

網路封包分析的好幫手—Wireshark 擷取分析、防範攻擊無所不包

蔡一郎

資訊安全是近幾年相當熱門的話題，在一個封閉的網路環境中，才有可能實現一個絕對安全的網路環境，在網際網路中是不太可能存在這樣的條件。目前，網路環境中大多建置了各式各樣的網路安全設備，如防火牆（Firewall）、入侵偵測防禦系統（IPS）、內容閘道器（Content Gateway）等，這些設備大多只能夠針對已知的特徵進行過濾和阻擋惡意行為，對於新型態或無法明確定義特徵的行為，則幾乎都達不到防護的要求。

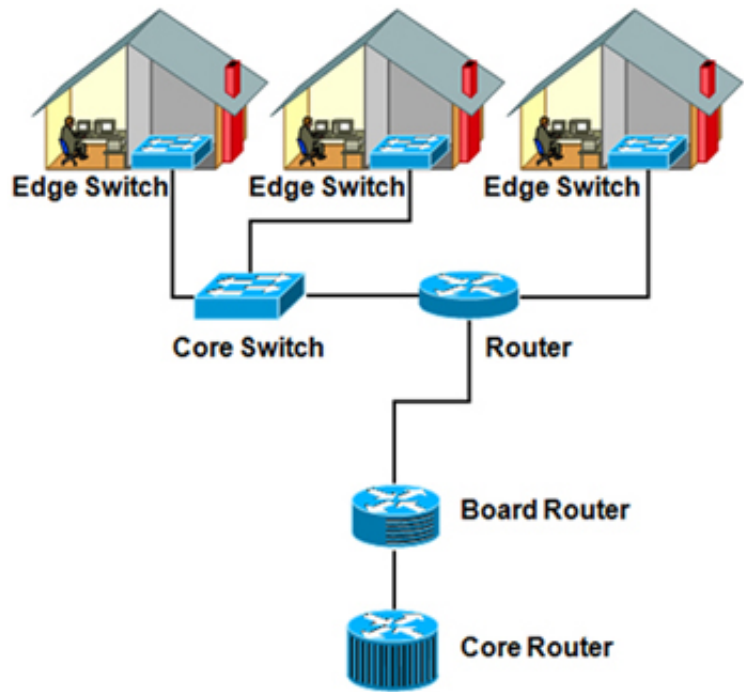
網路封包的解析是目前經常用來解決現有設備不足的最佳方案。分析網路封包，除了能夠找出異常的行為和網路流量之外，也可以用來學習各種不同通訊協定，是網路管理人員不可或缺的技能。網路提供使用環境，人類是網路的使用者，許多在真實社會發生的事件，仍然會在網路上重演，但是更為隱匿，這也是發展資訊安全技術的重點所在。

認識網路封包分析

網路封包是目前網路用來傳送資料的最小單位。封包因為不同的應用服務或通訊協定，而有各種不同的大小。一個封包由標頭（Header）和資料（Data）所組成，封包的屬性被詳細地定義在標頭中，包括所使用的通訊協定、來源的IP位址、來源的通訊埠、目的地的IP位址、目的地的通訊埠等欄位，不過並非所有的通訊協定都有相同的欄位資料，由於採用不同的通訊協定，網路封包的結構都有些許的差異。

在網路上傳送網路封包，路由器（Router）主要是依據封包標頭所記載的目的地IP位址進行路由的交換，以確定依據目前的路由表（Routing Table）能夠將封包送到目的地。因此，在網路架構中的適當位置擷取網路封包，就可以取得相關的資訊進行行為分析。目前常見的網路封包分析工具有Tcpdump、Sniffer、NetXRay、Wireshark（Ethereal）等，其中Wireshark雖然屬於Open Source軟體，但是所具備的功能卻足可媲美許多商業軟體。在GNU GPL通用授權的保障之下，使用者可以免費取得軟體及其程式碼，並擁有修改原始碼與客製化的權利。

一般而言，之所以想要解析網路封包，大致上有以下幾種原因：瞭解電腦網路目前進行的動作、監聽側錄另一台電腦網路連線、瞭解網路程式如何運行以及學習網路通訊協定。透過網路封包的工具，使用者可以掌握目前網路上的通訊和使用者行為模式。準備擷取網路封包時，必須配合Hub、Y-TAP或Switch進行網路介面的對應，這是因應Switch本身設備的特性而必須進行的設定。大多數中高階的交換器都會提供Port Mirror或Port Mapping功能，這樣才能夠確保安裝網路封包分析工具的設備能夠正確地擷取到網路封包。



▲ 網路的架構圖

網路封包分析工具 (Network Packet Analyzer) 並不是入侵偵測 (防禦) 系統，既不會對擷取到的網路封包提出警告，當然也不可能針對任何網路封包進行阻擋的動作。網路封包分析工具主要是解析網路封包，透過軟體的介面解析網路封包，以呈現使用者真實的網路行為。

通訊協定簡介

因應不同的網路服務，目前網路使用相當多不同類型的通訊協定，這些通訊協定可以視為「溝通」的語言，讓資訊透過相同的語言在網路上進行交流，以下列舉出在網路層、傳輸層與應用層常見的通訊協定。

TCP/IP的架構	通訊協定
網路層	IP(IPv4,IPv6,IPv9)、OSPF、IS-IS、BGP、IPsec、ARP、RARP、RIP、ICMP、ICMPv6等
傳輸層	TCP、UDP、DCCP、SCTP、RTP、RSVP、IGMP、PPTP等
應用層	DHCP、DNS、FTP、Gopher、HTTP、IMAP4、IRC、NNTP、XMPP、POP3、SIP、SMTP、SNMP、SSH、TELNET、RPC、RTCP、RTSP、TLS、SDP、SOAP、GTP、STUN、NTP等
連結層	Ethernet、Wi-Fi、MPLS等

目前網路上有許多不安全的通訊協定，這些通訊協定大多採用明碼的方式傳送，經常造成資訊外洩，如HTTP、TELNET、POP、SMTP等。這些通訊協定也都應用在常見的網路服務，包括網頁瀏覽、電子郵件接收與傳

送，以及遠端管理連線等。傳統的網路服務程序，因為在網路上用明文傳送數據、用戶帳號和用戶密碼，很容易受到中間人 (Man-in-the-middle) 方式的攻擊。

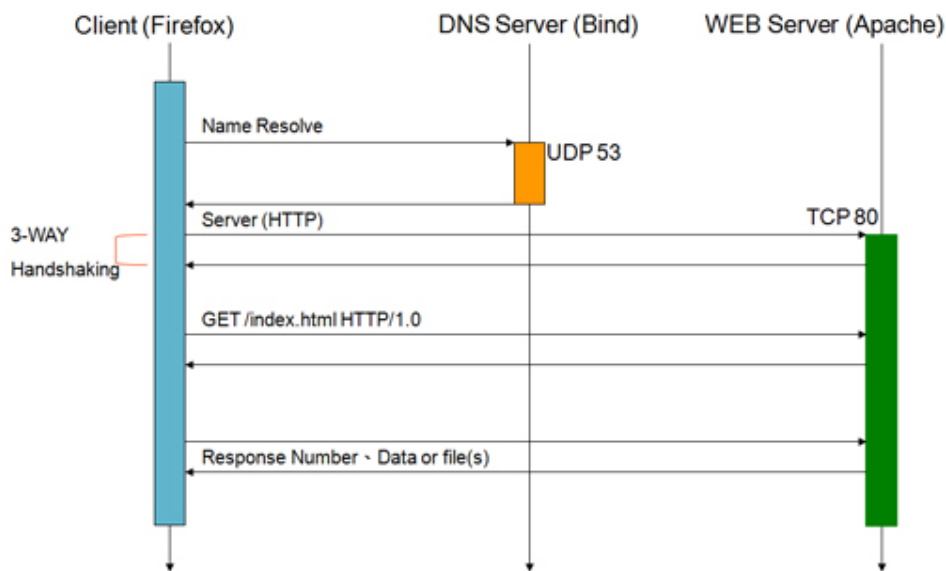
TCP是目前網路上最常見的通訊協定，屬於TCP/IP模型中的Application Layer (應用層)，能夠確保資料正確可靠地傳送到目的地，TCP連接包含連線建立、資料傳送和連線終止三個狀態。必須完成三向交握，才能夠建立連線。

Client→Server 發送 SYN

Server→Client 發送 SYN/ACK

Client→Server 發送 ACK

HTTP (HyperText Transfer Protocol) 是一種網際網路上應用相當廣泛的網路協定，使用者端和伺服器端之間可以透過HTTP來傳輸資料，因為在瀏覽大多數的網站時，都會採用網域名稱的方式，因此在整個建立連線的過程，會先查詢DNS。使用UDP 53埠向系統設定的DNS伺服器進行查詢，待取得解析後的IP位址後，才會進行TCP三向交握的處理，以建立使用者端與伺服器端的連線。



▲ HTTP通訊協定

Telnet協議是TCP/IP協議族中的一員，是Internet遠端登入服務的標準協議和主要方式，傳統Telnet連線通訊所傳輸的資料並未加密，這代表所輸入及顯示的資料，包括帳號名稱和密碼等隱密資料，可能會遭其他人竊聽，因此目前大多數設備都已經使用安全遠端登入的通訊協定SSH來取代Telnet。由於SSH採用了加密的機制來保護所傳送的資料，因此透過Wireshark就可以很容易地發現SSH所傳送的網路封包，其內容都經過加密處理，不像Telnet使用明文的方式來傳送資料。

Wireshark簡介

Wireshark的前身就是大名鼎鼎的Ethereal，目前最新的版本是1.0.2版，各位可以直接到Wireshark的官方網站 (www.wireshark.org) 下載，在網站上提供了許多不同作業系統的版本，可以安裝在各種常見的作業系統中，在資訊安全領域中，Wireshark被廣泛應用在網路封包的解析，目前已經能夠解析超過七百種的通訊協定，所以對於目前網路上所使用的通訊協定，幾乎都能夠辨識與解析。此外，Wireshark也結合了強大功能的過濾器，讓使用者可以針對特定的目標分析網路封包，有助於通訊協定的行為研究與異常行為的偵測。



▲ Wireshark官方網站 (www.wireshark.org)

Wireshark也支援其他軟體所擷取下來網路封包檔案，以下是目前能夠支援的格式，幾乎涵蓋了所有常見的工具軟體：

libpcap, tcpdump and various other tools using tcpdump's capture format

Sun snoop and atmsnoop

Shomiti/Finisar Surveyor captures

Novell LANalyzer captures

Microsoft Network Monitor captures

AIX's iptrace captures

Cinco Networks NetXray captures

Network Associates Windows-based Sniffer and Sniffer Pro captures

Network General/Network Associates DOS-based Sniffer (compressed or uncompressed) captures

AG Group/WildPackets EtherPeek/TokenPeek/

AiroPeek/EtherHelp/PacketGrabber captures

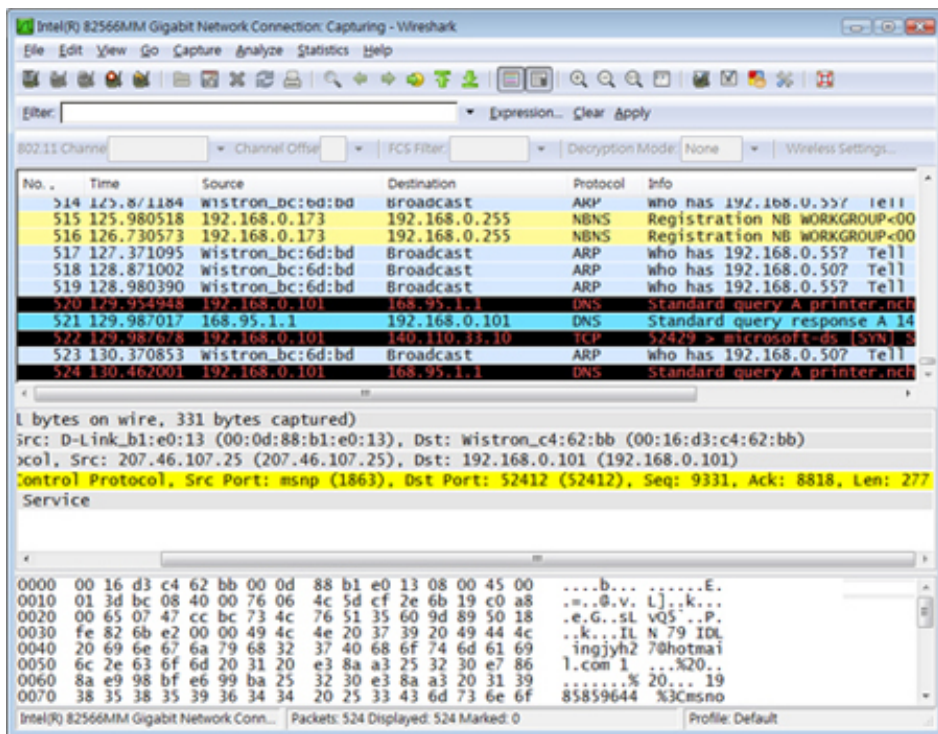
RADCOM's WAN/LAN Analyzer captures Network Instruments
Observer version 9 captures
Lucent/Ascend router debug output
HP-UX's nettl
Toshiba's ISDN routers dump output
ISDN4BSD i4btrace utility
traces from the EyeSDN USB S0
IPLog format from the Cisco Secure Intrusion
Detection System
pppd logs (pppdump format)
the output from VMS's TCPIPtrace/TCPtrace/ UCX\$TRACE utilities
the text output from the DBS Etherwatch VMS utility
Visual Networks' Visual UpTime traffic capture
the output from CoSine L2 debug
the output from Accellent's 5Views LAN agents
Endace Measurement Systems' ERF format captures
Linux Bluez Bluetooth stack hcidump -w traces
Catapult DCT2000 .out files

如果之前使用過上述的軟體擷取好檔案，就能夠直接透過Wireshark開啟並且運作所提供的各種過濾器與統計分析的功能進行處理，解決原工具可能無友善使用者介面的問題，例如純文字模式的tcpdump就無法提供像Wireshark一樣強大的過濾器與圖形介面。將tcpdump的檔案載入到Wireshark中，就能夠快速針對封包的內容與網路封包所隱藏的行為進行分析，使用上相當的方便。

Wireshark的操作介面

Wireshark雖然不是商業軟體，但是所提供軟體介面相當優秀，具備完整的過濾器和統計分析的功能。其操作介面分成幾個主要的部份，包括最上方的功能表和各種工具列、網路封包的清單、封包的標頭和封包的內容，並且以不同的顏色來代表各種不同的通訊協定或是過濾條件。這樣的設計讓使用者在擷取網路封包的過程中，就能夠即時瞭解目前網路上所傳送的網路封包類型。由於Wireshark可以解析超過七百種的通訊協定，因此幾乎所有協定都能夠解碼，就算將來有新的通訊協定推出，也會因為其採用開放原始碼的授權方式，而能夠快速地發展解析新通訊協定所需要的程式，這對於適應未來網路的發展相當重要。

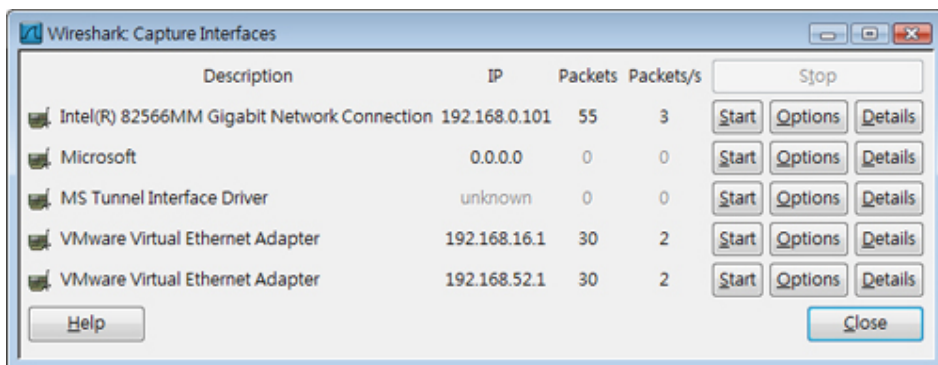
另外，在網路封包清單中，可以針對不同的網路通訊協定或過濾規則指定顏色，這種設計方式可以協助使用者快速辨識各種不同通訊協定，或是過濾規則符合目前網路流量的情況，能夠更直覺地進行後續處理。



▲ Wireshark的使用者介面

啟動Wireshark程式之後，將會自動載入通訊協定的解碼以及偵測目前系統上的網路介面。以目前Wireshark的版本而言，能夠辨識相當多的網路介面裝置，除了實體的網路介面卡之外，虛擬機器 (Virtual Machine) 所使用的虛擬網卡大多也能夠辨識，因此從系統上同時針對虛擬機器中的作業系統來分析網路通訊協定相當容易。在網路介面卡清單中，可以瀏覽即時的網路狀態，例如目前進入該網路介面的封包數和每秒的封包量。

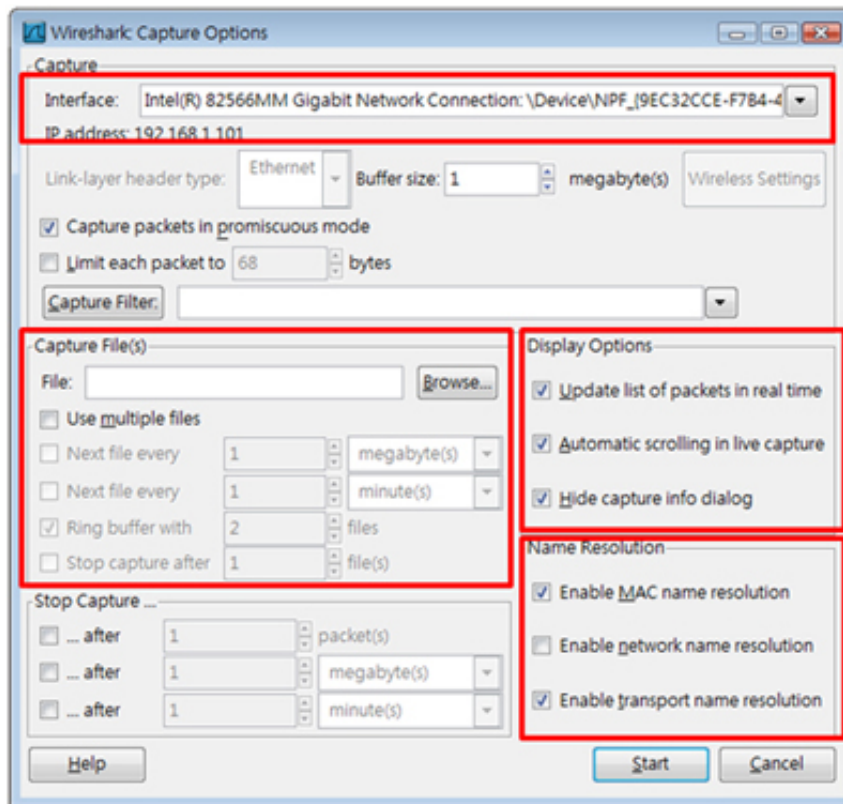
Wireshark另外也提供了三個控制按鈕，可以針對後續的處理程序進行控制，如果想要進一步的瞭解網路介面卡的細部資訊，按下〔Details〕按鈕即可查看。如果在準備擷取網路封包之前，想要設定擷取網路封包時的處理機制或是套用的過濾條件，可以按下〔Options〕按鈕進行修改。



▲ 網路介面卡清單與控制按鈕

在選項設定畫面中可以選擇準備擷取的網路介面卡，透過下拉式選單就能夠輕易地找到想要擷取的網路介面卡。在預設的情況下，Wireshark會將

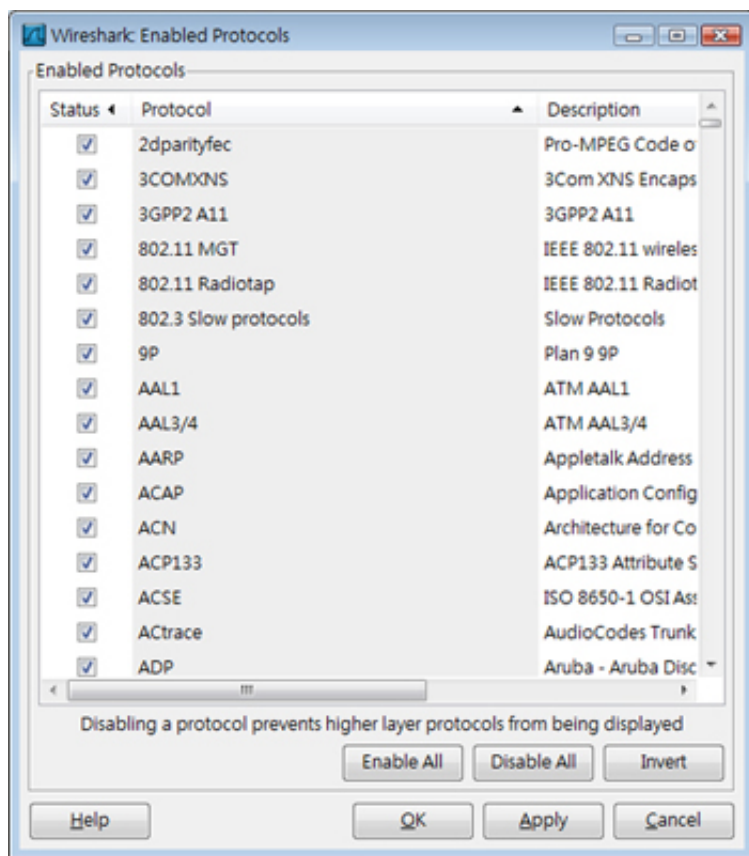
擷取到的網路封包儲存在記憶體中，不過這樣的方式不適用在長時間的網路封包收集上，因此如果想要進行長時間的網路封包收集，可以指定儲存的檔案名稱，以及是否要分割成多個檔案，並且可以指定分割檔案的規則等。另外，針對擷取網路封包時的畫面處理方式，建議在此勾選自動捲動（Automatic scrolling in live capture）功能，如此一來在主畫面上就能夠自動地捲動網路封包清單的捲軸，可以直接觀察到最新的網路封包資料。最後，在名稱的反解上，可以選擇是否啟動MAC Name、Network Name和Transport Name的解析，這個項目依據實際的需求來決定即可。



▲ 擷取網路封包的選項

此外，針對網路封包所使用的通訊協定，Wireshark在預設的情況下會啟用所有能夠辨識的通訊協定，不過使用者仍然可以自行選擇想要比對的通訊協定種類。

如果確定某些通訊協定並不存在於收集網路封包的環境中，則可以停用這些通訊協定，這在較繁忙的網路環境中將能降低比對的協定種類與數量，也可以避免因為硬體效能的問題而遺失原本打算擷取的網路封包。通訊協定清單中提供詳細的描述，可以做為是否啟用這些通訊協定的參考。

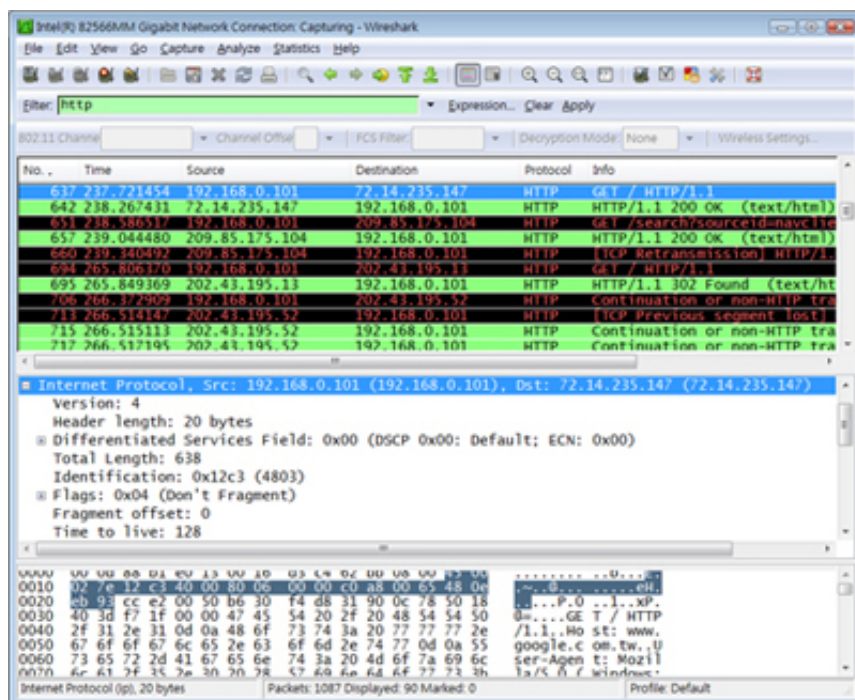


▲ 啟用的通訊協定

以Wireshark的操作介面配合滑鼠右鍵的快速功能表選單，就能夠輕易地過濾或追蹤所指定網路封包或特定的通訊協定，這對使用者而言是相當方便的設計。

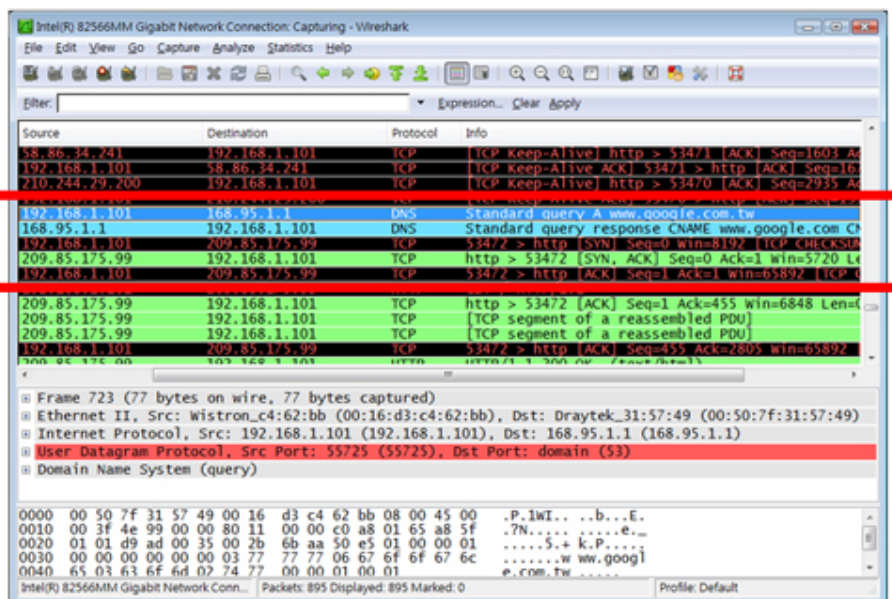
Wireshark的主要功能

Wireshark提供了圖形化的操作介面和功能完整的過濾器，提供使用者相當友善的操作方式，能夠快速地找到想要分析的網路封包。透過其內建的通訊協定解析功能，使用者可以掌握每一個網路封包的詳細資訊，除了能夠瞭解封包所傳送的内容之外，也可以學習各種通訊協定的行為模式。



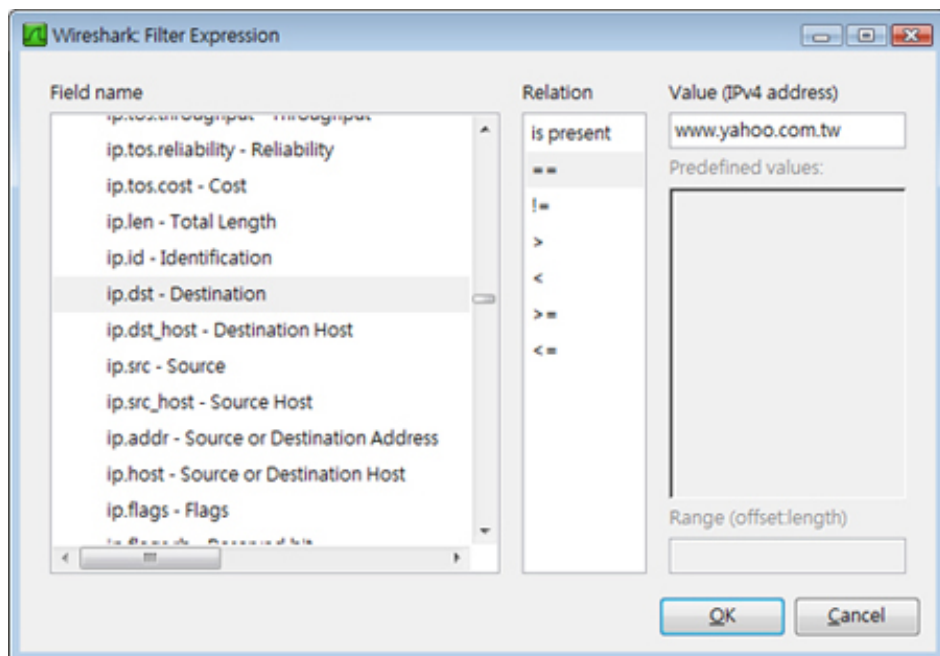
▲使用過濾條件 (http)

前面介紹了HTTP建立連線的過程，在輸入想要開啟的網址時，必須先透過DNS伺服器進行名稱的解析。藉由Wireshark所擷取到的網路封包，很容易觀察到這個現象，以驗證整個行為的模式是否符合預期。



▲DNS與TCP的三向交握

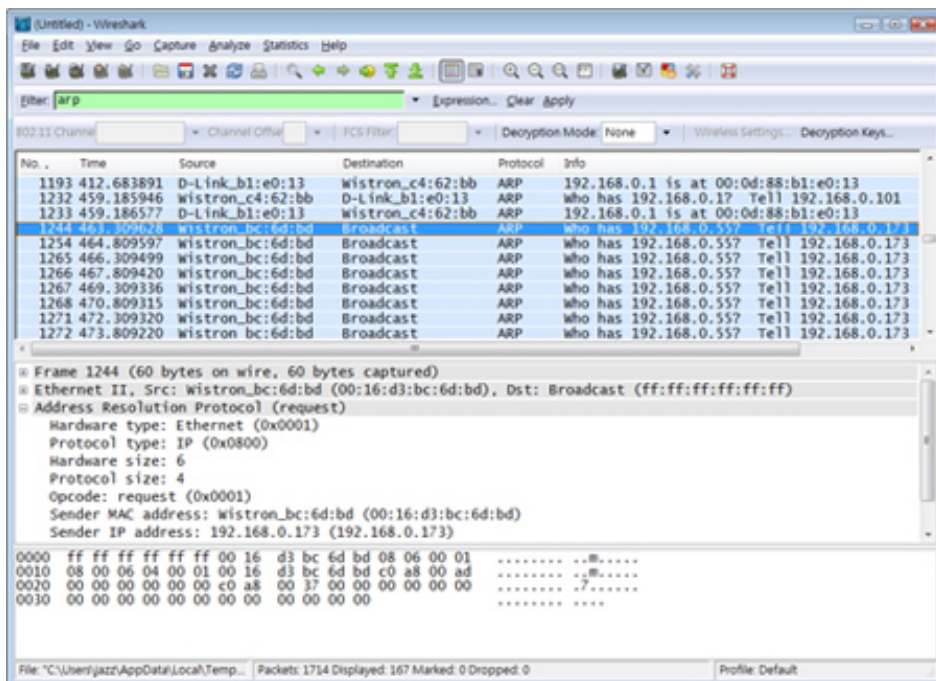
Wireshark具備功能十分完整的過濾器 (Filter)，使用者可以輸入關鍵字或條件，協助鎖定分析目標。在條件輸入的欄位內，如果使用的語法正確，底色將會變成綠色，反之，則會出現紅色底色，提醒使用者必須確認所輸入的過濾條件以及語法是否有誤。



▲ Wireshark具備功能完整的過濾器 (Filter)

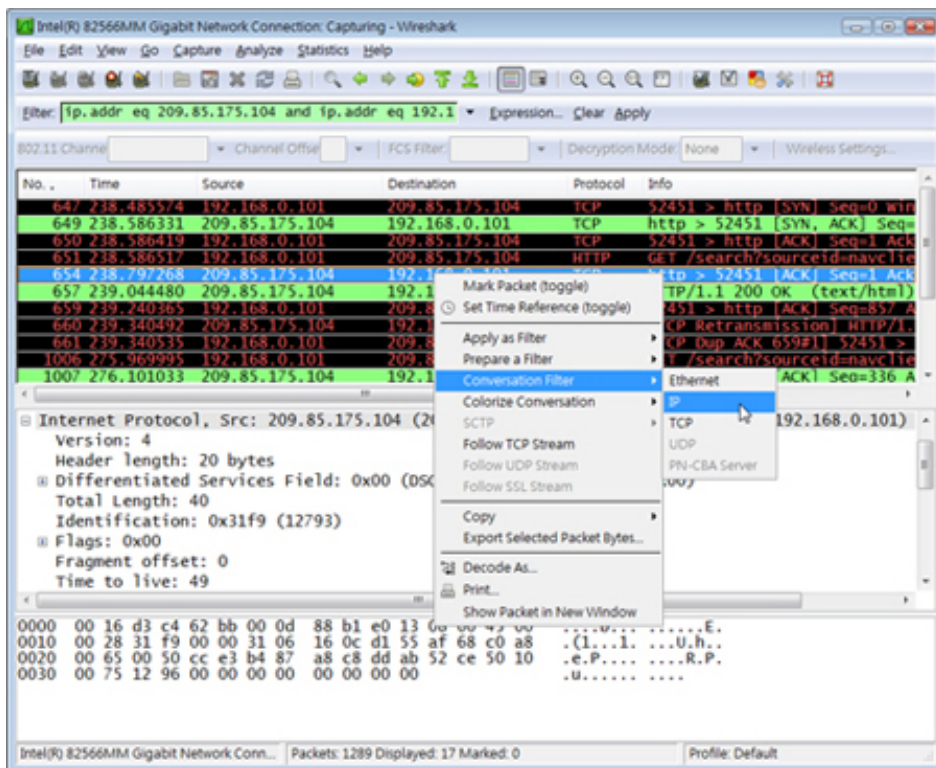
ARP是區域網路中常見的通訊協定，主要是用來查詢網路介面卡的實體位址。在區域網路中擷取封包時，若配合「arp」當作過濾的條件，將會發現如下圖的畫面，在這裡可以發現許多廣播封包正詢問區域網路中是否存在這些電腦。

在正常情況下，如果在區域網路內收到這類型的網路封包已連上網路的主機將會進行回應，因為經常會看到一些閘道器 (Gateway) 或路由器 (Router) 發送出來的詢問封包，而這些封包正在找尋該網段中電腦或設備所使用的MAC位址。若配合過濾器，則必須輸入「arp」以作為過濾的條件，這樣可以很容易地將焦點聚集在ARP這個通訊協定上。



▲ARP通訊協定

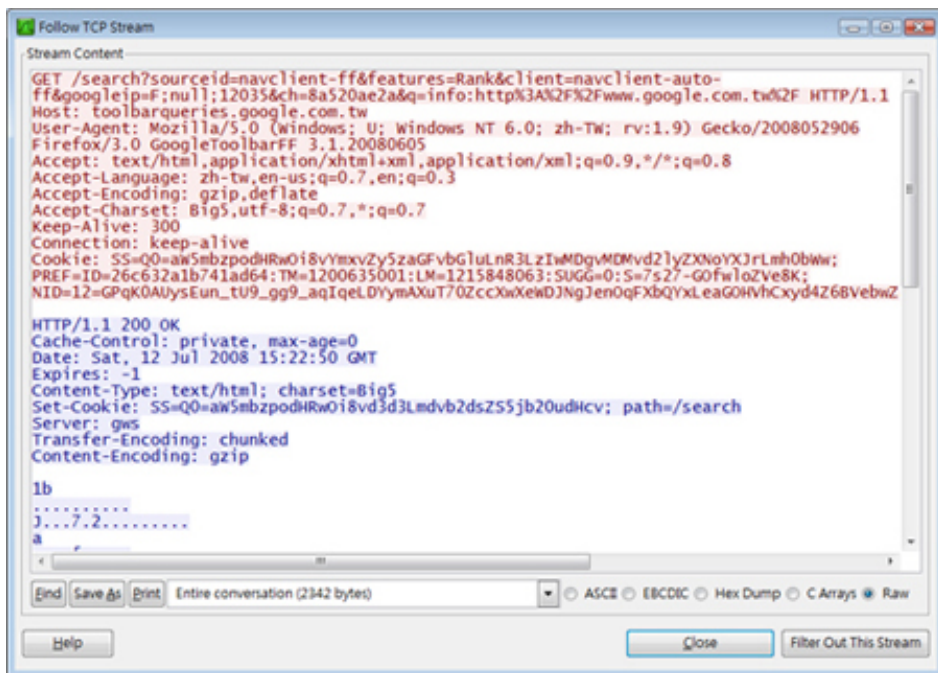
當發現有興趣進一步分析的網路封包，在點選該網路封包後，就可以透過滑鼠右鍵的功能表選單，直接指定交談時的過濾器，這樣就能夠很快地產生過濾條件，並且自動填入過濾規則的欄位中。



▲轉換過濾器的條件

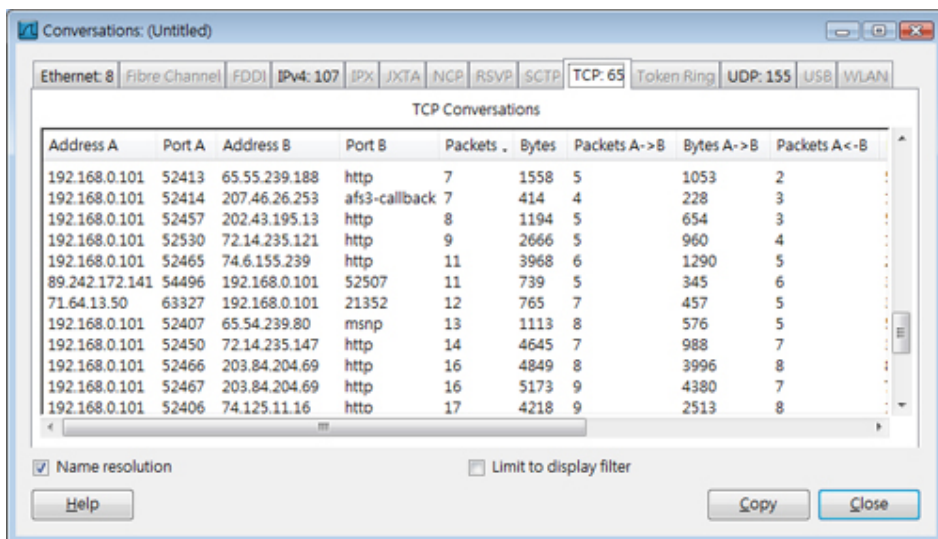
Wireshark針對通訊協定提供了完整的Follow TCP/UDP Stream功能，

能夠依序追蹤網路封包所傳送的内容，此種方式可以將有關聯性的網路封包一起呈現，如此在進行網路行為或通訊協定的行為分析時，將更為清楚易讀。



▲ Follow TCP Stream功能

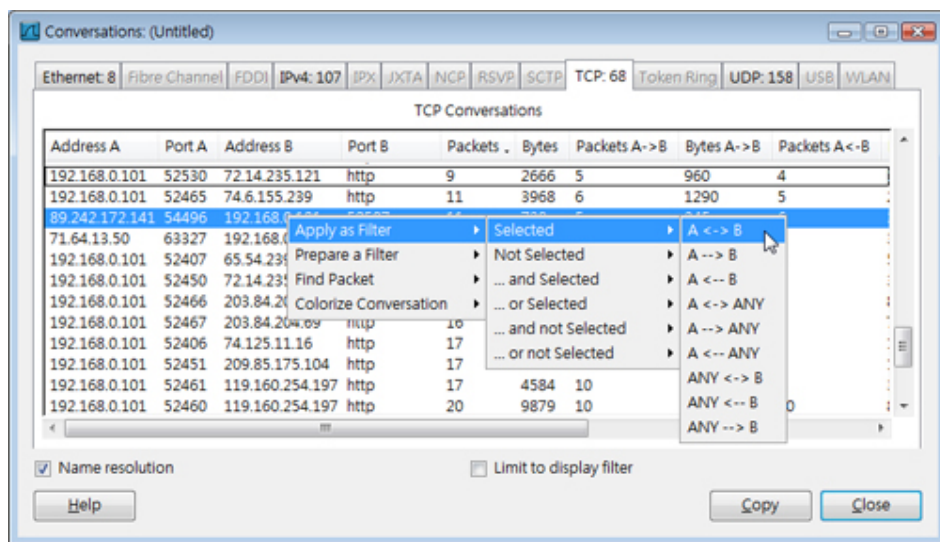
針對已收集到的網路封包，可以進一步針對來源和目的地地址進行交談行為的分析，透過清單的方式，很快地就會知道那些IP之間的通訊，以及所使用的通訊協定為何，在這個統計的分析中，仍然可以得知封包的數量、每秒的封包量以及封包的大小等等。



▲ 交談的統計

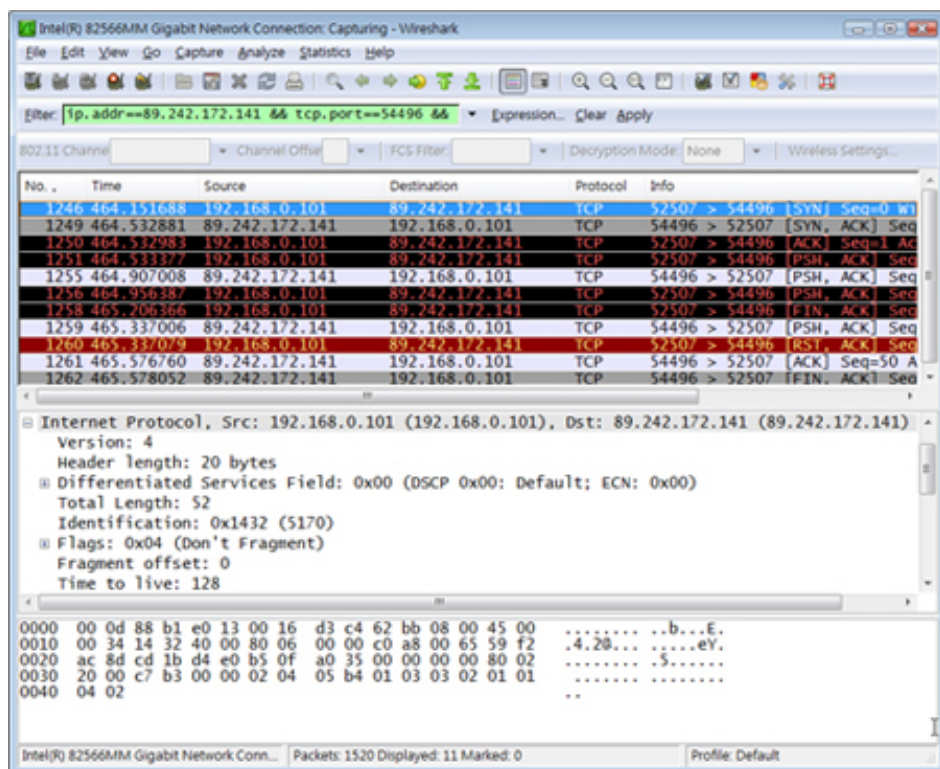
在統計分析的畫面，同樣可以快速地製作出過濾的規則。在指定的項目

上，透過滑鼠右鍵的功能表選單，直接指定【Apply as Filter】，並且選擇想要分析的流量。指定時必須仔細思考要觀察與不需要觀察的項目有那些，如此過濾規則時，可成為參考的依據。



▲ 建立過濾規則

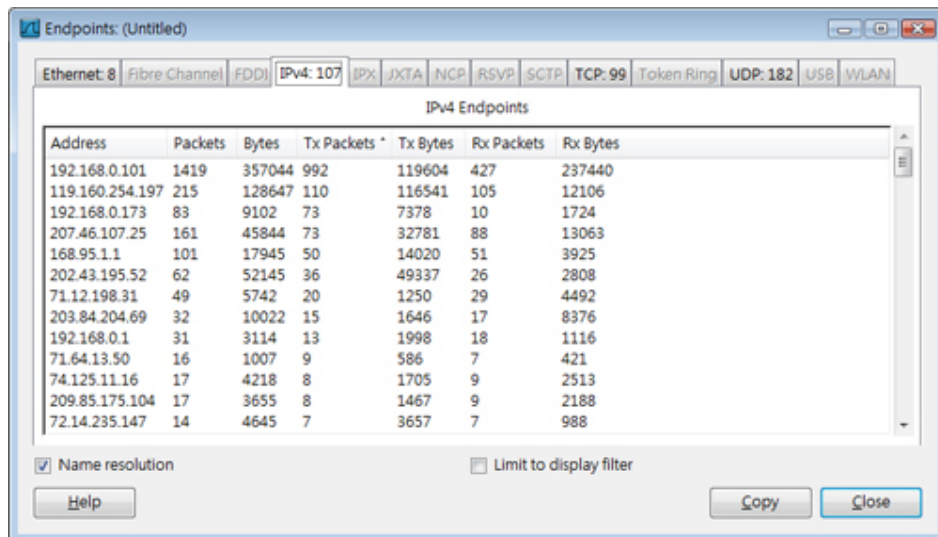
當完成過濾規則之後，將會自動將產生好的過濾條件，直接填入過濾器的欄位中，不論是正在收集或是單純想要分析以往收集的資料，都能夠透過這樣的方式分析網路封包。



▲ 自動產生過濾規則

Endpoint的統計畫面會統計目前收集到的封包，主要分成

「Ethernet」、「Fiber Channel」、「FDDI」、「IPv4」、「IPX」、「JXTA」、「NCP」、「RSVP」、「SCTP」、「TCP」、「Token Ring」、「UDP」、「USB」和「WLAN」進行統計與分析。每一個項目都將終端的主機詳列成清單，並且統計各個主機所傳送的網路封包數量與大小。



The screenshot shows the 'Endpoints: (Untitled)' window in Wireshark. The 'IPv4: 107' tab is selected, displaying a table of IPv4 endpoints. The table has columns for Address, Packets, Bytes, Tx Packets, Tx Bytes, Rx Packets, and Rx Bytes. Below the table, there are checkboxes for 'Name resolution' (checked) and 'Limit to display filter' (unchecked), along with 'Help', 'Copy', and 'Close' buttons.

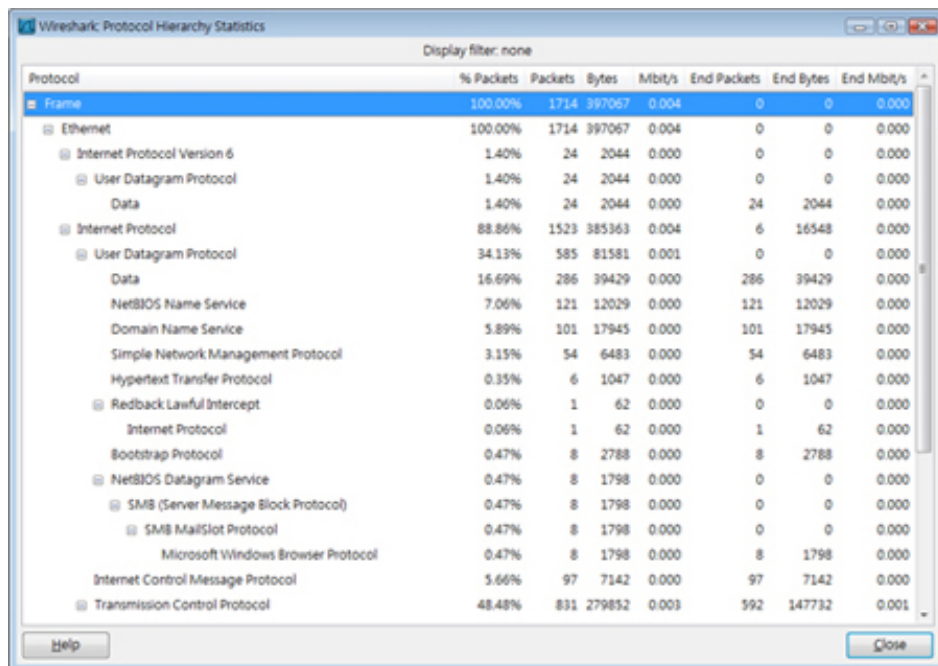
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
192.168.0.101	1419	357044	992	119604	427	237440
119.160.254.197	215	128647	110	116541	105	12106
192.168.0.173	83	9102	73	7378	10	1724
207.46.107.25	161	45844	73	32781	88	13063
168.95.1.1	101	17945	50	14020	51	3925
202.43.195.52	62	52145	36	49337	26	2808
71.12.198.31	49	5742	20	1250	29	4492
203.84.204.69	32	10022	15	1646	17	8376
192.168.0.1	31	3114	13	1998	18	1116
71.64.13.50	16	1007	9	586	7	421
74.125.11.16	17	4218	8	1705	9	2513
209.85.175.104	17	3655	8	1467	9	2188
72.14.235.147	14	4645	7	3657	7	988

▲ Endpoint的統計畫面

統計的資料可以事後分析，也可以即時分析，因此想要瞭解目前網路上的使用情況，透過統計分析的功能，就能夠更清楚掌握網路的現況。對於所收集到的網路封包，可以針對主機或是通訊協定進行分析，也可以選擇特定主機流入或流出的網路封包進行分析。當然，也可以依據通訊的雙方進行分析，不同的條件都可以在Wireshark中統計與分析，以提供不同的資訊給使用者。

Wireshark的應用

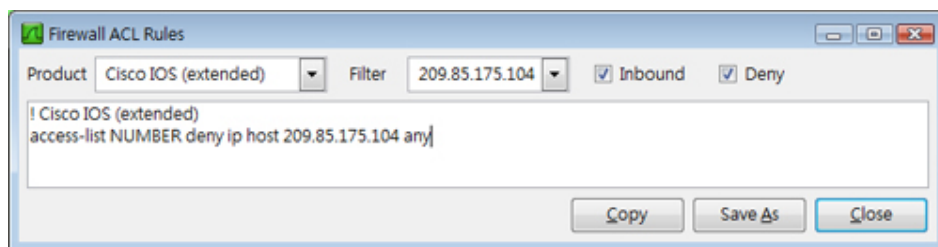
Wireshark提供完的網路協定分析功能，透過各種統計分析能夠掌握目前網路的狀態，目前支援相當多種不同層級的統計與分析方式，可以統計每一種通訊協定在整個收集網路封包的過程中，佔有多少的比例、封包的總量、封包大小的總和，以及每一秒送了多少Mbit的資料等，這些數據讓使用者能夠輕易地掌握目前網路的現況。



Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	1714	397067	0.004	0	0	0.000
Ethernet	100.00%	1714	397067	0.004	0	0	0.000
Internet Protocol Version 6	1.40%	24	2044	0.000	0	0	0.000
User Datagram Protocol	1.40%	24	2044	0.000	0	0	0.000
Data	1.40%	24	2044	0.000	24	2044	0.000
Internet Protocol	88.86%	1523	385363	0.004	6	16548	0.000
User Datagram Protocol	34.13%	585	81581	0.001	0	0	0.000
Data	16.69%	286	39429	0.000	286	39429	0.000
NetBIOS Name Service	7.06%	121	12029	0.000	121	12029	0.000
Domain Name Service	5.89%	101	17945	0.000	101	17945	0.000
Simple Network Management Protocol	3.15%	54	6483	0.000	54	6483	0.000
Hypertext Transfer Protocol	0.35%	6	1047	0.000	6	1047	0.000
Redback Lawful Intercept	0.06%	1	62	0.000	0	0	0.000
Internet Protocol	0.06%	1	62	0.000	1	62	0.000
Bootstrap Protocol	0.47%	8	2788	0.000	8	2788	0.000
NetBIOS Datagram Service	0.47%	8	1798	0.000	0	0	0.000
SMB (Server Message Block Protocol)	0.47%	8	1798	0.000	0	0	0.000
SMB MailSlot Protocol	0.47%	8	1798	0.000	0	0	0.000
Microsoft Windows Browser Protocol	0.47%	8	1798	0.000	8	1798	0.000
Internet Control Message Protocol	5.66%	97	7142	0.000	97	7142	0.000
Transmission Control Protocol	48.48%	831	279852	0.003	592	147732	0.001

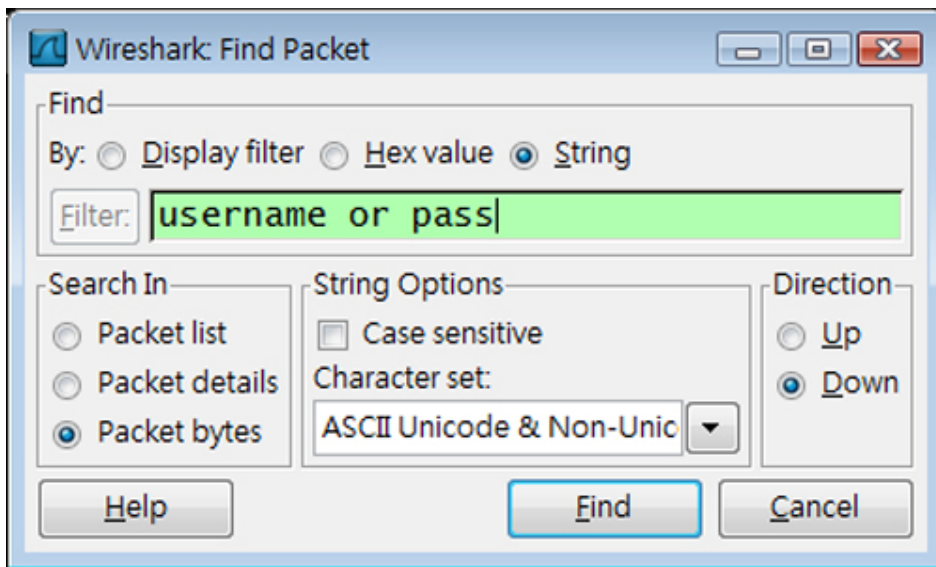
▲ 通訊協定的統計

Wireshark還提供了一項相當貼心的設計，針對目前所收集到網路封包，可以任意指定一個想要納入防火牆管理的網路封包，直接產生出不同平台使用的安全規則，這對於管理防火牆的工程師而言是相當好用的工具，因為能夠依據所產生好的安全規則直接組態設定到設備上，縮短相當多的處理時效。先指定好設備的廠牌後，就可以依據Filter的內容，配合所指定的處理方式，轉換成設備組態所需要的安全規則，使用上相當方便。



▲ 直接產生不同平台使用的安全規則

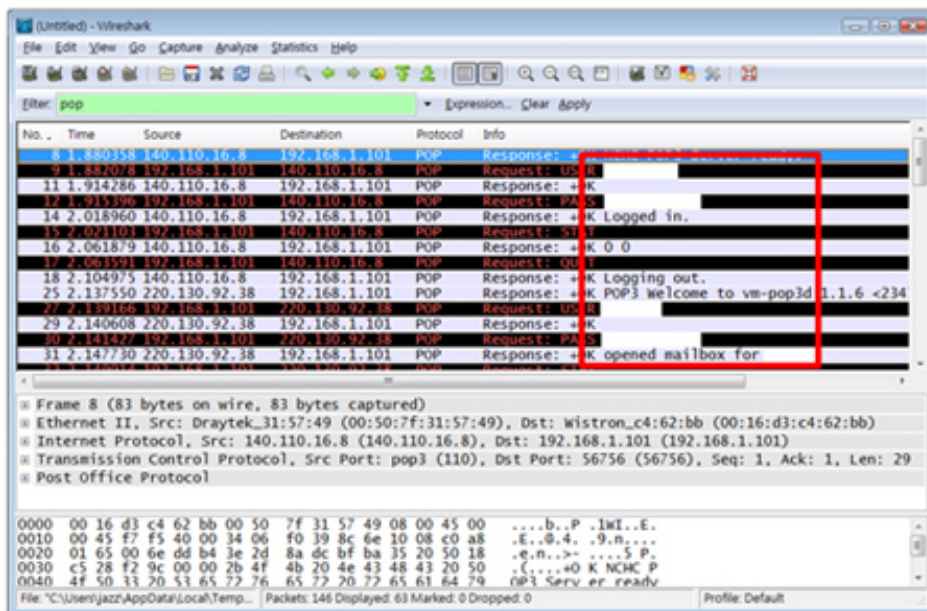
如果想要在網路封包中找尋特定的字串，可以利用Wireshark所提供的搜尋封包功能，開啟「Edit/Find Packet」功能之後，可以發現這裡提供了三種不同的模式：「Display filter」、「Hex value」以及在找尋字串時所要使用「String」模式。接著，輸入想要找尋的字串即可，例如username或pass等，這些必須是明文的字串才行，一般而言可以針對所傳送的參數進行搜尋。



▲ 尋找特定的字串

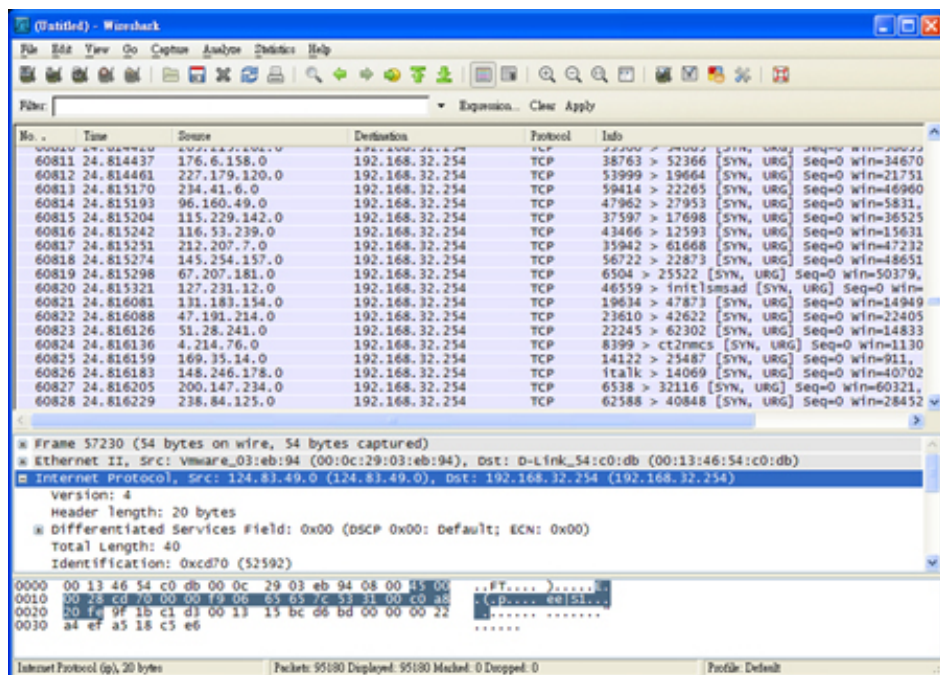
一些不安全的通訊協定（如POP），在使用者端的郵件軟體向郵件伺服器進行收信的動作時，會將使用者帳號與密碼以明文的方式進行傳送，此時如果透過Wireshark進行分析時，將會發現使用者的帳號與密碼資料，因而造成機敏資料外洩的問題。

在網路攻擊或異常流量的偵測上，以DDoS攻擊對於網路流量的影響最大。在極短的時間內會收集到相當多的封包，進而影響到網路的頻寬和伺服器本身的效能，例如遭受到大量的UDP網路封包攻擊時，透過網路封包的分析，就能夠得知許多假冒來源IP位址的網路封包正針對特定的目標傳送大量的UDP網路封包。



▲ 不安全的通訊協定（POP）

如果攻擊的方式是使用TCP進行，則可以看到三向交握的第一個SYN網路封包，這樣的攻擊模式會造成受到攻擊的主機必須耗費相當多的系統資源，等待遠端的電腦回應SYN/ACK的網路封包。當資源耗盡時，受攻擊的主機就無法再提供網路服務。這樣的攻擊行為同樣可以透過Wireshark所擷取到的網路封包進行分析，進而掌握攻擊者的攻擊方式。



▲ 遭受DDoS攻擊時的網路封包現象 (TCP)

Wireshark面對大量的攻擊封包時，有可能會因為系統效能不彰而影響到所收集到的網路封包，此時增加記憶體容量、使用Gigabit以上的網路介面卡或是更高速的中央處理器，就能夠改善這個問題。