows Live Messenger ，已不使用，但還是相容舊版 MSN Messenger。格式為:

```
MSG TrID TypeCode Length
```

TypeCode 類型為分為 U、A、N:

- 若為 U，則發送端不會收到 ACK
- 若為 A，接收端正確收到訊息，則接收端會自動發回 ACK 給發送端
- 若為 N，接收端未正確收到訊息，則接收端會自動發回 ACK 給發送端

細部規格在此不詳細描述，可參照 MSN Messenger Service 1.0 Protocol 以及 (參考 http://www.hypothetic.org/docs/msn/index.php)。MSN messenger 通常使用 TCP port 1863，且判斷 MSN 文字訊息協定識別正規表示式如下:
(參考 http://l7-filter.sourceforge.net/layer7-protocols/protocols/msnmessenger.pat)。

```
ver [0-9]+ msnp[1-9][0-9]? [\x09-\x0d -~]*cvr0\x0d\x0a$|usr 1 [!-~]+
[0-9. ]+\x0d\x0a$|ans 1 [!-~]+ [0-9. ]+\x0d\x0a$
```

而 MSN 傳送檔案識別正規表示式如下:

(參考:http://www.hypothetic.org/docs/msn/client/file_transfer.php)。

```
msn-filetransfer
^(ver [ -~]*msnftp\x0d\x0aver msnftp\x0d\x0ausr|method msnmsgr:)
```

其中 msnftp 為舊版 MSN 傳送檔案的協定規格表示方式，表示式的第二部份可辨別更新的 MSNSLP 規格，表 25 僅列出本範例使用之命令:

(參考 http://msnpiki.msnfanatic.com/index.php/MSNC:MSNSLP)。

表 25: MSN 命令

Command	From	To	Description
ANS	Client	Switchboard	Accepts a request for a switchboard server session.
IRO	Switchboard	Client	Provides the initial roster information for new users joining the session.
MSG	Client	Switchboard	Sends a message to the members of the current session.
MSG	Notification, Switchboard	Client	Delivers a message from Switchboard another client or from a server-side component.

(2) MSN 範例

以 User: shawnjohnjr@hotmail.com 與 archranger@hotmail.com 作為範例。

其中 shawnjohnjr@hotmail.com 使用者使用 Windows Live Messenger 而 archranger@hotmail.com 使用 Gaim 作為 MSN 用戶端。圖 29 為使用者進行 MSN 連線。表 26 則為此 MSN 連線範例之通訊訊息。

圖 29: MSN 連線畫面

表 26: MSN 通訊訊息

MSG shawnjohnjr@hotmail.com
*helpStay%20hungry,%20stay%20foolish.%20::.....
%20Giovanni.Ferria 96

MIME-Version: 1.0

Content-Type: text/x-msmsgscontrol

TypingUser: shawnjohnjr@hotmail.com

MSG shawnjohnjr@hotmail.com
*helpStay%20hungry,%20stay%20foolish.%20::.....
%20Giovanni.Ferria 155

MIME-Version: 1.0

Content-Type: text/plain; charset=UTF-8

X-MMS-IM-Format: FN=%E6%96%B0%E7%B4%B0%E6%98%8E%E9%AB%94; EF=; CO=80; CS=88; PF=12

hahahaha!

MSG shawnjohnjr@hotmail.com
*helpStay%20hungry,%20stay%20foolish.%20::.....
%20Giovanni.Ferria 96

MIME-Version: 1.0

Content-Type: text/x-msmsgscontrol

TypingUser: shawnjohnjr@hotmail.com

等同於 MSN 視窗介面顯示，用戶正在輸入文字之通知事件 (MSN Notification)。通知目前某使用者正在輸入訊息之樣式為:

MSG + MSN 帳號 + MSN 暱稱

MIME-Version: MIME 版本號

Content-Type: text/x-msmsgscontrol (MSN 控制訊息)

TypingUser: 目前正在輸入聊天文字的使用者帳號

下面協定區塊描述使用者送出的聊天訊息:

MSG shawnjohnjr@hotmail.com

*helpStay%20hungry,%20stay%20foolish.%20::.....%20Giovanni.Ferria 155

MIME-Version: 1.0

Content-Type: text/plain; charset=UTF-8

X-MMS-IM-Format: FN=%E6%96%B0%E7%B4%B0%E6%98%8E%E9%AB%94; EF=; CO=80; CS=88; PF=12

hahahaha!

其格式為:

MSG + MSN 帳號 + MSN 暱稱

MIME-Version: MIME 版本號

Content-Type: text/plain; charset=UTF-8 內容型態 與編碼型態

X-MMS-IM-Format: FN=%E6%96%B0%E7%B4%B0%E6%98%8E%E9%AB%94; EF=; CO=80; CS=88;

PF=12

5. 無線區網監聽計畫後置

5. 無線區網監聽雛型系統

5.1 雛型系統開發環境

甲、　軟體

	平台	開發語言	執行檔
監聽主控台	.Net framework 2.0	C#	
監聽命令伺服器	Ubuntu Server 7.04 feisty	C/Perl	decrypt.pl
擷取、解碼元件 (修改 Aircrack-ng 原始碼)	Ubuntu Server 7.04 feisty	C	擷取封包:airodump 破解 WEP/WPA 金鑰:aircrack-ng WEP/WPA 封包解密:airdecap-ng
監聽分析器	Ubuntu Server 7.04 feisty	C++	library: libnids、ACE、Boost、libvmime、libmysqlclient, uuid InterceptDecoder
通聯記錄檢視器	Ubuntu Server 7.04 feisty Tomcat Web Server Appfuse framework	Java/JSP	

乙、　硬體

無線網路卡	Dlink DWL-G122 H/W Ver:C.1 F/W Ver:3.00　(兩組) Dlink 802.1g/24.GHZ Wireless H/W Ver:C3 F/W Ver:4.31
無線網卡驅動程式	(RalinkRT73 (http://rt2x00.serialmonkey.com/rt73-cvs-daily.tar.gz) / Madwifi)

5.2 雛型系統監聽流程

本雛型系統可提供單點與多點 AP 模式的監聽。

(1)　多點 WIAP 監聽

若進行多點監聽，首先需設定監聽節點與種控台之連線，建立佈署環境檔。圖 30 為建立 3 台 AP 監聽目標與主控台連線。點選佈署檔設定，可填入連線細部設定資料，如圖 31 所示。

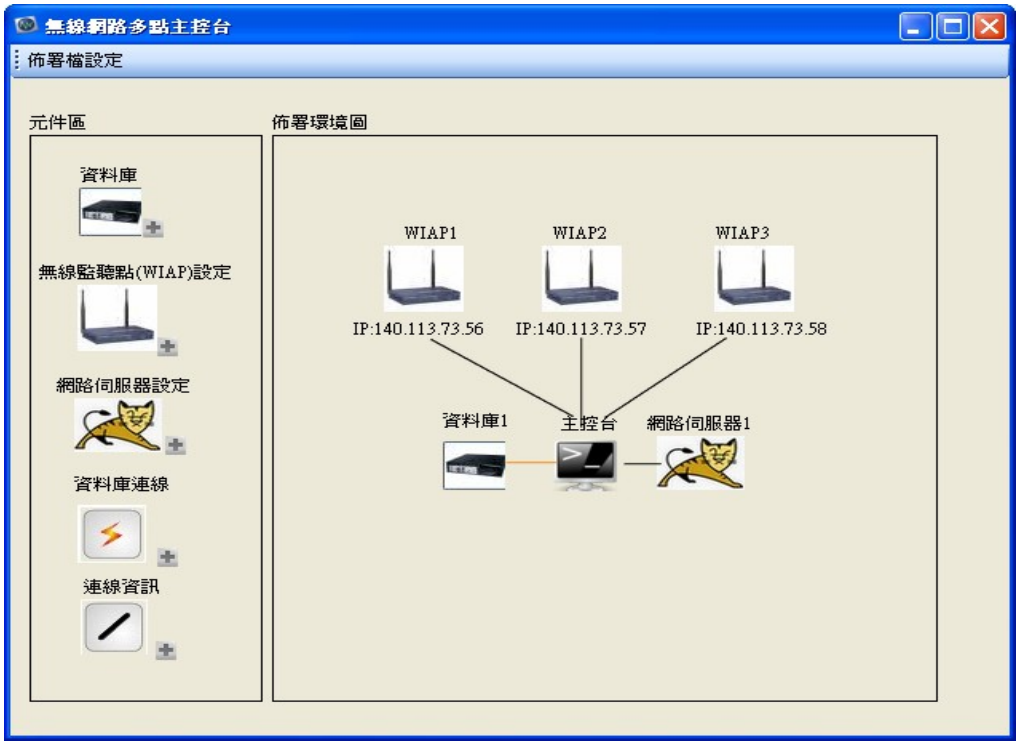


圖 30:多點監聽佈署環境

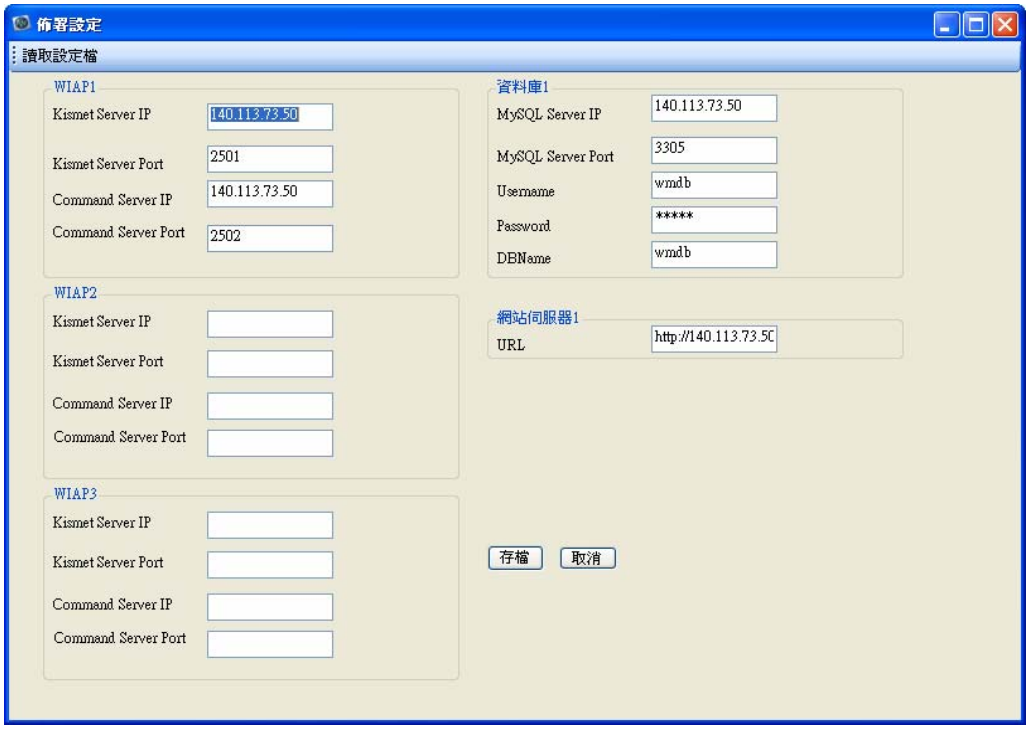


圖 31:多點監聽佈署設定

若點選單一 WIAP 圖示，則可啟動單一主控台操控選定的 WIAP，此時轉換為單點模式。

(2) 單點 WIAP 監聽

假設一開始使用者已經知道監聽目標之資訊。使用者需要將無線監聽主控台啟動，如圖 32，並連結監聽收集伺服器。通常無線監聽主控台佈署於運算能力較強的主機，負責主控移動式無線網路封包收集裝置，與執行還原封包與破解 WEP/WPA 金鑰。

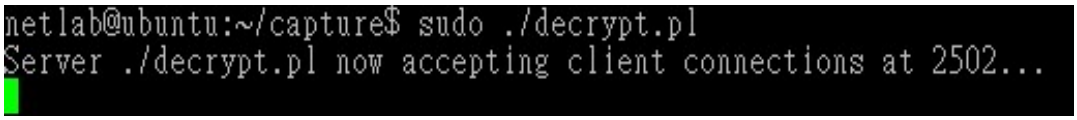


圖 32: 啟動監聽命令伺服器

與伺服器連線後，使用者可在 AP 模式獲知偵測到的無線存取點，並可選擇各 AP 查看其詳細資訊與存取該 AP 的 client。如下圖 33 為主控台 AP 模式畫面。

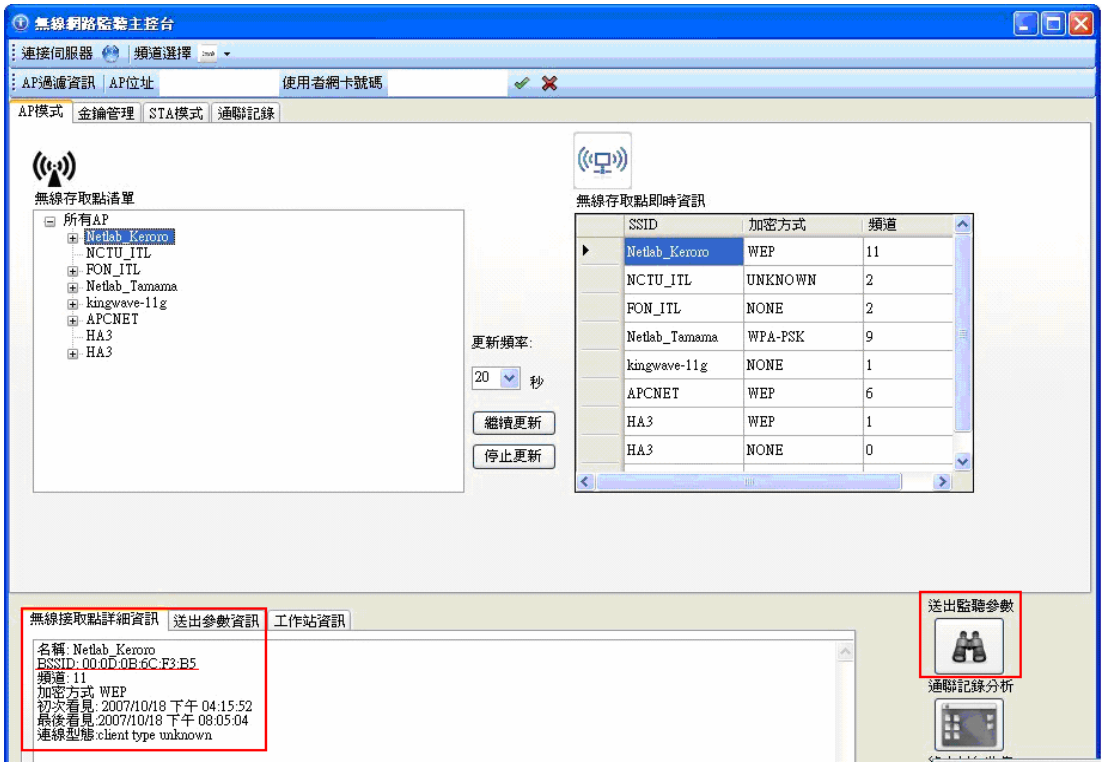
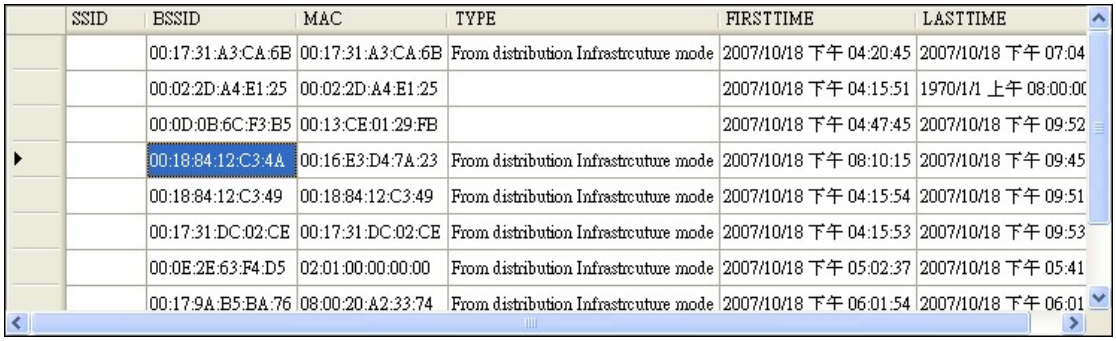


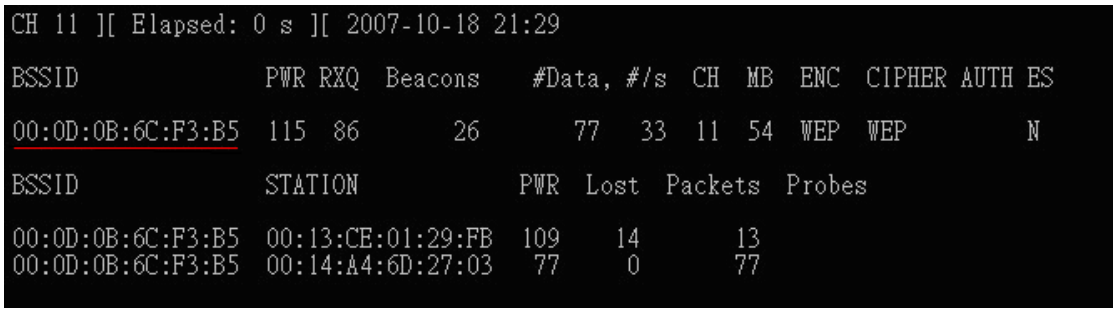
圖 33:主控台 AP 模式

使用者選擇 Netlab_Keroro 存取點後，按下送出監聽參數按鈕；或由 STA 檢視模式，在 STA 列表選擇監聽對象，如圖 34，並按下送出監聽參數，待監聽命令伺服器開始擷取無線網路封包，圖 35 顯示監聽命令伺服器開始擷取 AP 名稱: Netlab_Keroro，BSSID:00:0D:0B:6C:F3:B5 的無線封包。



	SSID	BSSID	MAC	TYPE	FIRSTTIME	LASTTIME
		00:17:31:A3:CA:6B	00:17:31:A3:CA:6B	From distribution Infrastrcuture mode	2007/10/18 下午 04:20:45	2007/10/18 下午 07:04
		00:02:2D:A4:E1:25	00:02:2D:A4:E1:25		2007/10/18 下午 04:15:51	1970/1/1 上午 08:00:00
		00:0D:0B:6C:F3:B5	00:13:CE:01:29:FB		2007/10/18 下午 04:47:45	2007/10/18 下午 09:52
▶		00:18:84:12:C3:4A	00:16:E3:D4:7A:23	From distribution Infrastrcuture mode	2007/10/18 下午 08:10:15	2007/10/18 下午 09:45
		00:18:84:12:C3:49	00:18:84:12:C3:49	From distribution Infrastrcuture mode	2007/10/18 下午 04:15:54	2007/10/18 下午 09:51
		00:17:31:DC:02:CE	00:17:31:DC:02:CE	From distribution Infrastrcuture mode	2007/10/18 下午 04:15:53	2007/10/18 下午 09:53
		00:0E:2E:63:F4:D5	02:01:00:00:00:00	From distribution Infrastrcuture mode	2007/10/18 下午 05:02:37	2007/10/18 下午 05:41
		00:17:9A:B5:BA:76	08:00:20:A2:33:74	From distribution Infrastrcuture mode	2007/10/18 下午 06:01:54	2007/10/18 下午 06:01

圖 34:主控台 STA 模式



```
CH 11 ][ Elapsed: 0 s ][ 2007-10-18 21:29

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ES

00:0D:0B:6C:F3:B5  115  86       26       77   33  11  54  WEP  WEP         N

BSSID              STATION            PWR  Lost  Packets  Probes

00:0D:0B:6C:F3:B5  00:13:CE:01:29:FB  109    14       13
00:0D:0B:6C:F3:B5  00:14:A4:6D:27:03   77     0       77
```

圖 35:監聽命令伺服器擷取封包

按下停止按鈕之後，結束擷取封包動作，並將擷取 BSSID:00:0D:0B:6C:F3:B5 的無線封包儲存為.cap 檔，檔名格式自動設定為時間_BSSID，如圖 36。

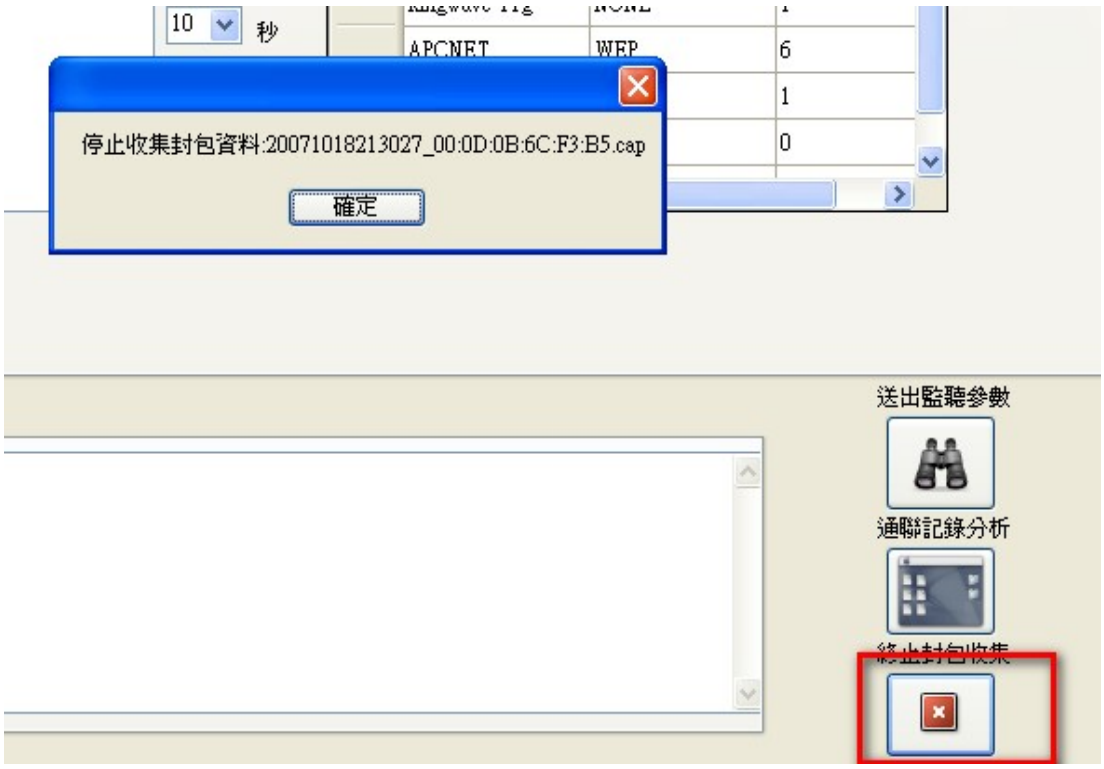


圖 36:終止封包收集

新擷取的網路封包存成.cap 檔後會加入”選擇來源分析檔”列表中，如下圖37，使用者選擇解密等級 64bit 預設為等級 2，加密的位元可 64/128/256 bits 擇一，其中選擇來源分析檔列表中型態 0 為 open system、WEP 為 1、WPA-PSK 為 2。選定需要進行金鑰破解的來源檔案，呼叫監聽命令伺服器開始破解金鑰，如下圖38 所示，監聽命令伺服器執行 aircrack-ng 進行 64bits，檔名為 20071018213027_00:0D:0B;6C:F3:B5.cap 之 WEP 金鑰破解。

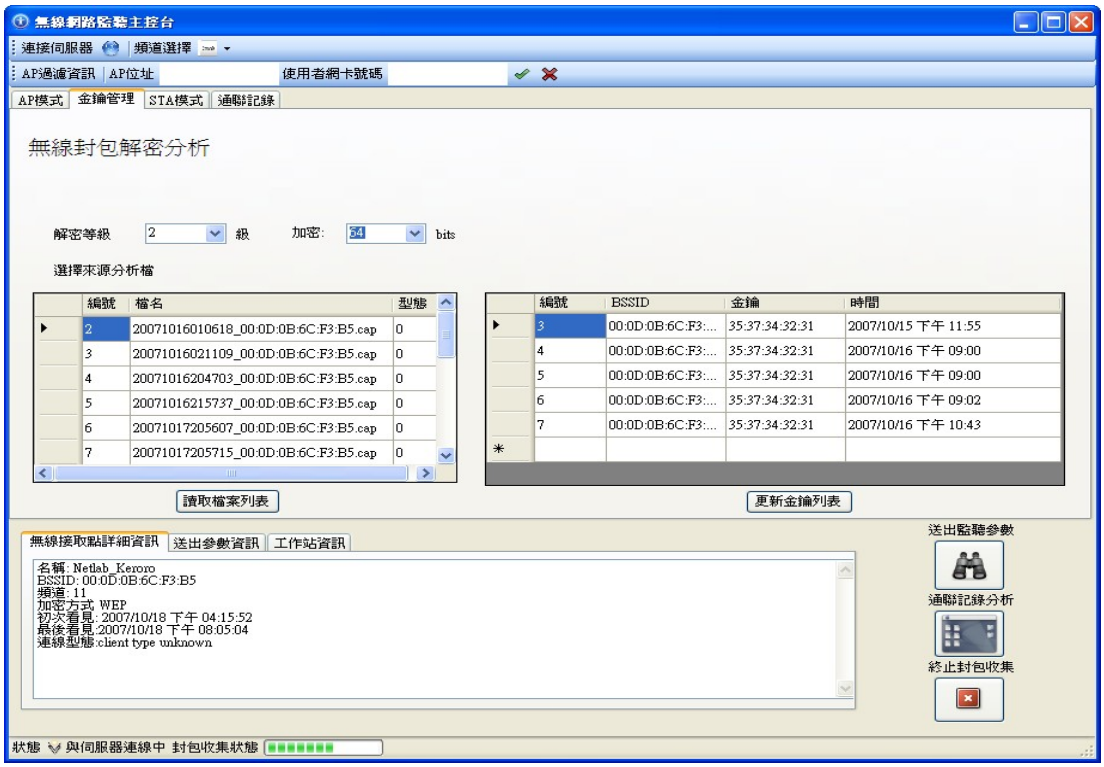


圖 37:選取破解金鑰檔案

```
The file name would be: 20071018214354_00:0D:0B:6C:F3:B5.cap
Connection from [net-ap.iim.nctu.edu.tw,6889] established.
Connection from [net-ap.iim.nctu.edu.tw,6891] established.
Connection from [net-ap.iim.nctu.edu.tw,6898] established.
Got DECRYPT with DECRYPT,00:0D:0B:6C:F3:B5,1,64,2,20071018214354 00:0D:0B:6C:F3:B5.cap
aircrack-ng starting...
```

圖 38:監聽命令伺服器破解金鑰

當金鑰破解完成後，金鑰會自動加入金鑰列表，如圖 39。

編號	BSSID	金鑰	時間
3	00:0D:0B:6C:F3:...	35:37:34:32:31	2007/10/15 下午 11:55
4	00:0D:0B:6C:F3:...	35:37:34:32:31	2007/10/16 下午 09:00
5	00:0D:0B:6C:F3:...	35:37:34:32:31	2007/10/16 下午 09:00
6	00:0D:0B:6C:F3:...	35:37:34:32:31	2007/10/16 下午 09:02
7	00:0D:0B:6C:F3:...	35:37:34:32:31	2007/10/16 下午 10:43

圖 39:破解後金鑰列表

使用者按下通聯記錄分析按鈕後，選擇指定分析檔案，系統會自動判斷該檔案是否已經存有金鑰，填入/更新金鑰欄位，使用者點選開始分析，系統將自動分析.cap 檔案，如圖 40 所示。

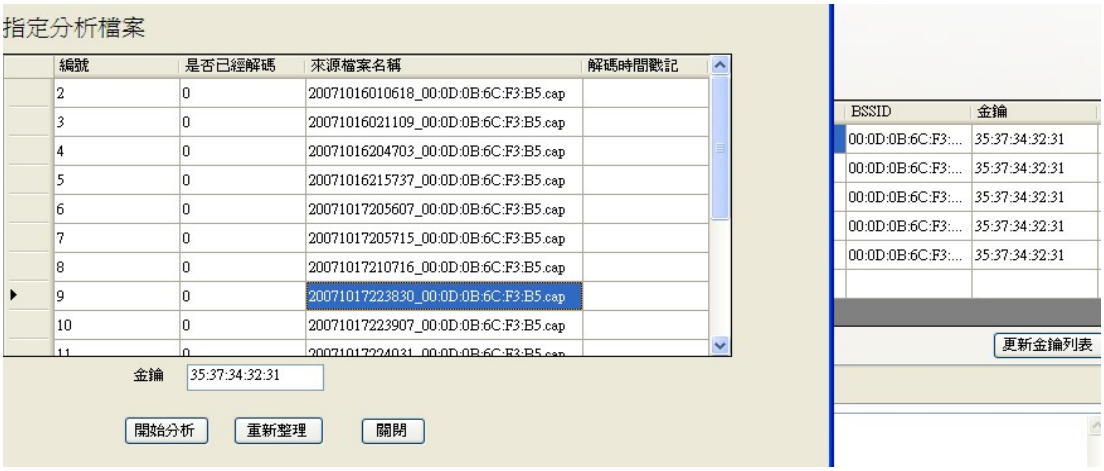


圖 40: 指定分析檔案

監聽命令伺服器接到分析命令，將會執行 decap(解密封包)，隨後執行 decode(分析封包)，如圖 41。待伺服器執行封包解密分析完畢，會將封包紀錄檔解析協定內容，並存入資料庫中，如圖 42，使用者可至通聯記錄表查詢內容。

```
Connection from [net-ap.iim.nctu.edu.tw,6909] established.
Got DECODE with DECODE,20071018214354_00:0D:0B:6C:F3:B5.cap,35:37:34:32:31
Decaping 20071018214354_00:0D:0B:6C:F3:B5.cap...
Total number of packets read         32746
Total number of WEP data packets     32474
Total number of WPA data packets         0
Number of plaintext data packets         0
Number of decrypted WEP  packets     32474
Number of decrypted WPA  packets         0
20071018214354_00:0D:0B:6C:F3:B5 cap
Processing 20071018214354_00:0D:0B:6C:F3:B5-dec.cap...
```

圖 41: 監聽命令伺服器解密/分析封包

圖 42: 指定檔分析完成

(3) Application View 通聯記錄檢視 web

使用者申請帳號登入通聯記錄檢視 web，登入畫面如圖 43。

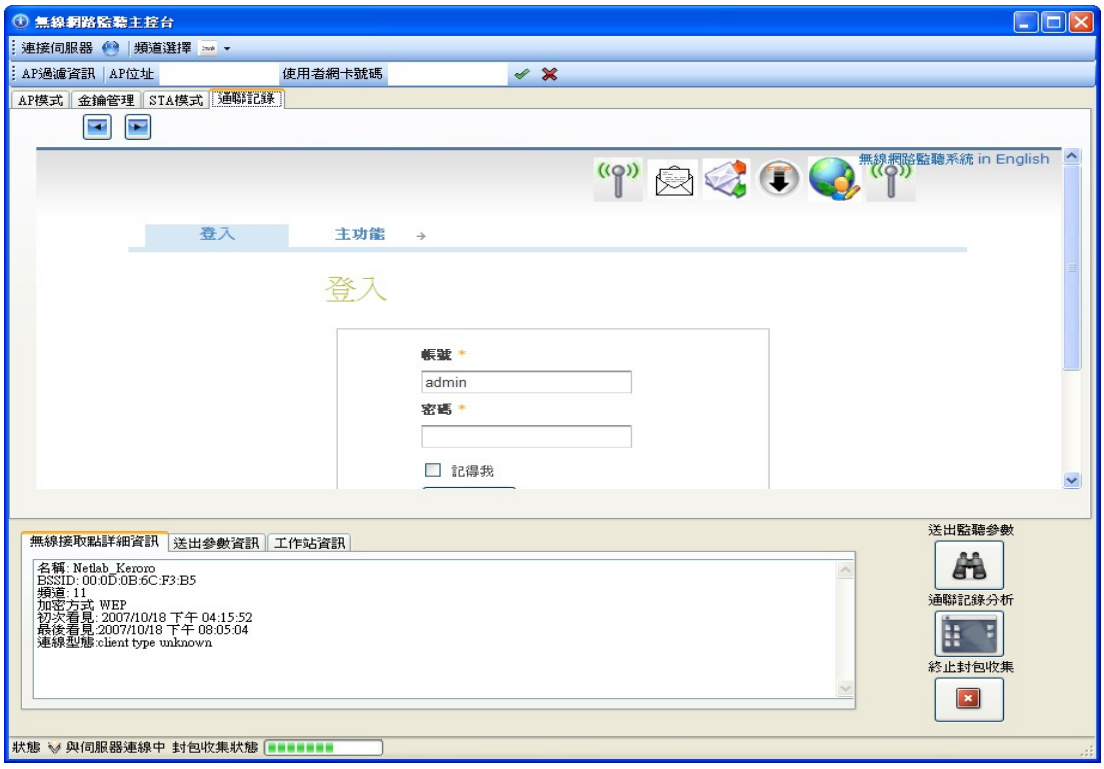


圖 43: 通聯記錄登入畫面

下拉主功能列表可以查詢不同通訊協定之監聽資料，如圖 44 所示。

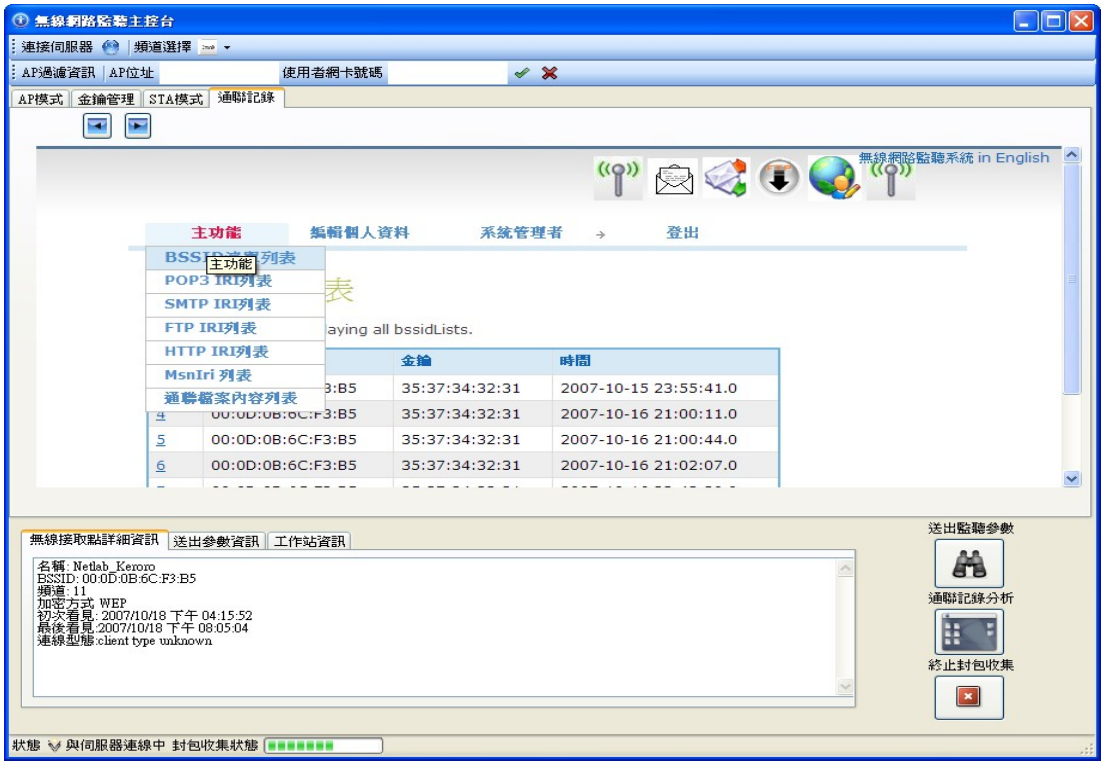


圖 44: 通聯記錄主功能列表

以下圖示為各通訊協定之通訊相關資訊(IRI)的列表與詳細資料。圖 45 為 FTPIRI 列表，清楚顯示使用者使用 FTP 之來源端 IP、目的端 IP、帳號、密碼與時間等通訊相關資訊。圖 46 顯示為單筆紀錄展開之詳細通訊資訊。

FTP IRI列表

6 ftpIris found, displaying all ftpIris.

編號	來源端IP	目的端IP	使用者名稱	使用者密碼	時間
23	192.168.11.10	140.113.73.40	momo	61x336	2007-10-12 Time:07:12:19
24	192.168.11.10	140.113.73.40	momo	61x336	2007-10-12 Time:07:12:42
25	192.168.11.10	140.113.73.40	momo	61x336	2007-10-12 Time:07:12:49
26	192.168.11.10	140.113.73.40	momo	61x336	2007-10-12 Time:07:12:19
27	192.168.11.10	140.113.73.40	momo	61x336	2007-10-12 Time:07:12:42

圖 45: FTPIRI 列表

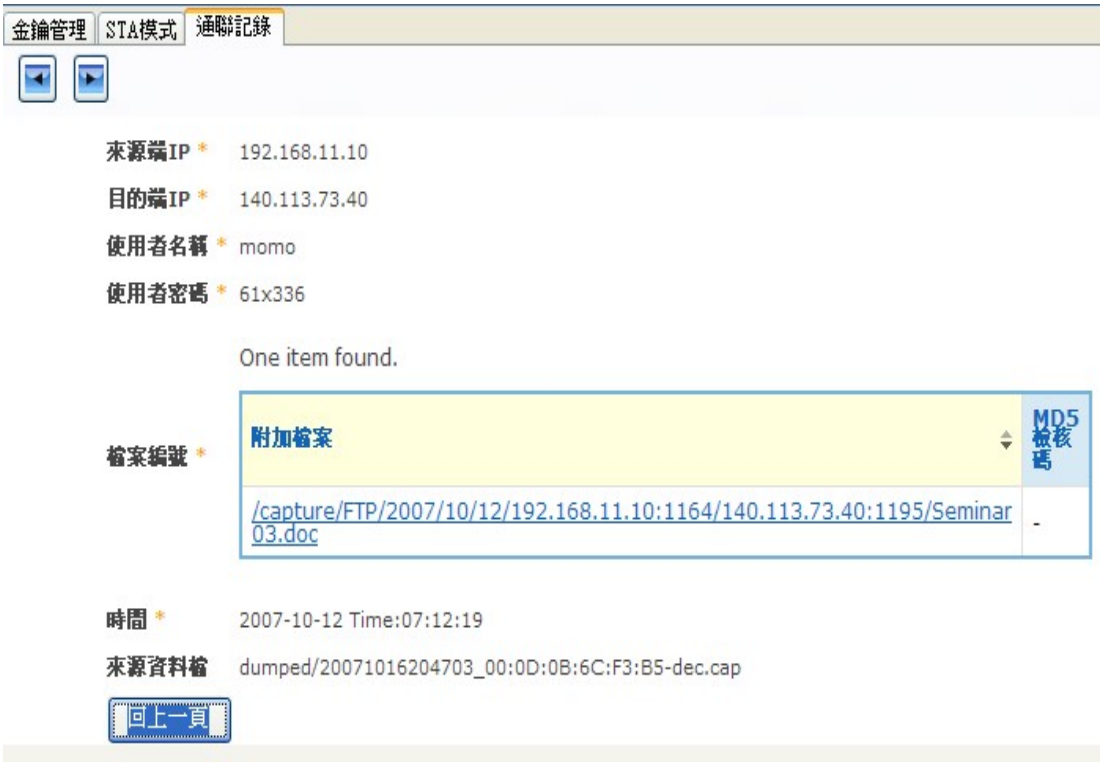


圖 46: FTPIRI 詳細資料

此 FTP 通聯記錄之附加檔案檔名為 Seminar03.doc，若要查詢附加檔案內容，可點選附加檔案之連結，並下載檢視。如下圖 47，進行 FTP 附加檔案下載。

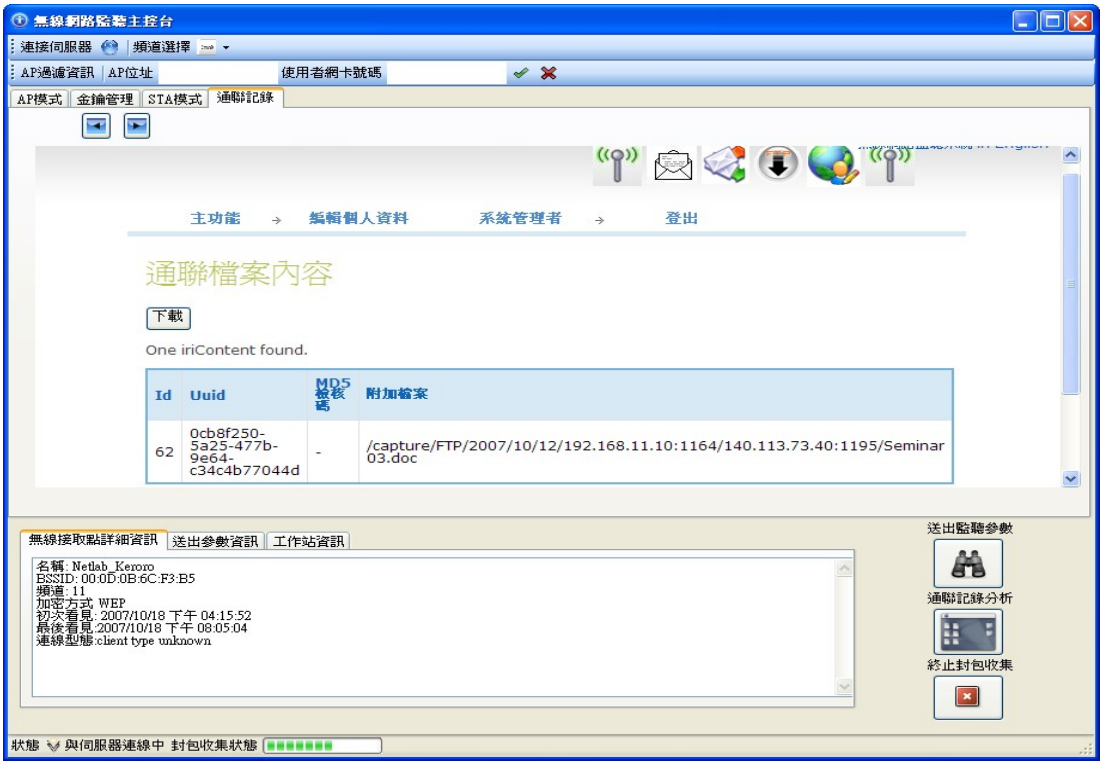


圖 47: FTP 附加檔案下載

圖 48 為 HTTPIRI 之列表。顯示使用者使用 HTTP 之來源端 IP、目的端 IP、URL、GET/POST 與時間等通訊相關資訊。

HTTP IRI列表

60 httpIris found, displaying 1 to 25. [First/Prev] **1**, 2, 3 [Next/Last]

編號	來源端IP	目的端IP	URL	Get	Post	時間
38	192.168.11.2	208.100.1.161	0	GET		2007-10-16 Time:12:37:26 GMT+08
39	192.168.11.2	208.100.1.161	0	GET		2007-10-16 Time:12:37:46 GMT+08
40	192.168.11.2	208.100.1.161	0	GET		2007-10-16 Time:12:37:56 GMT+08
41	192.168.11.2	208.100.1.161	0	GET		2007-10-16 Time:12:38:06 GMT+08
42	192.168.11.2	208.100.1.161	0	GET		2007-10-16 Time:12:38:16 GMT+08

圖 48: HTTP IRI 列表

圖 49 為 MSN IRI 之列表。顯示使用者使用 MSN 之來源端 IP、來源端埠號、目的端 IP、目的端埠號、使用者帳號、通話人數、對談者帳號等通訊相關資訊，並將此筆交談記錄儲存。圖 50 為單筆通話記錄的展開，其詳細資訊可獲知 MSN 通話時間與交談內容。

MsnIris

5 msnIris found, displaying all msnIris.

編號	來源端IP	來源端埠號	目的端IP	目的端埠號	對話Session擁有者ID	對話者人數	對談者ID	存檔路徑
30	192.168.11.5	35260	192.168.11.5	1863	shawnjohnjr@hotmail.com	1	archranger@hotmail.com	capture/imsniff/shawnj
31	64.4.36.41	1863	64.4.36.41	35266	shawnjohnjr@hotmail.com	1	hugo3318@hotmail.com	capture/imsniff/shawnj
32	192.168.11.2	1774	192.168.11.2	1863	fone@alumni.ccu.edu.tw	1	chiawei113@hotmail.com	capture/imsniff/fone@
33	207.46.27.55	1863	207.46.27.55	1784	fone@alumni.ccu.edu.tw	1	chiawei113@hotmail.com	capture/imsniff/fone@
34	192.168.11.5	4088	192.168.11.5	1863	shawnjohnjr@hotmail.com	1	lileo73@hotmail.com	capture/imsniff/shawnj

Export options: CSV | Excel | XML | PDF

圖 49: MSN IRI 列表

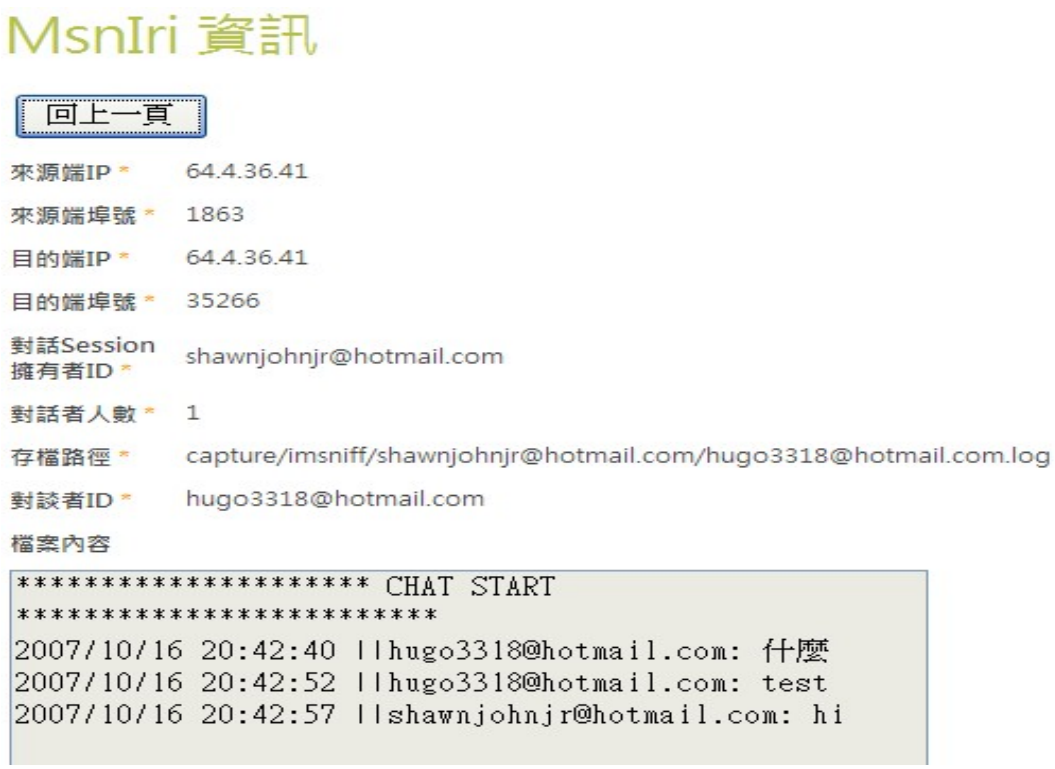


圖 50: MSN IRI 詳細資料

圖 51 為 POP3 IRI 之列表。顯示使用者使用 POP3 之來源端 IP、來源端埠號、目的端 IP、目的端埠號、寄件者、收件者、標題、信件大小與時間。圖 52 為此筆 POP3 紀錄的詳細資料。SMTP 通聯記錄與 POP3 相似，故略之。

圖 51: P0P3 IRI 列表

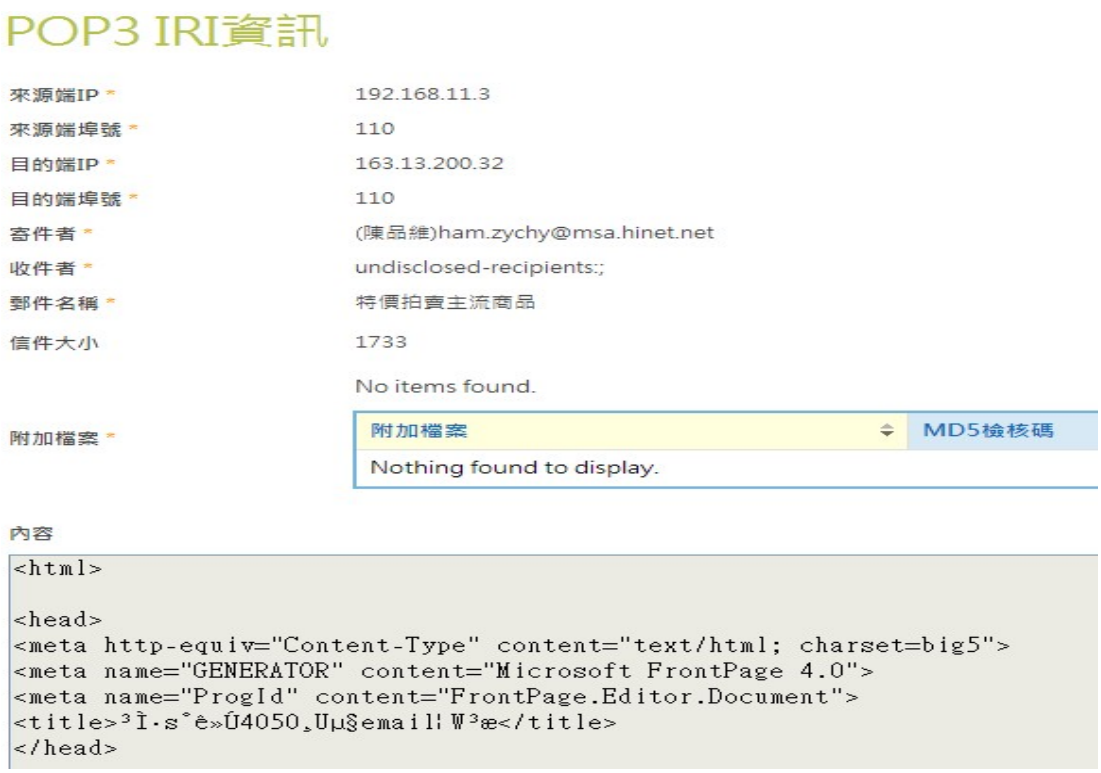


圖 52: P0P3 IRI 詳細資料

5.3 雛型系統評估

無線區網監聽雛型系統預計能達成的目標，主要著重於支援機動戰術性的移動監察活動。藉由本系統和筆記型電腦組合而成的移動平台，使用者可以輕易的在室內或室外進行無線網路的監察行動。

本雛型系統預期可完成處理以下監聽技術:

1. 了解目前空間有哪些 Wireless Network 正在運作。
2. 了解目前空間中所有 Wireless Networks 的加密狀況。
3. 指定某 Wireless Network (Access Point)為目標進行封包攔截。
4. 破解加密過後的 802.11 資料封包(包含 WEP、WPA 與 WPA2 加密*)。
5. 對資料封包進行分類重組、辨別類型。
6. 對特定類型資料封包進行內容分析。
7. 將封包重組後形成的原資料進行儲存供日後瀏覽。

以上目標實為本雛型系統監聽技術研究之重點，於監聽活動進行時依序進行。國軍預於資訊情報傳輸一新地點進行無線區網監聽，而不了解當地無線網路佈建狀況時，本雛型系統能夠提供搜尋無線網路的功能。有別於傳統無線網路連線狀況，本系統利用攔截 probe 資料的方式來確認空間中有哪些運行中的 AP 其 ESSID 與 BSSID，可以防止刻意關閉 Beacon 發送以隱藏 ESSID 的 AP。

為了能使攔截到的封包能順利被分析，本系統也提供破解無線網路加密系統的功能。目前預期能夠有效破解 WEP 加密以及對 WPA 與 WPA2 系列加密做嘗試破解的動作，前者只要利用蒐集封包中的 IV 值就能利用統計演算法進行比對運算，而 WPA 系列加密則需要耗時的暴力演算法進行破解。

資料封包經破解後可窺看其內容，而後本系統得以依照封包的來源與目的進行歸類，再以封包夾帶的資料類型進行重組的動作。預期可辨認出各個常用通訊協定(如 Telnet、FTP、HTTP、SMTP、MSN Messenger 等等)，再依照通訊協定的交談特性進行重組，成為使用者可輕易辨識的連續通聯資料。

參考資料

- Wireshark http://wireshark.cs.pu.edu.tw/
- Kismet http://www.kismetwireless.net/
- AirCrack-NG Suite http://www.aircrack-ng.org/
- Winpcap http://www.winpcap.org/
- Libpcap http://www.tcpdump.org
- IEEE 802.1X http://standards.ieee.org/getieee802/download/802.1X-2001.pdf
- ETSI TR 102 519 V1.1.1,"Lawful Interception (LI); Lawful Interception of public Wireless LAN Internet Access", 2006
- Wireless Security Blackpaper: http://www.arstechnica.com/paedia/w/wireless/security-1.html
- WiFi Hacking 無線網路駭客現形攻防戰，莊添發 著，旗標，2006
- 802.11 完全剖析無線網路技術，鄭同伯 著，博碩，2004
- 802.11 無線網路技術通論 第二版，黃裕彰 譯 ， O'REILLY, 2005
- 工研院電通所，無線區域網路認證技術及應用研究報告，CCL-9201-P104-063，2003