網路流量的錄製與重播

陳玟瑾 鄭宗寰 呂俊男 林盈達
交通大學 資訊工程系
{wenchin, raijin, cnlu, ydlin}@cs.nctu.edu.tw
October 20, 2008

摘要

評估網路設備的效能常需要利用流量錄製工具將真實的網路流量擷取下來，再用流量重播工具播放至網路設備上。本篇文章針對六種常使用的流量錄製工具以及四種流量重播工具進行功能上評比及討論；在錄製工具方面針對封包遺失率、功能完整性與統計分析這三大方面進行比較，Tcpdump 無法在時間單位裡將極大量的流量錄製下來，因此會造成封包的遺失，而這六種工具都具備了錄製、分析與統計資訊的功能，不過在統計分析方面，Sniffer、Observer 與 Omnipeek 由於本身為商業軟體，因此提供較豐富的分析流量資訊，所以略勝一籌。

在重播工具方面則是針對功能完整性、網路分邊方式與其狀態性三大方面進行比較，這四種重播工具都具備了重播流量的功能，除了 Packet Player 只使用到一張網路介面卡來進行重播的行為而無網路分邊之問題，Tcpreplay 可依據 Bridge、Router、Client 或 Server 方式將封包分成傳送方與接收方，其餘皆為根據原本錄製時送方與收方的分邊方式來進行重播。而狀態性則是觀察重播工具在進行流量的重播時，流量是否會因為網路的狀況而有所改變。

本文所提及的錄製工具與重播工具都各自有讓大眾廣泛使用的特色，經過評比後，Wireshark 操作簡單，容易上手的特性在錄製流量佔有一席之地，而 Tcpreplay 則是提供大量的功能指令讓使用者能依其所需靈活運用，在重播流量相對重要。

關鍵字：錄製、重播、真實流量

---

1 引言

在網際網路的環境中，通常會面臨到許多的網路威脅，例如網路病毒、駭客攻擊、色情網頁、垃圾郵件等，此時就需要相關網路防護裝置如入侵偵測系統 (Intrusion Detection System，IDS) [1]或入侵防禦系統 (Intrusion Prevention System，IPS) [2]來保護自己不被網路的有害物質感染。而為了評估這些網路防護裝置的效能優劣，我們需要一些供測試的網路流量，並將測試流量打在網路防護裝置上，如此一來便能得知網路防護裝置在碰到實際用途中會遇到的真實情況時是否會有預期的反應發生。

得到網路流量有很多種方法，通常會使用一些重製流量的工具將網路流

量重新製造，但可能無法重製出末端使用者曾經遇到的網路問題，而重製出來的網路流量也不夠貼近網路中真正存在的流量。為了提升網路防護裝置的可靠度與對於網路有害物質的防禦能力，我們必須先將真實情況中的網路流量用相關的流量截取工具錄製下來，得到大量且網路行為多樣化的真實流量後，再使用相關的流量播放工具播放到網路防護裝置上，如此一來，便可讓網路防護裝置彷彿置身於實際用途中真實的環境，進而達到仿真的目的。

2 錄製工具

為了取得真實的流量資料，我們將真實的流量用相關的工具錄製下來，許多相關的工具便應運而生。這些錄製工具設計上的考量在於開發環境的支援程度、統計分析功能的完善程度、是否有額外附加功能、所支援檔案格式等。開發環境能支援不同的作業系統，對使用者來說，方便性相對地提升不少，不需要因為操作的系統不同而得再去熟悉另一套工具，也不必因為開發環境的限制而有所顧忌；統計分析功能能讓使用者能迅速的了解當前網路設備的使用情形，如最常連絡的 IP 位址或是網路協定的使用分佈等，因此若某工具提供大量的統計分析功能，便可讓使用者透過不同的統計分析而交叉了解目前的網路使用狀況；額外附加功能對於商業軟體來說是主要的賣點，若能提供別的工具所沒有的功能，那麼便成了這個工具的特色；而支援的檔案格式則意味著相容的能力，如 *Wireshark[4]*標榜可以支援十餘種其他錄製工具的檔案格式，這便表示了 *Wireshark* 的相容程度很高。表一整理出六種錄製工具的基本功能：

表一 錄製工具的基本功能

Capture Tools		Tcpdump	Wireshark	Packetyzer	Sniffer Pro	Network Instruments Observer	OmniPeek
Environment	Linux	O	O	×	×	×	×
	Windows	O	O	O	O	O	O
License Type		Freeware	Freeware	Freeware	Demo ver.	Demo ver.	Demo ver.
Size		680KB	68.6MB	43.79MB	70.7MB	87.59MB	82.68MB
File Format		*.pcap, *.cap	*.pcap, *.cap, *.enc, *.trc, *.fdc, *.syc, *.bfr	Cannot save	*.cap, *.enc, *.trc, *.fdc, *.syc	*.bfr, *.cap, *.enc	*.pkt
Library		Libpcap	Winpcap, Libpcap	Libpcap	Not Found	Not Found	Not Found
Network Interface	Ethernet	O	O	O	O	O	O
	Wireless 802.11	×	a/b/g	a/b/g	a/b/g	a/b/g	a/b/g/n
	Bluetooth	×	O	×	×	O	×
	VoIP	×	×	×	×	×	O
Filter		O	O	O	O	O	O
Statistical Analysis	Decode	O	O	O	O	O	O
	Summary	O	O	O	O	O	O
	Protocol distribution	×	O	O	O	O	O
	Matrix	×	×	×	O	O	×
	Host table	×	×	×	O	×	×
	Top talkers	×	×	×	O	O	O
	Peer map	×	×	×	×	×	O
	Packet size distribution	×	×	×	×	×	O

在開發環境方面，*Tcpdump[3]*與 *Wireshark* 這兩個免費工具的移植性很高，支援許多的作業系統，讓使用者使用的彈性很大，不必因為環境平台不同而得使用不同工具。*Tcpdump* 主要運行於 Linux 環境，Windows 下的版本則為 *Windump[5]* ，而兩者皆為文字介面工具，皆須要以指令的下達來使其執行運作；而 *Wireshark* 以 Windows 為主要執行環境，在 Linux 下也有圖形介面可以使用。

在安裝時所占空間方面，由於 *Tcpdump* 藉著在終端機裡下達指令而有所動作，並無 GUI 圖形介面，因此並不占太大的硬碟空間，而 *Packetyzer[6]*則由於比 *Wireshark* 所支援的功能少，因此占硬碟空間也相對地小，其他 *Sniffer[7]*、*Observer[8]*、*OmniPeek[9]*商業軟體，都提供很多功能，因此占硬碟空間相當大。在支援的網路介面方面，大部份的工具都可以支援 802.11a/b/g 無線網路，除了 *Tcpdump* 並不支援，而 *OmniPeek* 則更可以支援到 802.11n，這是其中比較特別的地方。

在統計分析方面，錄製工具主要是將網路封包擷取下來並進行解碼，將封包內容解譯為有意義的資訊，在詳細資料窗格裡階層式地顯示某一封包裡各欄位的內容，並註明所代表的意義，讓使用者能夠直接看出此封包的功能和特性，因此在封包解碼方面是必備的。而 *Tcpdump* 本身是個簡易的工具，因此除了計算封包總數之外，並不支援其他統計封包資訊的功能。*Wireshark* 與 *Packetyzer* 為免費工具，開發的主要目的只是錄製與分析封包，因此只提供簡單的統計資訊。

而商業工具，主要是以「監控」為主要目的，「監控」指的是即時的監視與控管網路狀況，將網路流量依平時的封包流量與使用頻寬動態地建立安全流量等級，當封包流量不大於正常等級的 25 %時為安全狀態，一旦監測到網路上的封包大過於正常等級的 25 %時，便立即進入警戒狀態，同時立即會對網管人員發出可能遭受攻擊的警告訊息，此時網管人員便得以根據此訊息的內容來採取適度的應對措施。25%的預設警戒標準並非一成不變，網管人員可以依據網路流量的相關統計量來作適度的調整。如此便能有效的防止攻擊的發生，或降低傷害的程度，同時又兼顧系統使用的功能性。因此若能經由許多統計分析結果而讓使用者及時的發現發生問題的所在點，便成了商業工具的主要賣點。*Sniffer*、*Observer*、*OmniPeek* 提供非常多的統計分析方式，讓使用者能夠快速了解目前網路的使用狀況。表二整理出六種錄製工具附加的額外功能：

表二 錄製工具的額外功能

Capture Tools	Tcpdump	Wireshark	Packetyzer	Sniffer Pro	Observer	OmniPeek
Packet Geographic Location	×	×	×	×	×	○ (Install Google Map Plug-in)
Pick Packet to Save	×	×	○	○	○	○
Triggers and Alarms	×	×	×	○	○	○
Remote Engine Connections	×	×	×	×	×	○
Output Exported	None	XML, CSV, Plain text	None	XML, CSV	Plain text	None

額外附加功能對於錄製工具來說並不是必需，但有些工具有提供，便成為該產品的重要賣點。其中比較特別的是 Triggers and Alarms 功能，*Sniffer*、*Observer*、*OmniPeek* 三者以監控為目的，因此在監控網路流量的期間裡，若網路流量出現異常，可能是發生流量過大，或是偵測到攻擊流量的情況，便會發出「alarm」通知網管人員，即時地維護網路的安全。其中 *OmniPeek* 是個功能很強大的商業軟體，它提供許多額外的功能：如果加裝 Google Map 外掛，便可以得知封包是從哪個真實的地點來，另外還有遠端監控的功能，管理人員可以在遠端監控所有的網路流量，只要在被監控的主機上安裝 *OmniEngines*，便能實現遠端監控的理想。

就功能多寡的層面來看，*OmniPeek* 等商業軟體的確具備大量的功能供企業體充分使用，但若只單純的想了解自家的網路狀況，或許可以考慮 *Tcpdump*、*Wireshark* 與 *Packetyzer*。*Tcpdump* 與 *Wireshark* 還提供 Linux 版本以及 Windows 版本供使用者自由選擇，使用彈性便大幅地提升。

3 重播工具

重播工具通常是用在網路防護裝置上。開發人員藉著觀察重播具有攻擊性的網路流量時，網路裝置是否有如預期的反應發生，藉此評估網路防護裝置否正常運作及其效能為何。重播工具設計的考量在於其重播行為與網路分邊的方式，該如何實現重播的行為，是以封包的時間順序還是依照 TCP 的連接導向機制？若是以封包的時間順序播放，將會順利的把流量播放完畢，但要是在重播的途中有一方失去連線能力，而無法將封包送出時，另一方並不會發現連線出現異狀，繼續將其剩餘的封包依序播完，這樣無法依照當時的網路連線狀況做出適當的反應能力，便失去了播放真實流量的目的。換句話說，若是在重播流量時依照連接導向機制進行重播，此時另一方收不到該有的回應封包，便可要求重新傳送或是停止重播等反應動作，如此一來，此重播行為便重現了真實的封包傳輸情形。

當我們欲在一台 Replay site 上重現真實的流量發送，就必須有兩張網路介面卡以比擬為 Server 與 Client。重播工具是依照何種分邊機制將一個有大量封包的流量檔案分別由兩張網路介面卡播送？若是以其送方與收方的 IP 位址為分邊考量，那麼含有大量來源端與目的端的封包該如何是好？或是以

橋接方式為分邊考量，便可將傳送 SYN 封包、要求 DNS[14]與收到 ICMP[15]封包之一方當作 Client 端，反之為 Server 端，如此便可明確的將所有的封包有規則地經由兩張網路接面卡進行播送，重現真實的流量。

其它關於是否提供封包改寫的功能、送出封包時是否會將 IP 位址改寫等，則也可加以評估是否要提供該功能。表三整理出四種重播工具的功能比較，而其重播行為與網路分邊方式則藉由觀察實驗得知。

表三 重播工具的基本功能

Replay Tools	Tcpreplay	Tomahawk	Packet Player	Traffic IQ Pro
Environment	Linux	Linux	Windows	Windows
License Type	Free, Open Source	Free, Open Source	Freeware	Demo ver.
Size	1.18MB	2.1MB	9.36MB	37.39MB
Library	Libpcap	LibNet, Libpcap	Not Found	Traffic library
File Type	*.pcap, *.cap	*.pcap, *.cap	*.cap, *.pkt	*.kar
Packet Rewrite	○	×	×	○
Loop Sending	○	○	○	×
Burst Mode	○	×	○	×
IP Rewrite	×	○	×	○
Reporting	×	×	×	○

這四種重播工具較特別的是，*Tcpreplay[10]*與 *Traffic IQ[13]*能夠改寫流量檔案中的封包，並藉由改寫封包來觀察測試裝置的識別封包能力與反應能力，若改寫了其中一個回應封包，測試裝置是否能夠識別出這個被改寫的封包不是個正常的回應封包，而做出該有的反應如要求重新傳送的能力。

Burst Mode 是指在播放整個流量時，將封包與封包中間的間隔時間趨近於零，讓每個封包在播放時是一個接一個地送出，沒有時間空隙，這是 *Packet Player[12]*的重點功能，但其實 *Tcpeplay* 也能以不同的指令參數來實現。

Tcpreplay 與 *Pcaket Player* 在送出封包時，不會將來源 IP 與目的 IP 改寫為實際送出與接收的 IP 位址，而 *Tomahawk[11]*與 *Traffic IQ* 則可以自由選擇是否要將封包的來源 IP 與目的 IP 改寫成實際送收封包雙方的位址，讓待測物所感受到的是實際的兩方在傳送資料而非只是重播而已，如此更像是置身於真實情況。

Traffic IQ 還內建報文功能，可瀏覽封包檔案的內容，讓使用者在重播時可清楚的了解播放封包的過程，送方與收方是否成功完成，或是在哪個地方被停住了。其他的播放工具只顯示播放結束等資訊，並無法瀏覽所有的封包內容。在此由於 *Traffic IQ* 使用的是試用版，因此檔案格式只支援本身所附的範例檔案*.kar，但正式版可以支援*.pcap 檔案。

四種工具所代表的訴求皆不相同，*Tcpreplay* 與 *Tomahawk* 不僅達到重播流量的目的，還具備其他的功能，如改變重播速度等。*Pcaket Player* 則是較簡單，操作方便，功能也不複雜，非常容易上手。*Traffic IQ* 為商業軟體，支援很多功能，但較適合企業體使用。

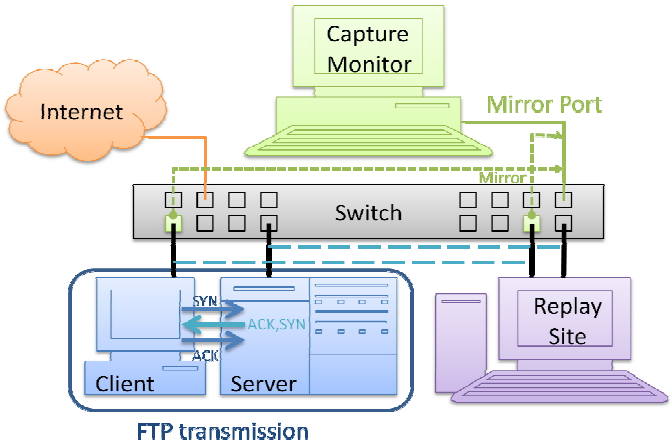
4 實驗觀察

前述提到了六種錄製工具以及四種重播工具之間功能的差異比較後，希望能藉由「觀察實驗」來觀察每一種工具其實際運作的方式。

需要的設備有桌上型主機*4 (Server、Client、Capture monitor、Replay site)、網路交換器 *1 (包含埠映射功能)、網路介面卡*5 (Replay site 搭配兩張網路介面卡，其餘皆搭配一張網路介面卡)

如圖一所示，利用 FTP 傳輸，當 Client 向 Server 取得資料時，將 Client 端的埠映射到 Capture monitor 上，從 Capture monitor 將所有經過 Client 的資料封包錄製下來，包括 Client 向 Server 取得資料的封包與 Server 回應給 Client 的封包，Capture monitor 便可觀察並分析所有封包的內容，主要是觀察在同樣的情況下所擷取到的封包數量有無異處、封包遺失的比率、儲存流量檔案的完整性等狀況。

重播時，將錄製好的流量檔案在 Replay site 進行重播，將 Replay site 的兩張網路介面卡一張視作 Server 端的網路介面，另一端則視作 Client 端的網路介面，模擬 Server 與 Client 在互相傳遞資料，並將重播的情形映射到 Capture monitor 上進行觀察，觀察各種重播工具是如何進行重播的行為、重播時是依照甚麼機制將封包檔案分別由不同網卡傳送等情形。



圖一 實驗環境

錄製流量結果分析

由於 *Observer* 與 *OmniPeek* 並無授權軟體可供使用，因此無法進行實驗分析。表四為 *Tcpdump*、*Wireshark*、*Packetyzer*、*Sniffer* 依照不同情況進行錄製後所得的封包數量。

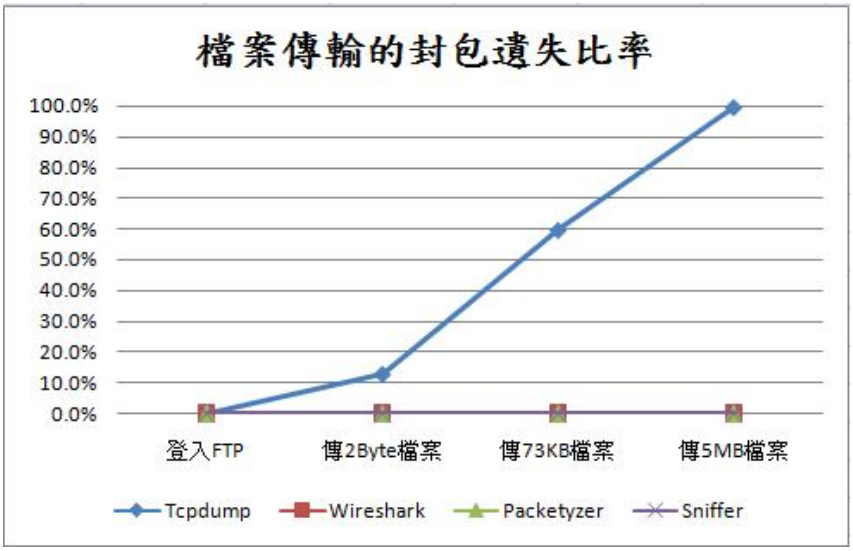
表四(a) 檔案傳輸時的封包數量

	Tcpdump	Wireshark	Packetyzer	Sniffer
登入 FTP	15	15	15	15
傳 2Byte 檔案	27	31	31	31
傳 73KB 檔案	27	227	227	227
傳 5MB 檔案	32	8842	8842	8842

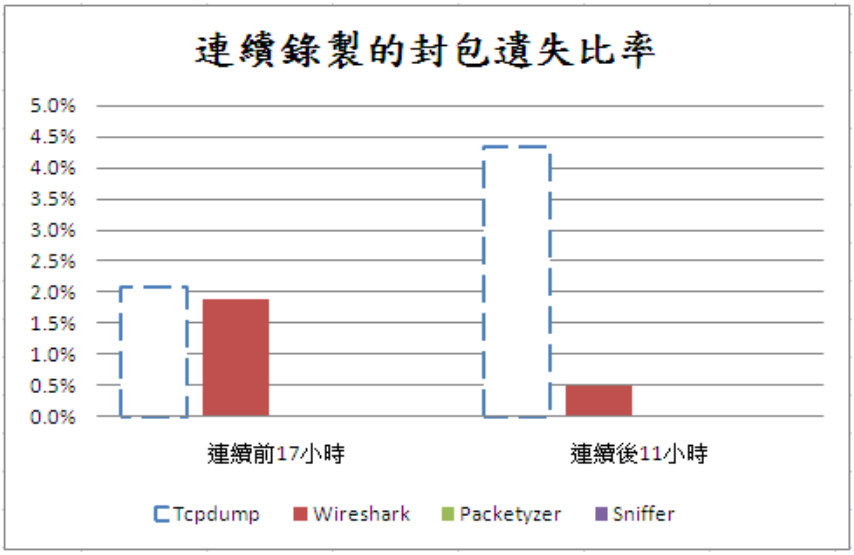
表四(b) 連續錄製時的封包數量

	Tcpdump	Wireshark	Packetyzer	Sniffer
24/24 小時	74770	75637	—	—
前 17/24 小時	53406	53479	54537	—
後 11/24 小時	34652	36020	—	36217

從封包數量我們可以計算其封包遺失率：遺失封包數/全部封包數。如圖二(a)所示，在短時間內傳送大量的封包 *Tcpdump* 無法擷取到全部的封包，因為在一個時間單位裡有太多的封包經過，讓 *Tcpdump* 反應不及而僅能擷取到部分的封包，而 *Wireshark*、*Packetyzer* 與 *Sniffer* 則能夠完整地擷取。如圖二(b)所示，Wireshark 在一段長時間的錄製下會有部分的封包遺失，而 *Packetyzer* 與 *Sniffer* 錄製的封包量較為完整，但 *Packetyzer* 在錄製時會限制流量的上限，因此若達到錄製的上限則 *Packetyzer* 會立即停止錄製，而測試時的流量上限為 1000 kilobyte，所以只錄到 17 小時的流量。而由於 *Sniffer* 用的是評估版，因此若錄製的流量超過某一上限則會將在一開始所錄製的封包刪去一些，保留空間錄製新的封包，所以就算流量容量有所限制，錄到的流量都還是最新的。



圖二(a)檔案傳輸時的封包遺失率



圖二(b)連續錄製時的封包遺失率

將封包擷取下來後，就要進行儲存的動作，而不同的錄製工具其錄製檔案的完整性為何？完整性是指儲存下來的部分封包佔整個封包的比例，如果是儲存整個封包，則是指完整性 100%，而這六種錄製工具其錄製檔案的完整性皆為 100%。表五列出了所有流量錄製工具在儲存封包時可選擇的條件：

表五 封包儲存選擇條件

	Tcpdump	Wireshark	Packetyzer	Sniffer	Observer	OmniPeek
全部	○	○	×	○	○	○
過濾結果	×	×	×	○	○	○
某一區間	×	×	×	×	○	○
隨意選擇	×	×	×	○	×	○

重播流量結果分析

Tcpreplay 的重播行為是依據流量檔案裡每個封包的時間戳記來播放，若是在重播的途中掉了封包或是另一方斷了連線，*Tcpreplay* 並不會發現，反而繼續將該播的封包依時間戳記全數播完。

Tomahawk 的重播行為根據 TCP 的三方交握，在途中若是發生另一方斷線，則 *Tomahawk* 在斷線前所送出去的封包便不會收到 ACK 的回應，此時 *Tomahawk* 便會自動重新傳送封包，重送的次數預設是 4 次，這個變數可利用-r 的指令更改。

Packet Player 的重播行為也是依照流量檔案裡每個封包的時間戳記來播放。而基本上他不會面臨另一方斷線的問題，由於 *Packet Player* 在播放的時候只以一張網卡來播放，因此是從一張網卡依錄製時的時間戳記一個

封包一個封包地播送至待測物上。

Traffic IQ 的重播行為跟 *Tomahawk* 很像，也是以 TCP 的三方交握為基礎，只是當另一方斷線時，*Traffic IQ* 偵測不到回應的封包時，他會馬上停止重播，並不會重送之前所送出去的封包。而比較不一樣的是，*Traffic IQ* 在播放時是把兩張網卡當作不同的兩台機器的介面來當作送方與收方。

在分邊方式方面，*Tcpreplay* 可以選擇要從一張網卡播放還是兩張，如果選擇的是一張網卡的話，那就沒有分邊的問題。但如果要選擇從兩張網卡播放的話，就必須先用 *Tcpreplay* 將原本的 pcap 檔依照指令內容 Auto/Bridge 或 Auto/Router 或 Auto/Client 或 Auto/Server 將封包分成傳送方與接收方。

Tomahawk 是用到兩張網卡來重播，而它分邊的依據是原本 pcap 檔的來源 IP 與目的 IP，而可以下指令-A 來決定是否重寫封包 IP，0 就是不改 IP 位址，1 則會將 IP 位址重寫。

重播時，*Packet Player* 只通過一張網卡，因此並無分邊的問題。

Traffic IQ 是用兩張網卡當作不同的兩台機器的介面進行重播，送方與收方分邊的依據也是依照流量檔案裡的來源 IP 與目的 IP，而 IP 位址的重寫則是可以在設定的畫面中進行設定。

5 結論

本篇文章整理出一些考量的條件，讓有不同需求的使用者可以很快速的選擇一個最適合的工具來使用。

實用性上的考量，以功能的實用程度為優先選擇基礎，空間與價格不列入考慮。以錄製工具而言，*OmniPeek* 提供了非常多其他工具所沒有的功能，而 *Sniffer* 是在統計分析封包資訊方面較為完善，*Observer* 則是附加的功能提供的較為多一些。若要長期錄製流量，由於使用的是評估版，因此 *Packetyzer* 與 *Sniffer* 無法長時間的錄製，錄到所限制的時間點時便會自行停止錄製流量，相較之下 *Tcpdump* 與 *Wireshark* 則較為適合用來長期錄製網路流量，雖然偶爾會漏掉一些廣播封包。以重播工具而言，*Traffic IQ* 不僅可以對封包進行改寫，還能瀏覽流量檔案的內容資訊，讓使用者對於重播的狀況能一目瞭然，重播時，以虛擬機器模擬送收雙方，讓待測設備彷彿置身於真實的環境中。*Tcpreplay* 安裝上較易完成，也較容易使用，但其重播是依照時間戳記來發送封包，而 *Tomahawk* 則必須自行編譯，對於新手來說較為困難，但重播時，若收不到對方回應即停止發送封包，對於達到仿真的目的，*Tomahawk* 較為符合。

金錢上的考量，主要是以免費工具為主要選擇基礎。以錄製工具而言，*Tcpdump*、*Wireshark* 與 *Packetyzer* 皆為免費工具，其中 *Wireshark* 與 *Packetyzer* 在 Windows 環境下，操作較容易上手，而且提供的分析資訊較 *Tcpdump* 多，而 *Packetyzer* 在錄製的效能上較 *Wireshark* 優異，在錄製一段

時間的流量時，*Wireshark* 會漏掉一些廣播封包，但比率不是很高。*Sniffer* 雖為商業工具，但其試用版提供了許多統計分析功能，在錄製一段時間的流量時，*Sniffer* 不會掉封包，但無法錄製超過 24 小時。以重播工具而言，*Tcpreplay*、*Tomahawk* 與 *Packet Player* 皆為免費工具，其中 *Tcpreplay* 較 *Tomahawk* 易於安裝，對於 Linux 系統的新手而言，*Tcpreplay* 是比較好的選擇。*Packet Player* 雖為 *Windows* 環境，但其操作畫面較簡單，只以重播流量為主要目的，功能提供便相對地較為不足。

空間上的考量，以安裝時所佔的硬碟空間為優先選擇基礎，其功能多寡則不列入考慮。以錄製工具而言，*Tcpdump* 為 Linux 下的文字模式工具，因此占硬碟空間相對小很多。而 *Wireshark* 與 *Sniffer* 則是有大量的 GUI 介面，較占硬碟空間。以重播工具而言，*Tcpreplay* 與 *Tomahawk* 皆為 Linux 下的文字模式工具，因此占硬碟空間相對小很多。而 *Packet Player* 則因有 GUI 介面，較占硬碟空間。

參考資源

[1] Paul Innella and Oba McMillan, “An Introduction to IDS”, http://www.securityfocus.com/infocus/1520

[2] Cyberoam, “Intrusion Prevention”, http://www.cyberoam.com/idp.html

[3] Tcpdump, http://www.tcpdump.org/

[4] Wireshark, http://www.wireshark.org/

[5] Windump, http://www.winpcap.org/windump/

[6] Packetyzer, http://sourceforge.net/projects/packetyzer/

[7] NAI Sniffer Pro, http://www.netscout.com/products/sniffer_global.asp

[8] Network Instruments Observer, http://www.netinst.com/products/observer/standard.html

[9] OmniPeek, http://www.wildpackets.com/products/omnipeek/professional_overview

[10] Tcpreplay, http://tcpreplay.synfin.net/trac/

[11] Tomahawk, http:// tomahawk.sourceforge.net/

[12] Colasoft Packet Player, http://www.sharewareplaza.com/Colasoft-Packet-Player-download_44632.html

[13] Traffic IQ, http://nsslabs.com/test-equipment/karalon-traffic-iq-pro.html

[14] DNS 線上教學研究計畫, http://dns-learning.twnic.net.tw/

[15] ICMP 協定, http://www.pcnet.idv.tw/pcnet/network/network_ip_icmp.htm

[16] Seung-Sun Hong1 and S. Felix Wu, “On Interactive Internet Traffic Replay”, *University of California, Davis CA 95616, USA, 2006*

[17] Marcos Paredes-Farrera, Martin Fleury and Mohammed Ghanbari, “Precision and Accuracy of Network Traffic Generators for Packet-by-Packet Traffic Analysis”,

2nd International IEEE TridentCom Conference, 2006
[18] Chi-Chung Luo, "Attack Session Extraction and Replay from Real Traffic", *College of Computer Science National Chiao Tung University,* 2005
[19] Olivier Bonaventure, "Software Tools for Networking", *IEEE Nerwork, Maylune 2004*.