網路安全的理論與實務

楊中皇 著

第十章 Ethereal封包分析軟體

http://crypto.nknu.edu.tw/textbook/

金禾圖書

伴 您 學 習 成 長 的 每 一 天

金禾資訊

第十章 Ethereal封包分析軟體

- Ethereal 簡介
- Ethereal的安裝方法
- Ethereal的使用

Ethereal 簡介-發展歷史

- Ethereal (http://www.ethereal.com/)是一個公開原始碼(open source)軟體，由Gnu Public License (GPL)授權
- 最初Ethereal由Gerald Combs發展其架構，但進一步研發和維護則由Ethereal team負責
- Ethereal的唸法，有兩種截然不同的發音，有人唸作ether-real，另外一種發音是e-the-real
- Ethereal有多項強大的特色，如幾乎支持所有的協定、豐富的過濾語言、易於查看TCP會談經重構後的數據流等等

Ethereal 簡介-操作平台

- Ethereal 適合大多數Linux/UNIX平台與Windows平台。以下平台皆可安裝與使用Ethereal：
  - AIX
  - BeOS
  - MacOS X
  - Tru64 UNIX (Digital UNIX)
  - Debian GNU/Linux, Gentoo Linux, Mandrake Linux, PLD Linux,
  - ROCK Linux, Red Hat Linux, S/390 Linux, Slackware Linux, SuSE Linux
  - Irix
  - HP/UX
  - SCO
  - FreeBSD, NetBSD, OpenBSD
  - Solaris/Intel, Solaris/SPARC
  - Windows 2000,Windows NT and Windows Me/98/95

Ethereal安裝-Linux

- 一般在Linux 下安裝應用軟體可區分RPM及Source code兩種方式，在安裝Ethereal之前，須先確定已安裝以下套件：需求套件有GTK+，Glib與libpcap（可由www.gtk.org下載）
- 預先套件安裝完畢，開始安裝Ethereal，ethereal-0.10.13.tar.gz，請依照下列步驟安裝
  - #tar zxvf ethereal-0.10.13.tar.gz
  - # cd ethereal.0.10.13
  - # ./configure --prefix=/usr/local/ethereal
- 進行編譯前的參數設定 --prefix=/usr/local/ethereal表示要將Ethereal安裝到此目錄下。
  - # make
- 開始編譯source code 成爲binary code。
  - # make install
- 將 Ethereal binary code 安裝到指定的目錄下，也就是/usr/local/ethereal。

Ethereal安裝-Linux

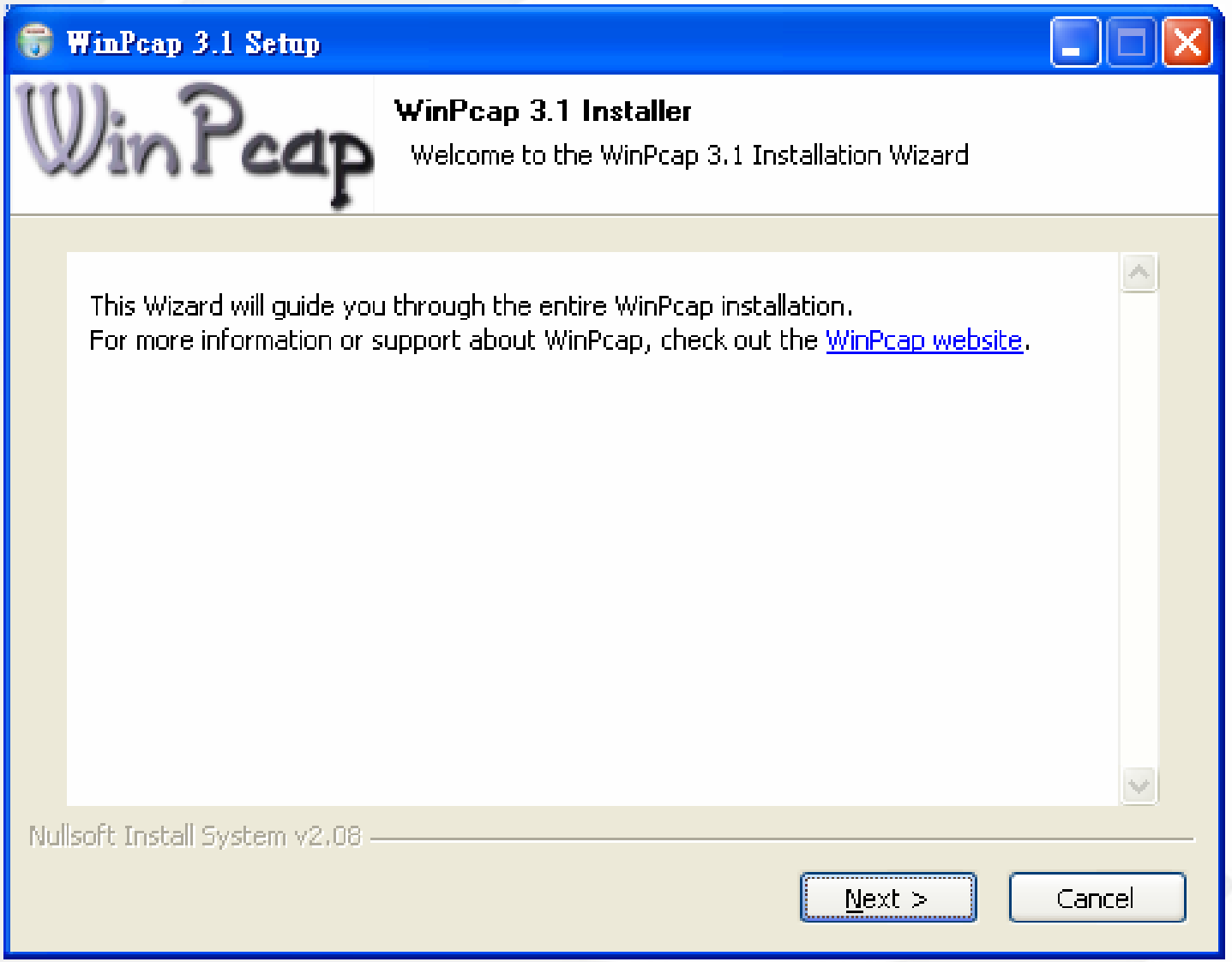
- 設定一些查詢相關功能
  - # vi /etc/man.config
- 加入底下一行路徑，這樣才可以使用”man”來查詢指令用法。
  - MANPATH /usr/local/ethereal/man
- 使用 RPM安裝Ethereal
  - # rpm -ivh ethereal-0.10.6-3.i386.rpm
- 要使用Ethereal，先將目錄切d換至/usr/local/ethereal/bin
  - # cd /usr/local/ethereal/bin
  - # ./ethereal

Ethereal在Linux啓動路徑

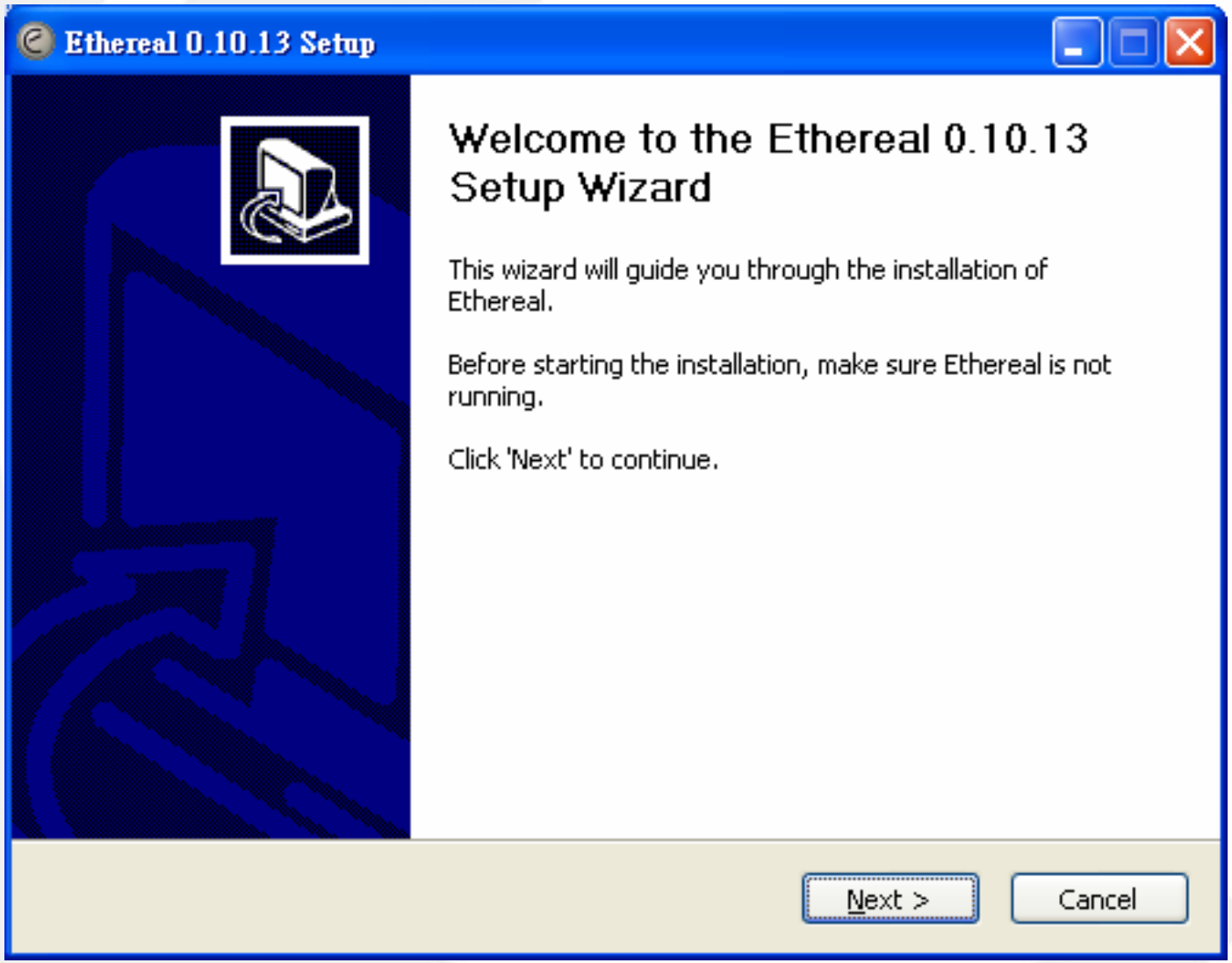
Ethereal安裝-Windows

- 若要在Windows平台上安裝Ethereal，除了下載Windows版本的Ethereal 程式外，須先安裝WinPcap (Windows系統所需要的封包擷取程式)
- 下載完 WinPcap_3_1.exe 和 ethereal-setup-0.10.13.exe 後，先安裝WinPcap_3_1.exe，並點選「Next」鈕，繼續完成安裝步驟。
- ＊如果WinPcap是舊版要更新成新版時，須先移除舊版且重新開機，再安裝新版WinPcap

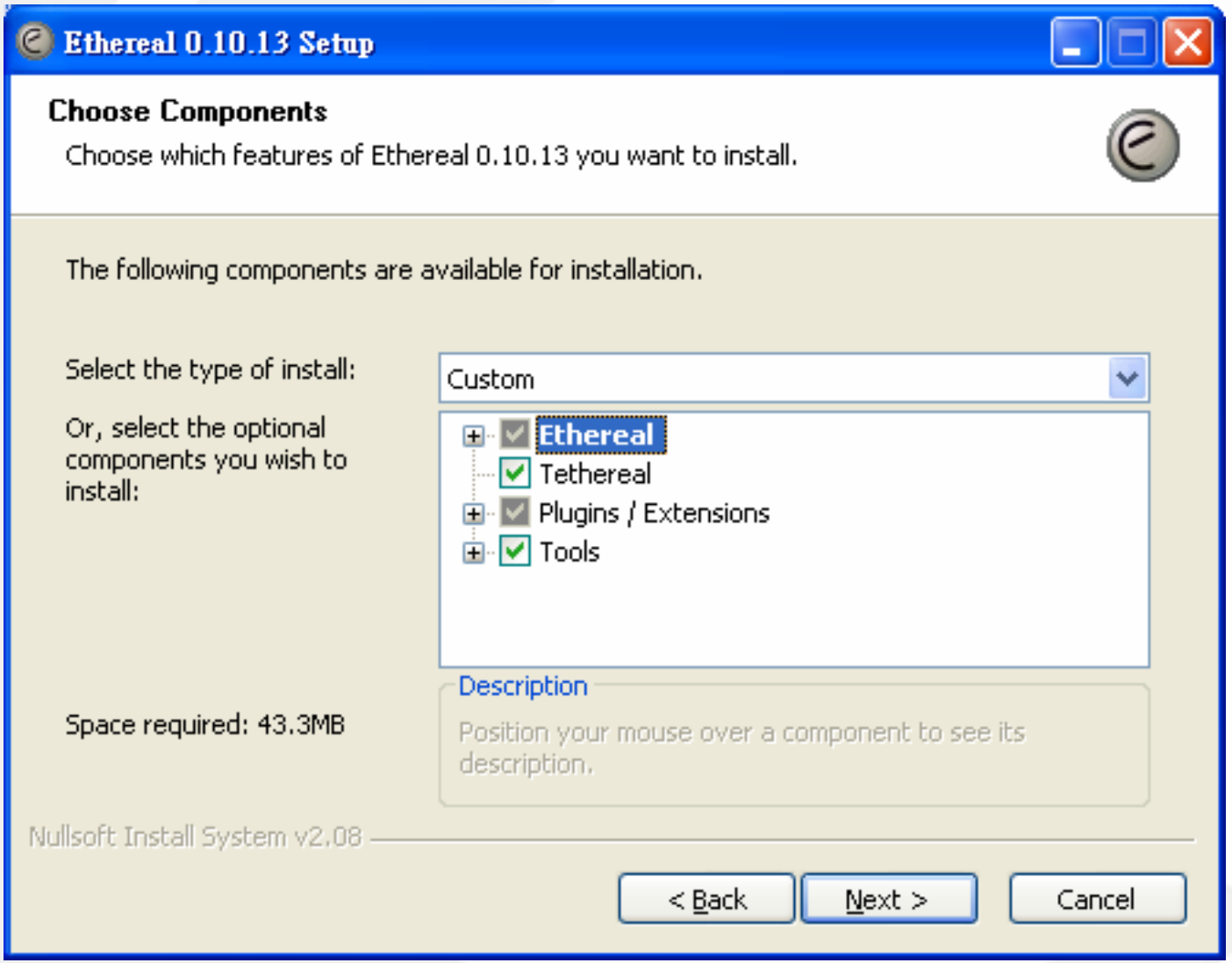
WinPcap3.1安裝畫面



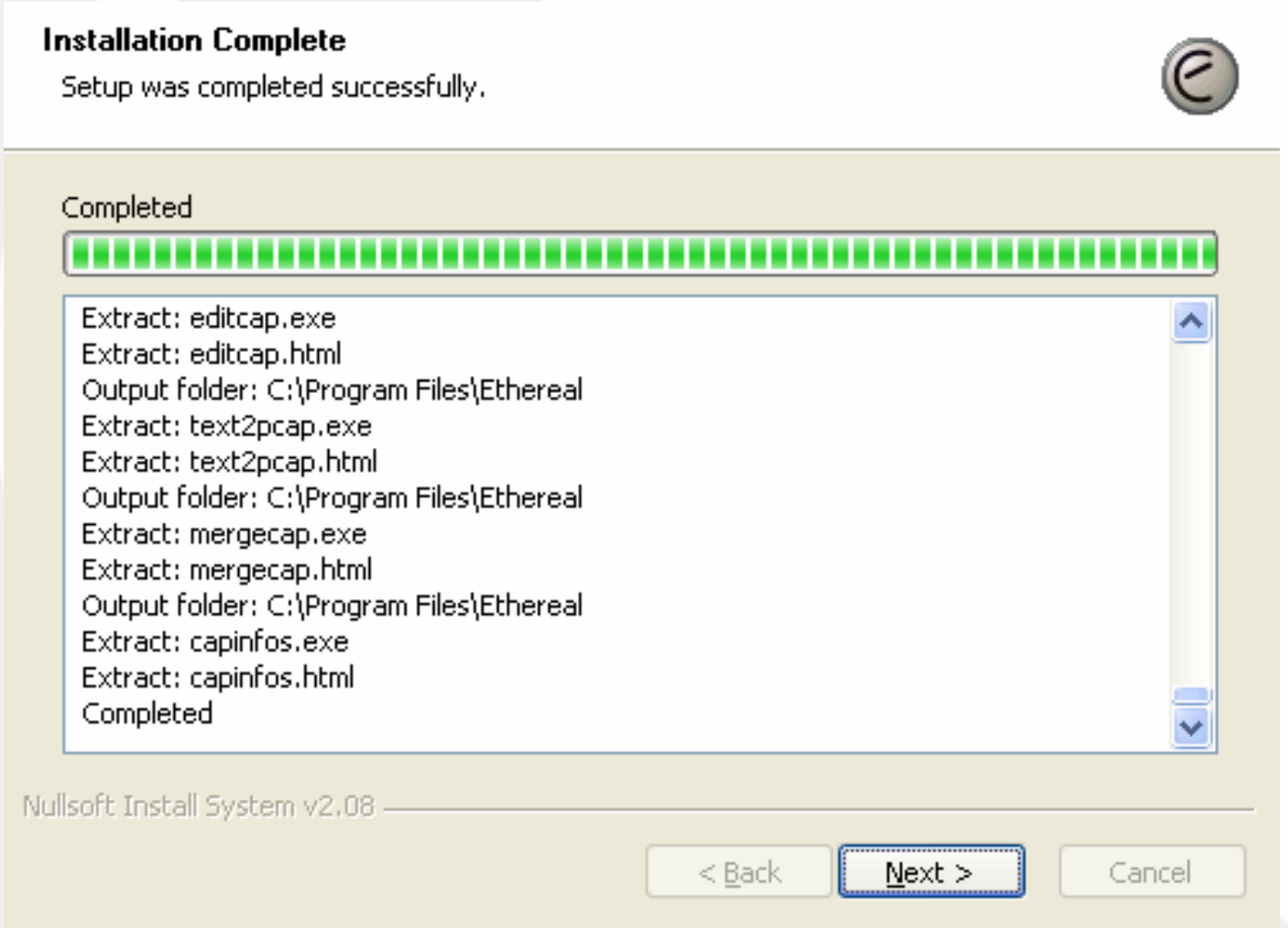
Ethereal Windows版本安裝畫面一



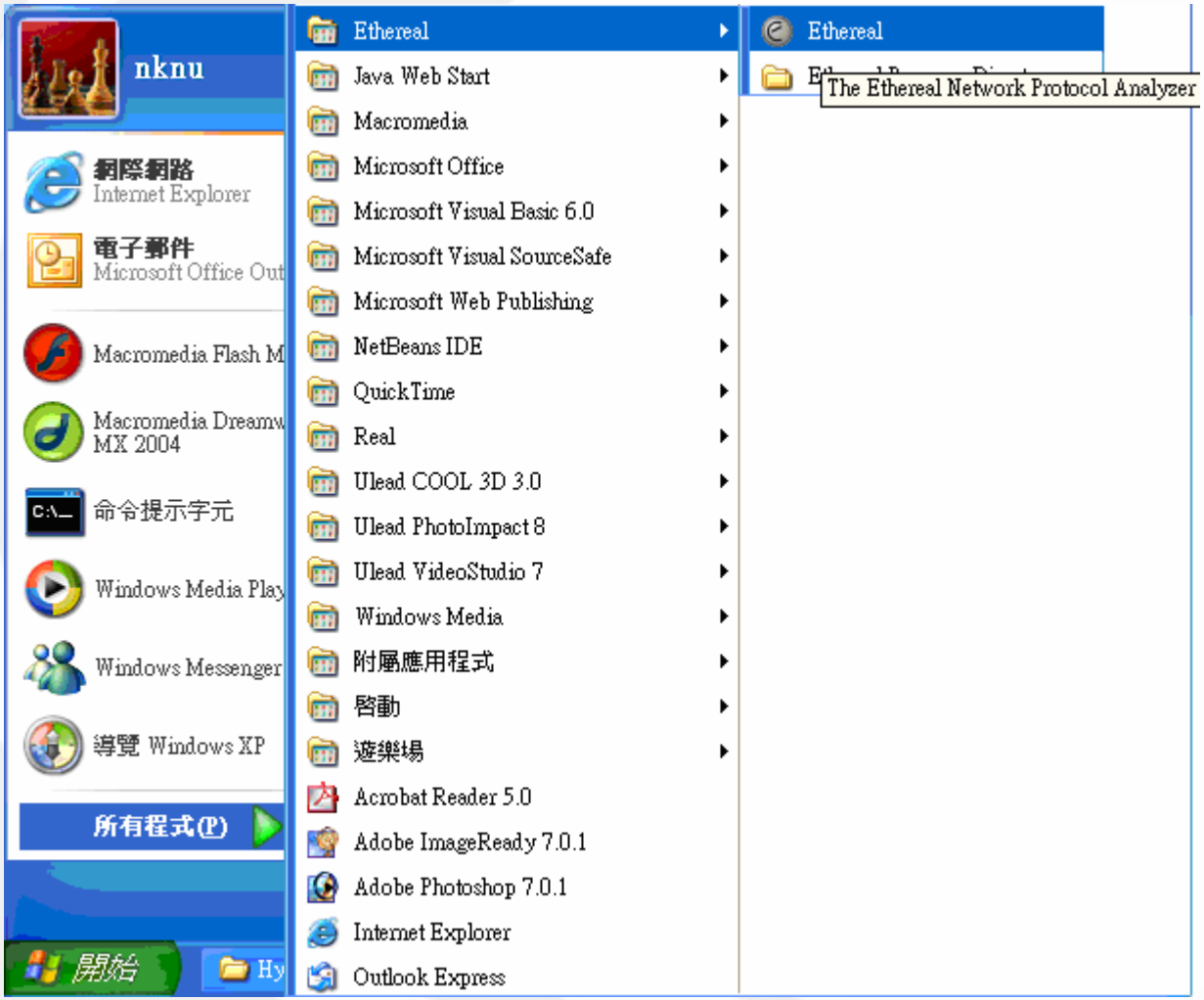
Ethereal Windows版本安裝畫面二



Ethereal Windows版本安裝畫面三



Ethereal在Windows啓動路徑

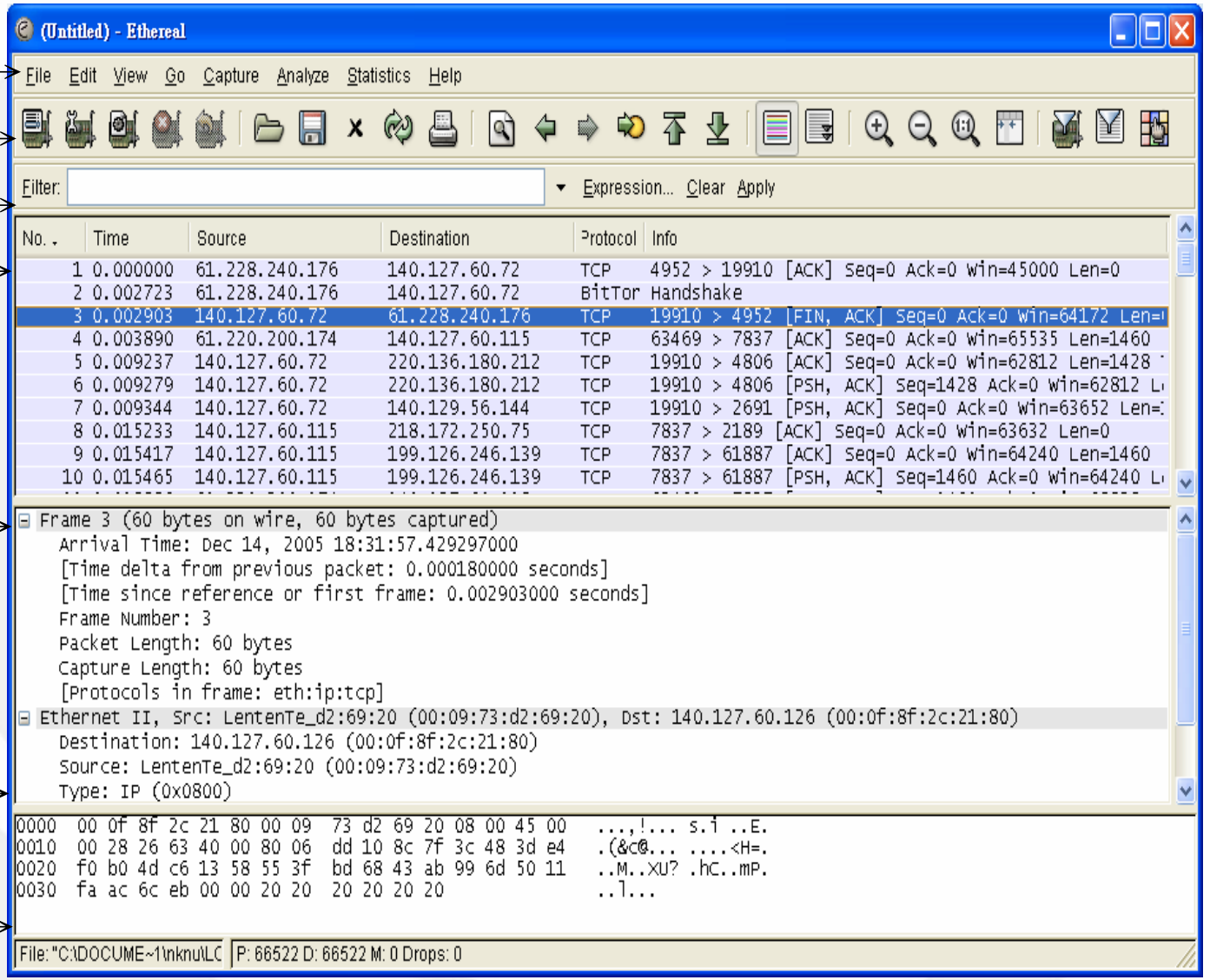


Ethereal的使用-通信協定

- Ethereal支援680多個通信協定和封包種類，可以在以下網站http://www.ethereal.com/docs/dfref/，查到Ethereal所支援的通信協定
- Ethereal主要視窗分成三個
  - 封包清單窗格(packet list pane)
  - 封包內容窗格(packet details pane)
  - 封包位元組窗格(packet bytes pane)

Ethereal的主要視窗

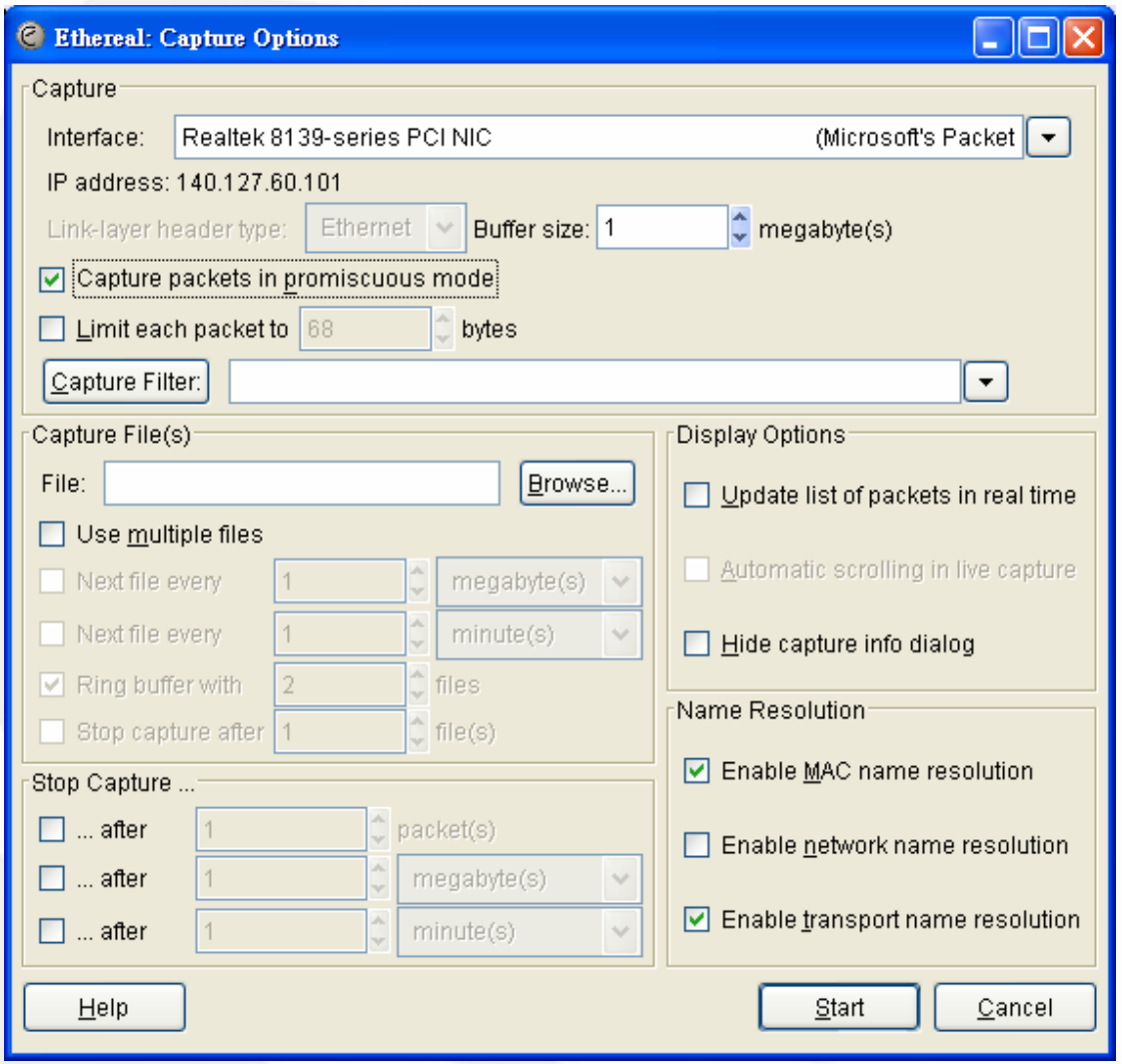
功能表列→
一般工具列→
篩選工具列→
封包清單窗格→
封包內容窗格→
封包內容窗格
(位元組格式)→
狀態列→



Ethereal主要視窗功能說明

- 功能表列：執行Ethereal各項功能。
- 一般功能列：快速啓動功能表列中常用功能。
- 篩選工具列：在filter欄位中輸入特定語法來過濾封包清單窗格中的封包，語法輸入錯誤時，欄位背景會呈現紅色，這類語法稱爲顯示篩選器(display filter)。
- 封包清單窗格(packet list pane) ：顯示封包列表，所列出的可能是目前擷取的封包，或是之前存檔的封包清單，預設值會以爲第一個欄位(流水號)來排序。
- 封包內容窗格(packet details pane) ：會依封包清單窗格所選擇的封包而改變，Ethereal將該封包內容解碼後，以較直覺、較易理解的分層形式顯示出來。
- 封包位元組窗格(packet bytes pane) ：顯示內容和封包內容窗格相同，但以位元組的格式來呈現，當使用者選取封包內容窗格中的協定欄位時，此處相對應的位元組會自動反白。
- 狀態列：顯示目前程式狀態或其他詳細資訊。

Capture功能視窗



Capture Options重要常用的欄位設定

- Interface：會顯示出Ethereal在系統上所找到的所有網路卡，但你只能選取一個作爲封包擷取的介面

- Capture packets in promiscuous mode：此選項可指定Ethereal使用雜亂模式(promiscuous mode)擷取封包，若選取此項，則所有經過選取網路卡的封包都會被擷取下來

- Capture Filter：指定擷取過濾器運算式，擷取想要的特定封包。這與篩選工具列的Filter是不一樣的。在這裡是指在封包擷取進行中且同時過濾封包(Filter while capturing)，這是使用linux的tcpdump命令primitive expressions來做過濾，而篩選工具列的Filter是指已擷取完畢，在上層的視窗中檢視封包時過濾出想要的封包(Filter packets while viewing)

Capture Options重要常用的欄位設定(續)

- Update list of packets in real time：若此項功能被選取，則Ethereal將會邊擷取邊轉換封包到主畫面。若無選取此項功能時，Ethereal的主畫面是沒有動作的，必須等到停止擷取後，Ethereal才會將剛剛擷取到的封包全部一次轉換成可分析型態顯示在主畫面上

- Automatic scrolling in live capture：此項功能須在Update list of packets in real time被選取的前提下才能啓用；而此功能會即時將主畫面捲到最新擷取的封包資料。否則就必須自己手動捲動畫面到最新的封包資料。

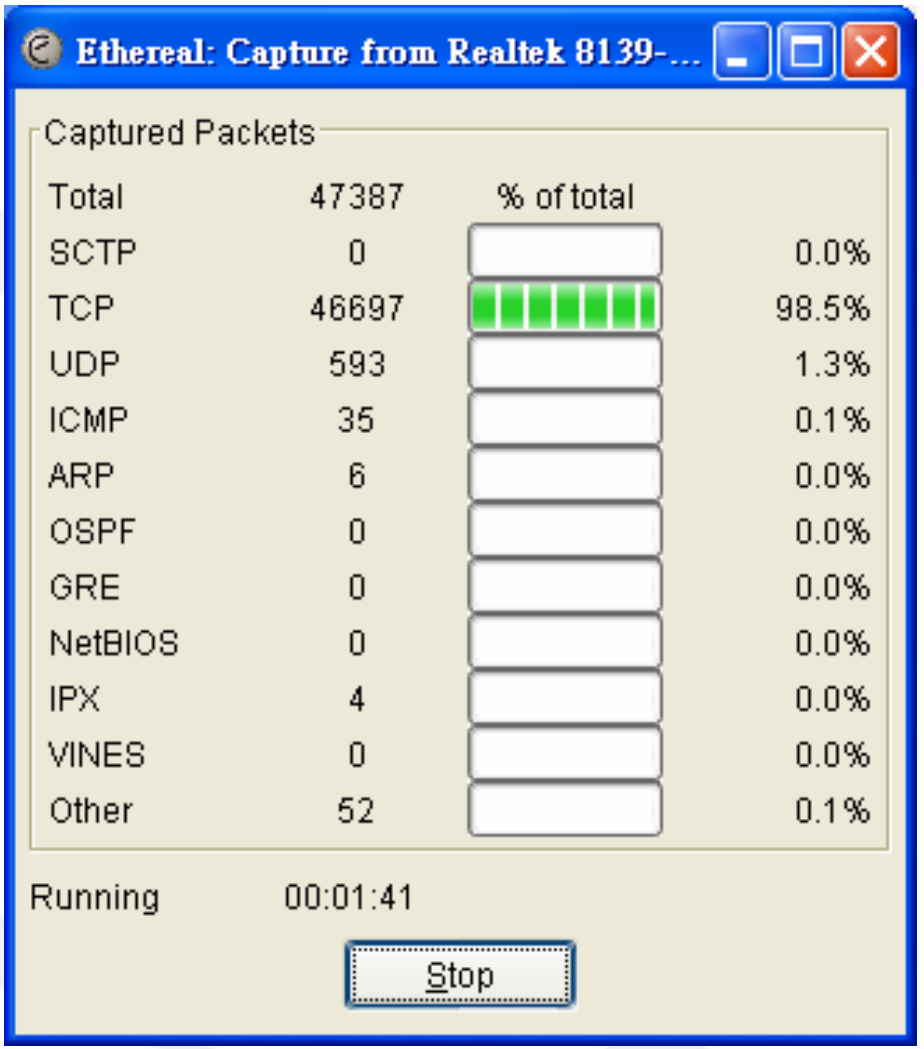
- Enable MAC name resolution：指定是否將網路卡MAC address的前三個位元組轉換成製造商名稱

- Enable network name resolution：指定是否將IP address轉換成DNS網域名稱

- Enable transport name resolution：指定是否將通信埠號碼(port numbers)轉換成協定名稱(protocols)

顯示擷取各類封包百分比

- 完成設定後，選擇按下Capture鈕，即開始擷取封包，並且跳出擷取的對話框。
- 擷取對話框顯示目前已擷取到各種協定封包的數量及佔所有總數的百分比(%)。
- 可以按Stop鈕停止擷取封包動作

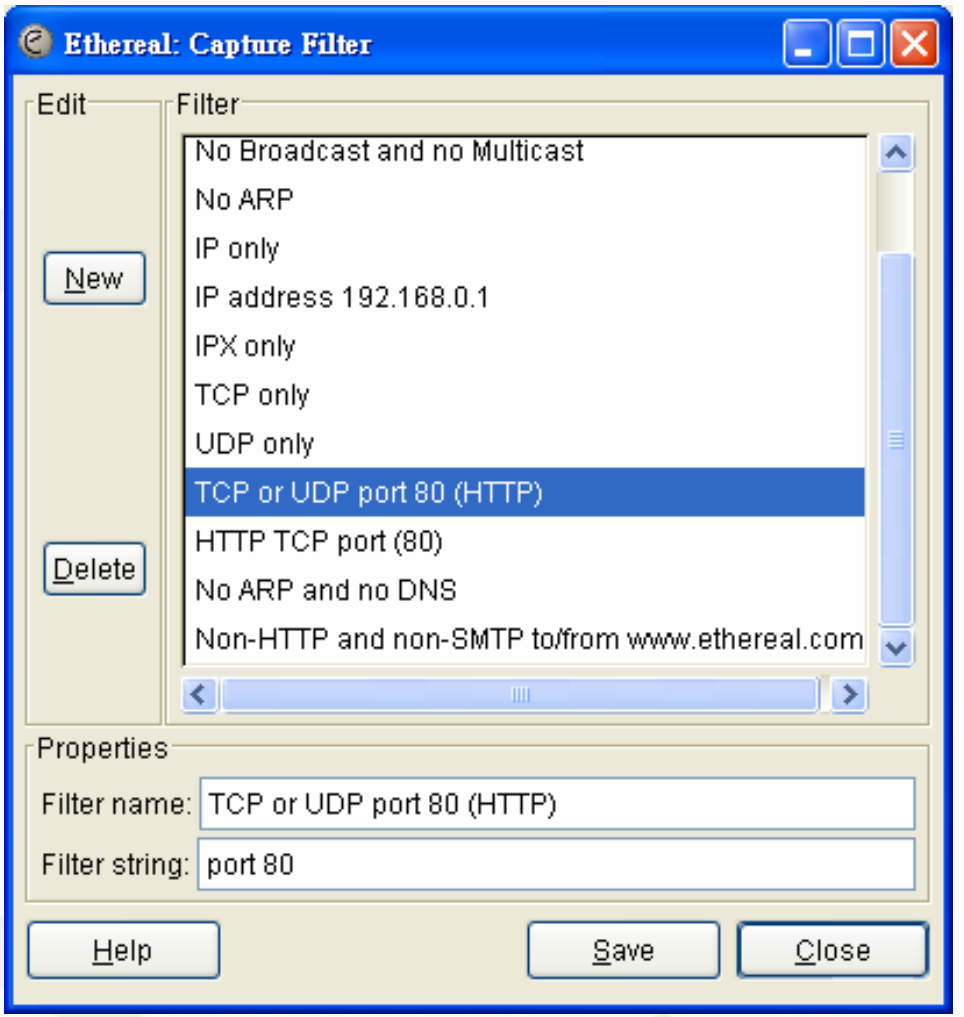


過濾資訊

- Ethereal有兩種過濾的語言
  - 一種是用在擷取進行中同時過濾封包(Filter while capturing)，意指在擷取封包過程中，已過濾符合條件的封包
  - 另一種則是顯示過濾封包(Filter packets while viewing)，意指在擷取完畢後，經由Filter顯示你有興趣的封包，隱藏不感興趣的封包。

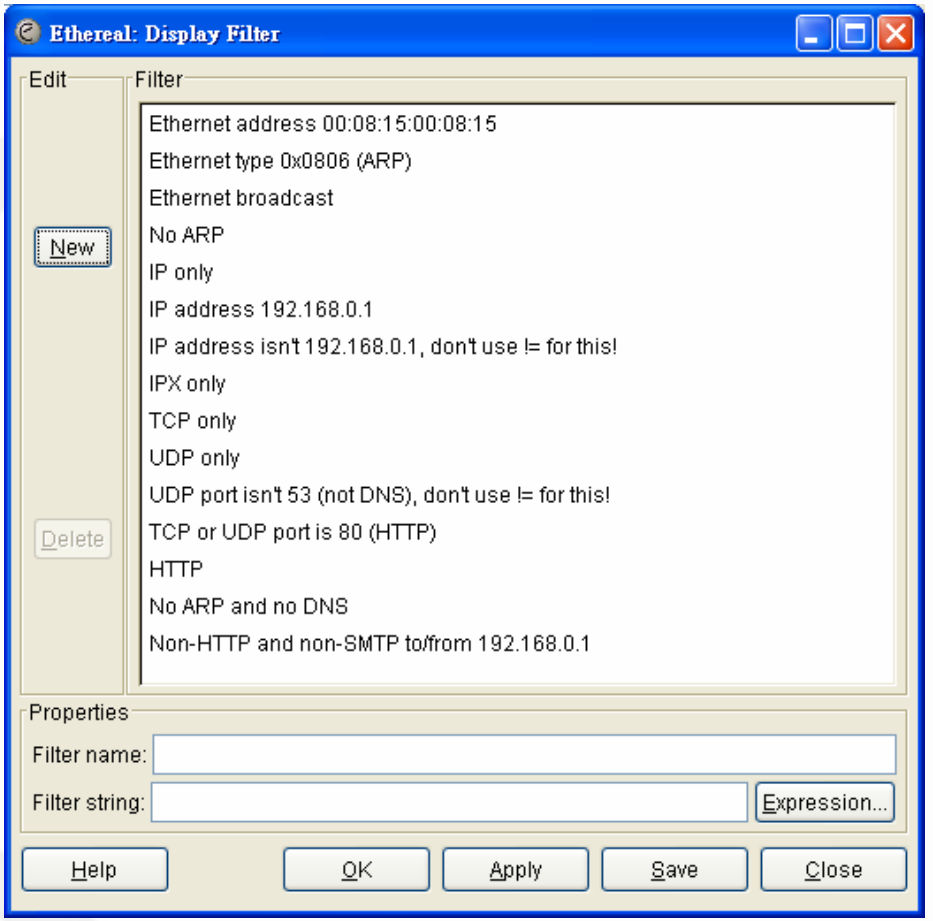
擷取中過濾(Filter while capturing)

- 選取Capture->Capture Filters會出現下列對話框，能利用此功能來編輯一個擷取過濾規則，儲存作爲以後之用。
- 可直接在Filter點選，亦可於Filter name輸入TCP or UDP port 80 作命名，在Filter string輸入port 80，按New鈕，即將此新規則加入Capture Filter，並按Save鈕儲存。
- 以後可在Capture Options的Capture Filter選取此規則做爲過濾選項。



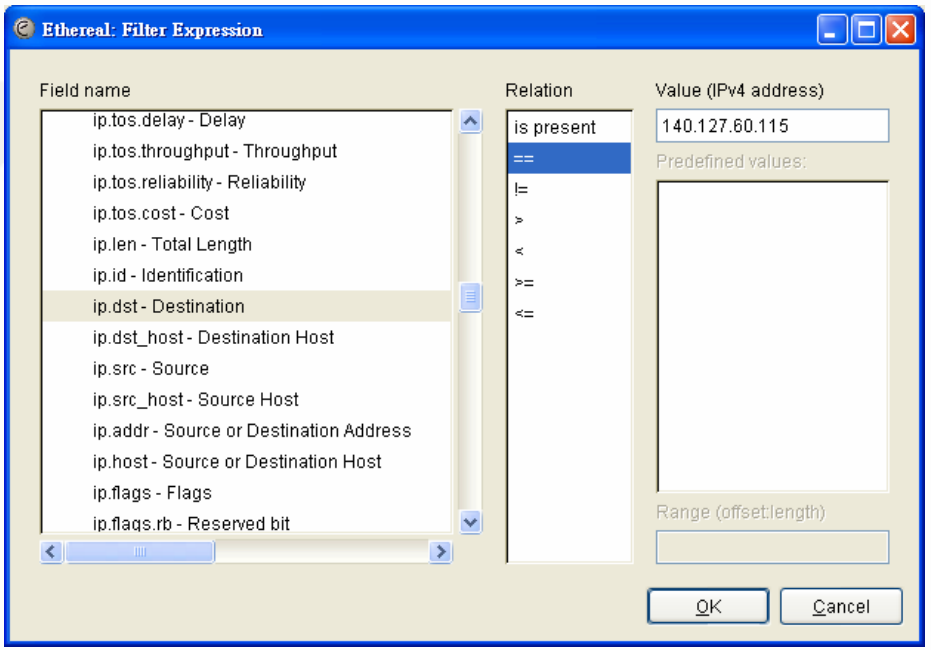
檢視中過濾(Filter packets while viewing)

- 假設對特定封包有興趣，例如，目的主機位址為140.127.60.115且協定為http也就是說TCP port為4097的封包
- 點選視窗左上角的Filter按鈕或是選取Analyze->Display Filters，將出現Display Filter交談框

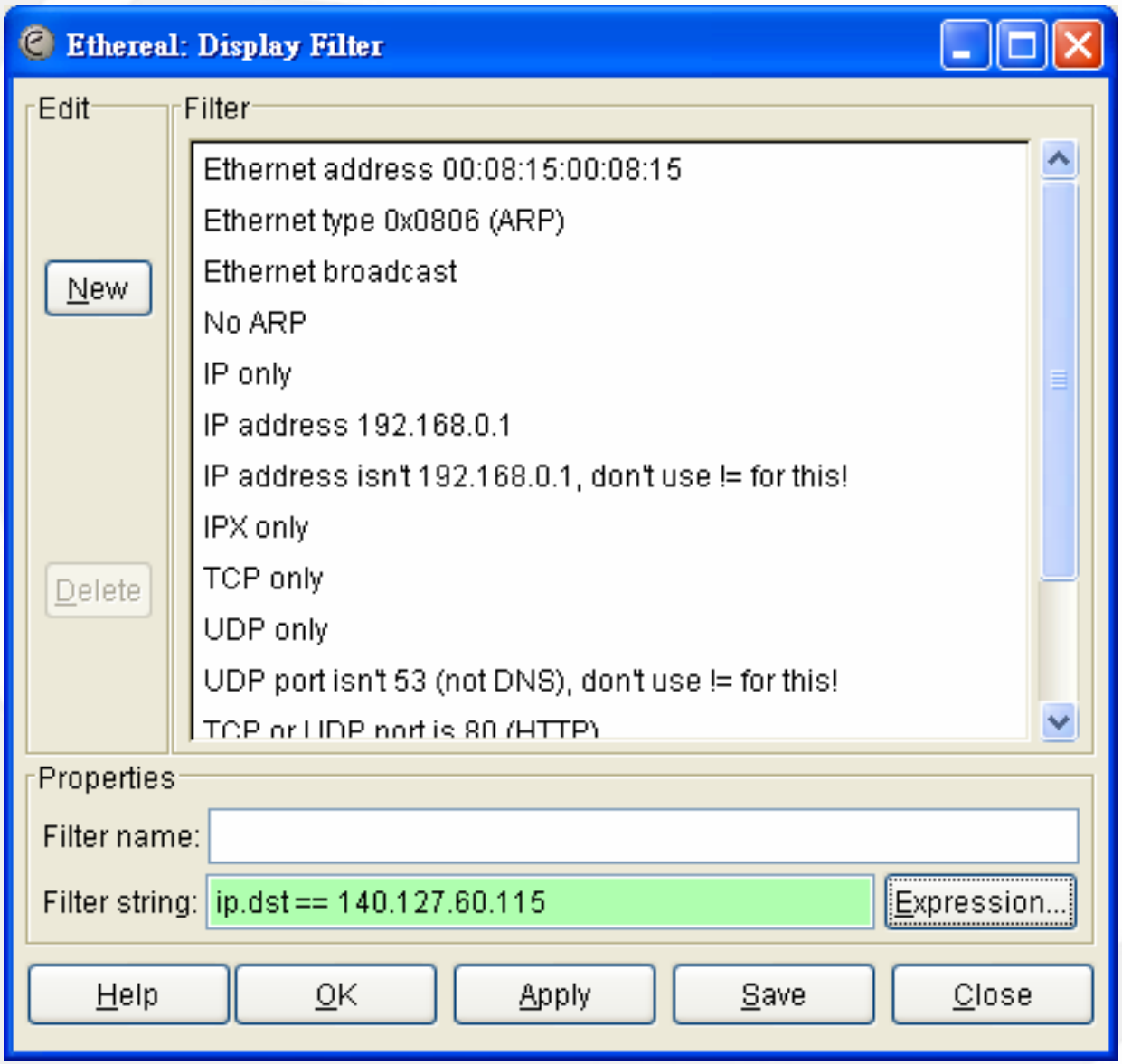


過濾運算式之一

- 開啓Filter Expression交談框
- 在Field name欄位捲動scroll bar找到IP並且展開樹狀結構，選取ip.dst，然後點選Relation欄位的==(等於)，在Value欄位輸入140.127.60.115
- 按下OK鈕即出現右圖中Filter string欄位所呈現的表示式

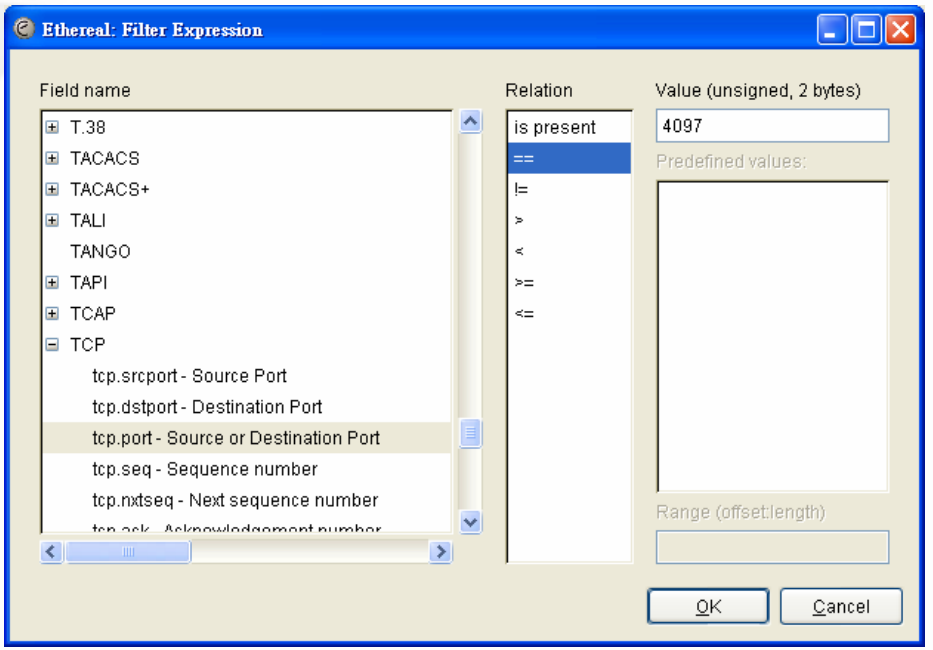


檢視中過濾之二

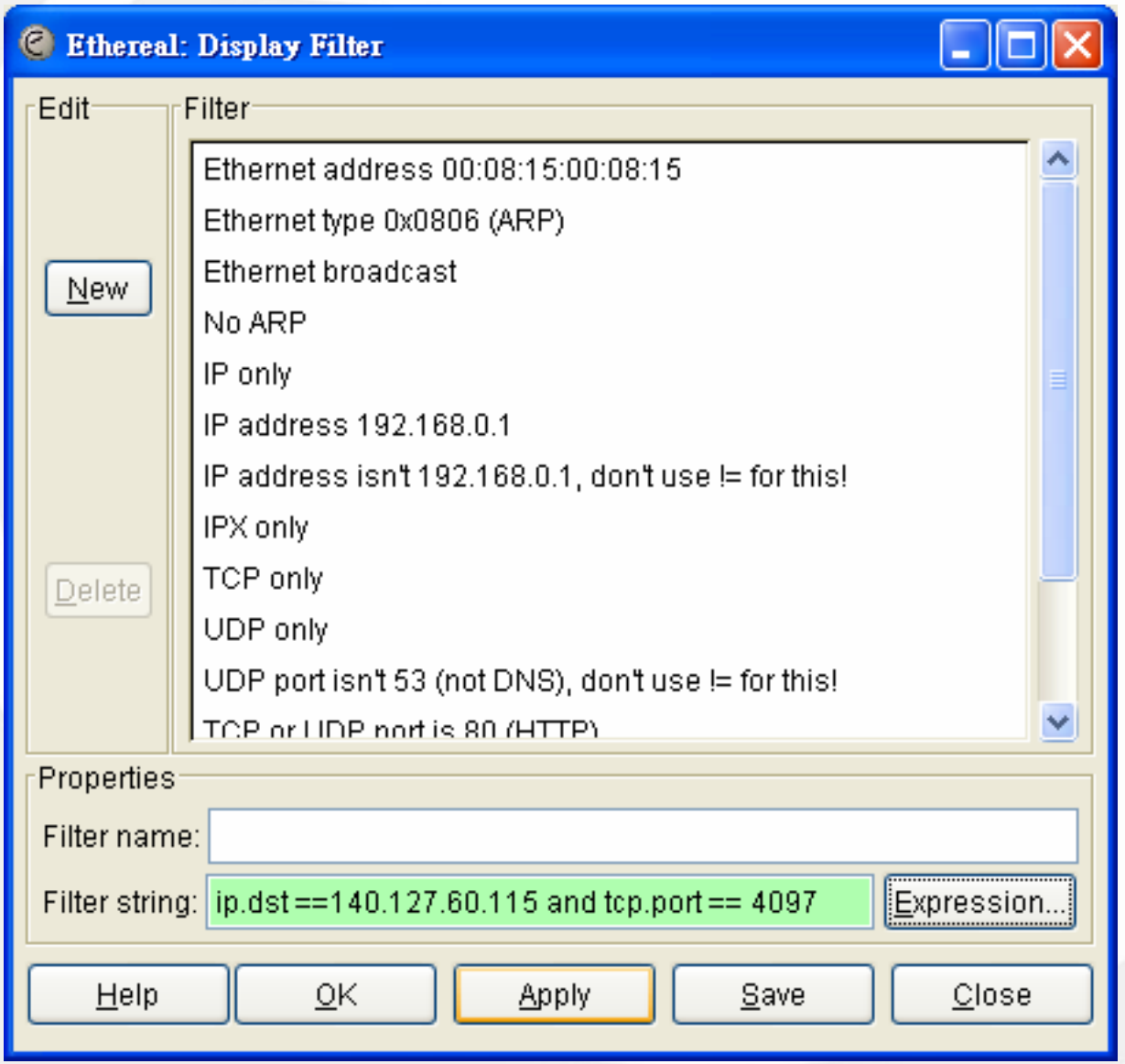

Ethereal: Display Filter
Edit
Filter
Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
Ethernet broadcast
No ARP
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
UDP port isn't 53 (not DNS), don't use != for this!
New
Delete
Properties
Filter name:
Filter string:
ip.dst == 140.127.60.115
Expression...
Help
OK
Apply
Save
Close

過濾運算式之二

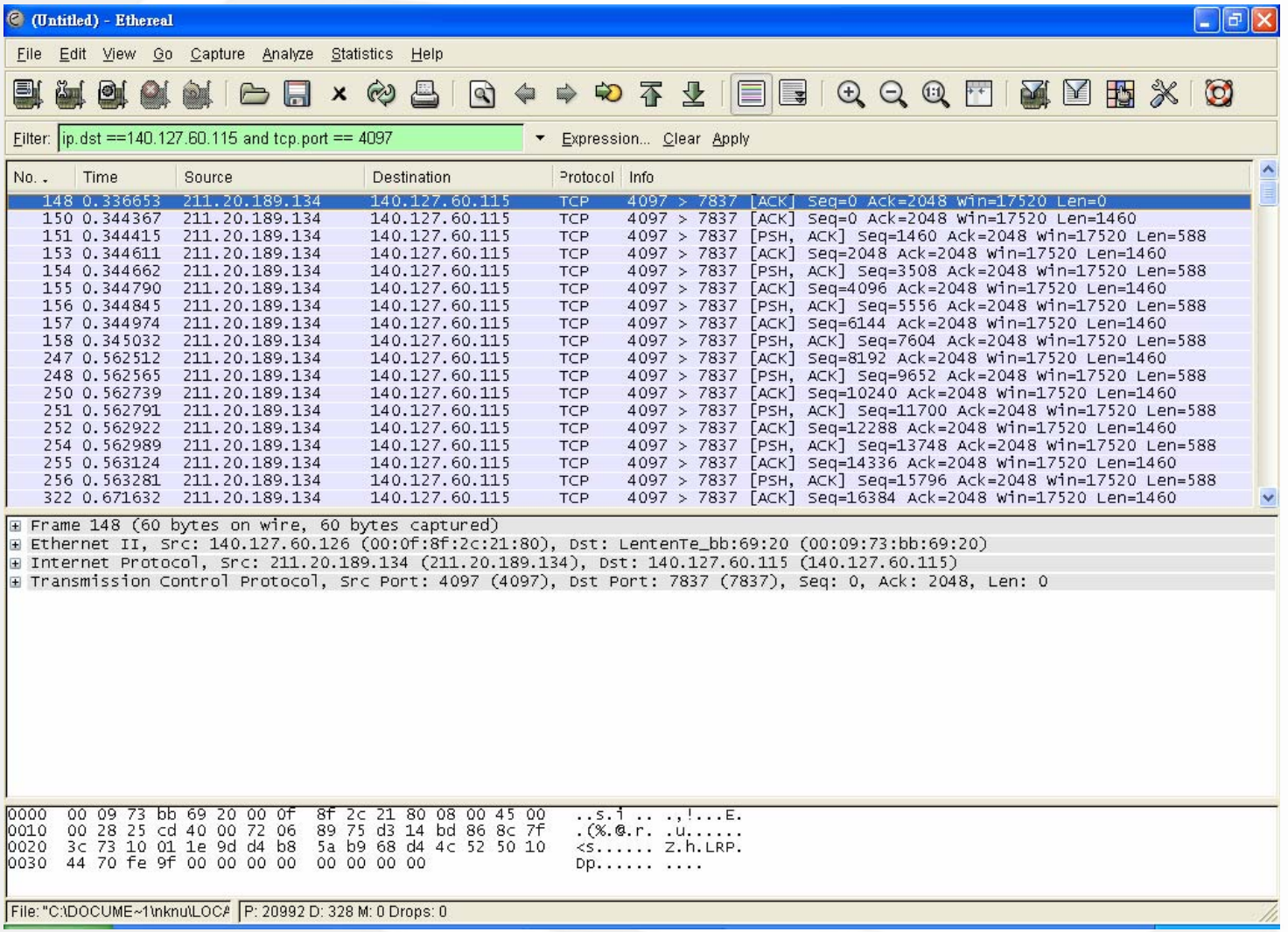
- 再開啓Filter Expression交談框
- 依照前面所提方式找到TCP展開並點選tcp.port，然後點選Relation欄位的==(等於)，在Value欄位輸入4097，如右圖



檢視中過濾之三


Ethereal: Display Filter
Edit
Filter
Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
Ethernet broadcast
No ARP
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
UDP port isn't 53 (not DNS), don't use != for this!
New
Delete
Properties
Filter name:
Filter string:
ip.dst ==140.127.60.115 and tcp.port == 4097
Expression...
Help
OK
Apply
Save
Close

過濾後結果

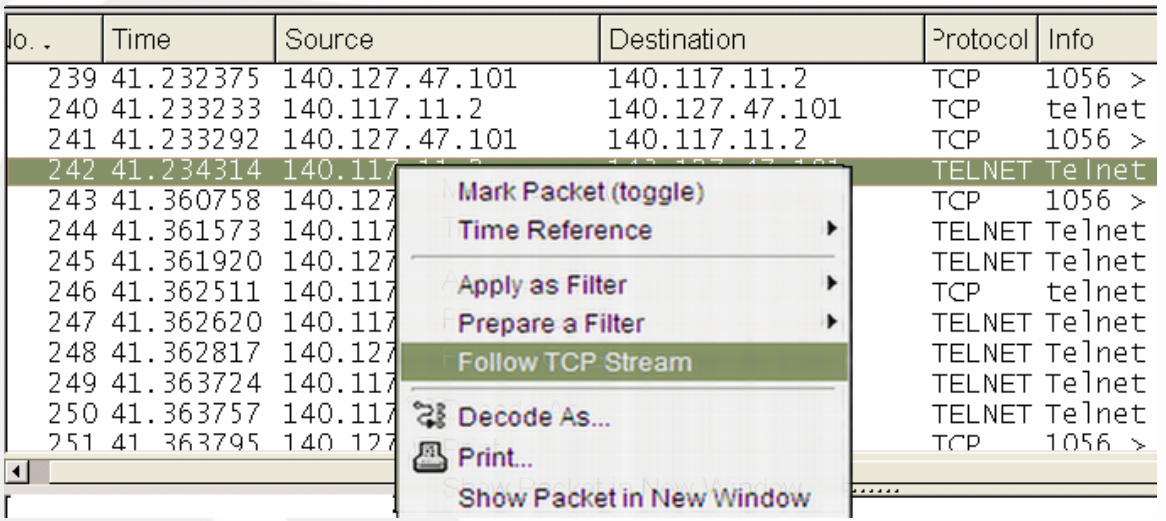

(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: ip.dst ==140.127.60.115 and tcp.port == 4097
Expression... Clear Apply
No. Time Source Destination Protocol Info
148 0.336653 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [ACK] Seq=0 Ack=2048 Win=17520 Len=0
150 0.344367 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [ACK] Seq=0 Ack=2048 Win=17520 Len=1460
151 0.344415 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [PSH, ACK] Seq=1460 Ack=2048 Win=17520 Len=588
153 0.344611 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [ACK] Seq=2048 Ack=2048 Win=17520 Len=1460
154 0.344662 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [PSH, ACK] Seq=3508 Ack=2048 Win=17520 Len=588
155 0.344790 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [ACK] Seq=4096 Ack=2048 Win=17520 Len=1460
156 0.344845 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [PSH, ACK] Seq=5556 Ack=2048 Win=17520 Len=588
157 0.344974 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [ACK] Seq=6144 Ack=2048 Win=17520 Len=1460
158 0.345032 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [PSH, ACK] Seq=7604 Ack=2048 Win=17520 Len=588
247 0.562512 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [ACK] Seq=8192 Ack=2048 Win=17520 Len=1460
248 0.562565 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [PSH, ACK] Seq=9652 Ack=2048 Win=17520 Len=588
250 0.562739 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [ACK] Seq=10240 Ack=2048 Win=17520 Len=1460
251 0.562791 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [PSH, ACK] Seq=11700 Ack=2048 Win=17520 Len=588
252 0.562922 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [ACK] Seq=12288 Ack=2048 Win=17520 Len=1460
254 0.562989 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [PSH, ACK] Seq=13748 Ack=2048 Win=17520 Len=588
255 0.563124 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [ACK] Seq=14336 Ack=2048 Win=17520 Len=1460
256 0.563281 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [PSH, ACK] Seq=15796 Ack=2048 Win=17520 Len=588
322 0.671632 211.20.189.134 140.127.60.115 TCP 4097 > 7837 [ACK] Seq=16384 Ack=2048 Win=17520 Len=1460
Frame 148 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 140.127.60.126 (00:0f:8f:2c:21:80), Dst: LentenTe_bb:69:20 (00:09:73:bb:69:20)
Internet Protocol, Src: 211.20.189.134 (211.20.189.134), Dst: 140.127.60.115 (140.127.60.115)
Transmission Control Protocol, Src Port: 4097 (4097), Dst Port: 7837 (7837), Seq: 0, Ack: 2048, Len: 0
0000 00 09 73 bb 69 20 00 0f 8f 2c 21 80 08 00 45 00
0010 00 28 25 cd 40 00 72 06 89 75 d3 14 bd 86 8c 7f
0020 3c 73 10 01 1e 9d d4 b8 5a b9 68 d4 4c 52 50 10
0030 44 70 fe 9f 00 00 00 00 00 00 00 00
File: "C:\DOCUME~1\nknu\LOCA
P: 20992 D: 328 M: 0 Drops: 0

Following TCP streams

- 如果想要知道telnet交談中傳送的密碼，或是想了解在整個TCP會談中，應用層下了那些命令、處理了那些資料、順序爲何，便可用Ethereal

- Ethereal提供一個很好用的工具，讓使用者更容易分析了解TCP 會談的過程。

選取Follow TCP Stream路徑



- 在此以TELNET爲例，使用Ethereal擷取TELNET封包結果。
- 先從packet list pane中選取其中Protocol爲TELNET的封包，滑鼠點右鍵顯示快捷功能表，選取Follow TCP Stream如上圖，會顯示出TELNET的TCP 會談的結果。

Follow TCP Stream顯示使用者ID和password

- 可以看到兩台主機在TCP 會談整個過程
- 包含在作登入動作時，輸入使用者身分(ID) 和通行 碼 (password) 都被解譯出來如右圖

觀看過濾結果的資料形式

- ASCII
- EBCDIC
- HEX Dump：以十六進位形式顯示(如下圖)

```
000000CB  20 20 20 20 20 20 20 20  3d 3d 0d 0a 3d 3d 20 20          ==..==
000000DB  20 20 20 20 2a 2a 2a 2a  2a 2a 2a 2a 2a 2a 2a 20      **** *******
000000EB  20 20 20 1b 5b 31 3b 33  32 6d ac fc c4 52 a4 a7     .[1;3 2m...R..
000000FB  ae 71 b9 71 a4 6c a7 47  a7 69 c4 e6 a8 74 b2 ce .q.q.l.G .i...t..
0000010B  1b 5b 30 3b 34 30 6d 20  20 20 20 2a 2a 2a 2a 2a .[0;40m     *****
```

- C Arrays：TCP stream會顯示成C 語言陣列形式

參考資料

- A. Orebaugh, G. Morris, E. Warnicke and G. Ramirez ，*Ethereal Packet Sniffing* ，SYNGRESS，2004.
- R. Sharpe and E. Warnicke，*Ethereal User's Guide*，http://www.ethereal.com/
- Ethereal，http://www.ethereal.com/
- WinPcap (Windows所需要的封包擷取程式)：http://www.ethereal.com/download.html