

目錄

前言.....	1
DAY 1-1 軟體安裝.....	3
關於 Wireshark.....	5
下載 Wireshark (ver2.0.x).....	6
安裝 Wireshark.....	7
Wireshark 安裝位置確認.....	19
Wireshark 的啟動方式.....	20
Wireshark 歡迎畫面.....	21
DAY 1-1 軟體操作.....	23
講義環境設定.....	24
封包擷取的準備動作.....	25
有線網路的封包擷取與停止.....	26
擷取方式一.....	26
擷取方式二.....	27
擷取方式三.....	28
停止方式一.....	29
停止方式二.....	29
無線網路的封包擷取與停止.....	30
擷取方式一.....	30
擷取方式二.....	31
擷取方式三.....	32
停止方式一.....	33
停止方式二.....	33
主畫面介紹.....	34
如何檢視封包資訊.....	35
封包列表 (Packet List).....	36
封包細節 (Packet Details).....	37
封包位元組 (Packet Bytes).....	40
DAY 1-1 封包過濾.....	41
講義環境設定.....	42
關於封包過濾 (Filter).....	43
擷取過濾 (Capture filter) 與顯示過濾 (Display filter).....	43
在何處過濾封包 (顯示過濾).....	44
如何取消或清除已存在的過濾條件.....	45
範例一：過濾出 arp 廣播封包.....	46
範例二：排除 arp 廣播封包.....	46

範例三：排除 arp 與 nbns 封包	47
範例四：僅列出 tcp 封包	48
範例五：列出 tcp 與 udp 封包	48
範例六：找出 HTTP 的封包	49
範例七：找出 DNS 的封包.....	50
範例八：過濾出 Gateway IP (192.168.2.1) 的封包.....	51
範例九：找出本區網段 (IP) 的廣播封包	51
範例十：找出與自己 IP 有關的但不是 HTTP 的封包	52
範例十一：過濾出加密封包和一般網頁封包.....	52
範例十二：過濾出是否有人以網頁 (網站) 方式上傳大量資料，假設超出 554bytes 就算大量 (主觀認定)。	53
範例十三：過濾出與自己 Mac Address 有關的封包.....	54
範例十四：排除跟自己 Mac Address 有關的封包.....	55
範例十五：找出區網內所有廣播封包.....	56
範例十六：排除區網內所有廣播封包.....	56
範例十七：找出區網內 hTc 品牌設備有關的封包	57
課後練習：	59
DAY 1-2 PART1 : PING	63
講義環境設定.....	64
Ping 到網路世界.....	65
Ping to Gateway	65
Frame header	69
Internetworking Protocol header	69
Internet Control Message Protocol header	69
Ping to Other	70
ARP header.....	74
課後練習：	75
01. Ping to Nobody.....	75
02. Ping to Wrong.....	76
03. Ping to Me	77
04. Ping to Me	78
DAY 1-2 PART2 : DNS	79
講義環境設定.....	80
DNS 與網路世界.....	81
了解目前網路組態設定.....	82
開始擷取 DNS 封包 (使用 Ping)	84
DNS header	87
DNS: Question	87

DNS: Answer, Authority, Additional	87
課後練習：	88
01.再度要求「Wireshark 網站」回應 (已經 PING 過)	88
02.要求「Wireshark 台灣網站」回應 (Domain 不存在).....	89
03.要求「sharkshark 網站」回應 (Domain 不存在).....	90
04.以不同 DNS 要求「Wireshark 網站」回應	91
DAY 2-1 PART1 : FTP	93
講義環境設定.....	94
網路中傳遞檔案的方式：FTP.....	95
開始擷取 FTP 封包 (ftp).....	95
TCP header	101
FTP header	101
課後練習：	102
01. FTP 的安全機制.....	102
DAY 2-1 PART2 : POP3	103
講義環境設定.....	104
資訊傳的傳遞與 Mail	105
開始擷取 POP3 封包 (telnet).....	105
POP3 header	109
課後練習：	110
01.POP3 的安全機制.....	110
02.中文信件	111
03.郵件收發軟體	112
04.網頁郵件	113
DAY 2-2 封包實作與發送	115
關於駭客.....	117
駭客 (Hacker) 與怪客 (Cracker)	117
合法、違法，一線之間.....	117
關於 Packet Builder	118
下載 Colasoft Packet Builder (ver1.0 Build 177).....	119
安裝 Colasoft Packet Builder	121
Colasoft Packet Builder 安裝位置確認	127
Colasoft Packet Builder 的啟動方式	128
啟動方式一.....	128
啟動方式二.....	128
Colasoft Packet Builder 主畫面	129
Colasoft Packet Builder 主畫面調整	130
封包設計與發送.....	132

Mission1	133
Mission2	134
Mission3	135
Mission4	136
Mission5	137
Mission6	138
附錄.....	139
Wireshark 各版 經典畫面	141
主畫面與功能屬性設定.....	145
Preferenes : Appearance (外觀)	147
Preferenes : Appearance / Layout (版面)	148
Preferenes : Appearance / Columns (欄位).....	149
Preferenes : Appearance / Font and Colors (字型與顏色).....	150
Preferenes : Capture (擷取).....	151
Preferenes : Name Resolution (名稱解析).....	152
過濾課後練習 參考答案.....	153
Protocol, Port, header field code	157
Protocol Numbers List (Last Updated 2016-03-07).....	158
Port Numbers List (Last Updated 2016-03-23)	161
ASCII Code	175
CODE: frame-type	176
CODE: icmp-type, code	177
CODE: ARP-Hardware Type	178
CODE: ARP-Operation Code	179
CODE: DNS-QR	180
CODE: DNS-Opcode.....	180
CODE: DNS-Type.....	181
CODE: DNS-Class	182
CODE: FTP Status and Error Codes (Return Code)	183
PowerPoint.....	185

前言

各位同學好，首先恭喜各位選擇這門擁有高度知識與應用的課程，因為您將可以從中學習到現行網路上的各種應用的實現。

您在使用網路上，有遇過什麼問題嗎？像是：「網路線有接，怎麼不能連線？」、「設備錯誤燈也沒亮，怎麼不會通？」、「網路卡設定也都正確，為什麼一直說有衝突？」、「大家都可以上網，怎麼只有我不能？」、「為什麼網路芳鄰裡面沒人？」、「檔案伺服器可登入，但是卻無法上傳或下載。」怎麼辦？這些好像常常在發生，但是真正的問題是什麼？

是啊！在網路的世界裡只是一連串 0 與 1 的電子訊號，網路不通或是無法連線，絕對是這個網路時代裡最嚴重的問題，就算您是個職場老手，在遇到問題時，一樣會常常摸不著頭緒，因為我們無法直視或觸摸那些電子訊號，頂多用經驗來猜測問題點，因為表面上看似相同的問題，卻「可能」不會是同一個解決方式，至於這個「可能」，現在的您都可以隨意的列出 100 種出來！但如果要用猜測方式來嘗試解決，會是十分費工耗時的。

所以本課程內容就是要讓各位利用 Wireshark 來「分析」並「觀察」網路狀態，進而解決網路問題，甚至能做到監視網路的作用，因為網路這個世界並沒有您想像中的簡單；本課程將以最清楚簡單的方式，帶領各位進入這個浩瀚的網路世界；相信我！這門課絕對是您未來的工作上一把無法丟棄的利器。

IT 的世界之大，無法獨身一人自修所有知識，所以希望藉由本課程來減少各位同學的學習時間，並期望各位能更了解網路架構與目前現況，更能推促各位學習未來新出現的知識與技術；而本課程採用互相交流與討論方式，也希望對於您未來的工作有所啟發或更深一層的了解。

在這門課上完後，您應該會：

- 熟悉 Wireshark 的操作。
- 了解不同服務會有哪些的通訊協定。
- 從封包中找出網路上可能的錯誤設定。

好好把握本課程的練習，希望可以帶給各位同學在未來職場上的闖蕩或學習有幫助，祝福各位。