P2P 軟體對網路安全的威脅與封包分析

新波科技
劉楨民
0932-212913, 02-2331-0789
電子郵件 dmliu@ms4.hinet.net

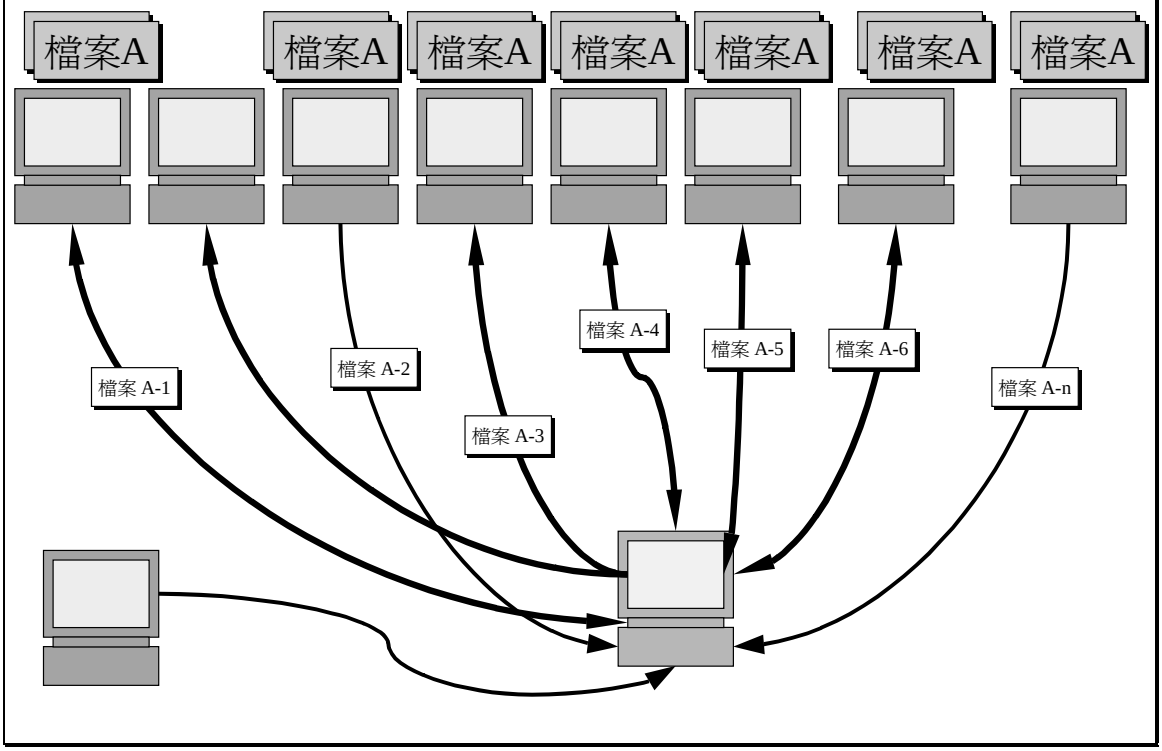
P2P 軟體對網路安全的威脅

- 甚麼是 P2P 軟體？
- P2P軟體的種類
- P2P 軟體可能影響網路安全的問題
- P2P 軟體誤用的漏洞範例
- 偵測 P2P 通訊的方式
- Q&A

甚麼是 P2P 軟體？

- P2P , Peer to Peer, 點對點通訊傳輸工具
- 傳統 HTTP/FTP 傳送檔案方式，採取用戶與主機的通訊模式(Client-Server Mode)
- 新制 P2P 檔案傳送，採取用戶與用戶的通訊模式，P2P傳送檔案的時候，可以同時連接多個下載點，分散式下載檔案。
- P2P可以快速完成檔案下載的目標。
- Skype也是P2P的一種應用工具。

Peer to Peer, 點對點通訊傳輸工具

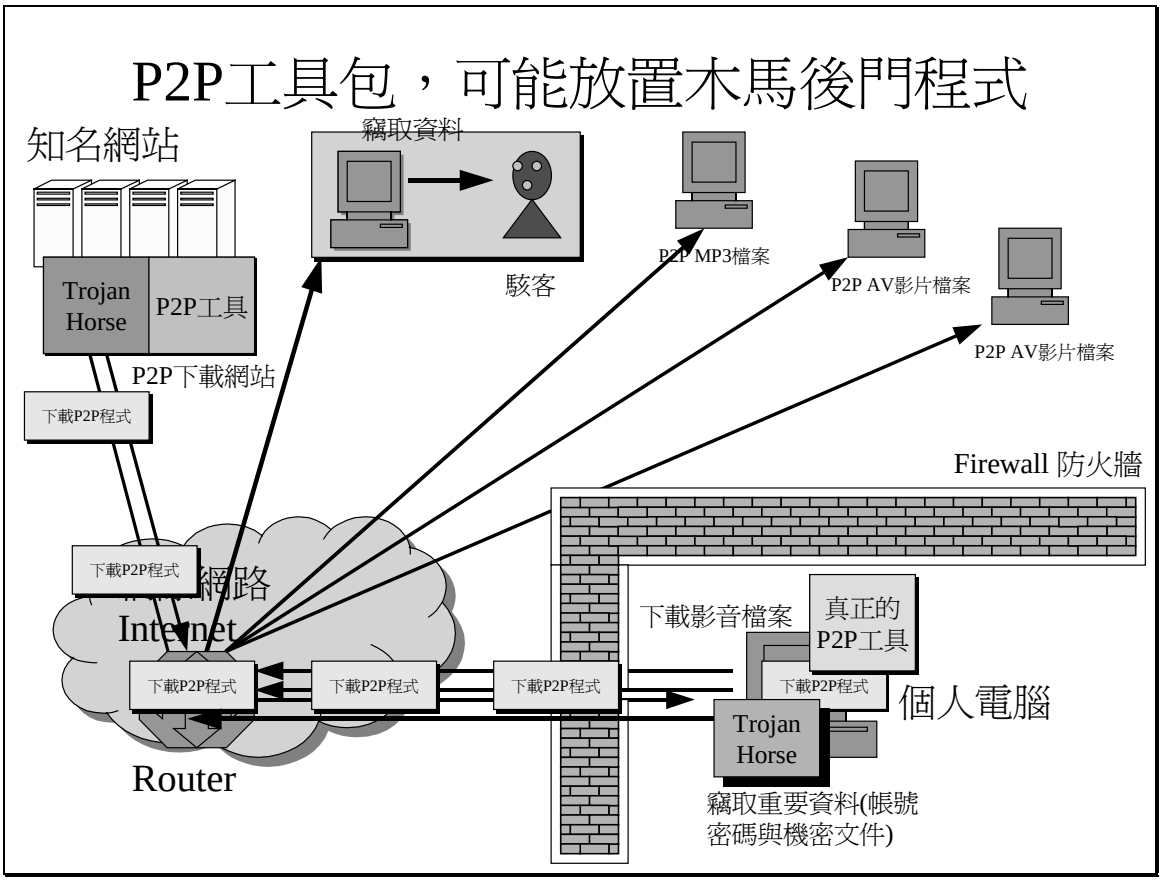


P2P軟體的種類

- BitTorrent系列(BT)，BitTorrent, BitComet, BTspirit、BitTorando等等
- eMule系列，eMule, eDonkey
- GnuTella系列，GnuTella, ezPeer, Mixie,
- FastTrack系列，FastTrack, Kazaa,
- WinMx系列，WinMx, Winny,

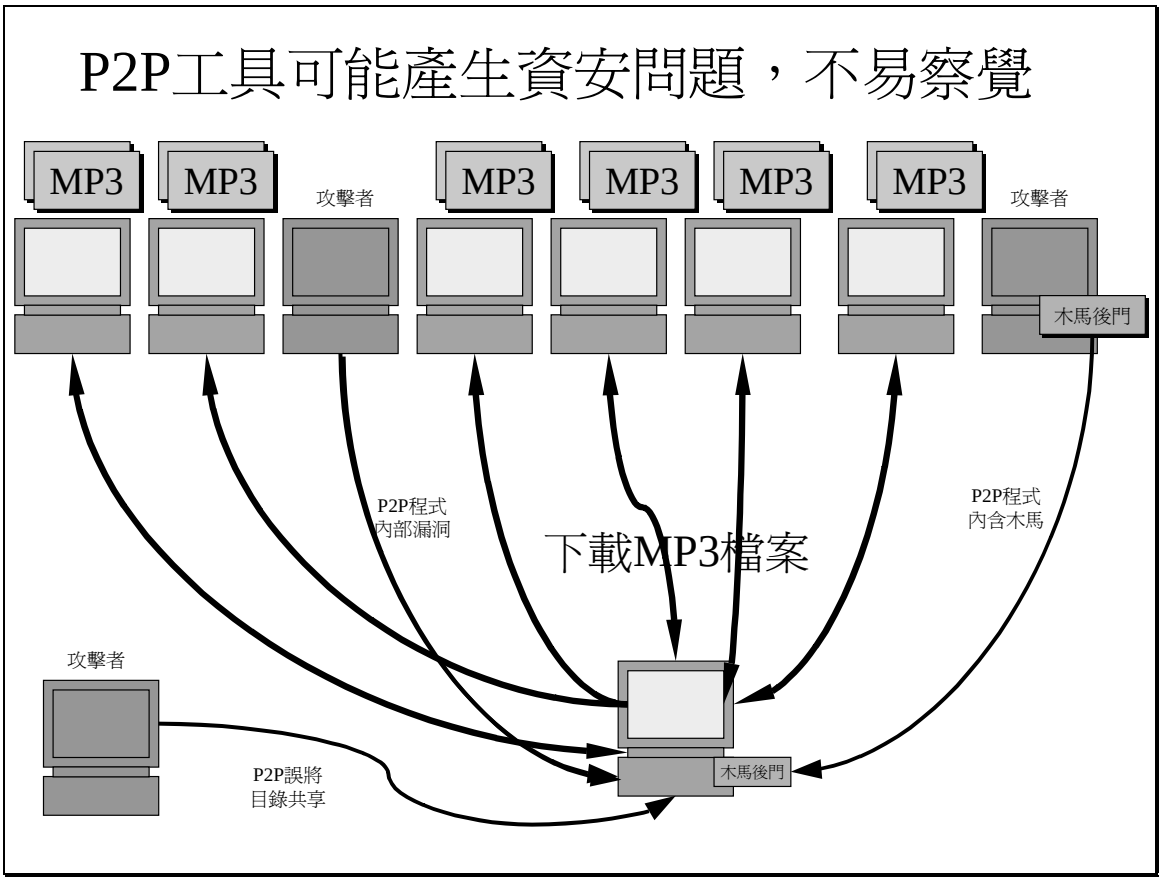
P2P 軟體可能影響網路安全的問題

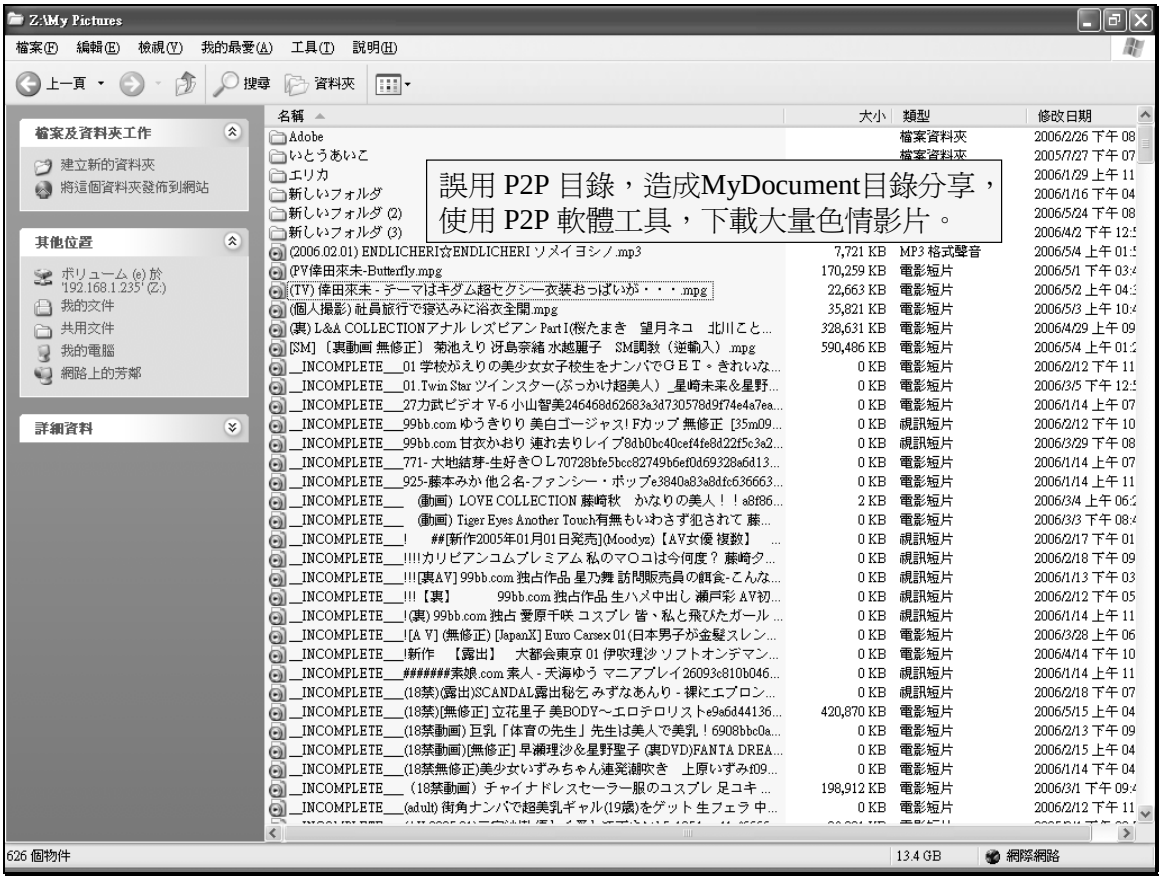
- P2P工具包，可能被惡意人員放置木馬後門程式，與病毒蠕蟲。
- P2P軟體本身的漏洞，造成駭客入侵。
- 使用P2P軟體時，誤將本機目錄開放共享。
- 使用P2P下載影音檔案，多半爲mp3與mpeg, avi等等檔案，可能造成侵權行爲。
- 使用P2P下載色情影片，影響正常工作與政府形象。

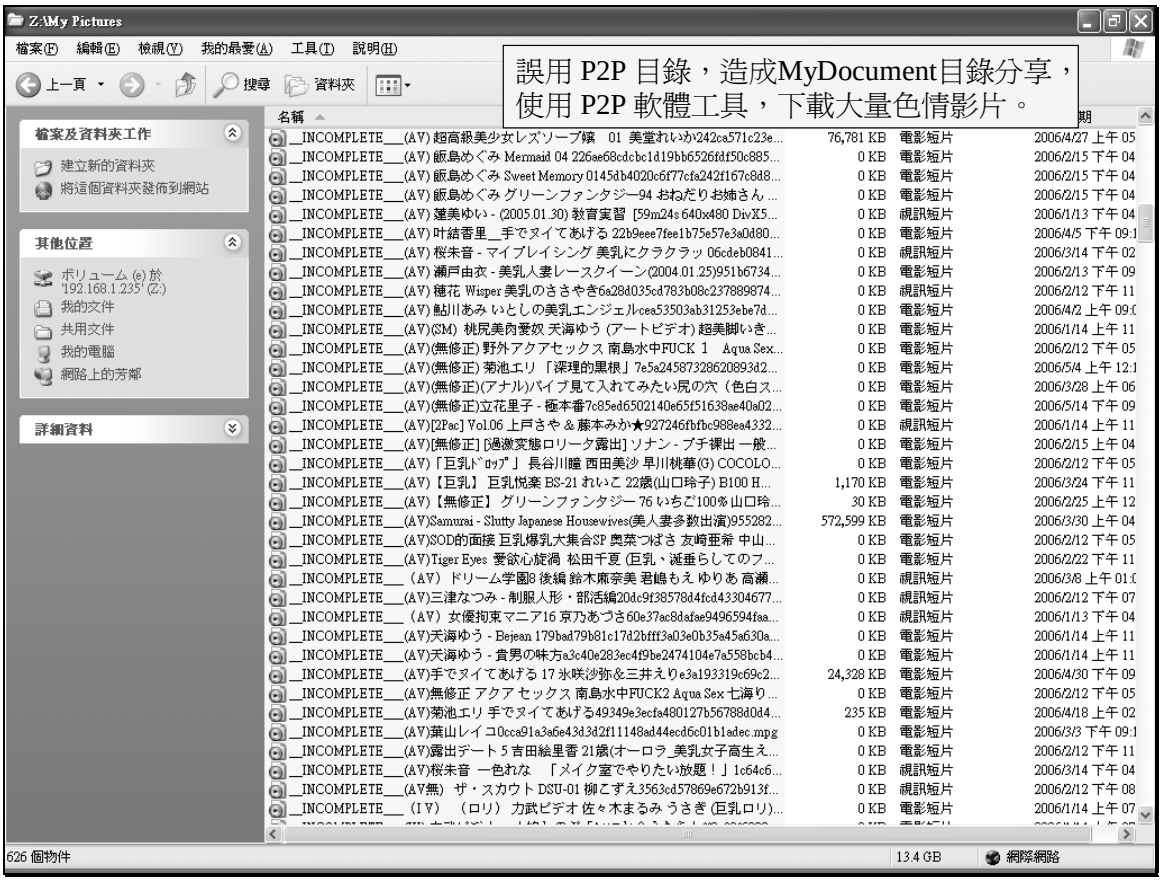


P2P 軟體可能影響網路安全的問題

- 使用P2P軟體工具，誤將MyDocument目錄分享出來。
- 如果該主機登入帳號爲空密碼(或簡單密碼)，對網路安全會產生立即危險。
- 測試指令 (DOS-Command Line 模式)
- `net use \\IP位址\IPC$ "" /user:administrator`
- 以下爲實際範例。

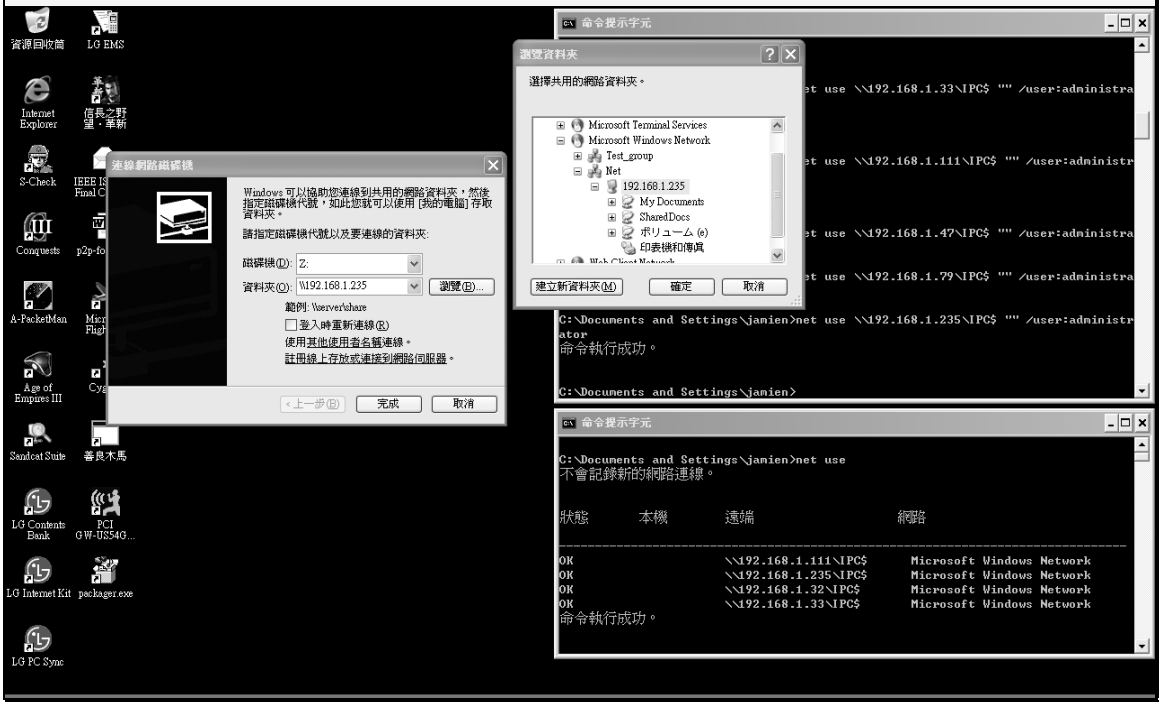

P2P工具可能產生資安問題，不易察覺
MP3
MP3
攻擊者
MP3
MP3
MP3
MP3
攻擊者
木馬後門
P2P程式
內部漏洞
下載MP3檔案
P2P程式
內含木馬
攻擊者
P2P誤將
目錄共享
木馬後門

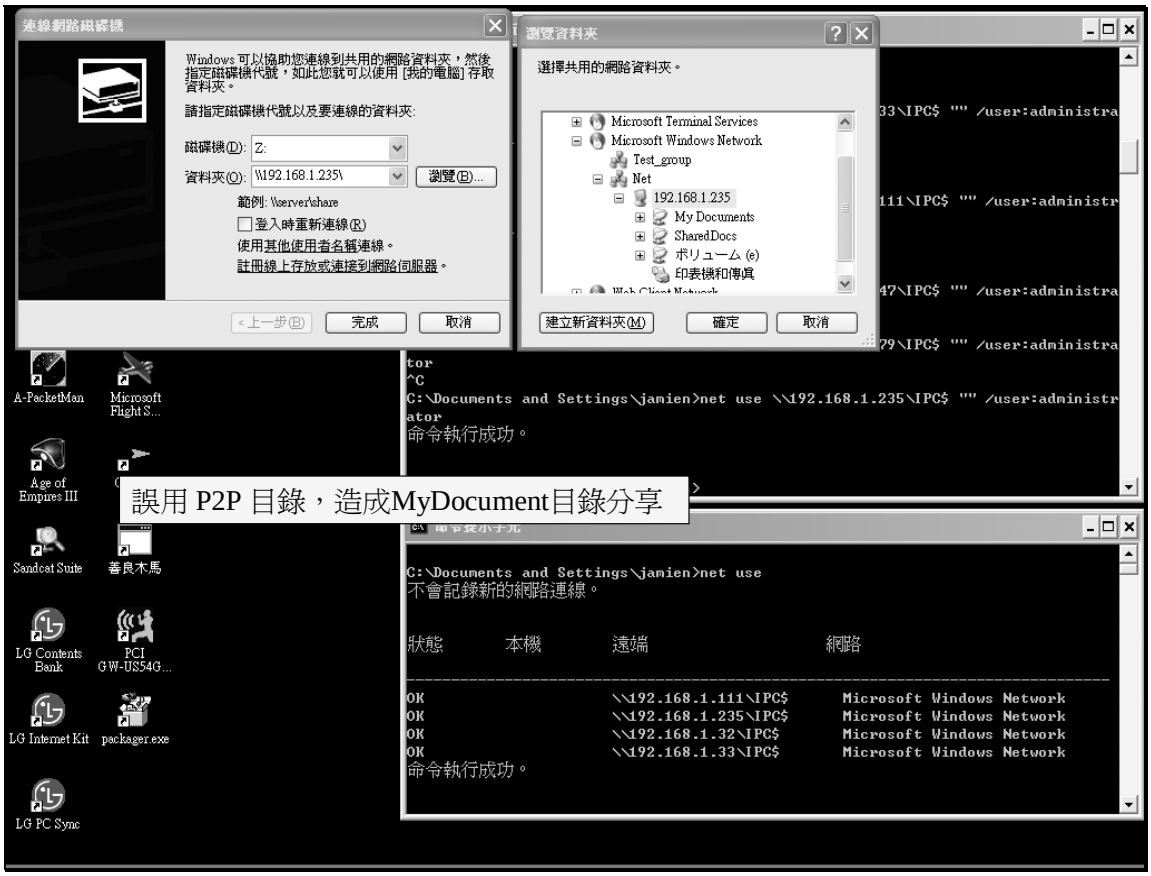

Z:\My Pictures
誤用 P2P 目錄，造成MyDocument目錄分享，
使用 P2P 軟體工具，下載大量色情影片。



輸入連接指令 net use \\IP位址\IPC$ "" /user:administrator

輸入檢視指令 net use

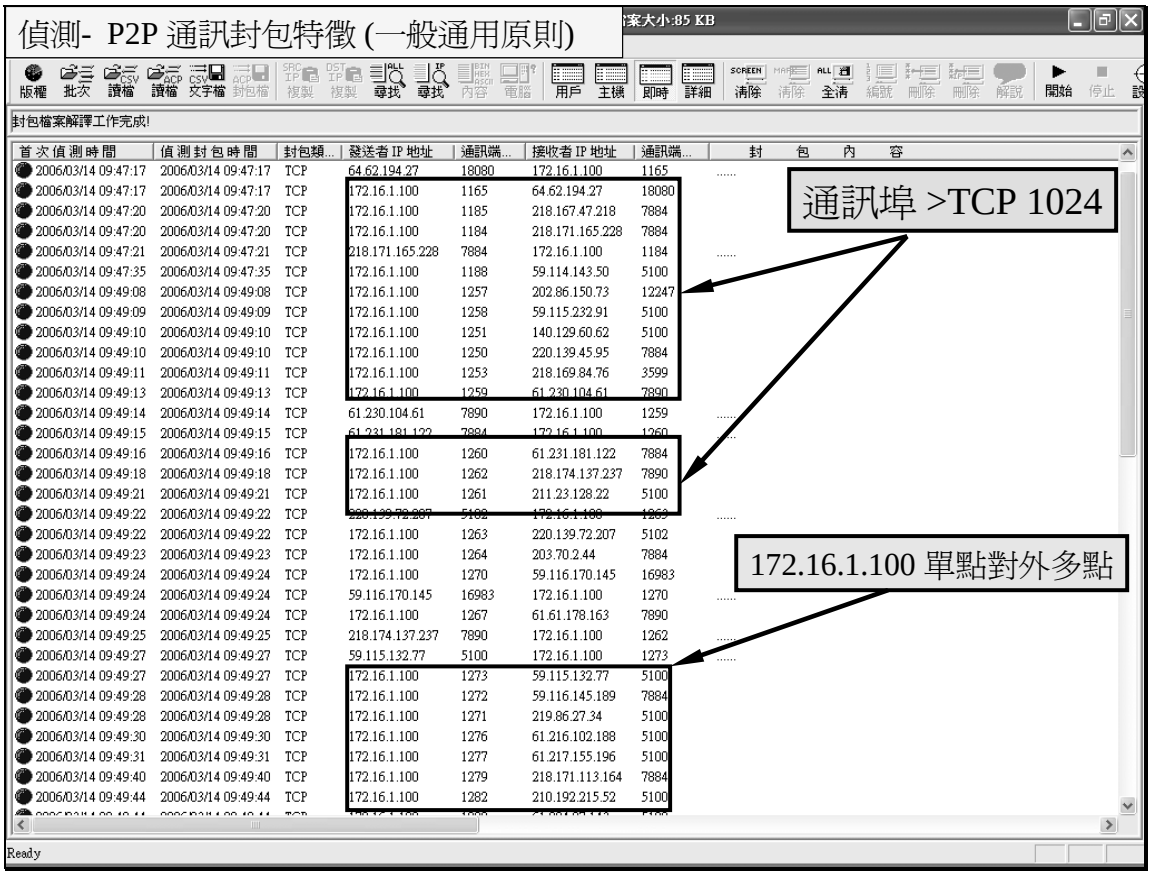


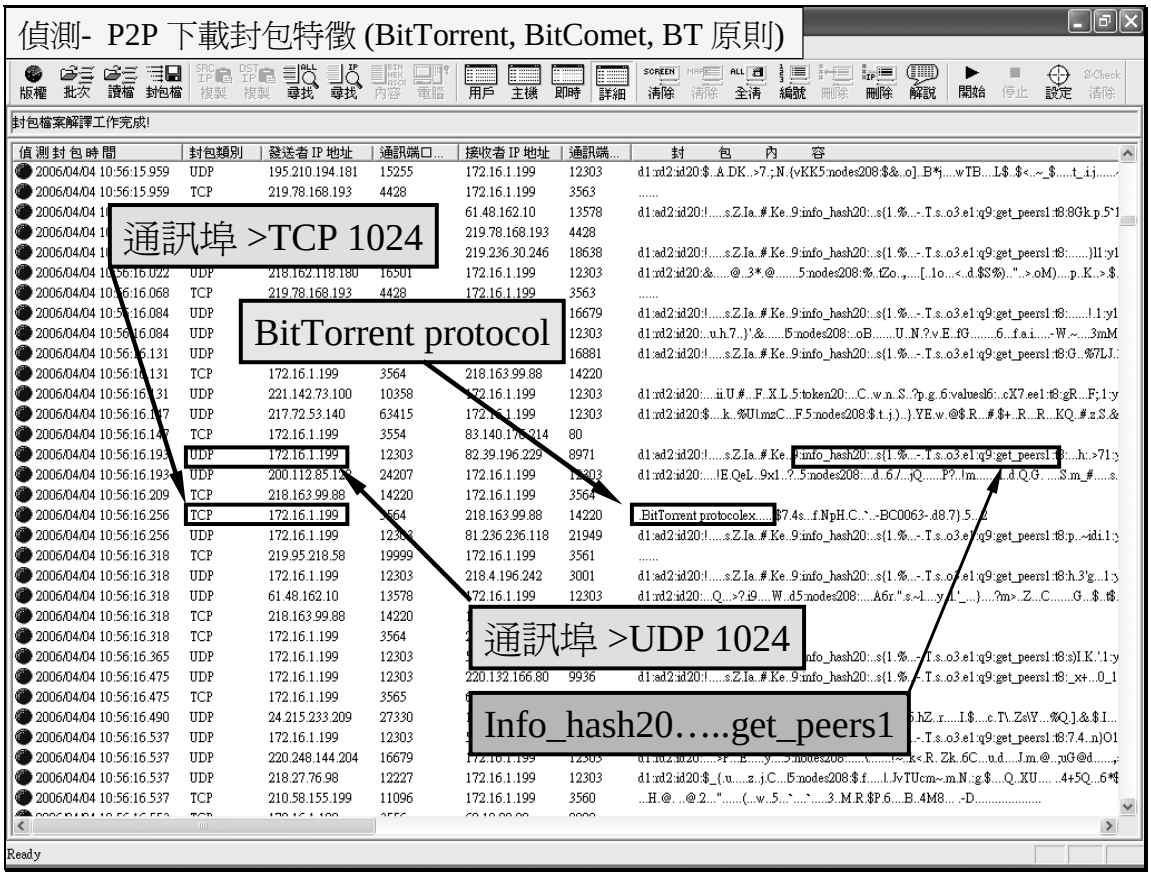

連線網路磁碟機
Windows 可以協助您連線到共用的網路資料夾，然後指定磁碟機代號，如此您就可以使用 [我的電腦] 存取資料夾。
請指定磁碟機代號以及要連線的資料夾:
磁碟機(D): Z:
資料夾(O): \\192.168.1.235\
瀏覽(B)...
範例: \\server\share
登入時重新連線(R)
使用其他使用者名稱連線。
註冊線上存放或連接到網路伺服器。
< 上一步(B)
完成
取消
瀏覽資料夾
選擇共用的網路資料夾。
Microsoft Terminal Services
Microsoft Windows Network
Test_group
Net
192.168.1.235
My Documents
SharedDocs
ボリューム (e)
印表機和傳真
建立新資料夾(M)
確定
取消
C:\Documents and Settings\jamien>net use \\192.168.1.235\IPC$ "" /user:administrator
命令執行成功。
誤用 P2P 目錄，造成MyDocument目錄分享
C:\Documents and Settings\jamien>net use
不會記錄新的網路連線。
狀態 本機 遠端 網路
OK \\192.168.1.111\IPC$ Microsoft Windows Network
OK \\192.168.1.235\IPC$ Microsoft Windows Network
OK \\192.168.1.32\IPC$ Microsoft Windows Network
OK \\192.168.1.33\IPC$ Microsoft Windows Network
命令執行成功。
A-PacketMan
Microsoft Flight S...
Age of Empires III
Sandcat Suite
善良木馬
LG Contents Bank
PCI GW-US54G...
LG Internet Kit
packager.exe
LG PC Sync

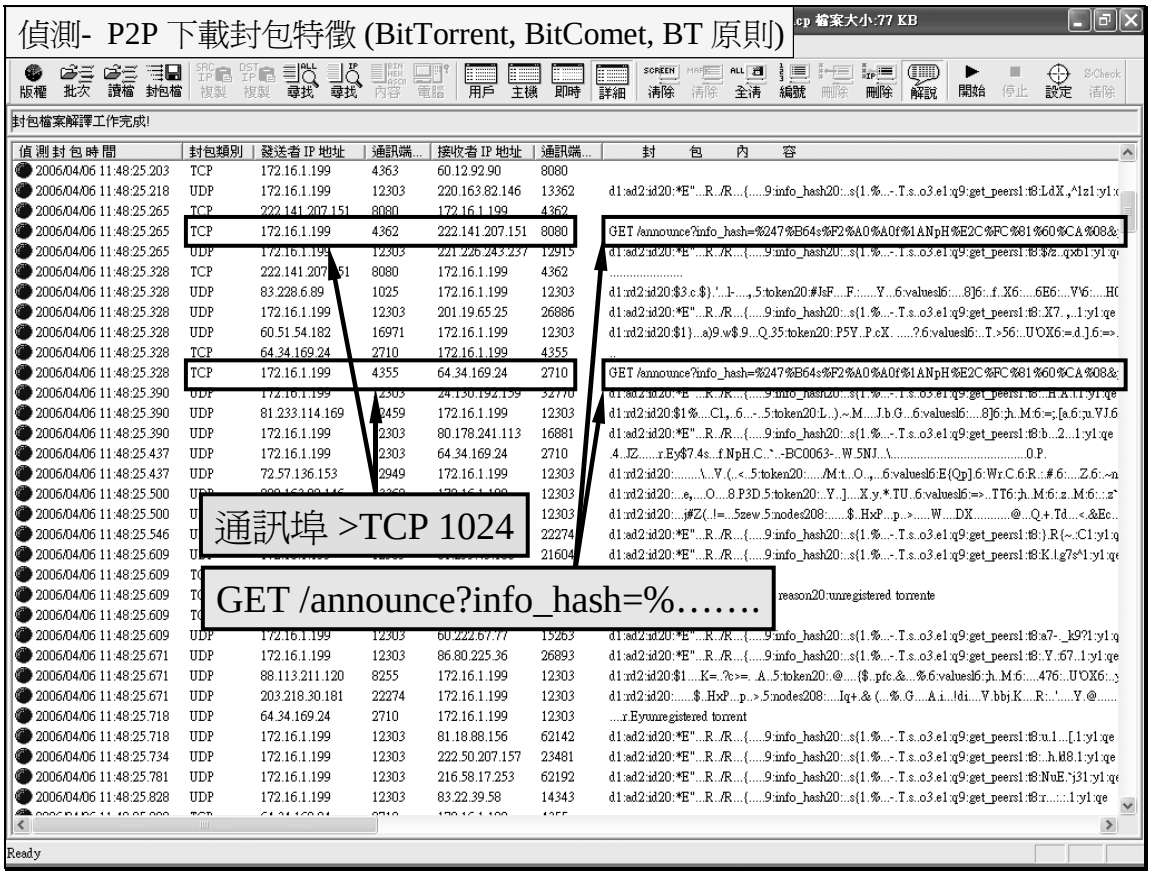

命令提示字元
C:\Documents and Settings\jamien>net use
不會記錄新的網路連線。
狀態 本機 遠端 網路
OK \\192.168.1.111\IPC$ Microsoft Windows Network
OK \\192.168.1.235\IPC$ Microsoft Windows Network
OK \\192.168.1.32\IPC$ Microsoft Windows Network
OK \\192.168.1.33\IPC$ Microsoft Windows Network
命令執行成功。
C:\Documents and Settings\jamien>
C:\Documents and Settings\jamien>net use \\192.168.1.235\IPC$ "" /user:administrator
命令執行成功。
C:\Documents and Settings\jamien>
誤用 P2P 目錄，造成MyDocument目錄分享
搜尋
資料夾
ダイセル
大下 龍也的影片
太平工業
東洋機器
神鋼ＥＮ＆Ｍ
desktop.ini
組態設定值
1 KB
G7.5洗浄制御機器リスト R6(060407).xls
Microsoft Excel 工作表
ボーリング.xls
Microsoft Excel 工作表
22 KB
注文書.xls
Microsoft Excel 工作表
224 KB
新工事項目 1.xls
Microsoft Excel 工作表
862 KB
新規工程表.xls
Microsoft Excel 工作表
220 KB
静岡38面取り配線表（新）.xls
Microsoft Excel 工作表
1,600 KB
FAX送信
48 KB
エアコン
14 KB
作業員名簿追加分.xls
Microsoft Excel 工作表
42 KB
配線表.xls
Microsoft Excel 工作表
647 KB
新作業員名簿.xls
Microsoft Excel 工作表
234 KB
新規配線表Vr1(2005.6).xls
Microsoft Excel 工作表
1,990 KB
5.85 MB
網際網路

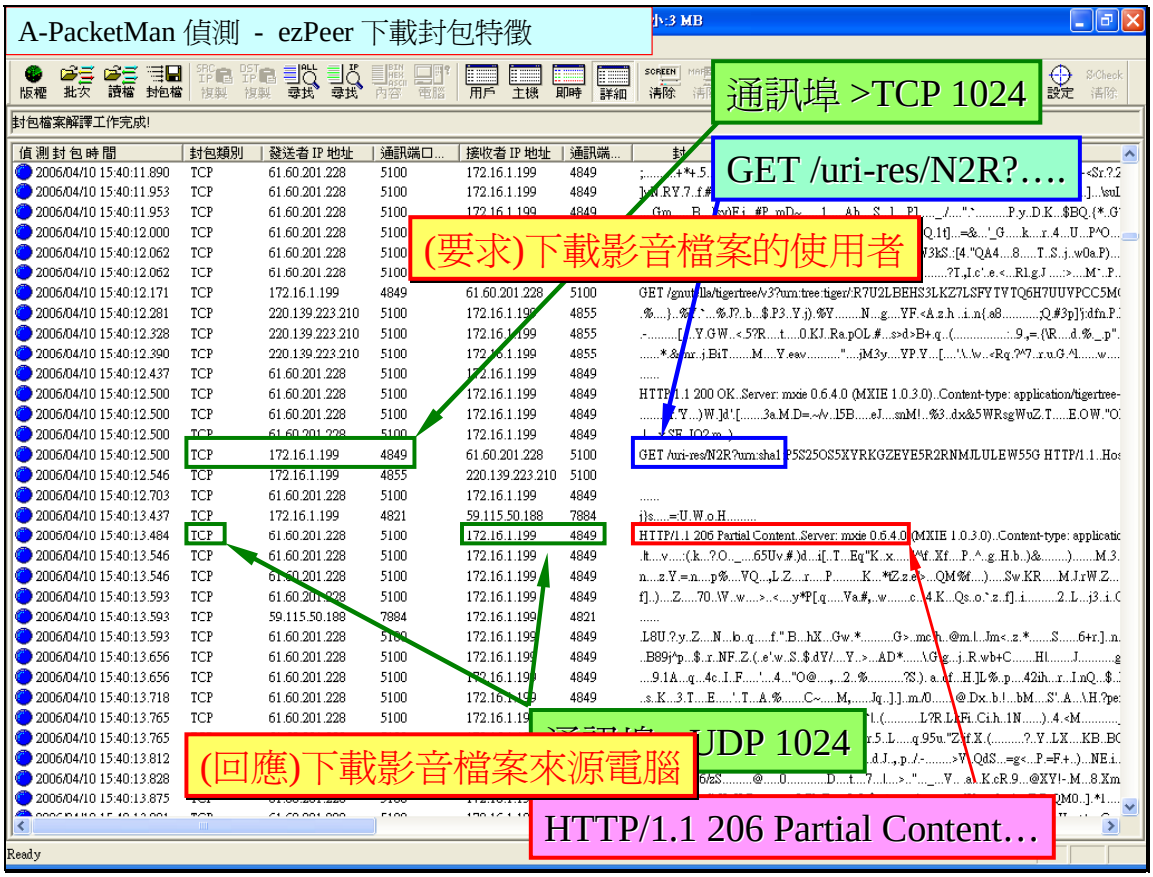
如何偵測與阻擋P2P通訊?

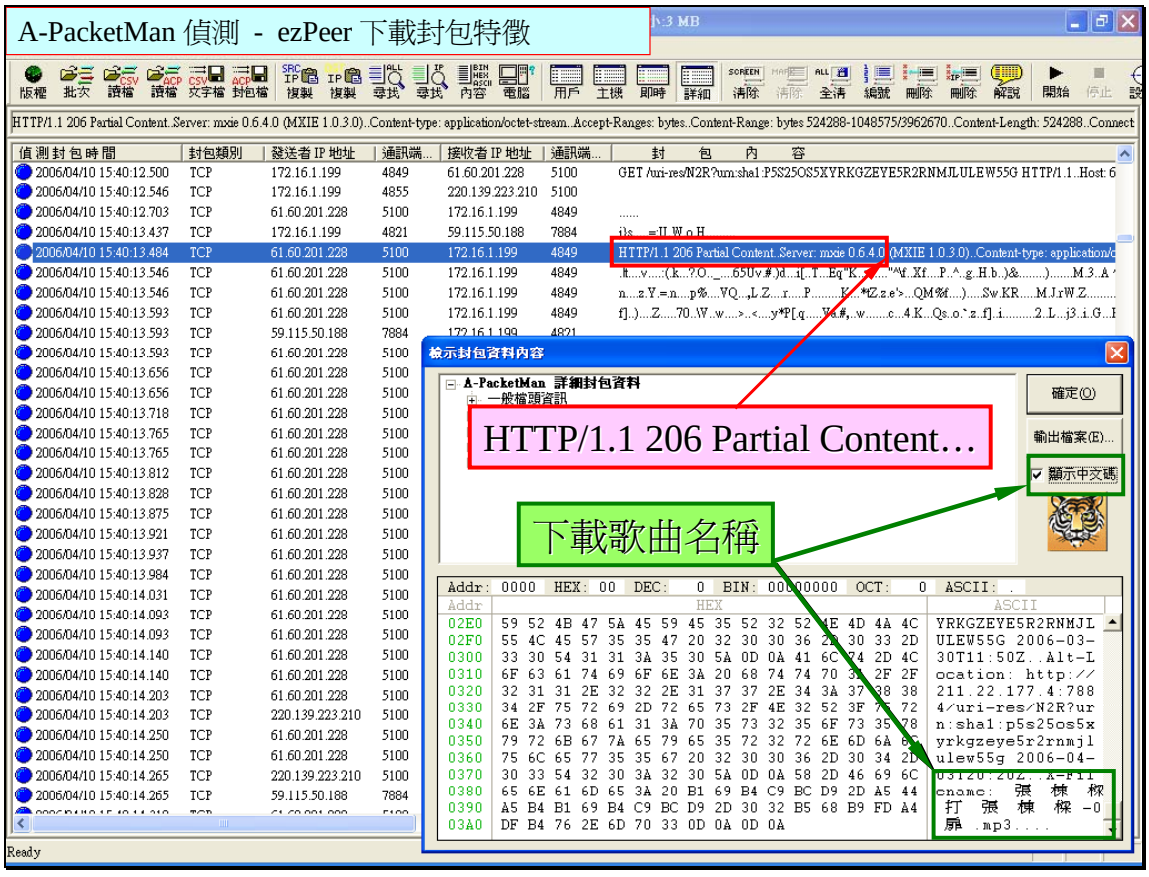
- 多數IPS/IDP/UTM軟硬體均號稱可以阻擋(偵測)P2P工具
  - P2P啓始點IP位址阻擋方式。
  - 通訊流量監控方式。
  - 關鍵字詞偵測方式。
- P2P通訊採用動態Port編號，對點IP位址也非固定IP位址。
- 建議學習P2P通訊的封包分析方式
  - 內網IP位址對外網多點IP位址的通訊。
  - 重要通訊特徵(關鍵字詞與下載歌曲名稱)

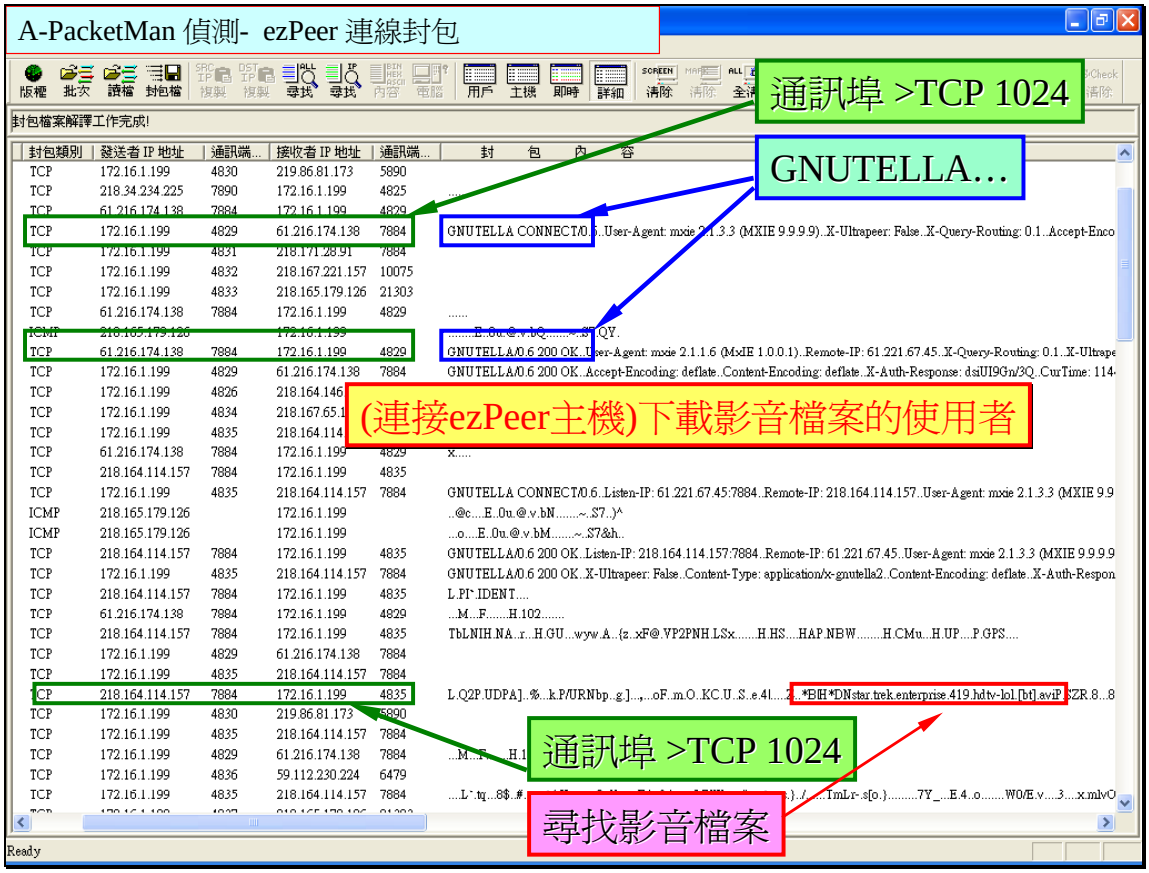


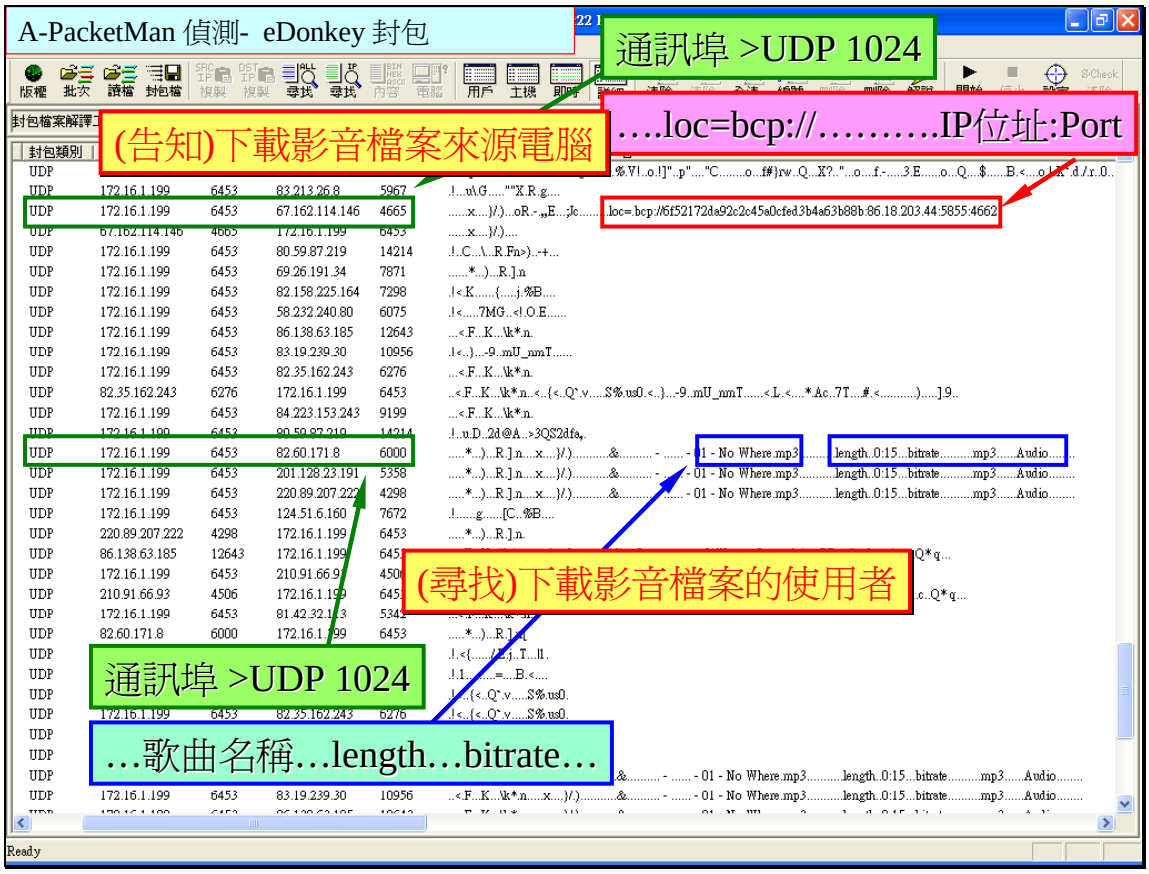

偵測- P2P 下載封包特徵 (BitTorrent, BitComet, BT 原則)
通訊埠 >TCP 1024
BitTorrent protocol
通訊埠 >UDP 1024
Info_hash20…..get_peers1


偵測- P2P 下載封包特徵 (BitTorrent, BitComet, BT 原則)
通訊埠 >TCP 1024
GET /announce?info_hash=%…….

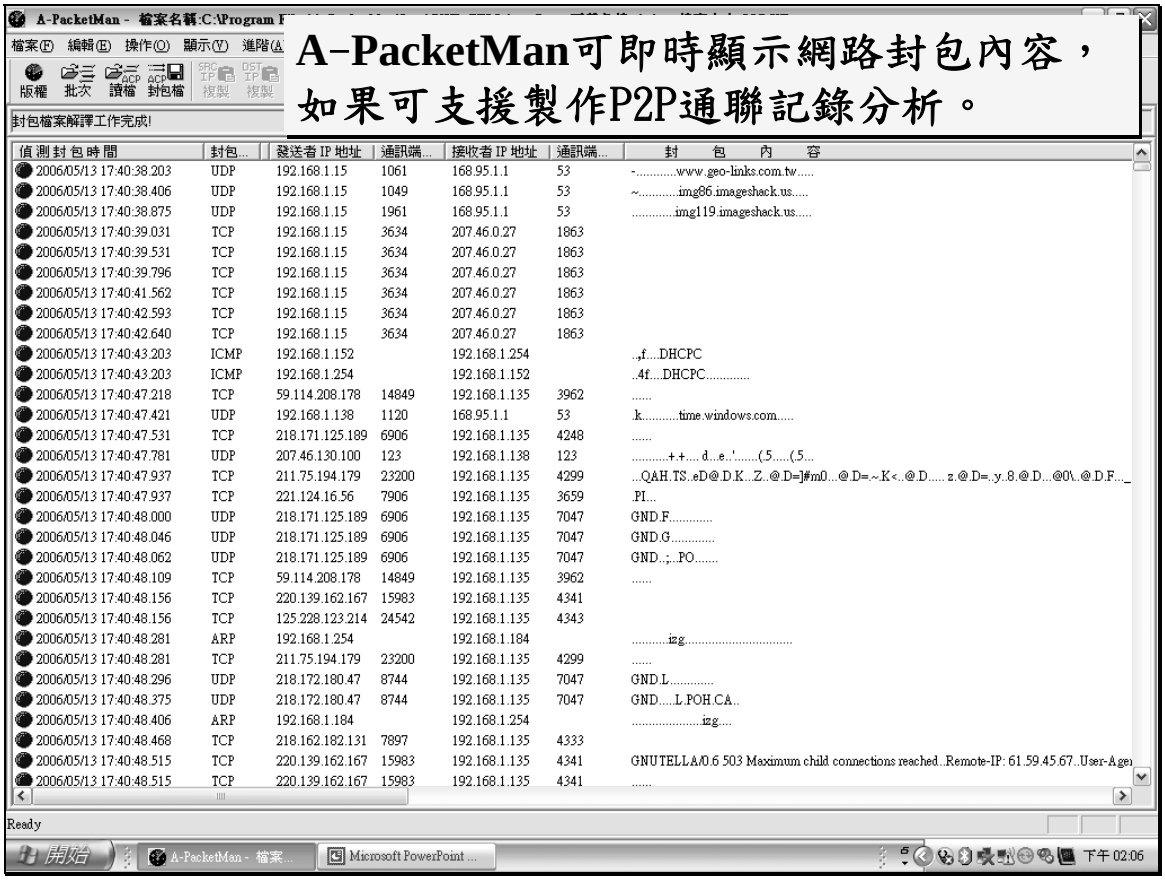




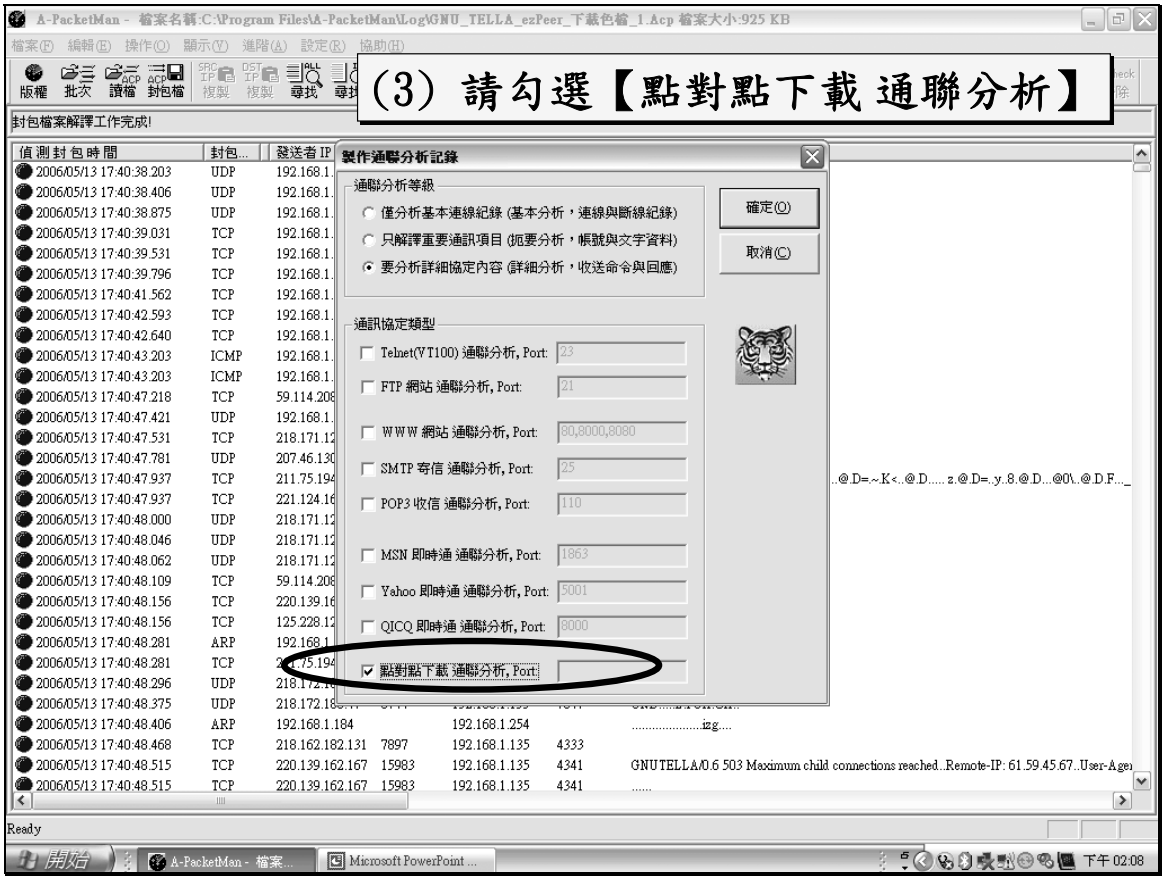

A-PacketMan 偵測- ezPeer 連線封包
通訊埠 >TCP 1024
GNUTELLA…
(連接ezPeer主機)下載影音檔案的使用者
通訊埠 >TCP 1024
尋找影音檔案

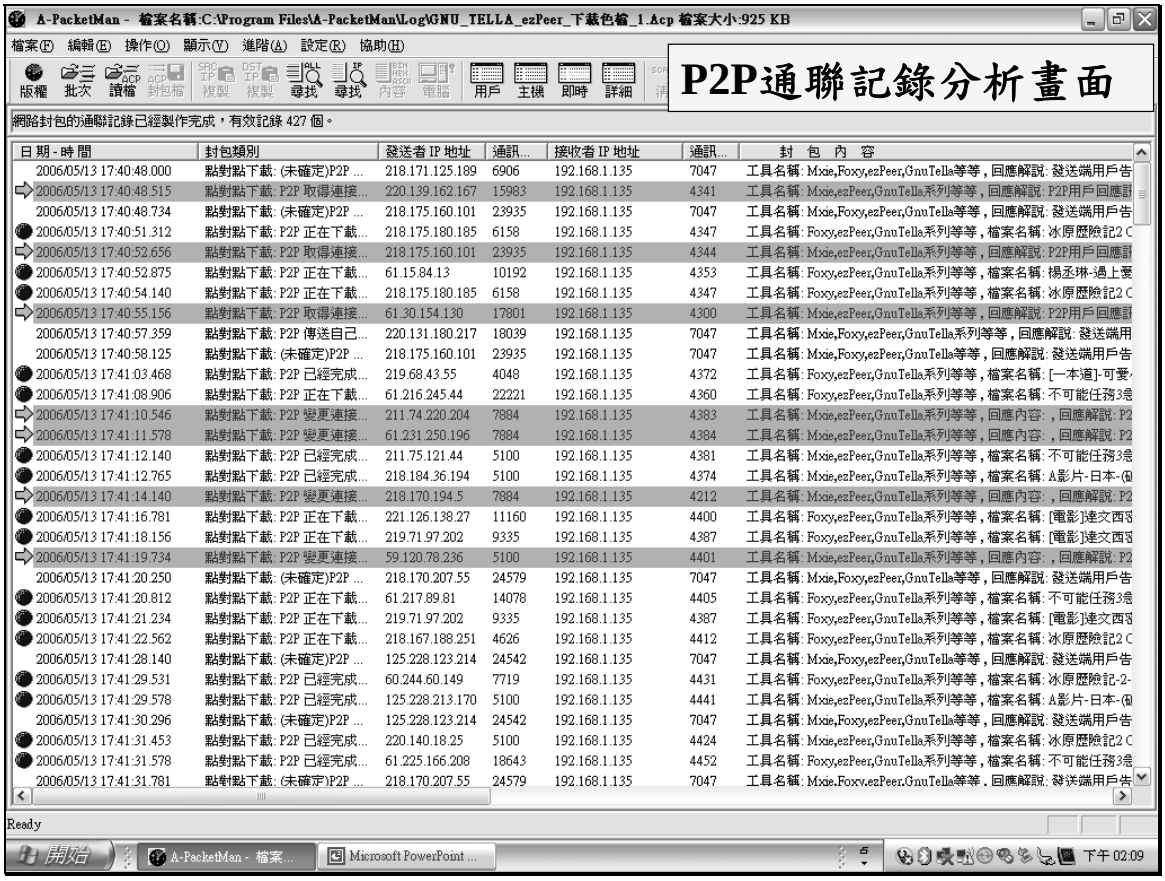

A-PacketMan 偵測- eDonkey 封包
通訊埠 >UDP 1024
(告知)下載影音檔案來源電腦
….loc=bcp://…….IP位址:Port
(尋找)下載影音檔案的使用者
通訊埠 >UDP 1024
…歌曲名稱…length…bitrate…

- P2P軟體會影響網路頻寬甚鉅。T3線路，只要少數人員使用P2P工具，會塞爆網路。
- P2P軟體不易阻擋，因爲多數P2P工具會自動變更Port與IP位址。
- 新版本P2P軟體，可能會更刁鑽難纏。
- 使用封包分析工具，可以隨即找出P2P用戶。




操作步驟：
(1) 請切換到【詳細】畫面。
(2) 請點選功能列【操作】→【製作通聯記錄】


(3) 請勾選【點對點下載 通聯分析】

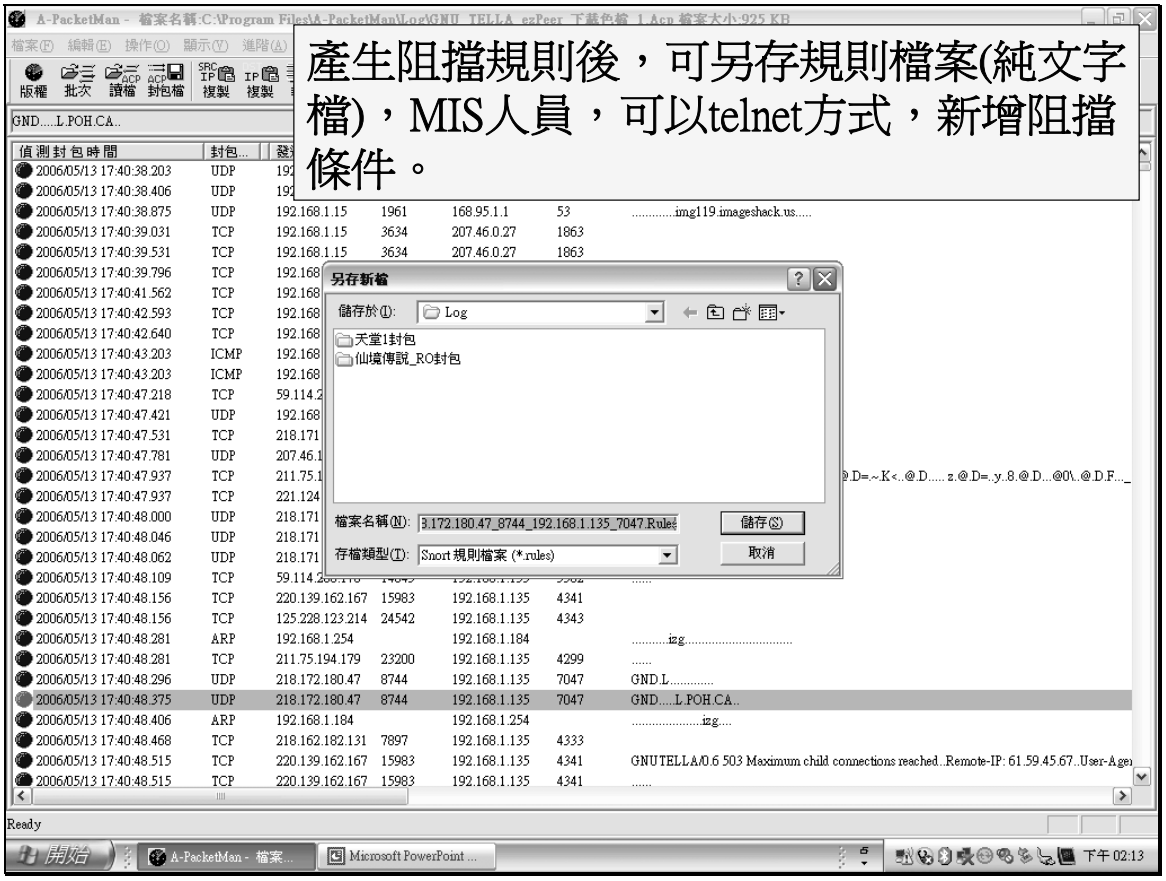


P2P通聯記錄分析畫面

可分析該**IP**位置之異常狀況，並將**P2P**下載的影音檔案名稱，解譯爲中文檔案名稱。

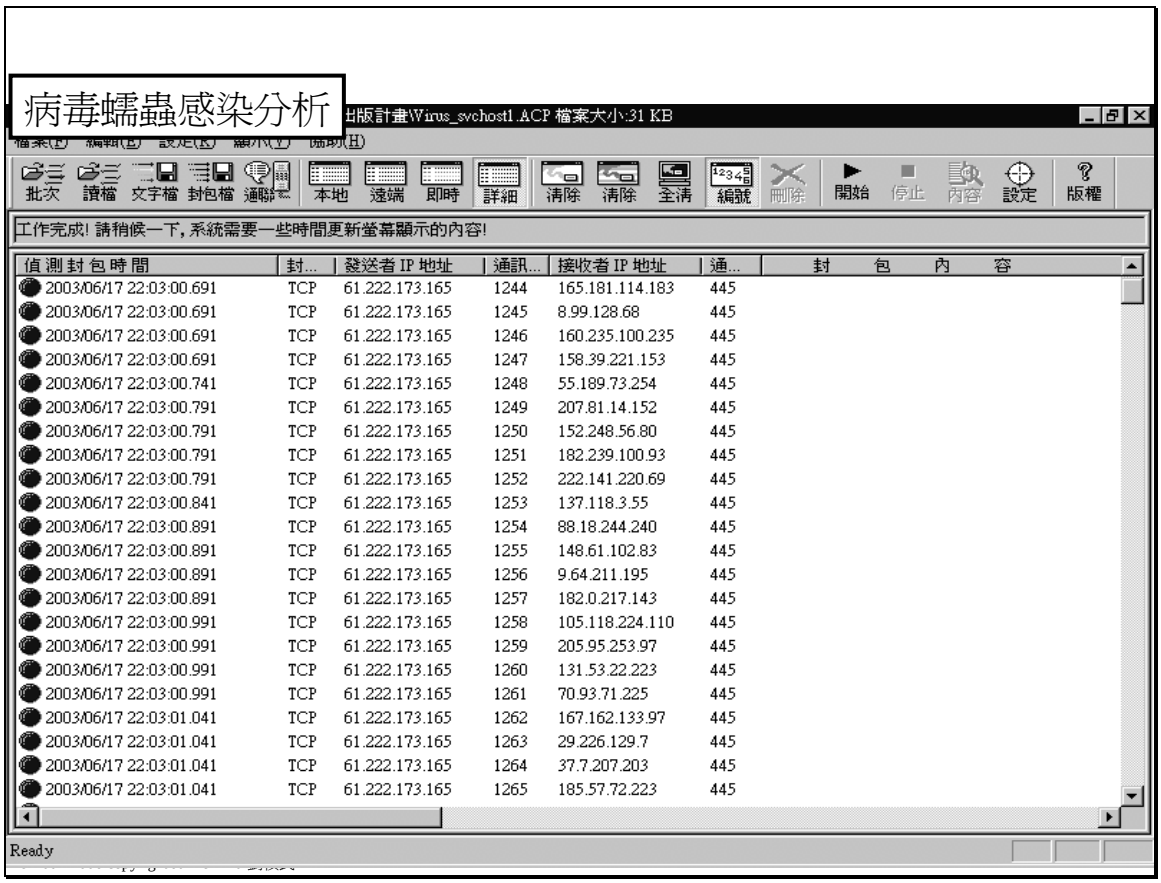

可根據封包內容特徵產生阻擋規則。
A-PacketMan - 檔案名稱:C:\Program Files\A-PacketMan\Log\GNU_TELLA_ezPeer_下載色檔_1.Acp 檔案大小:925 KB
清除程式(A) ...
產生規則(R)...
資安報告(S)...
無線網路連線 2
這個連線只有有限的或沒有連線能力，您可能無法存取網際網路或某些網路資源。如需其他資訊，請按這個訊息。

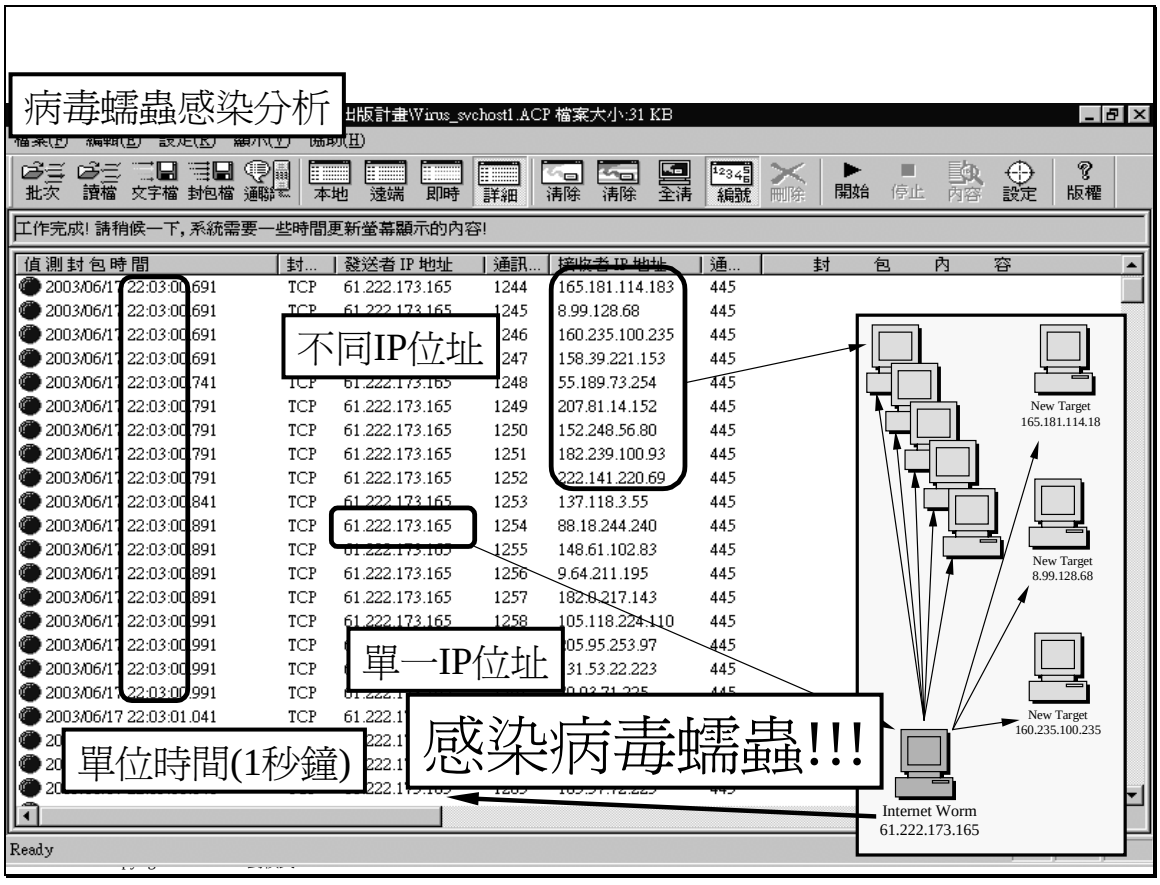

可製作Snort、FortiGate 、PIX …等阻擋規則
產生異常通訊的偵測(阻擋)規則
偵測(阻擋)的封包內容
警訊描述: 偵測 UDP 8744->7047 警訊 (請輸入詳細說明)
通訊協定: 3: UDP
警訊類型: Alert
封包檔頭:
SRC IP: 218.172.180.47
SRC Port: 8744
封包內容: GND.....L.POH.CA..
DST IP:
DST Port: 7047
存檔(O)
關閉(C)
偵測(阻擋)的命令與規則
(1) Snort:
或 相容入侵偵測 IDS 系統
Alert UDP 218.172.180.47 8744 -> any 7047 (msg:"偵測 UDP 8744->7047 警訊 (請輸入詳細說明)"; content:"GND.....L.POH.CA.."; flow
(2) FortiGate:
或 相容入侵防護 IPS 系統
F-SBID(--name 偵測 UDP 8744->7047 警訊 (請輸入詳細說明); --protocol UDP; --content "GND.....L.POH.CA.."; --src_addr 218.172.180
(3) IpTable:
或 相容防火牆 Linux Firewall 系統
iptables -A INPUT -i eth0 -o eth1 -p UDP -s 218.172.180.47 --sport 8744 --dport 7047 -j DROP
(4) Cisco PIX:
或 相容防火牆 Cisco Firewall 系統
access-list acl_in deny udp host 218.172.180.47 any
access-group acl_in in interface inside
(5) MS-XP Firewall:
或 相容防火牆 MS-Windows ICF Firewall
netsh firewall add portopening UDP 7047 A-PacketMan-Deny DISABLE ALL
注意事項說明：本功能市協助網路管理人員與資安維護人員，根據方包內容與通訊位址(通訊埠)，能夠輕鬆地阻斷異常網路封包對外通訊。 您應當視自己內部網路配置狀況與線常實際需求做適當的刪除與重組規則命令。
本規則僅作參考，請審慎計畫後，再自行決定阻斷規則命令。

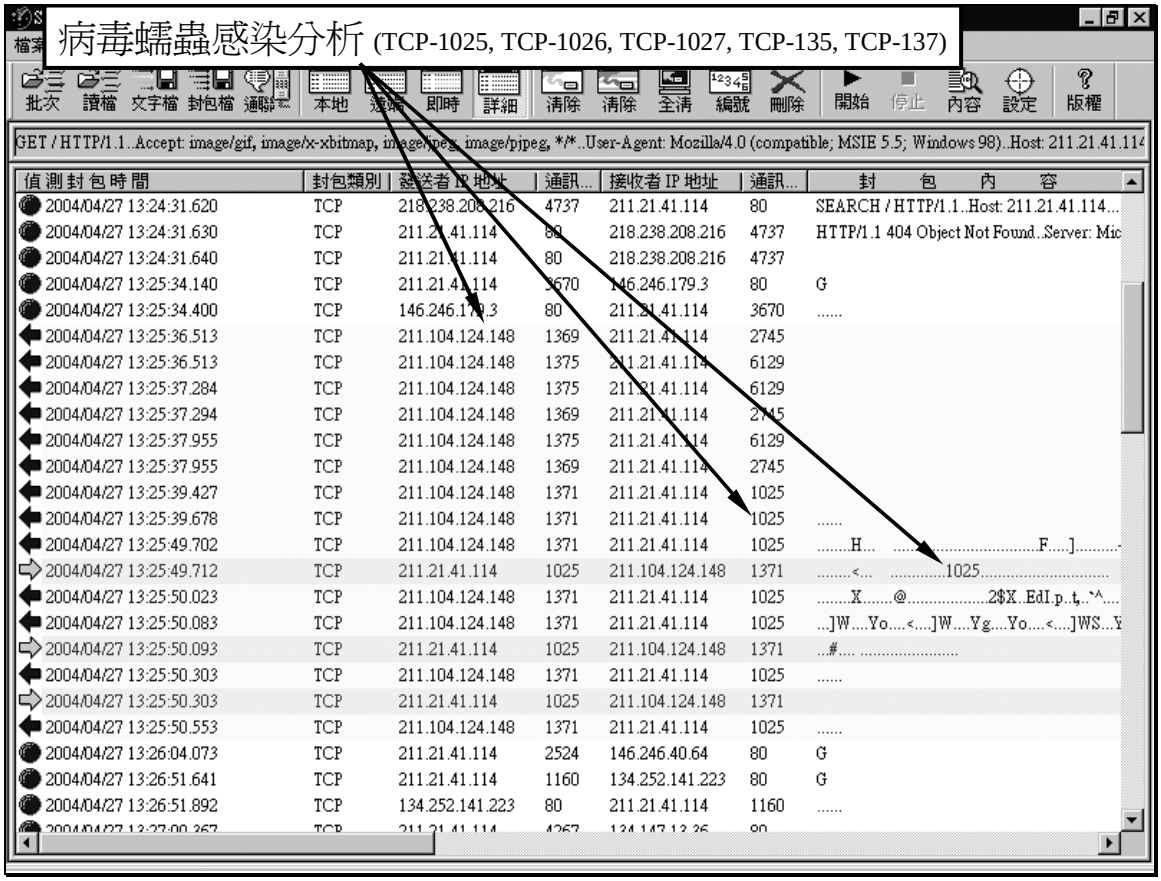


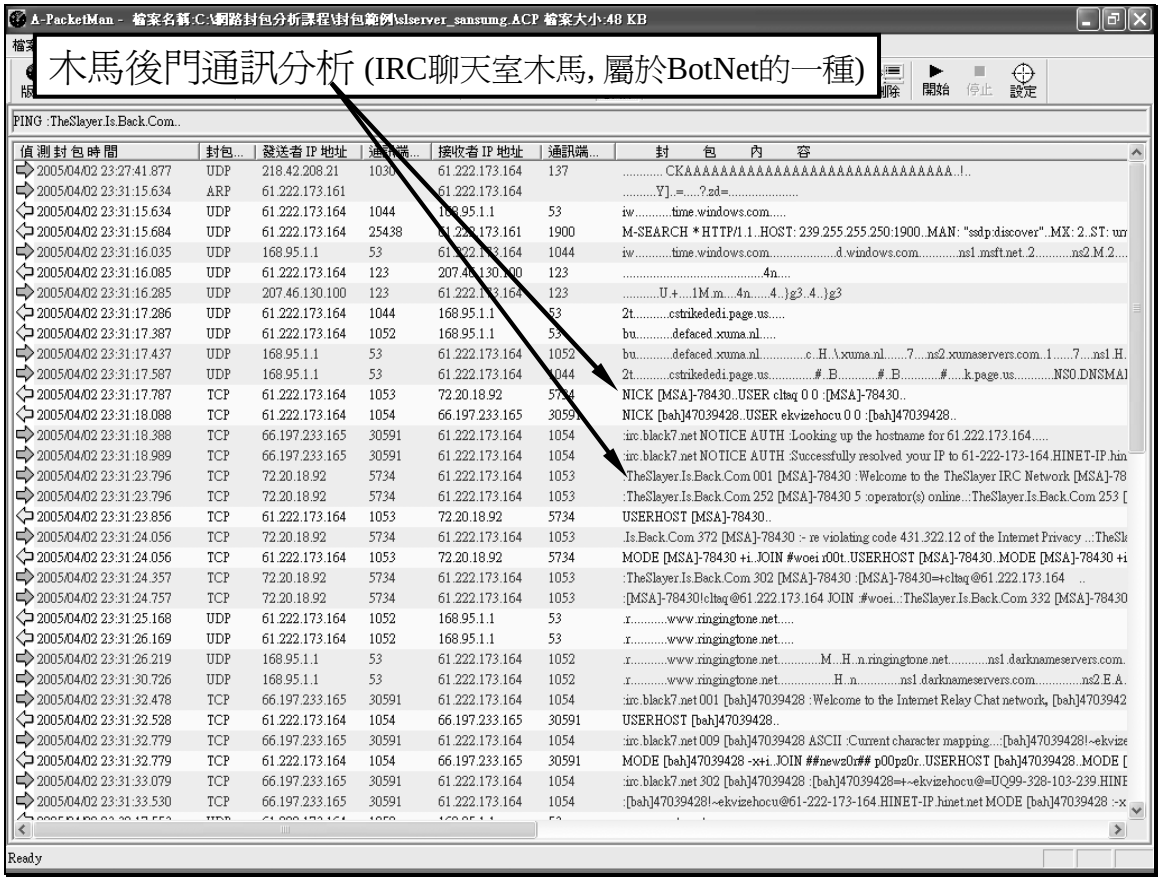
A-PacketMan 的應用範例

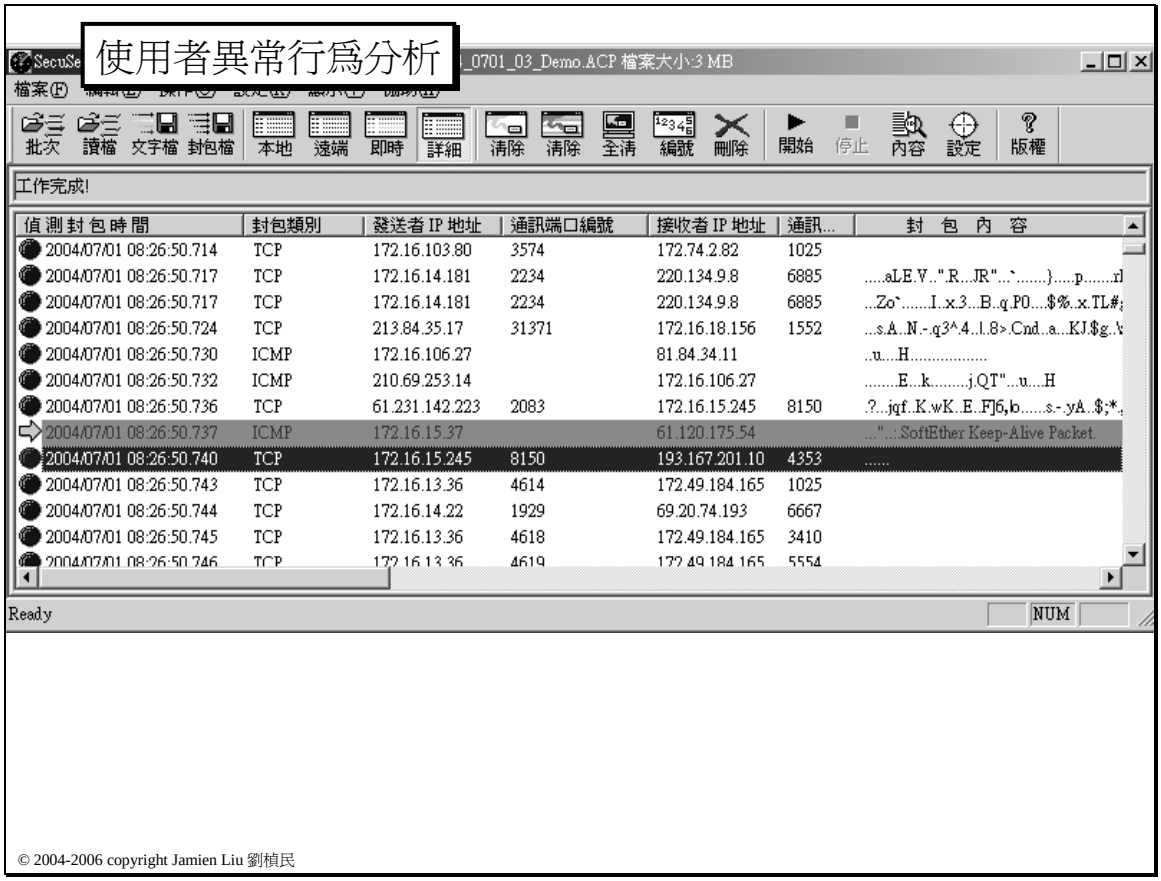
- 病毒蠕蟲感染分析
- 木馬後門通訊分析
- 使用者異常行爲分析
- 網路攻擊行爲分析
- 資料庫通訊分析

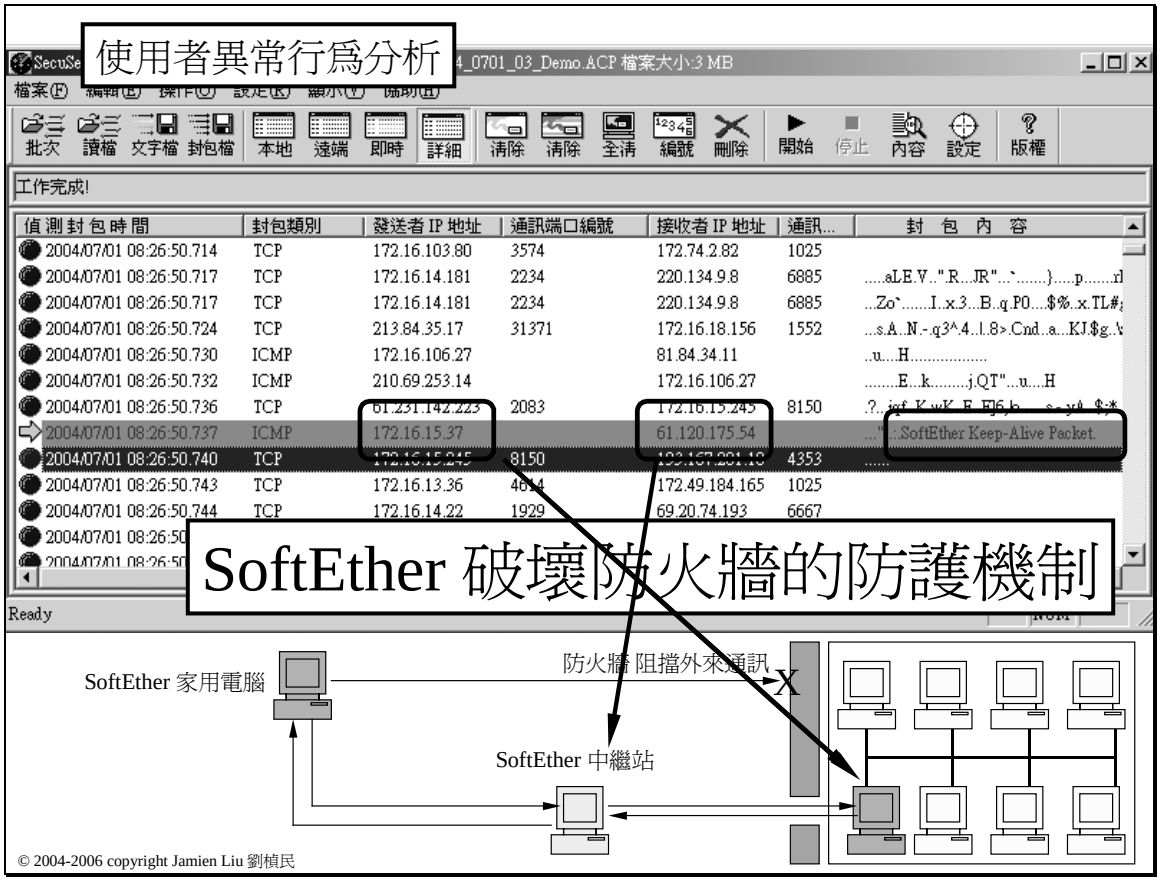

病毒蠕蟲感染分析
出版計畫\Virus_svchost1.ACP 檔案大小:31 KB
批次 讀檔 文字檔 封包檔 通聯 本地 遠端 即時 詳細 清除 清除 全清 編號 刪除 開始 停止 內容 設定 版權
工作完成! 請稍候一下, 系統需要一些時間更新螢幕顯示的內容!
值測封包時間 封... 發送者IP地址 通訊... 接收者IP地址 通... 封包內容
2003/06/17 22:03:00.691 TCP 61.222.173.165 1244 165.181.114.183 445
2003/06/17 22:03:00.691 TCP 61.222.173.165 1245 8.99.128.68 445
2003/06/17 22:03:00.691 TCP 61.222.173.165 1246 160.235.100.235 445
2003/06/17 22:03:00.691 TCP 61.222.173.165 1247 158.39.221.153 445
2003/06/17 22:03:00.741 TCP 61.222.173.165 1248 55.189.73.254 445
2003/06/17 22:03:00.791 TCP 61.222.173.165 1249 207.81.14.152 445
2003/06/17 22:03:00.791 TCP 61.222.173.165 1250 152.248.56.80 445
2003/06/17 22:03:00.791 TCP 61.222.173.165 1251 182.239.100.93 445
2003/06/17 22:03:00.791 TCP 61.222.173.165 1252 222.141.220.69 445
2003/06/17 22:03:00.841 TCP 61.222.173.165 1253 137.118.3.55 445
2003/06/17 22:03:00.891 TCP 61.222.173.165 1254 88.18.244.240 445
2003/06/17 22:03:00.891 TCP 61.222.173.165 1255 148.61.102.83 445
2003/06/17 22:03:00.891 TCP 61.222.173.165 1256 9.64.211.195 445
2003/06/17 22:03:00.891 TCP 61.222.173.165 1257 182.0.217.143 445
2003/06/17 22:03:00.991 TCP 61.222.173.165 1258 105.118.224.110 445
2003/06/17 22:03:00.991 TCP 61.222.173.165 1259 205.95.253.97 445
2003/06/17 22:03:00.991 TCP 61.222.173.165 1260 131.53.22.223 445
2003/06/17 22:03:00.991 TCP 61.222.173.165 1261 70.93.71.225 445
2003/06/17 22:03:01.041 TCP 61.222.173.165 1262 167.162.133.97 445
2003/06/17 22:03:01.041 TCP 61.222.173.165 1263 29.226.129.7 445
2003/06/17 22:03:01.041 TCP 61.222.173.165 1264 37.7.207.203 445
2003/06/17 22:03:01.041 TCP 61.222.173.165 1265 185.57.72.223 445
Ready

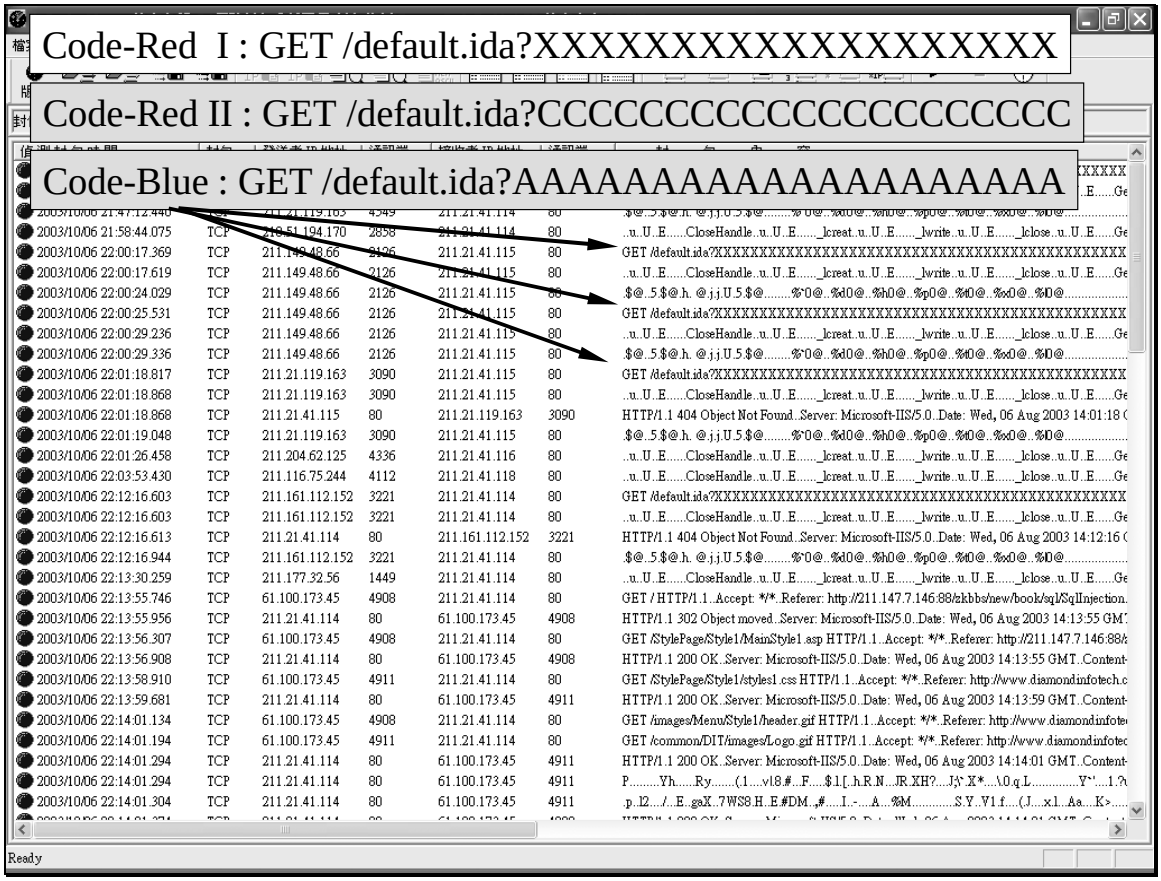

病毒蠕蟲感染分析
出版計畫\Virus_svchost1.ACP 檔案大小:31 KB
批次 讀檔 文字檔 封包檔 通聯 本地 遠端 即時 詳細 清除 清除 全清 編號 刪除 開始 停止 內容 設定 版權
工作完成! 請稍候一下, 系統需要一些時間更新螢幕顯示的內容!
值測封包時間 封... 發送者IP地址 通訊... 接收者IP地址 通... 封包內容
不同IP位址
單一IP位址
單位時間(1秒鐘)
感染病毒蠕蟲!!!
New Target 165.181.114.18
New Target 8.99.128.68
New Target 160.235.100.235
Internet Worm 61.222.173.165
Ready

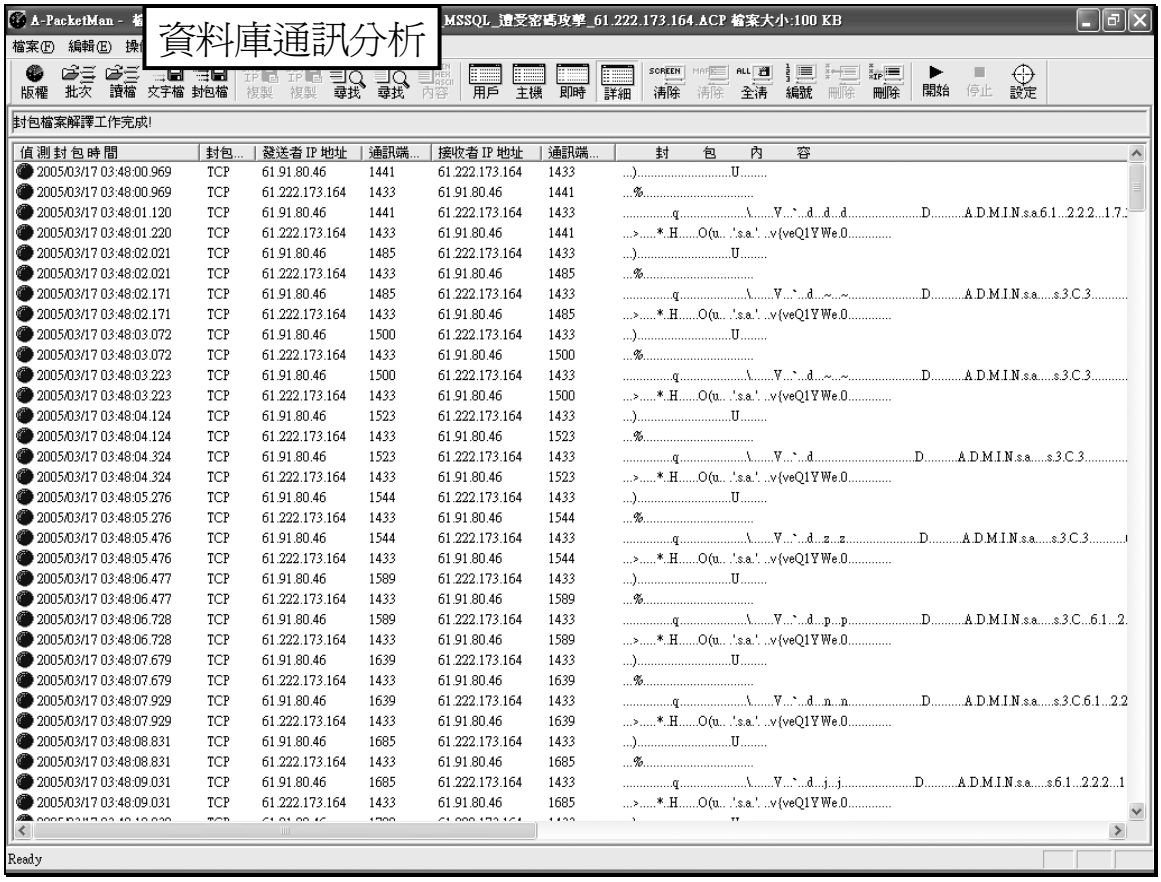


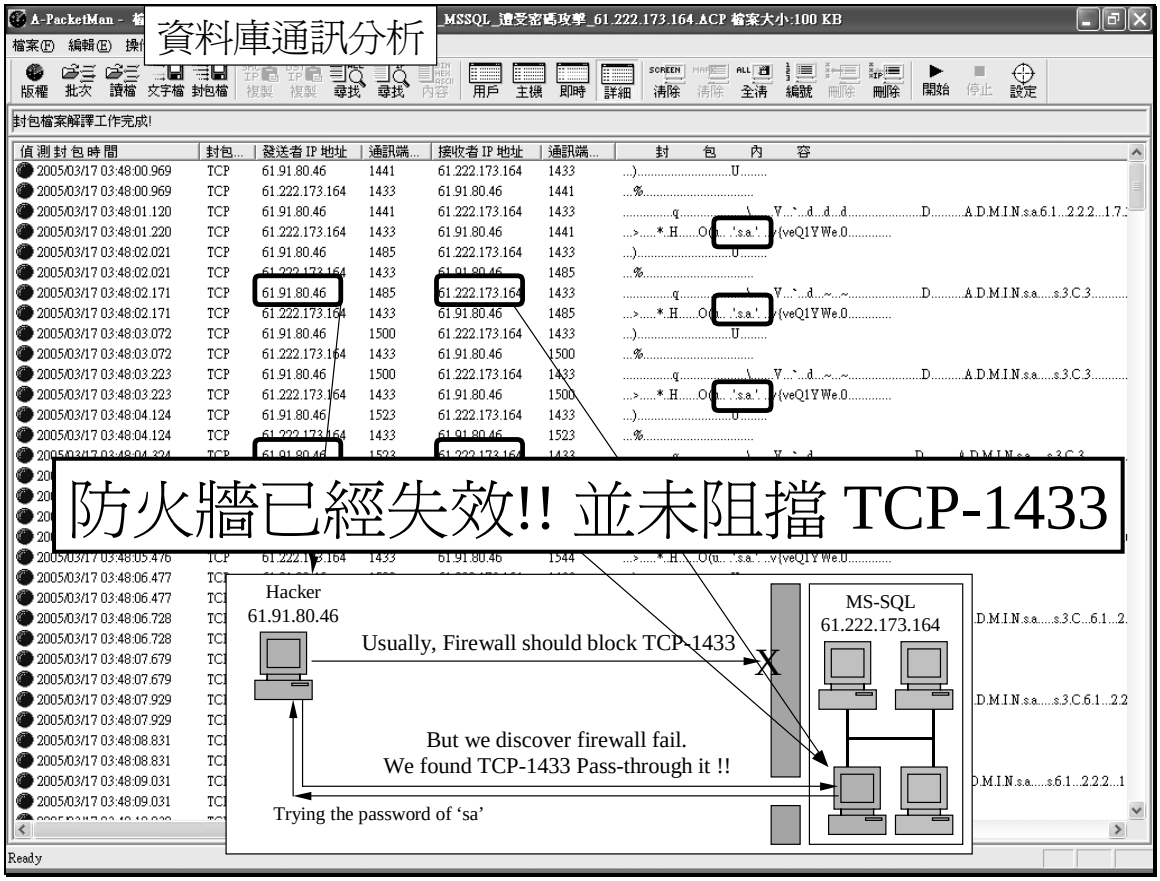



使用者異常行爲分析
© 2004-2006 copyright Jamien Liu 劉楨民


使用者異常行爲分析
SoftEther 破壞防火牆的防護機制
SoftEther 家用電腦
防火牆 阻擋外來通訊
SoftEther 中繼站
© 2004-2006 copyright Jamien Liu 劉楨民


Code-Red I : GET /default.ida?XXXXXXXXXXXXXXXXXXX
Code-Red II : GET /default.ida?CCCCCCCCCCCCCCCCCCCC
Code-Blue : GET /default.ida?AAAAAAAAAAAAAAAAAAAA


資料庫通訊分析



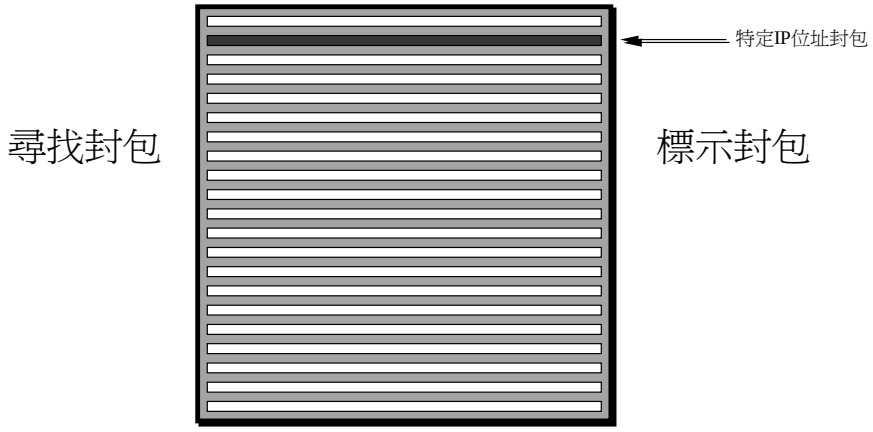
網路封包分析的基本技巧 (The skill of analysis packets)

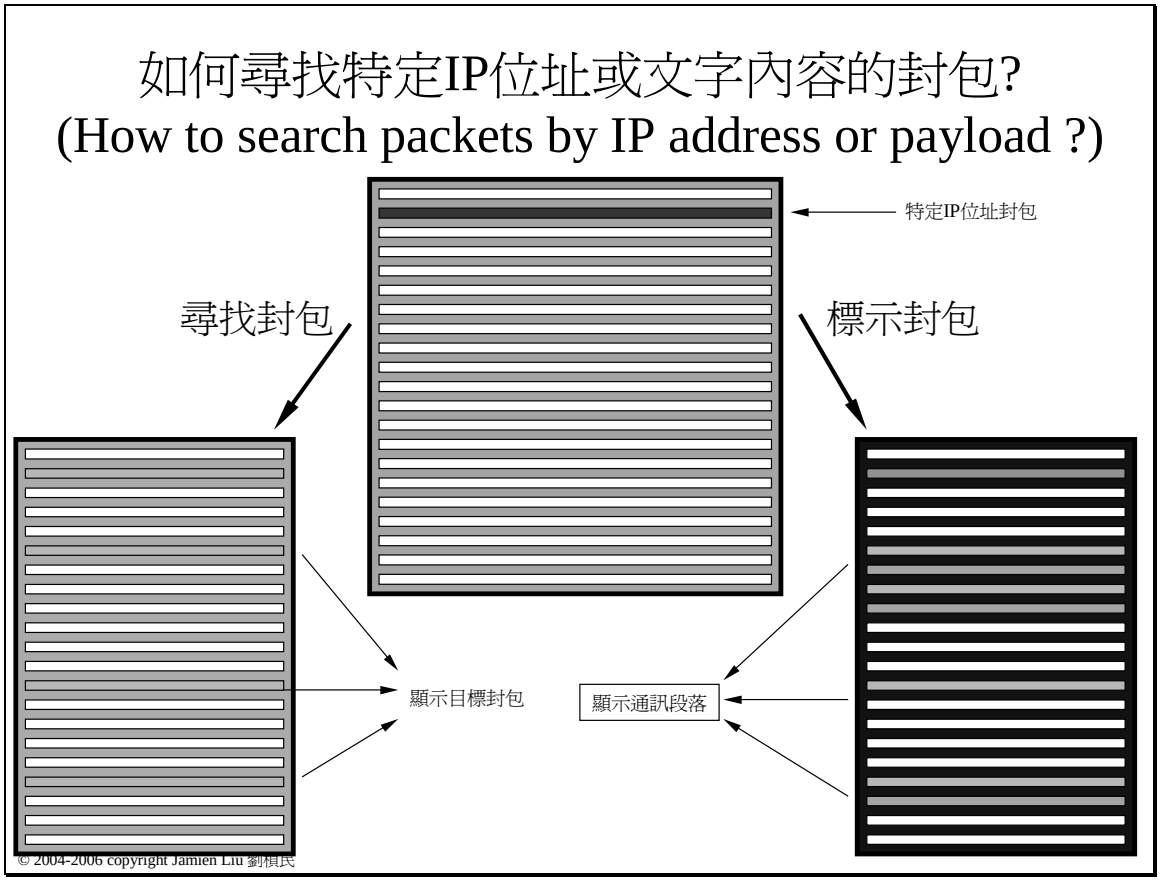
- 先學習正常封包通訊的情況，瞭解基本通訊，HTTP, SMTP, POP3, SMB/CIFS, DNS, MS-SQL, MySQL等等。
- 分析封包時，先排除已知正常通訊封包。
- 如果已經排除已知正常通訊封包，剩餘無法解釋的通訊封包，可能包括異常與未知通訊封包。
- 分析異常封包的主要原則:
  - 先觀察通訊雙方爲內網位址或外網位址?
  - 進一步觀察通訊雙方爲單向或雙向通訊?
  - 接著檢查此網路通訊爲禁止或開放的網路服務?
  - 傳送內容爲明碼資料? 編碼資料? 或加密資料?
  - 是否違反封包行爲分析(PBA)的原則?
  - 如果有無法解譯與分析的封包，可以將他從整個檔案萃取出來，方法如後所示。

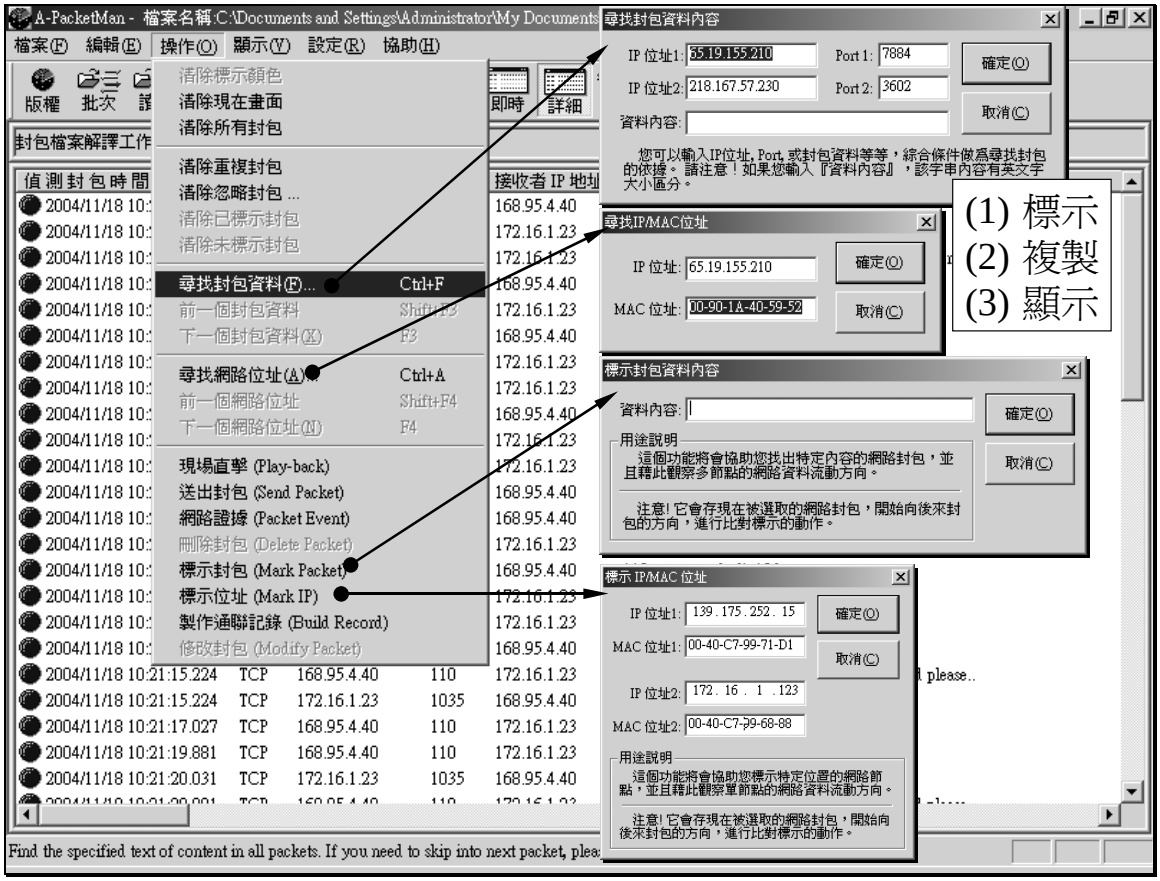
目標封包萃取歸納技巧 (The skill of analysis packets)

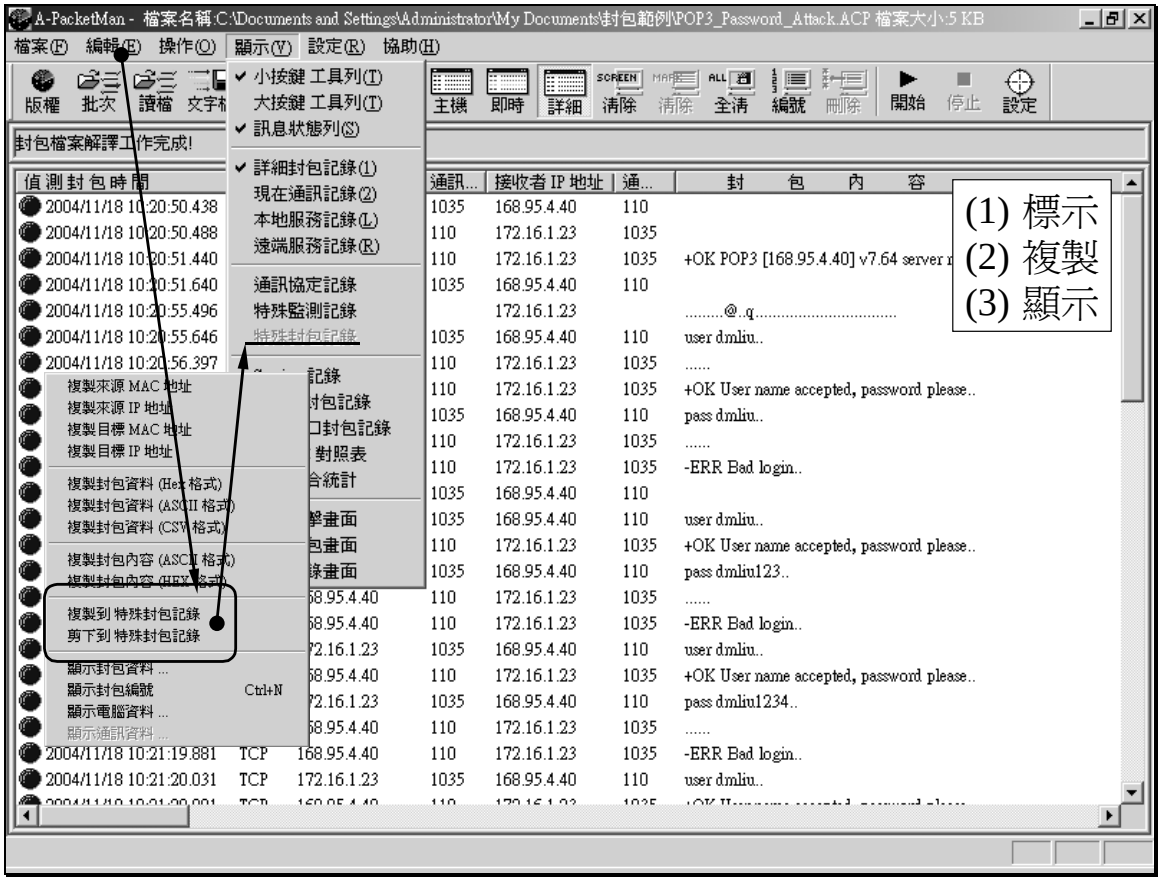
- 標示異常封包爲特殊封包(Mark Packets)
  - 根據 IP 位址
  - 根據封包內容
- 複製特殊區段封包(Copy Special Packets)
- 顯示特殊封包視窗(Display Special Packets)
- 儲存封包檔案(Save Special Packets)
- 如果已經確定爲禁止通訊的異常封包
  - A-PacketMan企業版，支援阻斷與清除的方式
  - 阻斷方式，產生相關阻斷規則，網管人員確認後，進行防火牆的指令更新。
  - 清除方式，需搭配S-Check程式，至電腦本機清除問題程式。

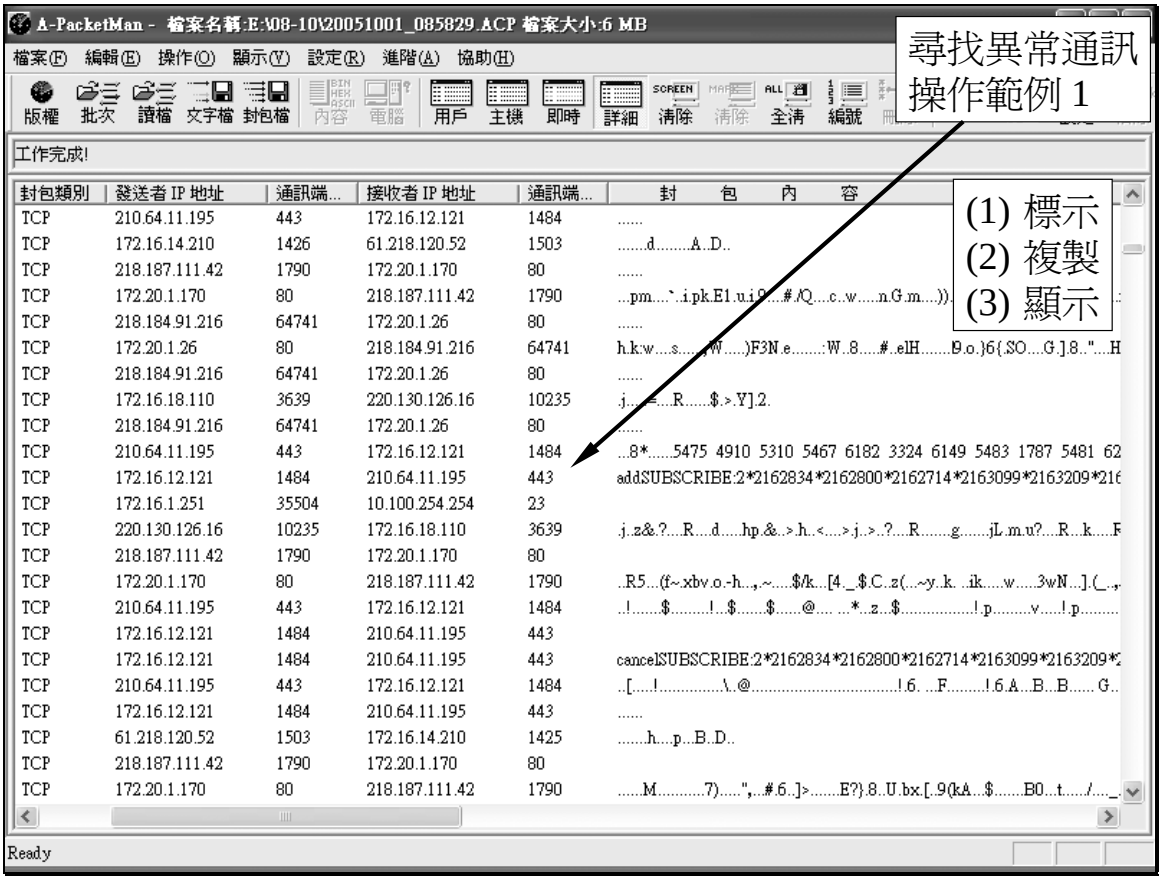
如何尋找特定IP位址或文字內容的封包? (How to search packets by IP address or payload ?)

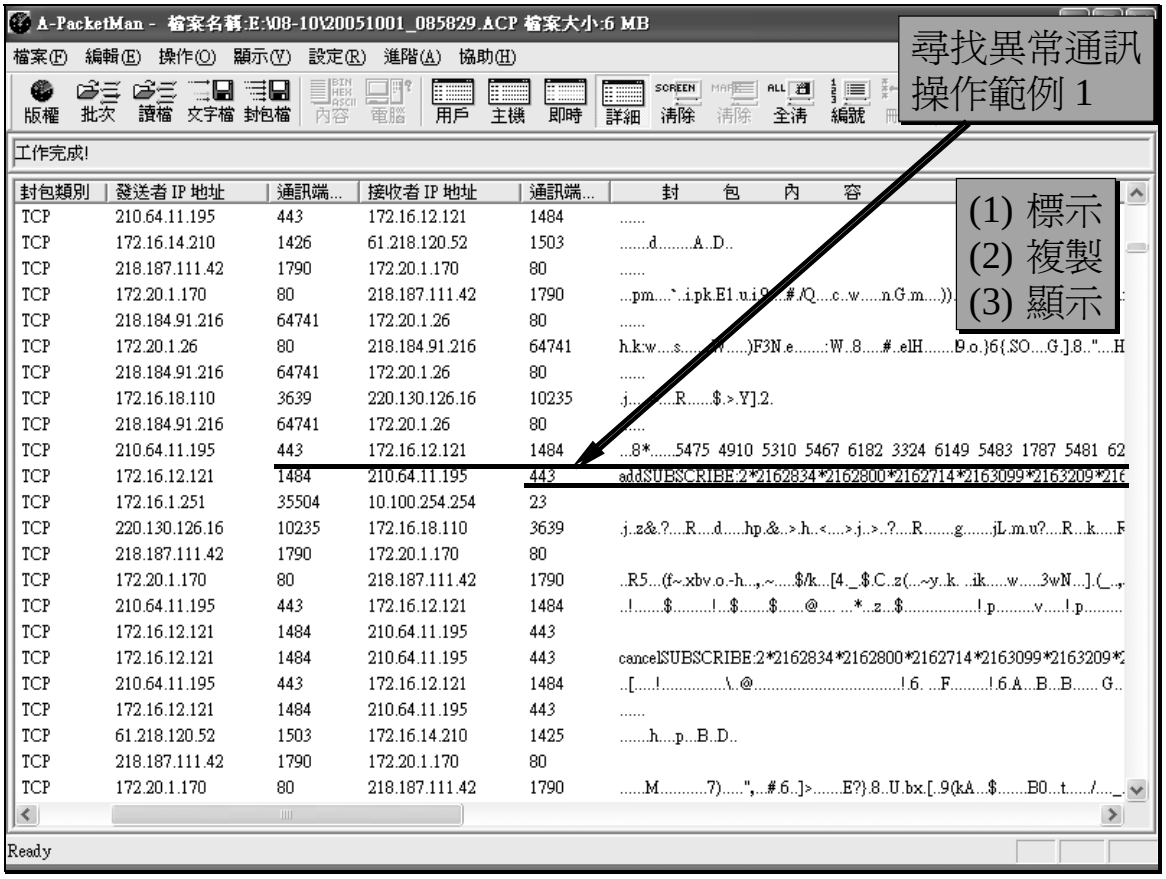


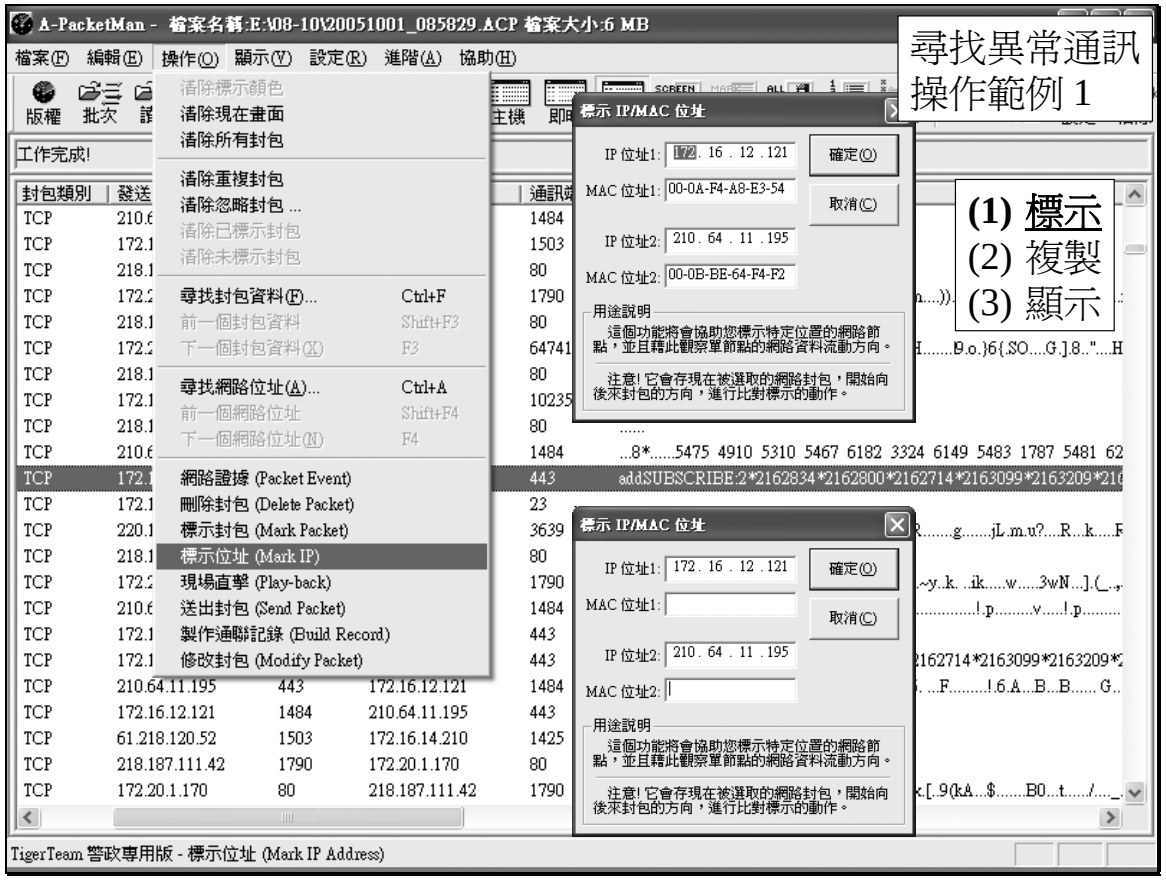

如何尋找特定IP位址或文字內容的封包?
(How to search packets by IP address or payload ?)
特定IP位址封包
尋找封包
標示封包
顯示目標封包
顯示通訊段落
© 2004-2006 copyright Jamien Liu 劉楨民

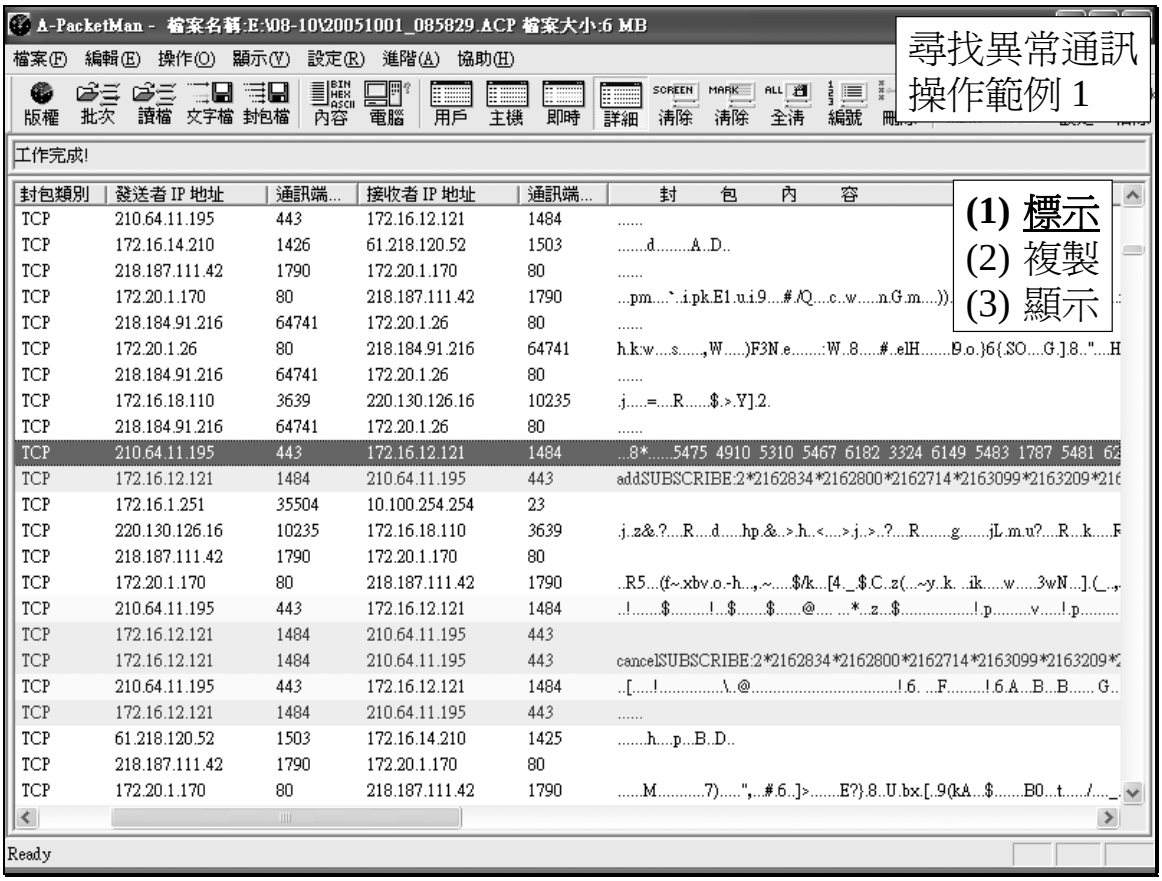

A-PacketMan - 檔案名稱:C:\Documents and Settings\Administrator\My Documents
檔案(F) 編輯(E) 操作(O) 顯示(V) 設定(R) 協助(H)
清除標示顏色
清除現在畫面
清除所有封包
清除重複封包
清除忽略封包 ...
清除已標示封包
清除未標示封包
尋找封包資料(F)... Ctrl+F
前一個封包資料 Shift+F3
下一個封包資料(X) F3
尋找網路位址(A)... Ctrl+A
前一個網路位址 Shift+F4
下一個網路位址(N) F4
現場直擊 (Play-back)
送出封包 (Send Packet)
網路證據 (Packet Event)
刪除封包 (Delete Packet)
標示封包 (Mark Packet)
標示位址 (Mark IP)
製作通聯記錄 (Build Record)
修改封包 (Modify Packet)
尋找封包資料內容
IP 位址1: 65.19.155.210
Port 1: 7884
IP 位址2: 218.167.57.230
Port 2: 3602
資料內容:
確定(O)
取消(C)
您可以輸入IP位址, Port, 或封包資料等等，綜合條件做爲尋找封包的依據。 請注意！如果您輸入『資料內容』，該字串內容有英文字大小區分。
尋找IP/MAC位址
IP 位址: 65.19.155.210
MAC 位址: 00-90-1A-40-59-52
(1) 標示
(2) 複製
(3) 顯示
標示封包資料內容
用途說明
這個功能將會協助您找出特定內容的網路封包，並且藉此觀察多節點的網路資料流動方向。
注意! 它會存現在被選取的網路封包，開始向後來封包的方向，進行比對標示的動作。
標示 IP/MAC 位址
IP 位址1: 139 . 175 . 252 . 15
MAC 位址1: 00-40-C7-99-71-D1
IP 位址2: 172 . 16 . 1 . 123
MAC 位址2: 00-40-C7-99-68-88
這個功能將會協助您標示特定位置的網路節點，並且藉此觀察單節點的網路資料流動方向。
注意! 它會存現在被選取的網路封包，開始向後來封包的方向，進行比對標示的動作。
2004/11/18 10:21:15.224 TCP 168.95.4.40 110 172.16.1.23
2004/11/18 10:21:15.224 TCP 172.16.1.23 1035 168.95.4.40
2004/11/18 10:21:17.027 TCP 168.95.4.40 110 172.16.1.23
2004/11/18 10:21:19.881 TCP 168.95.4.40 110 172.16.1.23
2004/11/18 10:21:20.031 TCP 172.16.1.23 1035 168.95.4.40
Find the specified text of content in all packets. If you need to skip into next packet, plea

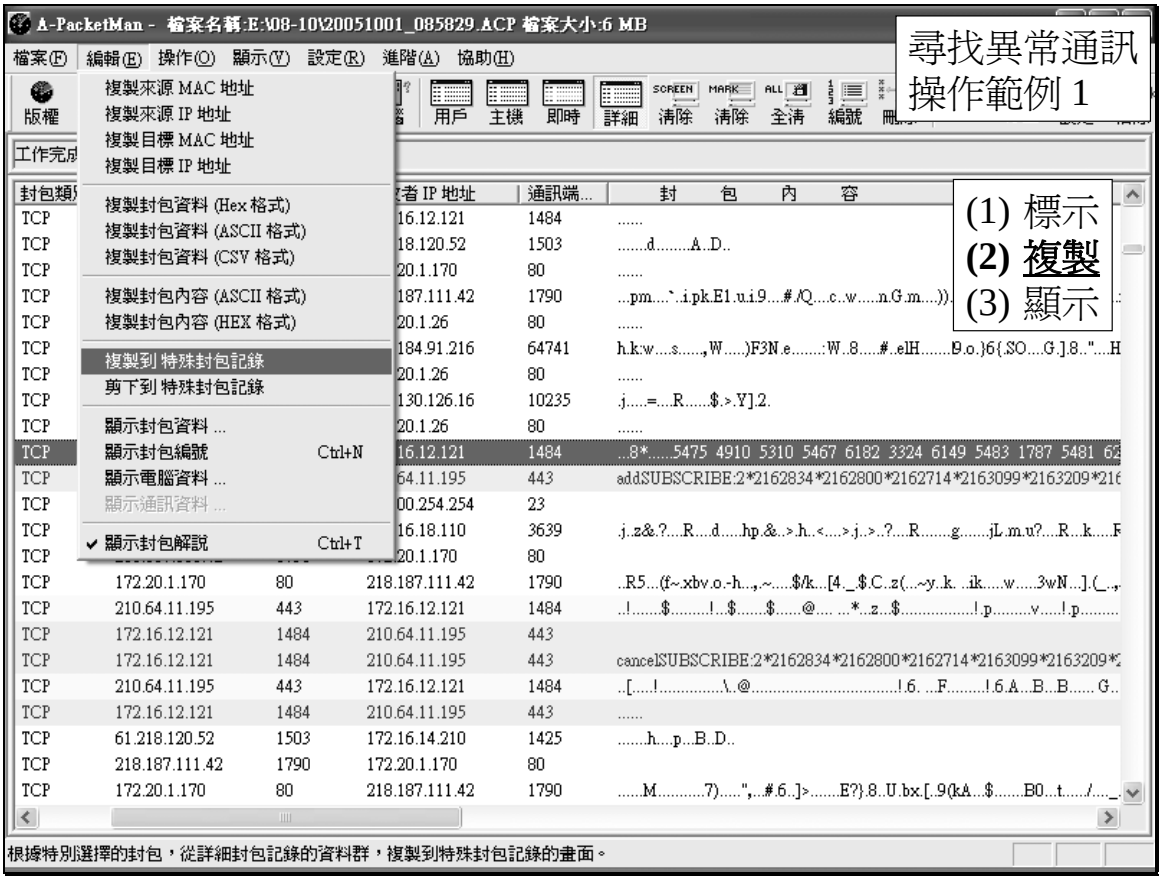




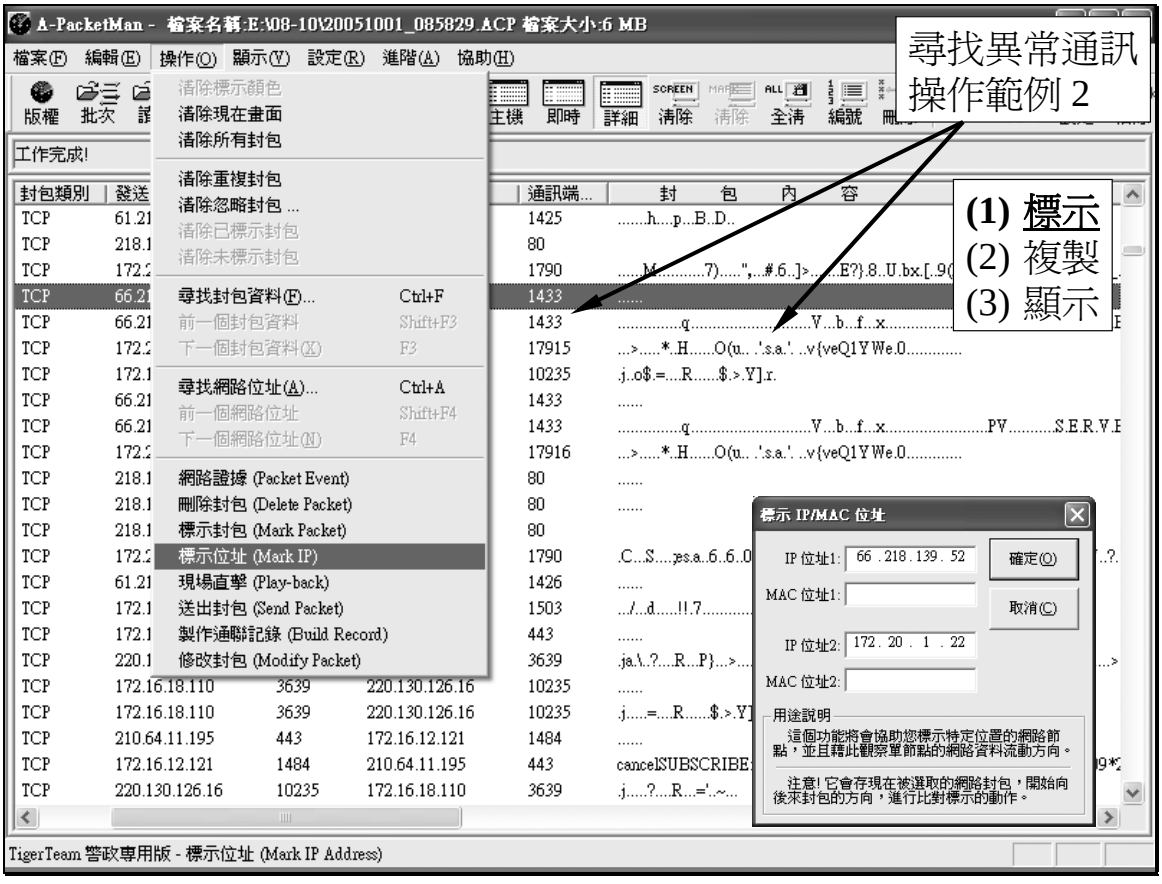

A-PacketMan - 檔案名稱:E:\08-10\20051001_085829.ACP 檔案大小:6 MB
檔案(F) 編輯(E) 操作(O) 顯示(V) 設定(R) 進階(A) 協助(H)
版權 批次 讀檔 文字檔 封包檔 內容 電腦 用戶 主機 即時 詳細 清除 清除 全清 編號
工作完成!
封包類別 發送者 IP 地址 通訊端... 接收者 IP 地址 通訊端... 封 包 內 容
TCP 210.64.11.195 443 172.16.12.121 1484
TCP 172.16.14.210 1426 61.218.120.52 1503
TCP 218.187.111.42 1790 172.20.1.170 80
TCP 172.20.1.170 80 218.187.111.42 1790
TCP 218.184.91.216 64741 172.20.1.26 80
TCP 172.20.1.26 80 218.184.91.216 64741
TCP 218.184.91.216 64741 172.20.1.26 80
TCP 172.16.18.110 3639 220.130.126.16 10235
TCP 218.184.91.216 64741 172.20.1.26 80
TCP 210.64.11.195 443 172.16.12.121 1484 ...8*.....5475 4910 5310 5467 6182 3324 6149 5483 1787 5481 62
TCP 172.16.12.121 1484 210.64.11.195 443 addSUBSCRIBE:2*2162834*2162800*2162714*2163099*2163209*216
TCP 172.16.1.251 35504 10.100.254.254 23
TCP 220.130.126.16 10235 172.16.18.110 3639
TCP 218.187.111.42 1790 172.20.1.170 80
TCP 172.20.1.170 80 218.187.111.42 1790
TCP 210.64.11.195 443 172.16.12.121 1484
TCP 172.16.12.121 1484 210.64.11.195 443
TCP 172.16.12.121 1484 210.64.11.195 443 cancelSUBSCRIBE:2*2162834*2162800*2162714*2163099*2163209*2
TCP 210.64.11.195 443 172.16.12.121 1484
TCP 172.16.12.121 1484 210.64.11.195 443
TCP 61.218.120.52 1503 172.16.14.210 1425
TCP 218.187.111.42 1790 172.20.1.170 80
TCP 172.20.1.170 80 218.187.111.42 1790
Ready
尋找異常通訊
操作範例 1
(1) 標示
(2) 複製
(3) 顯示

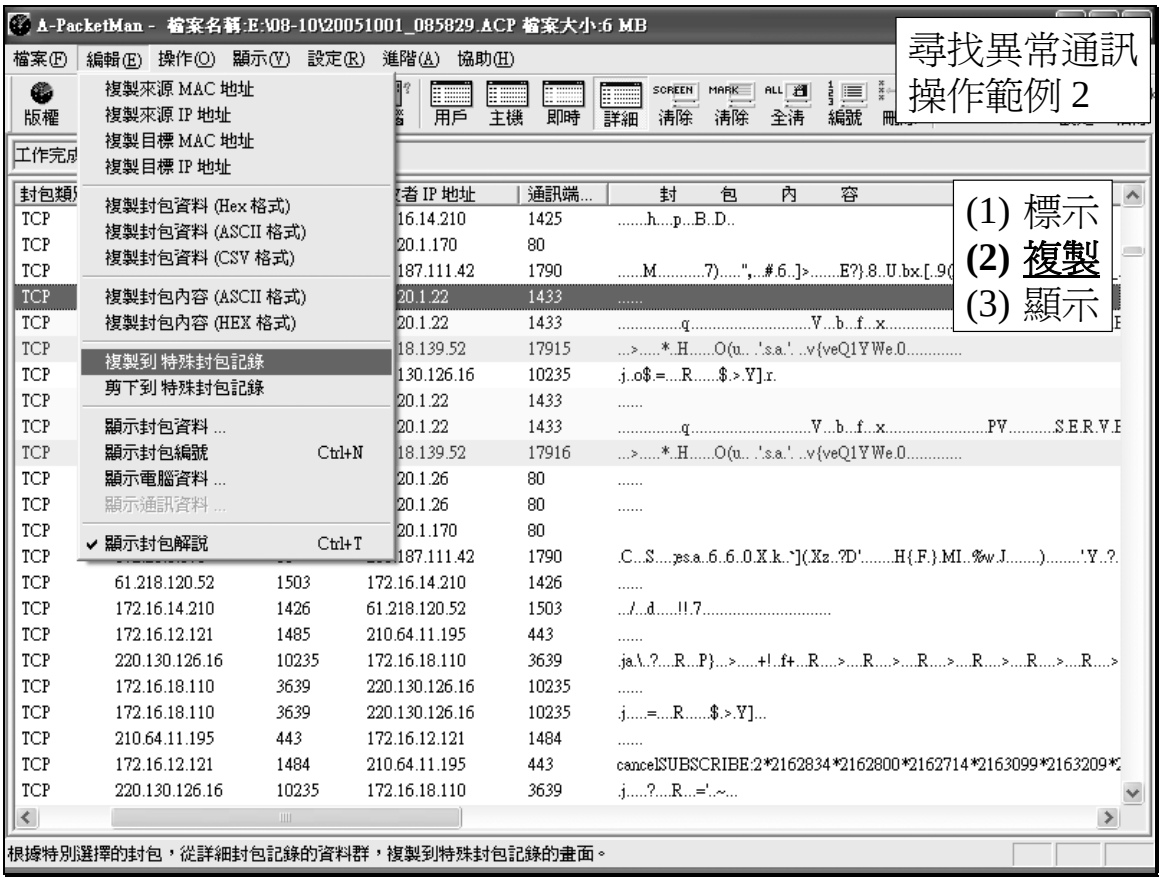

A-PacketMan - 檔案名稱:E:\08-10\20051001_085829.ACP 檔案大小:6 MB
檔案(F) 編輯(E) 操作(O) 顯示(V) 設定(R) 進階(A) 協助(H)
清除標示顏色
清除現在畫面
清除所有封包
清除重複封包
清除忽略封包 ...
清除已標示封包
清除未標示封包
尋找封包資料(F)... Ctrl+F
前一個封包資料 Shift+F3
下一個封包資料(X) F3
尋找網路位址(A)... Ctrl+A
前一個網路位址 Shift+F4
下一個網路位址(N) F4
網路證據 (Packet Event)
刪除封包 (Delete Packet)
標示封包 (Mark Packet)
標示位址 (Mark IP)
現場直擊 (Play-back)
送出封包 (Send Packet)
製作通聯記錄 (Build Record)
修改封包 (Modify Packet)
標示 IP/MAC 位址
IP 位址1: 172 . 16 . 12 . 121
MAC 位址1: 00-0A-F4-A8-E3-54
IP 位址2: 210 . 64 . 11 . 195
MAC 位址2: 00-0B-BE-64-F4-F2
確定(O)
取消(C)
用途說明
這個功能將會協助您標示特定位置的網路節點，並且藉此觀察單節點的網路資料流動方向。
注意! 它會存現在被選取的網路封包，開始向後來封包的方向，進行比對標示的動作。
TigerTeam 警政專用版 - 標示位址 (Mark IP Address)
尋找異常通訊
操作範例 1
(1) 標示
(2) 複製
(3) 顯示

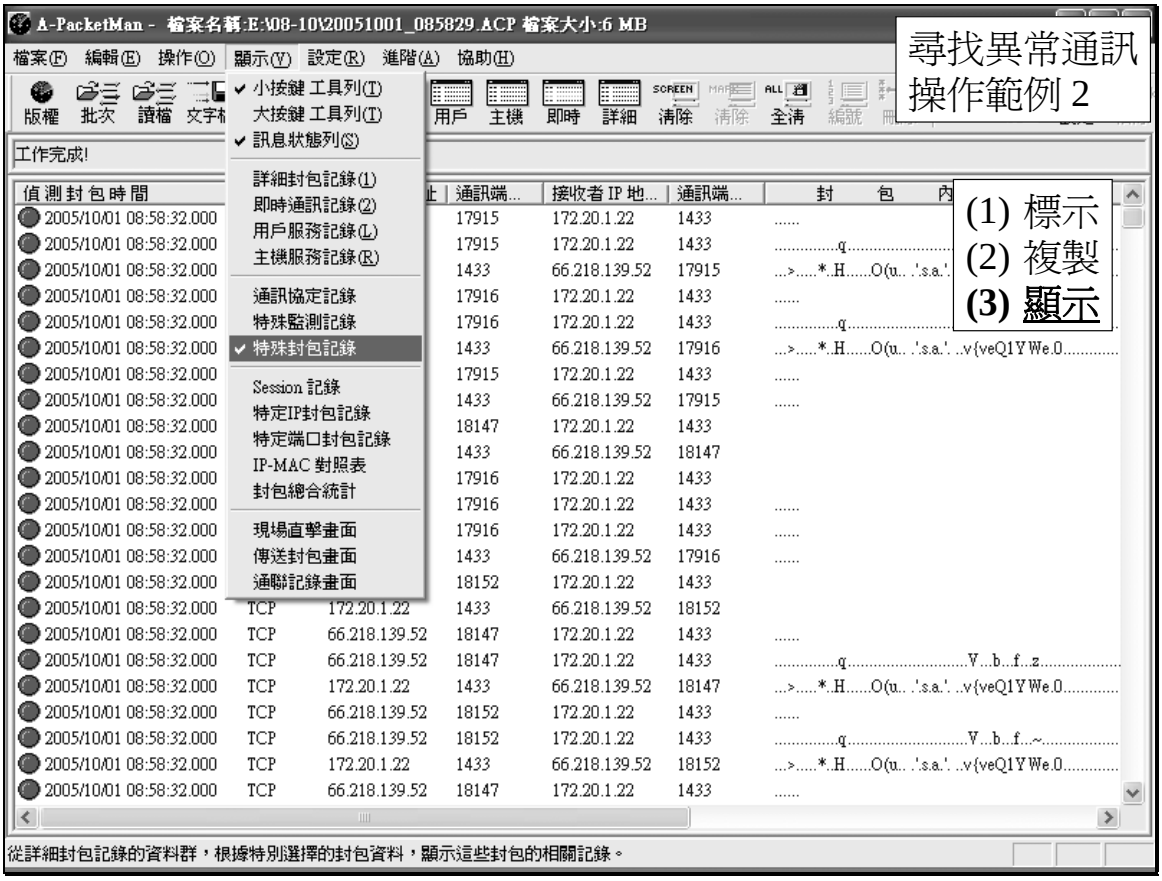




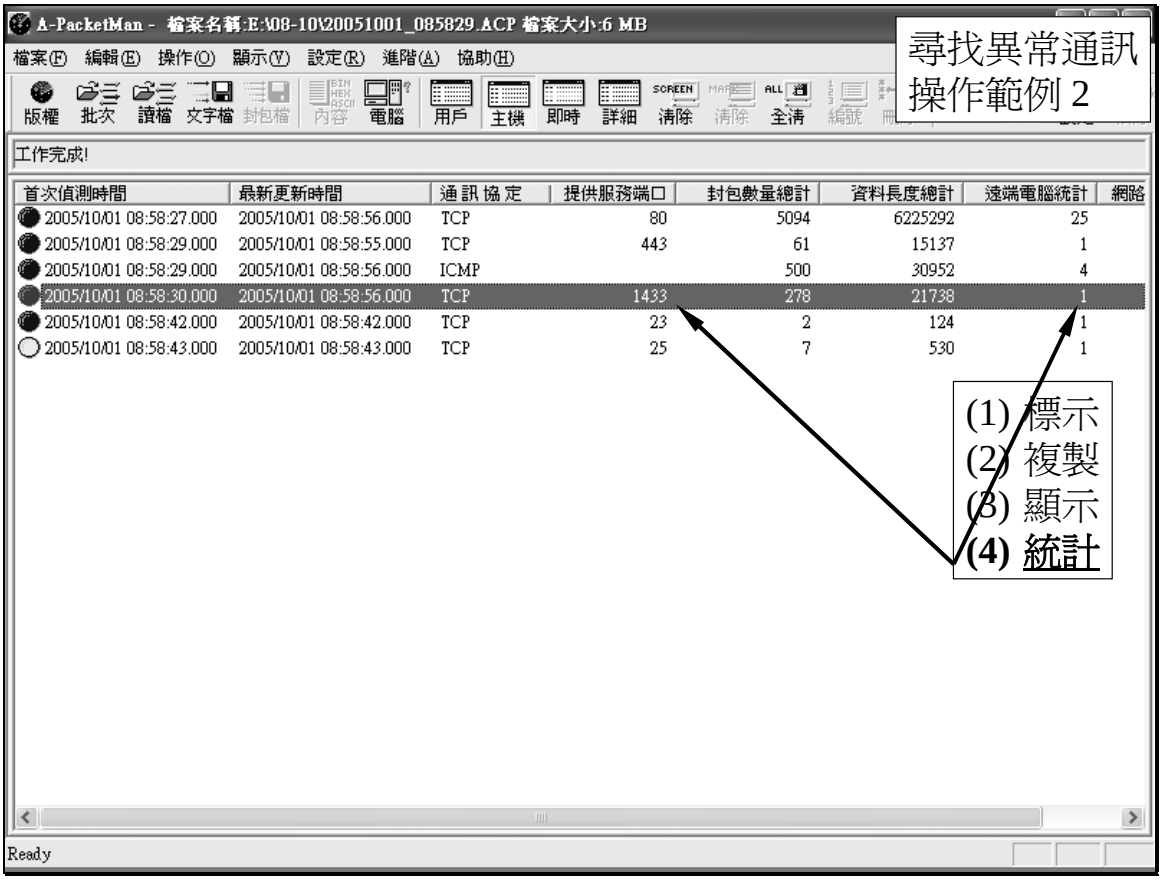

尋找異常通訊
操作範例 1
(1) 標示
(2) 複製
(3) 顯示
A-PacketMan - 檔案名稱:E:\08-10\20051001_085829.ACP 檔案大小:6 MB
檔案(F) 編輯(E) 操作(O) 顯示(V) 設定(R) 進階(A) 協助(H)
小按鍵 工具列(T)
大按鍵 工具列(T)
訊息狀態列(S)
詳細封包記錄(1)
即時通訊記錄(2)
用戶服務記錄(L)
主機服務記錄(R)
通訊協定記錄
特殊監測記錄
特殊封包記錄
Session 記錄
特定IP封包記錄
特定端口封包記錄
IP-MAC 對照表
封包總合統計
現場直擊畫面
傳送封包畫面
通聯記錄畫面
工作完成!
從詳細封包記錄的資料群，根據特別選擇的封包資料，顯示這些封包的相關記錄。

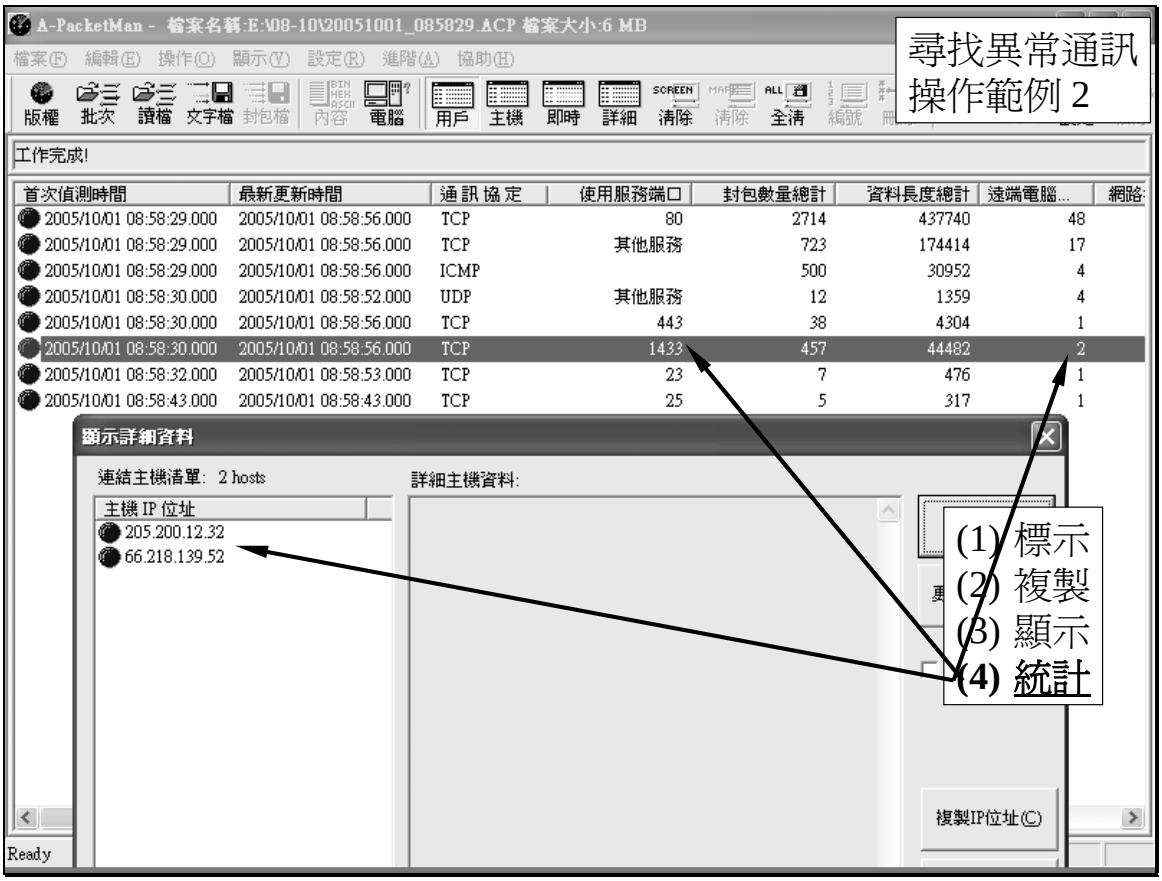

尋找異常通訊
操作範例 2
(1) 標示
(2) 複製
(3) 顯示
A-PacketMan - 檔案名稱:E:\08-10\20051001_085829.ACP 檔案大小:6 MB
檔案(F) 編輯(E) 操作(O) 顯示(V) 設定(R) 進階(A) 協助(H)
清除標示顏色
清除現在畫面
清除所有封包
清除重複封包
清除忽略封包 ...
清除已標示封包
清除未標示封包
尋找封包資料(F)... Ctrl+F
前一個封包資料 Shift+F3
下一個封包資料(X) F3
尋找網路位址(A)... Ctrl+A
前一個網路位址 Shift+F4
下一個網路位址(N) F4
網路證據 (Packet Event)
刪除封包 (Delete Packet)
標示封包 (Mark Packet)
標示位址 (Mark IP)
現場直擊 (Play-back)
送出封包 (Send Packet)
製作通聯記錄 (Build Record)
修改封包 (Modify Packet)
標示 IP/MAC 位址
IP 位址1: 66 . 218 . 139 . 52
MAC 位址1:
IP 位址2: 172 . 20 . 1 . 22
MAC 位址2:
確定(O)
取消(C)
用途說明
這個功能將會協助您標示特定位置的網路節點，並且藉此觀察單節點的網路資料流動方向。
注意! 它會存現在被選取的網路封包，開始向後來封包的方向，進行比對標示的動作。
工作完成!
TigerTeam 警政專用版 - 標示位址 (Mark IP Address)






尋找異常通訊
操作範例 2
A-PacketMan - 檔案名稱:E:\08-10\20051001_085829.ACP 檔案大小:6 MB
檔案(F) 編輯(E) 操作(O) 顯示(V) 設定(R) 進階(A) 協助(H)
版權 批次 讀檔 文字檔 封包檔 內容 電腦 用戶 主機 即時 詳細 清除 清除 全清 編號
工作完成!
偵測封包時間 封包類... 發送者IP地址 通訊端... 接收者IP地... 通訊端... 封包內容
2005/10/01 08:58:32.000 TCP 66.218.139.52 17915 172.20.1.22 1433 .....
Set the detail of Capture Network Packets
基本設定
設定封包擷取來源
擷取封包的優先順序
設定封包處理參數
忽略無效封包
其他選項設定
進階設定
資料設定
封包處理
建立分析樹，比對封包資料，尋找符合模式。
累計所有封包的結果 (即時現況 畫面)。
累計遠端服務使用比率: 1433
累計本地服務使用比率 1433
自動累計 TCP/UDP > 1024 的服務比率。
採用微量CPU計算使用
建立 TCP Session 追蹤表。
製作 IP-MAC 對照表。
分析監控對象(指定IP位址)的進出方向。(請選擇 指定擷取封包來源的
分析封包通訊範圍屬於內部或外部網路。
設定 路由器與交換器(
新偵測的封包要放置到最前面的項目。
解譯網路封包檔頭的旗標數值內容。
簡化通訊(即時現況)的電腦資料顯示項目。
少於10 Byte資料的封包，忽略不顯示記錄。
確定 取消 套用(A)
Ready
(1) 標示
(2) 複製
(3) 顯示
(4) 統計


尋找異常通訊
操作範例 2
A-PacketMan - 檔案名稱:E:\08-10\20051001_085829.ACP 檔案大小:6 MB
檔案(F) 編輯(E) 操作(O) 顯示(V) 設定(R) 進階(A) 協助(H)
版權 批次 讀檔 文字檔 封包檔 內容 電腦 用戶 主機 即時 詳細 清除 清除 全清 編號
工作完成!
首次偵測時間 最新更新時間 通訊協定 提供服務端口 封包數量總計 資料長度總計 遠端電腦統計 網路
2005/10/01 08:58:27.000 2005/10/01 08:58:56.000 TCP 80 5094 6225292 25
2005/10/01 08:58:29.000 2005/10/01 08:58:55.000 TCP 443 61 15137 1
2005/10/01 08:58:29.000 2005/10/01 08:58:56.000 ICMP 500 30952 4
2005/10/01 08:58:30.000 2005/10/01 08:58:56.000 TCP 1433 278 21738 1
2005/10/01 08:58:42.000 2005/10/01 08:58:42.000 TCP 23 2 124 1
2005/10/01 08:58:43.000 2005/10/01 08:58:43.000 TCP 25 7 530 1
Ready
(1) 標示
(2) 複製
(3) 顯示
(4) 統計



如何進一步學習封包分析技巧與累積經驗?

- 異常網路封包的危害判斷準則
  - 先排除所有已知的標準通訊協定, HTTP/SMTP/POP3/DNS/CIFS/MSN…
  - 內網或外網 (通訊雙方的IP位址是否爲Internet位址?)
  - 禁止或開放 (這類網路服務是否可以執行?)
  - 單向或雙向 (通訊雙方有無互相傳送資料?)
- 異常通訊的蒐證與分析步驟
  - 標示 (標示位址或是標示封包內容)
  - 複製 (將已經標示顏色的封包, 複製到 特殊封包視窗)
  - 顯示 (切換顯示畫面爲 特殊封包視窗)
  - 統計 (option, 如果要進一步瞭解攻擊來源或是受害對象)
- Q&A
- 學員論壇
  - http://forum.AntiHacker.com.tw
  - http://forum.DiamondInfoTech.com.tw

即時封包鑑識工具對於網路管理人員的益處

- 瞭解DMZ主機的運作情況
- 掌握防火牆的設定現況
- 監測使用者異常網路行爲
- 偵測病毒蠕蟲感染程度
- 分析可疑木馬後門程式的通訊
- 避免GSN或ISP通知異常，事先掌握情況
- 直接將異常(未知攻擊)通訊，轉換成爲已知規則，輸出爲Firewall, IDS, IDP/IPS的規則
  - 產生 Snort, FortiGate, IpTable 的偵測阻擋規則